Cisco Service Control Application for Broadband ユーザ ガイド

Cisco Service Control Application for Broadband User Guide

リリース 3.6.x
2010 年 3 月 28 日

Text Part Number: OL-21064-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Service Control Application for Broadband ユーザ ガイド

CONTENTS

このマニュアルについて

はじめに

ここでは、『*Cisco Service Control Application for Broadband ユーザ ガイド*』の対象読者、構成、ドキュメントの表記法、マニュアルの入手方法、およびテクニカル サポートについて説明します。

このガイドは、Service Control ソリューション、Service Control Engine（SCE）プラットフォーム、および関連コンポーネントの概念に関する基本的な知識があることを前提としています。

マニュアルの変更履歴

表 1 は、このマニュアルにおける変更内容を記録したものです。

表 1　　マニュアルの変更履歴

リビジョン	Cisco Service Control リリースおよび日付	変更点
OL-21064-01-J	リリース 3.6.x 2010 年 3 月 28 日	このマニュアルの初版 「Service Configuration Editor の使用方法：トラフィックの制御」（P.9-1）の「クォータの管理」（P.9-76）に示されているクォータ コンフィギュレーションの変更に関する説明を更新しました。

マニュアルの構成

表 2 に、このマニュアルの構成を示します。

表 2　　マニュアルの構成

セクション	タイトル	説明
1	「Cisco Service Control の概要」（P.1-1）	Service Control ソリューションの概要を示します。
2	「システムの概要」（P.2-1）	Service Control ソリューションの機能的な概要を示します。
3	「トラフィック処理の概要」（P.3-1）	Service Control ソリューションの技術的な概要を示します。
4	「使用する前に」（P.4-1）	SCA BB のインストール手順およびアップグレード手順を説明し、ツールの集合体としての Console について説明します。
5	「Network Navigator の使用方法」（P.5-1）	Service Control ソリューションの一部となる装置のモデルをネットワーク ナビゲータを用いて作成し、これらの装置をリモートで管理する方法を説明します。
6	「Service Configuration Editor の使用方法」（P.6-1）	Service Configuration Editor を使用してサービス コンフィギュレーションを管理する方法を説明します。
7	「Service Configuration Editor の使用方法：トラフィックの分類」（P.7-1）	サービス コンフィギュレーションを使用してトラフィックを分類する方法を説明します。
8	「Service Configuration Editor の使用方法：トラフィックのアカウンティングとレポート」（P.8-1）	サービス コンフィギュレーションを使用してトラフィックをレポートする方法を説明します。
9	「Service Configuration Editor の使用方法：トラフィックの制御」（P.9-1）	サービス コンフィギュレーションを使用してトラフィックを管理する方法を説明します。
10	「Service Configuration Editor の使用方法：その他のオプション」（P.10-1）	Service Configuration Editor のオプションを説明します。
11	「Subscriber Manager の GUI ツールの使用方法」（P.11-1）	SM GUI ツールを使用して SCMS-SM データベースにサブスクライバを設定する方法を説明します。
12	「Signature Editor の使用方法」（P.12-1）	Signature Editor ツールを使用して SCA BB にファイルを作成し、プロトコルをアップデートする方法を説明します。
13	「その他の管理ツールおよびインターフェイス」（P.13-1）	SCA BB で使用できるその他のツールについて説明します。

関連資料

この『*Cisco Service Control Application for Broadband ユーザ ガイド*』は、次のシスコ製品のマニュアルと併せてご利用ください。

- 『*Cisco Service Control Application for Broadband Reference Guide*』
- 『*Cisco Service Control Application for Broadband Service Configuration API Programmer Guide*』
- 『*Cisco Service Control Management Suite Collection Manager User Guide*』
- 『*Cisco Service Control Management Suite Subscriber Manager User Guide*』
- 『*Cisco Service Control Application Reporter User Guide*』
- 次の SCE プラットフォーム インストレーションおよびコンフィギュレーション ガイド
  - 『*Cisco SCE 1000 2xGBE Installation and Configuration Guide*』
  - 『*Cisco SCE 2000 Installation and Configuration Guide*』
  - 『*Cisco SCE8000 10GBE Installation and Configuration Guide*』
  - 『*Cisco SCE8000 GBE Installation and Configuration Guide*』
- 『*Cisco SCE 2000 and SCE 1000 CLI Command Reference*』
- 『*Cisco SCE8000 CLI Command Reference*』
- 『*Cisco SCE 2000 and SCE 1000 Software Configuration Guide*』
- 『*Cisco SCE8000 10GBE Software Configuration Guide*』
- 『*Cisco SCE8000 10GBE Software Configuration Guide*』

表記法

このマニュアルでは、次の表記法を使用しています。

表 3　　表記法

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは、**太字**で示しています。
イタリック体	マニュアルのタイトル、新出用語または強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string と見なされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注）　「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント　「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意　「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス　「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

警告　**「*警告*」の意味です。人身事故を予防するための注意事項が記述されています。**

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

Cisco Service Control の概要

はじめに

この章では、Cisco Service Control ソリューションの概要を示します。Cisco Service Control の概念および機能について説明します。

また、Service Control Engine（SCE）プラットフォームのハードウェア機能と、トータルな Cisco Service Control ソリューションをともに構成するシスコ固有のアプリケーションについても簡単に説明します。

Cisco Service Control ソリューション

Cisco Service Control ソリューションは、さまざまなサービス コントロールの課題を解決するハードウェアおよび特定のソフトウェア ソリューションの組み合わせで実現されます。サービス プロバイダーは SCE プラットフォームを使用してインターネットおよび IP トラフィックの分類、分析、および制御をサポートできます。

Service Control により、サービス プロバイダーは次のことが可能になります。

- 既存インフラストラクチャに投資できます。
- マルチギガビット ワイヤ回線速度で IP ネットワーク トラフィックを分析、課金、および制御できます。
- 余裕のあるコンテンツベース サービスを識別および実現できます。

電気通信業界の低迷が示すように、IP サービス プロバイダーは、利益を上げるためにビジネス モデルを再編する必要があります。プロバイダーは巨大なデータ リンクを構築するために莫大な資金を投入してきたため、多額の負債を抱え、コストは上昇しました。その一方で、アクセスおよび帯域幅という商品の価格は継続的に下落し、利益は消滅しました。現在、サービス プロバイダーは、付加価値のあるサービスを提供して、ネットワーク上で稼動するトラフィックやサービスからより多くの収入を得る必要があることを認識しています。

Cisco Service Control ソリューションを使用すれば、サービス プロバイダーは詳細なモニタリングと精度、リアルタイム制御、およびサービス提供時のサービス認識によって、IP サービスから利益を得ることができます。

ブロードバンド サービス プロバイダー向けのサービス コントロール

個人宅およびビジネス向けのユーザをターゲットとするアクセス技術（DSL、ケーブル、モバイル端末など）を提供するサービス プロバイダーは、強化された IP サービスによって差別化を図りながら、既存インフラストラクチャから最大限の収益を上げる新しい方法を見つける必要があります。

Service Control Application for Broadband を使用すると、既存ネットワークにサービス インテリジェンスおよび制御のレイヤが追加され、次のことが可能になります。

- 容量計画のための、サブスクライバ レベルおよび集約レベルでのネットワーク トラフィックのレポートおよび分析
- カスタマーが直感的に操作できる階層型アプリケーション サービスの提供、およびアプリケーションの Service Level Agreement（SLA; サービス レベル契約）の保証
- 各タイプのカスタマー、コンテンツ、またはアプリケーション向けのさまざまなサービス レベルの実装
- Acceptable Use Policy（AUP; アクセプタブル ユース ポリシー）に違反しているネットワーク悪用者の識別
- ピアツーピア トラフィック、NNTP（ニュース）トラフィック、およびスパム悪用者の識別および管理
- AUP の実施
- 既存のネットワーク要素、Business Support System（BSS）、および Operational Support System（OSS; オペレーション サポート システム）と Service Control ソリューションとの統合の簡素化

Cisco Service Control の機能

Cisco Service Control ソリューションの中心は、ネットワーク ハードウェア デバイスである Service Control Engine（SCE）です。SCE プラットフォームの中心機能は Service Control ソリューションを実現する幅広いアプリケーションをサポートしており、次の機能があります。

- サブスクライバおよびアプリケーション アウェアネス：アプリケーションレベルで IP トラフィックを調査することにより、サブスクライバ単位で使用率およびコンテンツを詳細かつリアルタイムに認識および制御することができます。
  - サブスクライバ アウェアネス：IP フローと特定のサブスクライバを対応付けて、SCE プラットフォーム経由でトラフィックを送信している各サブスクライバの状態を維持したり、このサブスクライバ トラフィックに適切なポリシーを適用することができます。

    サブスクライバ アウェアネス機能を実現するには、DHCP や RADIUS サーバなどのサブスクライバ管理リポジトリと統合するか、RADIUS または DHCP トラフィックをスニフィングします。
  - アプリケーション アウェアネス：アプリケーション プロトコル レイヤ（レイヤ 7）までのトラフィックを認識および分析できます。

    バンドルされたフローを使用して実装されたアプリケーション プロトコル（制御およびデータ フローを使用して実装された FTP など）の場合、SCE プラットフォームはフロー間のバンドリング接続を認識して、適切に処理します。
- アプリケーションレイヤでのステートフルなリアルタイム トラフィック制御：詳細な BandWidth（BW; 帯域幅）の測定やシェーピング、クォータ管理とリダイレクション、アプリケーション レイヤでのステートフルなリアルタイム トラフィック トランザクション処理の利用など、高度な制御機能を実行できます。そのためには、適応性の高いプロトコルおよびアプリケーション レベルのインテリジェンスが必要です。

- プログラマビリティ：新規プロトコルを迅速に追加し、サービス プロバイダー環境の新規サービスおよびアプリケーションに適応させることができます。プログラマビリティを実現するには、Cisco Service Modeling Language（SML）を使用します。

  プログラマビリティにより、新規サービスを迅速に配置し、ネットワーク、アプリケーション、またはサービスの拡張に合わせて容易にアップグレードできます。

- 強固で柔軟性のあるバックオフィス統合：サービス プロバイダーで、プロビジョニング システム、サブスクライバ リポジトリ、課金システム、OSS システムなどの既存のサード パーティ製システムと統合できます。SCE には、マニュアルが整備された一連の公開 API が用意されているので、迅速な統合プロセスを実現できます。

- スケーラブルで高性能なサービス エンジン：以上の操作をワイヤ スピードで実行できる機能です。

SCE プラットフォームの説明

プログラマブル ネットワーク デバイスである SCE ファミリには、IP トラフィックのアプリケーション レイヤ ステートフルフロー インスペクションを実行したり、設定可能な規則に基づいてトラフィックを制御する機能があります。SCE プラットフォーム デバイスでは ASIC コンポーネントおよび Reduced Instruction Set Computer（RISC; 縮小命令セット コンピュータ）プロセッサを利用します。これにより、パケットをカウントするだけでなく、ネットワーク トラフィックの内容を詳細に調べることができます。

SCE プラットフォーム デバイスの特徴は次のとおりです。

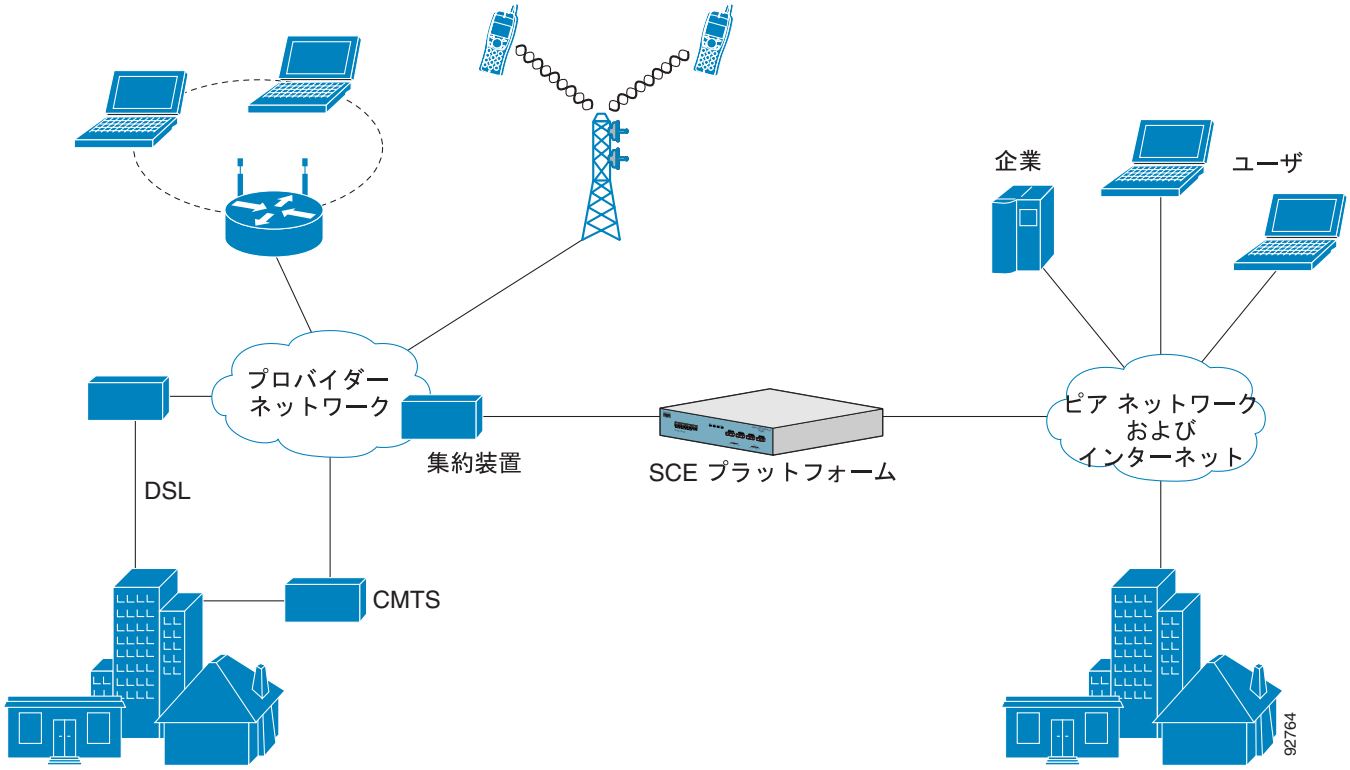
- プログラム可能です。
- 双方向トラフィック フローのステートフル インスペクションを実行したり、これらのフローとユーザ所有権を対応付けることができます。
- ネットワーク使用率をリアルタイムで分類できます。この分類は SCE プラットフォームの高度なトラフィック制御および帯域幅シェーピング機能の基礎となります。

一般的な帯域幅シェーパ機能が適用されない条件下でも、SCE プラットフォームは次のような制御およびシェーピング オプションを提供します。

- レイヤ 7 のワイヤ速度でのステートフル パケット インスペクションおよび分類
- 次のような 600 を超えるプロトコルおよびアプリケーションの確実なサポート
  - 一般 : HTTP、HTTPS、FTP、Telnet、Network News Transfer Protocol（NNTP）、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）、Post Office Protocol 3（POP3）、Internet Message Access Protocol（IMAP）、Wireless Application Protocol（WAP）など
  - Peer-to-Peer（P2P; ピアツーピア）ファイル共有 : FastTrack-KazaA、Gnutella、BitTorrent、Winny、Hotline、eDonkey、DirectConnect、Piolet など
  - P2P VoIP : Skype、Skinny、DingoTel など
  - ストリーミングおよびマルチメディア : Real Time Streaming Protocol（RTSP）、Session Initiation Protocol（SIP）、HTTP ストリーミング、Real Time Protocol（RTP）/Real Time Control Protocol（RTCP）など
- プログラム可能なシステム コアによる、柔軟性のあるレポートおよび帯域幅の制御
- トランスペアレントなネットワークおよび BSS/OSS と既存ネットワークの統合
- サブスクライバ アウェアネスによる、トラフィックおよび使用率と特定のカスタマーとの関連付け

図 1-1 に、ネットワーク内の一般的な SCE プラットフォーム配置例を示します。

図 1-1　ネットワーク内の SCE プラットフォーム



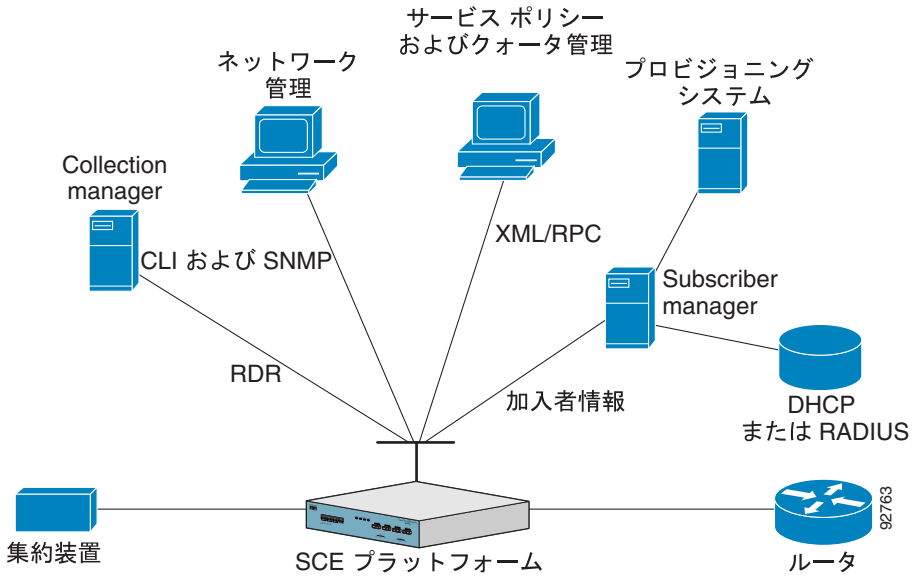
管理および収集

Service Control ソリューションには、Service Control ソリューションのあらゆる面を管理する、次の管理コンポーネントを備えた完全な管理インフラストラクチャが含まれています。

- ネットワーク管理
- サブスクライバ管理
- Service Control 管理

これらの管理インターフェイスの設計目的は、一般的な管理基準に準拠して、既存 OSS インフラストラクチャとの統合を容易にすることです（図 1-2 を参照）。

図 1-2　Service Control 管理インフラストラクチャ



ネットワーク管理

Cisco Service Control ソリューションは、完全な Fault, Configuration, Accounting, Performance, Security（FCAPS; 障害、設定、アカウンティング、パフォーマンス、セキュリティ）管理を実現します。

ネットワーク管理用に 2 つのインターフェイスが用意されています。

- Command-Line Interface（CLI; コマンドライン インターフェイス）: Console ポートまたは Telnet 接続でアクセスできます。設定およびセキュリティ機能に使用します。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）: SNMP トラップによる障害管理とパフォーマンス モニタリング機能を実行します。

サブスクライバ管理

Cisco Service Control Application for Broadband（SCA BB）ではサブスクライバごとに異なるポリシーを実行してサブスクライバ単位で使用状況を追跡しますが、Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）は OSS と SCE プラットフォームをブリッジングするミドルウェア コンポーネントとして使用されることがあります。サブスクライバ情報は SM データベースに格納され、実際のサブスクライバ配置に従って、複数のプラットフォーム間で配信できます。

SM ではネットワーク ID とサブスクライバ ID がマッピングされ、サブスクライバ アウェアネス機能が実現されます。SM は RADIUS サーバや DHCP サーバなどの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）デバイスと統合された専用統合モジュールを使用して、サブスクライバ情報を取得します。

サブスクライバ情報は、次の 2 つの方法のいずれかで取得できます。

- プッシュ モード：サブスクライバがログオンすると、SM はサブスクライバ情報を SCE プラットフォームに自動的にプッシュします。
- プル モード：SM は、SCE プラットフォームからのクエリーに答えて、サブスクライバ情報を SCE プラットフォームに送信します。

サービス コンフィギュレーション管理

サービス コンフィギュレーション管理は、Service Control アプリケーションの一般的なサービス定義を設定する機能です。トラフィック分類、アカウンティングとレポーティング、および制御を設定するサービス コンフィギュレーション ファイルが作成され、SCE プラットフォームに適用されます。SCA BB アプリケーションにより、これらのコンフィギュレーション ファイルは SCE プラットフォームに自動的に配置されます。こうした標準的なアプローチにより、大規模なネットワークでも複数の装置を簡単に管理できます。

Service Control には、これらのファイルを編集および作成するための GUI と、ファイルの作成を自動化するための一連の API が備わっています。

データ収集

データ収集は次のように実行されます。

1. SCE プラットフォームのすべての分析およびデータ処理機能により、Raw Data Record（RDR; 未加工データ レコード）が生成されます。SCE プラットフォームはこれを、単純な TCP ベースのプロトコル（RDR プロトコル）を使用して転送します。
2. RDR は Cisco Service Control Management Suite Collection Manager で処理されます。
3. Collection Manager ソフトウェアは、1 つまたは複数の SCE プラットフォームから RDR を受け取る収集システムを実装したものです。このソフトウェアはこれらのレコードを収集し、いずれかのアダプタで処理します。各アダプタは、RDR に対して特定のアクションを実行します。

RDR には、システムの設定に応じてさまざまな情報および統計情報が格納されます。RDR の 3 つの主要なカテゴリは次のとおりです。

- Transaction RDR：トランザクションがネットワーク トラフィック内で検出された単一イベントである場合に、*トランザクション*ごとに生成されるレコード。トランザクションの ID は、特定のアプリケーションおよびプロトコルによって決まります。
- Subscriber Usage RDR：定義期間中にサブスクライバによって生成されたトラフィックを記述する、サブスクライバ単位で生成されるレコード。
- Link RDR：定義期間中にリンク上で伝送されるトラフィックを記述する、リンク単位で生成されるレコード。

CHAPTER 2

システムの概要

はじめに

Cisco Service Control Application for Broadband（SCA BB）は、ブロードバンド サービス プロバイダーがネットワーク トラフィックの状況を把握し、ネットワーク リソースの配分を制御して、ビジネス戦略に適合するようにトラフィックを最適化するための Cisco Service Control ソリューションです。これにより、サービス プロバイダーは、ネットワーク コストを削減し、ネットワーク パフォーマンスおよびカスタマー エクスペリエンスを向上させ、新しい提供サービスおよびパッケージを作成できます。

システム コンポーネント

Service Control ソリューションは 4 つの主要コンポーネントで構成されます。

- Service Control Engine（SCE）プラットフォーム：柔軟で強力な専用のネットワーク使用状況モニタ。アプリケーション レベルでネットワーク トランザクションを分析およびレポートします。

  SCE プラットフォームのインストールおよび動作の詳細については、『*Cisco SCE Platform Installation and Configuration Guide*』を参照してください。

- Service Control Management Suite（SCMS）Subscriber Manager（SM）：サブスクライバ情報のダイナミック バインディングとポリシーが必要な場合に使用されるミドルウェア ソフトウェア コンポーネント。SM はサブスクライバ情報を管理し、複数の SCE プラットフォームに対してリアルタイムでプロビジョニングします。SM はサブスクライバ ポリシー情報を内部に格納し、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）システム（RADIUS、Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）など）と SCE プラットフォーム間のステートフル ブリッジとして機能することができます。

  SM のインストールおよび動作の詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

  Quota Manager（QM）は SM の任意コンポーネントです。QM を使用する Service Control ソリューション プロバイダーは、サブスクライバ セッションのサブスクライバ クォータを、高度な柔軟性で管理できます。

  QM のインストールおよび動作の詳細については、『*Cisco Service Control Management Suite Quota Manager User Guide*』を参照してください。

- Service Control Management Suite（SCMS）Collection Manager（CM）：1 つまたは複数の SCE プラットフォームから Raw Data Record（RDR; 未加工データ レコード）を受け取る収集システムを実装したものです。使用状況と統計情報を収集し、データベースに格納します。また、サブスクライバの使用状況と統計情報を単純なテキストベース ファイルに変換して、外部システムでさらに処理したり、収集することができます。

  CM のインストールおよび動作の詳細については、『*Cisco Service Control Management Suite Collection Manager User Guide*』を参照してください。

- Service Control Application（SCA）Reporter：CM が格納したデータを処理し、このデータの詳細なレポートのセットを提供するソフトウェア コンポーネントです。SCA Reporter は、単独実行することも Console に統合して実行することもできます。

  Reporter のインストールおよび動作の詳細については、『*Cisco Service Control Application Reporter User Guide*』を参照してください。

SCE プラットフォーム、SCMS-CM、SCMS-SM、および SCA Reporter の設計目的は、IP ネットワーク トラフィックの詳細な分類、分析、レポート、および制御をサポートすることです。SCMS-CM、SCA Reporter、および SCMS-SM は任意コンポーネントであり、Service Control ソリューションの配置によっては不要な場合があります。サードパーティによる収集やレポーティング アプリケーションを使用するサイト、ダイナミック サブスクライバ アウェアネス処理が不要なサイト、RADIUS または DHCP スニフィング オプションを使用するサイトの中には、これらのコンポーネントを必要としないものもあります。

図 2-1 に、Cisco Service Control ソリューション内の情報フローを示します。

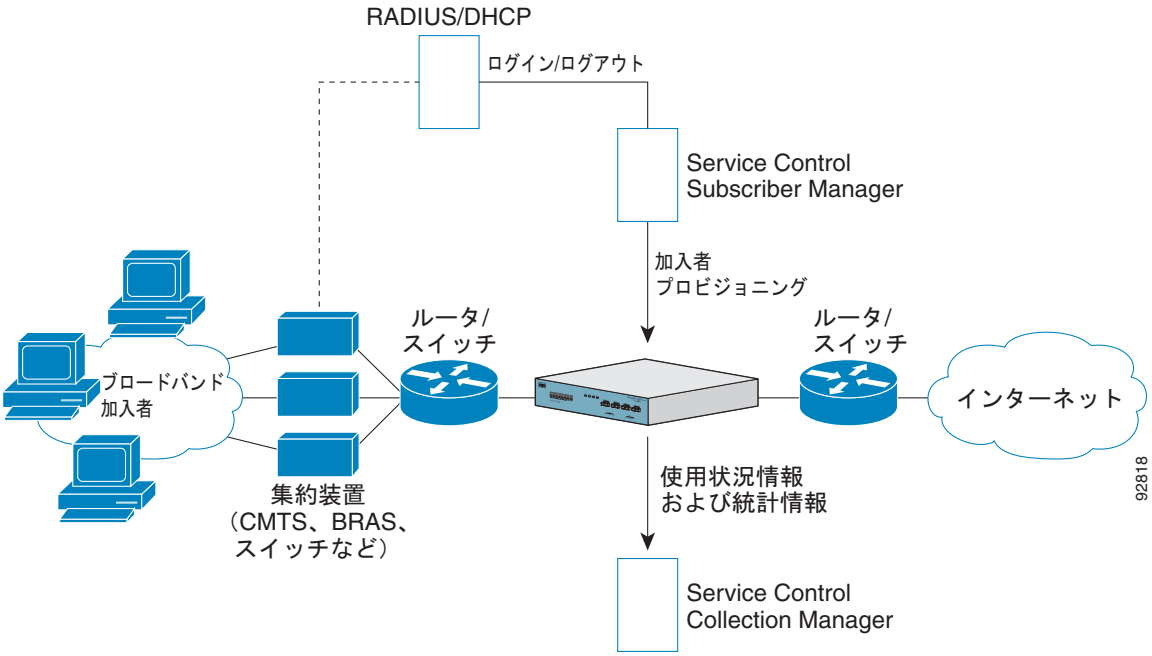
- 水平フロー：サブスクライバと IP ネットワークの間のトラフィックを表します。

  トラフィック フローは SCE プラットフォームでモニタされます。

- 垂直フロー：SCE プラットフォームから CM への RDR の伝送を表します。

  制御フローに SM を追加して、サブスクライバ データを提供できます。このようにすると、SCA BB でサブスクライバレベルの分析と制御を実行できます。

図 2-1　　SCA BB の情報フロー



サブスクライバおよびサブスクライバ モード

Cisco Service Control ソリューションの基本エンティティの 1 つに、*サブスクライバ*があります。サブスクライバは SCA BB が個別にモニタしたり、課金したり、ポリシーを適用できる最小のエンティティです。SCA BB システムの最小のインスタンスでは、サブスクライバはポリシーが個別に実行される、サービス プロバイダーの実際のカスタマーです。ただし、SCA BB を使用すると、より詳細にトラフィックをモニタおよび制御できます。たとえば、サブネットや集約装置でトラフィックをモニタまたは制御できます。

サービス コントロール ソリューションの設計にあたっては、どのサブスクライバをシステムに存在させるかが重要になります。この定義内容によって使用するサブスクライバ モードが決まり、さらに統合が必要な場合はその内容や、定義する実際のポリシーも決まります。次のセクションでは、サポートされているさまざまなサブスクライバ モード、それぞれのモードでサポートされている機能、および前提条件と必須コンポーネントについて説明します。

SCA BB がサポートするサブスクライバ モードは次の 4 つです。

- サブスクライバレス モード：サブスクライバは定義されません。グローバルなプラットフォーム単位で制御およびリンクレベル分析機能を実行します。
- アノニマス サブスクライバ モード：IP アドレスが個別に収集およびモニタされます。SCE プラットフォームは、使用された IP アドレスを自動的に識別し、パッケージに割り当てます。
- スタティック サブスクライバ モード：システム オペレータの設定に従って、着信 IP アドレスがバインドされ、「サブスクライバ」に静的にグループ化されます。
- サブスクライバアウェア モード：サブスクライバ情報は、現在サブスクライバが使用している IP アドレスに動的にバインドされます。IP アドレスをサブスクライバに割り当てるシステム（RADIUS、DHCP）と統合するか、この情報をスニフィングすると実行されます。ポリシー情報は SCA BB に直接管理されるか、統合によって動的にプロビジョニングされます。

サブスクライバレス モード

サブスクライバレス モードは、グローバルなプラットフォーム単位での制御および分析機能が必要となるサイトに適しています。たとえば、リンクを介して P2P トラフィック全体をモニタおよび制御する場合に使用できます。

サブスクライバレス モードでは統合する必要がないため、SCMS-SM が不要です。

（注） サブスクライバレス モードは、サブスクライバ数または着信 IP アドレス数の影響を受けません。したがって、モニタ対象リンクを利用するサブスクライバ総数は、SCE プラットフォームに関しては無制限になります。

アノニマス サブスクライバ モード

アノニマス サブスクライバ モードでは、サブスクライバ着信 IP アドレス単位でネットワーク トラフィックの分析と制御ができます。このモードは、サブスクライバごとに差別化された制御やサブスクライバレベルのクォータ トラッキングが不要な場合、IP レベルでの分析で十分である場合、または IP アドレス/サブスクライバ バインディングをオフラインで実行できる場合に使用します。たとえば、上位 IP アドレスを識別し、RADIUS/DHCP ログを使用して各サブスクライバに関係付けることにより、P2P トラフィックの生成量が最も多いサブスクライバを識別できます。サブスクライバごとに許可されている P2P トラフィックの合計帯域幅も制限できます。

アノニマス サブスクライバ モードでは使用する IP アドレスを統合したり、静的に設定する必要がないため、SCMS-SM が不要です。代わりに、SCE プラットフォームに IP アドレス範囲が直接設定されます。システムはサブスクライバ名として IP アドレスを使用して、このアドレスに「アノニマス」サブスクライバを動的に作成します。

（注）　SCE プラットフォームで同時にアクティブになっているアノニマス サブスクライバの総数は、同時にアクティブになっているサブスクライバの総数と同じです。

スタティック サブスクライバ モード

スタティック サブスクライバ モードは、着信 IP アドレスをグループにバインドし、定義済みサブスクライバに対するトラフィックをグループとして制御できるようにします。たとえば、（複数のサブスクライバで同時に使用される）特定のネットワーク サブネットに対するすべてのトラフィックを（仮想）「サブスクライバ」として定義し、グループとして制御 / 表示することができます。

スタティック サブスクライバ モードは、次のように、Service Control ソリューションで制御されるエンティティが、動的に変更されない固定 IP アドレスまたはアドレス範囲を使用している場合をサポートします。

- サブスクライバ IP アドレスが DHCP や RADIUS などから動的に変更されない環境
- 特定の集約装置などで処理されるすべての IP アドレスなど、共通の IP アドレス プールを使用するサブスクライバ グループをまとめて管理し、グループ全体で帯域幅を共有するような配置

SCE プラットフォーム上でスタティック サブスクライバを直接定義できるため、SCMS-SM などの外部管理ソフトウェアは不要です。サブスクライバ、サブスクライバの IP アドレス、関連パッケージのリストを定義するには、SCE プラットフォームの Command-Line Interface（CLI; コマンドライン インターフェイス）を使用します。

サブスクライバアウェア モード

サブスクライバアウェア モードでは、SCE には、サブスクライバが現在使用中の IP アドレスに動的にバインドされるサブスクライバ情報（Operational Support System（OSS; オペレーション サポート システム）ID およびポリシー）が読み込まれます。これにより、使用中の IP アドレスに関係なく、サブスクライバごとに差別化された動的な制御を行ったり、サブスクライバ レベルの分析を行うことができます。このモードを使用してトラフィックをサブスクライバ レベルで制御および分析し、サブスクライバの使用状況をモニタし、サブスクライバごとに制御ポリシー（パッケージ）を割り当てて実行します。

このモードでは、SCMS-SM を使用して SCE プラットフォームにサブスクライバ情報をプロビジョニングすることができます。

サブスクライバ モード：サマリー

表 2-1 に、システムでサポートされている各サブスクライバ モードのサマリーを示します。

表 2-1　サブスクライバ モードのサマリー

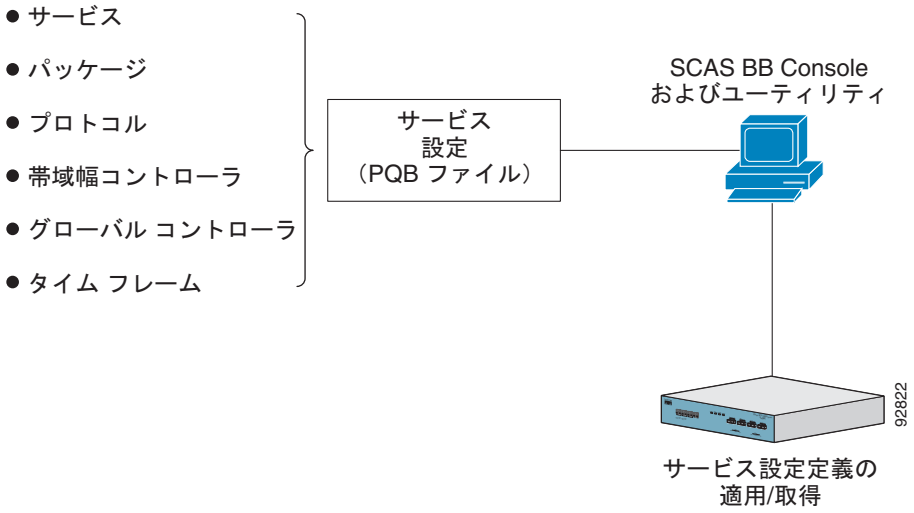
モード	サポートされている機能	主な利点	用途
サブスクライバレス モード	• グローバルな（プラットフォームレベルの）分析および制御	• サブスクライバ設定は不要	グローバルな制御ソリューションまたはサブスクライバレベルでの分析 例： • ピアリング ポイントで P2P アップロードを制御 • P2P の合計帯域幅を指定のパーセンテージに制限
アノニマス サブスクライバ モード	• グローバルな分析および制御 • 各 IP アドレスレベルでの分析および制御	• サブスクライバ設定は不要。使用するサブスクライバ IP アドレス範囲だけを指定 • 統合なしでサブスクライバレベルの制御を実行	サブスクライバごとに差別化されない、オフライン IP アドレスおよびサブスクライバ バインディングで対応可能な、IP レベルの分析または制御 例： • サブスクライバごとに P2P 帯域幅を制限 • 上位 IP アドレスを識別し、RADIUS/DHCP ログを使用して対応付けることにより、上位サブスクライバを識別
スタティック サブスクライバ モード	• グローバルな分析および制御 • SCE プラットフォームに静的に設定された各 IP アドレス / グループに基づく制御	• 1 回限りの静的なサブスクライバ設定（統合は不要） • 論理グループでサブスクライバ トラフィックを管理	サブスクライバ グループのトラフィックを制御 例： • 単一の CMTS デバイスを使用するサブスクライバ グループごとに P2P トラフィックの帯域幅制限を割り当て
サブスクライバアウェア モード	• すべてのシステム機能	• サブスクライバごとの差別化された動的な制御 • サブスクライバレベルでの分析（使用中の IP アドレスに関係しない）	サブスクライバ レベルでトラフィックを制御および分析 例： • IP アドレスに関係なく、サブスクライバの使用状況をモニタ • サブスクライバごとに異なる制御ポリシー（パッケージ）を割り当てて、パッケージを動的に変更

サービス コンフィギュレーション

サービス コンフィギュレーションは、SCE プラットフォームでトラフィックを分析および制御する方法を定義します。一般的には、図 2-2 に示すように、サービス コンフィギュレーションは次のものを定義します。

- プロトコルおよびサービス分類
- パッケージおよびポリシー
- 帯域幅コントローラ
- グローバル コントローラ

図 2-2　　サービス コンフィギュレーション



サービス コンフィギュレーションは、次のいずれかを使用して行います。

- Console
- SCA BB サービス コンフィギュレーション ユーティリティ
- Service Configuration API

SCA BB Console

SCA BB Console は GUI ツールのセットで、ソリューション コンポーネントの管理、設定、モニタに使用します。

Console については、このマニュアルの以降の章で詳細に説明します。

サービス コンフィギュレーション ユーティリティ

SCA BB サービス コンフィギュレーション ユーティリティ（**servconf**）は、簡単なコマンドライン ユーティリティで、PQB コンフィギュレーション ファイルを SCE プラットフォームに適用したり、SCE プラットフォームの現在のコンフィギュレーションを取得して PQB ファイルとして保存する場合に使用します。このユーティリティでは、PQB ファイルで定義されたサービス コンフィギュレーションを使って SCE プラットフォームを設定します。Windows または Solaris 環境にインストールして実行できます。

servconf についての詳細は、「SCA BB サービス コンフィギュレーション ユーティリティ」（P.13-1）を参照してください。

Service Configuration API

Service Configuration API は Java クラスのセットで、次の目的のために使用します。

- サービス コンフィギュレーションのプログラミングと管理
- SCE プラットフォームにサービス コンフィギュレーションを適用
- アプリケーションをサードパーティ製システムに統合

サービス プロバイダーはこの API を使用して、管理および運用作業を自動化および簡略化できます。

Service Configuration API については、『*Cisco Service Control Application for Broadband Service Configuration API Programmer Guide*』を参照してください。

CHAPTER 3

トラフィック処理の概要

はじめに

ここでは、Service Control Engine（SCE）プラットフォームにインストールした Cisco Service Control Application for Broadband（SCA BB）でトラフィックを処理する方法を説明します。

また、SCA BB システムの主な要素（サービス コンフィギュレーション エンティティ）と相互の関連性についても説明します。

ルーティング環境

トラフィック処理はルーティング環境によって異なります。シスコの Service Control ソリューションは次に示す 2 つの標準的なルーティング方法で動作可能です。

- 対称（通常）：インバウンドとアウトバウンドのほとんどのトラフィック フローが 1 つの SCE プラットフォームを通じてルーティングされます。この SCE プラットフォームを単方向だけしか通過しないフローはごくわずかです。
- 非対称：多くのフローは、この SCE プラットフォームを通じて一方向のトラフィック（インバウンドまたはアウトバウンド）だけがルーティングされます。他のフローは、両方向のトラフィックがこの SCE プラットフォームを通過します。

  あるフローのインバウンドとアウトバンドのトラフィックが同じ SCE プラットフォームを通過する場合、そのフローを双方向であるといいます。その SCE プラットフォームをインバウンド トラフィックとアウトバウンド トラフィックのいずれか一方だけ通過する場合は単方向フローです。

  Cisco Service Control ソリューションは、単方向フローと双方向フローの両方を処理できます。SCE プラットフォームは、対称と非対称のいずれかのルーティング環境で動作するように設定できます。非対称環境の SCE プラットフォームのトラフィック処理能力は対称環境の能力の一部分です。

非対称ルーティング環境に Cisco Service Control ソリューションを配置して、単方向分類を有効にすると、SCE プラットフォームの分類機能は、単方向のトラフィックの識別精度がよくなります。SCE プラットフォームは単方向フローを独立して処理し、反対方向のフローを処理する可能性のある他の SCE プラットフォームと同期をとりません。

トラフィック処理

トラフィック処理には 3 つの段階があります。

- トラフィックの分類：SCA BB はトラフィック フローを分析し、それぞれのタイプを判別します（たとえば、ブラウジング、E メール、ファイル共有、音声など）。
- トラフィック アカウンティングとレポート：SCA BB は課金処理を行い、Raw Data Record（RDR; 未加工データ レコード）を生成してネットワークを分析し、モニタします。
- トラフィック制御：SCA BB は、サービス、サブスクライバパッケージ、サブスクライバ クォータの状態などに応じてトラフィック フローを制限し、優先順位を指定します。

詳細は以降のセクションで説明します。

分類、レポート、制御を変更するには、サービス コンフィギュレーションを編集して SCE プラットフォームに適用します。

トラフィックの分類

トラフィック処理はトラフィックの分類から始まり、これによってネットワーク セッションがサービス別に分類されます。

Service Control ソリューションには、プロバイダーがサブスクライバに提供する商用サービスに対応するサービスが定義されています。このサービスを使用して、トラフィックの分類と識別、トラフィックの使用状況に基づくレポート、トラフィックの制御が行えます。

- 「サービス」（P.3-2）
- 「プロトコル」（P.3-4）
- 「開始側」（P.3-6）
- 「ゾーン」（P.3-7）
- 「フレーバ」（P.3-7）
- 「サービスへのフロー属性のマッピング」（P.3-9）

サービス

トラフィックの分類では、SCA BB はネットワーク セッションをサービスに分類します。

サービスは次の 2 つの部分で構成されています。

- サービス コンフィギュレーション（SCA BB はサービスごとに異なる規則を適用できるため）
- 使用状況を集約したレポート

プロバイダーにとっては、サービスとはサブスクライバに販売するネットワーク製品です。通常はサブスクライバが使用するネットワーク アプリケーションであり、ブラウジング、E メール、ファイル共有、音声などがあります。技術的な観点からは、サービスは 1 つまたは複数のサービス要素で構成されています。それぞれのサービス要素によってサービスが決定され、ネットワーク トラフィック フロー タイプに関連付けられます。

デフォルトのサービス コンフィギュレーションには多数のサービスが定義されています（詳細については『*Cisco Service Control Application for Broadband Reference Guide*』の「Default Service Configuration Reference Tables」の章を参照してください）。サービス コンフィギュレーションのサービスは、変更することも追加することもできます。

サービス コンフィギュレーションには最大 500 件のサービスを設定できます。

セッションの開始と同時に分類が行われます。分類の際はセッションの最初の数パケットが検証され、セッションが所属するサービスが決定されます。次に、セッションにサービス ID が割り当てられます。サービス ID は、そのセッションが終了するまで変わりません。

トラフィックは次のサービス要素に基づいて分類され、サービスにマッピングされます。

- プロトコル：使用されるプロトコル。たとえば、ブラウジング フローと E メール フローをそれぞれのサービスにマッピングできます。
- 開始側：フローを生成したサブスクライバ側またはネットワーク側。たとえば、サブスクライバ側とネットワーク側で開始されたピアツーピア トラフィックを、それぞれのサービスにマッピングできます。
- ゾーン：フローのネットワーク側ホスト IP アドレスのリスト。たとえば、特定のサーバに送信されるすべての音声フローを特定のサービスにマッピングできます。
- フレーバ：レイヤ 7 の特定のプロパティ。フローのネットワーク側ホストのホスト名などです。たとえば、一定のパターンと一致する URL の HTTP フローをすべて特定のサービスにマッピングできます。

（注） 単方向分類が有効になっている場合、フレーバは分類には使用されません。

SCA BB は、このようなフロー マッピングを使用して、SCA BB が通過するネットワーク接続をサービスにマッピングします。サービスごとに規則を定義し、制御ポリシーを実装できます。分類規則にはレイヤ 3 およびレイヤ 4 のパラメータ（ポート番号や IP アドレスなど）と、レイヤ 7 のパラメータ（HTTP 接続のホスト名とユーザ エージェント）を含めることができます。

（注） SCA BB は、すべての P2P サービスの分類を 100 % 達成することはできません。これは、永続的に接続を試行する P2P アプリケーションがあるためです。このようなアプリケーションは、さまざまな代替プロトコルと接続スキームを使用します。ネイティブ プロトコルは暗号化され、新しいバージョンがリリースされると、この暗号化はしばしば変更されます。これは、P2P トラフィックをブロックしようとしても、結果的にはクライアントが接続する場合もあることを意味します。完全にブロックするのではなく、トラフィックの帯域幅を制限し、そのトラフィックを無効にするほうがよい場合もあります。

サービス要素

サービスは 1 つまたは複数のサービス要素で構成されており、異なるネットワーク トラフィック フロー タイプが異なるサービス要素にマッピングされています。

サービス要素は特定のプロトコル、開始側、ゾーン、およびフレーバを、選択されたサービスに対応付けます。これらのパラメータの一部または全部にワイルドカードが使用できます。

（注）　単方向分類が有効になっている場合、サービス要素のフレーバは常にワイルドカード値となります。

次の 4 つの基準をすべて満たすトラフィック フローが特定のサービスにマッピングされます。

- フローがサービス要素の指定のプロトコルを使用している。
- フローの開始側が、サービス要素で指定された開始側と一致する。
- フローの宛先が、サービス要素の指定ゾーンに属するアドレスである。
- フローが、サービス要素の指定のフレーバと一致している。

  フローが 2 つのサービス要素と一致し、一方が他方よりも詳細であれば、このフローはより詳細なサービス要素にマッピングされます。

  たとえば、サービス A にブラウジングが定義され、サービス B に特定の URL リストのブラウジングが定義されているとします。サービス B のリストにある URL のブラウジング フローは、どちらのサービスとも一致しますが、この場合はサービス B にマッピングされます。

  任意のサービス要素の任意のパラメータに一致するフローが別の要素の別のパラメータにも一致する場合、一致するパラメータの優先順位はフレーバが最も高く、次がプロトコル、その次がゾーン、最後が開始側となります。

  たとえば、サービス A に E メールが、サービス B に指定されたネットワーク ゾーンのすべてのトラフィックが定義されているとします。指定されたネットワーク ゾーンの E メール フローは、どちらのサービスとも一致しますが、この場合はサービス A にマッピングされます。

サービスの例

表 3-1 に、サービスとそのネットワーク パラメータの例を示します。

表 3-1　サービスおよびサービス パラメータの例

サービス名	プロトコル	開始側	ゾーン	フレーバ
Web ブラウジング	HTTP HTTPS	サブスクライバ側	—	—
Web ホスティング （ネットワーク側開始ブラウジング）	HTTP HTTPS	ネットワーク側	—	—
ローカル SMTP	Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）	—	ローカルメール サーバ（215.53.64.0/24）	—

プロトコル

フローの主な分類の 1 つにセッションのプロトコル（セッションを開始したネットワーク アプリケーションのプロトコル）があります。

SCA BB システムで定義されているように、プロトコルは 1 つまたは複数のシグニチャ、1 つまたは複数のポート番号、および転送タイプの組み合わせで構成されています。ネットワーク フローのプロトコルはこれらのパラメータに従って識別されます。たとえばポート番号が 80、転送タイプが TCP であり、コンテンツが HTTP シグニチャと一致する場合、SCA BB はこのフローを HTTP プロトコルにマッピングします。

デフォルトのサービス コンフィギュレーションには、事前に定義されたプロトコルのリストがあります。プロトコルは追加できます。

TCP または UDP フローが特定のプロトコル定義に一致しない場合、SCA BB はこのフローを Generic TCP または Generic UDP プロトコルにマッピングします。

非 TCP または非 UDP フローが特定のプロトコル定義に一致しない場合、SCA BB はこのフローを Generic IP プロトコルにマッピングします。

単方向分類が有効になっている場合、プロトコル分類は、単方向 UDP フローを除いて、通常の方法で実行されます。この場合、SCA BB は最初のパケットの宛先ポートを使用して分類しようとします。完全に一致するものが見つからなければ、SCA BB は送信元ポートを使用してプロトコルを分類しようとします。

プロトコル要素

プロトコルは、プロトコル要素の集合です。

プロトコル要素は特定のシグニチャ、IP プロトコル、およびポート範囲を、選択されたプロトコルに対応付けます。パラメータにはワイルドカードを含めることができ、ポート番号を範囲で指定することもできます。

次の 3 つの基準をすべて満たすトラフィック フローが特定のプロトコルにマッピングされます。

- フローのシグニチャがプロトコル要素で指定されたシグニチャと一致する。
- フローのプロトコルがプロトコル要素の IP プロトコルと一致する。
- フローのポート範囲がプロトコル要素で指定されたポート範囲と一致する。
- フローが 2 つのプロトコル要素に一致し、一方が他方よりも詳細であれば、フローはより詳細なプロトコル要素にマッピングされる。

  たとえば、プロトコル A が FTP シグニチャと一致するフローに定義され、プロトコル B が TCP ポート 21 の FTP シグニチャと一致するフローに定義されているとします。ポート 21 の FTP フローは、どちらのプロトコルとも一致しますが、この場合はプロトコル B にマッピングされます。
- フローが、あるプロトコル要素のシグニチャと別のプロトコル要素のポートのどちらにも一致する場合、そのフローはシグニチャと一致するプロトコルにマッピングされる。

  たとえば、プロトコル A が FTP シグニチャと一致するフローに定義され、プロトコル B が TCP ポート 21 のフローに定義されているとします。ポート 21 の FTP フローは、どちらのプロトコルとも一致しますが、この場合はプロトコル A にマッピングされます。

ポートベース プロトコルの簡単な定義方法

特定ポートのすべての汎用（分類されていない）トラフィックは、<「Generic」シグニチャ , 特定ポート> という形式のプロトコル要素をプロトコルに追加することで、そのプロトコルに割り当てることができます。特定ポートの「Generic」シグニチャがプロトコルに割り当てられると、「Behavioral」シグニチャも自動的にそのプロトコルに割り当てられます。たとえばデフォルト コンフィギュレーションでは、ポート 555 の「Generic」シグニチャは H20 プロトコルに割り当てられるので、ポート 555 の「Behavioral Upload/Download」シグニチャも自動的に H20 プロトコルに割り当てられます。

この割り当ては自動的に実行されるため、ユーザは手動で割り当てを行う必要はありません。自動的に追加されるこれらのプロトコル要素は、GUI には表示されません。一方、ユーザが特定ポートの「Behavioral Upload/Download」シグニチャを別のプロトコルに割り当てるには、適切なプロトコル要素を作成し、それを別のプロトコルに割り当てます。

（注）　デフォルト コンフィギュレーションでは、プロトコル要素 <「Generic」シグニチャ , 特定ポート 80> を含めることで、HTTP プロトコル定義は HTTP シグニチャだけでなく、ポート 80 のその他の汎用（分類されていない）トラフィックもすべて受け入れます。前述したように、<「Generic」シグニチャ , 特定ポート > 形式のプロトコル要素が特定のプロトコル定義に使用されている場合、SCE はその特定ポートの Generic および Behavioral シグニチャの両方をそのプロトコルにマッピングします。

HTTP の場合は、「Behavioral Upload/Download」シグニチャとして分類されているポート 80 のトラフィックもその HTTP プロトコルに割り当てられます。ここまで述べてきたように、この動作の目的はポートベース プロトコルを簡単に定義することです。ただし、プロトコル要素 <「Behavioral」シグニチャ , 特定ポート > を他のプロトコルに追加すると、この動作を回避できます。

シグニチャ

SCA BB は、SCE プラットフォームの緻密なパケット検査機能でトラフィック フローを検査し、それぞれのフローとインストールされたプロトコル シグニチャのセットを比較して、フローを生成したネットワーク アプリケーションを特定します。

SCA BB には、一般的なネットワーク アプリケーションの定義済みシグニチャとプロトコルのセットが用意されています。たとえば、ブラウジング、E メール、ファイル共有、VoIP などです。

単方向分類が有効になっている場合、SCE プラットフォームを単方向フロー（インバウンドまたはアウトバウンド）が通過すると、そのフローは単方向プロトコル シグニチャの特定セットと照合されます。双方向フローが SCE プラットフォームを通過する場合、プロトコル ライブラリはそのフローを標準の（双方向）プロトコル シグニチャの 1 つと照合します。

シスコは新しいシグニチャを含むプロトコル パックを定期的に発行して、シグニチャをアップデートしています。これらのプロトコル パックを使用して SCA BB にインストールされたシグニチャのセットをアップデートすれば分類機能を強化できます。

ダイナミック シグニチャ

SCA BB が使用するシグニチャのほとんどは定義済みであり、ハードコード化されています。また、ユーザがダイナミック シグニチャを追加して独自に定義することもできます。

ダイナミック シグニチャは、Signature Editor ツールで作成および編集ができます。SCA BB の Dynamic Signature Script（DSS）エンジンでは、定義されたシグニチャのほかにこれらのユーザ定義シグニチャを使って分類を行います。

開始側

通常、SCE プラットフォームはプロバイダーのサブスクライバとネットワークの間に配置されます。サブスクライバ側で開始されたフローはサブスクライバからネットワークに伝送され、ネットワーク側で開始されたフローはネットワークからサブスクライバに伝送されます。

フロータイプによっては開始側を制限することができます。たとえば、HTTP フローの開始側をサブスクライバに制限できます。HTTP が開始されるのはサブスクライバがインターネットを利用するときなので、常にサブスクライバ側から開始されるからです。HTTP フローがネットワーク側から開始される場合は、サブスクライバのローカル マシン上で Web サーバがオープンになっており、着信 HTTP トラフィックを受信していると考えられます。プロバイダーはネットワーク側から開始される HTTP をブロックできます。

ゾーン

ゾーンは、ネットワーク側の IP アドレスの集合です。

共通の目的で接続されているグループごとに IP アドレスを割り振ることによってゾーンを設定できます。サブスクライバのネットワーク フローがサービスにマッピングされて、ゾーンに適用されることもあります。実際は、ゾーンには地理的な領域が定義されることがほとんどです。

ゾーンはネットワーク セッションを分類するために使用します。ネットワーク セッションは、宛先 IP アドレスに基づいてサービス要素に割り当てられます。

ゾーンの例

- 「囲いのある庭」: プレミアム ビデオ コンテンツを持つサーバ ファームの IP アドレス範囲。プロバイダーは特定のサブスクライバへのアクセスを制限し、トラフィックの優先順位を確保します。
- オフネットとオンネットのフローを区別するためのゾーン。

ゾーンをセッションに割り当てる例

- ゾーン A とゾーン B はいずれもユーザが定義したゾーンであり、ゾーン A の IP アドレスは 10.1.0.0/16、ゾーン B の IP アドレスは 10.2.0.0/16 であるとします。新しいセッションのネットワーク IP アドレスが 10.1.1.1 の場合、このセッションはゾーン A のセッションとなります。

ゾーン項目

ゾーンは、関連するゾーン項目の集合です。

ゾーン項目は、1 つの IP アドレスまたは IP アドレスの範囲です。

表 3-2 にゾーン項目の例を示します。

表 3-2　　ゾーン項目の例

ネットワーク アドレス	例
IP アドレス	123.123.3.2
IP アドレス範囲（およびマスク）	123.3.123.0/24 IP アドレスの最初の 24 ビットは指定通りであり、最後の 8 ビットは任意の値となります（すべての IP アドレスが 123.3.123.0 ～ 123.3.123.255 になります）。

フレーバ

フレーバは、ネットワーク セッションをシグニチャ固有のレイヤ 7 プロパティに基づいて詳細に分類するための要素です。

フレーバは、Service Control ソリューションのサービスをさらに細かく定義します。プロトコル フレーバは、サービスを分類する場合にプロトコル属性を追加し、このサービスをプロトコルだけに基づくサービスのフレーバにします。たとえば、HTTP プロトコルのユーザ エージェント属性をプロトコル フレーバとして追加すると、同じブラウザ タイプで生成されたすべての HTTP トラフィックの定義を 1 つのサービスにすることができます。ブラウザ タイプはユーザ エージェント フィールドで確認できます。

フレーバ タイプの例には、HTTP ユーザ エージェントや、Session Initiation Protocol（SIP）ソース ドメインがあります。

（注）　単方向分類が有効になっている場合、フレーバはトラフィックの分類には使用されません。

フレーバ項目

フレーバは、フレーバ項目の集合です。

フレーバ項目のタイプはフレーバ タイプによって異なります。使用できるフレーバ タイプのリストは、「フレーバ タイプとパラメータ」（P.7-48）を参照してください。

デフォルトのサービス コンフィギュレーションは、HTTP Streaming Agent（HTTP のフレーバ）や Vonage（SIP のフレーバ）などのように事前に定義されたフレーバです。

DSCP ToS

フレーバ タイプのひとつに Type of Service（ToS）があります。このタイプでは、Differentiated Service Code Point（DSCP; Diffserv コード ポイント）ToS を分類基準として使用できるので、特定のマーキングを伝送するパケットを、無制限の帯域幅やレポートなどが設定された定義済みサービスに割り当てることができます。DSCP ToS 分類プロセスは、他の分類メカニズムよりも優先されます。これにより、音声ゲートウェイなどの外部デバイスが、フローの処理方法を指示できます。DSCP ToS ベースの分類は、独自の管理サービスをマーキングするためのすぐれた方法です。SCA BB はアプリケーションを認識しませんが、DSCP ToS フィールドによってそれらを識別します。

コンテンツ フィルタリング

コンテンツ フィルタリングでは、要求された URL に従って、HTTP フローの分類と制御を行います。URL の分類は、外部データベースにアクセスして行われます。

サービス プロバイダーは、訴訟を回避したり保護者による管理ができるなど、サブスクライバにとって効果的な Web フィルタリングを必要としています。ここで問題になるのは、Web は大規模なうえに成長を続けている一方で、SCA BB や SCE プラットフォームは効果的なフィルタリングを必要とする巨大な URL データベースを追跡、管理するようには設計されていない点です。

そこで、SCA BB は、SurfControl Content Portal Authority（CPA）に統合された、コンテンツ フィルタリングを提供します。SurfControl の技術により、ネットワーク管理者は URL データベースを管理したりサーバと通信することなく SCA BB の URL 分類機能を強化し、強力なフィルタリング ソリューションを構築することができます。Web でのアクセスが非常に多いサイトや、性的な表現、人種差別、ハッカーなどリスク カテゴリ別に分類された URL のデータベースへのアクセスを、関連分野も含めて完全に網羅することができます。

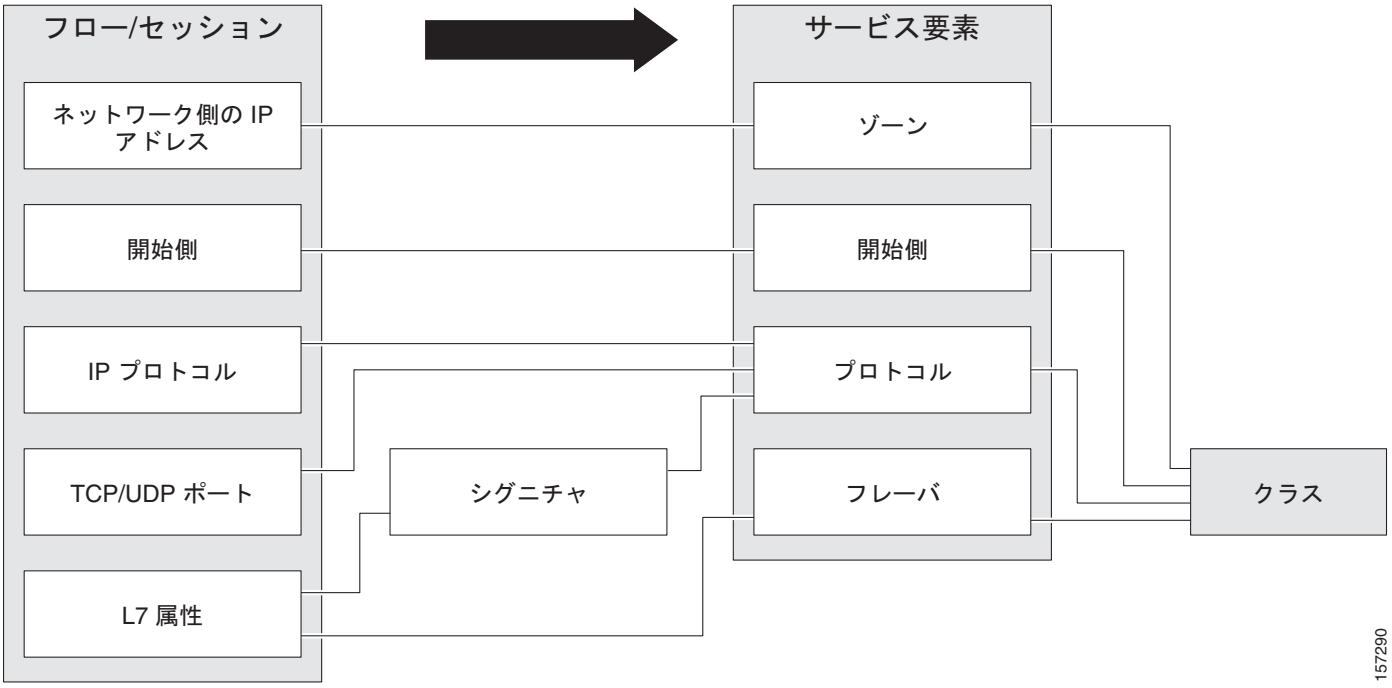
SurfControl の CPA を SCA BB に統合することで、必要な Web フィルタリング ソリューションが提供されます。SCA BB は SCE プラットフォーム上で実行され、CPA サーバに接続してサブスクライバが要求する Web サイトをカテゴリ化します。カテゴリは HTTP フローを分類するために使用され、この分類は、通常の SCA BB トラフィック制御とレポートに使用されます。

（注）　SCA BB には、HTTP URL フレーバ分類で使用される URL の内部データベースが含まれます。内部データベースと外部のコンテンツ フィルタリング データベースの両方で検出された URL は、内部データベースに従って分類されます。

サービスへのフロー属性のマッピング

図 3-1 は、セッションのフロー要素をサービスのサービス要素にマッピングする場合を示しています。

図 3-1　サービスへのフロー属性のマッピング



トラフィックのアカウンティングとレポート

SCE プラットフォームが収集したデータは、リアルタイム シグナリング、課金、レポートに使用できます。

ユーザ定義の使用カウンタに基づいて、さまざまなメトリックが異なるスコープで収集されます。グローバル（全リンク単位）、サービス単位（またはサービス グループ単位）、パッケージ単位（またはパッケージ グループ単位）、サブスクライバ単位があります。

- グローバル制御帯域幅はレイヤ 1 のボリュームに基づいています。
- サブスクライバ帯域幅制御（およびアカウンティング、レポート）は、レイヤ 3 ボリュームに基づいています。

使用カウンタの値にはプッシュ型とプル型があります。

- SCE プラットフォームは、フローや使用状況などのデータを含む RDR を生成し、伝送します。
- SCE プラットフォームは、外部システムが問い合わせる Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）MIB を保守します。

従量制課金

SCA BB は、さまざまなスコープのネットワーク メトリックをサービス単位で収集し、保守します。

次のネットワーク メトリックがあります。

- アップストリームのボリューム（L3 KB）
- ダウンストリームのボリューム（L3 KB）
- セッション
- アクティブなサブスクライバ
- 並列セッション
- セッション持続時間

（注）　SIP や Media Gateway Control Protocol（MGCP）などの VoIP サービスでは、同時セッション数使用カウンタは同時に行われる音声呼び出しの回数を、セッション持続時間利用使用カウンタは音声呼び出しの持続時間を表します。

サービス単位による課金は次のスコープで発生します。

- サブスクライバ単位
- サブスクライバのグループ単位（パッケージ）
- リンク単位（グローバル）

複数のサービスが 1 つのサービス使用カウンタを共有することがあります。たとえば、デフォルトのサービス コンフィギュレーションでは、SMTP サービスと Post Office Protocol 3（POP3）サービスが同じ E メール カウンタを共有します。使用カウンタへのサービスの割り当てはサービス階層によって決まります。サービス階層については次のセクションで説明します。同様に、複数のパッケージが 1 つのパッケージ使用カウンタを共有することもあります。この場合のパッケージと使用カウンタの割り当てはパッケージ*階層*（「パッケージ階層」（P.3-11）を参照）によって決まります。

サービス階層

*サービス*は階層ツリーに配置されます。単一のデフォルト サービスがルートにあり、ツリー内の任意の場所に新しいサービスをそれぞれ配置できます。詳細については、「サービス」（P.3-2）を参照してください。

サービスは親の規則を継承します。（特定のパッケージ内の）特定のサービスに規則が定義されている場合は、明示的に指定されていないかぎり、すべての子サービスがそのパッケージの同じ規則によって制御されます。

サービス使用カウンタ

サービス階層を使用すると、サービスをその意味に従って編成するだけでなく、使用カウンタを共有することもできます。サービスはサービス階層が定義したグループに応じて分類されます。各サービスには使用カウンタが割り当てられます。

サービスの使用カウンタには 2 つのカテゴリがあります。

- グローバル：Link Usage RDR、Package Usage RDR、およびレポートに使用されます。
- サブスクライバ：Real-Time Subscriber Usage RDR およびレポートに使用されます。

サービスごとにグローバル使用カウンタおよびサブスクライバ使用カウンタが 1 つずつ割り当てられます。特定のサービスに分類されたトラフィックだけのサービス使用量をカウントしたり、親サービスのトラフィックと併せてカウントすることができます。たとえば、「Premium Video Content」というサービスが「Streaming」の子として定義されている場合、オペレータは Premium Video Content 専用の使用カウンタを定義したり、「Streaming」と同じ使用カウンタを使うように設定することができます。グローバル使用カウンタとサブスクライバ使用カウンタは独立しています。サービスが同じ場合、一方の使用カウンタの親と子が同じでも他方の使用カウンタは子だけが同じということもあります。

パッケージ階層

パッケージは階層ツリーに配置されます。単一のデフォルト パッケージがルートにあり、ツリー内の任意の場所に新しいパッケージをそれぞれ配置できます。詳細については、「パッケージ」（P.3-13）を参照してください。

パッケージ使用カウンタ

パッケージ階層を使用すると、パッケージはその意味に従って編成され、パッケージ使用カウンタが共有されます。サービス コンフィギュレーションごとに最大 1024 個のパッケージ使用カウンタを定義して、そのうちの 1 つを Unknown Subscriber Traffic パッケージに使用できます。

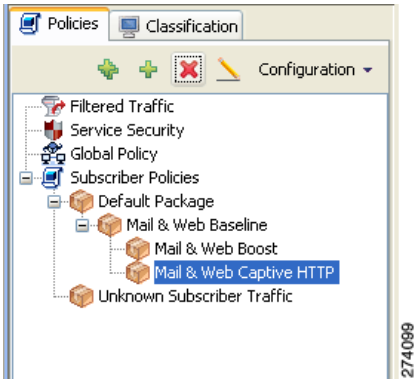
パッケージ レベルでの使用量レポートは、次のようにグループ化されます。

- 専用の使用カウンタが割り当てられたパッケージ：このパッケージに対応付けられたすべてのトラフィックは、割り当てられたカウンタで個別にカウントされます。その場合、専用カウンタが割り当てられていないすべての子も一緒にカウントされます。
- 専用のパッケージ使用カウンタが*割り当てられていない*パッケージ：このパッケージに対応付けられたすべてのトラフィックは、親パッケージと一緒にカウントされます。

図 3-2 に、パッケージ ツリーの例を示します。この例では、Mail &Web Baseline パッケージに専用カウンタが割り当てられていて、子パッケージに専用カウンタが割り当てられていない場合、すべての Package Usage RDR および派生レポート（「Package Bandwidth per Service」など）は、3 つのすべてのパッケージに割り当てられたサブスクライバの使用量を合計します。

ただし、Mail & Web Boost パッケージにも専用カウンタがある場合は、Main & Web Baseline および Mail & Web Captive HTTP のトラフィックが一緒にカウントされ、Mail & Web Boost のトラフィックは個別にカウントされます （一般的に、これは効率的なコンフィギュレーションではありません。階層構造は同じカウンタが共有できるグループ パッケージに使用すべきです）。

図 3-2　　パッケージ ツリーの例



レポート

SCA BB を実行する SCE プラットフォームは、サービス プロバイダーに関する情報が格納された RDR を生成して送信します。

RDR には、システム設定に応じてさまざまな情報および統計情報が格納されます。

RDR は、シスコ独自仕様のプロトコルを使用して送信されます。したがって、Cisco Service Control Management Suite（SCMS）Collection Manager（CM）を使用するか、または RDR を処理するソフトウェアを開発する必要があります。

一部の RDR 内のデータは、業界標準となっている NetFlow レポーティング プロトコルでもエクスポートできます。NetFlow レポーティングを使用すると SCA BB ソリューションを既存のデータ コレクタに簡単に統合できます。

- 「RDR」（P.3-12）
- 「NetFlow」（P.3-13）

RDR

RDR の主なカテゴリは次のとおりです。

- Usage RDR：定期的に生成されます。使用カウンタの状態がサービス単位およびアカウンティング スコープ単位で格納されます。Usage RDR には 4 つのタイプがあります。
  - Link Usage RDR：リンク全体のサービス単位でのグローバルな使用状況。
  - Package Usage RDR：サブスクライバ グループごとのサービス単位での使用状況。
  - Subscriber Usage RDR：サブスクライバごとのサービス単位での使用状況。全サブスクライバに生成されます。Cisco Service Control Management Suite（SCMS）Collection Manager（CM）および Cisco Service Control Application（SCA）Reporter は、この RDR を使用して上位サブスクライバ レポートと集約された使用量課金レコードを生成します。
  - Real-Time Subscriber Usage RDR：選択されたサブスクライバだけについて生成されます。SCMS-CS および SCA Reporter は、この RDR を使用して詳細なサブスクライバ アクティビティ レポートを生成します。
- Transaction RDR：フロー例について生成されます。上位 TCP ポートなどの統計グラフを作成する場合に使用されます。
- Transaction Usage RDR：ユーザ定義フィルタに合わせてフローごとに作成されます。ブラウジング、ストリーミング、音声フローについてレイヤ 7 の詳細情報が格納されます。フローベースの課金に使用されます。
- Real-Time Signaling RDR：フロー開始や終了など特定のネットワーク イベント時に生成されます。外部システムからネットワークへのリアルタイム アクションを許可する場合に使用されます。
- Malicious Traffic RDR：SCE プラットフォームが Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃などのトラフィック異常を検出した場合に生成されます。これらの RDR は、攻撃や攻撃者を検出し、これらの影響を軽減するために使用されます。

NetFlow

次の情報は、NetFlow プロトコルを使用してエクスポートできます。

- Usage：定期的に生成されます。使用カウンタの状態がサービス単位およびアカウンティング スコープ単位で格納されます。
- Malicious Traffic：SCE プラットフォームが DDoS 攻撃などのトラフィック異常を検出した場合に生成されます。

トラフィックの制御

トラフィックの制御は、サービス、サブスクライバ パッケージ、サブスクライバ クォータの状態などに応じて、トラフィック フローをブロック、制限、優先する方法を提供します。

- 「パッケージ」（P.3-13）
- 「サブスクライバが未知のトラフィック」（P.3-14）
- 「規則」（P.3-14）
- 「帯域幅の管理」（P.3-14）
- 「クォータ管理」（P.3-17）

パッケージ

パッケージは、サブスクライバ ポリシーを表す規則の集合です。パッケージには、指定したサブスクライバ グループに配信されるサービスのグループと、それぞれのサービスに対するシステムの動作が定義されています。ネットワーク フローの制限、フローの優先順位に関するガイドライン、フローをレポートする方法が格納されています。

ネットワークの各サブスクライバには、自分が所属するパッケージへの参照先が示されます。次に、ネットワークの各サブスクライバがシステムでどのように参照されるかを示します。

1. フローとサービス要素を一致させ、ネットワーク フローとサービスをマッピングする。
2. フローの発信元であるサブスクライバを 、サブスクライバのネットワーク ID（通常はサブスクライバの ID アドレス）に従って識別する。
3. サブスクライバが所属するパッケージを識別する。
4. サブスクライバのネットワーク フローのサービスに正しい規則を適用する。

もう 1 つの方法について、「仮想リンク モード」（P.3-13）で説明します。

仮想リンク モード

通常モードでは、各パッケージに帯域幅コントローラを定義します（「帯域幅の管理」（P.3-14）を参照）。仮想リンク モードでは、テンプレート帯域幅コントローラを定義します。サブスクライバがシステムに入ると、そのサブスクライバに実際の帯域幅パラメータが割り当てられます。これらのパラメータはサブスクライバのパッケージと仮想リンクの方向によって決まります。

詳細については、「クォータの管理」（P.9-76）を参照してください。

サブスクライバが未知のトラフィック

SCE プラットフォームは、トラフィック フローを処理するサブスクライバを識別しようとします。SCE プラットフォームはトラフィック フローの IP アドレスまたは VLAN を調べて、内部データベース内で、この IP アドレスまたは VLAN タグで識別されるサブスクライバを確認します。このようなサブスクライバがデータベース内にない場合、トラフィック フローは Unknown Subscriber Traffic カテゴリにマッピングされます。

規則

規則とは、特定サービスのネットワーク フローの処理方法を SCE プラットフォームに伝える一連の命令です。次のような規則があります。

- フローの処理を次のように指定する。
  - ブロックする。
  - 一定の帯域幅を割り当てる。
  - そのフローのパケット DSCP ToS を所定の値でマーキングする（「DSCP ToS マーキング」（P.3-20）を参照）。
- 集約ボリュームまたはセッション制限を定義し、フローに制限を適用する。
- 課金や分析のためにフローをレポートする方法を指定する。

カレンダー

カレンダーを使用して、1 週間を 4 つの時間枠に分割できます。

カレンダーの設定後、そのカレンダーを使用するパッケージに「タイムベース規則」（P.3-14）を追加できます。

タイムベース規則

タイムベース規則とは、1 つの時間枠だけに適用される規則です。タイムベース規則を使用すると、一定の時間だけに適用される規則パラメータを設定できます。たとえば、ピーク、オフピーク、夜間、週末用にそれぞれ異なる規則を定義する必要がある場合もあるでしょう。

規則には、タイムベース規則を追加できます。時間枠に対してタイムベース規則が定義されていない場合、親規則が適用されます。

異なる時間枠に同様の規則を適用する必要がある場合があります。タイムベース規則を追加するとき、親規則の設定を新しいタイムベース規則にコピーし、必要な変更を行うことができます。親規則に対してそれ以降に行った変更は、タイムベース規則には影響しません。

帯域幅の管理

システムを通過する帯域幅には絶対的な制限があり、これを物理リンク帯域幅と呼びます。SCE プラットフォームを通過する総帯域幅を物理リンクの帯域幅よりも小さい値に制限できます。たとえば、IP ストリーム上で SCE プラットフォームの隣に位置するデバイスの BW 容量が限られている場合、他のデバイスの容量に合わせて、SCE プラットフォームを通過する帯域幅を制限できます。

SCA BB の帯域幅制御には 2 つの段階があります。

- グローバル制御

- サブスクライバ帯域幅制御
- グローバル制御帯域幅はレイヤ 1 のボリュームに基づいています。
- サブスクライバ帯域幅制御（およびアカウンティング、レポート）は、レイヤ 3 ボリュームに基づいています。

グローバル帯域幅制御

全体の帯域幅使用状況はグローバル コントローラで制御します。グローバル コントローラは、SCE プラットフォームの仮想キューです。グローバル コントローラはシステム全体に設定し、サブスクライバごとには設定しません。

グローバル コントローラは、「Total Gold Subscriber Traffic」や「Total P2P Traffic」などといった大容量のグローバルなトラフィックを制限します。各グローバル コントローラは、特定のタイプのすべてのトラフィックに割り当てられる利用可能な合計帯域幅の最大割合を定義します。グローバル コントローラを使用すると、P2P などのシステム内のサービスの合計トラフィックを利用可能な合計帯域幅の指定した割合に制限できます。このようにして、このトラフィックで消費する合計帯域幅を管理できます。

デフォルトでは、アップストリーム インターフェイスとダウンストリーム インターフェイスには、リンク トラフィックを 100% 制御する、デフォルト グローバル コントローラが 1 つずつ割り当てられています。各インターフェイスには最大 1023 のグローバル コントローラを追加できます。また、各グローバル コントローラには合計リンク制限の最大割合を個別に割り当てることができます。

各グローバル コントローラには、利用可能な合計帯域の最大割合の値をタイム フレームごとに個別に定義できます （「カレンダー」（P.3-14）を参照）。

デュアルリンク システムでは、各リンクに異なる帯域幅の値を定義できます。また、2 つのリンクを通過する集約帯域幅を制限することもできます。

仮想リンク モードでは、テンプレート グローバル コントローラが使用されます。テンプレート グローバル コントローラは、仮想キューのテンプレートであり、システム内と同数の個別物理リンクに適用されます。それぞれの物理リンクの実際の帯域幅パラメータは、リンクによって異なります （詳細については、「クォータの管理」（P.9-76）を参照してください）。

サブスクライバ帯域幅制御

個別のサブスクライバが使用する帯域幅は、サブスクライバ BW Controller（BWC; BW コントローラ）で制御します。それぞれの BWC は、指定したサービスで利用できる帯域幅を制御します。特定の BWC が制御するサービスはパッケージごとに定義されますが、帯域幅制御はサービスごとに設定します。

BWC は次のパラメータで指定されます。

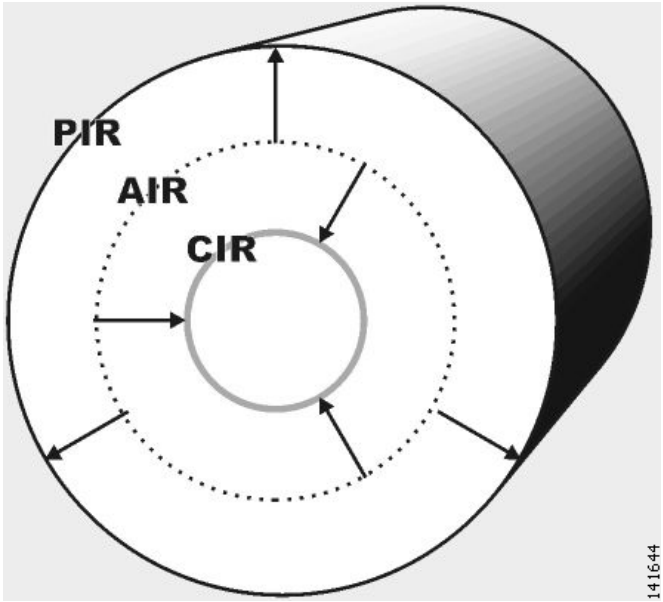
- [Committed Information Rate (CIR)]：BWC が制御するサービスに割り当てられる最小帯域幅
- [Peak Information Rate (PIR)]：BWC が制御するサービスに割り当てられる最大帯域幅
- [Global Controller]：この BWC のリンク先グローバル コントローラ
- [Assurance Level (AL)]：トラフィック輻輳時に利用可能な帯域幅が変化するレート

図 3-3 に示すように、利用可能な最大帯域幅（Admitted Information Rate（AIR））は CIR から PIR までの範囲になります。実際に消費される帯域幅は、常に AIR 未満です。

BWC には、さまざまな輻輳条件で AIR の判別方法を制御する 3 番めのパラメータがあります。システムは、ネットワークが輻輳していない場合は PIR を、ネットワークの輻輳が激しい場合は CIR を実現します。これらの 2 つの極端な状態の間では、AIR は 3 番めのパラメータ [Assurance Level (AL)] によって決定されます。AL は、輻輳増加時に AIR が PIR から CIR に低下する速度を、輻輳緩和時に AIR が CIR から PIR に増大する速度を制御します。AL が小さい場合よりも、AL の値が大きい方が、AIR が大きくなります。

BWC は、ネットワークが輻輳していても（PIR 輻輳）、最低限 CIR が保証されるようにします。同様に、BWC は、BWC に関連付けられているトラフィックがほとんどなくても、PIR を超えないように保証します。

図 3-3　　帯域幅制御レベル



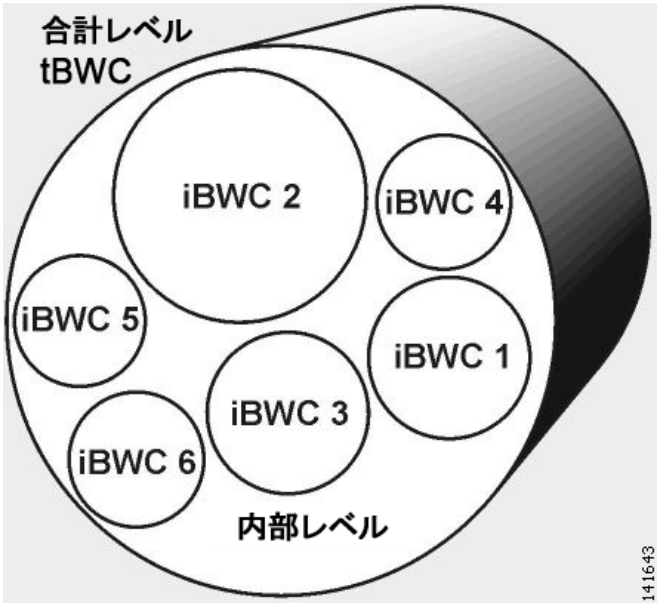
帯域幅は、調整可能な幅の仮想パイプとして考えることもできます。PIR は仮想パイプの最大許容幅です。CIR はこのパイプが収縮する際の最小幅です。AIR は、このパイプの実際の幅です。ネットワークの輻輳時は、システムは各パイプを個別に縮小して、サブスクライバ間およびサービス間で差別化します。

プライマリと内部の帯域幅の制御

図 3-4 に示すように、SCA BB では、各サブスクライバに独立した BWC セットがあります。この BWC セットは、そのサブスクライバに使用可能な総帯域幅を制御する単一のプライマリ（合計）BWC（tBWC）と、そのサブスクライバの一部のサービスに使用できる帯域幅を制御するいくつかの内部 BWC（iBWC）で構成されています。たとえば、ある BWC がストリーミング サービスを制御し、別の BWC がダウンロードと E メールのサービスをまとめて制御する場合があります。

関連付けられているサービスの最大帯域幅は PIR によって、最小帯域幅は CIR によって定義されます。

図 3-4　　2 つのレベルの帯域幅制御



iBWC は次の方法でトラフィックにリンクできます。

1. パッケージ全般を定義する場合は、1 つのサブスクライバ BWC を追加して、その CIR、PIR、AL、および CoS によって定義します。
2. 規則を定義する場合は、各サービスを 1 つのサブスクライバ BWC に割り当てます。

クォータ管理

指定したサービスのクォータ制限をサブスクライバに割り当てることができます。

各サブスクライバには 16 のクォータ バケットがあり、バケットごとにボリュームやセッションが定義できます。サブスクライバが特定のサービスを使用すると、使用したボリュームやセッション数の総計がいずれかのバケットから差し引かれます。

各サービスで使用するバケットはサービス コンフィギュレーションで指定します。ボリューム バケットの消費量は、L3 KB で測定します。セッション バケットの消費量はセッション数で測定します。たとえば、ブラウジングと E メール サービスをバケット #1 のクォータで消費し、P2P サービスをバケット #2 のクォータで消費し、その他のサービスはいずれも特定のバケットにバインドされないように定義することができます。

外部クォータ プロビジョニング システムでクォータ プロビジョニング API を使って、各バケットのクォータを動的に変更することができます。クォータ プロビジョニング API については、『*Cisco SCMS SCE Subscriber API Programmer's Guide*』を参照してください。たとえば、サブスクライバがクォータを追加購入した場合は特定のバケットのクォータを増やすことができます。これらの外部システムから各バケットのクォータの残量を問い合わせることもできます。この方法を使用すると、たとえば、サブスクライバ個人の Web ページにクォータの残量を表示させることができます。

外部クォータ プロビジョニングは、Quota Manager（QM）を使って取得することもできます。QM はシスコが提供するソリューションです。QM のインストールおよび動作の詳細については、『*Cisco Service Control Management Suite Quota Manager User Guide*』を参照してください。

外部クォータ プロビジョニングは、Gy クォータ モデルを使って取得することもできます。詳細については、『*Cisco Service Control Mobile Solution Guide*』を参照してください。

（注）　単方向分類が有効になっている場合、外部クォータ プロビジョニングはサポートされません。

内部 SCA BB クォータ プロビジョニング システムは、各クォータ バケットの容量が一定となるように一定の間隔で補充します。

バケットのクォータが使用できなくなった場合はサブスクライバに通知されます。

サブスクライバ通知

サブスクライバ通知機能を使用すると、サブスクライバ HTTP トラフィックを該当する Web ページにリダイレクトさせ、Web ベースのメッセージ（クォータの枯渇など）をサブスクライバに送信させることができます。HTTP のリダイレクションは、サブスクライバ通知がアクティブになると開始し、サブスクライバ通知が解除されると終了します。

（注）　単方向分類が有効になっている場合、サブスクライバ通知はサポートされません。

その他のトラフィック処理機能

このセクションでは、SCA BB のその他トラフィック処理機能について説明します。

- 「サービス セキュリティ」（P.3-18）
- 「トラフィック フィルタ」（P.3-20）
- 「Value Added Services サーバへのトラフィック フォワーディング」（P.3-20）

サービス セキュリティ

SCA BB にはサービス セキュリティ機能が用意されており、ネットワーク オペレータやサブスクライバを次のような攻撃や悪質なトラフィックから保護します。

- Denial of Service（DoS; サービス拒絶）攻撃
- DDoS 攻撃
- VoIP 脅威
- ワーム
- ハッカーの活動
- サブスクライバ コンピュータが悪質な乗っ取りに遭うこと
  - スパム ゾンビ
  - E メール ベースのウイルス

Service Control ソリューションを使用してもネットワークの脅威から完全に保護することは不可能ですが、ネットワーク内での悪質な活動を見抜き、ネットワーク全体のパフォーマンスを損なわないように広範囲にわたる悪質な活動を抑えることはできます。

ネットワーク オペレータは SCA BB で次のことが実行できます。

- 疑わしい動きのあるネットワーク トラフィックを監視する。
- 悪質なトラフィックをブロックする。

- 悪質なトラフィックを発生させているサブスクライバ、または影響を受けているサブスクライバに通知する。

悪質なトラフィックの検出

SCA BB には 3 つの脅威検出メカニズムがあります。

- 異常検出：ホスト IP アドレス同士の接続速度（成功した場合も失敗した場合も）をモニタします。接続速度が速い場合、または接続の成否の比率が低い場合は悪質なアクティビティであることを示します。

  異常検出機能により、次のカテゴリのアクティビティであることがわかります。

  - IP スウィープ：同一ポート上の複数の IP アドレスをスキャン（ワームの典型的な行動）
  - ポート スキャン：1 つの IP アドレスの全ポートをスキャン（ハッカーの典型的な行動）
  - DoS 攻撃：1 つの IP アドレスから 1 つの IP アドレスへの攻撃
  - DDoS 攻撃：複数の IP アドレスから 1 つの IP アドレスへの攻撃

（注）　SCA BB は、スプーフィングを行う DoS 攻撃を DDoS 攻撃と認識します（本物ではなく偽の IP アドレスが多数使用されます）。

- 異常検出メカニズムは、新しい脅威の出現に対応する場合に効果的です。脅威の本質やレイヤ 7 シグニチャについて知る必要がなく、ネットワーク アクティビティの特性に基づいているからです。
- 大量のメール配信の検出：個別のサブスクライバの SNMP セッション比率をモニタします（SCE プラットフォーム サブスクライバ アウェアネスを使用します。サブスクライバアウェア モードまたはアノニマス サブスクライバ モードで動作するからです）。単一サブスクライバからの SMTP セッション レートが高いということは、E メール送信に関連する悪質アクティビティを一般的に示します（E メールベースのウイルスまたはスパムゾンビ アクティビティ）。
- シグニチャ ベースの検出：SCE プラットフォームのステートフル レイヤ 7 機能を使用して、他のメカニズムでは検出が難しい悪質なアクティビティを検出します。オペレータはこのような脅威のシグニチャを追加し、新しい脅威に素早く反応することができます。

悪質なトラフィックへの応答

前のセクションで説明した検出メカニズムを設定する場合は、次の対策を実行します。

- これらのメカニズムで検出された悪質なアクティビティについてネットワークをモニタする。

  悪質なアクティビティ分析で収集したデータのグラフを Console に表示できます。
- SCE プラットフォームによって検出された悪質なアクティビティを自動的にブロックし、ネットワークに脅威が広まって悪影響が出るのを防ぐ。
- サブスクライバの Web セッションを専用ポータルにリダイレクトし、悪質なアクティビティの被害に遭っていることを知らせる。

SCA BB には高度な柔軟性があり、検出メソッドを調整して悪質なアクティビティを定義したり、悪質なアクティビティが検出された場合の対策を設定することができます。

トラフィック フィルタ

フィルタ規則はサービス コンフィギュレーションの一部です。フィルタ規則を指定すると、SCE プラットフォームに一部のフロー タイプ（フローのレイヤ 3 およびレイヤ 4 プロパティによる）を無視させ、フローを変更なしで伝送させることができます。

トラフィック フローが SCE プラットフォームに着信すると、SCE プラットフォームはこのフローにフィルタ規則が適用できるかどうかを調べます。このトラフィック フローにフィルタ規則を適用する場合、SCE プラットフォームは次の処理のいずれかを実行します。

- バイパス：SCE プラットフォームはトラフィック フローを伝送キューに渡します。このとき RDR は生成されず（分析を目的として生成されたレコードにはこのフローは含まれません）、サービス コンフィギュレーション規則も適用されません。
- クイック フォワーディング：遅延に影響されやすいフローの低遅延を保証するためのフロー フィルタ規則動作です。クイック フォワーディングで転送されたフローのパケットは複製され、別のパスを通じて送信されます。複製の一方が直接送信キューに入るので、遅延は最小限にとどまります。もう一方の複製は通常のパケット パスで送信されます。

フィルタ規則では、フィルタ処理されたトラフィックの DSCP ToS 値も設定できます （「DSCP ToS マーキング」（P.3-20）を参照）。

SCE プラットフォームを通過する Operational Support System（OSS; オペレーション サポート システム）プロトコル（Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）など）、およびルーティング プロトコル（Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）など）にフィルタ規則を追加することを推奨します。このようなプロトコルは一般的にポリシーの実施から影響を受けず、ボリュームが少ないので、レポートする必要性はあまりありません。

デフォルト サービス コンフィギュレーションには多数のフィルタ規則が用意されています。

特定プロトコルのフローを、そのフローのレイヤ 7 特性に基づいてフィルタリングすることもできます。

DSCP ToS マーキング

DSCP ToS マーキングは、ネットワーク要素間のフローのタイプとプライオリティを通知するために IP ネットワークで使用されます。DSCP ToS マーキングは、通常はネットワークでのトラフィックの処理方法を認識している要素によって実行されます。こうした要素は、音声ゲートウェイなどトラフィックを生成する要素の場合もあります。たとえばアプリケーション アウェアである SCA BB は、ビジネス モデルや、遅延に影響されやすいアプリケーション固有のニーズに基づいて、帯域幅リソースを割り当てることができます。

Value Added Services サーバへのトラフィック フォワーディング

Value Added Services（VAS）サーバへのトラフィック フォワーディング機能を利用すると、Service Control ソリューションで外部エキスパート システム（VAS サーバ）を使ってトラフィック処理を追加できます。SCE は事前設定された VAS サーバのロケーションにトラフィックを再ルーティングします。処理後はトラフィックが SCE に戻され、本来の宛先に送信されます。

（注）　単方向分類が有効になっている場合、VAS トラフィック フォワーディングはサポートされません。

サービス コンフィギュレーション

サービス コンフィギュレーションは、プロバイダーのビジネス戦略と展望を実現し強化します。

サービス コンフィギュレーションは、該当する SCE プラットフォームに伝播されて初めて有効になります。サービス コンフィギュレーションは、SCA BB を通過するネットワーク トラフィックを分析することで強化されます。

サービス コンフィギュレーションの構成は次のとおりです。

- トラフィック分類の設定：Web ブラウジングなどのサービス、ファイル共有、および VoIP。それぞれのサービスは、ネットワーク トラフィックとサービスのマッピング方法を定義する要素で構成されています。サービスのコンフィギュレーション構築ブロックは、プロトコル、ゾーン、フレーバ、シグニチャです。
- トラフィックのアカウンティングとレポートの設定：トラフィック フローおよびネットワークの従量制課金をレポートする方法に関する設定。
- トラフィック制御の設定：サービス別に定義された一連の規則（帯域幅レート制限やクォータ制限など）で構成されたパッケージ。パッケージの主なコンフィギュレーション構築ブロックは、規則、クォータ バケット、サブスクライバ BWC、グローバル コントローラです。

サービス コンフィギュレーション定義の実際

実際のサービス コンフィギュレーション定義は繰り返し処理です。

次の手順を推奨します。

1. システムをセット アップします。
2. デフォルトのサービス コンフィギュレーションを適用します。
3. データを収集します。
4. 分析します。
5. 次のいずれかまたは両方を実行します。
   - トラフィックをさらにサービスに分割してトラフィックを検出する。
   - サービスおよびサブスクライバのパッケージに基づいてトラフィックの制限や優先順位の規則を作成する。

CHAPTER 4

使用する前に

はじめに

ここでは、Cisco Service Control Application for Broadband（SCA BB）のインストールまたはアップグレードのプロセスを説明します。

- 新規およびアップデート済みシグニチャが含まれたプロトコル パケットのインストール方法を説明します。
- ツールの集合体としての Console の概念を説明し、各ツールとその役割を示して、ツールの起動方法およびツール間のナビゲーション方法について説明します。
- 最後の「クイック スタート」では、最初のサービス コンフィギュレーションの適用方法および最初のレポートの作成方法を説明します。

SCA BB のインストール方法

SCA BB のインストールは 2 段階のプロセスで行います。

1. SCA BB フロント エンドをインストールします。
   - SCA BB Console
   - SCA BB サービス コンフィギュレーション ユーティリティ、SCA BB シグニチャ コンフィギュレーション ユーティリティ、および SCA BB リアルタイム モニタリング コンフィギュレーション ユーティリティ
2. SCA BB アプリケーション コンポーネントをインストールします。
   - SCA BB Service Modeling Language Loadable Image（SLI; サービス モデリング言語ロード可能イメージ）および SCA BB Service Control Engine（SCE）
   - SCA BB Subscriber Manager 適用可能管理プラグイン（Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）のあるシステム用）

既存の SCA BB をアップグレードする場合は、「SCE Software Upgrade ウィザードを使用した SCE のアップグレード方法」（P.4-8）または「プロトコル パックの処理」（P.4-19）を参照してください。

SCA BB インストール パッケージ

SCA BB インストール パッケージは CCO（Cisco.com）にある ZIP ファイルです。

インストール パッケージは次のファイルで構成されています。

- Console のインストーラ：scas-bb-console-<version>-<build>.exe。
- 各種 SCE プラットフォーム のシスコ製インストール アプリケーション パッケージ ファイル（PQI ファイル）：各 PQI ファイルは、名前がプラットフォーム名のサブフォルダ内にあります。
- scas_bb_util.tgz ファイル：SCA BB サービス コンフィギュレーション ユーティリティ用のファイル（**servconf**）、SCA BB シグニチャ コンフィギュレーション ユーティリティ用のファイル（**sigconf**）、および SCA BB リアルタイム モニタリング コンフィギュレーション ユーティリティ用のファイル（**rtmcmd**）（リアルタイム モニタリング レポート用テンプレートを含む）で構成されています。
- PCubeEngageMib.mib ファイル：SCAS BB MIB を定義したもので、SNMP サブフォルダ内にあります。
- SCA BB Service Configuration Java API 配信ファイル：serviceconfig-java-api-dist.tgz。
- surfcontrol.xml ファイル：SurfControl Content Port Authority を使用するコンテンツ フィルタリング用のコンテンツ カテゴリを一覧表示します。URL Filtering フォルダ内にあります。

SCA BB アプリケーション コンポーネントのインストール

SCA BB には、SCE プラットフォームに常駐する次の 2 種類のソフトウェア コンポーネントがあります。

- SCA BB SLI：トラフィック処理を実行します。
- SCA BB SCE 適用可能管理プラグイン：サービス コンフィギュレーション操作を実行します。

SCA BB には、SM デバイスに常駐する次のソフトウェア コンポーネントがあります。

- SCA BB SM 適用可能管理プラグイン：アプリケーション固有のサブスクライバ管理操作を実行します。

Console からこれらのコンポーネントをインストールする場合は、「SCE デバイスへの PQI ファイルのインストール方法」（P.5-23）および「CM デバイスの管理」（P.5-27）を参照してください。

コマンドラインからこれらのコンポーネントをインストールする場合は、「コマンドラインからの PQI ファイルのインストール」（P.13-10）を参照してください。

前提条件

SCA BB をインストールする前に、SCE プラットフォーム、および使用している場合は SCMS-SM が操作可能で、適切なバージョンのソフトウェアが動作していることを確認してください。

- 「SCE プラットフォームが操作可能であることの確認方法」（P.4-3）
- 「SCE プラットフォームで適切な OS バージョンが動作していることの確認方法」（P.4-3）
- 「SM が正しくインストールされていることの確認方法」（P.4-3）
- 「適切な SM のバージョンが動作していることの確認方法」（P.4-3）

SCE プラットフォームが操作可能であることの確認方法

ステップ 1　SCE のステータス LED がグリーンに点滅していることを確認します（オレンジ：起動中、オレンジで点滅：警告、レッド：障害状態）。

SCE プラットフォームで適切な OS バージョンが動作していることの確認方法

ステップ 1　SCE プラットフォームの Command-Line Interface（CLI; コマンドライン インターフェイス）プロンプト（`SCE#`）で、`show version` と入力します。

ステップ 2　**Enter** キーを押します。

SCE プラットフォームで動作中の OS バージョンが応答に表示されます。

SM が正しくインストールされていることの確認方法

ステップ 1　SM への Telnet セッションを開きます。

ステップ 2　SM bin ディレクトリに移動し、`p3sm --sm-status` と入力します。

ステップ 3　**Enter** キーを押します。

このコマンドの応答で、SM の動作ステータスが表示されます。

適切な SM のバージョンが動作していることの確認方法

ステップ 1　SM への Telnet セッションを開きます。

ステップ 2　SM bin ディレクトリに移動し、`p3smversion` と入力します。

ステップ 3　**Enter** キーを押します。

このコマンドの応答で、SM のバージョンが表示されます。

SCA BB フロント エンドのインストール方法

次に示す SCA BB フロント エンドをインストールします。

- Console
- SCA BB サービス コンフィギュレーション ユーティリティ（**servcomf**）、SCA BB シグニチャ コンフィギュレーション ユーティリティ（**sigconf**）、および SCA BB リアルタイム モニタリング コンフィギュレーション ツール（**rtmcmd**）（リアルタイム モニタリング レポート用テンプレートを含む）
  - **servconf** には、Java Runtime Environment（JRE; Java ランタイム環境）へのアクセスが必要です（「Java ランタイム環境のインストール」（P.4-4）を参照）。

ハードウェア要件

- Console を実行するには、1024 MB 以上の RAM が必要です。
- Console がサポートする最小画面解像度は、1024 × 768 ピクセルです。

オペレーティング システム要件

SCA Reporter GUI フロント エンドは、Windows 2000 または Windows XP が動作するすべてのコンピュータにインストールできます。

Java ランタイム環境のインストール

SCA BB サービス コンフィギュレーション ユーティリティ **servconf** は、JRE バージョン 1.6 にアクセスする必要があります。

JRE は Sun™ の Web サイト http://java.com/en/download/ からダウンロードできます。

JRE がインストールされていることを確認するには、コマンド プロンプトから **java -version** を実行します。1.6 以降の Java バージョンが必要です。

ワークステーションに別の JRE のバージョンもインストールされている場合、該当する JRE の場所を検索するように **servconf** に通知する必要があります。それには、JAVA_HOME 環境変数を設定して JRE 1.6 インストール ディレクトリを指定します。たとえば、次のようになります。

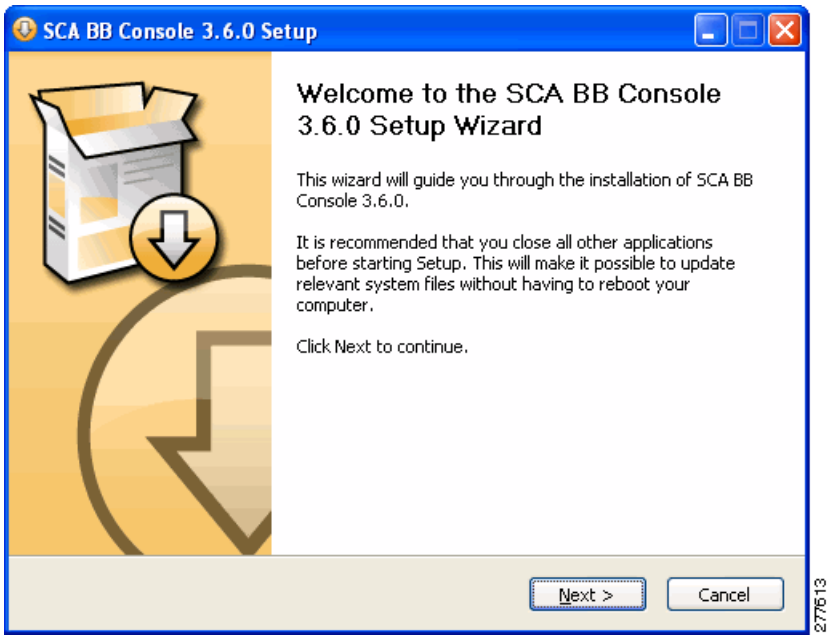
```
JAVA_HOME=C:¥Program Files¥Java¥j2re1.6_08
```

Console のインストール方法

ステップ 1　Console インストール ファイル sca-bb-console-3.6.0.exe に移動し、これをダブルクリックします。

SCAS BB Console 3.6.0 Setup ウィザードの [Welcome] ページが表示されます（図 4-1 を参照）。

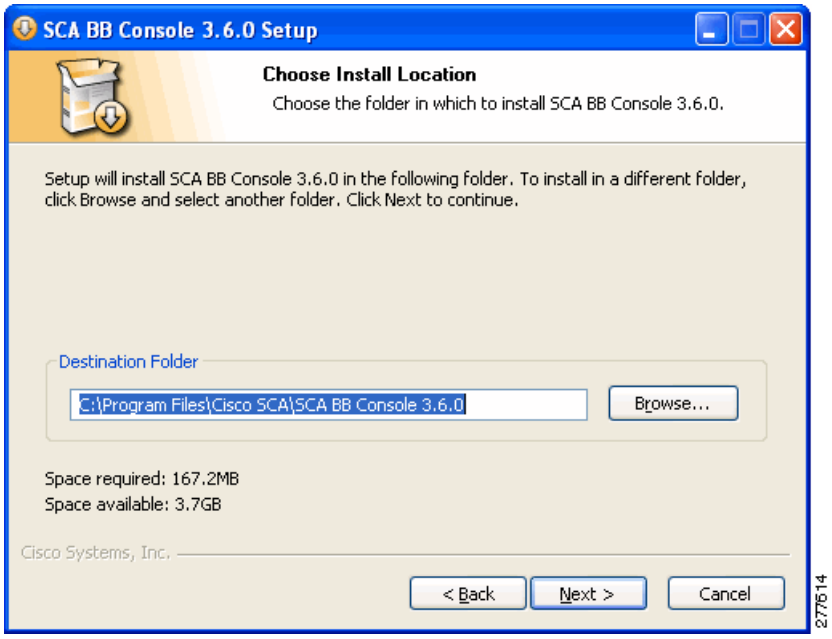
図 4-1　[Welcome to the SCA BB Console Setup Wizard]



ステップ 2　[Next] をクリックします。

Setup ウィザードの [Install Location] ページが開きます（図 4-2 を参照）。

図 4-2　[Choose Install Location]

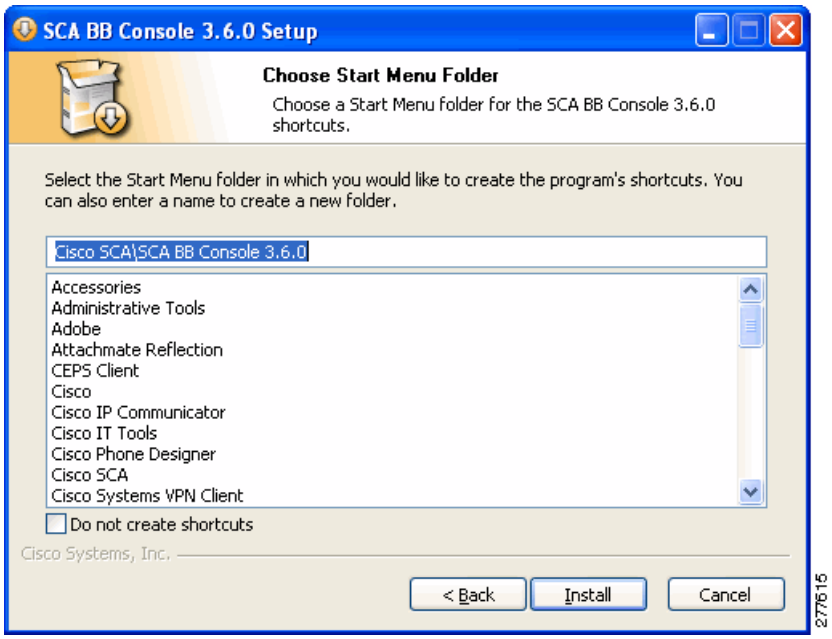


ステップ 3　（オプション）[Browse] をクリックして別の宛先フォルダを選択します。

ステップ 4　[Next] をクリックします。

Setup ウィザードの [Start Menu Folder] ページが開きます（図 4-3 を参照）。

図 4-3　[Choose Start Menu Folder]



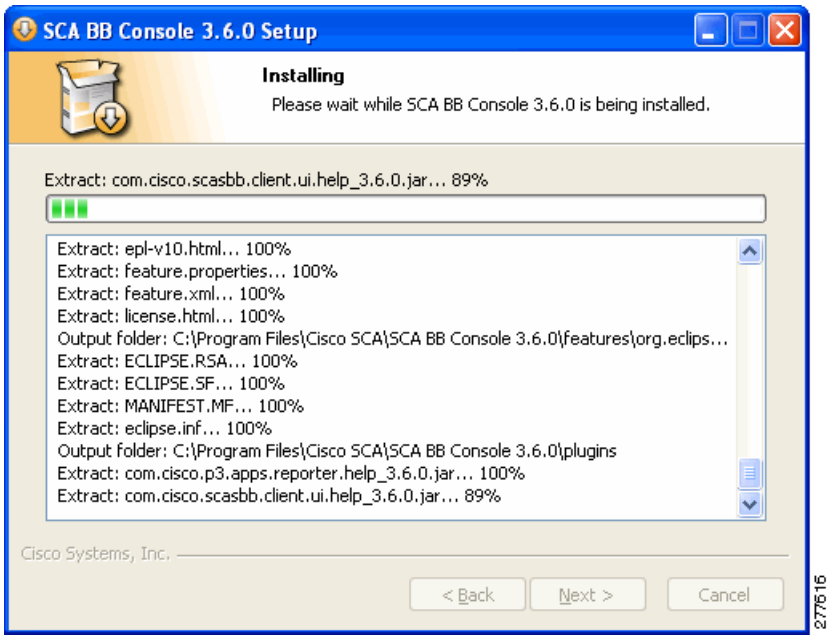
ステップ 5　（オプション）[Start Menu Folder] フィールドに別の Start Menu フォルダを入力します。

ステップ 6　（オプション）[Do not create shortcuts] チェックボックスをオンにします。

ステップ 7　[Install] をクリックします。

Setup ウィザードの [Installing] ページが開きます（図 4-4 を参照）。

図 4-4　[Installing]



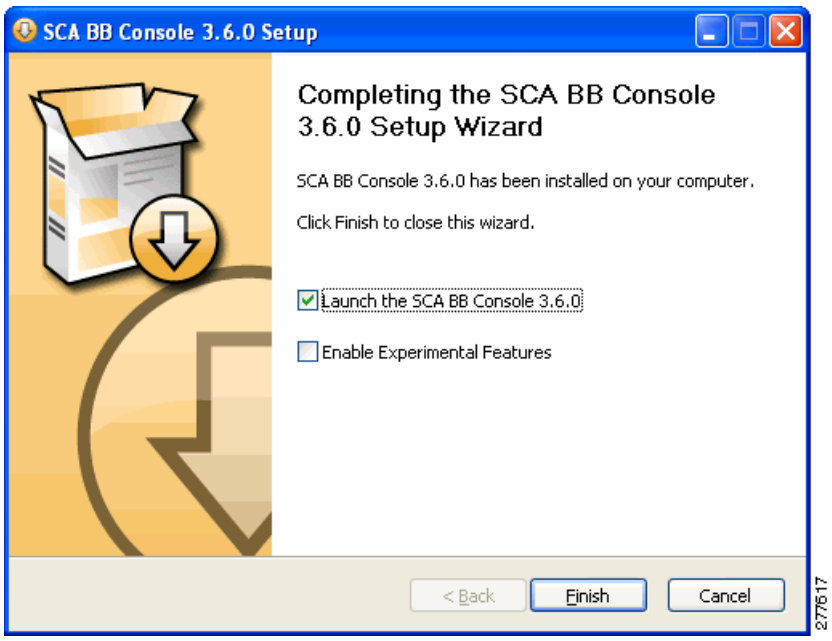
ステップ 8　インストールが完了するまで待機します。

[Next] ボタンがイネーブルになります。

ステップ 9　[Next] をクリックします。

Setup ウィザードの [Installation Complete] ページが開きます（図 4-5 を参照）。

図 4-5　[Completing the SCA BB Console 3.6.0 Setup Wizard]



ステップ 10　Console を起動するには、[Run SCA BB Console after installation] チェックボックスをオンにします。

ステップ 11　[Finish] をクリックします。

SCA BB Console 3.6.0 Setup ウィザードが閉じます。

Console がマシンにインストールされました。

[Start] メニューにショートカットが追加されます。

SCA BB コンフィギュレーション ユーティリティのインストール方法

ステップ 1　SCA BB インストール パッケージから、ファイル scas_bb_util.tgz を展開し、それを、Windows、Solaris、または Linux ワークステーションにコピーします。

ステップ 2　このファイルを新規フォルダで開きます。

SCA BB サービス コンフィギュレーション ユーティリティ（**servcomf**）、SCA BB リアルタイム モニタリング コンフィギュレーション ユーティリティ（**rtmcmd**）（リアルタイム モニタリング レポート用テンプレートを含む）、および SCA BB シグニチャ コンフィギュレーション ユーティリティ（**sigconf**）は、bin フォルダ内にあります。

SCA BB コンポーネントのアップグレード方法

SCA BB のアップグレードには、次の各ソフトウェア コンポーネントのアップグレードが含まれています。

- SCE ファームウェア
- SCE PQI ファイル
- プロトコル パック SPQI ファイル
- ポリシー ファイル

（注） このセクションでは、SCA BB アプリケーション コンポーネントのアップグレードに限定して説明します。シスコ ソリューション全体の詳細なアップグレード手順の説明については、正式リリースに添付されているソリューション アップグレード文書を参照してください。

- 古い PQB ファイルをアップグレードする際に、自動的に変更されるプロトコル ID もあります。変更を示すために次のようなメッセージが表示されます。

```
Protocol ID of BaiBao changed from 80 to 43
Protocol ID of PPLive changed from 81 to 44
```

- 新しい SPQI または PQI ファイルを使用してデバイスをアップグレードすると、アップグレードされないその他のデバイスが故障する可能性があります。
- 新しい SCA BB リリースは、デフォルトの Dynamic Signature Script（DSS）ファイル（前の SCA BB リリースでインストールされた同ファイルを参照）を使用しません。
- 新規リリースのプロトコル パックが使用可能な場合は、製品のインストール後にそのプロトコル パックをインストールします。新規製品のインストール時に古いプロトコル パックをインストール*しないでください*。

SCE Software Upgrade ウィザードを使用した SCE のアップグレード方法

SCE Software Upgrade ウィザードから Network Navigator を使用して SCE をアップグレードできます。

ステップ 1　Network Navigator を開きます。

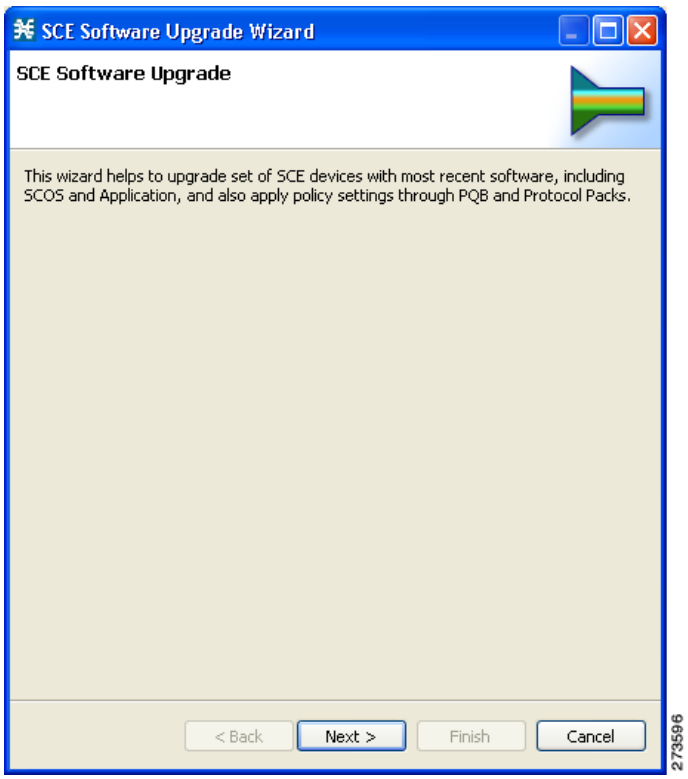
ステップ 2　[Site Manager] ツリーでデバイスを 1 つ以上選択します。

ステップ 3　選択したデバイスのいずれか 1 つを右クリックします。

ステップ 4　表示されるポップアップ メニューから SCE Software Upgrade ウィザードを選択します。

SCE Software Upgrade ウィザードが表示されます（図 4-6 を参照）。

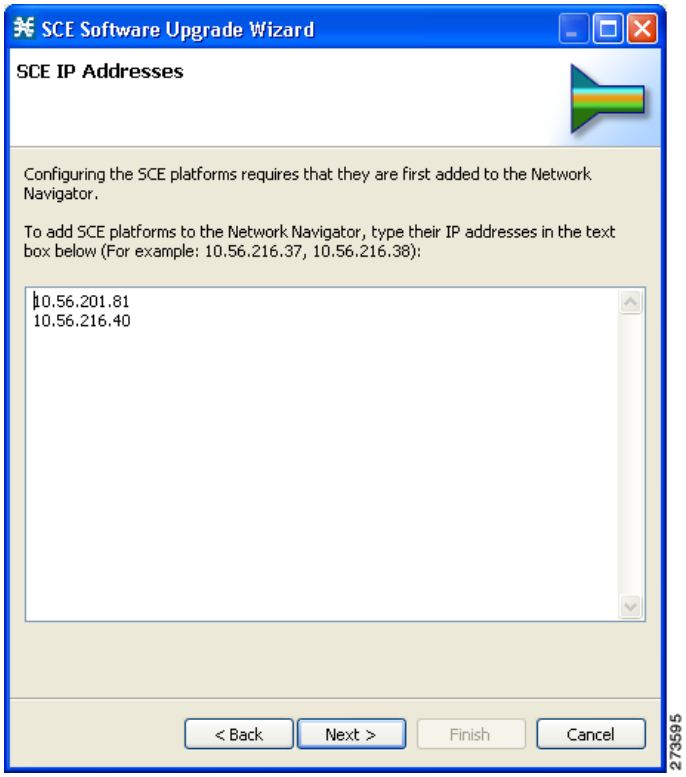
図 4-6　[SCE Software Upgrade]



ステップ 5　[Next] をクリックします。

SCE Software Upgrade ウィザードの [SCE IP Addresses] ページが開きます（図 4-7 を参照）。

図 4-7　　[SCE IP Address]

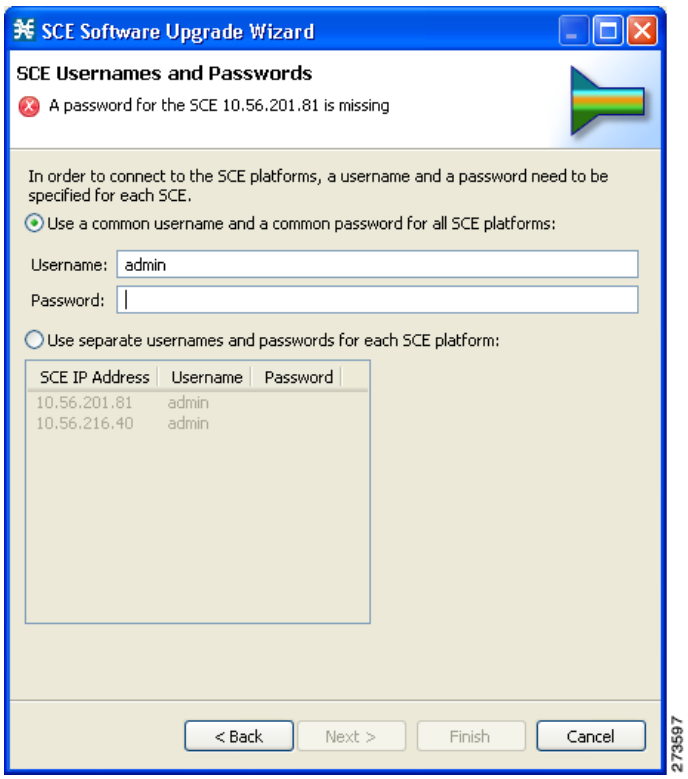


ステップ 6　（オプション）編集ボックスに追加の IP アドレスを入力します。

ステップ 7　[Next] をクリックします。

SCE Software Upgrade ウィザードの [SCE Usernames and Passwords] ページが開きます（図 4-8 を参照）。

図 4-8　[SCE Usernames and Passwords]



ステップ 8　SCE デバイスのユーザ名とパスワードを入力します。

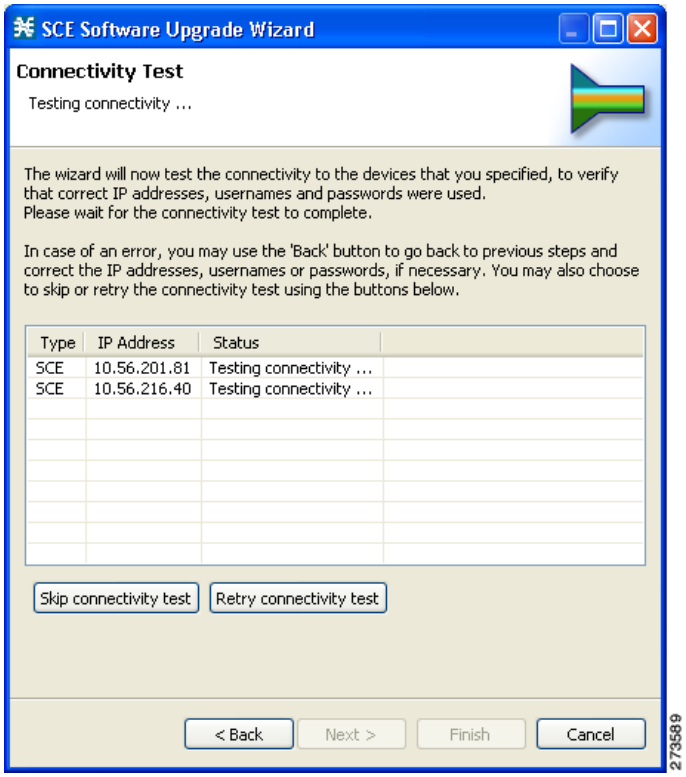
次のうちいずれかを実行します。

- 追加するすべての SCE デバイスに同じユーザ名とパスワードを使用するには、[Username] フィールドにユーザ名、[Password] フィールドにパスワードを入力します。
- 各 SCE デバイスに異なるユーザ名とパスワードのペアを設定するには、[Use separate usernames and passwords for each SCE platform] オプション ボタンを選択し、各 SCE デバイスごとに、テーブルの該当するセルにユーザ名とパスワードを入力します。

ステップ 9　[Next] をクリックします。

SCE Software Upgrade ウィザードの [Connectivity Test] ページが開きます（図 4-9 を参照）。

図 4-9　[Connectivity Test]



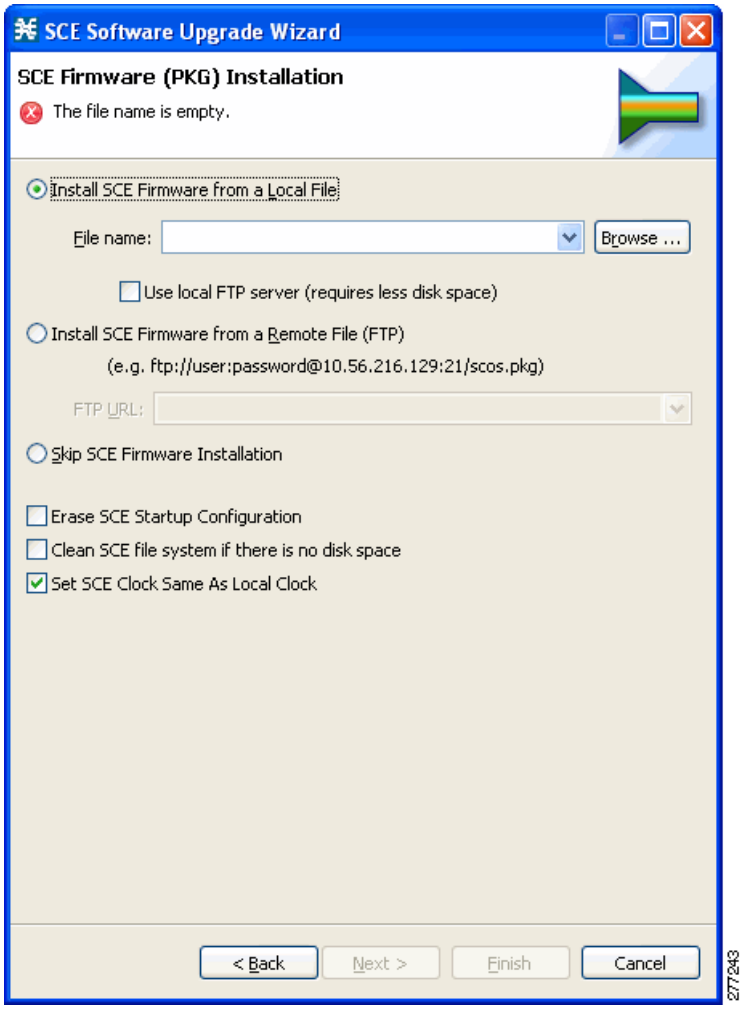
ウィザードは、定義済みデバイスへの接続が可能かどうかを確認するためのテストを実行します。

（注） 1 つ以上のデバイスに接続できない場合、または接続に何らかの問題がある場合（デバイスのバージョンが無効など）は、そのデバイスの横にエラーが表示されます。[Skip connectivity test] をクリックすると、このテストを省略できます。ウィザードの最後で [Finish] をクリックすると接続が検証されます。

ステップ 10　[Next] をクリックします。

SCE Software Upgrade ウィザードの [SCE Firmware (PKG) Installation] ページが開きます（図 4-10 を参照）。

図 4-10　[SCE Firmware (PKG) Installation]



SCE ファームウェアのインストール ファイルを選択します。

次のうちいずれかを実行します。

- SCE ファームウェアをローカル ファイルからインストールするには、[Browse] をクリックします。

  [Select file] ダイアログボックスが表示されます。

  インストールしている SCE ファームウェアのインストール ファイルをブラウズします。

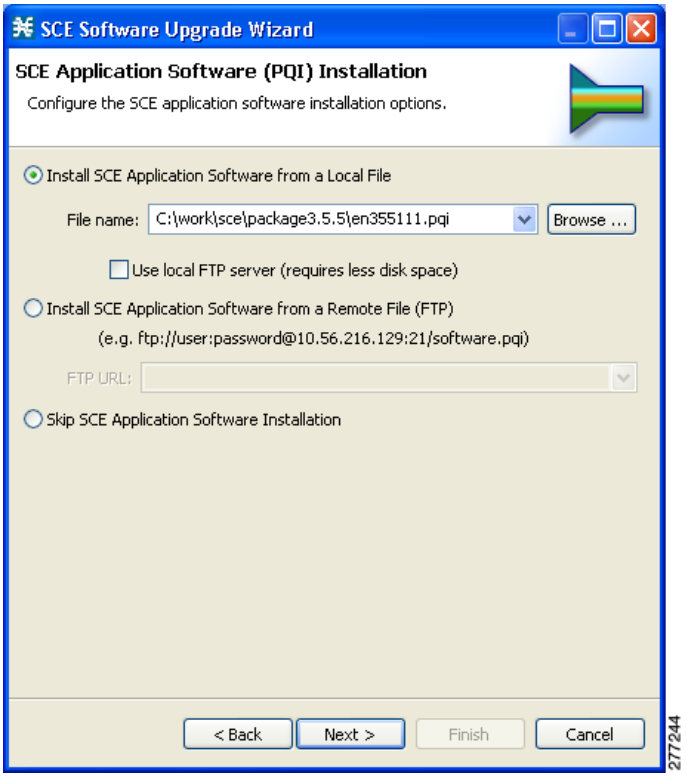
  ディスク スペースの使用量を減らすには、[Use local FTP server] チェックボックスをオンにします。
- SCE ファームウェアをリモート サイトからダウンロードするには、[Install SCE Firmware from a Remote File (FTP)] オプション ボタンを選択し、[FTP URL] フィールドに URL を入力します。

ステップ 11　[Skip SCE Firmware Installation] オプション ボタンを選択します。

ステップ 12　[Next] をクリックします。

SCE Software Upgrade ウィザードの [SCE Application Software (PQI) Installation] ページが開きます（図 4-11 を参照）。

図 4-11　[SCE Application Software (PQI) Installation]



ステップ 13　PQI のインストール ファイルを選択します。

次のうちいずれかを実行します。

- PQI ファイルをローカル ファイルからインストールするには、[Browse] をクリックします。

  [Select file] ダイアログボックスが表示されます。

  インストールしている PQI ファイルをブラウズします。

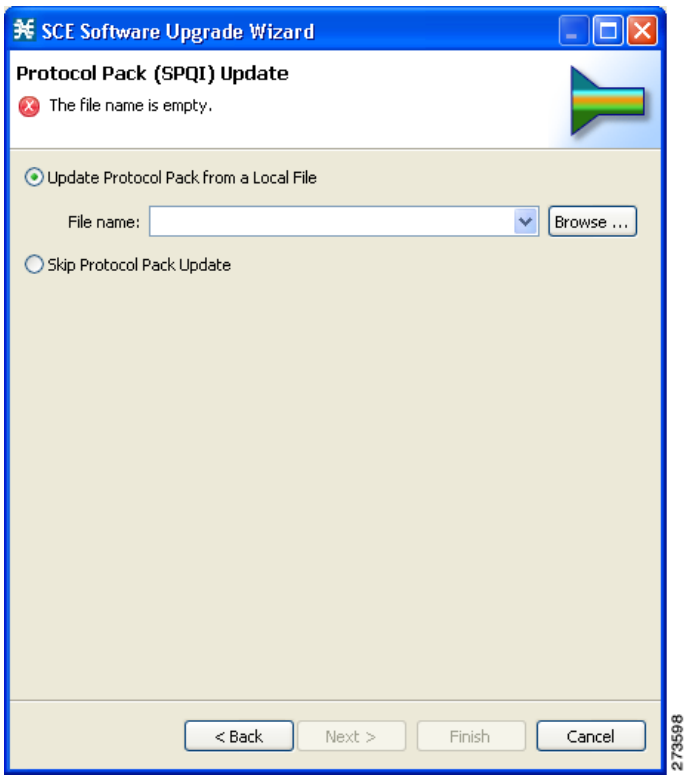
  ディスク スペースの使用量を減らすには、[Use local FTP server] チェックボックスをオンにします。
- PQI ファイルをリモート サイトからダウンロードするには、[Install SCE Application Software from a Remote File (FTP)] オプション ボタンを選択し、[FTP URL] フィールドに URL を入力します。

  [Skip SCE Software Application Installation] オプション ボタンを選択します。

ステップ 14　[Next] をクリックします。

SCE Software Upgrade ウィザードの [Protocol Pack (SPQI) Update] ページが開きます（図 4-12 を参照）。

図 4-12　[Protocol Pack (SPQI) Update]



ステップ 15　プロトコル パックをアップデートします。

次のうちいずれかを実行します。

- SPQI ファイルをローカル ファイルからアップデートするには、[Browse] をクリックします。

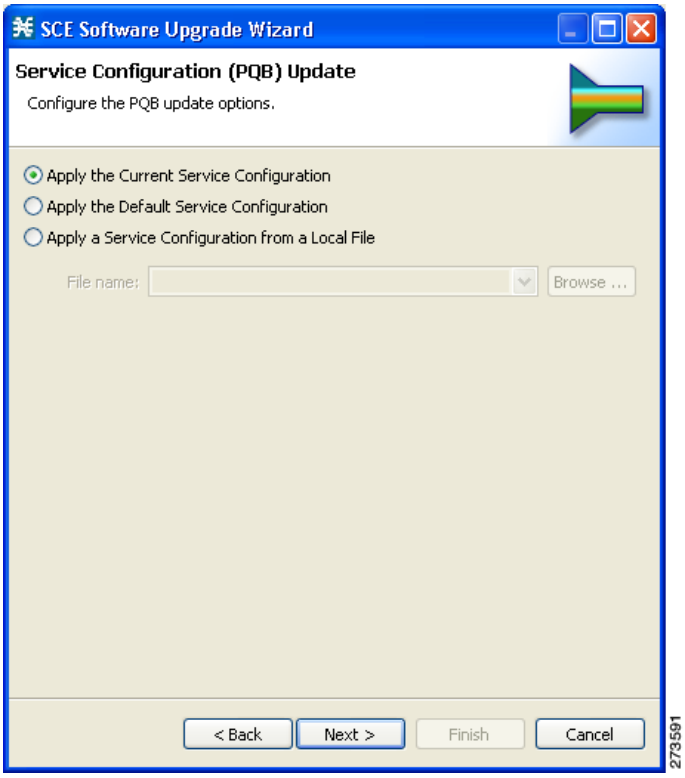
  [Select file] ダイアログボックスが表示されます。

  アップデートしている SPQI ファイルをブラウズします。
- [Skip Protocol Pack Update] オプション ボタンを選択します。

ステップ 16　[Next] をクリックします。

SCE Software Upgrade ウィザードの [Service Configuration (PQB) Update] ページが開きます（図 4-13 を参照）。

図 4-13　[Service Configuration (PQB) Update]



ステップ 17　次の PQB アップデート オプションのいずれかを選択します。

- [Apply the Current Service Configuration]：現在のサービス コンフィギュレーションを維持します。
- [Apply the Default Service Configuration]：製品に付属しているデフォルトのサービス コンフィギュレーションを適用します。
- [Apply the Service Configuration from a Local File]：サービス コンフィギュレーションをローカル ファイルから適用します。

ステップ 18　[Apply the Service Configuration form a Local File] オプション ボタンを選択した場合は、[Browse] をクリックします。

[Select file] ダイアログボックスが表示されます。

サービス コンフィギュレーションが含まれたファイルをブラウズします。

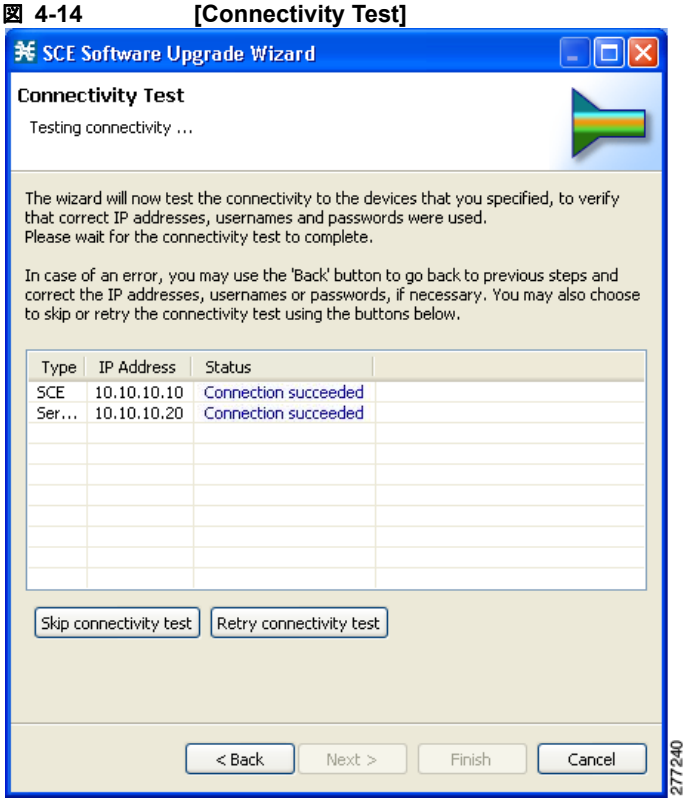
ステップ 19　[Next] をクリックします。

SCE Software Upgrade ウィザードの [Connectivity Test] ウィンドウが開きます。

接続テストにより、定義済みデバイスへの接続が確認されます。

（注）　1 つ以上のデバイスに接続できない場合、または接続に何らかの問題がある場合（デバイスのバージョンが無効など）は、そのデバイスの横にエラーが表示されます。[Skip connectivity test] をクリックすると、このテストを省略できます。ウィザードの最後で [Finish] をクリックすると接続が検証されます。

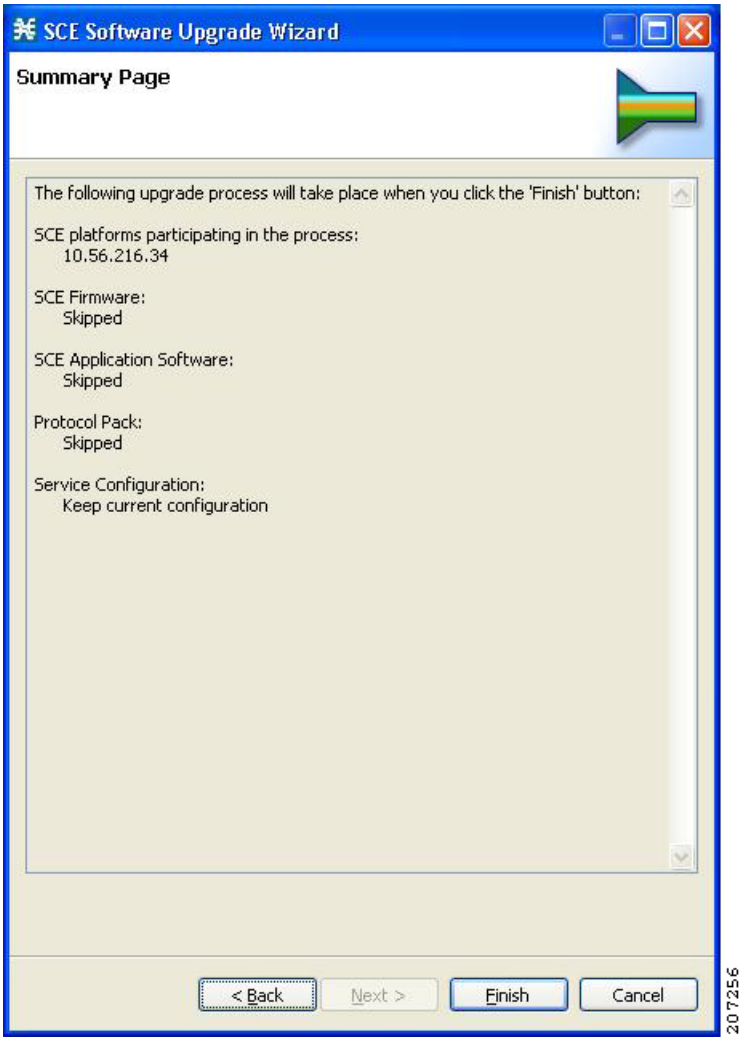
図 4-14　[Connectivity Test]



ステップ 20　[Next] をクリックします。

SCE Software Upgrade ウィザードの [Confirmation] ページが開きます（図 4-15 を参照）。

図 4-15　[Summary Page]

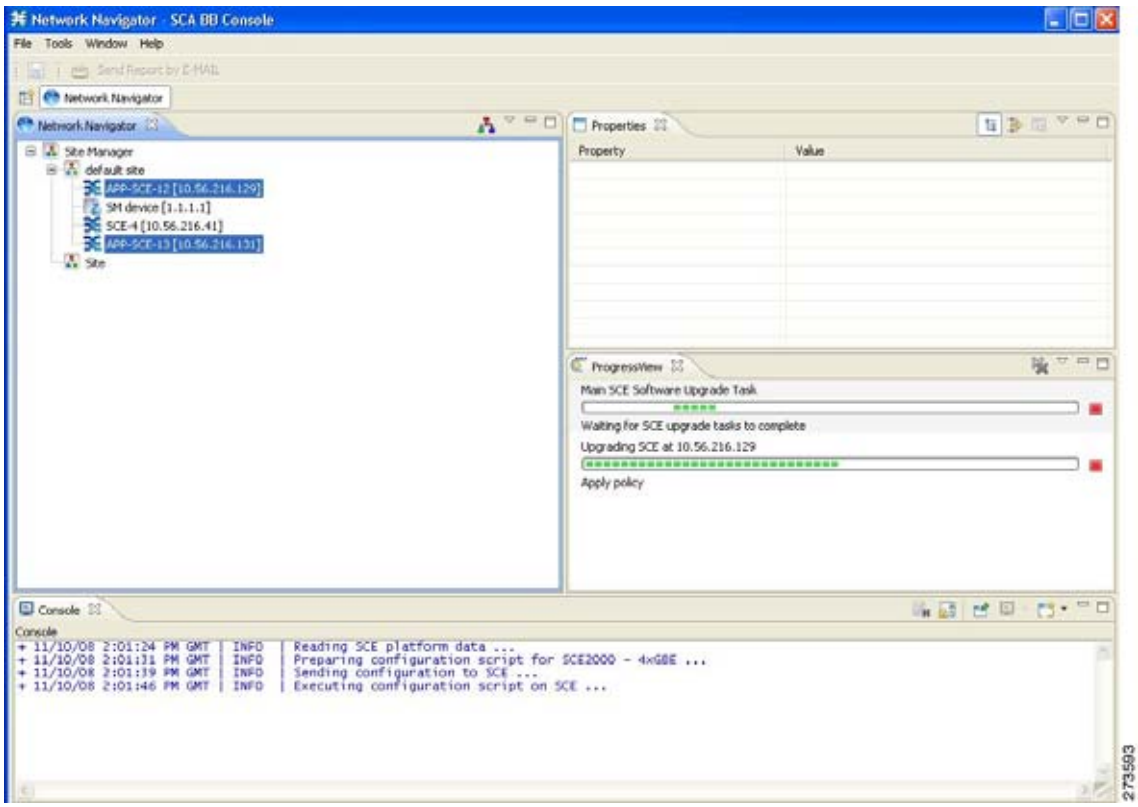


このページには、ウィザードでこれから実行される処理がリストされています。

ステップ 21　[Finish] をクリックします。

[ProgressView] で進捗を確認できます（図 4-16 を参照）。

図 4-16　[Progress]



プロトコル パックの処理

SCA BB は、トラフィック フローの分類で、ステートフル レイヤ 7 機能を使用します。

トラフィック フローがシステムで処理される際に、レイヤ 3 のセットに従ったシグニチャ ID がこのフローの特性を表すレイヤ 7 パラメータ（シグニチャ）に割り当てられます。一般的に、これらのシグニチャは SCA BB に組み込まれます。

変化を続けるプロトコル環境で迅速な応答を可能にするために、SCA BB はシグニチャを動的にアップデートできるように拡張されました。プロトコル サポート プラグインを動作中のシステムにロードして、システムの安定性を損なわずに（既存のソフトウェア コンポーネントのアップデートが不要）、サービス ダウンタイムなしでシステムのプロトコル サポートを強化することができます。

- 「プロトコル パック」（P.4-20）
- 「プロトコル パックのインストール」（P.4-20）
- 「サービス階層ツリーのインストール」（P.4-21）
- 「プロトコル パックのバージョン互換性確認方法」（P.4-27）
- 「プロトコル パックのインストール確認方法」（P.4-27）
- 「SLI の中断のないアップグレード」（P.4-28）

プロトコル パック

シスコでは、SCA BB 用の新規および改良されたプロトコル シグニチャを含むプロトコル パックを定期的に発行しています。一般的なプロトコル パックは、ネットワーク ワーム、一般的なピアツーピア アプリケーション、および他の関連プロトコルを検出するシグニチャを含むファイルです。SCE プラットフォームへのロード中に、これらのシグニチャが SCA BB 分類能力を改善します。

（注）　SCE プラットフォームにプロトコル パックをインストールできるのは、PQI がすでにプラットフォームにインストールされている場合だけです。

SCA BB のプロトコル パックは、DSS ファイルまたは SPQI ファイルのいずれかです。

- SCE プラットフォームに DSS ファイルをロードする場合、SCA BB またはプラットフォームのダウンタイムは不要です。
- SCE プラットフォームに SPQI ファイルをロードする場合、SCE アプリケーションのアップデートが必要です。
  - 中断のないアップグレード（「SLI の中断のないアップグレード」（P.4-28）を参照）がイネーブルになっている場合、SPQI ファイルのロード時に SCE プラットフォームのダウンタイムは発生しません。
  - 中断のないアップグレードが*イネーブルではない*場合、SPQI ファイルのロードには SCE プラットフォームに短時間のダウンタイム（最大 1 分）が必要です。この期間、ネットワーク トラフィックはプラットフォームをバイパスし、管理やレポートは行われません。

（注）　中断のないアップグレードがディセーブルになっている場合、SPQI のインストールによって、すべてのサブスクライバからパッケージ ID、リアルタイム モニタリング フラグ、クォータ設定のデータが失われる可能性があります。サブスクライバには、これらのプロパティのデフォルト値が割り当てられます。

プロトコル パックのインストール

SCE プラットフォームへのプロトコル パックのインストールには、次のいずれかを使用します。

- 「SCA BB サービス コンフィギュレーション ユーティリティ」（P.13-1）
- Network Navigator ツール（「プロトコル パックのインストール方法」（P.5-18）を参照）

（注）　プロトコル パックを SPQI ファイルにインストールすると、中断のないアップグレード CLI コマンドを使用して、中断のないアップグレード オプションをイネーブルにして設定することができます（「SLI の中断のないアップグレード」（P.4-28）を参照）。

ツールまたはユーティリティで次のステップを実行します。

1. SCE プラットフォームから現在のサービス コンフィギュレーションを取得して（任意で）ユーザが指定するフォルダにバックアップ コピーを格納します。
2. DSS または SPQI ファイルにあるシグニチャをサービス コンフィギュレーションにインポートします。これにより、すでにサービス コンフィギュレーションにインポートされた DSS が上書きされます。

3. バディ プロトコル属性（既存プロトコルに指定される属性）（「バディ プロトコル」（P.12-4）を参照）を含む各新規シグニチャの場合は、バディ プロトコルを含む全サービスに新規シグニチャを追加します。
4. プロトコル パックが SPQI ファイルの場合、SCE アプリケーションが置き換えられます。この場合、SCE プラットフォーム サービスに（最大 1 分の）短いダウンタイムが発生します。
5. 新規サービス コンフィギュレーションを SCE プラットフォームに適用します。

プロトコル パックが SPQI ファイルであり、中断のないアップグレード オプションがイネーブルになっている場合、「中断のないアップグレードの CLI コマンド」（P.4-28）を使用してアップグレードの進捗をモニタすることができます。

サービス階層ツリーのインストール

クライアント（GUI）を使用して PQB を開くと、サービス階層ツリー（シグニチャ、フレーバ、プロトコルなど）が表示されます。サービス コンフィギュレーションの階層はクライアントによって定義されます。

SCE から PQB ファイルをロードする場合、PQB 階層ツリーはクライアントの PQB 階層ツリーと同じバージョンである必要があります。つまり、PQB はクライアントと同じバージョンでなければならず、そうでない場合は PQB が開きません。

クライアントはバージョンの異なるさまざまな SCE と接続でき、各 PQB にはさまざまなサービス階層ツリーが定義されている可能性があるため、ユーザは PQB を開く前に、該当するサービス階層ツリーをクライアント（GUI）にインストールしておく必要があります。

クライアントには、SCE バージョンに基づいてサービス階層ツリーをインストールできる機能があります。GUI インストールには、サービス階層要素の固定セットが付属しており、関連する jar ファイル固有のバージョンに配置されています。したがって、ユーザは異なるバージョンに関連するさまざまな jar からファイルを選択できます。

（注）　SCE サービス階層ツリーは、クライアント バージョンとは違います。SCE にサービス階層ツリーをインストールする場合は、次の操作を実行してください。

- PPXY へのアップグレードを行う前に、必ずユーザ PQB をバックアップし、コピーを保存します。これは、PQB が変更されるからです。
- サービス ツリー プロトコルを削除または再インストールします。

サービス階層ツリーを表示、インストール、および削除するには、次の手順を実行します。

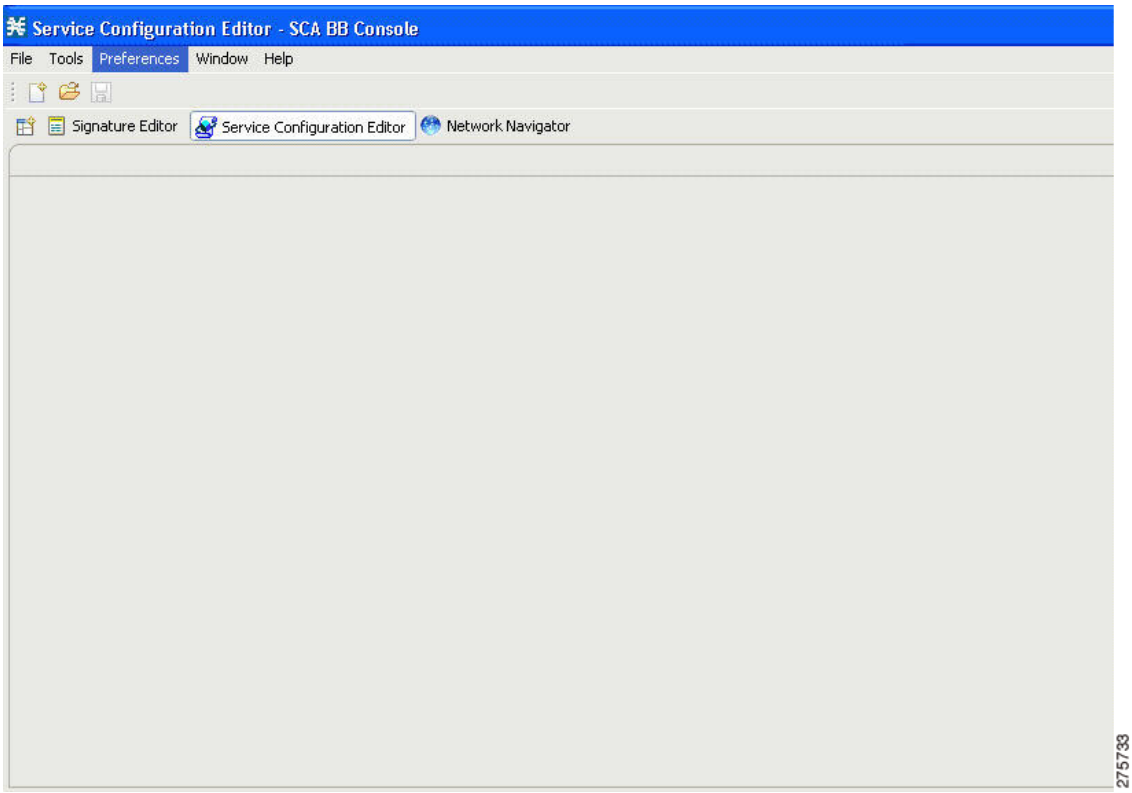
- 「サービス階層ツリーの表示およびインストール」（P.4-22）
- 「サービス階層ツリーの削除」（P.4-26）

サービス階層ツリーの表示およびインストール

ステップ 1　サービス階層ツリーを表示するには、[Protocol Pack] タブを開きます。

ステップ 2　ツールバーで、[Service Configuration Editor] を選択します（図 4-17 を参照）。

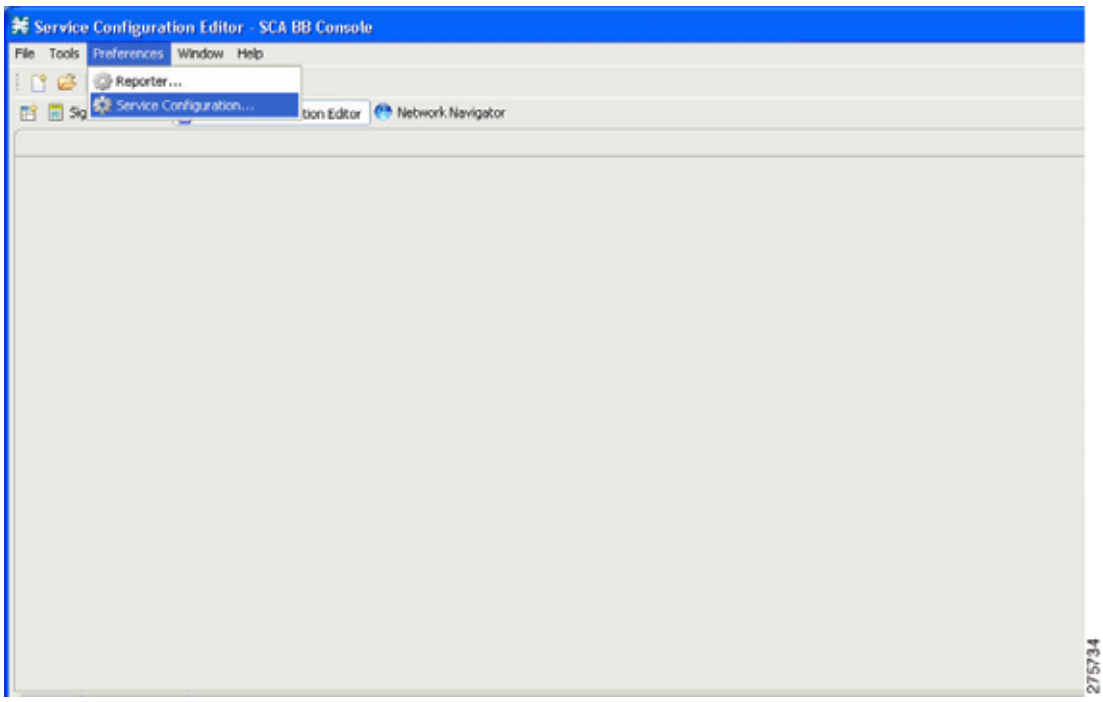
図 4-17　[Service Configuration Editor] : [Preferences]



ステップ 3　[Preferences] を選択し、[Service Configuration] を選択します。

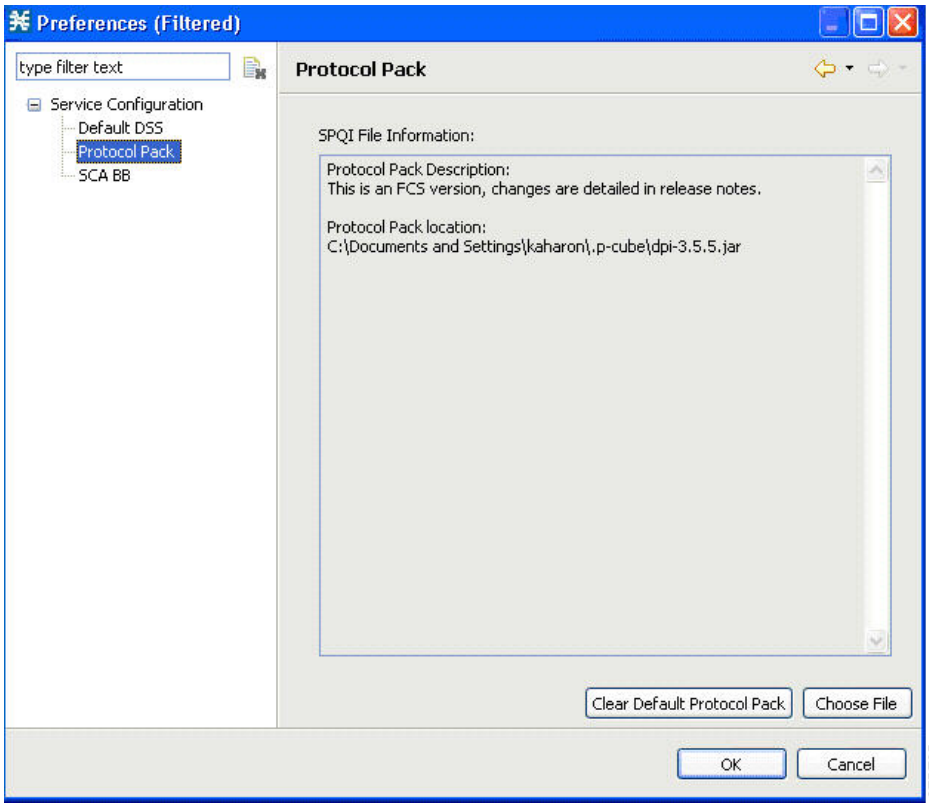
[Preferences] ウィンドウが開きます（図 4-18 を参照）。

図 4-18　[Service Configuration Editor] : [Service Configuration]



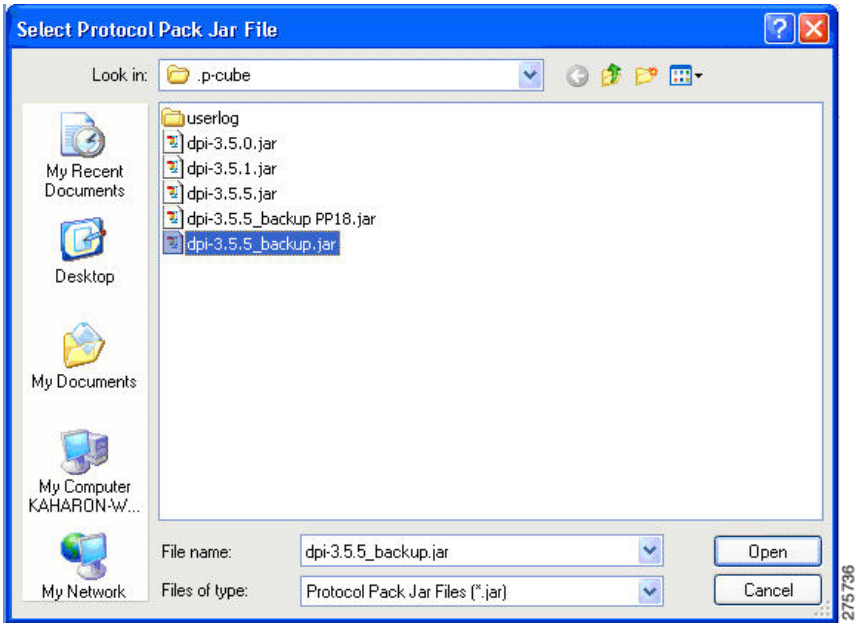
ステップ 4　[Service Configuration] ツリーから [Protocol Pack] を選択します（図 4-19 を参照）。ウィンドウ上部に、GUI に関連するサービス階層ツリーに関する情報が表示されます。

図 4-19　[Preferences (Filtered)]



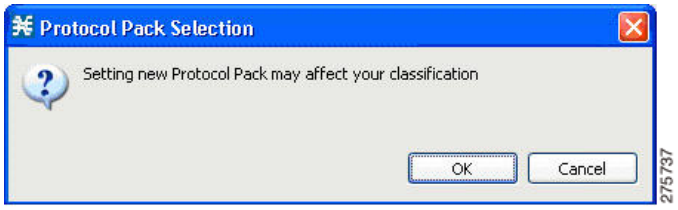
ステップ 5　新しいサービス階層ツリーをインストールするには、[Choose File] ボタンをクリックし、jar ファイルまたは SPQI ファイルを選択します（図 4-20 を参照）。

図 4-20　[Select Protocol Pack]



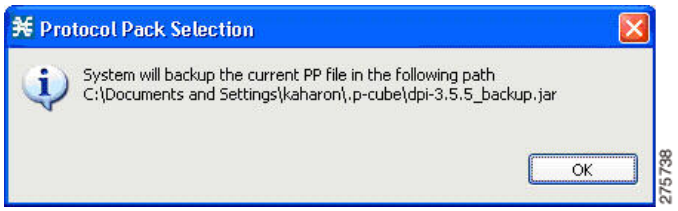
ステップ 6　[Open] を押し、[OK] を押して警告メッセージ（図 4-21 を参照）を承認します。

図 4-21　[Protocol Pack Selection] 警告メッセージ



ステップ 7　現在のプロトコル パックをバックアップして新しいサービス階層ツリーをインストールするには、[OK] を押してバックアップ メッセージ（図 4-22 を参照）を承認します。

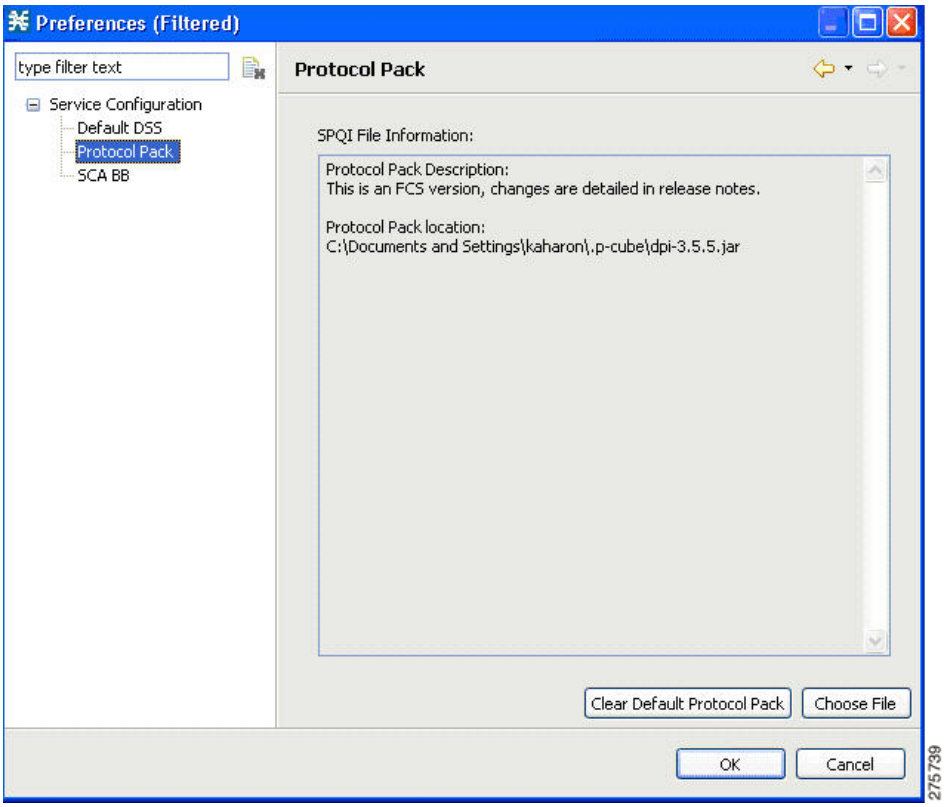
図 4-22　[Protocol Pack Selection] バックアップ メッセージ



サービス階層ツリーの削除

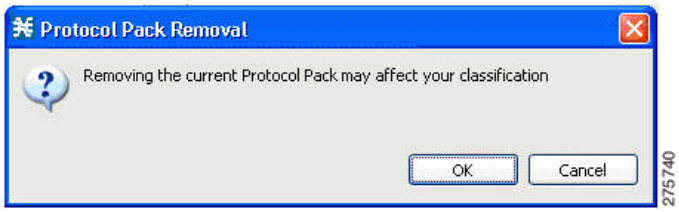
ステップ 1　サービス階層ツリーを削除してデフォルト コンフィギュレーションに戻すには、[Preferences] ウィンドウで [Clear Default Protocol Pack] ボタンを選択します（図 4-23 を参照）。

図 4-23　[Preferences (Filtered)]



ステップ 2　[Protocol Pack Removal] メッセージ画面で [OK] を押して、処理を確定します（図 4-24 を参照）。

図 4-24　[Protocol Pack Removal] メッセージ



サービス階層ツリーがシステムから削除されます。新しい PQB が開くと、クライアントはデフォルトのサービス分類をインストールします。

プロトコル パックのバージョン互換性確認方法

プロトコル パックは、特定のバージョンの SCE アプリケーションとだけ互換性があります。プロトコル パックの作業時には、プロトコル バージョンが SCE アプリケーション バージョンと一致していることを確認してください。たとえば、SCE アプリケーション バージョン 3.6.0 上では 3.6.0 用のプロトコル パックだけを使用します。

各プロトコル パックのバージョン互換性情報は、プロトコル パックのリリース ノートに含まれています。

ステップ 1　**servconf** の正しいバージョンがインストールされ、正常に実行中であることを確認します。

- コマンド プロンプトから `servconf --version` を入力します。
- **Enter** キーを押します。

ユーティリティのバージョンがプロトコル パックのバージョンと一致しているはずです。

ステップ 2　SCE アプリケーションの正しいバージョンがインストールされていることを確認します。

- SCE プラットフォームの CLI プロンプト（`SCE#`）で、`show version` と入力します。
- **Enter** キーを押します。

アプリケーションのバージョンがプロトコル パックのバージョンと一致しているはずです。

ステップ 3　サービス コンフィギュレーション（PQB）が SCE プラットフォームに適用されていることを確認します。

- Console で、現在の PQB を取得して表示します。

プロトコル パックのインストール確認方法

ステップ 1　SCE プラットフォームの CLI プロンプト（`SCE#`）で、**show version** と入力します。

ステップ 2　**Enter** キーを押します。

SCE プラットフォームで動作中の OS バージョンが応答に表示されます。これには、インストールされているプロトコル パックのバージョンに関する情報が含まれています。

ステップ 3　SCE プラットフォームから PQB を取得し、Console を使用してこれを表示します。

ステップ 4　プロトコル パックからの新規プロトコルがサービス コンフィギュレーションに追加されていることを確認します。

プロトコル パックのインストールが失敗した場合、その原因として考えられる問題と解決方法は次のとおりです。

- JRE のバージョンが欠落しているか、または不適切：正しいバージョンの JRE をインストールします（「Java ランタイム環境のインストール」（P.4-4）を参照）。
- SCE プラットフォーム上の SCE アプリケーション バージョンが不適切であるか、欠落している：正しいバージョンの SCE アプリケーションがインストールされていることを確認します（「プロトコル パックのバージョン互換性確認方法」（P.4-27）を参照）。
- SCE プラットフォームにサービス コンフィギュレーション（PQB）が適用されていない：Console を使用して新規 PQB を作成し、適用します。

- **servcomf** が PQB への新規シグニチャのインポートに失敗した：**servconf** 実行中に `--force-signature` アップデート シグニチャ オプションを使用します（「servconf 構文」（P.13-1）を参照）。

シスコに問題を報告する場合は、<user.home>¥.p-cube¥servconf.log にある **servconf** ログ ファイルを添付してください。Windows では、このファイルは通常、C:¥Documents and Settings¥<username>¥.p-cube¥servconf.log にマッピングされています。

SLI の中断のないアップグレード

中断のないアップグレードは、サービス ダウンタイムなしで SCE プラットフォームにあるソフトウェア コンポーネントをアップグレードする SCA BB の手法です。

- 中断のないアップグレードは、SCE 2000 および SCE 1000_2U プラットフォームで使用可能です。
- 中断のないアップグレードは、SCE 1000_1.5U プラットフォームで使用できません。

中断のないアップグレードがイネーブルの場合、SPQI ファイルのインストール中に分類、レポート、および管理は中断されません（「プロトコル パックの処理」（P.4-19）を参照）。Console または **servconf**（SCA BB サービス コンフィギュレーション ユーティリティ）を使用して SPQI ファイルをインストールすることができます。SPQI ファイルは、必要な（SLI）ファイルを含むパッケージです。

新規アプリケーションを SCE プラットフォームにロードすると、次のことが実行されます。

- 新規アプリケーションがすべての新規フローとバンドルを処理します。
- 古いアプリケーションが既存のフロー（および既存のフローのバンドルに属する新規フロー）の処理を継続します。
- 両方のアプリケーションで使用可能なメモリを共有します。

古いフローが終了するか停止するまで、中断のないアップグレードは進行中と見なされます。中断のないアップグレード処理をバインドするために、古いアプリケーションでまだ実行中のすべてのフローを明示的に停止させる基準を設定することができます。そのような基準には次の 2 種類があります。

- 処理が開始してから指定の期間が経過したとき
- 古いフローの数が指定したしきい値を下回ったとき

最初の基準のデフォルト値は 60（分）です。2 番めの基準のデフォルト値はゼロ（フロー）です。つまり、1 時間以内で置換操作が完了し、1 時間経過するまで古いフローを停止できないことが保証されています（ただし、古いフローが自然に終了した場合はこれよりも早くなります）。

これらの基準は CLI コマンドで設定可能です。

マニュアル コマンドを使用して古いフローを明示的に停止させることができます。

中断のないアップグレードの CLI コマンド

SCE プラットフォームのコマンドライン インターフェイス（CLI）を使用して、中断のないアップグレードの設定、モニタ、管理を行うことができます。SCE プラットフォーム CLI の詳細については、『*Cisco SCE8000 CLI Command Reference*』を参照してください。

ここに示すコマンドについては、次のセクションで説明します。

次の CLI コマンドを使用して、中断のないアップグレードを完了する基準を設定します。

```
replace completion time <minutes>
no replace completion time
default replace completion time
replace completion num-flows <num>
no replace completion num-flows
```

```
default replace completion num-flows
```

これらのコマンドは、ライン インターフェイス コンフィギュレーション コマンドです。これらのコマンドを実行するには、ライン インターフェイス コンフィギュレーション モード（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.4-30）を参照）を開始して、`SCE(config if)#` プロンプトを表示する必要があります。

次の 2 つの CLI コマンドは、EXEC モード コマンドです。

中断のないアップグレードの進捗をモニタするには、次の CLI コマンドを使用します。

```
show applications slot <num> replace
```

中断のないアップグレードを即座に完了させるには、次の CLI コマンドを使用します。

```
application slot <num> replace force completion
```

中断のないアップグレードの CLI コマンドに関する説明

表 4-1 で、前のセクションで示した中断のないアップグレードの CLI コマンドについて説明します。

表 4-1　中断のないアップグレードの CLI コマンド

コマンド	説明
replace completion time <*minutes*>	古いフローのすべてを停止して中断のないアップグレードを完了する時間基準を設定します。 値ゼロを指定すると、この基準がディセーブルになります。中断のないアップグレードは、フロー数の基準に合致した場合に限り完了します。
no replace completion time	中断のないアップグレードを完了する時間基準をゼロに設定します。
default replace completion time	置換操作を完了する時間基準をデフォルト値の 60 にリセットします。
replace completion num-flows <*num*>	中断のないアップグレード操作を完了するためのフロー数基準を設定します。 旧フローの数がこの基準の指定値を下回ると、残りのフローが停止されて、中断のないアップグレードが完了します。
no replace completion num-flows	中断のないアップグレードを完了するためのフロー数基準をゼロに設定します。
default replace completion num-flows	中断のないアップグレードを完了するためのフロー数基準をデフォルト値のゼロにリセットします。

表 4-1　中断のないアップグレードの CLI コマンド （続き）

コマンド	説明
show applications slot <*num*> **replace**	現在の中断のないアップグレード状態を示します。 • 現在の交換ステージ • 現在の完了基準 • 現在の完了ステータス（経過時間および各トラフィック プロセッサ上のフロー数） • アップグレードかダウングレードか • 予備メモリの値
application slot <*num*> **replace force completion**	現在の中断のないアップグレード プロセスを完了させます（旧フローをすべて停止させます）。

ライン インターフェイス コンフィギュレーション モードの開始方法

ライン インターフェイス コンフィギュレーション コマンドを実行するには、ライン インターフェイス コンフィギュレーション モードを開始し、`SCE(config if)#` プロンプトを表示する必要があります。

ステップ 1　SCE プラットフォームの CLI プロンプト（`SCE#` で **configure** と入力します。

ステップ 2　**Enter** キーを押します。

`SCE(config)#` プロンプトが表示されます。

ステップ 3　**interface LineCard 0** を入力します。

ステップ 4　**Enter** キーを押します。

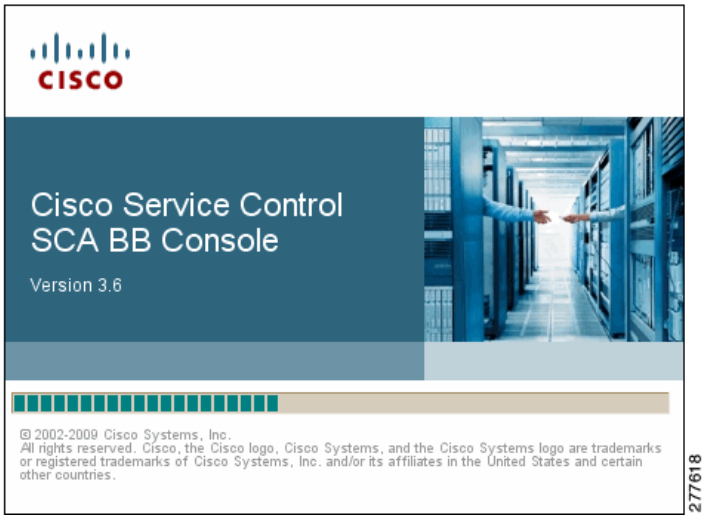
`SCE(config if)#` プロンプトが表示されます。

Console の起動方法

ステップ 1　[Start] > [All Programs] > [Cisco SCA] > [SCA BB Console 3.6.0] > [SCA BB Console 3.6.0] の順に選択します。

Cisco Service Control SCAS BB Console のスプラッシュ画面が表示されます（図 4-25 を参照）。

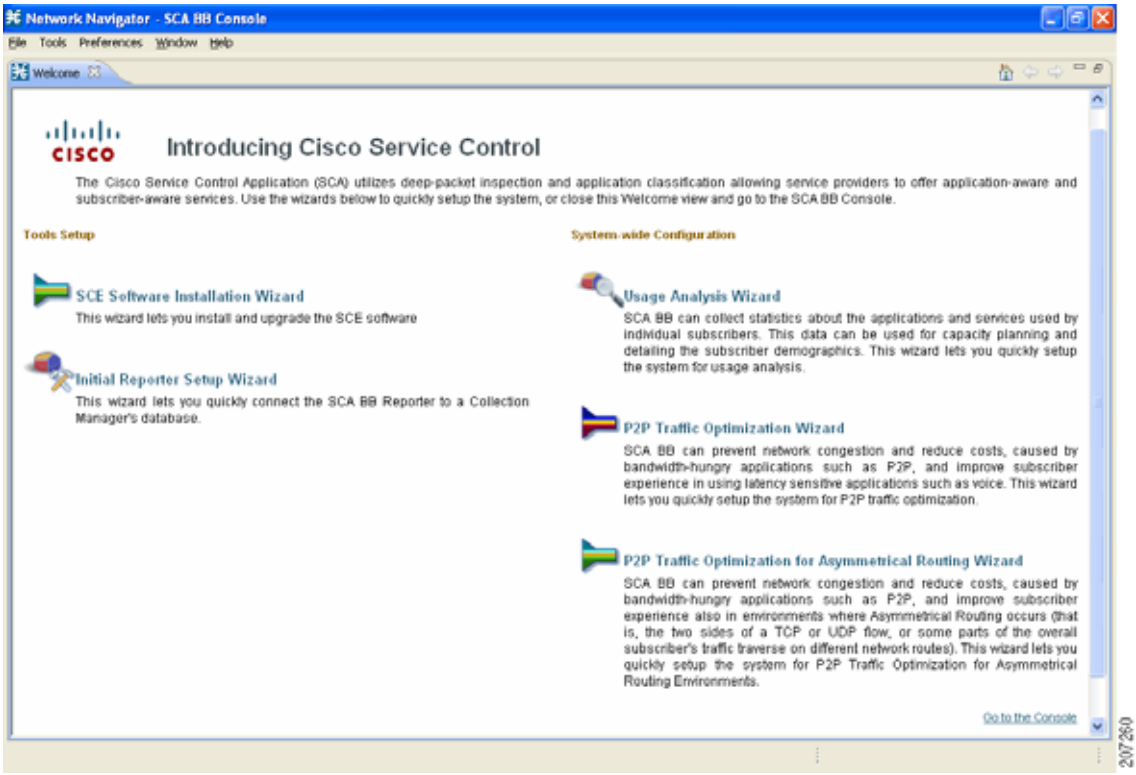
図 4-25　Cisco Service Control SCA BB Console



Console がロードされると、Console のメイン ウィンドウが表示されます。

Console を初めて起動する場合は、メイン ウィンドウに [Welcome] 画面が表示されます（図 4-26 を参照）。

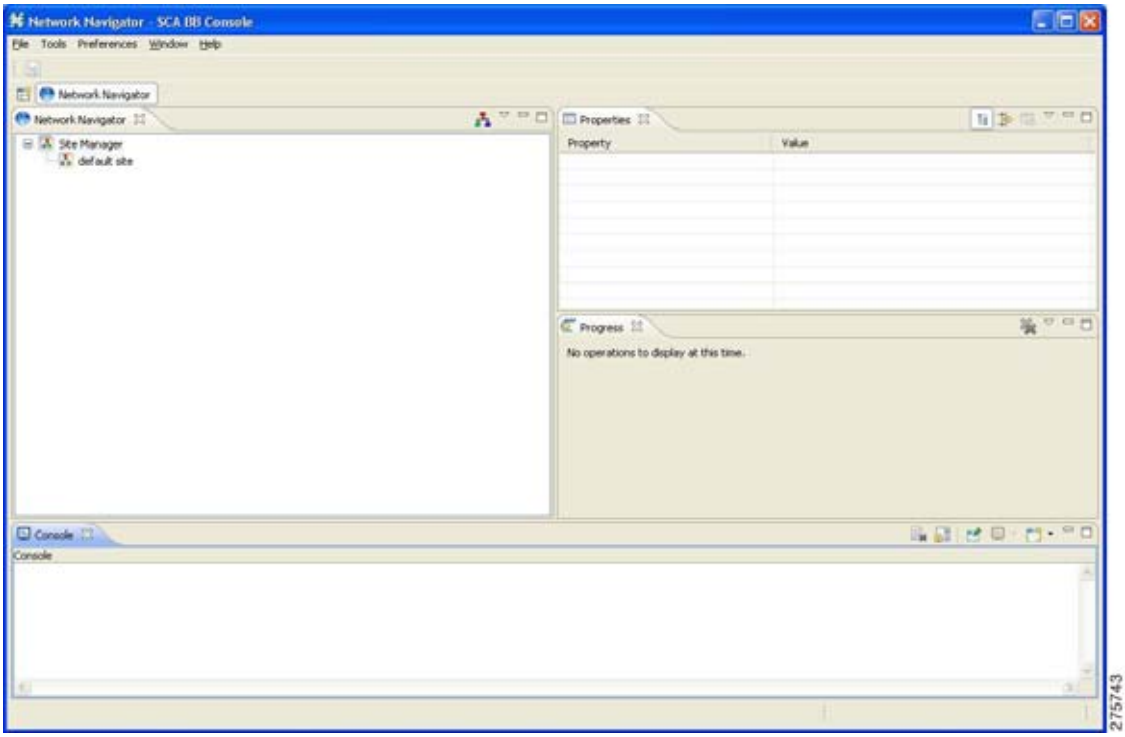
図 4-26　[Welcome] : [Introducing Cisco Service Control]



ステップ 2　[Welcome] 画面を閉じ、[Go to the console] をクリックします。

[Welcome] 画面が閉じます。Console で Network Navigator ツールが開きます（図 4-27 を参照）。

図 4-27　Network Navigator



（注）　Console は、終了時に開いていたツール、アクティブなツール、[Welcome] 画面が表示されたかどうかを記憶し、次回の起動時にこれを適用します。

Console の使用方法

Console は SCA BB のフロント エンドです。Console を使用して、SP がユーザに提供するサービスを設定します。

Console は次のツールで構成されています。

- Network Navigator ツール
- Service Configuration Editor ツール
- Signature Editor ツール
- Subscriber Manager GUI ツール
- Reporter ツール

Console GUI にはメニュー バーと標準ツールバーがあります（図 4-28 を参照）。ツールバーの下には、開いている Console ツールのボタンを示す別のバーがあります。ツールを起動すると、このバーにボタンが追加されます。開いているツールを切り替えるには、バー上の該当ボタンをクリックします。

図 4-28　Console GUI のメニュー バーとツールバー

（注）　Console ウィンドウのタイトルには、アクティブなツールとアクティブなサービス コンフィギュレーションが表示されます。

Console の [Welcome] 画面は、システムの最初の基本コンフィギュレーションを設定できるさまざまなコンフィギュレーション ウィザードにリンクしています。

- 「コンフィギュレーション ウィザード」（P.4-33）
- 「Network Navigator ツール」（P.4-68）
- 「Service Configuration Editor ツール」（P.4-69）
- 「Signature Editor ツール」（P.4-71）
- 「Subscriber Manager GUI ツール」（P.4-72）
- 「Reporter ツール」（P.4-73）
- 「オンライン ヘルプ」（P.4-74）

コンフィギュレーション ウィザード

[Welcome] 画面から、次のコンフィギュレーション ウィザードを使用できます（このうち 3 つのウィザードは Network Navigator ツールからも実行できます）。

- Usage Analysis ウィザード：デバイスの簡単なモデルを作成し、それらのデバイスに接続します。
- P2P Traffic Optimization ウィザード：
  - P2P Traffic Optimization ウィザード：デバイスの簡単なモデルの作成およびデバイスへの接続を行い、P2P トラフィックを利用可能な合計帯域幅の所定の割合に制限します。
  - P2P Traffic Optimization at a Peering Point ウィザード:デバイスの簡単なモデルの作成およびデバイスへの接続を行い、P2P トラフィックを利用可能な合計帯域幅の所定の割合に制限し、ユーザが非対称ルーティング分類モードを使用できるようにします。
- Reporter DB Configuration ウィザード：SCA BB Reporter ツールをデータベースに接続します。

非対称ルーティング

トラフィック処理はルーティング環境によって異なります。シスコの Service Control ソリューションは、2 つの標準的なルーティング方法（対称および非対称ルーティング）で動作可能です。非対称ルーティングでは、多くのフローは、SCE プラットフォームを通じて一方向（インバウンドまたはアウトバウンド）だけがルーティングされます。

アノニマス サブスクライバ モード

アノニマス サブスクライバ モードでは、IP アドレスとして定義されたエンティティがサブスクライバとして処理されます。

Usage Analysis ウィザードの使用方法

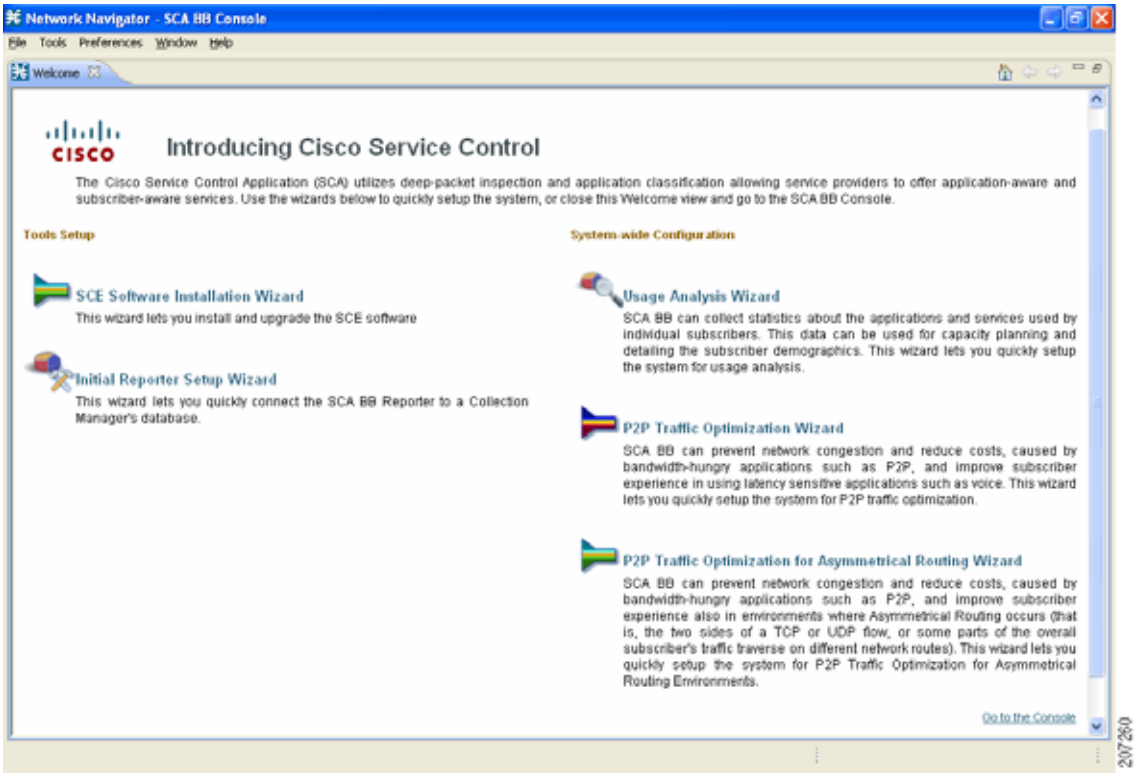
Usage Analysis ウィザードでは、デバイスの簡単なモデルを作成し、それらのデバイスに接続できます。

（注）　デバイスが存在しない場合は、このウィザードで定義されたデバイスが [Site Manager] ツリーのデフォルト サイトに追加されます。

ステップ 1　Console のメイン メニューで、[Help] > [Welcome] の順に選択します。

[Welcome] 画面が表示されます（図 4-29 を参照）。

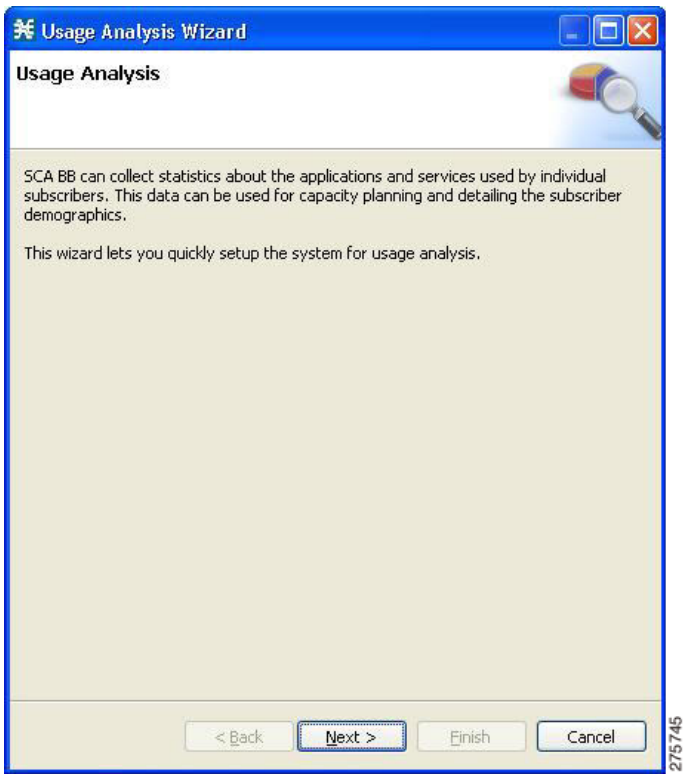
図 4-29　[Welcome] : [Introducing Cisco Service Control]



ステップ 2　[Usage Analysis Wizard] をクリックします。

Usage Analysis ウィザードの [Welcome] ページが表示されます（図 4-30 を参照）。

図 4-30　[Usage Analysis]



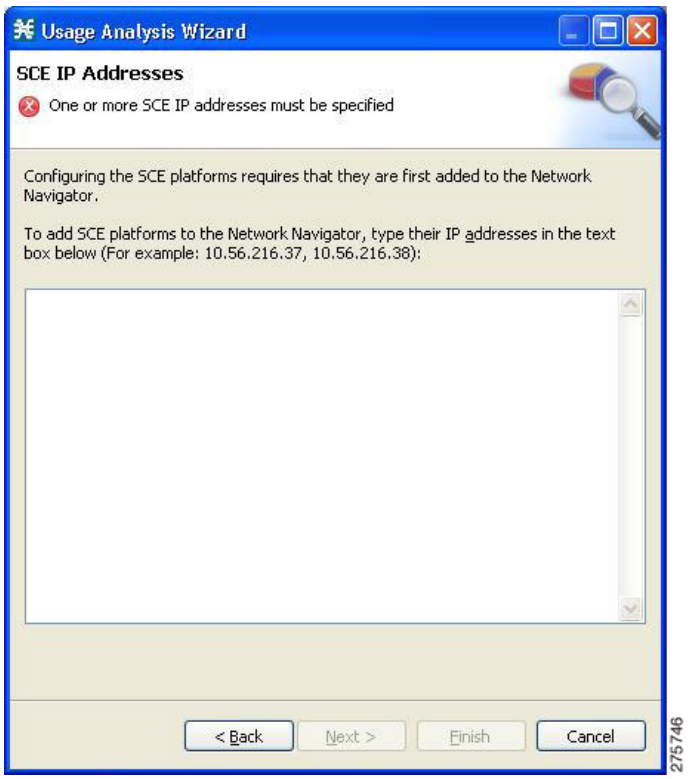
（注）　Usage Analysis ウィザードは Network Navigator ツールからも実行できます。

1. [Site Manager] ツリーでデバイスを 1 つ以上選択します。
2. 選択したデバイスのいずれか 1 つを右クリックします。
3. 表示されるポップアップ メニューで、[Configuration Wizards] > [Usage Analysis Configuration] の順に選択します。
4. このウィザードで設定できるのは、1 つの CM と 1 つの Reporter データベースだけです。複数の CM または Reporter データベースを選択した場合、1 つの CM と 1 つの Reporter データベースだけが選択され、警告メッセージが表示されます。[OK] をクリックして続行します。

ステップ 3　[Next] をクリックします。

Usage Analysis ウィザードの [SCE IP Addresses] ページが開きます（図 4-31 を参照）。

図 4-31　[SCE IP Addresses]



ステップ 4　編集ボックスで、モデルに追加する SCE デバイスの IP アドレスを入力します。

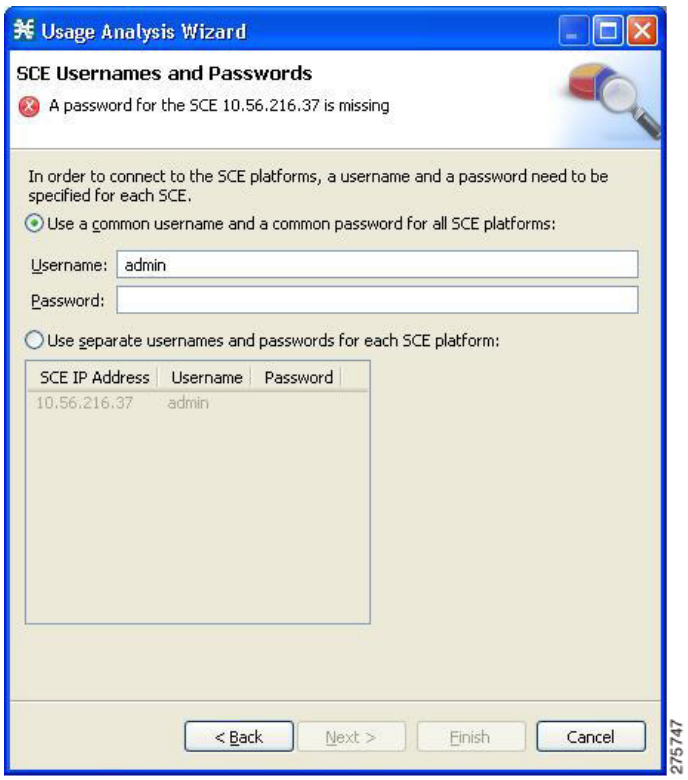
Network Navigator から操作を開始した場合は、選択した SCE デバイスの IP アドレスが編集ボックスに表示されます。アドレスは追加できます。

（注）　このウィザードでは、一度に最大 20 の SCE デバイスを操作できます。

ステップ 5　[Next] をクリックします。

Usage Analysis ウィザードの [SCE Usernames and Passwords] ページが開きます（図 4-32 を参照）。

図 4-32　[SCE Usernames and Passwords]



ステップ 6　SCE デバイスのユーザ名とパスワードを入力します。

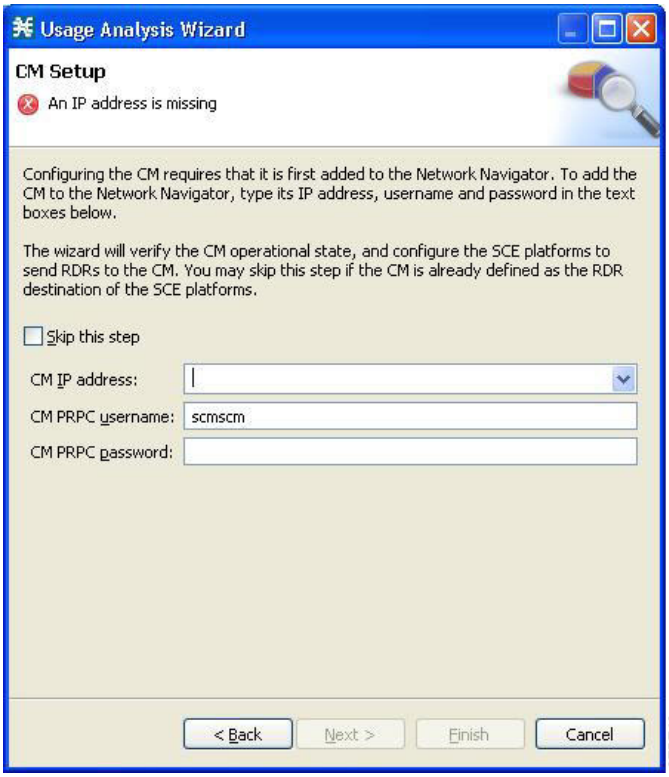
次のうちいずれかを実行します。

- 追加するすべての SCE デバイスに同じユーザ名とパスワードを使用するには、[Username] フィールドにユーザ名、[Password] フィールドにパスワードを入力します。
- 各 SCE デバイスに異なるユーザ名とパスワードのペアを設定するには、[Use separate usernames and passwords for each SCE platform] オプション ボタンを選択し、各 SCE デバイスごとに、テーブルの該当するセルにユーザ名とパスワードを入力します。

ステップ 7　[Next] をクリックします。

Usage Analysis ウィザードの [CM Setup] ページが開きます（図 4-33 を参照）。

図 4-33　[CM Setup]



ステップ 8　このコンフィギュレーションで使用する SCSM Collection Manager（CM）を定義します。

次のうちいずれかを実行します。

- 該当するフィールドに、CM デバイスの IP アドレス、ユーザ名、パスワードを入力します。

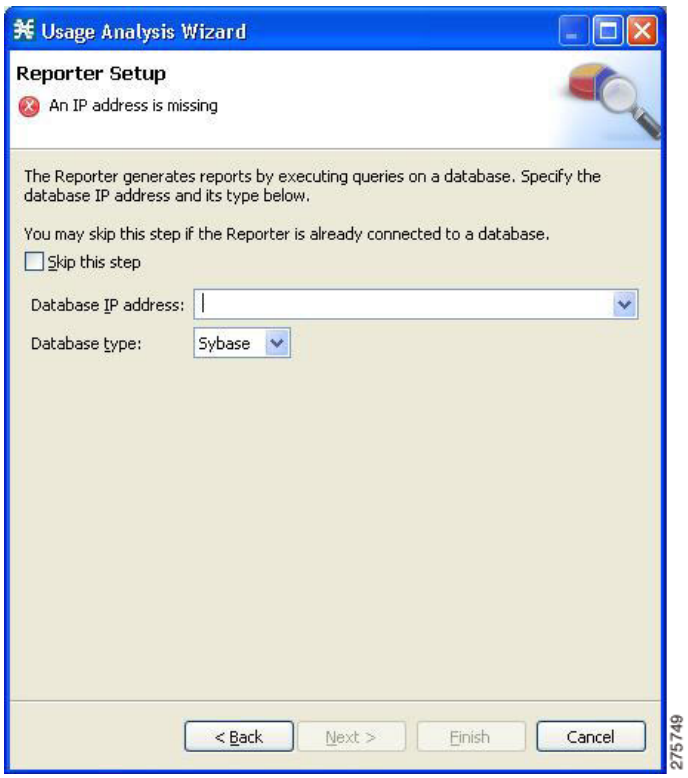
  Network Navigator から操作を開始した場合は、この情報が取得されて表示されます。これらのパラメータは変更できます。

- [Skip this step] チェックボックスをオンにします。

ステップ 9　[Next] をクリックします。

Usage Analysis ウィザードの [Reporter Setup] ページが開きます（図 4-34 を参照）。

図 4-34　[Reporter Setup]



ステップ 10　Reporter ツールを接続するデータベースを定義します。

次のうちいずれかを実行します。

- データベースの IP アドレスを入力し、データベース タイプを選択します。

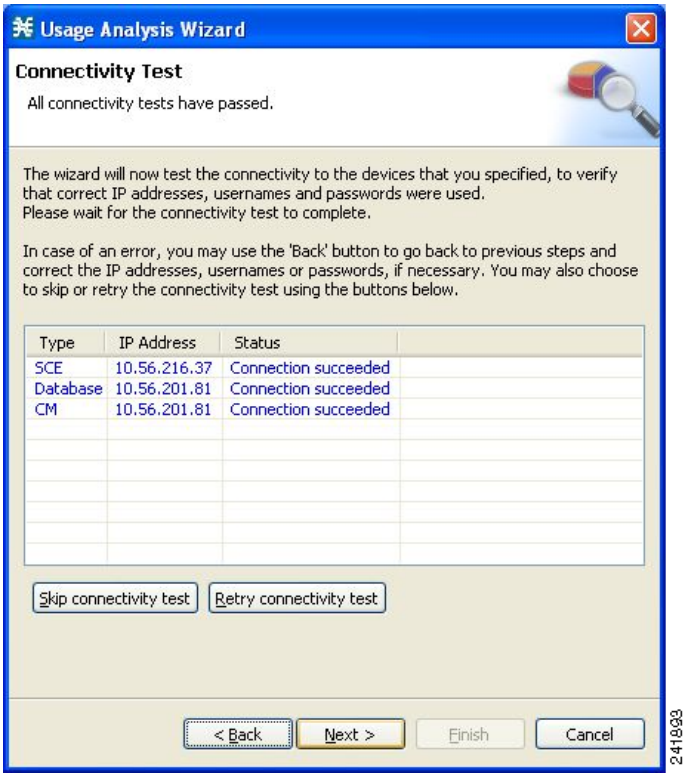
  Network Navigator から操作を開始した場合は、この情報が取得されて表示されます。これらのパラメータは変更できます。

- [Skip this step] チェックボックスをオンにします。

ステップ 11　[Next] をクリックします。

Usage Analysis ウィザードの [Connectivity Test] ページが開きます（図 4-35 を参照）。

図 4-35　[Connectivity Test]



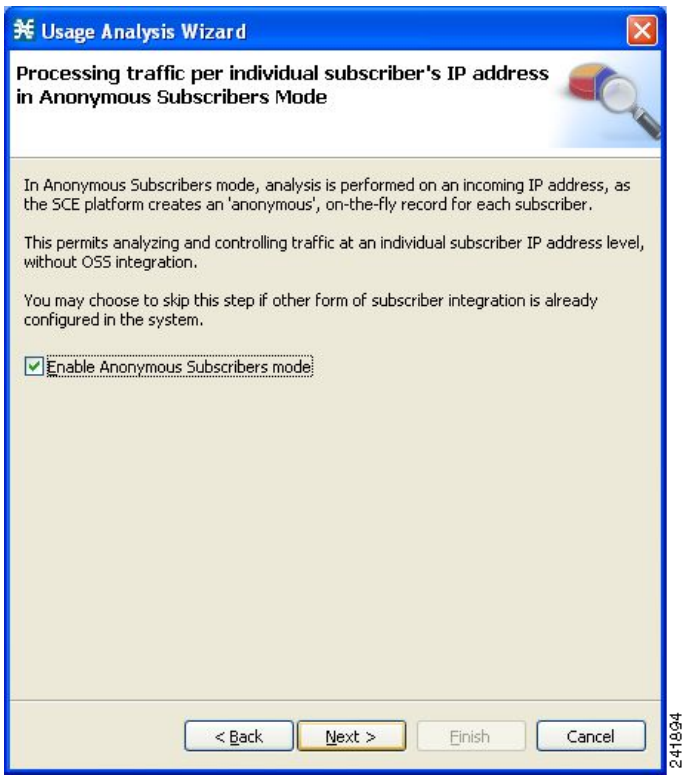
ウィザードは、定義済みデバイスへの接続が可能かどうかを確認するためのテストを実行します。

（注）　1 つ以上のデバイスに接続できない場合、または接続に何らかの問題がある場合（デバイスのバージョンが無効など）は、そのデバイスの横にエラーが表示されます。[Skip connectivity test] をクリックすると、このテストを省略できます。ウィザードの最後で [Finish] をクリックすると接続が検証されます。

ステップ 12　[Next] をクリックします。

Usage Analysis ウィザードの [Anonymous Subscribers] ページが開きます（図 4-36 を参照）。

図 4-36　[Anonymous Subscribers]

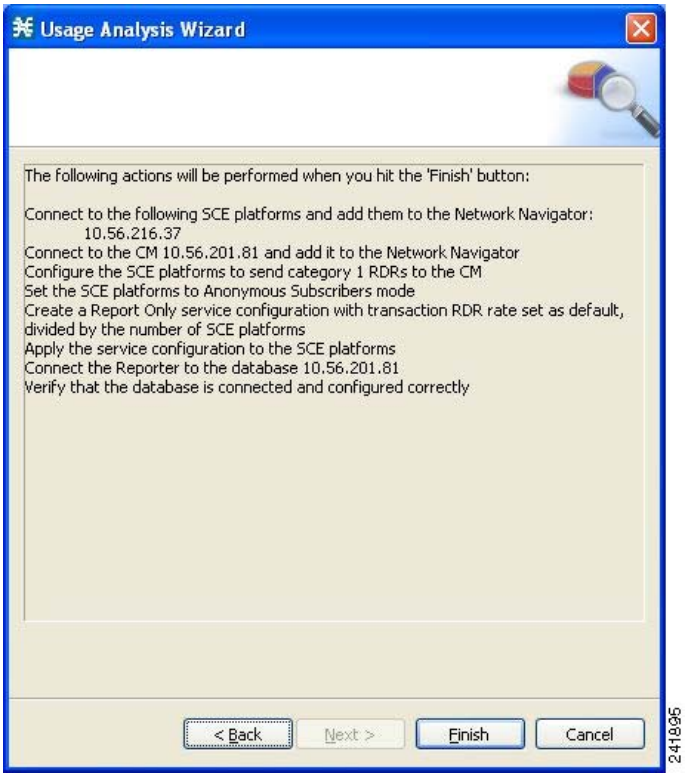


ステップ 13　アノニマス サブスクライバ モードをディセーブルにするには、[Enable Anonymous Subscribers mode] チェックボックスをオフにします。

ステップ 14　[Next] をクリックします。

Usage Analysis ウィザードの [Confirmation] ページが開きます（図 4-37 を参照）。

図 4-37　[Confirmation]

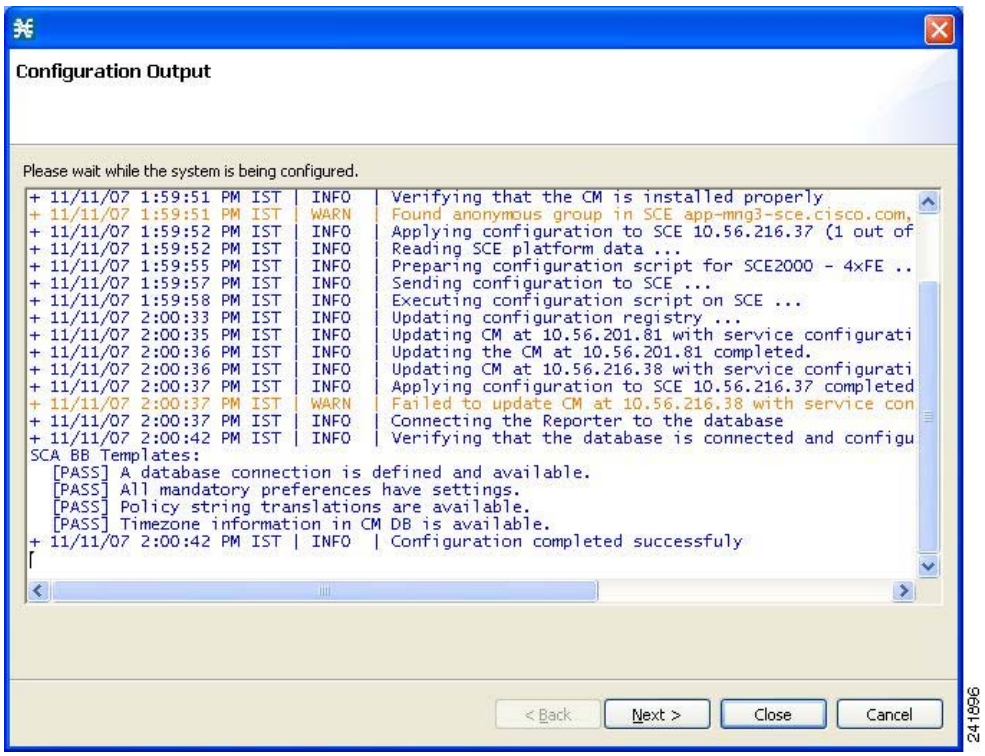


このページには、ウィザードでこれから実行される処理がリストされています。

ステップ 15　[Finish] をクリックします。

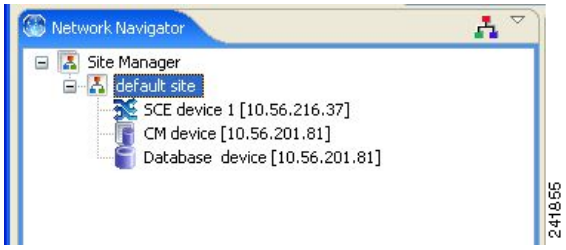
Usage Analysis ウィザードの [Configuration Output] ページが開きます（図 4-38 を参照）。

図 4-38　[Configuration Output]



Network Navigator の [Site Manager] ツリーのデフォルト サイトに新規デバイスが追加されます（図 4-39 を参照）。

図 4-39　[Site Manager] ツリー



ウィザードは、定義されたすべてのデバイスに対して接続を試行します。この処理は次の場合に失敗します。

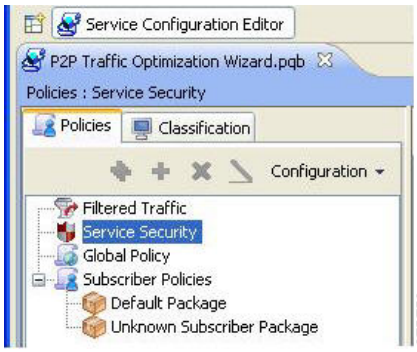
- ステップ 4 でリストされた SCE デバイスのいずれかにウィザードが接続できない。
- ステップ 8 で CM が定義されたが、ウィザードがこれに接続できない。
- ステップ 10 でデータベースが定義されたが、ウィザードがこれに接続できない。

ステップ 8 で CM が定義された場合、SCE デバイスはカテゴリ 1 の Raw Data Record（RDR; 未加工データ レコード）宛先だけが CM となるように設定されます。

（注）　RDR カテゴリは、異なるタイプの RDR を異なるコレクタに送信できるメカニズムです。RDR カテゴリの詳細については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」または『*Cisco SCE8000 GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」を参照してください。

Usage Analysis という名前の新しいサービス コンフィギュレーションが作成され、Service Configuration Editor で開きます（図 4-40 を参照）。

図 4-40　Service Configuration Editor



サービス コンフィギュレーションには、次のような特性があります。

- レポート専用モード。
- 最大トランザクション RDR レートは、デフォルト値（250）を SCE デバイス数で除算した値に設定されます（トランザクション RDR を設定するには、「Transaction RDR の管理方法」（P.8-5）を参照してください。トランザクション RDR のコンテンツと構造は、『*Cisco Service Control Application for Broadband Reference Guide*』の「Raw Data Records: Formats and Field Contents」にある「Transaction RDR」にリストされています）。

サービス コンフィギュレーションが SCE デバイスに適用されます。

ステップ 10 でデータベースを定義した場合は、次のようになります。

- 選択したデータベースに SCA BB Reporter ツールが接続されます。
- ステップ 4 で最初に入力した SCE プラットフォームが、サービス コンフィギュレーション データのソースとして選択されます。
- [Next] ボタンがイネーブルになります。

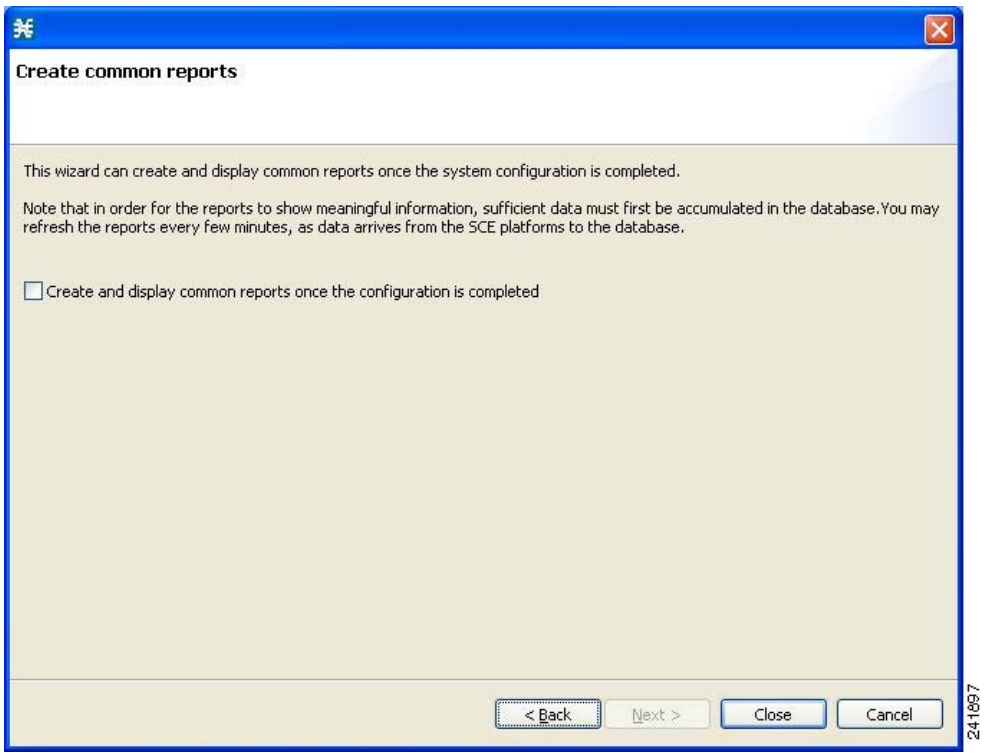
ステップ 16　ステップ 10 でデータベースを定義しなかった場合は、[Close] をクリックします。

Usage Analysis ウィザードが閉じます。

ステップ 17　[Next] をクリックします。

Usage Analysis ウィザードの [Create common reports] ページが開きます（図 4-41 を参照）。

図 4-41　[Create Common Reports]



ステップ 18　レポートを作成するには、[Create and display common reports] チェックボックスをオンにします。

（注）　次の 4 つの定義済みレポート タイプに対し、レポート インスタンスが作成されます。

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

ステップ 19　[Close] をクリックします。

ウィザードが閉じます。

Console で Reporter ツールが開きます。

4 つの各レポート タイプのレポート インスタンスが Reporter ツールの [Report View] で開きます。

P2P Traffic Optimization ウィザードの使用方法

P2P トラフィックを最適化するために、次の 2 つのウィザードがあります。

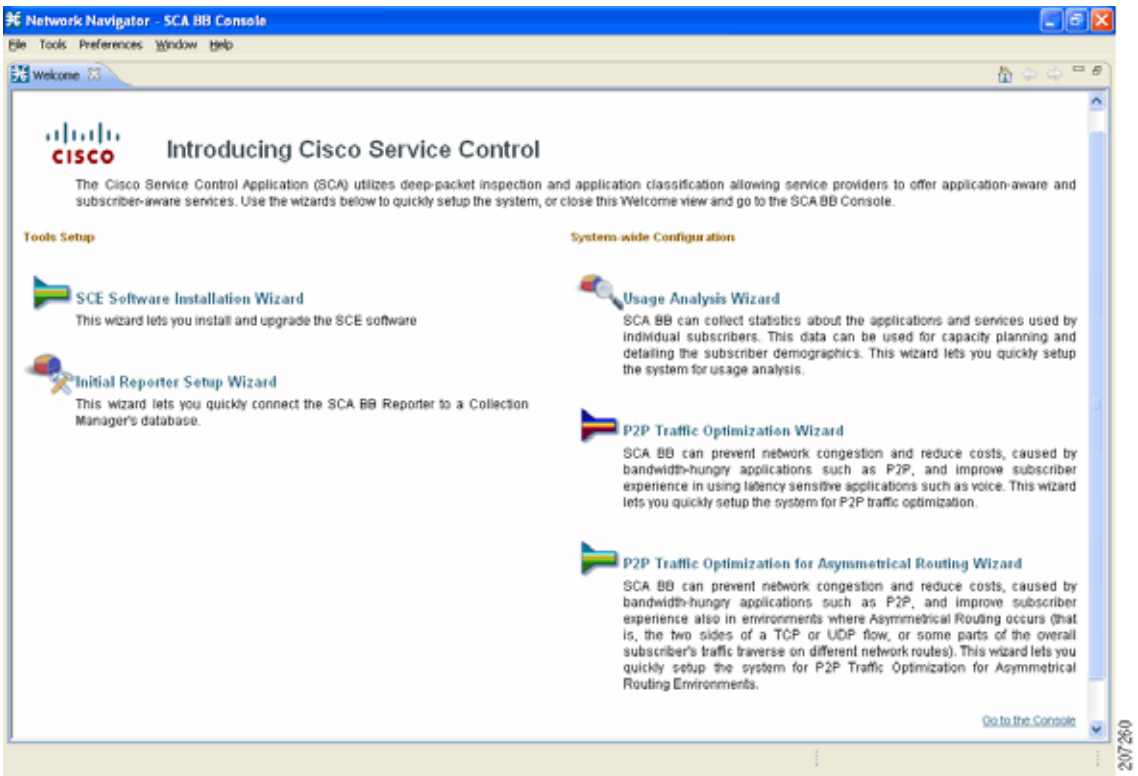
- P2P Traffic Optimization ウィザードでは、デバイスの簡単なモデルの作成とデバイスへの接続が可能です。また、P2P トラフィックを利用可能な合計帯域幅の所定の割合に制限することもできます。
- P2P Traffic Optimization at a Peering Point ウィザードでは、デバイスの簡単なモデルの作成、デバイスへの接続が可能です。また、P2P トラフィックを利用可能な合計帯域幅の所定の割合に制限し、非対称ルーティング分類モードをイネーブにすることができます。

（注）　デバイスが存在しない場合は、このウィザードで定義されたデバイスが [Site Manager] ツリーのデフォルト サイトに追加されます。

ステップ 1　Console のメイン メニューで、[Help] > [Welcome] の順に選択します。

[Welcome] 画面が表示されます（図 4-42 を参照）。

図 4-42　[Welcome] : [Introducing Cisco Service Control]



ステップ 2　[P2P Traffic Optimization Wizard] または [P2P Traffic Optimization for Asymmetrical Routing Wizard] をクリックします。

選択したウィザードの [Welcome] ページが表示されます（図 4-43 または図 4-44 を参照）。

図 4-43　[P2P Traffic Optimization]

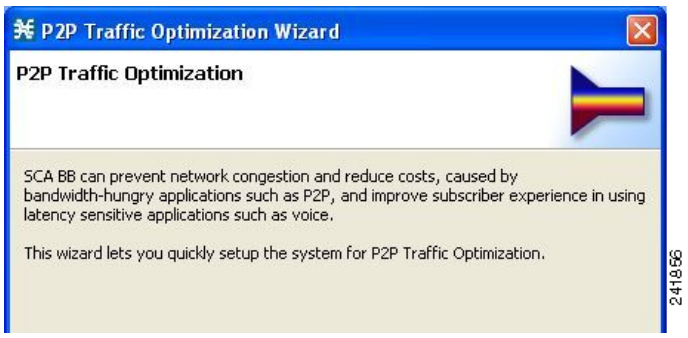
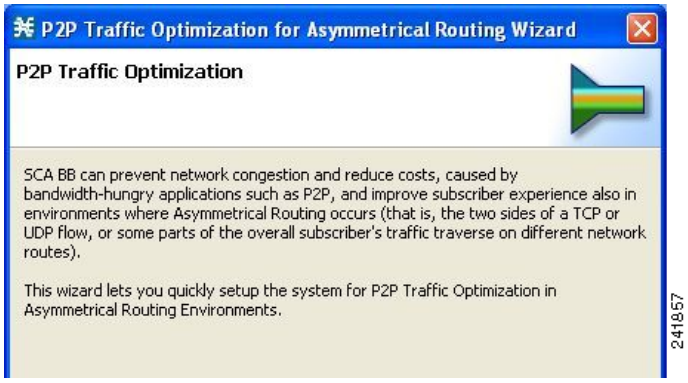


図 4-44　[P2P Traffic Optimization for Asymmetrical Routing]



（注） P2P Traffic Optimization ウィザードは Network Navigator ツールからも実行できます。

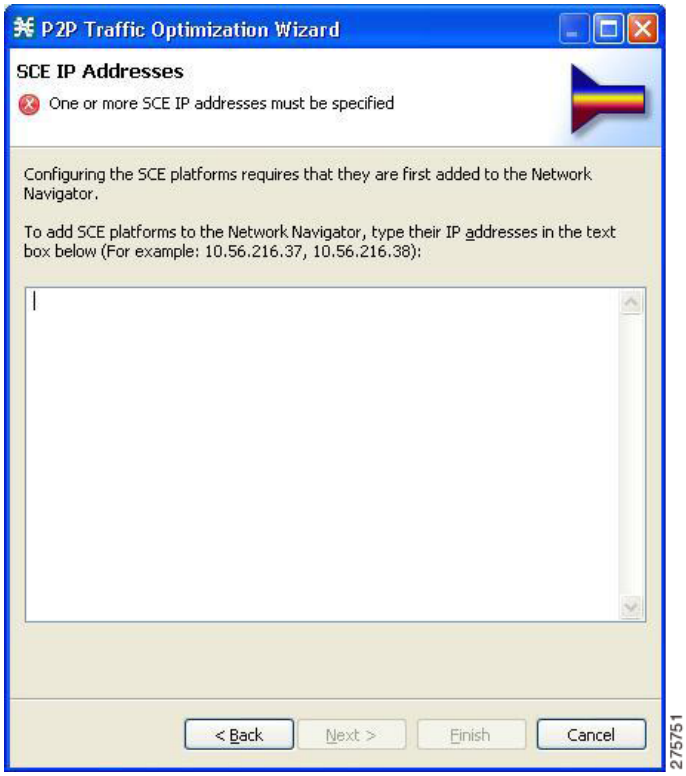
1. [Site Manager] ツリーでデバイスを 1 つ以上選択します。
2. 選択したデバイスのいずれか 1 つを右クリックします。
3. 表示されるポップアップ メニューで、[Configuration Wizards] > [P2P Traffic Optimization Wizard] または [Configuration Wizards] > [P2P Traffic Optimization for Asymmetrical Routing Wizard] の順に選択します。

（注） このウィザードで設定できるのは、1 つの CM と 1 つの Reporter データベースだけです。複数の CM または Reporter データベースを選択した場合、1 つの CM と 1 つの Reporter データベースだけが選択され、警告メッセージが表示されます。[OK] をクリックして続行します。

ステップ 3　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [SCE IP Addresses] ページが開きます（図 4-45 を参照）。

図 4-45　[SCE IP Addresses]



ステップ 4　編集ボックスで、モデルに追加する SCE デバイスの IP アドレスを入力します。

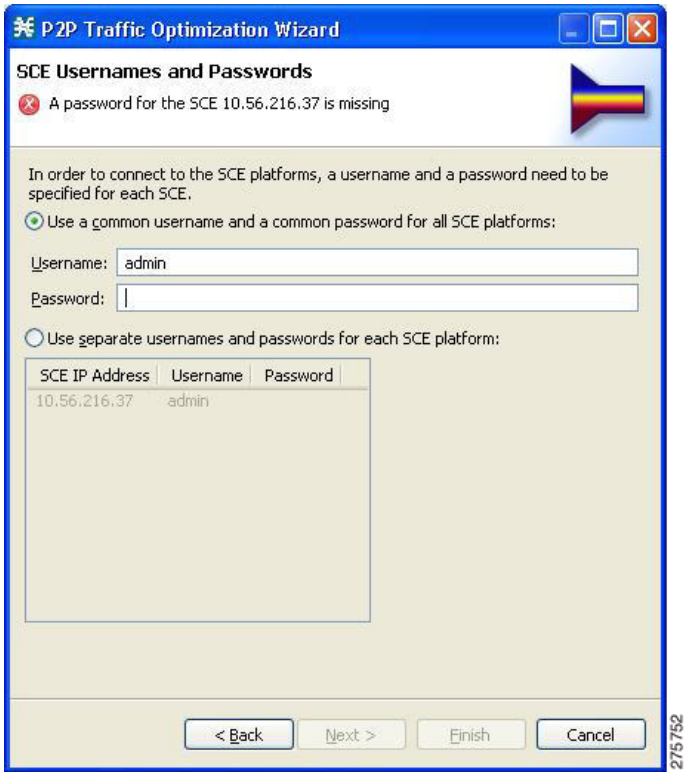
Network Navigator から操作を開始した場合は、選択した SCE デバイスの IP アドレスが編集ボックスに表示されます。アドレスは追加できます。

（注）　このウィザードでは、一度に最大 20 の SCE デバイスを操作できます。

ステップ 5　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [SCE Usernames and Passwords] ページが開きます（図 4-46 を参照）。

図 4-46　[SCE Usernames and Passwords]



ステップ 6　SCE デバイスのユーザ名とパスワードを入力します。

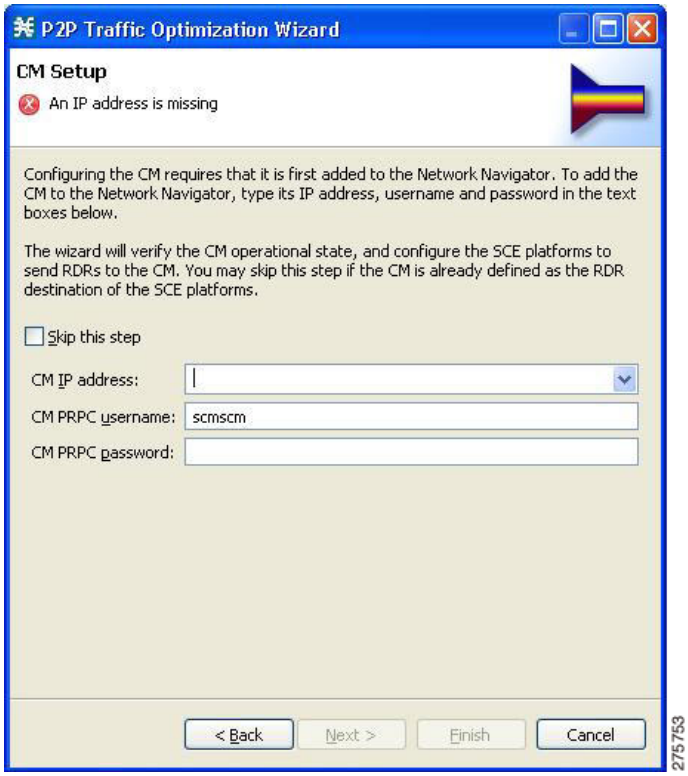
次のうちいずれかを実行します。

- 追加するすべての SCE デバイスに同じユーザ名とパスワードを使用するには、[Username] フィールドにユーザ名、[Password] フィールドにパスワードを入力します。
- 各 SCE デバイスに異なるユーザ名とパスワードのペアを設定するには、[Use separate usernames and passwords for each SCE platform] オプション ボタンを選択し、各 SCE デバイスごとに、SCE デバイス テーブルの該当するセルにユーザ名とパスワードを入力します。

ステップ 7　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [CM Setup] ページが開きます（図 4-47 を参照）。

図 4-47　[CM Setup]



ステップ 8　このコンフィギュレーションで使用する SCSM Collection Manager（CM）を定義します。

次のうちいずれかを実行します。

- 該当するフィールドに、CM デバイスの IP アドレス、ユーザ名、パスワードを入力します。

  Network Navigator から操作を開始した場合は、この情報が取得されて表示されます。これらのパラメータは変更できます。

- [Skip this step] チェックボックスをオンにします。

ステップ 9　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Reporter Setup] ページが開きます（図 4-48 を参照）。

図 4-48　[Reporter Setup]

ステップ 10　Reporter ツールを接続するデータベースを定義します。

次のうちいずれかを実行します。

- データベースの IP アドレスを入力し、データベース タイプを選択します。

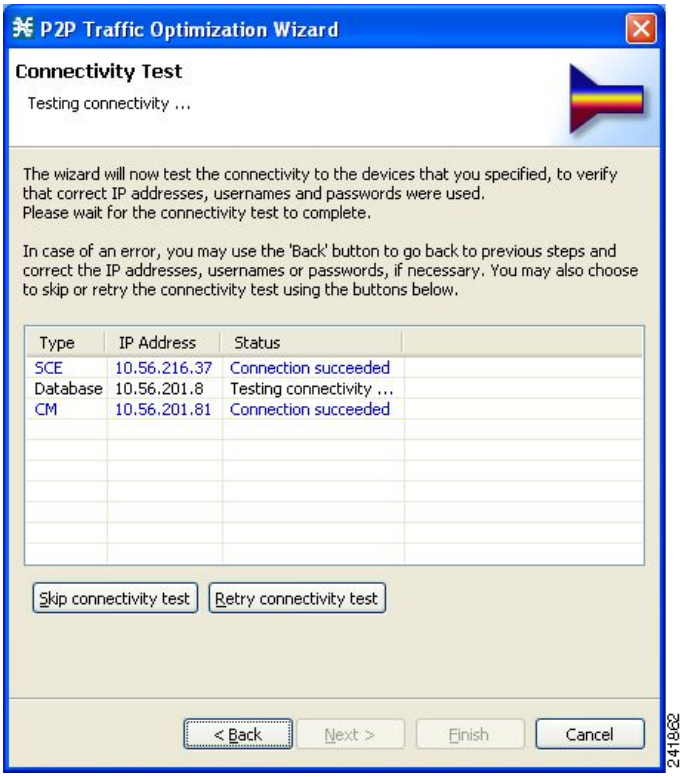
  Network Navigator から操作を開始した場合は、この情報が取得されて表示されます。これらのパラメータは変更できます。

- [Skip this step] チェックボックスをオンにします。

ステップ 11　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Connectivity Test] ページが開きます（図 4-49 を参照）。

図 4-49　[Connectivity Test]



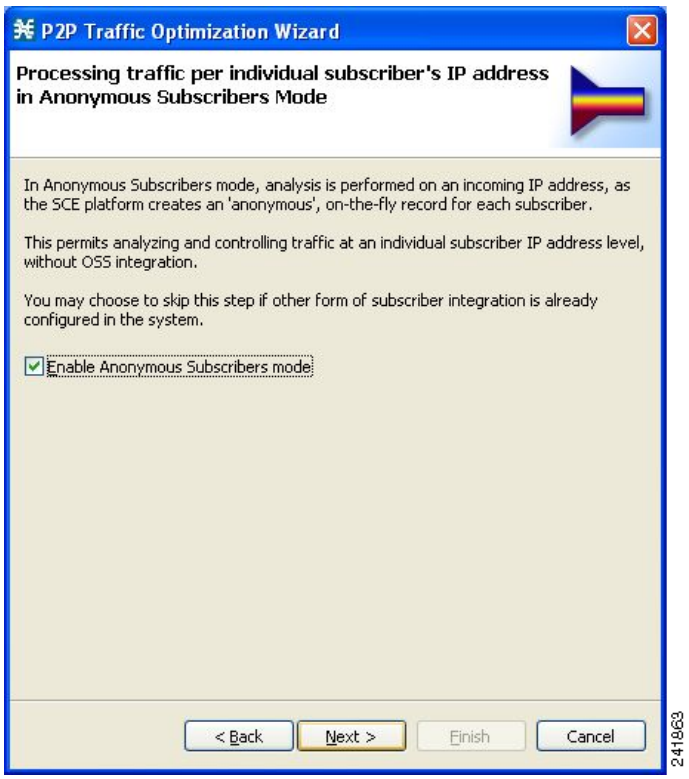
ウィザードは、定義済みデバイスへの接続が可能かどうかを確認するためのテストを実行します。

（注）　1 つ以上のデバイスに接続できない場合、または接続に何らかの問題がある場合（デバイスのバージョンが無効など）は、そのデバイスの横にエラーが表示されます。[Skip connectivity test] をクリックすると、このテストを省略できます。ウィザードの最後で [Finish] をクリックすると接続が検証されます。

ステップ 12　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Anonymous Subscribers] ページが開きます（図 4-50 を参照）。

図 4-50　[Anonymous Subscribers]

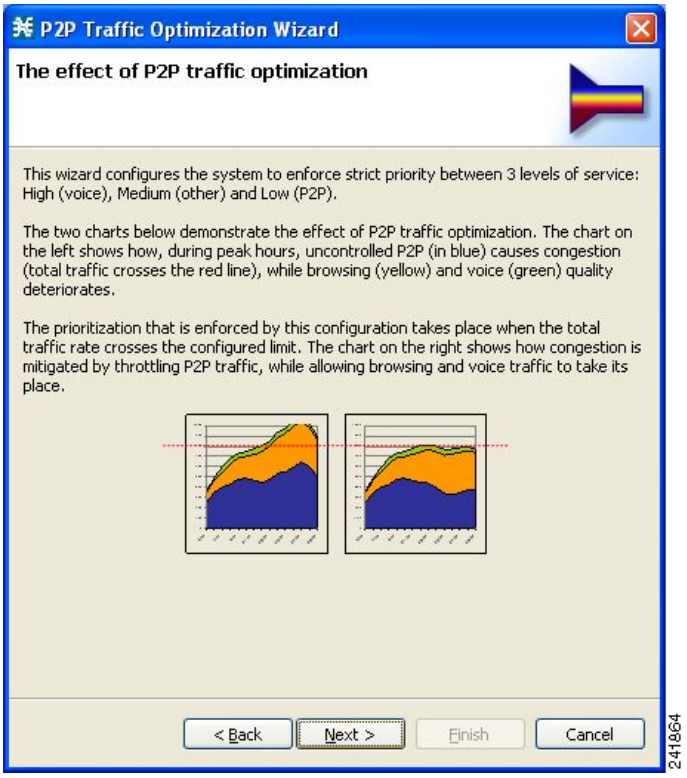


ステップ 13　アノニマス サブスクライバ モードをディセーブルにするには、[Enable Anonymous Subscribers mode] チェックボックスをオフにします。

ステップ 14　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [The effect of P2P traffic optimization] ページが開きます（図 4-51 を参照）。

図 4-51　[Effect of P2P Traffic Optimization]

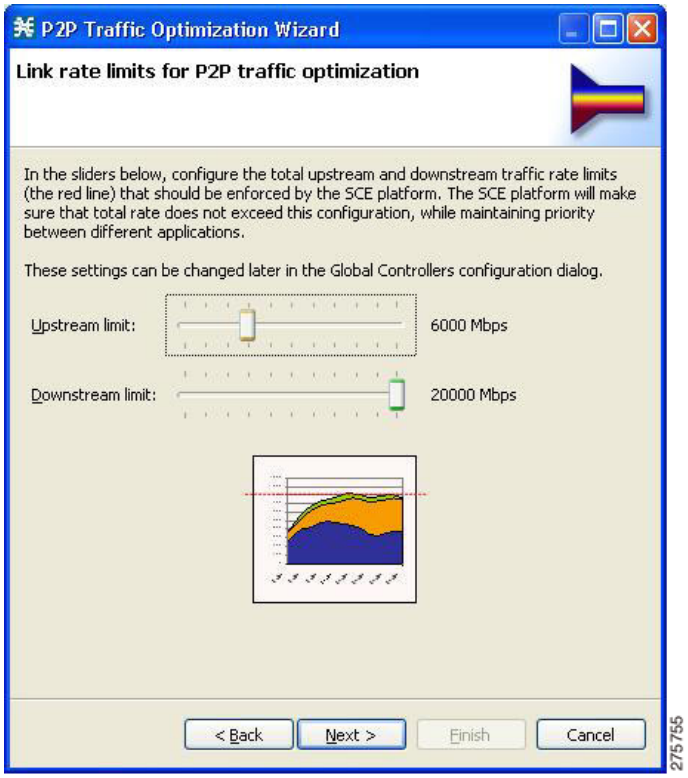


このページには、P2P トラフィックを最適化（制限）する理由が説明されています。

ステップ 15　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Link rate limits for P2P traffic optimization] ページが開きます（図 4-52 を参照）。

図 4-52　[Link Rate Limits]



ステップ 16　スライダを使用して、アップストリームおよびダウンストリームのリンク レートの制限を設定します。

各スライダの目盛りは、両リンクの集約帯域幅の割合を示しています。

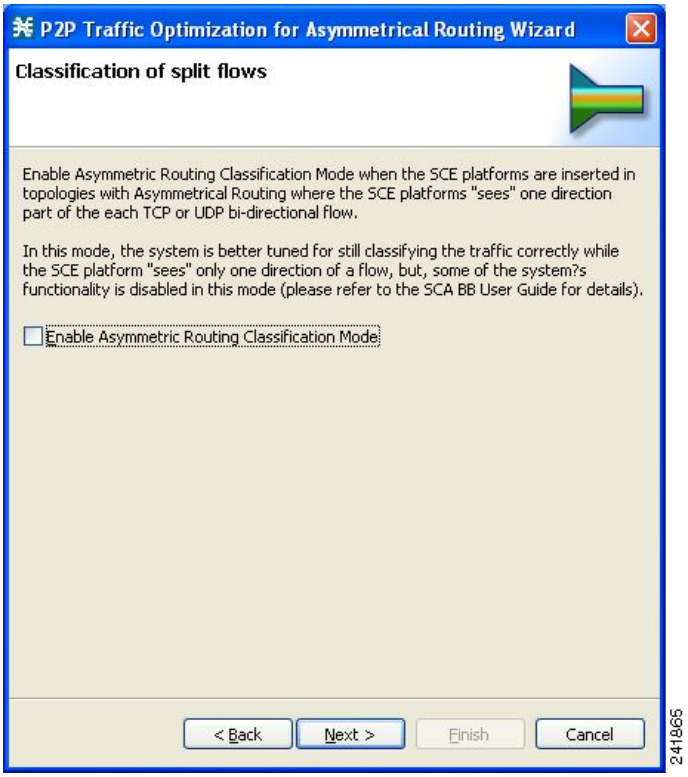
ステップ 17　P2P Traffic Optimization ウィザードを実行している場合は、ステップ 20 に進みます。

P2P Traffic Optimization for Asymmetrical Routing ウィザードを実行している場合は、次のステップに進みます。

ステップ 18　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Classification of split flows] ページが開きます（図 4-53 を参照）。

図 4-53　[Classification of Split Flows]

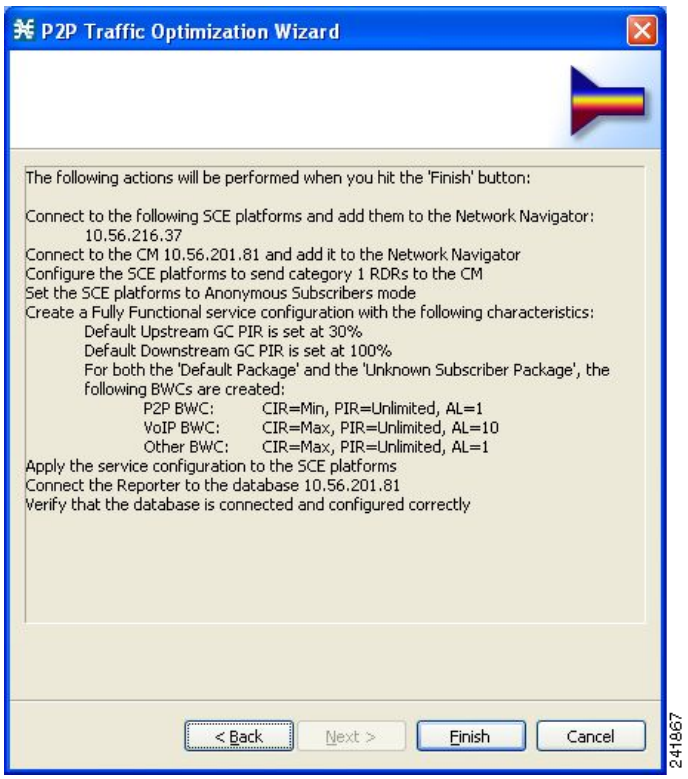


ステップ 19　非対称ルーティング分類モードをイネーブルにするには、[Enable Asymmetric Routing Classification Mode] チェックボックスをオンにします。

ステップ 20　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Confirmation] ページが開きます（図 4-54 を参照）。

図 4-54　[Confirmation]



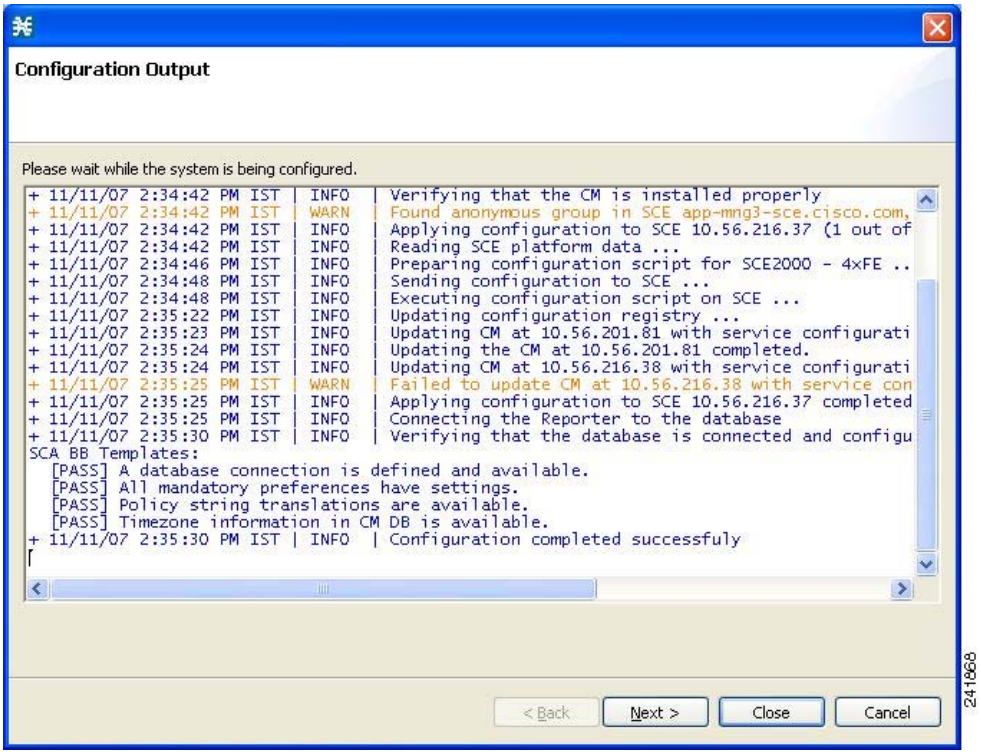
このページには、ウィザードでこれから実行される処理がリストされています。

帯域幅コントローラのパラメータについては、「サブスクライバ BWC パラメータ」（P.9-29）を参照してください。

ステップ 21　[Finish] をクリックします。

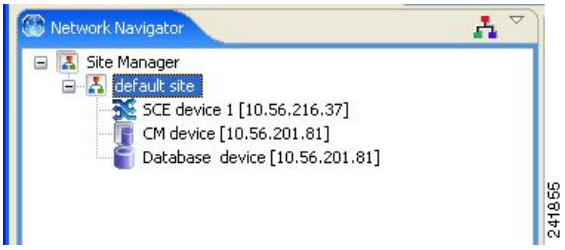
P2P Traffic Optimization ウィザードの [Configuration Output] ページが開きます（図 4-55 を参照）。

図 4-55　[Configuration Output]



Network Navigator の [Site Manager] ツリーのデフォルト サイトに新規デバイスが追加されます（図 4-56 を参照）。

図 4-56　Network Navigator



ウィザードは、定義されたすべてのデバイスに対して接続を試行します。この処理は次の場合に失敗します。

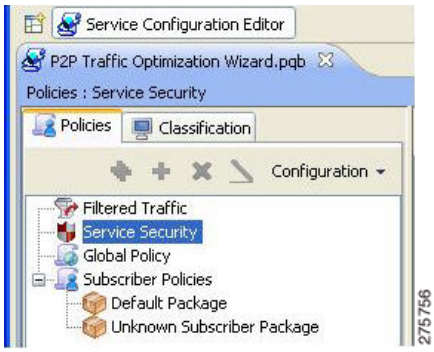
- ステップ 4 でリストされた SCE デバイスのいずれかにウィザードが接続できない。
- ステップ 8 で CM が定義されたが、ウィザードがこれに接続できない。
- ステップ 10 でデータベースが定義されたが、ウィザードがこれに接続できない。

ステップ 8 で CM が定義された場合、SCE デバイスはカテゴリ 1 の Raw Data Record（RDR; 未加工データ レコード）宛先だけが CM となるように設定されます。

（注）　RDR カテゴリは、異なるタイプの RDR を異なるコレクタに送信できるメカニズムです。RDR カテゴリの詳細については、『*Cisco Service Control Application for Broadband Reference Guide*』の「Raw Data Records: Formats and Field Contents」を参照してください。

P2P Traffic Optimization（または P2P Traffic Optimization for Asymmetrical Routing）という名前の新しいサービス コンフィギュレーションが作成され、Service Configuration Editor で開きます（図 4-57 を参照）。

図 4-57　Service Configuration Editor



サービス コンフィギュレーションには、次のような特性があります。

- フル機能モード。
- アップストリームおよびダウンストリームのデフォルト AGC は、ステップ 16 で定義したリンク制限値を使用して設定されます。
- デフォルト パッケージと Unknown Subscriber Traffic パッケージには、次のアップストリームおよびダウンストリーム BWC が作成されます（表 4-2）。

表 4-2　デフォルト パッケージと Unknown Subscriber Traffic パッケージの BWC

パッケージ	CIR	PIR	AL
P2P	0	<グローバル コントローラの設定値>	1
VOIP	<グローバル コントローラの設定値>	<グローバル コントローラの設定値>	10
P2P	<グローバル コントローラの設定値>	<グローバル コントローラの設定値>	1

サービス コンフィギュレーションが SCE デバイスに適用されます。

ステップ 10 でデータベースを定義した場合は、次のようになります。

1. 選択したデータベースに SCA BB Reporter ツールが接続されます。
2. ステップ 4 で最初に入力した SCE プラットフォームが、サービス コンフィギュレーション データのソースとして選択されます。
3. [Next] ボタンがイネーブルになります。

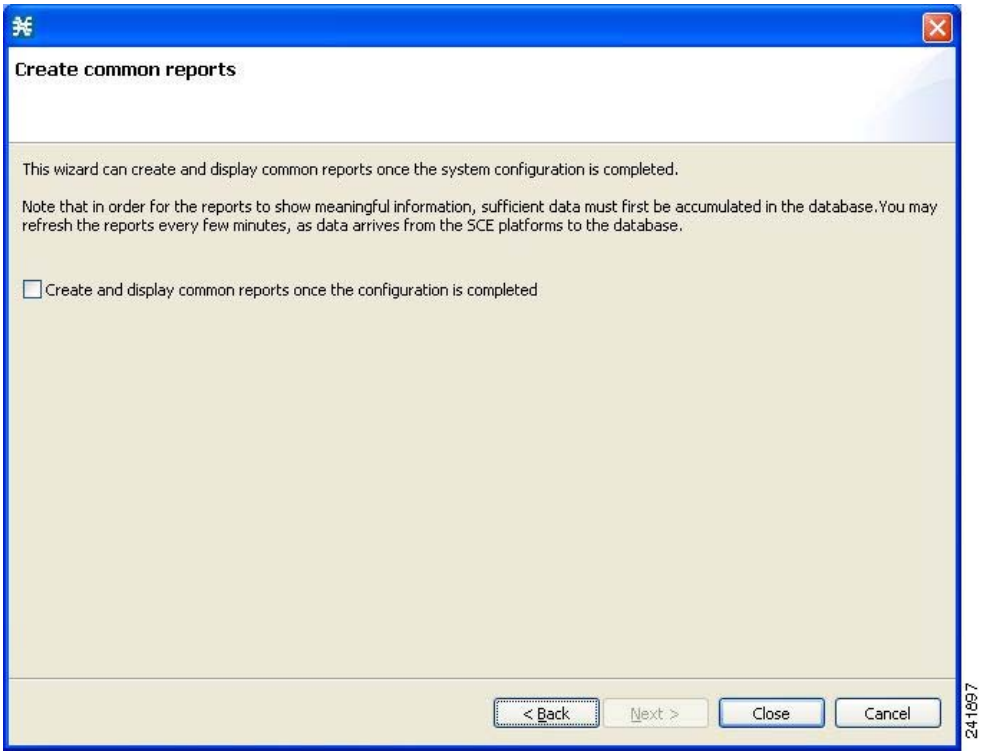
ステップ 22　ステップ 10 でデータベースを定義しなかった場合は、[Finish] をクリックします。

P2P Traffic Optimization ウィザードが閉じます。

ステップ 23　[Next] をクリックします。

P2P Traffic Optimization ウィザードの [Create common reports] ページが開きます（図 4-58 を参照）。

図 4-58　[Create Common Reports]



ステップ 24　レポートを作成するには、[Create and display common reports] チェックボックスをオンにします。

（注）　次の 4 つの定義済みレポート タイプに対し、レポート インスタンスが作成されます。

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

ステップ 25　[Close] をクリックします。

ウィザードが閉じます。

Console で Reporter ツールが開きます。

4 つの各レポート タイプのレポート インスタンスが Reporter ツールの [Report View] で開きます。

Reporter DB Configuration ウィザードの使用方法

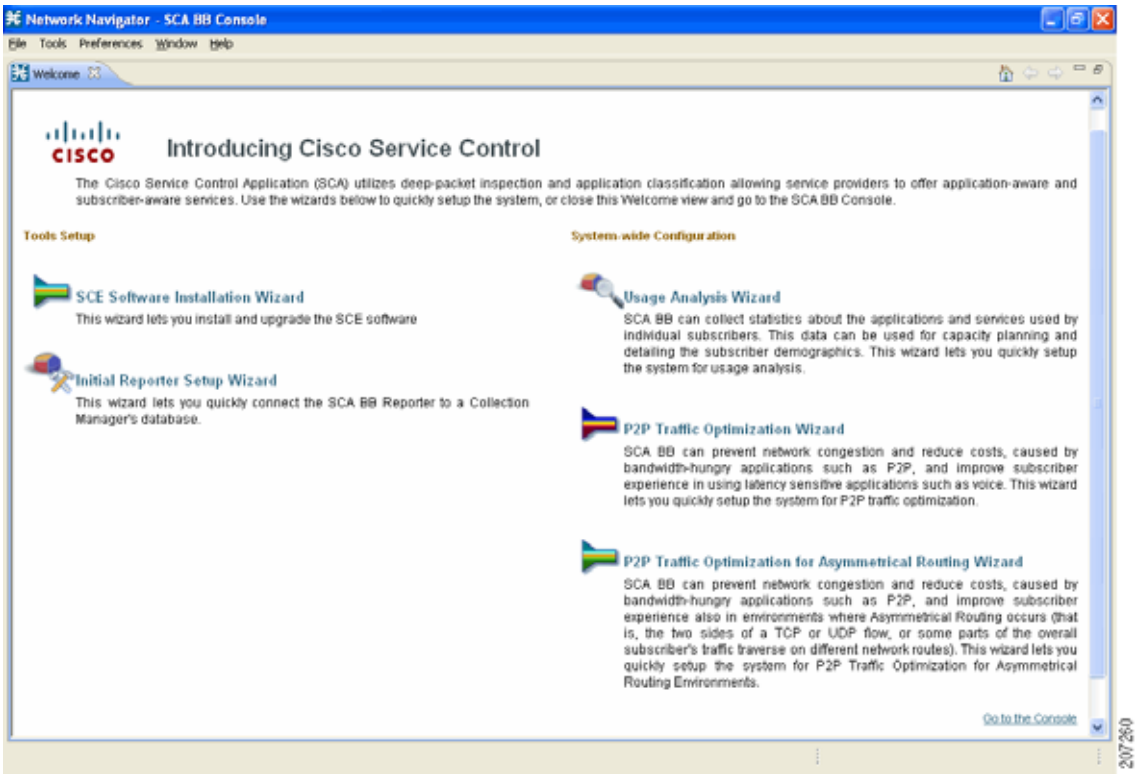
Reporter DB Configuration ウィザードでは、Reporter をデータベースに接続できます。

注意　Reporter DB Configuration ウィザードは、サービス コンフィギュレーションを SCE プラットフォームに適用してから実行してください。

ステップ 1　Console のメイン メニューで、[Help] > [Welcome] の順に選択します。

[Welcome] 画面が表示されます（図 4-59 を参照）。

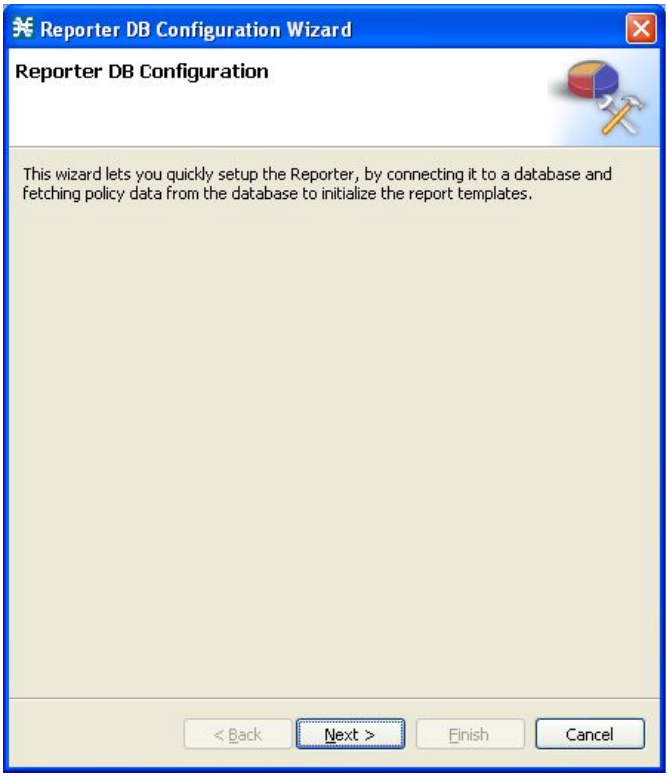
図 4-59　[Welcome] : [Introducing Cisco Service Control]



ステップ 2　[Initial Reporter Setup Wizard] をクリックします。

Reporter DB Configuration ウィザードの [Welcome] ページが表示されます（図 4-60 を参照）。

図 4-60　[Reporter DB Configuration]



ステップ 3　[Next] をクリックします。

Reporter DB Configuration ウィザードの [Reporter Setup] ページが開きます（図 4-61 を参照）。

図 4-61　[Reporter Setup]

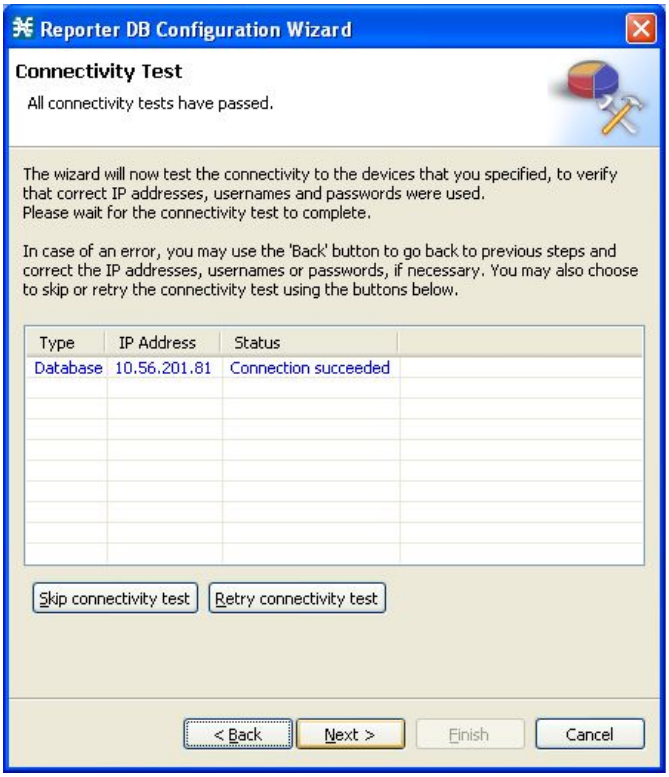
ステップ 4　[Configure the IP address of the database] フィールドにデータベースの IP アドレスを入力します。

ステップ 5　[Select the correct database type] ドロップダウン リストからデータベースのタイプを選択します。

ステップ 6　[Next] をクリックします。

Reporter DB Configuration ウィザードの [Connectivity Test] ウィンドウが開きます（図 4-62 を参照）。

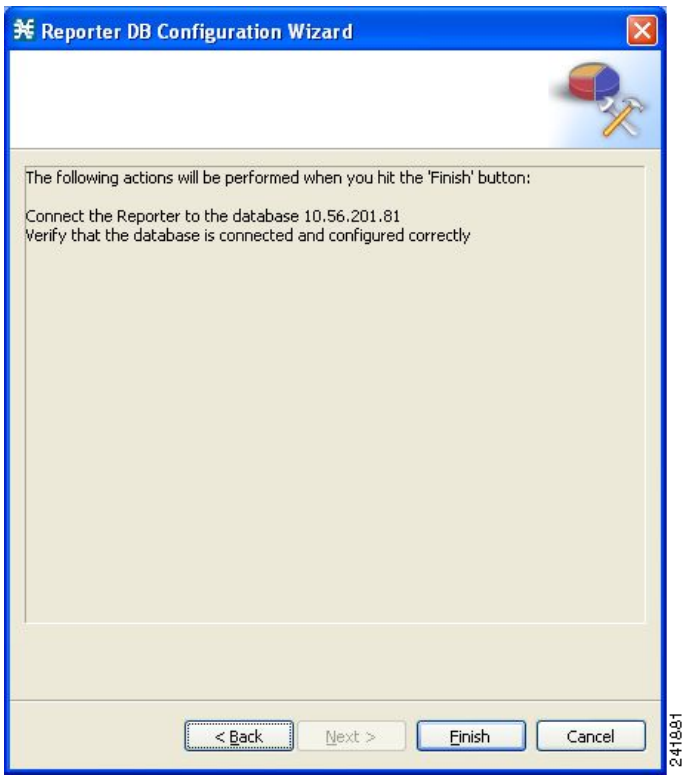
図 4-62　[Connectivity Test]



ステップ 7　[Next] をクリックします。

Reporter DB Configuration ウィザードの [Confirmation] ウィンドウが開きます（図 4-63 を参照）。

図 4-63　[Confirmation]

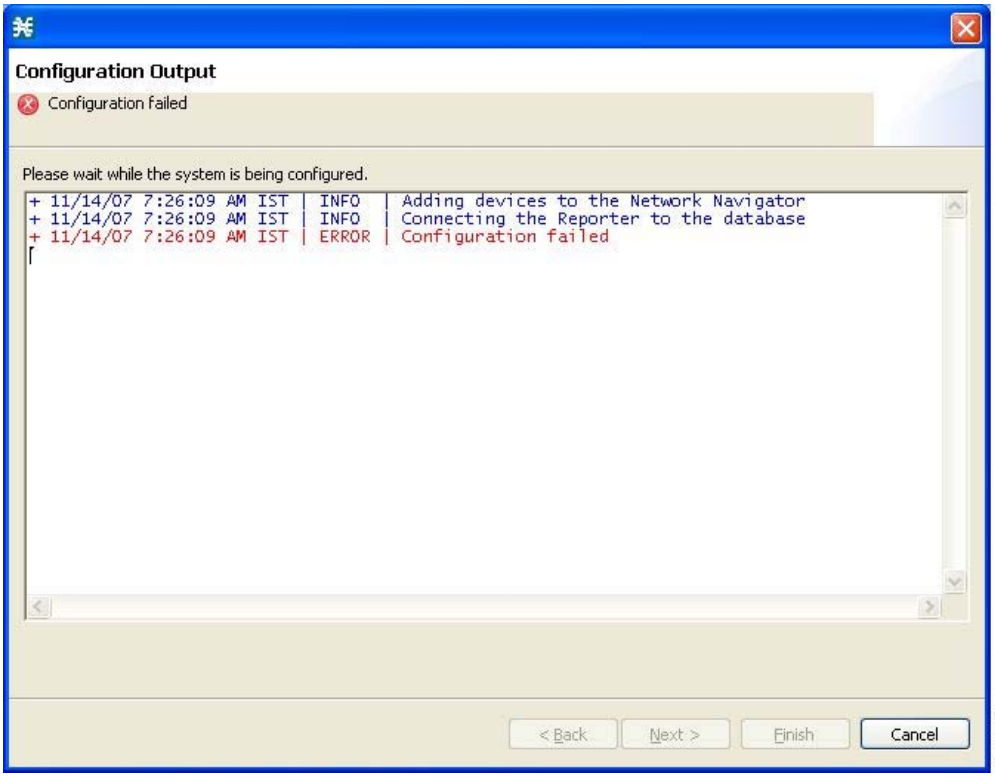


このページには、ウィザードでこれから実行される処理がリストされています。

ステップ 8　[Finish] をクリックします。

Reporter DB Configuration ウィザードの [Configuration Output] ページが開きます（図 4-64 を参照）。

図 4-64　[Configuration Output]



ウィザードは、選択されたデータベースに SCA BB Reporter ツールを接続しようとします。ウィザードがデータベースに接続できない場合、この処理は失敗します。

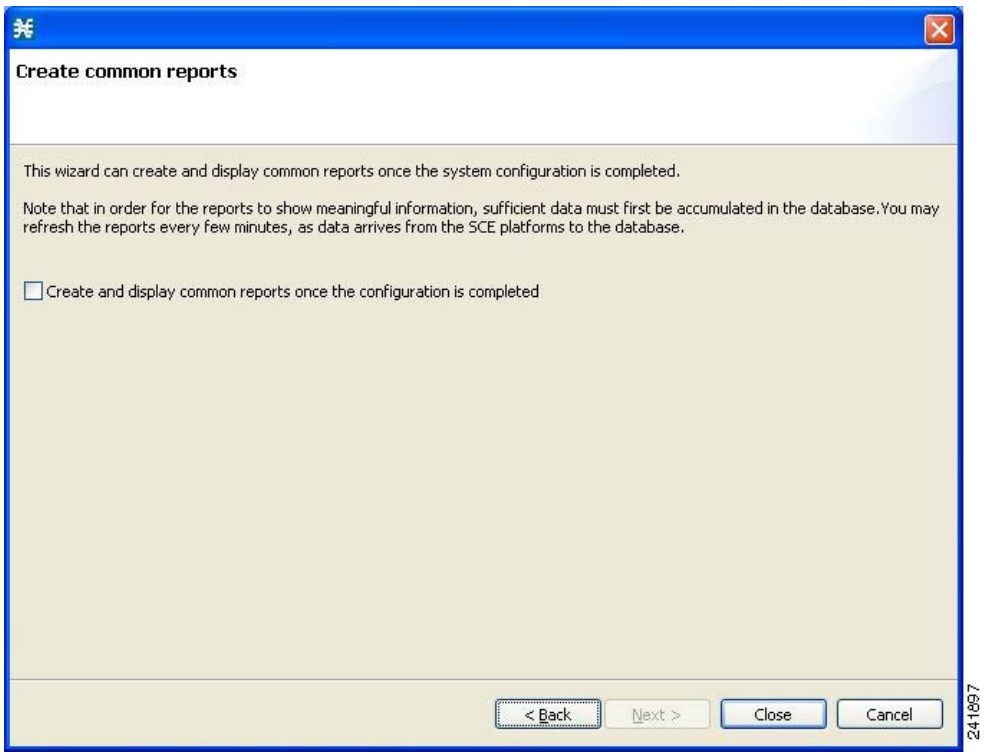
データベースのサービス コンフィギュレーション データが照会され、応答の最初の SCE デバイスがサービス コンフィギュレーション データのソースとして選択されます。

データベース デバイスが Network Navigator の [Site Manager] ツリーに追加されます。

ステップ 9　[Next] をクリックします。

Reporter DB Configuration ウィザードの [Create common reports] ページが開きます（図 4-65 を参照）。

図 4-65　[Create Common Reports]



ステップ 10　レポートを作成するには、[Create and display common reports] チェックボックスをオンにします。

（注）　次の 4 つの定義済みレポート タイプに対し、レポート インスタンスが作成されます。

- Global Bandwidth per Service
- Global Active Subscribers per Service
- Top P2P Protocols
- Global Hourly Call Minutes per Service (VoIP)

ステップ 11　[Close] をクリックします。

ウィザードが閉じます。

Console で Reporter ツールが開きます。

4 つの各レポート タイプのレポート インスタンスが Reporter ツールの [Report View] で開きます。

Network Navigator ツール

Network Navigator は、Cisco Service Control ソリューションに属するすべてのローカルおよびリモート デバイスの簡単なモデルを作成し、管理することができるツールです。

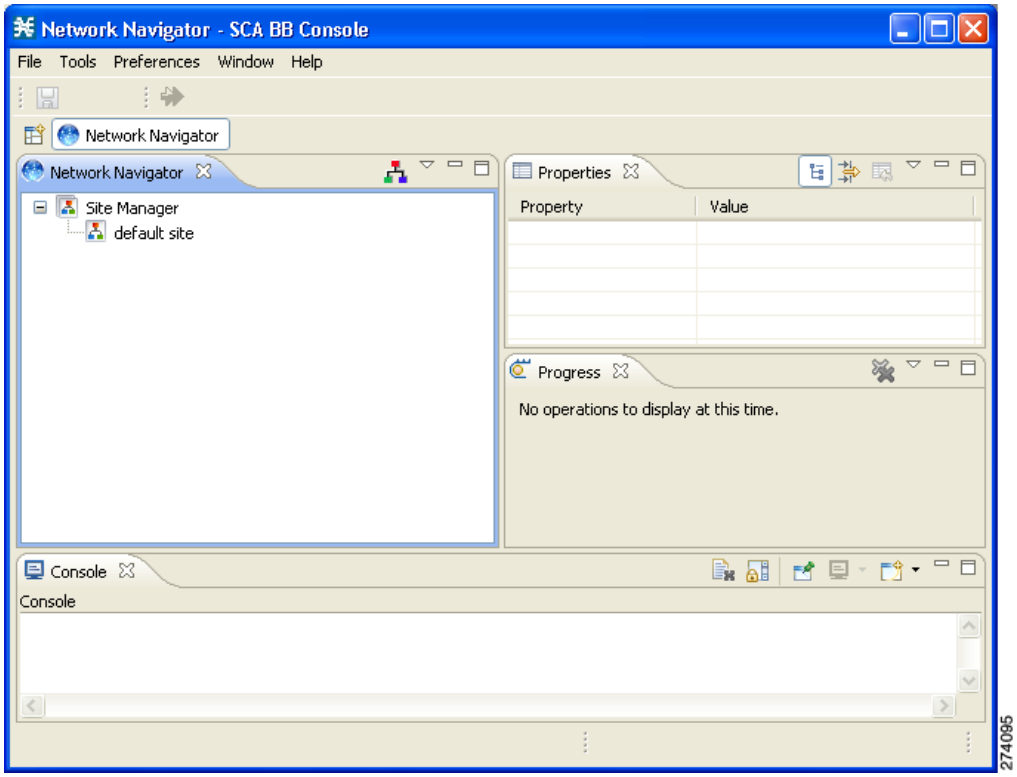
Network Navigator の詳細については、「Network Navigator の使用方法」（P.5-1）を参照してください。

Network Navigator ツールの開き方

ステップ 1　Console のメイン メニューで、[Tools] > [Network Navigator] の順に選択します。

Network Navigator ツールが開きます（図 4-66 を参照）。

図 4-66　Network Navigator



Network Navigator ツールの閉じ方

ステップ 1　[Network Navigator] ボタンを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Close] を選択します。

Network Navigator ツールが閉じます。

Service Configuration Editor ツール

Service Configuration Editor は、サービス コンフィギュレーションを作成できるツールです。サービス コンフィギュレーションは、SCE プラットフォームでのネットワーク トラフィックの分析方法、トラフィックに適用される規則、これらの規則を適用するために SCE プラットフォームが実行しなければならないアクションを定義するデータ構造です。

このマニュアルの大半は、Service Configuration Editor の使用方法について説明しています。「Service Configuration Editor の使用方法」（P.6-1）を参照してください。

Service Configuration Editor ツールの開き方

ステップ 1　Console のメイン メニューで、[Tools] > [Service Configuration Editor] の順に選択します。

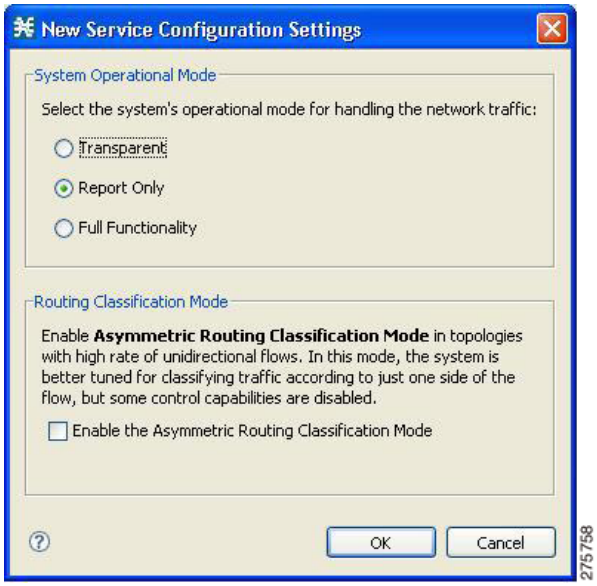
[No Service Configuration Is Open] ダイアログボックスが表示されます（図 4-67 を参照）。

図 4-67　[No Service Configuration Is Open]

ステップ 2　[Yes] をクリックします。

[New Service Configuration Settings] ダイアログボックスが表示されます（図 4-68 を参照）。

図 4-68　[New Service Configuration Settings]



ステップ 3　[System Operational Mode] のオプション ボタンをいずれか 1 つ選択します。

- [Transparent]：システムは RDR を生成せず、ネットワーク トラフィックにアクティブな規則を適用しません。
- [Report only]：システムは RDR の生成だけを実行します。ネットワーク トラフィックには、アクティブな規則は適用されません。
- [Full Functionality]：システムはアクティブな規則をネットワーク トラフィックに適用し、レポート機能を実行します（つまり、RDR を生成します）。

（注）　システムの動作モードはいつでも変更できます。

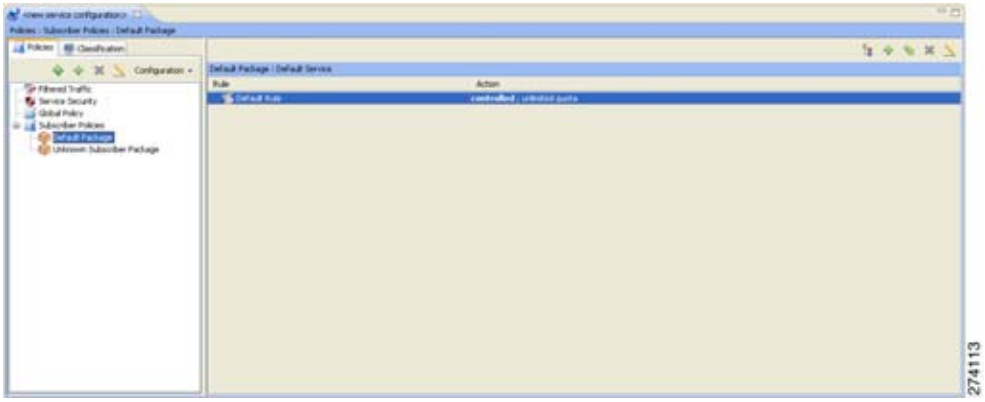
ステップ 4　非対称ルーティング分類モードに切り替えるために、[Enable the Asymmetric Routing Classification Mode] チェックボックスをオンにします（これはオプションですが、単方向フローの比率が高いシステムには強く推奨します）。

（注）　サービス コンフィギュレーションの作成後にはルーティング分類モードを変更しないことを推奨します。変更した場合は、サービス コンフィギュレーション データが失われるからです （「非対称ルーティング分類モード」（P.10-44）を参照）。

ステップ 5　[OK] をクリックします。

デフォルトのサービス コンフィギュレーションが Service Configuration Editor ツールで開きます（図 4-69 を参照）。

図 4-69　Service Configuration Editor



Service Configuration Editor ツールの閉じ方

ステップ 1　[Service Configuration Editor] ボタンを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Close] を選択します。

Service Configuration Editor ツールが閉じます。

Signature Editor ツール

Signature Editor は、SCA BB でプロトコルおよびプロトコル シグニチャの追加と変更が可能なファイルを作成し、変更することができるツールです。

Signature Editor の詳細については、「Signature Editor の使用方法」（P.12-1）を参照してください。

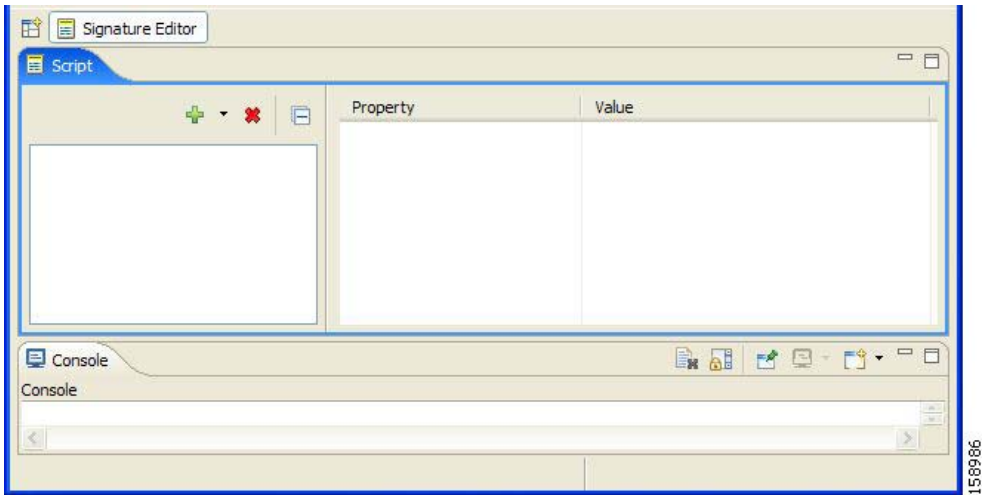
- 「Signature Editor ツールの開き方」（P.4-71）
- 「Signature Editor ツールの閉じ方」（P.4-71）

Signature Editor ツールの開き方

ステップ 1　Console のメイン メニューで、[Tools] > [Signature Editor] の順に選択します。

Signature Editor ツールが開きます（図 4-70 を参照）。

図 4-70　Signature Editor ツール



Signature Editor ツールの閉じ方

ステップ 1　[Signature Editor] ボタンを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Close] を選択します。

Signature Editor ツールが閉じます。

Subscriber Manager GUI ツール

Subscriber Manager（SM）GUI は、SCMS-SM に接続してサブスクライバを管理し、サブスクライバにパッケージを割り当て、サブスクライバ パラメータを編集し、手動でサブスクライバを追加することのできるツールです。

SCMS-SM への接続および SM GUI の使用方法に関する詳細は、「Subscriber Manager の GUI ツールの使用方法」（P.11-1）を参照してください。

SCMS-SM の詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

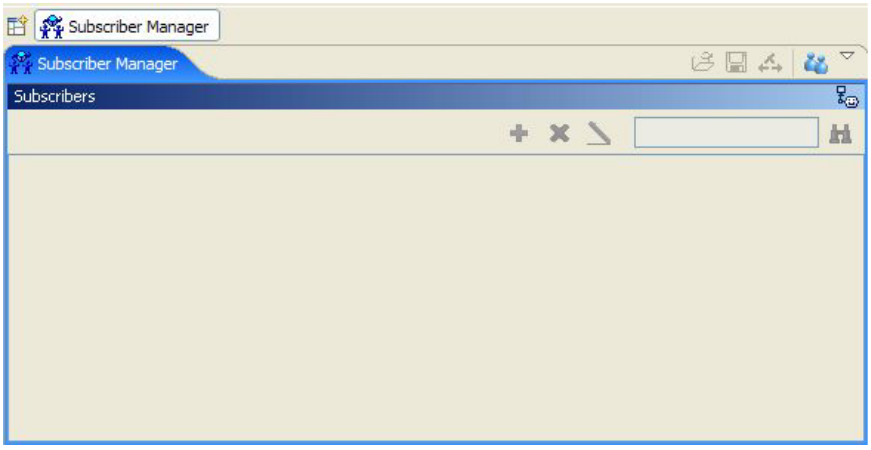
- 「SM GUI ツールの開き方」（P.4-72）
- 「SM GUI ツールの閉じ方」（P.4-72）

SM GUI ツールの開き方

ステップ 1　Console のメイン メニューで、[Tools] > [Subscriber Manager] の順に選択します。

SM GUI ツールが開きます（図 4-71 を参照）。

図 4-71　Subscriber Manager



SM GUI ツールの閉じ方

ステップ 1　[Subscriber Manager] ボタンを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Close] を選択します。

SM GUI ツールが閉じます。

Reporter ツール

Cisco Service Control Application（SCA）Reporter は、Cisco Service Control Management Suite（SCMS）Collection Manager（CM）RDR データベースに問い合わせて、結果を図や表に表示させることができます。このツールは、ネットワークで使用するアプリケーションおよびサブスクライバの動作やリソース消費の把握に役立ちます。また、各規則の有効性や、ネットワークに実装した場合の影響を評価する際にも役立ちます。レポートの表および図での表示、エクスポート、保存、外観の編集ができます。

Console 内では、SCA Reporter をスタンドアロンで実行することも、Reporter ツール内部で実行することも可能です。SCA Reporter の詳細については、『*Cisco Service Control Application Reporter User Guide*』を参照してください。

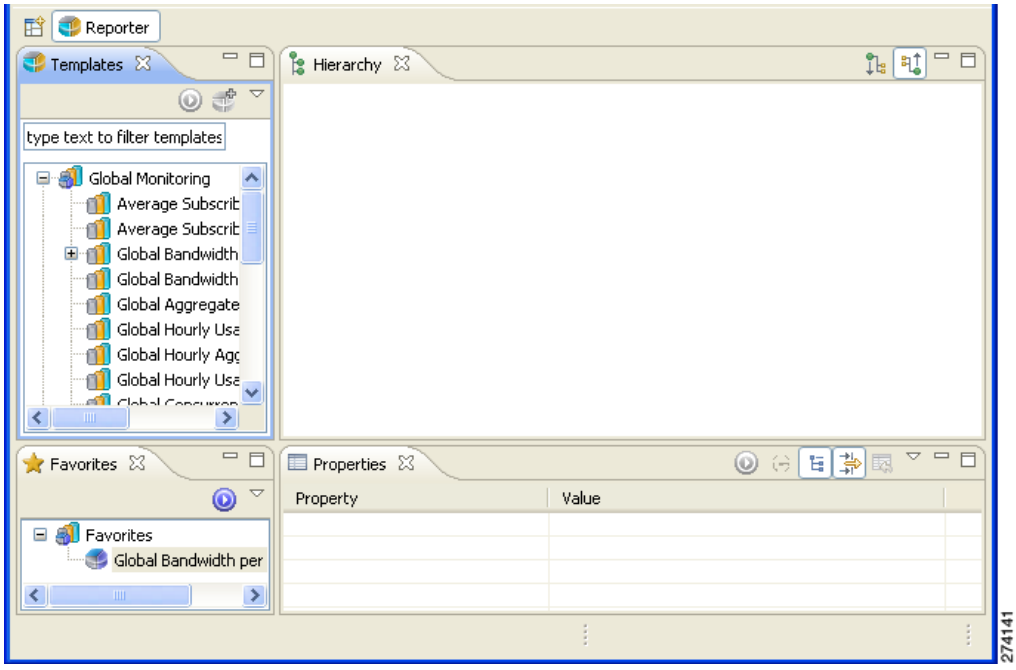
- 「Reporter ツールの開き方」（P.4-73）
- 「Reporter ツールの閉じ方」（P.4-74）

Reporter ツールの開き方

ステップ 1　Console のメイン メニューで、[Tools] > [Reporter] の順に選択します。

Reporter ツールが開きます（図 4-72 を参照）。

図 4-72　Reporter



（注）　SCA Reporter を使用すると、Console がデータベースに接続されている場合にだけ、レポートを生成できます（「データベースを SCA Reporter にアクセス可能にする方法」（P.5-28）を参照）。

Reporter ツールの閉じ方

ステップ 1　[Reporter] ボタンを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Close] を選択します。

Reporter ツールが閉じます。

オンライン ヘルプ

Console からこのユーザ ガイドの各部分にアクセスすることができます。

- 「オンライン ヘルプへのアクセス方法」（P.4-74）
- 「オンライン ヘルプの検索方法」（P.4-74）

オンライン ヘルプへのアクセス方法

ステップ 1　Console のメイン メニューで、[Help] > [Help Contents] の順に選択します。

オンライン ヘルプが別のウィンドウで開きます。

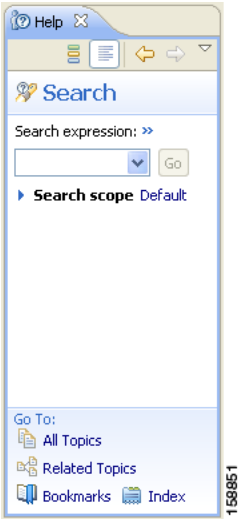
オンライン ヘルプの検索方法

現在のツールからもオンライン ヘルプを検索することができます。

ステップ 1　Console のメイン メニューで、[Help] > [Search] の順に選択します。

現在のツールの隣に、[Help] 画面が開きます（図 4-73 を参照）。

図 4-73　[Help]



ステップ 2　単語、句、またはさらに複雑な検索表現を [Search expression] フィールドに入力します。

[Go] ボタンがイネーブルになります。

（注）　検索表現の作成方法についての説明を表示するには、[>>]（[Expand]）をクリックします。

ステップ 3　[Go] をクリックします。

検索表現を含むヘルプ項目が [Local Help] の下に一覧表示されます。

ステップ 4　ヘルプ項目をクリックして、内容を表示させます。

（注）　あとで参照できるように項目にブックマークを付けることができます。

ステップ 5　[Help] 画面の下部で該当するリンクをクリックすると、次の部分への切り替えができます。

- [All topics]
- [Related topics]
- [Bookmarks]

Console のクイックスタート

このクイック スタート セクションは、初めて Console を使うときに役立ちます。ここでは、Network Navigator ツールと Service Configuration Editor を使用してデフォルトのサービス コンフィギュレーションを SCE プラットフォームに適用する方法を例示します。

例：Console の設定およびデフォルト サービス コンフィギュレーションの適用方法

この例では、SCE デバイスをデフォルト サイトに追加し、デフォルトのサービス コンフィギュレーションを SCE に適用します。

ステップ 1　Console を起動します。

[Start] > [All Programs] > [Cisco SCA] > [SCA BB Console 3.6.0] > [SCA BB Console 3.6.0] の順に選択します。

ステップ 2　必要に応じて [Welcome] 画面を閉じます。

ステップ 3　Network Navigator を開きます。

Console のメイン メニューで、[Tools] > [Network Navigator] の順に選択します。

このステップでは、ネットワーク デバイスの操作用に Console を設定します。

（注）　Console を最初に起動すると、Network Navigator ツールが開きます。

[Network Navigator] 画面にデフォルト サイトが表示されています。

ステップ 4　SCE デバイスをデフォルト サイトに追加します。

a. デフォルト サイトを右クリックし、表示されるポップアップ メニューで [New] > [SCE] の順に選択します。

Create new SCE ウィザードが表示されます。

[Address] フィールドに、SCE プラットフォームの実際の IP アドレスを入力します。

b. [Finish] をクリックします。

Create new SCE ウィザードが閉じます。

新規デバイスがサイトに追加されます。

ステップ 5　SCE プラットフォーム バージョンと動作状態をチェックします。

a. SCE デバイスを右クリックし、表示されるポップアップ メニューから [Online Status] を選択します。

[Password Management] ダイアログボックスが表示されます。

b. SCE を管理するためのユーザ名とパスワードを入力し、[Extract] をクリックします。

SCE オンライン ステータスが取得されます。

c. システムおよびアプリケーション バージョンが正しいことを確認し、動作状態が [Active] になっていることを確認します。

ステップ 6　Service Configuration Editor を開きます。

- Console のメイン メニューで、[Tools] > [Service Configuration Editor] の順に選択します。

Service Configuration Editor が開きます。

[No Service Configuration Is Open] ダイアログボックスが表示されます。

ステップ 7　新しいサービス コンフィギュレーションを作成します。

a. [No Editor Is Open] ダイアログボックスで [Yes] をクリックします。

[New Service Configuration Settings] ダイアログボックスが表示されます。

b. [OK] をクリックします。

デフォルトのサービス コンフィギュレーションが Service Configuration Editor で開きます。

ステップ 8　サービス コンフィギュレーションを SCE プラットフォームに適用します。

a. ツールバーから、  （[Apply Service Configuration to SCE Devices]）を選択します。

[Password Management] ダイアログボックスが表示されます。

b. SCE を管理するためのユーザ名とパスワードを入力し、[Apply] をクリックします。

サービス コンフィギュレーションが SCE プラットフォームに適用されます。

CHAPTER 5

Network Navigator の使用方法

はじめに

Service Control Engine（SCE）プラットフォーム、Subscriber Manager（SM）、Collection Manager（CM）などのネットワーク エンティティを Console で管理するには、まず Network Navigator でデバイスとして定義する必要があります。

この章では、Network Navigator ツールを使用して Cisco Service Control ソリューションに属するすべてのローカル / リモート サイトおよびデバイスのモデルを作成する方法、デバイスをリモートで管理する方法、および、Network Navigator ツールに装備されているその他の機能について説明します。

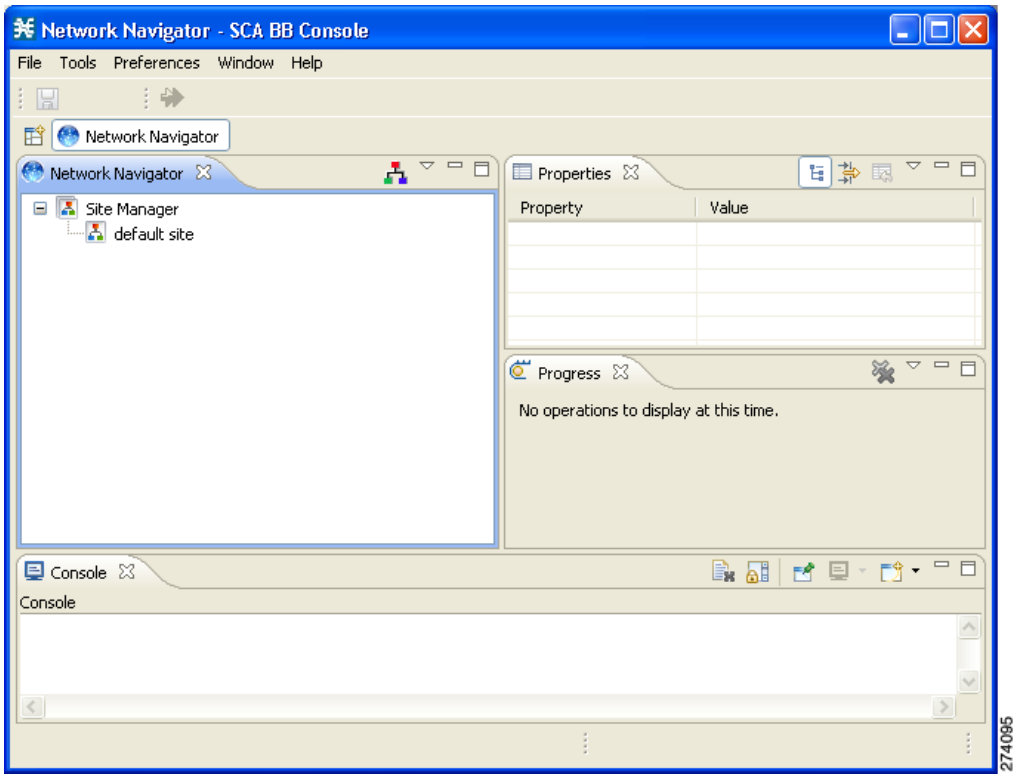
Usage Analysis ウィザードについてもこの章で説明します。このウィザードは、デバイスの簡単なモデルの作成と、デバイスの接続に使用できます。

Network Navigator ツール

Network Navigator ツール（図 5-1）は 4 つの画面で構成されています。

- [Network Navigator] 画面：システムの一部として定義したすべてのサイトとデバイスを [Site Manager] ツリーに表示します。
- [Properties] 画面：選択されたノードの編集可能プロパティを [Network Navigator] 画面の [Site Manager] ツリーに表示します。
- [Progress] 画面：[Site Manager] ツリーにあるサイトやデバイスでの操作時に、経過表示バーを表示します。
- [Console] 画面：Network Navigator ツールで実行されたアクションに関連するログ メッセージを表示します。

図 5-1　Network Navigator ツール



サイトの管理

ネットワーク エンティティが Network Navigator 内のデバイスに定義されている場合だけ、SCE、SM、または CM を Console から管理することができます。デバイスが Network Navigator に追加された場合、デバイスでの管理およびモニタリング操作を実行することができます。

デバイス グループの操作を実行することもできます。たとえば、同じサービス コンフィギュレーションを SCE プラットフォームのグループに適用することができます。Network Navigator により、同一サイトにデバイスを追加することでデバイスをグループ化することができます。サイトは互いに管理可能なデバイスのグループです。インストール時に、Network Navigator のデフォルト サイトにはデバイスが含まれていません。次のセクションで説明するように、デバイスをこのサイトに追加したり、他のサイトを追加したりすることができます。

サイト内のデバイスをグループ化すると、これらのデバイスのパスワード管理にも役立ちます（「パスワード管理」（P.5-7）を参照）。

Site Manager へのサイトの追加方法

デバイスを追加する前に、Site Manager にサイトを追加する必要があります。

ステップ 1　[Network Navigator] 画面で、[Site Manager] ノードを右クリックします。

ポップアップ メニューが表示されます（図 5-2）。

図 5-2　Site Manager メニュー

ステップ 2　メニューから、[New] > [Site] の順に選択します。

新規サイト ノードが Site Manager に追加されます。

ステップ 3　[Properties] 画面で、[Name] セルにサイト名を入力します。

ステップ 4　（オプション）[Version] セルにバージョン番号を入力します。

サイトへのデバイスの追加方法

SCE、SM、CM またはデータベース デバイスをサイトに追加することができます。

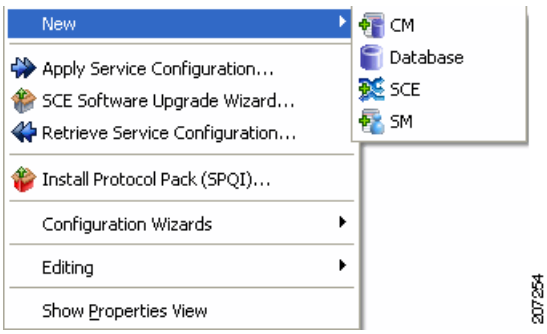
サイトへの SCE デバイスの追加方法

Network Navigator を使用して SCE プラットフォームのソフトウェアを設定、モニタ、アップデートするには、まず SCE プラットフォームをサイトに追加する必要があります。

ステップ 1　[Site Manager] ツリーで、サイトを右クリックします。

ポップアップ メニューが表示されます（図 5-3）。

図 5-3　[Site Manager] ツリー メニュー



ステップ 2　メニューから、[New] > [SCE] の順に選択します。

Create New SCE ウィザードが表示されます。

ステップ 3　[Address] フィールドに、SCE の IP アドレスを入力します。

ステップ 4　（オプション）[Name] フィールドに、SCE のわかりやすい名前を入力します。

ステップ 5　[Finish] をクリックします。

Create New SCE ウィザードが閉じます。

新規デバイスがサイトに追加されます。

サイトへの SM デバイスの追加方法

Network Navigator を使用して SM を設定、モニタ、アップデートするには、まず SM をサイトに追加する必要があります。

ステップ 1　[Site Manager] ツリーで、サイトを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　メニューから、[New] > [SM] の順に選択します。

Create New SM ウィザードが表示されます。

ステップ 3　[Address] フィールドに、SCMS-SM の IP アドレスを入力します。

ステップ 4　（オプション）[Name] フィールドに、SM のわかりやすい名前を入力します。

ステップ 5　[Finish] をクリックします。

Create New SM ウィザードが閉じます。

新規デバイスがサイトに追加されます。

サイトへの CM デバイスの追加方法

Network Navigator を使用して CM をモニタするには、まず CM をサイトに追加する必要があります。

ステップ 1　[Site Manager] ツリーで、サイトを右クリックします。
ポップアップ メニューが表示されます。

ステップ 2　メニューから、[New] > [CM] の順に選択します。
Create New CM ウィザードが表示されます。

ステップ 3　[Address] フィールドに、CM の IP アドレスを入力します。

ステップ 4　（オプション）[Name] フィールドに、CM のわかりやすい名前を入力します。

ステップ 5　[Finish] をクリックします。
Create New CM ウィザードが閉じます。
新規デバイスがサイトに追加されます。

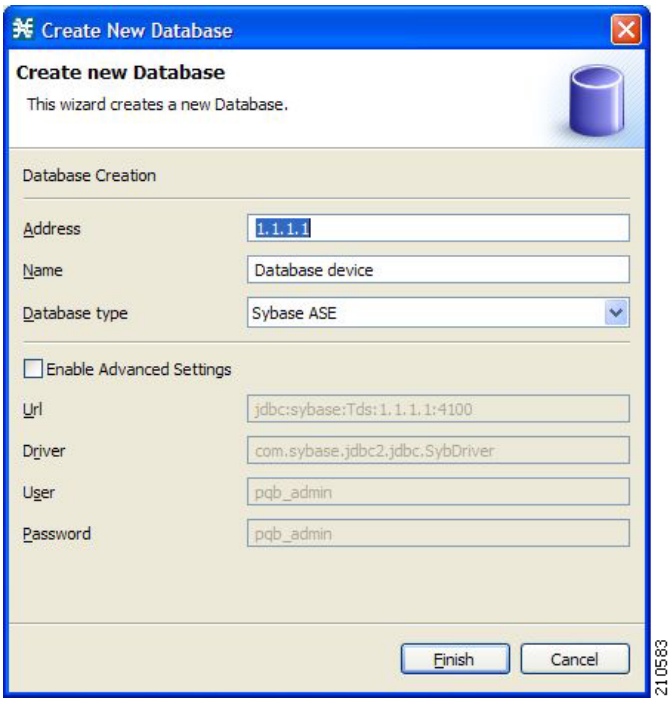
サイトへのデータベース デバイスの追加方法

Reporter ツールを使用してレポートを作成するには、最初にデータベースに接続する必要があります。

ステップ 1　[Site Manager] ツリーで、サイトを右クリックします。
ポップアップ メニューが表示されます。

ステップ 2　メニューから、[New] > [Database] の順に選択します。
Create New Database ウィザードが表示されます（図 5-4）。

図 5-4　[Create New Database]



ステップ 3　[Address] フィールドに、データベースの IP アドレスを入力します。

ステップ 4　（オプション）[Name] フィールドに、データベースのわかりやすい名前を入力します。

ステップ 5　[Database type] ドロップダウン リストで、データベース タイプを選択します。

ステップ 6　（オプション）[Enable Advanced Settings] チェックボックスをオンにして、[Url]、[Driver]、[User]、[Password] フィールドに新しい値を入力します。

ステップ 7　[Finish] をクリックします。

Create New Database ウィザードが閉じます。

新規デバイスがサイトに追加されます。

デバイスの削除方法

ステップ 1　[Site Manager] ツリーで、デバイスを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　メニューから [Delete] を選択します。

デバイスが削除されて [Site Manager] ツリーから削除されます。

サイトの削除方法

ステップ 1　[Site Manager] ツリーで、[Site Manager] ツリーにあるサイトを右クリックします。

ポップアップ メニューが表示されます。

- 要求された場合は、パスワードを入力します。

ステップ 2　メニューから [Delete] を選択します。

サイトとサイトの全デバイスが削除されて、サイトが [Site Manager] ツリーから削除されます。

デバイスの管理

Network Navigator により、SCE、SM、CM、データベース デバイスを管理することができます。

（注）　Usage Analysis ウィザードでは、デバイスの簡単なモデルを作成し、それらのデバイスに接続できます（「Usage Analysis ウィザードの使用方法」（P.4-34）を参照）。

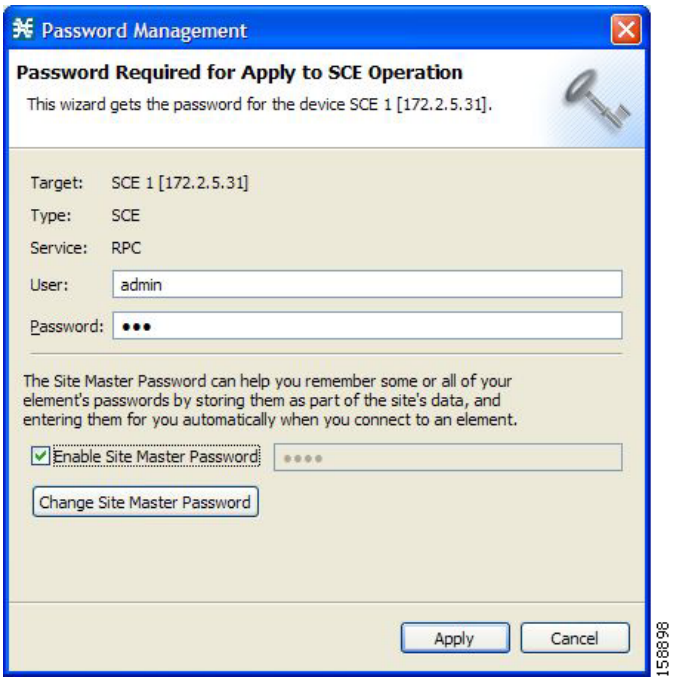
パスワード管理

通常、デバイス（SCE、SM、CM またはデータベース）にアクセスできるようになる前に、パスワードを入力する必要があります。サイト デバイスで操作を実行しようとする場合、Network Navigator はまずデバイスのユーザ名とパスワードを要求してきます （同じデバイスで同じ操作を繰り返す場合、パスワードを 2 回入力する必要がないこともあります）。

複数のデバイスで操作を実行する際に、パスワード入力が冗長になる場合もあります。Site Master Password は、サイトのデータの一部として格納すると、エレメントのユーザ名とパスワードの一部またはすべてを記憶し、エレメントに接続する際に自動的に入力します。

Site Master Password は、パスワード マネージャに保存されたユーザ名とパスワードを保護します。サイト パスワード マネージャを有効にする際、[Password Management] ダイアログボックス（図 5-5）でサイトのマスター パスワードを要求されます。複数のサイトがある場合、各サイトに個別のマスター パスワードが必要です。

図 5-5　[Password Management] ダイアログボックス



各サイトに対して、[Password Management] ダイアログボックスの表示時に、[Enable Site Master Password] チェックボックスをオンにします。

SCE デバイスの管理

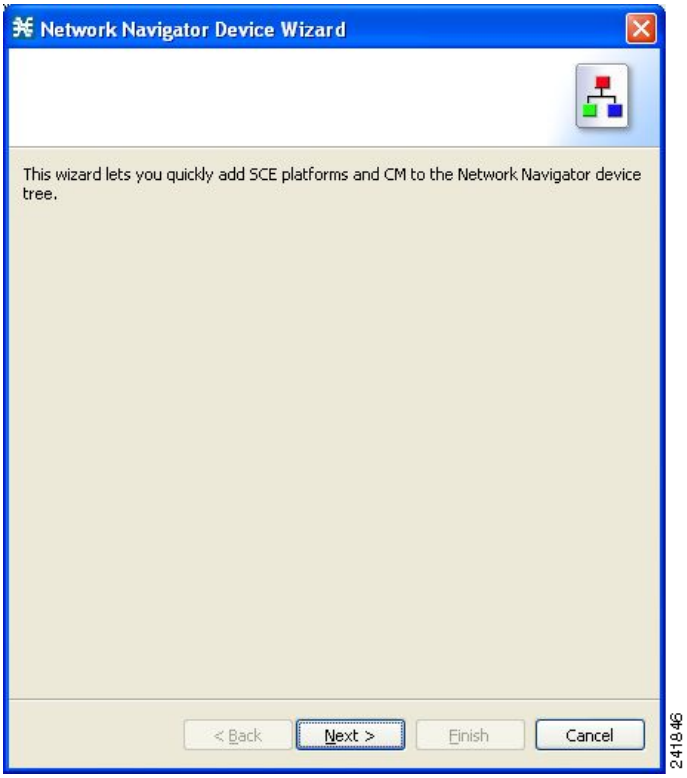
ウィザードを使用した SCE および CM デバイスの設定方法

Network Navigator Device ウィザードでは、SCA および CM デバイスを設定し、それらのデバイスに接続することができます。

（注）　デバイスが存在しない場合は、このウィザードで定義されたデバイスが [Site Manager] ツリーのデフォルト サイトに追加されます。

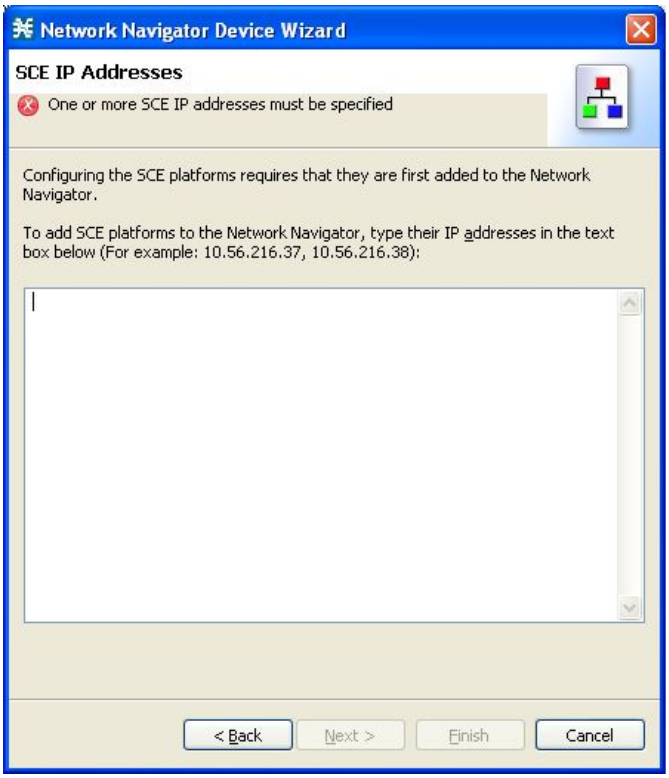
ステップ 1　[Network Navigator] 画面のツールバーで、([Configure SCE and CM devices]）をクリックします。
Network Navigator Device ウィザードの [Welcome] ウィンドウが表示されます（図 5-6）。

図 5-6　[Welcome] : [Network Navigator Device]



ステップ 2　[Next] をクリックします。
Network Navigator Device ウィザードの [SCE IP Addresses] ページが開きます（図 5-7）。

図 5-7　[SCE IP Addresses]



ステップ 3　編集ボックスで、モデルに追加する SCE デバイスの IP アドレスを入力します。

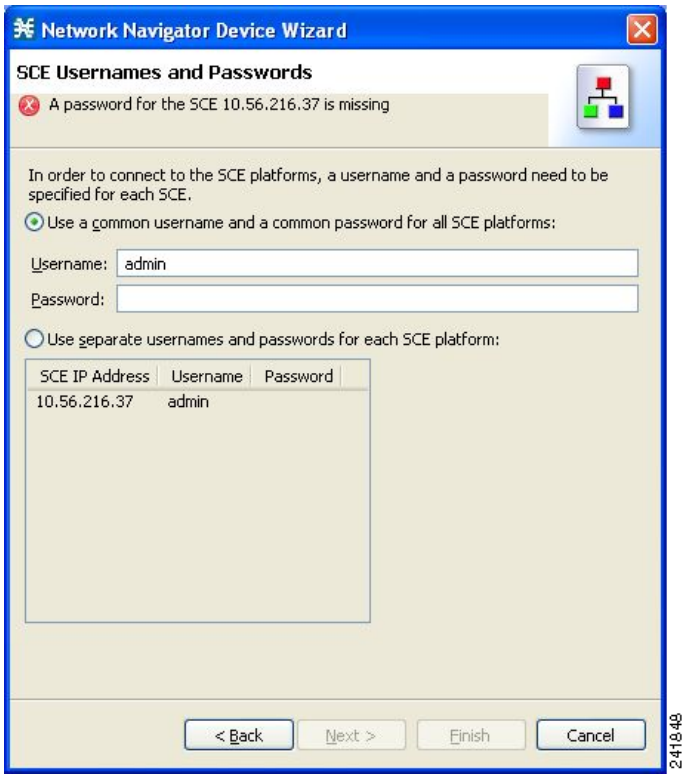
Network Navigator から操作を開始した場合は、選択した SCE デバイスの IP アドレスが編集ボックスに表示されます。アドレスは追加できます。

（注）　このウィザードでは、一度に最大 20 の SCE デバイスを操作できます。

ステップ 4　[Next] をクリックします。

Network Navigator Device ウィザードの [SCE Usernames and Passwords] ページが開きます（図 5-8）。

図 5-8　[SCE Usernames and Passwords]



ステップ 5　SCE デバイスのユーザ名とパスワードを入力します。

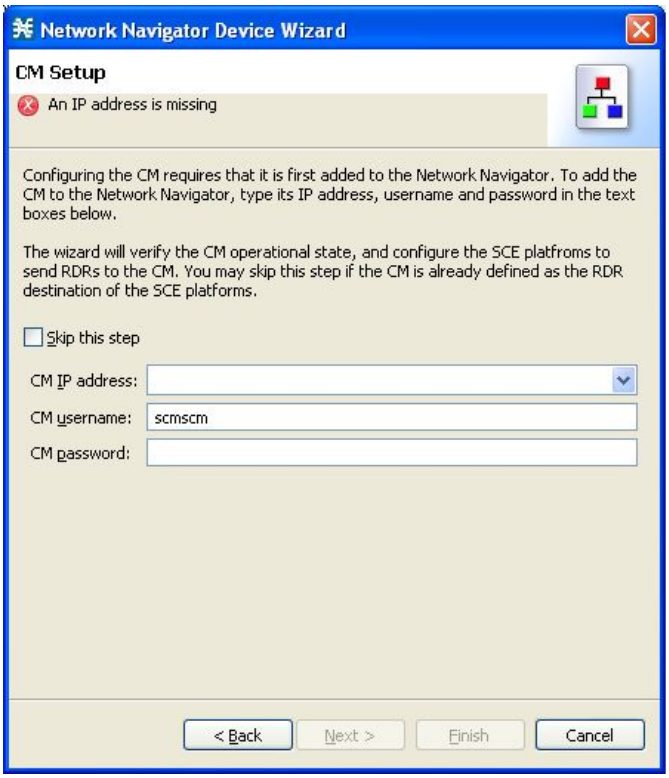
次のうちいずれかを実行します。

- 追加するすべての SCE デバイスに同じユーザ名とパスワードを使用するには、[Username] フィールドにユーザ名、[Password] フィールドにパスワードを入力します。
- 各 SCE デバイスに異なるユーザ名とパスワードのペアを設定するには、[Use separate usernames and passwords for each SCE device] オプション ボタンをオンにし、SCE デバイスごとに、SCE デバイス テーブルの該当するセルにユーザ名とパスワードを入力します。

ステップ 6　[Next] をクリックします。

Network Navigator Device ウィザードの [Setting CM devices] ページが開きます（図 5-9）。

図 5-9　[CM Setup]



ステップ 7　このコンフィギュレーションで使用する SCSM Collection Manager（CM）を定義します。

次のうちいずれかを実行します。

- 該当するフィールドに、CM デバイスの IP アドレス、ユーザ名、パスワードを入力します。

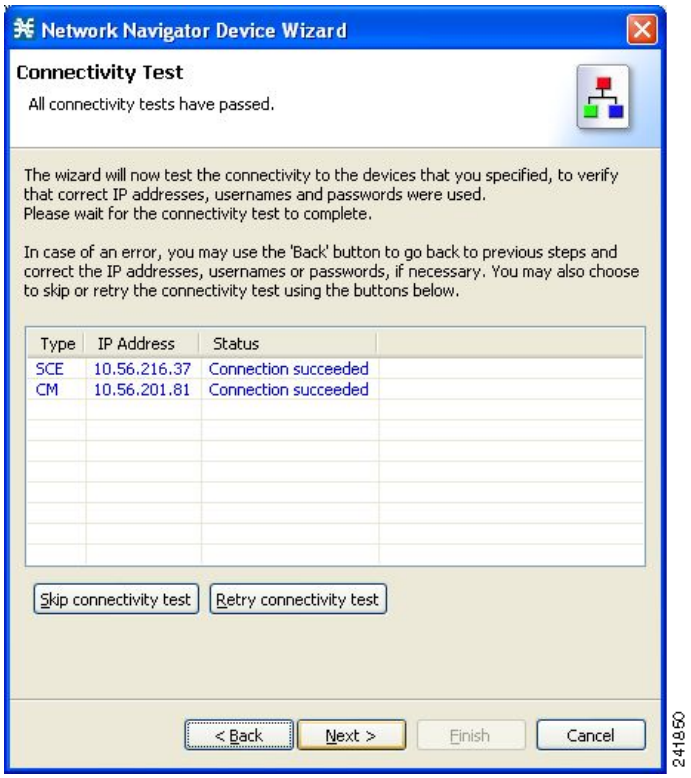
  Network Navigator から操作を開始した場合は、この情報が取得されて表示されます。これらのパラメータは変更できます。

- [Skip this step] チェックボックスをオンにします。

ステップ 8　[Next] をクリックします。

Network Navigator Device ウィザードの [Connectivity Test] ページが開きます（図 5-10）。

図 5-10　[Connectivity Test]



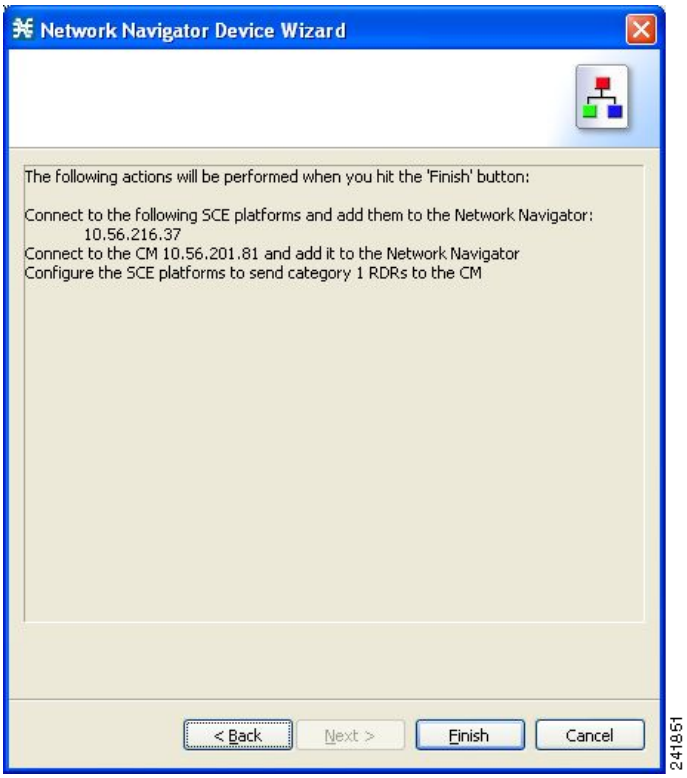
ウィザードは、定義済みデバイスへの接続が可能かどうかを確認するためのテストを実行します。

（注）　1 つ以上のデバイスに接続できない場合、または接続に何らかの問題がある場合（デバイスのバージョンが無効など）は、そのデバイスの横にエラーが表示されます。[Skip Connections] をクリックすると、このテストを省略できます。ウィザードの最後で [Finish] をクリックすると接続が検証されます。

ステップ 9　[Next] をクリックします。

Network Navigator Device ウィザードの [Confirmation] ページが開きます（図 5-11）。

図 5-11　[Confirmation]

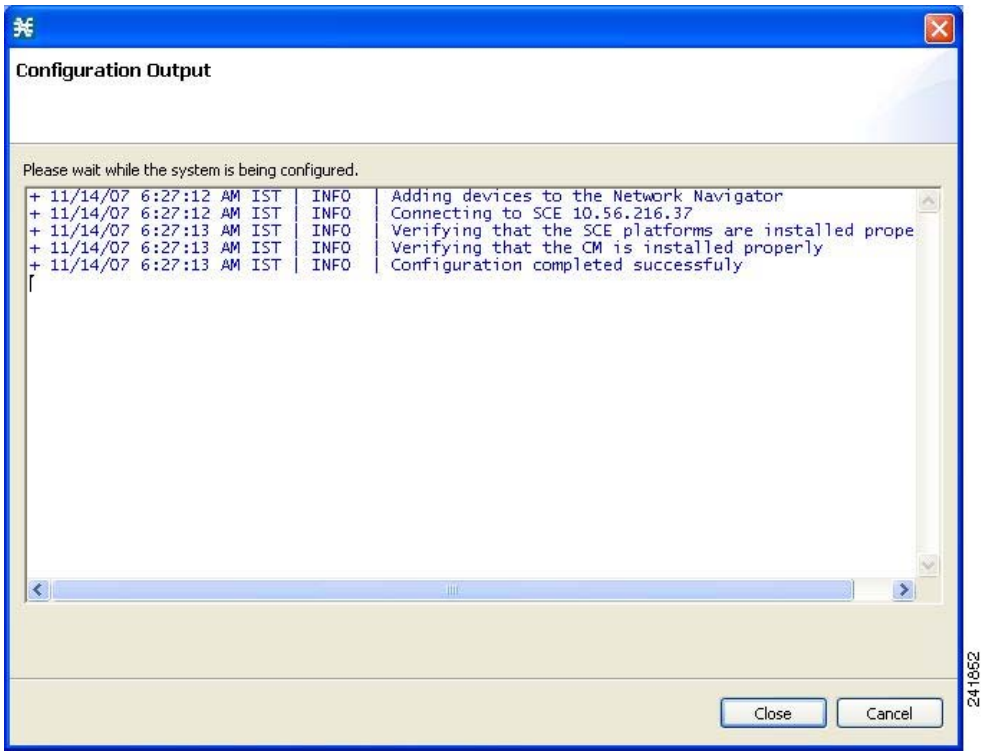


このページには、ウィザードでこれから実行される処理がリストされています。

ステップ 10　[Finish] をクリックします。

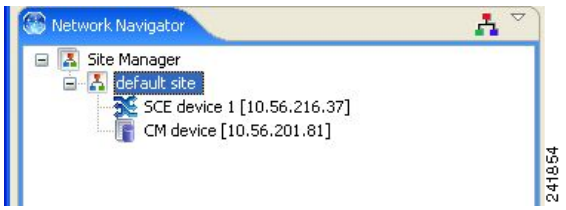
Network Navigator Device ウィザードの [Configuration Output] ページが開きます（図 5-12）。

図 5-12　[Configuration Output]



Network Navigator の [Site Manager] ツリーにあるデフォルト サイトに新規デバイスが追加されます（図 5-13）。

図 5-13　Network Navigator



ウィザードは、定義されたすべてのデバイスに対して接続を試行します。この処理は次の場合に失敗します。

- ステップ 3 でリストされた SCE デバイスのいずれかにウィザードが接続できない。
- ステップ 7 で CM が定義されたが、ウィザードがこれに接続できない。

ステップ 7 で CM が定義された場合、SCE デバイスはカテゴリ 1 の Raw Data Record（RDR; 未加工データ レコード）宛先だけが CM となるように設定されます。

（注）　RDR カテゴリは、異なるタイプの RDR を異なるコレクタに送信できるメカニズムです。RDR カテゴリの詳細については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」または『*Cisco SCE8000 GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」を参照してください。

新しいサービス コンフィギュレーションが作成されます。

- レポート専用モード。
- 最大トランザクション RDR レートは、デフォルト値（250）を SCE デバイス数で除算した値に設定されます（トランザクション RDR を設定するには、「Transaction RDR の管理方法」（P.8-5）を参照してください。トランザクション RDR のコンテンツと構造は、『*Cisco Service Control Application for Broadband Reference Guide*』の「Raw Data Records: Formats and Field Contents」にある「Transaction RDR」にリストされています）。

ステップ 11　[Finish] をクリックします。

Network Navigator Device ウィザードが閉じます。

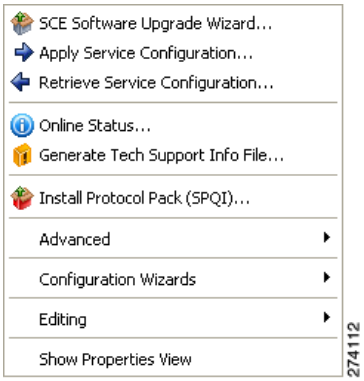
SCE デバイスのテクニカル サポート情報ファイルの生成方法

この操作では、シスコのテクニカル サポート スタッフが使用する SCE プラットフォームのサポート ファイルが生成されます。

ステップ 1　[Site Manager] ツリーで、SCE デバイスを右クリックします。

ポップアップ メニューが表示されます（図 5-14）。

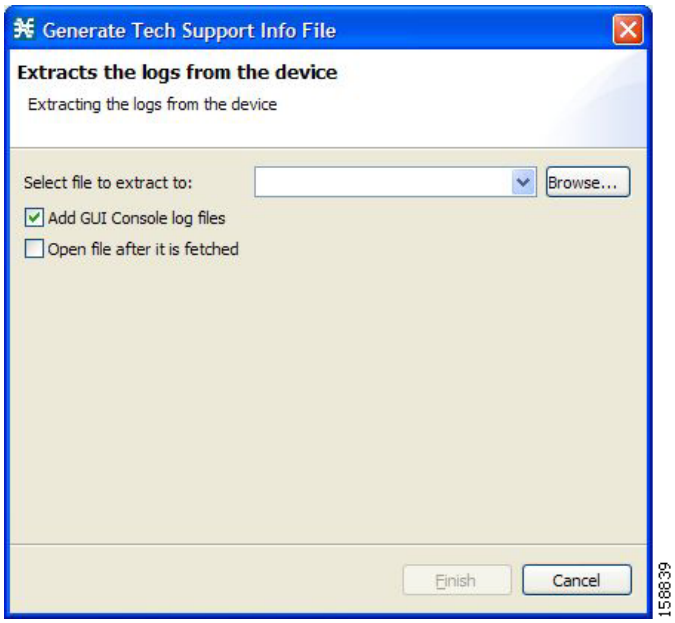
図 5-14　[Site Manager] ツリー メニュー



ステップ 2　メニューから、[Generate Tech Support Info File] を選択します。

[Generate Tech Support Info File] ダイアログボックスが表示されます（図 5-15）。

図 5-15　[Generate Tech Support Info File]



ステップ 3　[Browse] をクリックします。

[Select File] ダイアログボックスが表示されます。

ステップ 4　テクニカル サポート情報ファイルを保存するフォルダをブラウズします。

ステップ 5　[File name] フィールドで、新規ファイル名を入力するか、既存の zip ファイルを選択します。

ステップ 6　[Open] をクリックしてファイルを選択します。

ファイルが存在する場合、テクニカル サポート情報の生成時に上書きされます。

[Select File] ダイアログボックスが閉じます。

ステップ 7　（オプション）ログ ファイルを出力テクニカル サポート情報ファイルに追加するには、[Add GUI Console log files] チェックボックスをオンにします。

ステップ 8　（オプション）[Open file after it is fetched] チェックボックスをオンにします。

ステップ 9　[Finish] をクリックします。

[Generate Tech Support Info File] ダイアログボックスが閉じます。

[Password Management] ダイアログボックスが表示されます。

ステップ 10　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 11　[Generate] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Generate tech support info file] 経過表示バーが表示されます。

ファイルが生成されます。

SCE デバイスのオンライン ステータスの取得方法

この操作では、SCE プラットフォームの現在のソフトウェア バージョンと動作ステータスに関する情報を取得します。拡張 SCE オンライン ステータスは次のように分類されます。

- [System]：プラットフォーム情報が表示されます。
- [Configuration]：ホスト名が表示されます。
- [Status]：SCE の動作モードおよび合計トラフィックが表示されます。

SCE オンライン ステータスのモニタリングの詳細については、『*Cisco SCA BB Demo Kit Quick Start Guide*』を参照してください。

ステップ 1　[Site Manager] ツリーで、SCE デバイスを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　メニューから [Online Status] を選択します。

[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

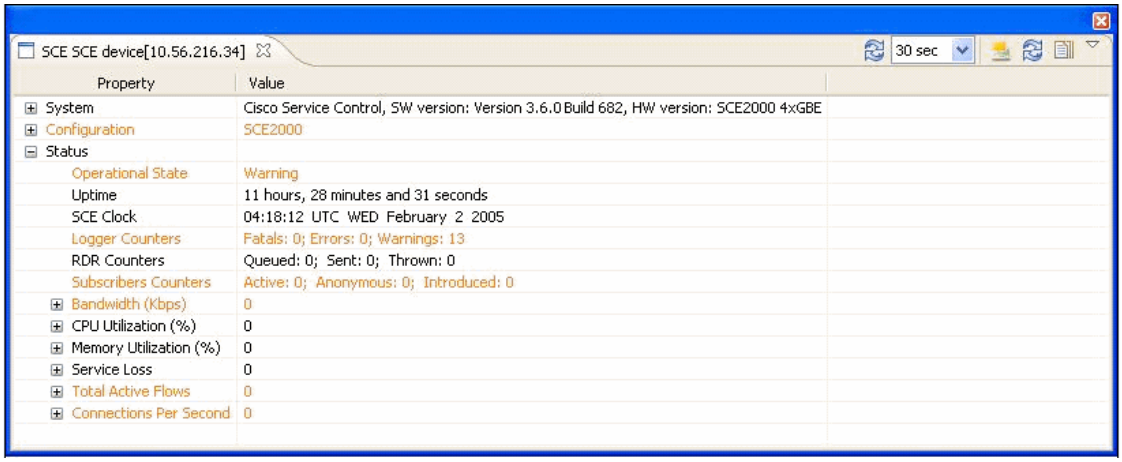
ステップ 4　[Extract] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Extracting info] 経過表示バーが表示されます。

SCE オンライン ステータスが取得されます（図 5-16）。

図 5-16　SCE オンライン ステータス



プロトコル パックのインストール方法

単一の SCE プラットフォーム、選択した複数の SCE プラットフォーム、または 1 つ以上の選択サイトにあるすべての SCE プラットフォームに、プロトコル パックをインストールすることができます。プロトコル パックの詳細については、「プロトコル パックの処理」（P.4-19）を参照してください。

（注）　複数の SCE プラットフォームにプロトコル パックをインストールする場合は、SCE Software Upgrade ウィザードを使用することを推奨します。

- 「単一の SCE プラットフォームへのプロトコル パックのインストール方法」（P.5-19）
- 「複数の SCE プラットフォームへのプロトコル パックのインストール方法」（P.5-20）

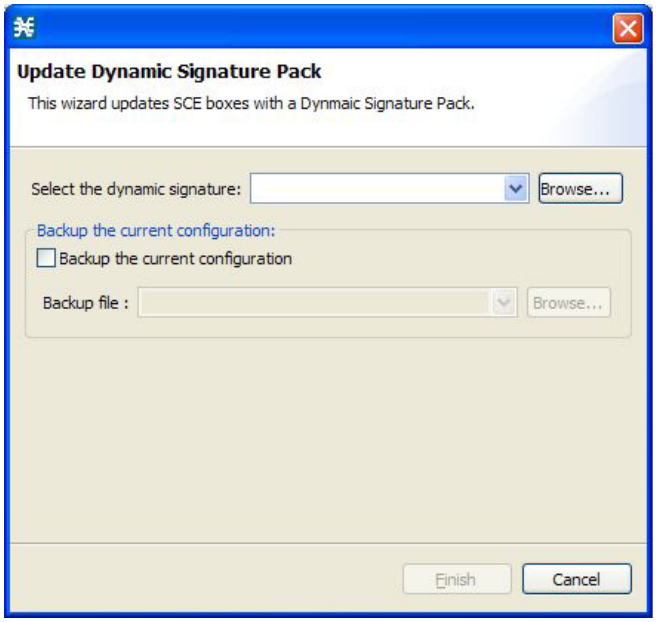
単一の SCE プラットフォームへのプロトコル パックのインストール方法

ステップ 1　[Site Manager] ツリーで、プロトコル パックをインストールする SCE を右クリックします。

ステップ 2　表示されるポップアップ メニューから [Update Dynamic Signature Pack] を選択します。

[Update Dynamic Signature Pack] ダイアログボックスが表示されます（図 5-17）。

図 5-17　[Update Dynamic Signature Pack]



ステップ 3　[Browse] をクリックします。

[Select file] ダイアログボックスが表示されます。

ステップ 4　[Files of type] ドロップダウン リストから、インストールするファイルに応じて [*.spqi] または [*.dss] を選択します。

ステップ 5　インストールするファイルをブラウズします。

ステップ 6　[Open] をクリックします。

[Select file] ダイアログボックスが閉じます。

ステップ 7　（推奨）[Backup the current configuration] チェックボックスをオンにして、[Browse] をクリックし、バックアップ ファイルを選択します。

ステップ 8　[Finish] をクリックします。

[Password Management] ダイアログボックスが表示されます。

ステップ 9　適切なパスワードを入力します

詳細については、「パスワード管理」（P.5-7）を参照してください。

ステップ 10　[Update] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Update Dynamic Signature Pack] ダイアログボックスが表示されます。

SCE プラットフォームのサービス コンフィギュレーションがアップデートされます。

複数の SCE プラットフォームへのプロトコル パックのインストール方法

SCE Software Upgrade ウィザードを使用して、複数の SCE プラットフォームにプロトコル パックをインストールできます。「SCE Software Upgrade ウィザードを使用した SCE のアップグレード方法」（P.4-8）を参照してください。

SCE デバイスへのサービス コンフィギュレーションの適用方法

単一 SCE プラットフォーム、選択した複数の SCE プラットフォーム、または 1 つ以上の選択サイト内にあるすべての SCE プラットフォームに、サービス コンフィギュレーションを適用することができます。

（注）　適用するサービス コンフィギュレーションは、Service Configuration Editor で開いている必要があります。

注意　悪質なトラフィックの異常ベース検出がイネーブルの場合、Service Control Engine（SCE）プラットフォームで設定されたものの、インターフェイス、アクセス マップ、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コミュニティ ストリングなどのいずれにも適用されていない Access Control List（ACL; アクセス コントロール リスト）は、サービス コンフィギュレーションがプラットフォームに適用されると削除される場合があります。

回避策：
悪質なトラフィックの異常ベース検出をディセーブルにする。
[Network Traffic] タブで [Service Security] を選択する。
サービス セキュリティ ダッシュボードで [Enable anomaly detection] チェックボックスをオフにする。

- 「単一の SCE プラットフォームへのサービス コンフィギュレーションの適用方法」（P.5-20）
- 「複数の SCE プラットフォームへのサービス コンフィギュレーションの適用方法」（P.5-21）

単一の SCE プラットフォームへのサービス コンフィギュレーションの適用方法

ステップ 1　[Site Manager] ツリーで、SCE デバイスを右クリックします。

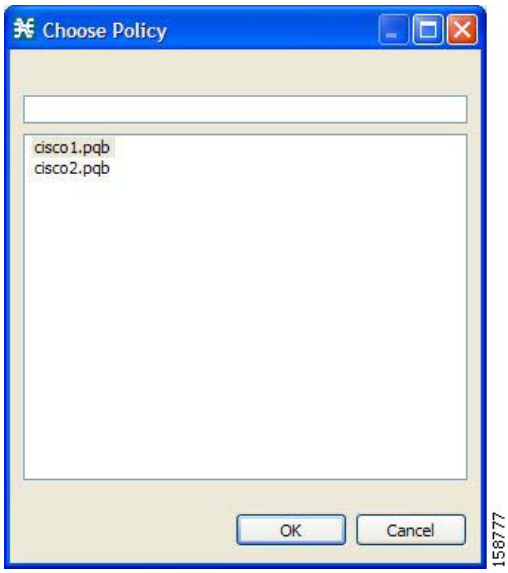
ポップアップ メニューが表示されます。

ステップ 2　メニューから [Apply Service Configuration] を選択します。

[Choose Policy] ダイアログボックスが表示され（図 5-18）、Service Configuration Editor で開いているすべてのサービス コンフィギュレーションが一覧表示されます。

（注）　Service Configuration Editor で開いているサービス コンフィギュレーションが 1 つだけの場合、[Password Management] ダイアログボックスが表示されます。ステップ 5 に進んでください（Service Configuration Editor でサービス コンフィギュレーションが開いていない場合は、エラー メッセージが表示されます）。

図 5-18　[Choose Policy]



ステップ 3　リストからサービス コンフィギュレーションを選択します。

ステップ 4　[OK] をクリックします。

[Password Management] ダイアログボックスが表示されます。

ステップ 5　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 6　[Apply] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Applying service configuration to SCE] 経過表示バーが表示されます。

選択された SCE プラットフォームにサービス コンフィギュレーションが適用されます。

複数の SCE プラットフォームへのサービス コンフィギュレーションの適用方法

ステップ 1　[Site Manager] ツリーで、サービス コンフィギュレーションを適用するサイトまたは SCE デバイスを選択し、それらのいずれかを右クリックします。

ステップ 2　表示されるポップアップ メニューから [Apply Service Configuration] を選択します。

[Choose Policy] ダイアログボックスが表示され、Service Configuration Editor で開いているすべてのサービス コンフィギュレーションが一覧表示されます。

（注）　Service Configuration Editor で開いているサービス コンフィギュレーションが 1 つだけの場合、[Password Management] ダイアログボックスが表示されます。ステップ 4 に進んでください（Service Configuration Editor でサービス コンフィギュレーションが開いていない場合は、エラー メッセージが表示されます）。

ステップ 3　リストからサービス コンフィギュレーションを選択し、[OK] をクリックします。

選択した SCE デバイスごとに個別の [Password Management] ダイアログボックスが表示されます。

ステップ 4　SCE デバイスごとにパスワードを入力し、[Apply] をクリックします。

サービス コンフィギュレーションが選択された SCE プラットフォームごとに順番に適用されます。

SCE デバイスからのサービス コンフィギュレーションの取得方法

単一 SCE プラットフォームから、選択した複数の SCE プラットフォーム、または 1 つ以上の選択サイト内にあるすべての SCE プラットフォームからサービス コンフィギュレーションを取得することができます。

- 「単一の SCE デバイスからのサービス コンフィギュレーションの取得方法」（P.5-22）
- 「複数の SCE プラットフォームからのサービス コンフィギュレーションの取得方法」（P.5-22）

単一の SCE デバイスからのサービス コンフィギュレーションの取得方法

ステップ 1　[Site Manager] ツリーで、SCE デバイスを右クリックします。

ポップアップ メニューが表示されます。

- 要求された場合は、パスワードを入力します。

ステップ 2　メニューから [Retrieve Service Configuration] を選択します。

[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します （詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 4　[Retrieve] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Retrieving from SCE] 経過表示バーが表示されます。

サービス コンフィギュレーションが SCE プラットフォームから取得され、Service Configuration Editor で開きます。

複数の SCE プラットフォームからのサービス コンフィギュレーションの取得方法

ステップ 1　[Site Manager] ツリーで、取得するサービス コンフィギュレーションのサイトまたは SCE デバイスを選択し、右クリックします。

ステップ 2　表示されるポップアップ メニューから [Retrieve Service Configuration] を選択します。

選択した SCE デバイスごとに個別の [Password Management] ダイアログボックスが表示されます。

ステップ 3　SCE デバイスごとにパスワードを入力し、[Retrieve] をクリックします。

各 SCE プラットフォームから順番にサービス コンフィギュレーションが取得され、Service Configuration Editor で開きます。

SCE デバイスへの PQI ファイルのインストール方法

この操作では、Cisco Service Control Application for Broadband（SCA BB）を SCE プラットフォームにインストールします。

（注）　複数の SCE デバイスに PQI ファイルをインストールする場合は、SCE Software Upgrade ウィザードを使用することを推奨します。「SCE Software Upgrade ウィザードを使用した SCE のアップグレード方法」（P.4-8）を参照してください。

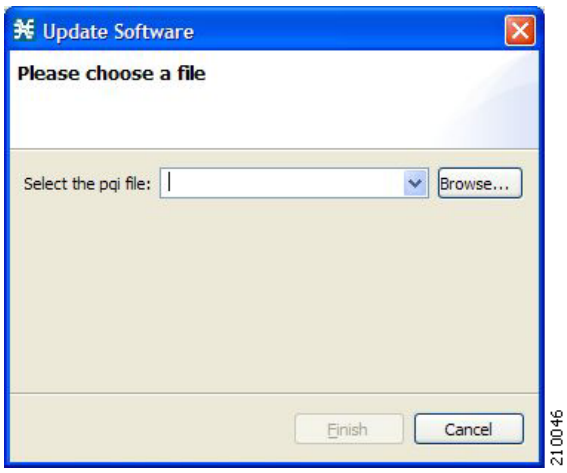
（注）　PQI ファイルのインストールには、通常数分かかります。

ステップ 1　[Site Manager] ツリーで、SCE デバイスを選択します。

ステップ 2　Console のメイン メニューで、[Network] > [Install PQI] の順に選択します。

[Update Software] ダイアログボックスが表示されます（図 5-19）。

図 5-19　[Update Software]



ステップ 3　[Browse] をクリックします。

[Select file] ダイアログボックスが表示されます。

ステップ 4　インストールしている PQI ファイルをブラウズします。

ステップ 5　[Open] をクリックします。

[Select file] ダイアログボックスが閉じます。

ステップ 6　[Finish] をクリックします。

[Password Management] ダイアログボックスが表示されます。

ステップ 7　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 8　[Apply] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Updating software to SCE] 経過表示バーが表示されます。

選択された SCE に PQI ファイルがインストールされます。

SCE デバイスへの SCE OS ソフトウェア パッケージのインストール方法

この操作では、SCE OS ソフトウェア パッケージ（SCE プラットフォームのオペレーティング システム ソフトウェアおよびファームウェア）をインストールします。

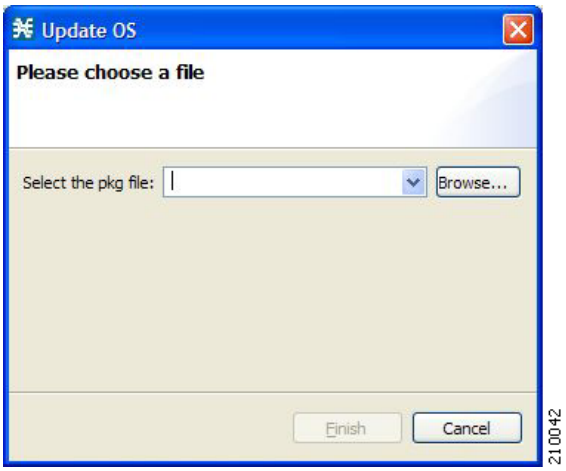
（注）　複数の SCE プラットフォームに SCE OS ソフトウェア パッケージをインストールする場合は、SCE Software Upgrade ウィザードを使用することを推奨します。「SCE Software Upgrade ウィザードを使用した SCE のアップグレード方法」（P.4-8）を参照してください。

ステップ 1　[Site Manager] ツリーで、SCE デバイスを選択します。

ステップ 2　Console のメイン メニューで、[Network] > [Upgrade SCE Platform Firmware (PKG)] の順に選択します。

[Update OS] ダイアログボックスが表示されます（図 5-20）。

図 5-20　[Update OS]



ステップ 3　[Browse] をクリックします。

[Select file] ダイアログボックスが表示されます。

ステップ 4　インストールする OS に含まれる PKG ファイルをブラウズします。

ステップ 5　[Open] をクリックします。

[Select file] ダイアログボックスが閉じます。

ステップ 6　[Finish] をクリックします。

[Password Management] ダイアログボックスが表示されます。

ステップ 7　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 8　[Apply] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Updating software to SCE] 経過表示バーが表示されます。

選択された SCE に PQI ファイルがインストールされます。

SM デバイスの管理

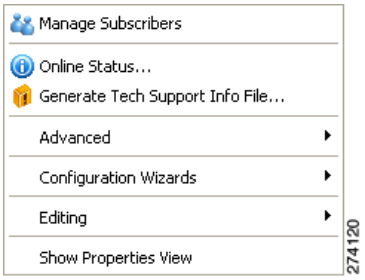
SM デバイスのテクニカル サポート情報ファイルの生成方法

この操作では、シスコのテクニカル サポート スタッフが使用する SM のサポート ファイルが生成されます。

ステップ 1　[Site Manager] ツリーで、SM デバイスを右クリックします。

ポップアップ メニューが表示されます（図 5-21）。

図 5-21　[Site Manager] ツリー メニュー



ステップ 2　メニューから、[Generate Tech Support Info File] を選択します。

[Tech Support Info File] ダイアログボックスが表示されます。

ステップ 3　[Browse] をクリックします。

[Select File] ダイアログボックスが表示されます。

ステップ 4　テクニカル サポート情報ファイルを保存するフォルダをブラウズします。

ステップ 5　[File name] フィールドで、新規ファイル名を入力するか、既存の zip ファイルを選択します。

ステップ 6　[Open] をクリックしてファイルを選択します。

ファイルが存在する場合、上書きされます。

[Select File] ダイアログボックスが閉じます。

ステップ 7　（オプション）ログ ファイルを出力テクニカル サポート情報ファイルに追加するには、[Add GUI Console log files] チェックボックスをオンにします。

ステップ 8　[Open file after it is fetched] チェックボックスをオンにします。

ステップ 9　[Finish] をクリックします。

[Generate Tech Support Info File] ダイアログボックスが閉じます。

[Password Management] ダイアログボックスが表示されます。

ステップ 10　適切なパスワードを入力します （詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 11　[Generate] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Generate tech support info file] 経過表示バーが表示されます。

ファイルが生成されます。

SM デバイスのオンライン ステータスの取得方法

この操作では、SM の現在のソフトウェア バージョンと動作ステータスに関する情報を取得します。

ステップ 1　[Site Manager] ツリーで、SM デバイスを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　メニューから [Online Status] を選択します。

[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

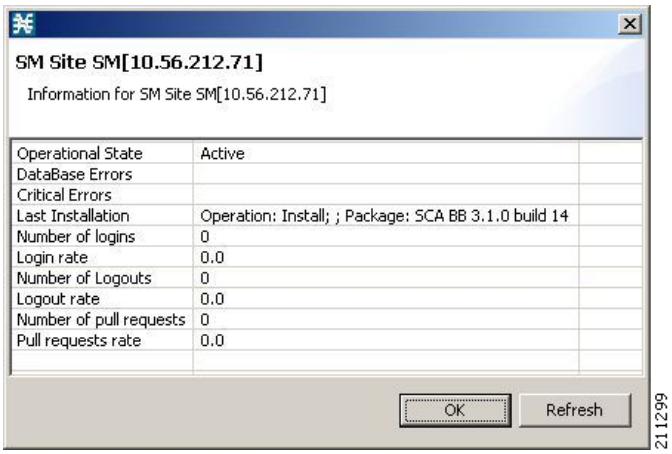
ステップ 4　[Extract] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Extracting info] 経過表示バーが表示されます。

SCMS-SM オンライン ステータスが取得されます（図 5-22）。

図 5-22　SCMS-SM オンライン ステータス



SM デバイスへの接続方法

SM GUI ツールを使用してサブスクライバを管理するためには、SM デバイスを接続する必要があります。

（注）　SM GUI ツールは、ポート 14374 への PRPC 接続を開き、[Password Management] ダイアログボックスに入力されたユーザ名とパスワードを使用してログインを試行することで、SCMS-SM での認証を実行します。このユーザを含む PRPC サーバが SCMS-SM で動作していない場合、認証はエラーになります。
SCMS-SM で PRPC ポートを変更した場合は、「ユーザ認証」（P.5-36）を参照してください。

ステップ 1　[Site Manager] ツリーで、SM デバイスを右クリックします。

ポップアップ メニューが表示されます。

ステップ 2　メニューから [Manage Subscribers] を選択します。

[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します （詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 4　[Connecting] をクリックします。

[Password Management] ダイアログボックスが閉じます。

接続の経過表示バーが表示されます。

SM に接続して、Console を SM GUI ツールに切り替えます。

操作の詳細については、「Subscriber Manager の GUI ツールの使用方法」（P.11-1）を参照してください。

CM デバイスの管理

ウィザードを使用して CM デバイスを設定できます （「ウィザードを使用した SCE および CM デバイスの設定方法」（P.5-8）を参照）。

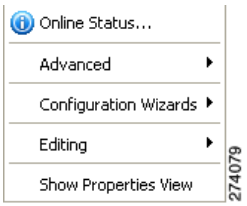
CM デバイスのオンライン ステータスの取得方法

この操作では、CM の現在のソフトウェア バージョンと動作ステータスに関する情報を取得します。

ステップ 1　[Site Manager] ツリーで、CM デバイスを右クリックします。

ポップアップ メニューが表示されます（図 5-23）。

図 5-23　[Site Manager] ツリー メニュー



ステップ 2　メニューから [Online Status] を選択します。

[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 4　[Extract] をクリックします。

[Password Management] ダイアログボックスが閉じます。

[Extracting info] 経過表示バーが表示されます。

SCMS-CM オンライン ステータスが取得されます。

取得されたオンライン ステータスのウィンドウ（SCE プラットフォームの）の例は、「SCE デバイスのオンライン ステータスの取得方法」（P.5-18）を参照してください。

データベース デバイスの管理

データベースを SCA Reporter にアクセス可能にする方法

- Reporter DB Configuration ウィザードでは、Reporter を単一のデータベースに接続できます（「Reporter DB Configuration ウィザードの使用方法」（P.4-61）を参照）。
- 代替手順については、『*Cisco Service Control Application Reporter User Guide*』の「*Using the Cisco Service Control Application Reporter*」にある「*Configuring Properties*」を参照してください。

ステップ 1　[Site Manager] ツリーで、データベース デバイスを右クリックします。

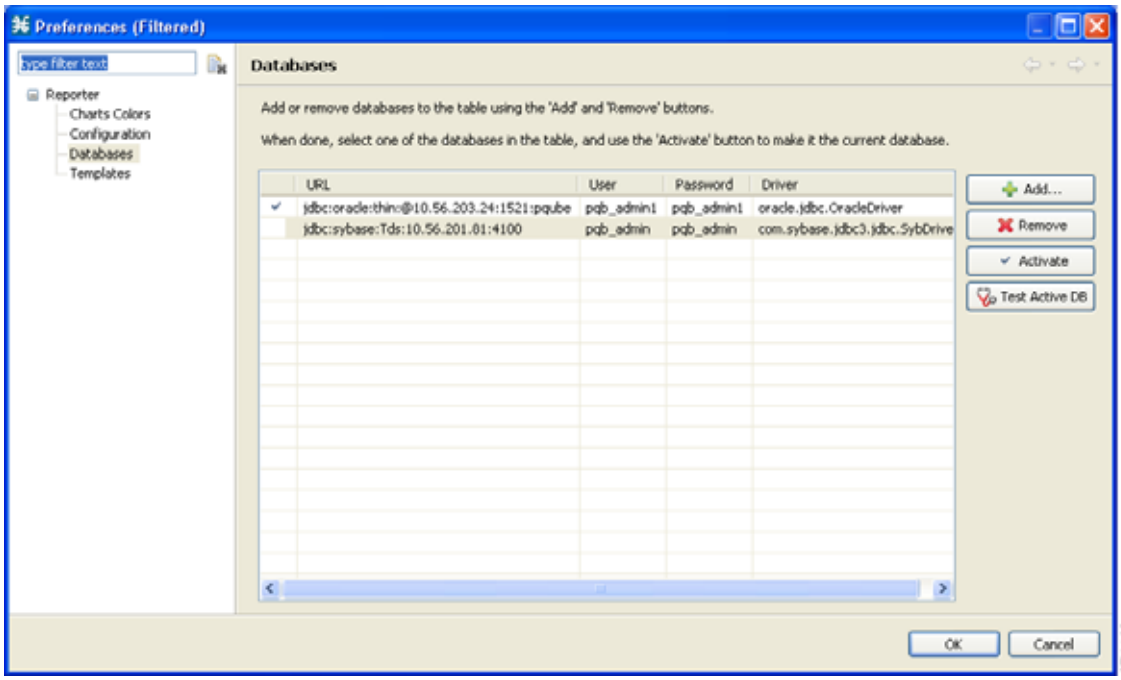
ポップアップ メニューが表示されます（図 5-24）。

図 5-24　[Site Manager] ツリー メニュー

ステップ 2　メニューから [Add to Reporter] を選択します。

[Preferences] ダイアログボックスが表示されます（図 5-25）。

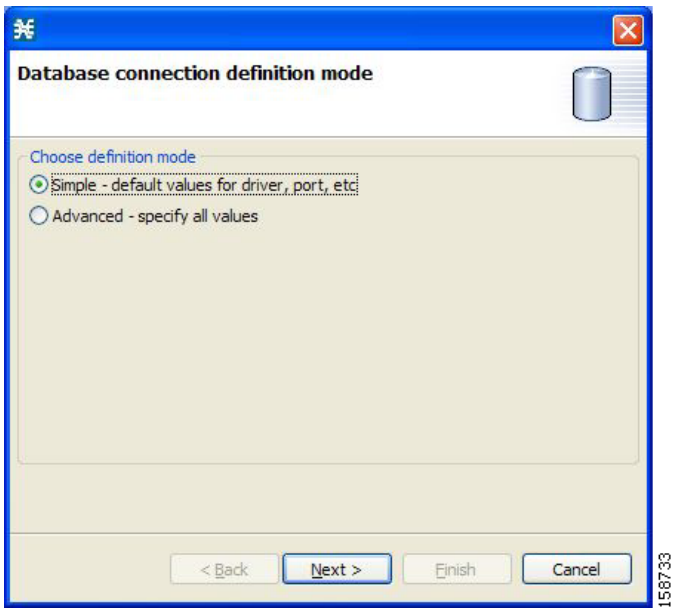
図 5-25　[Preferences]



ステップ 3　[Add] をクリックします。

Add Database ウィザードが表示されます（図 5-26）。

図 5-26　Add Database



ステップ 4　[Choose definition mode] のオプション ボタンをいずれか 1 つ選択します。

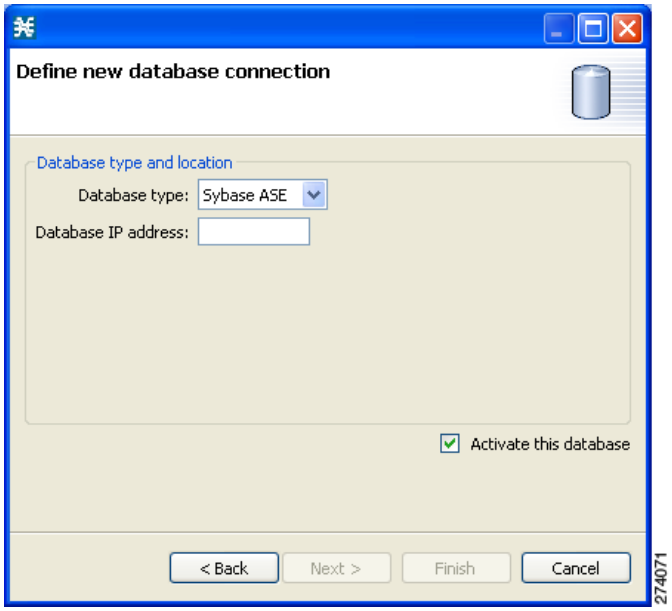
- **[Simple]**：ドライバ、ポートなどのデフォルト値です。
- **[Advanced]**：すべての値を指定します。

ステップ 5　[Next] をクリックします。

Add Database ウィザードの [Define new database connection] ページが表示されます。

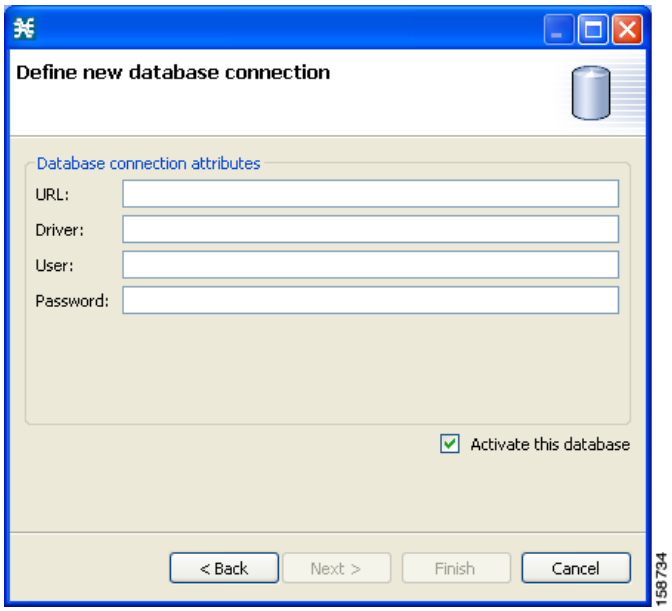
- ステップ 4 で [Simple] を選択した場合、[Define new database connection] ページは図 5-27 のようになります。

図 5-27　[Define New Database Connection] : [Simple]



- ステップ 4 で [Advanced] を選択した場合、[Define new database connection] ページは図 5-28 のようになります。

図 5-28　[Define New Database Connection] : [Advanced]



ステップ 6　すべてのフィールドに入力します。

ステップ 7　[Finish] をクリックします。

Add Database ウィザードが閉じます。

データベースの定義が [Preferences] ダイアログボックス内のリストに追加されます。

ステップ 8　他のデータベースについて、ステップ 3 ～ 7 を繰り返します。

ステップ 9　必要に応じて、[Preferences] ダイアログボックスのリストからデータベースを削除します。

ステップ 10　正しいデータベースがアクティブになっていることを確認します。

ステップ 11　[OK] をクリックします。

[Preferences] ダイアログボックスが閉じます。

Network Navigator コンフィギュレーション ファイルの処理

Network Navigator にサイトとデバイスを追加したあと、バックアップのためにこのデータをファイルにエクスポートすることができます。このデータは、Network Navigator 設定を Console にインポートできる他のユーザと共有することも可能です。

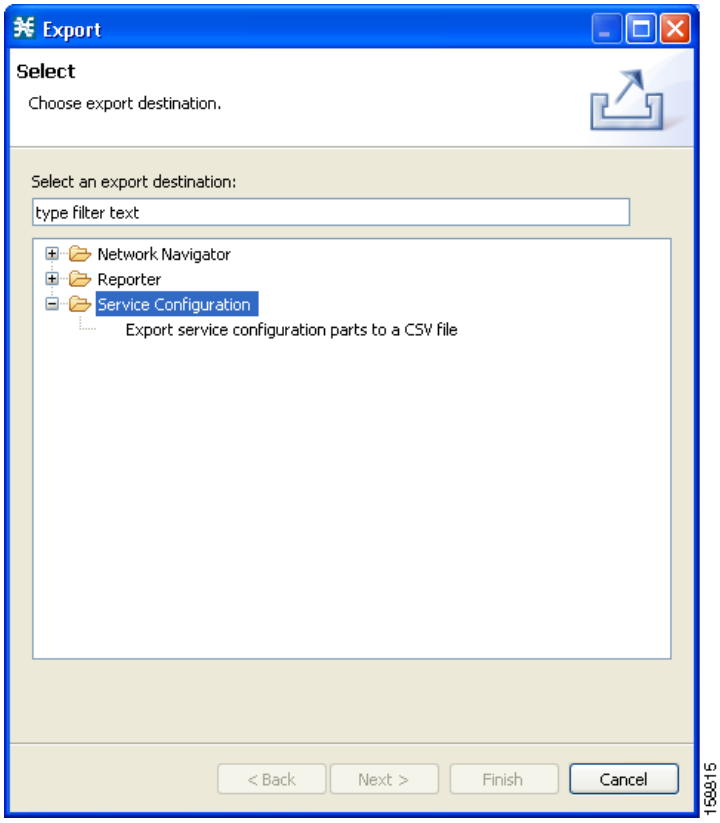
Site Master Password を使用してネットワーク デバイスのパスワードを格納する場合、暗号化形式でパスワードもエクスポートされます。つまり、このデータをインポートする他のユーザは、Site Master Password を入力するだけでデバイスにアクセスできます。

- 「Network Navigator 設定のエクスポート方法」（P.5-32）
- 「Network Navigator 設定のインポート方法」（P.5-34）

Network Navigator 設定のエクスポート方法

ステップ 1　Console のメイン メニューで、[File] > [Export] の順に選択します。
[Export] ダイアログボックスが表示されます（図 5-29）。

図 5-29　[Export]

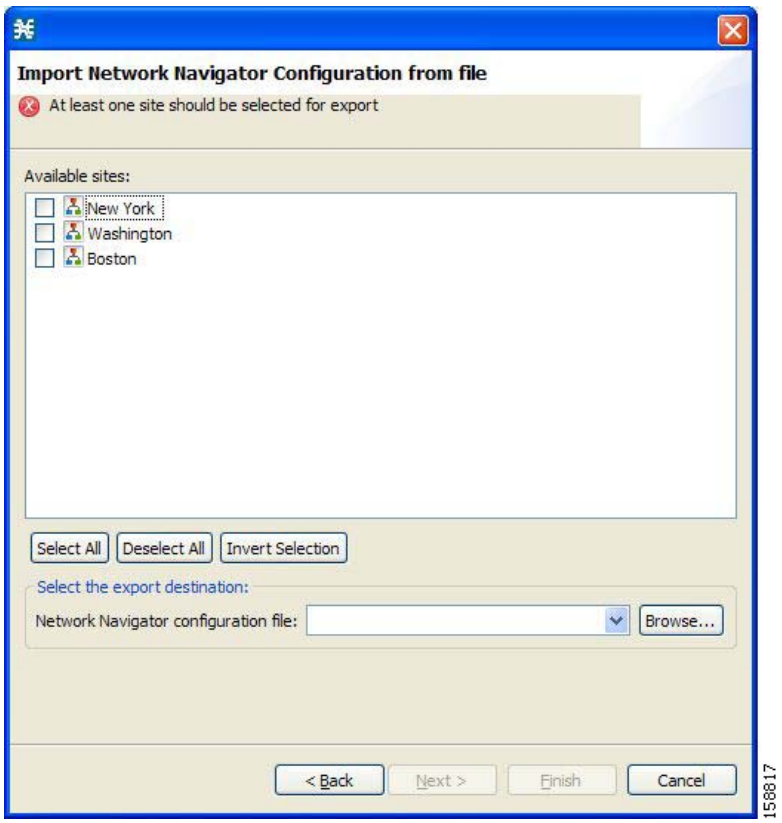


ステップ 2　エクスポート宛先リストから、[Network Navigator Configuration to a file] を選択します。

ステップ 3　[Next] をクリックします。

[Export Network Navigator Configuration to a file] ダイアログボックスが表示されます（図 5-30）。

図 5-30　[Import Network Navigator Configuration from File]



使用可能なサイトのペインに、設定内にあるすべてのサイトが表示されます。

ステップ 4　チェックボックスと選択ボタンを使用してエクスポートするサイトを選択します。

ステップ 5　[Select the export destination] 領域で [Browse] をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 6　コンフィギュレーション ファイルを保存するフォルダをブラウズします。

ステップ 7　[File name] フィールドで、新規ファイル名を入力するか、既存の site_xml ファイルを選択します。

ステップ 8　[Open] をクリックしてファイルを選択します。

（注）　ファイルが存在する場合、上書きされます。

[Open] ダイアログボックスが閉じます。

ステップ 9　[Finish] をクリックします。

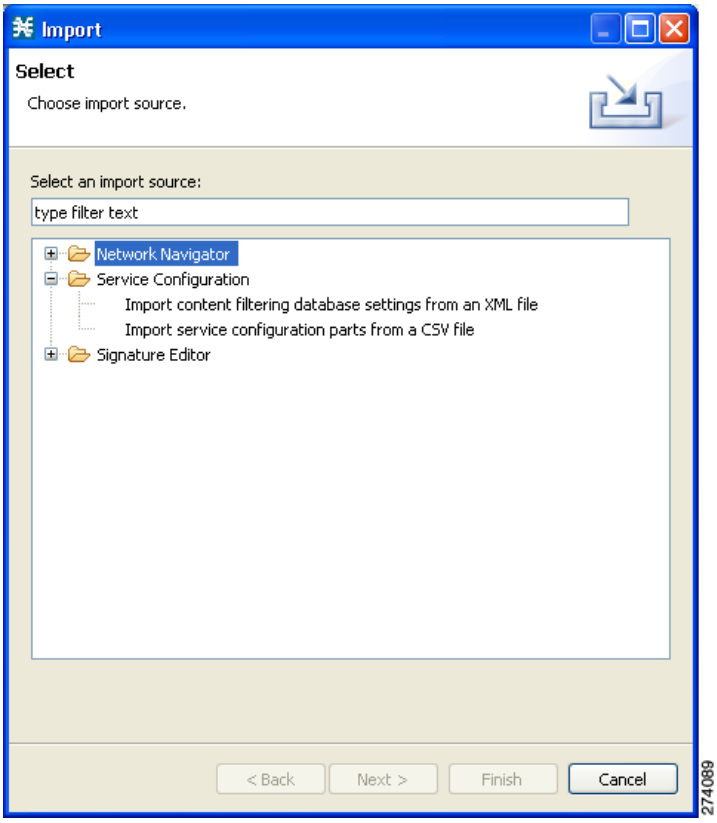
[Export Network Navigator Configuration] ダイアログボックスが閉じます。

設定がファイルに保存されます。

Network Navigator 設定のインポート方法

ステップ 1　Console のメイン メニューで、[File] > [Import] の順に選択します。
[Import] ダイアログボックスが表示されます（図 5-31）。

図 5-31　[Import]

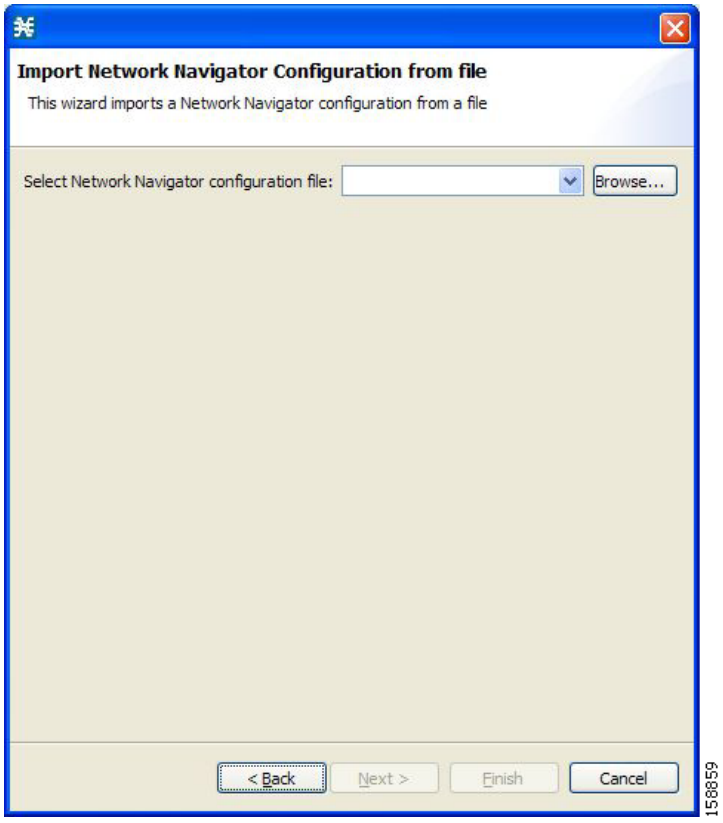


ステップ 2　インポート元リストから、[Network Navigator Configuration from file] を選択します。

ステップ 3　[Next] をクリックします。

[Import Network Navigator Configuration from file] ダイアログボックスが表示されます（図 5-32）。

図 5-32　[Import Network Navigator Configuration from File]



ステップ 4　[Browse] をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 5　インポートするファイルを含むフォルダをブラウズして、site_xml ファイルを選択します。

ステップ 6　[Open] をクリックしてファイルを選択します。

[Open] ダイアログボックスが閉じます。

ステップ 7　[Finish] をクリックします。

[Import Network Navigator Configuration] ダイアログボックスが閉じます。

設定がファイルからインポートされます。

ネットワーク設定要件

ファイアウォール/NAT 要件

表 5-1 は、Network Navigator が正しく動作するために必要なファイアウォール/NAT のオープン ポート設定の一覧です。

この表にリストされたポートはデフォルト値です。デバイスのポートを変更する場合は、それに応じてファイアウォール/NAT 設定を修正する必要があります（別の PRPC ポートに接続するよう Console の設定を変更する方法は、次のセクションで説明します）。

表 5-1　必要なファイアウォール/NAT 設定値

送信元	宛先	説明
ワークステーション	SCE ポート 14374/TCP	PRPC：すべての SCE 操作に必要
SCE	ワークステーション ポート 21/TCP	FTP：次の SCE 操作に必要 • OS のインストール • テクニカル サポート情報ファイルの生成
SCE	ワークステーション ポート 21000/TCP ～ 21010/TCP	FTP：ポート 21/TCP の代わりに、ポート 21/TCP がすでにワークステーション上の別のアプリケーションで使用されている場合に必要
ワークステーション	SM ポート 14374/TCP	PRPC：すべての SM 操作に必要
ワークステーション	CM ポート 14375/TCP	PRPC：CM オンライン ステータスの操作および CM 認証に必要

SCA Reporter には、データベースへの接続用追加要件が存在することもあります。詳細については、『*Cisco Service Control Application Reporter User Guide*』を参照してください。

ユーザ認証

SCE プラットフォーム、CM、または SM との PRPC 接続が行われる際にユーザ認証が実行されます。認証を成功させるには、PRPC サーバが宛先で実行されていること、またサーバのユーザのユーザ名とパスワードを把握していることが必要です。

（注） デバイス（SM/CM/SCE）の PRPC サーバ ポートを変更する場合、*engage.ini* コンフィギュレーション ファイルに次の行を追加する必要があります。

```
<IP address of device>.rpc.port=<port number>
```

例：

```
10.56.216.37.rpc.port=222
```

使用するポートごと（デフォルト以外）にこの行を追加してください。

engage.ini ファイルは
Program files¥Cisco SCA¥SCA BB Console 3.6.0¥plugins¥policy.contribution_3.6.0¥config¥ フォルダにあります。

ユーザ名とパスワードは、SCE プラットフォームのユーザ/パスワード メカニズム、または SM および CM のコマンドライン ユーティリティを使用して設定します。

ユーザ定義の詳細については、次を参照してください。

- SCE :『*Cisco SCE8000 10GBE Software Configuration Guide* 』の「Configuring the Management Interface and Security」にある「TACACS+ Authentication, Authorization, and Accounting」または『*Cisco SCE8000 GBE Software Configuration Guide*』の「Configuring the Management Interface and Security」にある「TACACS+ Authentication, Authorization, and Accounting」
- CM :『*Cisco Service Control Management Suite Collection Manager User Guide*』の「Managing the Collection Manager」にある「Managing Users 」
- SM :『*Cisco Service Control Management Suite Subscriber Manager User Guide*』の付録「Command-Line Utilities」にある「Information About the p3rpc Utility 」

（注）　デバイスの実際の IP アドレス以外の CM/SM/SCE IP アドレスに対しては、SCA BB Console からの PRPC 認証はサポートされません。これは、NATing ルータまたはファイアウォールの内部インターフェイス上に CM/SM/SCE がある場合は特に重要です。
回避策：

SCA BB Console に CM/SM/SCE の実際の IP アドレスが設定されるようにネットワークを再設計する。次のセクションで説明するように、SCE/CM/SM/SCE での PRPC 認証をディセーブルにする。

PRPC 認証の無効化

SCE プラットフォームでの PRPC 認証の無効化方法

ステップ 1　CLI を使用して PRPC をディセーブルにします。

次の CLI をコンフィギュレーション モードで実行します。

```
ip rpc-adapter security-level none
```

CM での PRPC 認証の無効化方法

ステップ 1　CM コンフィギュレーション ファイル を編集します。

cm/um/config/p3cm.cfg コンフィギュレーション ファイルを次のように編集します。

```
[RPC.Server]
security_level=none
```

ステップ 2　CM プロセスをリロードします。

SM での PRPC 認証の無効化方法

ステップ 1　SM コンフィギュレーション ファイルを編集します。

~pcube/sm/server/root/config/p3sm.cfg コンフィギュレーション ファイルを次のように編集します。

```
[RPC.Server]
security_level=none
```

ステップ 2　コンフィギュレーションをロードします。

次の CLU を実行します。

```
p3sm --load-config
```

CHAPTER 6

Service Configuration Editor の使用方法

はじめに

Service Control Engine（SCE）プラットフォームがトラフィックを処理するように設定するには、サービス コンフィギュレーションを定義し、それをプラットフォームに適用する必要があります。サービス コンフィギュレーションの作成、定義、管理には、Service Configuration Editor ツールを使用します。

ここでは、Service Configuration Editor ツールの使用法について説明します。

サービス コンフィギュレーション

*サービス コンフィギュレーション*は、SCE プラットフォームでのネットワーク トラフィックの分析方法、トラフィックに適用される規則、これらの規則を適用するために SCE プラットフォームが実行しなければならないアクションを定義するデータ構造です。

サービス コンフィギュレーションは、次に示す 2 つの主要要素で構成されます。

- サービス：トランザクションが分類されるカテゴリを定義します。
- パッケージ：さまざまなサービスからのトランザクション時に SCE プラットフォームがどのように動作するかを定義します。

サービス コンフィギュレーションは、PQB ファイルとして保存されます。

サービス コンフィギュレーションの管理

ここでは、次の操作について説明します。

- サービス コンフィギュレーションの管理
- サービス コンフィギュレーション データのエクスポートおよびインポート
- SCE プラットフォームへのサービス コンフィギュレーションの適用およびその取得

Service Configuration Editor ツールの開き方

Service Configuration Editor ツールを開いたり、このツールに切り替えたときに、開いているサービス コンフィギュレーションがない場合は、[No Service Configuration Is Open] ダイアログボックスが表示されます（図 6-1 を参照）。

図 6-1　[No Service Configuration Is Open]

- 新しいサービス コンフィギュレーションを作成する場合（「新規サービス コンフィギュレーションの追加方法」（P.6-2）を参照）は、[Yes] をクリックします。
- 既存のサービス コンフィギュレーションを開く場合（「既存のサービス コンフィギュレーションの開き方」（P.6-4）を参照）は、[No] をクリックします。

[Configuration] オプションがメイン メニューに含まれるのは、サービス コンフィギュレーションが 1 つ以上開いている場合だけです。

多くのサービス コンフィギュレーションを同時に開くことができます。それぞれが独自の画面に表示され、画面をクリックすると、その画面のサービス コンフィギュレーションがアクティブになります。

サービス コンフィギュレーションに未保存の変更があると、その画面の名前の前にアスタリスクが追加されます。

新規サービス コンフィギュレーションの追加方法

必要な場合にいつでも新規サービス コンフィギュレーションを追加することができます。

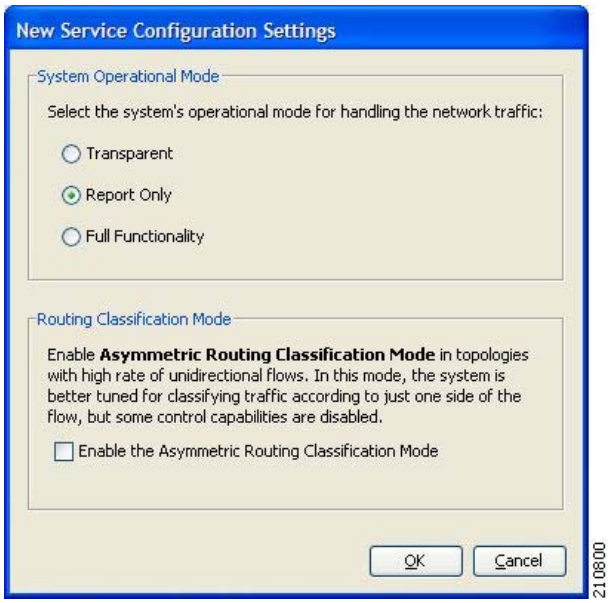
（注） 最初の新規サービス コンフィギュレーションを保存するまで、次のサービス コンフィギュレーションを追加できません。

新規サービス コンフィギュレーション ウィンドウが開くときに、Cisco Service Control Application for Broadband（SCA BB）から提供されるデフォルトのサービス コンフィギュレーションが含まれます。これには、デフォルトのサービス規則を含むデフォルトのパッケージが含まれています。

ステップ 1　Console のツールバーで、（[New Service Configuration]）をクリックします。

[New Service Configuration Settings] ダイアログボックスが表示されます（図 6-2）。

図 6-2　[New Service Configuration Settings]



ステップ 2　そのサービス コンフィギュレーションの動作モードを選択します。

ステップ 3　システムのルーティング分類モードを選択します。

非対称ルーティング分類モードを選択すると、単方向フローの比率が高いトポロジで、より正確なプロトコル分類を行うことができます。このモードがイネーブルになっている場合、一部の分類、レポート、制御の機能はサポートされません（「非対称ルーティング分類モード」（P.10-44）を参照）。

ステップ 4　[OK] をクリックします。

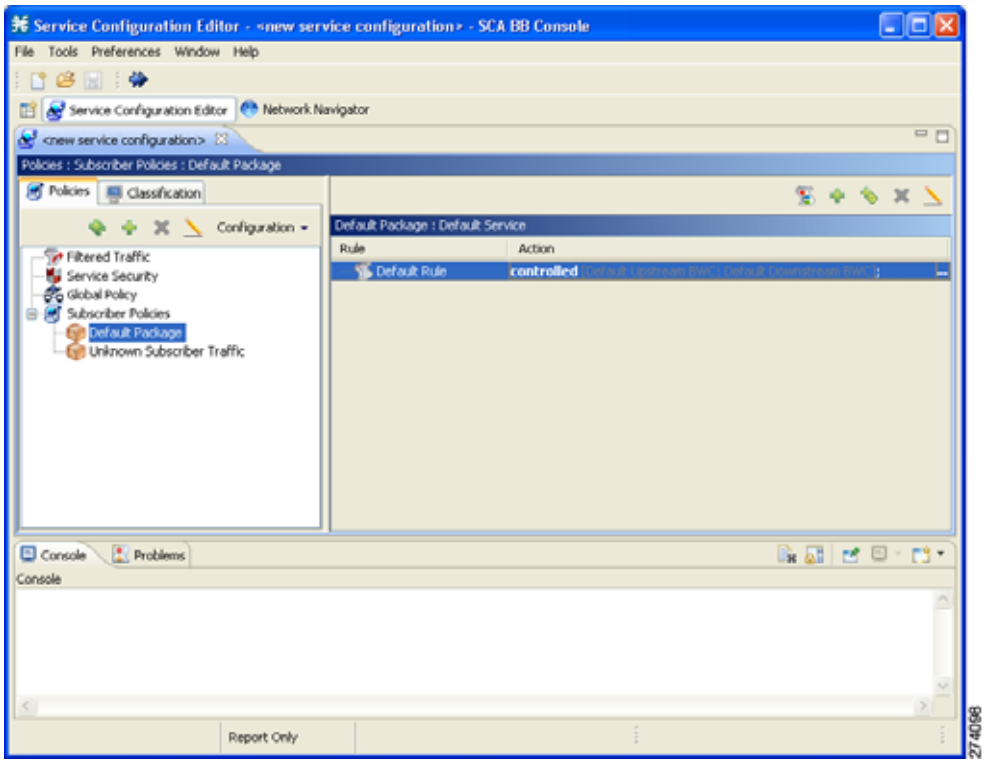
デフォルト DSS ファイルを設定した場合（「デフォルト DSS ファイル」（P.7-43）を参照）は、[Default Signature] メッセージが表示されます（図 6-3）。

図 6-3　[Default Signature]

- （推奨）[Yes] をクリックしてデフォルトの DSS ファイルをインポートします。
- デフォルト DSS ファイルをインポートせずに処理を続行するには、[No] をクリックします。

新規サービス コンフィギュレーションが [Console] ウィンドウに追加されて、[Network Traffic] タブに表示され、アクティブなサービス コンフィギュレーションとなります（図 6-4）。

図 6-4　Service Configuration Editor



既存のサービス コンフィギュレーションの開き方

表示や編集、または SCE プラットフォームに適用するために、保存されているサービス コンフィギュレーションを開くことができます。

サービス コンフィギュレーションには、拡張 PQB ファイルがあります。

ステップ 1　Console のツールバーで、（[Open A Service Configuration File]）をクリックします。Console のメイン メニューで、[File] > [Open Service Configuration] の順に選択します。

[Open] ダイアログボックスが表示されます。

ステップ 2　サービス コンフィギュレーション ファイルをブラウズします。

ステップ 3　[Open] をクリックします。

[Open] ダイアログボックスが閉じます。

デフォルトの DSS ファイルがサービス コンフィギュレーションにインポートされていない場合、[Default Signature] メッセージが表示されます（図 6-5）。

図 6-5　[Default Signature]

デフォルトの DSS ファイルがサービス コンフィギュレーションにインポートされていない場合、[Default Signature] メッセージが表示されます。

- （推奨）[Yes] をクリックしてデフォルトの DSS ファイルをインポートします。
- デフォルト DSS ファイルをインポートせずに処理を続行するには、[No] をクリックします。

サービス コンフィギュレーションが Console にロードされます。

- このサービス コンフィギュレーションがアクティブなサービス コンフィギュレーションになります。
- このサービス コンフィギュレーション名が [Console] ウィンドウのタイトルに含まれます。

現在のサービス コンフィギュレーションの保存方法

アクティブなサービス コンフィギュレーションを保存することができます。

- 「サービス コンフィギュレーション ファイルへの現在のサービス コンフィギュレーションの保存」（P.6-5）
- 「ロード元ファイルへの現在のサービス コンフィギュレーションの保存方法」（P.6-6）

サービス コンフィギュレーション ファイルへの現在のサービス コンフィギュレーションの保存

ステップ 1　Console のメイン メニューで、[File] > [Save As] の順に選択します。

[Save As] ダイアログボックスが表示されます。

- 要求された場合は、パスワードを入力します。

ステップ 2　サービス コンフィギュレーションを含むファイルを保存するフォルダをブラウズします。

ステップ 3　[File name] フィールドで、新規ファイル名を入力するか、既存の PQB ファイルを選択します。

ステップ 4　[Save] をクリックします。

サービス コンフィギュレーション ファイルが選択されたファイルに保存されます。ファイルが存在する場合、上書きされます。

処理中に [Saving Service Configuration File] メッセージが表示されます。

ロード元ファイルへの現在のサービス コンフィギュレーションの保存方法

ステップ 1　Console のツールバーで、（[Save]）をクリックします。

現在のサービス コンフィギュレーションが PQB ファイルからロードされていない場合（つまり、新規の場合や、SCE プラットフォームから取得した場合）、前の手順で [Save As] ダイアログボックスが開きます。

サービス コンフィギュレーションの閉じ方

ステップ 1　サービス コンフィギュレーション画面で、（[Close]）をクリックします。

- 未保存の変更がない場合、サービス コンフィギュレーション画面が閉じます。
- 未保存の変更がある場合、[Save Resource] メッセージが表示されます（図 6-6）。

図 6-6　[Save Resource]

- [Yes] をクリックします。
  - 既存の編集済みサービス コンフィギュレーションがある場合、変更が保存されてサービス コンフィギュレーション画面が閉じます。
  - 新規サービス コンフィギュレーションの場合は、[Save As] ダイアログボックスが開きます。

  サービス コンフィギュレーション名を入力し、[Save] をクリックします。

  [Save As] ダイアログボックスが閉じて変更が保存され、サービス コンフィギュレーション画面が閉じます。

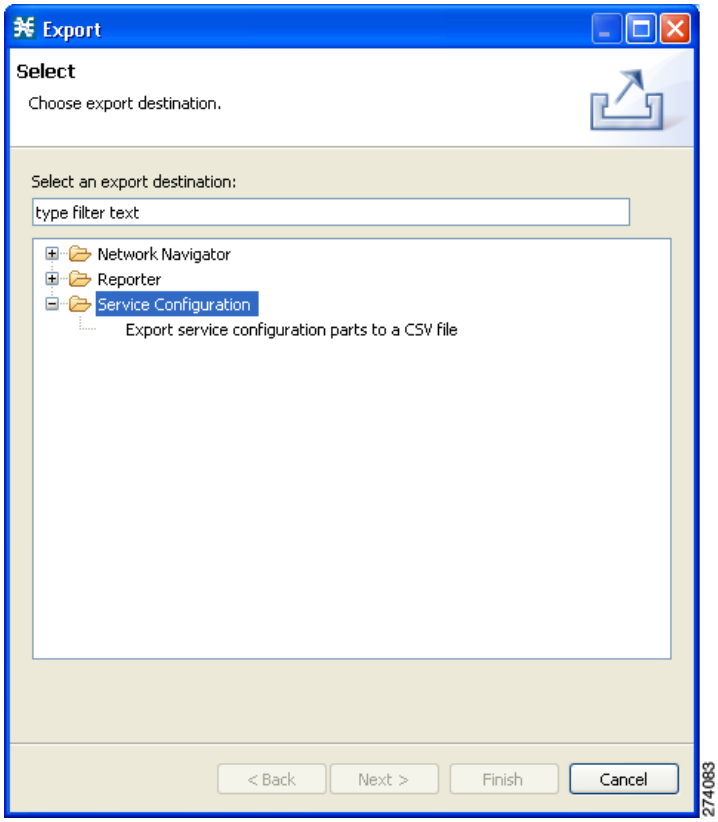
サービス コンフィギュレーション データのエクスポート方法

サービス コンフィギュレーション データを現在のサービス コンフィギュレーションから CSV ファイルにエクスポートすることができます。CSV ファイル形式については、『*Cisco Service Control Application Suit for Broadband Reference Guide*』の「CSV File Formats」の章を参照してください。

各タイプのサービス コンフィギュレーション要素は、個別のファイルにエクスポートされます。

ステップ 1　Console のメイン メニューで、[File] > [Export] の順に選択します。
[Export] ダイアログボックスが表示されます（図 6-7）。

図 6-7　[Export]

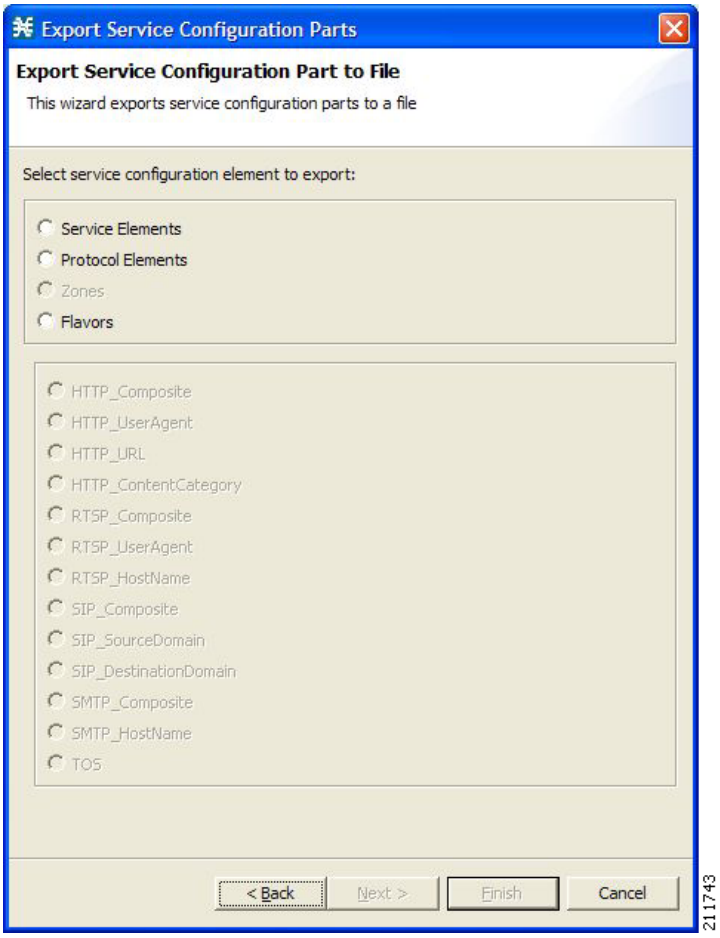


ステップ 2　エクスポート宛先リストから [Export service configuration parts to CSV file] を選択します。

ステップ 3　[Next] をクリックします。

[Export Service Configuration Parts] ダイアログボックスが表示されます（図 6-8）。

図 6-8　　[Export Service Configuration Parts to File]



ステップ 4　[Select service configuration element to export] のオプション ボタンをいずれか 1 つ選択します。

次のオプション ボタンがあります。

- [Service Elements]
- [Protocol Element]
- [Zone]
- [Flavors]

[Flavors] を選択すると、ダイアログボックス内にある [flavor] 領域のフレーバがイネーブルになります。

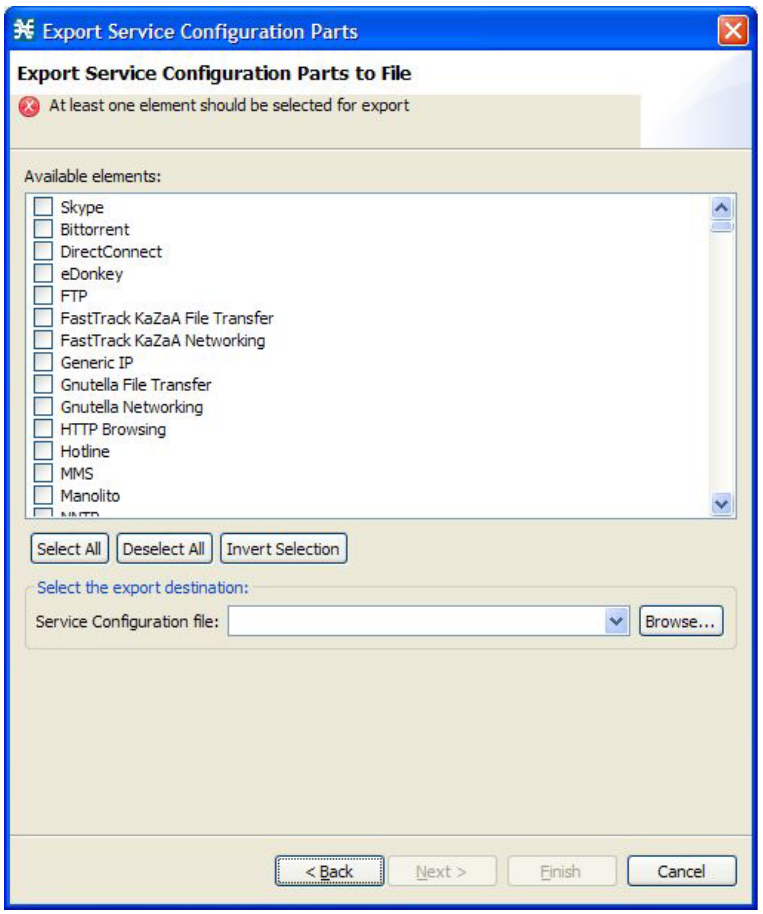
（注）　このサービス コンフィギュレーション内で flavor タイプが定義されているフレーバだけがイネーブルになります。

ステップ 5　[Flavors] を選択した場合は、[flavor type] のオプション ボタンをいずれか 1 つ選択します。

ステップ 6　[Next] をクリックします。

[Export Service Configuration Parts] ダイアログボックスの第 2 画面が開きます（図 6-9）。

図 6-9　[Export Service Configuration Parts to File]



使用可能な要素のペインに、選択されたタイプのサービス コンフィギュレーションにあるすべての要素が表示されます。

ステップ 7　チェックボックスと選択ボタンを使用して、エクスポートする要素を選択します。

ステップ 8　[Select the export destination] 領域で [Browse] をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 9　そのサービス コンフィギュレーション要素を含むファイルを保存するフォルダをブラウズします。

ステップ 10　[File name] フィールドで、新規ファイル名を入力するか、既存の CSV ファイルを選択します。

ステップ 11　[Open] をクリックしてファイルを選択します。

ファイルが存在する場合、上書きされます。

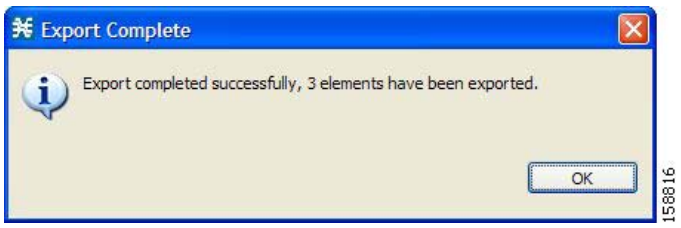
[Open] ダイアログボックスが閉じます。

ステップ 12　[Finish] をクリックします。

選択されたサービス コンフィギュレーション要素がファイルにエクスポートされます。

[Export Complete] メッセージが表示されます（図 6-10）。

図 6-10　[Export Complete]



ステップ 13　[OK] をクリックします。

[Export Service Configuration Parts] ダイアログボックスが閉じます。

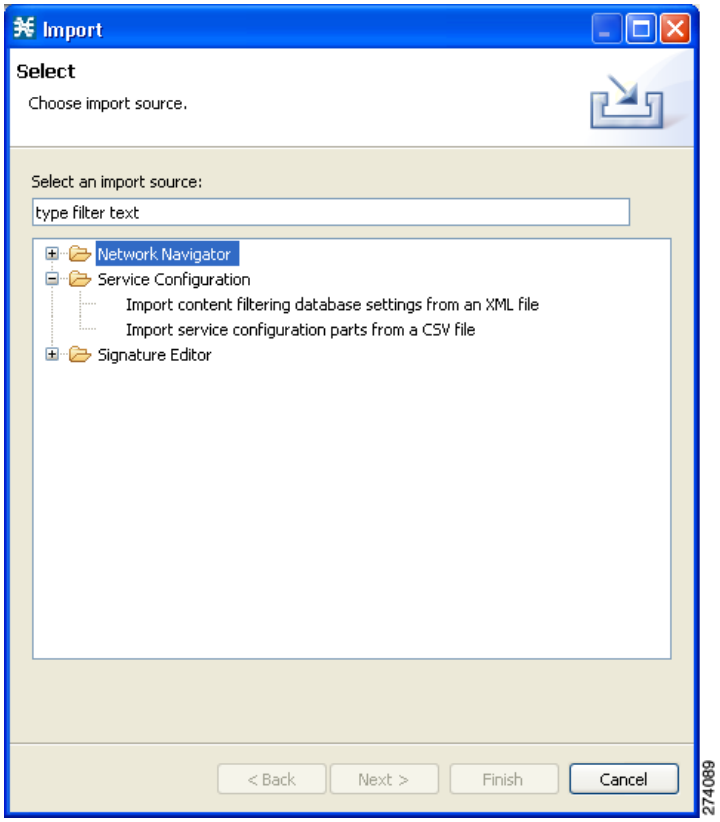
サービス コンフィギュレーション データのインポート方法

サービス コンフィギュレーション データを CSV ファイルから現在のサービス コンフィギュレーションにインポートすることができます。CSV ファイル形式については、『*Cisco Service Control Application Suit for Broadband Reference Guide*』の「CSV File Formats」の章を参照してください。

各タイプのサービス コンフィギュレーション要素は、個別のファイルにインポートされます。

ステップ 1　Console のメイン メニューで、[File] > [Import] の順に選択します。
[Import] ダイアログボックスが表示されます（図 6-11）。

図 6-11　[Import]

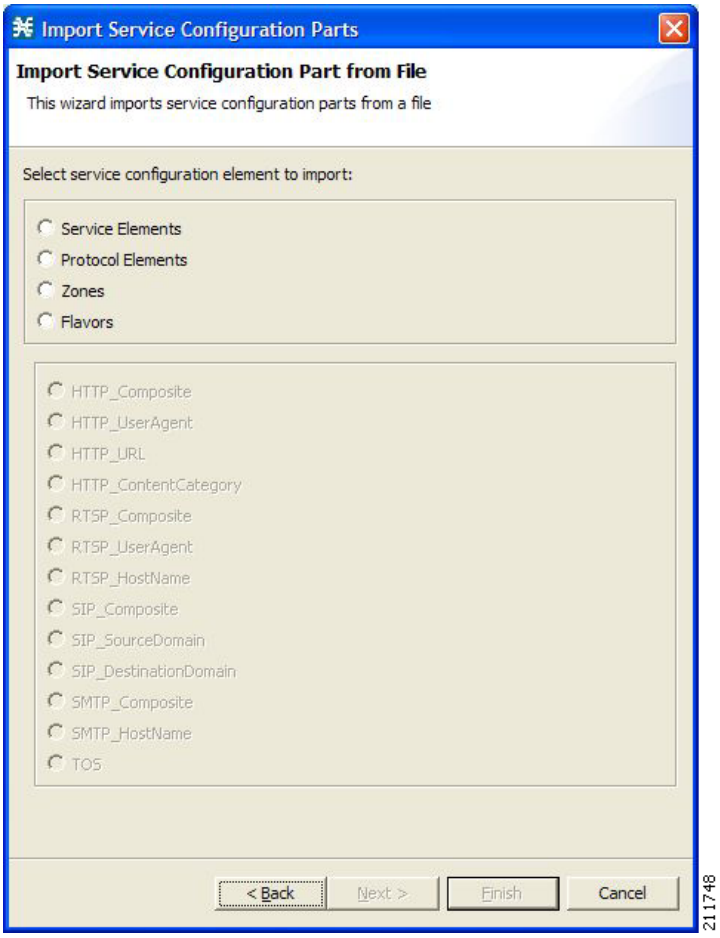


ステップ 2　[Select an import source] のリストから、[Import service configuration parts from CSV file] を選択します。

ステップ 3　[Next] をクリックします。

[Import Service Configuration Parts] ダイアログボックスが表示されます（図 6-12）。

図 6-12　[Import Service Configuration Parts from File]



ステップ 4　[Select service configuration element to import] のオプション ボタンをいずれか 1 つ選択します。

次のオプション ボタンがあります。

- [Service Elements]
- [Protocol Element]
- [Zone]
- [Flavors]

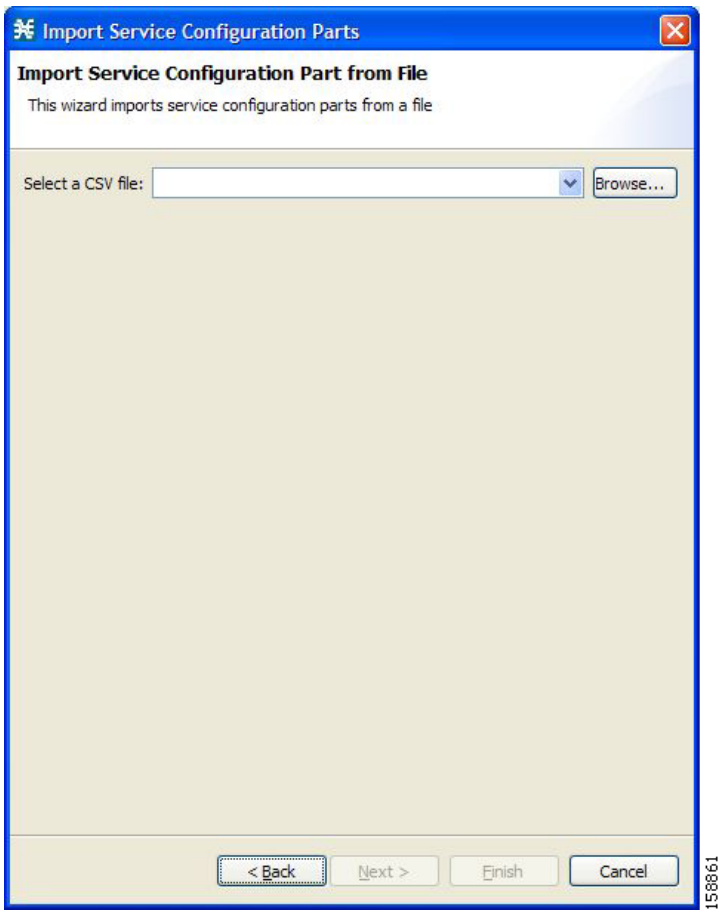
[Flavors] を選択すると、ダイアログボックス内にある [flavor] 領域のフレーバがイネーブルになります。

ステップ 5　[Flavors] を選択した場合は、[flavor type] のオプション ボタンをいずれか 1 つ選択します。

ステップ 6　[Next] をクリックします。

[Import Service Configuration Parts] ダイアログボックスの第 2 画面が開きます（図 6-13）。

図 6-13　[Import Service Configuration Parts from File]



ステップ 7　[Browse] をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 8　インポートするファイルを含むフォルダをブラウズして、CSV ファイルを選択します。

ステップ 9　[Open] をクリックしてファイルを選択します。

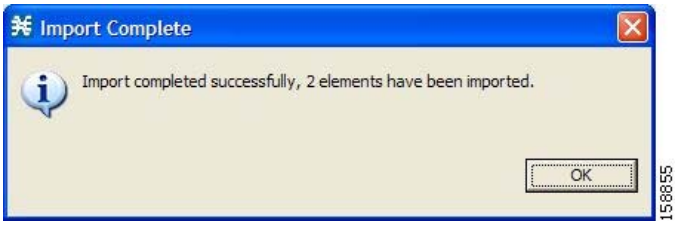
[Open] ダイアログボックスが閉じます。

ステップ 10　[Finish] をクリックします。

コンフィギュレーション要素がファイルからインポートされます。

[Import Complete] メッセージが表示されます（図 6-14）。

図 6-14　[Import Complete]



ステップ 11　[OK] をクリックします。

[Import Service Configuration Parts] ダイアログボックスが表示されます。

サービス コンフィギュレーションの適用および取得

新規または編集済みのサービス コンフィギュレーションを有効にするには、SCE プラットフォームに適用する必要があります。適用するまで、SCE プラットフォームには引き続き前のサービス コンフィギュレーションが適用されます。

Service Configuration Editor を使用してサービス コンフィギュレーションを SCE プラットフォームに適用することはできますが、サービス コンフィギュレーションを取得することはできません。

次の機能を使用すると、サービス コンフィギュレーションの適用または取得が可能です。

- 「Network Navigator ツール」（P.5-2）
- SCA BB サービス コンフィギュレーション ユーティリティ、**servconf**（「SCA BB サービス コンフィギュレーション ユーティリティ」（P.13-1）を参照）
- 「現在のサービス コンフィギュレーションの検証方法」（P.6-14）
- 「SCE プラットフォームへのサービス コンフィギュレーションの適用方法」（P.6-15）

現在のサービス コンフィギュレーションの検証方法

現在表示されている新しいサービス コンフィギュレーションまたはアップデートされたサービス コンフィギュレーションを検証するには、[Validate] オプションを使用します。検証プロセスは、サービス コンフィギュレーション全体の一貫性を調べ、サービス コンフィギュレーション内の問題点を識別するものです。

[Apply Service Configuration to SCE device] を選択すると検証プロセスが自動的に実行されます。手順でエラーが検出されたり、現在のサービス コンフィギュレーションに関連する警告が発行された場合だけ、[Validation Results] ダイアログボックスが表示されます。

ステップ 1　Console のメイン メニューで、[File] > [Validate] の順に選択します。

[Validation Results] ダイアログボックスが表示されます（図 6-15 または図 6-16）。

図 6-15　[Validation Results] : サービス コンフィギュレーションが有効な場合

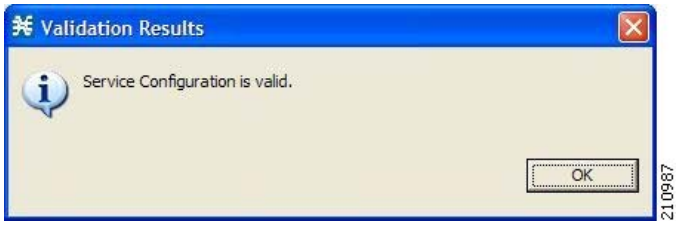
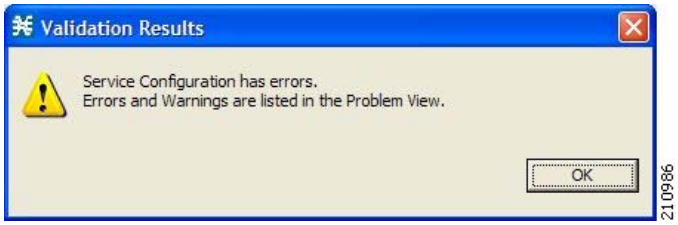


図 6-16　[Validation Results] : サービス コンフィギュレーションにエラーがある場合



サービス コンフィギュレーションに何か問題がある場合は [Problems] 画面に表示されます。

ステップ 2　[OK] をクリックします。

[Service Configuration Validation] ダイアログボックスが閉じます。

SCE プラットフォームへのサービス コンフィギュレーションの適用方法

[Apply Service Configuration to SCE Devices] をクリックすると、現在のサービス コンフィギュレーションに対して検証プロセスが自動的に実行されます。

（注）　サービス コンフィギュレーションを手動で検証するには、[Validate] メニュー コマンドを使用します。

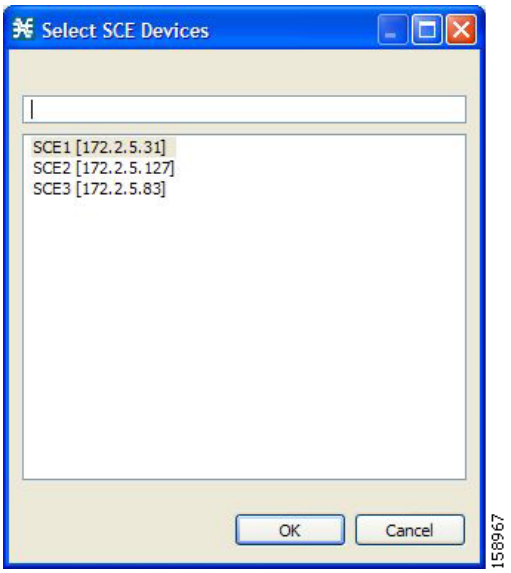
注意　悪質なトラフィックの異常ベース検出がイネーブルの場合、Service Control Engine（SCE）プラットフォームで設定されたものの、インターフェイス、アクセス マップ、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コミュニティ ストリングなどのいずれにも適用されていない Access Control List（ACL; アクセス コントロール リスト）は、サービス コンフィギュレーションがプラットフォームに適用されると削除される場合があります。

回避策
悪質なトラフィックの異常ベース検出をディセーブルにする。
[Network Traffic] タブで [Service Security] を選択する。
サービス セキュリティ ダッシュボードで [Enable anomaly detection] チェックボックスをオフにする。

ステップ 1　Console のツールバーで、（[Apply Service Configuration to SCE Devices]）をクリックします。

[Select SCE Devices] ダイアログボックスが表示されます（図 6-17）。

図 6-17　[Select SCE Devices]



Network Navigator に定義されたすべての SCE プラットフォームがダイアログボックスに一覧表示されます。

ステップ 2　リストから、1 つまたは複数の SCE プラットフォームを選択します。

ステップ 3　[OK] をクリックします。

選択されたプラットフォームごとに [Password Management] ダイアログボックスが表示されます。

ステップ 4　適切なパスワードを入力します

ステップ 5　[Apply] をクリックします。

[Password Management] ダイアログボックスが閉じます。

選択された SCE プラットフォームごとに [Applying service configuration to SCE] 経過表示バーが表示されます。

そのサービス コンフィギュレーションに対して検証プロセスが実行されます。

- 問題が発生し、警告またはエラーが表示されて検証プロセスが終了した場合は、[Validation Results] ダイアログボックスが表示されます。[OK] をクリックし、[Problems] 画面に表示された情報に基づいてサービス コンフィギュレーションを修正し、このステップを繰り返します。
- 検証プロセスが正常に実行されれば、選択された SCE プラットフォームにそのサービス コンフィギュレーションが適用されます。

CHAPTER 7

Service Configuration Editor の使用方法：トラフィックの分類

はじめに

Cisco Service Control Application for Broadband（SCA BB）サービス コンフィギュレーションを作成するには、まず、トラフィックの分類を行います。トラフィックはサービスに従って分類されます。

プロバイダーがサブスクライバに提供する商業サービスについて、対応するサービスは Cisco Service Control ソリューションで定義されています。このサービスを使用して、トラフィックの分類と識別、トラフィックの使用状況に基づくレポート、トラフィックの制御が行えます。

ここでは、サービス、その要素とサブ要素の使用法について説明します。

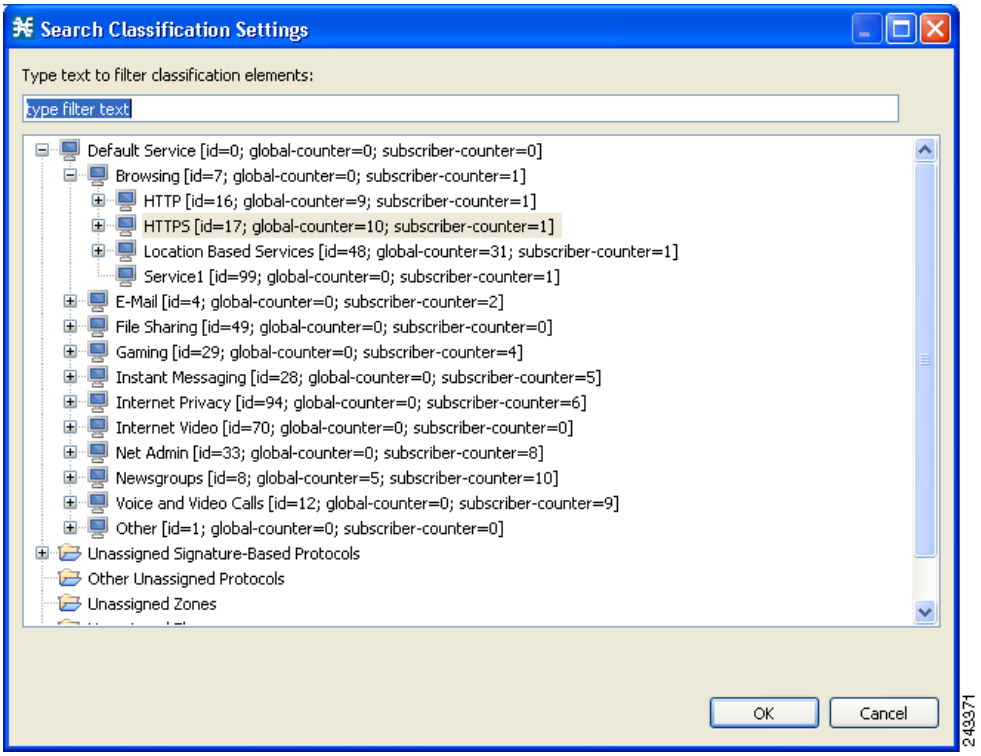
トラフィック分類設定の検索方法

分類の詳細は、名前あるいはサービス、プロトコル、ポート番号、カウンタの割り当てなどの番号 ID で検索できます。サービスに割り当てられていないプロトコルまたはシグニチャも検索できます。

ステップ 1　[Classification] タブで  （[Search Classification Settings]）をクリックします。

[Search Classification Settings] ダイアログボックスが表示されます（図 7-1）。

図 7-1　[Search Classification Settings]



ステップ 2　検索するテキストを入力します。

（注）　検索では、次のワイルドカードを含めることができます。

- ?：任意の文字
- •*：任意の文字列

ダイアログボックスに検索結果が表示されます。

ステップ 3　項目をダブルクリックして、その項目の編集画面に移動します。たとえば、プロトコルをダブルクリックすると、選択したプロトコル上でプロトコル ダイアログボックスが開きます。

サービスの管理

サービスは、制御されたトラフィックを分類するために使用します。

サービスは 1 つまたは複数のサービス要素で構成され、それぞれのサービス要素には固有のネットワーク トラフィック トランザクション タイプがマッピングされます。

トラフィックは、次の一部またはすべてに基づいて分類されます。

- プロトコル：トランザクションによって使用され、Service Control Engine（SCE）プラットフォームで識別されるプロトコル。
- 開始側：トランザクションを開始した側。
- ゾーン：トランザクションのネットワーク側ホストの IP アドレス。
- フレーバ：トランザクションの特定のレイヤ 7 プロパティ。たとえば、トランザクションのネットワーク側ホストのホスト名など。

サービス コンフィギュレーションには、最大で 500 のサービスと 10,000 のサービス要素を設定できます。サービス コンフィギュレーション内の各サービス要素は、一意でなければなりません。

サービス パラメータ

サービスは、次のパラメータで指定されます。

- General パラメータ：
  - [Name]：一意の名前
  - [Description]：（オプション）サービスの説明
- Hierarchy パラメータ：
  - [Parent Service]

    サービス階層の基本となるデフォルト サービスで、親を持ちません。

（注） 親サービスは、複数のサービスが使用カウンタを共有する場合に重要となります（次のパラメータを参照）。

  - [Service Usage Counters]：各サービスの総使用量に関するデータを生成するためにシステムによって使用されます。サービスは、自身の使用状況カウンタと親サービスの使用カウンタを使用できます。

    使用カウンタは、次の要素で構成されます。
  - システムによって割り当てられた名前（サービス名に基づいて作成）

（注） カウンタが複数のサービスに適用されている場合、サービス使用カウンタの名前にアスタリスクが付加されます。

  - 一意のカウンタ インデックス：カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。
- Advanced パラメータ：
  - [Service Index]：システムがサービスを識別するための一意の番号です（サービス名を変更しても SCE プラットフォームの動作には影響しません）。サービス インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

これらのパラメータは新しいサービスの追加時に定義されます（「サービス コンフィギュレーションへのサービスの追加方法」（P.7-4）を参照）。パラメータの修正はいつでもできます（「サービスの編集方法」（P.7-9）を参照）。

サービスの追加と定義

Console のインストレーション時に、サービス数があらかじめ定義されます。サービス コンフィギュレーションには、サービスを追加できます。ただし、1 つのサービス コンフィギュレーションにつき、設定可能なサービスは最大 500（あらかじめ定義されたサービスを含む）です。

新しいサービスの追加および定義を行ったあと、そのサービスにサービス要素を追加できます（「サービス要素の追加方法」（P.7-12）を参照）。

- 「サービス コンフィギュレーションへのサービスの追加方法」（P.7-4）
- 「サービスの階層設定の定義方法」（P.7-5）
- 「サービス インデックスの設定方法」（P.7-7）
- 「サービスの表示方法」（P.7-8）

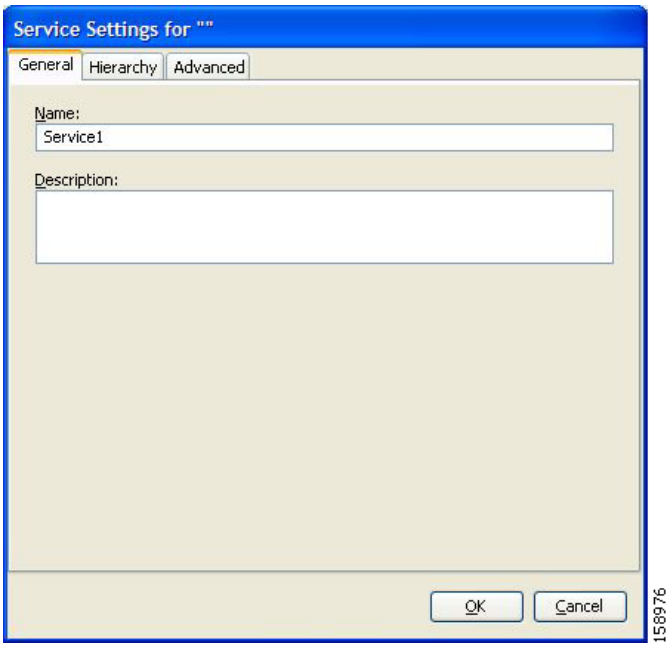
サービス コンフィギュレーションへのサービスの追加方法

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。このサービスは、追加するサービスの親になります。

ステップ 2　左ペインで、  （[Add Service]）をクリックします。

[Service Settings] ダイアログボックスが表示されます（図 7-2）。

図 7-2　[Service Settings]



ステップ 3　[Name] フィールドに、サービスに関連する一意の名前を入力します。

ステップ 4　[Description] フィールドに、サービスに関するわかりやすい説明を入力します。

ステップ 5　このサービス専用の使用カウンタを設定する場合、またはサービスの追加時に選択した親サービスを変更する場合は、「サービスの階層設定の定義方法」（P.7-5）を参照して設定してください。

ステップ 6　（オプション）このサービスのインデックスを指定する場合は、「サービス インデックスの設定方法」（P.7-7）を参照して指定ください。

（注）　新規に作成されたサービスには、空いている番号が自動的に割り当てられます。サービスに特定のインデックス値を割り当てる必要がある場合だけ、この番号を変更します。

ステップ 7　[OK] をクリックします。

[Service Settings] ダイアログボックスが閉じます。

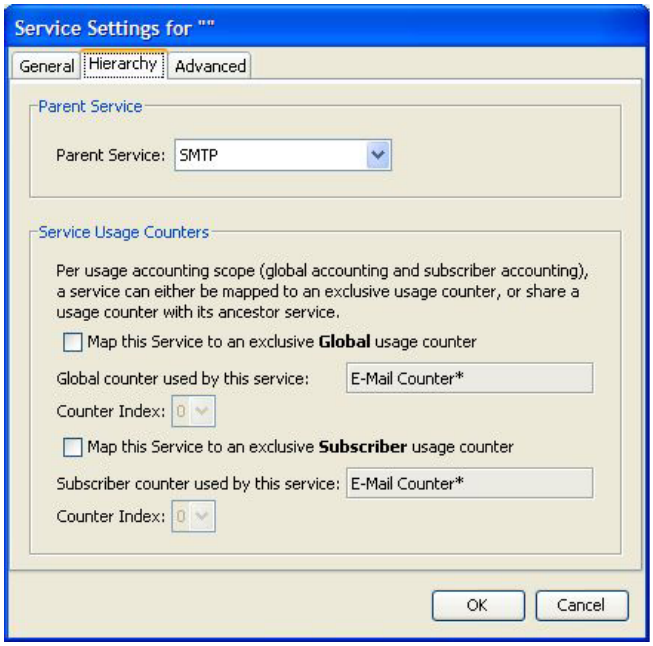
サービスが、階層で選択したサービスの子として、サービス ツリーに追加されます。

サービスの階層設定の定義方法

ステップ 1　[Service Settings] ダイアログボックスで、[Hierarchy] タブをクリックします。

[Hierarchy] タブが開きます（図 7-3）。

図 7-3　[Hierarchy] タブ



ステップ 2　別の親サービスを設定するには、[Parent Service] ドロップダウン リストで目的の親を選択します。

ステップ 3　デフォルトでは、新しいサービスに親のグローバル使用カウンタが使用されます。専用のグローバル使用カウンタを定義するには、[Map this Service to an exclusive Global usage counter] チェックボックスをオンにします。

このサービス フィールドの読み取り専用グローバル カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがイネーブルになります。

（オプション）[Counter Index] ドロップダウン リストでカウンタ インデックスの値を選択します。

（注）　カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

ステップ 4　デフォルトでは、新しいサービスに親のサブスクライバ使用カウンタが使用されます。専用のサブスクライバ使用カウンタを定義するには、[Map this Service to an exclusive Subscriber usage counter] チェックボックスをオンにします。

このサービス フィールドの読み取り専用サブスクライバ カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがイネーブルになります。

（オプション）[Counter Index] ドロップダウン リストでカウンタ インデックスの値を選択します。

（注）　カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

ステップ 5　このサービスのインデックスを指定する場合は、「サービス インデックスの設定方法」（P.7-7）を参照してください。

（注）　新規に作成されたサービスには、空いている番号が自動的に割り当てられます。サービスに特定のインデックス値を割り当てる必要がある場合だけ、この番号を変更します。

ステップ 6　[OK] をクリックします。

[Service Settings] ダイアログボックスが閉じます。

サービスが、[Parent Service] ドロップダウン リストで選択したサービスの子として、サービス ツリーに追加されます。

サービス インデックスの設定方法

ステップ 1　[Service Settings] ダイアログボックスで、[Advanced] タブをクリックします。

[Advanced] タブが開きます（図 7-4）。

図 7-4　[Advanced] タブ

ステップ 2　[Set the Index for this Service] ドロップダウン リストで、サービス インデックスを選択します。

サービス インデックスは、1 ～ 499 の整数とします。0 はデフォルト サービス用に予約されています。

（注）　新規に作成されたサービスには、空いている番号が自動的に割り当てられます。サービスに特定のインデックス値を割り当てる必要がある場合だけ、この番号を変更します。

ステップ 3　[OK] をクリックします。

[Service Settings] ダイアログボックスが閉じます。

サービスが、[Parent Service] ドロップダウン リストで選択したサービスの子として、サービス ツリーに追加されます。

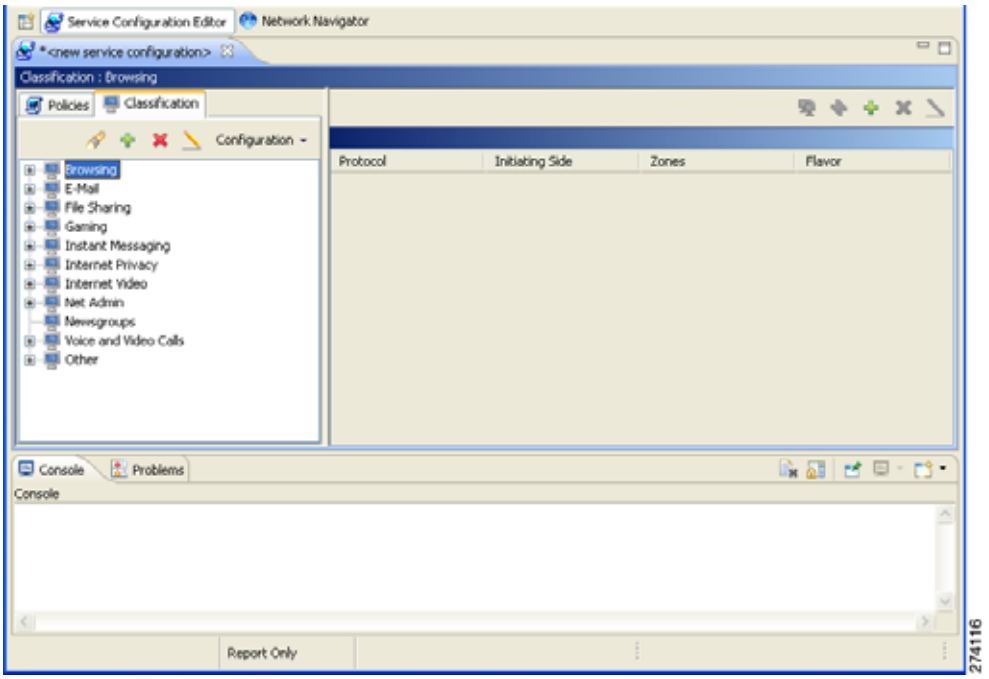
サービスの表示方法

既存のサービスの階層ツリーを表示し、関連するサービス要素を確認できます。

ステップ 1　現在のサービス コンフィギュレーションで、[Classification] タブをクリックします。

[Classification] タブが開きます（図 7-5）。

図 7-5　[Classification] タブ

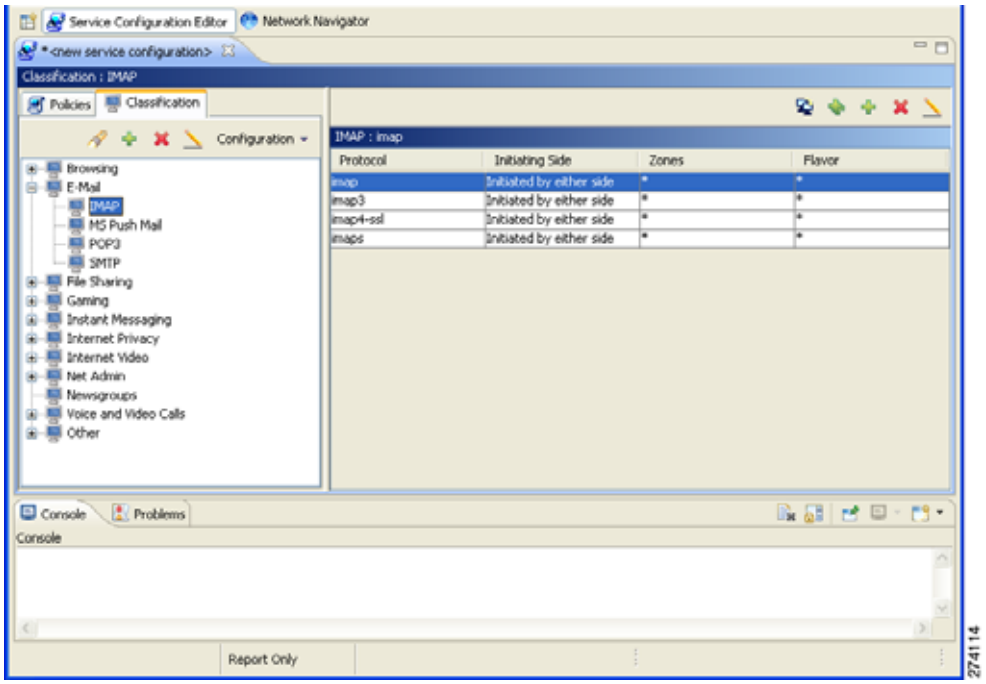


サービス ツリー（左側のペイン）に、サービスのリストが表示されます。

ステップ 2　サービス要素を表示するには、階層内のサービスをクリックします。

右側（サービス要素）のペインに、このサービスに対して定義されたすべてのサービス要素のリストが表示されます（図 7-6）。

図 7-6　　サービス要素



ステップ 3　サービスに関する詳細情報を表示するには、サービス ツリーからサービスを選択して、  （[Edit Service]）をクリックします。

[Service Settings] ダイアログボックスが表示されます。

ステップ 4　[OK] をクリックします。

[Service Settings] ダイアログボックスが閉じます。

サービスの編集方法

サービスのパラメータは、Console でインストールしたものも含めて、修正できます。

サービス要素の追加、変更、または削除を行う場合は、「サービス要素の管理」（P.7-12）を参照してください。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

ステップ 2　左のペインで、  （[Edit Service]）をクリックします。

[Service Settings] ダイアログボックスが表示されます。

ステップ 3　（オプション）サービスに新しい名前を付けます。

[Name] フィールドに新しい名前を入します。

ステップ 4　（オプション）サービスに新しい説明を付けます。

[Description] フィールドに新しい説明を入力します。

ステップ 5　階層設定を変更するには、[Hierarchy] タブをクリックします。

[Hierarchy] タブが開きます。

a. 別の親サービスを設定するには、[Parent Service] ドロップダウン リストで目的のサービスを選択します。

b. グローバル使用カウンタを親サービスと共有するには、[Map this Service to an exclusive Global usage counter] チェックボックスをオフにします。

このサービス フィールドで使用されるグローバル カウンタに、親サービスのカウンタの名前が表示されます。

c. 専用のグローバル使用カウンタを定義するには、[Map this Service to an exclusive Global usage counter] チェックボックスをオンにします。

このサービス フィールドの読み取り専用グローバル カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがイネーブルになります。

（注） カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

d. サブスクライバ使用カウンタを親サービスと共有するには、[Map this Service to an exclusive Subscriber usage counter] チェックボックスをオフにします。

このサービス フィールドで使用されるサブスクライバ カウンタに、親サービスのカウンタの名前が表示されます。

e. 専用のサブスクライバ使用カウンタを定義するには、[Map this Service to an exclusive Subscriber usage counter] チェックボックスをオンにします。

このサービス フィールドの読み取り専用サブスクライバ カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがイネーブルになります。

（注） カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

ステップ 6　サービス インデックスを変更するには、次の手順を実行します。

a. [Service Settings] ダイアログボックスで、[Advanced] タブをクリックします。

[Advanced] タブが開きます。

b. [Set the Index for this Service] ドロップダウン リストで、サービス インデックスを選択します。

サービス インデックスは、1 ～ 499 の整数とします。0 はデフォルト サービス用に予約されています。

（注） サービス インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

ステップ 7　[OK] をクリックします。

[Service Settings] ダイアログボックスが閉じます。

このサービスの変更内容が保存されます。

サービスの削除方法

サービスは、Console でインストールしたものも含めて、削除できます。ただし、デフォルト サービスは削除できません。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

ステップ 2　左のペインで、✖（[Delete Service]）をクリックします。

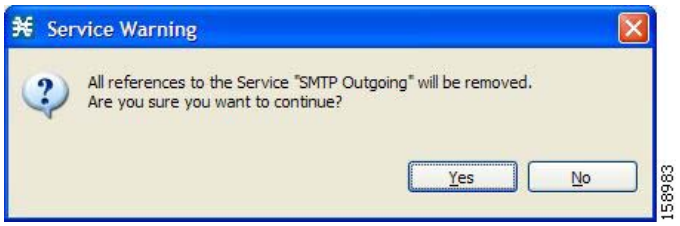
ステップ 3　[Service Warning] メッセージが表示されます（図 7-7）。

図 7-7　[Service Warning]

ステップ 4　[Yes] をクリックします。

- このサービスの規則が設定されているパッケージがある場合（「規則の管理」（P.9-56）を参照）、[Service Warning] メッセージがもう 1 つ表示されます（図 7-8）。

図 7-8　[Service Warning]



- [Yes] をクリックします。

サービスが削除され、サービス ツリーに表示されなくなります。サービスの規則も同時に削除されます。

削除されたサービスの子は削除されず、サービス ツリー内で 1 階層上に移動します。

サービス要素の管理

サービスとは、サービス要素の集合です。サービスの定義を完了するには、そのサービス要素を定義する必要があります。サービス要素は特定のプロトコル、開始側、ゾーン、およびフレーバを、選択されたサービスに対応付けます。

詳細は、「プロトコルの管理」（P.7-21）、「ゾーンの管理」（P.7-31）、および「フレーバの管理」（P.7-48）を参照してください。

サービス コンフィギュレーションには、最大で 10,000 のサービス要素を設定できます。それぞれのサービス要素は一意でなければなりません。

次の 5 つの基準をすべて満たすトラフィック フローは、サービス要素によってサービス要素のサービスにマッピングされます。

- フローがサービス要素の指定のプロトコルを使用している。
- フローが、サービス要素のために指定された側（ネットワーク、サブスクライバ、または両方）によって開始されている。
- フローの宛先が、サービス要素の指定ゾーンに属するアドレスである。
- フローが、サービス要素の指定のフレーバと一致している。
- サービス要素が、上記 4 つの基準を満たした、最も固有性の高いサービス要素である。

サービス要素の追加方法

必要に応じて、サービスに新しいサービス要素を追加できます （よく使用されるサービス要素は、Console のインストールに含まれています）。サービスには、任意の数のサービス要素を設定できます（1 つのサービス コンフィギュレーションにつき、設定可能なサービス要素の数は最大 10,000 です）。

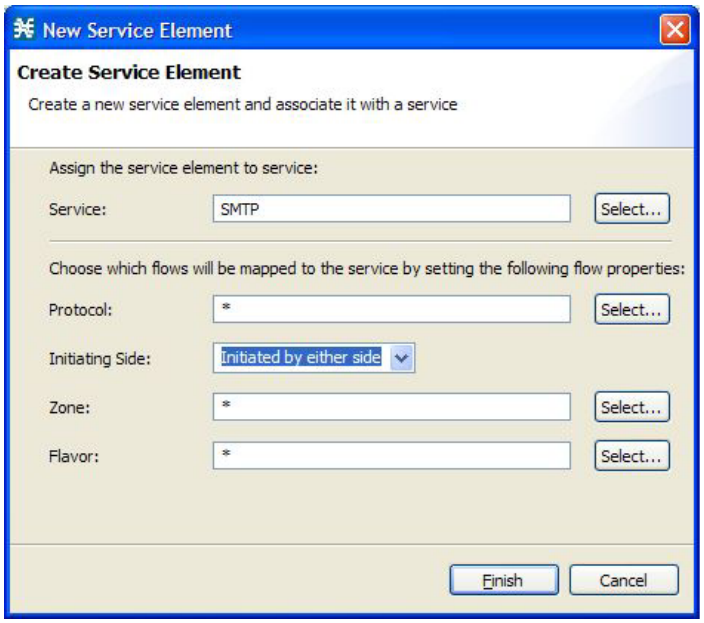
（注）　すべてのサービス要素は、一意でなければなりません。既存のサービス要素と同一のサービス要素を作成しようとすると、ダイアログボックスにエラー メッセージが表示され、[Finish] ボタンはグレー表示になります。この場合、少なくとも 1 つのフィールドの値を修正してください。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

ステップ 2　右側（サービス要素）のペインで、（[Add Service Element]）をクリックします。

[New Service Element] ダイアログボックスが表示されます（図 7-9）。

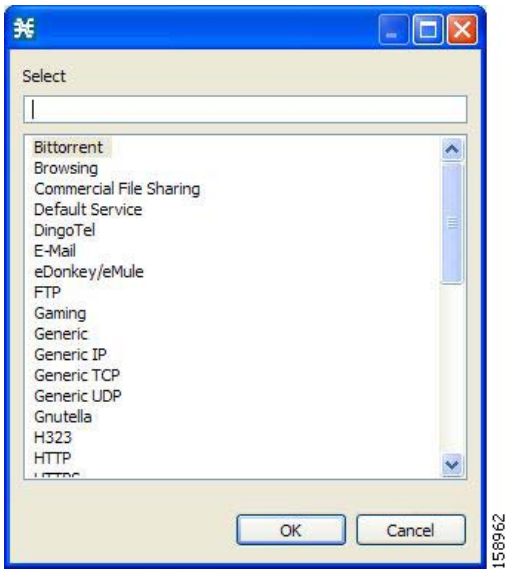
図 7-9　[New Service Element]



ステップ 3　このサービス要素を割り当てるサービスを変更するには、[Service] フィールドの隣の [Select] ボタンをクリックします。

[Select a Service] ダイアログボックスが開き（図 7-10）、全サービスのリストが表示されます。

図 7-10　[Select a Service]



ステップ 4　リストからサービスを選択します。

ステップ 5　[OK] をクリックします。

[Select a Service] ダイアログボックスが閉じます。

選択したサービスが、[New Service Element] ダイアログボックスの [Service] フィールドに表示されます。

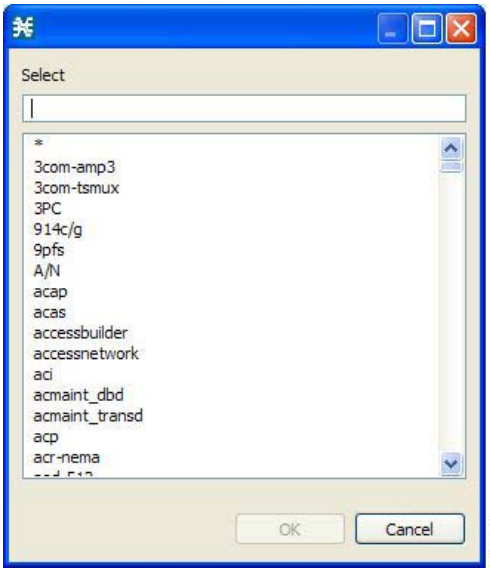
ステップ 6　[Protocol] フィールドの隣の [Select] ボタンをクリックします。

（注）　デフォルト値（アスタリスク、*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にプロトコルのチェックは行われません。

[Select a Protocol] ダイアログボックスが開き（図 7-11）、全プロトコルのリストが表示されます。

（注）　プロトコルを選択する前にフレーバを選択する（ステップ 15）と、選択したフレーバに関連するプロトコルだけが表示されます。

図 7-11　[Select a Protocol]



ステップ 7　リストからプロトコルを選択します。ダイアログボックス上部のフィールドに入力すると、目的のプロトコルが探しやすくなります。

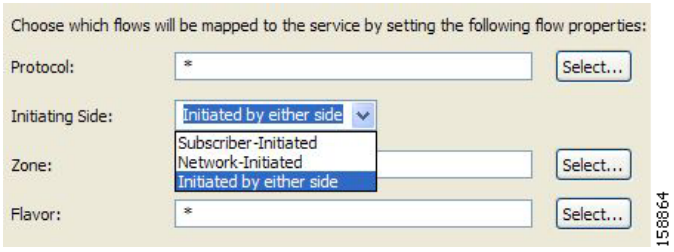
ステップ 8　[OK] をクリックします。

[Select a Protocol] ダイアログボックスが閉じます。

選択したプロトコルが、[New Service Element] ダイアログボックスの [Protocol] フィールドに表示されます。

ステップ 9　[Initiating Side] フィールド（図 7-12）で、ドロップダウン矢印をクリックします。

図 7-12　[Initiating Side] フィールド



ステップ 10　ドロップダウン リストから、該当する開始側を選択します。

次の中から選択できます。

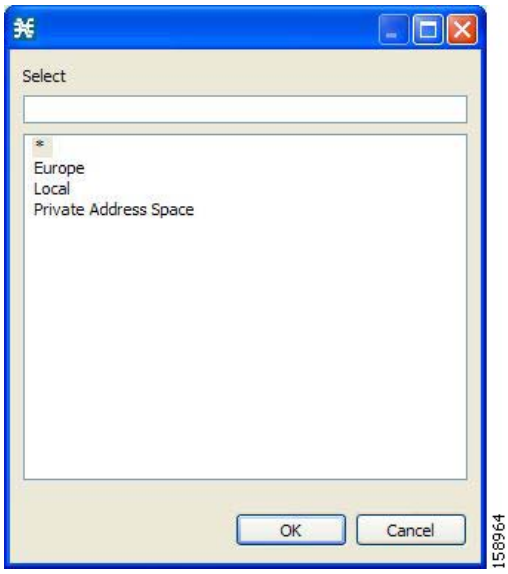
- [Subscriber-Initiated]：サブスクライバ側からネットワーク側（のサーバ）に向かってトランザクションが開始されます。
- [Network-Initiated]：ネットワーク側からサブスクライバ側（のサーバ）に向かってトランザクションが開始されます。
- [Initiated by either side]

ステップ 11　[Zone] フィールドの隣の [Select] ボタンをクリックします。

（注）　デフォルト値（アスタリスク、*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にゾーンのチェックは行われません。

[Select a Zone] ダイアログボックスが開き（図 7-13）、全ゾーンのリストが表示されます。

図 7-13　[Select a Zone]



ステップ 12　リストからゾーンを選択します。

ステップ 13　[OK] をクリックします。

[Select a Zone] ダイアログボックスが閉じます。

選択したゾーンが、[New Service Element] ダイアログボックスの [Zone] フィールドに表示されます。

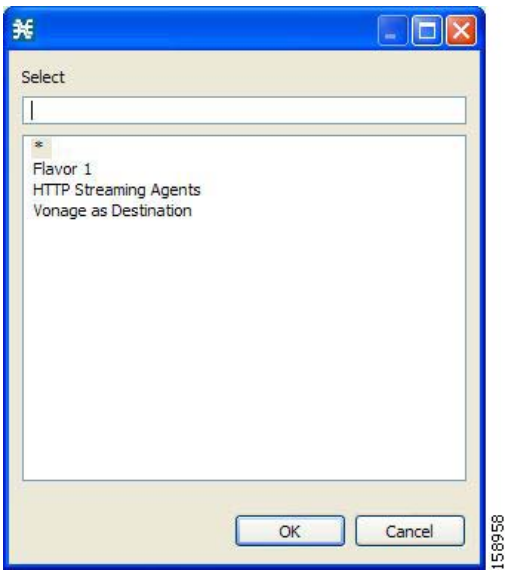
ステップ 14　[Flavor] フィールドの隣の [Select] ボタンをクリックします。

（注）　デフォルト値（アスタリスク、*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にフレーバのチェックは行われません。

[Select a Flavor] ダイアログボックスが開き（図 7-14）、ステップ 7 で選択したプロトコルに関連するすべてのフレーバのリストが表示されます。

（注）　プロトコルにデフォルト値（任意のプロトコルを意味する *）を選択した場合、選択できるフレーバは Type of Service（ToS）フレーバだけです。

図 7-14　　[Select a Flavor]



ステップ 15　リストからフレーバを選択します。

ステップ 16　[OK] をクリックします。

[Select a Flavor] ダイアログボックスが閉じます。

選択したフレーバが、[New Service Element] ダイアログボックスの [Flavor] フィールドに表示されます。

ステップ 17　[Finish] をクリックします。

[New Service Element] ダイアログボックスが閉じます。

サービスに新しいサービス要素が追加されます。

サービス要素ペインのサービス要素リストに、新しいサービス要素の行が追加されます。

サービス要素の複製方法

既存のサービス要素に類似した新しいサービス要素を追加する場合、既存のサービス要素の複製を行うのが便利です。サービス要素を複製してから変更する方が、サービス要素を最初から作成する方法よりも短時間で実行できます。

（注）　すべてのサービス要素は、一意でなければなりません。既存のサービス要素と同一のサービス要素を作成しようとすると、ダイアログボックスにエラー メッセージが表示され、[Finish] ボタンはグレー表示になります。この場合、少なくとも 1 つのフィールドの値を修正してください。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

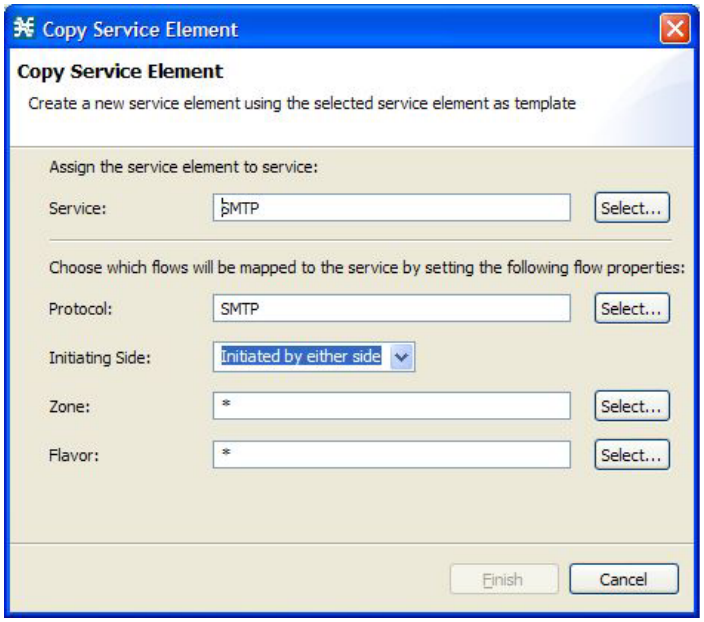
サービス要素ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　サービス要素ペインで、複製するサービス要素を選択します。

ステップ 3　（[Duplicate Service Element]）をクリックします。

[Copy Service Element] ダイアログボックスが表示されます（図 7-15）。

図 7-15　[Copy Service Element]



ステップ 4　サービス要素を変更します（「サービス要素の編集方法」（P.7-17）を参照）。

（注）　新しいサービス要素を保存するまえに、少なくとも 1 つのフィールドの値を変更する必要があります。

サービス要素の編集方法

サービス要素は、Console でインストーしたものも含めて、修正できます。

（注）　それぞれのサービス要素は一意でなければなりません。修正したサービス要素と同一のサービス要素がすでに存在する場合、ダイアログボックスにエラー メッセージが表示され、[Finish] ボタンはグレー表示になります。この場合、少なくとも 1 つのフィールドの値を修正してください。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

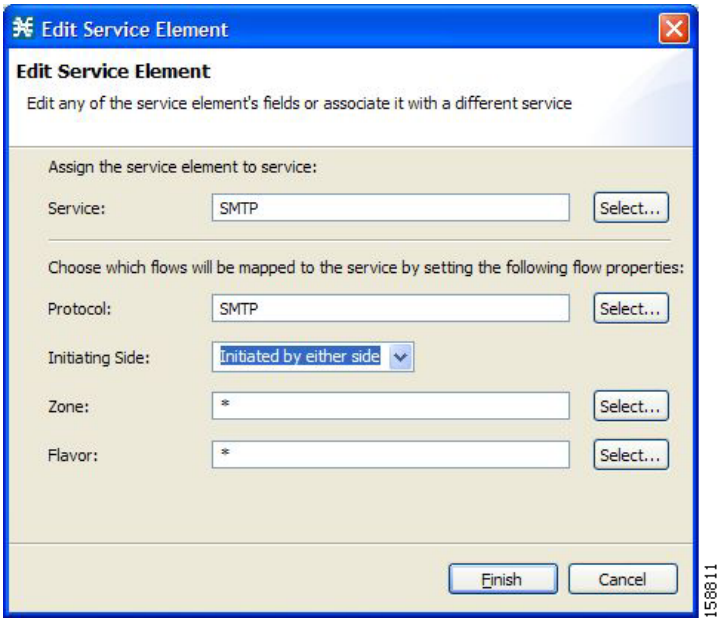
サービス要素ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　サービス要素ペインで、編集するサービス要素を選択します。

ステップ 3　サービス要素ペインで、（[Edit Service Element]）をクリックします。

[Edit Service Element] ダイアログボックスが表示されます（図 7-16）。

図 7-16　[Edit Service Element]



ステップ 4　このサービス要素を割り当てるサービスを変更するには、[Service] フィールドの隣の [Select] ボタンをクリックします。

[Select a Service] ダイアログボックスが開き、全サービスのリストが表示されます。

ステップ 5　リストからサービスを選択します。

ステップ 6　[OK] をクリックします。

[Select a Service] ダイアログボックスが閉じます。

選択したサービスが、[Edit Service Element] ダイアログボックスの [Service] フィールドに表示されます。

ステップ 7　このサービス要素のプロトコルを変更するには、[Protocol] フィールドの隣の [Select] ボタンをクリックします。

（注）　アスタリスク（*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にプロトコルのチェックは行われません。

[Select a Protocol] ダイアログボックスが開き、全プロトコルのリストが表示されます。

ステップ 8　リストからプロトコルを選択します。ダイアログボックス上部のフィールドに入力すると、目的のプロトコルが探しやすくなります。

ステップ 9　[OK] をクリックします。

[Select a Protocol] ダイアログボックスが閉じます。

選択したサービスが、[Edit Service Element] ダイアログボックスの [Protocol] フィールドに表示されます。

ステップ 10　このサービス要素の開始側を変更するには、[Initiating Side] フィールドのドロップダウン矢印をクリックします。

ステップ 11　ドロップダウン リストから、該当する開始側を選択します。

次の中から選択できます。

- [Subscriber-Initiated]：サブスクライバ側からネットワーク側（のサーバ）に向かってトランザクションが開始されます。
- [Network-Initiated]：ネットワーク側からサブスクライバ側（のサーバ）に向かってトランザクションが開始されます。
- [Initiated by either side]

ステップ 12　このサービス要素のゾーンを変更するには、[Zone] フィールドの隣の [Select] ボタンをクリックします。

（注）　アスタリスク（*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にゾーンのチェックは行われません。

[Select a Zone] ダイアログボックスが開き、全ゾーンのリストが表示されます。

ステップ 13　リストからゾーンを選択します。

ステップ 14　[OK] をクリックします。

[Select a Zone] ダイアログボックスが閉じます。

選択したゾーンが、[Edit Service Element] ダイアログボックスの [Zone] フィールドに表示されます。

ステップ 15　このサービス要素のフレーバを変更するには、[Flavor] フィールドの隣の [Select] ボタンをクリックします。

（注）　アスタリスク（*）の場合、フローがこのサービス要素にマッピングされていれば、テスト時にフレーバのチェックは行われません。

[Select a Flavor] ダイアログボックスが開き、全フレーバのリストが表示されます。

ステップ 16　リストからフレーバを選択します。

ステップ 17　[OK] をクリックします。

[Select a Flavor] ダイアログボックスが閉じます。

選択したフレーバが、[Edit Service Element] ダイアログボックスの [Flavor] フィールドに表示されます。

ステップ 18　[Finish] をクリックします。

[Edit Service Element] ダイアログボックスが閉じます。

サービス要素の変更内容が保存されます。

サービス要素ペインのサービス要素リストに、変更後のサービス要素が表示されます。

サービス要素の削除方法

サービス要素は、Console でインストールしたものも含めて、削除できます。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

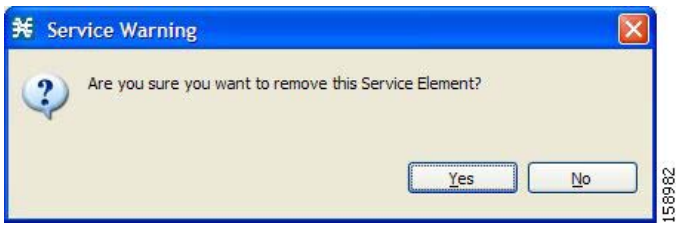
サービス要素ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　サービス要素ペインで、削除するサービス要素を選択します。

ステップ 3　サービス要素ペインで、✖（[Delete Service Element]）をクリックします。

[Service Warning] メッセージが表示されます（図 7-17）。

図 7-17　[Service Warning]



ステップ 4　[Yes] をクリックします。

サービス要素が削除され、選択したサービスから除外されます。

サービス要素の移動方法

サービス間で既存のサービス要素を移動できます。

ステップ 1　[Service] タブで、サービス ツリーからサービスを選択します。

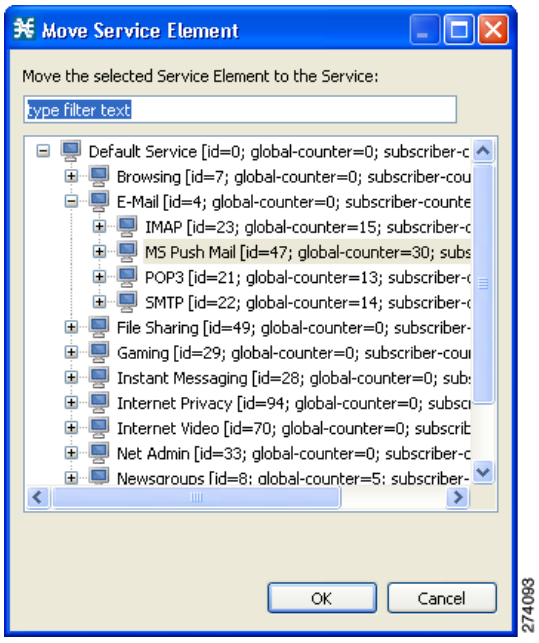
サービス要素ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　サービス要素ペインで、移動するサービス要素を選択します。

ステップ 3　（[Move Service Element to Another Service]）をクリックします。

[Move Service Element] ダイアログボックスが開き（図 7-18）、完全なサービス ツリーが表示されます。

図 7-18　[Move Service Element]



ステップ 4　サービス ツリーからサービスを選択します。

ステップ 5　[OK] をクリックします。

[Move Service Element] ダイアログボックスが閉じます。

選択したサービスにサービス要素が移動します。

プロトコルの管理

プロトコルは、アプリケーション プロトコル シグニチャ、宛先ポート、一意の名前および説明（オプション）で構成されます。

プロトコルは、サービス要素の定義に使用されます（「サービス要素の管理」（P.7-12）を参照）。

新しいプロトコルを追加できます（たとえば、特定のポートを使用する新しいゲーム用プロトコルを分類する場合）。既存のプロトコルを編集したり、削除したりすることもできます。

サービス コンフィギュレーションには、最大で 10,000 のプロトコルを設定できます。

SCA BB は、多様な商用および共通プロトコルをサポートしています。最新の SCA BB リリースに含まれるプロトコルの詳細なリストについては、『*Cisco Service Control Application for Broadband Reference Guide*』の「Default Service Configuration Reference Tables」にある「Information About Protocols」を参照してください。新しいプロトコルがリリースされると、サービス コンフィギュレーションにシグニチャの追加が行えるように、シスコでは新しいプロトコル シグニチャを記載したファイルを提供しています（「サービス コンフィギュレーションへの Dynamic Signature Script のインポート方法」（P.7-41）を参照）。

プロトコルの表示

プロトコルの表示方法

プロトコルのリストと、関連するプロトコル要素を表示できます。

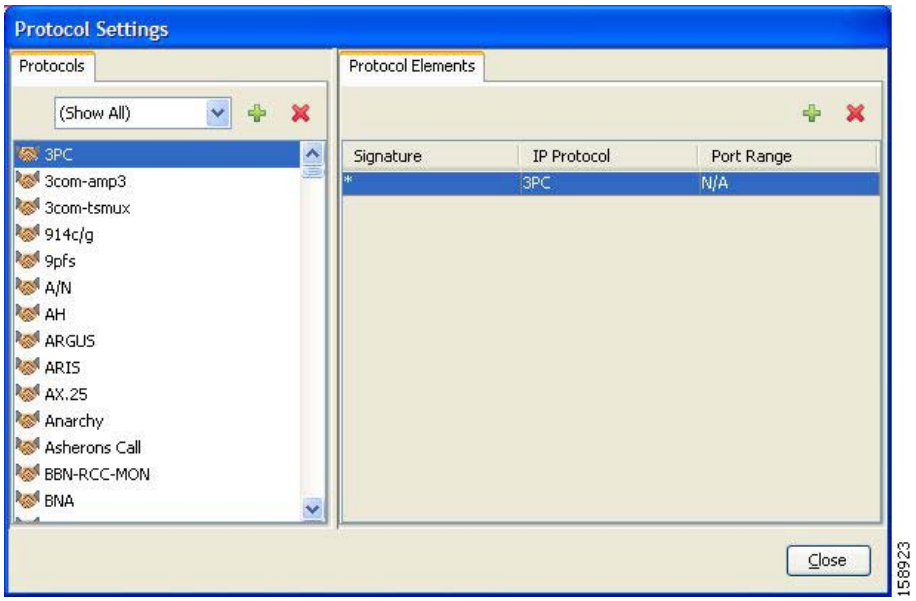
プロトコルは、ASCII のソート順序（0... 9、A... Z、a... z）で一覧表示されます。

プロトコル要素はソートされず、プロトコルに追加された順序で一覧表示されます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます（図 7-19）。

図 7-19　[Protocol Settings]

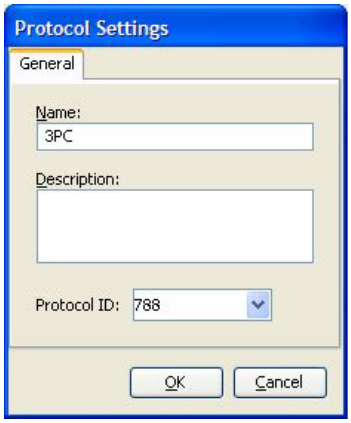


[Protocols] タブに、既存のプロトコルのリストが表示されます。

ステップ 2　プロトコルの説明と ID を表示するには、そのプロトコルをダブルクリックします。

[Protocol Settings] ダイアログボックスが開き（図 7-20）、プロトコル名、説明、ID が表示されます。

図 7-20　[Protocol Settings]



ステップ 3　[Cancel] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

ステップ 4　プロトコル要素のリストを表示するには、[Protocol Settings] ダイアログボックスのリストでプロトコルを選択します。

[Protocol Elements] タブに、プロトコル要素が表示されます。

ステップ 5　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコル リストのフィルタリング方法

プロトコルをタイプごとにフィルタリングし、選択したプロトコル タイプだけを [Protocols] タブに表示することができます。

プロトコルには次の 10 種類のカテゴリがあります。

- [Generic Protocols]：トランザクション用の汎用 IP、汎用 TCP、および汎用 UDP プロトコルで、他のプロトコル タイプによって特定のプロトコルにマッピングされていないもの。
- [IP Protocols]：TCP/UDP 以外のプロトコル（ICMP など）。トランザクションの IP プロトコル番号に従って識別されます。
- [Port-Based Protocols]：既知のポートに従って分類される TCP および UDP プロトコル。デフォルトのサービス コンフィギュレーションには、750 を超える一般的なポートベース プロトコルが含まれています。
- [Signature-Based Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類されたプロトコル。HTTP や FTP など最も一般的なプロトコル、および多数の一般的な P2P プロトコルが含まれます。
- [P2P Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類されたピアツーピア ファイル共有アプリケーション プロトコル。
- [VOIP Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された Voice over IP（VoIP）アプリケーション プロトコル。
- [SIP Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された、SIP プロトコル、または SIP 特性を持つプロトコル。
- [Worm Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された、インターネット ワームのトラフィック パターンに基づくプロトコル。
- [Packet Stream Pattern-Based Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類されたプロトコルで、パケットのペイロード内容ではなくパケット ストリームのパターン（たとえば、ストリームのシンメトリ、平均パケット サイズ、転送速度など）に基づくプロトコル。
- [Unidirectionally Detected Protocols]：単方向シグニチャを持つプロトコル。

（注） 複数のカテゴリに属するプロトコルもあります。特に、あらかじめ定義された P2P、VOIP、SIP、Worm、および Packet Stream Pattern-Based Protocols は、Signature-Based Protocols としても定義されています。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブのドロップダウン リストで、表示するプロトコルのタイプを選択します。

選択したタイプのプロトコルが、[Protocols] タブに表示されます。

ステップ 3　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

（注） ドロップダウン リストの設定が保存されます。次に [Protocol Settings] ダイアログボックスを開くと、すべてのプロトコルが表示されます。

プロトコルの追加方法

サービス コンフィギュレーションには、新しいプロトコルを追加できます。ただし、1 つのサービス コンフィギュレーションにつき、設定可能なプロトコルは最大 10,000 です。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブで、（[Add Protocol]）をクリックします。

[Protocol Settings] ダイアログボックスが表示されます（図 7-21）。

図 7-21　[Protocol Settings]

ステップ 3　[Name] フィールドに、新しいプロトコルの一意の名前を入力します。

ステップ 4　（オプション）[Protocol ID] ドロップダウン リストでプロトコルの ID を選択します。

プロトコル ID は、5000 ～ 9998 の整数でなければなりません。これより小さな値は、SCA BB で提供されるプロトコルのために予約されています。

（注）　プロトコル ID の値は、システムによって自動的に割り当てられます。この値は変更しないでください。

ステップ 5　[OK] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

[Protocols] タブに新しいプロトコルが表示されます。プロトコルにプロトコル要素を追加できます。「プロトコル要素の追加方法」（P.7-27）を参照してください。

プロトコルの編集方法

プロトコルのパラメータは、Console でインストールしたものも含めて、修正できます。

プロトコル要素の追加、変更、または削除を行う場合は、「プロトコル要素の管理」（P.7-26）を参照してください。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブで、プロトコルをダブルクリックします。

[Protocol Settings] ダイアログボックスがもう 1 つ表示されます（図 7-22）。

図 7-22　[Protocol Settings]

ステップ 3　[Protocol Settings] ダイアログボックスのフィールドを修正します。

- [Name] フィールドに、プロトコルの新しい名前を入力します。
- [Protocol ID] ドロップダウン リストでプロトコルの ID を選択します。

  プロトコル ID は、5000 ～ 9998 の整数でなければなりません。これより小さな値は、SCA BB で提供されるプロトコルのために予約されています。

（注）　プロトコル ID の値は、システムによって自動的に割り当てられます。この値は変更しないでください。

ステップ 4　[OK] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコル パラメータの新しい値が保存されます。

ステップ 5　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコルの削除方法

プロトコルは、Console でインストールしたものも含めて、削除できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

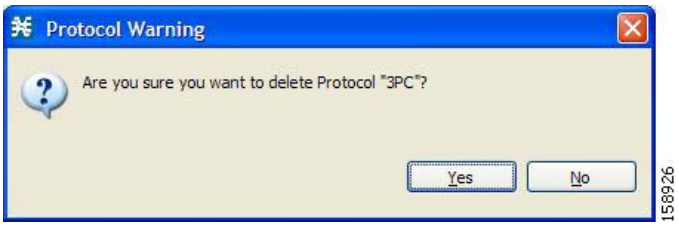
[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブで、プロトコルを選択します。

ステップ 3　[Protocols] タブで、  （[Delete Protocol]）をクリックします。

[Protocol Warning] メッセージが表示されます（図 7-23）。

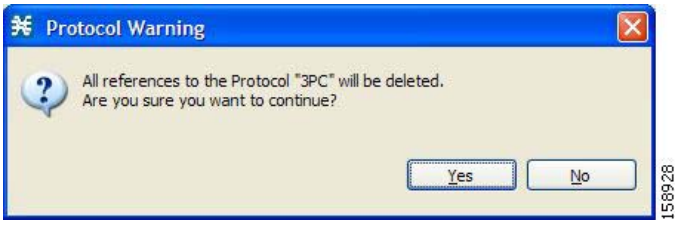
図 7-23　[Protocol Warning]



ステップ 4　[Yes] をクリックします。

- サービス要素により、選択されたプロトコルがサービスにマッピングされる場合（「サービス要素の管理」（P.7-12）を参照）、（サービスがパッケージで使用されていない場合でも）[Protocol Warning] メッセージがもう 1 つ表示されます（図 7-24 を参照）。

図 7-24　[Protocol Warning]



- [Yes] をクリックします。

[Protocols] タブからプロトコルが削除されます。

ステップ 5　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコル要素の管理

プロトコルは、プロトコル要素の集合です。

プロトコルの定義を完了するには、プロトコル要素を定義する必要があります。プロトコル要素は特定のシグニチャ、IP プロトコル、およびポート範囲を、選択されたプロトコルに対応付けます。サービス コンフィギュレーション内の各プロトコル要素は、一意でなければなりません。

トラフィック フローは、次の 4 つの基準をすべて満たしている場合、特定のプロトコルにマッピングされます。

- フローがプロトコル要素の指定のシグニチャに属している。
- フロー プロトコルがプロトコル要素の指定の IP プロトコルである。
- （IP プロトコルが TCP または UDP の場合）宛先ポートがプロトコル要素の指定のポート範囲内にある。
- プロトコル要素が、上記 3 つの基準を満たした、最も固有性の高いプロトコル要素である。

プロトコル要素の追加方法

プロトコルに、任意の数のプロトコル要素を追加できます。

（注）　プロトコル要素のパラメータを設定する場合、パラメータの値は入力時に保存されます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブで、プロトコルを選択します。

ステップ 3　[Protocol Elements] タブで、（[Add Protocol Element]）をクリックします。

そのプロトコルにプロトコル要素が追加されます。

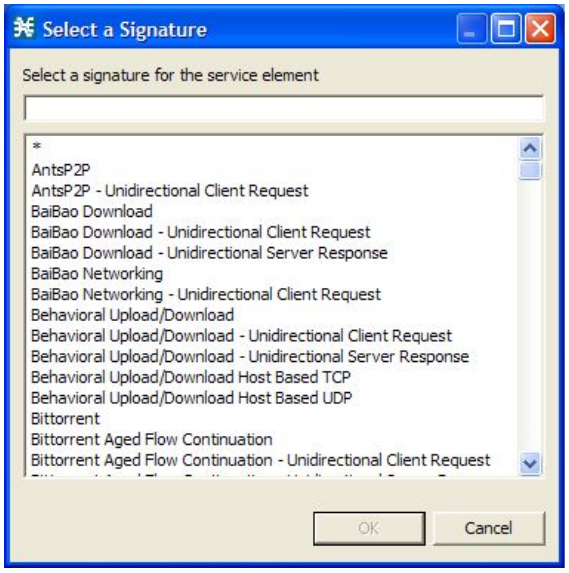
[Protocol Elements] タブのプロトコル要素リストに、新しいプロトコル要素の行が追加されます。

ステップ 4　プロトコル要素の [Signature] セルをクリックして、セルに表示される [Browse] ボタンをクリックします。

（注）　デフォルト値（アスタリスク、*）の場合、フローがこのプロトコル要素にマッピングされていれば、テスト時にシグニチャのチェックは行われません。

[Select a Signature] ダイアログボックスが開き（図 7-25）、全シグニチャのリストが表示されます。

図 7-25　[Select a Signature]



ステップ 5　リストからシグニチャを選択します。

（注）　プロトコル シグニチャ データベースに一致するシグニチャがないフローを、このプロトコル要素にマッピングするには、Generic シグニチャを選択します（フローが IP プロトコルや、プロトコル要素のポート範囲とも一致する場合）。

ステップ 6　[OK] をクリックします。

[Select a Signature] ダイアログボックスが閉じます。

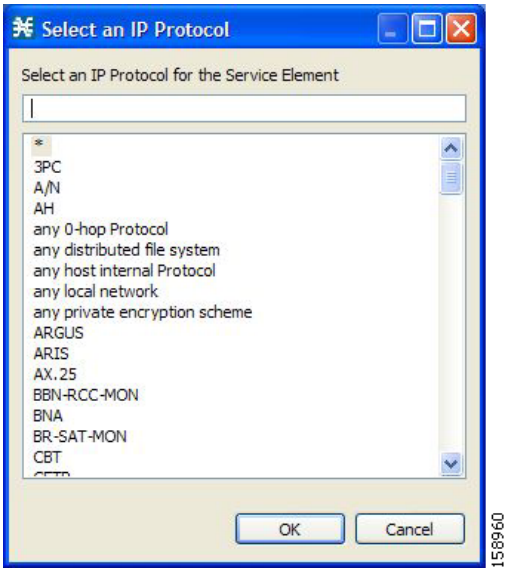
選択したシグニチャが、[Protocol Settings] ダイアログボックスの [Signature] セルに表示されます。

ステップ 7　プロトコル要素の [IP Protocol] セルをクリックして、セルに表示される [Browse] ボタンをクリックします。

（注）　デフォルト値（アスタリスク、*）の場合、フローがこのプロトコル要素にマッピングされていれば、テスト時に IP プロトコルのチェックは行われません。

[Select an IP Protocol] ダイアログボックスが開き（図 7-26）、全 IP プロトコルのリストが表示されます。

図 7-26　[Select an IP Protocol]



ステップ 8　リストから IP プロトコルを選択します。

ステップ 9　[OK] をクリックします。

[Select an IP Protocol] ダイアログボックスが閉じます。

選択した IP プロトコルが、[Protocol Settings] ダイアログボックスの [IP Protocol] セルに表示されます。

ステップ 10　[Port Range] セルに、1 つのポートまたはポートの範囲を入力します （ポートの範囲を入力する場合、最初のポートと最後のポートをハイフンでつなぎます）。

（注）　ポートの範囲が指定できるのは、指定する IP プロトコルが TCP または UDP の場合（または未定義で、ワイルドカードの「*」を使用する場合）だけです。

ポートがこれらのいずれかのポートと一致するフローだけが、このプロトコル要素にマッピングされます。

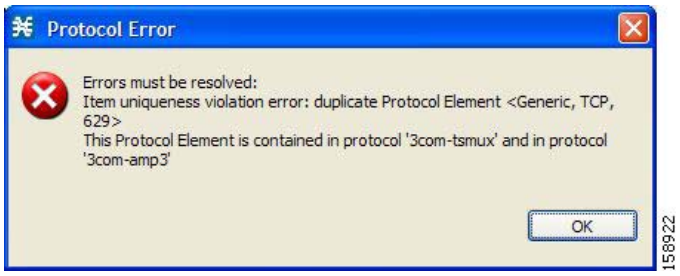
プロトコル要素が定義されます。

ステップ 11　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

- 定義したプロトコル要素がこのサービス コンフィギュレーション内で一意でない場合、[Protocol Error] メッセージが表示されます（図 7-27）。

図 7-27　[Protocol Error]



a.　[OK] をクリックします。

b.　プロトコル要素を修正または削除します。

c.　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコル要素の編集方法

プロトコル要素は、Console でインストールしたものも含めて、修正できます。

（注）　プロトコル要素の変更内容は、変更時に保存されます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブで、プロトコルを選択します。

ステップ 3　[Protocols Elements] タブで、プロトコル要素を選択します。

ステップ 4　プロトコル要素の [Signature] セルをクリックして、セルに表示される [Browse] ボタンをクリックします。

[Select a Signature] ダイアログボックスが表示されます。

ステップ 5　リストからシグニチャを選択します。

ステップ 6　[OK] をクリックします。

[Select a Signature] ダイアログボックスが閉じます。

ステップ 7　プロトコル要素の [IP Protocol] セルをクリックして、セルに表示される [Browse] ボタンをクリックします。

[Select an IP Protocol] ダイアログボックスが表示されます。

ステップ 8　リストから IP プロトコルを選択します。

ステップ 9　[OK] をクリックします。

[Select an IP Protocol] ダイアログボックスが閉じます。

ステップ 10　プロトコル要素の [Port Range] セルに、1 つのポートまたはポートの範囲を入力します。

プロトコル要素の変更内容は、変更時に保存されます。

ステップ 11　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

- 修正したプロトコル要素がこのサービス コンフィギュレーション内で一意でない場合、[Protocol Error] メッセージが表示されます。

a. [OK] をクリックします。

b. プロトコル要素を修正または削除します。

c. [Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

プロトコル要素の削除方法

プロトコル要素は、Console でインストールしたものも含めて、削除できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

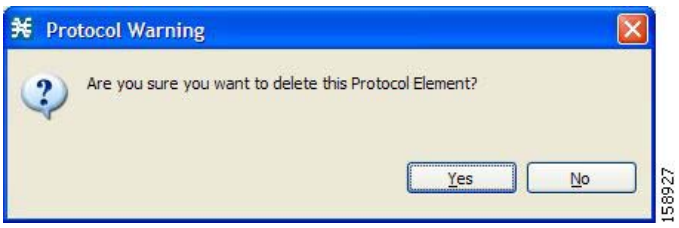
ステップ 2　[Protocols] タブでプロトコルを選択します。

ステップ 3　[Protocols Elements] タブで、プロトコル要素を選択します。

ステップ 4　[Protocol Elements] タブで、  （[Delete Protocol Element]）をクリックします。

[Protocol Warning] メッセージが表示されます（図 7-28）。

図 7-28　[Protocol Warning]



ステップ 5　[Yes] をクリックします。

[Protocol Elements] タブから、プロトコル要素が削除されます。

ステップ 6　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

ゾーンの管理

ゾーンとは、宛先 IP アドレスの集合で、通常は 1 つのゾーン内のアドレスが関連付けられます。

ゾーンはネットワーク セッションを分類するために使用され、各ネットワーク セッションは、宛先 IP アドレスに基づいてサービス要素に割り当てられます。

サービス コンフィギュレーションには、最大で 10,000 のゾーン項目を設定できます。それぞれのゾーン項目は一意でなければなりません。

ゾーンの表示方法

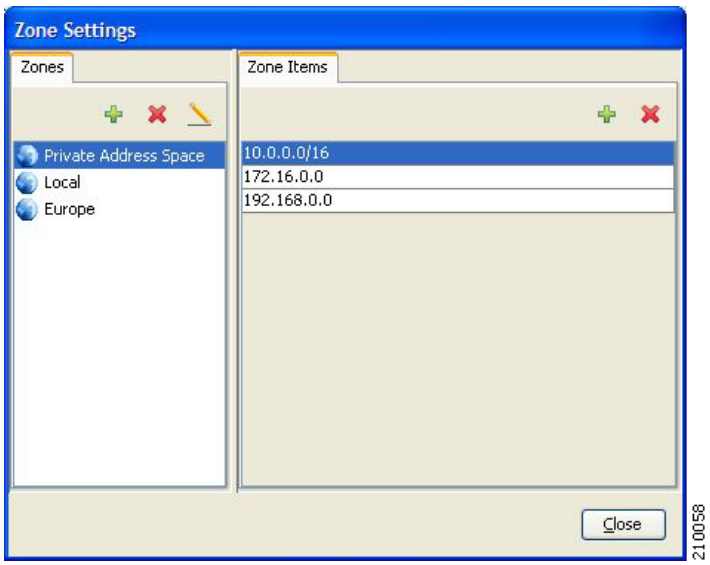
ゾーンのリストと、関連するゾーン項目を表示できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。

[Zone Settings] ダイアログボックスが表示されます（図 7-29）。

[Zones] タブに、ゾーンのリストが表示されます。リストの最初のゾーンが選択され、そのゾーン項目が [Zone Items] タブに表示されます。

図 7-29　[Zone Settings]



ステップ 2　ゾーン項目を表示するには、リスト内のゾーンをクリックします。

選択したゾーンのゾーン項目が [Zone Items] タブに表示されます。

ステップ 3　[Close] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

ゾーンの追加方法

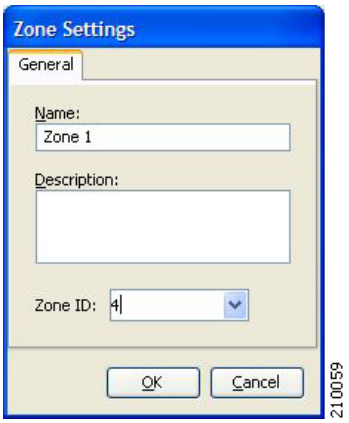
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。

[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、  （[Add Zone]）をクリックします。

[Zone Settings] ダイアログボックスが表示されます（図 7-30）。

図 7-30　[Zone Settings]



ステップ 3　[Name] フィールドに、新しいゾーンの一意の名前を入力します。

ステップ 4　（オプション）[Zone ID] ドロップダウン リストでゾーンの ID を選択します。

ゾーン ID は、1 ～ 32767 の正の整数でなければなりません。

（注）　ゾーン ID の値は、システムによって自動的に割り当てられます。この値は変更しないでください。

ステップ 5　[OK] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

[Zones] タブに新しいゾーンが追加されます。ゾーン項目を追加できます （「ゾーン項目の追加方法」（P.7-34）を参照）。

ゾーンの編集方法

ゾーン パラメータは、いつでも修正できます。

ゾーン項目の追加、変更、または削除を行う場合は、「ゾーン項目の管理」（P.7-34）を参照してください。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。

[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、ゾーンを選択します。

ステップ 3　([Edit Zone]）をクリックします。

[Zone Settings] ダイアログボックスが表示されます。

ステップ 4　ダイアログボックスのフィールドを修正します。

- [Name] フィールドに、ゾーンの新しい名前を入力します。
- [Zone ID] ドロップダウン リストでゾーンの ID を選択します。

  ゾーン ID は、1 ～ 32767 の正の整数でなければなりません。

（注）　ゾーン ID の値は、システムによって自動的に割り当てられます。この値は変更しないでください。

ステップ 5　[OK] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

ゾーン パラメータの新しい値が保存されます。

ステップ 6　[Close] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

ゾーンの削除方法

任意のゾーン、またはすべてのゾーンを削除できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。

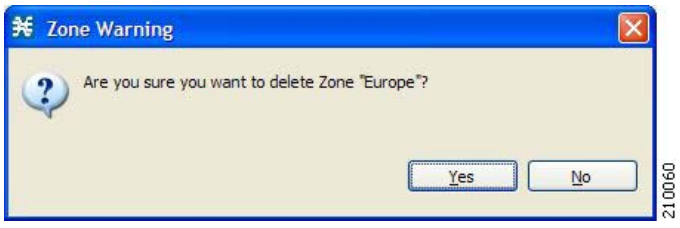
[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、ゾーンを選択します。

ステップ 3　[Zones] タブで、([Delete Zone]）をクリックします。

[Zone Warning] メッセージが表示されます（図 7-31）。

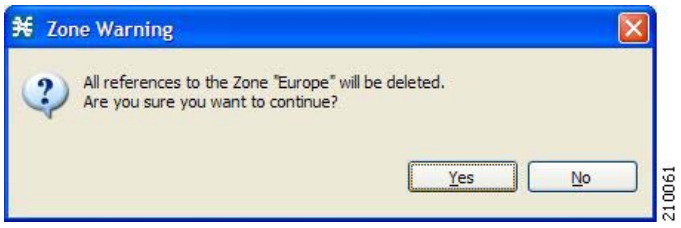
図 7-31　[Zone Warning]



ステップ 4　[OK] をクリックします。

- 選択したゾーンを参照するサービス要素がある場合、[Zone Warning] メッセージがもう 1 つ表示されます（図 7-32）。

図 7-32　[Zone Warning]



- [Yes] をクリックします。

  選択したゾーンを参照するサービス要素が削除されます。

ゾーンが削除され、[Zone] タブに表示されなくなります。

ステップ 5　[Close] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

ゾーン項目の管理

ゾーンは、関連するゾーン項目の集合です。

ゾーン項目は、1 つの IP アドレスまたは IP アドレスの範囲です。

サービス コンフィギュレーションには、最大で 10,000 のゾーン項目を設定できます。それぞれのゾーン項目は一意でなければなりません。

ゾーン項目の追加方法

ゾーンには、任意の数のゾーン項目を追加できます（ただし、1 つのサービス コンフィギュレーションにつき、設定可能なゾーン項目は最大 10,000 です）。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。

[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、ゾーンを選択します。

ステップ 3　[Zones Items] タブで、  （[Add Zone Item]）をクリックします。

[Zone Items] テーブルに新しい行が追加されます。

ステップ 4　新しいリスト項目をダブルクリックして、有効な値を入力します。

有効な値は、単一の IP アドレス（63.111.106.7 など）または IP アドレスの範囲（194.90.12.0/24 など）のいずれかです。

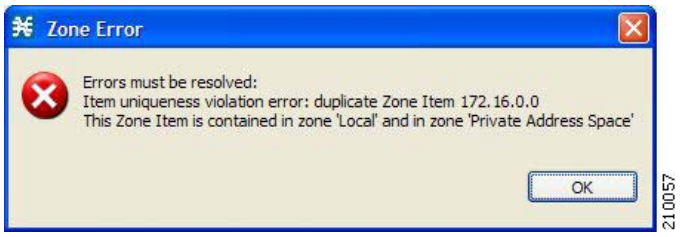
ステップ 5　このゾーンに属するその他の IP アドレスについて、ステップ 3 と 4 を実行します。

ステップ 6　[Close] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

- 定義したゾーン項目がこのサービス コンフィギュレーション内で一意でない場合、[Zone Error] メッセージが表示されます（図 7-33）。

図 7-33　[Zone Error]



a. [OK] をクリックします。
b. ゾーン項目を修正または削除します。
c. [Close] をクリックします。
[Zone Settings] ダイアログボックスが閉じます。

ゾーン項目の編集方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。
[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、ゾーンを選択します。

ステップ 3　[Zones Items] タブで、ゾーン項目をダブルクリックします。

ステップ 4　ゾーン項目の新しい値を入力します。
有効な値は、単一の IP アドレス（63.111.106.7 など）または IP アドレスの範囲（194.90.12.0/24 など）のいずれかです。

ステップ 5　[Close] をクリックします。
[Zone Settings] ダイアログボックスが閉じます。

- 修正したゾーン項目がこのサービス コンフィギュレーション内で一意でない場合、[Zone Error] メッセージが表示されます。

a. [OK] をクリックします。
b. ゾーン項目を修正または削除します。
c. [Close] をクリックします。
[Zone Settings] ダイアログボックスが閉じます。

ゾーン項目の削除方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Zones] の順に選択します。
[Zone Settings] ダイアログボックスが表示されます。

ステップ 2　[Zones] タブで、ゾーンを選択します。

ステップ 3　[Zones Items] タブで、ゾーン項目を選択します。

ステップ 4　[Zones Items] タブで、  （[Delete Zone Item]）をクリックします。
ゾーン項目が削除されます。

ステップ 5　[Close] をクリックします。

[Zone Settings] ダイアログボックスが閉じます。

プロトコル シグニチャの管理

プロトコル シグニチャは、プロトコルを一意に識別する一連のパラメータです。

シグニチャの表示

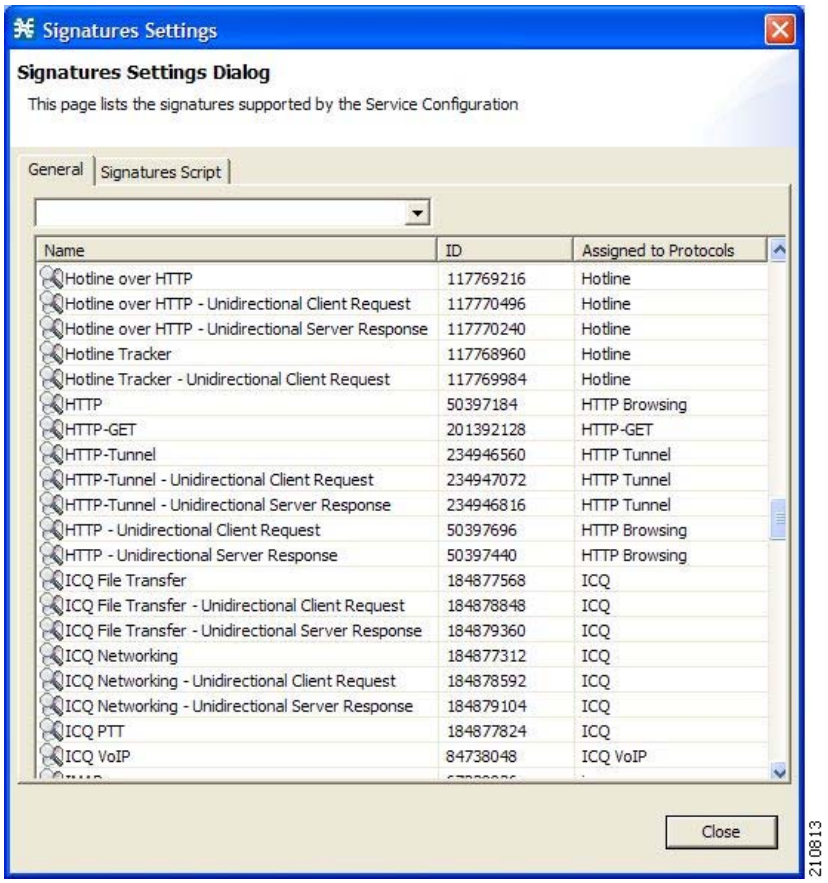
シグニチャの表示方法

シグニチャのリストと、各シグニチャが割り当てられるプロトコルを表示できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Signatures Settings] の順に選択します。

[Signatures Settings] ダイアログボックスが表示されます（図 7-34）。

図 7-34　[Signatures Settings]



ステップ 2　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

シグニチャ リストのフィルタリング方法

シグニチャをタイプごとにフィルタリングし、選択したシグニチャのタイプだけが [Signatures Settings] ダイアログボックスに表示されるようにできます。

シグニチャには次の 8 つのカテゴリがあります。

- [DSS Contributed Signatures]
- [Not Assigned to any Protocol]
- [P2P Signatures]
- [VOIP Signatures]
- [SIP Signatures]
- [Worm Signatures]
- [Packet Stream Pattern Based Protocols Signatures]
- [Unidirectionally Detected Signatures]

（注）　複数のカテゴリに属するシグニチャもあります。

ステップ 1　Console のメイン メニューで、[Configuration] > [Signatures Settings] の順に選択します。

[Signatures Settings] ダイアログボックスが表示されます。

ステップ 2　ドロップダウン リストで、表示するシグニチャのタイプを選択します。

選択したタイプのシグニチャがダイアログボックスに表示されます。

ステップ 3　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

ダイナミック シグニチャ

新しいプロトコルが常に公開されています。ダイナミック シグニチャとは、新しいプロトコルをプロトコル リストに追加し、そこからサービス コンフィギュレーションに追加するためのメカニズムです。これは、特に新しいプロトコル（P2P-Control ソリューションの新しい P2P プロトコルなど）のトラフィックを分類する場合に役立ちます。

- アクティブ サービス コンフィギュレーションに新しいシグニチャをインストールする場合は、「プロトコル パックの処理」（P.4-19）を参照してください。
- シグニチャの作成や変更を行う場合は、「Signature Editor の使用方法」（P.12-1）を参照してください。
- SCA BB のサービス コンフィギュレーション ユーティリティ、**servconf** を使用したシグニチャの適用については、「SCA BB サービス コンフィギュレーション ユーティリティ」（P.13-1）を参照してください。

次のセクションでは、Service Configuration Editor でダイナミック シグニチャを操作する方法について説明します。

Dynamic Signature Script ファイル

ダイナミック シグニチャは、Console または Service Configuration API を使用してサービス コンフィギュレーションに追加できる特殊な Dynamic Signature Script（DSS）ファイルに格納されています。DSS をサービス コンフィギュレーションにインポートすると、記述された新しいプロトコルは次のようになります。

- プロトコル リストに表示されます。
- サービスへの追加が可能です。
- レポートの表示に使用されます。

DSS で追加する新しいプロトコルの設定を簡単にするため、DSS では新しいプロトコルのバディ プロトコルを指定できます。DSS のロード時にアプリケーションがバディ プロトコルを検出すると、バディ プロトコルを使用する一連のサービス要素が自動的に複製され、バディ プロトコルへの参照がすべて新しいプロトコルへの参照に置換されます。新しいプロトコルとサービスの関係は、バディ プロトコルとサービスの関係と一致します。

DSS をサービス コンフィギュレーションにインポートすると、次の設定処理が自動的に実行されます。

- シグニチャがアップデートされ、新しいシグニチャがロードされます。
- 既存のプロトコルの新しいシグニチャに対してプロトコル要素が作成されます。
- 新しいプロトコルがプロトコル リストに追加され、それに対してプロトコル要素が作成されます。
- バディ プロトコルの設定に従って、新しいプロトコルのためのサービス要素が作成されます。

インポート手順では、サービスおよびプロトコル設定が保持されます。

（注）　DSS のインポート後、新しく追加されたプロトコルをサービスに関連付けてください。

DSS ファイルはカスタマー要件およびマーケット要求に応じて、シスコまたはパートナーから定期的にリリースされます。DSS ファイルは、新しいプロトコルとシグニチャが記述されており、以前の定義のシグニチャをアップデートします。新しい DSS でのサービス コンフィギュレーションのアップデートについては、「サービス コンフィギュレーションへの Dynamic Signature Script のインポート方法」（P.7-41）を参照してください。

（注）　独自の DSS ファイルの作成や、シスコからリリースされた DSS ファイルの修正は、Signature Editor ツールを使用して行います（「DSS ファイルの管理」（P.12-1）を参照）。

- 「現在のダイナミック シグニチャに関する情報の表示方法」（P.7-39）
- 「サービス コンフィギュレーションへの Dynamic Signature Script のインポート方法」（P.7-41）
- 「ダイナミック シグニチャの削除方法」（P.7-42）

現在のダイナミック シグニチャに関する情報の表示方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Signatures Settings] の順に選択します。

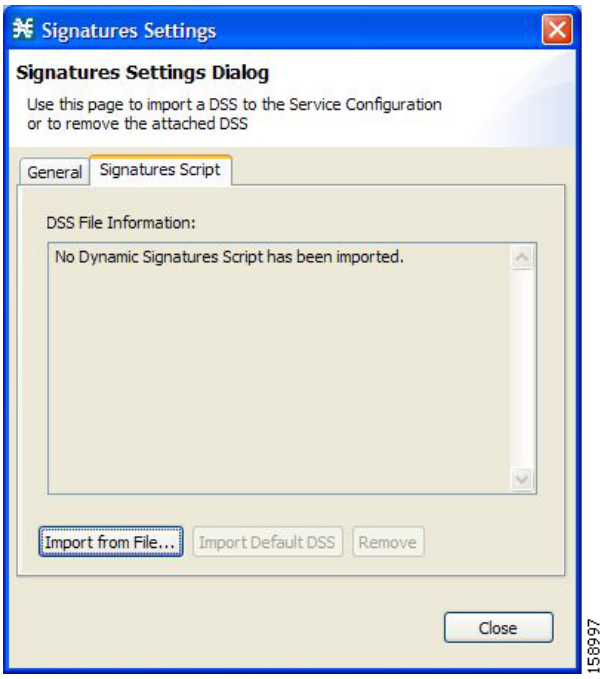
[Signatures Settings] ダイアログボックスが表示されます。

ステップ 2　[Signatures Script] タブをクリックします。

[Signatures Script] タブが開きます（図 7-35）。

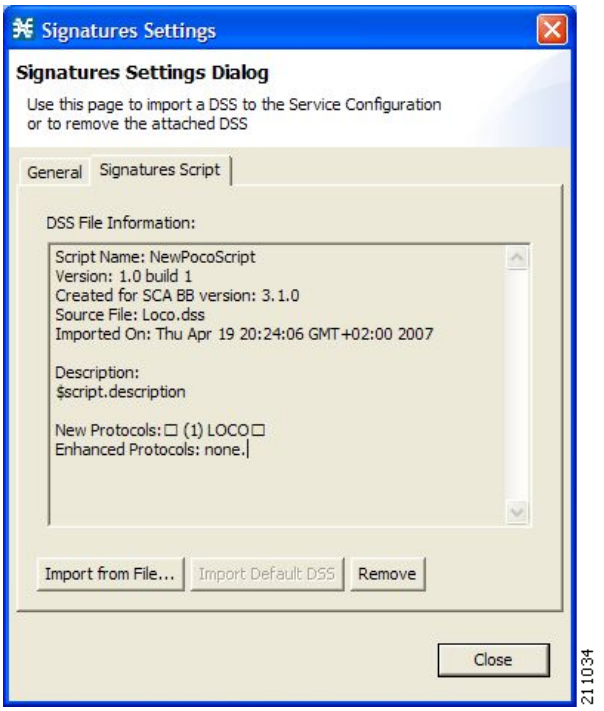
- 現在のサービス コンフィギュレーションに DSS ファイルがインポートされていない場合、[Signatures Settings] ダイアログボックスにメッセージが表示されます。

図 7-35　[Signature Settings]



- 現在のサービス コンフィギュレーションに DSS ファイルがインポートされている場合、[Signatures Settings] ダイアログボックスに、現在のダイナミック シグニチャとインポート元 DSS ファイルに関する情報が表示されます（図 7-36）。

図 7-36　[Signature Settings]



ステップ 3　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

サービス コンフィギュレーションへの Dynamic Signature Script のインポート方法

サービス コンフィギュレーションにシグニチャをインポートする際には、インポート元として、シスコ提供の DSS ファイル、シスコのパートナーの DSS ファイル（このセクションを参照）、あるいは Signature Editor ツール（「DSS ファイルの管理」（P.12-1）を参照）を使用して作成または修正した DSS ファイルを使用できます。

（注）　サービス コンフィギュレーションの作成時は最新のデフォルト DSS ファイルをインポートすることを推奨します（「デフォルト DSS ファイルを自動的にインポートする方法」（P.7-46）を参照）。この方法が推奨されるのは、新しい DSS を既存のサービス コンフィギュレーションに適用する場合だけです。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Signatures Settings] の順に選択します。

[Signatures Settings] ダイアログボックスが表示されます。

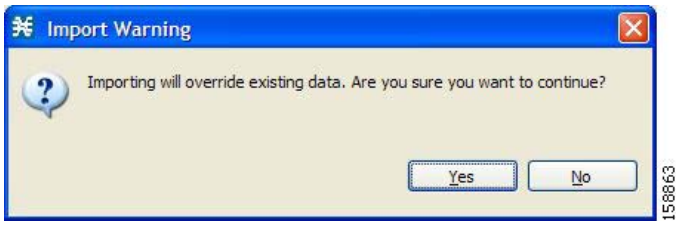
ステップ 2　[Signatures Script] タブをクリックします。

[Signatures Script] タブが開きます。

ステップ 3　[Import from File] をクリックします。

[Import Warning] メッセージが表示されます（図 7-37）。

図 7-37　[Import Warning]



ステップ 4　[Yes] をクリックします。

[Import from File] ダイアログボックスが表示されます。

ステップ 5　DSS ファイルをブラウズし、[Open] をクリックします。

[Import from File] ダイアログボックスが閉じます。

DSS ファイルのシグニチャが、サービス コンフィギュレーションにインポートされます。

インポートされたシグニチャとその DSS ファイルに関する情報が、[Signatures Settings] ダイアログボックスに表示されます。

ステップ 6　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

ダイナミック シグニチャの削除方法

インストールされたダイナミック シグニチャを、サービス コンフィギュレーションから削除できます。

（注）　DSS ファイルは削除されません。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Signatures Settings] の順に選択します。

[Signatures Settings] ダイアログボックスが表示されます。

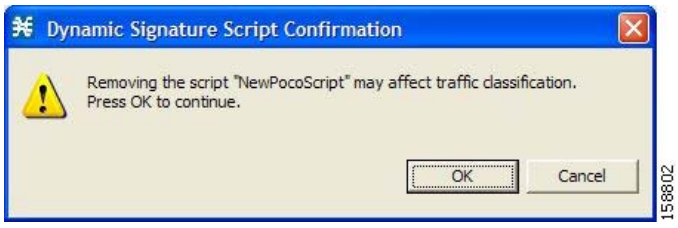
ステップ 2　[Signatures Script] タブをクリックします。

[Signatures Script] タブが開きます。

ステップ 3　[Remove] をクリックします。

[Dynamic Signature Script Confirmation] メッセージが表示されます（図 7-38）。

図 7-38　[Dynamic Signature Script Confirmation]



ステップ 4　[OK] をクリックします。

- インポートされた DSS ファイルにシグニチャが含まれているプロトコルを参照するサービス要素がある場合、[Dynamic Signature Script Removal Error] メッセージが表示されます（図 7-39）。

図 7-39　[Dynamic Signature Script Removal Error]

- [Yes] をクリックします。

  インポートされた DSS ファイルにシグニチャが含まれているプロトコルを参照するサービス要素が削除されます。

ダイナミック シグニチャが、サービス コンフィギュレーションから削除されます。

[Remove] ボタンがグレー表示になります。

ダイナミック シグニチャがデフォルト DSS ファイルからインポートされている場合、[Import Default DSS] ボタンがイネーブルになります。

ステップ 5　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

デフォルト DSS ファイル

シスコ（またはパートナー）からプロトコル パックが入手可能になったら、オフライン サービス コンフィギュレーション（ワークステーションに PQB ファイルとして格納）をアップデートする必要があります。プロトコル パック（「プロトコル パック」（P.4-20）を参照）は、SPQI または DSS ファイルとして提供されます。

ワークステーションで作成または編集された各サービス コンフィギュレーションに自動的にアップデートを提供するか、またはワークステーションから SCE プラットフォームにアップデートを適用することができます。最新のアップデートを利用可能にするには、最新の DSS または SPQI ファイルをデフォルト DSS ファイルとしてインストールします。ワークステーションへのファイルのインストールは、Console から、あるいは、「SCA BB シグニチャ コンフィギュレーション ユーティリティ」（P.13-7）に記載されている方法で実行できます。

- まだアップデートされていないサービス コンフィギュレーションに対して Console からサービス コンフィギュレーション オペレーション（新しいサービス コンフィギュレーションの作成や既存のサービス コンフィギュレーションの編集など）を実行すると、デフォルト DSS ファイルが自動的にインポートのために提供されます。
- デフォルト DSS ファイルは、**servconf**（「SCA BB シグニチャ コンフィギュレーション ユーティリティ」（P.13-7）を参照）を使用してサービス コンフィギュレーション オペレーション（既存のサービス コンフィギュレーションの適用など）を実行すると、デフォルトでインポートされます。このオプションはディセーブルにできます。

（注）　次のセクションで説明するように、新しいプロトコル パックを取得したら、管理ワークステーションのデフォルト DSS をアップデートしておいてください。

デフォルト DSS ファイルの設定とクリア

通常、デフォルト DSS ファイルは、シスコ（またはパートナー）が提供する最新のプロトコル パックでなければなりません。シスコから入手可能になるまでの間は、必要であれば、Signature Editor ツールを使用してプロトコル パックを修正し（「DSS ファイルの編集」（P.12-13）を参照）、新しいプロトコルのシグニチャを追加することで対応してください。

新しいプロトコル パックが入手可能になったら、デフォルト DSS ファイルとして設定してください。現在のデフォルト DSS ファイルをクリアする必要はありません。これは、新しいプロトコル パックによって上書きされます。

プロトコル パックをデフォルト DSS ファイルとして設定する方法

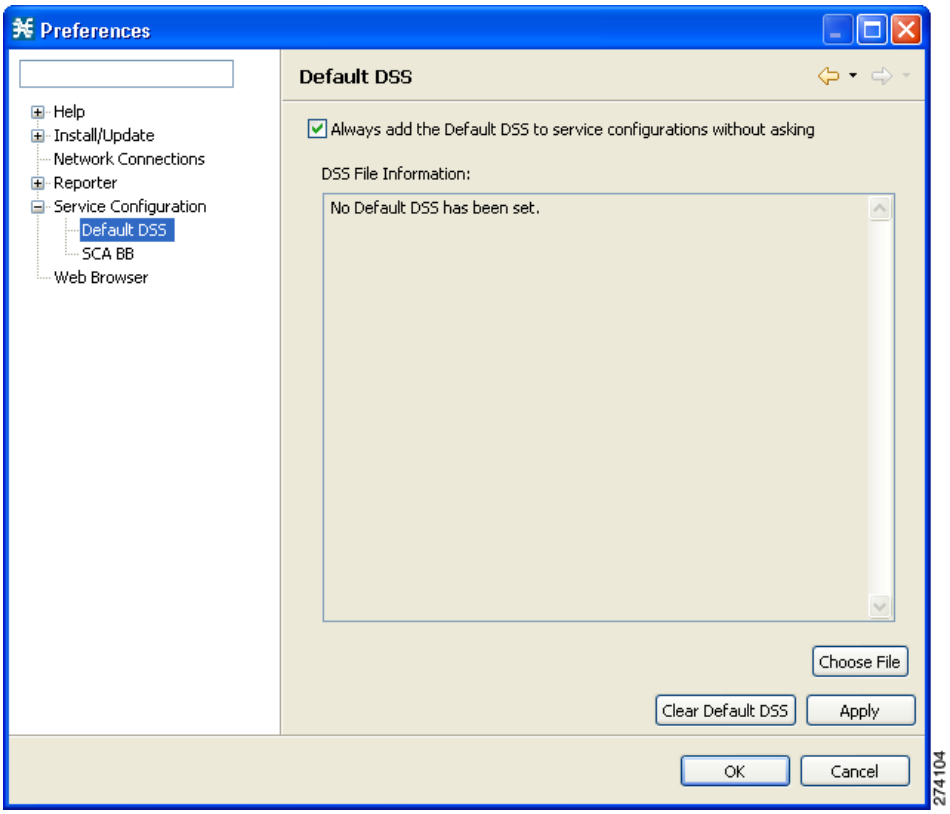
ステップ 1　Console のメイン メニューで、[Window] > [Preferences] の順に選択します。

[Preferences] ダイアログボックスが表示されます（図 7-40）。

ステップ 2　ダイアログボックスの左ペインのメニュー ツリーから、[Service Configuration] > [Default DSS] を選択します。

ダイアログボックスの右ペインに、[Default DSS] 領域が表示されます。

図 7-40　[Preferences]



ステップ 3　[Choose File] をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 4　[Files of type] ドロップダウン リストで、プロトコル パックのファイル タイプを選択します。

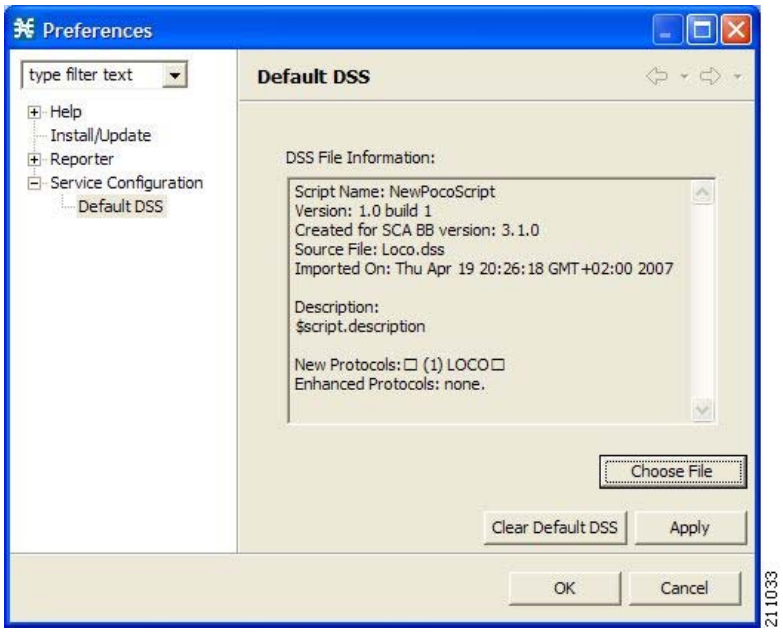
ステップ 5　プロトコル パックをブラウズします。

ステップ 6　[Open] をクリックします。

[Open] ダイアログボックスが閉じます。

[Preferences] ダイアログボックスの [Default DSS] 領域に、デフォルト DSS ファイルに関する情報が表示されます（図 7-41）。

図 7-41　[Preferences]：[Default DSS]



ステップ 7　[OK] をクリックします。

DSS ファイルが、デフォルト DSS ファイルとして、C:¥Documents and Settings¥<user name>¥.p-cube¥default3.1.7.dss にコピーされます。

[Preferences] ダイアログボックスが閉じます。

デフォルト DSS ファイルのクリア方法

ステップ 1　Console のメイン メニューで、[Window] > [Preferences] の順に選択します。

[Preferences] ダイアログボックスが表示されます。

ステップ 2　ダイアログボックスの左ペインのメニュー ツリーから、[Service Configuration] > [Default DSS] を選択します。

ダイアログボックスの右ペインに、[Default DSS] 領域が表示されます。

ステップ 3　[Clear Default DSS] をクリックします。

デフォルト DSS ファイル、C:¥Documents and Settings¥<user name>¥.p-cube¥default3.6.0.dss が削除されます。

[Default DSS] 領域のすべての情報が削除されます。

（注）　デフォルト DSS ファイルを削除しても、インポートされたダイナミック シグニチャは現在のサービス コンフィギュレーションから削除されません。

ステップ 4　[OK] をクリックします。

[Preferences] ダイアログボックスが閉じます。

デフォルト DSS ファイルからのダイナミック シグニチャのインポート

デフォルト DSS ファイルがインストールされている場合、新しいサービス コンフィギュレーションを作成するとき、または開こうとする既存のサービス コンフィギュレーションにシグニチャがインポートされていないときに、デフォルト DSS ファイルからダイナミック シグニチャをインポートするよう指示されます。または、ダイナミック シグニチャを手動でインポートすることもできます。

- 「デフォルト DSS ファイルを自動的にインポートする方法」（P.7-46）
- 「デフォルト DSS ファイルを手動でインポートする方法」（P.7-46）

デフォルト DSS ファイルを自動的にインポートする方法

ステップ 1　既存のサービス コンフィギュレーションを開くか、または新しいサービス コンフィギュレーションを作成します。

[Default Signature] メッセージが表示されます（図 7-42）。

図 7-42　[Default Signature]

ステップ 2　デフォルト DSS ファイルをインポートする場合は [Yes] を、デフォルト DSS ファイルをインポートせずに処理を続行する場合は [No] をクリックします。

デフォルト DSS ファイルを手動でインポートする方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Signatures Settings] の順に選択します。

[Signatures Settings] ダイアログボックスが表示されます（図 7-43）。

ステップ 2　[Signatures Script] タブをクリックします。

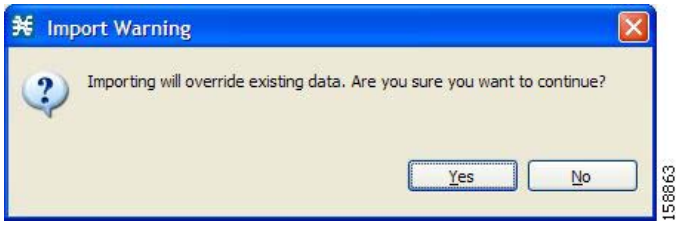
[Signatures Script] タブが開き、[Import Default DSS] ボタンがイネーブルになります。

図 7-43　[Signatures Settings]

ステップ 3　[Import Default DSS] をクリックします。

[Import Warning] メッセージが表示されます（図 7-44）。

図 7-44　[Import Warning]



ステップ 4　[Yes] をクリックします。

デフォルト DSS ファイルのシグニチャが、サービス コンフィギュレーションにインポートされます。

[Import Default DSS] ボタンがグレー表示になります。

インポートされたシグニチャとデフォルト DSS ファイルに関する情報が、[Signatures Settings] ダイアログボックスに表示されます。

ステップ 5　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

フレーバの管理

フレーバとは、ネットワーク セッションを細かく分類するための要素です。

フレーバは、特定のレイヤ 7 プロパティに基づいています。たとえば、ユーザは、HTTP フローの宛先 URL のさまざまな部分に基づいて、HTTP フローをサービスに関連付けることができます。

フレーバは一部のプロトコルに限定してサポートされており、このようなプロトコルでは、それぞれ使用可能なフレーバ タイプが異なります。フレーバ タイプを、次のセクションの表に一覧表示します。

各フレーバ タイプごとに、フレーバ項目の最大数の制限があります（「フレーバ タイプごとのフレーバ項目の最大数」（P.7-55）を参照）。各フレーバ タイプにおいて、それぞれのフレーバ項目は一意でなければなりません。

（注）　アクティブなサービス コンフィギュレーションで単方向分類が有効になっている場合、フレーバはトラフィック分類には使用されません。

フレーバ タイプとパラメータ

フレーバは、ネットワーク セッションをシグニチャ固有のレイヤ 7 プロパティに基づいて詳細に分類するための要素です。

レイヤ 7 アプリケーション プロパティが HTTP ユーザ エージェントなどでセッション パラメータとして使用された場合、それらのプロパティは文字列として処理されます。

レイヤ 7 パラメータベースのフレーバ項目は、レイヤ 7 プレフィクス（パラメータの先頭）、レイヤ 7 サフィックス（パラメータの末尾）、またはプレフィクスとサフィックスの組み合わせに適用されます。プレフィクスの場合は部分文字列の後ろに「*」を、サフィックスの場合は部分文字列の前に「*」を付加する必要があります。

表 7-1 に、使用可能なフレーバ タイプを示します。

表 7-1　SCA BB のフレーバ

フレーバ タイプ	照合されるセッション パラメータ	有効な値
HTTP Composite	HTTP User Agent、HTTP URL、HTTP Cookie、および HTTP Referer フレーバがセッション パラメータとして機能します。	<HTTP User Agent フレーバ, HTTP URL フレーバ, HTTP Cookie フレーバ, HTTP Referer フレーバ> • フレーバはフレーバ ブラウジングを使用して選択できます。
HTTP User Agent	HTTP <User-Agent プレフィクス> Request ヘッダー フィールドの Request ヘッダーの先頭から最初の「/」までを抽出した HTTP ユーザ エージェント。 たとえば､HTTP Request ヘッダー フィールドが Mozilla/4.0 の場合、抽出される HTTP User Agent は Mozilla です。	<User-Agent プレフィクス> 例： • <Moz*> は、「Moz」で始まる User-Agent フィールドを持つすべての HTTP セッションと一致します。 • <Mozilla> は、「Mozilla」と同じ User-Agent フィールドを持つすべての HTTP セッションと一致します。 • キーの最大長は 32 文字です。
HTTP URL	• ホスト：HTTP Host ヘッダー フィールドまたは Request URL から抽出。後者の場合、URL の先頭から最初の「/」までがホストと見なされます。 • パス：HTTP URL の最初の「/」から「?」までの部分を抽出。 • URL パラメータ：「?」のあとに続く文字列（このパラメータ プレフィクスは、「?」で始まっている必要はありません）。	< ホスト サフィックス , パス プレフィクス , パス サフィックス , URL パラメータ プレフィクス > • 1 つ以上のパラメータを指定する必要があります。未指定のパラメータは「*」として残しておきます。 • たとえば、次のようになります。 <*cisco.com,*,*,*> は、パスとパラメータの値に関係なく、「cisco.com」で終わるホストを持つすべての HTTP セッションと一致します。 • キーの最大長は 512 文字です。
HTTP Cookie	HTTP Request ヘッダーの Cookie フィールドから抽出された Cookie の「キーと値」のペア。 Cookie が多数の「キーと値」ペアで構成されている場合もありますが、計算されるのは最初の 3 ペアだけです。「キーと値」ペアのうちいずれか 1 つが指定された値と一致するか、Cookie が 3 ペアの制限を超えている場合、Cookie フレーバの計算は停止します。	< キー プレフィクス , 値プレフィクス > • 例：<act*,*> は、値に関係なく、キーが「act」で始まる Cookie ペアと一致します。 • Value フィールドが空になるようにフレーバを設定することができます。その場合は、フレーバ項目の Value フィールドを空にしておきます。 • 空白スペースと「=」は使用できません。「*」は、キーまたは値の末尾にだけ使用できます。 • Key および Value フィールドのキーの最大長は 100 文字です。

表 7-1　SCA BB のフレーバ（続き）

フレーバ タイプ	照合されるセッション パラメータ	有効な値
HTTP Referer	HTTP URL と似ていますが、パラメータは Referer HTTP ヘッダー フィールドから抽出されます。	<ホスト サフィックス, パス プレフィクス, パス サフィックス, URL パラメータ プレフィクス> • 1 つ以上のパラメータを指定する必要があります。未指定のパラメータは「*」として残しておきます。 • 例：<*cisco.com,*,*,*> は、パスとパラメータの値に関係なく、「cisco.com」で終わるホストを持つすべての HTTP セッションと一致します。 • すべてのキーの最大長は 512 文字です。
HTTP Content Category	コンテンツ カテゴリは、[Import] ダイアログボックスまたは [HTTP Content Filtering Settings] ダイアログボックスを使用してインポートできます。	[Select a Content Category] ダイアログボックスで選択した値。
RTSP User Agent	RTSP メッセージ ヘッダーから抽出された RTSP User-Agent フィールド。	<RTSP User Agent プレフィクス> • 例：<abc*> は、User-Agent が「abc」で始まるすべての RTSP セッションと一致します。 • キーの最大長は 128 文字です。
RTSP Host Name	RTSP メッセージ ヘッダーから抽出された RTSP Host フィールド。	<RTSP Host サフィックス> • 例：<*abc> は、Host が「abc」で終わるすべての RTSP セッションと一致します。 • キーの最大長は 128 文字です。
RTSP Composite	RTSP User Agent および RTSP Host Name フレーバがセッション パラメータとして機能します。	<RTSP User Agent フレーバ, RTSP Host Name フレーバ>
SIP Source Domain	SIP メッセージ ヘッダーから抽出された SIP Source Host フィールド。	<SIP Host サフィックス> • 例：<*abc> • キーの最大長は 128 文字です。
SIP Composite	SIP Source Host および SIP Destination Host がセッション パラメータとして機能します。	<SIP Source Domain, SIP Destination Domain>
SIP Destination Domain	SIP メッセージ ヘッダーから抽出された SIP Destination Host フィールド。	<SIP Host サフィックス> • 例：<*abc> • キーの最大長は 128 文字です。
SMTP Host Name	SMTP メッセージ ヘッダーから抽出された SMTP Host フィールド。	<SMTP Host サフィックス> • 例：<*abc> • キーの最大長は 128 文字です。
ToS	IP ヘッダーから抽出された Differentiated Service Code Point（DSCP; Diffserv コード ポイント）値。	DSCP ToS（0 ～ 63 の整数）

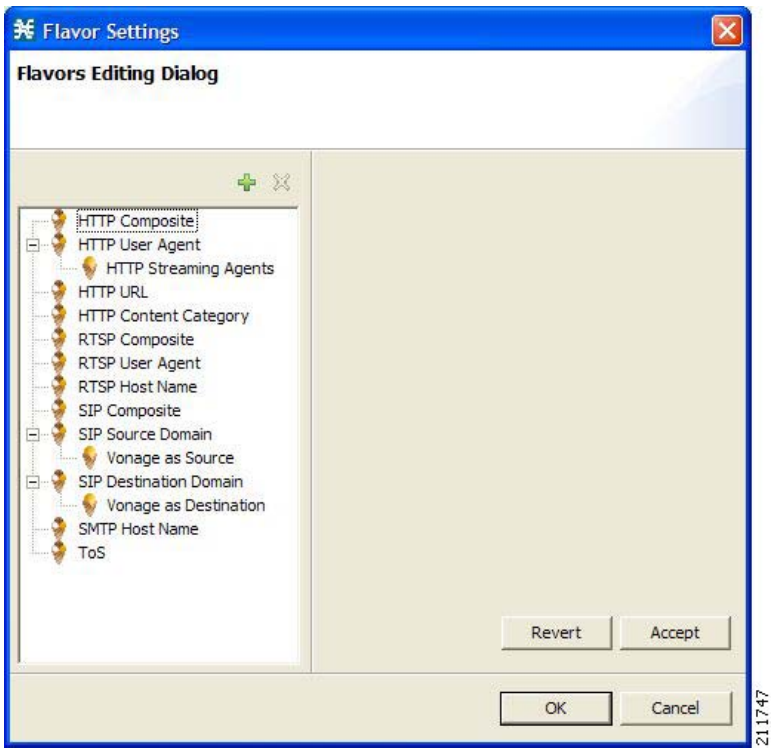
（注）　Composite フレーバは、定義された 2 つのフレーバのペアです。

フレーバの表示方法

フレーバのリストと、関連するフレーバ項目を表示できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。[Flavor Settings] ダイアログボックスが表示されます（図 7-45）。

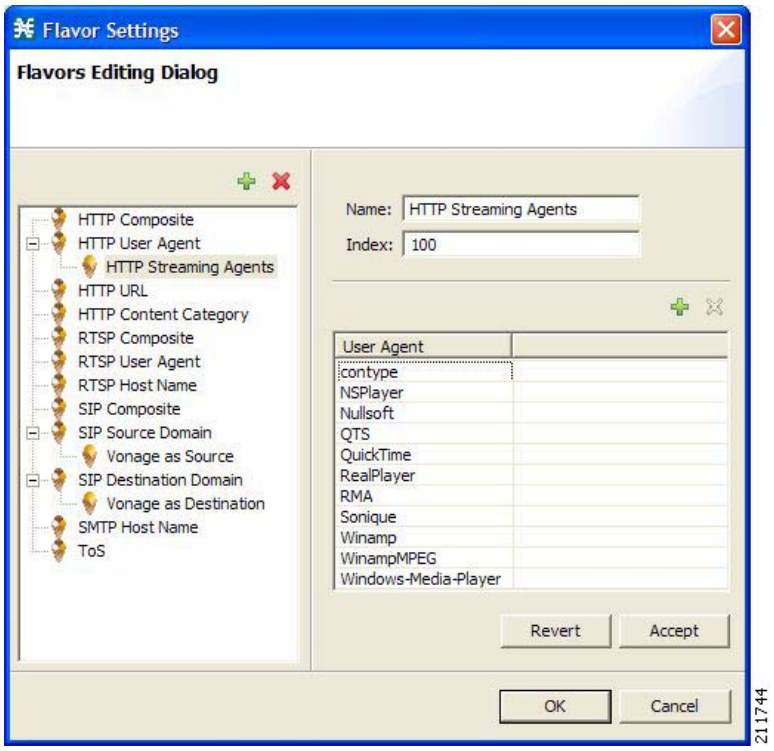
図 7-45　[Flavor Settings]



左の領域に、各フレーバ タイプのすべてのフレーバが、ツリー形式で表示されます。

ステップ 2　フレーバ項目を表示するには、ツリー内のフレーバをクリックします（図 7-46）。

図 7-46　[Flavor Settings]



右の領域に、フレーバ項目が表示されます。

ステップ 3　[OK] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

フレーバの追加方法

CSV ファイルからフレーバをインポートできます。CSV ファイルは、フレーバをエクスポートして作成することも、『*Cisco Service Control Application Suite for Broadband Reference Guide*』の「CSV File Formats」のように手動で作成することもできます。

サービス コンフィギュレーションに、任意の数のフレーバを追加できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

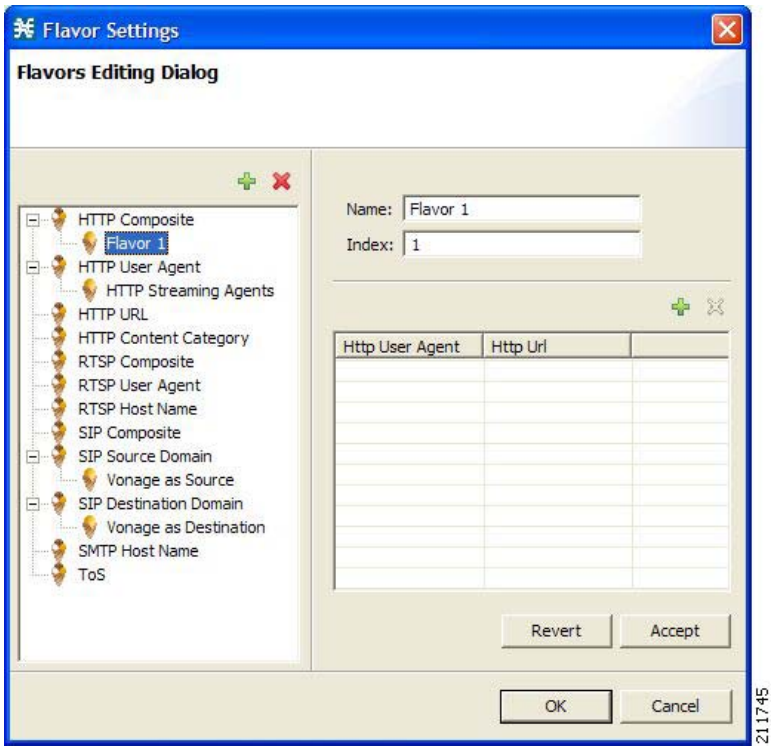
[Flavor Settings] ダイアログボックスが表示されます（図 7-47）。

ステップ 2　フレーバ ツリーでフレーバ タイプを選択します。

ステップ 3　 をクリックします。

フレーバ ツリーに、選択したタイプの新しいフレーバが追加されます。

図 7-47　[Flavor Settings]



ステップ 4　[Name] フィールドに、新しいフレーバの名前を入力します。

（注）　フレーバにはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

ステップ 5　（オプション）[Index] フィールドに、一意の整数値を入力します。

（注）　Index の値は、SCA BB によって割り当てられます。これは変更する必要はありません。

フレーバのインデックスは、1 ～ 32767 の正の整数でなければなりません。

これでフレーバは定義されました。フレーバ項目を追加できます（「フレーバ項目の追加方法」（P.7-55）を参照）。

フレーバの編集方法

フレーバ パラメータは、いつでも修正できます。

フレーバ項目の追加、変更、または削除を行う場合は、「フレーバ項目の管理」（P.7-55）を参照してください。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

[Flavor Settings] ダイアログボックスが表示されます。

ステップ 2　フレーバ ツリーでフレーバを選択します。

右の領域に、フレームの名前とインデックス（およびそのフレーム項目）が表示されます。

ステップ 3　ダイアログボックスのフィールドを次のように修正します。

- [Name] フィールドに、フレーバの新しい名前を入力します。
- [Index] フィールドに、フレーバの新しく一意のインデックスを入力します。

  フレーバのインデックスは、1 ～ 32767 の正の整数でなければなりません。

ステップ 4　[OK] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

フレーバの削除方法

任意のフレーバ、またはすべてのフレーバを削除できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

[Flavor Settings] ダイアログボックスが表示されます。

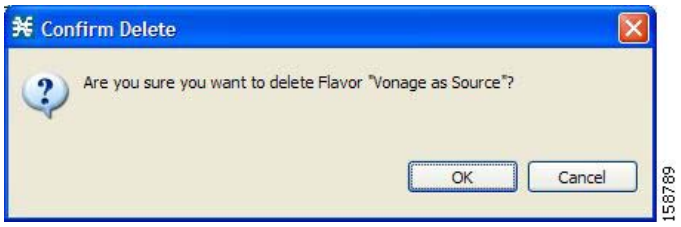
ステップ 2　フレーバ ツリーでフレーバを右クリックします。

ポップアップ メニューが表示されます。

ステップ 3　  （[Delete]）をクリックします。

[Confirm Delete] メッセージが表示されます（図 7-48）。

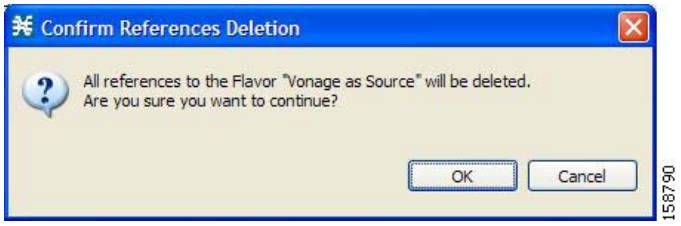
図 7-48　[Confirm Delete]



ステップ 4　[OK] をクリックします。

- 選択したフレーバを参照するサービス要素がある場合、[Confirm References Delete] メッセージが表示されます（図 7-49）。

図 7-49　[Confirm References Deletion]



- [Yes] をクリックします。

  選択したフレーバを参照するサービス要素が削除されます。

フレーバが削除され、フレーバ ツリーに表示されなくなります。

ステップ 5　[Close] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

フレーバ項目の管理

フレーバとは、関連するフレーバ項目の集合です。

フレーバ項目とは、フローの 1 つまたは複数のプロパティの値です。これらのプロパティはフレーバのタイプによって異なります（「フレーバ タイプとパラメータ」（P.7-48）を参照）。

各フレーバ タイプごとに、フレーバ項目の最大数の制限があります（次の項目を参照）。各フレーバ タイプにおいて、それぞれのフレーバ項目は一意でなければなりません。

- 「フレーバ タイプごとのフレーバ項目の最大数」（P.7-55）
- 「フレーバ項目の追加方法」（P.7-55）
- 「フレーバ項目の編集方法」（P.7-57）
- 「フレーバ項目の削除方法」（P.7-58）

フレーバ タイプごとのフレーバ項目の最大数

表 7-2 に、各フレーバ タイプのフレーバ項目の最大数を示します。

表 7-2　フレーバ タイプごとのフレーバ項目の最大数

フレーバ タイプ	フレーバ項目の最大数
HTTP Composite	10,000
HTTP User Agent	128
HTTP URL	100,000
HTTP Cookie	100
HTTP Referer	100
HTTP Content Category	—
RTSP Composite	10,000
RTSP User Agent	128
RTSP Host Name	10,000
SIP Composite	10,000
SIP Source Domain	128
SIP Destination Domain	128
SMTP Host Name	10,000
ToS	64

フレーバ項目の追加方法

フレーバには、任意の数のフレーバ項目を追加できます（ただし、1 つのサービス コンフィギュレーションにつき、設定可能なフレーバ項目のタイプの総数には制限があります）。

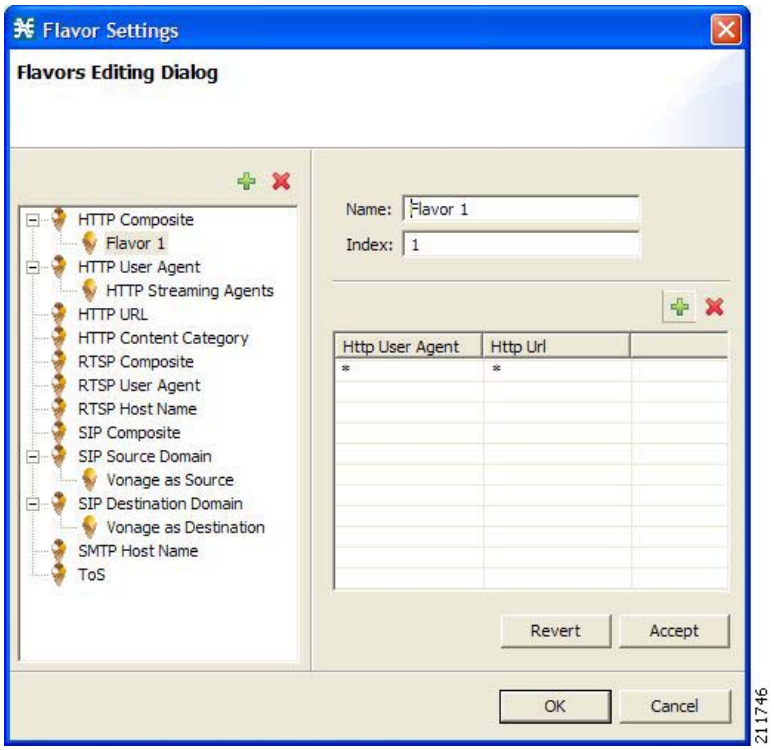
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

[Flavor Settings] ダイアログボックスが表示されます（図 7-50）。

ステップ 2　フレーバ ツリーでフレーバをクリックします。

ステップ 3　フレーバ項目リスト上で、（[Create New Flavor Item]）をクリックします。

図 7-50　[Flavor Settings]



フレーバ項目リストに、新しいフレーバ項目が追加されます。フレーバ項目のパラメータの数およびタイプは、フレーバ タイプによって異なります（「フレーバ タイプとパラメータ」（P.7-48）を参照）。

新しいフレーバ項目のデフォルト値は、すべてワイルドカード（アスタリスク、*）です。

ステップ 4　新しいフレーバ項目の各セルで、アスタリスクをクリックし、適切な値を入力します。

Composite フレーバと HTTP Content Category フレーバの場合は、次の手順を実行します。

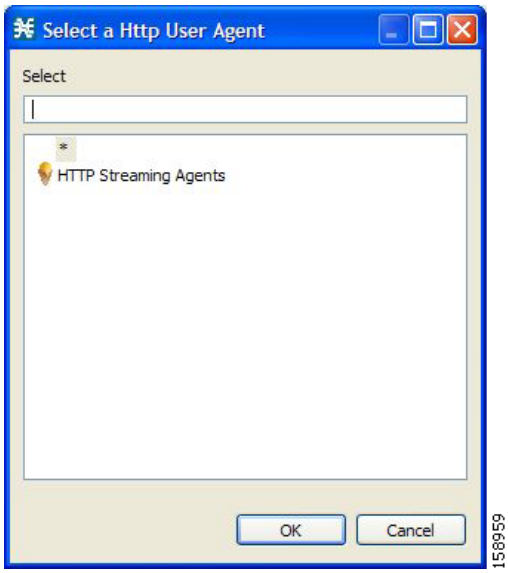
a.　アスタリスクをクリックします。

セルに [Browse] ボタンが表示されます。

b.　[Browse] ボタンをクリックします。

[Select] ダイアログボックスが開き（図 7-51）、そのパラメータの有効な値がすべて表示されます。

図 7-51　[Select a HTTP User Agent]



c. リストから適切な値を選択します。

d. [OK] をクリックします。

[Select] ダイアログボックスが閉じます。

該当するセルに、選択した値が表示されます。

ステップ 5　各フレーバ項目について、ステップ 3 と 4 を実行します。

ステップ 6　[OK] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

フレーバ項目の編集方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

[Flavor Settings] ダイアログボックスが表示されます。

ステップ 2　フレーバ ツリーでフレーバを選択します。

ステップ 3　フレーバ項目リストで、フレーバ項目を選択します。

ステップ 4　選択したフレーバ項目の各セルで、アスタリスクをクリックし、適切な値を入力します。

Composite フレーバと HTTP Content Category フレーバの場合は、次の手順を実行します。

a. アスタリスクをクリックします。

セルに [Browse] ボタンが表示されます。

b. [Browse] ボタンをクリックします。

[Select] ダイアログボックスが開き、そのパラメータの有効な値がすべて表示されます。

c. リストから適切な値を選択します。

d. [OK] をクリックします。

[Select] ダイアログボックスが閉じます。

該当するセルに、選択した値が表示されます。

ステップ 5　[OK] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

フレーバ項目の削除方法

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Flavors] の順に選択します。

[Flavor Settings] ダイアログボックスが表示されます。

ステップ 2　フレーバ ツリーでフレーバを選択します。

ステップ 3　フレーバ項目リストで、フレーバ項目の任意の場所を右クリックします。

ポップアップ メニューが表示されます。

ステップ 4　  （[Delete]）をクリックします。

フレーバが削除され、フレーバ項目リストに表示されなくなります。

ステップ 5　[Close] をクリックします。

[Flavor Settings] ダイアログボックスが閉じます。

例：URL リストのインポートおよび URL のブロック方法

次の例では、URL ファイルをインポートし、SCE を設定してこれらの URL をブロックする方法について説明します。

ステップ 1　「フレーバの追加方法」（P.7-52）で説明したように、HTTP URL フレーバ タイプの新しいフレーバを作成します。

ステップ 2　ブロックする URL が含まれた CSV ファイルをインポートします。

詳細については、「サービス コンフィギュレーション データのインポート方法」（P.6-10）を参照してください。

（注）　CSV ファイル形式については、『*Cisco Service Control Application Suit for Broadband Reference Guide*』の「CSV File Formats」の章を参照してください。

ステップ 3　サービスを定義します。

詳細については、「サービス コンフィギュレーションへのサービスの追加方法」(P.7-4)を参照してください。

ステップ 4　定義したサービスに、新しいフレーバを使用するサービス要素を追加します。

詳細については、「サービス要素の追加方法」（P.7-12）を参照してください。

ステップ 5　URL をブロックするパッケージに規則を追加し、それを新規サービスに関連付けます。

詳細については、「パッケージへの規則の追加」（P.9-58）を参照してください。

ステップ 6　フローをブロックする規則を設定します。

詳細については、「規則のためのフローごとのアクションの定義」（P.9-60）を参照してください。

コンテンツ フィルタリングの管理

コンテンツ フィルタリングでは、要求された URL に従って、HTTP フローの分類と制御を行います。URL の分類は、外部データベースにアクセスして行われます。

SCA BB では、SurfControl Content Portal Authority（CPA）サーバとの統合によりコンテンツ フィルタリングを提供しています。

（注）　単方向分類が有効になっている場合、コンテンツ フィルタリングはサポートされません。

コンテンツ フィルタリングについての情報

Cisco HTTP Content Filtering ソリューションは、次の項目で構成されます。

- SCE アプリケーション
- Cisco CPA クライアント
- SurfControl CPA サーバ

SCE アプリケーションは、CPA サーバから返されたカテゴリに従って、各 HTTP フローを分類します。この分類は、SCA BB トラフィック制御とレポートに使用されます。たとえば、ユーザは、「Adult/Sexually Explicit」カテゴリのブラウジングをブロックする規則や、「Kids」または「Shopping」カテゴリのブラウジングによって消費されたボリュームのレポートを生成する規則を定義できます。

SCE アプリケーション

Cisco Service Control Application は、SCE プラットフォーム上で動作します。トラフィックから抽出した HTTP URL を、CPA クライアントに転送し、カテゴリ化の結果に基づいて、サービスへの元の HTTP フローを分類します。この分類は、通常の SCA BB トラフィック制御とレポートに使用されます。

SCE アプリケーションは、Raw Data Record（RDR; 未加工データ レコード）を使用して CPA クライアントと通信します。「RDR フォーマッタの設定方法」（P.7-61）を参照してください。

Cisco CPA クライアント

Cisco CPA クライアントは、SCE プラットフォーム上で動作します。URL クエリーをカテゴリ化のために CPA サーバに送信し、カテゴリ化の結果に基づいて SCA BB をアップデートします。

CPA クライアントは、SCA BB アプリケーション（PQI）インストールの一部としてインストールされます。クライアントを設定およびモニタするには、SCE プラットフォーム Command-Line Interface（CLI; コマンドライン インターフェイス）（「コンテンツ フィルタリング CLI」（P.7-60）を参照）を使用します。

SurfControl CPA サーバ

CPA サーバは、専用のマシン上で動作します。CPA クライアントからカテゴリ化要求を受信し、SurfControl Content Database に接続し、照会された URL のカテゴリ ID を返します。

SurfControl CPA サーバは、SCE プラットフォームからアクセス可能な独立したサーバにインストールされます。インストールの詳細については、このマニュアルでは扱いません。

コンテンツ フィルタリング CLI

SurfControl CPA を使用するコンテンツ フィルタリングを設定およびモニタするには、SCE プラットフォーム コマンドライン インターフェイス（CLI）を使用します。SCE プラットフォーム CLI の詳細については、『*Cisco SCE8000 CLI Command Reference*』を参照してください。

CPA クライアント CLI コマンド

ここに示すコマンドについては、次のセクションで説明します。

- Cisco CPA クライアントの設定には、次の CLI コマンドを使用します。

```
[no] cpa-client
cpa-client destination <address> [port <port>]
cpa-client retries <number_of_retries>
```

- これらのコマンドは、ライン インターフェイス コンフィギュレーション コマンドです。これらのコマンドを実行するには、ライン インターフェイス コンフィギュレーション モードを開始する必要があります（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.7-62）を参照）。
- Cisco CPA クライアントの状態をモニタするには、EXEC モードで次の CLI コマンドを使用します。

```
show interface LineCard <slot> cpa-client
```

CPA クライアント CLI コマンドの説明

表 7-3 に、前のセクションで紹介した Cisco CPA クライアント CLI コマンドの説明と、そのデフォルト値を示します。

表 7-3　CPA クライアント CLI コマンド

コマンド	説明	デフォルト値
[no] cpa-client	CPA クライアントをイネーブルまたはディセーブルにします。	ディセーブル
cpa-client destination <address> [**port** <port>]	CPA クライアントをイネーブルにし、CPA サーバの IP アドレスとポートを設定します。	• Address：未定義 • Port：9020
cpa-client retries <number_of_retries>	CPA サーバへの送信のリトライ回数を設定します。	3
show interface LineCard <slot> **cpa-client**	CPA クライアントのステータスを監視します（次の表を参照）。	—

表 7-4 に、Cisco CPA クライアントのモニタリング時に表示される情報を示します。

表 7-4　CPA クライアント：モニタされるパラメータ

パラメータ	説明
[Mode]	イネーブルまたはディセーブル
[CPA Address]	—
[CPA Port]	—
[CPA Retries]	—
[Status]	（イネーブルの場合）アクティブまたはエラー（および最後のエラーの説明）
[Counters]	• 成功したクエリーの数 • サーバ応答がないために失敗したクエリーの数 • ペンディングのクエリーの数 • 1 秒あたりのクエリー数（直前の 5 秒間の平均）
[Timestamps]	• CPA の開始 • 最後のクエリー • 最後の応答 • 最後のエラー

RDR フォーマッタの設定方法

RDR フォーマッタでの HTTP カテゴリ化要求の発行を有効にするには、SCE プラットフォームで RDR フォーマッタを設定します。

ステップ 1　適切な SCE プラットフォーム CLI コマンドを発行します。

```
#>RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100
```

関連情報

RDR フォーマッタの設定については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」または『*Cisco SCE8000 GBE Software Configuration Guide*』の「Raw Data Formatting: The RDR Formatter and NetFlow Exporting」を参照してください。

ライン インターフェイス コンフィギュレーション モードの開始方法

ライン インターフェイス コンフィギュレーション コマンドを実行するには、ライン インターフェイス コンフィギュレーション モードを開始し、`SCE(config if)#` プロンプトを表示する必要があります。

ステップ 1　SCE プラットフォームの CLI プロンプト `(SCE#)` で `configure` と入力します。

ステップ 2　**Enter** キーを押します。

`SCE(config)#` プロンプトが表示されます。

ステップ 3　`interface LineCard 0` を入力します。

ステップ 4　**Enter** キーを押します。

`SCE(config if)#` プロンプトが表示されます。

コンテンツ フィルタリング設定の管理

HTTP URL コンテンツ フィルタリングを適用するには、Service Configuration Editor で次の手順を実行する必要があります。

1. サービス コンフィギュレーションにコンテンツ フィルタリング コンフィギュレーション ファイルをインポートします。

   デフォルトでは、SCA BB では、コンテンツ カテゴリごとに個別のフレーバ（HTTP Content Category タイプの）が作成され、新しいフレーバごとにサービス要素が作成されます。新しいトップレベル サービス「HTTP Browsing with Categories」が作成され、これらのサービス要素がその下に作成されます。

2. 新しいサービスを作成し、新しいカテゴリ フレーバをマッピングします。
3. 既存のパッケージにコンテンツ フィルタリング規則を追加するか、またはコンテンツ フィルタリング規則を持つ新しいパッケージを作成します。
4. 選択したパッケージに対して、コンテンツ フィルタリングを有効にします。
5. サービス コンフィギュレーションを適用します。

- 「コンテンツ フィルタリング カテゴリのインポート」（P.7-63）
- 「コンテンツ フィルタリングの設定方法」（P.7-69）
- 「コンテンツ フィルタリング設定の表示方法」（P.7-70）
- 「コンテンツ フィルタリング設定の削除方法」（P.7-71）

コンテンツ フィルタリング カテゴリのインポート

コンテンツに基づいて HTTP フローを制御するには、インストールにより提供される XML ファイルをインポートする必要があります。

インストール パッケージを解凍すると、このファイルが URL Filtering サブフォルダに格納されます。

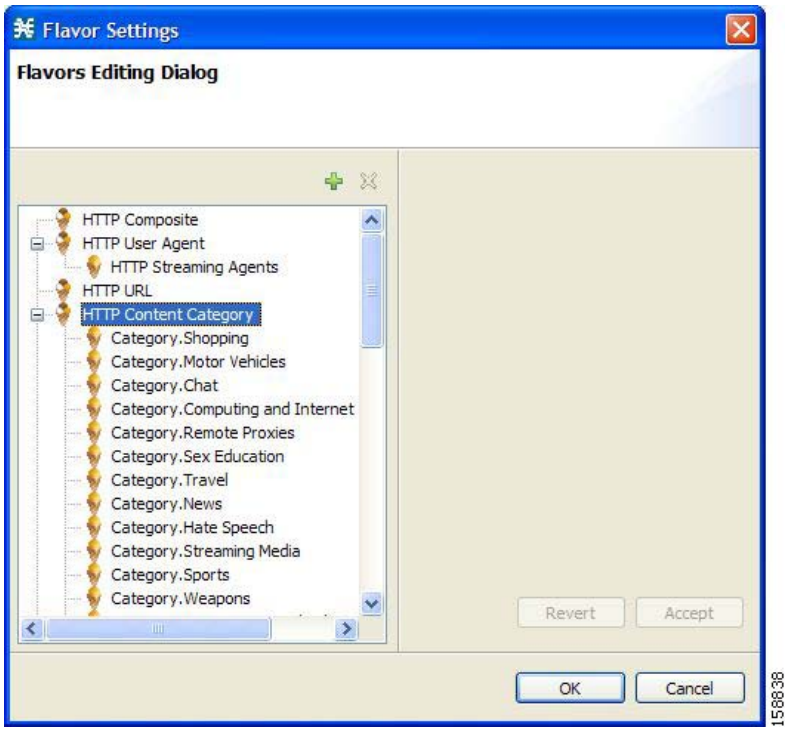
（注）　単方向分類が有効になっている場合、コンテンツ フィルタリング カテゴリはインポートできません。

- 「HTTP Content Category フレーバ」（P.7-63）
- 「カテゴリ サービス要素による HTTP ブラウジング」（P.7-64）
- 「[Import] ダイアログボックスを使用したコンテンツ フィルタリング カテゴリのインポート」（P.7-64）
- 「[HTTP Content Filtering Settings] ダイアログボックスを使用したコンテンツ フィルタリング カテゴリのインポート方法」（P.7-68）

HTTP Content Category フレーバ

デフォルトでは、SCA BB では、XML ファイルのインポート時に、コンテンツ カテゴリごとに個別のフレーバ（HTTP Content Category タイプ）が作成されます（図 7-52）。

図 7-52　[Flavor Settings]

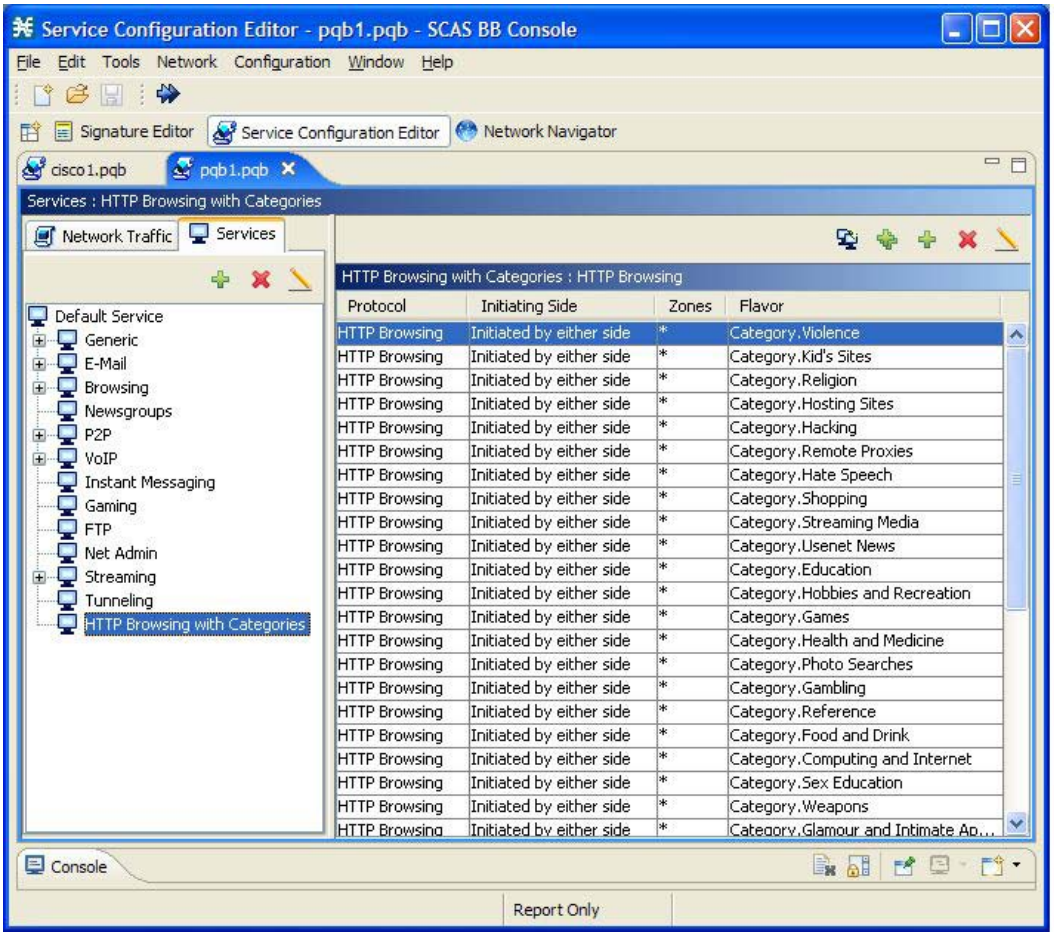


2 つ以上のコンテンツ カテゴリを含む HTTP Content Category フレーバを作成することもできます（「フレーバの追加方法」（P.7-52）を参照）。

カテゴリ サービス要素による HTTP ブラウジング

デフォルトでは、SCA BB は XML ファイルのインポート時に作成される各フレーバに対してサービス要素を作成します。新しいトップレベル サービス「HTTP Browsing with Categories」が作成され、これらのサービス要素がその下に作成されます（図 7-53）。

図 7-53　Service Configuration Editor



（注） この新しいサービスを表示するには、サービス コンフィギュレーションを保存して閉じてから、再度開く必要があります。

[Import] ダイアログボックスを使用したコンテンツ フィルタリング カテゴリのインポート

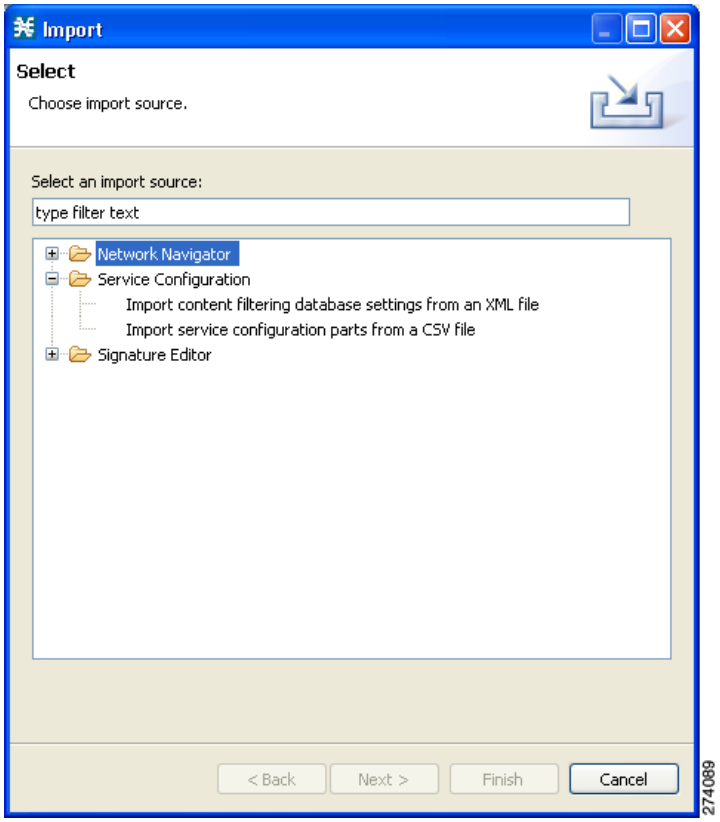
コンテンツ フィルタリング カテゴリをインポートするには、[File] > [Import] メニュー オプションまたは [Configuration] > [Content Filtering] メニュー オプションを使用します。

ここでは、[File] > [Import] メニュー オプションを使用するインポートの手順を説明します。

（注） これは、次の手順と同等です。

ステップ 1　Console のメイン メニューで、[File] > [Import] の順に選択します。
[Import] ダイアログボックスが表示されます（図 7-54）。

図 7-54　[Import]

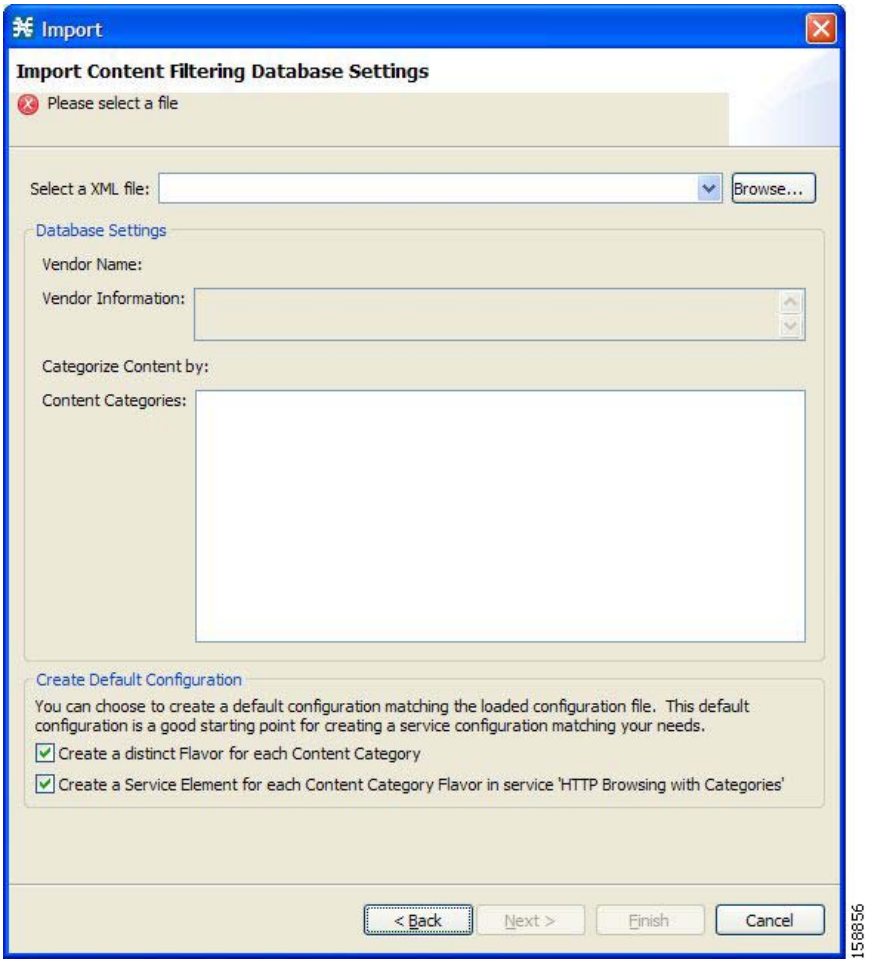


ステップ 2　インポート元リストから [Import content filtering database settings from XML file] を選択します。

ステップ 3　[Next] をクリックします。

[Import Content Filtering Database Settings] ダイアログボックスが表示されます（図 7-55）。

図 7-55　[Import Content Filtering Database Settings]



ステップ 4　[Select a XML file] フィールドの隣の [Browse] ボタンをクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 5　インポートするファイルのあるフォルダをブラウズし、該当ファイルを選択します。

（注）　SurfControl の CPA の場合、ファイル名は surfcontrol.xml となります。

ステップ 6　[Open] をクリックしてファイルを選択します。

[Open] ダイアログボックスが閉じます。

XML ファイルの内容に関する情報が、[Import Content Filtering Database Settings] ダイアログボックスの [Database Settings] ペインに表示されます。

ステップ 7　デフォルトでは、SCA BB では、XML ファイルのインポート時に、コンテンツ カテゴリごとに個別のフレーバ（HTTP Content Category タイプの）が作成されます。

- このオプションをディセーブルにするには、[Create a distinct Flavor for each Content Category] チェックボックスをオフにします。

（注）　このオプションはディセーブルにしないことを推奨します。

ステップ 8　デフォルトでは、SCA BB では前のステップで作成したフレーバごとにサービス要素が作成されます。新しいトップレベル サービス「HTTP Browsing with Categories」が作成され、これらのサービス要素がその下に作成されます。

- このオプションをディセーブルにするには、[Create a Service Element for each Content Category Flavor in Service ‘HTTP Browsing with Categories’] チェックボックスをオフにします。

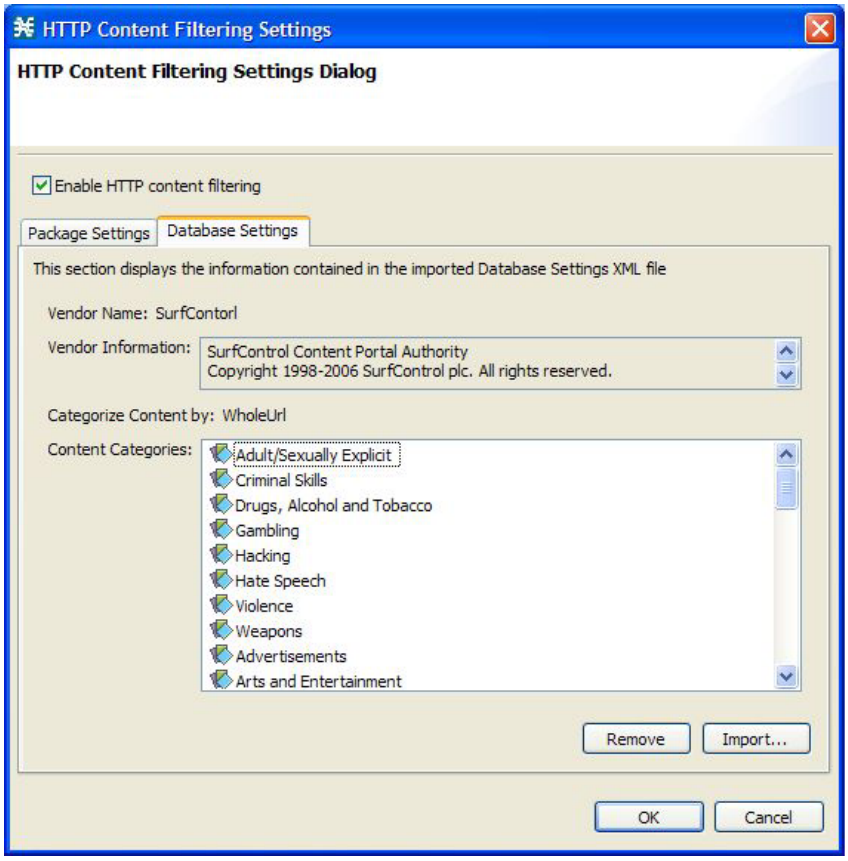
（注）　このオプションはディセーブルにしないことを推奨します。

ステップ 9　[Finish] をクリックします。

[Import Content Filtering Database Settings] ダイアログボックスが閉じます。

インポートされたファイルの情報が、[HTTP Content Filtering Settings] ダイアログボックスの [Database Settings] タブに表示されます（図 7-56）。

図 7-56　[HTTP Content Filtering Settings]



ステップ 10　[OK] をクリックします。

[HTTP Content Filtering Settings] ダイアログボックスが閉じます。

[HTTP Content Filtering Settings] ダイアログボックスを使用したコンテンツ フィルタリング カテゴリのインポート方法

コンテンツ フィルタリング カテゴリをインポートするには、[File] > [Import] メニュー オプションまたは [Configuration] > [Content Filtering] メニュー オプションを使用します。

ここでは、[Configuration] > [Content Filtering] メニュー オプションを使用するインポートの手順を説明します。

（注）　これは、「[Import] ダイアログボックスを使用したコンテンツ フィルタリング カテゴリのインポート」（P.7-64）の手順と同等です。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Content Filtering] の順に選択します。

[HTTP Content Filtering Settings] ダイアログボックスが表示されます。

ステップ 2　[Database Settings] タブをクリックします。

[Database Settings] タブが開きます。

ステップ 3　[Import] をクリックします。

[Import Content Filtering Database Settings] ダイアログボックスが表示されます。

ステップ 4　[Select a XML file] フィールドの隣の [Browse] ボタンをクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 5　インポートするファイルのあるフォルダをブラウズし、該当ファイルを選択します。

（注）　SurfControl の CPA の場合、ファイル名は surfcontrol.xml となります。

ステップ 6　[Open] をクリックしてファイルを選択します。

[Open] ダイアログボックスが閉じます。

XML ファイルの内容に関する情報が、[Import Content Filtering Database Settings] ダイアログボックスの [Database Settings] ペインに表示されます。

ステップ 7　デフォルトでは、SCA BB では、XML ファイルのインポート時に、コンテンツ カテゴリごとに個別のフレーバ（HTTP Content Category タイプの）が作成されます。

- このオプションをディセーブルにするには、[Create a distinct Flavor for each Content Category] チェックボックスをオフにします。

（注）　このオプションはディセーブルにしないことを推奨します。

ステップ 8　デフォルトでは、SCA BB では前のステップで作成したフレーバごとにサービス要素が作成されます。新しいトップレベル サービス「HTTP Browsing with Categories」が作成され、これらのサービス要素がその下に作成されます。

- このオプションをディセーブルにするには、[Create a Service Element for each Content Category Flavor in Service ‘HTTP Browsing with Categories’] チェックボックスをオフにします。

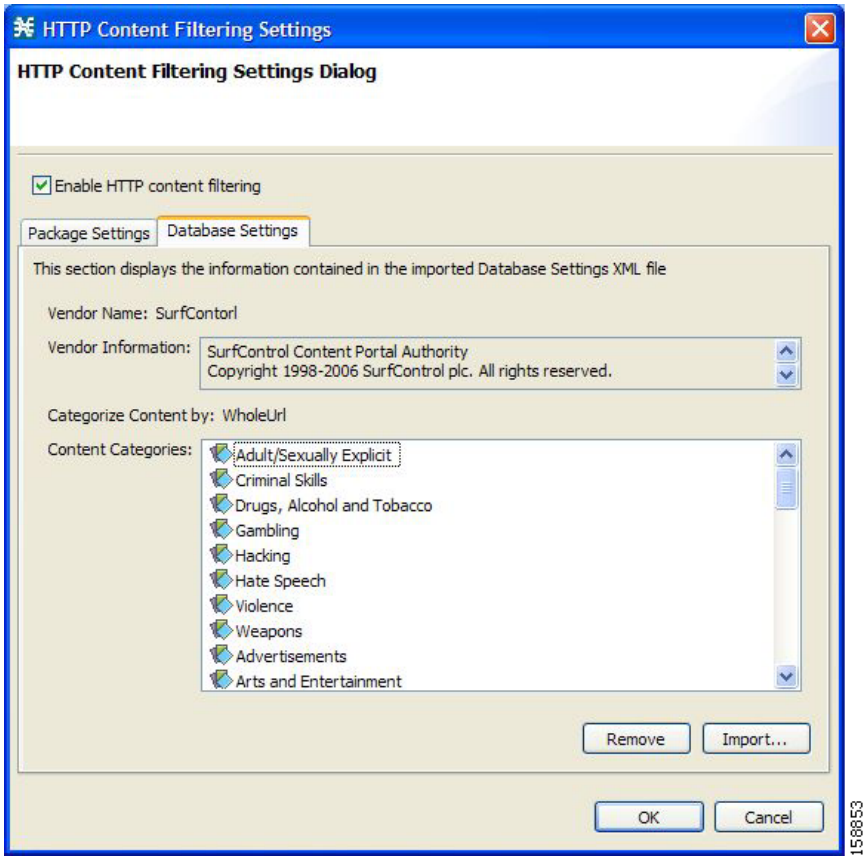
（注）　このオプションはディセーブルにしないことを推奨します。

ステップ 9　[Finish] をクリックします。

[Import Content Filtering Database Settings] ダイアログボックスが閉じます。

インポートされたファイルの情報が、[HTTP Content Filtering Settings] ダイアログボックスの [Database Settings] タブに表示されます（図 7-57）。

図 7-57　[HTTP Content Filtering Settings]



ステップ 10　[OK] をクリックします。

[HTTP Content Filtering Settings] ダイアログボックスが閉じます。

コンテンツ フィルタリングの設定方法

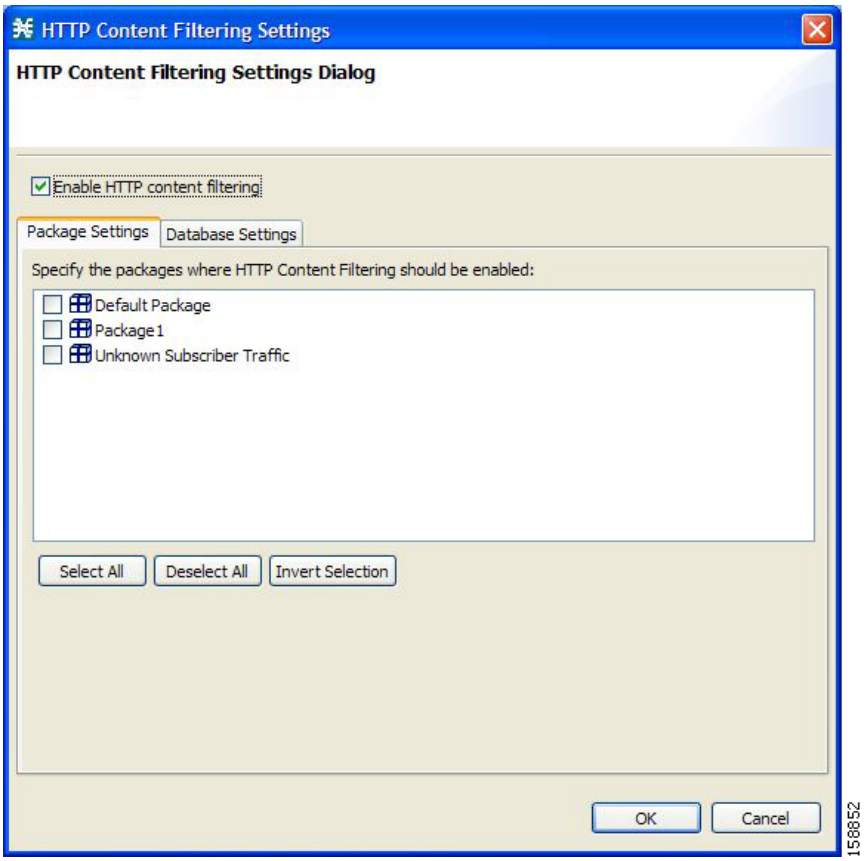
コンテンツ フィルタリングを有効にするパッケージを指定できます。コンテンツ フィルタリングを無効にしたパッケージでは、HTTP フローが通常通り分類されます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Content Filtering] の順に選択します。

[HTTP Content Filtering Settings] ダイアログボックスが表示されます（図 7-58）。

[Package Settings] タブに、現在のサービス コンフィギュレーション用に定義された全パッケージのリストが表示されます。

図 7-58　[HTTP Content Filtering Settings]



ステップ 2　[Enable HTTP content filtering] チェックボックスをオンにします。

ステップ 3　コンテンツ フィルタリングを適用するパッケージの隣のチェックボックスをオンにします。

ステップ 4　[OK] をクリックします。

[HTTP Content Filtering Settings] ダイアログボックスが閉じます。

コンテンツ フィルタリング設定の表示方法

コンテンツ フィルタリングをイネーブルにするかどうか、どのパッケージにコンテンツ フィルタリングを適用するか、またコンテンツ フィルタリングのベンダーと、ベンダーのコンテンツ カテゴリに関する情報を表示できます。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Content Filtering] の順に選択します。

[HTTP Content Filtering Settings] ダイアログボックスが表示されます。

[Package Settings] タブに、現在のサービス コンフィギュレーション用に定義された全パッケージのリストと、コンテンツ フィルタリングが有効になっているパッケージが表示されます。

ステップ 2　[Database Settings] タブをクリックします。

[Database Settings] タブが開きます。

このタブに、コンテンツ フィルタリングのベンダーとベンダーのコンテンツ カテゴリに関する情報が表示されます。

ステップ 3　[OK] をクリックします。

[HTTP Content Filtering Settings] ダイアログボックスが閉じます。

コンテンツ フィルタリング設定の削除方法

コンテンツ フィルタリング設定は、いつでも削除できます。

設定を削除するには、次の手順を実行します。

- フレーバからコンテンツ カテゴリ フレーバ項目を削除します。
- コンテンツ カテゴリ フレーバ項目をすべて削除します。
- コンテンツ フィルタリングをディセーブルにします。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Content Filtering] の順に選択します。

[HTTP Content Filtering Settings] ダイアログボックスが表示されます。

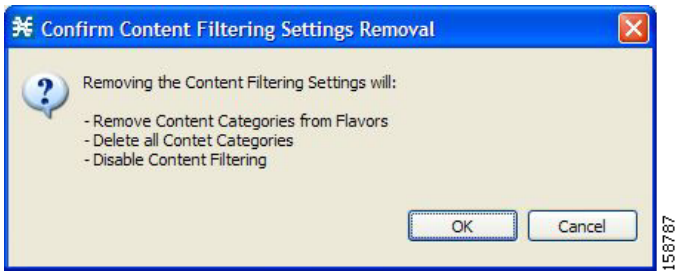
ステップ 2　[Database Settings] タブをクリックします。

[Database Settings] タブが開きます。

ステップ 3　[Remove] をクリックします。

[Confirm Content Filtering Settings Removal] ダイアログボックスが表示されます（図 7-59）。

図 7-59　[Confirm Content Filtering Settings Removal]



ステップ 4　[OK] をクリックします。

コンテンツ フィルタリング設定がすべて削除されます。

[HTTP Content Filtering Settings] ダイアログボックスから、ベンダー名、ベンダー情報、コンテンツ カテゴリが削除されます。

ステップ 5　[OK] をクリックします。

[HTTP Content Filtering Settings] ダイアログボックスが閉じます。

- [Generic Protocols]：トランザクション用の汎用 IP、汎用 TCP、および汎用 UDP プロトコルで、他のプロトコル タイプによって特定のプロトコルにマッピングされていないもの。
- [IP Protocols]：TCP/UDP 以外のプロトコル（ICMP など）。トランザクションの IP プロトコル番号に従って識別されます。
- [Port-Based Protocols]：既知のポートに従って分類される TCP および UDP プロトコル。デフォルトのサービス コンフィギュレーションには、750 を超える一般的なポートベース プロトコルが含まれています。

- [Signature-Based Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類されたプロトコル。HTTP や FTP など最も一般的なプロトコル、および多数の一般的な P2P プロトコルが含まれます。
- [P2P Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類されたピアツーピア ファイル共有アプリケーション プロトコル。
- [VOIP Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された Voice over IP（VoIP）アプリケーション プロトコル。
- [SIP Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された、SIP プロトコル、または SIP 特性を持つプロトコル。
- [Worm Protocols]：レイヤ 7 アプリケーション シグニチャに従って分類された、インターネット ワームのトラフィック パターンに基づくプロトコル。
- [Packet Stream Pattern-Based Protocols]: レイヤ 7 アプリケーション シグニチャに従って分類されたプロトコルで、パケットのペイロード内容ではなくパケット ストリームのパターン（たとえば、ストリームのシンメトリ、平均パケット サイズ、転送速度など）に基づくプロトコル。
- [Unidirectionally Detected Protocols]：単方向シグニチャを持つプロトコル。

（注） 複数のカテゴリに属するプロトコルもあります。特に、あらかじめ定義された P2P、VOIP、SIP、Worm、および Packet Stream Pattern-Based Protocols は、Signature-Based Protocols としても定義されています。

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [Protocols] の順に選択します。

[Protocol Settings] ダイアログボックスが表示されます。

ステップ 2　[Protocols] タブのドロップダウン リストで、表示するプロトコルのタイプを選択します。

選択したタイプのプロトコルが、[Protocols] タブに表示されます。

ステップ 3　[Close] をクリックします。

[Protocol Settings] ダイアログボックスが閉じます。

（注） ドロップダウン リストの設定が保存されます。次に [Protocol Settings] ダイアログボックスを開くと、すべてのプロトコルが表示されます。

CHAPTER 8

Service Configuration Editor の使用方法：トラフィックのアカウンティングとレポート

はじめに

この章では、使用カウンタと Raw Data Record（RDR; 未加工データ レコード）の使用法について説明します。

トラフィックのアカウンティングとレポートは、Cisco Service Control Application for Broadband（SCA BB）サービス コンフィギュレーションを作成するための 2 番めのステップです。

使用カウンタ

SCA BB は、サービスごとに、各種ネットワーク メトリック（セッションの数、容量など）を収集、保持します。このアカウンティングは、リンク全体について、サブスクライバごと、サブスクライバ グループ（パッケージまたはパッケージ グループ）ごとに行われます。

Service Usage Counters は、各サービスの総使用量に関するデータを生成するために、システムで使用されます。サービスは、自身の使用状況カウンタと親サービスの使用カウンタを使用できます。たとえば、デフォルトのサービス コンフィギュレーションでは、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サービスと Post Office Protocol 3（POP3）サービスは E メール サービス使用カウンタを共有します。使用カウンタへのサービスの割り当ては、サービス階層によって決定されます。サービス階層の設定方法については、「サービスの編集方法」（P.7-9）で説明しています。

SCA BB では、パッケージ単位でさまざまなネットワーク メトリックの収集と管理も行います。

Package Usage Counters は、各パッケージの総使用量に関するデータを生成するために、システムで使用されます。パッケージは、自身の使用状況カウンタと親パッケージの使用カウンタを使用できます。使用カウンタへのパッケージの割り当ては、パッケージ階層によって決定されます。パッケージ階層の設定方法については、「高度なパッケージ オプションの設定」（P.9-52）で説明しています。

Raw Data Record

Service Control Engine（SCE）プラットフォームは、サービス プロバイダーに関連する情報を表す Raw Data Record（RDR）を作成して、送信します。これらの RDR には、システム設定に応じてさまざまな情報および統計情報が格納されます。各種 RDR の内容と構造については、『*Cisco Service Control Application for Broadband Reference Guide*』の「Raw Data Records: Formats and Field Contents」を参照してください。

- RDR は、フィルタ処理されたトラフィックに関しては生成されません（「トラフィック フローのフィルタリング」（P.10-20）を参照）。
- RDR データは、レイヤ 3 ボリュームに基づいています。

NetFlow レコード

- NetFlow レコードのイネーブルとディセーブルには Command-Line Interface（CLI; コマンドライン インターフェイス）を使用します。

  サポートされる RDR の種類別にレコードをエクスポートできます。次の種類の RDR のデータは、NetFlow を使用してエクスポートできます。

  - Subscriber Usage RDR
  - Package Usage RDR
  - Link Usage RDR
- NetFlow レコードは複数の収集デバイスに送信できます。
- NetFlow レコードの生成は RDR と同時に行えます。

RDR 設定の管理

このセクションでは、さまざまなタイプの RDR の生成を設定する方法について説明します。

各種 RDR の内容と構造については、『*Cisco Service Control Application for Broadband Reference Guide*』の「Raw Data Records: Formats and Field Contents」を参照してください。

- RDR は、フィルタ処理されたトラフィックに関しては生成されません（「トラフィック フローのフィルタリング」（P.10-20）を参照）。
- RDR データは、レイヤ 3 ボリュームに基づいています。

[RDR Settings] ダイアログボックス

サービス コンフィギュレーション全体の RDR 生成を制御するには、[RDR Settings] ダイアログボックスを使用します。このダイアログボックスには、次の 7 つのタブがあります。

- [Usage RDRs] タブ：各種 Usage RDR の生成をイネーブルにし、その生成間隔を定義します。
- [Transaction RDRs] タブ：Transaction RDR の生成をイネーブルにし、生成の最大レートを定義します。
- [Quota RDRs] タブ：各種 Quota RDR の生成をイネーブルにし、その生成パラメータを定義します。
- [Transaction Usage RDRs] タブ：Transaction Usage RDR を生成するパッケージとサービスを指定できるようにします。

- [Log RDRs] タブ：Log RDR を生成するパッケージとサービスを指定できるようにします。
- [Real-Time Subscriber RDRs] タブ：Real-Time Subscriber Usage RDR の生成をイネーブルにし、その生成間隔と生成の最大レートを定義します。
- [Real-Time Signaling RDRs] タブ：Real-Time Signaling RDR を生成するパッケージとサービスを指定できるようにします。

（注）　Media Flow RDR と Malicious Traffic Periodic RDR のイネーブルと設定は、「詳細サービス コンフィギュレーション オプションの編集」（P.10-49）で行います。

Usage RDR の管理方法

次の 4 種類の Usage RDR には、サービス使用カウンタに含まれるすべてのサービスの総使用状況に関するデータが含まれています。

- Link Usage RDR：リンク全体が対象
- Package Usage RDR：特定のパッケージに対するすべてのサブスクライバが対象
- Subscriber Usage RDR：特定のサブスクライバが対象
- Virtual Links Usage RDR：仮想リンクの特定グループが対象

各種 Usage RDR の生成をイネーブルまたはディセーブルにし、各種 Usage RDR の生成間隔を設定できます。Subscriber Usage RDR の生成レートは制限できます。サブスクライバが多数の場合は制限することを推奨します。

デフォルトでは、4 種類の Usage RDR がすべてイネーブルです （Virtual Links Usage RDR は、サービス コンフィギュレーションの作成時に仮想リンク モードをイネーブルにした場合にだけ、デフォルトでイネーブルになります）。

（注）　ブロックされたセッションについては、Usage RDR は生成されません。セッションのブロックが発生するのは、セッションのマッピング先のサービスがこのユーザのパッケージに対してブロックされている場合（「規則のためのフローごとのアクションの定義」（P.9-60）を参照）、またはユーザがこのサービスに対して許可されているクォータを超過した場合（「クォータの管理」（P.9-76）を参照）です。

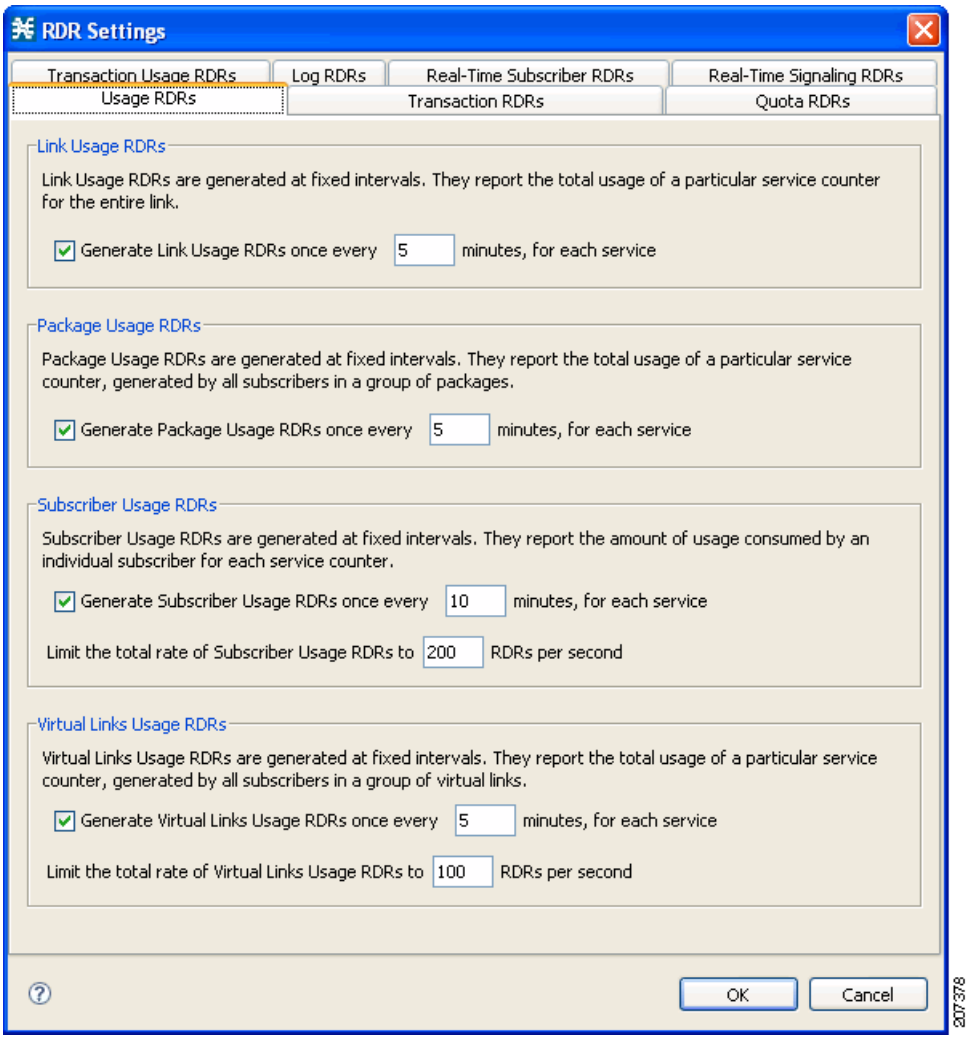
RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の次のセクションを参照してください。

- 「Link Usage RDR」
- 「Package Usage RDR」
- 「Subscriber Usage RDR」
- 「Virtual Link Usage RDR」

ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます（図 8-1）。

図 8-1　[RDR Settings]



ステップ 2　選択したタイプの Usage RDR の生成をイネーブルにするには、該当する [Generate Usage RDRs] チェックボックスをオンにします。

選択したタイプの Usage RDR の生成をディセーブルにするには、該当する [Generate Usage RDRs] チェックボックスをオフにします。

ステップ 3　選択したタイプの Usage RDR の生成間隔を変更するには、該当する [Generate Usage RDRs] フィールドに、このタイプの Usage RDR の生成間隔を分単位で入力します。

ステップ 4　Subscriber Usage RDR の生成レートを制限するには、[Limit the Total Rate of Subscriber Usage RDRs] フィールドに、1 秒間に生成される Subscriber Usage RDR の最大値を入力します。

ステップ 5　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Usage RDR 生成のための新しい設定が保存されます。

Transaction RDR の管理方法

各 Transaction RDR には、1 回のネットワーク トランザクションに関するデータが格納されます。SCE プラットフォームでは、サービス タイプを選択して Transaction RDR を生成できます。たとえば、この RDR を使用して、ネットワークを通過するトラフィックを示す統計グラフを作成することもできます。

Transaction RDR の生成をイネーブルまたはディセーブルにし、1 秒間に生成される Transaction RDR の最大数を設定し、それらの RDR を生成するサービスを選択できます。各サービスに相対ウェイトを割り当てることもできます。相対ウェイトに基づいて、他のサービスとの比較により、このサービスのために生成される Transaction RDR の相対数が決まります。

デフォルトでは、1 秒間に最大 100 の Transaction RDR が生成されます。どのサービスにも同じウェイトが割り当てられます。

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の「Transaction RDR」を参照してください。

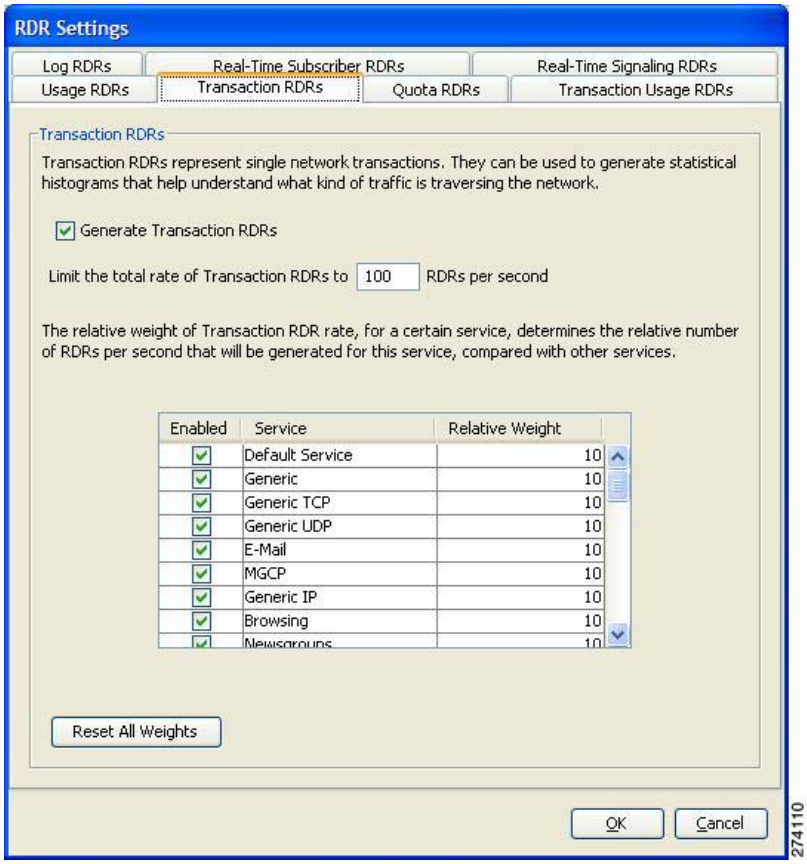
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Transaction RDRs] タブをクリックします。

[Transaction RDRs] タブが開きます（図 8-2）。

図 8-2　[Transaction RDRs] タブ



ステップ 3　Transaction RDR の生成をイネーブルにするには、[Generate Transaction RDRs] チェックボックスをオンにします。

Transaction RDR の生成をディセーブルにするには、[Generate Transaction RDRs] チェックボックスをオフにします。

ステップ 4　Transaction RDR の最大生成レートを変更するには、[Limit the Total Rate of Transaction RDRs] フィールドに目的のレートを入力します。

ステップ 5　選択したサービスの Transaction RDR をディセーブルにするには、サービス名の隣にある [Enabled] チェックボックスをオフにします。

ステップ 6　選択したサービスの相対ウェイトを設定するには、[Relative Weight] カラム内の該当するセルをダブルクリックして、目的のウェイトを入力します。

ステップ 7　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Transaction RDR 生成のための新しい設定が保存されます。

Quota RDR の管理方法

各 Quota RDR には、サブスクライバごとのデータが入っています。Quota RDR には、4 つのタイプがあります。

- Quota Breach RDR：クォータ違反が発生した時に生成されます。クォータ違反は、枯渇したクォータ バケットをサービスが消費しようとしたことを意味します。

  違反したサービスは、そのサービスの違反処理設定に従って処理されます。たとえば、サービスのクォータが消費された場合に、そのサービスのフローをブロックできます。

- Remaining Quota RDR：クォータの消費時に生成されますが、直前の Remaining Quota RDR が生成されて以降にバケットの状態が変化した場合だけです。

- Quota Threshold RDR：バケットの残りクォータがしきい値を下回った場合に生成されます。外部システムでこの RDR をクォータ要求として処理し、バケットが枯渇する前にサブスクライバに追加クォータを供給できます。

- Quota State Restore RDR：サブスクライバが導入されたときに生成されます。サブスクライバがログアウトすると、残りのクォータが Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）に格納されます。サブスクライバが再度ログインすると、このクォータが SM から復元されます。

各種 Quota RDR の生成をイネーブルまたはディセーブルにし、これらの RDR の生成レートを定義できます。

- Remaining Quota RDR では、生成間隔を設定し、生成レートを制限できます（サブスクライバが多数の場合に可能です）。
- Quota Threshold RDR では、しきい値を設定できます。

デフォルトでは、Quota RDR はすべてディセーブルです。

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の次のセクションを参照してください。

- 「Quota Breach RDR」
- 「Remaining Quota RDR」
- 「Quota Threshold Breach RDR」
- 「Quota State Restore RDR」

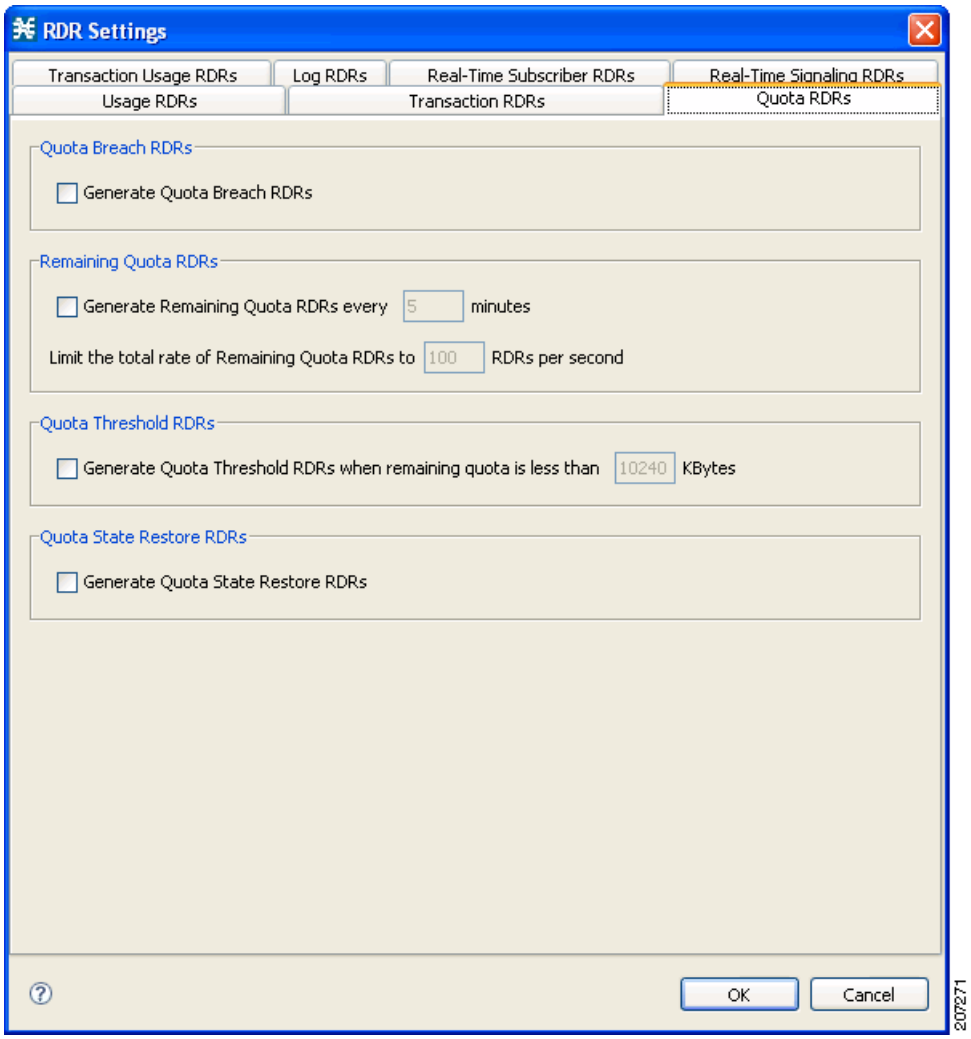
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Quota RDRs] タブをクリックします。

[Quota RDRs] タブが開きます（図 8-3）。

図 8-3　[Quota RDRs] タブ



ステップ 3　Quota Breach RDR の生成をイネーブルにするには、[Generate Quota Breach RDRs] チェックボックスをオンにします。

ステップ 4　Remaining Quota RDR の生成をイネーブルにするには、[Generate Remaining Quota RDRs] チェックボックスをオンにします。

ステップ 5　Remaining Quota RDR の生成間隔を変更するには、[Generate Remaining Quota RDRs] フィールドに、RDR の生成間隔を分単位で入力します。

ステップ 6　Remaining Quota RDR の最大生成レートを制限するには、[Limit the Total Rate of Remaining Quota RDRs] フィールドに、1 秒間に生成される Remaining Quota RDR の最大値を入力します。

ステップ 7　Quota Threshold RDR の生成をイネーブルにするには、[Generate Quota Threshold RDRs] チェックボックスをオンにします。

ステップ 8　Quota Threshold RDR のしきい値を変更するには、[Generate Quota Threshold RDRs] フィールドに、Quota Threshold RDR が生成されるしきい値を入力します。

ステップ 9　Quota State Restore RDR の生成をイネーブルにするには、[Generate Quota State Restore RDRs] チェックボックスをオンにします。

ステップ 10　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Quota RDR 生成のための新しい設定が保存されます。

Transaction Usage RDR の管理方法

Transaction Usage RDR は、選択したパッケージのすべてのトランザクション、またはパッケージごとに選択したサービスについて生成されます。各 Transaction Usage RDR には、1 回のネットワーク トランザクションに関するデータが格納されます。この RDR を使用すれば、特定のサービスやサブスクライバの詳細使用ログを作成してトランザクションベースの課金などに利用できます。

注意　トランザクションごとの RDR の生成や収集を行うと、パフォーマンスが低下することがあります。Transaction Usage RDR の生成は、モニタや制御が必要なサービスおよびパッケージに限定して行うようにしてください。

Transaction Usage RDR を生成するパッケージおよびサービスを選択できます。このようなパッケージおよびサービスについては、次の RDR も生成されます。

- HTTP Transaction Usage RDR
- RTSP Transaction Usage RDR
- VoIP Transaction Usage RDR

デフォルトでは、Transaction Usage RDR は生成されません。

（注）　Media Flow RDR のイネーブル化は、「詳細サービス コンフィギュレーション オプションの編集」（P.10-49）で行います（イネーブルにすると、SIP および Skype メディア フローの最後に Media Flow RDR が生成されます。これを元に、SIP 音声コールとビデオ コールを区別できます）。

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の次のセクションを参照してください。

- 「Transaction Usage RDR」
- 「HTTP Transaction Usage RDR」
- 「RTSP Transaction Usage RDR」
- 「VoIP Transaction Usage RDR」

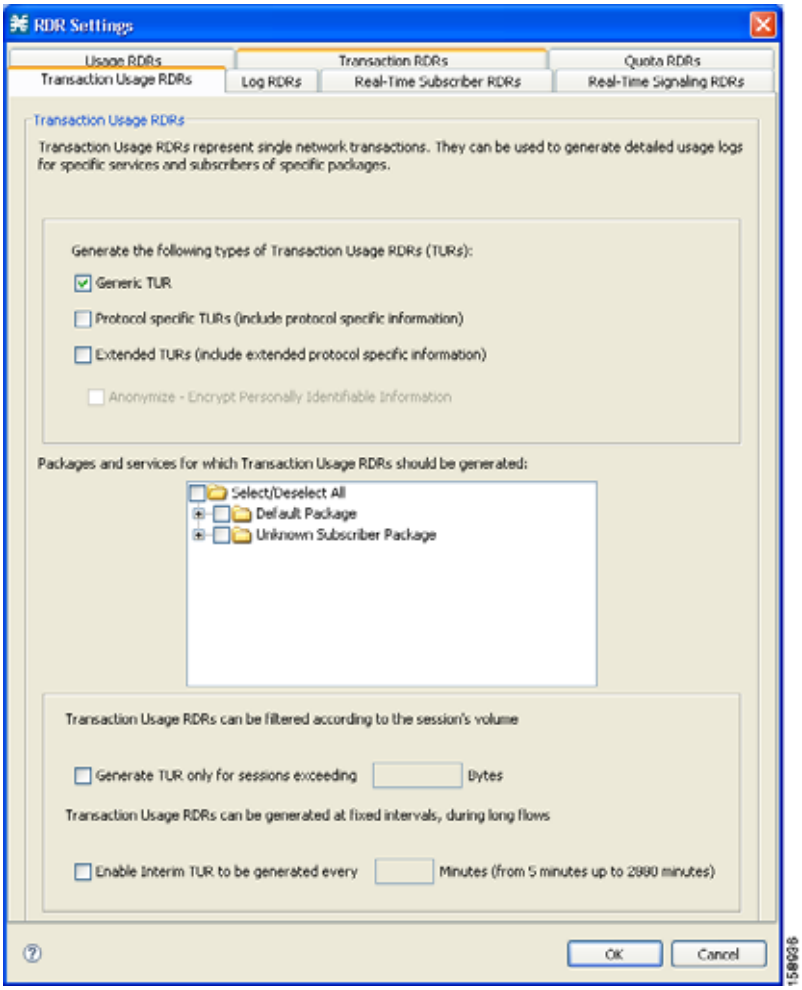
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Transaction Usage RDRs] タブをクリックします。

[Transaction Usage RDRs] タブが開きます（図 8-4）。

図 8-4　[Transaction Usage RDRs] タブ



ステップ 3　次のタイプの Transaction Usage RDR を 1 つ以上オンにして生成します。

- [Generic TUR]
- [Protocol Specific TURs (include protocol specific information)]
- [Extended TURs (include extended protocol specific information)]

[Extended TURs] をオンにすると、[Anonymize - Encrypt Personally Identifiable Information] チェックボックスがイネーブルになります。データを匿名にするには、このチェックボックスをオンにします。

ステップ 4　（任意）選択したパッケージの Transaction Usage RDR の生成をイネーブルにするには、パッケージ ツリーのパッケージ名の隣にあるチェックボックスをオンにします。

パッケージが展開されて、パッケージのすべてのコンポーネント サービスが、すべてのサービスが選択された状態で表示されます。

ステップ 5　パッケージの選択したサービスの Transaction Usage RDR の生成をイネーブルにします。

a. 目的のパッケージのノードを展開します。

b. 生成する Transaction Usage RDR の各サービスのサービス名の隣にあるチェックボックスをオンにします。

ステップ 6　（任意）Transaction Usage RDR の生成をセッション サイズで制限します。

a. [Generate TUR only for sessions exceeding] チェックボックスをオンにします。

[Bytes] フィールドがイネーブルになります。

b. セッションに対する Transaction Usage RDR 生成のしきい値となる、セッションの最低サイズをバイト単位で入力します。

ステップ 7　（任意）長いフローのための、追加の暫定的な Transaction Usage RDR の生成をイネーブルにするには、次の手順を実行します。通常、Transaction Usage RDR はフローの終了時にだけ生成されます。

a. [Enable Interim TUR to be generated every] チェックボックスをオンにします。

[Minutes] フィールドがイネーブルになります。

b. 各フローで必要な Transaction Usage RDR の生成間隔を分単位で入力します。

ステップ 8　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Transaction Usage RDR 生成のための新しい設定が保存されます。

Log RDR の管理方法

Log RDR は、システム イベントに関する情報を提供します。特定のアクションまたは状態の変化に応じて生成されます。Log RDR には次の 2 種類があります。

- Blocking RDR：トランザクションがブロックされるたびに生成されます。
- Breach RDR：バケットがグローバルしきい値を超えるたびに生成されます。

1 秒間に生成される Log RDR の最大数を設定できます。Blocking RDR を生成するパッケージおよびサービスを選択できます。

デフォルト設定は次のとおりです。

- Blocking RDR はすべてのパッケージを対象に生成されます。
- Breach RDR は常に生成されます。

（注）　1 秒間に生成可能な Log RDR の最大数は 20 です。

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の次のセクションを参照してください。

- 「Blocking RDR」
- 「Quota Breach RDR」

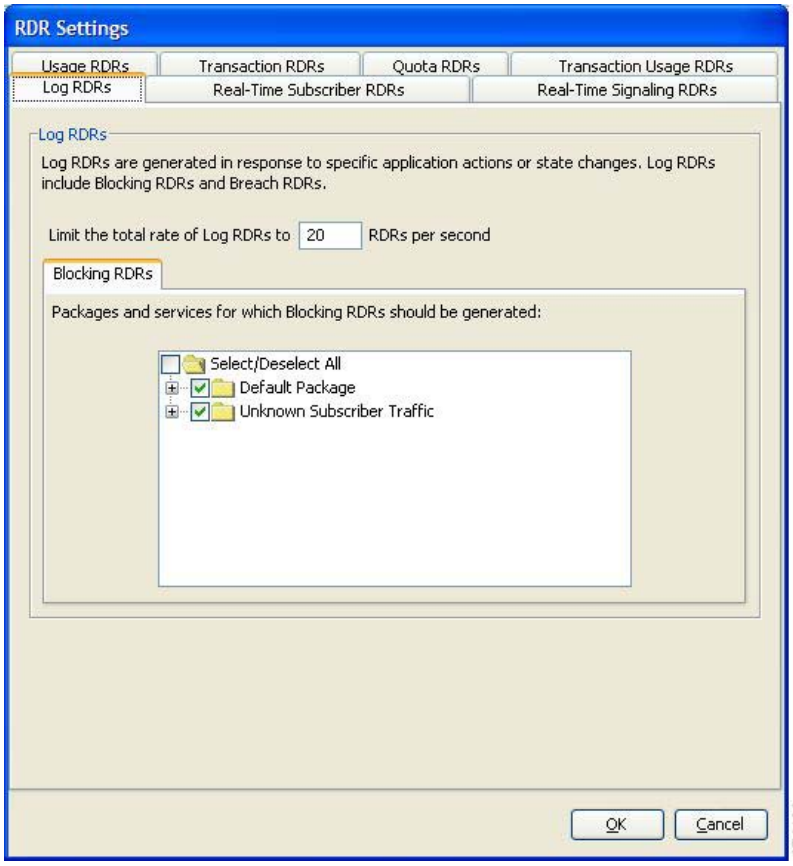
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Log RDRs] タブをクリックします。

[Log RDRs] タブが開きます（図 8-5）。

図 8-5　[Log RDRs] タブ



ステップ 3　Log RDR の最大生成レートを変更するには、[Limit the Total Rate of Log RDRs] フィールドに目的のレートを入力します。

ステップ 4　選択したパッケージの Blocking RDR の生成をイネーブルにするには、パッケージ ツリーのパッケージ名の隣にあるチェックボックスをオンにします。

パッケージが展開されて、パッケージのすべてのコンポーネント サービスが、すべてのサービスが選択された状態で表示されます。

ステップ 5　パッケージの選択したサービスの Blocking RDR の生成をイネーブルにします。

a.　目的のパッケージのノードを展開します。

b.　目的となる各サービスのサービス名の隣にあるチェックボックスをオンにします。

ステップ 6　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Log RDR 生成のための新しい設定が保存されます。

Real-Time Subscriber Usage RDR の管理方法

Real-Time Subscriber Usage RDR は、サブスクライバ使用量をレポートする RDR です。指定された間隔で、使用サービスごとに個々のサブスクライバについて生成されます。これらの RDR を使用すると、必要に応じて、選択されたサブスクライバをより詳細にモニタできます。

モニタ対象のサブスクライバを選択する方法については、「リアルタイムで使用量をモニタするサブスクライバの選択」（P.13-14）を参照してください。

注意　多くのサブスクライバで Real-Time Subscriber Usage RDR の生成および収集を行うと、パフォーマンスが低下することがあります。Real-Time Subscriber Usage RDR の生成は、モニタする必要のあるサブスクライバに限定してイネーブルにしてください。

Real-Time Subscriber Usage RDR の生成をイネーブルまたはディセーブルにし、RDR の生成間隔を設定し、1 秒間に生成される最大数を設定できます。

Real-Time Subscriber Usage RDR のデフォルト設定は次のとおりです。

- イネーブル（選択されたサブスクライバに限定）
- サブスクライバごとに 1 分間に 1 回生成
- 1 秒間の RDR 生成数を 100 に制限

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の「Real-Time Subscriber Usage RDR」を参照してください。

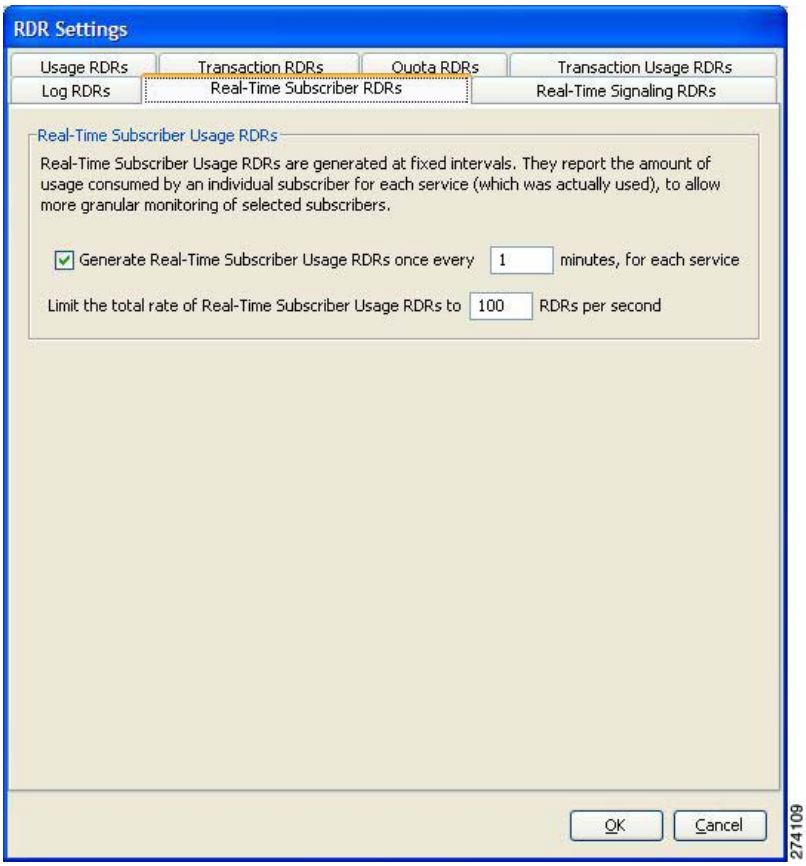
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Real-Time Subscriber RDRs] タブをクリックします。

[Real-Time Subscriber RDRs] タブが開きます（図 8-6）。

図 8-6　[Real_Time Subscriber RDRs] タブ



ステップ 3　Real-Time Subscriber Usage RDR の生成をイネーブルにするには、[Generate Real-Time Subscriber Usage RDRs] チェックボックスをオンにします。

ステップ 4　Real-Time Subscriber Usage RDR の生成間隔を変更するには、[Generate Real-Time Subscriber Usage RDRs] フィールドに、RDR の生成間隔を分単位で入力します。

ステップ 5　Real-Time Subscriber Usage RDR の生成レートを制限するには、[Limit the total rate of Real-Time Subscriber Usage RDRs] フィールドに、1 秒間に生成される Real-Time Subscriber Usage RDR の最大値を入力します。

ステップ 6　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Real-Time Subscriber Usage RDR 生成のための新しい設定が保存されます。

Real-Time Signaling RDR の管理方法

Real-Time Signaling RDR はフローの開始時と終了時、フロー開始後の指定間隔時、およびネットワーク攻撃の開始時と終了時に生成されます。この RDR を使用すると、SCE プラットフォームで検出されたイベントに関して外部システムに通知し、ネットワーク全体でリアルタイムに対応することが可能になります。

Real-Time Signaling RDR には、次の 2 つのグループがあります。

- Flow Signaling RDR：
  - Flow Start Signaling RDR
  - Flow Stop Signaling RDR
  - Flow Interim Signaling RDR
- Attack Signaling RDR：
  - Attack Start Signaling RDR
  - Attack Stop Signaling RDR

選択したパッケージ、またはパッケージごとに選択したサービスに対して、Flow Signaling RDR の生成をイネーブルにしたりディセーブルにしたりできます。Flow Interim Signaling RDR の生成間隔を設定できます。この RDR は、Flow Start and Flow Stop Signaling RDR がイネーブルになっている場合にだけ生成されます。

選択したパッケージに対して Attack Signaling RDR の生成のイネーブルとディセーブルを切り替えることができます。

（注）　Malicious Traffic Periodic RDR のイネーブルと設定は、「詳細サービス コンフィギュレーション オプションの編集」（P.10-49）で行います。

RDR の目的、デフォルトの宛先、コンテンツ、生成ロジック、タグ、フィールドについては、『*Cisco Service Control Application for Broadband Reference Guide*』の次のセクションを参照してください。

- 「Flow Start RDR」
- 「Flow End RDR」
- 「Ongoing Flow RDR」
- 「Attack Start RDR」
- 「Attack End RDR」

デフォルトでは、Real-Time Signaling RDR は生成されません。

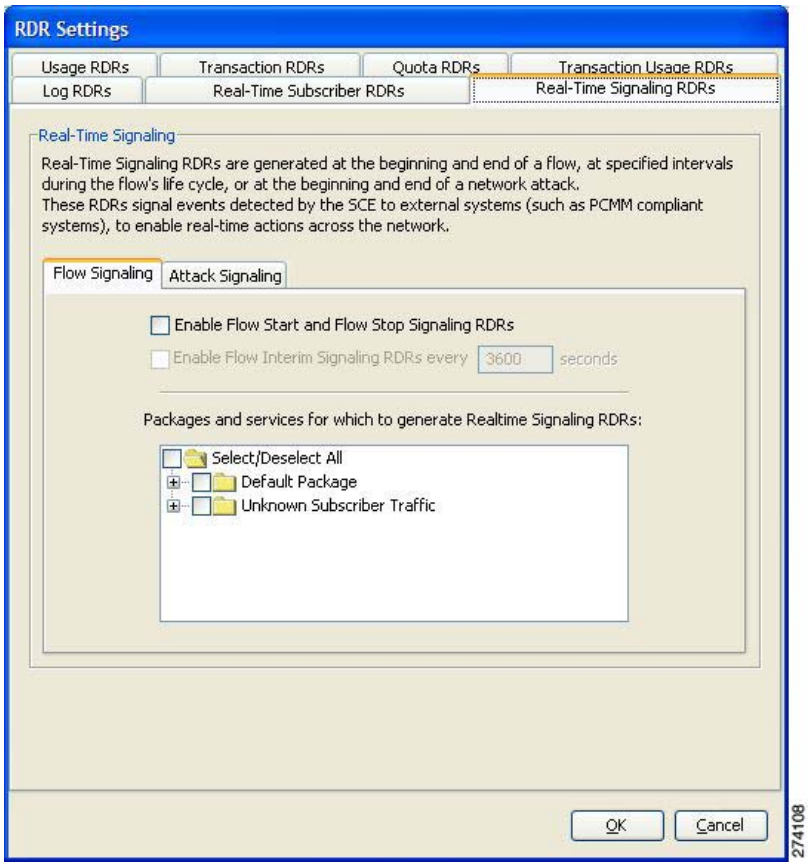
ステップ 1　左ペインの [Classification] タブで、[Configuration] > [RDR Settings] の順に選択します。

[RDR Settings] ダイアログボックスが表示されます。

ステップ 2　[Real-Time Signaling RDRs] タブをオンにします。

[Real-Time Signaling RDRs] タブが開きます（図 8-7）。

図 8-7　[Real-Time Signaling RDRs] タブ



ステップ 3　Flow Start and Flow Stop Signaling RDR の生成をイネーブルにするには、[Enable Flow Start and Flow Stop Signaling RDRs] チェックボックスをオンにします。

（注）　単方向分類が有効になっている場合、Flow Start and Flow Stop Signaling RDR の生成はサポートされません。単方向分類が有効になっているときに [Enable Flow Start and Flow Stop Signaling RDRs] チェックボックスをオンにしようとすると、[RDR Settings Error] メッセージが表示されます。

[OK] をクリックし、ステップ 8 に進んでください。

[Enable Flow Interim Signaling RDRs] チェックボックスがイネーブルになります。

ステップ 4　Flow Interim Signaling RDR の生成をイネーブルにするには、[Enable Flow Interim Signaling RDRs] チェックボックスをオンにします。

[Enable Flow Interim Signaling RDRs] フィールドがイネーブルになります。

ステップ 5　Flow Interim Signaling RDR の生成間隔を変更するには、[Enable Flow Interim Signaling RDRs] フィールドに、RDR の生成間隔を分単位で入力します。

ステップ 6　選択したパッケージの Flow Interim Signaling RDR の生成をイネーブルにするには、パッケージ ツリーのパッケージ名の隣にあるチェックボックスをオンにします。

パッケージが展開されて、パッケージのすべてのコンポーネント サービスが、すべてのサービスが選択された状態で表示されます。

ステップ 7　パッケージの選択したサービスの Flow Interim Signaling RDR の生成をイネーブルにするには、次の手順を実行します。

a.　目的のパッケージのノードを展開します。

b.　目的となる各サービスのサービス名の隣にあるチェックボックスをオンにします。

ステップ 8　Attack Signaling RDR の生成をイネーブルにするには、次の手順を実行します。

a.　[Real-Time Signaling RDRs] タブのボディで、[Attack Signaling] タブをクリックします（図 8-8）。

図 8-8　[Attack Signaling] タブ

b.　[Enable Attack Start and Attack Stop Signaling RDRs] チェックボックスをオンにします。

ステップ 9　選択したパッケージの Attack Signaling RDR の生成をイネーブルにするには、パッケージ リストのパッケージ名の隣にあるチェックボックスをオンにします。

ステップ 10　[OK] をクリックします。

[RDR Settings] ダイアログボックスが閉じます。

Real-Time Signaling RDR 生成のための新しい設定が保存されます。

CHAPTER 9

Service Configuration Editor の使用方法：トラフィックの制御

はじめに

Service Control Engine（SCE）プラットフォームのトラフィック制御機能と Cisco Service Control Application for Broadband（SCA BB）は、トラフィック フローの制限と優先順位付けのために使用されます。トラフィックの制御は、フローのサービス、サブスクライバのパッケージ、サブスクライバのクォータ状態などのパラメータに基づいて行われます。

帯域幅の管理

アップストリーム インターフェイスとダウンストリーム インターフェイスには、それぞれ 1 つずつデフォルト グローバル コントローラが割り当てられています。これ以外にも、グローバル コントローラを追加できます。

サービス コンフィギュレーションには、最大で 1024 のアップストリーム グローバル コントローラと 1024 のダウンストリーム グローバル コントローラ（デフォルト グローバル コントローラを含む）を設定できます。

グローバル コントローラの定義が完了すると、パッケージにサブスクライバ BW Controller（BWC; BW コントローラ）を追加し、これらのサブスクライバ BWC を異なるグローバル コントローラにマッピングすることが可能になります。

注意　仮想リンク モードのイネーブル化またはディセーブル化を行うと、サービス コンフィギュレーションからすべてのユーザ定義グローバル コントローラが削除されます。それまでユーザ定義グローバル コントローラを示していたサブスクライバ BWC は、デフォルト グローバル コントローラを示します （サブスクライバ BWC の他のパラメータは変更されません）。

グローバル帯域幅の管理

デフォルトでは、アップストリーム インターフェイスとダウンストリーム インターフェイスには、リンク トラフィック全体を制御するデフォルト グローバル コントローラが 1 つずつ割り当てられています。各インターフェイスに最大 1023 のグローバル コントローラを追加し、各グローバル コントローラに合計リンク制限の最大帯域幅を個別に割り当てることができます。

各インターフェイスに対して、帯域幅合計リンク制限を、SCE プラットフォームの物理容量よりも小さい値に個別に定義することもできます。IP ストリーム上で SCE プラットフォームの隣に位置するデバイスの BandWidth（BW; 帯域幅）容量が制限されている場合、この制限を他のデバイスで任意に適用する代わりに、ポリシーアウェア方式を使用して SCE プラットフォームで適用できます。

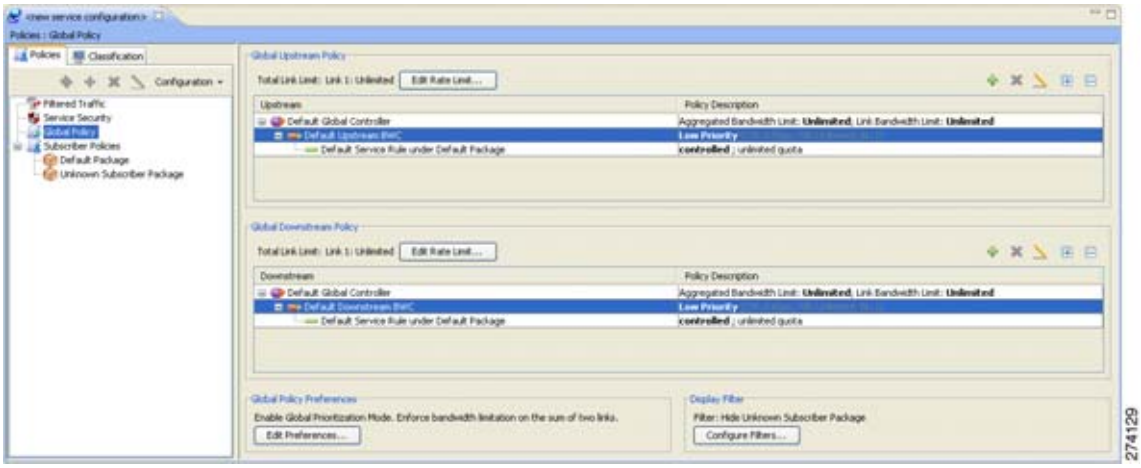
グローバル コントローラ設定の表示

（注）　グローバル コントローラ帯域幅は、レイヤ 1 ボリュームに基づいています（SCA BB のアカウンティング、レポート、およびサブスクライバ帯域幅制御は、レイヤ 3 ボリュームに基づいています）。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます（図 9-1）。

図 9-1　[Global Bandwidth Settings]



[Global Controllers] タブの上部にある 2 つのチェックボックスは、デュアルリンク システムだけで使用します（「グローバル コントローラの定義」（P.9-11）を参照）。

ペインの主要部は、アップストリームのグローバル コントローラを一覧表示する [Upstream] 領域と、ダウンストリームのグローバル コントローラを一覧表示する [Downstream] 領域からなります。各リストは次の 2 つのカラムで構成されています。

- [Upstream] または [Downstream]：グローバル コントローラ、帯域幅コントローラ、およびサービス規則の階層が表示されます。各グローバル コントローラには帯域幅コントローラが対応付けられており、グローバル コントローラの子として一覧表示されます。各帯域幅コントローラにはサービス規則が対応付けられており、帯域幅コントローラの子として一覧表示されます。
- [Policy Description]：グローバル コントローラ、帯域幅コントローラ、またはサービス規則の詳細が、対応するカラムに要約されています。グローバル コントローラの詳細が含まれる行には、このグローバル コントローラに許容される最大帯域幅の値が表示されます。

  各グローバル コントローラでは、デフォルト カレンダーによって定義される 4 つの時間枠に対し、それぞれ異なる最大帯域幅の値を設定できます（「カレンダーの管理」（P.9-69）を参照）。

  - このフィールドが 1 つの値の場合、このグローバル コントローラの最大帯域幅は定数です。
  - 時間枠ごとに最大帯域幅が異なる場合、それぞれの時間枠の最大帯域幅が、カンマで区切られて表示されます（図 9-2）。

図 9-2　　時間枠の表示

– 2 つの時間枠の最大帯域幅が同じである場合、同じ値は繰り返して表示されません（図 9-3）（したがって、**40,,,100** の場合、最初の 3 つの時間枠は最大帯域幅が合計リンク制限の 40% で、4 つめの時間枠は最大帯域幅が合計リンク制限と等しいことを意味します）。

図 9-3　　時間枠の詳細

Name	CIR (L3 Kbps)	PIR (L3 Kbps)
Primary Upstream BWC	0	Unlimited
Default Upstream BWC	0	Unlimited
BWC 1	9000	Unlimited

20727

各インターフェイスの領域（[Upstream] または [Downstream]）の上に、合計リンク制限が表示されます（図 9-4）。

図 9-4　　合計リンク制限

Name	CIR (L3 Kbps)	PIR (L3 Kbps)	Global Controller	AL
Primary Upstream BWC	0	Unlimited		
Default Upstream BWC	9000	Unlimited	Default Global Controller	1
BWC 1	9000	Unlimited	Default Global Controller	1

207258

グローバル コントローラのフィルタリング

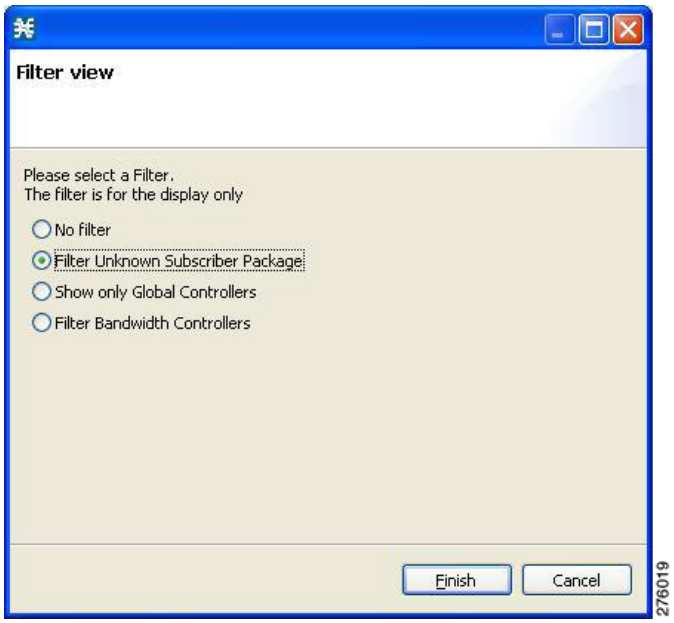
ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] が右の規則ペインに表示されます。

ステップ 2　[Configure Filters] をクリックします。

[Filter View] ダイアログボックスが表示されます（図 9-5）。

図 9-5　[Filter View]



ステップ 3　次のフィルタ オプション ボタンをいずれか 1 つ選択します。

- [No Filter]
- [Filter Unknown Subscriber Package]
- [Show only Global Controllers]
- [Filter Bandwidth Controllers]

ステップ 4　[Finish] をクリックします。

[Filter View] ダイアログボックスが閉じ、右の規則ペインが選択内容に応じてフィルタリングされます。

合計リンク制限の編集

SCE プラットフォームを通過する合計帯域幅を制限できます。

たとえば、IP ストリーム上で SCE プラットフォームの隣に位置するデバイスの BW 容量が限られている場合、他のデバイスの容量に合わせて、SCE プラットフォームを通過する帯域幅を制限できます。

アップストリーム トラフィックとダウンストリーム トラフィックの合計リンク制限は、別々に定義されます。

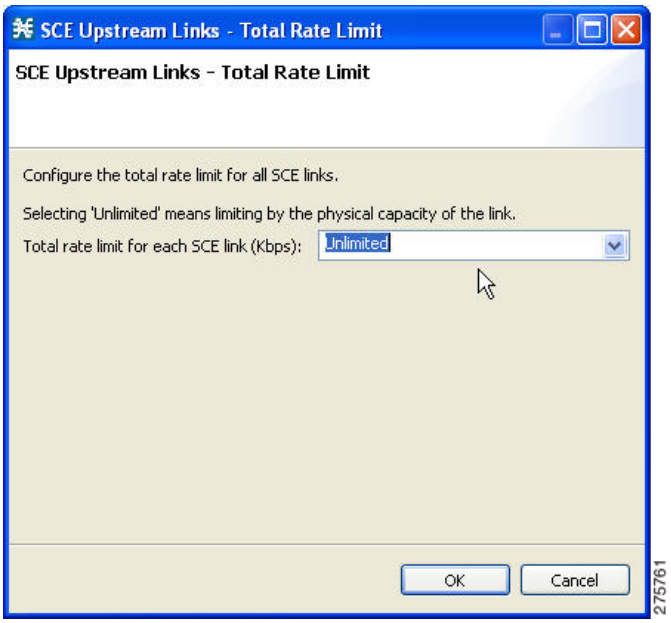
ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　[Upstream] または [Downstream] セクションで、[Edit Rate Limit] をクリックします（図 9-6）。

（注）　図 9-6 の表示内容は、グローバル コントローラのモード設定により異なります。

図 9-6　[SCE Upstream Links - Total Rate Limit]



ステップ 3　[Total rate limit for each SCE link (Kbps)] フィールドで、合計レート制限を選択します。

ステップ 4　[OK] をクリックします。

変更が保存されます。

[Global Controller Settings] ダイアログボックスが閉じます。

グローバル コントローラの追加

サービス コンフィギュレーションには、最大で 1023 のアップストリーム グローバル コントローラと 1023 のダウンストリーム グローバル コントローラを追加できます。

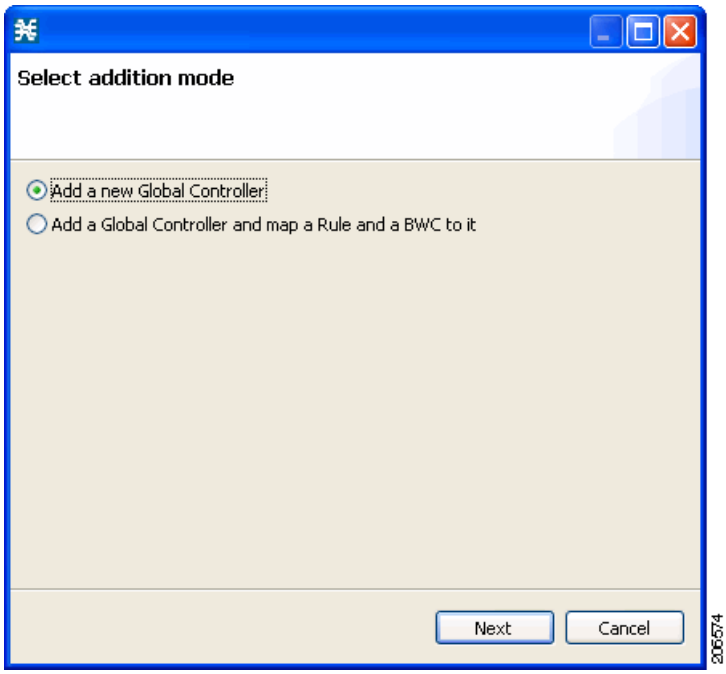
ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　目的のインターフェイスの領域（[Upstream] または [Downstream]）上で、([Add]）をクリックします。

[Select addition mode] ダイアログボックスが表示されます（図 9-7）。

図 9-7　[Select addition mode]



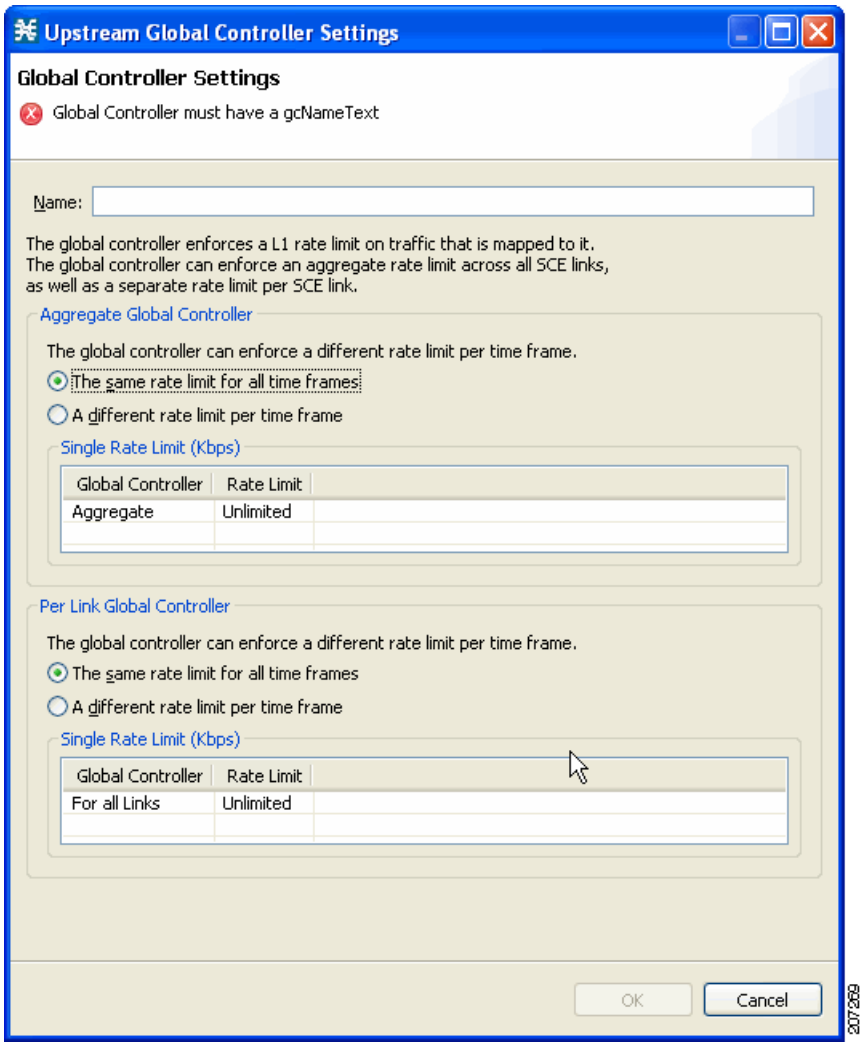
ステップ 3　新しいグローバル コントローラを追加するには、[Add a new Global Controller] オプション ボタンを選択します。

ステップ 4　[Finish] をクリックします。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-8）。

（注）　図 9-8 の表示内容は、グローバル コントローラのモード設定により異なります。

図 9-8　[Upstream Global Controller Settings]



ステップ 5　[Name] フィールドにわかりやすい名前を入力します。

ステップ 6　グローバル コントローラの最大帯域幅を編集するには、「グローバル コントローラの最大帯域幅の設定」（P.9-9）のセクションの手順を実行します。

ステップ 7　[OK] をクリックします。

変更が保存されます。

[Global Controller Settings] ダイアログボックスが閉じます。

グローバル コントローラの最大帯域幅の設定

グローバル コントローラを通過する最大帯域幅を編集できます。

4 つの時間枠に、それぞれ異なる最大帯域幅を設定できます。

各リンクと、全リンクの集約 BW に対し、異なる値を設定できます。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

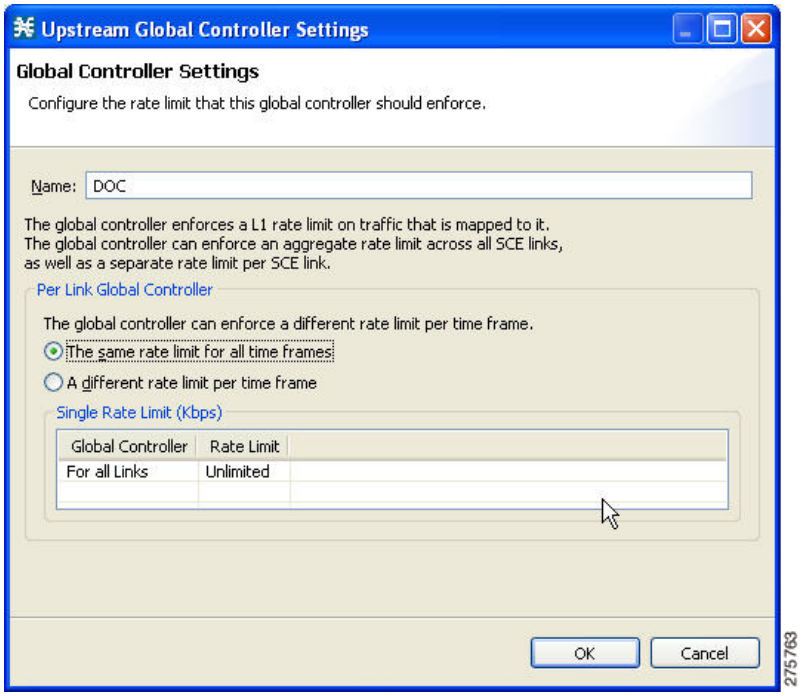
ステップ 2　グローバル コントローラを選択します。

ステップ 3　  ([Edit]）を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-9）。

（注）　図 9-9 の表示内容は、グローバル コントローラのモード設定により異なります。

図 9-9　[Upstream Global Controller Settings]



ステップ 4　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

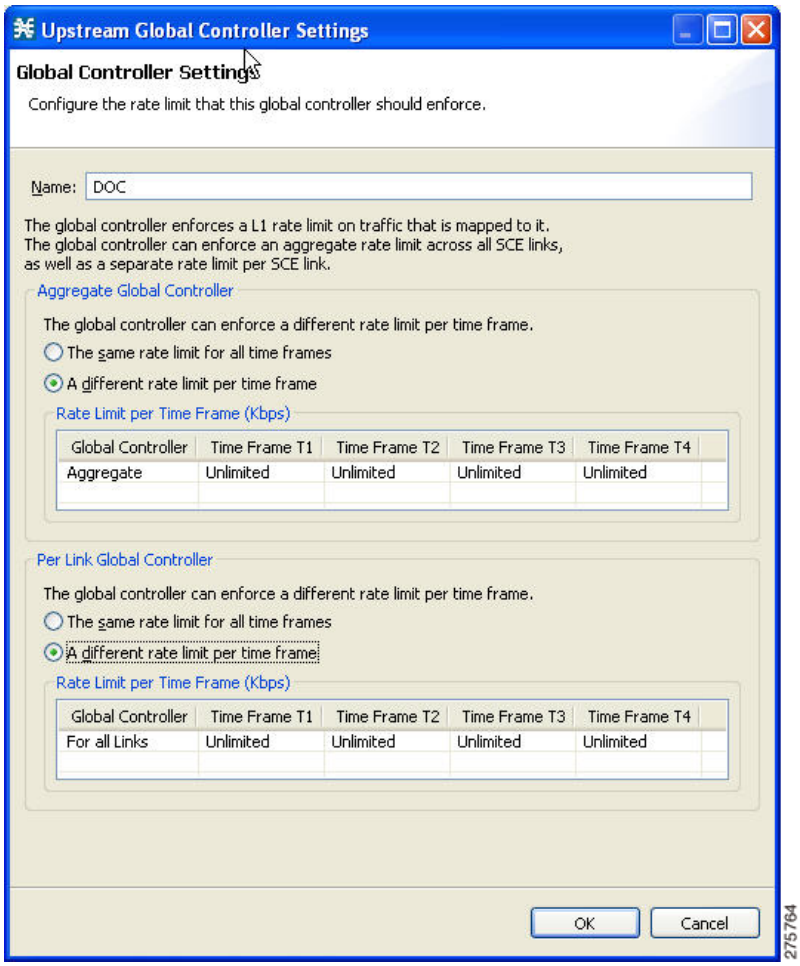
- [The same rate limit for all time frames] オプション ボタンを選択し、目的とする最大帯域幅の値を [Single Rate Limit (Kbps)] フィールドに Kbps 単位で入力します。

ステップ 5　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

- [A different rate limit per time frame] オプション ボタンを選択し、各時間枠の目的とする値を入力します（図 9-10）。

（注）　図 9-10 の表示内容は、グローバル コントローラのモード設定により異なります。

図 9-10　[Upstream Global Controller Settings]



（注）　これらの値が、デフォルト カレンダーの時間枠に適用されます。

ステップ 6　[OK] をクリックします。

変更が保存されます。

[Policy Description] カラムの値は、新しい帯域幅制限を反映して変化します。

ステップ 7　その他のグローバル コントローラに対してステップ 2 ～ステップ 6 を繰り返します。

グローバル コントローラの削除

使用していないグローバル コントローラは、いつでも削除できます。デフォルト グローバル コントローラおよび合計リンク制限は削除できません。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが表示されます。

ステップ 2　グローバル コントローラを選択します。

ステップ 3　  （[Delete]）をクリックします。

（注）　指定したグローバル コントローラがサブスクライバ BWC で使用されている場合（「パッケージ サブスクライバ BWC の編集」（P.9-29）を参照）、グローバル コントローラを削除できないことを示すメッセージが表示されます。グローバル コントローラは、すべてのサブスクライバ BWC の割り当てを解除するまで、削除できません。

グローバル コントローラが削除されます。

ステップ 4　[OK] をクリックします。

変更が保存されます。

[Global Bandwidth Settings] ダイアログボックスが閉じます。

グローバル コントローラの定義

ここでは、デュアルリンク システムおよびマルチギガビット イーサネット システムでグローバル コントローラを定義する方法について説明します。

いずれのシステムでも、同じレートを使用して各リンクを個別に定義したり、異なるレートを使用して各リンクを個別に定義したりすることができます。

あるいは、全リンクの集約として、またはリンクごとの個々の制御の集約として、帯域幅制限を適用することもできます。

次のことが実行できます。

1. すべてのリンクに同じレートを使用して、各リンクを個別に制御する。
2. リンクごとに異なるレートを使用して、各リンクを個別に制御する。
3. リンクを全体的に制御し、リンクごとの最大レートを全リンクで同じにする。
4. リンクを全体的に制御し、リンクごとに異なる最大レートを適用する。
5. 仮想リンク モードでリンクを制御する。

（注）　仮想リンク モードがイネーブルになっている場合、帯域幅制限はすべてのリンクの合計に対して適用されます。

（注）　無効なリンクのグローバル コントローラ帯域幅を変更しようとすると、ポリシーの適用中に次のようなエラー メッセージが表示されます。

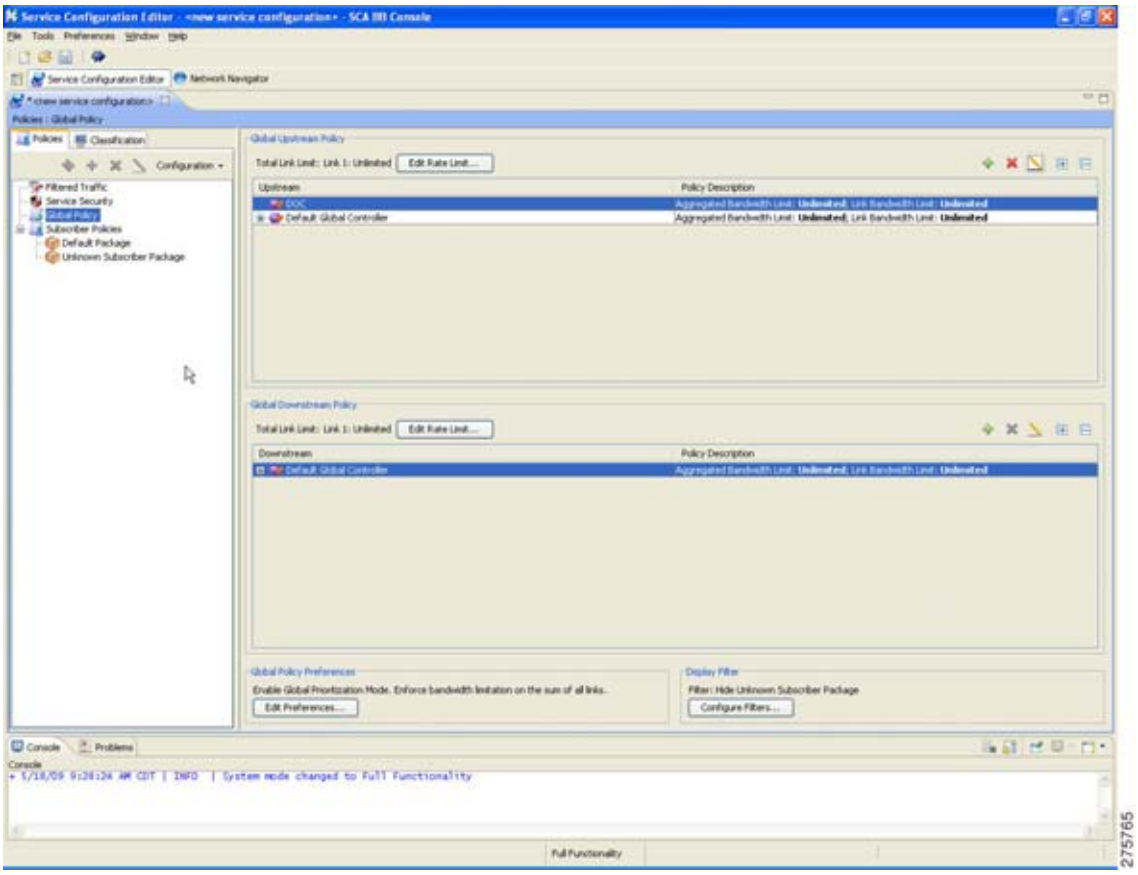
「Invalid value set on Link ID 6 for upstream GC 'Default Global Controller'.Link ID 6 does not exist.Available Link IDs: 1, 2, 3, 4」

グローバル コントローラ設定の各編集ダイアログは、次の操作でアクティブにすることができます（図 9-11）。

- グローバル ポリシー設定の右側のメイン パネルにあるグローバル コントローラ テーブル画面で、グローバル コントローラの行をダブルクリックします。
- グローバル ポリシー設定の右側のメインパネルの右上にある編集ボタンをクリックします。

（注）　アップストリームとダウンストリームのいずれの GC でも動作は同じです。

図 9-11　　グローバル コントローラ設定のアクティブ化



設定の詳細については、次のセクションを参照してください。

- 「全リンクに同一レートを使用するグローバル コントローラ帯域幅制限の設定」（P.9-13）
- 「リンクごとに異なるレートを使用するグローバル コントローラ帯域幅制限の設定」（P.9-15）
- 「各リンクに同一レートを使用し、グローバル コントローラ帯域幅制限を全リンクの合計として設定する方法」（P.9-18）
- 「リンクごとに異なるレートを使用し、グローバル コントローラ帯域幅制限を全リンクの合計として設定する方法」（P.9-21）
- 「仮想リンクのグローバル コントローラ帯域幅の設定」（P.9-25）

全リンクに同一レートを使用するグローバル コントローラ帯域幅制限の設定

すべてのリンクに同じレートを使用してグローバル コントローラを設定するには、次の手順を実行します。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

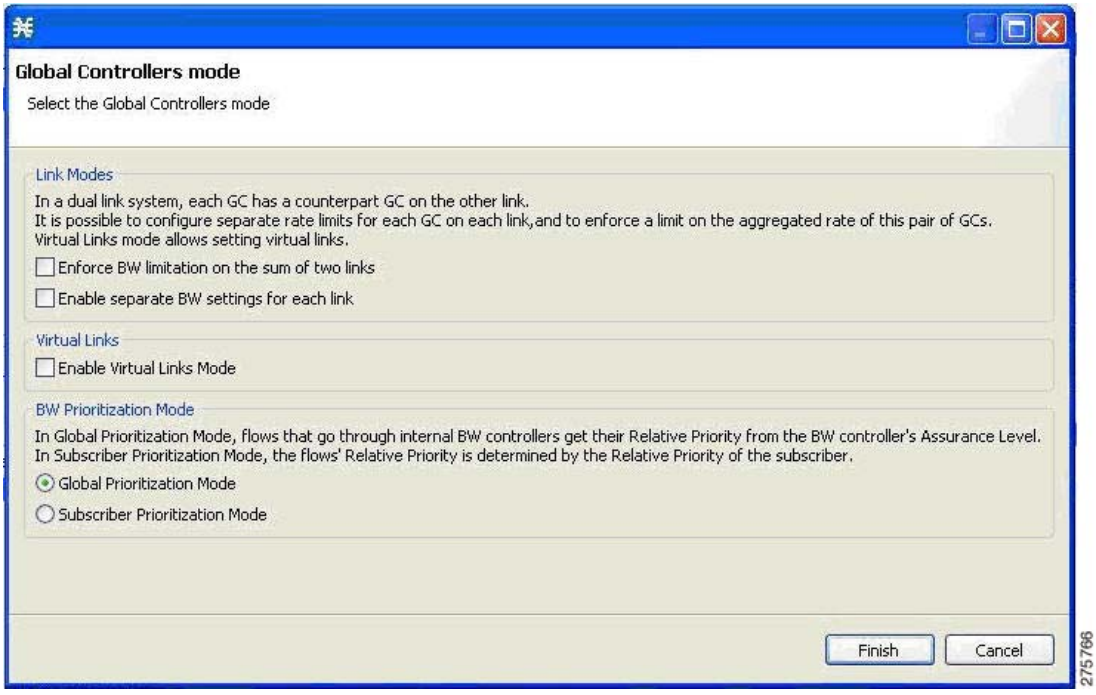
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　「グローバル コントローラの追加」（P.9-6）の説明に従って、グローバル コントローラを追加します。

ステップ 3　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-12）。

図 9-12　[Global Controllers mode]



ステップ 4　[Link Modes] のチェックボックスがオフになっていることを確認します。

ステップ 5　[Finish] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

ステップ 6　[Policies] タブで [Global Policy] をクリックします。

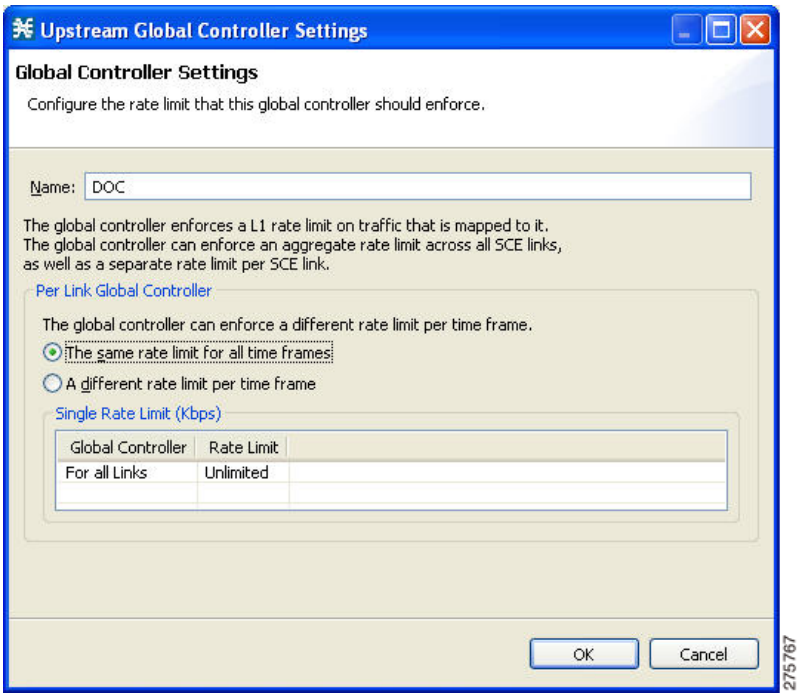
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 7　グローバル コントローラを選択します。

ステップ 8　([Edit]) を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-13）。

図 9-13　[Upstream Global Controller Settings]



（注）　すべての時間枠のレート制限を同じにする場合は、ステップ 9 を実行します。すべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 10 を実行します。

ステップ 9　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a.　[The same rate limit for all time frames] オプション ボタンを選択します。

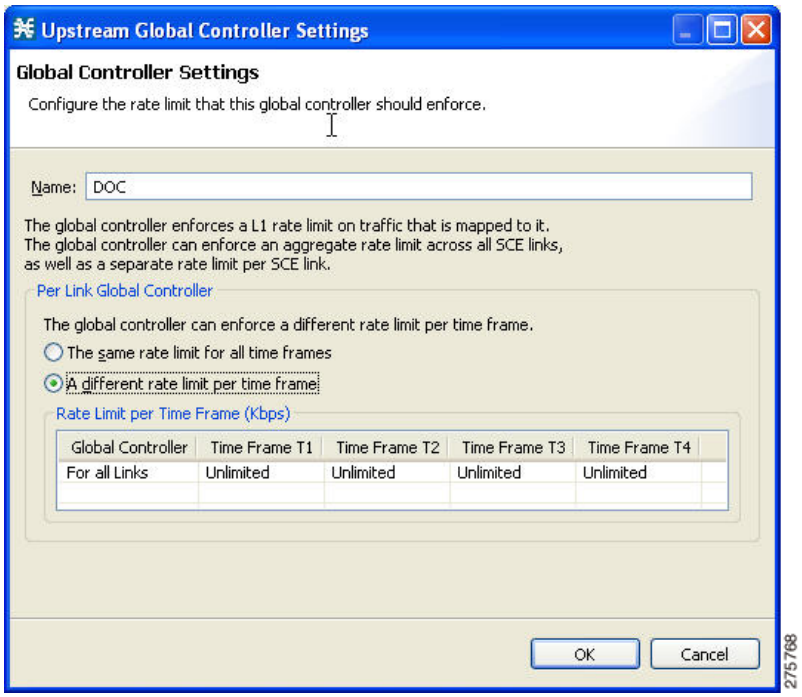
b.　[Rate limit for the Per Link Global Controller (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

ステップ 10　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a.　[A different rate limit per time frame] オプション ボタンを選択します。

b.　各時間枠で目的とする値を入力します（図 9-14）。

図 9-14　[Upstream Global Controller Settings]



ステップ 11　[OK] をクリックします。

変更が保存されます。

リンクごとに異なるレートを使用するグローバル コントローラ帯域幅制限の設定

リンクごとに異なるレートを使用してグローバル コントローラを設定するには、次の手順を実行します。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

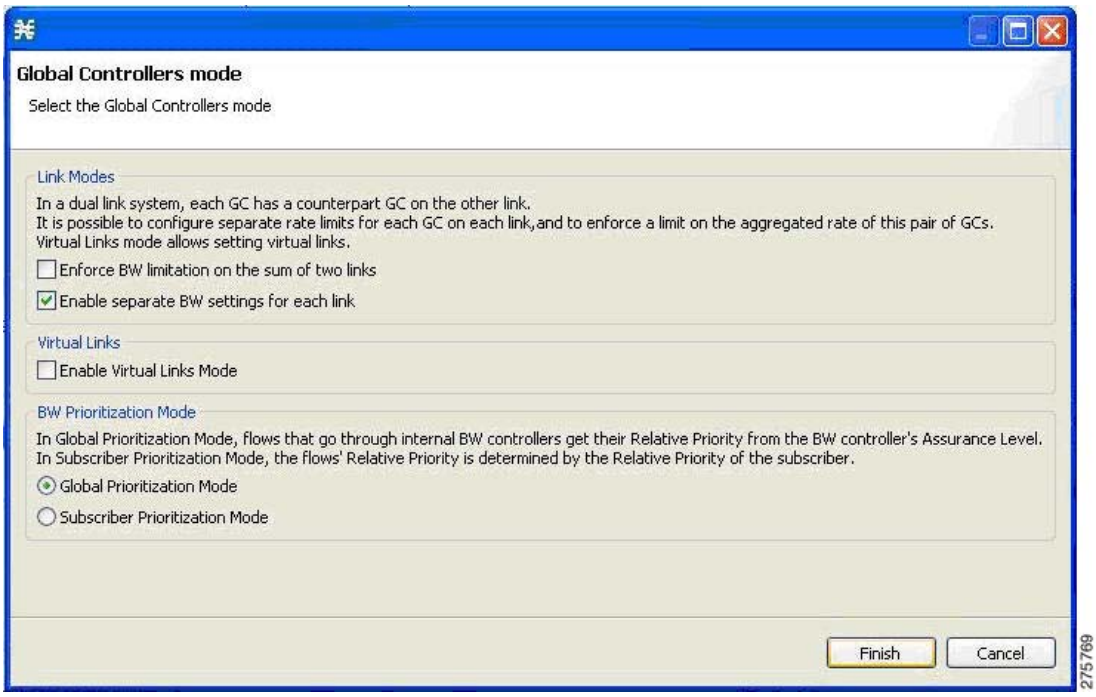
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　「グローバル コントローラの追加」（P.9-6）の説明に従って、グローバル コントローラを追加します。

ステップ 3　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-15）。

図 9-15　[Global Controllers mode]



ステップ 4　[Enable separate BW setting for each link] チェックボックスをオンにします。

ステップ 5　[Finish] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

ステップ 6　[Policies] タブで [Global Policy] をクリックします。

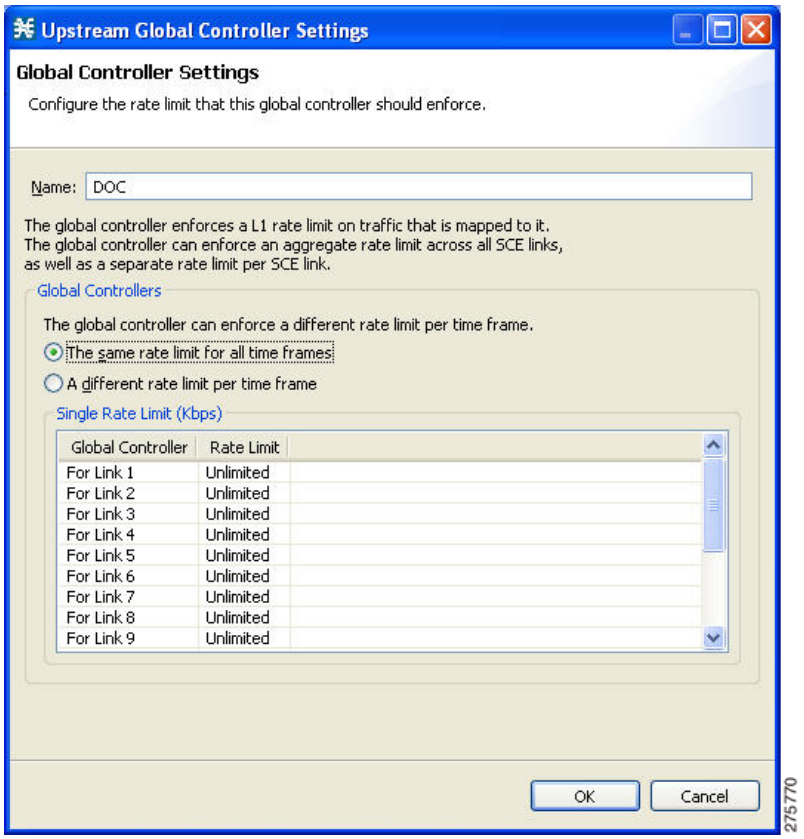
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 7　グローバル コントローラを選択します。

ステップ 8　([Edit]）を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-16）。

図 9-16　[Downstream Global Controller Settings]



（注）　すべての時間枠のレート制限を同じにする場合は、ステップ 9 を実行します。すべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 10 を実行します。

ステップ 9　各リンクについて、このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a.　[The same rate limit for all time frames] オプション ボタンを選択します。

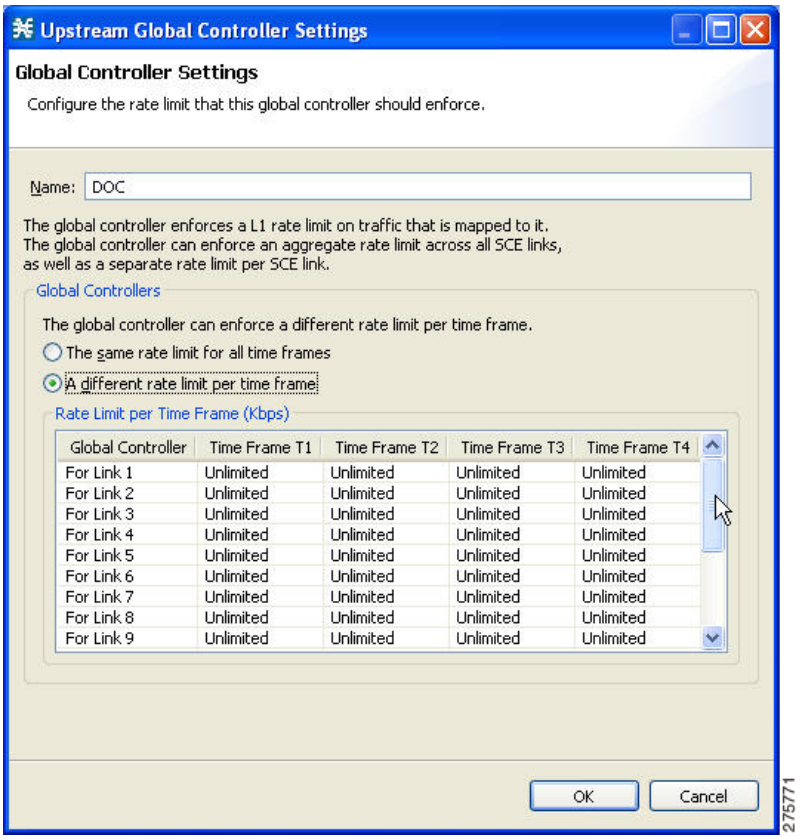
b.　[Rate limit for the Per Link Global Controller (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

ステップ 10　各リンクについて、このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a.　[A different rate limit per time frame] オプション ボタンを選択します。

b.　各時間枠で目的とする値を入力します（図 9-17）。

図 9-17　[Upstream Global Controller Settings]



ステップ 11　[OK] をクリックします。

変更が保存されます。

各リンクに同一レートを使用し、グローバル コントローラ帯域幅制限を全リンクの合計として設定する方法

このリンク制御モードでは、最大帯域幅制限が全リンクの合計として設定されます。このモードで GC を作成すると、リンクの集約グローバル コントローラを設定したうえで、リンクごとの最大レートを設定できます。このモードでは、全リンクの合計に帯域幅制限を適用し、リンクを全体的に制御したうえで、リンクごとの最大レートをすべてのリンクで同じにすることができます。

各リンクに同じレートを使用し、グローバル コントローラを全リンクの合計として設定するには、次の手順を実行します。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

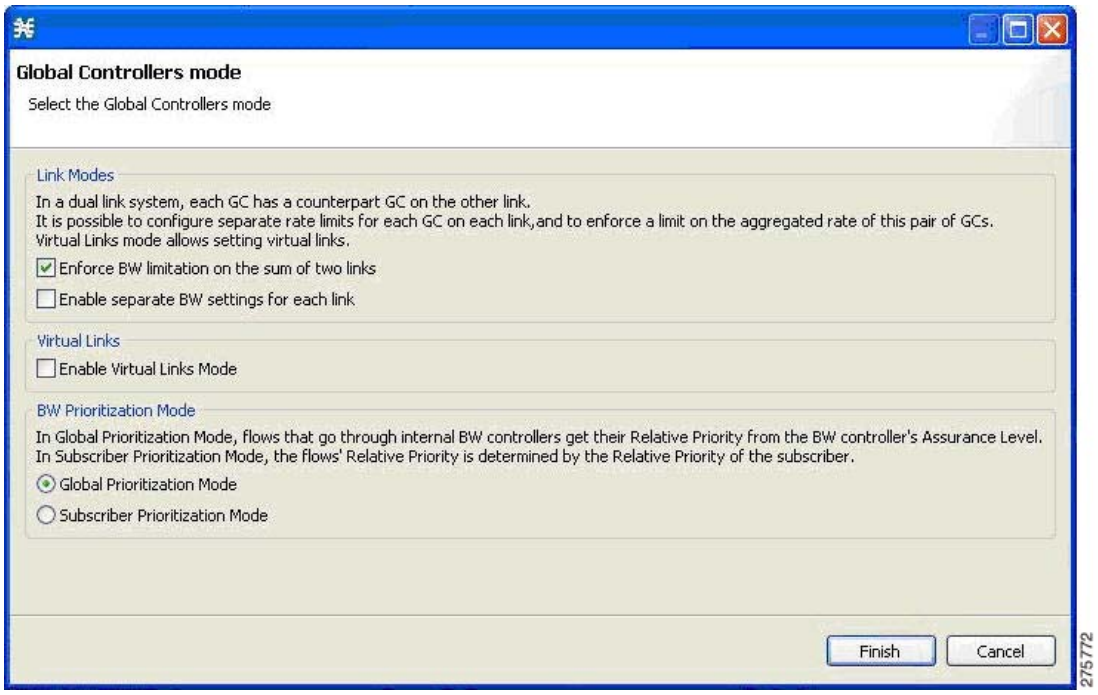
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　「グローバル コントローラの追加」（P.9-6）の説明に従って、グローバル コントローラを追加します。

ステップ 3　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-18）。

図 9-18　[Global Controllers mode]



ステップ 4　[Enforce BW limitation on the sum of the links] チェックボックスをオンにします。

ステップ 5　[Finish] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

ステップ 6　[Policies] タブで [Global Policy] をクリックします。

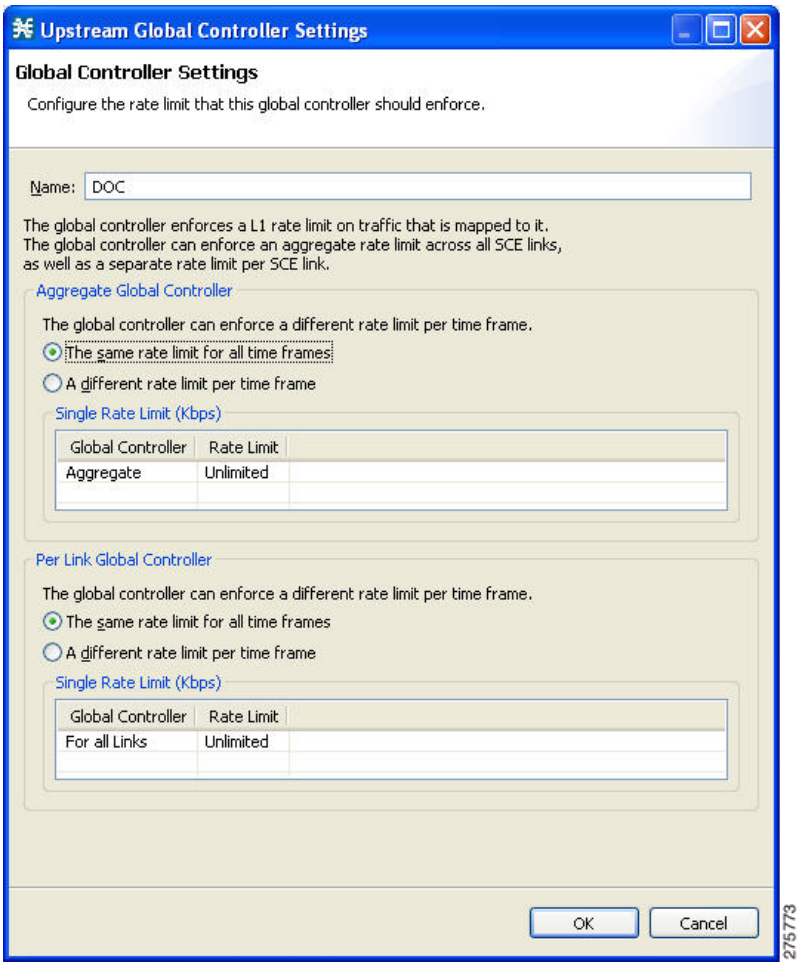
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 7　グローバル コントローラを選択します。

ステップ 8　([Edit]）を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-19）。

図 9-19　[Upstream Global Controller Settings]



（注）　すべての時間枠のレート制限を同じにする場合は、ステップ 9 を実行します。すべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 10 を実行します。

ステップ 9　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a. [Aggregate Global Controller] タブの [The same rate limit for all time frames] オプション ボタンを選択します。

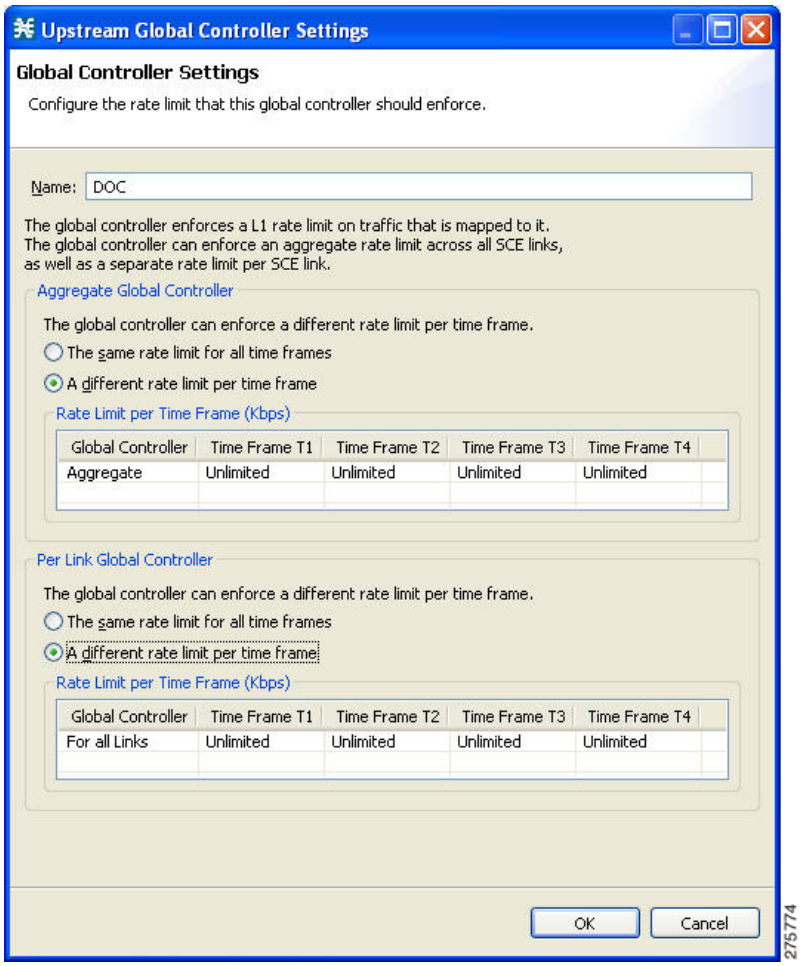
b. [Rate limit for the Per Link Global Controller (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

ステップ 10　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a. [Aggregate Global Controller] タブの [A different rate limit per time frame] オプション ボタンを選択します。

b. 各時間枠で目的とする値を入力します（図 9-20）。

図 9-20　[Upstream Global Controller Settings]



ステップ 11　[OK] をクリックします。

変更が保存されます。

リンクごとに異なるレートを使用し、グローバル コントローラ帯域幅制限を全リンクの合計として設定する方法

このリンク制御モードでは、最大帯域幅はリンクの合計ですが、帯域幅は、全リンクの最大帯域幅に達するまでリンクごとに設定できます。このモードで GC を作成すると、リンクの集約グローバル コントローラを設定したうえで、リンクごとに帯域幅制限を指定できます。このモードは、SCE が複数のエッジ デバイスのサーバとして動作しており、2 つの規則を適用する場合、つまり、1 つの集約的規則をすべてのリンクにまとめて適用し、もう 1 つの規則を個々のリンクに適用する場合に使用されます。このモードでは、全リンクの合計に帯域幅制限を適用し、個別の帯域幅設定をリンクごとにイネーブルにすることができます。リンクを全体的に制御し、リンクごとに異なる最大レートを設定できます。

リンクごとに異なるレートを使用し、グローバル コントローラを全リンクの合計として設定するには、次の手順を実行します。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

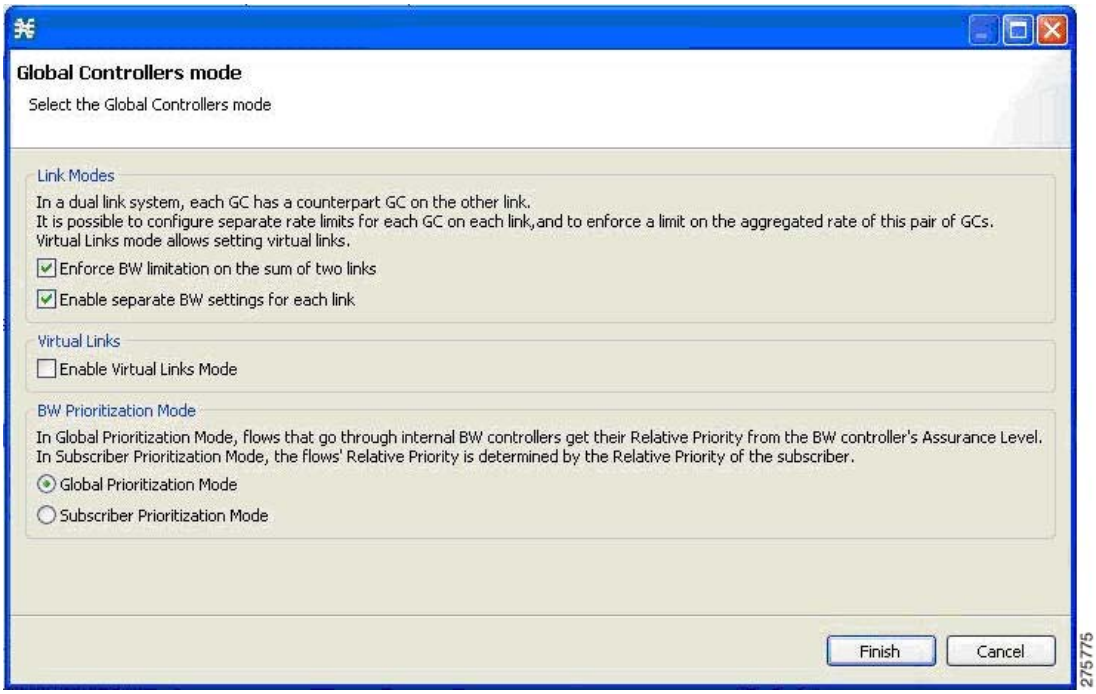
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　「グローバル コントローラの追加」（P.9-6）の説明に従って、グローバル コントローラを追加します。

ステップ 3　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-21）。

図 9-21　[Global Controllers mode]



ステップ 4　[Enforce BW limitation on the sum of the links] および [Enable separate BW setting for each link] チェックボックスを選択します。

ステップ 5　[Finish] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

ステップ 6　[Policies] タブで [Global Policy] をクリックします。

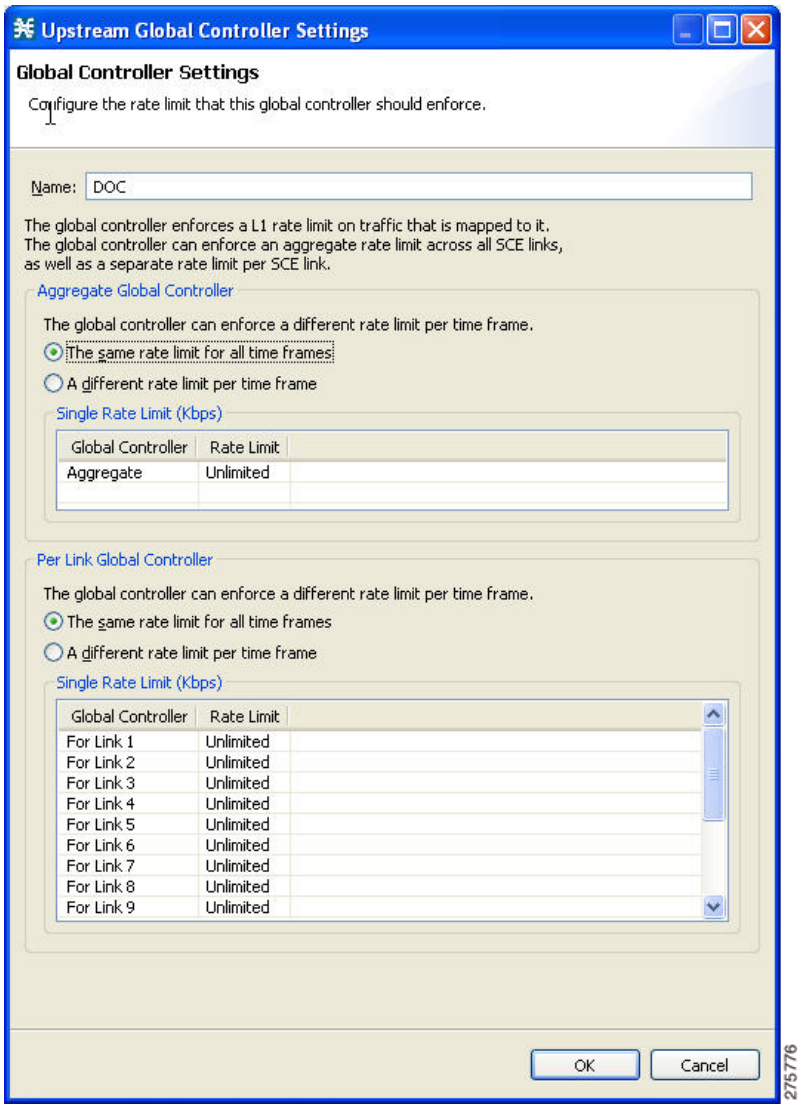
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 7　グローバル コントローラを選択します。

ステップ 8　  （[Edit]）を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-22）。

図 9-22　[Upstream Global Controller Settings]



（注）　すべての時間枠のレート制限を同じにする場合は、ステップ 9 を実行します。すべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 10 を実行します。

ステップ 9　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a. [Per Link Global Controller] タブの [The same rate limit for all time frames] オプション ボタンを選択します。

b. [Rate limit for the Link 1 (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

c. 各リンクに対してステップ 9b を繰り返します。

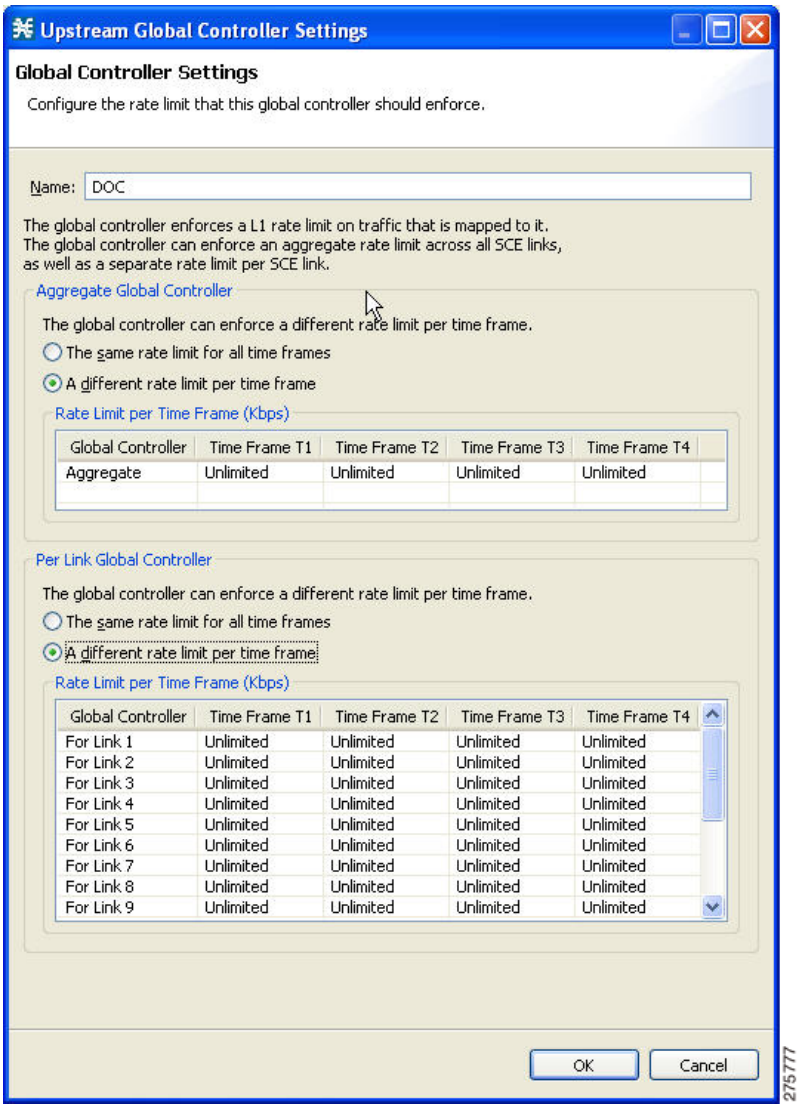
ステップ 10　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a. [Per Link Global Controller] タブの [A different rate limit per time frame] オプション ボタンを選択します。

b. 各時間枠で目的とする値を入力します。

c. 各リンクに対してステップ 10b を繰り返します（図 9-23）。

図 9-23　[Downstream Global Controller Settings]



ステップ 11　[OK] をクリックします。

変更が保存されます。

仮想リンクのグローバル コントローラ帯域幅の設定

このモードでは、設定済みのレート テンプレートとデフォルト レートを使用して各リンクを個別に制御できます。テンプレートのレート制限は、新しく作成される仮想リンクに適用されます。デフォルトのレート制限は、デフォルトの仮想リンク（仮想リンク 0）に適用されます。

仮想リンクにグローバル コントローラを設定するには、次の手順を実行します。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

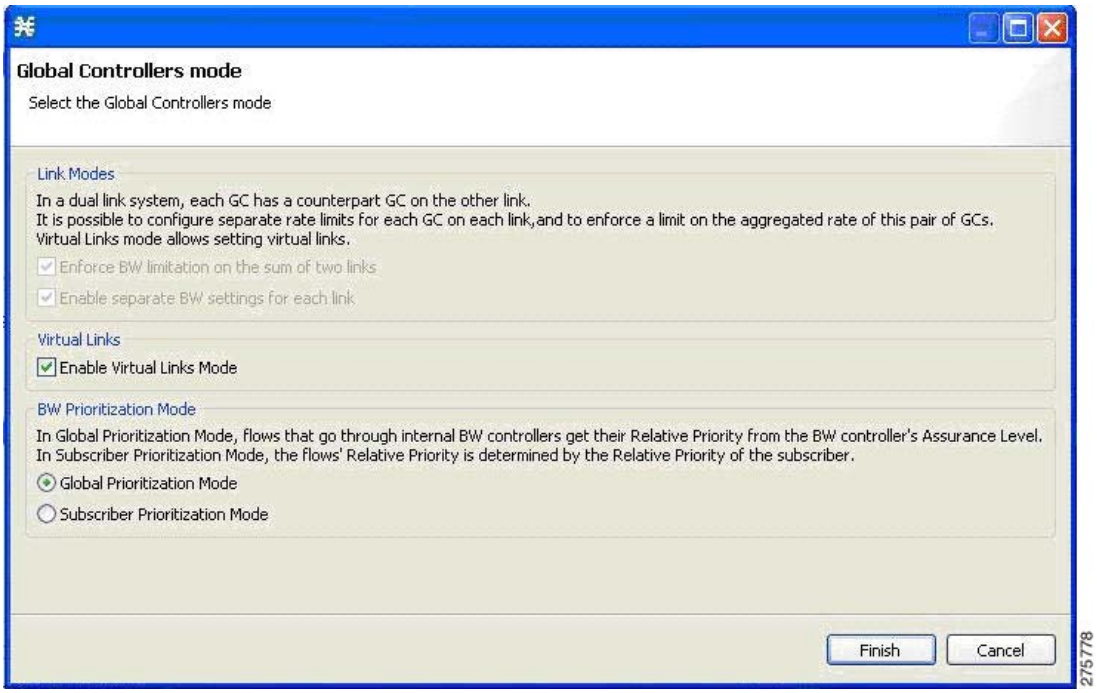
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　「グローバル コントローラの追加」（P.9-6）の説明に従って、グローバル コントローラを追加します。

ステップ 3　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-24）。

図 9-24　[Global Controllers mode]



ステップ 4　[Enable Virtual Links Mode] チェックボックスをオンにします。

ステップ 5　[Finish] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

ステップ 6　[Policies] タブで [Global Policy] をクリックします。

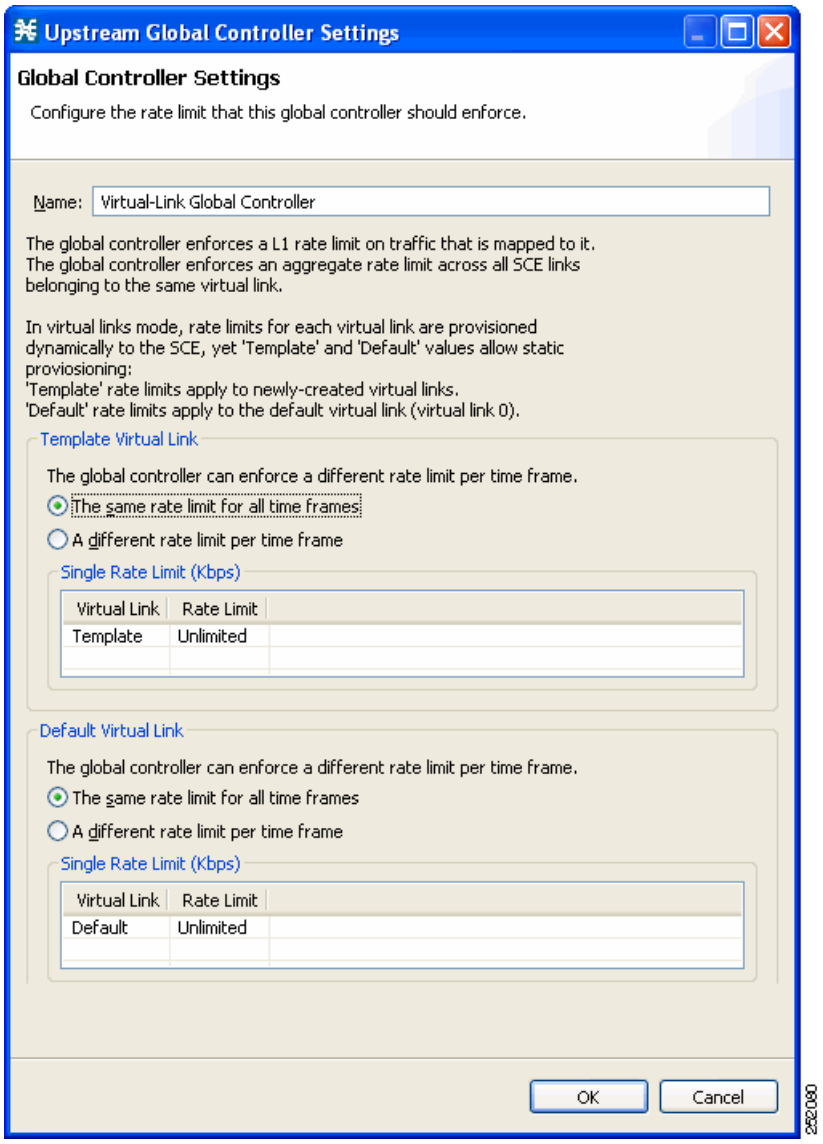
[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 7　グローバル コントローラを選択します。

ステップ 8　  （[Edit]）を選択します。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-25）。

図 9-25　[Upstream Global Controller Settings]



（注）　[Template Virtual Link] ですべての時間枠のレート制限を同じにする場合は、ステップ 9 を実行します。[Template Virtual Link] ですべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 10 を実行します。

ステップ 9　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a. [Template Virtual Link] タブの [The same rate limit for all time frames] オプション ボタンを選択します。

b. [Rate limit for the Link 1 (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

ステップ 10　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a. [Template Virtual Link] タブの [A different rate limit per time frame] オプション ボタンを選択します。

b. 各時間枠で目的とする値を入力します。

（注）　[Default Virtual Link] ですべての時間枠のレート制限を同じにする場合は、ステップ 11 を実行します。[Default Virtual Link] ですべての時間枠のレート制限を時間枠ごとに変える場合は、ステップ 12 を実行します。

ステップ 11　このグローバル コントローラを通過する最大帯域幅制限に単一の値を設定します。

a. [Default Virtual Link] タブの [The same rate limit for all time frames] オプション ボタンを選択します。

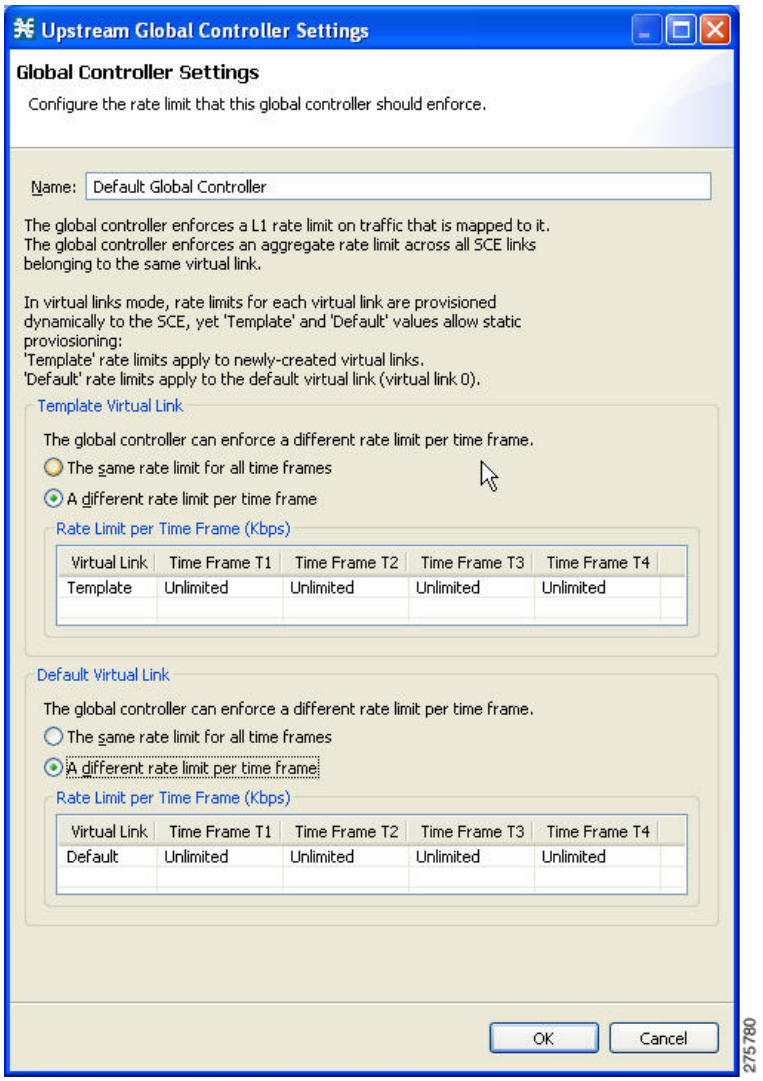
b. [Rate limit for the Link 1 (in Kbps)] フィールドに、目的とする最大帯域幅の値を Kbps 単位で入力します。

ステップ 12　このグローバル コントローラを通過する最大帯域幅制限を設定し、時間枠に応じて変化させます。

a. [Default Virtual Link] タブの [A different rate limit per time frame] オプション ボタンを選択します。

b. 各時間枠で目的とする値を入力します（図 9-26）。

図 9-26　[Upstream Global Controller Settings]



ステップ 13　[OK] をクリックします。

変更が保存されます。

サブスクライバ帯域幅の管理

グローバル コントローラの定義が完了すると、パッケージにサブスクライバ BWC を追加し、これらのサブスクライバ BWC を異なるグローバル コントローラにマッピングすることが可能になります。

サブスクライバ BWC では、アップストリームまたはダウンストリーム フローのサブスクライバ帯域幅消費を制御します。サービスまたはサービス グループのトラフィック フローが集約された帯域幅の制御と測定が行えます。

各パッケージには、各サービスのパッケージ サブスクライバごとに利用可能な帯域幅を決定する独自の BWC セットがあります。

2 つのプライマリ BWC（1 つはアップストリーム トラフィック用、もう 1 つはダウンストリーム トラフィック用）を使用すると、Committed Information Rate（CIR; 認定情報レート）、Peak Information Rate（PIR; 最大情報レート）、およびサブスクライバの相対的なプライオリティ設定に応じて、特定のサブスクライバに帯域幅を割り当てることができます。これらのパラメータの設定は可能ですが、プライマリ BWC の削除はできません。

アップストリーム トラフィック用とダウンストリーム トラフィック用の 2 つのデフォルト BWC があります。デフォルトでは、すべてのサービスはこれらの 2 つの BWC のいずれかにマッピングされます。BWC メカニズムは、CIR、PIR、および Assurance Level（AL）に基づいて、デフォルト BWC の割合制御内で割合のサブパーティショニングを制御します。これらのパラメータの設定は可能ですが、デフォルト BWC の削除はできません。

パッケージごとに最大 32 のユーザ定義 BWC を追加できます。

- サブスクライバ BWC は、サブスクライバ別のサービス レベルで動作します。サブスクライバ BWC は、BWC に設定された CIR、PIR、グローバル コントローラ、および Assurance Level（AL）に基づいて、各サブスクライバのサービスに帯域幅を割り当てます。各規則は、サービスのフローといずれかの BWC とのリンクを定義します（フローがブロックされていない場合）。「規則のためのフローごとのアクションの定義」（P.9-60）を参照してください。
- エキストラ BWC はサブスクライバ レベルでも動作します。エキストラ BWC（CIR、PIR、グローバル コントローラ、および AL に基づく）は、プライマリ BWC に含まれないサービスに割り当てることができます。ビデオ会議のように、頻繁に使用されるわけではないが厳格な帯域幅要件を持つサービスが該当します。エキストラ BWC は単一サービス（サービス グループ）を制御する BWC です。BWC がエキストラ BWC から帯域幅を借りたり、その逆を行うことはできません。

ユーザ定義 BWC は、ダウンストリーム トラフィックまたはアップストリーム トラフィックを制御します。

注意　仮想リンク モードのイネーブル化またはディセーブル化を行うと、サービス コンフィギュレーションからすべてのユーザ定義グローバル コントローラが削除されます。それまでユーザ定義グローバル コントローラを示していた BWC は、デフォルト グローバル コントローラを示します（BWC の他のパラメータは変更されません）。

- 「サブスクライバ BWC パラメータ」（P.9-29）
- 「パッケージ サブスクライバ BWC の編集」（P.9-29）

サブスクライバ BWC パラメータ

[Package Settings] ダイアログボックスの [Subscriber BW Controllers] タブには、次の設定パラメータがあります。

- [Name]：BWC の一意の名前
- [CIR (L3 Kbps)]：BWC で制御されるトラフィックに設定する必要がある最小帯域幅
- [PIR (L3 Kbps)]：BWC で制御されるトラフィックに許容される最大帯域幅

（注）　サブスクライバ BWC の帯域幅は、16 Kbps の細かさで設定できます。

たとえば、64 Kbps の帯域幅を指定した場合、帯域幅はこの値で安定します。

70 Kbps を指定した場合、帯域幅は安定せず 64 ～ 80 Kbps の間で変動します。

- [Global Controller]：現在の BWC を対応付けるグローバル コントローラ。グローバル コントローラは、帯域幅制御メカニズムに含まれる仮想キューです。同様の帯域幅制御プロパティを持つトラフィックを、同じグローバル コントローラに誘導します。
- [AL]：輻輳増加時に BW が PIR から CIR に低下する速度、または輻輳緩和時に BW が CIR から PIR に増大する速度。AL が小さい場合よりも、AL の値が大きい方が、帯域幅が大きくなります。最小の保証値は 1、最大の保証値は Persistent（永続的）です。

  AL が 10（永続的）の場合、合計回線レートが維持できない場合を除いて、関連する CIR を下回ることはありません。
- [Subscriber relative priority]：サブスクライバのプライマリ BWC に設定される AL。他のパッケージのサブスクライバと帯域幅を競合している場合に、すべてのサブスクライバ トラフィックに設定される保証値を決定します。最小の値は 1、最大の値は 10 です。

（注）　サブスクライバ帯域幅制御（およびアカウンティングとレポート）は、レイヤ 3 ボリュームに基づいています。
グローバル コントローラ帯域幅は、レイヤ 1 ボリュームに基づいています。

パッケージ サブスクライバ BWC の編集

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

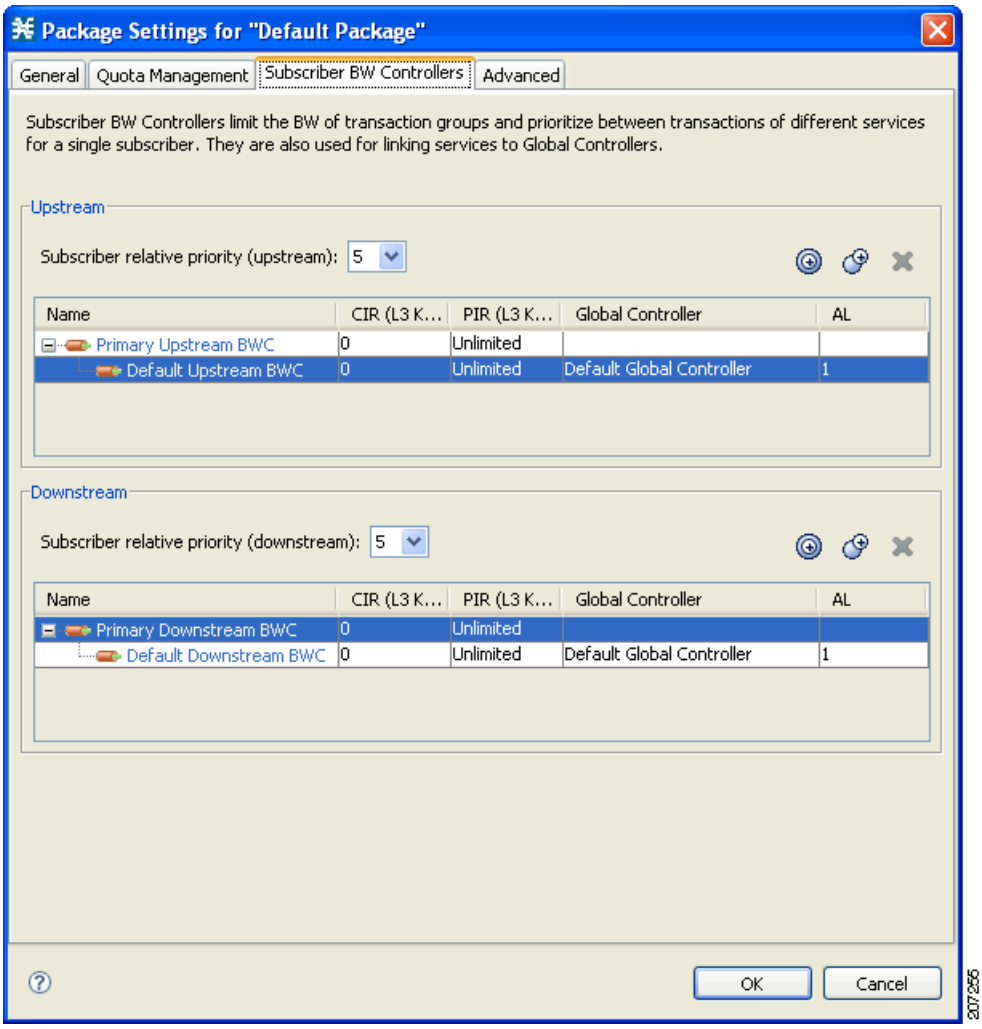
ステップ 2　右の規則ペインで BWC を選択し、  （[Edit]）をクリックします。

[Package Settings] ダイアログボックスが表示されます。

ステップ 3　[Package Settings] ダイアログボックスで、[Subscriber BW Controllers] タブをクリックします。

[Subscriber BW Controllers] タブが開きます（図 9-27）。

図 9-27　[Subscriber BW Controllers] タブ



ステップ 4　ダイアログボックスの [Upstream] 領域で、アップストリームの帯域幅制御の要件を設定します。

a. [Subscriber relative priority] ドロップダウン リストから値を選択します。

b. Primary Upstream BWC のパラメータを設定します。

- [CIR] フィールドに、BWC CIR を Kbps 単位で入力します。
- [PIR] フィールドで、ドロップダウン リストから [Unlimited] を選択するか、BWC PIR を Kbps 単位で入力します。

c. パッケージに BWC を追加するには、BWC を 1 つ追加するたびに  （[Add a sub BW Controller]）を 1 回クリックします。

d. パッケージにエキストラ BWC を追加するには、BWC を 1 つ追加するごとに  （[Add an extra BW Controller]）を 1 回クリックします。

e. 各 BWC（プライマリ BWC およびデフォルト BWC を含む）のパラメータを設定します。

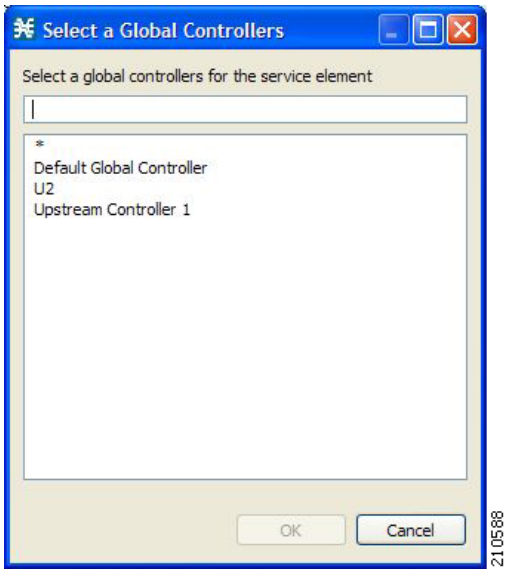
- （オプション）[Name] フィールドに、各 BWC のわかりやすい名前を入力します（プライマリ BWC とデフォルト BWC の名前は変更できません）。
- [CIR] フィールドに、BWC CIR の値を Kbps 単位で入力します。

- [PIR] フィールドで、ドロップダウン リストから [Unlimited] を選択するか、BWC PIR の値を Kbps 単位で入力します。
- 現在の BWC を対応付けるグローバル コントローラを設定するには、次の手順を実行します。

  BWC の [Global Controller] セルをクリックし、表示される [Browse] ボタンをクリックします。

  [Select a Global Controller] ダイアログボックスが表示されます（図 9-28）。

図 9-28　[Select a Global Controller]



- グローバル コントローラを選択し、[OK] をクリックします。
- [AL] ドロップダウン リストから値を選択します。

ステップ 5　ダイアログボックスの [Downstream] 領域でステップ 4 を実行し、ダウンストリームの帯域幅制御を設定します。

ステップ 6　[OK] をクリックします。

[Package Settings] ダイアログボックスが閉じます。

BWC 設定の変更内容が保存されます。

帯域幅の管理：実践例

ここでは、グローバル コントローラとサブスクライバ BWC の設定を組み合わせた効果的な帯域幅制御の実現方法と、実践例について説明します。

- 「合計帯域幅制御の設定」（P.9-32）
- 「例：Console を使用した P2P およびストリーミング トラフィックの制限」（P.9-32）

合計帯域幅制御の設定

ステップ 1　必要なグローバル コントローラを設定します。

問題が発生しやすいサービスと、それぞれに設定する必要がある最大合計帯域幅の値を確定します。問題が発生しにくいサービスやパッケージは設定する必要がありません。これは、デフォルト グローバル コントローラに組み込むことができます。

ステップ 2　パッケージのサブスクライバ BWC を設定します。

a.　制限するアップストリームまたはダウンストリームのトラフィック タイプごとにサブスクライバ BWC を追加して、CIR および PIR を適切に設定します。

b.　各サブスクライバ BWC に対して、適切なグローバル コントローラを選択します。

ステップ 3　独自の BWC を持つ各サービスに対して規則を作成し、適切なアップストリームおよびダウンストリーム BWC を選択します。

例：Console を使用した P2P およびストリーミング トラフィックの制限

（注）　この例は、トラフィック フローが双方向であることを前提としています。したがって、アップストリーム コントローラまたはダウンストリーム コントローラだけが必要であると判断できます。

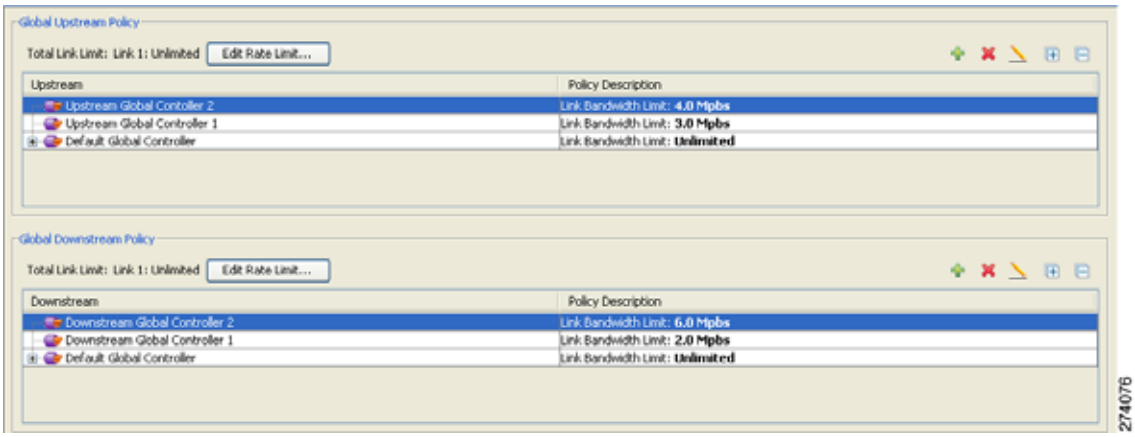
（注）　P2P Traffic Optimization ウィザードでは、デバイスの簡単なモデルの作成とデバイスへの接続が可能です。また、P2P トラフィックを所定の帯域幅に制限することもできます（「P2P Traffic Optimization ウィザードの使用方法」（P.4-46）を参照）。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　2 つのアップストリーム グローバル コントローラと 2 つのダウンストリーム グローバル コントローラを追加し、それぞれのグローバル コントローラに目的とする帯域幅を割り当てます（図 9-29）。

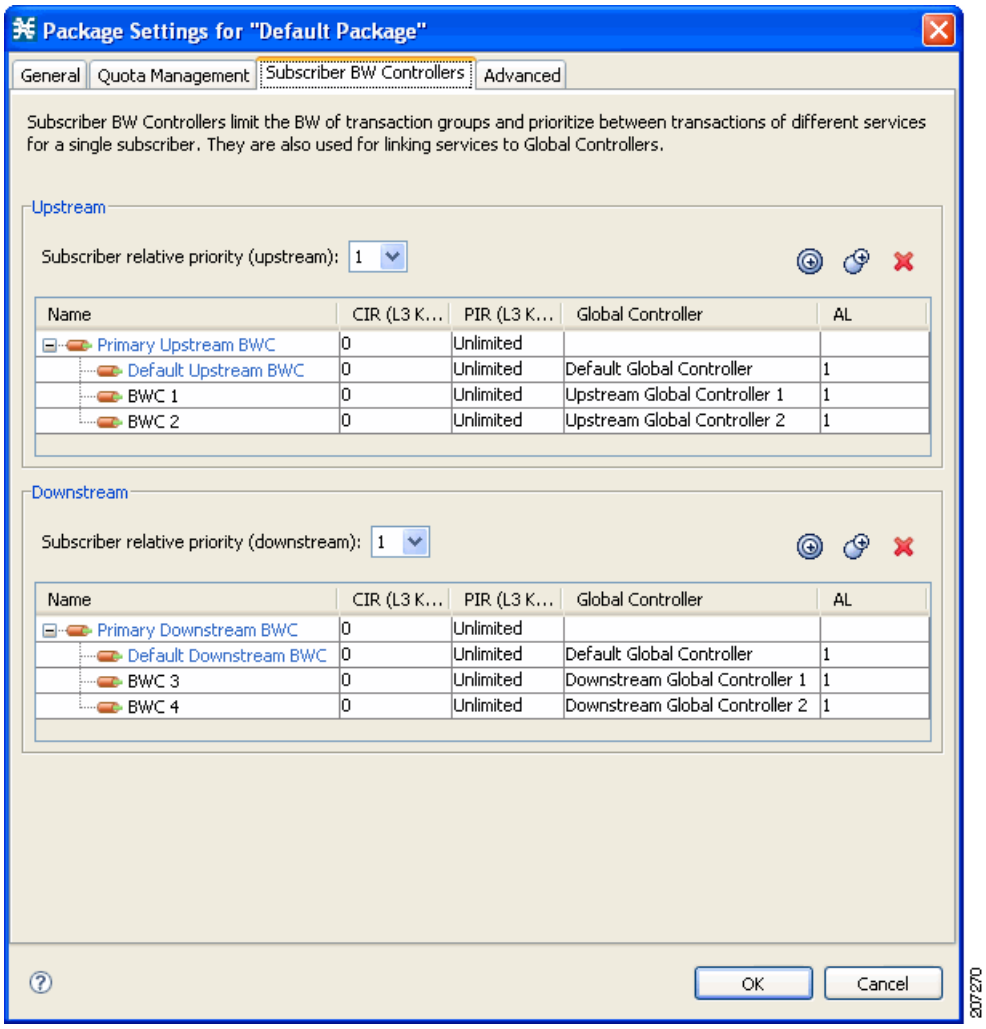
図 9-29　[Global Bandwidth Settings]



（ここでは、P2P トラフィックには Upstream Controller 1 および Downstream Controller 1、ストリーミング トラフィックには Upstream Controller 2 および Downstream Controller 2 が使用されます。）

ステップ 3　[Package Settings] ダイアログボックス（図 9-30）で、2 つのアップストリーム BWC と 2 つのダウンストリーム BWC を追加し、適切なグローバル コントローラにそれらをマッピングし、パラメータ（CIR、PIR、AL）を設定します。

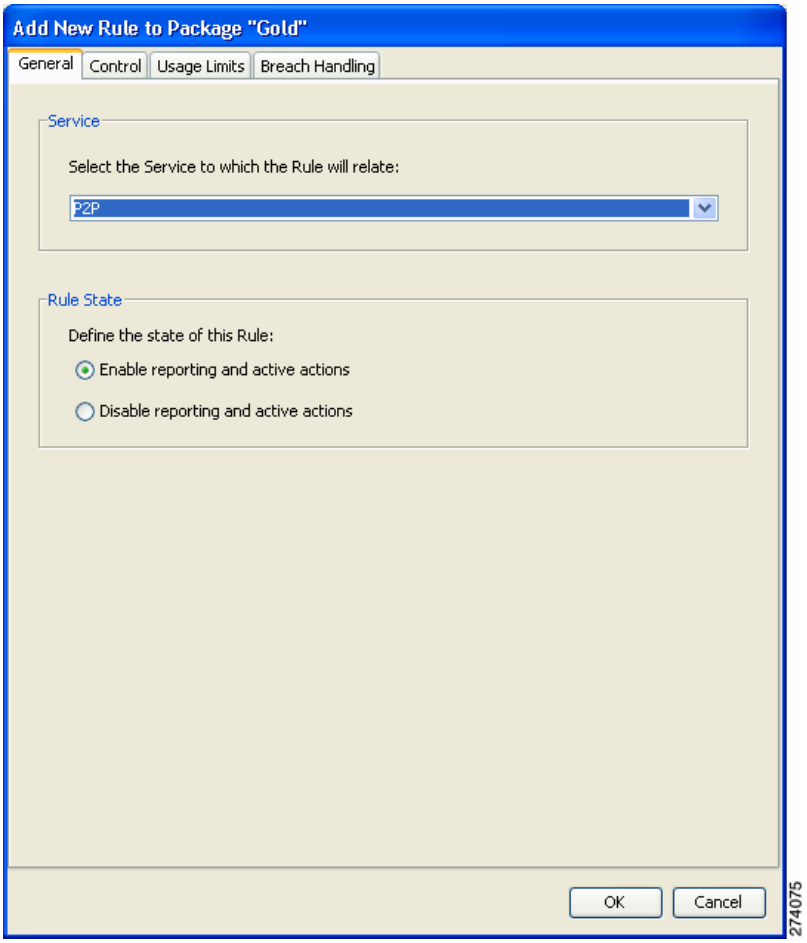
図 9-30　[Package Settings]



（ここでは、BWC1 はアップストリーム P2P トラフィック用、BWC3 はダウンストリーム P2P トラフィック用です。BWC2 はアップストリーム ストリーミング トラフィック用、BWC4 はダウンストリーム ストリーミング トラフィック用です）

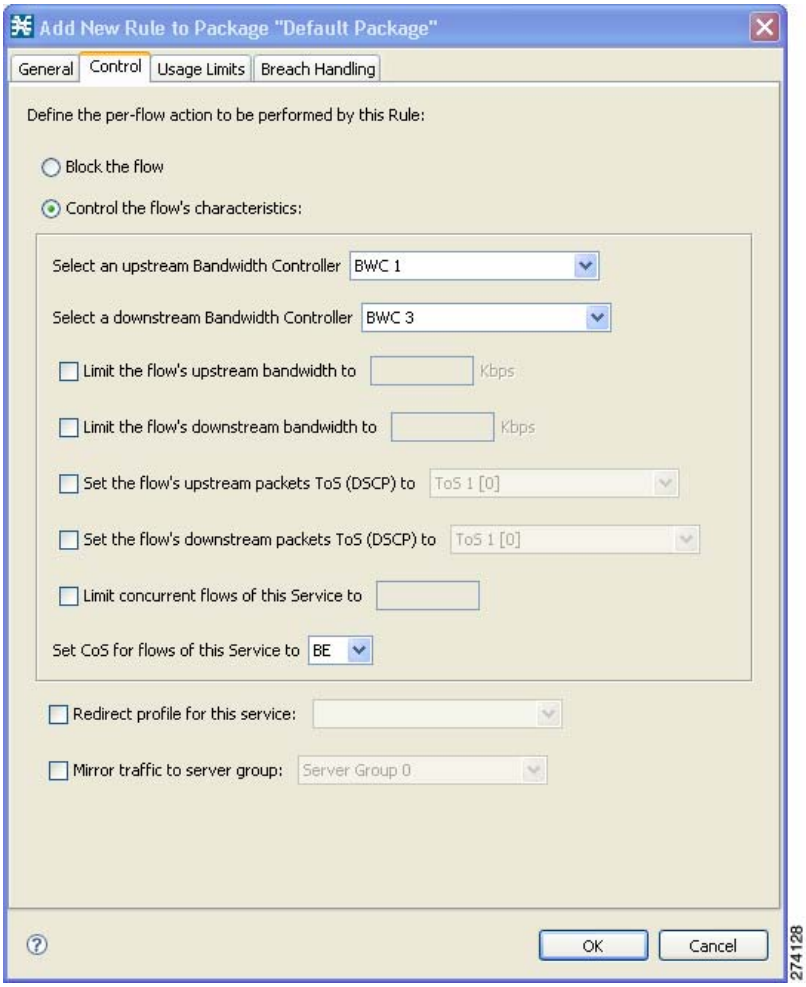
ステップ 4　P2P サービスの規則を追加します（図 9-31）。

図 9-31　[Add New Rule to Package]



ステップ 5　[Control] タブ（図 9-32）で、アップストリーム BWC として BWC 1 を、ダウンストリーム BWC として BWC 3 を割り当てます。

図 9-32　[Control] タブ

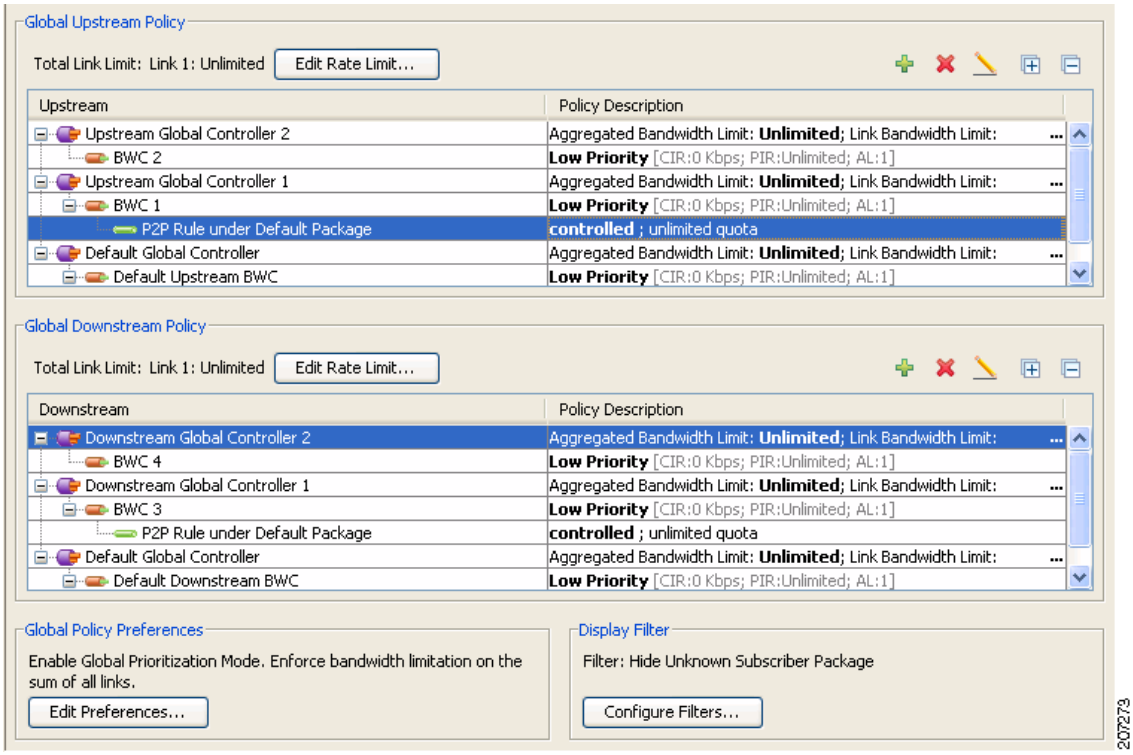


ステップ 6　ストリーミング サービスに対してステップ 4 およびステップ 5 を実行します(アップストリーム BWC には BWC 2 を、ダウンストリーム BWC には BWC 4 を使用)。

これらのサービスを使用するすべてのサブスクライバのトラフィックは、これらのキューに対する仮想キュー合計に加算されます。これらのキューがどれだけ「埋まっている」かに応じて、プロトコルに対してサブスクライバが使用できる帯域幅は変動します。

ステップ 7　[Global Policy] をクリックし、GC、BWC、および規則の階層を表示します（図 9-33）。

図 9-33　規則の階層



ウィザードを使用した規則、帯域幅コントローラ、およびグローバル コントローラの設定

[Global Policy] ウィンドウから、規則、BWC、および GC をまとめて設定できます。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] が右の規則ペインに表示されます。

ステップ 2　目的のインターフェイスの領域（[Upstream] または [Downstream]）上で、([Add]）をクリックします。

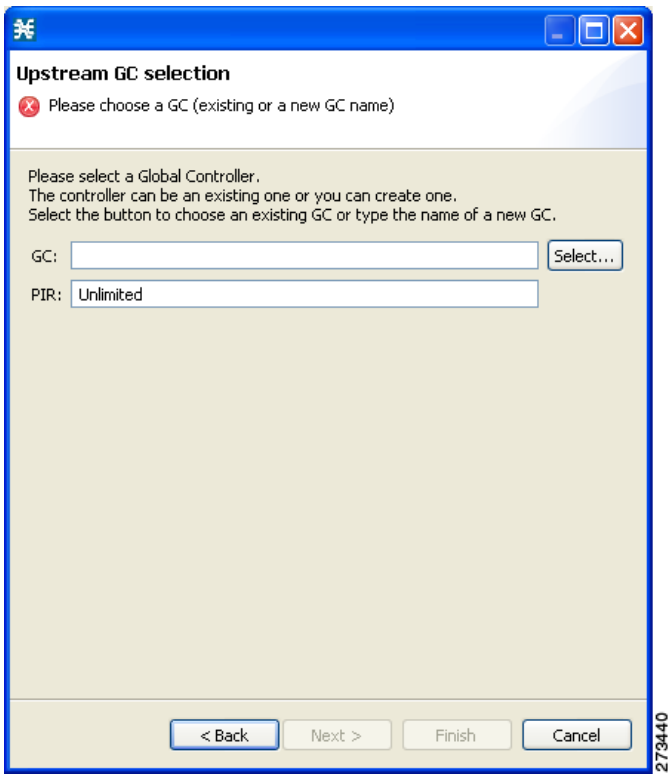
[Select addition mode] ダイアログボックスが表示されます。

ステップ 3　[Add a Global Controller and map a Rule and BWC to it] オプション ボタンを選択します。

ステップ 4　[Finish] をクリックします。

[GC Selection] ダイアログボックスが表示されます（図 9-34）。

図 9-34　[Upstream GC Selection]



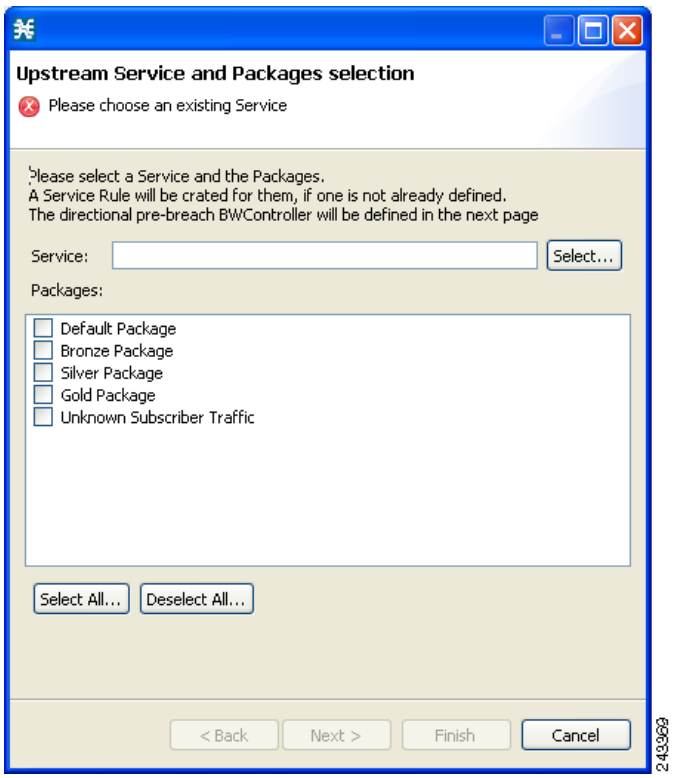
ステップ 5　[GC] フィールドに新しい GC 名を入力するか、[Select] をクリックして既存の GC を選択します。

ステップ 6　（オプション）[PIR] フィールドに、このグローバル コントローラを通過する最大帯域幅制限を Kbps 単位で入力します。

ステップ 7　[Next] をクリックします。

[Service and Packages selection] ダイアログボックスが表示されます（図 9-35）。

図 9-35　[Upstream Service and Packages Selection]



ステップ 8　[Service] フィールドで既存のサービスを選択します。

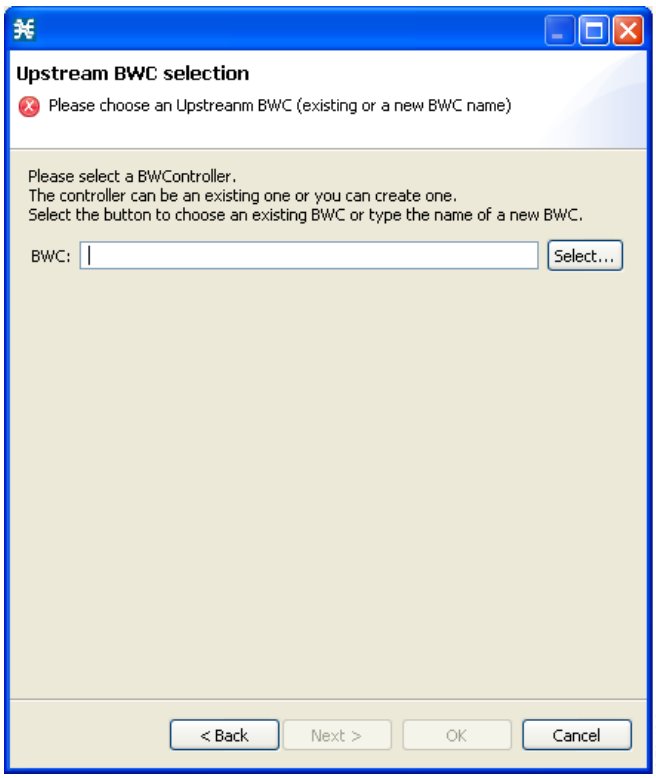
ステップ 9　[Packages] セクションで、規則を適用するパッケージを 1 つ以上選択します。

サービスに対応する規則がない場合は、規則を作成します。選択したパッケージに新規または既存の規則が適用されます。

ステップ 10　[Next] をクリックします。

[BWC selection] ダイアログボックスが表示されます（図 9-36）。

図 9-36　[Upstream BWC Selection]



ステップ 11　新しい BWC 名を入力するか、[Select] をクリックして既存の BWC を選択します。

ステップ 12　[OK] をクリックします。

BW 管理優先順位モードの設定

相対プライオリティは、内部 BWC（iBWC）が、帯域幅について他の iBWC と競合する場合に取得する保証レベルです。

iBWC を通過するフローの相対プライオリティは、次のモードのいずれかの相対プライオリティにより決定されます。

- iBWC：Global Prioritization Mode
- サブスクライバ：Subscriber Prioritization Mode

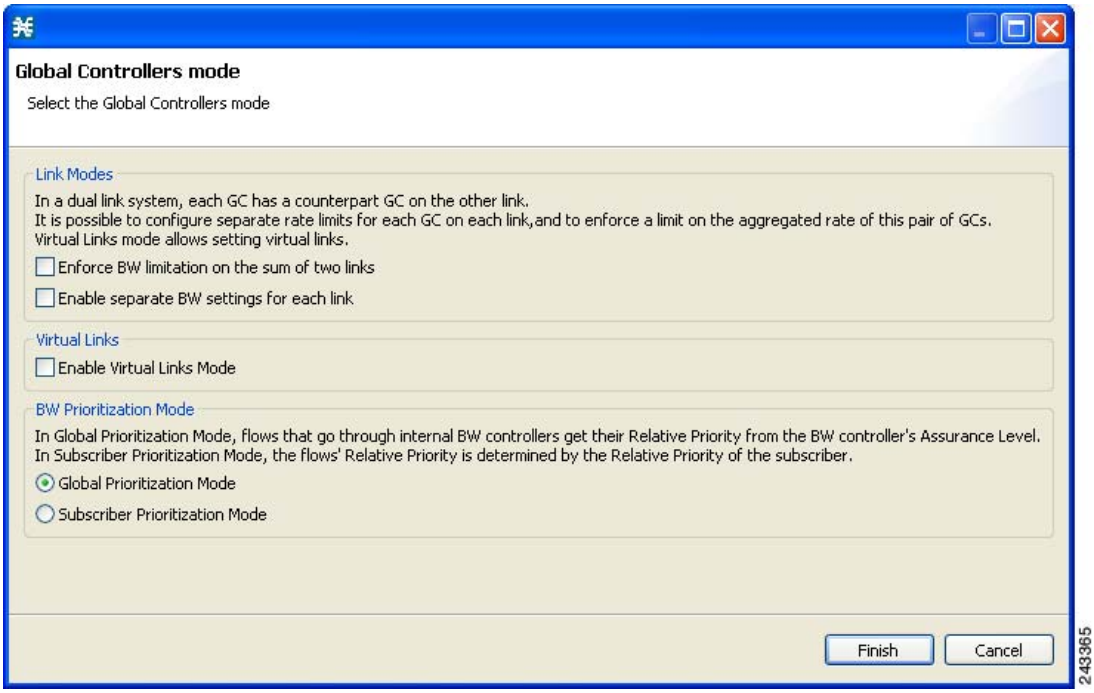
ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] が右の規則ペインに表示されます。

ステップ 2　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます（図 9-37）。

図 9-37　[Global Controllers mode]



ステップ 3　[BW Prioritization Mode] のオプション ボタンをいずれか 1 つ選択します。

- [Global Prioritization Mode]
- [Subscriber Prioritization Mode]

ステップ 4　[OK] をクリックします。

[Global Controllers mode] ダイアログボックスが閉じます。

選択した BW 管理パラメータが保存されます。

仮想リンクの管理

仮想リンク モードでは、テンプレート帯域幅コントローラがパッケージに定義されます。実際の帯域幅パラメータはサブスクライバがシステムにログインしたときに割り当てられますが、サブスクライバのパッケージ（テンプレート コントローラが定義されている）、およびサブスクライバに割り当てられた物理リンクに応じて異なります。

仮想リンク モードがイネーブルになっている各サービス コンフィギュレーションには、それぞれデフォルトのアップストリーム仮想リンクが 1 つとデフォルトのダウンストリーム仮想リンクが 1 つあります。アップストリーム インターフェイスとダウンストリーム インターフェイスには、それぞれ 1 つずつデフォルトのテンプレート グローバル コントローラが割り当てられています。

このほかにも、テンプレート グローバル コントローラを追加できます。仮想リンクを追加、削除、修正するには Command-Line Interface（CLI; コマンドライン インターフェイス）を使用します。

サービス コンフィギュレーションには、最大で 1024 のアップストリーム グローバル コントローラと 1024 のダウンストリーム グローバル コントローラ（デフォルト グローバル コントローラを含む）を設定できます。仮想リンクの最大数は、方向性を持つテンプレート グローバル コントローラの数により制限されます。テンプレート グローバル コントローラの数に仮想リンクの数を乗じた値は、1024 を超えることができません。

DOCSIS 3.0 ダウンストリーム ボンディングをサポートするためには、ワイドバンド チャネルに対して 2 つのレベルから成る仮想リンク階層を作成します。ワイドバンド チャネルは、入力信号強度の変動に関係なく一定の出力信号を提供する Aggregate Global Control（AGC）に関連付けられます。ワイドバンド チャネルは、2 つのレベルから成る階層で 3 つの AGC に関連付けられます。階層の下位レベルでは、ワイドバンドのすべての 3.0 モデムが 1 つの AGC に集約され、その他の AGC には従来のモデムと 3.0 モデムの両方が含まれます。階層の上位レベルの AGC は、ワイドバンド チャネルの集約帯域幅を制限するために使用されます。

DOCSIS 3.0 ソリューションのサポートの詳細については、『*Cisco Service Control for Managing Remote Cable MSO Links Solution Guide*』を参照してください。

仮想リンク グローバル コントローラの管理の詳細については、「仮想リンク グローバル コントローラの管理」（P.9-45）を参照してください。

注意　仮想リンク モードのイネーブル化またはディセーブル化を行うと、サービス コンフィギュレーションからすべてのユーザ定義グローバル コントローラが削除されます。それまでユーザ定義グローバル コントローラを示していたサブスクライバ BWC は、デフォルト グローバル コントローラを示します （サブスクライバ BWC の他のパラメータは変更されません）。

（注）　仮想リンク モードでポリシーを適用する際、新しいテンプレートに現在適用されているテンプレートとは異なる数のグローバル コントローラが含まれている場合は、[Reset all Virtual Links to Template Rate Limits] を選択する必要があります。これを選択しない場合、適用を実行すると、次のようなエラー メッセージが表示されます。

「Template Upstream Virtual Link differ from the one in the SCE - cannot apply without the force template virtual link option.」

仮想リンク モードでサービス コンフィギュレーションを設定する手順の概要を次に示します。手順は他のサービス コンフィギュレーションを設定する場合と同様ですが、CLI を使用して仮想リンクを追加する必要があります。

1. 新しいサービス コンフィギュレーションを作成します。
2. [Global Bandwidth Settings] ダイアログボックスを開き、[Enable Virtual Links Mode] チェックボックスをオンにします。
3. テンプレート グローバル コントローラを作成します。
4. パッケージを作成します。

   サブスクライバ BW コントローラをパッケージに追加し、該当するグローバル コントローラと関連付けます。
5. サービス コンフィギュレーションを適用します。

   デフォルト グローバル コントローラの帯域幅の値は設定されていますが、他のすべてのグローバル コントローラの値はテンプレートなので設定されていません。
6. CLI を使用して仮想リンクを追加します。

   各仮想リンクは、テンプレート グローバル コントローラ設定の PIR 値を持つグローバル コントローラのセットを取得します。

   必要に応じて、CLI を使用してグローバル コントローラの PIR 値を変更します。

7. サブスクライバを SCE プラットフォームに導入します。アップストリームとダウンストリームの仮想リンクを、サブスクライバとパッケージに関連付けます。
8. サブスクライバの各フローの規則解決は、サブスクライバのパッケージと仮想リンクのグローバル コントローラ設定に従います。

Collection Manager 仮想リンク名ユーティリティ

Collection Manager（CM）には、仮想リンクの名前を管理するためのコマンドライン ユーティリティが含まれています。

CM の仮想リンク名ユーティリティの詳細については、『*Cisco Service Control Management Suite Collection Manager User Guide*』の「Managing the Collection Manager」にある「Managing Virtual Links」を参照してください。

仮想リンク モードのイネーブル化

仮想リンクを使用するには、仮想リンク モードをイネーブルにする必要があります。

注意　仮想リンク モードのイネーブル化またはディセーブル化を行うと、サービス コンフィギュレーションからすべてのユーザ定義グローバル コントローラが削除されます。

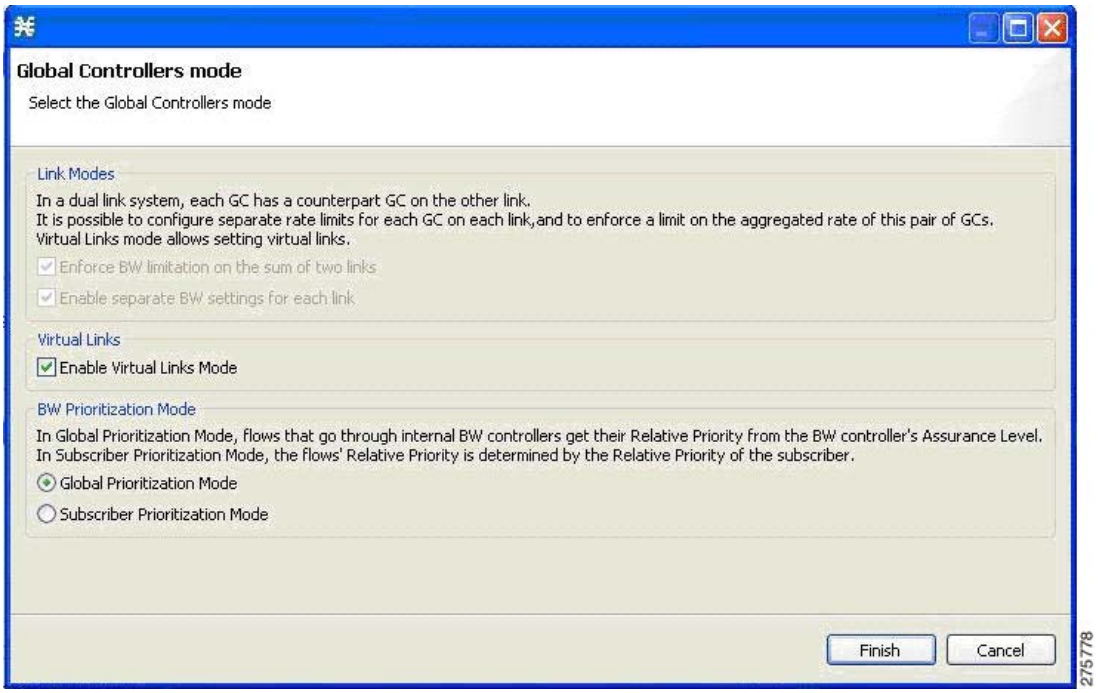
ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] が右の規則ペインに表示されます。

ステップ 2　[Edit Preferences] をクリックします。

[Global Controllers mode] ダイアログボックスが表示されます。

図 9-38　[Global Controllers mode]



ステップ 3　[Enable Virtual Links Mode] チェックボックスをオンにします。

（注）　すでにグローバル コントローラを追加していた場合や、非対称ルーティング分類モードを選択していた場合は、警告メッセージが表示されます。続行する場合は、[OK] をクリックします。

[Virtual Links Global Controllers] タブが開きます。

ステップ 4　[Finish] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが閉じます。

仮想リンク グローバル コントローラ設定の表示

（注）　グローバル コントローラ帯域幅は、レイヤ 1 ボリュームに基づいています
（SCA BB のアカウンティング、レポート、およびサブスクライバ帯域幅制御は、レイヤ 3 ボリュームに基づいています）。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] が右の規則ペインに表示されます。

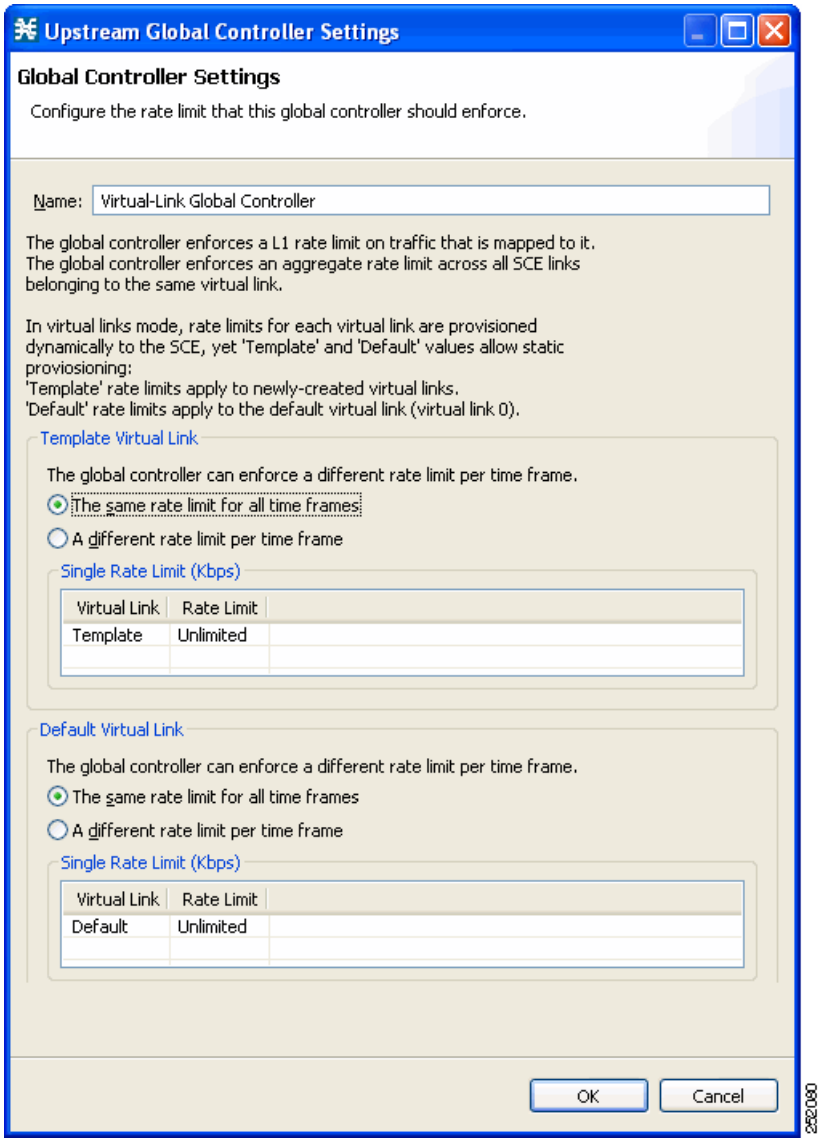
すべてのグローバル コントローラが使用できる最大帯域幅は、[Global Bandwidth Settings] の上部に次のように表示されます。

- [Total Link Upstream Bandwidth Limit: Link 1]
- [Total Link Downstream Bandwidth Limit: Link 1]

ステップ 2　グローバル コントローラを選択し、([Edit]) をクリックします。

[Global Controller Settings] ダイアログボックスが表示されます（図 9-39）。

図 9-39　[Upstream Global Controller Settings]



このダイアログボックスで定義されるグローバル コントローラの値は、[Global Bandwidth Settings] に表示される値により異なります。たとえば、[Total Link Upstream Bandwidth Limit: Link 1] の値が 10 Mbps の場合、アップストリームのデフォルト グローバル コントローラの値は 10 Mbps を超えることができません。

[Name] フィールドには、グローバル コントローラに割り当てられた一意の名前が表示されます。Controller 1、Controller 2 などの名前が自動的に割り当てられます。

このダイアログボックスには、次の 2 つのタブがあります。

- [Template Virtual Link]：すべての時間枠または各時間枠について、作成された仮想リンクのグローバル コントローラに許容される合計リンク制限のデフォルト最大値

- [Default Virtual Link]：すべての時間枠または各時間枠について、デフォルト仮想リンクのグローバル コントローラに許容される合計リンク制限の最大値

ステップ 3　[OK] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが閉じます。

仮想リンク グローバル コントローラの管理

仮想リンク グローバル コントローラは、通常のグローバル コントローラと同じ方法で追加、編集、および削除ができます。詳細については、次のセクションを参照してください。

- 「グローバル コントローラの追加」（P.9-6）
- 「グローバル コントローラの最大帯域幅の設定」（P.9-9）
- 「グローバル コントローラの削除」（P.9-11）
- 「サブスクライバ帯域幅の管理」（P.9-28）

仮想リンクの合計リンク制限の編集

物理リンクを通過する合計帯域幅を制限できます。

アップストリーム トラフィックとダウンストリーム トラフィックの合計リンク制限は、別々に定義されます。

仮想リンク モードでは、帯域幅制限は全リンクの合計に対して適用されます。

ステップ 1　[Policies] タブで [Global Policy] をクリックします。

[Global Bandwidth Settings] ダイアログボックスが右の規則ペインに表示されます。

ステップ 2　[Upstream] または [Downstream] セクションで、[Edit Rate Limit] をクリックします。

[Total Rate Limit] ダイアログボックスが表示されます。

ステップ 3　[Total Rate Limit for each SCE link (Kbps)] フィールドで、プラットフォームを通過する SCE プラットフォーム容量の最大帯域幅を入力するか、Unlimited と入力します。

ステップ 4　[OK] をクリックします。

[Total Rate Limit] ダイアログボックスが閉じます。

[Total Link Bandwidth Limit: Link 1] フィールドがアップデートされます。

CLI コマンドを使用した仮想リンクの管理

SCE プラットフォームの CLI を使用して、仮想リンクの設定、イネーブル化、およびディセーブル化を行うことができます。SCE プラットフォーム CLI の詳細については、『*Cisco SCE8000 CLI Command Reference*』を参照してください。

- 仮想リンクの管理には、次の CLI コマンドを使用します。

```
virtual-links index <index> direction [upstream | downstream]
```

```
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR 1, PIR2, PIR3, PIR4>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR
value <PIR for all timeframes>
virtual-links index <VL index> direction [upstream | downstream] gc <gc index>
reset-PIR
no virtual-links index <index> direction [upstream | downstream]
```

これらのコマンドは、ライン インターフェイス コンフィギュレーション コマンドです。これらのコマンドの実行については、「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.9-47）を参照してください。

- サブスクライバの仮想リンク インデックスを設定するには、次の CLI コマンドを使用します。

```
subscriber name <name> property name [vlUp | vlDown] value <vl index>
```

このコマンドは、ライン インターフェイス コンフィギュレーション コマンドです。このコマンドの実行については、「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.9-47）を参照してください。

- 仮想リンクの状態をモニタするには、EXEC モードで次の CLI コマンドを使用します。

```
Show interface LineCard 0 virtual-links [all | changed | different-from-template]
```

仮想リンクの CLI コマンド

表 9-1 で、仮想リンクの CLI コマンドについて説明します。

表 9-1　仮想リンクの CLI コマンド

コマンド	説明
virtual-links index <index> direction [upstream | downstream]	仮想リンクを追加します。
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR 1, PIR2, PIR3, PIR4>	仮想リンクのグローバル コントローラの PIR 値を更新します。時間枠ごとに値を区切ります。
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> set-PIR value <PIR for all timeframes>	仮想リンクのグローバル コントローラの PIR 値を更新します。すべての時間枠に 1 つの値です。
virtual-links index <VL index> direction [upstream | downstream] gc <gc index> reset-PIR	仮想リンクのグローバル コントローラの PIR 値を更新します。テンプレート グローバル コントローラに定義された値を使用します。
no virtual-links index <index> direction [upstream | downstream]	仮想リンクを削除します。
subscriber name <name> property name [vlUp | vlDown] value <vl index>	サブスクライバの仮想リンク インデックスを設定します。
show interface LineCard 0 virtual-links all	すべての仮想リンクの情報を表示します。
Show interface LineCard 0 virtual-links [all | changed | different-from-template]	変更された PIR またはテンプレート グローバル コントローラに定義された値と異なった PIR を持つ仮想リンクの情報を表示します。

ライン インターフェイス コンフィギュレーション モードの開始方法

ステップ 1　SCE プラットフォームの CLI プロンプト（SCE#）で **configure** と入力します。

ステップ 2　**Enter** キーを押します。

SCE(config)# プロンプトが表示されます。

ステップ 3　**interface LineCard 0** を入力します。

ステップ 4　**Enter** キーを押します。

SCE(config if)# プロンプトが表示されます。

パッケージの管理

パッケージとは、サブスクライバ ポリシーを記述したものです。パッケージは規則の集合であり、規則が関連するサービスにマッピングされているフローが発生した場合のシステムの反応が定義されています。最初にサービスを定義してから（「サービスの管理」（P.7-3）を参照）、パッケージの追加と定義を行うことを推奨します。

SCAS BB のサービス コンフィギュレーションには、削除できないルート パッケージである「デフォルト パッケージ」が含まれています。

他のパッケージが割り当てられなかった場合、または存在しないパッケージが割り当てられた場合は、サブスクライバがデフォルト パッケージにマッピングされます。

サービス コンフィギュレーションには、最大で 5000 のパッケージを設定できます。

パッケージのパラメータ

パッケージは、次のパラメータで定義されます。

- General パラメータ：
  - [Package Name]：パッケージの一意の名前
  - [Description]：（オプション）パッケージの説明
- Quota Management パラメータ：
  - [Quota Management Mode]：サブスクライバ クォータが外部クォータ マネージャによって管理されるか、または SCA BB によって定期的に補充されるかを指定します。
  - [Aggregation Period Type]：クォータが定期的に補充される場合に使用されるクォータ集約時間。
  - [Quota Buckets]：クォータ管理に使用される 16 のリソース バケット。

- Subscriber BW Controllers パラメータ：
  - [Subscriber relative priority]：ネットワーク輻輳時にパケットのサブスクライバに割り当てられる相対プライオリティ。

    アップストリーム フローとダウンストリーム フローには、それぞれ別のプライオリティが定義されます。
  - [Subscriber Bandwidth Controllers]：パッケージに属しているサービスで利用できる CW Controller（BWC）のリスト。各 BWC には、グローバル コントローラへのマッピングなど、各種パラメータが定義されています。

    アップストリーム フローとダウンストリーム フローには、それぞれ別の BWC が定義されます。
- Advanced パラメータ：
  - [Package Index]：システムがパッケージを識別するための一意の番号 （パッケージ名を変更しても、SCE プラットフォームの動作には影響しません）。パッケージ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。
  - [Parent Package]：パッケージ階層内で 1 つ上の階層にあるパッケージ。親パッケージは、複数のパッケージが使用カウンタを共有する場合に重要となります。デフォルト パッケージはパッケージ階層の基本となるパッケージで、親を持ちません。
  - [Package Usage Counters]：各パッケージの総使用量に関するデータを生成するためにシステムによって使用されます。パッケージでは、専用のパッケージ使用カウンタまたは、親パッケージのパッケージ使用カウンタを使用できます。

    使用カウンタは、次の要素で構成されます。
  - システムによって割り当てられた名前（パッケージ名に基づいて作成）。

（注）　カウンタが複数のパッケージに適用されている場合、パッケージ使用カウンタ名にアスタリスクが追加されます。

  - 一意のカウンタ インデックス：カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。
  - [Calendar]：パッケージのタイムベース規則の基礎として使用されるカレンダー。
  - [VAS Traffic Forwarding Table]：パッケージで使用されるフォワーディング テーブル。

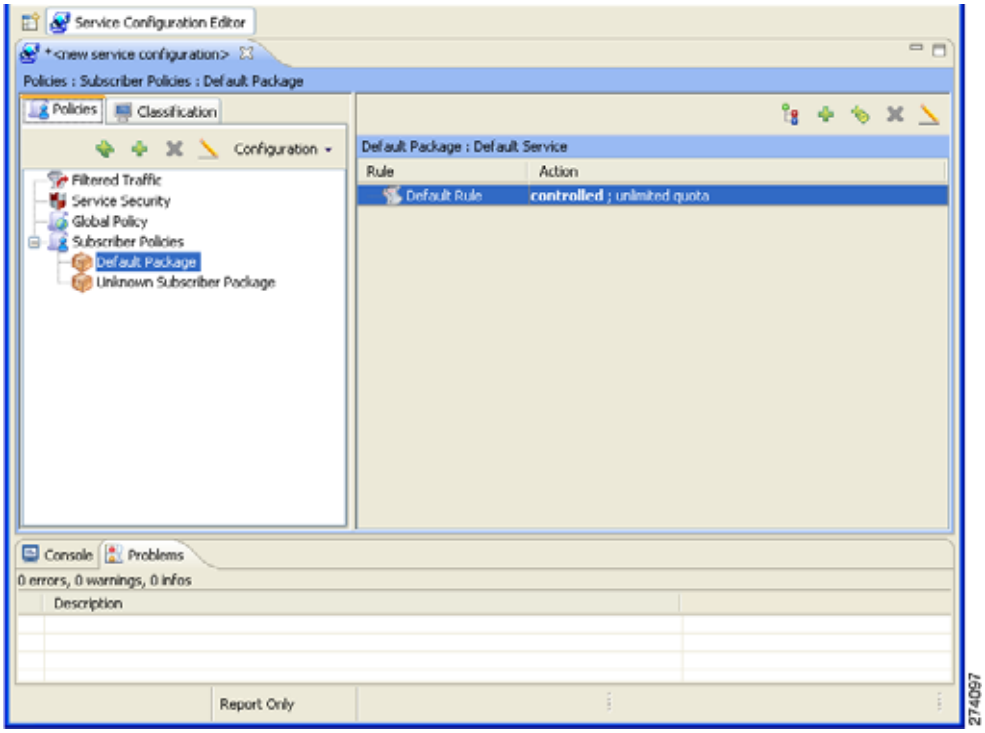
これらのパラメータは、新しいパッケージを追加するときに定義されます（「パッケージの追加」（P.9-50）を参照）。パラメータの修正はいつでもできます（「パッケージの編集」（P.9-54）を参照）。

パッケージの表示

既存のパッケージの階層ツリーを表示し、選択したパッケージに対して特定の規則が定義されたサービスのリストを確認できます。

ステップ 1　現在のサービス コンフィギュレーションで、[Policies] タブをクリックします（図 9-40）。

図 9-40　[Policies] タブ



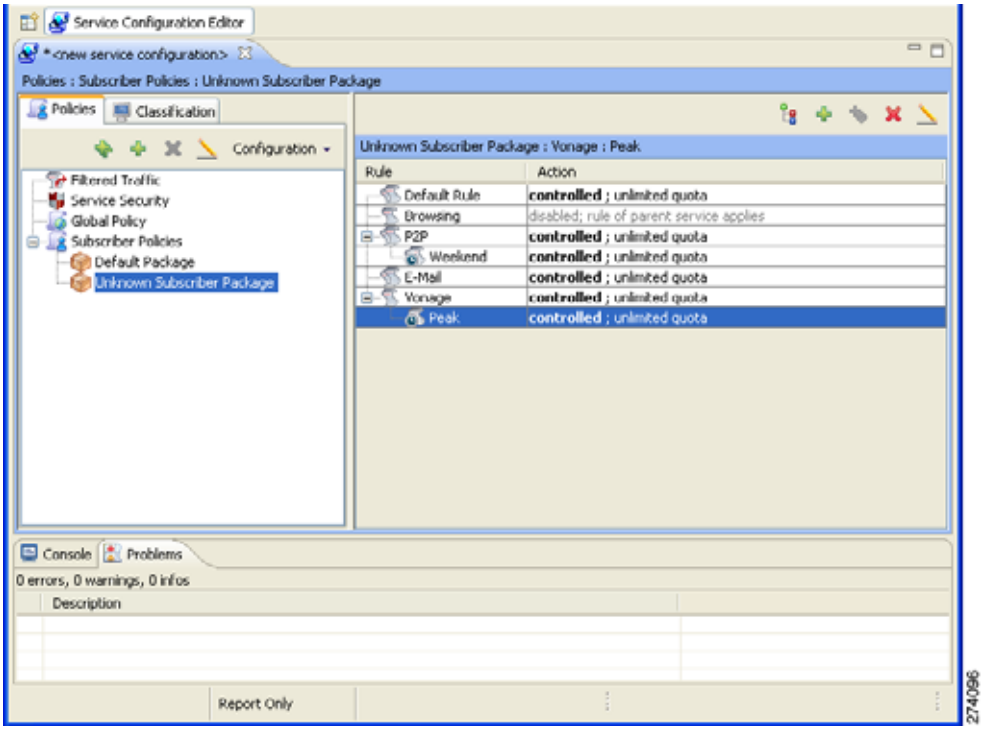
パッケージ ツリーに、パッケージのリストが表示されます。

（注）　パッケージの詳細情報を表示するには、[Package Settings] ダイアログボックスを開きます（「パッケージの編集」（P.9-54）を参照）。

ステップ 2　パッケージの規則を表示するには、階層内のパッケージをクリックします。

このパッケージの規則のリストが右の規則ペインに表示されます（図 9-41）。

図 9-41　Service Configuration Editor



パッケージの追加

Console のインストール時に、デフォルト パッケージがあらかじめ定義されます。サービス コンフィギュレーションには、新しいパッケージを追加できます。ただし、1 つのサービス コンフィギュレーションにつき、設定可能なパッケージは最大 5000 です。

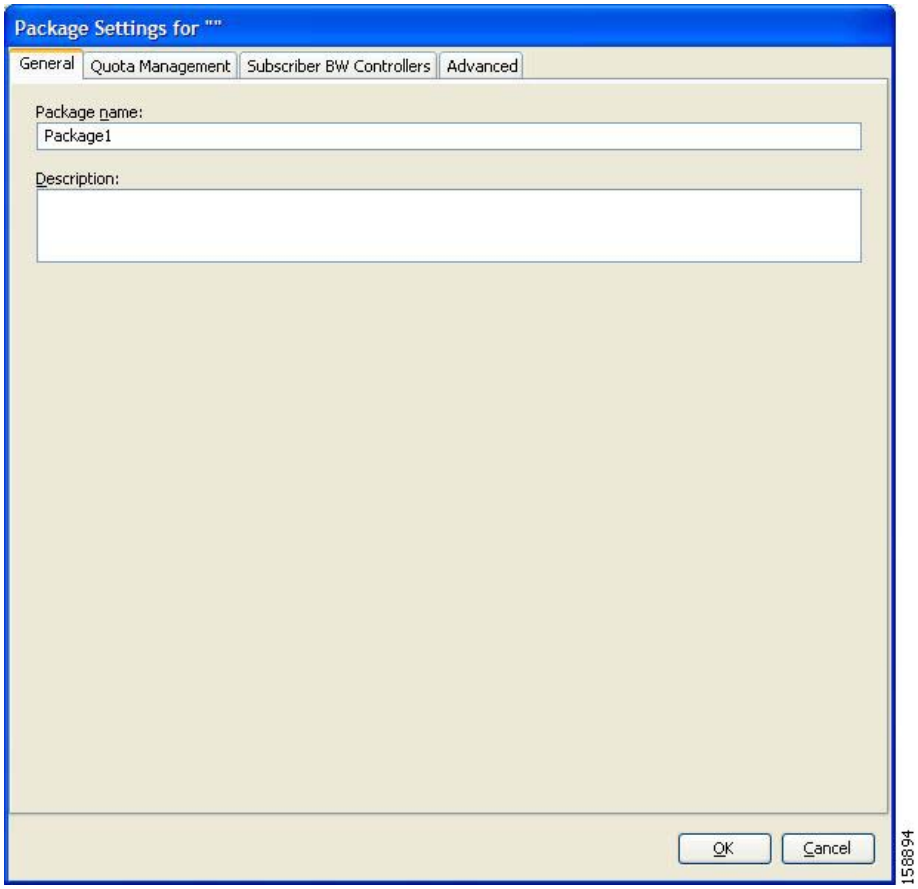
新しいパッケージを追加したら、パッケージの規則を定義できます（「パッケージへの規則の追加」（P.9-58）を参照）。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。このパッケージは、追加するパッケージの親になります。

ステップ 2　[Policies] タブで、  （[Add Package]）をクリックします。

[Package Settings] ダイアログボックスが表示されます（図 9-42）。

図 9-42　[Package Settings]



ステップ 3　[Package name] フィールドに、パッケージに関連する一意の名前を入力します。

ステップ 4　（オプション）[Description] フィールドに、パッケージに関するわかりやすい説明を入力します。

ステップ 5　[Advanced] タブのパラメータを設定するには、次のセクションのステップを実行します。

ステップ 6　[OK] をクリックします。

[Package Settings] ダイアログボックスが閉じます。

新しいパッケージが、パッケージ ツリーで選択されたパッケージの子として追加され、選択されたパッケージとなります。デフォルト サービス規則が右の規則ペインに表示されます。

デフォルト サービス規則を編集し、パッケージに新しい規則を追加する方法については、「規則の管理」（P.9-56）を参照してください。

次の作業

[Quota Management] タブのパラメータを設定するには、「パッケージのクォータ管理設定の編集」（P.9-83）を参照してください。

[Subscriber BW Controllers] タブのパラメータを設定するには、「パッケージ サブスクライバ BWC の編集」（P.9-29）を参照してください。

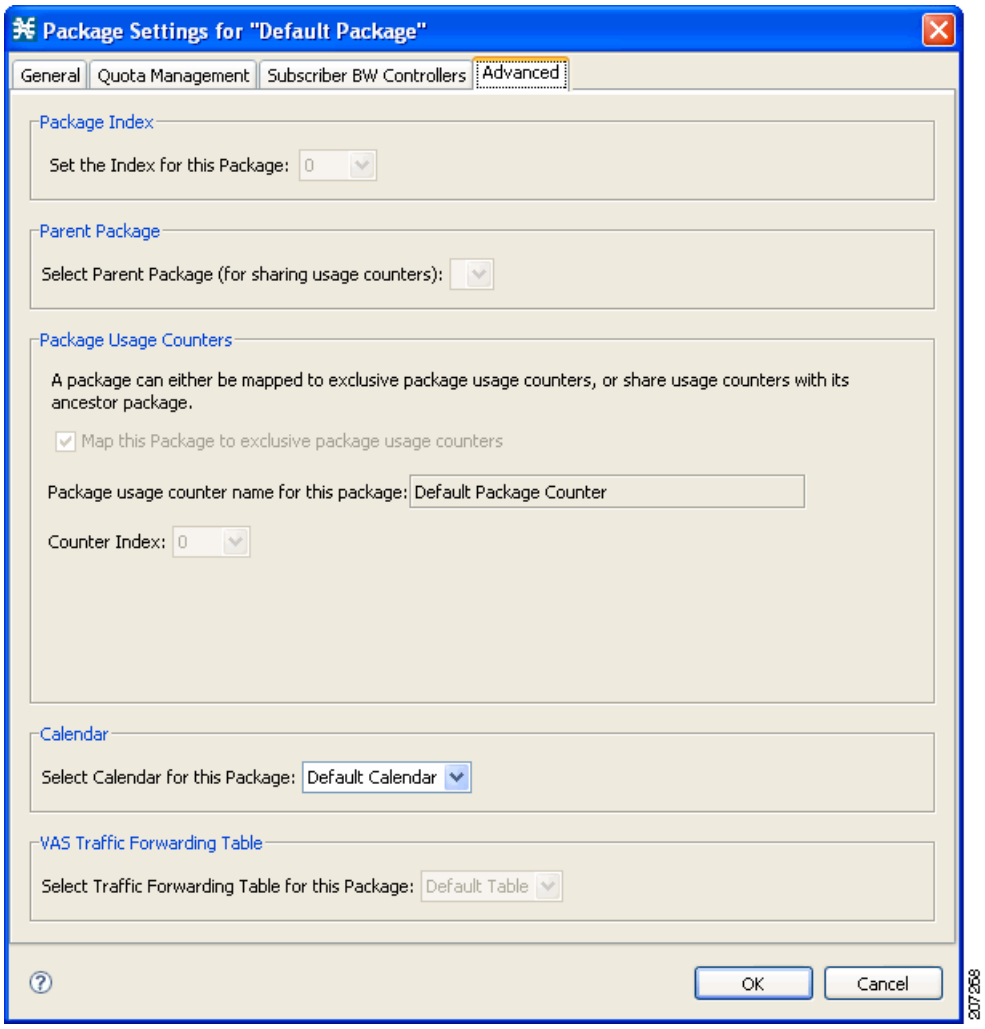
高度なパッケージ オプションの設定

パッケージのインデックスの変更、専用の使用カウンタの指定、またはパッケージのカレンダーの選択を行うには、[Advanced] タブを使用します。

ステップ 1　[Package Settings] ダイアログボックスで、[Advanced] タブをクリックします。

[Advanced] タブが開きます（図 9-43）。

図 9-43　[Advanced] タブ



ステップ 2　このパッケージのパッケージ インデックスを変更するには、[Set the Index for this Package] ドロップダウン リストでパッケージ インデックスを選択します。

（注）　インデックスのデフォルト値がシステムによって割り当てられます。パッケージに特定のインデックス値を割り当てる必要がある場合以外は、この値を修正しないでください。

ステップ 3　このパッケージに別の親パッケージを定義するには、[Select Parent Package] ドロップダウン リストで目的の親を選択します。

ステップ 4　デフォルトでは、新しいパッケージでは専用の使用カウンタが使用されます。親パッケージの使用カウンタを共有するには、[Map this Service to exclusive package usage counters] チェックボックスをオフにします。

このパッケージの読み取り専用パッケージ使用カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがグレー表示になります。

ステップ 5　カウンタ インデックスを変更するには（専用のパッケージ使用カウンタを使用している場合）、[Counter Index] ドロップダウン リストでインデックスの値を選択します。

（注）　インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

ステップ 6　（カレンダーの時間枠をタイムベース規則に使用するために）このパッケージにカレンダーを定義するには、[Select Calendar for this Package] ドロップダウン リストで目的のカレンダーを選択します。

ステップ 7　このパッケージに Value Added Service（VAS）トラフィック フォワーディング テーブルを設定するには、[Select Traffic Forwarding Table for this Package] ドロップダウン リストで目的のトラフィック フォワーディング テーブルを選択します。

（注）　VAS トラフィック フォワーディングがディセーブル（デフォルト）の場合、ドロップダウン リストはグレー表示になります。VAS トラフィック フォワーディングを有効にするには、「VAS トラフィック フォワーディングの有効化」（P.10-53）を参照してください。

ステップ 8　[OK] をクリックします。

[Package Settings] ダイアログボックスが閉じます。

新しいパッケージが、選択した親パッケージの子として追加され、選択されたパッケージとなります。デフォルト サービス規則が右の規則ペインに表示されます。

デフォルト サービス規則を編集し、パッケージに新しい規則を追加する方法については、「規則の管理」（P.9-56）を参照してください。

パッケージの複製

既存パッケージの複製は、既存パッケージに類似した新しいパッケージを作成する場合に便利です。パッケージを複製してから変更する方が、パッケージを最初から定義するよりも短時間で実行できます。

複製されたパッケージは、パッケージ ツリーの元のパッケージと同じレベルに追加されます。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　[Policies] タブで、([Duplicate Package]）をクリックします。

元のパッケージと同じ属性を持つ重複パッケージが作成されます。新しいパッケージの名前は、選択したパッケージの名前のあとに「(1)」（パッケージを複数回複製した場合は「(2)」など）を付加したものになります。

ステップ 3　パッケージのパラメータを修正します（「パッケージの編集」（P.9-54）を参照）。

パッケージの編集

パッケージのパラメータは、（デフォルト パッケージも含めて）いつでも修正できます。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　[Policies] タブで、([Edit Package]）をクリックします。

[Package Settings] ダイアログボックスが表示されます。

ステップ 3　[Package Name] フィールドに、パッケージの新しい名前を入力します。

ステップ 4　[Description] フィールドに、パッケージの新しい説明を入力します。

ステップ 5　（オプション）クォータ管理の設定を変更します。「パッケージのクォータ管理設定の編集」（P.9-83）を参照してください。

ステップ 6　（オプション）帯域幅制御の設定を変更します。「パッケージ サブスクライバ BWC の編集」（P.9-29）を参照してください。

ステップ 7　高度な設定を変更するには、[Advanced] タブをクリックします。

[Advanced] タブが開きます。

a.　このパッケージのパッケージ インデックスを変更するには、[Set the Index for this Package] ドロップダウン リストでパッケージ インデックスを選択します。

（注）　カウンタ インデックスのデフォルト値がシステムによって割り当てられます。パッケージに特定のインデックス値を割り当てる必要がある場合以外は、この値を修正しないでください。

b.　このパッケージの親パッケージを変更するには、[Select Parent Package] ドロップダウン リストで目的の親を選択します。

c.　親パッケージの使用カウンタを共有するには、[Map this Service to exclusive package usage counters] チェックボックスをオフにします。

このパッケージの読み取り専用パッケージ使用カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがグレー表示になります。

d.　専用のパッケージ使用カウンタを使用するには、[Map this Service to exclusive package usage counters] チェックボックスをオンにします。

このパッケージの読み取り専用パッケージ使用カウンタの名前が、選択内容を反映して変更されます。

[Counter Index] ドロップダウン リストがグレー表示になります。

e.　カウンタ インデックスを変更するには（専用のパッケージ使用カウンタを使用している場合）、[Counter Index] ドロップダウン リストでインデックスの値を選択します。

（注）　カウンタ インデックスのデフォルト値がシステムによって割り当てられます。この値は変更しないでください。

f. このパッケージで使用するカレンダーを変更するには、[Select Calendar for this Package] ドロップダウン リストで目的のカレンダーを選択します。

g. このパッケージの VAS トラフィック フォワーディング テーブルを変更するには、[Select Traffic Forwarding Table for this Package] ドロップダウン リストで目的のトラフィック フォワーディング テーブルを選択します。

（注）　VAS トラフィック フォワーディングがディセーブル（デフォルト）の場合、ドロップダウン リストはグレー表示になります。VAS トラフィック フォワーディングを有効にするには、「VAS トラフィック フォワーディングの有効化」（P.10-53）を参照してください。

ステップ 8　[OK] をクリックします。

[Package Settings] ダイアログボックスが閉じます。

パッケージ パラメータの変更内容が保存されます。

パッケージの削除

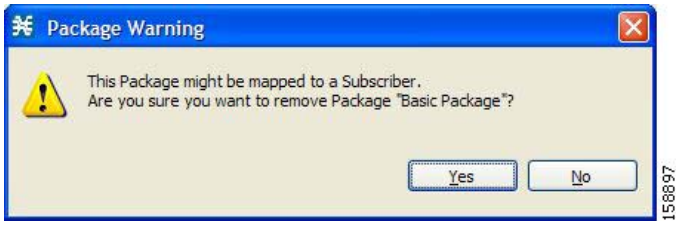
ユーザ定義パッケージは削除できます。デフォルト パッケージは削除できません。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　[Policies] タブで、  （[Delete Package]）をクリックします。

[Package Warning] メッセージが表示されます（図 9-44）。

図 9-44　[Package Warning]



ステップ 3　[Yes] をクリックします。

パッケージが削除され、パッケージ ツリーに表示されなくなります。

規則の管理

サービスと基本パッケージの定義が完了すると、パッケージの規則を定義できるようになります。

次の一部、またはすべてを実行する規則を設定できます。

- サービスのブロック
- サービスの最大帯域幅の定義
- フロー パケットの Differentiated Service Code Point（DSCP; Diffserv コード ポイント）Type of Service（ToS）値の変更
- サービスのクォータの設定
- このサービスのクォータで違反が発生したときの動作の定義

通常、規則は常に適用されます。柔軟な設定を行うため、1 週間を 4 つの時間枠に分割できます。各時間枠に対して、サブ規則（タイムベース規則）を定義できます。

デフォルト サービス規則

デフォルト サービス規則は、すべてのパッケージに割り当てられます。削除したりディセーブルにしたりすることはできません。

この規則のデフォルト値は次のとおりです。

- トラフィックを許可します（ブロックしません）。
- トラフィックをデフォルト BWC にマッピングします。
- アップストリームまたはダウンストリーム トラフィックのクォータを制限しません。

規則の階層

SCE プラットフォームは、最も固有性の高い規則をフローに適用します。

たとえば、E メールと POP3 の規則を定義すると、POP3 サービスにマッピングされたフローは POP3 の規則に従って処理され、SMTP サービスまたは IMAP サービスにマッピングされたフローは、E メールの規則に従って処理されます。そのため、たとえば POP3 には独自の使用制限が適用され、SMTP と IMAP は使用制限を共有することになります。

（注）　子サービスに規則を追加すると、親規則の設定は新しい規則にコピーされません。新しい規則は、デフォルト値で始まります。

子サービスにも適用される規則は、 で示されます。子サービスに適用されない規則は、 で示されます。

タイムベース規則は、関連規則の子として示されます。タイムベース規則のアイコンは、規則が子サービスに適用される場合にも示されます（ または ）。

「規則が影響するサービスの表示」（P.9-64）も参照してください。

パッケージの規則の表示

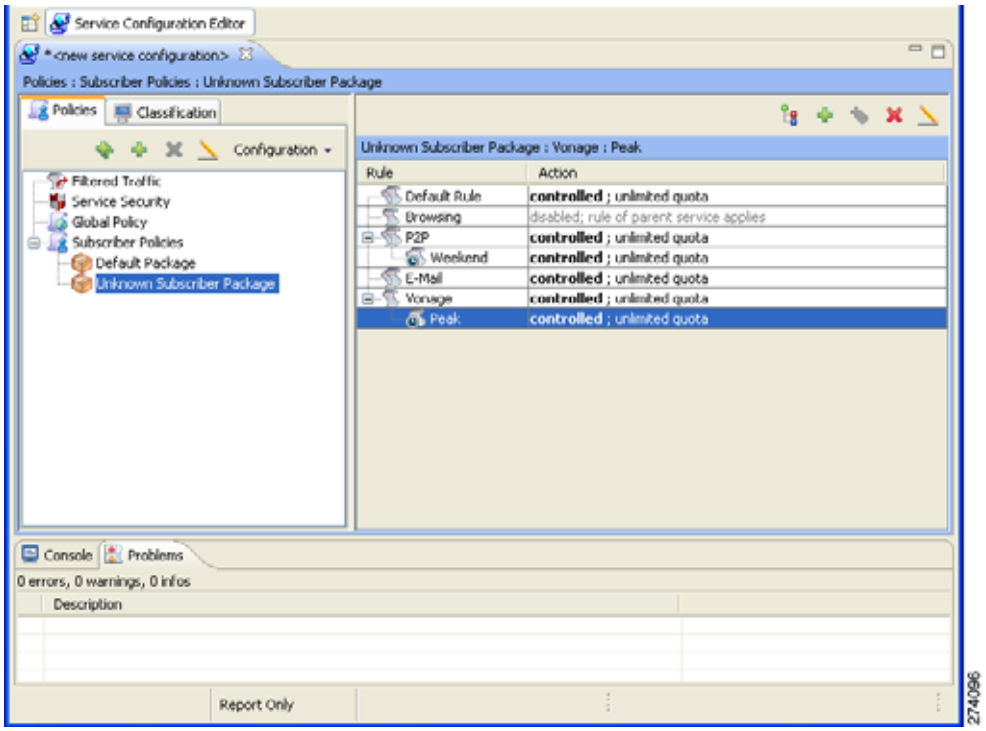
パッケージの規則のリストを表示できます。

各規則のリストには、アイコン、規則が適用されるサービスまたはサービス グループの名前、規則がイネーブルかディセーブルか、規則の簡単な説明が表示されます。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

このパッケージに定義された規則のリストが右の規則ペインに表示されます（図 9-45）。

図 9-45　Service Configuration Editor



次の作業

規則の詳細情報を表示するには、[Edit Rule for Service] ダイアログボックスを開きます（「規則の編集」（P.9-62）を参照）。

タイムベース規則の詳細情報を表示するには、[Edit Time-Based Rule for Service] ダイアログボックスを開きます（「タイムベース規則の編集」（P.9-67）を参照）。

パッケージへの規則の追加

デフォルト サービス規則は、すべてのパッケージに割り当てられます。パッケージに規則を追加することができます。

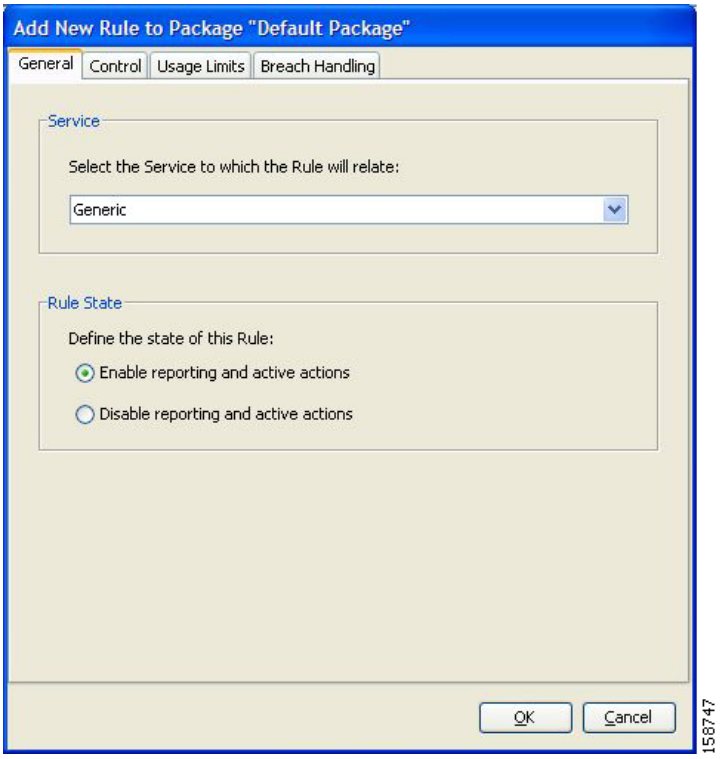
タイムベース規則の追加方法については、「規則へのタイムベース規則の追加」（P.9-65）を参照してください。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、  （[Add Rule]）をクリックします。

[Add New Rule to Package] ダイアログボックスが表示されます（図 9-46）。

図 9-46　[Add New Rule to Package]



ステップ 3　[Add New Rule to Package] ダイアログボックスの [Service] 領域で、[Select the Service to Which the Rule Relates] ドロップダウン リストからサービスを選択します。

（注）　このパッケージに対してすでに規則が定義されているサービスは、グレー表示になります。

ステップ 4　[Rule State] 領域で、[Define the state of this Rule] のオプション ボタンをいずれか 1 つ選択します。

- [Enable reporting and active actions]
- [Disable reporting and active actions]

（注）　規則のイネーブルとディセーブルは、いつでも切り替えができます（「規則の編集」（P.9-62）を参照）。

ステップ 5　（オプション）この規則のトラフィック フローごとの動作を設定するには、「規則のためのフローごとのアクションの定義」（P.9-60）のセクションの手順を実行します。

ステップ 6　[OK] をクリックします。

[Add New Rule to Package] ダイアログボックスが閉じます。

新しい規則が規則のリストに追加され、右の規則ペインに表示されます。

次の作業

使用制限と違反処理は、クォータ管理の一部です（「クォータの管理」（P.9-76）を参照）。

- [Usage Limits] タブのパラメータを設定するには、「規則のためのクォータ バケットの選択」（P.9-84）を参照してください。
- [Breach Handling] タブのパラメータを設定するには、「規則のための違反処理パラメータの編集」（P.9-86）を参照してください。

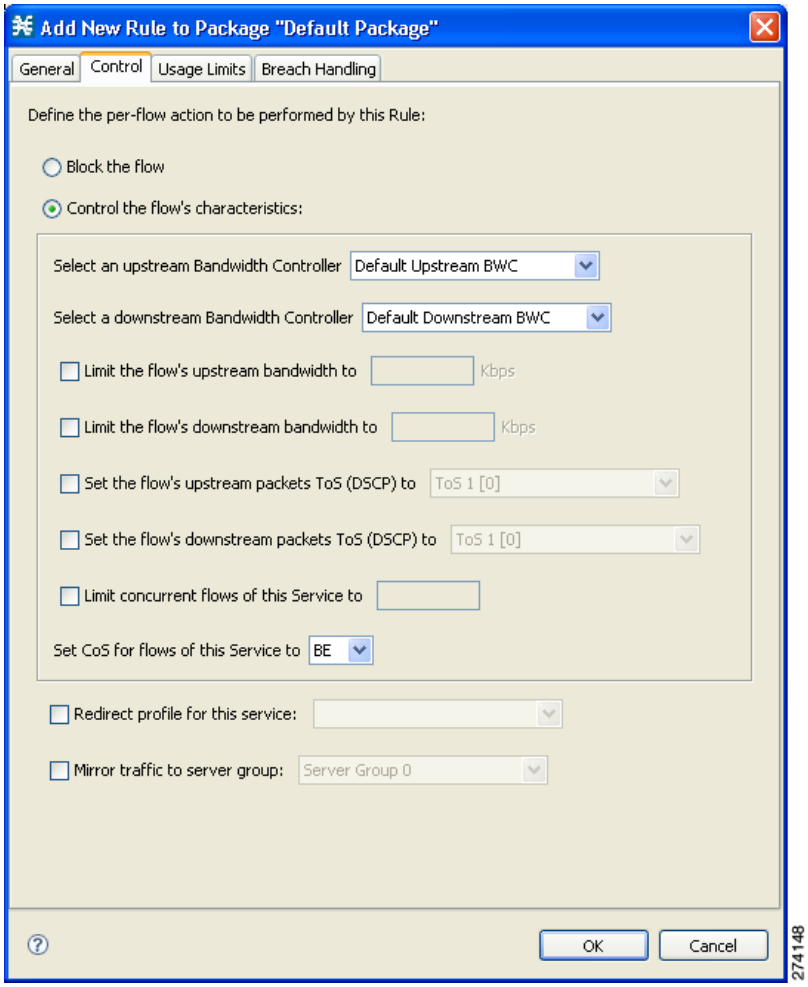
規則のためのフローごとのアクションの定義

[Add New Rule to Package] ダイアログボックスの [Control] タブを使用すると、現在のサービスにマッピングされているセッションに、トラフィック フローごとの動作を設定できます。

ステップ 1　[Add New Rule to Package] ダイアログボックスで、[Control] タブをクリックします。

[Control] タブが開きます（図 9-47）。

図 9-47　[Control] タブ



この規則のサービスにマッピングされているフローを制御するには、ステップ 3 に進みます。

ステップ 2　この規則のサービスにマッピングされているフローをブロックするには、[Block the flow] オプション ボタンを選択し、ステップ 12 に進みます。

ステップ 3　[Control the flow's characteristics] オプション ボタンを選択します。

[Flow Characteristic] 領域のオプションが使用可能になります。

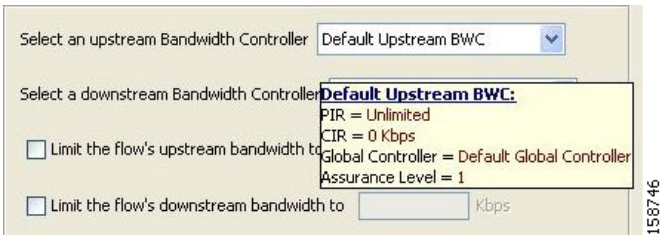
ステップ 4　アップストリームの [Bandwidth Controller] ドロップダウン リストで、アップストリーム BWC を選択します。これにより、選択した BWC の特性に基づいて、この規則にマッピングされたすべての同時フローの帯域幅測定が設定されます。

このドロップダウン リストの BWC は、パッケージの作成時または編集時に定義されます。

注意　タイムベース規則の場合：時間枠ごとに異なるグローバル コントローラ設定が必要な場合、1 つのグローバル コントローラで時間枠ごとに最大帯域幅を定義します。時間枠ごとに個別のグローバル コントローラを作成しないでください。

マウスをドロップダウン リスト上に合わせると、ツールチップ（図 9-48）に、選択した BWC のプロパティ（Peak Information Rate（PIR; 最大情報レート）、Committed Information Rate（CIR; 認定情報レート）、グローバル コントローラ、Assurance Level）が表示されます。

図 9-48　ドロップダウン リストのヒント



ステップ 5　ダウンストリームの [Bandwidth Controller] ドロップダウン リストで、ダウンストリーム BWC を選択します。

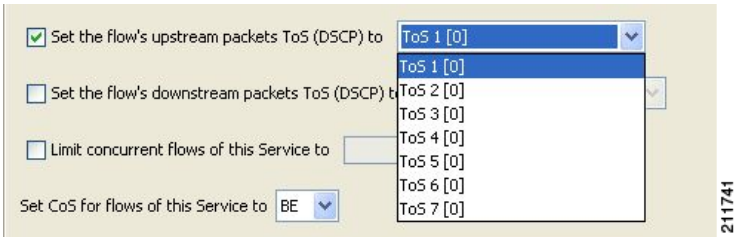
ステップ 6　（オプション）フローごとのアップストリーム帯域幅制限を設定するには、[Limit the flow's upstream bandwidth] チェックボックスをオンにし、[Kbps] フィールドに値を入力します。

（注）　フローごとの帯域幅は、1 Kbps ～ 57 Mbps の細かさで設定できます。

ステップ 7　（オプション）フローごとのダウンストリーム帯域幅制限を設定するには、[Limit the flow's downstream bandwidth] チェックボックスをオンにし、[Kbps] フィールドに値を入力します。

ステップ 8　（オプション）アップストリーム フローの全パケットの DSCP ToS マーカーを変更するには、[Set the flow's upstream packets ToS (DSCP) to] チェックボックスをオンにし、ドロップダウン リストから値を選択します（図 9-49）。

図 9-49　ドロップダウン リストの値



ステップ 9　（オプション）ダウンストリーム フローの全パケットの DSCP ToS マーカーを変更するには、[Set the flow's downstream packets ToS (DSCP) to] チェックボックスをオンにし、ドロップダウン リストから値を選択します。

ステップ 10　（オプション）サブスクライバに許容される（この規則にマッピングされた）同時フローの最大数を設定するには、[Limit concurrent flows of this Service] チェックボックスをオンにし、関連フィールドに値を入力します。

ステップ 11　[Set CoS for flows of this Service] ドロップダウン リストで、Class of Service（CoS; サービス クラス）を選択します。

ステップ 12　（オプション）サブスクライバのリダイレクションをイネーブルにするには、[Redirect profile for this service] チェックボックスをオンにし、ドロップダウン リストからリダイレクト プロファイルを選択します。

ステップ 13　（オプション）トラフィック ミラーリング をイネーブルにするには、[Mirror traffic to server group] チェックボックスをオンにし、ドロップダウン リストからサーバ グループを選択します。

（注）　[Mirror traffic to server group] チェックボックスがイネーブルになるのは、[VAS Settings] ダイアログボックスで [Traffic Mirroring] がイネーブルの場合だけです。

ステップ 14　[OK] をクリックします。

[Add New Rule to Package] ダイアログボックスが閉じます。

新しい規則が規則のリストに追加され、右の規則ペインに表示されます。

規則の編集

規則は、デフォルト サービス規則も含めて、編集できます。

（注）　デフォルト サービス規則は、ディセーブルにできません。

（注）　[Edit Rule for Service] ダイアログボックスのタブは、基本的に [Add New Rule to Package] ダイアログボックスのタブと同じです。ただし、[General] タブは異なり、規則が適用されたサービスは変更できません。

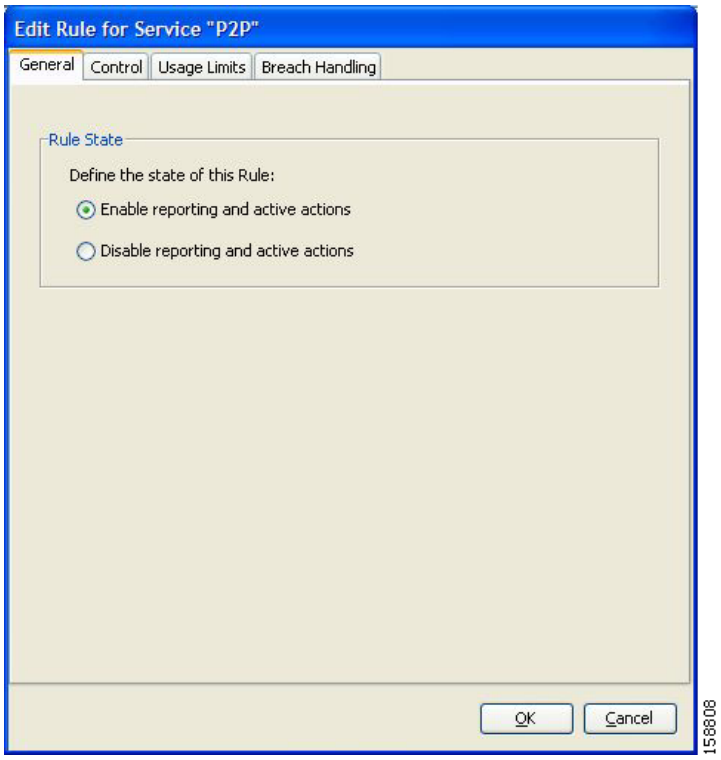
ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、規則を選択します。

ステップ 3　([Edit Rule]）をクリックします。

[Edit Rule for Service] ダイアログボックスが表示されます（図 9-50）。

図 9-50　[Edit Rule for Service]



ステップ 4　[Rule State] 領域で、[Define the state of this Rule] のオプション ボタンをいずれか 1 つ選択します。

- [Enable reporting and active actions]
- [Disable reporting and active actions]

ステップ 5　トラフィック フローごとの動作を変更します。

a. [Control] タブをクリックします。

[Control] タブが開きます。

b. 「規則のためのフローごとのアクションの定義」（P.9-60）の手順に従います。

ステップ 6　使用制限を変更します。

a. [Usage Limits] タブをクリックします。

[Usage Limits] タブが開きます。

b. 「規則のためのクォータ バケットの選択」（P.9-84）の手順に従います。

ステップ 7　クォータで違反が発生したときの動作を定義します。

a. [Breach Handling] タブをクリックします。

[Breach Handling] タブが開きます。

b. 「規則のための違反処理パラメータの編集」（P.9-86）の手順に従います。

ステップ 8　[OK] をクリックします。

[Edit Rule for Service] ダイアログボックスが閉じます。

この規則の変更内容が保存されます。

規則の削除

ユーザ定義規則は削除できます。デフォルト サービス規則は削除できません。

（注）　規則は、プロファイルを保持したまま*ディセーブル*にできます（「規則の編集」（P.9-62）のステップ 4を参照）。このため、あとから規則を再度イネーブルにするとき、パラメータを設定しなおす必要がありません。デフォルト サービス規則は、ディセーブルにできません。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、規則を選択します。

ステップ 3　規則ペインで、  （[Delete Rule]）をクリックします。

[Rule Warning] メッセージが表示されます（図 9-51）。

図 9-51　[Rule Warning]

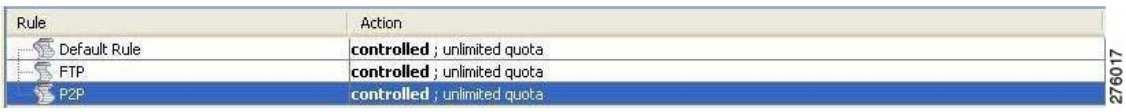
ステップ 4　[Yes] をクリックします。

選択した規則が削除されます。

規則が影響するサービスの表示

サービスは、別のサービスの子として定義できます（親サービスはサービス グループ）。子サービスに独自の規則を定義するまで、子サービスには親サービスの規則が適用されます。サービスの子に影響する規則は、図 9-52 の P2P 規則および FTP 規則のように、規則リスト内で異なるアイコンによって示されます。

図 9-52　規則



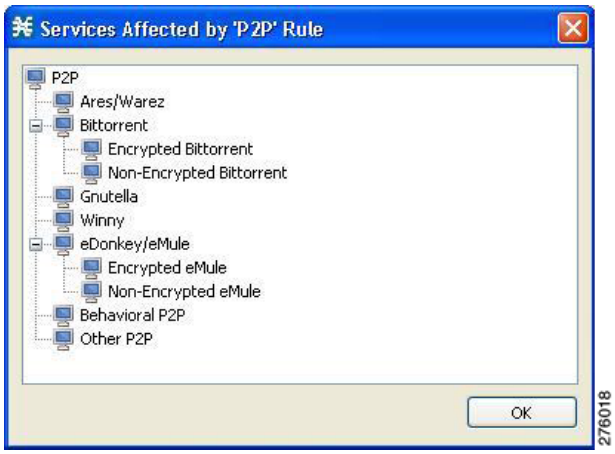
規則が影響するすべての（子）サービスを表示できます。

（注）　デフォルト サービス規則は、特定の規則が*定義されていない*すべてのサービスに適用されます。

ステップ 1　[Network Traffic] タブの右の規則ペインで規則を選択し、([Show All Services Affected By This Rule]）をクリックします。

[Services Affected] ダイアログボックスが表示されます（図 9-53）。

図 9-53　[Services Affected]



ステップ 2　[OK] をクリックします。

[Services Affected] ダイアログボックスが閉じます。

タイムベース規則の管理

Console を使用して、1 週間を 4 つの時間枠に分割できます（「カレンダーの管理」（P.9-69）を参照）。タイムベース規則とは、1 つの時間枠に適用される規則です。

規則には、タイムベース規則を追加できます。時間枠に対してタイムベース規則が定義されていない場合、親規則が適用されます。

異なる時間枠に同様の規則を適用する必要がある場合があります。タイムベース規則を追加するとき、親規則の設定を新しいタイムベース規則にコピーし、必要な変更を行うことができます。親規則に対してそれ以降に行った変更は、タイムベース規則には影響しません。

関連するタイムベース規則を定義する前に、カレンダーを定義する必要があります。

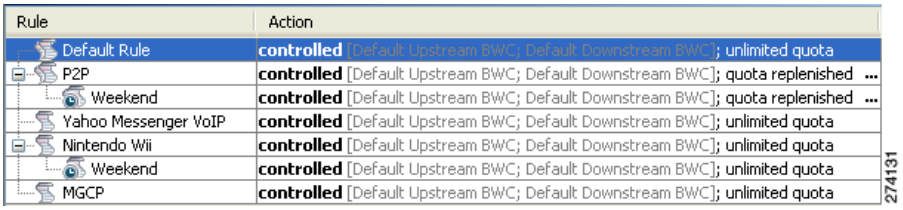
規則へのタイムベース規則の追加

規則にタイムベース規則を追加すると、特定の時間枠にだけ適用可能な代替規則パラメータを指定できます。時間枠に対してタイムベース規則が定義されていない場合、親規則が適用されます。

- タイムベース規則を追加するとき、最初は、パラメータには親規則に定義された値が設定されます。親規則に対してそれ以降に行った変更は、タイムベース規則には反映されません。
- [Add New Time-Based Rule] ダイアログボックスのタブは、基本的に [Add New Rule to Package] ダイアログボックスのタブと同じです。ただし、[General] タブは異なります。[Add New Rule to Package] ダイアログボックスではサービスを選択し、[Add New Time-Based Rule] ダイアログボックスでは時間枠を選択します。

タイムベース規則が子サービスに影響をおよぼすサービスは、図 9-54 に示す P2P 規則の Weekend タイムベース規則のように、規則リスト内で異なるアイコンによって示されます。

図 9-54　　P2P Weekend タイムベース規則



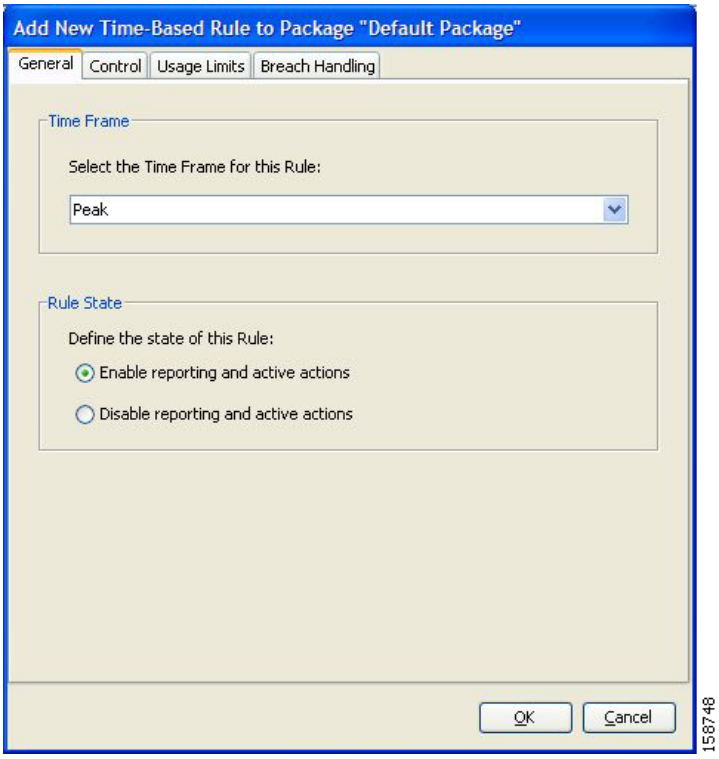
ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、規則を選択します。

ステップ 3　  （[Add Time-Based Rule]）をクリックします。

[Add New Time-Based Rule] ダイアログボックスが表示されます（図 9-55）。

図 9-55　　[Add New Time-Based Rule]



ステップ 4　[Time Frame] 領域の [Select the Time Frame for this Rule] ドロップダウン リストで、4 つの時間枠の中から 1 つを選択します。

ステップ 5　[Rule State] 領域で、[Define the state of this Rule] のオプション ボタンをいずれか 1 つ選択します。

- [Enable reporting and active actions]
- [Disable reporting and active actions]

ステップ 6　トラフィック フローごとの動作を定義します。

a. [Control] タブをクリックします。

[Control] タブが開きます。

b. 「規則のためのフローごとのアクションの定義」（P.9-60）の手順に従います。

ステップ 7　使用制限を変更します。

a. [Usage Limits] タブをクリックします。

[Usage Limits] タブが開きます。

b. 「規則のためのクォータ バケットの選択」（P.9-84）の手順に従います。

ステップ 8　クォータで違反が発生したときの動作を定義します。

a. [Breach Handling] タブをクリックします。

[Breach Handling] タブが開きます。

b. 「規則のための違反処理パラメータの編集」（P.9-86）の手順に従います。

ステップ 9　[OK] をクリックします。

[Add New Time-Based Rule] ダイアログボックスが閉じます。

新しいタイムベース規則が、規則の子として規則ペインに表示されます。

タイムベース規則の編集

タイムベース規則は編集できます。

（注）　[Edit Time-Based Rule for Service] ダイアログボックスのタブは、基本的に [Add New Time-Based Rule] ダイアログボックスのタブと同じです。ただし、[General] タブは異なります。規則が適用されている時間枠は変更できません。

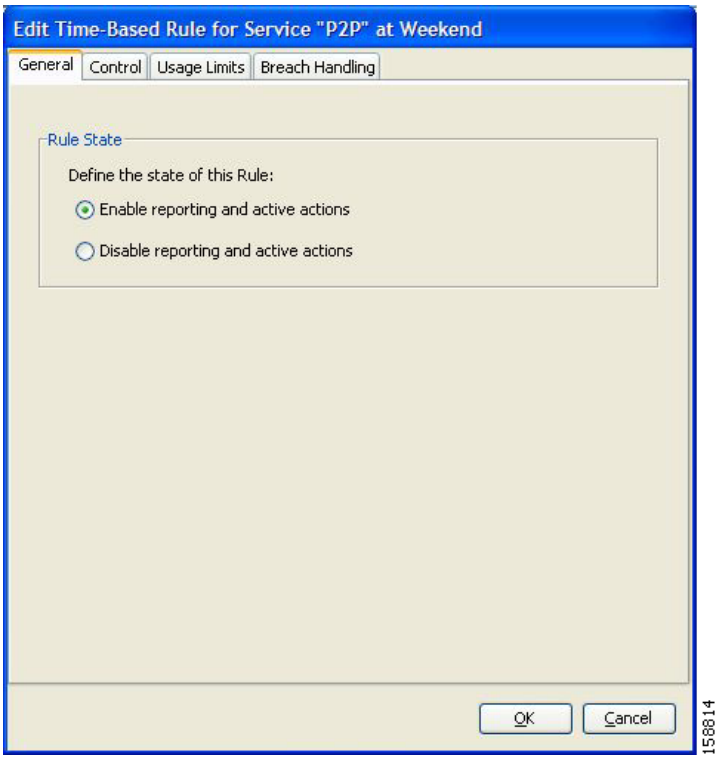
ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、タイムベース規則を選択します。

ステップ 3　  （[Edit Rule]）をクリックします。

[Edit Time-Based Rule for Service] ダイアログボックスが表示されます（図 9-56）。

図 9-56　[Edit Time-Based Rule for Service]



ステップ 4　[Rule State] 領域で、[Define the state of this Rule] のオプション ボタンをいずれか 1 つ選択します。

- [Enable reporting and active actions]
- [Disable reporting and active actions]

ステップ 5　トラフィック フローごとの動作を定義します。

a. [Control] タブをクリックします。

[Control] タブが開きます。

b. 「規則のためのフローごとのアクションの定義」（P.9-60）の手順に従います。

ステップ 6　使用制限を変更します。

a. [Usage Limits] タブをクリックします。

[Usage Limits] タブが開きます。

b. 「規則のためのクォータ バケットの選択」（P.9-84）の手順に従います。

ステップ 7　クォータで違反が発生したときの動作を定義します。

a. [Breach Handling] タブをクリックします。

[Breach Handling] タブが開きます。

b. 「規則のための違反処理パラメータの編集」（P.9-86）の手順に従います。

ステップ 8　[OK] をクリックします。

[Edit Time-Based Rule for Service] ダイアログボックスが閉じます。

このタイムベース規則の変更内容が保存されます。

タイムベース規則の削除

タイムベース規則は削除できます。

（注）　規則は、プロファイルを保持したまま*ディセーブル*にできます（「タイムベース規則の編集」（P.9-67）を参照）。このため、あとから規則を再度イネーブルにするとき、パラメータを設定しなおす必要がありません。

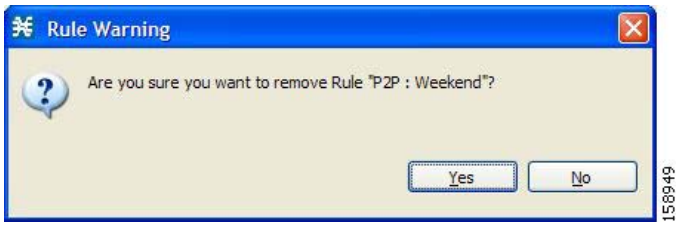
ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、タイムベース規則を選択します。

ステップ 3　規則ペインで、  （[Delete Rule]）をクリックします。

[Rule Warning] メッセージが表示されます（図 9-57）。

図 9-57　[Rule Warning]



ステップ 4　[Yes] をクリックします。

選択した規則が削除されます。

カレンダーの管理

カレンダーを使用して、1 週間を 4 つの時間枠に分割できます。

カレンダーの設定が完了すると、カレンダーを使用するパッケージにタイムベース規則を追加できるようになります。タイムベース規則とは、1 つの時間枠だけに適用される規則です。タイムベース規則を使用すると、特定の時間にだけ適用される規則パラメータを設定できます。たとえば、ピーク、オフピーク、夜間、週末用にそれぞれ異なる規則を定義する必要がある場合もあるでしょう。

各サービス コンフィギュレーションには、1 つのデフォルト カレンダーが組み込まれています。さらに、異なる時間枠を設定した 9 つのカレンダーを追加できます。パッケージごとに異なるカレンダーを使用できます。カスタマーが複数の時間帯に分散しているようなサービス プロバイダーの場合、1 時間ずつ時間をずらしてカレンダーを設定することにより、複数のカレンダーを使用することもできます。

- 「カレンダーの表示」（P.9-70）
- 「カレンダーの追加」（P.9-70）
- 「時間枠の名前変更」（P.9-71）
- 「カレンダーの削除」（P.9-72）
- 「時間枠の設定」（P.9-73）

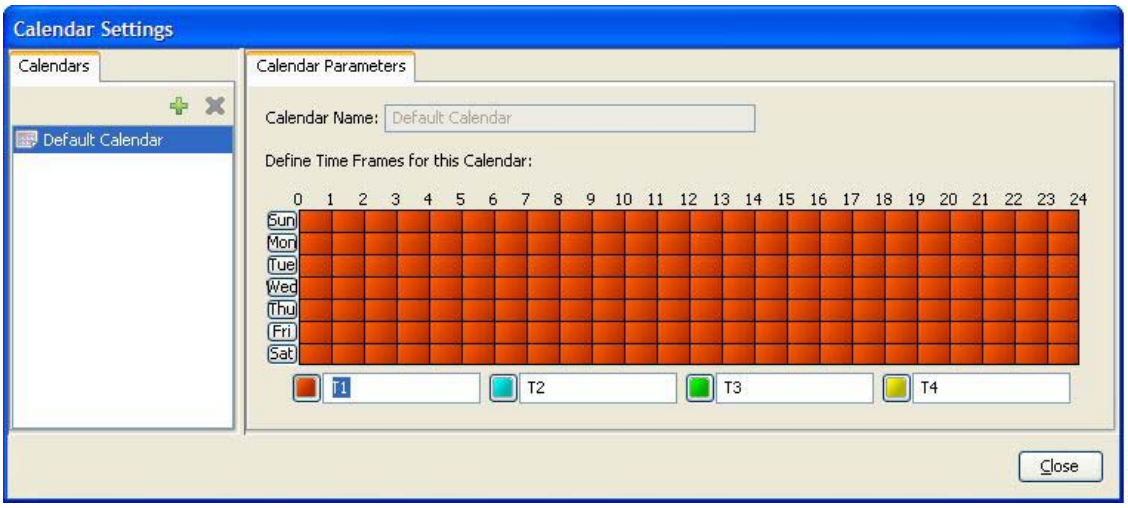
カレンダーの表示

既存のカレンダーのリストと、その時間枠を表示できます。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Weekly Calendars] の順に選択します。

[Calendar Settings] ダイアログボックスが表示されます（図 9-58）。

図 9-58　[Calendar Settings]



[Calendars] タブに、既存のカレンダーのリストが表示されます。リスト内のカレンダーをクリックすると、その時間枠設定が表示されます。

選択したカレンダーの時間枠が、[Calendar Parameters] タブに表示され、設定されます。

ステップ 2　[Close] をクリックします。

[Calendar Settings] ダイアログボックスが閉じます。

カレンダーの追加

各サービス コンフィギュレーションには、1 つのデフォルト カレンダーが組み込まれています。さらに、最大 9 つのカレンダーを追加できます。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Weekly Calendars] の順に選択します。

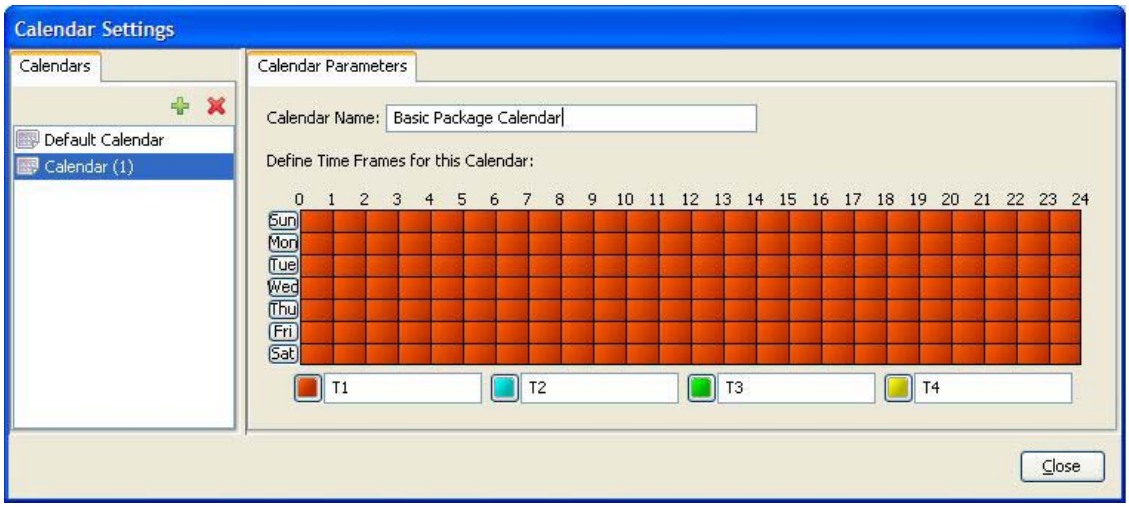
[Calendar Settings] ダイアログボックスが表示されます。

ステップ 2　[Calendar] タブで、  （[Add]）をクリックします。

Calendar (1) という名前の新しいカレンダーが追加されます。

ステップ 3　[Calendar Parameters] タブ（図 9-59）で [Calendar Name] フィールドをクリックし、このカレンダーの名前を入力します。

図 9-59　[Calendar Parameters] タブ



ステップ 4　[Close] をクリックします。

[Calendar Settings] ダイアログボックスが閉じ、新しいカレンダー名が保存されます。

時間枠の名前変更

デフォルトでは、時間枠名は T1、T2、T3、および T4 です。これらの名前は、いつでも変更できます。たとえば、時間枠に Peak、OffPeak、Night、Weekend という名前を付けることもできます。

（注）　カレンダーごとに異なる時間枠を設定できますが、時間枠の名前はすべてのカレンダーで共通です。1 つのカレンダーの設定時に名前を変更すると、他のカレンダーについても名前が変更されます。

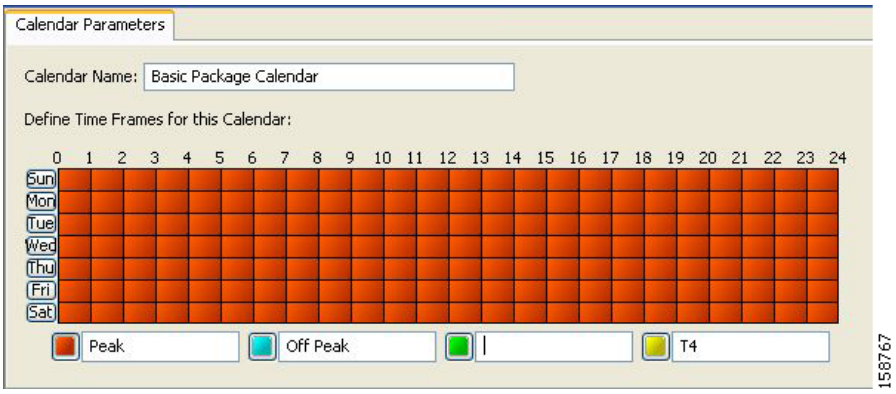
ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Weekly Calendars] の順に選択します。

[Calendar Settings] ダイアログボックスが表示されます。

[Calendar Parameters] タブ（図 9-60）のグリッドの下で、カラー表示された正方形の横にあるフィールドに、4 つの時間枠がそれぞれ表示されます。

ステップ 2　[Time Frame Name] フィールドをクリックして、時間枠の新しい名前を入力します。

図 9-60　[Calendar Parameters] タブ



ステップ 3　他の 3 つの時間枠についても、ステップ 2 を繰り返します。

ステップ 4　[Close] をクリックします。

[Calendar Settings] ダイアログボックスが閉じ、時間枠の変更後の名前が保存されます。

カレンダーの削除

ユーザが追加したカレンダーは削除できます。デフォルト カレンダーは削除できません。

（注）　パッケージで使用されているカレンダーは削除できません（カレンダーを選択したとき、[Delete] アイコンはグレー表示になっています）。このようなカレンダーを削除するには、まず、削除するカレンダーを使用しているそれぞれのパッケージに対し、別のカレンダーを選択する必要があります。パッケージに関連付けられているカレンダーの変更については、「高度なパッケージ オプションの設定」（P.9-52）を参照してください。

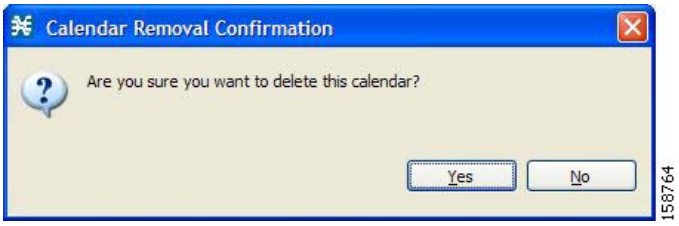
ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Weekly Calendars] の順に選択します。

[Calendar Settings] ダイアログボックスが表示されます。

ステップ 2　[Calendar] タブでカレンダーを選択し、  （[Delete]）をクリックします。

[Calendar Removal Confirmation] メッセージが表示されます（図 9-61）。

図 9-61　[Calendar Removal Confirmation]



ステップ 3　[Yes] をクリックします。

カレンダーが削除されます。

ステップ 4　[Close] をクリックします。

[Calendar Settings] ダイアログボックスが閉じます。

時間枠の設定

デフォルトでは、1 週間のすべての時間が 1 つの時間枠に属しています。Console を使用して、1 週間の 168（24 × 7）時間を 1 時間ごとに、4 つの時間枠のいずれかに割り当てることができます。この時間枠により、時間帯による差別化サービスを提供したり、サービスに制約を課したりできます。

たとえば、1 週間を次のように分割できます。

- ピーク
- オフピーク
- 夜間
- 週末

カレンダーごとに異なる時間枠を定義できます。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Weekly Calendars] の順に選択します。

[Calendar Settings] ダイアログボックスが表示されます。

ステップ 2　[Calendars] タブで、設定するカレンダーを選択します。

[Calendar Parameters] タブに、選択したカレンダーの [Define Time Frames for this Calendar] グリッドが表示されます。このグリッドは 1 週間を表し、24 時間×7 日の形式で配置されます。各セルが 1 時間に相当します。

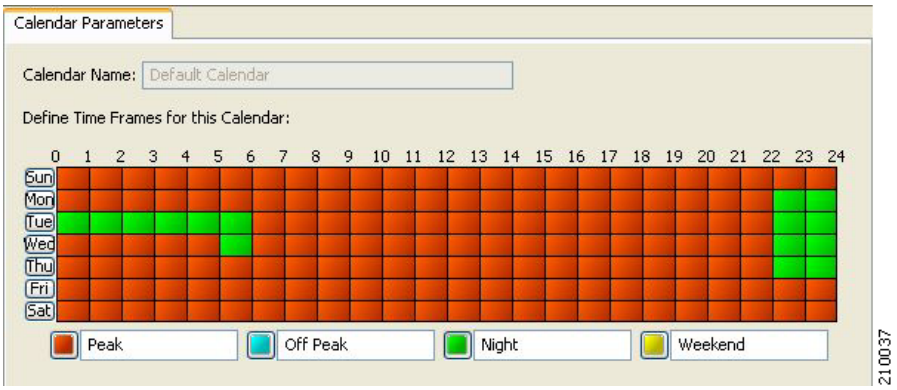
グリッドの下の、カラーのボタンの隣に、各時間枠の名前が表示されます。

ステップ 3　カラーのボタンのいずれかをクリックします。

ステップ 4　選択した時間枠に設定する時間のセルを、グリッド内で選択します。

セルのグループを選択するには、マウス ボタンを押したまま複数のセルをドラッグします（図 9-62）。

図 9-62　[Calendar Parameters] タブ

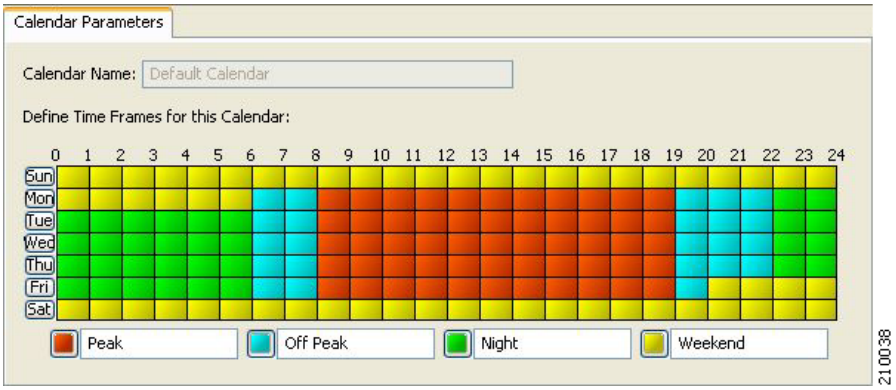


変更内容は、変更時にサービス コンフィギュレーションに書き込まれます。

ステップ 5　グリッド全体がマッピングされるまで、他の時間枠について、ステップ 3 および 4 を実行します。

1 週間が 4 つの時間枠にマッピングできました。図 9-63 に、時間の分割例を示します。

図 9-63　　時間の分割例



ステップ 6　[Close] をクリックします。

[Calendar Settings] ダイアログボックスが閉じます。

DSCP ToS マーカー値の管理

SCA BB では、フィルタ規則（「フィルタ規則の追加」（P.10-23）のステップ 11 を参照）またはサービス規則（「規則のためのフローごとのアクションの定義」（P.9-60）のステップ 10 および 11、「規則のための違反処理パラメータの編集」（P.9-86）のステップ 9 を参照）と一致するフロー パケットの DSCP ToS マーカーの値を変更できます。

SCA BB は、7 種類の ToS マーカー クラスをサポートしています。各クラスに特定の値を割り当て、それをフロー パケットに適用できます。

（注）　3.1.5 よりも前の SCA BB リリースで DSCP マーキングを使用していた場合、古いサービス コンフィギュレーションを変換するには、サービス コンフィギュレーションを再設定し、旧リリースと同じネットワーク動作を取得する必要があります。

DSCP ToS マーキング

DSCP ToS マーキングは、ネットワーク要素間のフローのタイプとプライオリティを通知する手段として IP ネットワークで使用されます。

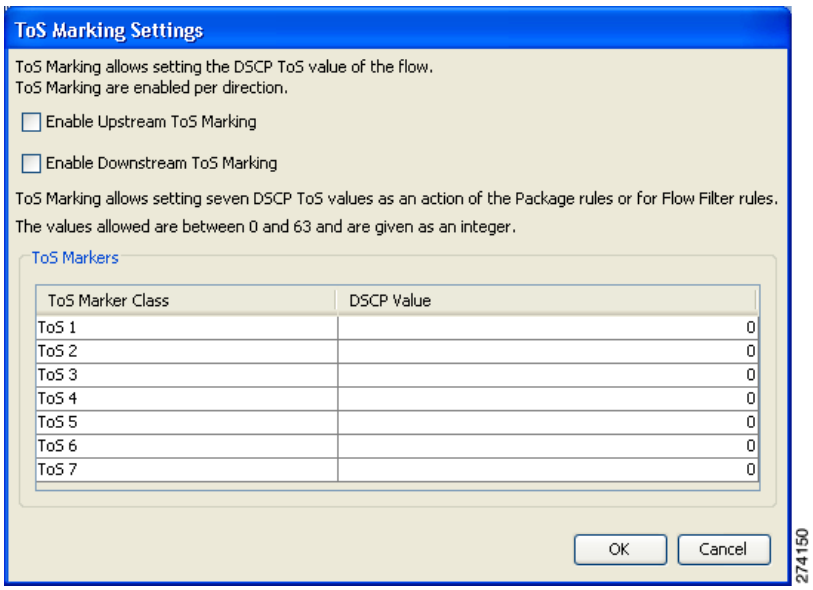
デフォルトのマーキング オプションでは、パケットはマークされません。分類では、確定のためにいくつかのパケットを必要とする場合があります。したがって、ToS マーキングがイネーブルの場合は、最初のいくつかのパケットがデフォルト オプションのままで処理されるためにマークされない可能性があることに注意が必要です。

注意　MPLS 環境では、SCE プラットフォームは DSCP ビットを MPLS ヘッダーの EXP ビットにマッピングしません。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [ToS Marking Settings] の順に選択します。

[ToS Marking Settings] ダイアログボックスが表示されます（図 9-64）。

図 9-64　[ToS Marking Settings]



ステップ 2　（オプション）アップストリーム フローの DSCP ToS マーキングをイネーブルにするには、[Enable Upstream ToS Marking] チェックボックスをオンにします。

アップストリーム ToS マーキングがディセーブルの場合、フィルタ規則およびサービス規則の設定は上書きされます。

ステップ 3　（オプション）ダウンストリーム フローの DSCP ToS マーキングをイネーブルにするには、[Enable Downstream ToS Marking] チェックボックスをオンにします。

ダウンストリーム ToS マーキングがディセーブルの場合、フィルタ規則およびサービス規則の設定は上書きされます。

ステップ 4　ToS マーカー クラスに一意の名前を付けます。

（注）　ToS マーカー クラスにはデフォルトの名前を使用できますが、わかりやすい名前を付けることを推奨します。

ステップ 5　ToS マーカー クラスに値を割り当てます。

値は 0 ～ 63 の範囲内で指定してください。

（注）　フィルタ規則とサービス規則を定義する際、ToS マーカー クラスの名前と値が「名前 [値]」の形式でドロップダウン リストに表示されます。たとえば、「ToS 1 [23]」や「My P2P ToS [1]」のようになります。

ステップ 6　[OK] をクリックします。

変更が保存されます。

[ToS Marking Settings] ダイアログボックスが閉じます。

クォータの管理

クォータ プロファイルの追加方法

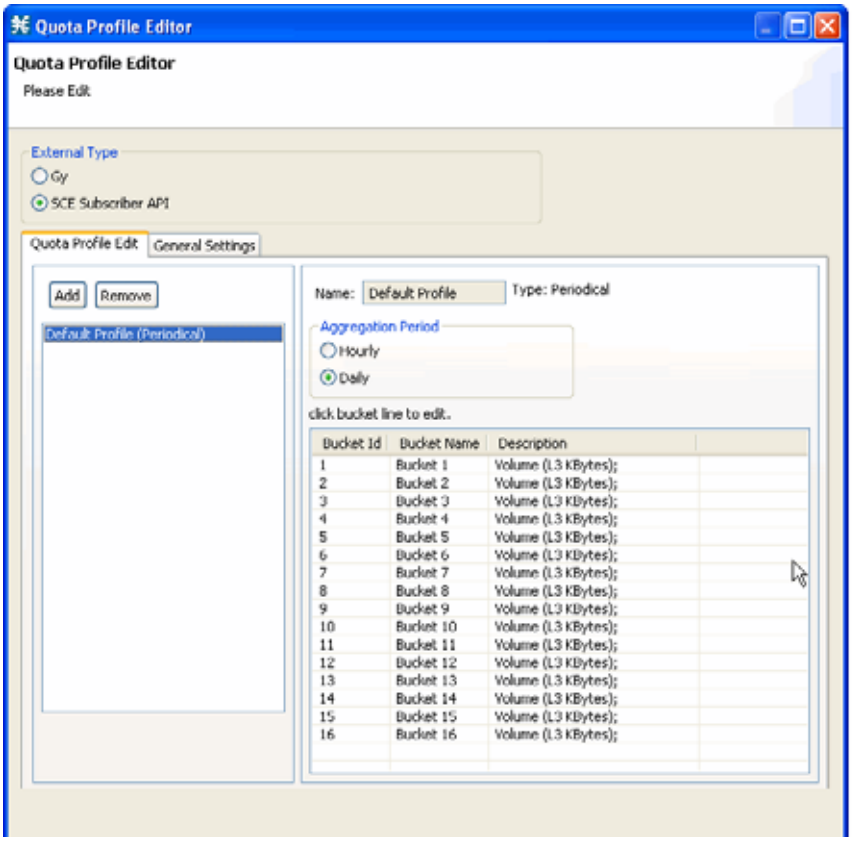
新しいプロファイルを追加および定義したり、既存のプロファイルを編集したりすることができます。また、最大 16 個の新しいバケットを追加できます。

パッケージに対応付けられるクォータ バケットの定義も行います。規則では、クォータ バケットに基づいて、特定のサービス グループの消費制限を設定できます（「規則のためのクォータ バケットの選択」（P.9-84）を参照）。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Policies] > [Quota Settings] の順に選択します。

[Quota Profile Editor] ダイアログボックスが表示されます（図 9-65）。

図 9-65　[Quota Profile Editor]



ステップ 2　[External Type] のオプション ボタンをいずれか 1 つ選択します。

- [Gy] : Gy クォータ モデルにより、Gy インターフェイス アダプタを外部クォータ管理に使用できるようになります。詳細については、『*Cisco Service Control Mobile Solution Guide*』を参照してください。
- [SCE Subscriber API] : Subscriber API により、サブスクライバ プロビジョニングのために外部アプリケーション（ポリシー サーバ）から SCE に直接接続できるようになります。詳細については、『*Cisco SCMS SCE Subscriber API Programmer Guide*』を参照してください。

（注）　定期的なクォータ管理を使用すると、すべてのサブスクライバのクォータが同時に補充されることのないようにクォータの補充を分散できます（「クォータ補充の分散」（P.9-83）を参照）。

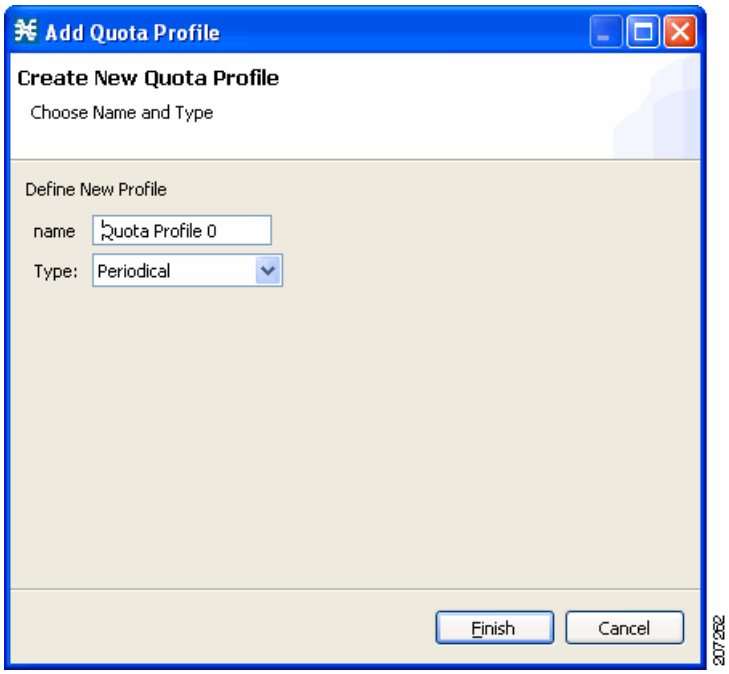
ステップ 3　[Periodical] クォータ プロファイルの場合は、[Aggregation Period] オプション ボタンのいずれかを選択して、パッケージのクォータを更新するタイミングを指定します。

- [Hourly] : 1 時間ごとにクォータを補充します。
- [Daily] : 深夜 0 時にクォータを補充します。

ステップ 4　[Quota Profile Edit] タブで、[Add] をクリックします。

[Add Quota Profile] ダイアログボックスが表示されます（図 9-66）。

図 9-66　[Add Quota Profile]



ステップ 5　新しいクォータ プロファイルの一意の名前を [Name] フィールドに入力します。

ステップ 6　ドロップダウン リストから、該当するタイプを選択します。

- [Periodical]
- [Subscriber SCE API]

ステップ 7　[Finish] をクリックします。

[Add Quota Profile] ウィンドウが閉じます。

新しいプロファイルがプロファイルのリストに追加され、左の [Quota Profile Edit] ペインに表示されます。

クォータ プロファイルの編集方法

プロファイルを編集してバケット プロファイルを更新できます。

（注）　デフォルト プロファイルは編集することも削除することもできません。

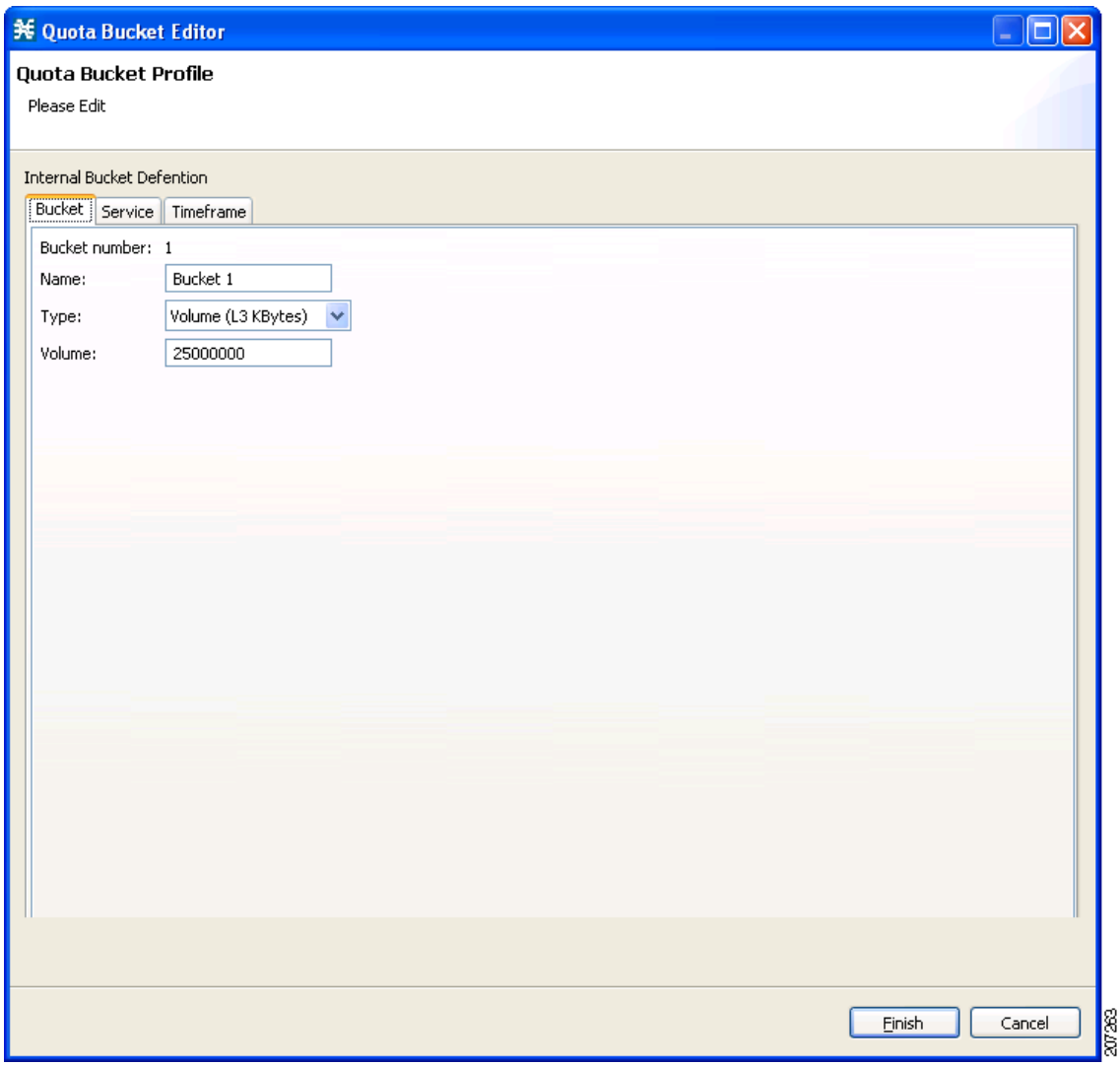
ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Policies] > [Quota Settings] の順に選択します。
[Quota Profile Editor] ダイアログボックスが表示されます（図 9-65）。

ステップ 2　プロファイル ツリーからクォータ プロファイルを選択します。
選択したプロファイルに対して定義されているすべてのバケットが右ペインに一覧表示されます。

ステップ 3　右ペインで、バケット行をダブルクリックします。

[Quota Bucket Editor] ウィンドウが表示されます（図 9-67）。

図 9-67　[Quota Bucket Editor]

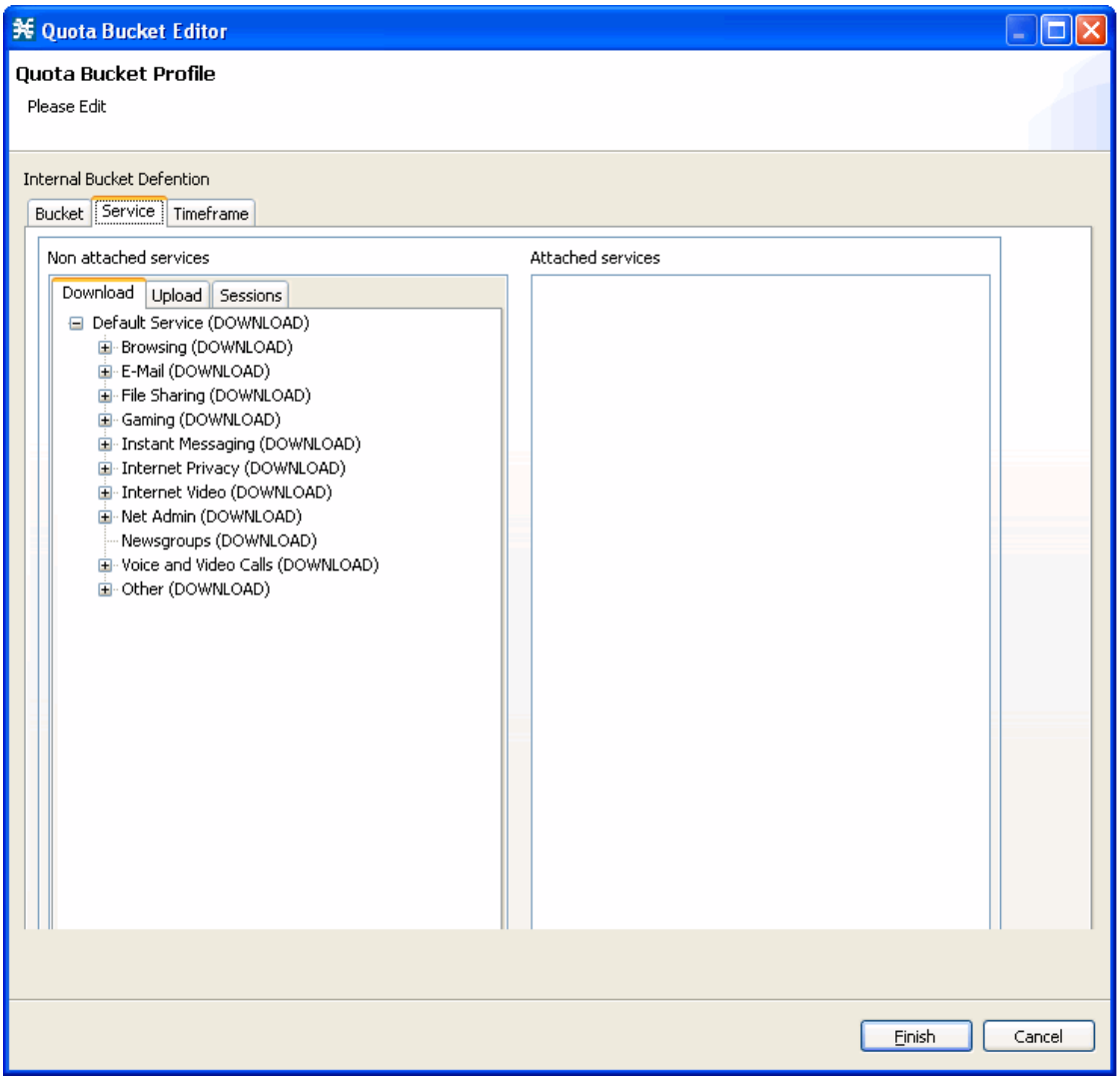


ステップ 4　[Name]、[Type]、および [Volume] を変更します。

（注）　バケットにはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

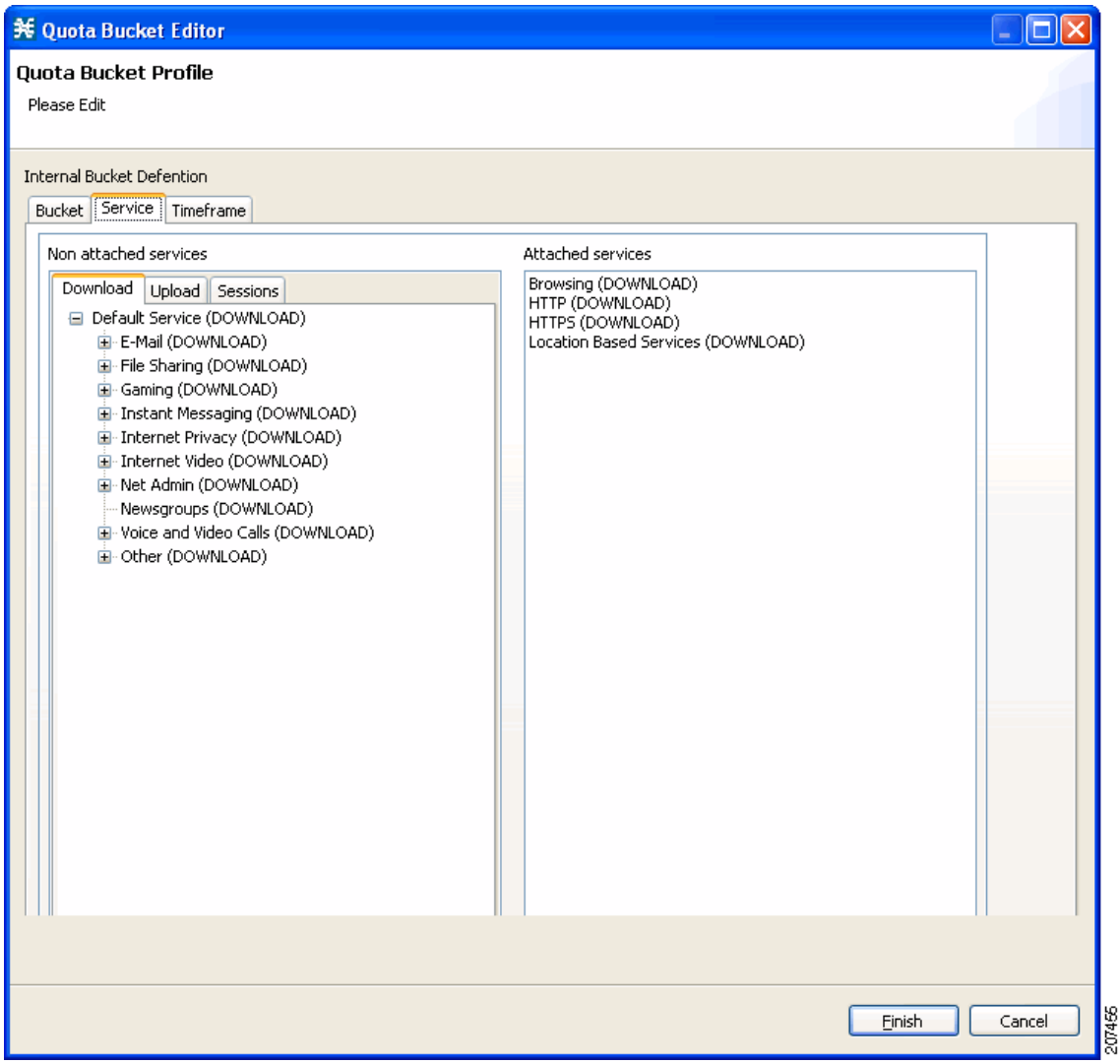
ステップ 5　サービスをクォータ プロファイルに関連付けるには、[Service] タブをクリックします（図 9-68）。

図 9-68　[Quota Bucket Editor]：[Service]



ステップ 6　[Non Attached Service] ペインからサービスを選択し、右側の [Attached Service] ペインに移動します。選択したサービスはそのサブ サービスとともに移動されます（図 9-69）。

図 9-69　[Quota Bucket Editor] : [Attached Service]

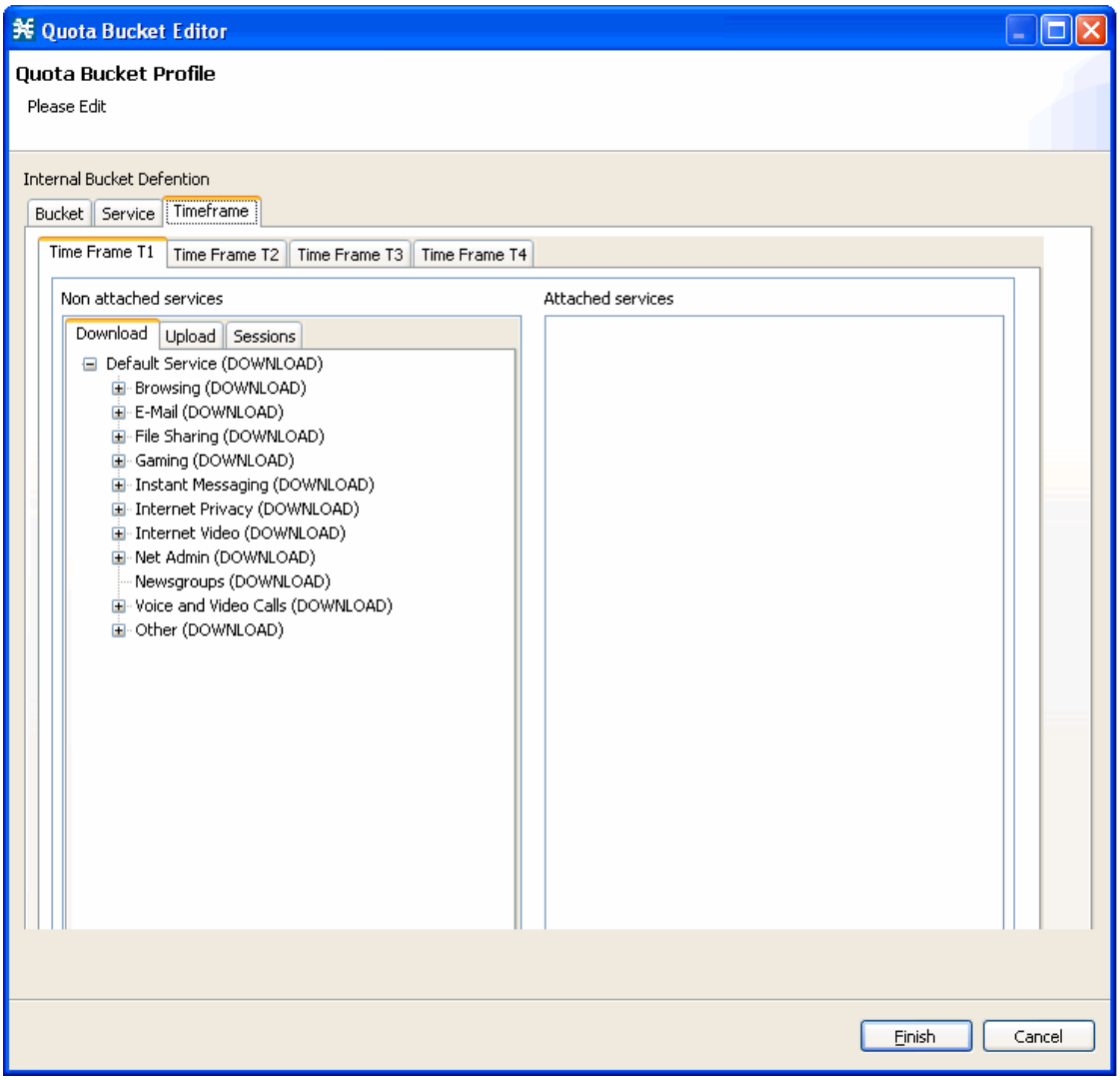


バケット タイプに基づいて、次のタブからサービスを選択できます。

- [Download]
- [Upload]
- [Session]

ステップ 7　各時間枠をクォータ プロファイルに関連付けるには、[Timeframe] タブをクリックします（図 9-70）。

図 9-70　[Quota Bucket Editor]：[Timeframe]



ステップ 8　[Non Attached Service] ペインからサービスを選択し、右側の [Attached Service] ペインに移動します。

選択したサービスはそのサブ サービスとともに移動されます。

バケット タイプに基づいて、次のタブからサービスを選択できます。

- [Download]
- [Upload]
- [Session]

ステップ 9　[Finish] をクリックします。

[Quota Bucket Editor] が閉じます。

ステップ 10　[Finish] をクリックします。[Quota Profile Editor] が閉じます。

次の作業

規則を関連付けるサービスを選択するには、「パッケージへの規則の追加」（P.9-58）を参照してください。

クォータ プロファイルの削除方法

（注）　デフォルト プロファイルは削除できません。

ステップ 1　左ペインの [Policies] タブで、[Configuration] > [Policies] > [Quota Settings] の順に選択します。

[Quota Profile Editor] ダイアログボックスが表示されます（図 9-65）。

ステップ 2　プロファイル ツリーからクォータ プロファイルを選択します。

ステップ 3　[Remove] をクリックします。

ステップ 4　[Finish] をクリックします。

[Quota Profile Editor] ダイアログボックスが閉じます。

パッケージのクォータ管理設定の編集

パッケージのクォータ管理を、外部のクォータ マネージャで行うか、SCA BB で行うかを定義できます。

クォータ補充の分散

定期的なクォータ管理を使用してサブスクライバ クォータが補充される場合、デフォルトではすべてのサブスクライバのクォータが同時に補充されます。クォータの補充を均等化する場合には、クォータの補充時間を分散させることができます。

この機能をアクティブにするには、[Systems Settings] ダイアログボックスの [Advanced Options] タブで、[Length of the time frame for quota replenish scatter (minutes)] プロパティにゼロ以外の値を入力します（「詳細サービス コンフィギュレーション オプションの管理」（P.10-46）を参照）。デフォルトではこのプロパティにゼロの値が入っており、すべてのクォータが同時に補充されます。

各サブスクライバのクォータの補充は、クォータ補充の分散時間枠内でランダムに行われますが、補充イベント自体はクォータ集約時間の前後に均等に分割されます。

分散時間枠とクォータ集約時間の長さを同一にすると最良の効果が得られ、補充イベントが完全に均等化されます （クォータ補充時間より大きな値は入力しないでください）。したがって、クォータ補充時間が 1 時間ごとの場合は、分散を 60 分に設定します。

クォータ補充の分散機能は、他のすべてのクォータ管理パラメータから独立しています。

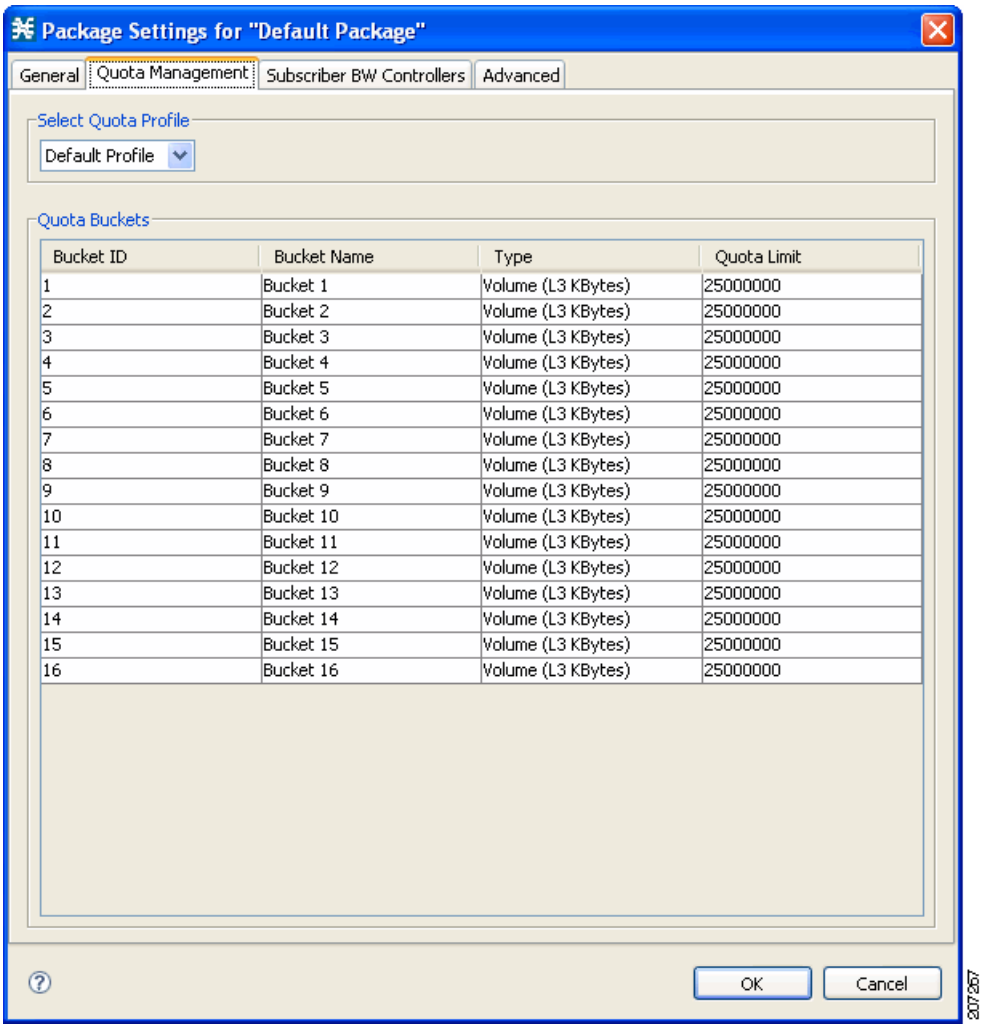
ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択し、（[Edit Package]）をクリックします。

[Package Settings] ダイアログボックスが表示されます。

ステップ 2　[Package Settings] ダイアログボックスで、[Quota Management] タブをクリックします。

[Quota Management] タブが開きます（図 9-71）。

図 9-71　[Quota Management] タブ



ステップ 3　ドロップダウン リストから、対象のクォータ プロファイルを選択します。

ステップ 4　[OK] をクリックします。

[Package Settings] ダイアログボックスが閉じます。

クォータ管理設定の変更内容が保存されます。

規則のためのクォータ バケットの選択

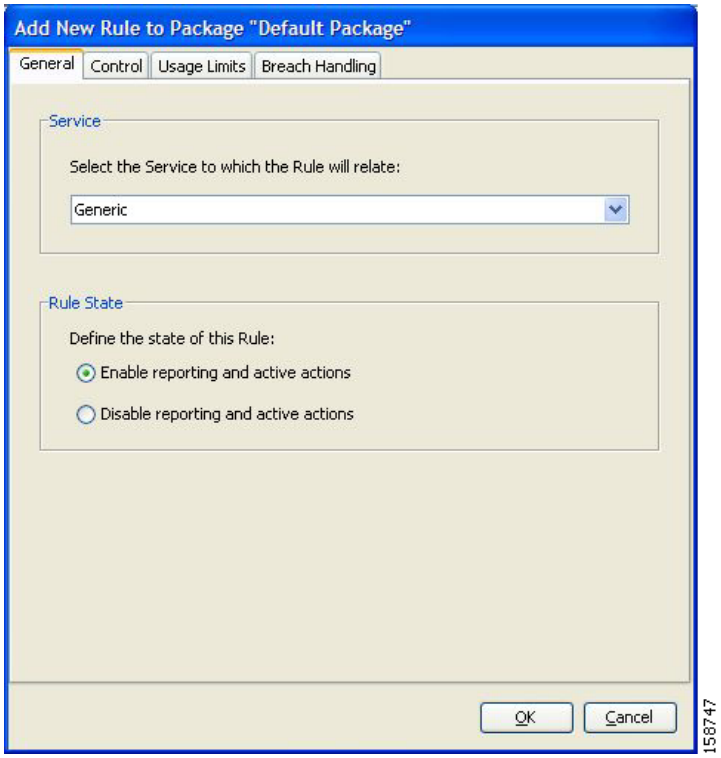
規則にマッピングされたフローで使用するクォータ バケットを選択します。クォータ バケットは、パッケージのセットアップ時に定義されます（「パッケージのクォータ管理設定の編集」（P.9-83）を参照）。規則に適したクォータ バケットがない場合は、パッケージに新しいクォータ バケットを追加するか、または既存バケットを編集する必要があります。

ステップ 1　[Network Traffic] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、（[Add Rule]）をクリックします。

[Add New Rule to Package] ダイアログボックスが表示されます（図 9-72）。

図 9-72　[Add New Rule to Package]



ステップ 3　[Service] 領域で、[Select the Service to Which the Rule Relates] ドロップダウン リストからサービスを選択します。

ステップ 4　[Usage Limits] タブをクリックします（図 9-73）。

図 9-73　[Usage Limits] タブ

ステップ 5　[Usage Limits] タブには、パッケージ プロファイルの詳細が表示されます。

規則に対して選択されたクォータ バケットが表示されます。クォータ プロファイルへのサービスの追加の詳細については、「クォータ プロファイルの編集方法」(P.9-78) のステップ 5 を参照してください。

ステップ 6　[OK] をクリックします。

[Edit Rule for Services] ダイアログボックスが閉じます。

規則のための違反処理パラメータの編集

集約ボリューム制限や合計セッション数制限を超過した場合の SCE プラットフォームの動作を定義できます。サブスクライバがクォータを超過した場合に、サブスクライバへの通知を行うこともできます。

違反処理パラメータ

[Edit Rule for Service Settings] ダイアログボックスの [Breach Handling] タブの設定パラメータを次に示します。

- クォータで違反が発生した場合に、この規則に属するフローのアクションを決定します。
  - [No changes to active control]：クォータで違反が発生したとき、この規則にマッピングされているフローは影響を受けません。SCA BB では、このオプションが選択されている場合でも、Quota Breach RDR を生成できます（「Quota RDR の管理方法」（P.8-6）を参照）。
  - [Block the flow]：クォータで違反が発生したとき、この規則にマッピングされているフローはブロックされます。

    [Redirect to]：指定のプロトコル依存 URL にフローがリダイレクトされます。開かれる Web ページに、リダイレクションの理由が表示されます。URL のリダイレクション セットは、[System Settings] ダイアログボックスで定義されます（「リダイレクション URL セットの追加」（P.10-41）を参照）。リダイレクションをサポートしているプロトコル タイプは、HTTP、HTTP Streaming、および RTSP の 3 つだけです。単方向分類が有効になっている場合、リダイレクションはサポートされません。
  - [Control the flow characteristics]：クォータで違反が発生したとき、この規則にマッピングされているフローの動作が変化します。

    [Select an upstream Bandwidth Controller]：この規則のトラフィック フローを特定のアップストリーム BW コントローラ（BWC）にマッピングします。これにより、選択した BWC の特性に基づいて、この規則にマッピングされたすべての同時フローの帯域幅測定が設定されます。

    [Select a downstream Bandwidth Controller]：上のオプションと基本的な機能は同じですが、ダウンストリーム フロー用です。

    [Limit the flow's upstream bandwidth]：フローごとのアップストリーム帯域幅制限を設定します（この規則のサービスにマッピングされたフロー用）。

    [Limit the flow's downstream bandwidth]：フローごとのダウンストリーム帯域幅制限を設定します。

    [Set the flow's upstream packets ToS]：アップストリーム フローの全パケットの DSCP ToS マーカーを設定します。

    [Set the flow's downstream packets ToS]：ダウンストリーム フローの全パケットの DSCP ToS マーカーを設定します。

    [Limit concurrent flows of this Service]：サブスクライバに許容される（この規則にマッピングされた）同時フローの最大数を設定します。
- [Activate a Subscriber Redirect]：サブスクライバがクォータ制限を超過した場合に、サブスクライバ リダイレクトをアクティブにします。
- [Activate a Subscriber Notification]：サブスクライバがクォータ制限を超過した場合に、サブスクライバ通知をアクティブにします。たとえば、この通知によりサブスクライバにクォータ違反状態を伝達し、追加クォータの取得方法を示すことができます。

（注）　単方向分類が有効になっている場合、サブスクライバ通知はサポートされません。

  サブスクライバ通知の定義方法については、「サブスクライバ通知の管理」（P.10-30）を参照してください。
- [Activate Traffic Mirroring]：サブスクライバがクォータ制限を超過した場合に、トラフィック ミラーリングをアクティブにします。

ステップ 1　[Policies] タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右の規則ペインで、規則を選択します。

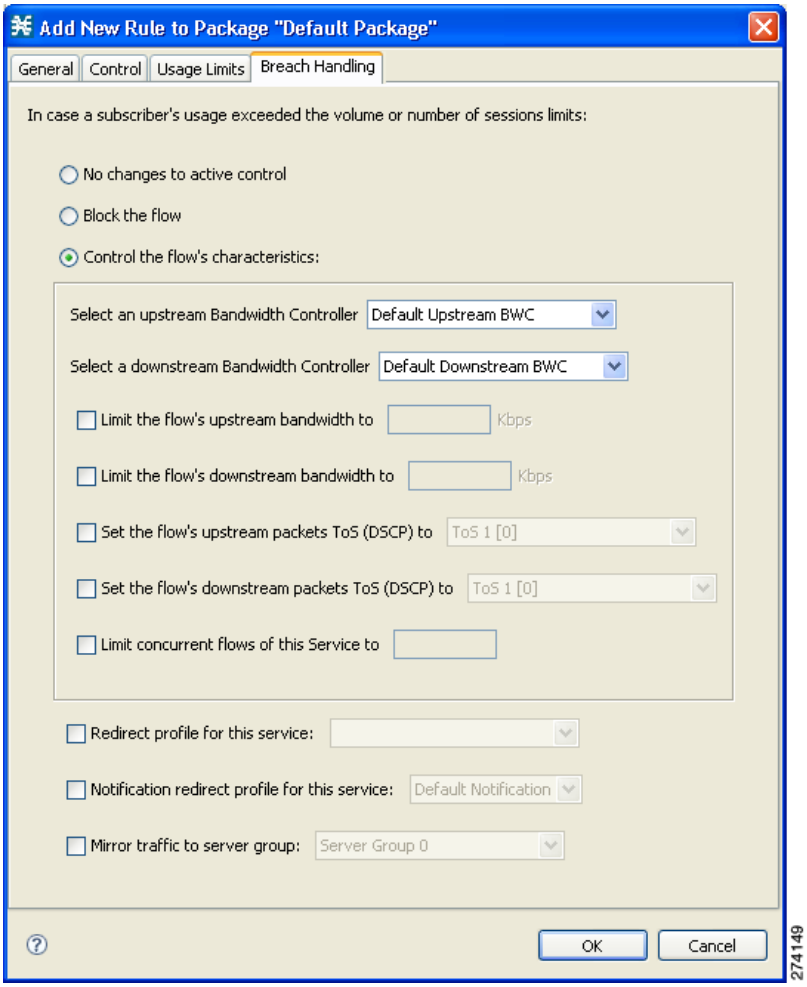
ステップ 3　（[Edit Rule]）をクリックします。

[Edit Rule for Service] ダイアログボックスが表示されます。

ステップ 4　[Breach Handling] タブをクリックします。

[Breach Handling] タブが開きます（図 9-74）。

図 9-74　[Breach Handling] タブ



ステップ 5　クォータの違反が発生した場合のフローの動作を設定します。

- クォータの違反が発生した場合にフローをブロックするには、ステップ 6 に進みます。
- クォータの違反が発生した場合にフローの特性を変更するには、ステップ 10 に進みます。
- クォータの違反が発生した場合もフローの動作を変更しないようにするには、[No changes to active control] オプション ボタンを選択し、ステップ 11 に進みます。

ステップ 6　フローをブロックするには、[Block the flow] オプション ボタンを選択します。

ステップ 7　ステップ 10 に進みます。

ステップ 8　フローの特性を変更します。

[Control the flow's characteristics] オプション ボタンを選択します。

[Flow Characteristic] 領域のオプションがイネーブルになります。

- アップストリームの [Bandwidth Controller] ドロップダウン リストで、アップストリーム BWC を選択します。

  このドロップダウン リストの BWC は、パッケージの作成時または編集時に定義されます。

マウスをドロップダウン リスト上に合わせると、ツールチップに、選択した BWC のプロパティ（Peak Information Rate（PIR）、Committed Information Rate（CIR）、Global Controller、Assurance Level）が表示されます。

- ダウンストリームの [Bandwidth Controller] ドロップダウン リストで、ダウンストリーム BWC を選択します。
- （オプション）[Limit the flow's upstream bandwidth] チェックボックスをオンにして、[Kbps] フィールドに値を入力します。
- （オプション）[Limit the flow's downstream bandwidth] チェックボックスをオンにして、[Kbps] フィールドに値を入力します。
- （オプション）[Set the flow's upstream packets ToS (DSCP) to] チェックボックスをオンにして、ドロップダウン リストから値を選択します。
- （オプション）[Set the flow's downstream packets ToS (DSCP) to] チェックボックスをオンにして、ドロップダウン リストから値を選択します。
- （オプション）[Limit concurrent flows of this Service] チェックボックスをオンにして、関連フィールドに値を入力します。

ステップ 9　（オプション）サブスクライバのリダイレクトをイネーブルにするには、チェックボックスをオンにして、ドロップダウン リストからリダイレクト プロファイルを選択します。

ステップ 10　（オプション）サブスクライバ通知をイネーブルにするには、[Notification redirect profile for this service] チェックボックスをオンにし、ドロップダウン リストから通知リダイレクト プロファイルを選択します。

（注）　サブスクライバ通知は、3 つの違反処理オプションに追加してアクティブにできます。

（注）　単方向分類が有効になっている場合、サブスクライバ通知はサポートされません。単方向分類が有効になっているときに [Activate a Subscriber Notification] チェックボックスをオンにしようとすると、[Rule Error] メッセージが表示されます。

ステップ 11　[OK] をクリックして続行します。

ステップ 12　（オプション）サーバ グループへのミラー トラフィックをイネーブルにするには、[Mirror traffic to server group] チェックボックスをオンにし、ミラー トラフィックの送信先となるサーバ グループを選択します。

（注）　[Mirror traffic to server group] チェックボックスがイネーブルになるのは、[VAS Settings] ダイアログボックスで [Traffic Mirroring] がイネーブルの場合だけです。

ステップ 13　[OK] をクリックします。

[Edit Rule for Service] ダイアログボックスが閉じます。

この規則の変更内容が保存されます。

例：階層型サブスクライバ サービスの作成

SCA BB Console を使用して、階層型サブスクライバ サービス実装できます。このようなサービスの定義は無限にあるため、このセクションでは、価値提案の説明で概説されている 2 つの階層の定義方法について説明します。2 つの階層は次のように定義されます。

- シルバー
  - 1 週間の帯域幅は 4.2 GB （1 日 600 MB の制限に相当）に制限
  - E メールおよびブラウジング サービスは 256 Kbps に制限
  - 音声およびビデオ ストリーミング サービスは 64 Kbps に制限
  - P2P サービス は 28 Kbps に制限
- ゴールド
  - 1 週間の帯域幅は 5.6 GB （1 日 800 MB の制限に相当）に制限
  - E メールおよびブラウジング サービスの帯域幅は無制限
  - 音声およびビデオ ストリーミング サービスは 128 Kbps に制限
  - P2P サービス は 28 Kbps に制限

次の手順は、「シルバー」と「ゴールド」のいずれのパッケージにも適用されます。

ステップ 1　「パッケージの追加」（P.9-50）の説明に従って新規パッケージを作成します。

ステップ 2　定期的（内部）クォータ管理をイネーブルにします。

a.　集約時間を [Daily] に設定します。

b.　クォータ制限を目的の値に設定し、クォータ バケットにわかりやすい名前を付けます。

詳細については、「パッケージのクォータ管理設定の編集」（P.9-83）を参照してください。

ステップ 3　必須サービス用の帯域幅コントローラを追加し、PIR を目的のレートに設定します。

（注）　帯域幅が制限されている各サービスには、サブ帯域幅コントローラが必要です。これは、エキストラ帯域幅コントローラではなく、プライマリ帯域幅コントローラの子です。

詳細については、「パッケージ サブスクライバ BWC の編集」（P.9-29）を参照してください。

ステップ 4　帯域幅が制限されている各サービスについて、パッケージに規則を追加します。

詳細については、「パッケージへの規則の追加」（P.9-58）を参照してください。

ステップ 5　関連サービスに対し、帯域幅コントローラでフローの特性を制御する規則を設定します。

詳細については、「規則のためのフローごとのアクションの定義」（P.9-60）を参照してください。

ステップ 6　ステップ 2 で定義した、クォータ バケットを使用するパッケージに使用制限を設定します。

詳細については、「規則のためのクォータ バケットの選択」（P.9-84）を参照してください。

サブスクライバが未知のトラフィック

フィルタ規則と一致しないトラフィック フロー（「トラフィック フローのフィルタリング」（P.10-20）を参照）は、SCE プラットフォームが処理します。SCE プラットフォームでは、このトラフィック フローと係わりのあるサブスクライバの識別を試みます。SCE プラットフォームの内部データベースにトラフィック フローの IP アドレスまたは VLAN タグで特定できるサブスクライバがないかどうかを確認します。該当するサブスクライバが存在しない場合は、トラフィック フローを Unknown Subscriber Traffic カテゴリにマッピングします。

Unknown Subscriber Traffic カテゴリは、[Network Traffic] タブのツリーに含まれていますが、パッケージ階層の一部ではありません。Unknown Subscriber Traffic カテゴリは削除できません。

（注）　サブスクライバが未知のトラフィック同士は、互いに区別できません。したがって、サブスクライバ BWC を使用してサブスクライバごとの使用制限や、サブスクライバ レベルの調整は設定できません。サブスクライバ BWC は、選択したサービスをグローバル コントローラにリンクする目的でのみ使用できます。

Unknown Subscriber Traffic カテゴリは、次のパラメータを持つパッケージと同様に機能します。

- [Package Name]：Unknown Subscriber Traffic
- [Package Index]：4999
- 次の 1 つのパッケージ使用カウンタ
  - [Counter Name]：Unknown Subscriber Traffic Counter
  - [Counter Index]：1023

次のことが実行できます。

- Unknown Subscriber Traffic パッケージ設定の編集
  - エキストラ BWC の追加（「パッケージ サブスクライバ BWC の編集」（P.9-29）を参照）
  - カレンダーの選択（「高度なパッケージ オプションの設定」（P.9-52）を参照）
- Unknown Subscriber Traffic カテゴリのデフォルト サービス規則の編集
  - 規則状態の変更（「規則の編集」（P.9-62）を参照）
  - 規則のためのフローごとのアクションの変更（「規則のためのフローごとのアクションの定義」（P.9-60）を参照）
- Unknown Subscriber Traffic パッケージへの規則の追加
  - 規則の追加（「パッケージへの規則の追加」（P.9-58）を参照）、編集（「規則の編集」（P.9-62）を参照）、および削除（「規則の削除」（P.9-64）を参照）
  - タイムベース規則の追加（「規則へのタイムベース規則の追加」（P.9-65）を参照）、編集（「タイムベース規則の編集」（P.9-67）を参照）、および削除（「タイムベース規則の削除」（P.9-69）を参照）

CHAPTER 10

Service Configuration Editor の使用方法：その他のオプション

はじめに

この章では、Service Configuration Editor で使用できるその他の詳細機能の使用法について説明します。

サービス セキュリティ ダッシュボード

サービス セキュリティ ダッシュボードでは、すべての Cisco Service Control Application for Broadband（SCA BB）セキュリティ機能を表示して制御できます。

サービス セキュリティ ダッシュボードは、ワーム、Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃、スパム ゾンビなどのセキュリティの脅威からネットワークを保護する一連の機能へのゲートウェイです。検出メカニズム（攻撃のしきい値など）、および攻撃が検出されたときに実行する処理も設定できます。

サービス セキュリティ ダッシュボードでは、Reporter ツールの悪質トラフィック レポートにアクセスすることもできます。

注意　悪質トラフィックの異常ベース検出が有効の場合、プラットフォームにサービス コンフィギュレーションを適用すると、Service Control Engine（SCE）プラットフォームで設定されているものの、インターフェイス、アクセス マップ、または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）コミュニティ ストリングなどいずれにも適用されていない任意の Access Control List（ACL; アクセス コントロール リスト）が削除されることがあります。

回避策：

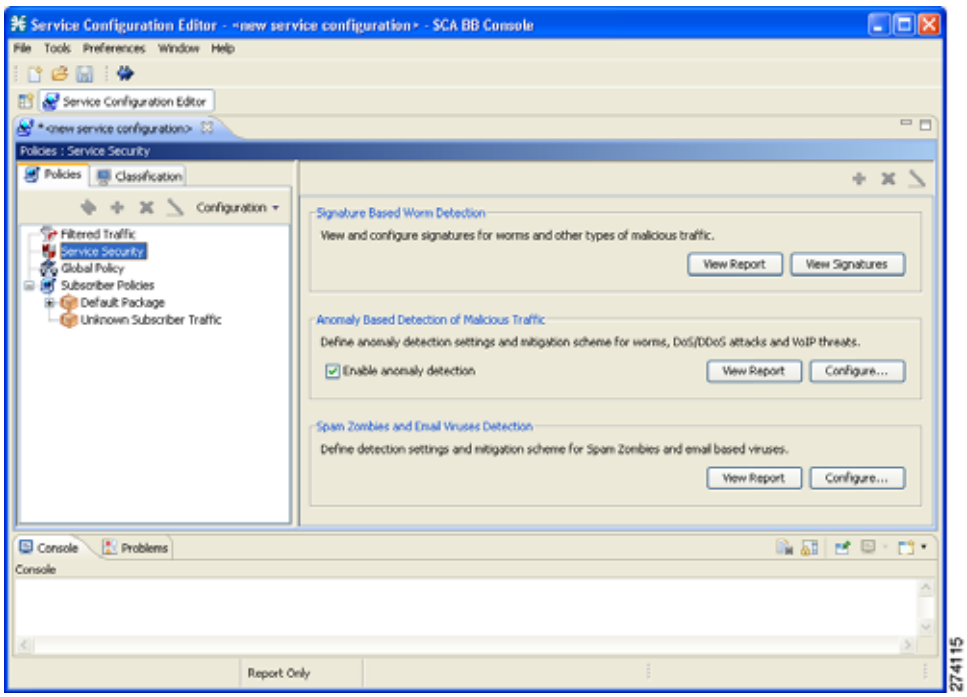
悪質トラフィックの異常ベース検出を無効にします （[Enable anomaly detection] チェックボックスをオフにします）。

サービス セキュリティ ダッシュボードの表示

ステップ 1　[Network Traffic] タブで [Service Security] を選択します。

ステップ 2　サービス セキュリティ ダッシュボードが右側ペインに表示されます（図 10-1）。

図 10-1　　サービス セキュリティ ダッシュボード



ワーム検出の管理

SCA BB では、ワームの検出に次の 3 つのメカニズムが使用されます。

- シグニチャ ベース検出：SCE プラットフォームのステートフル レイヤ 7 機能では、その他のメカニズムで容易に検出できない悪質アクティビティを検出できます。新しいワームのシグニチャを追加できます。
- 異常ベース検出：全体的なトラフィック分析により、ワーム アクティビティを示す可能性のある異常を検出できます。「異常検出の管理」（P.10-4）を参照してください。
- 大量メール送信ベース検出：E メール トラフィック分析により、E メールベース ワームを示すことがある異常を検出できます。「スパム検出の設定」（P.10-16）を参照してください。

サポートされるワーム シグニチャの表示

ステップ 1　サービス セキュリティ ダッシュボードで [View Signatures] をクリックします。

[Signature Type] ドロップダウン リストで [Worm Signatures] が選択された状態で [Signatures Settings] ダイアログボックスが表示されます。

サポートされているすべてのワーム シグニチャがリストされます。

ステップ 2　[Close] をクリックします。

[Signature Settings] ダイアログボックスが閉じます。

サービス コンフィギュレーションへの新規ワーム シグニチャの追加

シスコが提供する最新の Digital Signature Standard（DSS; デジタル シグニチャ規格）ファイルまたは SPQI ファイルをインポートするか、サービス コンフィギュレーションに追加する任意のワーム シグニチャが含まれる DSS ファイルを作成します。

関連情報

詳細については、「プロトコル シグニチャの管理」（P.7-36）を参照してください。

異常検出の管理

最も総合的な脅威検出方式は異常検出です。

異常検出

異常検出の基本原理は、システムが確認するすべての IP アドレスとの正常接続レート（Transmission Control Protocol（TCP; 伝送制御プロトコル）の場合は正しい確立、その他のプロトコルの場合は双方向）と異常接続レート（TCP の場合は不正な確立、その他のプロトコルの場合は単一方向）を監視すること、および次の基準のうちいずれかに基づく異常検出条件をトリガーすることです。

- 合計接続レートが定義済みしきい値を超える。
- 不審接続レートが定義済みしきい値を超え、かつ不審接続と非不審接続の比率が定義済みしきい値を超える。

比率メトリックは特に強力な悪質アクティビティ インジケータであり、信頼できる悪質アクティビティ識別子としてレート修飾子とともに動作します。

異常検出は、検出された異常条件の方向に基づいて、次の 3 つのカテゴリに分類されます。3 つのカテゴリで使用されるコンセプトは同じですが、検出される悪質アクティビティの性質はカテゴリごとに異なります。

- スキャンおよびスウィープ ディテクタ：IP アドレスからの接続レートにおける異常に基づく悪質アクティビティを検出します。
- Denial of Service（DoS; サービス拒絶）ディテクタ：一方が他方を攻撃している IP アドレスのペア間における接続レートの異常を検出します。単一の攻撃またはスケールが大きい DDoS 攻撃の一部である可能性があります。

- DDoS ディテクタ：IP アドレスに着信する接続レートで異常（その IP アドレスが攻撃されている）を検出します。攻撃は、単一 IP アドレス（DoS）または複数の IP アドレスによって行われる可能性があります。

すべての種類の異常検出条件において、次のそれぞれにしきい値および実行されるトリガー処理を定義できるので、柔軟性が最大になります。

- フロー方向
- フロー プロトコル
- （オプション）TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のポートの一意性

（注）　ここで説明する GUI 設定は、前リリースで使用できた、SCE プラットフォームの攻撃フィルタリング モジュールを設定する Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドの代わりとなります。

異常検出パラメータ

スキャンおよびスウィープ、DoS、DDoS という異常ディテクタ カテゴリごとに、1 つのデフォルト ディテクタがあります。カテゴリごとに別のディテクタを追加できます。各カテゴリのディテクタは順番に確認されます。ディテクタのしきい値設定に従った最初の一致によって検出がトリガーされます。ディテクタが確認される順序を設定できますが、デフォルト ディテクタは最後に確認されます。

異常ディテクタには、悪質トラフィックに関連する、最大 12 の異常タイプを含めることができます。

- ネットワーク主導：ネットワーク側から開始される悪質トラフィック
  - TCP：すべてのポートの集約 TCP トラフィック
  - TCP 特定ポート：すべての単一ポートの TCP トラフィック
  - UDP：すべてのポートの集約 UDP トラフィック
  - UDP 特定ポート：すべての単一ポートの UDP トラフィック
  - ICMP：すべてのポートの集約 ICMP トラフィック
  - その他：すべてのポートでその他のプロトコル タイプを使用した集約トラフィック
- サブスクライバ主導：サブスクライバ側から開始される悪質トラフィック
  - TCP
  - TCP 特定ポート
  - UDP
  - UDP 特定ポート
  - ICMP
  - その他

（注）　DoS 攻撃ディテクタでは、ICMP およびその他の異常タイプを使用できません。

ディテクタの各異常タイプには次の属性が関連します。

- 検出しきい値：2 つのしきい値があり、どちらかを超えるということは、攻撃が進行中であると定義されることになります。

- セッション レートしきい値：異常検出条件をトリガーする、単一 IP アドレスの指定ポートにおける 1 秒間のセッション数。
- 不審セッションしきい値：不審セッションとは、適切に確立されていないセッション（TCP の場合）、または単一方向セッション（その他のプロトコルの場合）のことです。不審セッション レート*および*不審セッション比率の両方を超えると、異常検出条件がトリガーされます。セッション レートが比較的高くて応答レートが低い場合は、一般的に悪質アクティビティを示します。

  不審セッション レート：単一 IP アドレスの指定ポートにおける、1 秒間の不審セッション数。

  不審セッション比率：不審セッション レートと合計セッション レートの比率（パーセンテージ）。比率が高い場合は多くのセッションが応答を受けないことを意味し、悪質アクティビティを示します。

- 処理：異常検出条件がトリガーされたとき、次の処理のうち 0 個以上を実行できます（デフォルトでは処理が有効になっていません）。

（注） デバイス上のログ ファイルに異常をログすること、および Raw Data Report（RDR; 未加工データ レコード）の生成を異常タイプごとに設定することはできません。

- ユーザ警告：SNMP トラップを生成し（シスコ独自の MIB については、『*Cisco Service Control Application for Broadband Reference Guide*』の「SCA BB Proprietary MIB Reference」の章を参照してください）、異常の始まりと終わりを示します。
- サブスクライバ通知：ブラウジング セッションをキャプティブ ポータルにリダイレクトし、悪質アクティビティについて関連サブスクライバに通知します。ネットワーク攻撃に関するサブスクライバ通知を設定するには、「サブスクライバ通知の管理」（P.10-30）を参照してください。
- 攻撃ブロック：関連セッションをブロックします。ブロックは、異常検出条件をトリガーした悪質トラフィックの仕様に基づいて実行されます。サブスクライバ通知を異常タイプで有効にしている場合、ブロックはブラウジングの関連ポート（デフォルトの場合は TCP ポート 80。「詳細サービス コンフィギュレーション オプションの管理」（P.10-46）を参照）に適用されません。

ユーザ定義ディテクタにも、次の属性のうち 1 つ以上を含めることができます。

- IP アドレス リスト：リストされている IP アドレス範囲に検出を制限します。IP スウィープおよびポート スキャンの検出時に、送信元 IP に適用されます。DoS 攻撃および DDoS 攻撃の検出時には送信先 IP に適用されます。
- TCP ポート リスト：リストされている送信先 TCP ポートに検出を制限します。このリストは、TCP 指定ポート異常タイプだけに適用されます。
- UDP ポート リスト：リストされている送信先 UDP ポートに検出を制限します。このリストは、UDP 指定ポート異常タイプだけに適用されます。

異常検出設定の表示

すべての異常検出のリストを表示できます。異常ディテクタはツリー構造で表示され、ディテクタ カテゴリ（スキャンおよびスウィープ、DoS、DDoS）に従ってグループ化されます。

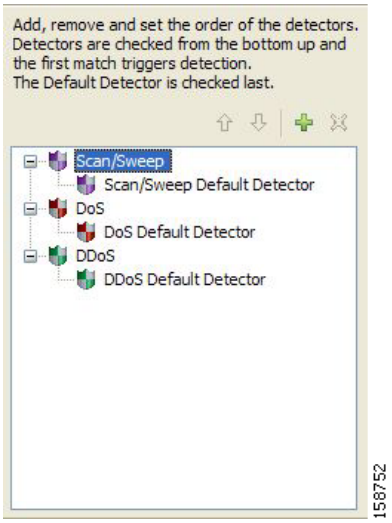
異常ディテクタごとに関連パラメータを表示し、ディテクタに組み込まれるすべての異常タイプのリスト、およびそのパラメータを表示できます。

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ディテクタ ツリーがダイアログボックスの左側領域に表示され、右側領域は空になります（図 10-2）。

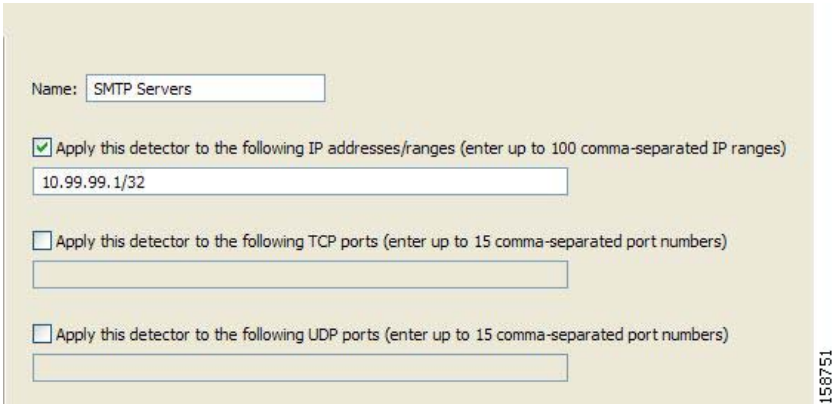
図 10-2　　ディテクタ ツリー



ステップ 2　ディテクタ ツリーでディテクタを選択します。

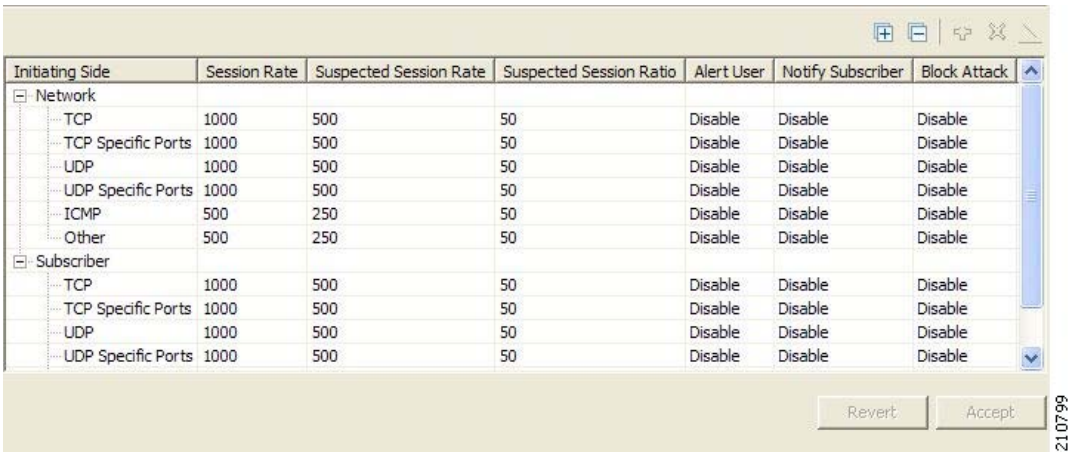
ディテクタのパラメータがダイアログボックスの右上の領域に表示されます（図 10-3）。

図 10-3　　ディテクタのパラメータ



ディテクタの定義済み異常タイプは、各パラメータの値とともにダイアログボックスの右下の領域にリスト表示されます。次の図は、スキャンおよびスウィープのデフォルト ディテクタのデフォルト パラメータ値を示しています（図 10-4）。

図 10-4　ディテクタの定義済み異常タイプ



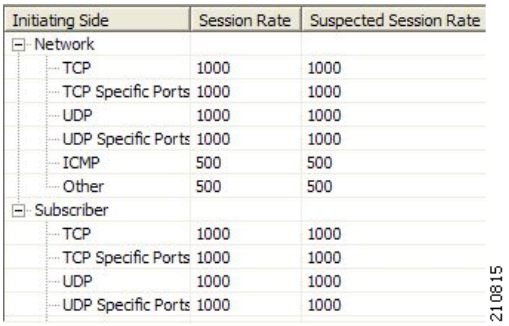
Initiating Side	Session Rate	Suspected Session Rate	Suspected Session Ratio	Alert User	Notify Subscriber	Block Attack
Network						
TCP	1000	500	50	Disable	Disable	Disable
TCP Specific Ports	1000	500	50	Disable	Disable	Disable
UDP	1000	500	50	Disable	Disable	Disable
UDP Specific Ports	1000	500	50	Disable	Disable	Disable
ICMP	500	250	50	Disable	Disable	Disable
Other	500	250	50	Disable	Disable	Disable
Subscriber						
TCP	1000	500	50	Disable	Disable	Disable
TCP Specific Ports	1000	500	50	Disable	Disable	Disable
UDP	1000	500	50	Disable	Disable	Disable
UDP Specific Ports	1000	500	50	Disable	Disable	Disable

Revert　Accept

210799

単方向分類が有効になっている場合、不審セッション レートとセッション レートは同じに設定されます。この設定では、不審セッションによりトリガーされる異常検出が実質的に無効になります（図 10-5）。

図 10-5　セッション レートと不審セッション レートの比較



Initiating Side	Session Rate	Suspected Session Rate
Network		
TCP	1000	1000
TCP Specific Ports	1000	1000
UDP	1000	1000
UDP Specific Ports	1000	1000
ICMP	500	500
Other	500	500
Subscriber		
TCP	1000	1000
TCP Specific Ports	1000	1000
UDP	1000	1000
UDP Specific Ports	1000	1000

210815

ステップ 3　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

異常ディテクタの追加

新しい異常ディテクタを追加できます。サービス コンフィギュレーションには 100 までの異常ディテクタを含めることができます。

新しいディテクタには、IP アドレス範囲、TCP ポートと UDP ポート、1 つの異常タイプを定義します。

ディテクタを定義したら、別の異常タイプを追加できます（「異常ディテクタの編集」（P.10-12）を参照）。

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

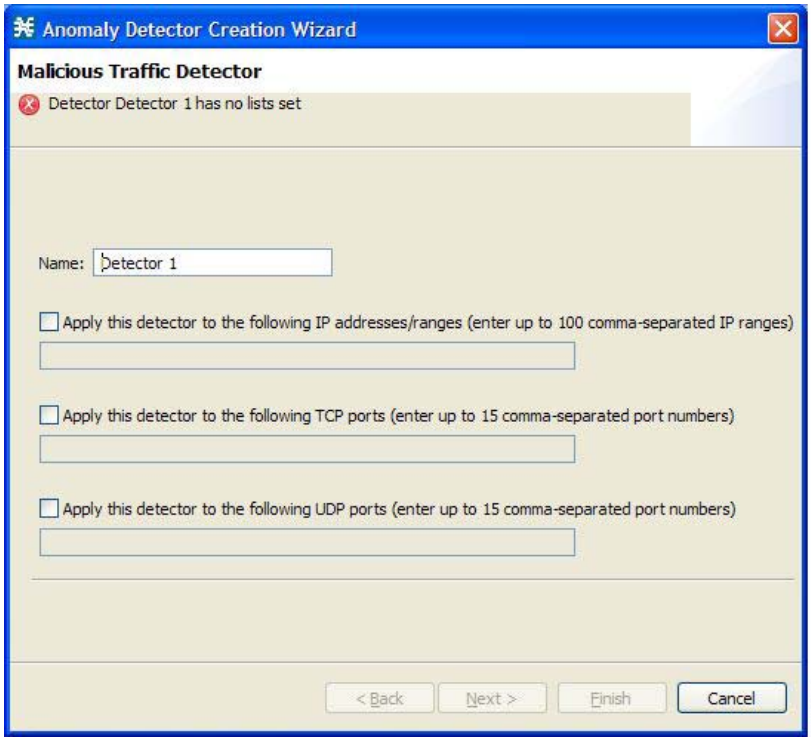
[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタ カテゴリを選択します。

ステップ 3　 をクリックします。

Anomaly Detector Creation ウィザードが表示され（図 10-6）、[Malicious Traffic Detector] ページが開きます。

図 10-6　Anomaly Detector Creation ウィザード：[Malicious Traffic Detector]



ステップ 4　ディテクタのわかりやすい名前を [Name] フィールドに入力します。

ステップ 5　1 つ以上のチェック ボックスをオンにして、ディテクタのスコープを制限します。

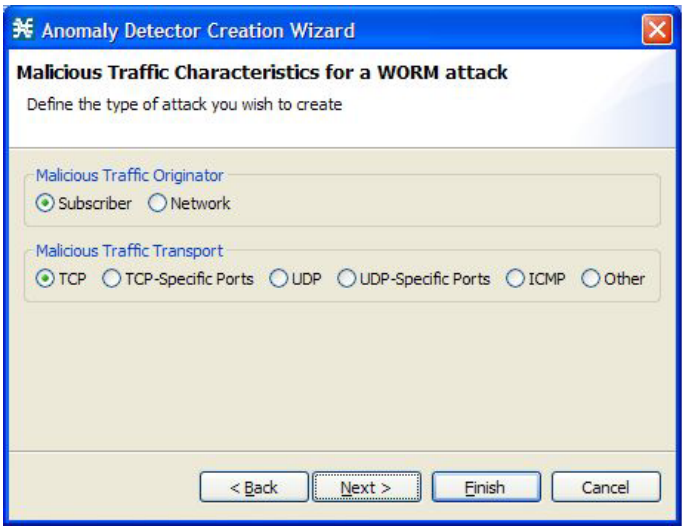
関連フィールドが有効になります。

ステップ 6　IP アドレスやポートのリストを関連フィールドに入力します。

ステップ 7　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Malicious Traffic Characteristics for a WORM attack] ページが開きます（図 10-7）。

図 10-7　[Malicious Traffic Characteristics for a Worm Attack]



ステップ 8　定義しているディテクタ タイプに応じて、発信側またはターゲット側を選択します。

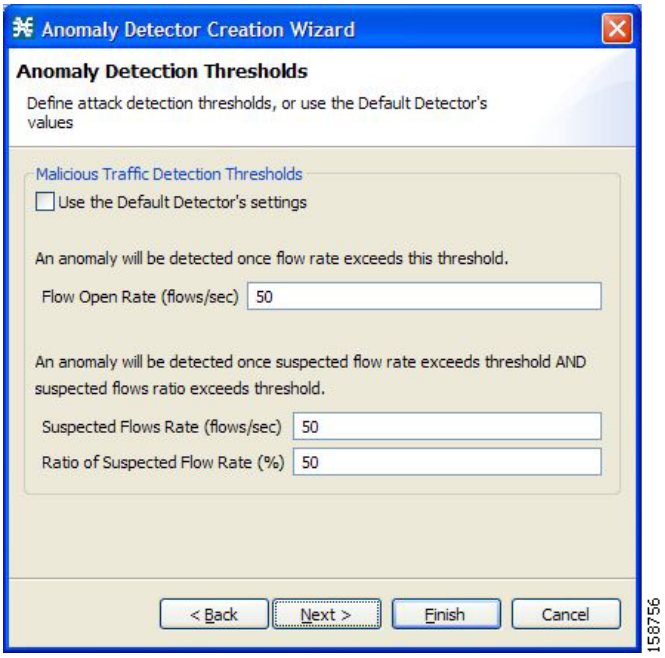
- スキャンおよびスウィープ ディテクタまたは DoS ディテクタを定義している場合は、定義している異常タイプの発信側を選択します。
- DDoS ディテクタを定義している場合は、定義している異常タイプのターゲット側を選択します。

ステップ 9　定義している異常タイプのトランスポート タイプを選択します。

ステップ 10　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Anomaly Detection Thresholds] ページが開きます（図 10-8）。

図 10-8　[Anomaly Detection Thresholds]



ステップ 11　この異常タイプのディテクタ設定を行います。

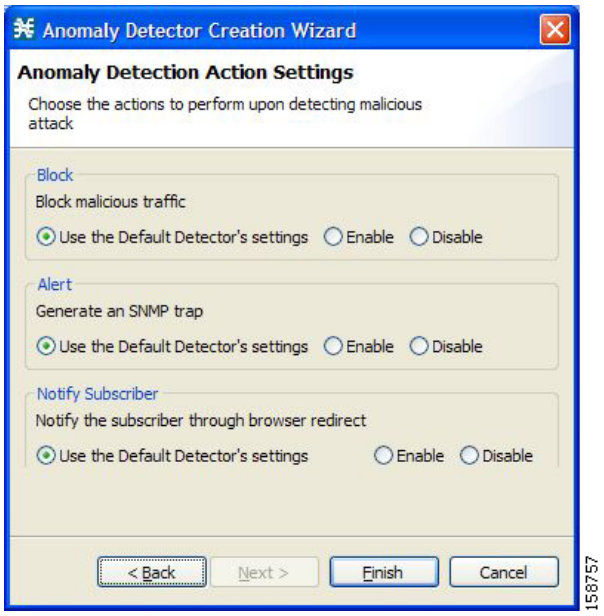
次のうちいずれかを実行します。

- デフォルト ディテクタの設定を使用するには、[Use the Default Detector's settings] チェックボックスをオンにします。
- [Flow Open Rate] フィールド、[Suspected Flows Rate] フィールド、[Ratio of Suspected Flow Rate] フィールドに値を入力します。

ステップ 12　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Anomaly Detection Action Settings] ページが開きます（図 10-9）。

図 10-9　[Anomaly Detection Action Settings]



ステップ 13　[Block]、[Alert]、[Notify Subscriber] の各処理を選択します。

ステップ 14　[Finish] をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

新しいディテクタがディテクタ ツリーに追加されます。

次の作業

別の異常タイプをディテクタに追加できます （「異常ディテクタの編集」（P.10-12）を参照）。

異常ディテクタの編集

ユーザ定義異常ディテクタでは、次の処理を実行できます。

- ディテクタ パラメータの編集
- 異常タイプの編集
- 異常タイプの追加
- 異常タイプの削除
- ディテクタ ツリーにおけるディテクタの順序の変更

  ディテクタ カテゴリごとに、ディテクタはディテクタ ツリーにリストされている順序で *下から上に*確認され、デフォルト ディテクタは最後に確認されます。

3 つのデフォルト ディテクタでは異常タイプを編集できます。

ディテクタ パラメータの編集

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタを選択します。

ディテクタのパラメータがダイアログボックスの右上の領域に表示されます。

ステップ 3　ディテクタの新しい名前を [Name] フィールドに入力します。

ステップ 4　IP アドレス範囲およびポートのチェックボックスのオンまたはオフを行います。

ステップ 5　IP アドレスやポートのリストの入力または修正を関連フィールドで行います。

ステップ 6　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

変更が保存されます。

異常タイプの編集

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタを選択します。

異常タイプに関する情報がダイアログボックスの右下に表示されます。

ステップ 3　異常タイプをダブルクリックします。

Anomaly Detector Creation ウィザードが表示され、[Anomaly Detection Thresholds] ページが開きます（「異常タイプの追加」（P.10-13）を参照）。

ステップ 4　この異常タイプのディテクタ設定を行います。

次のうちいずれかを実行します。

- デフォルト ディテクタの設定を使用するには、[Use the Default Detector's settings] チェックボックスをオンにします。
- [Flow Open Rate] フィールド、[Suspected Flows Rate] フィールド、[Ratio of Suspected Flow Rate] フィールドの値を変更します。

ステップ 5　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Anomaly Detection Action Settings] ページが開きます。

ステップ 6　[Block]、[Alert]、[Notify Subscriber] の各処理を変更します。

ステップ 7　[Finish] をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

異常タイプが変更した内容で更新されます。

ステップ 8　ステップ 3 ～ 7、またはステップ 2 ～ 7 をその他の異常タイプで繰り返します。

ステップ 9　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

異常タイプの追加

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタを選択します。

異常タイプがダイアログボックスの右下の領域にリスト表示されます。

ステップ 3　  （[Create New Detector Item Under Detector Items Feature]）をクリックします。

Anomaly Detector Creation ウィザードが表示され、[Malicious Traffic Characteristics for a WORM attack] ページが開きます（「異常ディテクタの追加」（P.10-8）を参照）。

ステップ 4　定義している異常タイプの発信元を選択します。

ステップ 5　定義している異常タイプのトランスポート タイプを選択します。

ステップ 6　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Anomaly Detection Thresholds] ページが開きます。

ステップ 7　この異常タイプのディテクタ設定を行います。

次のうちいずれかを実行します。

- デフォルト ディテクタの設定を使用するには、[Use the Default Detector's settings] チェックボックスをオンにします。
- [Flow Open Rate] フィールド、[Suspected Flows Rate] フィールド、[Ratio of Suspected Flow Rate] フィールドに値を入力します。

ステップ 8　[Next] をクリックします。

Anomaly Detector Creation ウィザードの [Anomaly Detection Action Settings] ページが開きます。

ステップ 9　[Block]、[Alert]、[Notify Subscriber] の各処理を選択します。

ステップ 10　[Finish] をクリックします。

Anomaly Detector Creation ウィザードが閉じます。

新しい異常タイプが異常タイプ リストに追加されます。

ステップ 11　ステップ 3 ～ 10、またはステップ 2 ～ 10 をその他の異常タイプで繰り返します。

ステップ 12　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

異常タイプの削除

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタを選択します。

異常タイプがダイアログボックスの右下の領域にリスト表示されます。

ステップ 3　異常タイプ リストで異常タイプを選択します。

ステップ 4　  をクリックします。

選択した異常タイプが異常タイプ リストから削除されます。

ステップ 5　ステップ 3 ～ 4、またはステップ 2 ～ 4 をその他の異常タイプで繰り返します。

ステップ 6　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

ディテクタが確認される順序の変更

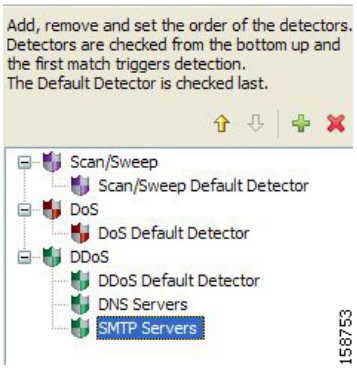
ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーでディテクタを選択します。

ツリーにおけるディテクタの位置により、上矢印か下矢印、またはその両方が有効になります（図 10-10）。

図 10-10　ディテクタ ツリー



ステップ 3　このナビゲーション矢印を使用し、目的の位置にディテクタを移動します。

ステップ 4　ステップ 2 ～ 3 をその他のディテクタに繰り返します。

ステップ 5　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

変更が保存されます。

異常ディテクタの削除

任意のユーザ定義ディテクタまたはすべてのユーザ定義ディテクタを削除できます。

3 つのデフォルト ディテクタは削除できません。

ステップ 1　サービス セキュリティ ダッシュボードの [Anomaly Based Detection of Malicious Traffic] ペインで [Configure] をクリックします。

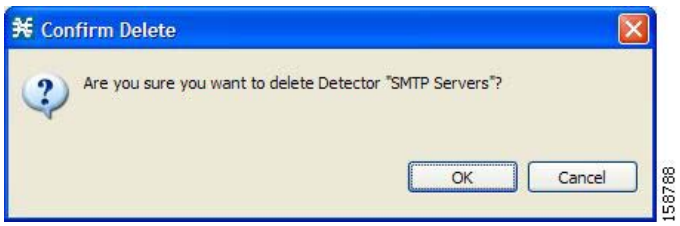
[Anomaly Detection Settings] ダイアログボックスが表示されます。

ステップ 2　ディテクタ ツリーで 1 つ以上のユーザ定義ディテクタを選択します。

ステップ 3　  をクリックします。

[Confirm Delete] メッセージが表示されます（図 10-11）。

図 10-11　[Confirm Delete]



ステップ 4　[OK] をクリックします。

選択したディテクタが削除され、ディテクタ ツリーに表示されなくなります。

ステップ 5　[OK] をクリックします。

[Anomaly Detection Settings] ダイアログボックスが閉じます。

スパム検出の管理

異常 E メール検出方式は、単一サブスクライバの SMTP セッション レートを監視します。単一サブスクライバからの SMTP セッション レートが高いということは、E メール送信に関連する悪質アクティビティを一般的に示します（E メールベースのウイルスまたはスパムゾンビ アクティビティ）。

この方式は、システムがサブスクライバアウェア モードまたはアノニマス サブスクライバ モードに設定されている場合に限り機能します。これにより SCE は、サブスクライバごとに開始される SMTP セッション数を正確にカウントできます。

この検出方式は、次の考え方に基づいています。

- 一般的なダッシュボード サブスクライバは、少数のセッションを開始します（最大でも、E メール メッセージを送信するたびに 1 つのセッション）。
- 一般的なダッシュボード サブスクライバは、通常、（メール クライアントで設定されているように）Internet Service Provider（ISP; インターネット サービス プロバイダー）の SMTP サーバをメール リレーのためだけに使用します。オフネットの SMTP サーバと通信することはありません。
- スパム ゾンビは、主にオフネット サーバ（メッセージの指定された受信者のメール サーバ）向けに多数の SMTP セッションを作成します。

スパム検出を設定する場合は、適切な監視対象サービスを選択します。デフォルトでは、組み込み SMTP サービスです。検出感度を向上させるために、さらに具体的なサービスを作成して検出のスコープを狭めることができます。次の 2 つのサービスを設定できます。

- 「発信 SMTP」：サブスクライバによって開始される SMTP セッション。
- 「オフネット SMTP」：サブスクライバの ISP の SMTP サーバをターゲットと*しない* SMTP セッション。サービスをオフネットに限定すると、正規セッションをカウントしないようにできます。

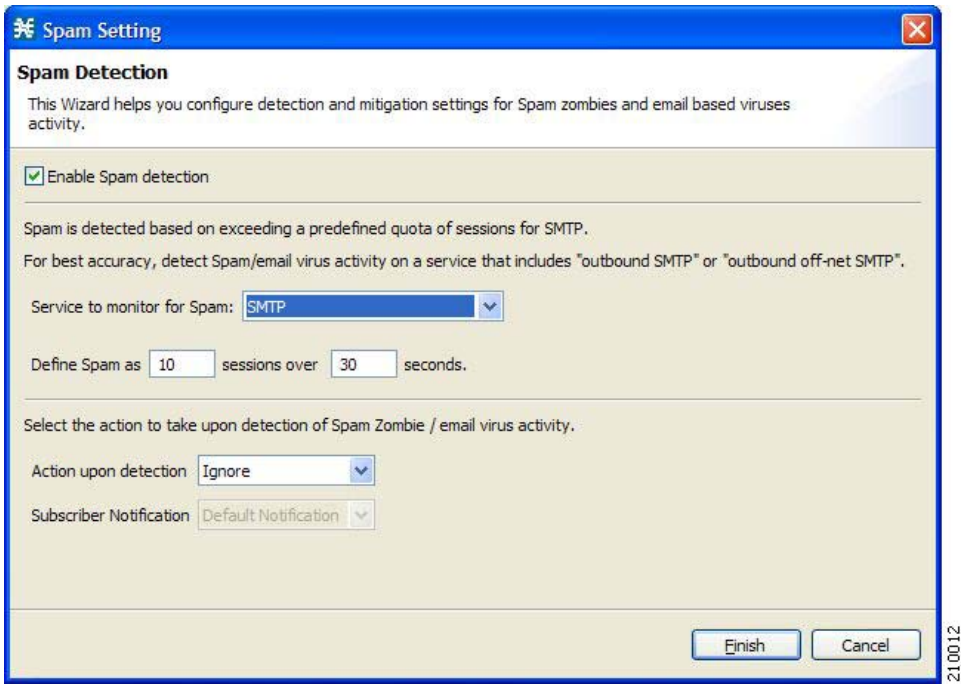
（注） 著名な非 ISP E メール プロバイダー（たとえば、Google および Yahoo!）は SMTP ベースのサービスを提供しているので、オフネットは、正規アクティビティと非正規アクティビティを良好に区別するとは言えなくなっています。オフネット サービスを改善するには、「オンネットの SMTP」サービス定義に SMTP サーバ リストを含める必要があります。これによって、他のすべての SMTP サーバがオフネットになります。

スパム検出の設定

ステップ 1　サービス セキュリティ ダッシュボードの [Spam Zombies and Email Viruses Detection] ペインの [Configure] をクリックします。

[Spam Detection and Mitigation Settings] ダイアログボックスが表示されます（図 10-12）。

図 10-12　[Spam Detection and Mitigation Settings]



ステップ 2　（オプション）スパム検出を無効にするには、[Enable Spam detection and mitigation] チェックボックスをオフにします。その他すべてのフィールドも無効になります。

ステップ 7 に進んでください。

ステップ 3　[Service to monitor for Spam] ドロップダウン リストから監視対象サービスを選択します。

（注）　「発信 SMTP」や「オフネット SMTP」などのさらに具体的なサービスを定義している場合を除いて、監視対象サービス（SMTP）のデフォルト値を変更しないでください。

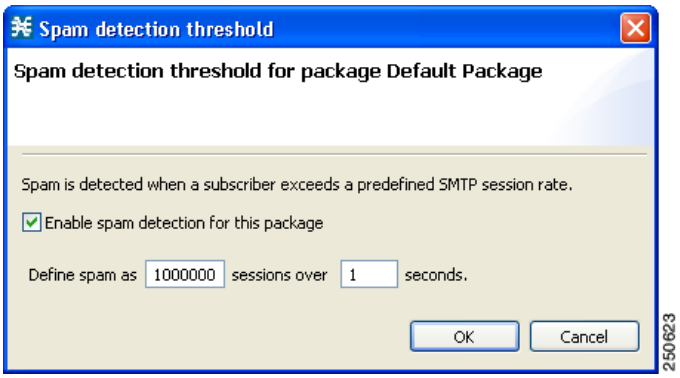
ステップ 4　各パッケージについて次の処理を実行します。

a. 異常な E メール アクティビティを示すために使用するクォータを定義します。クォータは、一定期間のセッション数として定義されます（セッション数と期間のいずれも設定可能）。これらのフィールドの値は、サブスクライバ アクティビティのベースライン監視に基づいて設定することが推奨されます。

- [Detection threshold] カラムをクリックします。

  [More] ボタン（）が表示されます。
- [More] ボタンをクリックします。
- 異常動作の E メール セッション レートのしきい値を定義します（図 10-13）。
- [OK] をクリックします。

図 10-13　[Spam Detection Threshold]



b. 大量メール送信アクティビティを検出した場合のアクションを 1 つ以上定義します。

次のアクションから選択できます。

- [Send RDR] : 1 つの RDR が SCE から Collection Manager（CM）に送信され、スパム送信者としてのサブスクライバのステータスが削除されると、第 2 の RDR が送信されます。CM は、ロギング目的でこれらの RDR を CSV ファイルに収集します。または、独自の RDR コレクタを実装して、これらの RDR を受信し、リアルタイムで応答できます。
- [Block selected service Traffic] : スパム SMTP トラフィックをブロックします。
- [Notify Subscriber (HTTP)] : サブスクライバのブラウジング セッションをキャプティブ ポータルにリダイレクトし、オペレータからのメッセージを示します。これは、「サブスクライバ通知」を使用して行います。
- [Mirror SMTP traffic] : スパム SMTP トラフィックをインライン スパム検出サービスに迂回させます。

（注）　[Send RDR] アクションでは、サブスクライバがスパム送信者として示されると 1 つの RDR が送信され、サブスクライバがスパム送信者と見なされなくなると第 2 の RDR が送信されます。しかし、ブロック、通知、およびミラーリングの各処理を使用する場合、サブスクライバがスパム送信者として示されると処理が開始され、サブスクライバがスパム送信者と見なされなくなるまで続行されます。

（注）　[Block selected service Traffic] および [Mirror SMTP traffic] の両方を選択することはできません。

ステップ 5　[Notify Subscriber (HTTP)] を選択した場合、サブスクライバへの通知を選択するか、入力します。

ステップ 6　[Mirror SMTP traffic] を選択した場合、サーバ グループを選択します。

ステップ 7　[Finish] をクリックします。

[Spam Detection and Mitigation settings] ダイアログボックスが閉じます。

悪質トラフィックに関するレポートの表示

検出されたトラフィック異常に関する情報は Collection Manager（CM）データベースに保存されます。この情報は、ネットワークの傾向調査、新しい脅威の検出、悪質ホストまたはサブスクライバの追跡に使用できます。

悪質トラフィックに関するレポート

Reporter ツールでは、悪質トラフィックに関する多くのレポートを表示できます。

- グローバル レポート
  - Global Scan/Attack Rate
  - Global DoS Rate
  - Infected Subscribers
  - Infected Subscribers versus Active Subscribers
  - DoS Attacked Subscribers
  - Top Scanned/Attacked ports
- 個別サブスクライバまたはホストのレポート
  - Top Scanning/Attacking hosts
  - Top DoS Attacked hosts
  - Top DoS Attacked Subscribers
  - Top Scanning/Attacking Subscribers

サービス セキュリティ レポートの表示

ステップ 1　サービス セキュリティ ダッシュボードの関連ペインで [View Report] をクリックします。

[Choose a report] ダイアログボックスが表示され、関連レポートのツリーが表示されます。

ステップ 2　レポートのツリーからレポートを選択します。

ステップ 3　[OK] をクリックします。

[Choose a report] ダイアログボックスが閉じます。

Reporter ツールが Console で開き、要求したレポートが表示されます。

ステップ 4　レポートの操作方法および保存方法については、『*Cisco Service Control Application Reporter User Guide*』の「Working with Reports」の章を参照してください。

トラフィック フローのフィルタリング

フィルタ規則はサービス コンフィギュレーションの一部です。フィルタ規則は、フローのレイヤ 3 プロパティおよびレイヤ 4 プロパティに基づいて、次のように Service Control Engine（SCE）プラットフォームに指示できます。

- [Bypass]：フローを無視し、変更無しで伝送します。
- [Quick forward]：フローを複製し、複製の一方を送信キューに送信して遅延を最小限にとどめます。もう一方の複製は、通常のパケット パスで送信されます。

トラフィック フローが SCE プラットフォームに着信すると、SCE プラットフォームはこのフローにフィルタ規則を適用するかどうかを確認します。

このトラフィック フローにフィルタ規則を適用する場合、SCE プラットフォームはトラフィック フローを送信キューに渡します。RDR の生成またはサービス コンフィギュレーションの実施は行われません。このフローは、分析用に生成されるレコードに現れず、アクティブなサービス コンフィギュレーションに属す規則によって制御されません。

SCE プラットフォームを通過する Operational Support System（OSS; オペレーション サポート システム）プロトコル（Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）など）、およびルーティング プロトコル（Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）など）にフィルタ規則を追加することを推奨します。このようなプロトコルは一般的にポリシーの実施から影響を受けず、ボリュームが少ないので、レポートする必要性はあまりありません。

すべての新しいサービス コンフィギュレーションには、多くの定義済みフィルタ規則が組み込まれます。

（注）　デフォルトの場合は、すべてではなく、一部の定義済みフィルタ規則がアクティブになっています。

特定プロトコルのフローを、そのフローのレイヤ 7 特性に基づいてフィルタリングすることもできます（「詳細サービス コンフィギュレーション オプションの管理」（P.10-46）を参照）。他のフィルタ処理されたフローの場合と同様に、レイヤ 7 によってフィルタ処理されたフローは制御されませんが、分類およびレポートは可能です。フィルタ処理可能なプロトコルのフローは一般的に短く、全体のボリュームは無視できます。したがって、これらのプロトコルをフィルタリングしてもネットワーク帯域幅と SCA BB レポートの精度にほとんど影響を与えません。

トラフィック フィルタリングについての情報

一部のタイプのトラフィックについてサービス プロバイダーは、SCE プラットフォームによって遅延およびジッタを低減したり、さらには SCE プラットフォームを迂回してトラフィック制御を回避する必要もあります。通常、このような決定はトラフィックの一部に対して行われ、音声など遅延に影響されやすいアプリケーションの遅延を低減し、ルーティング プロトコルなどミッションクリティカルなトラフィックを迂回させます。SCA BB Filtered Traffic メカニズムは、この必要性に対応するために使用されます。

（注）　音声トラフィックの大半は、SCE プラットフォームによって自動的に処理され、遅延を低減します（「メディア フローの自動クイック フォワーディング」（P.10-22）を参照）。

- 「SCA BB Filtered Traffic メカニズム」（P.10-21）
- 「フィルタ規則の処理」（P.10-22）
- 「フィルタ規則とサービス規則」（P.10-22）
- 「メディア フローの自動クイック フォワーディング」（P.10-22）

SCA BB Filtered Traffic メカニズム

SCA BB Filtered Traffic メカニズムは、関連フローに一致する *フィルタ規則* を定義し、これらのフローに正しいアクションを割り当てることによって遅延を低減したり、あるいはトラフィックの一部を完全に迂回させます。パケットのレイヤ 3 およびレイヤ 4 のプロパティに従って、フィルタ規則がパケットに一致します。これらのプロパティとは、IP アドレス、ポート番号、Differentiated Service Code Point（DSCP; Diffserv コード ポイント）Type of Service（ToS）、およびパケットの送信元である SCE プラットフォーム インターフェイス（サブスクライバまたはネットワーク）などです。フィルタ規則と一致するパケットについては、次の処理を適用できます。

- 現在のパケットを迂回する（遅延を低減し、トラフィック制御を回避するため）。

  この処理が適用されると、現在のパケットは、サービス コンフィギュレーションによる処理またはレポートを経ずに、SCE プラットフォームから直接送信されます。迂回されたパケットは、Class of Service（CoS; サービス クラス）にマップして、SCE プラットフォームの送信キューの 1 つに割り当てる必要があります。

  指定可能な CoS の値は、BE、AF1、AF2、AF3、AF4、および EF です。EF は、処理優先度が高いことを示し、他のクラスは通常の処理優先度であることを示します。

- フローのクイック フォワード（遅延低減のため）。

  この処理が適用されると、現在のパケットおよび同じフローに属する以降のすべてのパケットが複製され、2 つの異なるパスで送信されます。元のパケットは送信キューに直接送信されるので、最小限の遅延だけにとどまります。複製のパケットは、分類およびレポートのために通常のサービス コンフィギュレーション処理パスに送られてから破棄されます。

- フローを高処理優先度の入力キューに割り当てる（遅延低減のため）。

（注）　このオプションは、すべてのプラットフォームでサポートされているわけではありません。

- この処理が適用されると、現在のパケットおよび同じフローに属する以降のすべてのパケットが高処理優先度の入力キューに入ります。これらのパケットは、同時に到着する他のパケットよりも先に、通常のサービス コンフィギュレーション処理パスを通過します。フローは、EF CoS にマップして SCE プラットフォームの高処理優先度の送信キューに割り当てる必要があります。

（注）　Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）環境では、SCE プラットフォームは DSCP ビットを MPLS ヘッダーの EXP ビットにマッピングしません。

フィルタ規則は、上記のいずれかの処理と同時に、（パケットの DSCP ToS フィールドを変更することによって）一致したトラフィックの DSCP ToS マーキングを実行できます。

（注）　DSCP ToS マーキングおよび CoS への割り当ては、システムの動作モードが Full Functionality の場合に限り実行できます（「システムの動作モード」（P.10-44）を参照）。

フィルタ規則の処理

迂回処理およびクイック フォワード処理は、さまざまなスコープのトラフィックに適用されます。

- 迂回処理は、現在のパケットを迂回させるだけです。同じフローの以降のすべてのパケットは、Filtered Traffic メカニズムを通過します。つまり、たとえばトラフィックが宛先ポート番号に基づいて迂回される場合、双方向フローの両側からのパケットを一致させるためには 2 つの規則を作成する必要があります。

  たとえば、宛先ポート 23 に向かうすべてのトラフィックを迂回させるには、ネットワーク側のポート 23 を宛先とするサブスクライバ側から到着するパケット用に 1 つと、サブスクライバ側のポート 23 を宛先とするネットワークから到着するパケット用に 1 つの 2 つの規則が必要です。

- クイック フォワード処理は、フロー全体に適用されます。1 回識別されると、以降のすべてのパケットはフィルタ規則メカニズムではなく、通常のサービス コンフィギュレーション処理の対象となります。

パケットは、複数のフィルタ規則に一致する場合があります。迂回とクイック フォワードの両方に一致した場合、パケット / フローは最小限の遅延で迂回されます。さらに、迂回だけに一致した場合も、パケット / フローは最小限の遅延で迂回されます。

フィルタ規則とサービス規則

遅延を低減させるフィルタ規則の処理により、SCE プラットフォームがフローを制御できるようになります。つまり、サービス規則に一致する場合、フローをブロックしたり、限定された帯域幅を設定したりできます。たとえば、フィルタ規則が適用されて遅延が低減され、一方で同じトラフィックにサービス コンフィギュレーション規則が適用されてブロックされる場合、トラフィックはブロックされます。

迂回処理は、サービス コンフィギュレーション処理を回避するように設計されています。迂回されたトラフィックは、サービス規則の影響を受けません。

メディア フローの自動クイック フォワーディング

SCE プラットフォームは、分類時に SIP、MGCP、H323、Skinny、および Real-Time Streaming Protocol（RTSP）メディア フローに対してクイック フォワーディング処理を適用することによって、遅延に影響されやすい音声およびビデオのメディア フローの遅延を低減します。つまり、メディア フローがこれらのタイプの 1 つとして分類されると、ただちにクイック フォワーディングの対象となります。SCE プラットフォームは、フィルタ規則のコンフィギュレーションに関わらず、自動的にクイック フォワーディングを行います。これらのメディア フローがサービス規則に一致する場合には、ブロックされたり、限定的な帯域幅が提供されることがあります。

パッケージのフィルタ規則の表示

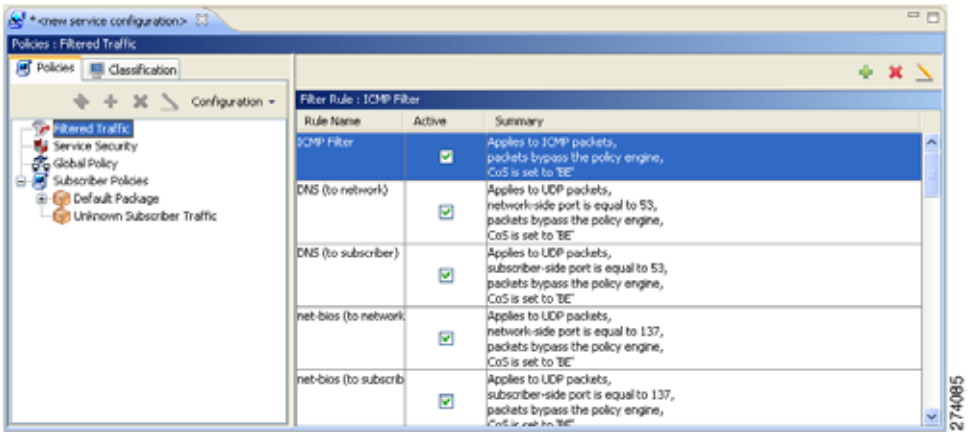
サービス コンフィギュレーションに組み込まれているフィルタ規則のリストを表示できます。

フィルタ規則ごとのリストには、規則の名前、ステータス、簡潔な説明（システムが生成）が含まれます。

フィルタ規則の詳細情報を表示するには、[Edit Filter Rule] ダイアログボックスを開きます（「フィルタ規則の編集」（P.10-28）を参照）。

ステップ 1　[Policies] タブで [Filtered Traffic] ノードを選択します。
すべてのフィルタ規則のリストが右の規則ペインに表示されます（図 10-14）。

図 10-14　　フィルタ規則



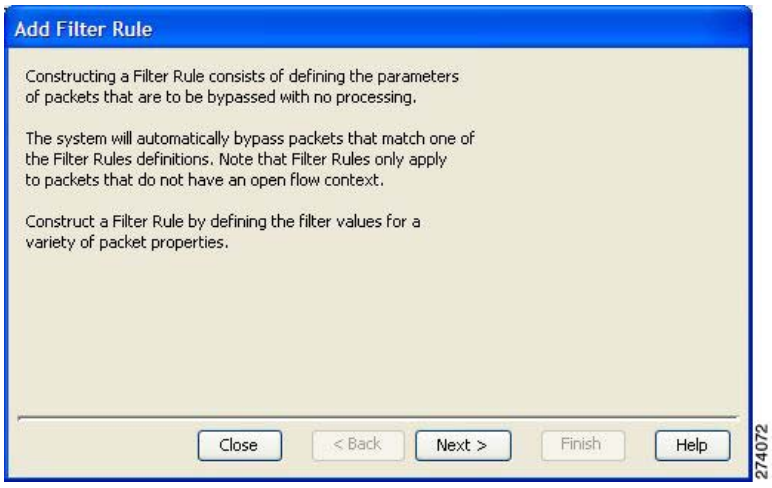
フィルタ規則の追加

Add Filter Rule ウィザードは、フィルタ規則の追加プロセスを示します。

ステップ 1　[Policies] タブで [Filtered Traffic] ノードを選択します。

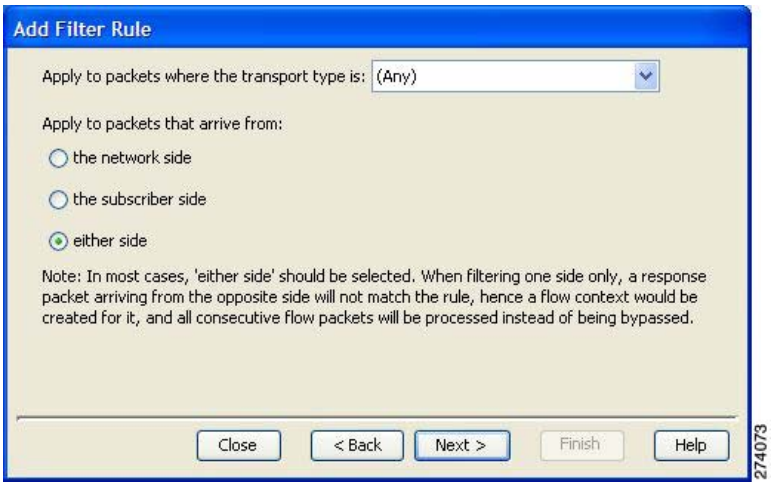
ステップ 2　右の規則ペインで、  （[Add Rules]）をクリックします。
Add Filter Rule ウィザードが表示されます（図 10-15）。

図 10-15　　Add Filter Rule



ステップ 3　[Next] をクリックします。
Add Filter Rule ウィザードの [Transport Type and Direction] ページが開きます（図 10-16）。

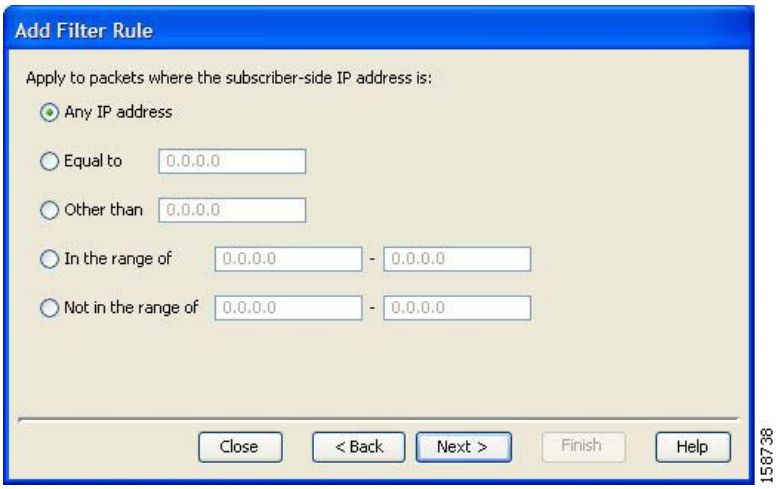
図 10-16　[Transport Type and Direction]



ステップ 4　トランスポート タイプおよび開始側を選択し、[Next] をクリックします。

Add Filter Rule ウィザードの [Subscriber-Side IP Address] ページが開きます（図 10-17）。

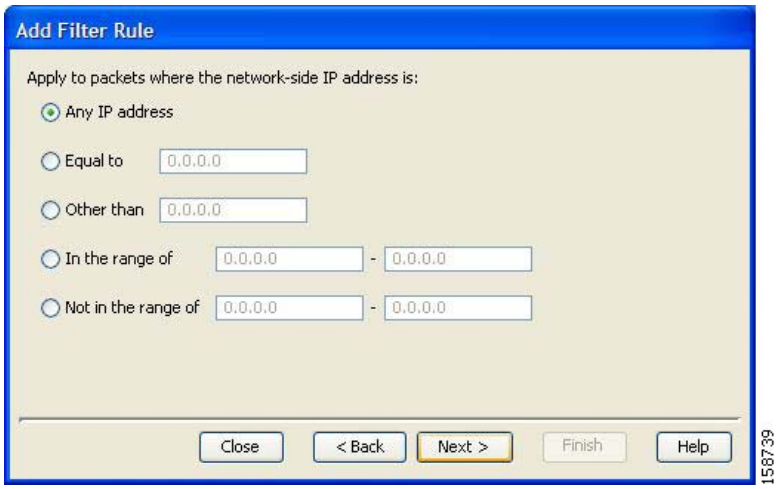
図 10-17　[Subscriber-Side IP Address]



ステップ 5　サブスクライバ側の IP アドレスを定義し、[Next] をクリックします。

Add Filter Rule ウィザードの [Network-Side IP Address] ページが開きます（図 10-18）。

図 10-18　[Network-Side IP Address]

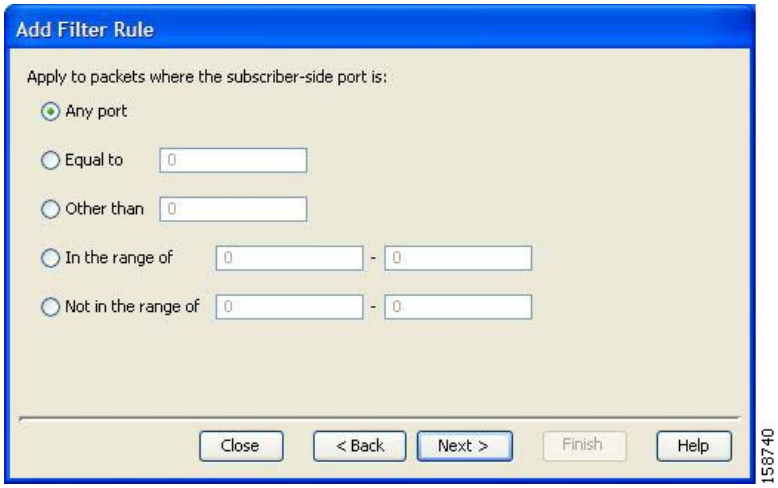


ステップ 6　ネットワーク側の IP アドレスを定義し、[Next] をクリックします。

ステップ 4 で選択したトランスポート タイプが TCP または UDP *ではない* 場合は、Add Filter Rule ウィザードの [ToS] ページが開きます。ステップ 9 に進んでください。

ステップ 4 で選択したトランスポート タイプが TCP か UDP の場合は、Add Filter Rule ウィザードの [Subscriber-Side Port] ページが開きます（図 10-19）。

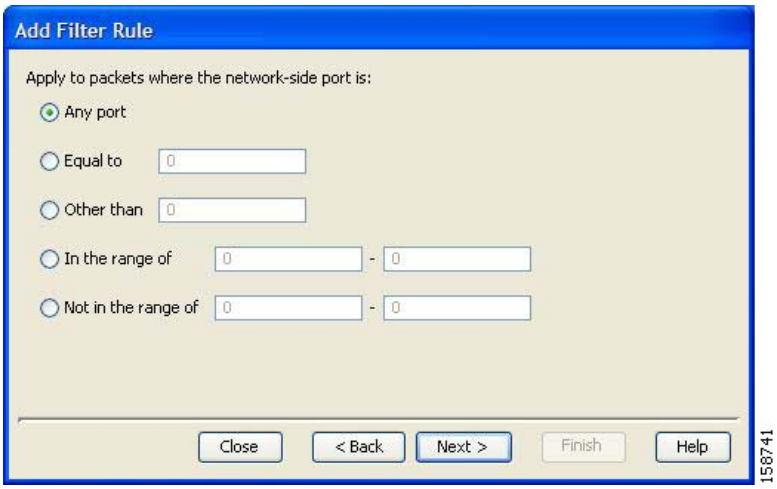
図 10-19　[Add Filter Rule]



ステップ 7　サブスクライバ側のポートを定義し、[Next] をクリックします。

Add Filter Rule ウィザードの [Network-Side Port] ページが開きます（図 10-20）。

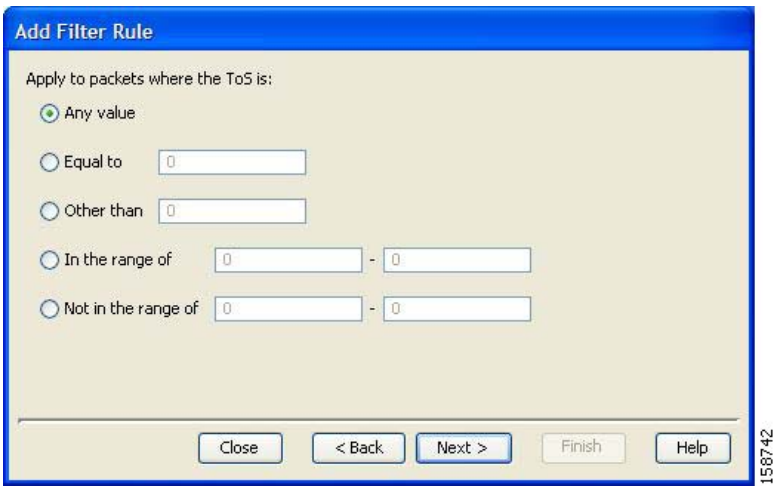
図 10-20　[Network-Side Port]



ステップ 8　ネットワーク側のポートを定義し、[Next] をクリックします。

Add Filter Rule ウィザードの [ToS] ページが開きます（図 10-21）。

図 10-21　[ToS]

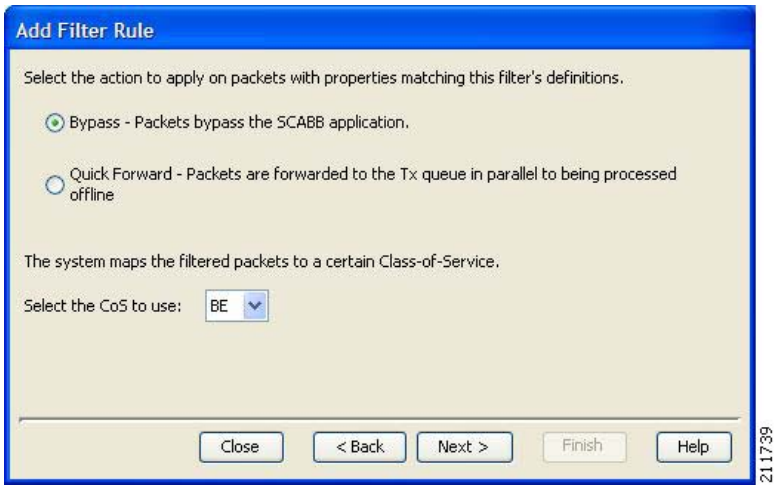


ステップ 9　ToS を定義し、[Next] をクリックします。

（注）　ToS に指定できる値は 0 ～ 63 です。

Add Filter Rule ウィザードの [Action and Class-of-Service] ページが開きます（図 10-22）。

図 10-22　[Action and Class-of-Service]



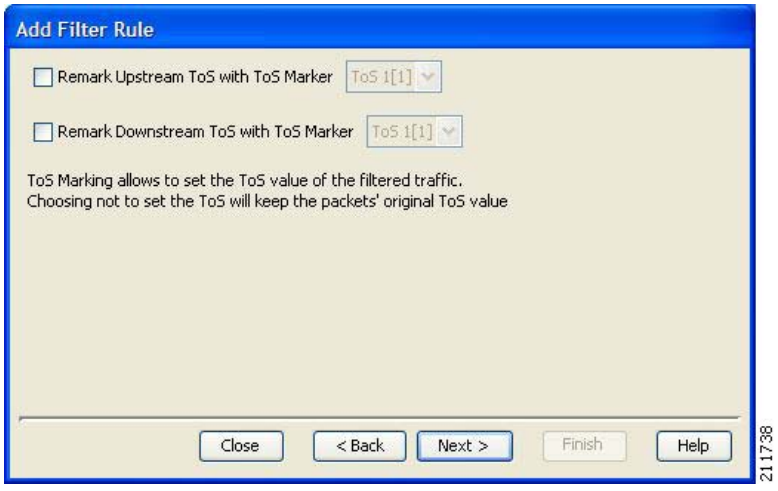
ステップ 10　必要な処理のオプション ボタンを選択します。

- [Bypass]：このフィルタ規則に一致するパケットは SCA BB に渡されません。
- [Quick Forward]：SCE プラットフォームでは、このフィルタ規則に一致するパケットの低遅延が保証されます（遅延に影響されやすいフローに使用）。パケットは複製され、SCA BB に渡されて処理されます。

ステップ 11　CoS の値を選択して [Next] をクリックします。

Add Filter Rule ウィザードの [ToS Marking] ページが開きます（図 10-23）。

図 10-23　[ToS Marking]



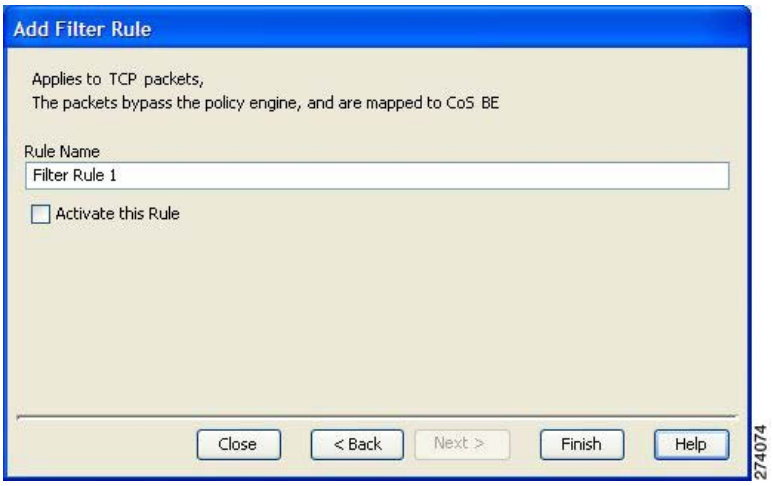
ステップ 12　（オプション）フィルタ処理されたトラフィックのパケットの DSCP ToS マーカーを変更するには、必要に応じて [Remark Upstream ToS with ToS Marker] チェックボックスおよび [Remark Downstream ToS with ToS Marker] チェックボックスをオンにし、ドロップダウン リストから必要な ToS マーカーを選択し、[Next] をクリックします。

- [ToS Marking Settings] ダイアログボックスで方向性の DSCP ToS マーキングを無効にした場合（「DSCP ToS マーカー値の管理」（P.9-74）を参照）、フィルタによる方向の DSCP ToS マーキングよりも優先されます（つまり、DSCP ToS 値は変更されません）。この場合、[Problems] 画面に警告が表示されます。

- ステップ 4 で一方向のフローをフィルタ処理したものの、このステップで別の方向の ToS マーキングを選択した場合、フィルタ規則は作成されますが、DSCP ToS の再マーキングは行われません。この場合、[Problems] 画面に警告が表示されます。
- 前のステップで [Quick Forward] を選択した場合、SCA BB は元のパッケージを受け取り、処理します。つまり、フィルタ規則で選択された ToS マーキング アクションに関係なく、元の DSCP ToS 値が認識されます。

Add Filter Rule ウィザードの [Finish] ページが開きます（図 10-24）。

図 10-24　[Finish]



ステップ 13　新しいフィルタ規則の一意の名前を [Rule Name] フィールドに入力します。

（注）　フィルタ規則にはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

ステップ 14　（オプション）フィルタ規則をアクティブにするには、[Activate this rule] チェックボックスをオンにします。トラフィックのフィルタリング基準となるのは、アクティブな規則だけです。

ステップ 15　[Finish] をクリックします。

Add Filter Rule ウィザードが閉じます。

フィルタ規則が追加され、[Filter Rule] テーブルに表示されます。

フィルタ規則の編集

フィルタ規則のパラメータを表示および編集できます。

ステップ 1　[Policies] タブで [Filtered Traffic] ノードを選択します。

すべてのフィルタ規則のリストが右の規則ペインに表示されます。

ステップ 2　[Filter Rule] テーブルで規則を選択します。

ステップ 3　([Edit Rule]）をクリックします。

Edit Filter Rule ウィザードの [Introduction] ページが表示されます。

Edit Filter Rule ウィザードは Add Filter Rule ウィザードと同じです。

ステップ 4　「フィルタ規則の追加」（P.10-23）のステップ 4 ～ 14 の手順に従います。

ステップ 5　[Finish] をクリックします。

フィルタ規則が変更され、関連変更内容が [Filter Rule] テーブルに表示されます。

フィルタ規則の削除

フィルタ規則を削除できます。サブスクライバ IP アドレスごとに定義された各規則に従って、IP アドレスおよびその属性の処理を再開する場合などにフィルタ規則を削除すると便利です。

ステップ 1　[Policies] タブで [Filtered Traffic] ノードを選択します。

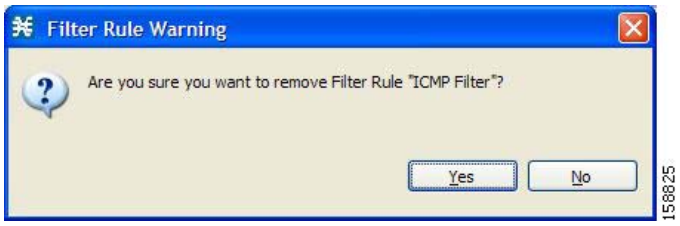
すべてのフィルタ規則のリストが右の規則ペインに表示されます。

ステップ 2　[Filter Rule] テーブルで規則を選択します。

ステップ 3　  （[Delete Rule]）をクリックします。

[Filter Rule Warning] メッセージが表示されます（図 10-25）。

図 10-25　[Filter Rule Warning]



ステップ 4　[Yes] をクリックします。

フィルタ規則が削除され、[Filter Rule] テーブルに表示されなくなります。

フィルタ規則の無効化と有効化

フィルタ規則の有効化または無効化はいつでも実行できます。フィルタ規則の無効化にはフィルタ規則の削除と同じ効果がありますが、パラメータはサービス コンフィギュレーションに保持され、あとでフィルタ規則を再び有効にすることができます。

ステップ 1　[Policies] タブで [Filtered Traffic] ノードを選択します。

すべてのフィルタ規則のリストが右の規則ペインに表示されます。

ステップ 2　[Filter Rule] テーブルで規則を選択します。

ステップ 3　規則を有効にするには、[Active] チェックボックスをオンにします。

ステップ 4　規則を無効にするには、[Active] チェックボックスをオフにします。

ステップ 5　ステップ 3 ～ 4 をその他の規則に繰り返します。

サブスクライバ通知の管理

サブスクライバ通知機能では、サブスクライバ HTTP トラフィックが関連 Web ページにリダイレクトされて、Web ベースのメッセージがサブスクライバに示されます。これらの Web ページには、クォータ枯渇の通知など、サブスクライバに関連する情報が含まれています。HTTP のリダイレクションは、サブスクライバ通知がアクティブになると開始し、サブスクライバ通知が解除されると終了します。

（注）　単方向分類が有効になっている場合、サブスクライバ通知はサポートされません。

サブスクライバ リダイレクション パラメータの各セットは、通知リダイレクト プロファイルを含んでいます。Cisco Service Control Application for Broadband（SCA BB）では、（通知プロファイルおよびリダイレクト プロファイルを含む）最大 128 のリダイレクト プロファイルがサポートされます。削除できないデフォルトのリダイレクト プロファイルには、デフォルト通知、ネットワーク攻撃通知、およびデフォルトのリダイレクションの 3 種類があります。規則を定義するときに使用する通知リダイレクト プロファイルを設定します。

- 「サブスクライバ通知パラメータ」（P.10-30）
- 「ネットワーク攻撃通知」（P.10-32）
- 「通知リダイレクト プロファイルの追加」（P.10-33）
- 「リダイレクション URL セットの追加」（P.10-41）

サブスクライバ通知パラメータ

各リダイレクト プロファイル タイプの通知には、次のサブスクライバ通知パラメータが含まれています。

（注）　[Activation trigger configuration] オプションは、リダイレクト プロファイル タイプのリダイレクトにだけ使用できます。

- [Name]：各プロファイルの名前は、一意である必要があります。

（注）　デフォルト通知またはネットワーク攻撃通知の名前を変更することはできません。

- [Redirect profile type]：各プロファイルは、次の 2 つのタイプのいずれかです。
  - [Notification]
  - [Redirect]
- [Set of Redirection URLs]：リダイレクションをアクティブにしたあとでサブスクライバの HTTP フローがリダイレクトされる、設定可能な宛先 URL。この Web ページには、通常、サブスクライバに伝達する必要があるメッセージが含まれています。このリダイレクション セットは、リダイレクト理由およびサブスクライバ ID を含む宛先 URL に追加される 1 つまたは複数のパラメータを含むことができます。

  宛先 Web サーバではこのパラメータを使用し、意味のあるメッセージをサブスクライバに伝えることができます。
- [Activation frequency]：通知リダイレクトをアクティブにする時期を示します。このアクティベーション頻度は、次のいずれかです。

（注）　[Periodically] オプションは、リダイレクト プロファイル タイプのリダイレクトの場合にだけ使用できます。

- [Only once]：サブスクライバは、条件が一致した初回だけ通知にリダイレクトされます。

  たとえば、クォータを超過した場合、サブスクライバが宛先 URL をブラウズすると、サブスクライバに通知されます（サブスクライバが引き続き違反状態である場合も同様です）。

- [Always]：サブスクライバは、条件が一致するたびに通知にリダイレクトされます。

  たとえば、クォータを超過した場合、サブスクライバが自身のクォータをリフレッシュする手順を完了するまで、何回もリダイレクトされます。

- [Until the subscriber browses to]：サブスクライバが宛先 URL から別の最終 URL に進むまで、条件が一致するたびに通知にリダイレクトされます。

  たとえば、クォータを超過した場合、宛先 URL にある Web ページで、メッセージを参照したあとに [Acknowledge] ボタンを押すように、サブスクライバに要求することができます。確認応答 URL は解除 URL として定義され、以降の通知は非アクティブになります。

  解除 URL は、URL ホスト名、URL パス、これらを区切るコロンで構成されます。フォーマットは次のとおりです。

  ```
  [*]<hostname>:<path>[*]
  ```

  - <**hostname**> の前にワイルドカード（*）を付加して、同じサフィックスを持つすべてのホスト名と一致させることができます。
  - パス要素は、常に「/」で開始する必要があります。
  - <**path**> のあとにワイルドカード（*）を付加して、共通のプレフィクスを持つすべてのパスと一致させることができます。

    たとえば、***.some-isp.net:/redirect/*** というエントリは、次のすべての URL と一致します。

    - www.some-isp.net/redirect/index.html
    - support.some-isp.net/redirect/info/warning.asp
    - noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

- [List of Allowed URLs]：リダイレクションがアクティブでも、ブロックとリダイレクトが行われない URL のリスト。

  リダイレクションをアクティブにしたあとで、宛先 URL および解除 URL へのフローを除くすべての HTTP フローはブロックされて、宛先 URL にリダイレクトされます。ただし、サブスクライバに追加 URL セットへのアクセスを許可することができます。たとえば、サブスクライバが詳細サポート情報にアクセスできるようにする場合は、これが便利です。

  許可 URL の形式は解除 URL と同じです。

これらのパラメータは、新しい通知リダイレクト プロファイルを追加したときに定義されます（「リダイレクション URL セットの追加」（P.10-41）を参照）。パラメータの修正はいつでもできます。

ネットワーク攻撃通知

サブスクライバ通知では、サブスクライバにマッピングされた IP アドレスに関連する現在の攻撃について、サブスクライバにリアルタイムで通知されます（これらの通知を有効にする方法は、「サービス セキュリティ ダッシュボード」（P.10-2）を参照してください）。SCA BB は、サブスクライバから送信された HTTP フローを、攻撃に関する情報を提供するサーバへリダイレクトして、攻撃についてサブスクライバに通知します。

サブスクライバ通知の 1 つであるネットワーク攻撃通知はこの通知専用であり、削除できません。ネットワーク攻撃通知は攻撃の最後で解除されず、サブスクライバは応答する*必要があります*。

トラフィックのブロック時にリダイレクションを許可するには、1 つの指定 TCP ポート（デフォルトではポート 80）を開いておくようにシステムを設定します。「詳細サービス コンフィギュレーション オプションの管理」（P.10-46）を参照してください。

注意　これまでのリリースの SCA BB では、CLI コマンドを使用してネットワーク攻撃通知を設定していました。CLI コマンドをこの目的に使用する必要はなくなりました。

ネットワーク攻撃通知パラメータ

ネットワーク攻撃が検出されると、サブスクライバの HTTP フローは設定可能な宛先 URL にリダイレクトされます。この Web ページでは、サブスクライバに伝達する必要がある警告が表示されます。

宛先 URL には、通知パラメータを含むクエリー部分を含めることもできます。宛先 Web サーバではこのパラメータを使用し、サブスクライバへの特定の警告を作成できます。

宛先 URL のクエリー部分の形式は次のとおりです。

```
?ip=<ip>&side=<side>&dir=<dir>&prot=<protocol>&no=<open-flows>&nd=<suspected-flows>&to=<open-flows-threshold>&td=<suspected-flows-threshold>&ac=<action>&nh=>handled-flows>
```

表 10-1 に、テール内の各フィールドの意味を示します。

表 10-1　テール フィールドの説明

フィールド	説明	指定可能な値
[ip]	検出された IP アドレス	
[side]	—	• s：サブスクライバ • n：ネットワーク
[dir]	—	• s：ソース • d：宛先
[protocol]	—	• TCP • UDP • ICMP • OTHER
[open-flows]	オープン フロー数	—
[suspected flows]	攻撃を受けた疑いのあるフロー数	—

表 10-1　テール フィールドの説明 （続き）

フィールド	説明	指定可能な値
[open-flows-threshold]	オープン フローのしきい値	—
[suspected-flows-threshold]	攻撃を受けた疑いのあるフローのしきい値	—
[action]	—	• R：レポート • B：ブロックおよびレポート
[handled-flows]	攻撃開始以降に処理されたフロー数 （攻撃中および攻撃の最後ではゼロ以外）	—

説明テールを含む URL の例

```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&proto=TCP&no=34&nd=4&to=34&td=10&ac=B&nh=100
```

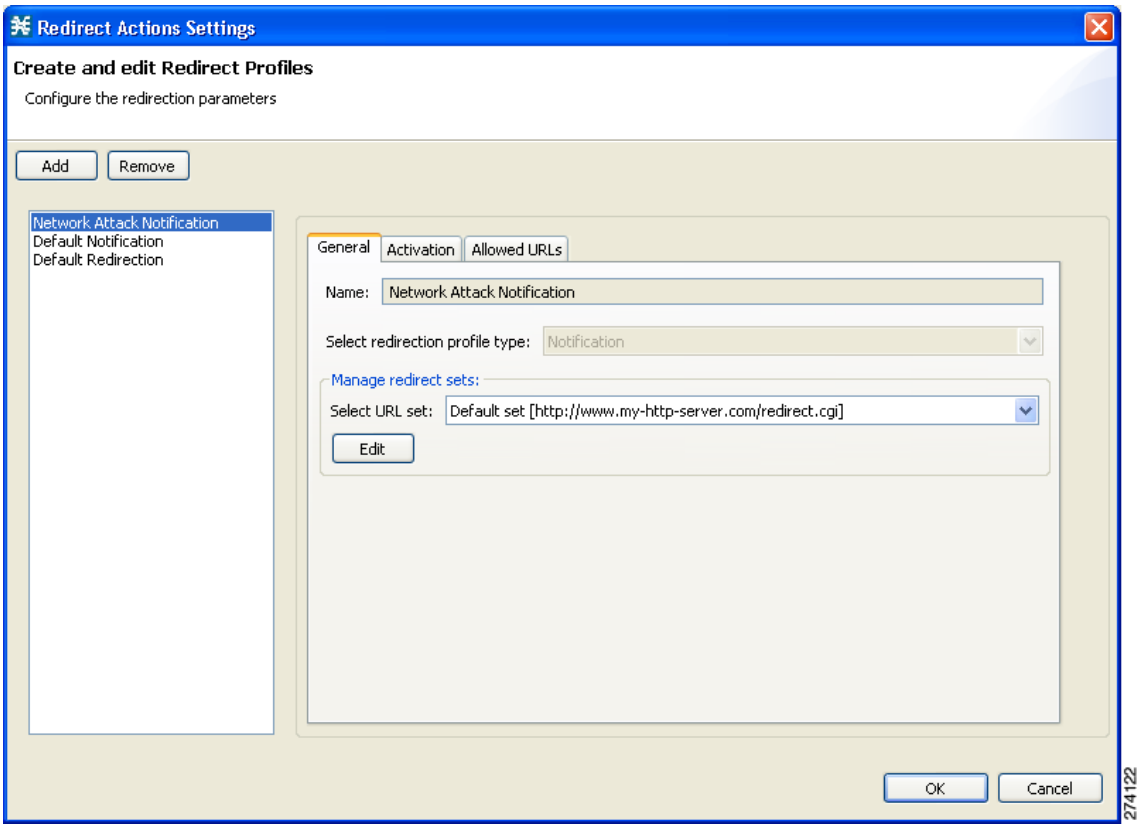
通知リダイレクト プロファイルの追加

（注）　通知リダイレクト プロファイルを作成しても、サブスクライバ通知機能はアクティブになりません。通知リダイレクト プロファイルを定義したら、特定のパッケージに対してアクティブにする必要があります

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [Subscriber Redirection] を選択します。

[Redirect Actions Settings] ダイアログボックスが表示されます（図 10-26）。

図 10-26　[Redirect Action Settings]：[General] タブ



ステップ 2　[Add] をクリックします。

デフォルトのリダイレクション URL セットを含む新しいリダイレクション プロファイルが、リダイレクション プロファイル リストに追加されます。

ステップ 3　新しい通知リダイレクト プロファイルの一意の名前を [Name] フィールドに入力します。

（注）　通知リダイレクト プロファイルにはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

ステップ 4　[Select redirection profile type] フィールドで、[Notification] を選択します。

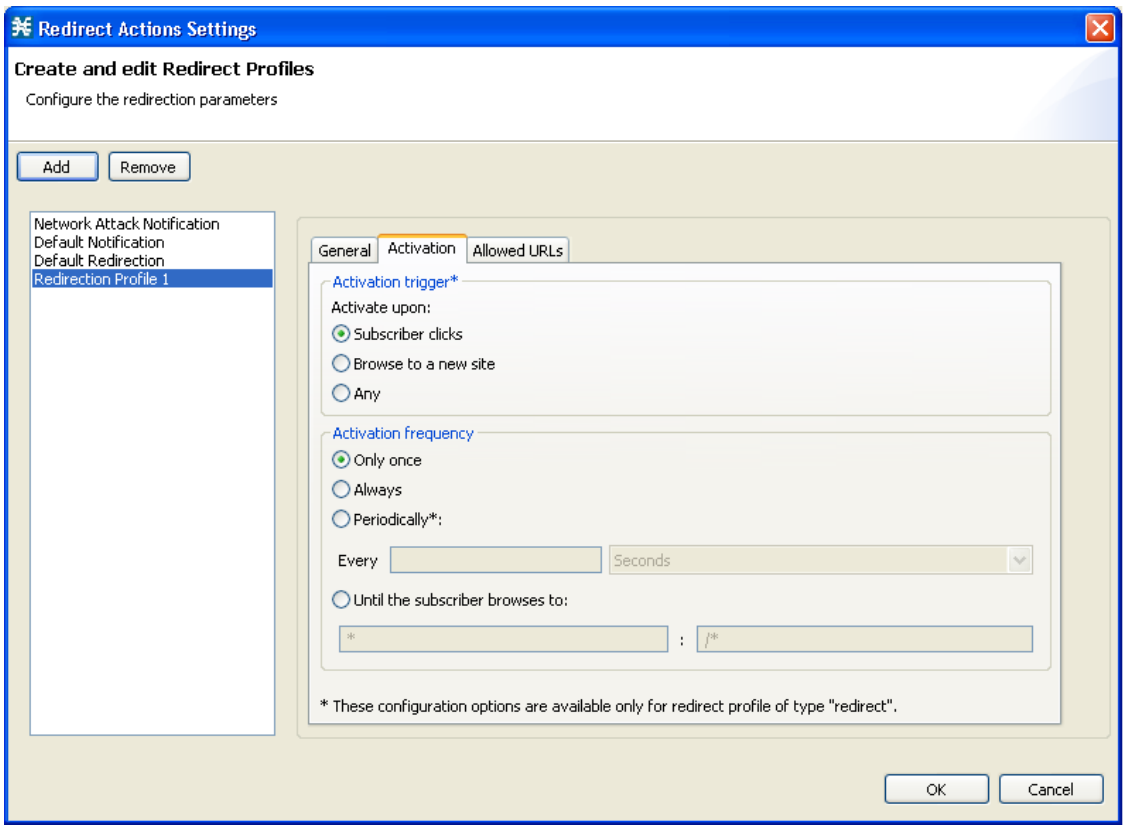
このステップを省略しないでください。省略した場合、通知リダイレクト プロファイルではなく、リダイレクト プロファイルが作成されます。

ステップ 5　URL セットを選択します。

ステップ 6　[Activation] タブを選択します。

[Activation] タブが表示されます（図 10-27）。

図 10-27　[Activation] タブ



ステップ 7　リダイレクションがトリガーされる頻度を設定します。次のいずれかの [Activation frequency] オプション ボタンを選択します。

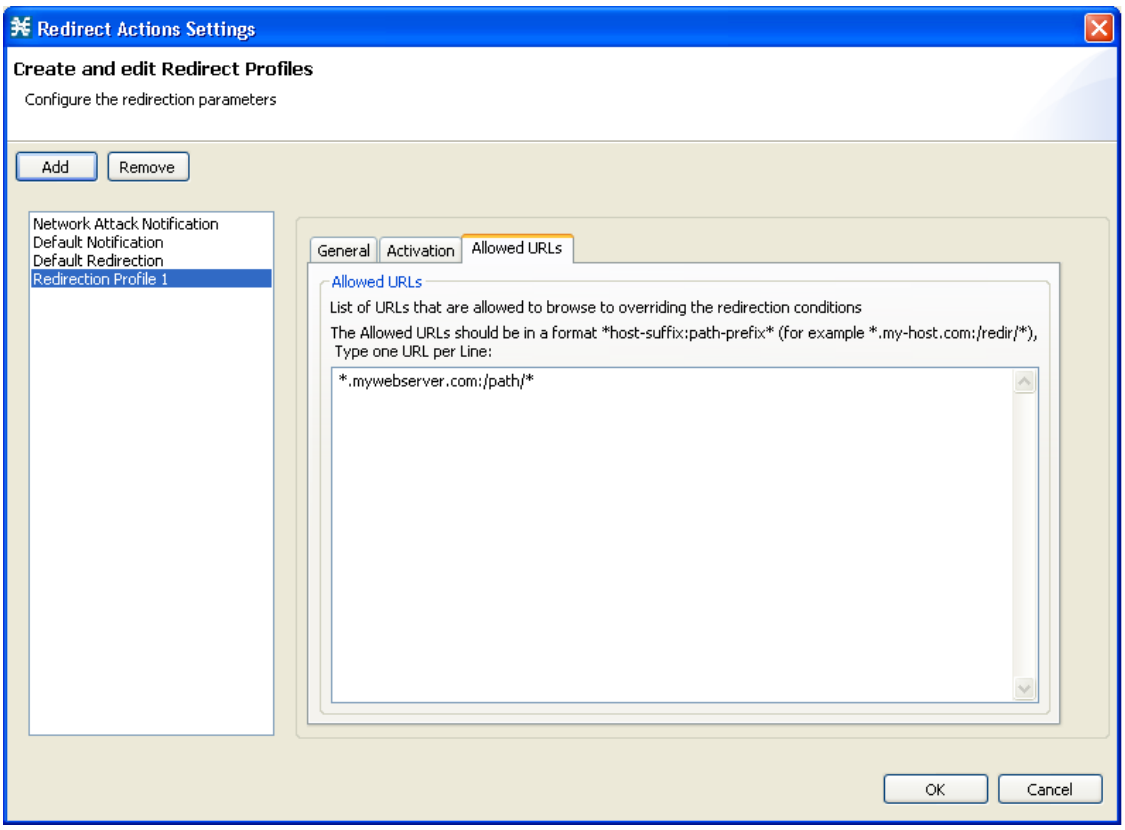
- [Only once]
- [Always]
- [Until the subscriber browses to]

ステップ 8　[Until the subscriber browses to] オプション ボタンを選択する場合は、表示されるフィールドに解除 URL ホストサフィックスおよびパスプレフィクスを入力します。

ステップ 9　[Allowed URLs] タブをクリックします。

[Allowed URLs] タブが開きます（図 10-28）。

図 10-28　[Allows URLs] タブ



ステップ 10　（オプション）許可 URL を 1 行に 1 つずつ入力します。

ステップ 11　[OK] をクリックします。

[Redirect Actions Settings] ダイアログボックスが閉じます。

通知リダイレクト プロファイルがプロファイル リストに追加されます。

サブスクライバ リダイレクションの管理

パッケージの規則によって、選択したプロトコルへのアクセスが拒否されることがあります。パッケージのサブスクライバが、ブロックされているプロトコルにアクセスしようとすると（たとえば「ゴールド」サブスクライバだけが使用可能なサービスに「シルバー」サブスクライバがアクセスしようとすると）、トラフィック フローはサーバにリダイレクトされ、リダイレクションの理由についてその Web ページで説明されます。この Web ページにより、パッケージをアップグレードする機会をサブスクライバに提供できます。規則を定義するときに使用するリダイレクション プロファイルを設定します。

（注）　単方向分類が有効になっている場合、リダイレクションはサポートされません。

各リダイレクト プロファイルは、一連のリダイレクト パラメータで構成されています。Cisco Service Control Application for Broadband（SCA BB）では、（通知リダイレクト プロファイルおよびリダイレクト プロファイルを含む）最大 128 のリダイレクト プロファイルがサポートされます。

サブスクライバ リダイレクト パラメータ

各リダイレクト タイプのリダイレクト プロファイルには、次のパラメータが含まれています。

- [Name]：各プロファイルの名前は、一意である必要があります。

（注）　デフォルトのリダイレクション プロファイルの名前は変更できません。

- [Redirect profile type]：各プロファイルは、次の 2 つのタイプのいずれかです。
  - [Notification]
  - [Redirect]
- [Set of Redirection URLs]：リダイレクションをアクティブにしたあとでサブスクライバの HTTP フローがリダイレクトされる、設定可能な宛先 URL。このリダイレクション セットは、リダイレクト理由またはサブスクライバ ID を含む宛先 URL に追加される 1 つまたは複数のパラメータを含むことができます。
- [Activation trigger]：リダイレクトをトリガーするアクション。このアクティベーション トリガーは、次のいずれかです。
  - [Subscriber clicks]：サブスクライバのリンク クリックによってリダイレクトがアクティブになる場合
  - [Browse to a new site]：ブラウジングによってリダイレクトがアクティブになる場合
  - [Any]：リンクまたはブラウジングによってリダイレクトがアクティブになる場合
- [Activation frequency]：リダイレクトをアクティブにする時期を示します。このアクティベーション頻度は、次のいずれかです。
  - [Only once]：サブスクライバは、条件が一致した初回だけリダイレクトされます。
  - [Always]：サブスクライバは、条件が一致するたびにリダイレクトされます。
  - [Triggering events]
  - [KBytes]
  - [Until the subscriber browses to]：サブスクライバが宛先 URL から別の最終 URL に進むまで、条件が一致するたびにリダイレクトされます。

    解除 URL は、URL ホスト名、URL パス、これらを区切るコロンで構成されます。フォーマットは次のとおりです。

    ```
    [*]<hostname>:<path>[*]
    ```

  - <**hostname**> の前にワイルドカード（*）を付加して、同じサフィックスを持つすべてのホスト名と一致させることができます。
  - パス要素は、常に「/」で開始する必要があります。
  - <**path**> のあとにワイルドカード（*）を付加して、共通のプレフィクスを持つすべてのパスと一致させることができます。

    たとえば、***.some-isp.net:/redirect/*** というエントリは、次のすべての URL と一致します。

    • www.some-isp.net/redirect/index.html

    • support.some-isp.net/redirect/info/warning.asp

    • noquota.some-isp.net/redirect/acknowledge.aspx?ie=UTF-8

- [List of Allowed URLs]：リダイレクションがアクティブでも、ブロックとリダイレクトが行われない URL のリスト。

  リダイレクションをアクティブにしたあとで、宛先 URL および解除 URL へのフローを除くすべての HTTP フローはブロックされて、宛先 URL にリダイレクトされます。ただし、サブスクライバに追加 URL セットへのアクセスを許可することができます。たとえば、サブスクライバが詳細サポート情報にアクセスできるようにする場合は、これが便利です。

  許可 URL の形式は解除 URL と同じです。

これらのパラメータは、新しい通知リダイレクト プロファイルを追加したときに定義されます。パラメータの修正はいつでもできます。

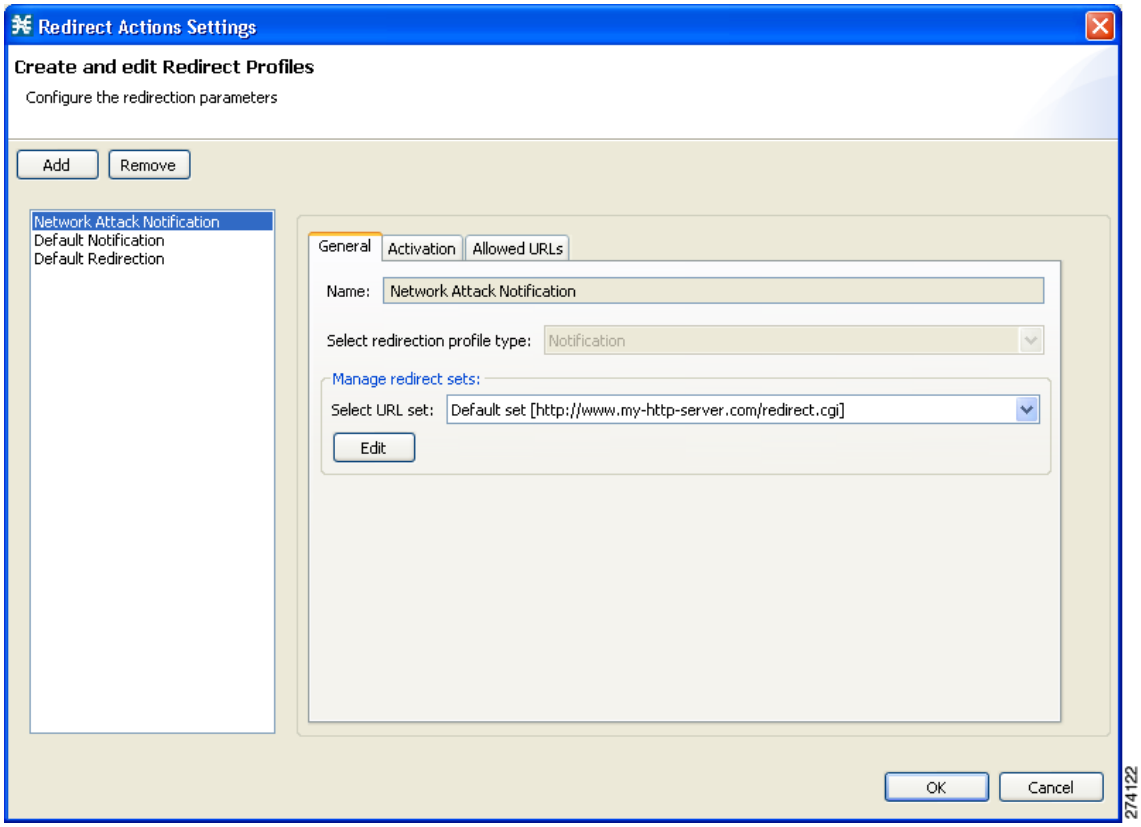
リダイレクト プロファイルの追加

リダイレクト プロファイルには、一連のリダイレクション URL およびリダイレクトをトリガーするアクションまたはリダイレクトが発生する頻度などリダイレクト機能を使用する条件が含まれています。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [Subscriber Redirection] を選択します。

[Redirect Actions Settings] ダイアログボックスが表示されます（図 10-29）。

図 10-29　[Redirect Actions Settings] : [General] タブ



ステップ 2　[Add] をクリックします。

デフォルトのリダイレクション URL セットを含む新しいリダイレクト プロファイルが、リダイレクト プロファイル リストに追加されます。

ステップ 3　新しいリダイレクト プロファイルの一意の名前を [Name] フィールドに入力します。

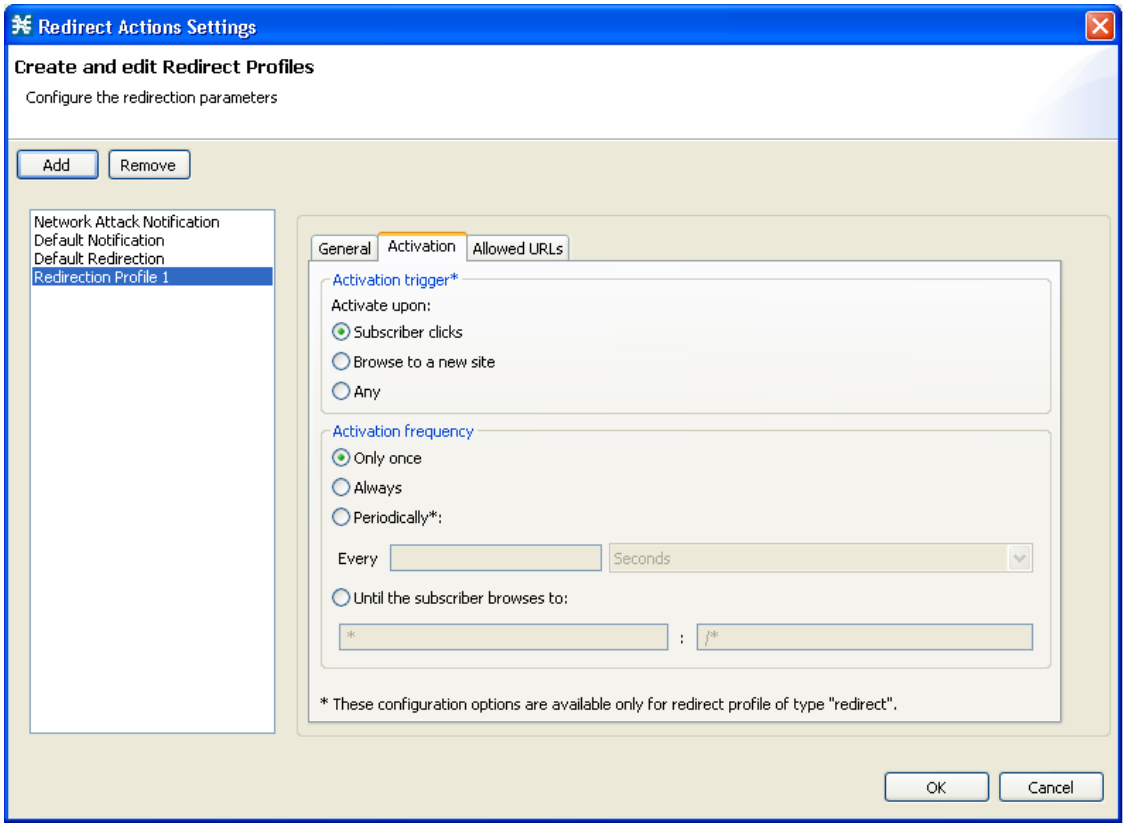
（注）　リダイレト プロファイルにはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

ステップ 4　URL セットを選択します。

ステップ 5　[Activation] タブを選択します。

[Activation] タブが表示されます（図 10-30）。

図 10-30　[Activation] タブ



ステップ 6　リダイレクションをトリガーするアクティビティを設定します。次のいずれかの [Activation trigger] オプション ボタンを選択します。

- [Subscriber clicks]
- [Browse to a new site]
- [Any]

ステップ 7　リダイレクションがトリガーされる頻度を設定します。次のいずれかの [Activation frequency] オプション ボタンを選択します。

- [Only once]
- [Always]
- [Periodically]
- [Until the subscriber browses to]

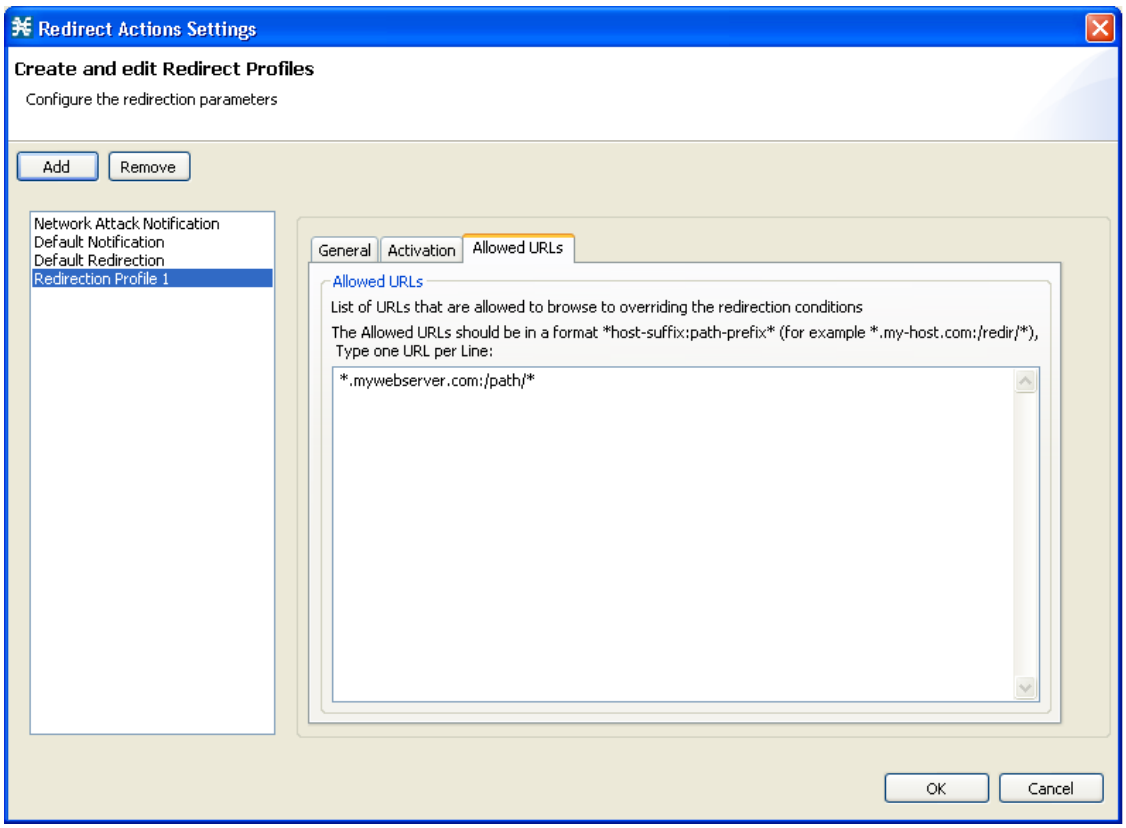
ステップ 8　[Periodically] オプション ボタンを選択した場合、[Every] フィールドに数字とインクリメントを入力してリダイレクションの発生頻度を指定します。

ステップ 9　[Until the subscriber browses to] オプション ボタンを選択した場合、表示されるフィールドに解除 URL を入力します。

ステップ 10　[Allowed URLs] タブをクリックします。

[Allowed URLs] タブが開きます（図 10-31）。

図 10-31　[Allowed URLs] タブ



ステップ 11　（オプション）ブラウズしてもよい 1 つまたは複数の URL を入力します。これは、リダイレクト条件よりも優先されます。

ステップ 12　[OK] をクリックします。

[Redirect Actions Settings] ダイアログボックスが閉じます。

リダイレクション プロファイルがリダイレクション プロファイル リストに追加されます。

リダイレクション プロファイルの削除

デフォルト リダイレクション プロファイルは削除できません。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [Subscriber Redirection] を選択します。

[Redirect Actions Settings] ダイアログボックスが表示されます。

ステップ 2　プロファイルの名前をクリックします。

ステップ 3　[Remove] をクリックします。

ステップ 4　[OK] をクリックします。

[Redirect Actions Settings] ダイアログボックスが閉じます。

リダイレクション設定が保存されます。

リダイレクション URL セットの追加

Console のリダイレクション機能では、次の 3 つのプロトコルだけがサポートされます。

- HTTP Browsing
- HTTP Streaming
- RTSP Streaming

リダイレクション セットには、これらの 3 つのプロトコルにそれぞれ対応したリダイレクション オプションが 1 つずつ含まれています。システムはデフォルトのリダイレクション セットを提供しますが、これは削除できません。最大で 127 のリダイレクション セットを追加できます。

各リダイレクション URL には、次のフォーマットの URL 指定名、サブスクライバ ID、およびサービス ID が含まれています。

```
<URL>?n=<subscriber-ID>&s=<service-ID>
```

URL には、1 つまたは複数のパラメータを追加することもできます。

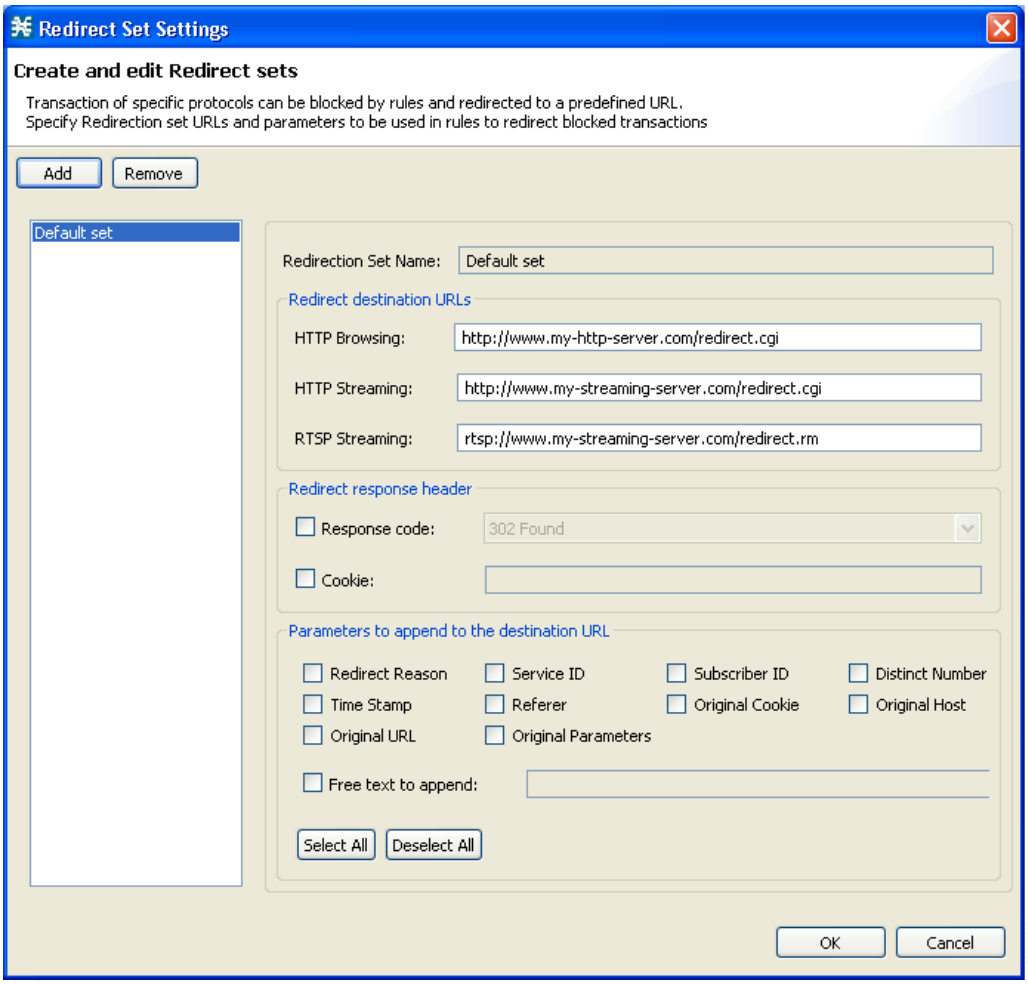
ステップ 1　左のペインの [Policies] タブで、[Configuration] > [Subscriber Redirection] を選択します。

[Redirect Actions Settings] ダイアログボックスが表示されます。

ステップ 2　[General] タブで、[Edit] をクリックします。

[Redirect Set Settings] ダイアログボックスが表示されます（図 10-32）。

図 10-32　[Redirect Set Settings]



ステップ 3　[Add] をクリックします。

デフォルトのリダイレクション URL を含む新しいリダイレクション セットが追加されます。

ステップ 4　新しいリダイレクション セットの一意の名前を [Redirection Set Name] フィールドに入力します。

（注）　リダイレクション セットにはデフォルトの名前を使用できますが、わかりやすい名前の入力を推奨します。

ステップ 5　新しいリダイレクション セットの [Redirection destination URLs] セクションに新しい値を入力します。

ステップ 6　（オプション）応答コードを含めるには、[Response code] チェックボックスをオンにし、ドロップダウン リストから応答コードを選択します。リダイレクション パラメータのリストおよび説明については、表 10-2 を参照してください。

ステップ 7　（オプション）Cookie を含めるには、[Cookie] チェックボックスをオンにし、値を入力します。リダイレクション パラメータのリストおよび説明については、表 10-2 を参照してください。

ステップ 8　（オプション）宛先 URL に追加する任意のパラメータのチェックボックスをオンにします。リダイレクション パラメータのリストおよび説明については、表 10-2 を参照してください。

[Free text to append] チェックボックスをオンにする場合、URL に追加するテキストをテキスト ボックスに入力します。リダイレクション パラメータのリストおよび説明については、表 10-2 を参照してください。

（注） 宛先 URL には、「<」および「>」は表示されません。

パラメータを含む宛先 URL の最大長は、500 文字です。

[Cookie] パラメータおよび [Referer] パラメータを使用できるのは、HTTP トラフィックだけです。

表 10-2　リダイレクション パラメータ

パラメータ	説明
[Reason]	通知の場合：通知番号。 DDoS 攻撃の場合：DDoS 攻撃 ID。 リダイレクトの場合：無効です。
[Subscriber ID]	SCE に表示されるサブスクライバの名前。
[Service ID]	SCE によって分類されたサービスの ID。
[Distinct Number]	リダイレクトされたフローの固有識別情報。<redirected flow number:cpu number> の形式です。
[Time Stamp]	時間（秒単位）。Unix 形式です。
[Free text to append]	フリー テキスト。
[Referer]	元のフロー要求に表示される参照元。参照元パラメータが設定されていない場合、“” が表示されます。
[Original Cookie]	元のフロー要求に表示される cookie ストリング。cookie パラメータが設定されていない場合、“” が表示されます。
[Original Host]	元のフロー要求に表示されるホスト名。
[Original URL]	元のフロー要求に表示される URL。
[Original Parameters]	元のフロー要求に表示される URL パラメータ。URL パラメータが設定されていない場合、“” が表示されます。

ステップ 9　[OK] をクリックします。

設定が保存され、[Redirect Set Settings] ダイアログボックスが閉じます。

リダイレクション URL セットの削除

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [Subscriber Redirection] を選択します。

[Redirect Actions Settings] ダイアログボックスが表示されます。

ステップ 2　[General] タブで、[Edit] をクリックします。

[Redirect Set Settings] ダイアログボックスが表示されます。

ステップ 3　リダイレクション セットの名前をクリックします。

ステップ 4　[Remove] をクリックします。

ステップ 5　[OK] をクリックします。

[Redirect Set Settings] ダイアログボックスが閉じます。

リダイレクション設定が保存されます。

システム設定の管理

Console では、次を制御するさまざまなシステム パラメータを判別できます。

- システムの動作状態
- 非対称ルーティング分類モードのイネーブル化とディセーブル化
- 詳細サービス コンフィギュレーション オプション

システム モードの設定

Console では、次を選択できます。

- システムの動作モード
- 非対称ルーティング分類モード

システム モードについての情報

- 「システムの動作モード」（P.10-44）
- 「非対称ルーティング分類モード」（P.10-44）

システムの動作モード

システムの動作モードは、システムがネットワーク トラフィックを処理する方法を定義します。

（注） 各規則には独自の動作モード（状態）があります。これがシステム モードと異なる場合、2 つのモードのうち「下位」のモードが使用されます。たとえば、規則が有効で、システム モードが Report Only の場合、規則は RDR の生成だけを行います。

3 つの動作モードは次のとおりです。

- Full Functionality：システムはアクティブな規則をネットワーク トラフィックに適用し、レポート機能を実行します（つまり、RDR を生成します）。
- Report Only：システムは RDR の生成だけを行います。ネットワーク トラフィックには、アクティブな規則は適用されません。
- Transparent：システムは RDR を生成せず、ネットワーク トラフィックにアクティブな規則を適用しません。

非対称ルーティング分類モード

単一方向のフロー レートが高い環境に SCE プラットフォームが配置されている場合、単方向分類モードを有効にすると分類の精度を大幅に向上させることができます。

- 「サポートされない機能」（P.10-45）

サポートされない機能

単方向分類が有効になっている場合、SCA BB の次の機能が使用できません。

- フレーバ
- 外部クォータ プロビジョニング
- サブスクライバ通知
- リダイレクション
- Flow Signaling RDR
- コンテンツ フィルタリング
- VAS トラフィック フォワーディング

単方向分類が有効になっている場合、Service Configuration Editor には（[Problems View] に）サービス コンフィギュレーションとこのモードでサポートされる機能が一致するかどうかが表示されます。

次の機能はサービス コンフィギュレーションの一部ではありませんが、単方向分類が有効になっている場合に影響を受けます。

- サブスクライバアウェア モード（サブスクライバ情報が、現在サブスクライバが使用している IP アドレスに動的にバインドされるモード）は、サポートされていません。
- 拡張フロー オープン モードをイネーブルにする必要があります。

上記の機能の状態がルーティング分類モードの状態と一致するかどうかは表示されません。

プロトコル分類

単方向分類が有効になっている場合、プロトコル分類は単一方向の UDP フローを除いて通常の方法で実行されます。単一方向 UDP フローのサーバ側を知ることは不可能なので、SCA BB は先頭パケットの宛先ポートを使用してプロトコルを分類します。完全に一致するものが見つからなければ、送信元ポートを使用してプロトコルの分類を試みます。

非対称ルーティング分類モードへの切り替え

対称モードでサービス コンフィギュレーションを作成し、非対称ルーティング分類モードに切り替えると、次の状態になります。

- 分類にフレーバは使用されません。
- 定期的なクォータ管理モードが使用されます。
- 非対称ルーティング分類モードに切り替えてもデータは失われませんが、サポートされない機能をすべてサービス コンフィギュレーションから削除するまでは SCE プラットフォームにサービス コンフィギュレーションを適用できません。

非対称ルーティング分類モードからの切り替え

非対称ルーティング分類モードでサービス コンフィギュレーションを作成すると、次の状態になります。

- すべての異常ディテクタの不審セッション レートとセッション レートは同じに設定されます。
- デフォルト サービス コンフィギュレーションにフレーバは作成されず、サービス要素は指定されたフレーバを持ちません。
- クォータ管理モードは、集約時間が 1 日 1 回の定期モードになります。

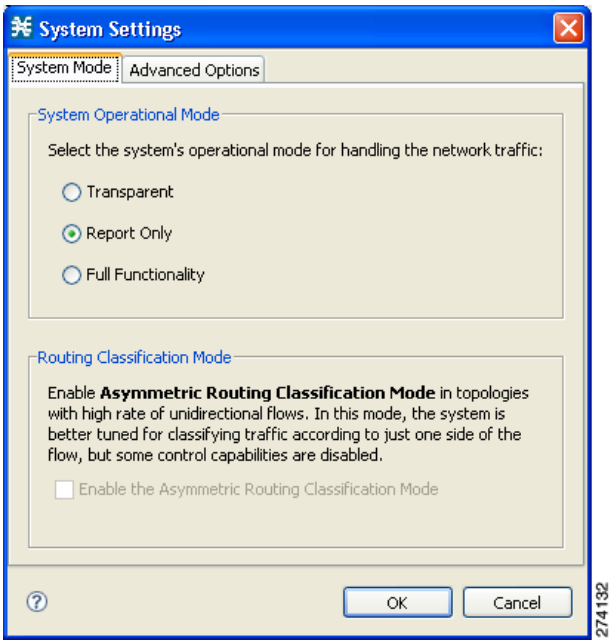
- 対称モードに切り替えても非対称ルーティング分類モードの制限は保持されます。制限を変更するには、サービス コンフィギュレーションを編集する必要があります。

システムの動作モードとトポロジ モードの設定

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [System Settings] を選択します。

[System Settings] ダイアログボックスが表示されます（図 10-33）。

図 10-33　[System Settings]



ステップ 2　次の [System Operational Mode] オプション ボタンのうち 1 つを選択します。

- [Transparent]
- [Report Only]
- [Full Functionality]

ステップ 3　ルーティング分類モードを変更するには、[Enable the Asymmetric Routing Classification Mode] チェックボックスをオンまたはオフにします。

ステップ 4　[OK] をクリックします。

[System Settings] ダイアログボックスが閉じます。

新しいシステム モード設定が保存されます。

詳細サービス コンフィギュレーション オプションの管理

詳細サービス コンフィギュレーション オプションでは、高度であまり変更しないシステム属性を制御します。このオプションは変更しないことを推奨します。

- 「詳細サービス コンフィギュレーション プロパティ」（P.10-47）
- 「詳細サービス コンフィギュレーション オプションの編集」（P.10-49）

詳細サービス コンフィギュレーション プロパティ

表 10-3 に詳細サービス コンフィギュレーション プロパティを示します。

表 10-3　詳細サービス コンフィギュレーション プロパティ

プロパティ	デフォルト値	説明
[Classification]		
[Guruguru detailed inspection mode enabled]	FALSE	Guruguru プロトコルは、日本で普及している Guruguru ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。 • Default：Guruguru トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。 • Detailed：Guruguru トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークだけで一般的です。
[Kuro detailed inspection mode enabled]	FALSE	Kuro プロトコルは、日本で普及している Kuro ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。 • Default：Kuro トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。 • Detailed：Kuro トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークだけで一般的です。
[Soribada detailed inspection mode enabled]	FALSE	Soribada プロトコルは、日本で普及している Soribada ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。 • Default：Soribada トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。 • Detailed：Soribada トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークだけで一般的です。
[TCP destination port signatures]	1720:H323	正しい分類にポート ヒントが必要であるシグニチャの TCP 宛先ポート番号。 有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。 適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、および DHCP です。
[UDP destination port signatures]	67:DHCP、68:DHCP、1812:Radius Access、1645:Radius Access、1813:Radius Accounting、1646:Radius Accounting	正しい分類にポート ヒントが必要であるシグニチャの UDP 宛先ポート番号。 有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。 適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、および DHCP です。

表 10-3　詳細サービス コンフィギュレーション プロパティ （続き）

プロパティ	デフォルト値	説明
[UDP ports for which flow should be opened on first packet]	5060、5061、67、68、69、1812、1813、1645、1646、2427、2727、9201、9200、123、1900、5190、10000	拡張フローオープン モードは指定 UDP ポートで無効になり、フローの先頭パケットに従った分類が可能になります。
[UDP source port signatures]	1812:Radius Access、1645:Radius Access、1813:Radius Accounting、1646:Radius Accounting	正しい分類にポート ヒントが必要であるシグニチャの UDP 送信元ポート番号。 有効な値は、カンマで区切った項目です。各項目は <port-number>:<signature-name> という形式にします。 適用可能なシグニチャ名は、H323、Radius Access、Radius Accounting、および DHCP です。
[V-Share detailed inspection mode enabled]	FALSE	V-Share プロトコルは、日本で普及している V-Share ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。 • Default：V-Share トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。 • Detailed：V-Share トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークだけで一般的です。
[Winny detailed inspection mode enabled]	FALSE	Winny P2P プロトコルは、日本で普及している Winny ファイル共有アプリケーションで使用されます。SCA BB では、このプロトコルの分類に、次の 2 つの検査モードが提供されます。 • Default：Winny トラフィックが少ないことが予想されるネットワークに適しています。日本以外のすべての国ではこれが一般的です。 • Detailed：Winny トラフィックが一般的になることが予想されるネットワークに適しています。日本のネットワークだけで一般的です。
[Malicious Traffic]		
[Malicious Traffic RDRs enabled]	TRUE	悪質トラフィック RDR を生成するかどうかを指定します。
[Number of seconds between Malicious Traffic RDRs on the same attack]	60	攻撃が検出されると、悪質トラフィック RDR が生成されます。悪質トラフィック RDR は、攻撃が続く間、ユーザが設定した間隔で定期的に生成されます。
[TCP port that should remain open for Subscriber Notification]	80	検出されたネットワーク攻撃の一部であるフローのブロックを選択できますが、これによって攻撃のサブスクライバ通知が妨害されることがあります。 指定 TCP ポートはブロックされず、攻撃通知をサブスクライバに送信できるようになります。
[Policy Check]		
[Ongoing policy check mode enabled]	TRUE	すでに開いているフローにポリシーの変更が影響するかどうかを指定します。

表 10-3　詳細サービス コンフィギュレーション プロパティ （続き）

プロパティ	デフォルト値	説明
[Time to bypass between policy checks]	30	すでに開いているフローにポリシーの変更が影響する前に経過する最長時間（秒単位）。
[Quota Management]		
[Grace period before first breach]	2	クォータ制限違反があったあと、違反処理を実行する前に待機する時間（秒単位）。 ポリシー サーバではこの時間を使用し、ログインしたサブスクライバにクォータをプロビジョニングします。
[Length of the time frame for quota replenish scatter (minutes)]	0	定期クォータ補充をランダムに分散する時間帯の長さ。
[Time to bypass between policy checks for quota limited flows]	30	すでに開いているフローにクォータ違反が影響する前に経過する最長時間（秒単位）。
[Volume to bypass between policy checks for quota limited flows]	0	すでに開いているフローにクォータ違反が影響する前に通過する最大フローボリューム（バイト単位）。 値をゼロにすると、ボリュームが無制限に通過します。
[Reporting]		
[Media Flow RDRs enabled]	TRUE	メディア フロー RDR を生成するかどうかを指定します。
[Subscriber Accounting RDR enabled]	FALSE	サブスクライバ課金 RDR を生成するかどうかを指定します。 サブスクライバ課金 RDR は、SM-ISG 統合に使用します。詳細については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Managing the SCMP」の章にある ISG 文書または『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Managing the SCMP」の章を参照してください。

詳細サービス コンフィギュレーション オプションの編集

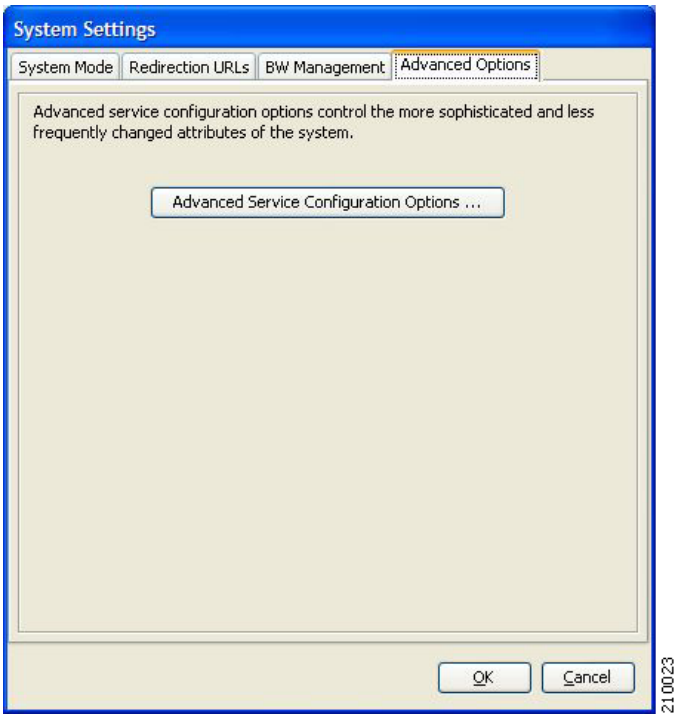
ステップ 1　左のペインの [Policies] タブで、[Configuration] > [System Settings] を選択します。

[System Settings] ダイアログボックスが表示されます。

ステップ 2　[Advanced Options] タブをクリックします。

[Advanced Options] タブが開きます（図 10-34）。

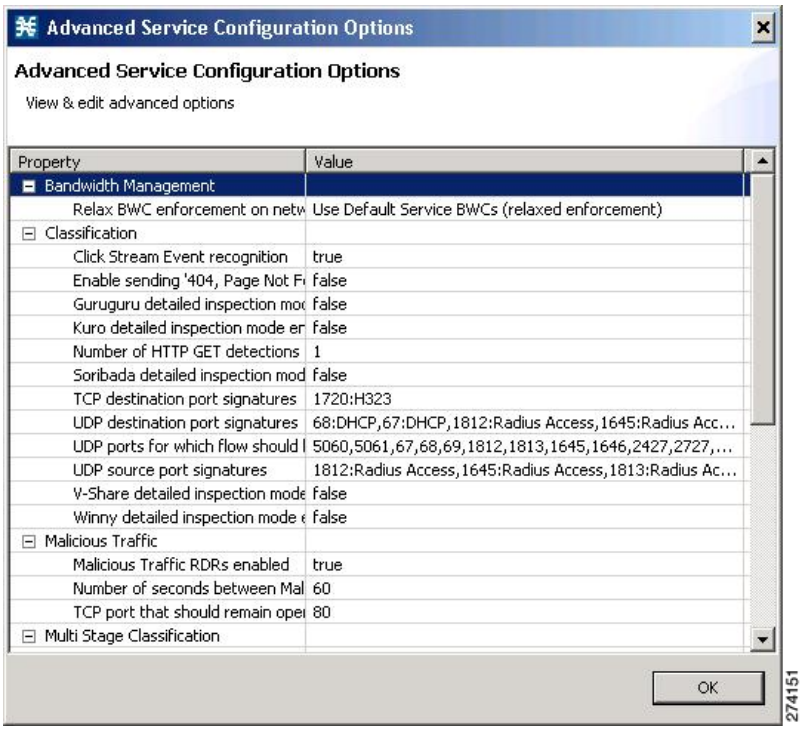
図 10-34　[Advanced Options] タブ



ステップ 3　[Advanced Service Configuration Options] をクリックします。

[Advanced Service Configuration Options] ダイアログボックスが開きます（図 10-35）。

図 10-35　[Advanced Service Configuration Options]



ステップ 4　設定オプションを変更します。

ステップ 5　[OK] をクリックします。

[Advanced Service Configuration Options] ダイアログボックスが閉じます。

詳細オプションの変更が保存されます。

ステップ 6　[OK] をクリックします。

[System Settings] ダイアログボックスが閉じます。

VAS 設定の管理

Value Added Service（VAS）設定には、次の機能が含まれます。

- トラフィック ミラーリング：トラフィック ミラーリングでは、SCE を使用してそのアプリケーションおよびサブスクライバ アウェアネスに基づいてトラフィックの一部をミラーリングできます。ミラーリング対象のトラフィックはそのままフォワーディングされ、パケットの複製は、対応する VAS の VLAN に送信されます。つまり、トラフィックは、最小化されます。
- トラフィック フォワーディング：トラフィック フォワーディング サーバでは、外部エキスパート システム（VAS サーバ）を使って侵入検知やサブスクライバのコンテンツ フィルタリングなどのトラフィック処理を追加できます。フローは処理後に SCE プラットフォームに送り返され、SCE プラットフォームはフローを元の宛先に送信します。

  フォワーディングされるフローは、サブスクライバ パッケージおよびフロー タイプ（IP プロトコル タイプおよび宛先ポート番号）に基づいて選択されます。

VAS ミラーリングには、次の制限があります。

- SCE 2000 および SCE8000 は、いずれもトラフィック ミラーリングをサポートします。
- トラフィック ミラーリングは、少なくとも 2 つのポートを備える任意の SCE プラットフォームでサポートされます。
- SCE8000 は、64 の VLAN を備えることができます。
- SCE 2000 は、8 の VLAN を備えることができます。

VAS フォワーディングには、次の制限があります。

- SCE 2000 4xGBE プラットフォームだけが VAS トラフィック フォワーディングをサポートします。
- 1 つの SCE プラットフォームでは、最大 8 の VAS サーバをサポートできます。
- サービス コンフィギュレーションには、最大 64 のトラフィックフォワーディング テーブルを含めることができます。
- トラフィックフォワーディング テーブルには、最大 64 のテーブル パラメータを含めることができます。
- 単方向分類が有効になっている場合、VAS トラフィック フォワーディングはサポートされません。

（注）　VAS 設定機能は複雑なので、VAS フローはグローバル帯域幅制御に影響されません。

VAS トラフィックフォワーディングを使用するには、SCE プラットフォームで VAS サービスを設定する必要もあります。詳細については、『*Cisco SCE2000 and SCE1000 Software Configuration Guide*』の「Value Added Services (VAS) Traffic Forwarding」の章を参照してください。

- 「VAS トラフィック フォワーディングの有効化」（P.10-53）
- 「VAS サーバ グループの名前変更」（P.10-54）
- 「VAS トラフィックフォワーディング テーブルの表示」（P.10-56）
- 「VAS トラフィックフォワーディング テーブルの削除」（P.10-57）
- 「VAS トラフィックフォワーディング テーブルの追加」（P.10-58）
- 「VAS テーブル パラメータの管理」（P.10-59）

VAS トラフィック フォワーディングの有効化

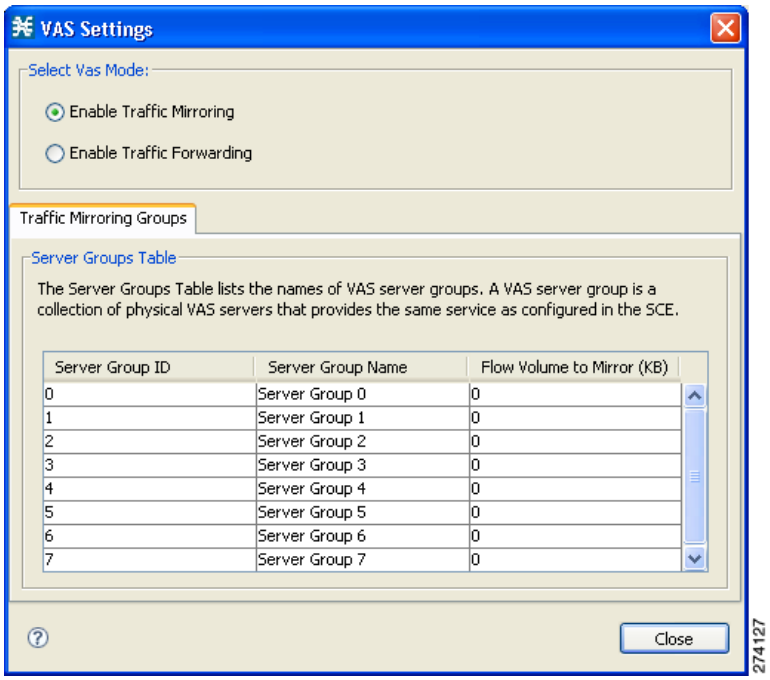
デフォルトの場合、VAS トラフィック フォワーディングは無効になっています。VAS トラフィック フォワーディングはいつでも有効にすることができます。

（注）　単方向分類が有効になっている場合、VAS トラフィック フォワーディングはサポートされません。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます（図 10-36）。

図 10-36　[VAS Settings]



ステップ 2　[Enable Traffic Forwarding] オプション ボタンをオンにします。

（注）　VAS トラフィック フォワーディングは、非対称ルーティング分類モードではサポートされません。非対称ルーティング分類モードが有効のときに [Enable Traffic Forwarding] オプション ボタンをオンにしようとした場合は、VAS のエラー メッセージが表示されます。

[OK] をクリックし、ステップ 4 に進みます。

VAS の警告メッセージが表示されます。

ステップ 3　[OK] をクリックします。

ステップ 4　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS トラフィック ミラーリングの有効化

トラフィック ミラーリングは、[VAS Setting] ダイアログボックスで有効化と設定を行います。しかし、使用するサーバ グループは、規則を定義するときに設定します。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Mirroring] オプション ボタンをオンにします。

VAS の警告メッセージが表示されます。

ステップ 3　[OK] をクリックします。

ステップ 4　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS サーバ グループの名前変更

SCE プラットフォームでは、最大 8 個の VAS サーバ グループにフローを転送できます。デフォルトでは、この 8 個のサーバ グループは「Server Group n」という名前です（n は、0 ～ 7 の値）。サーバ グループにわかりやすい名前を指定すると、指定した名前が [Add Rule to Package] ダイアログボックスの [Control and Breach Handling] タブのドロップダウン リスト（「高度なパッケージ オプションの設定」（P.9-52）を参照）と各トラフィックフォワーディング テーブルに追加されたテーブル パラメータの [Server Group] フィールド（「VAS テーブル パラメータの管理」（P.10-59）を参照）に表示されます。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

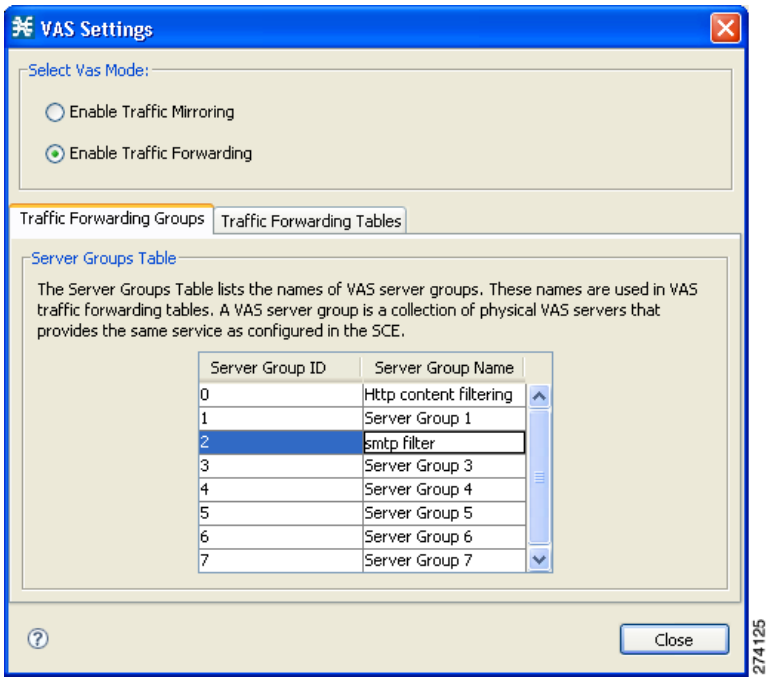
[VAS Settings] ダイアログボックスが表示されます（図 10-37）。

ステップ 2　[Server Groups Table] 領域のテーブルで、サーバ グループ名を含むセルをダブルクリックします。

ステップ 3　わかりやすい名前をセルに入力します。

ステップ 4　名前を変更する他のサーバ グループについてもステップ 2 およびステップ 3 を繰り返します。

図 10-37　[Traffic Forwarding Groups] タブ



ステップ 5　[Close] をクリックします。

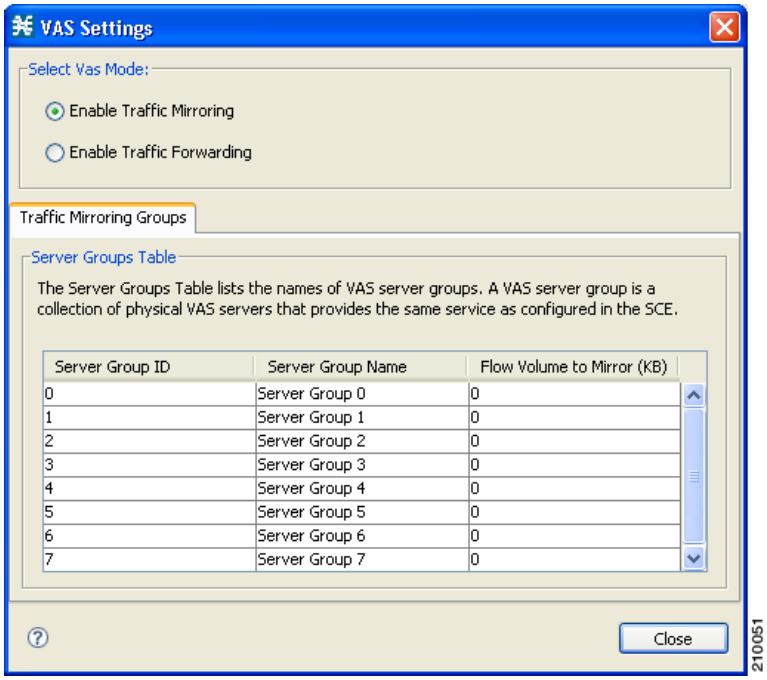
[VAS Settings] ダイアログボックスが閉じます。

VAS トラフィック ミラーリングの有効化

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます（図 10-38）。

図 10-38　[Traffic Mirroring Groups] タブ



ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　各サーバ グループについて、[Flow Volume to Mirror (KB)] カラムにミラーリングの最大量（KB 単位）を入力します。

ステップ 4　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS トラフィックフォワーディング テーブルの表示

SCA BB は、SCE プラットフォームを通過するフローを VAS サーバ グループに転送するかどうかをトラフィックフォワーディング テーブルに基づいて判断します。トラフィックフォワーディング テーブルの各エントリ（テーブル パラメータ）では、特定フローをどの VAS サーバ グループに転送するかが定義されます。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

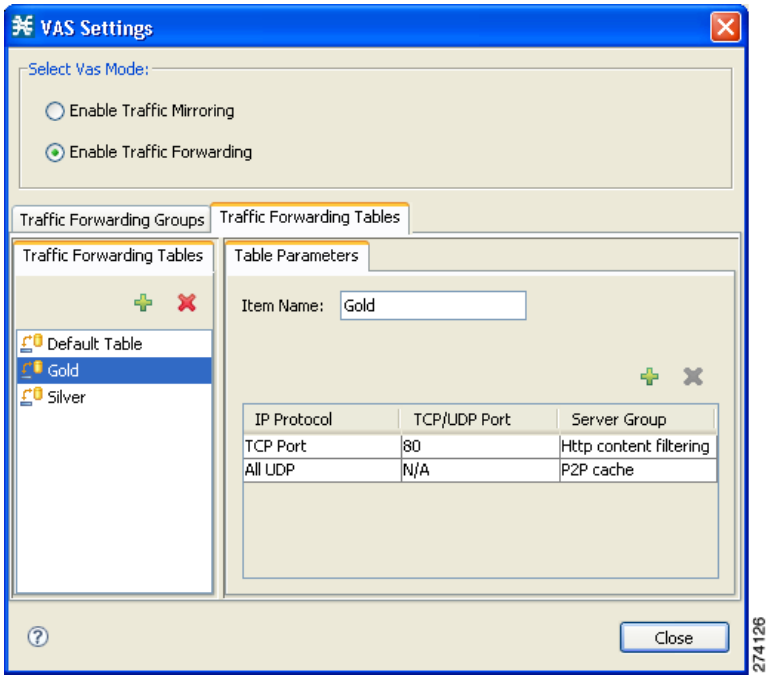
[Traffic Forwarding Tables] タブが開きます。

すべてのトラフィックフォワーディング テーブルのリストが、[Traffic Forwarding Tables] 領域に表示されます。

ステップ 4　トラフィックフォワーディング テーブルのリストのテーブルをクリックし、テーブル パラメータを表示します。

トラフィックフォワーディング テーブルに定義されているすべてのテーブル パラメータのリストが、[Table Parameters] タブに表示されます（図 10-39）。

図 10-39　[Traffic Forwarding Tables] タブ



ステップ 5　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS トラフィックフォワーディング テーブルの削除

ユーザが作成したすべてのトラフィックフォワーディング テーブルを削除できます。デフォルト トラフィックフォワーディング テーブルを削除することはできません。

（注）　パッケージに関連しているトラフィックフォワーディング テーブルを削除することはできません。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

[Traffic Forwarding Tables] タブが開きます。

ステップ 4　[Traffic Forwarding Tables] 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

ステップ 5　（[Delete]）をクリックします。

[VAS Warning] メッセージが表示されます（図 10-40）。

図 10-40　[VAS Warning]

ステップ 6　[Yes] をクリックします。

選択したテーブルが削除され、トラフィックフォワーディング テーブルのリストに表示されなくなります。

ステップ 7　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS トラフィックフォワーディング テーブルの追加

サービス コンフィギュレーションにはデフォルト トラフィックフォワーディング テーブルが組み込まれています。最大 63 のトラフィックフォワーディング テーブルをさらに追加し、さまざまなトラフィックフォワーディング テーブルを別々のパッケージに割り当てることができます。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

[Traffic Forwarding Tables] タブが開きます。

ステップ 4　[Traffic Forwarding Tables] 領域で （[Add]）をクリックします。

「Table (n)」（*n* は 1 ～ 63 の値）という名前の新しいテーブルが、[Traffic Forwarding Tables] 領域のトラフィックフォワーディング テーブルのリストに追加されます。

テーブル名は、[Table Parameters] タブの [Item Name] ボックスにも表示されます。

ステップ 5　トラフィックフォワーディング テーブルの一意でわかりやすい名前を [Item Name] フィールドに入力します。

新しいトラフィックフォワーディング テーブルにはテーブル パラメータを追加できます（「VAS テーブル パラメータの追加」（P.10-59）を参照）。

VAS テーブル パラメータの管理

テーブル パラメータは、IP プロトコル タイプ、関連 TCP/UDP ポート（該当する場合）、VAS サーバ グループまたは IP アドレスの範囲です。

トラフィックフォワーディング テーブルは関連テーブル パラメータの集合です。

トラフィックフォワーディング テーブルには、最大 64 のテーブル パラメータを含めることができます。

- 「VAS テーブル パラメータの追加」（P.10-59）
- 「VAS テーブル パラメータの編集」（P.10-60）
- 「VAS テーブル パラメータの削除」（P.10-61）

VAS テーブル パラメータの追加

最大 64 のテーブル パラメータをトラフィックフォワーディング テーブルに追加できます。

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

[Traffic Forwarding Tables] タブが開きます。

ステップ 4　[Traffic Forwarding Tables] 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

ステップ 5　[Traffic Parameters] タブで、  （[Add]）をクリックします。

[Table Parameters] タブのテーブル パラメータのリストに、新しいテーブル パラメータが追加されます。

（注）　それぞれの新しいテーブル パラメータには、表 10-4 に示されるデフォルト値が含まれます。

表 10-4　テーブル パラメータのデフォルト値

パラメータ	デフォルト値
[IP Protocol]	TCP Port
[TCP/UDP Port]	80
[Server Group]	Server Group 0

次のセクションで説明するように、新しいテーブル パラメータをここで編集できます。

ステップ 6　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS テーブル パラメータの編集

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

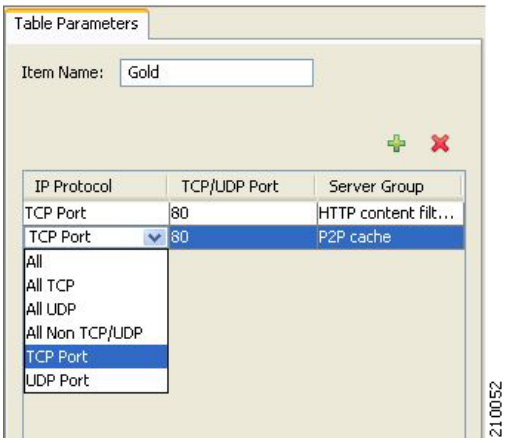
[Traffic Forwarding Tables] タブが開きます。

ステップ 4　[Traffic Forwarding Tables] 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

ステップ 5　[Table Parameters] タブのテーブルで、プロトコル、ポート、およびサーバ グループを選択します。

a. [IP Protocol] カラムのセルをクリックし、表示されるドロップダウン リストから IP プロトコル タイプを選択します（図 10-41）。

図 10-41　[Table Parameters] タブ



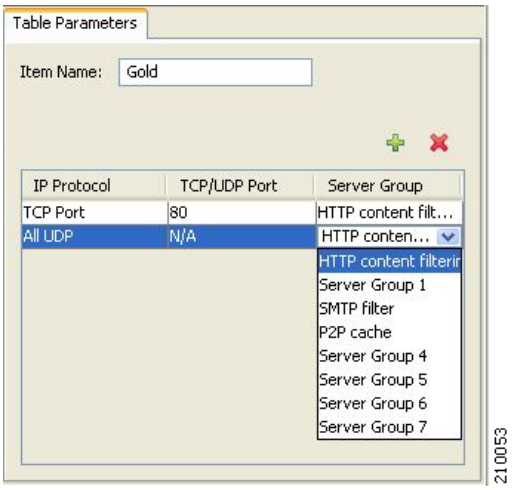
[All]、[All TCP]、[All UDP]、[All Non TCP/UDP] のうちいずれかを選択した場合は、テーブルの別のセルに移動すると、TCP/UDP Port セルに「N/A」と表示されます。

b. [TCP Port] または [UDP Port] を選択した場合は、[TCP/UDP Port] カラムのセルをダブルクリックし、ポート番号を入力します。

（注）　ポートの範囲を [TCP/UDP Port] セルに入力することはできません。ポートごとに別のテーブル パラメータを追加する必要があります。

c. [Server Group] カラムのセルをクリックし、表示されるドロップダウン リストからサーバ グループを選択します（図 10-42）。

図 10-42　[Tables Parameters] タブ



ステップ 6　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

VAS テーブル パラメータの削除

ステップ 1　左のペインの [Policies] タブで、[Configuration] > [VAS Settings] を選択します。

[VAS Settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Traffic Forwarding] オプション ボタンをクリックします。

ステップ 3　[Traffic Forwarding Tables] タブをクリックします。

[Traffic Forwarding Tables] タブが開きます。

ステップ 4　[Traffic Forwarding Tables] 領域のトラフィックフォワーディング テーブルのリストからテーブルを選択します。

ステップ 5　[Table Parameters] タブのテーブル パラメータのリストからテーブル パラメータを選択します。

ステップ 6　（[Delete]）をクリックします。

選択したテーブル パラメータが削除され、テーブル パラメータのリストに表示されなくなります。

ステップ 7　[Close] をクリックします。

[VAS Settings] ダイアログボックスが閉じます。

保護 URL データベースの管理

SCE 保護 URL データベースとは、「ブラックリスト」（立ち入り禁止、つまり危険と見なされる Web サイトのリスト）が含まれるデータベースです。サブスクライバがブラックリストに記載されているサイトへのアクセスを試みると、SCE が特定の処理（サイトをブロックするなど）を適用するように設定できます。

データベースは暗号化されているので、オペレータを含む誰もがブラックリストを表示することはできません。ブラックリストは SCE で管理され、管理 PC に引き出すことはできません。

ブラックリストに含まれるリンクにサブスクライバがアクセスしようとすると、RDR が作成されます。しかし、RDR には、サイトの URL またはホスト情報は含まれません。

ブラックリスト機能を有効にするためには、次の手順を実行します。

- HTTP フレーバを定義します。
- ブラックリスト サービスを作成します。
- HTTP フレーバをブラックリスト サービスに割り当てます。
- ブラックリスト サービスの規則を作成します。
- CLI を使用して、ブラックリストのエントリをフレーバに割り当てます。

保護 URL データベースの詳細については、『*Cisco Service Control URL Blacklisting Solution Guide*』を参照してください。

CHAPTER 11

Subscriber Manager の GUI ツールの使用方法

はじめに

この章では、Subscriber Manager（SM）の GUI ツールを使用して、Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）データベースでサブスクライバを設定する方法について説明します。

SM GUI ツールは、SCMS-SM がサブスクライバのスタティック リストを維持している場合、特に便利です。Cisco Service Control Application for Broadband（SCA BB）がサブスクライバレス モード（グローバル プラットフォームを解決するときだけ制御および分析モードを使用できるモード）またはアノニマス サブスクライバ モード（IP アドレスまたは Virtual LAN（VLAN; 仮想 LAN）として定義されるエンティティがサブスクライバとして処理されるモード）で動作する場合には該当しません。

SM GUI ツールの使用

SM GUI ツールでは、SCMS-SM でサブスクライバを管理できます。SCMS-SM は、Operational Support System（OSS; オペレーション サポート システム）プラットフォームと Service Control Engine（SCE）プラットフォームの間を橋渡しするミドルウェア ソフトウェアとして機能します。SCE プラットフォームはサブスクライバ情報を使用して、サブスクライバアウェア機能、サブスクライバ単位のレポート作成、およびポリシー適用を行います。サブスクライバ情報は SCMS-SM データベースに格納され、実際のサブスクライバ配置に従って、複数のプラットフォーム間で配信できます。

SM GUI ツールを使用してサブスクライバ ファイルのインポートとエクスポートを行ったり、新しいサブスクライバの追加、既存サブスクライバのパラメータの編集、サブスクライバの削除というような各サブスクライバの操作を行ったりすることができます。

（注） SM GUI ツールから SCMS-SM にアクセスするには、Network Navigator ツールの [Site Manager] ツリーに SCMS-SM を追加する必要があります（「サイトへの SM デバイスの追加方法」（P.5-4）を参照）。

SM GUI ツールでは、SM コマンドライン ユーティリティが提供する機能の一部しか提供されません。SCMS-SM の詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

SCMS-SM への接続

SCMS-SM には次のように接続できます。

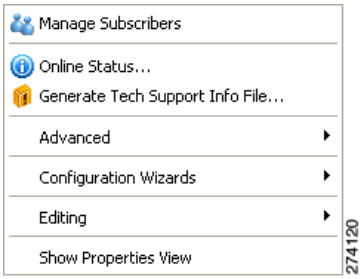
- Network Navigator ツールから
- Console のあらゆる場所から
- Subscriber Manager の GUI ツールから

（注）　SM GUI ツールは、ポート 14374 への PRPC 接続を開き、[Password Management] ダイアログボックスに入力されたユーザ名とパスワードを使用してログインを試行することで、SCMS-SM での認証を実行します。このユーザを含む PRPC サーバが SCMS-SM で動作していない場合、認証はエラーになります。
SCMS-SM で PRPC ポートを変更した場合は、「ユーザ認証」（P.5-36）を参照してください。

Network Navigator から SCMS-SM への接続

ステップ 1　[Network Navigator] タブの [Site Manager] ツリーで SM デバイスを右クリックします。
ポップアップ メニューが表示されます（図 11-1）。

図 11-1　SM デバイス ポップアップ メニュー



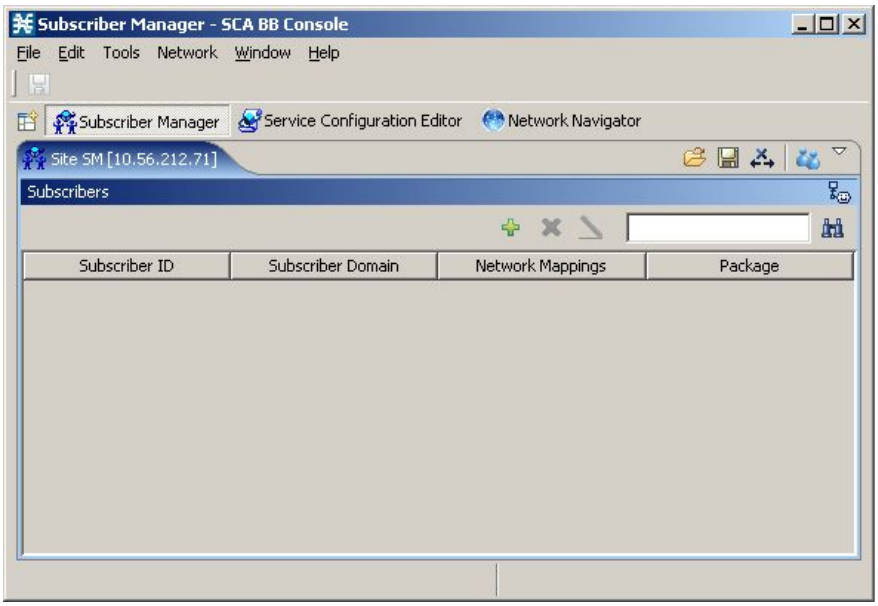
ステップ 2　メニューから [Manage Subscribers] を選択します。
[Password Management] ダイアログボックスが表示されます。

ステップ 3　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 4　[Connecting] をクリックします。
[Password Management] ダイアログボックスが閉じます。
接続の経過表示バーが表示されます。
システムが SCMS-SM に接続します。

（[Import subscribers from CSV file]）、  （[Export subscribers to CSV file]）、および  （[Disconnect from SM]）が有効になります（図 11-2）。

図 11-2　Subscriber Manager



Console から SCMS-SM への接続

（注）　（SM GUI ツールがすでに表示されている場合は、ステップ 3 から始めます）

ステップ 1　Console のメイン メニューで、[Tools] > [Subscriber Manager] の順に選択します。

SM GUI ツールが開きます。

Subscriber Manager が接続されていないというメッセージが表示されます（図 11-3）。

図 11-3　Subscriber Manager が接続されていないというメッセージ

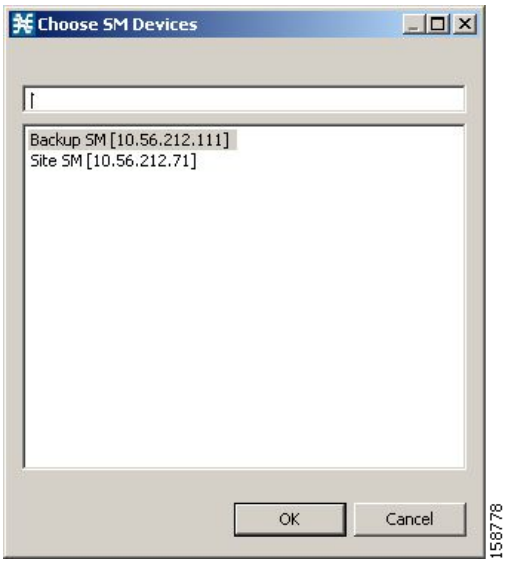
ステップ 2　[OK] をクリックします。

Subscriber Manager が接続されていないというメッセージが閉じます。

ステップ 3　SM GUI ツールバーで （[Connect to an SM]）をクリックします。

複数の SCMS-SM デバイスを Network Navigator で設定している場合は、[Choose SM Devices] ダイアログボックスが表示されます（図 11-4）。

図 11-4　[Choose SM Devices]



ステップ 4　デバイスを選択して [OK] をクリックします。

[Password Management] ダイアログボックスが表示されます。

ステップ 5　適切なパスワードを入力します（詳細については、「パスワード管理」（P.5-7）を参照してください）。

ステップ 6　[Connecting] をクリックします。

[Password Management] ダイアログボックスが閉じます。

接続の経過表示バーが表示されます。

システムが SCMS-SM に接続します。


（[Import subscribers from CSV file]）、  （[Export subscribers to CSV file]）、および  （[Disconnect from SM]）が有効になります。

現在の SCMS-SM からの切断

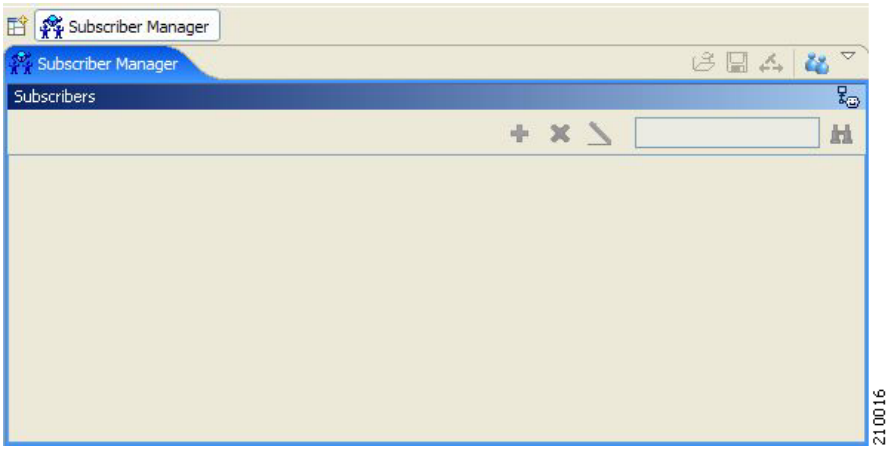
ステップ 1　SM GUI ツールバーで  （[Disconnect from SM]）をクリックします。

Console が SCMS-SM から切断しますが、SM GUI ツールは開いたまま残ります。


（[Import subscribers from CSV file]）、  （[Export subscribers to CSV file]）、および  （[Disconnect from SM]）が無効になります。

サブスクライバ リストは空になります（図 11-5）。

図 11-5　Subscriber Manager リスト



サブスクライバ CSV ファイルの処理

システムに導入する必要があるサブスクライバ数が多いため、サブスクライバ情報を手動で入力するのは適切でありません。通常は、RADIUS サーバや同様な送信元でサブスクライバ情報を生成してから、SM GUI ツールにインポートします。

更新したサブスクライバ情報を CSV ファイルにエクスポートすることもできます。

サブスクライバ CSV ファイルの形式については、『*Cisco Service Control Application for Broadband Reference Guide*』の「CSV File Formats」の章を参照してください。

- 「CSV ファイルからのサブスクライバ情報のインポート」（P.11-5）
- 「CSV ファイルへのサブスクライバ情報のエクスポート」（P.11-6）

CSV ファイルからのサブスクライバ情報のインポート

CSV ファイルにエクスポートされたサブスクライバ データを SM GUI ツールにインポートできます。

ステップ 1　SM GUI ツールバーの  （[Import subscribers from CSV file]）をクリックします。

[Import from File] ダイアログボックスが表示されます。

ステップ 2　インポートするファイルを選択し、[Open] をクリックします。

[Import Warning] メッセージが表示されます（図 11-6）。

図 11-6　[Import Warning]

ステップ 3　[Yes] をクリックします。

[Import from File] ダイアログボックスが閉じます。

選択したファイルが SM GUI ツールにインポートされ、インポートされたサブスクライバがサブスクライバ リストにリスト表示されます。

CSV ファイルへのサブスクライバ情報のエクスポート

サブスクライバ情報を CSV ファイルにエクスポートできます（たとえば SCMS-SM データベースのデータを更新した場合など）。

ステップ 1　データを保存するサブスクライバを選択します（「サブスクライバの選択」（P.11-8）を参照）。

ステップ 2　SM ツールバーの  （[Export subscribers to CSV file]）をクリックします。

[Export to File] ダイアログボックスが表示されます。

ステップ 3　エクスポート ファイルを保存するフォルダを選択します。

ステップ 4　[File name] フィールドにファイル名を入力します。

ステップ 5　[Save] をクリックします。

[Export to File] ダイアログボックスが閉じます。

選択したサブスクライバが CSV ファイルに保存されます。

サブスクライバの管理

サブスクライバをシステムにインポートしたら、データベースの保守および更新を行うことができます。

次の操作を実行できます。

- サブスクライバの追加
- 既存サブスクライバの情報の編集
- サブスクライバの削除

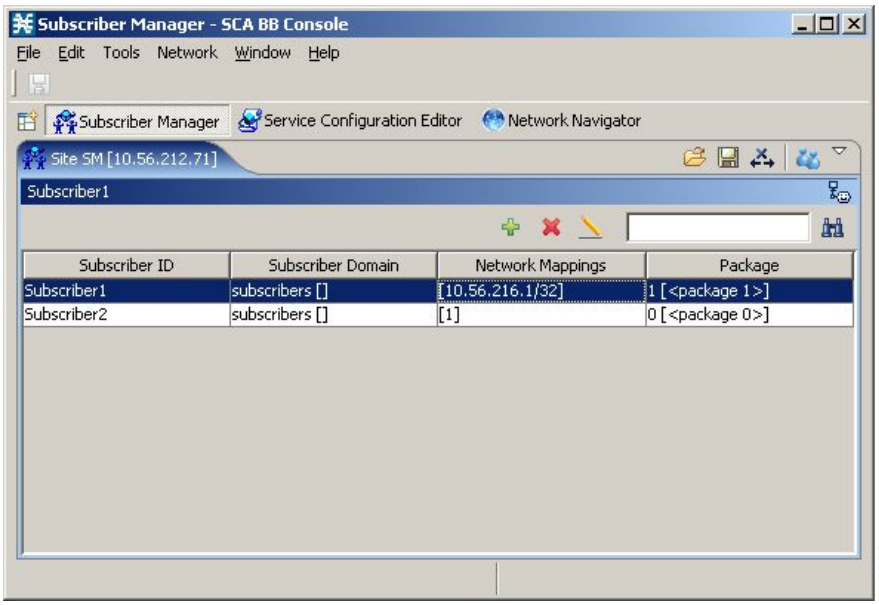
サブスクライバ情報

SCA BB に現在導入されているすべてのサブスクライバは、SM GUI ツールのリストに表示されます（図 11-7 を参照）。それぞれのサブスクライバまたはサブスクライバのグループを管理するには、このリストを使用します。サブスクライバのサブセットを表示するには検索機能を使用します（「サブスクライバまたはサブスクライバ グループの検索」（P.11-8）を参照）。

サブスクライバ リストには次のカラムがあります。

- [Subscriber ID]：システムにおけるサブスクライバの名前。
- [Subscriber Domain]：サブスクライバに割り当てられているドメイン。各ドメインに属する SCE プラットフォームの名前は角カッコ内に表示されます。
- [Network Mappings]：サブスクライバにマッピングされた IP アドレス、IP アドレス範囲、または VLAN タグ。
- [Package]：サブスクライバに割り当てられたパッケージ ID。パッケージの名前は角カッコ内に表示されます。

図 11-7　　Subscriber Manager：サブスクライバ リスト



サブスクライバの検索および選択

使いやすいように、SM GUI ツールには次の 2 つの標準機能が組み込まれています。

- 検索：特定のサブスクライバを検索します。
- 多重選択：サブスクライバの範囲または複数のサブスクライバを選択します。

サブスクライバまたはサブスクライバ グループの検索

この機能は、サブスクライバ ID プレフィクスに従って特定のサブスクライバまたはサブスクライバ グループを検索する場合に使用します。特定サブスクライバまたはサブスクライバのグループのパラメータを修正する場合に便利です（「サブスクライバの詳細編集」（P.11-11）を参照）。

ステップ 1　照合するプレフィクスを [Find] フィールド（図 11-8）に入力します。

図 11-8　[Find] フィールド

ステップ 2　  （[Find Subscribers]）をクリックします。

指定したプレフィクスと一致するサブスクライバだけが、サブスクライバ リストに表示されます。

サブスクライバの選択

サブスクライバ リストに表示されているサブスクライバを選択し、サブスクライバのグループを同時に編集、エクスポート、削除できます。選択できるサブスクライバ グループは、次のいずれかです。

- 連続する一連のサブスクライバ
- 連続しない一連のサブスクライバ
- 「サブスクライバ範囲の選択」（P.11-8）
- 「連続しない複数のサブスクライバの選択」（P.11-8）

サブスクライバ範囲の選択

ステップ 1　範囲の先頭のサブスクライバを選択します。

ステップ 2　**Shift** キーを押した状態で、範囲の最後のサブスクライバをクリックします。

範囲内のすべてのサブスクライバが選択されます。

この機能を検索機能と組み合わせて、特定サブスクライバを検索して表示してから、範囲全体を選択できます。

連続しない複数のサブスクライバの選択

ステップ 1　**Ctrl** キーを押した状態でサブスクライバを選択します。

一連のサブスクライバを選択する機能とこの機能を組み合わせて、一連のサブスクライバを選択してから別のサブスクライバを選択できます。

サブスクライバの追加

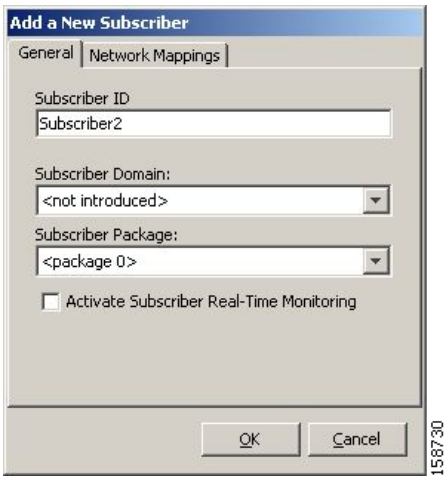
それぞれのサブスクライバを SCMS-SM に追加できます。

多数のサブスクライバを追加するには、RADIUS（または Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル））サーバから CSV ファイルに情報をエクスポートしたあと、その CSV ファイルをインポートします（「サブスクライバ CSV ファイルの処理」（P.11-5）を参照）。

ステップ 1　SM ツールバーの  （[Add Subscriber]）をクリックします。

[Add A New Subscriber] ダイアログボックスが表示されます（図 11-9）。

図 11-9　[Add a New Subscriber]



ステップ 2　サブスクライバを識別するテキストを [Subscriber ID] フィールドに入力します。

ステップ 3　新しいサブスクライバに適したドメインを [Subscriber Domain] ドロップダウン リストから選択します。

ステップ 4　[Subscriber Package] ドロップダウン リストで、このサブスクライバに割り当てるパッケージを選択します。

リストの内容は、選択したサブスクライバ ドメインによって決まります。

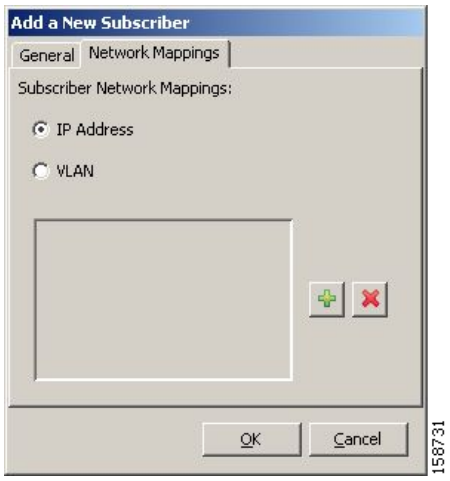
ステップ 5　サブスクライバのリアルタイム モニタを有効にするには、[Activate Subscriber Real-time Monitoring] チェックボックスをオンにします。SCE アプリケーションは、このサブスクライバの Real-Time Subscriber Usage RDR を生成します。

このサブスクライバのネットワーク マッピングを定義しない場合は、ステップ 11 に進みます。

ステップ 6　[Network Mappings] タブをクリックします。

[Network Mappings] タブが開きます（図 11-10）。

図 11-10　[Network Mappings] タブ



サブスクライバのネットワーク ID として、IP アドレスまたは VLAN タグがサポートされています。

ステップ 7　[Subscriber Network Mappings] オプション ボタンのうちいずれかを選択します。

- [IP Address]
- [VLAN]

ステップ 8　前のステップで選択したタイプのネットワーク マッピングを追加するには、 ([Add]) をクリックします。

新しいネットワーク マッピング エントリがサブスクライバ ネットワーク マッピング リストに追加され、デフォルト値が表示されます（図 11-11）。

ステップ 9　ネットワーク マッピング エントリを編集します。

図 11-11　ネットワーク マッピングのデフォルト値

ステップ 10　その他のネットワーク マッピングについて、ステップ 8 および 9 を繰り返します。

ステップ 11　[OK] をクリックします。

[Add A New Subscriber] ダイアログボックスが閉じます。

新しいサブスクライバが、データベース、および SM GUI ツールに表示されるサブスクライバ リストに追加されます。

サブスクライバの詳細編集

単一サブスクライバまたは複数サブスクライバを編集できます。

- 「単一サブスクライバの詳細編集」（P.11-11）
- 「サブスクライバ グループの詳細編集」（P.11-12）

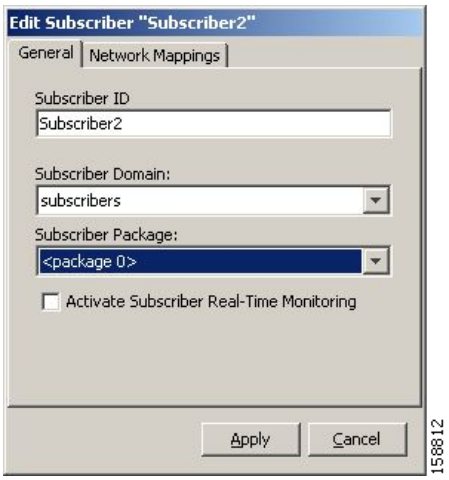
単一サブスクライバの詳細編集

ステップ 1　サブスクライバを検索し、選択します（「サブスクライバまたはサブスクライバ グループの検索」（P.11-8）を参照）。

ステップ 2　SM ツールバーの  （[Edit Subscriber]）をクリックします。

[Edit Subscriber] ダイアログボックスが表示されます（図 11-12）。

図 11-12　[Edit Subscriber]



ステップ 3　サブスクライバの詳細を次のように修正します。

- [Subscriber ID] フィールドのエントリを編集します。
- [Subscriber Domain] ドロップダウン リストで、サブスクライバ ドメインを選択します。
- [Subscriber Package] ドロップダウン リストで、このサブスクライバに割り当てるパッケージを選択します。

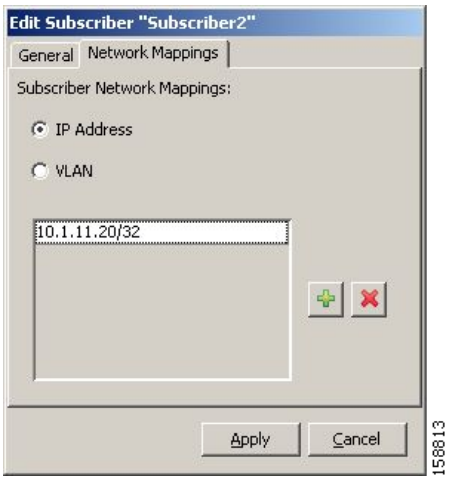
  リストの内容は、選択したサブスクライバ ドメインによって決まります。
- [Activate Subscriber Real-time Monitoring] チェックボックスをオンまたはオフにします。

このサブスクライバのネットワーク マッピングを編集しない場合は、ステップ 6 に進みます。

ステップ 4　[Network Mappings] タブをクリックします。

[Network Mappings] タブが開きます（図 11-13）。

図 11-13　[Network Mappings] タブ



ステップ 5　サブスクライバのネットワーク マッピングを次のように修正します。

a. [Subscriber Network Mappings] オプション ボタンのうちいずれかを選択します。

- [IP Address]
- [VLAN]

b. 新しいネットワーク マッピングをリストに追加するには、([Add]）をクリックし、[Subscriber Network Mappings] リストに追加するネットワーク マッピングのフィールドを編集します。

c. ネットワーク マッピングをリストから削除するには、サブスクライバのネットワーク マッピングのリストからエントリを選択して ([Delete]）をクリックします。

ステップ 6　[Apply] をクリックします。

[Edit Subscriber] ダイアログボックスが閉じます。

修正したサブスクライバ情報がデータベースに保存され、SM GUI ツールのサブスクライバ リストに表示されます。

サブスクライバ グループの詳細編集

同一パッケージまたはドメインを多くのサブスクライバに同時に割り当てることができます。

ステップ 1　修正するサブスクライバのグループを選択します（「サブスクライバの選択」（P.11-8）を参照）。

ステップ 2　SM ツールバーの ([Edit]）をクリックします。

[Edit Multiple Subscribers] ダイアログボックスが表示されます（図 11-14）。

図 11-14　[Edit Multiple Subscribers]

[Subscriber ID] フィールドおよび [Network Mappings] タブは使用できません。

ステップ 3　[General] タブのフィールドを修正します。

- [Subscriber Domain] ドロップダウン リストで、サブスクライバ ドメインを選択します。
- [Subscriber Package] ドロップダウン リストで、このサブスクライバに割り当てるパッケージを選択します。

  リストの内容は、選択したサブスクライバ ドメインによって決まります。
- [Activate Subscriber Real-time Monitoring] チェックボックスをオンまたはオフにします。

ステップ 4　[Apply] をクリックします。

[Edit multiple Subscribers] ダイアログボックスが閉じます。

修正したサブスクライバ情報がデータベースに保存され、SM GUI ツールのサブスクライバ リストに表示されます。

データベースからのサブスクライバの削除

サブスクライバは、データベースから削除できます。

ステップ 1　単一サブスクライバまたはサブスクライバのグループを選択します（「サブスクライバの選択」（P.11-8）を参照）。

ステップ 2　SM ツールバーの  （[Delete Subscriber]）をクリックします。

選択したサブスクライバを削除する前に、システムから確認を求められます（図 11-15）。

図 11-15　[Subscriber Warning]

ステップ 3　[Yes] をクリックして確認します。

選択したサブスクライバがデータベースから削除され、SM GUI ツールに表示されるサブスクライバリストから削除されます。

CHAPTER 12

Signature Editor の使用方法

はじめに

ここでは、Signature Editor ツールおよびこれを使用した Dynamic Signature Script（DSS）ファイルの作成と修正方法について説明します。

Signature Editor ツールでは、Cisco Service Control Application for Broadband（SCA BB）でまだサポートされていない新しいネットワーク プロトコルの知識に基づいて、SCA BB でプロトコルおよびプロトコル シグニチャの追加および修正ができる DSS ファイルの作成および修正ができます。

Signature Editor Console

Signature Editor は、適切な場合にログおよびエラー メッセージを Signature Editor Console（Console ビュー）に書き出します。

DSS ファイルの管理

- アクティブ サービス コンフィギュレーションに新しいシグニチャをインストールする場合は、「プロトコル パックの処理」（P.4-19）を参照してください。
- Service Configuration Editor でシグニチャを操作する方法については、「プロトコル シグニチャの管理」（P.7-36）を参照してください。
- サービス コンフィギュレーション ユーティリティ **servconf** を使用してシグニチャを適用する方法については、「SCA BB サービス コンフィギュレーション ユーティリティ」（P.13-1）を参照してください。

DSS ファイルのコンポーネント、および DSS ファイルの作成と編集については、次のセクションで説明します。

DSS ファイルのコンポーネント

DSS ファイルのコンポーネントは、Signature Editor の [Script] ペインにツリー構造で表示されます。DSS コンポーネント ツリーの適切なノードを選択すると、ノードに関連するプロパティを [Property] ペインで定義できるようになります。

以降のセクションでは DSS ファイルのコンポーネントについて説明します。

DSS ファイル

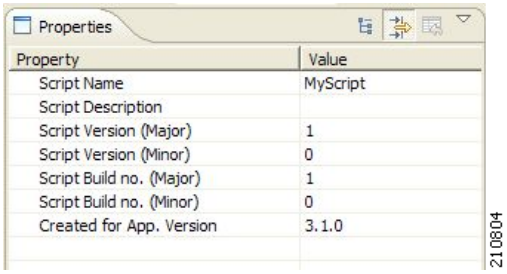
DSS ファイル名は、DSS ファイルのコンポーネント ツリーのルート ノードです。

ルート ノードを選択すると、DSS ファイルの次のプロパティを定義できるようになります。

- [Script Name]：スクリプトのわかりやすい名前を入力します。
- [Script Description]：スクリプトを作成した理由を入力し、その内容について説明します。
- [Script Version (Major)]
- [Script Version (Minor)]
- [Script Build Number (Major)]
- [Script Build Number (Minor)]
- [Created for Application Version]：定義済みの値のリストから選択します。

図 12-1 は、DSS ファイル プロパティのデフォルト値を示しています。

図 12-1　　DSS ファイル プロパティのデフォルト値



DSS ファイルには単一プロトコル リストが含まれます。

DSS プロトコル リスト

プロトコル リストには、定義するプロパティがありません。プロトコル リストには、追加、修正、拡張を行っているすべてのプロトコルが含まれます。

DSS プロトコルについての情報

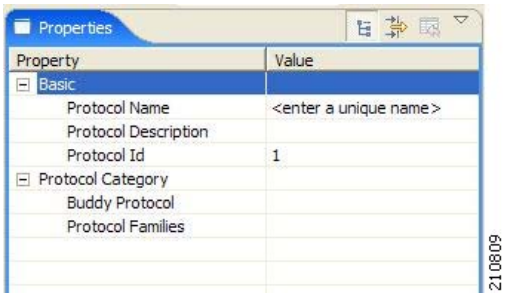
DSS ファイルのコンポーネント ツリーからプロトコル ノードを選択すると、プロトコルの次のプロパティを定義できるようになります。

- [Basic]
  - [Protocol Name]：「プロトコル名および ID の設定」（P.12-3）を参照してください。
  - [Protocol Description]
  - [Protocol ID]：「プロトコル名および ID の設定」（P.12-3）を参照してください。
- [Protocol Category]
  - [Buddy Protocol]：「バディ プロトコル」（P.12-4）を参照してください。
  - [Protocol Families]：1 つ以上のプロトコル ファミリにプロトコルを割り当てます。
  - [P2P]
  - [SIP]
  - [VOIP]
  - [Worm]

    プロトコル ファミリにプロトコルを関連付けると、ファミリに関するレポートに新しいプロトコルが組み込まれます。

図 12-2 は、プロトコル プロパティのデフォルト値を示しています。

図 12-2　プロトコル プロパティのデフォルト値



プロトコルにはシグニチャが含まれます。

プロトコル名および ID の設定

DSS には次の 2 種類のプロトコルを含めることができます。

- SCA BB にとって新しいプロトコル：DSS でプロトコルを定義します。
- SCA BB ですでにサポートされているプロトコル：プロトコルの識別の拡張または修正を DSS で行います。

名前および ID の選択方法は、この 2 つで次のように異なります。

- SCA BB にとって新しいプロトコルの場合、SCA BB がすでにサポートしているプロトコル名に名前を一致させることはできません。サポートされているプロトコルの名前のリストを表示するには、Service Configuration Editor で [Protocol Settings] ダイアログボックスを開きます（「プロトコルの表示方法」（P.7-21）を参照）。5000 ～ 9998 の範囲で一意の ID をプロトコルに割り当ててください。

- 既存プロトコルの場合、DSS のプロトコル名および ID は、サービス コンフィギュレーションのプロトコル名および ID と一致している必要があります。Service Configuration Editor の [Protocol Settings] ダイアログボックスで名前および ID を特定してください（「プロトコルの表示方法」（P.7-21）を参照）。

バディ プロトコル

DSS で追加する新しいプロトコルの設定を簡単にするため、DSS では新しいプロトコルのバディ プロトコルを指定できます。アプリケーションは、サービス コンフィギュレーションに DSS をインポートするとき、バディ プロトコルを参照するサービス要素を検出すると、バディ プロトコルを使用する一連のサービス要素を自動的に複製し、バディ プロトコルのすべての参照を新しいプロトコルの参照で置き換えます。新しいプロトコルとサービスの関係は、バディ プロトコルとサービスの関係と一致します。

DSS シグニチャ

プロトコルには、必要な数のシグニチャを含めることができます。

プロトコルには、次の 4 種類のシグニチャを追加できます。

- ストリング照合型シグニチャ
- ペイロード長シグニチャ
- Hypertext Transport Protocol（HTTP; ハイパーテキスト転送プロトコル）ユーザ エージェント シグニチャ
- HTTP x ヘッダー シグニチャ

4 つそれぞれのシグニチャ タイプは、フローの先頭ペイロード パケットでさまざまな条件を検証します。

以降のサブセクションでは、このシグニチャ タイプと条件について説明します。

ストリング照合型シグニチャおよびペイロード長シグニチャには、詳細検査句を含めることができます。先頭のペイロード パケット条件が満たされるシグニチャは、詳細検査句の条件も満たされる場合、フローを受け入れます。

DSS ストリング照合型シグニチャ

DSS ファイルのコンポーネント ツリーからストリング照合型シグニチャを選択すると、シグニチャの次のプロパティを定義できるようになります。

- [Signature Name]：一意の名前。
- [Signature Description]
- [Signature ID]：0xC010000 ～ 0xC0100FF（10 進数の 201392128 ～ 201392383）の範囲の値。
- [First Payload Packet Conditions]
  - [Fixed Size Byte String]：（表示のみ）次の 4 つのフィールドによって形成される文字列が表示されます。
  - [0]：文字列の第 1 バイトの ASCII コードを入力します。すべての値が受け入れ可能であることを示すには、「*」を入力します。
  - [1]：文字列の第 2 バイトの ASCII コードを入力します。すべての値が受け入れ可能であることを示すには、「*」を入力します。
  - [2]：文字列の第 3 バイトの ASCII コードを入力します。すべての値が受け入れ可能であることを示すには、「*」を入力します。
  - [3]：文字列の第 4 バイトの ASCII コードを入力します。すべての値が受け入れ可能であることを示すには、「*」を入力します。

- [String Position] : パケットにおける固定サイズ バイト文字列の位置。位置は、パケットの先頭バイトから数えた、文字列の先頭バイトの位置です。文字列をパケットの先頭と照合するには、この値をゼロにする必要があります。値は、4 で割り切れる整数にしてください。
- [Packet Direction] : ペイロードを含むフローの先頭パケットの開始側。このフィールドは、次の 3 つのうちいずれかの値になります。
- [From Server]
- [From Client]
- [Don’t Care]（両側）
- [Port Range] :（表示のみ）次の 2 つのフィールドから形成されるポート範囲。デフォルト値は、ポート範囲全体（0 ～ 65535）です。
- [From Port] : ポート範囲の下限（この値を含む）。
- [To Port] : ポート範囲の上限（この値を含む）。
- [Check before PL] : 値 **true** と **false** を切り替えます。

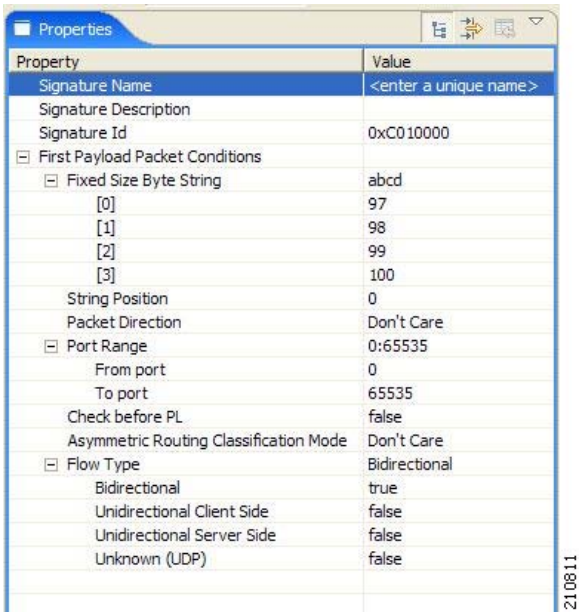
  このフィールドは、SCA BB の組み込み Protocol Library（PL; プロトコル ライブラリ）分類の前にシグニチャをテストするか、そのあとでシグニチャをテストするかを示します。組み込み分類の実行前にシグニチャをテストすると、フローがこのシグニチャと一致した場合、PL 分類はスキップされます。このフィールドを「false」に設定すると、PL 分類でサポート対象プロトコル シグニチャを識別できない場合に限り、このシグニチャはテストされます。
- [Asymmetric Routing Classification Mode] : シグニチャを非対称ルーティング分類モードの状態に従ってテストするかどうかを示します。次の 3 つの値のいずれかになります。
- [Don’t Care] : このシグニチャを非対称ルーティング分類モードが有効か無効かどうかテストすることを示します。
- [Disabled]
- [Enabled]
- [Flow Type] :（表示のみ）このフィールドには条件を適用するフロー タイプが示されます（複数のタイプに条件を適用可能）。非対称ルーティング分類モードが有効でないと無視されます。

  フロー タイプは次の 4 つのフィールドで指定されます。
- [Bidirectional] : 値 **true** と **false** を切り替えます。
- [Unidirectional Client Side] : 値 **true** と **false** を切り替えます。クライアント側からのパケットだけが検出された TCP フローに適用されます。
- [Unidirectional Server Side] : 値 **true** と **false** を切り替えます。サーバ側からのパケットだけが検出された TCP フローに適用されます。
- [Unknown (UDP)] : 値 **true** と **false** を切り替えます。一方向からのパケットだけが検出された UDP フローに適用されます。

注意　シグニチャが先頭ペイロード パケットだけに従ってプロトコルを識別する場合に限り、[Check before PL] を **true** に設定してください。シグニチャが詳細検査条件も使用してあとのパケットを調べて、シグニチャがフローと一致しない場合、PL 分類は適切に実行されません。

図 12-3 は、ストリング照合型シグニチャのプロパティのデフォルト値を示しています。

図 12-3　ストリング照合型シグニチャのプロパティのデフォルト値



ストリング照合型シグニチャの先頭ペイロード パケット条件と一致するフローは、シグニチャの詳細検査条件と比較されます（「DSS 詳細検査条件」（P.12-9）を参照）。

DSS ペイロード長シグニチャ

DSS ファイルのコンポーネント ツリーからペイロード長シグニチャを選択すると、シグニチャの次のプロパティを定義できるようになります。

- [Signature Name]：一意の名前。
- [Signature Description]
- [Signature ID]：0xC010000 ～ 0xC0100FF（10 進数の 201392128 ～ 201392383）の範囲の値。
- [First Payload Packet Conditions]
  - [Packet Direction]：ペイロードを含むフローの先頭パケットの開始側。このフィールドは、次の 3 つのうちいずれかの値になります。
  - [From Server]
  - [From Client]
  - [Don’t Care]（両側）
  - [Payload Length]：ペイロード パケットのバイト数。
  - [Port Range]：（表示のみ）次の 2 つのフィールドから形成されるポート範囲。デフォルト値は、ポート範囲全体（0 ～ 65535）です。
  - [From Port]：ポート範囲の下限（この値を含む）
  - [To Port]：ポート範囲の上限（この値を含む）
  - [Check before PL]：値 **true** と **false** を切り替えます。

このフィールドは、SCA BB の組み込みプロトコル ライブラリ（PL）分類の前にシグニチャをテストするか、そのあとでシグニチャをテストするかを示します。組み込み分類の実行前にシグニチャをテストすると、フローがこのシグニチャと一致した場合、PL 分類はスキップされます。このフィールドを「false」に設定すると、PL 分類でサポート対象プロトコル シグニチャを識別できない場合に限り、このシグニチャはテストされます。

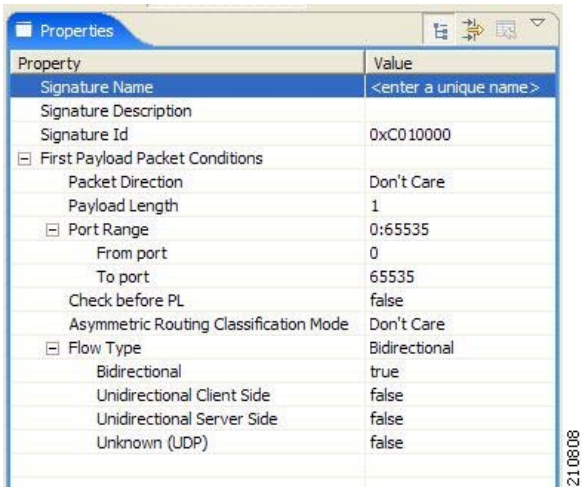
- [Asymmetric Routing Classification Mode]：シグニチャを非対称ルーティング分類モードの状態に従ってテストするかどうかを示します。次の 3 つの値のいずれかになります。
- [Don’t Care]：このシグニチャを非対称ルーティング分類モードが有効か無効かどうかテストすることを示します。
- [Disabled]
- [Enabled]
- [Flow Type]：（表示のみ）このフィールドには条件を適用するフロー タイプが示されます（複数のタイプに条件を適用可能）。非対称ルーティング分類モードが有効でないと無視されます。

  フロー タイプは次の 4 つのフィールドで指定されます。
- [Bidirectional]：値 **true** と **false** を切り替えます。
- [Unidirectional Client Side]：値 **true** と **false** を切り替えます。クライアント側からのパケットだけが検出された TCP フローに適用されます。
- [Unidirectional Server Side]：値 **true** と **false** を切り替えます。サーバ側からのパケットだけが検出された TCP フローに適用されます。
- [Unknown (UDP)]：値 **true** と **false** を切り替えます。一方向からのパケットだけが検出された UDP フローに適用されます。

注意　シグニチャが先頭ペイロード パケットだけに従ってプロトコルを識別する場合に限り、[Check before PL] を **true** に設定してください。シグニチャが詳細検査条件も使用してあとのパケットを調べて、シグニチャがフローと一致しない場合、PL 分類は適切に実行されません。

図 12-4 は、ペイロード長シグニチャのプロパティのデフォルト値を示しています。

図 12-4　ペイロード長シグニチャのプロパティのデフォルト値



ペイロード長シグニチャの先頭ペイロード パケット条件と一致するフローは、シグニチャの詳細検査条件と比較されます（「DSS 詳細検査条件」（P.12-9）を参照）。

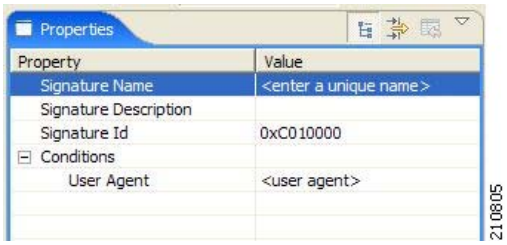
DSS HTTP ユーザ エージェント シグニチャ

DSS ファイルのコンポーネント ツリーから HTTP ユーザ エージェント シグニチャを選択すると、シグニチャの次のプロパティを定義できるようになります。

- [Signature Name]：一意の名前
- [Signature Description]
- [Signature ID]：0xC010000 ～ 0xC0100FF（10 進数の 201392128 ～ 201392383）の範囲の値
- [Conditions]
  - [User Agent]：HTTP ヘッダーの [User Agent] フィールドの値

図 12-5 は、HTTP ユーザ エージェント シグニチャ プロパティのデフォルト値を示しています。

図 12-5　HTTP ユーザ エージェント シグニチャ プロパティのデフォルト値



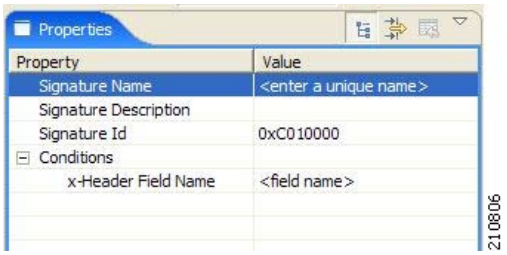
DSS HTTP x ヘッダー シグニチャ

DSS ファイルのコンポーネント ツリーから HTTP x ヘッダー シグニチャを選択すると、シグニチャの次のプロパティを定義できるようになります。

- [Signature Name]：一意の名前
- [Signature Description]
- [Signature ID]：0xC010000 ～ 0xC0100FF（10 進数の 201392128 ～ 201392383）の範囲の値
- [Conditions]
  - [x-Header Field Name]：HTTP ヘッダーの x ヘッダーにあるフィールドの名前

図 12-6 は、DSS ファイル プロパティのデフォルト値を示しています。

図 12-6　DSS ファイル プロパティのデフォルト値



DSS 詳細検査句

詳細検査句は、詳細検査条件の接続句です。シグニチャは、この句のすべての条件が満たされる場合に*限って*フローを受け入れます。

（注）　シグニチャに複数の詳細検査句がある場合、句およびそれぞれの句を構成する詳細検査条件は、詳細検査条件の Packet Number プロパティの値に基づいてテストされます。

最初のペイロード パケットが最初のペイロード パケット条件によって受け入れられたあとで、Packet Number が最も小さい条件を含む句がテストされます。この句のその他の条件は、Packet Number の昇順で確認されます。このため、句の条件の Packet Number を、それを継承する句の最大 Packet Number より小さくすることはできません。

DSS 詳細検査条件

詳細検査条件は、ストリング照合型シグニチャまたはペイロード長シグニチャの先頭ペイロード パケット条件選別を通過したフローに対してチェックする、一連の条件です。

DSS ファイルのコンポーネント ツリーから詳細検査条件ノードを選択すると、詳細検査条件の次のプロパティを定義できるようになります。

- [Packet Direction] : ペイロードを含むフローの先頭パケットの開始側。このフィールドは、次の 3 つのうちいずれかの値になります。
  - [From Server]
  - [From Client]
  - [Don’t Care]（両側）
- [Packet Number] : フローのパケット番号。ペイロード パケットの番号はゼロから始まり、パケットは両方向でカウントされます。
- [Payload Length] : バイト単位のパケットの長さ。あらゆる値が受け入れ可能であることを示すには、ゼロを入力します。
- [Printable Characters] : 検査パケットに印刷可能文字だけが含まれるかどうかをテストします。このフィールドは、次の 3 つのうちいずれかの値になります。
  - [Printable Characters Only]
  - [At Least One Non-Printable]
  - [Don't Care]
- [Substring Search] : 検索文字列をパケットの特定の位置と照合します。この条件が関係ない場合は、[Search String] フィールドを空にします。
  - [Position Offset] : パケットの検索文字列の検索を開始する位置。オフセットは、[Start Search From] フィールドに指定した位置を基準とした位置です。
  - [Start Search From] : 次の 2 つのうちいずれかの値を含めることができます。
  - [Packet beginning]
  - [Last match]

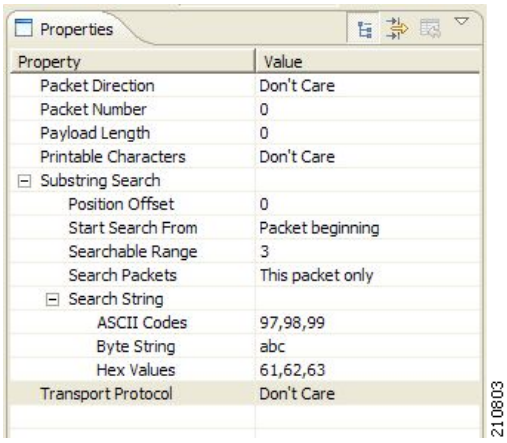
    [Last match] は、前回の検索で一致した文字列が終わる場所から検索文字列の検索が始まることを表します。最終一致は、前回のサブストリング検索から、または最終文字列ベース先頭ペイロード パケット条件からになります。
  - [Searchable Range] : 検索文字列のこのバイト数で検索が実行されます。

  - [Search Packets]：次の 2 つのうちいずれかの値を含めることができます。
  - [This packet only]
  - [Multiple packets]

    [Multiple Packets] は、[Searchable Range] フィールドに指定したバイト数より合計バイト数が小さい場合、複数のパケットにわたって検索が行われることを示します。
  - [Search String]：次の 3 つのうちいずれかのフィールドに検索文字列を入力します（その他 2 つのフィールドは自動的に更新されます）。
  - [ASCII Codes]：検索文字列の文字の ASCII コードを入力します。各コードはカンマで区切ります。
  - [Byte String]：実際の検索文字列を入力します。
  - [Hex Values]：検索文字列の文字の ASCII コードの 16 進値を入力します。各コードはカンマで区切ります。
- [Transport Protocol]：このフィールドは、次の 3 つのうちいずれかの値になります。
  - [TCP]
  - [UDP]
  - [Don’t Care]（TCP または UDP）

図 12-7 は、詳細検査条件プロパティのデフォルト値を示しています。

図 12-7　詳細検査条件プロパティのデフォルト値



詳細検査条件の構造は、文字列照合型シグニチャおよびペイロード長シグニチャと同じです。

DSS ファイルの作成

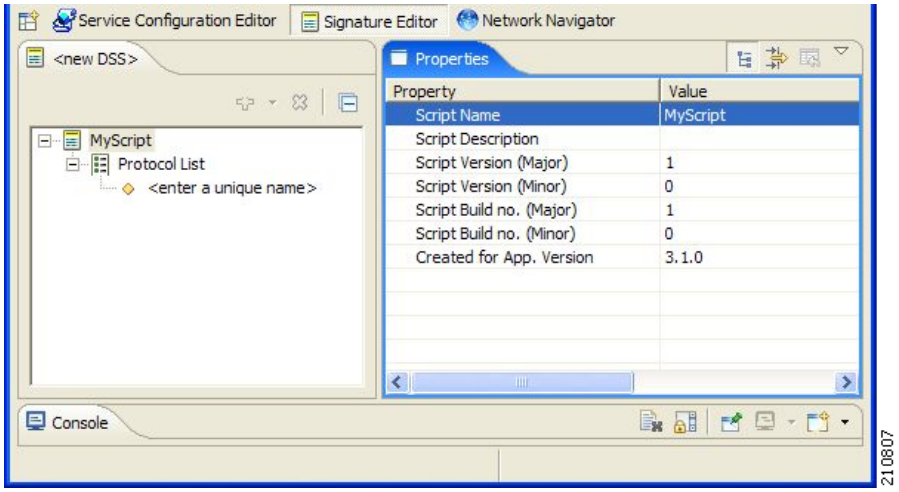
Signature Editor で DSS ファイルを開いている場合は、そのファイルを保存してから新しい DSS ファイルを作成してください。保存していないすべての変更内容は失われます。

ステップ 1　ツールバーの（[Create a New DSS File]）をクリックします。

DSS ファイル ノード、プロトコル リスト ノード、プロトコル ノードを含む DSS コンポーネント ツリーが、Script ビューに表示されます。

新しい DSS ファイルのデフォルト プロパティが Properties ビューに表示されます（図 12-8）。

図 12-8　[Properties] タブ



ステップ 2　DSS ファイル プロパティを編集します。

プロパティの説明については、「DSS ファイル」（P.12-2）を参照してください。

ステップ 3　プロトコル ノードをクリックします。

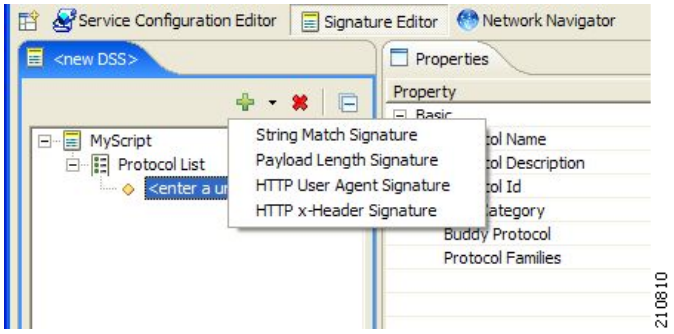
プロトコル プロパティが Properties ビューに表示されます（図 12-9）。

ステップ 4　プロトコル プロパティを編集します。

プロパティの説明については、「DSS プロトコルについての情報」（P.12-3）を参照してください。

ステップ 5　ボタンの横のドロップダウン矢印をクリックします。

図 12-9　プロトコル プロパティ

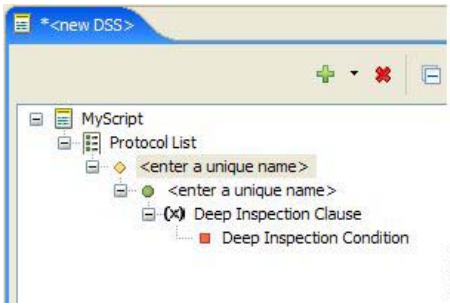


ステップ 6　表示されるドロップダウン メニューからシグニチャ タイプを選択します。

シグニチャ ノードがプロトコル ノードの下に追加されます。

ストリング照合型シグニチャまたはペイロード長シグニチャを選択した場合は、詳細検査句ノードおよび詳細検査条件ノードも追加されます（図 12-10）。

図 12-10　プロトコル リスト情報



ステップ 7　シグニチャ ノードをクリックします。

シグニチャ プロパティが Properties ビューに表示されます。

ステップ 8　シグニチャ プロパティを編集します。

プロパティの説明については、「DSS シグニチャ」（P.12-4）を参照してください。

ステップ 9　ストリング照合型シグニチャまたはペイロード長シグニチャを選択した場合は、詳細検査条件ノードをクリックして詳細検査条件プロパティを編集します。

詳細検査条件プロパティが Properties ビューに表示されます。

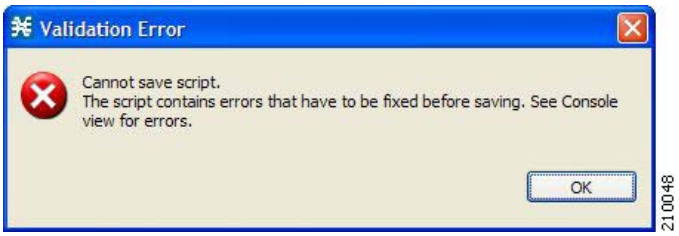
プロパティの説明については、「DSS 詳細検査条件」（P.12-9）を参照してください。

ステップ 10　詳細検査条件、詳細検査句、シグニチャ、プロトコルを必要に応じてさらに追加します。

ステップ 11　ツールバーの（[Save]）をクリックします。

- プロトコル名またはプロトコル ID が重複している場合は、[Validation Error] メッセージが表示されます（図 12-11）。

図 12-11　[Validation Error]



[OK] をクリックして重複を解決してから、（[Save]）を再びクリックします。

[Save As] ダイアログボックスが表示されます。

ステップ 12　新しい DSS ファイルを保存するフォルダを選択します。

ステップ 13　DSS ファイルの適切な名前を [File name] フィールドに入力します。

ステップ 14　[Save] をクリックします。

[Save As] ダイアログボックスが閉じます。

DSS ファイルが保存されます。

DSS ファイルの編集

既存の DSS ファイルを編集して新しいプロトコルを追加したり、既存プロトコルの修正または削除を行ったりすることができます。

注意　Signature Editor で DSS ファイルを開いている場合は、そのファイルを保存してから別の DSS ファイルを開いてください。保存していないすべての変更内容は失われます。

ステップ 1　ツールバーの（[Open a DSS File]）をクリックします。

[Open] ダイアログボックスが表示されます。

ステップ 2　編集する DSS ファイルを選択します。

ステップ 3　[Open] をクリックします。

[Open] ダイアログボックスが閉じます。

選択したファイルの DSS コンポーネント ツリーが Script ビューに表示されます。

DSS ファイル ノードが選択され、DSS ファイルのプロパティが Properties ビューに表示されます。

ステップ 4　DSS ファイル コンポーネントの追加、編集、削除を行います。

さまざまなコンポーネントのプロパティの説明については、「DSS ファイルのコンポーネント」（P.12-2）のサブセクションを参照してください。

ステップ 5　修正した DSS ファイルを保存します。

- 変更内容で現在の DSS ファイルを上書きするには、次のように操作します。
  - ツールバーの（[Save]）をクリックします。

    DSS ファイルの変更が保存されます。
- 修正した DSS ファイルを新しい名前で保存するには、次のように操作します。

1. [File] > [Save As] の順に選択します。

   [Save As] ダイアログボックスが表示されます。
2. 新しい DSS ファイルを保存するフォルダを選択します。
3. DSS ファイルの適切な名前を [File name] フィールドに入力します。
4. [Save] をクリックします。

   [Save As] ダイアログボックスが閉じます。

   修正した DSS ファイルが新しい名前で保存されます。

DSS ファイルのインポート

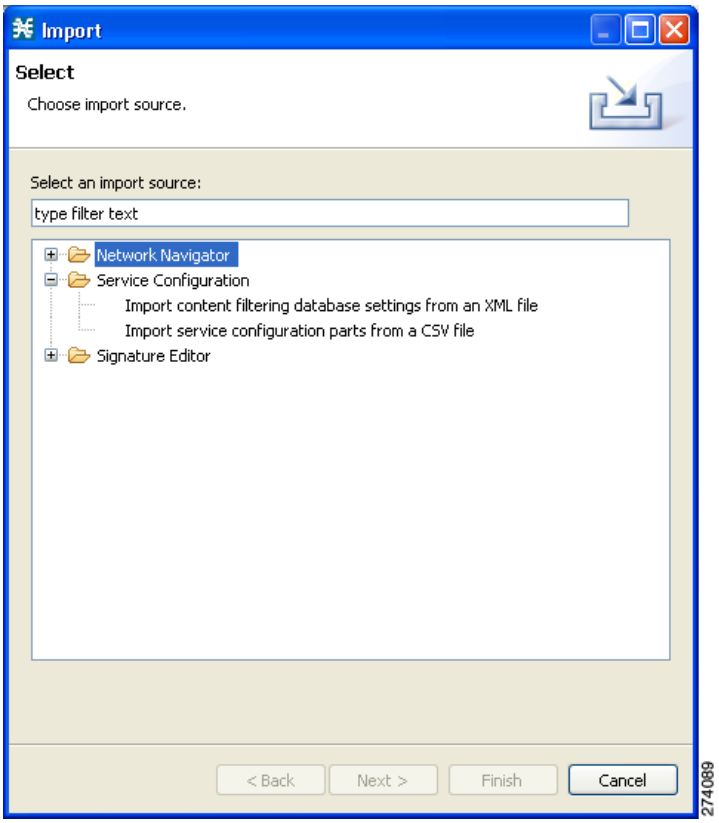
現在編集しているファイルに DSS ファイルをインポートできます。

（注）　シグニチャをインポートすると、プロトコル名またはプロトコル ID が重複することがあります。

ステップ 1　Console のメイン メニューで、[File] > [Import] の順に選択します。

[Import] ダイアログボックスが表示されます（図 12-12）。

図 12-12　[Import]

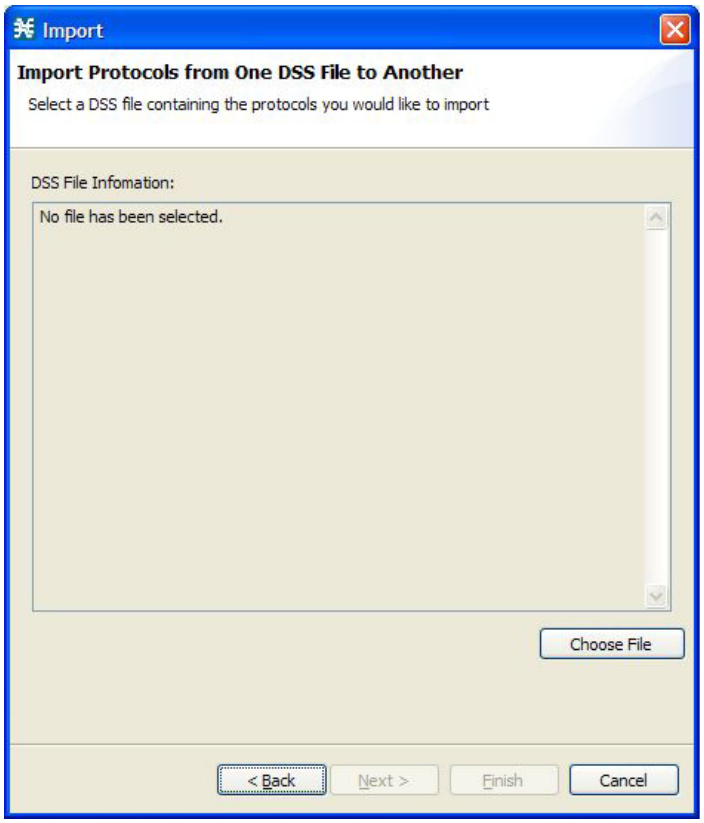


ステップ 2　インポート元リストから [Import protocols from one DSS file to another DSS] を選択します。

ステップ 3　[Next] をクリックします。

[Import] ダイアログボックスの第 2 画面が表示されます（図 12-13）。

図 12-13　[Import Protocols from One DSS File to Another]



ステップ 4　[Choose File] をクリックします。

[Open] ダイアログボックスが表示されます。

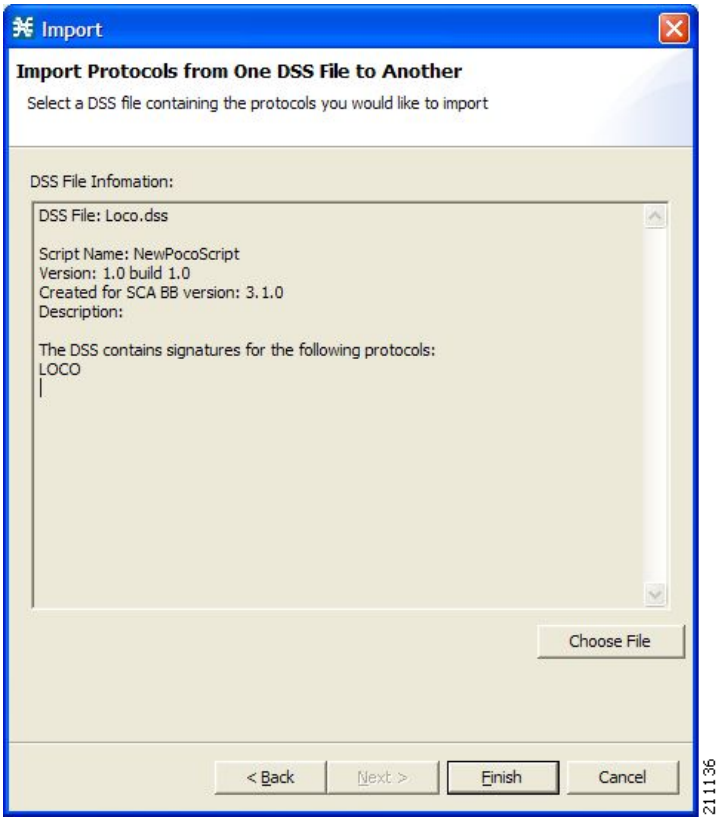
ステップ 5　インポートする DSS ファイルを選択します。

ステップ 6　[Open] をクリックします。

[Open] ダイアログボックスが閉じます。

選択した DSS ファイルに関する情報が、[DSS File Information] 領域に表示されます（図 12-14）。

図 12-14　[Import Protocols from One DSS File to Another]



ステップ 7　[Finish] をクリックします。

[Import] ダイアログボックスが閉じます。

選択した DSS ファイルの内容が Signature Editor にインポートされます。

CHAPTER 13

その他の管理ツールおよびインターフェイス

はじめに

この章の内容は次のとおりです。

SCA BB サービス コンフィギュレーション ユーティリティ

Cisco Service Control Application for Broadband（SCA BB）サービス コンフィギュレーション ユーティリティ（**servconf**）は、サービス コンフィギュレーションの適用および取得を行う Command-Line Utility（CLU; コマンドライン ユーティリティ）です。スクリプト環境で使用し、複数の Service Control Engine（SCE）プラットフォームにおけるサービス コンフィギュレーション タスクを自動化してください。

サービス コンフィギュレーション ユーティリティは、Windows 環境、Solaris 環境、Linux 環境で動作します。

servconf 構文

servconf のコマンドライン構文は次のとおりです。

```
servconf <operation> [<option>] [<option>]...
```

表 13-1 に、**servconf 処理**を示します。

表 13-2、表 13-3、表 13-4、表 13-5、および表 13-6 に **servconf** オプションを示します。

表 13-1　servconf 処理

処理	省略形	説明
--apply	**-a**	指定されたサービス コンフィギュレーション ファイルを、指定された SCE プラットフォームにコピーして、アクティブにします。
--retrieve	**-r**	現在のサービス コンフィギュレーションを取得します。
--update-dc	**-u**	Cisco Service Control Management Suite（SCMS）Collection Manager（CM）をサービス コンフィギュレーションの値で更新します。
--status	—	SCE プラットフォームのサービス コンフィギュレーション ステータスを表示します。
--update-signature	—	SCE プラットフォームを新しいプロトコル パックで更新します。
--update-signature-pqi	—	SCE プラットフォームを新しい SPQI プロトコル パックで更新します。
--signature-info	**-i**	Dynamic Signature Script（DSS）ファイルに関する情報を表示します。
--help	—	ヘルプを表示して終了します。
--version	—	プログラム バージョン番号を表示してから、終了します。

表 13-2　servconf のファイル オプション

ファイル オプション	省略形	説明
--file=*filename*	-f	サービス コンフィギュレーション ファイルまたは DSS ファイルを指定します。
--backup-directory=*directory*	-b	新しいプロトコル パックの適用前に、取得した PQB ファイルを保存するディレクトリを指定します。

表 13-3　servconf の接続オプション

ファイル オプション	省略形	説明
--se=*address*	**-S**	宛先 SCE プラットフォームの IP アドレスを指定します。 複数の SCE プラットフォームを指定するには、IP アドレスをセミコロンで区切ります（次のセクションの例 1 を参照）。 UNIX コマンドラインでセミコロンを使用する場合は、コマンドライン引数を引用符で囲む必要があります。
--dc=*address*	**-D**	宛先 SCMS-CM プラットフォームの IP アドレスを指定します（**--update-dc** 処理の場合にだけ必要）。

表 13-3　servconf の接続オプション（続き）

ファイル オプション	省略形	説明
--password=*password*	**-P**	SCE プラットフォームに接続するためのパスワードを指定します。
--username=*username*	**-U**	SCE プラットフォームに接続するためのユーザ名を指定します。このオプションを指定しない場合は、次のデフォルト値が使用されます。 • SCE - admin • CM - pcube • SM - pcube

表 13-4　servconf の参照 SCE オプション

ファイル オプション	説明
--refer-se=*address*	サービス コンフィギュレーションの値が参照する SCE プラットフォームの IP アドレスを指定します（**--update-dc** 処理の場合にだけ必要）。

表 13-5　servconf の適用オプション

ファイル オプション	説明
--no-dc	（オプション）--apply 処理で、サービス コンフィギュレーションの値を使用して SCMS-CM を自動更新しないように指定します。
--no-default-signature	デフォルト DSS を追加せずにサービス コンフィギュレーションを適用します。
--force-default-signature	既存 DSS のシグニチャがサービスにマッピングされていても、取得した PQB の DSS をデフォルト DSS で強制的に置き換えます。このフラグを指定しない場合は、DSS を含む PQB を更新しようとしてもエラーになります。

表 13-6　servconf の更新シグニチャ オプション

ファイル オプション	説明
--force-signature	既存 DSS のシグニチャがサービスにマッピングされていても、取得した PQB の DSS の置き換えを強制します。このフラグを指定しない場合は、DSS を含む PQB を更新しようとしてもエラーになります。

servconf の例

例 1

ローカル マシンから 2 つの SCE プラットフォーム（63.111.106.7 および 63.111.106.12）にサービス コンフィギュレーション ファイル config.pqb をコピーし、このコンフィギュレーションをアクティブにします。

```
servconf ”--se=63.111.106.7;63.111.106.12” --username Alice --password ***** --apply
--file config.pqb
```

例 2

63.111.106.7 の SCE プラットフォームから現在のサービス コンフィギュレーションを取得し、ローカル マシンのファイル my_files¥config.pqb に保存します。

```
servconf -S 63.111.106.7 -U Bob -P ***** --retrieve --file my_files\config.pqb
```

例 3

ファイル config.pqb のサービス コンフィギュレーションの値を使用して、SCMS-CM（63.121.116.17）を更新します。この処理は、サービス コンフィギュレーションの値を SCE プラットフォーム（63.111.106.7）に適用する場合と同様ですが、実際には適用されません。

```
servconf -D 63.121.116.17 -U Alice -P ***** --update-dc
--refer-se 63.111.106.7 --file config.pqb
```

例 4

10.56.216.33 および 10.56.216.36 の SCE プラットフォームに、プロトコル パック ファイル new_signature.spqi を配布します。

```
servconf --update-signature-pqi -f new_signature.spqi
-S ”10.56.216.33;10.56.216.36” -U user123 -P *****
```

SCA BB リアルタイム モニタ コンフィギュレーション ユーティリティの使用法

ネットワーク管理者は、MRTG などの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）ベースのモニタ ツールにより、ネットワーク デバイスのアクティビティおよび状態をリアル タイムでモニタできます。SCA BB には SNMP ベースのリアルタイム モニタ ソリューションが含まれており、このリアルタイム モニタ ソリューションは MRTG およびグラフィック ユーティリティ（RRDTool）で実装されています。

SCA BB リアルタイム モニタ コンフィギュレーション ユーティリティ（**rtmcmd**）は、MRTG ツールが必要とするファイルの生成を自動化するためのコマンドライン ユーティリティ（CLU）です。

インストール方法については、「SCA BB コンフィギュレーション ユーティリティのインストール方法」（P.4-7）を参照してください。SCA BB SNMP ベース リアルタイム モニタ ソリューションのインストールおよび使用方法については、『*Cisco SCA BB SNMP Real Time Monitoring User Guide*』を参照してください。

rtmcmd 構文

SCA BB リアルタイム モニタ コンフィギュレーション ユーティリティのコマンドライン構文は次のとおりです。

```
rtmcmd --sce <SCE (SNMP) addresses> {--file <PQB filename> | (--pqb-sce
<SCE (PQB) addresses> --username <username> --password <password>)} --source-dir <dir>
--dest-dir <dir> --config-file <file>
```

表 13-7 に **rtmcmd** オプションを示します。

表 13-7　rtmcmd オプション

オプション	省略形	説明
--sce *address*	**-S**	SNMP データの収集元の SCE プラットフォームの IP アドレスまたはホスト名を指定します。 複数の SCE プラットフォームを指定するには、IP アドレスをセミコロンで区切って示します。 UNIX コマンドラインでセミコロンを使用する場合は、コマンドライン引数を引用符で囲む必要があります。
--file *filename*	**-f**	(--pqb-sce を含めない場合に必要) 設定およびレポート ファイルの生成時に使用するサービス コンフィギュレーション ファイルを指定します。このオプションを指定しない場合は、**--username/-U** オプションおよび **--password/-P** オプションを指定できません。
--pqb-sce *address*	**-q**	(--file を指定しない場合に必要) サービス コンフィギュレーションの取得元となる SCE プラットフォームのホスト名または IP アドレスを指定します。このオプションでは、**--username/-U** オプションおよび **--password/-P** オプションが必要となります。
--username <*username*>	**-U**	(**--pqb-sce** を指定した場合に必要) SCE プラットフォームに接続するためのユーザ名を指定します。
--password <*password*>	**-P**	(**--username** を指定した場合に必要) SCE プラットフォームに接続するためのパスワードを指定します。
--source-dir <*dir*>	**-s**	レポート テンプレート ファイルの場所を指定します。
--dest-dir <*dir*>	**-d**	処理したレポート テンプレートを保存するディレクトリを指定します。
--config-file <*file*>	**-c**	コンフィギュレーション ファイルを指定します (「rtmcmd ユーザ コンフィギュレーション ファイル」(P.13-6) を参照)。

次の構文を使用してその他の処理を呼び出し (表 13-8 を参照)、**rtmcmd** に関する情報を表示できます。

```
rtmcmd <operation>
```

表 13-8　rtmcmd 処理

処理	説明
--version	プログラム バージョン番号を表示してから、終了します。
--help	ヘルプを表示して終了します。

rtmcmd の例

例 1

サービス コンフィギュレーション ファイル servicecfg.pqb を使用して、2 つの SCE プラットフォーム（63.111.106.7 および 63.111.106.12）から SNMP 情報を収集してレポートするための設定ファイルおよびレポート ファイルを作成するには、次のように入力します。

```
rtmcmd --sce="63.111.106.7;63.111.106.12" --file=servicecfg.pqb
--source-dir=/rtm-templates --dest-dir=/rtm-output -c./rtmcmd.cfg
```

例 2

63.111.106.7 の SCE プラットフォームにロードしたサービス コンフィギュレーションを使用して、2 つの SCE プラットフォーム（63.111.106.7 および 63.111.106.12）から SNMP 情報を収集してレポートするための設定ファイルおよびレポート ファイルを作成するには、次のように入力します。

```
rtmcmd -S "63.111.106.7;63.111.106.12" -U user123 -P **** --pqb-sce=63.111.106.7
--source-dir=/rtm-templates --dest-dir=/rtm-output -c./rtmcmd.cfg
```

rtmcmd ユーザ コンフィギュレーション ファイル

ユーザ コンフィギュレーション ファイルには、**rtmcmd** ユーティリティで必要となるユーザ固有の情報が含まれます。SCA BB ユーティリティの配信パッケージには、rtmcmd.cfg という名前のサンプル コンフィギュレーション ファイルが含まれています。設定の詳細に従ってこのファイルを編集してください。

表 13-9 に、ユーザ コンフィギュレーション ファイルに必要となるコンフィギュレーション パラメータを示します。

表 13-9　rtmcmd ユーザ コンフィギュレーション ファイルのパラメータ

パラメータ	説明	デフォルト値	必須/オプション
[rrdtool_bin_dir]	RRDTool および RRDCGI のバイナリ ファイルをインストールするディレクトリの絶対パス。	—	必須
[rtm_dir]	RRD アーカイブおよび CGI ファイルを保存するディレクトリの絶対パス。Web サーバの Web ディレクトリの下にします。	—	必須
[mrtg_bin_dir]	MRTG バイナリ ファイルをインストールするディレクトリの絶対パス。 crontab サンプル ファイルで MRTG 呼び出しコマンドを作成するために、この場所を使用します。	—	必須
[snmpCommunityString]	SCE プラットフォームへのアクセス時に使用する SNMP コミュニティ ストリング。	Public	必須

コンフィギュレーション テキスト ファイルはキーと値ペアのリストであり、キーは上記のいずれかのパラメータで、次の形式になっています。

- それぞれのキーと値のペアは別々の行にあります。

- 各行の末尾にバックスラッシュ「\」を入力し、キーと値のペアを複数の連続行に拡張できます。
- 値に実際のバックスラッシュを使用する（Windows のディレクトリ名など）には、「\\」のようにバックスラッシュを 2 つめのバックスラッシュでエスケープする（またはスラッシュ「/」を使用する）必要があります。
- コメント行は「#」または「!」で始めます。

たとえば、次のようになります。

```
# This is a comment line.
# Directory names should use escape backslashes:
rtm_dir=D:\\PROGRA~1\\APACHE~1\\Apache2.2\\htdocs
```

rtmcmd ユーザ コンフィギュレーション ファイルの例

```
#The absolute path to the RRD tool's execution files folder
#Use '\\' or '/' as path separator
rrdtool_bin_dir=C:/rrdtool-1.2.15/rrdtool/Release

#The absolute path where RTM files will be placed.
#This path will be used by MRTG to create and update the RRD files
#Note: path must not contain white spaces!
rtm_dir=C:/PROGRA~1/APACHE~1/Apache2.2/htdocs

#The absolute path to the MRTG bin folder.
#This path will be used to create file crontab.txt
mrtg_bin_dir=C:/mrtg-2.14.5/bin

#The SCE's community string
snmpCommunityString=public
```

SCA BB シグニチャ コンフィギュレーション ユーティリティ

SCA BB シグニチャ コンフィギュレーション ユーティリティ（**sigconf**）は、デフォルト DSS のインストールおよび管理を行うコマンドライン ユーティリティです。

シグニチャ コンフィギュレーション ユーティリティは、Windows 環境、Solaris 環境、Linux 環境で動作します。

インストール方法については、「SCA BB コンフィギュレーション ユーティリティのインストール方法」（P.4-7）を参照してください。

sigconf 構文

SCA BB シグニチャ コンフィギュレーション ユーティリティのコマンドライン構文は次のとおりです。

```
sigconf <operation> [--file <filename>]
```

表 13-10 に、**sigconf** 処理を示します。

表 13-11 に、**sigconf** オプションを示します。

表 13-10　sigconf 処理

処理	省略形	説明
--set-default-dynamic-signature	**-d**	このワークステーションにデフォルト DSS をインストールします。
--remove-default-dynamic-signature	—	このワークステーションからデフォルト DSS をアンインストールします。
--get-default-dynamic-signature	—	このワークステーションにインストールされているデフォルト DSS を取得します。
--help	—	ヘルプを表示して終了します。

表 13-11　sigconf のファイル オプション

ファイル オプション	省略形	説明
--file *filename*	**-f**	DSS を指定します。

sigconf の例

例 1

デフォルト DSS としてファイル new_signature.dss をインストールするには、次のように入力します。

```
sigconf --set-default-dynamic-signature --file new_signature.dss
```

例 2

インストールされているデフォルト DSS ファイルを取得して default_backup.dss として保存するには、次のように入力します。

```
sigconf --get-default-dynamic-signature --file default_backup.dss
```

SNMP、MIB、およびトラップの概要

シスコは、完全なネットワーク Fault, Configuration, Accounting, Performance, Security（FCAPS;（障害、設定、アカウンティング、パフォーマンス、セキュリティ）管理を提供します。

ネットワーク管理用のインターフェイスが 2 つ用意されています。

- コマンドライン インターフェイス（CLI）: SCE プラットフォームの前面パネルにある Console ポートまたは SCE プラットフォームへの Telnet 接続を介してアクセスできます。設定およびセキュリティ機能に使用します。
- 簡易ネットワーク管理プロトコル（SNMP）: 障害管理（SNMP トラップによる）およびパフォーマンス モニタリング機能を提供します。

SNMP

SNMP は、複雑なネットワークを管理するための一連のプロトコルです。SNMP は、Protocol Data Unit（PDU; プロトコル データ ユニット）というメッセージをネットワークのさまざまな部分に送信することで動作します。エージェントと呼ばれる SNMP 準拠デバイスは、自身に関するデータを Management Information Base（MIB; 管理情報ベース）に保存し、SNMP 要求者にこのデータを返します。

SCE プラットフォーム オペレーティング システムには、SNMP エージェントが含まれます。SNMP エージェント パラメータの設定方法および SNMP インターフェイスを有効にする方法については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Configuring the Management Interface and Security」の章または『*Cisco SCE8000 GBE Software Configuration Guide*』の「Configuring the Management Interface and Security」の章を参照してください。

MIB

管理情報ベース（MIB）はオブジェクトのデータベースであり、ネットワーク管理システムでモニタできます。SNMP は標準化 MIB 形式を使用し、MIB が定義したデバイスを標準 SNMP ツールでモニタできるようにします。

SCE プラットフォームでは次の MIB がサポートされます。

- MIB-II：RFC 1213「*Management Information Base for Network Management of TCP/IP-based Internets* 」で定義されています。
- Cisco Service Control Enterprise MIB：多くの MIB ファイルで記述されます。

シスコ独自の MIB を使用すると、外部管理システムは、SCE プラットフォームの動作ステータスとリソース利用率に関する一般情報を取得したり、帯域利用率とネットワーク統計情報のリアルタイム測定を抽出したり、クリティカル イベントとアラームの通知を受信したりできます。

SCA BB の設定およびランタイム ステータスを提供するシスコ独自の MIB 部分については、『*Cisco Service Control Application for Broadband Reference Guide*』の「SCA BB Proprietary MIB Reference」の章を参照してください。シスコ独自の MIB の他の部分については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の付録「Proprietary MIB Reference」または『*Cisco SCE8000 GBE Software Configuration Guide*』の付録「Proprietary MIB Reference」を参照してください。これらのマニュアルは、MIB のロード順についても説明しています。

トラップ

トラップは、SCE プラットフォーム内に常駐する SNMP エージェントによって生成される割り込みメッセージです。トラップは、イベントが発生すると生成されます。ネットワーク管理システムは、トラップ メッセージを受信すると、発生したイベントのログや信号の無視など、適切な処理を実行します。

SCE プラットフォームでは、トラップの 2 つの一般カテゴリがサポートされます。

- 標準 SNMP トラップ：RFC 1157 で定義され、使用する規定は RFC 1215 で定義されています。
- 独自の Cisco Service Control Enterprise トラップ：シスコ独自の MIB で定義されています。

  SNMP トラップの詳細および SNMP トラップ マネージャの設定方法については、『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Configuring the Management Interface and Security」の章にある「Configuring and Managing the SNMP Interface」または『*Cisco SCE8000 10GBE Software Configuration Guide*』の「Configuring the Management Interface and Security」の章にある「Configuring and Managing the SNMP Interface」を参照してください。

コマンドラインからの PQI ファイルのインストール

SCE プラットフォームでの SCA BB PQI ファイルのインストール

SCE プラットフォームのコマンドライン インターフェイス（CLI）を使用して、SCE プラットフォームに SCA BB PQI ファイルをインストールできます。

ステップ 1　PQI ファイルがインストールされていることを確認します。

次のうちいずれかを実行します。

- SCE プラットフォームで PQI ファイルを特定します。
- 適切な PQI ファイルを FTP で SCE にアップロードします。

ステップ 2　ライン インターフェイス コンフィギュレーション モードを開始します（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）。

ステップ 3　**pqi install file engXXXXX.pqi** と入力します。

ステップ 4　インストールが完了するまで進行状況をモニタします。

次の作業

Console のインストール後は、Network Navigator ツールを使用して PQI ファイルをインストールできます。「SCE デバイスへの PQI ファイルのインストール方法」（P.5-23）を参照してください。

ライン インターフェイス コンフィギュレーション モードの開始方法

ステップ 1　SCE プラットフォームの CLI プロンプト（`SCE#`）で **configure** と入力します。

ステップ 2　**Enter** キーを押します。

`SCE(config)#` プロンプトが表示されます。

ステップ 3　**interface LineCard 0** を入力します。

ステップ 4　**Enter** キーを押します。

`SCE(config if)#` プロンプトが表示されます。

その他のシステム コンポーネントによるサブスクライバの管理

Cisco Service Control ソリューションのその他のコンポーネントも、サブスクライバ管理の別の方法（Console の Subscriber Manager GUI ツールの使用以外）を提供します。

- Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）には、Console から使用できないオプションがあります。
- SCE プラットフォームには、幅広いサブスクライバ関連機能があります。

ここでは、SCA BB 固有のサブスクライバ管理オプションに重点を置いて、このような別の方法について概説します。詳細な説明については、該当する Service Control のマニュアルを参照してください。

- 「アノニマス サブスクライバ モード」（P.13-11）
- 「サブスクライバアウェア モード」（P.13-12）
- 「リアルタイムで使用量をモニタするサブスクライバの選択」（P.13-14）
- 「サブスクライバ CSV ファイルの管理」（P.13-16）

アノニマス サブスクライバ モード

アノニマス サブスクライバは、アノニマス サブスクライバ グループ指定に従って SCE プラットフォームが自動生成する名前を持つサブスクライバです。アノニマス サブスクライバは常に単一の IP アドレスにマッピングされます。システムはカスタマーの実際の ID を認識しません。

アノニマス グループは、指定された IP 範囲（通常は割り当てられたサブスクライバ テンプレート）です。アノニマス グループが設定されている場合に、指定された IP 範囲内の IP アドレスを持つトラフィックが検出されると、SCE プラットフォームはこのグループのアノニマス サブスクライバを生成します。このグループにサブスクライバ テンプレートが割り当てられる場合、生成されたアノニマス サブスクライバには、このテンプレートの定義に従ってプロパティが設定されます。サブスクライバ テンプレートが割り当てられない場合は、デフォルト テンプレートが使用されます。これはテンプレート インポート操作によって変更できません。最初は、パッケージ ID に 1 つずつ、200 のテンプレートが設定されています。

アノニマス サブスクライバ グループおよびサブスクライバ テンプレートは、SCE プラットフォーム コマンドライン インターフェイス（CLI）を使用して管理されます。CLI コマンドは Telnet セッションで入力できます。詳細については、『*Cisco SCE 8000 CLI Command Reference Guide*』または『*Cisco SCE 2000 and SCE 1000 CLI Command Reference Guide*』を参照してください。

CSV ファイルからアノニマス サブスクライバ グループおよびサブスクライバ テンプレートをインポートしたり、これらのファイルにサブスクライバ データをエクスポートしたりするには、次のコマンドを使用します。

- subscriber anonymous-group import csv-file
- subscriber anonymous-group export csv-file
- subscriber template import csv-file
- subscriber template export csv-file

（注）　上記の CLI コマンドは、ライン インターフェイス コンフィギュレーション コマンドです。ライン インターフェイス コンフィギュレーション モードを開始して（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）、SCE(config if)# プロンプトが表示されてからコマンドを入力してください。

アノニマス グループまたはサブスクライバ テンプレートをシステムから削除するには、次のコマンドを使用します。

- no subscriber anonymous-group [all] [name <groupname>]
- clear subscriber anonymous
- default subscriber template all

（注）　上記の CLI コマンドは、ライン インターフェイス コンフィギュレーション コマンドです。ライン インターフェイス コンフィギュレーション モードを開始して（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）、SCE(config if)# プロンプトが表示されてからコマンドを入力してください。

アノニマス サブスクライバ情報を表示するには、次のコマンドを使用します。

- show interface LineCard 0 subscriber templates [index]
- show interface LineCard 0 subscriber anonymous-group [all] [name <groupname>]
- show interface LineCard 0 subscriber amount anonymous [name <groupname>]
- show interface LineCard 0 subscriber anonymous [name <groupname>]

サブスクライバアウェア モード

サブスクライバアウェア モードの場合、各サブスクライバは外部生成名を持つ特定のカスタマーです。この外部生成名を使用すると、サブスクライバを複数の IP アドレスにマッピングしたり、識別したりすることができます。SCE プラットフォームで処理される各トラフィック セッション（単一 IP フロー、または関連する IP フロー グループ）は、設定されたサブスクライバ マッピングに基づいて、認識されたサブスクライバに割り当てられます。

これらのサブスクライバを導入してマッピングする方法は 3 つあります。

- SM GUI ツール（「SM GUI ツールの使用」（P.11-1）を参照）
- SCE プラットフォーム サブスクライバ CLI
- SM サブスクライバ 管理 CLU

SCE プラットフォーム サブスクライバ CLI

CSV ファイルからサブスクライバ データをインポートしたり、これらのファイルにサブスクライバ データをエクスポートしたりするには、次のコマンドを使用します。

```
subscriber import csv-file
subscriber export csv-file
```

（注）　上記の CLI コマンドは、ライン インターフェイス コンフィギュレーション コマンドです。ライン インターフェイス コンフィギュレーション モードを開始して（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）、SCE(config if)# プロンプトが表示されてからコマンドを入力してください。

システムからサブスクライバを削除するには、次のコマンドを使用します。

```
no subscriber [all] [name <subscriber-name>]
```

（注）　上記の CLI コマンドは、ライン インターフェイス コンフィギュレーション コマンドです。ライン インターフェイス コンフィギュレーション モードを開始して（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）、SCE(config if)# プロンプトが表示されてからコマンドを入力してください。

各基準を満たすサブスクライバを表示するには、次のコマンドを使用します。

```
show interface LineCard 0 subscriber [amount]
[prefix <prefix>] [property <propertyname> equals | greater-than | less-than
<property-val>]
show interface LineCard 0 subscriber [amount] prefix <prefix>
show interface LineCard 0 subscriber [amount] suffix <suffix>
show interface LineCard 0 subscriber mapping IP <iprange>
show interface LineCard 0 subscriber [amount] mapping intersecting IP <iprange>
show interface LineCard 0 subscriber mapping VLANid <vlanid>
```

特定のサブスクライバに関する情報を表示するには、次のコマンドを使用します。

```
show interface LineCard 0 subscriber properties
show interface LineCard 0 subscriber name <name>
show interface LineCard 0 subscriber name <name> mappings
show interface LineCard 0 subscriber name <name> counters
show interface LineCard 0 subscriber name <name> properties
```

SM サブスクライバ管理 CLU

SM サブスクライバ管理ユーティリティ（**p3subs**）は、サブスクライバを管理するための CLU です。このユーティリティを使用して、サブスクライバの追加または削除を実行できます。このユーティリティを使用すると、サブスクライバのプロパティおよびマッピングも管理できます。

p3subs の詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

p3subs 構文

p3subs は、Solaris シェル プロンプトで実行します。このユーティリティのコマンドライン構文は次のとおりです。

```
p3subs <operation> --subscriber=<Subscriber-Name> [--ip=<IP-address>]
[--property=<property-name=value>] [--domain=<domain-name>] [--overwrite]
```

次の表に、サブスクライバ管理に関連する **p3subs** の処理を示します。

表 13-12　p3subs サブスクライバ処理

処理	説明
--add	サブスクライバを追加したり、既存のサブスクライバ設定を置換します。
--set	指定サブスクライバのマッピングおよびプロパティを更新します。
--remove	指定されたサブスクライバを削除します。
--show	指定されたサブスクライバの情報を表示します。

リアルタイムで使用量をモニタするサブスクライバの選択

Real-Time Subscriber Usage RDR は、サービスごとおよびメトリックごとに単一サブスクライバのネットワーク アクティビティをリアルタイムでレポートします。モニタするサブスクライバごとに、これらの Subscriber Usage RDR の生成をイネーブルにする必要があります。

注意　多くのサブスクライバで Real-Time Subscriber Usage RDR の生成および収集を行うと、パフォーマンスが低下することがあります。Real-Time Subscriber Usage RDR の生成は、モニタする必要のあるサブスクライバに限定してイネーブルにしてください。

Real-Time Subscriber Usage RDR の生成は、`monitor` サブスクライバ プロパティで制御します。デフォルトの場合、RDR の生成はディセーブルになっています（`monitor = 0`）。RDR の生成をイネーブルにするには、このプロパティの値を 1 に変更します。

SM コマンドライン ユーティリティ（CLU）または SCE プラットフォーム CLI を使用して、選択したサブスクライバのこのプロパティを修正できます。

- 「SM によるサブスクライバ モニタリングの管理」（P.13-14）
- 「SCE プラットフォームによるサブスクライバ モニタリングの管理」（P.13-15）

SM によるサブスクライバ モニタリングの管理

Real-Time Subscriber Usage RDR の生成をイネーブルまたはディセーブルにするには、**SM p3subs** ユーティリティを使用します。サブスクライバをまとめて処理するファイルも作成できます。詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

- 「単一サブスクライバに対するサブスクライバ モニタリングのイネーブル化」（P.13-14）
- 「単一サブスクライバに対するサブスクライバ モニタリングのディセーブル化」（P.13-15）
- 「複数サブスクライバに対するサブスクライバ モニタリングのイネーブル化」（P.13-15）
- 「単一サブスクライバに対するサブスクライバがイネーブルであることの確認」（P.13-15）

単一サブスクライバに対するサブスクライバ モニタリングのイネーブル化

指定したサブスクライバのサブスクライバ モニタリングをイネーブルにできます。

ステップ 1　コマンドラインで、**sm/server/bin/p3subs --set --subscriber Smith --property monitor=1** を実行します。

単一サブスクライバに対するサブスクライバ モニタリングのディセーブル化

指定したサブスクライバのサブスクライバ モニタリングをディセーブルにできます。

ステップ 1　コマンドラインで、**sm/server/bin/p3subs --set --subscriber Smith --property monitor=0** を実行します。

複数サブスクライバに対するサブスクライバ モニタリングのイネーブル化

複数サブスクライバのモニタリングをイネーブルにできます。

ステップ 1　CLU 起動シーケンスを含むテキスト ファイル（この例では monitor.txt）を作成します。

ファイルは次のようになります。

```
p3subs --set --subscriber Jerry --property monitor=1
p3subs --set --subscriber George --property monitor=1
p3subs --set --subscriber Elaine --property monitor=1
p3subs --set --subscriber Kramer --property monitor=1
p3subs --set --subscriber Newman --property monitor=1
```

ステップ 2　コマンドラインで、**sm/server/bin/p3batch -f monitor.txt** を実行します。

単一サブスクライバに対するサブスクライバがイネーブルであることの確認

指定されたサブスクライバに対してサブスクライバ モニタリングがイネーブルかどうかを確認できます。

ステップ 1　コマンドラインで、**sm/server/bin/p3subs --show-property --subscriber Smith --property monitor** を実行します。

SCE プラットフォームによるサブスクライバ モニタリングの管理

SCE プラットフォームを使用して、Real-Time Subscriber Usage RDR の生成をイネーブルまたはディセーブルにすることもできます。詳細については、『*Cisco SCE8000 CLI Command Reference Guide*』を参照してください。

- 「単一サブスクライバに対するサブスクライバ モニタリングのイネーブル化」（P.13-15）
- 「単一サブスクライバに対するサブスクライバ モニタリングのディセーブル化」（P.13-16）
- 「複数サブスクライバに対するサブスクライバ モニタリングのイネーブル化」（P.13-16）
- 「単一サブスクライバに対するサブスクライバがイネーブルであることの確認」（P.13-16）

単一サブスクライバに対するサブスクライバ モニタリングのイネーブル化

指定したサブスクライバのサブスクライバ モニタリングをイネーブルにできます。

ステップ 1　ライン インターフェイス コンフィギュレーション モードを開始します（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）。

ステップ 2　`SCE(config if)#` プロンプトで、**subscriber name Smith property name monitor value 1** を実行します。

単一サブスクライバに対するサブスクライバ モニタリングのディセーブル化

指定したサブスクライバのサブスクライバ モニタリングをディセーブルにできます。

ステップ 1　ライン インターフェイス コンフィギュレーション モードを開始します（「ライン インターフェイス コンフィギュレーション モードの開始方法」（P.13-10）を参照）。

ステップ 2　`SCE(config if)#` プロンプトで、**subscriber name Smith property name monitor value 0** を実行します。

複数サブスクライバに対するサブスクライバ モニタリングのイネーブル化

複数サブスクライバのモニタリングをイネーブルにできます。

ステップ 1　CLI 起動シーケンスを含むテキスト ファイル（この例では monitor.txt）を作成し、適切な CLI モードにアクセスするためのコマンドを追加します。

ファイルは次のようになります。

```
configure
interface LineCard 0
subscriber name Jerry property name monitor value 1
subscriber name George property name monitor value 1
subscriber name Elaine property name monitor value 1
subscriber name Kramer property name monitor value 1
subscriber name Newman property name monitor value 1
```

ステップ 2　SCE プラットフォームの CLI プロンプト（`SCE#`）で、**script run monitor.txt** を実行します。

単一サブスクライバに対するサブスクライバがイネーブルであることの確認

指定されたサブスクライバに対してサブスクライバ モニタリングがイネーブルかどうかを確認できます。

ステップ 1　SCE プラットフォームの CLI プロンプト（`SCE#`）で、**show interface LineCard 0 subscriber name Smith properties** を実行します。

プロパティが表示されます。`monitor` が関連パラメータです。

```
Subscriber smith properties:
subscriberPackage=0
monitor=1
Subscriber 'smith' read-only properties
```

サブスクライバ CSV ファイルの管理

サブスクライバ CSV ファイルのインポートおよびエクスポートを行うには、**p3subsdb** SM ユーティリティを使用します。CSV ファイルから SM データベースに、サブスクライバ グループのサブスクライバ情報をインポートできます。SM データベースから CSV ファイルに、サブスクライバ情報をエクスポートすることもできます。

詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

CSV ファイル構造については、『*Cisco Service Control Application for Broadband Reference Guide*』の「CSV File Formats」の章を参照してください。

- 「サブスクライバ CSV ファイルのインポート」（P.13-17）
- 「サブスクライバ CSV ファイルのエクスポート」（P.13-17）

サブスクライバ CSV ファイルのインポート

ステップ 1　Solaris シェルプロンプトで、**p3subsdb --import <filename>** を実行します。

サブスクライバ CSV ファイルのエクスポート

ステップ 1　Solaris シェルプロンプトで、**p3subsdb --export <filename>** を実行します。

例：サブスクライバのフィルタリングとエクスポート

次の例では、名前が「a」で始まるすべてのサブスクライバが silverSubscriberFile.csv ファイルにエクスポートされます。

```
p3subsdb --export --prefix=a --output=silverSubscriberFile.csv
```