Cisco Security Agent 4.0.1.539-1.1.3 for Cisco CallManager Release 3.2(3)、3.3、および 4.0 のインストール

このマニュアルでは、Cisco Security Agent for Cisco CallManager 3.2(3), 3.3, および 4.0 のインストール手順および関連情報について説明します。Cisco CallManager と Cisco Customer Response Applications（CRA）が同一サーバ上に共存する場合、どちらの製品も同じセキュリティ ポリシーを使用するので、このマニュアルまたは『*Installing Cisco Security Agent 4.0.1.539-1.1(3) for Cisco Customer Response Applications Releases 2.2(5), 3.0(3), and 3.1(2)*』のマニュアルに従って、その共存サーバにエージェントをインストールすることができます。

目次

このマニュアルでは、次のトピックについて取り上げます。

Cisco Systems

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

OL-4836-02-J

はじめに

Cisco Security Agent（CSA）は、Cisco CallManager 3.2(3), 3.3, および 4.0 クラスタに対して侵入検知および侵入保護の機能を提供します。このエージェントは、一連の検証済みセキュリティ規則（ポリシー）に基づいて、Windows プラットフォームのセキュリティを実現します。ポリシーには、ホスト侵入検知と防止に関する厳密なレベルが設定されています。システム リソースへのアクセスが行われる前に、このエージェントは特定のシステム動作を許可または拒否するポリシーを適用することにより、システム運用を制御します。この処理は透過的に行われるためユーザからは見えず、システム全体のパフォーマンスにも影響しません。

（注） Cisco Security Agent for Cisco CallManager は、特に Cisco CallManager および Cisco CRA のソフトウェアに対応するよう設計されていますが、そのほかシスコが承認したサードパーティ製のアプリケーションもサポートしています。また、Web サービスおよびデータベース サービスのセキュリティも実現します。さらに、ホストベースの侵入検知システムとして機能する Network Shim がインストールされていれば、TCP/IP のセキュリティ チェックも実行します。エージェントの最新バージョンが提供されたときは、そのバージョンをインストールすることを強くお勧めします。

また、シスコが提供するオペレーティング システム サービスの最新リリースおよびアップグレードとこのエージェントを連動させることを強くお勧めします。シスコが提供するオペレーティング システム サービスのリリースとアップグレードを取得するには、表 1 を参照してください。

このマニュアルのインストール手順に従って、Cisco CallManager、Cisco CRA、リモート データベース サーバ、音声サーバ、スピーチ サーバなど、音声クラスタ内のすべてのサーバに CSA をインストールしてください。クライアント マシンにはエージェントをインストールしないでください。

Cisco Security Agent for Cisco CallManager のポリシーは、シスコが承認した多数のサードパーティ製のモニタリング ツールもサポートします。たとえば、次のアプリケーションをサポートします。

- Concord eHealth Monitor
- HP OpenView Operations Agent 7.1
- HP OpenView Performance Manager 3.3
- Integrated Research Prognosis
- McAfee VirusScan 7.0
- Micromuse Netcool
- NetIQ Vivinet Manager
- RealVNC
- Symantec Corporate Edition 8.0
- Trend Anti-Virus
- Windows Terminal Services

シスコが承認していないサードパーティ製のソフトウェア ツールを使用する場合は、Management Center for Cisco Security Agent（CSA MC）を購入してインストールする必要があります。また、シスコが承認したサードパーティ製のアプリケーションをサポートするようにポリシーをカスタマイズする方法については、Cisco Technical Assistance Center（TAC）にお問い合せください。TAC へのお問い合せについては、P.15 の「テクニカル サポート」を参照してください。CSA MC への移行の詳細については、P.9 の「Management Center for Cisco Security Agent への移行」を参照してください。

インストールを始める前に

Cisco Security Agent for Cisco CallManager をインストールする前に、次の情報を確認してください。

- Cisco Security Agent は、Cisco Media Convergence Server（MCS）およびシスコが承認したカスタマー向けのサーバをサポートします（これらの MCS やカスタマー向けのサーバには、Cisco CallManager Releases 3.2(3), 3.3(x), または 4.0、およびシスコが提供するオペレーティング システム バージョン 2000.2.4（またはそれ以降）をインストールする必要があります）。ただし、『*Cisco CallManager Compatibility Matrix*』に別途指示がある場合は、それに従います。『*Cisco CallManager Compatibility Matrix*』を入手するには、表 1 を参照してください。
- このセキュリティ エージェントは、Cisco CallManager および Cisco Customer Response Solutions /Cisco Customer Response Applications を実行している共存サーバも含め、Cisco CallManager クラスタ内のすべてのサーバにインストールしてください。
- 最初にエージェントをパブリッシャ データベース サーバにインストールし、そのインストールが正常に完了したことを確認してください。次に、エージェントをすべてのサブスクライバ サーバに 1 台ずつ順次インストールしてください。
- エージェントのインストールは、オペレーティング システムのインストールと Cisco CallManager のインストールの間には行わないでください。
- Cisco CallManager をアップグレードする前に、P.7 の「Cisco Security Agent サービスの無効化と有効化」の手順を実行して Cisco Security Agent を無効にする必要があります。また、Cisco CallManager のインストール中は、サービスを有効に戻さないでください。

注意

オペレーティング システム、Cisco CallManager、メンテナンス リリース、サービス リリース、サポート パッチ、プラグインなどのソフトウェアをインストール、アンインストール、またはアップグレードする前に、Cisco Security Agent のサービスを無効にする必要があります。

エージェントを無効にするには、P.7 の「Cisco Security Agent サービスの無効化と有効化」の手順を実行する必要があります。インストールまたはアップグレード中は、サービスを有効に戻さないでください。このときサービスを有効に戻すと、インストールまたはアップグレードで問題が発生する可能性があります。

ソフトウェアをインストールまたはアップグレードした後は、Cisco Security Agent サービスを有効に戻す必要があります。

サービスが無効になっていると、エージェントはサーバへの侵入を検知しません。

- Cisco CallManager 3.2(3) から Cisco CallManager 3.3 にアップグレードする場合、サーバでエージェントを実行しているときは、アップグレードを実施する前に Cisco Security Agent サービスを無効にする必要があります。Cisco CallManager 3.3 へのアップグレードによりエージェントが削除されるので、アップグレードが完了したら、クラスタ内のすべてのサーバに Cisco Security Agent を再インストールしてください。
- Cisco CallManager 3.3(2) から Cisco CallManager 3.3(3) または 4.0 にアップグレードする場合、サーバでエージェントを実行しているときは、アップグレードを実施する前に Cisco Security Agent サービスを無効にする必要があります。ただし、この場合、アップグレードの後にエージェントを再インストールする必要はありません。アップグレードが完了したら、必ず Cisco Security Agent サービスを有効にしてください。
- エージェントをインストールまたはアップグレードする前に、Cisco CallManager　のデータをバックアップしてください。この作業の実行方法の詳細については、該当バージョンの Cisco CallManager のバックアップに関するマニュアルを参照してください。Cisco CallManager のバックアップに関するマニュアルを入手するには、表 1 を参照してください。

- エージェントをインストールまたはアップグレードする前に、クラスタ内で実行するすべてのアプリケーションをバックアップしてください。詳細については、バックアップに関する該当のマニュアルを参照してください。
- Terminal Services を使用してエージェントをインストールまたはアップグレードしないでください。シスコは Terminal Services をインストールしますが、これは、Cisco Technical Assistance Center が管理タスクや設定タスクをリモートで実行できるようにするためです。また、Integrated Lights Out を使用してエージェントをインストールまたはアップグレードしないでください。

  必要な場合は、Virtual Network Computing（VNC）を使用してエージェントをインストールまたはアップグレードすることができます。VNC のマニュアルを入手するには、表 1 を参照してください。

注意 サーバで Cisco HIDS Agent（Entercept）を実行している場合は、Cisco Security Agent をインストールする前に、Add/Remove Programs からこのソフトウェアをアンインストールする必要があります。Cisco HIDS Agent をアンインストールせずに Cisco Security Agent をインストールすると、TCP スタックが削除されるため、セキュリティに必要なファイアウォール コンポーネントがインストールされません。

- エージェントのインストールにより、CPU の使用率が一時的に上昇します。コール処理の中断を最小限に抑えるために、エージェントのインストールは、コール処理が最小の時間帯に行うことをお勧めします。エージェントは、ソフトウェアのインストール直後からサーバの保護を開始しますが、サーバをリブートしなければ、エージェントの機能は完全には動作しません。

（注） サーバをリブートすると、コール処理が中断される場合があります。そのため、サーバのリブートは、営業時間の終了後、またはコール処理が最小の時間帯に実行することをお勧めします。

- エージェントをアップグレードするか、サーバにエージェントを再インストールするには、事前にエージェントをアンインストールしてから、ソフトウェアを再インストールする必要があります。

  Add/Remove Programs、または Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Security Agent を使用してエージェントをアンインストールする際に、アンインストールの確認を求めるプロンプトが表示されます。ここで、Yes をクリックして保護を無効にするには、一定時間内に Yes をクリックする必要があります。No を選択するか、保護が無効になるまで待つ場合は、セキュリティ モードが自動的に有効になります。

注意 ソフトウェアをアンインストールしたら、すぐにサーバをリブートしてください。サーバをすぐにリブートしないと、Windows 2000 のシステム トレイにはフラグが引き続き表示され、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）の Message タブにはエラーが表示されますが、この状態では、ソフトウェアによる保護は機能しません。

- インストール後に、エージェント設定タスクを実行する必要はありません。ソフトウェアはすぐに正常に作動します。セキュリティ ログがエージェント GUI の Message タブおよび Microsoft Event Viewer に表示され、security.txt ファイル（C:\Program Files\Cisco\CSAgent\log）にも記録されます。
- Cisco IP Telephony Applications Backup Utility は、エージェントが生成したログ ファイルやテキスト ファイルをバックアップしません。

何らかの理由で Cisco CallManager のデータをサーバに復元する場合は、Cisco CallManager のデータを復元した後に、エージェントを再インストールする必要があります。

ヒント エージェントのインストールまたはアンインストールに関する問題が発生した場合は、P.12 の「トラブルシューティング」を参照してください。

Cisco Security Agent のインストール

必要項目：Web からダウンロードした実行可能ファイル

確実にインストールするために、P.3 の「インストールを始める前に」の情報を再確認してください。Cisco Security Agent for Cisco CallManager をインストールするには、次の手順を実行します。

手順

ステップ 1 CallManager サーバから、http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml の「Voice Software Download URL」にアクセスします。

（注） Cisco Security Agent およびポリシーは、ボイス製品の Cryptographic Software サイトに掲載されています。このサイトには、音声アプリケーション（Cisco CallManager、CRS など）のソフトウェア ウィンドウからナビゲートできます。

ステップ 2 最新バージョンの Cisco Security Agent のファイル **CiscoCM-CSA-<version>-K9.exe** をダウンロードします。

たとえば、CiscoCM-CSA-4.0.1.nnn-1.n-K9.exe をダウンロードします。4.0.1.nnn-1.n はエージェントおよびポリシーのバージョンを表しています。

ステップ 3 ダウンロードしたファイルの保存先を書き留めます。

ステップ 4 ダウンロードしたファイルをダブルクリックしてインストールを開始します。

ステップ 5 Welcome ウィンドウが表示されたら、**Next** をクリックします。

ステップ 6 **Yes** をクリックして使用許諾契約に同意します。

ステップ 7 ソフトウェアのインストール先を選択し、**Next** をクリックします。

ステップ 8 **Next** をクリックして Network Shim をインストールします。

注意 エージェントの全機能を利用するには、Network Shim をインストールする必要があります。

ステップ 9 選択したオプションがステータス ウィンドウに表示されます。現在の設定値を受け入れる場合は、**Next** をクリックします。

ステップ 10 インストールが完了するまで待ちます。Cancel はクリックしないでください。

ステップ 11 **Yes** をクリックしてサーバをリブートします。

注意 サーバのリブートは、必要に応じて、営業時間の終了後に実行してもかまいません。サーバをリブートすると、コール処理が中断される場合があるためです。エージェントは、ソフトウェアのインストール直後からサーバの保護を開始しますが、サーバをリブートしなければ、エージェントの機能は完全には動作しません。

ステップ 12 **Finish** をクリックします。

ヒント インストールが完了すると、Windows 2000 のシステム トレイに赤色のフラグが表示されます。また、ソフトウェアがインストールされたとこは、Add/Remove Programs ウィンドウでも確認できます。ソフトウェアのインストールが完了していれば、このウィンドウに Cisco Security Agent が表示されます。

ステップ 13 この手順をクラスタ内の各サーバに対して実行します。

Cisco Security Agent サービスの無効化と有効化

ソフトウェアのインストール、アップグレード、アンインストールなど、サーバの再起動が必要な作業を実行する際には、CSA サービスを無効にしておく必要があります。CSA サービスが無効になっているときに、Cisco CallManager サーバのモニタリングを再開するには、事前に CSA サービスを有効に戻してください。

注意 オペレーティング システム、Cisco CallManager、メンテナンス リリース、サービス リリース、サポート パッチ、プラグインなどのソフトウェアをインストール、アンインストール、またはアップグレードする前に、この項の手順に従って Cisco Security Agent のサービスを無効にする必要があります。インストールまたはアップグレード中は、サービスを有効に戻さないでください。このときサービスを有効に戻すと、インストールまたはアップグレードで問題が発生する可能性があります。

ソフトウェアをインストール、アップグレード、またはアンインストールした後は、Cisco Security Agent サービスを有効に戻す必要があります。

サービスが無効になっていると、エージェントはサーバへの侵入を検知しません。

注意 次の手順を各サーバに対して 1 台ずつ順次実行することをお勧めします。ソフトウェアのインストール、アップグレード、またはアンインストールが完了したら、そのサーバのサービスを有効に戻します。続いて、次のサーバのサービスを無効にして同様にソフトウェアのインストール、アップグレード、またはアンインストールを実行します。

CSA サービスを無効にするには、次の手順を実行します。

手順

ステップ 1 **Start > Settings > Control Panel > Administrative Tools > Services** を選択します。

ステップ 2 Services ウィンドウで **Cisco Security Agent** を右クリックし、**Properties** を選択します。

ステップ 3 Properties ウィンドウに General タブが表示されていることを確認します。

ステップ 4 Service Status 領域で **Stop** をクリックします。

ステップ 5 Startup type ドロップダウン リストボックスから **Disabled** を選択します。

ステップ 6 **OK** をクリックします。

注意 Service ウィンドウで、CSA サービスの Startup Type が無効になっていることを確認します。

ステップ 7 この手順を、Cisco CallManager をインストールまたはアップグレードする対象の各サーバに対して実行します。

注意 ソフトウェアをインストール、アップグレード、またはアンインストールしたサーバについては、ステップ 4 に戻り、そこで **Start** をクリックして Cisco Security Agent サービスを有効に戻す必要があります。

Cisco Security Agent サービスの一時停止と再開

サービスを一時停止すると、そのサービスは仮死状態になります。サーバをリブートすると、仮死状態となったサービスは自動的に再開します。CSA サービスを一時停止するのは、サーバの再起動が不要な作業を実行する場合だけです。CSA サービスを一時停止するには、コマンド プロンプトで *net stop* コマンドを使用するか、または、Windows タスクバーの CSA アイコンの Suspend Security メニュー オプションを使用します。

注意 サーバでソフトウェアをインストール、アンインストール、またはアップグレードする場合は、事前に CSA サービスを停止する際にサービスを一時停止しないでください。これらの作業を実施する場合は、前項の手順に従ってエージェントを無効にしてください。

サーバにインストールされているエージェントのバージョンの確認

サーバにインストールされているエージェントのバージョンを確認するには、**C:\utils\MCSver.exe** ファイルを実行します。

Cisco Security Agent のアップグレード

Cisco Security Agent をアップグレードする前に、次の作業を実行してください。

1. サーバにインストールされている現在のバージョンをアンインストールします。
   P.11 の「Cisco Security Agent のアンインストール」を参照してください。
2. サーバに新しいバージョンをインストールします。
   P.5 の「Cisco Security Agent のインストール」を参照してください。

Management Center for Cisco Security Agent への移行

Cisco CallManager に含まれているセキュリティ エージェントは、変更や表示ができない静的ポリシーを使用します。Cisco Security Agent for Cisco CallManager に含まれている規則やポリシーを追加、削除、表示する場合、またはシスコが承認していないサードパーティ製のアプリケーションに対するサポートを追加する場合は、Management Center for Cisco Security Agent（CSA MC）を購入してインストールする必要があります。

CSA MC は次の 2 つのコンポーネントで構成されています。

- Management Center。このコンポーネントは、セキュアなサーバにインストールされ、Web サーバ、構成データベース、および Web ベースのインターフェイスを持っています。Management Center によって、規則やポリシーを定義することができます。また、他のネットワーク システムやサーバにインストールされているエージェントに配布するためのエージェント キットを作成することもできます。
- Cisco Security Agent（管理対象エージェント）。このコンポーネントは、クラスタ内のすべての Cisco CallManager サーバにインストールされ、セキュリティ ポリシーを運用します。管理対象エージェントは Management Center に登録され、ポリシーや規則のアップデートを受信します。また、Management Center にイベント ログ レポートを送信します。

作業を始める前に、次に示す CSA MC のマニュアルの最新版を入手する必要があります。

- *Installing Management Center for Cisco Security Agents*
- *Using Management Center for Cisco Security Agents*
- *Release Notes for Management Center for Cisco Security Agents*

これらのマニュアルは、
http://www.cisco.com/en/US/customer/products/sw/cscowork/ps5212/prod_technical_documentation.html からダウンロードできます。

Cisco CallManager 環境では、Management Center コンポーネントは別々のセキュアなサーバにインストールし、管理対象エージェント コンポーネントはクラスタ内のすべての Cisco CallManager サーバにインストールする必要があります。Management Center として使用するサーバは、『*Installing Management Center for Cisco Security Agents*』に記載されているシステム要件を満たしていなければなりません。

注意 Management Center は、Cisco CallManager がインストールされているサーバにはインストールしないでください。そのようなインストールを実行しようとすると、CSA MC のインストール時に、サーバで実行中の Microsoft SQL Server が検出され、CSA MC のインストールが自動的に打ち切られます。

CSA MC のパッケージとマニュアルを入手したら、次の手順を実行します。

ステップ 1 個々のサーバ（Cisco CallManager 以外のサーバ）で、「Cisco Security Agent のアンインストール」の項で説明する手順に従って、Cisco Security Agent をアンインストールします（インストールされている場合）。

ステップ 2 Cisco CallManager のポリシーを記述した最新版の XML ファイルをダウンロードします。このポリシーは、http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml の「Voice Software Download URL」で入手できます。

（注） Cisco Security Agent およびポリシーは、ボイス製品の Cryptographic Software サイトに掲載されています。このサイトには、音声アプリケーション（Cisco CallManager、CRS など）のソフトウェア ウィンドウからナビゲートできます。

ステップ 3 ダウンロードしたファイルの保存先を書き留めます。

ステップ 4 『*Installing Management Center for Cisco Security Agents*』の「MC installation」の項に記載されている手順に従って、CSA MC をインストールします。

ステップ 5 ステップ 2 でダウンロードしたポリシーを、『*Using Management Center for Cisco Security Agents*』の手順に従ってインポートします。

ステップ 6 『*Installing Management Center for Cisco Security Agents*』の「Quick Start Configuration」の項に従って、次の作業を実行します。

- グループの設定
- グループへのポリシーの追加
- エージェント キットの構築

ステップ 7 ステップ 6 で作成された新しい管理対象エージェントを、『*Installing Management Center for Cisco Security Agents*』の「Cisco Security Agent Installation and Overview」の項に記載されている手順に従って、配布およびインストールします。

Cisco Security Agent のアンインストール

注意 現在インストールされているバージョンに対して、同じバージョンのエージェントをインストールすることはできません。エージェントをアンインストールしてから、ソフトウェアを再インストールする必要があります。エージェントをアンインストールする場合は、アンインストールの確認を求めるプロンプトが表示されます。ここで、Yes をクリックして保護を無効にするには、一定時間内に Yes をクリックする必要があります。No を選択するか、保護が無効になるまで待つ場合は、セキュリティ モードが自動的に有効になります。

ソフトウェアをアンインストールしたら、すぐにサーバをリブートしてください。サーバをすぐにリブートしないと、Windows 2000 のシステム トレイにはフラグが引き続き表示され、GUI の Message タブにはエラーが表示されますが、この状態では、ソフトウェアによる保護は機能しません。

セキュリティ エージェントをアンインストールするには、次の手順を実行します。

手順

ステップ 1 次のいずれかの作業を実行します。

- **Start > Control Panel > Add/Remove Programs** を選択し、Cisco Security Agent に対して **Remove** をクリックし、ステップ 2 に進みます。
- **Start > Programs > Cisco Systems > Cisco Security Agent > Uninstall Cisco Security Agent** を選択し、ステップ 2 に進みます。

ステップ 2 **Yes** をクリックしてエージェントを停止します。

ステップ 3 **Yes** をクリックしてエージェントをアンインストールします。

ステップ 4 サーバをリブートします。

注意 ソフトウェアをアンインストールしたら、すぐにサーバをリブートしてください。サーバをすぐにリブートしないと、Windows 2000 のシステム トレイにはフラグが引き続き表示され、GUI の Message タブにはエラーが表示されますが、この状態では、ソフトウェアによる保護は機能しません。

トラブルシューティング

エージェントのインストールまたはアンインストールに関する問題が発生した場合は、次の作業を実行してください。

- サーバをリブートしたことを確認します。
- ソフトウェアのインストールまたはアップグレードに Terminal Services を使用しなかったことを確認します。
- インストールの前に Cisco HIDS Agent（Entercept）をアンインストールしたことを確認します。
- C:\Program Files\Cisco\CSAgent\log のインストール ログを入手します。
  Cisco Security AgentInstallInfo.txt ファイルおよび driver_install.log ファイルの内容を検査します。
- インストールの場合、Network Shim がインストールされていることを確認します。
  driver_install.log には、csanet2k.inf がインストールされたことが記述されていなければなりません。Network Shim がインストールされていない場合は、エージェントをアンインストールしてから再インストールしてください。

Cisco Security Agent の追加情報の入手

Cisco Security Agent の追加情報を入手するには、次の手順を実行します。

手順

ステップ 1 次のいずれかの作業を実行します。

- Windows 2000 のシステム トレイで、フラグを右クリックし、**Open Control Panel** を選択し、ステップ 2 に進みます。
- **Start > Programs > Cisco Systems > Cisco Security Agent > Cisco Security Agent** を選択し、ステップ 2 に進みます。

ステップ 2 ウィンドウの右上隅にある **?** アイコンをクリックします。

Cisco Security Agent のマニュアルが表示されます。

ヒント Cisco Security Agent 4.0 のマニュアルを入手するには、次の URL をクリックしてください。

http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html

Cisco CallManager の関連マニュアルの入手

表 1 に記載されている URL をクリックすると、Cisco CallManager の関連マニュアルにナビゲートできます。

表 1　URL のクイック リファレンス

関連情報およびソフトウェア	URL および追加情報
オペレーティング システムのマニュアルおよび Virtual Network Computing（VNC）のマニュアル （readme マニュアルではありません）	http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/index.htm
Cisco MCS のデータシート	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
ソフトウェア専用のサーバ（IBM、HP、Compaq、Aquarius）	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html
Cisco CallManager Compatibility Matrix	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager のマニュアル	http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm
Cisco CallManager のバックアップと復元に関するマニュアル	http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm
Cisco CallManager、SQL Server、オペレーティング システムのサービス リリース、アップグレード、readme に関するマニュアル	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml （注）オペレーティング システムおよび SQL Server 2000 のサービス リリースは、ボイス製品オペレーティング システムの Cryptographic Software ページに掲載されています。このページには、Cisco CallManager ソフトウェア ページからナビゲートできます。
Cisco IP テレフォニー アプリケーションに関するマニュアル	http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm
Cisco Integrated Communications System（ICS）7750	http://www.cisco.com/univercd/cc/td/doc/product/voice/ics/index.htm

マニュアルの入手

マニュアルやその他の技術リソースを入手したり、テクニカル サポートを受けたりするには、いくつか方法があります。ここでは、シスコシステムズから技術情報を入手する方法を紹介します。

Cisco.com

マニュアルの最新版は、WWW の次の URL で参照できます。

http://www.cisco.com/univercd/home/home.htm

シスコ Web サイトには、次の URL からアクセスできます。

http://www.cisco.com

各国のシスコ Web サイトには、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

マニュアルの発注方法

マニュアルの発注方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコのマニュアルは、次の方法でご発注いただけます。

- Cisco.com 登録ユーザ（シスコの直接顧客）は、Networking Products MarketPlace からシスコ製品のマニュアルを発注できます。
  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Assistance Center（TAC）の 24 時間テクニカル サポートを、オンラインと電話で利用することができます。Cisco.com は、オンラインのテクニカル サポートの最初の窓口として、Cisco TAC Web サイトを運営しています。

Cisco TAC Web サイト

Cisco TAC Web サイト（http://www.cisco.com/tac）は、オンラインのマニュアルやツールを提供することで、シスコ製品とその技術に関するトラブルシューティングを容易にします。Cisco TAC Web サイトは、年間を通して 1 日 24 時間利用できます。

Cisco TAC Web サイトのすべてのツールへのアクセスには、Cisco.com へのユーザ ID とパスワードが必要です。ログイン ID およびパスワードを取得されていない場合は、次の URL で登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

TAC Case ツールの利用

オンラインの TAC Case Open ツール（http://www.cisco.com/tac/caseopen）を使用すると、P3 と P4 の事例を短時間で検索できます（ご使用のネットワークの負荷が最小限であること、または製品情報を要求していること）。ユーザが状況を入力すると、TAC Case Open ツールがその状況をすぐに打開するために、自動的に迅速な解決策を提示します。これらの推奨事項で解決できない場合は、Cisco TAC のエンジニアが対応します。

P1 または P2 レベルの問題が発生した場合（ネットワークがダウンした、または機能が著しく低下した）、またはインターネットでアクセスできない場合は、Cisco TAC に電話で問い合せください。Cisco TAC の担当者がすぐに P1 および P2 の問題に対応し、業務をスムーズに遂行できるようにサポートします。

電話で問い合せるには、次の電話番号のいずれかを使用します。

アジア太平洋地域：+61 2 8446 7411（オーストラリア：1 800 805 227）
欧州アフリカ地域：+32 2 704 55 55
米国：1 800 553-2447

Cisco TAC の連絡先一覧は、次の URL を参照してください。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC の不具合の優先レベルの定義

すべての問題が標準のフォーマットで報告されるように、問題の優先レベルを定義しています。

優先レベル 1（P1）：使用中のネットワークが停止したために、お客様の業務に深刻な影響を及ぼしている。シスコはお客様と協力して、必要なリソースをすべて投入し、24 時間体制で問題を解決します。

優先レベル 2（P2）：使用中のネットワークのパフォーマンスが著しく低下したり、またはシスコ製品の不十分なパフォーマンスのために、お客様の業務に重大な悪影響を及ぼしている。シスコはお客様と協力して、問題解決のために、通常の営業時間内で専任のリソースを投入します。

優先レベル 3（P3）：ネットワークのパフォーマンスが低下したが、ほとんどの業務運用が機能している。シスコはお客様とともに、通常の営業時間内にリソースを投入して、サービスを満足いくレベルまで回復させます。

優先レベル 4（P4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要である。業務にほとんど影響しない、または影響しない。

その他の出版物や情報の入手

シスコの製品、技術、およびネットワーク ソリューションに関する情報は、各種オンラインで、また、出版物として入手できます。

- *Cisco Product Catalog* は、シスコシステムズが提供するネットワーク製品とその注文方法、およびカスタマー サポート サービスについて説明しています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- *Cisco Press* は、ネットワークに関する書籍を広範囲にわたって出版しています。初心者のユーザおよび熟練したユーザに次の書籍をお勧めします：『*Internetworking Terms and Acronyms Dictionary*』、『*Internetworking Technology Handbook*』、『*Internetworking Troubleshooting Guide*』、『*Internetworking Design Guide*』。現行の Cisco Press の発行書籍とその他の情報は、次の URL で Cisco Press online から参照できます。

  http://www.ciscopress.com

- 『*Packet*』は、シスコが 3 ヶ月に 1 回発行している出版物です。ネットワーク分野の最新動向、技術的な進展、シスコ製品、およびソリューションを提供することで、業界のプロフェッショナルがネットワーク事業への投資を最大限に活かすための情報を記載しています。これには、ネットワークの配置、トラブルシューティングのヒント、コンフィギュレーション例、お客様のケース スタディ、チュートリアルとトレーニング、認定情報、および詳細なオンライン リソースへの数多くのリンクが含まれています。『*Packet*』は、次の URL で参照いただけます。

  http://www.cisco.com/go/packet

- 『*iQ Magazine*』は、シスコが 2 ヶ月に 1 回発行している出版物で、インターネット ビジネス戦略に関する最新情報を企業の経営者に提供しています。『*iQ Magazine*』には、次の URL からアクセスできます。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、シスコシステムズが 3 ヶ月ごとに発行している雑誌で、パブリック インターネットおよびプライベート インターネット、パブリック イントラネットおよびプライベート イントラネットの設計、開発、運用に携わるエンジニアリングのプロフェッショナルを対象としています。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- トレーニング：ネットワーキングの高水準なトレーニングを提供しています。ネットワーク トレーニングの最新内容は、次の URL で参照できます。

  http://www.cisco.com/en/US/learning/index.html

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。
本書とあわせてご利用ください。

Cisco Connection Online Japan
http://www.cisco.com/japanese/manuals/

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

シスコシステムズマニュアルセンター
http://www2.hipri.com/cisco/

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合せください。

CISCO SYSTEMS

シスコシステムズ株式会社
URL:http://www.cisco.com/jp/
問合せ URL:http://www.cisco.com/jp/service/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL.03-5549-6500　FAX.03-5549-6501

OL-4836-02-J