アクセス コントロール リスト

この章では、アクセスコントロールリストのシステムサポートについて説明し、それらの設定方法を示します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。次に説明する手順を使用する前に、サービスモデルに最適な設定例を選択する必要があります。

重要 ACL を設定するためのライセンスは必要ありません。ただし、設定されている ACL の数は、パフォーマンスに大きく影響する可能性があります。

重要 すべてのコマンドとキーワード/変数を使用できるわけではありません。可用性はプラットフォームのタイプによって異なります。

この章は、次の項で構成されています。

概要

IP アクセスリスト（一般にアクセスコントロールリスト（ACL）と呼ばれる）は、システムに出入りするパケットのフローを制御します。これらはコンテキストごとに設定され、フィルタ基準に一致するパケットに対して実行されるアクションを制御する「ルール」（ACL ルール）またはフィルタで構成されます。設定が完了すると、ACL を次のいずれかに適用できます。

- 個別のインターフェイス
- コンテキストによって促進されるすべてのトラフィック（ポリシー ACL と呼ばれる）

- 個々のサブスクライバ
- 特定のコンテキストによって促進されるすべてのサブスクライバセッション

IPv4 と IPv6 のアクセスルートに個別の ACL を作成できます。

ACL の概要

この項では、システム上の ACL に関する 2 つの重要な側面について説明します。

- ルール （2 ページ）
- ルールの順序 （4 ページ）

重要 完全なコマンドシンタックスについては、『*Command Line Interface Reference*』の「*ACL Configuration Mode Commands*」および「*IPv6 ACL Configuration Mode Commands*」の章を参照してください。

ルール

単一の ACL は、1 つ以上の ACL ルールで構成されます。各ルールは、パケットが特定の基準に一致した場合に、特定のアクションを実行するように設定されたフィルタです。ACL ごとに最大 256 のルールを設定できます。

重要 ルールなしで構成されている設定済み ACL は、「deny any」ルールを示します。**deny** アクションおよび **any** 基準については、このセクションの後半で説明します。これは、空の ACL のデフォルトの動作です。

各ルールは、指定された基準にパケットが一致した場合に、実行するアクションを指定します。この項では、システムでサポートされているルールアクションと基準について説明します。

アクション

ACL は、指定された基準に一致するパケットに対して、次のいずれかのアクションを実行できるように指定します。

- **許可**：パケットは受け入れられ、処理されます。
- **拒否**：パケットは拒否されます。
- **リダイレクト**：パケットは特定のシステムインターフェイスまたは処理のために指定されたコンテキストを介して、指定されたネクストホップアドレスに転送されます。

重要 リダイレクトルールは、特定のサブスクライバ、特定のコンテキストによって促進されるすべてのサブスクライバ、またはUMTSサブスクライバ用の APN に適用される ACL の場合は無視されます。

基準

各 ACL は、パケットの比較基準を指定する 1 つまたは複数のルールで構成されます。

サポートされる基準は次のとおりです。

- **Any**：すべてのパケットをフィルタ処理します。
- **Host**：送信元ホストの IP アドレスに基づいてパケットをフィルタ処理します。
- **ICMP**：Internet Control Message Protocol（ICMP）のパケットをフィルタ処理します。
- **IP**：Internet Protocol（IP）パケットをフィルタ処理します。
- **Source IP Address**：1 つ以上の送信元 IP アドレスに基づいてパケットをフィルタ処理します。
- **TCP**：Transport Control Protocol（TCP）パケットをフィルタ処理します。
- **UDP**：User Datagram Protocol （UDP）パケットをフィルタ処理します。

上記の基準それぞれについては、以降の項で詳しく説明します。

重要 次の項では、基本的な ACL ルールのシンタックスについて説明します。コマンドシンタックスの詳細については、『*Command Line Interface Reference*』の「*ACL Configuration Mode Commands*」の章と「*IPv6 ACL Configuration Mode Commands*」の章を参照してください。

- **Any**：すべてのパケットにルールが適用されます。
- **Host**：IP アドレスによって決定される特定のホストにルールが適用されます。
- **ICMP**：特定の Internet Control Message Protocol（ICMP）パケット、タイプ、またはコードにルールが適用されます。ICMP のタイプとコードの定義については、*www.iana.org*（RFC 3232）を参照してください。
- **IP**：特定の Internet Protocol（IP）パケットまたはフラグメントにルールが適用されます。
- **IP Packet Size Identification Algorithm**：転送時にフラグメンテーションの特定の Internet Protocol（IP）パケット ID にルールが適用されます。

  この設定は、サブスクライバパケットがカプセル化されている場合（モバイル IP やその他のトンネリングカプセル化など）に、システムで使用される「IP ID フィールド」割り当てアルゴリズムに関連しています。システム内では、サブスクライバパケットのカプセ

ル化は分散型の方法で行われ、16 ビットの IP ID 空間が分割されてカプセル化を行う各エンティティに分散されるため、カプセル化時に一意の IP ID 値を IP ヘッダーに割り当てることができます。

この分散型の IP ID 空間は小規模であるため、ゼロ以外の一位の ID は、転送時にフラグメント化される可能性があるパケットのみに割り当てられます。これは、IP ID フィールドは、フラグメント化されたパケットのリアセンブルにのみ使用されるためです。IP パケットの合計サイズは、そのパケットがフラグメント化される可能性を判断するために使用されます。

- **Source IP Address**：特定の送信元アドレスまたは送信元アドレスのグループから発信される特定のパケットにルールが適用されます。
- **TCP**：任意の Transport Control Protocol（TCP）トラフィックにルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。TCP ポート番号の定義については、*www.iana.org* を参照してください。
- **UDP**：任意の User Datagram Protocol（UDP）トラフィックにルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。UDP ポート番号の定義については、*www.iana.org*を参照してください。

ルールの順序

複数のルールで 1 つの ACL を構成できます。各パケットは、一致が見つかるまで、各 ACL ルールを入力した順序で比較されます。一致が特定されると、後続のすべてのルールは無視されます。

追加のルールを既存の ACL に追加し、次のいずれかのオプションを使用して適切に順序付けすることができます。

- Before
- After

これらの配置オプションを使用するには、ACL 内に既存のルールを指定し、次のフローに示すように新しいルールを設定する必要があります。

[before | after] { *existing_rule* **}**

システム上での ACL の設定

ここでは、ACL の設定方法について説明します。

重要 この項では、システムでアクセスコントロールリストを設定するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*ACL Configuration Mode Commands*」の章と「*IPv6 ACL Configuration Mode Commands*」の章を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 の設定例に従って、アクセスコントロールリストを作成します。ACL の作成 （5 ページ）

ステップ 2 の設定例に従って、ACL リスト内のアクションのルールと基準を指定します。サブスクライバトラフィックのアクションと基準の設定 （5 ページ）

ステップ 3 オプションです。システムには、コンテキストへのすべてのパケットのデフォルトフィルタとして機能する「未定義」 ACL が用意されています。デフォルトのアクションは「permit all」です。の設定例に従って、「未定義」ACL のデフォルト設定を変更します。未定義の ACL の設定 （6 ページ）

ステップ 4 の手順に従って、ACL の設定を確認します。ACL 設定の確認 （6 ページ）

ステップ 5 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

ACL の作成

ACL を作成するには、システム CLI の Exec モードから次のコマンドシーケンスを入力します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      { ip | ipv6 } access-list acl_list_name
      end
```

注：

- コンテキストごとに設定できる ACL の最大数は、VPN Manager ソフトウェアタスクで使用可能なメモリ量によって制限されます。通常は、最大 200 未満です。

サブスクライバトラフィックのアクションと基準の設定

サブスクライバトラフィックを拒否/許可するルールを作成し、アクションの前後にルールを適用するには、システム CLI の Exec モードから次のコマンドシーケンスを入力します。

```
configure
  context acl_ctxt_name [ -noconfirm ]
    { ip | ipv6 } access-list acl_list_name
      deny { ip_address | any | host | icmp | ip | log | tcp | udp }
      permit { ip_address | any | host | icmp | ip | log | tcp | udp }
      after { deny | permit | readdress | redirect }
      before { deny | permit | readdress | redirect }
      end
```

注：

⚠

注意 ACL で指定されていない限り、システムは「deny any」ルールを適用しません。この動作は、ACL の最後に「deny any」ルールを追加することによって変更できます。

- ACL ごとに設定できるルールの最大数は、ACL がどのように使用されるかによって異なります。詳細については、「エンジニアリングルール」の章を参照してください。
- ACL を構成するルールを設定するには、アクションと基準に表示される情報を使用します。詳細については、『*Command Line Interface Reference* 』の「*Acl configuration mode commands*」および「*IPv6 acl configuration mode commands*」の章を参照してください。

未定義の ACL の設定

前述のように、システムでは、適用されている ACL が存在しない場合に、パケットのフィルタリングに「未定義」の ACL メカニズムが使用されます。このシナリオは、設定プロセス中に ACL 名が誤って入力されたなどの誤設定が原因である可能性があります。

このような状況に備えて、システムには、コンテキストへのすべてのパケットのデフォルトフィルタとして機能する「未定義」の ACL が用意されています。デフォルトのアクションは「permit all」です。

確認できない ACL のデフォルトの動作を変更するには、次の設定を使用します。

```
configure
  context acl_ctxt_name [-noconfirm]
    access-list undefined { deny-all | permit-all }
    end
```

注：

- コンテキスト名は、変更する「未定義」の ACL を含むコンテキストの名前です。詳細については、『*Command Line Interface Reference*』の「*Context Configuration Mode Commands* 」の章を参照してください。

ACL 設定の確認

ACL の設定を確認するには、Exec モードの **show { ip | ipv6 } access-list** コマンドを入力します。

次に、このコマンドの出力例を示します。この例では、*acl_1* という名前の ACL が設定されています。

```
ip access list acl_1
   deny host 10.2.3.4
   deny ip any host 10.2.3.4
   permit any 10.2.4.4
1 ip access-lists are configured.
```

IP ACL の適用

ACL を設定した後、有効にするには、ACL を適用する必要があります。

重要 これらの手順を開始する前に、システム上での ACL の設定 （4 ページ）の手順に従って、すべての ACL を設定し、検証する必要があります。また、次に示す手順では、サブスクライバが事前に設定されていることも前提としています。

前述のように、次のいずれかに ACL を適用できます。

- 個々のインターフェイスへの ACL の適用 （9 ページ）
- コンテキスト内のすべてのトラフィックへの ACL の適用 （11 ページ） （ポリシー ACL として知られている）
- 個々のサブスクライバへの ACL の適用 （13 ページ）
- 複数のサブスクライバへの単一 ACL の適用 （18 ページ）
- 複数のサブスクライバへの単一 ACL の適用 （18 ページ） （3GPP サブスクライバの場合のみ）

重要 ACLは、適用先のサブスクライバやインターフェイス内の同じコンテキストで設定する必要があります。同様に、コンテキストに適用される ACL は、そのコンテキストで設定する必要があります。

ACL が単一のコンテキスト内の複数のレベルで適用される場合（ACL がコンテキスト内のインターフェイスに適用され、コンテキスト全体に別の ACL が適用されるなど）、次の図と表に示すように処理されます。

図 *1 : ACL* の処理順序

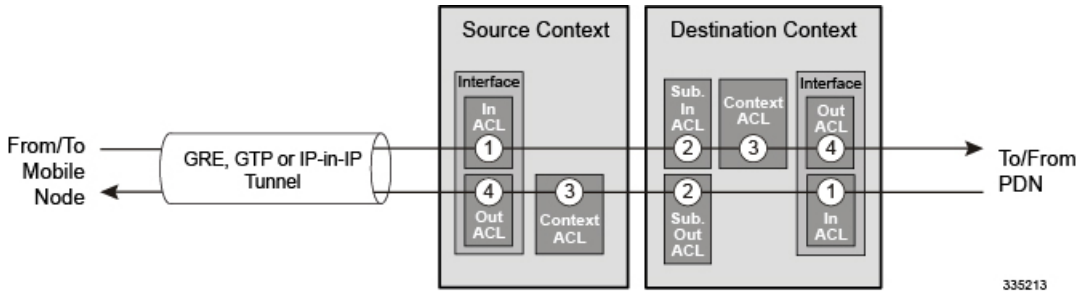

表 *1 : ACL* の処理順序の説明

モバイルノードからパケットデータネットワークに着信するパケット（左から右）	
順序	説明
1	送信元コンテキストの受信インターフェイス用に設定されたインバウンド ACL は、トンネリングされたデータ（外部 IP ヘッダーなど）に適用されます。その後、パケットは接続先コンテキストに転送されます。
2	サブスクライバに対して設定されたインバウンド ACL（特定のサブスクライバまたはコンテキストによって促進された任意のサブスクライバのいずれか）が適用されます。
3	接続先コンテキストで設定されたコンテキスト ACL（ポリシー ACL）は、転送前に適用されます。
4	パケットが転送される接続先コンテキストのインターフェイスに設定されたアウトバウンド ACL が適用されます。
パケットデータネットワークからモバイルノードに着信するパケット（右から左）	
順序	説明
1	接続先コンテキストで設定された受信インターフェイス用に、設定されたインバウンド ACL が適用されます。
2	サブスクライバに対して設定されたアウトバウンド ACL（特定のサブスクライバまたはコンテキストによって促進された任意のサブスクライバのいずれか）が適用されます。その後、パケットは送信元コンテキストに転送されます。
3	送信元コンテキストで設定されたコンテキスト ACL（ポリシー ACL）は、転送前に適用されます。
4	パケットが転送される送信元コンテキストのインターフェイスに設定されたアウトバウンド ACL が、トンネリングされたデータ（外部 IP ヘッダーなど）に適用されます。

設定されていない IP ACL が適用されている場合（たとえば、適用された ACL の名前が誤って設定されている場合）、システムはパケットのフィルタリングに「未定義」の ACL メカニズムを使用します。

この項では、ACL の適用および「未定義」の ACL の設定に関する情報と手順を示します。

インターフェイスへの ACL の適用

ACL をインターフェイスに適用するには、次の設定を使用します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      interface interface_name
         { ip | ipv6 } access-group acl_list_name { in | out } [ preference
]
         end
```

注：

- コンテキスト名は、ACL を適用するインターフェイスを含む ACL コンテキストの名前です。
- 適用する ACL は、このコマンドで指定されたコンテキストで設定する必要があります。
- ACL 内に設定されているルールの数が、そのインターフェイスの 128 ルールの制限を超えていない場合、最大 16 の ACL をグループに適用できます。

個々のインターフェイスへの ACL の適用

この項では、システムに設定されている個々のインターフェイスに 1 つまたは複数の ACL を適用するための情報と手順について説明します。

重要 この項では、システム上のインターフェイスに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Ethernet Interface Configuration Mode Commands*」の章を参照してください。

サブスクライバに ACL ファシリティを提供するようにシステムを設定するには、次のようにします。

手順

ステップ 1 設定例に従って、設定されたアクセスコントロールリストを適用します。 インターフェイスへの ACL の適用 （9 ページ）

ステップ 2 ステップに従って、ACL がインターフェイスに適切に適用されていることを確認します。 インターフェイス上の ACL 設定の確認 （10 ページ）

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

インターフェイス上の ACL 設定の確認

この項では、ACL 設定を確認する方法について説明します。

手順

Exec モードで、次のコマンドを入力します。

```
[local]host_name# show configuration context context_name
```

context_name は、ACL が適用されたインターフェイスを含むコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      service-redundancy-protocol
      exit
      interface interface_name
         ip address ip_address/mask
         exit
      subscriber default
      exit
      aaa group default
      exit
      gtpp group default
      end
```

コンテキストへの ACL の適用

ACL をコンテキストに適用するには、次の設定を使用します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      { ip | ipv6 } access-group acl_list_name [ in | out ] [ preference ]
      end
```

注：

- コンテキスト名は、ACL を適用するインターフェイスを含む ACL コンテキストの名前です。

- コンテキストレベルの ACL は、発信パケットに適用されます。これは、フロー一致基準が失敗して再度転送された場合にも、着信パケットに適用されます。

  in キーワードと **out** キーワードは廃止されており、後方互換性のためにのみ存在します。

  コンテキスト ACL は、次の場合に適用されます。

  - 外部ソースへの発信パケット。
  - 失敗したフローが一致し、再度転送される着信パケット。この場合、コンテキスト ACL が最初に適用され、通過した場合のみパケットが転送されます。

    転送中に、ACL ルールが宛先アドレスとしてループバックアドレスとして追加されると、コンテキスト ACL も適用されます。これは、StarOS がカーネル宛てのパケットをフォワーディング ルックアップで処理するためです。ACL ルールを着信パケットに適用するには、コンテキスト ACL の代わりにインターフェイス ACL を使用する必要があります。

- 適用する ACL は、このコマンドで指定されたコンテキストで設定する必要があります。
- ACL 内で設定されているルールの数が、そのインターフェイスの 256 ルールの制限を超えていない場合、最大 16 の ACL をグループに適用できます。

コンテキスト内のすべてのトラフィックへの ACL の適用

この項では、システム上の特定のコンテキスト内で設定されたコンテキストに 1 つ以上の ACL を適用する手順について説明します。適用される ACL（ポリシー ACL と呼ばれる）には、コンテキストによって容易になるすべてのトラフィックに適用されるルールが含まれています。

重要 この項では、コンテキスト内のすべてのトラフィックに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Context Configuration Mode Commands*」の章を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 の説明に従って、設定された ACL を適用します。コンテキストへの ACL の適用 （10 ページ）

ステップ 2 の説明に従って、ACL がインターフェイスに適切に適用されていることを確認します。コンテキストでの ACL 設定の確認 （12 ページ）

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

コンテキストでの ACL 設定の確認

ACL の設定を確認するには：

手順

Exec モードで次のコマンドを入力して、ACL リストが適切に適用されていることを確認します。

```
[local]host_name# show configuration context context_name
```

context_name は、ACL が適用されたコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      service-redundancy-protocol
      exit
      interface interface_name
         ip address ip_address/mask
         exit
      subscriber default
      exit
      aaa group default
      exit
      gtpp group default
               end
```

RADIUS ベースのサブスクライバにおける ACL の適用

IP ACL は、プロファイル内の属性を介してサブスクライバに適用されます。サブスクライバプロファイルは、システム上にローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。

ACL を RADIUS ベースのサブスクライバに適用するには、**フィルタ ID** 属性を使用します。

この属性の詳細については、『*AAA Interface Administration and Reference*』を参照してください。

この項では、プロファイルがシステム上でローカルに設定されている個々のサブスクライバに ACL を適用するための情報と手順について説明します。

重要 この項では、コンテキスト内のすべてのトラフィックに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Subscriber Configuration Mode Commands*」の章を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 設定例に従って、設定されたアクセスコントロールリストを適用します。個々のサブスクライバへの ACL の適用 （13 ページ）

ステップ 2 ステップに従って、ACL がインターフェイスに適切に適用されていることを確認します。個々のサブスクライバへの ACL 設定の確認 （13 ページ）

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

個々のサブスクライバへの ACL の適用

ACL を個々のサブスクライバに適用するには、次の設定を使用します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      subscriber name subs_name
         { ip | ipv6 } access-group acl_list_name [ in | out ]
         end
```

注：

- コンテキスト名は、ACL を適用するインターフェイスを含む ACL コンテキストの名前です。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- 適用する ACL は、このコマンドで指定されたコンテキストで設定する必要があります。
- ACL 内で設定されているルールの数が、そのインターフェイスの 128 ルールの制限を超えていない場合、最大 8 つの ACL をグループに適用できます。

個々のサブスクライバへの ACL 設定の確認

次の手順は、ACL の設定を確認するために使用されます。

手順

Exec モードで次のコマンドを入力して、ACL リストが適切に適用されていることを確認します。

```
[local]host_name# show configuration context context_name
```

context_name は、ACL が適用されたサブスクライバ *subs1* を含むコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      service-redundancy-protocol
      exit
      interface interface
         ip address ip_address/mask
         exit
      subscriber default
      exit
      subscriber name subscriber_name
         ip access-group access_group_name in
         ip access-group access_group_name out
         exit
      aaa group default
      exit
      gtpp group default
      exit
      content-filtering server-group cfsg_name
         response-timeout response_timeout
         connection retry-timeout retry_timeout
               end
```

default というサブスクライバへの ACL の適用

この項では、*default* という名前のサブスクライバに ACL を適用する方法について説明します。

重要 この項では、コンテキスト内のすべてのトラフィックに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Subscriber Configuration Mode Commands*」を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 設定例に従って、設定されたアクセスコントロールリストを適用します。 default というサブスクライバへの ACL の適用 （15 ページ）

ステップ 2 ステップに従って、ACL がインターフェイスに適切に適用されていることを確認します。 default というサブスクライバに対する ACL 設定の確認 （15 ページ）

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

default というサブスクライバへの ACL の適用

default というサブスクライバに ACL を適用するには、次の設定を使用します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      subscriber name subs_name
         { ip | ipv6 } access-group acl_list_name [ in | out ]
         end
```

注：

- コンテキスト名は、ACL を適用するインターフェイスを含む ACL コンテキストの名前です。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- 適用する ACL は、このコマンドで指定されたコンテキストで設定する必要があります。
- ACL 内で設定されているルールの数が、そのインターフェイスの 256 ルールの制限を超えていない場合、最大 16 の ACL をグループに適用できます。

default というサブスクライバに対する ACL 設定の確認

次の手順は、ACL の設定を確認するために使用されます。

手順

Exec モードで次のコマンドを入力して、ACL リストが適切に適用されていることを確認します。

```
[local]host_name# show configuration context context_name
```

context_name は、ACL が適用された default というサブスクライバを含むコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      service-redundancy-protocol
      exit
      interface interface
         ip address ip_address/mask
         exit
      subscriber name default
         ip access-group access_group_name in
         ip access-group access_group_name out
         exit
      aaa group default
      exit
      gtpp group default
      exit
      content-filtering server-group cfsg_name
         response-timeout response_timeout
         connection retry-timeout retry_timeout
               end
```

サービス指定のデフォルトのサブスクライバへの ACLの適用

この項では、さまざまなシステムサービスによって「デフォルト」のプロファイルとして使用されるサブスクライバへの ACL の適用について説明し、手順を示します。

重要 この項では、コンテキスト内のすべてのトラフィックに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Subscriber Configuration Mode Commands*」の章を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 default というサブスクライバへの ACL の適用 （14 ページ） の設定例に従って、設定されたアクセスコントロールリストを適用します。

ステップ 2 サービス指定のデフォルトのサブスクライバへの ACL 設定の確認 （17 ページ）の手順に従って、ACL がインターフェイスに正しく適用されていることを確認します。

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

サービス指定のデフォルトのサブスクライバへの ACLの適用

ACL をサービス指定のデフォルトサブスクライバに適用するには、次の設定を使用します。

```
configure
   context acl_ctxt_name [ -noconfirm ]
      { pdsn-service | fa-service | ha-service } service_name
         default subscriber svc_default_subs_name
         exit
      subscriber name svc_default_subs_name
         { ip | ipv6 } access-group acl_list_name [ in | out ]
         end
```

注：

- コンテキスト名は、ACL を適用するインターフェイスを含む ACL コンテキストの名前です。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- 適用する ACL は、このコマンドで指定されたコンテキストで設定する必要があります。
- ACL 内で設定されているルールの数が、そのインターフェイスの 128 ルールの制限を超えていない場合、最大 8 つの ACL をグループに適用できます。

サービス指定のデフォルトのサブスクライバへの ACL 設定の確認

ACL の設定を確認します。

手順

Exec モードで次のコマンドを入力して、ACL リストが適切に適用されていることを確認します。

```
[local]host_name# show configuration context context_name
```

context_name は、ACL が適用されたデフォルトのサブスクライバとともにサービスが含まれているコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      interface interface
         ip address ip_address/mask
         exit
      subscriber default
      exit
```

```
subscriber name subscriber_name
   ip access-group access_group_name in
   ip access-group access_group_name out
   exit
pdsn-service service_name
   default subscriber subscriber_name
         end
```

複数のサブスクライバへの単一 ACL の適用

前の項で説明したように、IP ACL は、プロファイル内の属性を介してサブスクライバに適用されます。サブスクライバプロファイルは、システム上にローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。

システムには、特定の属性が個々のサブスクライバのプロファイルに含まれていない場合にデフォルト値として機能するサブスクライバ機能の設定が用意されています。次の表で、これらの機能について説明します。

表 *2*:「デフォルト」サブスクライバ属性を提供するために使用される機能

機能	説明
default という名前のサブスクライバ	システムは各コンテキスト内に *default* というサブスクライバを作成し *default* というサブスクライバのプロファイルには、そのコンテキスト されたサブスクライバの属性値の設定テンプレートが備わっていま RADIUS ベースのサブスクライバプロファイルに含まれていないサブ イバ属性は、*default* というサブスクライバに定義されている属性の値 て設定されます。 **注**：*default* というサブスクライバのプロファイルを使用してローカル されているサブスクライバの欠落情報を提供することはできません。
default subscriber	このコマンドを使用すると、複数のサービスが複数のプロファイルの 「default」サブスクライバ情報を取得できます。

適切に設定されている場合は、上の表に記載されている機能を使用して ACL を以下に適用することができます。

- *default* というサブスクライバのプロファイルに ACL を適用することで、特定のコンテキスト内で促進されたすべてのサブスクライバ。
- サブスクライバのプロファイルに ACL を適用した後、**default subscriber** コマンドを使用してそのサブスクライバを「デフォルト」のプロファイルとして使用するように設定することで促進されたすべてのサブスクライバ。

複数のサブスクライバへの APN を介した ACL の適用

APN を介して複数のサブスクライバに ACL を適用するには、次の設定を使用します。

```
configure
  context dest_context_name [-noconfirm]
    apn apn_name
      { ip | ipv6 } access-group acl_list_name [ in | out ]
      end
```

注：

- 適用する ACL は、APN の接続先コンテキスト内にある必要があります（APN が設定されているコンテキストとは異なる場合があります）。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- このコマンドは、1 つの ACL のみをサポートします。ただし、ACL には最大 256 のルールを設定できます。
- 各 APN に対して 4 つのアクセスグループを適用できます。次に例を示します。

  ip access-group acl_list_name_1 in

  ip access-group acl_list_name_2 out

  ipv6 access-group acl_list_name_3 in

  ipv6 access-group acl_list_name_4 out

複数のサブスクライバへの APN を介した ACL の適用

IP ACL がプロファイル内の属性を使用してサブスクライバに適用される場合、サブスクライバプロファイルは、システム上にローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。

設定時間を短縮するために、代わりに ACL を GGSN サブスクライバの APN テンプレートに適用することができます。設定されている場合、APN テンプレートによって促進されたサブスクライバパケットには、関連付けられた ACL が適用されます。

この項では、APN テンプレートに ACL を適用する方法について説明します。

重要 この項では、コンテキスト内のすべてのトラフィックに ACL リストを適用するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*Subscriber Configuration Mode Commands*」の章を参照してください。

サブスクライバにアクセスコントロールリストの機能を提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 複数のサブスクライバへの APN を介した ACL の適用 （18 ページ） の設定例に従って、設定されたアクセスコントロールリストを適用します。

ステップ 2 APN への ACL 設定の確認 （20 ページ） のステップに従って、ACL がインターフェイスに適切に適用されていることを確認します。

ステップ 3 Exec モードの **save configuration** コマンドを使用して、設定をフラッシュメモリ、外部メモリデバイス、またはネットワークの場所に保存します。詳細については、「設定の確認と保存」の章を参照してください。

APN への ACL 設定の確認

ACL の設定を確認するには：

手順

Exec モードで次のコマンドを入力して、ACL リストが適切に適用されていることを確認します。

show configuration context *context_name*

context_name は、ACL が適用されたデフォルトのサブスクライバを持つ APN *apn1* を含むコンテキストの名前です。

このコマンドの出力には、コンテキスト全体の設定が表示されます。インターフェイス設定に関するコマンドの出力を確認します。このコマンドは、この手順を使用して適用された ACL を表示します。

```
configure
   context context_name
      ip access-list acl_name
         deny host ip_address
         deny ip any host ip_address
         exit
      ip access-group access_group_name
      interface interface
         ip address ip_address/mask
         exit
      subscriber default
      exit
      apn apn_name
         ip access-group access_group_name in
         ip access-group access_group_name out
               end
```

VPP でのインターフェイス ACL サポート

リリース 21.13 以降、インターフェイス ACL は VPP でサポートされています。

（注） 既存の ACL 設定 CLI コマンド、 **readdress** と **redirect** は VPP ではサポートされていません。ACL コマンドの詳細については『*Command Reference Guide*』を参照してください。

翻訳について
このドキュメントは、米国シスコ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。