Cisco Service Control Application for Broadband ユーザ ガイド

Release 3.1
May 2007

Text Part Number: OL-7205-05-J

CONTENTS

はじめに

May 30, 2007, OL-7205-05-J

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。

内容は次のとおりです。

対象読者

このガイドでは、SCA BB で作成され使用されるデータ構造について説明します。対象読者は次のとおりです。

- Cisco Service Control ソリューションの日常的な運用を担当している管理者
- SCA BB のアプリケーションを開発するインテグレータ

マニュアルの変更履歴

Service Control リリース	Part Number	発行日
Release 3.1.0	OL-7205-05	2007 年 5 月

変更内容

次の機能を追加しました。

- 仮想リンク（「仮想リンクの管理」[p.9-47] を参照）
- 非対称ルーティング分類モード（p.10-34）
- NetFlow（「NetFlow Export の管理」[p.8-4] を参照）
- クォータ補充の分散（p.9-54）

次のセクションを更新しました。

- 帯域幅の管理（p.9-31）
- システム モードの設定についての情報（p.10-34）
- 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.10-40）

Service Control リリース	Part Number	発行日
Release 3.0.5	OL-7205-04	2006 年 11 月

変更内容

次の機能を追加しました。

- SCA BB リアルタイム モニタ設定ユーティリティ（p.13-5）

次のセクションを更新しました。

- トラフィックの制御（p.3-14）

Service Control リリース	Part Number	発行日
Release 3.0.3	OL-7205-03	2006 年 5 月

変更内容

次の機能を追加しました。

- SLI の中断のないアップグレード（p.4-18）
- コンテンツ フィルタリングの概要（p.7-60）

- サービス セキュリティ ダッシュボード（p.10-2）

次の機能を削除しました。

- 攻撃フィルタリングおよびサブスクライバ通知

次の項を追加しました。

- Version 3.0.0 から Version 3.0.3 へのアップグレード

Service Control リリース	Part Number	発行日
Release 3.0.0	OL-7205-02	2005 年 12 月

変更内容

マニュアル名を『*Cisco Service Control Application for Broadband ユーザ ガイド*』に変更しました。

Cisco Service Control Application for Broadband (SCA BB) のルック アンド フィールおよび機能性はバージョン 3.0 向けのものでした。このため、このマニュアルは大幅に改訂されました。主な変更内容は次のとおりです。

- 2.5.5 リリース ユーザ ガイドの付録 B、C、D を新しいマニュアル（『*Cisco Service Control Application for Broadband Reference Guide*』）に移動しました。
- 2.5.5 リリース ユーザ ガイドの第 8 章および付録 A を新しいマニュアル（『*Cisco Service Control Application Suite Reporter User Guide*』）に移動しました。
- 『*Cisco Service Control Application Suite for Broadband Installation Guide*』が廃止され、「使用する前に」の章に統合されました。
- 2.5.5 リリース ユーザ ガイドの第 5 章「*Constructing Service Configurations*」は大幅に変更され、3 つの章に分割されました。
- Console の新しいツールである Network Navigator ツールおよび Signature Editor ツールに関する新たな章が追加されました。

Service Control リリース	Part Number	発行日
Release 2.5.5	OL-7205-01	2005 年 2 月

変更内容

『*Cisco Service Control Application Suite for Broadband ユーザ ガイド*』が作成されました。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

表 1

章	タイトル	
第 1 章	概要	Service Control ソリューションの概要を示します。
第 2 章	システムの概要	Service Control ソリューションの機能的な概要を示します。
第 3 章	トラフィック処理の概要	Service Control ソリューションの技術的な概要を示します。
第 4 章	使用する前に	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。
第 5 章	Network Navigator の使用	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。
第 6 章	Service Configuration Editor の使用	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。
第 7 章	Service Configuration Editor の使用方法：トラフィックの分類	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。
第 8 章	Service Configuration Editor の使用法：トラフィックのアカウンティングと レポート	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。
第 9 章	Service Configuration Editor の使用法：トラフィックの制御	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。
第 10 章	Service Configuration Editor の使用法：その他のオプション	Service Configuration Editor のオプションを説明します。
第 11 章	Subscriber Manager の GUI ツールの使用方法	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。
第 12 章	Signature Editor の使用方法	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。
第 13 章	その他の管理ツールおよびインターフェイス	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

Cisco Service Control Application for Broadband には次のマニュアルがあります。

- 『*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*』
- 以下の 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 4xGBE Installation and Configuration Guide*』
  - 『*Cisco SCE 2000 4/8xFE Installation and Configuration Guide*』
- 『*Cisco Service Control Engine (SCE) CLI Command Reference*』
- 『*Cisco Service Control Engine (SCE) Software Configuration Guide*』

表記法

このガイドでは、次の表記法を使用しています。

- コマンド、キーワード、およびボタンは**太字**で示しています。
- 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。
- 画面に表示される情報の例は `screen` フォントで示しています。
- ユーザが入力する情報の例は**太字**の **`screen`** フォントで示しています。
- 縦棒（|）は、選択要素の区切りを示しています。
- 角カッコ（[ ]）内の要素は省略可能です。
- 波カッコ（{}）内の要素は必須の選択肢です。
- 角カッコ内の波カッコ（[{}]）は省略可能な要素の中の必須選択肢を表します。

（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。

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。

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。

警告 **「*危険*」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。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。**

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアス、および一般的なシスコ マニュアルついては、下記のサイトで毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。この資料には、新規および改訂版の技術マニュアルの一覧が示されています。

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

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/

CHAPTER 1

概要

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、および Cisco Service Control ソリューションを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 の概念について

Cisco Service Control のソリューション

Cisco Service Control ソリューションは、サービス プロバイダーが直面するさまざまなサービス コントロールの課題を解決する専用ハードウェア、および特定のソフトウェア ソリューションが組み合わされて実現されます。SCE プラットフォームの設計目的は、インターネット /IP トラフィックの分類、分析、および制御をサポートすることです。

サービス プロバイダーは Service Control を使用することにより、既存インフラストラクチャに投資しながら、利益を上げる仕組みを新規に作成することができます。また、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、および制御することもできます。さらに、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するために必要なツールも利用できます。

電気通信業界の低迷が示すように、IP サービス プロバイダーのビジネス モデルが利益を上げるためには、モデルの再編が必要となります。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働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。ただし、IP サービスから実際に利益を得るには、データ リンク上でこれらのサービスを単に実行するだけでなく、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が必要となります。シスコが提供する Service Control ソリューションを使用すると、サービス プロバイダーはこのギャップを埋めることができます。

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

住宅およびビジネスのカスタマーをターゲットとし任意のアクセス技術（DSL、ケーブル、モバイル端末など）を持つサービス プロバイダーは、拡張 IP サービスによってサービスを差別化しながら、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新たなレベルのサービス インテリジェンスおよび制御機能が追加され、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　　サービスおよび保証アプリケーション SLA の提供
- 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、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および BSS/OSS システムと Service Control ソリューションとの統合の簡素化

Service Control の機能

Cisco Service Control ソリューションの中心には、専用ネットワーク ハードウェア デバイスである SCE があります。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保守したり、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 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、常に変化するサービス プロバイダー環境において新規サービスおよびアプリケーションを容易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 には公開され、マニュアルが整備されている一連の API が用意されていて、迅速かつ強固な統合プロセスを実行できます。
- 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。

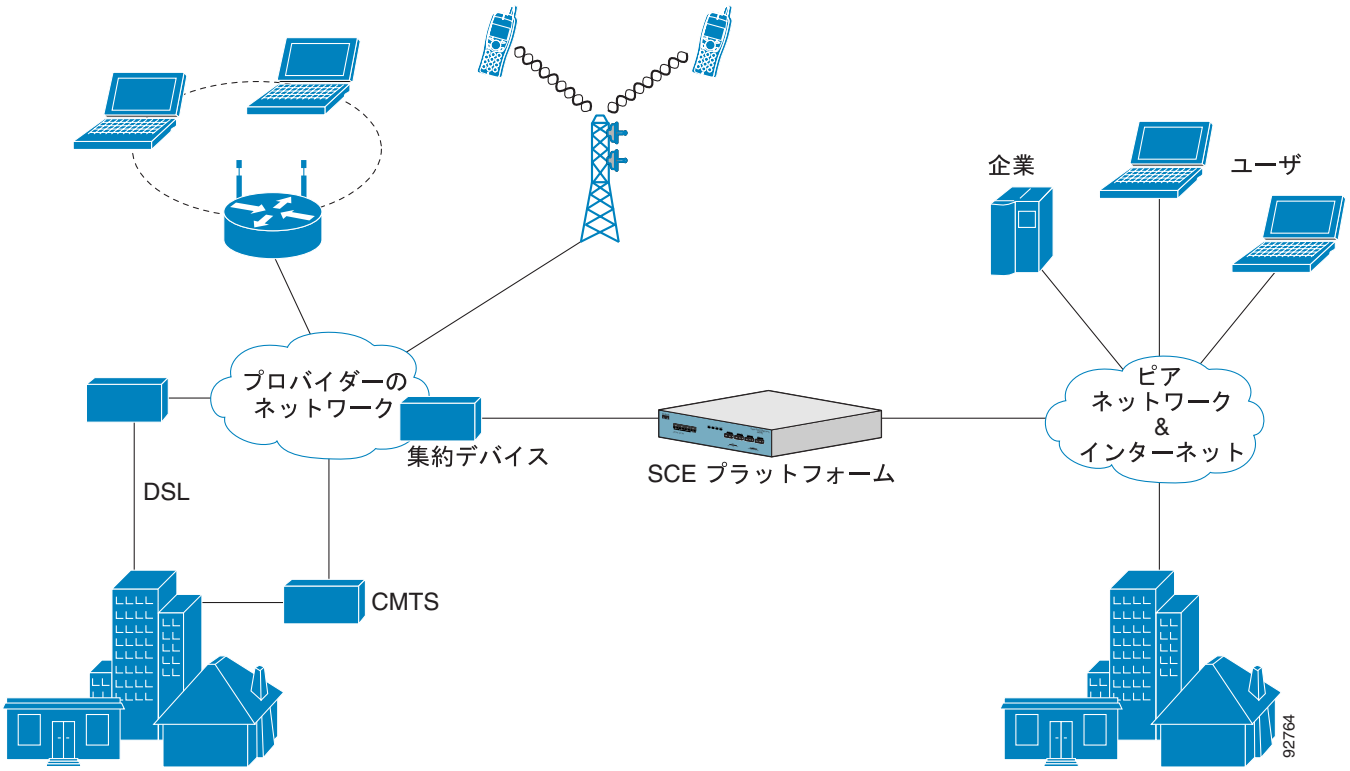
SCE プラットフォーム

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 プラットフォームは Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）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）プロセッサを利用する専用ネットワーク デバイスです。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。双方向トラフィック フローにプログラム可能なステートフル 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により、SCE プラットフォームはネットワーク使用率をリアルタイムで分類できます。この情報は 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 のステートフル ワイヤ速度パケット 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 / アプリケーションの確実なサポート
  - 一般的なプロトコル / アプリケーション ― HTTP、HTTPS、FTP、TELNET、NNTP、SMTP、POP3、IMAP、WAP など
  - P2P ファイル シェアリング ― 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 ― RTSP、SIP、HTTP ストリーミング、RTP/RTCP など
- プログラム可能なシステム コアによる、レポートおよび帯域幅の柔軟な制御
- 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

次の図に、ネットワーク内の SCE プラットフォームの配置例を示します。

図 1-1


企業
ユーザ
プロバイダーの
ネットワーク
集約デバイス
SCE プラットフォーム
ピア
ネットワーク
&
インターネット
DSL
CMTS
92764

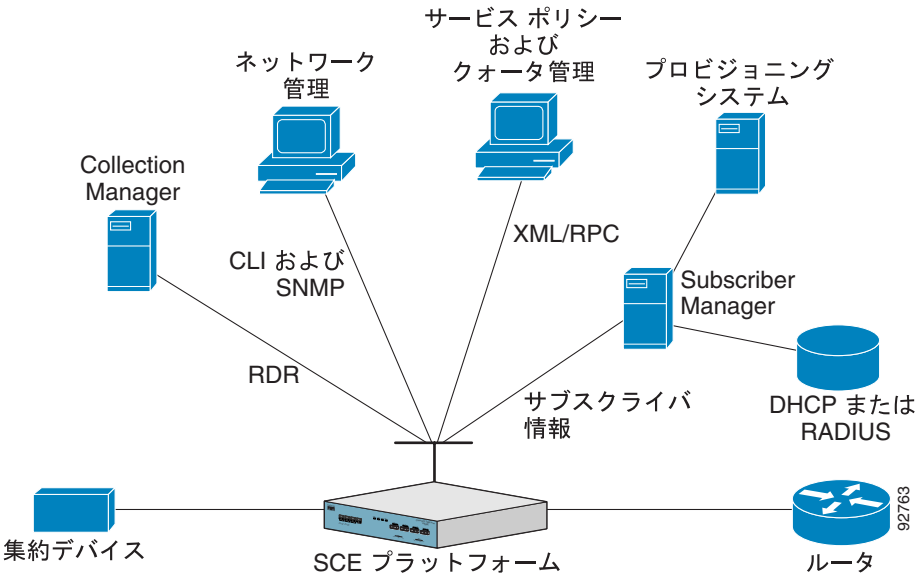
管理と収集について

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



- ネットワーク管理（p.1-6）
- サブスクライバの管理（p.1-7）
- サービス コンフィギュレーションの管理（p.1-7）
- データ収集（p.1-7）

ネットワーク管理

シスコは、完全なネットワーク FCAPS 管理（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）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。

- Command-Line Interface（CLI）— 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。
- 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。

サブスクライバの管理

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の管理

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。こうした簡単で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が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使いやすい 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

Service Control ソリューションは SCE プラットフォームの使用状況データおよび統計情報を生成し、単純な TCP ベース プロトコル（Raw Data Record [RDR] プロトコル）を使用して RDR として転送します。Cisco Service Control Management Suite（SCMS）Collection Manager（CM）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 を待ち受けて、ローカル マシン上でそれらを処理する収集システムが実装されたものです。データは格納されて分析およびレポート機能に使用されたり、収集されて課金など別の OSS システムに提供されます。

CHAPTER 2

システムの概要

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とポリシーのダイナミック バインディング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、DHCP 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します。

  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 Solution 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 プラットフォームの Raw Data Record（RDR）を受信す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。

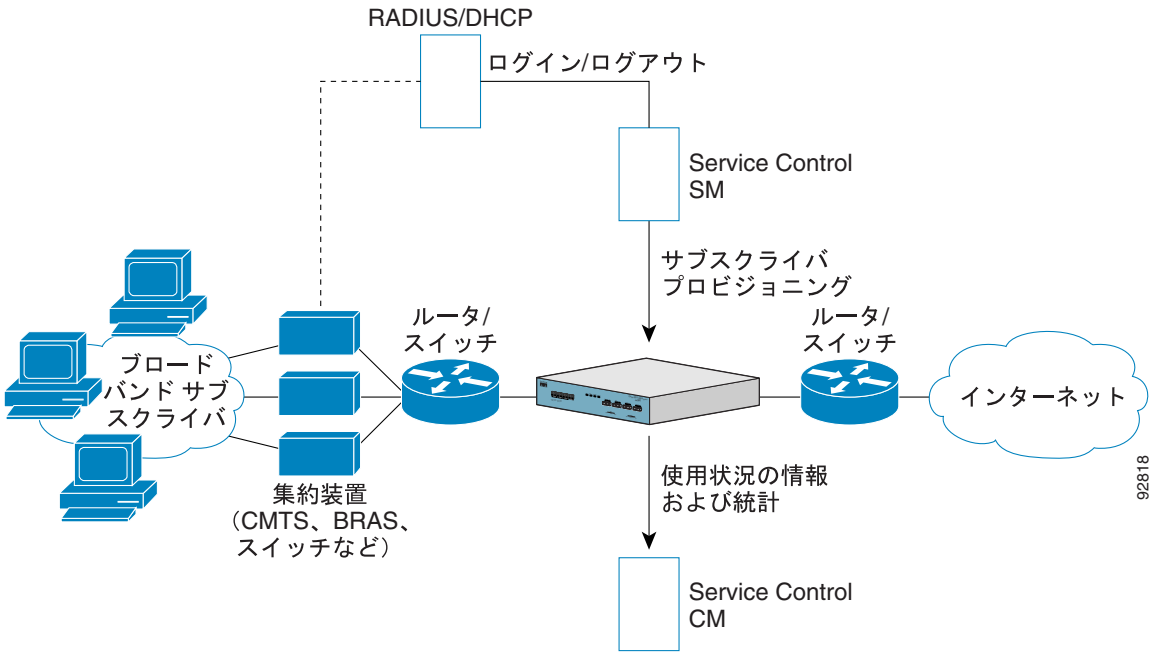
- Service Control Application（SCA）Reporter — CM が格納したデータを処理し、このデータの詳細なレポートのセットを提供するソフトウェア コンポーネント。SCA Reporter は、単独実行することも Console に統合して実行することもできます。

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。

次に、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 モードについて

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。SCAS 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したり、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したり、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 プラットフォームを解決するときに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 プラットフォームを解決するときだけ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 クォータ トラッキングが不要な場合や、IP レベルでの分析が十分な場合、またはオフラインで IP アドレス / サブスクライバ バインディングが実行可能な場合に使用します。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 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（OSS 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

次の表に、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

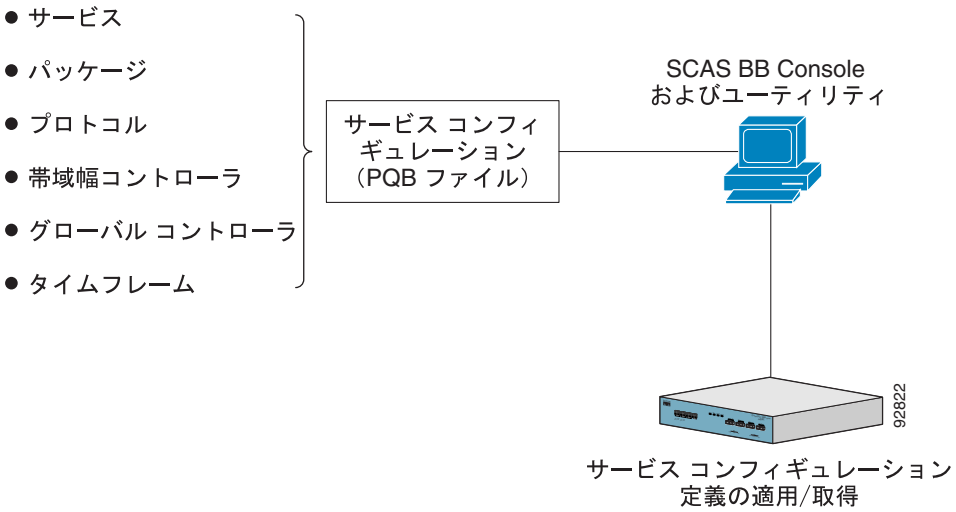
モード	サポートされている機能	主な利点	用途
サブスクライバレス モード	• グローバル（プラットフォームレベル）分析および制御	サブスクライバ設定は不要	グローバル制御ソリューションまたはサブスクライバレベル分析。 例： • ピアリング ポイントで P2P アップロードを制御 • P2P 帯域幅の総計の割合を指定
アノニマス サブスクライバ モード	• グローバルな分析および制御 • 各 IP アドレスレベルでの分析および制御	• サブスクライバ設定は不要。使用するサブスクライバ IP アドレス範囲のみを指定 • 統合なしでサブスクライバレベル制御を実行	サブスクライバごとに差別化されない、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 レベル分析または制御。 例： • サブスクライバごとに P2P 帯域幅を限定 • 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	• オンタイム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 CMTS デバイスを使用して、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について

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。一般に、サービス コンフィギュレーションで定義される内容は、次のとおりです。

- 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



SCA BB コンソール

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。

Service Configuration Utility

SCA BB Service Configuration Utility（**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 環境で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 Service Configuration Utility についての情報」（p.13-2）を参照してください。

サービス コンフィギュレーション API

サービス コンフィギュレーション 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設定と管理
- 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、管理および処理業務を自動化したり、簡略化できます。

サービス コンフィギュレーション API については、『*Cisco SCA BB Service Configuration API Programmer's Guide*』を参照してください。

CHAPTER 3

トラフィック処理の概要

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、*非対称ルーティング分類モード*をイネーブルにすると、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ティング ― SCA BB は課金処理を行い、Raw Data Record（RDR）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、レポーティング、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

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*にカテゴリ化します。

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ティング

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 件のサービスが設定できます。

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。
- 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)　非対称ルーティング分類モードがイネーブルに設定されている場合、フレーバは分類に使用されません。

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。

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） 非対称ルーティング分類モードがイネーブルに設定されている場合、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
- フローのフレーバがサービス要素で指定された *フレーバ* と一致する
- 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、次のようになります。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場合、どちらのサービスもサービス B のリストにある URL をブラウジングしますが、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、次のようになります。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場合、どちらのサービスも指定されたネットワーク ゾーンの E メール フローに一致しますが、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

次の表に、サービスとネットワーク 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	SMTP		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。

非対称ルーティング分類モードがイネーブルに設定されている場合、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。単方向 UDP フローの場合、SCA BB は最初のパケットの宛先ポートを使用してプロトコルを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ます。たとえば、次のようになります。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ており、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場合、ポート 21 の FTP フローはどちらのプロトコルにも一致しますが、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は、シグニチャと一致するプロトコルにマッピングされます。たとえば、次のようになります。プロトコル A が FTP シグニチャに一致するフローに定義されており、プロトコル B が TCP ポート 21 のフローに定義されている場合、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。

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。

非対称ルーティング分類モードがイネーブルになっている場合、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　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. ～ 123.3.123.255 になります）。

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。

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、SIP ソース ドメインがあります。

（注） 非対称ルーティング分類モードでは、トラフィックの分類にフレーバは使用されません。

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.7-51）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。

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、コンテント フィルタリングを提供します。SurfControl 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。

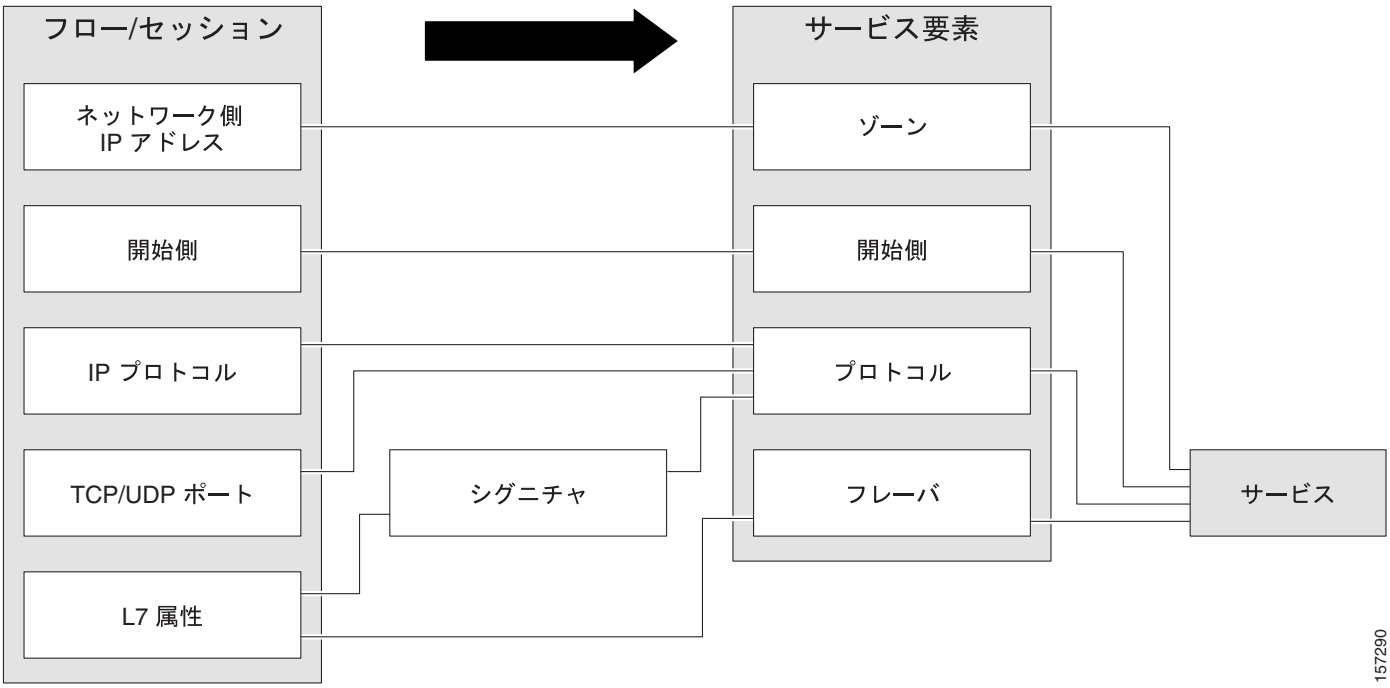
SurfControl の CPA を SCA BB に統合することで、必要な Web フィルタリング ソリューションが提供されます。SCA BB は SCE プラットフォーム上で実行され、CPA サーバに接続してサブスクライバが要求する Web サイトをカテゴリ化します。カテゴリは HTTP フローを分類するために使用され、この分類は、通常の SCA BB トラフィック制御とレポートに使用されます。

（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。

フロー属性のサービスへのマッピング

次の図は、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です。

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、レポーティングに使用できます。

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 BWC（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 SNMP 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 キロバイト）
- ダウンストリームのボリューム（L3 キロバイト）
- 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 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 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」（p.3-11）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。

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 と Package Usage の RDR と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。

- パッケージ使用カウンタ（p.3-11）

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。

たとえば、次の図に示すパッケージ ツリーの例では、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。

一方、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

Reporting

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 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ポートを生成します。
  - 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併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 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。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

*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。システムの動作は次のとおりです。

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）に応じて識別する
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 つの方法である仮想リンクモードについては、次のセクションで説明します。

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パッケージを定義します（「帯域幅の管理」[p.3-15] 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。

詳細は、「仮想リンクの管理」（p.9-47）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（仮想 LAN）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。

- フローをブロックする、またはフローに一定の帯域幅を割り当てる
- 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.3-15）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する規則パラメータが設定できます。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 BWC（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 パーセント制御する、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 コントローラが追加できます。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.3-15] 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（詳細は、「仮想リンクの管理」[p.9-47] 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 コントローラ（BWC）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。

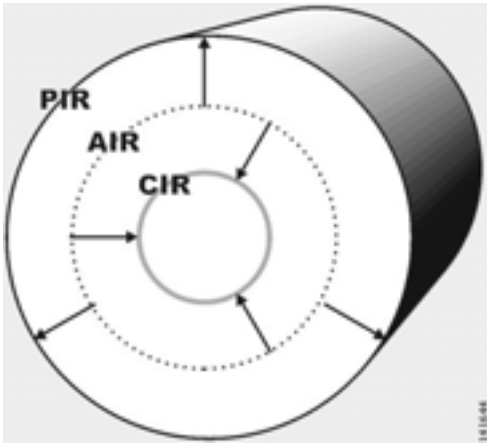
- Committed Information Rate（CIR; 認定情報レート）— BWC が制御するサービスに割り当てられる最小帯域幅
- PIR（Peak Information Rate; 最大情報レート）— BWC が制御するサービスに割り当てられる最大帯域幅
- Global Controller — この BWC のリンク先グローバル コントローラ
- Assurance Level（AL）— トラフィック輻輳時に利用可能な帯域幅が変化するレート

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 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



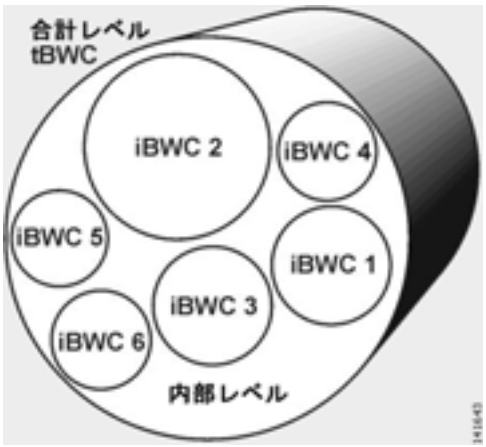
帯域幅は、調整可能な幅の仮想パイプとして考えることもできます。PIR は仮想パイプの最大許容幅です。CIR はこのパイプが収縮する際の最小幅です。AIR は、このパイプの実際の幅です。ネットワークの輻輳時は、システムは各パイプを個別に縮小して、サブスクライバ間およびサービス間で差別化します。

プライマリと内部の帯域幅の制御

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 Class of Service（CoS; サービス クラス）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 キロバイトで測定します。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 Solution Guide*』を参照してください。

（注） 非対称ルーティング分類モードでは、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） 非対称ルーティング分類モードでは、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

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。

- DoS 攻撃（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され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する（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する（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。

- 大量のメール配信を検出 — 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、電子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（電子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、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、SCE プラットフォームに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。フィルタ規則がこのトラフィック フローに適用できる場合、SCE プラットフォームはこのトラフィック 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。

SCE プラットフォームを通過する OSS プロトコル（DHCP など）およびルーティング プロトコル（BGP など）に対して、フィルタ規則を作成することを推奨します。通常、これらのプロトコルはポリシー適用の影響を受けず、ボリュームも小さいのでレポート作成に重要な役割を果たさないためです。

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。

クイック フォワーディング

クイック フォワーディングは、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。SCA BB アプリケーションのクイック フォワーディング フローはオフラインで扱われるので、制御できません。

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） 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。

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およびレポーティングの設定 ― トラフィック フローとネットワーク使用状況のアカウンティングをレポートするための方法を定義します。
- 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 アップする
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する
3. データを収集する
4. 分析する
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

ここでは、Cisco Service Control Application for Broadband（SCA BB）の使用を開始する際のプロセスについて説明します。

この章の内容は次のとおりです。

- 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。
- Console の各種コンポーネントを起動する方法を説明します。
- 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、ツール間のナビゲーション方法について説明します。
- 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するクイック スタート

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 Service Configuration Utility、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 サービス コントロール エンジン（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、「バージョン 2.5 から 3.1.0 へのアップグレード」（p.4-9）または「バージョン 3.0.x から 3.1.0 へのアップグレード」（p.4-11）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 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）：
  - SCE プラットフォームの各タイプ用 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。
  - SM 用の PQI ファイル。**SM** サブフォルダ内にあります。
- **scas_bb_util.tgz** ファイル ― SCA BB Service Configuration Utility 用のファイル（**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 サービス コンフィギュレーション 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 SCE 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 デバイスの PQI ファイルのインストール」（p.5-17）および「SM デバイスの PQI ファイルのインストール」（p.5-23）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

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

手順の概要

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。
2. Enter キーを押します。

手順の詳細

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。

SM が正しくインストールされていることの確認方法

手順の概要

1. SM への Telnet セッションを開きます。
2. SM **bin** ディレクトリに移動して **p3sm --sm-status** と入力します。
3. Enter キーを押します。

手順の詳細

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て **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て **p3sm version** 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 Service Configuration Utility（**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 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）
  - **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 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。

Java ランタイム環境のインストール

SCA BB Service Configuration Utility servconf は、JRE バージョン 1.4 または 1.5 にアクセスする必要があります。

JRE は Sun™ の Web サイト（http://java.sun.com/j2se/1.4.2/download.html）からダウンロード可能です。

JRE がインストールされていることを確認するために、コマンド プロンプトから **java -version** を実行します。Java バージョンが 1.4 または 1.5 で起動します。

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。JAVA_HOME 環境変数を設定して JRE 1.4 インストール ディレクトリを指定して実行します。たとえば、次のようになります。

```
JAVA_HOME=C:\Program Files\Java\j2re1.4.2_08
```

Console のインストール

手順の概要

1. Console インストール ファイル **scas-bb-console-3.1.0.exe** に進んで、これをダブルクリックします。
2. **Next** をクリックします。
3. **Browse** をクリックして別の宛先フォルダを選択します。
4. **Next** をクリックします。
5. Start Menu Folder フィールド内にある別の Start Menu フォルダを入力します。
6. **Do not create shortcuts** チェックボックスをオンにします。
7. **Install** をクリックします。
8. インストールが完了するまで待機します。
9. **Next** をクリックします。
10. **Finish** をクリックします。

手順の詳細

ステップ 1　Console インストール ファイル **scas-bb-console-3.1.0.exe** に進んで、これをダブルクリックします。

SCAS BB Console 3.1.0 Setup ウィザードの Welcome 画面が表示されます。

図 4-1

ステップ 2　**Next** をクリックします。

Setup ウィザードの Install Location 画面が開きます。

図 4-2

ステップ 3　**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 画面が開きます。

図 4-3

ステップ 5　Start Menu Folder フィールド内にある別の Start Menu フォルダを入力します。

ステップ 6　**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 画面が開きます。

図 4-4

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 画面が開きます。

図 4-5

ステップ 10 **Finish** をクリックします。

SCAS BB Console 3.1.0 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。

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

ステップ 1 SCA BB インストール パッケージから **scas_bb_util.tgz** ファイルを抽出し、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 ファイルを新規フォルダで開きます。

SCA BB Service Configuration Utility（**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 のアップグレード方法

バージョン 2.5 から 3.1.0 へのアップグレード

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。

- Console
- SCE PQI ファイル
- SM PQI 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ついてのみ説明します。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。

手順の概要

1. SCAS BB 2.5 Console を使用して、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（PQB）を取得し、ローカル ハードディスクに保存します。
2. SCA BB 3.1.0 Console をインストールします（「Console のインストール」[p.4-5] を参照）。
3. SCA BB 3.1.0 Console を開きます。
4. Network Navigator ツールを使用して、SCE プラットフォーム上にバージョン 3.1.0 の SCE PQI ファイルをインストールします。
5. Network Navigator ツール内に SCE デバイスを作成します（「サイトの管理」[p.5-4] を参照）。
6. PQI ファイルをインストールします（「SDE デバイスの管理」[p.5-11] を参照）。
7. SCE プラットフォームのオンライン ステータスを取得することでインストールが正常に実行されたことを確認します（「SDE デバイスの管理」[p.5-11] を参照）。
8. システムに SM が含まれている場合、Network Navigator ツールを使用して SM デバイス上にバージョン 3.1.0 の SM PQI ファイルをインストールします。
9. Network Navigator ツール内に SM デバイスを作成します（「サイトの管理」[p.5-4] を参照）。
10. PQI ファイルをインストールします（「SM デバイスの PQI ファイルのインストール」[p.5-23] を参照）。
11. 3.1.0 Service Configuration Editor ツールを使用して、ステップ 1 に保存されたサービス コンフィギュレーションを開きます。
12. 新しいシグニチャベースのプロトコルの一覧についてリリース ノートをチェックして、マニュアルでこれらのプロトコルをサービスに割り当てます。
13. 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。

手順の詳細

ステップ 1　SCAS BB 2.5 Console を使用して、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（PQB）を取得し、ローカル ハードディスクに保存します。

（注）　アップグレード手順で、SCAS BB 2.5 Console のアンインストールは不要です。

ステップ 2　SCA BB 3.1.0 Console をインストールします（「Console のインストール」[p.4-5] を参照）。

ステップ 3　SCA BB 3.1.0 Console を開きます。

ステップ 4　Network Navigator ツールを使用して、SCE プラットフォーム上にバージョン 3.1.0 の SCE PQI ファイルをインストールします。

a. Network Navigator ツール内に SCE デバイスを作成します（「サイトの管理」[p.5-4] を参照）。

b. PQI ファイルをインストールします（「SDE デバイスの管理」[p.5-11] を参照）。

c. SCE プラットフォームのオンライン ステータスを取得することでインストールが正常に実行されたことを確認します（「SDE デバイスの管理」[p.5-11] を参照）。

ステップ 5　システムに SM が含まれている場合、Network Navigator ツールを使用して SM デバイス上にバージョン 3.1.0 の SM PQI ファイルをインストールします。

a. Network Navigator ツール内に SM デバイスを作成します（「サイトの管理」[p.5-4] を参照）。

b. PQI ファイルをインストールします（「SM デバイスへの接続」[p.5-22] を参照）。

ステップ 6　3.1.0 Service Configuration Editor ツールを使用して、ステップ 1 に保存されたサービス コンフィギュレーションを開きます。

ステップ 7　新しいシグニチャベースのプロトコルの一覧についてリリース ノートをチェックして、マニュアルでこれらのプロトコルをサービスに割り当てます。

古い PQB ファイルをアップグレードする場合、新しいシグニチャベースのプロトコルをサービスに割り当てることができません（したがって汎用 TCP に分類されます）。

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。

- 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 SCA BB バージョンは、前の SCA BB バージョンでインストールされたデフォルトの Dynamic Signature Script（DSS）ファイル（「デフォルト DSS ファイル」[p.7-45]）を使用しません。
- 新規バージョンのプロトコル パックが使用可能な場合は、製品のインストール後にこれをインストールします（「Network Navigator を使用したプロトコル パックのインストール」[p.4-15] を参照）。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*。

バージョン 3.0.x から 3.1.0 へのアップグレード

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。

- Console
- SCE PQI ファイル
- SM PQI 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ついてのみ説明します。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。

手順の概要

1. SCA BB 3.0.x Console を使用して、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（PQB）を取得し、これをローカル ハードディスクに保存します。
2. SCA BB 3.1.0 Console をインストールします（「Console のインストール」[p.4-5] を参照）。
3. SCA BB 3.1.0 Console を開きます。
4. Network Navigator ツールを使用して、SCE プラットフォーム上にバージョン 3.1.0 の SCE PQI ファイルをインストールします。
5. Network Navigator ツール内に SCE デバイスを作成します（「SDE デバイスの管理」[p.5-11] を参照）。
6. PQI ファイルをインストールします（「SCE デバイスの PQI ファイルのインストール」[p.5-17] を参照）。
7. SCE プラットフォームのオンライン ステータスを取得することでインストールが正常に実行されたことを確認します（「CM デバイスのオンライン ステータスの取得」[p.5-24] を参照）。
8. システムに SM が含まれている場合、Network Navigator ツールを使用して SM デバイス上にバージョン 3.1.0 の SM PQI ファイルをインストールします。
9. Network Navigator ツール内に SM デバイスを作成します（「サイトへの SM デバイスの追加」[p.5-6] を参照）。
10. PQI ファイルをインストールします（「SM デバイスへの接続」[p.5-22] を参照）。
11. 3.1.0 Service Configuration Editor ツールを使用して、ステップ 1 に保存されたサービス コンフィギュレーションを開きます。
12. 新しいシグニチャベースのプロトコルの一覧についてリリース ノートをチェックして、マニュアルでこれらのプロトコルをサービスに割り当てます。
13. 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。

手順の詳細

ステップ 1　SCA BB 3.0.x Console を使用して、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（PQB）を取得し、これをローカル ハードディスクに保存します。

(注)　アップグレード手順で、SCAS BB 3.0.x Console のアンインストールは不要です。

ステップ 2　SCA BB 3.1.0 Console をインストールします（「Console のインストール」[p.4-5] を参照）。

ステップ 3　SCA BB 3.1.0 Console を開きます。

ステップ 4　Network Navigator ツールを使用して、SCE プラットフォーム上にバージョン 3.1.0 の SCE PQI ファイルをインストールします。

a. Network Navigator ツール内に SCE デバイスを作成します（「SDE デバイスの管理」[p.5-11] を参照）。

b. PQI ファイルをインストールします（「SCE デバイスの PQI ファイルのインストール」[p.5-17] を参照）。

c. SCE プラットフォームのオンライン ステータスを取得することでインストールが正常に実行されたことを確認します（「CM デバイスのオンライン ステータスの取得」[p.5-24] を参照）。

ステップ 5　システムに SM が含まれている場合、Network Navigator ツールを使用して SM デバイス上にバージョン 3.1.0 の SM PQI ファイルをインストールします。

a. Network Navigator ツール内に SM デバイスを作成します（「サイトへの SM デバイスの追加」[p.5-6] を参照）。

b. PQI ファイルをインストールします（「SM デバイスの PQI ファイルのインストール」[p.5-23] を参照）。

ステップ 6　3.1.0 Service Configuration Editor ツールを使用して、ステップ 1 に保存されたサービス コンフィギュレーションを開きます。

ステップ 7　新しいシグニチャベースのプロトコルの一覧についてリリース ノートをチェックして、マニュアルでこれらのプロトコルをサービスに割り当てます。

古い PQB ファイルをアップグレードする場合、新しいシグニチャベースのプロトコルをサービスに割り当てることができません（したがって汎用 TCP に分類されます）。

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。

- 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 SCA BB バージョンは、前の SCA BB バージョンでインストールされたデフォルトの Dynamic Signature Script（DSS）ファイル（「デフォルト DSS ファイル」[p.7-45] を参照）を使用しません。
- 新規バージョンのプロトコル パックが使用可能な場合、製品のインストール後にこれをインストールします（「Network Navigator を使用したプロトコル パックのインストール」[p.4-15] を参照）。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*。

SCA BB Service Configuration Utility のアップグレード

ステップ 1　新バージョンの SCA BB Service Configuration Utility、servconf を空のディレクトリにインストールします。

「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」[p.4-8] を参照してください。

プロトコル パックのインストール方法

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

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）　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のみ、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。

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がイネーブルになっている場合（「SLI の中断のないアップグレード」[p.4-18] を参照）、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ありません。
  - 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のパッケージ ID、リアルタイム モニタリング フラグ、クォータ設定値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。

プロトコルのアップデート

プロトコル パックの配布

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 Service Configuration Utility についての情報（p.13-2）
- Network Navigator ツール。「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」[p.4-15] を参照してください。

（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.4-18] を参照）。

ツールまたはユーティリティで以下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）を含む各新規シグニチャの場合（「バディ プロトコル」[p.12-4] を参照）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.4-19）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。

プロトコル パックのバージョン互換性確認

プロトコル パックは、特定バージョンの SCE プラットフォームでのみ互換性があります。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 3.1.0 上では 3.1.0 用のプロトコル パックのみを使用します。

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ていて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。

Network Navigator を使用したプロトコル パックのインストール

Network Navigator により、プロトコル パックを簡単にインストールすることができます。

プロトコル パックは、選択された 1 つ以上のサイトにある、1 つ、複数、またはすべての SCE プラットフォームにインストール可能です。

- 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（p.4-15）
- 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（p.4-17）
- プロトコル パックのインストール確認（p.4-17）

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

手順の概要

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。
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。
3. **Browse** をクリックします。
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。
5. インストールするファイルをブラウズします。
6. **Open** をクリックします。
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。
8. **Finish** をクリックします。
9. 適切なパスワードを入力します
10. **Update** をクリックします。

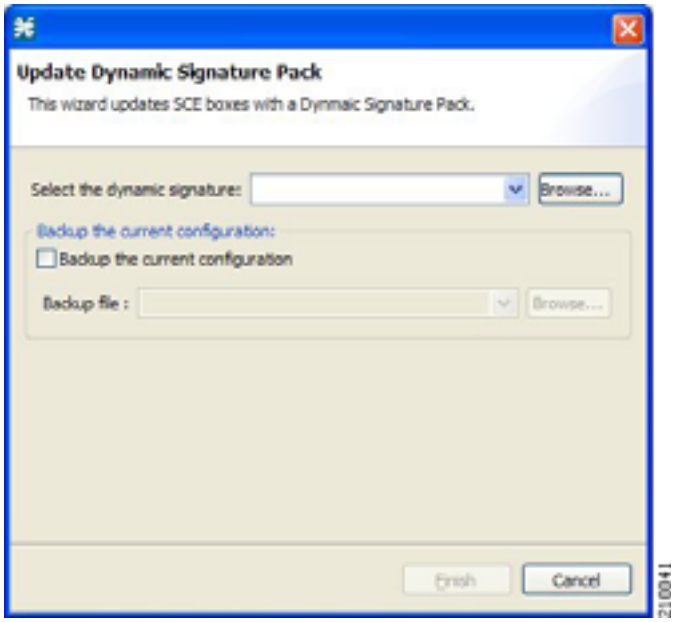
手順の詳細

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 4-6



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。

詳細は、「パスワード管理」（p.5-10）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

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、**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。

ステップ 3　インストールするプロトコル パックを選択します。

ステップ 4　（推奨）**Backup the current configuration** チェック ボックスをオンにして、バックアップ ディレクトリを選択します。

（注）　バックアップ ファイルの名前は、**backupPolicy_<SCE platform IP address>.pqb** になります。

ステップ 5　**Finish** をクリックします。

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

ステップ 6　各 SCE デバイスに対して、パスワードを入力して **Update** をクリックします。

プロトコル パックが順番に各 SCE プラットフォームにインストールされます。

プロトコル パックのインストール確認

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、インストール済のプロトコル パック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 を取得して Console を使用してこれを表示します。

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 バージョンが欠落しているか、または不適切 ― 正しい 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」[p.4-14] 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。

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** にマップされています。

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 200 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、および管理が中断しません（「プロトコル パックのインストール方法」[p.4-13] を参照）。Console または **servconf**（SCA BB Service Configuration Utility）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 時間以上経過したあと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。

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

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 CLI（コマンドライン インターフェイス）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 Service Control Engine (SCE) 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。

以下の 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させ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。

中断のないアップグレードの CLI コマンドに関する説明

以下の表では、前のセクションで挙げ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ています。

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のみ完了します。
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）。

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

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。

（注）　次の 2 つの CLI コマンドは、EXEC モード コマンドです。

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

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

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

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

Console の起動

SCAS BB Console Setup ウィザードが、Console のショートカットをスタートメニューに追加します。

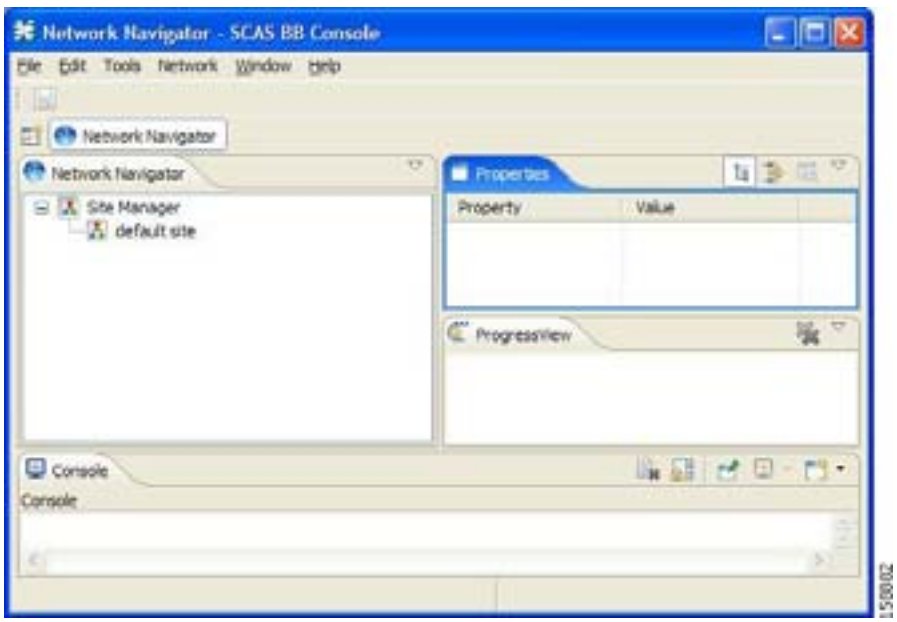
ステップ 1　**Start >All Programs >Cisco SCA >SCA BB Console 3.1.0 >SCA BB Console 3.1.0** の順番に選択します。

Cisco Service Control SCAS BB Console のスプラッシュ画面が表示されます。

図 4-7

Console のロード後、Console のメイン ウィンドウが表示され、Network Navigator ツールが開きます。

図 4-8



(注)　Console を閉じる際に、開いているツールとアクティブなツールが記憶されるので、Console を次に起動させるときに適用されます。

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 がクライアントに提供するサービスを設定します。

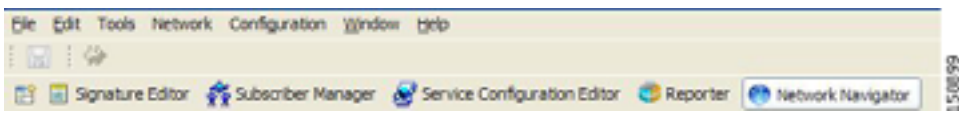
Console は次のツールで構成されています。

- 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。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。

Network Navigator ツール

図 4-9



(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。

Network Navigator により、Cisco Service Control ソリューションの一部であるすべてのローカルおよびリモート デバイスのシンプルなモデルを作成し、管理することができます。

Network Navigator についての詳細は、「Network Navigator の使用」（p.5-1）を参照してください。

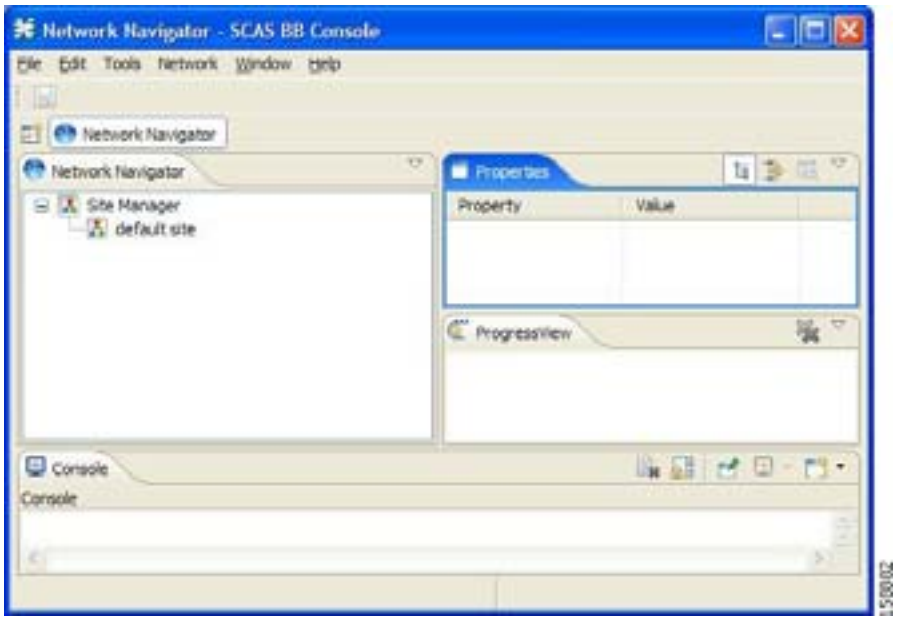
- Network Navigator ツールの開き方（p.4-23）
- Network Navigator ツールの閉じ方（p.4-23）

Network Navigator ツールの開き方

ステップ 1　Console のメイン メニューから **Tools >Network Navigator** の順番に選択します。

Network Navigator ツールが開きます。

図 4-10



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。

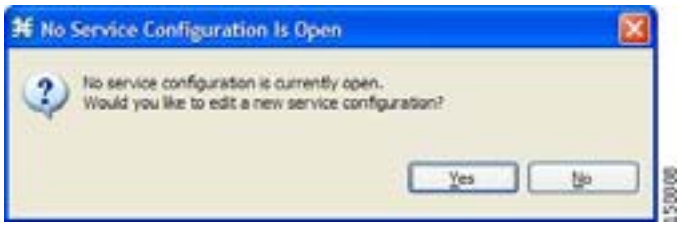
このマニュアルの大半は、Service Configuration Editor の使用方法について説明しています。「Service Configuration Editor の使用」（p.6-1）を参照してください。

Service Configuration Editor ツールの開き方

ステップ 1　Console のメイン メニューから **Tools >Service Configuration Editor** の順番に選択します。

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

図 4-11



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 4-12

ステップ 3　**System Operational Mode** オプション ボタンの 1 つを選択します。

- **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 の生成のみを実行します。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。

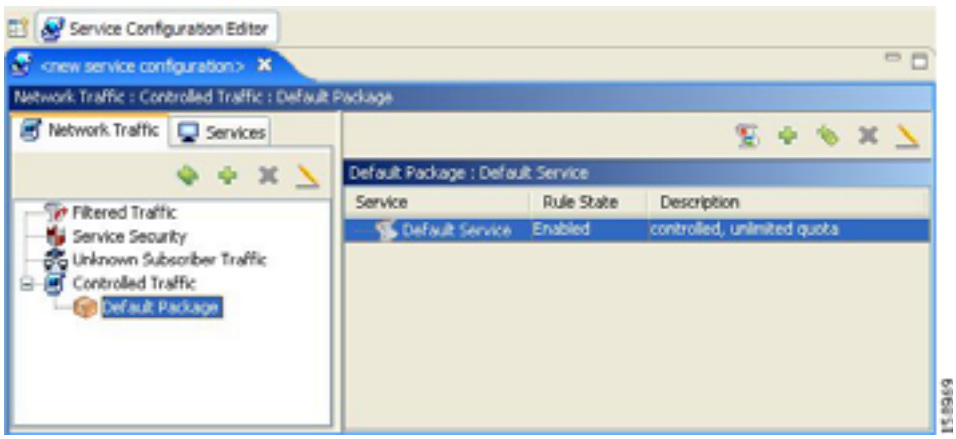
ステップ 4　非対称ルーティング分類モードに切り替えるために、**Enable the Asymmetric Routing Classification Mode** チェック ボックスをオンにします（単方向フローの比率が高いシステムの場合に強く推奨します）。

(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（ルーティング分類モードについては、「非対称ルーティング分類モード」[p.10-34] 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 で開きます。

図 4-13



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

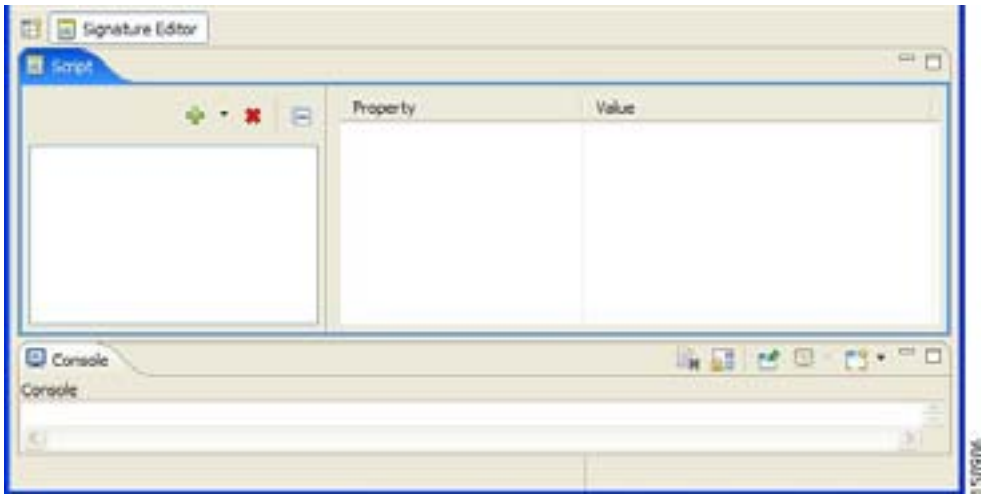
- Signature Editor ツールの開き方（p.4-26）
- Signature Editor ツールの閉じ方（p.4-26）

Signature Editor ツールの開き方

ステップ 1　Console のメイン メニューから **Tools >Signature Editor** の順番に選択します。

Signature Editor ツールが開きます。

図 4-14



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、マニュアル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。

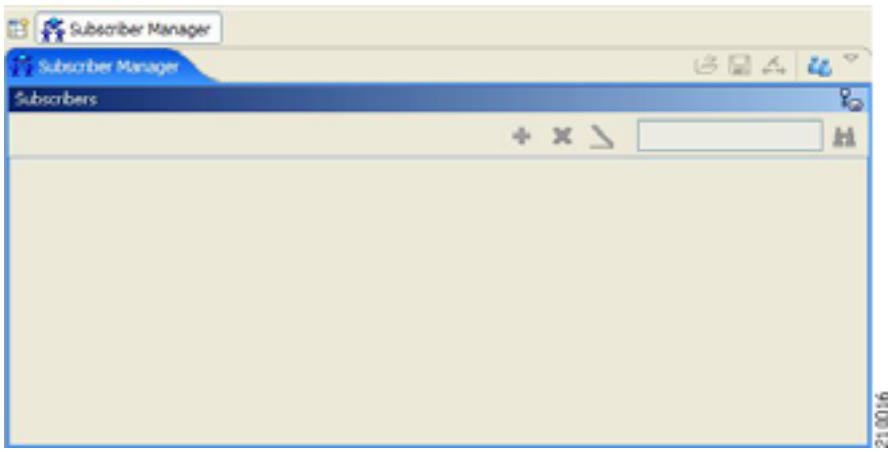
SCMS-SM の詳細については、『*Cisco Service Control Management Suite Subscriber Manager User Guide*』を参照してください。

SM GUI ツールの開き方

ステップ 1　Console のメイン メニューから **Tools >Subscriber Manager** の順番に選択します。

SM GUI ツールが開きます。

図 4-15



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、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。

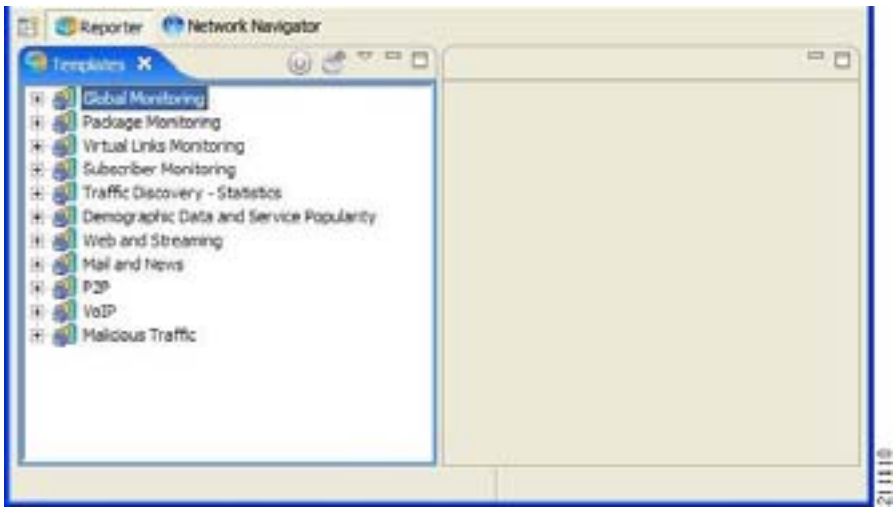
- Reporter ツールの開き方（p.4-28）
- Reporter ツールの閉じ方（p.4-29）

Reporter ツールの開き方

ステップ 1　Console のメイン メニューから **Tools >Reporter** の順番に選択します。

Reporter ツールが開きます。

図 4-16



（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（「データベースの SCA Reporter へのアクセス」[p.5-25] 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。

オンラインヘルプへのアクセス

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（p.4-29）
- オンライン ヘルプの検索（p.4-29）

オンラインヘルプへのアクセス

ステップ 1　Console のメイン メニューから **Help >Help Contents** の順番に選択します。

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

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。

手順の概要

1. Console のメイン メニューから **Help >Search** の順番に選択します。
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。
3. **Go** をクリックします。
4. ヘルプ項目をクリックして、内容を表示させます。
5. Help 画面の下部にある該当リンクをクリックします。

手順の詳細

ステップ 1　Console のメイン メニューから **Help >Search** の順番に選択します。

現在のツールの隣に、Help 画面が開きます。

図 4-17

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。

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　画面の下部にある該当リンクをクリックすると、次の部分への切り替えを行うことができます。

- 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。SCE デバイスをデフォルトのサイトに追加して、デフォルトのサービス コンフィギュレーションを SCE 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 3.1.0 >SCA BB Console 3.1.0 の順番に選択します。

ステップ 2　Network Navigator を開きます。

Console のメイン メニューから **Tools >Network Navigator** の順番に選択します。

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 画面に表示されたデフォルト サイトを確認できます。

ステップ 3　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て、表示されるポップアップ メニューから、**New >SCE** の順番に選択します。

   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 4　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て、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て、**Extract** をクリックします。

   SCE オンライン スタ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、動作ステータスが Active になっていることを確認します。

ステップ 5　Service Configuration Editor を開きます。

- Console のメイン メニューから **Tools >Service Configuration Editor** の順番に選択します。

  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 6　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 7　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て、**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

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。

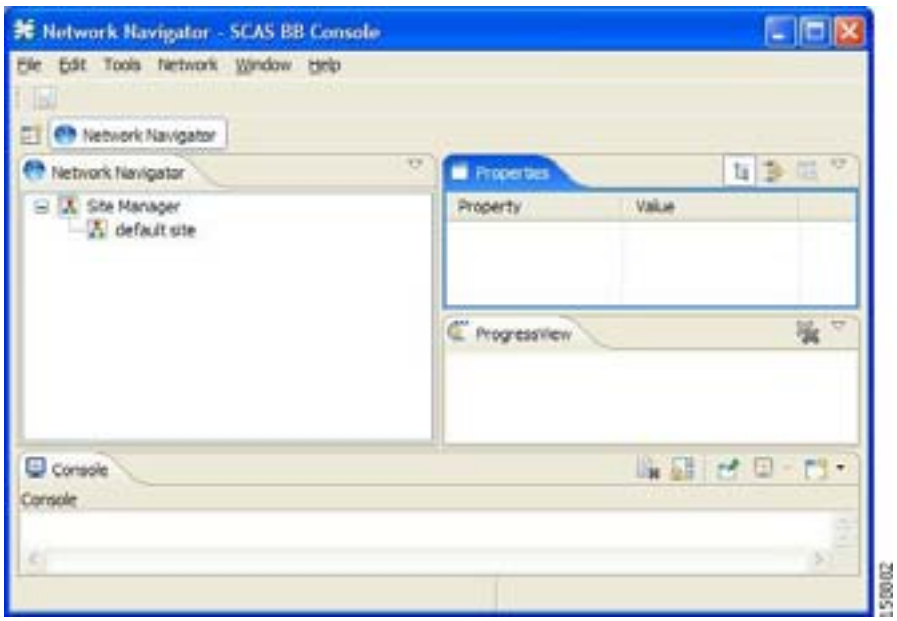
ここでは、Service Control ソリューションの一部となるローカルおよびリモートのすべてのサイトとデバイスの単純なモデルを Network Navigator ツールを用いて作成し、これらのデバイスをリモートで管理する方法を説明します。

Network Navigator ツール

Network Navigator ツールは 4 つの画面で構成されています。

- Network Navigator 画面 — Site Management ツリーで、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表示します。
- Properties 画面 — Network Navigator 画面の Site Manager ツリーで選択されたノードの編集可能プロパティを表示します。
- Progress View 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したログ メッセージを表示します。

図 5-1



ネットワーク設定要件

ファイアウォール /NAT 要件

以下の表は、Network Navigator が適切に動作するの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。

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 for more information*』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。

SM と CM のコマンドライン ユーティリティを使用するか、SCE プラットフォームのユーザ / パスワード メカニズムを使用して、ユーザ名とパスワードを定義します。

ユーザ定義の詳細については、以下を参照してください。

CM ― 『*Cisco Service Control Management Suite Collection Manager User Guide*』の「Managing the Collection Manager」の章にある「Managing Users」

- SM ― 『*Cisco Service Control Management Suite Subscriber Manager User Guide*』の付録「Command-Line Utilities」にある「p3rpc Utility」
- SCE ― 『*Cisco Service Control Engine (SCE) Software Configuration Guide*』の「Configuring the Management Interface and Security」の章にある「TACACS+ Authentication, Authorization, and Accounting」

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のみ、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。以下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、追加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を管理するのにも役立ちます（「パスワード管理」[p.5-10] を参照）。

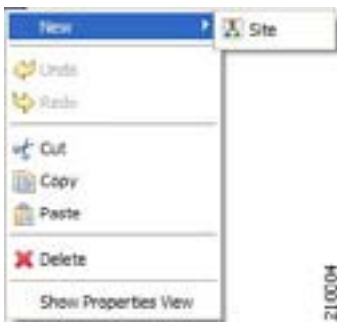
Site Manager へのサイトの追加

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



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 へ追加されます。

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　（任意）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

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

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。

SCE デバイスをサイトに追加するには、次の手順を実行します。

手順の概要

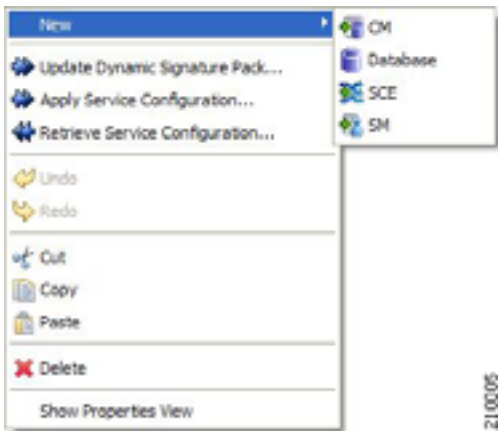
1. Site Manager ツリーで、サイトを右クリックします。
2. メニューから、**New >SCE** の順に選択します。
3. Address フィールドに、SCE の IP アドレスを入力します。
4. （任意）Name フィールドに、SCE のわかりやすい名前を入力します。
5. Finish をクリックします。

手順の詳細

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



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　（任意）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

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。

SM デバイスをサイトに追加するには、次の手順を実行します。

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　（任意）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 ウィザードを閉じます。

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

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。

CM デバイスをサイトに追加するには、次の手順を実行します。

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　（任意）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 ウィザードを閉じます。

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

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。

データベース デバイスをサイトに追加するには、次の手順を実行します。

手順の概要

1. Site Manager ツリーで、サイトを右クリックします。
2. メニューから、**New >Database** の順に選択します。
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。
4. （任意）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。
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。
6. （任意）**Enable Advanced Settings** チェック ボックスをオンにして、Url、Driver、User、Password フィールドに新規値を入力します。
7. Finish をクリックします。

手順の詳細

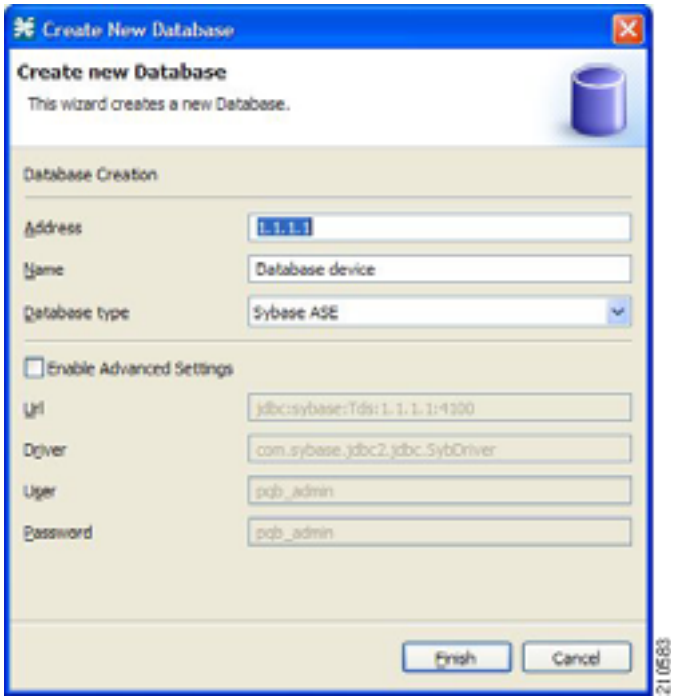
ステップ 1　Site Manager ツリーで、サイトを右クリックします。

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



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　（任意）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　（任意）**Enable Advanced Settings** チェック ボックスをオンにして、Url、Driver、User、Password フィールドに新規値を入力します。

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

デバイスを削除するには、次の手順を実行します。

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

サイトを削除するには、次の手順を実行します。

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。

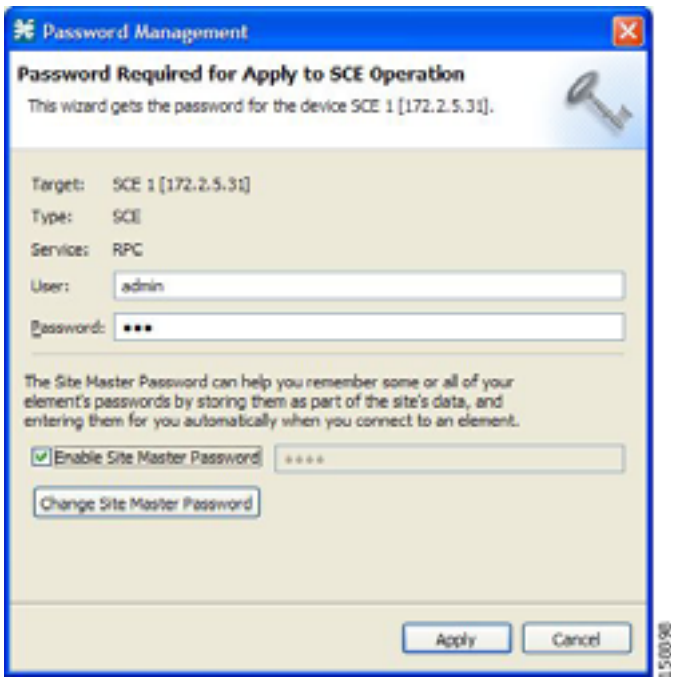
パスワード管理

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。Console は、サイト パスワード マネージャを有効にする際にサイトのマスタ パスワードを要求します。複数のサイトがある場合、各サイトに個別のマスタ パスワードが必要です。

図 5-5



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。

SDE デバイスの管理

SCE デバイスのテクニカル サポート情報ファイルの生成

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。

SCE のテクニカル サポート ファイルを作成するには、次の手順を実行します。

手順の概要

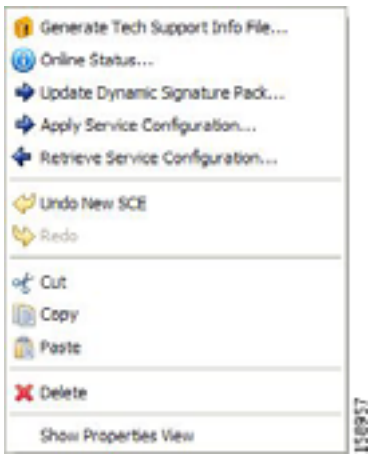
1. Site Manager ツリーで、SCE デバイスを右クリックします。
2. メニューから、**Generate Tech Support Info File** を選択します。
3. Browse をクリックします。
4. テクニカル サポート情報ファイルを保存するフォルダをブラウズします。
5. File name フィールドで、新規ファイル名を入力するか、既存の zip ファイルを選択します。
6. **Open** をクリックしてファイルを選択します。
7. ログファイルを出力テクニカル サポート情報ファイルに追加するには、**Add GUI Console log files** チェック ボックスをオンにします。
8. **Open file after it is fetched check box** チェック ボックスをオンにします。
9. **Finish** をクリックします。
10. 適切なパスワードを入力します（詳細は、「パスワード管理」[p.5-10] を参照してください）。
11. **Generate** をクリックします。

手順の詳細

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 5-6



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。

図 5-7

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　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 check box** 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（詳細は、「パスワード管理」[p.5-10] 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

この操作は、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提供します。

SCE デバイスのオンライン ステータスを取得するには、次の手順を実行します。

手順の概要

1. Site Manager ツリーで、SCE デバイスを右クリックします。
2. メニューから、**Online Status** を選択します。
3. 適切なパスワードを入力します（詳細は、「パスワード管理」[p.5-10] を参照してください）。
4. **Extract** をクリックします。

手順の詳細

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（詳細は、「パスワード管理」[p.5-10] を参照してください）。

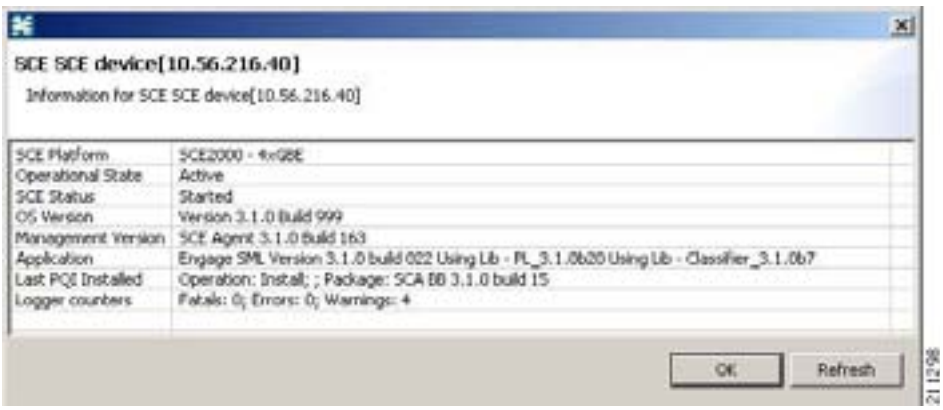
ステップ 4　**Extract** をクリックします。

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 スタータスが取得されます。

図 5-8



SCE デバイスのプロトコル パックのインストール

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、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 パックのインストール方法」[p.4-13] を参照）。

- 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（p.5-14）
- 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（p.5-16）
- 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（p.5-16）
- 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（p.5-17）
- SCE デバイスの PQI ファイルのインストール（p.5-17）
- 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（p.5-19）

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

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）　適用されたサービス 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。

単一 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には、次の手順を実行します。

手順の概要

1. Site Manager ツリーで、SCE デバイスを右クリックします。
2. メニューから、**Apply Service Configuration** を選択します。
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。
4. **OK** をクリックします。
5. 適切なパスワードを入力します（詳細は、「パスワード管理」[p.5-10] を参照してください）。
6. **Apply** をクリックします。

手順の詳細

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。

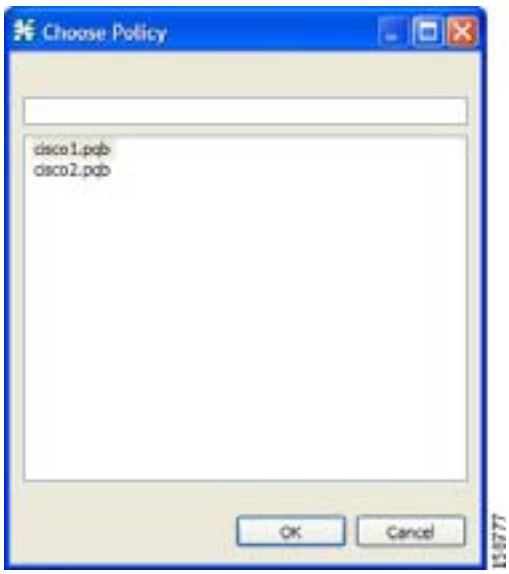
ポップアップ メニューが表示されます。

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、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 つのみの場合、Password Management ダイアログ ボックスが表示されます。ステップ 5 を続けます（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、エラー メッセージが表示されます）。

図 5-9



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（詳細は、「パスワード管理」[p.5-10] 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。

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

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

複数の 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には、次の手順を実行します。

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に適用されるサイトまたは SCE デバイスを選択し、それ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 つのみの場合、Password Management ダイアログ ボックスが表示されます。ステップ 4 を続けます（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、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て **OK** をクリックします。

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

ステップ 4　各 SCE デバイスに対して、パスワードを入力して **Apply** をクリックします。

ステップ 5　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

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 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には、次の手順を実行します。

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。

- 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（詳細は、「パスワード管理」[p.5-10] 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

複数の 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には、次の手順を実行します。

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。

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

ステップ 3　各 SCE デバイスに対して、パスワードを入力して **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 デバイスの PQI ファイルのインストール

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。詳細は、「SCA BB のインストール方法」[p.4-2] 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。

SCE デバイスに PQI ファイルをインストールするには、次の手順を実行します。

手順の概要

1. Site Manager ツリーで、SCE デバイスを選択します。
2. Console のメイン メニューから **Network >Install PQI** の順に選択します。
3. **Browse** をクリックします。
4. インストールしている PQI ファイルをブラウズします。
5. **Open** をクリックします。
6. **Finish** をクリックします。
7. 適切なパスワードを入力します（詳細は、「パスワード管理」[p.5-10] を参照してください）。
8. **Apply** をクリックします。

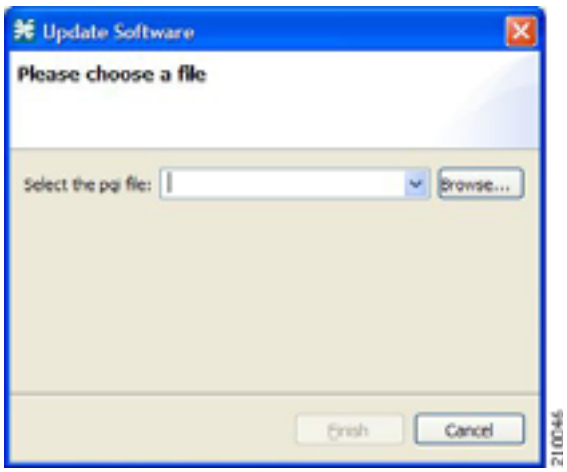
手順の詳細

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 メニューから **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 5-10



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（詳細は、「パスワード管理」[p.5-10] 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

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 OS 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

詳細については、『*Cisco Service Control Engine (SCE) Software Configuration Guide*』の「Operations」の章にある「Upgrading SCE Platform Firmware」を参照してください。

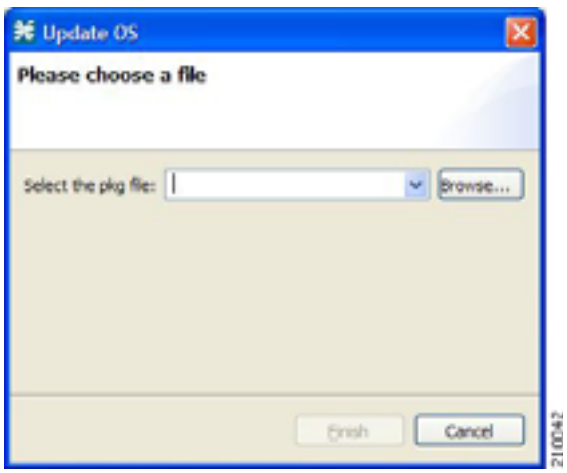
OS ファイルを SCE デバイスにインストールするには、次の手順を実行します。

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 メニューから **Network >Install OS** 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 5-11



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（詳細は、「パスワード管理」[p.5-10] 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

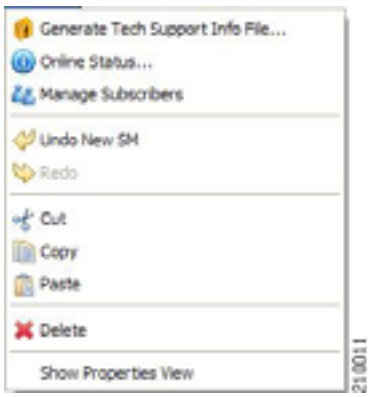
この操作では、シスコのテクニカル サポート スタッフが使用する SM のサポート ファイルが生成されます。

SM のテクニカル サポート ファイルを作成するには、次の手順を実行します。

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。

図 5-12



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　（任意）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　（任意）**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（詳細は、「パスワード管理」[p.5-10] 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

この操作は、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提供します。

SM デバイスのオンライン ステータスを取得するには、次の手順を実行します。

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（詳細は、「パスワード管理」[p.5-10] を参照してください）。

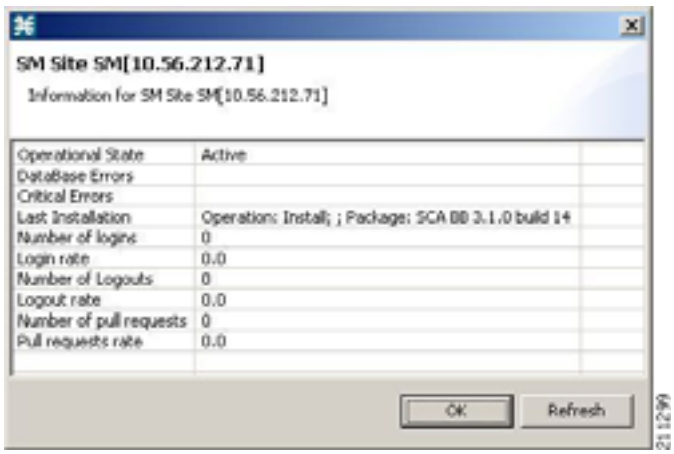
ステップ 4　**Extract** をクリックします。

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 スタータスが取得されます。

図 5-13



SM デバイスへの接続

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しようとして、SCMS-SM で認証を実行します。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。

SM デバイスに接続するには、次の手順を実行します。

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 **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（詳細は、「パスワード管理」[p.5-10] 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。

このツールの操作については、「Subscriber Manager の GUI ツールの使用方法」（p.11-1）を参照してください。

SM デバイスの PQI ファイルのインストール

(注)　PQI ファイルのインストールには、通常数分かかります。

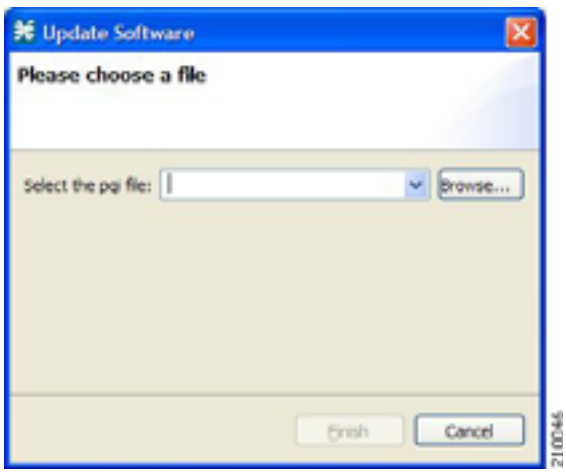
SM デバイスに PQI ファイルをインストールするには、次の手順を実行します。

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

ステップ 2　Console のメイン メニューから **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 5-14



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（詳細は、「パスワード管理」[p.5-10] 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 SM 経過表示バーが表示されます。

選択された SM に PQI ファイルがインストールされます。

CM デバイスの管理

CM デバイスのオンライン ステータスの取得

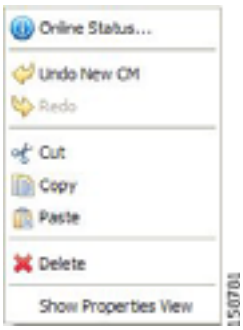
この操作は、CM の現在のソフトウェア バージョンと動作ステータスに関する情報を提供します。

CM デバイスのオンライン ステータスを取得するには、次の手順を実行します。

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 5-15



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（詳細は、「パスワード管理」[p.5-10] 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 スタ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」（p.5-13）を参照してください。

データベース デバイスの管理

データベースの SCA Reporter へのアクセス

(注)　代替手順については、『*Cisco Service Control Application Reporter User Guide*』の「Using the SCA Reporter」の章にある「Configuring a Database Connection」を参照してください。

データベースを SCA Reporter にアクセス可能にするには、次の手順を実行します。

手順の概要

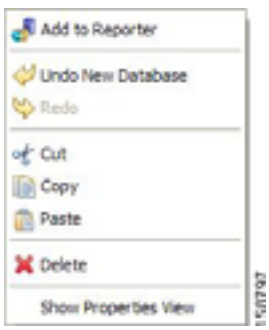
1. Site Manager ツリーで、データベース デバイスを右クリックします。
2. メニューから、**Add to Reporter** を選択します。
3. **Add** をクリックします。
4. **Choose definition mode** のオプション ボタンを 1 つ 選択します。
5. **Next** をクリックします。
6. すべてのフィールドに入力します。
7. **Finish** をクリックします。
8. 他のデータベースについて、ステップ 3 ～ 7 を繰り返します。
9. 必要に応じてデータベース接続情報を削除します。
10. 正しいデータベースがアクティブになっていることを確認します。
11. **OK** をクリックします。

手順の詳細

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。

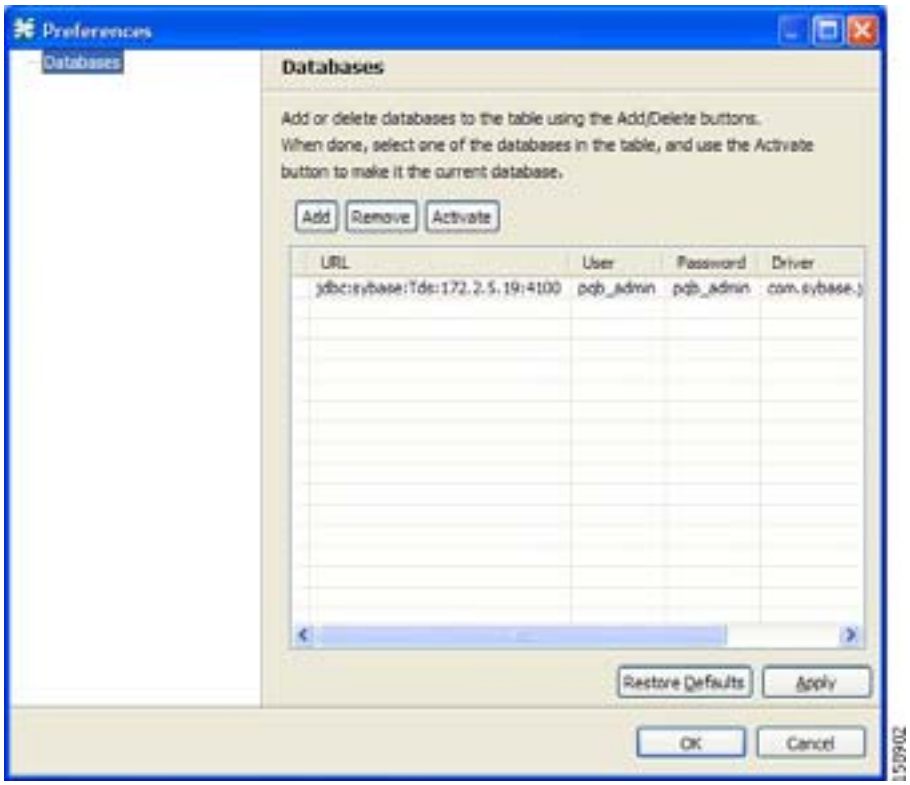
図 5-16



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。

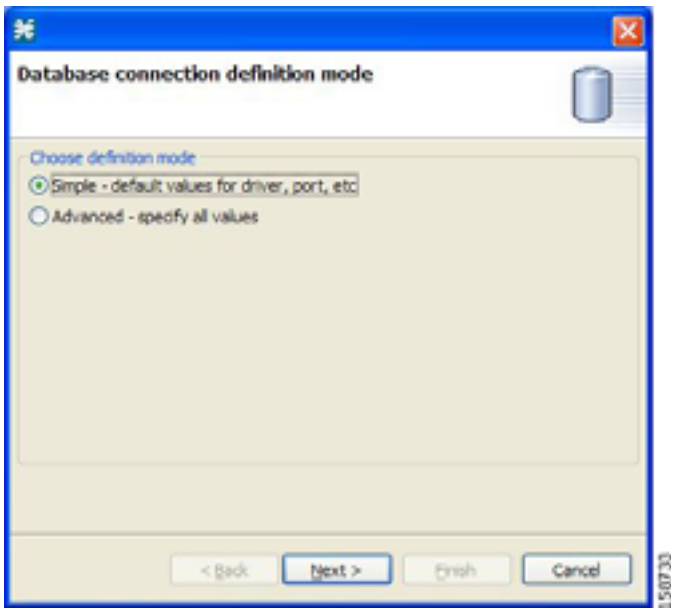
図 5-17



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 5-18



ステップ 4　**Choose definition mode** のオプション ボタンを 1 つ 選択します。

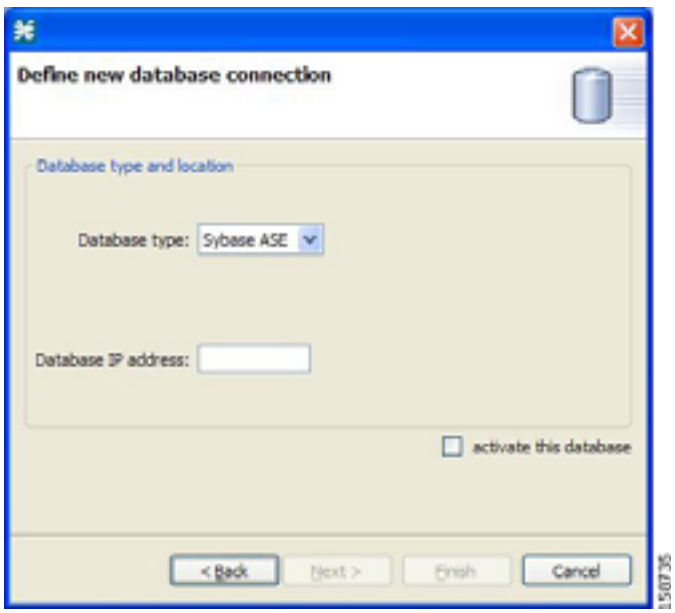
- **Simple**
- **Advanced**

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 画面は表示されます。

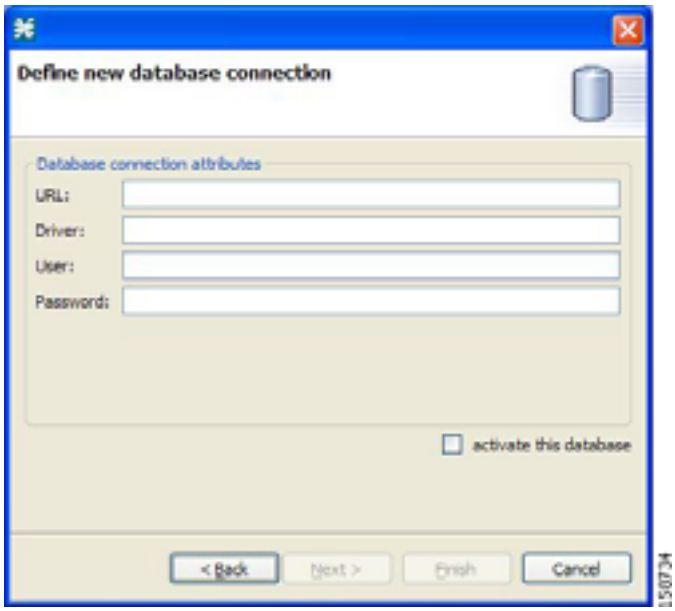
ステップ 4 で Simple を選択した場合、Define new database connection 画面は次のようになります。

図 5-19



ステップ 4 で Advanced を選択した場合、Define new database connection 画面が次のようになります。

図 5-20



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　必要に応じてデータベース接続情報を削除します。

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可能で、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できます。

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がデバイスにアクセスするには、Site Management Password を提供するだけです。

- Network Navigator 設定のエクスポート（p.5-29）
- Network Navigator 設定のインポート（p.5-32）

Network Navigator 設定のエクスポート

Network Navigator 設定をファイルにエクスポートするには、次の手順を実行します。

手順の概要

1. Console のメイン メニューから **File >Export** の順番に選択します。
2. エクスポート宛先一覧から、**Network Navigator Configuration to a file** を選択します。
3. **Next** をクリックします。
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。
5. Select the export destination 領域で、**Browse** をクリックします。
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。
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。
8. **Open** をクリックしてファイルを選択します。
9. **Finish** をクリックします。

手順の詳細

ステップ 1　Console のメイン メニューから **File >Export** の順番に選択します。

Export ダイアログ ボックスが表示されます。

図 5-21

ステップ 2　エクスポート宛先一覧から、**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 5-22

Available sites 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

Network Navigator 設定をファイルにインポートするには、次の手順を実行します。

手順の概要

1. Console のメイン メニューから **File >Import** の順番に選択します。
2. インポート元のリストから、**Network Navigator Configuration from file** を選択します。
3. **Next** をクリックします。
4. **Browse** をクリックします。
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。
6. **Open** をクリックしてファイルを選択します。
7. **Finish** をクリックします。

手順の詳細

ステップ 1　Console のメイン メニューから **File >Import** の順番に選択します。

Import ダイアログボックスが表示されます。

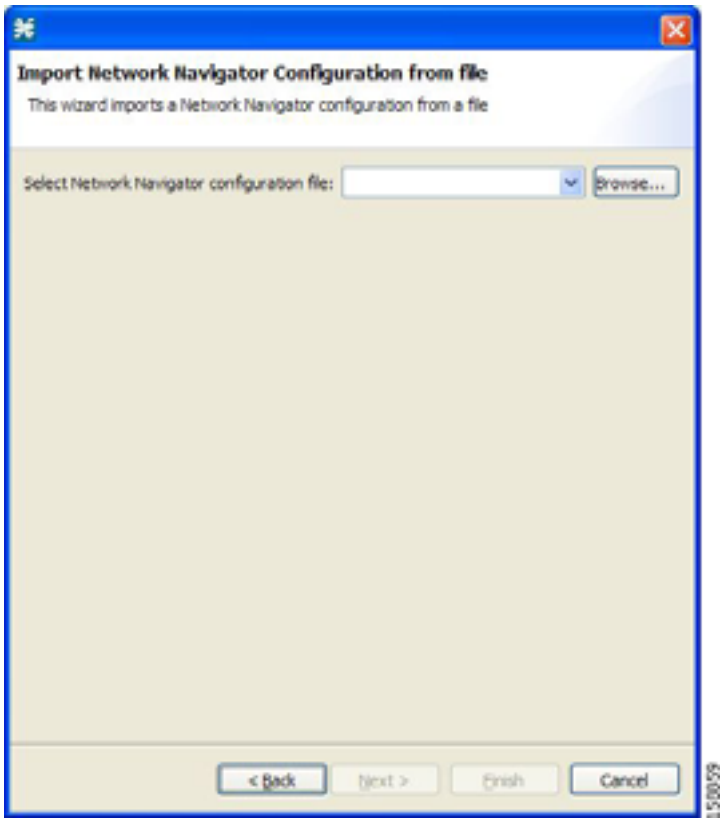
図 5-23

ステップ 2　インポート元のリストから、**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 5-24



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。

CHAPTER 6

Service Configuration Editor の使用

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。

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

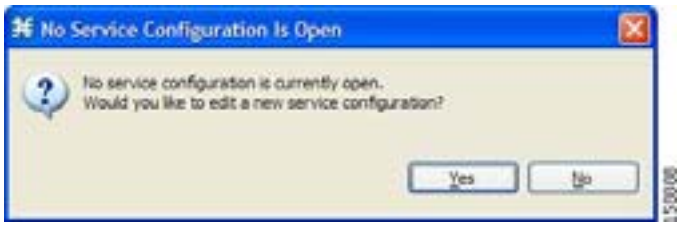
ここでは、次の操作について説明します。

- 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 1 つもないと、No Service Configuration Is Open ダイアログボックスが表示されます。

図 6-1



- 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（「新しいサービス コンフィギュレーションの追加」[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、開いているサービス コンフィギュレーションが 1 つ以上ある場合だけです。

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。

新しいサービス コンフィギュレーションの追加

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することはできません。

新しいサービス コンフィギュレーションを追加するには、次の手順を実行します。

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

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イネーブルにすると、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が可能です。このモードがイネーブルになっている場合、一部の分類、レポーティング、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.10-34] を参照）。

ステップ 4　**OK** をクリックします。

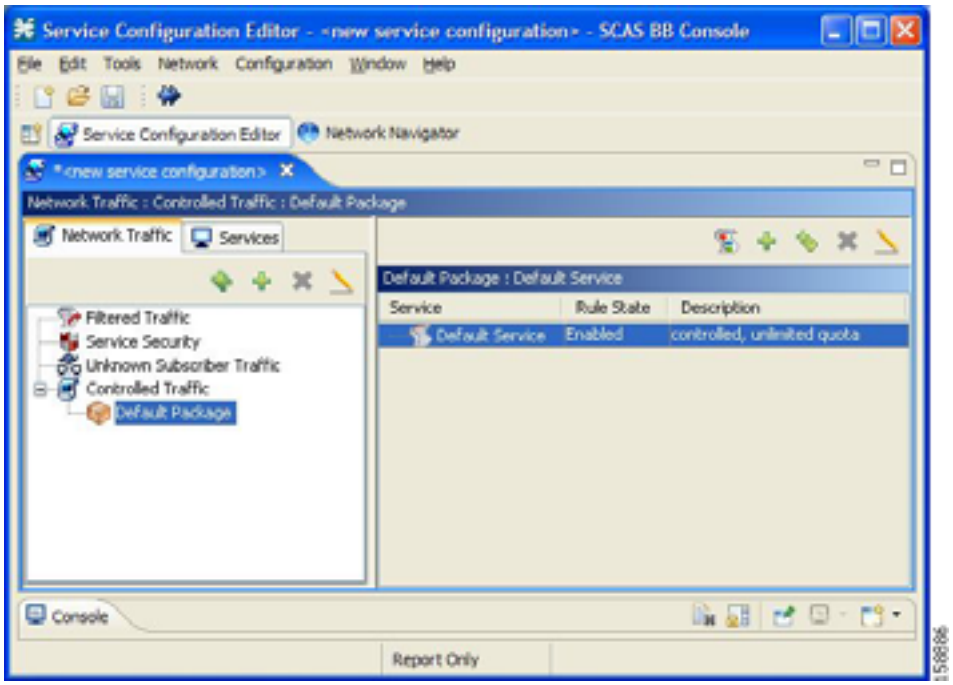
- デフォルト DSS ファイルを設定した場合（「デフォルト DSS ファイル」[p.7-45] を参照）は、Default Signature メッセージが表示されます。

図 6-3

- （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 タブが開き、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



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、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。

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。

サービス コンフィギュレーションファイルを開くには、次の手順を実行します。

ステップ 1　次のうちいずれかを実行します。

- Console のメイン メニューから **File >Open Service Configuration** の順番に選択します。
- Console のツールバーで、（**Open A Service Configuration 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　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。

ステップ 4　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

- （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。
- Console ウィンドウのタイトルには、このサービス コンフィギュレーション名が含まれます。

現在のサービス コンフィギュレーションの保存

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 ファイルに現在のサービス コンフィギュレーションを保存するには、次の手順を実行します。

ステップ 1　Console のメイン メニューから **File >Save As** の順番に選択します。

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

ステップ 1　Console のツールバーで、（**Save**）をクリックします。

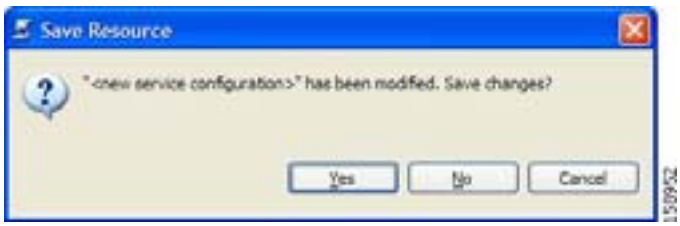
現在のサービス コンフィギュレーションが PQB ファイルからロードされていない場合（つまり、新規の場合や、SCE プラットフォームから取得した場合）、前の手順で Save As ダイアログ ボックスが開きます。

サービス コンフィギュレーションの閉じ方

ステップ 1　service configuration 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



ステップ 2　**Yes** をクリックします。

- 既存の編集済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、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て、**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

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。

1 つのサービス コンフィギュレーション要素を CSV ファイルにエクスポートするには、次の手順を実行します。

手順の概要

1. Console のメイン メニューから **File >Export** の順番に選択します。
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。
3. **Next** をクリックします。
4. **Select service configuration element to export** のオプション ボタンを 1 つ選択します。
5. Flavors を選択した場合は、**flavor type** オプション ボタンの 1 つを選択します。
6. **Next** をクリックします。
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。
8. Select the export destination 領域で、**Browse** をクリックします。
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。
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。
11. **Open** をクリックしてファイルを選択します。
12. **Finish** をクリックします。
13. **OK** をクリックします。

手順の詳細

ステップ 1　Console のメイン メニューから **File >Export** の順番に選択します。

Export ダイアログ ボックスが表示されます。

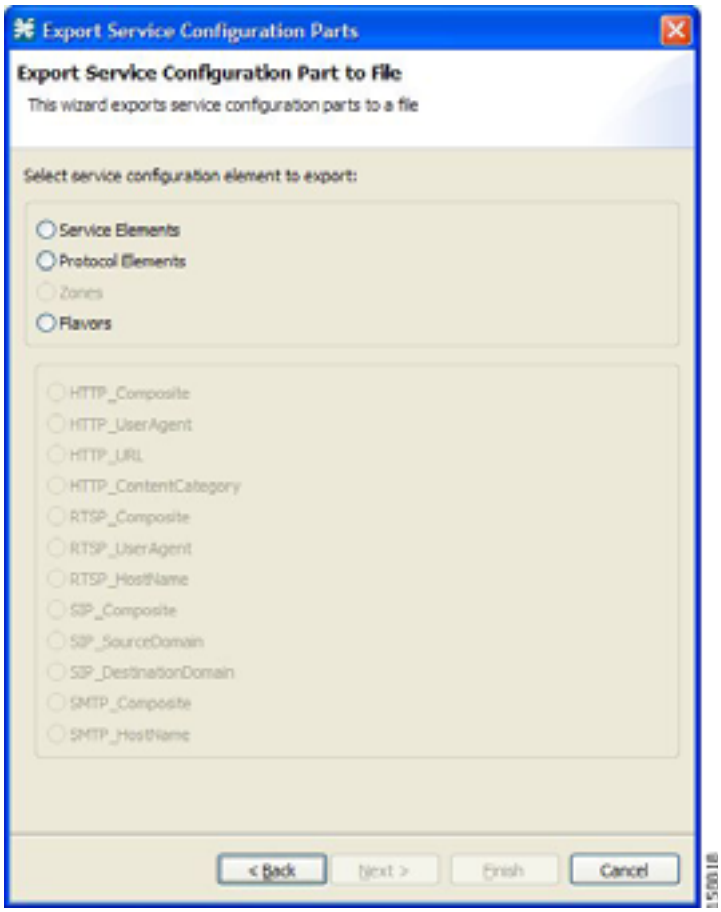
図 6-7

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



ステップ 4　**Select service configuration element to export** のオプション ボタンを 1 つ選択します。

- **Service Elements**
- **Protocol Element**
- **Zone**
- **Flavors**

Flavors を選択した場合、ダイアログ ボックス内にある flavor 領域の flavors がイネーブルになります。

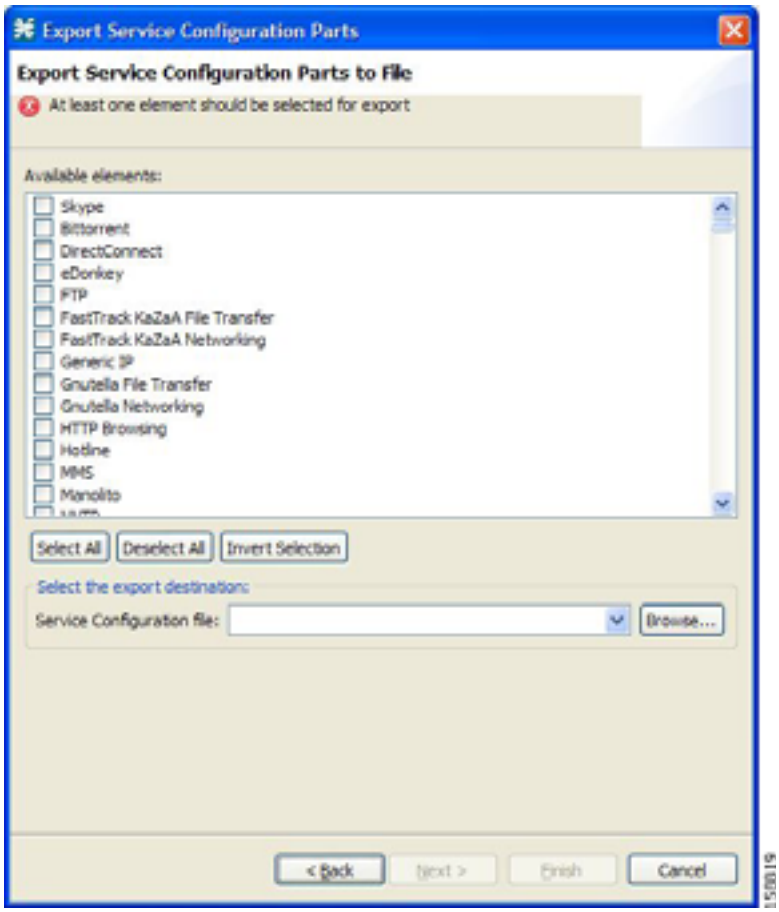
（注）　このサービス コンフィギュレーション内で flavor タイプが定義されている flavors のみがイネーブルになります。

ステップ 5　Flavors を選択した場合は、**flavor type** オプション ボタンの 1 つを選択します。

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 2 番めの画面が開きます。

図 6-9



Available elements 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。

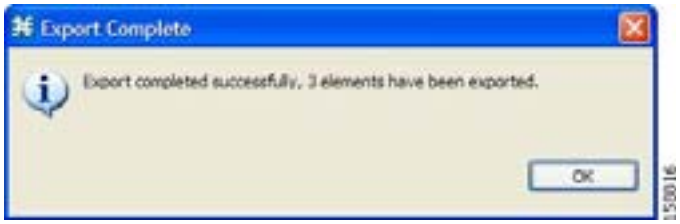
Open ダイアログボックスが閉じます。

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



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

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。

1 つのサービス コンフィギュレーション要素を CSV ファイルからインポートするには、次の手順を実行します。

手順の概要

1. Console のメイン メニューから **File >Import** の順番に選択します。
2. インポート元リストから、**Import service configuration parts from CSV file** を選択します。
3. **Next** をクリックします。
4. **Select service configuration element to import** のオプション ボタンを 1 つ選択します。
5. Flavors を選択した場合は、**flavor type** オプション ボタンの 1 つを選択します。
6. **Next** をクリックします。
7. **Browse** をクリックします。
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。
9. **Open** をクリックしてファイルを選択します。
10. **Finish** をクリックします。
11. **OK** をクリックします。

手順の詳細

ステップ 1　Console のメイン メニューから **File >Import** の順番に選択します。

Import ダイアログボックスが表示されます。

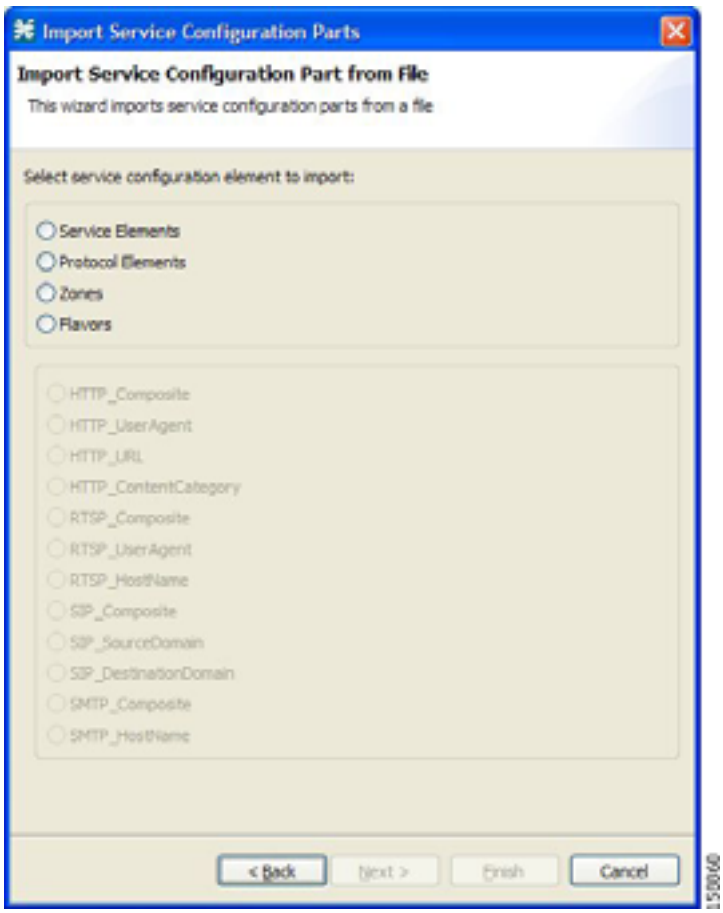
図 6-11

ステップ 2　インポート元リストから、**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



ステップ 4　**Select service configuration element to import** のオプション ボタンを 1 つ選択します。

- **Service Elements**
- **Protocol Element**
- **Zone**
- **Flavors**

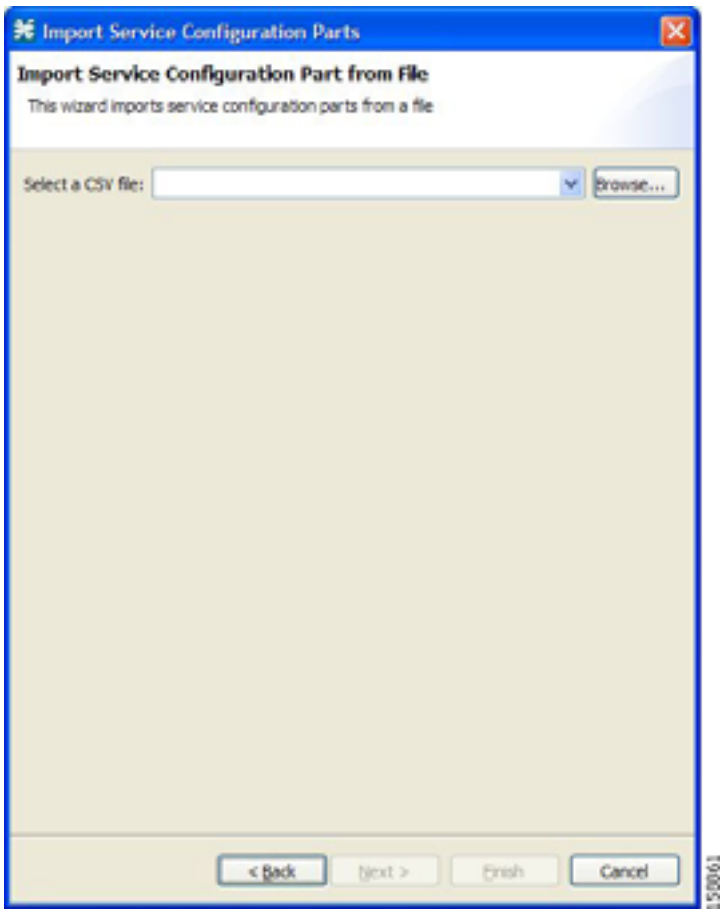
Flavors を選択した場合、ダイアログ ボックス内にある flavor 領域の flavors がイネーブルになります。

ステップ 5　Flavors を選択した場合は、**flavor type** オプション ボタンの 1 つを選択します。

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 2 番めの画面が開きます。

図 6-13



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。

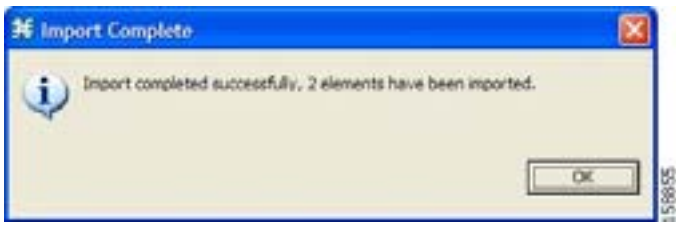
Open ダイアログボックスが閉じます。

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



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** の使用方法（「SCA BB Service Configuration Utility についての情報」[p.13-2] を参照）

現在のサービス コンフィギュレーションの検証

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更新済みサービス 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にのみ、Validation Results ダイアログ ボックスが表示されます。

現在のサービス コンフィギュレーションを検証するには、次の手順を実行します。

ステップ 1　Console のメイン メニューから **File >Validate** の順番に選択します。

Validation Results ダイアログボックスが表示されます。

図 6-15

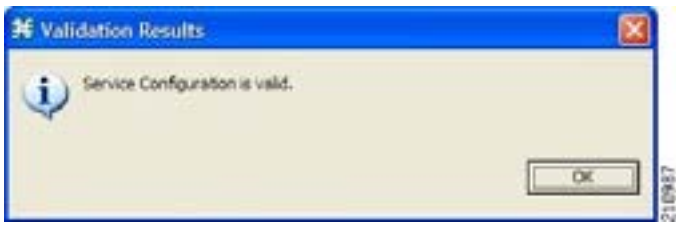
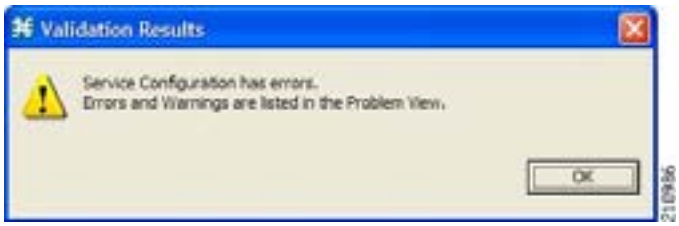


図 6-16



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

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。

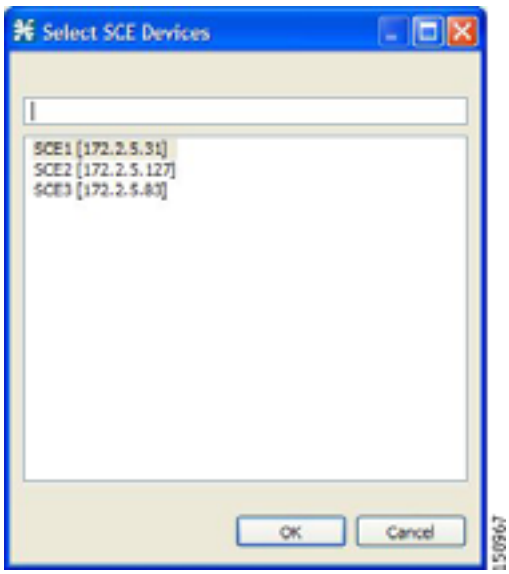
（注）　サービス コンフィギュレーションを手動で検証するには、**Validate** メニューを使用します。

SCE プラットフォームに現在のサービス コンフィギュレーションを適用するには、次の手順を実行します。

ステップ 1　Console のツールバーで、（**Apply Service Configuration to SCE Devices**）を選択します。

SCE Devices ダイアログ ボックスが表示されます。

図 6-17



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。

選択された各プラットフォームに対して 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（詳細は、「Network Navigator ツール」[p.5-2] を参照してください）。

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、この手順を繰り返します。
- 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

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。

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 ― （任意）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（「サービスの追加と定義」[p.7-3] を参照）。これらはいつでも変更できます（「サービスの編集」[p.7-8] を参照）。

サービスの追加と定義について

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。

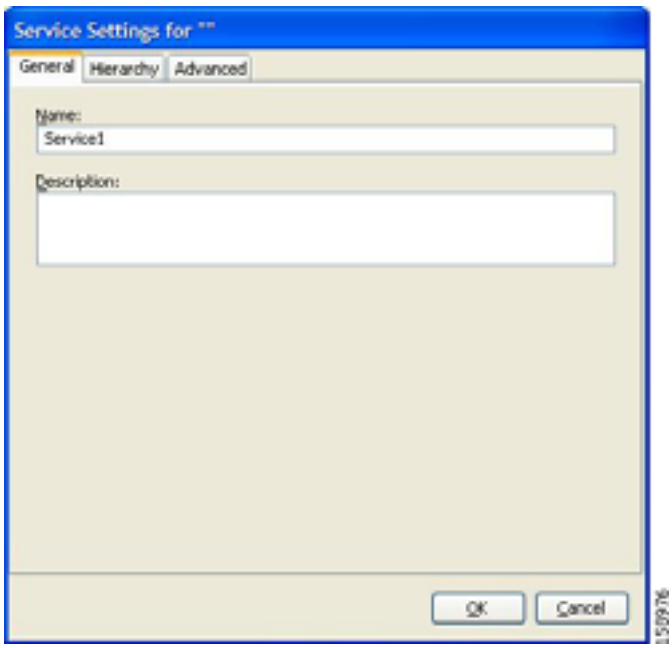
新しいサービスの追加および定義を行ったあと、そのサービスにサービス要素を追加できます（「サービス要素の追加」[p.7-11] を参照）。

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　左のペインで、 をクリックします（「**Add Service**」）。

Service Settings ダイアログボックスが表示されます。

図 7-1



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　（任意）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」（p.7-4）を参照して設定してください。

ステップ 6　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」（p.7-6）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 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。

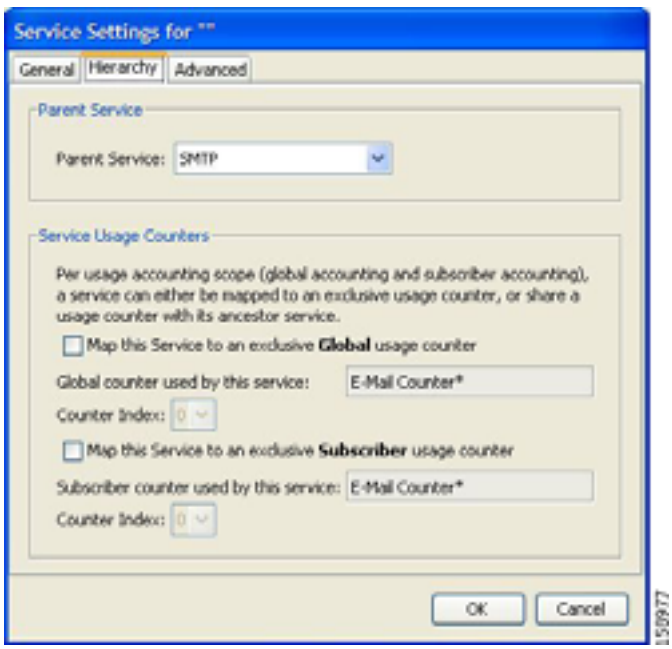
サービスが、階層で選択したサービスの子として、サービス ツリーに追加されます。

サービスの階層設定の定義

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 タブが表示されます。

図 7-2



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 リストが使用可能になります。

（任意）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 リストが使用可能になります。

（任意）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」（p.7-6）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

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 タブが表示されます。

図 7-3

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。

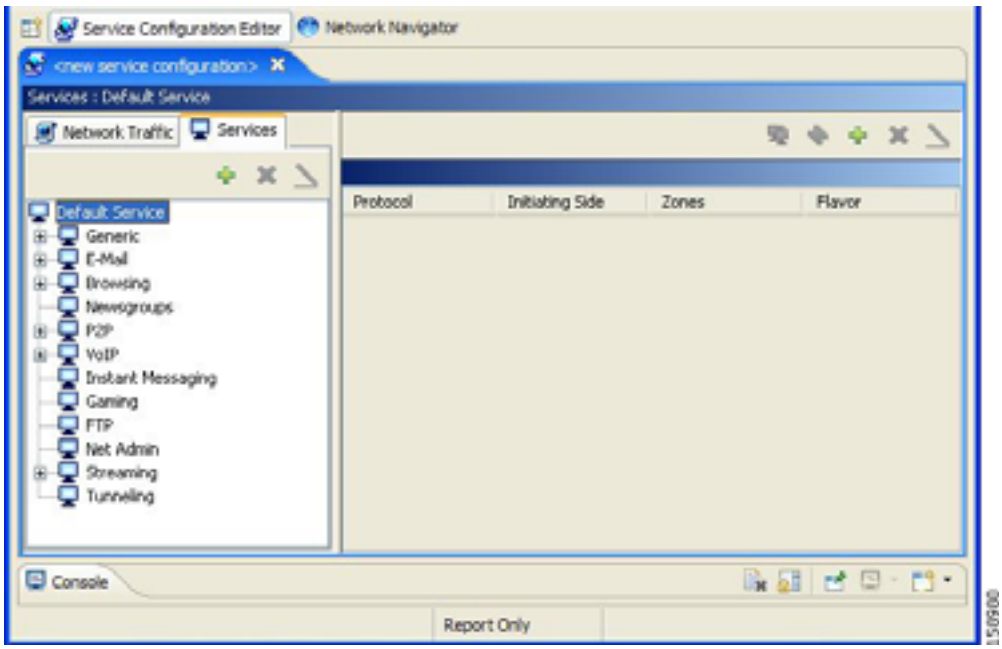
サービスの表示

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、**Services** タブをクリックします。

Services タブが表示されます。

図 7-4

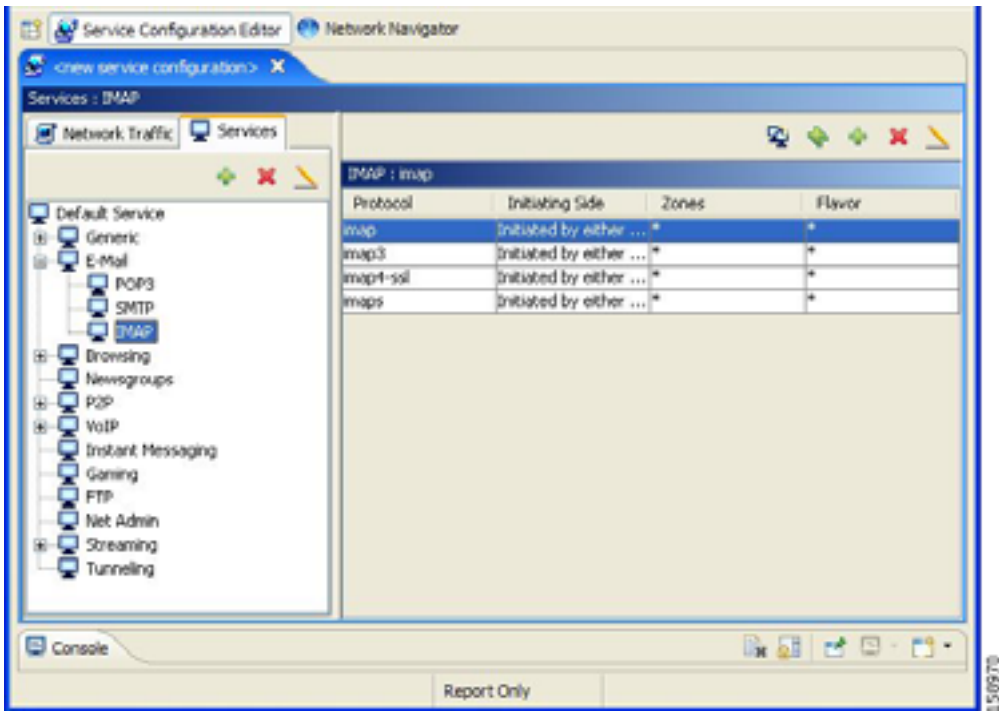


サービス ツリー（左側のペイン）に、サービスのリストが表示されます。

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。

右側のペイン（サービス要素）に、該当するサービスに対して定義されたサービス要素のリストが表示されます。

図 7-5



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。

サービスの編集

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.7-11）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　サービスに新しい名前を割り当てるには、Name フィールドに新しい名前を入力します。

ステップ 4　サービスに新しい説明を割り当てるには、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 タブが表示されます。

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、次の手順を実行します。

— **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 リストが使用可能になります。

(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、次の手順を実行します。

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 リストが使用可能になります。

f. 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。

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 タブが表示されます。

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

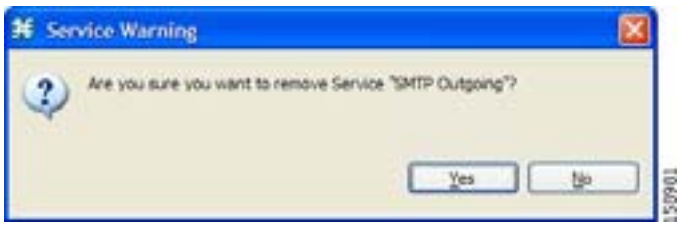
サービスは、Console でインストールしたものも含めて、削除できます。ただし、デフォルト サービスは削除できません。

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 7-6



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.9-12] を参照）、Service Warning メッセージがもう 1 つ表示されます。

図 7-7

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.7-22）、「ゾーンの管理」（p.7-33）、および「フレーバの管理」（p.7-51）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に一致している
- 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

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。

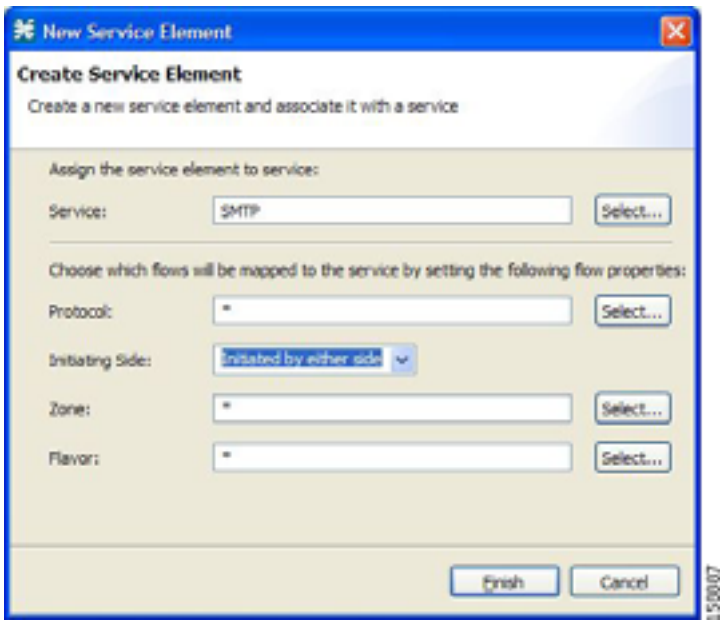
手順の詳細

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　右のペイン（サービス要素）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。

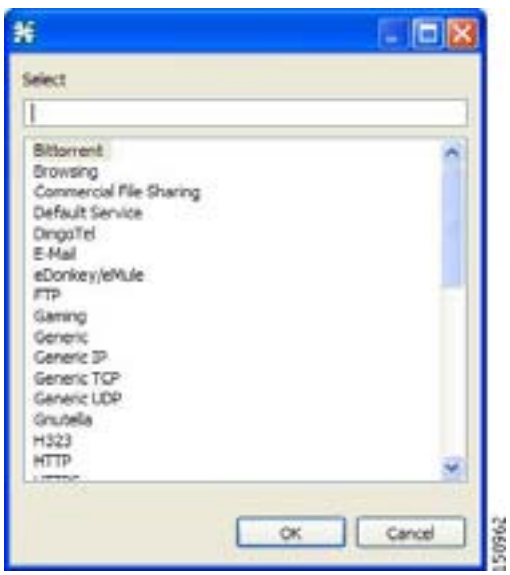
図 7-8



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、サービスのリストが表示されます。

図 7-9



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。

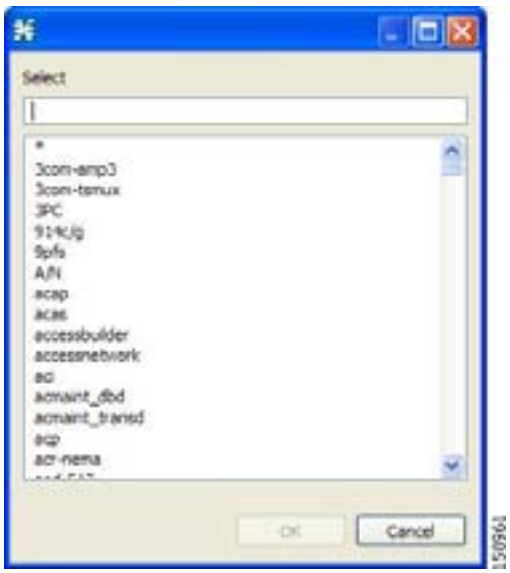
選択したサービスが、New Service Element ダイアログボックスの Service フィールドに表示されます。

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、プロトコルのリストが表示されます。

図 7-10



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。

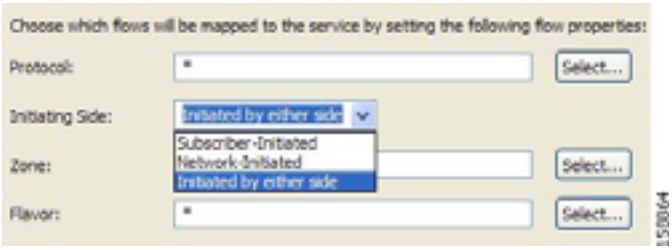
ステップ 8　**OK** をクリックします。

Select a Protocol ダイアログボックスが閉じます。

選択したサービスが、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 フィールドで、ドロップダウン アローをクリックします。

図 7-11



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、ゾーンのリストが表示されます。

図 7-12

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。

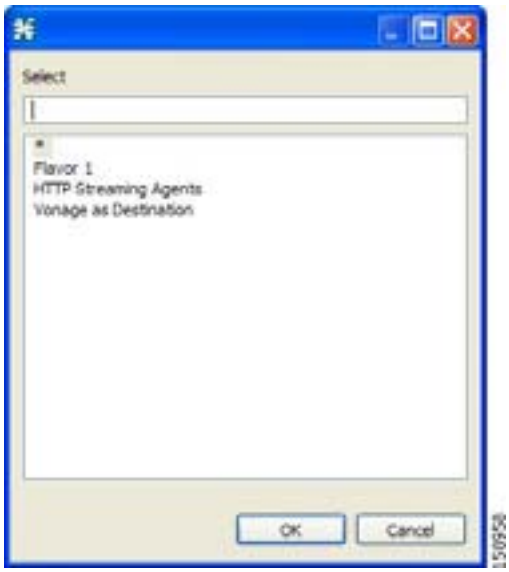
選択したゾーンが、New Service Element ダイアログボックスの Zone フィールドに表示されます。

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。

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、フレーバのリストが表示されます。

図 7-13



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。

Service Elements 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

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写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。

サービス要素を複製するには、次の手順を実行します。

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。

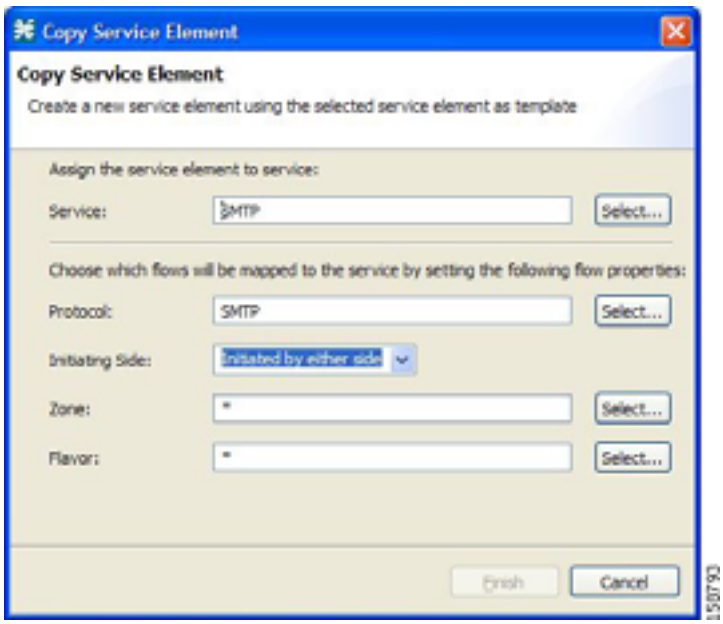
Service Elements ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　Service Elements 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 7-14



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」[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

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。

サービス要素を編集するには、次の手順を実行します。

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。

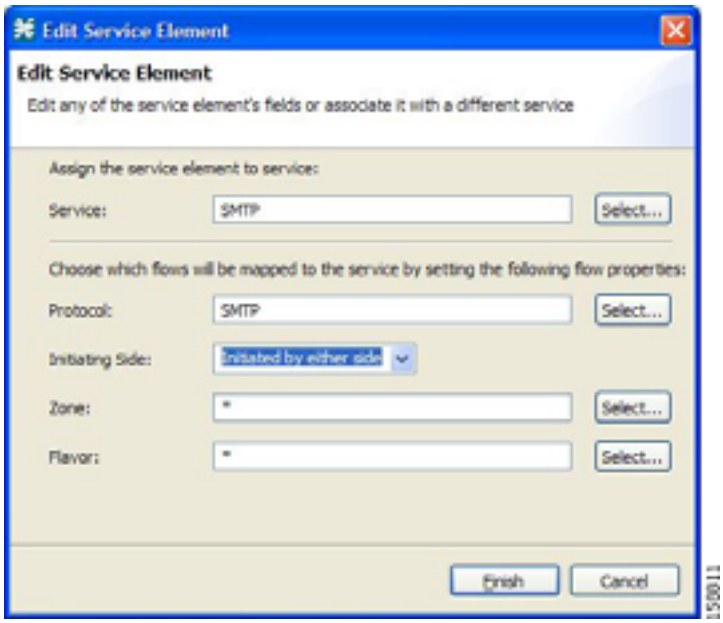
Service Elements ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　Service Elements 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　Services Elements 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 7-15



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、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、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 アローをクリックします。

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、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、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。

Service Elements 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

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。

サービス要素を削除するには、次の手順を実行します。

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。

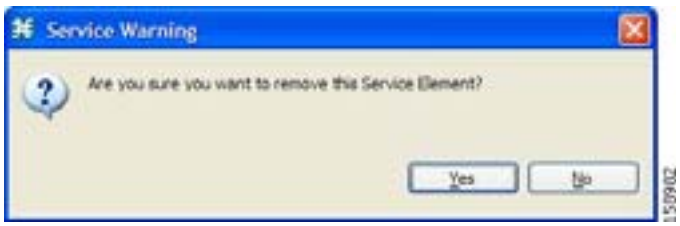
Service Elements ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　Service Elements 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　Service Elements 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 7-16



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

サービス間で既存のサービス要素を移動できます。

サービス要素を移動するには、次の手順を実行します。

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。

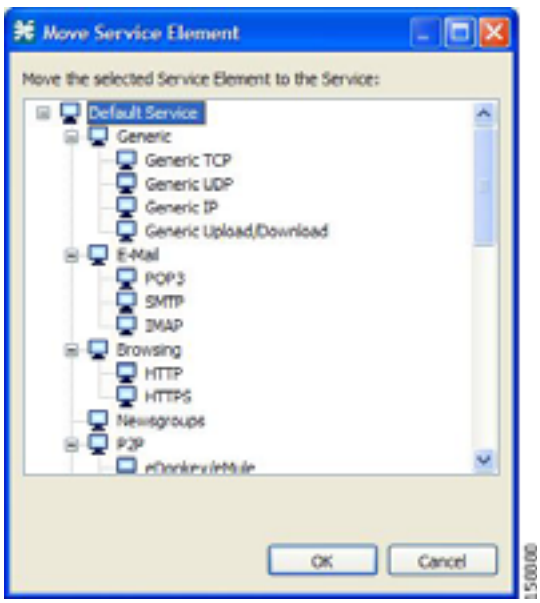
Service Elements ペインに、関連するサービス要素のリストが表示されます。

ステップ 2　Service Elements 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、完全なサービス ツリーが表示されます。

図 7-17



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、宛先ポートあるいはポート、一意の名前および説明（任意）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.7-11] 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」の章の「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シグニチャの追加」[p.7-43] 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。

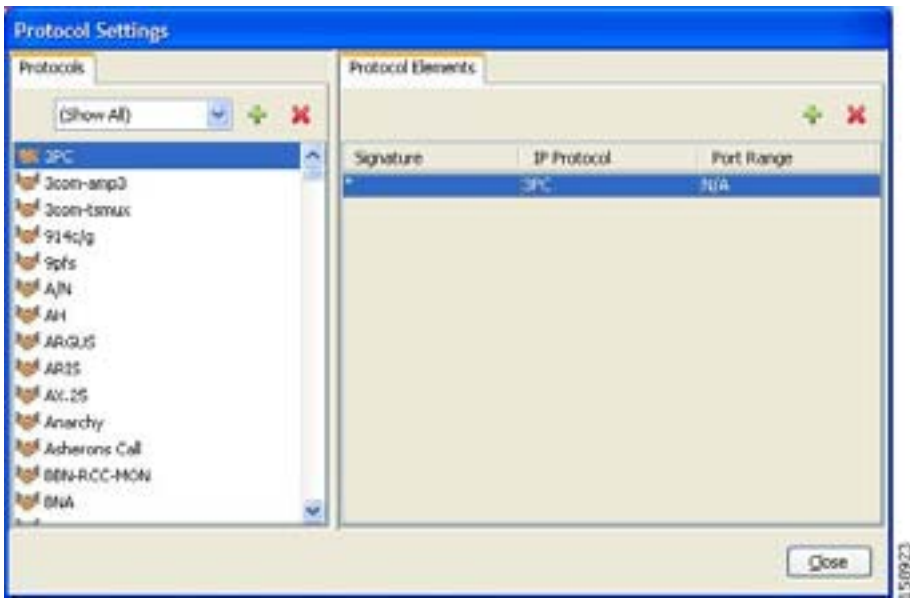
プロトコルは、ASCII の順（0 ... 9、A ... Z、a ... z）にソートされて表示されます。

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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

Protocol Settings ダイアログボックスが表示されます。

図 7-18



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、次の手順を実行します。

a. 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、プロトコル名、説明、ID が表示されます。

図 7-19

b. **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 3　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 4　**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。

Protocols View タブのリストのフィルタリング

Protocols View タブのリストのフィルタリング

プロトコルをタイプを基準としてフィルタリングし、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 9 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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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。

ステップ 4　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

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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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 7-20

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　（任意）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」（p.7-28）を参照してください。

プロトコルの編集

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.7-28）を参照してください。

ステップ 1　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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表示されます。

図 7-21

ステップ 3　ダイアログボックスの次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

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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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。

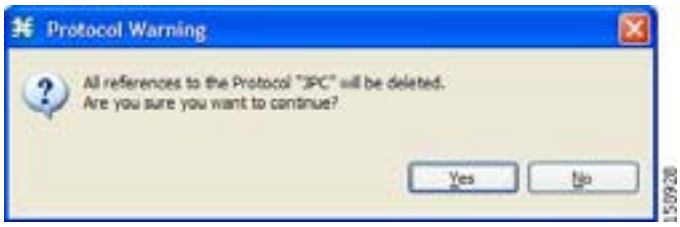
Protocol Warning メッセージが表示されます。

図 7-22

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.7-11] 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 7-23



- **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

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。

手順の詳細

ステップ 1　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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。

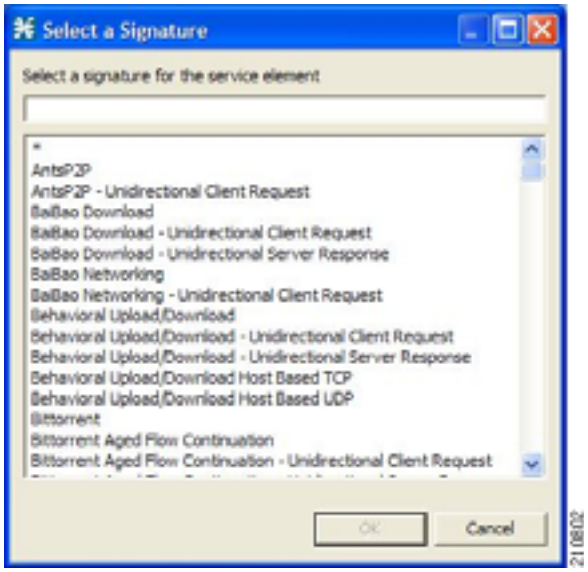
そのプロトコルにプロトコル要素が追加されます。

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。

図 7-24



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。

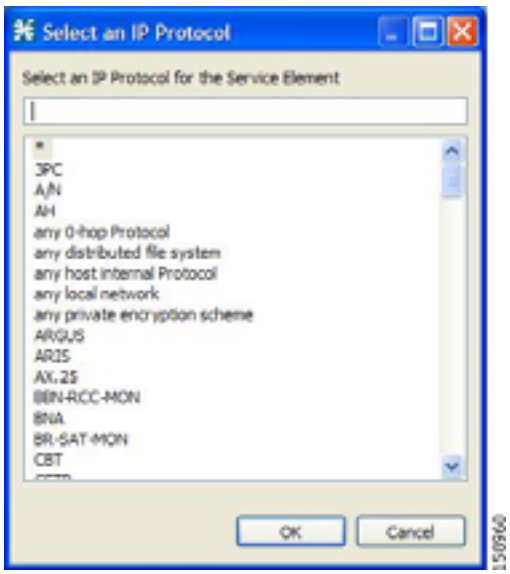
選択したシグニチャが、Protocol Settings ダイアログボックスの Signature セルに表示されます。

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、IP プロトコルのリストが表示されます。

図 7-25



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）のみです。

ポートがこれらのいずれかのポートと一致するフローのみが、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。

- 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 7-26

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

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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

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。

- 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

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　Console のメイン メニューから **Configuration >Protocols** の順番に選択します。

Protocol Settings ダイアログボックスが表示されます。

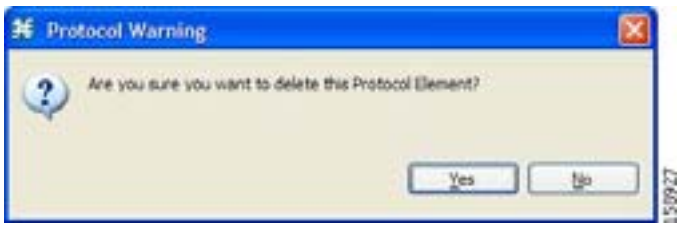
ステップ 2　Protocols タブでプロトコルを選択します。

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 7-27



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（p.7-33）
- ゾーンの追加（p.7-34）
- ゾーンの編集（p.7-35）
- ゾーンの削除（p.7-36）
- ゾーン項目の管理（p.7-37）

ゾーンの表示

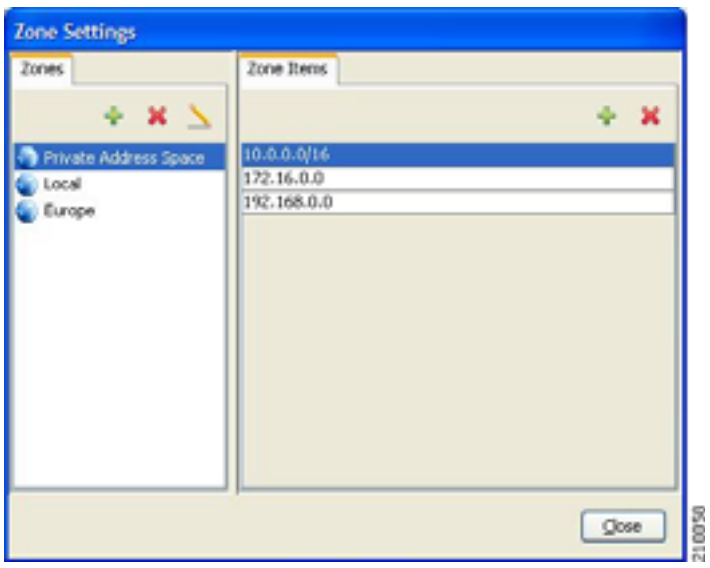
ゾーンのリストと、関連するゾーン項目を表示できます。

ステップ 1　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

Zone Settings ダイアログボックスが表示されます。

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 7-28



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

ステップ 1　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

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 7-29

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　（任意）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」[p.7-37] を参照）。

ゾーンの編集

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.7-37）を参照してください。

ステップ 1　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

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次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

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　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

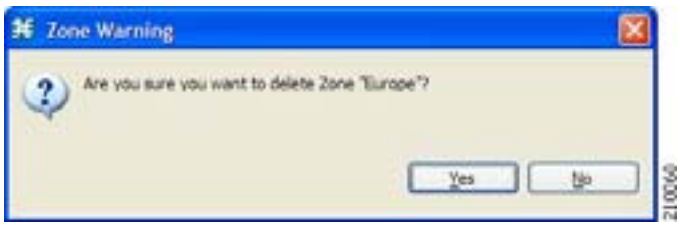
Zone Settings ダイアログボックスが表示されます。

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。

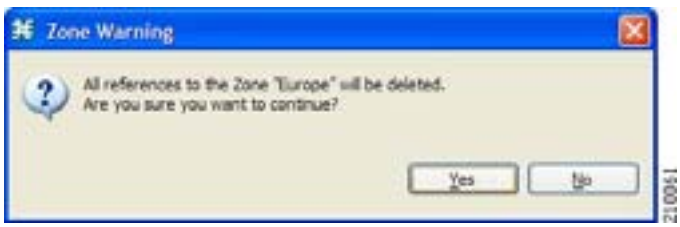
図 7-30



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 7-31



- **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

ゾーンとは、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（p.7-37）
- ゾーン項目の削除（p.7-37）

ゾーン項目の追加

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　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

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、1 つの IP アドレス（例：63.111.106.7）または IP アドレスの範囲（例：194.90.12.0/24）です。

ステップ 5　このゾーンに属するすべての 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。

- 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。

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

ステップ 1　Console のメイン メニューから **Configuration >Zones** の順番に選択します。

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

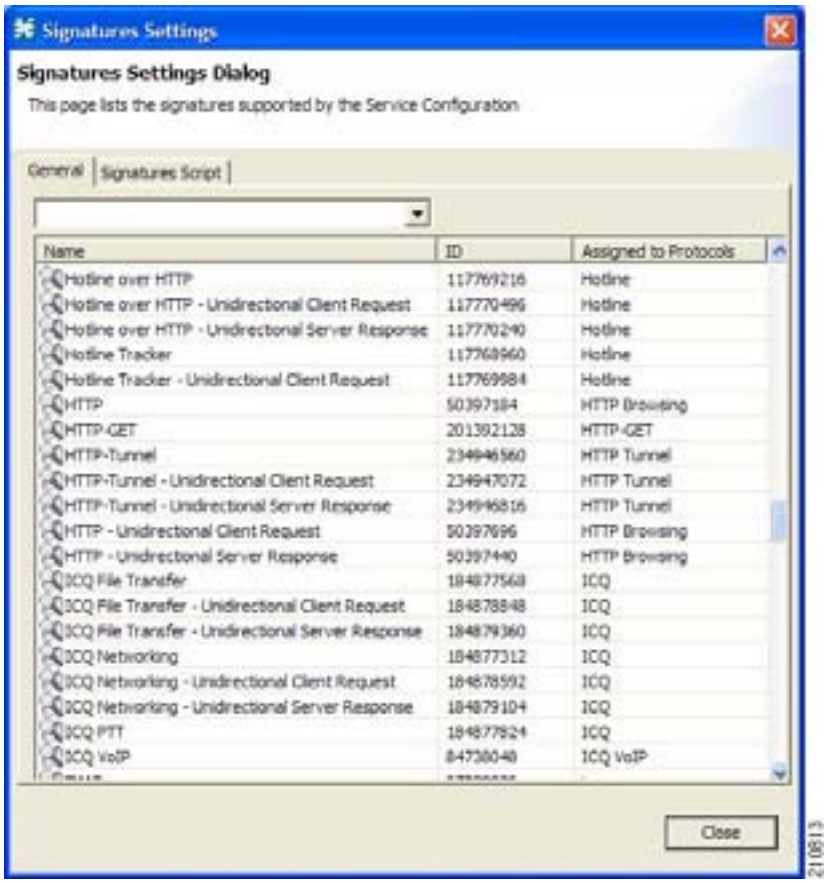
シグニチャの表示

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　Console のメイン メニューから **Configuration >Signatures Settings** の順番に選択します。

Signatures Settings ダイアログボックスが表示されます。

図 7-32



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。

シグニチャ設定のフィルタリング

シグニチャ設定のフィルタリング

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のみが 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 メニューから **Configuration >Signatures Settings** の順番に選択します。

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紹介されています。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有益です。

- 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 パックのインストール方法」（p.4-13）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 Service Configuration Utility についての情報」（p.13-2）を参照してください。

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） 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。

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シグニチャの追加」（p.7-43）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 ファイルの管理についての情報」[p.12-2] を参照）。

現在のダイナミック シグニチャ情報の表示

ステップ 1　Console のメイン メニューから **Configuration >Signatures Settings** の順番に選択します。

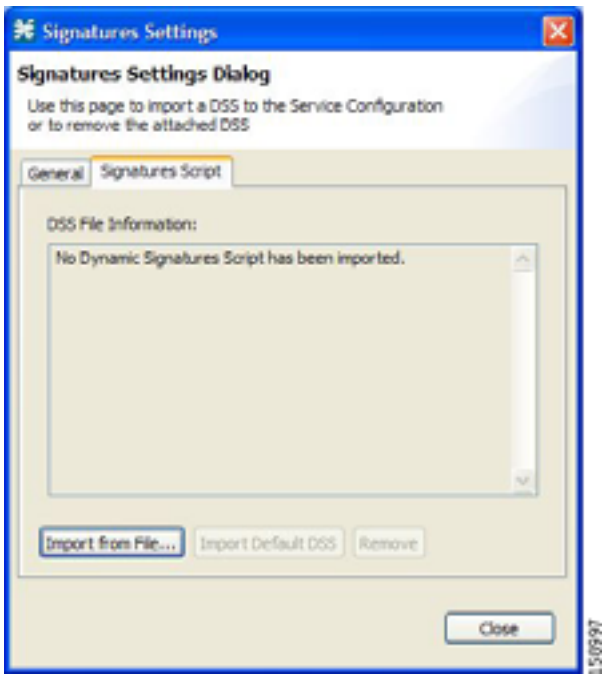
Signatures Settings ダイアログボックスが表示されます。

ステップ 2　**Signatures Script** タブをクリックします。

Signatures Script タブが表示されます。

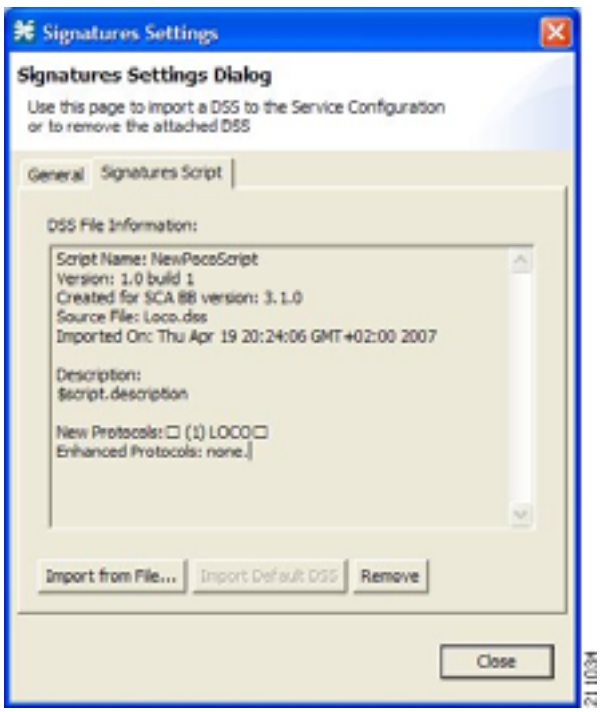
- 現在のサービス コンフィギュレーションに DSS ファイルがインポートされていない場合、Signatures Settings ダイアログボックスにメッセージが表示されます。

図 7-33



- 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 7-34



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シグニチャの追加

サービス コンフィギュレーションへのシグニチャの追加

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 ファイルの管理についての情報」[p.12-2] 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 ファイルからのダイナミック シグニチャのインポート」[p.7-48] 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　Console のメイン メニューから **Configuration >Signatures Settings** の順番に選択します。

Signatures Settings ダイアログボックスが表示されます。

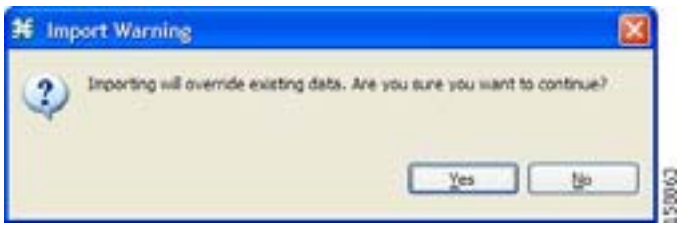
ステップ 2　**Signatures Script** タブをクリックします。

Signatures Script タブが表示されます。

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 7-35



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

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　Console のメイン メニューから **Configuration >Signatures Settings** の順番に選択します。

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 タブが表示されます。

ステップ 3　**Remove** をクリックします。

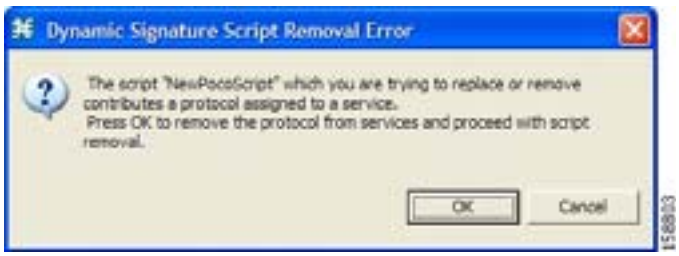
Dynamic Signature Script Confirmation メッセージが表示されます。

図 7-36

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 7-37



- **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 ボタンが使用可能になります。

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 パックは、SPQI ファイルまたは 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サービス コンフィギュレーションにアップデートを自動的に提供するか、またはワークステーションから SCE プラットフォームに適用します。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 ユーティリティについての情報」（p.13-8）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 ユーティリティについての情報」[p.13-8] 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

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.12-14] 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。

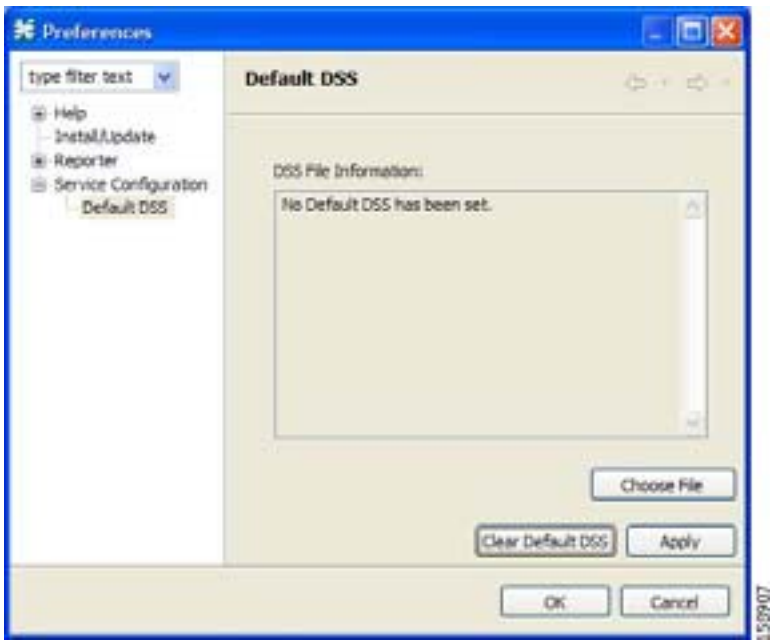
ステップ 1　Console のメイン メニューから **Window >Preferences** の順番に選択します。

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のペインのメニュー 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のペインに、Default DSS 領域が表示されます。

図 7-38



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の パックのファイル タイプを選択します。

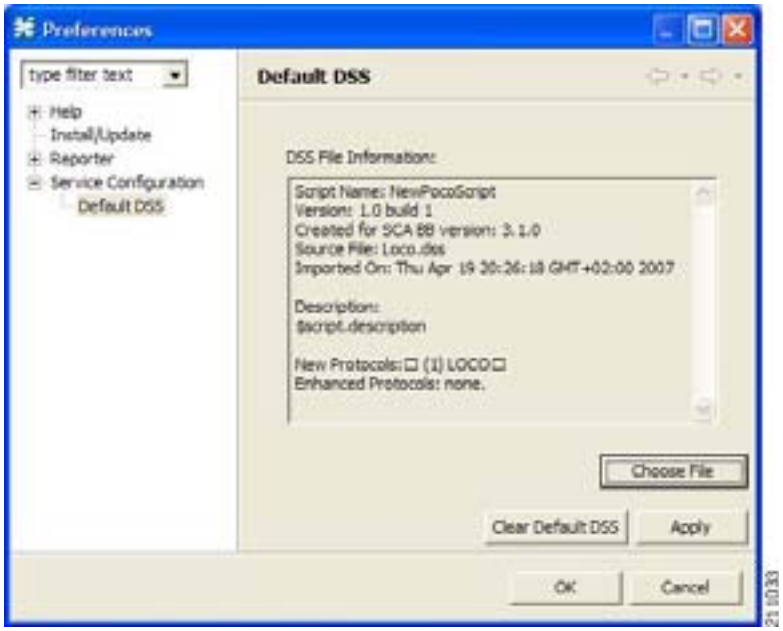
ステップ 5　プロトコル パックをブラウズします。

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 7-39



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\default3.1.0.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 ファイルの作成

ステップ 1　Console のメイン メニューから **Window >Preferences** の順番に選択します。

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のペインのメニュー 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のペインに、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\default3.1.0.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。

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 7-40

ステップ 2　次のうちいずれかを実行します。

- デフォルト DSS ファイルをインポートするには、**Yes** をクリックします。
- 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。

デフォルト DSS ファイルを手動でインポートするには

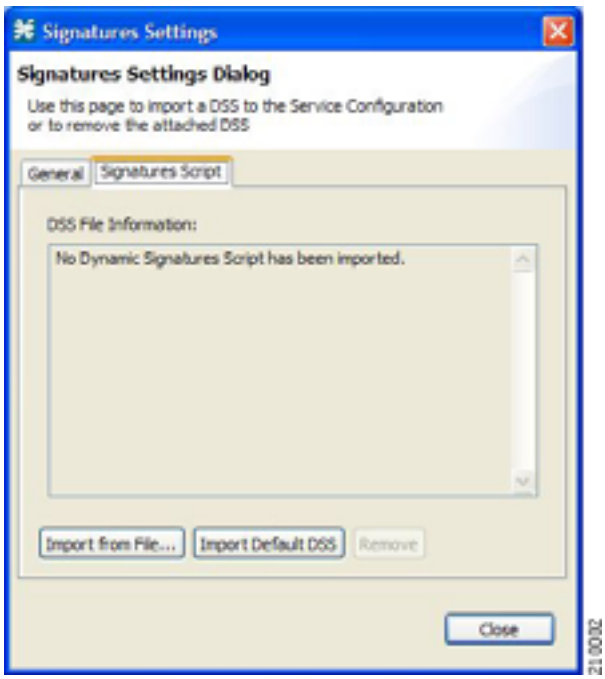
ステップ 1　Console のメイン メニューから **Configuration >Signatures Settings** の順番に選択します。

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、Import Default DSS ボタンがイネーブルになります。

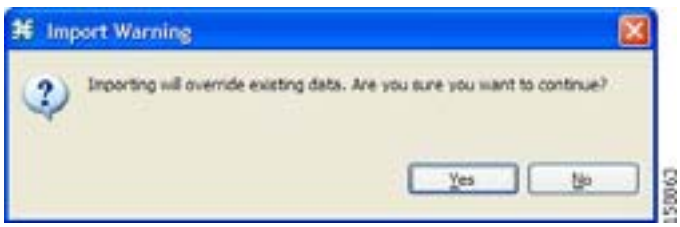
図 7-41



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 7-42



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ついてのみ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.7-56] 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 サービス コンフィギュレーションが非対称ルーティング分類モードで実行されている場合、トラフィックの分類にフレーバは使用されません。

フレーバ タイプとパラメータ

次の表に、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	有効な値
HTTP User Agent	プレフィクス文字列
HTTP URL	< 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 > • ホスト ― URL の初めから最初の「/」まで • パス ― 最初の「/」から「?」までのセクション • URL パラメータ ― 「?」の後ろのすべての文字列（パラメータのプレフィクスを「?」で開始する必要はありません）
HTTP Composite	<HTTP User Agent フレーバ、HTTP URL フレーバ >
HTTP Content Category	Select a Content Category ダイアログボックスで選択した値
RTSP User Agent	プレフィクス文字列
RTSP Host Name	ホスト サフィックス
RTSP Composite	<RTSP User Agent フレーバ、RTSP Host Name フレーバ >
SIP Source Domain	ホスト サフィックス
SIP Composite	<SIP Source Domain、SIP Destination Domain>
SMTP Host Name	ホスト サフィックス

（注） Composite フレーバは、定義された 2 つのフレーバのペアです。

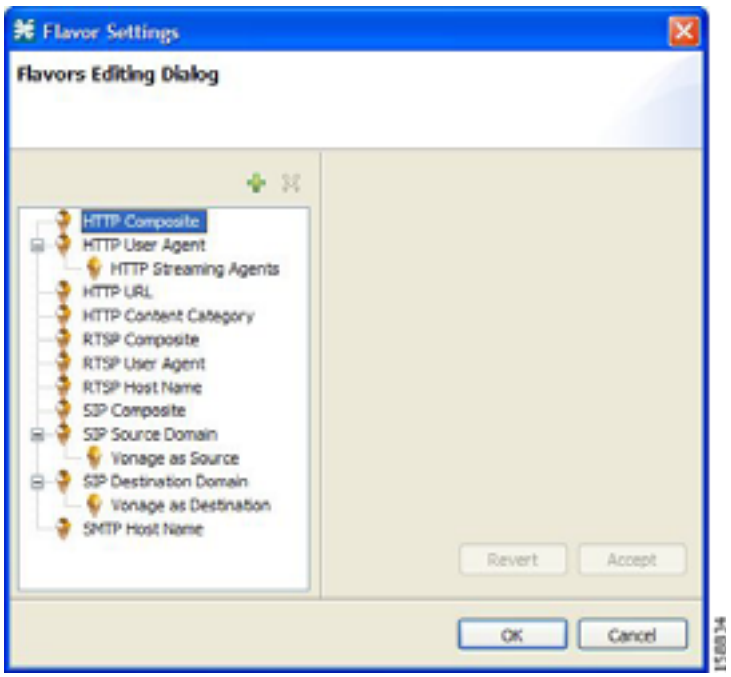
フレーバの表示

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　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

Flavor Settings ダイアログボックスが表示されます。

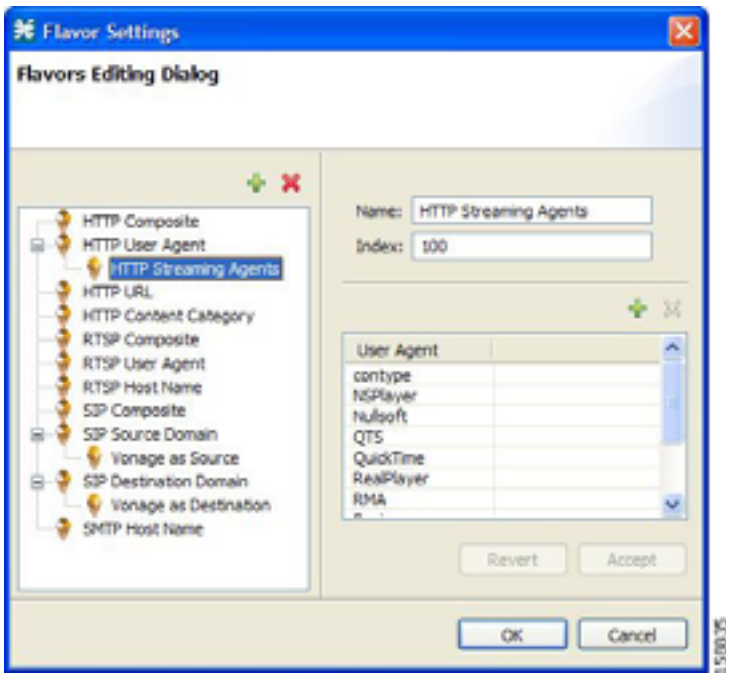
図 7-43



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 7-44



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

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　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

Flavor Settings ダイアログボックスが表示されます。

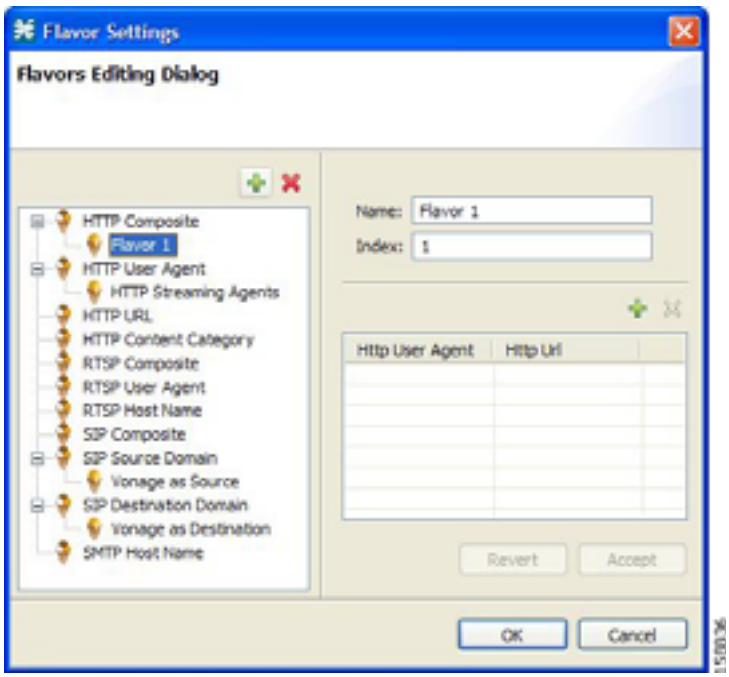
ステップ 2　フレーバ ツリーでフレーバ タイプを選択します。

グローバル コンフィギュレーション モードを開始します。

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 7-45



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)　フレーバのデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

ステップ 5　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」[p.7-57] を参照）。

フレーバの編集

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.7-56）を参照してください。

ステップ 1　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

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次のフィールドを修正します。

- 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

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　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

EnableThe Flavor Settings ダイアログボックスが表示されます。

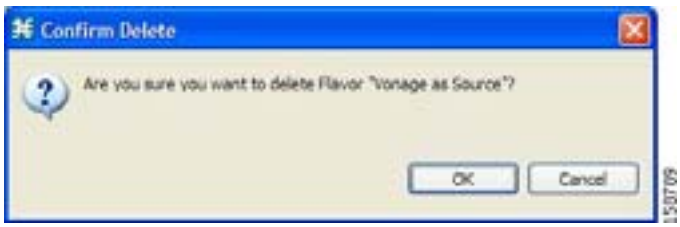
ステップ 2　フレーバ ツリーでフレーバを右クリックします。

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。

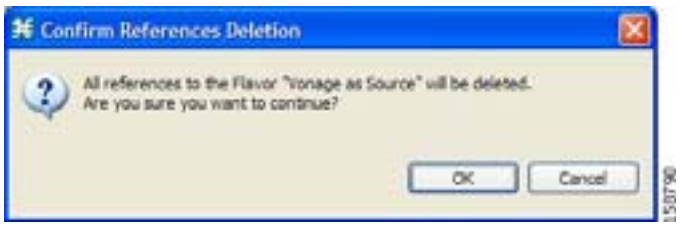
図 7-46



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 7-47



- **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.7-51] 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

次の表に、各フレーバ タイプごと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 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

フレーバ項目の追加

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）。

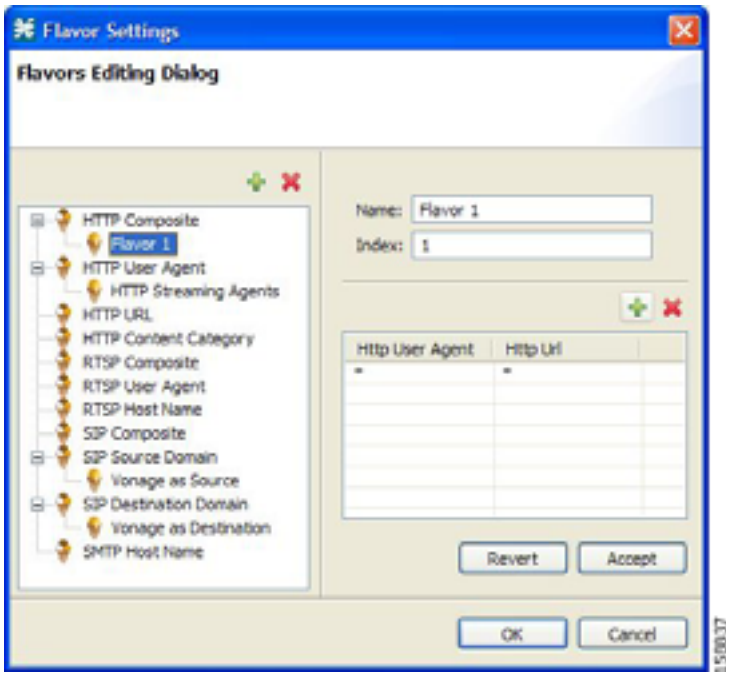
ステップ 1　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

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 7-48



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.7-51] 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に対して、次のいずれかを実行します。

- アスタリスクをクリックしてから、該当する値を入力します
- （Composite フレーバと HTTP Content Category フレーバの場合）。

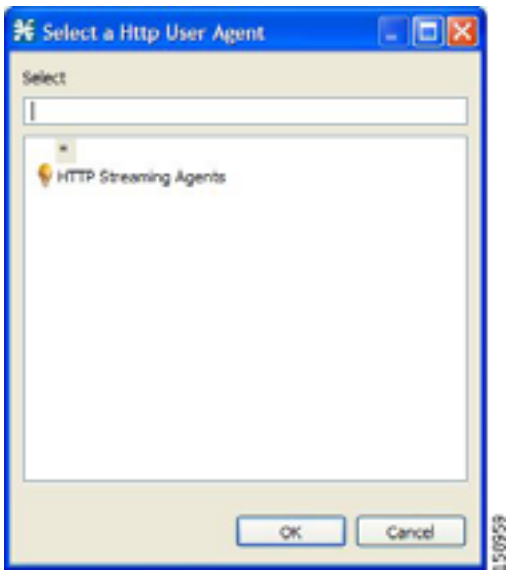
a. アスタリスクをクリックします。

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。

図 7-49



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

ステップ 1　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

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　新しいフレーバ項目の各セルに対して、次のいずれかを実行します。

- アスタリスクをクリックしてから、該当する値を入力します
- （Composite フレーバと HTTP Content Category フレーバの場合）。

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

ステップ 1　Console のメイン メニューから **Configuration >Flavors** の順番に選択します。

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。

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)　アクティブ サービス コンフィギュレーションが非対称ルーティング分類モードで実行されている場合、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 フィルタリングの概要

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 ― SCE プラットフォーム上で動作するシスコのサービス コントロール アプリケーション。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。
- Cisco CPA クライアント ― SCE プラットフォーム上で動作する CPA クライアント。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。
- SurfControl CPA サーバ ― 専用マシン上で動作する CPA サーバ。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。

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、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。

RDR フォーマッタの設定

SCE アプリケーションは、Raw Data Record（RDR）を使用して CPA クライアントと通信します。RDR フォーマッタでの HTTP カテゴリ化要求の発行を有効にするには、次の SCE プラットフォーム CLI を使用して、SCE プラットフォームで RDR フォーマッタを設定します。

```
#>RDR-formatter destination 127.0.0.1 port 33001 category number 4 priority 100
```

RDR フォーマッタの設定の詳細については、『*Cisco Service Control Engine (SCE) Software Configuration Guide*』の「Configuring the RDR Formatter」の章を参照してください。

SurfControl CPA サーバのインストール

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 を使用してコンテンツ フィルタリングを設定し、SCE プラットフォーム CLI を使用してモニタできます。SCE プラットフォーム CLI の詳細については、『*Cisco Service Control Engine (SCE) 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。

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 モードを開始して、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 #`）に `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。

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

次の表に、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）。	―

次の表には、Cisco CPA クライアントの監視時に表示される情報を示します。

表 7-4　CPA クライアント監視対象のパラメータ

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

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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

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。

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。

非対称ルーティング分類モードがイネーブルに設定されている場合、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。

ステップ 1　Console のメイン メニューから **File >Import** の順番に選択します。

Import ダイアログボックスが表示されます。

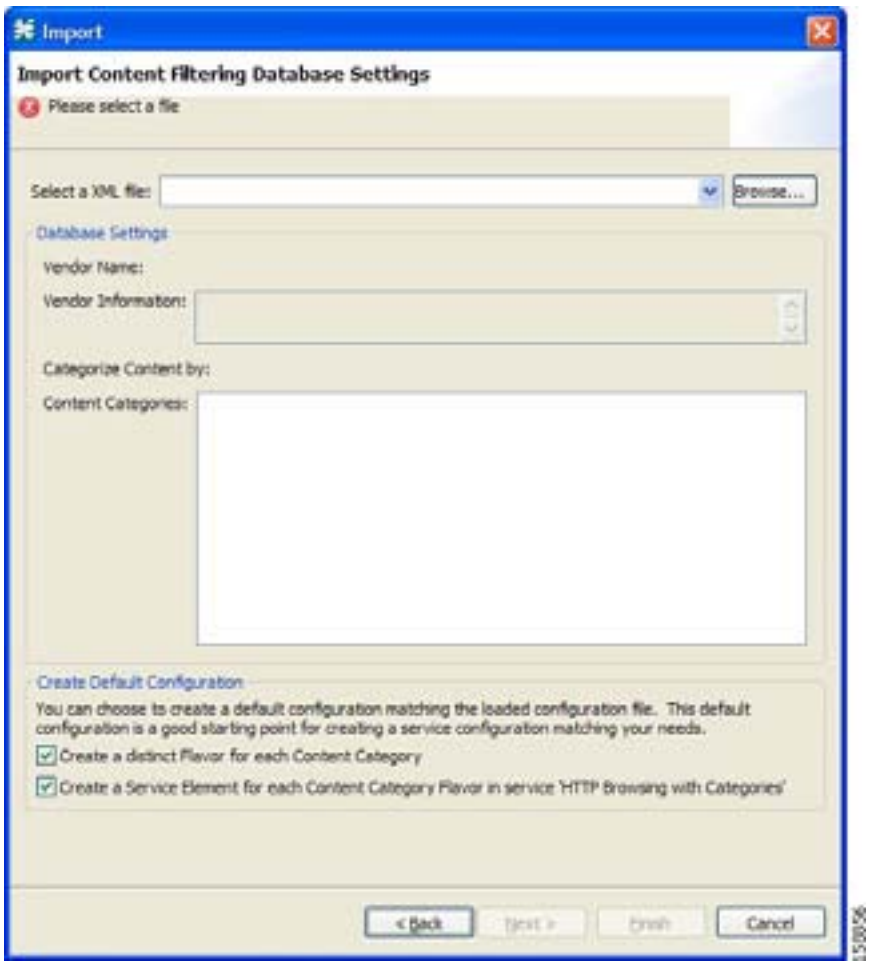
図 7-50

ステップ 2　インポート ソース 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 7-51



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。

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

（注）　これは、前の手順と同等です。

ステップ 1　Console のメイン メニューから **Configuration >Content Filtering** の順番に選択します。

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 タブが表示されます。

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。

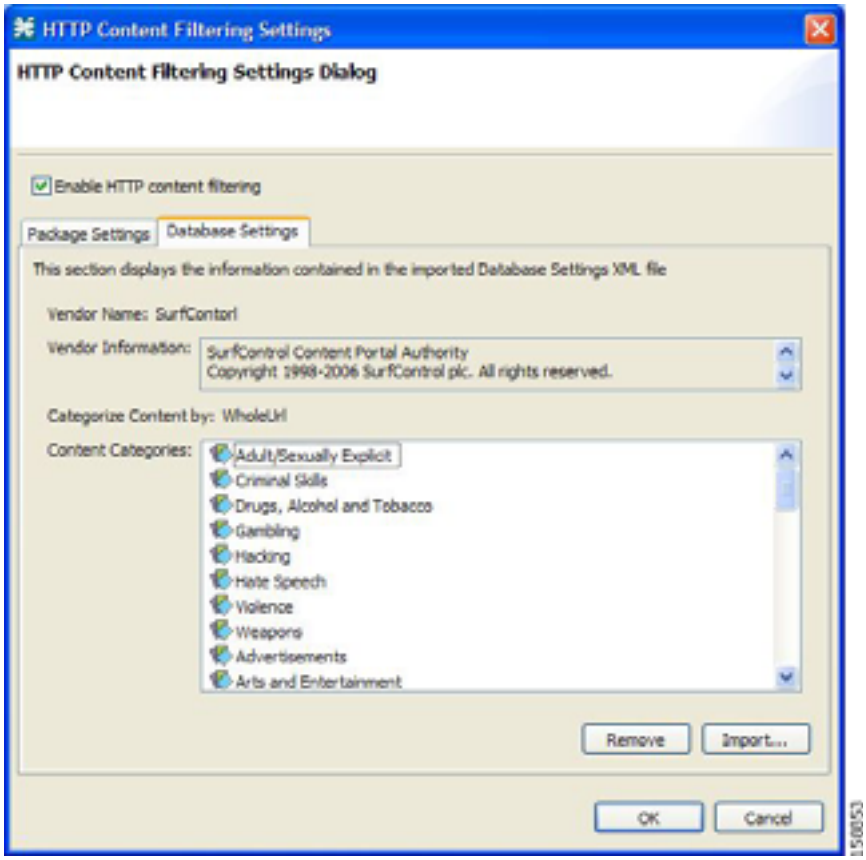
ステップ 4　前の手順のステップ 4 ～ 8 を実行します。

ステップ 5　**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 7-52



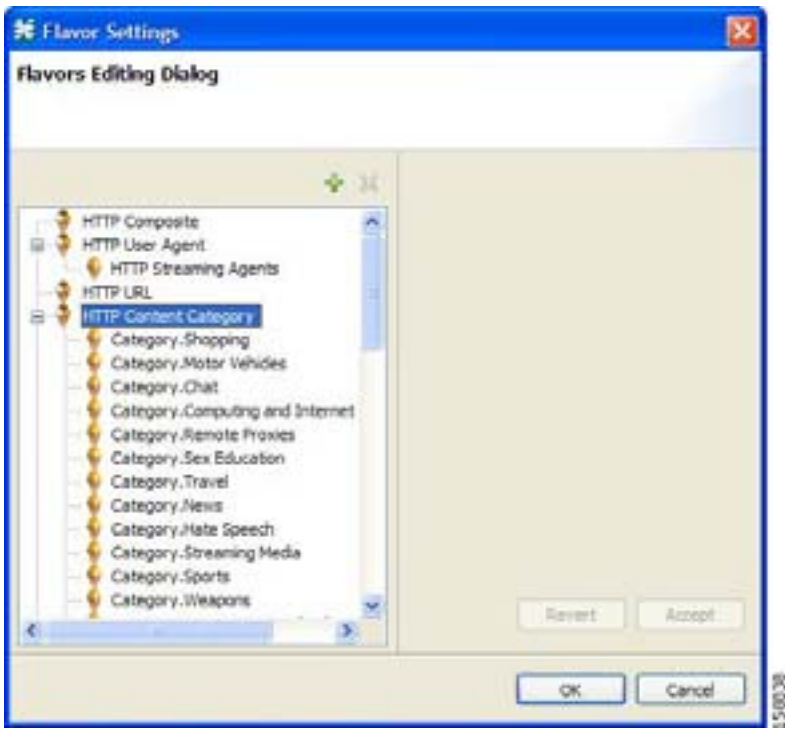
ステップ 6　**OK** をクリックします。

HTTP Content Filtering Settings ダイアログボックスが閉じます。

HTTP Content 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 タイプの）が作成されます。

図 7-53

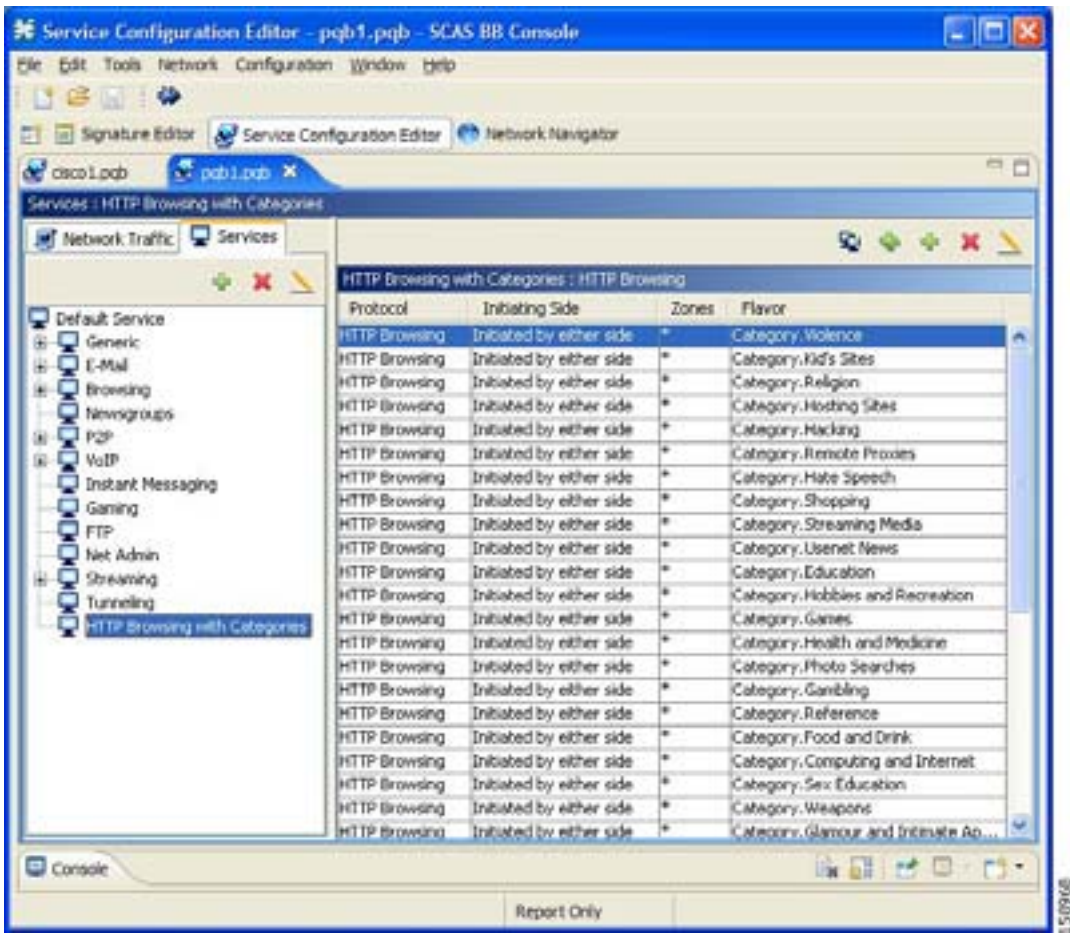


2 つ以上のコンテンツ カテゴリを含む HTTP Content Category フレーバを作成することもできます（「フレーバの追加」[p.7-53] を参照）。

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 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。

図 7-54



（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。

コンテンツ フィルタリングの設定

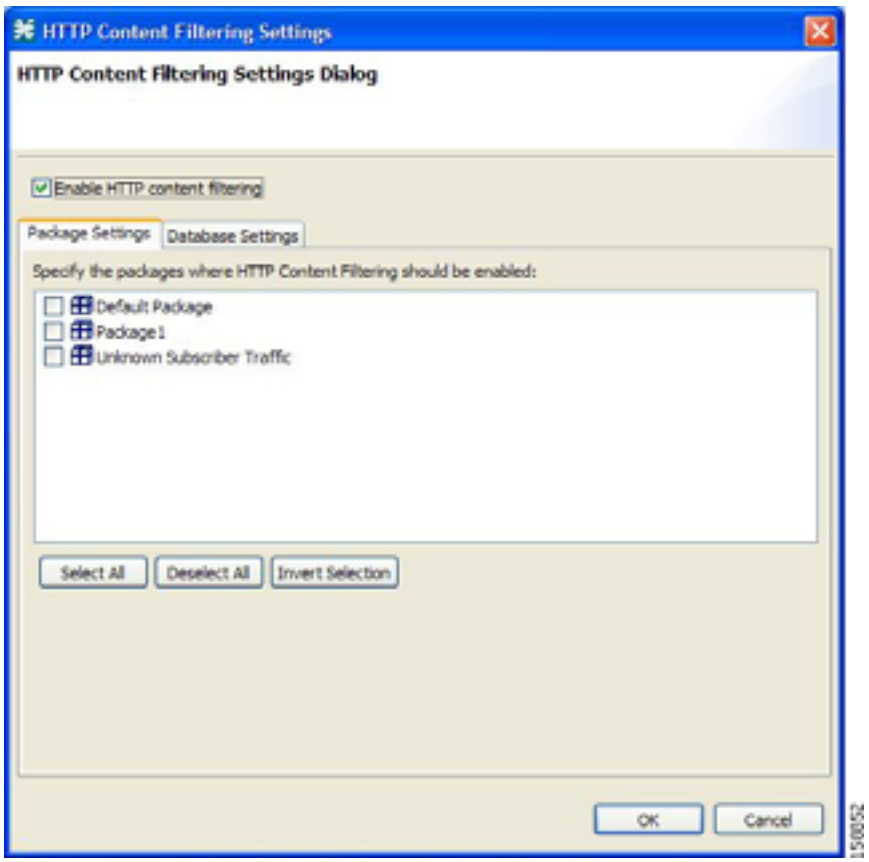
コンテンツ フィルタリングを有効にするパッケージを指定できます。コンテンツ フィルタリングを無効にしたパッケージでは、HTTP フローが通常通り分類されます。

ステップ 1　Console のメイン メニューから **Configuration >Content Filtering** の順番に選択します。

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パッケージのリストが表示されます。

図 7-55



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

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　Console のメイン メニューから **Configuration >Content Filtering** の順番に選択します。

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 タブが表示されます。

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

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　Console のメイン メニューから **Configuration >Content Filtering** の順番に選択します。

HTTP Content Filtering Settings ダイアログボックスが表示されます。

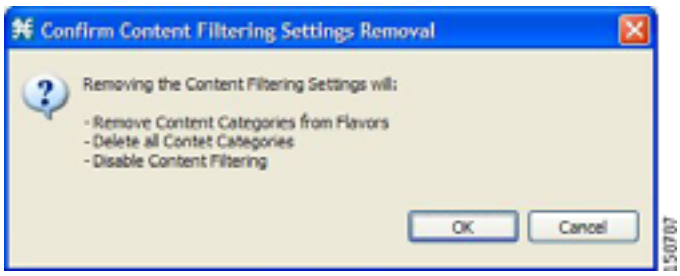
ステップ 2　**Database Settings** タブをクリックします。

Database Settings タブが表示されます。

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 7-56



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。

CHAPTER 8

Service Configuration Editor の使用法：トラフィックのアカウンティングとレポート

このモジュールでは、使用カウンタと Raw Data Record（RDR）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（SCABB）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。

使用カウンタの管理

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 ― 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、SMTP サービスと 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。「サービスの編集」（p.7-8）を参照してください。

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 ― 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。「高度なパッケージ オプションの設定」（p.9-7）を参照してください。

RDR 設定の管理

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」の章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.10-19] 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.10-44）で行います。

NetFlow Export の管理

- NetFlow レコードのイネーブルとディセーブルには CLI 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
  - Virtual Link Usage RDR
  - Malicious 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。

Usage RDR の管理

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 RDRs 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。

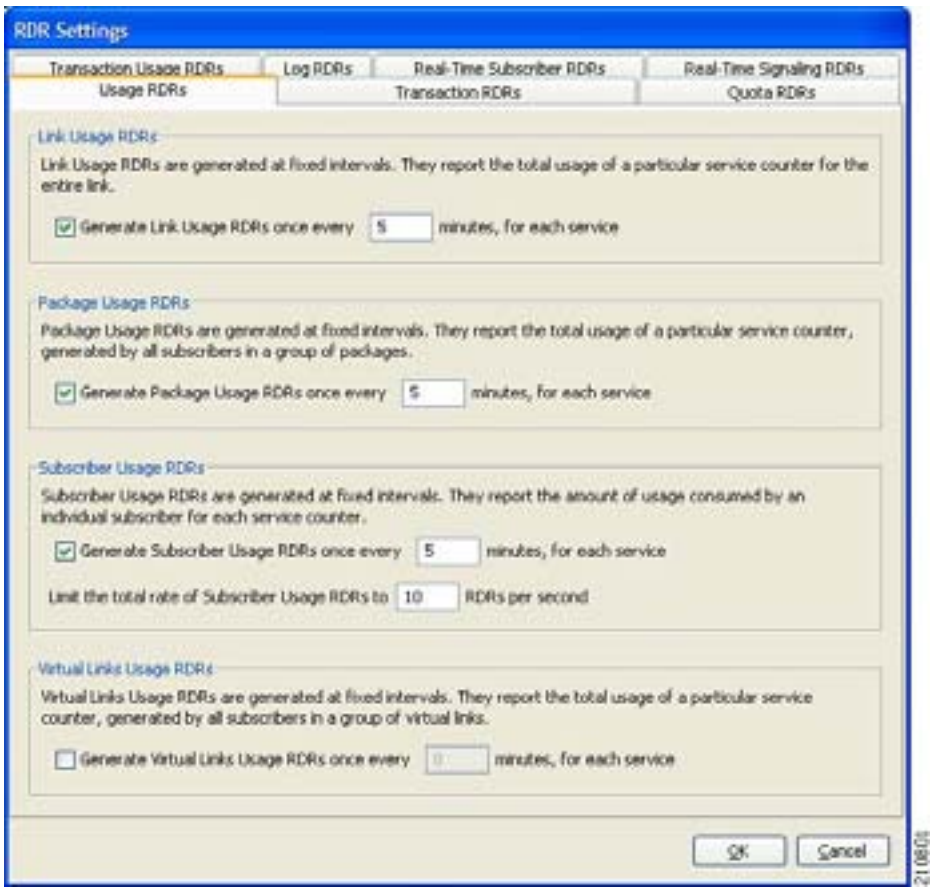
デフォルトでは、4 種類の Usage RDR がすべてイネーブルです。（Virtual Links Usage RDR は、サービス コンフィギュレーションの作成時に仮想リンク モードをイネーブルにした場合にのみ、デフォルトでイネーブルになります）。

（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.9-15] 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.9-53] を参照）です。

ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

RDR Settings ダイアログボックスが表示されます。

図 8-1



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

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。

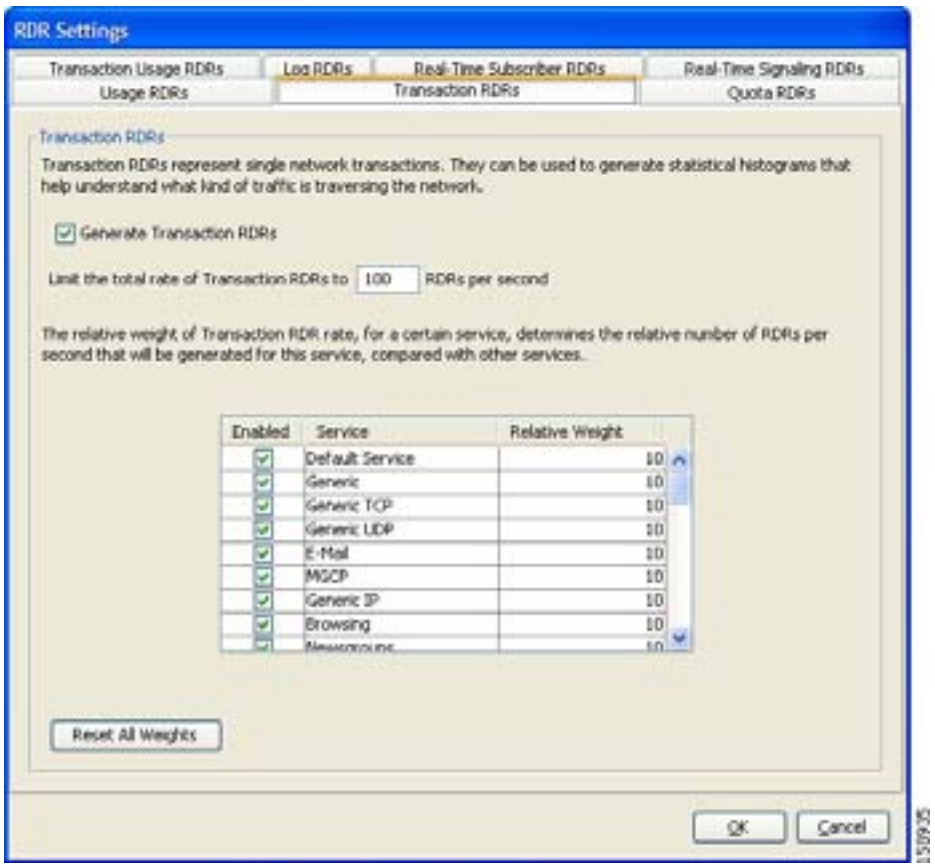
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-2



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

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 RDRs 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 RDRs 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。

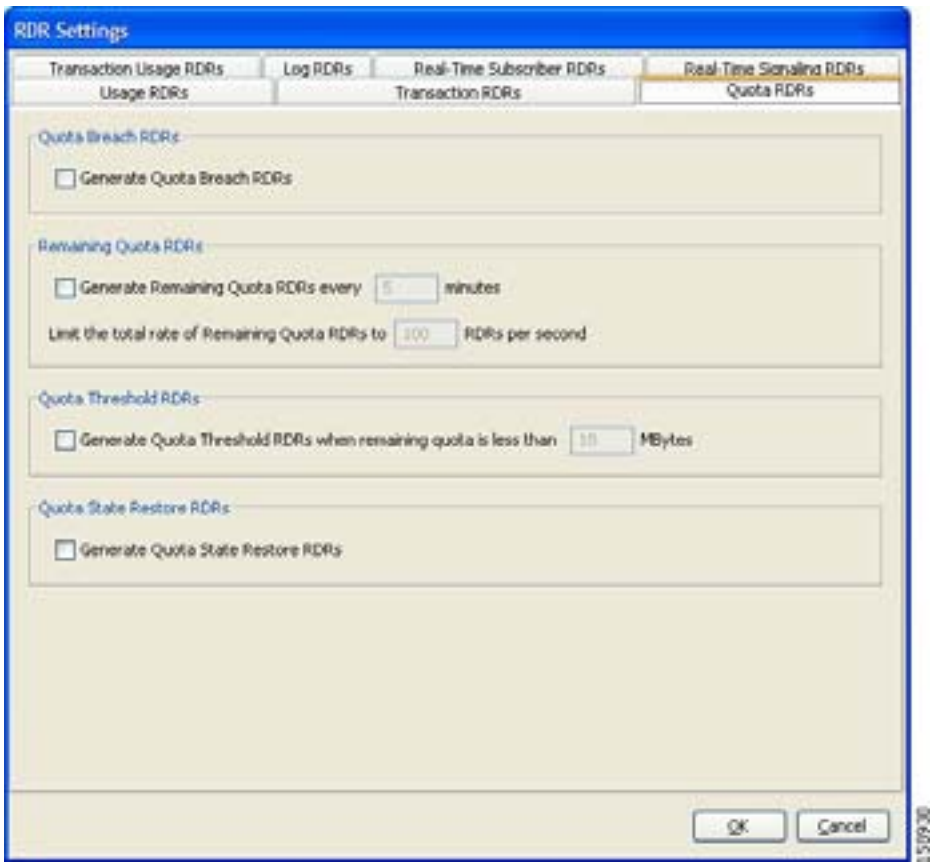
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-3



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

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。

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 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.10-44）でイネーブルにします。（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。）

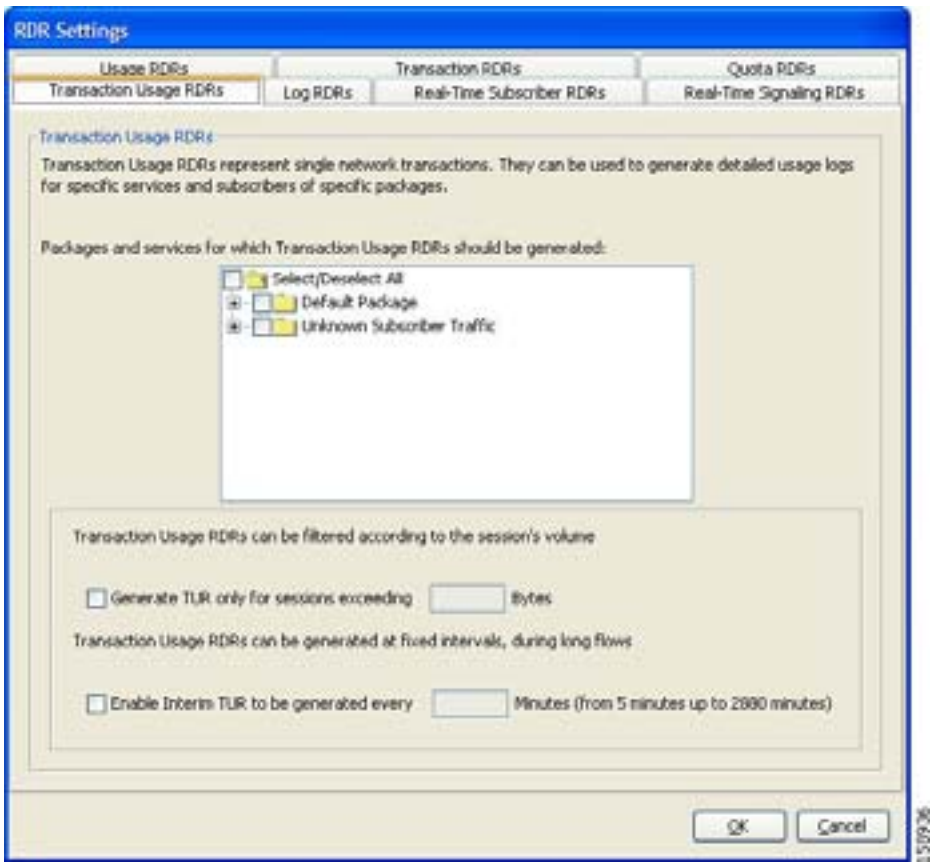
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-4



ステップ 3　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 4　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 5　セッション サイズで Transaction Usage RDR の生成を制限します。

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 6　通常、Transaction Usage RDR はフローの終了時にのみ生成されます。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。

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. 各フローのための Transaction Usage RDR の生成間隔を分単位で入力します。

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 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

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。

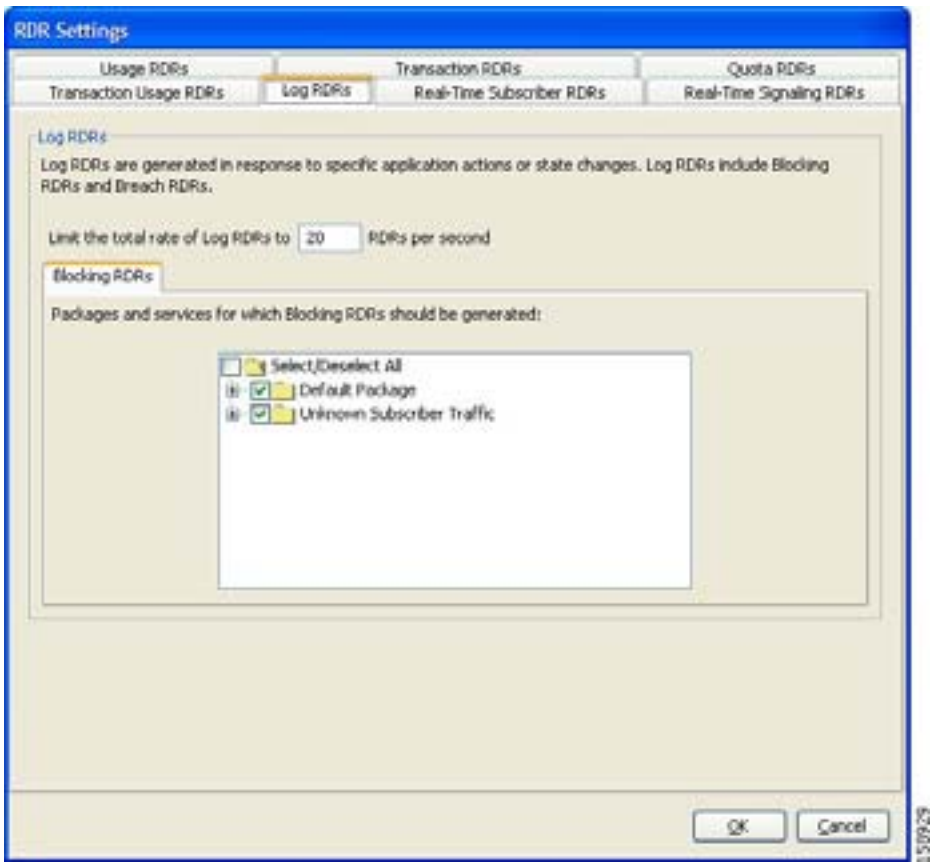
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-5



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 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

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.13-13）を参照してください。

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

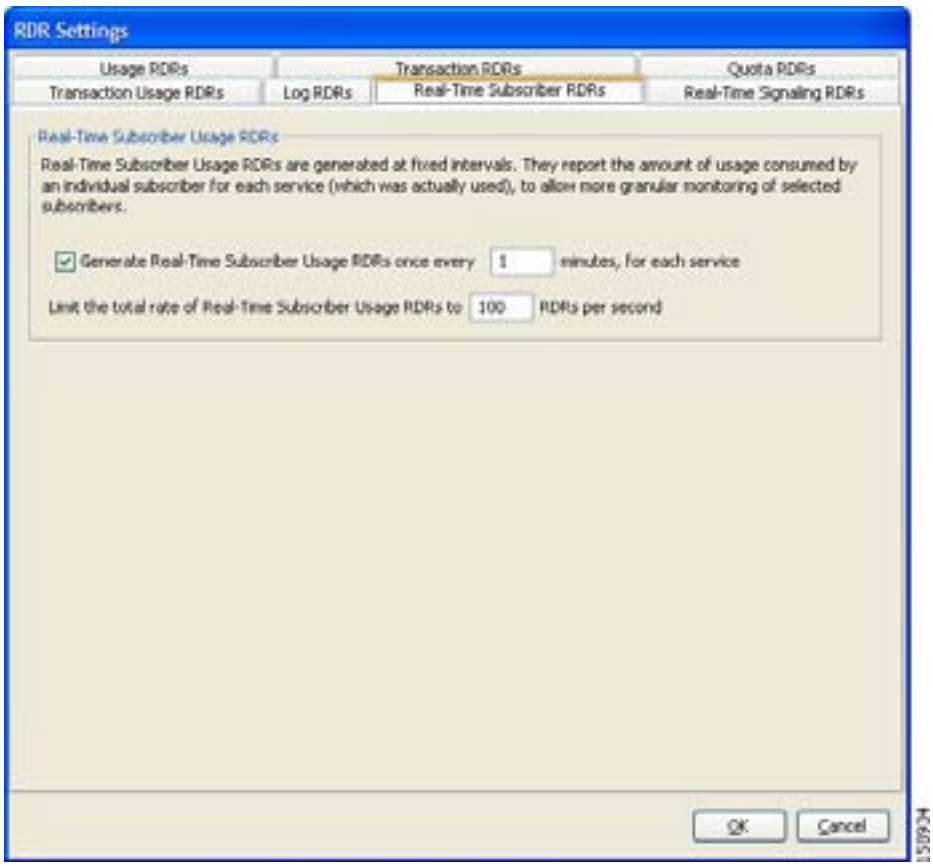
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-6



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

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のみ生成されます。

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 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.10-44）でイネーブルと設定を行います。

デフォルトでは、Real-Time Signaling RDR は生成されません。

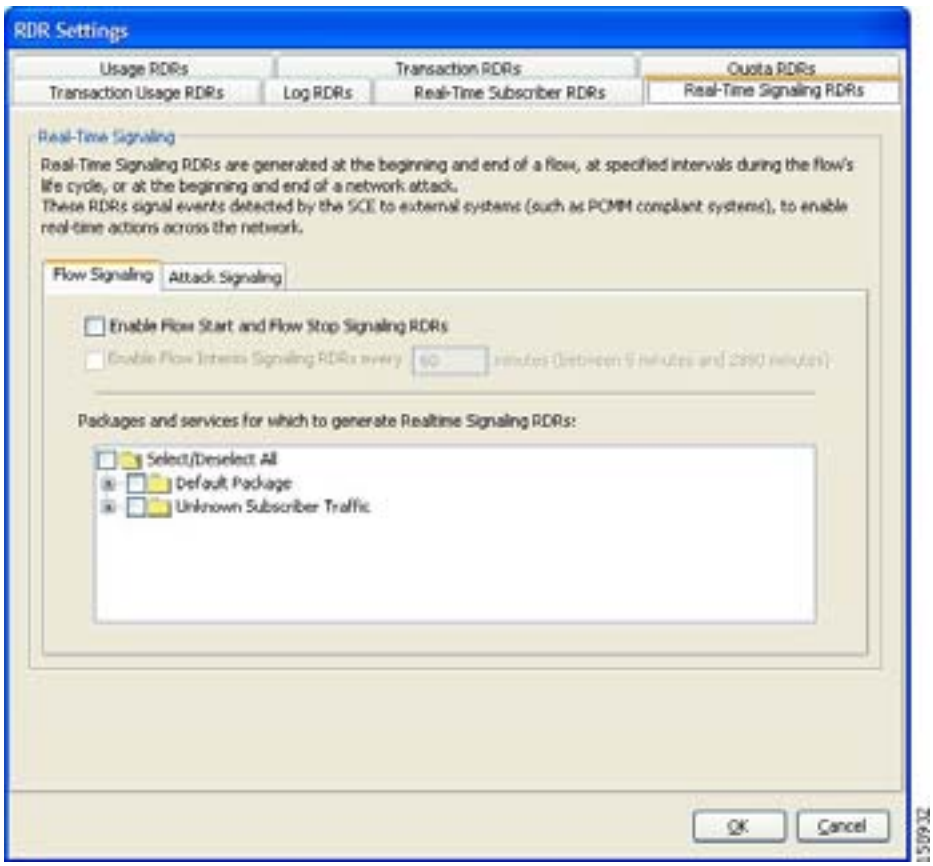
ステップ 1　Console メイン メニューから、**Configuration > RDR Settings** を選択します。

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 タブが表示されます。

図 8-7



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）　Flow Start and Flow Stop Signaling RDR の生成は、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イネーブル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 に進みます。

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

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 の使用法：トラフィックの制御

Service Control Engine（SCE）プラットフォームのトラフィックの制御機能と 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。

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.10-19] 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。

- 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.9-39] 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.9-7] 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.9-17] 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.9-15] 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.9-13] を参照）、編集（「規則の編集」[p.9-17] を参照）、および削除（「規則の削除」[p.9-19] 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.9-21] を参照）、編集（規則へのタイムベース規則の追加（p.9-21）を参照）、および削除（「タイムベース規則の削除」[p.9-25] を参照）

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す。これらの規則は、関連先の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を定義します。最初にサービスを定義してから（「サービスの管理」[p.7-2] 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。

ほか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 ―（任意）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 ― パッケージの一部であるサービスで利用可能な 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階層が 1 段階高いパッケージ。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）

- 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転送テーブル

これらのパラメータは、新しいパッケージを追加したときに定義されます（「パッケージの追加」[p.9-5] 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.9-9] を参照）。

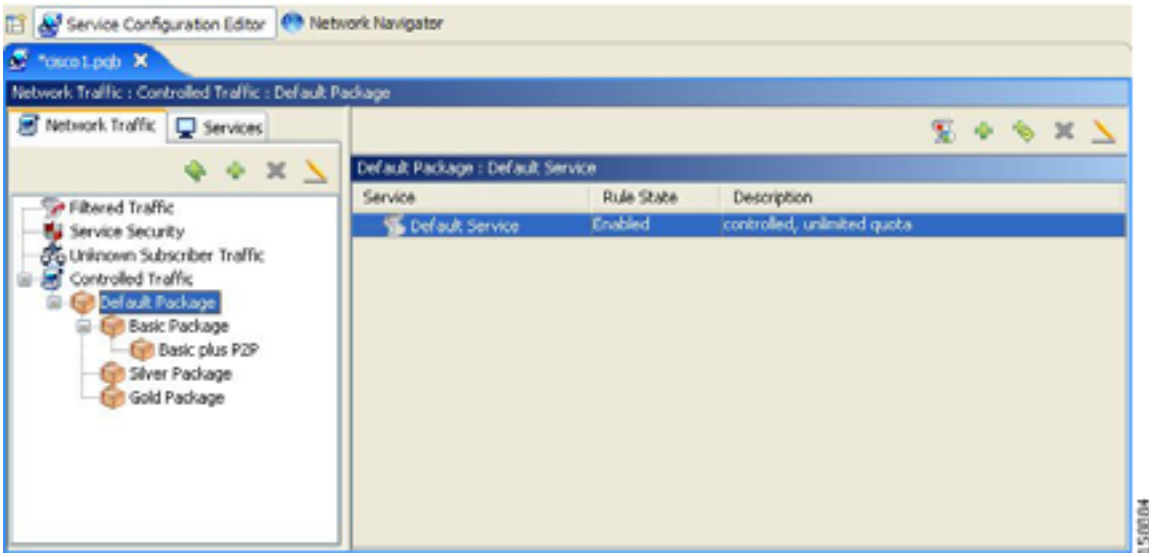
パッケージの表示

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、Network Traffic タブをクリックします。

Network Traffic タブが表示されます。

図 9-1



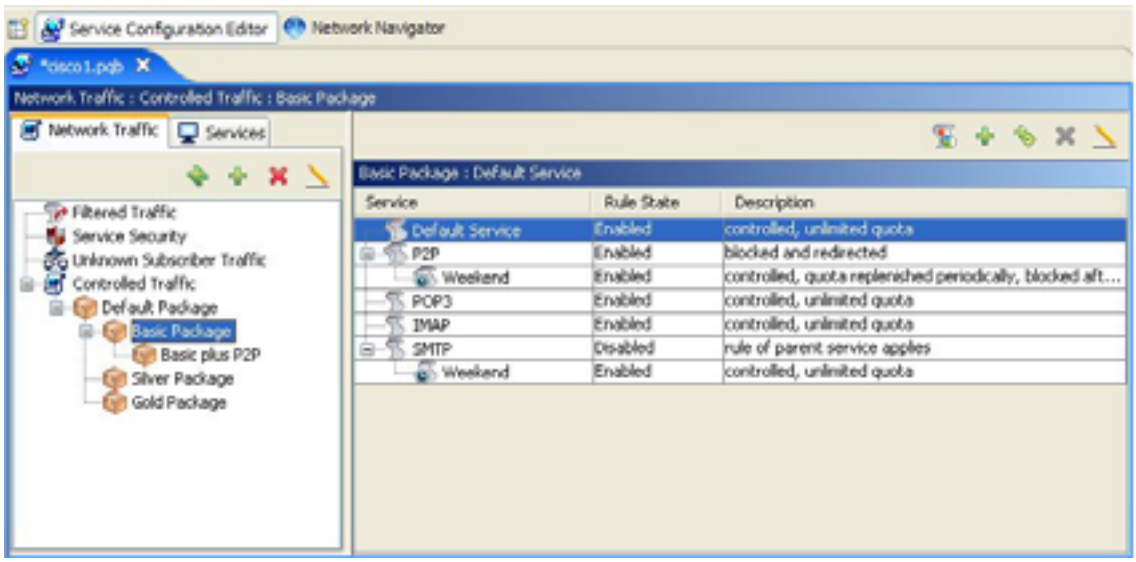
パッケージ ツリーに、パッケージのリストが表示されます。

- 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.9-9] 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。

右側のペイン（Rule）に、このパッケージの規則のリストが表示されます。

図 9-2



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。

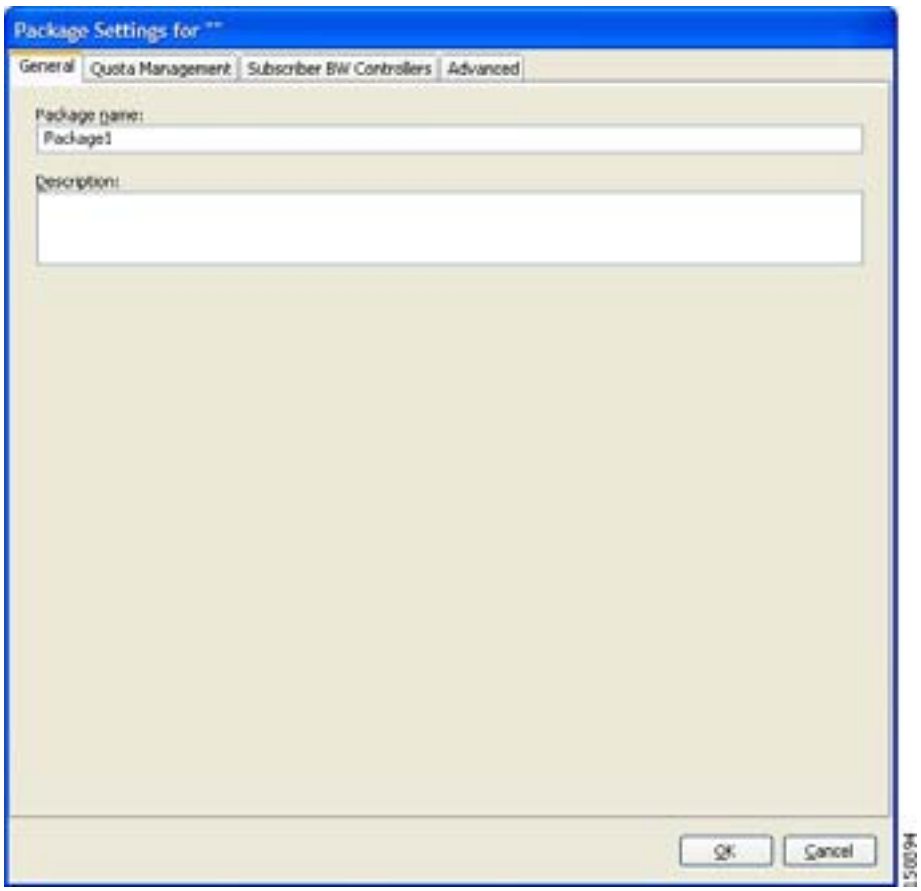
新しいパッケージを追加したら、パッケージの規則を定義できます（「パッケージへの規則の追加」[p.9-13] を参照）。

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。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　Network Traffic 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 9-3



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　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。右側のペイン（Rule）に、デフォルト サービス規則が表示されます。

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.9-12）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方法については、「パッケージのクォータ管理設定の編集」（p.9-54）（Quota Management タブ [Packages] を使用）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方法については、「パッケージ サブスクライバ BWC の編集」（p.9-39）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。

手順の概要

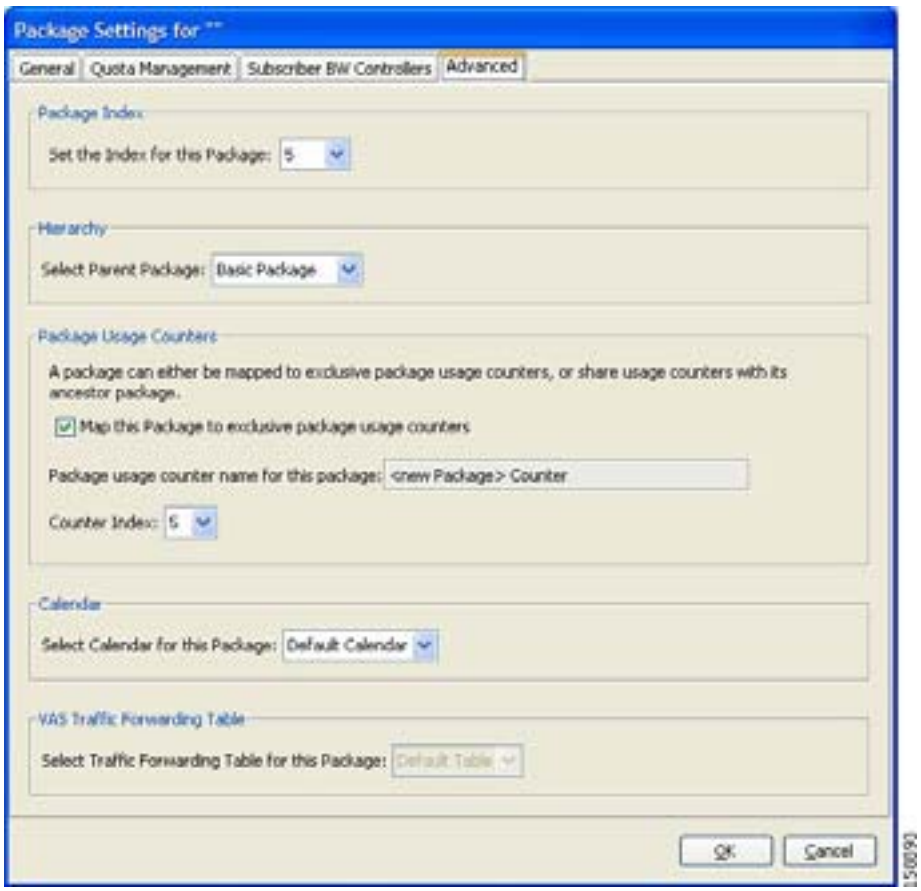
1. Package Settings ダイアログボックスで、**Advanced** タブをクリックします。
2. このパッケージのパッケージ インデックスを変更するには、Set the Index for this Package ドロップダウンリストでパッケージ インデックスを選択します。
3. このパッケージに別の親パッケージを定義するには、Select Parent Package ドロップダウン リストで目的の親を選択します。
4. デフォルトでは、新しいパッケージでは専用の使用カウンタが使用されます。親パッケージの使用カウンタを共有するには、**Map this Service to an exclusive package usage counters** チェックボックスをオフにします。
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。
6. このパッケージに（タイムベース規則にその時間枠を使用するために）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。
7. このパッケージに VAS トラフィック転送テーブルを定義するには、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転送テーブルを選択します。
8. **OK** をクリックします。

手順の詳細

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 タブが表示されます。

図 9-4



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。

- 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 an 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。

- 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　このパッケージに（タイムベース規則にその時間枠を使用するために）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 VAS トラフィック転送テーブルを定義するには、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転送テーブルを選択します。

- VAS トラフィック転送がディセーブル（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 フォワーディング設定の管理」（p.10-45）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。右側のペイン（Rule）に、デフォルト サービス規則が表示されます。

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.9-12）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方法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　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　Network Traffic 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には、選択したパッケージの名前のあとに「(1)」（または、パッケージを複数回複製した場合は「(2)」など）が付加されます。

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.9-9] 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　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　Network Traffic 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　クォータ管理設定を変更する方法については、「パッケージのクォータ管理設定の編集」（p.9-54）（Quota Management タブ [Packages] を使用）を参照してください。

ステップ 6　帯域幅制御設定を変更する方法については、「パッケージ サブスクライバ BWC の編集」（p.9-39）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 タブが表示されます。

1. 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。
   - 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。
2. 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。
3. 親パッケージの使用カウンタを共有するには、Map this Service to an 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。
4. 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 counter 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。
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。
   - 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。
6. 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。
7. このパッケージの VAS トラフィック転送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転送テーブルを選択します。
   - VAS トラフィック転送がディセーブル（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 フォワーディング設定の管理」（p.10-45）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

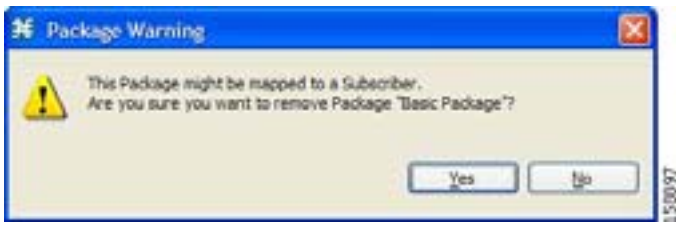
ユーザ定義パッケージは削除できます。デフォルト パッケージは削除できません。

ステップ 1　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　Network Traffic 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 9-5



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、パッケージの規則が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
- サービスのクォータの設定
- サービスの最大帯域幅の定義
- 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 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.9-20）も参照してください。

パッケージの規則の表示

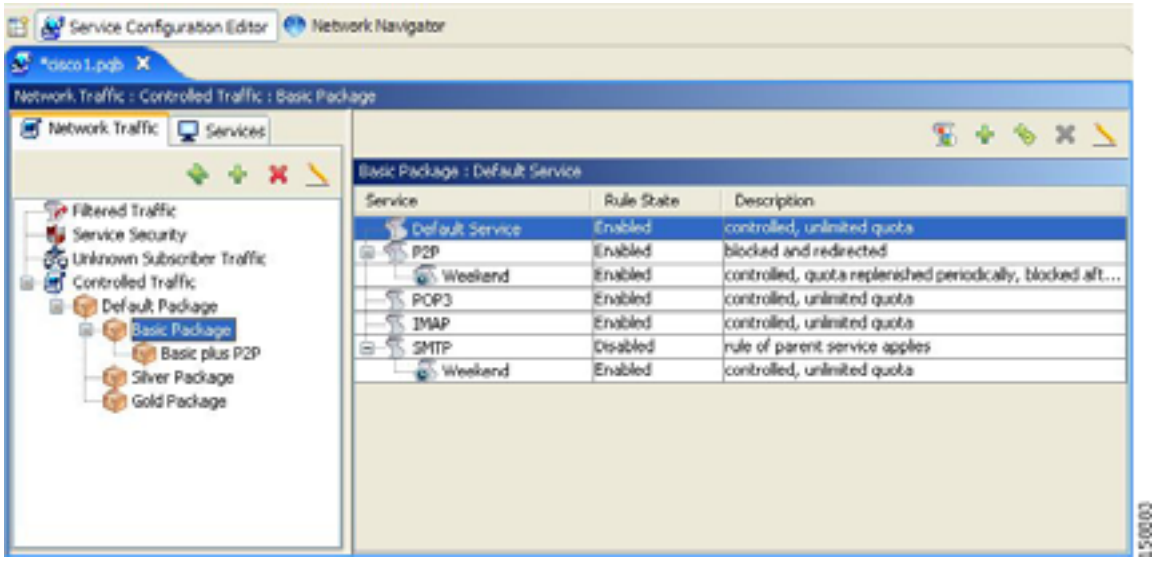
パッケージの規則のリストを表示できます。

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　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。

右側のペイン（Rule）に、このパッケージに定義された規則のリストが表示されます。

図 9-6



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.9-17] 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.9-23] を参照）。

パッケージへの規則の追加

- パッケージへの規則の追加（p.9-13）
- 規則のためのフローごとのアクションの定義（p.9-15）

パッケージへの規則の追加

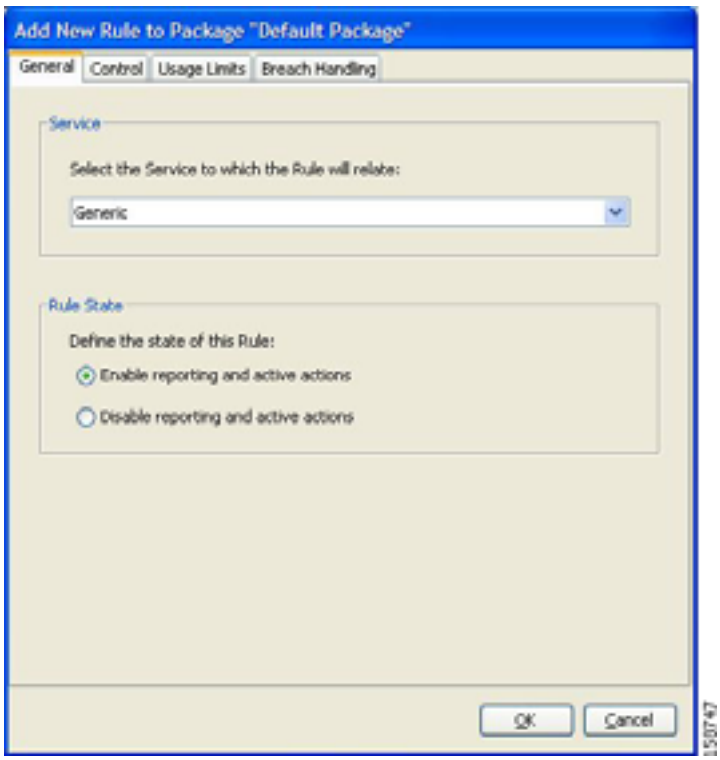
タイムベース規則の追加方法については、「規則へのタイムベース規則の追加」（p.9-21）を参照してください。

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　右側のペイン（Rule）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 9-7



ステップ 3　Add New Rule to Package ダイアログボックスの Service 領域の Select the Service to which the Rule will relate 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** オプション ボタンのいずれかを選択します。

- **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.9-17] を参照）。

ステップ 5　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.9-15）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、右側のペイン（Rule）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.9-53] 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.9-55）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.56）を参照してください。

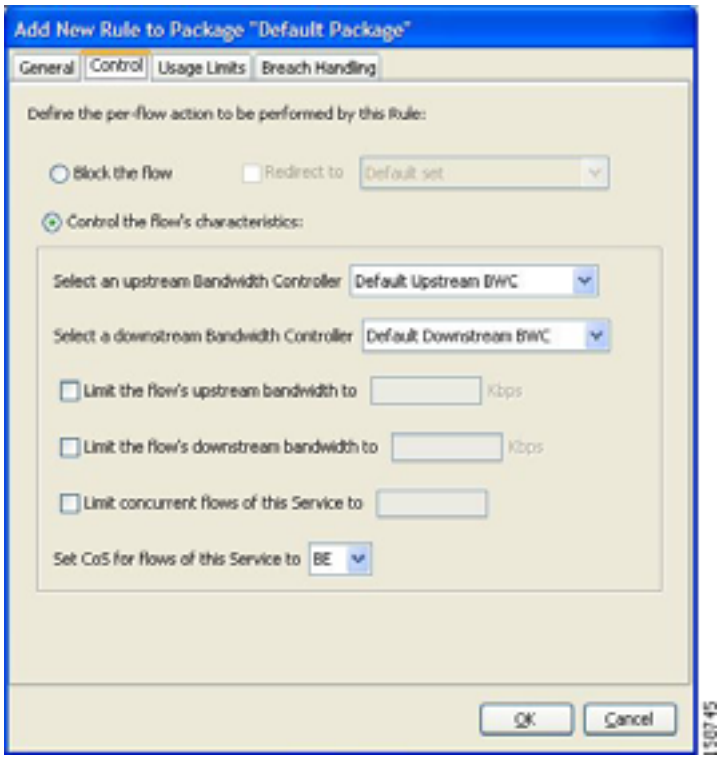
規則のためのフローごとのアクションの定義

Add New Rule to Package ダイアログボックスの Control 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 タブが表示されます。

図 9-8



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 5 以降を実行します。

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 ボタンを選択します。

Redirect to チェックボックスが使用可能になります。

（注） リダイレクションをサポートしているのは、HTTP、HTTP Streaming、および RTSP の 3 つのプロトコル タイプだけです。

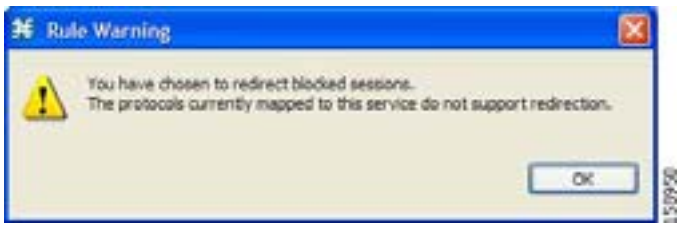
ステップ 3　ブロックされたフローをリダイレクトするには、**Redirect to** チェックボックスをオンにします。

（注） リダイレクションは、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。

Redirection URL Set ドロップダウン リストが使用可能になります。

- この規則のサービスまたはサービス　グループにリダイレクトできないプロトコルが含まれている場合、Rule Warning メッセージが表示されます。

図 9-9



- **OK** をクリックします。

Redirection URL Set ドロップダウン リストから、リダイレクション ターゲットとして設定された URL を選択します。（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 パラメータの設定」[p.10-36] を参照してください）。

ステップ 4　ステップ 12 に進んでください。

ステップ 5　**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 6　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（「パッケージ サブスクライバ BWC の編集」[p.9-39] を参照）。

（注） **タイムベース規則の特記事項：**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（「グローバル コントローラの最大帯域幅の設定」[p.9-35] を参照）。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。

図 9-10

ステップ 7　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 8　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 9　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 10　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る）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　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、右側のペイン（Rule）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。

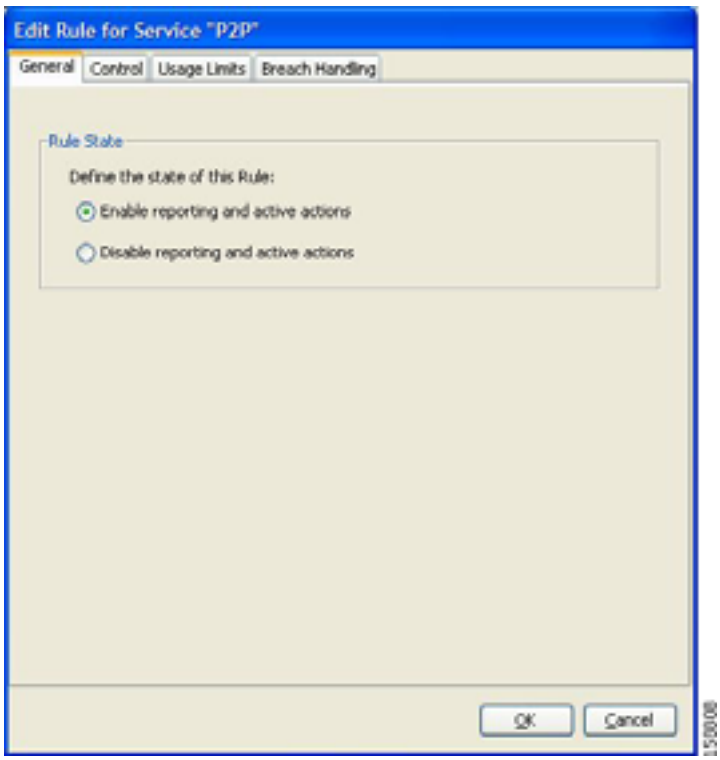
ステップ 1　Network Traffic タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右のペイン（Rule）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 9-11



ステップ 4　Rule State 領域で、**Define the state of this Rule** オプション ボタンのいずれかを選択します。

- **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するには、次の手順を実行します。

1. **Control** タブをクリックします。
   Control タブが表示されます。
2. 「規則のためのフローごとのアクションの定義」（p.9-15）の手順に従います。

ステップ 6　使用制限を変更するには、次の手順を実行します。

1. **Usage Limits** タブをクリックします。
   Usage Limits タブが表示されます。
2. 「規則のためのクォータ バケットの選択」（p.9-55）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するには、次の手順を実行します。

1. **Breach Handling** タブをクリックします。
   Breach Handling タブが表示されます。
2. 「規則のための違反処理パラメータの編集」（p.9-56）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.9-17] 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　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　右のペイン（Rule）で、規則を選択します。

ステップ 3　Rule 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 9-12

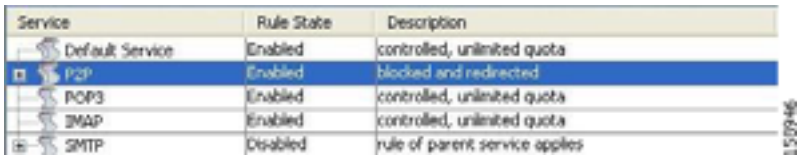
ステップ 4　**Yes** をクリックします。

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、次の図のデフォルト サービス規則や P2P 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 9-13



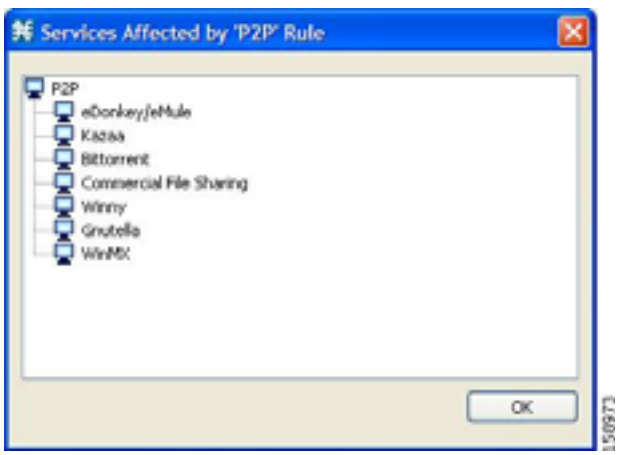
規則が影響するすべての（子）サービスを表示できます。

（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 タブの右のペイン（Rule）で、規則を選択して、（**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 9-14



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.9-25] 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（p.9-21）
- タイムベース規則の編集（p.9-23）
- タイムベース規則の削除（p.9-25）
- カレンダーの管理（p.9-25）

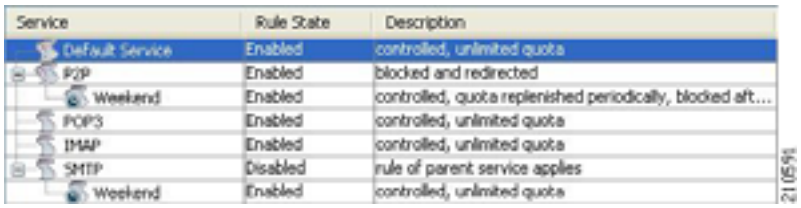
規則へのタイムベース規則の追加

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。

（注）　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。

タイムベース規則が子サービスに影響を及ぼすサービスは、次の画面図に示す 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 9-15



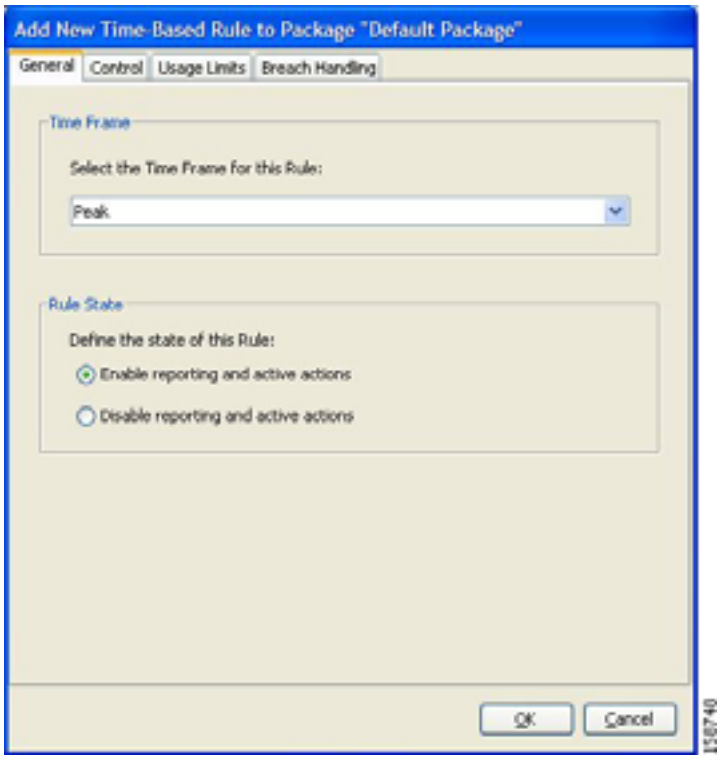
ステップ 1　Network Traffic タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右のペイン（Rule）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 9-16



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** オプション ボタンのいずれかを選択します。

- **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するには、次の手順を実行します。

1. **Control** タブをクリックします。
   Control タブが表示されます。
2. 「規則のためのフローごとのアクションの定義」（p.9-15）の手順に従います。

ステップ 7　使用制限を変更するには、次の手順を実行します。

1. Usage Limits タブをクリックします。
   Usage Limits タブが表示されます。
2. 「規則のためのクォータ バケットの選択」（p.9-55）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するには、次の手順を実行します。

1. Breach Handling タブをクリックします。
   Breach Handling タブが表示されます。
2. 「規則のための違反処理パラメータの編集」（p.9-56）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 Rule 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。

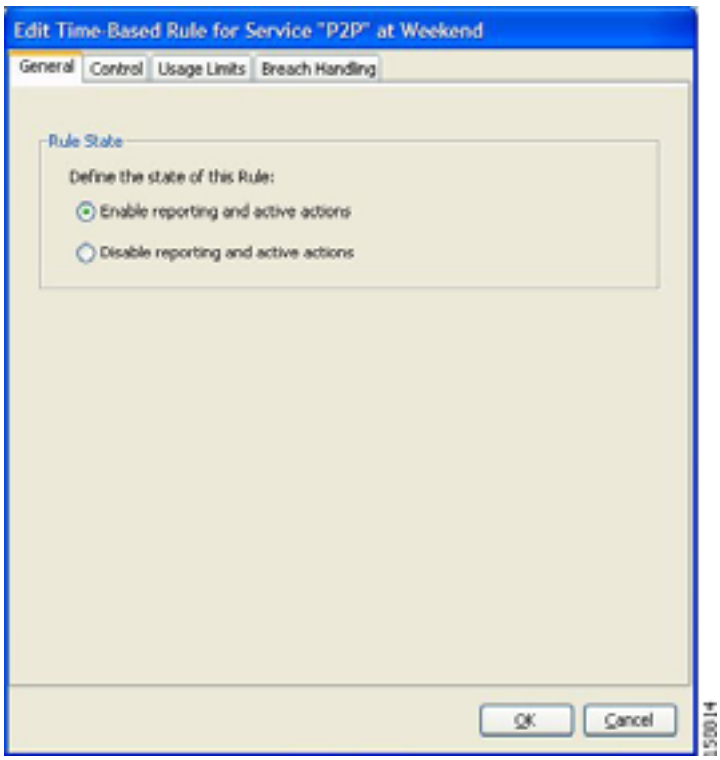
ステップ 1　Network Traffic タブで、パッケージ ツリーからパッケージを選択します。

ステップ 2　右のペイン（Rule）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 9-17



ステップ 4　Rule State 領域で、**Define the state of this Rule** オプション ボタンのいずれかを選択します。

- **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するには、次の手順を実行します。

1. **Control** タブをクリックします。
   Control タブが表示されます。
2. 「規則のためのフローごとのアクションの定義」（p.9-15）の手順に従います。

ステップ 6　使用制限を変更するには、次の手順を実行します。

1. Usage Limits タブをクリックします。
   Usage Limits タブが表示されます。
2. 「規則のためのクォータ バケットの選択」（p.9-55）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するには、次の手順を実行します。

1. Breach Handling タブをクリックします。
   Breach Handling タブが表示されます。
2. 「規則のための違反処理パラメータの編集」（p.9-56）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.9-23]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　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　右のペイン（Rule）で、タイムベース規則を選択します。

ステップ 3　Rule 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 9-18

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。

カレンダーの管理には、次の項目があります。

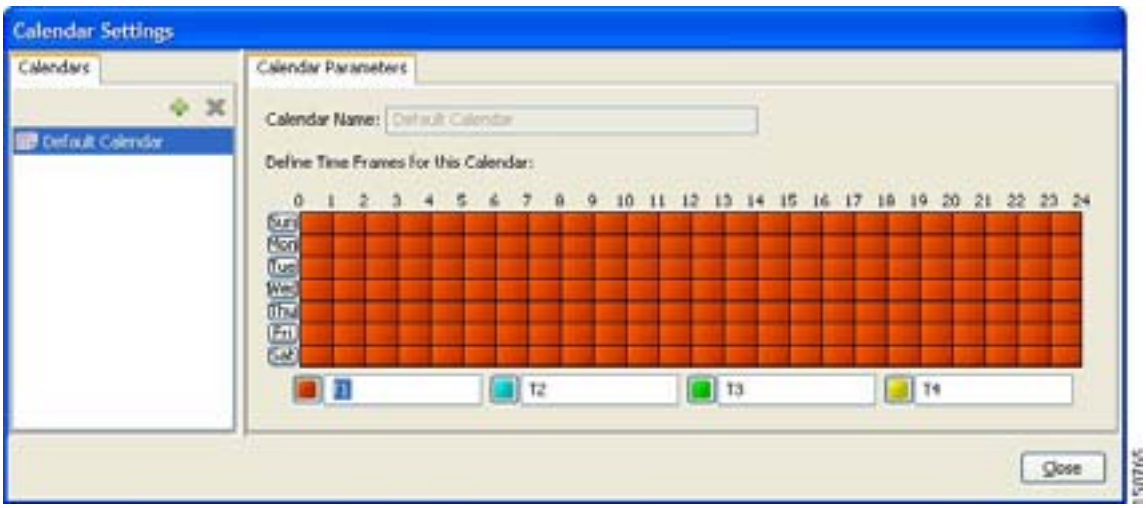
カレンダーの表示

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　Console メイン メニューから、**Configuration > Weekly Calendars** を選択します。

Calendar Settings ダイアログボックスが表示されます。

図 9-19



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　Console メイン メニューから、**Configuration > Weekly Calendars** を選択します。

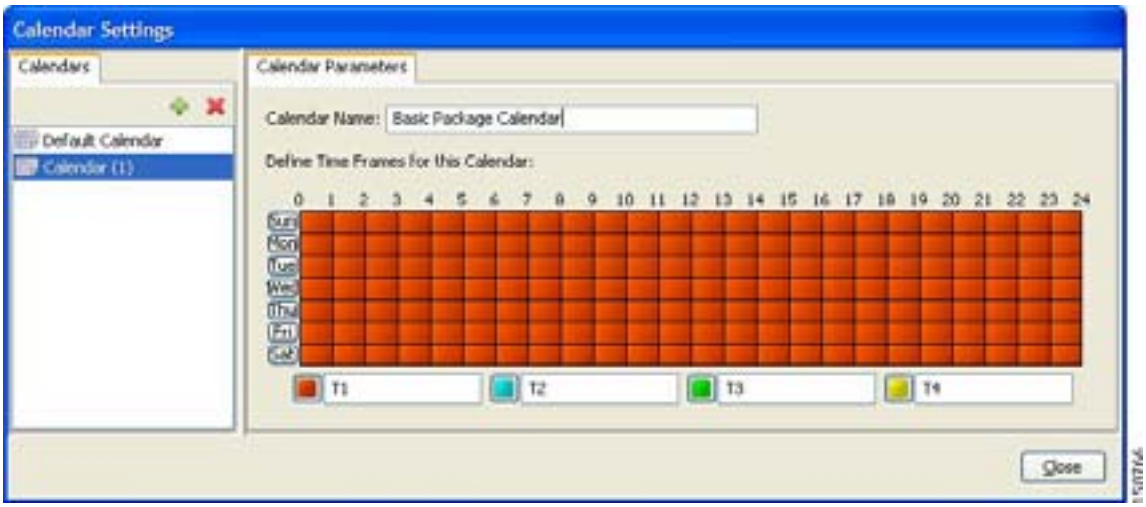
Calendar Settings ダイアログボックスが表示されます。

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 9-20



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終了し、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。

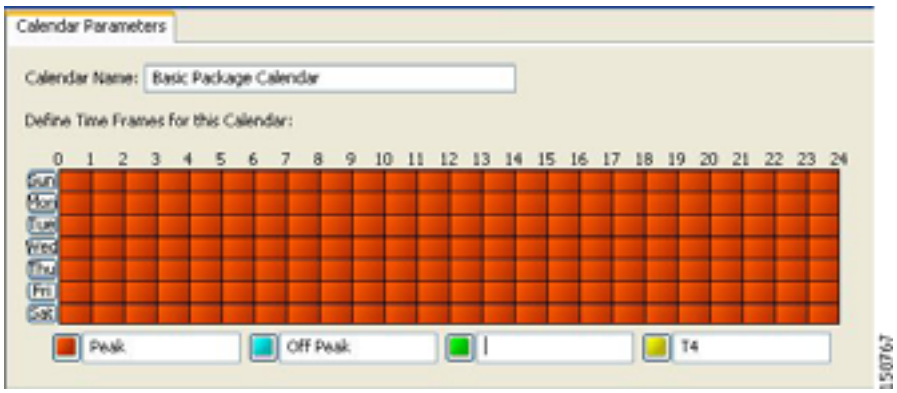
ステップ 1　Console メイン メニューから、**Configuration > Weekly Calendars** を選択します。

Calendar Settings ダイアログボックスが表示されます。

Calendar Parameters タブのグリッドの下、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 9-21



ステップ 3　他の 3 つの時間枠についても、ステップ 2 を実行します。

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終了し、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）　パッケージで使用し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）。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のために、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.9-7）を参照してください。

ステップ 1　Console メイン メニューから、**Configuration > Weekly Calendars** を選択します。

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。

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　Console メイン メニューから、**Configuration > Weekly Calendars** を選択します。

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。

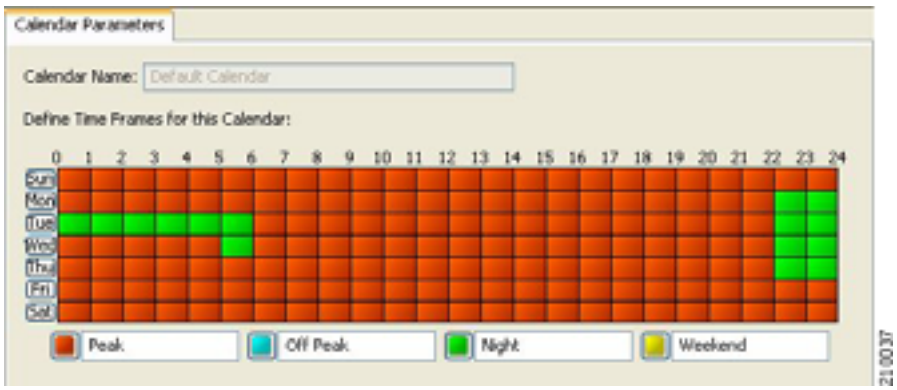
グリッドの下の、カラーのボタンの隣に、各時間枠の名前が表示されます。

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 9-22



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。

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。

1 週間が 4 つの時間枠にマッピングできました。以下に、時間の分割例を示します。

図 9-23

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 コントローラを含めて）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）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。

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 のほか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比率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 ストリーム上の SCE プラットフォームの次にある別のデバイスで BW 容量が制限されている場合に、この制限を、その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で（SCE プラットフォームで）適用できます。

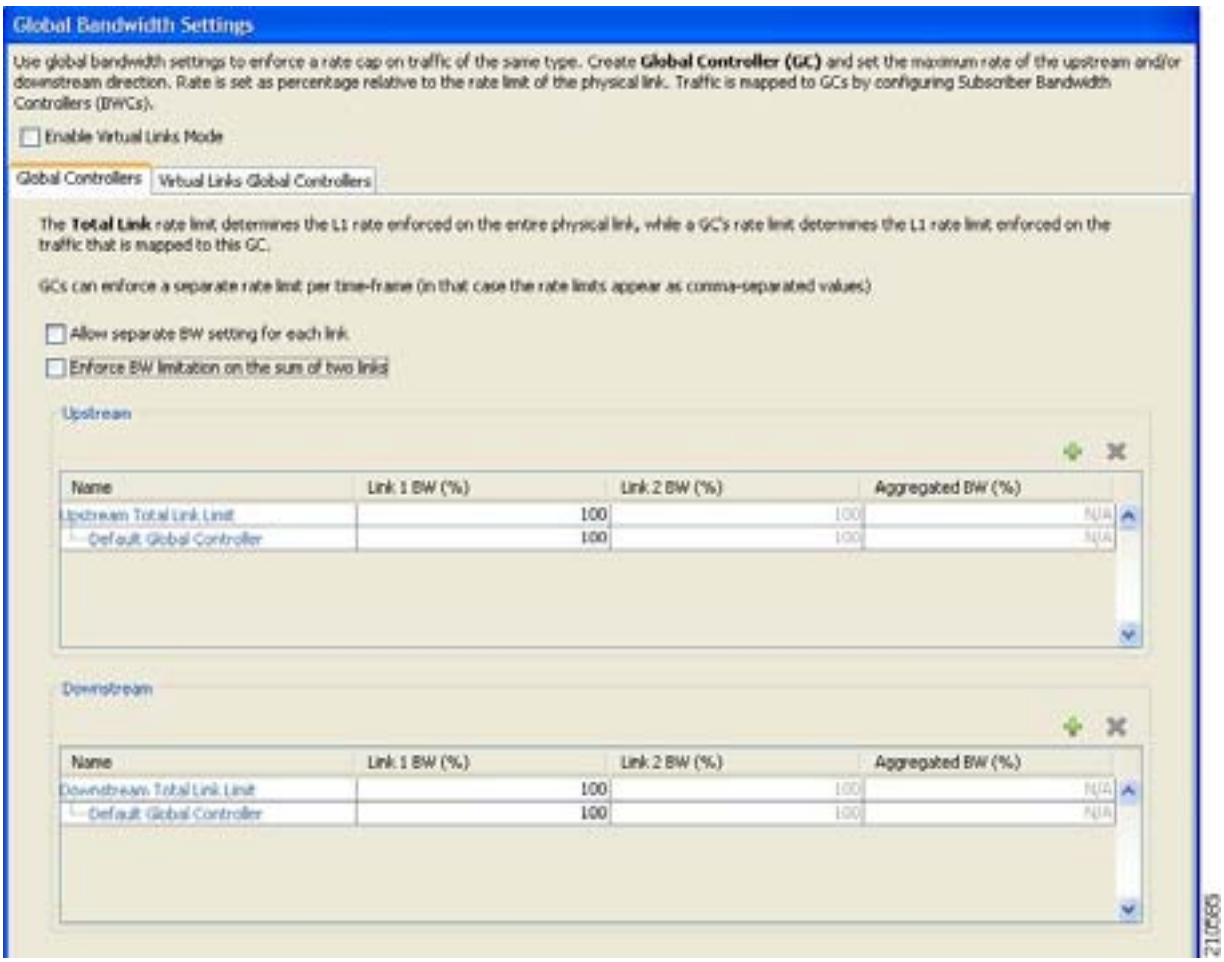
グローバル コントローラ設定の表示

（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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

図 9-24



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 システムでのみ使用します（「デュアルリンク システムのグローバル コントローラの定義」[p.9-37] を参照）。

ダイアログボックスの主要部は、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した 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した Downstream 領域からなります。各リストには 4 つのカラムがあり、第 3 カラムと第 4 カラムはデュアルリンク システムに関するものです。

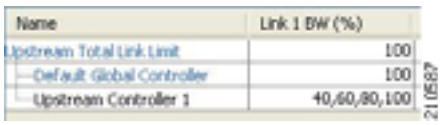
- **Name** ― グローバル コントローラに割り当てられた一意の名前。Controller 1、Controller 2 などの名前が自動的に割り当てられます。
- **Link 1 BW (%)** ― このグローバル コントローラに許可される合計リンク制限の最大割合。

  各グローバル コントローラについて、デフォルト カレンダーによって定義される 4 つの時間枠のそれぞれに対して、最大帯域幅のための異なる値を設定できます（「カレンダーの管理」[p.9-25] 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。

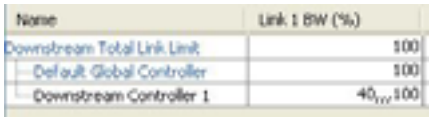
  ― 時間枠ごとに最大帯域幅が異なる場合、それぞれの時間枠の最大帯域幅が、カンマで区切られて表示されます。

図 9-25



— 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（そのため、**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に等しいことになります）。

図 9-26

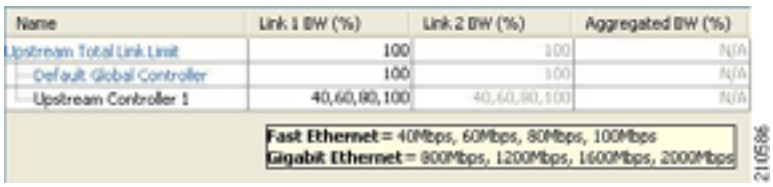


— 末尾のカンマは省略されます（そのため、**40,,,100** の場合、最初の時間枠は最大帯域幅が合計リンク制限の 40% で、続く 3 つの時間枠は最大帯域幅が合計リンク制限に等しいことになります）。

ステップ 2　実際の最大帯域幅の値を表示するには、カーソルを Link 1 BW (%) のセル上に合わせます。

ツールチップに、このグローバル コントローラに許可された実際の最大帯域幅が Mbps 単位で表示されます。この数値は、SCE タイプ（ギガビット イーサネットまたはファスト イーサネット）、コントローラの最大帯域幅割合、およびリンク帯域幅の合計割合に基づいて、自動的に計算されます。

図 9-27



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。

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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

ステップ 2　Upstream Total Link Limit または Downstream Total Link Limit の Link 1 BW (%) セルをクリックし、プラットフォームを通過させる SCE プラットフォーム容量の最大割合を入力します。

Link 1 BW (%) セルのすべてのセルのツールチップに表示される値は、新しい合計リンク制限を反映して変化します。

ステップ 3　**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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

ステップ 2　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。

新しいグローバル コントローラがインターフェイス グローバル コントローラ リストに追加され、最大帯域幅が合計リンク制限の 100% になります。

ステップ 3　新しいグローバル コントローラの Name セルに、わかりやすい名前を入力します。

（注）　グローバル　コントローラのデフォルト名を使用することもできますが、わかりやすい名前の入力を推奨します。

ステップ 4　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.9-35）のセクションの手順を実行します。

ステップ 5　**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（合計リンク制限の割合として）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。

デュアルリンク システムでは、各リンクと、2 つのリンクの集約 BW に、異なる値を設定できます。

ステップ 1　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

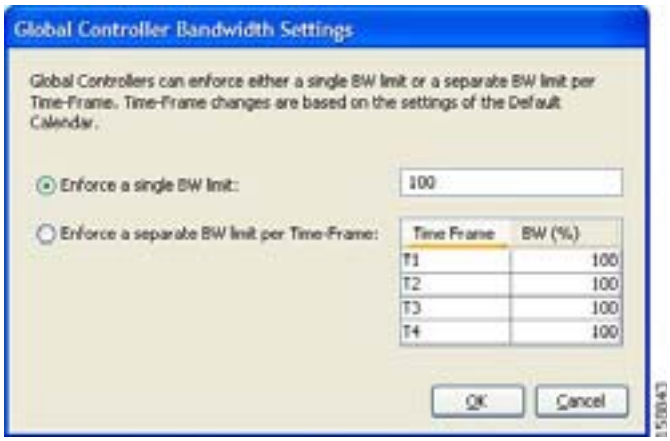
ステップ 2　グローバル コントローラ リストの BW (%) セルをクリックします。

セルに Browse ボタンが表示されます。

ステップ 3　**Browse** ボタンをクリックします。

Global Controller Bandwidth Settings ダイアログボックスが表示されます。

図 9-28



ステップ 4　このグローバル コントローラを通過する合計リンク制限の最大割合に単一の値を設定するには、次の手順を実行します。

- **Enforce a single BW limit** を選択し、帯域幅の最大割合の値を入力します。

ステップ 5　このグローバル　コントローラを通過する合計リンク制限の最大割合を時間枠によって変化させるには、次の手順を実行します。

- **Enforce a separate BW limit per Time Frame** を選択し、各 BW (%) セルに適切な値を入力します。

（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。

BW (%) セルの値は、新しい帯域幅制限を反映して変化します。

ステップ 7　各グローバル コントローラについて、ステップ 2 ～ 6 を実行します。

ステップ 8　**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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

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.9-39] を参照）、グローバル コントローラ削除不能の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。

デュアルリンク システムのグローバル コントローラの定義

デュアルリンク システムの場合は、リンクごとにグローバル コントローラの最大帯域幅を個別に定義できます。

または、2 つのリンクの合計に帯域幅制限を適用することもできます。

(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 2 つのリンクの合計に対して適用されます。

- リンクごとに個別にグローバル コントローラの帯域幅制限を設定（p.9-37）
- 2 つのリンクの合計としてグローバル コントローラの帯域幅制限を設定（p.9-37）

リンクごとに個別にグローバル コントローラの帯域幅制限を設定

ステップ 1　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

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 コントローラの追加」（p.9-34）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　**Allow separate BW setting for each link** チェックボックスをオンにします。

Link 2 BW (%) カラムのセルが使用可能になります。

各セルの値は、Link 1 BW (%) カラムの平行セルの値と同じです。

ステップ 4　Link 1 のグローバル コントローラの帯域幅割合（Link 1 BW (%)）を定義します。

帯域幅割合を変更しても、変更後の値は Link 2 タブにコピーされません。

ステップ 5　Link 2 BW (%) カラムで、Link 2 のグローバル コントローラの帯域幅割合を定義します。

ステップ 6　**OK** をクリックします。

変更が保存されます。

Global Bandwidth Settings ダイアログボックスが閉じます。

2 つのリンクの合計としてグローバル コントローラの帯域幅制限を設定

ステップ 1　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

ステップ 2　**Enforce BW limitation on the sum of two links** チェックボックスをオンにします。

Aggregated BW (%) カラムのセルが使用可能になり、値 100 が入ります。

ステップ 3　**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。

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、もう 1 つはダウンストリーム トラフィック）を使用すると、Committed Information Rate（CIR）、Peak Information Rate（PIR）、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 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 はサブスクライバごとのサービス レベルで動作します。これらは、BWC に設定された CIR、PIR、グローバル コントローラ、Assurance Level（AL）に基づいて、各サブスクライバのサービスのための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.9-15）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けれども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。

仮想リンク モードのイネーブルまたはディセーブルにすると、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るので注意が必要です。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 のほかのパラメータは変更されません）。

帯域幅制御については、「サブスクライバ帯域幅制御」（p.3-16）のセクションで詳しく説明しています。

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。

たとえば、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（「グローバル帯域幅制御」[p.3-15] を参照）。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。
- サブスクライバ BWC（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 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

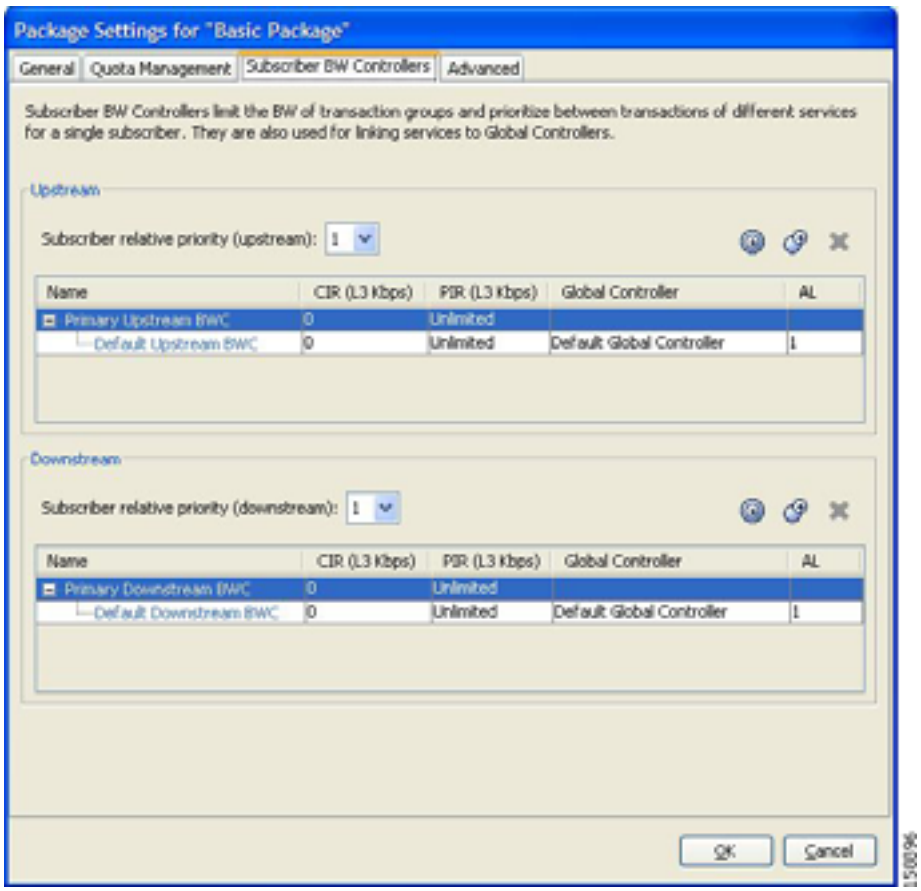
ステップ 1　Network Traffic タブで、パッケージ ツリーからパッケージを選択し、（**Edit Package**）をクリックします。

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、**Subscriber BW Controllers** タブをクリックします。

Subscriber BW Controllers タブが表示されます。

図 9-29



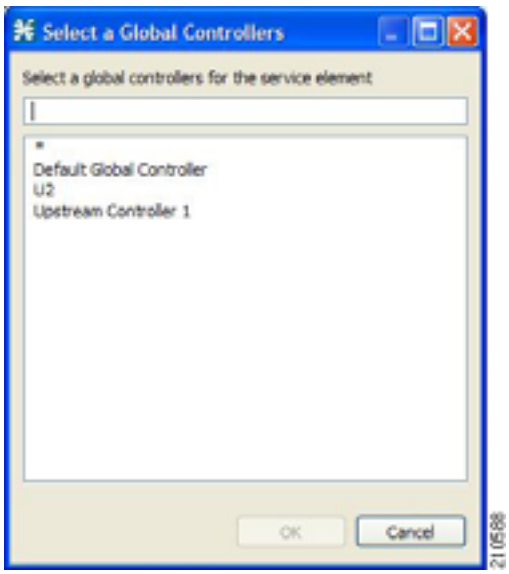
ステップ 3　ダイアログボックスの Upstream 領域に、アップストリームの帯域幅制御の要件を設定します。

1. Subscriber relative priority ドロップダウン リストから値を選択します。
2. Primary Upstream BWC のパラメータを設定します。
   - CIR フィールドに、Kbps 単位で BWC CIR を入力します。
   - 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、または kbps 単位で BWC PIR を入力します。
3. パッケージに BWC を追加するには、BWC を 1 つ追加するごとに （**Add a sub BW Controller**）を 1 回クリックします。
4. 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。
5. 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。
   - （任意）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、kbps 単位で BWC CIR の値を入力します。
   - 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、または kbps 単位で BWC PIR の値を入力します。
   - 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 セルをクリックして、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 9-30



- グローバル コントローラを選択して、**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 4　ダイアログボックスの Downstream 領域で、ダウンストリームの帯域幅制御を設定するため、ステップ 3 を実行します。

ステップ 5　**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.9-41）
- 例：P2P およびストリーミング トラフィックの制限（p.9-42）

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、およびそれぞれに設定する必要がある合計帯域幅に対する割合の最大値を確定します。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。

1. 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。
2. 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　専用の BWC が必要なサービスの場合は次の手順を実行します。

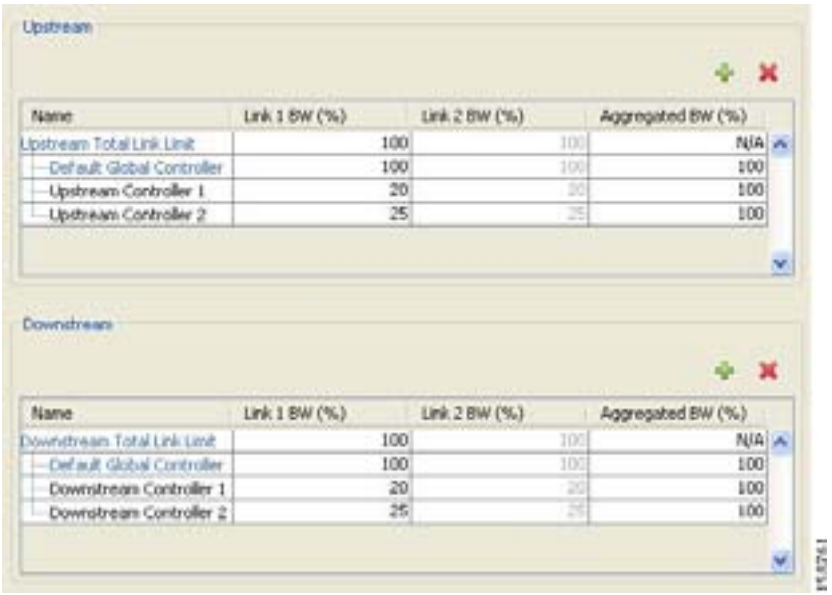
1. 規則を作成します。
2. 適切なアップストリームおよびダウンストリーム BWC を選択します。

例：P2P およびストリーミング トラフィックの制限

（注）　この例では、トラフィック フローが双方向であることを前提としており、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 コントローラのみが必要であると判断できます。

ステップ 1　Global Bandwidth Settings ダイアログボックスで、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、各グローバル コントローラに適切なトラフィックの割合を割り当てます。

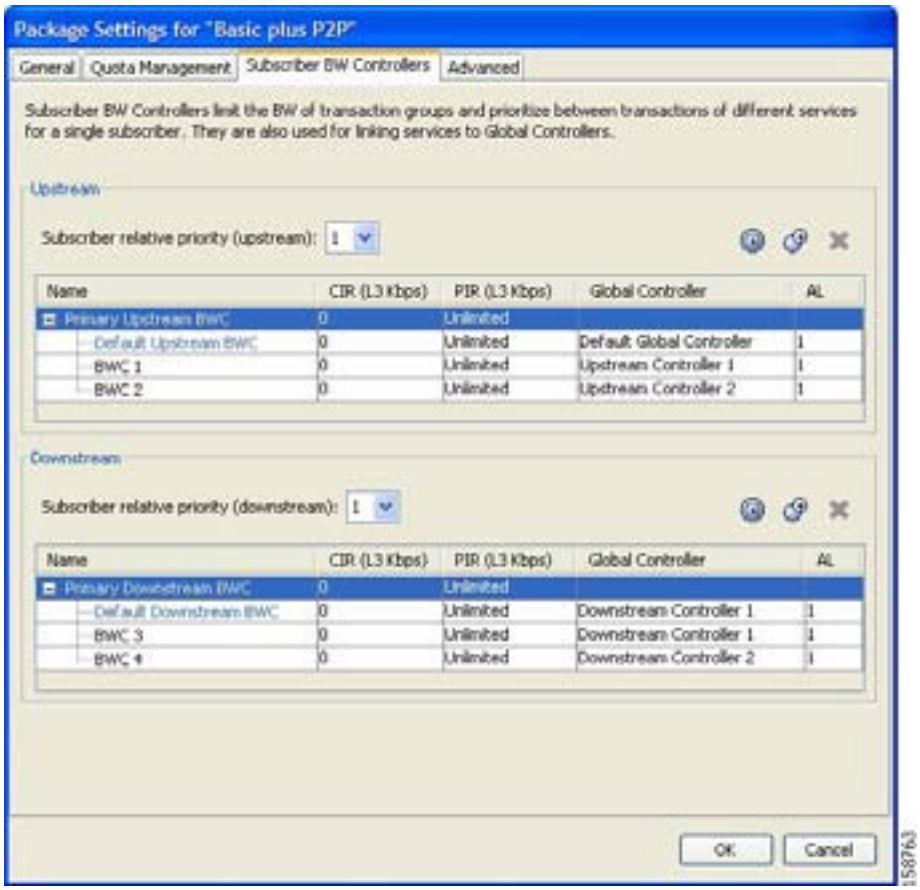
図 9-31



（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 2　Package Settings ダイアログボックスで、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、該当するグローバル コントローラにマッピングし、パラメータ（CIR、PIR、AL）を設定します。

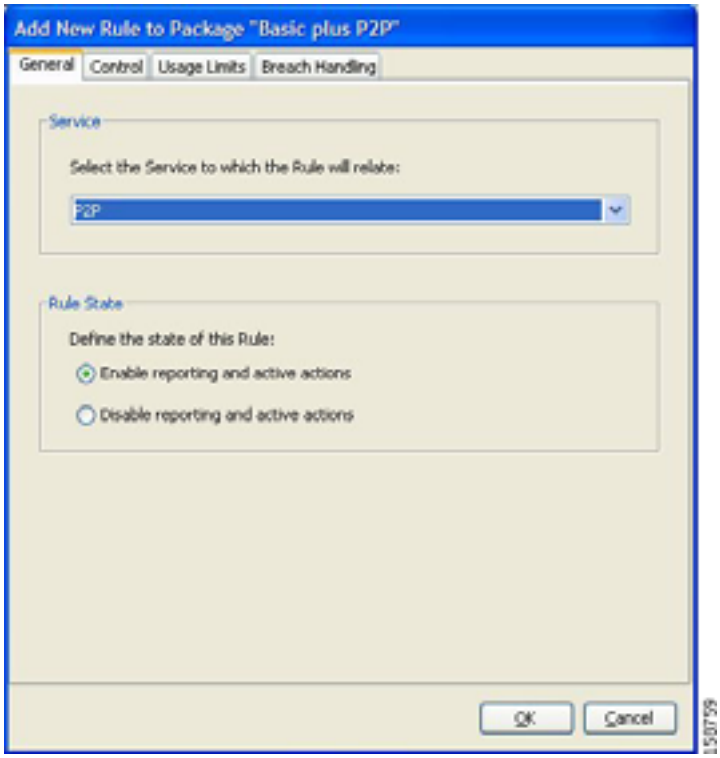
図 9-32



（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。）

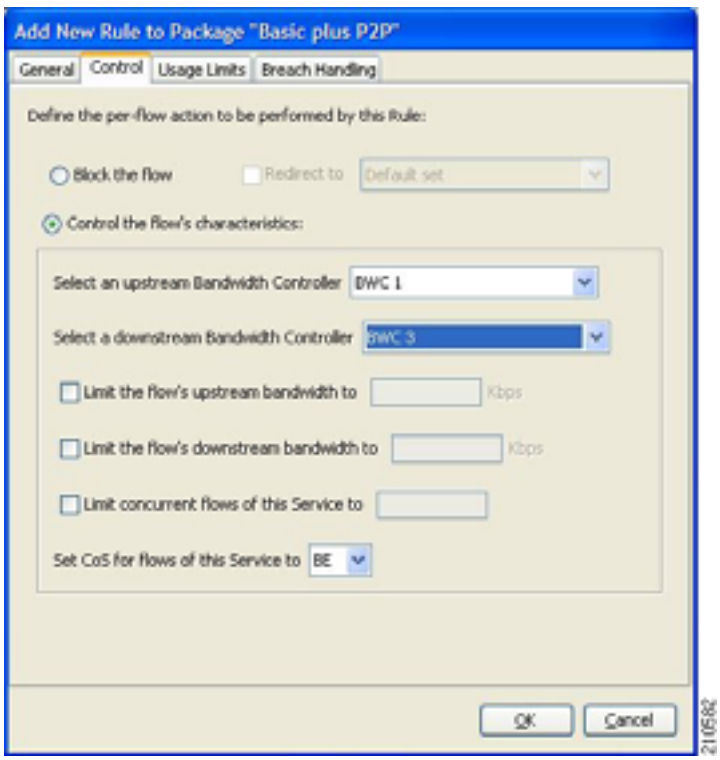
ステップ 3　P2P サービスのための規則を追加します。

図 9-33



ステップ 4　Control タブで、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 9-34



ステップ 5　ストリーミング サービスについてステップ 3 および 4 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。

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、帯域幅についてほかの 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

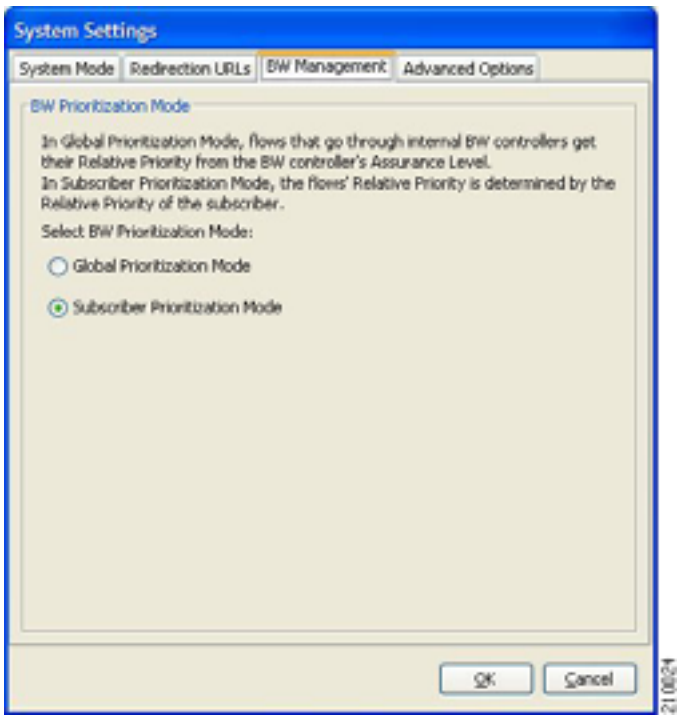
ステップ 1　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

ステップ 2　**BW Management** タブをクリックします。

BW Management タブが表示されます。

図 9-35



ステップ 3　**BW Prioritization Mode** オプション ボタンのいずれかを選択します。

- **Global Prioritization Mode**
- **Subscriber Prioritization Mode**

ステップ 4　**OK** をクリックします。

System Settings 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。仮想リンクの追加、削除、修正には 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 コントローラを含めて）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。

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 のほかのパラメータは変更されません）。

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。手順はほかのサービス 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、ほか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」の章にある「Managing Virtual Links」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

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.9-34）
- グローバル コントローラの最大帯域幅の設定（p.9-35）
- グローバル コントローラの削除（p.9-36）
- サブスクライバ帯域幅の管理（p.9-38）

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。

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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

ステップ 2　**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イネーブルにしていた場合には、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 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。

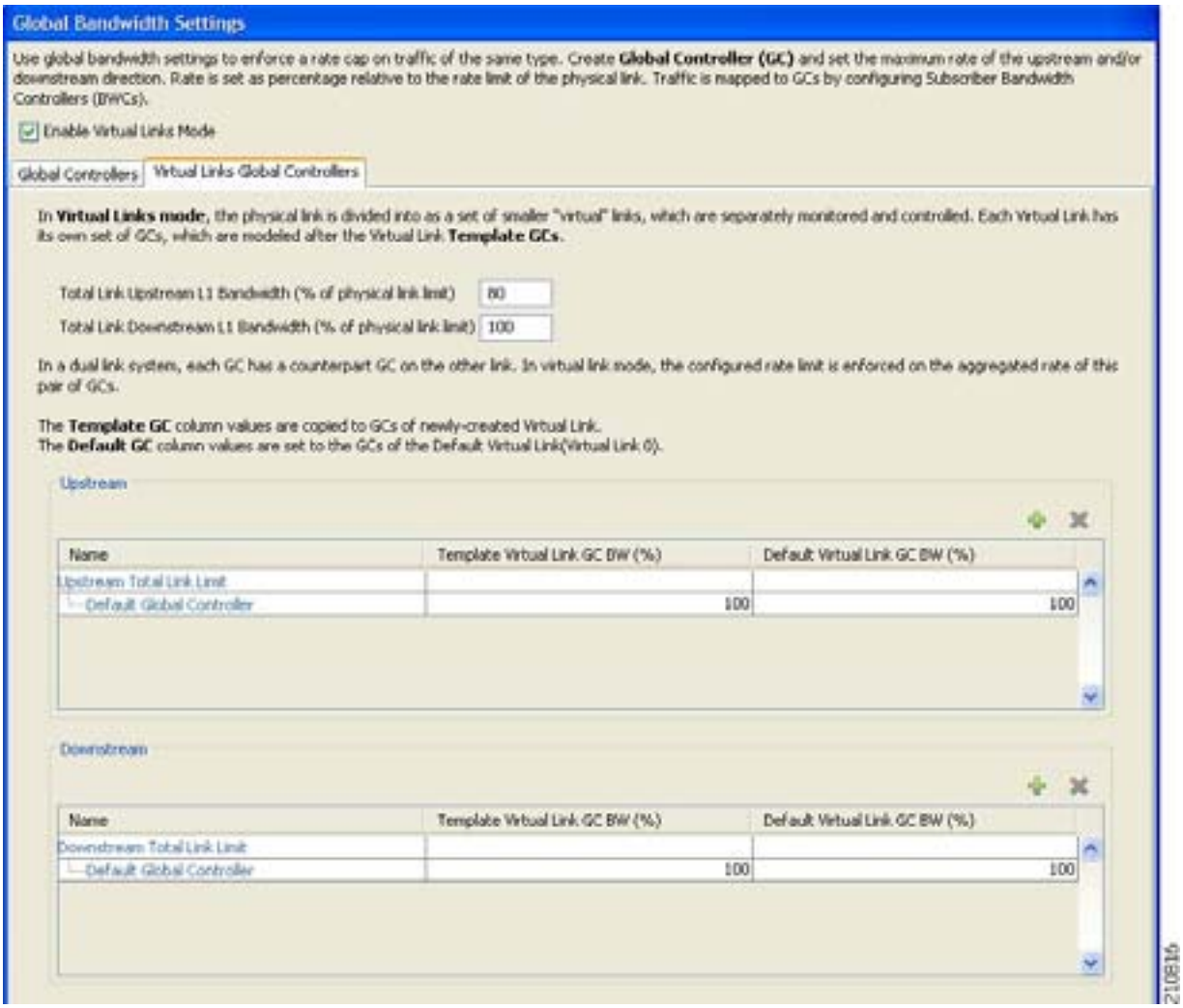
仮想リンク グローバル コントローラ設定の表示

(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　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

図 9-36



すべてのグローバル コントローラが使用できる物理リンク合計帯域幅の最大割合は、Virtual Links Global Controllers タブの上部に次のように表示されます。

- **Total Link Upstream L1 bw (% of physical link limit)**
- **Total Link Downstream L1 bw (% of physical link limit)**

ダイアログボックスのほかの部分でグローバル コントローラに関して定義するパーセント値は、ここで表示される値で決まります。そのため、たとえば Total Link Upstream L1 bw (%) の値が 80 で、アップストリームのデフォルト グローバル コントローラの値が 100> の場合、物理リンク帯域幅の 80> のうちの 100> を意味します。

ダイアログボックスの主要部は、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した 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した Downstream 領域からなります。それぞれ、次の 3 つのカラムで構成されています。

- **Name** ― グローバル コントローラに割り当てられた一意の名前。Controller 1、Controller 2 などの名前が自動的に割り当てられます。
- **Template Virtual Link GC BW (%)** ― 作成されたすべての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割合
- **Default Virtual Link GC BW (%)** ― 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割合

  これらの 2 つのカラムの値の説明については、「グローバル コントローラ設定の表示」（p.9-31）を参照してください。

ステップ 2　実際の最大帯域幅の値を表示するには、カーソルを Link 1 BW (%) のセル上に合わせます。

ツールチップに、このグローバル コントローラに許可された実際の最大帯域幅が Mbps 単位で表示されます。この数値は、SCE タイプ（ギガビット イーサネットまたはファスト イーサネット）、コントローラの最大帯域幅割合、およびリンク帯域幅の合計割合に基づいて、自動的に計算されます。

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。

デュアルリンク システムの場合、帯域幅制限は 2 つのリンクの合計に対して適用されます。

ステップ 1　Console メイン メニューから、**Configuration > Global Bandwidth Settings** を選択します。

Global Bandwidth Settings ダイアログボックスが表示されます。

ステップ 2　リンクを通過させる物理リンク容量の最大割合を、**Total Link Upstream L1 bw (% of physical link limit)** フィールドまたは **Total Link Downstream L1 bw (% of physical link limit)** フィールドに入力します。

Link 1 BW (%) セルのすべてのセルのツールチップに表示される値は、新しい合計リンク制限を反映して変化します。

ステップ 3　**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。

CLI コマンドによる仮想リンクの管理

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。CE プラットフォームの CLI に関する詳細については、『*Cisco Service Control Engine (SCE) 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 モードを開始して、`SCE(config if)#` プロンプトを表示する必要があります。

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 モードを開始して、`SCE(config if)#` プロンプトを表示する必要があります。

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]**

ライン インターフェイス コンフィギュレーション モードを開始するには、次の手順に従います。

- 仮想リンクの CLI コマンド（p.9-51）

仮想リンクの CLI コマンド

以下の表に、このセクションで挙げた仮想リンクの 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。

表 9-1　仮想リンクの CLI コマンド（続き）

コマンド	説明
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 changed	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。

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** と入力します。

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。

クォータの管理

違反処理パラメータ

以下は、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です。

- 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」[p.8-8] 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 パラメータの設定」[p.10-36] を参照）。リダイレクションをサポートしているのは、HTTP、HTTP Streaming、および RTSP の 3 つのプロトコル タイプだけです。リダイレクションは、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。
  - 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 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。
  - 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 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） サブスクライバ通知は、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。

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.10-27）を参照してください。

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。

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（次のセクションを参照）。

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 タブの 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.10-40] 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）。クォータ補充時間が 1 時間ごとの場合は、したがって分散を 60 分に設定します。

クォータ補充の分散機能は、ほか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　Network Traffic 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 タブが表示されます。

ステップ 3　**Select quota management mode** オプション ボタンのいずれかを選択します。

- **External** ― 外部から要求があった場合に補充します。

（注）　外部クォータ管理は、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イネーブルのときに External オプション ボタンを選択しようとした場合は、Package Error 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。

- **Periodical** ― 集約時間の終了時にクォータを自動的に補充します。

(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.9-54] を参照）。

ステップ 4　Periodical オプション ボタンを選択した場合は、**Aggregation Period** オプション ボタンのいずれかを選択して、パッケージのためにクォータを更新するタイミングを指定します。

- **Hourly Resolution** ― 1 時間ごとに補充します。
- **Daily Resolution** ― 深夜 0 時に補充します。

ステップ 5　クォータ バケットを設定します。

1. （任意）Name セルに、バケットの名前を入力します。

(注)　バケットのデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

2. Type セルをクリックし、セルに表示されるドロップダウン アローをクリックして、ドロップダウン リストから **Volume (L3 Kbytes)** または **Number of sessions** を選択します。
3. Quota Limit セルに、選択した Type に応じて、このバケットの実際の制限を KB またはセッション数で入力します。

(注)　クォータ制限は、ステップ 4 で Periodical オプション ボタンを選択した場合のみ設定できます。

設定が、パッケージに適用する規則に適しているか確認します。たとえば、バケットを設定するときに Type にセッション数を指定しない場合は、セッション数に関する使用制限を含む規則を定義できません。

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。

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が使用するためのクォータ バケットを選択できます。ドロップダウン リストのクォータ バケットは、パッケージのセットアップ時に定義されたものです（「パッケージのクォータ管理設定の編集」[p.9-54] Quota Management タブ [Packages] を使用する説明を参照）。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　右のペイン（Rule）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　**Usage Limits** タブをクリックします。

Usage Limits タブが表示されます。

ステップ 5　ドロップダウン リストから該当するバケットを選択します。

- Select Quota Bucket for upstream traffic
- Select Quota Bucket for downstream traffic
- Select Quota Bucket for sessions

（注）　無制限クォータの場合、**None (Unlimited)** を選択します。

ステップ 6　クォータの違反が発生した場合の動作を定義するには（すべてのクォータ バケットが無制限クォータの場合は該当しない）、次のセクションのステップを実行します。

ステップ 7　**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。

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　右のペイン（Rule）で、規則を選択します。

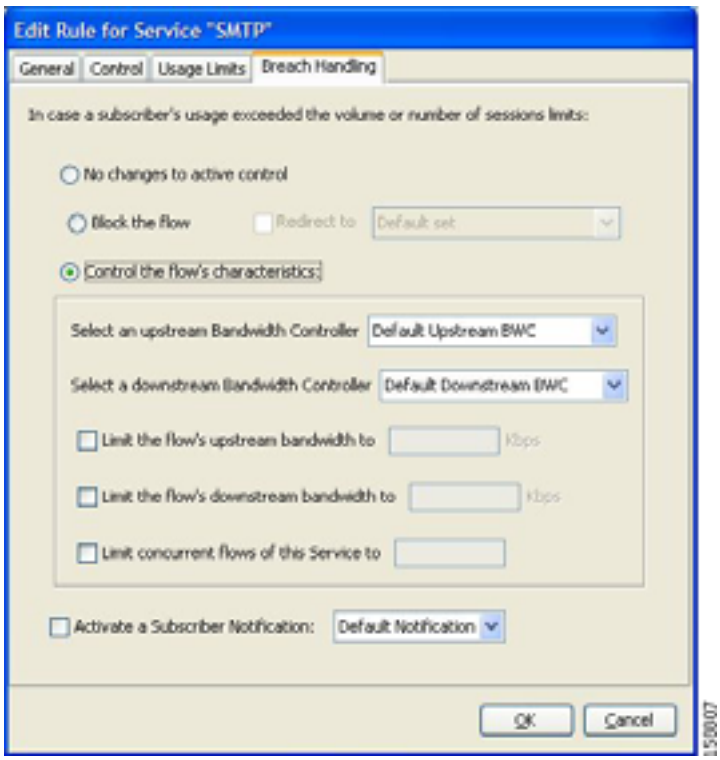
ステップ 3　（**Edit Rule**）をクリックします。

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 タブが表示されます。

図 9-37



ステップ 5　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 7 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 9 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 ボタンを選択します。

ステップ 6　ステップ 10 に進んでください。

ステップ 7　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、以下を実行します。

1. Block the flow オプション ボタンを選択します。

   Redirect to チェックボックスが使用可能になります。
2. （任意）ブロックされたフローをリダイレクト（HTTP、HTTP Streaming、RTSP の場合）するには、Redirect to チェックボックスをオンにします。

（注）　リダイレクションは、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イネーブルのときに Redirect to チェックボックスをオンにしようとした場合は、Rule Error 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。

3. Redirection URL Set ドロップダウン リストが使用可能になります。

(注) この規則のサービスまたはサービス　グループにリダイレクトできないプロトコルが含まれている場合、Rule Warning メッセージが表示されます。

OK をクリックし、ステップ 10 に進みます。

4. Redirect ドロップダウン リストからリダイレクション URL セットを選択します。

ステップ 8　ステップ 10 に進んでください。

ステップ 9　**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。

- 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（「パッケージ サブスクライバ BWC の編集」[p.9-39] を参照）。

  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。
- （任意）**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。
- （任意）**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。
- （任意）**Limit concurrent flow of this Service** チェックボックスをオンにして、関連するフィールドに値を入力します。

ステップ 10　サブスクライバ通知をアクティブにします。

(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。

- **Activate a Subscriber Notification** チェックボックスをオンにして、ドロップダウン リストで目的のサブスクライバ通知を選択します。

(注) サブスクライバ通知は、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イネーブル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した場合は、Rule Error メッセージが表示されます。

(注) **OK** をクリックして続行します。

ステップ 11　**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。

CHAPTER 10

Service Configuration Editor の使用法：その他のオプション

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 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、DDoS 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を設定できます。

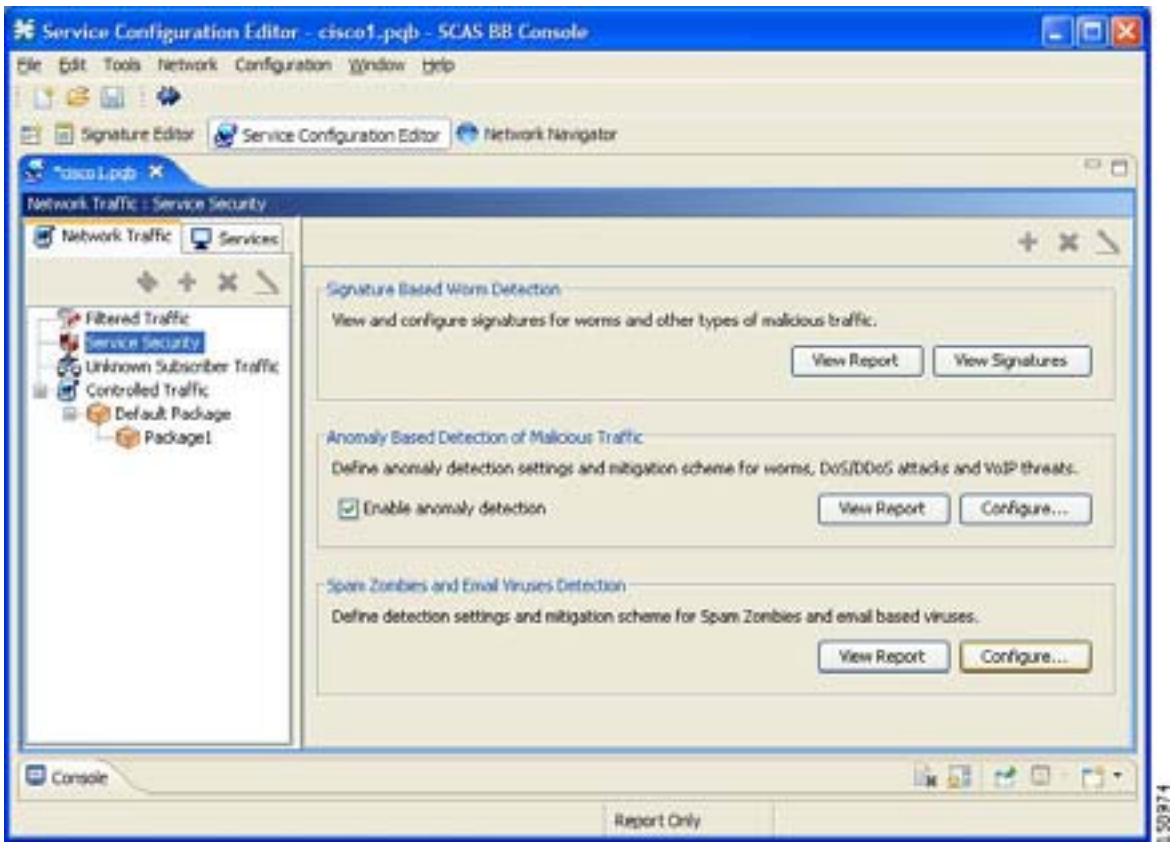
サービス セキュリティ ダッシュボードでは、Reporter ツールの悪質トラフィック レポートにアクセスすることもできます。

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



さまざまな検出メカニズムの表示と設定、および悪質トラフィック レポートの表示については、次のセクションで説明します。

ワーム検出

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 — Service Control Engine（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ことがある異常を検出できます。「異常検出の管理」（p.10-3）を参照してください。
- 大量メール送信ベース検出 — 電子メール トラフィック分析により、電子メールベース 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 リストから 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

次のうちいずれかを実行します。

ステップ 1　シスコが提供する最新 DSS ファイルまたは SPQI ファイルをインポートします。

ステップ 2　サービス コンフィギュレーションに追加するワーム シグニチャを含む DSS ファイルを作成します。

関連情報

詳細情報については、「プロトコル シグニチャの管理」（p.7-39）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（TCP 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。
- DoS ディテクタ ― 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。一方が他方を攻撃している IP アドレスのペア間において、接続レートで異常を検出します。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を検出します（その IP アドレスが攻撃されている）。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 UDP 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 CLI 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アトリビュートが関連します。

- 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 RDR 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（シスコ固有の 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）、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.10-27）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.10-40] を参照）に適用されません。

ユーザ定義ディテクタにも、次のアトリビュートのうち 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のみに適用されます。

- 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のみに適用されます。

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。

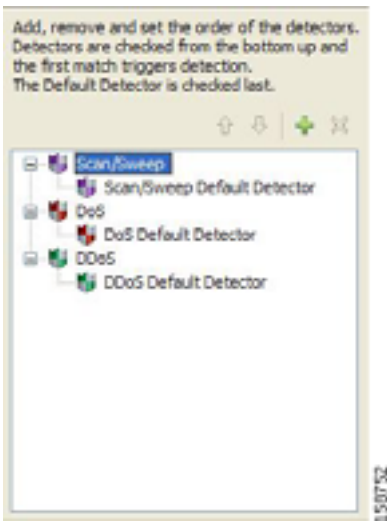
異常ディテクタごとに関連パラメータを表示し、ディテクタに組み込まれるすべての異常タイプのリスト、およびそのパラメータを表示できます。

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



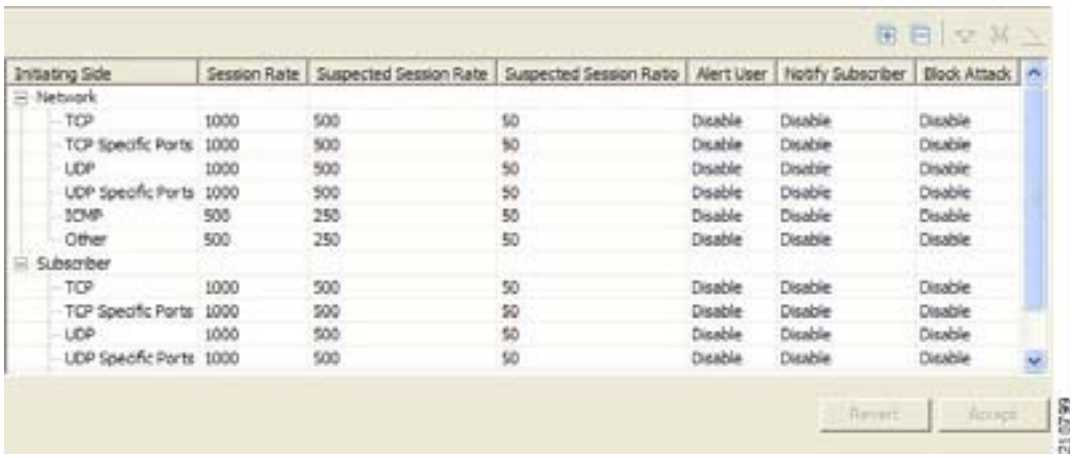
ステップ 2　ディテクタ ツリーでディテクタを選択します。

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

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



非対称ルーティング分類モードがイネーブルになっている場合、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ディセーブルになります。

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.10-11] 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。

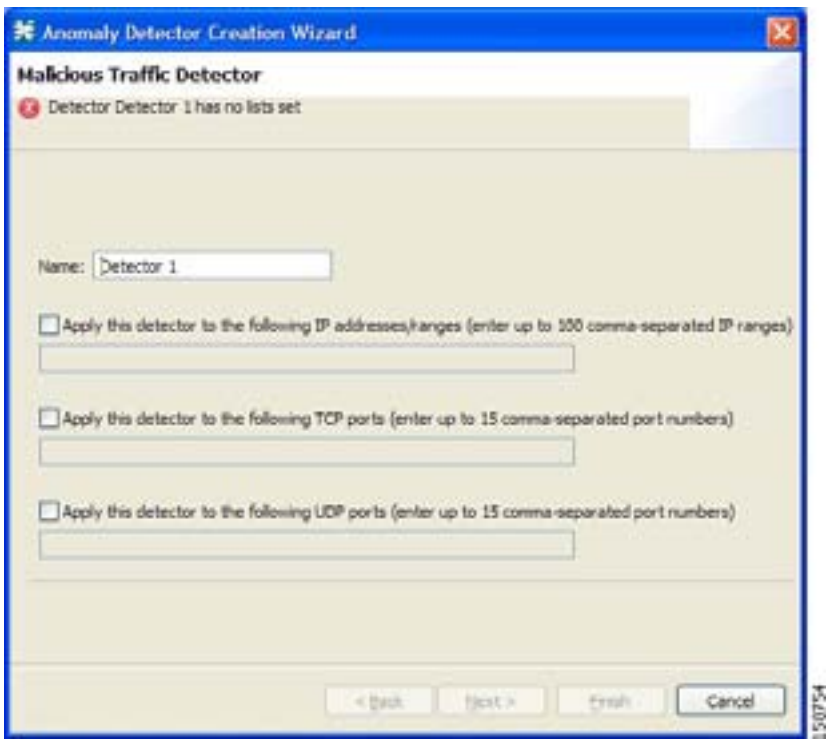
Anomaly Detection Settings ダイアログボックスが表示されます。

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、Malicious Traffic Detector 画面が開きます。

図 10-5



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、ディテクタの範囲を制限します。

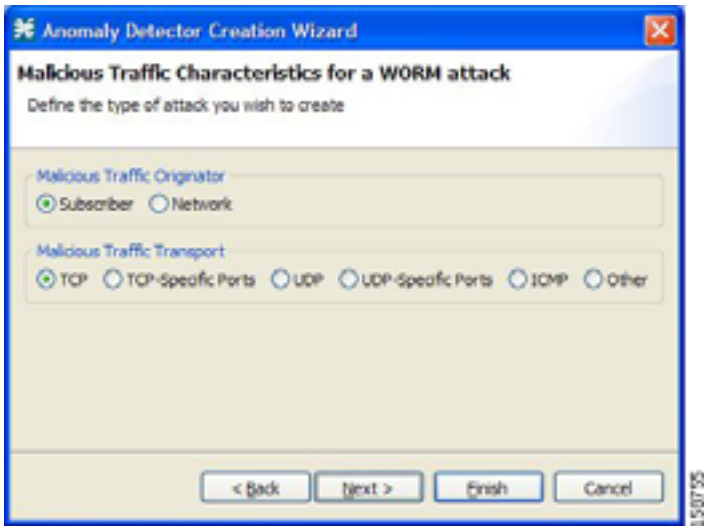
関連フィールドが有効になります。

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 画面が開きます。

図 10-6



ステップ 8　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。

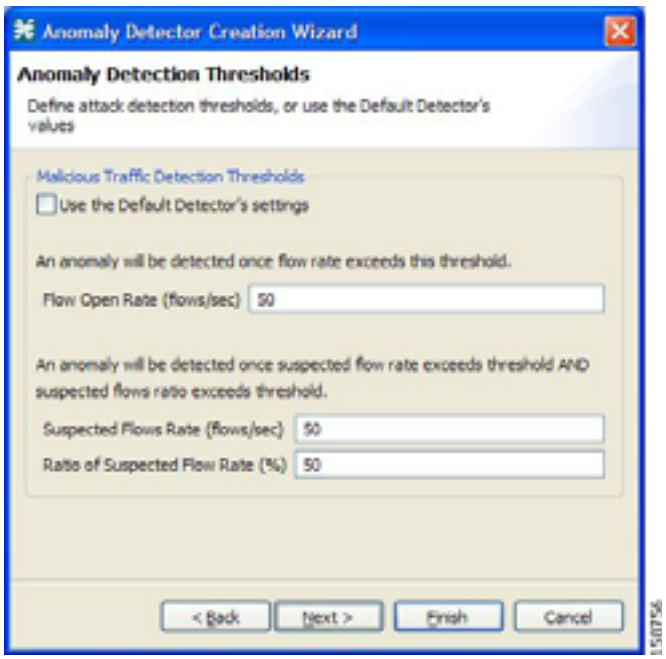
DDoS ディテクタを定義している場合は、定義している異常タイプのターゲット側を選択します。

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 画面が開きます。

図 10-7



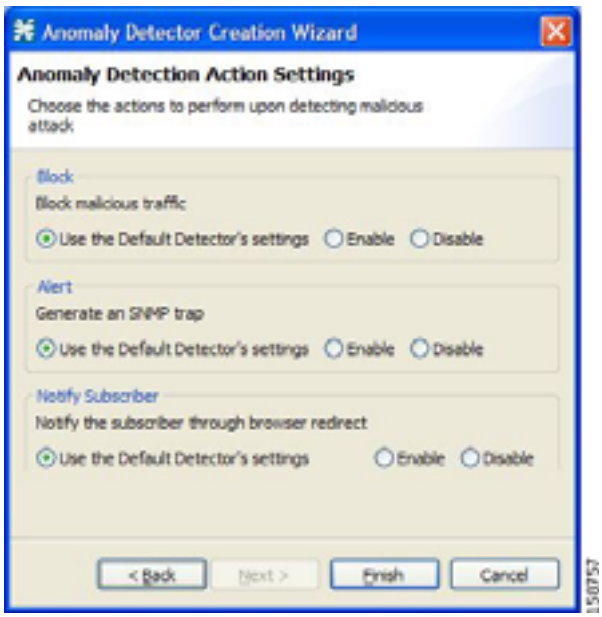
ステップ 11　次のうちいずれかを実行します。

- この異常タイプにデフォルト　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 画面が開きます。

図 10-8



ステップ 13　Block、Alert、Notify Subscriber のアクションを選択します。

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。

ステップ 15　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.10-11] 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 画面が開きます（「異常タイプの追加」[p.10-13] を参照）。

ステップ 4　次のうちいずれかを実行します。

- この異常タイプにデフォルト 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 画面が開きます。

ステップ 6　Block、Alert、Notify Subscriber のアクションを変更します。

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 画面が開きます（「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 画面が開きます。

ステップ 7　次のうちいずれかを実行します。

- この異常タイプにデフォルト 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 画面が開きます。

ステップ 9　Block、Alert、Notify Subscriber のアクションを選択します。

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 10-9

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。

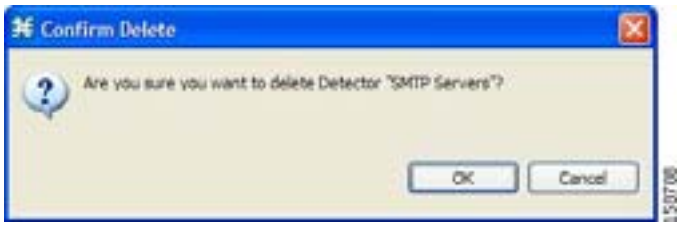
Anomaly Detection Settings ダイアログボックスが表示されます。

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 10-10



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。

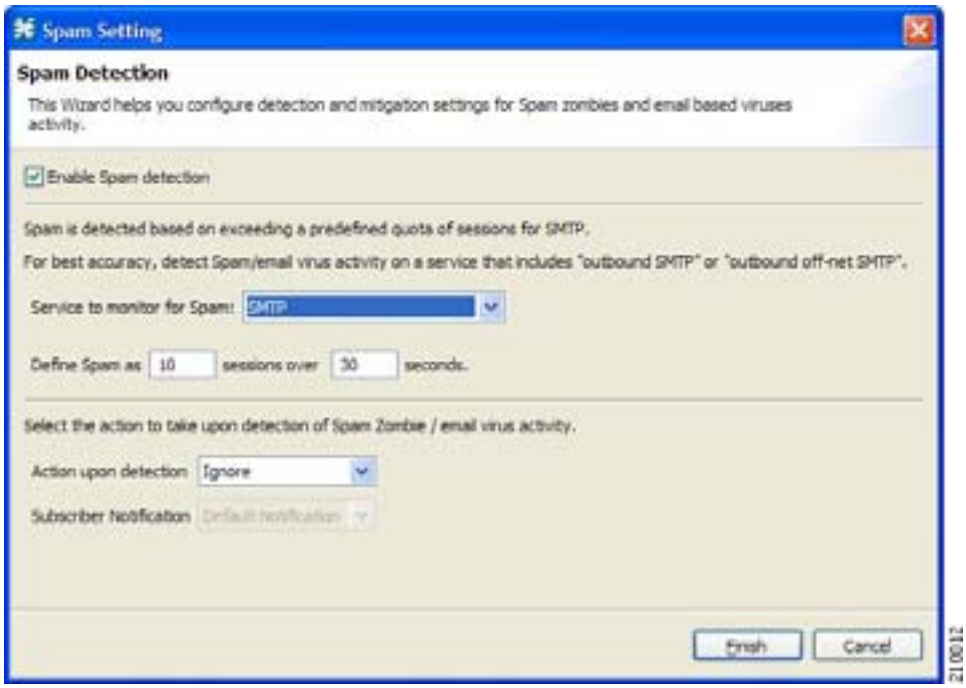
Anomaly Detection Settings ダイアログボックスが閉じます。

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 Setting ダイアログボックスが表示されます。

図 10-11



ステップ 2　**Enable Spam detection** チェック ボックスをオフにします。スパム検出が無効になります。

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 リストからサービスを選択します。

(注)　「発信 SMTP」や「オフネット SMTP」などの限定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　異常動作の電子メール セッション レートのしきい値を定義します。

ステップ 5　悪質アクティビティの検出時に実行する処理を Action upon detection ドロップダウン リストから選択します。

- Ignore（無視）
- Block（ブロック）
- Notify（通知）
- Block and notify（ブロックおよび通知）

ステップ 6　Notify または Block and notify を選択すると、Subscriber Notification ドロップダウン リストが有効になります。サブスクライバ通知を選択してください。

(注)　適切なサブスクライバ通知を定義するには、「サブスクライバ通知の管理」（p.10-27）を参照してください。

ステップ 7　**Finish** をクリックします。

Spam Setting 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についての情報

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。

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
  - 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。フィルタ規則では、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一部のフロー タイプを無視し、フローを変更せずに転送するように、Service Control Engine（SCE）プラットフォームに指示できます。

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 OSS プロトコル（DHCP など）、およびルーティング プロトコル（BGP 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。

特定のプロトコルのフローでは、フローのレイヤ 7 の特性によってもフィルタ処理ができます（「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.10-40] を参照）。ほかのフィルタ処理されたフローの場合と同様に、レイヤ 7 によるフィルタ処理がされたフローは、分類、制御、レポートが行われません。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。

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。

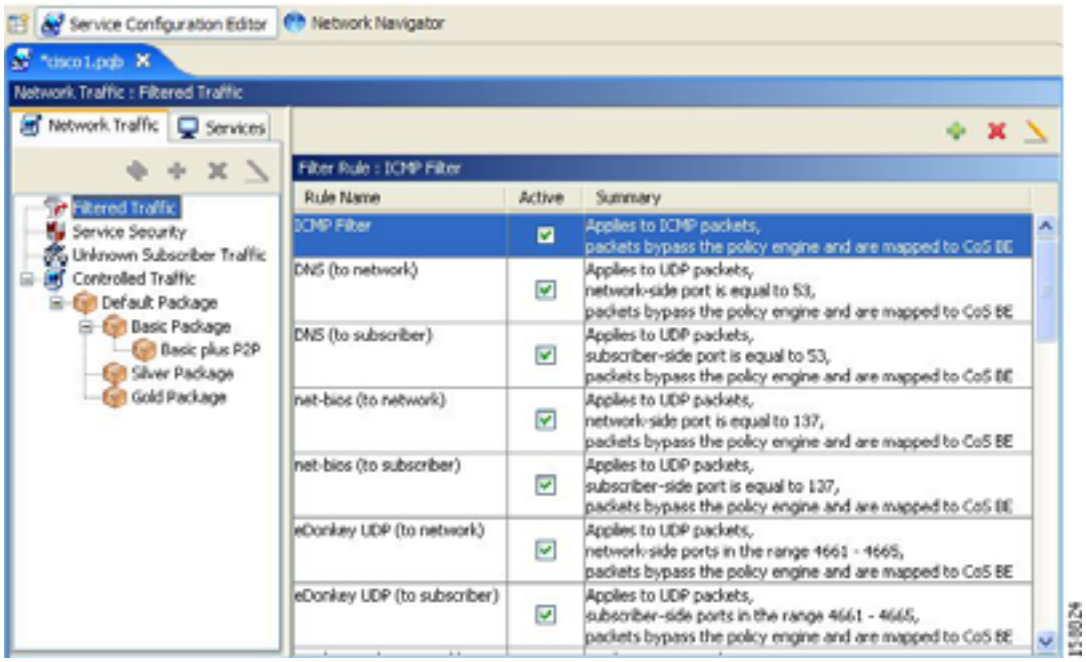
フィルタ規則ごとのリストには、規則の名前、ステータス、簡潔な説明（システムが生成）が含まれます。

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.10-25] を参照）。

ステップ 1　Network Traffic 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 10-12



フィルタ規則の追加

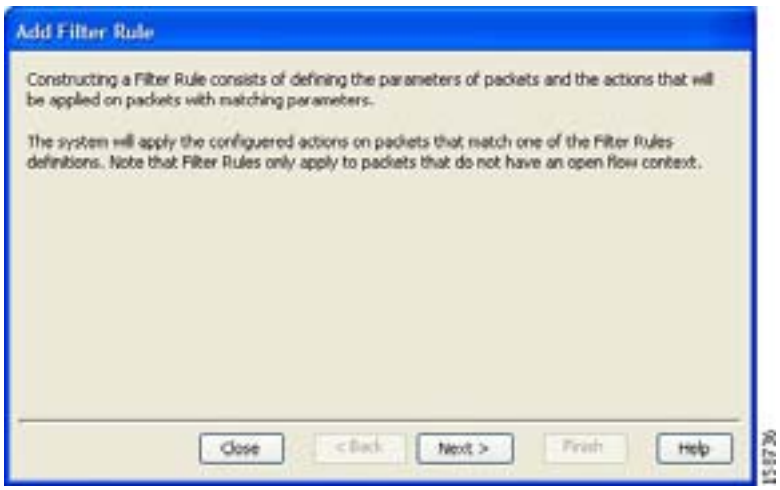
Add Filter Rule ウィザードは、フィルタ規則の追加プロセスを示します。

ステップ 1　Network Traffic 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 10-13



ステップ 3　**Next** をクリックします。

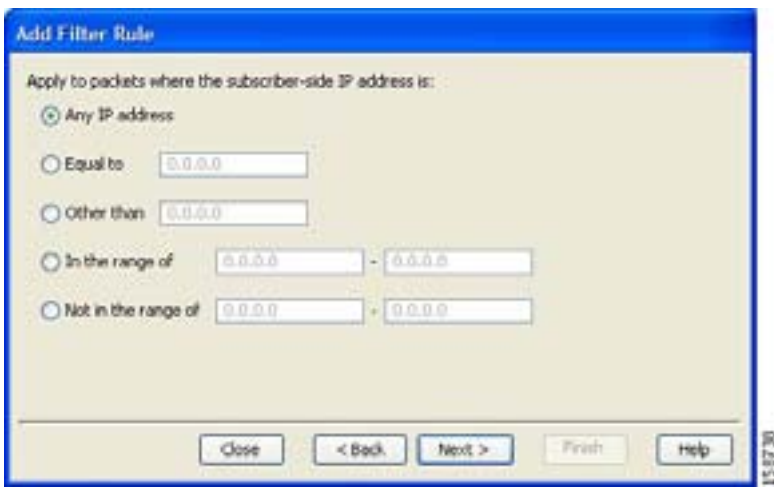
Add Filter Rule ウィザードの Transport Type and Direction 画面が開きます。

図 10-14

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 画面が開きます。

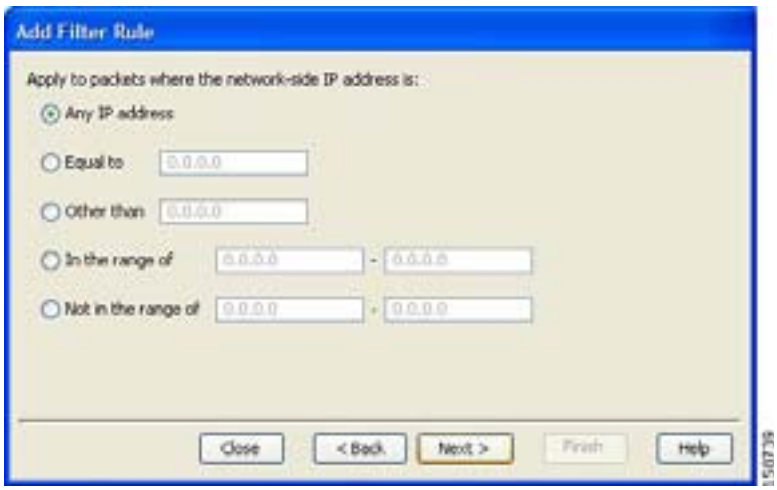
図 10-15



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 画面が開きます。

図 10-16



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 か UDP でない場合は、Add Filter Rule ウィザードの ToS 画面が開きます。ステップ 9 に進んでください。

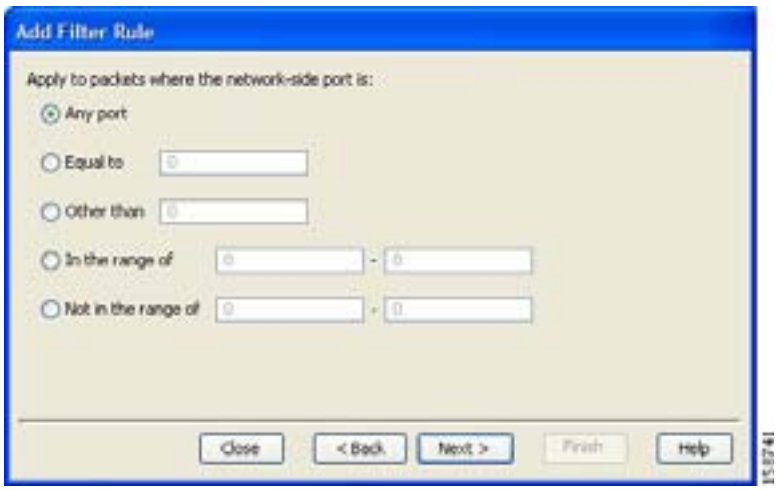
ステップ 4 で選択したトランスポート タイプが TCP か UDP である場合は、Add Filter Rule ウィザードの Subscriber-Side Port 画面が開きます。

図 10-17

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 画面が開きます。

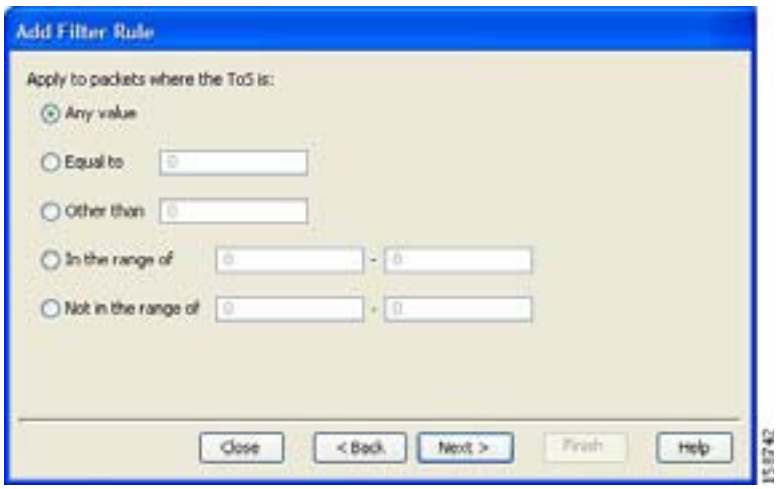
図 10-18



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 画面が開きます。

図 10-19



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 画面が開きます。

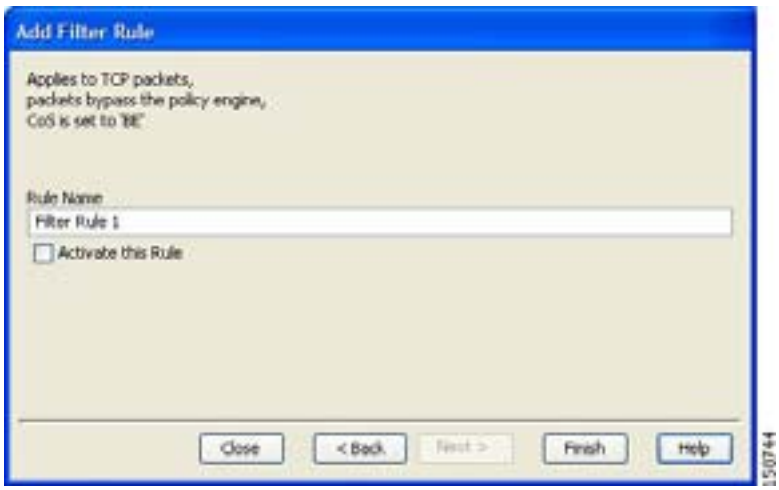
図 10-20

- 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。
- Bypass and 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 SCA BB に渡されません。

ステップ 10　必要なアクションのオンまたはオフを行い、サービス クラス値を選択して Next をクリックします。

Add Filter Rule ウィザードの Finish 画面が開きます。

図 10-21



ステップ 11　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)　フィルタ規則にデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

ステップ 12　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 13　**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　Network Traffic 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 画面が表示されます。

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.10-20）のステップ 4 ～ 11 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アトリビュート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　Network Traffic タブで **Filtered Traffic** ノードを選択します。

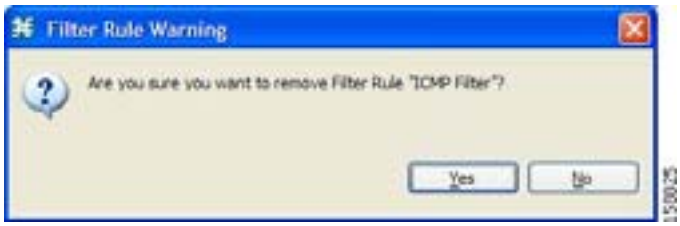
すべてのフィルタ規則のリストが右の規則ペインに表示されます。

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。

フィルタ規則の警告メッセージが表示されます。

図 10-22



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　Network Traffic 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)　サブスクライバ通知は、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。

Cisco Service Control Application for Broadband（SCA BB）では、デフォルト通知およびネットワーク攻撃通知も含めて最大 31 のサブスクライバ通知がサポートされます。

- サブスクライバ通知パラメータ（p.10-27）
- ネットワーク攻撃通知についての情報（p.10-29）
- サブスクライバ通知の表示（p.10-30）
- サブスクライバ通知の追加（p.10-31）
- サブスクライバ通知の編集（p.10-32）
- サブスクライバ通知の削除（p.10-33）

サブスクライバ通知パラメータ

サブスクライバ通知は次のパラメータで定義します。

- Name ― 各サブスクライバ通知には一意の名前を付ける必要があります。

(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。

  - ― Destination URL ― リダイレクションを有効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。
  - ― 通知パラメータ ― リダイレクション時にオプションとして追加できる宛先 URL のクエリー部分。

  宛先 URL に追加される通知パラメータのフォーマットは、次のとおりです。

- `?n=<notification-ID>&s=<subscriber-ID>`

  <notification-ID> はサブスクライバにリダイレクトされた通知の ID、<subscriber-ID> はサブスクライバ名です。

(注)　「ネットワーク攻撃通知パラメータ」（p.10-29）にはフォーマットが異なるものがあります。

- 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。
- Dismissal method ― 通知状態を解除（非アクティブ）にする時期を指定します。この解除方式は次のいずれかです。

— Subscriber browses to destination URL（デフォルト）— サブスクライバは、宛先 URL をブラウズするとすぐに通知されたとみなされ、通知状態が解除になります。

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 をブラウズするとただちに通知状態が解除され、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）。

— The condition that activated the notification no longer holds — 通知状態の解除は、サブスクライバではなく条件の決定によって決まります。

たとえば、クォータを超過した場合、通知状態が解除されるのは、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したときだけです。

(注) ネットワーク攻撃通知ではこのオプションを使用できません。サブスクライバが通知に対応してから、通知を解除する必要があります。

- Subscriber browses to dismissal URL — サブスクライバが宛先 URL から別の最終 URL に進むまで、通知状態は解除されません。

  サブスクライバが解除 URL にアクセスして通知が解除されるまで、すべての HTTP フローはリダイレクトされます。デフォルトでは、宛先 URL は解除 URL でもあるため、最初のリダイレクションが発生すると、通知が解除されます。ただし、サブスクライバが通知を確認応答するように、別の解除 URL を定義できます。

  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、共通のプレフィッ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、次のように入力します。
- `*.some-isp.net:/redirect/*`

  この場合は次のすべての 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有効でも、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、新しいサブスクライバ通知を追加したときに定義されます（「サブスクライバ通知の追加」[p.10-31] を参照）。パラメータの修正はいつでもできます（「サブスクライバ通知の編集」[p.10-32] を参照）。

ネットワーク攻撃通知についての情報

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.10-40] を参照してください。

（注） これまでのバージョンの 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>
```

次の表に、テール内の各フィールドの意味を示します。

表 10-1

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 ― 送信元 • 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	
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

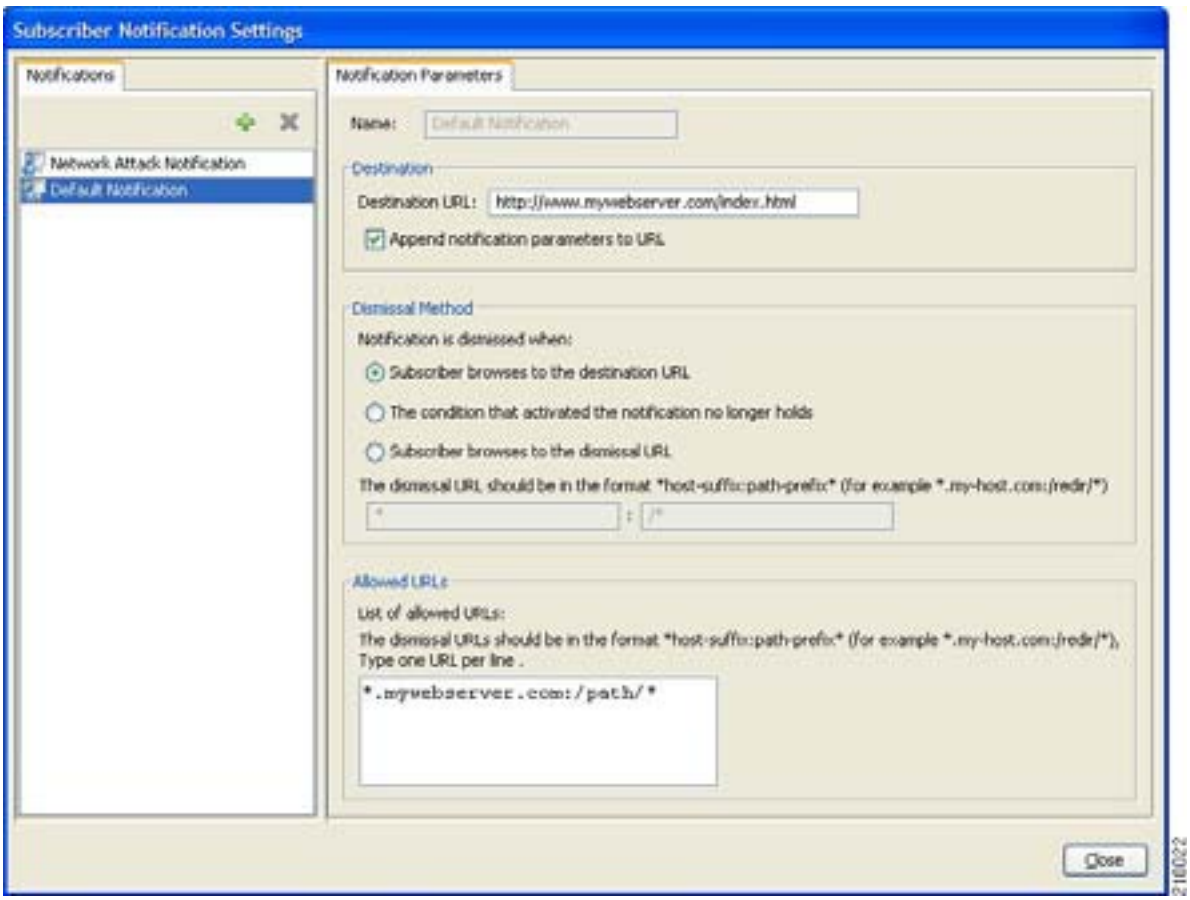
```
http://www.some-isp.net/warning?ip=80.178.113.222&side=s&proto=TCP&no=3
4&nd=4&to=34&td=10&ac=B&nh=100
```

サブスクライバ通知の表示

ステップ 1　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

図 10-23



すべてのサブスクライバ通知のリストが Notifications タブに表示されます。

ステップ 2　パラメータを表示するサブスクライバ通知をリストからクリックします。

サブスクライバ通知のパラメータが Notification Parameters タブに表示されます。

ステップ 3　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

サブスクライバ通知の追加

最大 29 のサブスクライバ通知をサービス コンフィギュレーションに追加できます。

(注)　サブスクライバ通知を作成しても、サブスクライバ通知機能は有効になりません。サブスクライバ通知を定義したら、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（「規則のための違反処理パラメータの編集」[p.9-56] を参照）。

ステップ 1　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

ステップ 2　（**Add**）をクリックします。

ステップ 3　新しいサブスクライバ通知の一意の名前を Name フィールドに入力します。

（注）　サブスクライバ通知にデフォルト名を使用できます。わかりやすい名前の入力を推奨します。

ステップ 4　Destination URL フィールドに宛先 URL を入力します。

ステップ 5　通知パラメータを宛先 URL に付ける場合は、**Append notification parameters to URL** チェック ボックスをオンにします。

ステップ 6　**Dismissal Method** オプション ボタンのいずれかを選択します。

- **Subscriber browses to the destination URL**
- **The condition that activated the notification no longer holds**
- **Subscriber browses to the dismissal URL**

ステップ 7　ステップ 6 で Subscriber browses to the dismissal URL を選択した場合は、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ックスを入力します。

ステップ 8　Allowed URL テキスト ボックスに、許可 URL を 1 行に 1 つずつ入力します。

ステップ 9　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

サブスクライバ通知の編集

ステップ 1　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

ステップ 2　Notifications タブでサブスクライバ通知をクリックします。パラメータが表示されます。

ステップ 3　サブスクライバ通知のパラメータを Notification Parameters タブで編集します。

ステップ 4　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

サブスクライバ通知の削除

サブスクライバ通知はいつでも削除できます。

デフォルト通知またはネットワーク攻撃通知を削除することはできません。

ステップ 1　Console メイン メニューから、**Configuration > Subscriber Notifications** を選択します。

Subscriber Notifications Settings ダイアログボックスが表示されます。

ステップ 2　Notifications タブでサブスクライバ通知をクリックします。

ステップ 3　（**Delete**）をクリックします。

ステップ 4　**Yes** をクリックします。

ステップ 5　**Close** をクリックします。

Subscriber Notifications Settings ダイアログボックスが閉じます。

システム設定の管理

Console では、以下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
- リダイレクションをサポートするプロトコルのリダイレクション URL
- BW 優先順位モード（「BW 管理優先順位モードの設定」[p.9-45] を参照）
- 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 モードの設定についての情報

- システムの動作モード（p.10-34）
- 非対称ルーティング分類モード（p.10-34）

システムの動作モード

Console では、システムの動作モードを選択できます。この機能では、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 トラフィックで実施し、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 の生成のみを行います。ネットワーク トラフィックには、アクティブな規則適用は実行されません。
- 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規則を適用しません。

非対称ルーティング分類モード

Console から非対称ルーティング分類モードをイネーブルにしたりディセーブルにしたりできます。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、このモードをイネーブル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。ただし、このモードをイネーブルにした場合には、SCA BB の次の機能が使用できません。

- Flavors
- 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

- 異常検知（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した場合、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 レートが同じに設定されます（「異常検出設定の表示」[p.10-6] を参照）。これにより異常検知は実質的にディセーブルになります。

非対称ルーティング分類モードがイネーブルの場合、Service Configuration Editor には（Problems View 画面に）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、非対称ルーティング分類モードがイネーブルの場合に影響を受けます。

- サブスクライバ アウェア モードはサポートされません。
- 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

非対称ルーティング分類モードがイネーブルになっている場合、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。

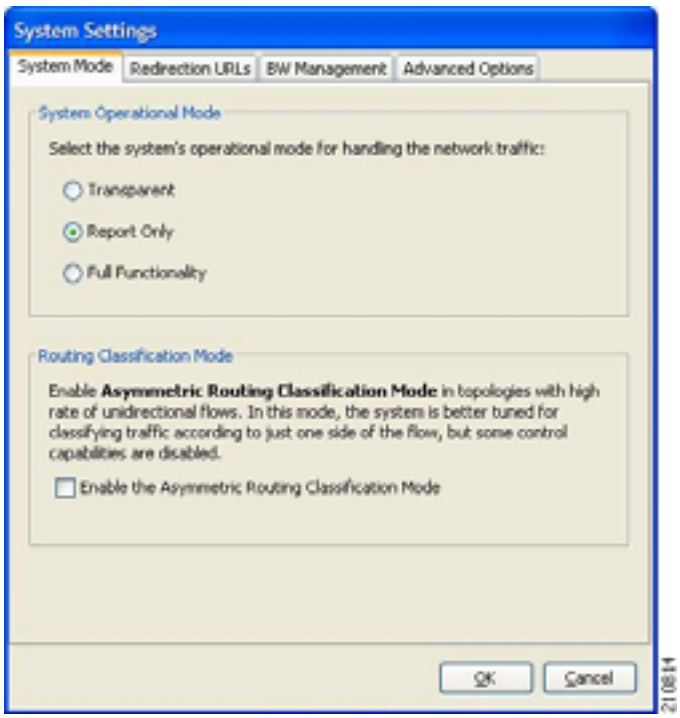
- すべての異常ディテクタの不審セッション レートとセッション レートは同じに設定されます。
- デフォルト サービス コンフィギュレーションにフレーバは作成されず、サービス要素は指定されたフレーバを持ちません。
- クォータ管理モードは、集約時間が 1 日 1 回の定期モードになります。
- 対称モードに切り替えても非対称ルーティング分類モードの制限は保持されます。制限を変更するには、サービス コンフィギュレーションを編集する必要があります。

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　Console メイン メニューから、**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 10-24



ステップ 2　**System Operational Mode** オプション ボタンのいずれかを選択します。

- **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。

リダイレクション パラメータの設定

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」サブスクライバのみ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。規則を定義する際に、使用するリダイレクション セットを設定できます（「規則のためのフローごとのアクションの定義」[p.9-15] を参照）。

(注)　リダイレクションは、非対称ルーティング分類モードがイネーブルの場合はサポートされません。

Console のリダイレクション機能では、次の 3 つのプロトコルのみ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 49 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>
```

リダイレクション URL セットの追加

最大で 49 のリダイレクション セットを追加できます。

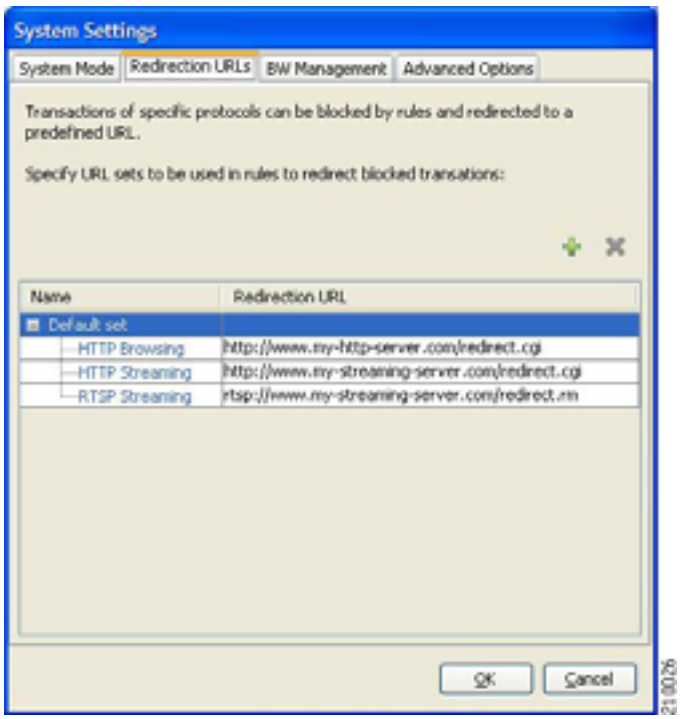
ステップ 1　Console メイン メニューから、**Configuration > System Settings** を選択します。

System Settings ダイアログボックスが表示されます。

ステップ 2　**Redirection URLs** タブをクリックします。

Redirection URL タブが開きます。

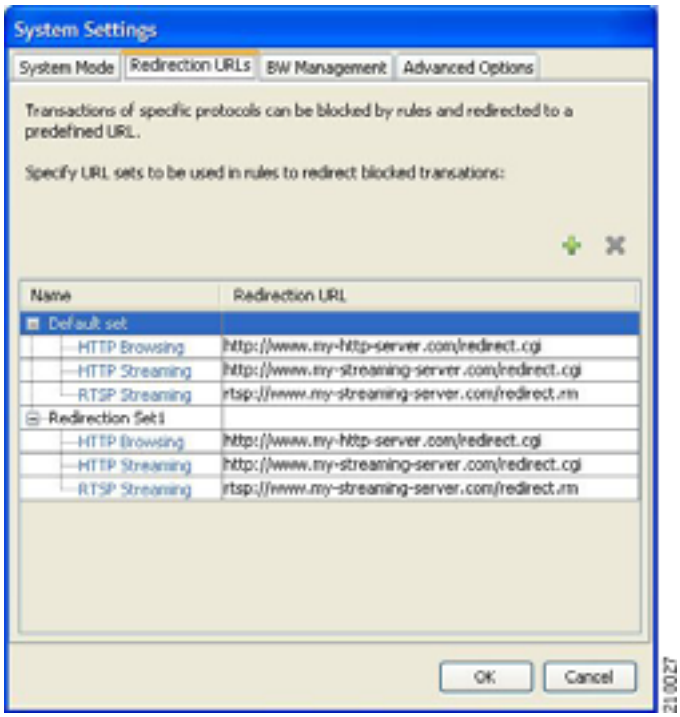
図 10-25



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、リダイレクション セット リストに追加されます。

図 10-26



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 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 URL セルに新しい値を入力します。

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。

リダイレクション グループがリダイレクション セット リストに追加されます。

リダイレクション パラメータの編集

ステップ 1　Console メイン メニューから、**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　**Redirection URLs** タブをクリックします。

Redirection URL タブが開きます。

ステップ 3　**Redirection URL** カラムの URL をクリックします。

ステップ 4　新しい URL を入力します。

ステップ 5　**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。
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 セットの削除

ステップ 1　Console メイン メニューから、**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　**Redirection URLs** タブをクリックします。

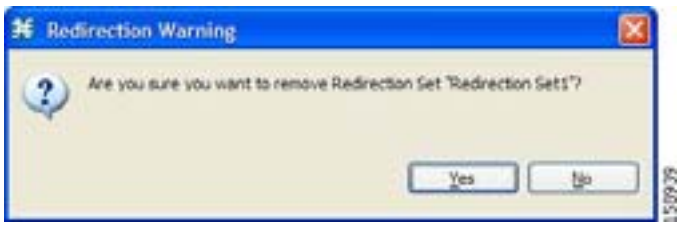
Redirection URL タブが開きます。

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　（**Delete**）をクリックします。

Redirection Warning メッセージが表示されます。

図 10-27



ステップ 5　**Yes** をクリックします。

リダイレクション セットが削除されます。

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。

リダイレクション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。

このオプションについて、次の表で説明します。

表 10-2　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		
Classification based on recent classification history enabled	TRUE	最新分類履歴は学習メカニズムであり、以前のトラフィック分類決定に従ってフローを分類するために使用します。 このメカニズムでは、Warez、Skype、Winny2 のフローの分類が改善されます。
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のみで一般的です。
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のみで一般的です。

表 10-2　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
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のみで一般的です。
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、DHCP です。
UDP destination port signatures	67: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、DHCP です。
UDP ports for which flow should be opened on first packet	5060, 5061, 67, 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、DHCP です。

表 10-2　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
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のみで一般的です。
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のみで一般的です。
L7 Filtered Traffic		
DHT filter enabled	TRUE	DHT フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。
Gnutella 2 Networking filter enabled	TRUE	Gnutella 2 Networking フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。
Gnutella filter enabled	TRUE	Gnutella フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。
L7 filtering enabled	TRUE	L7 Filtered Traffic 機能をイネーブルにするかどうかを指定します。 レイヤ 7 フィルタ処理されたフローは SCA プラットフォームに渡されないので、分類、制御、レポートのいずれも行われません。
Warez filter enabled	TRUE	Warez フローを、フローのレイヤ 7 特性に基づいて検出およびフィルタリングするかどうかを指定します。

表 10-2　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
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。
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 Service Control Engine (SCE) Software Configuration Guide*』の「Managing the SCMP」の章にある ISG 文書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

手順の詳細

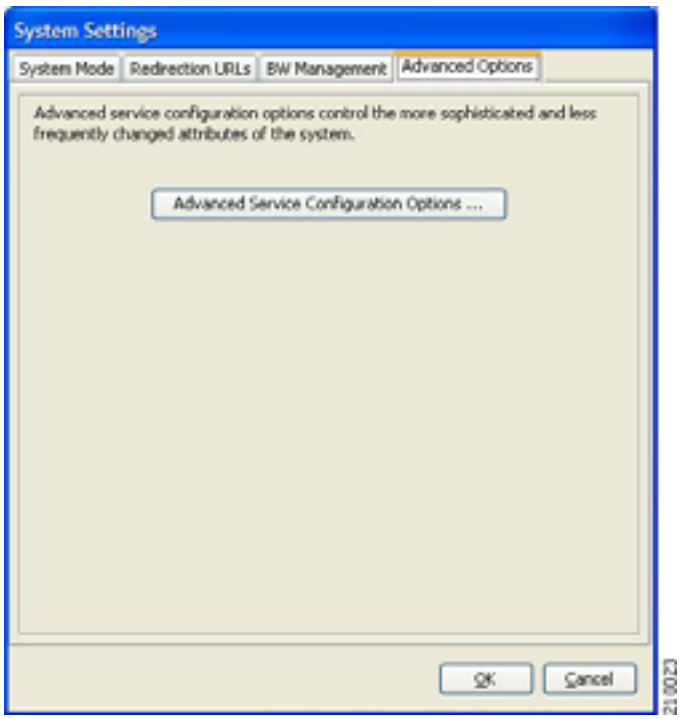
ステップ 1　Console メイン メニューから、**Configuration > System Settings** を選択します。

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。

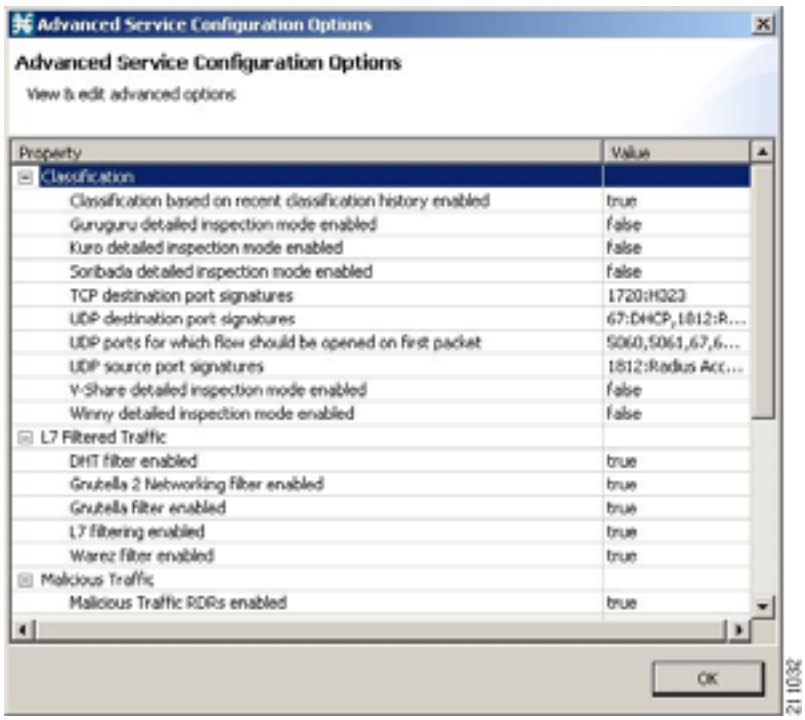
図 10-28



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 10-29



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。

VAS トラフィック フォワーディング設定の管理

Value Added Service（VAS）サーバへのトラフィック フォワーディングでは、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詳細トラフィック処理に外部エキスパート システム（VAS サーバ）を使用できます。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 トラフィック フォワーディングには次の制限があります。

- SCE 2000 4xGBE プラットフォームのみが 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 8 までの 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、64 までのテーブル パラメータを含めることができます。
- 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。

(注) VAS トラフィックフォワーディング機能は複雑なので、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 Service Control Engine (SCE) 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

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) 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。

VAS トラフィック フォワーディングの有効化

ステップ 1　Console メイン メニューから、**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 to VAS Servers** チェック ボックスをオンにします。

(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イネーブルのときに Enable Traffic Forwarding to VAS Servers チェックボックスをオンにしようとした場合は、VAS Error メッセージが表示されます。

OK をクリックし、ステップ 3 に進みます。

Package Settings ダイアログボックスの Advanced タブの VAS Traffic Forwarding Table ドロップダウン リストが有効になります（「高度なパッケージ オプションの設定」[p.9-7] を参照）。

ステップ 3　**Close** をクリックします。

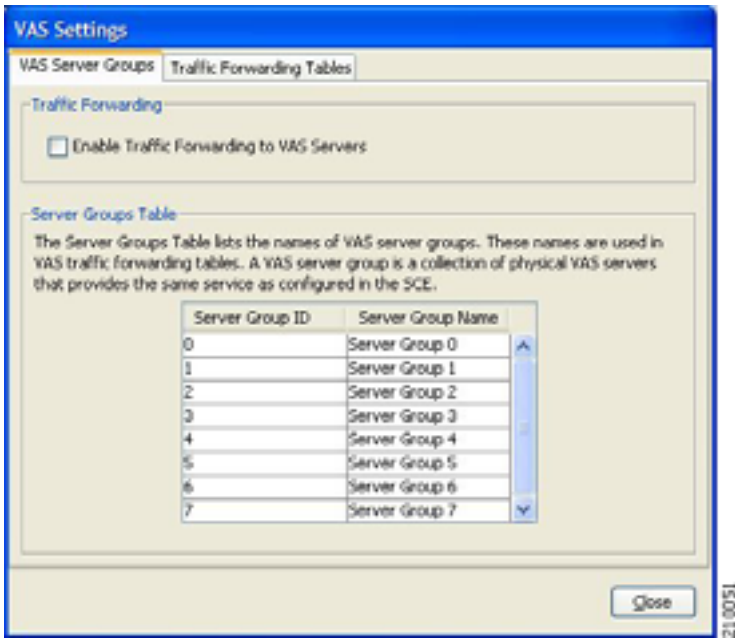
VAS Settings ダイアログボックスが閉じます。

VAS トラフィック フォワーディングの無効化

ステップ 1　Console メイン メニューから、**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 10-30



ステップ 2　**Enable Traffic Forwarding to VAS Servers** チェック ボックスをオフにします。

VAS トラフィック フォワーディングが無効になります。

ステップ 3　**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、8 までの VAS サーバ グループにフローを転送できます。デフォルトの場合、8 つのサーバ グループには、「Server Group n」（n は 0 ～ 7 の値）という名前が付きます。サーバ グループにわかりやすい名前を付けてください。付けた名前は、Package Settings ダイアログボックスの Advanced 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.9-7] を参照）、および各トラフィックフォワーディング テーブルに追加したテーブル 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.10-51] を参照）に表示されます。

ステップ 1　Console メイン メニューから、**Configuration > VAS Settings** を選択します。

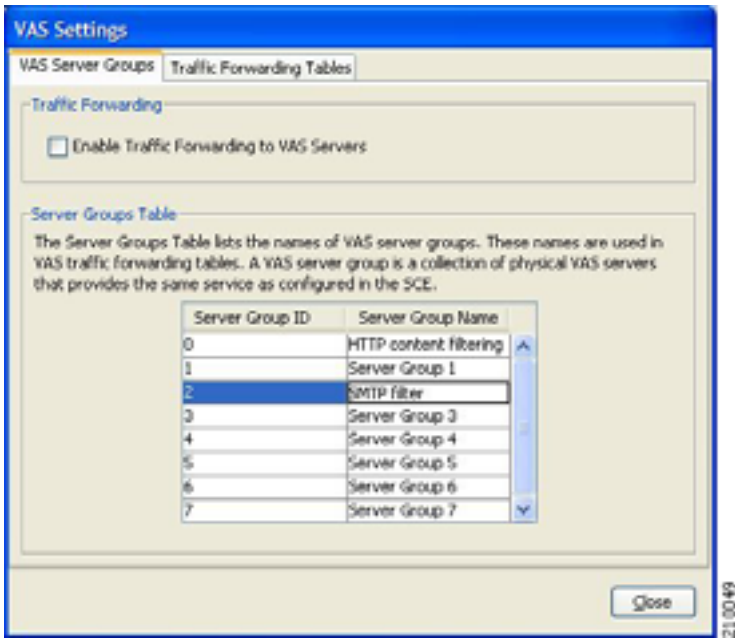
VAS Settings ダイアログボックスが表示されます。

ステップ 2　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　名前を変更するその他のサーバ グループに、ステップ 2 および 3 を繰り返します。

図 10-31



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　Console メイン メニューから、**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　**Traffic Forwarding Tables** タブをクリックします。

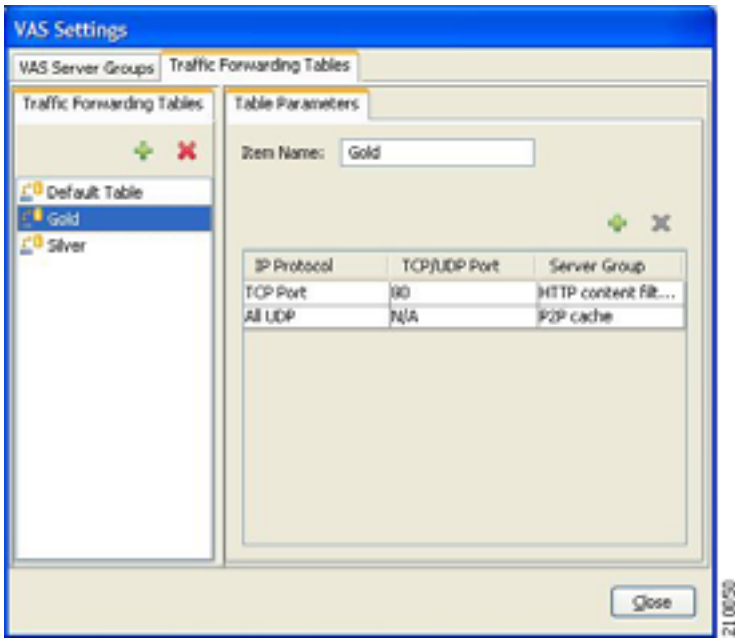
Traffic Forwarding Tables タブが開きます。

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 3　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 10-32



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　Console メイン メニューから、**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　**Traffic Forwarding Tables** タブをクリックします。

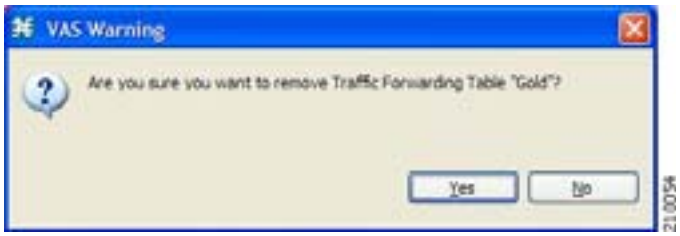
Traffic Forwarding Tables タブが開きます。

ステップ 3　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 4　（**Delete**）をクリックします。

VAS Warning メッセージが表示されます。

図 10-33



ステップ 5　**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 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 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　Console メイン メニューから、**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　**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 3　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 4　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.10-51] 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、64 までのテーブル 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

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　Console メイン メニューから、**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　**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 3　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 4　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、次のデフォルト値が含まれます。

IP プロトコル = TCP ポート
TCP/UDP ポート = 80
サーバ グループ = 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 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 テーブル パラメータの編集

ステップ 1　Console メイン メニューから、**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　**Traffic Forwarding Tables** タブをクリックします。

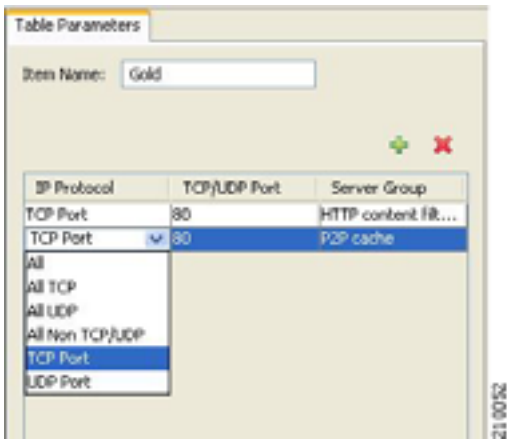
Traffic Forwarding Tables タブが開きます。

ステップ 3　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 4　Table Parameters タブのテーブルで次のように操作します。

1. 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 10-34

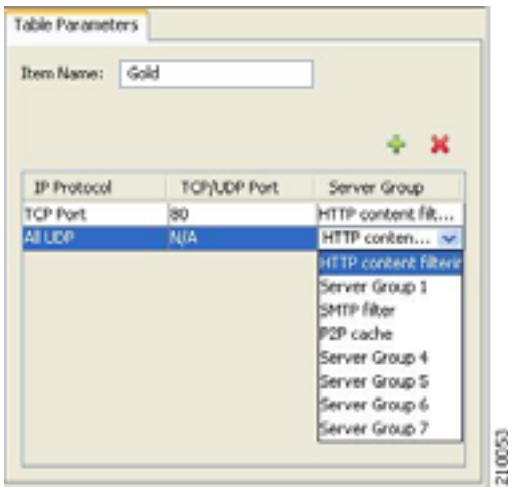


2. All、All TCP、All UDP、All Non TCP/UDP のうちいずれかを選択した場合は、テーブルの別のセルに移動したとき、TCP/UDP Port セルに「N/A」と表示されます。
3. TCP Port または UDP Port を選択した場合は、TCP/UDP Port カラムのセルをダブルクリックし、ポート番号を入力します。

（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。

4. 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 10-35



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 テーブル パラメータの削除

ステップ 1　Console メイン メニューから、**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　**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 3　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 4　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 5　（**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 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。

CHAPTER 11

Subscriber Manager の GUI ツールの使用方法

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 モードまたはアノニマス サブスクライバ モードで動作している場合は該当しません。

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、OSS 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。

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（p.11-2）
- 現在の SCMS-SM からの切断（p.11-5）

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しようとして、SCMS-SM で認証を実行します。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。

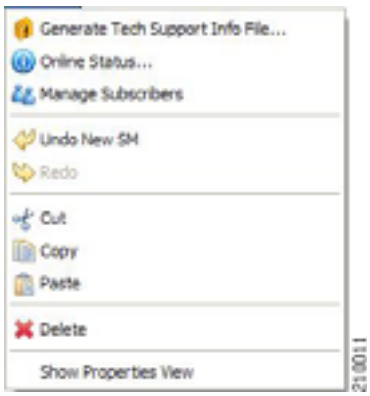
- Network Navigator から SCMS-SM への接続（p.11-2）
- Console から SCMS-SM への接続（p.11-4）

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



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

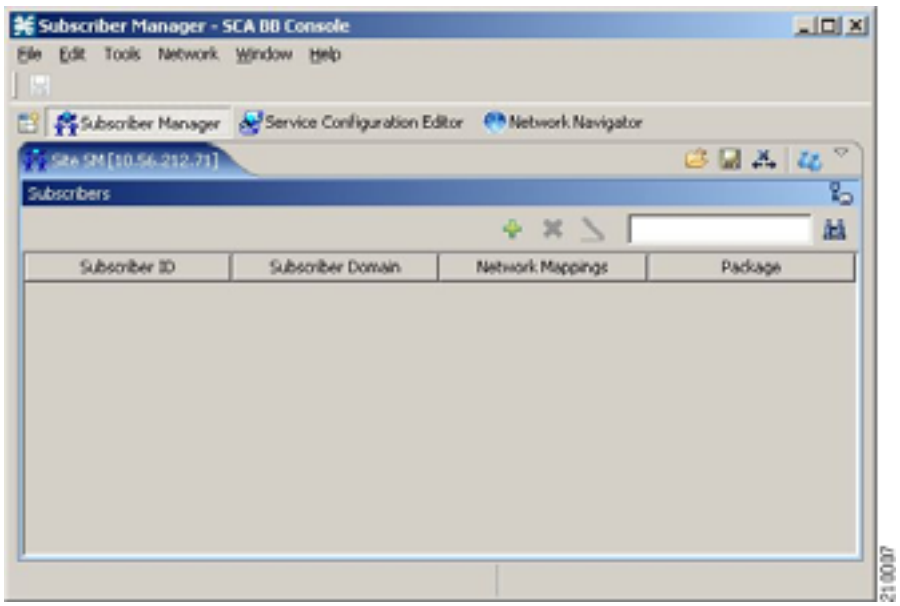
ステップ 4　**Connecting** をクリックします。

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**）、（**Disconnect from SM**）が有効になります。

図 11-2



Console から SCMS-SM への接続

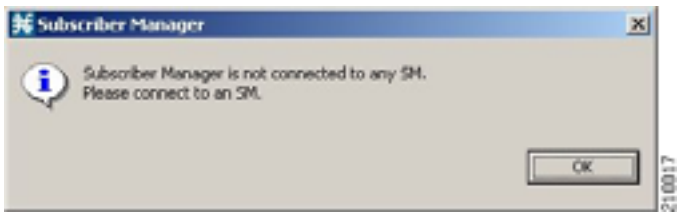
（注）（SM GUI ツールがすでに表示されている場合は、ステップ 3 から始めます。）

ステップ 1　Console のメイン メニューから、**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



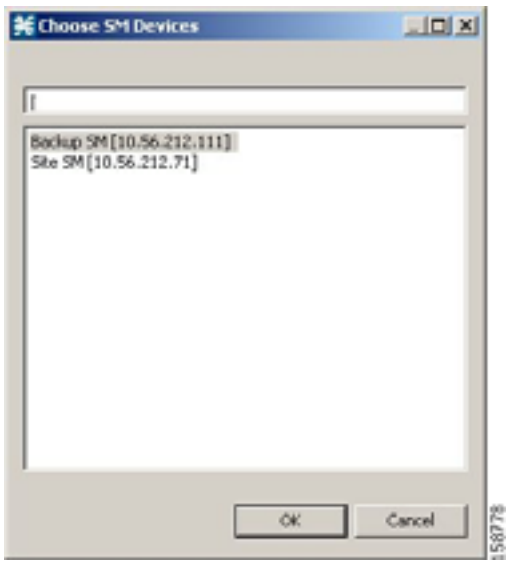
ステップ 2　**OK** をクリックします。

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



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

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

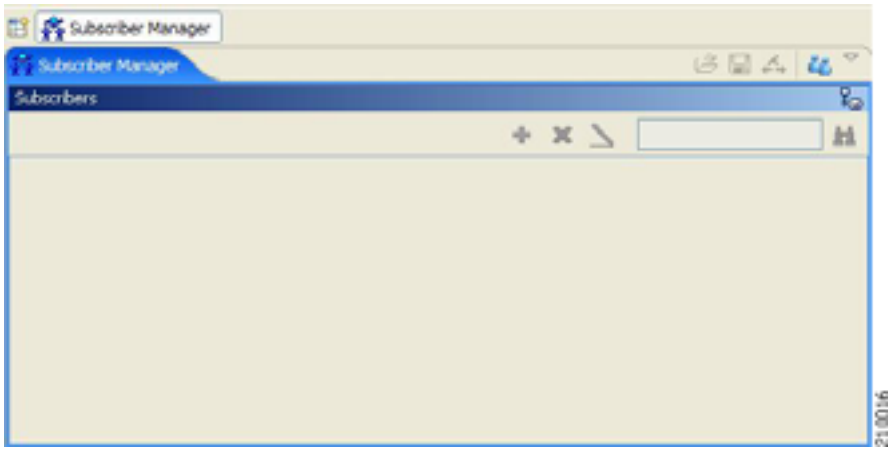
ステップ 1　SM GUI ツールバーで　（**Disconnect from SM**）をクリックします。

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



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 ファイルを使用した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。

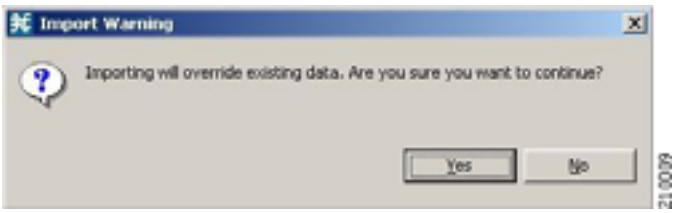
ステップ 1　SM GUI ツールバーの （**Import subscribers from CSV file**）をクリックします。

Import form 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



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.11-9] 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

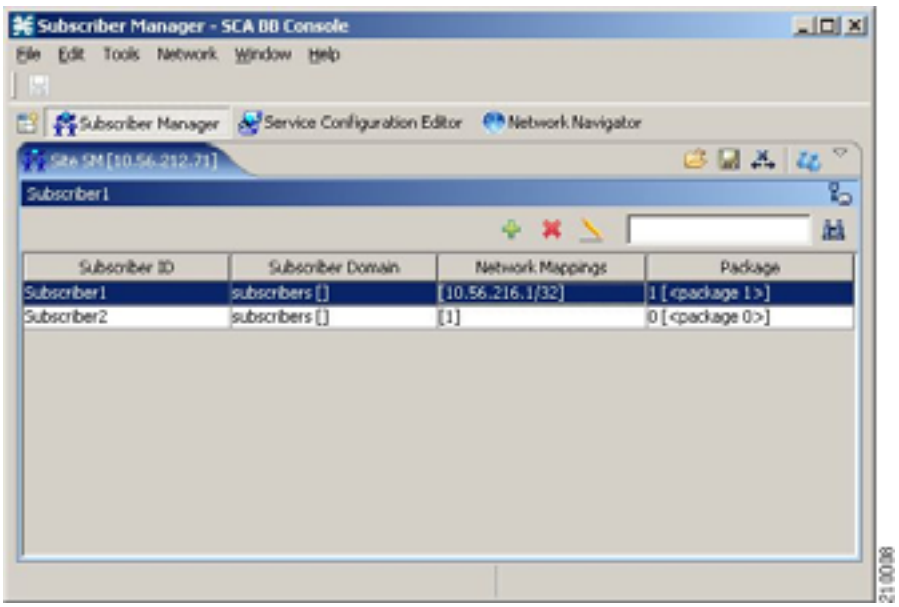
サブスクライバ情報

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。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.11-9] 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 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（仮想 LAN）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



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 — 複数のサブスクライバからなるサブスクライバ範囲を選択します。

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.11-12] を参照）。

ステップ 1　照合するプレフィックスを検索フィールド（下の図を参照）に入力します。

図 11-8

ステップ 2　（**Find Subscribers**）をクリックします。

指定したプレフィックスと一致するサブスクライバのみが、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

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。

多くのサブスクライバを追加するには、RADIUS（または DHCP）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.11-6] 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

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。詳細については、「Managing Real-Time Subscriber Usage RDRs」を参照してください。

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

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。

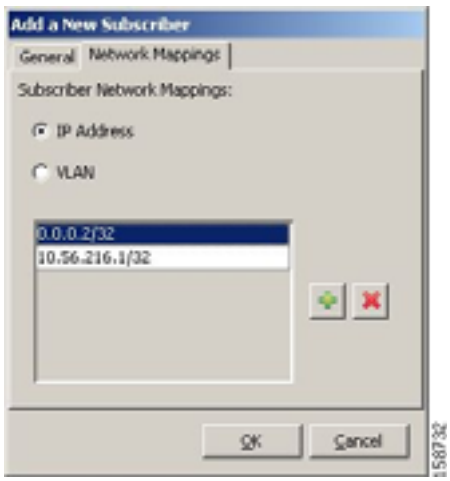
- IP Address
- VLAN

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。

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



ステップ 10　その他のネットワーク マッピングにステップ 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サブスクライバ グループのパラメータを編集できます。

- 単一サブスクライバの編集（p.11-12）
- サブスクライバ グループの詳細編集（p.11-14）

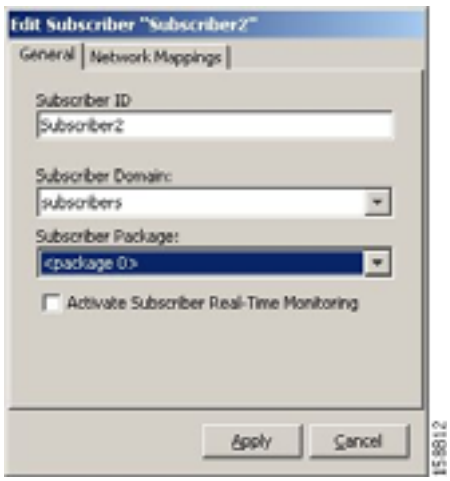
単一サブスクライバの編集

ステップ 1　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」[p.11-9] 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



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。

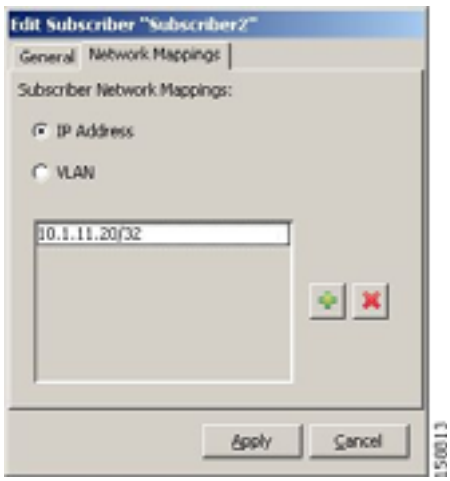
  リストの内容は、選択したサブスクライバ ドメインによって決まります。
- **Activate Subscriber Real-time Monitoring** チェック ボックスをオンまたはオフにします。

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



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.11-9] 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

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。

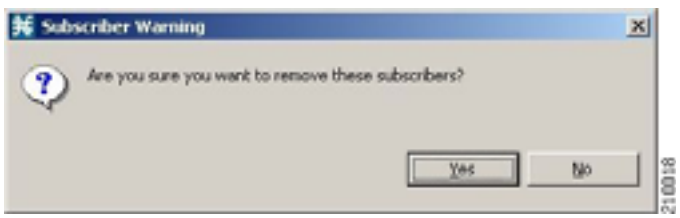
データベースからのサブスクライバの削除

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.11-9] 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



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は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

このモジュールでは、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、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、Cisco Service Control Application for Broadband（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。

DSS ファイルの管理についての情報

- アクティブなサービス　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方法については、「プロトコル パックのインストール方法」（p.4-13）で説明します。
- 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.7-39）で説明します。
- サーバ設定ユーティリティ　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 Service Configuration Utility についての情報」（p.13-2）で説明します。

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についての情報（p.12-2）

DSS ファイルのコンポーネントについての情報

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。

次のセクションでは 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（p.12-2）
- DSS プロトコル リスト（p.12-3）
- DSS プロトコルについての情報（p.12-3）
- DSS シグニチャについての情報（p.12-4）
- DSS 詳細検査句（p.12-9）
- DSS 詳細検査条件（p.12-9）

DSS ファイル

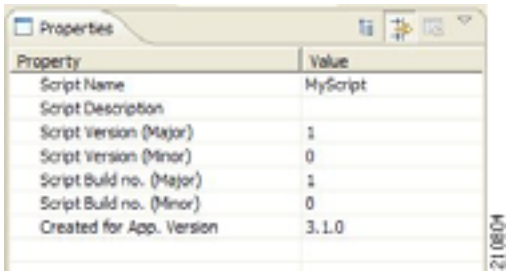
DSS ファイル名は、DSS ファイルのコンポーネント ツリーのルート ノードです。

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。

次の図は、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

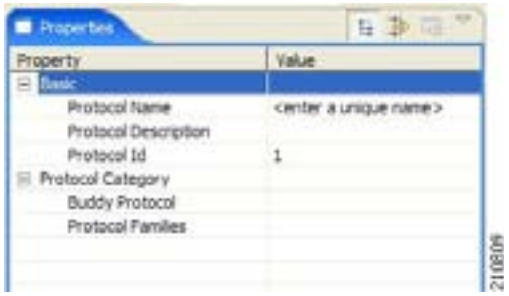
DSS ファイルのコンポーネント ツリーからプロトコル ノードを選択すると、プロトコルの次のプロパティを定義できるようになります。

- Basic
  - Protocol Name ― 「プロトコル名および ID の設定」（p.12-4）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.12-4）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。

次の図は、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.7-22] 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.7-22] 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 シグニチャについての情報

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
- HTTP 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。

次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かぞえた、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。このフィールドには、
  - ― 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、0 ～ 65535 の全ポート範囲です。
  - ― 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。
  - ― 非対称ルーティング分類モード ― 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。

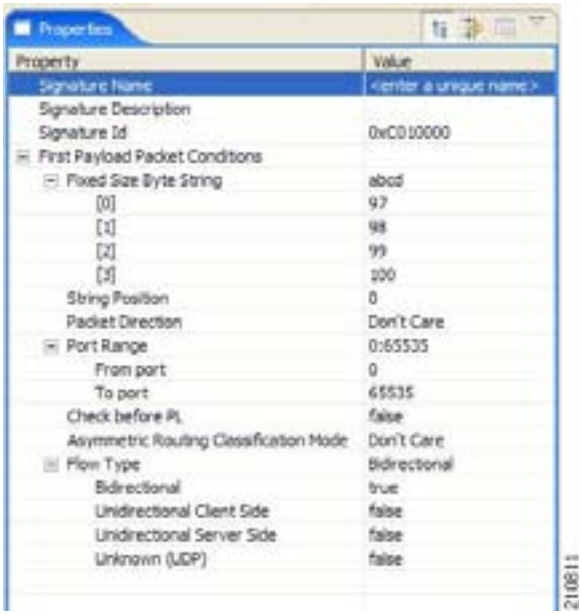
  フロー タイプは次の 4 つのフィールドで指定されます。
  - ― Bidirectional ― 値 **true** と **false** を切り替えます。
  - ― Unidirectional Client Side ― 値 **true** と **false** を切り替えます。クライアント側からのパケットのみ検出された TCP フローに適用されます。
  - ― Unidirectional Server Side ― 値 **true** と **false** を切り替えます。サーバ側からのパケットのみ検出された TCP フローに適用されます。

— Unknown（UDP）— 値 **true** と **false** を切り替えます。一方向からのパケットのみ検出された UDP フローに適用されます。

シグニチャが先頭ペイロード パケットのみ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後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。

次の図は、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。このフィールドには、
  - 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、0 ～ 65535 の全ポート範囲です。
  - 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。

- 非対称ルーティング分類モード ― 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。

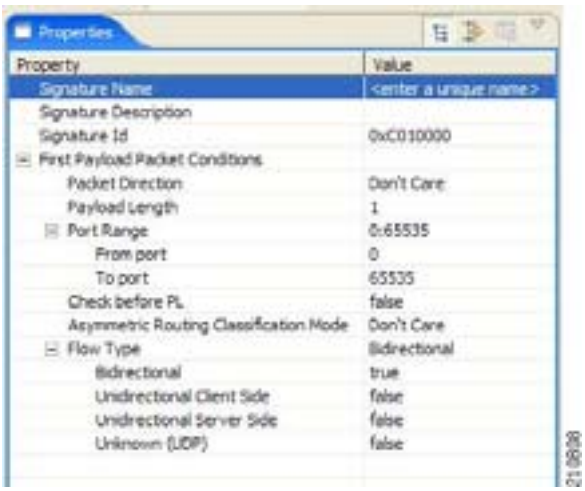
フロー タイプは次の 4 つのフィールドで指定されます。

- 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のみ検出された 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のみ検出された 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のみ検出された UDP フローに適用されます。

シグニチャが先頭ペイロード パケットのみ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。

次の図は、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）。

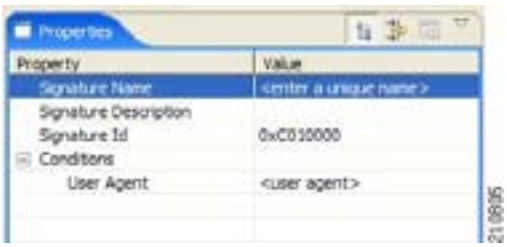
DSS HTTP ユーザ エージェント シグニチャ

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 ヘッダーのユーザ エージェント フィールドの値

次の図は、HTTP ユーザ エージェント 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 12-5



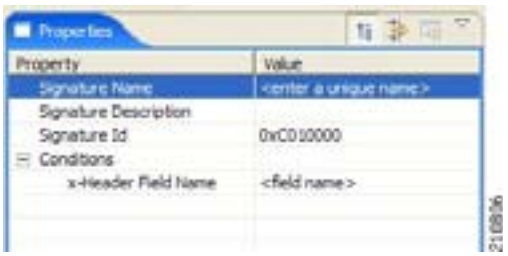
DSS HTTP x ヘッダー シグニチャ

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

次の図は、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 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。

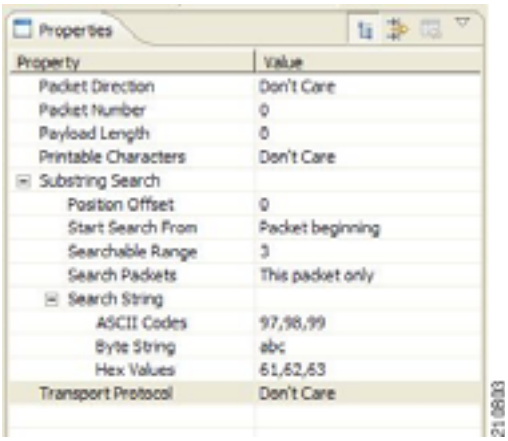
DSS ファイルのコンポーネント ツリーから詳細検査条件ノードを選択すると、詳細検査条件の次のプロパティを定義できるようになります。

- Packet Direction ― ペイロードを含むフローの先頭パケットの開始側。このフィールドには、From Server、From Client、Don't Care（両側）の 3 つのうちいずれかの値になります。
- 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のみが含まれるかどうかをテストします。このフィールドには、Printable Characters Only、At Least One Non-Printable、Don’t Care の 3 つのうちいずれかの値を含めることができます。
- 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）

次の図は、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。

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。

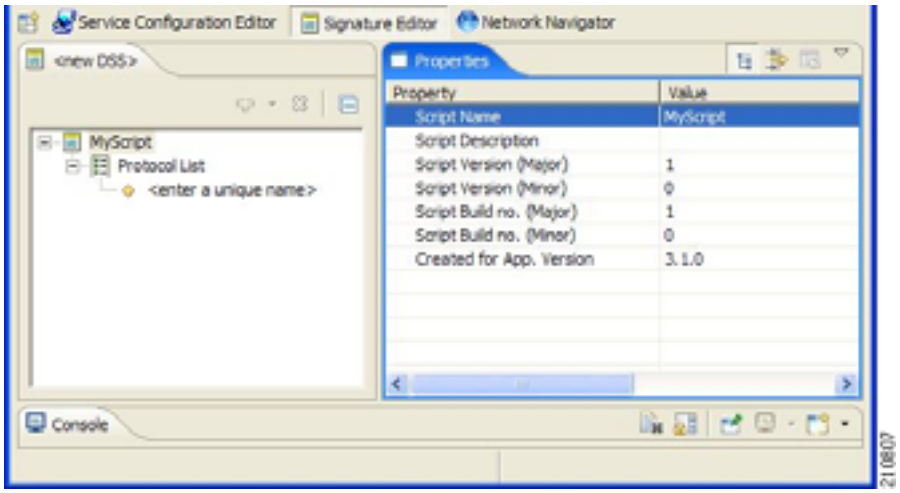
DSS ファイルの作成

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 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



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。

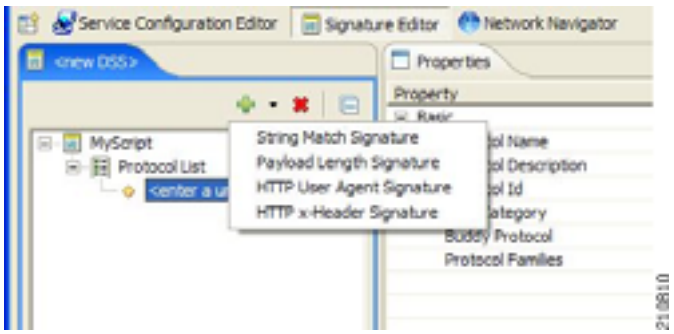
プロトコル プロパティが Properties ビューに表示されます。

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

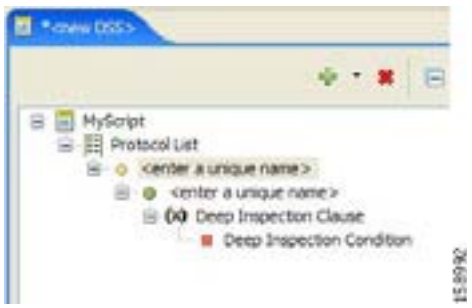


ステップ 6　表示されるドロップダウン メニューからシグニチャ タイプを選択します。

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



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 シグニチャについての情報」（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、次のように操作します。

a. Deep Inspection Condition ノードをクリックします。

詳細検査条件プロパティが Properties ビューに表示されます。

b. 詳細検査条件プロパティを編集します。

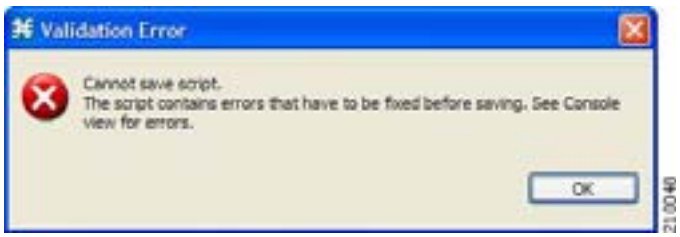
プロパティの説明については、「DSS 詳細検査条件」（p.12-9）を参照してください。

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



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。

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についての情報」（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。
  — **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。
  — 新しい DSS ファイルを保存するフォルダを選択します。
  — 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。
  — **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。

シグニチャのインポート

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 メニューから、**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。

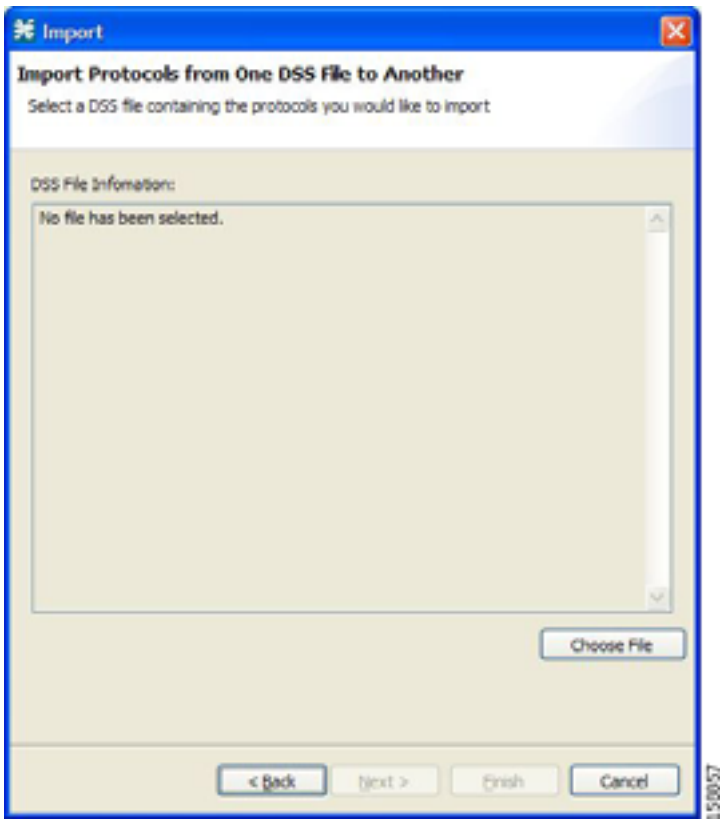
図 12-12

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



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。

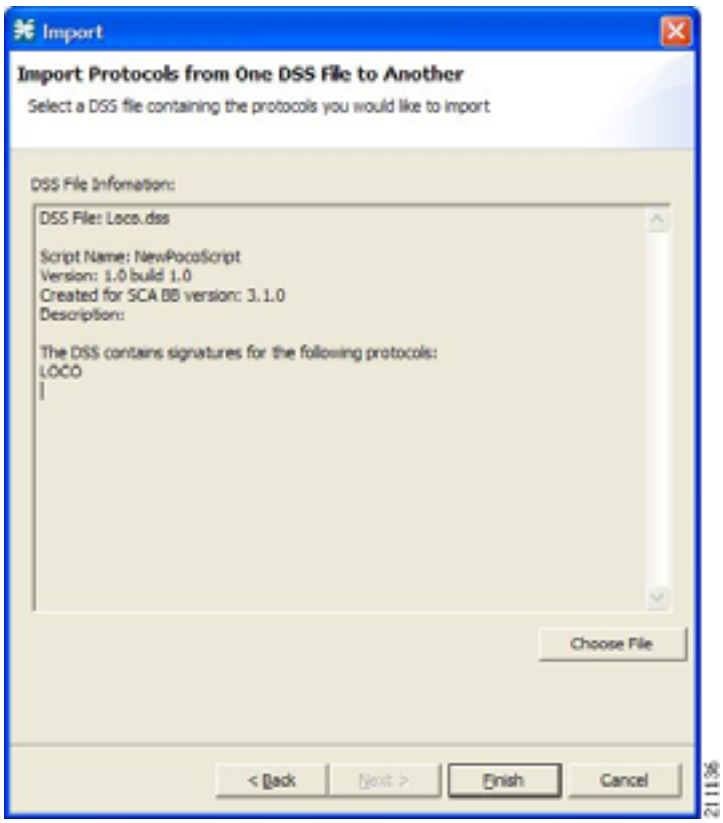
ステップ 5　インポートする DSS ファイルを選択します。

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



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

SCA BB Service Configuration Utility についての情報

Cisco Service Control Application for Broadband（SCA BB）の Service Configuration Utility（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。

Service Configuration Utility 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」（p.4-8）を参照してください。

SCA BB Service Configuration Utility の使用方法

SCA BB Service Configuration Utility のコマンドライン構文は次のとおりです。

```
servconf <operation>[<option>] [<option>] ...
```

次の表に、**servconf** の処理およびオプションを示します。

表 13-1　servconf 処理

処理	省略形（適用可能な場合）	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 処理のみに必要）。
*--**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。

SCA BB Service Configuration Utility 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 モニタ設定ユーティリティ

ネットワーク管理者は、MRTG などの SNMP 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 モニタ設定ユーティリティ（**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 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」（p.4-8）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。

SCA BB リアルタイム モニタ設定ユーティリティの使用法

SCA BB リアルタイム モニタ設定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>
```

rtmcmd のオプションについて、次の表で説明します。

表 13-7　rtmcmd のオプション

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。

表 13-7　rtmcmd のオプション（続き）

オプション	省略形	説明
--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***	「ユーザ コンフィギュレーション ファイル」（p.13-6）を指定します。

次の構文を使用してその他の処理を呼び出し、**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。

SCA BB リアルタイム モニタ設定ユーティリティの例

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
```

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。

次の表では、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 パラメータについて説明します。

表 13-9　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	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には（Windows のディレクトリ名など）、「\\」のようにバックスラッシュを 2 つ続けて入力します（またはスラッシュ「/」を使用）。
- 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 ユーティリティについての情報

SCA BB シグニチャ設定ユーティリティ（**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」（p.4-8）を参照してください。

SCA BB シグニチャ設定ユーティリティの使用方法

SCA BB シグニチャ設定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>]
```

次の表に、**sigconf** の処理および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 ファイルを指定します。

SCA BB シグニチャ設定ユーティリティの例

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、およびトラップについての情報：概要

シスコは、完全なネットワーク FCAPS 管理（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）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。

- CLI（コマンドライン インターフェイス）― 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。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）― 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 MIB（management information base; 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 Service Control Engine (SCE) Software Configuration Guide*』の「Configuring the Management Interface and Security」の章を参照してください。

MIB

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。

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 Service Control Engine (SCE) Software Configuration Guide*』の「Configuring the Management Interface and Security」の章にある「SNMP Configuration and Management」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 CLI（コマンドライン インターフェイス）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　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　SCE プラットフォームの CLI プロンプト（SCE#）に configure と入力します。

ステップ 3　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 4　interface linecard 0 と入力します。

ステップ 5　Enter キーを押します。

SCE(config if)# プロンプトが表示されます。

ステップ 6　pqi install file engXXXXX.pqi と入力します。

ステップ 7　インストールが完了するまで進行状況をモニタします。

PQI ファイルがインストールされます。

（注）　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。第 5 章「Network Navigator の使用」を参照してください。

SM デバイスでの SCA BB PQI ファイルのインストール

Cisco Service Control Management Suite（SCMS）Subscriber Manager（SM）では、SM CLU を使用して SCA BB PQI ファイルをインストールできます。

ステップ 1　適切な PQI ファイルを FTP で SM にアップロードします。

ステップ 2　SM への Telnet セッションを開きます。

ステップ 3　SM の bin ディレクトリに移動し、p3inst --install --file=sm_engXXXXX.pqi と入力します。

ステップ 4　Enter キーを押します。

ステップ 5　インストールが完了するまで進行状況をモニタします。

PQI ファイルがインストールされます。

（注）　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。第 5 章「Network Navigator の使用」を参照してください。

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

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（「サブスクライバおよびサブスクライバ モードについて」[p.2-3] を参照）。

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、32 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 CLI（コマンドライン インターフェイス）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 Service Control Engine (SCE) CLI Command Reference*』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、`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、`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>]`

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。

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 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

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。

- サブスクライバ「Smith」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.13-13）
- サブスクライバ「Smith」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.13-14）
- サブスクライバ グループ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）
- サブスクライバ「Smith」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の表示（p.13-14）

サブスクライバ「Smith」に対するサブスクライバ モニタリングのイネーブル化

ステップ 1　コマンド ラインから以下を実行します。

sm/server/bin/p3subs --set --subscriber Smith --property monitor=1

サブスクライバ「Smith」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

ステップ 1　コマンド ラインから以下を実行します。

sm/server/bin/p3subs --set --subscriber Smith --property monitor=0

サブスクライバ グループに対するサブスクライバ モニタリングのイネーブル化

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 ラインから以下を実行します。

sm/server/bin/p3batch -f monitor.txt

サブスクライバ「Smith」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の表示

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 ラインから以下を実行します。

sm/server/bin/p3subs --show-property --subscriber Smith --property monitor

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 Service Control Engine (SCE) CLI Command Reference*』を参照してください。

次の例では、プロンプトの変化を示すためにプロンプトも記載してあります。実際にサブスクライバ コマンドを起動するには、`SCE(config if)#` プロンプトを表示する必要があります。

- サブスクライバ「Smith」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）
- サブスクライバ「Smith」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.13-14）
- サブスクライバ グループ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）
- サブスクライバ「Smith」に対するサブスクライバ　モニタリングがイネーブルかどうかの表示（p.13-15）

サブスクライバ「Smith」に対するサブスクライバ モニタリングのイネーブル化

ステップ 1　コマンド ラインから以下を実行します。

```
SCE# configure
SCE(config)# interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 1
```

サブスクライバ「Smith」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

ステップ 1　コマンド ラインから以下を実行します。

```
SCE# configure
SCE(config)# interface LineCard 0
SCE(config if)# subscriber name Smith property monitor value 0
```

サブスクライバ グループに対するサブスクライバ モニタリングのイネーブル化

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 monitor value 1
subscriber name George property monitor value 1
subscriber name Elaine property monitor value 1
subscriber name Kramer property monitor value 1
subscriber name Newman property monitor value 1
```

ステップ 2　コマンド ラインから以下を実行します。

```
SCE# script run monitor.txt
```

サブスクライバ「Smith」に対するサブスクライバ モニタリングがイネーブルかどうかの表示

ステップ 1　コマンド ラインから以下を実行します。

```
SCE# show interface LineCard 0 subscriber name Smith properties
```

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 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 ツールの使用（p.11-2）
- SCE プラットフォーム サブスクライバ CLI（p.13-16）
- SM CLU を使用したサブスクライバの管理（p.13-17）
- SCE プラットフォーム サブスクライバ CLI（p.13-16）
- SM CLU を使用したサブスクライバの管理（p.13-17）

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、`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、`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 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 CLU を使用したサブスクライバの管理

サブスクライバを管理するには、**p3subs** SM ユーティリティを使用します。サブスクライバを追加または削除できます。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。

ステップ 1　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。Solaris シェル プロンプトで入力するコマンドは、次のような一般的なフォーマットを使用します。

```
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。

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。

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、次の一般的なフォーマットを使用してコマンドを入力します。

p3subsdb --import *filename*

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、次の一般的なフォーマットを使用してコマンドを入力します。

p3subsdb --export *filename*

フィルタリング オプションを含むサブスクライバを指定 CSV ファイルにエクスポートするには、次のコマンドを入力します。

```
p3subsdb --export --prefix=a --output=silverSubscriberFile.csv
```