CISCO SYSTEMS

Cisco Content Services Switch セキュリティ コンフィギュレーション ガイド

Software Version 8.20
November 2006

Text Part Number: OL-8242-02-J

CONTENTS

はじめに

このマニュアルでは、Cisco 11500 シリーズの Content Services Switch（CSS; コンテント サービス スイッチ）の高度な機能の設定方法について説明します。このマニュアルの記載情報は、特に指示がない限り、CSS の全モデルに共通です。

CSS ソフトウェアには、標準機能セットまたはオプションの拡張機能セットが用意されています。プロキシミティ データベースおよびセキュア管理はオプションの機能です。セキュア管理には、Device Management ソフトウェア用の Secure Shell Host （SSH）および強度の高い Secure Socket Layer （SSL）暗号化の機能が含まれます。

ここでの主な内容は次のとおりです。

対象読者

このマニュアルは、次のような、十分な経験とスキルを持つ CSS の設定担当者を対象としています。

- Web マスター
- システム管理者
- システム オペレータ

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	内容
第 1 章「CSS のアクセス制御」	ユーザおよびネットワーク トラフィックのアクセスなど、CSS へのアクセスを制御します。
第 2 章「SSHD プロトコルの設定」	Secure Shell Daemon (SSHD) プロトコルを設定して、保護されていないネットワーク経由で通信する 2 つのホスト間で、通信内容を暗号化して保護します。
第 3 章「RADIUS サーバのクライアントとしての CSS の設定」	Remote Authentication Dial-In User Service (RADIUS) プロトコルを、クライアントとして CSS に設定します。
第 4 章「TACACS+ サーバのクライアントとしての CSS の設定」	Terminal Access Controller Access Control System (TACACS+) プロトコルを、クライアントとして CSS に設定します。
第 5 章「ファイアウォール ロード バランシングの設定」	セキュリティ強化のために、CSS 間にファイアウォール ロード バランシングを設定します。

関連資料

Content Services Switch マニュアルには、このマニュアルの他に次のものがあります。

マニュアル名	内容
Release Note for the Cisco 11500 Series Content Services Switch	Cisco CSS 11500 シリーズに関する運用上の考慮事項、注意事項、および Command Line Interface（CLI; コマンドライン インターフェイス）コマンドについて説明しています。
Cisco 11500 Series Content Services Switch Hardware Installation Guide	Cisco CSS 11500 シリーズの設置、ケーブル接続、および電源投入について説明しています。また、CSS の仕様、ケーブルのピン配置、ハードウェアのトラブルシューティングについても説明しています。
Cisco Content Services Switch Getting Started Guide	次のような CSS の初期管理作業と設定作業について説明しています。 • CSS の初回ブートと通常ブート、および CSS へのログイン • ユーザ名とパスワード、イーサネット管理ポート、スタティック IP ルート、および日付と時刻の設定 • ホスト名解決を行う DNS サーバの設定 • スティッキ クッキーの設定（スティッキの概要説明と、クッキーによる高度なロード バランシング方式） • CSS の設定に使用するブラウザ ベースのユーザ インターフェイス CSS Cisco View Device Manager (CVDM) のインストール • 作業リストと CSS のマニュアルでの説明箇所 • ブート プロセスのトラブルシューティング

マニュアル名	内容
Cisco Content Services Switch Administration Guide	CSS ソフトウェアのアップグレードや次に示す項目の設定など、CSS での管理作業の実行方法について説明しています。 • ログ メッセージの表示と sys.log メッセージの意味などのログ機能 • ユーザ プロファイルおよび CSS パラメータ • SNMP • RMON • XML 文書による CSS の設定 • CSS スクリプト言語 • **Offline Diagnostic Monitor (Offline DM)** メニュー
Cisco Content Services Switch Routing and Bridging Configuration Guide	次に示す項目の設定など、CSS のルーティングおよびブリッジングの設定作業について説明しています。 • 管理用のポート、インターフェイス、および回線 • スパニングツリー ブリッジ • Address Resolution Protocol（ARP; アドレス解決プロトコル） • Routing Information Protocol（RIP; ルーティング情報プロトコル） • Internet Protocol（IP; インターネット プロトコル） • Open Shortest Path First (OSPF) プロトコル • Cisco Discovery Protocol （CDP; シスコ検出プロトコル） • Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）リレー エージェント

マニュアル名	内容
Cisco Content Services Switch Content Load-Balancing Configuration Guide	次に示す項目の設定など、CSS のコンテンツ ロード バランシングの設定作業について説明しています。 • フロー マッピングおよびポート マッピング • サービス • サービス、グローバル、スクリプト キープアライブ • ソース グループ • サービスの負荷 • Server/Application State Protocol（SASP） • Dynamic Feedback Protocol（DFP） • 所有者 • コンテンツ ルール • スティッキ パラメータ • HTTP ヘッダー ロード バランシング • コンテンツ キャッシング • コンテンツ レプリケーション
Cisco Content Services Switch Global Server Load-Balancing Configuration Guide	次に示す項目の設定など、CSS のグローバル ロード バランシングの設定作業について説明しています。 • Domain Name Service（DNS; ドメイン ネーム サービス） • DNS スティッキ • コンテンツ ルーティング エージェント • クライアント側アクセラレータ • ネットワーク プロキシミティ

マニュアル名	内容
Cisco Content Services Switch Redundancy Configuration Guide	次に示す項目の設定など、CSS の冗長化設定作業について説明しています。 • VIP および仮想インターフェイスの冗長性 • 適応型セッションの冗長性 • ボックスツーボックス冗長性
Cisco Content Services Switch SSL Configuration Guide	次に示す項目の設定など、CSS の SSL 設定作業について説明しています。 • SSL 証明書およびキー • SSL 終了 • バックエンド SSL • SSL 開始 • HTTP データ圧縮
Cisco Content Services Switch Command Reference	すべての CLI コマンドをアルファベット順に示し、シンタックス、オプションおよび関連コマンドも含めて説明しています。

記号と表記法

このマニュアルでは、次の記号と表記法を使用して、記載情報の種類を示しています。

注意 注意が必要であることを示します。装置の故障またはデータの損失につながることがあるので、慎重に作業してください。

警告 **危険を表します。作業者が負傷したり、装置が故障する危険があるので、慎重に作業してください。**

（注） 注釈です。重要な関連情報や、注意事項、推奨事項を示します。

文章中のコマンドは、**太字**で表します。

CLI プロンプトも含めてコマンドラインに表示される文字は、`courier` フォントで表します。

コマンドラインに入力するコマンドや文字は、**太字**の **`courier`** フォントで表します。

新しい用語、マニュアル名、強調する内容、およびユーザが値を設定する変数は、*イタリック体*で表します。

1. 番号付き項目のリストは、その順序に意味があることを表します。
   a. アルファベット順の 2 次項目のリストは、その順序に意味があることを表します。
- ドット付きのトピックのリストは、その順序に意味がないことを表します。
  - 字下げされたサブトピックのリストは、その順序に意味がないことを表します。

技術情報の入手方法

ここでは、シスコが提供する製品マニュアルのリソースについて説明します。

Web サイト

日本語のマニュアルは、次の Web サイトから入手できます。

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

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの 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

各国のシスコ 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/public/countries_languages.shtml

Product Documentation DVD （英語版）

Product Documentation DVD は、ポータブルなメディアに収録された、テクニカル マニュアルのライブラリです。この DVD では、シスコのハードウェア製品およびソフトウェア製品のインストレーション ガイド、コンフィギュレーション ガイド、およびコマンド ガイドを利用できます。また、シスコの次の URL の Web サイトに掲載されている HTML 形式のマニュアルや一部の PDF ファイルを利用できます。

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

Product Documentation DVD は定期的に作成、公開されます。この DVD は、単体でも定期購読でもご利用いただけます。Cisco.com の登録ユーザの場合、次の URL の Cisco Marketplace の Product Documentation Store から Product Documentation DVD (Part Number DOC-DOCDVD= または DOC-DOCDVD=SUB) を発注できます。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法（英語版）

Cisco Marketplace をご利用いただくには、Cisco.com にご登録いただく必要があります。登録されている場合、次の URL の Product Documentation Store でシスコの英文マニュアルを発注できます。

http://www.cisco.com/go/marketplace/docstore

ユーザ ID とパスワードをお持ちでない場合は、次の URL でご登録いただけます。

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

シスコ製品のセキュリティの概要

シスコでは、無料のオンライン Security Vulnerability Policy（セキュリティの脆弱性のポリシー）ポータル サイトを次の URL で提供しています。

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

シスコ製品のセキュリティ上の問題の報告

シスコは、信頼性の高い製品をお届けするように最大限の努力を払っています。製品のリリース前には内部で製品をテストし、すべての脆弱性をすばやく解決するように努めています。シスコ製品に脆弱性があると考えられる場合には、製品をお買い上げの弊社販売代理店にお問い合せください。

テクニカル サポート

テクニカル サポートについては、製品をお買い上げの弊社販売代理店にお問い合せください。

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

その他の資料および情報の入手方法

シスコの製品、テクノロジー、ネットワーク ソリューションに関する情報は、各種のオンライン情報や印刷物から入手できます。

- Cisco Online Subscription Center Web サイトでは、電子メールによるシスコのさまざまなニュースレターやその他のお知らせの購読を申し込むことができます。このページでプロファイルを作成し、受信したいサービスの購読を選択します。Cisco Online Subscription Center には、次の URL からアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 『*Cisco Product Quick Reference Guide*』は、販売代理店で取り扱われているシスコ製品について、製品の概要と特徴、サンプルの製品番号、および技術仕様の要約などが掲載されている、コンパクトなリファレンス ツールです。このガイドは年に 2 度改定され、シスコ販売代理店が提供する最新の製品が掲載されています。『*Cisco Product Quick Reference Guide*』の発注、および詳細については、次の URL の Web ページを参照してください。

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

- Cisco Marketplace では、さまざなシスコの本、リファレンス ガイド、マニュアルおよびロゴ入り商品を提供しています。シスコ直営の Cisco Marketplace には、次の URL からアクセスしてください。

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

- Cisco Press では、ネットワーク、トレーニング、および資格関連の出版物を幅広く発行しています。初心者から上級者まで役立つ、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL でアクセスできます。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、およびカスタマー サポート サービスには、次の URL からアクセスしてください。

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

- Networking Professionals Connection は、ネットワークのプロがネットワーク製品およびテクノロジーに関する質問や提案、および情報をシスコの専門技術者および他のネットワークのプロと交換する Web サイトです。意見交換には、次の URL から参加できます。

  http://www.cisco.com/discuss/networking

- 『What's New in Cisco Documentation』は、シスコ製品のマニュアルについての最新情報を提供するオンライン ドキュメントです。このオンライン ドキュメントの情報は、製品カテゴリ別に分類されており、ご使用の製品のマニュアルをすばやく探すことができます。『What's New in Cisco Documentation』は毎月更新されます。最新版の『What's New in Cisco Documentation』には、次の URL からアクセスしてください。

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。日本におけるトレーニングに関する情報は次の URL からアクセスできます。

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

CHAPTER 1

CSS のアクセス制御

この章では、ネットワーク トラフィックなどの CSS へのアクセスの設定方法を説明します。この章の記載情報は、特に指示がない限り、CSS の全モデルに共通です。

この章の主な内容は次のとおりです。

- 管理者のユーザ名とパスワードの変更
- ユーザ名とパスワードの作成
- CSS へのリモート アクセスの制御
- CSS への管理アクセスの制御
- アクセス コントロール リストによる CSS ネットワーク トラフィックの制御
- ACL へのネットワーク修飾子リストの設定

管理者のユーザ名とパスワードの変更

CSS に初めてログインするときは、デフォルトのユーザ名 **admin** とデフォルトのパスワード **system** を小文字で入力します。セキュリティを確保するため、管理者のユーザ名とパスワードは変更する必要があります。出荷時には、すべての CSS で管理者のユーザ名とパスワードが同一に設定されているため、CSS のセキュリティが損なわれる可能性があります。

管理者のユーザ名とパスワードは、nonvolatile random access memory（NVRAM; 不揮発性 RAM）に保持されています。CSS を再度ブートするたびに、ユーザ名とパスワードが NVRAM から読み取られ、ユーザ データベースに書き込まれます。管理者のユーザ名には、デフォルトで SuperUser ステータスが割り当てられています。

管理者のユーザ名とパスワードは変更できますが、これらの値は NVRAM 内に保持されているため、完全に削除することはできません。管理者のユーザ名を **no username** コマンドで削除すると、そのユーザ名は running-config ファイルから削除されますが、再度ブートすると NVRAM から復元されます。

管理者のユーザ名とパスワードを変更するには、**username-offdm** *name* **password** *text* コマンドを使用します。

（注） ブート時に **Offline DM** メニューの **Security Options** メニューを使用して、管理者のユーザ名とパスワードを変更することもできます。**Offline DM** メニューの詳細については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

たとえば、デフォルトの管理者のユーザ名とパスワードを変更するには、次のように入力します。

```
(config)# username-offdm bobo password secret
```

ユーザ名とパスワードの作成

CSS にログインするには、ユーザ名とパスワードが必要です。CSS は、管理者や技術者用のユーザ名を含め、最大で 32 個のユーザ名をサポートします。各ユーザには、SuperUser か User のステータスを割り当てることができます。

- **User** ：一部のコマンド群を使用して CSS パラメータの監視や表示を実行できますが、CSS パラメータを変更することはできません。User ステータスのプロンプトには、末尾に > が付きます。
- **SuperUser**：User ステータスで使用できる各コマンドを含む CSS のすべての CLI コマンドを使用して CSS を設定できます。SuperUser ステータスのプロンプトには、末尾に # が付きます。

  SuperUser モードでは、グローバル設定モードと、その下位の各設定モードを利用できます。新しいユーザを設定する際に **superuser** オプションを指定しないと、新しいユーザはデフォルトで User ステータスになります。

注意　ユーザ名やパスワードを作成したり変更したりできるのは、管理者または技術者として識別される CSS ユーザだけです。この制限は、**restrict user-database** コマンドが実行済みかどうかによって左右されます。

CSS にログインするためのユーザ名とパスワードは、**username** コマンドで作成します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

username *name* [**des-password**|**password**] *password* {**superuser**} {**dir-access** *access*}

次の例では、ユーザ名 *picard*、パスワード *captain* のユーザが、SuperUser ステータスで作成されます。

```
(config)# username picard password "captain" superuser
```

このコマンドのオプションと変数は次のとおりです。

- *name* ：割り当てまたは変更するユーザ名を設定する。スペースを含まない 16 文字以内の文字列を、引用符で囲まずに指定します。既存のユーザ名のリストを表示するには、**username ?** コマンドを使用します。

- **des-password** ：Data Encryption Standard （DES; データ暗号化規格）でパスワードを暗号化する。このオプションは、スクリプトや起動設定ファイルとして使用するファイルを作成する場合のみに使用します。DES のパスワードとして、6 ～ 64 文字の文字列を引用符で囲まずに、大文字と小文字を区別して入力します。
- **password** ：パスワードを暗号化しない。このオプションは、CLI で必要に応じてユーザを作成するときに使用します。
- *password* ：パスワード。スペースを含まない 6 ～ 16 文字の文字列を、引用符で囲まずに指定します。CSS では、パーセント記号（%）を除いたすべての特殊文字をパスワードに使用できます。

（注） **des-password** オプションを指定すると、CSS に正しくログインするには、暗号化されたパスワードが必要になります。CSS 暗号化パスワードは実行設定に含まれています。CSS　の実行設定を表示するには、**show running-config** コマンドを使用します（「ユーザ名とパスワードの作成」参照）。

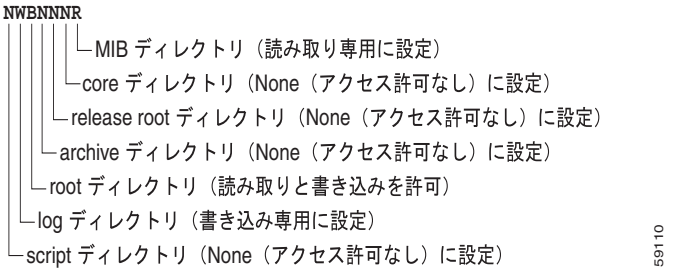
- **superuser** ：ユーザに SuperUser モードの利用を許可する。このオプションを指定しない場合、ユーザが利用できるのは User モードだけです。
- **dir-access**：（オプション）指定した名前のユーザを対象に、CSS ディレクトリへのアクセス権を指定する。CSS の 7 つのディレクトリ、つまり script、log、root （インストール済み CSS ソフトウェア）、archive、release root （設定ファイル）、core、MIB の各ディレクトリには、この順序でアクセス権が割り当てられています。デフォルトでは、7 つのディレクトリすべてに対して読み取りと書き込みの両方の権限（B）がユーザに与えられます。管理者や技術者は **dir-access** オプションによって、これらの各ディレクトリへの一連のアクセス権を、ユーザごとに設定できます。アクセス権の変更は、ディレクトリ関連の CLI コマンドの使用にも影響を与えます。

  dir-access オプションを使用するには、その前に **restrict user-database** コマンドを実行し、CSS ユーザ データベースにセキュリティ制限を設定する必要があります。

- *access*：指定した名前のユーザを対象に、ディレクトリへのアクセス権を指定する。デフォルトでは、7 つのディレクトリすべてに対して読み取りと書き込みの両方の権限（B）がユーザに与えられます。これらの各ディレクトリへのアクセス権を表す次のコードを、連結した文字列として入力します。
  - **R**：CSS ディレクトリへの読み取り専用アクセス
  - **W**：CSS ディレクトリへの書き込み専用アクセス
  - **B**：CSS ディレクトリへの読み取りおよび書き込みを許可
  - **N**：CSS ディレクトリへのアクセスを許可しない

図 1-1 に、ユーザのディレクトリへのアクセス権の例を示します。

図 1-1　CSS ディレクトリへのアクセス権



たとえば、ユーザ名 *picard* のディレクトリへのアクセス権を設定するには、次のように入力します。

```
(config)# username picard password "captain" superuser NWBNNNR
```

既存のユーザ名のリストを表示するには、次のように入力します。

```
(config)# username ?
```

既存のユーザ名を削除するには、次のように入力します。

```
(config)# no username picard
```

ユーザのパスワードを変更するには、**username** コマンドを実行して、新しいパスワードを指定します。ユーザのステータスが SuperUser の場合には、superuser オプションも忘れずに指定してください。たとえば、次のように設定します。

```
(config)# username picard password "flute" superuser
```

注意　**no username** コマンドはユーザを完全に削除します。このコマンドは、いったん実行すると元に戻せないため、注意して使用してください。

CSS へのリモート アクセスの制御

CSS へのアクセスを制御するには、リモート（仮想）ユーザまたはコンソール ユーザを認証するように CSS を設定します。CSS では、ローカル ユーザ データベース、RADIUS サーバ、または TACACS+ サーバを使用してユーザを認証できます。また、認証を行わずにユーザ アクセスを許可したり、すべてのリモート ユーザを許可しないようにしたりすることもできます。

認証方式は、最大 3 種類（プライマリ、セカンダリ、またはターシャリ）まで設定できます。プライマリ認証方式が最初に使用されます。プライマリ認証方式が失敗すると（たとえば、RADIUS サーバがダウンしているか到達不能）、セカンダリ方式が使用されます。セカンダリ認証方式が失敗した場合は、ターシャリ認証方式が使用されます。ターシャリ認証方式も失敗した場合は、認証エラー メッセージが表示されます。

次の条件下ではセカンダリ認証方式もターシャリ認証方式も使用されません。

- 認証方式が **local** であり、ローカル ユーザ名がローカル ユーザ データベースにない。
- 認証方式が **local** であり、ローカル ユーザ名がローカル ユーザ データベースにあるが、パスワードが無効である。
- 認証方式が **radius** であり、RADIUS サーバが CSS からのプライマリ認証要求を拒否する。
- 認証方式が **tacacs** であり、TACACS+ サーバが CSS のプライマリ認証要求を拒否する。

RADIUS または TACACS+ を仮想認証方式またはコンソール認証方式で使用するには、先に RADIUS または TACACS+ セキュリティ サーバとの通信を可能にしておく必要があります。これには **radius-server** コマンド（第 3 章「RADIUS サーバのクライアントとしての CSS の設定」参照）または **tacacs-server** コマンド（第 4 章「TACACS+ サーバのクライアントとしての CSS の設定」参照）を使用します。

ここでは、次の内容について説明します。

仮想認証設定およびコンソール認証設定を表示するには、**show user-database** コマンドを使用します。

仮想認証の設定

仮想認証では、FTP、Telnet、SSHD、または CiscoView Device Manager（CVDM）インターフェイスを使用しているリモート ユーザがユーザ名とパスワードを使用して CSS にログインできます。また、ユーザ名とパスワードを使用しなくてもログインすることができます。CSS ですべてのリモート ユーザのアクセスを拒否することもできます。

CSS では、ローカル ユーザ データベース、RADIUS サーバ、または TACACS+ サーバを使用してユーザを認証するように設定できます。デフォルトでは、ローカル ユーザ データベースがユーザのプライマリ認証方式として使用され、セカンダリ認証方式とターシャリ認証方式ではユーザ アクセスが禁止されます。

プライマリ、セカンダリ、ターシャリのいずれかの仮想認証方式を設定するには、**virtual authentication** コマンドを使用します。このグローバル設定コマンドのシンタックスは次のとおりです。

virtual authentication [**primary**|**secondary**|**tertiary**
[**local**|**radius**|**tacacs**|**disallowed**]]

このコマンドのオプションは次のとおりです。

- **primary** ：CSS で最初に使用する認証方式を定義する。デフォルトのプライマリ仮想認証方式は、ローカル ユーザ データベースです。
- **secondary** ：CSS で最初の認証方式が失敗した場合に次に使用する認証方式を定義する。デフォルトのセカンダリ仮想認証方式では、すべてのユーザ アクセスが禁止されます。

（注） TACACS+ サーバをプライマリ認証方式として設定する場合は、セカンダリ認証方式（**local** など）を定義する必要があります。

- **tertiary** ：CSS で 2 番目の認証方式が失敗した場合に次（3 番目）に使用する認証方式を定義する。デフォルトのターシャリ仮想認証方式では、すべてのユーザ アクセスが禁止されます。
- **local** ：認証にローカル ユーザ データベースを使用する。
- **radius** ：認証に設定済みの RADIUS サーバを使用する。
- **tacacs** ：認証に設定済みの TACACS+ サーバを使用する。

- **disallowed**：すべてのリモート ユーザのアクセスを禁止する。このオプションを指定しても、既存の接続は終了しません。

すでに CSS にログインしているユーザを削除するには、**disconnect** コマンドを使用します。

TACACS+ サーバをプライマリ仮想認証方式として定義するには、次のように入力します。

```
#(config) virtual authentication primary tacacs
```

ローカル ユーザ データベースをセカンダリ仮想認証方式として定義するには、次のように入力します。

```
#(config) virtual authentication secondary local
```

コンソール認証の設定

コンソール認証では、ユーザがユーザ名とパスワードを使用して、コンソール ポートに接続された端末経由で CSS にログインできるように設定できます。また、ユーザのユーザ名とパスワードがなくてもログインできるように設定することも可能です。CSS では、プライマリ認証方式でユーザ アクセスを禁止することができません。ただし、セカンダリ認証方式またはターシャリ認証方式では、ユーザ アクセスを禁止できます。

CSS では、ローカル ユーザ データベース、RADIUS サーバ、または TACACS+ サーバを使用してユーザを認証するように設定できます。デフォルトでは、ローカル ユーザ データベースがユーザのプライマリ認証方式として使用され、セカンダリ認証方式とターシャリ認証方式ではユーザ アクセスが禁止されます。

プライマリ、セカンダリ、ターシャリのいずれかのコンソール認証方式を設定するには、**console authentication** コマンドを使用します。このグローバル設定コマンドのシンタックスは次のとおりです。

console authentication [**primary** [**local**|**radius**|**tacacs**|**none**]|**secondary**|**tertiary** [**local**|**radius**|**tacacs**|**none**|**disallowed**]]

このコマンドのオプションは次のとおりです。

- **primary**：CSS で最初に使用する認証方式を定義する。デフォルトのプライマリ コンソール認証方式は、ローカル ユーザ データベースです。

- **local** ：認証にローカル ユーザ データベースを使用する。
- **radius** ：認証に設定済みの RADIUS サーバを使用する。
- **tacacs** ：認証に設定済みの TACACS+ サーバを使用する。
- **none** ：認証方式を使用しない。すべてのユーザが CSS にアクセスできます。
- **secondary** ：CSS で最初の認証方式が失敗した場合に次に使用する認証方式を定義する。デフォルトのセカンダリ コンソール認証方式では、すべてのユーザ アクセスが禁止されます。

（注） TACACS+ サーバをプライマリ認証方式として設定する場合は、セカンダリ認証方式（**local** など）を定義する必要があります。セカンダリ認証方式を設定しないで、デフォルトの **disallowed** を使用すると、CSS にログインできない可能性があります。

- **tertiary** ：CSS で 2 番目の認証方式が失敗した場合に次（3 番目）に使用する認証方式を定義する。デフォルトのターシャリ コンソール認証方式では、すべてのユーザ アクセスが禁止されます。
- **disallowed** ：すべてのユーザのアクセスを禁止する（セカンダリまたはターシャリ認証方式のみ）。このオプションを指定しても、既存の接続は終了しません。

すでに CSS にログインしているユーザを削除するには、**disconnect** コマンドを使用します。

TACACS+ サーバをプライマリ コンソール認証方式として定義するには、次のように入力します。

```
#(config) console authentication primary tacacs
```

ローカル ユーザ データベースをセカンダリ コンソール認証方式として定義するには、次のように入力します。

```
#(config) console authentication secondary local
```

コンソール ポートで認証を無効にして、ユーザがユーザ名とパスワードを指定しなくても CSS にアクセスできるようにするには、次のように入力します。

```
#(config) no console authentication
```

CSS への管理アクセスの制御

デフォルトでは、コンソール、FTP、SSH、SNMP および Telnet を使ったアクセスが有効に設定されています。CSS では、最大でそれぞれ 4 つの FTP セッションと Telent セッションがサポートされます。コンソール、FTP、SNMP、SSH、Telnet、ユーザ データベース、保護された XML と保護されていない XML、および CVDM による CSS へのデータ転送を有効または無効にするには、**restrict** および **no restrict** コマンドを使用します。

restrict コマンドを指定しても、CSS はアクセス制限されたポートでの接続試行を傍受します。TCP 接続の場合、CSS は TCP 3 ウェイ ハンドシェイクが完了した後でエラーで接続を終了し、データが転送されないようにします。UDP SNMP 接続の場合は、単にパケットを廃棄します。

制限付きポートを不正アクセスから保護するには、通常のトラフィックは CSS 内を通過させ、これらのポート宛てのパケットは拒否するように access control list（ACL; アクセス コントロール リスト）句を設定します。また、ACL を使用して CSS 自体を保護することもできます。CSS への ACL の設定方法については、「アクセス コントロール リストによる CSS ネットワーク トラフィックの制御」を参照してください。

CSS への管理アクセスの有効化

CSS へのコンソール、FTP、SNMP、SSH、Telnet、ユーザ データベース、保護された XML と保護されていない XML、CVDM アクセスを有効にするには、次の各 **no restrict** コマンドを使用します。

- **no restrict console** ：CSS へのコンソール アクセスを有効にする。デフォルトでは、有効に設定されています。
- **no restrict ftp** ：CSS への FTP アクセスを有効にする。デフォルトでは、有効に設定されています。
- **no restrict ssh** ：CSS への SSH アクセスを有効にする。デフォルトでは、有効に設定されています。
- **no restrict snmp** ：CSS への SNMP アクセスを有効にする。デフォルトでは、有効に設定されています。
- **no restrict telnet** ：CSS への Telnet アクセスを有効にする。デフォルトでは、有効に設定されています。

- **no restrict user-database** ：ユーザによる running-config ファイルの削除、およびユーザ名の作成や変更を有効にする。これらの操作は、管理者ユーザと技術者ユーザだけに許可されています。デフォルトでは、有効に設定されています。
- **no restrict secure-xml**：保護された HTTPS SSL 接続による CSS への XML 設定ファイルの転送を有効にする。デフォルトでは、無効に設定されています。
- **no restrict xml**：保護されていない HTTP 接続による CSS への XML 設定ファイルの転送を有効にする。デフォルトでは、無効に設定されています。
- **no restrict web-mgmt** ：CSS への CiscoView Device Manager（CVDM）からのアクセスを有効にする。デフォルトでは、無効に設定されています。

（注） Secure Shell Host（SSH; セキュア シェル ホスト）サーバを使用する場合は、Telnet アクセスを無効にします。SSH の設定については、第 2 章「SSHD プロトコルの設定」を参照してください。

たとえば、CVDM ユーザのアクセスを有効にするには、次のように入力します。

```
(config)# no restrict web-mgmt
```

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の設定についての詳細は、『*Cisco Content Services Switch Administration Guide*』を参照してください。XML を使用して、CSS に Web ベースでの設定変更を行う方法については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

CSS への管理アクセスの無効化

CSS へのコンソール、FTP、SNMP、SSH、Telnet、ユーザ データベース、保護された XML と保護されていない XML、CVDM アクセスを無効にするには、次の各 **restrict** コマンドを使用します。

- **restrict console** ：CSS へのコンソール アクセスを無効にする。デフォルトでは、有効に設定されています。
- **restrict ftp** ：CSS への FTP アクセスを無効にする。デフォルトでは、有効に設定されています。
- **restrict snmp** ：CSS への SNMP アクセスを無効にする。デフォルトでは、有効に設定されています。
- **restrict ssh** ：CSS への SSHD アクセスを無効にする。デフォルトでは、有効に設定されています。
- **restrict telnet** ：CSS への Telnet アクセスを無効にする。デフォルトでは、有効に設定されています。
- **restrict user-database** ：ユーザによる running-config ファイルの削除や、ユーザ名の作成、変更ができないようにする。これらの操作は、管理者ユーザと技術者ユーザだけに許可されています。デフォルトでは、有効に設定されています。
- **restrict secure-xml** ：保護された HTTPS SSL 接続による CSS への XML 設定ファイルの転送を無効にする。デフォルトでは、無効に設定されています。
- **restrict xml**：保護されていない HTTP 接続による CSS への XML 設定ファイルの転送を無効にする。デフォルトでは、無効に設定されています。
- **restrict web-mgmt** ：CSS への CVDM アクセスを無効にする。デフォルトでは、無効に設定されています。

たとえば、Telnet アクセスを無効にするには、次のように入力します。

```
(config)# restrict telnet
```

アクセス コントロール リストによる CSS ネットワーク トラフィックの制御

CSS には、アクセス コントロール リスト（ACL）を使用したトラフィックのフィルタリング機能が用意されています。ACL では、CSS のインターフェイスでパケットを転送するかブロックするかを制御することにより、着信ネットワーク トラフィックをフィルタ処理します。ACL は、ルーティング対象のネットワーク プロトコルに対して設定することができます。これにより、そのプロトコルのパケットが CSS を通過するときに、それらのパケットをフィルタリングすることができます。

ここでは、ACL の設定方法について説明します。

ACL の概要

CSS に ACL を設定すると、ネットワークへのアクセスに対して基本レベルのセキュリティが確立されます。ACL を設定していない CSS では、VLAN 回線を経由するすべてのパケットがネットワークに入ってくる可能性があります。ACL を使用すると、たとえば、CSS 回線に入ってくるすべての電子メール トラフィックを許可し、Telnet トラフィックをブロックするようなことが可能です。また、ACL を使用することにより、あるクライアントに対してネットワークの一部へのアクセスを許可し、別のクライアントに対して同じ領域へのアクセスを拒否することもできます。

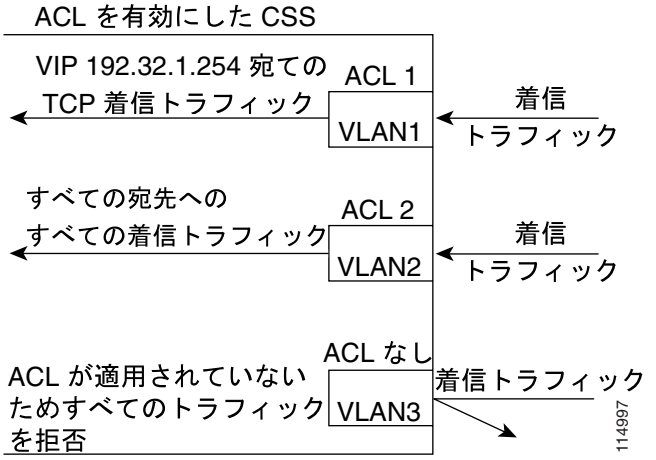
ACL は、ユーザ定義の句から構成されます。CSS では、これらの句を使用して、VLAN 回線での各パケットの処理方法を決定します。CSS は各パケットを検査し、パケットが ACL の句に一致するかどうかに基づいてそのパケットを転送またはブロックします。トラフィックが回線を通過できるようにするには、ACL に permit 句を設定する必要があります。ACL の最後には、暗黙的な「deny all」句があります。

CSS に ACL を設定する際には、CSS の各 VLAN について ACL を適用して、着信トラフィックを制御する必要があります。回線に ACL を適用すると、ACL とその句が、その回線に割り当てられます。

各 CSS 回線に ACL を適用したら、ACL を有効化する必要があります。ACL をグローバルに有効化すると、CSS のすべての回線に適用されます。ACL を有効化すると、すべての ACL に含まれる句が使用されて、すべての回線でトラフィックが許可または拒否されます。ACL が設定されていない回線には、暗黙的な「deny all」が適用され、この回線のすべてのトラフィックが拒否されます。

例として、図 1-2 に CSS の 3 本の VLAN 回線を示します。

図 1-2　CSS で有効化された ACL



VLAN1 で、宛先 VIP アドレス 192.32.1.254 へのすべての TCP トラフィックを許可するには、ACL 1 を作成し、次のように句を設定します。

clause 15 permit tcp any destination 192.32.1.254

その後に ACL 1 を VLAN1 に適用します。

VLAN2 で、任意の宛先へのすべてのトラフィックを許可するには、ACL 2 を作成し、次のように句を設定します。

clause 15 permit any any destination any

その後に ACL 2 を VLAN2 に適用します。

CSS で ACL を有効にすると、ACL に設定した permit 句の定義どおりに、VLAN1 と VLAN2 のトラフィックが許可されます。VLAN3 には ACL が適用されていないので、この回線には暗黙的な「deny all」が適用され、この回線のすべてのトラフィックが拒否されます。

注意　ACL は一種のファイアウォールとして機能し、セキュリティを確保します。*ACL を有効にする前に*、まず各 CSS 回線にトラフィックを許可する ACL を設定することが非常に重要です。トラフィックをまったく許可しない場合、ネットワークへの接続性が失われます。ただし接続が失われても、コンソール ポートには影響しません。

ACL をグローバルに有効化すると、各回線に ACL が割り当てられているかどうかに関係なく、*すべての* CSS 回線のすべてのトラフィックが影響を受けます。ACL を有効化すると、個々の ACL の permit 句に設定されていない回線のトラフィックはすべて*拒否されます*。各回線に ACL を適用していない場合、その回線へのトラフィックは拒否されます。

CSS で ACL を使用する際には、CSS のハードウェアに、レイヤ 3 またはレイヤ 4 の簡単な句を使用できる ACL が最大 10 個実装されます。CSS ソフトウェアには、より複雑なレイヤ 5 の句を使用できる ACL が実装されます。

（注）　ACL は、CSS のイーサネット管理ポートではサポートされません。

ACL は、ARP パケットをブロックしません。

ソース グループを指定した ACL 句を使用して、SSL モジュール宛てのトラフィックの送信元アドレス変換を行うことはできません。CSS はこの句を受け入れますが、SSL モジュールで終了するフローがあってもこの句を無視します。SSL 処理後にサーバに向かう接続に対して、NAT を適用することができます。

パッシブ FTP サーバのロード バランシングを実行している場合に、ACL を使用してソース グループを適用するには、そのソース グループに直接サービスを設定する必要があります。ソース グループによる FTP セッションのサポートの詳細は、『*Cisco Content Services Switch Content Load-Balancing Configuration Guide*』を参照してください。

ACL 設定のクイック スタート

表 1-1 に示すクイックスタートの手順を使用して、ACL を設定します。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。各機能の詳細については、この手順の後に示す各項を参照してください。

（注） 各 CSS 回線に設定する ACL には、1 つ以上の permit 句を含める必要があります。permit 句を 1 つも指定しないと、その回線へのすべてのトラフィックが拒否されます。

表 1-1　ACL 設定のクイック スタート

作業とコマンドの例
1. グローバル設定モードに入ります。 `# config` `(config)#`
2. ACL を作成して ACL モードにアクセスします。ACL インデックス番号を 1 ～ 99 の範囲で入力します。 `(config)# acl 7` `Create ACL <7>, [y,n]:y` `(config-acl[7])#`

表 1-1　ACL 設定のクイック スタート（続き）

作業とコマンドの例
3. ACL に句を設定します。これらの句は、ACL を適用する回線（VLAN1 など）へのトラフィックを制御するために使用されます。1 ～ 254 の句番号を入力し、clause パラメータを定義します。句を定義するためのシンタックスは次のとおりです。 **clause** *number* **permit**|**deny**|**bypass** *protocol* [*source_info* {*source_port*}] **dest** [*dest_info* {*dest_port*}] {**log**} {**prefer** *servicename*} {**sourcegroup** *name*} **clause** コマンドのオプションについては、表 1-2 を参照してください。たとえば、ネットワークの外部から CSS の 1 本の回線を通ってポート 20 ～ 23 へ着信するユーザ アクセスをすべてブロックするには、次のように入力します。 `(config-acl[7])# clause 10 deny any any destination range 20 23` その回線を通るその他のトラフィックをすべて許可するには、次のように入力します。 `(config-acl[7])# clause 15 permit any any destination any`
4. ACL を特定の回線に適用します。この例では、VLAN は 1 本だけ（デフォルトの VLAN1）です。たとえば、acl7 を回線 VLAN1 に適用するには、次のように入力します。 `(config-acl[7])# apply circuit-(VLAN1)` **apply all** コマンドを使用して、ACL 7 を CSS のすべての回線に適用することもできます。
5. その他のすべての回線についてステップ 1 ～ 4 を繰り返し、1 つ以上の permit 句を含む ACL を作成し、これらの回線に適用します。CSS で ACL を有効にした場合、ACL が適用されていない回線へのトラフィックは拒否されます。

表 1-1　ACL 設定のクイック スタート（続き）

作業とコマンドの例
6. すべての ACL を有効にします。すべての ACL に対してグローバルな **acl enable** コマンドを入力すると、CSS のすべての回線に適用されます。 **注意** ACL をグローバルに有効化すると、CSS のすべての回線へのすべてのトラフィックが対象となるので、個々の ACL 内の permit 句に指定した回線のトラフィックだけが許可されます。ACL を適用していない回線には、暗黙的な「deny all」が適用され、この回線へのすべてのトラフィックが拒否されます。 次に例を示します。 `(config)# **acl enable**`

次の実行設定例は、表 1-1 で説明したコマンドを入力した結果を示しています。

```
!************************** ACL ***************************
acl 7
    clause 10 deny any any destination range 20 23
    clause 15 permit any any destination any
  apply circuit-(VLAN1)

!************************** GLOBAL ***************************
acl enable
```

ACL の作成

ACL には、CSS の回線上のトラフィックを制御する句を記述します。CSS で ACL をグローバルに有効化すると、すべての回線に適用されるので、各回線について ACL を作成する必要があります。1 つの ACL を、複数の回線に適用することが可能です。また、1 つの ACL を CSS のすべての回線に適用することもできます。

（注） ACL が設定されていない回線には、暗黙的な「deny all」が適用され、この回線のすべてのトラフィックが拒否されます。

ACL を作成して ACL モードにアクセスするには、**acl** *index number* コマンドを使用します。1 ～ 99 のインデックス番号で ACL を定義します。既存の ACL のリストを表示するには、**acl ?** コマンドを使用します。

```
(config)# acl 7
```

このモードにアクセスすると、プロンプトは作成したインデックス番号の ACL モードに変わります。たとえば、次のように入力します。

```
(config-acl[7])#
```

ACL を作成した後には、句を追加する必要があります。詳細については、「句の設定」を参照してください。

ACL の削除

ACL とその句が不要になった場合は、その ACL を CSS から 削除できます。ACL を削除すると、ACL 内のすべての句も削除されます。ACL を削除するには、**no acl** コマンドを使用します。たとえば、ACL 7 を削除するには、次のように入力します。

```
(config)# no acl 7
```

CSS で ACL が有効化されている場合に、現在、回線に適用されている特定の ACL を削除すると、その ACL がその回線から削除され、CSS のその回線へのトラフィックが拒否されるようになります。この回線へのトラフィックを許可したい場合は、CSS で ACL をグローバルに無効化します。これにより、その回線へのすべてのトラフィックが許可されます。

たとえば、次のように操作します。

1. グローバル設定モードで、CSS のすべての ACL を無効化します。

   ```
   (config)# acl disable
   ```

2. ACL モードで、回線から ACL を削除します。次のように入力します。

   ```
   (config-acl[7])# remove circuit-(VLAN1)
   ```

3. グローバル設定モードで、ACL を削除します。次のように入力します。

```
(config)# no acl 7
```

4. その回線に別の ACL を適用します。回線に ACL を適用していない場合に CSS でグローバルに ACL を有効にすると、その回線へのトラフィックが拒否されます。
5. CSS のすべての ACL を再度有効にします。次のように入力します。

```
(config)# acl enable
```

句の設定

ACL に設定した句によって、回線のトラフィックが CSS でどのように処理されるかが決定されます。句を設定する際には、句に番号を割り当てる必要があります。各句に割り当てる番号は重要です。ACL は、句 1 から順に処理されます。句に番号を割り当てる際は、最も詳細な一致条件の句に最も小さい番号を割り当てます。一致条件が一般的になるにつれ、大きい値を割り当てます。

句は、番号順に入力する必要はありません。CSS により、句は適切な順序で ACL に自動挿入されます。たとえば、句 10 と句 24 を入力した後に句 15 を挿入すると、これらの句は正しい順序で挿入されます。

回線へのトラフィックを許可、拒否、またはバイパスする句を作成するには、**clause** コマンドを使用します。句*番号*は、句に割り当てる番号です。1 ～ 254 の番号を入力します。

(注) CSS で ACL が有効化されているときに ACL に新しい句を追加した場合は、その回線にその ACL を再度適用する必要があります。詳細については、「ACL をグローバルに有効化した場合の句の追加」を参照してください。

作成した句は、修正できません。句を修正するには、いったんその句を削除して、新しい句を作成する必要があります。句の削除の詳細は、「句の削除」の項を参照してください。

CSS は、すべての ACL に対し、255 番目の句としてデフォルトの暗黙の「deny all」句を適用します。このため、管理トラフィックなどのトラフィックを許可する permit 句を指定する必要があります。

clause コマンドのシンタックスは次のとおりです。

- **clause** *number* **bypass** ：回線へのトラフィックを*許可*し、そのトラフィックに適用されるコンテンツ ルールをバイパスする（処理しない）ための句を作成する。**clause bypass** のシンタックスは次のとおりです。

  clause *number* **bypass** *protocol* [*source_info* {*source_port*}]**dest** [*dest_info* {*dest_port*}] {**sourcegroup** *name*} {**prefer** *servicename*}

（注） **bypass** オプションでは、トラフィックでコンテンツ *ルールだけを*バイパスします。このため、Network Address Translating（NATing; ネットワーク アドレス変換）が行われません。ソース グループを指定する ACL 句では、**bypass** オプションを使用しないでください。**bypass** オプションは、ソース グループの NATing に影響しません。

- **clause** *number* **deny** ：回線へのトラフィックを拒否するための句を ACL に作成する。**clause deny** のシンタックスは次のとおりです。

  clause *number* **deny** *protocol* [*source_info* {*source_port*}]**dest** [*dest_info* {*dest_port*}] {**sourcegroup** *name*} {**prefer** *servicename*}

- **clause** *number* **permit** ：回線へのトラフィックを許可するための句を ACL に作成する。ACL に permit 句を設定すると、permit 句で指定されていないすべてのトラフィックは、デフォルトで拒否されます。**clause permit** のシンタックスは次のとおりです。

  clause *number* **permit** *protocol* [*source_info* {*source_port*}]**dest** [*dest_info* {*dest_port*}] {**sourcegroup** *name*} {**prefer** *servicename*}

（注） ACL 句内の宛先がレイヤ 5 コンテンツ ルールの場合、CSS は接続をスプーフしないため、ACL 句は予想したとおりに機能しません。これを解決するために、TCP/IP アドレスとポートを許可する追加の句を設定することができます。この場合、両方の句でコンテンツが一致することに注意してください。たとえば、次のようになります。

clause 14 permit any any destination content Layer5/L5 eq 80（元の句）

clause 15 permit tcp any destination 200.200.200.200 eq 80（これは、SYN を処理する追加の句です。この句では宛先の IP アドレスがレイヤ 5 コンテンツ ルールに設定されている IP アドレスになっています。この句番号には、宛先のコンテンツ ルールを指定する句番号よりも大きい値を指定する必要があります。）

表 1-2 に、**clause** コマンドの変数とオプションを示します。太字のシンタックスは、コマンドラインに入力するキーワードを表します。イタリック体は、値を入力する変数（IP アドレスやホスト名など）を表します。

表 1-2　clause コマンドのオプション

変数とオプション	パラメータ
number	句に割り当てる番号。1 ～ 254 の番号を入力します。
action	句に割り当てるアクション。**bypass**、**deny**、**permit** のいずれかを入力します。
protocol	トラフィックの種類に対応するプロトコル。**any**、**icmp**、**igp**、**igmp**、**ospf**、**tcp**、**udp** のいずれかを入力します。
source_info	トラフィックの送信元。次のいずれかを入力します。 • *ip_address*：送信元 IP アドレスとオプションのマスクの IP アドレス。*サブネット マスク*は、IP アドレス形式のみで指定可能（省略可）。 • *hostname*　：送信元のホスト名。ホスト名は、ニーモニック名形式で入力します。最初に CSS の DNS クライアントを設定して、CSS でのホスト名の変換を有効にします。 • **any**：送信元 IP アドレスおよびホスト名情報の任意の組み合わせ。 • **nql** *nql_name*：IP アドレスのリストで構成されている既存の Network Qualifier List（NQL; ネットワーク修飾子リスト）

表 1-2　clause コマンドのオプション（続き）

変数とオプション	パラメータ
source_port	トラフィックの送信元ポート。送信元ポートを指定しない場合、この句は、すべてのポート番号からのトラフィックを許可します。次のいずれかを入力します。 • **eq** *port* ：指定したポート番号と同じポート • **lt** *port* ：指定したポート番号より小さいポート • **gt** *port* ：指定したポート番号より大きいポート • **neq** *port* ：指定したポート番号と異なるポート • **range** *low high* ：ポート番号の範囲。1 ～ 65535 の範囲の番号を入力します。*low* と *high* の番号は、スペースで区切ります。
destination_info	トラフィックの宛先に関する情報。次のいずれかを入力します。 • **destination any** ：宛先に関する情報の任意の組み合わせ • **destination content** *owner_name/rule_name* ：所有者のコンテンツ ルール。所有者とルール名は、/ 文字で区切ります。 • **destination** *ip_address* ：宛先 IP アドレスとオプションのサブネット マスクの IP アドレス。*サブネット マスク*は、IP アドレス形式だけで入力します。CIDR アドレス形式は使用できません。 • **destination** *hostname* ：宛先のホスト名。*hostname* を使用するには、最初に CSS の DNS クライアントを設定して、CSS でのホスト名の変換を有効にします。 • **nql** *nql_name*：ホストの IP アドレスで構成される既存の NQL。NQL の名前を入力します。

表 1-2　clause コマンドのオプション（続き）

変数とオプション	パラメータ
destination_port	宛先のポート。次のいずれかを入力します。ポート番号またはポート名（オプションを指定）を使用できます。 • **eq** *port* ：指定したポート番号と同じポート • **lt** *port* ：指定したポート番号より小さいポート • **gt** *port* ：指定したポート番号より大きいポート • **neq** *port* ：指定したポート番号と異なるポート • **range** *low high* ：ポート番号の範囲。1 ～ 65535 の範囲の番号を入力します。*low* と *high* の番号は、スペースで区切ります。 • *port names* ： — **https** = ポート 443 Https — **ldap** = ポート 389 Ldap — **bgp** = ポート 179 Bgp — **ntp** = ポート 123 Ntp — **nntp** = ポート 119 Nntp — **pop** = ポート 110 Pop — **http** = ポート 80 Http — **gopher** = ポート 70 Gopher — **domain** = ポート 53 Domain — **smtp** = ポート 25 Smtp — **telnet** = ポート 23 Telnet — **ftp** = ポート 21 Ftp — **ftp-data** = ポート 20 Ftp-data — **none** = なし 宛先ポートを指定しない場合、この句では、すべてのポートへのトラフィックが許可されます。

表 1-2　clause コマンドのオプション（続き）

変数とオプション	パラメータ
sourcegroup *name*	トラフィックの宛先のソース グループ。グループ名を入力します。ソース グループのリストを表示するには、次のように入力します。 `show group ?` **（注）** **clause** *number* **bypass** コマンドは、ソース グループの NATing に影響しません。 ソース グループを指定した ACL 句を使用して、SSL モジュール宛てのトラフィックの送信元アドレス変換を行うことはできません。CSS はこの句を受け入れますが、SSL モジュールで終了するフローがあってもこの句を無視します。SSL 処理後にサーバに向かう接続に対して、NAT を適用することができます。

表 1-2　clause コマンドのオプション（続き）

変数とオプション	パラメータ
prefer *service_name*	トラフィックの宛先として、指定したサービスを他のサービスより優先させます。優先サービスを複数定義する場合は、各サービスをカンマ（,）で区切ります。サービスは、最大 2 つまで定義できます。 Application Peering Protocol（APP）セッションで学習されるサービスを優先サービスに設定することはできません。APP で学習されたリモート サービスは ap-redirect@192.168.138.118 の形式になり、**show service summary** 画面に表示されます。ACL 句を設定するときには、このサービスを優先サービスとして使用できません。起動設定にこの句を保存して CSS を再起動すると、起動障害が発生します。この時点では APP を通してこのサービスを学習していないためです。たとえば、次のような句です。 `clause 10 permit any any destination any prefer ap-redirect@192.168.138.118` **（注）** 優先サービスが設定された ACL は、スティッキ性よりも優先されます。 1 つの句内にソース グループと優先サービスの両方を指定する場合、先にソース グループを指定してから優先サービスを指定する必要があります。

ACL に句を作成すると、その ACL を回線に適用できます。詳細については、「回線または DNS 問い合せへの ACL の適用」の項を参照してください。

ACL をグローバルに有効化した場合の句の追加

CSS で ACL がグローバルに有効化されているときに、既に適用されている ACL に新しい句を追加した場合、その句を有効にするには、**apply circuit** コマンドを使用してその回線にその ACL を再度適用する必要があります。

たとえば、ACL 7 を VLAN1 に適用し、ACL をグローバルに有効化したとします。その後、ACL 7 に句を追加して、この句を有効にするには、次のように入力します。

```
(config-acl[7])# clause 200 permit any any destination any
(config-acl[7])# apply circuit-(VLAN1)
```

句の削除

既存の句を変更するには、ACL からいったんその句を削除して、再度追加する必要があります。句を削除するには、**no clause** コマンドを使用します。たとえば、句 6 を削除するには、次のように入力します。

```
(config-acl[7]) no clause 6
```

回線に ACL が適用され、有効化されている場合、その CSS ではこれらの ACL を使用中であると見なします。使用中の ACL から句を削除することはできません。句を削除するには、適用されている ACL を回線から削除してから、句を削除し、その ACL を再度回線に適用します。

たとえば、回線 VLAN1 の ACL7 から句 6 を削除するには、次のように操作します。

1. ACL モードで、回線 VLAN1 から ACL 7 を削除します。次のように入力します。

   ```
   (config-acl[7]) remove circuit-(VLAN1)
   ```

2. 次のように入力して、句 6 を削除します。

   ```
   (config-acl[7]) no clause 6
   ```

3. 回線 VLAN1 に ACL 7 を再度適用します。次のように入力します。

   ```
   (config-acl[7]) apply circuit-(VLAN1)
   ```

（注） 適用されている ACL を回線から削除すると、この回線に暗黙的な「deny all」が適用され、この回線へのすべてのトラフィックが拒否されます。適用されている ACL を回線から削除するときに、CSS でその回線へのトラフィックを許可したい場合は、グローバル設定モードで **acl disable** コマンドを使用して、ACL をグローバルに無効化します。CSS ですべての ACL を無効化することにより、すべての回線へのすべてのトラフィックが許可されます。

SSL モジュール発信トラフィックからの ACL 句の除外

デフォルトでは、ACL 内のすべての句が SSL モジュールからの発信トラフィックに適用されます。SSL モジュール発信トラフィックから、ACL 内のすべての句または特定の句を除外するには、ACL 設定モードで **exclude** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

exclude ssl circuit-(VLAN*number***)** {*acl_clause*}

このコマンドには次の変数があります。

- *number*：ACL 句を除外する回線の番号
- *acl_clause*：（オプション）除外する句の番号。1 つ以上の句、または句の範囲を設定できます。複数入力する場合は、各番号をカンマで区切ります。スペースは使用しません。句の範囲を入力するには、最初と最後の番号をダッシュ (-) でつなぎます。スペースは使用しません。

  句を指定しないと、すべての句が除外されます。

たとえば、VLAN1 で ACL 7 の句 1、5、および 10 ～ 20 を除外する場合は次のように入力します。

```
(config-acl[7])# exclude ssl circuit-(VLAN1) 1,5,10-20
```

すべての ACL 句を、SSL モジュールからの発信トラフィックに再適用するには、**exclude** コマンドの **no** 形式を使用します。たとえば、次のように入力します。

```
(config-acl[7])# no exclude ssl circuit-(VLAN1)
```

exclude コマンドを使用する場合は、次の要件を考慮してください。

- **exclude** コマンドを使用する SSL モジュールが CSS に取り付けられている必要があります。
- ACL に **exclude** コマンドを再設定するには、先に **exclude** コマンドの **no** 形式を使用する必要があります。これを行わないと、エラーが表示されます。

  ```
  Must issue <no exclude ssl circuit-(VLAN#)> command first
  ```

- 1 つの ACL につき、1 つの **exclude** コマンドしか設定できません。exclude が設定されている VLAN 以外の VLAN での **no exclude** コマンドの使用についても、このルールが適用されます。複数設定しようとすると、次のエラー メッセージが表示されます。

  ```
  Only one <exclude ssl circuit-(VLAN#)> command per-ACL
  ```

- **exclude** コマンドは、複数の ACL で同じ VLAN に対して使用できません。使用すると、次のエラー メッセージが表示されます。

  ```
  Command <exclude ssl circuit-(VLAN#)> command found on different
  ACL
  ```

- ACL に **exclude** コマンドを設定すると、その ACL には 1 つの **apply** コマンドしか設定できません。複数設定しようとすると、次のエラー メッセージが表示されます。

  ```
  Only one <apply circuit-(VLAN#)> command allowed with exclude
  configured
  ```

  ACL に複数の **apply** コマンドを設定すると、**exclude** コマンドは設定できません。

  apply コマンドを設定しなくても **exclude** コマンドを設定できますが、**apply** コマンドを設定するまで有効になりません。

- ACL に **exclude** と **apply** コマンドを設定する場合は、両方のコマンドで同じ回線 VLAN 番号を指定する必要があります。回線 VLAN 番号が異なる場合は、次のエラー メッセージが表示されます。

  ```
  No circuit apply command or exclude ssl circuit mismatch
  ```

- 1 本の回線上に **exclude** コマンドと **apply** コマンドを設定する場合は、同じ ACL に指定する必要があります。異なる場合は、次のエラー メッセージが表示されます。

  ```
  Command <exclude ssl circuit-(VLAN#)> command on different ACL
  than apply
  ```

- **apply** コマンドを設定してから **exclude** コマンドかその **no** 形式を設定すると、内部で **apply** コマンドが再発行されてその ACL が回線に再度適用されます。このコマンドが再発行されることにより、リモートのセッション プロセッサで SSL 設定が更新されます。
- 次のコマンド セットは、回線 VLAN が削除されると **exclude** コマンドを無効にします。

  interface *slot/subslot* コマンド

  no bridge vlan コマンド

回線または DNS 問い合せへの ACL の適用

ACL に句を設定したら、**apply** コマンドを使用してすべての回線、個別の回線、または DNS 問い合せに ACL を割り当てます。

(注) 適用されている ACL に新しい句を追加するには、**apply circuit** コマンドを使用して、その回線に ACL を再度適用します。これにより、追加した句が有効になります。

空の ACL を回線に適用することはできません。適用しようとすると、エラーメッセージ「`Cannot apply ACL for it has no clauses`」が表示されます。

この ACL モード コマンドのシンタックスとオプションは次のとおりです。

- **apply all** ：既存のすべての回線に ACL を適用する。たとえば、次のように入力します。

  ```
  (config-acl[7])# apply all
  ```

- **apply circuit - (***circuit_name***)**：個別の回線に ACL を適用する。たとえば、acl7 を回線 VLAN1 に適用するには、次のコマンドを入力します。

  ```
  (config-acl[7])# apply circuit-(VLAN1)
  ```

  回線のリストを表示するには、**apply ?** を入力します。

- **apply dns** ：DNS 問い合せに ACL を追加する。

  ```
  (config-acl[7])# apply dns
  ```

add dns *domain_ name* コマンドを使用して CSS のコンテンツ ルールにドメイン名を設定すると、そのドメイン名への DNS 問い合せは、**apply dns** コマンドで設定された ACL と*一致します*。

ただし、CSS に **dns-server** コマンドが設定されている場合に、**host** コマンドで CSS に設定されたドメイン名への DNS 問い合せを CSS が受信すると、この DNS 問い合せは、**apply dns** コマンドで設定された ACL と*一致しません*。

ACL を適用した後に、CSS で ACL が無効になっている場合は、**acl enable** グローバル設定コマンドを入力して、CSS で ACL を有効にする必要があります。**acl enable** コマンドの詳細については、この章で後述する「CSS での ACL の有効化」の項を参照してください。

回線または DNS 問い合せからの ACL の削除

ACL から句を削除する場合、回線に適用した ACL を削除する場合、または DNS 問い合せから ACL を削除する場合は、回線からその ACL を削除します。すべての回線、特定の回線、または DNS 問い合せから ACL を削除するには、**remove** コマンドを使用します。この ACL モード コマンドのシンタックスとオプションは次のとおりです。

- **remove all** ：すべての回線から ACL を削除する。

  ```
  (config-acl[7])# remove all
  ```

- **remove circuit - (***circuit_name***)**：特定の回線から ACL を削除する。たとえば、次のように入力します。

  ```
  (config-acl[7])# remove circuit-(VLAN1)
  ```

  削除可能な回線のリストを表示するには、**remove ?** を入力します。

- **remove dns** ：DNS 問い合せから ACL を削除する。次に例を示します。

  ```
  (config-acl[7])# remove dns
  ```

回線から ACL を削除する前に、ACL をグローバルに無効化することをお勧めします。CSS で ACL が有効になっている場合にある回線から ACL を削除すると、その回線に暗黙的な「deny all」が適用され、この回線へのすべてのトラフィックが拒否されるようになります。この回線へのトラフィックが拒否されないようにするには、CSS ですべての ACL を無効にした後に、その回線から ACL を削除する必要があります。CSS ですべての ACL を無効化することにより、すべての回線へのすべてのトラフィックが許可されます。

たとえば、次のように操作します。

1. グローバル設定モードで、CSS のすべての ACL を無効化します。

```
(config)# acl disable
```

2. ACL モードで、対象の回線から ACL を削除します。

```
(config-acl[7])# remove circuit-(VLAN1)
```

3. ACL に変更を加えます。

   回線から ACL を削除した場合は、permit 句を含む別の ACL をその回線に設定し、適用します。この操作を行わないと、CSS で ACL を再度有効にしたときに、その回線へのトラフィックが拒否されるようになります。

4. ACL を回線に再度適用します。

```
(config-acl[7])# apply circuit-(VLAN1)
```

5. グローバル設定モードで、CSS のすべての ACL を再度有効化します。

```
(config)# acl enable
```

CSS での ACL の有効化

ACL とその句を設定した後に、その ACL を各 CSS 回線に適用すると、すべての ACL をグローバルに有効化し、CSS で使用できるようになります。すべての ACL をグローバルに有効化すると、CSS のすべての回線へのすべてのトラフィックが影響を受け、permit 句が指定されている ACL が設定された回線へのトラフィックだけが許可されるようになります。

注意　*ACL を有効にする前に*、まず各 CSS 回線にトラフィックを許可する ACL を設定することが非常に重要です。ACL を有効化すると、すべての回線が対象になります。トラフィックをまったく許可しない場合は、ネットワークへの接続性が失われます。ACL を有効化すると、個々の ACL の permit 句に設定されていない回線のトラフィックはすべて*拒否されます*。ACL が適用されていない回線には、暗黙的な「deny all」句が適用されます。

たとえば、CSS に 3 本の回線（VLAN1、VLAN2、および VLAN3）を設定したとします。次に、ACL を VLAN1 だけに設定したとします。ACL をグローバルに有効化すると、VLAN1 では、その ACL に基づいてトラフィックが流れますが、VLAN2 と VLAN3 には ACL が設定されていないため、これらの回線に暗黙的な「deny all」句が適用され、これらの回線へのパケットは廃棄されます。

CSS で ACL をグローバルに有効化する前に、コンソールにアクセスできることを確認してください。ACL の設定が原因でネットワーク接続が失われた場合でも、コンソール ポートには影響がありません。

acl enable グローバル設定コマンドを使用して、CSS ですべての ACL を有効化します。すべての ACL をグローバルに有効にするには、次のコマンドを入力します。

```
(config)# acl enable
```

CSS での ACL の無効化

ACL を追加、変更、または削除する場合、または ACL の句を削除する場合は、回線からその ACL を削除する前に、すべての ACL を CSS で無効にすることをお勧めします。ACL をグローバルに無効化する前に、ある回線から ACL を削除すると、その回線に暗黙的な「deny all」が適用され、この回線へのすべてのトラフィックが拒否されます。

（注）　CSS で ACL をグローバルに無効化すると、CSS のすべての ACL が無効化され、すべての CSS 回線へのすべてのトラフィックが許可されるようになります。

CSS のすべての ACL をグローバルに無効にするには、次のコマンドを入力します。

```
(config)# acl disable
```

ACL の表示

show acl コマンドを使用して、アクセス コントロール リストおよびその句を表示します。**show acl** コマンドは、すべてのモードで使用できます。

回線に適用された ACL 句を表示すると、次の項目が示されます。

- **Content Hits** ：フローとは、クライアント / サーバ間の UDP および TCP パケットストリームとして定義できます。CSS が完全にフローを確立するには、クライアントおよびサーバから多数のパケットを受信する必要があります。フローが完全に確立される前に受信するこれらのパケットは、すべて ACL チェックを受ける必要があります。このため、ACL コンテンツ ヒット カウンタが増加することがあります。
- **Router Hits** ：TCP と UDP 以外のパケットはすべて ACL チェックを受ける必要があるので、ACL ルータ ヒット カウンタが増加します。CSS で終端するすべての UDP および TCP トラフィック（たとえば、Telnet または FTP セッション）でも、ACL ルータ ヒットカウンタが増加します。
- **DNS Hits**：ACL の句が DNS 問い合せに適用された場合に、ACL 句に一致し通過した DNS フローのパケット数。DNS ルックアップの数をカウントする DNS ヒット カウンタが表示されます。

CSS が受信したそれぞれのパケットの ACL ヒットの合計数は、フロー タイプと ACL マッチの有無によって異なります。CSS は、ACL のフローが完全に確立されるまで、受信したすべてのパケットに対して ACL のチェックを実行します。いったん ACL フローが確立されると、CSS は受信したそのフローに関連する残りのパケットに対して ACL チェックを行いません。このため ACL ヒットのカウンタは増加しません。

このコマンドのシンタックスは次のとおりです。

- **show acl** ：すべての ACL とその句を表示する。
- **show acl** *index* ：指定した ACL インデックス番号の句を表示する（有効な番号は 1 ～ 99）。
- **show acl config** ：ACL のグローバルな設定を表示する。このコマンドでは、どの ACL がどの回線に適用されているかが示されます。

このコマンドは、次のように入力します。

```
(config)# show acl 2
```

表 1-3 に、**show acl** コマンドで表示されるフィールドを示します。

表 1-3　show acl コマンドのフィールド

フィールド	説明
Acl	ACL に割り当てられた番号（1 ～ 99）
Clause	句に割り当てられた番号（1 ～ 254）
Action	着信トラフィックを、句（permit、deny、または bypass）とそのトラフィック タイプのプロトコルで制御する方式
Source	設定されたトラフィックの送信元
Destination	設定されたトラフィックの宛先
Log	指定した句の ACL ロギングが有効または無効のどちらであるかを示します。
Content Hits	フローが確立されるまでに CSS が受信したパケットの増分カウント
Router Hits	Telnet または FTP セッションで、あるいは TCP または UDP 以外のパケットから CSS に直接転送されたパケットの増分カウント
DNS Hits	DNS フローで ACL 句に一致するパケットの増分カウント

ACL カウンタ表示の 0 への設定

zero counts コマンドを使用して、特定の ACL に対して、**show acl** コマンド画面内のコンテンツと DNS のヒット カウンタをゼロにリセットします。このコマンドを実行するには、ACL のモードに入っている必要があります。このコマンドでは、その ACL のカウンタだけがクリアされます。

このコマンドのシンタックスとオプションは次のとおりです。

```
(config-acl[7])# zero counts
```

ACL アクティビティのロギング

ACL アクティビティをロギングするように設定すると、句と ACL に一致するパケットのイベントがロギングされます。ログ情報は、**logging** コマンドで指定した場所に送信されます。**logging** コマンドの詳細については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

(注) ACL またはその句のロギングは、お勧めしません。ACL またはその句のロギングを有効にすると、CSS のパフォーマンスが低下する可能性があります。
特定の ACL 句にロギングを設定する前に、グローバルな ACL ロギングが有効になっていることを確認してください。グローバルな ACL ロギングを有効にするには、グローバル設定モードで **logging subsystem acl level debug-7** コマンドを使用します。
CSS は、**clause log enable** コマンドを実行設定に保存しないため、CSS を再度ブートした場合は、ロギングを再度有効にする必要があります。

既存の ACL 句のロギングを有効化するには、次のように **clause** コマンドに **log enable** オプションを指定します。

```
(config-acl[7])# clause 1 log enable
```

CSS で ACL をグローバルに有効化している場合、次のように既存の ACL 句のロギングを設定します。

1. グローバル設定モードで、CSS のすべての ACL を無効化します。

   ```
   (config)# acl disable
   ```

2. ロギングを有効にする対象の ACL モードに入ります。

   ```
   (config)# acl 7
   (config-acl[7])#
   ```

3. 回線から ACL を削除します。

   ```
   (config-acl[7]) remove circuit-(VLAN1)
   ```

4. 既存の句のロギングを有効にします。

```
(config-acl[7])# clause 1 log enable
```

5. ACL を回線に再度適用します。

```
(config-acl[7])# apply circuit-(VLAN1)
```

6. グローバル設定モードで、CSS のすべての ACL を再度有効化します。

```
(config)# acl enable
```

特定の句の ACL ロギングを無効にするには、次のように入力します。

1. グローバル設定モードで、CSS のすべての ACL を無効化します。

```
(config)# acl disable
```

2. ロギングを無効にする対象の ACL モードに入ります。

```
(config)# acl 7
(config-acl[7])#
```

3. 回線から ACL を削除します。

```
(config-acl[7]) remove circuit-(VLAN1)
```

4. 既存の句のロギングを無効にします。

```
(config-acl[7])# clause 1 log disable
```

5. ACL を回線に再度適用します。

```
(config-acl[7])# apply circuit-(VLAN1)
```

6. グローバル設定モードで、CSS のすべての ACL を再度有効化します。

```
(config)# acl enable
```

すべての ACL 句のロギングをグローバルに無効にするには、次のように入力します。

```
(config)# no logging subsystem acl
```

ACL の例

次の ACL では、1 本の VLAN（VLAN1）で CSS、Server1 および Server2 にセキュリティを設定します。この ACL は次のように動作します。

- サブネット 172.16.107.x からのクライアントに対し、さまざまなアプリケーション（Telnet、FTP、TFTP など）を使用して VLAN1 の Server1 および Server2 にアクセスすることを許可します。
- サブネット 172.16.107.x からのクライアントに対し、URL 172.16.107.35（VIP アドレス）でブラウザを起動することを許可します。
- 172.16.107.x 以外のサブネットにあるクライアントが、VLAN1、Server1、Server2 にアクセスできないようにします。

各句では、次のセキュリティが提供されます。

- 句 20 では、送信元のサブネット 172.16.107.0 から Server1 （IP アドレス 172.16.107.15）へのすべてのプロトコルを許可します。
- 句 30 では、送信元のサブネット 172.16.107.0 から Server2 （IP アドレス 172.16.107.16）へのすべてのプロトコルを許可します。
- 句 40 では、送信元のサブネット 172.16.107.0 から VIP アドレス 172.16.107.35 ポート 80（HTTP）へのすべてのプロトコルを許可します。
- 句 50 では、キープアライブを含む、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）のすべてのトラフィックに対し VLAN への双方向通信を許可します。キープアライブ サービスを使用している場合は、キープアライブ トラフィックを許可する句を設定する必要があります。
- 句 60 では、UDP を使用した VLAN のポート 520 への Routing Information Protocol（RIP; ルーティング情報プロトコル）のアップデートを許可します。この句は、使用中のルータが 172.16.107.x 以外のサブネットに存在する場合に必要です。

- 句 70 では、ACL で許可されていないすべてのトラフィックを拒否します。

```
!*************************** ACL ***************************
acl 1
clause 20 permit any 172.16.107.0 255.255.255.0 destination
172.16.107.15
clause 30 permit any 172.16.107.0 255.255.255.0 destination
172.16.107.16
clause 40 permit any 172.16.107.0 255.255.255.0 destination
172.16.107.35 eq 80
clause 50 permit ICMP any destination any
clause 60 permit udp any destination any eq 520
clause 70 deny any any destination any
apply circuit-(VLAN1)
```

ACL へのネットワーク修飾子リストの設定

NQL 設定モードでは、ネットワーク修飾子リスト（NQL）を設定することができます。NQL は、IP アドレスおよびサブネット マスクにより識別される、ネットワークまたは特定のサービスのリストです。NQL は ACL 句に送信元または宛先として割り当てます。複数のネットワークを NQL にグループ化して、その NQL を 1 つの ACL 句に割り当てると、そのグループにその 1 つの句を作成するだけで済みます。ネットワークごとに個別の句を作成する必要はありません。

CSS では、次のものを最大 512 個まで設定できます。

- NQL あたりのネットワークまたはサービス
- CSS あたりの NQL

この機能は、特定のネットワークをバイパスしてコンテンツ要求を元のサーバ（コンテンツが保存されているサーバ）に直接送信するキャッシング環境などで役立ちます。また、特定のネットワークに基づいて、あるサービスを優先させる場合にも NQL を使用できます。

NQL 設定モードにアクセスするには、**nql** コマンドを使用します。プロンプトは、(config-nql [name]) に変わります。NQL モードでこのコマンドを使用して他の NQL にアクセスすることもできます。

NQL の設定については、次の項を参照してください。

- NQL の作成
- NQL の説明の記述
- NQL へのネットワークの追加
- ACL 句への NQL の追加
- NQL 設定の表示

NQL の作成

作成する新しい NQL または既存の NQL の名前を入力します。名前は、スペースを含まない 31 文字以内のテキスト文字列を引用符で囲まずに入力します。CSS ごとに最大 512 個の NQL を作成できます。

たとえば、次のように入力します。

```
(config)# nql bypass_nql
(config-nql[bypass_nql])#
```

既存の NQL のリストを表示するには、**nql ?** を入力します。NQL が存在しない場合は、新しい名前を入力するよう指示されます。

既存の NQL を削除するには、**no nql** コマンドを使用します。たとえば、次のように入力します。

```
(config)# no nql bypass_nql
```

NQL の説明の記述

NQL の説明を記述するには、NQL モードで **description** コマンドを使用します。NQL の説明は、63 文字以内のテキスト文字列を引用符で囲んで入力します。

たとえば、次のように入力します。

```
(config-nql[bypass_nql])# description “Bypass services”
```

NQL へのネットワークの追加

最大 512 個のネットワークまたはサービスを NQL に追加するには、**ip address** コマンドを使用します。IP アドレスを、サブネット プレフィクスまたはサブネット アドレスと共に入力します。必要に応じて、IP アドレスの説明を追加したり、ロギングをオンにしたりすることもできます。

このコマンドのシンタックスおよびオプションは、次のとおりです。

ip address *ip_address*[*/subnet_prefix*| *subnet_mask*] {**“***description***”**}{**log**}

変数とオプションは、次のとおりです。

- *ip_address* ：宛先のネットワーク アドレス。IP アドレスをドット付き 10 進表記で入力します（例 192.168.0.0）。
- *subnet_prefix*|*subnet_mask* ：CIDR ビット数表記の IP サブネット マスク プレフィクス長（/16 など）。有効なプレフィクス長の範囲は 8 ～ 32 です。IP アドレスとプレフィクス長の間にはスペースを入れないでください。
- *subnet_mask* ：ドット付き 10 進表記の IP サブネット マスク（たとえば、255.255.0.0）
- **“***description***”** ：IP アドレスの説明。63 文字以内のテキスト文字列を引用符で囲んで入力します。
- **log** ：NQL に関連するイベントのログ。このオプションを入力しない場合、イベントのログは記録されません。NQL イベントのログを記録するには、グローバルな NQL ロギングを有効にする必要があります。グローバルな NQL ロギングを有効にするには、**(config) logging subsystem nql level debug-7** コマンドを使用します。ロギングの詳細については、『*Cisco Content Services Switch Administration Guide*』を参照してください。

たとえば、NQL bypass_nql に 2 つのネットワークを追加するには、次のように入力します。

```
(config-nql[bypass_nql])# ip address 192.168.0.0/16 “Network of
dynamic mail content” log
(config-nql[bypass_nql])# ip address 123.123.123.0/24
```

ネットワークで発生したイベントのログを記録するには、グローバルな NQL ロギングを有効にする必要があります。たとえば、次のように入力します。

```
(config)# logging subsystem nql level debug-7
```

（注） エントリの作成時に説明を追加したり、ロギング機能を有効にしないで、これらの作業を後で行う場合は、最初にそのエントリを削除してから、希望のオプションを指定してこのエントリを再度追加してください。

NQL から IP アドレスを削除するには、**no ip address** コマンドを使用します。次に例を示します。

```
(config-nql[bypass_nql])# no ip address 192.168.0.0/16
```

ACL 句への NQL の追加

NQL を ACL 句に追加するには、次の手順に従います。

1. ACL を作成します。たとえば、次のように入力します。

   ```
   (config)# acl 10
   ```

2. 送信元または宛先として NQL を含む句を定義します。

   次の句の例では、任意の送信元から、NQL bypass_nql で定義された宛先ネットワークのポート 80 に発信されたトラフィックに対してコンテンツ ルールがバイパスされます。

   ```
   (config-acl[10])# clause 1 bypass any any destination nql
   bypass_nql eq 80
   ```

NQL 設定の表示

NQL 設定の情報を表示するには、**show nql** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

- **show nql** ：すべての NQL に関する情報を表示する。NQL モードでこのコマンドを入力すると、現在の NQL のアドレスだけが表示されます。
- **show nql** *nql_name* ：指定した NQL の情報を表示する。NQL 名は、大文字小文字を区別したスペースを含まないテキスト文字列を引用符で囲まずに入力します。既存の NQL 名のリストを表示するには、**show nql ?** コマンドを使用します。

たとえば、次のように入力します。

```
(config-nql[bypass_nql])# show nql
```

表 1-4 に、**show nql** コマンドで表示されるフィールドを示します。

表 1-4　show nql コマンドのフィールド

フィールド	説明
Name	NQL の名前
Description	NQL に関連付けられている説明
IP Addresses	NQL でサポートされる IP アドレスとサブネット マスク。説明が設定されている場合、アドレスの後に説明が表示されます。

CHAPTER 2

SSHD プロトコルの設定

Secure Shell Daemon （SSHD）プロトコルは、保護されていないネットワーク経由で通信する 2 つのホスト間で、通信内容を暗号化して保護します。CSS では、OpenSSH を実装して、通信を保護することができます。SSHD では、CSS のログイン プロンプトでユーザ名とパスワードを入力する、標準の CSS ログイン シーケンスを使用します。

CSS の SSHD では、SSH v1 プロトコルと v2 プロトコルの両方がサポートされます。SSH v1 では、3DES や Blowfish などの暗号化方式で通信が暗号化されます。SSH v2 では、128 ビットの AES、Blowfish、3DES、CAST128、Arcfour、192 ビットの AES、または 256 ビットの AES が使用できます。

注意 SSHD を使用する場合は、リモート システムにある、ネットワーク マウントしたファイル システムから CSS をブートするような環境（ディスクレス環境）に設定されていないことを確認してください。CSS をネットワーク マウントしたファイル システムからブートする場合は、SSHD プロトコルがサポートされないことに留意してください。

ネットワーク マウントしたファイル システムから CSS がブートされた場合は、SSHD プロトコルにより初期化が行われるときに、次に示す SSHD からのエラー メッセージが記録され、初期化動作が終了します。

```
Unable to initialize sshd; failure to seed random number generator
```

この章の主な内容は次のとおりです。

SSH の有効化

CSS の SSH 機能を有効にするには、セキュア管理ソフトウェア オプションを購入する必要があります。セキュア管理ソフトウェア オプションを購入した場合は、権利証明書が次の方法でお手元に届きます。

- CSS の注文の際に購入した場合は、アクセサリ キットに権利証明書が同封されています。
- CSS　をすでに購入している場合、権利証明書は郵送によりお手元に届きます。

(注) セキュア管理オプションの権利証明書がアクセサリ キットにない場合は、製品をお買い上げの弊社販売代理店にお問い合わせください。

権利証明書の指示に従って、セキュア管理ソフトウェア ライセンス キーを入手します。

セキュア管理ライセンス キーをインストールして SSH を有効にするには、次の操作を実行します。

1. CSS にログインして、**license** コマンドを実行します。

```
# license
```

2. セキュア管理ライセンス キーを入力します。

```
Enter the Software License Key (q to quit): nnnnnnnnnnnn
```

セキュア管理ライセンス キーはこれで正常にインストールされ、SSH 機能がアクティブになります。

SSH アクセスの設定

SSH による CSS へのアクセスは、**no restrict ssh** コマンドによりデフォルトで有効になっています。SSH アクセスの選択状態は、running-config ファイル内で調べることができます。

SSHD 使用時にセキュリティを強化するには、Telnet アクセスを無効にします（Telnet アクセスはデフォルトで有効に設定されています）。第 1 章「CSS のアクセス制御」の説明に従って、**telnet-access disable** コマンドを使用します。

SSH による CSS へのアクセスを有効にするには、次のコマンドを入力します。

```
(config)# no restrict ssh
```

SSH によるアクセスを無効にするには、次のように入力します。

```
(config)# restrict ssh
```

CSS での SSHD の設定

CSS に SSHD を設定するためのコマンドは、次のとおりです。

- **sshd keepalive** ：TCP キープアライブ メッセージを有効にする。
- **sshd port** ：SSHD ポートを指定する。
- **sshd server-keybits** ：エフェメラルなプロトコル サーバ キーのビット数を設定する（SSH v1 だけ）。
- **sshd version** ：CSS でサポートされる SSH プロトコルのバージョンを設定する。

SSHD から CSS へのアクセスが有効化され、SSHD が SSH クライアントからの接続を受信できることを確認します。デフォルトでは、SSH アクセスは、**no restrict ssh** コマンドによってグローバルに有効化されています。

SSHD キープアライブの設定

CSS では、クライアントに TCP キープアライブ メッセージを送信して、サーバからクライアントへの SSHD 接続が機能しているかどうか（たとえば、ネットワークが停止しているか、または、クライアントが応答不能になっているか）を確認できます。クライアントへの SSHD キープアライブの送信を無効にすると、サーバ上でセッションが無期限に停止し、システム リソースを大量に使用することがあります。

SSHD キープアライブを有効にするには、**sshd keepalive** コマンドを使用します。SSHD キープアライブは、デフォルトで有効に設定されています。

クライアントへの SSHD キープアライブの送信を有効にするには、次のコマンドを入力します。

```
(config)# sshd keepalive
```

SSHD キープアライブの送信を無効にするには、次のように入力します。

```
(config)# no sshd keepalive
```

SSHD ポートの設定

SSH のデフォルト ポート番号は 22 です。サーバがクライアントからの接続を監視するポート番号を指定するには、**sshd port** コマンドを使用します。22、または 512 ～ 65535 のポート番号を入力します。

（注） 新しい sshd ポートを設定すると、ポートが無効または使用不可であることを通知するメッセージが表示される場合があります。このメッセージが表示されるのは、ポートが CSS の内部で使用中の場合です。このメッセージが表示された場合は、別のポート番号を入力してください。

たとえば、ポート番号 65530 を SSHD ポートとして設定するには、次のように入力します。

```
(config)# sshd port 65530
```

ポート番号をデフォルトの 22 に戻すには、次のように入力します。

```
(config)# no sshd port
```

SSHD サーバキービットの設定

エフェメラルなプロトコル サーバ キーのビット数を指定するには、**sshd server-keybits** コマンドを使用します。**sshd server-keybits** コマンドは、SSH v1 の接続だけを対象としています。512 ～ 1024 （有効な範囲）のビット数を入力します。デフォルトは 768 です。

（注） このコマンドの有効な範囲は 512 ～ 1024 です。ただし、CSS では、バージョン 5.00 との下位互換性を維持するために、512 ～ 32768 の値を入力することができます。1024 を超える値を入力した場合、値はデフォルトの 768 に変更されます。CSS を再度ブートしたときに、有効な範囲を知らせる次のエラー メッセージが表示されます。

```
NETMAN-3: sshd: Bad server key size <configured value>; range 512 to
1024; defaulting to 768
```

たとえば、サーバ キーのビット数を 1024 に設定するには、次のように入力します。

```
(config)# sshd server-keybits 1024
```

ビット数をデフォルトの 768 に戻すには、次のように入力します。

```
(config)# no sshd server-keybits
```

SSHD バージョンの設定

デフォルトでは、CSS は SSH v1 と v2 の両プロトコルをサポートします。SSH v1 と v2 をサポートするように CSS を設定するには、**sshd version** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

sshd version v1|v2

キーワードの意味は次のとおりです。

- **v1** ：SSH v1 プロトコルだけをサポートするように CSS を設定
- **v2** ：SSH v2 プロトコルだけをサポートするように CSS を設定

たとえば、SSH v1 プロトコルだけをサポートするように CSS を設定するには、次のように入力します。

```
(config)# sshd version v1
```

SSH v2 プロトコルだけをサポートするように CSS を設定するには、次のように入力します。

```
(config)# sshd version v2
```

SSH v1 と v2 の両プロトコルをサポートするデフォルト設定に CSS をリセットするには、次のように入力します。

```
(config)# no sshd version
```

SSHD を使用する場合の Telnet アクセスの設定

デフォルトでは、CSS への Telnet アクセスが有効に設定されています。SSHD を使用する場合は、CSS への 安全でない Telnet アクセスを無効にすることができます。SSHD 使用時のセキュリティ強化のため、Telnet アクセスを無効にすることをお勧めします。CSS への Telnet アクセスを無効にするには、グローバルな **restrict telnet** コマンドを使用します。

Telenet アクセスを無効にするには、次のように入力します。

```
(config)# restrict telnet
```

CSS への Telnet アクセスを有効に戻すには、次のコマンドを入力します。

```
(config)# no restrict telnet
```

SSHD 設定の表示

SSHD の設定を表示するには、**show sshd** コマンドを使用します。このコマンドには、次のオプションがあります。

- **show sshd config** ：SSHD の設定を表示する。
- **show sshd sessions** ：現在アクティブな SSHD サーバ セッションの要約を表示する。このコマンドでは、SSH クライアントが設定されている場合だけ、データが表示されます。
- **show sshd version** ：CSS で現在動作中の SSHield パッケージを表示する。

SSHD 設定を表示するには、次のように入力します。

```
# show sshd config
```

表 2-1 に、**show radius config** コマンドで表示されるフィールドを示します。

表 2-1　show sshd config コマンドのフィールド

フィールド	説明
Maximum Sessions Allowed	同時に実行できる SSHD セッションの最大数（最大 5 セッション）
Active Sessions	現在アクティブな SSHD セッションの数
Log Level	現在のログ レベル
Listen Socket Count	SSHD が現在監視しているソケットの数。このバージョンでは設定できません。デフォルト値は 1 です。
Listen Port	SSHD がクライアントとの接続の監視に使用するポート番号。ポート番号を指定するには、**sshd port** コマンドを使用します。デフォルト値（SSH 用のデフォルト ポート）は 22 です。指定できるポート番号は、22、または 512 ～ 65535 の値です。
Listen Address	SSHD がクライアントの接続の監視に使用するアドレス。このバージョンでは設定できません。デフォルト値は 0.0.0.0 です。

表 2-1　show sshd config コマンドのフィールド（続き）

フィールド	説明
Server Key Bits	SSHv1 サーバ キーの生成に使用するサーバ キーのビット数。デフォルトは 768 です。範囲は 512 ～ 1024 です。
RSA Protocol (SSH1)	SSHv1 アクセスの状態。このバージョンでは設定できません。デフォルトで有効に設定されています。
Empty Passwords	使用不可。ユーザ名には、必ずパスワードを関連付ける必要があります。
Keepalive	クライアントへの TCP キープアライブ送信の状態（Enabled または Disabled）。SSHD キープアライブは、デフォルトで有効に設定されています。
SSH2 Cipher List	クライアントとサーバの間で認証、暗号化、およびデータ保全性の確保に使用される SSHv2 暗号スイートのリスト

SSHD セッションを表示するには、次のように入力します。

```
# show sshd sessions
```

表 2-2 に、**show sshd sessions** コマンドで表示されるフィールドを示します。

表 2-2　show sshd sessions コマンドのフィールド

フィールド	説明
Session_ID	セッションの ID
Conn_TID	接続を処理する SSHD サーバの接続タスク ID（tSshConn）
Login_TID	接続を処理するログイン タスク ID （tSshCli）
PTY_FD	ログイン タスクが CSS CLI とやり取りするために使用するファイル記述子。 PTY_FD ファイル記述子を使用すると、SSH クライアント セッションを、**show lines** コマンドの実行結果で Line フィールドに表示されるセッションと関連させることができます。たとえば、**show sshd sessions** コマンドを実行すると、PTY_FD32 に関連する SSH クライアント セッションが表示されます。**show lines** コマンドを入力すると、sshc32 （SSH クライアントの場合は pty_fd32）を含む行が表示されます。この関係によって、**show lines** コマンドで、SSH セッションのログイン時刻、アイドル時間、およびクライアントの場所を確認できます。
Remote IP/Remote Port	SSHD セッションのリモート IP とポート番号

SSHD バージョンを表示するには、次のように入力します。

```
# show sshd version
SSHield version 1.5, SSH version OpenSSH_3.0.2p1
```

CHAPTER 3

RADIUS サーバのクライアントとしての CSS の設定

Remote Authentication Dial-In User Service（RADIUS）プロトコルは、不正なアクセスからネットワークを保護する、分散型のクライアント サーバ プロトコルです。RADIUS では、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用して、CSS 認証クライアントと、ユーザ認証およびネットワーク サービス アクセス情報をすべて格納しているアクティブな認証サーバとの間で認証情報と設定情報を交換します。通常、RADIUS ホストは、RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。

ユーザが、RADIUS クライアントとして稼働中の CSS にリモートからログインすると、CSS は認証要求（ユーザ名、暗号化パスワード、クライアントの IP アドレス、およびポート ID）を中央の RADIUS サーバに送信します。RADIUS サーバは、ユーザ接続要求の受信、ユーザの認証、およびクライアントでユーザにサービスを提供するために必要な設定情報の返信を行います。RADIUS クライアントと RADIUS サーバの間でのやりとりは、共有秘密情報を使用して認証されます。

RADIUS サーバは、認証要求を受信すると、送信側のクライアントを確認してログイン要求と一致するユーザのデータベースを調べます。一定時間内に RADIUS サーバから応答が得られない場合は、事前定義されている回数だけ認証要求が再送信されます。プライマリ サーバが停止した場合やサーバに到達できない場合、RADIUS クライアントは要求を代わりのセカンダリ RADIUS サーバに転送できます。

プライマリ RADIUS サーバとセカンダリ RADIUS サーバの両方が指定された設定では、どちらか一方または両方の RADIUS サーバが到達不可能になると、CSS は自動的にキープアライブ認証要求を送信して、サーバに問い合せます。CSS は、（RADIUS サーバのキーで暗号化された）ユーザ名「query」とパスワード「areyouup」を RADIUS サーバに送信し、サーバの状態を確認します。CSS は、RADIUS サーバが使用可能になるまで、キープアライブ認証要求を送り続けます。

RADIUS サーバ ホスト（プライマリ RADIUS サーバ、およびオプションでセカンダリ RADIUS サーバ）、通信時間間隔の設定、および共有秘密情報テキスト文字列を指定するには、**radius-server** コマンドとそのオプションを使用します。このコマンドは、グローバル設定モードで実行できます。

この章の主な内容は次のとおりです。

- RADIUS 設定のクイック スタート
- CSS で使用するための RADIUS サーバの設定
- プライマリ RADIUS サーバの指定
- セカンダリ RADIUS サーバの指定
- RADIUS サーバのタイムアウトの設定
- RADIUS サーバの再送信回数の設定
- RADIUS サーバのデッドタイムの設定
- RADIUS サーバ設定情報の表示

RADIUS サーバを設定した後に、**virtual authentication** コマンドと **console authentication** コマンドを使用して、コンソール ログインと仮想ログイン（ユーザ名とパスワードのペアがローカル ユーザのデータベースに存在しない場合）での RADIUS 認証を有効にします。この 2 つのコマンドの詳細については、第 1 章「CSS のアクセス制御」を参照してください。

RADIUS 設定のクイック スタート

表 3-1 に、CSS に RADIUS 機能を設定するために必要な手順の概要を説明します。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドの各機能とすべてのオプションの詳細については、次の表の後に示す各項目を参照してください。

表 3-1　RADIUS 設定のクイック スタート

作業とコマンドの例
1. Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）で Cisco Secure ACS の認証を設定し、次のフィールドに入力します。 • **AAA Client Hostname** • **AAA Client IP Address** • **Key** • **Authenticate Using** 「認証の設定」を参照してください。
2. CSS にアクセスするユーザの権限レベルを決定するために、RADIUS サーバにユーザ アカウントを設定します。「権限付与の設定」を参照してください。
3. **radius-server primary** コマンドを使用して、CSS RADIUS クライアントからのユーザ情報の認証（コンソール認証または仮想認証）に使用するするプライマリ RADIUS サーバを指定します。「プライマリ RADIUS サーバの指定」を参照してください。 `(config)# radius-server primary 172.27.56.76 secret Hello`
4. **radius-server secondary** コマンドを使用して、CSS RADIUS クライアントからのユーザ情報を認証（コンソール認証または仮想認証）するセカンダリ RADIUS サーバを指定します。「セカンダリ RADIUS サーバの指定」を参照してください。 `(config)# radius-server secondary 172.27.56.79 secret Hello`

表 3-1　RADIUS 設定のクイック スタート（続き）

作業とコマンドの例
5. **virtual authentication** コマンドを使用して、プライマリ、セカンダリ、およびターシャリの仮想認証方式を設定します。第 1 章「CSS のアクセス制御」を参照してください。 `#(config) virtual authentication primary radius`
6. （推奨）**show radius** コマンドを使用して、RADIUS サーバ設定に関する情報および統計情報を表示します。「RADIUS サーバ設定情報の表示」を参照してください。 `(config)# show radius config all` `(config)# show radius statistics all`

次の実行設定例は、表 3-1 で説明したコマンドを入力した結果を示しています。

```
!************************** GLOBAL **************************
  radius-server primary 172.27.56.76 secret Hello auth-port 1645
  radius-server secondary 172.27.56.79 secret Hello auth-port 1645
  virtual authentication primary radius
```

CSS で使用するための RADIUS サーバの設定

ここでは、RADIUS サーバ設定の背景的な情報を説明します。ここで説明する内容は、RADIUS サーバと、RADIUS クライアントとして運用する CSS との間で正しく通信するための指針です。

次の例は、Cisco Secure Access Control Server （ACS）を中央集中型の RADIUS サーバとして CSS とともに使用する場合に推奨する設定です。

認証の設定

Cisco Secure ACS の認証を設定するには、Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）に進み、次のフィールドに入力します。

- **AAA Client Hostname** ：CSS に割り当てる名前を入力する。
- **AAA Client IP Address**：CSS と Cisco Secure ACS との通信設定に応じて CSS イーサネット管理ポートまたは CSS 回線の IP アドレスを入力する。
- **Key** ：CSS と Cisco Secure ACS でトランザクションの認証に使用する共有秘密情報を入力する。正しく動作させるには、CSS と Cisco Secure ACS で同一の共有秘密情報を入力する必要があります。このキーは、大文字と小文字を区別します。
- **Authenticate Using** ：CSS で標準の IETF RADIUS アトリビュートを使用するために、**RADIUS（IETF）**ネットワーク セキュリティ プロトコルを選択する。

権限付与の設定

CSS にアクセスするユーザの権限レベルを決定するために、RADIUS サーバにユーザ アカウントを設定する必要があります。

グループ権限を設定するには、次の操作を実行します。

1. Cisco Secure ACS HTML インターフェイスの **Group Setup** セクション（**Group Setup Select** ページ）で、RADIUS 設定を指定するグループを選択します。

2. Cisco Secure ACS HTML インターフェイスの **Group Settings** セクションで、**IETF RADIUS Attributes, [006] Service-Type** チェックボックスをクリックします。次に **Administrative** を選択します。CSS への特権ユーザ（スーパーユーザ）接続に対する RADIUS 認証を有効にするには、**Administrative** を有効にする必要があります。

グループにユーザを追加するには、Cisco Secure ACS HTML インターフェイスの **User Setup** セクションに進みます。

- **User Setup Select** ページでユーザ名を指定します。
- **User Setup Edit** ページで次のように指定します。
  - **Password Authentication** ：リストから適切な認証タイプを選択する。
  - **Password** ：パスワードと確認用パスワードを入力する。
  - **Group**：事前に作成した RADIUS グループを選択してユーザを割り当てる。

プライマリ RADIUS サーバの指定

CSS RADIUS クライアントからのユーザ情報の認証（コンソール認証または仮想認証）に使用するするプライマリ RADIUS サーバを指定するには、**radius-server primary** コマンドを使用します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

radius-server primary *ip_address* **secret** *string* {**auth-port** *port_number*}

このコマンドのオプションと変数は次のとおりです。

- **primary** *ip_address*：プライマリ RADIUS サーバの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（たとえば、192.168.11.1）またはニーモニック ホスト名（たとえば、myhost.mydomain.com）で入力します。
- **secret** *string* ：プライマリ RADIUS サーバと CSS RADIUS クライアント間の共有秘密情報文字列。共有秘密情報により、クライアントとプライマリ RADIUS サーバの間で認証トランザクションを行うことができます。共有秘密情報は、大文字と小文字を区別したスペースを含まない 16 文字以内の文字列で入力します。
- **auth-port** *port_number*：（オプション）RADIUS クライアントから認証パケットを受信するために割り当てられたプライマリ RADIUS サーバの UDP ポート。有効な入力値は 0 ～ 65535 です。デフォルトは 1645 です。

プライマリ RADIUS サーバを指定するには、次のように入力します。

```
(config)# radius-server primary 172.27.56.76 secret Hello auth-port
30658
```

プライマリ RADIUS サーバを削除するには、次のように入力します。

```
(config)# no radius-server primary
```

セカンダリ RADIUS サーバの指定

CSS は、指定したプライマリ RADIUS サーバが使用できない場合に、認証要求をセカンダリ RADIUS サーバに送信します。CSS RADIUS クライアントからのユーザ情報を認証（コンソール認証または仮想認証）するセカンダリ RADIUS サーバを指定するには、**radius-server secondary** コマンドを使用します。

（注） セカンダリ RADIUS サーバの設定は省略可能です。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

radius-server secondary *ip_address* **secret** *string* {**auth-port** *port_number*}

このコマンドのオプションと変数は次のとおりです。

- **secondary** *ip_address* ：セカンダリ RADIUS サーバの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（たとえば、192.168.11.1）またはニーモニック ホスト名（たとえば、myhost.mydomain.com）で入力します。
- **secret** *string* ：セカンダリ RADIUS サーバと CSS RADIUS クライアントの間の共有秘密情報文字列。共有秘密情報により、クライアントとセカンダリ RADIUS サーバの間で認証トランザクションを行うことができます。共有秘密情報は、大文字と小文字を区別したスペースを含まない 16 文字以内の文字列で入力します。
- **auth-port** *port_number* ：（オプション）RADIUS クライアントから認証パケットを受信するために割り当てられたセカンダリ RADIUS サーバの UDP ポート。有効な入力値は 0 ～ 65535 です。デフォルトは 1645 です。

セカンダリ RADIUS サーバを指定するには、次のように入力します。

```
(config) radius-server secondary 172.27.56.79 secret Hello auth-port
30658
```

セカンダリ RADIUS サーバを削除するには、次のように入力します。

```
(config)# no radius-server secondary
```

RADIUS サーバのタイムアウトの設定

CSS は、デフォルトで、RADIUS サーバ（プライマリまたはセカンダリ）への認証要求を再送信するまでに、RADIUS サーバからの応答を 10 秒待機します。CSS で認証応答の待機を開始してから RADIUS サーバ（プライマリまたはセカンダリ）へ要求を再送信するまでの時間間隔を指定するには、**radius-server timeout** コマンドを使用します。サーバへの要求の再送信回数を設定するには、**radius-server retransmit** コマンドを使用します（「RADIUS サーバの再送信回数の設定」を参照）。有効な入力値は、1 ～ 255 秒です。

たとえば、RADIUS サーバのタイムアウト間隔を 1 分（60 秒）に設定するには、次のように入力します。

```
(config)# radius-server timeout 60
```

RADIUS サーバの再送信要求間隔をデフォルトの 10 秒にリセットするには、次のコマンドを実行します。

```
(config)# no radius-server timeout
```

RADIUS サーバの再送信回数の設定

CSS は、デフォルトで、タイムアウトした RADIUS サーバへの認証要求の再送信を 3 回行った後、サーバが停止しているものと判断して送信を停止します。タイムアウトした RADIUS サーバへの認証要求の再送信を開始してから、サーバが停止しているものと判断して送信を停止するまでの再送信回数を指定するには、**radius-server retransmit** コマンドを使用します。セカンダリ RADIUS サーバが確認されると、そのサーバがアクティブ サーバとして選択されます。有効な入力値は、1 ～ 30 回です。

RADIUS サーバが要求を再送信した CSS に応答しない場合、その RADIUS サーバは停止したものとみなされ、送信が停止されます。また、この時点から **radius-server dead-time** コマンドで定義したデッド タイマーが起動します（「RADIUS サーバのデッドタイムの設定」を参照）。セカンダリ サーバが設定されている場合、CSS はそのセカンダリ サーバに要求を送信します。セカンダリ サーバが要求に応答しなければ、サーバ停止と判断してデッド タイマーを開始します。アクティブなサーバがない場合は、RADIUS プライマリ サーバが有効になるまで、要求の送信は停止します。

たとえば、RADIUS サーバの再送信回数を 5 回に設定するには、次のように入力します。

```
(config)# radius-server retransmit 5
```

RADIUS サーバの要求の再送信回数をデフォルトの 3 回にリセットするには、次のコマンドを実行します。

```
(config)# no radius-server retransmit
```

RADIUS サーバのデッドタイムの設定

CSS は、デッドタイム時間内にプローブ アクセス要求パケットを送信して、RADIUS サーバ（プライマリまたはセカンダリ）が使用できるかどうか、および認証要求を受信できるかどうかを確認します。デッドタイム間隔は、サーバが応答せずに、認証要求の再送信が **radius-server retransmit** コマンドを使って設定した回数に達した時点から開始されます。サーバがプローブ アクセス要求パケットに応答すると、CSS は認証要求をサーバに送信します。

応答がないサーバが動作中であるかどうかを確認する時間間隔を設定するには、**radius-server dead-time** コマンドを使用します。有効な入力値は、1 ～ 255 秒です。デフォルトは 5 秒に設定されています。

プローブ アクセス要求を有効にして、RADIUS サーバのデッドタイムを 15 秒に設定するには、次のように入力します。

```
(config)# radius-server dead-time 15
```

RADIUS サーバのデッドタイムをデフォルトの 5 秒にリセットするには、次のように入力します。

```
(config)# no radius-server dead-time
```

RADIUS サーバ設定情報の表示

RADIUS サーバ設定に関する情報および統計情報を表示するには、**show radius** コマンドを使用します。このコマンドのシンタックスとオプションは次のとおりです。

- **show radius config** [**all**|**primary**|**secondary**] ：タイプで識別される特定のサーバ、またはすべてのサーバの RADIUS 設定情報を表示する。
- **show radius statistics** [**all**|**primary**|**secondary**] ：タイプで識別される特定のサーバ、またはすべてのサーバの RADIUS 認証統計情報を表示する。

プライマリ RADIUS サーバの設定を表示するには、次のように入力します。

```
(config)# show radius config primary
```

セカンダリ RADIUS サーバの認証統計情報を表示するには、次のように入力します。

```
(config)# show radius statistics secondary
```

表 3-2 に、**show radius config** コマンドで表示されるフィールドを示します。

表 3-2　show radius config コマンドのフィールド

フィールド	説明
Server IP Address	指定された RADIUS サーバの IP アドレスまたはホスト名
Secret	指定された RADIUS サーバと CSS RADIUS クライアントの間の共有秘密情報
Port	指定された RADIUS サーバで CSS RADIUS クライアントから認証パケットを受信するために割り当てられた UDP ポート。デフォルトのポート番号は 1645 です。
State	RADIUS サーバの稼働状態（ALIVE、DOWN、UNKNOWN）
Dead Timer	応答しない RADIUS サーバ（プライマリまたはセカンダリ）を CSS がプローブして、稼働しているかどうか、また認証要求を受信できるかどうかを確認する間隔（秒単位）

表 3-2　show radius config コマンドのフィールド（続き）

フィールド	説明
Timeout	CSS RADIUS クライアントが RADIUS サーバからの応答の待機を開始してから、そのサーバへ要求を再送信するまでの間隔（秒単位）
Retransmit Limit	CSS RADIUS クライアントが、タイムアウトした RADIUS サーバへ認証要求の再送信を開始してから、そのサーバへの送信を停止するまでの再送信回数
Probes	RADIUS サーバが利用可能かどうか、およびそのサーバで認証要求を受信できるかどうかを判断する手段として、CSS RADIUS クライアントから自動的に送信されるパケット

表 3-3 に、**show radius statistics** コマンドで表示されるフィールドを示します。

表 3-3　show radius statistics コマンドのフィールド

フィールド	説明
Server IP address	指定された RADIUS サーバの IP アドレスまたはホスト名
Accepts	RADIUS サーバが CSS RADIUS クライアントからの認証要求を受け付けた回数
Requests	CSS RADIUS クライアントが RADIUS サーバへ認証要求を実行した回数
Retransmits	CSS RADIUS クライアントが、タイムアウトが発生した後にアクティブな RADIUS サーバへ認証要求を再送信した回数
Rejects	CSS RADIUS クライアントが認証要求を確立しようとしている間に RADIUS サーバから拒否通知を受信した回数
Bad Responses	CSS RADIUS クライアントが RADIUS サーバから不正な送信を受信した回数
Bad Authenticators	RADIUS サーバが CSS RADIUS クライアントからの認証要求を拒否した回数
Pending Requests	RADIUS サーバに対して保留中の認証要求の数
Timeouts	CSS RADIUS クライアントが、認証要求に対する RADIUS サーバからの応答を待機している間に指定されているタイムアウト間隔に達した回数
Discarded Authentication Requests	プライマリまたはセカンダリの RADIUS サーバが停止している間に破棄された認証要求数

CHAPTER 4

TACACS+ サーバのクライアントとしての CSS の設定

Terminal Access Controller Access Control System （TACACS+）プロトコルを使用すると、ルータ、network access server（NAS; ネットワーク アクセス サーバ）などのデバイスで、デーモン サーバ経由のアクセスを制御できます。TACACS+ は、NAS とデーモン サーバの間のトラフィックを TCP 通信によってすべて暗号化して、送信内容を保護します。

CSS を TACACS+ サーバのクライアントとして設定し、ユーザ認証の方法、また、設定コマンドやその他のコマンドの権限の付与とアカウンティングの方法とすることもできます。

この章の主な内容は次のとおりです。

- TACACS+ 設定のクイック スタート
- CSS で使用する TACACS+ サーバのユーザ アカウントの設定
- グローバルな TACACS+ アトリビュートの設定
- TACACS+ サーバの定義
- TACACS+ 権限付与の設定
- TACACS+ アカウンティングの設定
- TACACS+ サーバの設定情報の表示

CSS で TACACS+ サーバを設定した後で、仮想認証またはコンソール認証用に TACACS+ 認証を設定します。詳細については、第 1 章「CSS のアクセス制御」を参照してください。

TACACS+ 設定のクイック スタート

表 4-1 に、CSS に TACACS+ 機能を設定するために必要な手順の概要を説明します。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドに関する各機能とすべてのオプションの詳細については、この手順の後に示す各項を参照してください。

表 4-1　TACACS+ 設定のクイック スタート

作業とコマンドの例
1. Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）で Cisco Secure ACS の認証を設定し、次のフィールドに入力します。 • **AAA Client Hostname** • **AAA Client IP Address** • **Key** • **Authenticate Using** 「認証の設定」を参照してください。
2. CSS　にアクセスするユーザの権限レベルを決定するために、TACACS+ サーバにユーザ アカウントを設定します。「権限付与の設定」を参照してください。
3. （オプション）TACACS+　サーバで使用するグローバルなタイムアウト、キープアライブの間隔、または暗号キーのアトリビュートを設定する場合は、サーバを設定する前にこれらのパラメータを設定する必要があります。グローバルな TACACS+ アトリビュート設定の詳細については、「グローバルな TACACS+ アトリビュートの設定」を参照してください。
4. **tacacs-server** コマンドを使用して、サーバを定義します。このコマンドには、サーバの IP アドレスとポート番号を指定します。オプションで、特定のタイムアウト時間、暗号キーまたはキープアライブ間隔を定義して、このサーバをプライマリ サーバに指定できます。「TACACS+ サーバの定義」を参照してください。 `(config)# tacacs-server 192.168.11.1 12 20 “summary” primary frequency 10`

表 4-1　TACACS+ 設定のクイック スタート（続き）

作業とコマンドの例
5. **virtual authentication** コマンドを使用して、プライマリ、セカンダリ、およびターシャリの仮想認証方式を設定します。 `#(config)` **`virtual authentication primary tacacs`**
6. （推奨）TACACS+ サーバの設定を検証します。「TACACS+ サーバの設定情報の表示」を参照してください。 `(config)#` **`show tacacs-server`**

次の実行設定例は、表 4-1 のコマンドの入力結果を表しています。

```
!************************* GLOBAL ************************
virtual authentication primary tacacs
tacacs-server 192.168.11.1 12 20 6dab4b3gibcbef3e primary frequency 10
```

CSS で使用する TACACS+ サーバのユーザ アカウントの設定

ここでは、TACACS+ サーバ設定の背景的な情報を説明します。ここで説明する内容は、TACACS+ サーバと、TACACS+ クライアントとして運用する CSS との間で正しく通信するための指針です。

ここでは、Cisco Secure Access Control Server （ACS）TACACS+ のユーザ認証と権限付与に関する推奨設定を説明します。

認証の設定

Cisco Secure ACS の認証を設定するには、Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）に進み、次のフィールドに入力します。

- **AAA Client Hostname**：CSS に割り当てる名前を入力する。
- **AAA Client IP Address**：CSS と Cisco Secure ACS との通信設定に応じて CSS イーサネット管理ポートまたは CSS 回線の IP アドレスを入力する。
- **Key** ：CSS と Cisco Secure ACS でトランザクションの認証に使用する共有秘密情報を入力する。正しく動作させるには、CSS と Cisco Secure ACS で同一の共有秘密情報を入力する必要があります。このキーは、大文字と小文字を区別します。
- **Authenticate Using** ：**TACACS+ (Cisco IOS)** を選択する。

権限付与の設定

CSS にアクセスするユーザの特権レベルを決定するために、**privilege** コマンドの実行を許可するか、または拒否するかを、TACACS+ サーバのユーザ アカウントに設定する必要があります。CSS は、**privilege** コマンドの実行権限があるかどうか TACACS+ サーバに照会します。**privilege** コマンドの実行をサーバから許可された場合は、CSS へのアクセス特権（SuperUser モードおよび設定モード）がユーザに認められます。**privilege** コマンドの実行がサーバから拒否された場合は、CSS へのアクセス特権以外のアクセス権限（User モード）がユーザに認められます。

グループ権限付与を設定するには、次の操作を実行します。

1. Cisco Secure ACS HTML インターフェイスの **Group Setup** セクション（**Group Setup Select** ページ）から、TACACS+ 設定を指定するグループを選択します。
2. **Shell Command Authorization Set** ページで、**Per Group Command Authorization** のチェックボックスをクリックします。
3. **Unmatched Cisco IOS Commands** で、privilege コマンドの実行を許可または拒否するように設定します。
   - CSS で SuperUser 特権を持つグループには、**Permit** を選択します。SuperUser は、すべての CSS コマンドを実行できます。
   - CSS で User 権限を持つグループには、**Deny** を選択します。User 権限を持つユーザは、CSS の設定を変更しない CSS コマンド（**show** コマンドなど）を実行できます。

また、次の方法で、グループ認証を設定することもできます。

1. **Shared Profile Components**（**Shell Command Authorization Sets** ページ）を選択します。
2. **Add** ボタンをクリックしてセットを追加するか、または既存のセットを編集します。
3. 名前と説明を入力します。
4. **Unmatched Commands** の隣に移動し、privilege コマンドの実行を許可または拒否するように設定します。
   - CSS で SuperUser 特権を持つユーザには、**Permit** を選択します。SuperUser は、すべての CSS コマンドを実行できます。
   - CSS で User 特権を持つユーザには、**Deny** を選択します。User 権限を持つユーザは、CSS の設定を変更しない CSS コマンド（**show** コマンドなど）を実行できます。
5. **Group Setup Select** ページの **Group Setup** セクションから、TACACS+ 設定を指定するグループを選択します。
6. **Shell Command Authorization Set** セクションで **Assign a Shell Command Authorization Set for any network device** を選択します。
7. リストからセットを選択します。

グループにユーザを追加するには、Cisco Secure ACS HTML インターフェイスの **User Setup** セクションに進みます。

- **User Setup Select** ページでユーザ名を指定します。
- **User Setup Edit** ページで次のように指定します。
  - **Password Authentication** ：リストから適切な認証タイプを選択する。
  - **Password** ：パスワードと確認用パスワードを入力する。
  - **Group**：事前に作成した TACACS+ グループを選択してユーザを割り当てる。

グローバルな TACACS+ アトリビュートの設定

TACACS+ のタイムアウト時間、暗号キー、およびキープアライブ間隔にはそれぞれデフォルト値があり、TACACS+ サーバにはそれらのデフォルト値が適用されます。サーバの設定時に、これらのアトリビュートをサーバに固有な値に設定することも、サーバに固有な値は設定せず、デフォルト値を使用することもできます。これらのグローバルなアトリビュートのデフォルト値はすべて変更できます。ここでは、次の内容について説明します。

- グローバルな CSS TACACS+ タイムアウト時間の設定
- グローバルな暗号キーの定義
- グローバルな TACACS+ キープアライブ間隔の設定

（注） TACACS+ サーバの設定時に定義したタイムアウト、暗号キー、キープアライブ間隔は、グローバルなアトリビュートより優先されます（「TACACS+ サーバの定義」参照）。

グローバルな CSS TACACS+ タイムアウト時間の設定

CSS では、設定したすべての TACACS+ サーバで使用するグローバルな TACACS+ タイムアウト時間を定義できます。TACACS+ サーバが使用可能かどうかを判断するために、CSS から TACACS+ サーバに TCP キープアライブ プローブが定期的に送信されます。タイムアウト時間内にサーバがプローブに応答しない場合、CSS ではサーバが使用不能と判断されます。

CSS は、サーバとの通信を試みても、定義されているタイムアウト値以内に応答を得られなかった場合、別のサーバを使用します。設定されている次のサーバとの通信が試みられ、同じ処理が繰り返されます。別の（または 3 つ目）の TACACS+ サーバが認識されている場合は、そのサーバがアクティブなサーバとして選択されます。

CSS から 3 つの TACACS+ サーバのすべてに接続できない場合は、ユーザ認証が実行されず、ユーザは CSS にログインできません。ただし、**virtual** コマンドまたは **console** コマンドを実行して、TACACS+ サーバと RADIUS サーバ（またはローカル サーバ）を併用するように定義している場合を除きます。この 2 つのコマンドの詳細については、第 1 章「CSS のアクセス制御」を参照してください。

タイムアウト時間を変更するには、**tacacs-server timeout** コマンドを使用します。有効な入力値は 1 ～ 255 で、デフォルトは 5 秒です。変更されたグローバルなタイムアウト時間は動的に適用され、新しい値は次の TACACS+ 接続にも自動的に適用されます。

たとえば、タイムアウト時間を 60 秒に設定するには、次のように入力します。

```
#(config) tacacs-server timeout 60
```

タイムアウト時間をデフォルトの 5 秒にリセットするには、次のように入力します。

```
#(config) no tacacs-server timeout
```

（注） TACACS+ サーバの指定時に設定したタイムアウト時間は、グローバルなタイムアウト時間より優先されます（「TACACS+ サーバの定義」参照）。

グローバルな暗号キーの定義

CSS では、設定したすべての TACACS+ サーバとの通信に使用するグローバルな暗号キーを定義できます。CSS と TACACS+ サーバの間の TACACS+ パケット トランザクションを暗号化するには、暗号キーを定義する必要があります。暗号キーを定義しない場合は、パケットは暗号化されません。このキーは、共有秘密情報の値であり、TACACS+ サーバに保存される値と同じになります。CSS とサーバの間の共有秘密情報を指定するには、**tacacs-server key** コマンドを使用します。

共有秘密キーを入力する場合は、クリア テキストを引用符で囲んで入力するか、または、DES 暗号化秘密キーを入力します。クリア テキスト キーは、実行設定に入力される前に DES で暗号化されます。どちらのキーも 100 文字以内で入力します。変更されたキーは動的に適用され、新しい値は次の TACACS+ 接続にも自動的に適用されます。

たとえば、クリア テキスト キーを定義するには、次のように入力します。

```
#(config) tacacs-server key “market”
```

DES 暗号キーを定義するには、次のように入力します。

```
#(config) tacacs-server key acskefterefesdtx
```

キーを削除するには、次のように入力します。

```
#(config) no tacacs-server key
```

（注） TACACS+ サーバの指定時に設定した共有秘密情報は、グローバルな暗号キーより優先されます（「TACACS+ サーバの定義」参照）。

グローバルな TACACS+ キープアライブ間隔の設定

CSS では、設定したすべての TACACS+ サーバで使用するグローバルな TACACS+ キープアライブ間隔を定義できます。TACACS+ サーバが使用可能かどうかを判断するために、CSS から TACACS+ サーバに TCP キープアライブ プローブが定期的に送信されます。設定されたタイムアウト時間内にサーバがプローブに応答しない場合、CSS ではサーバが使用不能と判断されます。

TACACS+ サーバにキープアライブを送信する場合、CSS はサーバとの固定接続を使用しようとします。サーバに固定接続が設定されていない場合、CSS はキープアライブを送信するたびに新しい接続を開きます。

グローバルな TACACS+ キープアライブ間隔を設定するには、グローバル設定モードで **tacacs-server frequency** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

tacacs-server frequency *number*

number 変数は、キープアライブ間隔を秒単位で定義します。0 ～ 255 の整数を入力します。デフォルトは 5 秒です。0 に設定するとキープアライブは無効になります。変更されたキープアライブ間隔は動的に適用され、ただちに新しい値でキープアライブが再開されます。

たとえば、グローバルな TACACS+ キープアライブ間隔を 50 秒に設定するには、次のように入力します。

```
(config)# no tacacs-server frequency 50
```

（注） TACACS+ サーバの指定時に設定したキープアライブ間隔は、グローバルなキープアライブ間隔より優先されます（「TACACS+ サーバの定義」参照）。

グローバルな TACACS+ キープアライブ間隔をデフォルトの 5 秒にリセットするには、**no tacacs-server frequency** コマンドを使用します。

たとえば、次のように入力します。

```
(config)# no tacacs-server frequency
```

TACACS+ サーバの定義

TACACS+ サーバには、TACACS+ の認証情報、権限付与情報、およびアカウンティング データベースが保存されています。CSS には、最大 3 つのサーバを設定できます。ただし、一度に使用できるサーバは 1 つだけです。CSS は、設定されたプライマリ サーバを優先して、利用できるサーバを選択します。CSS からは、定期的に TCP キープアライブ プローブが 5 秒ごとに TACACS+ サーバに送信され、運用状態（Alive、Dying、または Dead）が確認されます。CSS では、TCP キープアライブの間隔を設定できません。

（注） 推奨される TACACS+ サーバ（この例では Cisco Secure Access Control Server）設定の概要については、「TACACS+ 設定のクイック スタート」を参照してください。

タイムアウト時間、キープアライブ間隔、または共有秘密情報などの TACACS+ のグローバルなアトリビュートを TACACS+ サーバに適用するには、グローバルなアトリビュートを設定してからサーバを設定します。変更したグローバルなアトリビュートを設定済みの CSS TACACS+ サーバに適用する場合は、サーバを削除してから再設定してください。

サーバを定義するには、**tacacs-server** コマンドを使用します。このコマンドには、サーバの IP アドレスとポート番号を指定します。オプションで、タイムアウト時間と暗号キーを定義して、このサーバをプライマリ サーバに指定できます。

このグローバル設定コマンドのシンタックスは次のとおりです。

tacacs-server *ip_address port* {*timeout* [**“***cleartext_key***”**|*des_key*]} {**primary**} {**frequency** *number*}

このコマンドの変数とオプションは次のとおりです。

- *ip_address* ：TACACS+ サーバの IP アドレス。IP アドレスはドット付き 10 進表記で入力します。
- *port* ：TACACS+ サーバの TCP ポート。デフォルトのポートは 49 です。1 ～ 65535 のポート番号を入力できます。

- *timeout* ：（オプション）サーバからの応答を待つ時間。有効な入力値は 1 ～ 255 で、デフォルトは 5 秒です。このオプションを定義すると、**tacacs-server timeout** コマンドが無効になります。TACACS+ のタイムアウト時間とグローバルなタイムアウト設定の詳細については「グローバルな CSS TACACS+ タイムアウト時間の設定」を参照してください。
- **“***cleartext_key***”|***des_key* ：（オプション）CSS とサーバの間の共有秘密情報。CSS と TACACS+ サーバの間の TACACS+ パケット トランザクションを暗号化するには、暗号キーを定義する必要があります。暗号キーを定義しない場合は、パケットは暗号化されません。

  この共有秘密情報の値は、TACACS+ サーバに保存されている値と同じです。共有秘密キーを入力する場合は、クリア テキストを引用符で囲んで入力するか、または、DES 暗号化秘密キーを引用符で囲まずに入力します。クリア テキスト キーは、実行設定に入力される前に DES で暗号化されます。どちらのキーも 100 文字以内で入力します。

  このオプションを定義すると、**tacacs-server key** コマンドが無効になります。グローバルな暗号キーの定義については、「グローバルな暗号キーの定義」を参照してください。
- **primary** ：（オプション）この TACACS+ サーバの優先度を、設定されている他のサーバよりも高く設定する。指定できるプライマリ サーバは、1 つだけです。
- **frequency** *number* ：（オプション）指定された TACACS+ サーバにキープアライブ間隔を設定できるようにする。デフォルトの number 変数は 5 秒です。この変数の範囲は 0 ～ 255 です。0 に設定するとキープアライブは無効になります。このオプションを定義すると、**tacacs-server frequency** コマンドが無効になります。

（注） 特定のサーバのタイムアウト時間や共有秘密情報を変更する場合は、サーバを削除してから、新しいパラメータで再度定義してください。

たとえば、IP アドレスが 192.168.11.1、デフォルト ポートが 49、タイムアウト時間が 12 秒、クリア テキストの共有秘密情報が「summary」、キープアライブ間隔が 10 秒である TACACS+ サーバをプライマリ TACACS+ サーバとして指定するには、次のように入力します。

```
#(config) tacacs-server 192.168.11.1 12 20 “summary” primary frequency 10
```

IP アドレスが 192.168.11.1 でデフォルト ポートが 49 の TACACS+ サーバを削除するには、次のように入力します。

```
#(config) no tacacs-server 192.168.11.1 49
```

TACACS+ サーバを設定した後に、**virtual authentication** コマンドと **console authentication** コマンドを使用して、コンソール ログインと仮想ログイン（ユーザ名とパスワードのペアがローカル ユーザのデータベースに存在しない場合）での TACACS+ 認証を有効にします。この 2 つのコマンドの詳細については、第 1 章「CSS のアクセス制御」を参照してください。

TACACS+ 権限付与の設定

TACACS+ 権限付与を設定すると、ユーザが実行できる CSS コマンドを TACACS+ サーバで個別に制御できます。CSS の権限付与では、コマンド セットが次の 2 種類に分類されます。

- CSS の実行設定を変更するための設定コマンド。たとえば、グローバル設定モードのすべてのコマンドがこのコマンドに該当します。すべてのグローバル設定モード コマンドのリストについては、『*Cisco Content Services Switch Command Reference*』を参照してください。
- 実行設定を変更しない設定用以外のコマンド。これらのコマンドには、モード変更コマンド、表示コマンド、管理コマンドなどが含まれます。たとえば、**cls**（clear screen）、**endbranch**、**help**、**ping**、**show**、**terminal**、**traceroute** などのコマンドがあります。設定用以外のすべてのコマンドのリストについては、『*Cisco Content Services Switch Command Reference*』を参照してください。

（注） CSS に TACACS+ を設定すると、CSS は スクリプトが TACACS+ サーバを通過することを許可しません。CSS はすべての XML コマンドをスクリプトに変換するため、XML コマンドが TACACS+ サーバを通過することも許可しません。

デフォルトでは、権限付与が無効に設定されています。権限付与を有効にすると、試行されたコマンドの実行を許可するか拒否するかが TACACS+ サーバで判断されます。

権限付与を有効にした場合は、TACACS+ サーバと CSS の間の通信によってコマンドの実行が遅延します。TACACS+ サーバに障害が発生すると、すべての権限付与要求が失敗し、ユーザ アクティビティが一時停止します。ただし、別のサーバが接続可能な場合を除きます。この場合にユーザがコマンドを実行できるようにするには、フェールオーバー認証方式をローカル ユーザ データベースに設定します。ユーザは CSS にログインしなおす必要があります。

7.30.1.05 より前のリリースでは、CLI モードの移行時に（設定モードからサービス モードに移る場合など）サービスが存在すると、設定コマンドでもまたは設定以外のコマンドでも、TACACS+ 権限付与が有効になっているかどうかに関係なく、コマンドに対する許可は実行されませんでした。サービスの作成中、設定コマンドの権限付与が有効化されている場合は、TACACS+ サーバに対してユーザにコマンドを実行する権限があるかどうかの照会が行われました。7.30.1.05 以降のソフトウェア バージョンでは、既存のサービス上でモードが移行した場合、設定以外のコマンドが有効化されている場合も、TACACS+ サーバに対してコマンド権限付与要求が送信されます。

実行設定を変更するすべてのコマンドの権限付与を有効にするには、**tacacs-server authorize config** コマンドを使用します。たとえば、次のように入力します。

```
#(config) tacacs-server authorize config
```

実行設定を変更しないすべてのコマンドの権限付与を有効にするには、**tacacs-server authorize non-config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server authorize non-config
```

これらのコマンドに **no** を指定すると、権限付与が無効になります。たとえば、実行設定に影響するコマンドの権限付与を無効にするには、次のように入力します。

```
#(config) no tacacs-server authorize config
```

実行設定に影響しないコマンドの権限付与を無効にするには、次のように入力します。

```
#(config) no tacacs-server authorize non-config
```

TACACS+ サーバへの完全な CSS コマンドの送信

CSS ユーザは、短縮形のシンタックスで入力したコマンドを TACACS+ サーバに送信することができます。デフォルトでは、短縮形でコマンドを入力した場合でも、完全なコマンド シンタックスの形に変換されて送信されます。短縮形のコマンドを完全なシンタックスに変換することにより、TACACS+ 権限付与コマンドが失敗する可能性を減らします。

CSS から完全なコマンドを送らずに、ユーザが入力したとおりにコマンドを送る場合は、コマンドに **no** を指定します。たとえば、次のように入力します。

```
#(config) no tacacs-server send-full-command
```

完全なコマンド シンタックスの送信を再度有効にするには、**tacacs-server send-full-command** コマンドを使用します。たとえば、次のように入力します。

```
#(config) tacacs-server send-full-command
```

TACACS+ アカウンティングの設定

TACACS+ アカウンティングを設定すると、ユーザが実行できるコマンドのアカウンティング レポートを TACACS+ サーバで受信できます。CSS のアカウンティングでは、コマンド セットが次の 2 種類に分類されます。

- CSS の実行設定を変更するための設定コマンド
- 実行設定を変更しない設定用以外のコマンド。これらのコマンドには、モード変更コマンド、表示コマンド、管理コマンドなどが含まれます。

デフォルトでは、CSS のアカウンティングは無効に設定されています。アカウンティングを有効にすると、設定コマンドと非設定コマンドの両方または一方のアカウンティングが可能になります。

(注) TACACS+ サーバに障害が発生しても、ユーザ アクティビティは一時停止しません。

実行設定を変更するすべてのコマンドのアカウンティング レポートを TACACS+ サーバに送信できるようにするには、**tacacs-server account config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server account config
```

実行設定を変更しないすべてのコマンドのアカウンティング レポートを TACACS+ サーバに送信できるようにするには、**tacacs-server account non-config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server account non-config
```

これらのコマンドに **no** を指定すると、アカウンティングが無効になります。たとえば、実行設定に影響するコマンドのアカウンティングを無効にするには、次のように入力します。

```
#(config) no tacacs-server account config
```

実行設定に影響しないコマンドのアカウンティングを無効にするには、次のように入力します。

```
#(config) no tacacs-server account non-config
```

TACACS+ サーバの設定情報の表示

TACACS+ サーバの設定情報を表示するには、**show tacacs-server** コマンドを使用します。この情報を表示するには、次のように入力します。

```
(config)# show tacacs-server
```

表 4-2 に、**show tacacs-server** コマンドで表示されるフィールドを示します。

表 4-2　show tacacs-server コマンドのフィールド

フィールド	説明
IP/Port	TACACS+ サーバの IP アドレスとポート番号
State	内部 TCP キープアライブで判断されるサーバの運用状態（Alive、Dying、または Dead）
Primary	このレコードがプライマリ TACACS+ サーバであるかどうかが表示されます。
Authen	TACACS+ サーバに対する認証要求の数
Author	TACACS+ サーバに対する権限付与要求の数
Account	TACACS+ サーバに対するアカウンティング要求の数
Key	TACACS+ サーバに設定された共有秘密情報
Server Timeout	CSS が TACACS+ サーバからの応答を待機するタイムアウト時間
Server Frequency	TACACS+ サーバのキープアライブ間隔（秒単位）
Global Timeout	CSS が TACACS+ サーバからの応答を待機するグローバルなタイムアウト時間
Global KAL Frequency	TACACS+ サーバのグローバルなキープアライブ間隔（秒単位）

表 4-2　show tacacs-server コマンドのフィールド（続き）

フィールド	説明
Global Key	すべての TACACS+ サーバで使用されるグローバルな共有秘密情報。サーバに対して個別に共有秘密情報が設定されている場合は、個別の共有秘密情報が使用されます。
Authorize Config Commands	設定コマンドが権限付与を受け付けるかどうかが表示されます。
Authorize Non-Config	設定以外のコマンドが権限付与を受け付けるかどうかが表示されます。
Account Config Commands	実行設定を変更するすべてのコマンドのアカウンティング レポートを CSS から TACACS+ サーバに送信するかどうかを示します。
Account Non-Config	実行設定を変更しないすべてのコマンドのアカウンティング レポートを CSS から TACACS+ サーバに送信するかどうかを示します。

CHAPTER 5

ファイアウォール ロード バランシングの設定

この章では、CSS の Firewall Load Balancing （FWLB; ファイアウォール ロード バランシング）機能の設定方法について説明します。この章の記載情報は、特に指示がない限り、CSS の全モデルに共通です。

この章の主な内容は次のとおりです。

FWLB の概要

ファイアウォール ロード バランシング（FWLB）機能を使用すると、1 台の CSS に対して最高 15 個までのファイアウォールを設定することができます。複数のファイアウォールを設定することにより、ファイアウォールの性能が向上し、すべてのトラフィックが単一のファイアウォールだけを通過する場合に発生するシングル ポイント障害を防止できます。FWLB 機能により、CSS は、同じ送信元 IP アドレスと宛先 IP アドレスを持つパケットをすべて必ず同じファイアウォール経由で転送します。この処理は、CSS が送信元 IP アドレスと宛先 IP アドレスに XOR を実行することにより実現されます。

CSS は、ファイアウォールのどちら側にも設置できるため、トラフィックを複数のファイアウォール経由で同時にバランシング処理することができます。各ファイアウォールは、ファイアウォールのロード バランシング アルゴリズムで使用可能です。CSS は、このアルゴリズムで送信元 IP アドレスと宛先 IP アドレスを使用し、各フローに対してどのファイアウォールを使用するかを計算します。

CSS は、ファイアウォールの反対側にあるリモート CSS にカスタムの ICMP キープアライブ要求を毎秒送信して、ファイアウォールの状態を監視します。リモート CSS からキープアライブ要求が 3 ～ 16 秒間（タイムアウト時間は設定可能）届かない場合、CSS はファイアウォール パスが使用不能であると宣言します。各 CSS は、送信側の CSS に応答せず、他の CSS とは全く関係なく独自のキープアライブ要求を毎秒送信します。キープアライブ タイムアウト設定の詳細については、「ファイアウォールのキープアライブ タイムアウトの設定」を参照してください。

FWLB はレイヤ 3 デバイスとして動作します。ファイアウォールへの各接続は、独立した IP サブネットです。1 組の IP アドレス間にあるすべてのフローは、双方向とも同じファイアウォールを通過します。FWLB はルーティング機能を実行します。FWLB の決定にはコンテンツ ルールは適用されません。

（注） ファイアウォールでは、Network Address Translation（NAT; ネットワーク アドレス変換）を実行することはできません。NAT の設定が必要な場合は、CSS で、この機能を使用するためのコンテンツ ルールまたはソース グループを設定してください。

FWLB を設定するには、ローカルおよびリモートの CSS 上で、ファイアウォールを通過する各パスに対して次のパラメータを定義する必要があります。

- ファイアウォール インデックス（物理的なファイアウォールを特定）、ローカル ファイアウォールの IP アドレス、リモート ファイア ウォールの IP アドレス、および CSS VLAN の IP アドレス
- CSS が各ファイアウォールに対して使用するスタティック ルート

FWLB の設定に関しては、以降の項を参照してください。

ファイアウォールの同期

Check Point™ FireWall-1® などの、ステートフル インスペクション機能が搭載されたファイアウォール ソリューションでは、デバイスを経由するすべての接続（UDP や RPC などのステートレスなプロトコルを含む）に対して仮想状態が作成、維持されます。NAT についての詳細などのステート情報は、転送されたデータに応じて更新されます。これにより、異なるコンピュータ上で実行されている複数のファイアウォール モジュール（1 つの FWLB 環境内にある複数のモジュールなど）間で、接続に関するステート情報が相互に更新されて、情報の共有が可能になります。

ファイアウォールの同期（図 5-1 参照）には大きな利点があり、この機能によってファイアウォールの各デバイスは、ファイアウォール ロード バランシング環境にあるすべての接続を認識し、一部のファイアウォールに障害が発生した場合でも、ユーザに透過的にただちに障害から回復します。

（注） ファイアウォールの同期を設定する場合、詳細はそのファイアウォール製品のマニュアルを参照してください。FireWall-1 デバイスの設定の詳細については、『*Check Point Software FireWall-1 Architecture and Administration* guide』の「Active Network Management」の章を参照してください。

FWLB の設定

CSS は、ファイアウォールの両側に設置して、各フローに対して使用するファイアウォールの管理を行う必要があります。ファイアウォールの設定では、ローカルおよびリモートの各 CSS に同じファイアウォール インデックス番号を設定する必要があります。

パケット漏れを防止するため、CSS では、1 組の IP アドレスの間に存在するパケットをすべて同じファイアウォールに送出します。これは、どちらの方向で送信されるパケットに対しても適用されます。あるパス上で障害が発生した場合、すべてのトラフィックは、残りのパスが 1 つの場合はそのパスを使用し、残りのパスが複数の場合は、それらのパスに分散されます。

（注） ファイアウォールのインデックスは、ファイアウォール ルートを指定する前に定義する必要があります。インデックスを定義しない場合、エラー メッセージが返されます。ルートの設定方法は、**ip route... firewall** コマンドの記述を参照してください。

ファイアウォールのパラメータは、ローカルおよびリモートの CSS で、ファイアウォールを通過するパスそれぞれに対して定義する必要があります。ファイアウォールのパラメータを定義するには、**ip firewall** コマンドを使用します。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

ip firewall *index local_firewall_IP_address remote_firewall_IP_address remote_switch_IP_address*

変数の内容は次のとおりです。

（注） すべての IP アドレスはドット付き 10 進表記（たとえば、192.168.11.1）で入力します。

- *index*：ファイアウォールを識別するためのインデックス番号。1 ～ 254 の数値を入力します。

- *local_firewall_IP_address* ：CSS に接続されたサブネット上にあるファイアウォールの IP アドレス
- *remote_firewall_IP_address*：リモートの CSS に接続されたリモート サブネット上にあるファイアウォールの IP アドレス
- *remote_switch_IP_address* ：リモートの CSS の IP アドレス

たとえば、次のように入力します。

```
(config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
```

ファイアウォールのインデックスを削除するには、次のコマンドを入力します。

```
(config)# no ip firewall 1
```

注意　ファイアウォールのインデックスを削除すると、そのインデックスに関連するルートもすべて削除されます。

ファイアウォールのキープアライブ タイムアウトの設定

CSS は、ファイアウォールの反対側にあるリモート CSS にカスタムの ICMP キープアライブ要求を毎秒送信します。ファイアウォール構成のエンドポイントにある 2 台の CSS スイッチでは、ファイアウォール キープアライブのタイムアウト値に同じ値を使用する必要があります。同じ値を設定しないと、一方の CSS 上のルートがもう一方の CSS 上のルートと同時にフェールオーバーせず、そのファイアウォールをはさんで非対称のルーティングが起こる可能性があります。

CSS がリモート CSS からのキープアライブ メッセージを待機した結果、ファイアウォールが到達不可能であると宣言するまでの時間を、秒数で指定するには、**ip firewall timeout** *number* コマンドを使用します。タイムアウトの範囲は 3 ～ 16 秒です。デフォルトは 3 秒です。

（注）　ファイアウォール パスが利用できるようになるまでに必要な時間は、このコマンドの影響を受けず 3 秒のままです。

たとえば、タイムアウトを 16 に設定するには、次のように入力します。

```
(config)# ip firewall timeout 16
```

タイムアウトをデフォルトの 3 秒にリセットするには、次のように入力します。

```
(config)# no ip firewall timeout
```

ファイアウォール用 IP スタティック ルートの設定

ファイアウォールに使用するスタティック ルートを設定するには、**ip route... firewall** コマンドを使用します。また、オプションで、この IP ルートに対して管理上の距離を設定することもできます。

(注) ファイアウォールのインデックスは、ファイアウォールのスタティック ルートを指定する前に定義する必要があります。インデックスを定義しない場合、エラー メッセージが返されます。ファイアウォールのインデックスの設定方法は、**ip firewall** コマンドの記述を参照してください。

このコマンドのシンタックスは次のとおりです。

ip route *ip_address subnet_mask* **firewall** *index distance*

変数の内容は次のとおりです。

- *ip_address* ：宛先のネットワーク アドレス。IP アドレスは、ドット付き 10 進表記（192.168.11.1 など）で入力します。
- *subnet_mask* ：IP サブネット マスク。マスクは次のいずれかの形式で入力します。
  - CIDR ビット数表記（たとえば、/24）。IP アドレスとプレフィクス長との間にはスペースを入力しないでください。
  - ドット付き 10 進表記（たとえば、255.255.255.0）
- *index*：ファイアウォール ルートの既存のインデックス番号。ファイアウォール インデックスの設定方法については、**ip firewall** コマンドの項を参照してください。

- *distance* ：（オプション）管理上の距離。1 ～ 254 の整数を入力します。できるだけ小さい数値を指定します。デフォルト値は 1 です。

（注） CLI では、宛先アドレスと管理コストが同じ IP スタティック ルートで、ファイアウォール ルートであるものとそれ以外のものを同時に設定できません。ファイアウォール ルートとファイアウォール以外のルートの、コストかアドレスのいずれかを変更する必要があります。

たとえば、次のように入力します。

```
(config)# ip route 192.168.2.0/24 firewall 1 2
```

ファイヤウォールのルートを削除するには、次のように入力します。

```
(config)# no ip route 192.168.2.0/24 firewall 1
```

ファイアウォール ルートをアドバタイズするための OSPF の設定

他のプロトコルからのファイアウォール ルートを OSPF でアドバタイズするには、**ospf redistribute firewall** コマンドを使用します。これらのルートは、再配布すると OSPF 外部ルートになります。

任意で、次の処理を行えます。

- **metric** オプションを使用して、ルートのネットワーク コストを定義します。1 ～ 16,777,215 の範囲内の数値を指定します。デフォルトは 1 です。
- **tag** オプションを使用して、各外部ルートをアドバタイズするための 32 ビット タグ値を定義します。この値は、autonomous system boundary router（ASBR; 自律システム境界ルータ）間で情報を交換するために使用できます。
- **type1** オプションを指定して、ルートを ASE タイプ 1 としてアドバタイズします。デフォルトは、ASE タイプ 2 です。タイプ 1 とタイプ 2 ではコストの計算方法が異なります。タイプ 2 の ASE では、同一の宛先への複数のパスを比較する際に外部コスト（メトリック）だけが考慮されます。タイプ 1 の ASE では、外部コストと ASBR へ到達するためのコストが組み合わされます。

たとえば、次のように入力します。

```
(config)# ospf redistribute firewall metric 3 type1
```

ファイアウォール ルートのアドバタイジングを中止するには、次のコマンドを入力します。

```
(config)# no ospf redistribute firewall
```

ファイアウォール ルートをアドバタイズするための RIP の設定

他のプロトコルからのファイアウォール ルートを RIP でアドバタイズするには、**rip redistribute firewall** コマンドを使用します。また、このルートをアドバタイズする際に CSS が使用するオプションのメトリックを追加することもできます。1 ～ 15 の値を入力します。デフォルトは 1 です。

たとえば、RIP を使用してファイアウォール ルートをアドバタイズするには、次のように入力します。

```
(config)# rip redistribute firewall 3
```

（注） RIP は、デフォルトで RIP ルートと、RIP を実行するインターフェイスのローカル ルートをアドバタイズします。このコマンドは他のルートもアドバタイズします。

ファイアウォール ルートのアドバタイジングを中止するには、次のコマンドを入力します。

```
(config)# no rip redistribute firewall
```

FWLB スタテック ルート設定の例

ここでは、2 台の CSS 間に 2 つのファイアウォールを設置する構成で FWLB を設定する方法について説明します。FWLB のスタティック ルートを設定するには、ローカル（クライアント側）およびリモート（サーバ側）の両方の CSS 上で、ファイアウォールを経由する各パスに対して次のパラメータを定義する必要があります。

- ファイアウォール インデックス（物理的なファイアウォールを特定）、ローカル ファイアウォールの IP アドレス、リモート ファイアウォールの IP アドレス、および CSS VLAN の IP アドレス。スタティック ルートを設定する前に、**ip firewall** コマンドを設定する必要があります。設定しない場合、エラー メッセージが返されます。
- CSS が各ファイアウォールに対して使用するスタティック ルート

図 5-1 の CSS-A （ネットワークのクライアント側に設置）を設定するには、次の手順を実行します。

1. **ip firewall** コマンドを使用して、ファイアウォール 1 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 1 192.168.28.1 192.168.27.1 192.168.27.3
   ```

2. **ip route** コマンドを使用して、ファイアウォール 1 のスタティック ルートを定義します。たとえば、次のように入力します。

   ```
   (config)# ip route 192.168.2.0/24 firewall 1
   ```

3. **ip firewall** コマンドを使用して、ファイアウォール 2 を定義します。たとえば、次のように入力します。

   ```
   (config)# ip firewall 2 192.168.28.2 192.168.27.2 192.168.27.3
   ```

4. **ip route** コマンドを使用して、ファイアウォール 2 のスタティック ルートを定義します。たとえば、次のように入力します。

   ```
   (config)# ip route 192.168.2.0/24 firewall 2
   ```

図 5-1 の CSS-B（ネットワークのサーバ側に設置）を設定するには、次の手順を実行します。

1. **ip firewall** コマンドを使用して、ファイアウォール 1 を定義します。たとえば、次のように入力します。

```
(config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
```

2. **ip route** コマンドを使用して、ファイアウォール 1 のスタティック ルートを定義します。たとえば、次のように入力します。

```
(config)# ip route 0.0.0.0/0 firewall 1
```

3. **ip firewall** コマンドを使用して、ファイアウォール 2 を定義します。たとえば、次のように入力します。

```
(config)# ip firewall 2 192.168.27.2 192.168.28.2 192.168.28.3
```

4. **ip route** コマンドを使用して、ファイアウォール 2 のスタティック ルートを定義します。たとえば、次のように入力します。

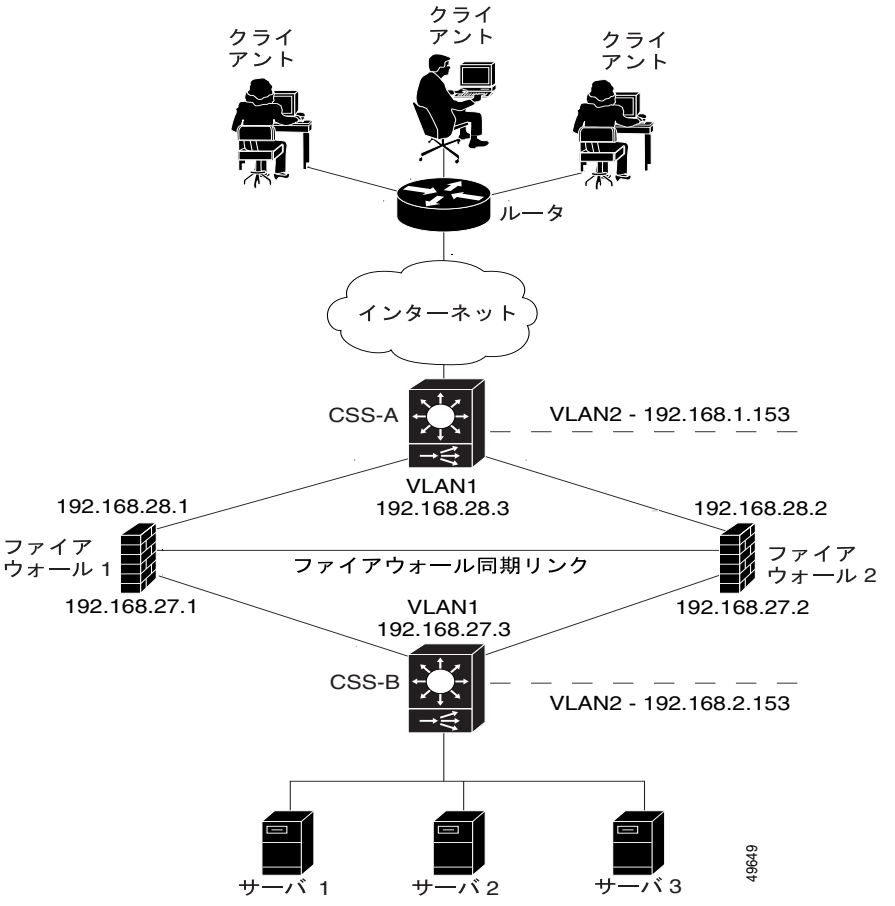
```
(config)# ip route 0.0.0.0/0 firewall 2
```

ファイアウォールの設定は、実行設定の IP 部分に表示されます。たとえば、次のように入力します。

```
(config)# show running-config
```

図 5-1 に、上記のファイアウォール コマンドで定義した構成を示します。

図 5-1　FWLB の例



VIP および仮想インターフェイスの冗長設定と FWLB の設定

FWLB の設定時に、VIP および仮想インターフェイスの冗長設定を行うと、次のような利点があります。

- フェールオーバーの高速化（通常 1 ～ 3 秒）
- シングル ポイント障害の回避
- すべての CSS がトラフィックを転送（アクティブ / バックアップ設定）

（注） VIP および仮想インターフェイスの冗長設定の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

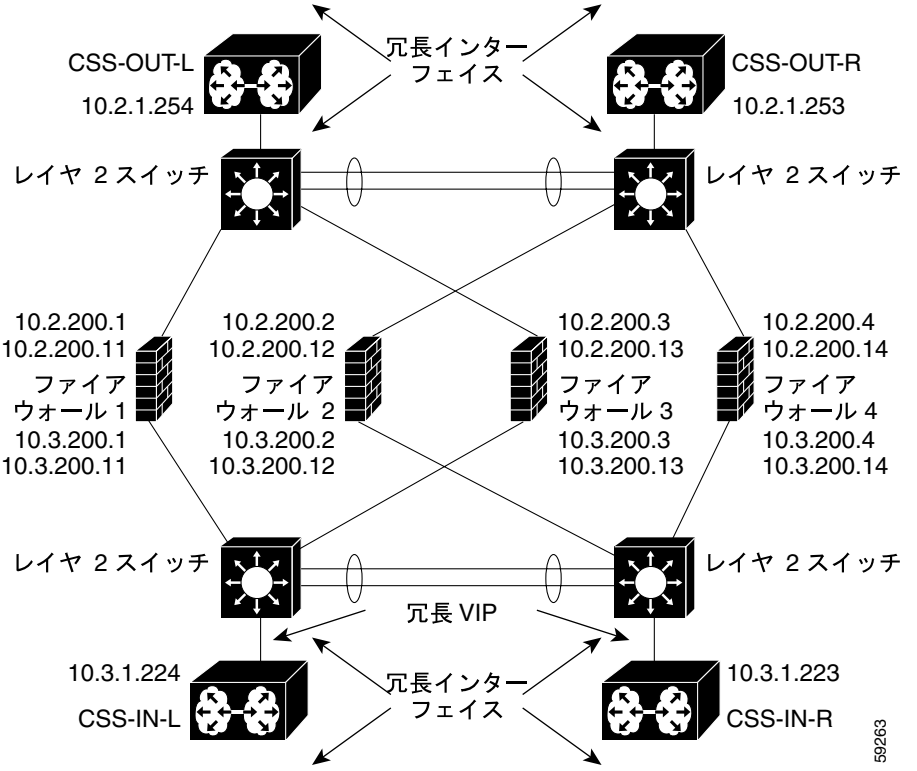
この設定では、ファイアウォールのそれぞれの側に 2 台の冗長 CSS と 2 台の L2 デバイスを使用します。1 台の CSS に障害が発生すると、ファイアウォールの同じ側の冗長 CSS が残りの負荷を引き受けます。

（注） FWLB を、VIP および仮想インターフェイスの冗長化を行うように設定した場合、共有 VIP は設定しないでください。共有 VIP は FWLB トポロジではサポートしていません。共有 VIP の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

VIP は、サービスが直接接続されているか、レイヤ 2 デバイスを介して接続されている CSS 上で設定する必要があります。サービスが、ファイアウォールの向こう側に置かれ、FWLB のメンバーである別の CSS に接続されている場合、CSS に VIP を使用したコンテンツ ルールを設定することはできません。このような設定は、非対称パスとなり、ステートフル インスペクションを行うファイアウォールによって接続が中断される可能性があります。

図 5-2 では、CSS-OUT-L と CSS-IN-L にサービスするレイヤ 2 スイッチに奇数番号のファイアウォールが接続されています。CSS-OUT-R と CSS-IN-R にサービスするレイヤ 2 スイッチには、偶数番号のファイアウォールが接続されています。

図 5-2　VIP/ インターフェイスが冗長化された FWLB



各ファイアウォールにはその両側に 2 つずつアドレスを設定する必要があります。最初のアドレスは、低コストのスタティック（プライマリ）パス上のネクストホップに使用します。2 番目のアドレスは、高コストのフローティングスタティック（セカンダリ）パス上のネクストホップに使用します。

フローティングスタティック パスには、スタティック パスとして指定したパス（通常はコスト 1）より高いコスト（通常はコスト 10）を設定します。1 台の CSS（たとえば、CSS-OUT-L）が故障すると、CSS-OUT-R が CSS-IN-L に高いコストのパスを使用してトラフィックを送るようになります。

ファイアウォールがマルチネッティングをサポートする場合、そのファイアウォールに複数のアドレスを設定することでマルチネッティングを使用できます。ファイアウォールが物理インターフェイスごとに複数のアドレスをサポートしない場合、ap-kal-fwlb-multinet スクリプトを使用してファイアウォールの複数のアドレスをシミュレートします。このスクリプトは、引数 realAddress secondaryAddress をとります。このスクリプトにより、各ファイアウォール インターフェイスにつき、スタティック ARP エントリが 1 つ作成されます。

（注） 手動でスタティック ARP エントリを入力することもできますが、スクリプトを使用するほうが、ファイアウォールを交換したことによって MAC アドレスが変わった場合に、ARP エントリも変更されるので便利です。

フェールオーバー時間は、次の理由で 1 ～ 3 秒と非常に高速です。

- フローティングスタテック パスがすでに起動している
- ファイアウォール パス情報が交換されている
- 回線が動作している

レイヤ 2 スイッチの 1 台に障害が発生すると、1 つおきのファイアウォールについてハッシュ値が再度計算されトラフィックのパスが決められます。ファイアウォールが偶数個ある場合、トラフィックの 50 パーセントが同じファイアウォールに再ハッシュされます。

（注） CSS の両側に冗長インターフェイスを設定する場合は、クリティカル サービスを使用して、一方のインターフェイスに障害が発生してバックアップに切り替わった場合にもう一方のインターフェイスでも同じことが行われるようにします。複数のインターフェイスを実装する場合は、ファイアウォール インターフェイスを外側の CSS 上のクリティカル サービスとして使用し、サービス タイプを redundancy-up として設定したファイアウォール インターフェイスとバックエンド サーバを内側の CSS 上のクリティカル サービスとして使用します。クリティカル サービスの設定および冗長アップリンク サービスの設定の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。

ファイアウォールとルート設定の例

次の **ip firewall** と **ip route** の設定例は、4 つのアクティブなファイアウォールからなる図 5-2 で有効です。

CSS-OUT-L の設定

```
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip route 10.3.0.0 255.255.0.0 firewall 1 1
ip route 10.3.0.0 255.255.0.0 firewall 2 1
ip route 10.3.0.0 255.255.0.0 firewall 3 1
ip route 10.3.0.0 255.255.0.0 firewall 4 1
ip route 10.3.0.0 255.255.0.0 firewall 11 10
ip route 10.3.0.0 255.255.0.0 firewall 12 10
ip route 10.3.0.0 255.255.0.0 firewall 13 10
ip route 10.3.0.0 255.255.0.0 firewall 14 10
```

CSS-OUT-R の設定

```
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip route 10.3.0.0 255.255.0.0 firewall 11 1
ip route 10.3.0.0 255.255.0.0 firewall 12 1
ip route 10.3.0.0 255.255.0.0 firewall 13 1
ip route 10.3.0.0 255.255.0.0 firewall 14 1
ip route 10.3.0.0 255.255.0.0 firewall 1 10
ip route 10.3.0.0 255.255.0.0 firewall 2 10
ip route 10.3.0.0 255.255.0.0 firewall 3 10
ip route 10.3.0.0 255.255.0.0 firewall 4 10
```

CSS-IN-L の設定

```
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip route 0.0.0.0 0.0.0.0 firewall 1 1
ip route 0.0.0.0 0.0.0.0 firewall 2 1
ip route 0.0.0.0 0.0.0.0 firewall 3 1
ip route 0.0.0.0 0.0.0.0 firewall 4 1
ip route 0.0.0.0 0.0.0.0 firewall 11 10
ip route 0.0.0.0 0.0.0.0 firewall 12 10
ip route 0.0.0.0 0.0.0.0 firewall 13 10
ip route 0.0.0.0 0.0.0.0 firewall 14 10
```

CSS-IN-R の設定

```
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip route 0.0.0.0 0.0.0.0 firewall 11 1
ip route 0.0.0.0 0.0.0.0 firewall 12 1
ip route 0.0.0.0 0.0.0.0 firewall 13 1
ip route 0.0.0.0 0.0.0.0 firewall 14 1
ip route 0.0.0.0 0.0.0.0 firewall 1 10
ip route 0.0.0.0 0.0.0.0 firewall 2 10
ip route 0.0.0.0 0.0.0.0 firewall 3 10
ip route 0.0.0.0 0.0.0.0 firewall 4 10
```

ファイアウォール フローの要約の表示

CSS の Switch Processor （SP; スイッチ プロセッサ）上で、特定の送信元 IP アドレスのフロー要約、または特定の送信元アドレスとその宛先 IP アドレスのフロー要約を表示するには、**show flows** コマンドを使用します。1 台の SP につき 4096 までのフローを表示できます。

この情報によって、次のことがわかります。

- 特定のフローに対して使用されるファイアウォールの識別
- フローの表示して FWLB の正常な動作を確認

このコマンドのシンタックスは次のとおりです。

show flows *source_address destination_address*

変数の内容は次のとおりです。

- *source_address* ：フローの送信元 IP アドレス。アドレスをドット付き 10 進表記（たとえば、192.168.11.1）で入力します。
- *destination_address* ：宛先 IP アドレス。アドレスをドット付き 10 進表記（たとえば、192.168.11.1）で入力します。

たとえば、次のように入力します。

```
(config)# show flows 192.165.22.1 192.163.2.3
```

特定の送信元 IP アドレスのフローを表示するには、次のように入力します。

```
(config)# show flows 192.165.22.1
```

特定の送信元 IP アドレスおよび宛先 IP アドレスのフローを表示するには、次のように入力します。

```
(config)# show flows 192.165.22.1 192.163.2.3
```

表 5-1 に、**show flows** コマンドで表示されるフィールドについて説明します。

表 5-1　show flow コマンドのフィールド

フィールド	説明
Src Address	フローの送信元アドレス
SPort	フローの送信元ポート
Dst Address	フローの宛先アドレス
DPort	フローの宛先ポート
NAT Dst Address	NAT 対象の宛先アドレス
Prot	フローのプロトコル（TCP または UDP）
InPort	入側フローのインターフェイス ポート
OutPort	出側フローのインターフェイス ポート

ファイアウォール IP ルートの表示

すべてのスタティック ファイアウォール ルートを表示するには、**show ip routes firewall** コマンドを使用します。たとえば、次のように設定します。

```
(config)# show ip routes firewall
```

表 5-2 に、**show ip routes firewall** コマンドで表示されるフィールドについて説明します。

表 5-2　show ip routes firewall コマンドのフィールド

フィールド	説明
Prefix/length	ルートの IP アドレスとプレフィクス長
Next hop	ネクスト ホップの IP アドレス
If	ifIndex 値。そのルートで、ネクスト ホップに到達する前に通過するローカル インターフェイスです。
Type	ルート エントリのタイプ。タイプはリモートです。
Proto	ルートのプロトコル。ファイアウォールです。
Age	ルートの最大経過時間
Metric	ルートのメトリック コスト

ファイアウォール IP 情報の表示

IP ファイアウォールのキープアライブ タイムアウトに設定された値と、CSS に設定されている各ファイアウォール パスの状態を表示するには、**show ip firewall** コマンドを使用します。たとえば、次のように入力します。

```
(config)# show ip firewall
```

表 5-3 に、**show ip firewall** コマンドのフィールドについて説明します。

表 5-3　show ip firewall コマンドのフィールド

フィールド	説明
IP Firewall KAL Timeout	CSS がリモート CSS からのキープアライブ メッセージを待機する秒数。この秒数の後、ファイアウォールが到達不可能であると宣言します。
Firewall Index	ファイアウォールを識別するためのインデックス番号
State	リモート スイッチへの接続の現在の状態（Init、Reachable、Unreachable のいずれか）
Next Hop	ネクストホップの IP アドレス
Remote Firewall	リモートの CSS に接続されたリモート サブネット上にあるファイアウォールの IP アドレス
Remote Switch	リモート CSS の IP アドレス
Time Since Last KAL Tx	最後のキープアライブ メッセージを送信してから経過した時間
Time Since Last KAL Rx	最後のキープアライブ メッセージを受信してから経過した時間

INDEX

R

S

T

W

X

あ

か

き

く

こ

さ

し

せ

そ

た

ち

て

と

ね

は

ひ

ふ

へ

ま

む

ゆ

ら

り

る

れ

ろ