CHAPTER 5

管理インターフェイスとセキュリティの設定

概要

ここでは、物理管理インターフェイス（ポート）と多様な管理インターフェイス アプリケーション（SNMP、SSH、TACACS+ など）の設定方法について説明します。また、ユーザ、パスワード、IP 構成、クロックとタイム ゾーン、およびドメイン名を設定する方法についても説明します。

管理インターフェイスとセキュリティ

サービス コントロール モジュールは、RJ-45 管理（MNG）ポートを備えています。このギガビット イーサネット ポートを使用すると、リモートの管理コンソールから LAN 経由で SCE プラットフォームへアクセスできます。

管理インターフェイスと管理インターフェイスのセキュリティを設定するには、次のタスクを実行します。

- 管理ポートの設定：
  - 物理パラメータ
- 管理インターフェイス セキュリティの設定
  - 許可および非許可の IP アドレスの設定

管理ポートの設定

管理ポートを設定するには、次のタスクを実行します。

- IP アドレスとサブネット マスクの設定
- 物理パラメータの設定：
  - Speed
  - Duplex

ステップ 1　管理ポートを LAN 経由でリモート管理コンソールに接続します。

ステップ 2　管理ポートの物理パラメータを設定します（「管理ポートの物理パラメータの設定」（P.5-2）を参照）。

管理インターフェイス コンフィギュレーション モードを開始する方法

GBE 管理インターフェイスは次のように設定します。

- モード：ギガビット イーサネット インターフェイス コンフィギュレーション モード
- インターフェイスの指定：1/1

ステップ 1　**configure** を入力して、**Enter** キーを押します。

グローバル コンフィギュレーション モードに移行します。

コマンド プロンプトが SCE(config)# に変わります。

ステップ 2　**interface GigabitEthernet 1/1** を入力して、**Enter** キーを押します。

GigabitEthernet インターフェイス コンフィギュレーション モードに移行します。

コマンド プロンプトは SCE(config-if)# に変わります。

管理ポートの物理パラメータの設定

これはギガビット イーサネット インターフェイスであり、管理操作および RDR（トラフィック分析と管理操作の出力）の伝送に使用されます。

- 「管理インターフェイスの IP アドレスとサブネット マスクの設定」（P.5-3）
- 「管理インターフェイスの speed パラメータと duplex パラメータの設定」（P.5-3）
- 「管理インターフェイスを監視する方法」（P.5-5）

管理インターフェイスの IP アドレスとサブネット マスクの設定

管理インターフェイスの IP アドレスを定義する必要があります。

オプション

次のオプションを使用できます。

- **IP address**：管理インターフェイスの IP アドレス。
- **subnet mask**：管理インターフェイスのサブネット マスク。

Telnet 経由で管理インターフェイスの IP アドレスを変更すると、Telnet 接続の損失が生じ、インターネットに再接続できなくなります。

ステップ 1　SCE(config if)# プロンプトに、**ip address** *ip-address subnet-mask* を入力して、**Enter** キーを押します。

新規の IP アドレスとサブネット マスクに定義された新規のサブネットに含まれないルーティング テーブルのエントリがあると、このコマンドが失敗する可能性があります。

（注）　Telnet 経由で管理インターフェイスの IP アドレスを変更すると、Telnet 接続の損失が生じ、インターネットに再接続できなくなります。

（注）　IP アドレスの変更後は、SCE プラットフォームのすべての内部コンポーネントおよび外部コンポーネントに変更が適切に反映されるように、SCE プラットフォームをリロードする必要があります（「SCE プラットフォームのリブートとシャットダウン」（P.3-17）を参照）。

管理インターフェイスの IP アドレスとサブネット マスクの設定：例

次に、SCE プラットフォームの IP アドレスを 10.1.1.1 に設定し、サブネット マスクを 255.255.0.0 に設定する例を示します。

```
SCE(config if)#ip address 10.1.1.1 255.255.0.0
```

管理インターフェイスの speed パラメータと duplex パラメータの設定

ここでは、管理インターフェイスの speed と duplex を設定する方法を説明する手順の例を示します。

これらの両方のパラメータは、各ポートで個別に設定する必要があります。

- 「speed と duplex のインターフェイス ステートの関係」（P.5-4）
- 「管理インターフェイスの速度を設定する方法」（P.5-4）
- 「管理インターフェイスのデュプレックス動作を設定する方法」（P.5-5）

speed と duplex のインターフェイス ステートの関係

表 5-1 に、インターフェイス ステートと、speed および duplex との関係を示します。

次の点に注意してください。

- 一方のパラメータを「Auto」に設定し、もう一方を別のパラメータに設定することはできません。speed または duplex が「Auto」に設定されている場合、両方のパラメータは「Auto」に設定されたように動作します。
- インターフェイスの性質から、1000 Mbps の操作が可能なのは、オートネゴシエーションがイネーブルの場合だけです。

表 5-1　speed と duplex のインターフェイス ステートの関係

Speed	Duplex	実際の FE インターフェイス ステート
Auto	Auto	オートネゴシエーション
Auto	Full/Half	オートネゴシエーション
10/100	Auto	オートネゴシエーション
10	Full	10 Mbps および全二重
10	Half	10 Mbps および半二重
100	Full	100 Mbps および全二重
100	Half	100 Mbps および半二重

管理インターフェイスの速度を設定する方法

オプション

次のオプションを使用できます。

- **speed**：現在選択されている管理ポート（0/1 または 0/2）の速度（Mbps）。
  - **10**
  - **100**
  - **auto**（デフォルト）：オートネゴシエーション（リンクに速度を強制しません）

duplex パラメータが **auto** に設定されている場合、speed パラメータを変更しても効果がありません。

ステップ 1　SCE(config if)# プロンプトに、**speed 10|100|auto** を入力して、**Enter** キーを押します。

必要な speed オプションを指定します。

管理インターフェイスの速度の設定：例

次に、このコマンドを使用して、管理ポートを 100 Mbps の速度に設定する例を示します。

```
SCE(config-if)#speed 100
```

管理インターフェイスのデュプレックス動作を設定する方法

オプション

次のオプションを使用できます。

- **duplex**：管理ポート（1/1）のデュプレックス動作。
  - full
  - half
  - auto（デフォルト）：オートネゴシエーション（リンクにデュプレックスを強制しません）

speed パラメータが **auto** に設定されている場合、duplex パラメータを変更しても効果がありません。

ステップ 1　SCE(config if)# プロンプトに、**duplex auto|full|half** を入力して、**Enter** キーを押します。

必要な duplex オプションを指定します。

管理インターフェイスのデュプレックス動作の設定：例

次に、このコマンドを使用して、管理ポートを半二重モードに設定する例を示します。

```
SCE(config-if)#duplex half
```

管理インターフェイスを監視する方法

管理インターフェイスの次の情報を表示するには、このコマンドを使用します。

- オートネゴシエーション
- IP アドレス
- アクティブ ポート

ステップ 1　SCE# プロンプトに、**show GigabitEthernet interface Mng 1/1 [auto-negotiate|ip address]** を入力して、Enter キーを押します。

GBE 管理インターフェイス コンフィギュレーションを表示します。オプションを指定しない場合、すべての管理インターフェイス情報が表示されます。

使用可能なインターフェイスの設定

SCE プラットフォームと外部コンポーネントを管理する計画内容に従って、Telnet および SNMP のインターフェイスを設定できます。

- 「TACACS+ 認証、認可、およびアカウンティング」（P.5-6）
- 「ACL の設定」（P.5-19）
- 「Telnet インターフェイスの管理」（P.5-21）
- 「SSH サーバの設定」（P.5-22）
- 「SNMP インターフェイスのイネーブル化」（P.5-24）

TACACS+ 認証、認可、およびアカウンティング

TACACS+ 認証、認可、およびアカウンティングに関する情報

TACACS+ 認証、認可、およびアカウンティング

TACACS+ は、ネットワーク要素にアクセスしようとしているユーザを中央で認証する機能を持つセキュリティ アプリケーションです。TACACS+ プロトコルを実装すると、SCE プラットフォームに対して 1 つまたは複数の認証サーバを設定できます。その結果、認証サーバが各ユーザを認証するため、SCE プラットフォームを安全に管理できるようになります。また、認証データベースが集中管理されるため、SCE プラットフォームを管理しやすくなります。

TACACS+ サービスは、ワークステーション（通常は UNIX または Windows NT）で実行されている TACACS+ サーバのデータベースで保守されます。ネットワーク要素上の設定済み TACACS+ 機能を使用するには、TACACS+ サーバにアクセス権があり、TACACS+ サーバを設定する必要があります。

TACACS+ プロトコルを使用すると、ネットワーク要素と TACACS+ ACS 間で認証できます。また、ネットワーク要素と TACACS+ サーバ間のすべてのプロトコル交換を暗号化して、キーを設定した場合に機密保持することもできます。

TACACS+ プロトコルには、次の 3 つの機能があります。

- ログイン認証
- 特権レベルの許可
- アカウンティング

ログイン認証

SCE プラットフォームは、CLI、Telnet、および SSH アクセスに TACACS+ ASCII 認証メッセージを使用します。

TACACS+ を使用すると、ユーザの認証に必要な情報をサーバが取得するまで、サーバとユーザ間で任意の対話が可能になります。そのために、通常、ユーザ名とパスワードの組み合わせを入力するプロンプトが表示されます。

ログインとパスワードのプロンプトは、TACACS+ サーバが表示することがあります。また、TACACS+ サーバがプロンプトを表示しない場合、ローカル プロンプトが表示されます。

ユーザのログイン情報（ユーザ名とパスワード）は TACACS+ サーバに送信され、認証されます。TACACS+ サーバは、そのユーザを認証しないことを示す場合、ユーザ名とパスワードのプロンプトを再表示します。プロンプトの再表示は、ユーザ設定可能な回数行われます。その回数を超えると、失敗したログイン試行は SCE プラットフォームのユーザ ログに記録され、telnet セッションは中止されます（ただし、ユーザがコンソール ポートに接続している場合は除きます）。

最終的に、SCE プラットフォームは TACACS+ サーバから次の応答のいずれかを受信します。

- ACCEPT：ユーザは認証され、サービスを開始できます。
- REJECT：ユーザの認証に失敗しました。TACACS+ サーバによって異なりますが、ユーザは以降のアクセスを拒否されるか、ログイン シーケンスの再試行を求められます。
- ERROR：認証中にエラーが発生しました。たとえば、サーバ エラーサーバ エラーや、SCE プラットフォーム間のネットワーク接続エラーなどです。ERROR 応答を受信した場合、SCE プラットフォームは、ユーザの認証に代替の方法 / サーバの使用を試行します。
- CONTINUE：追加の認証情報を求めるプロンプトが表示されます。

サーバを使用できない場合、次の認証方法が試行されます（「一般的な AAA フォールバックと回復メカニズム」（P.5-8）を参照）。

アカウンティング

TACACS+ のアカウンティングは、次の機能をサポートしています。

- 実行した各コマンド（有効なコマンド）は、TACACS+ アカウンティング メカニズムを使用して記録されます（login コマンドおよび exit コマンドなど）。
- コマンドが正常に実行された場合、実行前と実行後の両方に記録されます。
- 各アカウンティング メッセージには次の情報が含まれます。
  - ユーザ名
  - 現在の時刻
  - 実行された処理
  - コマンドの特権レベル

TACACS+ のアカウンティングでは、通常のローカル アカウンティングに加え、SCE プラットフォーム dbg ログも使用しています。

特権レベルの許可

ログイン後は、0 というデフォルトの特権レベルがユーザに付与され、限られた数のコマンドを実行できるようになります。特権レベルを変更するには、「enable」コマンドを実行します。このコマンドで、特権レベルの許可メカニズムが初期化されます。

SCE プラットフォームで特権レベルを許可するには、「enable」コマンドの認証要求を使用します。「enable」コマンドを使用して特定の特権レベルの許可を要求すると、SCE プラットフォームから TACACS+ サーバに対して、要求された特権レベルを示す認証要求が送信されます。SCE プラットフォームは、TACACS+ サーバが以下を実行してから、要求された特権を付与します。

- 「**enable**」コマンド パスワードを認証する。
- 要求された特権レベルを開始できる特権をユーザが持っていることを検証する。

ユーザの特権レベルが決定されると、認められたレベルに従って、特定のコマンド セットにアクセスできるようになります。

ログインの認証と同様に、サーバを使用できない場合、次の認証方法が試行されます（「一般的な AAA フォールバックと回復メカニズム」（P.5-8）を参照）。

一般的な AAA フォールバックと回復メカニズム

SCE プラットフォームはフォールバック メカニズムを使用して、エラー発生時のサービスの可用性を維持しています。

使用できる AAA メソッドは次のとおりです。

- **TACACS+**：AAA は TACACS+ サーバを使用して実行され、認証、許可、およびアカウンティングの機能があります。
- **Local**：AAA はローカル データベースを使用して実行され、認証と許可の機能があります。
- **Enable**：AAA はユーザ設定パスワードを使用して実行され、認証と許可の機能があります。
- **None**：認証/許可/アカウンティングは実行されません。

現在の実装では、使用するメソッドの順序は設定できませんが、使用するメソッドは選択できます。現在の順序は次のとおりです。

- **TACACS+**
- **Local**
- **Enable**
- **None**

（注）　重要：サーバで AAA エラーが発生すると、AAA メソッドの 1 つが復元されるまで、SCE プラットフォームはアクセスできなくなります。この問題を回避するには、最後の AAA メソッドとして「none」メソッドを使用することをお勧めします。SCE プラットフォームにアクセスできなくなった場合、shell 関数「AAA_MethodsReset」を使用して、現在の AAA メソッド設定を削除し、使用する AAA メソッドを「Enable」に設定できます。

TACACS+ の設定について

次に、TACACS+ を設定する手順の概要について説明します。以降、この項では、すべての手順について詳細に説明します。

1. リモートの TACACS+ サーバを設定します。

   プロトコル用にリモート サーバを設定します。次のガイドラインについて注意してください。

   - サーバとクライアントが使用する暗号キーを設定します。
   - 最高のユーザ特権レベルとイネーブル パスワード（イネーブル コマンドを実行するときに使用されるパスワード）を指定します。
   - 設定には常にルート ユーザを含め、15 の特権レベルを付与します。

- Viewer（特権レベル 5）および Superuser（特権レベル 10）のユーザ ID も、この時点で設定します。

1. サーバ設定の詳細については、使用する各 TACACS+ サーバに対応するコンフィギュレーション ガイドを参照してください。
2. TACACS+ サーバを操作する SCE クライアントを設定します。
   - サーバのホスト名
   - ポート番号
   - 共有の暗号キー（クライアントとサーバが通信するには、設定した暗号キーが、サーバに設定された暗号キーと一致する必要があります）
3. （任意）使用する場合、ローカル データベースを設定します。
   - 新規ユーザの追加

   ローカル データベースと TACACS+ の両方が設定されている場合、TACACS+ とローカル データベースの両方で同じユーザ名を設定することをお勧めします。こうすると、TACACS+ サーバでエラーが発生した場合でも、SCE プラットフォームにアクセスできます。

（注）　ログイン方法に TACACS+ を使用する場合、TACACS+ のユーザ名は enable コマンドで自動的に使用されます。そのため、TACACS+ とローカル データベースの両方で同じユーザ名を設定し、enable コマンドがそのユーザ名を認識できるようにすることが重要です。

   - パスワードの指定
   - 特権レベルの定義
4. SCE プラットフォームで認証方法を設定します。
   - ログイン認証方法
   - 特権レベルの許可方法
5. 設定を見直します。

   設定を表示するには、「**show running-config**」コマンドを使用します。

SCE プラットフォームの TACACS+ クライアントの設定

SCE プラットフォームの TACACS+ クライアントを設定する方法

TACACS+ プロトコルのリモート サーバを設定する必要があります。次に、TACACS+ サーバを操作できるように、SCE プラットフォームの TACACS+ クライアントを設定します。次の情報を設定する必要があります。

- TACACS+ サーバ ホストの定義：最大 3 つのサーバがサポートされます。

  サーバ ホストごとに、次の情報を設定できます。
  - ホスト名（必須）

  - ポート
  - 暗号キー
  - タイムアウト間隔
- デフォルトの暗号キー（オプション）：グローバルなデフォルトの暗号キーを定義できます。サーバ ホストを定義するときにキーが明示的に設定されないサーバ ホストには、デフォルトの暗号キーが使用されます。

  デフォルトの暗号キーが設定されない場合、キーが明示的に設定されていないサーバには、キーのデフォルトは割り当てられません。
- デフォルトのタイムアウト間隔（オプション）：グローバルなデフォルトのタイムアウト間隔を定義できます。サーバ ホストを定義するときにタイムアウト間隔が明示的に設定されないサーバ ホストには、デフォルトのタイムアウト間隔が使用されます。

  デフォルトのタイムアウト間隔が設定されない場合、タイムアウト間隔が明示的に設定されていないサーバには、5 秒というデフォルト値が割り当てられます。

ここでは、SCE プラットフォームの TACACS+ クライアントの設定手順について説明します。

- 「新しい TACACS+ サーバ ホストを追加する方法」（P.5-10）
- 「TACACS+ サーバ ホストを削除する方法」（P.5-11）
- 「グローバルなデフォルト キーを設定する方法」（P.5-11）
- 「グローバルなデフォルトのタイムアウトを設定する方法」（P.5-11）

新しい TACACS+ サーバ ホストを追加する方法

SCE プラットフォームの TACACS+ クライアントに使用できる新しい TACACS+ サーバ ホストを定義するには、このコマンドを使用します。

サービス コントロール ソリューションでは、最大 3 つの TACACS+ サーバ ホストをサポートします。

オプション

次のオプションを使用できます。

- **host-name**：サーバの名前
- **port number**：TACACS+ のポート番号
  - デフォルト = 49
- **timeout interval**：サーバ ホストからの応答がタイムアウトまで待機する時間（秒）
  - デフォルト = 5 秒、またはユーザ設定のグローバルなデフォルトのタイムアウト間隔（「グローバルなデフォルトのタイムアウトを定義する方法」（P.5-12）を参照）。
- **key-string**：サーバとクライアントが相互に通信するときに使用する暗号キー。指定したキーが実際に TACACS+ サーバ ホストに設定されていることを確認します。
  - デフォルト = キーなし、またはユーザ設定のグローバルなデフォルト キー（「グローバルなデフォルト キーを定義する方法」（P.5-11）を参照）。

ステップ 1　SCE(config)# プロンプトに、**tacacs-server host** *host-name* **[port** *portnumber***] [timeout** *timeout-interval***] [key** *key-string***]** を入力して、**Enter** キーを押します。

TACACS+ サーバ ホストを削除する方法

オプション

次のオプションを使用できます。

- **host-name**：削除するサーバの名前

ステップ 1　SCE(config)# プロンプトに、**no tacacs-server host** *host-name* を入力して、**Enter** キーを押します。

グローバルなデフォルト キーを設定する方法

TACACS+ サーバ ホストのグローバルなデフォルト キーを設定するには、このコマンドを使用します。特定の TACACS+ サーバ ホストでは、その TACACS+ サーバ ホストに異なるキーを明示的に設定することで、デフォルトのキーを上書きできます。

オプション

次のオプションを使用できます。

- **key-string**：すべての TACACS+ サーバとクライアントが相互に通信するときに使用するデフォルトの暗号キー。指定したキーが実際に TACACS+ サーバ ホストに設定されていることを確認します。
  - デフォルト = 暗号化なし

グローバルなデフォルト キーを定義する方法

ステップ 1　SCE(config)# プロンプトに、**tacacs-server key** *key-string* を入力して、**Enter** キーを押します。

グローバルなデフォルト キーをクリアする方法

ステップ 1　SCE(config)# プロンプトに、**no tacacs-server key** を入力して、**Enter** キーを押します。

グローバルなデフォルト キーは定義されなくなります。明示的にキーが定義されている TACACS+ サーバ ホストのキー定義はそのままです。ただし、明示的にキーが定義されていない（つまりグローバルなデフォルト キーを使用する）サーバ ホストは、キーを使用しないように設定されます。

グローバルなデフォルトのタイムアウトを設定する方法

TACACS+ サーバ ホストのグローバルなデフォルトのタイムアウトを設定するには、このコマンドを使用します。特定の TACACS+ サーバ ホストでは、その TACACS+ サーバ ホストに異なるタイムアウトを明示的に設定することで、デフォルトのタイムアウトを上書きできます。

オプション

次のオプションを使用できます。

- **timeout interval**：サーバ ホストからの応答がタイムアウトまで待機するデフォルトの時間（秒）。
  - デフォルト = 5 秒

グローバルなデフォルトのタイムアウトを定義する方法

ステップ 1　SCE(config)# プロンプトに、**tacacs-server timeout** *timeout-interval* を入力して、**Enter** キーを押します。

グローバルなデフォルトのタイムアウトをクリアする方法

ステップ 1　SCE(config)# プロンプトに、**no tacacs-server timeout** を入力して、**Enter** キーを押します。

グローバルなデフォルトのタイムアウト間隔は定義されなくなります。明示的にタイムアウト間隔が定義されている TACACS+ サーバ ホストのタイムアウト間隔の定義はそのままです。ただし、タイムアウト間隔が明示的に定義されていない（つまりグローバルなデフォルト タイムアウト間隔を使用する）サーバ ホストには、5 秒のタイムアウト間隔が設定されます。

ユーザ データベースの管理

TACACS+ はローカル ユーザ データベースを管理します。このローカル データベースには最大 100 ユーザを設定できます。また、すべてのユーザに次のような情報を設定できます。

- ユーザ名
- パスワード：暗号化の有無を設定可能
- 特権レベル

ここでは、ローカル ユーザ データベースの管理手順について説明します。

- 「ローカル データベースに新しいユーザを追加する方法」（P.5-12）
- 「ユーザの特権レベルを定義する方法」（P.5-14）
- 「特権レベルとパスワードを使用して新しいユーザを追加する方法」（P.5-14）
- 「ユーザを削除する方法」（P.5-16）

ローカル データベースに新しいユーザを追加する方法

ローカル データベースに新しいユーザを追加するには、このコマンドを使用します。最大 100 ユーザを定義できます。

- 「オプション」（P.5-13）
- 「クリア テキスト パスワードを使用してユーザを追加する方法」（P.5-13）
- 「パスワードなしでユーザを追加する方法」（P.5-13）
- 「クリア テキストで入力した MD5 暗号化パスワードを使用してユーザを追加する方法」（P.5-14）
- 「MD5 暗号化文字列として入力した MD5 暗号化パスワードを使用してユーザを追加する方法」（P.5-14）

オプション

ユーザ名と共にパスワードを定義します。次のように複数のパスワード オプションがあります。

- パスワードなし：**nopassword** キーワードを使用します。
- パスワード：パスワードはローカルのリストにクリア テキスト形式で保存されます。

  password パラメータを使用します。
- 暗号化されたパスワード：パスワードはローカルのリストに暗号化（MD5）された形式で保存されます。シークレット キーワードを使用します。

  パスワードを定義するには、次のいずれかの方法を使用します。
  - クリア テキスト パスワードを指定します。このパスワードは MD5 暗号化形式で保存されます。
  - MD5 暗号化文字列を指定します。この文字列はユーザの MD5 暗号化シークレット パスワードとして保存されます。

次のオプションを使用できます。

- **name**：追加するユーザの名前。
- **password**：クリア テキストのパスワード。次の 2 つの形式のいずれかで、ローカル リストに保存できます。
  - クリア テキスト形式
  - シークレット キーワードを使用する場合は MD5 暗号化形式
- **encrypted-secret :** MD5 暗号化文字列パスワード

次のキーワードを使用できます。

- **nopassword**：このユーザに関連付けられるパスワードはありません。
- **secret :** MD5 暗号化フォームでパスワードが保存されます。次のいずれかのキーワードを使用して、コマンドに入力するパスワードの形式を指定します。
  - **0**：MD5 暗号化形式で保存されるクリア テキスト パスワードを指定する場合、**password** オプションを使用します
  - **5**：ユーザの MD5 暗号化シークレット パスワードとして保存される MD5 暗号化文字列を指定するには、**encrypted-secret** オプションを使用します

クリア テキスト パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **password** *password* を入力して、**Enter** キーを押します。

パスワードなしでユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **nopassword** を入力して、**Enter** キーを押します。

クリア テキストで入力した MD5 暗号化パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **secret 0** *password* を入力して、**Enter** キーを押します。

MD5 暗号化文字列として入力した MD5 暗号化パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **secret 5** *encrypted-secret* を入力して、**Enter** キーを押します。

ユーザの特権レベルを定義する方法

- 「ユーザの特権レベルについて」（P.5-14）
- 「オプション」（P.5-14）

ユーザの特権レベルについて

SCE プラットフォームで特権レベルを許可するには、「**enable**」コマンドの認証要求を使用します。「**enable**」コマンドを使用して特定の特権レベルの許可を要求すると、SCE プラットフォームから TACACS+ サーバに対して、要求された特権レベルを示す認証要求が送信されます。TACACS+ サーバが「**enable**」コマンドのパスワードを認証し、要求された特権レベルを使用できる特権をユーザが持っていることを検証し終わってから、SCE プラットフォームは要求された特権レベルをユーザに付与します。

オプション

次のオプションを使用できます。

- **name**：特権レベルを設定するユーザの名前
- **level**：指定したユーザに許可されている特権レベル。このレベルは、**enable** コマンドで入力される CLI 認可レベルに対応します。
  - 0：User
  - 10：Admin
  - 15（デフォルト）：Root

ステップ 1　SCE(config)# プロンプトに、**username** *name* **privilege** *level* を入力して、**Enter** キーを押します。

特権レベルとパスワードを使用して新しいユーザを追加する方法

1 つのコマンドで、パスワードと特権レベルを含め、新しいユーザを定義するには、このコマンドを使用します。

（注）　設定ファイル（**running config** と **startup config**）では、このコマンドは 2 つのコマンドとして表示されます。

- 「オプション」（P.5-15）

- 「特権レベルとクリア テキスト パスワードを使用してユーザを追加する方法」（P.5-15）
- 「特権レベルとクリア テキストで入力した MD5 暗号化パスワードを使用してユーザを追加する方法」（P.5-15）
- 「特権レベルと MD5 暗号化文字列として入力した MD5 暗号化パスワードを使用してユーザを追加する方法」（P.5-16）

オプション

次のオプションを使用できます。

- **name**：特権レベルを設定するユーザの名前
- **level**：指定したユーザに許可されている特権レベル。このレベルは、**enable** コマンドで入力される CLI 認可レベルに対応します。
  - 0：User
  - 10：Admin
  - 15（デフォルト）：Root
- **password**：クリア テキストのパスワード。次の 2 つの形式のいずれかで、ローカル リストに保存できます。
  - クリア テキスト形式
  - シークレット キーワードを使用する場合は MD5 暗号化形式
- **encrypted-secret**：MD5 暗号化文字列パスワード

次のキーワードを使用できます。

- **secret**：MD5 暗号化フォームでパスワードが保存されます。次のいずれかのキーワードを使用して、コマンドに入力するパスワードの形式を指定します。
  - **0**：MD5 暗号化形式で保存されるクリア テキスト パスワードを指定する場合、**password** オプションを使用します
  - **5**：ユーザの MD5 暗号化シークレット パスワードとして保存される MD5 暗号化文字列を指定するには、**encrypted-secret** オプションを使用します

特権レベルとクリア テキスト パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、`username` *name* `privilege` *level* `password` *password* を入力して、**Enter** キーを押します。

特権レベルとクリア テキストで入力した MD5 暗号化パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **privilege** *level* **secret 0** *password* を入力して、**Enter** キーを押します。

特権レベルと MD5 暗号化文字列として入力した MD5 暗号化パスワードを使用してユーザを追加する方法

ステップ 1　SCE(config)# プロンプトに、**username** *name* **privilege** *level* **secret 5** *encrypted-secret* を入力して、**Enter** キーを押します。

ユーザを削除する方法

オプション

次のオプションを使用できます。

- **name**：削除するユーザの名前。

ステップ 1　SCE(config)# プロンプトに、**no username** *name* を入力して、**Enter** キーを押します。

AAA ログイン認証の設定

ログイン認証で設定する機能には、次の 2 つがあります。

- Telnet ログインの最大試行回数
- ログイン時に使用される認証方法（「一般的な AAA フォールバックと回復メカニズム」（P.5-8）を参照）

ここでは、ログイン認証の設定手順について説明します。

- 「ログインの最大試行回数を設定する方法」（P.5-16）
- 「ログイン認証方法を設定する方法」（P.5-17）

ログインの最大試行回数を設定する方法

セッションが中止される前に実行できるログインの最大試行回数を設定するには、このコマンドを使用します。

オプション

次のオプションを使用できます。

- **number-of-attempts**：Telnet セッションが中止される前に実行できるログインの最大試行回数。

  これは Telnet セッションの場合にだけ関係があります。ローカル コンソールからの場合、再試行回数は無制限です。

  - デフォルト = 3

ステップ 1　SCE(config)# プロンプトに、**aaa authentication attempts login** *number-of-attempts* を入力して、**Enter** キーを押します。

ログイン認証方法を設定する方法

プライマリ ログイン認証方法が失敗した場合に使用される、「バックアップ」のログイン認証方法を設定できます（「一般的な AAA フォールバックと回復メカニズム」（P.5-8）を参照）。

使用するログイン認証方法と優先順位を指定するには、このコマンドを使用します。

- 「オプション」（P.5-17）
- 「ログイン認証方法を指定する方法」（P.5-17）
- 「ログイン認証方法リストを削除する方法」（P.5-17）

オプション

次のオプションを使用できます。

- **method**：使用するログイン認証方法。使用する順番に、最大 4 つの方法を指定できます。
  - **group TACACS+**：TACACS+ 認証を使用します。
  - **local**：認証にローカル ユーザ データベースを使用します。
  - **enable**（デフォルト）：認証に「**enable**」パスワードを使用します。
  - **none**：認証を使用しません。

ログイン認証方法を指定する方法

ステップ 1　SCE(config)# プロンプトに、**aaa authentication login default method1 [method2...]** を入力して、**Enter** キーを押します。

最大 4 つの方法を列挙できます。4 つの方法については、前述の説明を参照してください。優先度が高い順にメソッドを列挙します。

ログイン認証方法リストを削除する方法

ステップ 1　SCE(config)# プロンプトに、**no aaa authentication login default** を入力して、**Enter** キーを押します。

ログイン認証方法リストを削除すると、デフォルトの認証方法だけ（イネーブル パスワード）が使用されます。TACACS+ 認証は使用されません。

AAA 特権レベルの許可方法の設定

- 「オプション」（P.5-17）
- 「AAA 特権レベルの許可方法を指定する方法」（P.5-18）
- 「AAA 特権レベルの許可方法リストを削除する方法」（P.5-18）

オプション

次のオプションを使用できます。

- **method**：使用するログイン許可方法。使用する順番に、最大 4 つの方法を指定できます。
  - **group TACACS+**：TACACS+ 許可を使用します。

- **local**：許可にローカル ユーザ データベースを使用します。
- **enable**（デフォルト）：許可に「**enable**」パスワードを使用します。
- **none**：許可を使用しません。

AAA 特権レベルの許可方法を指定する方法

ステップ 1　SCE(config)# プロンプトに、**aaa authentication enable default method1 [method2...]** を入力して、**Enter** キーを押します。

最大 4 つの方法を列挙できます。4 つの方法については、前述の説明を参照してください。優先度が高い順にメソッドを列挙します。

AAA 特権レベルの許可方法リストを削除する方法

ステップ 1　SCE(config)# プロンプトに、**no aaa authentication enable default** を入力して、**Enter** キーを押します。

特権レベルの許可方法リストを削除すると、デフォルトのログイン認証方法だけ（イネーブル パスワード）が使用されます。TACACS+ 認証は使用されません。

AAA アカウンティングの設定

TACACS+ アカウンティングをイネーブルまたはディセーブルにするには、このコマンドを使用します。

- 「オプション」（P.5-18）
- 「AAA アカウンティングをイネーブルにする方法」（P.5-18）
- 「AAA アカウンティングをディセーブルにする方法」（P.5-19）

TACACS+ アカウンティングがイネーブルの場合、各コマンドの実行後に、SCE プラットフォームから TACACS+ サーバにアカウンティング メッセージが送信されます。アカウンティング メッセージは TACACS+ サーバで記録され、ネットワーク管理者に使用されます。

デフォルトで、TACACS+ のアカウンティングはディセーブルです。

オプション

次のオプションを使用できます。

- **level**：TACACS+ のアカウンティングをイネーブルにする特権レベル

AAA アカウンティングをイネーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**aaa authentication accounting commands** *level* **default stop-start group tacacs+** を入力して、**Enter** キーを押します。

start-stop キーワード（必須）は、CLI コマンドが正常に実行された場合、コマンドの開始時と終了時にアカウンティング メッセージが送信されることを示します。

AAA アカウンティングをディセーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**aaa authentication accounting commands** *level* **default** を入力して、**Enter** キーを押します。

TACACS+ サーバのモニタリング

TACACS+ サーバの統計情報を表示するには、このコマンドを使用します。

- 「TACACS+ サーバの統計情報を表示する方法」（P.5-19）
- 「TACACS+ サーバの統計情報、キー、およびタイムアウトを表示する方法」（P.5-19）

TACACS+ サーバの統計情報を表示する方法

ステップ 1　SCE# プロンプトに、**show tacacs** を入力して、**Enter** キーを押します。

TACACS+ サーバの統計情報、キー、およびタイムアウトを表示する方法

ステップ 1　SCE# プロンプトに、**show tacacs all** を入力して、**Enter** キーを押します。

ほとんどの show コマンドは Viewer レベルのユーザでも使用できますが、**'all'** オプションを使用できるのは Admin レベルだけです。**'enable 10'** コマンドを使用して、Admin レベルにアクセスします。

TACACS+ ユーザのモニタリング

パスワードを含め、ローカル データベースのユーザを表示するには、このコマンドを使用します。

ステップ 1　SCE# プロンプトに、**show users** を入力して、**Enter** キーを押します。

ほとんどの show コマンドは Viewer レベルのユーザでも使用できますが、このコマンドを使用できるのは Admin レベルだけです。**'enable 10'** コマンドを使用して、Admin レベルにアクセスします。

ACL の設定

- 「オプション」（P.5-20）
- 「ACL にエントリを追加する方法」（P.5-20）
- 「ACL を削除する方法」（P.5-21）
- 「ACL をイネーブルにする方法」（P.5-21）

SCE プラットフォームに Access Control List（ACL; アクセス コントロール リスト）を設定できます。ACL は、管理インターフェイスの着信接続をグローバルに許可または拒否するために使用されます。アクセス リストは、IP アドレスの範囲を定義する IP アドレスとオプションのワイルドカード「マスク」、および許可 / 拒否フィールドで構成されているエントリの順序付きリストです。

リスト内のエントリの順序は重要です。接続に一致する最初のエントリのデフォルト アクションが使用されます。アクセス リストのエントリが接続に一致しない場合、またはアクセス リストが空白である場合、デフォルト アクションは deny になります。

システム アクセスの設定は、2 段階で行われます。

1. アクセス リストの作成 （「ACL にエントリを追加する方法」（P.5-20）を参照）。
2. アクセス リストのイネーブル化（「ACL をイネーブルにする方法」（P.5-21）を参照）。

アクセス リストの作成は、最初から最後までエントリごとに行われます。

システムがアクセス リストに IP アドレスがあるかどうかを確認する場合、システムはアクセス リストの各行（最初のエントリから開始して、順番に最後のエントリまで移動）を確認します。検出された最初の一致が（つまり、調べていた IP アドレスが、エントリによって定義された IP アドレス範囲内にあった場合）、一致したエントリの許可/拒否フラグに従って、結果を決定します。アクセス リストに一致するエントリがない場合は、アクセスが拒否されます。

最大 99 のアクセス リストを作成できます。

ACL をイネーブルにするには、**ip access-class** コマンドを使用します。ACL がイネーブルの場合、SCE に要求を送信すると、まずその IP アドレスからのアクセスについて権限があるかどうかが確認されます。許可がない場合、SCE はこの要求に応答しません。基本的な IP インターフェイスは低いレベルのもので、インターフェイスに到達する前に IP パケットをブロックします。

ACL がイネーブルではない場合、すべての IP アドレスからのアクセスが許可されます。

（注）　SCE プラットフォームは、アクセスが許可された IP アドレスから送信された **ping** コマンドだけに応答します。ping は ICMP プロトコルを使用するので、未認証のアドレスから送信された ping は、SCE プラットフォームからの応答を受信しません。

オプション

次のオプションを使用できます。

- **number**：アクセス コントロール リストに割り当てる ID 番号。
- **ip-address**：許可または拒否するインターフェイスの IP アドレス。x.x.x.x 形式で入力します。
- **ip-address/mask**：x.x.x.x y.y.y.y 形式のアドレスの範囲を設定します。この x.x.x.x は、範囲内のすべての IP アドレスに共通のプレフィクス ビットを示します。y.y.y.y は、無視するビットを示すワイルドカードビットのマスクです。この表記では、「0」が無視するビットです。

次のキーワードを使用できます。

- **permit**：指定した IP アドレスは、SCE プラットフォームにアクセスする権限を持ちます。
- **deny**：指定した IP アドレスは、SCE プラットフォームへのアクセスが拒否されます。

ACL にエントリを追加する方法

ステップ 1　**configure** を入力して、**Enter** キーを押します。

グローバル コンフィギュレーション モードをイネーブルにします。

ステップ 2　対象の IP アドレスを 1 つまたは複数入力します。

- IP アドレス タイプを 1 つ設定するには

  access-list *number* **permit|deny** *ip-address* を入力して、**Enter** キーを押します。

- 複数の IP アドレスを設定するには

  access-list *number* **permit|deny** *ip-address/mask* を入力して、**Enter** キーを押します。

ACL に新規のエントリを追加する場合、エントリは常にリストの末尾に追加されます。

ACL へのエントリの追加：例

次に、アクセス リスト番号 1 に 10.1.1.0 ～ 10.1.1.255 の範囲の IP アドレスだけにアクセスを許可するエントリを追加する例を示します。

```
SCE(config)#access-list 1 permit 10.1.1.0 0.0.0.255
```

ACL を削除する方法

すべてのエントリを含め ACL を削除するには、このコマンドを使用します。

ステップ 1　SCE(config)# プロンプトに、**no access-list** *number* を入力して、**Enter** キーを押します。

すべてのエントリを含め、指定した ACL が削除されます。

ACL をイネーブルにする方法

ACL によって、SCE プラットフォームへのすべてのトラフィックが許可または拒否されます。

ステップ 1　SCE(config)# プロンプトに、**ip access-class** *number* を入力して、**Enter** キーを押します。

SCE プラットフォームにアクセスを試みるすべてのトラフィックに対して、指定した ACL が適用されます。

Telnet インターフェイスの管理

- 「Telnet アクセスを防ぐ方法」（P.5-22）
- 「Telnet のタイムアウトを設定する方法」（P.5-22）

ここでは、SCE プラットフォームの Telnet インターフェイスについて説明します。Telnet セッションは、SCE プラットフォームの CLI インターフェイスに接続する最も一般的な方法です。

Telnet インターフェイスに次のパラメータを設定できます。

- インターフェイスのイネーブル化およびディセーブル化
- Telnet セッションのタイムアウト（セッションにアクティビティが存在しない場合に、Telnet 接続を自動切断するまでに SCE プラットフォームが待機する時間）

Telnet インターフェイスに関連するコマンドは、次のとおりです。

- **line vty**
- **[no] access list**
- **[no] service telnetd**

- **[no] timeout**
- **show line vty timeout**

Telnet アクセスを防ぐ方法

Telnet によるアクセスを全体的にディセーブルにするには、このコマンドを使用します。

ステップ 1　SCE(config)# プロンプトに、**no service telnetd** を入力して、**Enter** キーを押します。

現在の Telnet セッションは切断されていませんが、新規の Telnet セッションが許可されなくなります。

Telnet のタイムアウトを設定する方法

SCE プラットフォームは、非アクティブの Telnet セッションのタイムアウトをサポートしています。

オプション

次のオプションを使用できます。

- **timeout**：非アクティブな Telnet セッションがタイムアウトするまでの時間（分）。
  - デフォルト：30 分

ステップ 1　SCE(config-line)# プロンプトに、**timeout** *timeout* を入力して、**Enter** キーを押します。

SSH サーバの設定

SSH サーバ

標準 Telnet プロトコルの欠点は、インターネット上でパスワードとデータを暗号化せずに転送するため、セキュリティが万全ではない点です。セキュリティを懸念する場合には、Telnet ではなく Secure Shell（SSH; セキュア シェル）サーバの使用を推奨します。

SSH サーバは Telnet サーバに類似していますが、SSH サーバは、通信のプライバシーを保証することにより、安全でないネットワーク上で SSH クライアントとの通信を行うことができる暗号技術を使用しています。CLI コマンドは、SSH でも Telnet とまったく同じ方法で実行されます。

SSH サーバは、SSHv1 と SSHv2 の両方のプロトコルをサポートしています。SSHv2 だけを実行するには、SSHv1 をディセーブルにします。

SSH サーバがサポートする暗号化方法は次のとおりです。

- aes256-ctr、aes192-ctr、aes128-ctr（RFC-4344、セクション 4）。

- 3des-cbc、blowfish-cbc、aes256-cbc、aes192-cbc、aes128-cbc、arcfour、cast128-cbc（RFC-4253、セクション 6.3）。
- arcfour128、arcfour256（RFC-4345、セクション 4）。
- rijndael-cbc@lysator.liu.se（OpenSSH 4.7p1 の指定に従います）。

キーの管理

各種のクライアントとの通信を行う場合、各 SSH サーバは、キー（DSA2、RSA2、および RSA1）のセットを定義する必要があります。キー セットとは、パブリック キーとプライベート キーのペアです。サーバは不揮発性メモリにプライベート キーを置きながら、パブリック キーを発行し、SSH クライアントに伝送することはありません。キーは tffs0 ファイル システムに置かれます。これは、「enable」パスワードの知識があるユーザがプライベート キーとパブリック キーの両方にアクセスできることを意味します。SSH サーバの実装は、SCE プラットフォームの管理通信チャネルを監視できる盗聴者に対する保護を提供していますが、「enable」パスワードの知識があるユーザに対する保護は提供していません。

特定の CLI コマンドを介して、ユーザがキーの管理を実行します。SSH サーバをイネーブルにする前に、最低 1 回、キーのセットを生成する必要があります。

暗号キーのサイズは、常に 2048 ビットです。

SSH サーバの管理

SSH サーバを管理するには、これらのコマンドを使用します。実行内容は、次のとおりです。

- SSH キー セットの生成
- SSH サーバのイネーブル化/ディセーブル化
- SSHv1 のイネーブル化/ディセーブル化（SSHv1 をディセーブルにすることで、SSHv2 だけを実行できます）
- 既存の SSH キーの削除

SSH キーのセットを生成する方法

SSH サーバをイネーブルにする前に、SSH キーのセットを生成する必要があります。

ステップ 1　SCE(config)# プロンプトに、**ip ssh key generate** を入力して、**Enter** キーを押します。

新規の SSH キー セットが生成され、すぐに不揮発性メモリに保存されます（キー セットは、コンフィギュレーション ファイルには含まれません）。キーのサイズは、常に 2048 ビットです。

SSH サーバをイネーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**ip ssh** を入力して、**Enter** キーを押します。

SSH サーバをディセーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**no ip ssh** を入力して、**Enter** キーを押します。

SSHv2 だけを実行する方法

ステップ 1　SCE(config)# プロンプトに、**ip ssh** を入力して、**Enter** キーを押します。

ステップ 2　SCE(config)# プロンプトに、**no ip ssh sshv1** を入力して、**Enter** キーを押します。

SSHv1 を再びイネーブルにするには、**ip ssh SSHv1** コマンドを使用します。

既存の SSH キーを削除する方法

ステップ 1　SCE(config)# プロンプトに、**ip ssh key remove** を入力して、**Enter** キーを押します。

既存の SSH キー セットが不揮発性メモリから削除されます。

SSH サーバは起動時にだけ不揮発性メモリからキーを読み取るので、SSH サーバが現在イネーブルにされている場合は、継続して動作します。ただし、SSH サーバがイネーブルにされていることをスタートアップ設定が示す場合、キーが削除されていると、SCE プラットフォームが起動時に SSH サーバを起動できません。このような状況を回避するには、このコマンドの実行後、**リロード**を使用して SCE プラットフォームが再起動される前に、次のいずれかを必ず実行してください。

- 新規のキー セットを生成する
- SSH サーバをディセーブルにし、設定を保存する

SSH サーバのステータスを監視する方法

現在の SSH セッションを含む SSH サーバのステータスを監視するには、このコマンドを使用します。

ステップ 1　SCE> プロンプトに、**show ip ssh** を入力して、**Enter** キーを押します。

これは ユーザ EXEC コマンドです。他のモードを終了して、ユーザ EXEC コマンド モードに移行してください。

SNMP インターフェイスのイネーブル化

明示的に SNMP インターフェイスをイネーブルにするには、このコマンドを使用します。

snmp-server コマンドを実行して任意の SNMP パラメータを設定すると、SNMP インターフェイスは暗黙的にイネーブルにされます。ホスト、コミュニティ、場所、およびトラップ先ホストなど、SNMP パラメータの設定および管理の詳細については、see 「SNMP インターフェイスの設定と管理」（P.5-25）を参照してください。

- 「SNMP インターフェイスをイネーブルにする方法」（P.5-25）

- 「SNMP インターフェイスをディセーブルにする方法」（P.5-25）

SNMP インターフェイスをイネーブルにする方法

SNMP アクセスを許可するには、最低 1 つコミュニティ ストリングを定義する必要があります。コミュニティ ストリングの詳細については、「SNMP コミュニティ ストリングの設定」（P.5-28）を参照してください。

ステップ 1　SCE(config)# プロンプトに、**snmp-server enable** を入力して、**Enter** キーを押します。

SNMP インターフェイスをディセーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**no snmp-server** を入力して、**Enter** キーを押します。

SNMP インターフェイスの設定と管理

SNMP インターフェイスについて

ここでは、SNMP エージェントのパラメータの設定方法について説明します。また、SNMP 通知と関連する CLI コマンドの簡単な概要についても説明します。

SNMP プロトコル

SNMP は、複雑なネットワークの管理用のプロトコル セットです。SNMP は、Protocol Data Unit（PDU; プロトコル データ ユニット）と呼ばれるメッセージをネットワークの別の部分に送信することによって機能します。エージェントと呼ばれる SNMP ここに準拠のデバイスは、Management Information Bases（MIB; 管理情報ベース）にそのデバイスに関するデータを保存し、このデータを SNMP 要求者に戻します。

SCE プラットフォームは、オリジナルの SNMP プロトコル（別名、SNMPv1）、およびコミュニティ ベースの SNMPv2 と呼ばれる新規のバージョン（別名、SNMPv2C）をサポートしています。

- **SNMPv1**：RFC 1155 と RFC 1157 で定義されている完全なインターネット標準である SNMP の最初のバージョンです。SNMPv1 は、コミュニティベースの形式によるセキュリティを使用します。
- **SNMPv2c**：プロトコル パケットのタイプ、トランスポート マッピング、および MIB 構造の要素の部分が SNMPv1 から改善されているものの、既存の SNMPv1 管理構造を使用している、改訂版のプロトコルです。RFC 1901、RFC 1905、および RFC 1906 で定義されています。

SNMP の SCE プラットフォーム実装は、RFC 1213 に記述されているすべての MIB II 変数をサポートし、RFC 1215 に記述されているガイドラインを使用して SNMP トラップを定義します。

SNMPv1 と SNMPv2C の仕様は、SCE プラットフォームでサポートされている次の基本操作を定義しています。表 5-2 に、要求タイプとその説明を示します。

表 5-2　　要求タイプ

要求タイプ	説明	備考
Set-request	エージェントによって管理されている 1 つ以上のオブジェクトに新規のデータを書き込みます。	操作を設定すると、SCE プラットフォームの running-config にすぐに影響しますが、startup-config には影響しません。
Get-request	エージェントによって管理されている 1 つ以上のオブジェクトの値を要求します。	
Get-next-request	エージェントによって管理されている次のオブジェクトの Object Identifier（OID; オブジェクト識別子）と値を要求します。	
Get-response	エージェントによって戻されたデータが含まれます。	
Trap	エージェント システムでイベントまたはエラーが発生したことを示す非送信請求通知をエージェントからマネージャに送信します。	SNMPv1 または SNMPv2 スタイルのいずれかのトラップを送信するように、SCE プラットフォームを設定できます。
Get-bulk-request	1 つの要求/応答トランザクションで大量のオブジェクト情報を取得します。Get-bulk は、1 つの要求/応答によって実行されていますが、Get-next の要求/応答が繰り返し実行されているかのように動作します。	これは、新しく定義された SNMPv2c メッセージです。

セキュリティの考慮事項

デフォルトでは、SNMP エージェントの読み取りと書き込みの両方の操作がディセーブルにされています。イネーブルにすると、管理ポート上でだけ SNMP がサポートされます（帯域内管理はサポートされません）。

また、SCE プラットフォームは、マネージャのコミュニティによる読み書きまたは読み取り専用のアクセスをサポートしています。

CLI について

SCE プラットフォームは、SNMP エージェントの操作を制御する CLI コマンドをサポートしています。Admin 許可レベルでは、すべての SNMP コマンドを使用できます。SNMP エージェントは、デフォルトでディセーブルにされており、明示的にディセーブルのコマンドが使用されている場合を除いて、任意の SNMP コンフィギュレーション コマンドによって、SNMP エージェントがイネーブルになります。

SNMP の設定に使用する CLI コマンド

次に、SNMP の設定に使用できる CLI コマンドを示します。これらはグローバル コンフィギュレーション モード コマンドです。

- **snmp-server enable**
- **no snmp-server**
- **[no] snmp-server community [all]**
- **[no | default] snmp-server enable traps**
- **[no] snmp-server host [all]**
- **[no] snmp-server contact**
- **[no] snmp-server location**

SNMP のモニタリングに使用する CLI コマンド

次に、SNMP のモニタリングに使用できる CLI コマンドを示します。これらは Viewer モード コマンドです。SNMP エージェントがイネーブルの場合に使用できます。

- show snmp（SNMP エージェントがディセーブルにされている場合に使用できます）
- show snmp community
- show snmp contact
- show snmp enabled
- show snmp host
- show snmp location
- show snmp MIB（SNMP エージェントがイネーブルで、コミュニティが設定されていた場合に使用できます）
- show snmp traps

MIB について

MIB は、NMS による監視が可能なオブジェクトのデータベースです。SNMP は、MIB によって定義されたデバイスのモニタを SNMP ツールに許可する標準 MIB 形式を使用します。

Cisco SCE8000 プラットフォームで使用する MIB の詳細については、「シスコ サービス コントロール MIB」（P.A-1）を参照してください。

SNMP による設定

SCE プラットフォームは、SNMP による設定が可能な限られた変数のセット（読み書き変数）をサポートしています。CLI と同様に SNMP を介して変数を設定すると、すぐに実行コンフィギュレーションに影響します。次の再起動用（スタートアップ コンフィギュレーション）にこのコンフィギュレーションを保存するには、シスコ製エンタープライズ MIB オブジェクトを使用して、CLI または SNMP 経由でこのコンフィギュレーションを明示的に指定する必要があります。

SCE プラットフォームでは、このデータベースの変更が可能な複数のインターフェイスによって、1 つのコンフィギュレーション データベースが処理されることにも注意してください。そのため、CLI または SNMP を介して **copy running-config startup-config** コマンドを実行して、SNMP または CLI で行ったすべての変更内容を永久に残します。

SNMP コミュニティ ストリングの設定

SNMP 管理をイネーブルにするには、SNMP コミュニティ ストリングを設定して、SNMP マネージャとエージェント間の関係を定義する必要があります。

SNMP 要求を受信すると、SNMP エージェントは、要求に含まれたコミュニティ ストリングとエージェントに設定されたコミュニティ ストリングを照らし合わせます。次の環境において、要求が有効になります。

- 要求に含まれたコミュニティ ストリングが読み取り専用コミュニティに一致する場合、SNMP の *Get*、*Get-next*、および *Get-bulk* の要求が有効です。
- 要求に含まれたコミュニティ ストリングがエージェントの読み書きコミュニティに一致する場合、SNMP の *Get*、*Get-next*、*Get-bulk*、および *Set* の要求が有効です。

コミュニティ ストリングを定義する方法

オプション

次のオプションを使用できます。

- **community-string**：SNMP サーバにアクセスできるマネージャのコミュニティを指定するセキュリティ文字列

次のキーワードを使用できます。

- **ro**：読み取り専用（デフォルトのアクセシビリティ）
- **rw**：読み取りと書き込み

ステップ 1　SCE(config)# プロンプトに、**snmp-server community** *community-string* **ro|rw** を入力して、**Enter** キーを押します。

必要に応じてコマンドを繰り返し、すべてのコミュニティ ストリングを定義します。

コミュニティ ストリングの定義：例

次に、読み取り専用権限を使用して「mycommunity」というコミュニティ ストリングを設定する例を示します。

読み取り専用はデフォルトなので、明示的に定義する必要はありません。

```
SCE(config)#snmp-server community mycommunity
```

コミュニティ ストリングを削除する方法

ステップ 1　SCE(config)# プロンプトに、**no snmp-server community** *community-string* を入力して、**Enter** キーを押します。

コミュニティ ストリングの削除：例

次に、「mycommunity」というコミュニティ ストリングを削除する例を示します。

```
SCE(config)#no snmp-server community mycommunity
```

設定済みのコミュニティ ストリングを表示する方法

ステップ 1　SCE> プロンプトに、**show snmp-server community** *community-string* を入力して、**Enter** キーを押します。

設定済みのコミュニティ ストリングの表示：例

次に、設定済みの SNMP コミュニテイを表示する例を示します。

```
SCE>show snmp community
Community: public, Access Authorization: RO, Access List Index: 1
SCE>
```

SNMP 通知を設定する方法

設定には、このコマンドを使用します。

- SNMP 通知を受信する宛先（ホスト）
- 通知を送信するタイプ（トラップ）
- 「SNMP ホストを定義する方法」（P.5-30）

通知は、イベントが発生したときに、SCE プラットフォームに内蔵された SNMP エージェントが生成する非送信請求メッセージです。Network Management System（NMS; ネットワーク管理システム）が通知メッセージを受信すると、イベントの発生を記録したり、信号を無視したり、適切なアクションを行うことができます。

デフォルトでは、SCE プラットフォームが SNMP トラップを送信するように設定されていません。SCE プラットフォームから通知を送信する NMS を定義する必要があります（設定可能な通知のリストについては、以下の表の「設定可能な通知」を参照）。通知を誘発するイベントのいずれかが SCE プラットフォームで発生すると、必ず SNMP 通知が SCE プラットフォームからユーザが定義する IP アドレスのリストに送信されます。

SCE プラットフォームは、2 つの一般的なカテゴリの通知をサポートしています。

- 標準の SNMP 通知：RFC 1157 に定義されており、RFC 1215 に定義された表記法を使用しています。
- 独自のサービス コントロール エンタープライズ通知：サービス コントロールの独自の MIB の定義に従います（表 A-20（P.A-20）を参照）。

通知を受信するように 1 つまたは複数のホストを設定すると、デフォルトでは、SCE プラットフォームからホストに対して、AuthenticationFailure 通知を除き、SCE プラットフォームがサポートするすべての通知が送信されます。SCE プラットフォームは、この通知に加えて、一部の SCE エンタープライズ通知の送信を明示的にイネーブルまたはディセーブルにするオプションを提供しています。

SNMPv1 または SNMPv2 スタイルの通知を生成するように SCE プラットフォームを設定できます。デフォルトでは、SCE プラットフォームは SNMPv1 通知を送信します。

次の処理を実行する手順の例を示します。

- SNMP エージェントが通知を送信する先のホスト（NMS）を構成する
- 受信通知からホスト（NMS）を削除/ディセーブルにする
- SNMP エージェントから認証エラー通知を送信できるようにする
- SNMP エージェントからエンタープライズ通知を送信できるようにする
- すべての通知をデフォルト設定にリセットする

SNMP ホストを定義する方法

SCE プラットフォームから通知を受信するホストを定義するには、このコマンドを使用します。

- 「オプション」（P.5-30）
- 「ホスト（NMS）に通知を送信するように SCE プラットフォームを設定する方法」（P.5-30）
- 「ホストへの通知送信を停止するように SCE プラットフォームを設定する方法」（P.5-31）
- 「SNMP トラップを設定する方法」（P.5-31）

オプション

次のオプションを使用できます。

- **ip-address**：SNMP サーバ ホストの IP アドレス
- **community-string**：SNMP サーバにアクセスできるマネージャのコミュニティを指定するセキュリティ文字列
- **version**：システムで実行されている SNMP のバージョン。1 または 2c に設定できます。
  - デフォルト：1（SNMPv1）

ホスト（NMS）に通知を送信するように SCE プラットフォームを設定する方法

ステップ 1　SCE(config)# プロンプトに、**snmp-server host** *ip-address community-string* を入力して、**Enter** キーを押します。

バージョンを指定しない場合、SNMPv1 であると想定されます。

1 つのコマンドで指定できるのは 1 つのホストだけです。複数のホストを定義するには、1 ホストにつき 1 コマンドを実行します。

複数のホストに通知を送信する SCE プラットフォームの設定：例

次に、SNMPv1 通知を複数のホストに送信するように SCE プラットフォームを設定する例を示します。

```
SCE(config)#snmp-server host 10.10.10.10 mycommunity
SCE(config)#snmp-server host 20.20.20.20 mycommunity
SCE(config)#snmp-server host 30.30.30.30 mycommunity
SCE(config)#snmp-server host 40.40.40.40 mycommunity
```

ホストへの通知送信を停止するように SCE プラットフォームを設定する方法

ステップ 1　SCE(config)# プロンプトに、**no snmp-server host** *ip-address* を入力して、**Enter** キーを押します。

ホストへの通知送信を停止する SCE プラットフォームの設定：例

次に、[192.168.0.83] の IP アドレスを持つホストを削除する例を示します。

```
SCE(config)#no snmp-server host 192.168.0.83
```

SNMP トラップを設定する方法

定義済みのホストに送信される通知を設定するには、このコマンドを使用します。

- 「オプション」（P.5-31）
- 「SNMP サーバによる認証エラー通知の送信をイネーブルにする方法」（P.5-32）
- 「SNMP サーバによるすべてのエンタープライズ通知の送信をイネーブルにする方法」（P.5-32）
- 「SNMP サーバによる特定のエンタープライズ通知の送信をイネーブルにする方法」（P.5-32）
- 「すべての通知をデフォルトのステータスに戻す方法」（P.5-32）

オプション

次のオプションを使用できます。

- **snmp**：すべて、または特定の SNMP トラップをイネーブルまたはディセーブルにするオプションのパラメータ。

  デフォルトで、SNMP トラップはディセーブルです。

  snmp trap name：イネーブルまたはディセーブルにする特定の SNMP トラップを指定するオプションのパラメータ。

  現在、このパラメータに使用できる値は、**Authentication** だけです。

- **enterprise**：すべて、または特定のエンタープライズ トラップをイネーブルまたはディセーブルにするオプションのパラメータ。

  デフォルトで、エンタープライズ トラップはイネーブルです。

- **enterprise trap name**：イネーブルまたはディセーブルにする特定のエンタープライズ トラップを指定するオプションのパラメータ。

  値：attack、chassis、link-bypass、logger、operational-status、port-operational-status、pull-request-failure、RDR-formatter、session、SNTP、subscriber、system-reset、telnet、vas-traffic-forwarding

このパラメータは次のように使用します。

- ある種類のすべてのトラップをイネーブル/ディセーブルにするには、**snmp** または **enterprise** だけを指定します。

- 1 つの特定のトラップだけをイネーブル/ディセーブルにするには、**snmp** または **enterprise** に、目的のトラップ名を指定した trap name パラメータを追加します。
- すべてのトラップをイネーブル/ディセーブルにするには、**snmp** または **enterprise** を指定しません。

SNMP サーバによる認証エラー通知の送信をイネーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**snmp-server enable traps snmp authentication** を入力して、**Enter** キーを押します。

SNMP サーバによるすべてのエンタープライズ通知の送信をイネーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**snmp-server enable traps enterprise** を入力して、**Enter** キーを押します。

SNMP サーバによる特定のエンタープライズ通知の送信をイネーブルにする方法

ステップ 1　SCE(config)# プロンプトに、**snmp-server enable traps enterprise** *[attack|chassis|link-bypass|logger|operational-status|port-operational-status|pull-request-failure|RDR-formatter|session| SNTP|subscriber|system-reset|telnet|vas-traffic-forwarding]* を入力して、**Enter** キーを押します。

目的のエンタープライズ トラップ タイプを指定します。

SNMP サーバによる特定のエンタープライズ通知の送信のイネーブル化：例

次に、logger エンタープライズ 通知だけを送信するように SNMP サーバを設定する例を示します。

```
SCE(config)#snmp-server enable traps enterprise logger
```

すべての通知をデフォルトのステータスに戻す方法

ステップ 1　SCE(config)# プロンプトに、**default snmp-server enable traps** を入力して、**Enter** キーを押します。

SCE プラットフォームがサポートしているすべての通知が、デフォルトのステータスにリセットされます。