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、SNMP、SSH、TACACS+ のなどのさまざまな管理インターフェイスを設定する方法について説明します。また、ユーザ、パスワード、IP 設定、クロックおよび時間帯、ドメイン名を設定する方法も説明します。

管理インターフェイスとセキュリティ

Service Control Module には、1 つの RJ-45 管理（MNG）ポートが装備されています。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 セキュリティを設定するには、次のタスクを実行します。

- 管理ポートを設定します。
  - 物理パラメータ。
- 管理インターフェイス セキュリティを設定します。
  - 許可済みと非許可の IP アドレスを設定する。

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 アドレスおよびサブネット マスクを設定します。
- 次の物理パラメータを設定します。
  - 速度
  - デュプレックス

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て、必要な管理ポートをケーブル接続します。

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 モードを開始するには

GBE 管理インターフェイスは、次のとおりに設定されます。

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

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

グローバル コンフィギュレーション モードが開始されます。

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** と入力し、**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 モードが開始されます。

コマンド プロンプトが 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、管理動作と RDR（トラフィック分析と管理動作の出力）の伝送用に使用されます。

- 「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速度パラメータとデュプレックス パラメータの設定」（P.5-3）
- 「管理インターフェイスをモニタリングするには」（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

ユーザは、管理インターフェイスの IP アドレスを設定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)# プロンプトで、**ip address** *ip-address subnet-mask* と入力し、**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、SCE プラットフォームのすべての内外のコンポーネントで変更が有効になるよう、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.3-16）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速度パラメータとデュプレックス パラメータの設定

ここでは、管理インターフェイスの速度とデュプレックスを設定する方法を説明する手順の例を示します。

これらのパラメータは、両方、各ポートで別々に設定する必要があります。

- 「速度とデュプレックス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には」（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には」（P.5-5）

速度とデュプレックス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、速度、デュプレックスの間の関係を要約します。

次の点に注意してください。

- 一方のパラメータを "Auto" に、もう一方のパラメータを別の値に、設定することはできません。いずれかの速度またはデュプレックスが "Auto" に設定された場合、両方のパラメータが "Auto" に設定されているかのように動作します。
- インターフェイスの性質のため、1000 Mbps の動作は、オートネゴシエーションがイネーブルの場合にのみ使用できます。

表 5-1　速度とデュプレックスのインターフェイス ステートの関係

速度	デュプレックス	実際の FEI インターフェイス ステート
Auto	Auto	自動ネゴシエーション
Auto	Full/Half	自動ネゴシエーション
10/100	Auto	自動ネゴシエーション
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には

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 Mbps 単位での速度
  - **10**
  - **100**
  - **auto**（デフォルト）：オートネゴシエーション（リンクで速度を強制的に実行しない）

デュプレックス パラメータが **auto** に設定されている場合、速度パラメータを変更しても影響はありません。

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

必要な速度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には

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（リンクでデュプレックスを強制的に実行しない）

速度パラメータが **auto** に設定されている場合、デュプレックス パラメータを変更しても影響はありません（ を参照）。

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

必要なデュプレックス 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モニタリングするには

管理インターフェイスに関する次の情報を表示するには、ここで説明する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# プロンプトで、**show GigabitEthernet interface Mng 1/1 [auto-negotiate|ip address]** と入力し、Enter キーを押します。

GBE 管理インターフェイスの設定が表示されます。オプションが指定されなかった場合、管理インターフェイスのすべての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システムの外部コンポーネントの管理設計に基づいて、Telnet と SNMP（簡易ネットワーク管理プロトコル）のインターフェイスを設定できます。

- 「TACACS+ の認証、認可、アカウンティング」（P.5-6）
- 「ACL の設定」（P.5-20）
- 「Telnet インターフェイスの管理」（P.5-22）
- 「SSH サーバの設定」（P.5-23）
- 「SNMP インターフェイスのイネーブル化」（P.5-25）

TACACS+ の認証、認可、アカウンティング

TACACS+ の認証、認可、アカウンティングについて

TACACS+ の認証、認可、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の、一元的な認証機能を提供するセキュリティ アプリケーションです。TACACS+ プロトコルの実装により、ユーザは、認証サーバで各ユーザを認証することによって、SCE プラットフォームを安全に管理できるよう、SCE プラットフォームの 1 つまたは複数の認証サーバを設定できます。次に、認証データベースを一元化し、SCE プラットフォームの管理をより簡単にします。

TACACS+ サービスは、UNIX または Windows NT のワークステーションで通常実行される TACACS+ サーバにあるデータベースで管理されます。ネットワーク要素上で設定されている TACACS+ 機能を使用可能にするには、まず TACACS+ サーバにアクセスし、TACACS+ サーバを設定する必要があります。

TACACS+ プロトコルにより、ネットワーク要素と TACACS+ ACS との間の認証が行われます。また、キーが設定されている場合は、ネットワーク要素と TACACS+ との間のすべてのプロトコルのやり取りを暗号化することによって、機密保持を行うことができます。

TACACS+ プロトコルは、次の 3 つの機能を提供します。

- ログイン認証
- 権限レベルの認可
- アカウンティング

ログイン認証

SCE プラットフォームでは、CLI、Telnet、および SSH へのアクセスに、TACACS+ ASCII 認証メッセージが使用されます。

TACACS+ を使用すると、ユーザの認証に十分な情報をサーバで受信するまで、サーバとユーザの間では、任意通信を行えます。これは、通常、ユーザ名とパスワードの組み合わせのプロンプトを表示することによって行われます。

ログインとパスワードのプロンプトは、TACACS+ サーバによって表示されることがあります。または、TACACS+ サーバによってプロンプトが表示されない場合、ローカル プロンプトが使用されます。

情報にあるユーザ ログ（ユーザ名およびパスワード）は、認証の目的で、TACACS+ サーバに送信されることがあります。TACACS+ サーバにより、ユーザが認証されないことが示されると、ユーザに対して、ユーザ名とパスワードの入力を促すプロンプトが再表示されます。（ユーザがコンソール ポートに接続されている場合を除き、）失敗したログインが SCE プラットフォームのユーザ ログに記録され、Telnet セッションが強制終了された後で、ユーザに対し、ユーザ設定が可能な回数の入力を促すプロンプトが表示されます。

SCE プラットフォームでは、最後に、TACACS+ サーバから次の応答の 1 つを受信します。

- ACCEPT：ユーザは認証され、サービスを開始できます。
- REJECT：ユーザは、認証に失敗しました。ユーザは、今後のアクセスを拒否されるか、または、TACACS+ サーバによっては、ログイン シーケンスを再試行するプロンプトが表示されます。
- ERROR：認証中のいずれかの時点で、エラーが発生しました。これは、サーバと SCE プラットフォームの間での、サーバまたはネットワーク接続のいずれかで発生した可能性があります。エラーの応答を受信した場合、SCE プラットフォームでは、ユーザの認証に代替の方法またはサーバの使用を試みます。
- CONTINUE：ユーザに対し、追加の認証情報の入力を促すプロンプトが表示されます。

「AAA フォールバックおよびリカバリの通常のメカニズム」（P.5-8）で説明しているように、サーバが使用できない場合、次の認証方法が試行されます。

アカウンティング

TACACS+ アカウンティングでは、次の機能がサポートされます。

- 実行される（有効な）各コマンドは、（ログインと終了のコマンドを含む）TACACS+ メカニズムを使用して記録されます。
- コマンドは、正常実行の前と後の両方で記録されます。
- 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
  - 実行されるアクション
  - コマンドの権限レベル

TACACS+ のアカウンティングは、SCE プラットフォームの dbg ログを使用した通常のローカル アカウンティングに加えて実行されます。

権限レベルの認可

正常なログイン後、ユーザには、デフォルト権限レベルの 0 が付与されます。ユーザには、限定的な数のコマンドを実行できる権限が付与されます。**"enable"** コマンドを実行することによって、権限レベルの変更が行われます。このコマンドにより、権限レベルの認可メカニズムが開始されます。

SCE プラットフォームでの権限レベルの認可は、**"enable"** コマンド認証要求の使用によって実行されます。ユーザが、**"enable"** コマンドを使用することによって、指定された権限レベルの認可を要求すると、SCE プラットフォームでは、要求された権限レベルを指定して TACACS+ サーバに認証要求を送信します。SCE プラットフォームでは、TACACS+ サーバによって次の操作が実行された後で、要求された権限レベルが付与されます。

- **" enable "** コマンド パスワードを認証する
- ユーザが、要求された権限レベルを開始するために十分な権限を付与されていることを確認する

ユーザ権限レベルが決定されると、ユーザは、付与されたレベルに従って、指定されたコマンドのセットへのアクセスが付与されます。

ログイン認証では、サーバが使用できない場合、「AAA フォールバックおよびリカバリの通常のメカニズム」（P.5-8）で説明している認証方法が試行されます。

AAA フォールバックおよびリカバリの通常のメカニズム

SCE プラットフォームでは、フォールバック メカニズムを使用して、エラーの場合のサービス アベイラビリティが維持されます。

使用可能な AAA 方式は、次のとおりです。

- **TACACS+**：AAA は、TACACS+ サーバの使用によって実行され、認証、認可、アカウンティングを実行できます。
- **Local**：AAA は、ローカル データベースの使用によって実行され、認証と認可を実行できます。
- **Enable**：AAA は、ユーザが設定したパスワードの使用によって実行され、認証と認可を実行できます。
- **None**：認証、認可、アカウンティングは実行されません。

現在の実装では、使用される方式の順序は設定できませんが、ユーザは、使用する方式を選択できます。現在の順序は、次のとおりです。

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

（注） 重要：サーバが AAA フォルトに進む場合、AAA 方式の 1 つが復元されるまで、SCE プラットフォームにはアクセスできません。これを防ぐためには、最後の AAA 方式として "none" を使用することをお勧めします。SCE プラットフォームがアクセスできなくなった場合、シェル関数 "AAA_MethodsReset" を使用すると、現在の AAA 方式の設定を削除し、使用する AAA 方式を "Enable" に設定できます。

TACACS+ の設定について

次に、TACACS+ を設定する手順を要約します。このセクションの残りの部分では、すべての手順を詳細に説明します。

1. リモート TACACS+ サーバを設定します。

   このプロトコルのリモート サーバを設定します。次の注意事項に従ってください。

   - サーバとクライアントで使用される暗号キーを設定します。
   - 最高のユーザ権限レベルと有効なパスワード（**enable** コマンドの実行時に使用されるパスワード）を、指定する必要があります。
   - 設定には、常に、root ユーザを含め、権限レベルを 15 に設定する必要があります。
   - ビューア（権限レベル 5）とスーパーバイザ（権限レベル 10）のユーザ ID も、この時点で設定する必要があります。

2. サーバ構成の詳細は、使用する TACACS+ サーバの、該当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。

3. TACACS+ サーバとともに動作する 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
   - 共用の暗号キー（クライアントとサーバが通信するためには、設定されている暗号キーが、サーバ上に設定されている暗号キーと一致する必要があります）

4. （任意）ローカル データベースを使用する場合、次の設定を行います。

   - 新しいユーザの追加

   ローカル データベースと TACACS+ が両方とも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、同じユーザを設定することを推奨します。これによって、ユーザは、TACACS+ サーバの障害の発生時に、SCE プラットフォームにアクセスできます。

（注） ログイン方式として TACACS+ が使用される場合、**enable** コマンドで TACACS+ ユーザ名が自動的に使用されます。したがって、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が重要です。これによって、**enable** コマンドにより、このユーザ名を認識できます。

   - パスワードの指定
   - 権限レベルの定義

5. SCE プラットフォームで、認証方式を設定します。

   - ログイン認証方式
   - 権限レベル認可方式

6. 設定を見直します。

   " **show running-config** " コマンドを使用して、設定を参照します。

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には

ユーザは、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。SCE プラットフォームの TACACS+ クライアントは、TACACS+ サーバと動作するよう設定する必要があります。次の情報を設定する必要があります。

- TACACS+ サーバのホスト定義：最大で 3 台のサーバがサポートされます。

  サーバごとに、次の情報を設定できます。

  - ホスト名（必須）
  - ポート
  - 暗号キー
  - タイムアウトの間隔
- デフォルト暗号キー（任意）：グローバルなデフォルト暗号キーを設定できます。このキーは、サーバ ホストが定義される際に、キーが明示的に設定されていない任意のサーバ ホストのキーとして、設定されます。

  デフォルト暗号キーが設定されていない場合、キーがない状態のデフォルトが、キーが明示的に設定されていないサーバに割り当てられます。
- デフォルト タイムアウト間隔（任意）：グローバルなデフォルト タイムアウト間隔を定義できます。サーバ ホストが定義される際に、このタイムアウト間隔は、タイムアウト間隔が明示的に設定されていないサーバ ホストのタイムアウト間隔として定義されます。

  デフォルト タイムアウト間隔が設定されていない場合、デフォルトの 5 秒が、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割り当てられます。

SCE プラットフォームの TACACS+ クライアントを設定する手順は、次のセクションで説明します。

新しい TACACS+ サーバ ホストを追加するには

SCE プラットフォームの TACACS+ クライアントで使用可能な新しい TACACS+ サーバ ホストを定義するには、ここで説明するコマンドを使用します。

Service Control ソリューションでは、最大で 3 台の 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+ ポート番号。
  - デフォルト = 49
- **timeout interval**：タイムアウトの前に、サーバ ホストからの応答をサーバが待つ秒数。
  - デフォルト = 5 秒、またはユーザが定義したグローバルなデフォルト タイムアウト間隔（「グローバル デフォルト タイムアウトを定義するには」（P.5-12）を参照）
- **key-string**：相互通信時に、サーバおよびクライアントで使用される暗号キー。指定したキーが実際に TACACS+ サーバ ホストで設定されていることを確認してください。
  - デフォルト = キーがない、またはユーザが定義したグローバルなデフォルト キー（「グローバル デフォルト キーを定義するには」（P.5-11）を参照）

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

TACACS+ サーバ ホストを削除するには

オプション

次のオプションを使用できます。

- **host-name**：削除されるサーバの名前

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

グローバル デフォルト キーを設定するには

TACACS+ サーバ ホストのグローバル デフォルト キーを定義するには、ここで説明するコマンドを使用します。また、TACACS+ サーバ ホストで異なるキーを明示的に設定することによって、特定の TACACS+ ホストのデフォルト 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**：相互通信時に、すべての TACACS+ サーバとクライアントで使用されるデフォルト暗号キー。指定されるキーが実際に TACACS+ サーバ ホストで設定されていることを確認してください。
  - デフォルト = 暗号なし

グローバル デフォルト キーを定義するには

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

グローバル デフォルト キーをクリアするには

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

グローバル デフォルト キーは、定義されません。各 TACACS+ サーバ ホストでは、定義されている特定のキーがある可能性があります。ただし、明示的に定義されているキーがないサーバ ホスト（グローバル デフォルト キーを使用）は、キーを使用しないように設定されています。

グローバル デフォルト タイムアウトを設定するには

TACACS+ サーバ ホストのグローバル デフォルトのタイムアウト間隔を定義するには、ここで説明するコマンドを使用します。TACACS+ サーバ ホストで異なるタイムアウト間隔を明示的に設定することによって、特定の TACACS+ ホストのデフォルト タイムアウト間隔を上書きできます。

オプション

次のオプションを使用できます。

- **timeout interval**：タイムアウトの前に、サーバ ホストからの応答をサーバが待つデフォルトの秒数。
  - デフォルト = 5 秒

グローバル デフォルト タイムアウトを定義するには

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

グローバル デフォルト タイムアウトをクリアするには

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

グローバル デフォルトのタイムアウト間隔は、定義されません。各 TACACS+ サーバ ホストでは、定義されている特定のタイムアウト間隔がある可能性があります。ただし、明示的に定義されているタイムアウト間隔がないサーバ ホスト（グローバル デフォルト タイムアウト間隔を使用）は、5 秒のタイムアウト間隔で設定されています。

ユーザ データベースの管理

TACACS+ では、ローカル ユーザ データベースが管理されます。このローカル データベースには、最大 100 ユーザまでを設定できます。このローカル データベースには、すべてのユーザが使用する次の情報が含まれています。

- ユーザ名
- パスワード：暗号形式または非暗号形式で使用可
- 権限レベル

ローカル ユーザ データベースを管理する手順は、次のセクションで説明します。

- 「ローカル データベースに新しいユーザを追加するには」（P.5-13）

- 「ユーザ権限レベルを定義するには」（P.5-14）
- 「権限レベルとパスワードを持つ新しいユーザを追加するには」（P.5-15）
- 「ユーザを削除するには」（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には

ローカル データベースに新しいユーザを追加するには、ここで説明するコマンドを使用します。最大 100 の 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 パスワードを持つユーザを追加するには」（P.5-14）
- 「パスワードなしのユーザを追加するには」（P.5-14）
- 「クリア テキストで入力された MD5 暗号化パスワードを持つユーザを追加するには」（P.5-14）
- 「MD5 暗号化文字列で入力された MD5 暗号化パスワードを持つユーザを追加するには」（P.5-14）

オプション

パスワードは、ユーザ名で定義されます。いくつかのパスワード 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、クリア テキスト形式でローカル リストに保存されます。

  password パラメータを使用します。
- 暗号化パスワード：パスワードは、暗号化（MD5）形式でローカル リストに保存されます。シークレット キーワードを使用します。

  パスワードは、次のいずれかの方式で定義できます。
  - クリア テキスト パスワードを指定し、MD5 暗号化形式で保存します。
  - MD5 暗号化文字列を指定し、ユーザの MD5 暗号化形式のシークレット パスワードとして保存します。

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 パスワード。次の 2 つのいずれかの形式でローカル 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 キーワードが使用されている場合は、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たパスワードはありません。
- **secret**：パスワードは MD5 暗号化形式で保存されます。次のいずれかのキーワードを使用して、コマンドで入力したとおりにパスワードの形式を示します。
  - **0**：**password** オプションとともに使用して、クリア テキスト パスワードを指定します。MD5 暗号化形式で保存されます。
  - **5**：**encrypted-secret** オプションとともに使用して、MD5 暗号化文字列を指定します。ユーザ定義の MD5 暗号化シークレット パスワードとして保存されます。

クリア テキスト パスワードを持つユーザを追加するには

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

パスワードなしのユーザを追加するには

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

クリア テキストで入力された MD5 暗号化パスワードを持つユーザを追加するには

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

MD5 暗号化文字列で入力された MD5 暗号化パスワードを持つユーザを追加するには

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

ユーザ権限レベルを定義するには

- 「ユーザ権限レベルについて」（P.5-14）
- 「オプション」（P.5-14）

ユーザ権限レベルについて

SCE プラットフォームでの権限レベルの認可は、" **enable** " コマンド認証要求の使用によって実行されます。ユーザが、"**enable**" コマンドを使用することによって、指定された権限レベルの認可を要求すると、SCE プラットフォームは、要求された権限レベルを指定して TACACS+ サーバに認証要求を送信します。SCE プラットフォームでは、TACACS+ サーバによって " **enable** " コマンド パスワードが認証され、要求された権限レベルを開始するためにユーザが十分な権限が付与されていることを確認した後でのみ、要求された権限レベルが付与されます。

オプション

次のオプションを使用できます。

- **name**：権限レベルが設定されるユーザの名前。
- **level**：指定されたユーザに許可される権限レベル。CLI 認可レベルに対応するこれらのレベルは、**enable** コマンドを介して入力されます。
  - 0：User
  - 10：Admin
  - 15（デフォルト）：Root

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

権限レベルとパスワードを持つ新しいユーザを追加するには

1 つのコマンドで、パスワードおよび権限レベルを含む新しいユーザを定義するには、ここで説明するコマンドを使用します。

（注） config ファイル（**running config** および **startup config**）では、このコマンドは 2 つの別々のコマンドとして表示されます。

- 「オプション」（P.5-15）
- 「権限レベルとクリア テキスト パスワードを持つユーザを追加するには」（P.5-16）
- 「権限レベルおよびクリア テキストで入力された MD5 暗号化パスワードを持つユーザを追加するには」（P.5-16）
- 「権限レベルおよび MD5 暗号化文字列で入力された MD5 暗号化パスワードを持つユーザを追加するには」（P.5-16）

オプション

次のオプションを使用できます。

- **name**：権限レベルが設定されるユーザの名前。
- **level**：指定したユーザに許可される権限レベル。CLI 認可レベルに対応するこれらのレベルは、**enable** コマンドを介して入力されます。
  - 0：User
  - 10：Admin
  - 15（デフォルト）：Root
- **password**：クリア テキスト パスワード。次の 2 つのいずれかの形式でローカル 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 キーワードが使用されている場合は、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**：パスワードは MD5 暗号化形式で保存されます。次のいずれかのキーワードを使用して、コマンドで入力したとおりにパスワードの形式を示します。
  - **0**：**password** オプションとともに使用して、クリア テキスト パスワードを指定します。MD5 暗号化形式で保存されます。
  - **5**：**encrypted-secret** オプションとともに使用して、MD5 暗号化文字列を指定します。ユーザ定義の MD5 暗号化シークレット パスワードとして保存されます。

権限レベルとクリア テキスト パスワードを持つユーザを追加するには

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

権限レベルおよびクリア テキストで入力された MD5 暗号化パスワードを持つユーザを追加するには

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

権限レベルおよび MD5 暗号化文字列で入力された MD5 暗号化パスワードを持つユーザを追加するには

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

ユーザを削除するには

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)# プロンプトで、**no username** *name* と入力し、**Enter** キーを押します。

AAA ログイン認証の設定

ログイン認証には、設定する 2 つの機能があります。

- 許可される最大の Telnet ログイン試行回数
- ログイン時に使用される認証方式（「AAA フォールバックおよびリカバリの通常のメカニズム」（P.5-8）を参照）

ログイン認証を設定する手順は、次のセクションで説明します。

- 「最大ログイン試行回数を設定するには」（P.5-16）
- 「ログイン認証方式を設定するには」（P.5-17）

最大ログイン試行回数を設定するには

セッションの強制終了前に許可されるログイン試行の最大回数を設定するには、ここで説明する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 セッションの強制終了前に許可されるログイン試行の最大回数。

  これは、Telnet セッションにのみ該当します。再試行の回数は、ローカル コンソールから制限されます。

  - デフォルト = 3

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

ログイン認証方式を設定するには

主要ログイン認証方式の障害の場合に使用する「バックアップ」ログイン方式を設定できます（「AAA フォールバックおよびリカバリの通常のメカニズム」（P.5-8）を参照）。

使用するログイン認証方式と、そのプリファレンスの順序を設定するには、ここで説明するコマンドを使用します。

- 「オプション」（P.5-17）
- 「ログイン認証方式を指定するには」（P.5-17）
- 「ログイン認証方式リストを削除するには」（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式。最大 4 つの異なる方式を、使用する順序で指定できます。
  - **group TACACS+**：TACACS+ 認証を使用します。
  - **local**：認証に、ローカル ユーザ名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**：認証は使用しません。

ログイン認証方式を指定するには

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

最大 4 つの方式をリストできます。前述の説明にある 4 つのすべての方式を指定できます。優先順位の順序でリスト表示します。

ログイン認証方式リストを削除するには

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

ログイン認証方式リストが削除されると、デフォルトのログイン認証方式のみ（enable パスワード）が使用されます。TACACS+ 認証は使用されません。

AAA 権限レベル認可方式の設定

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可方式。最大 4 つの異なる方式を、使用する順序で指定できます。
  - **group TACACS+**：TACACS+ 認可を使用します。
  - **local**：認可に、ローカル ユーザ名データベースを使用します。
  - **enable**（デフォルト）：認可に、" **enable** " パスワードを使用します。
  - **none**：認可は使用しません。

AAA 権限レベル認可方式を設定するには

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

最大 4 つの方式をリストできます。前述の説明にある 4 つのすべての方式を指定できます。優先順位の順序でリスト表示します。

AAA 権限レベル認可方式リストを削除するには

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

権限レベル認可方式リストが削除されると、デフォルトのログイン認証方式のみ（enable 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、ここで説明するコマンドを使用します。

TACACS+ アカウンティングがイネーブルの場合、SCE プラットフォームでは、各コマンドの実行後に TACACS+ サーバにアカウンティング メッセージを送信します。アカウンティング メッセージは、ネットワーク管理者が使用する TACACS+ サーバに記録されます。

デフォルトでは、TACACS+ アカウンティングがディセーブルにされています。

オプション

次のオプションを使用できます。

- **level**：TACACS+ アカウンティングをイネーブルにする権限レベル

AAA アカウンティングをイネーブルにするには

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

start-stop キーワード（必須）は、（コマンドが正常実行された場合に）CLI コマンドの実行の最初と最後でアカウンティング 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には

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

TACACS+ サーバのモニタリング

TACACS+ サーバの統計を表示するには、ここで説明するコマンドを使用します。

- 「TACACS+ サーバの統計を表示するには」（P.5-19）
- 「TACACS+ サーバの統計、キー、タイムアウトを表示するには」（P.5-19）

TACACS+ サーバの統計を表示するには

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

TACACS+ サーバの統計、キー、タイムアウトを表示するには

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

ほとんどの表示コマンドはビューア レベルでアクセスできますが、'**all**' オプションは、管理者レベルでのみ使用できます。管理者レベルにアクセスするには、'**enable 10**' コマンドを使用します。

TACACS+ ユーザのモニタリング

ローカル データベースでユーザ（パスワードを含む）を表示するには、ここで説明するコマンドを使用します。

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

ほとんどの表示コマンドはビューア レベルでアクセスできますが、このコマンドは、管理者レベルでのみ使用できます。管理者レベルにアクセスするには、**' enable 10 '** コマンドを使用します。

ACL の設定

SCE プラットフォームに Access Control List（ACL; アクセス制御リスト）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 のエントリを追加するには」（P.5-21）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には」（P.5-22）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 は、**ip access-class** コマンドでイネーブルにされます。ACL がイネーブルの場合、要求が着信すると、SCE プラットフォームでは、その IP アドレスからアクセスする許可があるかどうかを確認します。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。

イネーブルな ACL がない場合、アクセスは、すべての IP アドレスから許可されます。

（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ため、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**：ACL に割り当てられる ID 番号。
- **ip-address**：許可または拒否されるインターフェイスの IP アドレス。x.x.x.x の形式で入力します。
- **ip-address/mask**：このコマンドでは、x.x.x.x y.y.y.y 形式のアドレスの範囲を設定します。ここで、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**：指定された IP アドレスは、SCE プラットフォームへのアクセスを許可されます。
- **deny**：指定された IP アドレスは、SCE プラットフォームへのアクセスを拒否されます。

ACL のエントリを追加するには

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

グローバル コンフィギュレーション モードがイネーブルにされます。

ステップ 2　必要な IP アドレスを入力します。

- IP アドレス タイプを 1 つ設定するには

  access-list *number* **permit|deny** *ip-address* と入力し、**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* と入力し、**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 を削除するには

ACL とそのすべてのエントリを削除するには、ここで説明するコマンドを使用します。

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

指定した ACL とそのすべてのエントリが削除されます。

ACL をイネーブルにするには

ACL では、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)# プロンプトで、**ip access-class** *number* と入力し、**Enter** キーを押します。

SCE プラットフォームにアクセスしようとしているすべてのトラフィックに対して、指定された ACL が適用されます。

Telnet インターフェイスの管理

- 「Telnet アクセスを防ぐには」（P.5-22）
- 「Telnet タイムアウトを設定するには」（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 アクセスを防ぐには

Telnet によってアクセスをすべてディセーブルにするには、ここで説明するコマンドを使用します。

ステップ 1　SCE(config)# プロンプトで、**no service telnetd** と入力し、**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 タイムアウトを設定するには

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になる前の分数
  - デフォルト：30 分

ステップ 1　SCE(config-line)# プロンプトで、**timeout** *timeout* と入力し、**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。SSHv1 をディセーブルにすると、SSHv2 だけを実行することができます。

SSH サーバでは、次の暗号鍵がサポートされます。

- 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 によって提供）

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 サーバでは、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 キーを公開し、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」パスワードを認識でき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モニタリングできる盗聴者からの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からの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、ここで説明する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と、SSHv2 のみを実行できます。）
- 既存の SSH キーの削除

SSH キーのセットを生成するには

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)# プロンプトで、**ip ssh key generate** と入力し、**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には

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

SSH サーバをディセーブルにするには

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

SSHv2 のみを実行するには

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

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

SSHv1 を再度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 キーを削除するには

ステップ 1　SCE(config)# プロンプトで、**ip ssh key remove** と入力し、**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ため、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 コンフィギュレーションが示す場合、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、**reload** 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、コンフィギュレーションを保存する

SSH サーバ ステータスをモニタリングするには

現在の SSH セッションを含む SSH サーバのステータスをモニタリングするには、ここで説明するコマンドを使用します。

ステップ 1　SCE> プロンプトで、**show ip ssh** と入力し、**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 コマンドを開始していることを確認してください。

SNMP インターフェイスのイネーブル化

SNMP インターフェイスを明示的にイネーブルにする設定するには、ここで説明するコマンドを使用します。

snmp-server コマンドが実行されて、SNMP パラメータが設定されると、SNMP インターフェイスは黙示的にイネーブルに設定されます。SNMP パラメータ（ホスト、コミュニティ、コンタクト、ロケーション、トラップ宛先のホスト）の詳細については、「SNMP インターフェイスの設定と管理」（P.5-26）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には」（P.5-25）
- 「SNMP インターフェイスをディセーブルにするには」（P.5-25）

SNMP インターフェイスをイネーブルにするには

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)# プロンプトで、**snmp-server enable** と入力し、**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には

ステップ 1　SCE(config)# プロンプトで、**no snmp-server** と入力し、**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。SNMP 通知および関連する CLI コマンド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 準拠のデバイスは、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 で定義されている正規の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 は、要求タイプとその説明のリストです。

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。	

表 5-2　要求タイプ （続き）

要求タイプ	説明	備考
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 ID）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、管理ポート上でのみ 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

- 「SNMP を設定する CLI コマンド」（P.5-27）
- 「SNMP をモニタリングする CLI コマンド」（P.5-28）

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 を設定する CLI コマンド

SNMP の設定に使用できる CLI コマンドのリストは、次のとおりです。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 をモニタリングする CLI コマンド

SNMP のモニタリングに使用できる CLI コマンドのリストは、次のとおりです。これらはビューア モード コマンドで、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でも使用できます）
- 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る場合でも使用できます）
- show snmp traps

MIB について

MIB（管理情報ベース）は、NMS によるモニタリング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リングを 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される MIB についての詳細は、「Cisco Service Control 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。次のリブート用（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

- 「コミュニティ ストリングを定義するには」（P.5-29）
- 「コミュニティ ストリングを削除するには」（P.5-29）
- 「設定されているコミュニティ ストリングを表示するには」（P.5-30）

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 *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には

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特定するセキュリティ ストリング。

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ス機能）。
- **rw**：読み取りと書き込み。

ステップ 1　SCE(config)# プロンプトで、**snmp-server community** *community-string* **ro|rw** と入力し、**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持つ "mycommunity" コミュニティ ストリングを設定する例を示します。

読み取り専用がデフォルトのため、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には

ステップ 1　SCE(config)# プロンプトで、**no snmp-server community** *community-string* と入力し、**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" 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
```

設定されているコミュニティ ストリングを表示するには

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

設定されているコミュニティ ストリングの表示例

次に、設定された SNMP コミュニティ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 通知を設定するには

次の設定を行うには、ここで説明するコマンドを使用します。

- SNMP 通知を受信する宛先（ホスト）
- 送信される通知のタイプ（トラップ）
- 「SNMP ホストを定義するには」（P.5-31）

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）がトラップ メッセージを受信すると、イベントの発生を記録したり、信号を無視したりなどの、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 通知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の通知が送信される必要がある 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」を参照してください）。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 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：SCE の独自の MIB に定義されています（表 A-20（P.A-20）を参照）。

ホストが通知を受信するように設定されると、デフォルトにより、SCE プラットフォームは、このホストに SCE プラットフォームがサポートしているすべての通知（AuthenticationFailure 通知以外）を送信します。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。

以下は、次の内容を実行するサンプル手順です。

- SNMP エージェントから通知を送信する必要がある送信先のホスト（NMS）を設定する
- 通知の受信からホスト（NMS）を除外または削除する
- authentication-failure 通知を送信するよう SNMP エージェントをイネーブルにする
- エンタープライズ通知を送信するよう SNMP エージェントをイネーブルにする
- すべての通知をデフォルト設定にリセットする

SNMP ホストを定義するには

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、ここで説明するコマンドを使用します。

- 「オプション」（P.5-31）
- 「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には」（P.5-31）
- 「ホストへの通知の送信を停止するように SCE プラットフォームを設定するには」（P.5-31）
- 「SNMP トラップの設定方法」（P.5-32）

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特定するセキュリティ ストリング。
- **version**：システムで実行中の SNMP 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には

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

バージョンが指定されない場合、SNMPv1 であると見なされます。

1 コマンドにつき 1 つのホストのみを指定できます。複数ホストを定義するには、各ホストにつき 1 つのコマンドを実行します。

複数のホスト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例

次に、SNMPv1 通知をサーバ 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
```

ホストへの通知の送信を停止するように SCE プラットフォームを設定するには

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

ホストへの通知の送信を停止するように SCE プラットフォームを設定する例

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 トラップの設定方法

定義されているホストに送信する通知を設定するには、ここで説明する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。

- **snmp**：すべてまたは特定の SNMP トラップをイネーブルにする必要があるか、ディセーブルにする必要があるかを指定する、オプションのパラメータ。

  デフォルトでは、SNMP トラップはディセーブルにされています。

  snmp trap name：特定の SNMP トラップをイネーブルにする必要があるか、ディセーブルにする必要があるかを指定する、オプションのパラメータ。

  このパラメータで、現在受け付けられる唯一の値は、**Authentication** 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にする必要があるか、ディセーブルにする必要があるかを指定する、オプションのパラメータ。

  デフォルトでは、エンタープライズ トラップはディセーブルにされています。

- **enterprise trap name**：特定のエンタープライズ トラップをイネーブルにする必要があるか、ディセーブルにする必要があるかを指定する、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

これらのパラメータは、次のように使用します。

- 1 つのタイプの全トラップをイネーブルまたはディセーブルにするには、**snmp** または **enterprise** を指定します。
- 1 つの特定のトラップをイネーブルまたはディセーブルにするには、必要なトラップのトラップ名パラメータを追加して、**snmp** または **enterprise** を指定します。
- 全トラップをイネーブルまたはディセーブルにするには、**snmp** も **enterprise** も指定しません。

SNMP サーバによる認証失敗通知の送信をイネーブルにするには

ステップ 1　SCE(config)# プロンプトで、**snmp-server enable traps snmp authentication** と入力し、**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には

ステップ 1　SCE(config)# プロンプトで、**snmp-server enable traps enterprise** と入力し、**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には

ステップ 1　SCE(config)# プロンプトで、**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]* と入力し、**Enter** キーを押します。

必要なエンタープライズ トラップ タイプが指定されます。

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例

次に、logger エンタープライズ通知のみを送信するように 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には

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

SCE プラットフォームによってサポートされるすべての通知が、デフォルトのステータスにリセットされます。