CHAPTER 5

管理インターフェイスとセキュリティの設定

この章では、物理的な管理インターフェイス（ポート）のほか、SNMP、SSH、および TACACS+ などの各種の管理インターフェイス アプリケーションを設定する方法について説明します。ユーザ、パスワード、IP の設定、クロックおよびタイム ゾーン、およびドメイン名の値の設定方法についても説明します。

管理インターフェイスおよびセキュリティについて

Service Control Module には、RJ-45 管理（MNG）ポートが搭載されています。ギガビット イーサネット ポートを使用すると、LAN 経由でリモート管理コンソールから 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、次の作業を実行します。

- 管理ポートを設定する
  - 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する
  - 許可された IP アドレスおよび禁止された 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、次の作業を実行します。

- IP アドレスとサブネット マスクを設定する
- 次の物理パラメータを設定する
  - 速度
  - デュプレックス

ステップ 1　管理ポートをケーブル接続し、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.5-3] を参照）。

管理インターフェイス コンフィギュレーション モードの開始方法

interface Mng GBE 管理インターフェイスは次のように設定されます。

- 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** と入力して、**Enter** キーを押します。

グローバル コンフィギュレーション モードを開始します。

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** と入力して、**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 モードを開始します。

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、管理動作および RDR の送信に使用します。これらはトラフィック分析の出力と管理動作です。

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

ユーザは、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 接続が中断し、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部コンポーネントと外部コンポーネントに変更内容が正常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およびシャットダウン」[p.3-15] 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手順の例を示しながら説明します。

これらのパラメータは両方とも、各ポートに個別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

次の表に、速度とデュプレックスのインターフェイス ステートの関係をまとめています。

次の事項に注意してください。

- 1 つのパラメータを「auto」に設定して、他のパラメータを指定することはできません。速度またはデュプレックスのいずれかを「auto」に設定すると、両方のパラメータは「auto」に設定されているように機能します。
- インターフェイスの性質により、自動ネゴシエーションがイネーブルになっている場合のみ、1000 Mbps での動作が可能です。

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 FE 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の設定方法

オプション

次のオプションを使用できます。

- **speed** — 現在選択した管理ポート（0/1 または 0/2）の速度（Mbps）
  - **10**
  - **100**
  - **auto**（デフォルト）— 自動ネゴシエーション（リンク速度は指定しません）

duplex パラメータが **auto** に設定されている場合、speed パラメータの変更は効果がありません。

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。

必要な速度の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の設定方法

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）— 自動ネゴシエーション（リンクのデュプレックスは指定しません）

speed パラメータが **auto** に設定されている場合、duplex パラメータの変更は効果がありません。

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の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のモニタリング方法

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。

- 自動ネゴシエーション
- 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]*** を入力し、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 のインターフェイスを設定できます。

TACACS+ AAA

TACACS+ AAA について

TACACS+ AAA

Terminal Access Controller Access Control System Plus（TACACS+）はセキュリティ アプリケーションで、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認証を中央集中的に管理します。TACACS+ プロトコルを実装することで、カスタマーは 1 つまたは複数の SCE プラットフォームの認証サーバを設定できます。これにより、認証サーバが各ユーザを認証する際に、SCE プラットフォームの管理にセキュリティが提供されます。TACACS+ は認証データベースを中央集中型にしているため、SCE プラットフォームの管理が容易になります。

TACACS+ サービスは、稼働している TACACS+ サーバのデータベース内（通常、UNIX または Windows NT ワークステーション）で管理されています。設定した TACACS+ 機能をネットワーク要素で使用する前に、TACACS+ サーバにアクセスし、これを設定する必要があります。

TACACS+ プロトコルは、ネットワーク要素と TACACS+ ACS との間で認証機能を提供します。また、キーが設定されている場合、ネットワーク要素と TACACS+ サーバの間ですべてのプロトコル交換を暗号化することで機密性も保障されます。

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 アクセスに対して TACACS+ ASCII 認証メッセージを使用します。

TACACS+ を使用すると、サーバがユーザを認証するために十分な情報を受け取るまで、サーバとユーザ間で任意の対話を確立できます。これは、通常、ユーザ名とパスワードの組み合わせをプロンプトに入力することで実行されます。

ログインとパスワードのプロンプトは TACACS+ サーバによって与えられますが、TACACS+ サーバがプロンプトを提供しない場合、ローカルのプロンプトが使用されます。

ユーザのログイン情報（ユーザ名とパスワード）は、認証のため TACACS+ サーバに転送されます。TACACS+ サーバからユーザ認証失敗の通知があった場合、ユーザに再度ユーザ名とパスワードのプロンプトが表示されます。ユーザには、ユーザが設定した回数分プロンプトが繰り返し表示されます。ログインへの失敗は SCE プラットフォームのユーザ ログに記録されており、回数分プロンプトが表示されたあとは、（ユーザがコンソール ポートに接続していないかぎり）Telnet セッションが切断されます。

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 — ユーザが認証され、サービスが開始されます。
- REJECT — ユーザ認証に失敗しました。TACACS+ サーバの設定に応じて、ユーザはそれ以上のアクセスが禁止される場合と、ログイン シーケンスを再度実行するためのプロンプトが表示される場合があります。
- ERROR — 認証中の特定の段階でエラーが発生しました。このエラーはサーバ側で発生しているか、またはサーバと SCE プラットフォーム間のネットワーク接続で発生しています。ERROR 応答を受信した場合、SCE プラットフォームは、ユーザ認証に代替方法または代替サーバを使用します。
- CONTINUE — ユーザは追加の認証情報を求められます。

サーバが使用できない場合、「一般的な AAA フォールバックと復旧メカニズム」（p.5-8）で説明されているような次の認証方式が実行されます。

アカウンティング

TACACS+ アカウンティングは、次の機能をサポートします。

- それぞれ実行されたコマンド（有効なコマンドである必要があります）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 および exit コマンドを含む）。
- コマンドは正常に実行された場合、その前後が記録されます。
- 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
  - 現在の時間
  - 実行されたアクション
  - コマンドの権限レベル

TACACS+ アカウンティングは、通常のローカル アカウンティングに加え、SCE プラットフォームの dbg ログを使用します。

権限レベル許可

正常にログインしたあと、ユーザはデフォルトの権限レベル 0 を与えられます。このレベルでは、実行できるコマンドの数が制限されます。権限レベルを変更するには、「enable」コマンドを実行します。このコマンドは権限レベル許可のメカニズムを開始します。

SCE プラットフォームの権限レベル許可は、「enable」コマンド認証要求を使用して実行されます。ユーザが「enable」コマンドを使用して指定の権限レベルの許可を要求した場合、SCE プラットフォームは、その要求の権限レベルを指定する TACACS+ サーバに認証要求を送信します。SCE プラットフォームは、TACACS+ サーバが次の内容を実行したあとにのみ、要求の権限レベルを与えます。

- 「**enable**」コマンド パスワードを認証
- ユーザが要求した権限レベルを開始するのに十分な権限を持っていることを証明

ユーザの権限レベルが決まると、ユーザはそれに応じた特定のコマンド群の使用を許可されます。

ログイン認証を使用していてサーバが使用できない場合、「一般的な AAA フォールバックと復旧メカニズム」（p.5-8）で説明されているような次の認証方式が実行されます。

一般的な AAA フォールバックと復旧メカニズム

SCE プラットフォームは、エラーが発生してもサービスのアベイラビリティを維持するために、フォールバック メカニズムを使用します。

SCE プラットフォームは、エラーが発生してもサービスのアベイラビリティを維持するために、フォールバック メカニズムを使用します。

使用できる Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）方式は、次のとおりです。

- **TACACS+** — AAA は TACACS+ サーバによって、認証、認可、およびアカウンティングが実行されます。
- **Local** — AAA はローカル データベースによって、認証および認可が実行されます。
- **Enable** — AAA はユーザ設定のパスワードによって、認証および認可が実行されます。
- **None** — 認証、認可、およびアカウンティングは実行されません。

現在の実装ではこれらの方式を使用する順番を設定することはできませんが、カスタマーはその使用順を選択できます。現在の順番は、次のとおりです。

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

（注）　重要 : サーバが AAA 障害に遭遇した場合、その AAA 方式のいずれかが回復するまで、SCE プラットフォームにアクセスできなくなります。これを回避するために、最後の AAA 方式として「none」を使用することを推奨します。SCE プラットフォームにアクセスできない場合、シェル機能「AAA_MethodsReset」を使用することで、現在の AAA 方式の設定を削除し、使用する AAA 方式に「Enable」を設定できます。

TACACS+ の設定について

次に、TACACS+ を設定する手順の概要を示します。詳細なすべてのステップについては、このセクションの他の部分で説明されています。

1. リモート TACACS+ サーバを設定します。

   プロトコルに対してリモート サーバを設定します。次の注意事項を確認してください。

   - 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。
   - 最大ユーザ権限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際に使用されるパスワード）を指定します。
   - 設定には権限レベル 15 を持つルート ユーザが常に含まれている必要があります。
   - 表示ユーザ（権限レベル 5）とスーパーユーザ（権限レベル 10）のユーザ ID も同時に設定する必要があります。

2. 詳細なサーバ設定については、使用する TACACS+ サーバで該当する設定マニュアルを参照してください。

3. TACACS+ サーバと連動する 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
   - 共有暗号キー（クライアントとサーバ間の通信のために、設定した暗号キーはサーバに設定した暗号キーと対になる必要があります）

4. （任意）必要に応じてローカル 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+ の両方を設定する場合、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推奨します。こうすることで、TACACS+ サーバに障害が発生しても、ユーザは SCE プラットフォームにアクセスできます。

（注）　TACACS+ がログイン方法として使用されている場合、TACACS+ ユーザ名が自動的に enable コマンドで使用されます。そのため、enable コマンドがこのユーザ名を認識できるように、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。

   - パスワードの指定
   - 権限レベルの定義

5. SCE プラットフォームの認証方式を設定します。

   - ログイン認証方式
   - 権限レベル許可方式

6. 設定を確認します。

   show running-config コマンドを実行し、設定を表示します。

SCE プラットフォームの TACACS+ クライアントの設定方法

SCE プラットフォームの TACACS+ クライアントの設定

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。その次に SCE プラットフォームの TACACS+ クライアントを設定し、TACACS+ サーバと連動させてください。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 3 つのサーバがサポートされます。

  各サーバ ホストに、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（任意） — グローバルなデフォルトの暗号キーを定義できます。このキーは、サーバ ホストが定義されておらず、キーが明示的に設定されていない場合に使用される、すべてのサーバ ホスト キーとして定義されます。

  デフォルトの暗号キーが設定されていない場合、キーが明示的に設定されていないすべてのサーバにデフォルトとして何もないキーが割り当てられます。
- デフォルトのタイムアウト間隔（任意）— 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。このタイムアウト間隔は、サーバ ホストが定義されておらず、タイムアウト間隔が明示的に設定されていない場合に使用される、すべてのサーバ ホストのタイムアウト間隔として定義されます。

  デフォルトのタイムアウト間隔が設定されていない場合、タイムアウト間隔が明示的に設定されていないすべてのサーバにデフォルト設定として 5 秒が割り当てられます。

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されています。

- TACACS+ サーバ ホストの新規追加方法（p.5-10）
- TACACS+ サーバ ホストの削除方法（p.5-11）
- グローバルなデフォルト キーの設定方法（p.5-11）
- グローバルなデフォルト タイムアウトの設定方法（p.5-12）

TACACS+ サーバ ホストの新規追加方法

SCE プラットフォームの TACACS+ クライアントで使用できる新しい 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。

Service Control ソリューションは、最大 3 つの TACACS+ 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** — サーバ名
- **port number** — TACACS+ ポート番号
  - デフォルト = 49
- **timeout interval** — タイムアウトするまで、サーバがサーバ ホストからの応答を待機する時間を秒で示します。
  - デフォルトは、5 秒です。またはユーザが設定したグローバルなデフォルト タイムアウト間隔が設定されています（「グローバルなデフォルト タイムアウトの定義方法」[p.5-12] を参照）。
- **key-string** — サーバとクライアントの通信時に互いが使用する暗号キーを設定します。指定のキーが実際に TACACS+ サーバ ホストに設定されているかどうかを確認してください。

— デフォルトではキーが指定されていません。またはユーザが設定したグローバルなデフォルト キーが設定されています（「グローバルなデフォルト キーの定義方法」[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 ホストの削除方法

オプション

次のオプションを使用できます。

- **host-name** — 削除するサーバ名

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。

グローバルなデフォルト キーの設定方法

グローバルなデフォルト キーを TACACS+ サーバ ホストに定義するには、このコマンドを使用します。特定の TACACS+ サーバ ホストに異なるキーが明示的に設定されていれば、その TACACS+ サーバ ホストでは、このデフォルト キーは使用されません（上書きされます）。

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の通信時に互いが使用するデフォルトの暗号キーを設定します。指定のキーが実際に TACACS+ サーバ ホストに設定されているかどうかを確認してください。
  — デフォルトでは暗号化は設定されていません。

グローバルなデフォルト キーの定義方法

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

グローバルなデフォルト キーのクリア方法

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。

グローバルなデフォルト キーは定義されていない状態です。各 TACACS+ サーバ ホストには特定のキーが定義されている場合もありますが、明示的にキーが定義されていないサーバはすべて（グローバルなデフォルト キーを使用した場合）、キーの設定がなくなります。

グローバルなデフォルト タイムアウトの設定方法

グローバルなデフォルト タイムアウトを TACACS+ サーバ ホストに定義するには、このコマンドを使用します。特定の TACACS+ サーバ ホストに異なるタイムアウト間隔が明示的に設定されていれば、その TACACS+ サーバ ホストでは、このデフォルト タイムアウト間隔は使用されません（上書きされます）。

オプション

次のオプションを使用できます。

- **timeout interval** — タイムアウトするまで、サーバがサーバ ホストからの応答を待機するデフォルトの時間を秒で示します。
  - デフォルト — 5 秒

グローバルなデフォルト タイムアウトの定義方法

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。

グローバルなデフォルト タイムアウトのクリア方法

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。

グローバルなデフォルト タイムアウト間隔は定義されていない状態です。各 TACACS+ サーバ ホストには特定のタイムアウト間隔が定義されている場合もありますが、明示的にタイムアウト間隔が定義されていないサーバはすべて（グローバルなデフォルト タイムアウト間隔を使用した場合）、5 秒のタイムアウト間隔になります。

ユーザ データベースの管理方法

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 のユーザを設定できます。各ユーザには次のような情報が設定されています。

- ユーザ名
- パスワード — 設定に暗号化が使用されている場合と使用されていない場合があります
- 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されています。

- ローカル データベースに新しくユーザを追加する方法（p.5-12）
- ユーザの権限レベルの定義方法（p.5-14）
- 権限レベルおよびパスワードでの新規ユーザの追加方法（p.5-14）
- ユーザの削除方法（p.5-16）

ローカル データベースに新しくユーザを追加する方法

ローカル データベースに新しくユーザを追加するには、これらの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 パスワードでのユーザの追加方法（p.5-13）
- パスワードなしでのユーザの追加方法（p.5-13）
- クリア テキストで入力された MD5 暗号化パスワードでのユーザの追加方法（p.5-14）
- MD5 暗号化文字列で入力された MD5 暗号化パスワードでのユーザの追加方法（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。パスワードには複数の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 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。
- 暗号化パスワード — パスワードはローカル リストに暗号化（MD5）されて保存されます。secret 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。
  - 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
  - ユーザの MD5 暗号化 secret パスワードとして保存される MD5 暗号化文字列を指定

次のオプションを使用できます。

- **name** — 追加するユーザ名
- **password** — クリア テキスト パスワード。次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
  - MD5 暗号化形式（secret キーワードが使用されている場合）
- **encrypted-secret** — MD5 暗号化文字列パスワード

次のキーワードが使用できます。

- **nopassword** — このユーザに関連し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。コマンド入力時に次のいずれかのキーワードを使用して、パスワード形式を指定します。
  - **0** — **password** オプションと一緒に使用して、MD5 暗号化形式で保存されるクリア テキスト パスワードを指定します。
  - **5** — **encrypted-secret** オプションと一緒に使用して、ユーザの MD5 暗号化 secret パスワードとして保存される MD5 暗号化文字列を指定します。

クリア テキスト パスワードでのユーザの追加方法

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。

パスワードなしでのユーザの追加方法

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 暗号化パスワードでのユーザの追加方法

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 暗号化パスワードでのユーザの追加方法

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。

ユーザの権限レベルの定義方法

- ユーザの権限レベルについて（p.5-14）
- オプション（p.5-14）

ユーザの権限レベルについて

SCE プラットフォームの権限レベル許可は、「**enable**」コマンド認証要求を使用して実行されます。ユーザが「**enable**」コマンドを使用して指定の権限レベルの許可を要求した場合、SCE プラットフォームは、その要求の権限レベルを指定する TACACS+ サーバに認証要求を送信します。TACACS+ サーバが「**enable**」コマンド パスワードを認証し、ユーザが要求した権限レベルを開始するために十分な権限を持っていることが証明された場合にのみ、SCE プラットフォームは要求された権限レベルを許可します。

オプション

次のオプションを使用できます。

- **name** — 権限レベルを設定するユーザ名
- **level** — 特定のユーザに許可する権限レベル。これらのレベルは、**enable** コマンドで入力される CLI 許可レベルに対応しています。
  - 0 — User
  - 10 — Admin
  - 15（デフォルト設定）— 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。

権限レベルおよびパスワードでの新規ユーザの追加方法

パスワードや権限レベルをはじめ、単一のコマンドで新しいユーザを定義するには、これらの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

次のオプションを使用できます。

- **name** — 権限レベルを設定するユーザ名
- **level** — 特定のユーザに許可する権限レベル。これらのレベルは、**enable** コマンドで入力される CLI 許可レベルに対応しています。
  - 0 — User
  - 10 — Admin
  - 15（デフォルト設定）— Root
- **password** — クリア テキスト パスワード。次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
  - MD5 暗号化形式（secret キーワードが使用されている場合）
- **encrypted-secret** — MD5 暗号化文字列パスワード

次のキーワードが使用できます。

- **secret** — パスワードは MD5 暗号化形式で保存されます。コマンド入力時に次のいずれかのキーワードを使用して、パスワード形式を指定します。
  - **0** — **password** オプションと一緒に使用して、MD5 暗号化形式で保存されるクリア テキスト パスワードを指定します。
  - **5** — **encrypted-secret** オプションと一緒に使用して、ユーザの MD5 暗号化 secret パスワードとして保存される MD5 暗号化文字列を指定します。

権限レベルとクリア テキスト パスワードでのユーザの追加方法

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 暗号化パスワードでのユーザの追加方法

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 暗号化パスワードでのユーザの追加方法

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。

ユーザの削除方法

オプション

次のオプションを使用できます。

- **name** — 削除するユーザ名

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

ログイン認証の設定には、2 つの機能があります。

- 許可する Telnet ログインの最大数
- ログイン時に使用する認証方式（「一般的な AAA フォールバックと復旧メカニズム」[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されています。

- 最大ログイン数の設定（p.5-16）
- ログイン認証方式の設定方法（p.5-16）

最大ログイン数の設定

セッションを切断するまでに許可する最大ログイン数を設定するには、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 セッションを切断するまでに許可する最大ログイン数

  これは Telnet セッションにのみ関係します。ローカル コンソールからであれば、再試行数に制限はありません。

  ー　デフォルトは 3 に設定されています。

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。

ログイン認証方式の設定方法

プライマリ ログイン認証方式が失敗したときに使用される「バックアップ」ログイン認証方式を設定できます（「一般的な AAA フォールバックと復旧メカニズム」[p.5-8] を参照）。

使用するログイン認証方式とその順番を指定するには、このコマンドを使用します。

- オプション（p.5-17）
- ログイン認証方式の指定方法（p.5-17）
- ログイン認証方式リストの削除方法（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式。最大 4 つの異なる方式を使用する順番で指定できます。
  - **group TACACS+** — TACACS+ 認証を使用します。
  - **local** — 認証にローカル ユーザ名の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。

ログイン認証方式の指定方法

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。

上記で説明した最大 4 つの方式を入力できます。プライオリティに従って順番に入力してください。

ログイン認証方式リストの削除方法

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。

ログイン認証方式を削除した場合、デフォルトのログイン認証方式（enable パスワード）のみが使用されます。TACACS+ 認証は使用されません。

AAA 権限レベル許可方式の設定

オプション

次のオプションを使用できます。

- **method** — 使用するログイン許可方式。最大 4 つの異なる方式を使用する順番で指定できます。
  - **group TACACS+** — TACACS+ 許可を使用します。
  - **local** — 許可にローカル ユーザ名の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 権限レベル許可方式の指定方法

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。

上記で説明した最大 4 つの方式を入力できます。プライオリティに従って順番に入力してください。

AAA 権限レベル許可方式リストの削除方法

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。

権限レベル許可方式リストを削除した場合、デフォルトのログイン認証方式（enable パスワード）のみが使用されます。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。

- AAA アカウンティングについて（p.5-18）
- オプション（p.5-18）
- AAA アカウンティングのイネーブル化の方法（p.5-18）
- AAA アカウンティングのディセーブル化の方法（p.5-18）

AAA アカウンティングについて

TACACS+ アカウンティングがイネーブルの場合、SCE プラットフォームは、各コマンドの実行後にアカウンティング メッセージを TACACS+ サーバに送信します。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できるように 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設定されています。

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 アカウンティングのイネーブル化の方法

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、CLI コマンド実行時の最初と最後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（コマンドが正常に実行された場合）。

AAA アカウンティングのディセーブル化の方法

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+ サーバの統計情報を表示するには、これらのコマンドを使用します。

- TACACS+ サーバの統計情報の表示方法（p.5-19）
- TACACS+ サーバの統計情報、キー、およびタイムアウトの表示方法（p.5-19）

TACACS+ サーバの統計情報の表示方法

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+ サーバの統計情報、キー、およびタイムアウトの表示方法

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。

多くの show コマンドは Viewer レベルのユーザでも使用できますが、「**all**」オプションに関しては Admin レベルでしか使用できないことに注意してください。Admin 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

パスワードなど、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# プロンプトで、**show users** と入力し、**Enter** キーを押します。

多くの show コマンドは Viewer レベルのユーザでも使用できますが、このコマンドに関しては Admin レベルでしか使用できないことに注意してください。Admin 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

- ACL について（p.5-19）
- オプション（p.5-20）
- ACL へのエントリの追加方法（p.5-20）
- ACL の削除方法（p.5-21）
- ACL をイネーブルにする方法（p.5-21）

ACL について

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 へのエントリの追加方法 [p.5-20] ）
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 は **ip access-class** コマンドによってイネーブルです。ACL がイネーブルである場合に要求が来ると、まず SCE プラットフォームが、その IP アドレスからのアクセスに対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。

ACL がイネーブルでない場合、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** — ACL に割り当てられた 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。

次のキーワードが使用できます。

- **permit** — SCE プラットフォームへのアクセスを許可する指定の IP アドレス
- **deny** — SCE プラットフォームへのアクセスを拒否する指定の IP アドレス

ACL へのエントリの追加方法

ステップ 1　**configure** と入力して、**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　必要な IP アドレスを入力します（複数可）。

- IP アドレスを 1 つ設定するには、次のコマンドを使用します。
  access-list *number* ***permit|deny*** *ip-address*（最後に **Enter** キーを押します）。
- 複数の IP アドレスを設定するには、次のコマンドを使用します。
  access-list *number* ***permit|deny*** *ip-address/mask*（最後に **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 の削除方法

すべてのエントリと一緒に 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)# プロンプトで、**no access-list** *number* と入力し、**Enter** キーを押します。

すべてのエントリと一緒に指定した ACL を削除します。

ACL をイネーブルにする方法

ACL は SCE プラットフォームへのすべてのトラフィックを許可または拒否します。

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。

指定された ACL を、SCE プラットフォームにアクセスしようとするすべてのトラフィックに適用します。

Telnet インターフェイスの管理

Telnet インターフェイスについて

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は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 アクセスの回避方法

Telnet からのアクセスを完全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 タイムアウトの設定方法

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** — 非アクティブの Telnet セッションがタイムアウトするまでの分単位の時間
  - デフォルト — 30 分

ステップ 1　SCE(config)# 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、SSH-1 と SSH-2 の両方のプロトコルをサポートしています。

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モニタリング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 ステータスのモニタリング方法（p.5-24）

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。これらのコマンドを使用して、次の操作を実行できます。

- SSH キー セットの生成
- SSH サーバのイネーブル化およびディセーブル化
- SSHv1 のイネーブル / 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 セットの生成方法

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、ただち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 サーバのイネーブル化の方法

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 サーバのディセーブル化の方法

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 のみを実行する方法

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 キーの削除方法

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 セットを不揮発性メモリから削除します。

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 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 ステータスのモニタリング方法

現在の SSH セッションを含む SSH サーバのステータスをモニタリングするには、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。他のモードを終了することにより、ユーザ EXEC コマンドに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 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なります。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、およびトラップ宛先のホストを含む）の設定と管理の詳細については、「SNMP インターフェイスの設定および管理」（p.5-26）を参照してください。

- SNMP インターフェイスのイネーブル化の方法（p.5-25）
- SNMP インターフェイスのディセーブル化の方法（p.5-25）

SNMP インターフェイスのイネーブル化の方法

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 インターフェイスのディセーブル化の方法

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および管理

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 通知とそのサポート対象の MIB 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 準拠のデバイスは、MIB 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　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 つまたは複数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 つまたは複数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

CLI

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 を設定するための CLI コマンド

SNMP を設定する場合に使用できる CLI コマンドのリストは、次のとおりです。グローバル コンフィギュレーション モードのコマンドになります。

- **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ための CLI コマンド

SNMP をモニタリングする場合に使用できる CLI コマンドのリストは、次のとおりです。ビューアモードのコマンドになります。SNMP エージェントがイネーブルのときに使用できます。

- **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る場合に使用できます）
- **show snmp traps**

MIB について

MIB

MIB 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する MIB の詳細については、「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を利用して、1 つのコンフィギュレーション データベースを処理す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、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 ストリングの定義方法（p.5-29）
- コミュニティ ストリングの削除方法（p.5-29）
- 設定したコミュニティ ストリングの表示方法（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 の *Get*、*Get-next*、*Get-bulk*、および *Set* の要求が有効です。

コミュニティ ストリングの定義方法

オプション

次のオプションを使用できます。

- **community-string** — SNMP サーバへのアクセスが許可された管理者のコミュニティを特定するセキュリティ ストリング

次のキーワードが使用できます。

- **ro** — 読み取り専用（デフォルトのアクセス）
- **rw** — 読み書き

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。

読み取り専用はデフォルトなので、この場合、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 ストリングの削除方法

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
```

設定したコミュニティ ストリングの表示方法

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。

設定したコミュニティ ストリングの表示：例

次に、設定した 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 通知の設定方法

SNMP 通知を設定するには、次の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 通知について（p.5-30）
- SNMP ホストの定義方法（p.5-31）

SNMP 通知について

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 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）。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、MIB 単位の設定に従って、2 つの一般的なカテゴリの通知をサポートしています（ここでサポート リスト TBD へのリンクを追加）。

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 Service Control Enterprise 通知 — サービス コントロール独自の MIB に定義されています（表 A-22 [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。

次には、次の内容を実行するサンプル手順を示します。

- SNMP エージェントが通知を送信するホスト（NMS）を設定
- 受信通知からホスト（NMS）を削除またはディセーブル化
- AuthenticationFailure 通知を送信する SNMP エージェントのイネーブル化
- エンタープライズ通知を送信する SNMP エージェントのイネーブル化
- すべての通知をデフォルト設定にリセット

SNMP ホストの定義方法

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.5-31）
- 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方法（p.5-31）
- ホストに通知を送信しないように 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 サーバへのアクセスが許可された管理者のコミュニティを特定するセキュリティ ストリング
- **version** — システムで実行されている SNMP バージョン。1 または 2c にすることができます。
  - 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。

バージョンを指定しないと、SNMPv1 とみなされます。

1 つのコマンドに対して指定できるのは、1 つのホストだけです。複数のホストを定義するには、各ホストに対して 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ための 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 SNMP 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
```

ホストに通知を送信しないように SCE プラットフォームを設定する方法

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

ホストに通知を送信しないための 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 トラップの設定方法

定義した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.5-32）
- SNMP サーバをイネーブルにして、認証失敗通知を送信する方法（p.5-32）
- SNMP サーバをイネーブルにして、すべてのエンタープライズ通知を送信する方法（p.5-33）
- SNMP サーバをイネーブルにして、特定のエンタープライズ通知を送信する方法（p.5-33）
- デフォルトの状態へのすべての通知の復旧方法（p.5-33）

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指定するオプション パラメータ

  デフォルトでは、snmp トラップがディセーブルです。

  snmp trap name — 特定の snmp トラップをイネーブルまたはディセーブルに指定するオプション パラメータ

  このパラメータで現在許可されている値は、**authentication** だけです。
- **enterprise** — すべてまたは特定の enterprise トラップをイネーブルまたはディセーブルに指定するオプション パラメータ

  デフォルトでは、enterprise トラップがイネーブルです。
- **enterprise trap name** — 特定の snmp トラップをイネーブルまたはディセーブルに指定するオプション 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を次のように使用します。

- 1 つのタイプのすべてのトラップをイネーブル / ディセーブルにする場合：**snmp** または **enterprise** だけを指定します。
- 1 つの特定のトラップをイネーブル / ディセーブルにする場合：必要なトラップを指定する追加のトラップ名のパラメータとともに **snmp** または **enterprise** を指定します。
- すべてのトラップをイネーブル / ディセーブルにする場合：**snmp** および **enterprise** のいずれも指定しません。

SNMP サーバをイネーブルにして、認証失敗通知を送信する方法

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 サーバをイネーブルにして、すべてのエンタープライズ通知を送信する方法

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 サーバをイネーブルにして、特定のエンタープライズ通知を送信する方法

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 enterprise トラップ タイプを指定します。

特定のエンタープライズ通知を送信するための SNMP サーバのイネーブル化：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
```

デフォルトの状態へのすべての通知の復旧方法

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 プラットフォームがサポートしているすべての通知を、デフォルトの状態にリセットします。

IP の設定

IP ルーティング テーブルの設定

IP ルーティング テーブルについて

SCE プラットフォームは、帯域外 MNG ポートの IP パケットを処理するために、スタティック ルーティング テーブルを保持しています。パケットが送信されると、システムは、ルーティング テーブルで正しいルーティングを調べ、それに従ってパケットを転送します。パケットのルートを判別できない場合、SCE プラットフォームはデフォルト ゲートウェイにパケットを送信します。

SCE プラットフォームは、デフォルトのネクスト ホップ ルータとしてデフォルト ゲートウェイの設定をサポートしています。また、異なるサブネットに対して異なるネクスト ホップ ルータを提供するために、ルーティング テーブルの設定をサポートしています（最大設定数は、10 サブネット）。

次のセクションでは、CLI コマンドを使用して、各種のパラメータを設定する方法を示します。

IP ルーティング テーブルに関連するコマンドは、次のとおりです。

- **ip default-gateway**
- **ip route prefix mask next-hop**
- **no ip route all**
- **no ip route prefix mask**
- **show ip route**
- **show ip route prefix**
- **show ip route prefix mask**

デフォルト ゲートウェイの設定方法

オプション

次のオプションを使用できます。

- ip-address — デフォルト ゲートウェイの IP アドレス

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

特権 EXEC モードをイネーブルにします。

- プロンプトが表示されたら、パスワードを入力します。

デフォルトのゲートウェイの設定：例

次に、SCE プラットフォームのデフォルト ゲートウェイの IP を 10.1.1.1 に設定する例を示します。

```
SCE(config)#ip default-gateway 10.1.1.1
```

IP ルーティング テーブルへのエントリの追加方法

オプション

次のオプションを使用できます。

- **prefix** — ルーティング エントリの IP アドレス（ドット表記）
- **mask** — 関連するサブネット マスク（ドット表記）
- **next-hop** — ルート内のネクスト ホップの IP アドレス（ドット表記）
  MNG インターフェイス サブネット内である必要があります。

ステップ 1　SCE(config)# プロンプトで、`ip route` *prefix mask next-hop* と入力し、**Enter** キーを押します。

指定した IP ルーティング エントリをルーティング テーブルに追加します。

IP ルーティング テーブルへのエントリの追加方法：例

次に、ルータ 10.1.1.250 をサブネット 10.2.0.0 へのネクスト ホップとして設定する例を示します。

```
SCE(config)#ip route 10.2.0.0 255.255.0.0 10.1.1.250
```

IP ルーティング テーブルの表示方法

- IP ルーティング テーブル全体の表示方法（p.5-35）
- 指定したサブネットの IP ルーティング テーブルの表示方法（p.5-36）

IP ルーティング テーブル全体の表示方法

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

ルーティング テーブルの全体とデフォルト ゲートウェイの宛先を表示します。

IP ルーティング テーブル全体の表示：例

次に、ルーティング テーブルを表示する例を示します。

```
SCE#show ip route
gateway of last resort is        10.1.1.1
|    prefix       |     mask          |    next hop     |
|-----------------|-------------------|-----------------|
|        10.2.0.0 |     255.255.0.0   |      10.1.1.250 |
|        10.3.0.0 |     255.255.0.0   |      10.1.1.253 |
|        198.0.0.0 |       255.0.0.0 |      10.1.1.251 |
|        10.1.60.0 |   255.255.255.0 |      10.1.1.5   |
```

指定したサブネットの IP ルーティング テーブルの表示方法

オプション

次のオプションを使用できます。

- **prefix** — ルーティング エントリの IP アドレス（ドット表記）
- **mask** — 関連するサブネット マスク（ドット表記）

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

指定したサブネット（プレフィクス / マスク）のルーティング テーブルを表示します。

指定したサブネットの IP ルーティング テーブルの表示：例

次に、指定したサブネットのルーティング テーブルを表示する例を示します。

```
SCE#show ip route 10.1.60.0 255.255.255.0
|    prefix        |     mask         |    next hop     |
|------------------|------------------|-----------------|
|       10.1.60.0 |   255.255.255.0 |        10.1.1.5 |
sce#
```

IP アドバタイジング

- IP アドバタイジングの設定（p.5-37）
- 現在の IP アドバタイジング設定の表示方法（p.5-37）

IP アドバタイジングは、設定された間隔で、設定されたアドレスに ping 要求を定期的に送信する動作です。これは、長期間にわたる非アクティブの状態においても、スイッチなどのアダプティブ ネットワーク要素のメモリ内で SCE プラットフォームの IP/MAC アドレスを維持します。

IP アドバタイジングに関連するコマンドは、次のとおりです。

- **[no] ip advertising**
- **ip advertising destination**
- **ip advertising interval**
- **default ip advertising destination**
- **default ip advertising interval**
- **show ip advertising**
- **show ip advertising destination**
- **show ip advertising interval**

IP アドバタイジングの設定

IP アドバタイジングを設定するには、まず IP アドバタイジングをイネーブルにする必要があります。次に、ping 要求が送信される宛先アドレスや ping 要求の頻度（間隔）を指定できます。宛先または間隔を明示的に設定しない場合は、デフォルト値であるとみなされます。

オプション

IP アドバタイジング コマンドで、次のオプションを使用できます。

- **interval** — ping 間の間隔（秒単位）
  デフォルトの間隔 = 300 秒
- **destination** — ping 要求の宛先の IP アドレス
  デフォルトの宛先 = 127.0.0.1

IP アドバタイジングのイネーブル化の方法

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

IP アドバタイジングをイネーブルにします。

IP アドバタイジングの宛先の設定方法

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

IP アドバタイジング ping の宛先を設定します。

IP アドバタイジング間隔の設定方法

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

IP アドバタイジング ping の頻度を設定します。

IP アドバタイジングの設定：例

次に、10.1.1.1 の宛先と 240 秒の間隔を指定して、IP アドバタイジングを設定する例を示します。

```
SCE(config)#ip advertising destination 10.1.1.1
SCE(config)#ip advertising interval 240
```

現在の IP アドバタイジング設定の表示方法

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

IP アドバタイジングのステータス（イネーブルまたはディセーブル）、設定された宛先、および設定された間隔を表示します。

管理インターフェイスの IP アドレスの設定方法

ユーザは、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。

（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部コンポーネントと外部コンポーネントに変更内容が正常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およびシャットダウン」[p.3-15] を参照）。

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。両方の管理ポートが接続されてバックアップ管理リンクが使用できる場合、この IP アドレスは、現在アクティブになっている物理ポートに関わらず、現在のアクティブ管理ポートに対して仮想 IP アドレスとして機能します。
- **subnet mask** — 管理インターフェイスのサブネット マスク

ステップ 1　ローカル コンソールに SCE プラットフォームを直接接続します。

設定した IP アドレスに左右されない SCE プラットフォームとの接続を確立します。

ステップ 2　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。

管理インターフェイスの新規の IP アドレスを設定します。

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。

管理インターフェイスの IP アドレスの設定：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
```

タイム クロックおよびタイム ゾーンの設定

SCE プラットフォームには、設定可能な 3 つのタイプ（クロック、カレンダー、およびタイム ゾーン）の時間設定があります。クロックおよびカレンダーをローカル時間に同期化させ、タイム ゾーンを正確に設定することが重要です。SCE プラットフォームは、サマータイムを自動追跡しないので、時間が半年ごとに変わるたびに、タイム ゾーンを更新する必要があります。

SCE プラットフォームには、2 つのタイム ソースがあります。

- カレンダーと呼ばれるリアルタイム クロック。SCE プラットフォームが起動していないときでも継続して時間を追跡します。SCE プラットフォームがリブートされると、システム クロックを設定するためにカレンダー時間が使用されます。カレンダーは、システム動作時の時間の追跡には使用されません。
- システム　クロック。通常の動作時に、すべてのタイム　スタンプを作成します。システムがシャットダウンされると、このクロックは消去されます。システム起動時に、クロックが初期化され、カレンダーが示す時間を表示します。

クロックとカレンダーの読み取りコマンドを使用して、確実に両者を同期化すれば、どちらのクロックを先に設定するかどうかは、問題になりません。

タイム ゾーンの設定は、システムと他のタイム ゾーンによる他のシステムとの正常な通信を可能にするため、重要です。システムは、Coordinated Universal Time（UTC; 世界標準時）に基づいて設定されています。UTC は、他のメーカーのハードウェアとソフトウェアとの連携に使用される業界標準です。たとえば、太平洋標準時間は PST-10 のように記述されます。これは、タイム ゾーンの名前が PST で、UTC から 10 時間遅れていることを意味します。

時間の設定と表示を行う場合、常に設定されたローカル タイム ゾーンに従って、時間が入力されたり、表示されたりします。

システム時間の表示

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

システム時間の表示：例

次の例は、現在のシステム クロックを表示します。

```
SCE#show clock
12:50:03  UTC  MON  November 13 2001
sce#
```

カレンダー時間の表示

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

カレンダー時間の表示：例

次の例は、現在のシステム カレンダーを表示します。

```
SCE#show calendar
12:50:03  UTC  MON  May 11 2007
sce#
```

システム クロックの設定

オプション

次のオプションを使用できます。

- **time-date** — 設定する日時。次の形式で設定します。
  hh:mm:ss day month year

ステップ 1　SCE# プロンプトで、**clock set** *time-date* と入力し、**Enter** キーを押します。

指定した日時にシステム クロックを設定します。

システム クロックの設定：例

次に、2007 年 5 月 13 日午前 10 時 20 分にクロックを設定し、カレンダーを更新してから、時間を表示する例を示します。

```
SCE#clock set 10:20:00 13 may 2007
SCE#clock update-calendar
SCE#show clock
10:21:10  UTC  THU  May  13  2007
```

カレンダーの設定

カレンダーは、システムのシャットダウン後も機能するシステム クロックです。

オプション

次のオプションを使用できます。

- **time-date** — 設定する日時。次の形式で設定します。
  hh:mm:ss day month year

ステップ 1　SCE# プロンプトで、**calendar set** *time-date* と入力し、**Enter** キーを押します。

指定した日時にシステム カレンダーを設定します。

このコマンドで指定した時間は、設定されたタイム ゾーンとの関係によって決まります。

ステップ 2　SCE# プロンプトで、**clock read-calendar** と入力し、**Enter** キーを押します。

設定したカレンダー時間にシステム クロックを同期させます。

カレンダーの設定：例

次に、カレンダーを 2007 年 5 月 13 日の午前 10 時 20 分に設定する例を示します。その後、クロックがカレンダー設定に同期化されます。

```
SCE#calendar set 10:20:00 13 may 20017
SCE#clock read-calendar
SCE#show calendar
10:21:06  UTC  THU  May  13  2007
```

タイム ゾーンの設定

オプション

次のオプションを使用できます。

- **zone** — 表示するタイム ゾーンの名前
  デフォルト = GMT
- **hours** — UTC からのオフセットの時間数。–23 ～ 23 の整数範囲にする必要があります。
  デフォルト = 0
- **minutes** — UTC からのオフセットの分数。0 ～ 59 の整数範囲にする必要があります。オフセットを時間だけで測定できない場合にさらに分で指定するには、このパラメータを使用します。
  デフォルト = 0

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

指定したタイムゾーン名と設定したオフセット（時間と分数）で、タイムゾーンを設定します。

タイム ゾーンの設定：例

次に、UTC より 10 時間遅れたオフセットによる太平洋標準時間にタイム ゾーンを設定する例を示します。

```
SCE(config)#clock timezone PST -10
SCE(config)#
```

現在のタイム ゾーン設定の削除

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

タイムゾーンの設定を削除し、タイムゾーンをデフォルトの値（UTC）にリセットします。

サマータイムの設定

指定された日付に、SCE プラットフォームが自動的にサマータイムに切り替わり、標準時間に戻るように設定できます。さらに、サマータイムが多様な場合は、必要に応じて、タイム ゾーン コードを設定できます（たとえば、米国東部では、標準時間が EST に指定され、サマータイムが EDT に指定されます）。

- オプション（p.5-42）
- 注意事項（p.5-43）
- 繰り返されるサマータイムの遷移を定義する方法（p.5-43）
- 繰り返されないサマータイムの遷移を定義する方法（p.5-43）
- サマータイムの設定のキャンセル方法（p.5-44）
- 現在のサマータイムの設定の表示方法（p.5-44）

オプション

特定の場所でサマータイムの開始日と終了日をどのように決めているかに応じて、サマータイムへの遷移時間、またはサマータイムからの遷移時間を 2 つの方法のいずれかに設定できます。

- 繰り返し — サマータイムが毎年、同じ日に開始し、終了する場合（例：米国）、**clock summer-time recurring** コマンドを使用します。サマータイムの開始日と終了日を 1 回で設定でき、システムが毎年、切り替えを自動的に実行します。
- 繰り返しなし　—　サマータイムの開始と終了が毎年異なる場合（例：イスラエル）、**clock summer-time** コマンドを使用します。この場合、その年に特有の遷移を毎年設定する必要があります（「年度」は、必ずカレンダー通りの年度になるわけではありません。遷移日が秋に決められた場合は、その年の秋と来春の遷移を設定できます）。

さまざまな方法で、遷移日を定義できます。

- 具体的な日付 — たとえば、2004 年 3 月 29 日。年度も含まれる具体的な日付は、繰り返しなしの設定に定義します。
- 特定の月の最初の曜日 / 最後の曜日 — たとえば、3 月の最終日曜日。これは、繰り返しの設定に使用します。
- 特定の月の特定の週の曜日 — たとえば、3 月の第 4 日曜日（これは、月に 5 回、日曜日がある場合の最終日曜日とは異なります）。これは、繰り返しの設定に使用します。

次のオプションを使用できます。

- **zone** — サマータイムのタイム ゾーン コード
- **week**（繰り返しの場合のみ）— サマータイムが開始し（week1）、終了する（week2）月の週
- **day**（繰り返しの場合のみ）— サマータイムが開始し（day1）、終了する（day2）週の曜日
- **date**（繰り返しなしの場合のみ）— サマータイムが開始し（date1）、終了する（date2）月の日付
- **month** — 開始し（month1）、終了する（month2）サマータイムの月
- **year**（繰り返しなしの場合のみ）— 開始し（year1）、終了する（year2）サマータイムの年

- **offset** — 標準時間とサマータイムの誤差（分単位）
  デフォルト値は 60 分です。

注意事項

サマータイムの遷移を設定する際の一般的な注意事項は、次のとおりです。

- サマータイムにタイム ゾーン コードを指定します。
- 繰り返し — 月の中から 1 日（週の番号 | 最初 | 最後 / 曜日 / 月）を指定します。
- 繰り返しなし — 具体的な日付（月 / 日 / 年）を指定します。
- 2 つの日付を定義します。
  - Day1 = サマータイムの開始日
  - Day2 = サマータイムの終了日
- 南半球では、サマータイムが秋に始まり、春に終わるので、month1 の前に month2 が来る必要があります。
- 遷移が行われる正確な時間（24 時間のクロック）を指定します。
  - サマータイムへの遷移時間 — ローカル標準時間に従います。
  - サマータイムからの遷移時間 — ローカル サマータイムに従います。
- **clock summer-time recurring** コマンドでは、デフォルト値が米国の遷移規則になります。
  - サマータイムの開始 — 3 月の第 2 日曜日の午前 2 時
  - サマータイムの終了 — 11 月の第 1 日曜日の午前 2 時

繰り返されるサマータイムの遷移を定義する方法

ステップ 1　SCE(config)# プロンプトで、**clock summer-time** *zone* ***recurring*** [*week1 day1 month1 time1 week2 day2 month2 time2* [*offset*]] と入力し、**Enter** キーを押します。

毎年指定した日に開始および終了するサマータイムを設定します。

繰り返されるサマータイムの遷移の定義：例

次に、タイム ゾーンが次のように「DST」に指定された場合の繰り返しのサマータイムを設定する例を示します。

- サマータイムの開始 — 3 月の最終日曜日の 0:00
- サマータイムの終了 — 11 月の第 4 土曜日の 23:59
- オフセットは、1 時間です（デフォルト）。

```
SCE(config)# clock summer-time DST recurring last Sunday March 00:00  4 Saturday
November 23:59
```

繰り返されないサマータイムの遷移を定義する方法

ステップ 1　SCE(config)# プロンプトで、**clock summer-time** *zone* [*date1 month1 year1 time1 date2 month2 year2 time2* [*offset*]] と入力し、**Enter** キーを押します。

繰り返されないサマータイムの遷移の定義：例

次に、タイム ゾーンが次のように「DST」に指定された場合の繰り返しなしのサマータイムを設定する例を示します。

- サマータイムの開始 — 2004 年 4 月 16 日の 0:00
- サマータイムの終了 — 2004 年 10 月 23 日の 23:59
- オフセットは、1 時間です（デフォルト）。

```
SCE(config)# clock summer-time DST April 16 2004 00:00 October 23 2004 23:59
```

サマータイムの設定のキャンセル方法

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

すべてのサマータイムの設定を削除します。

現在のサマータイムの設定の表示方法

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

現在のタイム ゾーンとサマータイムの設定を表示します。

DNS の設定

ホスト名または IP アドレスを要求する CLI コマンドのパラメータとしてホスト名が与えられる場合、次の内容に従って、IP アドレスが名前に変換されます。

1. 名前がドット付き表記（x.x.x.x の形式）である場合、該当する IP アドレスに直接変換されます。
2. 名前にドット文字（.）が含まれない場合、システムは IP ホスト テーブルを調べます。テーブルに名前がある場合は、該当する IP アドレスにマッピングされます。**ip host** コマンドを使用して、IP ホスト テーブルを設定できます。
3. 名前にドット（.）文字が含まれず、ドメイン名機能がイネーブルにされ（**ip domain-lookup** コマンドを参照）、デフォルトのドメイン名が指定されている場合（**ip domain-name** コマンドを参照）、デフォルトのドメイン名は、完全に記述したドメイン名を形成するために所定の名前に追加されます。これは、IP アドレスに名前を変換する Domain Name Server（DNS）クエリーの実行にも使用されます。
4. それ以外の場合は、ドメイン名機能がイネーブルにされると、名前が完全に記述されているものとしてみなされ、IP アドレスに名前を変換する DNS クエリーの実行に使用されます。

DNS の設定に関連するコマンドは、次のとおりです。

- **ip name-server**
- **ip domain-name**
- **no ip domain-name**
- **ip domain-lookup**
- **show hosts**

DNS lookup の設定

DNS lookup のイネーブル化の方法

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

DNS lookup をイネーブルにします。

DNS lookup のディセーブル化の方法

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

ネーム サーバの設定

オプション

次のオプションを使用できます。

- **server-ip-address** — DNS の IP アドレス。複数の DNS サーバ（server-ip-address1、server-ip-address2、server-ip-address3）を定義できます。

DNS の定義方法

名前およびアドレス解決に 1 つまたは複数のネーム サーバのアドレスを指定するには、このコマンドを使用します。

ステップ 1　SCE(config)# プロンプトで、**ip name-server** *server-address1 [server-address2 [server-address3]]* と入力し、**Enter** キーを押します。

指定したアドレスのサーバを DNS として定義します。

DNS の定義：例

次に、2 つのネーム サーバ（DNS）の IP アドレスを設定する例を示します。

```
SCE(config)#ip name-server 10.1.1.60 10.1.1.61
```

DNS の削除方法

ステップ 1　SCE(config)# プロンプトで、**no ip name-server** *server-address1 [server-address2 [server-address3]]* と入力し、**Enter** キーを押します。

DNS リストから指定したサーバを削除します。

DNS の削除：例

次に、ネーム サーバ（DNS）の IP アドレスを削除する例を示します。

```
SCE(config)#no ip name-server 10.1.1.60 10.1.1.61
```

すべての DNS の削除方法

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

設定したすべての DNS サーバを削除します。

ホストをホスト テーブルに追加する方法

オプション

次のオプションを使用できます。

- **hostname** — ホストの名前
- **ip-address** — ホストの IP アドレス

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

指定したホストをホスト テーブルに追加します。

削除するホストのホスト テーブルへの追加：例

次に、ホスト テーブルにホストを追加する例を示します。

```
SCE(config)#ip host PC85 10.1.1.61
```

次に、すべての IP マッピングとホスト名を同時に削除する例を示します。

```
SCE(config)#no ip host PC85
```

現在の DNS 設定の表示方法

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

現在の DNS 設定値を表示します。

現在の DNS 設定値の表示：例

次に、現在の DNS 情報を表示する例を示します。

```
SCE#show hosts
Default domain is Cisco.com
Name/address lookup uses domain service
Name servers are 10.1.1.60, 10.1.1.61
Host                 Address
----                 -------
PC85                 10.1.1.61
sce#
```