CHAPTER 5

管理インターフェイスの接続および初期システム設定の実行

概要

この章では、SCE 1000 プラットフォームをローカル コンソールに接続し、自動実行されるセットアップ ウィザードから初期システム設定を実行する方法について説明します。

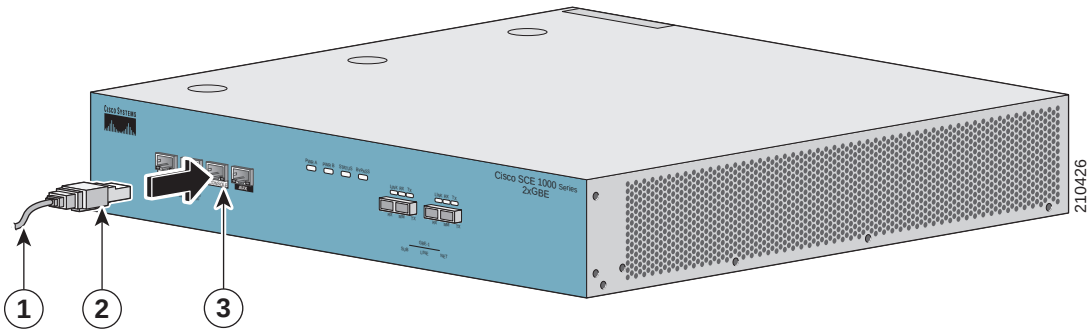
また、ファスト イーサネット管理インターフェイスのケーブル接続手順も示します。

ローカル コンソールのセットアップ方法

リモートの位置から SCE 1000 を管理する場合でも、まずローカル コンソールに装置を接続して SCE 1000 の初期設定を行い、リモート管理がサポートされるようにする必要があります。初期接続を確立したら、セットアップ ユーティリティが自動的に起動し、初期システムの実行を求めるプロンプトが表示されます（図 5-1）。

ここでは、セットアップ ユーティリティを使用して SCE 1000 システムの初期システム設定を実行できるように、ワークステーションのローカル端末を設定する手順を示します。

図 5-1　ローカル コンソールと SCE 1000 CON ポートの接続



端末が次のように設定されていることを確認します。

- 9,600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット
- フロー制御なし

上記の SCE 1000 ポート パラメータは固定されていて、設定を変更できません。

ステップ 1　SCE 1000 付属の <SKIP> シリアル ケーブルを、SCE 1000 の前面パネルにある CON ポートに差し込みます。

RJ-45 コネクタ（<SKIP> シリアル ケーブルに装着）が完全に挿入され、カチッという音がしてレセプタクルに固定されるまで、コネクタを押し込みます。ゆっくりとプラグを引っ張り、プラグがソケットに固定されているかどうかを確認します。

ステップ 2　シリアル ケーブルの他端（装着された DB-9 コネクタ）を VT100 互換ローカル（シリアル）端末に接続します。

ステップ 3　ローカル端末が、固定された SCE 1000 CON ポート パラメータに従って、VT-100 端末として設定されていることを確認します。

ステップ 4　ローカル端末にシスコ ロゴが表示され、設定ダイアログが開始するまで、Enter キーを数回押します。

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' followed by 'Enter' for help.
Use ctrl-C to abort configuration dialog at any prompt.
Use ctrl-Z to jump to the end of the configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Would you like to continue with the System Configuration Dialog? [yes/no]: y
```

ステップ 5　**y** を入力して、Enter キーを押します。システム設定ダイアログが開始します。

初期システム設定の実行

初期システム設定

セットアップ コマンド

上記の説明に従ってローカル端末との最初の接続を確立すると、システム設定ウィザードが自動的に起動し、セットアップ プロセス全体の手順が示されます。ウィザードではすべての必須パラメータの入力が求められます。デフォルト値が適用できる場合は、デフォルト値が表示されます。デフォルト値を受け入れたり、他の値を定義することができます。

ダイアログが完了したら、新しい設定を適用する前に、確認することができます。変更されなかったパラメータを含めて、設定が表示されます。また、この設定で検出されたエラーも表示されます。設定が満足のいくものである場合は、新しい設定を適用し、保存することができます。

次の表に、初期設定に含まれるパラメータをすべて示します。この時点で設定するすべてのパラメータ値は、セットアップを開始する前に取得しておくことを推奨します。

（注）　設定手順または特定のパラメータの詳細については、『*Cisco SCE 2000 and SCE 1000 Software Configuration Guide*』を参照してください。

セットアップ コマンド パラメータ

表 5-1 にセットアップ コマンド パラメータを示します。

表 5-1　セットアップ コマンド パラメータ

パラメータ	定義
IP address	SCE 1000 の IP アドレス。
subnet mask	SCE 1000 のサブネット マスク。
default gateway	デフォルト ゲートウェイ。
hostname	SCE 1000 の識別に使用される文字列（最大 20 文字）。
admin password	Admin レベル パスワード。英文字で開始する 4 ～ 100 文字の文字列。
root password	Root レベル パスワード。英文字で開始する 4 ～ 100 文字の文字列。
password encryption status	パスワード暗号化のイネーブル化/ディセーブル化。
時間設定	
time zone name and offset	標準タイム ゾーンの省略形および UTC（協定世界時）からのオフセット（分）。
local time and date	現在のローカル時刻および日付。フォーマットは次のとおりです。00:00:00 1 January 2002
SNTP 設定	

表 5-1　セットアップ コマンド パラメータ （続き）

パラメータ	定義
broadcast client status	SNTP ブロードキャスト クライアントのステータスを設定します。イネーブルな場合、SCE はローカル時刻と、SNTP ブロードキャスト サーバから受信したアップデートを同期させます。
unicast query interval	アップデートに関するユニキャスト要求の秒単位のインターバル（64 ～ 1024）。
unicast server IP address	SNTP ユニキャスト サーバの IP アドレス。
DNS の設定	
DNS lookup status	IP DNS ベース ホスト名変換のイネーブル化/ディセーブル化。
default domain name	修飾されていないホスト名を完成するために使用されるデフォルト ドメイン名。
IP address	ドメイン ネーム サーバの IP アドレス（最大 3 台のサーバ）。
TCP Port number	RDR フォーマッタ送信先の TCP ポート番号。
Access Control List（ACL; アクセス制御リスト）	
Access Control List number	必要な ACL 数。管理インターフェイスごとにアクセスを許可/拒否する IP アドレス。次の場合に ACL が必要です。 • すべての IP アクセス • Telnet アクセス • SNMP GET アクセス • SNMP SET アクセス
list entries（リストごとに最大 20）	IP アドレス、アクセスの許可/拒否。
IP access ACL	IP アクセスを制御する ACL の ID 番号。
telnet ACL	Telnet アクセスを制御する ACL の ID 番号。
SNMP agent status	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）管理のイネーブル化/ディセーブル化。
GET community names	GET アクセスを許可するコミュニティ ストリング、および対応する ACL（最大 20）。
SET community names	SET アクセスを許可するコミュニティ ストリング、および対応する ACL（最大 20）。
trap managers （最大 20）	トラップ マネージャの IP アドレス、コミュニティ ストリング、および SNMP バージョン。
Authentication Failure trap status	認証失敗トラップのステータスを設定します。
enterprise traps status	エンタープライズ トラップのステータスを設定します。
system administrator	システム管理者の名前。

表 5-1　セットアップ コマンド パラメータ （続き）

パラメータ	定義
トポロジの設定	
connection mode	SCE 1000 がインライン トポロジで取り付けられているか、または外部光スプリッタを使用した受信専用トポロジで取り付けられているか。
link bypass mode on operational status	SCE 1000 が動作可能な場合に、トラフィックをバイパスする必要があるかどうか。
redundant SCE 1000 platform?	冗長 SCE 1000 がバックアップとして取り付けられているかどうか。
link bypass mode on non-operational status	SCE 1000 が動作不能な場合に、トラフィックをバイパスするか、または切断するか。
operational status of the SCE after abnormal boot	障害が原因でリブートを行ったあとに、SCE 1000 を障害ステータスのままにするか、または他の問題が検出されない場合に動作可能ステータスに移行するか。

設定ダイアログに関する一般的な手順を次に示します。

- すべてのデフォルト値は、角カッコ [default] 内に表示されます。

  カッコ [ ] 内に値がない場合、または複数のオプションが表示される場合（[yes/no]）は、このパラメータにデフォルト値がありません。
- デフォルト値を受け入れるには、**Enter** キーを押します。
- パラメータの詳細が必要な場合は、**?** を入力して、**Enter** キーを押します。

  パラメータの想定フォーマットおよびその他の要件を示すヘルプ メッセージが表示されます。
- 任意の時点で設定ダイアログの末尾にジャンプして、残りのデフォルト値をすべて受け入れる場合は、^z を押します。
- 場合によっては、メニュー内に論理的に関連したパラメータが複数表示されることがあります。このような場合は、すべての関連パラメータを設定するまで、設定ダイアログの末尾にジャンプできません。設定ダイアログの末尾にジャンプしようとすると、次のメッセージが表示されます。

  `"Sorry, Skipping is not allowed at this stage."`
- 設定ダイアログ内のサブダイアログまたはメニューには、関連性のある各パラメータ（時刻、日付、SNTP 設定など）がグループごとに分類されています。メニュー全体を省略すると、メニュー内のパラメータのデフォルト値をすべて受け入れることができます。

  各関連パラメータ グループの先頭で、メニューを開始するかどうかを尋ねる質問が表示されます。メニューを省略するには、質問に「n」と答えます。

例：

```
Would you like to enter the SNMP configuration menu? n
```

設定を変更しないで、任意の時点で設定ダイアログを打ち切る場合は、^c を押します。入力済みの変更は、時間設定を除いてすべて失われます。

ステップ 1：初期設定

次に示す、SCE 1000 の初期設定を確認します。

- IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ

すべての値は、「X.X.X.X」形式のインターネット アドレスです。各文字は 0 ～ 255 の 10 進数に対応しています。

ステップ 1　IP アドレスを設定します。

現在の IP アドレスが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、「x.x.x.x」形式で目的の値を入力し、Enter キーを押します。

ステップ 2　サブネット マスクを設定します。

現在のサブネット マスクが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、「x.x.x.x」形式で目的の値を入力し、Enter キーを押します。

ステップ 3　デフォルト ゲートウェイを設定します。

デフォルト ゲートウェイの現在の IP アドレスが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、「x.x.x.x」形式で目的の値を入力し、Enter キーを押します。

例：

次の例は、IP アドレス（10.1.5.109）、サブネット マスク（255.255.0.0）、およびデフォルト ゲートウェイ（10.1.1.3）の一般的な設定を示します。

IP アドレスおよびサブネット マスクは関連しているため、IP アドレスを変更した場合、サブネット マスクのデフォルト値は存在しなくなり、明示的に入力する必要が生じます。

```
Enter IP address [10.1.1.201]:10.1.5.109
Enter IP subnet mask:255.255.0.0
Enter IP address of default gateway [10.1.1.3]:
```

ステップ 2：ホスト名の設定

ホスト名は SCE 1000 を識別するのに使用されます。ホスト名は CLI プロンプトの一部として表示され、MIB-II の sysName オブジェクトの値としても返されます。

最大長は、20 文字です。

デフォルトのホスト名は、SCE 1000 です。

ステップ 1　SCE プラットフォームのホスト名を指定します。

デフォルトのホスト名が表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、目的の文字列を入力し、Enter キーを押します。

```
Enter hostname [SCE 1000]:
```

ステップ 3：パスワードの設定

次のようにパスワードを設定します。

- 認証レベル（User、Admin、Root）ごとにパスワードを設定します。
- パスワード暗号化をイネーブルまたはディセーブルにします。パスワード暗号化がイネーブルの場合、入力済みのパスワードが暗号化されます。

（注）　パスワードは、許可されていないユーザによる SCE 1000 へのアクセスを防止するために、あらゆる認証レベルで必要になります。Admin レベルは、ネットワーク管理者が使用するものです。Root レベルは、シスコの技術者が使用します。

パスワードは次の基準を満たしている必要があります。

- 最小：4 文字
- 最大：100 文字
- 英文字で開始
- 出力可能な文字だけを含めることができる

（注）　パスワードは大文字と小文字が区別されます。

（注）　すべてのレベルのデフォルト パスワードは、Cisco です。

ステップ 1　User パスワードを設定します。

デフォルト User パスワードが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、必要な文字列を入力し、Enter キーを押します。

ステップ 2　Admin パスワードを設定します。

デフォルト Admin パスワードが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、必要な文字列を入力し、Enter キーを押します。

ステップ 3　Root パスワードを設定します。

デフォルト Root パスワードが表示されます。

- 表示された値を受け入れるには、Enter キーを押します。
- 値を変更するには、必要な文字列を入力し、Enter キーを押します。

ステップ 4　パスワード暗号化を設定します。デフォルトでは、パスワード暗号化はディセーブルです。

- パスワード暗号化をディセーブルにするには、Enter キーを押します。
- パスワード暗号化をイネーブルにするには、y を入力して、Enter キーを押します。

例：

次に、すべてのパスワードを変更する例を示します。パスワード暗号化はディセーブルです（デフォルト）。

```
Enter a User password [Cisco]: userin
Enter an Admin password [Cisco]: mng123
Enter a Root password [Cisco]: cistech
Enable passwords encryption? [no]:
```

ステップ 4：時間設定

時間設定メニューは、システム内のすべての日時関連パラメータを設定します。時間設定メニューには、次が含まれています。

- タイム ゾーン
- ローカル時刻
- 日付
- SNTP メニュー

SNTP 設定を設定するには、時間設定メニューを開始する必要があります。すべてのデフォルト値を受け入れる場合は、時間設定メニューを省略できます。

（注）　時間設定は、システム設定で定義されるその他のすべての設定と異なり、設定は設定プロセスの終了時でなく、ただちに適用されます。

ステップ 1　時間設定メニューを開始します。

```
Would you like to enter the Time settings menu? [no]: y
```

y を入力して、Enter キーを押します。

ステップ 2　タイム ゾーンを設定します。

タイム ゾーンの省略形を入力し、Enter キーを押します。

```
Enter time zone name [UTC]: CET
```

ステップ 3　UTC からのオフセットを指定します。

UTC からのオフセット（分）を入力し、Enter キーを押します。

```
Enter time zone minutes offset from UTC: 60
```

ステップ 4　ローカル時刻および日付を確認します。

ローカル時刻および日付が表示され、これらを変更するかどうかが確認されます。

```
The local time and date is 15:00:01 CET FRI 01 July 2002
Would you like to set a new time and date? [no]:
```

- 日時が正しい場合は、「ステップ 5：DNS 設定」に進みます。
- 日時が正しくない場合は、上記質問に yes と応答して、Enter キーを押します。

```
Would you like to set a new time and date? [no]: y
Confirm your response and type the new time and date.
This change will take effect immediately both on the system clock and calendar; it
will also set the time zone you entered. Are you sure? [yes/no]: y
Enter new local time and date: 14:00:01 1 July 2002
Time zone was successfully set.
The system clock and the calendar were successfully set.
```

ステップ 5　SNTP 設定メニューを開始します。

SNTP を設定しない場合は、このセクションの残りの部分を省略し、「ステップ 5：DNS 設定」（P.5-10）に進みます。

SNTP 設定ダイアログを開始するには、y を入力して、Enter キーを押します。

```
Would you like to enter the SNTP configuration menu? [no]: y
```

ステップ 6　SNTP ブロードキャスト クライアントを設定します。デフォルトでは、SNTP ブロードキャスト クライアントはディセーブルです。

- SNTP ブロードキャスト クライアントをディセーブルにするには、Enter キーを押します。
- SNTP ブロードキャスト クライアントをイネーブルにするには、y を入力して、Enter キーを押します。

```
Enable SNTP broadcast client? [no]:
```

ステップ 7　ユニキャスト アップデート間のインターバルを定義します。

- 表示されたデフォルト値を受け入れるには、Enter キーを押します。

```
Enter time interval in seconds between unicast updates [1024]:
```

ステップ 8　SNTP ユニキャスト サーバの IP アドレスを指定します。

ホスト名または x.x.x.x 形式の IP アドレスを入力して、Enter キーを押します。

```
Would you like to configure SNTP unicast servers? [no]: y
Enter IP address or hostname of SNTP unicast server: 10.1.1.1
```

例：

次に、時間設定ダイアログの例を示します。タイム ゾーンが設定されるだけでなく、日時が変更され、SNTP ユニキャスト アップデートが設定されます。

```
Would you like to enter the Time settings menu? [no]: y
Enter time zone name [UTC]: ISR
Enter time zone minutes offset from UTC: 120
The local time and date is 15:35:23 ISR FRI July 19 2002
Would you like to set a new time and date? [no]: y
This change will take effect immediately both on the system clock
and the calendar; it will also set the time zone you entered.
Are you sure? [yes/no]: y
Enter new local time and date: 14:35:23 19 July 2002
Time zone was successfully set.
The system clock and the calendar were successfully set.
Would you like to enter the SNTP configuration menu? [no]: y
Enable SNTP broadcast client? [no]: y
Enter time interval in seconds between unicast updates [900]:
Would you like to configure SNTP unicast servers? [no]: y
Enter IP address or hostname of SNTP unicast server: 10.1.1.1
```

ステップ 5：DNS 設定

DNS 設定メニューでは、DNS lookup に使用されるドメイン ネーム サーバの IP アドレス、および修飾されていないホスト名を完成させる場合に使用されるデフォルト ドメイン名を定義します。

すべてのデフォルト値を受け入れる場合は、DNS 設定メニューを省略できます。

ステップ 1　DNS 設定メニューを開始します。

```
Would you like to enter the DNS configuration menu? [no]: y
```

y を入力して、Enter キーを押します。

DNS 設定ダイアログが開始します。

ステップ 2　DNS lookup をイネーブルまたはディセーブルにします。

- DNS lookup をイネーブルにするには、Enter キーを押します。
- DNS lookup をディセーブルにするには、n を入力して、Enter キーを押します。

```
Enable IP DNS-based hostname translation? [yes]:
```

DNS lookup をディセーブルにする場合は、このセクションの残りの部分を省略し、に進みます。ダイアログの残りは表示されません。DNS lookup がディセーブルな場合、これらは関係しなくなるためです。

ステップ 3　使用するデフォルト ドメイン名を入力し、Enter キーを押します。

デフォルト ドメイン名は存在しません。

デフォルト ドメイン名を受け入れるか、または新しいドメイン名を入力することができます。

```
Enter default domain name []:
```

ステップ 4　プライマリ ドメイン ネーム サーバを設定します。

プライマリ ドメイン ネーム サーバの IP アドレスを入力して、Enter キーを押します。

```
Enter Primary DNS IP address:
```

このパラメータのデフォルト値は存在しません。

ステップ 5　他に設定するドメイン ネーム サーバがあれば設定します。

ドメイン サーバは 3 つまで設定できます。

```
Would you like to add another Name Server? [no]:
```

- DNS 設定ダイアログを終了するには、Enter キーを押します。
- 別のドメイン サーバを追加するには、y を入力して、Enter キーを押します。

次のドメイン ネーム サーバの IP アドレスを入力するように求められます。

```
Enter Secondary DNS IP address:
```

ステップ 6　ダイアログを終了します。

すべてのサーバの IP アドレスを入力したら、Enter キーを押してダイアログを終了します。

```
Would you like to add another Name Server? [no]:
```

例：

次に、DNS 設定ダイアログの例を示します。デフォルト ドメイン名は pcube.com、ドメイン ネーム サーバの IP アドレスは 10.1.1.230 です。

```
Would you like to enter the DNS configuration menu? [no]: y
Enable IP DNS-based hostname translation? [yes]:
Enter default domain name []: pcube.com
Enter Primary DNS IP address: 10.1.1.230
Would you like to add another Name Server? [no]:
```

ステップ 6：RDR フォーマッタ送信先の設定

SCE 1000 は Raw Data Records（RDR; 未加工データ レコード）を、RDR フォーマッタから外部収集システムに送ります。データが正しい場所に到達するように、外部収集システムの IP アドレスおよびポート番号を設定する必要があります。

ステップ 1　RDR フォーマッタ設定メニューを開始します。

```
Would you like to enter the RDR-formatter configuration menu? [no]: y
```

y を入力して、Enter キーを押します。

RDR フォーマッタ送信先ダイアログが開始されます。

ステップ 2　RDR フォーマッタ送信先の IP アドレスを指定します。

RDR フォーマッタ送信先の IP アドレスを入力して、Enter キーを押します。

```
Enter RDR-formatter destination's IP address:
```

このパラメータのデフォルト値は存在しません。

ステップ 3　RDR フォーマッタ送信先の TCP ポート番号を指定します。

RDR フォーマッタ送信先の TCP ポート番号を入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

```
Enter RDR-formatter destination's TCP port number:
```

例：

次に、IP アドレスおよび TCP ポート番号を割り当てる、RDR フォーマッタ設定ダイアログの例を示します。

```
Would you like to enter the RDR-formatter configuration menu? [no]: y
Enter RDR-formatter destination's IP address: 10.1.1.230
Enter RDR-formatter destination's TCP port number: 33000
```

ステップ 7：アクセス制御リスト（ACL）の設定

アクセス制御リストについて

ACL の設定

任意の管理インターフェイスへの着信接続を許可または拒否することができるアクセス制御リスト（ACL）を SCE 1000 に設定します。

（注）　ACL #0 は、すべての IP アドレスへのアクセスを許可する定義済みリストです。

アクセス制御リストの設定は、2 つの手順からなります。

1. アクセス制御リストを作成します。

   それぞれ最大 20 のエントリを持つ ACL を 99 作成できます。各エントリには IP アドレス、およびこの IP アドレスへのアクセスを許可するか、または拒否するかの指定が含まれています。

2. 適切な管理インターフェイスに ACL を割り当てます。

   このダイアログでは、ACL の作成/編集を省略して、ただちに管理インターフェイスへの ACL の割り当てに進むことができます。

エントリのフォーマット

各 ACL はすべての IP アドレス、1 つ以上の IP アドレス範囲、または 1 つ以上の個別 IP アドレスへのアクセスを許可または拒否することができます。これらのオプションをサポートするために、3 つのエントリ フォーマットが用意されています。

- すべての IP アドレス：「any」と入力します。すべての IP アドレスへのアクセスが許可または拒否されます。
- IP アドレス範囲：目的の範囲の先頭 IP アドレスを入力してから、範囲を定義するワイルドカード ビットを入力します。

  このワイルドカードは、逆マスクのように機能します。ワイルドカード内のすべての「1」ビットは、IP アドレス内の対応するビットを無視することを示します。その他のすべてのビットは、指定された IP アドレス内の対応するビットと一致する必要があります。例については、表 5-2 を参照してください。

  各 IP アドレス範囲へのアクセスを許可または拒否するように設定できます。
- 個別の IP アドレス：目的の IP アドレスを入力してから、ワイルドカード ビット 0.0.0.0 を入力します。

  各 IP アドレスへのアクセスを許可または拒否するように設定できます。

表 5-2　IP アドレス/ワイルドカード ビットの例

初期 IP アドレス	ワイルドカード ビット	範囲
10.1.1.0	0.0.0.255	10.1.1.0 ～ 10.1.1.255
10.1.1.0	0.0.0.63	10.1.1.0 ～ 10.1.1.63
10.1.1.0	0.0.0.0	10.1.1.0（個別のエントリ）

エントリの順序

リスト内のエントリの順序は重要です。リスト内のエントリは順にテストされ、接続先 IP アドレスと一致する最初のエントリによってアクションが決定されます。したがって、アクセス制御リスト内にエントリ「any」が存在する場合、それ以降のすべてのエントリは無関係になります。

同じエントリを異なる順序で含む、2 つの ACL の例について検討します。

次のリストは、10.1.1.0 を含む、すべての IP アドレスへのアクセスを許可します。

```
permit any
deny 10.1.1.0
```

「any」エントリのあとに、別のエントリを追加できないため、セットアップ ユーティリティを使用して上記リストを実際に作成できません。

次のリストは、IP アドレス 10.1.1.0 へのアクセスを拒否しますが、その他のすべてのアドレスへのアクセスは許可します。

```
deny 10.1.1.0
permit any
```

割り当てられたアクセス制御リスト内のどのエントリも接続と一致しない場合、またはアクセス制御リストが空の場合、デフォルト アクションは deny です。

アクセス制御リストを作成する手順は、次のとおりです。

ステップ 1　アクセス制御リスト設定メニューを開始します。

```
Would you like to enter the Access lists configuration menu? [no]:y
```

y を入力して、Enter キーを押します。

アクセス制御リスト設定ダイアログが開始します。

ステップ 2　アクセス制御リストを設定または変更することができます。また、このセクションを省略して、目的の管理インターフェイスに既存の ACL を割り当てる作業にただちに進むこともできます。

```
Would you like to create new Access lists or modify existing lists? [no]: y
```

アクセス制御リストの作成や編集を行わない場合は、に進みます。

ステップ 3　設定するアクセス制御リスト数（1 ～ 99）を入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

ステップ 4　選択したリストにエントリを追加します。

このエントリへのアクセスを許可するか、または拒否するかを指定します。

- アクセスを許可するには、Enter キーを押します。
- アクセスを拒否するには、n を入力して、Enter キーを押します。

ステップ 5　このリストに追加する IP アドレスを入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

```
Enter IP address or the word 'any' to denote any IP address:
```

ステップ 6　特定の IP アドレスを入力した場合は、IP アドレス範囲を定義するワイルドカード ビットを入力して、Enter キーを押します（「エントリのフォーマット」（P.5-13）を参照）。

個別の IP アドレスを定義するには、0.0.0.0 を入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

```
Enter wildcard bits:
```

ステップ 7　ACL の最大エントリ数は 20 です。

「any」オプションを使用した場合は、その他の IP アドレスをリストに追加できません。

- さらにエントリを追加するには、y を入力して、Enter キーを押します。

  ```
  Would you like to add another entry to this list? [no]:y
  ```

- ステップ 5 およびステップ 6 の説明に従って、最大 20 のエントリを入力します。
- すべてのエントリを追加したら、Enter キーを押します。

  ```
  Would you like to add another entry to this list? [no]:
  ```

ステップ 8　すべてのエントリをリストに追加したら、別の ACL を作成するかどうかが確認されます。最大 99 の ACL を定義できます。

- 別の ACL を作成するには、y を入力して、Enter キーを押します。

```
Would you like to configure another list? [no]: y
```

- ステップ 5 およびステップ 6 の説明に従って、この新しい ACL に最大 20 の IP アドレスを入力します。
- すべての ACL を作成したら、Enter キーを押します。

```
Would you like to configure another list? [no]:
```

- 目的の ACL を割り当てて、IP および Telnet アクセスを制限するように求められます。

ステップ 9　適切な ACL を割り当てて、SCE 1000 に対する IP アクセスを制限します。

IP アクセスに割り当てる ACL 数を入力して、Enter キーを押します。

デフォルト ACL を受け入れるには、Enter キーを押します。

```
Enter IP access-class [0]:
```

ステップ 10　適切な ACL を割り当てて、SCE 1000 に対する Telnet アクセスを制限します。

Telnet インターフェイスに割り当てる ACL 数を入力して、Enter キーを押します。

デフォルト ACL を受け入れるには、Enter キーを押します。

```
Enter Telnet access-class [0]: 2
```

例

例 1：

次に、一般的なアクセス制御の例を示します。次のように想定します。

- 管理ポート上で、すべてのステーションから SCE プラットフォームへのアクセスを許可します（ping、SNMP ポーリングなど）。
- Telnet アクセスは、許可された一部のステーションに限定する必要があります。

したがって、2 つのアクセス制御リストを作成する必要があります。

- 一般的な IP アクセス：すべての IP アドレスへのアクセスを許可します。
- Telnet アクセス：指定された IP アドレスへのアクセスを許可し、それ以外のすべてのアドレスへのアクセスを拒否します。

ACL #1 = すべての IP アドレスを許可します。IP アクセスに割り当てます。

ACL #2 = 10.1.1.0、10.10.10.1 へのアクセスを許可し、その他のすべてのアドレスへのアクセスを拒否します。Telnet アクセスに割り当てます。

```
Would you like to enter the Access lists configuration menu? [no]: y
Would you like to create new Access lists or modify existing lists? [no]: y
Enter ACL number: 1
Does this entry permit access? [yes]:
Enter IP address or the word ‘any’ to denote any IP address: any
This entry matches every IP address, no use in adding more entries to this list.
Would you like to configure another list? [no]: y
Enter ACL number: 2
Does this entry permit access? [yes]:
Enter IP address or the word ‘any’ to denote any IP address: 10.1.1.0
Enter wildcard bits: 0.0.0.0
```

```
Would you like to add another entry to this list? [no]:y
Does this entry permit access? [yes]:
Enter IP address or the word 'any' to denote any IP address: 10.10.10.1
Enter wildcard bits: 0.0.0.0
Would you like to add another entry to this list? [no]:y
Does this entry permit access? [yes]:n
Enter IP address or the word 'any' to denote any IP address: any
This entry matches every IP address, no use in adding more entries to this list.
Would you like to configure another list? [no]:
Enter IP access-class [0]: 1
Enter Telnet access-class [0]: 2
```

例 2：

次に、ダイアログの最初のセクション（作成/変更）を省略し、既存 ACL の割り当てにただちに進む例を示します。

```
Would you like to enter the Access lists configuration menu? [no]: y
Would you like to create new Access lists or modify existing lists? [no]:
Enter IP access-class [0]: 10
Enter Telnet access-class [0]: 22
```

ステップ 8：SNMP の設定

SCE 1000 の管理には、SNMP をサポートする Network Management System（NMS; ネットワーク管理システム）を使用することもできます。SCE 1000 のデフォルトでは、SNMP がディセーブルに設定されています。

SNMP 管理をイネーブルにするには、次の基本的な SNMP パラメータを設定する必要があります。

- SNMP トラップ ステータスおよびマネージャ
- コミュニティ ストリング（SNMP コミュニティ ストリングは、SCE 1000 の SNMP エージェントへのアクセスを許可するパスワードと同様に機能するテキスト ストリング）
-

ステップ 1　SNMP 設定メニューを開始します。

```
Would you like to enter the SNMP configuration menu? [no]: y
```

y を入力して、Enter キーを押します。

SNMP 設定ダイアログが開始されます。

ステップ 2　SNMP 管理をイネーブルにします。

y を入力して、Enter キーを押します。

```
Enable SNMP management? [no]: y
```

SNMP 管理をディセーブルにする場合は、このセクションの残りの部分を省略し、に進みます。ダイアログの残りは表示されません。SNMP 管理がディセーブルな場合、これらは無関係になるためです。

ステップ 3　SNMP GET コミュニティ名を設定します。

a. SNMP GET コミュニティ名を入力して、Enter キーを押します。

SCE 1000 内に常駐する SNMP エージェントが応答するのは、このコミュニティ ストリングを使用する GET 要求に対してだけです。

```
Enter SNMP GET community name:
```

このパラメータのデフォルト値は存在しません。

b. アクセス リストを割り当てて、この GET コミュニティを使用できる SNMP 管理ステーションを制限します。

数値（1 ～ 99）を入力するか、または「0」（すべての IP アドレスへのアクセスを許可）を入力して、Enter キーを押します。

```
Enter Access list number allowing access with this community string, use ‘0’ to allow
all:
```

ステップ 4　他の GET コミュニティ名を設定します。

GET コミュニティの最大数は 20 です。

a. さらにエントリを追加するには、デフォルトを受け入れないようにします。

```
Would you like to add another SNMP GET community? [no]:
```

y を入力して、Enter キーを押します。

b. ステップ 3 に従って最大 20 の SNMP GET コミュニティ名を入力します。

c. すべてのエントリを追加したら、デフォルトを受け入れます。

```
Would you like to add another SNMP GET community? [no]:
```

Enter キーを押して、デフォルトを受け入れます。

ステップ 5　SNMP SET コミュニティ名を設定します。

a. SNMP SET コミュニティ名を入力して、Enter キーを押します。

SCE 1000 内に常駐する SNMP エージェントが応答するのは、このコミュニティ ストリングを使用する SET 要求に対してだけです。

```
Enter SNMP SET community name:
```

このパラメータのデフォルト値は存在しません。

b. アクセス リストを割り当てて、この SET コミュニティを使用できる SNMP 管理ステーションを制限します。

数値（1 ～ 99）を入力するか、または「0」（すべての IP アドレスへのアクセスを許可）を入力して、Enter キーを押します。

```
Enter Access list number allowing access with this community string, use ‘0’ to allow
all:
```

ステップ 6　他の SET コミュニティ名を設定します。

a. さらにエントリを追加するには、デフォルトを受け入れないようにします。

```
Would you like to add another SNMP SET community? [no]:
```

y を入力して、Enter キーを押します。

b. ステップ 5 の説明に従って最大 20 の SNMP SET コミュニティ名を入力します。

c. すべてのエントリを追加したら、デフォルトを受け入れます。

```
Would you like to add another SNMP SET community? [no]:
```

Enter キーを押して、デフォルトを受け入れます。

ステップ 7　SNMP トラップ マネージャを設定します。

a. SNMP トラップ マネージャ メニューを開始します。

```
Would you like to configure SNMP trap managers? [no]: y
```

y を入力して、Enter キーを押します。

SNMP トラップ マネージャ ダイアログが開始します。

SNMP トラップ マネージャを設定しない場合、ダイアログは認証失敗トラップ ステータスに進みます（ステップ 9 を参照）。

b. トラップ マネージャの IP アドレスを設定します。

```
Enter SNMP trap manager IP address:
```

トラップ マネージャのコミュニティ ストリングを入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

c. トラップ マネージャのコミュニティ ストリングを設定します。

```
Enter SNMP trap manager community string:
```

トラップ マネージャのコミュニティ ストリングを入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

d. トラップ マネージャの SNMP バージョンを設定します。

```
Enter trap manager SNMP version:
```

トラップ マネージャの SNMP バージョン番号（1 または 2c）を入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

ステップ 8　他のトラップ マネージャを設定します。

トラップ マネージャの最大数は 20 です。

a. さらにエントリを追加するには、デフォルトを受け入れないようにします。

```
Would you like to add another SNMP trap manager? [no]:
```

y を入力して、Enter キーを押します。

b. ステップ 7 の説明に従って、最大 20 のトラップ マネージャを入力します。

c. すべてのエントリを追加したら、デフォルトを受け入れます。

```
Would you like to add another SNMP trap manager? [no]:
```

Enter キーを押して、デフォルトを受け入れます。

ステップ 9　認証失敗トラップ ステータスを設定します。

- 認証失敗トラップをディセーブルにするには、Enter キーを押します。
- 認証失敗トラップをイネーブルにするには、y を入力して、Enter キーを押します。

```
Enable the 'Authentication Failure' trap [no]:
```

ステップ 10　SCE エンタープライズ トラップ ステータスを設定します。

- SCE エンタープライズ トラップをディセーブルにするには、n を入力して、Enter キーを押します。
- SCE エンタープライズ トラップをイネーブルにするには、y を入力して、Enter キーを押します。

```
Enable the SCE enterprise traps []:
```

ステップ 11　システム管理者を指定します。

システム管理者の名前を入力して、Enter キーを押します。

このパラメータのデフォルト値は存在しません。

```
Enter system administrator contact name []:
```

例：

次の SNMP 設定例では、トラップ マネージャを 1 つ、GET コミュニティを 1 つ、SET コミュニティを 1 つ設定し、認証失敗トラップおよびすべてのエンタープライズ トラップをイネーブルにします。

```
Would you like to enter the SNMP configuration menu? [no]: y
Enable SNMP management? [no]: y
Enter SNMP GET community name[]: public
Enter Access list number allowing access with this community string, use '0' to allow all:
0
Would you like to add another SNMP GET community? [no]:
Enter SNMP SET community name[]: private
Enter Access list number allowing access with this community string, use '0' to allow all:
2
Would you like to add another SNMP SET community? [no]:
Would you like to configure SNMP trap managers? [no]: y
Enter SNMP trap manager IP address: 10.1.1.253
Enter SNMP trap manager community string: public
Enter trap manager SNMP version: 2c
Would you like to add another SNMP trap manager? [no]:
Enable the 'Authentication Failure' trap [no]: y
Enable SCE enterprise traps []: y
Enter system administrator contact name []: John Smith
```

ステップ 9：トポロジ依存パラメータの設定

- トポロジ依存パラメータについて
- 例

トポロジ依存パラメータについて

トポロジ設定メニューは、ネットワーク内の SCE 1000 の配置および動作モードに関連する一連の質問をガイドしながら表示します。ユーザ応答に基づいて、パラメータ値が設定されます。

希望どおり確実にシステムが機能するように、システムを設定する前に、各パラメータが正しい値であることを確認しておく必要があります（トポロジおよび関連パラメータの詳細については、「トポロジについて」を参照してください）。

3 つのトポロジ関連パラメータがあります。

- Connection mode：SCE 1000 の物理的な設置に基づいて、Inline または Receive-only に設定できます。
- Bypass state when the SCE 1000 is not operational (on-failure)：このパラメータは、SCE 1000 に障害が発生した場合に、システムがトラフィックを切断するか、バイパスするかを決定します。
- Status after reboot caused by fatal error or abnormal shutdown：このパラメータは、障害発生後、SCE 1000 が正常な動作状態に戻るかどうかを決定します。

下記の手順は、トポロジ設定に関するすべての質問の例です。実際には、1 つの設定における質問をここにすべて表示することはできません。ダイアログのこの部分は他のセクションのような線形ではなく、入力したパラメータ値に応じて質問が分岐するためです。

下記の例を参照して、各トポロジの手順を理解してください。

ステップ 1　トポロジ設定メニューを開始します。

```
Would you like to enter the Topology configuration menu? [no]: y
```

- プロンプトが表示されたら、パスワードを入力します。

  y を入力して、Enter キーを押します。

  トポロジ設定ダイアログを開始します。

ステップ 2　接続モードを指定します。

- inline 接続モードを定義するには、Enter キーを押します。
- receive-only 接続モードを定義するには、2 を入力して Enter キーを押します。

```
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]:
```

ステップ 3　障害時動作リンクを指定します。

- Bypass を指定するには、Enter キーを押します。
- Cutoff を指定するには、2 を入力して Enter キーを押します。

```
Enter On-failure behavior:
1- bypass
2- cutoff
Enter your choice [1]:
```

ステップ 4　異常起動後の SCE 1000 の管理ステータスを指定します。

- 異常起動後に Not-Operational ステータスを指定するには、Enter キーを押します。
- 異常起動後に Operational ステータスを指定するには、1 を入力して Enter キーを押します。

異常起動後の SCE の管理ステータスを入力します。

```
1- Operational
2- Not-Operational
Enter your choice [1]:
```

例

次に、さまざまなトポロジのトポロジ関連パラメータを設定する手順例を示します。各トポロジに適したパラメータ値の概要については、「トポロジについて」を参照してください。

- 「例 1：」（P.5-21）
- 「例 2：」（P.5-21）
- 「例 3：」（P.5-22）

例 1：

次に、外部スイッチを使用したトポロジのトポロジ設定例を示します。

- 障害時のリンク バイパス モード：Bypass
- 異常起動後の SCE の管理ステータス：Operational

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
Data collection for the system configuration is completed.
```

その他のすべてのパラメータ値は、自動的に割り当てられます。

例 2：

次に、非冗長 BITW（インライン）トポロジのトポロジ設定例を示します。

すべての値はシステムのデフォルト値であるため、応答で入力する必要はありません。行ごとに Enter キーを押すだけで済みます。

- Connection mode：Inline
- 非冗長トポロジの場合、障害時のリンク バイパスは Bypass になるため、トラフィックは引き続きリンク内を流れます。
- システム動作が再開され、SCE 1000 がリブートされると、SCE 1000 は動作を再開します
- （異常リブート後の管理ステータスは Operational です）。

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]:
Enter On-failure behavior:
1- Bypass
```

```
2- Cutoff
Enter your choice [1]:
Enter admin status of the SCe after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:
Data collection for the system configuration is completed.
```

例 3：

次に、冗長インライン トポロジのトポロジ設定例を示します。

- Connection mode：Inline
- 冗長トポロジの場合、障害時のリンク バイパスは Cutoff になるため、処理はバックアップ リンクに切り替えられます。
- システム動作が再開され、SCE 1000 がリブートされると、SCE 1000 は動作を再開します（異常リブート後の管理ステータスは Operational です）。

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
Enter On-failure behavior:
1- Bypass
2- Cutoff
Enter your choice [1]:2
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:
Data collection for the system configuration is completed.
```

ステップ 10：設定の完了および保存

設定全体を完了すると、システムによるエラー チェックが実行されます。エラーが検出されると、警告メッセージが表示されます。設定にエラーがない場合は、設定を適用し、保存することができます。

設定を完了して保存する手順は、次のとおりです。

ステップ 1　新しい設定を確認します。

データ収集の完了が通知されます。

新しい設定を適用する前に、設定全体を表示することを推奨します。

y を入力して、Enter キーを押します。

デフォルトは存在しません。

エラーがない場合は、ステップ 3 に進みます。

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]: y
```

ステップ 2　エラーを表示します（エラーが発生している場合）。

エラーが検出された場合は、エラーを表示できます。

Enter キーを押します。

```
Found errors in the new configuration, would you like to view them? [yes]:
The following errors were found:
Warning - RDR formatter destination 10.1.1.1 is not allowed in the IP access-class.
```

ステップ 3　設定を適用して保存します。

設定を適用して保存するかどうかが確認されます。

```
Apply and Save this configuration? [yes/no]:
```

設定を適用して保存するには、y を入力して、Enter キーを押します。

```
Setup procedure aborted, no configuration changes made.
```

設定を打ち切ると、ダイアログが終了します。

ステップ 4　設定の適用と保存を確認します。

エラーが存在しない場合は、操作ミスを防止するために、yes または no の確認応答の入力が求められます。

適切な応答（y または n）を入力して、Enter キーを押します。

```
The running configuration would be overwritten by the changes you have just entered, are
you sure? [yes/no]:
The selected action is carried out by the system.
```

選択したアクションが実行されます。

適用および保存アクションを承認しなかった場合は（no）、設定は打ち切られます。

```
Setup procedure aborted, no configuration changes made.
```

適用および保存アクションを承認した場合は（yes）、設定が適用および保存されます。

```
The new running configuration will be saved to the startup configuration.
```

ステップ 5　設定をリモート位置へ保存します。

設定を適用および保存した場合は、バックアップ コピーをリモート ステーションのファイルに保存することもできます。

```
Do you want to save a copy of the startup configuration file in a remote station? [no]:
```

設定をリモート ステーションに保存するには、y を入力して、Enter キーを押します。

FTP（ファイル転送プロトコル）パスの入力が求められます。

```
Enter a full FTP path of the remote destination:
```

ステップ 6　これで、SCE 1000 プラットフォームの初期設定手順は完了です。

設定の完了が通知されます。

```
Committing configuration...
Configuration completed successfully.
Saving configuration...
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
Done!
```

例

例 1：

次に、設定中に検出されたエラーのためにユーザが中止した設定の例を示します。

設定を中止する場合、確認は要求されません。エラーが存在しない場合は、設定を中止する前に確認が要求されます。

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]: n
Found errors in the new configuration, would you like to view them? [yes]: y
The following errors were found:
Warning - RDR formatter destination 10.1.1.1 is not allowed in the IP access-class.
Warning - default Gateway 10.1.1.1 is not allowed in the IP access-class.
Warning - IP Access list (1) conflicts with Telnet Access list (2) as follows:
Access list 2 permits all addresses while Access list 1 denies it.
Apply and Save this configuration? [yes/no]: n
Setup procedure aborted, no configuration changes made.
```

例 2：

次に、スタートアップ コンフィギュレーションおよび FTP サイトに設定を適用および保存した例を示します。

この例には示されていませんが、設定を適用する前に、必ず表示することを推奨します。

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]:
Apply and Save this configuration? [yes/no]: y
(New configuration would be displayed here)
The running configuration would be overwritten by the changes you have just entered, are
you sure? [yes/no]:y
The new running configuration will be saved to the startup configuration.
Do you want to save a copy of the startup configuration file in a remote station? [no]:y
Enter a full FTP path of the remote destination:
ftp://vk:vk@10.1.1.253/h:/copyofstartup.txt
Committing configuration...
Configuration completed successfully.
Saving configuration...
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
Done!
```

例 3：

次に、エラーが検出されなかったにもかかわらず、設定を中止した例を示します。

```
Data collection for the system configuration is completed.
Would you like to view the new configuration before it is applied? [yes/no]:
Apply and Save this configuration? [yes/no]: n
The changes you have just entered would be discarded, are you sure? [yes/no]:y
Setup procedure aborted, no configuration changes made.
```

管理インターフェイスの接続

SCE プラットフォームには、2 つの RJ-45 管理（MNG）ポートが装備されています。これらのポートにより、リモート管理コンソールから SCE プラットフォームへの LAN 接続が可能になります。これら 2 つのポートにより冗長管理インターフェイスを実現できるため、管理リンクのいずれかで障害が発生した場合でも、SCE プラットフォームへの管理アクセスが確保されます。

管理ポートのいずれか 1 つだけを使用する場合、目的のポートは単に LAN と直接接続されるだけです。両方の管理ポートを使用する場合は、スイッチを介して両方のポートを管理コンソールに接続する必要があります。この方法の場合、MNG ポートの IP アドレスは、現在アクティブである物理ポートに関わらず、常に同じになります。

ここでは、管理ポートのケーブル接続手順、および SCE 1000 とリモート管理ホスト間の接続テストの手順について説明します。

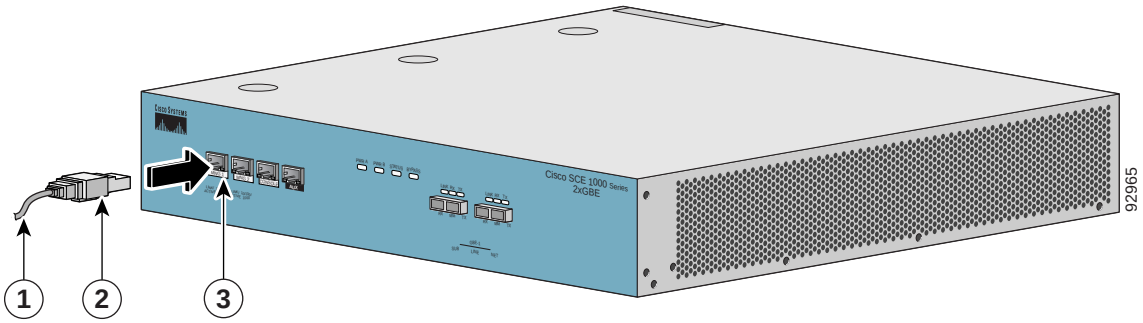
- 管理ポートのケーブル接続方法
- 管理インターフェイスの接続の確認方法

管理ポートのケーブル接続方法

SCE 1000 には MNG 1 と MNG 2 の 2 つの管理ポートがあります。

ステップ 1　付属のイーサネット ケーブル（RJ-45 コネクタを装備）を取り出して、SCE 1000 の前面パネルにある使用対象の MNG ポートに差し込みます（図 5-2 を参照）。

図 5-2　　管理ポートのケーブル接続



ステップ 2　イーサネット ケーブルの他端を管理ネットワークに接続します。

- 1 つの管理ポートしか使用しない場合、そのポートを直接 LAN に接続します。
- 両方の管理ポートを使用する場合、2 つともスイッチ経由で LAN に接続します。

カチッという音がして、RJ-45 コネクタが完全に挿入され、レセプタクルに固定されるまで、コネクタを押し込みます。ゆっくりとプラグを引っ張り、プラグがソケットに固定されているかどうかを確認します。

SCE 1000 管理ポートの LINK LED が点灯しない場合は、ケーブルを取り外して、モジュール ソケットにしっかりと装着し直します。ソケットからプラグを外す場合は、プラグ上部の高い部分を押し下げて、ラッチを解除します。カチッという音が聞こえれば、ラッチは解除されています。慎重にソケットからプラグを引き抜きます。

それでも SCE 1000 の管理ポートの LINK LED が点灯しない場合は、反対側の適切なネットワーク要素にケーブルが正しく接続されているかどうかを確認します。

管理インターフェイスの接続の確認方法

SCE 1000 プラットフォームに電源を投入したあと、SCE 1000 とリモート管理ホスト間で接続が確立されたかを確認するためテストを行ってください。SCE 1000 プラットフォームに電源が投入されていない場合は、SCE 1000 プラットフォームを起動してから、この手順を実行します。

ステップ 1　適切な Mng ポートおよびネットワークにケーブルを接続したら、関連する Mng ポートの LED を調べます。

MNG LED は、LINK/ACTIVE と 10/100/1000 の 2 つあります（前面パネルを参照）。

この時点で、LINK/ACTIVE LED がグリーンであるかを調べます。

10/100/1000 LED の状態は、イーサネット ネットワーク設定によって変わります。

グリーンは 100 Mbps を、「Off」は 10 Mbps を示します。

ステップ 2　接続をテストします。リモート管理に使用するホストから SCE 1000 に ping を実行します。ping を実行するには、ping の後に SCE 1000 の IP アドレスを入力して、Enter キーを押します（次の例を参照）。

（注）　リモート管理ホスト（MNG ポート接続）から実行するのは、上記のステップだけであることに注意してください。

これにより、指定されたステーションと管理ポート間にアクティブな接続が存在することが確認されます。

ping プログラムは IP アドレスにエコー要求パケットを送信し、応答を待機します。ping の出力を確認することで、パス/ホストの信頼性、パス上の遅延、およびホストへの到達可能性やホストの機能を評価することができます。

例：

次に、ターゲット IP アドレスが 10.1.1.201 である場合の一般的な ping 応答を示します。

```
C:¥>ping 10.1.1.201
pinging 10.1.1.201 ...
PING 10.1.1.201: 56 data bytes
64 bytes from host (10.1.1.201): icmp_seq=0. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=1. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=2. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=3. time=0. ms
----10.1.1.201 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```