



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

この章では、**SCE 2000** 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 ウィザードを通して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。



(注)

カスケード型システムを設置する場合は、規定の手順に従うことがきわめて重要です。

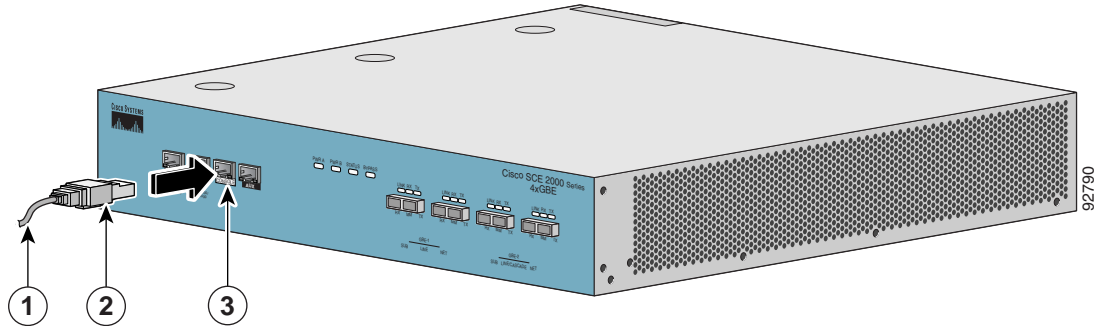
- [ローカル コンソールのセットアップ方法 \(p.5-2\)](#)
- [初期システム設定 \(p.5-4\)](#)
- [管理インターフェイスの接続 \(p.5-30\)](#)

ローカル コンソールのセットアップ方法

SCE 2000 をリモート管理する場合でも、まずローカル コンソールに装置を接続し、SCE 2000 の初期設定を行う必要があります。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、初期システム設定の実行を求めるプロンプトが表示されます。

ここでは、セットアップユーティリティを使用して SCE 2000 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 2000 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 2000 ポート パラメータは固定であり、設定できません。

手順の概要

1. SCE 2000 付属の RS-232 シリアル ケーブルを、SCE 2000 の前面パネルにある CON ポートに差し込みます。
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。
3. ローカル端末が、固定された SCE 2000 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。
4. ローカル端末にシスコ ログが表示され、設定ダイアログが開始するまで、**Enter** キーを数回押します。
5. **y** を入力して、**Enter** キーを押します。

手順の詳細

-
- ステップ 1** SCE 2000 付属の RS-232 シリアル ケーブルを、SCE 2000 の前面パネルにある CON ポートに差し込みます。

「カチッ」という音が聞こえて、RJ-45 コネクタ (RS-232 シリアル ケーブルに装着) 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。

- 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、固の SCE 2000 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 ログが表示され、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

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、ほかの値を定義することができます。

入力直後に有効となる時間設定を除き、新しい設定はユーザによる承認ダイアログが終了した場合のみ、適用および保存されます。したがって、設定ダイアログが打ち切られた場合、時間設定（入力された場合）以外の設定は変更されません。

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 Service Control Engine (SCE) 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 セットアップコマンドパラメータ

| パラメータ | 定義 |
|----------------------------|----------------------------------------------------------------------------------------------|
| IP アドレス | SCE 2000 の IP アドレス |
| subnet mask | SCE 2000 のサブネット マスク |
| default gateway | デフォルト ゲートウェイ |
| Hostname | SCE 2000 を識別するために使用される最大 20 字の文字列最大 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 | |
| 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 |

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 |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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) |
| RDR フォーマッタ送信先の設定 | |
| IP address | RDR フォーマッタ送信先の IP アドレス |
| 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。 <ul style="list-style-type: none"> 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 (maximum 20 per list) | 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 の設定 | |
| SNMP agent status | SNMP 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 (maximum 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 |
| トポロジの設定 | |
| Connection mode | SCE 2000 がインライン トポロジで取り付けられているか、または光スプリッタを使用して受信専用トポロジで取り付けられているか。 |
| type of deployment | 2 台の SCE 2000 がカスケードポートを通して接続された、カスケードトポロジであるか。または、単一プラットフォームトポロジであるか。 |

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 |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| physically connected link (カスケードトポロジの場合のみ) | カスケード配置の場合、この SCE 2000 が配置されたリンクのインデックスを設定します。 SCE 2000 のオプションは link-0 または link-1 です。 単一 SCE 2000 プラットフォーム配置の場合、1 つの SCE 2000 が両方のリンク上に配置されているため、このパラメータは関連しません。この場合、ポート 1 ~ 2 に接続されたリンクがデフォルトで link-0 になり、ポート 3 ~ 4 に接続されたリンクがデフォルトで link-1 になります。 |
| priority (カスケードトポロジの場合のみ) | カスケードトポロジの場合、この SCE 2000 がプライマリとセカンダリのいずれの SCE 2000 であるか。 |
| on-failure behavior (インライン接続モードの場合のみ) | この SCE 2000 がインラインで配置されている場合、障害後にリンクをバイパスするか、または切断するか。 |
| Admin status of the SCE 2000 after abnormal boot | 障害による再起動が発生したあとに、 SCE 2000 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。IP アドレス設定ダイアログの末尾にジャンプしようとする、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ず。メニューを省略するには、質問に「**n**」と応えます。
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 : 初期設定の方法

次に示す、**SCE 2000** 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。

手順の概要

1. 現在の IP アドレスが表示されます。
2. 現在のサブネット マスクが表示されます。
3. 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。

手順の詳細

ステップ 1 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 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なくなり、明示的に入力する必要があります。

```
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 : ホスト名の設定方法

を識別するために使用するホスト名。ホスト名は **SCE 2000** を識別するのに使用されます。このホスト名は、CLI (コマンドライン インターフェイス) プロンプトの一部として表示され、MIB-II オブジェクト `sysName` の値としても戻されます。

最大長は、20 文字です。

デフォルトのホスト名は、**SCE 2000** です。

ステップ 1 現在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。

例 :

```
Enter hostname [SCE 2000]:
```

ステップ 3 : パスワードの設定方法

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 2000** 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。

- 最小長 — 4 文字
- 最大長 — 100 文字
- 英文字で開始
- 出力可能な文字のみ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。

手順の概要

1. デフォルト User パスワードが表示されます。
2. デフォルト Admin パスワードが表示されます。
3. デフォルト Root パスワードが表示されます。
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。

手順の詳細

ステップ 1 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、目的の文字列を入力し、**Enter** キーを押します。

ステップ 2 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、目的の文字列を入力し、**Enter** キーを押します。

ステップ 3 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、目的の文字列を入力し、**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 : 時間の設定方法

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、以下が含まれています。

- 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。

手順の概要

1. 時間設定メニューを開始します。
2. タイムゾーンの省略形を入力し、**Enter** キーを押します。
3. UTC からのオフセット (分) を入力し、**Enter** キーを押します。
4. 日時が正しい場合は、次のステップに進みます。
5. SNTP 設定メニューを開始するかどうかを確認されます。
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。
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。
8. SNTP ユニキャストサーバの IP アドレスを入力できます。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。

手順の詳細

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。

時間設定ダイアログが開始します。

ステップ 2 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 (分) を入力し、**Enter** キーを押します。

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

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を確認されます。

```
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]:
```

ステップ4 日時が正しい場合は、次のステップに進みます。

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するかどうかを確認されます。

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 の設定方法](#)」(p.5-12) 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。
- 値を変更するには、目的の秒数 (64 ~ 1024) を入力して、**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 アドレスを入力できます。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 の設定方法

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。

手順の概要

1. DNS 設定メニューを開始します。
2. DNS lookup をイネーブルまたはディセーブルにします。
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。
4. 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。
5. ドメインサーバは 3 つまで設定できます。
6. 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。

手順の詳細

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、「[ステップ 6 : RDR フォーマッタ送信先の設定方法](#)」(p.5-14)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 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 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方法

SCE 2000 は Raw Data Records (RDR) を、RDR フォーマッタを介して外部収集システムに渡します。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。

手順の概要

1. RDR フォーマッタ設定メニューを開始します。
2. 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。
3. 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。

手順の詳細

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 : ACL の設定

SCE 2000 に ACL を設定して、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。

ACL の設定は、2 つの手順で構成されています。

1. ACL 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 (「[ステップ 9 : トポロジ依存パラメータの設定方法](#)」 [p.5-23] を参照)。

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。

ACL の設定方法

SCE 2000 に ACL を設定して、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。

ACL の設定は、2 つの手順で構成されています。

1. ACL 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 (「[ステップ 9 : トポロジ依存パラメータの設定方法](#)」 [p.5-23] を参照)。

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、次の表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

| 初期の IP アドレス / ワイルドカード ビット範囲 | ワイルドカード ビットの範囲 | 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順は重要です。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、ACL 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することはできません。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 ACL 内のどのエントリも接続と一致しない場合、または ACL が空の場合、デフォルトアクションは *deny* です。

手順の概要

1. ACL 設定メニューを開始します。
2. ACL 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。
3. 設定する ACL 数 (1 ~ 99) を入力して、**Enter** キーを押します。
4. 選択したリストにエントリを追加します。
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。
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.5-15] 参照)。
7. ACL の最大エントリ数は 20 です。
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を確認されます。最大 99 の ACL を定義できます。
9. 適切な ACL を割り当てて、**SCE 2000** に対する IP アクセスを制限します。
10. 適切な ACL を割り当てて、**SCE 2000** に対する Telnet アクセスを制限します。

手順の詳細

ステップ 1 ACL 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。

ACL 設定ダイアログが開始します。

ステップ 2 ACL 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
```

ACL の作成や編集を行わない場合は、「[ステップ 9: トポロジ依存パラメータの設定方法](#)」[p.5-23]に進みます。

ステップ 3 設定する ACL 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。

```
Does this entry permit access? [yes]:
```

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。

ACL にすべての IP アドレスを含めるには、「any」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.5-15] 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 と 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を確認されます。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**

説明に従って最大 20 の IP アドレスを新しい ACL に入力します。

- 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 2000** 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 2000** 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 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 ACL 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。
- Telenet 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]: 1Enter 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 の設定方法

SCE 2000 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。デフォルトでは、SNMP は SCE 2000 上でディセーブルです。

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 2000 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)

手順の概要

1. SNMP 設定メニューを開始します。
2. SNMP 管理をイネーブルにします。
3. SNMP GET コミュニティ名を入力して、**Enter** キーを押します。
4. 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。
5. GET コミュニティの最大数は 20 です。
6. SNMP SET コミュニティ名を入力して、**Enter** キーを押します。
7. 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。

8. SET コミュニティの最大数は 20 です。
9. SNMP トラップ マネージャ メニューを開始します。
10. トラップ マネージャの IP アドレスを入力して、**Enter** キーを押します。
11. トラップ マネージャのコミュニティ スtring を入力して、**Enter** キーを押します。
12. 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。
13. トラップ マネージャの最大数は 20 です。
14. 認証失敗トラップ ステータスを設定します。
15. SCE エンタープライズ トラップ ステータスを設定します。
16. システム管理者の名前を入力して、**Enter** キーを押します。

手順の詳細

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、[「ステップ 9: トポロジ依存パラメータの設定方法」](#)[p.5-23]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 コミュニティ名を入力して、**Enter** キーを押します。

SCE 2000 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tring を使用する GET 要求に対してのみです。

```
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。

ステップ 4 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 5 GET コミュニティの最大数は 20 です。

- 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 SNMP GET community? [no]:y
```

- 説明に従って最大 20 の 20 SNMP GET コミュニティ名を入力します。
- 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 SNMP GET community? [no]:
```

ステップ 6 SNMP SET コミュニティ名を入力して、**Enter** キーを押します。

SCE 2000 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tring を使用する SET 要求に対してのみです。

```
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。

ステップ 7 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 8 SET コミュニティの最大数は 20 です。

- 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 SNMP SET community? [no]:y
```

- ステップ 6 とステップ 7 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。
- 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 SNMP SET community? [no]:
```

ステップ 9 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 14 を参照)。

ステップ 10 トラップ マネージャの IP アドレスを入力して、**Enter** キーを押します。

```
Enter SNMP trap manager 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 11 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。

Enter SNMP trap manager community string:

ステップ 12 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。

Enter trap manager SNMP version:

ステップ 13 トラップ マネージャの最大数は 20 です。

- 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 SNMP trap manager? [no]:y
- ステップ 10 から 12 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。
- 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 SNMP trap manager? [no]:

ステップ 14 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 15 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 16 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: 0Would 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方法

トポロジ設定メニューは、ネットワーク内の **SCE 2000** の配置および動作モードに関連する一連の誘導型質問形式です。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](#)」 [p.3-1] を参照)。



(注)

すべてのトポロジ依存パラメータに値が要求されるわけではありません。一部のトポロジに適用されないパラメータがあるためです。

6 つのトポロジ関連パラメータがあります。

- **Connection mode** — **SCE 2000** の物理的な設置に基づいて、次のいずれかに設定できます。
 - Inline
 - Receive-only
- **Type of deployment** — 実際の配置に基づいて、次のいずれかに設定できます。
 - Single-SCE Platform — 単一 **SCE 2000** が 1 つまたは 2 つの GBE リンク上に配置されます。
 - Cascade — 2 つのカスケード接続された **SCE 2000** が 2 つの GBE リンク上に配置され、完全な冗長ソリューションとして機能します。
- **Physically connected link (カスケード トポロジの場合のみ)** — カスケード トポロジの場合、ユーザは各リンクにインデックスを割り当てる必要があります。このインデックスは、リンクごとのサービスを識別するために使用されます。

単一 SCE プラットフォーム配置の場合、ユーザはリンクのインデックスを変更できません。各インデックスは、次のようになります。

- link-0 — ポート 1 およびポート 2 に接続されたリンク
- link-1 — ポート 3 およびポート 4 に接続されたリンク

- カスケード配置の場合、どのリンクがどの **SCE 2000** に接続されているのかを定義する必要があります。インデックスは **SCE 2000** ごとに異ならなければなりません。この場合、ユーザは次のいずれかを選択することができます。

- Link-0 — この **SCE 2000** に接続されたリンクが 0 として識別されます。
- Link-1 — この **SCE 2000** に接続されたリンクが 1 として識別されます。

- **Priority (カスケード トポロジの場合のみ)** — カスケード トポロジの場合、このパラメータは、「アクティブ選定」手順においてアクティブ **SCE 2000** として選択される **SCE 2000** を決定します。この決定が行われるのは、両方の **SCE 2000** が同時に起動した場合のみです。1 台の **SCE 2000** が起動している場合に、もう 1 台を起動すると、機能中のプラットフォームが自動的にアクティブに選択され、別のプラットフォームがスタンバイになります。このパラメータは、次のいずれかに設定できます。
 - Primary
 - Secondary
- **On-Failure behavior** — 障害時または再起動時の **SCE 2000** の動作を決定します。**SCE 2000** の障害時または再起動時は、次のいずれかのリンク モードを選択できます。
 - Bypass — 内部バイパス カードを使用して、トラフィックがバイパスされます。
 - Cutoff — リンクが強制的にダウンします。
- **Admin status after abnormal reboot** — このパラメータは、異常（ユーザが要求しない）起動後に、**SCE 2000** が完全に動作可能なモードに戻るのか、あるいは、動作不能モード（**SCE 2000** が障害モードとして動作する）にとどまるのかを決定します。このパラメータは、次のいずれかに設定できます。
 - Operational（動作可能）
 - Non-operational（動作不能）

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。実際は、配置されたトポロジによっては、特定の設定に対する質問が一部表示されないことがあります。

下記の例を調べて、各トポロジの手順を理解してください。

手順の概要

1. トポロジ設定メニューを開始します。
2. 接続モードを指定します。
3. 配置タイプを指定します。
4. 物理接続リンクのインデックスを指定します。
5. **SCE 2000** のプライオリティを指定します。
6. 障害時動作リンクを指定します。
7. 異常起動後の **SCE 2000** のステータスを指定します。

手順の詳細

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
```

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が開始されます。

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 配置タイプを指定します。

- **Single-SCE Platform** 配置を指定するには、**Enter** キーを押します。
- **Cascade** 配置を指定するには、**y** を入力して、**Enter** キーを押します。

```
Is this a cascade deployment? [no]:
```

ステップ 4 物理接続リンクのインデックスを指定します。

- **link-0** を指定するには、**Enter** キーを押します。
- **link-1** を指定するには、**1** を入力して、**Enter** キーを押します。

```
Enter Physically connected link:
0- link-0
1- link-1
Enter your choice [0]:
```

ステップ 5 SCE 2000 のプライオリティを指定します。

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

```
Enter SCE 2000 priority:
1- primary
2- secondary
Enter your choice [1]:
```

ステップ 6 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 7 異常起動後の SCE 2000 のステータスを指定します。

- 異常起動後に **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 **Not-Operational** ステータスを指定するには、**2** を入力して、**Enter** キーを押します。

```
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]:
```

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。

例1:

次に、光スプリッタを使用した非冗長トポロジの設定例を示します。単一の **SCE 2000** が、1 つまたは2 つの GBE リンクと受信専用接続モードで接続されています。

```
Would you like to enter the Topology configuration menu? [no]: y
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 2
Is this a cascade deployment? [no]: no
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]: 1
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:

次に非冗長インライン トポロジのトポロジ設定例を示します。このトポロジでは、単一の **SCE 2000** が1 つまたは2 つの GBE リンクに接続されます。

インライン接続モードが指定されている場合、ユーザは障害時のリンク動作を指定する必要があります。

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

次に、冗長インライン トポロジにおけるセカンダリ **SCE 2000** のトポロジ設定例を示します。このトポロジでは、2 つの **SCE 2000** が、カスケード GBE ポート (ポート3 および4) を介してカスケード接続されます。各 **SCE 2000** は1 つの GBE リンクの両側 (サブスクリバ/ネットワーク) にインライン接続されます。

この場合、ユーザは物理接続リンクのインデックス (この例では link-0)、**SCE 2000** のプライオリティ、および障害時のリンク動作を指定する必要があります。

```
Would you like to enter the Topology configuration menu? [no]: y
Enter Connection mode:
1- inline
2- receive-only
Enter your choice [1]: 1
Is this a cascade deployment ? [no]: yes
Enter Physically connected link:
0- link-0
1- link-1
Enter your choice [0]: 0
Enter SCE 2000 priority:
1- primary
2- secondary
```

```
Enter your choice [1]: 2
Enter On-failure behavior:
1- bypass
2- cutoff
Enter your choice [1]: 1
Enter admin status of the SCE after abnormal boot:
1- Operational
2- Not-Operational
Enter your choice [1]: 1
Data collection for the system configuration is completed.
```

ステップ 10 : 設定の完了と保存の方法

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。

手順の概要

1. データ収集の完了が通知されます。
2. エラーが検出された場合は、エラーを表示できます。
3. 設定を適用して保存するかどうかを確認されます。
4. エラーが存在しない場合は、操作ミスを防ぐために、**yes** または **no** の確認応答の入力が求められます。
5. 設定を適用および保存した場合は、設定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。
6. 設定の完了が通知されます。

手順の詳細

ステップ 1 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するかどうかを確認されます。

```
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。
- 設定を適用または保存せずに設定手順を打ち切るには（エラーが存在する場合に推奨）、**n** 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 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]:
```

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（**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 設定を適用および保存した場合は、設定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 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 1 :

次に、設定中に検出されたエラーのためにユーザが打ち切った設定の例を示します。

設定を打ち切る場合、確認は要求されません。エラーが存在しない場合は、設定を打ち切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
(新しい設定がここに設定される)
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、設定を打ち切った例を示します。

```
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 つのみを使用する場合、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 2000 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 (p.5-30)
- 管理インターフェイスの接続確認の方法 (p.5-31)

管理ポートのケーブル接続方法

SCE 2000 には、2つの管理ポート (Mng1 および Mng2) が装備されています。

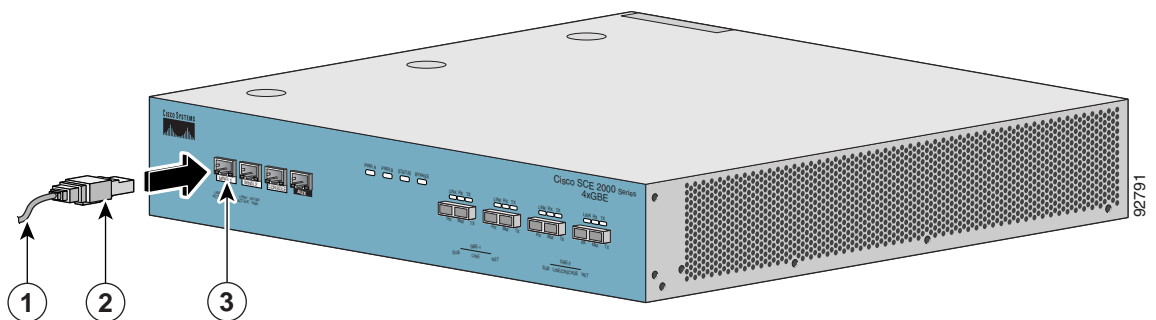
手順の概要

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 2000 の前面パネル上の MNG ポートに差し込みます (次の図を参照)。
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。

手順の詳細

- 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 2000 の前面パネル上の MNG ポートに差し込みます (次の図を参照)。

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。

- 管理ポートのいずれか 1 つのみが使用される場合 — ポートを LAN に直接接続します。
- 両方の管理ポートが使用される場合 — 両方のポートをスイッチを介して LAN に接続します。

カチッという音が聞こえて、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 2000 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 2000** の管理ポートの LINK LED が点灯しない場合は、ケーブルが反対側の適切なネットワーク要素に正しく接続されているか確認します。

管理インターフェイスの接続確認の方法

SCE 2000 プラットフォームに電源を投入したら、**SCE 2000** とリモート管理ホスト間で接続が確立されたかどうか確認テストを実行します。**SCE 2000** プラットフォームに電源が投入されていない場合は、**SCE 2000** 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。

手順の概要

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。
2. 接続をテストします。リモート管理を使用するホストから **SCE 2000** に ping を実行します。そのためには、ping および **SCE 2000** 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）。

手順の詳細

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。

2つの Mng LED があります — LINK/ACTIVE および 10/100/1000 です（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。リモート管理を使用するホストから **SCE 2000** に ping を実行します。そのためには、ping および **SCE 2000** 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、上記のステップのみ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 出力を使用すると、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
```