CHAPTER 3

管理ネットワークへの接続とセキュア アクセス

この章では、管理ネットワークへの Cisco Nexus 7000 シリーズ スイッチの接続および CLI へのセキュア アクセスについて、Cisco NX-OS で推奨するベスト プラクティスについて説明します。

この章で説明する内容は、次のとおりです。

- 「アウトオブバンド管理の接続」
- 「コンソール ポートの設定」
- 「VTY ポートの設定」
- 「スーパーバイザ管理ポートの設定」
- 「アクセス リスト ロギング」
- 「スーパーバイザ CMP ポートの設定」

アウトオブバンド管理の接続

Nexus 7000 は、通常、異なる接続方式の組み合わせを使用して管理されます。ネットワーク管理者は、CLI にアクセスし、SNMP、Syslog、NTP などの IP 管理プロトコルを使用するシャーシを管理することができます。次の表に、Nexus 7000 シャーシの管理に使用可能な異なる接続方式を示します。アウトオブバンド方式を組み合わせて使用し、実稼動トラフィックから管理トラフィックを分離して、シャーシを管理することを推奨します。このアプローチでは、悪意のあるユーザから発信されたか、不注意によって発生した過剰な購読トラフィックによる、Denial of Service（DoS; サービス拒絶）攻撃を防ぎ、セキュリティが強化されます。

スーパーバイザ モジュール CMP ポートが提供する機能について理解することが重要です。CMP ポートによって、停電時の CLI コンソール アクセスが提供され、SSHv2 または Telnet を使用して IP ネットワークを経由してスーパーバイザ モジュールにアクセスできます。CMP ポートを使用すると、管理者は、コンソールに接続し、コンソールをモニタリングし、スーパーバイザ モジュールまたはシャーシ全体をリロードできます。SNMP または NTP のような IP プロトコルのインバンド管理機能は提供されません。

表 3-1　ポート タイプおよびモジュール タイプの接続オプション

接続オプション	ポート タイプ	モジュールのタイプ
アウトオブバンド（RS-232 シリアル CLI）	コンソール ポート（推奨）	スーパーバイザ
	補助ポート	スーパーバイザ

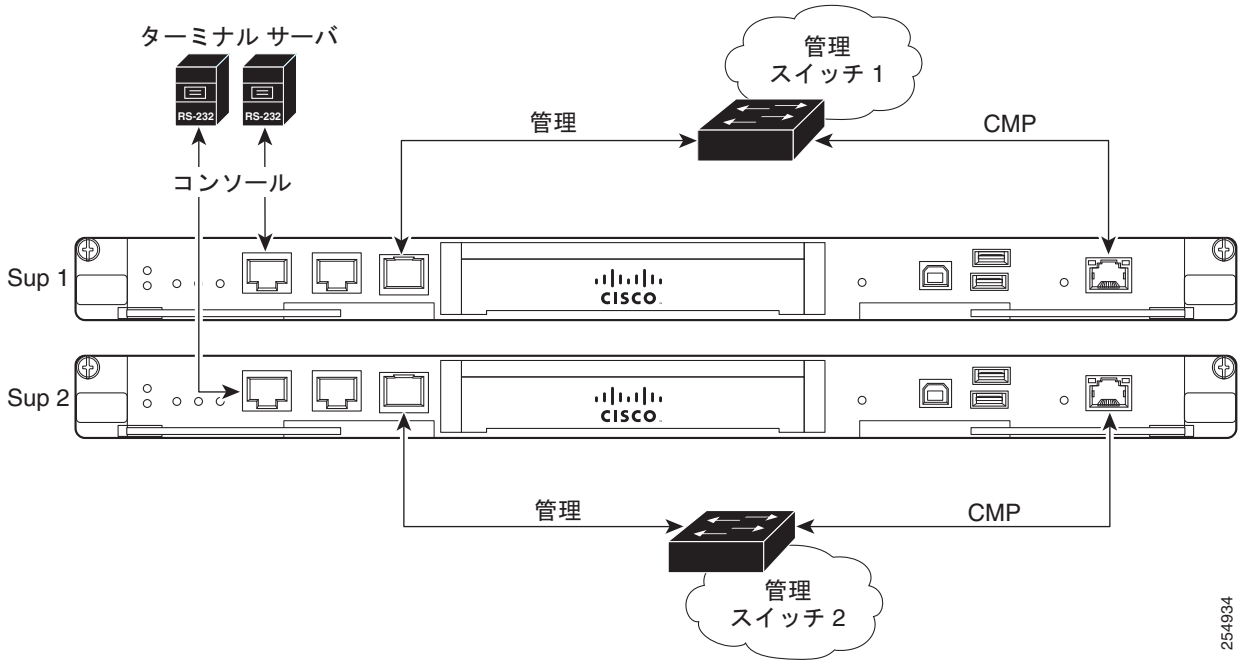
表 3-1　ポート タイプおよびモジュール タイプの接続オプション（続き）

接続オプション	ポート タイプ	モジュールのタイプ
アウトオブバンド（SSH/Telnet CLI）	Connectivity Management Port（CMP）推奨	スーパーバイザ
アウトオブバンド（SSH/Telnet CLI および IP Mgmt）	管理ポート（mgmt0）推奨	スーパーバイザ
インバンド（SSH/Telnet CLI および IP Mgmt）	イーサネット/ループバック/SVI など	I/O モジュール

2 つのスーパーバイザ モジュールで Nexus 7000 への接続を失う可能性を抑制するには、スーパーバイザ モジュールごとにコンソール ポート、CMP、および管理ポートを接続することを推奨します。

コンソールポートを 2 つの異なるターミナル サーバおよびスーパーバイザ CMP に接続し、mgmt0 ポートを冗長アウトオブバンド イーサネット ネットワークに接続して、可用性およびセキュリティを改善する必要があります。次の図に、冗長スーパーバイザ モジュールでシャーシごとに必要な接続を示します。

図 3-1　冗長スーパーバイザ モジュールでのシャーシごとの接続



（注）　このアウトオブバンド管理の設計では、イーサネット、ループバック、ポート チャネル、SVI などの I/O モジュール ポートに設定されている IP アドレスがある場合、インバンド管理プロトコルを拒否するよう、CoPP ポリシーを変更する必要があります。

（注）　これは単なる基本例です。冗長ネットワーク管理の設計は、このマニュアルに記載の範囲を超える場合があります。

コンソール ポートの設定

ここでは、コンソール ポートで Cisco NX-OS が推奨するベスト プラクティスについて説明します。

Exec-Timeout

導入：Cisco NX-OS Release 4.0(1)

コンソール ポートでは、指定された時間の間アイドル状態の管理者が自動的にログアウトするよう、タイムアウトを設定する必要があります。コンソールの **exec-timeout** は、デフォルトでディセーブルです。ほとんどのセキュリティ ポリシーでは、通常、10 ～ 15 分のタイムアウトが受け付けられます。

```
n7000(config)# line console
n7000(config-console)# exec-timeout 10
```

ポート速度

導入：Cisco NX-OS Release 4.0(1)

コンソール ポートの速度（ボー レート）は、接続されているターミナル サーバでサポートされている最大値まで増やす必要があります。コンソールの速度は、デフォルトで 9,600 bps で、最大で 115,200 bps まで設定できます。最大値によって、コンソール ポートに表示されるデータの速度が大きくなり、ユーザー エクスペリエンスが改善されます。

```
n7000(config)# line console
n7000(config-console)# speed 115200
```

VTY ポートの設定

ここでは、SSHv2 セッションおよび Telnet セッションで使用される VTY（ターミナル）ポートの設定に関する、Cisco NX-OS 推奨のベスト プラクティスについて説明します。

Exec-Timeout

導入：Cisco NX-OS Release 4.0(1)

VTY ポートでは、指定された時間の間アイドル状態のユーザが自動的にログアウトするよう、タイムアウトを設定する必要があります。VTY の **exec-timeout** は、デフォルトでディセーブルです。ほとんどのセキュリティ ポリシーでは、通常、10 ～ 15 分のタイムアウトが受け付けられます。

```
n7000(config)# line vty
n7000(config-line)# exec-timeout 10
```

セッションの制限

導入：Cisco NX-OS Release 4.0(1)

VTY セッションの限度では、SSHv2 セッションの数、Telnet セッションの数、または両方のセッションを同時にアクティブにできる数が決定されます。session-limit では、デフォルトで 32 のアクティブ セッションが認められます。セキュリティを強化するには、5 セッションまたは 10 セッションなどの実用的な制限まで削減する必要があります。

```
n7000(config)# line vty
n7000(config-line)# session-limit 5
```

アクセス リスト

導入：Cisco NX-OS 5.1(1)

セキュリティを強化するには、特定のソースおよび宛先 IP アドレスに対する SSH アクセスおよび Telnet アクセスを制限することによって、アクセス クラスを VTY ポートに適用する必要があります。VTY ポートに設定するアクセス クラスは、インバンドまたはアウトオブバンドの管理手順の使用時に適用できます。access-class はトラフィックの方向ごとに設定されます。**in** はインバンド セッションに適用され、**out** はアウトバンド セッションに適用されます。

統計は、アクセス リスト **statistics per-entry** でイネーブルにすることができます。次に、特定のサブネットから現在の VDC に設定されているすべての IP アドレスへの SSH トラフィックを許可する基本ポリシーの例を示します。すべてのトラフィックは、access-class が VTY ポートに適用され、関連付けられている access-list が設定から削除される場合に、許可されます。

```
n7000(config)# ip access-list vty-acl-in
n7000(config-acl)# permit tcp x.x.x.x/24 any eq 22

n7000(config)# line vty
n7000(config-line)# ip access-class vty-acl-in in
```

スーパーバイザ管理ポートの設定

ここでは、スーパーバイザ モジュール mgmt0 ポートで Cisco NX-OS が推奨するベスト プラクティスについて説明します。

アクセス リスト

導入：Cisco NX-OS Release 4.0(1)

セキュリティを強化するには、Nexus 7000 に設定されている特定の管理プロトコル宛ての特定のソース ホスト/サブネット アドレスへのアクセスを制限することによって、インバンド アクセス リストでスーパーバイザ モジュール mgmt0 ポートを設定する必要があります。access-list エントリは、イネーブルにされている管理ポートによって異なります。ACL コマンド **statistics per-entry** が設定されている場合、access-list 統計は ACL エントリごとに追跡できます。access-list が mgmt0 ポートに適用されるときに、スーパーバイザ モジュール CPU によって access-list の処理が実行されます。

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# statistics per-entry
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq snmp
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs
n7000(config-acl)# permit udp x.x.x.x/x b.b.b.b/32 eq ntp

n7000(config)# interface mgmt0
n7000(config-if)# ip access-group mgmt0-access in
n7000(config-if)# ip address b.b.b.b/xx
```

アクセス リスト ロギング

導入：Cisco NX-OS Release 5.0(2a)

アクセス リストは、**log** キーワードを使用して mgmt0 ポートに設定し、エントリごとに追加データを収集できます。access-list ロギング キャッシュを表示して、記録された access-list エントリから収集されるデータを監査できます。

```
n7000(config)# ip access-list mgmt0-access
n7000(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22 log

n7000# show log ip access-list cache
Source IP        Destination IP     S-Port  D-Port    Interface   Protocol          Hits
------------------------------------------------------------------------------------------
x.x.x.x          x.x.x.x             60741   22        mgmt0      (6)TCP            136

Number of cache entries: 1
------------------------------------------------------------------------------------------
```

スーパーバイザ CMP ポートの設定

ここでは、スーパーバイザ モジュール Connectivity Management Port（CMP）の設定に Cisco NX-OS が推奨するベスト プラクティスについて説明します。

アクセス リスト

導入：Cisco NX-OS Release 4.0(1)

セキュリティを強化するには、CMP ポートでイネーブルに設定されている特定の管理プロトコル宛ての特定のソース ホスト/サブネット アドレスへのアクセスを制限することによって、アクセス リストでスーパーバイザ モジュール CMP ポートを設定する必要があります。SSHv2 は、通常、CMP ポートでのみ必要なプロトコルです。**attach cmp** コマンドを使用して、access-list で CMP ポートを設定します。

```
n7000-cmp5(config)# ip access-list cmp-access
n7000-cmp5(config-acl)# permit tcp x.x.x.x 0.0.0.0 range 1024 65535 b.b.b.b 0.0.0.0 range 22 22

n7000-cmp5(config)# interface cmp-mgmt
n7000-cmp5(config-if)# ip address b.b.b.b/xx
n7000-cmp5(config-if)# ip access-group cmp-access in
```

（注）　CMP ポートの access-list の構文は、Cisco NX-OS の access-list の構文と異なります。