CHAPTER 5

ハードウェア バイパス モード

この章では、Cisco ISA 3000 Industrial Security Appliancesがバイパス モードで動作する方法について説明します。バイパス モードは、銅線ポートが電源喪失時にCisco ISA 3000をバイパスし、エンドツーエンド接続を継続できることと定義されます。この機能はプログラム可能です。システムが起動したら、ソフトウェアにより、バイパス モードがオフになります。

この章の構成は、次のとおりです。

- ハードウェア バイパスのシナリオ（5-1ページ）
- ハードウェア バイパスとファイアウォール モードの互換性（5-2ページ）
- ポートのバイパス LED（5-3ページ）
- イベント メッセージ（5-3ページ）
- CLI インターフェイス コマンド（5-3ページ）

ハードウェア バイパスのシナリオ

ハードウェア バイパス機能では、停電時にトラフィックが次のインターフェイス ペア間で自由に通過できます。

- ギガビット イーサネット 1/1 と 1/2
- ギガビット イーサネット 1/3 と 1/4

ハードウェア バイパス動作は設定可能です。詳細については、お使いのソフトウェア バージョンの ASA 一般操作の構成ガイドを参照してください。

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

インターフェイスのペアごとに、次のイベント時のハードウェア バイパス動作を設定できます。

- 電源切断
- 運用システムへの電源供給

ハードウェア バイパスは手動でもイネーブル、またはディセーブルにできます。

電源切断とは、電源の再投入によるCisco ISA 3000のリロードまたは再起動、または完全な電源喪失を意味します。ISA で設定されていた場合、電源切断により ISA のデータ ポートがバイパスされます。電源投入後にもハードウェア バイパスが続行するように設定すると、すべてのトラフィックが内部ポートから外部ポートに、またその逆に通過できます。電源が復旧すると、システム ソフトウェアがシステムの起動の進行状況をモニターし、システムの準備ができた（ファイアウォールによるパケット処理準備ができた）場合にのみバイパスをディセーブルにします。

電源投入とは、電源が復旧した後に、ユーザ設定に従ってデータ ポートのバイパス モードをシステムが続行することを意味します。すべてのトラフィックは、ユーザが手動でバイパスをディセーブルにするまで、内部ポートから外部ポートに、またはその逆に通過できます。電源が復旧した後、電源復旧後もシステムがバイパス モードであることを示すために、イベント/トラップが管理システムに送信されます。

手動でハードウェア バイパスをイネーブルにすると、システムはバイパス モードをイネーブルにし、ユーザがバイパスをディセーブルにするコマンドを発行するまで、すべてのファイアウォール/VPN または IPS 機能が適用されません。クリティカル イベントは、システムによる保護が提供されないことを示すために、管理システムに送信されます。ユーザは他の機能を設定している間にバイパス機能をイネーブルにするか、またはディセーブルにするかを考慮する必要があります。

（注） バイパスをディセーブルにしない場合、すべての変更内容は適用されないことをユーザに通知するためのシステム設定（ファイアウォール ルールなど）を変更しようとすると、警告メッセージが出されます。

（注） システムには、フェイル オーバーとバイパス設定を決して同時に設定しないでください。シスコは、こうした設定をサポートしていません。

注意 システムのリロードはソフトウェアのリセットではなく、ハードウェアのリセットです。これは、電源をバイパス モードにしておくのと同じです。つまり、ソフトウェア アップデート後にシステムをスティッキ設定でリロードすると、システムはバイパス モードのままになります。

注意 各セグメントに接続されるネットワーク機器のサポート範囲は通常 100 m ですが、デバイスがバイパス モードの場合、これがわずか 50 m になります。

ハードウェア バイパスとファイアウォール モードの互換性

（注） ハードウェア バイパスは、トランスペアレント ファイアウォール モードでのみ設定できます。

トランスペアレント モードは、ブリッジ モードのレイヤ 2 スイッチに似ています。インターフェイスには IP アドレスがなく、1 個の IP アドレスがブリッジ インターフェイスに割り当てられるだけです。ネイバー デバイスはデバイスの存在を認識しません。バイパスは設定できます。

ルーテッド モードはレイヤ 3 ルータ モードで動作します。各インターフェイスには IP アドレスが割り当てられ、また、他の一般的なレイヤ 3 属性が割り当てられます。2 つのサブネットがアクティブな場合、ボックスをバイパス モードにすることはできません。

ポートのバイパス LED

各ポートにはポートの状態を示す 2 色（グリーンとオレンジ）の LED が搭載されています。LED の各状態を以下に示します。

LED	アクティブな状態	説明
イーサネット ポート	バイパス モード インジケータ	消灯：リンクなし グリーンが点灯：リンクが確立 グリーンが点滅：データの送受信中 オレンジ：エラー（リンクなしを意味する） ポート 1&2 または 3&4 の LED が同時にオレンジで点滅：これらの 2 つのポートはバイパス モードであり、システムが起動している

イベント メッセージ

ユーザは syslog および snmp により警告メッセージを受け取ります。

メッセージの詳細については、『ASA Syslog Guide』を参照してください。

CLI インターフェイス コマンド

次のコマンドは、ハードウェア バイパスの状態を表示するために使用します。

```
ISA3000# show hardware-bypass
                        Status              Powerdown            Powerup
Gigabitethernet 1/1-1/2   Enable/Disable      Enable/Disable     Enable/Disable
Gigabitethernet 1/3-1/4   Enable/Disable      Enable/Disable     Enable/Disable
```

このコマンドは、電源切断および電源投入中にバイパスモードをイネーブル、またはディセーブルにするために使用します。この例では、スティッキとは電源切断時にハードウェア バイパスがイネーブルになり、ソフトウェアが起動された後でも、デバイスがイネーブルのままになることを意味します。

```
ISA3000(config)#[no] hardware-bypass gigabitethernet {1/1-1/2|1/3-1/4} [sticky]
```

ハードウェア バイパスをイネーブルにすると、システムの電源が喪失しても、トラフィックはバイパス ポート ペアに流れ続けます。

次のコマンドはハードウェア バイパス モードを手動オプションでイネーブルにするのに使用されます。

```
ISA3000# hardware-bypass manual gigabitethernet 1/1-1/2
```

このコマンドは、スティッキで電源切断および電源投入をイネーブルにするために使用されます。

```
ISA3000# hardware-bypass GigabitEthernet 1/1-1/2 [sticky]
```

次のコマンドは、SFR モジュールの準備ができたときに、システムのバイパス モードを終了するのに使用されます。

```
ISA3000# hardware-bypass boot-delay module-up sfr
```

詳細については、ASA コマンド リファレンスを参照してください。

手動でハードウェア バイパスをイネーブルまたはディセーブルにする

このコマンドは、Cisco ISA 3000の実行中にバイパス機能をイネーブルまたはディセーブルにするのに使用されます。これは電源切断や電源投入オプションに依存しません。

```
ISA3000#[no] hardware-bypass manual gigabitethernet {1/1-1/2|1/3-1/4}
```

手動オプションによりハードウェア バイパスがイネーブルにされた場合、リロード後のバイパス状態は設定された電源切断および電源投入動作に従います。