



ハードウェア バイパス

この章は、次の項で構成されています。

- [概要 \(1 ページ\)](#)
- [ポートのバイパス LED \(2 ページ\)](#)

概要

ISA 3000 は、ASA または Firepower Threat Defense のバイパスモードで動作できます。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。

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



(注) ハードウェアバイパス機能は、銅線ポートでのみ使用できます。

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

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。電源投入後もハードウェアバイパスが継続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、ユーザー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、ユーザー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、ユーザー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。ユーザー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。

設定情報については、<https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/products-installation-and-configuration-guides-list.html> にある Firepower Threat Defense および ASA のソフトウェアガイドを参照してください。

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。

表 1: LED の説明

LED	アクティビティ	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

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。