クイック スタート ガイド

Cisco IPS モジュール（ASA）

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

1 ASA の IPS モジュールについて
2 管理インターフェイス ケーブルの接続
3 ASA での Adaptive Security Device Manager（ASDM）の起動
4 （ASA 5505）管理用 IPS モジュールのセットアップ
5 IPS セキュリティ ポリシーの設定
6 ASA で IPS モジュールを使用するための設定
7 次の作業

関連資料

- ASA に関連するすべてのドキュメントには、次の URL からアクセスできます。
  http://www.cisco.com/go/docs
- IPS に関連するすべてのドキュメントには、次の URL からアクセスできます。
  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_documentation_roadmaps_list.html

1 ASA の IPS モジュールについて

ASA モデルのソフトウェアおよびハードウェアと IPS モジュールとの互換性については、http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html の『*Cisco ASA Compatibility*』を参照してください。

IPS モジュールは、フル機能の予防的な侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前にこれらを阻止します。

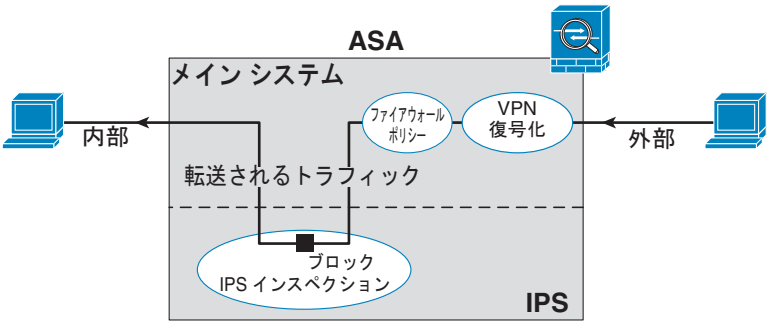
IPS モジュールは ASA から個別のアプリケーションを実行します。IPS モジュールに外部管理インターフェイスが搭載されている場合は、IPS モジュールに直接接続することができます。管理インターフェイスが搭載されていない場合は、ASA インターフェイスを介して IPS モジュールに接続できます。お使いのモデルで、IPS モジュールのその他のインターフェイスを利用できる場合、それらのインターフェイスは ASA トラフィックのみに使用されます。

トラフィックは、ファイアウォール検査を通過してから IPS モジュールへ転送されます。ASA で IPS インスペクションのトラフィックを識別する場合、トラフィックは次のように ASA および IPS モジュールを通過します。

注：この例は「インライン モード」に対応しています。ASA でトラフィックのコピーを IPS モジュールに送信するだけの「無差別モード」については、『ASA Configuration Guide』を参照してください。

1. トラフィックが ASA に入ります。	**2.** 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。	**4.** トラフィックが IPS モジュールに送信されます。
5. IPS モジュールがセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。	**6.** 有効なトラフィックが ASA に返送されます。IPS モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。	**8.** トラフィックが ASA から出ます。

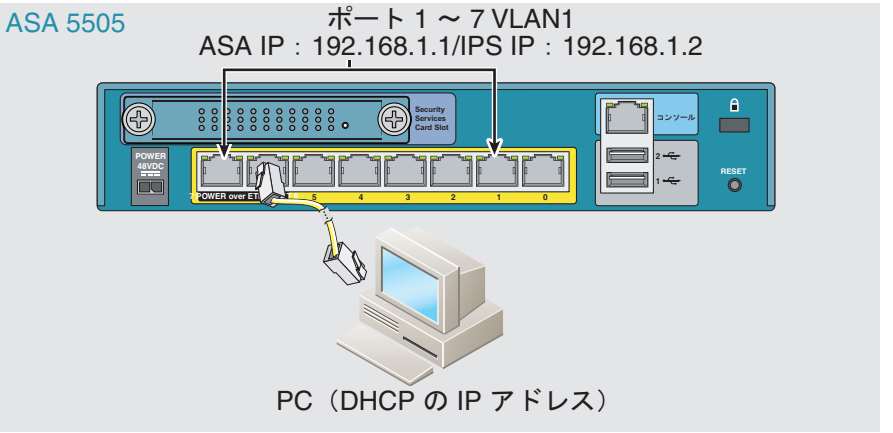
次の図に、IPS モジュールをインライン モードで使用する場合のトラフィック フローを示します。この例では、IPS モジュールが攻撃と見なしたトラフィックは、自動的にブロックされています。それ以外のトラフィックは、ASA を経由して転送されます。



2 管理インターフェイス ケーブルの接続

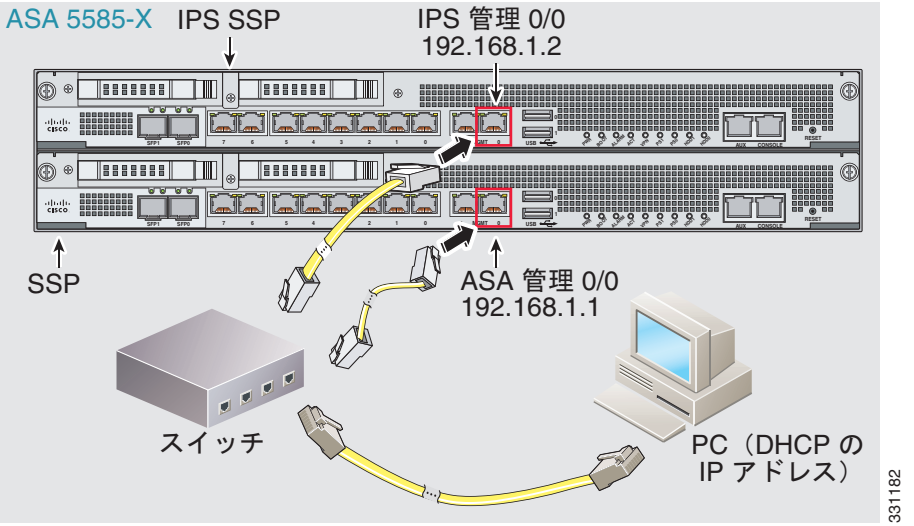
- ASA 5505

  ASA 5505 には専用の管理インターフェイスがありません。内部 IP 管理アドレスにアクセスするには、バックプレーン経由で ASA VLAN を使用する必要があります。管理 PC をイーサネット 0/1 ～ 0/7 のいずれかのポートに接続します。



- ASA 5510、ASA 5520、ASA 5540、ASA 5580、ASA 5585-X

  管理 PC、ASA 管理インターフェイス、IPS 管理インターフェイスをスイッチに接続します。



（注） デフォルト以外のネットワークを使用して管理を行いたい場合は、ASA と IPS CLI にアクセスし、各デバイス上で **setup** コマンドを実行して管理 IP アドレスを変更する必要があります。**setup** の詳細については、ASA および IPS ソフトウェアのコンフィギュレーション ガイドを参照してください。

ASA 5505 の場合は、CLI で **setup** を使用して ASA IP アドレスを変更した後、ASA CLI または ASDM を使用して IPS 管理 IP アドレスを設定できます。IPS CLI にアクセスする必要はありません。

3 ASA での Adaptive Security Device Manager（ASDM）の起動

ステップ 1 管理 PC で Web ブラウザを起動します。

ステップ 2 [Address] フィールドに **https://192.168.1.1/admin** と入力します。

ステップ 3 [Run ASDM] をクリックして Java Web Start アプリケーションを実行します。あるいは、ASDM-IDM Launcher をダウンロードすることもできます（Windows のみ）。詳細については、『ASA Configuration Guide』を参照してください。

ステップ 4 表示されたダイアログボックスに従って、任意の証明書を受け入れます。[Cisco ASDM-IDM Launcher] ダイアログボックスが表示されます。

ステップ 5 ユーザ名とパスワードのフィールドを空のまま残し、[OK] をクリックします。メイン ASDM ウィンドウが表示されます。

4 （ASA 5505）管理用 IPS モジュールのセットアップ

ステップ 1 IPS モジュールを初めて設定する場合は、ASDM のメイン ウィンドウで [Configuration] > [Device Setup] > [SSC Setup] を選択します。

（注） IPS モジュールの設定完了前に [IPS] タブをクリックすると、[Stop] ダイアログボックスが表示されます。ASDM で [SSC Setup] ペインを再度表示するには、[OK] をクリックします。GUI のいずれかの部分にアクセスするには、まず [SSC Setup] ペインで設定を定義する必要があります。

ステップ 2 [Management Interface] および [Management Access List] エリアで、デフォルト設定を受け入れます。

ステップ 3 [IPS Password] エリアで、次の手順を実行します。

a. パスワードを入力します。デフォルトのパスワードは cisco です。

b. 新しいパスワードを入力し、変更を確認します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーションの設定を保存します。[SSC Setup completed] ダイアログボックスは、初期設定後にだけ表示されます。

5 IPS セキュリティ ポリシーの設定

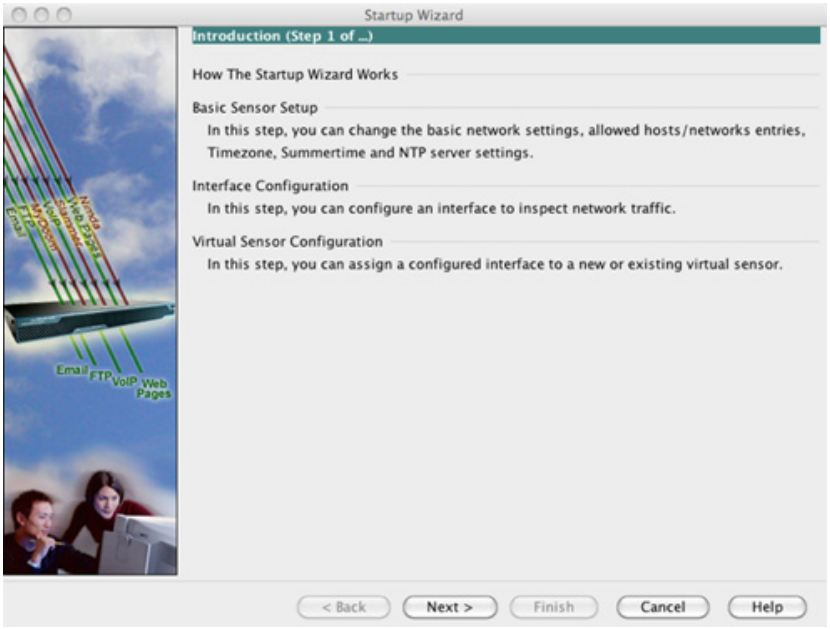
ステップ 1 ASDM から IPS Device Manager（IDM）にアクセスするには、[Configuration] > [IPS] をクリックします。ユーザ名とパスワードのほか、IPS モジュールの IP アドレスまたはホスト名の入力を要求されます。

ステップ 2 デフォルトの IP アドレスとポート（192.168.1.2:443）を受け入れます。デフォルトのユーザ名は cisco です。デフォルトのパスワードは cisco です。ASA 5505 でモジュールの初期設定時にパスワードを変更した場合は、その新しいパスワードをここに入力します。お使いのローカル PC にログイン情報を保存するには、[Save IPS login information on local host] チェックボックスをオンにします。

ステップ 3 [Continue] をクリックします。[Startup Wizard] ペインが表示されます。

（注） IPS モジュールで 5.x 以前のバージョンが実行されている場合、ASDM に IDM へのリンクが表示されます。

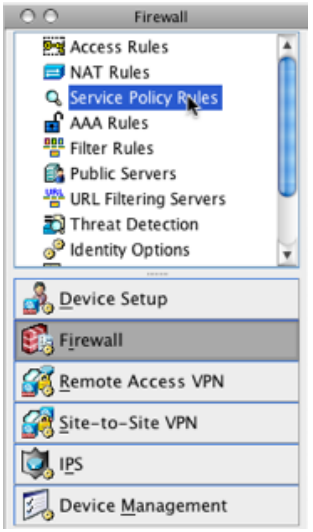
ステップ 4 [Launch Startup Wizard] をクリックします。プロンプトに従って画面を完了します。詳細については、IDM オンライン ヘルプを参照してください。



6 ASA で IPS モジュールを使用するための設定

バックプレーン経由で IPS モジュールに送信されたすべてのトラフィックには、IPS セキュリティ ポリシーが適用されています。次の手順を実行し、IPS モジュールに送信するトラフィックを定義します。

ステップ 1 [Configuration] > [Firewall] > [Service Policy Rules] を選択します。

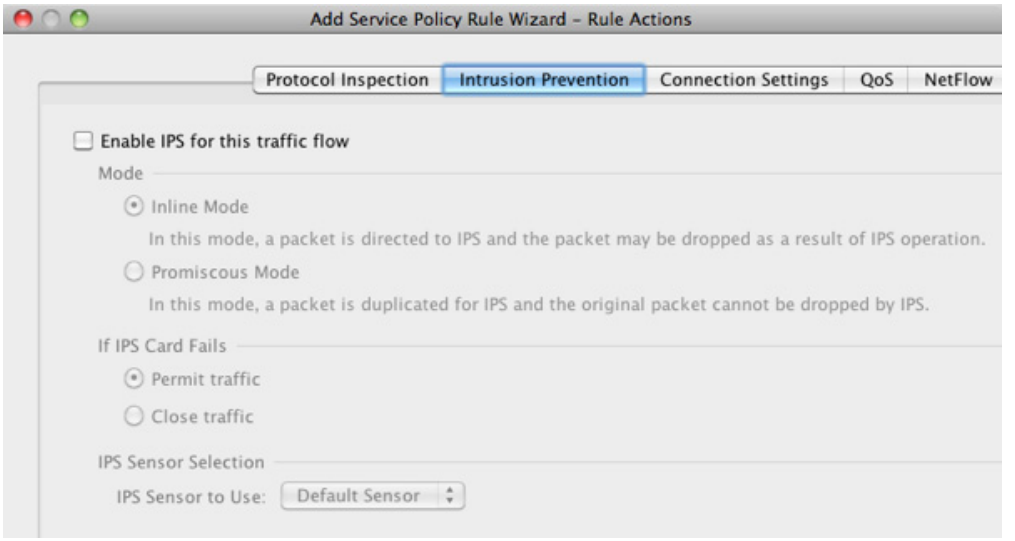


ステップ 2 [Add] > [Add Service Policy Rule] を選択します。[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3 [Service Policy] ダイアログボックスを完了してから、必要に応じて [Traffic Classification Criteria] を完了します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4 [Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 5　[Intrusion Prevention] タブをクリックします。



ステップ 6　[Enable IPS for this traffic flow] チェックボックスをオンにします。

ステップ 7　[Mode] エリアで、[Inline Mode] または [Promiscuous Mode] をクリックします。

ステップ 8　[If IPS Card Fails] エリアで、[Permit traffic] または [Close traffic] をクリックします。[Close traffic] オプションを選択すると、ASA は IPS モジュールが使用できない場合にすべてのトラフィックをブロックします。[Permit traffic] オプションを選択すると、ASA は IPS モジュールが使用できない場合に、すべてのトラフィックの通過を検査なしで許可します。[IPS Sensor Selection] エリアの詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 9　[OK] をクリックし、次に [Apply] をクリックします。

ステップ 10　この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

7 次の作業

- （任意）仮想センサーなどの高度な IPS オプションを設定します。IDM オンライン ヘルプを参照するか、次の URL でお使いのバージョンに対応したドキュメント ロードマップを確認してください。

  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_documentation_roadmaps_list.html

- （任意）ASA で仮想センサーを設定します。オンライン ヘルプを参照するか、次の URL でお使いの ASA バージョンに対応したコンフィギュレーション ガイドで IPS の章を確認してください。

  http://www.cisco.com/go/docs

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00 ～ 12:00、13:00 ～ 17:00
http://www.cisco.com/jp/go/contactcenter/