クイック スタート ガイド

Cisco ASA CX モジュール

【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 CX モジュールに関する情報
2 ASA CX 管理インターフェイスの接続
3 ASA での Adaptive Security Device Manager（ASDM）の起動
5 （ASA 5512-X ～ ASA 5555-X で必要な場合あり）ソフトウェア モジュールのインストール
4 （ASA 5585-X）ASA CX 管理 IP アドレスの変更
6 ASA CX CLI での基本的な ASA CX の設定
7 ASA CX モジュールへのトラフィックのリダイレクト
8 PRSM を使用した ASA CX モジュールでのセキュリティ ポリシーの設定
9 次の作業

改訂日：2012 年 12 月 3 日

1 ASA CX モジュールに関する情報

ASA CX モジュールは、ご使用の ASA モデルに応じて、ハードウェア モジュールである場合とソフトウェア モジュールである場合があります。ASA モデルのソフトウェアおよびハードウェアと ASA CX 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。

ASA CX モジュールを使用すると、ある状況の完全なコンテキストに基づいてセキュリティを実施できます。このコンテキストには、ユーザのアイデンティティ（誰が）、ユーザがアクセスを試みているアプリケーションまたは Web サイト（何を）、アクセス試行の発生元（どこで）、アクセス試行の時間（いつ）、およびアクセスに使用されているデバイスのプロパティ（どのように）が含まれます。ASA CX モジュールでは、フローの完全なコンテキストを抽出してきめ細かいポリシーを実施できます。たとえば、Facebook へのアクセスは許可するが Facebook のゲームへのアクセスは拒否する、あるいは財務担当者による企業の機密データベースへのアクセスは許可するが他の社員によるアクセスは拒否する、といったポリシーです。

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。ASA CX モジュールを設定するには、Cisco Prime Security Manager（PRSM）を使用した ASA CX ポリシー設定、および ASAASDM を使用した ASA CX モジュールへのトラフィックのリダイレクト ポリシーの 2 つの部分が必要です。

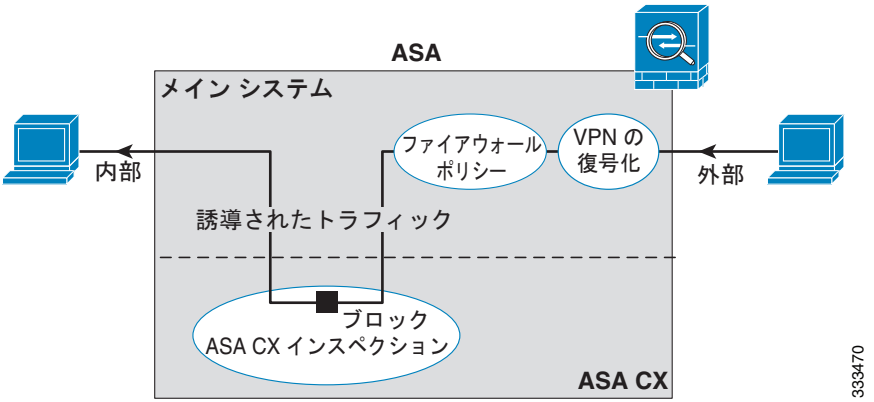
ASA CX モジュールには、外部管理インターフェイス（およびコンソール ポート）が含まれる場合があるため、ASA CX モジュールに直接接続できます。管理インターフェイスがない場合は、ASA インターフェイスを使用して ASA CX モジュールに接続できます。お使いのモデルで、ASA CX モジュールのその他のインターフェイスを利用できる場合、それらのインターフェイスは ASA トラフィックのみに使用されます。

トラフィックが ASA CX モジュールに転送される前に、ASA ファイアウォールのチェックが行われます。ASA で ASA CX インスペクション対象のトラフィックを識別する場合、次の手順で説明するように、トラフィックは ASA および ASA CX モジュールを通過します。

1. トラフィックは 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 ASA CX モジュールに送信されます。
5. ASA CX モジュールはセキュリティ 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。ASA CX 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。

次の図は、ASA CX モジュールを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、ASA CX モジュールは、特定のアプリケーションでは許可されていないトラフィックを自動的にブロックします。それ以外のトラフィックは、ASA を通って転送されます。

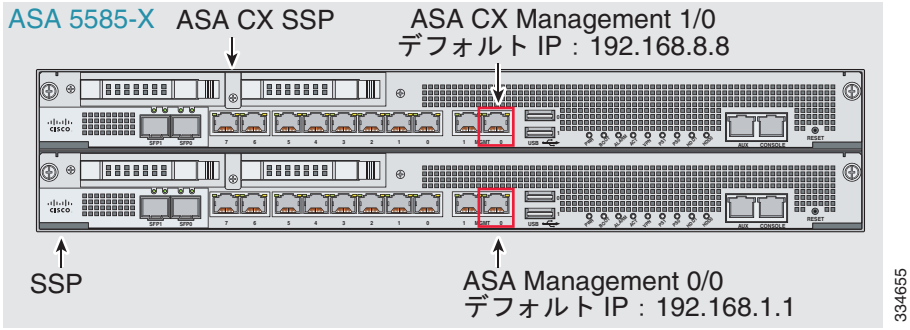


2 ASA CX 管理インターフェイスの接続

ASA CX モジュールへの管理アクセスを提供する以外に、ASA CX 管理インターフェイスは、シグニチャ アップデートなどのために、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスが必要です。この項では、推奨されるネットワーク設定について説明します。ご使用のネットワークによって異なる場合があります。

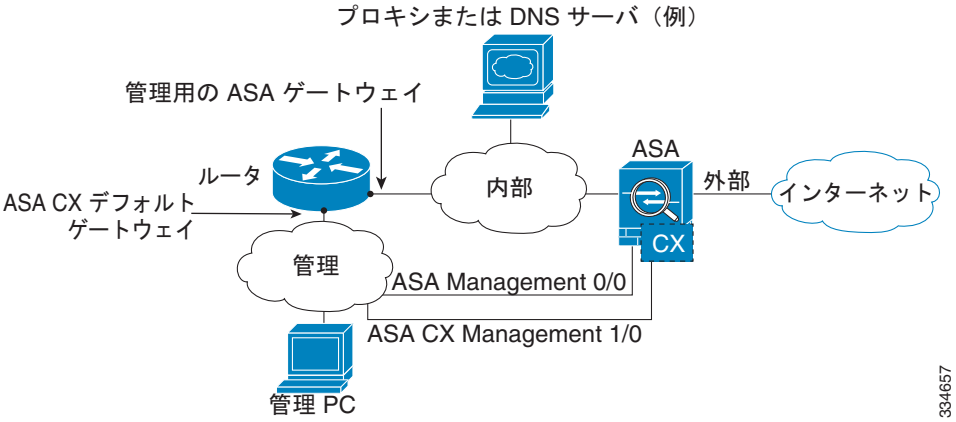
ASA 5585-X（ハードウェア モジュール）

ASA CX モジュールには、ASA とは個別の管理インターフェイスが含まれています。



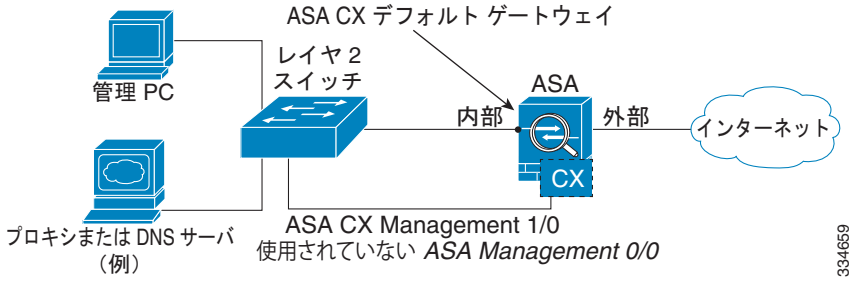
内部ルータがある場合

内部ルータがある場合、管理ネットワーク間でルーティングできます。これには、ASA Management 0/0 および ASA CX Management 1/0 の両方のインターフェイス、およびインターネット アクセスのための ASA 内部ネットワークが含まれることがあります。内部ルータを介して管理ネットワークにアクセスするには、ASA で忘れずにルートも追加してください。



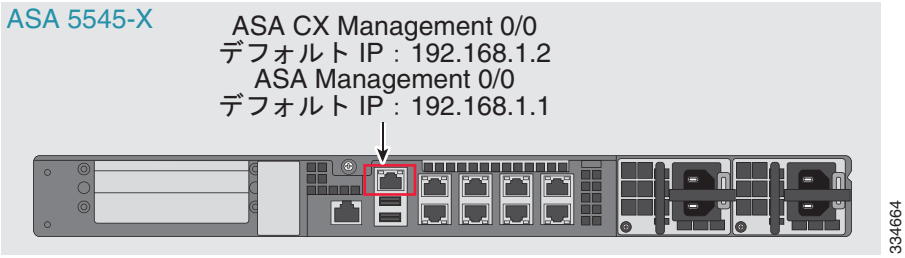
内部ルータがない場合

内部ネットワークが 1 つのみある場合、別個の管理ネットワークも使用することはできず、内部ルータをネットワーク間でルーティングする必要があります。この場合、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA CX モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上にあるように ASA CX Management 1/0 アドレスを設定できます。



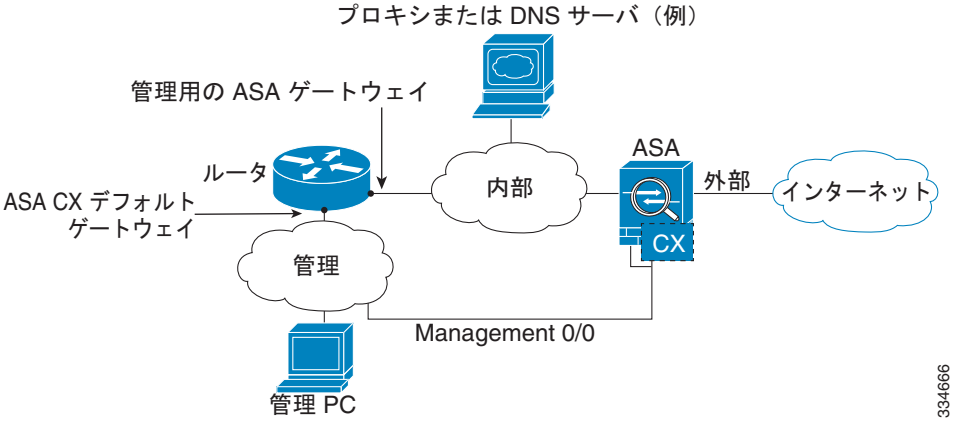
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、ASA CX モジュールをソフトウェア モジュールとして実行し、ASA CX 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。



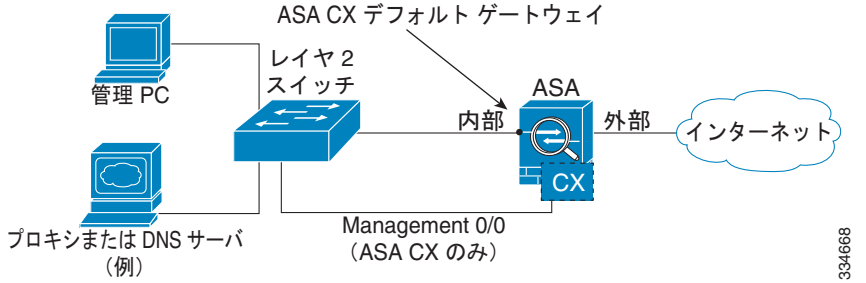
内部ルータがある場合

内部ルータがある場合、Management 0/0 ネットワーク間でルーティングできます。これには、ASA および ASA CX の両方の管理 IP アドレス、およびインターネット アクセス用の内部ネットワークが含まれます。内部ルータを介して管理ネットワークにアクセスするには、ASA で忘れずにルートも追加してください。



内部ルータがない場合

内部ネットワークが 1 つのみある場合、別の管理ネットワークも使用することはできません。この場合、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA 設定の名前を Management 0/0 インターフェイスから削除する場合、そのインターフェイスの ASA CX IP アドレスを引き続き設定できます。ASA CX モジュールは基本的には ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上にあるように ASA CX 管理アドレスを設定 できます。



（注） Management 0/0 に対して ASA が設定した名前を削除する必要があります。これが ASA で設定されている場合、ASA CX アドレスは、ASA と同じネットワーク上に存在する必要があり、これによって、その他の ASA インターフェイス上ですでに設定されたネットワークはすべて除外されます。名前が設定されていない場合、ASA CX は、任意のネットワーク上（たとえば、ASA 内部ネットワーク）に存在することができます。

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

デフォルトの ASA 設定を使用すると、デフォルトの管理 IP アドレス（192.168.1.1）に接続できます。ネットワークによっては、ASA 管理 IP アドレスを変更しなければならないか、場合によっては ASDM アクセスのために追加の ASA インターフェイスを設定しなければならないことがあります（「ASA CX 管理インターフェイスの接続」（P.4）を参照）。ASA 5512-X ～ ASA 5555-X では、別個の管理ネットワーク（「内部ルータがない場合」（P.7）を参照）がない場合、管理用の内部インターフェイスを設定し、さらに Management 0/0 インターフェイスから名前を削除する必要があります。インターフェイスおよび管理設定を変更するには、『ASA Configuration Guide』を参照してください。

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 URL **https://***ASA_IP_address*/**admin** を入力します。デフォルトの ASA 管理 IP アドレスは 192.168.1.1 です。

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。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。

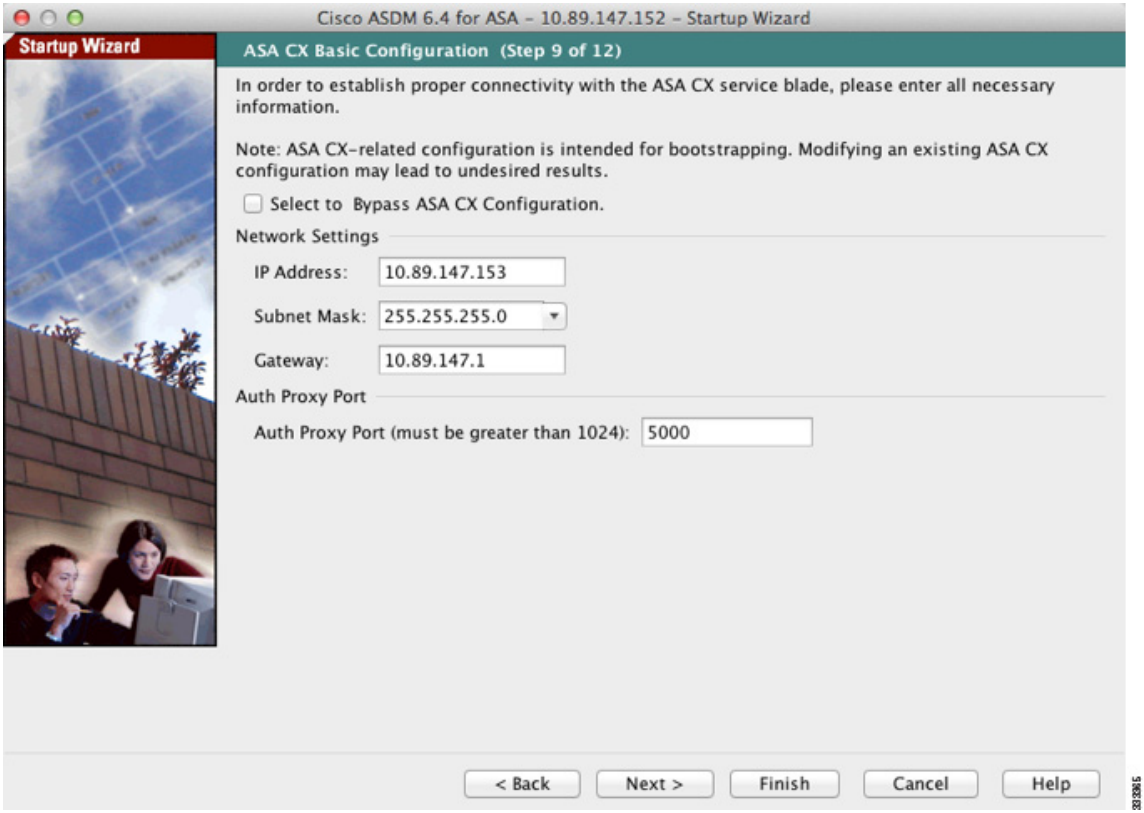
4 （ASA 5585-X）ASA CX 管理 IP アドレスの変更

デフォルトの管理 IP アドレスを使用できない場合、ASA から管理 IP アドレスを設定できます。管理 IP アドレスを設定した後、SSH を使用して ASA CX モジュールにアクセスして、初期設定を実行できます。

（注） ソフトウェア モジュールの場合、ASA CX CLI にアクセスして、ASA CLI からのセッション接続によって設定を実行できます。その後、設定の一部として ASA CX 管理 IP アドレスを設定できます。「ASA CX CLI での基本的な ASA CX の設定」（P.13）を参照してください。

ステップ 1 ASDM で、[Wizards] > [Startup Wizard] を選択します。

ステップ 2 ASA CX の [Basic Configuration] 画面が表示されるまで、[Next] をクリックして、初期画面を進みます。



ステップ 3 新しい管理 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。ネットワークの要件については、「ASA CX 管理インターフェイスの接続」（P.4）を参照してください。

ステップ 4 （任意）認証プロキシ ポートを変更します。

ステップ 5　[Finish] をクリックして残りの画面をスキップするか、[Next] をクリックして残りの画面を進み、ウィザードを完了します。

5　（ASA 5512-X ～ ASA 5555-X で必要な場合あり）ソフトウェア モジュールのインストール

ASA CX モジュールとともに ASA を購入した場合、モジュール ソフトウェアおよびソリッド ステート ドライブ（SSD）は事前にインストールされており、すぐに使用できます。既存の ASA に ASA CX を追加する場合、または SSD を交換する必要がある場合は、この手順に従って ASA CX ブート ソフトウェアをインストールし、SSD を分割する必要があります。物理的に SSD を取り付けるには、『ASA Hardware Guide』を参照してください。

ステップ 1　Cisco.com からコンピュータに ASA CX ブート ソフトウェアをダウンロードします。Cisco.com のログインをお持ちの場合は、次の Web サイトからブート ソフトウェアを入手できます。

http://www.cisco.com/cisco/software/release.html?mdfid=284325223&softwareid=28439946

ブート ソフトウェアを使用すると、基本的な ASA CX ネットワーク設定を行い、SSD を分割し、より大きいシステム ソフトウェアを任意のサーバから SSD にダウンロードできます。

ステップ 2　ASA CX 管理インターフェイスからアクセス可能な HTTP、HTTPS、または FTP サーバに、Cisco.com から ASA CX システム ソフトウェアをダウンロードします。Cisco.com のログインをお持ちの場合は、次の Web サイトからシステム ソフトウェアを入手できます。

http://www.cisco.com/cisco/software/release.html?mdfid=284325223&softwareid=28439944

ステップ 3　ASDM で、[Tools] > [File Management] を選択し、次に [File Transfer] > [Between Local PC and Flash] を選択します。ブート ソフトウェアを ASA 上の disk0 に転送します。システム ソフトウェアは転送しないでください。これは後で SSD にダウンロードされます。

ステップ 4　ASA CLI に接続し、特権 EXEC モードを開始します。ASA CLI にアクセスするには、『ASA Configuration Guide』ガイドの章「Getting Started」を参照してください。

ステップ 5 IPS モジュールを ASA CX モジュールと交換する場合は、IPS モジュールをシャットダウンしてアンインストールし、次に ASA をリロードします。

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

ASA のリロード後に、ASA CLI に再接続します。

ステップ 6 次のコマンドを入力して、ASA disk0 で ASA CX モジュール ブート イメージの場所を設定します。

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

例：

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-boot-9.1.1.img
```

ステップ 7 次のコマンドを入力して、ASA CX ブート イメージをロードします。

```
hostname# sw-module module cxsc recover boot
```

ステップ 8 ASA CX モジュールが起動するまで約 5 分待ってから、現在実行中の ASA CX ブート イメージへのコンソール セッションを開きます。デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **Admin123** です。

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

ステップ 9 SSD を分割します。

```
asacx-boot> partition
....
Partition Successfully Completed
```

ステップ 10 「ASA CX CLI での基本的な ASA CX の設定」（P.13）に従って、**setup** コマンドを使用して基本的なネットワーク設定を実行し（ASA CX CLI を終了しないでください）、この手順に戻ってソフトウェア イメージをインストールします。

ステップ 11 サーバからシステム ソフトウェアをインストールします。

```
asacx-boot> system install url
```

例：

次のコマンドは asacx sys9.1.1.pkg システム ソフトウェアをインストールします。

```
asacx-boot> system install
https://upgrades.example.com/packages/asacx-sys-9.1.1.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:
        Requires reboot:
Cisco ASA CX System Upgrade
Yes
Do you want to continue with upgrade? [n]: Y
Warning: Please do not interrupt the process or turn off the system. Doing so
might leave system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade. Press Enter to reboot the system.
```

ステップ 12 ASA CX モジュールをリブートするには、Enter キーを押します。モジュールをリブートすると、コンソール セッションが閉じます。アプリケーション コンポーネントのインストールと ASA CX サービスの起動には 10 分以上かかります。

6 ASA CX CLI での基本的な ASA CX の設定

セキュリティ ポリシーを設定する前に、ASA CX モジュールで基本的なネットワーク設定およびその他のパラメータを設定する必要があります。

ステップ 1 次のいずれかを実行します。

- （すべてのモデル）SSH を使用して ASA CX 管理 IP アドレスに接続します。
- （ASA 5512-X ～ ASA 5555-X）ASA CLI からモジュールへのコンソール セッションを開きます（ASA CLI にアクセスするには、『ASA Configuration Guide』の章「Getting Started」を参照してください）。

  ```
  hostname# session cxsc console
  ```

ステップ 2 ユーザ名 **admin** およびパスワード **Admin123** を使用してログインします。この手順の一環としてパスワードを変更します。

ステップ 3　次のコマンドを入力します。

```
asacx> setup
```

例：

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

次に、ウィザードを使用して、通常のパスを表示する例を示します。**注**：スタティック IPv6 アドレスを設定するときのプロンプトで **N** と応答することで、IPv6 ステートレス自動設定にすることができます。

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management
interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n)
[N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N] Y
Enter the local domain name: example.com
Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com,
2.ntp.example.com
```

ステップ 4　最後のプロンプトが完了すると、設定のサマリーが示されます。サマリーに目を通して値が正しいことを確認し、変更した設定を適用するには **Y** を入力します。変更をキャンセルするには **N** を入力します。

例：

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after
that
...
Done.
```

```
Press ENTER to continue...
asacx>
```

ステップ 5 NTP を使用しない場合は、時刻を設定します。デフォルトの時間帯は UTC 時間帯です。時間設定を変更するには、次のコマンドを使用できます。

```
asacx> config timezone
asacx> config time
```

ステップ 6 次のコマンドを入力して、admin パスワードを変更します。

```
asacx> config passwd
```

例：

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

ステップ 7 **exit** コマンドを入力してログアウトします。

7 ASA CX モジュールへのトラフィックのリダイレクト

この項では、ASA から ASA CX モジュールにリダイレクトするトラフィックを識別します。ASA でこのポリシーを設定します。

（注） PRSM をマルチ デバイス モードで使用する場合、ASDM を使用する代わりに、PRSM 内の ASA CX モジュールにトラフィックを送信するための ASA ポリシーを設定できます。ただし、ASA サービス ポリシーを設定する場合、PRSM にはいくつかの制限があります。詳細については、『ASA CX User Guide』を参照してください。

この手順を使用して ASA で認証プロキシをイネーブルにする場合は、ASA CX モジュールで認証用のディレクトリ レルムも設定してください。詳細については、『ASA CX User Guide』を参照してください。

（ASA CX と交換した）IPS モジュールにトラフィックをリダイレクトするアクティブ サービス ポリシーがある場合は、ASA CX サービス ポリシーを設定する前にそのポリシーを削除する必要があります。

ステップ 1 ASDM で、[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。

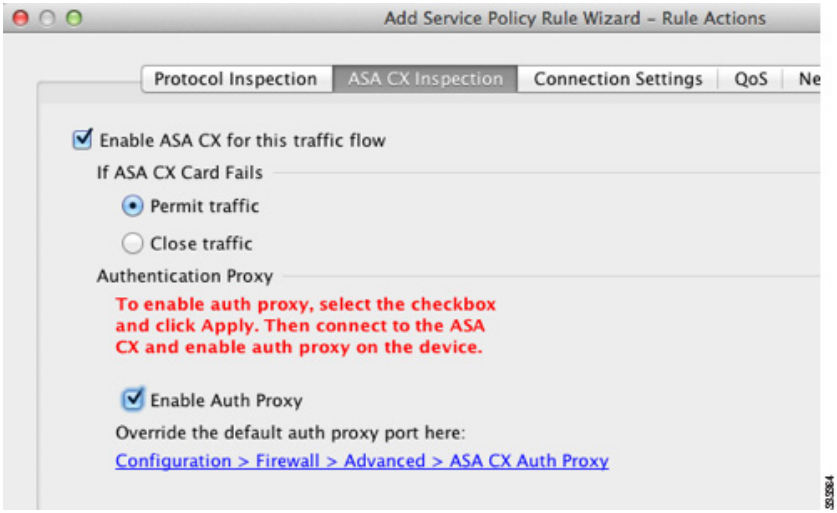
ステップ 3 必要に応じて [Service Policy] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4 [Next] をクリックします。[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5 必要に応じて [Traffic Classification Criteria] ダイアログボックスに入力します。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 6 [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 7　[ASA CX Inspection] タブをクリックします。



ステップ 8　[Enable ASA CX for this traffic flow] チェックボックスをオンにします。

ステップ 9　[If ASA CX Card Fails] 領域で、[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 ASA CX モジュールが使用不可の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 ASA CX モジュールが使用不可の場合に、すべてのトラフィックの通過を検査なしで許可します。

ステップ 10　アクティブ認証に必要な認証プロキシをイネーブルにするには、[Enable Auth Proxy] チェックボックスをオンにします。

ステップ 11　[OK] をクリックしてから、[Apply] をクリックします。

ステップ 12　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。

8 PRSM を使用した ASA CX モジュールでのセキュリティ ポリシーの設定

この項では、ASA CX モジュール アプリケーションを設定するために PRSM を起動する方法について説明します。PRSM を使用した ASA CX セキュリティ ポリシーの設定に関する詳細については、http://www.cisco.com/en/US/docs/security/asacx/roadmap/asacxprsmroadmap.html で ASA CX ドキュメント ロードマップを参照してください。

（注） ASA CX でポリシーを設定しない場合、ASA CX にリダイレクトされるすべてのトラフィックがデフォルトで許可され、トラフィックを分析するために ASA CX Web インターフェイスでさまざまなレポートを確認できます。

PRSM は、Web ブラウザから起動するか、ASDM から起動することができます。

- 次の URL を入力して、Web ブラウザから PRSM を起動します。

  `https://ASA_CX_management_IP`

  この場合、ASA CX 管理 IP アドレスは、「ASA CX CLI での基本的な ASA CX の設定」（P.13）で設定したアドレスです。

- [Home] > [ASA CX Status] を選択し、[Connect to the ASA CX application] リンクをクリックして、ASDM から PRSM を起動します。

9 次の作業

- ASA CX モジュールの詳細については、次のドキュメント ロードマップを参照してください。

  http://www.cisco.com/en/US/docs/security/asacx/roadmap/asacxprsmroadmap.html。

- 次の ASA CX ホーム ページも参照してください。

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

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/