CHAPTER 66

ASA CX モジュールの設定

この章では、ASA で実行される ASA CX モジュールを設定する方法について説明します。この章の内容は、次のとおりです。

ASA CX モジュールに関する情報

ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。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 モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。

この項では、次のトピックについて取り上げます。

ASA CX モジュールがどのように ASA と連携するか

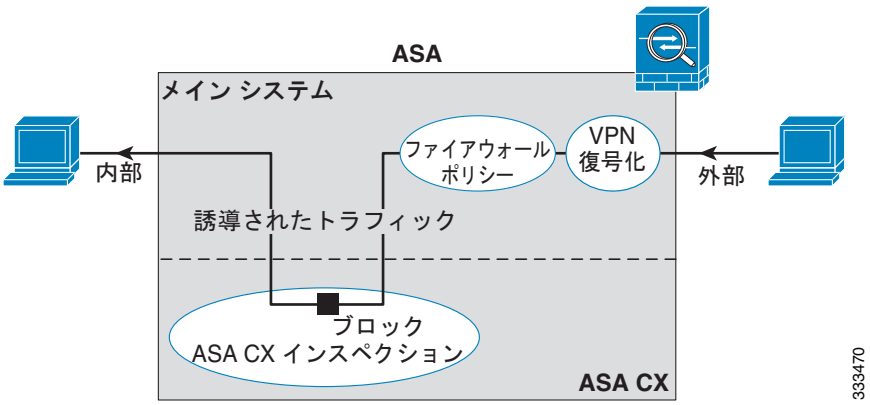
ASA CX モジュールは、ASA とは別のアプリケーションを実行します。ASA CX モジュールは外部管理インターフェイスを備えているので、ASA CX モジュールに直接接続できます。ASA CX モジュールのデータ インターフェイスは ASA のトラフィックだけに使用されます。

トラフィックは、ファイアウォール検査を通過してから ASA CX モジュールへ転送されます。ASA で ASA CX インスペクション対象として指定されたトラフィックは、次に示すように 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。

図 66-1 は、ASA CX モジュールを使用するときのトラフィック フローを示しています。この例では、特定のアプリケーションに対して許可されていないトラフィックを ASA CX モジュールが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。

図 66-1　　ASA での ASA CX モジュールのトラフィック フロー



（注） 2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

ASA CX 管理に関する情報

初期設定

初期設定を行うには、ASA CX モジュールの CLI を使用して **setup** コマンドを実行し、その他の任意の設定値を設定する必要があります。

CLI にアクセスするには、次の方法を使用します。

- ASA CX コンソール ポート：ASA CX コンソール ポートは、独立した外部コンソール ポートです。
- ASA CX 管理 1/0 インターフェイス（SSH を使用）：デフォルトの IP アドレス（192.168.8.8）に接続することも、ASDM を使用して管理 IP アドレスを変更してから SSH を使用して接続することもできます。ASA CX 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。

（注）　**session** コマンドを使用して ASA バックプレーンを介して ASA CX モジュール CLI にアクセスすることはできません。

ポリシー設定および管理

初期設定を実行した後で、Cisco Prime Security Manager（PRSM）を使用して ASA CX ポリシーを設定します。その後で、トラフィックを ASA CX モジュールに送信するための ASA ポリシーを、ASDM または ASA CLI を使用して設定します。

（注）　PRSM をマルチ デバイス モードで使用するときは、トラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。PRSM を使用すると、管理を単一の管理システムに集約できます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

認証プロキシに関する情報

ASA CX が HTTP ユーザを認証する必要がある場合は（アイデンティティ ポリシーを利用するために）、認証プロキシとして動作するように ASA を設定する必要があります。つまり、ASA CX モジュールは認証要求を ASA インターフェイス IP アドレス/プロキシ ポートにリダイレクトします。デフォルトでは、ポートは 885 です（ユーザ設定可能）。この機能は、トラフィックを ASA から ASA CX モジュールに誘導するサービス ポリシーの一部として設定します。認証プロキシをイネーブルにしない場合は、パッシブ認証のみを使用できます。

（注）　2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

VPN および ASA CX モジュールに関する情報

ASA は、トラフィックを ASA CX モジュールに転送するときに、VPN クライアントおよびユーザ認証のメタデータを組み込みます。したがって、ASA CX モジュールはこの情報をポリシー検索基準の一部として使用できます。VPN メタデータは、セッション ID が格納された Type-Length-Value（TLV）とともに、VPN トンネルの確立時にだけ送信されます。ASA CX モジュールは、各セッションの VPN メタデータをキャッシュします。トンネリングされた接続のそれぞれからセッション ID が送信されるので、ASA CX モジュールはそのセッションのメタデータを検索できます。

ASA の機能との互換性

ASA には、多数の高度なアプリケーション インスペクション機能があり、HTTP インスペクションもその一つです。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。
- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにした場合は、ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX モジュールによる処理を受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

ASA CX モジュールのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

ASA CX モジュールおよび PRSM には追加ライセンスが必要です。詳細については、ASA CX のマニュアルを参照してください。

注意事項と制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。マルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

フェールオーバーを直接にはサポートしていません。ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX によるインスペクションを受けることなく ASA の通過を許可されます。

ASA クラスタリングのガイドライン

クラスタリングはサポートされません。

IPv6 のガイドライン

IPv6 をサポートします。

モデルのガイドライン

ASA 5585-X でのみサポートされます。詳細については、『*Cisco ASA Compatibility Matrix*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

その他のガイドラインと制限事項

- 「ASA の機能との互換性」（P.66-4）を参照してください。
- モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA CX モジュールに、後で別のソフトウェアをインストールすることはできません。

デフォルト設定

表 66-1 に、ASA CX モジュールのデフォルト設定値を示します。

表 66-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
Management IP address	管理 1/0 192.168.8.8/24
Gateway	192.168.8.1/24
SSH Username	admin
Password	Admin123

ASA CX モジュールの設定

この項では、ASA CX モジュールを設定する方法について説明します。次の項目を取り上げます。

ASA CX モジュールのタスク フロー

ASA CX モジュールの設定プロセスでは、ASA CX セキュリティ ポリシーを ASA CX モジュール上で設定してから、トラフィックを ASA CX モジュールに送信するように ASA を設定します。ASA CX モジュールを設定するには、次の手順に従います。

ステップ 1　ケーブルで ASA CX 管理インターフェイスに接続します（任意でコンソール インターフェイスにも）。「ASA CX 管理インターフェイスの接続」（P.66-7）を参照してください。

ステップ 2　（任意）ASA で、最初の SSH アクセス用の ASA CX モジュール管理 IP アドレスを設定します。「ASA CX 管理 IP アドレスの設定」（P.66-8）を参照してください。

ステップ 3　ASA CX モジュールで、基本設定値を設定します。「ASA CX CLI での基本的な ASA CX 設定値の設定」（P.66-8）を参照してください。

ステップ 4　ASA CX モジュールで、PRSM を使用してセキュリティ ポリシーを設定します。「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」（P.66-10）を参照してください。

ステップ 5　（任意）ASA で、認証プロキシ ポートを設定します。「（任意）認証プロキシ ポートの設定」（P.66-11）を参照してください。

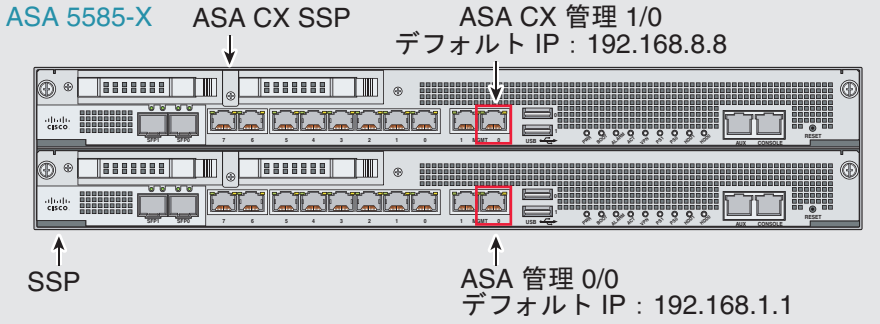
ステップ 6　ASA で、ASA CX モジュールに誘導するトラフィックを指定します。「ASA CX モジュールへのトラフィックのリダイレクト」（P.66-11）を参照してください。

（注）　PRSM をマルチ デバイス モードで使用するときは、トラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

ASA CX 管理インターフェイスの接続

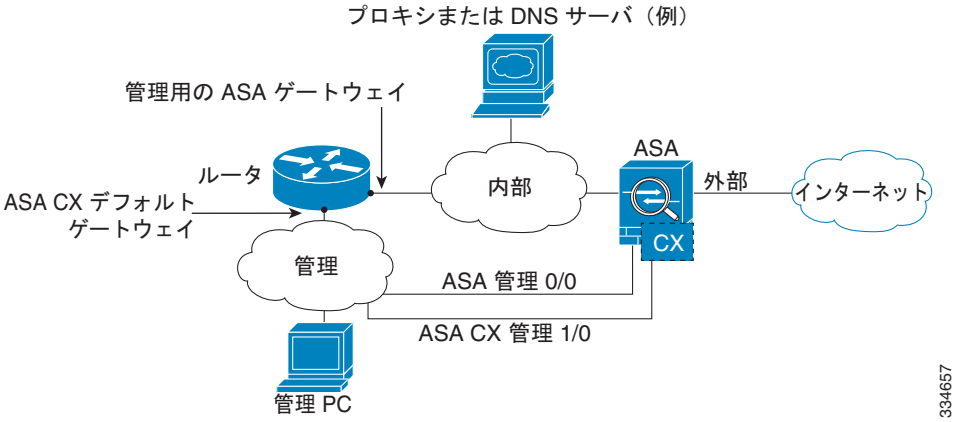
ASA CX モジュールへの管理アクセスを提供する以外に、ASA CX 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。これは、シグニチャ アップデートなどのためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

ASA CX モジュールには、ASA とは別の管理およびコンソール インターフェイスが含まれます。初期設定を行うには、デフォルト IP アドレス（192.168.8.8/24）を使用して ASA CX 管理 1/0 インターフェイスに SSH で接続できます。デフォルト IP アドレスを使用できない場合は、コンソール ポートを使用するか、ASDM を使用して SSH を使用できるように管理 IP アドレスを変更します。



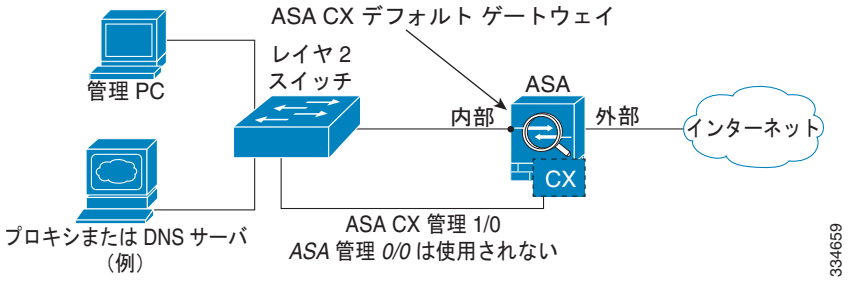
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA 管理 0/0 インターフェイスおよび ASA CX 管理 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます（インターネット アクセス用）。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、管理 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 ASA CX 管理 1/0 アドレスを設定できます。



次の作業

- （任意）ASA CX 管理 IP アドレスを設定します。「ASA CX 管理 IP アドレスの設定」（P.66-8）を参照してください。
- 基本的な ASA CX 設定値を設定します。「ASA CX CLI での基本的な ASA CX 設定値の設定」（P.66-8）を参照してください。

ASA CX 管理 IP アドレスの設定

デフォルトの管理 IP アドレス（192.168.8.8）を使用できない場合は、管理 IP アドレスを ASA から設定できます。管理 IP アドレスを設定した後は、初期設定を実行するために SSH を使用して ASA CX モジュールにアクセスできます。

手順の詳細

コマンド	目的
session 1 do setup host ip *ip_address*/*mask*,*gateway_ip* **例：** `hostname# session 1 do setup host ip 10.1.1.2/24,10.1.1.1`	ASA CX 管理 IP アドレス、マスク、およびゲートウェイを設定します。

ASA CX CLI での基本的な ASA CX 設定値の設定

セキュリティ ポリシーを設定する前に、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 ASA CX モジュール上で設定する必要があります。

手順の詳細

ステップ 1　ASA CX CLI に接続します。

- ASA CX 管理 1/0 インターフェイスへの SSH を使用：ユーザ名 **admin** とパスワード **Admin123** でログインします。この手順の中で、パスワードを変更します。
- ASA CX コンソール ポートを使用。

ステップ 2　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 [ ]
```

セットアップ ウィザードでは入力が求められます。次の例は、ウィザードでの一般的な順序を示しています。プロンプトで N ではなく Y を入力した場合は、追加の設定を行うことができます。次に、IPv4 および IPv6 両方のスタティック アドレスの設定例を示します。IPv6 ステートレス自動設定を設定するには、スタティック IPv6 アドレスを設定するかどうかを尋ねるプロンプトで **N** と応答します。

```
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 3　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>
```

（注）　ホスト名を変更した場合は、ログアウトして再びログインするまでプロンプトに新しい名前は表示されません。

ステップ 4　NTP を使用しない場合は、時刻を設定します。デフォルトのタイム ゾーンは UTC タイム ゾーンです。現在の設定を表示するには、**show time** コマンドを使用します。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 5　次のコマンドを入力して、admin の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 6　**exit** コマンドを入力してログアウトします。

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 を使用して ASA CX セキュリティ ポリシーを設定する方法の詳細については、ASA CX ユーザ ガイドを参照してください。

手順の詳細

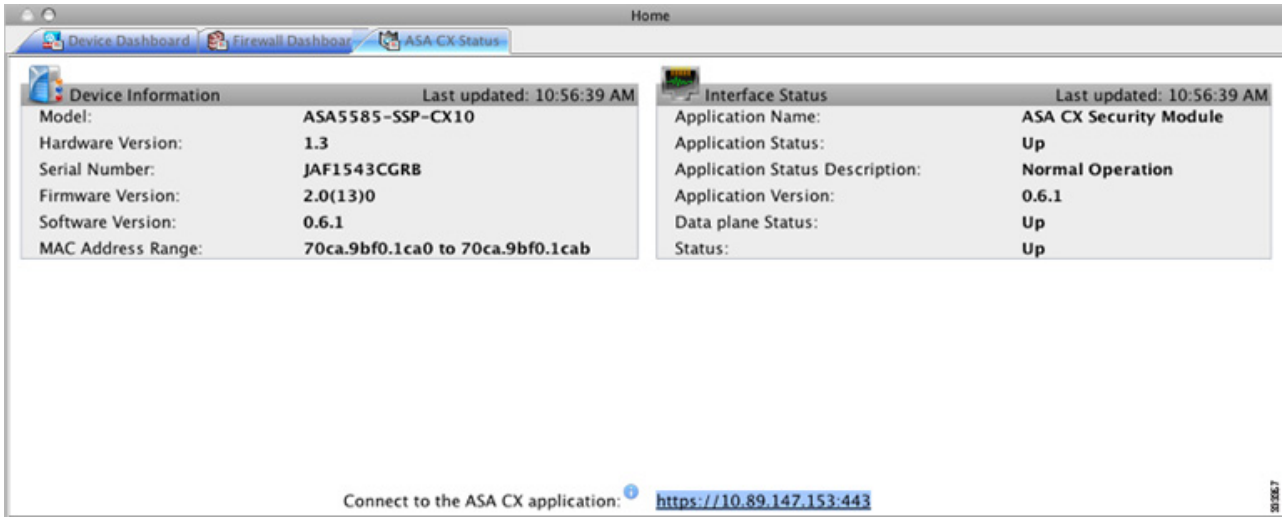
PRSM は、Web ブラウザから起動することも、ASDM から起動することもできます。

- Web ブラウザから PRSM を起動するには、次の URL を入力します。

  `https://ASA_CX_management_IP`

  ASA CX 管理 IP アドレスは、「ASA CX CLI での基本的な ASA CX 設定値の設定」（P.66-8）で設定したアドレスです。

- PRSM を ASDM から起動するには、[Home] > [ASA CX Status] を選択し、[Connect to the ASA CX application] リンクをクリックします。



次の作業

- （任意）認証プロキシ ポートを設定します。「（任意）認証プロキシ ポートの設定」（P.66-11）を参照してください。
- ASA CX モジュールにトラフィックを転送します。「ASA CX モジュールへのトラフィックのリダイレクト」（P.66-11）を参照してください。

（任意）認証プロキシ ポートの設定

デフォルトの認証ポートは 885 です。認証プロキシ ポートを変更するには、次の手順を実行します。認証プロキシの詳細については、「認証プロキシに関する情報」（P.66-3）を参照してください。

（注）　このポートは、ASDM Startup Wizard の中で設定することもできます。「ASA CX CLI での基本的な ASA CX 設定値の設定」（P.66-8）を参照してください。

手順の詳細

コマンド	目的
cxsc auth-proxy port *port* **例：** `hostname(config)# cxsc auth-proxy port 5000`	1024 よりも大きい認証プロキシ ポートを設定します。デフォルトは 885 です。

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指定します。このポリシーは、ASA で設定します。

（注）　PRSM をマルチ デバイス モードで使用するときは、トラフィックを ASA CX モジュールに送信するための ASA ポリシーの設定を、ASDM または ASA CLI を使用する代わりに PRSM の中で行うことができます。ただし、PRSM では、ASA サービス ポリシーを設定するときにいくつかの制限があります。詳細については、ASA CX のユーザ ガイドを参照してください。

前提条件

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、必ず 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 ユーザ ガイドを参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *name* **例：** `hostname(config)# class-map cx_class`	ASA CX モジュールに送信するトラフィックを指定するためのクラス マップを作成します。 ASA CX モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。
ステップ 2	**match** *parameter* **例：** `hostname(config-cmap)# match access-list cx_traffic`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.36-12）を参照してください。
ステップ 3	**policy-map** *name* **例：** `hostname(config)# policy-map cx_policy`	クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。
ステップ 4	**class** *name* **例：** `hostname(config-pmap)# class cx_class`	ステップ 1 で作成したクラス マップを識別します。
ステップ 5	**cxsc** {**fail-close** | **fail-open**} [**auth-proxy**] **例：** `hostname(config-pmap-c)# cxsc fail-close auth-proxy`	トラフィックが ASA CX モジュールに送信されるように指定します。 **fail-close** キーワードを指定すると、ASA CX モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。 **fail-open** キーワードを指定すると、ASA CX モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。 **auth-proxy** キーワードを指定すると、アクティブ認証に必要な認証プロキシがイネーブルになります。

	コマンド	目的
ステップ 6	（任意） **class** *name2* **例：** hostname(config-pmap)# class cx_class2	ASA CX トラフィックに対して複数のクラス マップを作成した場合は、ポリシーに対して別のクラスを指定できます。 ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.36-3）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。
ステップ 7	（任意） **cxsc** {**fail-close** | **fail-open**} [**auth-proxy**] **例：** hostname(config-pmap-c)# cxsc fail-close auth-proxy	2 番目のクラスのトラフィックが ASA CX モジュールに送信されるように指定します。 これらのステップを繰り返して、必要な数のクラスを追加します。
ステップ 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy cx_policy interface outside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

ASA CX モジュールの管理

この項では、モジュールの管理に役立つ手順について説明します。次の項目を取り上げます。

- 「パスワードのリセット」（P.66-13）
- 「モジュールのリロードまたはリセット」（P.66-14）
- 「モジュールのシャットダウン」（P.66-15）

（注） イメージのインストールまたはアップグレードを、ASA CX モジュール内から実行できます。詳細については、ASA CX モジュールのマニュアルを参照してください。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **admin** のデフォルトのパスワードは **Admin123** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュールのパスワードをデフォルトの「Admin123」にリセットするには、次の手順を実行します。

手順の詳細

コマンド	目的
hw-module module 1 password-reset **例：** `hostname# hw-module module 1 password-reset`	ユーザ **admin** のモジュール パスワードを **Admin123** にリセットします。

モジュールのリロードまたはリセット

モジュールをリロードまたはリセットするには、ASA CLI で次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
hw-module module 1 reload **例：** `hostname# hw-module module 1 reload`	モジュール ソフトウェアをリロードします。
hw-module module 1 reset **例：** `hostname# hw-module module 1 reset`	リセットを実行してから、モジュールをリロードします。

モジュールのシャットダウン

ASA を再起動したときに、モジュールは自動的には再起動されません。モジュールをシャットダウンするには、ASA CLI で次の手順を実行します。

手順の詳細

コマンド	目的
hw-module module 1 shutdown **例：** `hostname# hw-module module 1 shutdown`	モジュールをシャットダウンします。

ASA CX モジュールのモニタリング

（注） ASA CX 関連の syslog メッセージについては、syslog メッセージ ガイドを参照してください。ASA CX の syslog メッセージは、メッセージ番号 429001 から始まります。

モジュール ステータスの表示

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

コマンド	目的
show module	ステータスを表示します。
show module 1 details	ステータスの追加情報を表示します。

例

次に、ASA CX SSP がインストールされている ASA での **show module** コマンドの出力例を示します。

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
  1 ASA 5585-X CX Security Services Processor-10 ASA5585-SSP-CX10   JAF1510BLSA

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
```

```
  0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.7(6)78
  1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     0.6.1

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 ASA CX Security Module         Up               0.6.1

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

モジュールの統計情報の表示

モジュールの統計情報を表示するには、次のコマンドを入力します。

コマンド	目的
show service-policy cxsc	ASA CX の統計情報およびステータスをサービス ポリシーごとに表示します。

例

次に示す **show service-policy** コマンドの出力例では、認証プロキシがディセーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

次に示す **show service-policy** コマンドの出力例では、認証プロキシがイネーブルになっているときの、ASA CX ポリシーと現在の統計情報およびモジュールのステータスが表示されています。この場合は、proxied カウンタもインクリメントされます。

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

モジュール接続のモニタリング

ASA CX モジュールを通過する接続を表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show asp table classify domain cxsc	トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。
show asp table classify domain cxsc-auth-proxy	ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。
show asp drop	ドロップされたパケットを表示します。次のドロップ タイプが使用されます。 フレーム ドロップ： • cxsc-bad-tlv-received：これが発生するのは、ASA が CXSC から受信したパケットにポリシー ID TLV がないときです。非制御パケットのアクション フィールドで Standy Active ビットが設定されていない場合は、この TLV が存在している必要があります。 • cxsc-request：CXSC 上のポリシーが理由で、フレームをドロップするよう CXSC から要求されました。このポリシーによって、CXSC はアクションを Deny Source、Deny Destination、または Deny Pkt に設定します。 • cxsc-fail-close：パケットがドロップされたのは、カードが動作中ではなく、設定済みのポリシーが「fail-close」であったからです（対照的に、「fail-open」の場合は、カードがダウンしていてもパケットの通過が許可されます）。 • cxsc-fail：既存のフローに対する CXSC コンフィギュレーションが削除されており、CXSC で処理できないため、ドロップされます。これが発生することは、ほとんどありません。 • cxsc-malformed-packet：CXSC からのパケットに無効なヘッダーが含まれます。たとえば、ヘッダー長が正しくない可能性があります。 フロー ドロップ： • cxsc-request：フローを終了させることを CXSC が要求しました。アクション ビット 0 が設定されます。 • reset-by-cxsc：フローの終了とリセットを CXSC が要求しました。アクション ビット 1 が設定されます。 • cxsc-fail-close：フローが終了させられたのは、カードがダウン状態であり、設定済みのポリシーが「fail-close」であったからです。
show asp event dp-cp cxsc-msg	この出力には、dp-cp キューにある ASA CX モジュール メッセージの数が表示されます。現時点では、ASA CX モジュールからの VPN クエリーのみが dp-cp に送信されます。
show conn	このコマンドの出力では、接続がモジュールへの転送対象の場合に「X - inspected by service module」フラグが表示されます。ASA CX モジュールに転送される接続にも、「X」フラグが表示されます。

例

次に、**show asp table classify domain cxsc** コマンドの出力例を示します。

```
hostname# show asp table classify domain cxsc
Input Table
in  id=0x7ffedb4acf40, priority=50, domain=cxsc, deny=false
    hits=15485658, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=outside, output_ifc=any
in  id=0x7ffedb4ad4a0, priority=50, domain=cxsc, deny=false
    hits=992053, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=inside, output_ifc=any
in  id=0x7ffedb4ada00, priority=50, domain=cxsc, deny=false
    hits=0, user_data=0x7ffedb4ac840, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=m, output_ifc=any

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

次に、**show asp table classify domain cxsc-auth-proxy** コマンドの出力例を示します。次の出力の最初のルールでは、宛先の「port=2000」は **cxsc auth-proxy port 2000** コマンドで設定された認証プロキシ ポートであり、宛先の「ip/id=192.168.0.100」は ASA インターフェイス IP アドレスです。

```
hostname# show asp table classify domain cxsc-auth-proxy
Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
in  id=0x7ffed86cce20, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=2.2.2.2, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=new2, output_ifc=identity
in  id=0x7ffed86cd7d0, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=172.23.58.52, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=mgmt, output_ifc=identity
in  id=0x7ffed86caa80, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.5.172, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=outside, output_ifc=identity
in  id=0x7ffed86cb3c0, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=::/0, port=0
        dst ip/id=fe80::5675:d0ff:fe5b:1102/128, port=2000
    input_ifc=outside, output_ifc=identity
in  id=0x7ffed742be10, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=::/0, port=0
    dst ip/id=1:1:1:1::10/128, port=2000
    input_ifc=outside, output_ifc=identity
```

```
Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

次に、**show asp drop** コマンドの出力例を示します。この出力は単なる例であり、ASA CX モジュールからドロップされるフレームまたはフローの原因として考えられるものがすべて表示されています。

```
hostname# show asp drop
Frame drop:
  CXSC Module received packet with bad TLV's (cxsc-bad-tlv-received)           2
  CXSC Module requested drop (cxsc-request)                                    1
  CXSC card is down (cxsc-fail-close)                                          1
  CXSC config removed for flow (cxsc-fail)                                     3
  CXSC Module received malformed packet (cxsc-malformed-packet)                1

Last clearing: 18:12:58 UTC May 11 2012 by enable_15

Flow drop:
  Flow terminated by CXSC (cxsc-request)                                       2
  Flow reset by CXSC (reset-by-cxsc)                                           1
  CXSC fail-close (cxsc-fail-close)                                            1

Last clearing: 18:12:58 UTC May 11 2012 by enable_15
```

次に、**show asp event dp-cp cxsc-msg** コマンドの出力例を示します。

```
hostname# show asp event dp-cp cxsc-msg
DP-CP EVENT QUEUE                   QUEUE-LEN  HIGH-WATER
Punt Event Queue                            0           5
Identity-Traffic Event Queue                0           0
General Event Queue                         0           4
Syslog Event Queue                          4          90
Non-Blocking Event Queue                    0           2
Midpath High Event Queue                    0          53
Midpath Norm Event Queue                 8074        8288
SRTP Event Queue                            0           0
HA Event Queue                              0           0
Threat-Detection Event Queue                0           3
ARP Event Queue                             0        2048
IDFW Event Queue                            0           0
CXSC Event Queue                            0           1
EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
cxsc-msg                1          0        1        0        1          0
```

次に、**show conn detail** コマンドの出力例を示します。

```
hostname# show conn detail
0 in use, 105 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

```
TCP outside 208.80.152.2:80 inside 192.168.1.20:59928, idle 0:00:10, bytes 79174, flags
XUIO
```

モジュール トラフィックのキャプチャ

ASA CX モジュール用のパケット キャプチャを設定および表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
capture *name* **interface asa_dataplane**	ASA CX モジュールと ASA の間のパケットをバックプレーン上でキャプチャします。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	キャプチャを ASA コンソールに表示します。

（注） キャプチャされたパケットに含まれている追加 AFBP ヘッダーを、PCAP ビューアが認識しないことがあります。このようなパケットを表示するには、適切なプラグインを使用してください。

ASA CX モジュールのトラブルシューティング

モジュールのデバッグ

ASA CX デバッグをイネーブルにするには、次のコマンドを入力します。

コマンド	目的
debug cxsc [**error** | **event** | **message**]	エラー、イベント、またはメッセージ レベルのデバッグをイネーブルにします。

認証プロキシをイネーブルにすると、ASA から ASA CX モジュールに認証プロキシ TLV が送信されるときにデバッグ メッセージが生成されるので、IP とポートの詳細がわかります。

```
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: inside4.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: cx_inside.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: cx_outside.
```

インターフェイス IP アドレスが変更されると、auth-proxy tlv アップデートが CXSC に送信されます。

```
DP CXSC Event: Sent Auth proxy tlv for removing Auth Proxy for interface inside.
DP CXSC Event: Sent Auth proxy tlv for adding Auth Proxy on interface: inside.
```

フローが ASA 上で解放されると、ASA CX モジュールに通知が送られるので、そのフローをクリーンアップできるようになります。

```
DP CXSC Msg: Notifying CXSC that flow (handle:275233990) is being freed  for
192.168.18.5:2213 -> 10.166.255.18:80.
```

ASA CX モジュールが認証のためにリダイレクトをクライアントに送信すると、そのリダイレクトが ASA に送信され、ASA から ASA CX モジュールに送信されます。この例では、192.168.18.3 がインターフェイス アドレスで、ポート 8888 は、認証プロキシ機能用にそのインターフェイス上で予約された認証プロキシ ポートです。

```
DP CXSC Msg: rcvd authentication proxy data from 192.168.18.5:2214 -> 192.168.18.3:8888,
forwarding to cx
```

VPN 接続が ASA 上で確立されると、ASA から ASA CX モジュールに接続情報が送信されます。

```
CXSC Event:   Dumping attributes from the vpn session record
CXSC Event:   tunnel->Protocol:        17
CXSC Event:   tunnel->ClientVendor:    SSL VPN Client
CXSC Event:   tunnel->ClientVersion:   Cisco AnyConnect VPN Agent for Windows 2.4.1012
CXSC Event:   Sending VPN RA session data to CXSC
CXSC Event:   sess index:      0x3000
CXSC Event:   sess type id:    3
CXSC Event:   username:        devuser
CXSC Event:   domain:          CN=Users,DC=test,DC=priv
CXSC Event:   directory type:  1
CXSC Event:   login time:      1337124762
CXSC Event:   nac result:      0
CXSC Event:   posture token:
CXSC Event:   public IP:       172.23.34.108
CXSC Event:   assigned IP:     192.168.17.200
CXSC Event:   client OS id:    1
CXSC Event:   client OS:
CXSC Event:   client type:     Cisco AnyConnect VPN Agent for Windows 2.4.1012
CXSC Event:   anyconnect data: , len: 0
```

認証プロキシの問題

認証プロキシ機能を使用するときに問題が発生した場合は、次の手順に従って設定および接続のトラブルシューティングを行います。

1. コンフィギュレーションを確認します。
   - ASA で、**show asp table classify domain cxsc-auth-proxy** コマンドの出力を調べて、ルールがインストールされていて正しいことを確認します。
   - PRSM で、ディレクトリのレルムが作成されていて正しいクレデンシャルが指定されていることを確認するとともに、接続をテストして、認証サーバに到達可能であることを確認します。また、認証用のポリシー オブジェクトが設定されていることを確認します。
2. **show service-policy cxsc** コマンドの出力を見て、プロキシされたパケットがあるかどうかを調べます。
3. バックプレーンでのパケット キャプチャを行い、正しく設定されたポート上でトラフィックがリダイレクトされているかどうかを確認します。「モジュール トラフィックのキャプチャ」（P.66-20）を参照してください。設定済みのポートを調べるには、**show running-config cxsc** コマンドまたは **show asp table classify domain cxsc-auth-proxy** コマンドを使用します。

（注）　2 つの ASA インターフェイス上でホスト間が接続されており、ASA CX のサービス ポリシーがインターフェイスの一方のみについて設定されている場合は、これらのホスト間のすべてのトラフィックが ASA CX モジュールに送信されます。これには、ASA CX インターフェイス以外からのトラフィックも含まれます（この機能は双方向です）。ただし、ASA が認証プロキシを実行するのは、サービス ポリシーが適用されているインターフェイス上のみです。これは、入力のみの機能であるからです。

例 66-1　　ポート 2000 が一貫して使用されていることを確認してください。

1. 認証プロキシのポートを確認します。

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 認証プロキシ ルールを確認します。

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. パケット キャプチャでは、リダイレクト要求が宛先ポート 2000 に送られる必要があります。

ASA CX モジュールの設定例

次の例では、すべての HTTP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合はすべての HTTP トラフィックがブロックされます。

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
hostname(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list my-cx-acl
hostname(config)# class-map my-cx-class2
hostname(config-cmap)# match access-list my-cx-acl2
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap)# class my-cx-class2
hostname(config-pmap-c)# cxsc fail-open auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy interface outside
```

ASA CX モジュールの機能履歴

表 66-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 66-2　ASA CX モジュールの機能履歴

機能名	プラットフォーム リリース	機能情報
ASA 5585-X での ASA CX SSP のサポート	8.4(4.1)	ASA CX モジュールを使用すると、特定の状況の完全なコンテキストに基づいてセキュリティを強制することができます。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 モジュールを使用すると、フローの完全なコンテキストを抽出して、細分化したポリシーを適用することができます。たとえば、Facebook へのアクセスを許可するが Facebook でのゲームへのアクセスは禁止する、あるいは企業の機密データベースへのアクセスを財務担当者に許可するが他の社員には禁止するといったことが可能です。 **capture**、**cxsc**、**cxsc auth-proxy**、**debug cxsc**、**hw-module module password-reset**、**hw-module module reload**、**hw-module module reset**、**hw-module module shutdown**、**session do setup host ip**、**session do get-config**、**session do password-reset**、**show asp table classify domain cxsc**、**show asp table classify domain cxsc-auth-proxy**、**show capture**、**show conn**、**show module**、**show service-policy** の各コマンドが導入または変更されました。 *この機能は、バージョン 8.6(1) では使用できません。*