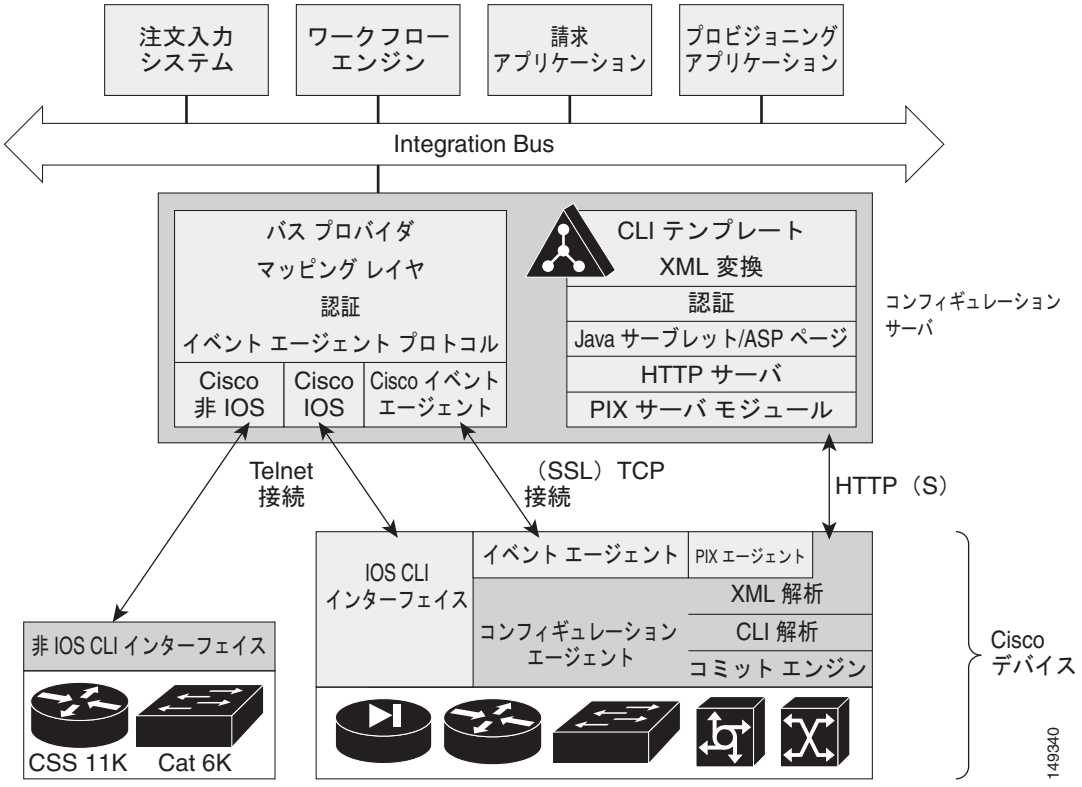
CHAPTER 21

PIX ファイアウォール デバイスのサポート

Cisco Configuration Engine は、設定管理およびイメージ サービスを Cisco PIX ファイアウォール デバイス（PIX デバイス）に提供します。図 21-1 に、PIX デバイス インターフェイス モジュールを含む Cisco Configuration Engine 機能のブロック図を示します。

図 21-1　　PIX 互換 Configuration Engine モジュールの相互関係



（注）　暗号化が Cisco Configuration Engine でサポートされるようにするには、暗号化を PIX デバイスのセットアップ中に有効にしておく必要があります。

PIX デバイスでの更新に関するポーリング

PIX デバイスは、そのデバイスに関する情報を報告するために Cisco Configuration Engine 内の PIX モジュールと通信します。この報告は、PIX が起動したとき、報告済みの情報が変更されたときに実行されるほか、PIX 側で更新があるかどうかをチェックする場合に任意のタイミングで実行されます。PIX は **DeviceDetails** メッセージをサーバに対して送信します。**DeviceDetails** は、Cisco Configuration Engine に対し、そのデバイスが現在実行中のソフトウェア バージョンの更新を示します。**DeviceDetails** 内で受信した情報は、参照のためにログ ファイル（*pix.log*）に記録されます。

サーバは **UpdateInfo** メッセージに応答します。このメッセージの内容（省略可能）

- PIX が実行する必要があるコンフィギュレーション ファイルのチェックサムと URL
- PIX イメージのチェックサムと URL
- PIX Device Manager（PDM）イメージのチェックサムと URL
- 任意のエラーを報告するための URL

PIX はメッセージ内のチェックサムを対象のコンポーネントの現在のチェックサムと比較します。また、設定の場合、実行中の設定の暗号化チェックサムを計算し、そのチェックサムを、設定が前回 Cisco Configuration Engine から更新された際に計算されたチェックサムと比較します。チェックサム（または暗号化チェックサム）が異なる場合は、更新が必要です。

ソフトウェアまたは設定の更新が必要な場合、PIX はそれぞれの URL で要求を送信します。

設定の処理

設定の更新が必要な場合、PIX は返された URL に HTTPS GET 要求を送信します。コンフィギュレーション ファイルは、適用前にローカル バッファに完全に読み込まれます。これは、接続エラーによって PIX が部分的に設定された状態になるのを回避するためです。コンフィギュレーション コマンドの適用中にエラーが発生しない場合（または **config-data** メッセージの *errors* アトリビュートが *continue*）、実行中の設定は **write memory** コマンドでフラッシュにコピーされます。すべてのコンフィギュレーション ファイルは *replace* モードで機能します。

PIX デバイスでの設定のダウンロードが完了すると、*pix.log* と同じエントリを示すログ ファイル エントリが生成されます。

（注） このログ エントリは、PIX デバイスに対する設定の適用が成功したことを意味するものではありません。PIX デバイスが設定ファイルをダウンロードしたことを意味するだけです。

イメージの処理

初期 HTTPS POST と一緒に送信された **DeviceDetails** XML には、オプションで PIX イメージに関する情報（バージョンとチェックサム）が含まれます。Cisco Configuration Engine は、ディレクトリ内のエントリに基づいて、イメージ URL を含む UpdateInfo XML およびチェックサムを返します。PIX はイメージを順々にダウンロードして適用します。また、必要に応じて PIX 自体をリロードします。エラーが発生した場合、次に説明する方法で処理されます。

（注） イメージの配信は Cisco Configuration Engine の外部である場合があり、PIX サーバは同一であることを追跡し続けられないため、イメージのダウンロードが成功したことを示す通知はありません。また、PIX デバイスもイメージ アップグレートが成功したことを示しません。

エラーの処理

すべてのエラーは、HTTPS POST で **ErrorList** メッセージを使用してエラー URL に報告されます。

各設定エラー レポート（type=error、warning、または info）は Cisco Configuration Engine が *pix.log* に記録します。ディスク スペースの使用率を節約するために、ログ ファイルは循環式になっています。エラーメッセージの内容は、PIX デバイス自体からのエラー XML です。

（注）　設定中に発生するエラーは、ダウンロードされた設定が PIX にまったく適用されなかったことを意味するものではありません。ログ ファイルで示されているエラーが、この特定のデバイスに関して発生したことを意味するだけです。

Cisco Configuration Engine から受信した URL のいずれかでデータを取得中に、エラーまたは通知（type= warning、notification、informational、debugging、emergency、alert、critical および error）が発生した場合、ログ ファイル エントリが生成されます。

サーバからの UpdateInfo 応答にあるいずれかの URL の処理中にエラーが発生した場合、そのエラーは Error URL に報告されます。また、現在のコール ホームで受信したすべての URL の処理は中止されます。処理の続行は、PIX が再びホームをコールするまで延期されます。

すべてのアップデートが正常に完了すると、PIX デバイスは別の **DeviceDetails** メッセージを Cisco Configuration Engine に送信します。Cisco Configuration Engine は再度 **UpdateInfo** とチェックサムを送信します。PIX デバイスはチェックサムを比較し、これ以上の更新が不要であることを確認します。

PIX デバイスからの DeviceDetails 要求の処理

PIX デバイスからの DeviceDetails 要求の処理手順は次のとおりです。

1. PIX デバイスは、HTTPS ポスト要求で **DeviceDetails** を XML ペイロードとして使用して Cisco Configuration Engine と通信します。
2. 新しい PIX Configuration サーブレットが要求を受信し、XML を解析し、DeviceID を取得します。
3. デバイスが認証されます。
4. この DeviceID と関連付けられているテンプレートが処理され、コンフィギュレーション ファイルが生成されます。
5. コンフィギュレーション ファイルが PIX DTD に従って XML 形式に変換されて保存されます（この DeviceID のファイルがすでに存在する場合は上書きされます）。
6. XML コンフィギュレーション ファイルのチェックサムが計算され、URL が示されます。
7. PIX イメージおよび PDM イメージの URL とチェックサムが、PIX デバイスと関連付けられているイメージ オブジェクトから取得されます。
8. 対応するチェックサムが異なる場合、コンフィギュレーション ファイルおよび各イメージのチェックサムと URL、および Error URL が HTTP 応答として XML ペイロード（UpdateInfo）とともに PIX デバイスに送信されます。
9. この時点でデバイスは、UpdateInfo 応答の内容に基づいて設定またはイメージを要求します。
10. エラーが発生した場合は、情報がエラー URL に発行されます。
11. エラー サーブレットがエラーを *pix.log* に記録します。

PIX DeviceID

次に示す PIX CLI によって、PIX が DeviceDetails 要求で送信する DeviceID の値が決定されます。

[no] auto-update device-id hardware-serial | hostname | ipaddress [*if-name*] | mac-address [*if-name*] | string text

- **auto-update device-id** コマンドで、管理サーバをポーリングするときに送信するデバイス ID が指定されます。
- **no auto-update device-id** コマンドでデバイス ID がデフォルトのホスト名にリセットされます。
- **hardware-serial** オプションに、PIX シリアル番号が使用されます。
- **hostname** オプションに PIX ホスト名が使用されます。
- **ipaddress** オプションに、**if-name** の名前と一緒にインターフェイスの IP アドレスが使用されます。

  インターフェイス名が指定されていない場合、リモート管理サーバとの通信に使用されるインターフェイスの IP アドレスが使用されます。
- **mac-address** オプションに、*if-name* の名前と一緒にインターフェイスの MAC アドレスが使用されます。

  インターフェイス名が指定されていない場合、リモート管理サーバとの通信に使用されるインターフェイスの MAC アドレスが使用されます。
- **string** オプションに *text* が指定されます。

  このテキストには、ホワイト スペースまたは文字 ‘、“、<、>、& および ? は使用できません。

（注） PIX が提供する DeviceID は、Cisco Configuration Engine の ConfigID および EventID に内部的にマッピングされるため、ハイフン（-）、アンダースコア（_）、ピリオド（.）、および英数字だけがサポートされます。

セキュリティに関する考慮事項

PIX デバイスはファイアウォール デバイスであり、設定情報は大変重要なため、この情報の転送は SSL を使用して保護されます。

あらゆる状況で、PIX デバイスと Cisco Configuration Engine との間の転送プロトコルとして、HTTPS が強制的に適用されます。**DeviceDetails**、**Update Info**、**ErrorInfo** およびコンフィギュレーション ファイルは、HTTPS を使用した場合だけ転送されます。Configuration Service で使用される認証メカニズムは、PIX サーバ モジュールで利用されます。PDM または PIX イメージの URL が提供される場合、HTTP または HTTPS を使用できます。

PIX デバイス ポーリングのセットアップ

PIX デバイスは、設定またはイメージのアップデートについて、Cisco Configuration Engine に対して定期的にポーリングするように設定できます。このエントリは、PIX デバイス自体に行う必要があります。詳細については、PIX デバイスのマニュアルを参照してください。この設定を行うための CLI 形式は、次のとおりです。

使用方法：auto-update device-id hardware-serial | hostname |

ipaddress [<if_name>] | mac-address [<if_name>] | string <text>

no auto-update device-id

auto-update poll-period <poll-period> [<retry-count>

[<retry-period>]]

no auto-update poll-period

auto-update server <url> [verify-certificate]

no auto-update server

auto-update timeout <period>

no auto-update timeout

例：

```
auto-update device-id string myPIXDevice
auto-update poll-period 120
auto-update server https://********@cns-ie2100/cns/PIXConfig
```

Cisco Configuration Engine 上でポーリングされる URI は次のとおりです。

/cns/PIXConfig

auto-update poll-period コマンドに、管理サーバへの設定またはイメージの更新についてのポーリング頻度を指定します。*poll-period* パラメータに、更新をチェックする頻度（分単位）を指定します。デフォルトは 720 分（12 時間）です。*retry-count* オプションに、サーバに対する最初の接続試行が失敗した場合に再試行する回数を指定します。デフォルトは 0 です。*retry-period* オプションに、次の再試行までの待機時間（分単位）を指定します。デフォルトは 5 です。

no auto-update poll-period コマンドでデフォルトのポーリング間隔がリセットされます。

また、PIX デバイス上のサーバ ホスト名をそのサーバの IP アドレスを使用してマップする必要もあります。*name* コマンドを次のように使用し、これを実行できます。

pixfirewall# **conf t**

pixfirewall(config)# **name <ip_address of the server> <hostname of the server>**

設定と制約事項

PIX 互換モジュールは、システムの初期設定の間にコンフィギュレーション サービスと一緒に設定されます。PIX 互換性を有効にするために特別な操作を行う必要はありません。

ソフトウェア バージョン 6.2.1 以降を使用する PIX デバイスは、Cisco Configuration Engine でサポートされています（PIX デバイス側での自動更新はこのバージョンで導入されました）。ソフトウェア バージョン 6.2.1 以上を実行する PIX ハードウェア プラットフォームはすべてサポートされます。

コンフィギュレーション ファイルは、config-action= **replace** オプションおよび errors=**revert** オプションを使用して生成されます。その他のオプションはサポートされません。