APPENDIX C

AUS と連動するためのデバイスのブートストラップ

AUS とデバイス間で通信できるようにするには、デバイスのトランスポートを設定してから、AUS または Security Manager のインベントリに追加します。デバイスは必要に応じて設定してください。

セキュリティ アプライアンスのブートストラップ

AUS を使用して PIX ファイアウォールまたは ASA デバイスを管理する前に、デバイスで基本的な接続ができるように最低限のコンフィギュレーションをデバイスで行います。基本的な接続の設定に関する詳細については、『*User Guide for Cisco Security Manager*』を参照してください。

基本的な接続に加えて、AUS 固有の設定を行う必要があります。次の手順では、デバイスのコマンドライン インターフェイスを使用してこの設定を実行および検証する方法を説明します。また、PIX Firewall Device Manager（PDM）セットアップ ウィザード（PIX バージョン 6.3 デバイスの場合）または Adaptive Security Device Manager（ASDM）セットアップ ウィザード（PIX 7.0+ または ASA デバイスの場合）を使用して設定できます。詳細については、ASA、ASDM、および PDM のマニュアルを参照してください。

（注） AUS を使用して ASDM および ASA ソフトウェア イメージを管理するには、**asdm image** および **boot system** コマンドを使用して ASA デバイスをブートストラップする必要があります。詳細については、「「起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション」（P.C-2）」を参照してください。

PIX または ASA デバイスを AUS と連動するようにブートストラップするには、デバイスのコンソール ポートに接続されたコンソール端末から次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *password*	特権 EXEC モードを開始します。
ステップ 2	**config terminal**	コンフィギュレーション モードに入ります。
ステップ 3	**http server enable**	デバイスの HTTP サーバを有効にして、ブラウザまたは HTTP 接続からコンフィギュレーションをモニタまたは変更できるようにします。

	コマンド	目的
ステップ 4	**http** *ip_address* [*netmask*] [*if_name*]	デバイスへの HTTP 接続を開始する権限を与えられたホストまたはネットワークを指定します。HTTP アクセスを許可するホストそれぞれにこのコマンドを入力します。 • *ip_address* : デバイスへの HTTP 接続を開始する権限を与えられたホストまたはネットワークの IP アドレスです。このコマンドを使用して少なくとも AUS および Security Manager サーバのアドレスを指定してください。 • *netmask* : IP アドレスのネットワーク マスクです。 • *if_name* : デバイスのインターフェイス名（デフォルトは **inside**）です。これを介して AUS または Security Manager によって HTTP 接続が開始されます。 **（注）** 即時自動更新を実行するには、これを設定してください。この設定によって、ASDM/PDM またはその他の HTTP 接続を介してデバイスにアクセスできるホストも決定されます。
ステップ 5	**auto-update server https://***username***:***password@AUSserver_IP_address***:***port***/autoupdate/AutoUpdateServlet**	デバイスを AUS に接続します。 • *username* : AUS サーバに入るためのログイン名です。 • *password* : ユーザのパスワードです。 • *AUSserver_IP_address* : AUS サーバの IP アドレスです。 • *port* : AUS サーバのポート番号です（通常は 443）。
ステップ 6	**auto-update poll-period** *poll_period [retry_count] [retry_period]*	AUS のポーリング時間を設定します。 • *poll_period* : 2 つの更新の間のポーリング期間間隔。デフォルトは 720 分（12 時間）です。 • *retry_count* : サーバへの接続が失敗した場合に再試行する回数です。デフォルトは 0 です。 • *retry_period* : 再試行の間隔です（分）。デフォルトは 5 です。
ステップ 7	**auto-update device-id [hardware-serial | hostname | ip_address** [*if_name*] **| mac-address** [*if_name*] **| string** *text* **]**	指定したデバイス ID を使用して自身を識別するようにデバイスが設定されます。 • *if_name* : デバイス インターフェイス名です（デフォルトは **inside**）。 • *text* : デバイスを識別するテキストです。 次の例では、ホスト名がデバイス ID として使用されています。 `auto-update device-id hostname`
ステップ 8	**write memory**	設定を保存します。
ステップ 9	**show auto-update**	AUS URL、ポーリング時間、タイムアウト、およびデバイス ID を表示します。設定を確認できます。
ステップ 10	**exit**	設定モードを終了します。

起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション

デフォルトでは、セキュリティ アプライアンスによって内蔵フラッシュ メモリで最初に検出されたソフトウェア イメージが使用されます。また、内蔵フラッシュ メモリで最初に検出された ASDM イメージまたは、イメージがない場合は次に、外付けフラッシュ メモリで最初に検出されたイメージが起動されます。複数のイメージがある場合は、起動するイメージを指定してください。ASDM イメージの

場合、起動するイメージを指定しないと、イメージが 1 つのみインストールされている場合でも、セキュリティ アプライアンスによって **asdm image** コマンドが実行されているコンフィギュレーションに挿入されます。自動更新で発生する問題を回避するため（設定されている場合）、または起動時に毎回イメージが検索されないようにするためには、スタートアップ コンフィギュレーションで起動する ASDM イメージを指定してください。

AUS を使用してデバイスにダウンロードされたイメージのバージョンをセキュリティ アプライアンスで **boot system** および **asdm image** コマンドを使用して示す必要があります。これを実行しないと、セキュリティ アプライアンスのイメージは、AUS からダウンロードされた最新のバージョンによって上書きされ、ASDM イメージの更新に失敗する場合があります。

また、セキュリティ アプライアンスに割り当てられたコンフィギュレーション ファイルは、デバイスに設定された同じブート ソフトウェア イメージおよび ASDM イメージを示す必要があります。示されていない場合、セキュリティ アプライアンスにある既存のイメージは、AUS からダウンロードされる最新のバージョンによって上書きされます。

セキュリティ アプライアンスで次のメッセージが表示された場合、セキュリティ アプライアンスの ASDM イメージが現行のバージョンと互換性があることを確認してください。この条件は、デバイスで **show run** コマンドの出力を表示することで確認できます。

```
Auto-update client: Sent DeviceDetails to /autoupdate/AutoUpdateServlet of server
10.1.1.200
Auto-update client: Processing UpdateInfo from server 10.1.1.200
Auto-update client: Failed to contact: https://10.1.1.200/autoupdate/AutoUpdateServlet,
reason: ErrorList error code: CALLHOME-PARSER-ERROR, description: The XML parser
encountered an error: The content of element type "DeviceDetails" must match
"(DeviceID,HostName,PlatformFamily,PlatformType,SerialNumber,SysObjectId,IPAddress+,Versio
nInfo*,Memory*)
```

次では、これらをデバイスのコマンド ラインを使用して設定する手順を説明します。また、Security Manager で [Platform] > [Device Admin] > [Boot Image/Configuration] ポリシーを使用しても設定できます。

- 起動するソフトウェア イメージを設定するには、次のコマンドを入力します。

  hostname(config)# **boot system** *url*

  url に次のいずれかを入力します。

  - {**flash:/** | **disk0:/** | **disk1:/**}[*path/*]*filename*

    flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内蔵フラッシュ メモリを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内蔵フラッシュ メモリには、**flash:/** または **disk0:/** と入力できます。**disk1:/** キーワードは、ASA の外付けフラッシュ メモリを示します。

  - **tftp://**[*user*[**:*password***]**@**]*server*[*:port*]/[*path/*]*filename*

    このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみサポートされます。

  最大 4 つの **boot system** コマンド エントリを入力して、ブートする別々のイメージを順番に指定することができます。セキュリティ アプライアンスでは、最初に検出されたイメージがブートされます。**boot system tftp:** コマンドは 1 つのみ設定でき、最初に設定する必要があります。

- ブートする ASDM イメージを設定するには、次のコマンドを入力します。

  hostname(config)# **asdm image** {**flash:/** | **disk0:/** | **disk1:/**}[*path***/**]*filename*