CHAPTER 1

AUS の紹介

Auto Update Server（AUS）を使用すると、自動アップデート機能を使用する PIX ファイアウォールおよび Adaptive Security Appliances（ASA; 適応型セキュリティ アプライアンス）上でデバイス コンフィギュレーション ファイルやソフトウェア イメージをアップグレードする際に Web ベースのインターフェイスを利用できます。

自動更新機能を使用するセキュリティ アプライアンスは、定期的に AUS に接続して、デバイス コンフィギュレーション ファイルを更新し、デバイスおよびステータス情報を渡します。

（注） AUS およびその他の関連サーバ アプリケーションのインストール方法については、『*Installation Guide for Cisco Security Manager*』を参照してください。

次に、AUS の基本的な使用方法について説明します。

Auto Update Server の概要

Cisco Security Management Suite のコンポーネントである Auto Update Server（AUS）は、PIX ファイアウォール ソフトウェア イメージ、ASA ソフトウェア イメージ、PIX Device Manager（PDM）イメージ、Adaptive Security Device Manager（ASDM）イメージ、および PIX ファイアウォールと ASA の各コンフィギュレーション ファイルを更新するツールです。

ASA または PIX デバイスすべてのソフトウェアおよび ASDM/PDM イメージを更新できますが、コンフィギュレーション ファイルの更新には、Security Manager アプリケーションを使用してコンフィギュレーションを作成および展開する必要があります。

AUS は Security Manager でサポートされている任意の ASA または PIX デバイスおよびオペレーティング システムのバージョンで使用できます（デバイスのリストについては、Cisco.com の『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください）。ただし、デバイスはシングルコンテキスト モードで実行されている必要があります。セキュリティ コンテキストをホストするデバイスでは AUS は使用できません。AUS サーバ 1 台でデバイスを 1000 台まで管理できます。

AUS はスタティック IP アドレスを使用するデバイスまたは DHCP を介してダイナミックに IP アドレスを取得するデバイスで使用できます。DHCP を使用するデバイスでコンフィギュレーションを更新する場合は、AUS を使用してください。ネットワーク管理サーバでは IP アドレスを事前に知ることができないため、DHCP を使用してインターフェイス アドレスを取得するデバイスとは直接通信を開始できません。さらに、管理システムで変更が必要な場合にこれらのデバイスが実行されていないか、ファイアウォールおよび NAT 境界をまたいで実行されている可能性があります。

自動更新機能を使用するように設定した場合、デバイスがスタティックまたはダイナミック IP アドレスのいずれを使用していても、デバイスは定期的に AUS に接続します。デバイスによって AUS に現在の状態とデバイス情報が提供されます。それに対して AUS は、デバイスで実行するべきソフトウェア イメージおよびコンフィギュレーション ファイルのバージョン リストを提供してデバイスに答えます。デバイスによってファイル バージョンは、実行しているファイル バージョンと比較されます。バージョンが異なる場合は、デバイスによって新しいバージョンが AUS によって提供された URL からダウンロードされます。新しいファイル バージョンによってデバイスが最新の状態になると、デバイスによって AUS に状態およびデバイス情報が再度送信されます。

また、AUS を使用して、デバイスがサーバに接続するのを待たず、オンデマンドでデバイスのコンフィギュレーションまたはソフトウェア イメージを更新できます。この機能は、緊急の驚異に対応するためデバイスを更新する場合に有用です。

次のトピックでは、AUS に関する詳細を説明します。

- 「NAT 境界をまたいだ AUS の展開」（P.1-2）
- 「デバイスの AUS への追加」（P.1-3）
- 「AUS データベースのバックアップおよび復元」（P.1-3）
- 「ユーザ ロールおよび権限について」（P.1-3）

NAT 境界をまたいだ AUS の展開

NAT 境界をまたいで企業ネットワーク内またはエンタープライズ DMZ 内のいずれかで AUS を展開する場合、AUS によって管理される PIX ファイアウォールおよび ASA デバイスは NAT 境界をまたぐことはできません。たとえば、NAT 境界をまたいだ DMZ で AUS を展開して、インターネット上でのみ展開されたデバイスを管理できますが、一部のデバイスが境界内でプライベート アドレスを使用し、一部のデバイスがインターネット上の外部にある場合、NAT 境界をまたいだ DMZ 上に AUS を展開できません。

AUS が NAT 境界をまたいでいる場合、デバイスが AUS への接続に使用するアドレスは多くの場合、AUS サーバの実際の IP と異なります。したがって、NAT 境界のパブリック側のデバイスが AUS のアクセスに使用する IP アドレスを指定する必要があります。たとえば、通常の設定は次のようになります。

AUS のパブリック アドレス 209.165.201.1 で、AUS の内部アドレス、192.168.0.1 に対応します。

デバイスはすべてパブリック アドレスに接続するため、[NAT Settings] ページの IP アドレスを 209.165.201.1 に設定する必要があります。NAT 境界がかかわらない場合は、ローカル マシンの IP アドレスであるデフォルト値のままにします。

（注）　デバイスはすべて NAT 境界をまたぐことはできません。NAT 境界をまたいだデバイスのコンフィギュレーションでは、AUS サーバが 2 台必要です。

ステップ 1　[Admin] > [NAT Settings] を選択します。[NAT Settings] ページが表示されます。

ステップ 2　[NAT Address] を選択して、サーバの IP アドレスに変換される IP アドレスを入力します。

（NAT を使用しない場合、または後で NAT の使用をやめる場合は [Actual Host Address] を選択します）

ステップ 3　[OK] をクリックして変更を適用します。

デバイスの AUS への追加

Security Manager を使用してデバイスに AUS を介してコンフィギュレーションを展開する場合、デバイスが正常に AUS に接続してコンフィギュレーションを取得した後、デバイスは自動的に AUS インベントリに追加されます。これは、デバイスを追加する通常の方法です。

ただし、AUS を使用して Security Manager によって管理されていないデバイスのソフトウェアおよび ASDM/PDM イメージの更新を管理する場合、またはトラブルシューティングする場合には、手動でデバイスを追加できます。詳細については、「デバイスを直接 AUS に追加する」を参照してください。

デバイスを AUS に追加する場合、Security Manager にはイネーブル パスワードおよび HTTP ユーザ名/パスワード（AUS では TACACS+ ユーザ名およびパスワードとして定義）が含まれます。これらの資格情報は、デバイスで即時にコンフィギュレーションを更新するために [Update Now] アクションを実行する場合（即時自動更新）に使用されます。詳細については、「即時自動更新の要求」（P.2-6）を参照してください。

AUS データベースのバックアップおよび復元

AUS データベースをバックアップおよび復元するには、標準の Security Manager/CiscoWorks バックアップおよび復元ユーティリティを使用します。データベース バックアップは、AUS をサーバ新しいサーバにインストールして、データベースを復元する場合に使用できます。

これらのツールの使用方法については、『*User Guide for Cisco Security Manager*』を参照してください。

ユーザ ロールおよび権限について

AUS では、CiscoWorks Server または Cisco Secure Access Control Server（ACS）を使用した 2 種類の認証方式がサポートされます。AUS および Security Manager をインストールすると、使用する方式を設定できます。詳細については、付録 B「ユーザ ロールおよび権限」を参照してください。

Auto Update Server へのログインと終了

Auto Update Server には、Cisco Security Management Suite のホーム ページからログインできます。また、ホーム ページから Security Manager クライアントをインストールしたり、Common Services、Performance Manager、RME、および Common Services にインストールされたその他のソフトウェアにアクセスしたりできます。

手順

ステップ 1　Web ブラウザで、次のいずれかの URL を開きます。*AUSServer* は AUS がインストールされたコンピュータの名前を表します。[Security Alert] ウィンドウが表示された場合は、すべて [Yes] をクリックします。

- SSL を使用しない場合は、http://*AUSServer*:1741 を開きます。
- SSL を使用する場合は、https://*AUSServer*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。このページで JavaScript およびクッキーがイネーブルになっており、サポートされたバージョンの Web ブラウザを実行していることを確認します。Security Manager を実行できるようにブラウザを設定する方法については、『*Installation Guide for Cisco Security Manager*』を参照してください。

（注）　適切なセキュリティを確保するため、SSL を使用することを推奨します。また、Security Manager と AUS 間で適切に通信できるようにするため、AUS を実行するマシンのブラウザのセキュリティ モードをイネーブルにしてください。詳細については、「ブラウザとサーバ間のセキュリティの設定」（P.1-4）を参照してください。

ステップ 2　ユーザ名およびパスワードを使用して Cisco Security Management Suite サーバにログインします。サーバを初めてインストールした場合は、ユーザ名 **admin** および製品のインストール時に定義したパスワードを使用してログインします。

ステップ 3　ログインすると、Cisco Security Management Suite ホーム ページが表示されます。ホーム ページには、サーバにインストールされたスイートのアプリケーションがリスト表示されます。AUS を実行するサーバでは、少なくとも次の機能を使用できます。他の機能は製品のインストール方法に応じて使用できます。

- Auto Update Server：この項目をクリックすると、Auto Update Server インターフェイスが開きます。
- Server Administration：この項目をクリックすると、CiscoWorks Common Services Server ページが開きます。CiscoWorks Common Services は、サーバを管理する基本ソフトウェアです。サーバ管理およびトラブルシューティング、ローカル ユーザの定義など、バックエンド サーバ機能の設定および管理に使用します。
- CiscoWorks リンク（ページ右上）：このリンクをクリックすると、CiscoWorks Common Services ホーム ページが開きます。このページからは AUS にもアクセスできます。

ステップ 4　アプリケーションを終了するには、画面右上の [Logout] をクリックします。サーバのいずれかのウィンドウ（[AUS] ウィンドウまたは Security Manager ホーム ページなど）からログアウトすると、すべてのウィンドウからログアウトされます。

ログイン セッションは、2 時間アクティビティがないとタイムアウトされます。

ブラウザとサーバ間のセキュリティの設定

Security Manager で AUS に適切にコンフィギュレーション ファイルを展開するため、Security Manager デバイス インベントリに追加する AUS によって管理されるデバイスでは、ブラウザとサーバ間のセキュリティ モードがイネーブルである必要があります。

Common Services では、クライアント ブラウザと AUS 間および AUS とデバイス間でセキュアなアクセスを提供するため、SSL を使用します。Common Services では次でセキュアなアクセスを実現します。

- クライアント ブラウザおよび管理サーバ（AUS）間。
- AUS および Security Manager 間。
- AUS およびデバイス間。

SSL はアプリケーションレベルのプロトコルで、プライバシー、認証、およびデータ整合性により、データのセキュアなトランザクションを実現します。証明書、公開キー、および秘密キーを使用します。SSL によってクライアントとサーバ間の転送チャネルが暗号化されます。CiscoWorks サーバでは、クライアント ブラウザと管理サーバ間のセキュア アクセスの認証に証明書を使用します。

クライアント ブラウザと管理サーバ間および AUS と Security Manager 間のアクセスをセキュアにするには、SSL をイネーブルにしてください。ただし、スタンドアロン AUS アプリケーション（Security Manager に統合されていない AUS）を実行する場合は、SSL をディセーブルにできます。

手順

ステップ 1　Cisco Security Management Suite ホーム ページで、[Server Administration] をクリックして、Common Services を開きます。

ステップ 2　Common Services で、[Server] > [Security] > [Browser-Server Security Mode Setup] を選択します。

ステップ 3　[Enable] チェックボックスを選択します。

ステップ 4　[Apply] をクリックします。

ステップ 5　CiscoWorks セッションからログアウトして、すべてのブラウザ セッションを終了します。

ステップ 6　CiscoWorks サーバ CLI を使用して Daemon Manager を再起動します。

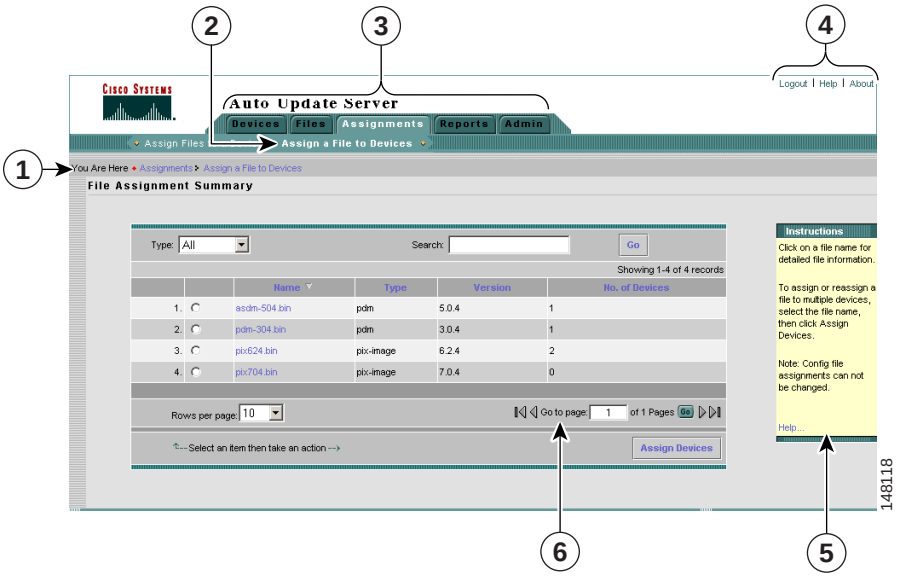
a. **net stop crmdmgtd** を入力

b. **net start crmdmgtd** を入力

ユーザ インターフェイスについて

Auto Update Server アプリケーションはブラウザ上で実行されます。アプリケーションの操作には、ブラウザのボタンではなく、インターフェイスのリンクおよびボタンを使用します。図 1-1 にインターフェイスの図と、詳細な説明を示します。

図 1-1　AUS GUI



参照番号	場所	説明
1	パス バー	表示されたページのコンテキストが表示されます。タブ、オプション、および現在のページが表示されます。リンクをクリックすると階層の中のそのページに移動できます。
2	オプション バー	選択したタブで利用可能なオプションが表示されます。オプションをクリックすると、そのページが表示されます。
3	タブ	製品の主な機能にアクセスできます。タブをクリックしてそのオプションにアクセスします。 • Devices：AUS によって管理されているデバイスに関する概要情報が表示されます。詳細については、第 2 章「デバイスおよび更新スケジュールの管理」を参照してください。 • Files：ソフトウェア イメージ、PDM と ASDM イメージ、およびコンフィギュレーション ファイルに関する情報を表示し、ソフトウェア イメージとデバイス マネージャ イメージを追加および削除できます。詳細については、第 3 章「ファイルの管理」を参照してください。 • Assignments：割り当て情報を表示し、デバイスからイメージへの割り当て、およびイメージからデバイスへの割り当てを変更できます。詳細については、第 4 章「ファイル割り当ての管理」を参照してください。 • Reports：レポートを表示します。詳細については、第 5 章「レポートの表示」を参照してください。 • Admin：NAT 設定を実行できます。詳細については、「NAT 境界をまたいだ AUS の展開」（P.1-2）を参照してください。
4	リンク	次のリンクを使用できます。 • Logout：CiscoWorks からログアウトします。 • Help ：新しいウィンドウを開きます。このウィンドウには、表示されたページの状況依存型ヘルプが表示されます。 • About：アプリケーションのバージョンを表示します。
5	指示ボックス	ページの使用方法の概要が表示されます。[Help] リンクをクリックすると追加情報を参照できます。

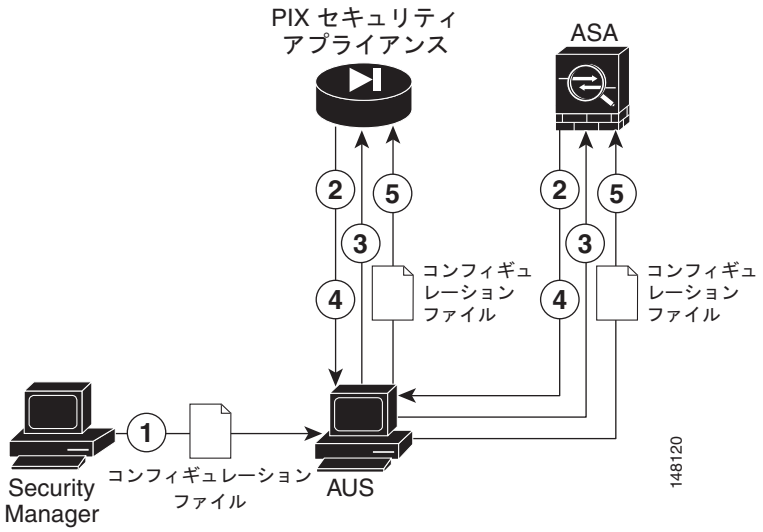
参照番号	場所	説明
6	ページ	アプリケーション タスクを実行する領域が表示されます。 画像で示すような多くのページには表があります。表の項目を操作するには、左端のカラムにあるチェックボックスをオンにして、表の下にある実行したいアクションに対応するボタンをクリックします。 ソートするカラムの見出しをクリックすると、表をソートできます。検索文字列を入力して、[Go] をクリックすると、表の項目を検索できます。 また、表の上にあるフィールドを選択することで、表の項目をフィルタ（関心のある項目のみを表示する）できます。この操作によって、表のみがフィルタされ、データベースからデータは削除されません。

コンフィギュレーション ファイルの更新

Security Manager では、管理されている PIX ファイアウォールおよび ASA デバイスのコンフィギュレーションを更新する媒体として AUS が使用されます。これらのコンフィギュレーションの作成および展開には、Security Manager を使用する必要があります。AUS のみを使用して、コンフィギュレーションの展開を実行できません。

図 1-2 に仕組みを示します。また、後続の手順では、Security Manager および AUS を併用して、コンフィギュレーションを展開する方法を説明します。

図 1-2　Security Manager および AUS を使用したコンフィギュレーション ファイルの更新



参照番号	説明
1	Security Manager では、PIX ファイアウォールまたは ASA コンフィギュレーション ファイルを AUS に展開します。
2	設定されたスケジュールに基づいて、デバイスは更新のため、AUS に接続します。

3	AUS によってイメージ ファイルまたはコンフィギュレーション ファイル（または両方）の URL リストと一緒にデバイスで実行すべきファイルのチェックサムが送信されます。
4	デバイスによって AUS から受信したチェックサムが参照され、実行中のファイルが正しいことが検証されます。正しくない場合は、AUS にファイルが要求されます。
5	ファイルがデバイスにダウンロードされます。

手順

ステップ 1　AUS サーバを使用するようにデバイスを設定します。付録 C「AUS と連動するためのデバイスのブートストラップ」を参照してください。

ステップ 2　Security Manager で New Device ウィザードで利用できる任意の方法を使用してデバイスを追加します。

- [Add New Device] または [Add Device from File] を選択すると、ウィザード上でデバイスを管理する AUS サーバを選択できます。これは、ブートストラップ時に設定したサーバと同じです。AUS サーバがインベントリですでに定義されていない場合は、デバイスの追加時に定義できます。
- [Add Device from Network] または [Add from Configuration Files] を選択すると、ウィザード上で AUS サーバを選択できません。代わりに、デバイスを追加した後に、[Tools] > [Device Properties] を選択して、[General] タブで AUS サーバを選択します。AUS サーバがインベントリですでに定義されていない場合は、デバイスのプロパティから定義できます。

デバイスを管理する AUS サーバを指定する他に、次の情報をウィザードまたはデバイスのプロパティで定義してください。

- デバイス ID：デバイスをブートストラップする際、ID として使用する文字列を設定します。これは通常、デバイスのホスト名です。ウィザードまたはデバイスのプロパティのいずれかに ID を入力します。
- 資格情報：イネーブル パスワードを入力します。AAA を使用してデバイスへのアクセスを制御している場合、デバイスで要求される HTTP のユーザ名およびパスワードを入力してください。

デバイスおよび AUS サーバをインベントリに追加する手順、およびこの手順で説明したその他の Security Manager のタスクについては、Security Manager のオンライン ヘルプを参照してください。

ステップ 3　Security Manager でデバイスの AUS ポリシーを設定します。次のいずれかを実行します。

- 単一のデバイスに対してポリシーを設定します。デバイス ビューでデバイスを選択して、[Device Policy] セレクタから [Platform] > [Device Admin] > [Server Access] > [AUS] を選択します。
- 同じ AUS を共有する複数のデバイスに割り当てられる共有ポリシーを設定します。ポリシー ビューで [Policy Types] セレクタから [PIX/ASA/FWSM Platform] > [Device Admin] > [Server Access] > [AUS] を選択します。[AUS] を右クリックして、[New AUS Policy] を選択してポリシーを作成するか、[Policies] セレクタから既存のポリシーを選択してポリシーを変更します。[Assignments] タブを選択して、特定のデバイスにポリシーを割り当てます。

必要に応じてデバイスに展開するコンフィギュレーションを実装するために、他のポリシーも設定します。

ヒント　Security Manager で他のファイルをデバイスにダウンロードすることが要求されるコンフィギュレーションは AUS に正常に展開できません。たとえば、一部のリモート アクセス VPN ポリシーでは、プラグイン、Anyconnect クライアント、および Cisco Secure Desktop コンフィギュレーションを設定できます。これらのファイルは AUS に送信されません。このタイプのポリシーを設定する場合は、AUS を使用しないでください。

ステップ 4　Security Manager で [Deploy to Device] 展開方法を使用してコンフィギュレーションを展開します。Security Manager によってコンフィギュレーションが AUS に送信され、そこでネットワーク デバイスによって取得されます。

デバイスを初めて展開すると、Security Manager によってデバイスが AUS インベントリに追加されます。デバイスで AUS インターフェイスを使用して即時自動更新などの（Update Now アクション）操作を実行する前に、AUS を介してデバイスを正常に展開する必要があります。正常に展開するには、デバイスが AUS に接続して、コンフィギュレーションを取得する必要があります。

ステップ 5　コンフィギュレーションが更新されたことを確認します。Event Report を表示すると、AUS に接続したデバイスに関する情報を表示できます。「Event Report の表示」（P.5-4）を参照してください。

デバイスの更新には少し時間がかかる場合があります。更新情報が表示されない場合は、数分待機してから再度レポートを確認してください。それでも情報が更新されない場合は、付録 A「AUS のトラブルシューティング」を参照してください。

関連項目

- 「PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新」
- 「デバイスの AUS への追加」（P.1-3）
- 「デバイスを直接 AUS に追加する」

PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新

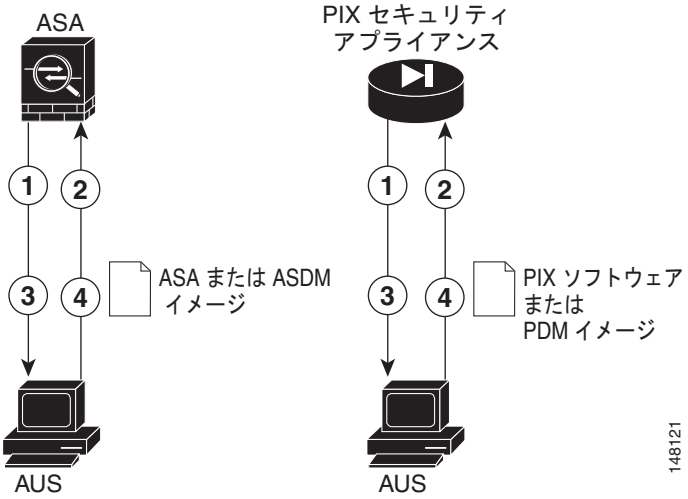
AUS を使用して PIX ファイアウォール ソフトウェア、ASA ソフトウェア、ASDM、および PDM イメージを更新できます。これらのイメージ更新には、Security Manager が使用されません。したがって、更新は Security Manager でコンフィギュレーションが管理されていないデバイスで実行できます。

ソフトウェアまたはデバイス マネージャ イメージを更新する際、次の点に注意してください。

- 新しい PIX または ASA ソフトウェア イメージがデバイスで実行されているコンフィギュレーション ファイルで使用できることを確認します。互換性のないソフトウェア イメージがダウンロードされると、デバイスによってすべてのサポートされないコマンドがドロップされ、コンフィギュレーション エラーが発生する場合があります。
- 新しい PDM または ASDM イメージが、デバイスで実行されている既存のソフトウェア イメージで使用できることを確認します。互換性のない PDM または ASDM イメージがダウンロードされると、PDM または ASDM が起動しない可能性があります。

（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。

図 1-3　AUS を使用した PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新



参照番号	説明
1	設定されたスケジュールに基づいて、デバイスは更新のため、AUS に接続します。
2	AUS によってイメージ ファイルまたはコンフィギュレーション ファイル（または両方）の URL リストと一緒にデバイスで実行すべきファイルのチェックサムが送信されます。
3	デバイスによって AUS から受信したチェックサムが参照され、実行中のファイルが正しいことが検証されます。正しくない場合は、AUS にファイルが要求されます。
4	ファイルがデバイスにダウンロードされます。

手順

ステップ 1　AUS サーバを使用するようにデバイスを設定します。付録 C「AUS と連動するためのデバイスのブートストラップ」を参照してください。

ステップ 2　デバイスが Security Manager によるコンフィギュレーションの展開時または「デバイスを直接 AUS に追加する」（P.2-3）の手順に従って手動で AUS に追加されたことを確認してください。

ステップ 3　イメージを AUS に追加します。詳細については、「ソフトウェア イメージの追加」（P.3-2）を参照してください。

ステップ 4　ファイルを 1 つ以上のデバイスに追加します。

- ファイルを単一のデバイスに追加する方法ついては、「単一デバイスへのファイルの割り当て / 割り当て解除」（P.4-3）を参照してください。
- ファイルを複数のデバイスに追加する方法ついては、「複数のデバイスへのファイルの割り当て / 割り当て解除」（P.4-5）を参照してください。

設定したスケジュールに基づいてセキュリティ アプライアンスは AUS に接続して、新しいソフトウェア、ASDM、または PDM イメージをダウンロードします。これらのアクションにはユーザの介入は不要です。

ソフトウェア イメージを更新すると、デバイスは自動的に再起動されます。再起動によって接続が切断され、ファイアウォールを通じたすべての既存のセッションは中断されます。

このことから、トラフィックのピークを避けた時間帯にセキュリティ アプライアンス イメージ更新してください。すべてのファイアウォールがピークを避けた時間帯に更新されるようにするため、制限のあるポーリング時間を設定できます。たとえば、3 時間のポーリング時間を設定して、更新が午前 12 時に実行されるように設定できます。ファイアウォールはすべて午前 12 時から午前 3 時の間に更新されます。ポーリング間隔の設定に関する詳細については、「セキュリティ アプライアンスのブートストラップ」（P.C-1）を参照してください。デバイスが Security Manager によって管理されている場合は、これらの設定を AUS ポリシーで設定してください（「コンフィギュレーション ファイルの更新」（P.1-7）を参照）。

ステップ 5　イメージが更新されたことを確認します。Event Report を表示すると、AUS に接続したデバイスに関する情報を表示できます。「Event Report の表示」（P.5-4）を参照してください。

デバイスの更新には少し時間がかかる場合があります。更新情報が表示されない場合は、数分待機してから再度レポートを確認してください。それでも情報が更新されない場合は、付録 A「AUS のトラブルシューティング」を参照してください。