CHAPTER 6

クライアントのインストールと設定

Security Manager アプリケーションと一緒に使用する重要なクライアント アプリケーションが 2 つあります。

- Security Manager クライアント。これは、ワークステーション上にインストールされ、通常は別のサーバ上にインストールされている Security Manager サーバ上で動作しているデータベースと相互作用するクライアント / サーバ アプリケーションです。このクライアントは一部の機能で Web ブラウザも使用します。
- Web ブラウザ。AUS を使用したり、Security Manager サーバや Common Services を使用する他のサーバを設定したりするために Web ブラウザを使用します。

次のトピックで、クライアントを実行するブラウザの設定方法と、Security Manager クライアントのインストール方法について説明します。

Web ブラウザ クライアントの設定

Web ブラウザが、特定の種類のコンテンツを許可し、アプリケーションを実行しているサーバからのポップアップ ウィンドウをブロックしないように設定されていることを確認する必要があります。Web ブラウザは、オンライン ヘルプだけでなく、機能的なアプリケーション ウィンドウを表示するために使用されます。次の項で、ブラウザをアプリケーション クライアントとして効率的に使用するために必要な設定方法について説明します。

HTTP/HTTPS プロキシ例外

HTTP/HTTPS プロキシを使用する場合は、Security Manager サーバ用のプロキシ例外を設定する必要があります。

この要件は、Internet Explorer と Firefox に適用されます。それぞれに対する追加設定の詳細を以降に説明します。

ブラウザ クッキーの設定

複数のブラウザがインストールされている場合、デフォルト ブラウザのクッキーを有効にする必要があります。具体的には、Internet Explorer のプライバシー設定は、中レベル以下（IE > [Tools] > [Internet Options] > [Privacy Settings] <= [Medium]）に設定する必要があります。

クッキーをブロックすることにより、Security Manager のユーザ ログインは Security Manager のクリーン インストール後も失敗する場合があります。ユーザ ログインが Security Manager のクリーン インストール後に失敗した場合は、次のエラー メッセージが表示される場合があります。「CMF session id cannot be assigned.」

Internet Explorer の設定

Security Manager とそのアプリケーションを正しく機能させるために必要な Internet Explorer の設定がいくつかあります。Internet Explorer は、オンライン ヘルプ、アクティビティ レポート、CS-MARS ルックアップ情報などの表示に使用されます。この手順では、Internet Explorer に必要な設定について説明します。

手順

ステップ 1　Internet Explorer 8 を使用している場合は、互換表示を使用します。Internet Explorer 8 は、互換表示の場合にのみサポートされています。互換表示を使用するには、Internet Explorer 8 を開いて、[Tools] > [Compatibility View Settings] に移動し、[website to be displayed in Compatibility View] として Security Manager サーバを追加します。

ステップ 2　次の手順を実行して、Security Manager のポップアップ ブロックをオフにします。

a. Internet Explorer を開きます。

b. [Tools] > [Pop-up Blocker] > [Pop-up Blocker Settings] に移動します。

c. [Address of website to allow] フィールドに、Security Manager サーバの IP アドレスを入力して、[Add] をクリックします。
http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions を参照してください。

注意　ポップアップ ブロックをオフにしなかった場合は、Security Manager でデバイスを検出できない可能性があります。

ヒント　「ポップアップ ブロックは、ポップアップの大半を制限またはブロックする Internet Explorer の機能です。」 http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions を参照してください。

ステップ 3　Internet Explorer で、[Tools] > [Internet Options] を選択します。この手順内の以降のステップは、[Internet Options] ダイアログボックス上で実行します。

ステップ 4　アクティブ コンテンツを許可するには、次の手順を実行します。

a. [Advanced] タブをクリックして、[Security] セクションにスクロールし、[Allow active content to run in files on My Computer] を選択します。

b. [Apply] をクリックして変更内容を保存します。

ステップ 5　ブラウザのセキュリティ設定が、暗号化されたページをディスクに保存できるようになっていることを確認します。暗号化されたページを保存できない場合は、クライアント ソフトウェア インストーラをダウンロードできません。

[Advanced] タブの [Security] エリアで、[Do not save encrypted Pages to Disk] を選択解除します。設定を変更する必要がある場合は、[Apply] をクリックして変更を保存します。

ステップ 6　一時ファイル用のディスク キャッシュのサイズが、ダウンロードを予定しているクライアント ソフトウェア インストーラのサイズを上回っていることを確認します。キャッシュ割り当てが少なすぎる場合は、インストーラをダウンロードできません。キャッシュ サイズを変更するには、次の手順を実行します。

a. [General] タブをクリックします。

b. [Temporary Internet Files] グループで [Settings] をクリックします。

c. 必要に応じて、インターネット一時ファイルに使用されるディスク スペースの容量を増やして [OK] をクリックします。

d. [Apply] をクリックして変更内容を保存します。

ステップ 7　（任意）CS-MARS と Security Manager 間でデータをやり取りするときに、セキュア コンテンツとノンセキュア コンテンツの両方が含まれたページを開かなければならないことがあります。デフォルトで、Internet Explorer からノンセキュア項目を表示するかどうかが尋ねられます。このプロンプトで [Yes] をクリックすると、ソフトウェアを正常に機能させることができます。

必要な場合は、プロンプトが表示されず、混合コンテンツ、つまり、セキュア コンテンツとノンセキュア コンテンツの両方が含まれるページが自動的に表示されるように Internet Explorer の設定を変更できます。混合コンテンツ ページを表示するように Internet Explorer を設定するには、次の手順を実行します。

a. [Security] タブをクリックします。

b. ダイアログボックス下部の [Custom Level] をクリックします。

c. [Miscellaneous] 見出しの下で、[Display mixed content] 設定に対応する [Enable] オプション ボタンを選択します。（[Disable] が選択されていないことを確認してください）。

d. [Apply] をクリックして変更内容を保存します。

ステップ 8　[OK] をクリックして [Internet Options] ダイアログボックスを閉じます。

Firefox の設定

Security Manager とそのアプリケーションを正しく機能させるために必要な Firefox の設定がいくつかあります。Firefox は、オンライン ヘルプ、アクティビティ レポート、CS-MARS ルックアップ情報などの機能の表示に使用します。この手順では、Firefox の設定に必要なオプションについて説明します。

プリファレンス ファイルの編集

手順

プリファレンス ファイルを編集するには、次の手順を実行します。

ステップ 1　メモ帳などのテキスト エディタで、\Mozilla Firefox\defaults\pref サブディレクトリにある **firefox.js** を開きます。

ステップ 2　次の式を追加します。

```
pref("dom.allow_scripts_to_close_windows", true);
```

ステップ 3　編集したファイルを保存して閉じます。

ディスク キャッシュのサイズの編集

一時ファイル用のディスク キャッシュのサイズが、ダウンロードを予定しているクライアント ソフトウェア インストーラのサイズを上回っていることを確認します。キャッシュ割り当てが少なすぎる場合は、インストーラをダウンロードできません。

手順

キャッシュ サイズを変更するには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Advanced] をクリックします。

ステップ 2　設定が少なすぎる場合は、より多くのキャッシュ スペースを確保して、[OK] をクリックします。

ポップアップ ブロックのディセーブル化またはホワイト リストの作成

手順

ポップアップ ブロックをディセーブルにするには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Contents] アイコンをクリックします。

ステップ 2　[Block pop-up windows] チェックボックスをオフにします。

または、ポップアップを受け入れる信頼できるソースのホワイト リストを作成するには、[Block pop-up windows] チェックボックスをオンにしてから、[Exceptions] をクリックして [Allowed Sites - Popups] ダイアログボックスで次の手順を実行します。

a. [Address of web site] フィールドに **http://**<*SERVER_NAME*>（ここで、*SERVER_NAME* は Security Manager サーバの IP アドレスまたは DNS ルーティング可能名）と入力してから、[Allow] をクリックします。

b. **file:///***C:*/**Documents%20and%20Settings/**<*USER_NAME*>**/Local%20Settings/Temp/**（ここで、*C:* は Windows がインストールされているクライアント システムのディスク ドライブで、*USER_NAME* はクライアント システム上の Windows ユーザ名）と入力してから、[Allow] をクリックします。

c. [Close] をクリックします。

ステップ 3　[OK] をクリックします。

JavaScript のイネーブル化

手順

JavaScript をイネーブルにするには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Contents] アイコンをクリックします。

ステップ 2　[Enable JavaScript] チェックボックスをオンにします。

ステップ 3　[Advanced] をクリックし、[Advanced JavaScript Settings] ダイアログボックスで、[Allow scripts to] エリア内のすべてのチェックボックスをオンにします。

ステップ 4　[OK] をクリックします。

最新ウィンドウ内の新しいタブ上でのオンライン ヘルプの表示と以降の要求に対する既存のウィンドウの再利用

初めてオンライン ヘルプにアクセスしたときに、2 つの新しいブラウザ ウィンドウ（空のページとヘルプ コンテンツが含まれるページ）が開くことがあります。その後、オンライン ヘルプにアクセスしようとしたときに、既存のブラウザ ウィンドウが再利用されないこともあります。

手順

最近開かれたブラウザ ウィンドウの新しいタブ上にオンライン ヘルプを表示し、それ以降は既存のブラウザ ウィンドウを再利用するように Firefox を設定するには、次の手順を実行します。

ステップ 1　アドレス バーに、**about:config** と入力して、Enter を押します。ユーザ プリファレンスのリストが表示されます。

ステップ 2　[browser.link.open_external] をダブルクリックして、表示されたダイアログボックスに **3** と入力します。この値は、外部アプリケーションからのリンクが、最後に開かれたブラウザ ウィンドウ内の新しいタブで開かれることを意味します。

ステップ 3　[browser.link.open_newwindow] をダブルクリックして、それを **1** に設定します。この値は、リンクがアクティブなタブまたはウィンドウで開かれることを意味します。

ステップ 4　[browser.link.open_newwindow.restriction] をダブルクリックして、それを **0** に設定します。この値は、新しいウィンドウのすべてがタブとして開かれることを意味します。

ステップ 5　[about:config] ページを閉じます。

（注）　ブラウザのステータス バーに Done というステータスが表示された後でも、状況依存のヘルプを開いたときに空白のページが開く場合があります。この問題が発生した場合は、数分待てば、コンテンツがダウンロード可能になり、表示されます。

サードパーティ製ツールでの例外のイネーブル化と設定

一部のサードパーティ製ポップアップ ブロックを使用すれば、通常はポップアップを拒否しながら、特定のサイトまたはサーバからのポップアップだけを許可できます。ポップアップ ブロックでホワイト リストに例外を含めることができない場合、または、そのオプションでは要件が満たせない場合は、すべてのポップアップを許可するようにユーティリティを設定する必要があります。信用されたサイトからのポップアップを許可する方式は、使用されているユーティリティによって異なります。詳細については、サードパーティ製品のマニュアルを参照してください。

Security Manager クライアントのインストールに関するヒント

Security Manager クライアントを使用してデバイスを設定します。クライアントで変更を保存すると、それらはワークステーションに保存されます。続いて、変更をデータベースに送信して、サーバ上のデータベースを更新する必要があります。

クライアントを使用している間は、クライアントとサーバ間で継続的に相互通信が行われます。この点を踏まえて、クライアントをインストールしてそのパフォーマンスを向上させるためのヒントを考慮してください。

- サーバと同じコンピュータ上でクライアントを日常業務として実行しないでください。クライアントをサーバ上にインストールした場合は、トラブルシューティングの目的にのみ使用してください。
- ネットワーク遅延の問題を避けるために、クライアントはサーバからあまり離れていないワークステーション上にインストールします。たとえば、米国にサーバを設置しながら、インド国内のネットワークからクライアントを実行した場合は、遅延が生じて応答性能が低下する可能性があります。この問題を軽減するには、クライアントがサーバと同じデータセンター内に設置される、リモート デスクトップまたはターミナル サーバ配置を採用する必要があります。
- 1 台のコンピュータ上には 1 つのクライアントのコピーしかインストールできません。クライアントとサーバのバージョンは完全に一致する必要があります。したがって、2 つの異なるバージョンの Security Manager 製品を実行する場合は、それぞれのクライアントを実行する 2 台のワークステーションを用意する必要があります。

  一方で、クライアントを複数回起動して、同じバージョンを実行している複数の Security Manager サーバに接続できます。

Security Manager クライアントのインストール

Security Manager クライアントは、ワークステーション上にインストールする個別のプログラムです。このクライアントを使用して、Security Manager サーバにログインして、デバイスに関するセキュリティ ポリシーを設定します。Security Manager クライアントは、製品と一緒に使用するメイン アプリケーションです。

サーバ ソフトウェアがインストールされていれば、Security Manager サーバ上にクライアントがインストールされている可能性があります。ただし、サーバと同じシステム上でクライアントを使用する場合は、製品の日常的な使用を避けることを推奨します。代わりに、次の手順を使用して、クライアントを別のワークステーションにインストールしてください。ワークステーション システムの要件とサポートされているブラウザのバージョンについては、「クライアントの要件」（P.3-10）を参照してください。

インストール中に問題が発生した場合は、次のトピックを参照してください。

- 「インストールを阻止するセキュリティ設定の処理」（P.6-10）
- 「以前のバージョンのクライアントからアップグレードできない」（P.6-11）
- 「インストール中のクライアント障害」（P.A-10）

はじめる前に

- ブラウザが正しく設定されていることを確認します。「Web ブラウザ クライアントの設定」（P.6-1）を参照してください。
- Windows ファイアウォールが正しく設定されていることを確認します。Security Manager でサポートされるオペレーティング システムでは、Windows ファイアウォールはデフォルトでイネーブルになっています。その結果、HTTP、HTTPS、および syslog の着信接続がブロックされます。たとえば、管理者はサーバの Security Manager クライアントのインストール URL にローカルでアクセスできますが、リモート ワークステーションからはアクセスできません。また、syslog データは Event Viewer に表示されません。Windows ファイアウォールをディセーブルにするか、問題になっている管理トラフィックを許可する着信ルールを設定する必要があります。

注意　ワークステーションの Windows ファイアウォールをディセーブルにすると、Windows ファイアウォールのイネーブル時に防御されていた悪意のあるアクティビティに対して無防備になります。

- クライアント ソフトウェア インストーラをダウンロードする前に、クライアント システム上の Temp ファイルを手動で削除することを推奨します。このようなファイルを削除することによって、使用可能な十分なスペースを確保できる可能性があります。
- ワークステーションに Cisco Security Agent がインストールされている場合は、クライアントのインストール プロセスの前または中に、それをディセーブルにする必要があります。インストール プロセス中にクライアント インストーラが Cisco Security Agent をディセーブルできなかった場合は、プロセスが中断して、クライアントのインストールを再開する前に、Cisco Security Agent を手動でディセーブルにするように要求されます。

ヒント ワークステーション上の Cisco Security Agent をディセーブルにするには、次の 2 つの方法のいずれかを使用します：(1) システム トレイ内の Cisco Security Agent アイコンを右クリックし、[Security Level] > [Off] を選択するか、(2) [Services] を開き（[Control Panel] > [Administrative Tools] > [Services]）、[Cisco Security Agent] を右クリックし、[Stop] をクリックします。2 つのどちらの方法の場合でも、Windows のバージョンによっては、次の手順を実行する必要があります。[Services] を開き、[Cisco Security Agent Monitor] をクリックして [Stop] をクリックします。クライアントのインストール終了後、Cisco Security Agent を再起動します。

注意 ワークステーション上で Cisco Security Agent がディセーブルになっている間は、Cisco Security Agent のイネーブル時に防御されていた悪意のあるアクティビティに対して無防備になります。

- すでに Security Manager クライアントがワークステーション上にインストールされている場合は、インストール プログラムが最新のクライアントをインストールする前に Security Manager クライアントをアンインストールする必要があります。ウィザードからこの必要があるかどうかが尋ねられます。

手順

ステップ 1　Windows 管理者特権を持つユーザ アカウントを使用してクライアント ワークステーションにログインします。

ステップ 2　Web ブラウザで、次の URL のいずれかを開きます。ここで、*SecManServer* は、Security Manager がインストールされているコンピュータの名前です。いずれかのセキュリティ アラート ウィンドウで [Yes] をクリックします。

- SSL を使用していない場合は、**http://***SecManServer***:1741** を開きます。
- SSL を使用している場合は、**http://***SecManServer***:443** を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。

ステップ 3　ユーザ名と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。初めてサーバをインストールする場合は、ユーザ名の **admin** と製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 4　Cisco Security Management Suite のホームページで、[Cisco Security Manager Client Installer] をクリックします。

ファイルを開くまたは実行するのか、ディスクに保存するのかが尋ねられます。いずれかのオプションを選択できます。ファイルのディスクへの保存を選択した場合は、ファイルのダウンロード後にプログラムを実行します（ファイルをダブルクリックするか、ブラウザから尋ねられたときに [Run] オプションを選択します）。

ヒント 「a problem was detected」や「the publisher cannot be verified」などのアプリケーションに関するセキュリティ警告、または、未確認のアプリケーションがコンピュータにアクセスしようとしているという内容のセキュリティ警告が表示された場合は、アクセスが許可されていることを確認します。複数のボタンをクリックしなければならない場合があります。ボタン名はアプリケーションのプロンプトによって異なります（[Allow]、[Yes]、[Apply] など）。

ステップ 5　インストール ウィザードの [Welcome] 画面が開き、次の文が表示されます。「Install these Cisco Security Manager 4.5 client applications:」

- Configuration Manager
- Event Viewer
- Report Manager
- Health and Performance Manager
- Image Manager
- ダッシュボード

Security Manager クライアントは、6 台のアプリケーション スイートとしてインストールされます。Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Manager およびダッシュボード。各アプリケーションは、次の 3 つの方法のいずれかで別々に起動できます（各アプリケーションの起動方法の詳細については、「Security Manager クライアントを使用した Security Manager へのログイン」（P.6-12）を参照してください）。

- [Start] > [All Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client]
- （ログイン画面）
- （いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）

（注）　Cisco Security Manager のデスクトップ アイコンも作成されます。このアイコンで Cisco Security Management Suite のホーム ページを開きます。

ステップ 6　インストール ウィザードの指示に従います。インストール中に、次の情報の入力が要求されます。

- [Server name]：Security Manager サーバ ソフトウェアがインストールされているサーバの DNS 名または IP アドレス。通常は、クライアント インストーラをダウンロードしたサーバです。
- [Protocol]：HTTPS または HTTP。Security Manager サーバで使用されるプロトコルを選択します。ほとんどのサーバは HTTPS を使用するように設定されます。どれを選択していいかがわからない場合は、システム管理者にお問い合わせください。また、サーバが非デフォルト ポートを使用するように設定されていることがわかっている場合は、「非デフォルト HTTP または HTTPS ポートの設定」（P.6-10）内の情報を使用してインストール後にポートを設定します。
- [Shortcuts]：自分専用のショートカットだけを作成するのか、このワークステーションにログインしているすべてのユーザ アカウント用のショートカットを作成するのか、またはどのユーザ用のショートカットも作成しないのか。これによって、誰の [Start] メニューに Cisco Security Manager Client が表示されるかが決定されます。クライアントは、[Start] > [Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client] またはデスクトップ上のアイコンから起動できます。
- [Installation location]：クライアントをインストールするフォルダ。他の場所にインストールする特別な理由がなければ、デフォルトを受け入れます。デフォルトの場所は、C:\Program Files\Cisco Systems です。

ステップ 7　インストール ウィザードの指示に従って続行します。

ステップ 8　[Done] をクリックしてインストールを完了したら、アンチウイルス アプリケーションを一時的にディセーブルにしていた場合はイネーブルに戻します。

クライアント インストーラによってワークステーション上の Cisco Security Agent が停止されていた場合は、インストールの完了時に再起動されます。ただし、システム上で Cisco Security Agent を手動でディセーブルにしていた場合は、クライアントのインストールが完了してからそれをイネーブルにする必要があります。

インストールを阻止するセキュリティ設定の処理

ワークステーション上のセキュリティ設定を構成可能な複数の方法と、Security Manager クライアントのインストールを阻止するためにインストール可能な複数の製品が存在します。インストール中に問題が発生した場合は、Windows ユーザ アカウントにソフトウェアのインストールに必要な管理特権が付与されていることを確認してから、次のヒントを考慮してください。

- （Windows XP）Internet Explorer セキュリティ強化のデフォルト設定では、サーバからのインストール ユーティリティのダウンロードが阻止される可能性があります。この場合は、次のメッセージが表示されます。

  ```
  Internet Explorer cannot download CSMClientSetup.exe from <server>.Internet Explorer
  was not able to open this Internet site.The requested site is either unavailable or
  cannot be found.Please try again later.
  ```

  この問題を解決するには、[Start] > [Settings] > [Control Panel] > [Add or Remove Programs] を選択してから、[Add/Remove Windows Components] をクリックします。Windows コンポーネント ウィザード ウィンドウで、[Internet Explorer Enhanced Security Configuration] チェックボックスをオフにして、[Next] をクリックし、[Finish] をクリックします。
- （Windows XP SP2）向上したセキュリティ機能によって、次のメッセージが表示される可能性があります。

  ```
  Security Warning Message.The publisher could not be verified.Are you sure you want to
  run this software?
  ```

  このメッセージが表示されたら、[Yes] をクリックして継続します。

非デフォルト HTTP または HTTPS ポートの設定

Security Manager サーバは、443 の HTTPS と 1741 の HTTP のデフォルト ポートを使用します。組織で別のポートを使用するように Security Manager サーバをインストールしていた場合は、非標準ポートを使用するようにクライアントを設定する必要があります。そうしなければ、クライアントとサーバを接続できません。

クライアントの別のポートを設定するには、メモ帳などのテキスト エディタを使用して **C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars\client.info** ファイルを編集します。次の設定を追加して、<*port number*> の場所にカスタム ポート番号を指定します。

- HTTPS_PORT=<*port number*>
- HTTP_PORT=<*port number*>

これらの設定は、次のクライアントを起動したときに使用されます。

以前のバージョンのクライアントからアップグレードできない

古いバージョンのクライアントがインストールされている、または、クライアントがインストールされていたことがあるワークステーション上に Security Manager クライアントをインストールしようとした場合は、クライアント インストーラによって新しいバージョンがインストールされる前に古いバージョンがアンインストールされます。「Could not find main class.Program will exit」というエラー メッセージが表示された場合は、インストーラでクライアントをインストールできません。

手順

この問題は、システム内に古いレジストリ エントリが残っている場合に発生します。この問題を解決するには、次の手順を実行します。

ステップ 1　[Start] > [Run] を選択して、**regedit** と入力することによって、レジストリ エディタを起動します。

ステップ 2　次のレジストリ キーを削除します。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\f427e21299b0dd254754c0d2778feec4-837992615

ステップ 3　以前のインストール ディレクトリ（通常は、C:\Program Files\Cisco Systems\Cisco Security Manager Client）を削除します。

ステップ 4　次のフォルダの名前を変更します。

C:\Program Files\Common Files\InstallShield\Universal\common\Gen1

ステップ 5　[Start] > [Control Panel] > [Add or Remove Programs] を選択します。Cisco Security Manager Client がまだ表示されている場合は、[Remove] をクリックします。「Program already removed; do you want to remove it from the list?」というメッセージが表示されたら、[Yes] をクリックします。

まだ Security Manager クライアントを再インストールできない場合は、C:\Program Files\Common Files\InstallShield ディレクトリの名前を変更して、もう一度試してみてください。「インストール中のクライアント障害」（P.A-10）も参照してください。

クライアントのパッチング

サービス パックまたはポイント パッチを Security Manager サーバに適用したら、サーバにログインしたときに Security Manager クライアントからアップデートを適用するかどうかが尋ねられます。クライアント ソフトウェアのバージョン番号は、サーバ ソフトウェアのバージョン番号と同じにする必要があります。

必要なソフトウェア アップデートをダウンロードして適用するかどうかが尋ねられた場合は、Web ブラウザがアップデートのダウンロードに使用されます。ファイルを開くまたは実行するのか、ディスクに保存するのかが尋ねられます。いずれかのオプションを選択できます。ファイルのディスクへの保存を選択した場合は、ファイルのダウンロード後にプログラムを実行します（ファイルをダブルクリックするか、ブラウザから尋ねられたときに [Run] オプションを選択します）。

パッチのインストールは、クライアントのインストールに似ているため、Cisco Security Agent またはインストーラの起動を可能にするためにインストールしたその他のセキュリティ ソフトウェアからの任意のセキュリティ アラートを許可（または [Yes] をクリック）する必要があります。

インストールの場所が尋ねられたら、クライアントがインストールされているフォルダが選択されていることを確認して、ファイルを上書きするかどうかが尋ねられたら [Yes to All] を選択します。

ヒント　URL が取得できない、または、接続がタイムアウトしたことを伝えるエラー メッセージが表示された場合は、Security Manager クライアントをアンインストールしてから、フレッシュ コピー（すでにパッチが適用されている）をインストールする必要があります。詳細については、「Security Manager クライアントのアンインストール」（P.6-14）および「Security Manager クライアントのインストール」（P.6-7）を参照してください。

アプリケーションへのログイン

サーバ アプリケーションをインストールし、Web ブラウザを設定し、Security Manager クライアントをインストールしたら、アプリケーションにログインできます。

Security Manager クライアントを使用した Security Manager へのログイン

Security Manager クライアントは、6 台のアプリケーション スイートとしてインストールされます。Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Manager およびダッシュボード。各アプリケーションは、後述の手順内で示される 3 つの方法のいずれかで別々に起動できます。

ほとんどの Security Manager タスクは、Configuration Manager アプリケーション（Security Manager クライアント アプリケーション スイートの一部）を使用して実行します。

ヒント　Security Manager クライアントを十分に活用できる管理者特権が付与された Windows ユーザ アカウントを使用してクライアント ワークステーションにログインする必要があります。より低い特権を使用してクライアントを操作しようとした場合は、一部の機能が正しく機能しない場合があります。

手順

ステップ 1　Configuration Manager、Event Viewer、Report Manager、Health and Performance Monitor、Image Manager またはダッシュボードのいずれかを起動します。各アプリケーションは、次の 3 つの方法のいずれかで別々に起動できます。

- [Start] > [All Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client]
- （ログイン画面）
- （いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）。ログイン ダイアログ ウィンドウは表示されません。

ステップ 2　Security Manager のログイン ダイアログ ウィンドウで、ログインするサーバの DNS 名を入力または選択します。

（注）　DNS 名ではなく IP アドレスを入力または選択すると、Internet Explorer 7 環境において一部の機能が意図したとおりに動作しない可能性があります。すべての Security Manager 機能を正しく動作させるには、ログインするサーバの DNS 名を入力します。

ステップ 3　Security Manager のユーザ名とパスワードを入力します。

ステップ 4　サーバが接続に HTTPS を使用する場合は、[HTTPS] チェックボックスがオンになっていることを確認します。HTTPS を使用しない場合は、そのチェックボックスをオフにします。[Login] をクリックします。

ステップ 5　サーバからクライアント ソフトウェア アップデートのダウンロードとインストールが要求された場合は、「クライアントのパッチング」（P.6-11）を参照してください。

ステップ 6　ご使用のクライアントよりも新しいバージョンを実行している Security Manager サーバにログインすると、通知が表示され、一致するクライアント バージョンをダウンロードするオプションが提供されます。

ステップ 7　入力したユーザ名とパスワードで実行中のセッションがない場合は、クライアント アプリケーション（Configuration Manager、Event Viewer、Report Manager、Health and Performance Monitor、Image Manager、またはダッシュボード）がサーバにログインして、クライアント インターフェイスを開きます。

ステップ 8　入力したユーザ名とパスワードで実行中のセッションがすでに存在する場合は、既存のアプリケーションから同一セッションで新しいアプリケーションを簡単に起動できる方法があることを知らせる情報メッセージが表示されます。その方法とは、次のとおりです。

（いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）。

ステップ 9　新しいアプリケーションが既存のセッションから起動されるか、すでに実行中ならばそのアプリケーションがフォーカス状態になります。

ヒント　クライアントは 120 分間アイドル状態が続くと自動的に閉じます。アイドル タイムアウトを変更するには、[Tools] > [Security Manager Administration] を選択して、目次から [Customize Desktop] を選択し、必要なタイムアウト期間を入力します。この機能をディセーブルにして、クライアントが自動的に閉じないようにすることもできます。

ステップ 10　Security Manager を終了する場合は、[File] > [Exit] を選択します。

Web ブラウザを使用したサーバ アプリケーションへのログイン

正規の Windows アプリケーションを使用してクライアント アプリケーションをホストするのは、Security Manager サーバだけです。Security Manager（Common Services アプリケーション経由）、CiscoWorks、および Auto Update Server のサーバ管理機能を含め、その他すべてのアプリケーションは Web ブラウザ内でホストされます。

これらのアプリケーションへのログイン方法は同じです。1 台のサーバ上に複数のアプリケーションをインストールした場合は、インストールしたすべてのアプリケーションに同時にログインします。これは、ログインが CiscoWorks によって制御され、これらのアプリケーションはすべて CiscoWorks の制御下でホストされるためです。

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。*server* は、サーバ アプリケーションがインストールされているコンピュータの名前です。いずれかのセキュリティ アラート ウィンドウで [Yes] をクリックします。

- SSL を使用していない場合は、http://*server*:1741 を開きます。
- SSL を使用している場合は、http://*server*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。アプリケーションを実行するようにブラウザを設定する方法については、「Web ブラウザ クライアントの設定」（P.6-1）を参照してください。

ステップ 2　ユーザ名と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。初めてサーバをインストールする場合は、ユーザ名の **admin** と製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 3　Cisco Security Management Suite のホームページで、サーバ上にインストールされた機能にアクセスできます。このホームページには、インストールされているものによって異なる項目を含めることができます。

- 実行するアプリケーション（**Auto Update Server** など）に対応するパネルをクリックします。
- [Server Administration] パネルをクリックして、CiscoWorks Common Services サーバ メニューを開きます。このリンクをクリックすれば、Common Services 内の任意の場所に移動できます。CiscoWorks Common Services は、サーバを管理する基盤ソフトウェアです。このソフトウェアを使用して、サーバの保守とトラブルシューティングやローカル ユーザ定義などのバックエンド サーバ機能を設定して管理します。
- [CiscoWorks] リンク（ページの右上）をクリックして、サーバ上で CiscoWorks ホームページを開きます。
- [Cisco Security Manager Client Installer] をクリックして、Security Manager クライアントをインストールします。このクライアントは、Security Manager サーバを使用するためのメイン インターフェイスです。

ステップ 4　アプリケーションを終了するには、画面右上にある [Logout] をクリックします。ホームページと Security Manager クライアントの両方を同時に開いている場合は、ブラウザ接続を終了しても Security Manager クライアントが終了しません。

Security Manager クライアントのアンインストール

Security Manager クライアントをアンインストールする場合は、[Start] > [Programs] > [Cisco Security Manager Client] > [Uninstall Cisco Security Manager Client] を選択して、アンインストール ウィザードの指示に従います。