CHAPTER 40

Trend Micro Content Security の設定

この章では、CSC SSM 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。

- CSC SSM への接続（P. 40-2）
- CSC SSM の管理（P. 40-3）
- CSC SSM のセットアップ（P. 40-9）
- Web（P. 40-21）
- Mail（P. 40-22）
- File Transfer（P. 40-24）
- Updates（P. 40-25）

CSC SSM への接続

ASDM で各セッションを開始する際、CSC SSM 関連機能への初回アクセス時に、管理 IP アドレスを指定し、CSC SSM のパスワードを入力する必要があります。CSC SSM に正常に接続すると、管理 IP アドレスとパスワードの入力を再度要求されることはありません。新しい ASDM セッションを開始する場合、CSC SSM への接続はリセットされ、IP アドレスと CSC SSM パスワードをもう一度入力する必要があります。また、適応型セキュリティ アプライアンスの時間帯を変更したときも、CSC SSM への接続がリセットされます。

（注） CSC SSM には、ASDM のパスワードとは別に保持されるパスワードがあります。2 つのパスワードを同一に設定できますが、CSC SSM のパスワードを変更しても ASDM のパスワードは変更されません。

CSC SSM に接続するには、次の手順を実行します。

ステップ 1　ASDM アプリケーションのメイン ウィンドウで、**Content Security** タブをクリックします。

ステップ 2　Connecting to CSC ダイアログボックスで、次のオプションのいずれかを選択します。

- Management IP Address：SSM の管理ポートの IP アドレスに接続します。ASDM では、適応型セキュリティ アプライアンスの SSM の IP アドレスを自動的に検出します。検出できない場合は、管理 IP アドレスを手動で指定できます。
- Other IP Address or Hostname：SSM の代替 IP アドレスまたはホスト名に接続します。

ステップ 3　Port フィールドにポート番号を入力し、**Continue** をクリックします。

ステップ 4　CSC Password ダイアログボックスで、CSC パスワードを入力し、**OK** をクリックします。

（注） CSC Setup Wizard を完了していない場合は、Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup ウィンドウで CSC Setup Wizard の設定を完了します。ここでは、デフォルトのパスワード「cisco」の変更も行います。

パスワードの入力後 10 分間は、CSC SSM GUI の他の部分にアクセスするために CSC SSM パスワードを再入力する必要はありません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC SSM の管理

この項では、CSC SSM を管理する方法について説明します。次の項目を取り上げます。

- CSC SSM について（P. 40-3）
- CSC SSM の準備（P. 40-4）
- スキャンするトラフィックの指定（P. 40-6）
- CSC スキャンのルール アクション（P. 40-8）

CSC SSM について

ASDM では、アクティベーション コードなど、Content Security and Control（CSC）SSM および CSC 関連機能の基本操作パラメータを設定できます。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、CSC SSM をサポートします。CSC SSM は、Content Security and Control ソフトウェアを実行します。CSC SSM により、ウイルス、スパイウェア、スパム、およびその他の不要トラフィックから保護されます。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように適応型セキュリティ アプライアンスを設定しておきます。

（注） CSC SSM は、適応型セキュリティ アプライアンスで FTP 検査がイネーブルの場合にのみ、FTP ファイル転送をスキャンできます。デフォルトでは、FTP 検査はイネーブルです。

システムの設定と CSC SSM の監視には、ASDM を使用します。CSC SSM ソフトウェアにコンテンツ セキュリティ ポリシーを設定するには、ASDM 内のリンクをクリックして、CSC SSM の Web ベース GUI にアクセスします。別の Web ブラウザ ウィンドウに CSC SSM GUI が表示されます。CSC SSM にアクセスするには、CSC SSM パスワードを入力する必要があります。CSC SSM GUI を使用するには、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

（注） ASDM と CSC SSM では、別個のパスワードが保持されています。それらのパスワードを同一にすることはできますが、2 つのパスワードのうち一方を変更しても、もう一方に影響することはありません。

ASDM を実行しているホストと適応型セキュリティ アプライアンスの間の接続は、適応型セキュリティ アプライアンスの管理ポートを通じて確立されます。CSC SSM GUI への接続は、SSM の管理ポートを通じて確立されます。これら 2 つの接続は CSC SSM の管理に必要であるため、ASDM を実行しているすべてのホストは適応型セキュリティ アプライアンスの管理ポートと SSM の管理ポートの両方の IP アドレスに到達できる必要があります。

CSC SSM の準備

CSC SSM のセキュリティ効果を得るには、SSM のハードウェア インストールだけでなく、他にもいくつかのステップを実行する必要があります。

適応型セキュリティ アプライアンスおよび CSC SSM を設定するには、次の手順を実行します。

ステップ 1　CSC SSM が Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスにプレインストールされていない場合は、CSC SSM をインストールし、ネットワーク ケーブルを SSM の管理ポートに接続します。SSM のインストールと接続については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

CSC SSM ソフトウェアの管理と自動アップデートを可能にするには、CSC SSM の管理ポートがネットワークに接続されている必要があります。また、CSC SSM は、電子メール通知とシステム ログ メッセージ生成にも管理ポートを使用します。

ステップ 2　CSC SSM には、Product Authorization Key（PAK）が付属しています。PAK を使用して、次の URL で CSC SSM を登録します。

http://www.cisco.com/go/license

登録すると、アクティベーション キーが電子メールで届きます。ステップ 5 を完了するには、アクティベーション キーが必要です。

ステップ 3　ステップ 5 で必要となる次の情報を収集します。

- ステップ 2 を完了した後に受信したアクティベーション キー。
- SSM 管理ポートの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス。SSM 管理ポートの IP アドレスは、ASDM の実行に使用するホストがアクセスできるものである必要があります。SSM 管理ポートの IP アドレスと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、異なるサブネットに属していてもかまいません。
- DNS サーバの IP アドレス。
- HTTP プロキシ サーバの IP アドレス（セキュリティ ポリシーで、インターネットへの HTTP アクセスにプロキシ サーバの使用が求められている場合に限り必要）。
- SSM のドメイン名とホスト名。
- 電子メール通知に使用する、電子メール アドレスおよび SMTP サーバの IP アドレスとポート番号。
- CSC SSM を管理できるホストまたはネットワークの IP アドレス。
- CSC SSM 用のパスワード。

ステップ 4　ASDM で、セキュリティ アプライアンス上の時刻設定を確認します。時刻設定が正確であることは、セキュリティ イベントのロギングや CSC SSM ソフトウェアの自動アップデートで重要です。

- 時刻設定を手動で制御する場合は、時間帯を含むクロック設定を確認します。**Configuration > Device Setup > System Time > Clock** を選択します。
- NTP を使用している場合は、NTP 設定を確認します。**Configuration > Device Setup > System Time > NTP** を選択します。

ステップ 5　CSC Setup Wizard を終了します。

- **Configuration > Trend Micro Content Security** を選択します。CSC SSM に接続しログインします。**CSC Setup > Wizard Setup** を選択し、**Launch Setup Wizard** をクリックします。
- CSC Setup Wizard を再度実行する場合、上記の箇条書きと同じ手順を実行します。

CSC Setup Wizard については、**Help** をクリックします。

ステップ 6　サービス ポリシーを設定して、スキャンするトラフィックを CSC SSM に誘導します。

グローバル ポリシーを作成してスキャンするトラフィックを誘導する場合、サポートされているプロトコルのトラフィック（着信と発信）がすべてスキャンされます。適応型セキュリティ アプライアンスおよび CSC SSM のパフォーマンスを最大化するために、信用できない送信元からのトラフィックのみスキャンしてください。

トラフィックを CSC SSM に誘導するための最良の方法については、P.40-6 の「スキャンするトラフィックの指定」を参照してください。

スキャンするトラフィックを誘導するグローバル ポリシーを作成する場合は、次の手順を実行します。

a. **Configuration > Firewall > Service Policy Rules** を選択して、**Add** をクリックします。

Add Service Policy Rule Wizard ウィンドウが表示されます。

b. **Global - applies to all interfaces** オプションをクリックして、**Next >** をクリックします。

Traffic Classification Criteria ウィンドウが表示されます。

c. **Create a new traffic class** オプションをクリックして、隣のフィールドにトラフィック クラスの名前を入力し、**Any traffic** チェックボックスをオンにしてから、**Next >** をクリックします。

Rules Actions ウィンドウが表示されます。

d. **CSC Scan** タブをクリックして、**Enable CSC scan for this traffic flow** チェックボックスをオンにします。

e. **If CSC card fails, then** というラベルの付いた領域で適切な選択を行って、CSC SSM が使用不可の場合に、選択したトラフィックの通過をセキュリティ アプライアンスで許可するか拒否するかを選択します。

f. **Finish** をクリックします。

Service Policy Rules ペインに新しいサービス ポリシーが表示されます。

g. **Apply** をクリックします。

適応型セキュリティ アプライアンスは、購入したライセンスによってイネーブルになったコンテンツ セキュリティ スキャンを実行する CSC SSM へのトラフィックの誘導を開始します。

ステップ 7　（オプション）CSC SSM GUI で、デフォルトのコンテンツ セキュリティ ポリシーを確認します。デフォルトのコンテンツ セキュリティ ポリシーは、ほとんどの実装に適しています。これらの修正には高度な設定が必要であるため、必ず『*Cisco Content Security and Control SSM Administrator Guide*』を読んでから実行してください。

（注）　コンテンツ セキュリティ ポリシーを確認するには、イネーブルになっている機能を CSC SSM GUI で表示します。使用できる機能は、購入したライセンスによって異なります。デフォルトでは、購入したライセンスに含まれているすべての機能がイネーブルです。

基本ライセンスの場合、デフォルトでイネーブルになっている機能は、SMTP ウイルス スキャン、POP3 のウイルス スキャンとコンテンツ フィルタリング、Web メール ウイルス スキャン、HTTP ファイル ブロッキング、FTP のウイルス スキャンとファイル ブロッキング、ロギング、および自動アップデートです。

Plus ライセンスのデフォルトでイネーブルになっている追加機能は、SMTP アンチスパム、SMTP コンテンツ フィルタリング、POP3 アンチスパム、URL ブロッキング、および URL フィルタリングです。

ASDM の CSC SSM GUI にアクセスするには、**Configuration > Trend Micro Content Security** を選択し、**Web**、**Mail**、**File Transfer**、**Updates** のいずれかのリンクをクリックします。CSC SSM GUI を開くには、これらのペイン上のいずれかのリンクをクリックします。

スキャンするトラフィックの指定

CSC SSM は、FTP、HTTP、POP3、SMTP のトラフィックをスキャンできますが、これらのプロトコルは、接続要求パケットの宛先ポートがそのプロトコルに設定されたポートである場合に限りサポートされます。CSC SSM がスキャンできるのは次の接続だけです。

- TCP ポート 21 に対して開かれた FTP 接続
- TCP ポート 80 に対して開かれた HTTP 接続
- TCP ポート 110 に対して開かれた POP3 接続
- TCP ポート 25 に対して開かれた SMTP 接続

これらすべてのプロトコルのトラフィックをスキャンすることも、任意の組み合せをスキャンすることもできます。たとえば、ネットワーク ユーザに POP3 電子メールの受信を許可しない場合に、POP3 トラフィックを CSC SSM に誘導するように適応型セキュリティ アプライアンスを設定する必要はありません。代わりに、POP3 トラフィックをブロックするように設定できます。

適応型セキュリティ アプライアンスと CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先の間のトラフィックなど、スキャンする必要のないトラフィックまでも誘導すると、ネットワーク パフォーマンスに悪影響を与える可能性があります。

（注）　最初にトラフィックが CSC 検査用に分類されるとき、フローに基づいて分類されます。トラフィックが既存の接続の一部である場合、その接続のポリシー セットに直接移動します。

Add Service Policy Rule Wizard Rule Actions ウィンドウの CSC Scan タブで、CSC SSM でのトラフィック スキャンをイネーブルにします。CSC スキャンが含まれるサービス ポリシーはグローバルに適用することも、特定のインターフェイスに適用することもできるため、CSC スキャンについても、グローバルにイネーブルにするか、特定のインターフェイスに対してイネーブルにするかを選択できます。詳細については、P.40-8 の「CSC スキャンのルール アクション」を参照してください。

csc コマンドをグローバル ポリシーに追加すると、適応型セキュリティ アプライアンスを通過する暗号化されていないすべての接続は、確実に CSC SSM でスキャンされます。ただし、このように設定すると、信頼できる送信元からのトラフィックが不必要にスキャンされることもあります。

CSC スキャンをインターフェイス固有のサービス ポリシーでイネーブルにした場合、これらのスキャンは双方向性を持ちます。双方向性のスキャンとは、適応型セキュリティ アプライアンスが新しい接続を開くとき、その接続の着信インターフェイスまたは発信インターフェイスのいずれかで CSC スキャンがアクティブで、サービス ポリシーでスキャン対象のトラフィックが特定されていれば、適応型セキュリティ アプライアンスはそのトラフィックを CSC SSM に誘導するということです。また、スキャンに双方向性があることにより、特定のインターフェイスを通過するサポート対象のトラフィック タイプを CSC SSM に誘導した場合に、信頼できる内部ネットワークからのトラフィックに対して不必要なスキャンを実行する可能性もあります。たとえば、DMZ ネットワークの Web サーバから要求された URL およびファイルが内部ネットワークのホストに対してコンテンツ セキュリティ リスクをもたらす可能性は低いため、そのようなトラフィックを適応型セキュリティ アプライアンスで CSC SSM に誘導する必要はほとんどありません。

したがって、CSC スキャンを定義するサービス ポリシーでアクセスリストを使用して、選択したトラフィックを制限することを強くお勧めします。特に、次の接続と一致するアクセスリストを使用することをお勧めします。

- 外部ネットワークへの HTTP 接続
- 適応型セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部サーバへの FTP 接続
- 適応型セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部サーバへの POP3 接続
- 内部メール サーバを宛先とする着信 SMTP 接続

inside-policy では、最初のクラス inside-class1 によって、適応型セキュリティ アプライアンスが内部ネットワークと DMZ ネットワークの間の HTTP トラフィックをスキャンしないようにします。Match カラムは、「Do not match」アイコンを表示することでこの設定を示します。この設定は、192.168.10.0 ネットワークから 192.168.20.0 ネットワークの TCP ポート 80 に送信されたトラフィックを適応型セキュリティ アプライアンスがブロックするという意味ではありません。この設定は、トラフィックを内部インターフェイスに適用されるサービス ポリシーによる照合から免除することで、適応型セキュリティ アプライアンスがこのトラフィックを CSC SSM に送信できないようにするという意味です。

inside-policy の 2 つ目のクラス inside-class は、内部ネットワークとすべての宛先間の FTP、HTTP、および POP3 トラフィックを照合します。inside-class1 設定によって、DMZ ネットワークへの HTTP 接続は免除されます。前述のとおり、特定のインターフェイスに CSC スキャンを適用するポリシーは、着信トラフィックと発信トラフィックの両方に対して有効ですが、送信元ネットワークとして 192.168.10.0 を指定することで、inside-class1 は内部ネットワークのホストによって開始された接続のみと照合します。

outside-policy では、outside-class は外部の送信元から DMZ ネットワークへの SMTP トラフィックを照合します。この設定によって、SMTP サーバを保護し、SMTP クライアントからサーバへの接続をスキャンせずに、DMZ ネットワーク上の SMTP サーバから電子メールをダウンロードする内部ユーザを保護します。

DMZ ネットワークの Web サーバで、HTTP によって外部ホストからアップロードされるファイルを受け取る場合、すべての送信元から DMZ ネットワークへの HTTP トラフィックを照合する外部ポリシーにルールを追加できます。このポリシーは外部インターフェイスに適用されるため、ルールは、適応型セキュリティ アプライアンス外の HTTP クライアントからの接続のみを照合します。

CSC スキャンのルール アクション

CSC Scan タブでは、CSC SSM が、現在のトラフィック クラスによって特定されるトラフィックをスキャンするかどうかを判別できます。このタブは、CSC SSM を適応型セキュリティ アプライアンスにインストールしないと表示されません。

CSC SSM は、HTTP、SMTP、POP3、および FTP のトラフィックのみをスキャンします。使用するサービス ポリシーに、これら 4 種類のプロトコル以外のプロトコルをサポートするトラフィックが含まれていると、他のプロトコルのパケットは、スキャンされることなく CSC SSM を通過します。CSC SSM の負荷を軽減するには、CSC SSM にパケットを送信するサービス ポリシー ルールで、HTTP、SMTP、POP3、または FTP トラフィックのみをサポートするように設定します。

フィールド

- Enable CSC scan for this traffic flow：このトラフィック フローでの CSC SSM の使用をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- If CSC card fails：CSC SSM が動作不能になった場合に実行するアクションを設定します。
  - Permit traffic：CSC SSM で障害が発生した場合はトラフィックを許可します。
  - Close traffic：CSC SSM で障害が発生した場合はトラフィックをブロックします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC SSM のセットアップ

CSC Setup の各ペインで、CSC SSM の基本操作パラメータを設定できます。各ペインで個別に設定する前に、少なくとも 1 回 CSC Setup Wizard を実行する必要があります。CSC Setup Wizard を終了した後は、このウィザードを再度使用しなくても各ペインを個別に変更できます。

また、CSC Setup Wizard が完了するまで、Home > Trend Micro Content Security > Content Security Tab or Monitoring > Trend Micro Content Security > Content Security タブのペインにアクセスできません。このウィザードが完了する前にそれらのペインにアクセスしようとすると、ダイアログボックスが表示され、そこからウィザードに直接アクセスして設定を完了させることができます。

CSC SSM の概要については、P.40-3 の「CSC SSM について」を参照してください。詳細については、次の項目を参照してください。

- Activation/License（P. 40-9）
- IP Configuration（P. 40-10）
- Host/Notification Settings（P. 40-11）
- Management Access Host/Networks（P. 40-12）
- Password（P. 40-13）
- デフォルト パスワードの復元（P. 40-13）
- Wizard Setup（P. 40-14）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、CSC Setup ノードのペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Activation/License

Activation/License ペインでは、CSC SSM の次の 2 つのコンポーネントにアクティベーション コードを設定できます。

- 基本ライセンス
- Plus ライセンス

ASDM を使用して、2 つのライセンスにそれぞれ一度だけ CSC ライセンスを設定できます。ソフトウェアのアップデートをスケジュールしておくと、更新されたライセンス アクティベーション コードが自動的にダウンロードされます。ライセンス ステータス ページと CSC UI ホームページへのリンクがこのウィンドウの下部に表示されます。割り当てられたライセンスのシリアル番号が自動的に入力されます。

フィールド

- Product：表示のみ。コンポーネントの名前を表示します。
- Activation Code：対応する Product フィールドのアクティベーション コードが含まれています。
- License Status：表示のみ。ライセンスのステータスに関する情報を表示します。ライセンスが有効な場合、有効期限が表示されます。有効期限が過ぎている場合は、このフィールドにライセンスの有効期限が切れている旨が表示されます。
- Nodes：表示のみ。CSC SSM の基本ライセンスでサポートされているネットワーク デバイスの最大数が表示されます。Plus ライセンスはサポートされているネットワーク デバイスの数に影響しません。したがって、Plus License 領域には Nodes フィールドが表示されません。
- 表示されたリンクをクリックしてライセンス ステータスを確認するか、ライセンスを更新します。
- 表示されたリンクをクリックして ASDM の CSC ホームページに移動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、Activation/License ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

IP Configuration

IP Configuration ペインでは、CSC SSM の IP アドレスやその他の関連情報、使用する DNS サーバ、および CSC SSM ソフトウェアのアップデートを取得するためのプロキシ サーバを設定できます。

フィールド

- Management Interface：CSC SSM への管理アクセスのためのパラメータが含まれています。
  - IP Address：CSC SSM への管理アクセスのための IP アドレスを設定します。
  - Mask：CSC SSM の管理 IP アドレスが含まれるネットワークのネットマスクを設定します。
  - Gateway：CSC SSM の管理 IP アドレスが含まれるネットワークのゲートウェイ デバイスの IP アドレスを設定します。
- DNS Servers：CSC SSM の管理 IP アドレスが含まれるネットワークの DNS サーバに関するパラメータが含まれています。
  - Primary DNS：プライマリ DNS サーバの IP アドレスを設定します。
  - Secondary DNS：（オプション）セカンダリ DNS サーバの IP アドレスを設定します。
- Proxy Server：CSC SSM が CSC SSM ソフトウェアのアップデート サーバに接続するために使用する、オプションの HTTP プロキシ サーバのパラメータが含まれています。ネットワーク コンフィギュレーションが、CSC SSM でプロキシ サーバの使用を必要としていない場合、このグループのフィールドを空白のままにできます。
  - Proxy Server：（オプション）プロキシ サーバの IP アドレスを設定します。
  - Proxy Port：（オプション）プロキシ サーバの受信ポートを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、IP Configuration ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Host/Notification Settings

Host/Notification Settings ペインでは、ホスト名、ドメイン名、電子メール通知、および詳細なスキャンから除外する電子メールのドメイン名に関する詳細を設定できます。

フィールド

- Host and Domain Names：CSC SSM のホスト名とドメイン名に関する情報が含まれています。
  - HostName：CSC SSM のホスト名を設定します。
  - Domain Name：CSC SSM が含まれているドメイン名を設定します。
- Incoming E-mail Domain Name：SMTP ベースの電子メールに対する信頼できる着信電子メール ドメイン名の情報が含まれています。
  - Incoming Email Domain：着信電子メールのドメイン名を設定します。CSC SSM は、このドメインに送信された SMTP 電子メールをスキャンします。CSC SSM がスキャンする脅威のタイプは、購入した CSC SSM のライセンスと、CSC SSM ソフトウェアのコンフィギュレーションによって異なります。

（注） CSC SSM では、さまざまな着信電子メールのドメイン リストを設定できます。ASDM には、リストの最初のドメインのみが表示されます。着信電子メールのドメインを追加設定するには、CSC SSM インターフェイスにアクセスします。そのためには、**Configuration > Trend Micro Content Security > Email** を選択し、リンクのいずれかをクリックします。CSC SSM にログインしたら、**Mail (SMTP) > Configuration** を選択して **Incoming Mail** タブをクリックします。

- Notification Settings：イベントの電子メール通知に必要な情報が含まれています。
  - Administrator E-mail：電子メール通知の送信先となるアカウントの電子メール アドレスを設定します。
  - E-mail Server IP Address：SMTP サーバの IP アドレスを設定します。
  - Port：SMTP サーバがリスンするポートを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、Host/Notification Settings ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Management Access Host/Networks

Management Access Host/Networks ペインでは、CSC SSM への管理アクセスを許可するホストとネットワークを制御できます。許可するホストまたはネットワークを 1 つ以上指定する必要があります。許可するホストとネットワークは 8 つまで指定できます。

フィールド

- IP Address：Selected Hosts/Network リストに追加するホストまたはネットワークのアドレスを設定します。
- Mask：IP Address フィールドに指定したホストまたはネットワークのネットマスクを設定します。

  すべてのホストとネットワークを許可するには、IP Address フィールドに **0.0.0.0** と入力し、Mask リストから **0.0.0.0** を選択します。
- Selected Hosts/Networks：CSC SSM への管理アクセスに信頼できるホストまたはネットワークが表示されます。ASDM では、ホストまたはネットワークを 1 つ以上設定する必要があります。ホストとネットワークは 8 つまで設定できます。

  リストからホストまたはネットワークを削除するには、リストでエントリを選択して **Delete** をクリックします。
- Add >>：Selected Hosts/Network リストに、IP Address フィールドで指定したホストまたはネットワークを追加します。
- Delete：Selected Hosts/Networks リストで選択したホストまたはネットワークを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、Management Access Host/Networks ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Password

Password ペインでは、CSC SSM への管理アクセスに必要なパスワードを変更できます。CSC SSM には、ASDM のパスワードとは別に保持されるパスワードがあります。それらに同じパスワードを設定できますが、CSC SSM のパスワードを変更しても ASDM のパスワードは変更されません。

ASDM が CSC SSM に接続されているときに CSC SSM パスワードを変更すると、CSC SSM への接続はドロップされます。その結果、ASDM には確認ダイアログボックスが表示されるので、パスワードを変更する前に応答する必要があります。

ヒント　CSC SSM への接続がドロップされた場合は、常にその接続を再確立できます。そのためには、ステータスバーの **Connection to Device** アイコンをクリックして Connection to Device ダイアログボックスを表示し、**Reconnect** をクリックします。ASDM には CSC SSM パスワードを入力するプロンプトが表示されるので、定義した新しいパスワードを入力します。

パスワードの長さは、5 ～ 32 文字で指定します。

パスワードを入力するとアスタリスクで表示されます。

（注）　デフォルトのパスワードは「cisco」です。

フィールド

- Old Password：CSC SSM に管理アクセスするために現在のパスワードが必要です。
- New Password：CSC SSM に管理アクセスするための新しいパスワードを設定します。
- Confirm New Password：CSC SSM に管理アクセスするための新しいパスワードを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、Password ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」

デフォルト パスワードの復元

ASDM を使用して CSC SSM のパスワードをリセットできます。このパスワードは、「cisco」（かぎカッコなし）というデフォルト値に戻すことができます。CSC パスワードリセット ポリシーが「Denied」に設定されていると、ASDM CLI を使用してパスワードをリセットすることはできません。このポリシーを変更するには、CSC SSM のセッションを開始する必要があります。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

（注）　SSM がインストールされていないと、このオプションはメニューに表示されません。

CSC SSM パスワードをデフォルト値にリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーで、**Tools > CSC Password Reset** を選択します。

CSC Password Reset confirmation ダイアログボックスが表示されます。

ステップ 2　**OK** をクリックして、CSC SSM パスワードをデフォルト値にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。パスワードがリセットされなかったときは、適応型セキュリティ アプライアンスでバージョン 8.0（2）のソフトウェアを使用していること、および CSC SSM で最新のバージョン 6.1.x ソフトウェアを使用していることを確認してください。

ステップ 3　**Close** をクリックしてダイアログボックスを閉じます。

ステップ 4　パスワードをリセットしたら、一意のパスワードに変更する必要があります。

（注）　この機能は、システム コンテキストのマルチコンテキスト モードのみで使用できます。

詳細情報

P.40-13 の「Password」を参照してください。

Wizard Setup

Wizard Setup ペインでは、CSC Setup Wizard を起動できます。

CSC Setup で他のペインに直接アクセスする前に、CSC Setup Wizard を完了する必要があります。このウィザードには、次のペインがあります。

- CSC Setup Wizard Activation Codes Configuration（P. 40-15）
- CSC Setup Wizard IP Configuration（P. 40-16）
- CSC Setup Wizard Host Configuration（P. 40-16）
- CSC Setup Wizard Management Access Configuration（P. 40-17）
- CSC Setup Wizard Password Configuration（P. 40-17）
- CSC Setup Wizard Traffic Selection for CSC Scan（P. 40-18）
- CSC Setup Wizard Summary（P. 40-19）

CSC Setup Wizard を完了したら、CSC Setup Wizard を再度使用することなく CSC SSM に関連するペインで設定を変更できます。

フィールド

- Launch Setup Wizard：CSC Setup Wizard を起動します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	• [1]	—

1. マルチコンテキスト モードでは、Wizard Setup ペインは管理コンテキストのみで使用できます。

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC Setup Wizard Activation Codes Configuration

CSC Setup Wizard Activation Codes Configuration ウィンドウには、CSC SSM の機能をイネーブルにするために入力したアクティベーション コードが、ライセンスのタイプに応じて表示されます。

フィールド

- Activation Codes：表示のみ。このウィンドウで行ったアクティベーション コードの設定を表示します。
  - Base License：アクティベーション コードを表示します。基本ライセンスには、アンチウイルス、アンチスパイウェア、およびファイル ブロッキングが含まれます。
  - Plus License：アクティベーション コードを入力した場合は、そのアクティベーション コードを表示します。入力していないときは、空白になります。Plus ライセンスには、アンチスパム、アンチフィッシング、コンテンツ フィルタリング、および URL ブロッキングと URL フィルタリングが含まれます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC Setup Wizard IP Configuration

CSC Setup Wizard IP Configuration ウィンドウには、CSC SSM 用に入力した IP コンフィギュレーション設定が表示されます。

フィールド

- IP Address：CSC SSM の管理インターフェイスの IP アドレスを表示します。
- Mask：ドロップダウン リストから選択した CSC SSM の管理インターフェイスのネットワーク マスクを表示します。
- Gateway：CSC SSM 管理インターフェイスが含まれるネットワークのゲートウェイ デバイスの IP アドレスを表示します。
- Primary DNS：プライマリ DNS サーバの IP アドレスを表示します。
- Secondary DNS（オプション）：セカンダリ DNS サーバの IP アドレスが設定されていれば表示します。
- Proxy Server（オプション）：プロキシ サーバが設定されていれば表示します。
- Proxy Server（オプション）：プロキシ ポートが設定されていれば表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC Setup Wizard Host Configuration

CSC Setup Wizard Host Configuration ウィンドウには、CSC SSM 用に入力したホスト名とドメイン名、着信電子メールのドメイン名、管理者の電子メール アドレス、電子メール サーバの IP アドレス、およびポート番号が表示されます。

フィールド

- Hostname：CSC SSM のホスト名を表示します。
- Domain Name：CSC SSM が常駐するドメインの名前を表示します。
- Incoming Email Domain：着信電子メールのドメイン名を表示します。
- Administrator E-mail：ドメイン管理者の電子メール アドレスを表示します。
- E-mail Server IP Address：電子メール サーバの IP アドレスを表示します。
- Port：CSC SSM への接続に使用するポート番号を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

「CSC SSM の管理」を参照してください。

CSC Setup Wizard Management Access Configuration

CSC Setup Wizard IP Configuration ウィンドウには、CSC SSM へのアクセス権を付与するために入力したサブネットおよびホスト設定が表示されます。

フィールド

- IP Address : CSC SSM への接続が許可されているネットワークおよびホストの IP アドレスを表示します。
- Mask : ドロップダウン リストから選択した CSC SSM への接続が許可されているネットワークとホストのネットワーク マスクを表示します。
- Add：CSC SSM への接続を許可するネットワークとホストの IP アドレスを追加します。
- Delete : CSC SSM への接続が必要なくなったネットワークおよびホストの IP アドレスを削除します。
- Selected Hosts/Networks：CSC SSM への接続を追加したネットワークおよびホストの IP アドレスを一覧表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC Setup Wizard Password Configuration

CSC Setup Wizard Password Configuration ウィンドウには、CSC SSM へのアクセス権を付与するために入力したパスワード設定が表示されます。

フィールド

- Old Password：CSC SSM にアクセスするために現在のパスワードが必要です。
- New Password：CSC SSM にアクセスするための新しいパスワードを設定します。

- Confirm New Password：CSC SSM にアクセスするための新しいパスワードを確認のために入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

CSC Setup Wizard Traffic Selection for CSC Scan

CSC Setup Wizard Traffic Selection for CSC Scan ウィンドウには、CSC スキャン対象のトラフィックを選択するために行った設定が表示されます。

フィールド

- Interface：ドロップダウン リストから選択した CSC SSM へのインターフェイスを指定します。
- Source：CSC SSM がスキャンするネットワーク トラフィックの送信元を指定します。
- Destination：CSC SSM がスキャンするネットワーク トラフィックの宛先を指定します。
- Service：CSC SSM がスキャンする送信元サービスまたは宛先サービスを指定します。
- Add：CSC スキャンに関する追加のトラフィック詳細を指定します。詳細については、P.40-19 の「Specify traffic for CSC Scan」を参照してください。
- Edit：CSC スキャンに関する追加のトラフィック詳細を変更します。詳細については、P.40-19 の「Specify traffic for CSC Scan」を参照してください。
- Delete：CSC スキャンに関する追加のトラフィック詳細を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Specify traffic for CSC Scan

Specify traffic for CSC Scan ダイアログボックスでは、CSC スキャン対象のトラフィックを選択するための追加の設定を定義、変更、または削除できます。

フィールド

- Interface：CSC SSM へのインターフェイスのタイプをドロップダウン リストから指定します。指定できる設定値は、global（すべてのインターフェイス）、inside、management、outside です。
- Source：CSC SSM がスキャンするネットワーク トラフィックの送信元をドロップダウン リストから指定します。
- Destination：CSC SSM がスキャンするネットワーク トラフィックの宛先をドロップダウン リストから指定します。
- Service：CSC SSM がスキャンするサービスのタイプをドロップダウン リストから指定します。
- Description：CSC SSM がスキャンするように定義したネットワーク トラフィックについて説明します。
- If CSC card fails：CSC カードに障害が発生した場合に、CSC SSM にネットワーク トラフィックのスキャンを許可するかどうかを指定します。

  スキャンされていないトラフィックの通過を許可するには、**Permit** をクリックします。スキャンされていないトラフィックが通過しないようにするには、**Close** をクリックします。**OK** をクリックして設定内容を保存します。CSC Setup Wizard Traffic selection for CSC Scan ウィンドウに、追加したトラフィック詳細が表示されます。これらの設定内容を破棄して CSC Setup Wizard Traffic selection for CSC Scan ウィンドウに戻るには、**Cancel** をクリックします。**Cancel** をクリックすると、ASDM にはユーザの決定を確認するダイアログボックスが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-18 の「CSC Setup Wizard Traffic Selection for CSC Scan」を参照してください。

CSC Setup Wizard Summary

CSC Setup Wizard Summary ウィンドウには、CSC Setup Wizard で行った設定が表示されます。ウィザードを終了する前に選択内容を確認できます。設定を変更する場合は、**< Back** をクリックして変更する設定のウィンドウまで戻り、必要な変更を加えてから **Next >** をクリックしてこのウィンドウに戻ります。

（注）　**Finish** をクリックした後は、CSC Setup Wizard を再度使用することなく CSC SSM に関連するいずれのウィンドウも変更できます。

フィールド

- Activation Codes：表示のみ。Activation Codes Configuration ウィンドウで行った設定の要約を表示します。
  - Base：基本ライセンスのアクティベーション コードを表示します。
  - Plus：Plus ライセンスのアクティベーション コードを入力した場合は、そのアクティベーション コードを表示します。入力していないときは、空白になります。
- IP Parameters：表示のみ。IP Configuration ウィンドウで行った設定の要約を表示します。次の情報が含まれています。
  - CSC SSM の管理インターフェイスの IP アドレスとネットマスク。
  - CSC SSM 管理インターフェイスが含まれるネットワーキング用のゲートウェイ デバイスの IP アドレス。
  - プライマリ DNS サーバの IP アドレス。
  - セカンダリ DNS サーバの IP アドレス（設定している場合）。
  - プロキシ サーバおよびポート（設定している場合）。
- Host and Domain Names：表示のみ。Host Configuration ウィンドウで行った設定の要約を表示します。次の情報が含まれています。
  - CSC SSM のホスト名。
  - CSC SSM が含まれるドメインのドメイン名。
  - 着信電子メールのドメイン名。
  - 管理者の電子メール アドレス。
  - 電子メール サーバの IP アドレスとポート番号。
- Management Access List：Management Access Configuration ウィンドウで行った設定の要約を表示します。ドロップダウン リストには、CSC SSM が管理接続を許可するホストとネットワークが含まれています。
- Password：表示のみ。Password Configuration ウィンドウでパスワードを変更したかどうかを示します。
- < Back：CSC Setup Wizard の前のペインに移動します。
- Next >：グレー表示されています。ただし、**Back >** をクリックしてこのウィザード内の前のウィンドウにアクセスした場合は、**Next >** をクリックするとこのウィンドウに戻ります。
- Finish：CAC Setup Wizard を終了し、ウィザードで行ったすべての設定を保存します。
- Cancel：選択した設定内容を保存しないで CSC Setup Wizard を終了します。**Cancel** をクリックすると、ASDM にはユーザの決定を確認するダイアログボックスが表示されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Web

Web ペインでは、Web 関連機能がイネーブルになっているかどうかを確認したり、CSC SSM にアクセスして Web 関連機能を設定することができます。

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザ ウィンドウのセッションがタイムアウトになります。CSC SSM ブラウザ ウィンドウを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- URL Blocking And Filtering：URL ブロッキングおよび URL フィルタリングに関連する情報とリンクが含まれています。
  - URL Blocking：表示のみ。CSC SSM で URL ブロッキングがイネーブルになっているかどうかを示します。
  - Configure URL Blocking：CSC SSM で URL ブロッキングを設定するためのウィンドウを開きます。
  - URL Filtering：表示のみ。CSC SSM で URL フィルタリングがイネーブルになっているかどうかを示します。
  - Configure URL Filtering Rules：CSC SSM で URL フィルタリング ルールを設定するためのウィンドウを開きます。
  - Configure URL Filtering Settings：CSC SSM で URL フィルタリング設定を行うためのウィンドウを開きます。
- File Blocking：CSC SSM の HTTP ファイル ブロッキングに関するフィールドとリンクが含まれています。
  - File Blocking：表示のみ。CSC SSM でファイル ブロッキングがイネーブルになっているかどうかを示します。
  - Configure File Blocking：CSC SSM で HTTP ファイル ブロッキング設定を行うためのウィンドウを開きます。
- Scanning：CSC SSM の HTTP スキャンに関するフィールドとリンクが含まれています。
  - HTTP Scanning：表示のみ。CSC SSM で HTTP スキャンがイネーブルになっているかどうかを示します。
  - Configure Web Scanning：CSC SSM で HTTP スキャンを設定するためのウィンドウを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Mail

Mail ペインでは、電子メール関連の機能がイネーブルになっているかどうかを確認し、CSC SSM にアクセスして電子メール関連機能を設定できます。

この領域の設定の詳細については、次の項目を参照してください。

- SMTP タブ（P. 40-22）
- POP3 タブ（P. 40-23）

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SMTP タブ

SMTP タブには、CSC SSM の SMTP 電子メール機能に固有のフィールドとリンクが表示されます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- Scanning：SMTP スキャンに関するフィールドとリンクが含まれています。
  - Incoming Scan：表示のみ。CSC SSM で着信 SMTP スキャン機能がイネーブルになっているかどうかを示します。
  - Configure Incoming Scan：CSC SSM で着信 SMTP スキャン設定を行うためのウィンドウを開きます。
  - Outgoing Scan：表示のみ。CSC SSM で発信 SMTP スキャン機能がイネーブルになっているかどうかを示します。
  - Configure Outgoing Scan：CSC SSM で発信 SMTP スキャン設定を行うためのウィンドウを開きます。
- Content Filtering：SMTP コンテンツ フィルタリングに関するフィールドとリンクが含まれています。
  - Incoming Filtering：表示のみ。CSC SSM で着信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。
  - Configure Incoming Filtering：CSC SSM で着信 SMTP コンテンツ フィルタリングを設定するためのウィンドウを開きます。
  - Outgoing Filtering：表示のみ。CSC SSM で発信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。
  - Configure Outgoing Filtering：CSC SSM で発信 SMTP コンテンツ フィルタリングを設定するためのウィンドウを開きます。

- Anti-spam：SMTP アンチスパム機能に関するフィールドとリンクが含まれています。
  - Spam Prevention：表示のみ。CSC SSM で SMTP アンチスパム機能がイネーブルになっているかどうかを示します。
  - Configure Anti-spam：CSC SSM で SMTP アンチスパムを設定するためのウィンドウを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

POP3 タブ

POP3 タブには、CSC SSM の POP3 電子メール機能に固有のフィールドとリンクが表示されます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- Scanning：表示のみ。CSC SSM で POP3 電子メール スキャンがイネーブルになっているかどうかを示します。
- Configure Scanning：CSC SSM で POP3 電子メール スキャンを設定するためのウィンドウを開きます。
- Anti-spam：表示のみ。CSC SSM で POP3 アンチスパム機能がイネーブルになっているかどうかを示します。
- Configure Anti-spam：CSC SSM で POP3 アンチスパム機能を設定するためのウィンドウを開きます。
- Content Filtering：表示のみ。CSC SSM で POP3 電子メール コンテンツ フィルタリング機能がイネーブルになっているかどうかを示します。
- Configure Content Filtering：CSC SSM で POP3 電子メール コンテンツ フィルタリングを設定するためのウィンドウを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

File Transfer

File Transfer ペインでは、FTP 関連の機能がイネーブルになっているかどうかを確認し、CSC SSM にアクセスして FTP 関連機能を設定できます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- File Scanning：表示のみ。CSC SSM で FTP ファイル スキャンがイネーブルになっているかどうかを示します。
- Configure File Scanning：CSC SSM で FTP ファイル スキャン設定を行うためのウィンドウを開きます。
- File Blocking：表示のみ。CSC SSM で FTP ファイル ブロッキングがイネーブルになっているかどうかを示します。
- Configure File Blocking：CSC SSM で FTP ファイル ブロッキング設定を行うためのウィンドウを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。

Updates

Updates ペインでは、アップデートのスケジュール設定がイネーブルになっているかどうかを確認し、CSC SSM にアクセスしてアップデートのスケジュールを設定できます。

（注）　CSC SSM GUI にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

フィールド

- Scheduled Updates：表示のみ。CSC SSM でアップデートのスケジュール設定がイネーブルになっているかどうかを示します。
- Scheduled Update Frequency：アップデートを実行するスケジュールに関する情報が表示されます。「Hourly at 10 minutes past the hour」など。
- Component：アップデート可能な CSC SSM ソフトウェアのコンポーネントの名前が表示されます。
- Scheduled Updates：表示のみ。対応するコンポーネントでアップデートのスケジュール設定がイネーブルになっているかどうかを示します。
- Configure Updates：CSC SSM でアップデートのスケジュール設定を行うためのウィンドウを開きます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

詳細情報

P.40-3 の「CSC SSM の管理」を参照してください。