CHAPTER 36

Trend Micro Content Security の設定

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。

CSC SSM の管理

ここでは、次の項目について説明します。

CSC SSM について

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。

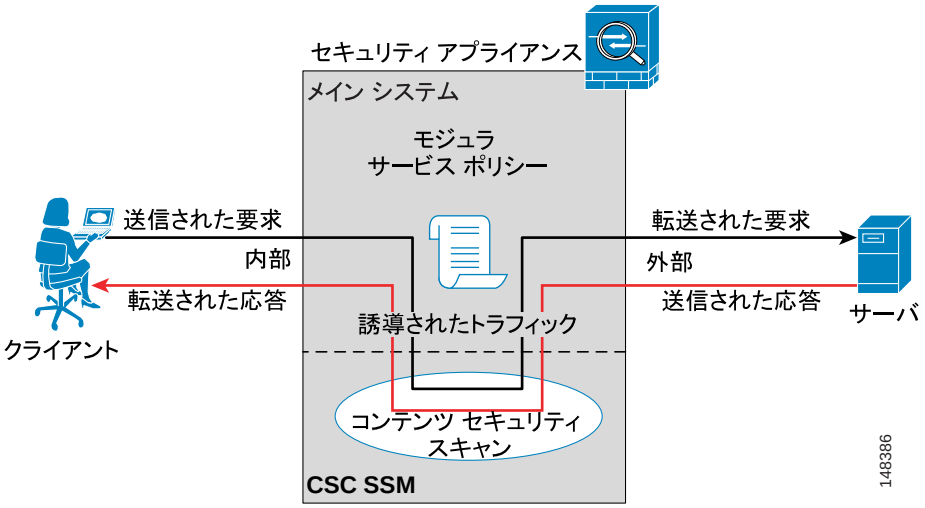
図 36-1 は、次の構成の適応型セキュリティ アプライアンスを通過するトラフィックのフローを示しています。

- CSC SSM がインストール、設定されている。
- どのトラフィックを SSM に誘導し、スキャンするかを指定するサービス ポリシーがある。

この例では、クライアントのネットワーク ユーザは、Web サイトにアクセスしているか、FTP サーバからファイルをダウンロードしているか、POP3 サーバから電子メールを取得している可能性があります。SMTP スキャンは、適応型セキュリティ アプライアンスによって保護された SMTP サーバに向けて外部から送信されたトラフィックをスキャンするように、適応型セキュリティ アプライアンスを設定する必要がある点で異なります。

（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限り、FTP ファイル転送をスキャンします。デフォルトでは、FTP 検査はイネーブルです。

図 36-1　CSC SSM でスキャンされるトラフィックのフロー



システムの設定と CSC SSM の監視には、ASDM を使用します。CSC SSM ソフトウェアのコンテンツ セキュリティ ポリシーに高度な設定を行うには、ASDM で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 ブラウザに CSC SSM GUI が表示され、CSC SSM パスワードを要求されることがあります。CSC SSM GUI の使用方法については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

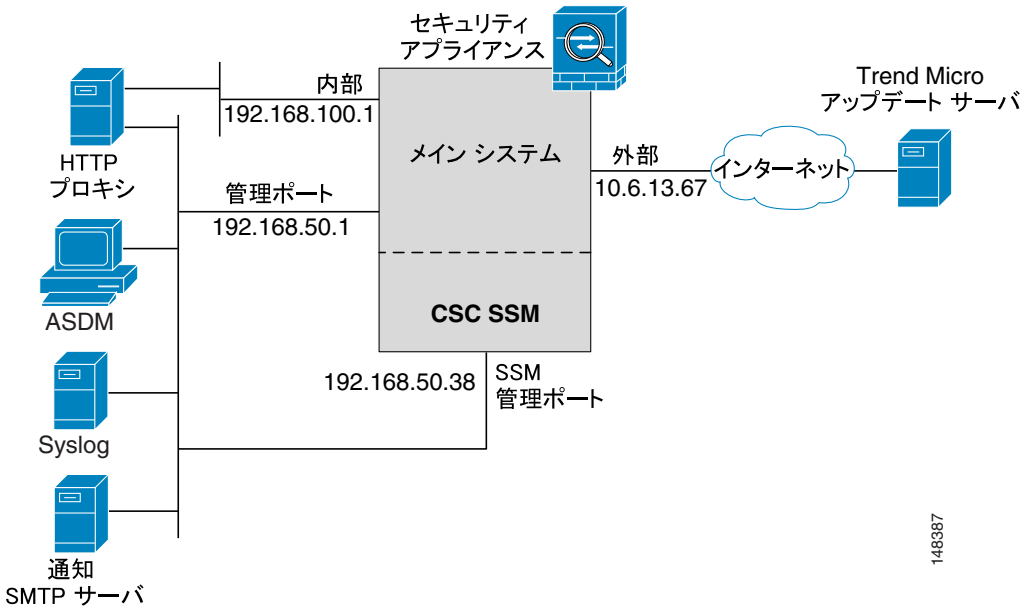
（注）　ASDM と CSC SSM では、別個のパスワードが保持されています。それらのパスワードを同一にすることはできますが、2 つのパスワードのうち一方を変更しても、もう一方に影響することはありません。

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。

図 36-2 に、専用の管理ネットワークに接続されている CSC SSM を持つ適応型セキュリティ アプライアンスを示します。専用の管理ネットワークの使用は必須ではありませんが、使用することをお勧めします。図 36-2 で特に重要な点は次のとおりです。

- HTTP プロキシ サーバが内部ネットワークと管理ネットワークに接続されている。これによって、CSC SSM は Trend Micro アップデート サーバに接続できます。
- 適応型セキュリティ アプライアンスの管理ポートが管理ネットワークに接続されている。適応型セキュリティ アプライアンスと CSC SSM の管理を可能にするには、ASDM を実行しているホストは管理ネットワークに接続されている必要があります。
- 管理ネットワーク内には、CSC SSM への電子メール通知に使用される SMTP サーバと、CSC SSM がシステム ログ メッセージを送信できる syslog サーバがある。

図 36-2　管理ネットワークを備えた CSC SSM 構成



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。次の手順では、それらのステップの概要を示します。

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、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 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 syslog ロギング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、適応型セキュリティ 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 > Properties > Device Administration > 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 > Properties > Device Administration > NTP** を選択します。

ステップ 5　CSC Setup Wizard を実行します。

- CSC Setup Wizard を実行していない場合は、**Configuration > Trend Micro Content Security** を選択すると、Setup Wizard が自動的に起動します。
- Setup Wizard を再実行する場合は、**Configuration > Trend Micro Content Security** を選択して、CSC SSM に接続およびログインし、**CSC Setup > Wizard Setup** を選択して **Launch Wizard Setup** をクリックします。

CSC Setup Wizard のウィンドウについては、**Help** ボタンをクリックしてください。

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 サービス 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。

トラフィックの CSC SSM への誘導における最良の方法については、「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 サービス ポリシーを作成する場合は、次の手順を実行します。

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

   Add Service Policy Rule Wizard が表示されます。

b. **Global - applies to all interfaces** オプション ボタンをクリックして、**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 ボタンをクリックして、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ます。**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、適応型セキュリティ アプライアンスで選択したトラフィックを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るコンテンツ セキュリティ スキャンを実行する CSC SSM にトラフィックを誘導し始めます。

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。これらの修正は高度な設定であるため、必ず『*Cisco Content Security and Control SSM Administrator Guide*』を読んでから実行してください。

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 レベル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、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。

CSC SSM GUI にアクセスするには、ASDM で **Configuration > Trend Micro Content Security** を選択し、次のいずれかを選択します。**Web**、**Mail**、**File Transfer**、または **Updates**。これらのペインにある、「Configure」という単語で始まる青色のリンクをクリックすると、CSC SSM GUI が開きます。

スキャンするトラフィックの指定

CSC SSM は、FTP、HTTP、POP3、および SMTP トラフィックをスキャンできます。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のウェルノウン ポートである場合に限りサポートされます。つまり、CSC SSM がスキャンできる接続は次のものに限られます。

- 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（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。

Add Service Policy Rule Wizard—Rule Actions ウィンドウの CSC Scan タブで、CSC SSM でのトラフィックのスキャン アクションはイネーブルになっています。CSC スキャン アクショ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。

csc コマンドをグローバル ポリシーに追加した場合、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、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になる場合もあります。

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。つまり、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 に誘導します。

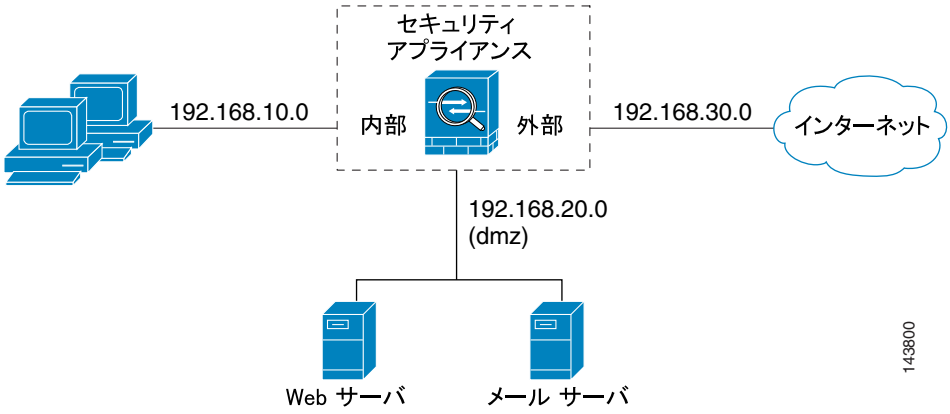
ただし、双方向性があることにより、特定のインターフェイスを通過するサポート対象のトラフィック タイプを CSC SSM に誘導した場合に、信頼できる内部ネットワークからのトラフィックに対して不必要なスキャンを実行することになる可能性があります。たとえば、DMZ ネットワークの Web サーバから要求された URL およびファイルが内部ネットワークのホストに対してコンテンツ セキュリティ リスクをもたらす可能性は低いため、そのようなトラフィックを適応型セキュリティ アプライアンスで CSC SSM に誘導する必要はほとんどありません。

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って、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のサーバへの 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のサーバへの POP3 接続
- 内部メール サーバを宛先とする着信 SMTP 接続

図 36-3 では、適応型セキュリティ アプライアンスは、CSC SSM にトラフィックを誘導するように設定されています。内部ネットワークのクライアントから外部ネットワークへの HTTP、FTP、および POP3 接続要求、および外部ホストから DMZ ネットワークのメール サーバへの着信 SMTP 接続要求が誘導されます。内部ネットワークから DMZ ネットワークの Web サーバへの HTTP 要求はスキャンされません。

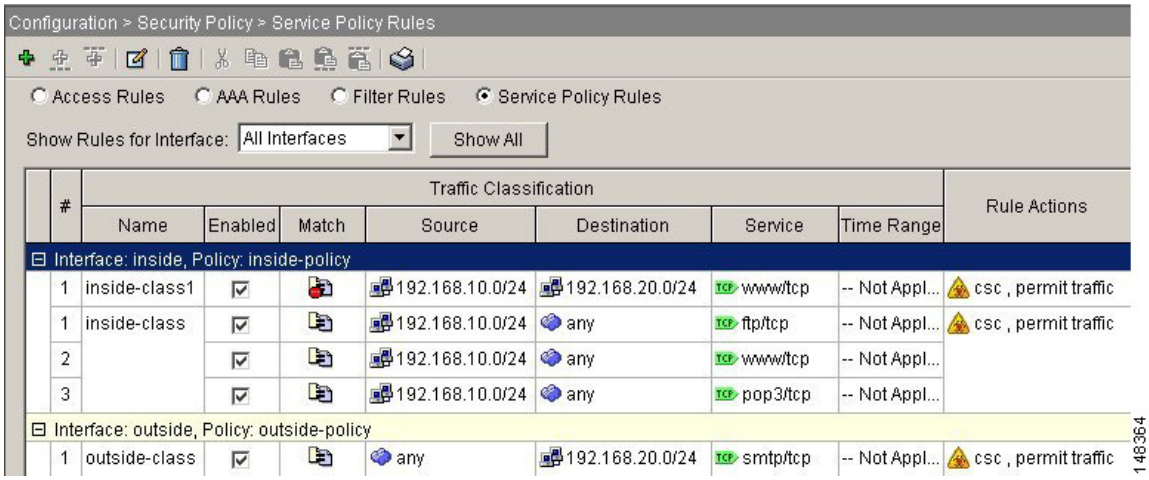
図 36-3　CSC SSM スキャンの一般的なネットワーク構成



スキャン対象のトラフィックを特定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方法は多数あります。その 1 つは、内部インターフェイスに対するサービス ポリシーと外部インターフェイスに対するサービス ポリシーの 2 つのサービス ポリシーを定義することです。各サービス ポリシーには、スキャンするトラフィックと一致するアクセスリストを含めます。

図 36-4 は、スキャンが必要なトラフィックのみを選択するサービス ポリシー ルールを示します。

図 36-4　CSC スキャンの最適なトラフィック選択



inside-policy では、最初のクラス inside-class1 によって、内部ネットワークおよび DMZ ネットワーク間の HTTP トラフィックは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れを示します。これは、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。これは単に、この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、ネットワークおよびすべての宛先間の FTP、HTTP および POP3 トラフィックを照合します。inside-class1 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 アクションを適用するポリシーは、入力トラフィックと出力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。これによって、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 Setup

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には、先に Setup Wizard を完了する必要があります。Setup Wizard を完了したら、Setup Wizard を再度使うことなく各ペインを個別に変更することができます。

また、Setup Wizard を完了するまで、Home > Content Security or Monitoring > Trend Micro Content Security のペインにアクセスできません。Setup Wizard を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、Setup Wizard 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、「CSC SSM について」を参照してください。

- Activation/License
- IP Configuration
- Host/Notification Settings
- Management Access Host/Networks
- Password
- Restoring the Default Password
- Wizard Setup
- Summary

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。

参考資料

CSC SSM の管理

Activation/License

Configuration > Trend Micro Content Security > CSC Setup > 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。

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。

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。

参考資料

CSC SSM の管理

IP Configuration

Configuration > Trend Micro Content Security > CSC Setup > 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 : ゲートウェイ デバイスの IP アドレスを設定します。これは、CSC SSM の管理 IP アドレスが含まれるネットワーク用のゲートウェイ デバイスです。
- 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：（オプション）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 でのプロキシ サーバの使用を必要としていない場合、このグループのボックスを空のままにすることができます。
  - 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。

参考資料

CSC SSM の管理

Host/Notification Settings

Configuration > Trend Micro Content Security > CSC Setup > 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 メッセージ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。　このインターフェイスにアクセスするには、**Configuration > Trend Micro Content Security > Email** を選択し、リンクを 1 つクリックして CSC SSM にアクセスします。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：電子メール通知を送信す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。

参考資料

CSC SSM の管理

Management Access Host/Networks

Configuration > Trend Micro Content Security > CSC Setup > 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。

参考資料

CSC SSM の管理

Password

Configuration > Trend Micro Content Security > CSC Setup > 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 のパスワードに影響することはありません。

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。そのため、ASDM には、パスワードを変更する前に確認ダイアログボックスが表示されます。

ヒント　CSC SSM への接続がドロップされたときは、ステータス バーの Connection to Device アイコンを使って再確立することができます。この場合、アイコンをクリックしてから、Connection to Device ダイアログボックスの **Reconnect** をクリックします。ASDM は、CSC SSM パスワードに設定した新しいパスワードの入力を要求します。

（注）　デフォルトのパスワードは「cisco」です。

パスワードを入力するとアスタリスクで表示されます。

パスワードの長さは、5 ～ 32 文字で指定します。

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。

参考資料

CSC SSM の管理

Restoring the Default Password

Tools > CSC Password Reset

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。

（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設定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設定にリセットします。

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 7.2（2）以降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 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。

参考資料

Password

Wizard Setup

Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup

Wizard Setup ペインで、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、Setup Wizard を完了する必要があります。

Setup Wizard を完了したら、Setup Wizard を再度使用することなく CSC SSM に関連するいずれのペインも変更することができます。

フィールド

- Launch Setup Wizard：CSC SSM 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 ペインは管理コンテキストのみで使用できます。

参考資料

CSC SSM の管理

Summary

Configuration > Trend Micro Content Security > CSC Setup > Wizard Setup (Summary)

Summary ペインには、CSC Setup Wizard で行った作業結果が表示されます。ウィザードを終了する前に、Summary ペインで作業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ペインまで戻り、必要な変更を加えてから **Next >** をクリックして Summary ペインに戻ります。

（注）　**Finish** をクリックした後に、Setup Wizard を再度使用することなく CSC SSM に関連するいずれのペインも変更することができます。

フィールド

- Activation Codes：表示のみ。Activation Codes Configuration ペインで行った設定の要約が表示されます。
  - Base：基本ライセンスのアクティベーション コードが表示されます。
  - Plus：入力した場合は、Plus ライセンスのアクティベーション コードが表示されます。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 ペインで行った設定の要約が表示されます。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を含む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 ペインで行った設定の要約が表示されます。次の情報が含まれています。
  - CSC SSM のホスト名。
  - CSC SSM を含む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 : 表示のみ。Management Access Configuration ペインで行った設定の要約が表示されます。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 ペイン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できます。
- Next > : Summary ペインでは、このボタンはグレー表示になっていますが、Back > を使用してウィザードの前のペインに移動したときに、このボタンをクリックすると Summary ペインに戻ります。
- Finish : CAC Setup Wizard を完了し、ウィザードで行ったすべての設定を保存します。
- Cancel : 行った設定を保存しないで 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
•	•	•	•	—

参考資料

CSC SSM の管理

Web

Configuration > Trend Micro Content Security > 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 のパスワードが必要で、CSC SSM GUI を示すブラウザによって入力が求められます。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 ブロッキング機能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が開きます。
  - URL Filtering：表示のみ。CSC SSM で URL 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 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が開きます。
  - Configure URL Filtering Settings：CSC SSM で URL フィルタリングの設定を行うためのウィンドウが開きます。
- File Blocking：CSC SSM の HTTP ファイル ブロッキング機能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 ブロッキング機能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 スキャン機能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 スキャン機能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
•	•	•	•	—

参考資料

CSC SSM の管理

Mail

Configuration > Trend Micro Content Security > 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たり、CSC SSM にアクセスして電子メール関連機能を設定することができます。

これらの領域の設定の詳細については、次の項を参照してください。

- Mail > SMTP タブ
- Mail > POP3 タブ

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
•	•	•	•	—

Mail > SMTP タブ

Configuration > Trend Micro Content Security > Mail > 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 にアクセスするには CSC SSM のパスワードが必要で、CSC SSM GUI を示すブラウザによって入力が求められます。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 スキャンを設定する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 Incoming Scan：CSC SSM で発信 SMTP スキャンを設定する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
•	•	•	•	—

参考資料

CSC SSM の管理

Mail > POP3 タブ

Configuration > Trend Micro Content Security > Mail > 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 にアクセスするには CSC SSM のパスワードが必要で、CSC SSM GUI を示すブラウザによって入力が求められます。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 スキャン機能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
•	•	•	•	—

参考資料

CSC SSM の管理

File Transfer

Configuration > Trend Micro Content Security > File Transfer

File Transfer ペインでは、FTP 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 FTP 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 のパスワードが必要で、CSC SSM GUI を示すブラウザによって入力が求められます。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 スキャン機能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 ブロッキング機能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
•	•	•	•	—

参考資料

CSC SSM の管理

Updates

Configuration > Trend Micro Content Security > 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たり、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することができます。

（注）　CSC SSM にアクセスするには CSC SSM のパスワードが必要で、CSC SSM GUI を示すブラウザによって入力が求められます。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 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
•	•	•	•	—

参考資料

CSC SSM の管理

CSC への接続 /Content Security and Control のパスワード

Home > Content Security

Configuration > Trend Micro Content Security

Monitoring > Trend Micro Content Security

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。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。

フィールド

- Connecting to CSC：CSC SSM の管理ポートの IP アドレスを指定できます。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。
  - Management IP Address : CSC SSM への接続用の管理 IP アドレスを ASDM が検出した IP アドレスに設定します。これがデフォルトの選択です。
  - Other IP Address or Hostname：管理 IP アドレスをユーザが入力した値に設定します。
- CSC Password : CSC SSM にアクセスするためのパスワードを指定できます。パスワードを指定すると、ASDM は CSC SSM への接続を確立できます。ASDM では、この接続を使用して、CSC SSM でイネーブルになっている機能に関する情報など、監視およびステータス情報を取得します。

  パスワードを入力してから 10 分間、CSC SSM GUI を開くリンクのクリックでは、CSC SSM GUI を表示するブラウザでの CSC SSM パスワードの再入力が不要になります。
  - Password：CSC SSM のパスワードが必要です。Configuration > Trend Micro Content Security > CSC Setup で Setup Wizard を完了していない場合は、デフォルトの CSC パスワードを使用します。次に、Setup Wizard で設定を完了します。その際、デフォルトのパスワードの変更も行います。

（注）　デフォルトの CSC SSM パスワードは、「cisco」です。

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
•	•	•	•	—

参考資料

CSC SSM の管理