Content Security and Control SSM の概要

この章では、Content Security and Control Security Services Module （CSC SSM）の概要について説明します。この章は、次の項で構成されています。

概要

Trend Micro InterScan for Cisco CSC SSM （Content Security and Control Security Services Module）は、ネットワーク用統合アンチウイルスおよびスパイウェア管理ソリューションです。このマニュアルでは、Cisco アプライアンスに常駐して次の機能を実行する CSC SSM を管理する際の考え方について説明します。

- SMTP、POP3、HTTP、FTP を使用するネットワーク トラフィックに対するウイルス、ワーム、トロイの木馬、その他の脅威を検出し、適切な処置を取ります

（注）　HTTPS など他のプロトコルを使用するトラフィックを CSC SSM はスキャンしません。

- 圧縮ファイルまたは指定されたパラメータを超える非常に大きなファイルをブロックします
- スキャンによってスパイウェア、アドウェア、および他のタイプのグレーウェアを見つけ、削除します

CSC SSM ソフトウェアの Base ライセンスを持つユーザはすべて、上記の機能を利用できます。Base ライセンスに加えて CSC SSM ライセンスの Plus レベルを購入した場合は、次の機能も利用できます。

- SMTP および POP3 トラフィックでスパムを減らし、フィッシング詐欺から保護します
- キーワードやフレーズを含む電子メール トラフィックを、許可または禁止するようにできるコンテンツ フィルタをセットアップします
- 社員にアクセスさせたくない URL または隠された目的や悪意の目的がある URL をブロックします
- 成人向けコンテンツ、ゲーム、チャット / インスタント メッセージ、ギャンブルのサイトなどを許可または禁止する定義済みのカテゴリに従って、URL トラフィックをフィルタリングします

Base ライセンスおよび Plus ライセンスの詳細については、P.1-12 の「ライセンス」を参照してください。

トラフィックのスキャンを開始するには、1 つ以上のサービス ポリシー規則を ASDM で作成し、スキャンするトラフィックを CSC SSM に送信する必要があります。詳細については、ASDM のオンライン ヘルプを参照してください。

Trend Micro InterScan for Cisco CSC SSM を使用すると、ウイルスからの保護、スパイウェアのブロック、スパム検出、コンテンツ フィルタリング用のアプリケーションを別々にインストールする必要がありません。これらの機能すべてが 1 つのパッケージで利用できます。Trend Micro InterScan for Cisco CSC SSM では、主要なトラフィック プロトコル、たとえば SMTP、HTTP、FTP、および POP3 トラフィックを保護し、社員が個人の電子メール アカウントから知らないうちにウイルスを取り込むのを防ぐことができます。また、このアプリケーションは保守管理が容易です。インストールし、初期設定を行った後は、このマニュアルを再度参照する必要はありません。

アプライアンスの詳細については、シスコのマニュアルを参照してください。セットアップ ウィザードでは、インストール プロセスを順を追って案内します。

このマニュアルでは、Trend Micro InterScan for Cisco CSC SSM ユーザ インターフェイスについて説明し、インストール後に微調整を行う場合の、コンフィギュレーション設定について説明します。このマニュアルには、ユーザ インターフェイスのウィンドウのフィールドごとの説明は含まれていません。固有のウィンドウのフィールドの説明については、CSC SSM のオンライン ヘルプを参照してください。

機能および利点

Trend Micro InterScan for Cisco CSC SSM は、ネットワークへの脅威に対処するのに役立ちます。表 1-1 に、機能および利点の概要を示します。

表 1-1　機能および利点

機能
スキャンによってウイルスが含まれているトラフィックを見つけ、感染したメッセージやファイルを管理します
スキャンによって下限しきい値レベルから上限しきい値レベルでスパムを見つけ、スパムの処理方法を決めることができます
攻撃的なコンテンツや不適切なコンテンツをフィルタリングします
ネットワークに被害を及ぼす可能性のあるファイル タイプの着信をブロックします
メッセージのサイズに制限を設定して、DoS 攻撃（サービス拒絶攻撃）を防ぎます
ファイルおよび URL のブロッキングについて、承認する送信者およびブロックする送信者を指定する機能を提供します
URL へのアクセスをカテゴリによってフィルタリングします
企業ポリシーによって禁止されている URL サイトや FTP サイトへの接続をブロックします
利点
シスコの強力なファイアウォール保護と組み合せることにより、Trend Micro InterScan for Cisco CSC SSM は、脅威、スパム、および好ましくないコンテンツからネットワークを保護します
ユーザ フレンドリなセットアップ プログラムにより、インストールが容易に行えます
アンチウイルス、スパイウェア / グレーウェア検出、ファイル ブロッキング、およびネットワーク トラフィックのセキュリティ リスクに対するその他の保護が、ASDM と統合されます
インストール後にスキャン、アンチスパム、およびフィルタリングの諸機能のコンフィギュレーションを微調整することができます
Trend Micro から新しいバージョンが入手できるようになったときは、ウイルス パターン ファイル、スキャン エンジン、およびスパム検出の各コンポーネントを自動的にアップデートするように設定できます
電子メール通知および syslog 通知を送信して、ユーザがアクティビティについての情報を常に得られるようにします
30 日後に自動的に消去されるログ ファイルを提供します
タスクの手順を案内するオンライン ヘルプといった、ユーザ フレンドリなコンソールが用意されています
ライセンスの期限満了が近づくと自動的に通知します

利用可能なマニュアル

この製品のマニュアルは、ファイアウォールの管理およびネットワークの管理の基本的な概念を理解しているシステム管理者を対象としています。また、ネットワークのセキュリティ アプライアンスを管理する特権を持っていることを前提としています。

先に進む前に、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』も読んでおくことをお勧めします。この *Quick Start Guide* には、購入したアプライアンスにまだ SSM がインストールされていない場合に CSC SSM をインストールするためのマニュアルが含まれています。

Trend Micro InterScan for Cisco CSC SSM で利用可能なマニュアルは次のとおりです。

- 本マニュアル：『*Cisco Content Security and Control SSM アドミニストレータ ガイド*』
- オンライン ヘルプ：次の 2 種類のオンライン ヘルプが利用できます。
  - 状況依存スクリーン ヘルプ。1 つのウィンドウでタスクを実行する方法を説明します。
  - 一般ヘルプ。複数のウィンドウでアクションが必要なタスク、またはタスクの実行に必要な周辺知識について説明します。
- Knowledge Base：問題解決およびトラブルシューティングの情報のオンライン データベース。Knowledge Base には、既知の製品問題に関する最新情報があります。Knowledge Base を利用するには、次の URL にアクセスしてください。

  kb.trendmicro.com/solutions/solutionSearch.asp

重要な用語

マニュアルおよびオンライン ヘルプで使用されている専門用語の中には、あまりなじみのないものや、予想とは異なる方法で使用されているものがあります。専門用語の定義は、用語集に説明されています。

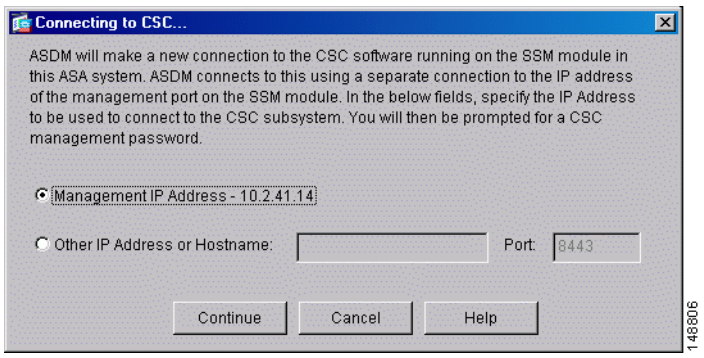
ASDM Content Security タブの概要

ASDM Home ページには、Content Security と呼ばれるタブがあります。メイン ASA システム ホームページはデフォルト表示です。Content Security タブをクリックすると、CSC SSM アクティビティの要約が表示されます。

CSC SSM へ接続するよう求められます。ダイアログボックスが表示され、ASDM に認識されている IP アドレスまたは代替アドレスを選択することができます。代替アドレスは、NAT デバイスを介して ASDM にアクセスする場合に使用される場合があります。NAT デバイスでは、コンピュータに表示される SSM の IP アドレスは、CSC SSM 管理ポートの実際の IP アドレスと異なります。

ダイアログボックスは次のように表示されます。

図 1-1　CSC SSM への接続のプロンプト



ローカル ホストまたは代替ホストを選択した後、**Continue** をクリックします。次に、インストール中に設定した CSC SSM のパスワードを入力するように求められます。パスワードを入力し、**OK** をクリックします。

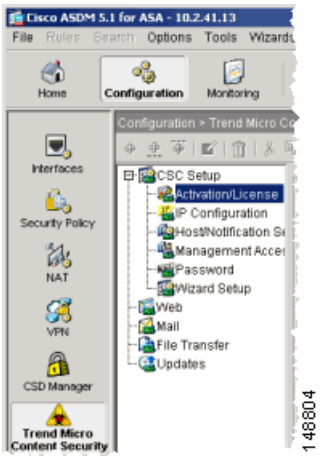
Content Security タブが表示されます。詳細については、P.7-2 の「Content Security タブの機能」を参照してください。

Content Security の設定

ASDM コンソールで、**Configuration > Trend Micro Content Security** をクリックしてコンフィギュレーション オプションを表示します。オプションは次のとおりです。

- CSC Setup：CSC SSM をインストールおよび設定するセットアップ ウィザードを起動します
- Web：Web スキャン、ファイル ブロッキング、URL フィルタリング、および URL ブロッキングを設定します
- Mail：着信および発信する SMTP メールと POP3 メールのスキャン、コンテンツ フィルタリング、およびスパム防御を設定します
- File Transfer：ファイル スキャンおよびファイル ブロッキングを設定します
- Updates：コンテンツ セキュリティ スキャン コンポーネント（ウイルス パターン ファイル、スキャン エンジンなど）のアップデートのスケジュールを設定します

図 1-2　ASDM のコンフィギュレーション オプション



セットアップ オプションは、『*Cisco ASA5500 Adaptive Security Appliance Getting Started Guide*』に説明があります。これらの各オプションの詳細については、オンライン ヘルプも参照してください。

Web、Mail、File Transfer、および Updates のオプションは、この『*アドミニストレータ ガイド*』の別の章でより詳しく説明されています。

- Web コンフィギュレーション：第 4 章「Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定」を参照してください。
- Mail コンフィギュレーション：第 3 章「メール トラフィック（SMTP および POP3）の設定」を参照してください。
- File Transfer コンフィギュレーション：第 4 章「Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定」を参照してください。
- Updates：第 5 章「アップデートおよびログ クエリーの管理」を参照してください。

CSC SSM コンソールの概要

Trend Micro InterScan for Cisco CSC SSM を正常にインストールし、CSC SSM にトラフィックを送信するように ASA を設定すると、ウイルス スキャンおよび検出機能がアクティブになり、ネットワーク トラフィックはデフォルト設定を使用してスキャンされます。スパイウェア / グレーウェア検出などの追加機能は、デフォルトではイネーブルになっていません。CSC SSM インターフェイスで設定できます。

CSC SSM インターフェイスに入るには、**Configuration > Trend Micro Content Security** をクリックします。Configuration メニュー（上記の図 1-2 を参照）で、タスクを選択します。たとえば、Web スキャンを設定するには、**Configuration > Trend Micro Content Security** メニューで **Web** を選択します。Configuration ウィンドウの右側（上には示されていません）には、目的のタスクを実行するためのリンクがあります。たとえば、Configure Web Scanning リンクをクリックすると、CSC SSM インターフェイスの **HTTP Scanning** 画面が表示され、Web スキャン設定を行うことができます。

CSC SSM インターフェイスに初めてログインすると、ASDM によってセキュリティ証明書が表示され、続いて **Connecting to CSC < リンク名 >** 画面が表示されます。CSC SSM インターフェイスを終了した後 ASDM からログアウトしないで戻った場合は、セキュリティ証明書のみが表示されます。

CSC SSM インターフェイスでは、ブラウザ ウィンドウが表示されます。Trend Micro InterScan for Cisco CSC SSM コンソールのデフォルト表示は状況依存で、選択したリンクによって決まります。次に例を示します。

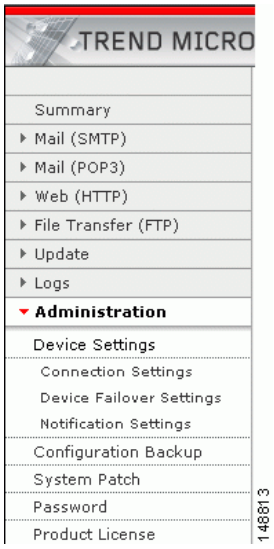
図 1-3　Configure Web Scanning リンクをクリックした場合に表示される HTTP Scanning ウィンドウ

ログオフするには、図 1-3 に示すように画面ヘッダーに表示されている **Log Off** をクリックします。次にブラウザ ウィンドウを閉じます。

ナビゲーション パネル

Trend Micro CSC SSM コンソールの左ペインはメイン メニューで、ナビゲーション ペインの役割も果たします。ナビゲーション ペインの選択項目をクリックすると、対応するウィンドウが開きます。選択項目は、矢印が右を向いているときは縮小されており、矢印が下を向いているときは展開されています。ナビゲーション ペインで選択項目をクリックするまで、対応するペインはリフレッシュされません。

図 1-4　Trend Micro CSC SSM Console のナビゲーション ペイン



パス名 **Mail (SMTP) > Scanning > Incoming > Action** という表現は、次のような意味を表しています。

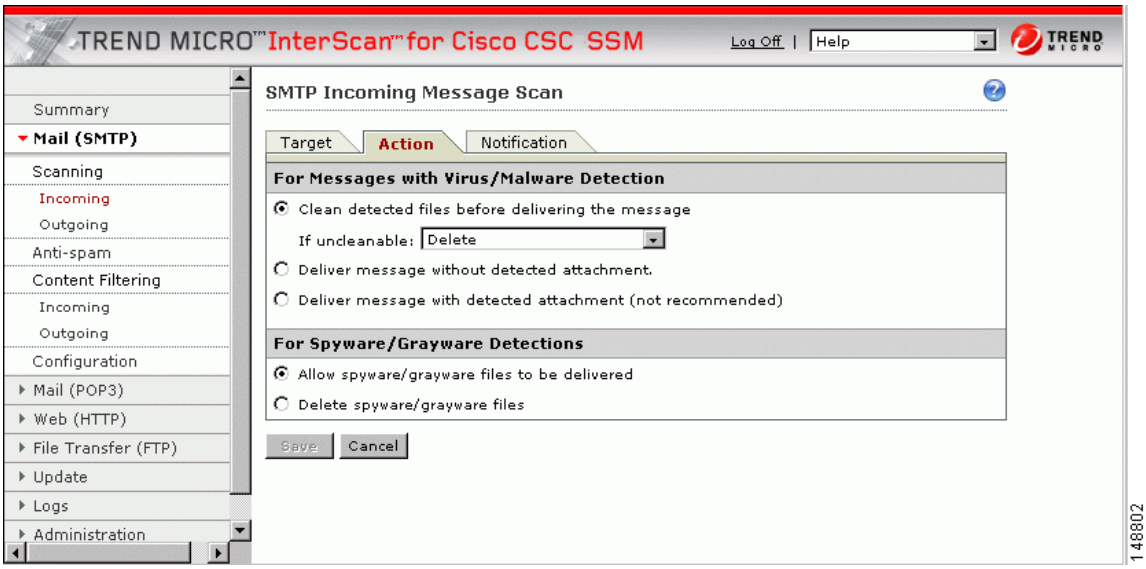
- ナビゲーション ペインの主選択は Mail （SMTP）です
- 第 2 の選択は Scanning です
- 第 3 の選択は Incoming です
- SMTP Incoming Message Scan 画面の選択されたタブは Action タブです

タブの動作

CSC SSM コンソールの右側に選択を行うための対話型の画面が表示されます。ユーザ インターフェイスの大部分のウィンドウには複数のビューがあります。たとえば、SMTP Incoming Message Scan ウィンドウには、Target、Action、および Notification という 3 つのビューがあります。ビューの切り替えは、表示する情報に該当するタブをクリックして行います。アクティブなタブは、名前が赤で表示され、アクティブでないタブは、黒で表示されます。

通常、これらのタブは関連しており、総合的に動作します。たとえば、次の図では、着信 SMTP トラフィックのウイルス スキャンを設定するために、3 つのタブすべてが必要です。

図 1-5　総合的に動作するタブ



- **Target**：アクティビティの対象となる範囲を定義することができます
- **Action**：トリガー イベントが発生したときに実行するアクション（たとえば無害化または削除）を定義することができます
- **Notification**：通知メッセージを作成し、イベントおよびアクションの通知相手を定義することができます

上記のような関連するタブでは、一度 **Save** をクリックすると、3 つのタブすべてに対して行った作業が保存されます。

Save ボタン

Save ボタンは、見れば保存する必要があるかどうかがわかります。**Save** ボタンはウィンドウが最初に開いたときには使用できません。ウィンドウでタスクを実行すると、**Save** ボタンの文字がグレーから黒に変わります。黒に変化したボタンは、実行した作業を有効にするには **Save** をクリックして保存する必要があることを示します。

デフォルト値

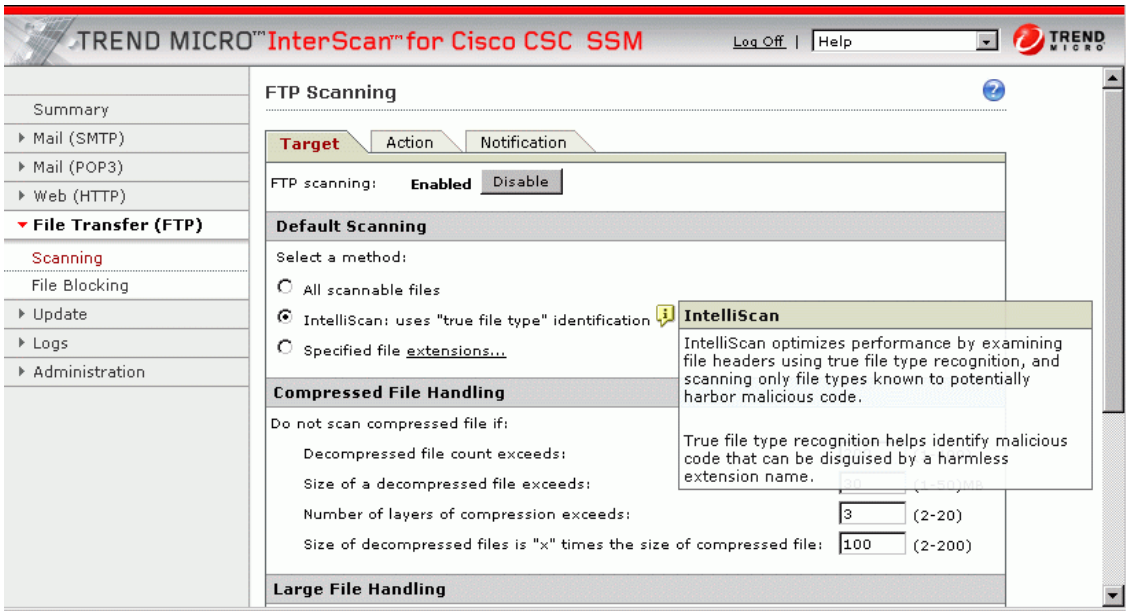
Trend Micro for Cisco CSC SSM ユーザ インターフェイスの多くのウィンドウには、デフォルトの選択値が含まれているフィールドがあります。デフォルトの選択値は大部分のユーザに最適な選択を表わしますが、別の選択が環境に適している場合は自由に変更できます。個々のフィールドのエントリの詳細については、オンライン ヘルプを参照してください。

通知を作成できるフィールドには、デフォルトのメッセージが含まれています。既存のエントリの上に入力して、デフォルトの通知を変更することができます。

ツールチップ アイコン

CSC SSM コンソールの一部のウィンドウには、ツールチップと呼ばれる情報アイコンがあります。マウスをツールチップ アイコンの上に置くと、ポップアップ テキストボックスが開き、決定を行ったりタスクを完了したりするのに役立つ追加情報が表示されます。次の例では、ツールチップ アイコンの上にマウスを置くことにより、ウイルス スキャン オプションの 1 つである IntelliScan に関する詳細が表示されています。

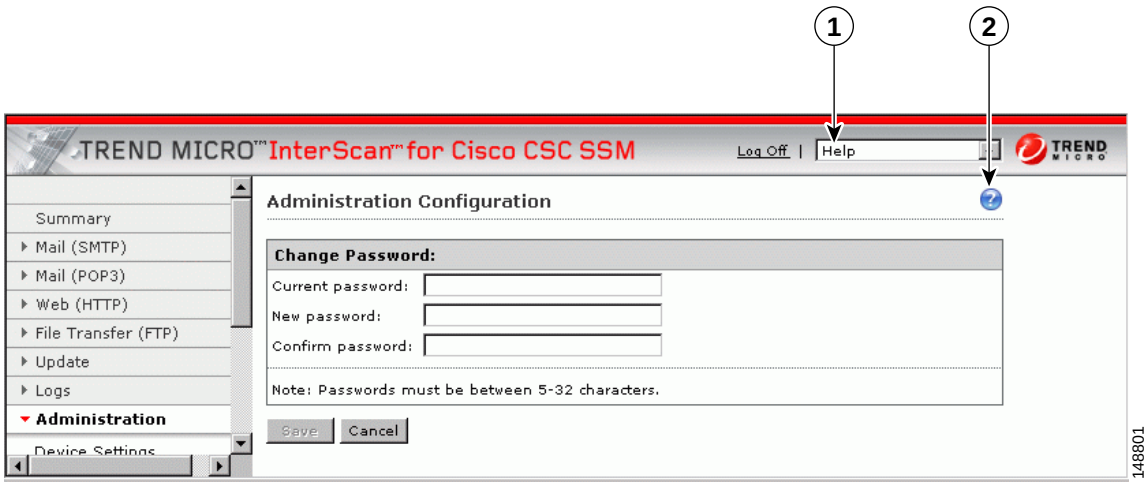
図 1-6　情報アイコン（ツールチップ）



オンライン ヘルプ

Trend Micro InterScan for Cisco CSC SSM では、2 種類のオンライン ヘルプが利用できます。一般ヘルプと状況依存ヘルプがあります。

図 1-7　一般オンライン ヘルプおよび状況依存オンライン ヘルプ



1	Help ドロップダウン メニュー	2	Help アイコン

Trend Micro InterScan for Cisco CSC SSM バナーの Help ドロップダウン メニューから Contents タブおよび Index タブをクリックして、一般ヘルプを起動します。2 番目のブラウザ ウィンドウが開き、ヘルプの内容を表示することができます。プラス記号をクリックして、ヘルプ トピックを展開します。

図 1-8　オンライン ヘルプの内容

概要に続いて、オンライン ヘルプ トピックの構成が、ユーザ インターフェイスの左メニューの構成に似た形で表示されます。オンライン ヘルプの内容の最後にコンピュータ ウイルスに関する有用な情報があります。

Index タブをクリックしてオンライン ヘルプのインデックスを表示するか、**Search** をクリックしてキーワードを使用して情報を検索します。

状況依存ヘルプを起動するには、ウィンドウのヘルプ アイコン（）をクリックします。2 番目のブラウザ ウィンドウが開き、現在ユーザ インターフェイスに表示されているウィンドウについての情報が表示されます。

オンライン ヘルプのリンク

オンライン ヘルプにはリンクがあり、青い下線が引かれた文字列で表示されています。リンクをクリックすると、別のヘルプ ウィンドウが表示されるか、ポップアップ テキストボックスが開き、定義などの追加情報が表示されます。オンライン ヘルプのこの機能を使用するには、ブラウザのポップアップ ブロッキングをディセーブルにしておきます。

オンライン ヘルプの大部分の情報は、この『*アドミニストレータ ガイド*』には記載されていません。Trend Micro InterScan for Cisco CSC SSM の詳細については、必ずオンライン ヘルプを参照してください。

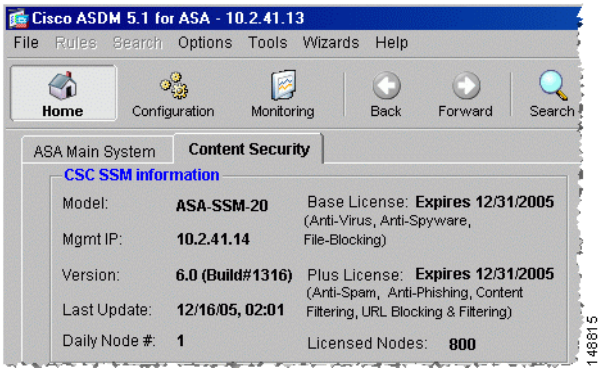
ライセンス

この章の概要で説明したように、Trend Micro InterScan for CSC SSM のライセンスには、Base ライセンスと Plus ライセンスの 2 つのレベルがあります。Base ライセンスでは、アンチウイルス、アンチスパイウェア、およびファイル ブロッキング機能が提供されます。Plus ライセンスでは、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 フィルタリング機能が追加されます。Plus ライセンスを有効にするには、Base ライセンスが必要です。

Base ライセンスのみを購入した場合、ライセンスのない機能が CSC SSM コンソールに表示されることがありますが、それらの機能は動作しません。しかし、オンライン ヘルプでライセンスのない機能を表示することはできます。また、Plus ライセンスで提供される追加機能を後で購入することもできます。

購入したライセンスのレベルがわからない場合は、Content Security タブの CSC SSM Information セクションを調べてください。このセクションにライセンス情報が要約されています。

図 1-9　Content Security タブのライセンス情報の場所



または、CSC SSM コンソールで、**Administration > Product License** をクリックして Product License ウィンドウを表示します。ウィンドウの Plus License セクションまでスクロールして、**Status** フィールドを確認します。このフィールドに「Activated」が表示されている場合は、Plus ライセンスの機能があります。Plus ライセンスの機能がない場合、このフィールドには「Not Activated」が表示されています。

Plus ライセンスが必要なウィンドウ

表 1-2 に、Base ライセンスだけで有効な CSC SSM コンソールのウィンドウと、追加の Plus ライセンスを購入した場合にのみ有効なウィンドウを示します。

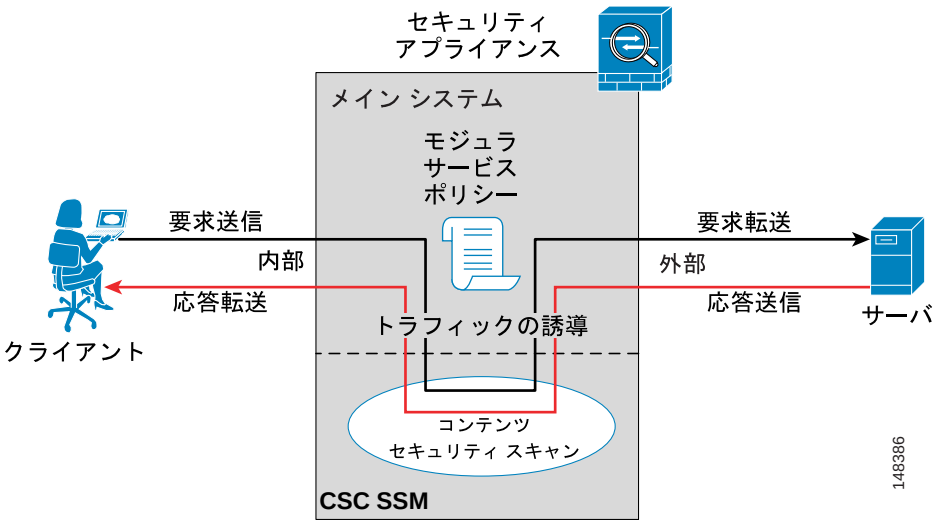
表 1-2　使用可能なウィンドウとライセンス

画面のタイトル	Base ライセンス	Plus ライセンス
Summary > Status/Mail (SMTP)/Mail (POP3)/Web (HTTP)/File Transfer (FTP)	X	
Mail (SMTP) > Scanning > Incoming > Target/Action/Notification	X	
Mail (SMTP) > Scanning > Outgoing > Target/Action/Notification	X	
Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam Target/Action		X
Mail (SMTP) > Content Filtering > Incoming > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Content Filtering > Outgoing > SMTP Incoming Content Filtering Target/Action/Notification		X
Mail (SMTP) > Configuration > Message Filter/Disclaimer/Incoming Mail Domain	X	
Mail (POP3) > Scanning > POP3 Scanning > Target/Action/Notification	X	
Mail (POP3) > Anti-spam > POP3 Anti-spam Target/Action		X
Mail (POP3) > Content Filtering > POP3 Content Filtering Target/Action/Notification		X
Web (HTTP) > Scanning > Target/Webmail Scanning/Action/Notification	X	
Web (HTTP) > File Blocking > Target/Notification	X	
Web (HTTP) > URL Blocking > Via Local List/PhishTrap/Notification		X
Web (HTTP) > URL Filtering > Filtering Rules		X
Web (HTTP) > URL Filtering > Settings > URL Filtering Settings URL Categories/Exceptions/Schedule/Re-classify URL		X
File Transfer (FTP) > Scanning > FTP Scanning Target/Action/Notification	X	
File Transfer (FTP) > File Blocking> Action/Notification	X	
Update > すべての画面	X	
Logs > すべての画面	X	
Administration > すべての画面	X	

プロセス フロー

図 1-10 に、セキュリティ アプライアンスに CSC SSM がインストールされている場合のトラフィックのフローを示します。要求がクライアント ワークステーションからサーバに送信されます。この要求は、セキュリティ アプライアンスによって処理されるとき、コンテンツ セキュリティ スキャンのために CSC SSM に誘導されます。セキュリティ リスクが検出されなければ、この要求はサーバに転送されます。応答の場合も逆順で同じパターンになります。

図 1-10　プロセス フロー



セキュリティ リスクが検出された場合は、CSC SSM の設定状況に従って、無害化または削除されます。