初期セットアップの確認

この章では、Trend Micro InterScan for Cisco CSC SSM が正しく動作していることを確認する方法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。

ASA クロック セットアップの確認

セットアップの確認を開始するには、まず ASA クロックが正しく設定されていることを確認する必要があります。この設定を確認するには、**Configuration > Properties** をクリックします。Properties メニューで、Device Administration トピックを展開し、**Clock** をクリックします。詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』を参照してください。

CSC SSM のアクティベーションの確認

次に、CSC SSM が正しくアクティブになっていることを確認します。実際のデバイスに近づくことができる場合は、デバイスの背部にあるステータス LED を確認してください。ステータス LED は緑色に点灯している必要があります。LED がオレンジで点灯または点滅している場合は、カードがアクティブになっていないか、サービスが開始されていません。詳細については、P.2-6 の「ステータス LED の表示」を参照してください。

実際のデバイスに近づくことができない場合は、ASDM の Content Security タブを確認してください（図 1-9（P.1-12）を参照）。Content Security タブの左上部に表示されているデバイスの型番、管理 IP、バージョンなどを確認する必要があります。確認できない場合は、TAC に問い合せてサポートを受けてください。

スキャンの確認

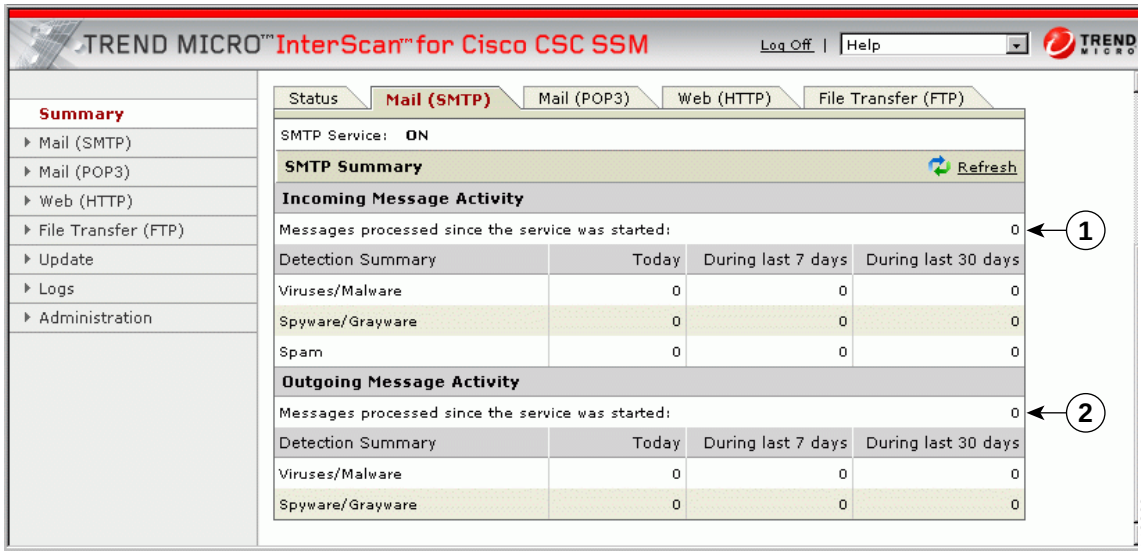
SSM にトラフィックを転送するように ASA を設定すると、CSC SSM コンソールにログオンする前であっても、Trend Micro InterScan for Cisco CSC SSM は、ウイルスやその他のマルウェアがないかどうか、すぐにスキャンを開始します。スキャンは、ログオンしているかどうかにかかわらず実行され、手動でオフにしない限り実行され続けます。

Trend Micro InterScan for Cisco CSC SSM が SMTP ネットワーク トラフィックをスキャンしていることを確認するには、次の手順を実行します。

- ASDM で、Content Security タブの Email Scan ペインを調べます。Email Scanned Count グラフが増加している必要があります。
- CSC SSM コンソールで、Summary ウィンドウの **Mail (SMTP)** タブをクリックします。Summary - Mail (SMTP) ウィンドウの「Incoming Message Activity」および「Outgoing Message Activity」セクションにある **Messages processed since the service was started** フィールドを調べます。図 2-1 に例を示します。

（注） また、コマンドライン インターフェイスから、パケットが CSC SSM に転送されていることを確認することもできます。**show service-policy csc** コマンドを使用します。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

図 2-1　Summary ウィンドウでのスキャンの確認



1	着信メッセージ アクティビティ カウンタ	2	発信メッセージ アクティビティ カウンタ

メッセージ アクティビティ カウンタは、トラフィックがネットワークを通過するにつれて増加します。カウンタをアップデートするには、Refresh リンクをクリックします。

（注） サービスが再開始されると、常にカウンタもリセットされます。

POP3 トラフィックについて同様のテストを実行するには、**Mail (POP3)** タブをクリックするか、POP3 トラフィックのカウントが示す ASDM の Email Scanned Count グラフを表示します。

アンチウイルス機能のテスト

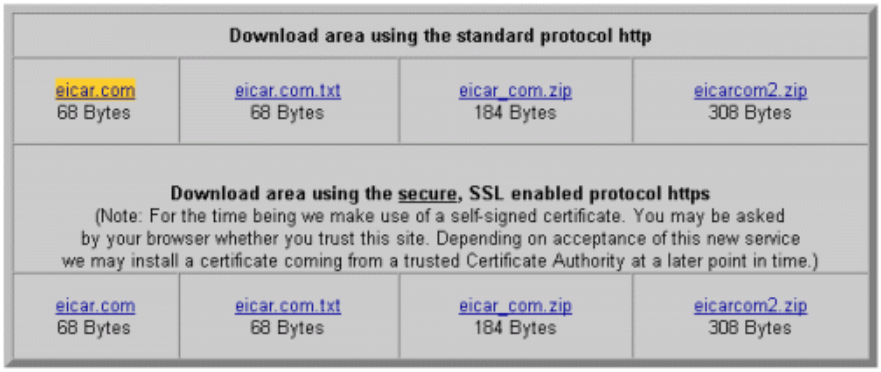
European Institute for Computer Antivirus Research （EICAR）は、Trend Micro InterScan for Cisco CSC SSM などのアンチウイルス テクノロジーによって本物のウイルスとして検出される、安全なテスト ウイルスを開発しました。このテスト ウイルスは、.com 拡張子を持つテキスト ファイルで、ウイルス コードは断片であれ、まったく含まれていません。このテスト ウイルスを使用してウイルス事象を発生させ、電子メール通知およびウイルス ログが正しく動作することを確認します。

テストを実行するには、ブラウザ ウィンドウを開いて次の URL にアクセスします。

http://www.eicar.com/anti_virus_test_file.htm

図 2-2 に示す情報ボックスが表示されるまでスクロールします。

図 2-2　EICAR ダウンロード エリア



eicar.com リンクをクリックします。セキュリティ イベントが発生したことを知らせる通知が、すぐにブラウザで受信されます。CSC SSM コンソールで **Logs > Query** に移動して、ウイルス / マルウェア ログ ファイルをクエリーし、ログに記録されたテスト ウイルスの検出を確認することができます。また、インストール時に（**Host Configuration** インストール ウィンドウで）選択した管理者の電子メール アドレスにも通知が送信されます。

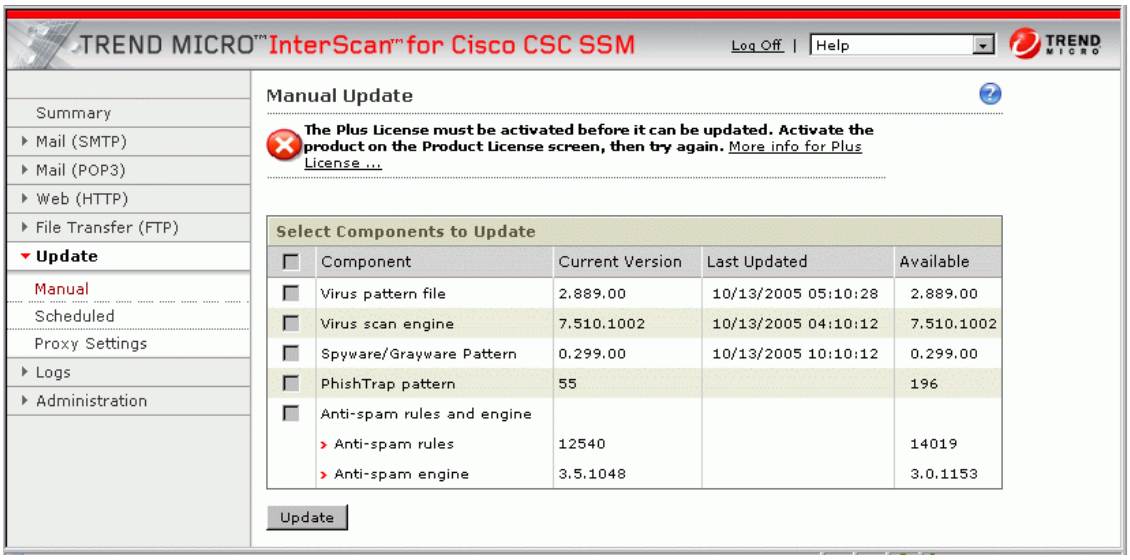
送信されない場合は、次のいずれかが考えられます。

1. CSC SSM がアクティブになっていない可能性があります。P.2-1 の「CSC SSM のアクティベーションの確認」の情報によってデバイスがアクティブになっていることを確認します。
2. ASA の設定が誤っている可能性があります。詳細については、P.8-12 の「不正な ASA ファイアウォール ポリシー設定のためにスキャンが動作しない」を参照してください。
3. CSC SSM が、リブート処理中である、またはソフトウェア障害が発生しているといった、障害状態となっています。実際に障害の場合は、syslog エラー 421007 が生成されています。このエラーがあるかどうか、syslog をチェックしてください。また、TAC に問い合せる前に、P.8-12 の「CSC SSM が失敗ステータスにあるためにスキャンが動作しない」で詳細を確認してください。

コンポーネントのステータスの確認

最新のウイルス パターン ファイル、スキャン エンジン、スパイウェア パターン ファイル、PhishTrap パターン、アンチスパム ルール、およびアンチスパム エンジンが CSC SSM コンソールにあるかどうかを確認するには、**Update > Manual** をクリックして、**Manual Update** ウィンドウを表示します。図 2-3 を参照してください。

図 2-3　Manual Update ウィンドウ



より新しいバージョンが使用できる場合は、アップデート バージョン番号が **Available** カラムに赤で表示されます。アップデートするコンポーネントを選択し、**Update** をクリックして選択したコンポーネントの最新バージョンをダウンロードします。

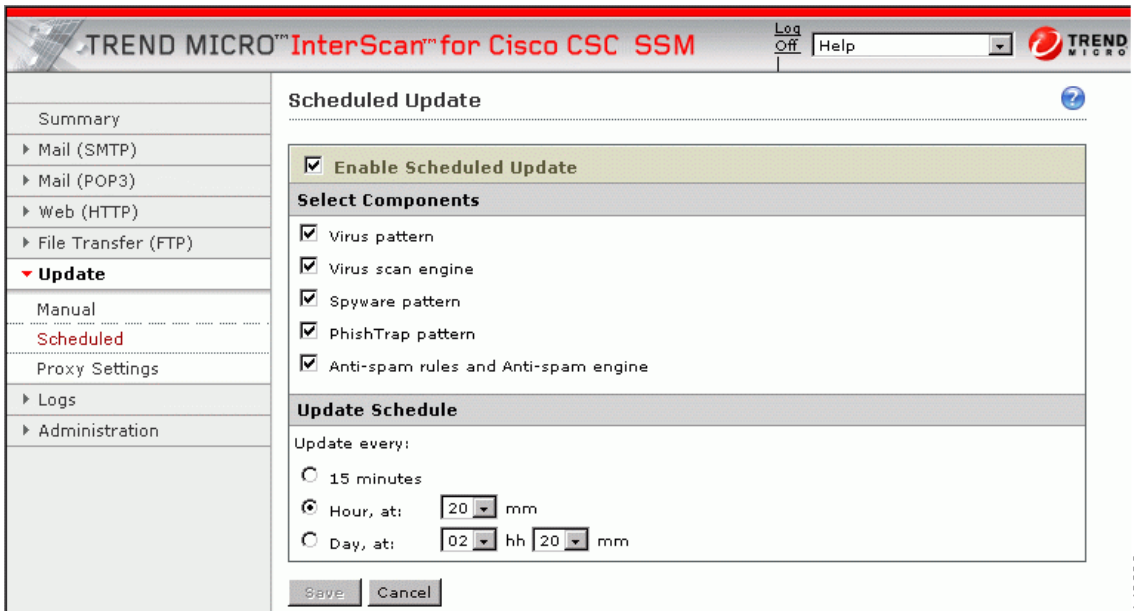
ヒント

現在のバージョンと使用可能なバージョンが同じで、新しいバージョンが入手できると考えられる場合、または **Available** カラムが空白の場合は、次のいずれかの可能性があります。

1. Trend Micro ActiveUpdate サーバがダウンしている。
2. ネットワークに問題がある。
3. 使用可能な新しいコンポーネントは存在せず、すべて実際に最新のものである。
4. Trend Micro InterScan for Cisco CSC SSM が正しく設定されていない。

不確定要素を回避するには、**Update > Scheduled** をクリックして、Scheduled Update ウィンドウを表示します。図 2-4 を参照してください。

図 2-4　Scheduled Update ウィンドウ

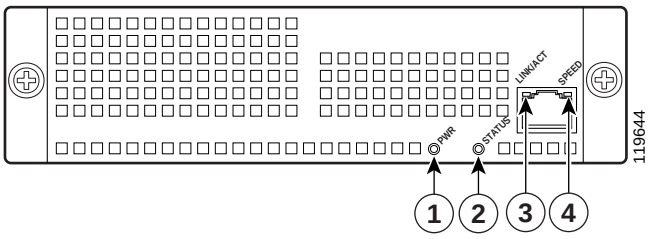


デフォルトでは、Trend Micro InterScan for Cisco CSC SSM は定期的にコンポーネントをアップデートし、スケジュールされたアップデートの実行後に自動的に通知を行います。スケジュールされたアップデートの間隔を変更して、アップデートの頻度を多くしたり少なくしたりすることができます。

ステータス LED の表示

アプライアンスの背面に、ASA SSM インジケータの**ステータス** LED があります。図 2-5 を参照してください。

図 2-5　ASA SSM インジケータ



ステータス LED には **2** のラベルが付いています。**ステータス** LED には、次の表に示す複数の状態があります。

表 2-1　ASA-SSM インジケータ

	LED	色	状態	説明
1	電源	緑	オン	システムは通電状態です。
2	ステータス	緑色およびオレンジ	点滅	SSM は動作中でアクティブですが、スキャン サービスはダウンしています。点滅が 1 分以上続く場合は、CSC SSM が新しいパターン ファイル / スキャン エンジンをロード中であるか、または、問題のトラブルシューティングを行う必要がある場合です。
		緑	点灯	SSM は起動されていますが、アクティブではありません。
		オレンジ	点灯	SSM は電源投入診断に合格しました。これは通常の動作ステータスです。
3	リンク / アクティブ	緑	点灯	イーサネット リンクがあります。
			点滅	イーサネット アクティビティが発生しています。
4	速度	緑	100 MB	ネットワーク アクティビティが発生しています。
		オレンジ	1000 MB（ギガビット イーサネット）	ネットワーク アクティビティが発生しています。

（注）　**1**、**3**、および **4** のラベルが付いた LED は CSC SSM ソフトウェアでは使用されません。

SSM 管理ポート トラフィックについて

インストール時に（IP Configuration インストール ウィンドウで）、管理インターフェイスの IP アドレス、ゲートウェイ IP、およびマスク IP を選択します。次に管理ポートを使用するトラフィックのリストを示します。

- **ActiveUpdate**：Trend Micro InterScan for Cisco CSC SSM が新しいパターン ファイルおよびスキャン エンジンのアップデートをダウンロードする Trend Micro アップデート サーバとの通信
- **URL rating lookups**：URL ブロッキングおよびフィルタリングを実行する Plus ライセンスを購入した場合に使用される、URL フィルタリング データベースのダウンロード
- **Syslog**：このポートは Trend Micro InterScan for Cisco CSC SSM から syslog サーバへのデータのアップロードに使用されます
- **Email notifications**：ウイルス検出などのトリガー イベントの通知が SSM 管理ポート経由で送信されます
- **DNS lookup**：管理ポートは、Trend Micro サーバ IP を検索するために、パターン ファイルのアップデートに使用されるホスト名の解決にも使用されます
- **Cisco ASDM/Trend Micro GUI access**：管理ポートは Cisco ASDM インターフェイスと Trend Micro InterScan for Cisco CSC SSM インターフェイスの間の通信を可能にします