Trend Micro InterScan for Cisco CSC SSM の管理

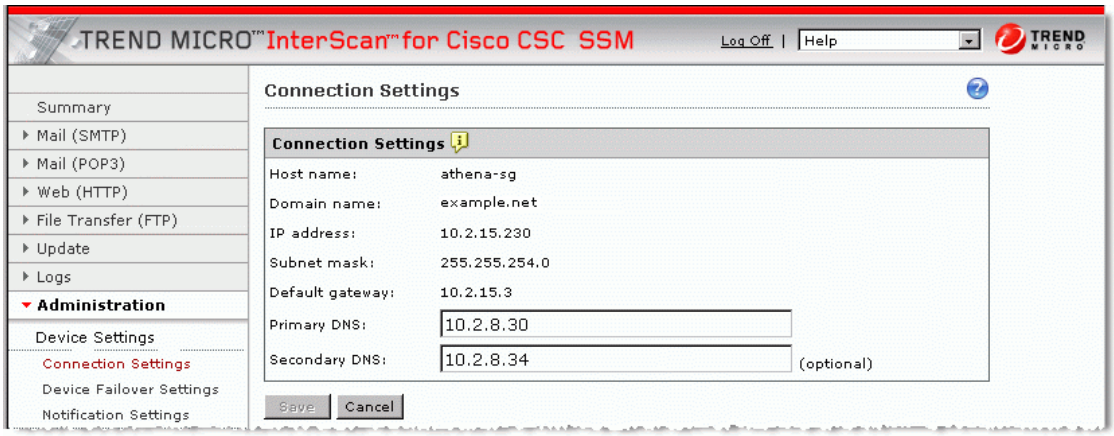
この章では、パッチのインストールなど実行頻度が少ないタスクについて説明します。この章は、次の項で構成されています。

- 接続設定（P.6-2）
- 管理電子メールおよび通知の設定の管理（P.6-3）
- コンフィギュレーションのバックアップの実行（P.6-4）
- フェールオーバーの設定（P.6-5）
- システム パッチのインストール（P.6-7）
- 製品ライセンスの表示（P.6-8）

接続設定

ネットワークの接続設定を表示するには、**Administration > Device Settings > Connection Settings** を選択します。**Connection Settings** ウィンドウ（図 6-1 を参照）に、インストール時に行った選択が表示されます。

図 6-1　Connection Settings ウィンドウ



この画面では、**Primary DNS** および **Secondary DNS** の IP アドレス フィールドを変更することができます。ホスト名、ドメイン名、または IP アドレスなど、その他の接続設定を変更するには、**Configuration > Trend Micro Content Security** と進み、メニューから **CSC Setup** を選択します。

これらの設定は、コマンドライン インターフェイス（CLI）を使用して変更することもできます。CLI にログインし、**session 1** コマンドを発行します。CLI に初めてログインする場合は、デフォルトのユーザ名（cisco）とパスワード（cisco）を使用します。パスワードを変更するよう求められます。

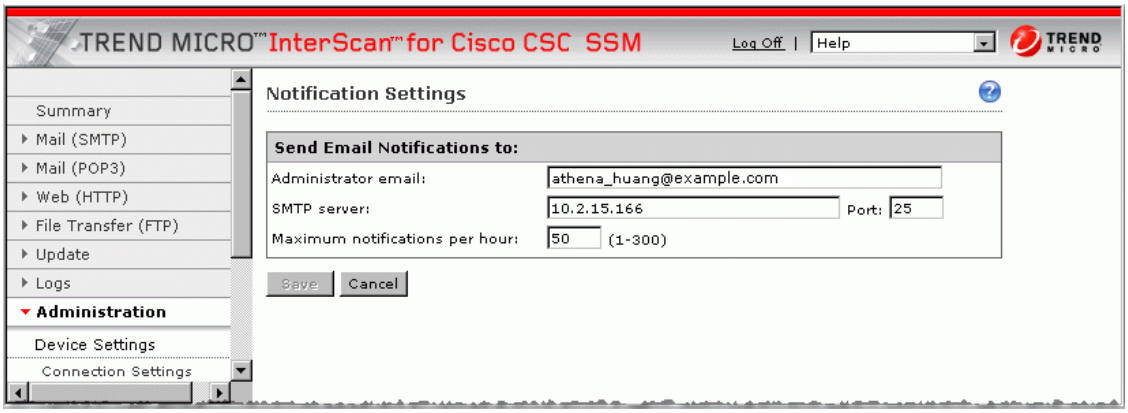
ログインした後、Trend Micro InterScan for Cisco CSC SSM Setup Wizard メニューからオプション **1** の Network Settings を選択します。プロンプトに従って設定を変更します。詳細については、P.A-6 の「インストールの手順」を参照してください。

管理電子メールおよび通知の設定の管理

Notification Settings ウィンドウ（図 6-2 を参照）では、次の作業を行うことができます。

- インストール時に（**Host Configuration** ウィンドウで）選択した管理者電子メール アドレスの表示または変更（あるいはその両方）
- インストール時に（**Host Configuration** ウィンドウで）選択した SMTP サーバの IP およびポートの表示
- 1 時間あたりの管理者通知の最大数の設定

図 6-2　Notification Settings ウィンドウ



このウィンドウで変更を行うには、新しい情報を入力し、**Save** をクリックします。

これらの変更は、ASDM で **Configuration > Trend Micro Content Security** を選択した後、メニューから **CSC Setup** を選択して行うこともできます。

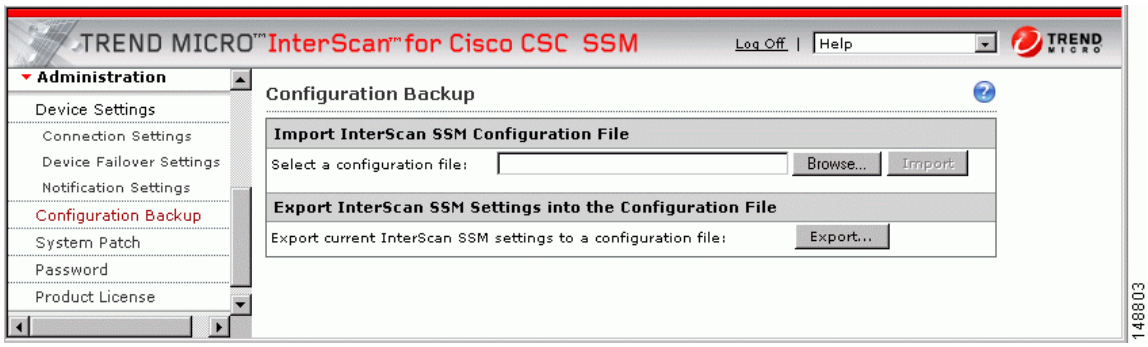
コンフィギュレーションのバックアップの実行

Trend Micro InterScan for Cisco CSC SSM には、デバイスのコンフィギュレーションをバックアップして圧縮ファイルに保存する機能があります。保存したコンフィギュレーションをインポートし、システムを保存時の設定に復元することができます。

（注）　ASDM/Web GUI パスワードを忘れた場合、コンフィギュレーションのバックアップはリカバリにきわめて重要です。詳細については、P.8-7 の「失ったパスワードの回復」を参照してください。

前の章の手順に従って Trend Micro InterScan for Cisco CSC SSM の設定が終了したら、すぐにコンフィギュレーションのバックアップを実行してください。**Administration > Configuration Backup** と進んで、**Configuration Backup** ウィンドウを表示します。図 6-3 を参照してください。

図 6-3　Configuration Backup ウィンドウ



コンフィギュレーションのエクスポート（保存）

Export をクリックして、コンフィギュレーション設定を保存します。**File Download** ダイアログボックスが表示されます。デフォルトで config.tgz という名前のファイルを開くか、ファイルをコンピュータに保存することができます。

コンフィギュレーションのインポート

保存したコンフィギュレーション ファイルを復元するには、**Configuration Backup** ウィンドウで、**Browse** をクリックします。config.tgz ファイルを見つけて、**Import** をクリックします。ファイル名が **Select a configuration file** フィールドに表示されます。保存されていたコンフィギュレーション設定がアプライアンスに復元されます。

保存されていたコンフィギュレーション ファイルをインポートすると、スキャン サービスが再開されます。たとえば、**Summary** ウィンドウのカウンタがリセットされることに注意する必要があります。

フェールオーバーの設定

Trend Micro InterScan for Cisco CSC SSM には、ASA のデバイス フェールオーバー機能をサポートして、コンフィギュレーションをピア装置に複製する機能があります。ピア装置または CSC SSM をフェールオーバー デバイスに設定する前に、まずプライマリ デバイスの設定を終了します。つまり、スパイウェア / グレーウェア スキャンをイネーブルにし、通知をカスタマイズする予定がある場合は、カスタマイズするなどです。

プライマリ デバイスが必要な動作を行うように設定したら、次のチェックリストの手順を実行して、フェールオーバー ピアを設定します。チェックリストを印刷して、進捗に応じて手順を記録するのに使用します。

手順	フェールオーバー設定のチェックリスト	確認チェック
1	プライマリ デバイスとして動作するアプライアンス、およびセカンダリ デバイスとして動作させるアプライアンスを決定します。ここにそれぞれの IP アドレスを記録します。 **メモ：** _____ _____	❑ ❑
2	ブラウザのウィンドウを開き、次の URL を **Address** フィールドに入力します。http://<primary device IP address>:8443。**Logon** ウィンドウが表示されます。ログインして、**Administration > Device Settings > Device Failover Settings** と移動します。	❑
3	2 番目のブラウザのウィンドウを開き、次の URL を **Address** フィールドに入力します。http://<secondary device IP address>:8443。ステップ 2 では、ログインして **Device Failover Settings** ウィンドウに移動します。	❑
4	プライマリ デバイスの **Device Failover Settings** ウィンドウで、セカンダリ デバイスの IP アドレスを **Peer IP address** フィールドに入力します。1 ～ 8 文字の英数字の暗号キーを **Encryption key** フィールドに入力します。**Save** をクリックし、次に **Enable** をクリックします。ウィンドウ タイトルの下に次のメッセージが表示されます。 `InterScan for CSC SSM could not establish a connection because the failover peer device is not yet configured. Please configure the failover peer device, then try again.` このメッセージは正常で、ピアがまだ設定されていないために表示されます。この時点ではこのメッセージに注意する必要はありません。	❑
5	セカンダリ デバイスの **Device Failover Settings** ウィンドウで、プライマリ デバイスの IP アドレスを **Peer IP address** フィールドに入力します。1 ～ 8 文字の英数字の暗号キーを **Encryption key** フィールドに入力します。暗号キーは、プライマリ デバイスに入力したキーと同じにする必要があります。**Save** をクリックし、次に **Enable** をクリックします。ウィンドウ タイトルの下に次のメッセージが表示されます。 `InterScan for CSC SSM has successfully connected with the failover peer device.` *この時点ではセカンダリ デバイスで他の操作をしないでください。*	❑

手順	フェールオーバー設定のチェックリスト	確認チェック
6	プライマリ デバイスの **Device Failover Settings** ウィンドウに戻り、**Synchronize with peer** をクリックします。	❑
7	ウィンドウの下部にある **Status** フィールドのメッセージは、次のように同期化の日時を表示するはずです。 `Status: Last synchronized with peer on: 09/29/2005 15:20:11`	❑

注意　ステップ 5 の最後で、セカンダリ デバイスの **Device Failover Settings** ウィンドウがまだ表示されている間は、絶対に **Synchronize with peer** をクリックしないでください。クリックした場合、プライマリ デバイスですでに設定したコンフィギュレーションが消去されます。ステップ 6 の手順に従って、プライマリ デバイスから手動で同期化を実行する必要があります。

チェックリストの手順を完了すると、フェールオーバー関係が正常に設定されています。

将来コンフィギュレーションを変更する場合、たとえば、スパム フィルタリングしきい値を Low から Medium に変更する場合は、プライマリ デバイスのみでコンフィギュレーションを変更する必要があります。Trend Micro InterScan for Cisco CSC SSM はコンフィギュレーションのミスマッチを検出し、最初のデバイスで行ったコンフィギュレーションの変更でピアをアップデートします。

自動同期化機能の例外は、システム パッチのアップロードです。パッチは、プライマリ デバイスとセカンダリ デバイスの両方に適用する必要があります。詳細については、P.6-7 の「システム パッチのインストール」を参照してください。

何らかの理由でピア デバイスを使用できない場合は、電子メール通知が管理者に送信されます。ピアの問題が解決されるまでメッセージは定期的に送信され続けます。

システム パッチのインストール

既知の問題を修正するシステム パッチ、または新しい機能を提供するシステム パッチが、必要に応じ利用可能になります。まず Web サイトまたは提供された CD からシステム パッチをダウンロードしてから、**Administration > System Patch** と進んで **System Patch** ウィンドウを表示します。図 6-4 を参照してください。

図 6-4　System Patch ウィンドウ

注意　パッチ アプリケーションはシステム サービスを再開始し、システムの運用を中断する場合があります。デバイスの動作中にシステムにパッチを適用すると、ウイルスやマルウェアが含まれているトラフィックにネットワークの通過を許可することがあります。

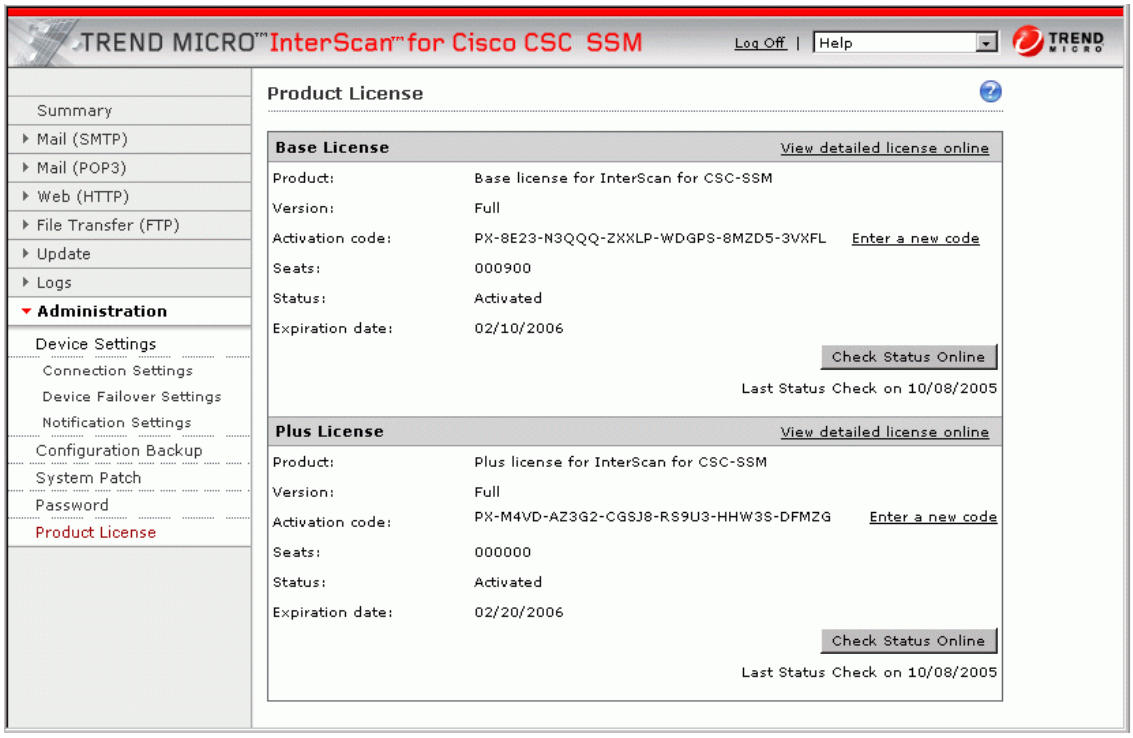
システム パッチの適用と削除の詳細については、このウィンドウのオンライン ヘルプを参照してください。

製品ライセンスの表示

Product License ウィンドウ（図 6-5 を参照）では、製品ライセンスの次の項目のステータスを確認することができます。

- 有効なライセンス（Base ライセンスのみ、または Base ライセンスと Plus ライセンス）
- ライセンスのバージョン（一時的に「Evaluation」コピーを使用している場合を除き、「Full」を示している必要があります）
- ライセンスのアクティベーション コード
- ライセンス許諾数（ユーザ）：この情報は、Plus ライセンスを購入した場合にも、Base ライセンスに対してのみ表示されます。
- ステータス。「Activated」である必要があります。
- ライセンスの有効期限：Base ライセンスと Plus ライセンスの両方がある場合、有効期限が異なる場合があります。

図 6-5　Product License ウィンドウ



ライセンスが更新されなかった場合、アンチウイルス スキャンは、期限切れに短い猶予期間を加えた時点で有効だったパターン ファイルのバージョン、およびスキャン エンジンで続行されます。しかし、その他の機能は使用できなくなる場合があります。詳細については、ライセンスの有効期限の項を参照してください。

ライセンスの有効期限

有効期限に近づいたとき、および有効期限を過ぎたとき、ウィンドウ ヘッダーの下の **Summary** ウィンドウに、図 6-6 の例に示すようなメッセージが表示されます。

図 6-6　ライセンスの有効期限のメッセージ

製品ライセンスの期限が切れた場合、Trend Micro InterScan for Cisco CSC SSM を継続して使用できますが、（ウイルス パターン ファイル、スキャン エンジンなどの）アップデートを受け取ることはできません。ネットワークは新しいセキュリティ上の脅威に対して保護されなくなる場合があります。

Plus ライセンスの期限が切れた場合、コンテンツ フィルタリングおよび URL フィルタリングは使用できなくなります。その場合、トラフィックはコンテンツまたは URL のフィルタリングなしで通過します。

Base ライセンスを購入してインストールした後に Plus ライセンスを購入した場合は、期限の期日が異なります。更新日が近づいたときに各ライセンスを別々に更新することができます。

ライセンス情報リンク

Product License ウィンドウには複数の役立つリンクがあります。リンクは次のとおりです。

- View detailed license online
- Check Status Online

View detailed license online リンクでは、Trend Micro オンライン登録 Web サイトにアクセスしてライセンスに関する情報を表示し、更新の方法を知ることができます。**Check Status Online** では、**Product License** ウィンドウのタイトルの下に、前の図の例と同様のライセンスのステータスを示すメッセージが表示されます。

詳細については、**Product License** ウィンドウのオンライン ヘルプを参照してください。