CHAPTER 5

アップデートおよびログ クエリーの管理

この章では、アップデート、プロキシ設定、syslog 設定、およびログ クエリー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。

コンポーネントのアップデート

今や、新しいウイルスやその他のセキュリティ リスクは、インターネットまたは他の配布方法を介して毎日絶え間なく「未開の地」（世界的なコンピューティング コミュニティで悪事をはたらくことを意味します）に送り出されています。TrendLabs はただちに新しい脅威を分析し、ウイルス パターン ファイルなどの新しい脅威の検出に必要なコンポーネントをアップデートする適切な手順を実行します。この迅速な対応によって、たとえば、今日の午前 3 時にアムステルダムで悪意のあるハッカーのコンピュータから新しいワームが送り出されたとしても、Trend Micro InterScan for Cisco CSC SSM は、これを検出することができます。

新しい脅威がネットワークに侵入しないように、コンポーネントを最新の状態に保つことがきわめて重要です。コンポーネントを最新の状態に保つには、次の作業を実行します。

- いつでもオンデマンドでコンポーネントの手動アップデートを実行します
- コンポーネントを定期的に自動でアップデートするアップデート スケジュールを設定します

手動またはスケジュールによって管理されるコンポーネントは次のとおりです。

- ウイルス パターン ファイル
- ウイルス スキャン エンジン
- スパイウェア パターン ファイル（他のタイプのグレーウェアのパターンも含む）
- PhishTrap パターン ファイル
- アンチスパム規則
- アンチスパム エンジン

PhishTrap パターン ファイル、アンチスパム規則、およびアンチスパム エンジンというコンポーネントは、Plus ライセンスを購入されている場合にのみアクティブでアップデートされます。

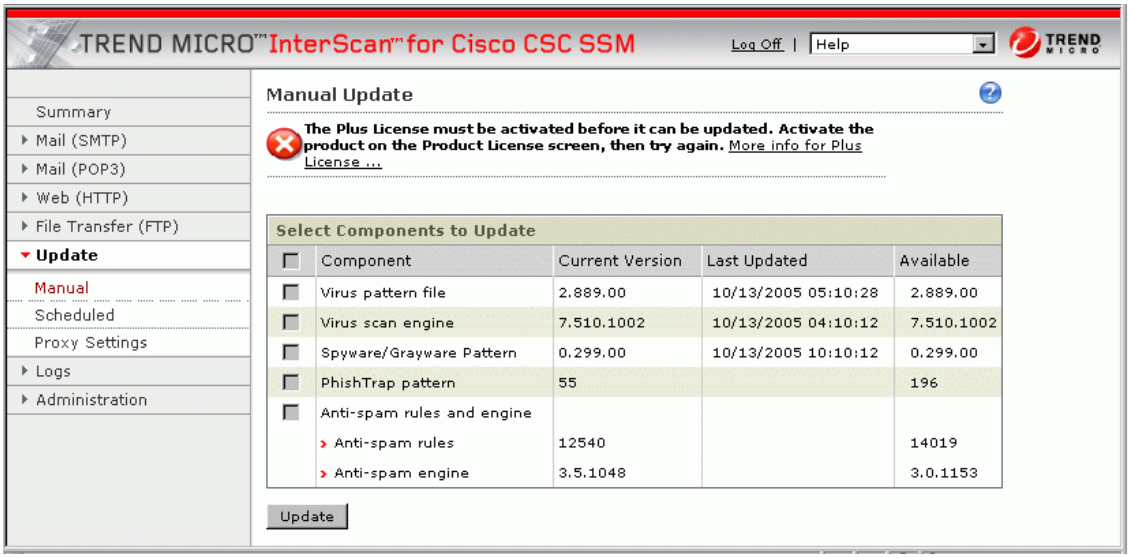
最新のコンポーネントがインストールされているかどうかを確認するには、**Manual Update** ウィンドウに進んでコンポーネントのステータスをチェックします。

（注） CSC SSM ソフトウェアは、スキャン エンジンおよびパターン ファイルのこれらのアップデートのロールバックはサポート*していません*。

手動アップデート

コンポーネントのステータスを表示するには、またはコンポーネントを手動でアップデートするには、**Updates > Manual** に進みます。**Manual Update** ウィンドウが表示されます（図 5-1 を参照）。

図 5-1　Manual Update ウィンドウ



ウィンドウの右側にある **Available** カラムをスキャンして、コンポーネントが古くなっているかどうかを即座に確認できます。より新しいコンポーネントを使用できる場合は、コンポーネントのバージョンが赤で表示されます。

たとえば、**Update** をクリックして最新のパターン ファイルのバージョンをダウンロードします。新しいパターン ファイルのダウンロード中は、進捗メッセージが表示されます。アップデートが完了すると、**Manual Update** ウィンドウがリフレッシュされ、最新のアップデートが適用されたことが表示されます。

この機能の詳細については、オンライン ヘルプを参照してください。

スケジュール アップデート

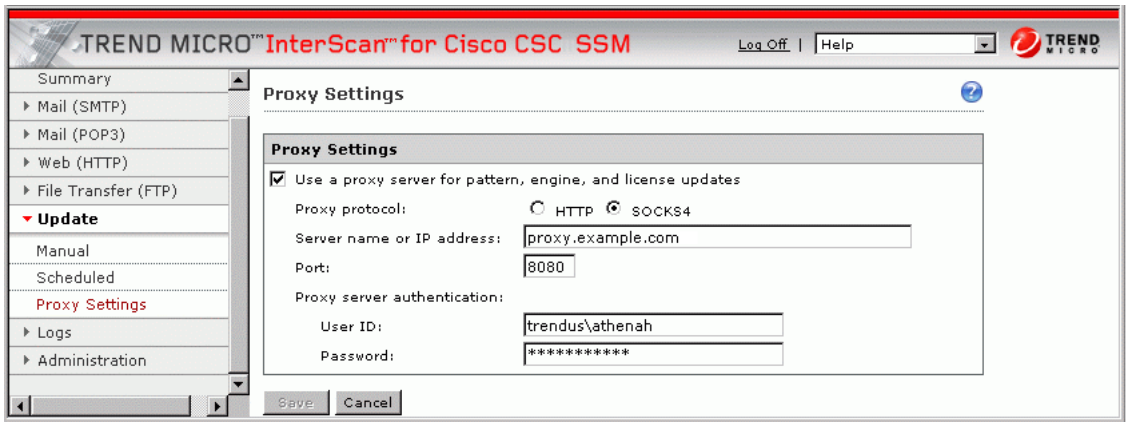
Scheduled Update ウィンドウでは、コンポーネントの更新を 15 分ごとに行うように設定できます。**Updates > Scheduled** と進んで、**Scheduled Update** ウィンドウを表示します。アップデート スケジュールごとにアップデートするコンポーネントを選択します。

スケジュールをそのままにするか、頻度を変更します。詳細については、オンライン ヘルプを参照してください。**Save** をクリックして、設定をアップデートします。

プロキシ設定

Trend Micro ActiveUpdate サーバとの通信にプロキシ サーバを使用している場合は、インストール時にプロキシ サーバの IP とポートを指定しています。**Update > Proxy Settings** をクリックすると、**Proxy Settings** ウィンドウにこれらの設定が表示されます。図 5-2 を参照してください。

図 5-2　プロキシ設定ウィンドウ



インストール時にプロキシを設定する場合、デフォルトで HTTP プロキシ プロトコルが設定されます。SOCKS4 に変更するには、**SOCKS4** オプション ボタンをクリックします。詳細については、オンライン ヘルプを参照してください。

このウィンドウで可能なその他の変更としては、オプションのプロキシ認証ユーザ名とパスワードを **User ID** および **Password** フィールドに追加することに限られます。終了したら、**Save** をクリックして設定をアップデートします。

Syslog 設定

インストール後に、ウイルスまたはスパイウェア / グレーウェアの検出などのログ データが一時的に保存されます。ログ データを格納するには、少なくとも 1 台（最大 3 台）の syslog サーバを設定します。**Logs > Settings** と進んで、**Log Settings** ウィンドウを表示します。

少なくとも 1 台の syslog サーバを設定します。**Enable** チェックボックスをオンにし、次に syslog サーバの IP、ポート、および優先プロトコル（UDP または TCP）を入力します。詳細については、オンライン ヘルプを参照してください。

デフォルトでは、検出されたセキュリティ リスクがロギングされます。使用していない機能のロギングをオフにすることができます。たとえば、Plus ライセンスを購入していない場合は、URL ブロッキング / アンチフィッシングおよび URL フィルタリングをオフにすることができます。

ログ データの選択と表示の詳細については、P.5-5 の「ログ データの表示」を参照してください。syslogs は ASDM から表示することもできます。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。

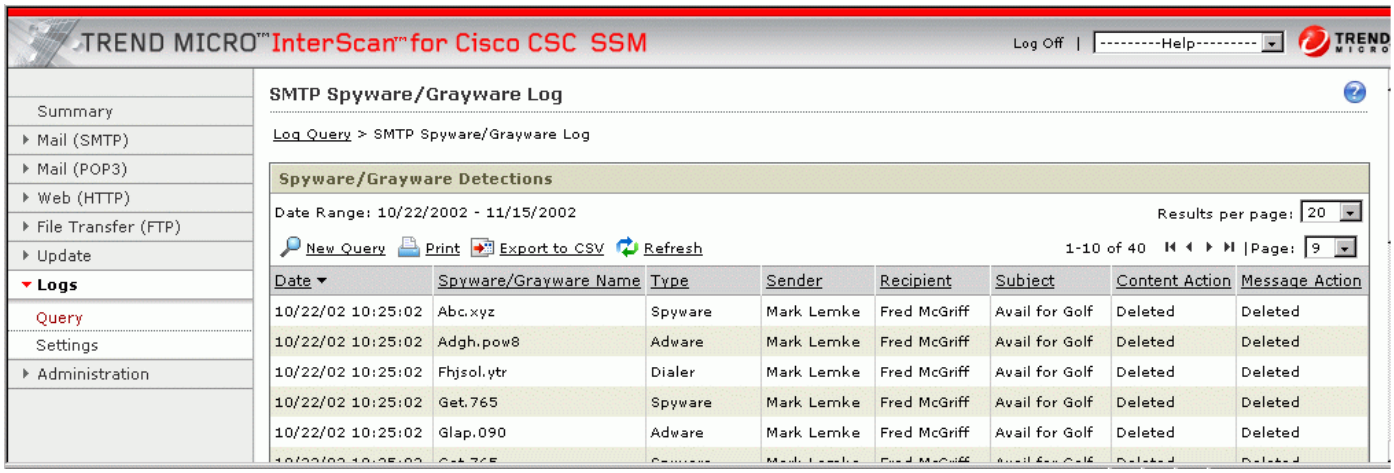
ログ データの表示

Trend Micro InterScan for Cisco CSC SSM をインストールして設定した後、セキュリティ リスクが検出され、それぞれのリスクのタイプに対して選択したアクションに従って処理されます。これらのイベントはログに記録されます。システム リソースを節約するため、これらのログは定期的に消去される場合があります。

ログを表示するには、**Logs > Query** と進んで **Log Query** ウィンドウを表示します。問い合せパラメータを指定し、**Display Log** をクリックしてログを表示します。詳細については、オンライン ヘルプを参照してください。

図 5-3 に、スパイウェア / グレーウェアのログの例を示します。

図 5-3　スパイウェア / グレーウェアのログ



スキャン パラメータの例外のロギング

Target タブで指定する次のスキャン パラメータの例外がウイルス / マルウェア ログに表示されます。

SMTP、POP3、HTTP および FTP の場合は、次のとおりです。

- 圧縮解除時に、指定したファイル数制限を越える圧縮ファイル
- 圧縮解除時に、指定したファイル サイズ制限を越える圧縮ファイル
- 圧縮レイヤ数が制限を越える圧縮ファイル
- 圧縮比率の制限を超える圧縮ファイル（圧縮解除されたファイルのサイズは圧縮ファイルのサイズの「x」倍）
- パスワード保護されたファイル（削除に対して設定されている場合）

HTTP および FTP のみの場合は、次のとおりです。

- スキャンを行うには大きすぎるファイルまたはダウンロード

これらのファイルは、ウイルス / マルウェア名の代わりに次のようなメッセージで示されます。

- Decompressed_File_Size_Exceeded
- Large_File_Scanning_Limit_Exceeded