

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 (P.5-2)
- プロキシ設定 (P.5-4)
- Syslog 設定 (P.5-4)
- ログデータの表示 (P.5-5)

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。



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)。

	Man	– Manual Update 🥑					
Summary Mail (SMTP) Mail (POP3) Web (HTTP)	mmary il (SMTP) ii (POP3) ib (HTTP)						
File Transfer (FTP)	Sel	ect Components to Update					
• Update		Component	Current Version	Last Updated	Available		
Manual		Virus pattern file	2.889.00	10/13/2005 05:10:28	2.889.00		
Scheduled		Virus scan engine	7.510.1002	10/13/2005 04:10:12	7.510.1002		
Proxy Settings		Spyware/Grayware Pattern	0.299.00	10/13/2005 10:10:12	0.299.00		
Logs		PhishTrap pattern	55		196		
Administration	- E	Anti-spam rules and engine					
		> Anti-spam rules	12540		14019		
		> Anti-spam engine	3.5.1048		3.0.1153		

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

	O‴InterScan″for Cisco	CSC SSM		END
Summary ▶ Mail (SMTP) ▶ Mail (POP3)	Proxy Settings		Ø	
 Web (HTTP) File Transfer (FTP) 	Proxy Settings Image: Construction of the set of the s	n, engine, and license updates		
✓ Update Manual Scheduled	Server name or IP address: Port:	proxy.example.com		
Proxy Settings Logs	Proxy server authentication: User ID:	trendus\athenah		
Administration	Password:			

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

Summary	SMTP Spyware/	SMTP Spyware/Grayware Log						2
Mail (SMTP)	Log Query > SMTP S	Log Query > SMTP Spyware/Grayware Log						
Mail (POP3)	Snyware/Graywa	are Detections						
▶ Web (HTTP)	Data Bases 10/22/							
File Transfer (FTP)	Date Kange: 10/22/	Porte Range: 10/22/2002 - 11/13/2002 Results per page: [20]						
▶ Update	New Query 🚢 🛛	Image: Print Pri						Page: 9 💌
- Logs	Date 🔻	Spyware/Grayware Name	Туре	Sender	Recipient	Subject	Content Action	Message Action
Query	10/22/02 10:25:02	Abc.×yz	Spyware	Mark Lemke	Fred McGriff	Avail for Golf	Deleted	Deleted
Settings	10/22/02 10:25:02	Adgh.pow8	Adware	Mark Lemke	Fred McGriff	Avail for Golf	Deleted	Deleted
Administration	10/22/02 10:25:02	Fhjsol.ytr	Dialer	Mark Lemke	Fred McGriff	Avail for Golf	Deleted	Deleted
	10/22/02 10:25:02	Get.765	Spyware	Mark Lemke	Fred McGriff	Avail for Golf	Deleted	Deleted
	10/22/02 10:25:02	Glap.090	Adware	Mark Lemke	Fred McGriff	Avail for Golf	Deleted	Deleted
	10/00/00 10:05:00	A-1 7/5	C	Manula I analia		a	N-1-4-4	Deleted.

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

