コンテンツ セキュリティのモニタリング

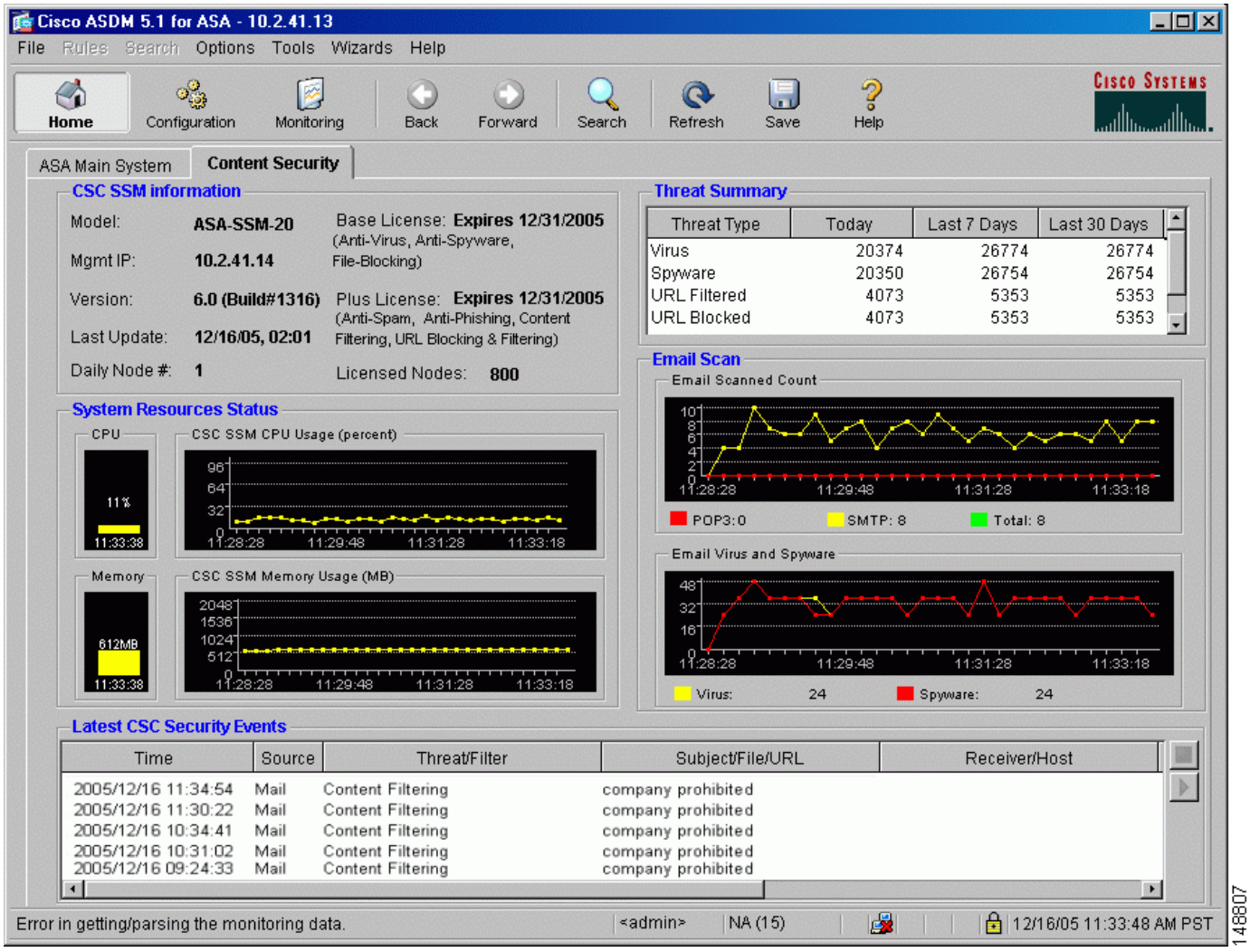
この章では、ASDM のコンテンツ セキュリティについて説明します。次の項で構成されています。

Content Security タブの機能

CSC SSM に接続すると、図 7-1 に示すように、Content Security タブが表示されます。Content Security タブでは、次のコンテンツ セキュリティ ステータスを一目で確認することができます。

- CSC SSM Information：製品モデル番号、デバイスの IP アドレス、CSC SSM ソフトウェアのバージョンおよびビルド番号、重要な通知情報
- Threat Summary：検出された脅威の当日、7 日、30 日ごとの検出数を表形式で表示
- System Resources Status：SSM の CPU およびメモリの使用状況の確認が可能
- Email Scan：スキャンされた電子メールの数およびスキャンした電子メールで検出された脅威の数をグラフィックで表示
- Latest CSC Security Events：最近ログに記録されたセキュリティ イベント 25 個をリスト表示

図 7-1　Content Security タブ



Help アイコンをクリックすると、このウィンドウに表示された情報の詳細が表示されます。

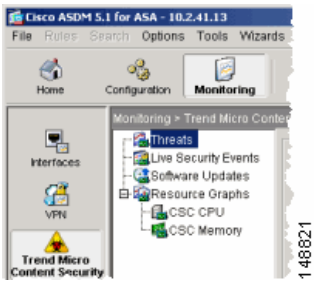
コンテンツ セキュリティのモニタリング

Monitoring > Trend Micro Content Security の順にクリックして、モニタリングのオプションを表示します。次のオプションがあります。

- Threats：最近検出された脅威をもたらすアクティビティを、後述のカテゴリ別にグラフで表示します。
- Live Security Events：モニタリング対象プロトコルで最近検出された、セキュリティ イベント（コンテンツフィルタリング違反、スパム、ウィルス検出、スパイウェア検出など）のレポートを表示します。
- Software Updates：コンテンツのセキュリティをスキャンする各種コンポーネント（ウィルス パターン ファイル、スキャン エンジン、スパイウェア / グレイウェア パターンなど）の、バージョンおよび最近のアップデート日時 / 時刻を表示します。
- Resource Graphs：SSM の CPU 使用状況とメモリの使用状況をグラフで表示します。

図 7-2 に、ASDM の Monitoring オプションの表示画面を示します。

図 7-2　ASDM のコンテンツ セキュリティの Monitoring オプション



脅威のモニタリング

Monitoring ペインで Threats をクリックすると、図 7-2 に示すように、最大 4 種類のグラフ表示用のカテゴリから選択できます。次のカテゴリ別に、最新アクティビティの件数を表示することができます。

- 検出されたウィルスおよび他の脅威
- ブロックされたスパイウェア
- 検出されたスパム（この機能を使用するには Plus ライセンスが必要です）
- URL フィルタリング アクティビティ、および URL ブロッキング アクティビティ（この機能を使用するには Plus ライセンスが必要です）

たとえば、Base と Plus の両方のライセンスがある場合は、上記の 4 種類すべての脅威タイプのモニタリングを選択できます。図 7-3 に、グラフの表示例を示します。

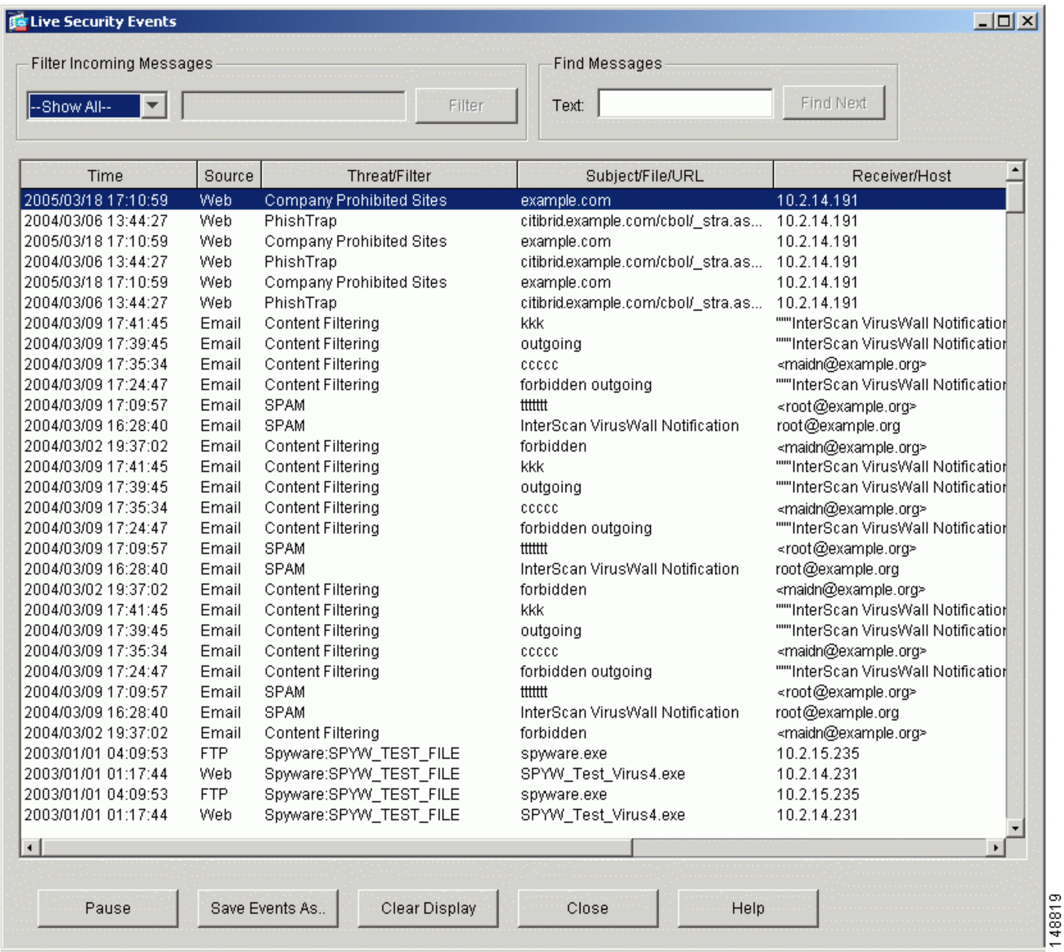
図 7-3　脅威のモニタリング グラフ

グラフは一定の時間間隔（通常は 10 秒）でリフレッシュされるため、最新のアクティビティが一目で分かります。詳細については、オンライン ヘルプを参照してください。

セキュリティ イベントのライブによるモニタリング

Monitoring ペインで Live Security Events をクリックして、**View** をクリックすると、図 7-4 のようなレポートが作成されます。

図 7-4　Live Security Events モニタリング レポート

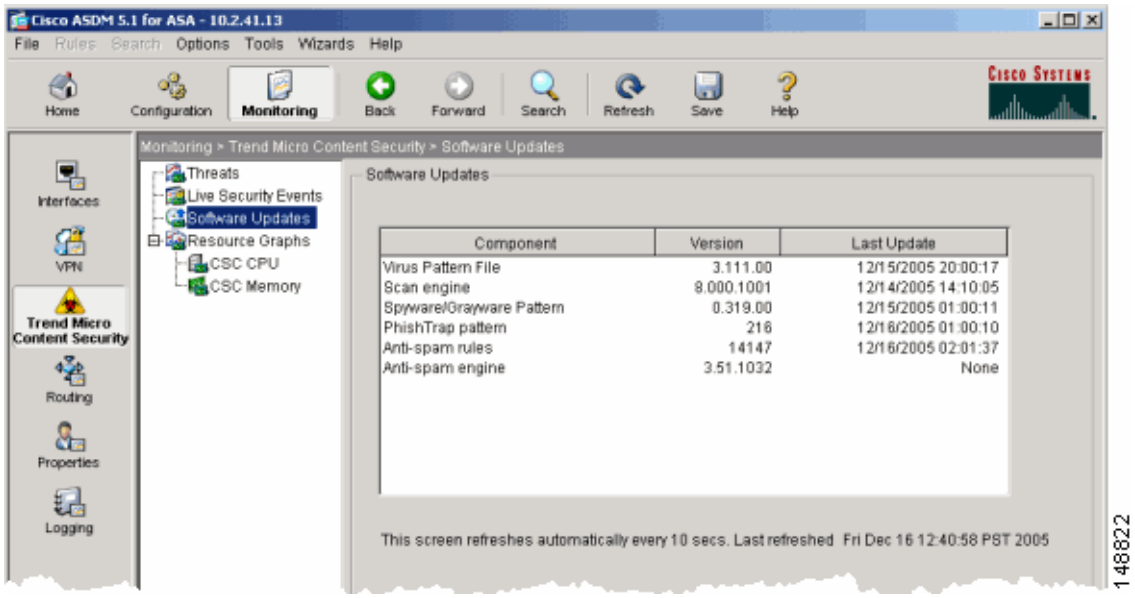


このレポートには、CSC SSM で検出されたすべてのイベントがリスト表示されます。**Source** カラムでは、検出ソースが SMTP と POP3 の両プロトコルの場合は「Email」と表示されます。縦横のスクロール バーで、画面に表示されなかった追加部分のレポート内容が確認できます。画面上部でフィルタリングを行うと、特定のイベントが検索されるように調整できます。詳細については、オンライン ヘルプを参照してください。

ソフトウェアのアップデートのモニタリング

図 7-5 のように、Monitoring ペインで Software Updates をクリックすると、CSC SSM のコンポーネントに関する情報が次のように表示されます。

図 7-5　Software Updates モニタリング ウィンドウ



ASDM で **Monitoring > Trend Micro Content Security > Software Updates** の順にクリックすると表示される、**Configure Updates** リンクをクリックすると、Scheduled Update ウィンドウが CSC SSM コンソールに表示されます。図 2-4（P.2-5）を参照してください。

Scheduled Update ウィンドウでは、CSC SSM が Trend Micro ActiveUpdate サーバからコンポーネントのアップデートを受信する間隔を、1 日、1 時間、または 15 分から選択して指定できます。

SCS SSM コンソールの Manual Update ウィンドウでは、オンデマンドでコンポーネントを手動アップデートすることもできます。図 5-1（P.5-3）を参照。いずれのアップデートについても、詳細はオンラインヘルプを参照してください。

リソースのモニタリング

Monitoring ペインで Resource Graphs をクリックすると、モニタリング可能な 2 種類のリソースである、CPU 使用状況とメモリが表示されます。これらのリソースの使用状況が 100% に近いと表示された場合は、次のいずれかを推奨します。

- ASA-SSM-20 にアップグレードする（現在 ASA-SSM-10 を使用している場合）、または
- 他の ASA アプライアンスを購入する

CPU またはメモリの使用状況を表示するには、表示する情報の種類を選択してから **Show Graphs** をクリックします。次に例を示します。

図 7-6　メモリ モニタリング グラフ