Web（HTTP）トラフィックおよびファイル転送（FTP）トラフィックの設定

インストール後、デフォルトで、HTTP トラフィックおよび FTP トラフィックは、ウイルス、ワーム、およびトロイの木馬がないかどうかスキャンされます。スパイウェアなどのマルウェアやその他のグレーウェアを検出するには、コンフィギュレーションを変更する必要があります。この章では、これらのコンフィギュレーションのアップデートの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。

デフォルトの Web および FTP のスキャン設定

表 4-1 に、Web およびファイル転送のコンフィギュレーション設定、およびインストール後に動作するデフォルト値の要約を示します。

表 4-1　デフォルトの Web および FTP のスキャン設定

機能	デフォルト設定
ファイル ダウンロードの Web（HTTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
Web メール スキャン	デフォルトで、Yahoo™、AOL™、MSN™、および Google™ の Web メール サイトをスキャンするように設定されています
ファイル転送に対するファイル転送（FTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
Web からのダウンロードに対する Web（HTTP）圧縮ファイル処理、および FTP サーバからのファイル転送に対するファイル転送（FTP）圧縮ファイル処理	次の場合は圧縮ファイルのスキャンを省略するように設定されています • 圧縮解除されるファイル数が 200 よりも多い場合 • 圧縮解除されるファイル サイズが 30 MB を超える場合 • 圧縮レイヤ数が 3 を超える場合 • 圧縮解除 / 圧縮ファイルのサイズ比率が 100/1 を超える場合
Web （HTTP）およびファイル転送（FTP）の大容量ファイル処理（指定サイズより大きいファイルをスキャンしません - 指定サイズより大きいファイルの据え置きスキャンのイネーブル化）	50 MB より大きいファイルのスキャンを省略し、2 MB より大きいファイルの据え置きスキャンをイネーブルにするように設定されています
Web （HTTP）ダウンロード、およびマルウェアが検出されたファイルのファイル転送（FTP）アクション	マルウェアが検出されたダウンロードまたはファイル（あるいはその両方）を修復します 修復できない場合は、削除します
Web （HTTP）ダウンロード、およびスパイウェア / グレーウェアが検出されたファイルのファイル転送（FTP）アクション	ファイルは削除されます
Web （HTTP）ダウンロード、およびマルウェアが検出された場合のファイル転送（FTP）通知	InterScan for CSC SSM によってユーザが転送しようとしているファイルがスキャンされ、セキュリティ リスクが検出されたことを示すインライン通知がユーザのブラウザに掲載されます

これらのデフォルト設定では、Trend Micro InterScan for Cisco CSC SSM をインストールした後に Web および FTP のトラフィックに多少の保護が適用されます。これらの設定は変更できます。たとえば、マルウェアの検出に **All Scannable Files** ではなく、**Scan by specified file extensions...** オプションを使用できます。変更する前に、これらの選択の詳細についてオンライン ヘルプで慎重に検討してください。

インストール後にアップデートすることで、Web および FTP のトラフィックを最大限に保護する追加のコンフィギュレーション設定があります。これらの追加設定については、この章の残りのページで説明します。

URL ブロッキング、アンチフィッシング、および URL フィルタリング機能を使用できる Plus ライセンスを購入した場合は、これらの機能を設定する必要があります。デフォルトでは動作しません。

大容量ファイルのダウンロード

HTTP Scanning ウィンドウおよび FTP Scanning ウィンドウの Target タブを使用すると、スキャンする最大ダウンロードのサイズを定義することができます。たとえば、20 MB 未満のダウンロードはスキャンするが、20 MB より大きいダウンロードはスキャンしないように指定することができます。

さらに、次の指定ができます。

- これらのスキャンされない大容量のダウンロードの送信を、スキャンなしで許可するかどうかを指定します。スキャンなしの場合、セキュリティ リスクが発生する可能性があります。または、
- 指定した制限を越えるダウンロードを削除することを指定します

デフォルトでは、CSC SSM ソフトウェアは 50 MB 未満のファイルはスキャンし、50 MB 以上のファイルはスキャンせずに要求クライアントに送信するように指定されています。

据え置きスキャン

据え置きスキャン機能はデフォルトではイネーブルになっていません。この機能をイネーブルにした場合、ユーザはダウンロード全体をスキャンせずにデータのダウンロードを開始することができます。そのため、据え置きスキャンでは、ユーザは情報の本体すべてがスキャンされるのを長時間待つことなく、データの表示を開始することができます。

注意　据え置きスキャンがイネーブルの場合、情報のスキャンされない部分ではセキュリティ リスクが発生する可能性があります。

据え置きスキャンがイネーブルでない場合は、ユーザに示される前にダウンロードの内容全体がスキャンされる必要があります。しかし、クライアント ソフトウェアの中には、スキャンするファイル全体を構成するのに十分なネットワーク パケットの収集に要する時間が長いために、タイムアウトするものがあります。

次に要約を示します。

方式	利点	欠点
据え置きスキャンがイネーブルの場合	クライアントのタイムアウトを防ぎます	セキュリティ リスクが発生する可能性があります
据え置きスキャンがディセーブルの場合	より安全です。ユーザに提示される前にファイル全体がセキュリティ リスクがないかどうかスキャンされます	ダウンロードが完了する前にクライアントのタイムアウトが発生する可能性があります

HTTPS トラフィックのスキャン

CSC SSM ソフトウェアは、HTTPS プロトコル経由で移動するトラフィックについては、ウイルスおよびその他の脅威がないかどうか、スキャンを行うことはできません。

スパイウェア / グレーウェアの検出

グレーウェアは、正当か、好ましくないか、または悪意があるかが不明確なソフトウェアのカテゴリです。ウイルス、ワーム、トロイの木馬などの脅威とは異なり、グレーウェアは、データが感染したり、データの複製やデータの破壊を行ったりすることはありませんが、プライバシーが侵害される可能性があります。グレーウェアの例としては、スパイウェア、アドウェア、リモート アクセス ツールなどがあります。

スパイウェア / グレーウェア検出は、デフォルトではイネーブルになっていません。Web トラフィックおよびファイル転送トラフィックで、スパイウェアとスパイウェアの変形、およびその他のグレーウェアの検出を開始するには、次のウィンドウでこの機能を設定します。

- **Web (HTTP) > Scanning > HTTP Scanning/Target**
- **File Transfer (FTP) > Scanning > FTP Scanning/Target**

ASDM の **Configuration > Trend Micro Content Security > Web** で Configure Web Scanning リンクをクリックして、HTTP Scanning ウィンドウの Target タブに直接進むことができます。ASDM の **Configuration > Trend Micro Content Security > File Transfer** で Configure File Scanning リンクをクリックして、FTP Scanning ウィンドウの Target タブに直接進むことができます。

詳細については、P.3-4 の「SMTP および POP3 スパイウェア / グレーウェア検出のイネーブル化」を参照してください。上記のウィンドウについては、オンライン ヘルプも参照してください。

Web メールのスキャン

注意　Web メールだけをスキャンするように選択した場合、HTTP スキャンは **Web (HTTP) > Scanning > HTTP Scanning** ウィンドウの Webmail Scanning タブで指定したサイトに限定されます。その他の HTTP トラフィックはスキャンされません。

表 4-1 に示したように、Yahoo、AOL、MSN、および Google の Web メール スキャンはデフォルトですでに設定されています。サイトを追加するには、ASDM の **Configuration > Trend Micro Content Security > Web** で Configure Web Scanning リンクをクリックします。**HTTP Scanning** ウィンドウの Target タブが表示されます。**Webmail Scanning** タブをクリックします。

次の情報を使用して **Name** フィールドに Web メール サイトを入力します。

- 正確な Web サイト名
- URL キーワード
- 文字列

（注）　Web メールを介して管理されるメッセージの添付ファイルはスキャンされます。

スキャンする追加の Web メール サイトを設定する方法の詳細については、オンライン ヘルプを参照してください。設定されたサイトは、ごみ箱アイコンをクリックしてウィンドウの **Scan Webmail at following sites** セクションから削除しないかぎりスキャンされます。**Save** をクリックして設定をアップデートします。

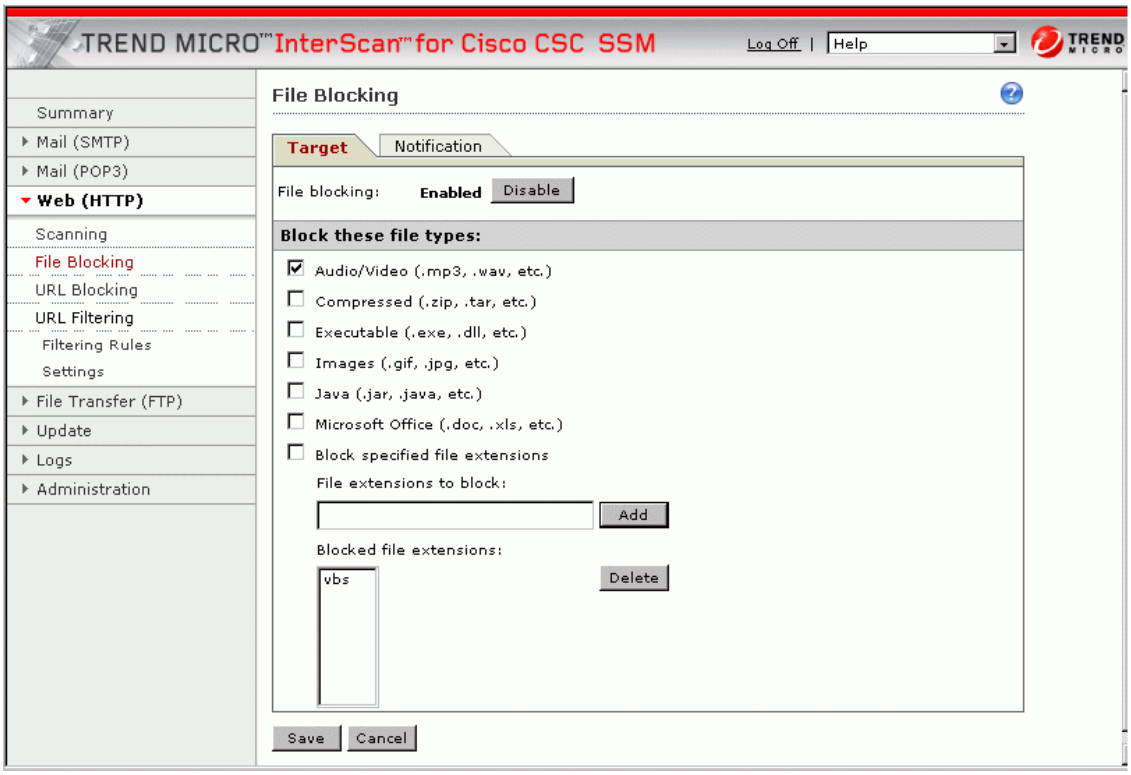
ファイル ブロッキング

この機能はデフォルトでイネーブルになっていますが、ブロックするファイルのタイプを指定するまで、いずれのファイルもブロックされません。ファイル ブロッキングは、勤務時間中のインターネットおよびその他のコンピューティング リソースの使用に関する組織のポリシーを適用するのに役立ちます。たとえば、従業員の生産性のためだけでなく、法律上の問題のために、会社で音楽のダウンロードを禁止しているとします。

HTTP プロトコルを介したダウンロードをブロックするには、ASDM の **Configuration > Trend Micro Content Security > Web** で Configure File Blocking リンクをクリックして、**File Blocking** ウィンドウを表示します。FTP プロトコルを介したダウンロードをブロックするには、ASDM の **Configuration > Trend Micro Content Security > File Transfer** で Configure File Blocking リンクをクリックします。**File Blocking** ウィンドウはどちらのプロトコルの場合も同じです。

File Blocking ウィンドウの **Target** タブで Audio/Video をオンにして音楽ファイルの転送をブロックします。図 4-1 を参照してください。

図 4-1　ファイル ブロッキングのイネーブル化



ファイル名拡張子によって追加のファイル タイプを指定できます。**Block specified file extensions** をオンにして、この機能をイネーブルにします。次に、**File extensions to block** フィールドにファイル タイプを追加し、**Add** をクリックします。例では、.vbs ファイルもブロックされます。

ファイル ブロッキングの詳細、およびブロッキングを停止するファイル拡張子の削除に関する情報については、オンライン ヘルプを参照してください。

File Blocking ウィンドウの **Notifications** タブをクリックすると、ファイル ブロッキング イベントがトリガーされた場合にユーザのブラウザ /FTP クライアントに表示されるデフォルトの通知が表示されます。デフォルトのメッセージを強調表示して上書きすることで、これらのメッセージのテキストをカスタマイズすることができます。管理者に対するオプションの通知を HTTP ファイル ブロッキングで使用できますが、デフォルトではオフになっています。**Send the following message...** チェックボックスをオンにして、通知をアクティブにします。

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。

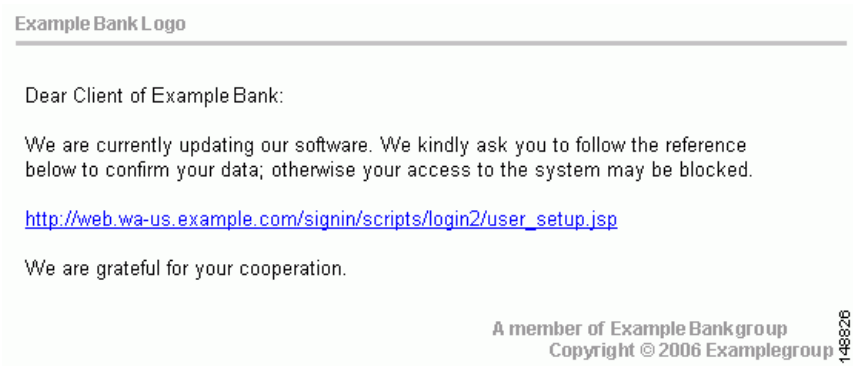
URL ブロッキング

（注）　この機能には Plus ライセンスが必要です。

URL ブロッキング機能では、社員が禁止されている Web サイトにアクセスするのを防ぐことができます。たとえば、組織のポリシーでデート サービスやオンライン ショッピング サービスの使用、および攻撃的なサイトの閲覧を禁止するために、一部のサイトをブロックすることを想定します。

また、フィッシングなどの詐欺行為を行うことが知られているサイトもブロックします。フィッシングは、犯罪者が使用する手法で、合法的な組織から来たように*見える*電子メール メッセージを送信して、銀行口座番号などの個人情報を提供するようにユーザを誘導します。図 4-2 に、フィッシングに使用される電子メール メッセージの一般的な例を示します。

図 4-2　フィッシングの例



デフォルトでは URL ブロッキングはイネーブルですが、ブロックする追加のサイトを指定するまで、TrendMicro PhishTrap パターン ファイルのサイトのみがブロックされます。

ローカル リストによるブロック

URL ブロッキングを設定するには、次の手順を実行します。

ステップ 1　ASDM の **Configuration > Trend Micro Content Security > Web** で **Configure URL Blocking** をクリックして、**URL Blocking** ウィンドウを表示します。

ステップ 2　**URL Blocking** ウィンドウの **Via Local List** タブで、**Match** フィールドにブロックする URL を入力します。次の項目で指定できます。

- 正確な Web サイト名
- URL キーワード
- 文字列

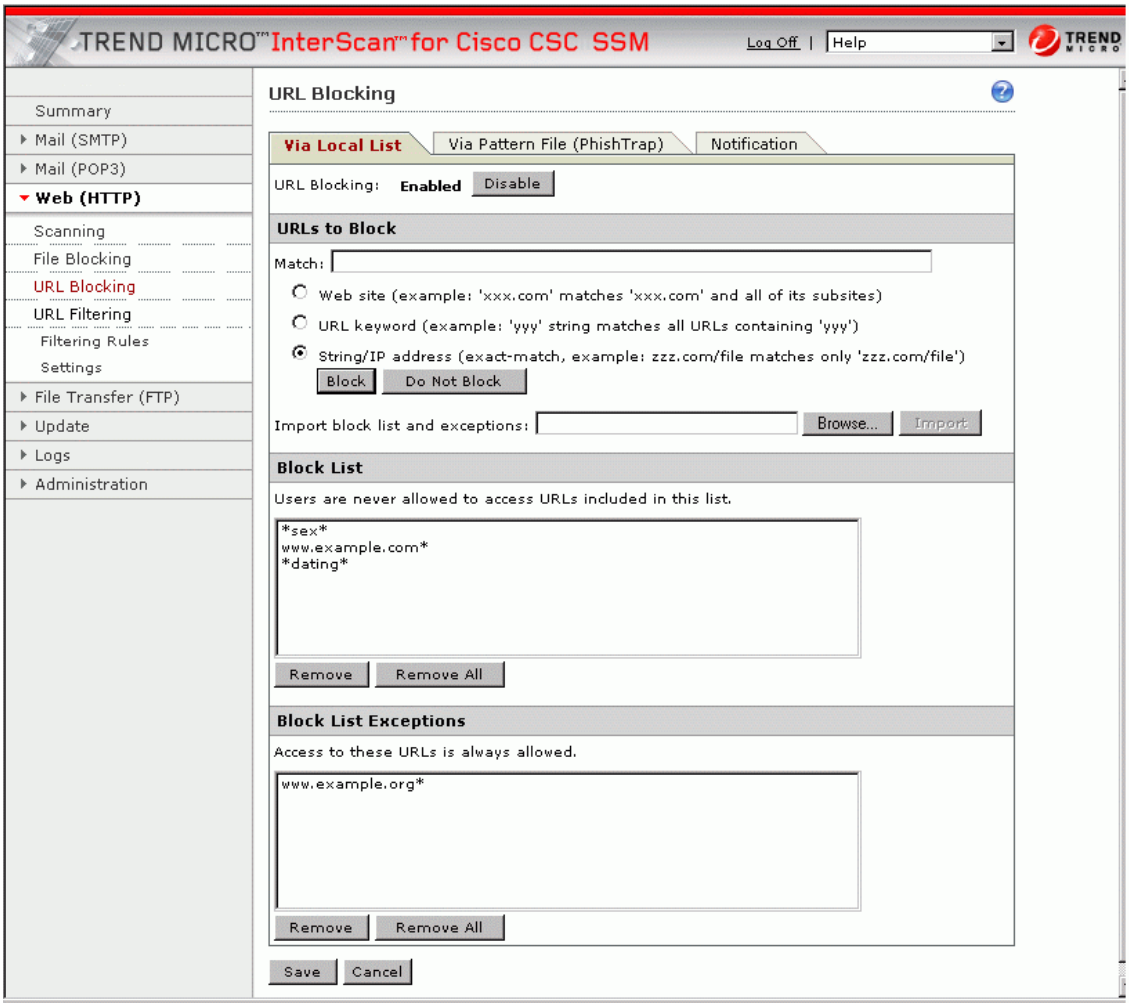
Match フィールドのエントリのフォーマッティングの詳細については、オンライン ヘルプを参照してください。

ステップ 3　エントリを 1 つ入力するたびに **Block** をクリックして、**Block List** に URL を移動します。エントリを例外に指定するには、**Do Not Block** をクリックしてエントリを **Block List Exceptions** に追加します。エントリは削除するまでブロック対象または例外のままです。

（注）　ブロックまたは例外のリストをインポートすることもできます。インポートするファイルは特定のフォーマットである必要があります。方法については、オンライン ヘルプを参照してください。

図 4-3 に、エントリがある **URL Blocking** ウィンドウ（**Via Local List** タブ）の例を示します。

図 4-3　URL ブロッキング ウィンドウ



パターン ファイル（PhishTrap）によるブロッキング

ASDM の **Configuration > Trend Micro Content Security > Web** で Configure URL Blocking リンクをクリックして、**URL Blocking** ウィンドウを表示します。次に、**Via Pattern File (PhishTrap)** タブをクリックします。

デフォルトでは、Trend Micro PhishTrap パターン ファイルは既知のフィッシング サイト、スパイウェア サイト、ウイルス加担サイト（既知の不正利用に関連付けられたサイト）、およびウイルス媒介サイト（悪意の目的のためのみに存在する Web サイト）を検出し、ブロックします。**Submit the Potential Phishing URL to TrendLabs** フィールドを使用して、PhishTrap パターン ファイルに追加する必要があると思われるサイトを送付してください。TrendLabs ではサイトを評価して、そのようなアクションが適切である場合はサイトを追加することがあります。

Notification タブをクリックして、ブロックされているサイトにアクセスしようとした場合にユーザのブラウザに表示される、デフォルトのメッセージのテキストを検討します。オンライン ヘルプに例が示されています。デフォルトのメッセージを強調表示して上書きすることで、テキストをカスタマイズします。

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。

URL フィルタリング

（注）　この機能には Plus ライセンスが必要です。

前述の **URL Blocking** ウィンドウで定義した URL は、常に許可されるか、常に禁止されるかのいずれかです。しかし、URL フィルタリング機能を使用すると、URL をカテゴリで設定し、特定の時間（休憩時間として定義）には許可し、勤務時間中には禁止するようにスケジュールすることができます。

次の 6 つの URL カテゴリがあります。

- Company-prohibited
- Not work related
- Research topics
- Business function
- Customer defined
- Others

デフォルトでは、会社で禁止したサイトは勤務時間と休憩時間の両方でブロックされます。

フィルタリング設定

URL フィルタリング機能を設定するには、次の手順を実行します。

ステップ 1　ASDM の **Configuration > Trend Micro Content Security > Web** で **Configure URL Filtering Settings** をクリックして、**URL Filtering Settings** ウィンドウを表示します。URL Categories タブで、表示されているサブカテゴリおよび各カテゴリに割り当てられたデフォルトの分類を検討して、割り当てが組織に適切かどうかを判断します。たとえば、「Illegal Drugs」は、「Company-prohibited」カテゴリのサブカテゴリです。投資情報サービス会社の場合は、このカテゴリを Company-prohibited に分類したままにすることができます。**Illegal Drugs** チェックボックスをクリックして、違法薬物に関連するサイトのフィルタリングをイネーブルにします。ただし、法執行機関の場合は、「Illegal Drugs」サブカテゴリを「Business function」カテゴリに再分類する必要がある可能性があります。再分類の詳細については、オンライン ヘルプを参照してください。

ステップ 2　サブカテゴリの分類を検討し、調整した後、サブカテゴリのチェックボックスをオンにして、フィルタリングを実行するすべてのサブカテゴリをイネーブルにします。

ステップ 3　イネーブルにしたサブカテゴリの中にフィルタリングを行わないサイトがある場合は、**URL Filtering Exceptions** タブをクリックします。フィルタリングから除外する URL を **Match** フィールドに入力します。次の項目で指定できます。

- 正確な Web サイト名
- URL キーワード
- 文字列

Match フィールドのエントリのフォーマッティングの詳細については、オンライン ヘルプを参照してください。

ステップ 4　エントリを 1 つ入力するたびに **Add** をクリックして、**Do Not Filter the Following Sites** リストに URL を移動します。エントリは削除するまで例外のままです。

（注）　例外のリストをインポートすることもできます。インポートするファイルは特定のフォーマットである必要があります。方法については、オンライン ヘルプを参照してください。

ステップ 5　**Schedule** タブをクリックして、勤務時間と見なす曜日および 1 日の時間を定義します。勤務時間として指定しなかった時間は、自動的に休憩時間として指定されます。

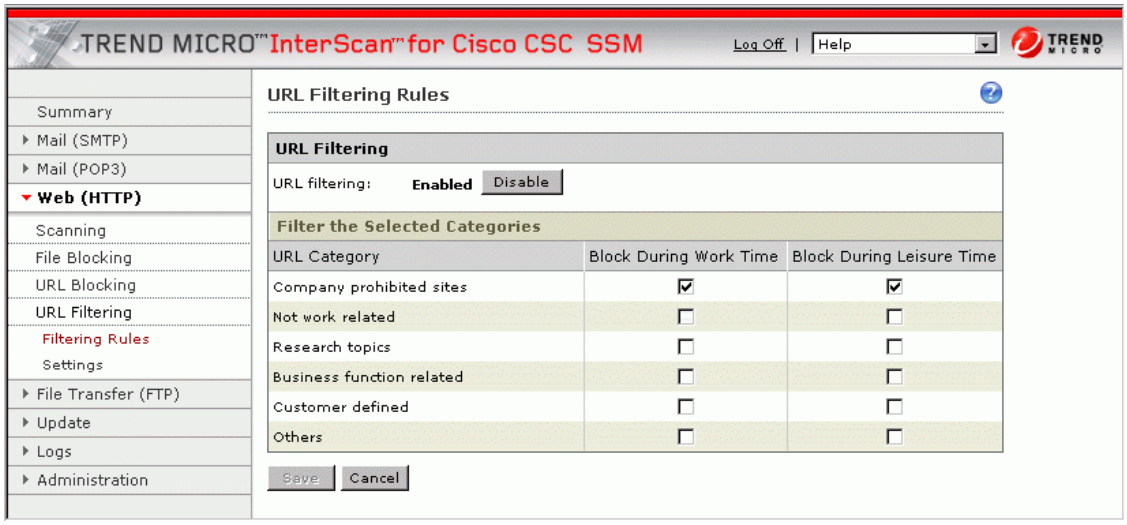
ステップ 6　**Save** をクリックして、URL フィルタリング設定をアップデートします。

Reclassify URL タブをクリックして、不確かな URL を評価するために TrendLabs に送付します。

フィルタリング規則

URL サブカテゴリを、組織に適切なカテゴリ、定義された例外（存在する場合）、および作成された勤務時間 / 休憩時間スケジュールに割り当てた後、カテゴリでフィルタリングを行うタイミングを決定するフィルタリング規則を割り当てます。ASDM の **Configuration > Trend Micro Content Security > Web** で Configure URL Filtering Rules リンクをクリックして、**URL Filtering Rules** ウィンドウを表示します。図 4-4 を参照してください。

図 4-4　URL Filtering Rules ウィンドウ



6 つの主要カテゴリについて、そのカテゴリの URL をブロックするかどうかをそれぞれ指定します。ブロックする場合は、勤務時間、休憩時間、またはその両方を指定します。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。