Cisco Start Router

設定マニュアル Cisco Cloud Web Security Cisco 841M J

2016 年 2 月 26 日
第 1.0 版

www.networld.co.jp

株式会社ネットワールド

Networld

改訂履歴

版番号	改訂日	改訂者	改訂内容
1.0	2016 年 2 月 26 日	ネットワールド	● 新規

免責事項

- 本書のご利用は、お客様ご自身の責任において行われるものとします。本書に記載する情報については、株式会社ネットワールド（以下 弊社）が慎重に作成および管理いたしますが、弊社がすべての情報の正確性および完全性を保証するものではございません。
- 弊社は、お客様が本書からご入手された情報により発生したあらゆる損害に関して、一切の責任を負いません。また、本書および本書にリンクが設定されている他の情報元から取得された各種情報のご利用によって生じたあらゆる損害に関しても、一切の責任を負いません。
- 弊社は、本書に記載する内容の全部または一部を、お客様への事前の告知なしに変更または廃止する場合がございます。なお、弊社が本書を更新することをお約束するものではございません。

表記規則

表記	表記の意味
「」（括弧記号）	キー、テキストボックス、ラジオボタンなどのオブジェクト
bold（ボールド文字）	入力または選択するシステム定義値
<italic>（イタリック文字）	入力または選択するユーザー定義値
□（囲み線）	入力または選択するオブジェクト
“”（二重引用符記号）	表示されるメッセージ
■（蛍光マーカー）	確認するメッセージ

表記の例）

(1)「Exec」ラジオボタンを選択します。

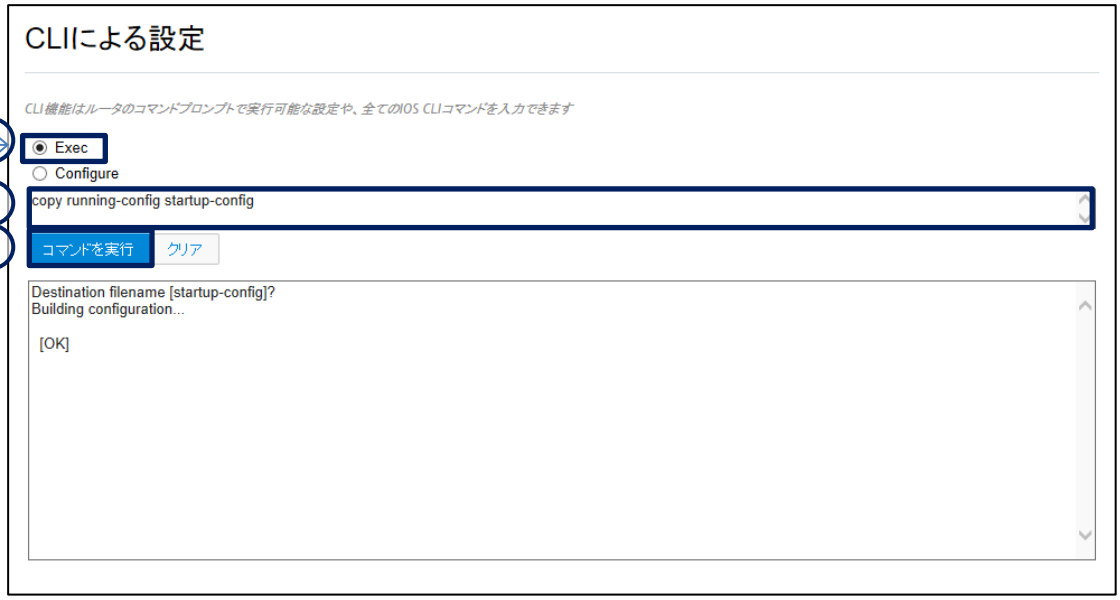
(2) テキストボックスに以下のコマンドを入力します。

Copy running-config *<file name>*

(3)「コマンドを実行」ボタンをクリックします。正常に実行されれば、画面に”[OK]”が表示されます。

```
Destination filename [startup-config]?
Building configuration…
```

[OK]



目次

1. はじめに

本書は、Cisco Configuration Professional Express（以下 CCP Express）のアドバンスドセットアップ、および ScanCenter を使用して、Cisco 841M J シリーズの Cisco Cloud Web Security（以下 CWS）の初期セットアップを実行する手順を説明した資料です。CWS はクラウド型の Web セキュリティソリューションで、Web フィルタリングやアンチマルウェアなどのインターネット脅威防御機能をサービスとしてクラウドで提供します。CWS はプライマリータワーおよびバックアップタワーと呼ばれる 2 つのプロキシサーバーから成り、99.999%の稼働率で SLA を実現します。CWS に接続した製品は、アウトバウンドの Web トラフィックを CWS にリダイレクトします。CWS にリダイレクトされるトラフィックには、中央管理された設定による一貫したセキュリティポリシーが適用され、シグニチャ、レピュテーション、コンテンツ分析、ヒューリスティック、サンドボックス、レトロスペクションなどで脅威から保護されます。これらのプロセスは、Web の使用状況と脅威情報として、CWS によって細部までレポートされます。CWS はクラウドサービスのため、既存のインフラを変更する必要がなく、さらに、メンテナンスや拡張に伴うコストも大幅に低減します。本書では、CWS に Web トラフィックをリダイレクトする CWS Connector として製品を設定し、ScanCenter で製品を制御します。ScanCenter は、アカウント、ライセンスキー、フィルター、およびレポートなどを中央管理する、CWS の管理ポータルです。CCP Express は、Web UI を備えた組み込みのデバイス管理ツールです。CCP Express のアドバンスドセットアップを使用すると、WAN、LAN、およびセキュリティなど、製品の詳細設定を簡単に実行できます。CWS の初期セットアップは、スーパーユーザーアカウントの権限で実行します。CWS の初期セットアップが完了すると、製品に接続されたネットワーク上のデバイスが、Cisco Systems（以下 Cisco）社の高度なグローバル脅威可視化ネットワークによって、継続的且つ安定的にインターネットの最新の脅威から保護されます。

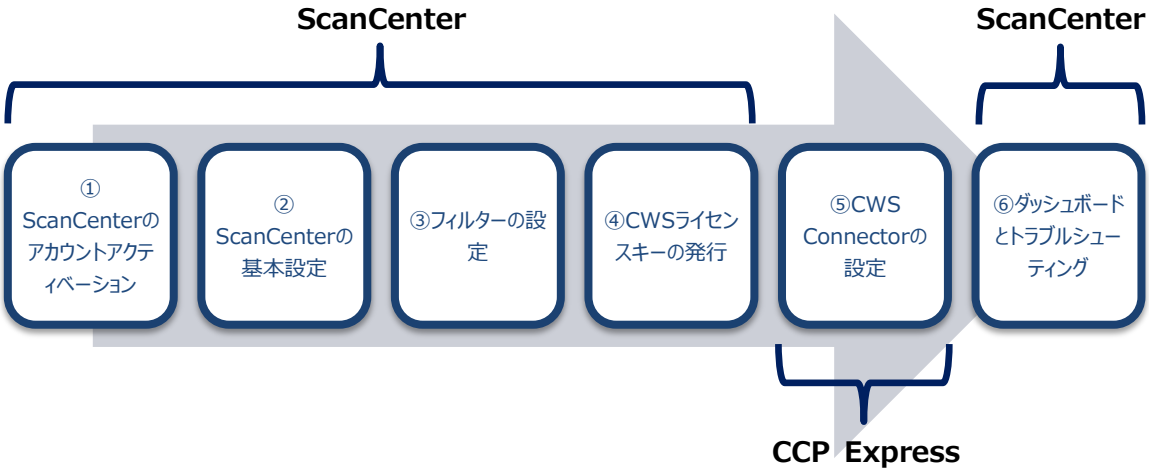


図 1 本書で実行する設定

1.1 対象製品

本書を使用して CWS の初期セットアップを実行できる製品は、以下のとおりです。

表 1 本書の対象製品（Cisco 841M J シリーズ）

C841M-4X-JSEC/K9	C841M-4X-JAIS/K9	C841M-8X-JAIS/K9
☐	☑	☑

表 2 本書の対象製品（CWS）

CWS-1Y-S1	CWS-3Y-S1	CWS-5Y-S1	CWS-AMP-1Y-S1	CWS-AMP-3Y-S1	CWS-AMP-5Y-S1
☑	☑	☑	☑	☑	☑

ASA/ASAv、WSA/WSAv、Cisco 841M J シリーズ以外の ISR G2、AnyConnect、スタンドアロン、およびモバイルブラウザーを使用した CWS の設定は、本書の対象外です。

1.2 CWS のライセンスと機能

Cisco 841M J シリーズで使用できる CWS の期間、規模、および機能は、ライセンスの種類によって決まります。Cisco 841M J シリーズがサポートする CWS ライセンスは、以下のとおりです。期間が 1 年間未満、規模が 25 ユーザー未満の場合でも、CWS-1Y-S1、または CWS-AMP-1Y-S1 を選択する必要があります。また、規模が 200 ユーザー以上の数量ベースの CWS ライセンス、および使用帯域幅ベースの CWS ライセンスは、Cisco 841M J シリーズではサポートされません。

表 3 CWS ライセンスの種類

型番	種類	期間	規模
CWS-1Y-S1	CWS Essentials	1 年間	25～199 ユーザー
CWS-3Y-S1	CWS Essentials	3 年間	25～199 ユーザー
CWS-5Y-S1	CWS Essentials	5 年間	25～199 ユーザー
CWS-AMP-1Y-S1	CWS Premium	1 年間	25～199 ユーザー
CWS-AMP-3Y-S1	CWS Premium	3 年間	25～199 ユーザー
CWS-AMP-5Y-S1	CWS Premium	5 年間	25～199 ユーザー

CWS ライセンスがサポートする CWS 機能は、以下のとおりです。Cisco Advanced Malware Protection（以下 Cisco AMP）と Cognitive Threat Analytics（以下 CTA）は CWS Premi

um ライセンスを使用した環境で自動的に有効化されます。ユーザーによるこれらの設定やチューニングは実行できません（アラート通知設定を除く）。また、ログ抽出 API を使用するための Advanced Threat Detection ライセンスは、Cisco 841M J シリーズではサポートされません。

表 4 CWS 機能の種類

機能	CWS ライセンス
Web フィルタリング	CWS Essentials
マルウェアスキャニング	CWS Essentials
アウトブレイクインテリジェンス	CWS Essentials
Web レピュテーション	CWS Essentials
アプリケーションの可視性と制御	CWS Essentials
動的コンテンツ分析	CWS Essentials
中央管理およびレポート	CWS Essentials
ラップトップでのローミングユーザー保護	CWS Essentials
Cisco AMP	CWS Premium
CTA	CWS Premium

CWS のセキュリティ機能を大別すると、Web セキュリティ、Web フィルタリング、Cisco AMP/CTA に分類できます。

1.2.1 Web セキュリティ

Web セキュリティはスパイウェアや Web ウィルスからネットワークを保護する機能です。既定で有効化され、追加の設定は必要ありません。既定では、受信したすべてのアドウェア、スパイウェア、望ましくない可能性があるアプリケーション、および Web レピュテーションスコアの低い Web サイトが CWS でブロックされます。ZIP ファイルなどのアーカイブに対しても Web セキュリティは適用されます。パスワードで保護されたアーカイブは検査できないため、これは望ましくない可能性があるアプリケーションに分類されます。何らかの理由で望ましくない可能性があるアプリケーションとして分類されたトラフィックを許可したい場合は、望ましくない可能性があるアプリケーションのホワイトリストを作成できます。ただし、望ましくない可能性があるアプリケーションが CWS に分類されるまで、そのホワイトリストは作成できません。また、ホワイトリストに追加できないアプリケーションもあります。Web レピュテーションスコアの低い Web サイトに対しても、ホワイトリストを作成できます。

表 5 CWS の Web セキュリティでブロックされるトラフィックとホワイトリストの関係

ブロックされるトラフィック	ホワイトリストへの追加
アドウェア	可
スパイウェア	可

望ましくない可能性があるアプリケーション（Cisco 社による分類）	可
ウィルス	不可
ワーム	不可
トロイの木馬	不可
バックドア	不可
キーロガー	不可
その他の悪質なコード	不可
既知のフィッシング事例	不可
グレーウェア（Web の閲覧操作を乗っ取る、スポンサーサイトにユーザーを誘導する、機密ではないブラウジング習慣をモニターする、迷惑なポップアップ広告を作成する等）	可
パスワードで保護されているアーカイブ	可
Web レピュテーションスコアの低い Web サイト	可（Web レピュテーション専用のホワイトリスト）

1.2.2 Web フィルタリング

Web フィルタリングはネットワークに出入りするコンテンツを制御する機能です。既定で有効化されますが、セキュリティやコンプライアンスの要件に合わせて追加の設定が必要です。既定では、すべてのコンテンツが CWS で許可されます。Web フィルタリングで制御できるコンテンツは、フィルタータイプまたはアプリケーション制御エンジンで分類されたものです。一部のフィルタータイプは、Outbound Content Control（以下 OCC）を有効にした場合のみ使用できます。OCC は、Cisco 社のカスタマーサポートに依頼することで有効化できます。アプリケーション制御エンジンには、Cisco 社によって制御用のプラットフォーム（Facebook 等）、アプリケーション（チャット等）、グループ（ゲーム等）、アクション（いいね等）が定期的に追加されます。何らかの理由で Web フィルタリングの適用を除外したい場合は、Web フィルタリングのホワイトリストを作成できます。

表 6 CWS の Web フィルタリングで使用できるフィルタータイプとアプリケーション制御エンジン

ブロックする条件	フィルタリングの種類	フィルタリングの方向	OCC
カテゴリー（HTTP）	フィルタータイプ	受信	不要
カテゴリー（HTTPS）	フィルタータイプ	受信	不要
ドメイン／URL	フィルタータイプ	受信	不要
コンテンツタイプ	フィルタータイプ	受信	不要
ファイルタイプ	フィルタータイプ	受信	不要
アプリケーション	フィルタータイプ	送受信	不要
例外	フィルタータイプ	送受信	不要
プロトコル	フィルタータイプ	送受信	不要

ユーザーエージェント	フィルタータイプ	送受信	不要
ファイル照合	フィルタータイプ	送信	必要
キーワード	フィルタータイプ	送信	必要
発信ファイルタイプ	フィルタータイプ	送信	必要
事前設定済み ID	フィルタータイプ	送信	必要
正規表現	フィルタータイプ	送信	必要
回避アプリケーション（アノニマイザーや暗号化トンネル等）	アプリケーション制御	送信	不要
コラボレーションアプリケーション（Cisco WebEx、インスタントメッセージ等）	アプリケーション制御	送信	不要
リソースを大量消費するアプリケーション（ストリーミングメディア等）	アプリケーション制御	送信	不要

1.2.3 Cisco AMP/CTA

Cisco AMP と CTA は先進的な脅威からネットワークの保護を強化する機能です。ただし、これらはセキュリティ侵害発生後のフェーズで動作する機能のため、トラフィックはブロックされません。Cisco AMPとCTA は CWS Premium ライセンスを使用した環境で自動的に有効化されます。ユーザーによるこれらの設定やチューニングは実行できません（アラート通知設定を除く）。Cisco AMP は、ファイルレピュテーションとファイルレトロスペクションを組み合わせて CWS を通過するファイルを検査し、不明ないしは良好なファイルにおいても、7 日後まで警告対象として管理します。7 日以内にファイルレピュテーションやファイルレトロスペクションが不良判定に変化した場合、ScanCenter でインシデントとして報告されます。CTA は、高度な統計モデルと機械学習を利用して CWS のログを解析します。マルウェア感染またはデータ侵害の兆候を識別した場合、ScanCenter でインシデントとして報告されます。

表 7 CWS の Cisco AMP と CTA で識別される主な脅威

識別される脅威	Cisco AMP / CTA
ダウンロード済みの悪意のあるファイル	Cisco AMP
ドメイン生成アルゴリズムによって生成されたドメインとの通信	CTA
悪意のあるコードを含む URL を通じたデータ転送	CTA
生成したドメインへの URL を通じたデータ転送	CTA
複数の拡張子を持つ悪意のある実行ファイルのダウンロード	CTA
疑わしい実行ファイルのダウンロード	CTA
userAgent、MIME タイプ、リファラーのない、疑わしい非ブラウザーHTTP トラフィック	CTA
Web プロキシ自動発見（WPAD）サービスの不正使用	CTA

異常な HTTP トラフィック	CTA
Raw サーバーIP アドレスへのシングルフローの異常な孤立シーケンス	CTA
ポリシー違反の可能性があるもの（Tor 匿名化アプリケーションに関連するトラフィック、Teamviewer アプリケーションに関連するトラフィック）	CTA
コンテキストの動作（HTTP ではない接続プロトコルによる異常なフロー、ホストとサーバー間の証明書の交換、ソフトウェア更新）	CTA
正当なサービスの異常なトラフィック（Pandora、CFEngine）	CTA

CWS の管理機能を大別すると、ダッシュボードとレポートに分類できます。

1.2.4 ダッシュボード

ダッシュボードは過去 24 時間の Web 使用状況の概要を表示する機能です。ScanCenter には、次の情報を表示するダッシュボードが実装されています。

- すべてのブロック件数
- Facebook の利用状況
- Web セキュリティ（マルウェア）によるブロック件数
- Web セキュリティ（スパイウェア）によるブロック件数
- Web フィルタリングによるブロック件数
- Cisco AMP によるブロック件数

1.2.5 レポート

レポートは条件や属性に基づく定義済み検索設定または保存済み検索設定を使用して、さまざまな角度から Web 使用状況の詳細を表示する機能です。ScanCenter のレポート機能を使用すると、次の情報を分析できます。

- アプリケーション
- 帯域幅
- ブロック件数
- 閲覧時間
- ブラウザー
- カテゴリー
- Facebook
- グループ
- ホスト
- 法的責任

- マルウェア
- セキュリティ
- ユーザー

1.3 CWS Connector のシステム要件

CWS Connector を使用できる Cisco IOS は、次のとおりです。

- Cisco IOS 15.2(1)T1～、推奨は 15.3(3)M3～

1.4 ScanCenter のシステム要件

ScanCenter を使用できる Web ブラウザーは、次のとおりです。ScanCenter では Web ブラウザーの「戻る」ボタンを使用せず、ScanCenter のフォームに設置された「Cancel」ボタンを使用してください。

- Microsoft Internet Explorer 11
- Google Chrome 47～
- Mozilla Firefox 40～

1.5 CCP Express のシステム要件

CCP Express を使用できる Cisco IOS および Web ブラウザーは、次のとおりです。なお、本書では CCP Express のセキュリティ機能（ゾーン、ポリシー、VPN などのセキュリティ設定）を使用するため、製品にバージョン 15.5(1)T 以上の Cisco IOS がインストールされている必要があります。

- Cisco IOS 15.2(4)M2～、または 15.3(1)T～、セキュリティ機能は 15.5(1)T～
- Microsoft Internet Explorer 10
- Google Chrome 17～
- Mozilla Firefox 10～

1.6 クイックリンク

Cisco 841M J シリーズの公式の情報は、以下の URL から入手できます。

- Cisco Start Router ホーム:
  http://www.cisco.com/web/JP/smb/c800m/index.html

- 製品カタログ:
  http://www.cisco.com/web/JP/product/catalog/pdf/1082_en_start_catalog.pdf

- データシート:
  http://www.cisco.com/web/JP/smb/c800m/docs/c800mj_data_sheet_c78-732678.pdf

- サポートコミュニティ:
  https://supportforums.cisco.com/ja/start

- よくある質問:
  http://www.cisco.com/web/JP/smb/c800m/c800m-faq.html

- サポート窓口:
  http://www.cisco.com/web/JP/smb/c800m/c800m-support.html

CWS の公式の情報は、以下の URL から入手できます。

- CWS ホーム:
  http://www.cisco.com/web/JP/product/hs/security/cloud_web/index.html

- 製品概要:
  http://www.cisco.com/web/JP/product/hs/security/cloud_web/ov_list.html

- ソリューション概要:
  http://www.cisco.com/web/JP/product/hs/security/cloud_web/sov_list.html

- データシート:
  http://www.cisco.com/web/JP/product/hs/security/cloud_web/ds_list.html

- よくある質問:

https://supportforums.cisco.com/document/12110031/cisco-cloud-web-security-cws-isr-g2-faq

2. システム構成

CWS の初期セットアップの手順は、以下の構成で説明します。

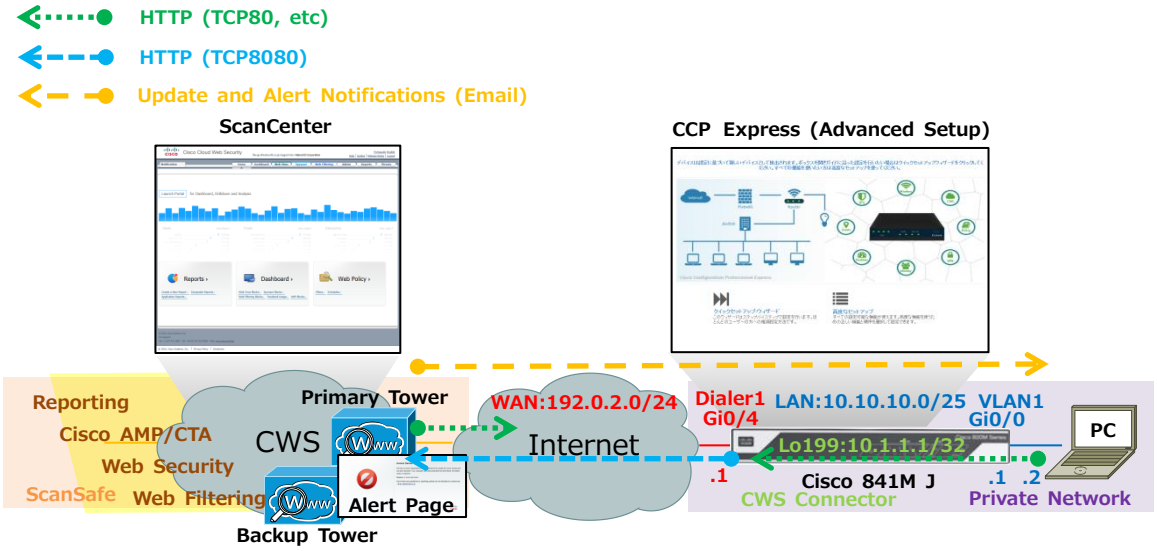


図 2 CWS の初期セットアップで構成するシステム

製品は、CWS Connector（プロキシクライアント）として、プライベートネットワークのホストから送信される Web トラフィックを CWS のプライマリータワー（プロキシサーバー）にリダイレクトします。このとき、宛先ポート番号は CWS Connector によって TCP8080 番に変換されます。プライマリータワーでは、Web フィルタリング、Web セキュリティ、および Cisco AMP/CTA などの ScanSafe サービスによって、トラフィックが検査されます。トラフィックが安全な場合は、プライマリータワーによって元の宛先ポート番号で目的の宛先にトラフィックが転送されます。トラフィックが安全でない場合は、プライマリータワーによってトラフィックは破棄され、ホストに警告を表示します。プライマリータワーが停止した場合、フェイルオーバーによってバックアップタワーがプライマリータワーの役割を担い、CWS Connector はこれを検知してトラフィックのリダイレクト先を変更します。プライベートネットワークのスーパーユーザーは、ScanCenter を使用して Web フィルタリング、Web セキュリティ、Cisco AMP/CTA、レポート、アップデート通知、およびアラート通知を構成します。なお、本書では、製品はクイックセットアップウィザードを使用したインターフェースや VLAN などの LAN 側の基本設定、PPPoE、デフォルトルート、NAT などの WAN 側の基本設定、およびインターネット接続用の標準的なファイアウォール設定が完了しているものとします。クイックセットアップウィザードを使用した製品の初期セットアップについては、クイックスタートガイドをご参照ください。

- Cisco Start Router 設定マニュアル クイックスタートガイド Cisco 841M J:
  http://www.networld.co.jp/download_file/4574/7266/

2.1 本書に含まない機能

CWS には多くの高度な機能が実装されていますが、そのすべてを説明すると本書の目的を逸脱するため、以下の機能に関する設定方法の説明は割愛します。

- ASA/ASAv、WSA/WSAv、Cisco 841M Jシリーズ以外のISR G2、AnyConnect、スタンドアロン、およびモバイルブラウザーを使用した CWS
- 望ましくない可能性があるアプリケーションおよび Web レピュテーションスコアの低い Web サイトに対する Web セキュリティをバイパスするホワイトリスト
- Web フィルタリングのクォータ
- Webフィルタリングの拡張機能（SearchAhead、安全検索、ローカライゼーション、個別のHTTPS 制御、利用許可ポリシーの表示、未分類 Web サイトの動的分類、コンテンツ範囲ヘッダーの有効化、サンドボックス）
- 特定の Web サイトに対する Web フィルタリングをバイパスするホワイトリスト
- フィルターのバックアップおよびリストア
- CWS Connector のパブリック IP アドレスの識別
- スーパーユーザーアカウント以外の管理アカウントの作成と権限の委任
- ユーザーやグループ毎のトラフィックの識別または認証
- スタンドアロン用の PAC 設定ファイルと AnyConnect 用の Web セキュリティ設定ファイルの管理
- カスタム HTTP ヘッダーの追加
- HTTPS Inspection
- ScanCenterのアクセスとアクティビティ、ログ抽出APIの実行、およびレポートの管理と実行の監査
- OCC
- Portal 1.0 を使用した詳細なフィルターおよびレポート
- Portal 2.0 を使用した詳細なフィルターおよびレポート
- CWS をバイパスするホワイトリスト

2.2 使用した機材

本書で使用した機材は、以下のとおりです。

表 8 本書で使用した機材

機材	製品型番または名称	備考
Cisco 841M J シリーズ	C841M-4X-JAIS/K9 15.5(3)M	
デバイス管理ツール	CCP Express 3.1.2	
PC	Windows 7 x64 Professional	

	SP1	
Web ブラウザー	Internet Explorer x64 11.0.9600.18163	
CWS	CWS-AMP-1Y-S1	評価版
CWS 管理ポータル	ScanCenter February 19, 2016	
CTA	CTA 1.0.612	

3. CWS の設定手順

CWS の初期セットアップを実行します。CWS の初期セットアップでは、Portal 1.0 の基本設定、Portal 2.0 の基本設定、基本的なフィルターの設定、および CWS ライセンスキーの発行を実行します。

3.1 ScanCenter のスーパーユーザーアカウントのアクティベーション

CWS のサブスクリプションを初めて発注した場合、Cisco 社によるサービスのプロビジョニングが完了すると、注文時に Cisco 社に提供した優先連絡先電子メールアドレス宛に ScanSafe サービスから以下の情報が送信されます。アカウントアクティベーションは、電子メールに記載の URL を使用して ScanCenter のスーパーユーザーアカウントのパスワードを設定することで完了します。なお、電子メールを受信した時間から 24 時間以内に、アカウントアクティベーションを完了させる必要があります。

- プライマリータワーの FQDN
- バックアップタワーの FQDN
- ScanCenter のスーパーユーザーアカウントの名前（注文時の優先連絡先電子メールアドレス）
- ScanCenter のスーパーユーザーアカウントのポータル ID
- ScanCenter のスーパーユーザーアカウントのアクティベーション用 URL

ScanCenter のスーパーユーザーアカウントに既定で付与されるアクセス権限は、次のとおりです。

表 9 ScanCenter の既定のスーパーユーザーアカウントのアクセス権限

領域	権限	備考
ユーザーメッセージ	Read / Write	
電子メールアラート	Read / Write	
検索／時系列分析	Read / Write	
詳細検索	Read / Write	
フィルターセット	Read / Write	
検索結果の保存／保存した検索結果の削除	Read / Write	
複合レポートの管理	Read / Write	
複合レポートの作成／編集	Read / Write	
スケジュール設定されたレポートの管理	Read / Write	
スケジュール設定されたレポートの作成／編集	Read / Write	
電子メール受信者の管理	Read / Write	
許可トラフィックレポート	Read	
スパイウェア	Read / Write	

Web フィルタリング	Read / Write
アカウントの詳細情報	Read / Write
パスワードの変更	Read / Write
IP アドレスのスキャン	Read / Write
管理ユーザー	Read / Write
ダイナミック DNS	Read / Write
認証	Read / Write
クライアントレス認証	Read / Write
ユーザー／グループ管理	Read / Write
監査の設定	Read / Write
アクティビティ／アクセス監査	Read
ディクショナリー／ファイル情報データベース	Read / Write
ユーザーリストのインポート	Read / Write
HTTPS トラフィック検査	Read / Write
ホストされているコンフィギュレーションファイル	Read / Write

(1) ScanCenter のスーパーユーザーアカウントのパスワード設定画面に移動します。「Administrator Portal Login」リンクラベルをクリックします。

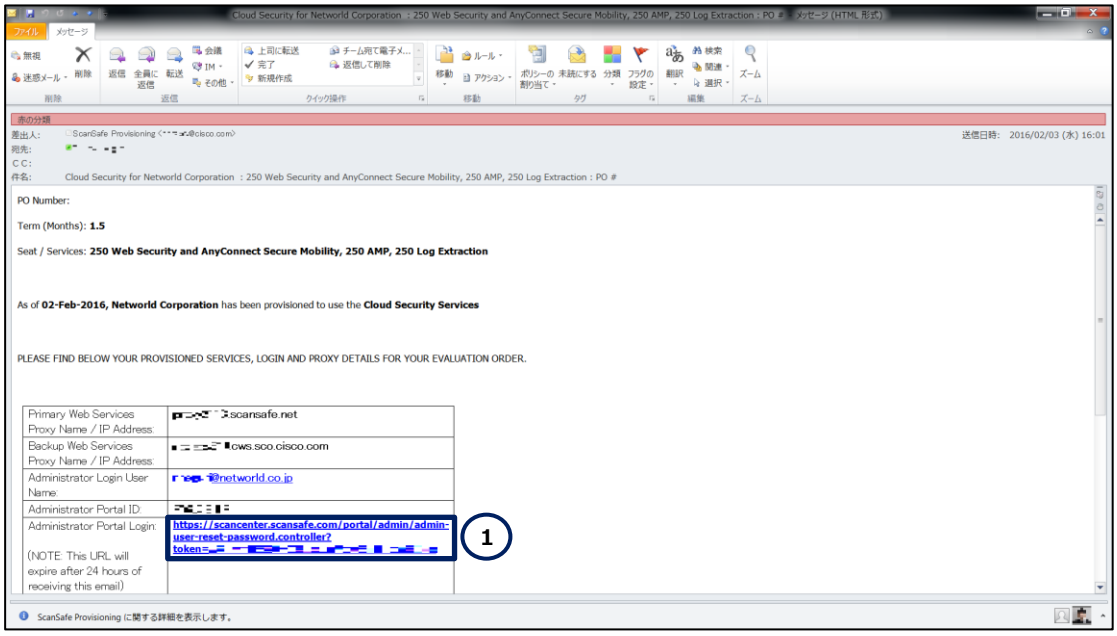


図 3 ScanCenter のスーパーユーザーアカウントの情報

(2) ScanCenter のスーパーユーザーアカウントのパスワードを設定します。「Password:」テキストボックスにパスワードを入力します。「Confirm Password:」テキストボックスに直前で入力したパスワー

ドと同じ値を入力します。「Save」ボタンをクリックします。スーパーユーザーアカウントがロックアウトされることはありませんが、ScanCenter へのログインに複数回失敗するとパスワードがリセットされ、仮のパスワードが優先連絡先電子メールアドレス宛に送信されます。なお、ScanCenter のスーパーユーザーアカウントのパスワードには、以下の要件が設定されています。要件が満たされると、各要件の右側に表示される「X」アイコンが「✓」アイコンに変わります。

- 8 文字以上
- 1 つ以上の英小文字
- 1 つ以上の英大文字
- 1 つ以上の数字
- 1 つ以上の次の特殊文字 @#$%^&+=_!:?
- 90 日間の有効期限
- 直近の 5 つのパスワードと異なる文字列

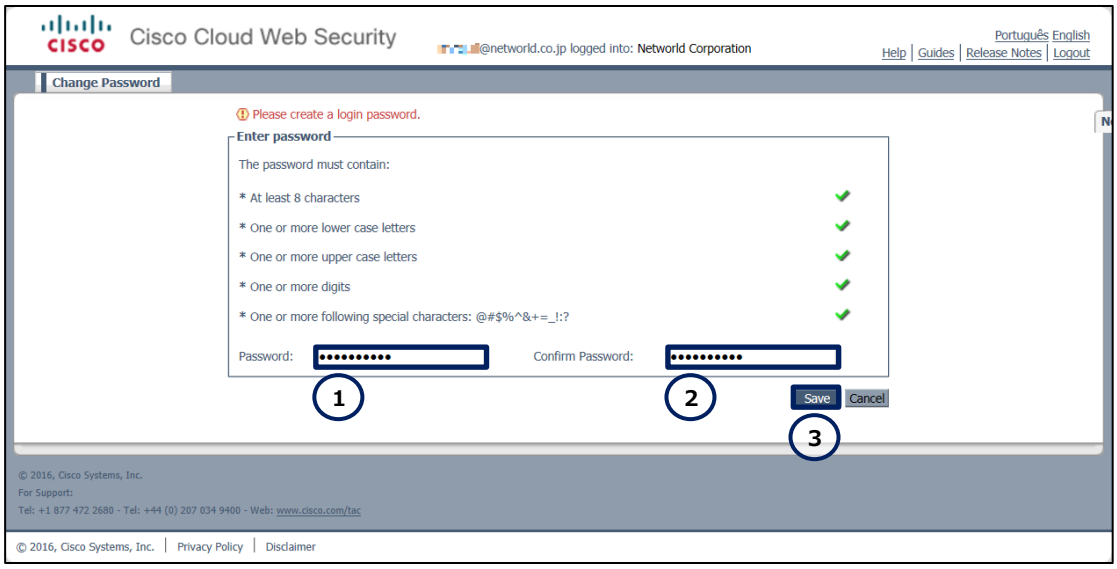


図 4 ScanCenter のスーパーユーザーアカウントのパスワードの設定

(3) ScanCenter のスーパーユーザーアカウントのアクティベーションが完了すると、ScanCenter に自動的に接続されます。なお、Web ブラウザーから直接、ScanCenter にログインするには、以下の URL を使用します。

- https://scancenter.scansafe.com/portal/admin/login.jsp

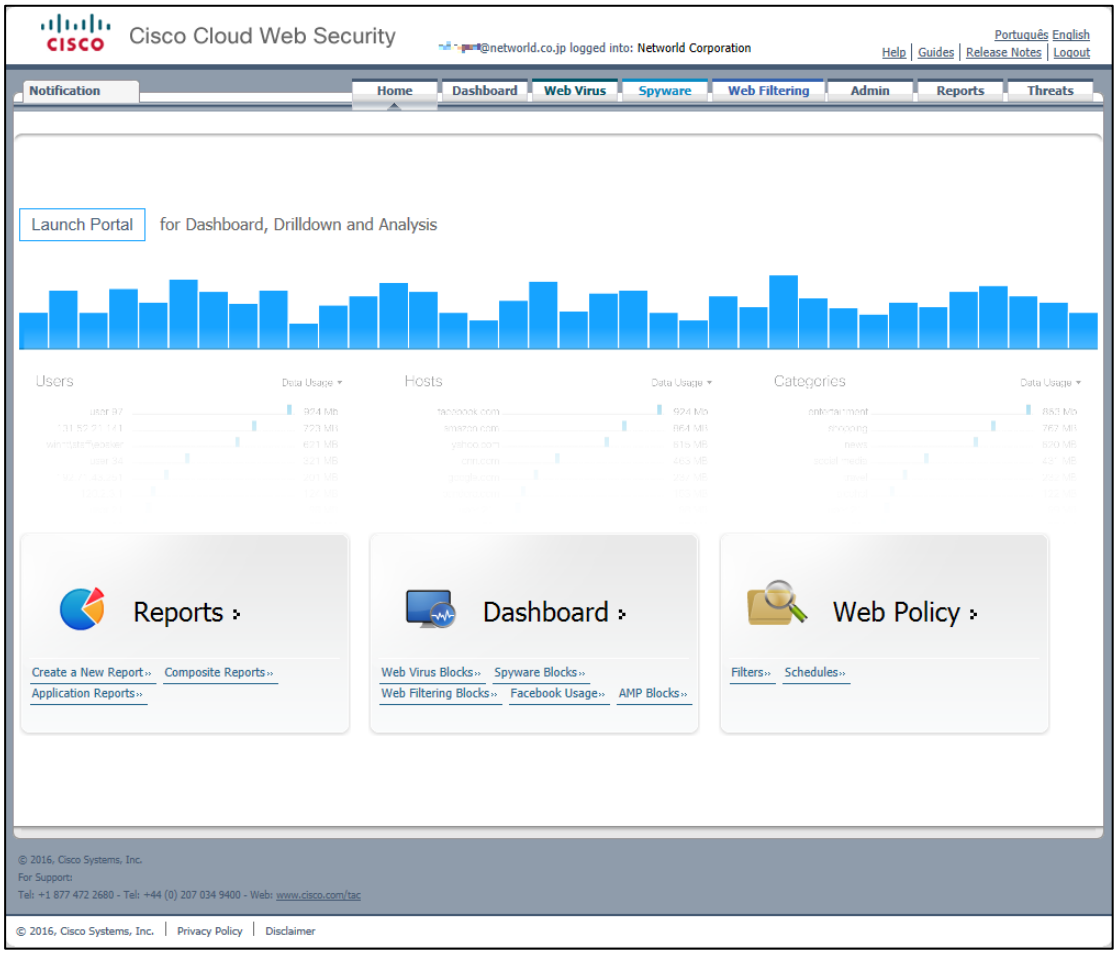


図 5 ScanCenter のホーム

図 6 ScanCenter のユーザー認証

3.2 ScanCenter の基本設定

ScanCenter の表示言語、スーパーユーザーアカウント、アップデート通知、アラート通知、および Portal 2.0 の設定を実行します。現在のバージョンの ScanCenter には、初期バージョンの Portal 1.0 と、Portal 2.0 が混在しています。本書では、Portal 2.0 と明記しない限り、各機能の基盤は Portal 1.0 を指しているものとします。

3.2.1 表示言語の設定

ScanCenter で使用する言語を設定します。

(1) ScanCenter の表示言語を設定します。「English」リンクラベルまたは「Portugues」リンクラベルをクリックします。ScanCenter が現在サポートしている言語は、英語とポルトガル語の 2 種類です。

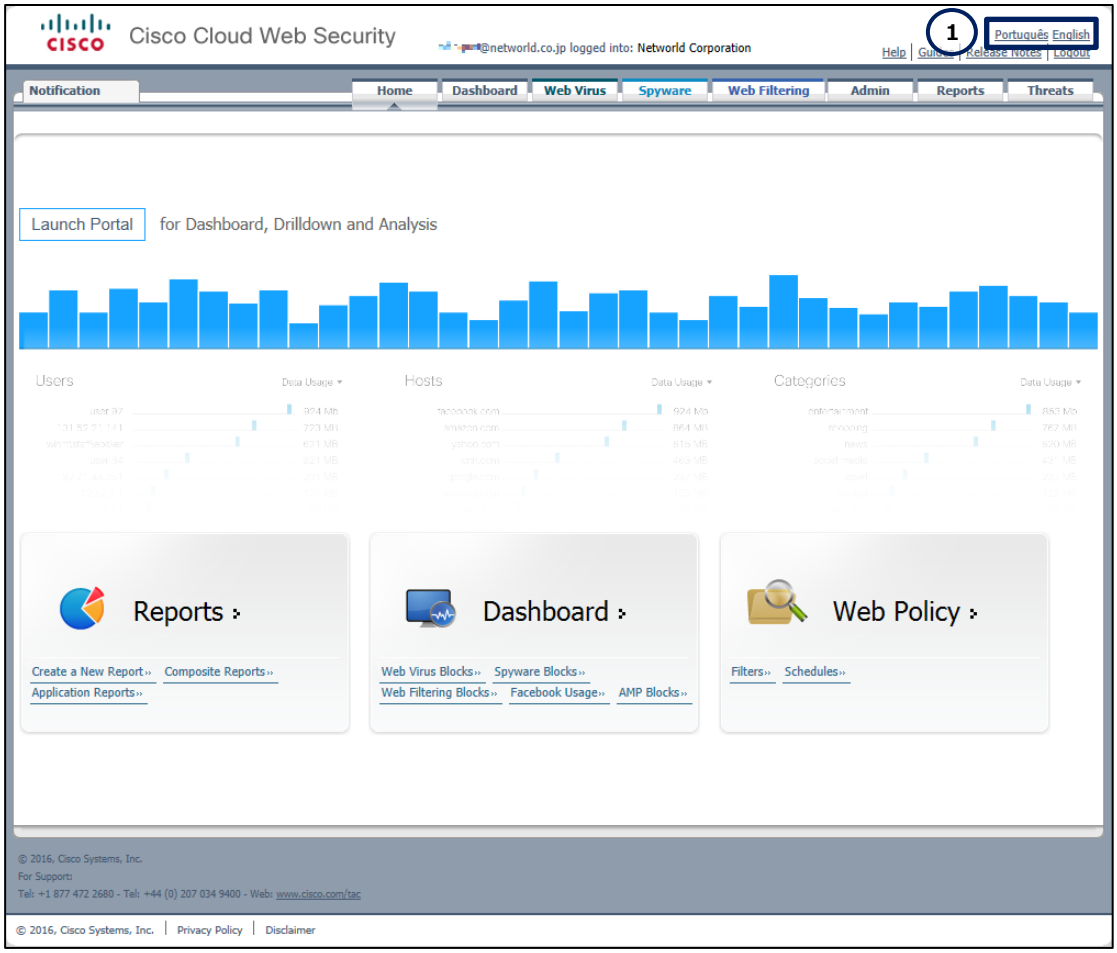


図 7 ScanCenter の表示言語の設定

3.2.2 スーパーユーザーアカウントの設定

ScanCenter のスーパーユーザーアカウントを設定します。ScanCenter では、初回のアクティベーションプロセスで使用したアカウントがスーパーユーザーアカウントとして有効化され、ScanCenter の完全なアクセス権限を付与されます。

(1) ScanCenter のスーパーユーザーアカウントの設定画面に移動します。「Admin」タブをクリックします。「Your Account」ドロップダウンリストから「Account Details」リストをクリックします。

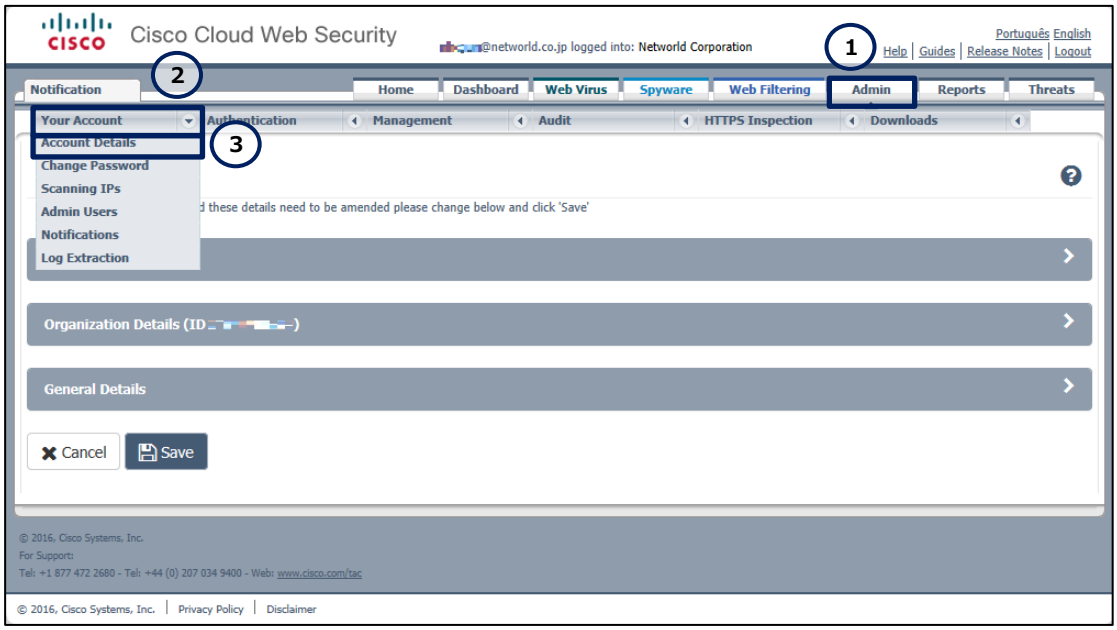


図 8 ScanCenter のスーパーユーザーアカウントの設定

(1) ScanCenter のスーパーユーザーアカウントの個人情報の詳細を登録します。「*」ラベルが記載された設定は、必須の設定です。なお、既定で CWS のサブスクリプションを発注したときに使用した個人情報が登録されています。

① 「Personal Details」プルダウンをクリックします。
② 「Title」ドロップダウンリストからアカウント使用者の敬称を選択します。
③ 「First Name」テキストボックスにアカウント使用者の名を入力します。
④ 「Last Name」テキストボックスにアカウント使用者の姓を入力します。
⑤ 「Mobile Phone」テキストボックスにアカウント使用者の携帯電話番号を入力します。
⑥ 「Save」ボタンをクリックします。

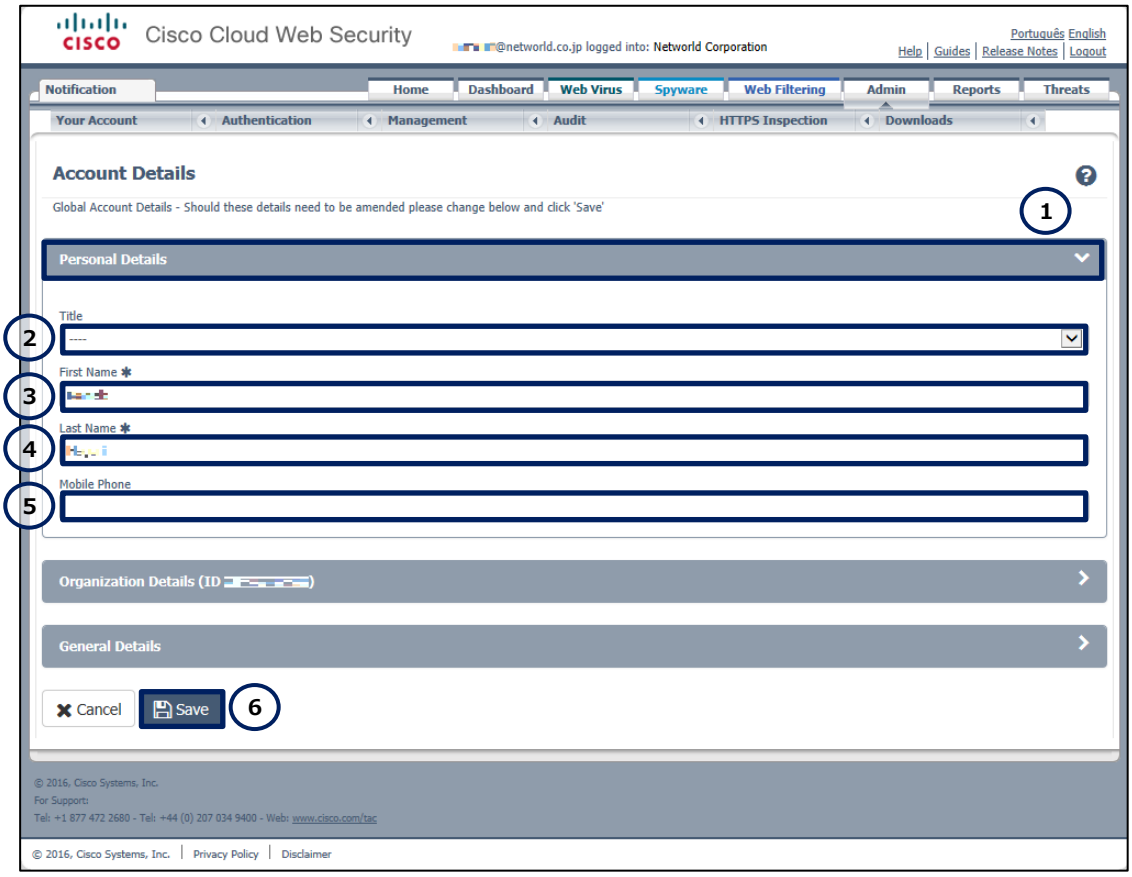


図 9 ScanCenter のスーパーユーザーアカウントの個人情報の設定

(2) ScanCenter のスーパーユーザーアカウントの会社情報の詳細を登録します。「*」ラベルが記載された設定は、必須の設定です。なお、既定で CWS のサブスクリプションを発注したときに使用した会社情報が登録されています。

① 「Organization Details」プルダウンをクリックします。
② 「Job Title」テキストボックスにアカウント使用者の役職名を入力します。
③ 「Organization Name」テキストボックスに会社名を入力します。この設定は変更できません。
④ 「Telephone」テキストボックスに会社の電話番号を入力します。
⑤ 「Fax」テキストボックスに会社の FAX 番号を入力します。
⑥ 「City」テキストボックスに会社の市区町村を入力します。
⑦ 「Address 1」テキストボックスに会社の住所を入力します。
⑧ 「Address 2」テキストボックスに会社の住所の補足（番地等）を入力します。
⑨ 「Address 3」テキストボックスに会社の住所の補足（ビル名等）を入力します。
⑩ 「Website」テキストボックスに会社のホームページの URL を入力します。
⑪ 「Save」ボタンをクリックします。

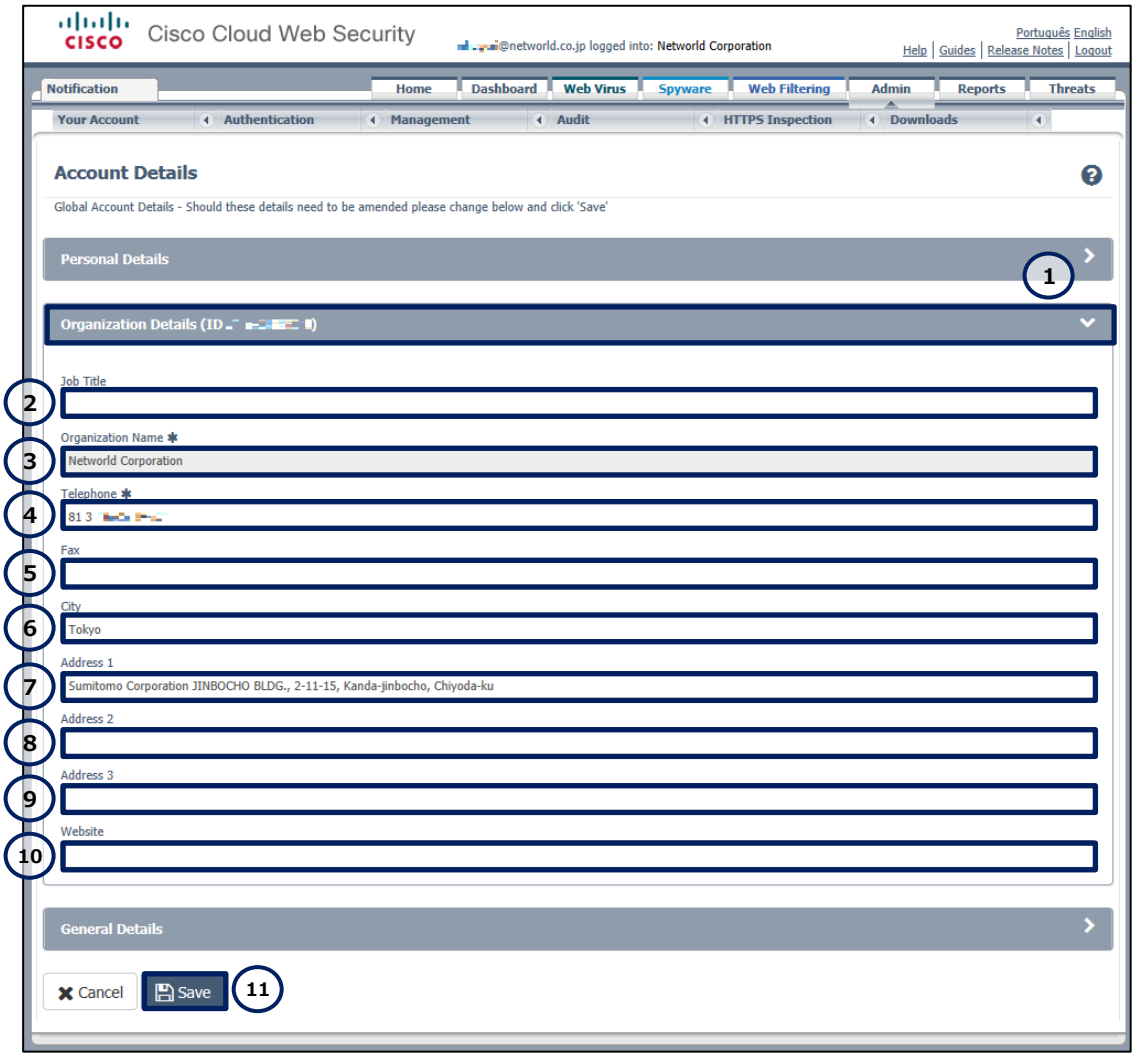


図 10 ScanCenter のスーパーユーザーアカウントの会社情報の設定

(3) ScanCenter のスーパーユーザーアカウントの一般情報の詳細を登録します。「*」ラベルが記載された設定は、必須の設定です。なお、既定で CWS のサブスクリプションを発注したときに使用した一般情報が登録されています。

① 「General Details」プルダウンをクリックします。
② 「Country」ドロップダウンリストから **Japan** を選択します。
③ 「Time Zone」ドロップダウンリストから **timezones.GMT+9:00** を選択します。
④ 「ZIP/Post Code」テキストボックスに会社の郵便番号を入力します。
⑤ 「Expiry Date」テキストボックスに CWS サブスクリプションの有効期限を入力します。この設定は変更できません。
⑥ 「Seats」テキストボックスに CWS サブスクリプションの有効ユーザー数を入力します。この設定は変更できません。
⑦ 「Save」ボタンをクリックします。

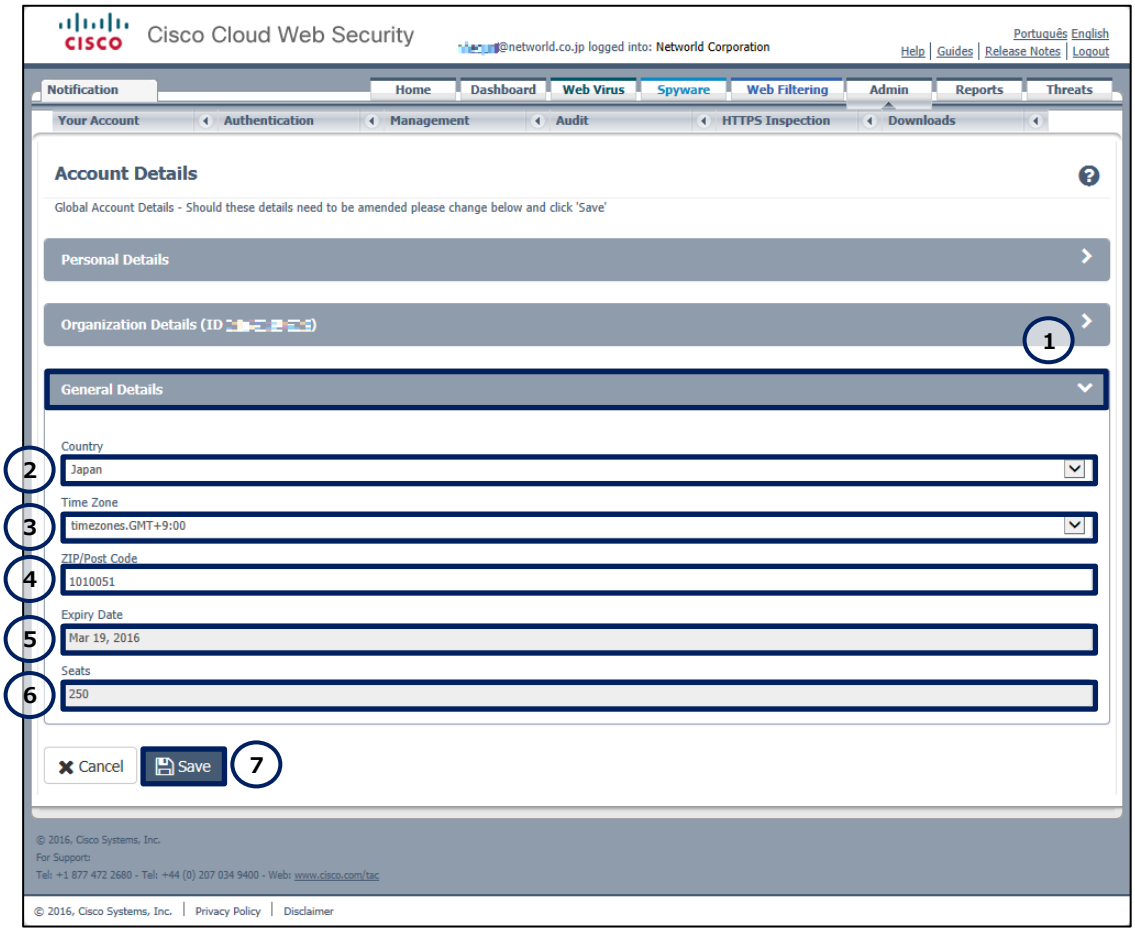


図 11 ScanCenter のスーパーユーザーアカウントの一般情報の設定

3.2.3 アップデート通知の設定

サービスのメンテナンスや停止、プロダクトの新機能追加や機能変更の情報は、ScanCenter で確認できます。これらの情報を電子メールで受信したい場合は、通知する情報毎に送信先の電子メールアドレスを設定します。ここで設定する電子メールアドレスは、本アップデート通知の目的のみで ScanSafe サービスに使用されます。

(1) ScanCenter のアップデート通知の設定画面に移動します。「Admin」タブをクリックします。「Your Account」ドロップダウンリストから「Notifications」リストをクリックします。

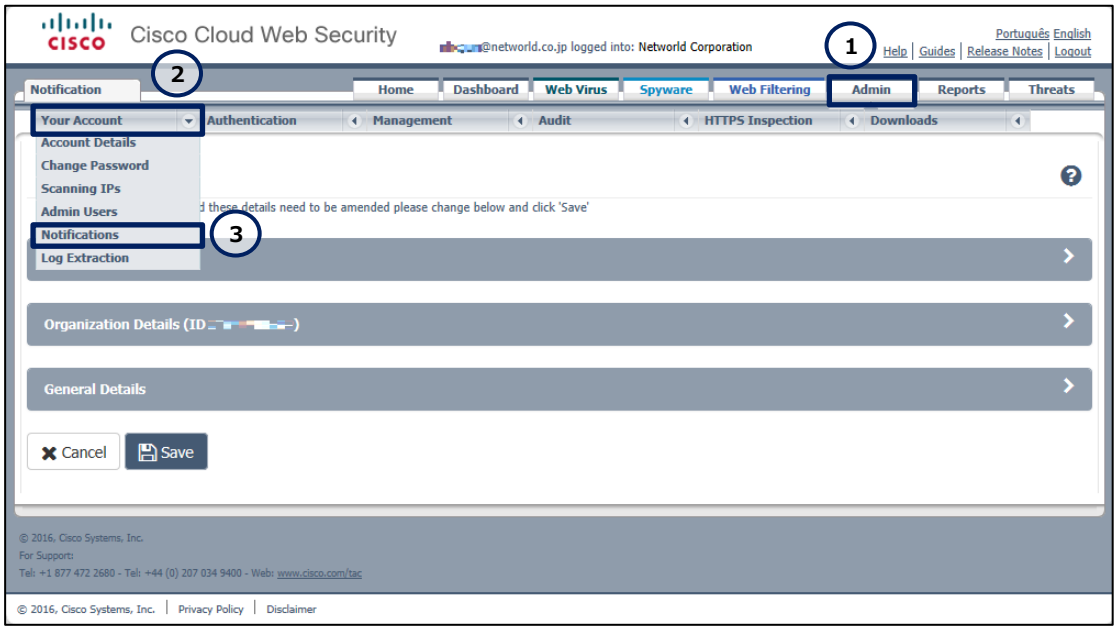


図 12 ScanCenter のアップデート通知の設定

(2) 通知を受け取るアップデートの種類と、アップデート通知先の電子メールアドレスを設定します。アップデート通知先の電子メールアドレスを複数登録する場合は、③と④、または⑥と⑦を電子メールアドレスの数だけ繰り返します。

① 「Manage Service Update Settings」プルダウンをクリックします。
② サービスに関する情報を受け取る場合は、「Send Service Update Emails」チェックボックスにチェックを入れます。
③ サービスに関する情報を受け取る場合は、「Send Service Update Emails」テキストボックスにアップデート通知先の電子メールアドレスを入力します。
④ 「Add Recipient」ボタンをクリックします。
⑤ プロダクトに関する情報を受け取る場合は、「Send Product and Feature Update Emails」チェックボックスにチェックを入れます。
⑥ プロダクトに関する情報を受け取る場合は、「Send Product and Feature Update Emails」テキストボックスにアップデート通知先の電子メールアドレスを入力します。
⑦ 「Add Recipient」ボタンをクリックします。
⑧ 「Apply」ボタンをクリックします。

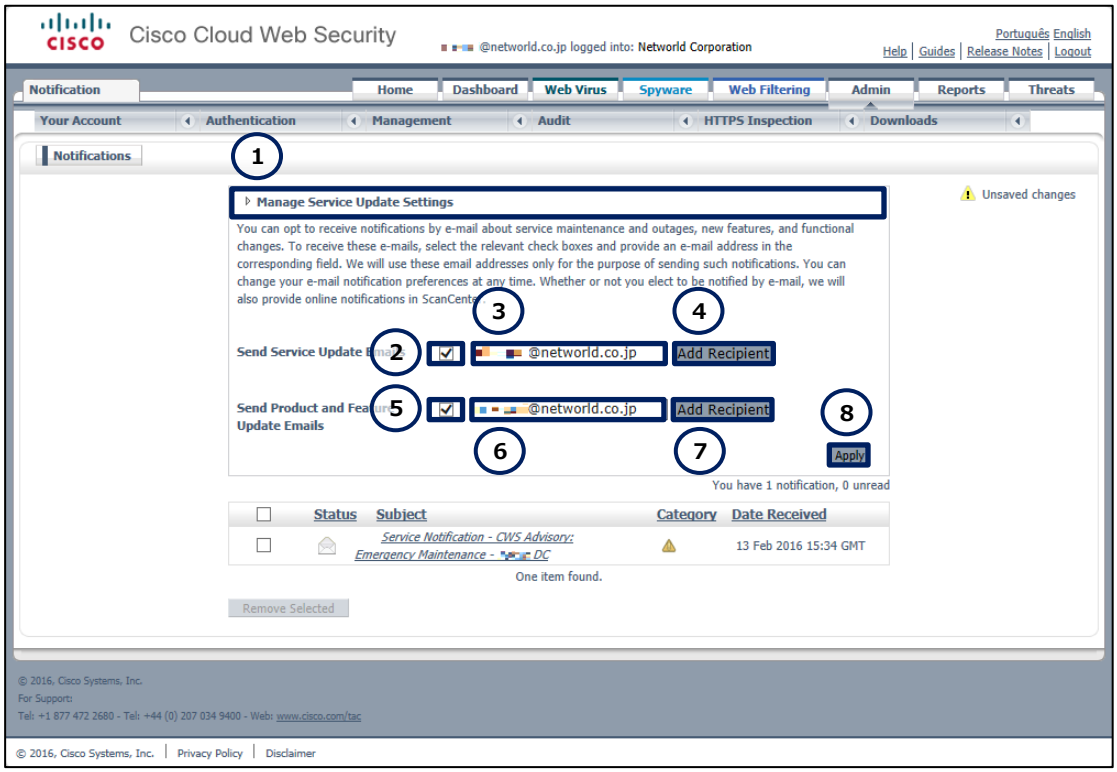


図 13 ScanCenter のアップデート通知の設定（詳細）

3.2.4 アラート通知の設定

ScanCenter のログインに失敗した場合に、特定の宛先に電子メールでアラート通知を送信できます。この情報を電子メールで受信したい場合は、通知する宛先の電子メールアドレスを設定します。また、ここでは、ScanCenter へのログインに複数回失敗してロックされたアカウントがロックの解除を依頼する宛先の電子メールアドレスも併せて設定します。

(1) ScanCenter のアラート通知の設定画面に移動します。「Admin」タブをクリックします。「Audit」ドロップダウンリストから「Access Settings」リストをクリックします。

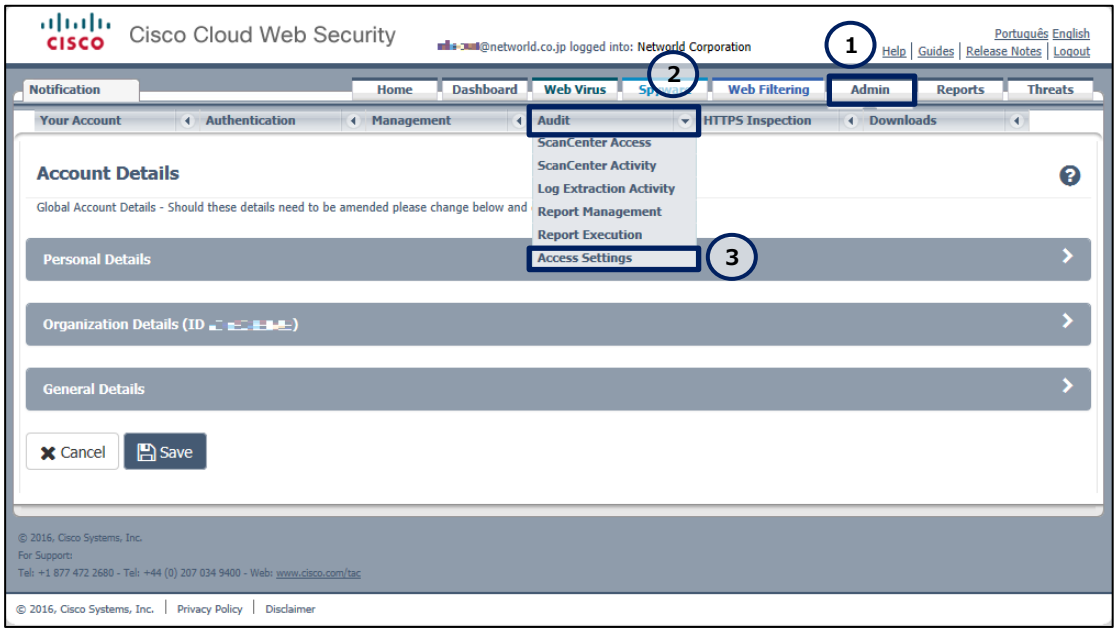


図 14 ScanCenter のアラート通知の設定

(2) アラート通知の送信元電子メールアドレス、アカウントロック解除依頼先の電子メールアドレス、アラート通知先の電子メールアドレス、およびアラート通知の実行間隔を設定します。アラート通知先の電子メールアドレスを複数登録する場合は、④を電子メールアドレスの数だけ繰り返します。

① 「Alert email sender address:」テキストボックスにアラート通知の送信者の電子メールアドレスを入力します。この値を指定しない場合、既定で noreply@scansafe.net が送信者として設定されます。

② 「Contact email in the login failure message:」テキストボックスにアカウントロック時のロック解除の依頼先の電子メールアドレスを入力します。この値を指定しない場合、既定でスーパーユーザーアカウントの電子メールアドレスが依頼先として設定されます。

③ 「Enable email alerts」チェックボックスにチェックを入れます。

④ 「Email addresses to be alerted in the event of login failures」テキストボックスにアラート通知を受信する電子メールアドレスを入力します。最大で 5 つの電子メールアドレスを設定できます。

⑤ 「Limit the rate of email alerts（Max frequency）」ドロップダウンリストから一括処理する件数を選択します。アラート通知の数がこの設定に達した場合に電子メールが送信されます。

⑥ 「Limit the rate of email alerts（Period）」ドロップダウンリストから送信間隔を選択します。アラート通知の間隔がこの設定に達した場合に電子メールが送信されます。

⑦ 「Save」ボタンをクリックします。

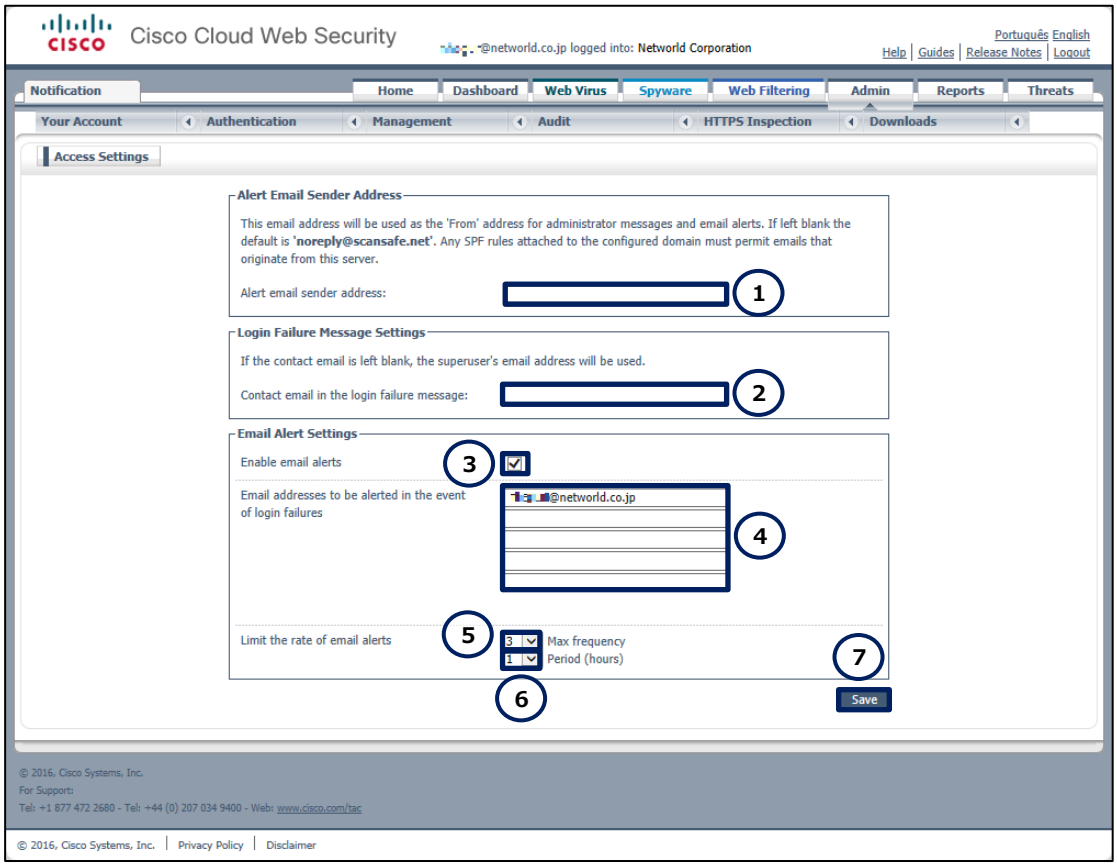


図 15 ScanCenter のアラート通知の設定（詳細）

3.2.5 Portal 2.0 の設定

ここまで使用した ScanCenter の機能は、Portal 1.0 によって提供されています。ここでは、新管理ポータルの Portal 2.0 の基本設定を実行します。Portal 2.0 では、CWS のアクティビティを分析するためのより高度、高速、柔軟なインターフェースが提供されます。

(1) ScanCenter の Portal 2.0 に移動します。「Home」タブをクリックします。「Launch Portal」ボタンをクリックします。

図 16 ScanCenter のホーム

(2) ScanCenter の Portal 2.0 の設定画面に移動します。「タイル」ボタンをクリックします。

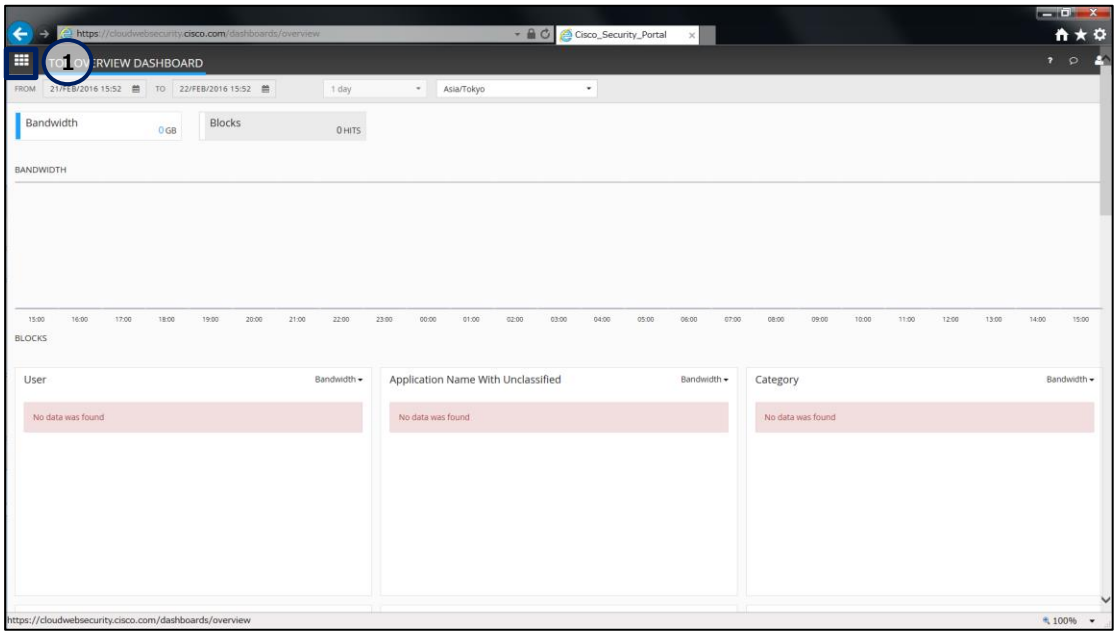


図 17 Portal 2.0 のダッシュボード

(3) ScanCenter の Portal 2.0 の設定画面に移動します。「PREFERENCES」ボタンをクリックします。

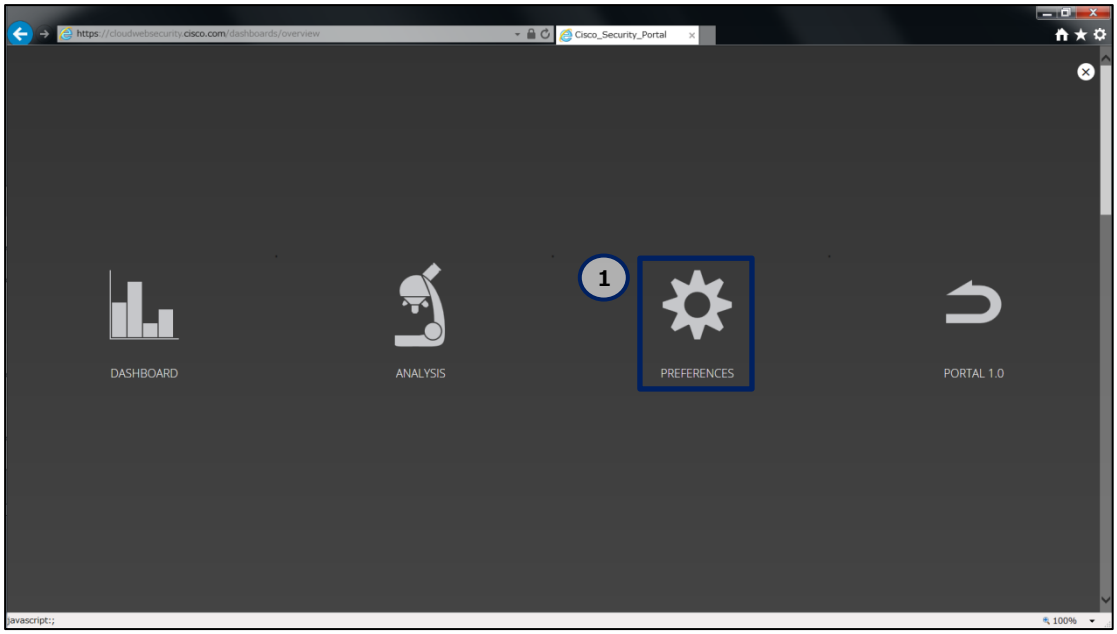


図 18 Portal 2.0 の設定

(3) ScanCenter の Portal 2.0 の設定を実行します。

① 「Time Zone」ドロップダウンリストから **Asia/Tokyo** を選択します。

② 「Date Format」ドロップダウンリストから日付の表示形式を選択します。
③ 「Preferred Language」ドロップダウンリストから Portal 2.0 の表示言語を選択します。Portal 2.0 が現在サポートしている言語は、英語とポルトガル語の 2 種類です。
④ 「Save」ボタンをクリックします。

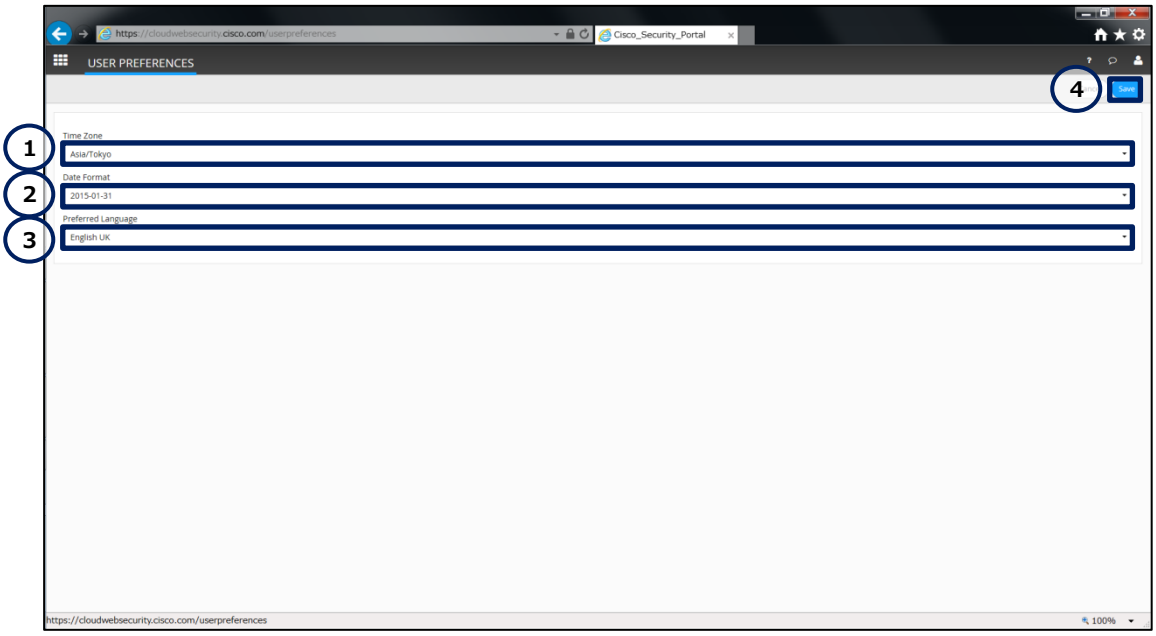


図 19 Portal 2.0 の設定（詳細）

3.3 Web セキュリティ（マルウェア）の基本設定

Web セキュリティ（マルウェア）のユーザー警告、およびアラート通知の設定を実行します。

3.3.1 ユーザー警告の設定

Web セキュリティ（マルウェア）の機能によってトラフィックが CWS にブロックされた場合にユーザーに表示する警告を設定します。

(1) Web セキュリティ（マルウェア）のユーザー警告の設定画面に移動します。「Web Virus」タブをクリックします。「Notifications」ドロップダウンリストから「User Messages」リストをクリックします。

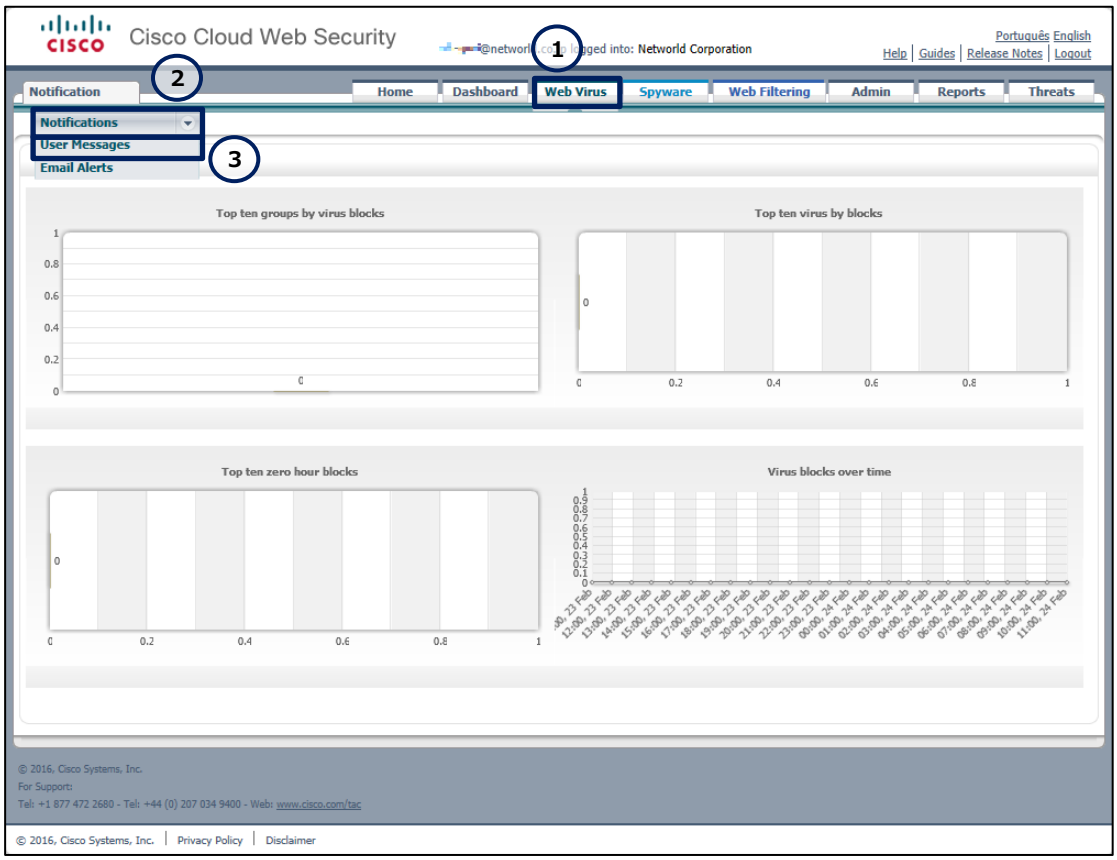


図 20 Web セキュリティ（マルウェア）のユーザー警告の設定

(2) Web セキュリティ（マルウェア）のユーザー警告を設定します。

① 既定のユーザー警告を含める場合は、「Include standard HTML page template for block page」チェックボックスにチェックを入れます。

② 「Customized Alert Page」テキストボックスにカスタムのユーザー警告をプレーンテキストまたは HTML 形式で入力します。次の文字列を置換可能な変数として使用できます。

- #category
- #reason
- #url
- #username

③ 「Save」ボタンをクリックします。

④ ユーザー警告を確認する場合は、「Preview」ボタンをクリックします。

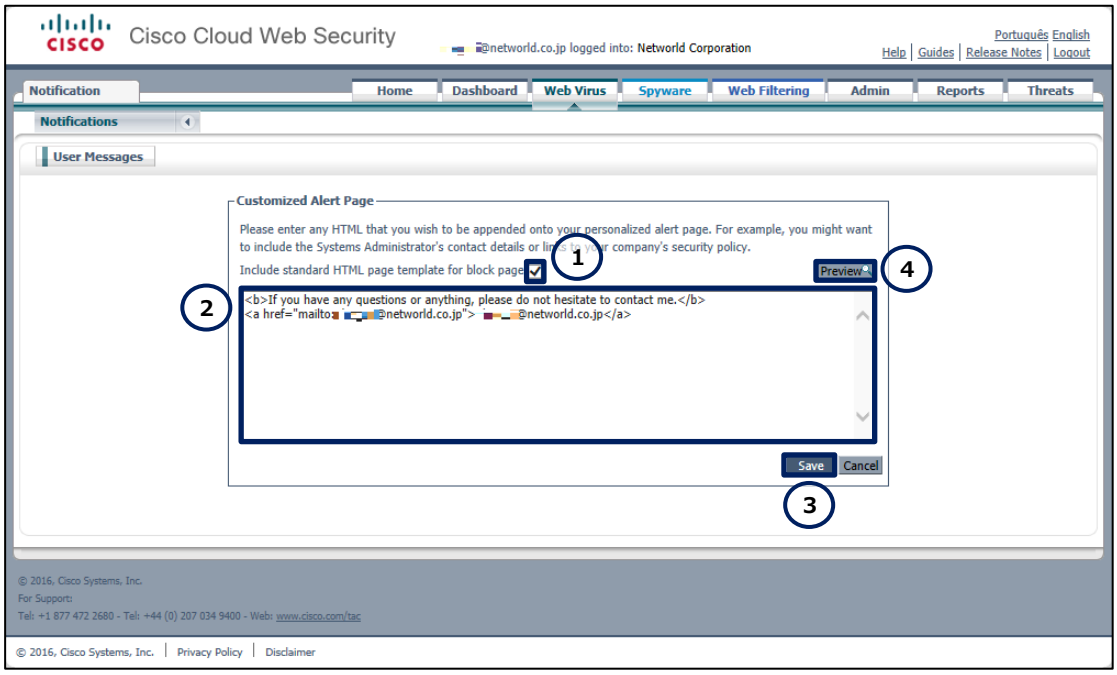


図 21 Web セキュリティ（マルウェア）のユーザー警告の設定（詳細）

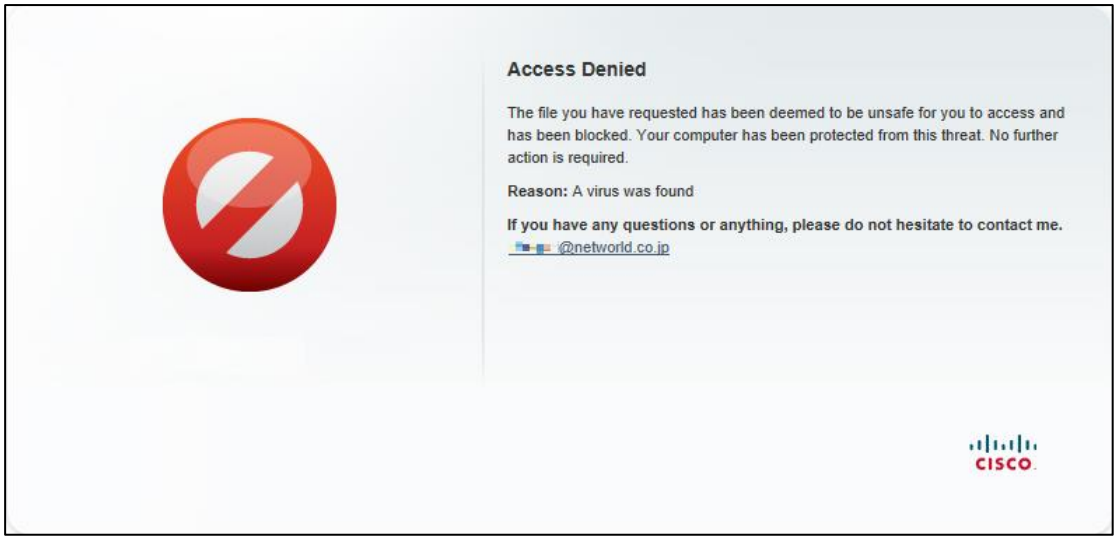


図 22 Web セキュリティ（マルウェア）のユーザー警告

3.3.2 アラート通知の設定

Web セキュリティ（マルウェア）の機能によってトラフィックが CWS にブロックされた場合に、特定の宛先に電子メールでアラート通知を送信できます。この情報を電子メールで受信したい場合は、通知する宛先の電子メールアドレスを設定します。

(1) Web セキュリティ（マルウェア）のアラート通知の設定画面に移動します。「Web Virus」タブをク

リックします。「Notifications」ドロップダウンリストから「Email Alerts」リストをクリックします。

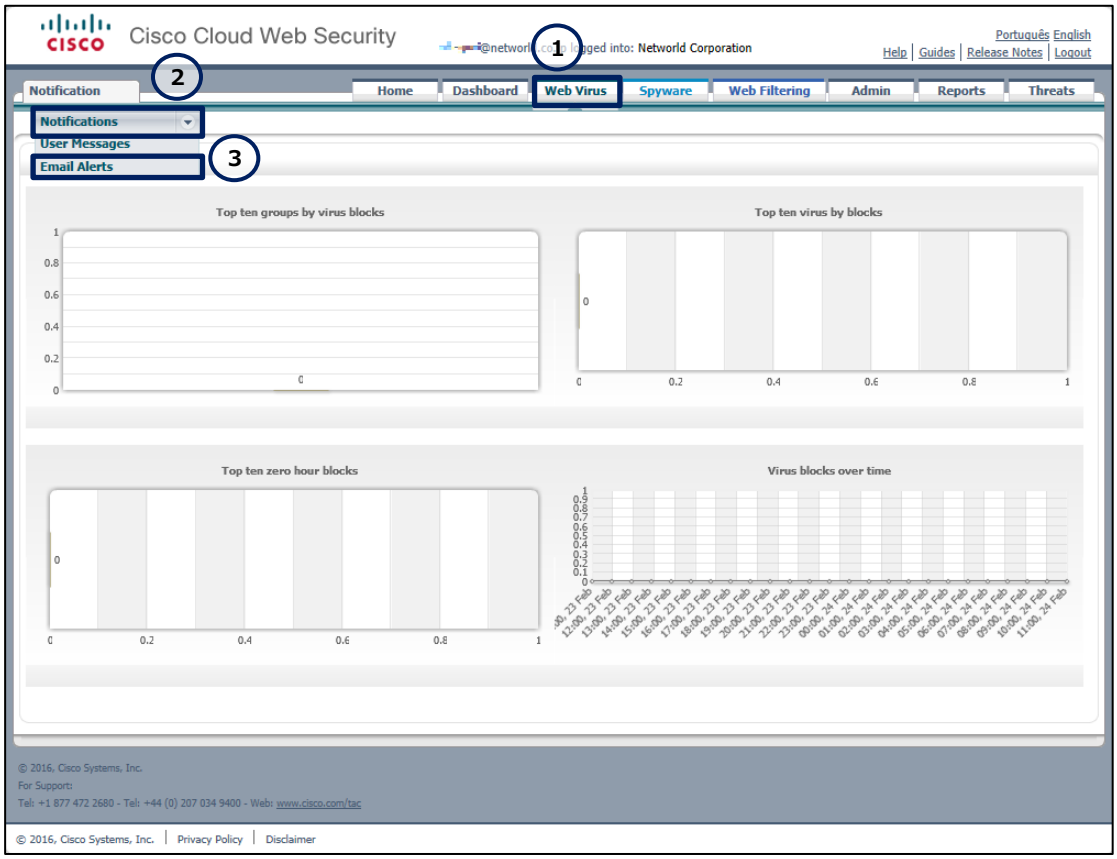


図 23 Web セキュリティ（マルウェア）のアラート通知の設定

(2) Web セキュリティ（マルウェア）のアラート通知を設定します。

① 「Do you with to be notified when a page is blocked?」ドロップダウンリストから **Yes** を選択します。

② 「Email address(es) for notifications to be sent to:」テキストボックスにアラート通知を受信する電子メールアドレスを入力します。最大で 5 つの電子メールアドレスを設定できます。

③ 「Limit email alerts to（per）」ドロップダウンリストから一括処理する件数を選択します。アラート通知の数がこの設定に達した場合に電子メールが送信されます。

④ 「Limit email alerts to（hour）」ドロップダウンリストから送信間隔を選択します。アラート通知の間隔がこの設定に達した場合に電子メールが送信されます。

⑤ 「Save」ボタンをクリックします。

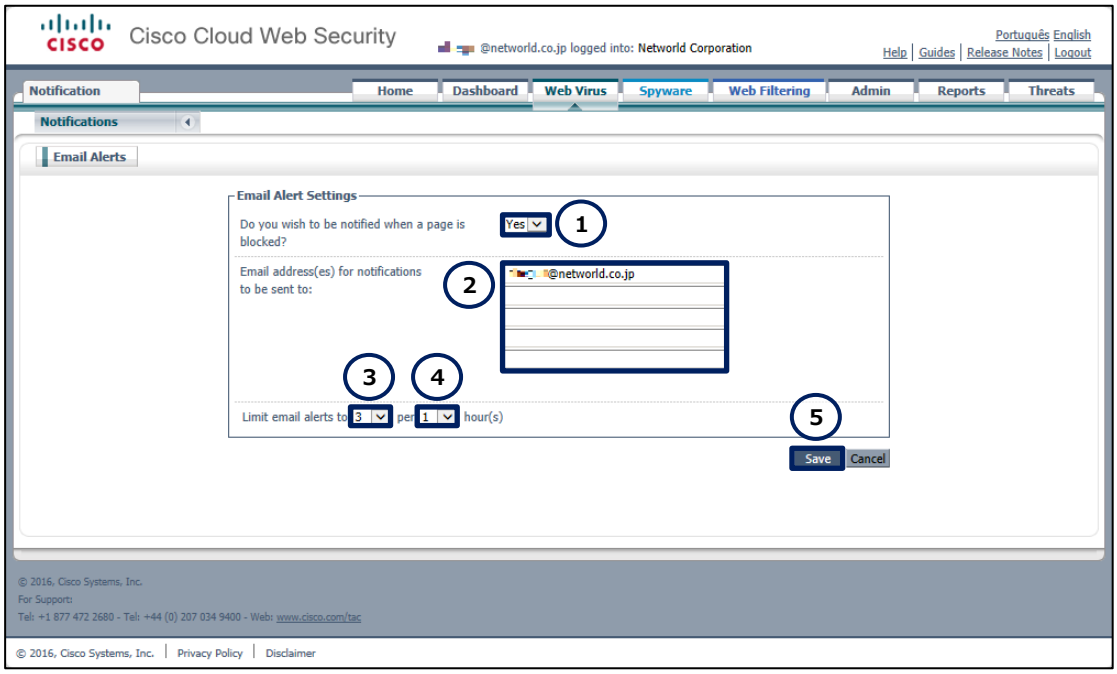


図 24 Web セキュリティ（マルウェア）のアラート通知の設定（詳細）

3.4 Web セキュリティ（スパイウェア）の基本設定

Web セキュリティ（スパイウェア）のユーザー警告、およびアラート通知の設定を実行します。

3.4.1 ユーザー警告の設定

Web セキュリティ（スパイウェア）の機能によってトラフィックが CWS にブロックされた場合にユーザーに表示する警告を設定します。

(1) Web セキュリティ（スパイウェア）のユーザー警告の設定画面に移動します。「Spyware」タブをクリックします。「Notifications」ドロップダウンリストから「User Messages」リストをクリックします。

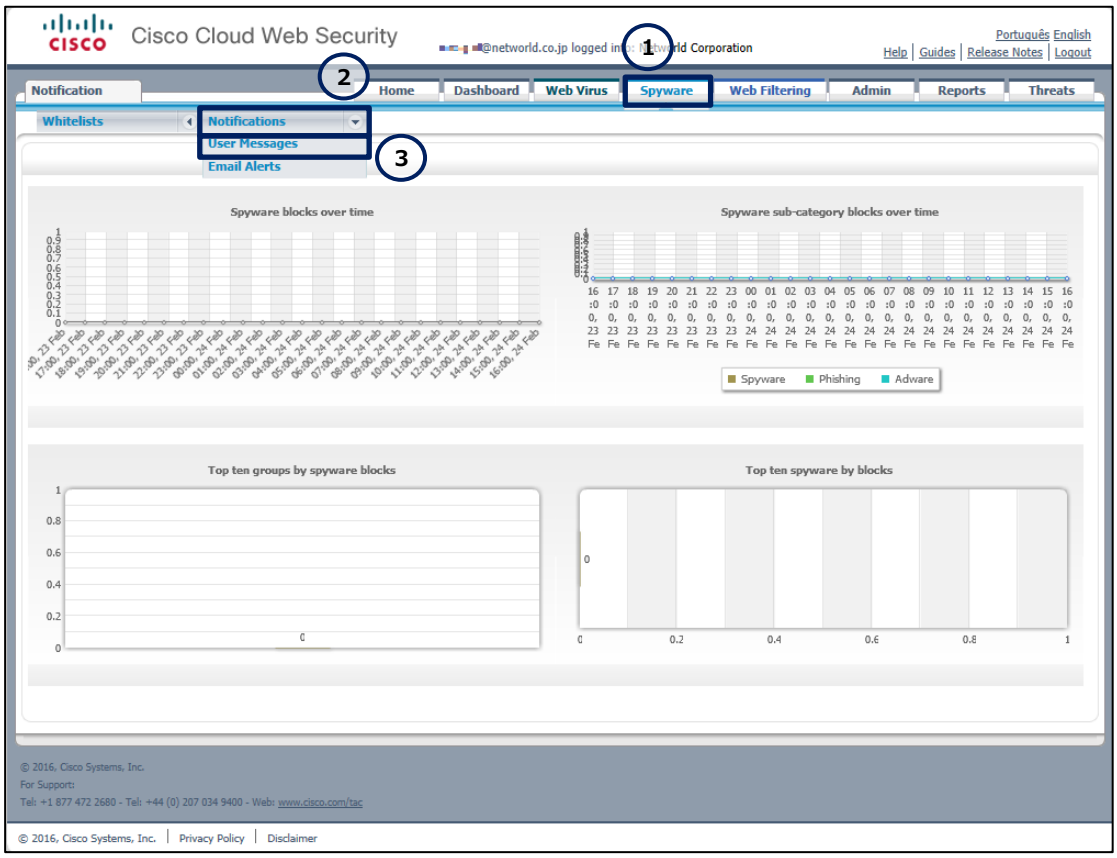


図 25 Web セキュリティ（スパイウェア）のユーザー警告の設定

(2) Web セキュリティ（スパイウェア）のユーザー警告を設定します。

① 既定のユーザー警告を含める場合は、「Include standard HTML page template for block page」チェックボックスにチェックを入れます。

② 「Customized Alert Page」テキストボックスにカスタムのユーザー警告をプレーンテキストまたは HTML 形式で入力します。次の文字列を置換可能な変数として使用できます。

- #category
- #reason
- #url
- #username

③ 「Save」ボタンをクリックします。

④ ユーザー警告を確認する場合は、「Preview」ボタンをクリックします。

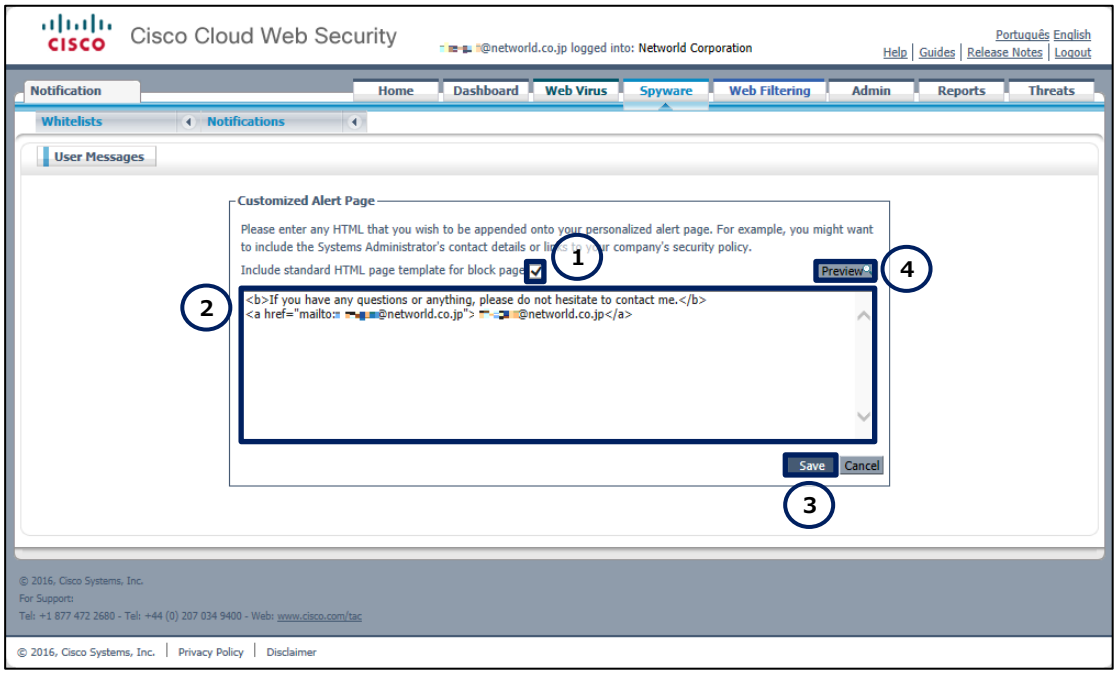


図 26 Web セキュリティ（スパイウェア）のユーザー警告の設定（詳細）

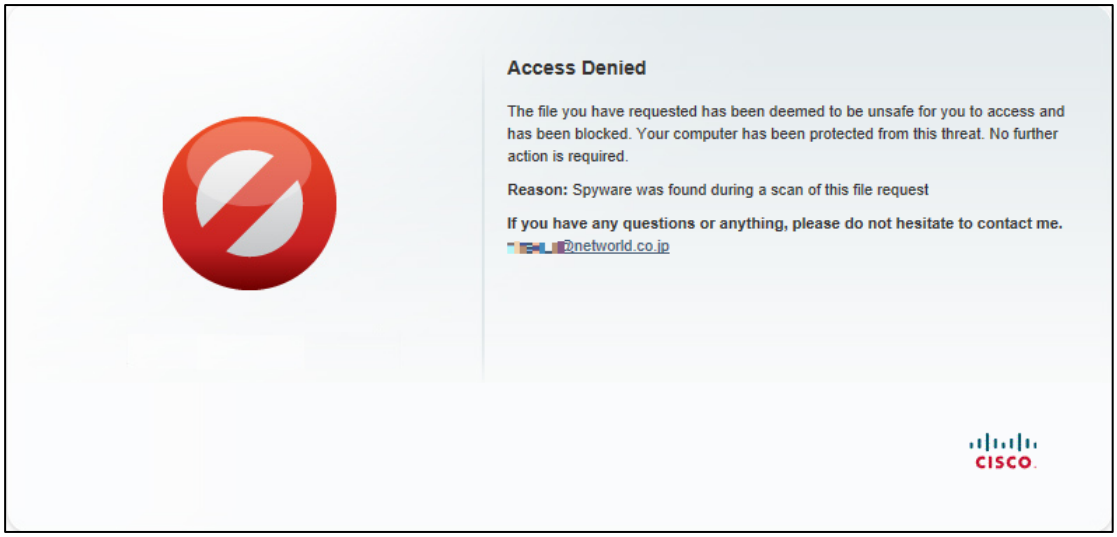


図 27 Web セキュリティ（スパイウェア）のユーザー警告

3.4.2 アラート通知の設定

Web セキュリティ（スパイウェア）の機能によってトラフィックが CWS にブロックされた場合に、特定の宛先に電子メールでアラート通知を送信できます。この情報を電子メールで受信したい場合は、通知する宛先の電子メールアドレスを設定します。

(1) Web セキュリティ（スパイウェア）のアラート通知の設定画面に移動します。「Spyware」タブをク

リックします。「Notifications」ドロップダウンリストから「Email Alerts」リストをクリックします。

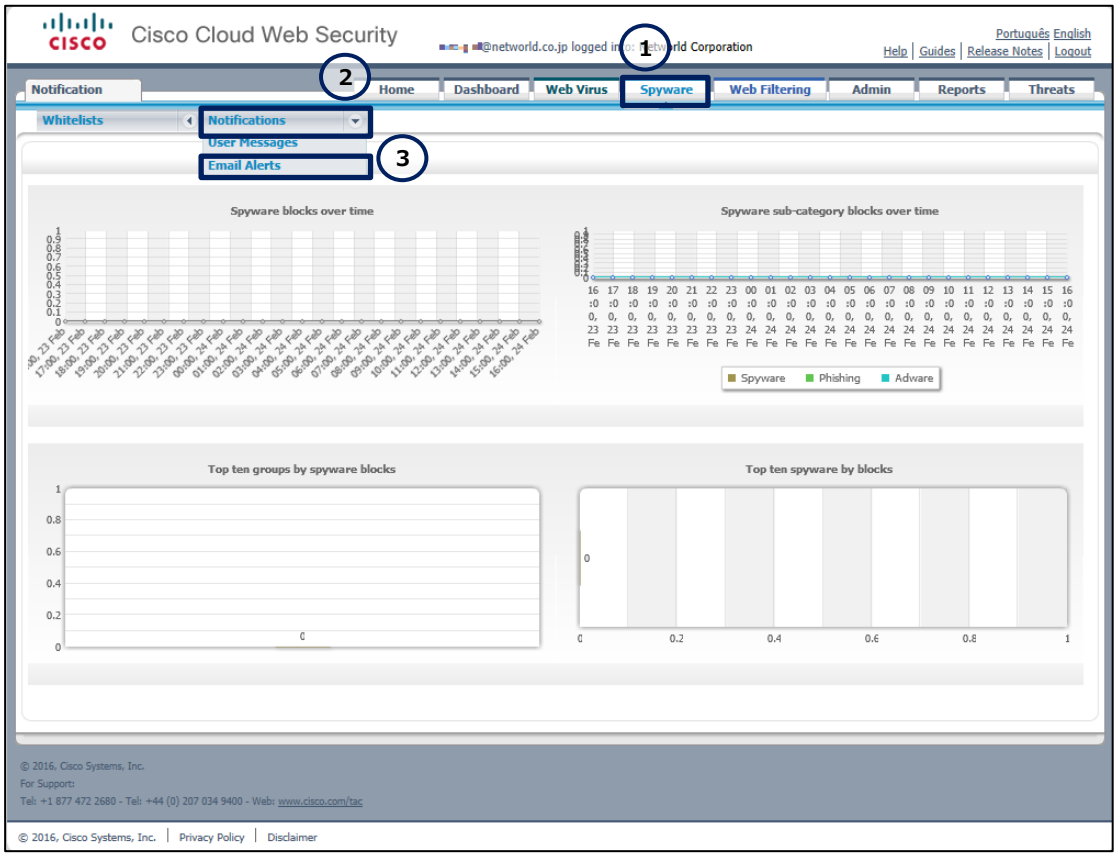


図 28 Web セキュリティ（スパイウェア）のアラート通知の設定

(2) Web セキュリティ（スパイウェア）のアラート通知を設定します。

① 「Do you with to be notified when Spyware/Adware/Cookies are blocked?」ドロップダウンリストから **Yes** を選択します。

② 「Email address(es) for notifications to be sent to:」テキストボックスにアラート通知を受信する電子メールアドレスを入力します。最大で 5 つの電子メールアドレスを設定できます。

③ 「Limit email alerts to（per）」ドロップダウンリストから一括処理する件数を選択します。アラート通知の数がこの設定に達した場合に電子メールが送信されます。

④ 「Limit email alerts to（hour）」ドロップダウンリストから送信間隔を選択します。アラート通知の間隔がこの設定に達した場合に電子メールが送信されます。

⑤ 「Save」ボタンをクリックします。

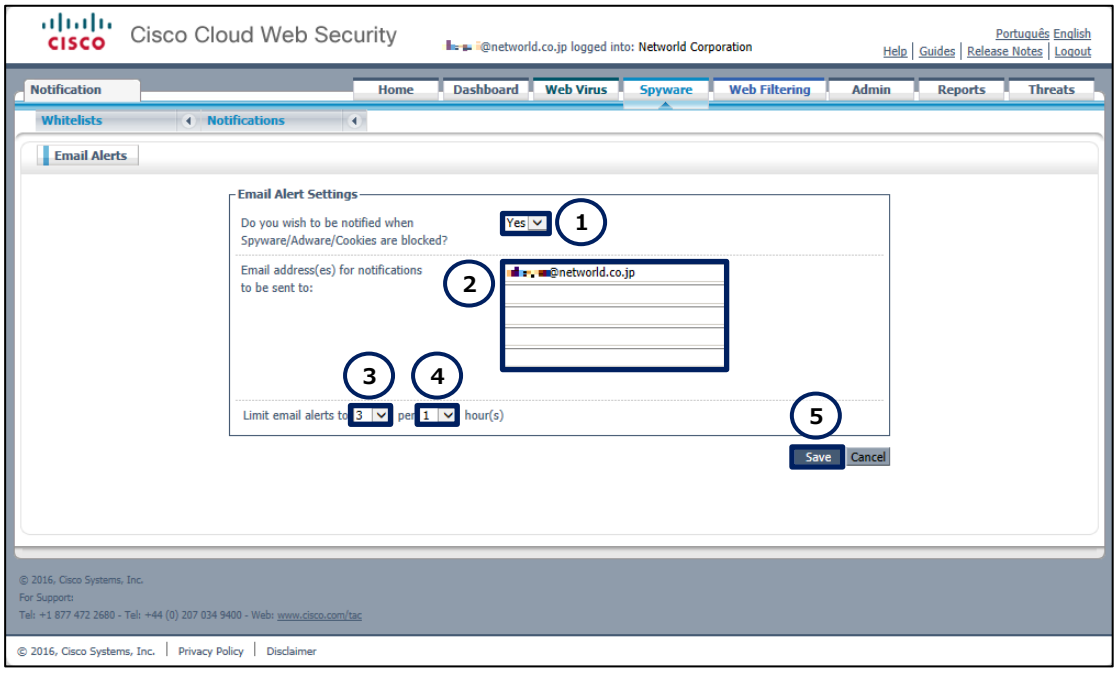


図 29 Web セキュリティ（スパイウェア）のアラート通知の設定（詳細）

3.5 Web フィルタリングの基本設定

Web フィルタリングのユーザー警告、およびアラート通知の設定を実行します。

3.5.1 ユーザー警告の設定

Web フィルタリングの機能によってトラフィックが CWS にブロックされた場合にユーザーに表示する警告を設定します。

(1) Web フィルタリングのユーザー警告の設定画面に移動します。「Web Filtering」タブをクリックします。「Notifications」ドロップダウンリストから「User Messages」リストをクリックします。

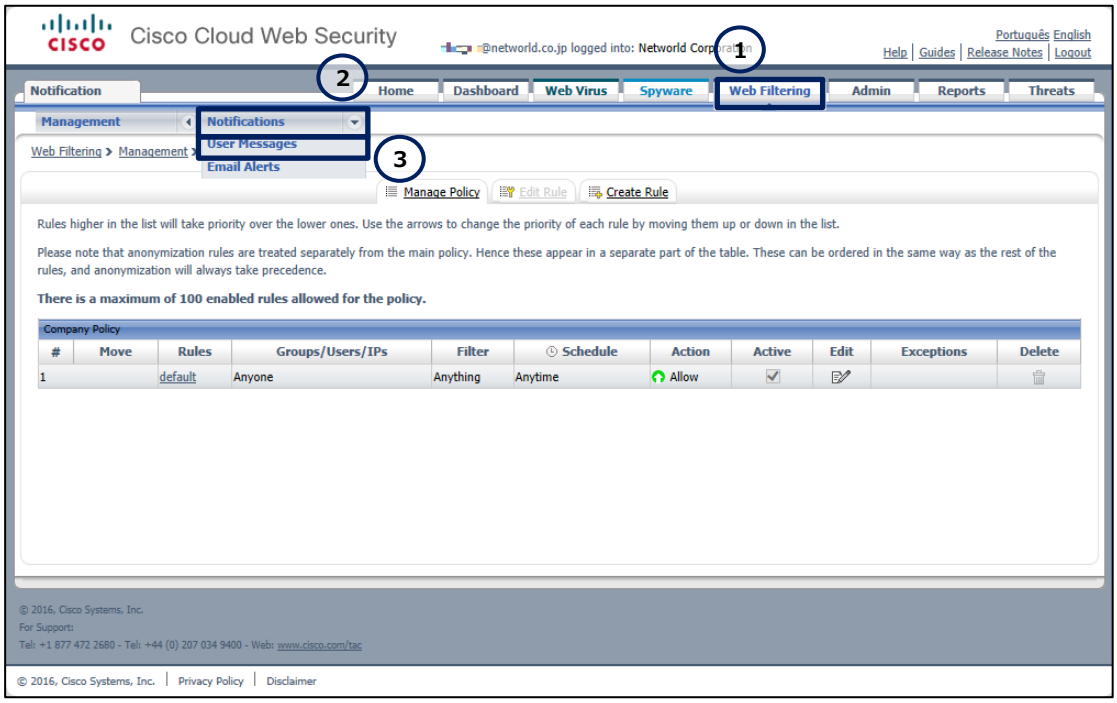


図 30 Web フィルタリングのユーザー警告の設定

(2) Web フィルタリングのユーザー警告および注意を設定します。

① 既定のユーザー警告を含める場合は、「Include standard HTML page template for block page」チェックボックスにチェックを入れます。

② 「Customized Alert Page」テキストボックスにカスタムのユーザー警告をプレーンテキストまたは HTML 形式で入力します。次の文字列を置換可能な変数として使用できます。

- #category
- #reason
- #url
- #username

③ 「Save」ボタンをクリックします。

④ ユーザー警告を確認する場合は、「Preview」ボタンをクリックします。

⑤ 「Timeout Value」ドロップダウンリストから繰り返し警告を表示する間隔を選択します。0 を選択した場合はセッションベースの Cookie、1～24 を選択した場合はタイムベースの Cookie を使用して警告の表示を制御します。

⑥ 既定のユーザー注意を含める場合は、「Include standard HTML page template for warning page」チェックボックスにチェックを入れます。

⑦ 「Customized Warn Alert Page」テキストボックスにカスタムのユーザー注意をプレーンテキストまたは HTML 形式で入力します。次の文字列を置換可能な変数として使用できます。

- #category
- #reason
- #url
- #username

⑧ 「Save」ボタンをクリックします。

⑨ ユーザー注意を確認する場合は、「Preview」ボタンをクリックします。

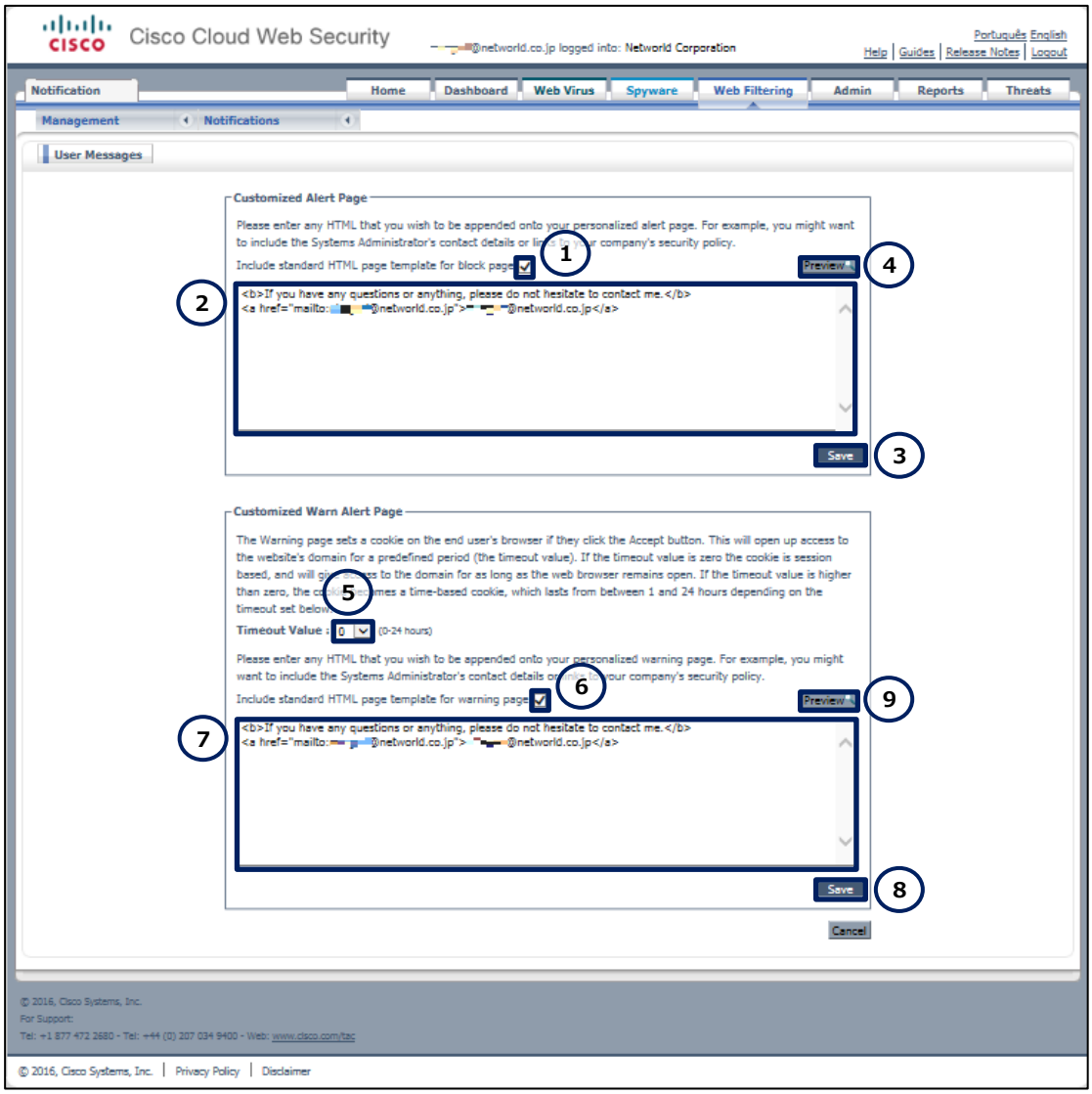


図 31 Web フィルタリングのユーザー警告の設定（詳細）

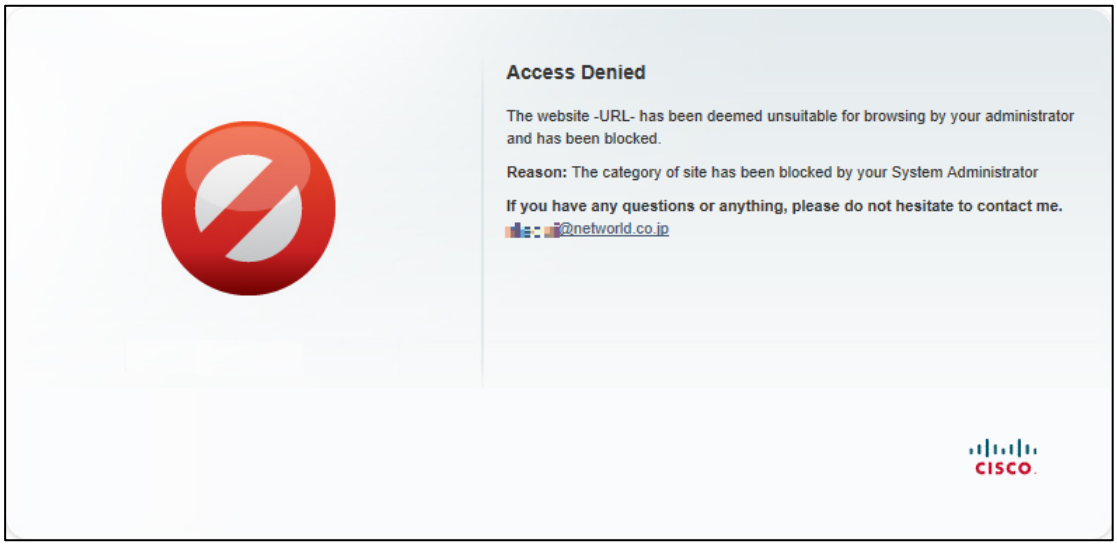


図 32 Web フィルタリングのユーザー警告

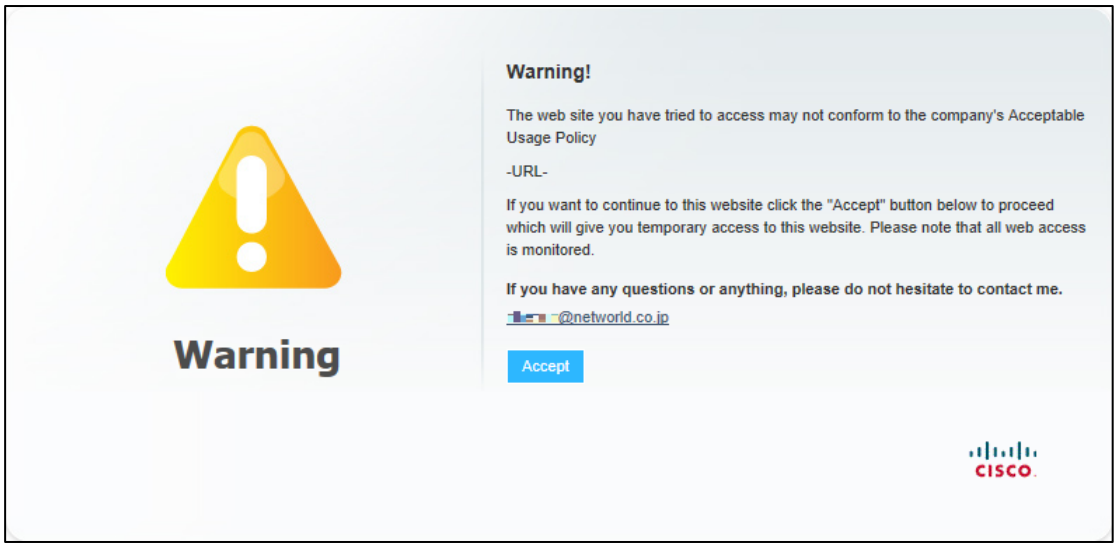


図 33 Web フィルタリングのユーザー注意

3.5.2 アラート通知の設定

Webフィルタリングの機能によってトラフィックがCWSにブロックされた場合に、特定の宛先に電子メールでアラート通知を送信できます。この情報を電子メールで受信したい場合は、通知する宛先の電子メールアドレスを設定します。

(1) Web フィルタリングのアラート通知の設定画面に移動します。「Web Filtering」タブをクリックします。「Notifications」ドロップダウンリストから「Email Alerts」リストをクリックします。

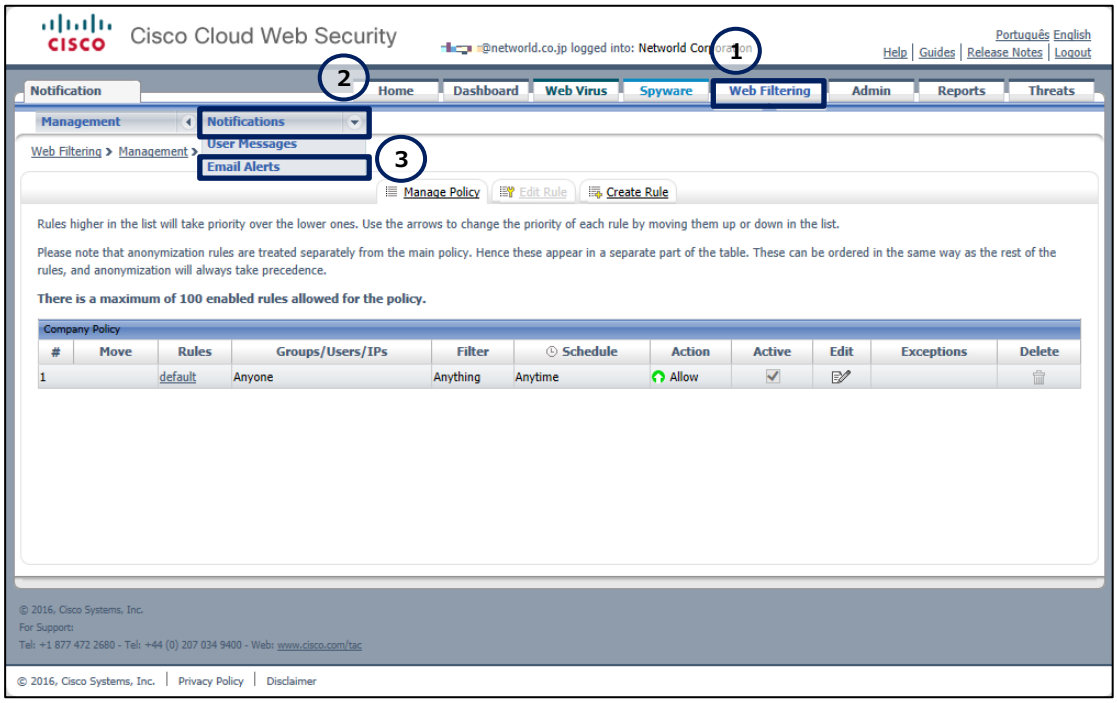


図 34 Web フィルタリングのアラート通知の設定

(2) Web フィルタリングのアラート通知を設定します。

① 「Do you with to be notified when a page is blocked?」ドロップダウンリストから **Yes** を選択します。

② 「Email address(es) for notifications to be sent to:」テキストボックスにアラート通知を受信する電子メールアドレスを入力します。最大で 5 つの電子メールアドレスを設定できます。

③ 「Limit email alerts to（per）」ドロップダウンリストから一括処理する件数を選択します。アラート通知の数がこの設定に達した場合に電子メールが送信されます。

④ 「Limit email alerts to（hour）」ドロップダウンリストから送信間隔を選択します。アラート通知の間隔がこの設定に達した場合に電子メールが送信されます。

⑤ 「Save」ボタンをクリックします。

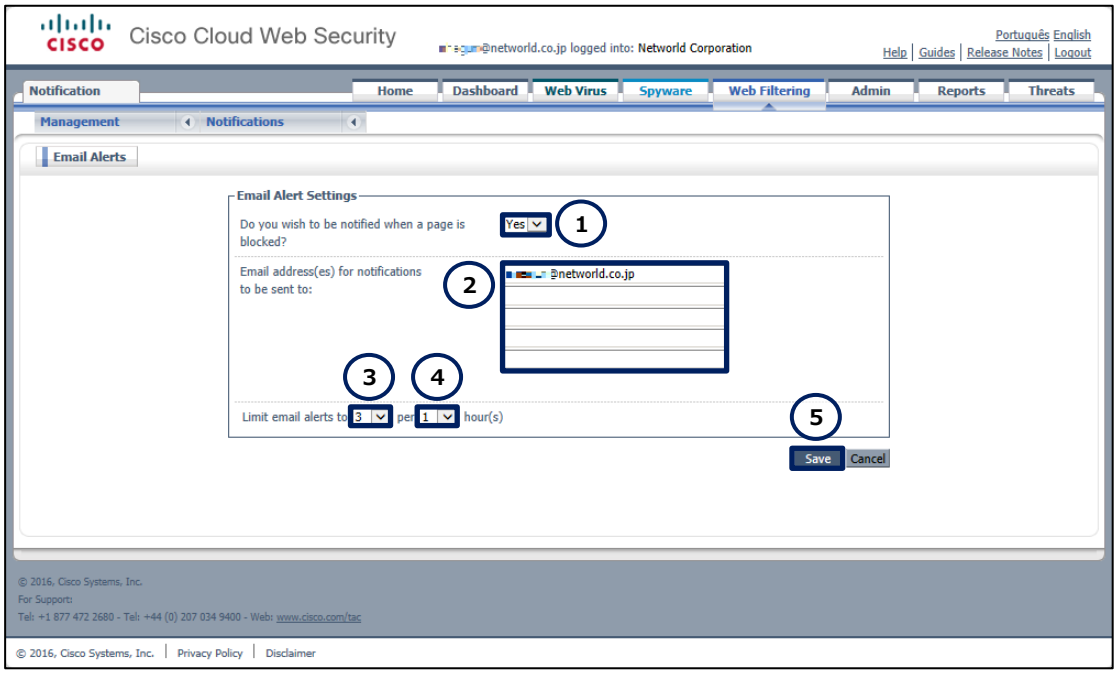


図 35 Web フィルタリングのアラート通知の設定（詳細）

3.6 Cisco AMP/CTA の基本設定

Cisco AMP/CTA のアラート通知の設定を実行します。

3.6.1 アラート通知の設定

Cisco AMP/CTA の機能によって CWS が脅威を検出した場合に、特定の宛先に電子メールでアラート通知を送信できます。この情報を電子メールで受信したい場合は、通知する宛先の電子メールアドレスを設定します。

(1) Cisco AMP/CTA のアラート通知の設定画面に移動します。「Threats」タブをクリックします。「Tile」ドロップダンリストから「EMAIL NOTIFICATIONS」リストをクリックします。

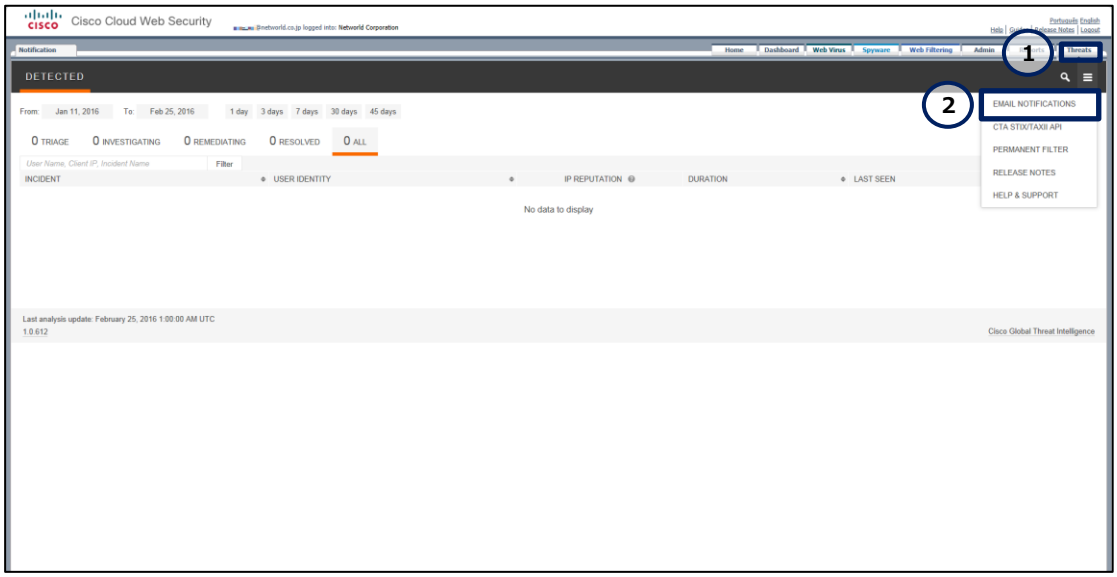


図 36 CTA のアラート通知の設定

(2) Cisco AMP/CTA のアラート通知を設定します。

① 「EMAIL NOTIFICATIONS」テキストボックスにアラート通知を受信する電子メールアドレスを入力します。最大で 5 つの電子メールアドレスを設定できます。

② 「Save」ボタンをクリックします。

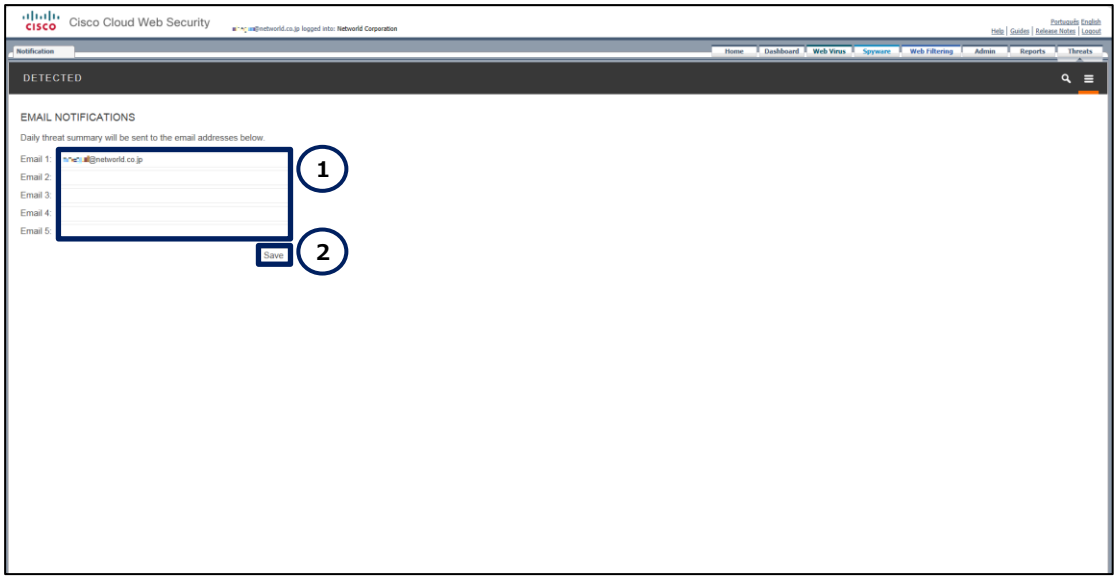


図 37 CTA のアラート通知の設定（詳細）

3.7 フィルターの設定

Web フィルタリングのフィルターの設定を実行します。フィルターの構造は、以下のとおりです。

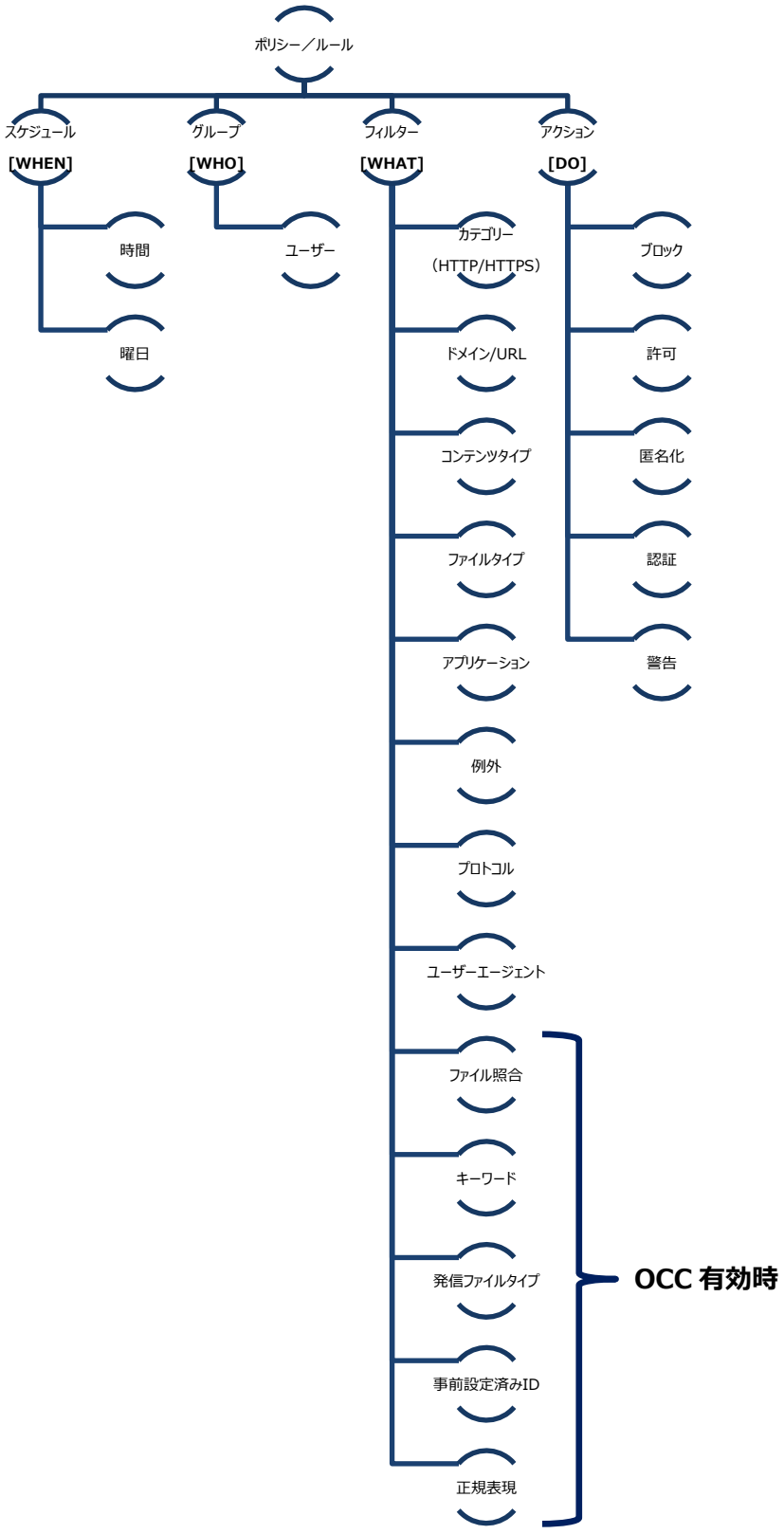


図 38 フィルターの構造

ここでは、すべてのユーザーに対して、終日 YouTube への接続をブロックするフィルターを作成します。

3.7.1 フィルターの作成

何（WHAT）をフィルターの対象にするかを、フィルターで設定します。

(1) Web フィルタリングのフィルターの設定画面に移動します。「Web Filtering」タブをクリックします。「Management」ドロップダウンリストから「Filters」リストをクリックします。

図 39 Web フィルタリングのフィルターの設定

(2) Web フィルタリングのフィルターを作成します。「Create Filter」タブをクリックします。

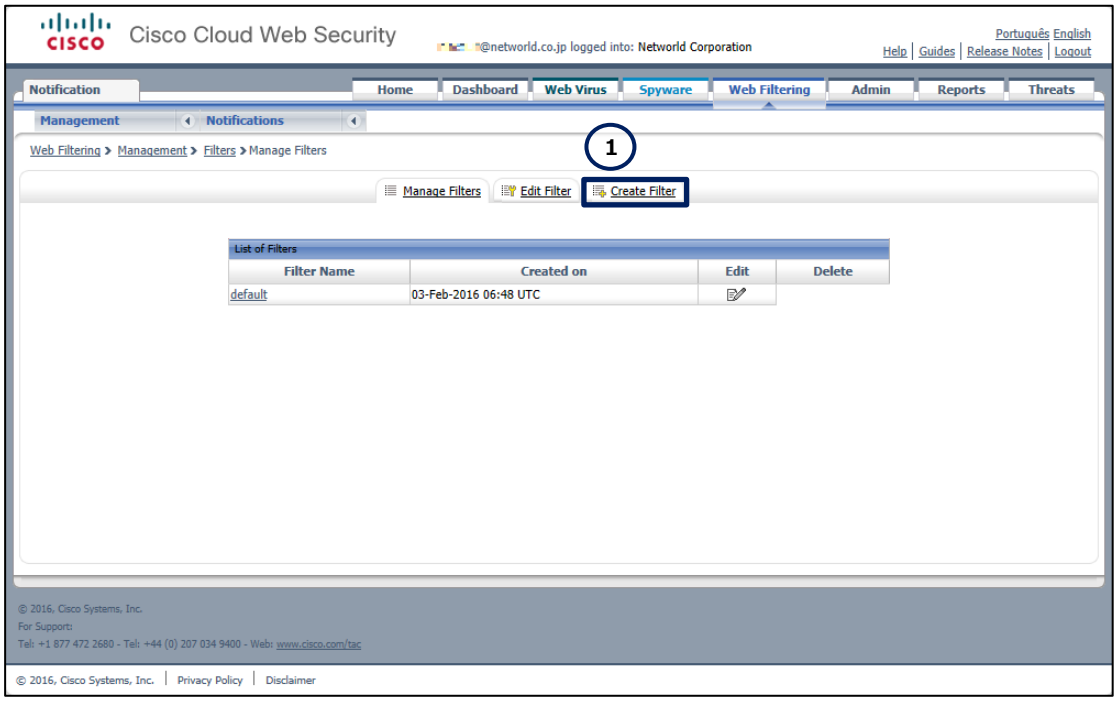


図 40 Web フィルタリングのフィルターの設定（管理）

(3) Web フィルタリングのフィルターを設定します。

① 「Filter Name:」テキストボックスにフィルターの名前を入力します。

② 「Domains」リンクラベルをクリックします。

③ 「Domains」テキストボックスに **youtube.com** を入力します。このテキストボックスには、複数のドメイン名を列挙できます。複数のドメイン名を使用する場合は、１行に１つのドメイン名を入力します。

④ 「Save all Settings」ボタンをクリックします。

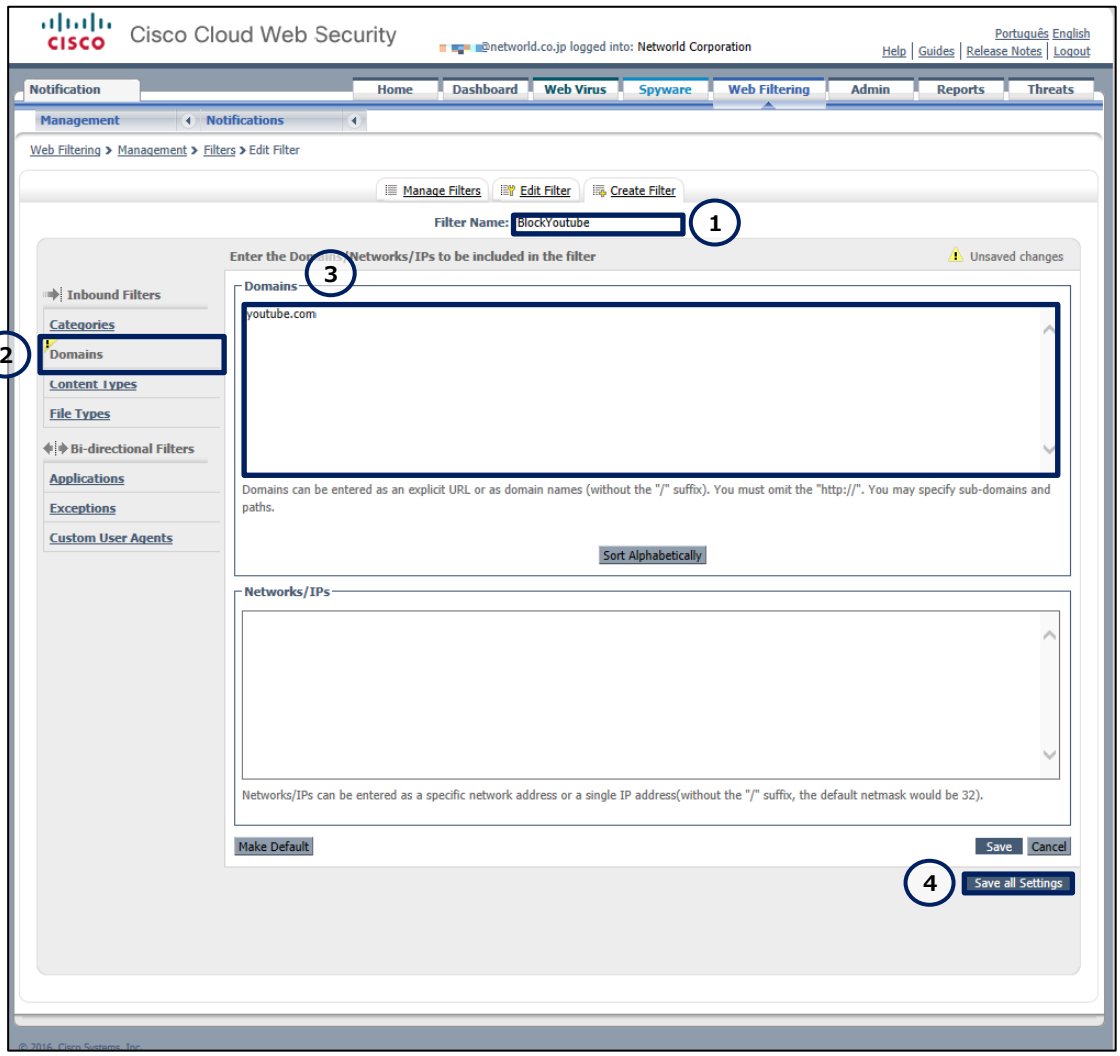


図 41 Web フィルタリングのフィルターの設定（詳細）

3.7.2 スケジュールの作成

いつ（WHEN）フィルターの対象にするかを、スケジュールで設定します。

(1) Web フィルタリングのスケジュールの設定画面に移動します。「Web Filtering」タブをクリックします。「Management」ドロップダウンリストから「Schedules」リストをクリックします。

図 42 Web フィルタリングのスケジュールの設定

(2) Web フィルタリングのスケジュールを作成します。「Create Schedule」タブをクリックします。

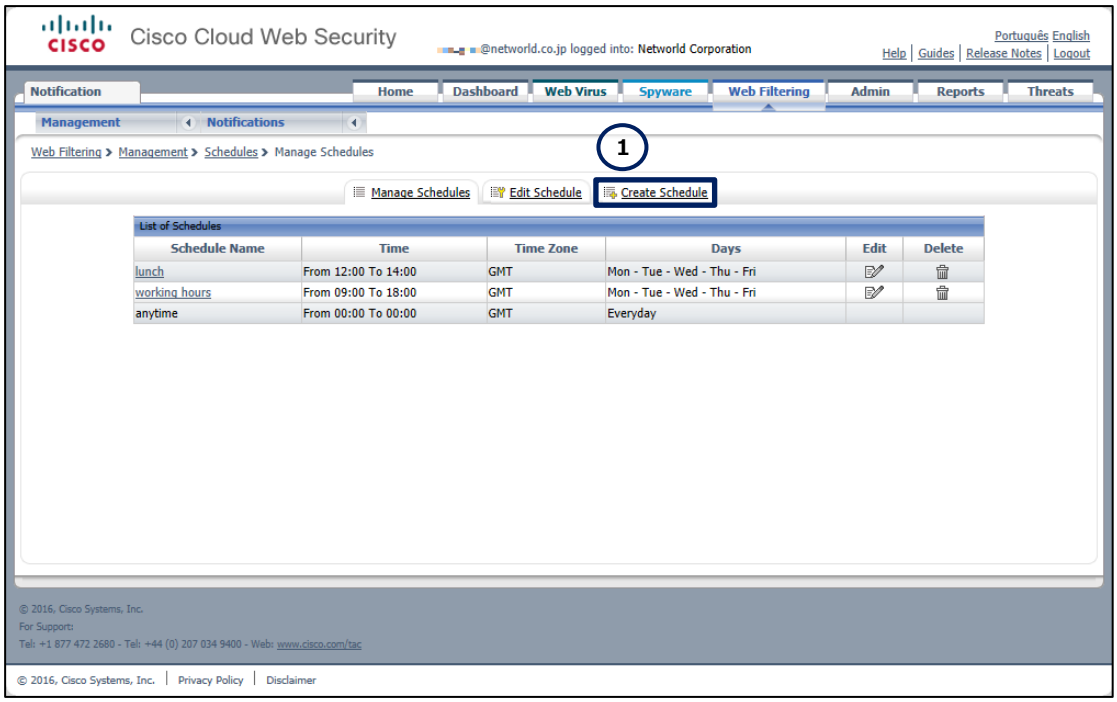


図 43 Web フィルタリングのスケジュールの設定（管理）

(3) Web フィルタリングのスケジュールを設定します。

① 「Schedule Name:」テキストボックスにスケジュールの名前を入力します。
② 「From:(Hours)」ドロップダウンリストから **00** を選択します。
③ 「From:(Mins)」ドロップダウンリストから **00** を選択します。
④ 「To:(Hours)」ドロップダウンリストから **00** を選択します。
⑤ 「To:(Mins)」ドロップダウンリストから **00** を選択します。
⑥ 「Time Zone」ドロップダウンリストから **GMT+09:00** を選択します。
⑦ 「Everyday」チェックボックスにチェックを入れます。これを設定すると、すべての曜日のチェックボックスに自動的にチェックが入ります。
⑧ 「Create Schedule」ボタンをクリックします。

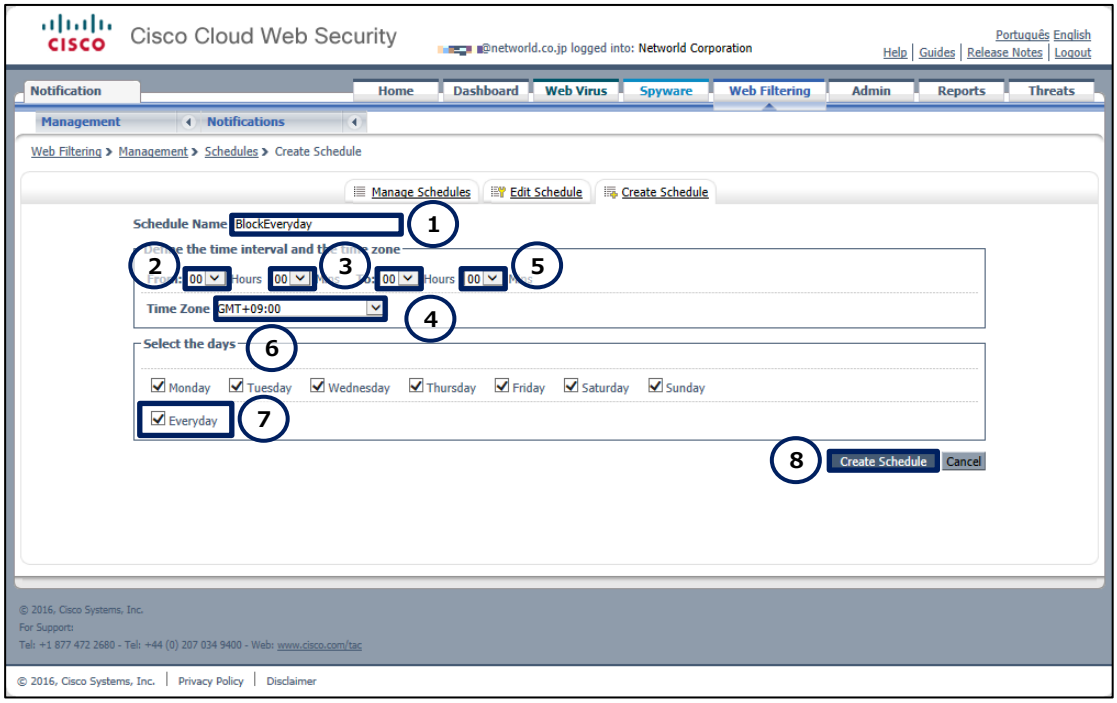


図 44 Web フィルタリングのスケジュールの設定（詳細）

3.7.3 ルールの作成

フィルターで誰（WHO）に何を実行（DO）するかを、ルールで設定します。なお、本書ではユーザーやグループ毎のトラフィックの識別または認証を使用していないため、すべてのユーザーに共通のルールが適用されます。

(1) Web フィルタリングのルールの設定画面に移動します。「Web Filtering」タブをクリックします。「Management」ドロップダウンリストから「Policy」リストをクリックします。

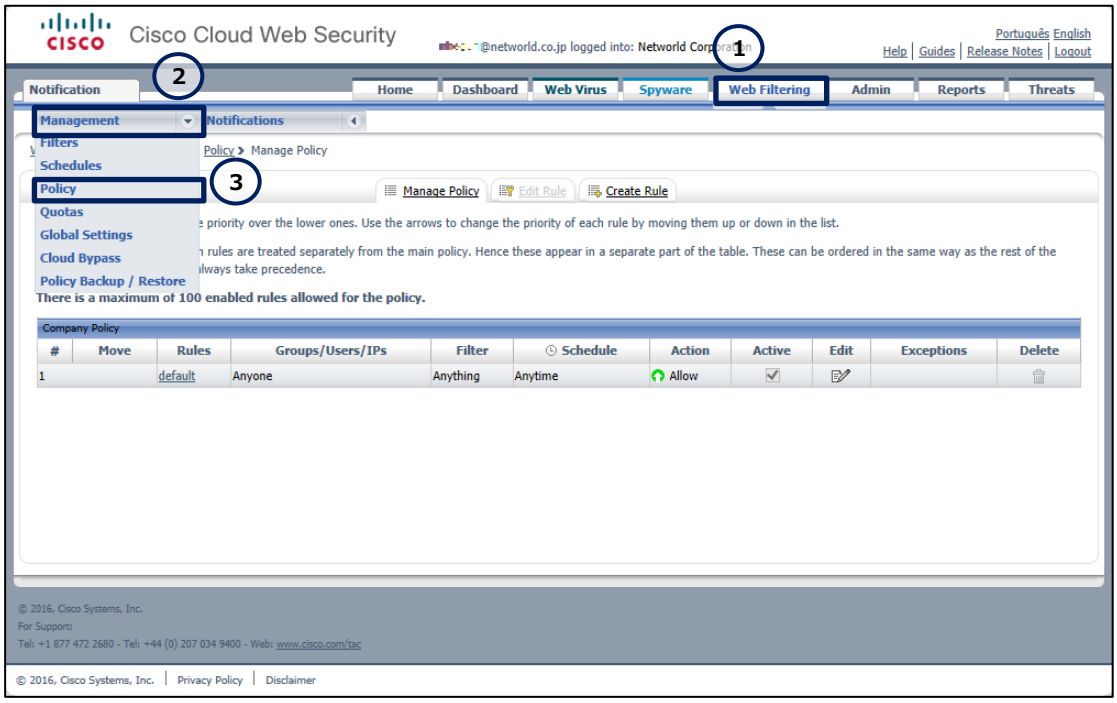


図 45 Web フィルタリングのルールの設定

(2) Web フィルタリングのルールを作成します。「Create Rule」タブをクリックします。

図 46 Web フィルタリングのルールの設定（管理）

(3) Web フィルタリングのルールを設定します。

① 「Name」テキストボックスにルールの名前を入力します。
② 「Active」チェックボックスにチェックを入れます。
③ 「Description」テキストボックスにルールの説明を入力します。
④ 「Rule Action」ドロップダウンリストから **Block** を選択します。
⑤ 「Add Filter」ドロップダウンリストから **BlockYoutube** を選択します。
⑥ 「Add＋」ボタンをクリックします。
⑦ 「Add Schedule」ドロップダウンリストから **BlockEveryday** を選択します。
⑧ 「Add＋」ボタンをクリックします。
⑨ 「Delete」ボタンをクリックして、「Schedule」リストから anytime スケジュールを削除します。
⑩ 「Create Rule」ボタンをクリックします。

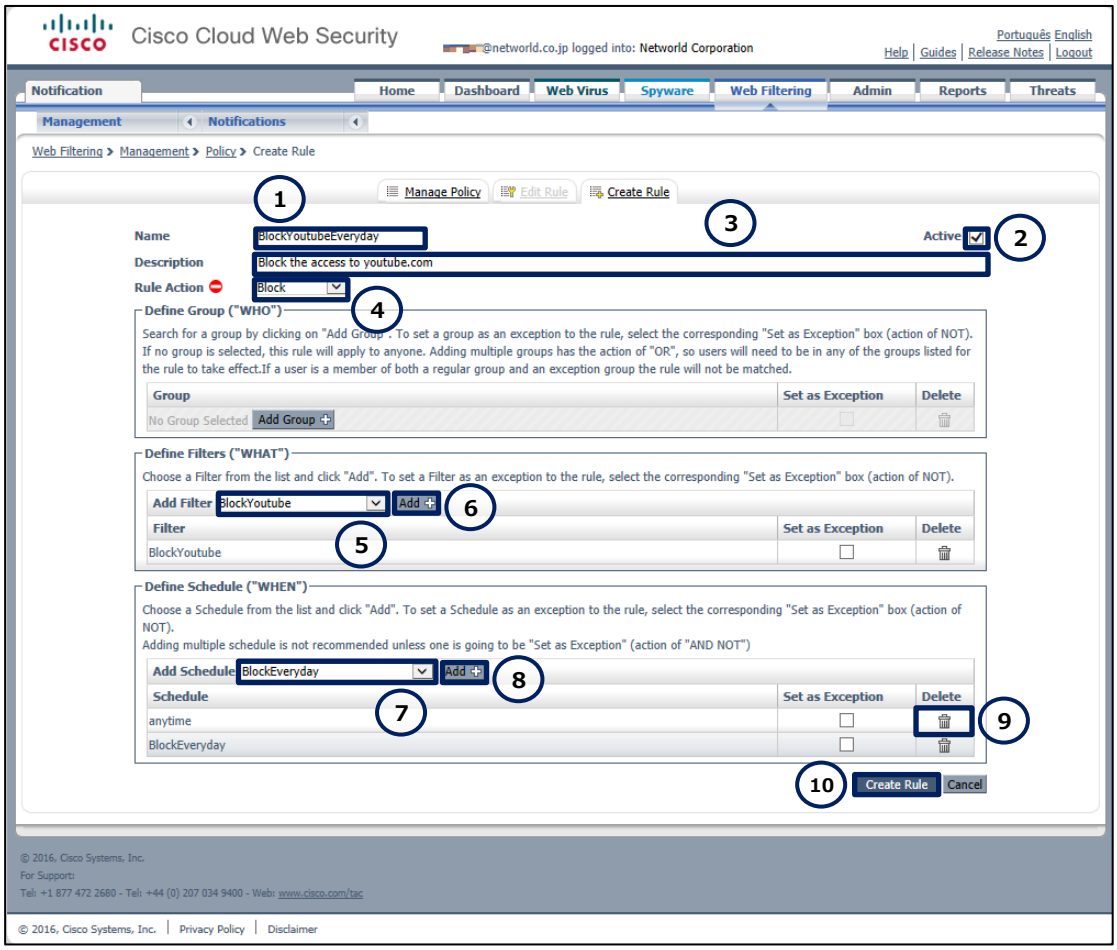


図 47 Web フィルタリングのルールの設定（詳細）

3.8 CWS ライセンスキーの発行

組織全体で共有する CWS ライセンスキーを発行します。この種の CWS ライセンスキーは会社キーと呼ばれ、このキーで認証されたすべてのトラフィックに共通のセキュリティポリシーが適用されます。セキュリテ

ィポリシーの粒度を上げるには、ユーザーやグループ単位で制御するためのユーザーキーまたはグループキーを使用できますが、本書ではそれらの説明は割愛します。

(1) ScanCenter の認証の設定画面に移動します。「Admin」タブをクリックします。「Authentication」ドロップダウンリストから「Company Key」リストをクリックします。

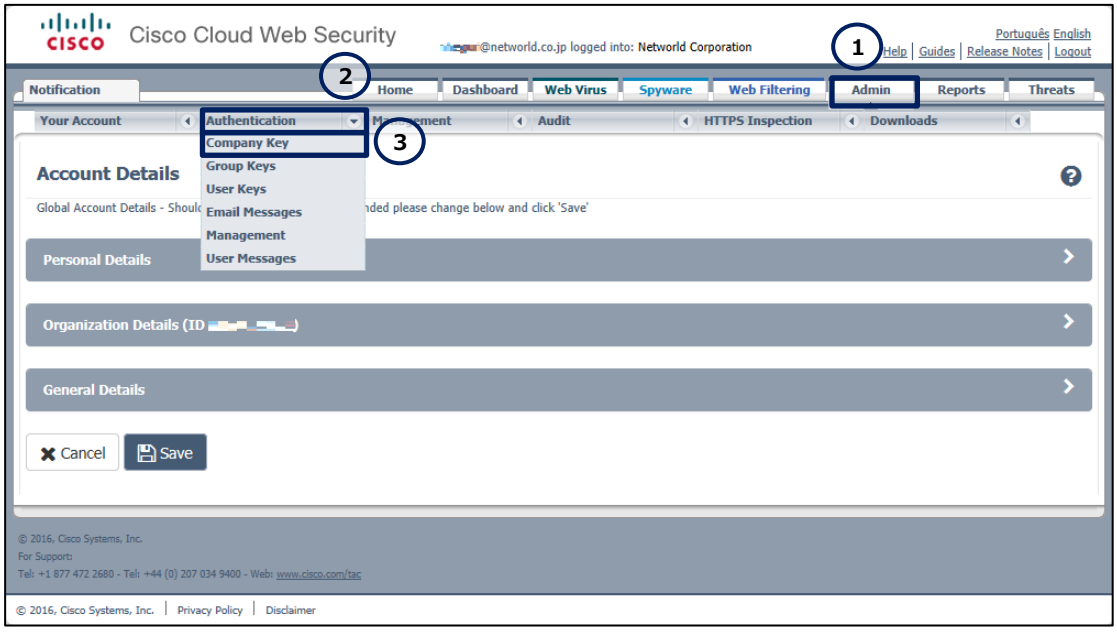


図 48 ScanCenter の認証の設定

(2) 会社キーを作成します。「Create New」ボタンをクリックします。

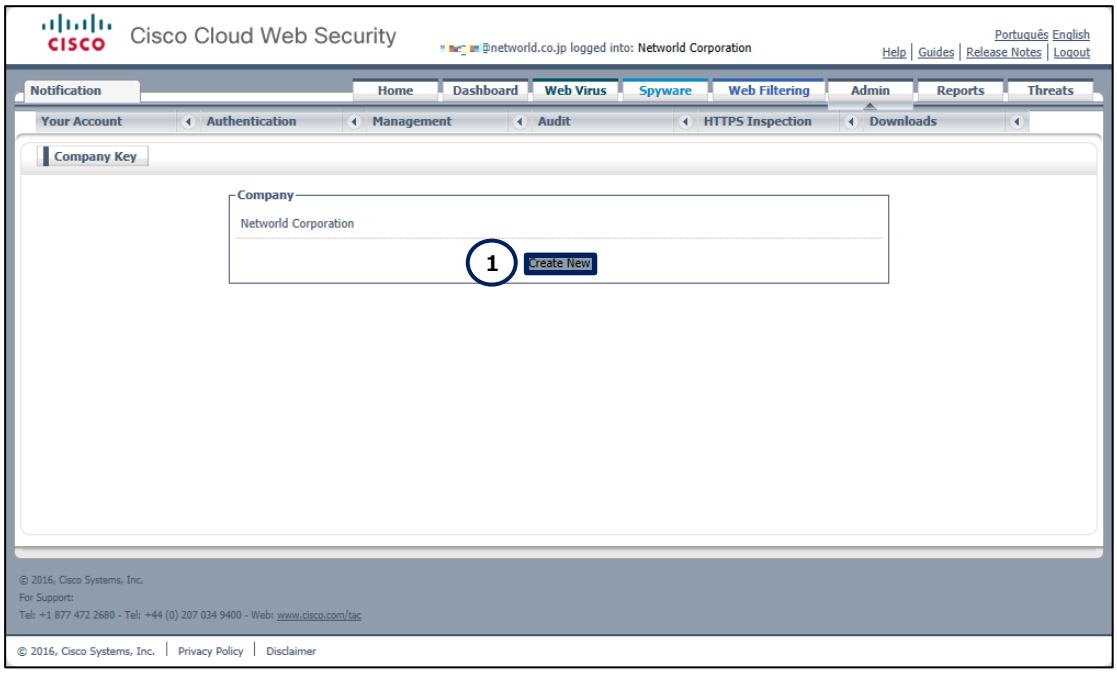


図 49 会社キーの作成

(3) 会社キーを確認します。会社キーの完全な文字列が表示されるのは作成直後のみです。2 回目以降の表示では会社キーの文字列が省略されるため、初回表示時に会社キーの文字列を安全な場所にコピーして管理してください。会社キーの文字列を失念した場合は、会社キーを非アクティブにするか、あるいは削除して、会社キーを再作成してください。会社キーが非アクティブになるか、あるいは削除されると、会社キーで認証されていたすべてのトラフィックが CWS に接続できなくなるため、会社キーの運用には注意してください。

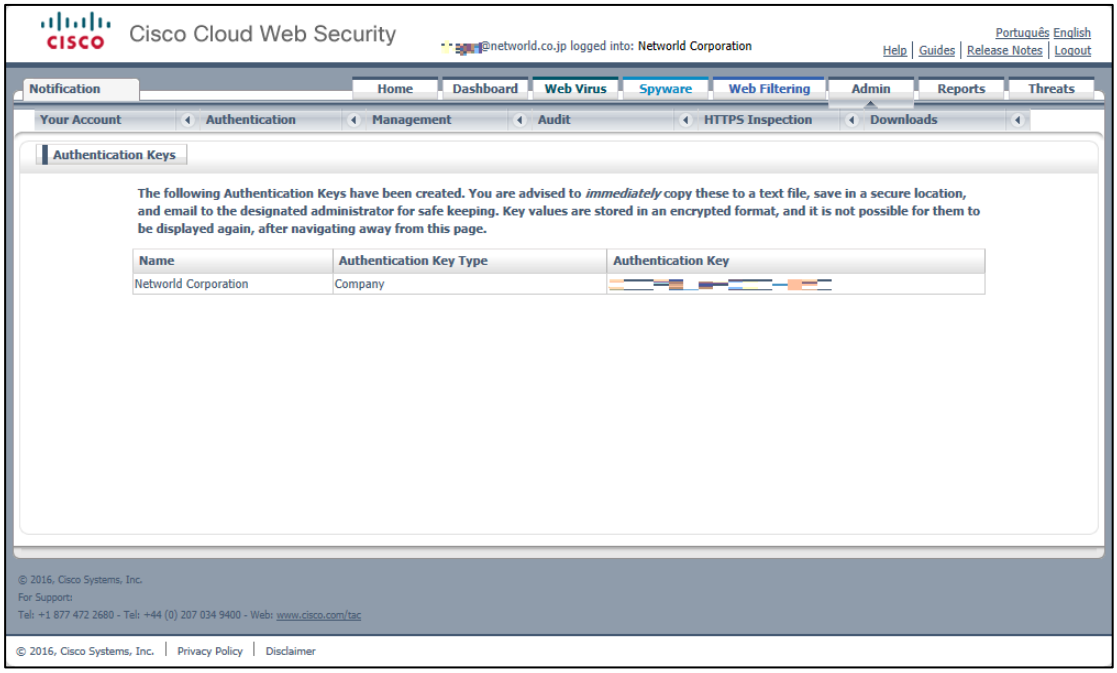


図 50 会社キーの確認（初回）

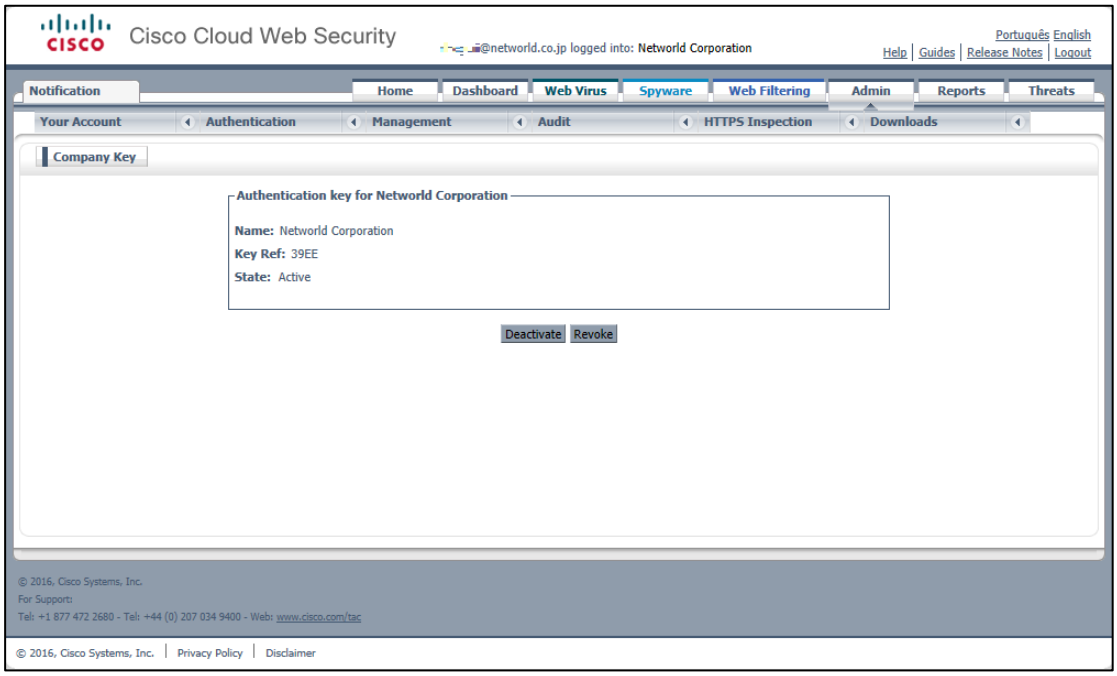


図 51 会社キーの確認（2 回目以降）

4. Cisco 841M Jの設定手順

Cisco 841M Jシリーズの CWS Connectorの初期セットアップを実行します。

4.1 ゾーンの設定

既定の WANゾーンと LANゾーンに、CWSで使用するインターフェースを割り当てます。ゾーンはポリシーの前提条件で、ポリシーはゾーンのペアに対して適用されます。製品に接続されたホストが CWS Connectorによって CWSにリダイレクトされるためには、CWSで使用するインターフェースが所属するゾーンに対して、接続を許可するポリシーを設定する必要があります。ゾーンに対してポリシーが割り当てられていない場合、既定ですべてのトラフィックが破棄（Drop）されます。

4.1.1 WANゾーンの設定

既定の WANゾーンに、CWSで使用する WAN側インターフェースを割り当てます。

(1) インターフェースの設定画面に移動します。「インターフェイスと接続」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「インターフェイス」ボタンをクリックしてください。

図 52 CCP Express のホーム（インターフェイスと接続）

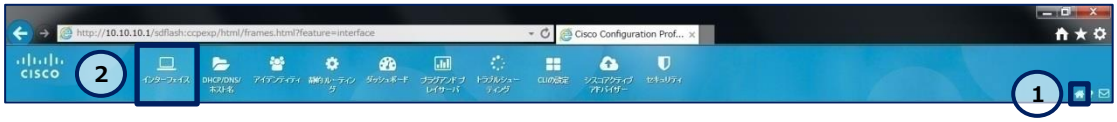


図 53 CCP Express のショートカット（ホームとインターフェイス）

(2) WAN 側インターフェースを編集します。「GigabitEthernet0/4」ラベル内の「編集」ボタンをクリックします。

図 54 インターフェイスの編集

(3) WAN 側インターフェースを既定の WAN ゾーンに割り当てます。「WAN ゾーンに移動」チェックボックスにチェックを入れます。「はい」ボタンをクリックします。この設定はプライマリ WAN インターフェースの既定の設定のため、ほとんどの場合、当該インターフェースはすでに WAN ゾーンに割り当てられています。

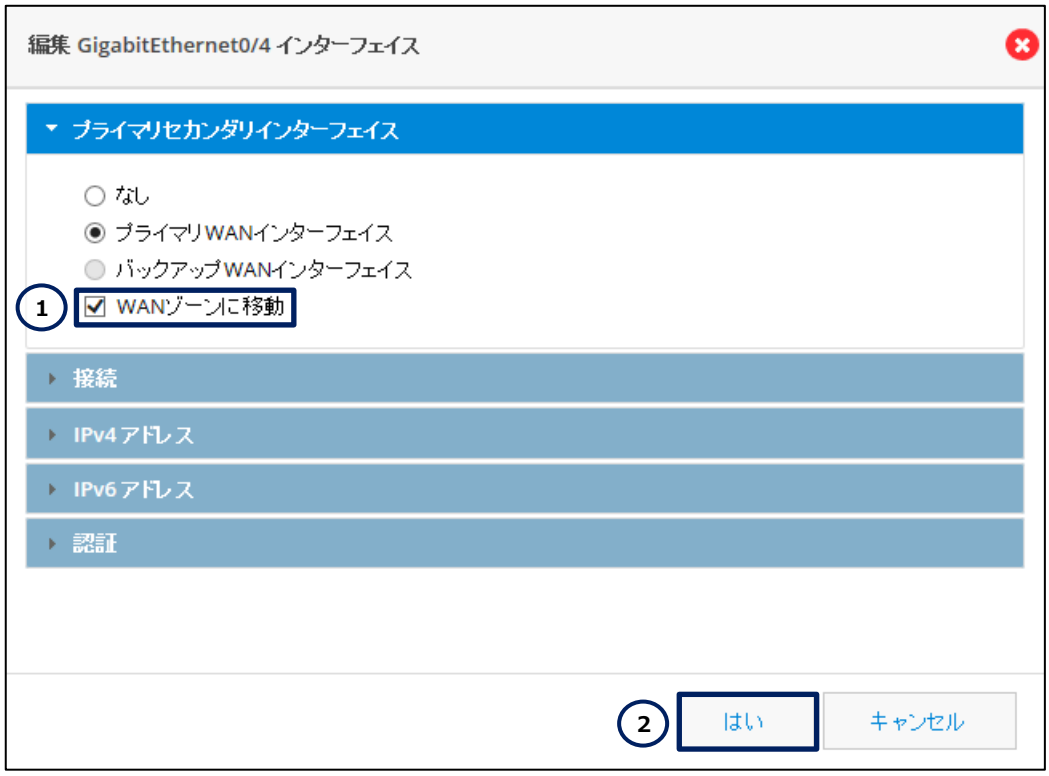


図 55 インターフェイスの編集（詳細）

4.1.2 LAN ゾーンの設定

既定の LAN ゾーンに、CWS で使用する LAN 側インターフェースを割り当てます。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。

図 56 CCP Express のホーム（セキュリティ）

図 57 CCP Express のショートカット（ホームとセキュリティ）

(2) LAN 側インターフェースを既定の LAN ゾーンに割り当てます。「ゾーン」タブをクリックします。「使用可能なインターフェイス」リスト内の「Vlan1」ラベルをドラッグし、「ゾーン LAN」リストにドロップします。「適用する」ボタンをクリックします。この設定は製品の初期セットアップにクイックセットアップウィザードを使用した場合の既定の設定のため、ほとんどの場合、当該インターフェースはすでに LAN ゾーンに割り当てられています。

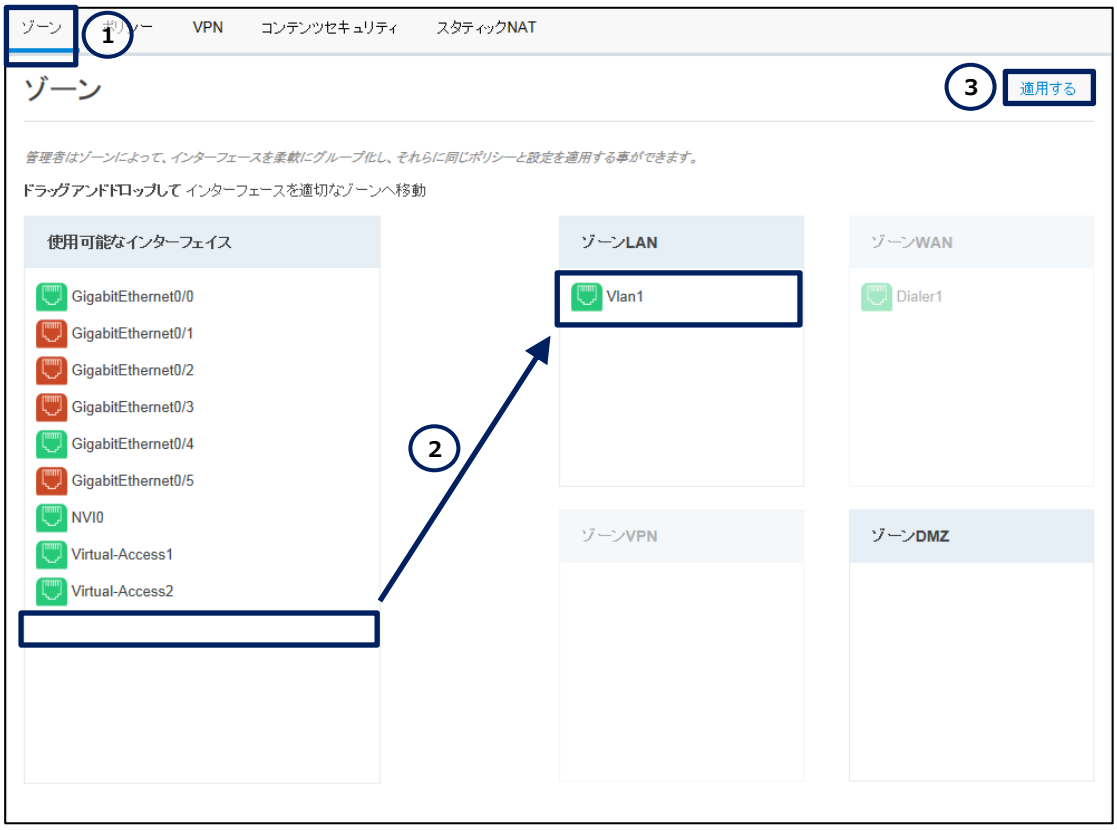


図 58 セキュリティの編集（ゾーン）

4.2 CWS Connector の設定

製品を CWS に接続します。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。

図 59 CCP Express のホーム（セキュリティ）

図 60 CCP Express のショートカット（ホームとセキュリティ）

(2) CWS Connector を設定します。「*」ラベルが記載された設定は、必須の設定です。

① 「コンテンツセキュリティ」タブをクリックします。
② 「クラウド Web セキュリティを有効にする」チェックボックスにチェックを入れます。
③ 「プライマリサーバ」テキストボックスにプライマリータワーの FQDN を入力します。
④ 「セカンダリサーバ」テキストボックスにセカンダリータワーの FQDN を入力します。
⑤ 「暗号化」ラジオボタンで**いいえ**をクリックします。
⑥ 「ライセンス」テキストボックスに CWS ライセンスキーを入力します。
⑦ 「適用」ボタンをクリックします。

図 61 コンテンツセキュリティの編集

4.3 ポリシーの設定

ポートフォワーディングで使用するインターフェースが所属するゾーンに対して、ポリシーを設定します。

4.3.1 LAN-WAN ゾーンのポリシーの設定

既定の LAN ゾーンから既定の WAN ゾーンに向かうゾーンペアに対して、Web トラフィックを許可するポリシーを設定します。

(1) セキュリティの設定画面に移動します。「セキュリティ」ボタンをクリックします。ホーム画面が表示されていない場合は、「ホーム」ボタンをクリックするか、またはショートカットメニューから「セキュリティ」ボタンをクリックしてください。

図 62 CCP Express のホーム（セキュリティ）

図 63 CCP Express のショートカット（ホームとセキュリティ）

(2) ポリシーを追加します。

① 「ポリシー」タブをクリックします。

② 「追加」ボタンをクリックします。

図 64 ポリシーの編集

(3) 既定の LAN ゾーンから既定の WAN ゾーンに向かう Web トラフィックに対する許可ポリシーを設定します。この設定は製品の初期セットアップにクイックセットアップウィザードを使用した場合の既定の設定のため、ほとんどの場合、このポリシーはすでに作成されています。

① 「ポリシー名」テキストボックスにポリシー名を入力します。
② 必要に応じて、「ポリシーの説明」テキストボックスにポリシーの説明を入力します。
③ 「送信元ゾーン」ドロップダウンリストで **LAN** を選択します。
④ 「宛先ゾーン」ドロップダウンリストで **WAN** を選択します。
⑤ 「アクション」ドロップダウンリストで**許可**を選択します。
⑥ 「アプリケーション」タブをクリックします。
⑦ 「利用可能なアプリケーション」リスト内の「http」ラベルをドラッグし、「選択されたアプリケーション」リストにドロップします。
⑧ 「セーブ」ボタンをクリックします。

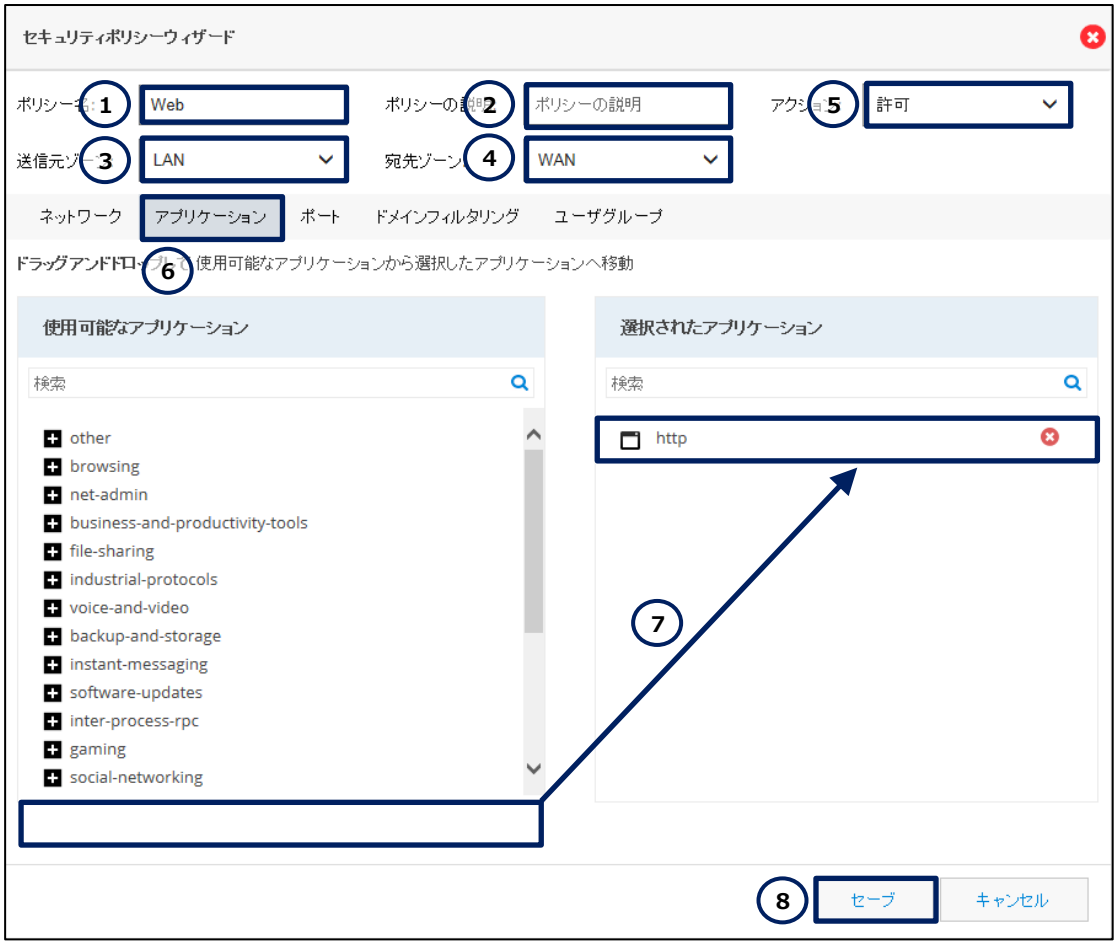


図 65 ポリシーの編集（詳細 – アプリケーション）

5. 動作確認

eicar などのテストウイルスを使用して、Web セキュリティの機能によってアプリケーションが CWS でブロックされること、ユーザー警告が表示されること、アラート通知が電子メールで送信されることなどを確認してください。また、Web ブラウザー等を使用して、ScanCenter で設定したフィルターのとおりにトラフィックが CWS でブロックされること、ユーザー警告が表示されること、アラート通知が電子メールで送信されることなどを確認してください。これらの動作確認を補足する目的で、ScanSafe のトラブルシューティングツールおよび ScanCenter のダッシュボードを使用します。

5.1 ScanSafe のトラブルシューティング

CWS には、接続やポリシーの問題を解決するために、接続診断用の URL と、ポリシー診断用のポリシートレースツールが用意されています。

5.1.1 接続の診断

プライベートネットワークのホストから次の URL に接続することで、CWS への接続性を確認できます。何らかの理由で CWS に正しく接続されていない場合、"User is not currently using the service" が表示されます。

- http://whoami.scansafe.net

表 10 接続に関する診断情報

診断情報	診断情報の意味	備考
authUserName	認証済みユーザー名	
authenticated	認証の成否	
companyName	組織の名前	
connectorVersion	接続を提供している CWS Connector のバージョン	
countryCode	国番号	
externalIP	出力 IP アドレス	
groupNames	ユーザーが所属するグループ	
hash	組織のハッシュ値	
internalIP	入力 IP アドレス	
logicalTowerNumber	現在接続しているタワー	
staticGroupNames	ユーザーが所属するグループの一覧	
userName	ユーザー名	

5.1.2 ポリシーの診断

プライベートネットワークのホストから次の URL に接続することで、現在適用されているポリシーの情報を確認できます。

- http://policytrace.scansafe.net

5.2 ダッシュボード

ダッシュボードを使用して、Web セキュリティと Web フィルタリングのブロック件数を確認します。

5.2.1 Web セキュリティのダッシュボード

ダッシュボードを使用して、Web セキュリティ（マルウェア）または Web セキュリティ（スパイウェア）のブロック件数を確認します。

(1) ダッシュボードの Web セキュリティの概要表示画面に移動します。「Dashboard」タブをクリックします。「Dashboard」ドロップダウンリストから「Spyware Blocks」リストまたは「Web Virus Blocks」リストをクリックします。

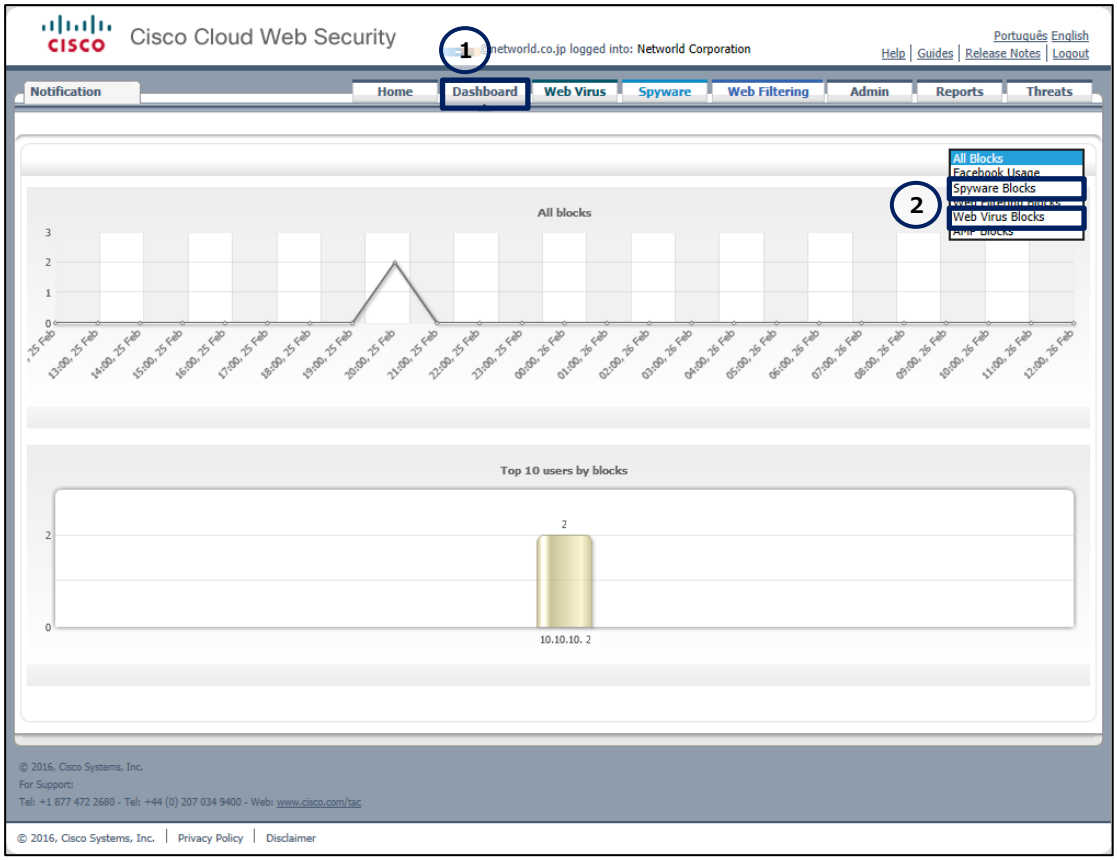


図 66 ダッシュボードの All Blocks 画面

(2) Web セキュリティ機能によって 1 件の Spyware がブロックされたことを確認できます。

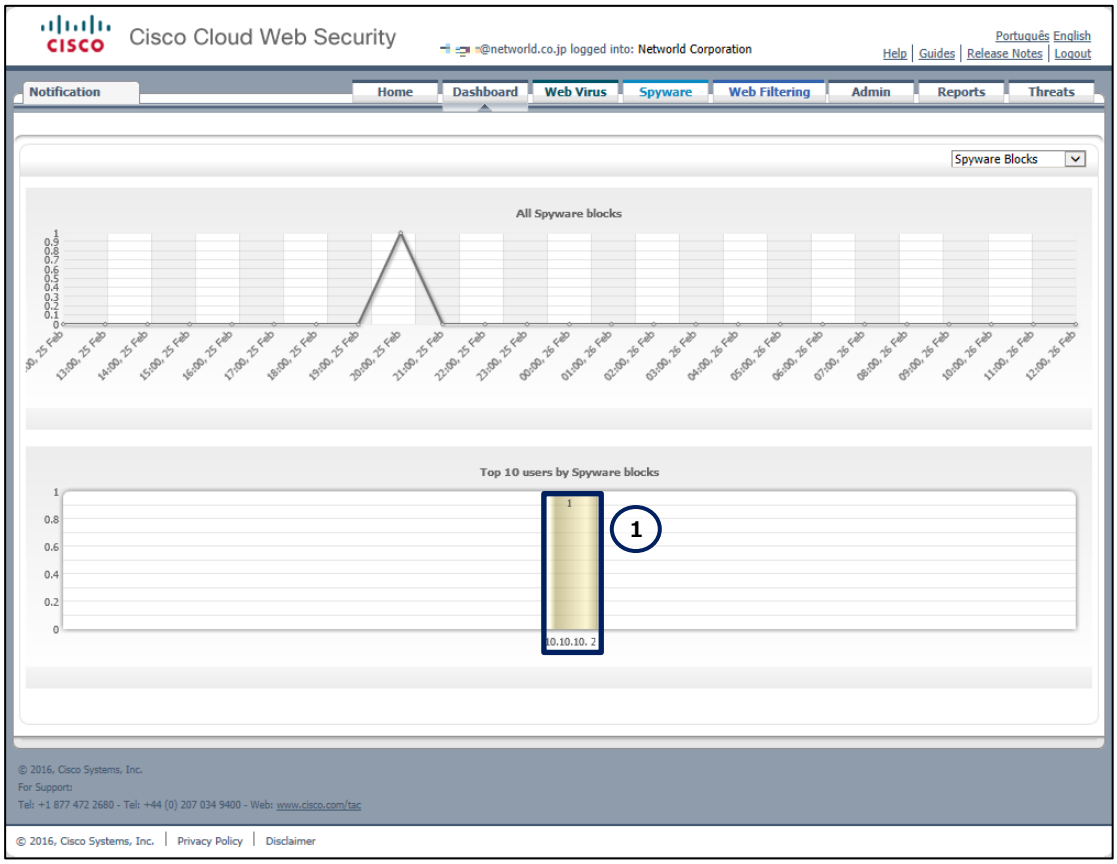


図 67 ダッシュボードの Spyware Blocks 画面

5.2.2 Web フィルタリングのダッシュボード

ダッシュボードを使用して、Web フィルタリングのブロック件数を確認します。

(1) ダッシュボードの Web フィルタリングの概要表示画面に移動します。「Dashboard」タブをクリックします。「Dashboard」ドロップダウンリストから「Web Filtering Blocks」リストをクリックします。

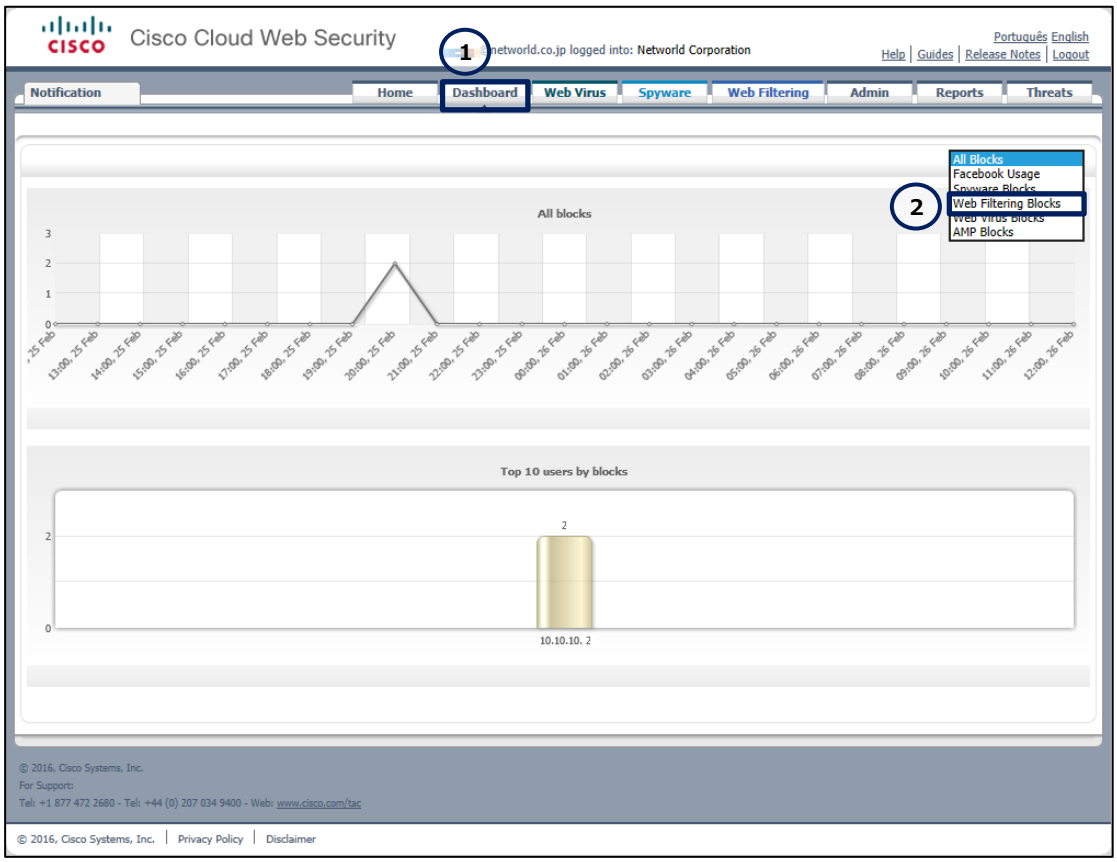


図 68 ダッシュボードの All Blocks 画面

(2) Web フィルタリング機能によって 1 件の Web アクセスがブロックされたことを確認できます。

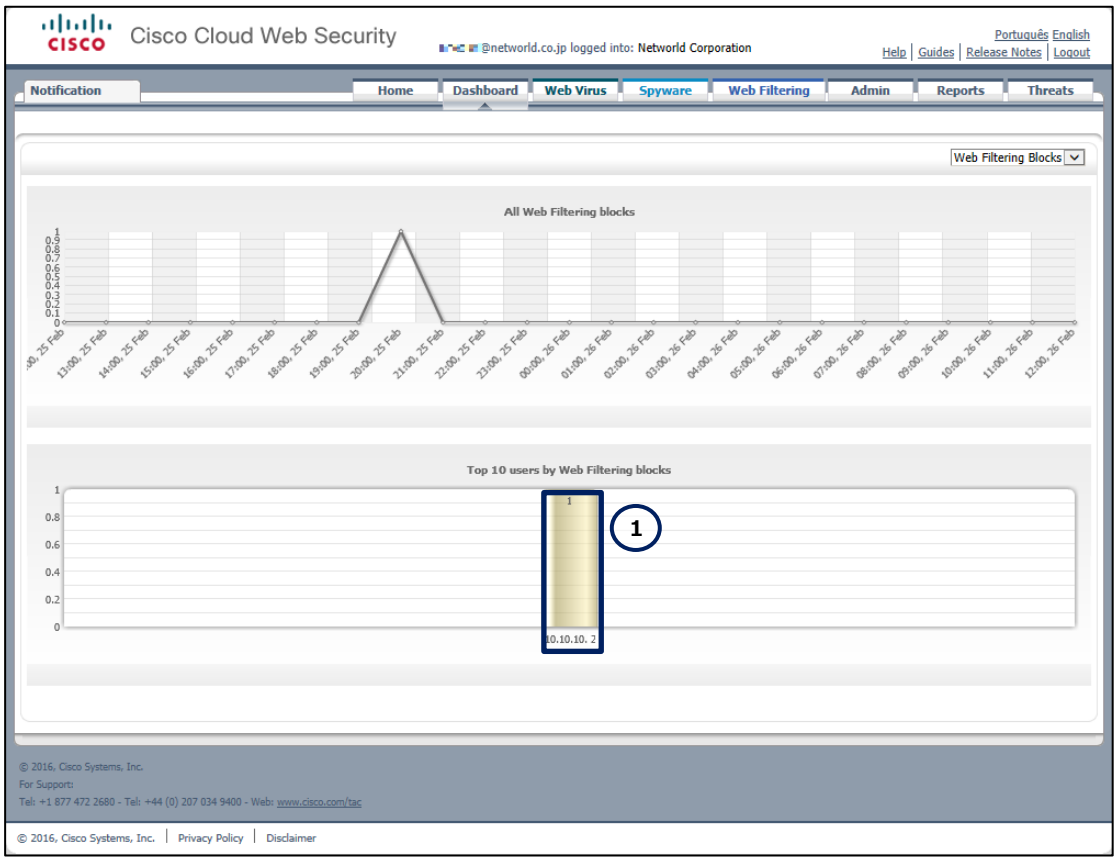


図 69 ダッシュボードの Web Filtering Blocks 画面

6. 設定ファイル

本書で追加または変更される設定（クイックスタートガイドを使用した設定との差分）は、以下のとおりです。

```
001: aaa new-model
002: aaa authentication login local_access local
003: aaa session-id common
004: parameter-map type cws global
005:  server primary name xxxx.scansafe.net port http 8080 https 8080
006:  server secondary name yyyy.cws.sco.cisco.com port http 8080 https 8080
007:  license 0 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
008:  source interface Loopback199
009:  timeout server 10
010:  timeout session-inactivity 100
011:  logging
012:  server on-failure block-all
013: object-group service INTERNAL_UTM_SERVICE
014: object-group network local_cws_net
015:  host 10.1.1.1
016: class-map type inspect match-any INTERNAL_DOMAIN_FILTER
017:  match protocol msnmsgr
018:  match protocol ymsgr
019: zone security VPN
020: zone security DMZ
021: interface Loopback199
022:  ip address 10.1.1.1 255.255.255.255
023:  ip virtual-reassembly in
024: interface Dialer1
025:  ip virtual-reassembly out
026:  cws out
027: ip access-list extended nat-list
028:  permit ip object-group local_cws_net any
029: line con 0
030:  login authentication local_access
031: line vty 0 4
```

```
032: login authentication local_access
```

お問い合わせ

Q　製品のご購入に関するお問い合わせ

https://info-networld.smartseminar.jp/public/application/add/152

Q　ご購入後の製品導入に関するお問い合わせ

弊社担当営業にご連絡ください。

Q　製品の保守に関するお問い合わせ

保守開始案内に記載されている連絡先にご連絡ください。

www.networld.co.jp

株式会社ネットワールド

Networld