Sophos Firewall 評価導入手順書

(ブリッジモード)

(初期設定～インターネット接続まで)

第 3.0 版

本ドキュメントに関する注意事項

このドキュメントは、弊社サービスで使用する一般的な設定を、簡単なステップで構築するための補助資料であり、導入に際して必要な全てのトピックについて網羅・解説することを意図したものではありません。個々のトピックについての詳細は、弊社 Web に公開されておりますユーザガイドやナレッジベース記事をご確認頂くようお願いします。

サービスの仕様は予告なく変更されるため、本ドキュメントに記載した内容と異なる場合がございます。

弊社テクニカルサポートでは、本ドキュメントに関するサポートはいたしません。本ドキュメントに関するご質問は、ご購入前の技術的なお問い合わせ先までご連絡頂くか、該当箇所をマニュアルで確認のうえ、テクニカルサポートまでご質問ください。

- ソフォス株式会社
  https://www.sophos.com/ja-jp.aspx
- Sophos Firewall ユーザーガイド
  https://docs.sophos.com/nsg/sophos-firewall/21.0/help/ja-jp/webhelp/onlinehelp/index.html
- 評価導入手順書・オンラインデモ
  https://news.sophos.com/ja-jp/2022/04/15/japanese-manual/
- ナレッジベース
  https://support.sophos.com/support/s/?language=ja
- ご購入前の技術的なお問い合わせ
  メールアドレス: techjp@sophos.co.jp

評価対象製品バージョン： Sophos Firewall　OS 21.0.0

作成日時	作成担当者	変更内容	改訂版数
2022/4/6	JPSE	新規作成	第 1.0 版
2022/7/19	JPSE	1 部リンク切れを修正	第 2.0 版
2025/1/23	JPSE	SFOS 最新版に対応	第 3.0 版

目次

1 はじめに

このたびは Sophos Firewall をご評価いただきまして誠にありがとうございます。

評価導入における本手順書の位置づけは以下のとおりです。

- **目的: Sophos Firewall を評価導入頂く際、既存ネットワークを大きく変更せずブリッジモードの Sophos Firewall を介してインターネット接続できるまでの初期設定手順をご提供すること。**

本手順書ではシンプルにただ順番に沿って設定を進めて頂くことにより、下記のようなシステム構成環境にて、既存ネットワークを大きく変更せず端末から Sophos Firewall を介してインターネット接続できるようになります。
管理端末には、Windows など Web ブラウザを使用できる PC をご用意ください。
なお、 Sophos Firewall 初期設定時に Sophos Firewall からインターネット接続できることが前提となります。
インターネット接続が無くても初期設定は可能ですが、ライセンスサーバーとの同期ができないため、30 日以内にインターネット接続を行う必要があります。

本手順書により習得できる内容は以下になります。

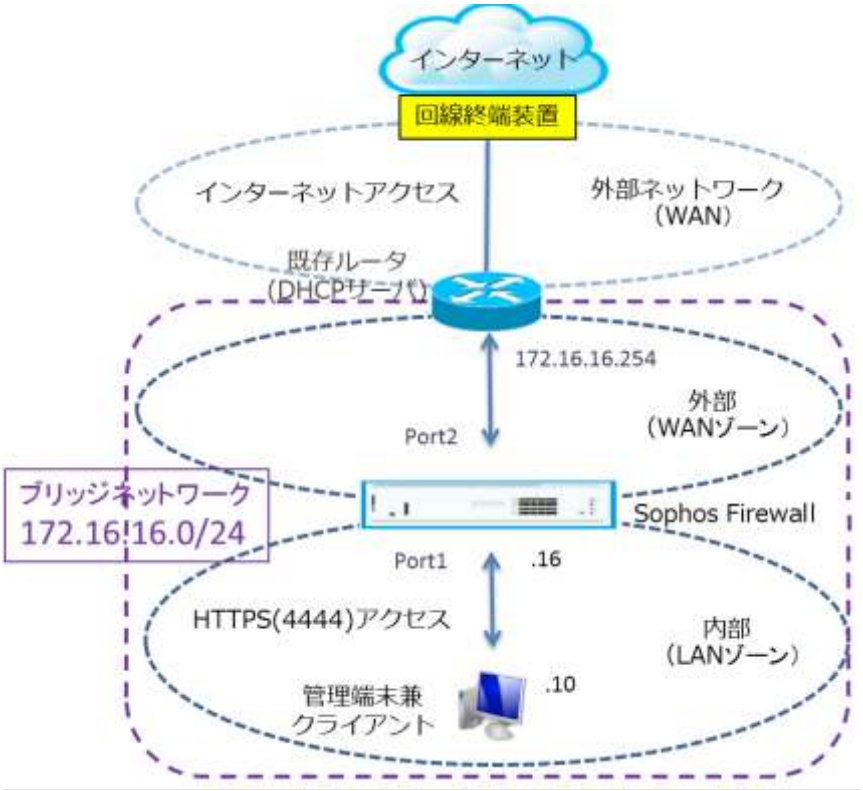
- Sophos Firewall のセキュリティ機能を使用する前に必要になる設定方法。
- 既存ネットワークを大きく変更せずに Sophos Firewall を介してインターネット接続を行うための設定方法。

※1 サブスクリプションにより利用可能となる各種機能の手順について、本書には記載しておりません。必要に応じて、Sophos Firewall ユーザーガイドを参照ください。

※2 Sophos Firewall OS では、Sophos Firewall の設定と管理にグラフィカルユーザーインターフェイスを使用しています。Chrome、Edge、Firefox、Safari など、一般的に使用されているブラウザのほとんどをサポートしています。ブラウザのバージョンは最新のものを使用することをお勧めします。

2 Sophos Firewall の初期設定

Sophos Firewall は工場出荷時の状態で LAN インタフェース（Port1 LAN）に 172.16.16.16/24 の IP アドレスが割り当てられています。次の手順で初期設定を行います。



(1) 管理端末と Sophos Firewall の LAN インタフェース（Port1 LAN）を、既存ルータと Sophos Firewall の WAN インタフェース（Port2 WAN）をそれぞれ LAN ケーブルで接続します。
そうしますと、上記のような構成になります。

(2) 管理端末の IP アドレスを次のように設定します。

IP アドレス	172.16.16.10
サブネットマスク	255.255.255.0
デフォルト ゲートウェイ	172.16.16.16

(3) Sophos Firewall の電源を投入してシステムを起動します。

(4) 管理端末のブラウザを起動して、https://172.16.16.16:4444/ を開きます。

(5) 接続に成功後、SSL の警告画面が表示されますが「172.16.16.16 にアクセスする（安全ではありません）」をクリックしてアクセスします。 （Google Chrome の表示例）

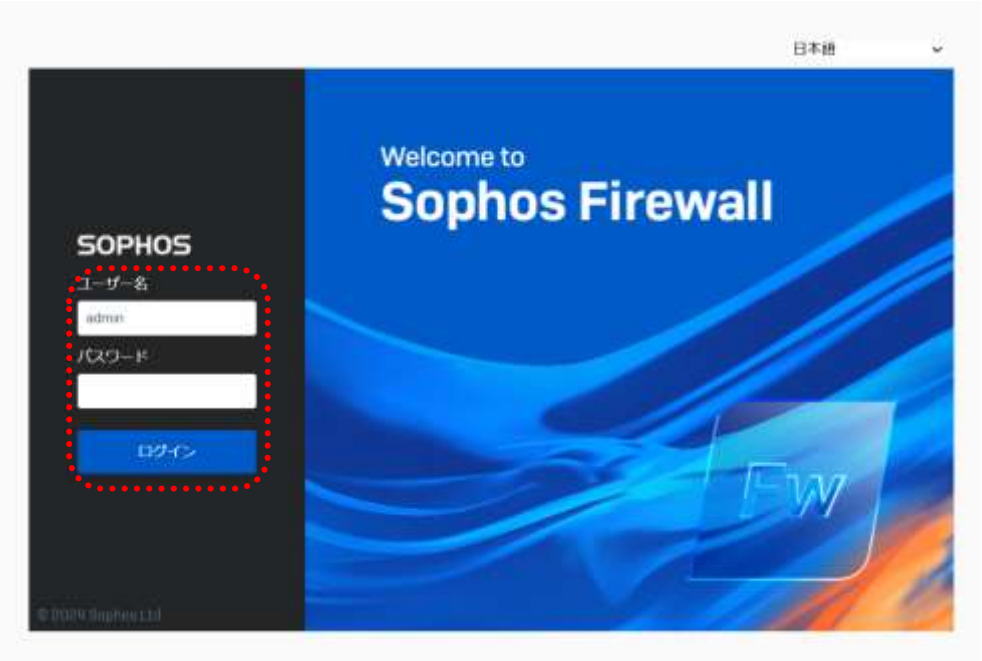
(6) 右上のプルダウンから日本語を選択し、「ソフォスのエンドユーザー利用規約に同意します」にチェックを入れて「セットアップの開始」をクリックします。

(7) 「基本設定」画面にて、管理者パスワードを推奨事項に従って決定してください。また、「設定中に最新のファームウェアを自動的にインストールする」にもチェックを入れてください。

(8) ファームウェアを最新にするため更新が必要な場合があります。（表示されない場合は（9）に進みます）

以下の画面が表示された場合は、画面右下の“更新”をクリックし、ファームウェアの更新、および Sophos Firewall の再起動を実施してください。

Sophos Firewall の再起動後、Sophos Firewall のログイン画面が表示されます。ユーザー名「admin」、パスワードは（7）にて設定したものを入力し、ログインします。



(9) セキュアストレージマスターキーを設定します。パスワードを推奨事項に従って決定してください。入力が完了しましたら、“続行”をクリックします。

(10)ハードウェア版のファイアウォールの場合、「ファイアウォール名」はシリアル番号になります。

タイムゾーンを設定するために地図で日本の上をでクリックしてください。

表示された時間を確認して「続行」をクリックします。

(11) WAN（Port2）の設定を行います。この段階で WAN ネットワークがインターネットに接続していない場合、「手動設定」をクリックして、設定が必要になります。

※既に WAN ポートが DHCP で IP アドレス等を取得している場合、以下の画面は表示されません。（14）まで手順をスキップしてください。

(12) インターフェースの種類で「静的 IP アドレス」を選択、その後各種設定を行います。

(13)設定を確認し「続行」をクリックします。

(14)評価ライセンス登録完了しましたという画面が出ます。

本来ここでライセンスの登録画面が出ますが、評価機は既にライセンス登録がされているので、登録されているライセンス情報が表示されます。

「続行」をクリックして先に進みます。

(15)ゲートウェイを選択で「インターネットゲートウェイ[ブリッジモード]」を選択し、使用するポートを選択します。最後に LAN IP アドレス等を確認して「続行」をクリックします。

(16)保護する項目にチェックを入れて「続行」をクリックします。

(17) 最新のバックアップと通知をメールで受け取るようにメールアドレスと暗号化パスワードを入力し、「続行」をクリックします。

(18) 設定の最終確認を行い、「完了」をクリックします。

(19) 設定変更と Sophos Firewall の再起動が行われます。ここまでの設定が、初期設定で必要な設定です。

3 【任意】DHCP パケットの透過設定

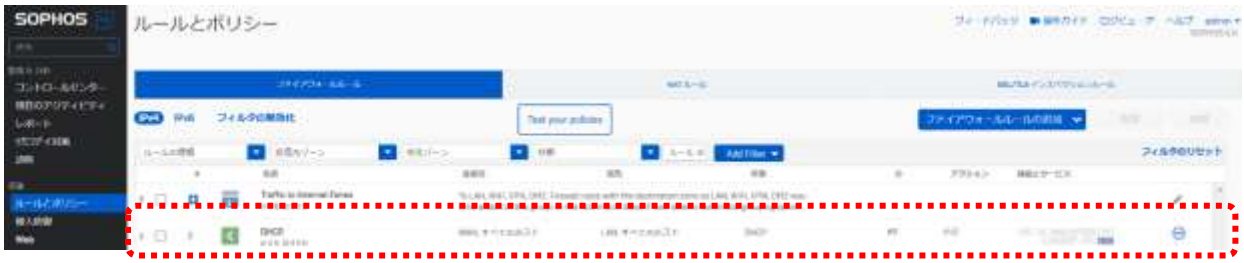
上位ルータが DHCP サーバーになっている時、以下の設定を行うことで DHCP クライアントと通信を行う事が可能になります。

(1) Sophos Firewall の Web Admin Console へユーザー名[admin]、パスワードおよび CAPTCHA コードを入力してログインします。 (パスワードは 2 章[Sophos Firewall の初期設定]の(7)で設定したパスワード)

(2) Web Admin Console で「保護」-「ルールとポリシー」-「ファイアウォールルールの追加」から「新しいファイアウォールルール」をクリックします。

(3) 下記のように設定し、「保存」をクリックします。

(4) 下記のように上記(3)のルールが作成されたことを確認します。



クライアントのネットワーク設定を固定⇒IP 自動取得へ変更し、ipconfig /release、ipconfig /renew コマンドにて、既存ルータより IP アドレス取得できることを確認します。

(5) ブラウザを起動、http://www.yahoo.co.jp へ接続できることを確認します。

4 IPS の設定

初期設定では IPS が少し強めにかかっているため設定を変更します。また、ログを出力しない設定になっているので出力するように設定します。

(1) 「保護」-「侵入防御]」て「IPS ポリシー」をクリックし、IPS 保護を「ON」に設定します。

(2) Web Admin Console で[保護]-[ルールとポリシー]にて、[#Default Network Policy]をクリックします。

(3) 「エクスプロイトの検出・防止（IPS）」で「LAN TO WAN」を選択し、「保存」します。

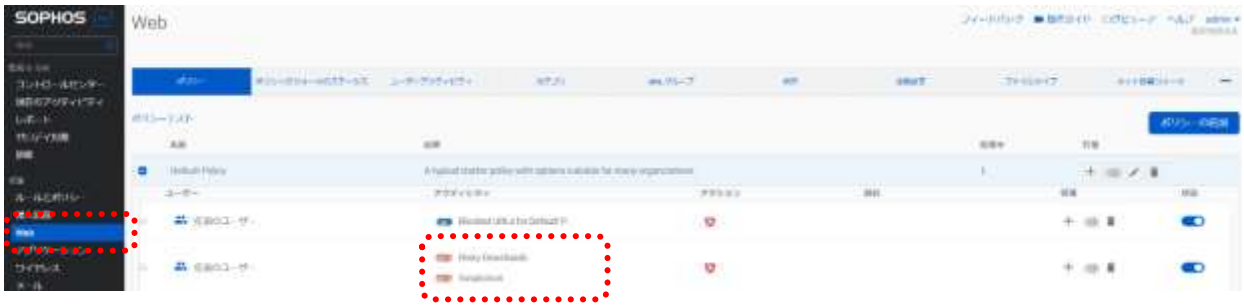
(4) ログの出力を有効にするため、ポリシー設定の上部にある「ファイアウォールのトラフィックのログ」にチェックを入れて、「保存」します。

5 Web フィルタの設定

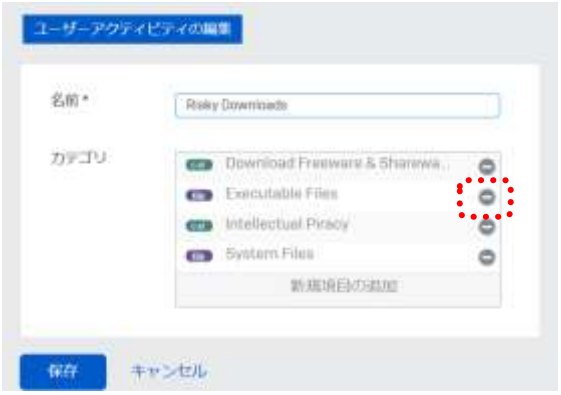
初期設定は[Default Policy]を使用しており、実行ファイルのダウンロードがブロックされてしまいますので、設定変更が必要になります。

実行ファイルのダウンロードを有効にする設定

(1) 「保護」-「Web」にて「Risky Downloads, Suspicious」の上でクリックします。



(2) 「Risky Downloads」の右側の編集マーク（鉛筆）をクリックし、「Executable Files」の右側の削除マーク（⊖）をクリックして「保存」します。



6 SSL/TLS インスペクションの設定

近年 90%以上の通信が暗号化通信を行っており、Sophos Firewall を含む UTM は何もしないと暗号化の中身をチェックできず、暗号化のトンネルを通りエンドポイントまで届く脅威に対応出来ません。SSL/TLS インスペクションは暗号化を一旦紐解いて中身をチェックする機能になります。この機能を有効にするためには下記 2 つの準備が必要となります。

1 SSL/TLS インスペクションのポリシーを作成する

2 Sophos Firewall が発行した SSL 証明書をクライアントにインストールする

6.1SSL/TLS インスペクションのポリシーを作成する

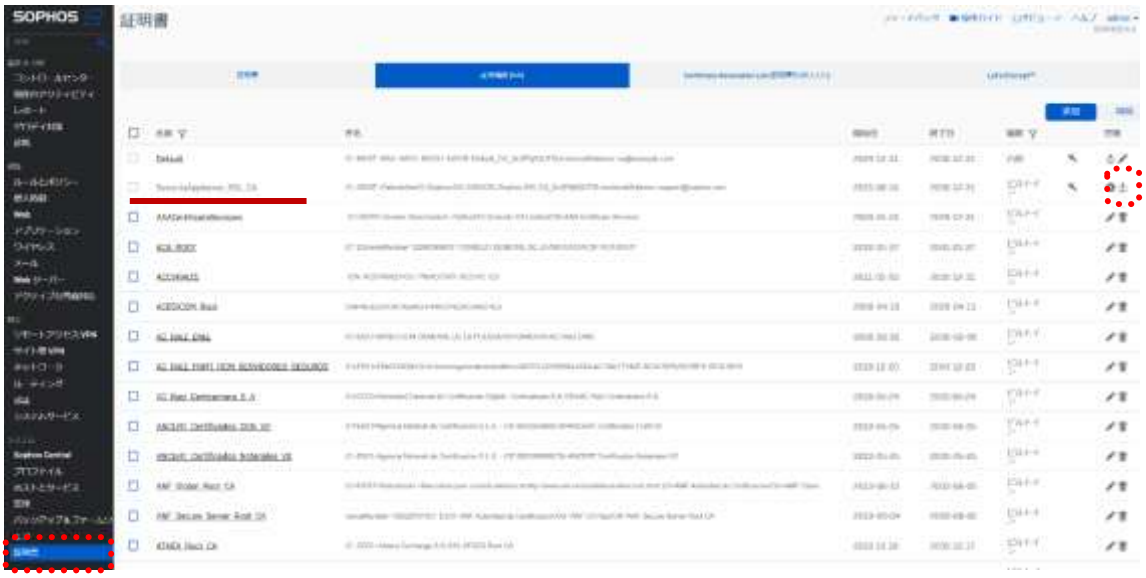
※このポリシーを作成すると、証明書をインストールしていないクライアントでインターネットへ通信を行う時に証明書エラーで Web アクセス等がうまくできなくなりますので、お試し頂く際はご注意ください。

Web Admin Console で「保護」-「ルールとポリシー」にて、SSL/TLS インスペクションのタブをクリックします。次に右上の「追加」をクリックしてポリシーを追加します。

以下のように設定し、「保存」します。

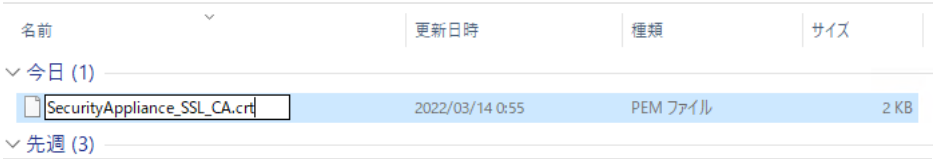
6.2Sophos Firewall が発行した SSL 証明書をクライアントにインストールする

「システム」-「証明書」-「証明書機関[CA]」にて、「SecurityAppliance_SSL_CA」をダウンロードします。



ダウンロードした証明書(.pem 形式)の名前の変更を行い、拡張子を「.crt」に変更します。

※Windows をご使用されている場合、事前に「エクスプローラー」-「表示」にて「ファイル名拡張子」の□ボックスに✓を入れて拡張子を表示できるようにしてください。

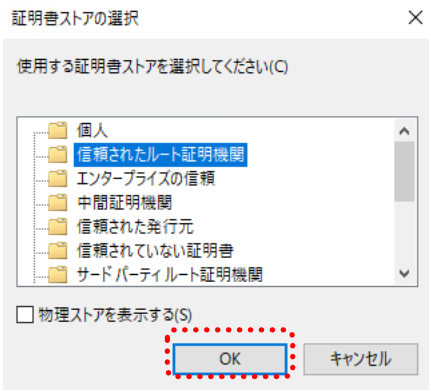


拡張子を変更した証明書を「ダブルクリックして」PC 上で「開く」をクリックします。

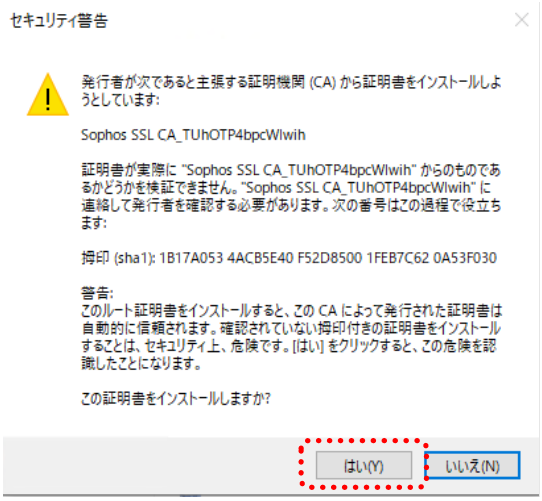
「証明書のインストール」をクリックします。

「現在のユーザー」を選択して「次へ」をクリックします。

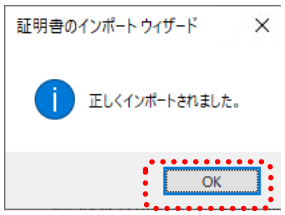
「証明書ストアの選択」で「信頼されたルート証明機関」を選択して「OK」をクリックします。



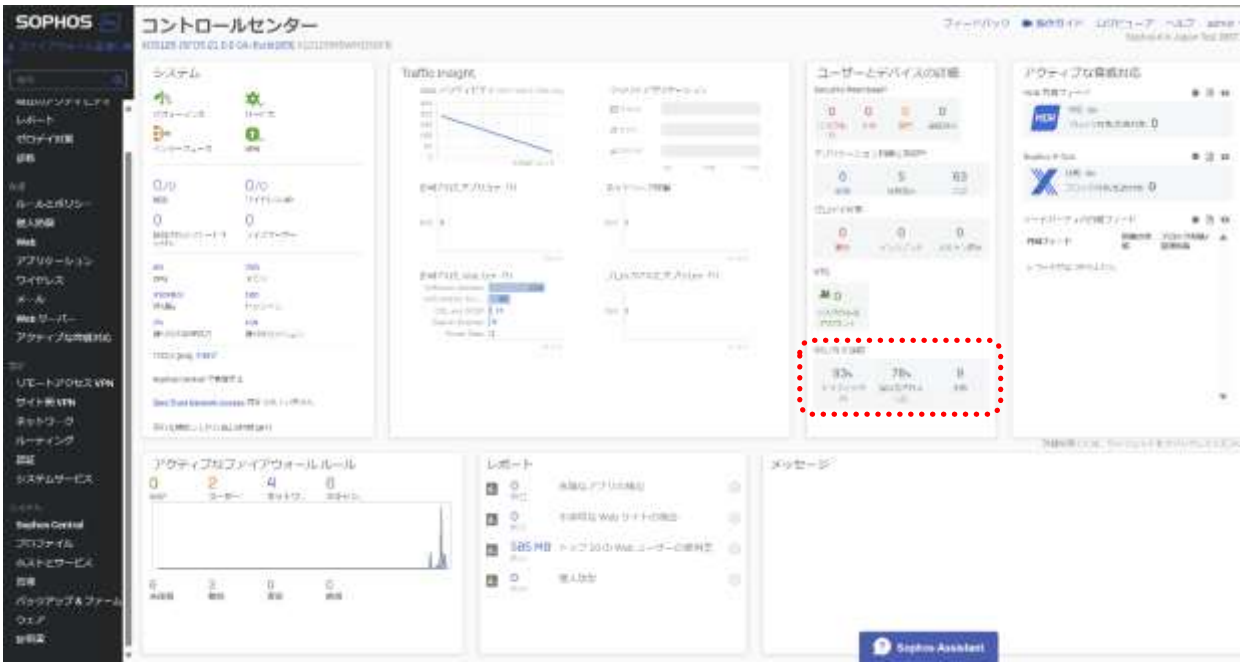
証明書の適用の最後で下記セキュリティ警告が出ますので、「はい」をクリックします。



正しくインポートされましたポップアップが出ますので「OK」をクリックすると、証明書のインストールが完了します。



正しく設定されている場合は、Sophos Firewall のコントロールセンターで SSL 通信が復号化されていることが確認できます。



7 設定手順で不明点がある場合

オンラインヘルプは開いている画面上部のボタンバーにあるアイコンをクリックして開くことができます。現在選択しているメニュー、サブメニューに関するオンラインヘルプ画面が自動的に表示されますが、最新のファームウェアは英語で表記されます。

以上