Sophos Firewall 評価導入手順書

(ルータモード)

(初期設定～インターネット接続まで)

第 2.0 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、一般的な評価環境を簡単なステップで構築するための補助資料です。

導入に際して必要な全てのトピックについての網羅的な解説は意図しておりません。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製品マニュアル、およびレッジベース記事をご確認頂くようお願い致します。尚、弊社テクニカルサポートでは、本ドキュメントについて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、セールスエンジニアリング部にご連絡頂くか、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へご質問ください。

- ソフォス株式会社
  http://www.sophos.com/ja-jp/

評価対象製品バージョン：Sophos Firewall XGS

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

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、を評価導入頂く際、ルータモードの Sophos Firewall を介してインターネット接続できるまでのわかりやすい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、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。

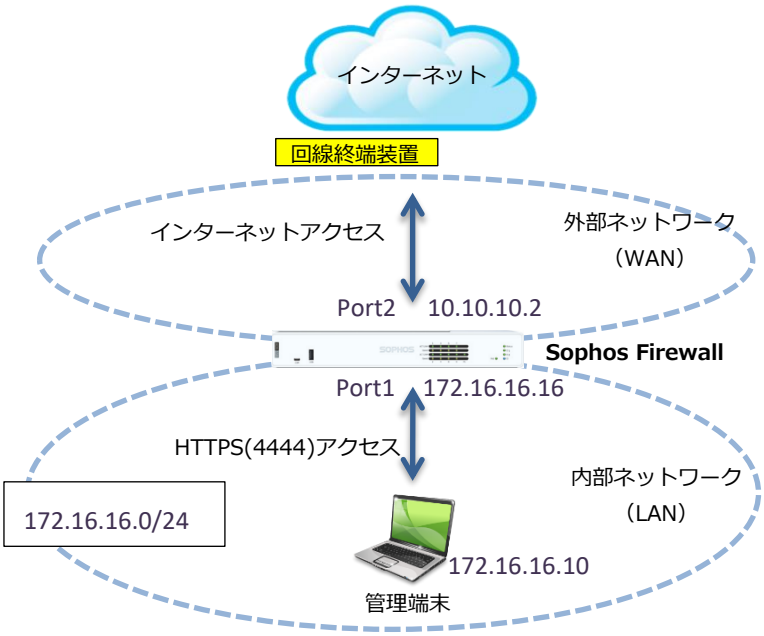
- Sophos Firewall のセキュリティ機能を使用する前に必要になる設定方法。
- Sophos Firewall を介してインターネット接続を行うための設定方法。

※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 評価導入手順書_〇〇編]という各別紙をご参照願います。(※[〇〇]部分に機能を記載しております。)

※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（Web Admin Console）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、「使用許諾契約に同意する」にチェックを入れて「Start Setup」をクリックします。

(7) Admin パスワード設定画面。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。

(9) 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「次へ」をクリックします。

(10)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設定が必要です。なお、PPPoE 接続の場合はウィザード終了後の設定になりますので、(11)までスキップしてください。

※既に WAN ポートが DHCP で IP アドレス等を取得している場合、この画面は表示されませんので、(11)まで手順をスキップしてください。

(11)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。

(12)　設定を確認し「次へ」をクリックします。

(13)　評価ライセンス登録完了しましたという画面が出ます。

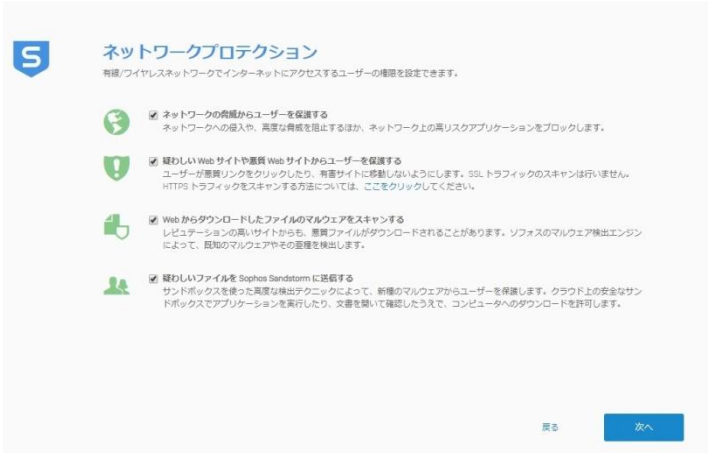
本来ここでライセンスの登録画面が出ますが、評価機は既にライセンス登録がされているので、登録されているライセンス情報が表示されます。「次へ」をクリックして先に進みます。

(14)ゲートウェイを選択で「インターネットゲートウェイ[ルータモード]」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「次へ」をクリックします。

DHCP サーバーとして使う場合、DHCP リース範囲を設定してください。

DHCP サーバーとして使わない場合、DHCP の有効化のチェックを外してください。

(15)　保護する項目にチェックを入れて「次へ」をクリックします。



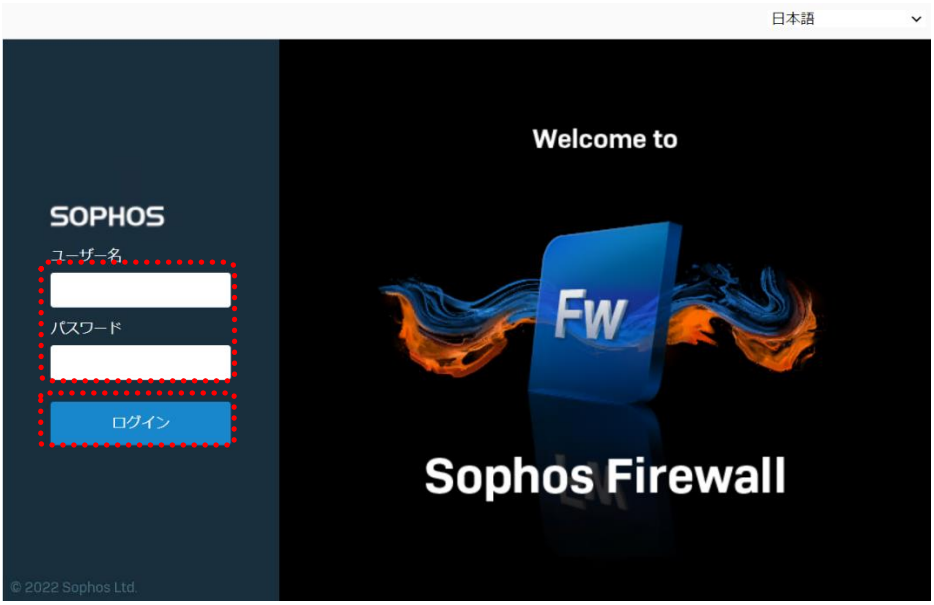
(16)　最新のバックアップと通知をメールで受け取るようにメールアドレスを入力します。

(17)　設定の最終確認を行い、「終了」をクリックします。

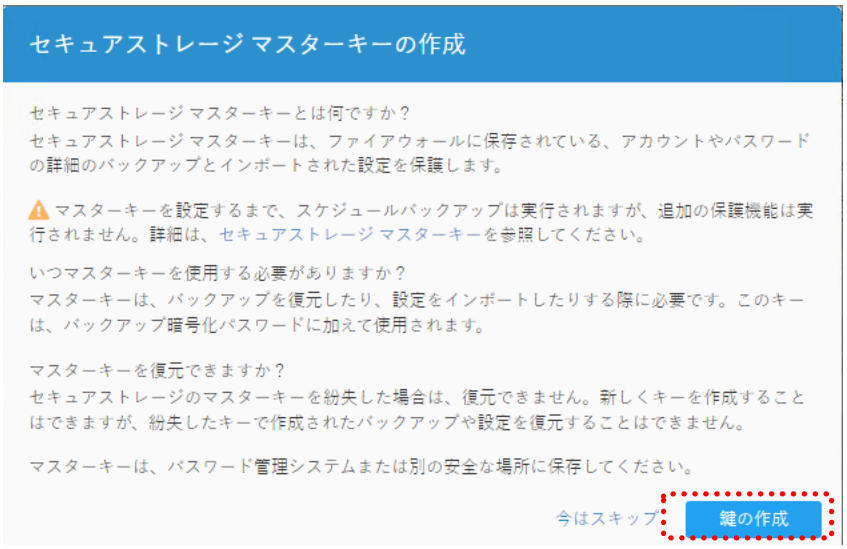
(18)　ファームウェアのダウンロード、設定変更等がシステム上でセットアップされます。

(19)リスタート中です。終わるまで待ちます。（機種にもよりますが、10 分程かかります）

(20)Sophos Firewall のログイン画面が立ち上がってくるので、ユーザー名「admin」、パスワードを入れてログインします。(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)

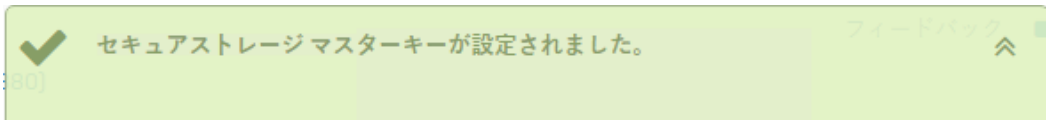


(21)セキュアストレージマスターキーの作成画面が出てくるので、[鍵の作成]をクリックします。



(22)セキュアストレージマスターキーを推奨事項に従って決定し、「鍵の作成」をクリックします。

(23)セキュアストレージマスターキーの設定完了です。



ここまでの設定が、初期設定で必要な設定です。

※PPPoE 回線をご利用の場合は次ページをご参照ください。

PPPoE 回線向け WAN インターフェース設定

PPPoE 回線をご利用の場合、下記設定が必要となります。

「ネットワーク」から「Port2」をクリックします。

ネットワークゾーンが「WAN」であることを確認し、IP の割り当てで「PPPoE(DSL)」を選択、任意のゲートウェイ名を入力し、回線契約時に入手した PPPoE 接続用の「ユーザー名」、「パスワード」を入力します。

次に設定画面の一番下にある「詳細設定」を展開し、MTU 値を設定します。

※MTU・MSS 値は正しく設定されていないと通信不具合などを発生させることがありますので、忘れずに設定してください。なお、推奨 MTU 値は PPPoE 回線によって異なりますので、回線業者にご確認ください。

参考：NTT 東/西日本 フレッツ回線 MTU：1545, MSS:1406

下記のように入力したら「保存」をクリックして PPPoE 設定を完了します。

疎通確認

(1) Sophos Firewall で DHCP サーバーを有効にしているとき

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、Sophos Firewall から IP アドレス取得できることを確認します。

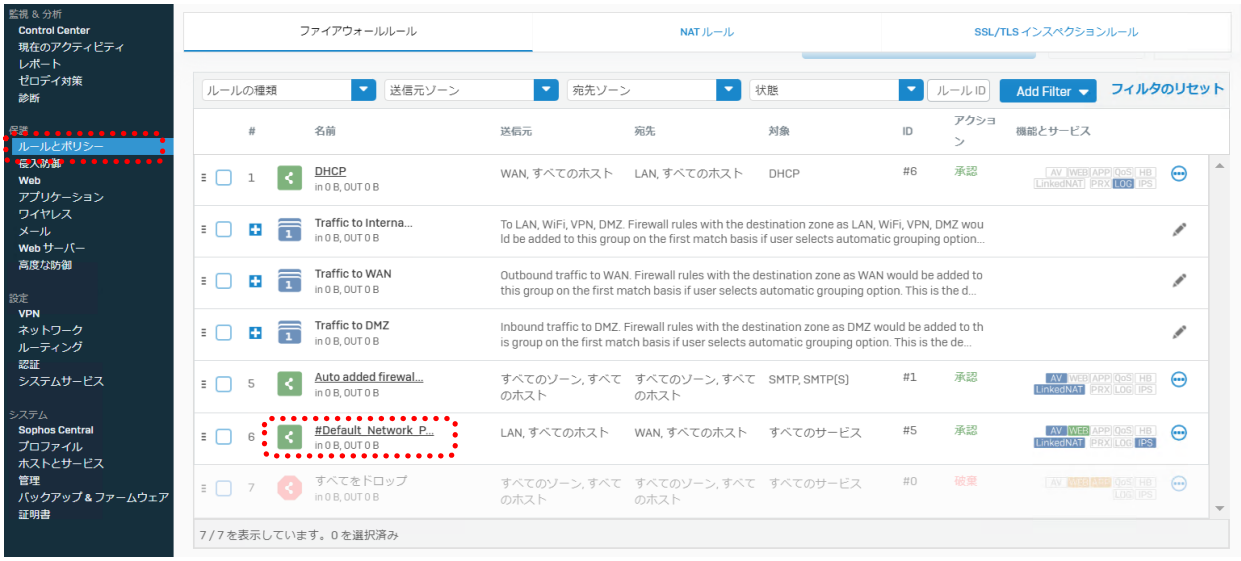
(2) ブラウザを起動、http://www.yahoo.co.jp へ接続できることを確認します。

2 IPS の設定

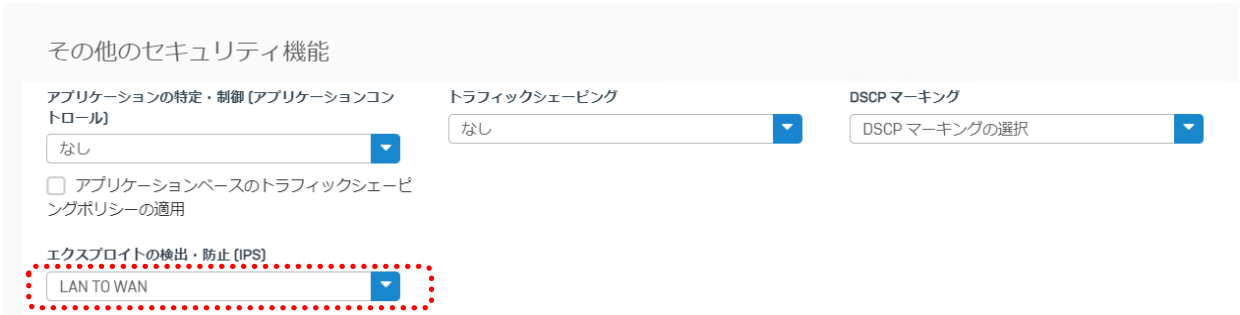
初期設定では IPS が少し強めにかかっているため設定を変更します。また、ログを出力しない設定になっているので出力するように設定します。

(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。



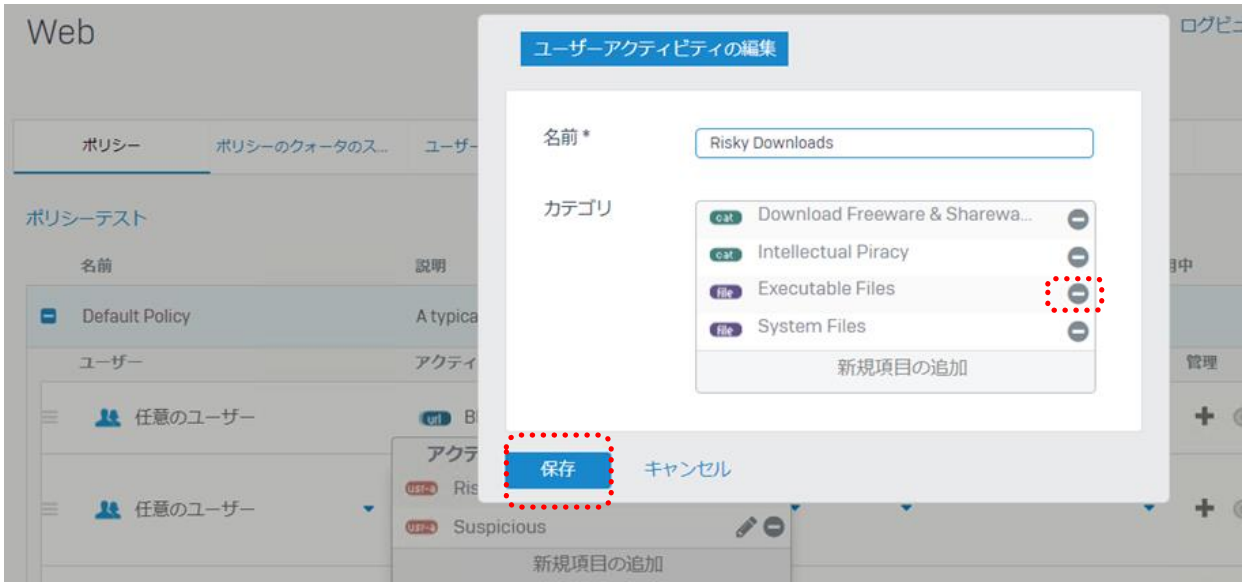
3 Web フィルタの設定

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。



4 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

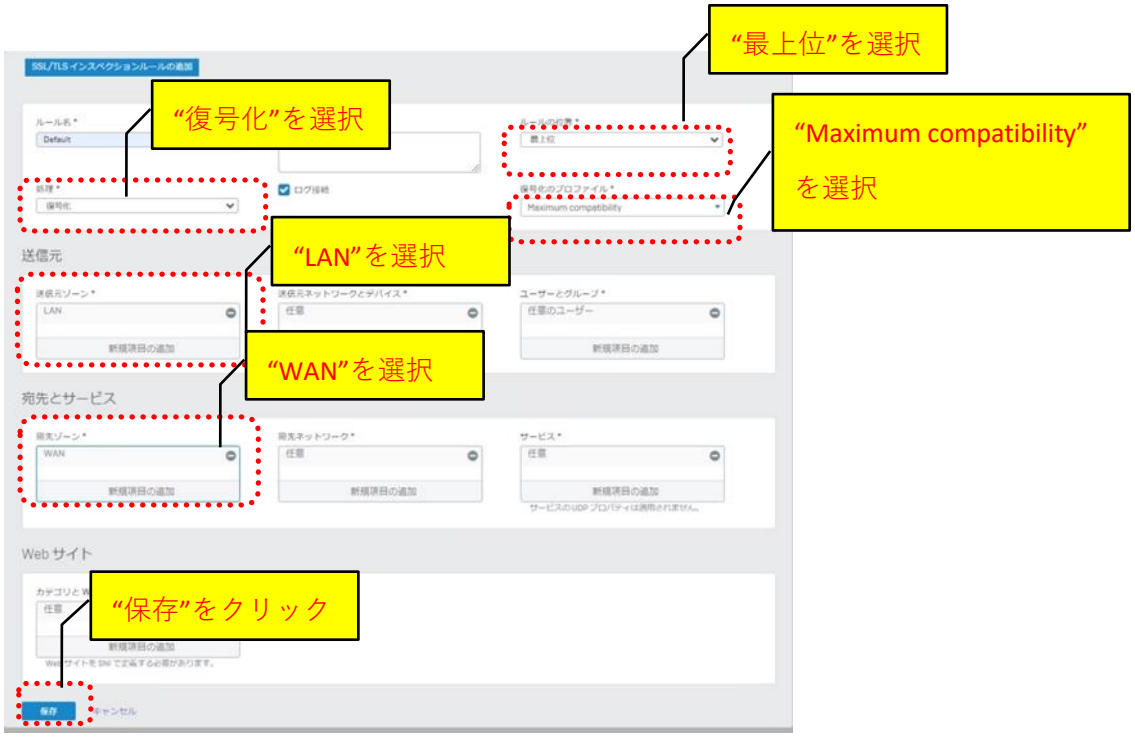
2 Sophos Firewall が発行した SSL 証明書をクライアントにインストールする

4.1 SSL/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。

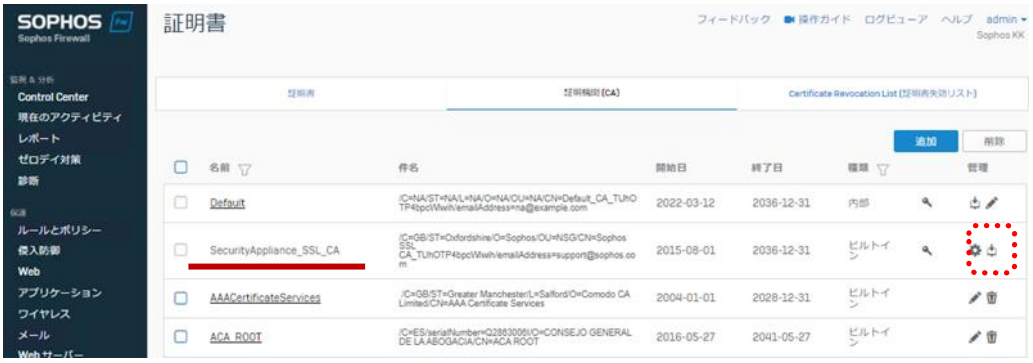
Web Admin Console で[保護]-[ルールとポリシー]にて、SSL/TLS インスペクションのタブをクリックします。次に右上の[追加]をクリックしてポリシーを追加します。

以下のように設定し、「保存」します。



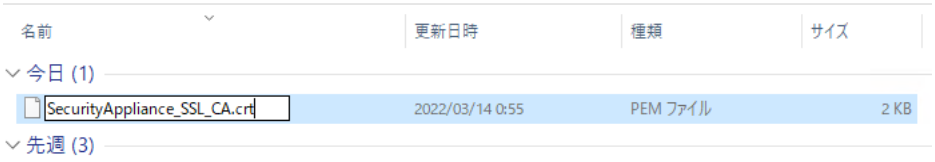
4.2 Sophos Firewall が発行した SSL 証明書をクライアントにインストールする

「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」に変更する

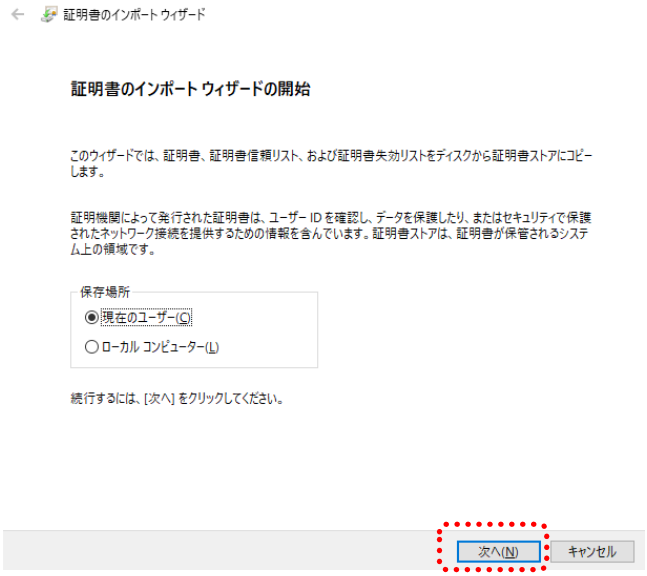
※Windows をご使用されている場合、事前に「エクスプローラー」-「表示」にて「ファイル名拡張子」のロボックスに✓を入れて拡張子を表示できるようにしてください。



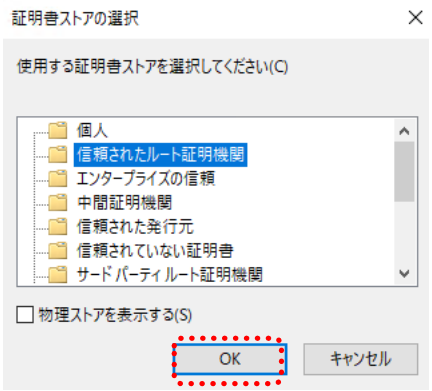
拡張子を変更した証明書を「ダブルクリックして」PC 上で「開く」をクリックします。

「証明書のインストール」をクリックします。

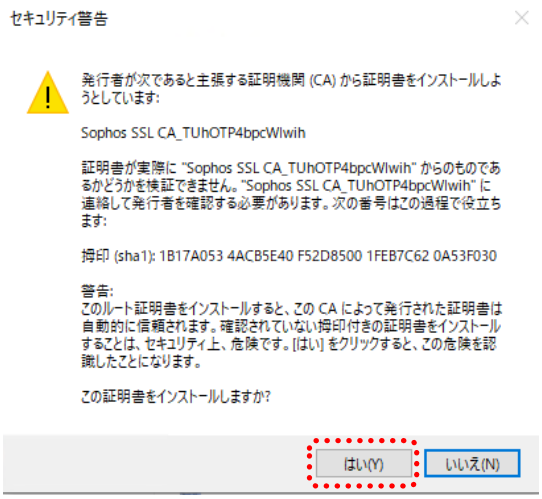
「現在のユーザー」を選択して「次へ」をクリックします。



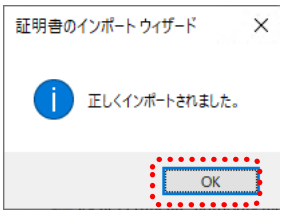
「証明書ストアの選択」で「信頼されたルート証明機関」を選択して「OK」をクリックします。



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。



5 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。