

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/>

Sophos Firewall 評価導入手順書(ルータモード)

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.....	4
2	Sophos Firewall の初期設定.....	5
	PPPoE 回線向け WAN インターフェース設定.....	16
	疎通確認.....	18
3	IPS の設定.....	19
4	Web フィルタの設定.....	20
	実行ファイルのダウンロードを有効にする設定.....	20
5	SSL/TLS インспекションの設定.....	21
	4.1 SSL/TLS インспекションのポリシーを作成する.....	21
	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.....	23
6	設定手順で不明点がある場合.....	27

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。

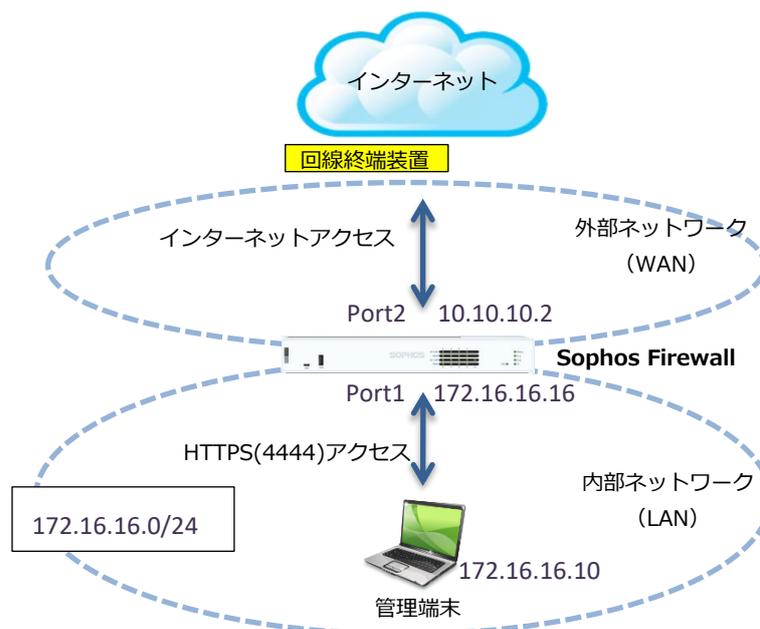
※1 サブスクリプションにより利用可能となる各種機能の手順について、本書には記載しておりません。必要に応じて、【Sophos Firewall 評価導入手順書_〇〇編】という各別紙をご参照願います。(※[〇〇]部分に機能を記載しております。)

※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。

Sophos Firewall 評価導入手順書(ルータモード)

- (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。

Sophos Firewall 評価導入手順書(ルータモード)

- (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。

Sophos Firewall 評価導入手順書(ルータモード)

S **基本設定**

現在のところ、ファイアウォールにログインするには、管理アカウントを使用する必要があります。次に進む前に、パスワードを作成してください。パスワードには文字、数字、記号も混ぜた長いものも設定し、パスワードの強度を高めることをお勧めします。既存の設定も使いたい場合や、HAの既存のファイアウォールに接続したい場合は、以下のオプションを選択してください。

バックアップを復元する

新しい管理アカウントの作成

新しい管理者パスワード:
.....

パスワードの再入力:
.....

推奨事項:

- 10文字
- うち英大文字を1文字以上
- うち英小文字を1文字以上
- うち数字を1文字以上
- うち特殊文字を1文字以上

パスワードの強度:

決定中に、最新のファームウェアを自動的にインストール

戻る **次へ**

(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。

S **ファームウェアの更新 (必須)**

必ずダウンロードして、インストールしてください。

戻る **変更**

(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。

インターネットに接続しました



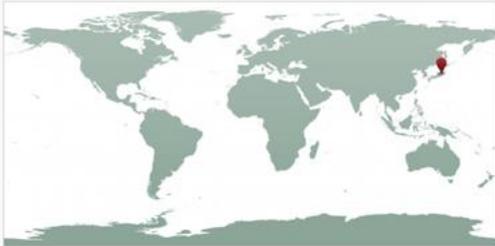
名前とタイムゾーン

ファイアウォール名を入力してください。このデバイスの完全修飾ドメイン名 (FQDN) を使用することを推奨します。

ファイアウォール名

タイムゾーン

地図または下のドロップダウンリストからタイムゾーンを選択してください。
必ず正しいタイムゾーンを選択するようにしてください。イベントのスケジュールや、ログ、レポートに影響します。



Asia/Tokyo

現在の時刻: Monday, September 27, 2021, 12:12 PM

戻る 次へ

Sophos Firewall 評価導入手順書(ルータモード)

(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。

① 「静的 IP アドレス」を選択

手動設定

サービスプロバイダによって特定のインターネット設定が指定されている場合は、ここに入力してください。

設定するポート: Port2

インターフェースの種類: **静的 IP アドレス**

IP アドレス: []

サブネット: /30 [255.255.255.252]

ゲートウェイ名: DHCP_Port2_GW

ゲートウェイの IP アドレス: 128.0.0.1

DNS サーバー-1: 127.0.0.1

DNS サーバー-2: []

アップストリームプロキシの設定

ドメイン名 / DNS アドレス: []

ポート: []

パスワード: []

リセット キャンセル **適用**

② 【例】

IP アドレス : 10.10.10.2

サブネットマスク : 255.255.255.252

ゲートウェイの IP アドレス : 10.10.10.1

DNS サーバー-1 : 8.8.8.8

Sophos Firewall 評価導入手順書(ルータモード)

(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。



Sophos Firewall 評価導入手順書(ルータモード)

(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。



Sophos Firewall 評価導入手順書(ルータモード)

(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。

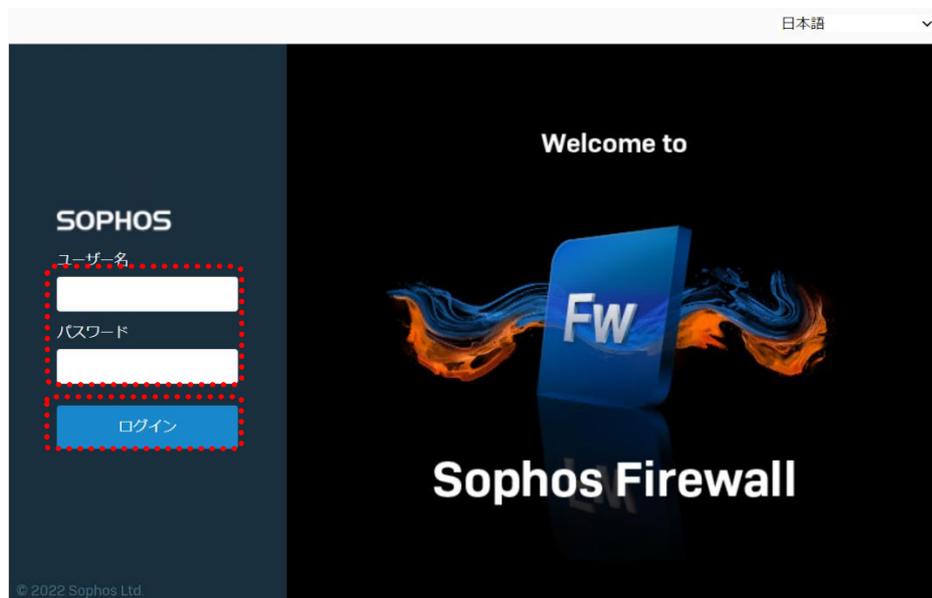


Sophos Firewall 評価導入手順書(ルータモード)

(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)



Sophos Firewall 評価導入手順書(ルータモード)

(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。

セキュアストレージ マスターキーの作成

セキュアストレージ マスターキーとは何ですか？
 セキュアストレージ マスターキーは、ファイアウォールに保存されている、アカウントやパスワードの詳細のバックアップとインポートされた設定を保護します。

⚠ マスターキーを設定するまで、スケジュールバックアップは実行されますが、追加の保護機能は実行されません。詳細は、セキュアストレージ マスターキーを参照してください。

いつマスターキーを使用する必要がありますか？
 マスターキーは、バックアップを復元したり、設定をインポートしたりする際に必要です。このキーは、バックアップ暗号化パスワードに加えて使用されます。

マスターキーを復元できますか？
 セキュアストレージのマスターキーを紛失した場合は、復元できません。新しくキーを作成することはできますが、紛失したキーで作成されたバックアップや設定を復元することはできません。

マスターキーは、パスワード管理システムまたは別の安全な場所に保存してください。

今はスキップ 鍵の作成

(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。

セキュアストレージ マスターキーの作成

マスターキーを作成する前に、マスターキーをパスワード管理システムまたは別の安全な場所に保存できることを確認してください。

⚠ セキュアストレージのマスターキーを紛失した場合は、復元できません。

セキュアストレージ マスターキーの入力

..... 👁

キーの強度: 強い

キーを確認入力します。

.....

複雑性の要件:

- ✔ 最低 12文字
- ✔ うち英大文字を 1文字以上
- ✔ うち英小文字を 1文字以上
- ✔ うち数字 [0-9] を 1文字以上
- ✔ うち特殊文字を 1文字以上

マスターキーをパスワードマネージャ、または別の安全な場所に保存しました

戻る 鍵の作成

(23)セキュアストレージマスターキーの設定完了です。

✔ **セキュアストレージ マスターキーが設定されました。** 👁

ここまでの設定が、初期設定に必要な設定です。

※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。

The screenshot shows the Sophos Firewall web interface. On the left is a navigation menu with categories like '監視 & 分析' (Monitoring & Analysis), '保護' (Protection), '設定' (Configuration), and 'システム' (System). The '設定' menu is expanded, and 'ネットワーク' (Network) is selected. The main content area is titled 'ネットワーク' and contains a table of network interfaces. The 'Port2' interface is highlighted with a red dashed box. The table columns are 'インターフェース' (Interface), 'ステータス/インターフェース速度' (Status/Interface Speed), and 'IP アドレス' (IP Address).

インターフェース	ステータス/インターフェース速度	IP アドレス
GuestAP WiFi ワイヤレスプロテクション	未接続 自動ネゴシエーション	10.255.0.1/255.255.255.0 スタティック
Port1 LAN 物理	接続済み 1000 Mbps - Full Duplex 自動ネゴシエーション	172.16.16.16/255.255.255.0 スタティック
Port2 未設定 物理	無効 自動ネゴシエーション	該当なし
Port3 未設定 物理	無効 自動ネゴシエーション	該当なし
Port4 未設定 物理	無効 自動ネゴシエーション	該当なし

Sophos Firewall 評価導入手順書(ルータモード)

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。

The screenshot shows the 'ネットワーク' (Network) configuration page. The 'WAN リンクマネージャ' (WAN Link Manager) tab is active. Under '全般設定' (General Settings), the following fields are visible:

- 名前*: Port2
- ハードウェア: Port2
- ネットワークゾーン: WAN (highlighted with a red dotted box)
- IPv4 設定
- IPの割り当て: スタティック PPPoE (DSL) DHCP (highlighted with a red dotted box)
- IPv4/ネットマスク: /24 (255.255.255.0)
- 推奨IP: (empty)
- ゲートウェイの詳細 (expanded):
 - ゲートウェイ名*: GW1 (highlighted with a red dotted box)
 - ゲートウェイIP: (empty)
 - ユーザー名*: kkhdppouep (highlighted with a red dotted box)
 - パスワード*: (masked with dots, highlighted with a red dotted box)

Buttons at the bottom: 保存 (Save), 接続 (Apply), キャンセル (Cancel).

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。

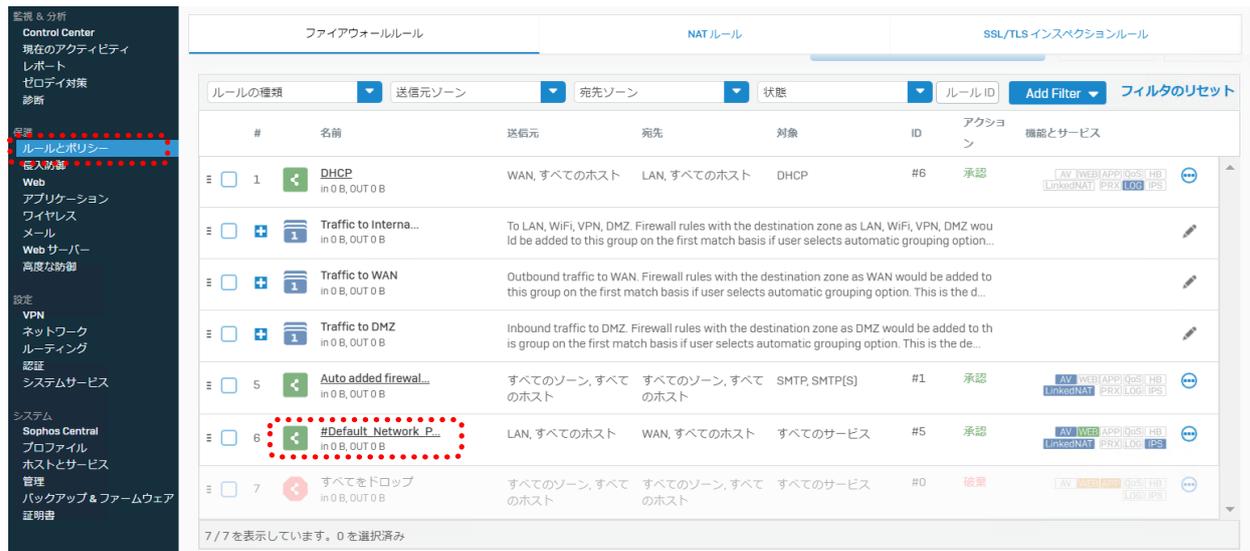
2 IPS の設定

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。

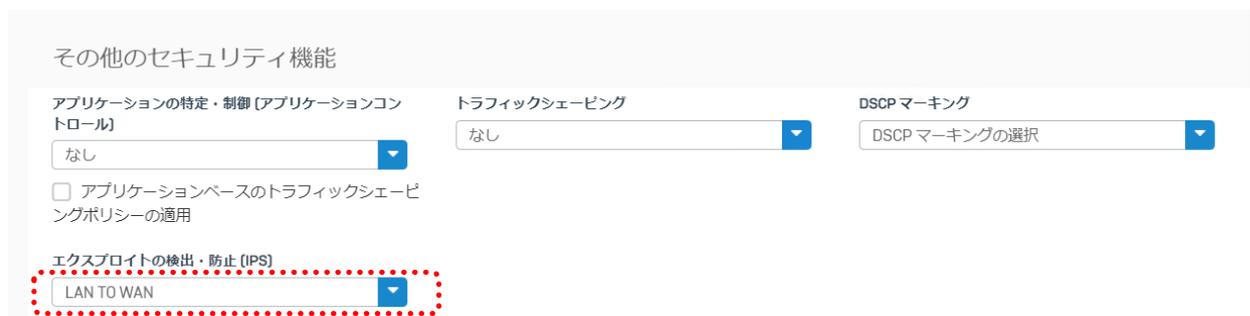
(1) 「保護」 - 「侵入防御」で「IPS ポリシー」をクリックし、IPS 保護を「ON」に設定します。



(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。

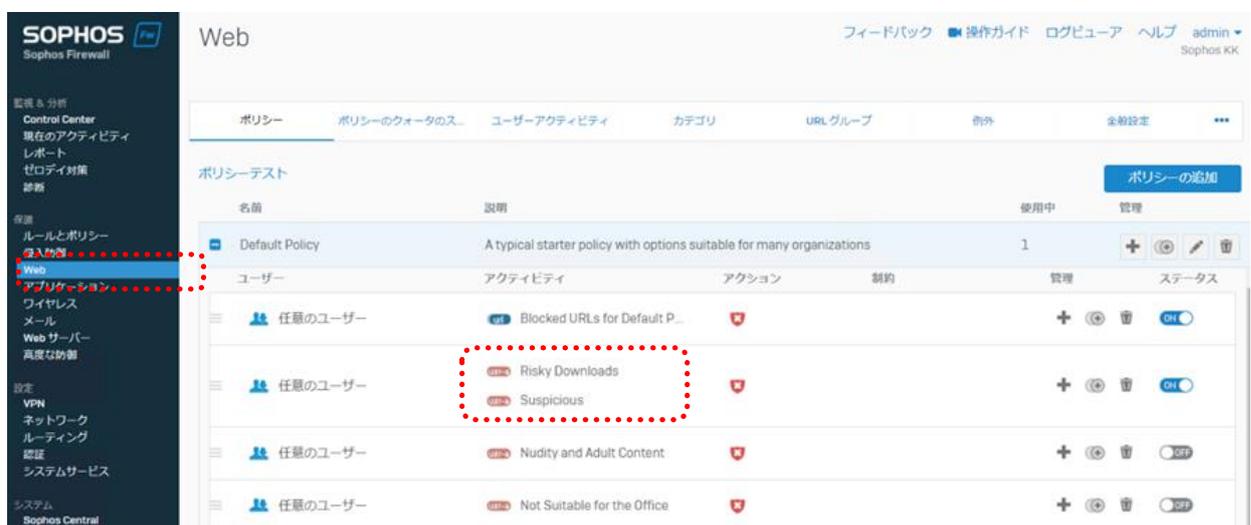


3 Web フィルタの設定

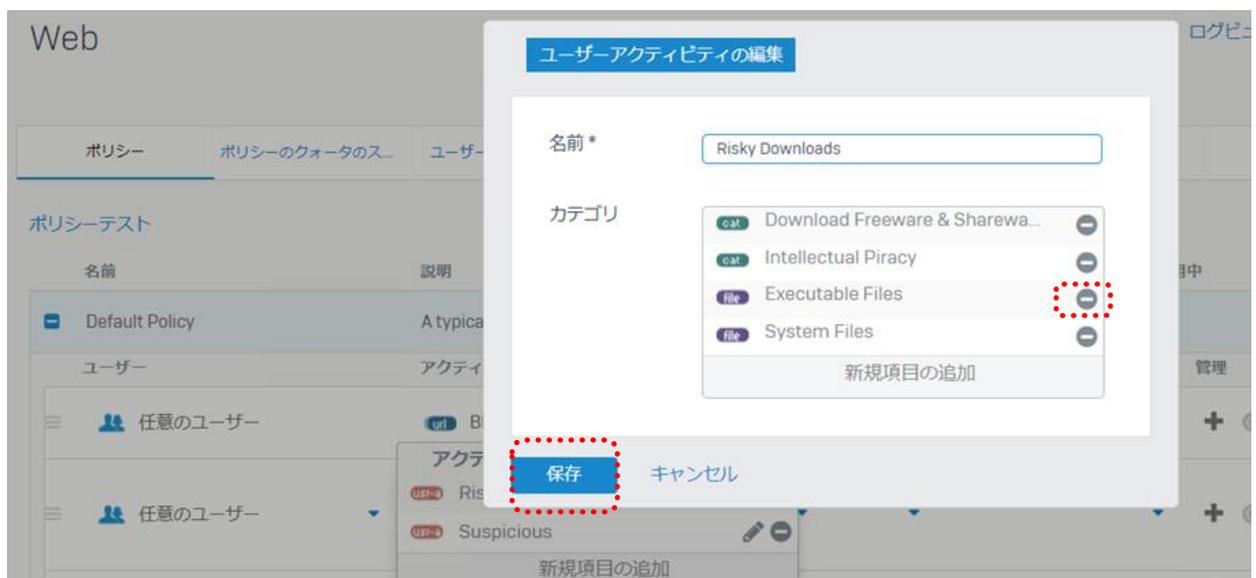
初期設定は[Default Policy]を使用しており、実行ファイルのダウンロードがブロックされてしまいますので、設定変更が必要になります。

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спек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спек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спек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спек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спек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。

The screenshot shows the 'Rules and Policies' configuration page in the Sophos Firewall Web Admin Console. The 'SSL/TLS Inspection Rules' tab is selected and highlighted with a red dashed box. The 'Add' button is also highlighted with a red dashed box. The left sidebar shows 'Rules and Policies' selected. Below the tabs, there are dropdown menus for 'Source Zone' and 'Destination Zone', and a 'Rule ID' field. A table lists existing rules, including one named 'Exclusions by website'.

ID	名前	送信元	宛先	対象	プロファイル	アクション	管理
1	Exclusions by website in S, Out O S	すべてのゾーン、すべてのホスト、任意の...	すべてのゾーン、すべてのホスト	Local TLS exclusion list, Manag...	Maximum competi...	復号化しない	

Sophos Firewall 評価導入手順書(ルータモード)

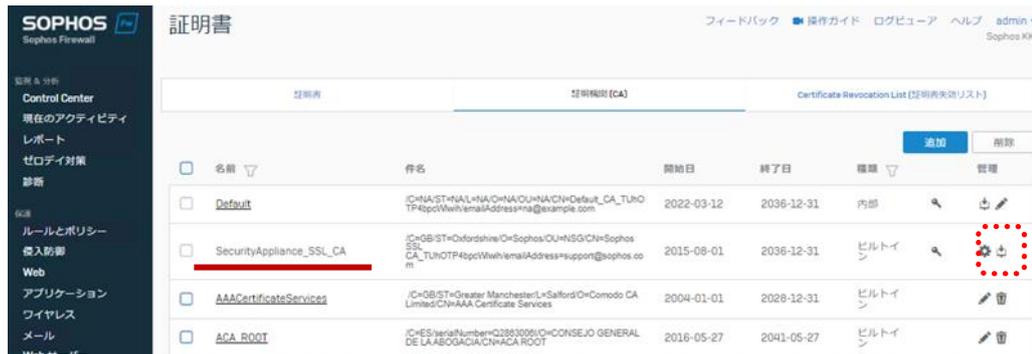
以下のように設定し、「保存」します。

The screenshot shows the configuration page for an SSL/TLS inspection rule. The following settings are highlighted with red dashed boxes and annotated with yellow callout boxes:

- ルール名:** Default (Annotated: "復号化"を選択)
- 動作:** 復号化 (Annotated: "復号化"を選択)
- ログ保持:** (Annotated: "最上位"を選択)
- 動作の互換性レベル:** Maximum compatibility (Annotated: "Maximum compatibility"を選択)
- 送信元:** LAN (Annotated: "LAN"を選択)
- 送信元ゾーン:** LAN (Annotated: "LAN"を選択)
- 送信元ネットワークとデバイス:** 任意 (Annotated: "WAN"を選択)
- 宛先とサービス:** WAN (Annotated: "WAN"を選択)
- 宛先ネットワーク:** 任意 (Annotated: "WAN"を選択)
- サービス:** 任意 (Annotated: "WAN"を選択)
- Web サイト:** 任意 (Annotated: "保存"をクリック)
- 保存ボタン:** 保存 (Annotated: "保存"をクリック)

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」のロボツクスに✓を入れて拡張子を表示できるようにしてください。



Sophos Firewall 評価導入手順書(ルータモード)

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。



Sophos Firewall 評価導入手順書(ルータモード)

「現在のユーザー」を選択して「次へ」をクリックします。

← 証明書のインポートウィザード

証明書のインポートウィザードの開始

このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。

証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。

保存場所

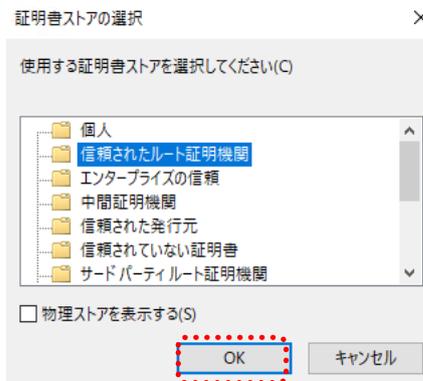
- 現在のユーザー(C)
- ローカル コンピューター(L)

続行するには、[次へ] をクリックしてください。

次へ(N)

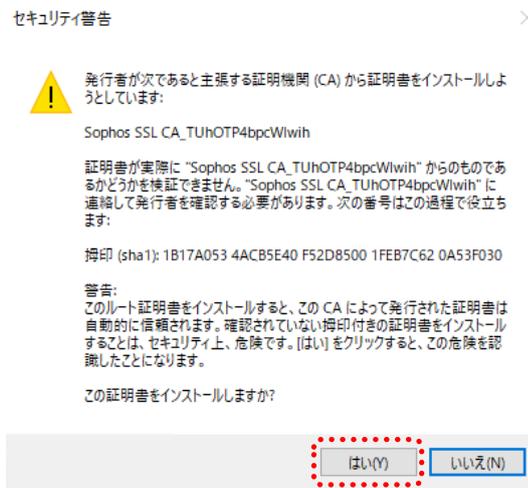
キャンセル

「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。

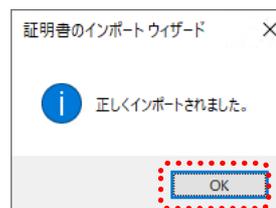


Sophos Firewall 評価導入手順書(ルータモード)

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。

