

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 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

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(ブリッジモード)

評価対象製品バージョン： Sophos Firewall

| 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 |
| 3 | 【任意】 DHCP パケットの透過設定..... | 15 |
| 4 | IPS の設定..... | 18 |
| 5 | Web フィルタの設定..... | 19 |
| | 実行ファイルのダウンロードを有効にする設定..... | 19 |
| 6 | SSL/TLS インспекションの設定..... | 20 |
| 6.1 | SSL/TLS インспекションのポリシーを作成する..... | 20 |
| 6.2 | 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..... | 22 |
| 7 | 設定手順で不明点がある場合..... | 26 |

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、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。

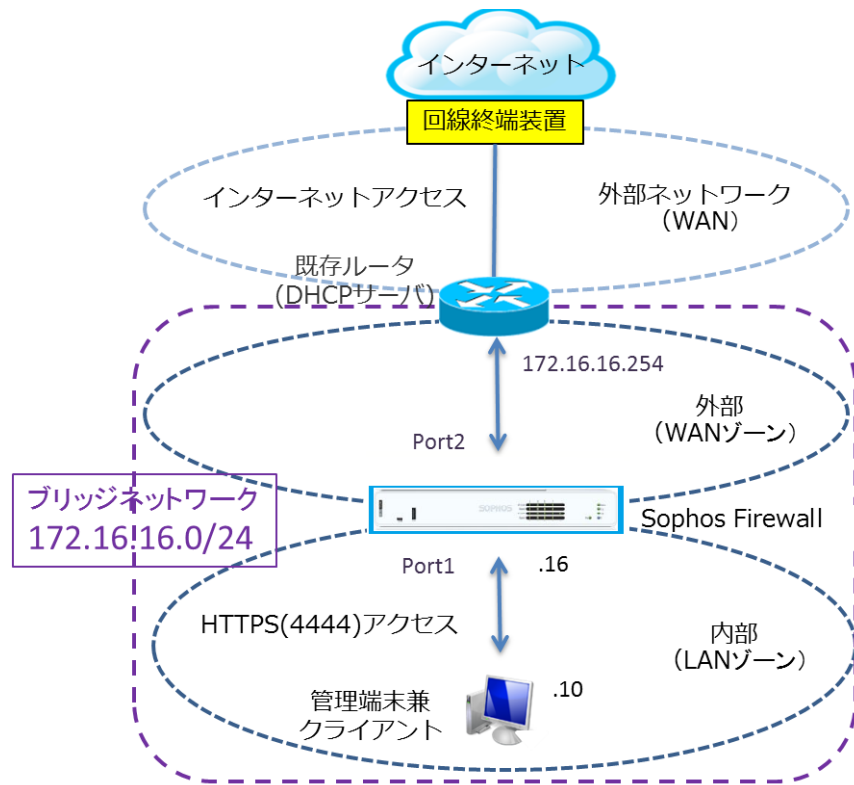
※1 サブスクリプションにより利用可能となる各種機能の手順について、本書には記載しておりません。必要に応じて、[Sophos Firewall 評価導入手順書_〇〇編]という各別紙をご参照願います。(※[〇〇]部分に機能を記載しております。)

※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。

Sophos Firewall 評価導入手順書(ブリッジモード)

- (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) 「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。

Sophos Firewall 評価導入手順書(ブリッジモード)

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、管理員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、記号を混ぜた長いものを設定し、パスワードの強度を高めることもお勧めします。既設の設定を復元したい場合や、HAの既設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](#)

新しい管理員アカウントの作成

新しい管理員パスワード:

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:

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

[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](#) [更新](#)

(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。

Sophos Firewall 評価導入手順書(ブリッジモード)

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) を使用することをお勧めします。

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(ブリッジモード)

(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

② 【例】

IP アドレス : 172.16.16.200

サブネットマスク : 255.255.255.0

ゲートウェイの IP アドレス : 172.16.16.254

DNS サーバー1 : 172.16.16.30

(12)設定を確認し「次へ」をクリックします。

Sophos Firewall 評価導入手順書(ブリッジモード)



(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(ブリッジモード)

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



(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(ブリッジモード)

(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。

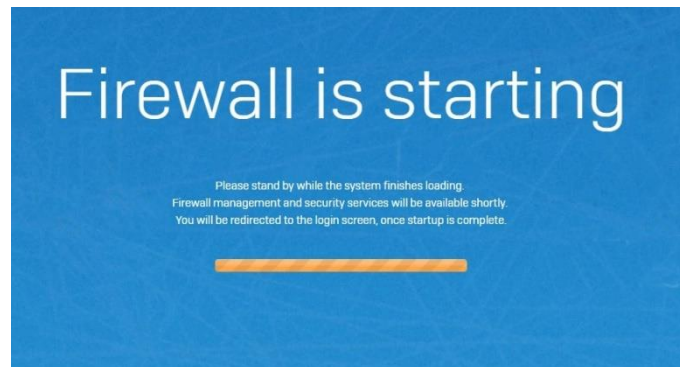
(17) 設定の最終確認を行い、「終了」をクリックします。

(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。

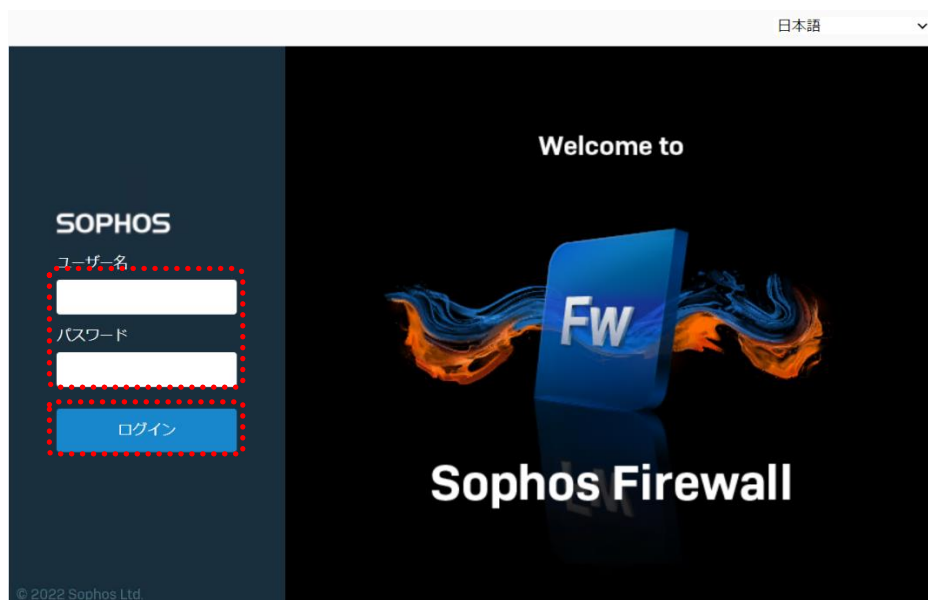


Sophos Firewall 評価導入手順書(ブリッジモード)

(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(ブリッジモード)

(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:

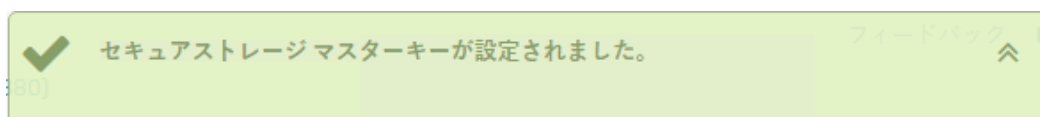
- 最低 12文字
- うち英大文字を 1文字以上
- うち英小文字を 1文字以上
- うち数字 [0-9] を 1文字以上
- うち特殊文字を 1文字以上

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。

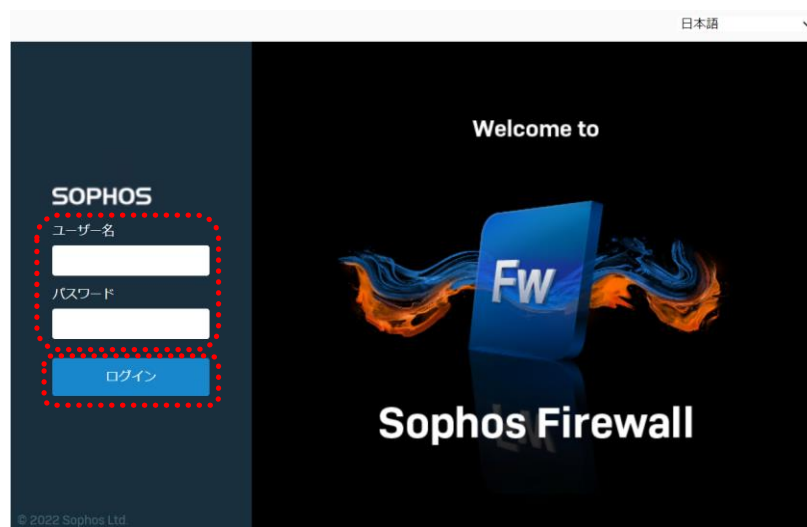
ここまでの設定が、初期設定で必要な設定です。



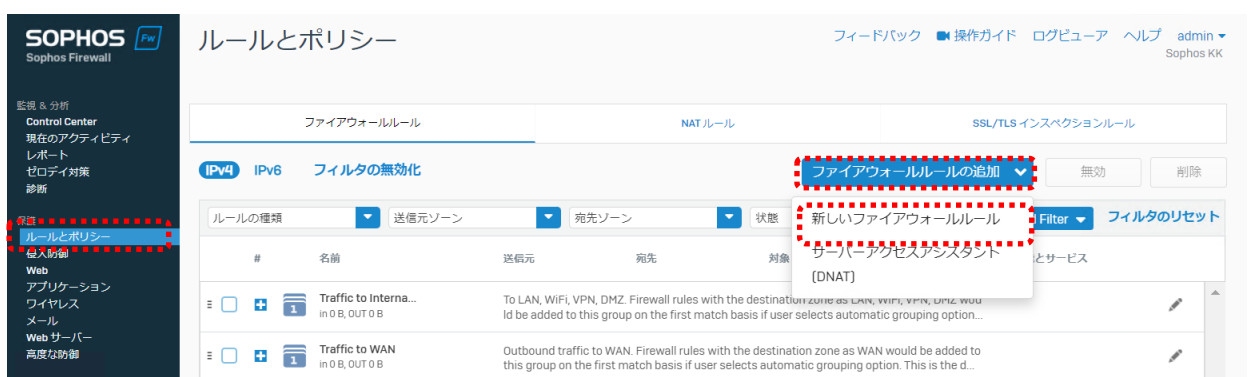
3 【任意】 DHCP パケットの透過設定

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 ユーザー名[admin]、パスワ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」 - 「新しいファイアウォールルールの追加」をクリックします。



Sophos Firewall 評価導入手順書(ブリッジモード)

(3) 下記のように設定し、「保存」をクリックします。

このスクリーンショットは、Sophos Firewallの「ファイアウォールルールの追加」設定画面を示しています。以下の設定が確認できます：

- ルールのステータス: ON
- ルール名: DHCP
- 優先順位: 最上位
- ファイアウォールトラフィックのログ: チェックが入っています
- 送信元ゾーン: WAN
- 送信元ネットワークとデバイス: 任意
- 宛先ゾーン: LAN
- 宛先ネットワーク: 任意
- サービス: DHCP
- 通知のユーザーを一致: OFF
- 操作ボタン: 保存 (Save)

(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。

| # | 名前 | 送信元ゾーン | 宛先ゾーン | サービス | 状態 | アクション |
|---|--|--|--------------|------|-------|-----------|
| 1 | DHCP in 0 B, OUT 0 B | WAN, すべてのホスト | LAN, すべてのホスト | DHCP | #6 承認 | [編集] [削除] |
| | Traffic to Interna... in 0 B, OUT 0 B | To LAN, WiFi, VPN, DMZ. Firewall rules with the destination zone as LAN, WiFi, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option... | | | | |
| | Traffic to WAN in 0 B, OUT 0 B | Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d... | | | | |

Sophos Firewall 評価導入手順書(ブリッジモード)

- (5) 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。
- (6) 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。

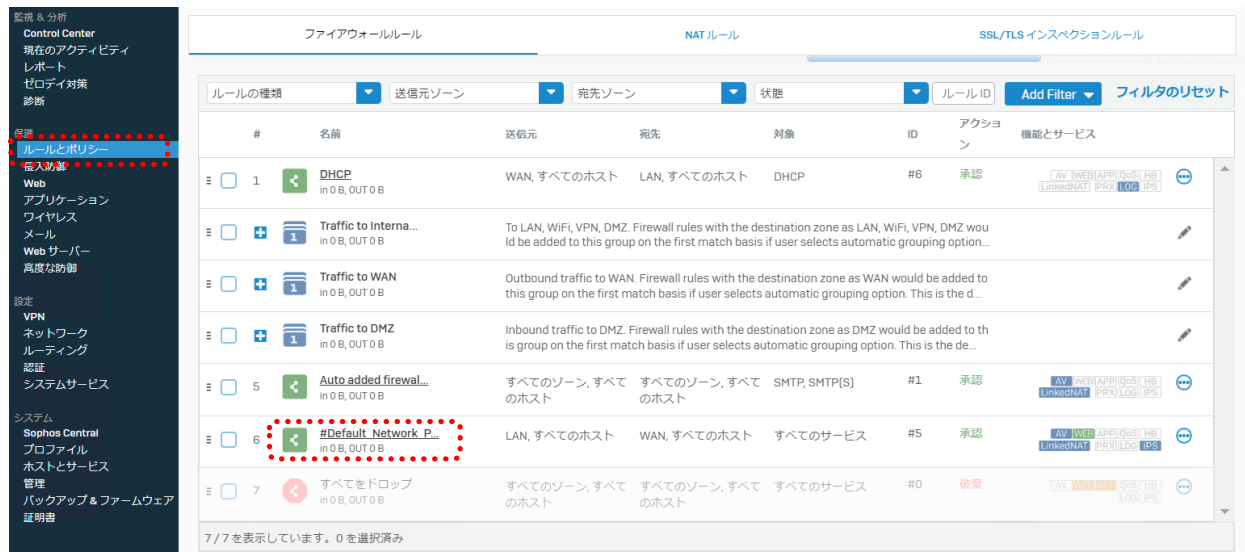
4 IPS の設定

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。

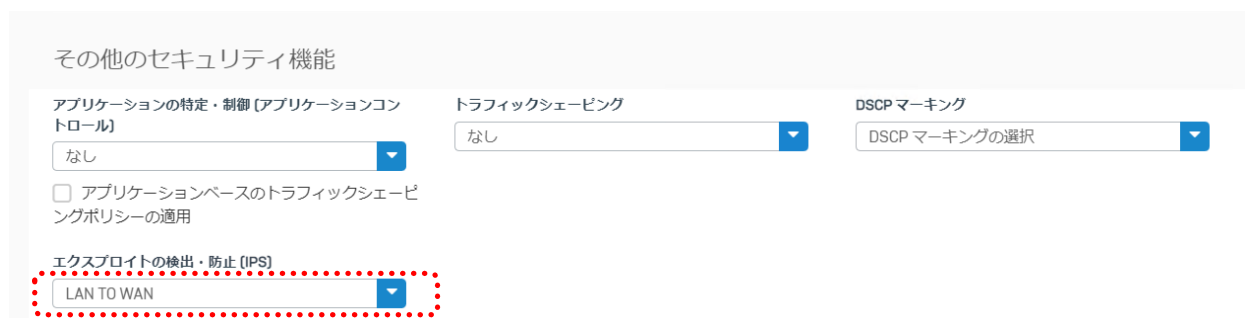
(1) 「保護」 - 「侵入防御」で「IPS ポリシー」をクリックし、IPS 保護を「ON」に設定します。



(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。

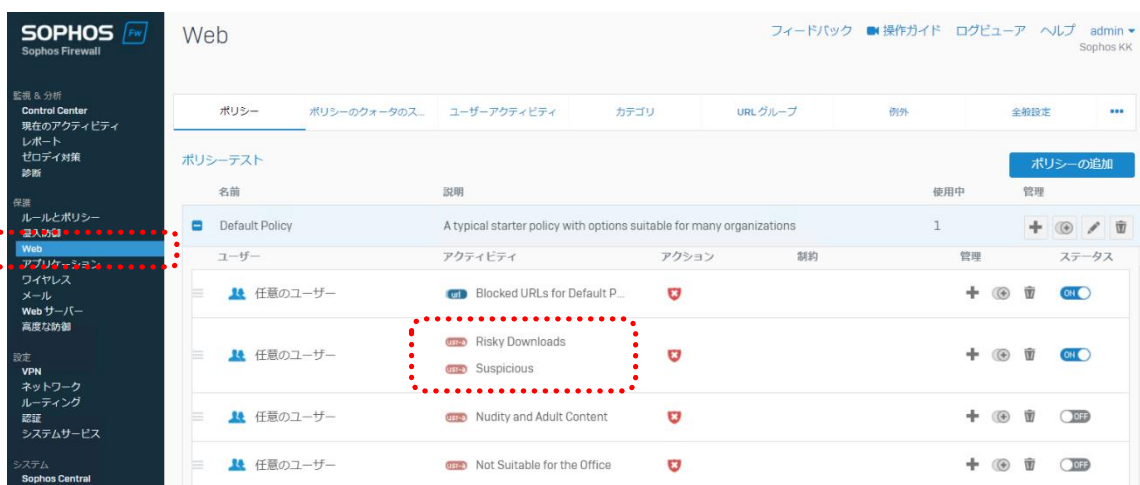


5 Web フィルタの設定

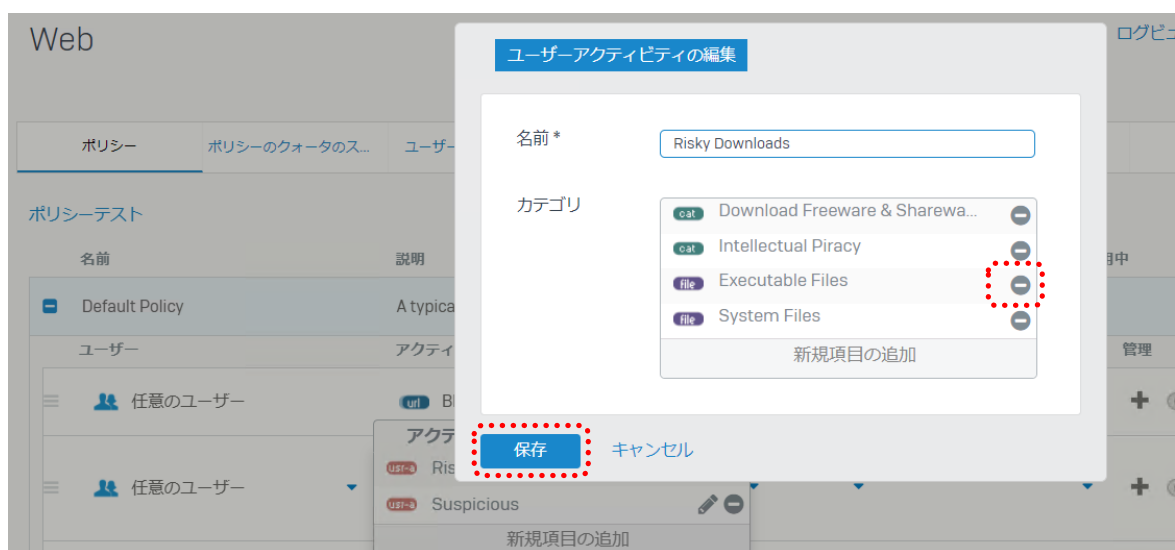
初期設定は[Default Policy]を使用しており、実行ファイルのダウンロードがブロックされてしまいますので、設定変更が必要になります。

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

6.1 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。



Sophos Firewall 評価導入手順書(ブリッジモード)

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 yellow callout boxes and red dashed boxes:

- “復号化”を選択**: The "処理" (Action) dropdown menu is set to "復号化" (Decrypt).
- “最上位”を選択**: The "優先順位" (Priority) dropdown menu is set to "最上位" (Highest).
- “Maximum compatibility”を選択**: The "互換性" (Compatibility) dropdown menu is set to "Maximum compatibility".
- “LAN”を選択**: The "送信元" (Source) dropdown menu is set to "LAN".
- “WAN”を選択**: The "宛先" (Destination) dropdown menu is set to "WAN".
- “保存”をクリック**: The "保存" (Save) button at the bottom left is highlighted.

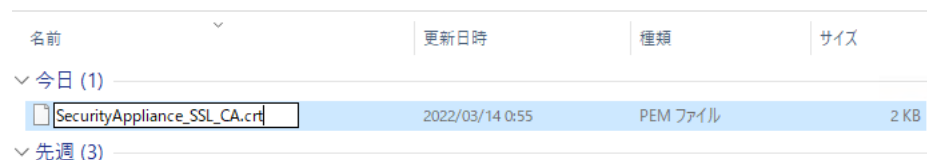
6.2 Sophos Firewall が発行した SSL 証明書をクライアントにインストールする

「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(ブリッジモード)

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。

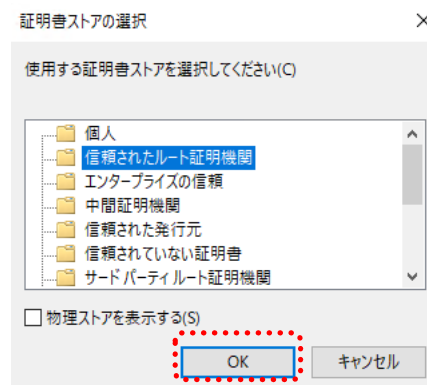


Sophos Firewall 評価導入手順書(ブリッジモード)

「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。

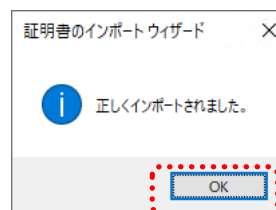


Sophos Firewall 評価導入手順書(ブリッジモード)

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。



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。

