さくらのクラウド向け

Owlook

# 仮想型 UTM マネジメント

# サービス利用手順書

## Sophos Firewall
## Web サーバープロテクション（WAF）編

第 3.1 版

2023 年 8 月 29 日

興安計装株式会社

KOANKEISO

# 目　次

## 内容

## 改訂履歴

| 版数 | 更新日 | 更新内容 | 更新者 |
|---|---|---|---|
| 1.0 | 2020/5/25 | 初版作成 | 興安計装株式会社 |
| 2.0 | 2021/2/4 | v18 アップグレードに伴う改定 | 興安計装株式会社 |
| 3.0 | 2022/4/20 | v18.5 アップグレードに伴う改定 | 興安計装株式会社 |
| 3.1 | 2023/8/29 | OS バージョン差分修正 | 興安計装株式会社 |
| | | | |

## はじめに

**本手順書に関する注意事項**

この手順書は、さくらのクラウド環境において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、ユーザーアシスタントをご確認頂くようお願い致します。

**Sophos Firewall ユーザーアシスタント**

https://doc.sophos.com/nsg/sophos-firewall/19.5/help/en-us/webhelp/onlinehelp/index.html

**本サービスにおけるお問い合わせは、さくらインターネット株式会社が提供するサポート窓口をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。本サービスの製品 Sophos Firewall の開発元であるソフォス株式会社への直接の問い合わせを固く禁じます。**

**本手順書の目的と位置づけ**

**目的:**

1. **バックエンド（保護対象の Web サーバー）の作成**
2. **保護ポリシーの作成※モニターモード**
3. **HTTPS 証明書の作成**
4. **ユーザポータルのポート変更**
5. **WAF ポリシーの作成**
6. **Web サイトへのアクセスログを確認**
7. **ルール ID を抽出**
8. **スキップルールの設定と、ポリシーを拒否モードで動作**

本手順書は以下の手順書に沿って Sophos Firewall が展開されアクティベートされた、状態を前提としております。

**初期導入編**

https://www.owlook.jp/public/document/sophos_xg_intruduction.pdf

**ファイアウォールの設定、DNAT の設定編**

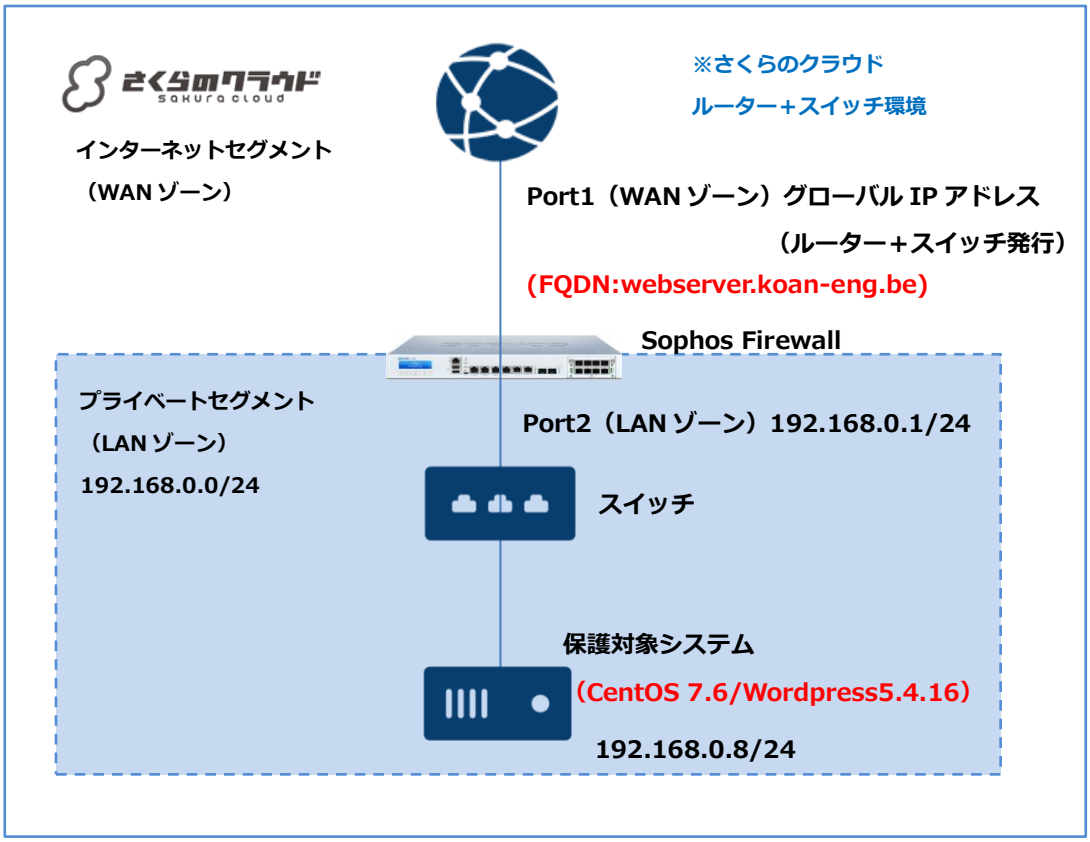
https://www.owlook.jp/public/document/sophos_xg_fw_dnat.pdf

**ネットワークプロテクション編**

https://www.owlook.jp/public/document/sophos_nrtworkprotection.pdf

## 1．ご利用環境の構成

本手順書では以下の構成であることを前提に記載いたします。



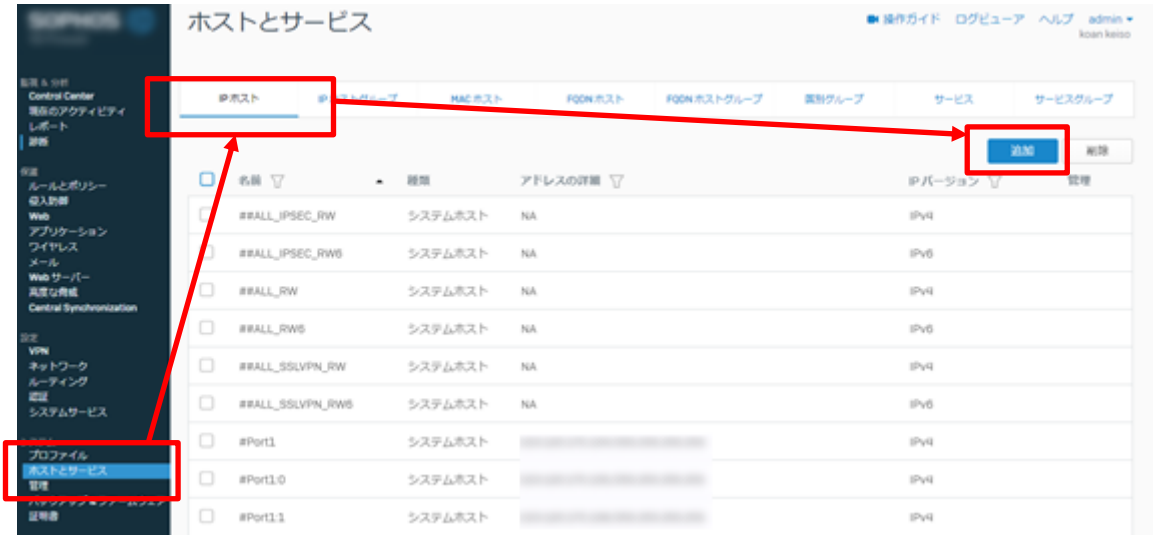

【構成要件】

- Sophos Firewall はご利用の環境におけるインターネットとの接続点へ導入します。
- Sophos Firewall は WAN ゾーン側と LAN ゾーン側の 2 つの NIC を持ちます。LAN 側の IP アドレスは 192.168.0.1/24 を持ちます。
- WAN ゾーンは Port1 を接続したルーター＋スイッチの保持するグローバル IP アドレスを設定します。
- LAN ゾーンは 192.168.0.0/24 のネットワーク帯域で構成します。
- LAN ゾーンはスイッチを利用しセグメントを構築します。
- 保護対象システムの IP アドレスは 192.168.0.8/24 を持ちます。
- 保護対象システムのリッスンポートは HTTP（80）です。
- 保護対象システムのデフォルトゲートウェイは Sophos Firewall の LAN ゾーン側の IP アドレス 192.168.0.1/24 を向いています。
- 保護対象システムは Wordpress5.4.16 です。
- 保護対象システムの FQDN は webserver.koan-eng.be です。

## 2．バックエンド Web サーバーの作成

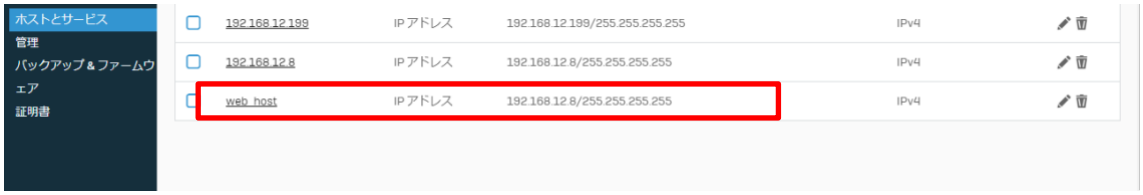
**※今回の手順では「１．ご利用環境の構成」に基づき記載します。**

①ホストとサービス ＞ IP ホストタブ ＞ 追加をクリックします。

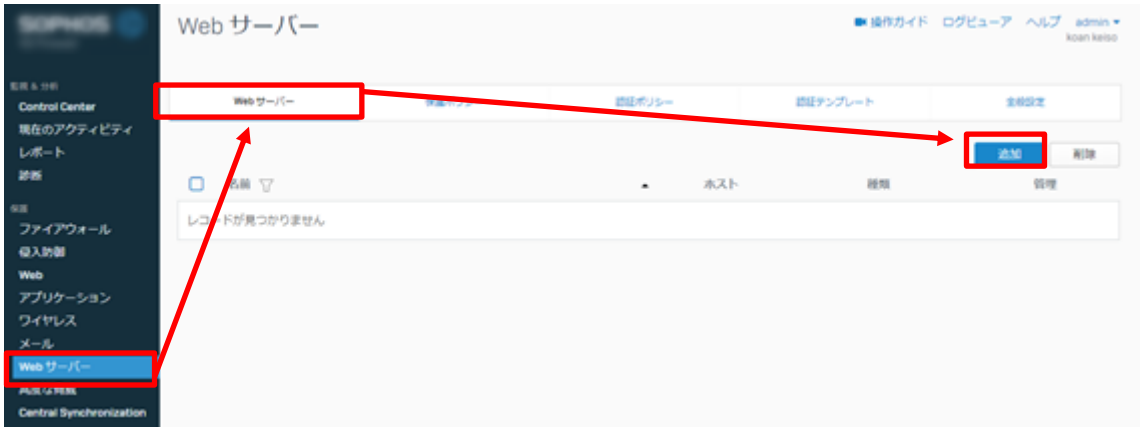



②今回は名前を「web_host」、IP アドレスを「192.168.0.8」とし保存をクリックします。

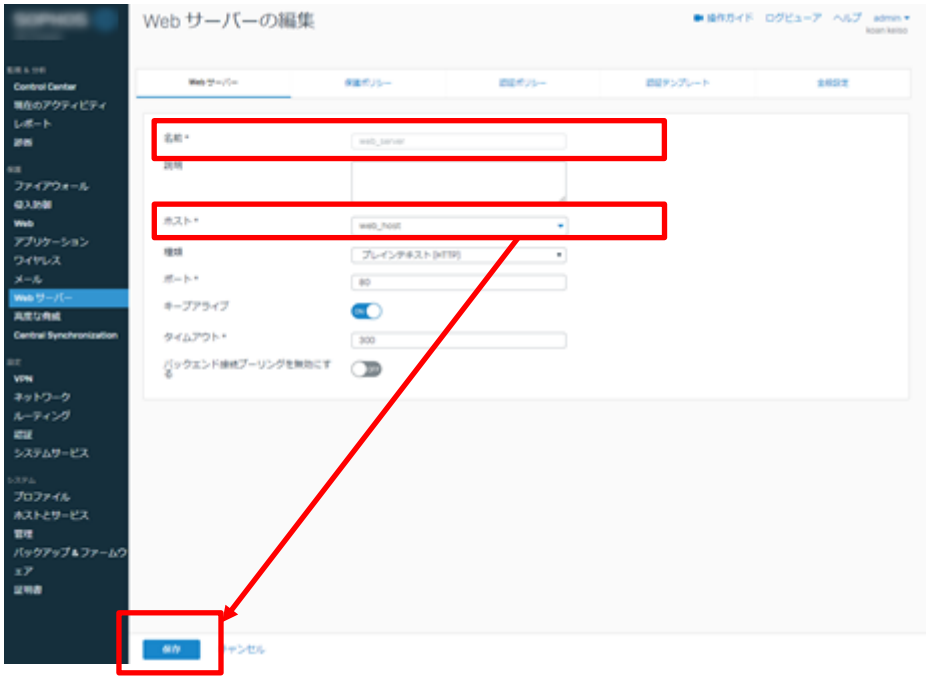

③web_host が生成されていることを確認します。



④Web サーバー ＞ web ポリシータブ ＞ 追加をクリックします。




⑤名前は任意ですが、今回は「web-server」、ポート「80」とします。ホストは①～③で作成した「web_host」を選択し、他の項目はデフォルトのまま保存をクリックします。

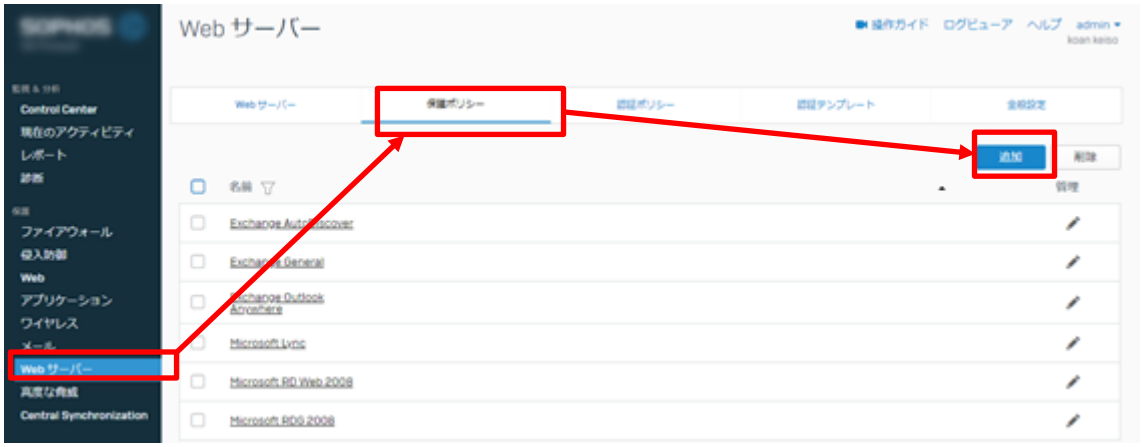


⑥web-server が作成されていることを確認します。


**※Web サーバーについては、実サーバーのリッスンしているポートが HTTP（80）か HTTPS（443）かで、設定を適宜変更してください。今回の手順では「１．ご利用環境の構成」に基づき記載します。**

## 3．保護ポリシーの作成

①Web サーバー ＞ 保護ポリシータブ ＞ 追加をクリックします。

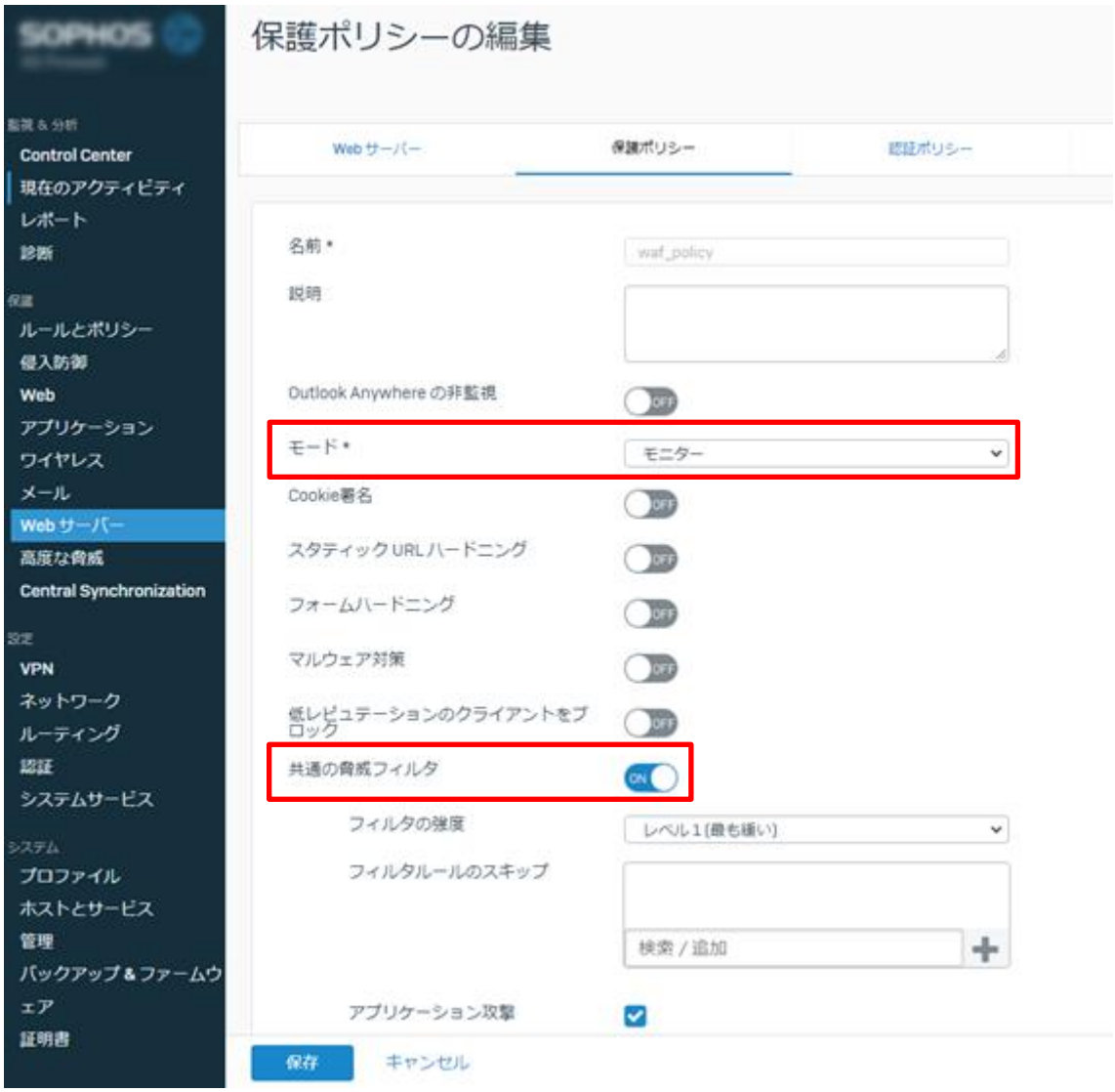



②任意で名前を入力します。今回は「waf_policy」と入力します。


　このポリシー設定ではさまざまなセキュリティ検査ポリシーを設定することができます。保護機能の詳細は Sophos Firewall ユーザーアシスタントをご覧いただくか、本サービスの仕様書をご覧ください。

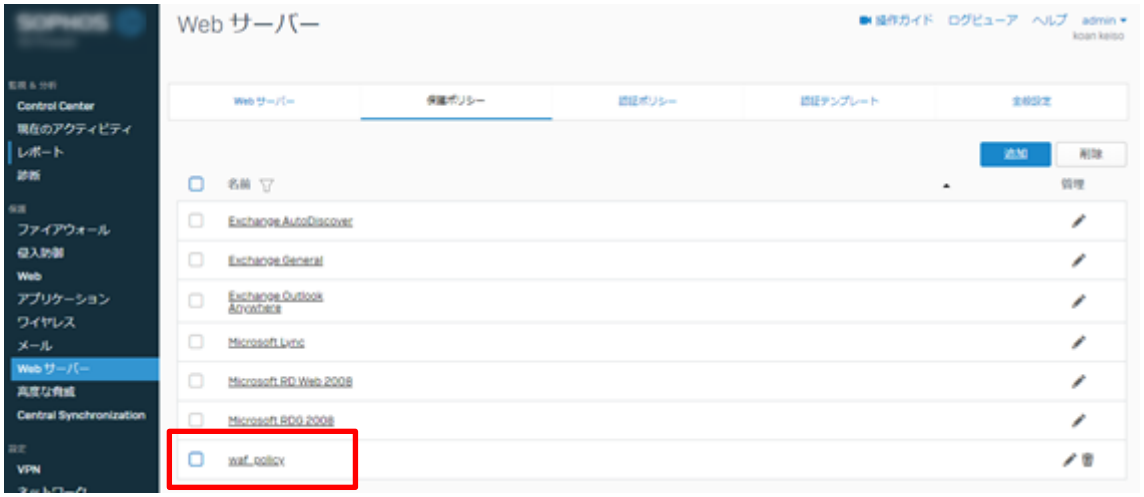
Sophos Firewall ユーザーアシスタント
https://doc.sophos.com/nsg/sophos-firewall/19.5/help/en-us/webhelp/onlinehelp/index.html
Sophos Firewall イメージ提供の仕様書
https://www.owlook.jp/public/document/sophos_xg_shiyou.pdf

③今回はモードを「モニター」、「共通の脅威フィルタ」を ON にします。



④共通の脅威フィルタを ON にすると、画面下部に脅威フィルタのカテゴリが表示されます。今回はすべてのカテゴリが ON の状態で保存をクリックします。またフィルタの強度をレベル１（最も緩い）からレベル４（最も厳しい）まで設定可能です。今回はレベル１で設定ます。


⑤waf_policy が生成されていることを確認します。

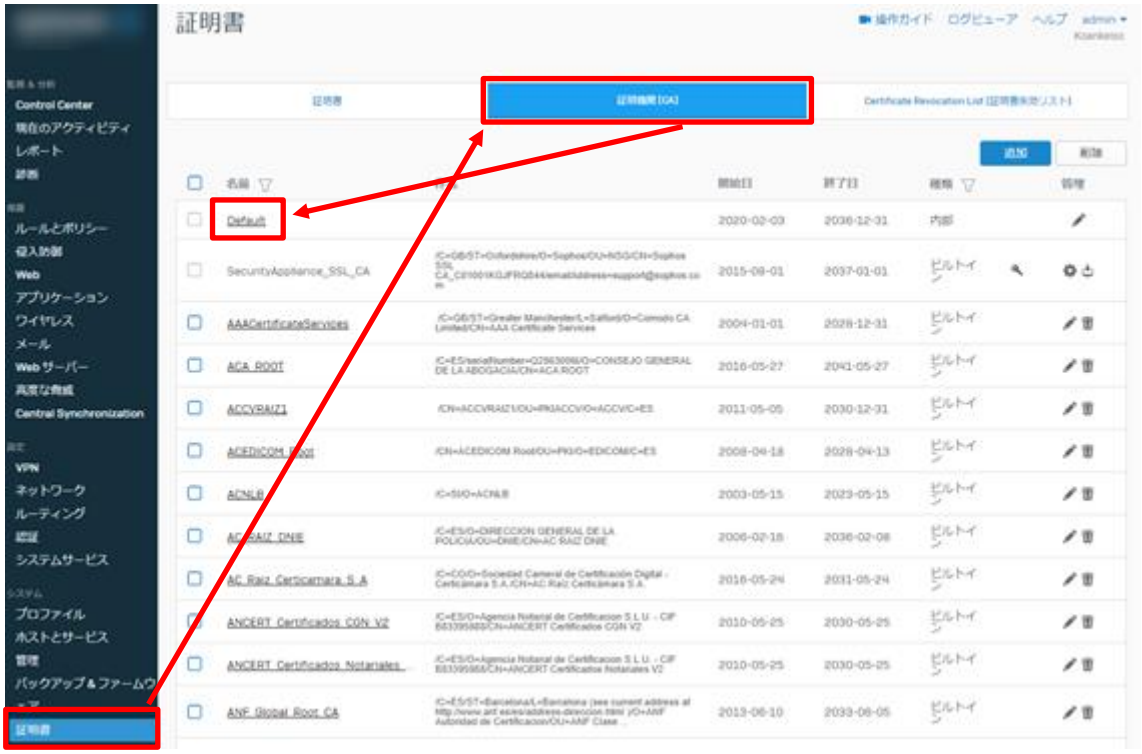


## ４．証明書の作成

HTTPS サーバー証明書は、Web サイトの実在性を確認し、ブラウザとウェブサーバー間で通信データの暗号化を行うための電子証明書です。認証機関から発行されます。HTTPS サーバー証明書には、Web サイトの所有者の情報や、暗号化通信に必要な鍵、発行者の署名データが含まれています。

ローカル署名した証明書を生成する際は、Default の証明機関の設定を先に行う必要があります。

証明書 ＞ 証明機関(CA)タブ ＞ Default のオブジェクトをクリックします。




### （１）Default の証明機関を設定する。

Sophos Firewall 内部で SSL 証明書を生成する場合に、証明機関として参照する設定を行います。

① 証明機関の詳細を以下の例示を参考に設定します。

・国名：Japan
・都道府県：Tokyo
・地域名：Chiyoda-ku
・組織名：koan keiso ※会社名等
・組織単位名：sales ※部署名等
・一般名（CN）：koan keiso ※会社名等
・メールアドレス：任意のメールアドレス

・秘密鍵のパスワード：任意のパスワード

・鍵の種類：デフォルトのまま使用します。※デフォルトは RSA です。

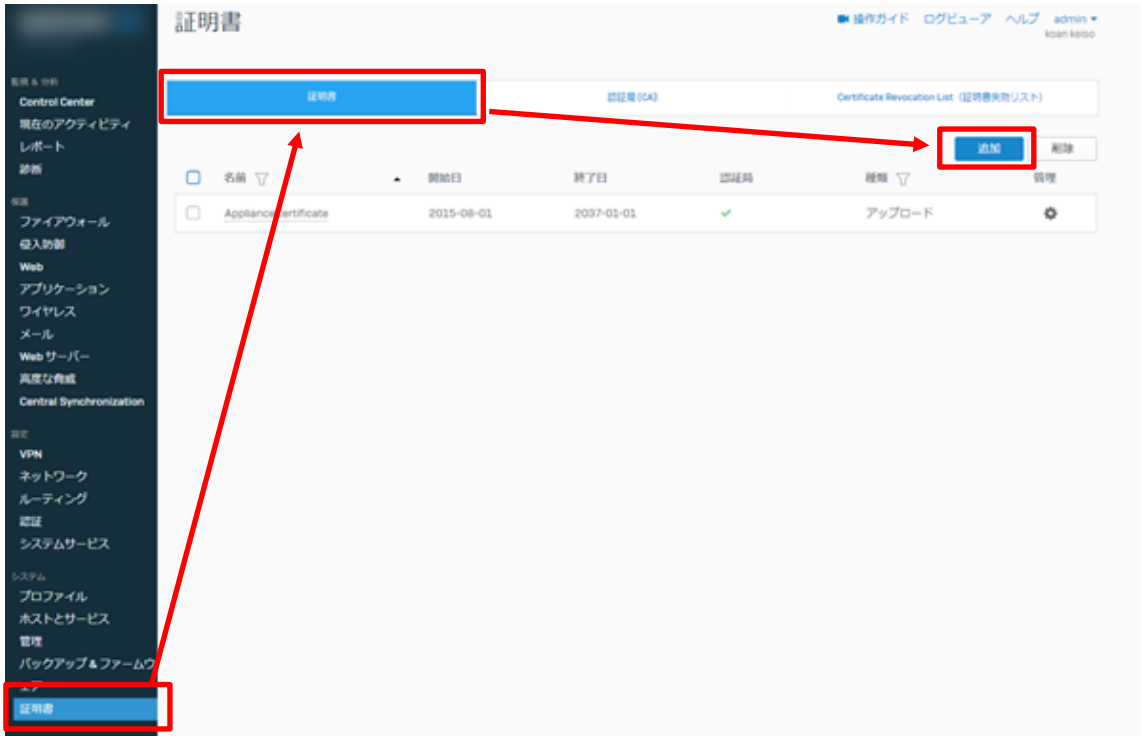
・鍵長：デフォルトのまま使用します。※デフォルトは 2048 です。

・セキュアハッシュ：デフォルトのまま使用します。※デフォルトは SHA-256 です。

下部の保存ボタンをクリックします。


続いて、ローカル署名した証明書の作成を行います。

証明書 ＞ 証明書タブ ＞ 追加をクリックします。



## （２）SSL 証明書を Sophos Firewall で作成する。（自作 SSL 証明書）

Sopohos Firewall 内部で SSL 証明書を生成する場合の手順です。今回はこの手順で生成する証明書を利用して設定を行います。

① ローカル署名した証明書の生成を選択します。


② 証明書の詳細セクションを以下の通り設定します。

・名前：webserver.koan-eng.be　※Web サーバーの FQDN を使用します。

・開始日、終了日：デフォルトのまま使用します。※デフォルトは 1 年です。

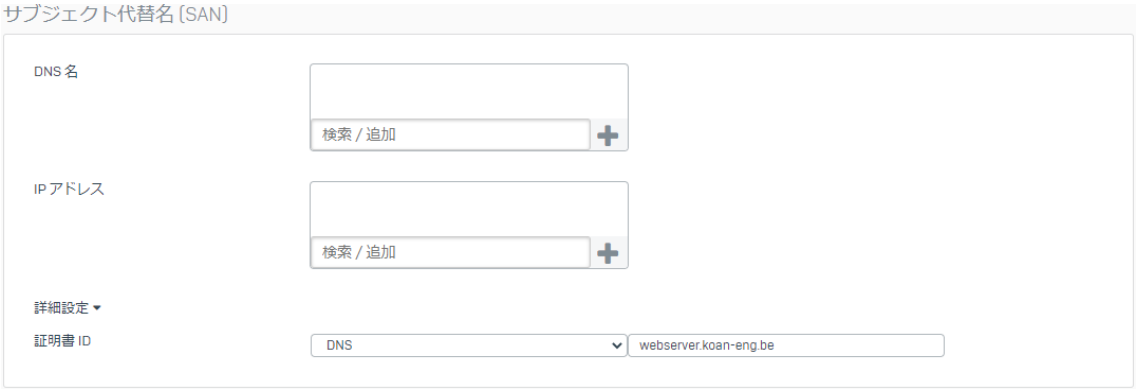
・鍵長：デフォルトのまま使用します。※デフォルトは 2048 です。

・セキュアハッシュ：デフォルトのまま使用します。※デフォルトは SHA-256 です。


③ サブジェクト名の属性セクションは、Default 認証機関から引用されている部分はそのまま利用し、不足箇所について設定を行います。

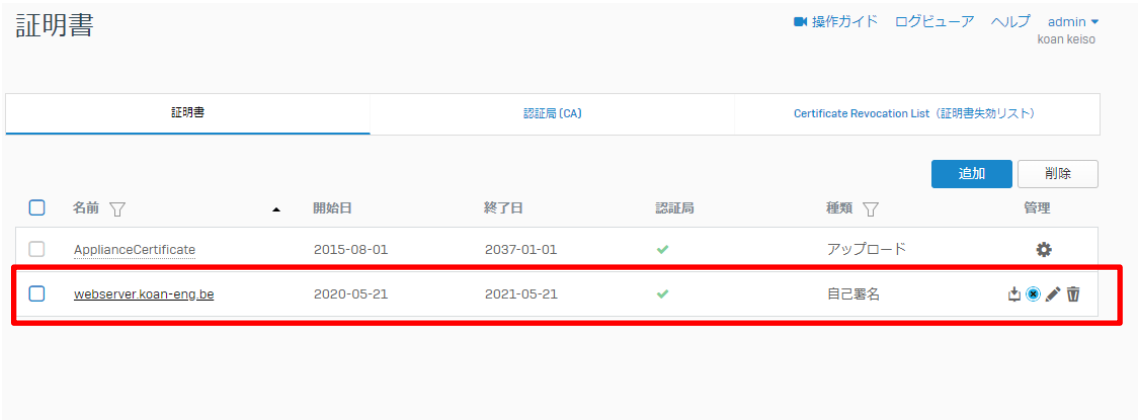
・一般名（CN）：webserver.koan-eng.be　※Web サーバーの FQDN を使用します。

④ サブジェクト代替名(SAN)セクションは、詳細設定を開き、証明書 ID に DNS を選択して Web サーバーの FQDN を設定します。




下部の保存ボタンをクリックします。

⑤ 証明書の一覧から自己証明書が生成されていることを確認します。




### （2）発行済の SSL 証明書をアップロードする。

パブリックな認証局より発行された証明書等、既に発行済の HTTPS 証明書を設定する場合の手順です。※今回の手順では使用しません。参考までに記載します。

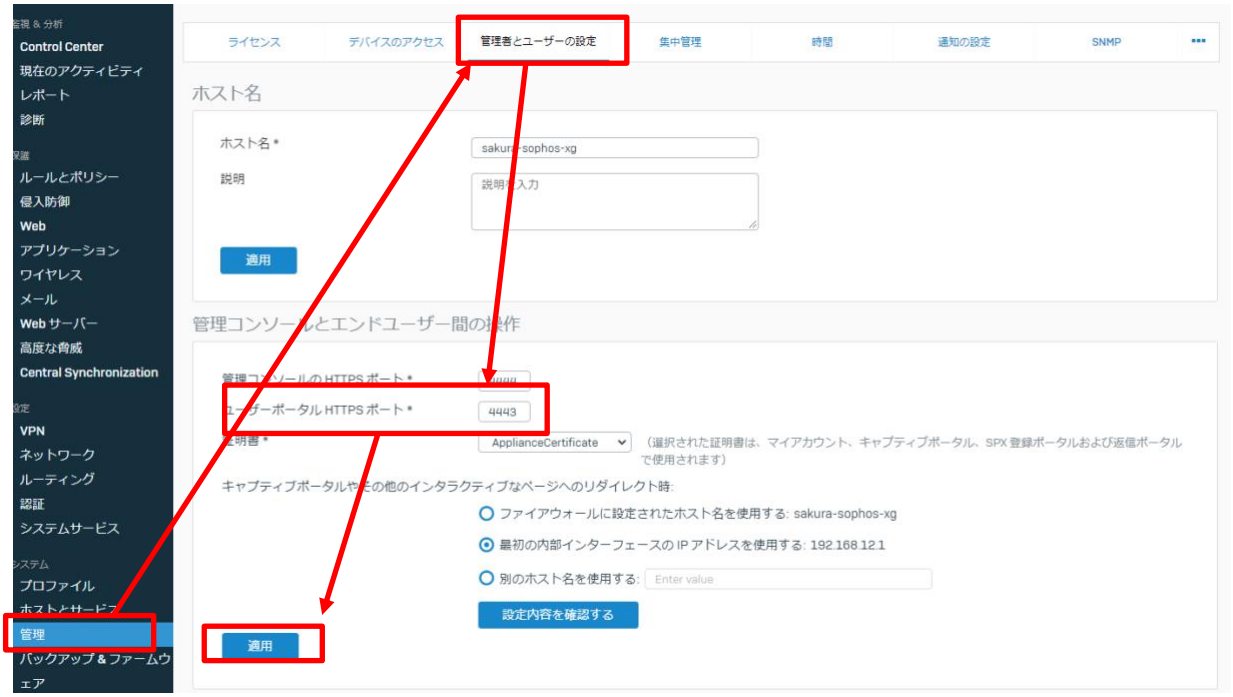
①証明書アップロードを選択します。必須項目として名前、証明書ファイルの形式を選択し、HTTPS 証明書ファイルをアップロードします。HTTPS 証明書の形式により、任意で秘密鍵、パスフレーズを入力し保存をクリックします。

## 5．ユーザーポータルの HTTPS ポート設定変更

Sophos Firewall はユーザ向けのリモートアクセス等の機能提供用にユーザポータル機能があります。デフォルトでは、HTTPS ポートを使用している設定になっているため、今回設定する手順とポートが重複するため以下の通り、変更が必要です。

管理 ＞ 管理者とユーザの設定 ＞ 管理コンソールとエンドユーザ間の操作セクション　より

ユーザポータルの HTTPS ポートを、今回は 443 から 4443 へ変更し適用をクリックします。



## 6.WAF ポリシーの作成

ここまで、以下のコンポーネントと関連項目の設定をしてきました。

・バックエンド（保護対象）Web サーバー
・保護ポリシー
・SSL 証明書
・ユーザポータルの HTTPS ポート変更

これらのコンポーネントを使用して、ファイアウォールのルールに WAF ポリシーを追加します。

①ルールとポリシー ＞ ファイアウォールルールの追加 ＞ 新しいファイアウォールルールをクリックします。


② アクション ＞ 承認　のプルダウンメニューで「Web サーバープロテクションで保護する」を選択します。今回はルール名を waf_rule とし、ルールの位置を最上位を選択します。

③ホスト型サーバーセクションを以下の通り設定します。

・ホスト型アドレス：＃Port1

・HTTPS、HTTP のリダイレクト：チェック

・リスニングポート：443

・HTTPS 証明書：webserver.koan-eng.be

・ドメイン：webserver.koan-eng.be　※HTTPS 証明書の内容を読み取るため自動的に設定されます。


④保護されたサーバーセクションを以下の通り設定します。

・Web サーバー：web_server　※選択してチェックします。


⑤詳細設定セクションを以下の通り設定します。

・ポリシー保護対策：waf_policy を選択

・ホストヘッダをパス：チェック

画面下部の保存をクリックします。

## 7.WAF のアクセスログ確認とフィルタルールのスキップ設定

Sophos Firewall の保護ポリシーはデフォルト設定が厳格なため、誤検知を防ぐために下記の作業が必要になります。

1． 保護ポリシーでモニターモードで設定
2． Web サイトへ正常系アクセス試験を一通り実施しアクセスログを確認
3． 検出されたルール ID を「フィルタルールをスキップ」リストへ設定

**※今回の手順では「1．ご利用環境の構成」に基づき記載します。**

### （1）サイトへの正常系アクセスログを確認

アクセスログの確認は GUI で提供されるログビューア―機能では、ルール ID を確認することができません。SSH でアクセスし、Advance Shell 機能を利用する必要があります。本手順では、AdvancedShell によるログ確認方法を記載します。

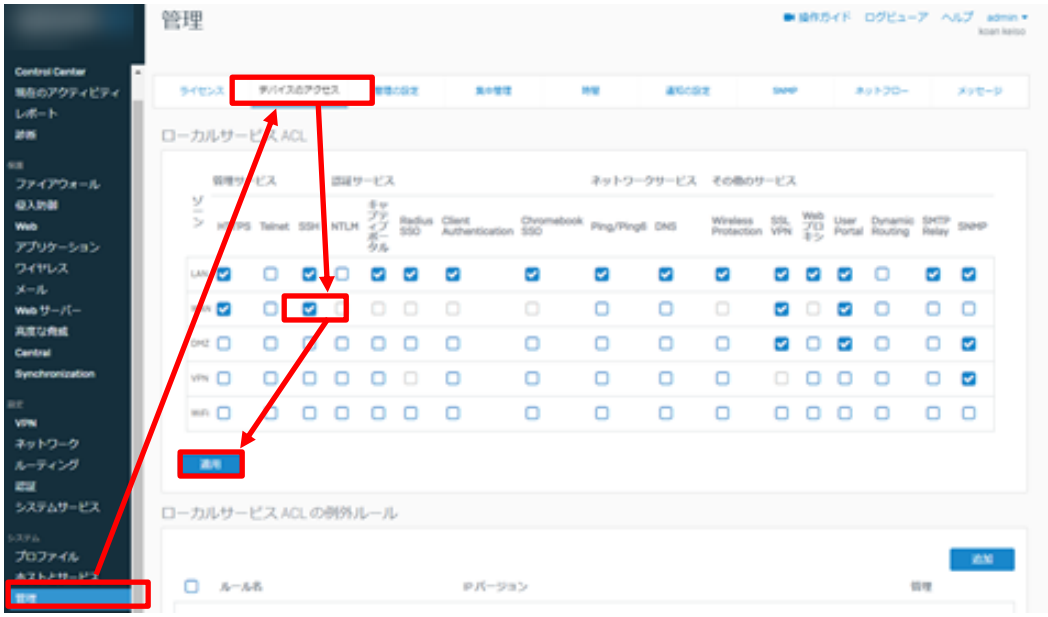
**尚、Advance Shell（CLI）の操作方法についてはサポート対象外となるため、ご利用者様の責任において操作いただくようお願いします。**

①アクセスログの確認準備をします。

本手順では一時的に WAN 側の SSH アクセスを許可しアクセス方法を記載します。

**※安全の為、LAN 側からのアクセスを推奨します。**

管理 ＞ デバイスアクセス ＞ WAN ＞ SSH にチェックを入れ適用をクリックします。



②任意のターミナルソフトから SSH でログインします。
この時のアカウントは Webadmin へのアクセスアカウントと同様です。


③ログイン後メニューが表示されます。５．Device Management ＞ ３．Advanced Shell を選択します。


④ログイン後、以下のコマンドでリアルタイム出力をキャプチャする準備をします。この時、以下のキーワードを指定します。

・Web サーバーの FQDN：webserver.koan-eng.be

・ModSecurity による Pattern match：security2:erro

```
# tail -f /log/reverseproxy.log | grep "webserver.koan-eng.be" | grep "security2:error"
```

⑤Web サーバーへアクセスし、一通り正常にアクセスできることを確認します。

https://webserver.koan-eng.be/


https://webserver.koan-eng.be/wp-login.php

⑥ログ出力の内容を確認します。

```
～ 一部抜粋 ～

[Mon May 25 17:24:20.627329 2020] [security2:error] [pid 18358:tid 140426983933696] [client XXX.XXX.XXX.XXX:42914] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Operator LT matched 5 at TX:inbound_anomaly_score. [file "/content/waf/2.7.3/modsecurity_crs_correlation.conf"] [line "33"] [id "981203"] [msg "Inbound Anomaly Score (Total Inbound Score: 3, SQLi=1, XSS=): Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded"] [hostname "webserver.koan-eng.be"] [uri "/wp-admin/load-styles.php"] [unique_id "XsuAs38AAAEAAEe2opYAAAAa"], referer: https://webserver.koan-eng.be/wp-admin/

[Mon May 25 17:27:50.489546 2020] [security2:error] [pid 18358:tid 140426849650432] [client XXX.XXX.XXX.XXX:33583] [client XXX.XXX.XXX.XXX] ModSecurity: Warning. Pattern match "¥¥¥¥W{4,}" at ARGS:submit. [file "/content/waf/2.7.3/modsecurity_crs_generic_attacks.conf"] [line "37"]
[id "960024"] [rev "2"] [msg "Meta-Character Anomaly Detection Alert - Repetative Non-Word Characters"] [data "Matched Data: ¥¥xe3¥¥x82¥¥xb3¥¥xe3¥¥x83¥¥xa1¥¥xe3¥¥x83¥¥xb3¥¥xe3¥¥x83¥¥x88¥¥xe3¥¥x82¥¥x92¥¥xe9¥¥x80¥¥x81¥¥xe4¥¥xbf¥¥xa1 found within ARGS:submit: ¥¥xe3¥¥x82¥¥xb3¥¥xe3¥¥x83¥¥xa1¥¥xe3¥¥x83¥¥xb3¥¥xe3¥¥x83¥¥x88¥¥xe3¥¥x82¥¥x92¥¥xe9¥¥x80¥¥x81¥¥xe4¥¥xbf¥¥xa1"] [ver "OWASP_CRS/2.2.7"] [maturity "9"] [accuracy "8"] [hostname "webserver.koan-eng.be"] [uri "/wp-comments-post.php"] [unique_id "XsuBhn8AAAEAAEe2orkAAAAq"], referer: https://webserver.koan-eng.be/2020/05/13/hello-world/

～ 一部抜粋 ～
```

[id "9XXXXX"]セクションが、WAF のルールにマッチした ID です。

**※AdvancedShell(CLI)による確認方法を、WAN 側からのアクセス方法で記載しましたが、安全の為、LAN 側からのアクセスを推奨します。または目的とする行為が完了後に WAN 側の SSH アクセスを無効化するようお願いします。**

### （2）出力されたルール ID を確認

ログに出力されたルール ID は、下記の 2 つです。ルール ID にはインフラストラクチャルールというルールが含まれます。

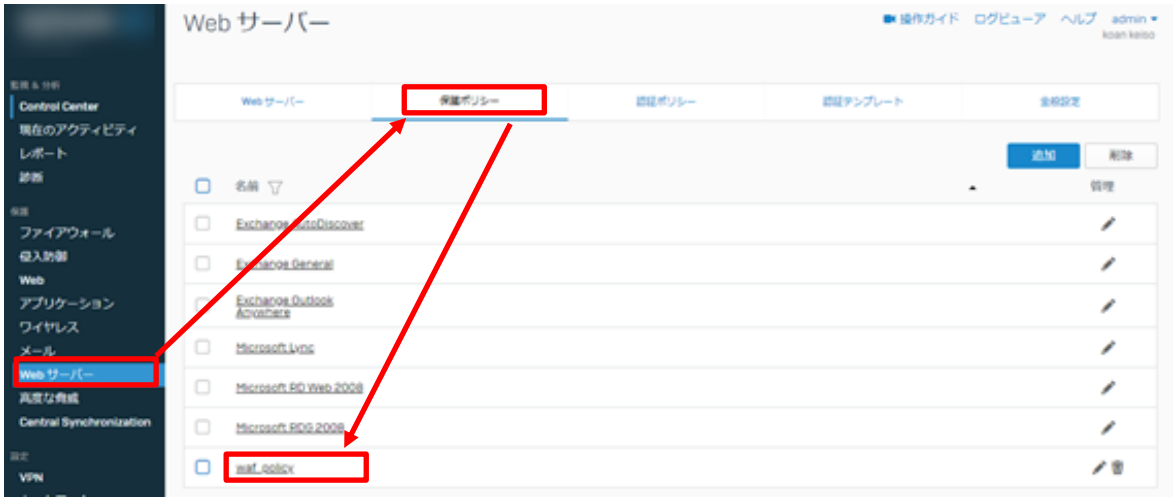
```
[id "981203"] ←インフラストラクチャルール
[id "960024"]
```

検出されたルール ID のうちインフラストラクチャールール以外の ID を「フィルタルールのスキップ」リストに追加します。

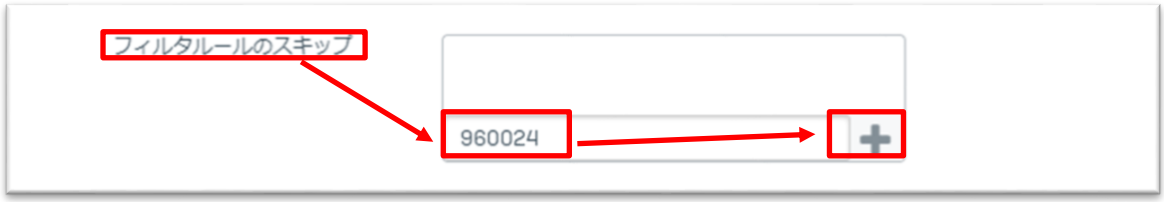
```
[id "960024"]
```

### （3）「フィルタルールのスキップ」へ、誤検出のルール ID を追加

①Web サーバー＞ 保護ポリシー ＞ waf_policy タブをクリックし 3．保護ポリシーで作成した waf_policy を編集します。




②フィルターのスキップセクションから id を入力し、＋マークをクリックします。




フィルターのスキップに id が追加されました。


**※本手順はサンプルの為、id を一つのみ記載しましたが、実際の環境に合わせて検出されたフィルターのスキップ id を追加してください。**

③フィルターのスキップリストの入力が完了したら、モードを「モニター」から「拒否する」に変更し画面下部の保存をクリックします。


**※保存をクリックした時点で、Web サーバーに対する防御機能がオンになります。**

### （4）インフラストラクチャルールについて

インフラストラクチャルールと呼ばれる特定のルールがあります。それらは WAF ModSecurity の中核となるルールです。これらのルールに基づいて他のルールは構築されています。**インフラストラクチャルールがフィルタールールのスキップリストに追加されている場合、関連するルールが無効となり潜在的な攻撃に対して脆弱になるため、以下に記載されたインフラストラクチャールールは無効にしないことを推奨します。**

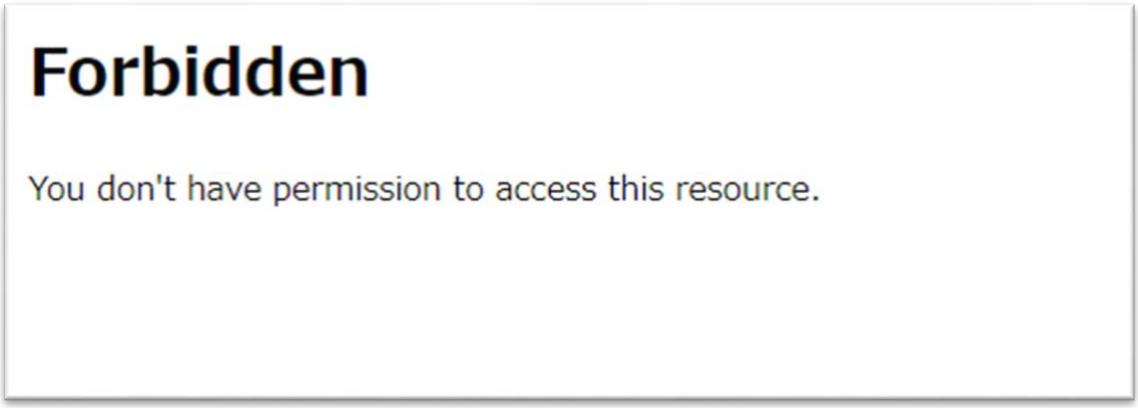
- 901100
- 901110
- 949100
- 949190
- 949110
- 959100
- 980100
- 980110
- 980120
- 980130
- 980140

## 8.WAF の動作確認

簡易的な攻撃を実行し実際の検知を確認します。トップページに意図的なクエリを含め Web サーバーへリクエストします。※具体的な攻撃方法の解説は省略します。

https://webserver.koan-eng.be/?auth=1'

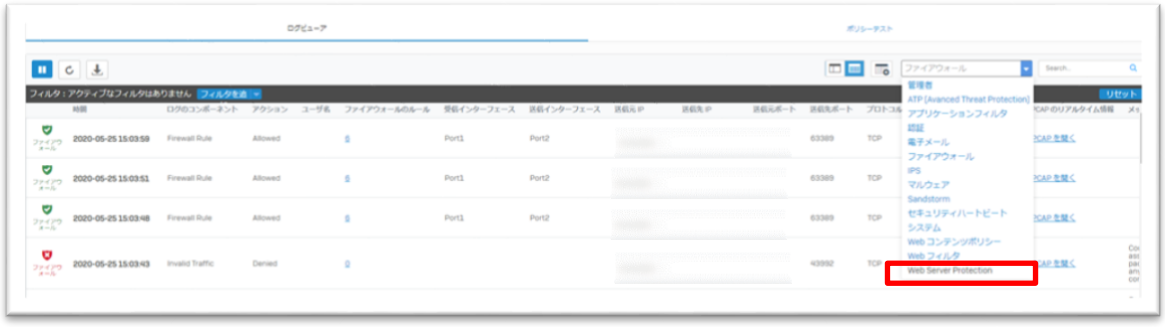

不正なクエリを検出し、「You don't have permission to access this resource.」(403)と表示されました。ブラウザの表示は下記になります。



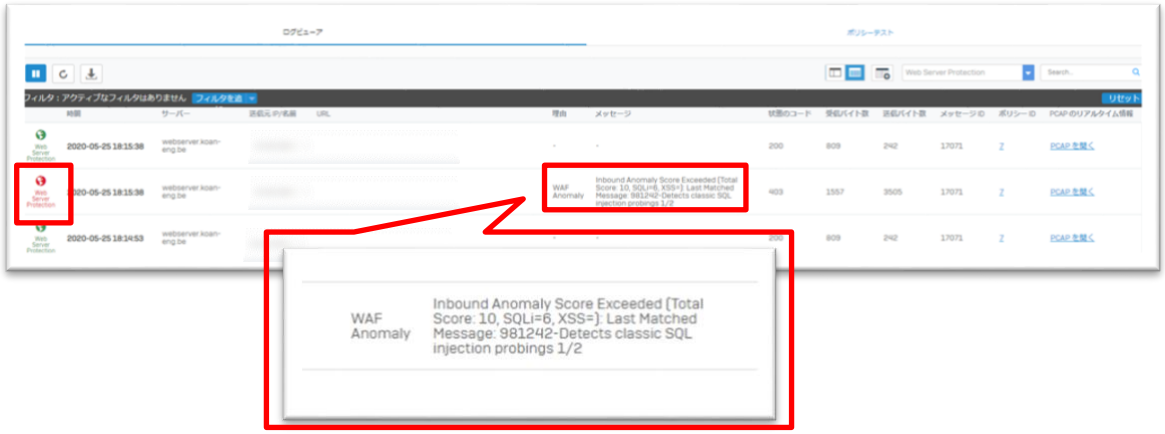

攻撃後の WAF のログを確認します。Advanced Shell による確認（CLI）、ログビューアーによる確認（GUI）、いずれの方法でも確認することが可能です。
Advanced Shell による確認（CLI）は先に記載した通りですので、ここではログビューアーによる確認（GUI）を記載します。

①画面右上のログビューアーをクリックします。


③　ログビューア―を開き、Web サーバープロテクションでフィルタをかけます。




③該当の通信が WAF Anormaly として検知されていることが確認できます。



## ９．設定のまとめ

WAF を設定するために、以下に記すコンポーネントを WAF のポリシーに関連付けます。

1．バックエンド（保護対象の Web サーバー）の作成
2．保護ポリシーの作成※モニターモード
3．HTTPS 証明書の作成
4．ユーザポータルのポート変更
5．WAF ポリシーの作成

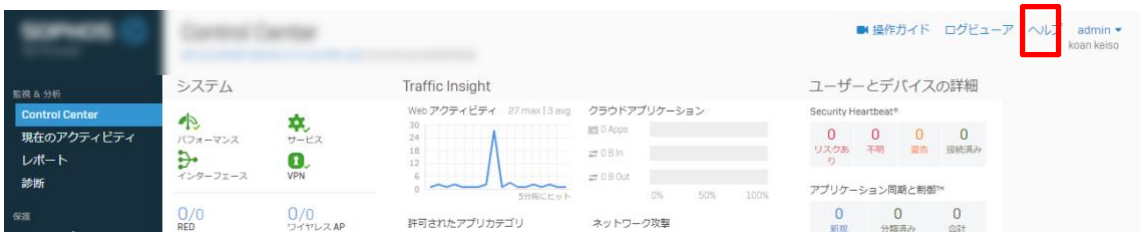
ポリシーを作成したら、以下に記すステップでポリシールールのチューニング行います。

6．Web サイトへのアクセスログを確認
7．ルール ID を抽出
8．スキップルールの設定と、ポリシーを拒否モードで動作

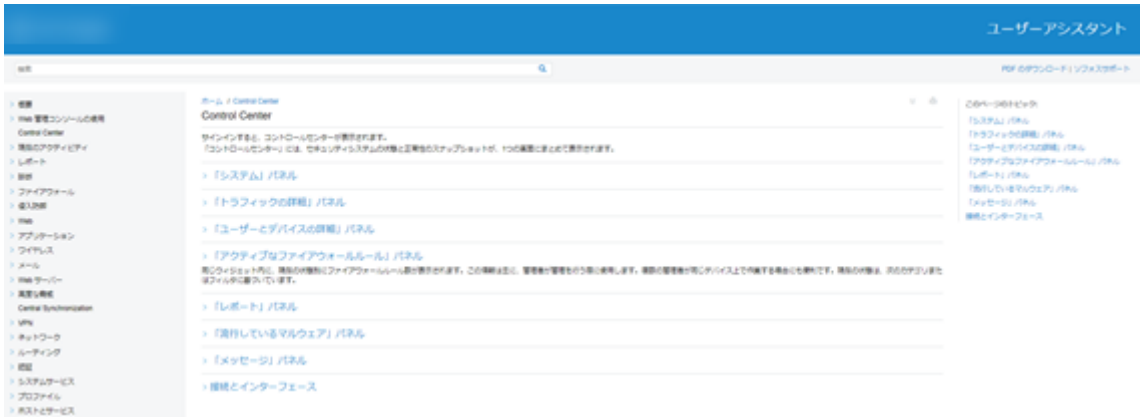
これらを段階的に実施することで、最適な WAF ポリシーを構築することが可能です。

## １０．詳細の機能と設定を知りたい時

Sophos Firewall はヘルプより各画面ごとにユーザーアシスタントへリンクされており、必要なときに必要な個所を閲覧することが可能です。画面の上部フレーム内のヘルプを押下します。




以下のようなユーザーアシスタント（オンラインヘルプ）が別タブで開きます。




以上