

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 かんたん初期導入編

第 4.0 版

2023 年 8 月 31 日



興安計装株式会社

目次

内容

改訂履歴.....	3
はじめに.....	4
1. サービスについて	5
(1) サービス提供内容	5
(2) サービス提供範囲	5
(3) サービス利用条件	6
①ご利用環境	6
②推奨導入構成.....	6
③サイジング	7
(4) サービス利用の流れ	8
①新規ライセンスの取得から利用開始まで.....	8
②ライセンス変更申請	9
③ライセンス終了申請	9
④ライセンス終了申請	9
2. ご利用環境の構成	11
3. Sophos Firewall のライセンス取得方法	12
4. Sophos Firewall の初期展開	14
(1) IP アドレス自動取得 (DHCP) 環境への展開.....	14
(2) IP アドレス手動割当 (ルータ+スイッチ) 環境への展開	21
(3)	ライセンス適用手順
.....	27
5. 初期設定.....	33
5-1. Sophos Firewall の初期設定.....	33
(1) 基本情報変更手順.....	33
(2) 管理者パスワード変更手順.....	35
(3) Shell アクセス設定手順.....	35
(4) Syslog 連携手順.....	42
(5) 固定グローバル IP アドレス割り当て手順.....	45
(6) LAN ゾーンの IP アドレス割り当て手順.....	47

(7) バックアップ取得手順.....	51
(8) リストア手順.....	52
5 – 2. 保護対象システム (WindowsServer2016) の初期設定.....	57
6. さくらのクラウド環境における制約事項	61
①アーカイブ Disk サイズについて.....	61
②Disk 修正について.....	61
③冗長化構成について	61
④バックアップについて.....	61
7. 詳細の機能と設定方法を知りたい時.....	62

改訂履歴

版数	更新日	更新内容	更新者
1.0	2020/4/10	初版作成	興安計装株式会社
1.1	2020/5/20	4. SophosXGFirewall の初期展開 (3) ライセンス適用手順 P.27 SophosCentral アカウントについて注意事項を追記	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版	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版	興安計装株式会社
4.0	2023/8/31	v19.5 アップグレードに伴う改版	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 オンラインヘルプ

<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:保護対象システム（サーバ若しくはクライアント）を Sophos Firewall の配下に展開するまでの初期設定手順をご提供すること。

シンプルに順番に沿って設定を進めて頂くことにより、Sophos Firewall によるシステムの保護に必要な初期構成が可能となります。サブスクリプションにより利用可能となる各種プロテクションの手順については、本手順書には記載しておりません。

1. サービスについて

(1) サービス提供内容

提供項目	内容
Sophos Firewall アーカイブイメージ	一部機能を除き、動作検証及び初期設定が完了した状態のアーカイブイメージを提供します。
Sophos Firewall ライセンス	当社が提供したアーカイブイメージから展開した Sophos Firewall のみが適用可能なライセンスを提供します。

※Sophos XG（対象 SFOS v17、18.0 系）は Sophos Firewall（対象 SFOSv18.5 以降）に名称が変更となりました。

(2) サービス提供範囲

本サービスで提供される Sophos Firewall の機能は以下の通りです。

提供サブスクリプション	機能
Base Firewall	ファイアウォール、VPN、監視・分析機能、基本管理機能
Network Protection	IPS（侵入防御）、RED、ATP
Web Protection	Web マルウェア対策、アプリケーションコントロール
Email Protection	マルウェア対策、スパム対策、ファイル保護、データ保護、SPX 暗号化
Web Server Protection	Web アプリケーションファイアウォール、リバースプロキシ
Zero-Day Protection	機械学習、サンドボックスファイル分析、脅威インテリジェンス

本サービスで提供される Sophos Firewall の詳細機能については Owlook セキュリティマネジメントサービス仕様書内の 3. 提供機能の詳細をご参照ください。

Owlook セキュリティマネジメントサービス仕様書（Sophos Firewall）

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

(3) サービス利用条件

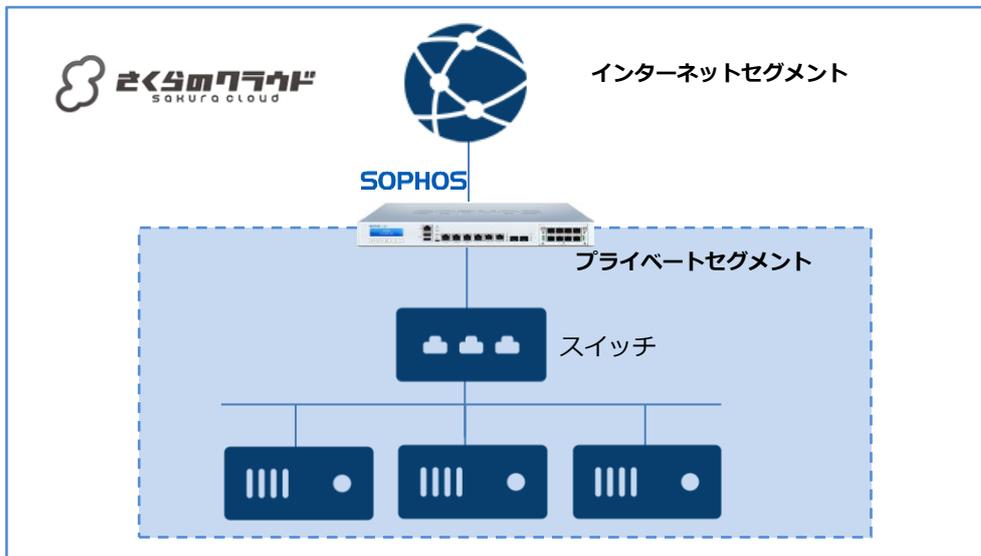
本サービスの利用条件は以下の通りです。

①ご利用環境

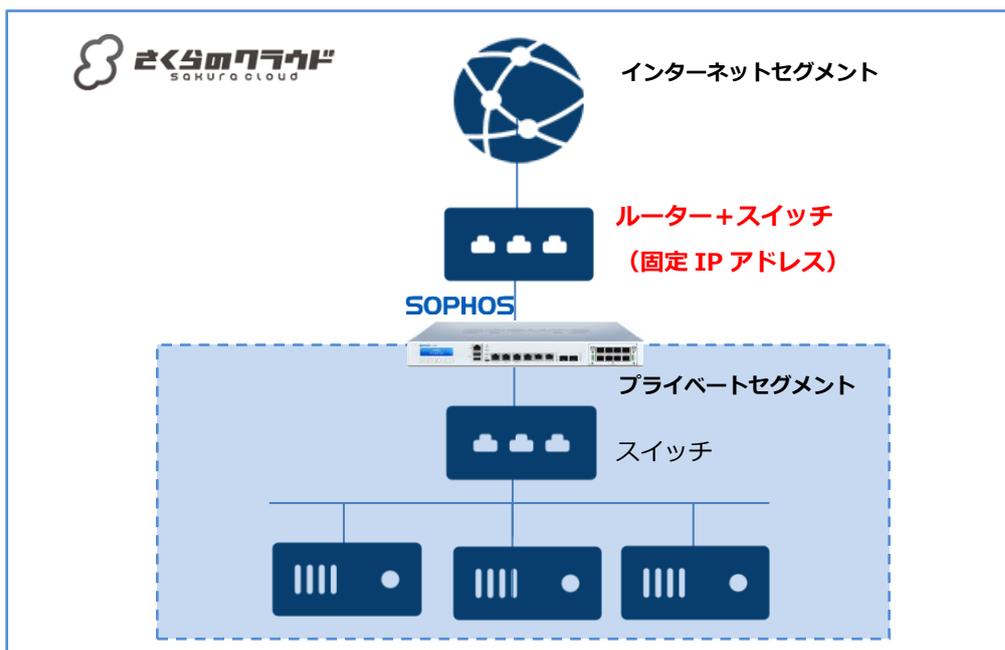
さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

②推奨導入構成

Sophos Firewall はご利用の環境における外部（インターネット）との接続点へ導入し、内部はスイッチを利用しセグメントを構築してください。



また以下のように、ルーター+スイッチ機能で Sophos Firewall へ任意の IP アドレスを設定することが可能です。



③サイジング

本サービスの最小利用要件は以下の通りです。

vCPU	メモリ	NIC	Disk
1Core	4GB	2	100GB※1

※1 Disk サイズはアーカイブイメージで 100GB 固定です。ログの保持容量の拡張は別途 Syslog サーバへの転送機能を推奨します。

さくらのクラウドサービス環境へ展開した場合のスペック目安です。 ※2 ※3

vCPU	2	4	6	8
メモリ(GB)	4	6	8	16
FW スループット (Mbps)	3,850	7,700	39,000	47,000
IPS スループット (Mbps)	1,200	2,500	7,000	10,500
脅威対策スループット (Mbps)	280	720	1,500	2,000
同時接続数	1,600,000	1,600,000	6,500,000	12,260,000
新規セッション (秒)	35,700	61,500	148,000	186,500
IPsec VPN スループット (Mbps)	3,000	4,800	20,500	25,000
SSL/TLS インスペクション スループット (Mbps)	375	650	1,450	2,470
IPsec VPN 同時接続数	500	1,500	5,000	6,500
SSL/TLS 同時接続数	8,192	8,192	18,432	55,296

※2 Sophos より提供される仮想アプライアンスにおける目安のサイズでありパフォーマンスを保証するものではありません。ハイパーバイザーのご利用環境によって最大 10%までのパフォーマンスの低下が予想されます。

※3 表内の数値は Sophos より提供される製品ガイドに基づく指標です。

<https://assets.sophos.com/X24WTUEQ/at/krpwbqq8qgr3bq7knxfpkg/sophos-firewall-brja.pdf>

(4) サービス利用の流れ**①新規ライセンスの取得から利用開始まで**

本サービスご利用までの流れは以下の通りとなります。

No	実施内容	詳細
1	さくらのクラウドサービス アカウント取得	本サービスはさくらのクラウドサービス上で提供可能なサービスとなります。その為、利用者はさくらのクラウドサービスが利用できる状態であることが前提となります。
2	Sophos Firewall の展開	利用者はさくらのクラウド管理コントロールパネルより Sophos Firewall のアーカイブイメージをパブリックアーカイブから展開します。
3	Sophos Firewall 利用ライセンス申請	利用者はさくらのクラウド管理コントロールパネルよりご利用されるライセンス形態を選択し申請します。ライセンス形態については「2. ライセンスについて」をご参照ください。
4	利用規約へ同意	利用者はさくらのクラウド管理コントロールパネルより表示される URL より利用規約を確認し、同意頂きます。
5	ライセンスの払い出しと 有効化	利用者宛にライセンス（シリアルコード）が送付されます。送付はさくらのクラウドでご登録いただいたメールアドレス宛に送付されます。利用者はライセンスを Sophos Firewall へ入力しアクティベートを行います。※詳細手順については「ご利用開始ガイド」をご参照ください。
6	管理サーバーへの接続	Sophos Firewall へ当社が提供する管理サーバへの接続設定を行います。管理サーバへの接続が一定期間確認できない場合、ライセンスが無効化される場合があります。
7	利用開始	Sophos Firewall の機能がご利用いただけるようになり、利用者にて設定が可能となります。

②ライセンス変更申請

サービスのライセンス変更申請の流れは以下の通りとなります。

No	実施内容	詳細
1	Sophos Firewall ライセンス変更申請	利用者はさくらのクラウド管理コントロールパネルより変更したいライセンス形態を申請します。ライセンス形態については「2. ライセンスについて」をご参照ください。
2	ライセンスの変更反映	申請が受理されると当日中にライセンスの変更内容が反映されます。※通信環境により変更反映まで最大 4 時間程度かかります。
3	Sophos Firewall の 同期処理	利用者は Sophos Firewall よりライセンスサーバとの同期を行います。※詳細手順については「ご利用開始ガイド」をご参照ください。

※FullGuard ライセンスは FullGuard Plus に統合され、さくらモデルの 1 種類のみ提供となっております。

③ライセンス終了申請

本サービスのライセンス終了申請はさくらのクラウド管理コントロールパネルより利用停止の申請を行います。申請が受領次第ライセンスが無効化されます。

④ライセンス種別

本サービスで提供される Sophos Firewall 利用ライセンスはパブリックアーカイブから展開されるインスタンスサイズによって分類されます。

vCPU	メモリ
1C	4GB
2C	4GB
4C	6GB
6C	8GB
8C	16GB

展開されたインスタンスサイズが上記の分類と異なる場合、Sophos Firewall が認識するリソースは提供されるライセンスのリソースが上限となります。インスタンスのサイズを包括するライセンスの申請をお願いします。

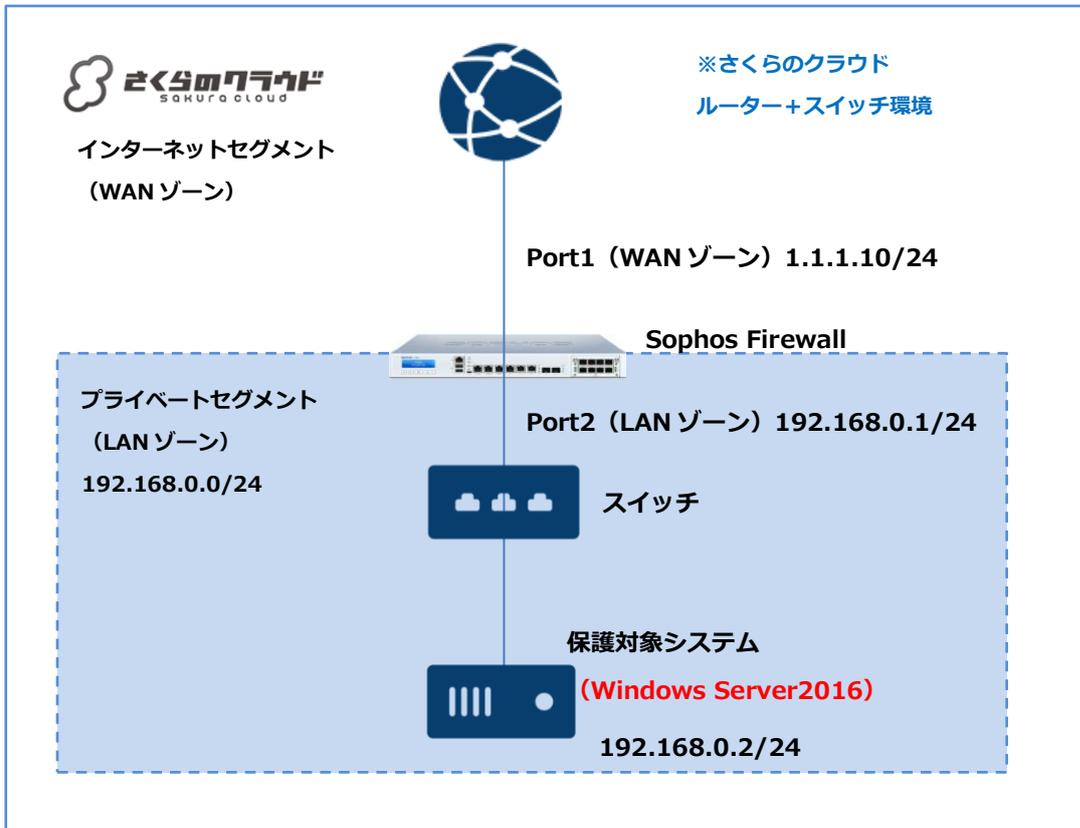
例：インスタンスサイズが 2C6GB、ライセンスが 1C4GB だった場合、Sophos Firewall は 1C4GB と認識します。

本サービスで提供されるライセンスでご利用いただけるサブスクリプションタイプは以下の通りです。

機能 \ 種別	さくらモデル
Base Firewall	○
Network Protection	○
Web Protection	○
Email Protection	○
WebServer Protection	○
Zero-Day Protection	○

2. 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 1.1.1.10 のグローバル IP アドレスを持ちます。
- 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 192.168.0.2/24 を持ちます。
- 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。

※IP アドレス等、設定値については、それぞれの環境に読み替えてご参照ください。

3. Sophos Firewall のライセンス取得方法

①リソースマネージャ > マーケットプレイス > 作成を押下します。



②必要な情報を入力し作成を押下します。

ライセンス : Sophos 関連製品

ライセンス数 : 必要数を選択

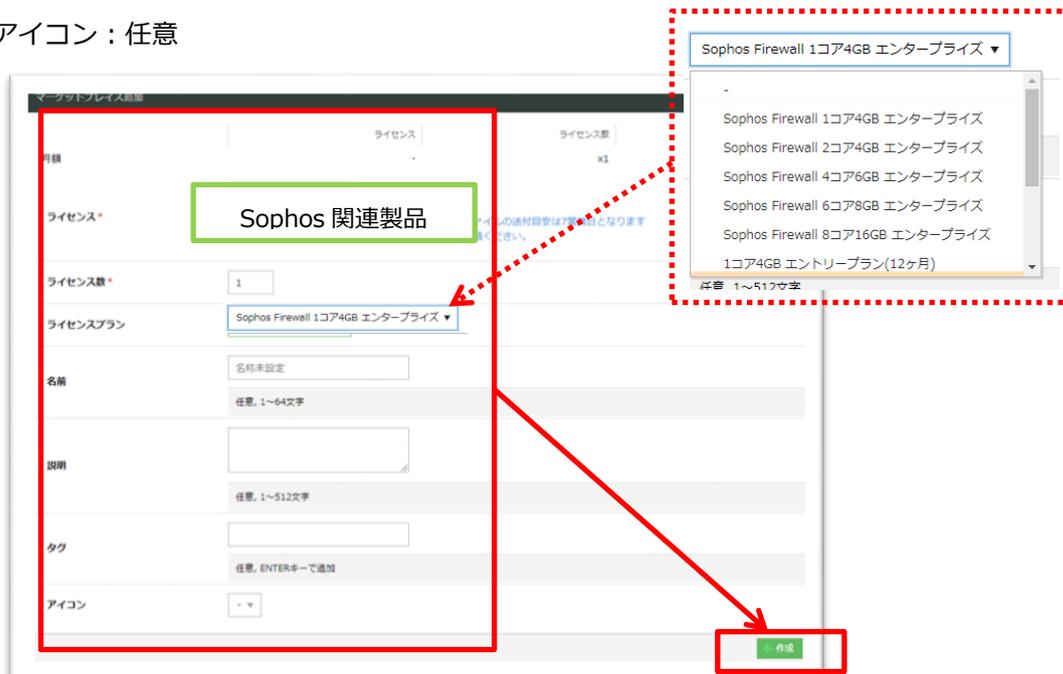
ライセンスプラン : コア数に応じて選択

名前 : 任意

説明 : 任意

タグ : 任意

アイコン : 任意



③サービス利用規約をお読みいただき、同意するをチェックし作成を押下します。

操作確認 ×

マーケットプレイス追加

作成にあたり以下についてご確認のうえ、同意していただく必要があります。

・製品使用許諾、個人情報の取扱いについて

本サービス申込前に、Sophos Firewall製品使用許諾契約の同意が必要となります。

URL : <https://manual.sakura.ad.jp/cloud/marketplace/sophos/sfos-ready.html#id6>

上記をご確認の上、同意するにチェックをお願いいたします。

同意する

・マーケットプレイス約款の同意

本サービス申込前に、マーケットプレイス約款の確認、同意が必要となります。

URL : <https://www.sakura.ad.jp/agreement/>

上記をご確認の上、同意するにチェックをお願いいたします。

同意する

キャンセル 作成

コントロールパネルからお申込後ライセンスファイルの送付目安は7営業日となります。サービスの解約は、さくらインターネット会員メニュー内のお問合せよりご連絡ください。

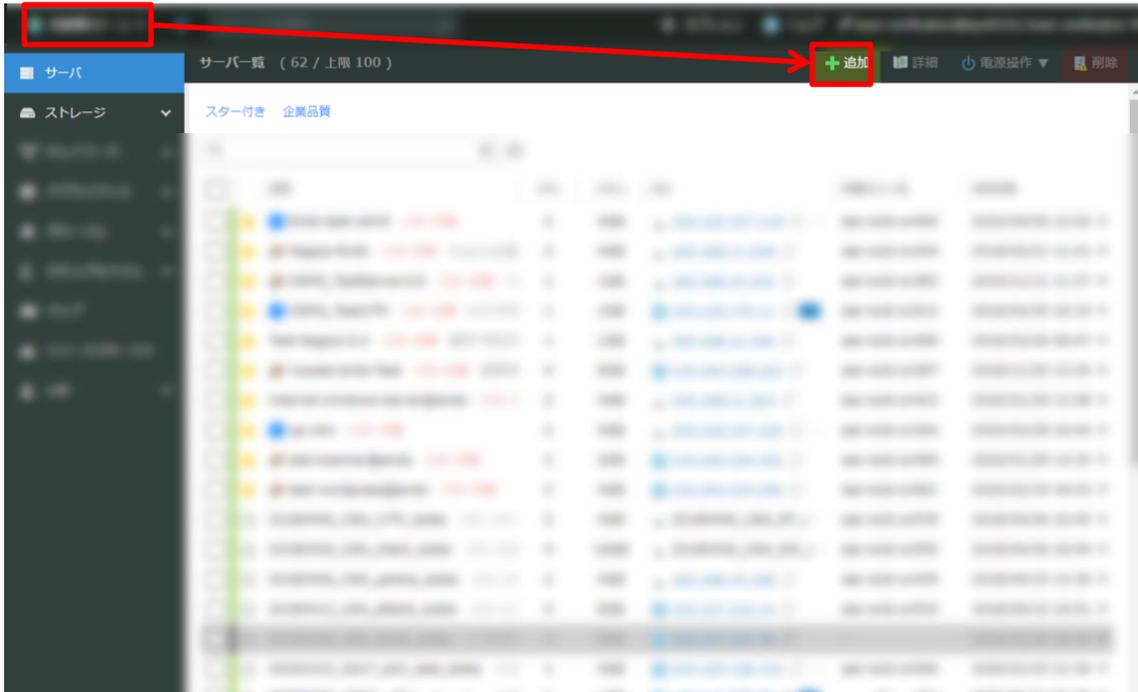
ライセンス取得方法は以上です。

4. Sophos Firewall の初期展開

(1) IP アドレス自動取得 (DHCP) 環境への展開

インターネット側 (WAN ゾーン) の IP アドレスが自動的に割り当てられる環境の展開手順です。

① 展開先のゾーンを選択し、「追加」ボタンを押下します。



② 適切なサーバプランを選択します。



- ③ 適切なディスクプランを選択し、アーカイブから Sophos Firewall のアーカイブを選択します。

● 新規ディスクを作成 ○ 既存ディスクを接続 ○ ディスクレス (なし)

ディスクプラン
● SSDプラン ○ 標準プラン

ディスクソース
● アーカイブ ○ マイアーカイブ ○ マイディスクをコピー ○ ブランク (空のディスク)

さくらにて用意した初期設定済みOSイメージはアーカイブとして提供されています

アーカイブ選択

Sophos Firewall

ディスク

・サーバ、ディスク料金その他、オプション(マーケットプレイス)にてライセンスの購入が必要となります。
[オプション\(マーケットプレイス\)申込画面](#)
・サーバを作成後、GUI操作によりライセンスファイルをインポート、必要に応じた初期設定を行ってください
・初期設定されているユーザ名は「admin」です。
初期パスワードは 2o1Y1m5S50 をご利用ください。
こちらは100GB固定サイズのアーカイブです。
100GBのディスクにインストールしてお使いください。

- ④ 適切なディスクサイズを選択します。

ディスクサイズ

100GB ▼

別のストレージに収容する

指定されたディスクとは別のストレージにディスクを作成します

準仮想化 モードを使う (Virtio)

有効にすると、ディスクアクセスが高速になります。別途ドライバが必要になる場合があります。

- ⑤ Sophos Firewall に自動的にグローバル IP アドレスを割り当てる場合、インターネットに接続を選択します。



Sophos Firewall に手動でグローバル IP アドレスを割り当てる場合は、ルータ+スイッチに接続する必要があります。スイッチに接続を選択します。



Sophos Firewall に手動で IP アドレスを割り当てる場合、「5 - 1. Sophos Firewall の初期設定 (5) 固定グローバル IP アドレス割り当て手順」を必ず行ってください。

- ⑥ Sophos Firewall のアーカイブに対し、ディスク修正は利用できません。



⑦シンプル監視は任意で有効にします。

5. シンプル監視 シンプル監視を有効にする
作成するサーバにシンプル監視を適用します。無料でご利用いただけます。

⑧サーバの情報は任意の内容で入力します。

6. サーバの情報

名前
1~61文字
サーバを一括作成した場合は、ホスト名、リソース名の後ろに連番が付与されます (例: hostname-01, hostname-02...)

説明
1~512文字

タグ
...

アイコン
...

⑨作成後すぐに起動のチェックを外します。

その他のオプション

仮想サーバ上のキーボードをUS配列として設定する* (@keyboard-usタグ)

*: 仮想サーバ上の設定に合わせてください

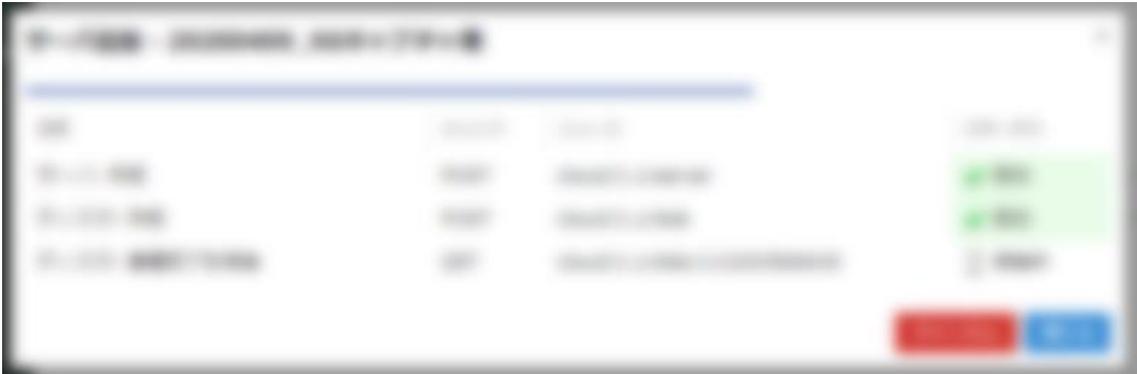
作成後すぐに起動

⑩作成ボタンを押下します。

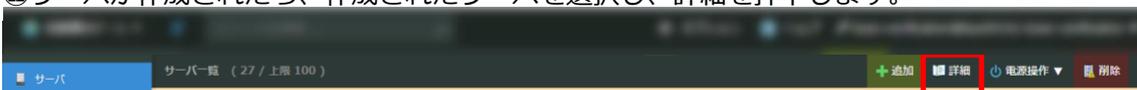
作成数 * 1

作成

⑪サーバの追加プロセスが開始されます。



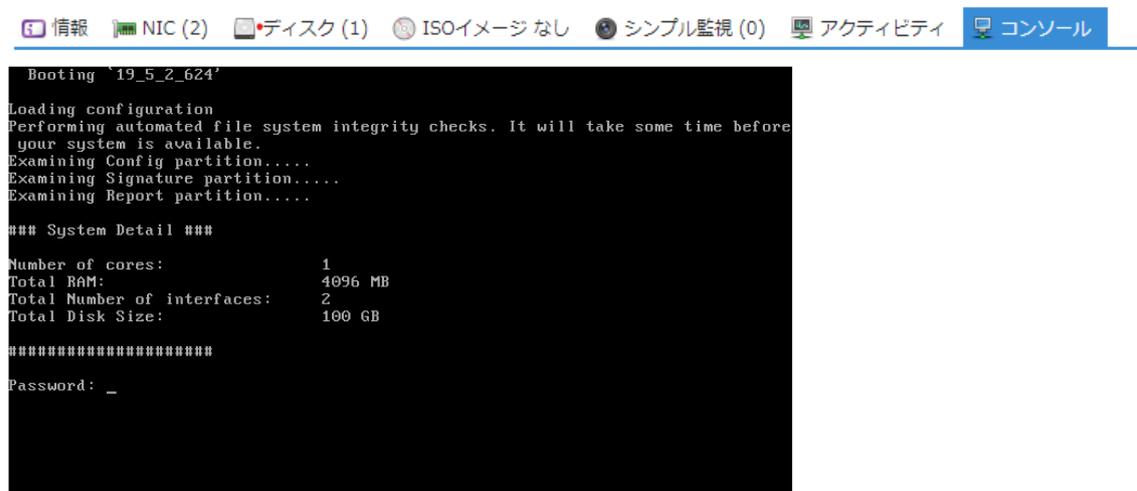
⑫サーバが作成されたら、作成されたサーバを選択し、詳細を押下します。



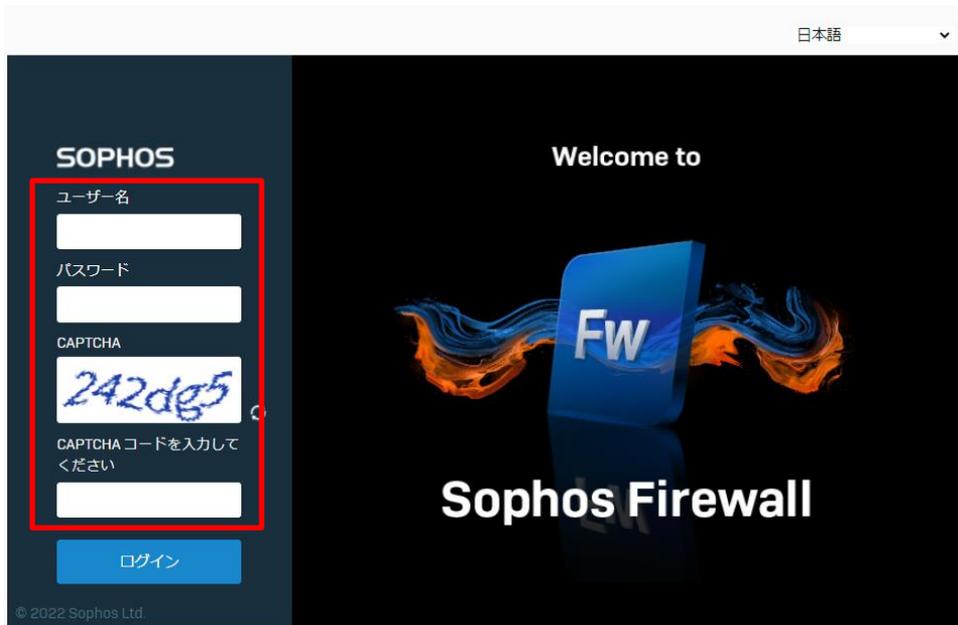
⑬NIC タブより追加ボタンを押下し、NIC を追加します。※Sophos Firewall の起動要件として NIC が2つ必要となります。



⑭電源操作より起動を押下し、Sophos Firewall を起動させます。以下の画面は「コンソール」表示です。



⑭自動的に割り当てられたグローバル IP アドレスを確認し、ブラウザより https:// (IP アドレス) :4444 でアクセスします。

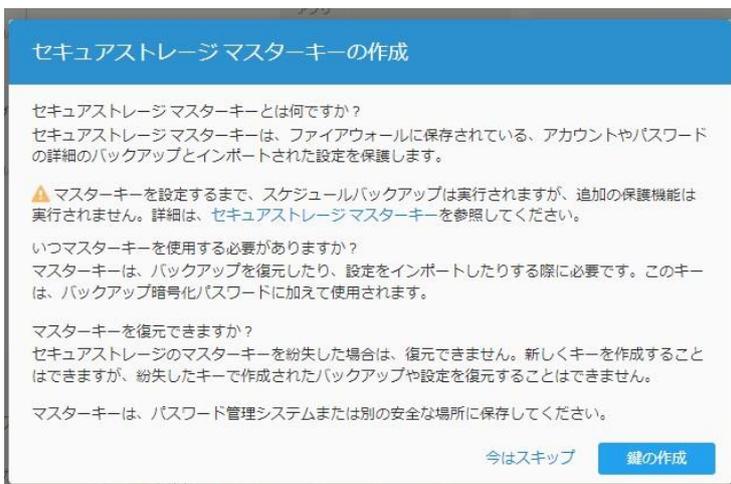


⑮ユーザ名とパスワードは以下の通りです。ランダムなワンタイム文字コードも入力します。

admin
9T23y!1s55

admin アカウントでログインします。

⑯ログイン直後、ストレージマスターキーの作成を求められるますが、「今はスキップ」を押下します。



⑩管理 > ライセンス タブより「ここをクリック」を押下しライセンスの登録画面に遷移します。ファイアウォールの登録画面が表示されます。



以上で、IP アドレス自動取得 (DHCP) 環境への展開手順は完了です。

(2) IP アドレス手動割当 (ルータ+スイッチ) 環境への展開

インターネット側に任意の IP アドレスを割り振る環境での展開手順です。

※ (1) 共有セグメントへの展開手順①~④まで同様です。

※Sophos XG Firewall アーカイブを展開する際に、ルータ+スイッチへの接続が前提となります。

本手順書の環境

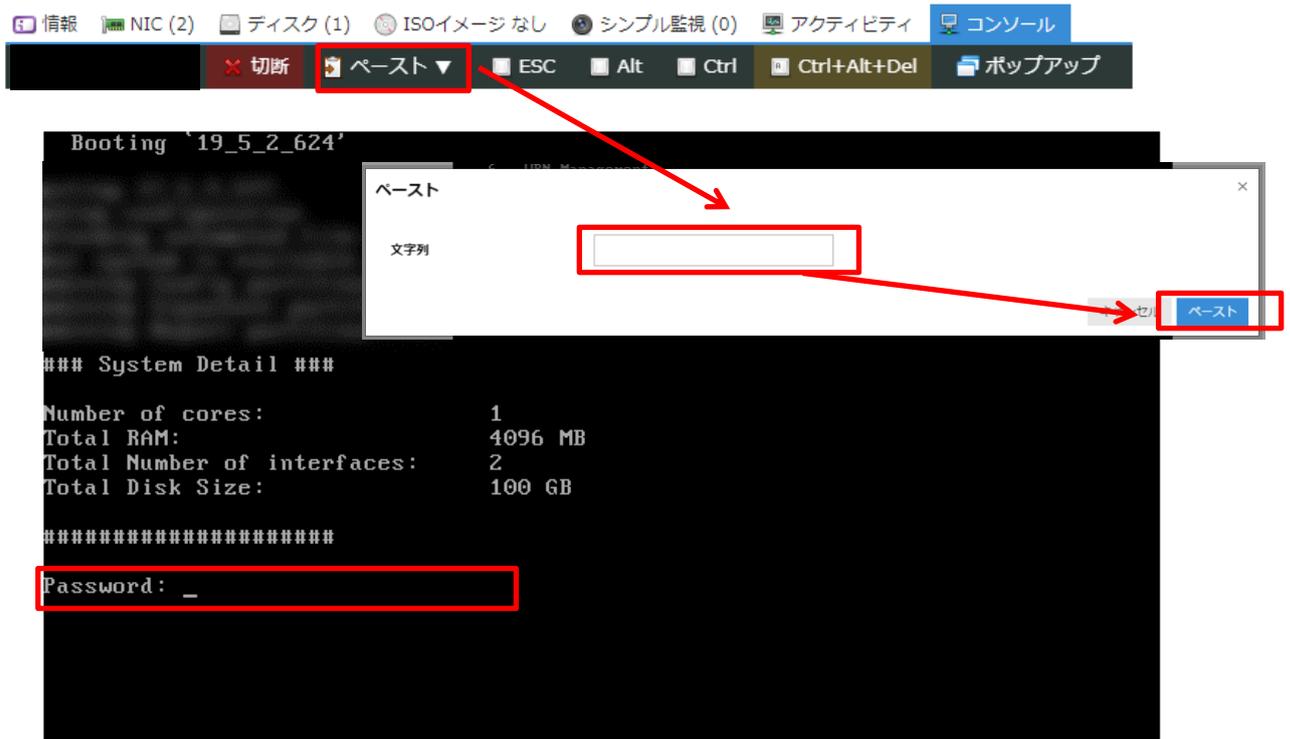
■割り当てたい IP アドレス : 1.1.1.10/24

■デフォルトゲートウェイ : 1.1.1.1/24

①コンソールタブに切り替え、以下のパスワードでログインします。

9T23y!1s55

※キー配列は US 配列です。配置がわからない場合、ペースト機能をご利用ください。



②ログイン後、「5. Device Management」を選択するため、Select Menu Number で「5」を選択します。

```
Main Menu
AA. Device Activation
 1. Network Configuration
 2. System Configuration
 3. Route Configuration
 4. Device Console
 5. Device Management
 6. UPN Management
 7. Shutdown/Reboot Device
 0. Exit

Select Menu Number [0-7]:
```

③「3. Advanced Shell」を選択するため、Select Menu Number で「3」を選択します。

```
Device Management
 1. Reset to Factory Defaults
 2. Show Firmware(s)
 3. Advanced Shell
 4. Flush Device Reports
 0. Exit

Select Menu Number [0-4]: _
```

- ④ Advanced Shell に画面が遷移します。

```
Sophos Firewall
=====
(C) Copyright 2000-2023 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For Sophos End User Terms of Use - https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use.aspx

NOTE: If not explicitly approved by Sophos support, any modifications
done through this option will void your support.

SF01U_SD01_SFOS 19.5.2 MR-2-Build624# _
```

- ⑤ Advanced Shell では、IP アドレスとデフォルト GW の設定をコマンドラインで行います。

- 割り当てたい IP アドレス : 1.1.1.10/24
- デフォルトゲートウェイ : 1.1.1.1/24

```
#ifconfig Port1 1.1.1.10 netmask 255.255.255.0
#route add default gw 1.1.1.1
#exit
```

※記載の IP アドレスはサンプルです。実際の環境に置き換えて捜査ください。

- ⑤ 「Device Management」を Exit するため、Select Menu Number で「0」を選択します。

```
Sophos Firmware Version: SFOS 19.5.2 MR-2-Build624
Model: SF01U
Hostname: sakura_sophos_firewall_v19.5

Device Management

  1. Reset to Factory Defaults
  2. Show Firmware(s)
  3. Advanced Shell
  4. Flush Device Reports
  0. Exit

Select Menu Number [0-4]:
```

- ⑥ 「Main Menu」を Exit するため、Select Menu Number で「0」を選択します。

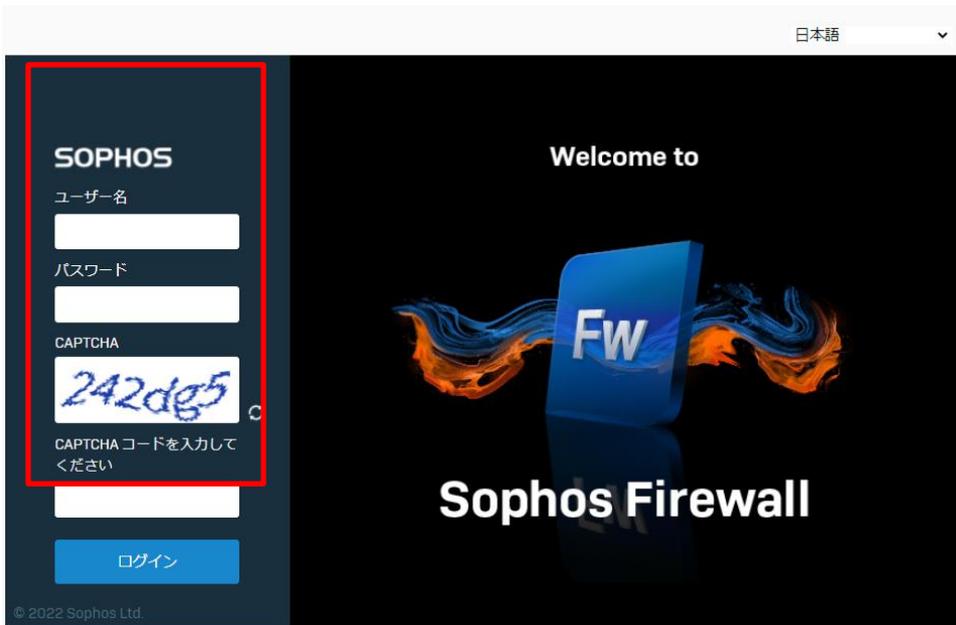
```
Sophos Firmware Version: SFOS 19.5.2 MR-2-Build624
Model: SF01U
Hostname: sakura_sophos_firewall_v19.5

Main Menu

AA. Device Activation
  1. Network Configuration
  2. System Configuration
  3. Route Configuration
  4. Device Console
  5. Device Management
  6. UPN Management
  7. Shutdown/Reboot Device
  0. Exit

Select Menu Number [0-7]: _
```

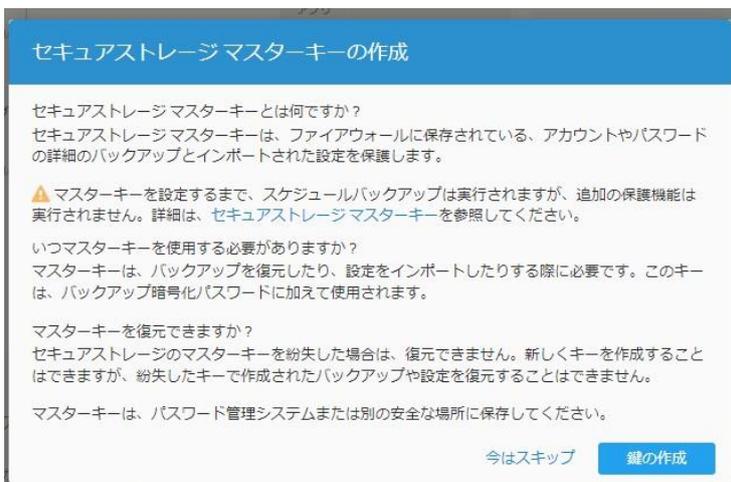
⑦割り当てたグローバル IP アドレスを確認し、ブラウザより https:// (IP アドレス) :4444 でアクセスします。



⑧admin アカウントでログインします。ユーザ名とパスワードは以下の通りです。ランダムなワンタイム文字コードも入力します。

admin 9T23y!1s55

⑩ログイン直後、ストレージマスターキーの作成を求められるますが、「今はスキップ」を押下します。



⑨管理 > ライセンス タブより「ここをクリック」を押下しライセンスの登録画面に遷移します。ファイアウォールの登録画面が表示されます。



以上で、IP アドレスの手動割り当て展開手順は完了です。

(3) ライセンス適用手順

①取得したライセンスを「既存のシリアル番号がある」へ入力し、次へを押下します。

ファイアウォールの登録

ファイアウォールには、シリアル番号が必要です。自動的にシリアル番号を取得します。未使用のシリアル番号がある場合は、それを指定することもできます。

既存のシリアル番号がある

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

いったんファイアウォールを登録すると、シリアル番号を変更することはできません。シリアル番号が2つ以上ある場合は、正しいものを選択するようにしてください。ホームユーザーの方は、XG Firewall Home Edition のシリアル番号をここから入手して使用するようにしてください。

シリアル番号がない (試用を開始)

自動的にシリアル番号が発行され、30日間試用することができます。この期間の間、Sophos XG Firewall の全機能を試用することが可能です。自宅で使用の場合は、このオプションを使用しないでください。

UTM 9 のライセンスを今すぐ移行する

[参照](#)

シリアル番号が自動的に発行されます。UTM 9 の同等ライセンスが変換され、XG Firewall に適用されます。

いったん変換すると、元に戻すことはできません。今すぐ移行しない場合は、「試用を開始」をクリックしてください。XG Firewall を試用してから、ライセンスを移行することができます。

今は登録しない

この場での登録をスキップできます。次にログインしたときに、登録を促すメッセージが表示されます。登録しないまま、後 0 日間使用することができます。

[次へ](#)

基本設定が完了しました

基本設定が完了しました。ファイアウォールを次のライセンスで登録しました。

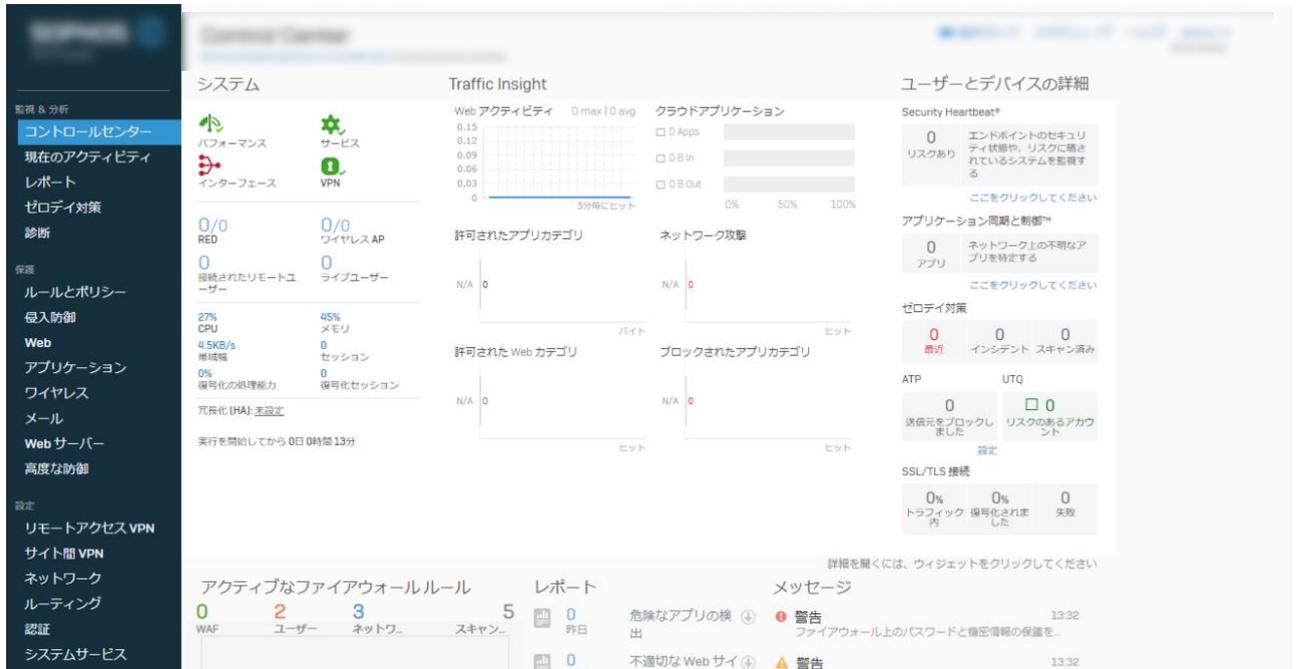
ライセンス登録サブスクリプション: Xstream Protection with WAF and Email MSP /バンドル。
ここで選択したサブスクリプションの詳細は、後ほど「管理 > ライセンス」で確認できます。

サブスクリプション名	ステータス	有効期限
Xstream Protection with WAF and Email MSP /バンドル	有効	2023/10/01 - 2024/10/01
...

[ライセンスの追加](#)

[続行](#)

②ライセンス適用後、「Control Center」に遷移します。



⑦ 「Sophos Central」メニューに遷移し登録ボタンを押下します。

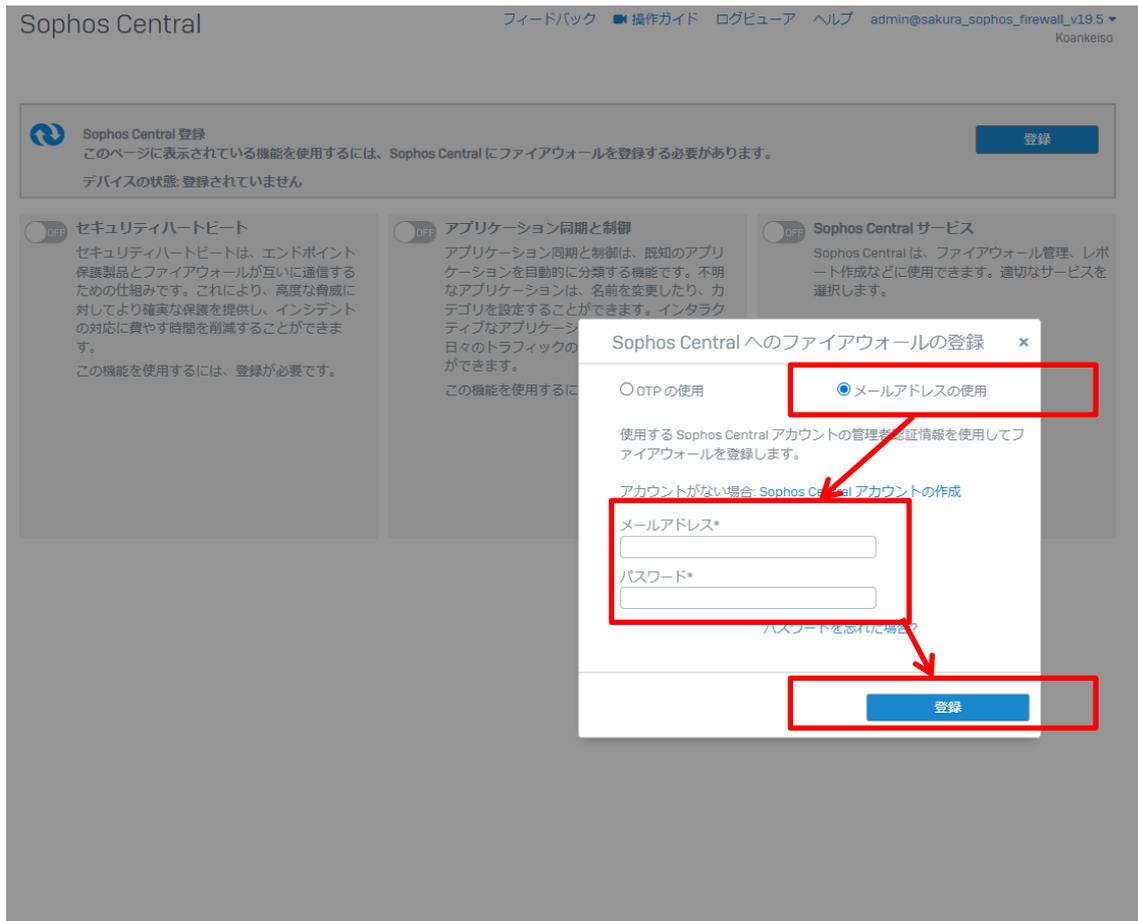


⑧ 「Sophos Central へのファイアウォールの登録」画面がポップアップで表示されます。

以下のメールアドレスとパスワードで登録を行います。

sophos-support@sakura.ad.jp
Wz9HEEjWqjNF

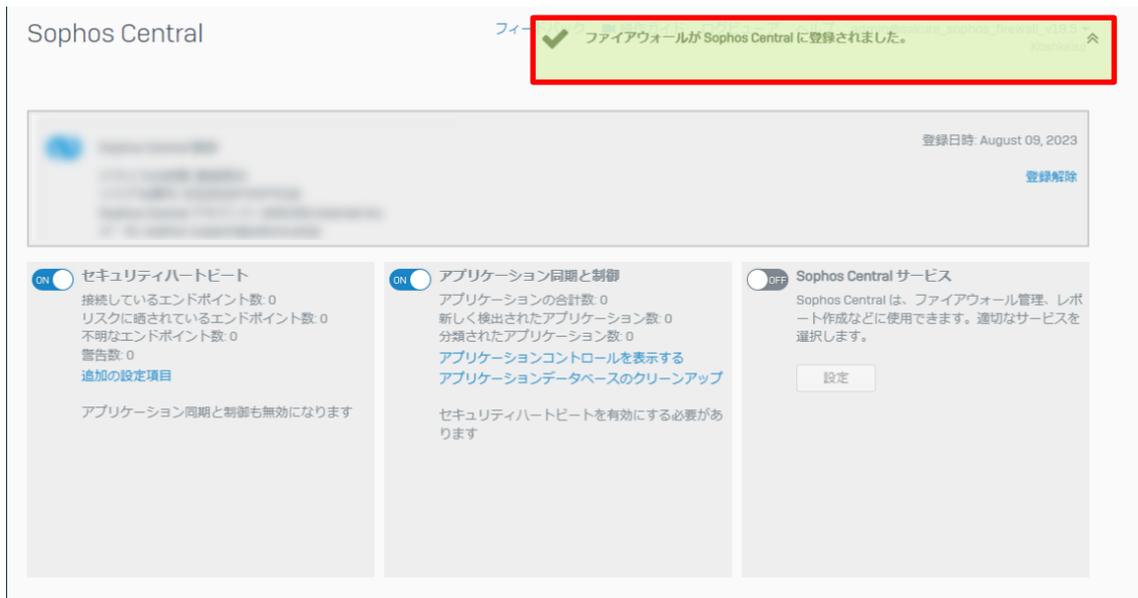
※記載された Sophos Central アカウントは本サービスのみで有効なアカウントです。本サービス以外では SophosCentral サービスをご利用いただく事は出来ませんのでご注意ください。



※本手続きを行わなかった場合、また上記メールアドレス以外でのご登録頂いた場合、当社からのアクティベート確認が取れないため、一定期間後にライセンスが無効になりますのでご注意ください。

⑨ 下記ポップアップが表示され、正しく登録されたことを確認します。

※同時に有効化される「セキュリティハートビート」、「アプリケーション同期と制御」は、エンドポイントとの連携となります。本サービスではこの機能含め Sophos Central から提供されるすべてのサービスをご利用いただけません。



⑩この登録作業をもって正しくライセンスをご利用いただく事ができます。「管理」よりライセンスの状況が確認する事ができます。

The screenshot shows the Sophos management console interface. On the left is a dark sidebar with a menu. The '管理' (Management) option is highlighted with a red box and a red arrow. The main content area is titled '管理' and has a sub-menu with 'ライセンス' (Licenses) selected. Below this is a table of licenses:

	ステータス	有効期限日
Xstream Protection with WAF and Email MSP bundle		
ベースファイアウォール ステートフルファイアウォール、VPN、ワイヤレス	登録済み	Dec 31, 2999
ネットワークプロテクション IPS、ATP、SD-RED デバイス管理	登録済み	Dec 31, 2999
Web プロテクション Web セキュリティおよび制御、アプリケーション制御、Web マルウェア対策	登録済み	Dec 31, 2999
メールプロテクション スパム対策、マルウェア対策、DLP、暗号化、メールマルウェア対策	登録済み	Dec 31, 2999
Web サーバードテクション Web アプリケーションファイアウォール	登録済み	Dec 31, 2999
ゼロデイ対策 機械学習、サンドボックスファイル分析、脅威インテリジェンス	登録済み	Dec 31, 2999
Central オークストレーション SD-WAN VPN オークストレーション、CFR Advanced	登録済み	Dec 31, 2999
拡張サポート 拡張サポート	登録済み	Dec 31, 2999

Below this table is another section for '個別のサブスクリプションモジュール' (Individual Subscription Modules):

	ステータス	有効期限日
拡張プラスサポート 拡張プラスサポート	未登録	-

以上で、ライセンス適用手順は完了です。

(参考) セキュアストレージマスターキーの生成

①任意のタイミングで再ログイン後にセキュアストレージマスターキーの生成が求められます。鍵の作成を押下します。

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

②セキュアストレージマスターキーを設定し、「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。」にチェックし鍵の作成を押下します。

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: 入力されていません

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

セキュアストレージマスターキーは必ず作成し厳重に保存してください。

5. 初期設定

5-1. Sophos Firewall の初期設定

(1) 基本情報変更手順

ここでは Sophos Firewall ホスト名、管理者メールアドレス変更を行います。

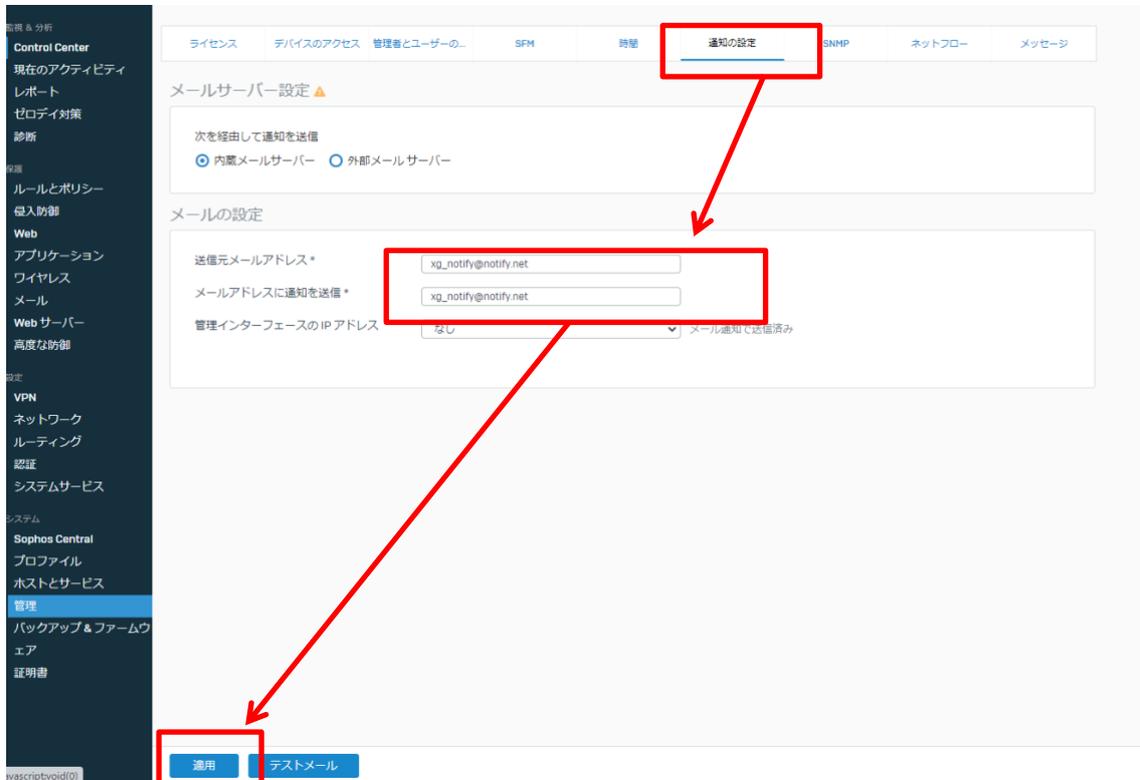
①管理 > 管理者とユーザの設定 タブを押下、ホスト名を入力、適用ボタンを押下します。

The screenshot shows the Sophos Firewall management console interface. On the left is a dark sidebar with a menu. The 'Management' (管理) option is highlighted with a red box. The main content area is titled 'Host Name' (ホスト名) and contains several configuration fields:

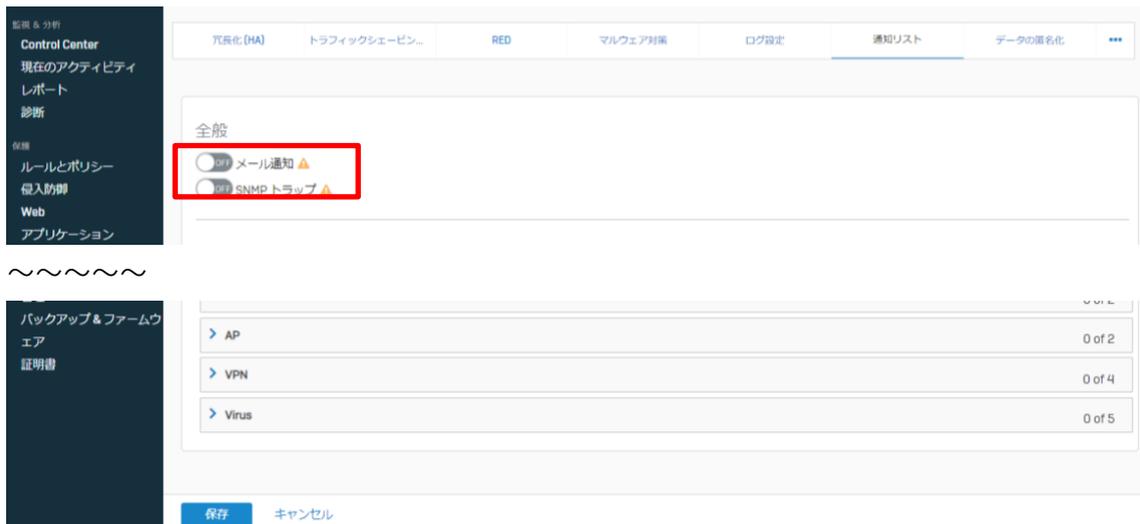
- Host Name:** A text input field with a red box around it.
- Description:** A text area with the placeholder text '説明を入力'.
- Buttons:** A blue '適用' (Apply) button is highlighted with a red box.
- Management Console and End User Operations:** A section containing:
 - Management Console HTTPS Port: 4444
 - User Portal HTTPS Port: 443
 - Certificate: A dropdown menu set to 'ApplianceCertificate'.
 - Options for redirecting CAPTIVE portal:
 - Use the host name set in the firewall: sakura_sophos_firewall_v18.5
 - Use the IP address of the initial internal interface: 172.16.16.16
 - Use a different host name: Enter value
 - A blue '設定内容を確認する' (Check settings) button.
 - A blue '適用' (Apply) button at the bottom.

Red arrows indicate the navigation path: from the 'Management' menu item to the 'Management and User Settings' tab, then to the 'Host Name' input field, and finally to the 'Apply' button.

②管理 > 通知の設定 タブを押下しメールアドレスに通知を送信に通知先としたいメールアドレスを入力し、適用を押下します。テストメールを送ることも可能です。



③システムサービス >通知リスト タブをメール通知を ON にし、画面下部の適用ボタンを押下します。この設定により各種アクションによるメール通知が有効になります。



(2) 管理者パスワード変更手順

①管理 > デバイスのアクセス > デフォルトの管理者パスワードの設定よりパスワードを変更し適用を押下します。

The screenshot shows the Sophos Firewall management console. The left sidebar contains a navigation menu with '管理' (Management) highlighted. The main content area is titled 'デバイスアクセス' (Device Access) and includes a 'ローカルサービス ACL' (Local Services ACL) table and a 'デフォルト管理者のパスワードの設定' (Default Administrator Password Settings) form. The form contains fields for 'ユーザー名' (admin), '現在のパスワード' (password), '新しいパスワード' (password), and '確認パスワード' (confirm password). A red box highlights the 'デフォルト管理者のパスワードの設定' section, and a red arrow points to the '適用' (Apply) button below it.

ゾーン	HTTPS	SSH	AD SSO	キャプティブポータル*	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web プロキシ	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									

管理者パスワードの変更は必ず行うようお願いいたします。

(3) Web 管理コンソールのアクセス制御手順

Sophos Firewall はインターネットを通じて WAN 側のインターフェースを経由して管理コンソールにアクセスします。Sophos 社は、あらゆる攻撃の可能性を減らすために、すべての WAN ソース (インターネット全体) からの Web 管理コンソールへのアクセスをオフにすることを推奨されています。よってさくらのクラウド環境でご利用の場合、特定の IP アドレス (もしくはネットワーク) を許可設定し、WAN から Web 管理コンソールへのアクセスを制御することが推奨されます。

ご利用環境に合わせて、Web 管理コンソールにアクセスする IP アドレス、もしくはネットワークの情報をご準備ください。

- ① 管理 > デバイスのアクセス > ローカルサービス ACL の例外ルール より既定の設定である「webadmin」を押下します。

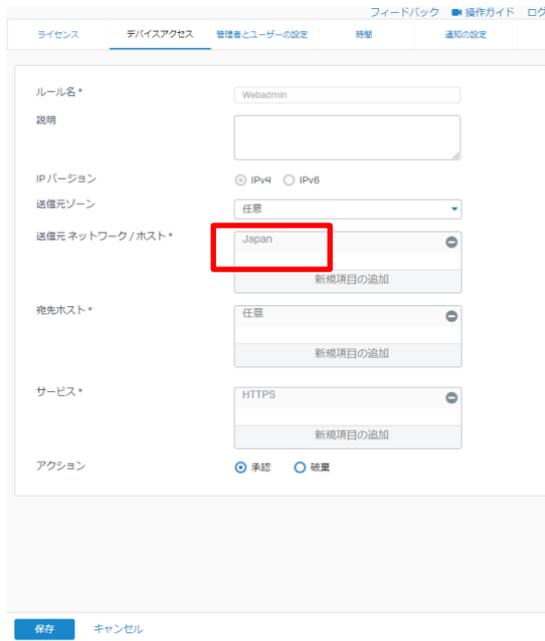
The screenshot shows the Sophos Firewall management console. The left sidebar contains navigation menus. The main content area is titled '管理' (Management) and shows the 'ローカルサービス ACL' (Local Services ACL) configuration. The 'デバイスアクセス' (Device Access) menu item is highlighted in the top navigation bar. The 'ローカルサービス ACL' table shows various services and their status for different zones. The 'Webadmin' rule is highlighted in the 'ローカルサービス ACL の例外ルール' (Local Services ACL Exception Rules) section.

ゾーン	管理サービス				認証サービス				ネットワークサービス				その他のサービス			
	HTTPS	SSH	AD SSO	キャプティブポータル*	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web プロキシ	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>									

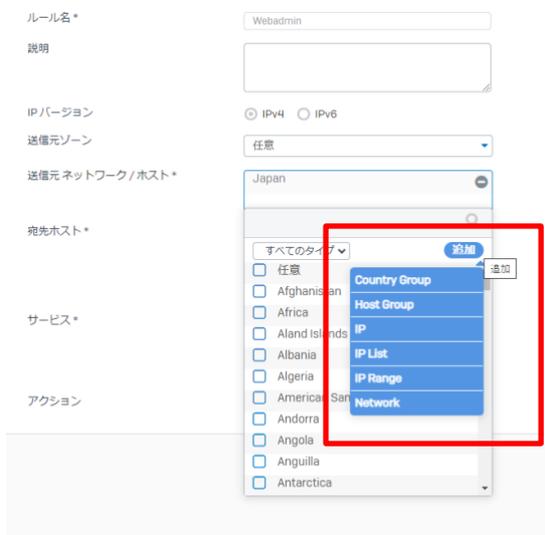
ローカルサービス ACL の例外ルール

ルール名	IPバージョン	追加	管理
Webadmin	IPv4	<input type="button" value="追加"/>	<input type="button" value="管理"/>

② 現状では日本国内のアクセスをすべて許可している設定です。



③ 「送信元ネットワーク/ホスト」の設定箇所から「追加」を押下すると、以下のよう
に Country Group、Host Group、IP、IP List、IP Range、Network と表示されます。最低
限のセキュリティ確保の観点から、本手順では「IP」の設定について記載します。



③ 「IP」を押下するとポップアップウィンドウが表示されます。

この画面から以下の通り設定します。

- ・名前：設定するうえでの登録名です。登録後は左メニューの「ホストとサービス」から確認できます。

- ・IPバージョン：IPv4 限定です。設定変更はできません。

- ・種類：登録種類を選ぶことができます。キャプチャ画面では IP アドレスを入力していません。

- ・IP アドレス：アクセスを許可したい IP アドレスを入力します。

入力が完了したら「保存」ボタンを押下します。

④ 入力が完了すると、「送信元ネットワーク/ホスト」に追加されます。このままでは「Japan」の Country Group が残ってしまうので、「-」ボタンで「Japan」を削除します。

送信元 ネットワーク/ホスト*

- ⑤ 設定が完了したら「保存」を押下します。保存されたタイミングでアクセス制御が有効となるので注意してください。

The screenshot shows the configuration page for a rule named 'Webadmin'. The tabs at the top are 'ライセンス', 'デバイスアクセス', '管理者とユーザーの設定', '時間', and '通知の設定'. The 'デバイスアクセス' tab is active. The configuration fields are as follows:

- ルール名*: Webadmin
- 説明: (Empty text area)
- IPバージョン: IPv4 IPv6
- 送信元ゾーン: 任意
- 送信元 ネットワーク/ホスト*: Web管理コンソールへアクセスで... (with a '新規項目の追加' button below)
- 宛先ホスト*: 任意 (with a '新規項目の追加' button below)
- サービス*: HTTPS (with a '新規項目の追加' button below)
- アクション: 承認 破棄

At the bottom left, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel). The '保存' button is highlighted with a red rectangular box.

(4) Web 管理コンソールにアクセスできなくなった場合の復旧方法

- ① さくらのクラウドコントロールパネルより、「コンソール」画面に遷移しログインします。

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SFU1C4MSP
Hostname: sakura_sophos_firewall_v19.5

Main Menu

 1. Network Configuration
 2. System Configuration
 3. Route Configuration
 4. Device Console
 5. Device Management
 6. UPN Management
 7. Shutdown/Reboot Device
 0. Exit

Select Menu Number [0-7]: _
```

- ② 「4」を入力、Enter を押下し、「4.Device Console」に遷移します。

```
Sophos Firmware Version: SFOS 19.5.3 MR-3-Build652
Model: SFU1C4MSP
Hostname: sakura_sophos_firewall_v19.5

console>
```

- ③ system appliance_access enable と入力し Enter を押下します。

```
console> system appliance_access enable
This will override the configured Appliance Access and allow access to all the s
ervices. All internet traffic will be dropped.
Appliance access enabled.
console> _
```

すべての設定が上書きされ、アクセスが可能となります。

- ④設定が復旧出来たら、この画面から system appliance_access disable と入力し Enter を押下します。すべてアクセス可能な状態から、Web 管理コンソールからアクセス制御の設定が効いた状態となります。

```
console> system appliance_access disable
Appliance access disabled.
console> _
```

exit コマンドで Console 画面を終了させます。

(5) Syslog 連携手順

Syslog サーバは利用者にて用意する必要があります。本手順は必要な場合のみ実施してください。

① システムサービス > ログ設定タブより Syslog サーバ追加を押下します。

The screenshot shows the Sophos Firewall management console. On the left is a navigation menu with 'システムサービス' highlighted. The main content area shows the 'ログ設定' (Log Settings) page. At the top, there are tabs for various settings, with 'ログ設定' selected. Below the tabs is a 'Syslog サーバー' section with a table for adding servers. A red box highlights the '追加' (Add) button. Below that is a 'ログ設定' (Log Settings) table with columns for log type, suppression, and local reporting.

ログの種類 (システム)	ログの抑制	ローカルレポート
すべて	<input type="checkbox"/>	<input type="checkbox"/>
ファイアウォール	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ファイアウォールルール		<input checked="" type="checkbox"/>
無効なトラフィック		<input checked="" type="checkbox"/>
ローカル ACL		<input checked="" type="checkbox"/>
DoS 攻撃		<input type="checkbox"/>
破棄された ICMP リダイレクトパケット		<input type="checkbox"/>
送信元ポートが指定された欠落パケット		<input type="checkbox"/>
破棄された断片化トラフィック		<input type="checkbox"/>
MAC フィルタリング		<input type="checkbox"/>
IP-MAC ペアフィルタリング		<input type="checkbox"/>
IP なりすまし防止		<input type="checkbox"/>
SSL VPN トンネル		<input type="checkbox"/>
保護されたアプリケーションサーバー		<input type="checkbox"/>
ハートビート		<input checked="" type="checkbox"/>
ICMP エラーメッセージ		<input type="checkbox"/>
ブリッジ ACL		<input type="checkbox"/>

②必要項目を入力し保存を押下します。

名前：任意

IP アドレス/domain：任意

ポート：通信ポート（514）

ファシリティ：選択

重要度レベル：選択

ファイル名：選択

The screenshot shows the configuration interface for a service in Sophos Firewall. The 'Log Settings' tab is selected. The form contains the following fields:

Field Name	Value
名前 *	入力名前
IP アドレス / domain *	入力 IP アドレス
ポート *	入力ポート
ファシリティ *	DAEMON
重要度レベル *	緊急
ファイル形式 *	Device Standard Format

At the bottom of the form, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel). The '保存' button is highlighted with a red box, and a red arrow points from the form fields to it.

③ 転送したいログ種別を選択し適用を押下します。

ログ設定

ログの種類(システム)	ローカル	test	Syslog
	<input type="checkbox"/>	<input type="checkbox"/>	
ファイアウォール	<input type="checkbox"/>	<input type="checkbox"/>	
ファイアウォールルール	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
無効なトラフィック	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
ローカルACL	<input type="checkbox"/>	<input type="checkbox"/>	
DoS 攻撃	<input type="checkbox"/>	<input type="checkbox"/>	
破棄されたICMP リダイレクト/パケット	<input type="checkbox"/>	<input type="checkbox"/>	
送信元レートが指定された欠落/パケット	<input type="checkbox"/>	<input type="checkbox"/>	
破棄された断片化トラフィック	<input type="checkbox"/>	<input type="checkbox"/>	
MAC フィルタリング	<input type="checkbox"/>	<input type="checkbox"/>	
IP-MAC ペアフィルタリング	<input type="checkbox"/>	<input type="checkbox"/>	
IP なりすまし防止	<input type="checkbox"/>	<input type="checkbox"/>	
SSL VPN トンネル	<input type="checkbox"/>	<input type="checkbox"/>	
保護されたアプリケーションサーバー	<input type="checkbox"/>	<input type="checkbox"/>	
ハートビート	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
ICMP エラーメッセージ	<input type="checkbox"/>	<input type="checkbox"/>	
IPS	<input type="checkbox"/>	<input type="checkbox"/>	
変則	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
シグネチャ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
マルウェア対策	<input type="checkbox"/>	<input type="checkbox"/>	
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
POP3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
IMAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

(6) 固定グローバル IP アドレス割り当て手順

Sophos Firewall への IP アドレスを手動で割り当てた場合、アクティベートされた初期状態では Port1 (WAN ゾーン) インタフェースの IP アドレスは一時的な状態です。**その為、再起動を行うと設定が消えてしまいます。**本手順の設定により情報を書き込む必要があります。共有セグメントへ展開 (グローバル IP アドレスを自動割り当て) した場合、本手順は不要です。

① ネットワーク > インターフェースタブより Port1 を押下します。



② 画面が設定画面に遷移し以下の情報を入力します。

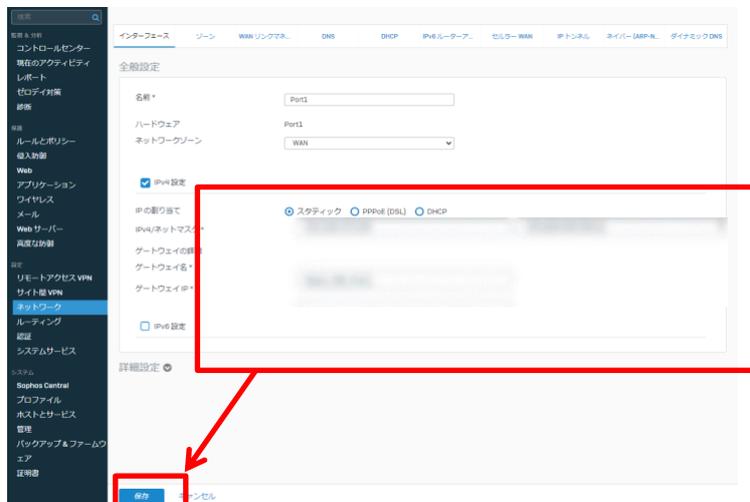
IP の割り当て : スタティック

IPv4/ネットマスク : 1.1.1.10/24

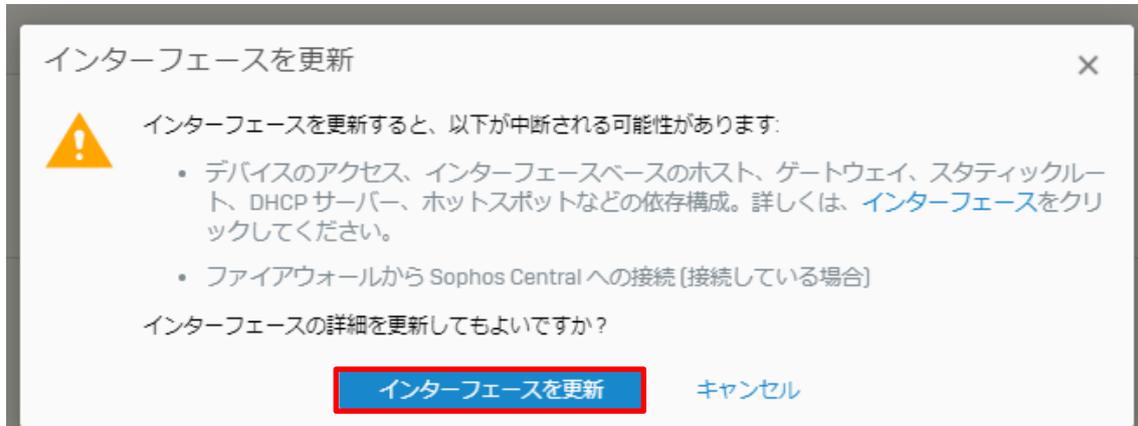
ゲートウェイ名 : 任意

ゲートウェイ名 : 1.1.1.1

保存ボタンを押下します。



③ インターフェースを更新を押下します。



(7) LAN ゾーンの IP アドレス割り当て手順

Sophos Firewall はアクティベートされた初期状態で Port2 (LAN ゾーン) インタフェースが作成されています。ご利用いただくために、Port2 インタフェースを有効にし、スイッチへの接続設定を行います。

- ① ネットワーク > インタフェースタブより Port2 を押下します。

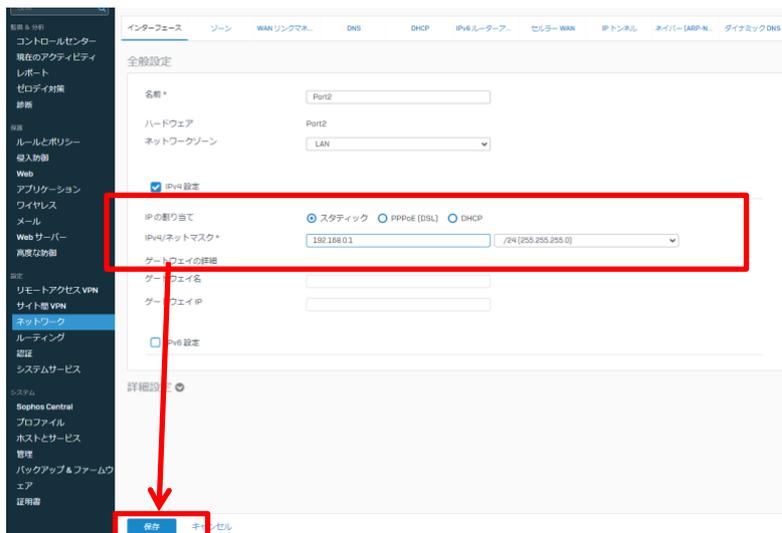


- ② 画面が設定画面に遷移します。

IP の割り当て : スタティック

IPv4/ネットマスク : 192.168.0.1/24

保存ボタンを押下します。



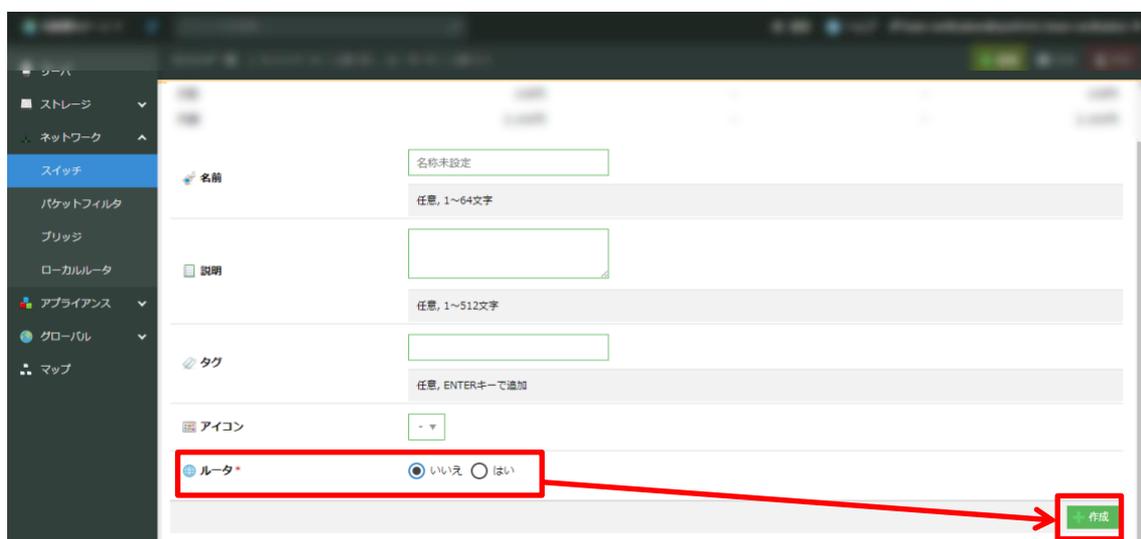
③Port2（LAN ゾーン）配下のスイッチに接続するために、画面右上の admin をクリックし、デバイスのシャットダウンを押下します。



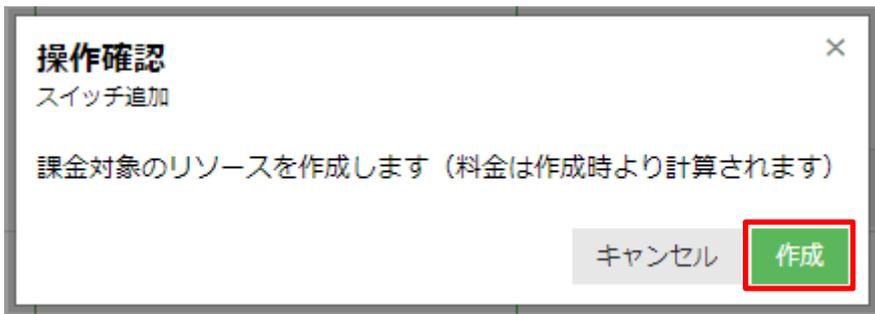
④さくらのクラウドコントロールパネルよりスイッチ追加の手続きを行います。ネットワークメニューよりスイッチを選択し、追加ボタンを押下し、スイッチの追加手続きを行います。ここで作成されるスイッチはさくらのクラウドが提供する有料のサービスです。



⑤必要な項目を入力します。この時、ルータの項目は「いいえ」を選択し、作成ボタンを押下します。



確認メッセージで追加を押下し、スイッチ追加プロセスを実行します。



名前	メソッド	リソース	ステータス
スイッチ: 作成	POST	cloud/1.1/switch	成功

中断 閉じる

⑥追加したスイッチに接続します。

「1 未接続」の NIC 列の最右のメニューを展開し、接続を編集を押下します。



⑦ スイッチに接続を選択し、スイッチを選択し更新を押下します。

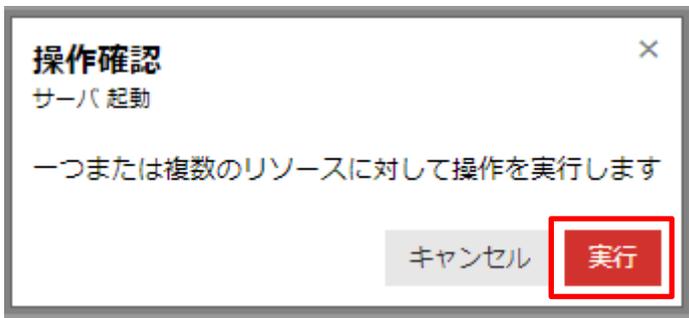


NIC 接続プロセスが成功したことを確認します。

⑧ さくらのクラウドコントロールパネルより Sophos Firewall のインスタンスの起動処理を行います。サーバメニューより、Sophos Firewall のインスタンスを選択し、電源操作 > 起動を押下します。



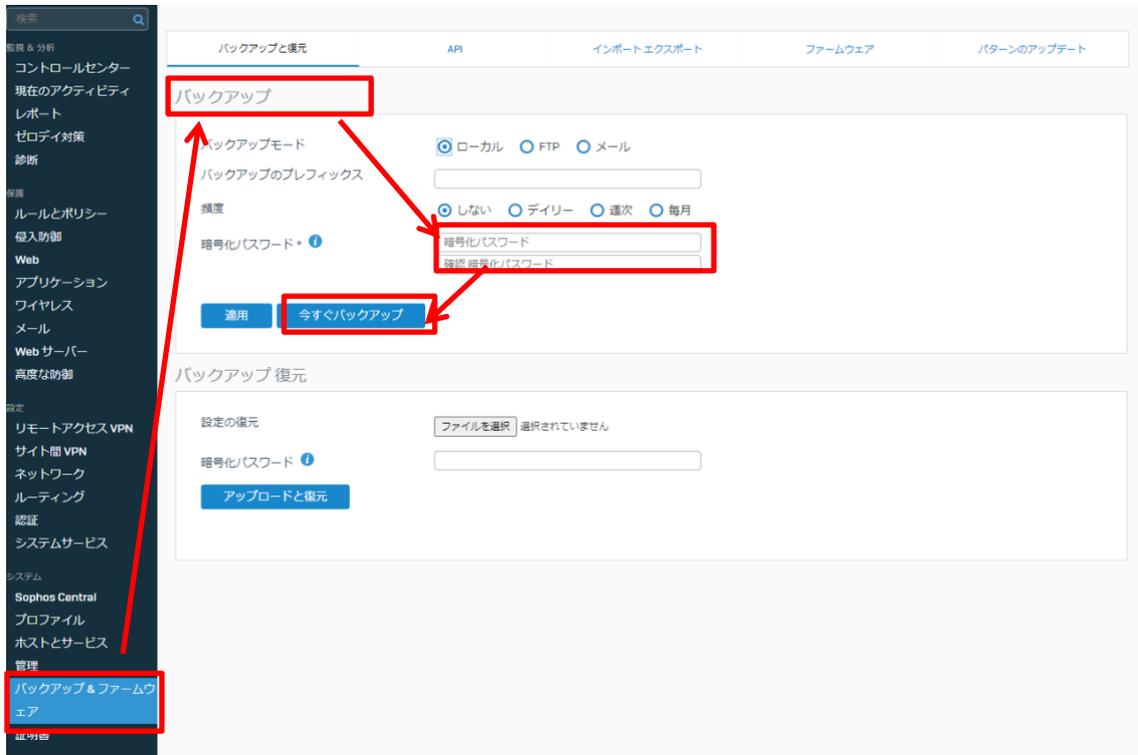
確認画面より実行ボタンを押下します。



サーバ起動プロセスが成功したことを確認します。

(8) バックアップ取得手順

①バックアップ&ファームウェア > バックアップと復元タブより、暗号化パスワードを任意の12文字以上で設定し今すぐバックアップを押下します。



② バックアップが作成されたらダウンロードを押下します。



③バックアップのダウンロードを押下します。



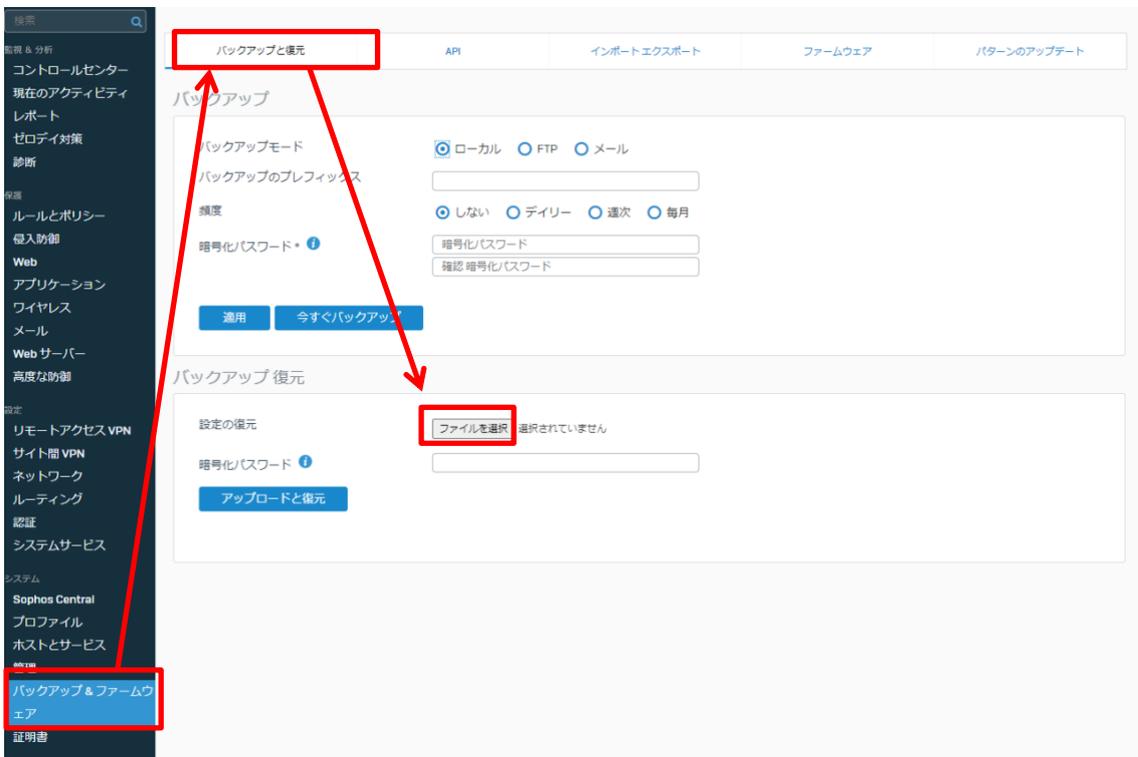
バックアップファイルがダウンロードされます。

他にも、スケジュールに基づく取得や、メール通知機能も設定することが可能です。詳細はヘルプをご参照ください。

(9) リストア手順

※リストア時、Sophos Firewall は再起動します。

④バックアップ&ファームウェア > バックアップと復元タブより、ファイルを選択を押下し、取得したバックアップファイルを選択します。



②バックアップ取得時に設定したパスワードを入力しアップロードと復元を押下します。

バックアップ復元

設定の復元

ファイルを選択 Backup_0010_0_1943.02

パスワード ⓘ

アップロードと復元

③セキュアストレージマスターキーを入力します。

バックアップを復元する

Enter the secure storage master key.

This backup configuration uses a secure storage master key to encrypt sensitive information, such as passwords. The key belongs to the firewall where this backup was created.

Secure storage master key

キャンセル 復元

④内容を確認し OK を押下します。

このバックアップを復元すると現在の設定が上書きされ、デバイスが再起動します。これによって、元の IP アドレスが復元されるため、接続が切断される場合があります。このバックアップを復元してもよいですか？

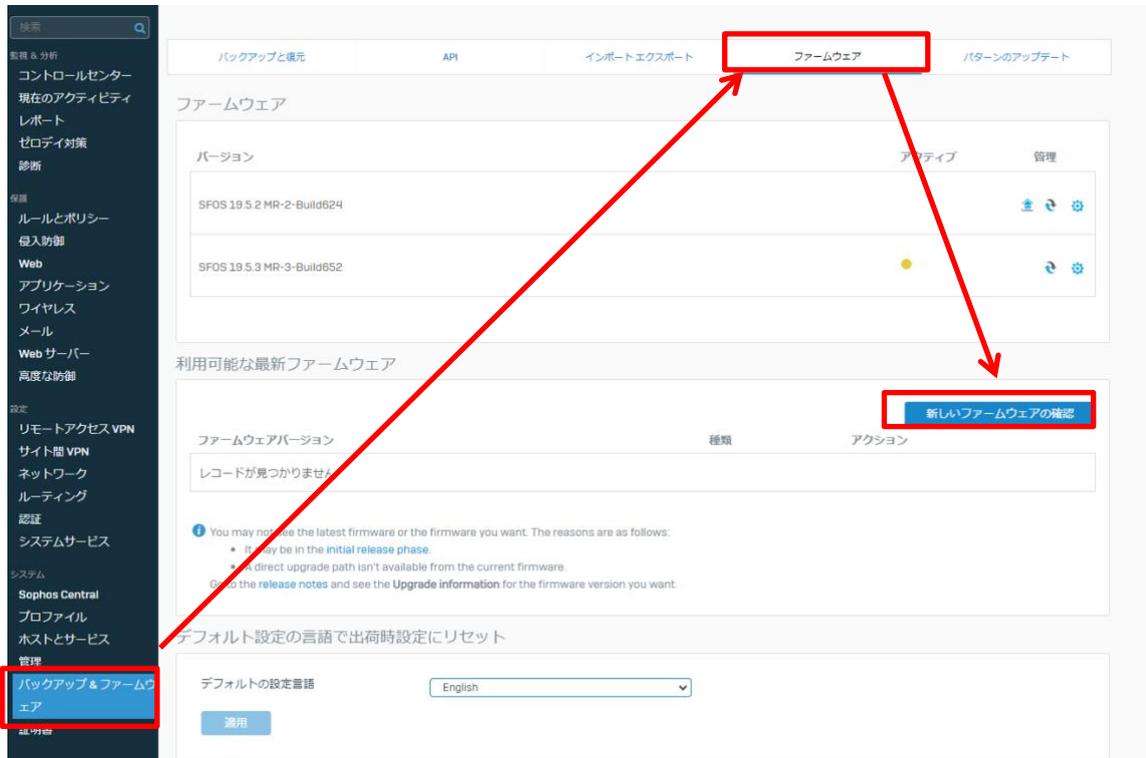
OK キャンセル

⑤再度、WebAdmin にログインしバックアップ内容が反映されていることを確認します。またリストアに際して、Sophos Firewall のバージョンが同一でないとリストアすることができません。

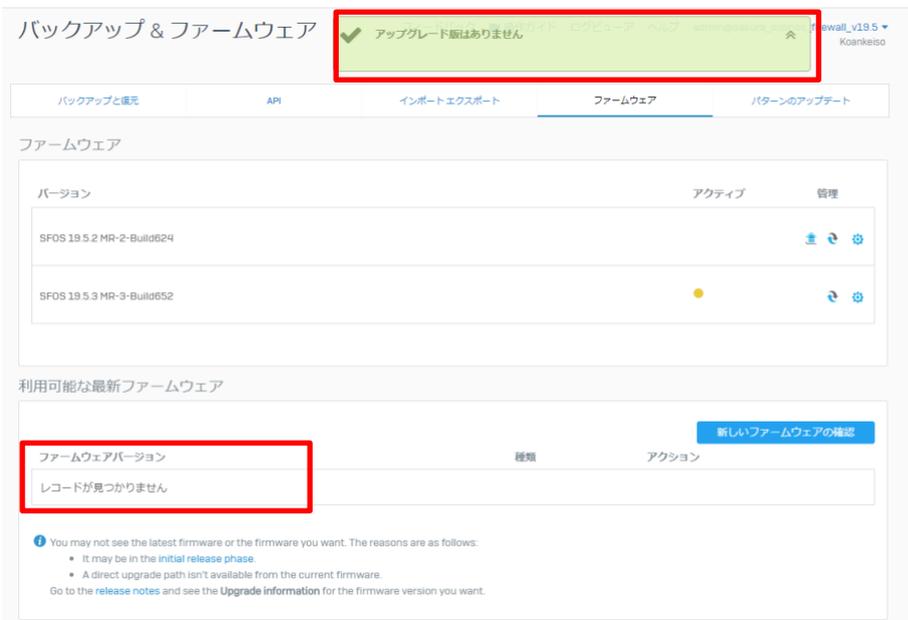
(10) ファームウェア (SFOS) 更新手順

ファームウェアは機能の追加、脆弱性の修正を目的とし、定期的に更新されます。初期展開後はファームウェア (SFOS : Sophos Firewall OS) を最新版に更新しご利用ください。

- ① バックアップ&ファームウェア > ファームウェアタブより、新しいファームウェアの確認を押下し、最新のファームウェアの有無を確認します。



新しいファームウェアがなければ以下の通り特に表示はされません。



- ② ファームウェアが見つかった場合、以下の通り表示されます。

バックアップと復元 API インポート/エクスポート **ファームウェア** パターンのアップデート

SFOS 19.5.1 MR-1-Build278

新しいファームウェアの確認

ファームウェアバージョン	種類	アクション
SFOS 19.5.2 MR2-Build624	GA	ダウンロード
SFOS 19.5.3 MR3-Build652	MR (staging)	ダウンロード

! You may not see the latest firmware or the firmware you want. The reasons are as follows:

- It may be in the [initial release phase](#).
- A direct upgrade path isn't available from the current firmware.

Go to the [release notes](#) and see the [Upgrade information](#) for the firmware version you want.

ホットフィックス

Sophos Assistant

- ③ ダウンロードを押下し、ファームウェアをダウンロードします。アクションとしてダウンロード状況が表示されます。

アクション

0.1% x

- ④ ダウンロードが完了すると「インストール」が表示されますので、「インストール」ボタンを押下し、インストールを行います。**インストールが完了すると再起動し、最新のファームウェアで再起動します。**
- ⑤ 最新のファームウェアで起動し、起動中のファームウェアで「○（黄色）」マークが点灯します。バックアップ&ファームウェア > ファームウェアタブの画面から確認できます。

ファームウェア

バージョン	アクティブ	管理
SFOS 19.5.2 MR-2-Build624		🔄 ⚙️
SFOS 19.5.3 MR-3-Build652	●	🔄 ⚙️

- ⑥ もし設定を戻したい場合には、以下のマークをクリックすることで、任意のファームウェアで Sophos Firewall を起動させることが可能です。**Sophos Firewall 内で保持できるファームウェアは2つまでです。**

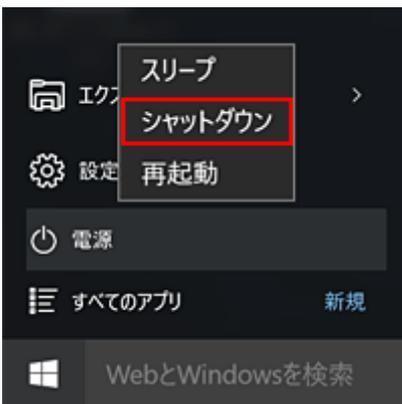


5-2. 保護対象システム（WindowsServer2016）の初期設定

保護対象システムを Sophos Firewall で保護するためには、インターネットへのアクセスを必ず Sophos Firewall を経由させる必要があります。その為、プライベートセグメントに展開したスイッチに保護対象を接続し、デフォルトゲートウェイを Sophos Firewall に対し設定する必要があります。

①保護対象システムをスイッチに接続するために、シャットダウンを実行します。

Windows マークを押下し、電源マークからシャットダウンを押下します。

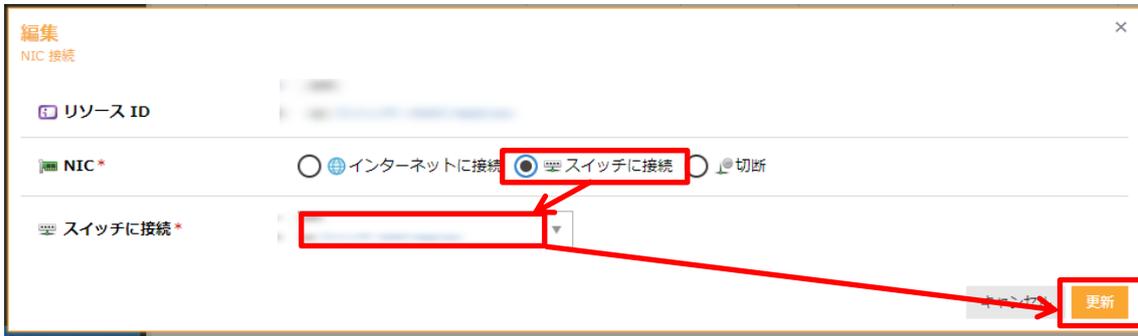


②NIC を作成したスイッチに接続します。

NIC 列の最右のメニューを展開し、接続を編集を押下します。



③ スイッチに接続を選択し、対象のスイッチを選択し更新を押下します。



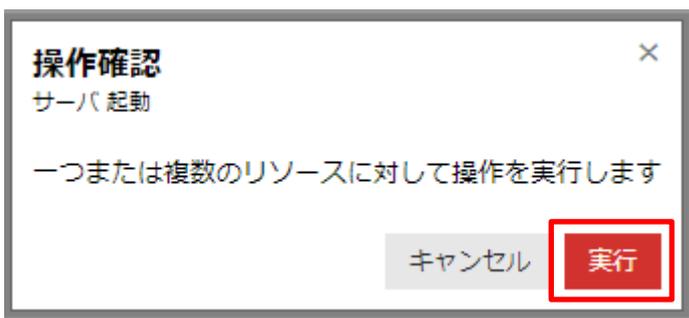
NIC 接続プロセスが成功したことを確認します。



④ さくらのクラウドコントロールパネルより保護対象システムのインスタンスの起動処理を行います。サーバメニューより、インスタンスを選択し、電源操作 > 起動 を押下します。

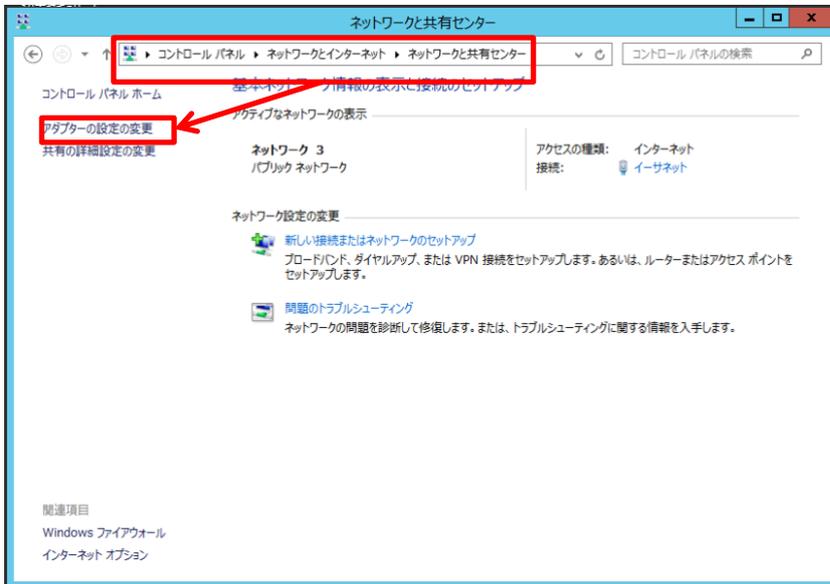


確認画面より実行ボタンを押下します。

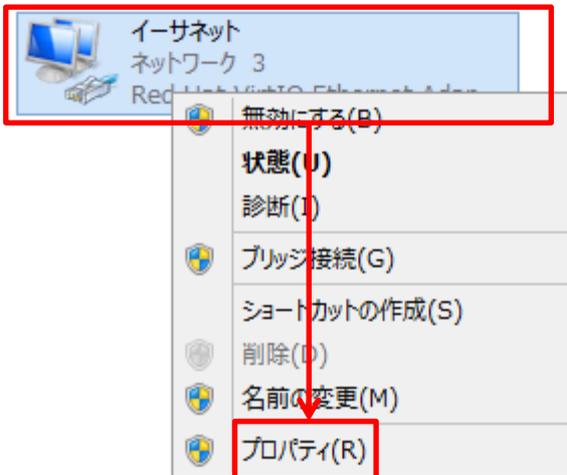


サーバ起動プロセスが成功したことを確認します。

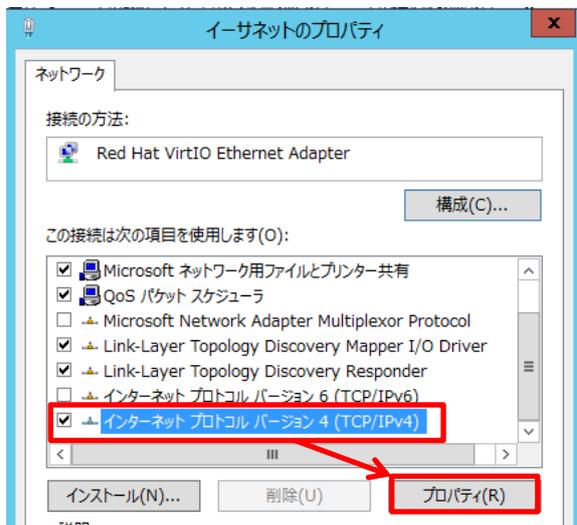
⑤保護対象システムへアクセスし IP アドレスとデフォルトゲートウェイの設定を行います。
 コントロール パネル > ネットワークとインターネット > ネットワークと共有センター
 を開き、アダプターの設定変更を押下します。



⑥該当の NIC (アダプター) を右クリックしプロパティを押下します。



⑦インターネットプロトコルバージョン 4 (TCP/IP4) を選択し、プロパティを押下します。



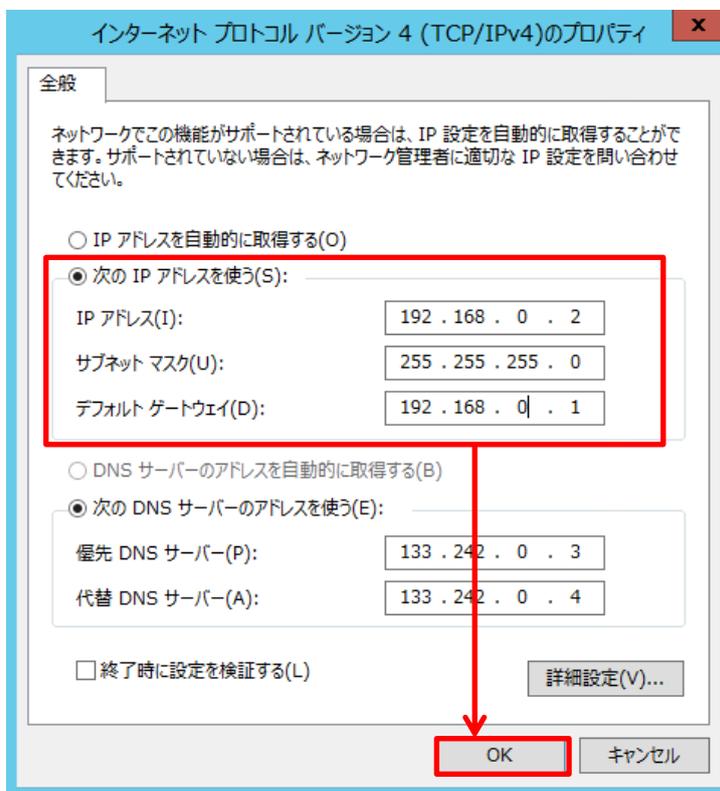
⑧プロパティ画面から以下の通り、設定を入力し、OK ボタンを押下します。

- 次の IP アドレスを使う：チェック

IP アドレス：192.168.0.2

サブネットマスク：255.255.255.0

デフォルトゲートウェイ：192.168.0.1



プロパティ画面に戻るので OK ボタンを押下し、アダプターの設定変更画面を閉じます。

6. さくらのクラウド環境における制約事項

本サービスはさくらのクラウドが提供する機能が一部ご利用いただけませんのでご注意ください。

①アーカイブ Disk サイズについて

本サービスで提供されるイメージの Disk サイズは 100GB 固定となります。Disk サイズを増やしても Sophos Firewall 内の Disk パーティションは修正されません。

②Disk 修正について

本サービスで提供されるイメージに対するサーバ追加のオプションとしてある Disk 修正はご利用いただけません。Disk は修正されず起動に失敗します。

③冗長化構成について

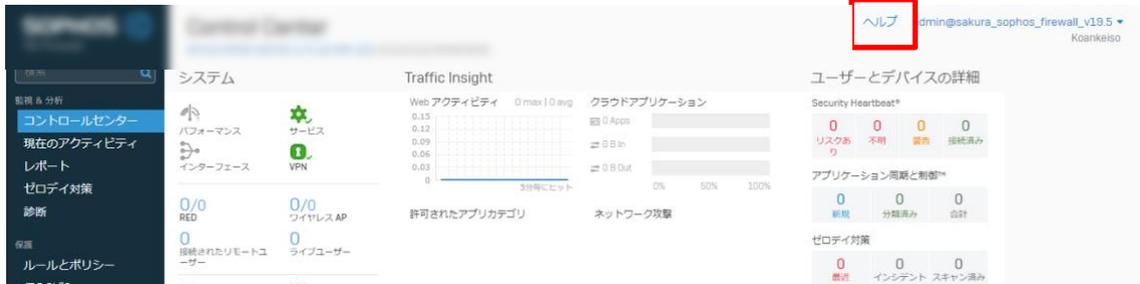
さくらのクラウド環境では、Sophos Firewall が具備する HA 機能をご利用いただけます。VRRP のようなネットワーク通信プロトコルには対応しておりません。

④バックアップについて

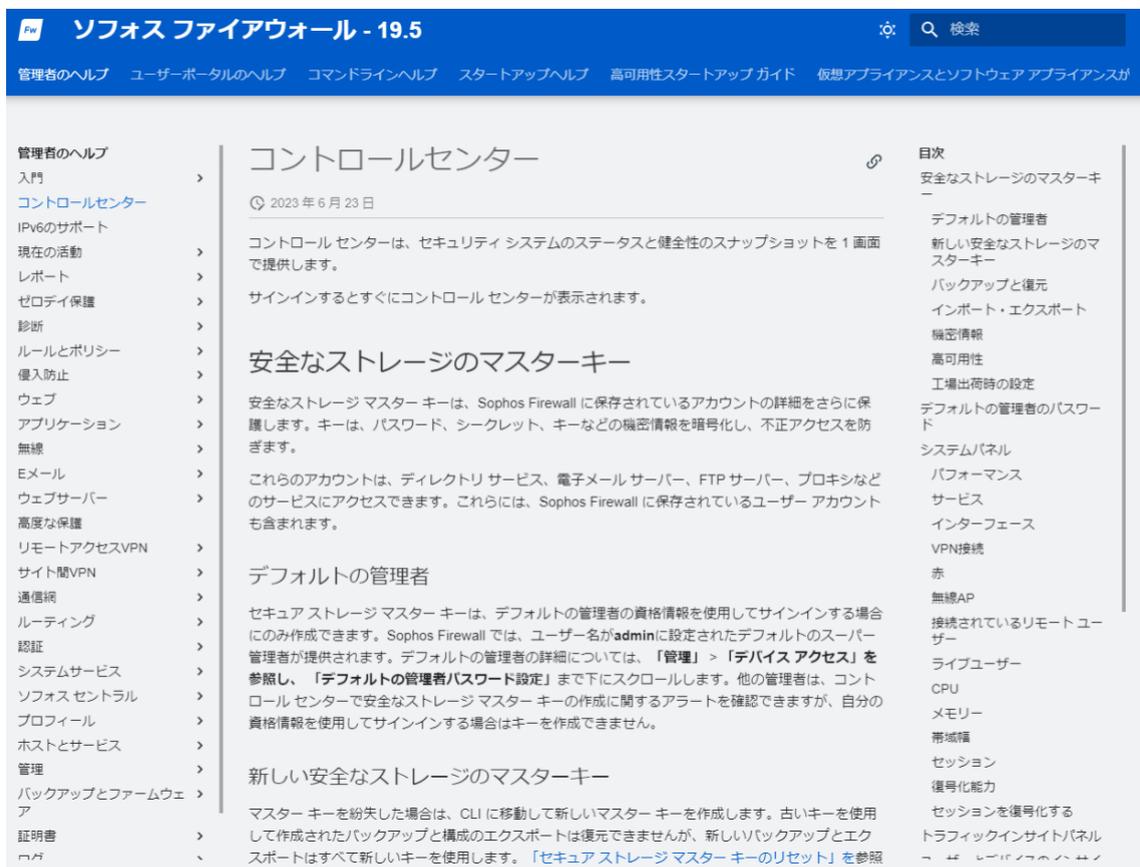
さくらのクラウド環境で提供されるアーカイブや Disk コピーでのバックアップが可能です。ただし、コピーした Sophos Firewall を同ライセンスで同時に起動した場合、ライセンス違反となりますのでご注意ください。また Sophos Firewall が具備するバックアップ機能はそのままご利用いただけます。

7. 詳細の機能と設定方法を知りたい時

Sophos Firewall はヘルプより各画面ごとにユーザーアシスタントヘリンクされており、必要なときに必要な箇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が開きます。



以上