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

KOANKEISO

興安計装株式会社

目　次

内容

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

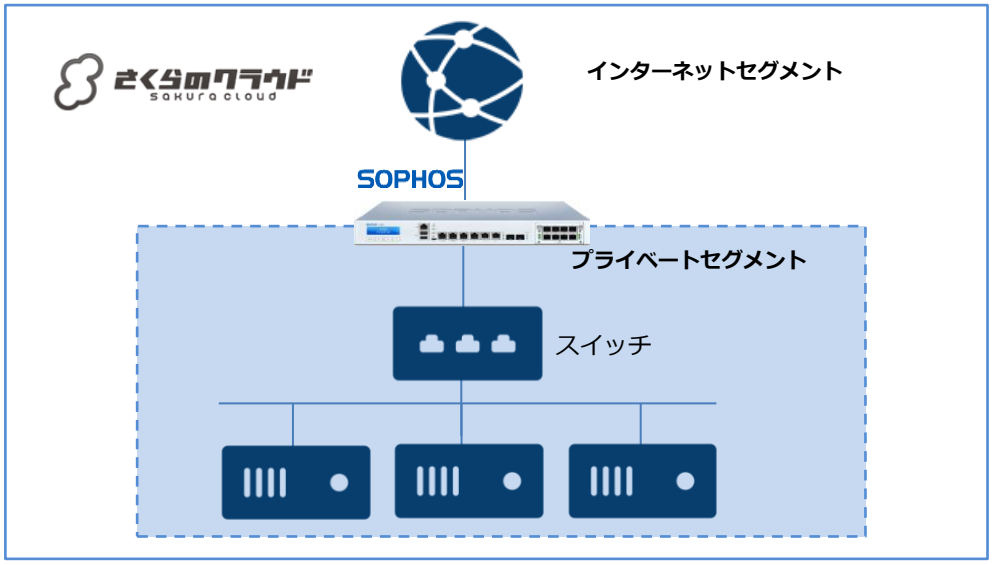
本サービスの利用条件は以下の通りです。

①ご利用環境

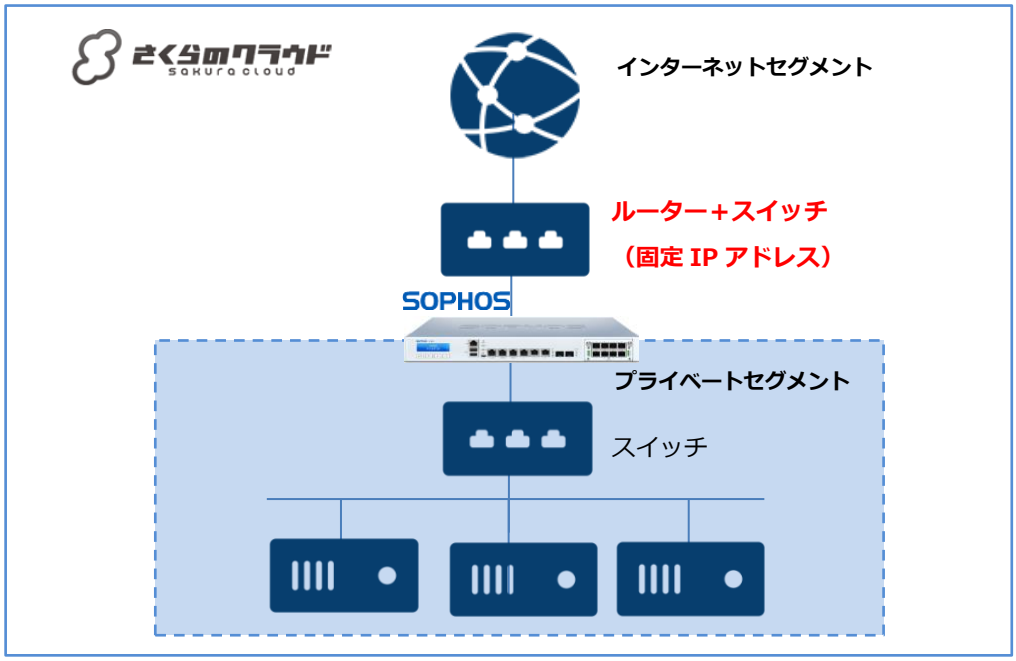
さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

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	2500	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 種類のみの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。

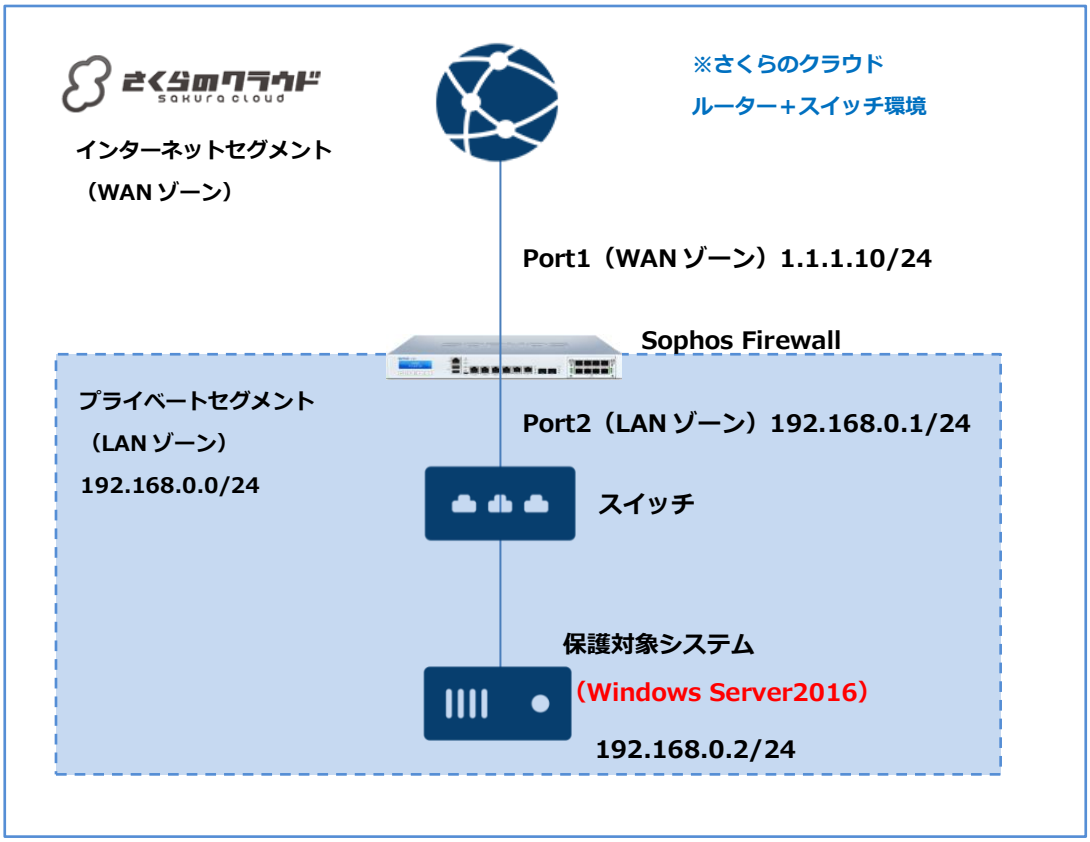
例：インスタンスサイズが 2C6GB、ライセンスが 1C4GB だった場合、Sophos Firewall は 1C4GB と認識します。

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。

種別 / 機能	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。



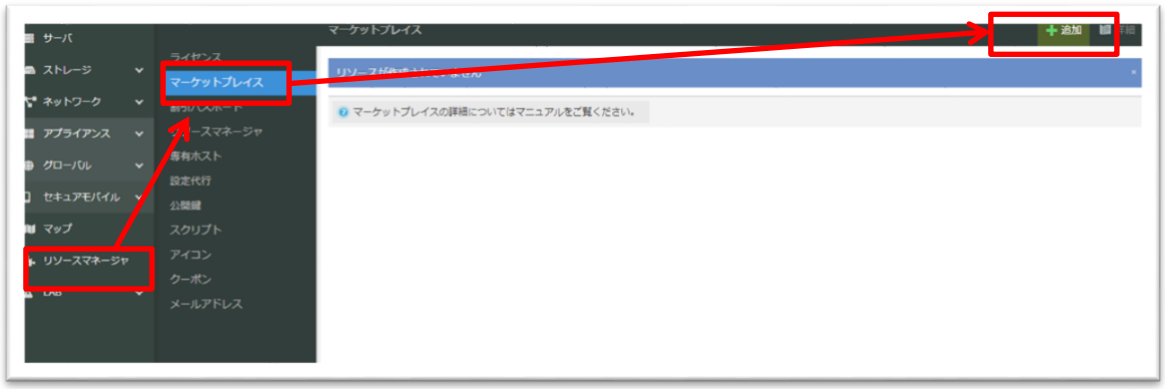
【構成要件】

- 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

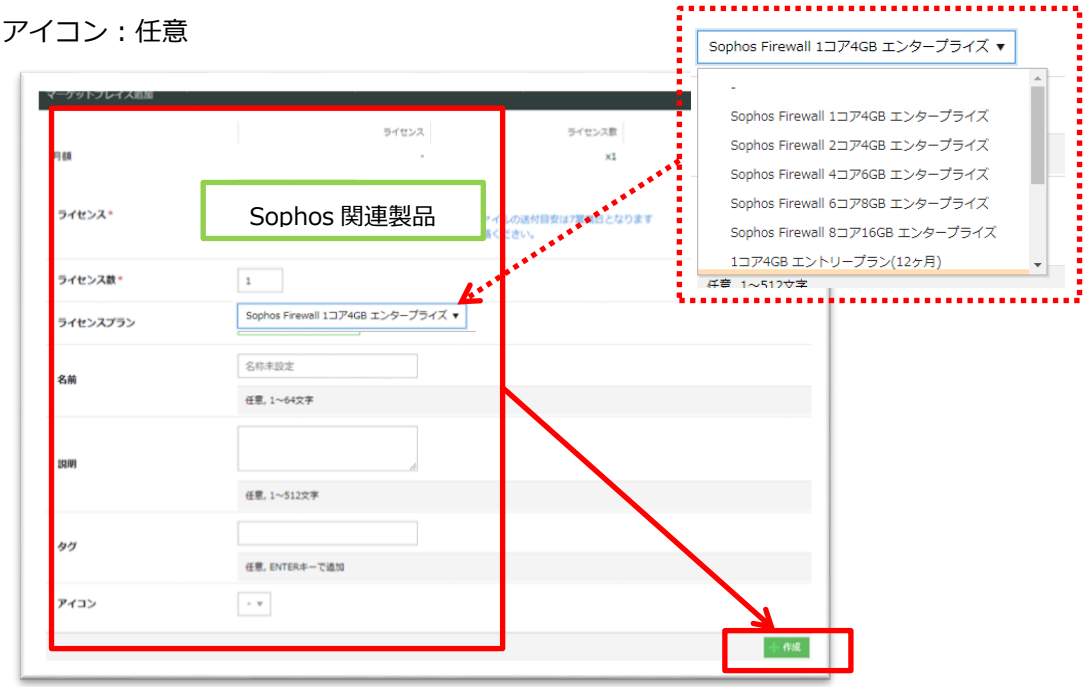
ライセンスプラン：コア数に応じて選択

名前：任意

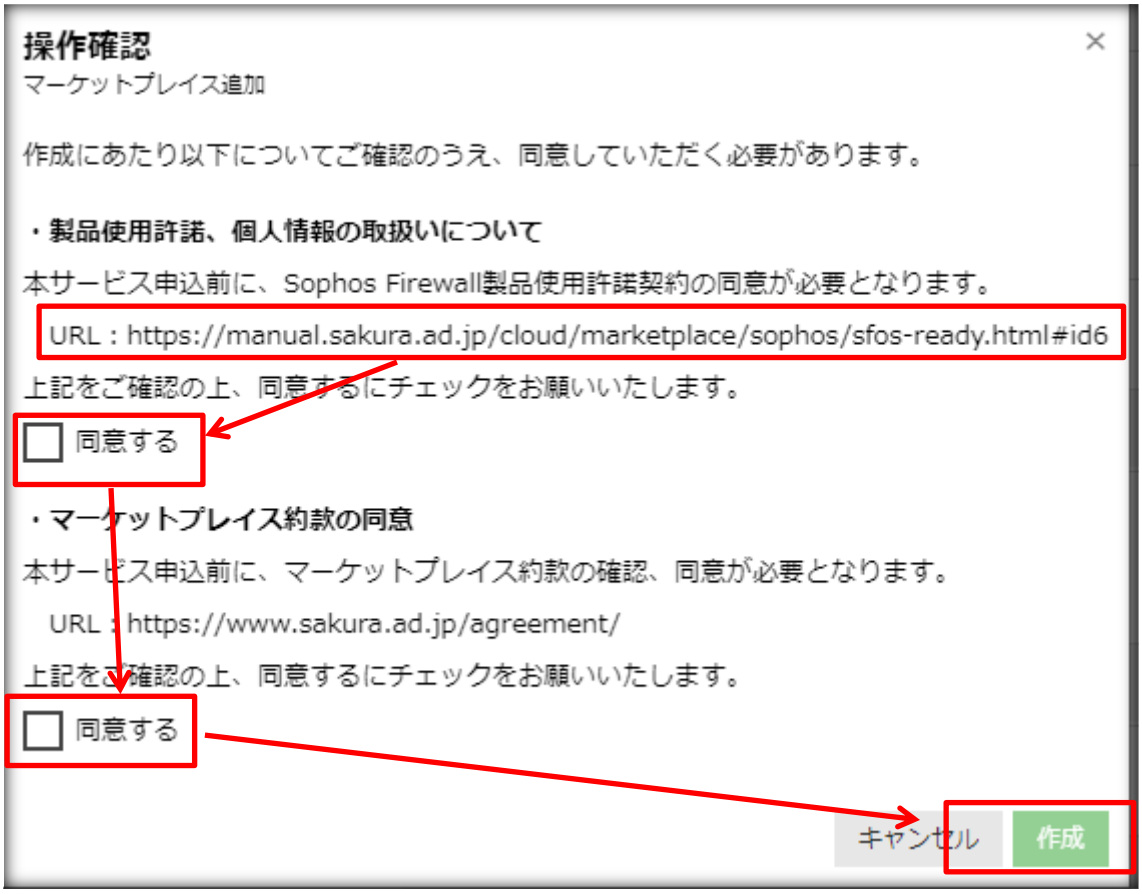
説明：任意

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。



コントロールパネルからお申込後ライセンスファイル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。

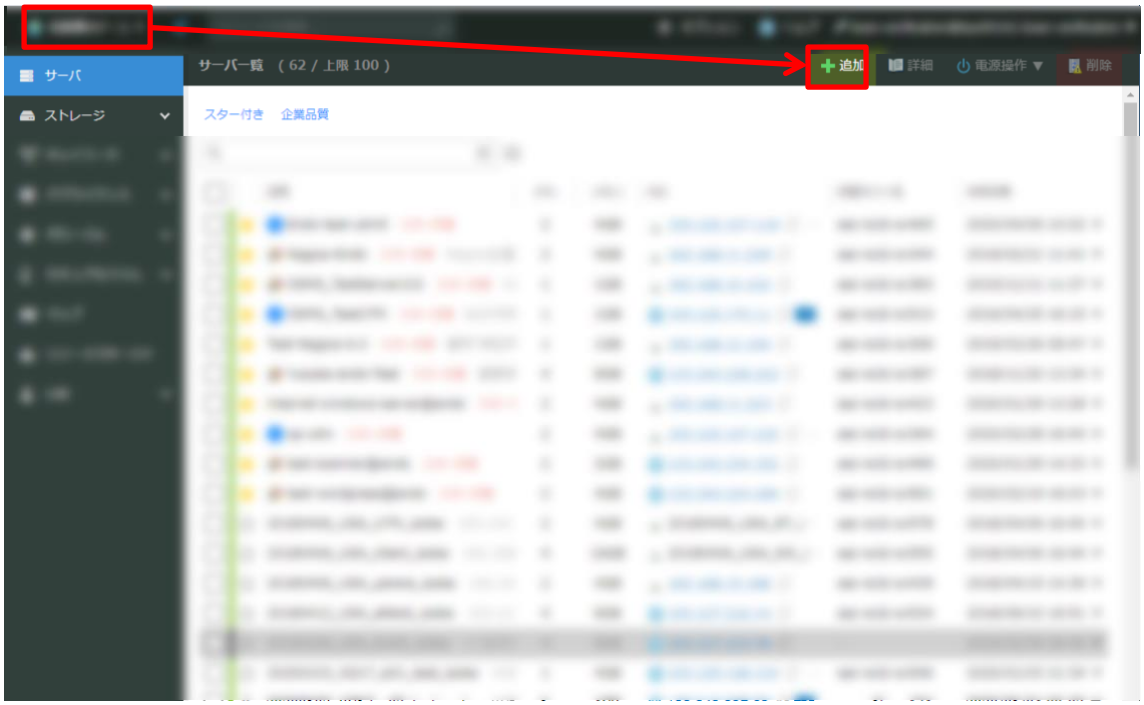
ライセンス取得方法は以上です。

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。

④ 適切なディスクサイズを選択します。

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 に手動でにグローバル 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 アドレスを割り当た場合、「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。

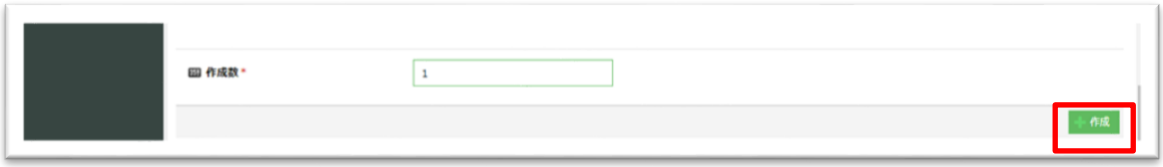
⑥ Sophos Firewall のアーカイブに対し、ディスク修正は利用できません。

⑦シンプル監視は任意で有効にします。

⑧サーバの情報は任意の内容で入力します。

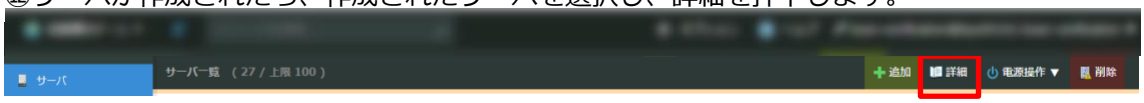
⑨作成後すぐに起動のチェックを外します。

⑩作成ボタンを押下します。



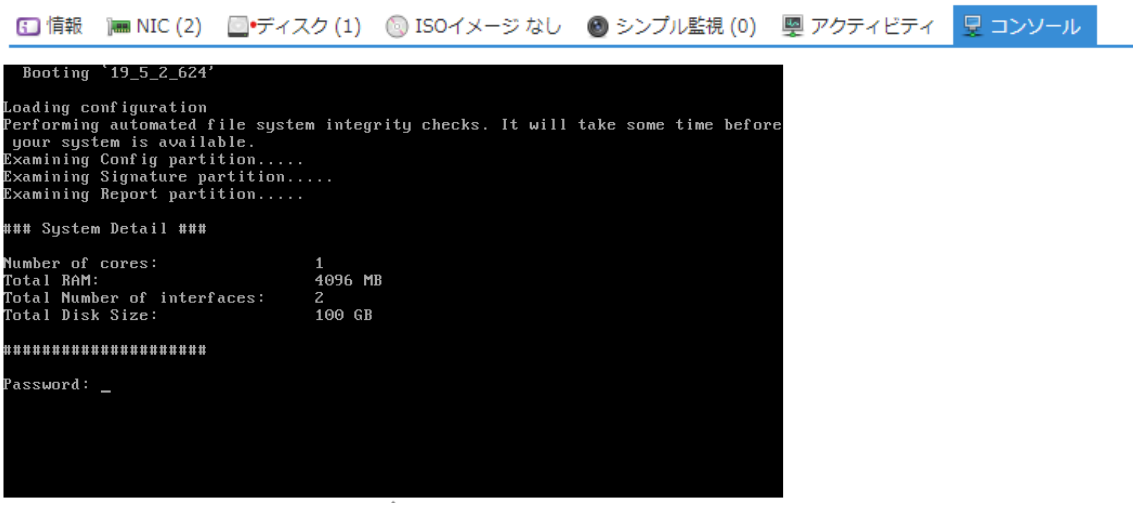
⑪サーバの追加プロセスが開始されます。

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。

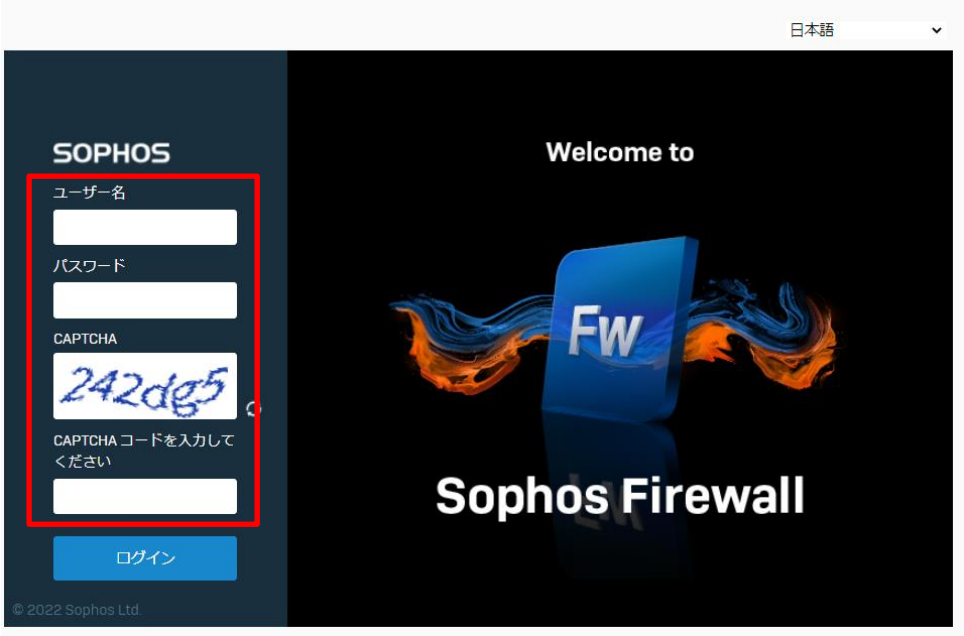


⑬NIC タブより追加ボタンを押下し、NIC を追加します。※Sophos Firewall の起動要件として NIC が 2 つ必要となります。

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。



⑮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。

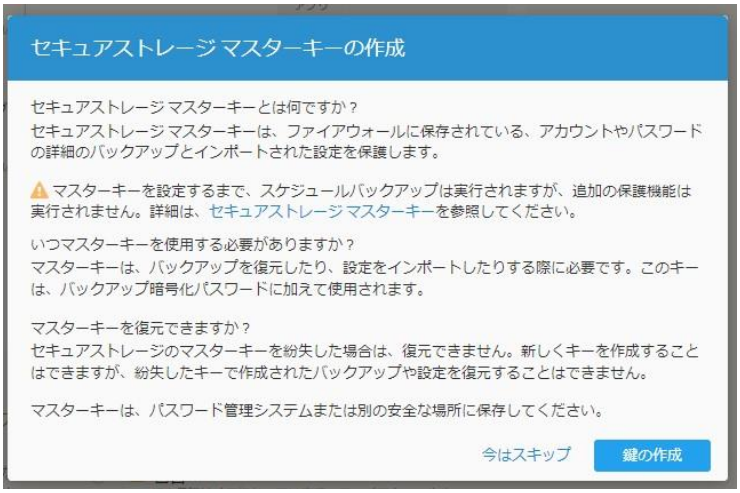


⑯ユーザ名とパスワードは以下の通りです。ランダムなワンタイム文字コードも入力します。

admin **9T23y!1s55**

admin アカウントでログインします。

⑰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。



⑱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①～⑭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

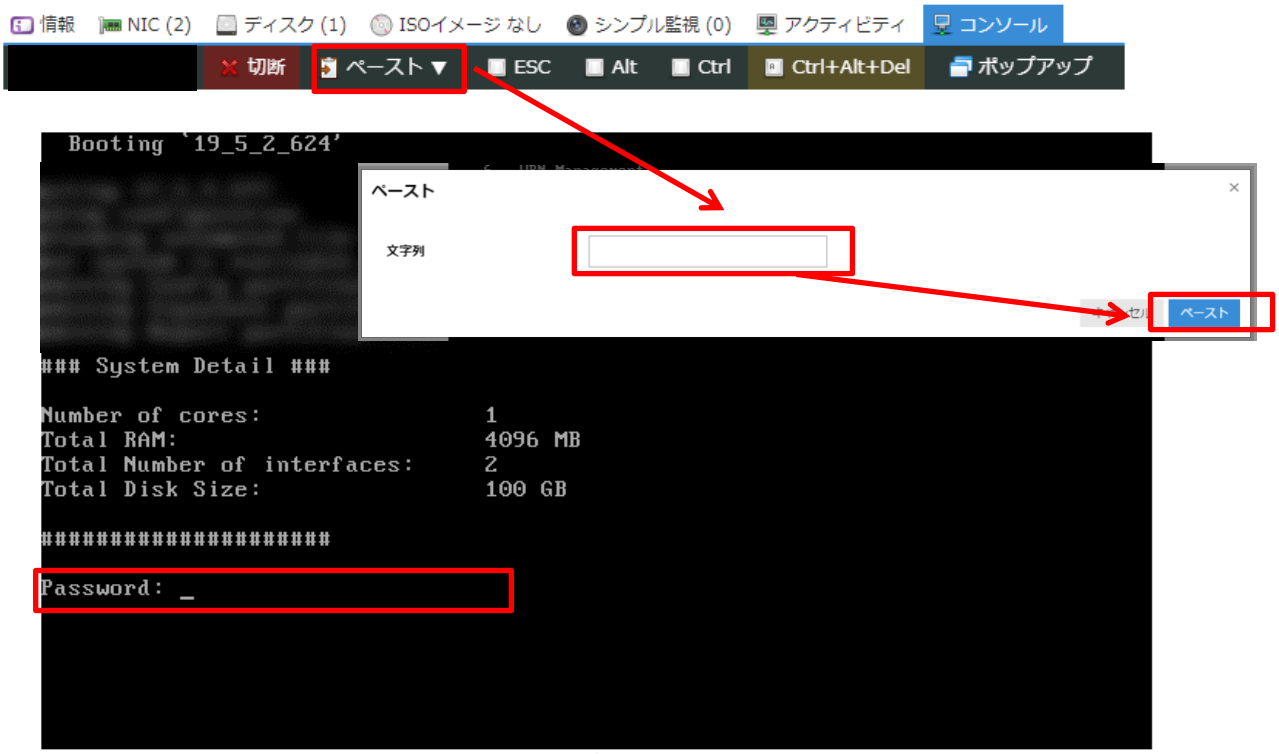
■割り当てたい IP アドレス：1.1.1.10/24

■デフォルトゲートウェイ：1.1.1.1/24

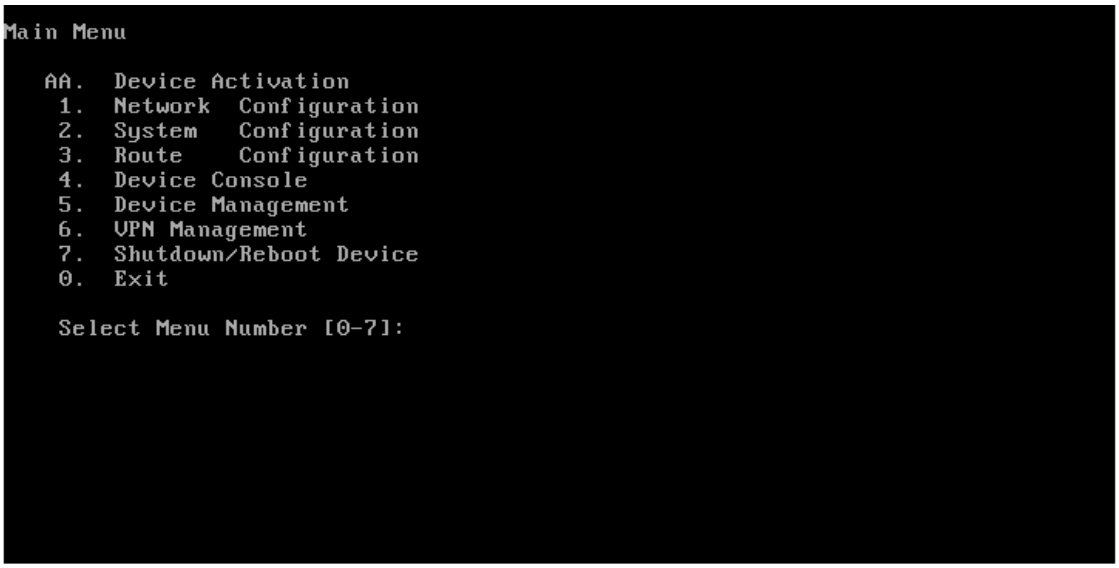
①コンソールタブに切り替え、以下のパスワードでログインします。

9T23y!1s55

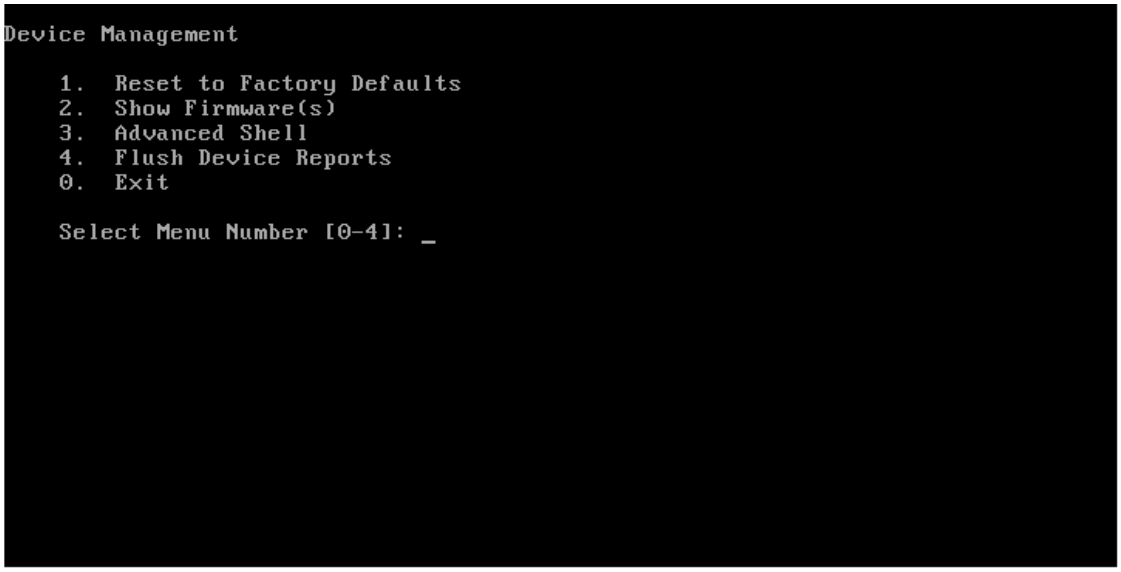
※キー配列は US 配列です。配置がわからない場合、ペースト機能をご利用ください。



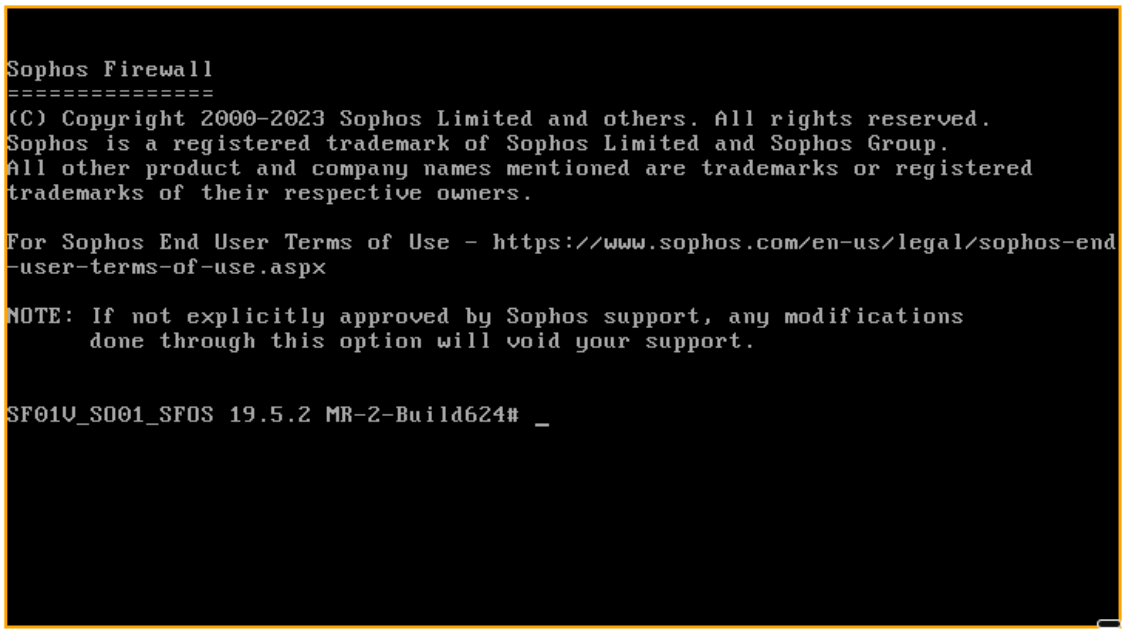
②ログイン後、「５． Device Management」を選択するため、Select Menu Number で「５」を選択します。



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



④ Advanced Shell に画面が遷移します。



⑤Advanced 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。

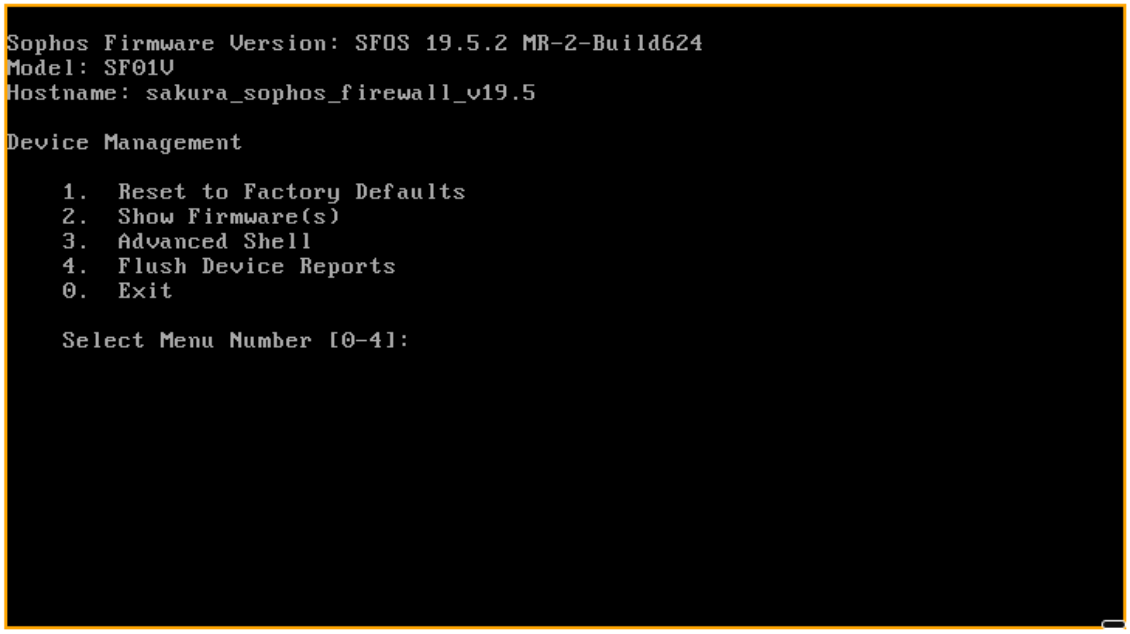
■割り当てたい IP アドレス：1.1.1.10/24

■デフォルトゲートウェイ：1.1.1.1/24

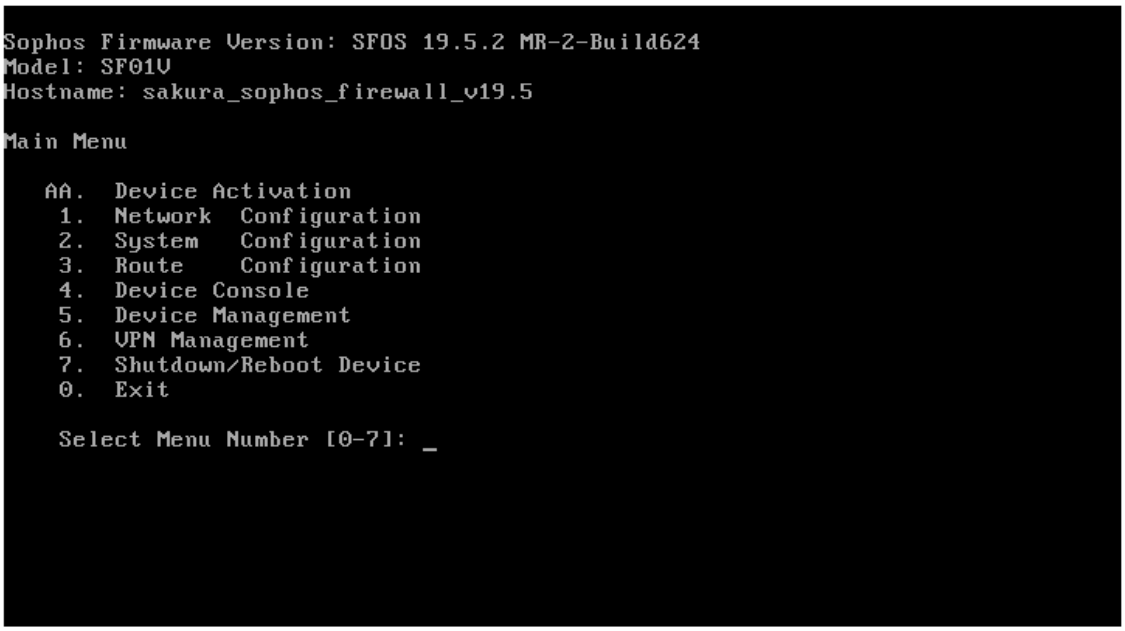
```
#ifconfig Port1 1.1.1.10 netmask 255.255.255.0
#route add default gw 1.1.1.1
#exit
```

※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。

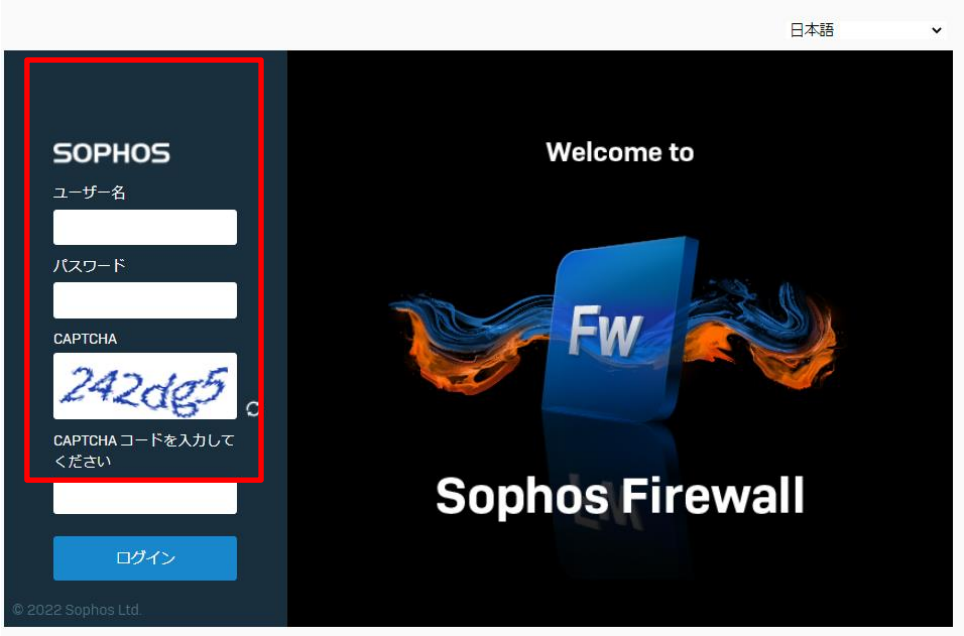
⑤　「Device Management」を Exit するため、Select Menu Number で「 0 」を選択します。



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



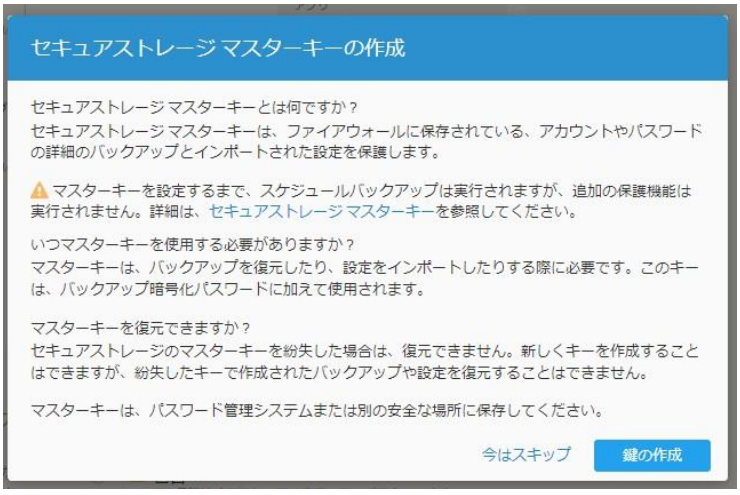
⑦割り当てたグローバル IP アドレスを確認し、ブラウザより https://（IP アドレス）:4444 でアクセスします。



⑦admin 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**

⑧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。

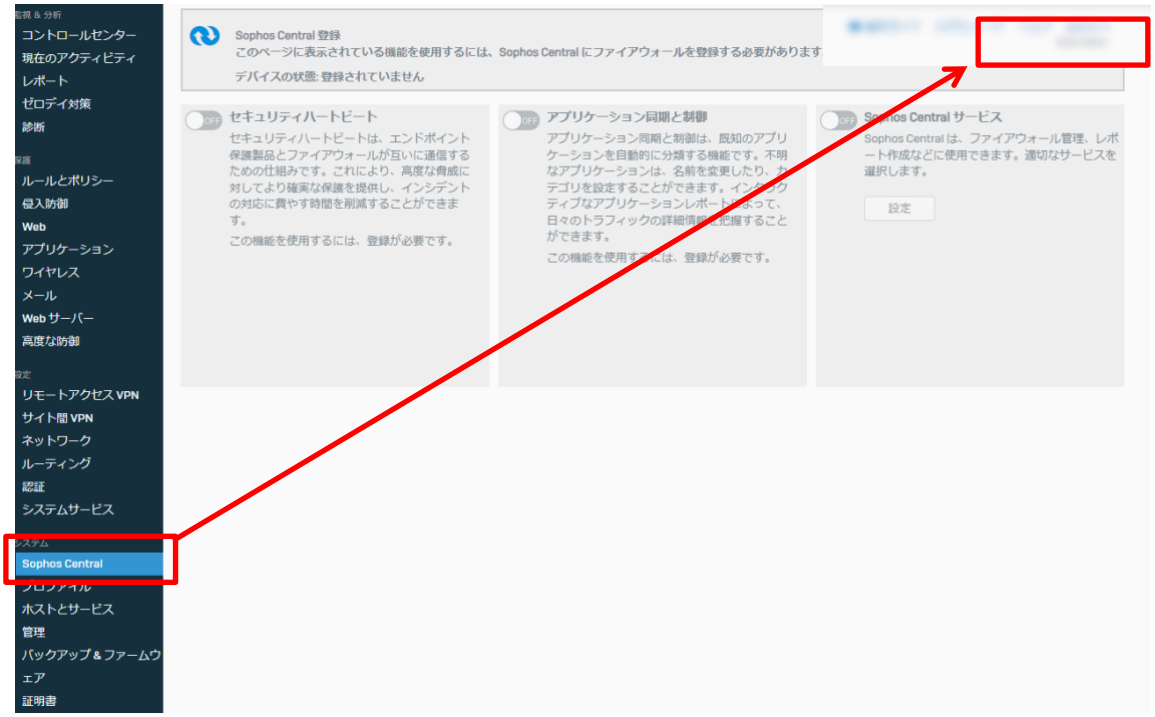
以上で、IP アドレスの手動割り当て展開手順は完了です。

（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。

②ライセンス適用後、「Control Center」に遷移します。

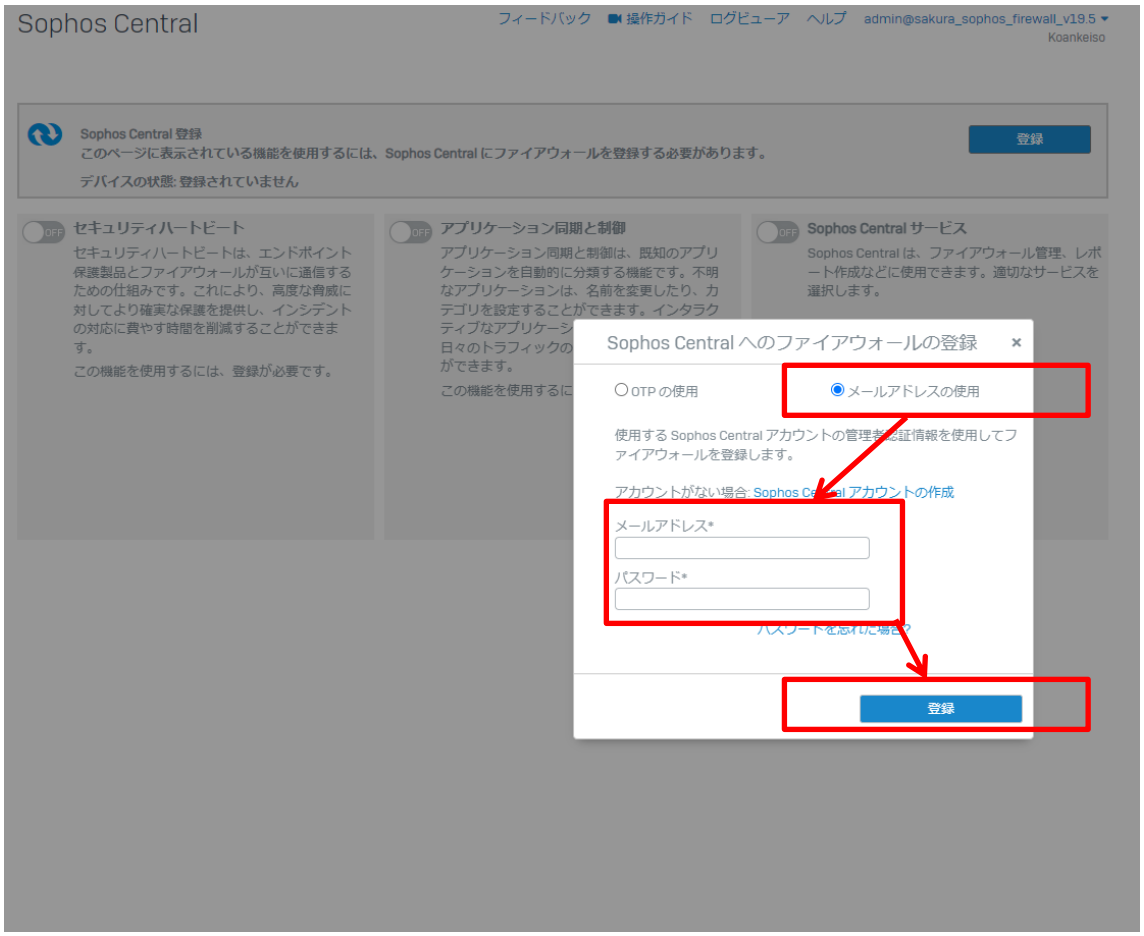
⑦　「Sophos Central」メニューに遷移し登録ボタンを押下します。



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**

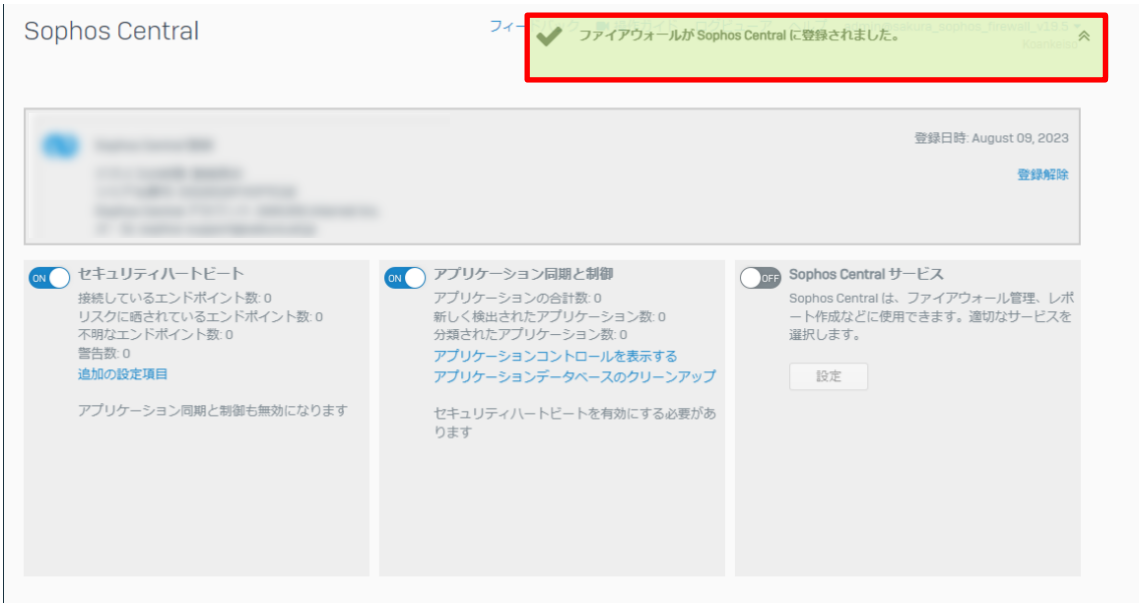
※記載された Sophos Central アカウントは本サービスのみで有効なアカウントです。本サービス以外では SophosCentral サービスをご利用いただく事は出来ませんのでご注意ください。



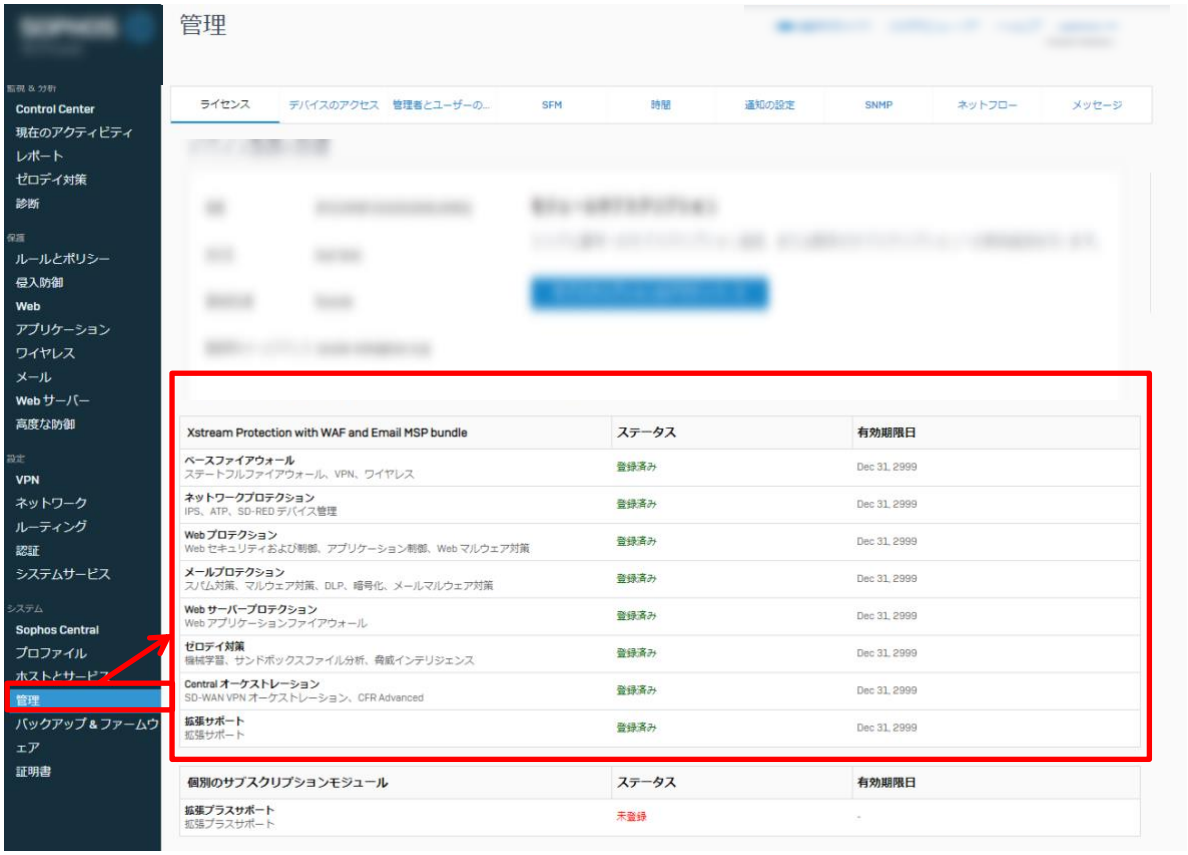
※本手続きを行わなかった場合、また上記メールアドレス以外でのご登録頂いた場合、当社からのアクティベート確認が取れないため、一定期間後にライセンスが無効になりますのでご注意ください。

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。



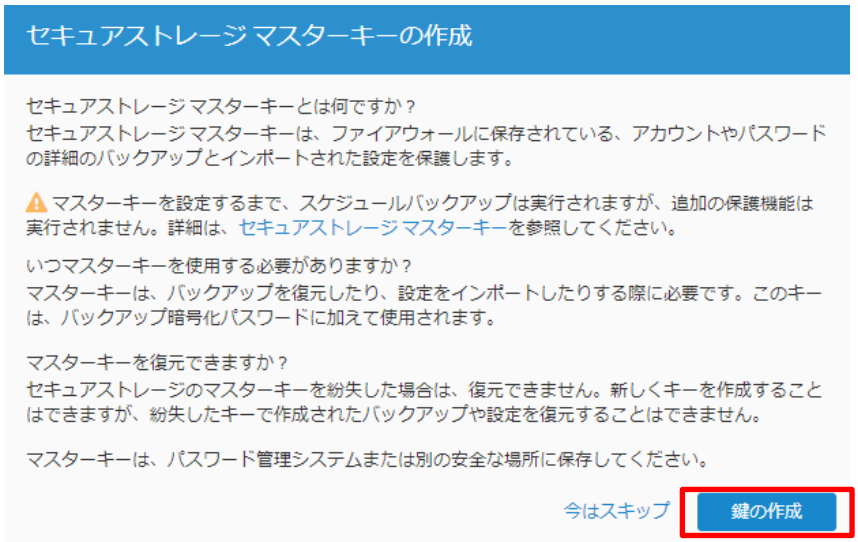
⑩この登録作業をもって正しくライセンスをご利用いただく事ができます。「管理」より
ライセンスの状況が確認する事ができます。



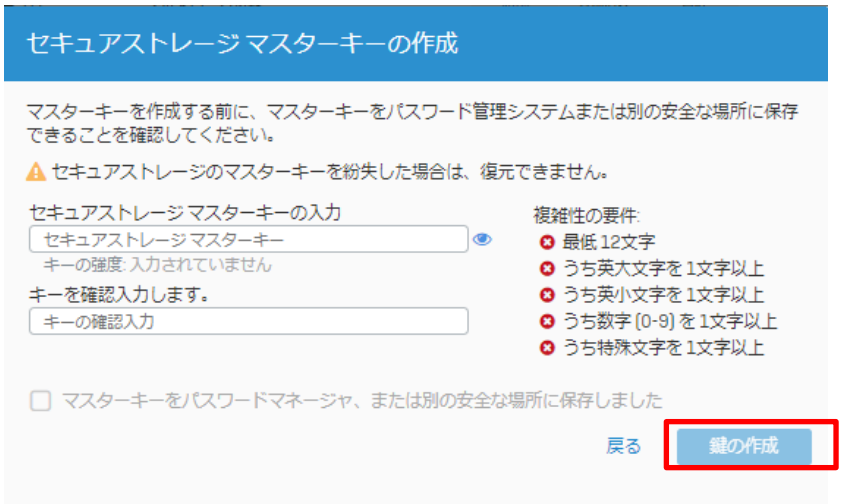
以上で、ライセンス適用手順は完了です。

（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。



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

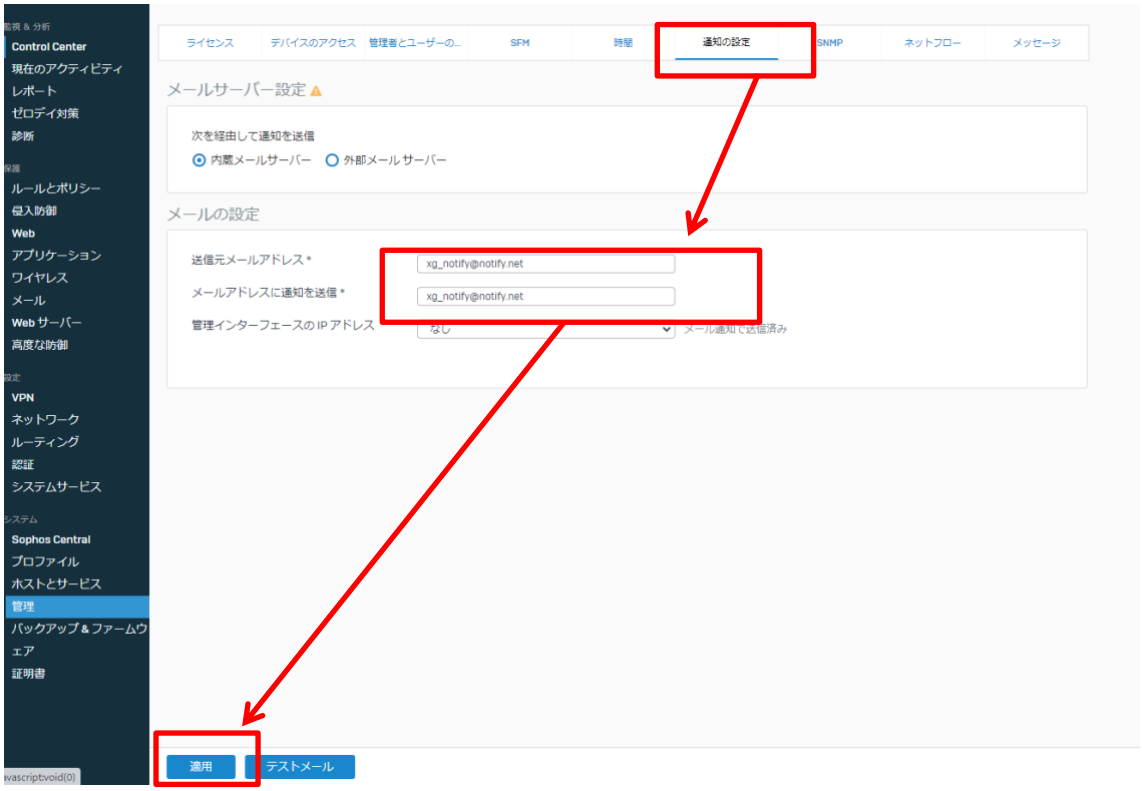
5－1．Sophos Firewall の初期設定

（1）基本情報変更手順

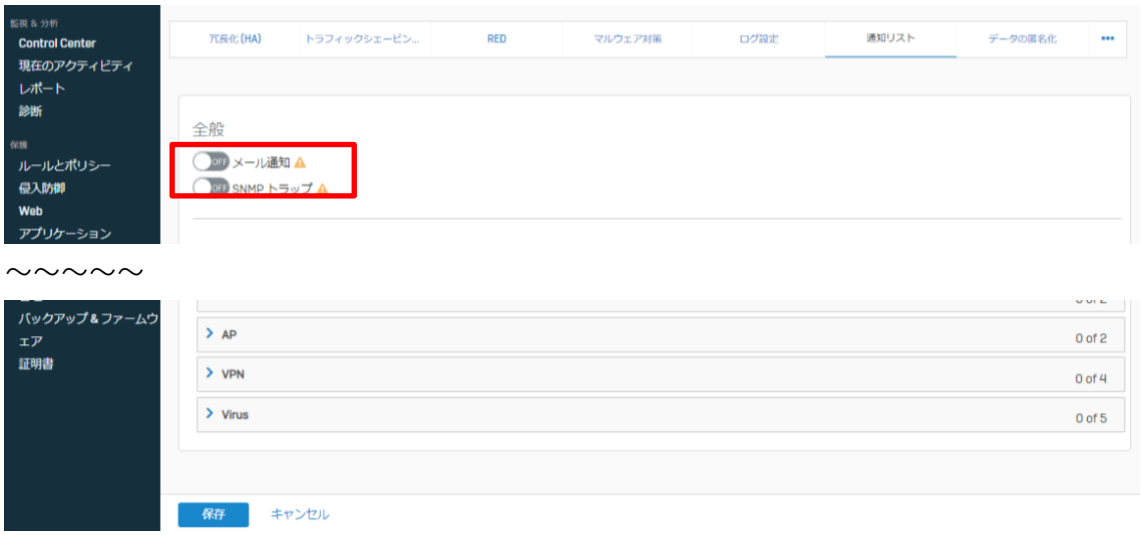
ここでは Sophos Firewall ホスト名、管理者メールアドレス変更を行います。

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。

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。



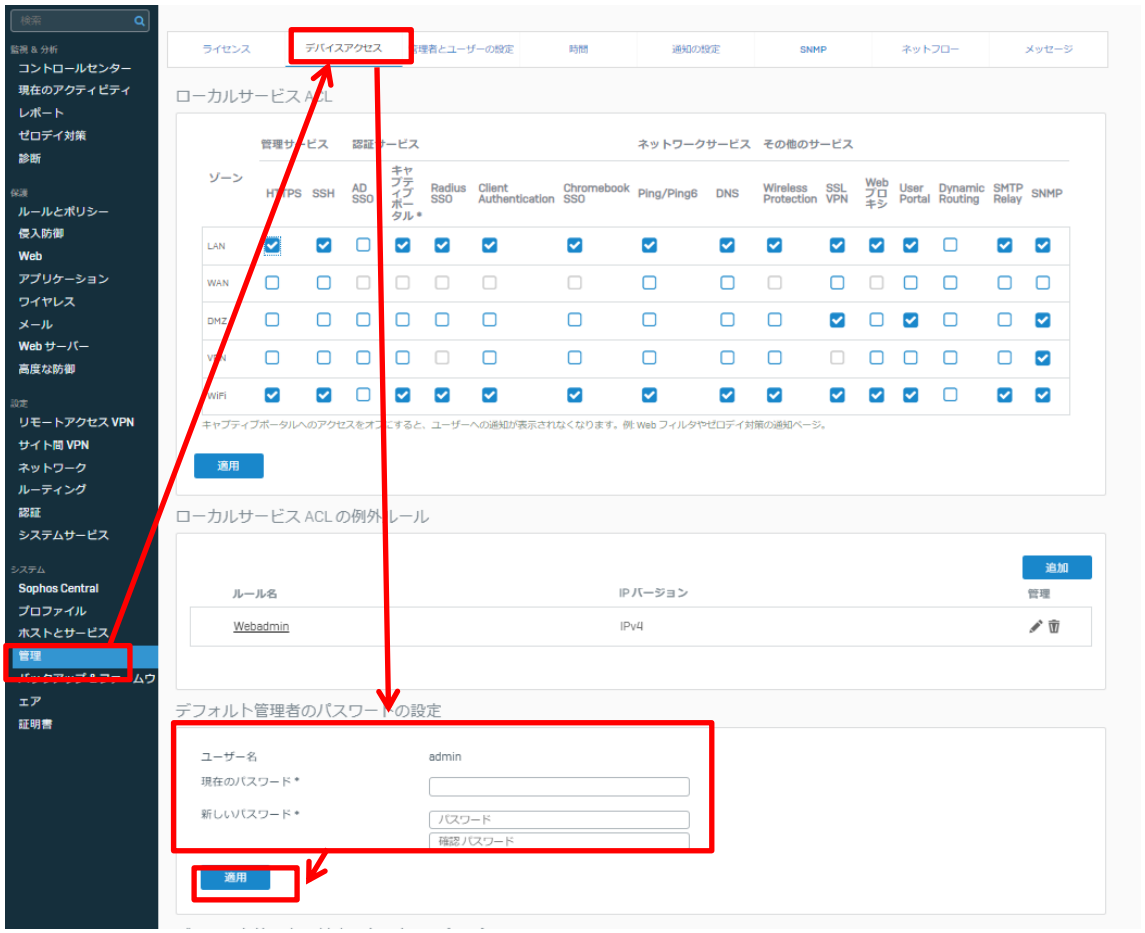
③システムサービス ＞通知リスト タブをメール通知を ON にし、画面下部の適用ボタンを押下します。この設定により各種アクションによるメール通知が有効になります。



～～～～～

（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。



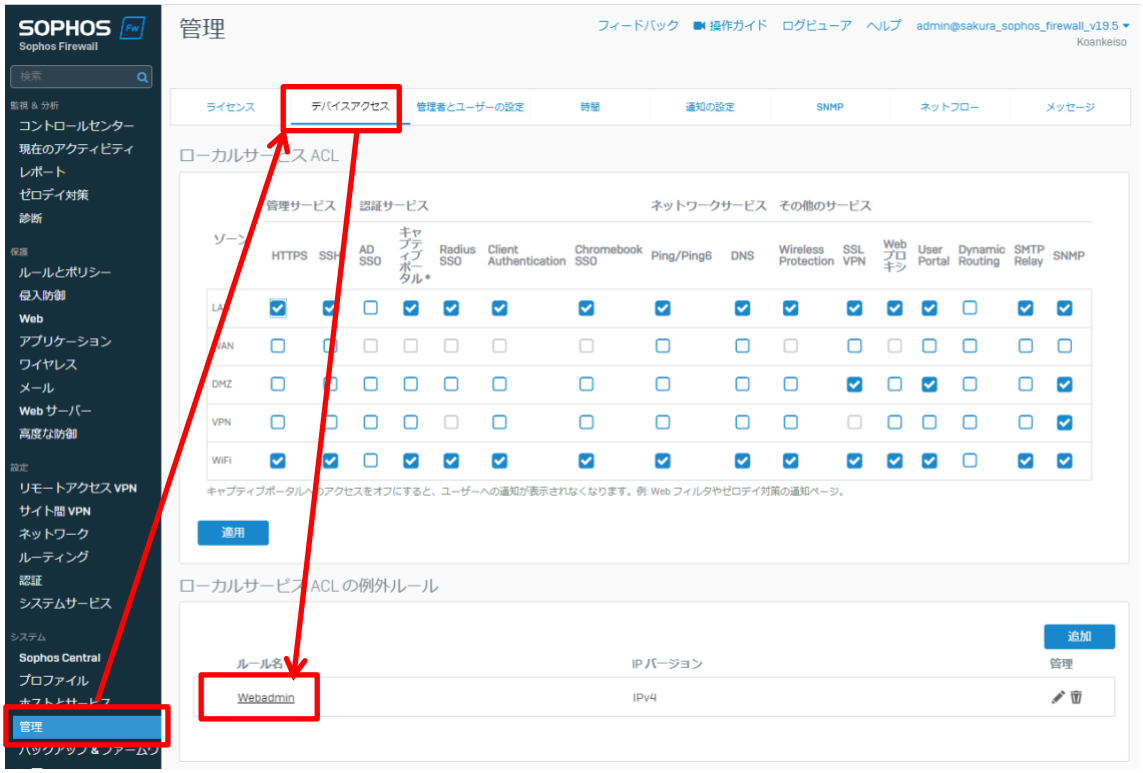
管理者パスワードの変更は必ず行うようお願いいたします。

（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。

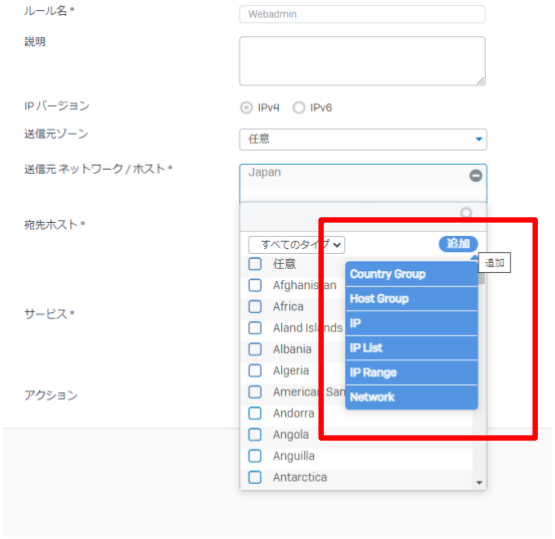
ご利用環境に合わせて、Web 管理コンソールにアクセスする IP アドレス、もしくはネットワークの情報をご準備ください。

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。



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」の設定個所から「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。



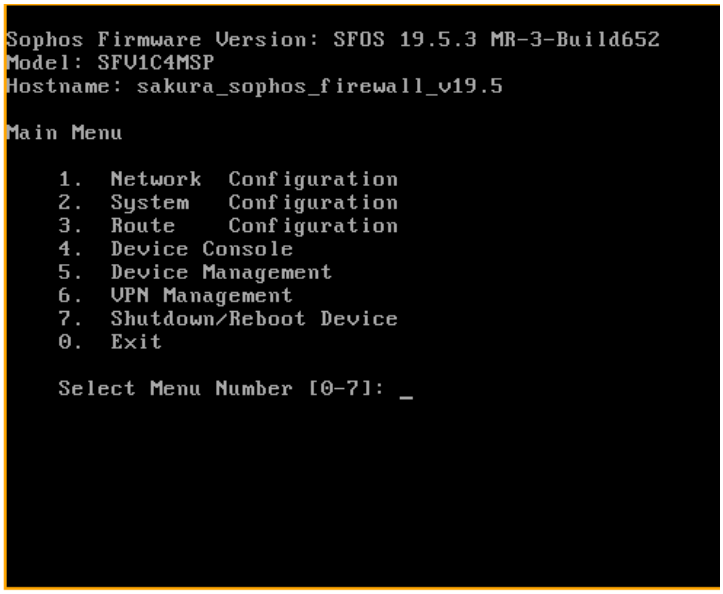
③　「IP」を押下するとポップアップウインドウが表示されます。
この画面から以下の通り設定します。
・名前：設定するうえでの登録名です。登録後は左メニューの「ホストとサービス」から確認できます。
・IP バージョン：IP v 4 限定です。設定変更はできません。
・種類：登録種類を選ぶことができます。キャプチャ画面では IP アドレスを入力しています。
・IP アドレス：アクセスを許可したい IP アドレスを入力します。
入力が完了したら「保存」ボタンを押下します。

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。

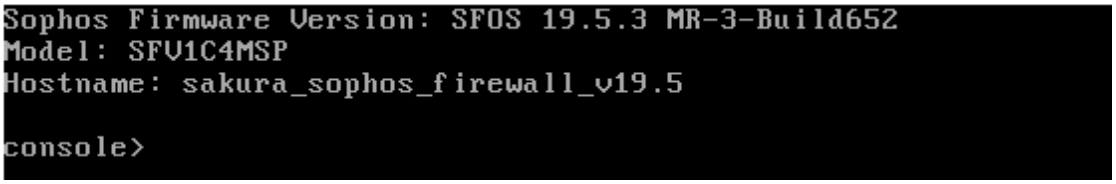
⑤ 設定が完了したら「保存」を押下します。保存されたタイミングでアクセス制御が有効となるので注意してください。

（4）Web 管理コンソールにアクセスできなくなってしまった場合の復旧方法

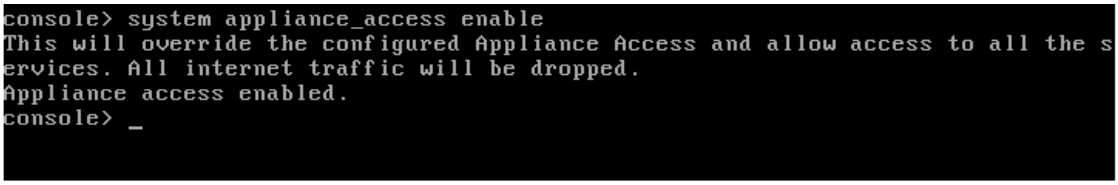
①さくらのクラウドコントロールパネルより、「コンソール」画面に遷移しログインします。



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



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



すべての設定が上書きされ、アクセスが可能となります。

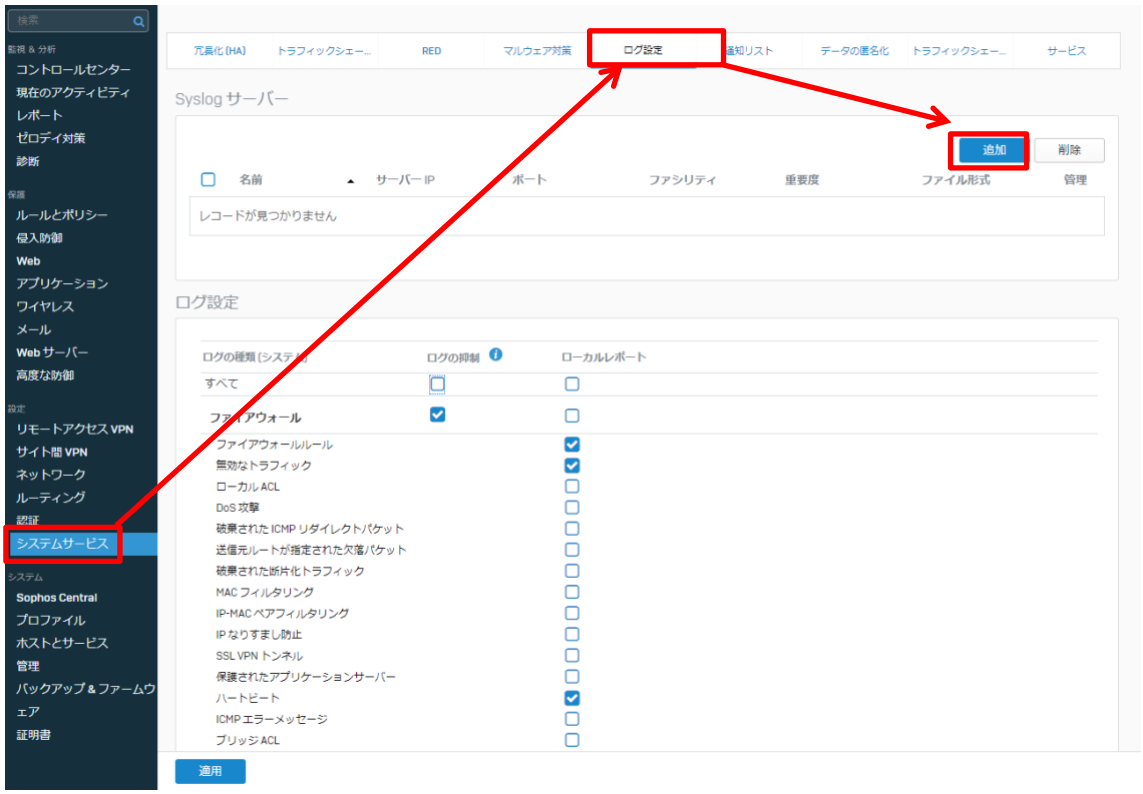
④設定が復旧出来たら、この画面から system appliance_access disable と入力し Enter を押下します。すべてアクセス可能な状態から、Web 管理コンソールからアクセス制御の設定が効いた状態となります。

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。



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

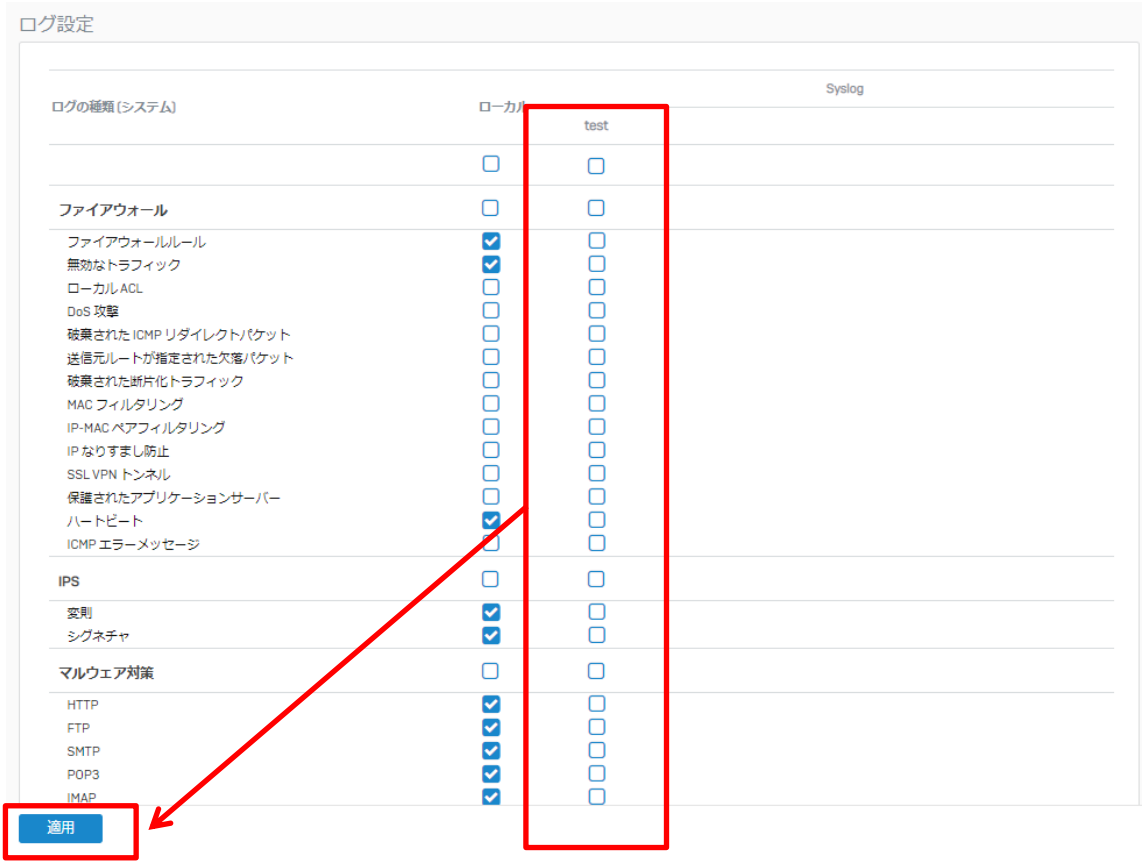
ポート：通信ポート（514）

ファシリティ：選択

重要度レベル：選択

ファイル名：選択

③ 転送したいログ種別を選択し適用を押下します。



（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。

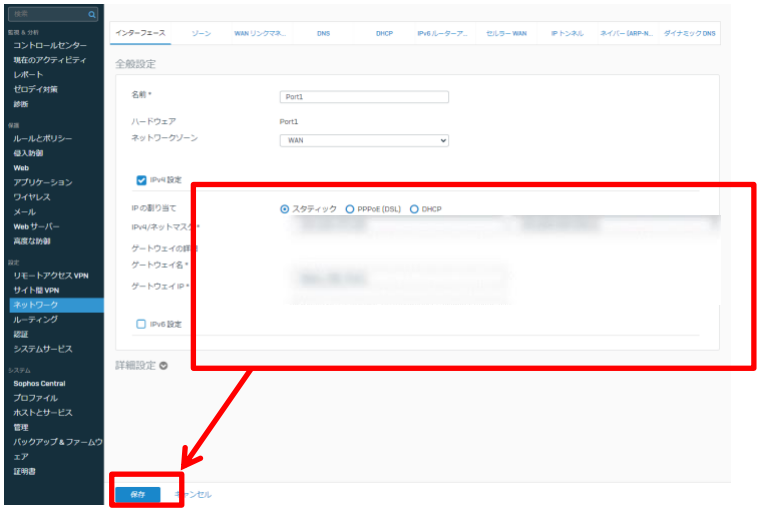
IP の割り当て：スタティック

IPv4/ネットマスク：1.1.1.10/24

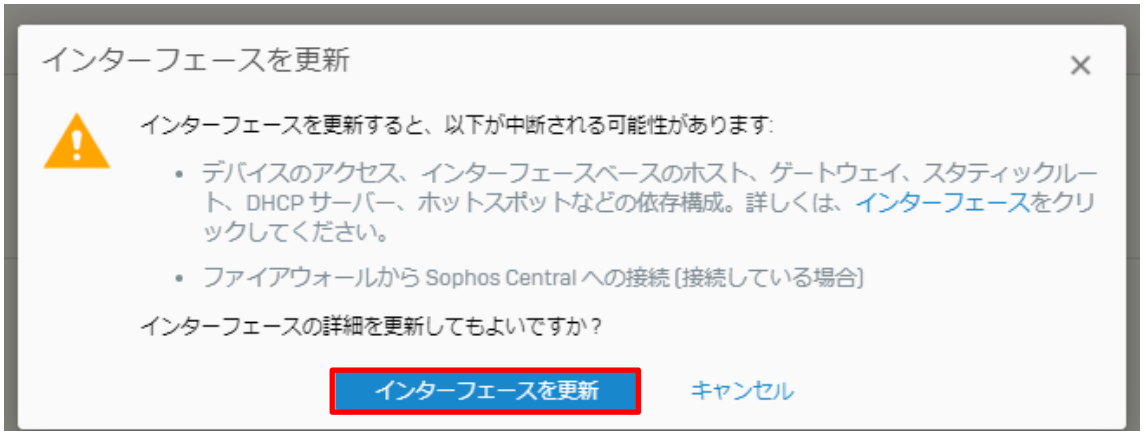
ゲートウェイ名：任意

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 インターフェースを有効にし、スイッチへの接続設定を行います。

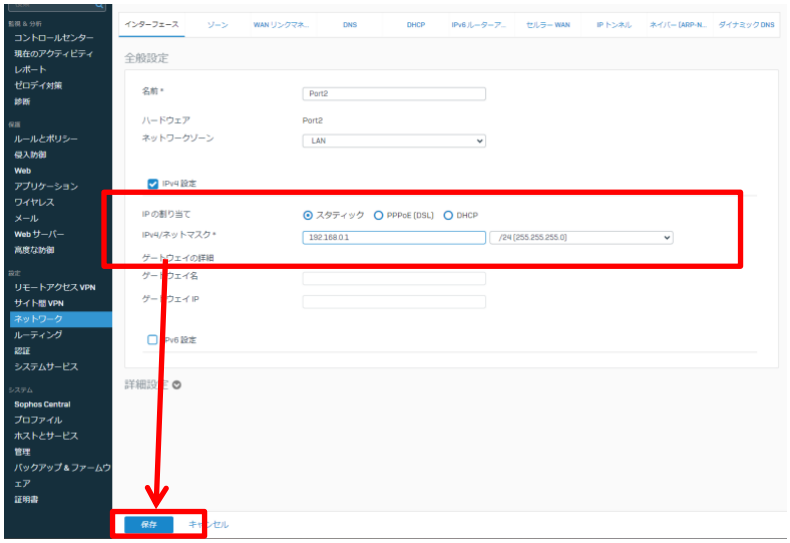
① ネットワーク ＞ インターフェースタブより Port2 を押下します。

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

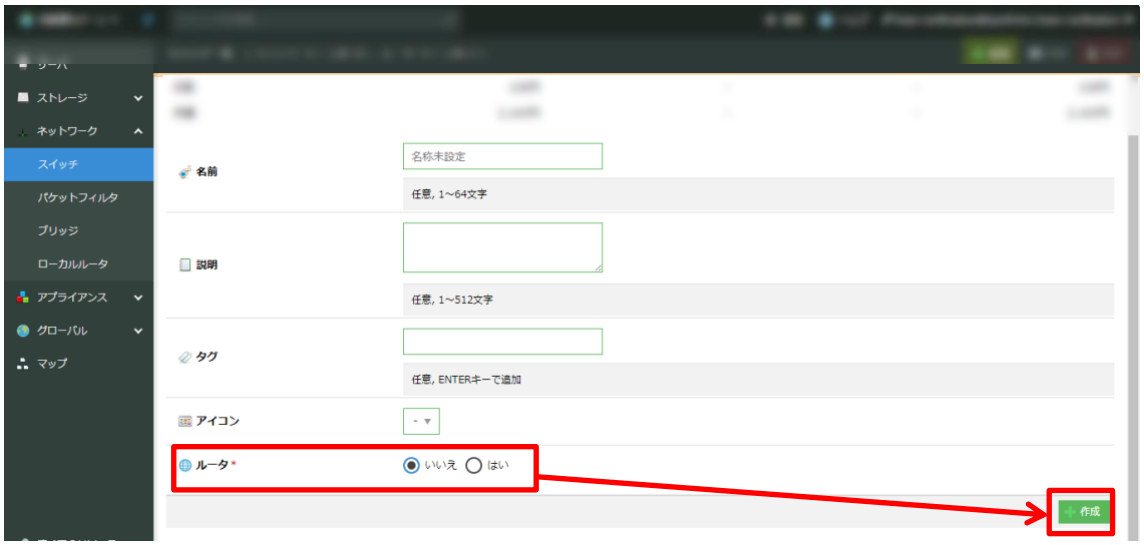
保存ボタンを押下します。



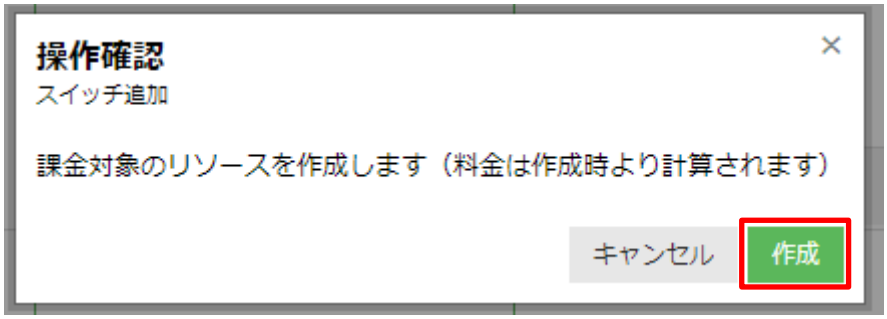
③Port2（LAN ゾーン）配下のスイッチに接続するために、画面右上の admin をクリックし、デバイスのシャットダウンを押下します。

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。



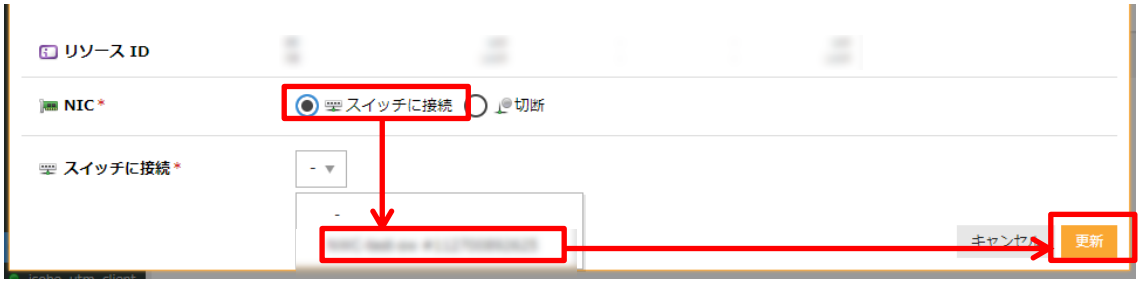
確認メッセージで追加を押下し、スイッチ追加プロセスを実行します。



⑥追加したスイッチに接続します。

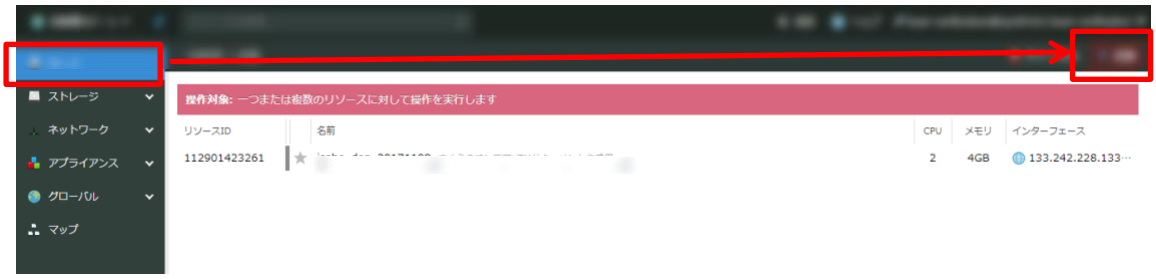
「１未接続」の NIC 列の最右のメニューを展開し、接続を編集を押下します。

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。

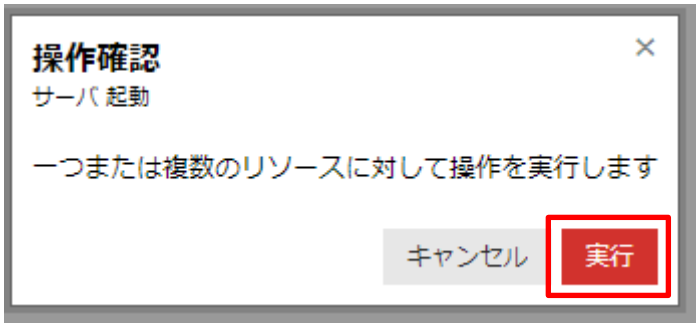


NIC 接続プロセスが成功したことを確認します。

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。



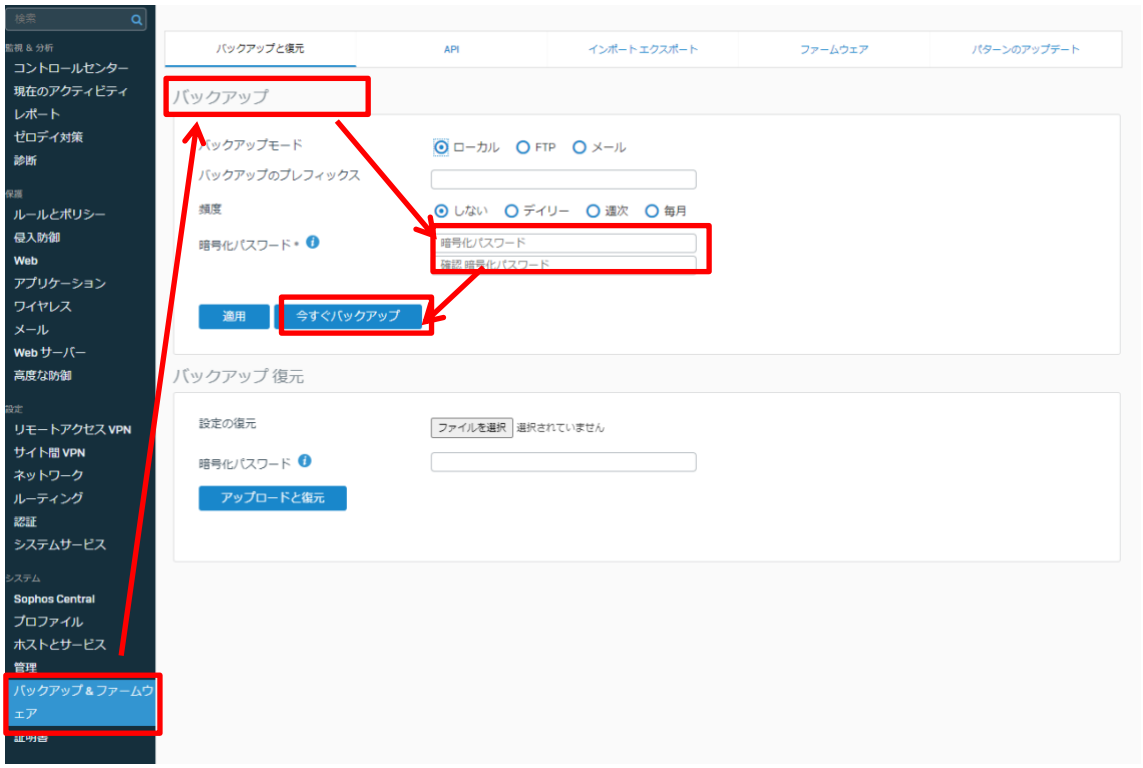
確認画面より実行ボタンを押下します。



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。

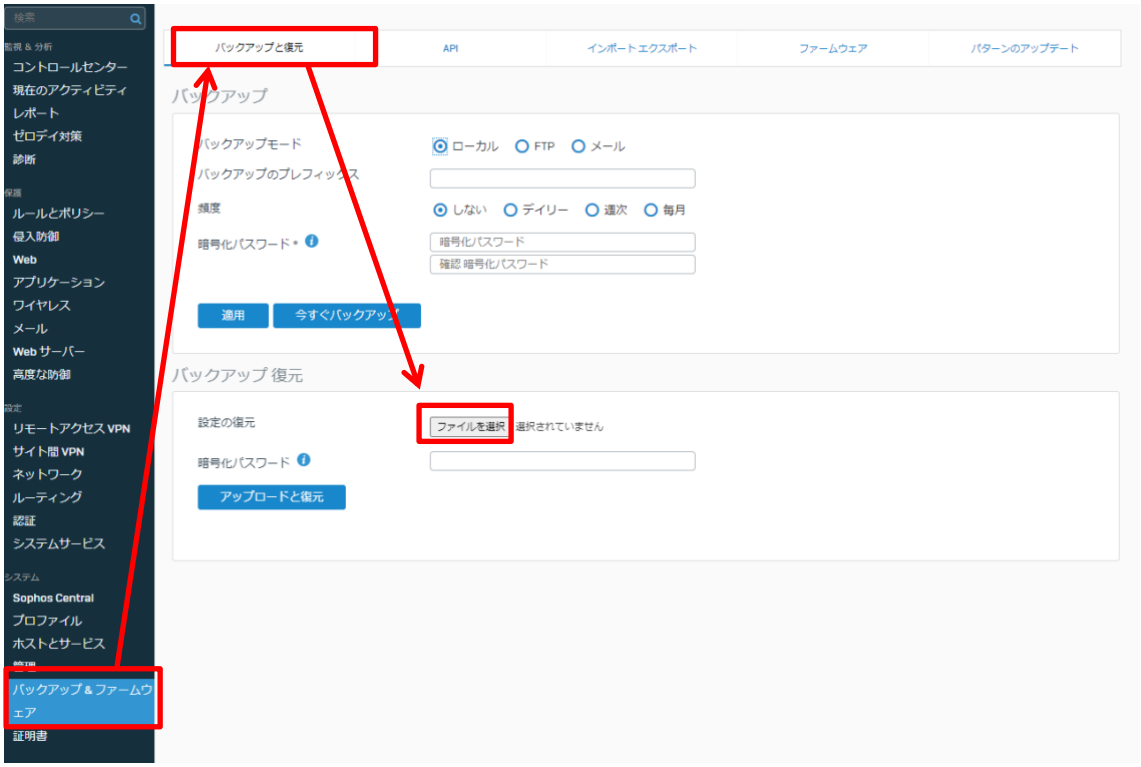
③バックアップのダウンロードを押下します。

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。

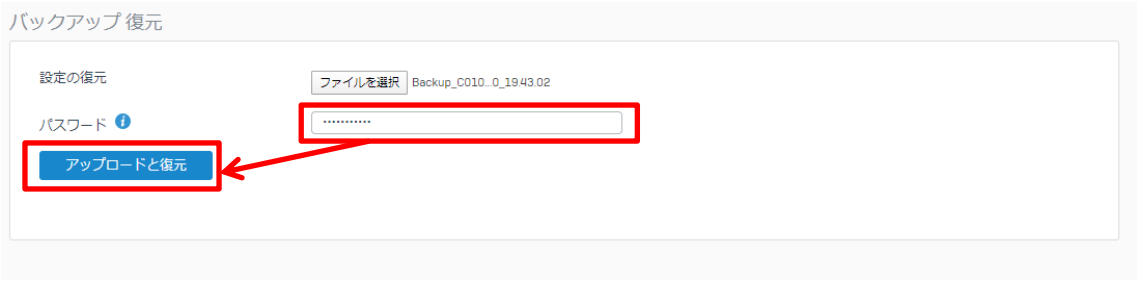
（9）リストア手順

※リストア時、Sophos Firewall は再起動します。

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、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。

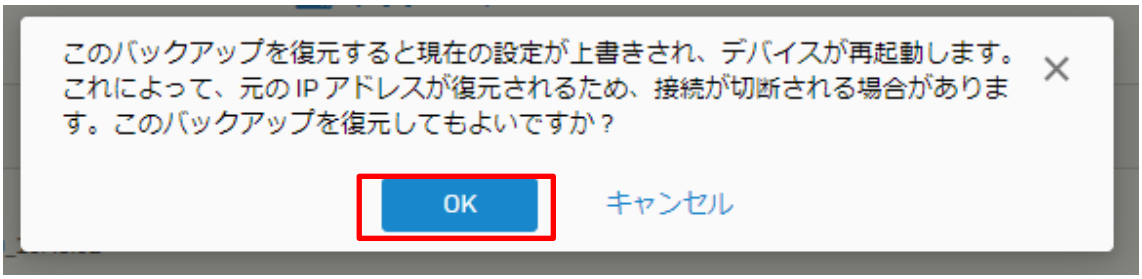


②バックアップ取得時に設定したパスワードを入力しアップロードと復元を押下します。



③セキュアストレージマスターキーを入力します。

④内容を確認し OK を押下します。

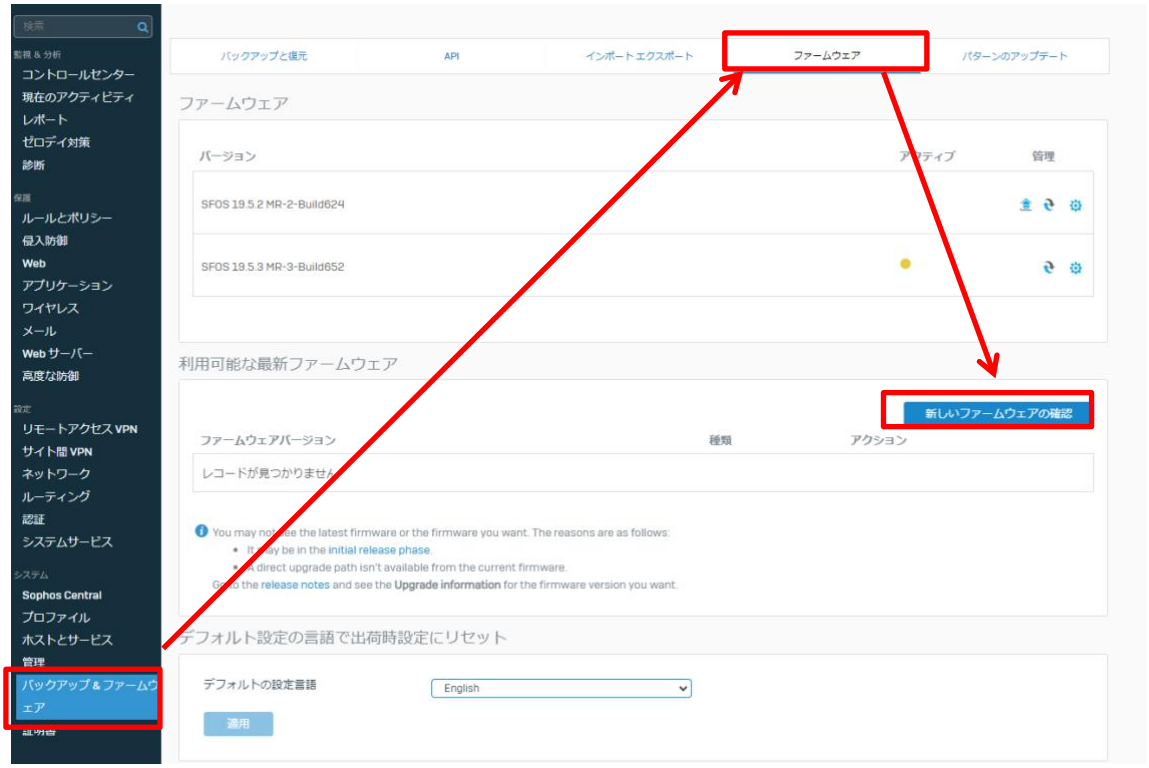


⑤再度、WebAdmin にログインしバックアップ内容が反映されていることを確認します。
またリストアに際して、Sophos Firewall のバージョンが同一でないとリストアすることができません。

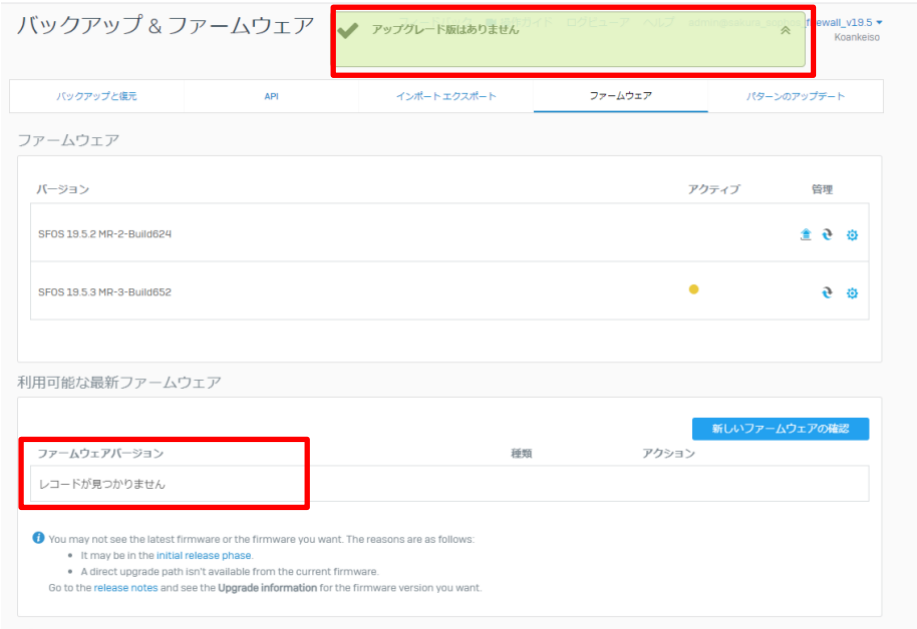
（１０）ファームウェア（SFOS）更新手順

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。

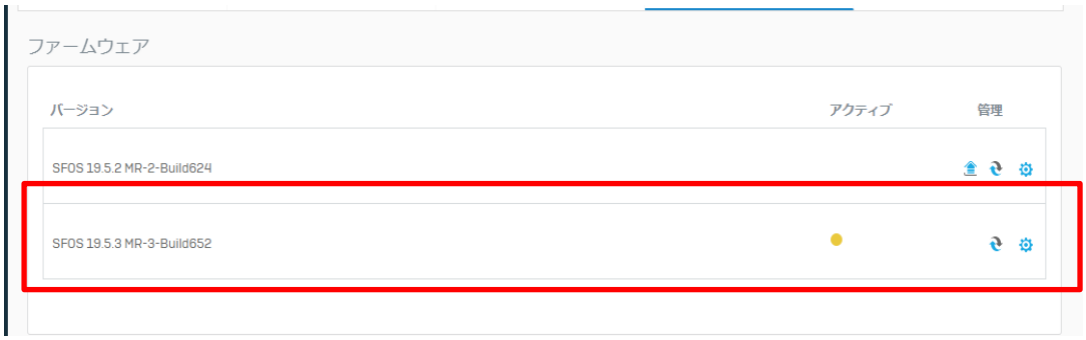


② ファームウェアが見つかった場合、以下の通り表示されます。

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。

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「〇（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。

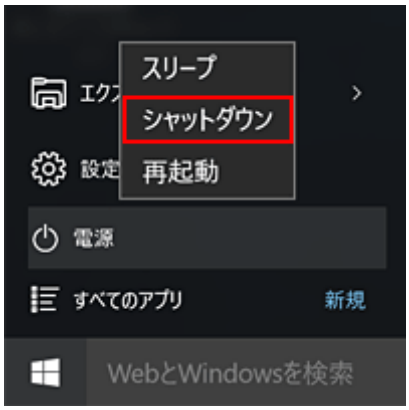


⑥ もし設定を戻したい場合には、以下のマークをクリックすることで、任意のファームウェアで Sophos Firewall を起動させることが可能です。**Sophos Firewall 内で保持できるファームウェアは 2 つまでです。**

5－2．保護対象システム（WindowsServer2016）の初期設定

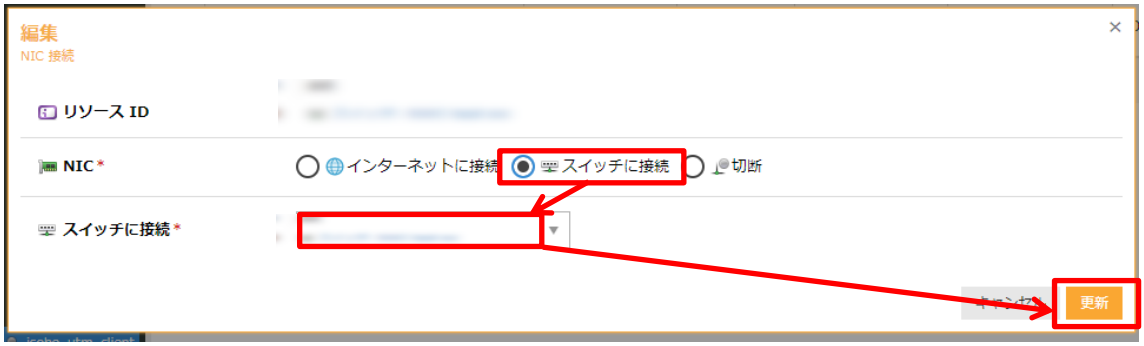
保護対象システムを Sophos Firewall で保護するためには、インターネットへのアクセスを必ず Sophos Firewall を経由させる必要があります。その為、プライベートセグメントに展開したスイッチに保護対象を接続し、デフォルトゲートウェイを Sophos Firewall に対し設定する必要があります。

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。



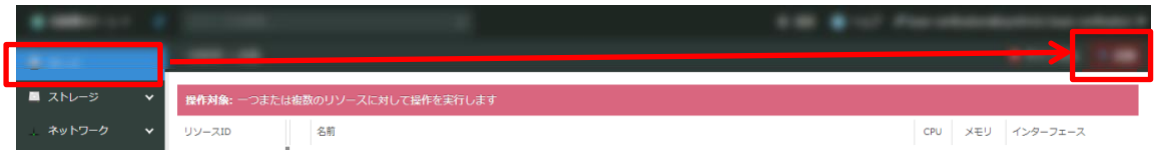
②NIC を作成したスイッチに接続します。
NIC 列の最右のメニューを展開し、接続を編集を押下します。

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。

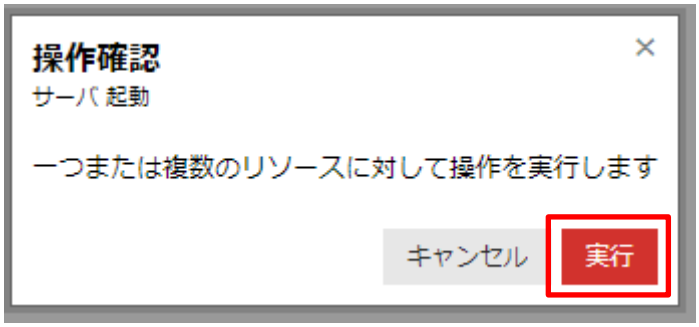


NIC 接続プロセスが成功したことを確認します。

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。

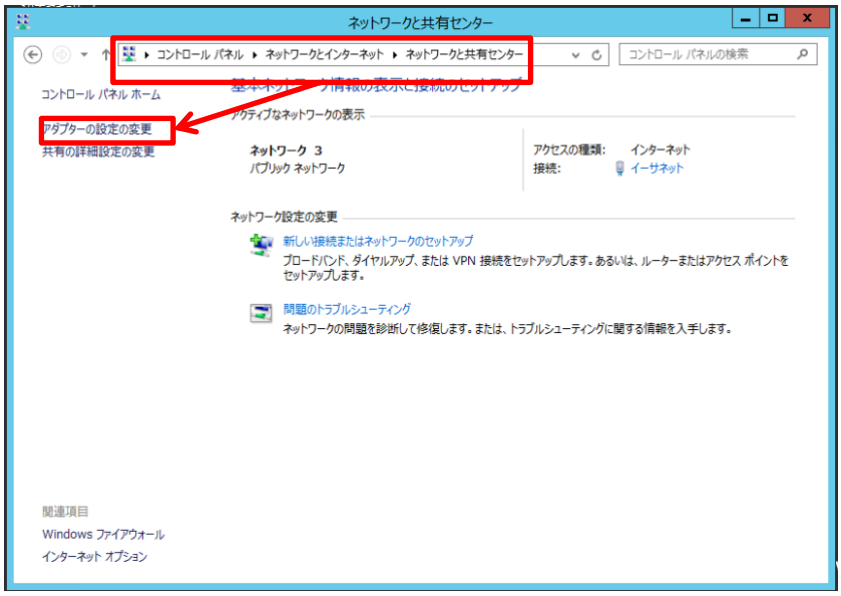


確認画面より実行ボタンを押下します。

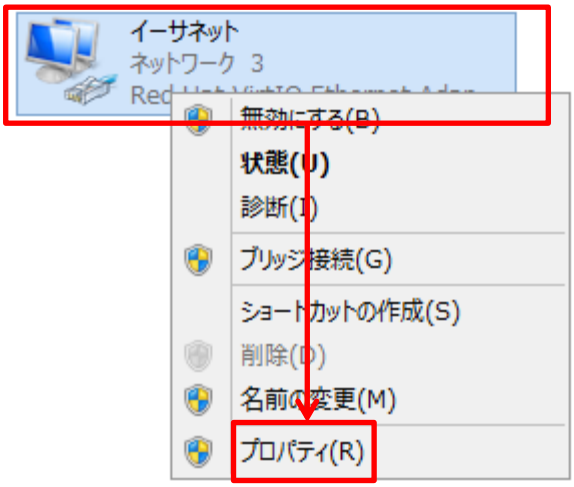


サーバ起動プロセスが成功したことを確認します。

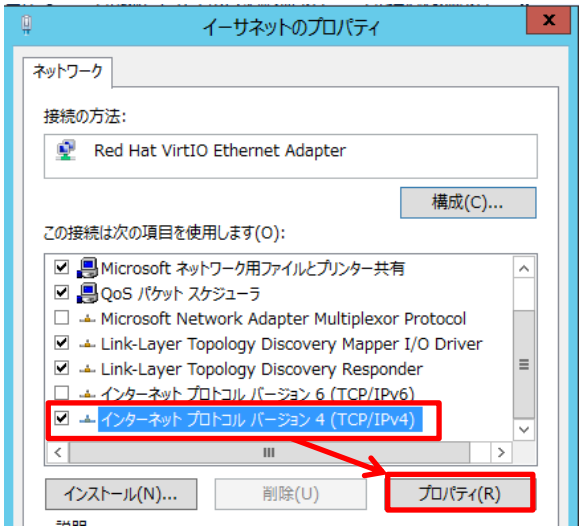
⑤保護対象システムへアクセスし IP アドレスとデフォルトゲートウェイの設定を行います。
コントロール パネル ＞ ネットワークとインターネット ＞ ネットワークと共有センター
を開き、アダプターの設定変更を押下します。



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。



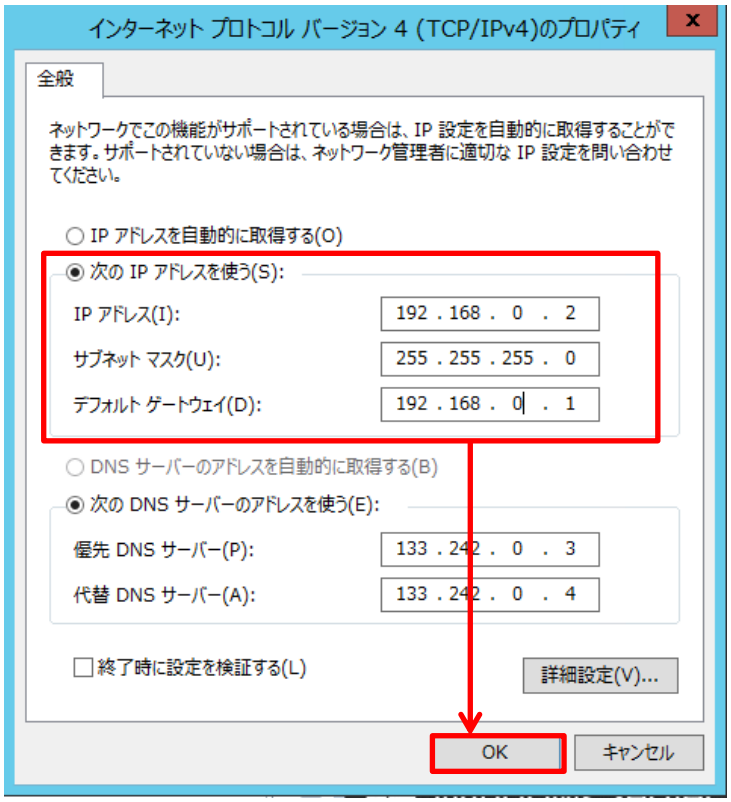
⑧プロパティ画面から以下の通り、設定を入力し、OK ボタンを押下します。

●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しの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

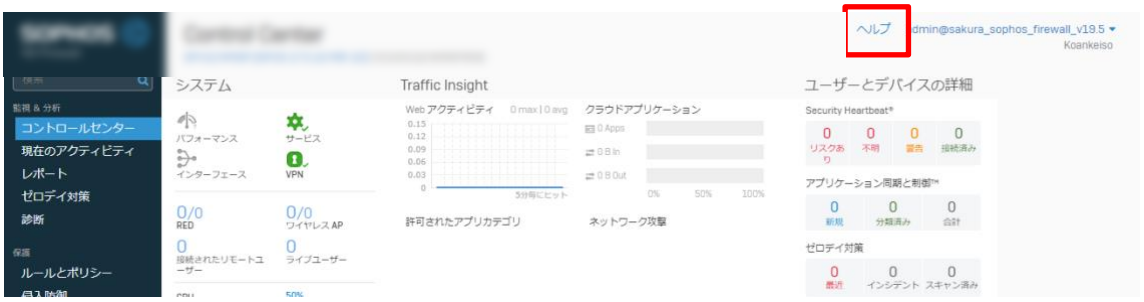
さくらのクラウド環境では、Sophos Firewall が具備する HA 機能をご利用いただけます。VRRP のようなネットワーク通信プロトコルには対応しておりません。

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が開きます。

以上