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

HA 編

第 1.1 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	2022/4/20	初版作成	興安計装株式会社
1.1	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. **Sophos Firewall での HA を含む構成例**
2. **HA 動作モードの説明**
3. **HA 構築手順（アクティブ－パッシブモード）**
4. **HA 構築手順（アクティブ－アクティブモード）**
5. **HA ノードに対するオペレーション**
6. **詳細の機能と設定を知りたい時**

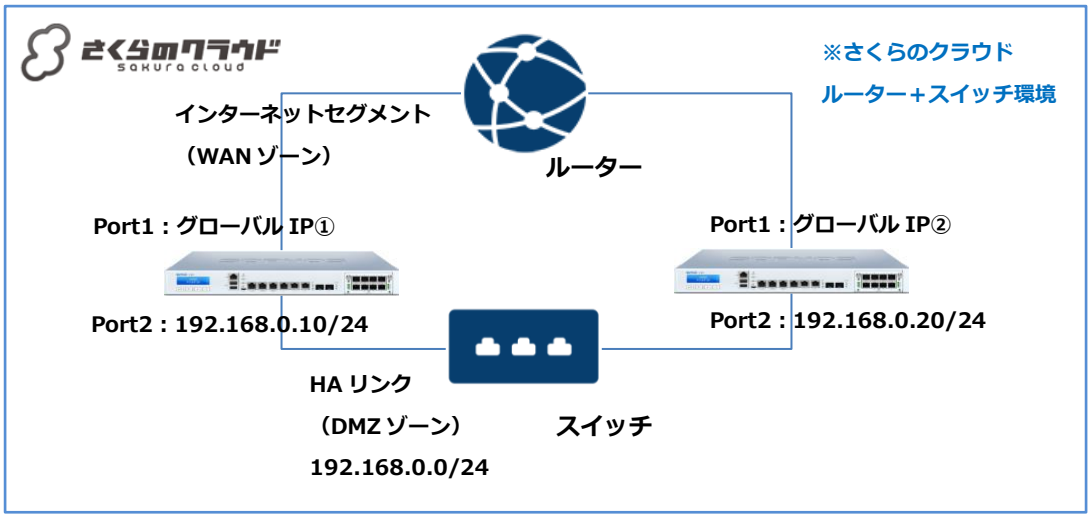
本手順書は以下の手順書に沿って Sophos Firewall が展開されアクティベートされた、状態を前提としております。

初期導入編

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

1. Sophos Firewall での HA を含む構成例

本手順書では以下の構成例を前提に記載いたします。



【構成要件】

- Sophos Firewall は同様のサイズ、同様の OS バージョンのインスタンスを 2 つ用意します。
- Sophos Firewall は WAN ゾーン側と DMZ ゾーン側の 2 つの NIC を持ちます。
- WAN ゾーン側の NIC はさくらのクラウド「ルーター＋スイッチ」にて 2 つ以上のグローバル IP アドレスを利用可能なルーターを構築して接続します。
- DMZ ゾーン側の NIC はさくらのクラウド「ルーター＋スイッチ」にてスイッチを構築して接続します。
- Sophos Firewall の WAN 側 NIC には、それぞれに同一のルーター＋スイッチから払い出されるグローバル IP アドレスを設定します。
- Sophos Firewall の DMZ 側 NIC には、スイッチ内で相互に通信可能なプライベートアドレスを設定します。（例では 192.168.0.10/24、192.168.0.20/24）
- HA を構築したうえで、保護対象を収容する場合は、必要に応じて NIC を追加いただきますが、2 台のインスタンスの NIC 構成は必ず同様の構成としてください。
- HA を構成する Sophos Firewall を、それぞれさくらのクラウドの別リージョンに構築することも可能です。その場合は、WAN 側、DMZ 側両方をスイッチに接続し、スイッチ同士をさくらのクラウド「ブリッジ」で接続し、WAN 側スイッチに別途インターネットと通信可能な VPC ルーター等の機器を接続してください。
- 別リージョン同士の Sophos Firewall で HA を構成した場合、インターネット経路上の不具合によってキープアライブが欠落すると、機器に異常がなくともアクティブノードが切り替わる可能性があるため、キープアライブ設定を適切に調整する必要があります。

2. HA 動作モードの説明

2.1 「アクティブ－パッシブモード」「アクティブ－アクティブモード」について

Sophos Firewall では、2 台の同一サイズ、同一 OS バージョン、同一 NIC 構成のノードを冗長構成として動作させることができ、これを HA（High Availability）と呼びます。

HA の動作モードには、2 台のノードのうち 1 台のみが動作し、動作ノードに障害が発生した場合にもう一台のノードが変わって動作する「アクティブ－パッシブモード」と、2 台のノードが同時に動作し、一方に障害が発生しても 1 台のみで縮退運転を行う「アクティブ－アクティブモード」の 2 種類の動作モードがあります。

2.2 ライセンス体系について

「アクティブ－パッシブモード」で動作させる場合、ライセンスはアクティブ側の機器 1 台分のみで動作させることが可能です。

HA 構成を構築完了するまで、パッシブ側として動かすホストのライセンスは 30 日分のトライアルライセンスにて構築してください。

トライアルライセンスの適用は、インスタンスデプロイ後の初回アクセス時、ファイアウォールの登録画面で「シリアル番号がない（試用を開始）」を選択いただき、「Sign In」ボタンから以下のメールアドレスとパスワードで登録を行うことで、登録から 30 日間利用可能となります。

sophos-support@sakura.ad.jp Wz9HEEjWqjNF

※ 上記のメールアドレス、パスワードを使用したトライアルライセンスの利用は、さくらのクラウド上のインスタンスでのみご利用いただけます。

「アクティブ－アクティブモード」で動作させる場合、ライセンスは 2 台分をご用意いただく必要があります。

構築時には、2 台分のライセンスを用意して、それぞれのノードを構築してください。

2.3 HA 動作について

HA 切り替わりに関する詳細な動作仕様については、Sophos 社の提供するドキュメントを参照ください。

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

3. HA 構築手順（アクティブ－パッシブモード）

3.1. デバイスアクセス設定の変更（両ノードとも）

システム> 管理> デバイスのアクセス> ローカルサービスの ACL

DMZ ゾーンにて SSH の許可をチェックします。

その他のゾーン、サービスについては用途にあわせて適切に設定してください。

3.2. 補助ノードの設定（トライアルライセンスで動作させている側）

設定> システムサービス> 冗長化[HA]> 冗長化の設定

初期のデバイスのロール：補助

HA 設定モード：対話側モード

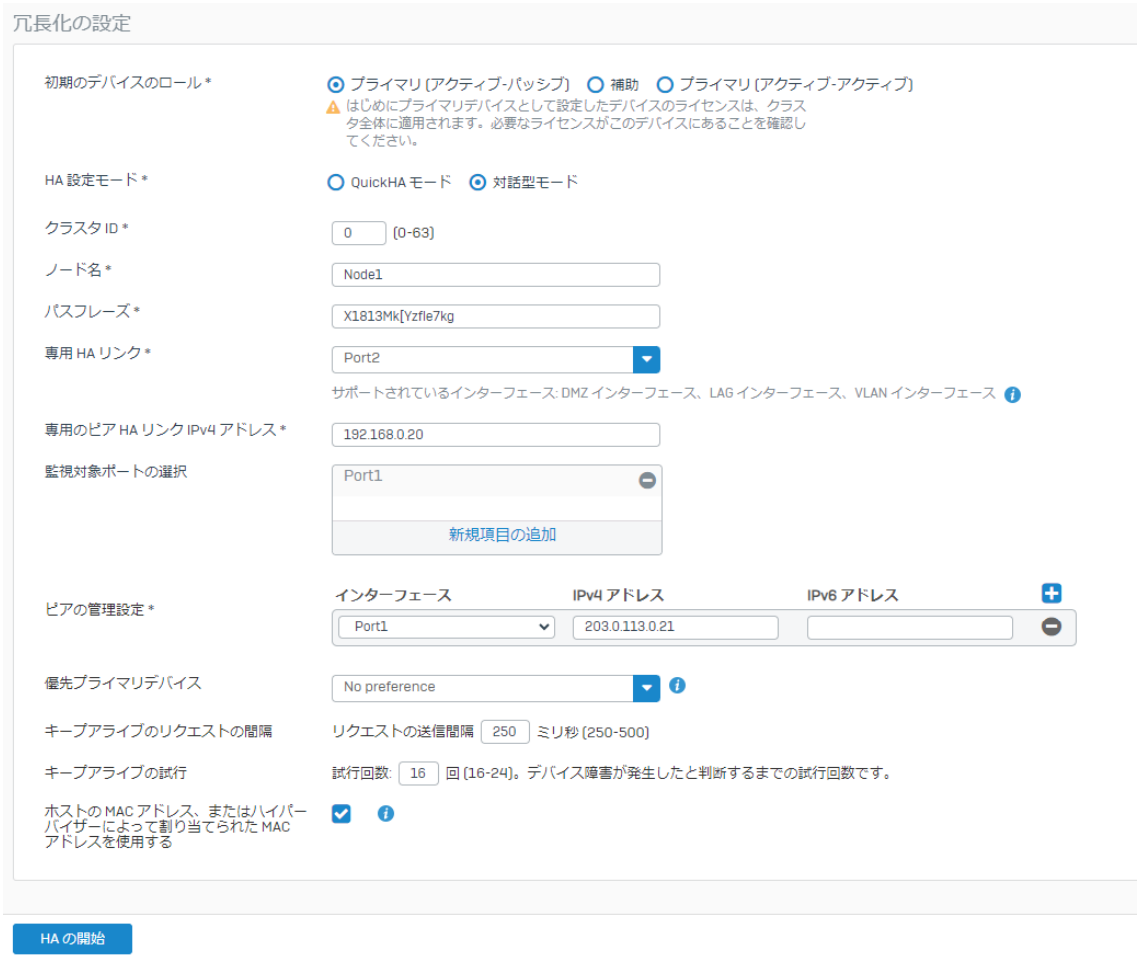
パスフレーズ：任意（プライマリ側にも同様のフレーズを設定するのでメモしておく）

専用 HA リンク：HA リンク用に設定した DMZ 側 NIC（今回は Port2）

保存ボタンを押下して、HA 構築待ちの状態になることを確認する。

3.3. プライマリノードの設定（正規ライセンスで動作させている側）

設定> システムサービス> 冗長化[HA]> 冗長化の設定



初期のデバイスのロール：プライマリ（アクティブ－パッシブ）

HA 設定モード：対話側モード

クラスタ ID：初期値（0）

ノード名：任意

パスフレーズ：任意（補助側にて設定したフレーズ）

専用 HA リンク：HA リンク用に設定した DMZ 側 NIC（今回は Port2）

専用のピア HA リンク IPv4 アドレス:補助側の Port2 に設定したアドレス(今回は 192.168.0.20)

監視対象ポートの選択：ポート故障監視対象ポートの選択（今回は Port1 のみ選択）

※　ここで設定したポートに不具合があった場合、アクティブノードが切り替わります。

※　HA リンクポートは選択できません。

ピアの管理設定：

　　インターフェース：Port1

　　IPv4 アドレス：補助側の Port2 に設定したアドレス（今回はグローバルアドレス②）

　　IPv6 アドレス：初期値のまま（空欄）

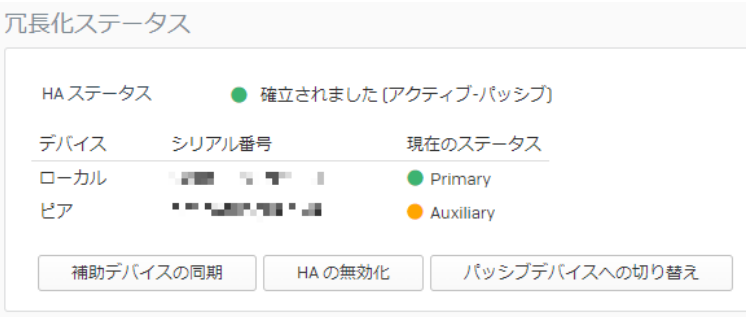
優先プライマリデバイス：初期値のまま（No preference）

※　本項目で優先プライマリデバイスを指定した場合、障害発生による切り替わり後、指定デバイスが復旧次第フェイルバックが行われる動作となります。

キープアライブのリクエストの間隔：初期値のまま（250）

キープアライブの試行：初期値のまま（16）

ホストまたはハイパーバイザーに割り当てられた MAC アドレスを使用する：チェックあり



HA の開始を押下し、数分間待機し、HA ステータスが確立されたことを確認する。

4. HA 構築手順（アクティブ－アクティブモード）

4.1. デバイスアクセス設定の変更（両ノードとも）

システム> 管理> デバイスのアクセス> ローカルサービスの ACL

DMZ ゾーンにて SSH の許可をチェックします。

その他のゾーン、サービスについては用途にあわせて適切に設定してください。

4.2. 補助ノードの設定

設定> システムサービス> 冗長化[HA]> 冗長化の設定

初期のデバイスのロール：補助

HA 設定モード：対話側モード

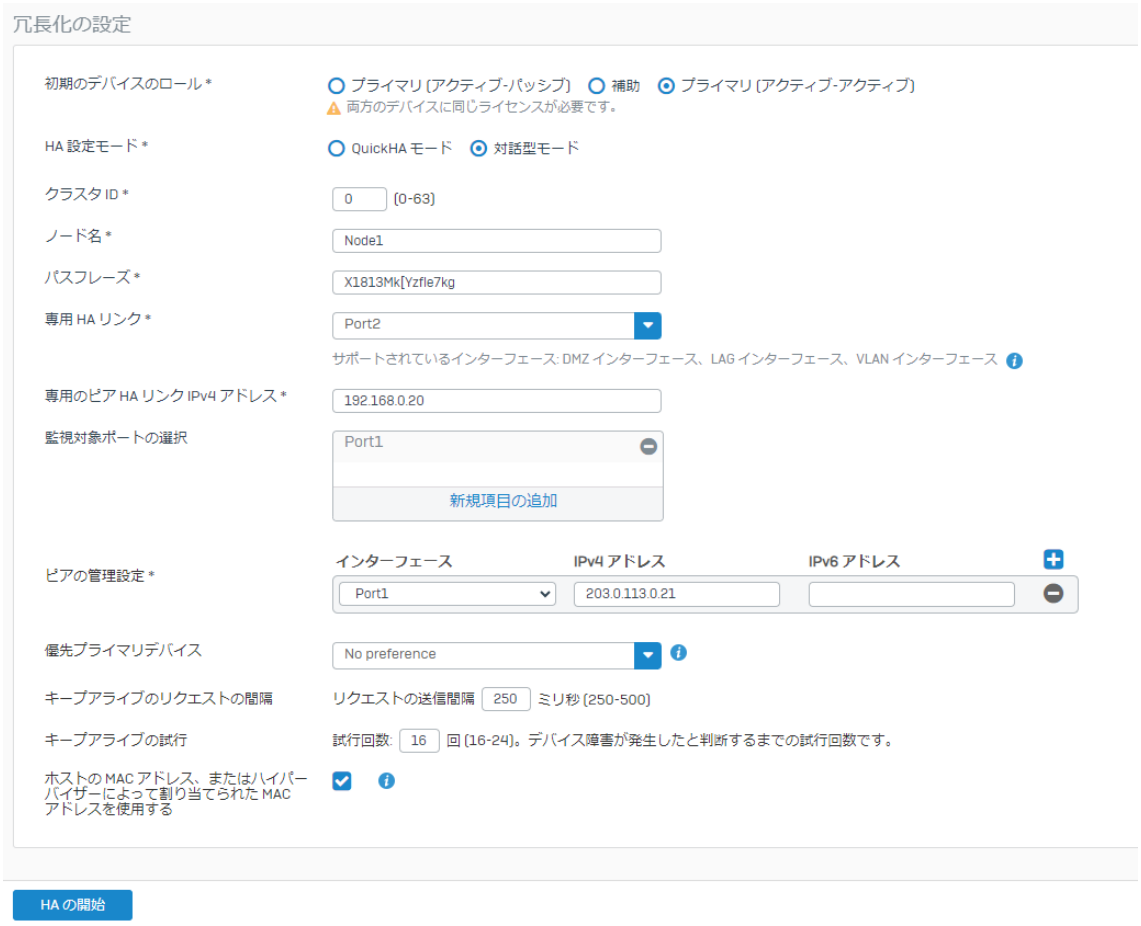
パスフレーズ：任意（プライマリ側にも同様のフレーズを設定するのでメモしておく）

専用 HA リンク：HA リンク用に設定した DMZ 側 NIC（今回は Port2）

保存ボタンを押下して、HA 構築待ちの状態になることを確認する。

4.3. プライマリノードの設定

設定> システムサービス> 冗長化[HA]> 冗長化の設定



初期のデバイスのロール：プライマリ（アクティブ－アクティブ）

HA 設定モード：対話側モード

クラスタ ID：初期値（0）

ノード名：任意

パスフレーズ：任意（補助側にて設定したフレーズ）

専用 HA リンク：HA リンク用に設定した DMZ 側 NIC（今回は Port2）

専用のピア HA リンク IPv4 アドレス:補助側の Port2 に設定したアドレス(今回は 192.168.0.20)

監視対象ポートの選択：ポート故障監視対象ポートの選択（今回は Port1 のみ選択）

※　ここで設定したポートに不具合があった場合、アクティブノードが切り替わります。

※　HA リンクポートは選択できません。

ピアの管理設定：

インターフェース：Port1

IPv4 アドレス：補助側の Port2 に設定したアドレス（今回はグローバルアドレス②）

IPv6 アドレス：初期値のまま（空欄）

優先プライマリデバイス：初期値のまま（No preference）

※　本項目で優先プライマリデバイスを指定した場合、障害発生による切り替わり後、指定デバイスが復旧次第フェイルバックが行われる動作となります。

キープアライブのリクエストの間隔：初期値のまま（250）

キープアライブの試行：初期値のまま（16）

ホストまたはハイパーバイザーに割り当てられた MAC アドレスを使用する：チェックあり

HA の開始を押下し、数分間待機し、HA ステータスが確立されたことを確認する。

5. HA ノードに対するオペレーション

5.1. アクセス

Webadmin への接続は、HA 構築前と同様に可能です。

アクティブ－パッシブモードで構築した場合、パッシブとして動作している側のノードへは、HA 構築時に「ピアの管理設定」で指定した IP アドレスにて接続できます。

5.2. 切り替え

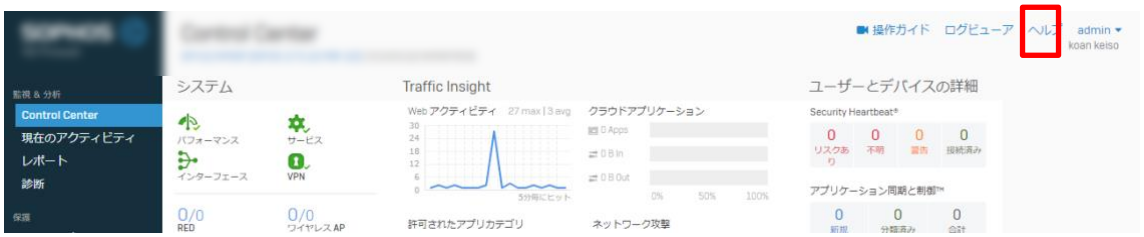
アクティブ－パッシブモードで構築した場合、アクティブとパッシブの切り替えは、

設定＞システムサービス＞冗長化[HA]　画面にて「パッシブデバイスへの切り替え」ボタンで実施できます。

その他、詳細の操作に関しては Sophos 社の提供するドキュメントを参照ください。

6. 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