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

IPsec VPN リモートアクセス接続導入編

第 2.1 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	2021/11/17	初版作成	興安計装株式会社
2.0	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
2.1	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 IPsec VPN リモートアクセス接続を導入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：IPsec による VPN リモートアクセス接続設定および、クライアントアプリ（Sophos Connect）の導入手順をご提供すること。

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

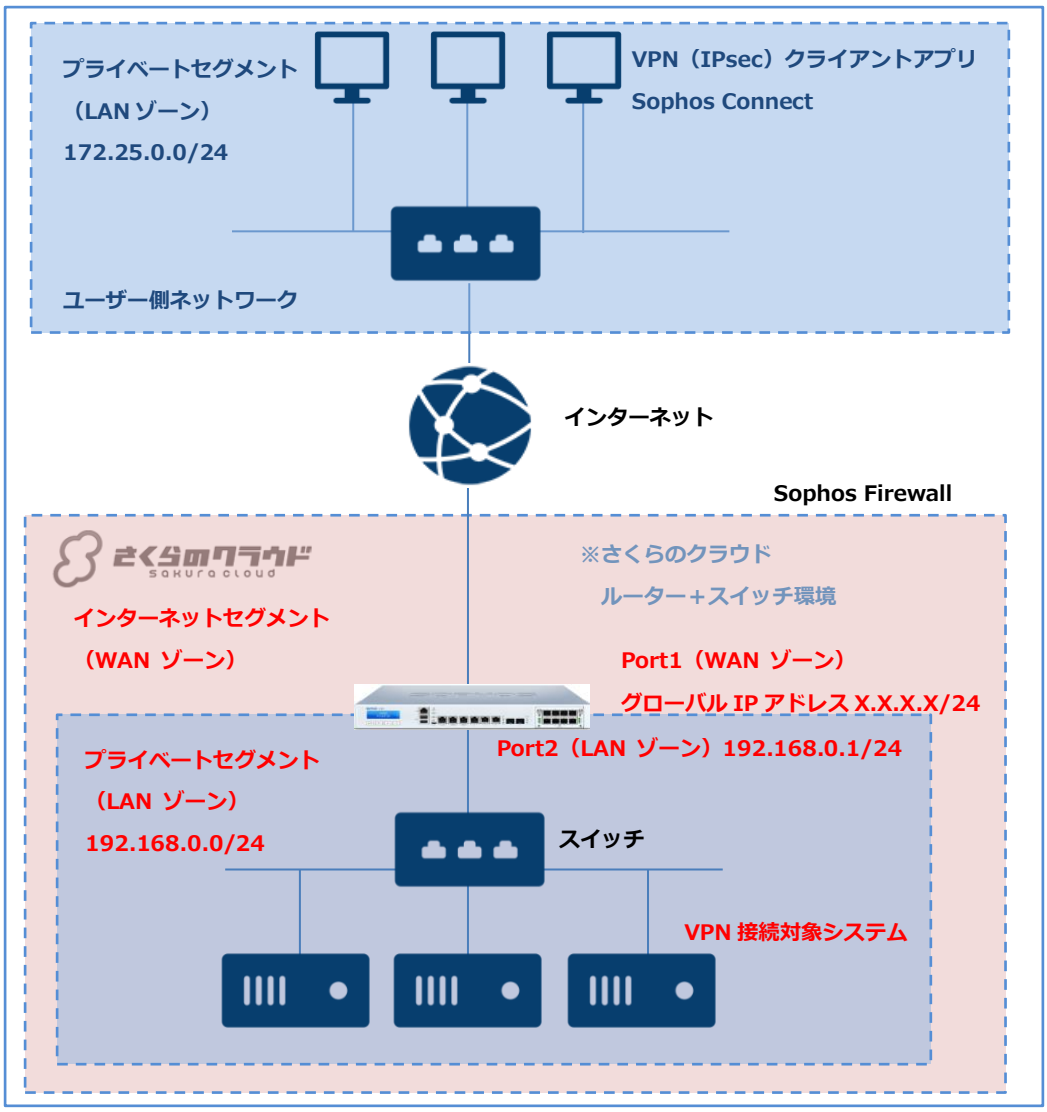
https://www.owlook.jp/public/document/sophos_xg_fw_dnat.pdf

ネットワークプロテクション編

https://www.owlook.jp/public/document/sophos_xg_networkprotection.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。
- さくらのクラウド側の WAN ゾーンは **X.X.X.X/24 のグローバル IP アドレス**を持ちます。
- さくらのクラウド側の 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。
- さくらのクラウド側の LAN ゾーンはスイッチを利用しセグメントを構築します。
- VPN 接続対象システムの IP アドレスはセグメント内のいずれかを持ちます。

- VPN 接続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。
- ユーザー側のプライベートセグメントは 172.25.0.0/24 とします。
- IPsec による VPN 接続はクライアントソフトウェア（Sophos Connect）を使用します。
- **※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。**

2. VPN 接続向けグループ・ユーザーの作成

VPN 接続の許可を与えるグループ・ユーザーの作成を行います。

※本項の設定は管理者が行う設定手順となります。

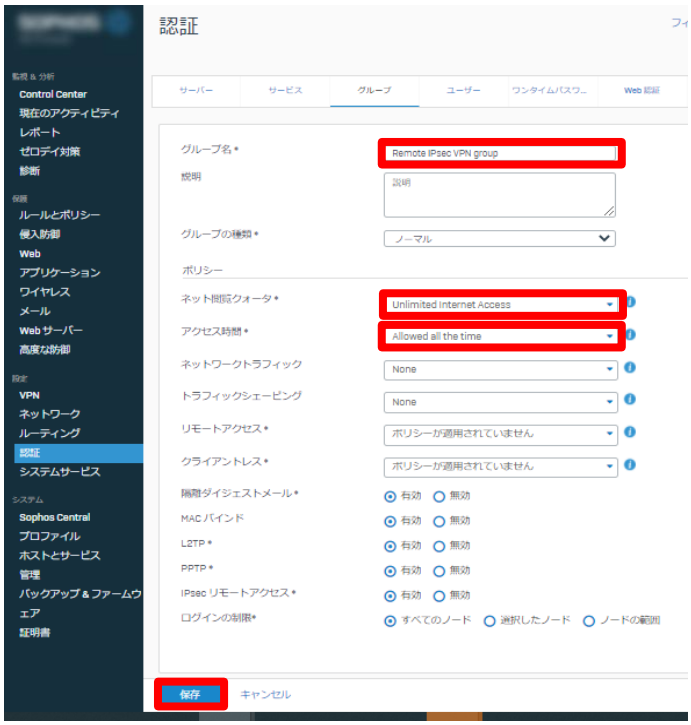
① 認証 > グループ > 追加を押下します。

② 必要な情報を入力し保存を押下します。

グループ名：Remote IPsec VPN group（任意）

ネット閲覧クォータ：Unlimited Internet Access

アクセス時間：Allowed all the time



③ グループ一覧画面に戻るため、Remote IPsec VPN group が追加されたことを確認します。

④ ユーザー ＞ 追加 を押下します。

⑤ 必要な情報を入力し保存を押下します。

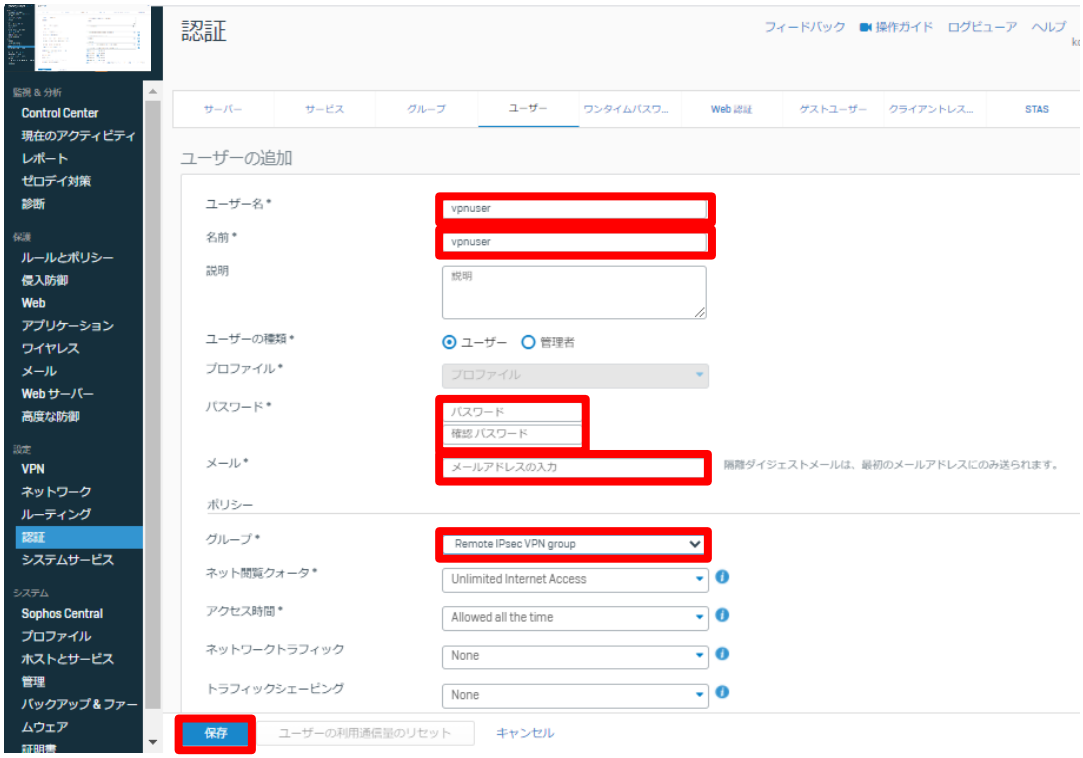
ユーザー名：vpnuser（任意）（Sophos Connect の接続で使用）

名前：vpnuser（任意）

パスワード：任意（Sophos Connect の接続で使用）

メール：任意

グループ：Remote IPsec VPN group



⑥ vpnuser が追加され、ステータスが有効であることを確認します。

3. VPN 接続向け IP ホストの作成

ユーザー側のプライベートセグメントから VPN 接続する IP ホストと、さくらのクラウド側の VPN 接続される IP ホストを作成します。

※本項の設定は管理者が行う設定手順となります。

① ホストとサービス ＞ IP ホスト ＞ 追加 を押下します。

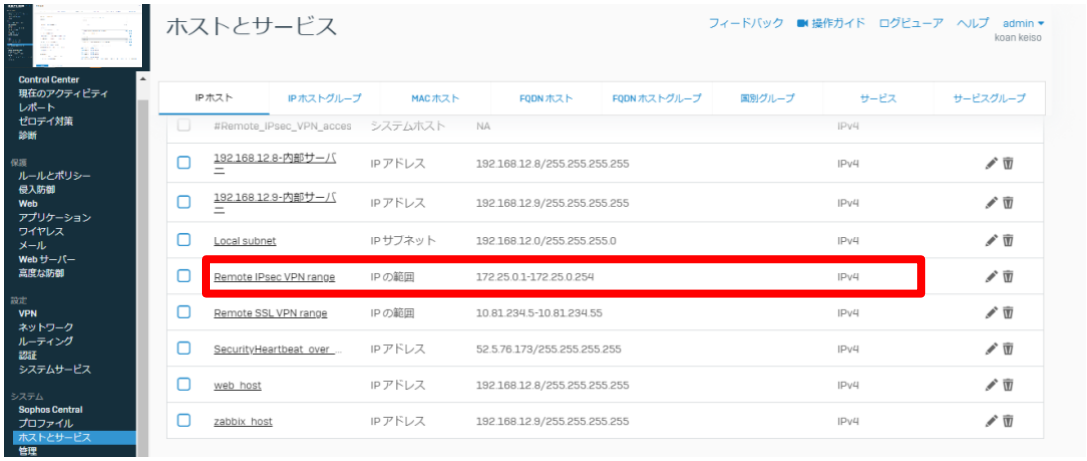
② 必要な情報を入力し保存を押下します。

名前：Remote IPsec VPN range（任意）

種類：IP の範囲

IP アドレス：172.25.0.1 – 172.25.0.254

③ Remote IPsec VPN range が追加されたことを確認します。



次にさくらのクラウドに展開された、Sophos Firewall 側の VPN 接続対象システム側の LocalSubnet を定義します。

④ IP ホスト ＞ 追加 を押下します。

⑤ 必要な情報を入力し保存を押下します。

名前：Local Subnet（任意）

種類：ネットワーク

IP アドレス：192.168.0.0

サブネット：/24(255.255.255.0)

⑥ Local subnet が追加されたことを確認します。

4. ファイアウォールの追加

ファイアウォールへ VPN による IP ホストへの接続の許可を追加します。

※本項の設定は管理者が行う設定手順となります。

① ルールとポリシー ＞ ファイアウォールルール ＞ 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 を押下します。

② 必要な情報を入力し保存を押下します。

ルール名：Remote IPsec VPN access（任意）

ルールの位置：最上位

ルールグループ：なし

送信元ゾーン：VPN

送信元ネットワークとデバイス：Remote IPsec VPN range

宛先ゾーン：LAN

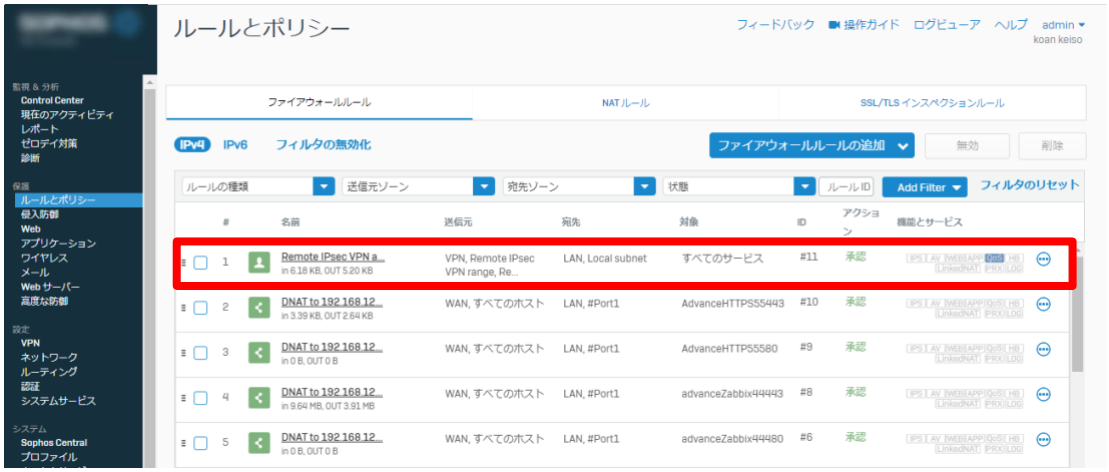
宛先ネットワーク：Local subnet

既知のユーザーを一致にチェック

ユーザーやグループ：Remote IPsec VPN group

設定が完了したら保存を押下します。

③ Remote IPsec VPN access が追加されたことを確認します。



5. IPsec（リモートアクセス）の設定

IPsec による VPN リモートアクセス接続のための設定を行います。

※本項の設定は管理者が行う設定手順となります。

① リモートアクセス VPN ＞ IPsec を押下し、必要な情報を入力後、適用を押下します。

【全般設定】

IPsec リモートアクセス：有効にチェック

インターフェース：Port1（WAN 側のインターフェースを指定）

IPSec プロファイル：DefaultRemoteAccess

承認の種類：事前共有鍵

事前共有鍵：任意

ローカル ID：IP アドレス 192.168.0.0（任意）※さくらのクラウドに展開された SophosFirewall 側

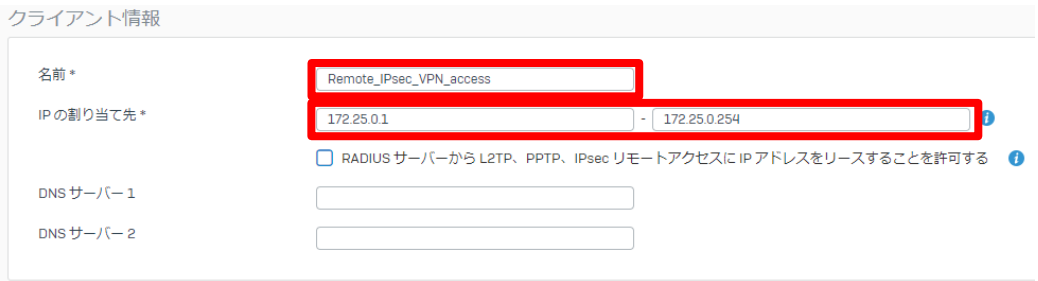
リモート ID：IP アドレス 172.25.0.0（任意）※ユーザーが接続する環境

共有するユーザーとグループ：Remote IPsec VPN group

【クライアント情報】

名前：Remote_IPsec_VPN_access（任意）

IP の割り当て先：172.25.0.1 – 172.25.0.254（ユーザー側のプライベート IP 範囲）



【詳細設定】

デフォルトのゲートウェイとして使用：OFF

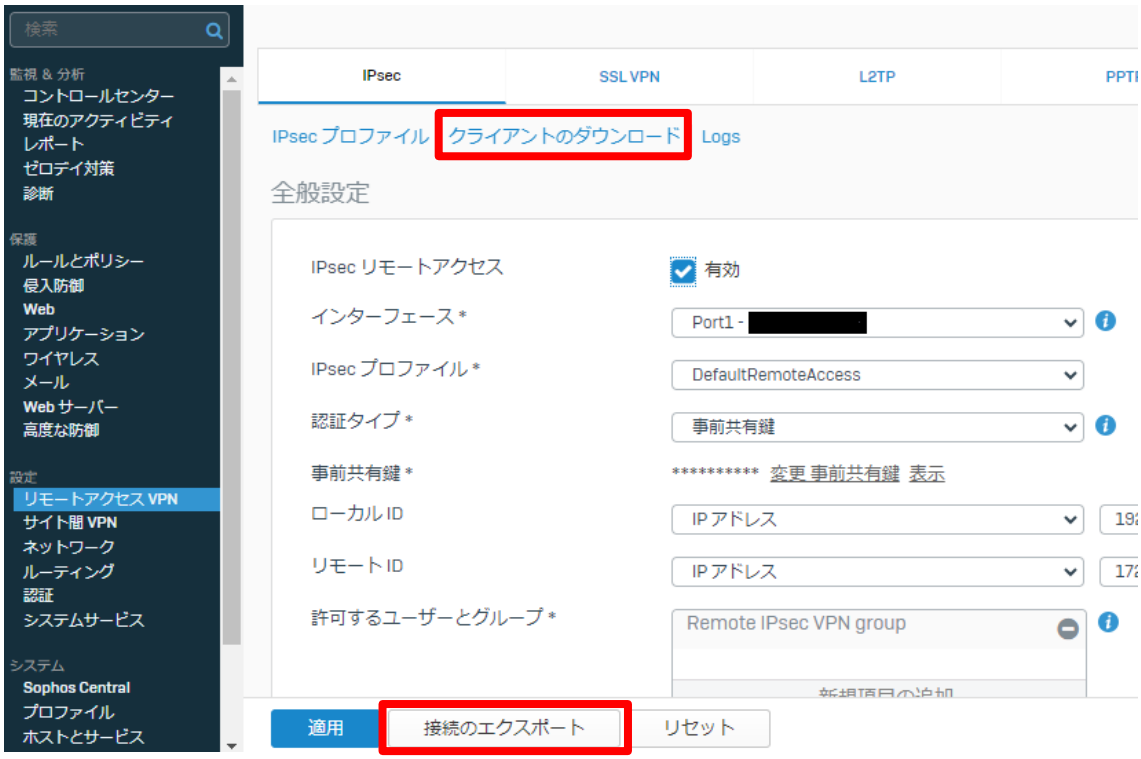
許可するネットワークリソース[IPv4]：Local subnet

「トンネル経由でセキュリティハートビートを送信する」にチェック

「ユーザー名とパスワードの保存をユーザーに許可する」にチェック

② 画面上部に リモートアクセス IPsec VPN を更新しました メッセージが出力されること
を確認します。

③ この画面よりクライアントソフトウェア及び接続の設定をダウンロードする事ができます。接続のエクスポート および クライアントのダウンロード を押下し、保存します。次項よりクライアント側の設定で必要となる為、保存した圧縮ファイルを解凍します。



※注意※

ユーザーにクライアントソフトウェア（Sophos Connect）に配布するためにユーザーポータルを利用する事も可能です。次項ではユーザーポータルからクライアントソフトウェア（Sophos Connect）をダウンロードする方法を記載します。**接続の設定ファイルはこの画面からのみダウンロードが可能です。**

6. Sophos Connect のインストール

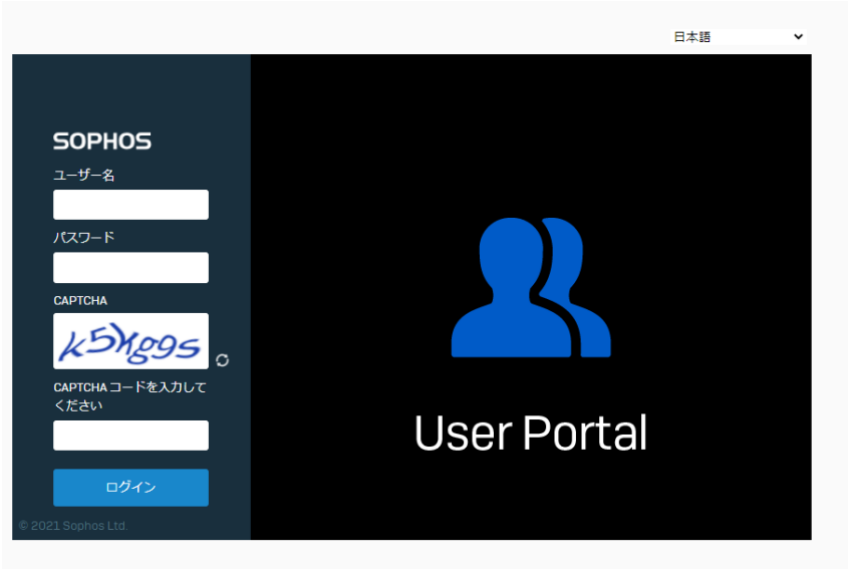
VPN 接続で使用するクライアントアプリ（Sophos Connect）をインストールします。

※本項の設定はユーザー各自が行う設定手順となります。

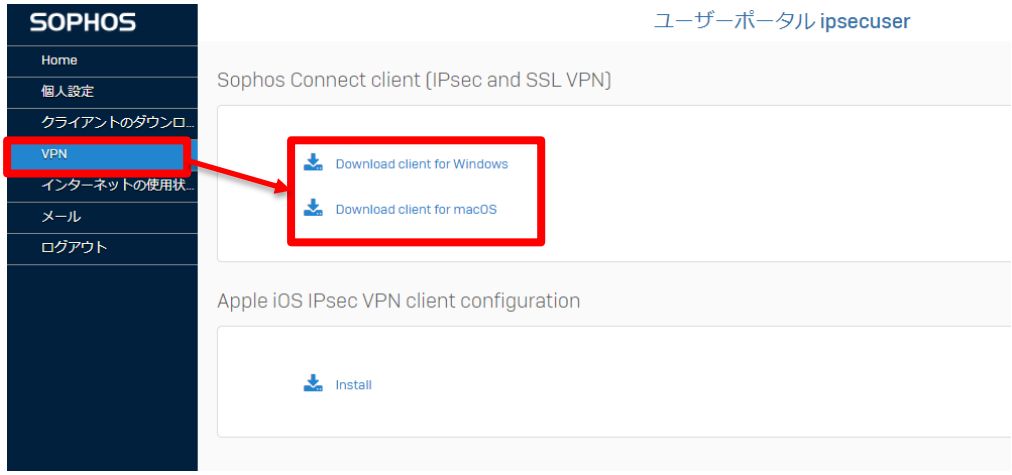
① Sophos Firewall が提供するユーザーポータルサイトにログインします。ログインアカウントは本手順で作成した「vpnuser」でログインする事ができます。

https://X.X.X.X:4443

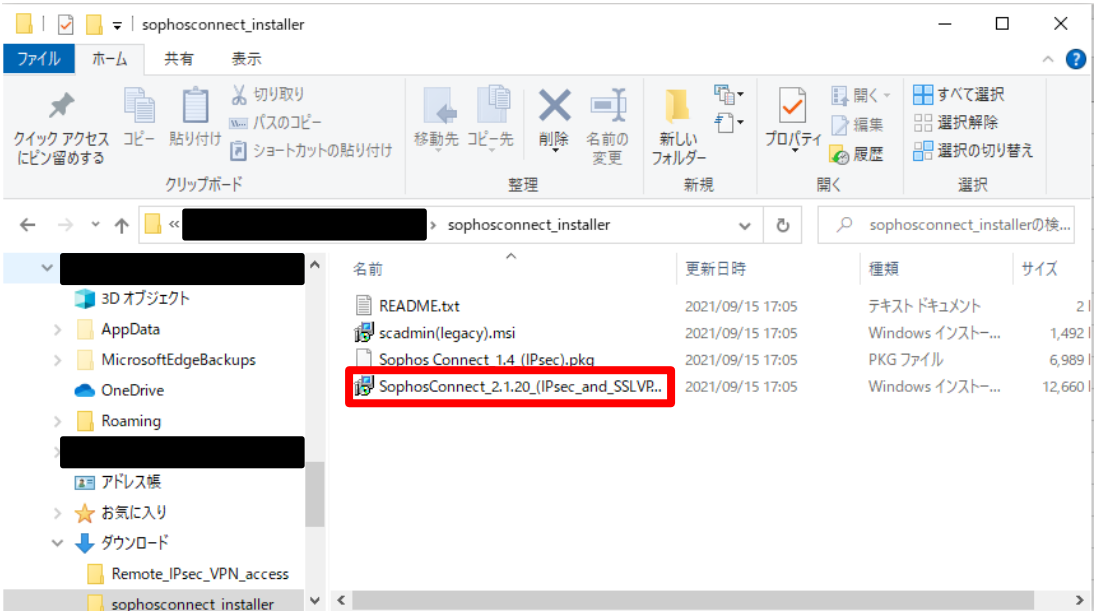
※Sophos Firewall ではデフォルトで WAN 側の IP アドレス＋ポート 4443 で設定されています。この設定は　管理 ＞ 管理者とユーザの設定で変更する事ができます。



② 「VPN」からクライアントがもつパソコンの OS に合わせて「Download client for Windows」か「Download client for macOS」を選択しインストールしてください。

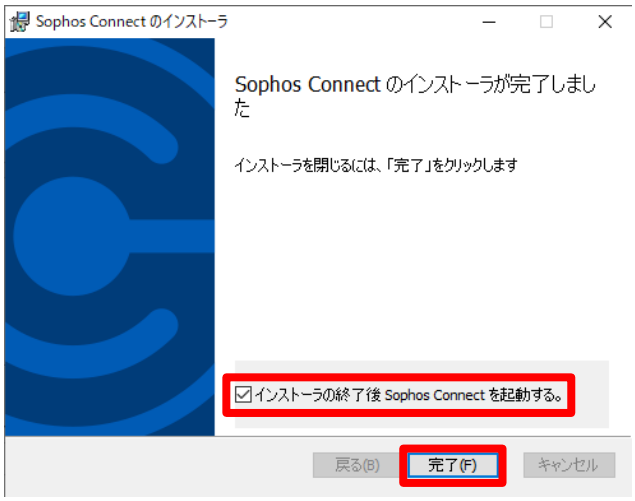


③ ダウンロードして保存した圧縮ファイルを解凍後、
SophosConnect_2.1.20_(IPsec_and_SSLVPN).msi ファイルを実行します。



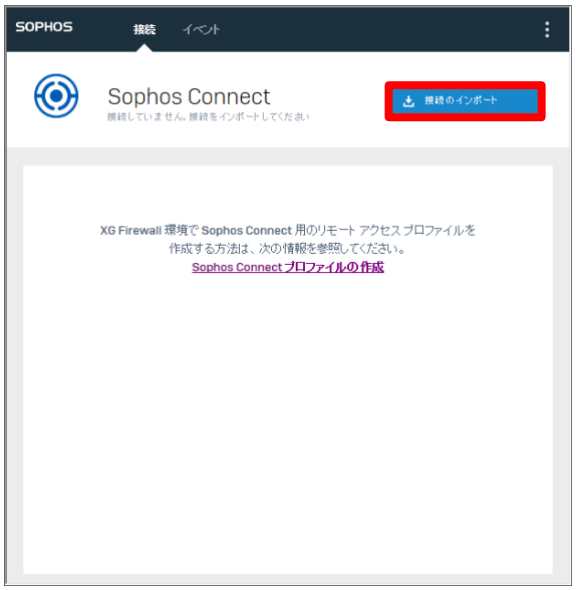
④ Sophos Connect のインストーラが起動するため、エンドユーザー使用許諾契約書および個人情報保護方針に同意し、インストールを押下します。

⑤ インストール完了後、「インストーラの終了後 Sophos Connect を起動する。」をチェックし、完了を押下します。



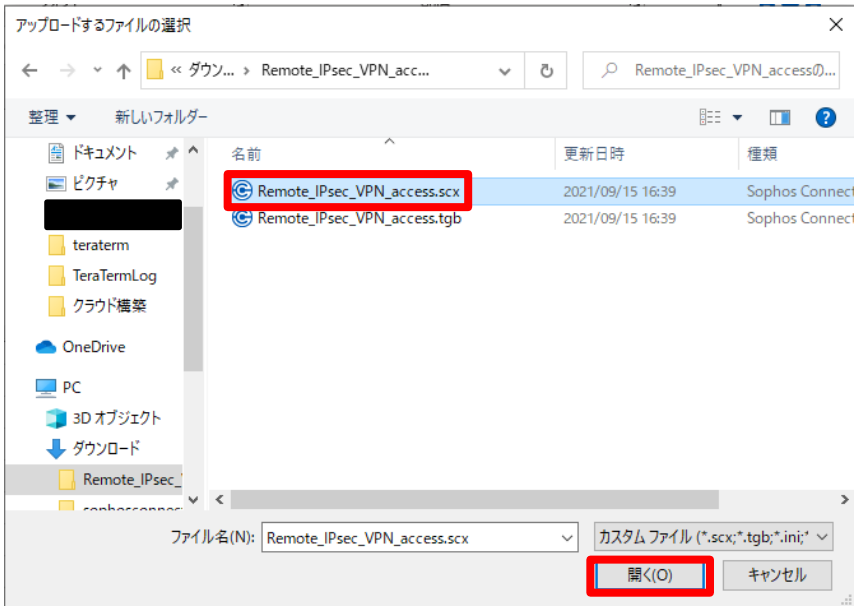
⑥ インジケーターに Sophos Connect が表示されるため、これを押下します。

⑦ Sophos Connect の接続設定画面が表示されます。
接続のインポートを押下します。

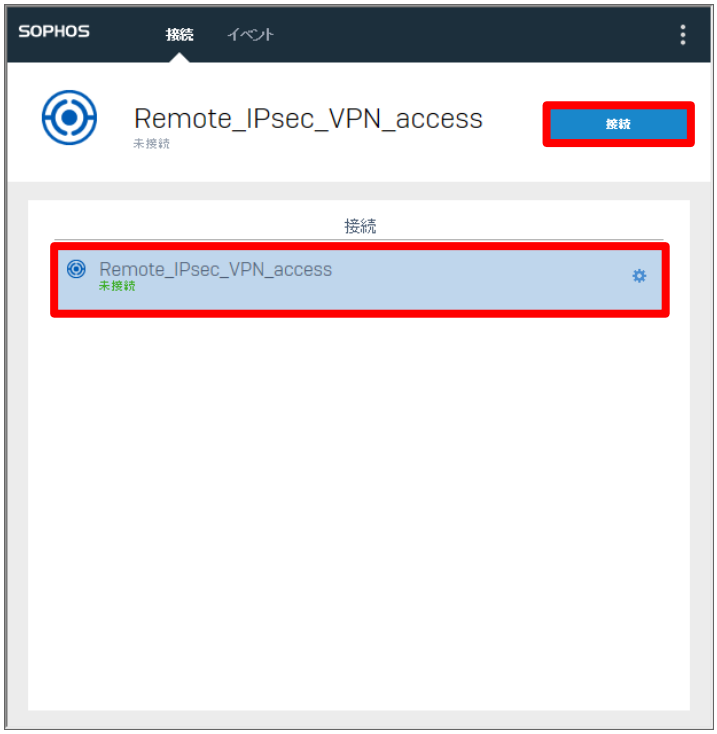


⑧ ファイルの選択ポップアップが表示されるため、解凍た設定ファイルを選択し、開くを押下します。

設定ファイル名：Remote_IPsec_VPN_access.scx

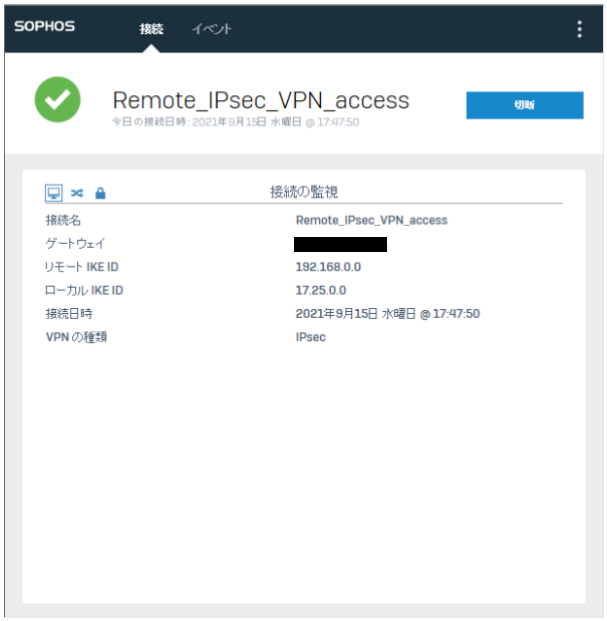


⑨ Sophos Connect へ設定が追加されたことを確認し、接続を押下します。



⑩ ユーザー認証画面が表示されるため、ユーザー名/パスワードを入力し、サインインを押下します。

⑪ 画面が遷移するため、接続が確立したことを確認します。

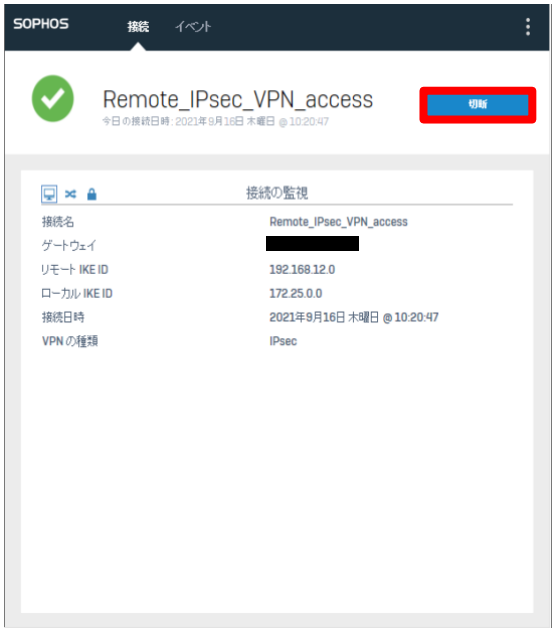


※ VPN 接続状態は Sophos 側でも確認できます。

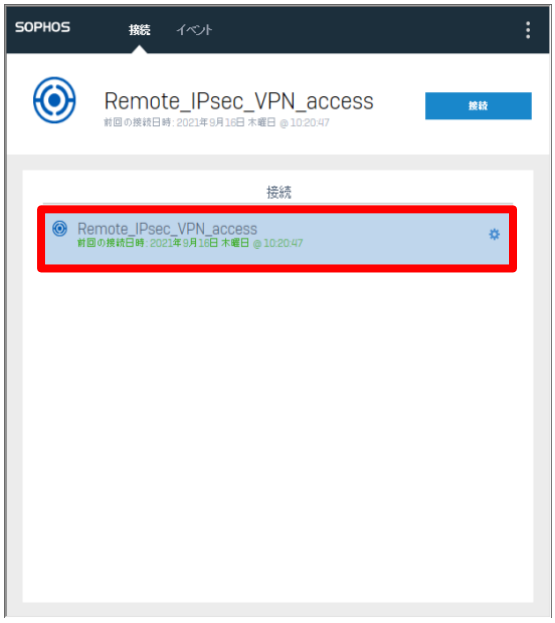
現在のアクティビティ ＞ ライブユーザー を押下することで、VPN 接続中のユーザーが表示されます。

7. Sophos Connect の終了

① Sophos Connect 接続設定画面から、切断を押下します。



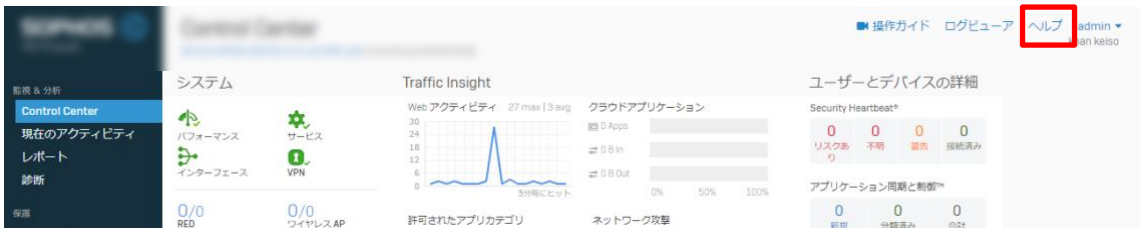
② Sophos Connect 接続設定画面が、接続の選択画面に遷移したことを確認します。



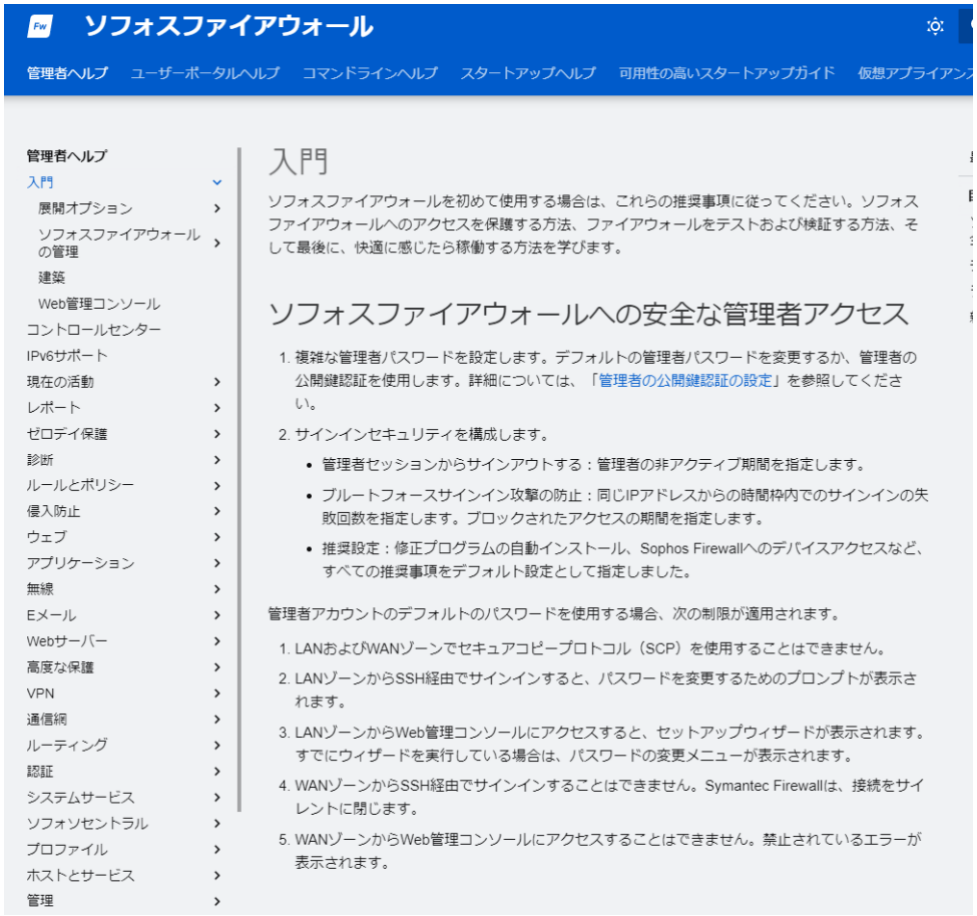
※次回接続時は 接続 を押下することで接続を確立できます。

8. 最後に

本手順書では、IPsec の設定について記載しました。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