

サービス利用手順書

SSL VPN リモートアクセス接続導入編

第 3.0 版 2023 年 8 月 31 日



さくらのクラウド「仮想型 UTM マネジメント」サービス利用手順書 Sophos Firewall SSL VPN リモートアクセス接続導入編



内容

改調	汀履歴	2
は	じめに	2
1.	ご利用環境の構成	4
2.	VPN 接続向けグループ・ユーザーの作成	6
3.	VPN 接続向け IP ホストの作成	9
4.	ファイアウォールの追加	. 12
5.	SSL VPN(リモートアクセス)ポリシーの設定	. 15
6.	Sophos Connect のインストール	. 18
7.	Sophos Connect の終了	. 23
8.	最後に	. 24

改訂履歴

版数	更新日	更新内容	更新者
1.0	2021/11/22	初版作成	興安計装株式会社
2.0	2021/2/4	v18.5 アップグレードに伴う改版	興安計装株式会社
3.0	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/enus/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 ロ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:SSL 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_firewall_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_firewall_fw_dnat.pdf

ネットワークプロテクション編

https://www.owlook.jp/public/document/sophos firewall 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 10.81.234.0/24 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。

-	即心司	E		フィードバック 🔳	暖作ガイド ログビューア ヘルプ admin ♥ koan keiso
Control Center 4 現在のアクティビティ レポート ゼロティが筆	9-	-バー サービス	グループ ユーザー ワンタイ	ムパスワ Web 認証 ゲストユーザー	クライアントレス STAS ***
診断	這加	項目の表示			<u>追加</u> 削除 並べ替え
保護 ルールとポリシー 侵入防御		グループ名 🏹	トラフィックシェービング	パーク ネット閲覧クォータ	管理
Web アプリケーション		<u>Open Gran</u>	ポリシーがあ りません	Unlimited Internet Acce	oss 🖍 🕅
ワイヤレス メール Web サーバー	0	entless Open Group(C)	ポリシーがあ りません	ポリシーがありません	1
高度な防御 設定		Guest Group	ポリシーがあ りません	Unlimited Internet Acce	265 🖍 🕅
VPN ネットワーク リーティング		Remote SSL VPN group	ポリシーがあ りません	Unlimited Internet Acce	ess 🖍 🕅

- ② 必要な情報を入力し保存を押下します。
- グループ名:Remote SSL 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

trol Center	サーバー サービス	グループ ユーザー ワンタイムパスワ Web	211
のアクティビティ			
	<i>H</i> ∥_ <i>T</i> タ ∗	Domoto SSI VDN group	
テイ対策	10-24		
	875-973	說見明	
·ルとポリシー	グループの種類*	ノーマル・	
(V) (BU			
, プリケーション	ポリシー		
ヤレス	ネット閲覧クォータ*	Unlimited Internet Access	
JL			
bサーバー	アクセス時間*	Allowed all the time 🗸 🚺	
な防御	ネットワークトラフィック	None 🗸 🕽	
	トラフィックシェーピング	None 🗸 🚺	
トワーク	リモートアクセス*	Demote SSLVDN Dolicy	
ティング		Relifice SSE VPR Policy	
E	クライアントレス*	ポリシーが適用されていません 🗸 🚺	
マテムサービス	隔離ダイジェストメール*	 ● 有効 ● 無効 	
4	MACバインド	• 有効 • 無効	
hos Central	12TD *		
ファイル	DDTD +		
	* PTP	 有効 無効 	
ー ・クアップ&ファームウ	IPsec リモートアクセス*	 有効 無効 	
,	ログインの制限*	⊙ すべてのノード ○ 違択したノード ○ ノードの	範囲
書			

監視&分析 Control Center 現在のアクティビティ	÷	-)(-	サービス	グループ	ユーザー	<u>7>91617</u>	Web 認証	ゲストユーザー	クライアントレス		STAS	
レポート	追加	項目の表示	7						追加	削除	世へ	皆え
ゼロデイ対策 診断		グルーフ	7名 🍸		トラフィックシ	ェービング	ネッ	ット閲覧クォータ			管理	
保護		<u>Open Gr</u>	roup		ポリシーがあ りません		Un	limited Internet Acce	ISS		<i>•</i>	Ŵ
ルールとポリシー 侵入防御		Clientle	ss Open Group(C)		ポリシーがあ りません		ボ	リシーがありません				Ŵ
Web アプリケーション		Guest G	froup		ポリシーがあ りません		Un	limited Internet Acce	955		-	Ŵ
ワイヤレス メール		Remote	Psec VPN group		ポリシーがあ りません		Un	limited Internet Acce	ess		-	Ŵ
Web サーバー 高度な防御		Remote	SSL VPN group		ポリシーがあ りません		Un	limited Internet Acce	9SS		-	Ŵ
高度な防御												

③ グループ一覧画面に戻るため、Remote SSL 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。

	認証						フィードバック 🖿	操作ガイド ログビ:	ューア ヘルプ	admin 🔻 koan keiso
監視 & 分析 Control Center 現在のアクティビティ	₩-/(-	サ−ビス	グループ	ユーザー	72976/27-	Web SSE	グストユーザー	クライアントレス	STAS	
レポート ゼロデイ対策 診断 ^{役回}	追加項目の表示	L.				始加	削除 ス	アクテ・ テータスの変更	ィブユーザーの ADユーザー	合計数1/1 の消去

⑤ 必要な情報を入力し保存を押下します。

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

名前:sslvpnuser(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 SSL VPN group

Control Center	サーバー	サービス	グループ	ユーザー	ワンタイムパスワ	Web 認証	ゲストユーザー	クライアントレス	STAS
現在のアクティビティ									
レポート	ユーザーの追	加							
ゼロデイ対策			_						
≥ 断	ユーザー名*		sslv	pnuser					
ŧ	名前*		sslv	pnuser					
レールとポリシー	説明		eH as						
是入防御			132 PF						
Veb						11			
アプリケーション	ユーザーの種類	題*	⊙ ⊐	ーザー 🔵 管理	者				
フィヤレス	プロファイル		-1-			-			
				177176	_				
高度な防御	バスワード *								
Ĕ									
/PN	×-//*		sslv	pnuser@notify.net			シェストメールは、最	別のメールアトレスにのの	か送られます。
ネットワーク	ポリシー								
レーティング									
SEE	クループ*		Rer	mote SSL VPN grou	p	~			
システムサービス	ネット閲覧ク:	ォータ*	Uni	imited Internet Ac	Cess	- 0			
ム テム	マクセス味用								
ophos Central	アラセス時間	•	Allo	wed all the time		• 0			
プロファイル	ネットワーク	トラフィック	Nor	ie		• 0			
ホストとサービス	h = n + - h	s							
An anna	トラフィック:	シェーヒンク	Nor	ie		- 0			
^{管理}									
^{言理} 「ックアップ&ファームウ - マ		s							

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。

100 C	認証						フィードバック 🗨 課	作ガイド ログビュ	Lーア ヘルプ K	admin 🔻 pankeiso
^{監視 & 分析} Control Center 現在のアクティビティ	サーバー	サービス	グループ	ユーザー	<u> フンタイムパスワ</u>	Web 認証	ゲストユーザー	クライアントレス	STAS	
レポート ゼロデイ対策 診断	追加項目の表示	- ID 名前 🏹	ユーザー名	☆ ▲ 種類	ā ;	追加 プロファイル	削除 ステ グループ ♡	アクティータスの変更 ステータス	r ブユーザーの合計 AD ユーザーの注 管理	数3/3 消去
_{保護} ルールとポリシー	7	IPsecuser	ipsecuser		-ザー -		Remote IPsec VPN gro	up 有効	1	Ŵ
侵入防御 Web	10	sslvpnuser	ssivpnuser	-ב	-ザー ・	-	Remote SSL VPN group	p 有効	1	Ŵ

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。

		ホス	、トとサービン	ス				フィードバック 🔳 操作	作ガイド ログビュー:	ア ヘルプ admin マ koan keiso
Control Center 現在のアクティビティ レポート ゼロデイ対策		IP	#ZF IP#Z1	グループ	MACホスト	FQDNホスト	FQDN ホストグループ	国別グループ	サ ービス	サービスグループ
診断 保護 ルールとポリシー 母 3 防御	L		名前 🖓	•	種類	アドレスの詳細 🍸			・ 「 「 「 「 「 」 「 」 「 」	自加 削除 管理
Web アプリケーション	Ι.	þ	##ALL_IPSEC_RW		システムホスト	NA			IPv4	
ワイヤレス メール Web サーバー			##ALL_IPSEC_RW6		システムホスト	NA			IPv6	
高度な防御			##ALL_RW		システムホスト	NA			IPv4	
設定 VPN ネットワーク	L		##ALL_RW6		システムホスト	NA			IPv6	
ルーティング 認証	L		##ALL_SSLVPN_RW		システムホスト	NA			IPv4	
элтир-ел элти	L		##ALL_SSLVPN_RW6		システムホスト	NA			IPv6	
Sophos Centra プロファイル ホストとサービス			#Portl		システムホスト	153.120.22.116/255.255.	255.255		IPv4	
함표			#Dort0		ミ,フテ / 赤フト	100160101/05505505	5 955		IDu/I	

② 必要な情報を入力し保存を押下します。

名前:Remote SSL VPN range (任意)

種類:IPの範囲

IP アドレス: 10.81.234.5 – 10.81.234.5

	IP ホストの)編集				フィードバック 🔳 操作	作ガイド ログビュー:	ア ヘルプ admin マ Koankeiso
 監視&分析 Control Center 現在のアクティビティレポート ポロティ対策 	IP #Z h	IP ホストグループ	MACTICA	FQDN /ሺスト	FQDN ホストグルー:	ブ 国別グループ	サービス	サービスグループ
診断	名前 *		Remote SSL VP	V range				
保護 ルールとポリシー	IP バージョン*		IPv4					
侵入防御 Web	種類 *		IP の範囲					
アプリケーション	IP アドレス *		10.81.234.5]-[10.0	81.234.55		
ンイヤレス メール Web サーバー 高度な防御	IP ホストグルー	ブ						•
設定				新規項目の追加				
VPN ネットワーク								
ルーティング 認証 システムサービス								
システム Sophos Central 및	保存また	アンセル						

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

	ホストとサ	ーヒス			71	ードバック 🔳 操作力	イド ロクビューア	ヘレフ admin • Koankeiso
現 & 分町 Control Center 現在のアクティビティ	IP ホスト	IPホストグループ	MACホスト	FQDN ホスト	FQDN ホストグループ	国別グループ	サービス	サービスグループ
レポート ゼロデイ対策 診断	#Port2		システムホスト	192.168.12.1/255.255	255.255	1	Pv4	
i ž	#Remote_IP	sec_VPN_acces	システムホスト	NA)	Pv4	
ルールとボリシー 侵入防御 Web	Local subnet	8 D	IPサブネット	192 168 12:0/255.255	255.0	10	Pv4	* W
アプリケーション ワイヤレス	Remote IPse	c VPN range	IPの範囲	172 25 0 1-172 25 0 25	4)	Pv4	<i>*</i> 1
メール Web サーバー 高度な防御	Remote SSL	VPN range	IPの範囲	10.81.234.5-10.81.234	55	10	Pv4	1
ε	SecurityHea	rtbeat_over	IPアドレス	52.5.76.173/255.255.2	55.255		Pv4	1 1
PN ネットワーク ルーディング	レーサーバ		IPアドレス	192 168 12.8/255 255	255.255	13	Pv4	·* 🗊
ざ証 システムサービス	Zabbix host		IPアドレス	192 168 12 9/255 255	255.255		Pv4	* 1

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。
------------	----	---------

	;	ホス	トとサービス			フィードバック 🔳 操作	₱ガイド ログビューア	へレプ admin ▼ koan keiso
Control Center 現在のアクティビティ レポート ゼロデイ対策 診断		IP 7	ホスト	MACTRAN	FQDNホスト FQDNホストグループ	風別グループ	サービス	サービスグループ
保護 ルールとポリシー			名前 🖓 🔹	種類	アドレスの詳細 🙄		IP X=v≥1	管理
安入的941 Web アプリケーション			##ALL_IPSEC_RW	システムホスト	NA		IPv4	
ワイヤレス メール Web サーバー			##ALL_IPSEC_RW6	システムホスト	NA		IPv6	
高度な防御			##ALL_RW	システムホスト	NA		IPv4	
設定 VPN ネットワーク			##ALL_RW6	システムホスト	NA		IPv6	
ルーティング 認証 ミュニティサービュ			##ALL_SSLVPN_RW	システムホスト	NA		IPv4	
システム システム			##ALL_SSLVPN_RW6	システムホスト	NA		IPv6	
Sophos Central プロファイル ホストとサービス			#Portl	システムホスト	153.120.22.116/255.255.255.255		IPv4	
台理			HDort2	≈.7∓/.±7 k	100 180 10 1 /055 055 055 055		IDu/I	

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)

	IPホストの追加		フィードバック	▶ 操作ガイド ログビューア へいし
Control Center 現在のアクティビティ レポート ゼロディ対策 診断	IPホスト IPホストグループ	мас ホスト FQDN ホスト FQDI	NN ホストグループ 国別グループ	9 -ビス 9 -ビン
G== ルールとポリシー 役入防御 Web アプリケーション ワイヤレス メール Web サーバー 高度な防御	名前* IP バージョン* 理頭* IP アドレス*	Local subnet IPv4 O IPv6 IP O ネットワーク IPの範囲 O I 19216800	IP リスト サ /24 (255 255 255 0) ブ	×
^{設定} VPN ネットワーク ルーティング 認証 システムサービス システム Sophos Central	ルホストグループ	新規項目の追加	4	
プロファイル ホストとサービス 管理 パックアップ&ファームウ ェア 証明書	発芽 キャンセル			

⑥ Local subnet が追加されたことを確認します。

	ホス	ストとサービス				5	フィードバック 🔳 握	推力イド ログビュー	-ア ヘルプ admin ▼ koan keiso
Control Center 現在のアクティビティ レポート	IF	P#スト IP#ストグ	リレープ MAC	ホスト	FQDN ホスト	FQDN ホストグループ	国別グループ	サービス	サービスグループ
ゼロデイ対策 診断		#Remote_IPsec_VPN_ac	ces システムホス	KH NA				IPv4	
保護 ルールとポリシー		<u>192168128-内部サー/</u> 二	IP アドレス	192	2 168 12 8/255 255 2	55.255		IPv4	≁ Ū
侵入防御 Web アプリケーション		<u>192.168.12.9-内部サー/</u> 二	IP アドレス	192	2 168 12 9/255 255 2	55.255		IPv4	. ▲* 面
ワイヤレス メール		Local subnet	IP サブネット	 192 	2.168.0.0/255.255.25	5.0		IPv4	× 🗊
高度な防御		Remote IPsec VPN range	IP の範囲	172	25.0.1-172.25.0.254			IPv4	× 1
設定 VPN ネットワーク		Remote SSL VPN range	IP の範囲	10.0	81.234.5-10.81.234.5	5		IPv4	× 1
ルーティング 認証		SecurityHeartbeat over	IP アドレス	52.5	5.76.173/255.255.25	5.255		IPv4	1
УХТЦЈ-ЕХ УХ<u>Т</u><u></u>		web_host	IPアドレス	192	2 168 12 8/255 255 2	55.255		IPv4	1
Sophos Central プロファイル ポストとサービス		zabbix host	IPアドレス	192	2 168 12 9/255 255 2	55.255		IPv4	1 1

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。

 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。

	ルールと	ポリシー			フィー	ドバック 🔳 操作ガイド	ログビューア ヘルプ admin マ koan keiso
監視 & 分析 Control Center 現在のアクティビティ		ファイアウォールルール		NATルール		SSL/TLS	インスペクションルール
レポート ゼロデイ対策 診断	IPv4 IPv6	フィルタの無効化			ファイアウ	フォールルールの追加 🔨	無効 削除
	ルールの種類	▼ 送信元ゾーン	 宛先ゾー 	> 🔽	状態 新しいファ	・イアウォールルール	i Filter 👻 フィルタのリセット
SEANDSH Web		名前	送信元	宛先	_{対象} サーバーフ (DNAT)	<i>"</i> クセスアシスタント	とサービス
アプリケーション ワイヤレス メール	= 🗌 1 <	Remote IPsec VPN a in 13.59 MB, OUT 1.94 MB	VPN, Remote IPsec VPN range	LAN, Local subnet	すべしのリーヒス	# AL /2140	LINKEDAPP QCS HB
Web サーバー 高度な防御	E 🗌 2 📢	DNAT to 192.168.12	WAN, すべてのホスト	LAN, #Port1	AdvanceHTTPS554	43 #10 承認	

- ② 必要な情報を入力し保存を押下します。
- ルール名: Remote SSL VPN access (任意)
- ルールの位置:最上位
- ルールグループ:なし

ファイアウォールトラフィックログ:チェック(任意)

	ファイアウォールルールの追加	П	フィードバック ■ 操作ガイド ログピューア	ヘルプ admin ▼ koan keiso
 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	(1) ハールのステータス ルール名・ Remate SSL VPN access アクラヨン 承認 マ マ アクラヨン アクラヨン マ	34明 入力 説明 ノ	ルールの位置 <u> 最上位</u> 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 SSL VPN range

宛先ゾーン:LAN

宛先ネットワーク: Local subnet

	ファイアウォールルール	レの追	加	74-	-ドバック 🔳 操作ガー	רא סלצב-ד	へレプ admin • koan keiso
 監視&分析 Control Center 現在のアクティビティ レポート 	送信元 送信元のゾーン、ネットワーク、デバイス スケジュールした期間の間、これらの送信	くを選択して 『元からのト	ください。 ラフィックにルールが適用されます。				
ゼロデイ対策	送信元ゾーン*		送信元ネットワークとデバイス*		スケジュールされた時間	朝内	
1 Sept.	VPN	0	Remote SSL VPN range	10	常時		-
保護					選択すると、特定	の期間および曜日にルー	しが適用さ
侵入防御	新規項目の追加		新規項目の追加				X L32 9 a
アプリケーション ワイヤレス メール Web サーバー 高度な防御	宛先とサービス ^{疫先のソーン、ネットワーク、デバイス、}	サービスを	選択してください。				
設定 VPN	これらの宛先へのトラフィックにルールカ	「適用されま	वे .				
ネットワーク	宛先ゾーン*		宛先ネットワーク*		サービス・		
ルーティンク 認証 システムサービス	LAN	0	Local subnet	10	任意		0
システム	新規項目の追加		新規項目の追加		新	規項目の追加	
Sophos Central プロファイル ホストとサービス					サービスとはトラ とポートの	フィックの種類であり、 組み合わせに基づいて決	プロトコル まります。

既知のユーザーを一致にチェック

ユーザーやグ	ブループ:Remote SSL VPN	l group					
	ファイアウォールルールの追加	Д	フィードバック	■ 操作ガイド	ログビューア	へレプ k	admin 🔻
 製用 あ 分析 Control Centre 服在のアクライビティレパート ビロライ対策 参照 ク選 ルールとポリシー 良人気樹 Web アブリケーション 	 ▼ 長知のユーザーを一致 □ 不明なユーザーに Web 認証を使用する 	Remote SSL VPN group 新規項目の追加 データ利用通信量の計算からこのユー ィビディを除外	・ ザーアクテ				
ワイヤレス メール Web サーバー 高度な防御	> 除外の追加 0						
^{設定} VPN ネットワーク ルーティング 設証 システムサービス	リンク NAT ルールの作成 🟮						
_{システム} Sophos Contral プロファイル ホストとサービス 管理	セキュリティ機能 > Web フィルタリング						
バックアップ&ファームウ ェア 証明書	保存 キャンセル						
광문까도기!	たら促在を地下します						

設定か完了したら保存を押下します。

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

anime ()	ルールとフ	ポリシー			フィート	ドバック 🛛	▶ 操作ガイド	ログビューア	イ へレプ admin ▼ Koankeiso
^{脳視 & 分析} Control Center 現在のアクティビティ	:	ファイアウォールルール	マーの先ゾーン		状態		SSL/TLS	インスペクション Add Filter マ	ルール フィルタのリセット
レホート ゼロデイ対策 診断		名前 Remote SSL VPN acc	送信元 VPN Permite SSI VPN	宛先	対象	ID #13	アク ショ 承認	機能とサービス	
保護		in 0 B, OUT 0 B	range, Remo	LAN, LOUI SUBICE	9. (CO)9 - C/(LinkedNA	PRX LOG

5. SSL VPN(リモートアクセス)ポリシーの設定

SSL 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証明書の設定を行います。※本手順では Sophos Firewall にデフォルトで含まれる自己証 明書で設定する事を前提としています。

証明書 >証明書機関[CA] > Default をクリックします。

	証明書					フィードバック	■ 操作ガイド	ログビューア	ヘルプ	admin • Koankeisc
^{審視 & 分析} Control Center 現在のアクティビティ レポート ゼロデイ対策		紅明書	-		証明機關 (CA)		Certificate Rev	ocation List (証明書	失効リスト	·)
診断 8:#	C 1.0	0	11.34			00.00 - C	× 7 H		4	用 版
^{~~} ルールとポリシー 侵入防御 Web	Defaul	L				2021-10-21	2036-12-31	内部	٩	۵/
アノリケーション ワイヤレス メール	Securi	tyAppliance_SSL_CA	/C=GB/S1 SSL CA/e	=Oxfordshire/O=Sophos/OU mailAddress=support@soph	J=NSG/CN=Sophos los.com	2015-08-01	2036-12-31	ビルトイン	٩	\$ \$
Web サーバー 高度な防御	AAACe	rtificateServices	/C=GB/S Limited/C	T=Greater Manchester/L=Sa N=AAA Certificate Services	iford/O=Comodo CA	2004-01-01	2028-12-31	ビルトイン		
設定 MINN	—	007	/C=ES/set	rialNumber=Q2863006I/O=C	ONSEJO GENERAL	0010 05 07	0040 OF 07	ドルトイ		2.00

各項目が空白の部分について任意の値を設定し保存します。



②リモートアクセス VPN > SSL VPN 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】

名前:Remote SSL VPN Policy

【ID】

ポリシーメンバー: Remote SSL VPN group

	IPsec	SSL VPN	LZTP	РРТР	クライアントレス SSL VPN ポリ	IPsec (レガシー)
コン・13 ルビンン 現在のアクティビティ レポート	全般設定					
ビロテイ対策 診断	名前*	Remote	SSL VPN Policy			
『 ルールとポリシー 昼入防御 Web	説明	Remote	SSL VPN Policy	10		
アプリケーション フイヤレス メール	7					
Veb サーバー 気度な防御	ポリシーメンバー	Remot	e SSL VPN group user	0 0		
Jモートアクセス VPN サイト間 VPN			新規項目の追加			

③ 画面上部「SSL VPN グローバル設定を表示」をクリックします。

IPeac SSL VPN L2TP PPTP クライアントレス SSL VPN ポリ. IPeac (レガシ・ パリカン・ SSL VPN グロー/い説を アントのダウンロード Logs アシスタント 送知 1 名前 豆 ・ デフォルトのグートウェイとして使用 豆 説明 管 Remote SSL VPN Policy レルス Remote SSL VPN Policy レルス	IPac SSLVPN L2TP PPTP クライアントレス SSL VPN ポリー IPac によろ SSL VPN グローバ以設定 クラ・アントのダウンロード Logs アシスタント 送加 名前 マ ・ デフォルトのゲートウェイとして使用 マ 説明 留 Bemote SSL VPN Policy いいえ Remote SSL VPN Policy ・							
SSL VPN グローバル設定 クラ アントのダウンロード Logs アシスタント idul ③ 名前 豆 ・ デフォルトのグートウェイとして使用 豆 説明 ◎ Remote SSL VPN Policy レいえ Remote SSL VPN Policy	SSL VPN グロー/じは設定 クラ アントのダウンロード Logs アシスタント 述加 名前 マ ・ デフォルトのゲートウェイとして使用 マ 説明 説明 Bernote SSL VPN Policy いいえ		IPsec	SSL VPN	L2TP	PPTP	クライアントレス SSL VPN ポリ	IPsec (レガシー)
2 名前 豆 デフォルトのゲートウェイとして使用 豆 説明 管 Bremote SSL VPN Policy いいえ Remote SSL VPN Policy の	名前 マ デフォルトのゲートウェイとして使用 マ 説明 第 Bernote SSL VPN Policy いいえ Remote SSL VPN Policy 4	SSL V	'PN グローバル設定 クラ	(アントのダウンロード Log	S			
名前 丁 ・ デフォルトのゲートウェイとして使用 丁 説明 管 Remote SSL VPN Policy いいえ Remote SSL VPN Policy /	名前 マ デフォルトのゲートウェイとして使用 マ 説明 目 Remote SSL VPN Policy いいえ Remote SSL VPN Policy 4						アシスタント	追加 前
C Remote SSL VPN Policy いいえ Remote SSL VPN Policy	Remote SSL VPN Policy いいえ Remote SSL VPN Policy		名前 🖓	▲ デフォル	トのゲートウェイとして使用	∇	說明	管理
			Remote SSL VPN Polic	<u>y.</u> いいえ			Remote SSL VPN Policy	

SSL サーバー証明書: ApplianceCertificate

ホスト名の上書き: WAN 側のグローバル IP アドレス(任意)

IPv4 リース範囲: Remote SSL VPN range で設定した範囲(任意)

適用をクリックします。

<u></u>	リモートアクヤス VPN	フィードバック	ク ■ 操作ガイド ログビューア ヘルプ
	SSL VPN グローバル設定		
検索			
临視 & 分析	SSL VPN の設定		
コントロールセンター			
現在のアクティビティ	プロトコル *	● TCP ● UDP パフォーマンスを向上するには	t UDP を選択してください]
レポート	SSL サーバー証明書 *	ApplianceCertificate	
セロテイ対策	ホスト名の上書き		
診断	#_ b *		
呆護	W-L.	8443	[1~65535]
ルールとポリシー	IPv4 アドレスの割り当て *	10.81.234.5 /24 (255.255.255.0)	✓ ()
侵入防御	IPv6 アドレスの割り当て *	2001:db8::1:0	/ 64
Web	リースモード*		·
アノリクーション			
		•	
ン ル Webサーバー			
高度な防御	IPv4 DNS	プライマリ	セカンダリ
	IPv4 WINS	プライマリ	セカンダリ
	ドメイン名		
ネットワーク	デットビアの接続を解除するまでの時 間:*	180	秒 [60-1800]
ルーティング	アイドルピアの接続を解除するまでの時 間:*	15	分 [15-360]
認証			
システムサービス	陸島仏の部合		
5771	咱亏1600設正		
Sophos Central	暗号ルフルゴルブム		
プロファイル		AES-128-CBC	
ホストとサービス	認証アルゴリズム	SHA2 256	
管理	鍵サイズ	2048 bit	
バックアップ&ファームウ			
ェア	3種の2円 X71月1間	28800	秒
証明書			

※注意※

ユーザーにクライアントソフトウェア(Sophos Connect)及び接続の設定方法を配布するためにユーザーポータルを利用します。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。

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「sslvpnuser」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。

SUPHUS	1-9-M-9/Dipsecuser
Home	Carbon Connect alignt (IDage and COL VIDN)
個人設定	Sophos Connect client (IPsec and SSL VPN)
クライアントのダウンロ	
VPN	📩 Download client for Windows
インターネットの使用状	
メール	Download client for macOS
ログアウト	
	Apple iOS IPsec VPN client configuration
	🛃 Install

③ 同様の画面から設定ファイルもダウンロードします。

SOPHOS	ユーザー	ーポータル sslvpnuser
Home 個人設定	Sophos Connect client (IPsec and SSL VPN)	
クライアントのダウンロ		
インターネットの使用状 メール ログアウト	 Download client for Windows Download client for macOS 	
	Apple iOS IPsec VPN client configuration	
	🛃 Install	
	SSL VPN クライアント	
	 Windows 向けクライアントと設定のダウンロード Windows 向け設定のダウンロード その他の OS 向け設定のダウンロード Android/iOS 向け設定のダウンロード 	

 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。

歸 Sophos Connect のインストー	5 – 🗆	×
	Sophos Connect のインストーラが完了しました	,
	インストーラを閉じるには、「完了」をクリックします	
	「インストーラの終了後 Sophos Connect を起動する。	
	戻る(B) 完了(F) キャンセ	ll -

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、開くを押下します。

設定ファイル名:sslvpnuser__ssl_vpn_config.exe

🐼 sslvpnuser_ssl_vpn_config.exe	アプリケーション	120 K

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。

SOPHOS	接続	イベント				:
٢	未接續			■ (按标	i
			接続			
•						\$

① 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。

SOPHOS	#続 イベント	:
۲	Remote_IPsec_VPN_access ユーザー認証情報を入力してください	
	ユーザーの認証	
	接続するにはユーザー名とバスワードを入力して、「サインイン」をクリッ 久ます。	
	sslvpnuser	
	•••••••	
	□ ユーザー名とバスワードを保存する	
	サインイン	

① 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。

	現在のアクティビ	ティ		フィードバック 🔳 操作ガイド	E ログピューア ヘルプ admin ▼ koan keiso
 監視る分析 Control Conter 現在のアクティビティ ゼロディ対策 	ライブユーザー 同時ユーザー1	ライブ接続	ライブ接続 IPv6	IPsec 接続	リモートユーザー
^診 断 ^{保護} ルールとポリシー 侵入防御 Web	□ ユーザー ロ ユーザー	3 マ クライアントの# マ マ	—기대 및 데 <i>시도</i> 차 ^{嚴重}	ジョン MAC 開ジ	切断 出時刻 アップロード
アプリケーション ワイヤレス メール Web サーバー 高度な防御		IPsec VPN	172.25.0.1 IPv4	20	21-09-16 09:17 0.00 KB

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。

SOPHOS	搬行	1121	:
		016	
② × ▲ 接続名 ゲートウェイ リモート IKE ID ローカル IKE ID 接続日時 VPN の種類		₩0%	

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、SSL VPN(リモートアクセス)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ヘリンクされており、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。

	Control O	-			■ 操作力	イド ログビュー	ア へレプ admin マ Juan ketso
點視 & 分析	システム		Traffic Insight		ユーザーとデバ	イスの詳細	
Control Center	4 b	-	Web アクティビティ 27 max [3 avg	クラウドアプリケーション	Security Heartbeat®		
現在のアクティビティ レポート	107-752		30 24 18 12	ied G Apps ≓ 0 B In	000 リスクあ 不明 り	0 0 書店 服統系計	
診断	インターフェース	VPN	6	2 0 8 Out	アプリケーション同期	と制御™	
保護	0/0 RED	0/0 21722 AP	許可されたアプリカテゴリ	ネットワーク攻撃		0	

🖭 ソフォスフ	(アウォール		tột
管理者ヘルプ ユーザーボー	ヘルプ コマンドラインヘルプ スタートアップヘルプ 可ノ	用性の高いスタートアップガイド	仮想アプライアンス
darm the stand	7.00		
官埋有ヘルプ	人門		1
入口 屋間オプション	ソフォスファイアウォールを初めて使用する場合は、これ	いらの推奨事項に従ってください。	ソフォス 『
夜開オフション ソフォスファイアウォール。	ファイアウォールへのアクセスを保護する方法、ファイフ	アウォールをテストおよび検証する	る方法、そ
の管理	して最後に、快適に感じたら稼働する方法を学びます。		
建築			
Web管理コンソール	ソフォスファイアウォールへの	安全か管理者アク	177
コントロールセンター			
IPv6サポート	1. 複雑な管理者パスワードを設定します。デフォルトの)管理者パスワードを変更するか、	管理者の
現在の活動	公開鍵認証を使用します。詳細については、「管理者	「の公開鍵認証の設定」を参照して	こくださ
レポート	61.		
ゼロデイ保護	2. サインインセキュリティを構成します。		
診断	 管理者セッションからサインアウトする:管理者 	師非アクティブ期間を指定します	5.
ルールとポリシー	• ブルートフォースサインイン攻撃の防止:同じIF	アドレスからの時間枠内でのサイ	インインの失
侵入防止	敗回数を指定します。ブロックされたアクセスの)期間を指定します。	
ウェブ	• 推奨設定:修正プログラムの自動インストール、	Sophos Firewallへのデバイスアク	ウセスなど、
アプリケーション	すべての推奨事項をデフォルト設定として指定し	ました。	
無線			
Eメール	管理者アカワントのデフォルトのバスワードを使用するな	場合、次の制限が適用されます。	
Webサーバー	1. LANおよびWANゾーンでセキュアコピープロトコル	(SCP) を使用することはできま	せん。
局度な保護	2. LANゾーンからSSH経由でサインインすると、パスワ	リードを変更するためのプロンプト	トが表示さ
VPN	れます。		
通信網	3. LANゾーンからWeb管理コンソールにアクセスすると	、セットアップウィザードが表示	<u>示されます。</u>
ルーティング exper	すでにウィザードを実行している場合は、パスワート	『の変更メニューが表示されます。	
	4. WANゾーンからSSH経由でサインインすることはで	きません。Symantec Firewallは、	接続をサイ
システムリーヒス	レントに閉じます。		
プロファイル	5. WANゾーンからWeb管理コンソールにアクセスする	ことはできません。禁止されてい	るエラーが
ホストとサービス	表示されます。		
管理			
ウェブ アプリケーション 無線 Eメール Webサーバー 高度な保護 VPN 通信網 ルーティング 認証 システムサービス ソフォソセントラル プロファイル ホストとサービス 管理	 ・ 推奨設定:修正プログラムの自動インストール、 すべての推奨事項をデフォルト設定として指定し [*]管理者アカウントのデフォルトのパスワードを使用する場 LANおよびWANゾーンでセキュアコピープロトコル LANゾーンからSSH経由でサインインすると、パスワ れます。 LANゾーンからWeb管理コンソールにアクセスすると すでにウィザードを実行している場合は、パスワート WANゾーンからSSH経由でサインインすることはで レントに閉じます。 WANゾーンからSSH経由でサインインすることはで WANゾーンからSSH経由でサインインすることはで よントに閉じます。 WANゾーンからWeb管理コンソールにアクセスする 表示されます。 	Sophos Firewallへのデパイスアク ました。	マセスなど、 せん。 、が表示さ 京されます。 接続をサイ るエラーが

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