

拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

サイト・セキュリティ・プロファイル

SID ※

VSR名称 ※

シリアル ※

※バリオセキュア記入欄

本用紙はお客様のサイトのネットワーク構成ならびにセキュリティ・ポリシーを策定して頂くためにご利用頂くものです。
本情報に基づきVSRが設定されます。

【注意】「※」印の項目は必須項目です。必ずご記入下さい。

ご契約者様会社名※			設置希望日時 ※ 年 月 日 時
契約情報※	☐ 新規 ☐ 変更 ☐ WAN側IPアドレス変更 ☐ その他 ()		機器到着希望日時 年 月 日 時 ※設置希望日時はプロフィール確定後 15営業日以降にてご記入下さい。
機器設置場所※	会社名※		
	郵便番号		
	住所※		
機器送付先※	下記に機器送付先をご記入下さい		
	郵便番号		
	住所※		
	会社名※		
	部署名		
	担当者様氏名※		
	電話番号※		
納品書送付先※	☐ 同上 ☐ その他(下記に送付先をご記入下さい)		
	郵便番号		
	住所※		
	会社名※		
	部署名		
	担当者様氏名※		
	電話番号※		
	Mail Address		

機器情報			
ご使用機器	VSR700	作業費用	☐ オンサイト設置: ¥40,000/1回 ☐ 時間外作業 (オンサイト対応): ¥104,000/1回 ☐ 時間外作業 (リモート対応): ¥64,000/1回

設置希望日時について

サイト・セキュリティ・プロファイルが確定後 **15営業以降の日時**をご指定ください。

例) 設置希望日時を4月16日としたい場合、4月1日までにサイト・セキュリティ・プロファイルを作成する必要があります。

4月 日 月 火 水 木 金 土 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	開通希望日時 4月16日	4月 日 月 火 水 木 金 土 ① 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	SSP作成完了日 4月1日
			SSP完了日から 15営業日

機器到着希望日時について

サイト・セキュリティ・プロファイルが確定後 **14営業以降の日時**をご指定ください。

例) 設置希望日時を4月16日としたい場合、4月1日までにサイト・セキュリティ・プロファイルを作成する必要があります。

4月 日 月 火 水 木 金 土 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	開通希望日時 4月15日	4月 日 月 火 水 木 金 土 ① 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	SSP作成完了日 4月1日
			SSP完了日から 14営業日

拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

セキュリティオフィサー

SID ※

VSR名称 ※

シリアル ※

※バリオセキュア記入欄

ご契約者様会社名

設置希望日

年 月 日

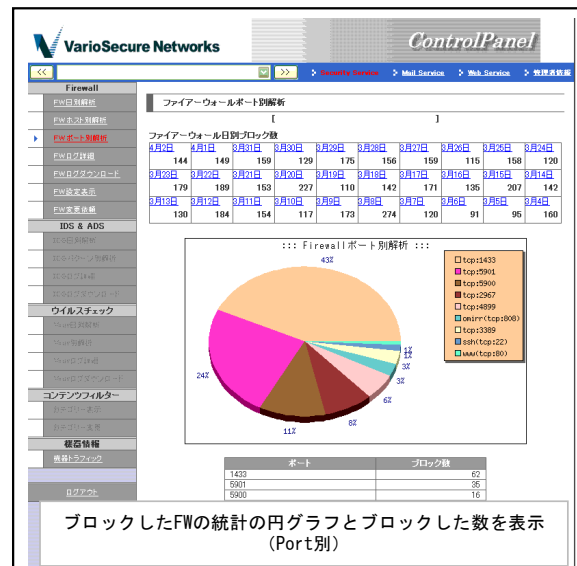
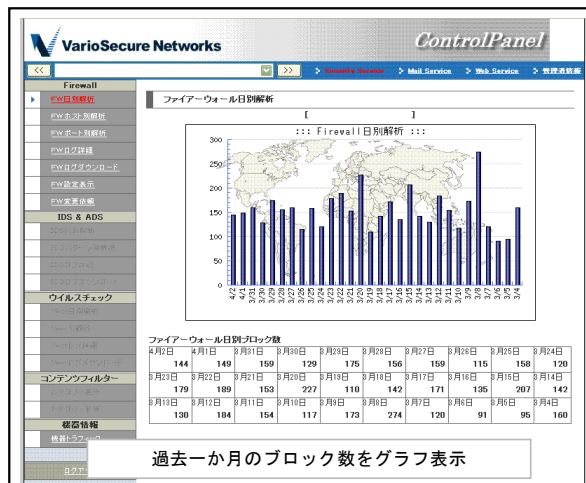
VSR管理担当者様（セキュリティオフィサー）のご記入をお願い致します。セキュリティオフィサー様はVSRのログ・トラフィック情報などを確認いただけるコントロールパネルの閲覧が可能となります。（別途ID/パスワードを画面にてお送り致します）また、VSRに関するお問い合わせを頂く方は、お客様サイトの安全のためご記入頂いた担当者様からのみ受け付けて頂きます。ご担当者様は2名様以上をご記入頂きますようお願い致します。

管理者情報「※」は必須項目となります。必ずご記入下さい

第1管理者	会社名※		部署名	
	氏名※		個人用Mail※	
	住所※	〒		
	TEL※		FAX	
第2管理者	会社名※		部署名	
	氏名※		個人用Mail※	
	住所※	〒		
	TEL※		FAX	
第3管理者	会社名※		部署名	
	氏名※		個人用Mail※	
	住所※	〒		
	TEL※		FAX	

管理者情報について

- コントロールパネルについて
ファイアウォールやIDSで検知したログを自動解析してコントロールパネルより提供します。
グラフ表示により、毎日のトラフィック量、不正アクセス数、ブロック数などをチェックできます。



拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

接続情報

SID ※			
VSR名称 ※			
シリアル ※			
		※バリオセキュア記入欄	
		設置希望日	
		年 月 日	
ご契約者様会社名			

機器情報					
接続回線情報	回線品目			回線速度	Mbps
	接続形態	☐ イーサネット接続 ☐ PPPoE接続（下記に認証IDとパスワードを記入ください）			
		PPPoE認証ID	パスワード		
インターフェース情報	お客様割り当てIPアドレス				
	WAN インターフェース(eth0)				
	インターフェースアドレス/プレフィックス				
	通信モード	Speed	☐ Auto ☐ 100 ☐ 10	Duplex	☐ Auto ☐ Full ☐ Half
	LAN インターフェース(eth1)				
	インターフェースアドレス/プレフィックス				
	通信モード	Speed	☐ Auto ☐ 100 ☐ 10	Duplex	☐ Auto ☐ Full ☐ Half

特記事項	
------	--

接続回線情報について

「回線品目」「回線速度」をご記入ください。「接続形態」には「イーサネット接続」と、「PPPoE接続」があります。
PPPoE接続の場合は「PPPoE認証ID」「パスワード」の記入が必要になります。

拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

拠点間VPN(拠点情報)

SID ※	
VSR名称 ※	
シリアル ※	

※バリオセキュア記入欄

設置希望日

年 月 日

ご契約者様会社名

拠点名称

ブリガナ

拠点間VPN機器情報

VPN種別

L3VPN

拠点情報

拠点名

接続IP(GlobalAddress)

拠点間VPNについて

拠点間VPNはインターネット上にお客様専用の仮想回線を構築し、さくら側拠点とお客様拠点をセキュアに接続することで、インターネットを介した仮想的な1つのLANを構築できます。

■ 拠点名称

お客様側拠点の名称をご記入下さい

■ VPN種別

L3・・・VSRをルータとして動作させるモードです。各拠点で異なるセグメントをご利用頂けます。

■ 拠点情報

接続する全ての拠点名（さくら側拠点以外）と、IPアドレス情報をご記入下さい。

拠点間VPN接続

さくら側拠点

専用サーバPlatformネットワーク

お客様側

インターネット

暗号通信(トンネル)

お客様拠点A

お客様拠点B

お客様拠点C

拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

Router

SID ※

VSR名称 ※

シリアル ※

※バリオセキュア記入欄

設置希望日

ご契約者様会社名

年

月

日

複数のLAN（セグメント）が存在する場合には、これらのLANからインターネットをご利用頂くためにVSRにルーティング情報を設定する必要があります。各LANのネットワークアドレスとVSRからこれらのLANに到達するためのゲートウェイのアドレスをご記入ください。

スタティックルーティング

ネットワークIPアドレス/プレフィックス

ゲートウェイIPアドレス

デフォルトゲートウェイ

インターフェース

ネットワークIPアドレス

Metric

WANインターフェース (eth0)

LANインターフェース (eth1)

スタティックルーティングについて

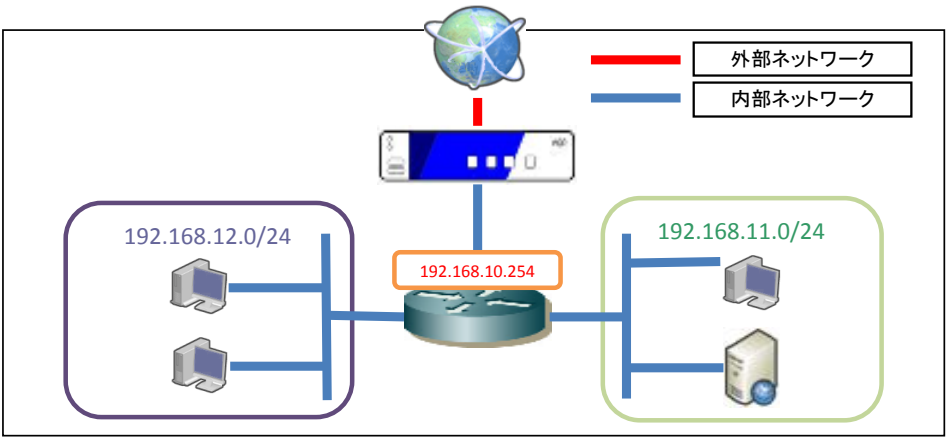
お客様のネットワークに複数のセグメントが存在している場合、VSRにルーティングの設定を行う必要があります。

■「ネットワークIPアドレス/プレフィックス」

対象のセグメントのネットワークアドレス、サブネットワークをプレフィックス表記で記入します。

■ゲートウェイIPアドレス

ネクストホップになるアドレスを記入します。



拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

Router

SID ※	
VSR名称 ※	
シリアル ※	

※バリオセキユア記入欄

設置希望日

ご契約者様会社名

年 月 日

LANがプライベートアドレスであり、かつ外部からアクセスする必要のあるサーバが設置されている場合には、これらのサーバのプライベートアドレスにグローバルアドレスを対応させる必要があります。以下に、プライベートアドレスとグローバルアドレスの対応を記述してください。

[illegible]

LANにプライベートアドレスをご利用の場合には、インターネットを利用するにあたりIPマスカレードを使用する必要があります。

[illegible]

スタティックNATについて

LANがプライベートアドレスであり、かつ外部からアクセスする必要があるサーバが設置されている場合には、これらのサーバのプライベートアドレスにグローバルアドレスを対応させる必要があります。

■グローバルIPアドレス

対応づけるグローバルIPアドレスを記入します。

■インターフェース

NAT変換を行うインターフェースを記入します。基本的には「eth0 (WAN)」インターフェースを記入します。

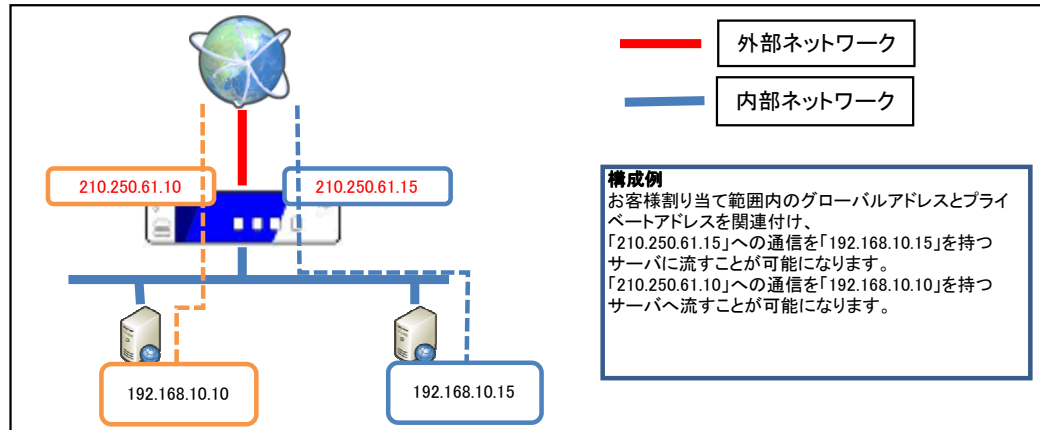
■プライベートIPアドレス

グローバルIPアドレスと関連づくプライベートアドレスを記入します。

■All I/F

「Yes」を指定すると、NAT変換を全てのインターフェースに対して行います。

「No」を指定すると「インターフェース」で指定したインターフェースを通過した通信のみNAT変換が行われます。



IPマスカレードについて

LANにプライベートアドレスをご利用の場合には、インターネットを利用するにあたりIPマスカレードを使用する必要があります。

■インターフェース

マスカレードを利用するインターフェースを指定します。通信が向うインターフェースを指定します。

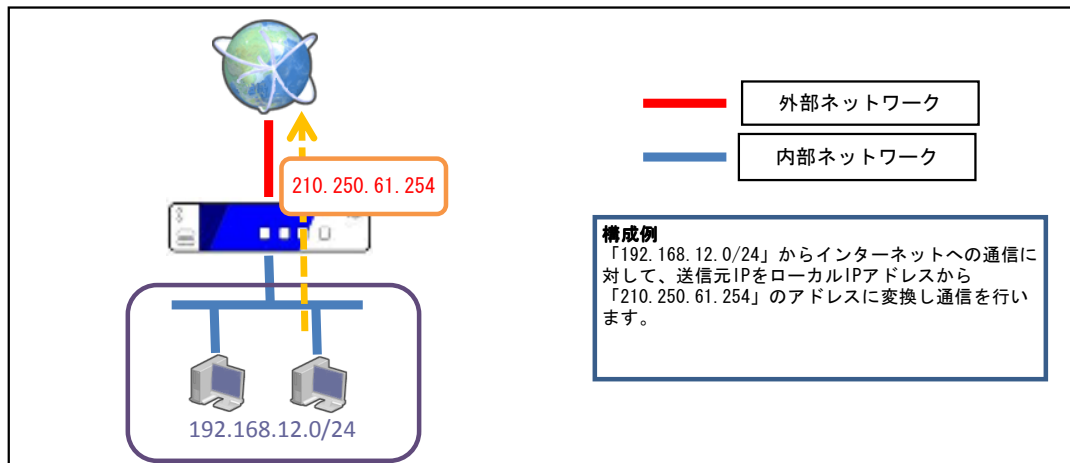
インターネットへの通信でマスカレードを利用する場合は、WANのインターフェース「eth0」を記入します。

■プライベートネットワークアドレス/プレフィックス

LANに複数プライベートネットワークがある場合、それぞれのネットワークアドレスに対して記入します。

■グローバルIPアドレス

プライベートアドレスに対応づけるグローバルIPアドレスを記入します。



拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

Router

SID ※

VSR名称 ※

シリアル ※

※バリオセキュア記入欄

設置希望日

ご契約者様会社名

年 月 日

LAN等のクライアントホストにDHCP機能を使用しVSRからIPアドレスを配布することが可能です。以下に詳細な情報をご記入下さい。

DHCPサーバ機能	☐ 利用する ☐ 利用しない	
	配布IPアドレス	開始IPアドレス
		終了IPアドレス
	DNS情報	プライマリDNS IPアドレス
		セカンダリDNS IPアドレス
	WINS情報	プライマリWINS IPアドレス
セカンダリWINS IPアドレス		

NTPサーバ機能は標準で機能しております。ご使用になる場合は、各端末のNTPサーバとしてVSRの各インターフェース(LAN,DMZ等)のIP Addressを設定して下さい。

NTPサーバ機能

記入して頂く情報はありません。

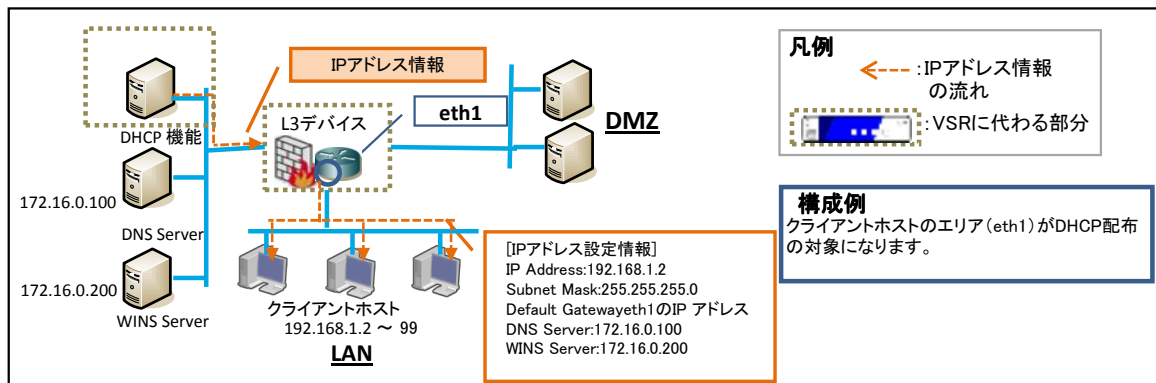
VSRのDNSリゾルバ機能ご利用(する・しない)を以下に反映願います。

DNSリゾルバ機能

☐ 利用する☐ 利用しない

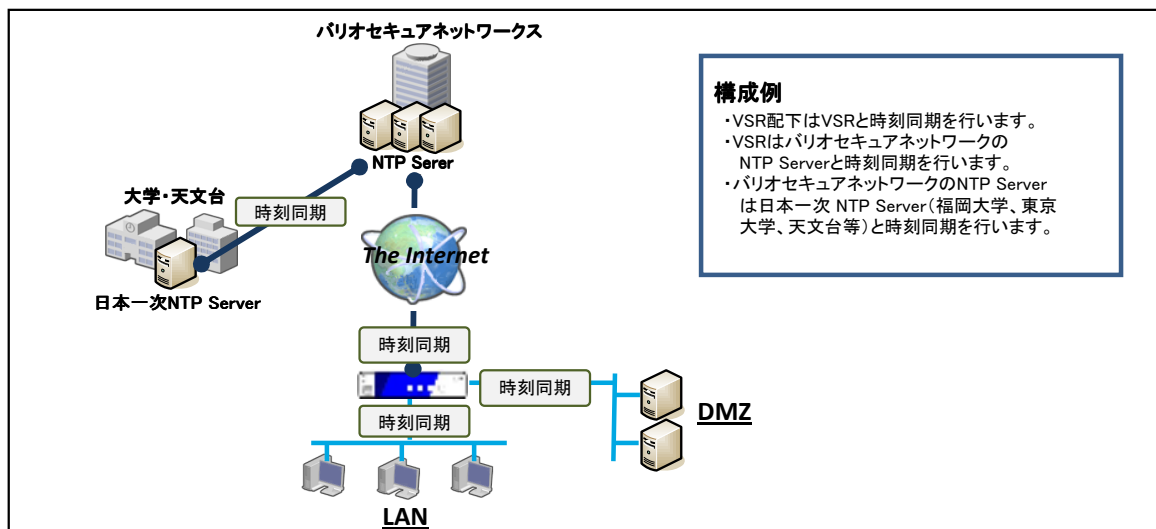
DHCP機能について

DHCPはクライアントホストに自動的にIPアドレス情報を設定する機能で、サーバアプリケーションです。



NTPサーバ機能について

NTPとはコンピュータの内部時計を、ネットワークを介して正しく調整するプロトコルです。



拠点間VPN（ベースセット） / サテライト追加用（VarioSecure VSR700）

設定ヒヤリングシート

FireWall

SID	
VSR名称	
シリアル	

ご契約者様会社名

* バリオセキュア記入欄
設置希望日

年 月 日

Firewallに設定するセキュリティ・ポリシーを策定して頂きます。

用語	アクション		ゾーン名			
	ACCEPT	パケットの通過を許可	net	WANポートを定義するゾーン	fw	VSR自体のゾーン
	DROP	パケットを破棄	loc	LANポートを定義するゾーン	***	カスタムゾーン指定
	REJECT	パケットを拒否	vpn	スプーク拠点を定義するゾーン		

お客様にてご指定いただきましたポリシーに該当しない場合、以下のデフォルトルールが適用されます。
お客様のポリシーに従って変更して頂くことも可能です。

※サテライト拠点が2拠点以上の場合のみご利用いただけます

基本ポリシー	ルール 選択	ポリシー名称	アクション	送信元 ゾーン	送信先 ゾーン	
	☐	標準設定	ACCEPT	loc	net	すべての拠点間の通信を許可する設定です。
			ACCEPT	loc	loc	
	☐	※スプーク間アクセス拒否	ACCEPT	loc	net	スプーク拠点間のアクセスをすべて拒否する設定です。ハブ拠点とスプーク拠点の通信はすべて許可します。
			ACCEPT	loc	vpn	
			ACCEPT	vpn	loc	
	全ポリシー共通設定		REJECT	vpn	vpn	
			DROP	net	net	全ポリシーの共通設定です。共通設定を変更することはできません。
			DROP	net	all	
			REJECT	all	all	

[VarioSecure管理用ルール]

以下は弊社監視センターから管理用に使用するセキュリティポリシーとなります。この項目は管理上、変更することはできません。

VarioSecure 管理用ルール	アクション	送信元		送信先			
		ゾーン	IPアドレス	ゾーン	IPアドレス	プロトコル	ポート
	ACCEPT	net	\$VARIOSECURE	fw	-	icmp	-
	ACCEPT	net	\$VARIOSECURE	fw	-	tcp	ssh,snmp
	ACCEPT	net	\$VARIOSECURE	fw	-	udp	snmp,snmptrap
	ACCEPT	loc	-	fw	-	udp	domain,bootps,ntp
	ACCEPT	loc	-	fw	-	tcp	domain
	ACCEPT	loc	-	fw	-	icmp	echo-request
	ACCEPT	dmz	-	fw	-	udp	domain,bootps,ntp
	ACCEPT	dmz	-	fw	-	tcp	domain
	ACCEPT	dmz	-	fw	-	icmp	echo-request

[VarioSecure基本ルール]

BlasterW@rmでのパケットの抑制やNetBIOSをインターネットへ遮断するなどの基本ルールセットです。

VarioSecure 基本ルール	アクション	送信元		送信先			
		ゾーン	IPアドレス	ゾーン	IPアドレス	プロトコル	ポート
	DROP	loc	-	net	-	tcp	35,139,445,593,4444,666
	DROP	loc	-	net	-	udp	69,135,139,445
	DROP	dmz	-	net	-	tcp	35,139,445,593,4444,666
	DROP	dmz	-	net	-	udp	69,135,139,445
	REJECT	net	-	loc	-	tcp	auth
	REJECT	net	-	dmz	-	tcp	auth
	DROP	all	-	net	-	tcp	6667

さくらインターネット管理用ルール

（※こちらの項目はさくらインターネットにて管理用に使用するセキュリティポリシーとなります。この項目は管理上変更することはできません）

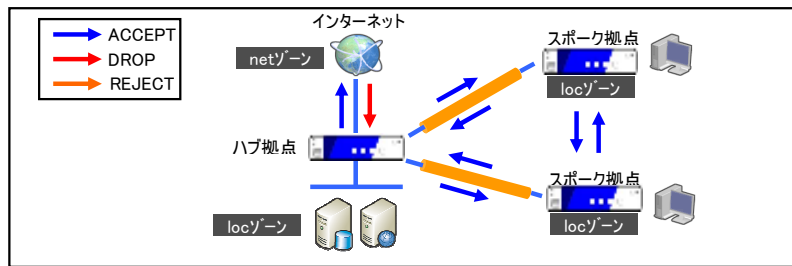
さくらインターネット 管理用ルール	アクション	送信元		送信先			
		ゾーン	IPアドレス	ゾーン	IPアドレス	プロトコル	ポート
	ACCEPT	net	\$SAKURANET	-	お客様ネットワーク	全て	全て
	ACCEPT	net	\$SAKURANET	-	お客様ネットワーク	全て	全て

基本ポリシーについて

基本ポリシーからお客様のネットワーク環境に応じたポリシー設定が可能です。
標準で用意されている3パターンの基本ポリシーから適当なポリシーを選択してください。
(下図は、サテライト拠点が2拠点以上の場合を想定したものとなります)

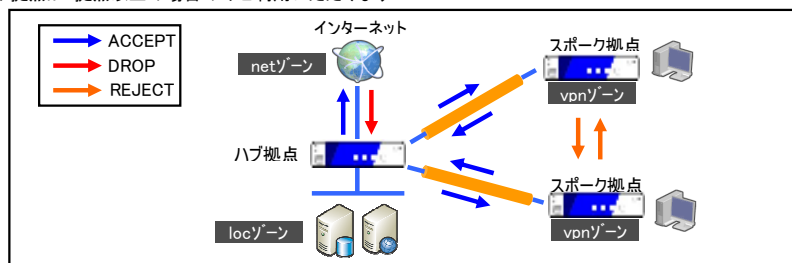
【標準設定】

VPN間の通信をすべて許可するポリシーです。スポーク拠点のゾーンをハブ拠点のネットワークと同じ「loc」ゾーンに割り当て、「loc」to「loc」のポリシーをACCEPT指定することでVPN間の通信を許可します。



【スポーク間アクセス拒否】

スポーク拠点間の通信を一切拒否するポリシーです。スポーク拠点とハブ拠点の通信はすべて許可します。スポーク拠点をすべて「vpn」ゾーンを定義し、「vpn」to「vpn」のポリシーをREJECT指定することでスポーク拠点間の通信を拒否します。
※サテライト拠点が2拠点以上の場合のみご利用いただけます



設定ヒヤリングシート

[illegible]

追加ルールについて

■基本ポリシーで「loc」to「net」のポリシーを“REJECT”、または“DROP”指定した場合に追加ルールを記載ください。

■アクション

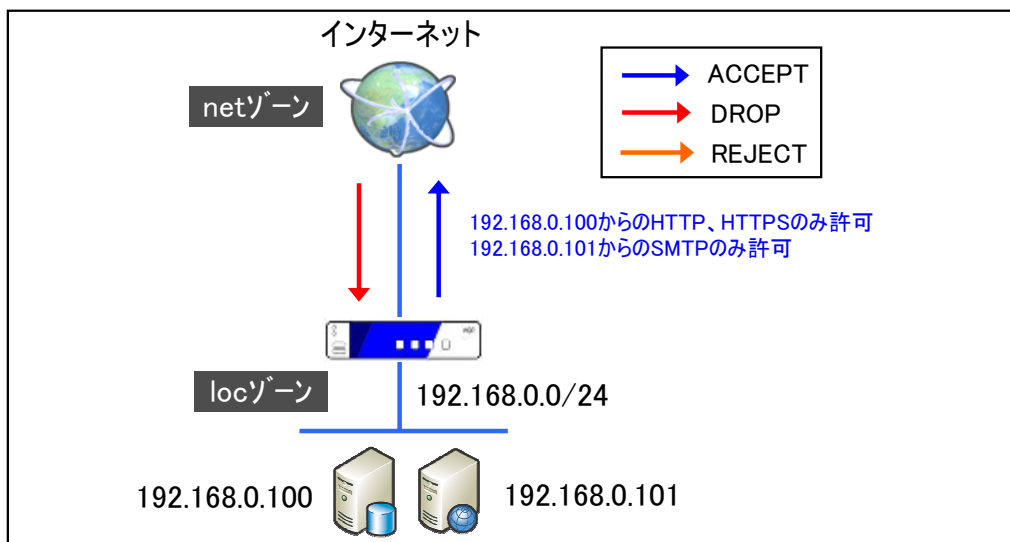
ACCEPT、REJECT、DROPからご指定いただけます。

■プロトコル・ポート

RFCに準拠した名前での記載をお願い致します。

※記入例

アクション	送信元		送信先			
	ゾーン	IPアドレス	ゾーン	IPアドレス	プロトコル	ポート
ACCEPT	loc	192.168.0.100	net	any	tcp	http,https
ACCEPT	loc	192.168.0.101	net	any	tcp	smtp



※注意

公開サーバへのアクセス(インバウンド)ルールはサービス仕様上 設定することができません。

※インバウンド通信ポリシー「net」to「loc」はすべて拒否(DROP)する設定となります。

変数定義について

■変数名

大文字ローマ字で入力をお願いします。特殊文字は「アンダーバー」[_]のみご利用できます。

■変数

IPアドレス・ポート番号をご指定できます。複数入力する際は「カンマ」区切りで記入します。