

『ファイアウォール+IDS/ADS+ロードバランサー(L4)』(VarioSecureVSR)

設定ヒヤリングシート

サイト・セキュリティ・プロフィール

SID(弊社記入欄)

※下欄の太枠内をご記入ください

ご契約名

設置希望日

年 月 日

会員ID

※さくらインターネット会員IDをお持ちの方はこちらをご記入ください

管理者情報

	管理者 1	管理者 2	管理者 3
会社名			
部署			
氏名			
TEL			
FAX			
Mail			

機器情報

ご使用機器	VSR2000	オプション	☒ Firewall ☒ IDS/ADS ☒ ロードバランサー
-------	---------	-------	---

『ファイアウォール+IDS/ADS+ロードバランサー(L4)』(VarioSecureVSR)

設定ヒヤリングシート

Firewall

※下欄の太枠内をご記入ください

SID(弊社記入欄)

ご契約名

設置希望日

年 月 日

会員ID

※さくらインターネット会員IDをお持ちの方はこちらをご記入ください

ファイアウォールに設定するセキュリティポリシーを策定していただきます。

許可/拒否をご指定の上、それぞれのゾーン(net側、dmz側、loc側)及びIPアドレスより特定のIPアドレス/ポートに対するポリシーをご記入ください。

セキュリティポリシー

		アクション		ゾーン名				
		ACCEPT	パケットの通過を許可	net	WANからの通信に対するゾーン		fw	VSR自体のゾーン
		DROP	パケットを破棄	loc	LANからの通信に対するゾーン			
		REJECT	パケットを拒否	dmz	DMZからの通信に対するゾーン		ext	VSR2000以上のextに対するゾーン
基本ポリシー		アクション	送信元ゾーン			送信先ゾーン		
		REJECT	loc			net		
		ACCEPT	loc			dmz		
		ACCEPT	loc			ext		
		ACCEPT	dmz			net		
		REJECT	dmz			loc		
		REJECT	dmz			ext		
		ACCEPT	rvpn			net		
		ACCEPT	rvpn			loc		
		ACCEPT	rvpn			dmz		
		ACCEPT	rvpn			ext		
		ACCEPT	ext			net		
		REJECT	ext			loc		
		REJECT	ext			ext		
		DROP	net			net		
		DROP	net			all		
		REJECT	all			all		
		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,nto
ACCEPT	loc			—	fw	—	tcp	domain
ACCEPT	loc			—	fw	—	icmp	echo-request
ACCEPT	dmz			—	fw	—	udp	domain,bootps,nto
ACCEPT	dmz			—	fw	—	tcp	domain
ACCEPT	dmz			—	fw	—	icmp	echo-request
ACCEPT	ext			—	fw	—	udp	domain,bootps,nto
ACCEPT	ext			—	fw	—	tcp	domain
ACCEPT	ext			—	fw	—	icmp	echo-request
(※お客様のポリシーにてご指定いただきましたポリシーに該当しない場合、右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。ご希望の設定変更内容は、下欄「追加ポリシー」へご記入ください。)								
(※こちらの項目はVarioSecure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)								

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を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)	送信元			送信先			
	アクション	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	指定なし(全て)	指定なし(全て)
	ACCEPT	net	\$SAKURANET	-	お客様ネットワーク	指定なし(全て)	指定なし(全て)
VarioSecure 基本ルール (BlasterW@rmでのパケットの抑制やNetBIOSwo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。この項目は管理上変更することはできません)	送信元			送信先			
	アクション	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	135,139,445,593,4444
	DROP	loc	-	net	-	udp	69,135,139,445
	DROP	dmz	-	net	-	tcp	135,139,445,593,4444
	DROP	dmz	-	net	-	udp	69,135,139,445
	DROP	ext	-	net	-	tcp	135,139,445,593,4444
	DROP	ext	-	net	-	udp	69,135,139,445
	REJECT	net	-	loc	-	tcp	auth
	REJECT	net	-	dmz	-	tcp	auth
	REJECT	net	-	ext	-	tcp	auth
追加ポリシー (以下の項目にポリシーをご記入いただくことにより、基本ポリシーに優先されルールが適用されます。 ※ご記入いただきました順番にてポリシーチェックが実行され、ポリシーにマッチした時点で、許可・拒否の処理が行われます。)	送信元			送信先			
	アクション	ゾーン	IPアドレス	ゾーン	IPアドレス	プロトコル	ポート
変数定義 (プロトコル名、ポート名はRFCに準拠した名前でご記入ください。 RFCに準拠していないポート番号やIPアドレスブロックを変数にて定義することが可能です。 前頁のIPアドレスの欄にて変数を使用する際は[\$変数]という書き方をお願いします。)	変数名			変数			

『ファイアウォール+IDS/ADS+ロードバランサー(L4)』(VarioSecureVSR)

設定ヒヤリングシート

IDS/ADS

SID(弊社記入欄)

※下欄の太枠内をご記入ください

ご契約名

設置希望日

年 月 日

会員ID

※さくらインターネット会員IDをお持ちの方はこちらをご記入ください

「IDS」・・・Intrusion Detection System

「ADS」・・・Active Defense System

※ADSセーフティゾーン

ADSにてブロックしない安全とみなすIPアドレスをご記入ください。

ADSセーフティゾーン

	送信元/送信先	IPアドレス				/プレフィックス

『ファイアウォール+IDS/ADS+ロードバランサー(L4)』(VarioSecureVSR)

設定ヒヤリングシート

ロードバランサ

SID(弊社記入欄)

※下欄の太枠内をご記入ください

ご契約名

設置希望日

年 月 日

会員ID

※さくらインターネット会員IDをお持ちの方はこちらをご記入ください

※ロードバランシングする際に使用する公開用IPアドレス番号をA～として、そのA～のバランシンググループに所属させたいサーバ番号 **サーバ①** ～ **サーバ⑩** をご記入下さい。(「サーバ番号」とは別紙「利用申込書」内のサーバ番号を指します)

ロードバランサ

グループ名	振り分け方法	☐ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
グループ名	振り分け方法	☐ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
グループ名	振り分け方法	☐ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
グループ名	振り分け方法	☐ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
グループ名	振り分け方法	☐ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			

グループ名	振り分け方法	Webグループ	6 分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
グループ名	振り分け方法	☒ ラウンドロビン ☐ リーストコネクション ☐ パーシスタンス	6 分
バランシンググループ番号	バランシンググループ 及び 属させるサーバ番号	ポート	ウェイト
上記のバランシンググループに属させるサーバ			
	A	http	
	サーバ①	https	50
	サーバ③		25
	サーバ⑦		25

ご記入例