

SG3600LM,SG3600LG,SG3600LJ V8.2, V8.3

冗長化機能説明書

2019年10月3版

<u>目 次</u>

1.	概要		1
	1. 1.	動作概要	1
	1. 2.	冗長化構成の条件	2
2.	冗長化構	靠成手順	3
	2.1.	セットアップ	3
	2. 2.	運用系 冗長化機能の設定	4
	2.3.	待機系 冗長化機能の設定・起動	9
	2.4.	冗長化機能の起動	13
	2.5.	ルール設定の同期	17
	2.6.	バックアップについて	19
	2.7.	フェイルオーバ時のメール通報について	19
	2.8.	フェイルオーバ時のメールデータ移行について	19
	2.9.	冗長化機能のログについて	19
	2. 10.	冗長化構成時の複数パッチ適用について	19
	2.11.	冗長化構成時の待機系追加について	20
3.	注意事項	[21

1. 概要

本章では、SGを冗長化構成で構築する場合の動作や条件について説明します。

1.1. 動作概要

SG を2台設置して冗長化設定を行うことで、片方が停止しても、もう片方のSGが処理 を引き継ぐことができ、障害時の業務停止時間を最小限に抑えることができます。また、 プロセスの異常を検出した場合や通信が不能になった場合にも、処理を引き継ぐことが可 能です。以下に通常運用時、障害発生時の動作について説明します。

なお本書では、通常運用時に処理を行うSGを「運用系」、障害発生時などに運用系か ら切り替わって処理を引き継ぐSGを「待機系」と呼びます。

通常運用時

- 運用系のSGを利用して通信を実現しています。この時、運用系に設定された仮想IPアドレスが有効になっています。
- 待機系は起動していますが、設定された仮想IPアドレスは無効になっています。
- 運用系と待機系は互いに状態を監視します。
- 運用系 障害時
 - 一待機系が運用系のダウンを検出します。自動でフェイルオーバが実行されます。
 - 待機系のファイアウォール機能が仮想 IPアドレスを有効にします。
 - 通信処理は待機系が引き継ぎます。
 - 切り替わりに伴う設定の変更は必要ありません。
- 運用系 復旧時
 - 一 待機系が運用系の復旧を検出します。「自動フェイルバック」の設定が「する」の場合は自動でフェイルバックが実行されます。「しない」の場合は手動でフェイルバック(冗長化切替)を実行します。
 - 待機系のファイアウォール機能が仮想 IPアドレスを無効にします。
 - 運用系のファイアウォール機能が仮想 IPアドレスを有効にします。
 - フェイルバック時に、通信処理は運用系に切り戻されます。
 - 切り替わりに伴う設定の変更は必要ありません。
- フェイルオーバが起きる条件(運用系)
 - 対向となるSGの送信パケットが受信できない。
 - 仮想IPアドレスを設定しているインタフェースが停止する。
 - 仮想IPアドレス設定が削除される。
 - 基本ファイアウォールが停止する。
 - 仮想ファイアウォールの起動/停止状態が管理者の意図した状態と異なる。
 - 冗長化のプロセスの異常を検出する。
 - 監視対象IPアドレスとの通信途絶が発生する。

1.2. 冗長化構成の条件

SGを冗長化する場合、次の条件を満たしていないと正しく動作しません。

- 冗長構成を組む2台のSGに、それぞれの実IPアドレス紐付いたライセンスキーとサポートキーが登録されていること。ライセンスキーとサポートキーがそれぞれのSGに投入されている状態にしてください。
- 運用系と待機系のソフトウェアのバージョンが完全に一致していること。
 なお、ソフトウェアのアップデートを行う場合は、待機系、運用系の順番で実施してください。
- 運用系と待機系の冗長化基本設定とセキュリティポリシーの設定内容が完全に一致 していること(SG本体に割り当てるIPアドレスなどのシステム基本設定は除く)
- 運用系と待機系とも冗長化機能のサービスが起動していること

2. 冗長化構成手順

本章では、SG を冗長化構成で構築する場合の手順について説明します。 運用系、待機系それぞれの主な構築の流れは以下のとおりです。



2.1. セットアップ

製品添付のセットアップ手順説明書に従い、SGを2台、初期導入まで行い準備します。

2.2. 運用系 冗長化機能の設定

以下の手順で、運用系のManagement Consoleにて設定を行います。なお、手順中の画像で入力しているIPアドレス、ホスト名などは設定例です。お客様環境にあわせて適宜読み 替えてください。

(1) [基本設定]にて、冗長化機能を「使用」に変更し、画面下部の [設定]ボタンをクリックします。

SG3600LM Ver8.	0.0 @ sg.com		Ž.	States 2.	- 55	<u>п</u> бл
2- 設定			,			
				基本設定		
, , , , , , , , , , , , , , , , , , , ,						Fo u =
inistrator 👻	全个议上					<u>ENU</u>
	■ 其大語史(※종물중산■①1	百日1+設空亦 面	後に再わわれ心す	5 次才)	
ジ <u>ファイアウォール</u>	操作設	定項目	用间酸准氮类	「使」に伴れた動力が少しる	e (y)	
■ <u>サービス</u> ■ パッケージ	 ホスト名() 	FQDN)	secom			
<u>システム</u>	-		IPv4アドレス	IPv4ネットマスク	IPv6アドレス(リンクローカ)	ル) MTU値
基本設定	-	内側	192.168.1.71	255.255.255.0	fe80::20c:29ff:fe77:a5b4/	64 1500
<u>7-172</u>	-	外側	192.168.2.71	255.255.255.0	fe80::20c:29ff:fe77:a5be/	64 1500
] <u>リモートメンテナンス</u>	-	DMZ			fe80::20c:29ff:fe77:a5c8/	/64
	-	予備			fe80::20c:29ff:fe77:a5d2/	64
	-	eth4				
	-	eth5	10.71.50.100	055 055 055 0	[[00 00 00((77 5/0)	1500
		ethb	10.71.52.102	255.255.255.0	jte80::20c:29tt:te77:abt07	64 1500
	-	eth /	<u> </u>		J	
		etho oth0				/64
	- インタフェー	-ス	IPv6アドレス/プリ	ノフィックス長 (1番日)	IPv67ドレス/プレフィックス	7.長(2番目)
	-	内側		//////////////////////////////////////		04 (2 8 2)
	-	外側			1	
	-	DMZ			<u> </u>	
	-	予備			Î	
	-	eth4			Ĩ	
	-	eth5				
	-	ethô				
	-	eth7				
	-	eth8				
	-	eth9				
	- bondine-11	ノタフェース	IPv4アドレス	IPv4ネットマスク	IPv6アドレス	MTU值
	- IPud ==	etn4_! ルトゲートウェイ	192 168 1 254	200.200.200.0		Metric
	- IP-6="	ルトゲートウェイ	102.100.1.204			
	-		IPv4アドレス	IPv4ネットマスク	IPv4ゲートウェイ	インタフェース
	IP v4 青色りノ 追加	レーティング 1				自動 👻
	-		IPv6アドレス/プレ	ノフィックス長 IPv	6ゲートウェイ	インタフェース
	這加	1				自動 ▼
	追加 <u>ネームサ</u> ー	<u>-)រ</u> ំ				
	- 管理者メ-	・ルアドレス	sø@sø			
	- IPv4メール	ゲートウェイ	未使用 ▼			
	ー IPv6メール	ゲートウェイ	未使用 ▼			
	追加TRAP送信	先ホスト 1				
	追加 同期するト	<u>TPサーバ</u> 1				
	TE /1.404	als.	(書田 _			

(2) [サービス] > [冗長化機能] > [設定]画面にて、冗長化設定を行います。
 各設定項目を入力後、画面下部の[設定]ボタンをクリックします。
 各項目の詳細は、表 1 冗長化機能 設定項目一覧 を参照ください。

SG3600LM Ver8.0.0	sg.com	Ţ	i for	Ë S	24 D 055	アウト	
モニター 設定							
[ファイアウォール]				設定			
Administrator •	<u>ナービス</u> > <u>冗長化機能</u> > 🏻	定				<u>.71</u>	
		(1)	(2)		 必須設定項目 任意設定項目 		
	■ 基本設定						
▶ (F) <u>10(3) アイアリォール</u> 基本設定		標準	内側	192.168.1.70			
<u> </u>		標準	外側	192.168.2.70			
リモートメンテナンス		標準	eth6	10.71.52.100			
		標準	eth7				
		標準	eth8				
	仮想IPアドレス	標準	eth4_t	10.71.51.100			
		vse1	内側	10.71.31.100			
		vse1	外側	10.71.32.100			
		vsv1	内側	10.71.41.100			
		vsv1	外側	10.71.42.100			
		vsv1	予備	10.71.43.100			
		ファイアウォール	名 種別	リモートSGの同期用IPアドレス	ローカルSGの インタフェース		
	設定同期・状態取得	標進	メイン	10.71.51.101	eth4_b: 10.71.51.102 🗸		
			サブ		-		
		運用系サーバ	☑ 運	用糸として動作させる			
	■ 詳細設定						
	VRRP VRID	91)				
	広告パケット送信間隔	(秒) 3					
	自動フェイルバック	ック うする のしない					
	フェイルバック待ち時間	劉(秒) 11					
	監視対象IPアドレス	1	2.168.1.1				
			設定	キャンセル			

項目名	設定内容
仮想IPアドレス	設定同期用インタフェースを除く全インタフ
① ファイアウォール名(基本ファイアウォールは「標準」と	ェースに仮想IPアドレスを設定します。仮想フ
表示されます)	ァイアウォールは起動しているもののみ表示
 インタフェース名(* 内側、* 外側、DMZ、予備、eth4~ 	されます。SG経由の通信は原則仮想IPアドレ
eth11、eth4_b~eth11_b)	スを使用する必要があります。
リモートSGの同期用IPアドレス(* メイン, サブ)	設定同期と状態取得で使用する対向SGのIPア
	ドレスを設定します。同期できる設定はファイ
	アウォールメニュー配下の設定のみとなりま
	す。対向SGとの設定の同期はファイアウォー
	ルメニューから行うことができます。サブを設
	定すると、メインの設定で対向マシンとの通信
	が失敗した際に、サブの設定で対向マシンと通
	信を行います。
ローカルSGのインタフェース(* メイン, サブ)	設定同期と状態取得で使用する接続中のSGの
	ネットワークインタフェースを選択します。メ
	インは必須項目です。サブを設定すると、メイ
	ンの設定で対向マシンとの通信が失敗した際
	に、サブの設定で対向マシンと通信を行いま
	す。
* 運用系サーバ	運用系として動作させるかどうかを選択しま
	す。選択しなかった方が、待機糸となります。
* VRRP VRID	VRRP VRIDを指定します。同一セグメントに
	冗長構成にしているSGの組が複数存在する場
	合は、それぞれの組で異なるIDを指定するよう
	にします。対向のSGと同じ値を設定する必要
	かめります。 1から255までの登剱を指定しま +
* さたぷん…し光信明頃(か)	
「広告ハケット送信间啊(桜)	VRRP 広告ハケットの送信间隔を砂単位で設 ローキオー対応のCCトロドはた記会オモッ亜
	たしまり。対问の3Gと问し値を設たりる必要
	かめりより。 から000よどの症候を指定しよ
	² 。
	と用来、守機米が初の物理マンクで起動してい る場合は 3(秒)以上の設定を推奨します
	自動フェイルバックを行うかどうか選択しま
	^。 「する」を選択した場合は、運用系復帰時に自
	動で運用系に業務を切り戻します。
* フェイルバック待ち時間(秒)	フェイルバックするまでの待ち時間を秒単位
	で指定します。対向のSGと同じ値を設定する
	必要があります。1から600までの整数を指定
	します。
監視対象IPアドレス	監視対象として設定されたIPアドレスとの通
	信が途絶した場合は、待機系にフェイルオーバ
	します。本項目の設定は省略することができま
	す。指定できるIPアドレスの最大数は8です。

表 1 冗長化機能 設定項目一覧

※ 各項目先頭のアスタリスク(*) は必須項目

(3) [サービス]画面にて、冗長化機能を起動します。 冗長化機能の起動は、[起動]ボタンをクリックすることで行います。

SG3600LM Ver8.0.0	a sg.com	25	3. IN E		
[ファイアウォール]			÷	ービス	
Administrator 🔻	₩-ビス				[ブルブ]
	■ サービ	ג'			
 ▶ 10 1-y=-y ▶ 22.5-4 ▶ 10 (22.5-4) ▶ 10 (20.7-4.7-7) x=-1/4 	OS 起動時 の状態	現在の 状態	(再)起動	停止	サービス
	—	起動中	再起動	停止	<u>SMTPサーバ</u>
	起動 ▼	起動中	再起動	停止	<u>POPサーバ</u>
	停止 👻	停止中	起動	停止	<u>SSL-VPN機能</u>
	停止 ▼	停止中	起動	停止	<u>L2TP/IPsec-VPN機能</u>
	-	煮効	-	-	<u>リモート管理サービス</u>
	停止 👻	停止中	起動	停止	Webキャッシュサーバ
	停止 👻	停止中	記動	停止	IPv6 RA設定機能
	停止 マ	停止中	起動	停止	
	停止 ▼	得止甲	起動	停止	RIP/RIPng設定機能
	-	起動甲	用起朝	-	
		停止中	武三里川	19IE	
	(高山 -	信止由		「信止」	<u>GRE1版能</u> 转動監視機能
	停止 -	停止中	記録の	停止	One Point Wall
	停止 ▼	停止中	起動	停止	OPWアラート通知
			[設定	
	※ One F するこ ※ L2TP, 能を同	Point Wall とはでき /IPsec-V 同時に利用	とWebキャッ ません。 PN機能とつ 用することに	ッシュサ ファイア はできま	ーバの機能を同時に利用 ウォールメニューのVPN機 せん。

(4) [ファイアウォール]画面にて、[かんたん設定]のウィザードを実行します。 すでに設定済みの場合でも再設定します。



(5) [サービス]画面にて、冗長化機能を停止します。 冗長化機能の停止は、[停止]ボタンをクリックすることで行います。

SG3600LM Ver8.0.0	@ sg.com		J. T. S.	ES S	• *	A Land	ログアウト
モニター 設定							
[ファイアウォール]				サ	ービス		
Administrator 👻	€-±⊅						[ヘルプ]
		■ サービ	ג'				
▶ 13-27>> ▶ 13-27>>> ▶ 13-22万五 ■ 165877-47-11+11+		OS 起動時 の状態	現在の 状態	(再)起動	停止	サービス	
□ 基本設定		-	停止中	起動	停止	<u>SMTPサーバ</u>	
		起動 👻	起動中	再起動	停止	<u>POPサーバ</u>	
<u>0++30370X</u>		停止 👻	停止中	起動	停止	<u>SSL-VPN機能</u>	
		停止 👻	停止中	起動	停止	<u>L2TP/IPsec-VPN機能</u>	
		-	煮効	-	-	<u>リモート管理サービス</u>	
		停止 👻	停止中	起動	停止	<u>Webキャッシュサーバ</u>	
		停止 👻	停止中	起動	停止	IPv6 RA設定機能	
		起動 ▼	起動中	再起動	停止	<u>元長化機能</u>	
		停止 👻	停止中	起動	停止	RIP/RIPng設定機能	
		-	起動中	再起動	-	<u>NTPサーバ</u>	
		停止 👻	停止中	起動	停止	ネームサーバ	
		-	-	-	-	<u>GRE機能</u>	
		停止 ▼	停止中	起動	停止	<u>稼動監視機能</u>	
		19止 🔻	停止中	226肋	19止	One Point Wall	
		19止 🔻	停止甲	配置の	19止		
				[读定		

2.3. 待機系 冗長化機能の設定・起動

以下の手順で、待機系のManagement Consoleにて設定を行います。なお、手順中の画像で入力しているIPアドレス、ホスト名などは設定例です。お客様環境にあわせて適宜読み 替えてください。

(1) [基本設定]にて、冗長化機能を「使用」に変更し、画面下部の

5G3600LM V	er8.().()	_)	SPE 1	3 Gal	7
(ファイアウォール)				ž	基本設定		
Administrator 👻	本設定)					
 ▶ 2 <u>774775</u> 3 − 1 ▶ <u>9 7 − ビス</u> 	■ 基:	本設定(※背景色が	一の耳	原目は設定変更	後に再起動が必要	ह्रिंग)	
▶ 10 バッケージ	操作	設定項目			10		
▷ 🗿 <u>ジステム</u>	-	ホスト名 (FQDN)		secom			
基本設定	-			IPv4アドレス	IPv4ネットマスク	IPv6アドレス(リンクローカル)	MTU
2442	-		内側	192.168.1.72	255.255.255.0	fe80::20c:29ff:fe5d:2a85/64	150
<u>リモートメンテナンス</u>	-		外側	192.168.2.72	255.255.255.0	fe80::20c:29ff:fe5d:2a8f/64	1500
	-		DMZ			fe80::20c:29ff:fe5d:2a99/64	
	-		予備			fe80::20c:29ff:fe5d:2aa3/64	
	-		eth4				
	-		eth5]	
	-		eth6	10.71.52.101	255.255.255.0	fe80::20c:29ff:fe5d:2ac1/64	1500
	-		eth7				
	-		eth8				
	-		eth9		1	fe80::20c:29ff:fe5d:2adf/64	- T
	-	インタフェース		IPv6アドレス/プレ	ノフィックス長(1番目)	IPv6アドレス/ブレフィックス長	(2番目)
	-		内側				
	-		外側			1	
	-		DMZ			1	
	-		子信			1	
	-		eth4			1	
	-		eth5				
	-		athf			I.	
	_		eth 0				
	-		etha				
	-		ethy				
	-	bondineインタフェース	added by	IPv47FUZ	IPv4ネットマスク	IPv6アドレス	MTU
		10-4 デフィルトダートウィイ	em+_b	100.160.1.054	200.200.200.0		Metr
		エッキアンオルトゲート・ウェイ		192.100.1.204	_		
	-	IPv6デフォルトゲートワェイ		an employ on		10.117.1ml / //	
	-	IP v4 静的ルーティング		IPW47FUX	IPWネットマスク	IPW07-F014 40	1917±
	1970		1			1 10	····
	-	IPv6青釉5ルーティング		IPV6アドレス/ラレ	ノフィックス長 IPv	67-1911	インタフェ
	0.00		1				E 90
	1000	ネームサーバ	1				
	-	管理者メールアドレス		sellse			
	-	IP・4メールゲートウェイ		未使用 ▼			
	-	IPv6メールゲートウェイ		未使用 ▼			
	這加	TRAP送信先ホスト	1				
	Sitte	TERMS	1				

(2) [サービス] > [冗長化機能] > [設定]画面にて、冗長化設定を行います。

各設定項目を入力する際、「運用系サーバ」のチェックを外します。また、「VRRP VRID」、「広告パケット送信間隔(秒)」、「フェイルバック待ち時間(秒)」は対向 のSGと同一にする必要があります。

入力後、画面下部の[設定]ボタンをクリックします。

GG SG3600LM Vert	8.0.0 @ sg.cor	n	S. J.S.	fs s	3 South	ログアウト	
モニター 設定							
[ファイアウォール]				設定			
Administrator 👻	<u>サービス</u> > <u>冗長化機</u>	<u>能</u> >設定				[ヘルプ]	
					 必須設定 任意設定 	官項目 官項目	
▶ ③ システム ▶ 同 仮想ファイアウォール	■ 基本設定		1.001				
○ <u>基本設定</u>		標準	内側	192.168.1.70		_	
		標準	911回	192.168.2.70		_	
<u> 92 13257 28</u>	-	標準	eth6	10.71.52.100			
		標準	eth7				
		標準	eth8			_	
	仮想Pアドレス	標準	eth4_b	10.71.51.100			
		vsg1	内側	10.71.31.100		_	
		vsg1	外側	10.71.32.100		_	
		vsv1	内側	10.71.41.100			
		vsv1	外側	10.71.42.100			
		vsv1	予備	10.71.43.100			
		ファイアウォール	名 種別	リモートSGの同期用IPアドレス	ローカルSGの インタフェース		
	設定同期・状態取得	槽淮	メイン	10.71.51.102	eth4_b: 10.71.51.101	-	
		104-4-	サブ			-	
		運用系サーバ	 3 3 3 3 4 4	用系として動作させる			
	■ 詳細設定						
	VRRP VRID	ç	90				
	広告パケット送信間隔	(秒) 3	3				
	自動フェイルバック) इठ 🤍	Jal 1			
	フェイルバック待ち時間	間(秒) 1	120				
	監視対象IPアドレス	1	192.168.1.1				
			設定	キャンセル			

(3) [サービス]画面にて、冗長化機能を起動します。 冗長化機能の起動は、[起動]ボタンをクリックすることで行います。



(4) [ファイアウォール]画面にて、[かんたん設定]のウィザードを実行します。 すでに設定済みの場合でも再設定します。

SG3600LM	Ver8.0.0 59 20m
モニター 設定	
[ファイアウォール]	ファイアウォール
Administrator 👻	マティアウォール [へルブ]
 ▶ 〒 マ<u>アイアウォール</u> ▶ ● ● <u>サーム</u> ▶ ● ● <u>サーム</u> ▶ ● ● <u>メッケージ</u> ▶ ● ● <u>レステム</u> ▶ ● ● <u>し、システム</u> ▶ ● ● <u>し、セステム</u> 	■ ルール設定 かんたん設定 詳細設定
 	■ 情報表示 状態表示
	 ■ ログ・アラート 表示 ダウンロード/アップロード
	■ ライセンス 確認/登録
	システムメンテナンス ソフトウェアアップデート バッグアップ・リストア ルール設定の同期

2.4. 冗長化機能の起動

以下の手順で、冗長化機能を起動し、冗長化構成での運用を開始します。

(1) 運用系のManagement Consoleにて、[サービス]画面より、冗長化機能を起動します。 冗長化機能の起動は、[起動]ボタンをクリックすることで行います。

SG3600LM Ver8.0.0	@ sg.com		2.39		б° <u>п</u> блон
モニター 設定					
			サ	ービス	
Administrator 🔻	₩-ビス				[ヘルブ]
	■ サ-	-ビス			
	OS 起動 の状	寺 現在の 状態	(再)起動	停止	サービス
▶ <u> </u>	-	起動中	再起動	停止	<u>SMTPサーバ</u>
	起動	▼ 起動中	再起動	停止	<u>POPサーバ</u>
<u>7€1727728</u>	停止	▼ 停止中	起動	停止	<u>SSL-VPN機能</u>
	停止	▼ 停止中	起動	停止	L2TP/IPsec-VPN機能
	-	煮効	-	-	<u>リモート管理サービス</u>
	停止	▼ 停止中	起動	停止	Webキャッシュサーバ
	停止	▼ 停止中	記動	停止	IPv6 RA設定機能
	停止	▼ 停止中	起動	停止	冗長化機能
	停止	▼ 停止中	建正要力	停止	<u>RIP/RIPng設定機能</u>
	-	起動中	再起動	-	<u>NTPサーバ</u>
	停止	▼ 停止中	起動	停止	<u>ネームサーバ</u>
	-	-	-	-	<u>GRE機能</u>
	停止	▼ 停止中	起動	停止	稼動監視機能
	停止	▼ 停止中	起動	停止	One Point Wall
	停止	▼ 停止中	起動	停止	<u>OPWアラート通知</u>
			[定	
	※ One する ※ L21 能を	e Point Wal ことはでき ア/IPsec-V E同時に利J	とWebキャッ ません。 (PN機能とつ 用することに	יシュサ 'ァイア' tできま	ーバの機能を同時に利用 フォールメニューのVPN機 せん。

(2) 運用系のManagement Consoleにて、[サービス] > [冗長化機能] > [状態表示]画面より、各SGの動作状態を確認します。運用系が「待機」、待機系が「現用」となっていることを確認します。各項目の詳細は、表 2 冗長化機能状態表示一覧を参照ください。

SG3600LM Ver8.0.0	◎ sg.com	ログアウト
モニター 設定		
[ファイアウォール]	状態表示	
Administrator 👻	<u> サービス > 冗長化機能 > 状態表示</u>	[ヘルブ]
	画面を更新する	
▶	■ 冗長化碳能 2015/05/12 1355.45	
 → 基本設定 ディスク リモートメンテナンス 	* ローカル:ss 1.0-0 リモート:ss ローカル	
	ローガル リモート 動作状態 VRRP VRID つ 10	
	優先度 200 100 仮想1Pアドレス(標準ファイアウォール) 内側: 192.166.1.70 - 0K	
	· 카베: 192,168.2,70 - 0K eth6: 10.271.52,100 - 0K eth4_b: 10.71.51.100 - 0K	
	仮想1Pアドレス(vst)) 内側: 10.71.31.100 - 0K 外間: 10.71.32.100 - 0K	
	仮想 IP アドレス (vav1) 内街: 10.71.41.100 - 0K 外街: 10.71.42.100 - 0K	
	子傭: 10.71.43.100 - OK モジュールステータス の の	
	ファイアウォール UK UK 仮想ファイアウォール OK OK クラスタ OK OK	
	自木スト監視対象1Pアドレス 192,168,1.1 0K -	
	- 110 小人「商U/JIAR // JR // アイレンス - OK 192,1858,1,1 - OK	
	冗長化切替	

表 2 冗長化機能 状態表示一覧

項目名		説明
ローカル:		冗長構成にしたSGのホスト名をそれぞれ表示します。先頭にアスタ
リモート:		リスク(*)のついている方が、現在接続中のSGです。
動作状態		冗長化機能の状態を表示します。現用、待機、異常のいずれかを表
		示します。
VRRP VRID		VRRP VRIDを表示します。ローカル列とリモート列の情報は同じ
		である必要があります。一致していない場合は設定内容を見直して
		ください。
優先度		優先度を表示します。「200」は運用系、「100」は待機系であるこ
		とを示します。
仮想IPアドレス	κ	仮想IPアドレスの状態を表示します。「OK」は仮想IPアドレスが付
		与されていることを示します。 「-(ハイフン)」は仮想IPアドレスが
		付与されていないことを示します。
モジュール	ファイアウォール	基本ファイアウォール機能の状態を表示します。「OK」は正常動作
ステータス		していることを示します。「NG」は正常動作していないことを示し
		ます。
	仮想ファイアウォ	仮想ファイアウォール機能の状態を表示します。「OK」は正常動作
	ール	していることを示します。「NG」は正常動作していないことを示し
		ます。仮想ファイアウォールを複数構築していて、いずれかの仮想
		ファイウォールが正常動作していない場合、「NG」と表示されます。
	クラスタ	冗長化機能の状態を表示します。「OK」は正常動作していることを
		示します。「NG」は正常動作していないことを示します。
自ホスト監視対	対象IPアドレス	接続中のSGが監視している装置の状態を表示します。「OK」は正
		常動作していることを示します。「NG」は正常動作していないこと
		を示します。
対向ホスト監視	見対象IPアドレス	対向のSGが監視している装置の状態を表示します。「OK」は正常
		動作していることを示します。「NG」は正常動作していないことを
		示します。

(3) [冗長化切替]ボタンをクリックします。

しばらくして画面上部の[画面を更新する]をクリックし、運用系が「現用」、待機系 が「待機」となっていることを確認します。切替途中では、[画面を更新する]をクリ ックしても「異常」と表示されることがございます。その場合は時間を少しあけて[画 面を更新する]をクリックします。[冗長化切替]ボタンをクリックした後、[画面を更 新する]をクリックせずに再度[冗長化切替]ボタンをクリックしても、冗長化切り替え は行われません。

また、冗長化切替が正常に行えない場合は、「広告パケット送信間隔(秒)」の設定値 を大きくするなどお試しください。



愛 SG3600LM Ver8.0.0 ます.com クリークテクト モニター 設定				
[ファイアウォール] Administrator ▼	状態表示			
▶ [] <u>2ァイアウォール</u> ▶ [] <u>サービス</u>	<u>サービス > 冗長化機能 > 状態表示</u> 画面を更新する	\supset	[~]/]	
▶ ₩ <u>ハッワーン</u> ▶ ① システム	■ 冗長化機能			
▶ 10 仮想ファイアウォール		2015/05	5/12 14:01:11	
 基本設定 第 2 2 2 	* ローカル:sg		1.0-0	
U <u>ナイムン</u> Uモートメンテナンス	リモート:sg	ローカル	リモート	
		現用	待機	
	VRRP VRID	000	50	
	圏元母 仮想IPアドレス(標準ファイアウォール)	200	100	
	内側: 192.168.1.70 外側: 192.168.2.70	0K 0K	:	
	eth6: 10.71.52.100 eth4 b: 10.71.51.100	OK OK	:	
	(仮想 IP アドレフ (ver1)			
	内側: 10.71.31.100	OK	-	
	97191: 10.71.32.100	UK		
	仮想IPアドレス(vsv1) 内側: 10,71,41,100	ОК		
	外側: 10.71.42.100 予備: 10.71.43.100	0K		
	エジュールファータフ	0		
	ファイアウォール	ОК	ОК	
	仮想ファイアウォール クラスタ	OK	OK	
	 自ホスト監視対象IPアドレス 192.168.1.1	ок		
		-	ОК	
	/L#elCV/m	J		

2.5. ルール設定の同期

冗長化構成構築後に、以下の手順で運用系、待機系のファイアウォールルールを同期し ておくことを推奨します。万が一のフェイルオーバ時に同じルールで、運用を続けること ができます。なお、運用中にルールの新規登録・変更をする場合も本手順で行います。

- (1) 運用系のManagement Consoleにて、ファイアウォールルールを登録・変更します。
- (2) 運用系のManagement Consoleにて、[ファイアウォール]画面の[ルール設定の同期]を クリックします。

 			
王二夕一 設定			
	ファイアウォール		
Administrator 👻	ファイアウォール [<u>ヘルブ]</u>		
 ▶ 7 2747ウォール ▶ 2 ± ť 2 ▶ 1 ± ť 2 ▶ 2 ± ť 2 ▶ 2 ± ź 25 4 ▶ 7 仮想ファイアウォール 基本設定 ▶ 5 4 2 2 ▶ 5 4 2 2 ▶ 1 ± 1 ± 2 2 	■ ルール設定 かんたん設定 [詳細設定]		
	■ 情報表示		
	■ ログ・アラート 表示 ダウンロード/アップロード		
	■ ライセンス 確認/登録		
	 ■ システムメンテナンス ソプトウェアアップデート パッグアップ・リストア ルール設定の同期 		

2.6. バックアップについて

設定変更のミスなど万が一に備え、バックアップを採取しておくことを推奨します。運用系、待機系、それぞれのManagement Consoleにて、[システム] >[バックアップ/リストア]画面で「システム基本情報」のバックアップを採取します。

バックアップデータのリストアは、待機系、運用系の順番で実行してください。

2.7. フェイルオーバ時のメール通報について

フェイルオーバ時に管理者宛にメール通報が可能です。運用系、待機系、それぞれのMa nagement Consoleの基本 ファイアウォールの[基本設定]画面にて設定されている「管理者 メールアドレス」宛てにメールが送付されます。設定するメールアドレスは基本ファイア ウォールから到達可能である必要があります。仮想ファイアウォールの[基本設定]画面にて 設定されている「管理者メールアドレス」宛てにメールは送付されません。

2.8. フェイルオーバ時のメールデータ移行について

SGのSMTPサーバ、POPサーバへ仮想IPでアクセスする運用の場合、フェイルオーバ時 にメールデータを待機系から運用系へ移行することが可能です。フェイルオーバ発生後、 待機系システムが復旧した時点で運用系へSSH接続を行い下記のコマンドを実行します。

\$ sudo /opt/nec/hasg/bin/backup_mspool.sh

backup_mspool.sh は、Management Console 用のポート番号を使用し待機系へ接続を 行い、待機系に残っているメールキュー、およびメールボックスを運用系へ移動します。 メールボックスについては単なる移動ではなく、待機系より移動したメールボックスの後 ろに運用系のメールボックスをマージします。rpc, admin, root, www-data のメールボッ クスは移行対象外となります。

2.9. 冗長化機能のログについて

運用系、待機系、それぞれのManagement Consoleにて、[システム] >[ログ管理]にて、 冗長化機能のログを参照可能です。動作などで疑問点がございましたら、本ログをダウン ロードしお問い合わせください。

2.10. 冗長化構成時の複数パッチ適用について

All Rights Reserved, Copyright(C) 2019 NEC Corporation

パッチ適用手順書に下記のような記載があり、複数パッチ適用時は、パッチ毎に冗長化 切り替えを行なう必要はございません。下記の該当パッケージは"適用対象の複数のパッ ケージ"と読み替えて実施ください。

- (1) 待機側のSG2に該当パッケージを適用します。
- (2) 待機側のSG2において、冗長化切替を行ないます。 (待機側と現用側が切り替わり、SG1が待機側となります)
- (3) 待機側となったSG1に該当パッケージを適用します。
- (4) 待機側となったSG1おいて、冗長化切替を行ないます。(待機側と現用側が切り替わり、元の状態になります)

※系切替を行なうため、システムが一時的に停止いたしますので、 業務に支障のない時間帯に実施してください。

2.11. 冗長化構成時の待機系追加について

冗長化構成時、現用系でのみ運用し、途中で待機系を追加する場合は下記の手順を実施 ください。パッチ適用時と同様の手順となります。

- (1) 現用系のSG1が運用している環境に待機系のSG2を追加し電源ON。
- (2) 待機系のSG2において、冗長化切替を行ないます。 (待機側と現用側が切り替わり、SG1が待機側となります)
- (3) 待機側となったSG1おいて、冗長化切替を行ないます。 (待機側と現用側が切り替わり、元の状態になります)
- ※系切替を行なうため、システムが一時的に停止いたしますので、 業務に支障のない時間帯に実施してください。

3. 注意事項

- 冗長化構成で、フェイルオーバ(運用系から待機系への切替)およびフェイルバック (待機系から運用系への切戻し)が発生した場合、基本ファイアウォールが保有して いるセッション(通信)情報は維持されますが、仮想ファイアウォールが保有してい るセッション(通信)情報は維持されません。
- 冗長化構成で、運用系と待機系のメールキュー、およびメールボックスは、手動で同期する必要があります(2.8節参照)。
- 運用系のSGにおいて、基本ファイアウォール、仮想ファイアウォールのいずれかで異常が検知された場合、フェイルオーバが発生します。
- 待機系で監視対象IPアドレスとの通信途絶が発生している場合、運用系でリソース異常が発生しても待機系に業務は引き継がれません。
- 冗長化を構成した後、および解除した後は必ず「かんたん設定」を実行してください。
 また、「かんたん設定」の中でインタフェースに関する設定が正しいことを確認してください。
- 本機能はIPv6には対応していません。

以上