

# **SG3600LM,SG3600LG,SG3600LJ v8.0**

## **InterSecVM/SG v4.0**

### **仮想ファイアウォール機能 説明書**

2016 年 5 月 4 版

# 目 次

1. はじめに .....	1
2. 機能概要 .....	2
3. 設定手順 .....	5
3.1 仮想ファイアウォールの作成 .....	5
3.2 仮想ファイアウォール管理者の作成 .....	8
3.3 仮想ファイアウォール管理者の利用 .....	10
3.4 基本設定 .....	10
3.5 仮想ファイアウォールの起動 .....	12
3.6 仮想ファイアウォールのルールの登録 .....	15
3.7 VMware vSphere の設定(InterSecVM/SG for VMware の場合) .....	15
4. その他機能 .....	24
4.1 インタフェース一覧 .....	24
5. 注意事項 .....	27

# 1. はじめに

本手順書は、SGシリーズの仮想ファイアウォール機能の設定手順書です。仮想ファイアウォール機能を使用する場合は本手順書を参考に設定を行ってください。

※本機能はSG3600LM、InterSecVM/SGでは標準のライセンスで使用可能な機能です。SG3600LG、SG3600LJでは、使用にマイナンバー対応ライセンスのご購入・登録が必要になります。使用する際は、マイナンバー対応ライセンスをご購入いただき、同梱の「SG3600マイナンバー対応ライセンス ご使用の手引き」にて登録手順及び注意事項をご確認ください。

## 2. 機能概要

- 仮想ファイアウォール機能は、1 台のアプライアンス上で複数のファイアウォールを実行することができます。
- 各仮想ファイアウォールに独立したファイアウォールルールを設定することができ、それぞれ管理者を分けることもできます。

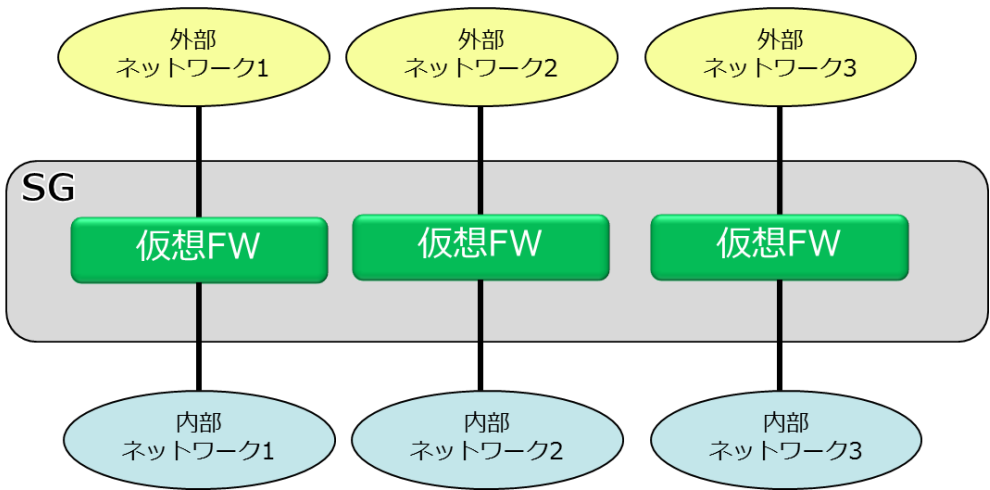


図 2-1 仮想ファイアウォール機能

仮想ファイアウォール機能では、以下の表 2-1 の機能を提供します。

表 2-1 仮想ファイアウォール機能の概要

No.	名称	説明															
1	仮想ファイアウォールの作成/更新/削除	システム管理者、運用管理者は、仮想ファイアウォールの作成/更新/削除を行うことができます。															
2	パケットフィルタリング	仮想ファイアウォール毎に、個別のネットワーク設定、ファイアウォールルールの登録/更新/削除を行い、流れるパケットを制御することができます。															
3	ログ機能	仮想ファイアウォール毎に、ファイアウォールより出力されるログを閲覧することができます。															
4	仮想ファイアウォール管理者	<p>システム管理者、運用管理者は、仮想ファイアウォール管理者の作成/更新/削除を行うことができます。</p> <p>仮想ファイアウォール管理者は、管理を許可されているファイアウォールのみ設定を行うことができます。</p> <p>Management Console で利用可能な、各管理者の設定可能範囲の違いを以下の表 2-2 に示します。</p> <table><tr><th colspan="3">表 2-2 管理者ごとの差異</th></tr><tr><th>管理者名</th><th>設定可能範囲</th><th>人数</th></tr><tr><td>システム管理者</td><td>すべての機能を設定可能</td><td>1</td></tr><tr><td>運用管理者</td><td>システム管理者が[システム-&gt;権限委譲]の画面より許可した機能のみ設定可能</td><td>1</td></tr><tr><td>仮想ファイアウォール管理者</td><td>仮想ファイアウォールに関する機能のみ設定可能</td><td>12 まで作成可</td></tr></table>	表 2-2 管理者ごとの差異			管理者名	設定可能範囲	人数	システム管理者	すべての機能を設定可能	1	運用管理者	システム管理者が[システム->権限委譲]の画面より許可した機能のみ設定可能	1	仮想ファイアウォール管理者	仮想ファイアウォールに関する機能のみ設定可能	12 まで作成可
表 2-2 管理者ごとの差異																	
管理者名	設定可能範囲	人数															
システム管理者	すべての機能を設定可能	1															
運用管理者	システム管理者が[システム->権限委譲]の画面より許可した機能のみ設定可能	1															
仮想ファイアウォール管理者	仮想ファイアウォールに関する機能のみ設定可能	12 まで作成可															

5	システムリソースの確認	CPU/メモリ使用状況やネットワークの使用状況、接続状況、経路状況をチェックすることができます。
6	冗長化機能	冗長化機能使用時に、仮想ファイアウォールの障害を検知して自動的にフェイルオーバーします。

仮想ファイアウォールを使用する場合のネットワーク構成例は以下の通りです。

VLAN を使用しない場合

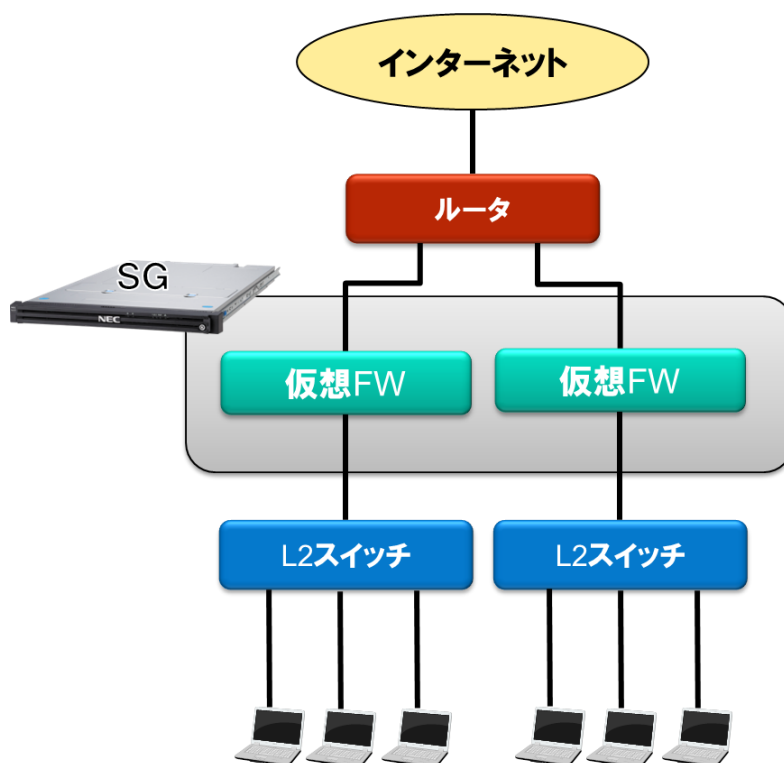


図 2-2 仮想ファイアウォールのネットワーク構成例(VLAN なし)

VLAN を使用する場合

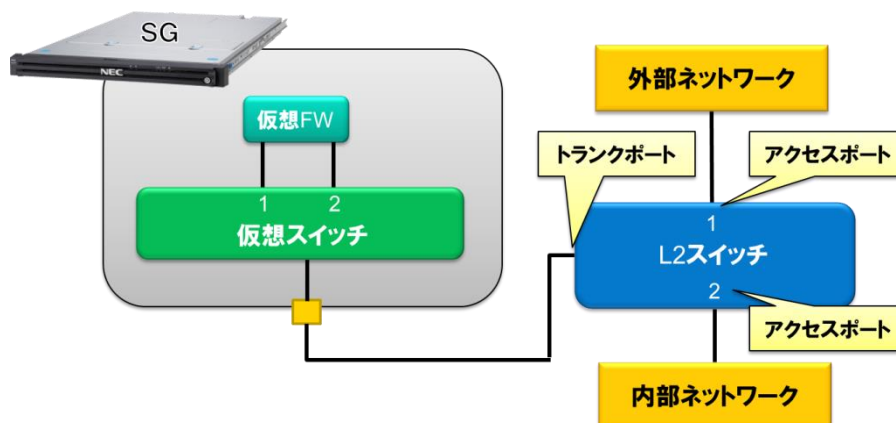
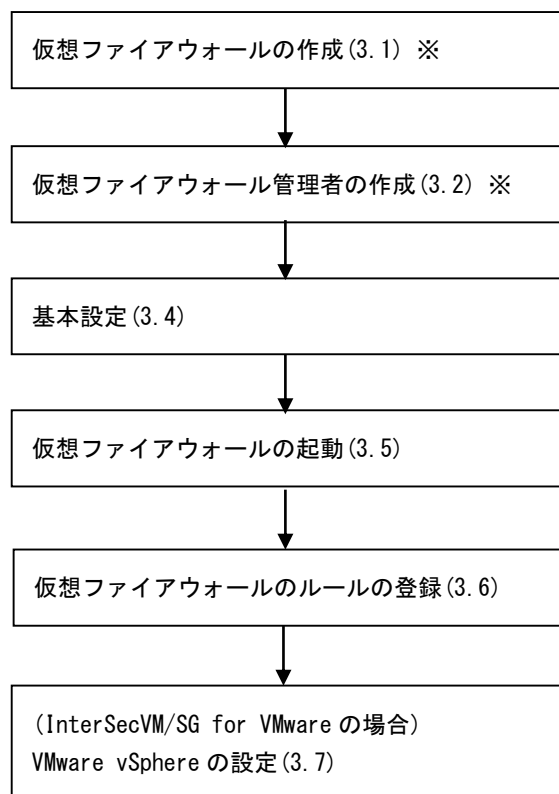


図 2-3 仮想ファイアウォールのネットワーク構成例(VLAN あり)

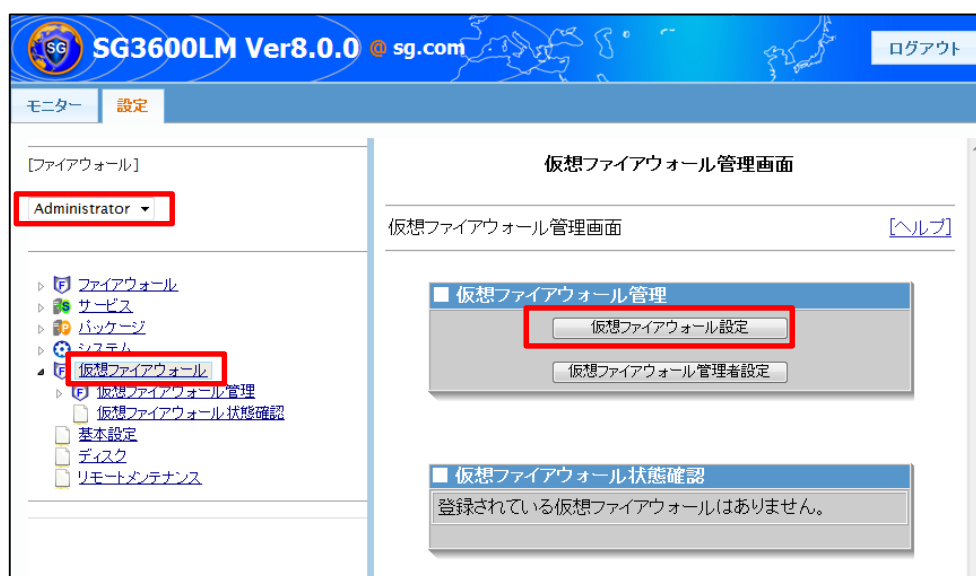
### 3. 設定手順

仮想ファイアウォール機能を使用するための設定方法について説明します。仮想ファイアウォール機能を使用するには、以下のフローに従って設定を行います。フロー中の※は、システム管理者、もしくは権限を与えられた運用管理者のみ設定可能な項目です。

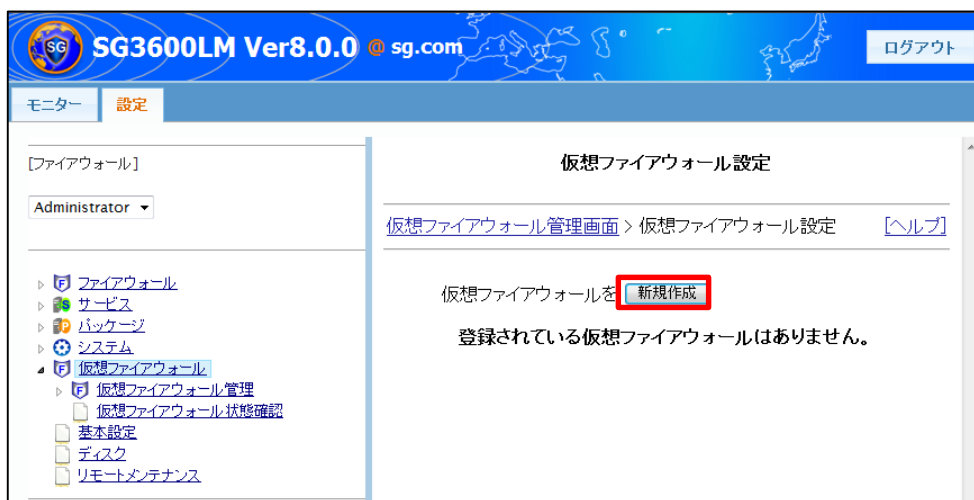


#### 3.1 仮想ファイアウォールの作成

- (1) システム管理者のアカウントで Management Console にログインします。
- (2) ツリーメニューの[仮想ファイアウォール]のリンクをクリックします。
- (3) [仮想ファイアウォール管理]の[仮想ファイアウォール設定]のボタンをクリックします。

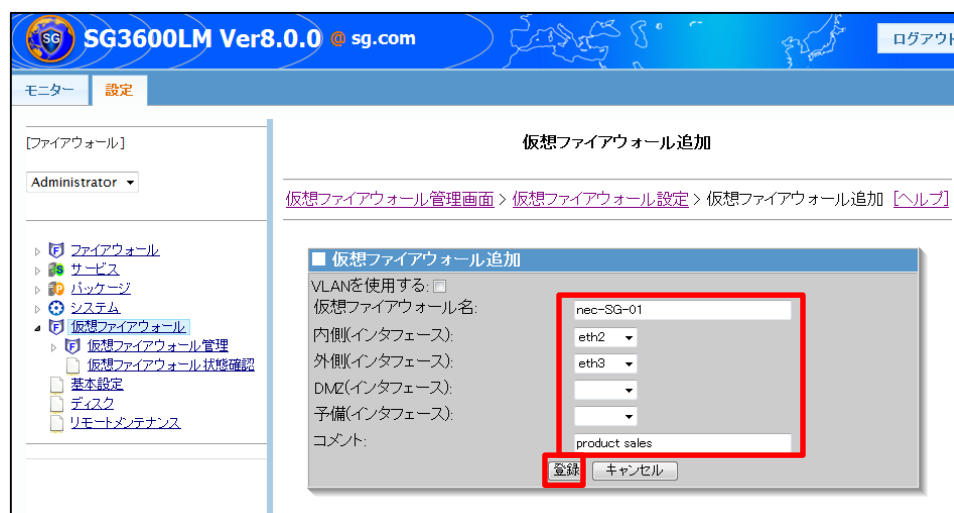


- (4) [新規作成]ボタンをクリックします。



(5) [仮想ファイアウォール追加]のテーブルの各項目に必要事項を記入し、[登録]ボタンをクリックします。

#### VLAN を使用しない場合



#### VLAN を使用する場合



各項目の説明は表 3-1 の通りです。



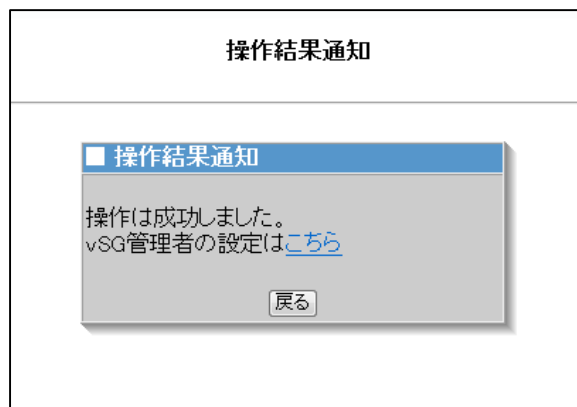
表 3-1 仮想ファイアウォール追加時の設定項目

項目	説明
VLAN を使用する	VLAN を使用するかどうかを選択します。 チェックの有無で、オン、オフの表示を切り替えます。 本項目は新規作成の際のみ変更可能であり、更新するためには、削除後の再作成が必要です。
仮想ファイアウォール名	仮想ファイアウォールの名称を入力します。 4 文字から 10 文字までの英数文字列、ハイフン(-)、アンダースコア(_)を受け付けます。 本項目を更新するためには、削除後の再作成が必要です。
インタフェース(注 1)	仮想ファイアウォールが使用するインタフェースを選択します。 使用可能なネットワークインタフェースのみ表示されます。 eth2 以降のインタフェースのみ選択可能で、内側、外側については入力が必須です。
VLAN ID	[VLAN を使用する]にチェックが入っている場合のみ入力でき、使用する VLAN ID を入力します。 入力できる VLAN ID は 0 から 4095 までの半角数字です。 内側、外側については入力が必須です。
コメント	仮想ファイアウォールについてのコメントを入力します(任意)。 「"」、「;」、「&」を除く 100 バイトまでの日本語英数字を受け付けます。 コメントは、仮想ファイアウォール管理者は確認できません。

(注 1)

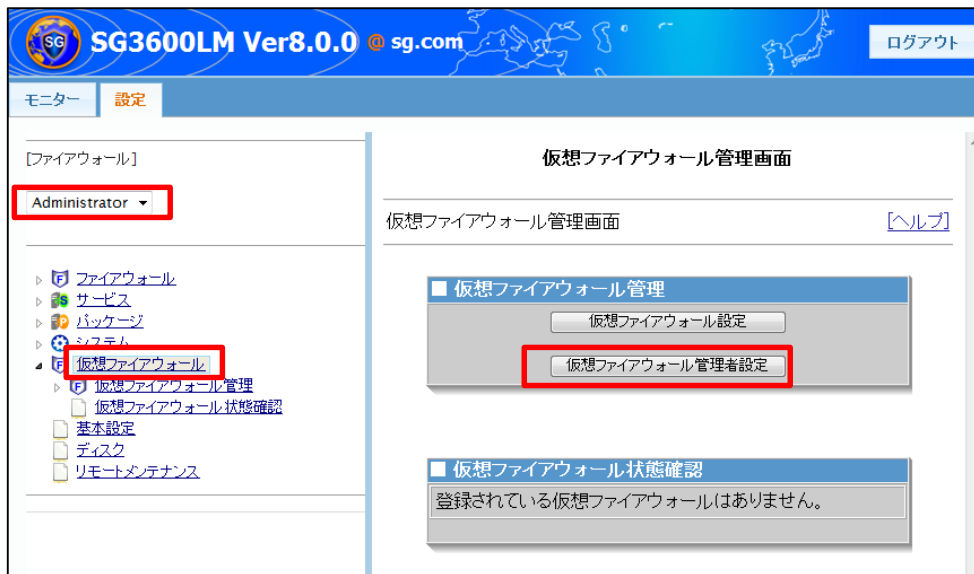
- リンクアグリゲーション機能を使用している場合は、bonding インタフェースが表示され、slave インタフェースは表示されません。
- ポートミラーリング機能を使用している場合は、監視ポートとして使用しているネットワークインタフェースが表示され、ミラーポート、標準ポートとして使用しているネットワークインタフェースは表示されません。
- [VLAN を使用する]にチェックが入っていない場合、他の仮想ファイアウォールで使用しているネットワークインタフェースは表示されません。
- [VLAN を使用する]にチェックが入っている場合、他の VLAN を使用していない仮想ファイアウォールで使用しているネットワークインタフェースは表示されません。
- [VLAN を使用する]にチェックが入っている場合、リンクアグリゲーション機能、ポートミラーリング機能で使用しているネットワークインタフェースは表示されません。

(6) 仮想ファイアウォールの作成に成功すると、下図のように表示されます。仮想ファイアウォール管理者の設定を行う場合は、[こちら]のリンクをクリックして、3.2 章の(3)へと進んでください。

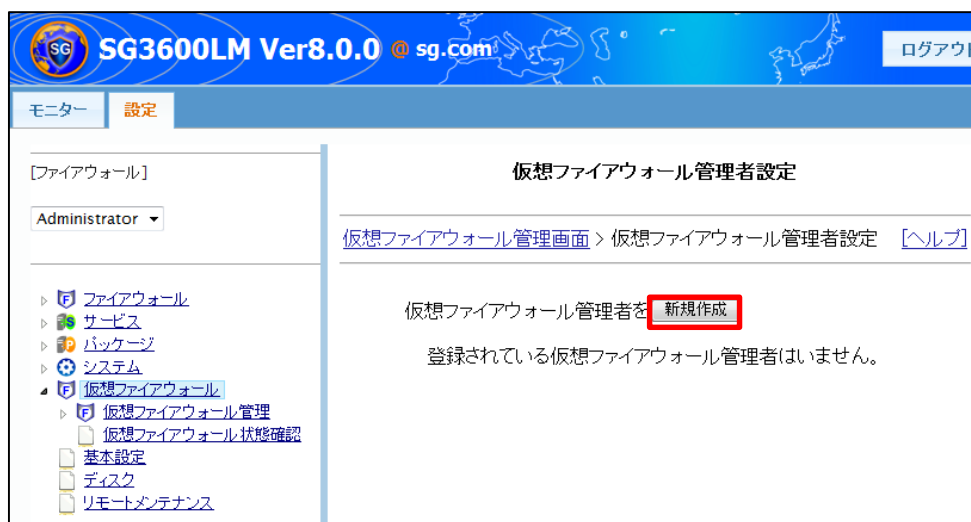


### 3.2 仮想ファイアウォール管理者の作成

- (1) ツリーメニューの[仮想ファイアウォール]のリンクをクリックします。
- (2) [仮想ファイアウォール管理]の[仮想ファイアウォール管理者設定]のボタンをクリックします。



- (3) [新規作成]ボタンをクリックします。



- (4) [仮想ファイアウォール追加]のテーブルの各項目に必要事項を記入し、[登録]ボタンをクリックします。



各項目の説明は表 3-2 の通りです。

表 3-2 仮想ファイアウォール追加時の設定項目

項目	説明
仮想ファイアウォール管理者名	仮想ファイアウォール管理者の名称を入力します。 4 文字から 16 文字までの英数文字列、ハイフン(-)、アンダースコア(_)を受け付けます。仮想ファイアウォール管理者の情報を更新する際は、本項目は変更できません。
パスワード	仮想ファイアウォール管理者が Management Console にログインする際のパスワードを入力します。 6 文字から 16 文字までの英数文字列、ハイフン(-)、アンダースコア(_)を受け付けます。 仮想ファイアウォール管理者の情報を更新する際は、本項目の入力は任意です(空欄の場合、パスワードは変更されません)。
パスワード(確認用)	「パスワード」エリアに入力されたパスワードに誤りがないかを確認するため、パスワードを再入力します。
管理する仮想ファイアウォール名	作成済の仮想ファイアウォールの一覧から、仮想ファイアウォール管理者が管理する仮想ファイアウォールを選択します(複数選択可、任意)。

(5) 仮想ファイアウォール管理者の作成に成功すると、下図のように表示されます。



### 3.3 仮想ファイアウォール管理者の利用

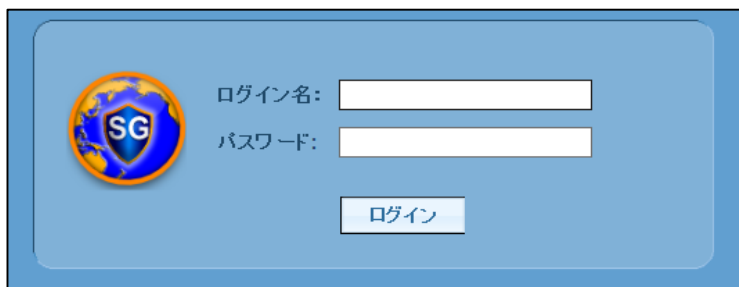
本章より、個々の仮想ファイアウォールの設定を行います。

- システム管理者にて設定を行う場合、3.4 節にお進みください。
- 運用管理者にて設定を行う場合、[システム > 権限委譲]のヘルプをご参照ください。
- 仮想ファイアウォール管理者にて設定を行う場合、本章をご確認ください。

- (1) ツリーメニューの[システム]のリンクをクリックし、[権限委譲]をクリックします。
- (2) 各項目を入力し、[設定]ボタンをクリックします。



- (3) 「https://[IP アドレス]:[ポート番号]」にアクセスします。
  - [IP アドレス]は、基本設定にて、eth0 に設定した IP アドレスをご指定ください。
  - [ポート番号]は、(2)で設定したポート番号をご指定ください。
  - (2)で、セキュリティモードを「レベル 1(パスワード)」に指定した場合は、https ではなく、http にてアクセスしてください。
- (4) 3.3 節で設定した仮想ファイアウォール管理者の「仮想ファイアウォール管理者名」を「ログイン名」に入力し、「パスワード」を入力した上で、[ログイン]をクリックします。



- (5) 正しく設定が行われていれば、仮想ファイアウォール管理者でログインできます。

### 3.4 基本設定

- (1) ツリーメニュー上部のプルダウンから作成した仮想ファイアウォール名(ここでは[nec-SG-01])を選択します。
- (2) ツリーメニューの[基本設定]のリンクをクリックします。

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]  
nec-SG-01

基本設定 (nec-SG-01) ヘルプ

基本設定 (nec-SG-01)

操作	設定項目	値
-	ホスト名 (FQDN)	sg.com
-	内側 (eth2)	IPアドレス ネットマスク MTU値 VLAN ID (任意)
-	外側 (eth3)	
-	DMZ (-)	
-	予備 (-)	
-	デフォルトゲートウェイ	
追加	静的ルーティング	1 IPアドレス ネットマスク ゲートウェイ インタフェース 自動
追加	ネームサーバ	1
-	管理者メールアドレス	
-	アドレス変換(NAT/NAPT)	無効
-	操作可能ホスト	

※本項目は、設定後に仮想ファイアウォールの再起動が必要です。

設定 元に戻す

(3) [基本設定]のテーブルの各項目に必要な事項を記入し、[設定]ボタンをクリックします。

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]  
nec-SG-01

基本設定 (nec-SG-01) ヘルプ

基本設定 (nec-SG-01)

操作	設定項目	値
-	ホスト名 (FQDN)	sg.com
-	内側 (eth2)	192.168.2.245 255.255.255.0 1500
-	外側 (eth3)	192.168.3.245 255.255.255.0 1500
-	DMZ (-)	
-	予備 (-)	
-	デフォルトゲートウェイ	192.168.2.254
追加	静的ルーティング	1 IPアドレス ネットマスク ゲートウェイ インタフェース 自動
追加	ネームサーバ	1
-	管理者メールアドレス	sg@sg
-	アドレス変換(NAT/NAPT)	無効
-	操作可能ホスト	192.168.2.1

※本項目は、設定後に仮想ファイアウォールの再起動が必要です。

設定 元に戻す

各項目の説明は表 3-3 の通りです。

表 3-3 基本設定画面の設定項目

項目	説明
ホスト名 (FQDN)	ホスト名が表示されます。 表示のみで編集することはできません。
インタフェース (必須項目) (IP アドレス/ネットマスク /MTU 値)	各インタフェースの IPv4 アドレス、ネットマスクおよび MTU 値を入力します。 内側と外側インタフェースの設定は必須ですが、その他のインタフェースの設定は任意です。
デフォルトゲートウェイ (設定必須)	デフォルトゲートウェイの IP アドレスを入力します。 1 つの IP アドレスのみ設定できます。

静的ルーティング (IP アドレス/ネットマスク/ゲートウェイ)	宛先アドレスとネットマスクおよびゲートウェイの組み合わせを指定します。
ネームサーバ(IP アドレス)	ネームサーバの設定が表示されます。 ホスト側の設定と同じになります。表示のみで編集することはできません。
管理者メールアドレス (設定必須)	1つのメールアドレスのみ設定できます。
アドレス変換(NAT/NAPT)	仮想ファイアウォールでアドレス変換(NAT/NAPT)を行いたい場合は有効を選択します。
操作可能ホスト	Management Console を操作することができるホスト(管理クライアント)の IP アドレスを指定します。仮想ファイアウォールを起動している状態で、この項目を変更した場合は、設定後に仮想ファイアウォールを再起動する必要があります。  設定後は、「https://[仮想ファイアウォールに設定されている IP アドレス]:18800」のアドレスよりログインを行うことが可能になります。

(4) 基本設定に成功したら、下図のように表示されます。

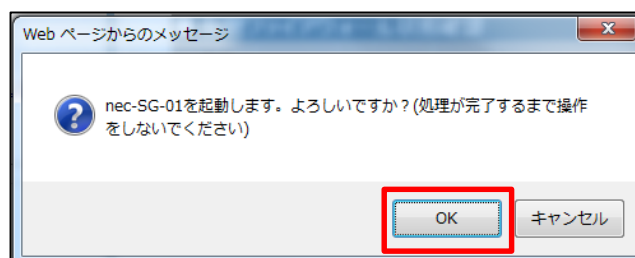


### 3.5 仮想ファイアウォールの起動

- (1) ツリーメニューの[仮想ファイアウォール]のリンクをクリックします。
- (2) [仮想ファイアウォール状態確認]テーブルから、起動する仮想ファイアウォール(この例では nec-SG-01)の[起動]ボタンをクリックします。



- (3) 下図のようなダイアログボックスが表示されたら、[OK]ボタンをクリックします。[OK]ボタンをクリックした後、(4)の画面が表示されるまで操作をしないでください。



- (4) 仮想ファイアウォールの起動に成功したら、下図のように表示されます。



※基本設定を完了していない場合、仮想ファイアウォールの起動に失敗します。

- (5) 元の画面に戻ると、下図のように起動した仮想ファイアウォールの[現在の状態]が[起動中]であることが確認できます。

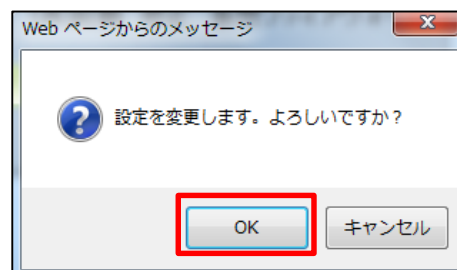


- (6) OS 起動時に仮想ファイアウォールを起動したい場合は、[仮想ファイアウォール状態確認]テーブルで、対象となる仮想ファイアウォールの[OS 起動時の状態]のプルダウンを[停止]から[起動]に変更し、[設定]ボタンをクリックします。



※基本設定を完了していない場合、仮想ファイアウォールの[OS 起動時の状態]を[起動]に変更しないでください。

(7) 下図のようなダイアログボックスが表示されたら、[OK]ボタンをクリックします。



(8) OS 起動時の状態の変更に成功すると、下図のように表示されます。



(9) 元の画面に戻ると、下図のように設定を変更した仮想ファイアウォールの[OS 起動時の状態]が[起動]であることが確認できます。





### 3.6 仮想ファイアウォールのルールの登録

仮想ファイアウォールルールの登録方法は、[詳細設定]画面のヘルプ画面をご参照ください。



### 3.7 VMware vSphere の設定(InterSecVM/SG for VMware の場合)

本節では、InterSecVM/SG for VMware をご利用の方のみ必要な VMware vSphere の設定方法について述べます。

#### 3.7.1. 無差別モードの設定

仮想ファイアウォールで使用するネットワークインタフェースと接続している仮想スイッチのポートに対して、無差別モードの設定を行う必要があります。

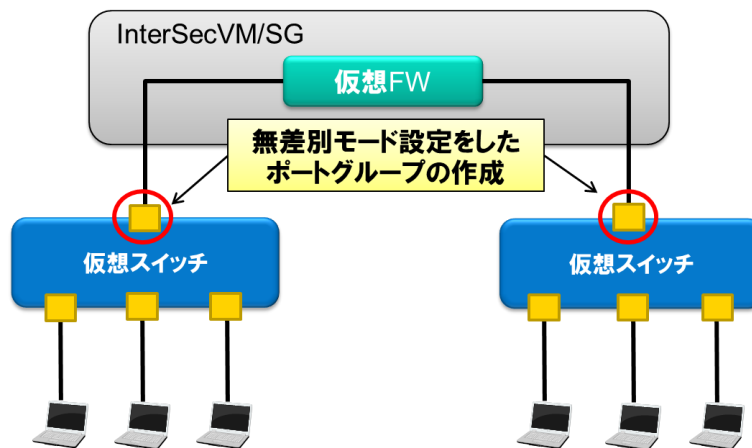


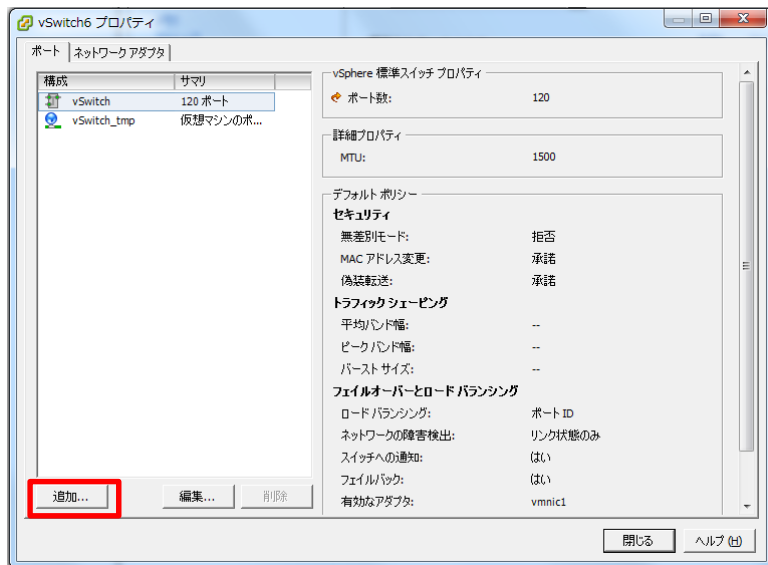
図 3-1 仮想スイッチに対する無差別モードの設定

以下では、仮想スイッチにおける無差別モードの設定方法を述べます。

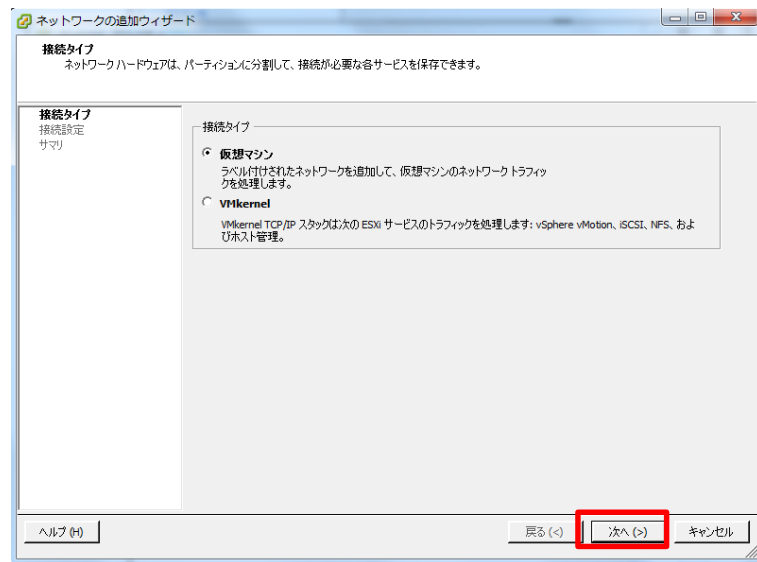
- (1) ESXi をインストールしているマシンの IP アドレスを選択します。
- (2) [構成]タブをクリックします。
- (3) [ネットワーク]をクリックします。
- (4) 仮想ファイアウォールで使用する仮想スイッチの[プロパティ]をクリックします。



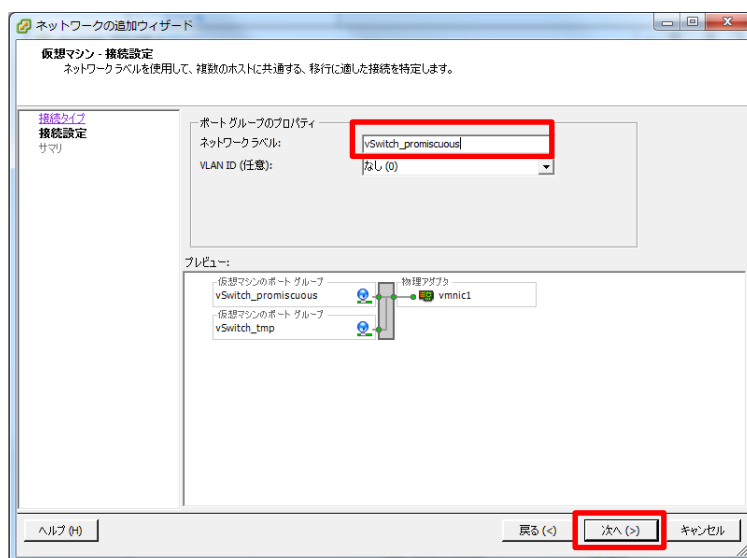
- (5) 新たにポートグループを追加する場合は[追加]ボタンをクリックし、既存のポートグループの設定を変更する場合は、対象とするポートグループを選択した上で[編集]をクリックします。以下の説明では[追加]ボタンを押下した場合の設定方法について述べます。



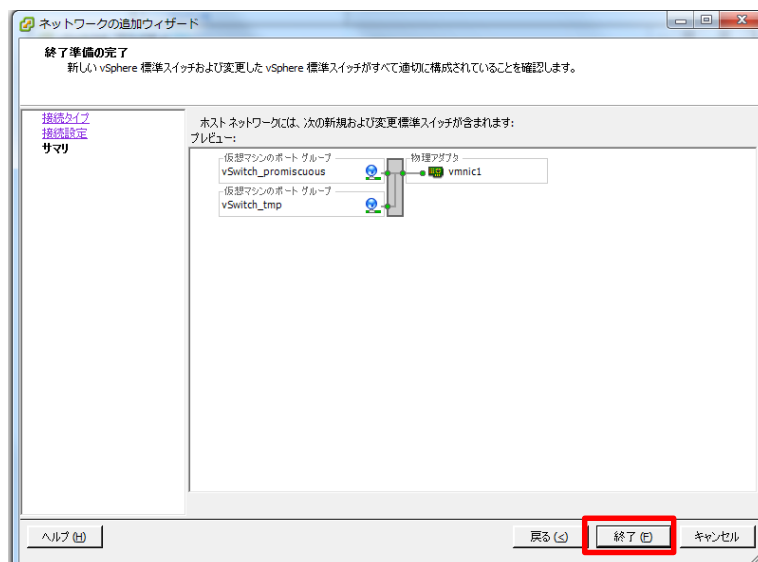
(6) [次へ]をクリックします。



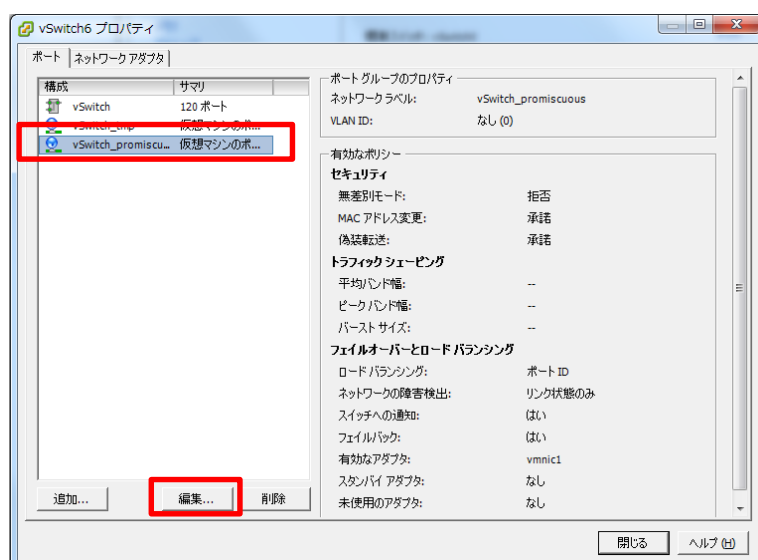
(7) ネットワークラベルを入力し、[次へ]をクリックします。



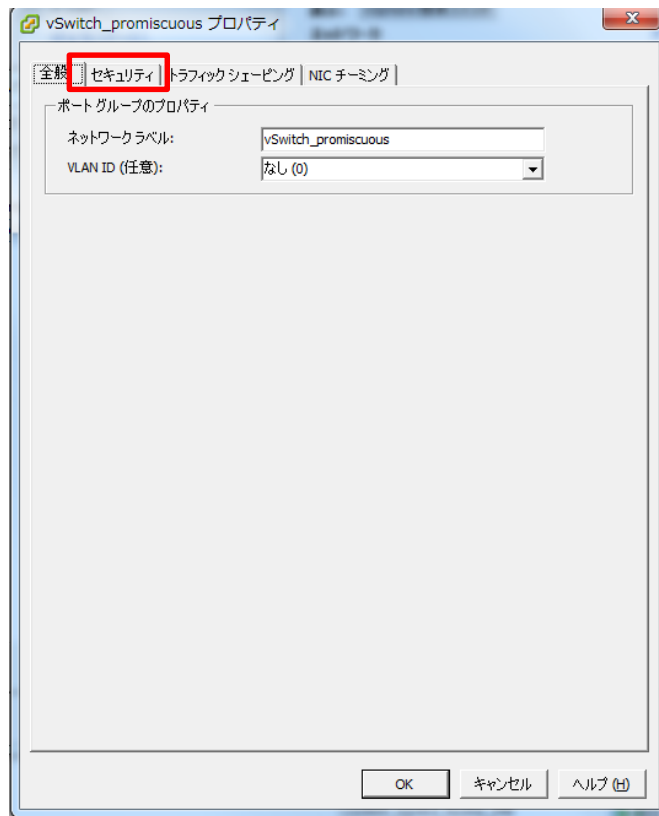
(8) 設定内容を確認し、[終了]をクリックします。



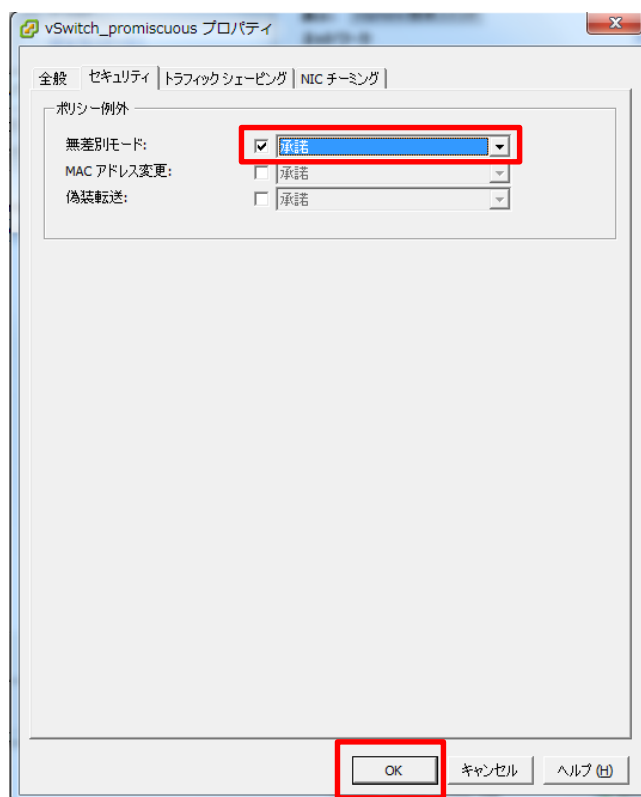
(9) 作成したポートグループを選択し、[編集]をクリックします。



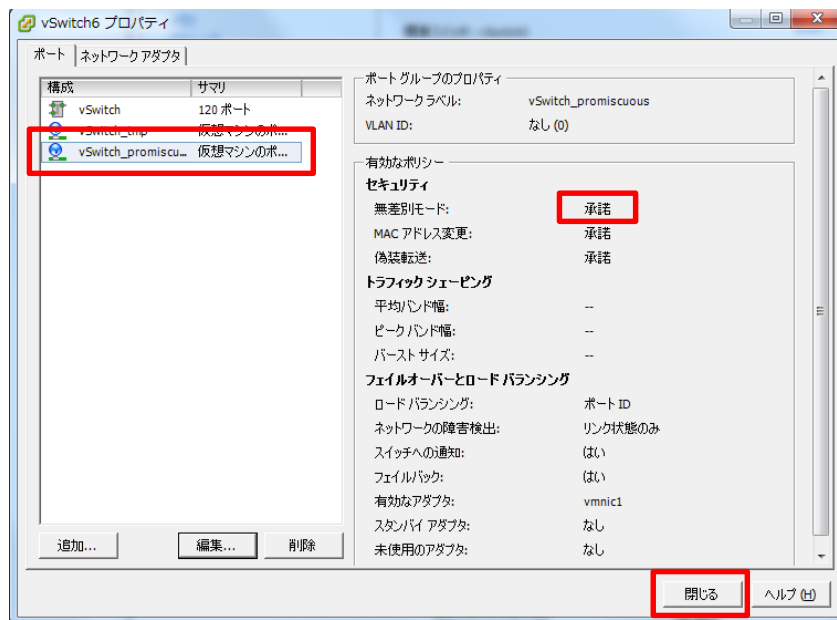
(10) [セキュリティ]タブをクリックします。



(11) [無差別モード]のチェックボックスにチェックを入れ、プルダウンから[承諾]を選択し、[OK]をクリックする。



(12) 作成したポートグループの[無差別モード]が[承諾]になっていることを確認し、[閉じる]をクリックする。



### 3.7.2. VLAN の設定

仮想ファイアウォールで VLAN を使用する場合、仮想ファイアウォールの VLAN 設定(3.1 節参照)に加え、仮想スイッチにも VLAN の設定をする必要があります。仮想スイッチに対する設定としては、内側と外側のネットワークなどと接続するポート(アクセスポート)と、SG と接続するポート(トランクポート)に対する設定が必要になります(図 2-3 参照)。

以下では、仮想スイッチに対するアクセスポート及びトランクポートの設定方法を述べます。

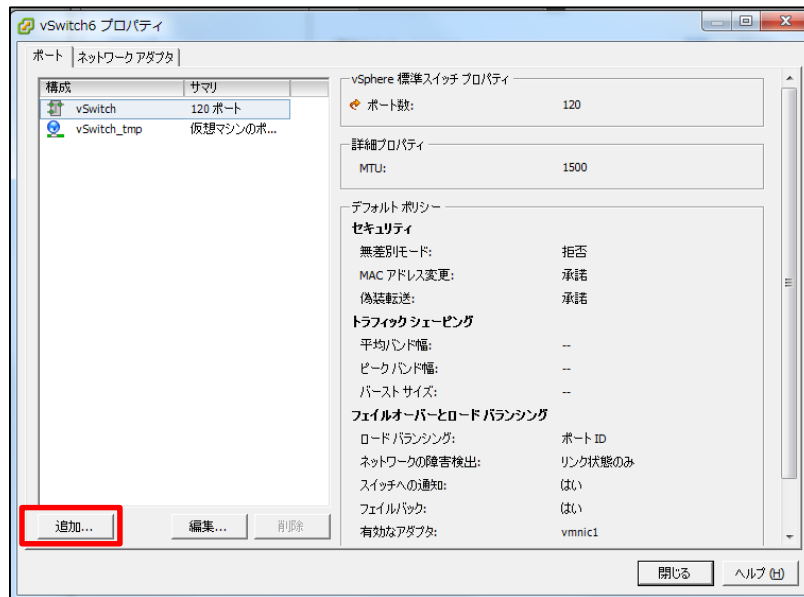
#### アクセスポートの設定

- (1) VMware vSphere をインストールしているマシンの IP アドレスを選択します。
- (2) [構成]タブをクリックします。
- (3) [ネットワーク]をクリックします。
- (4) 仮想ファイアウォールで使用する仮想スイッチの[プロパティ]をクリックします。

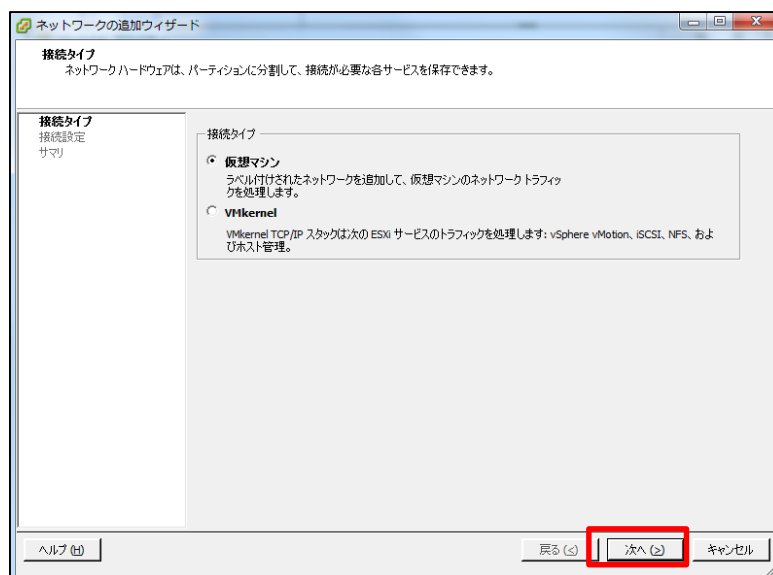


- (5) 新たにポートグループを追加する場合は[追加]ボタンをクリックし、既存のポートグループの設定を変更

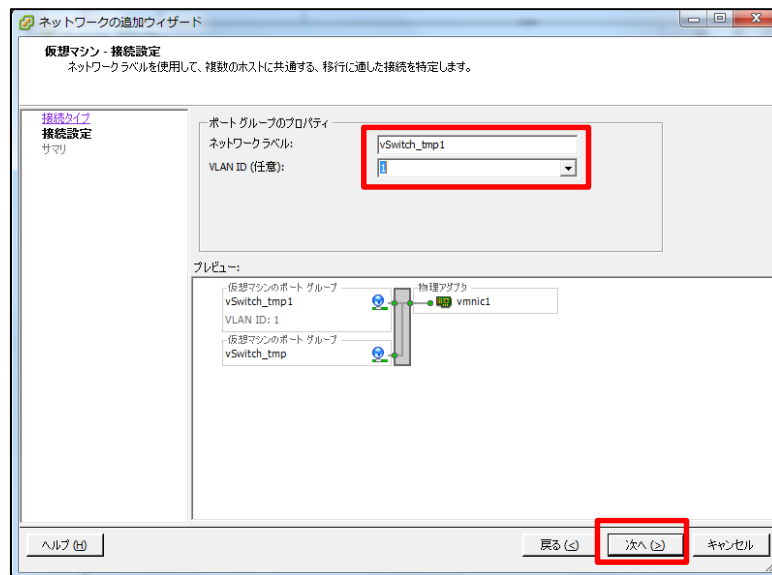
する場合は、対象とするポートグループを選択した上で[編集]をクリックします。以下の説明では[追加]ボタンを押下した場合の設定方法について述べます。



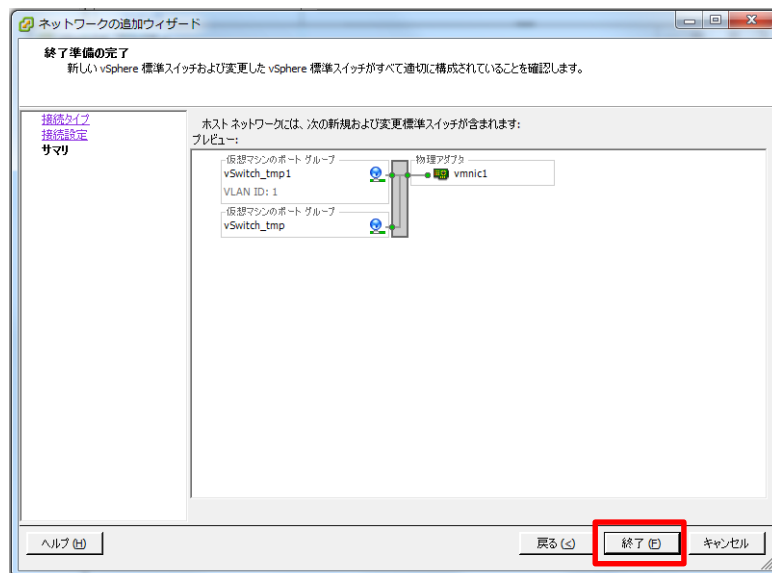
(6) [次へ]をクリックします。



(7) ネットワークラベルを入力し、ポートグループに設定する VLAN ID を入力します。プルダウンになっていますが、直接入力することも可能です。入力が終わりましたら、[次へ]をクリックします。



(8) 設定内容を確認し、[終了]をクリックします。

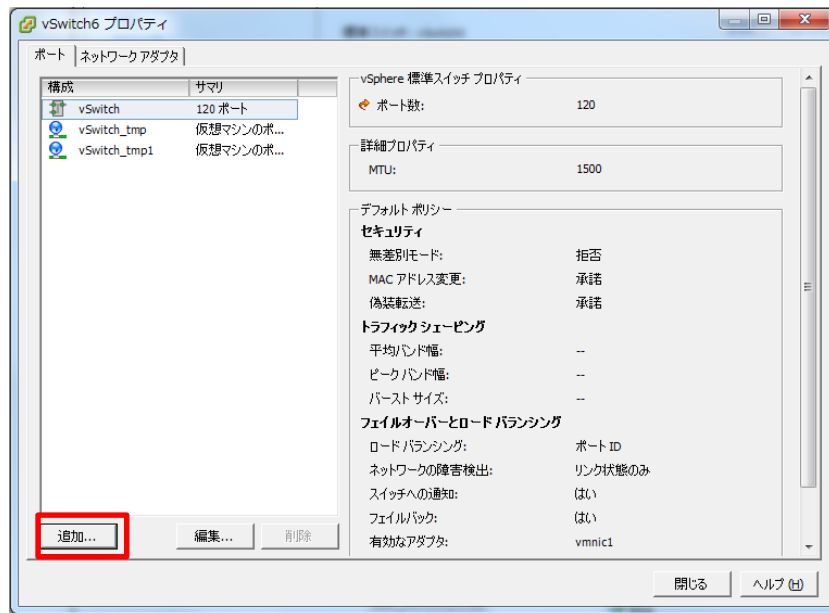


## トランクポートの設定

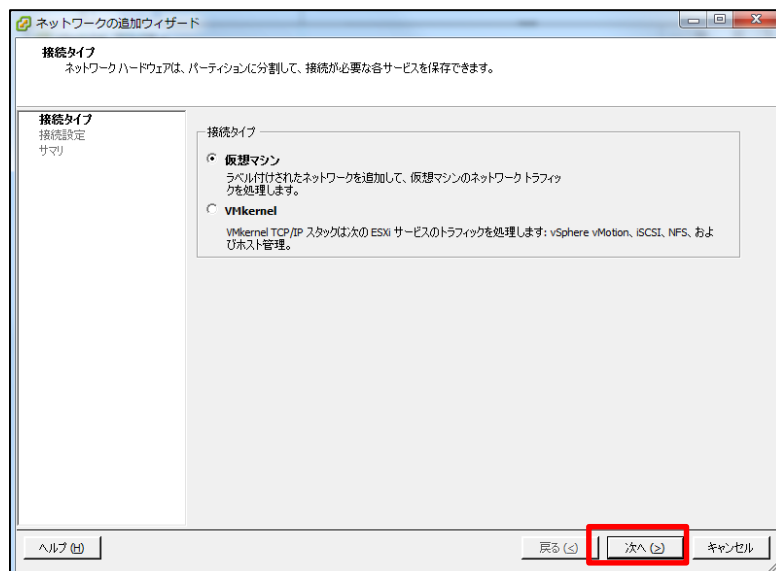
(9) 本節の(1)～(4)の手順に沿って進めます。

(10) 新たにポートグループを追加する場合は[追加]ボタンをクリックし、既存のポートグループの設定を変更する場合は、対象とするポートグループを選択した上で[編集]ボタンをクリックします。以下の説明では[追加]ボタンを押下した場合の設定方法について述べます。

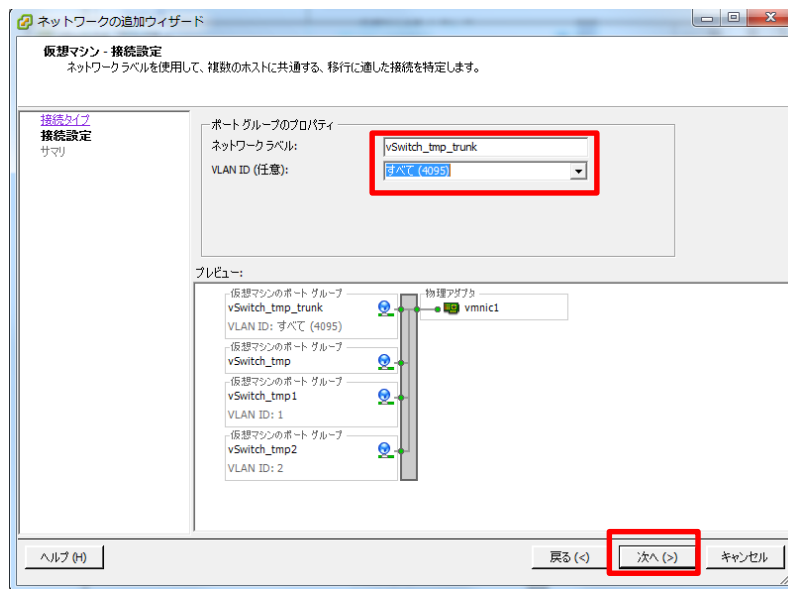




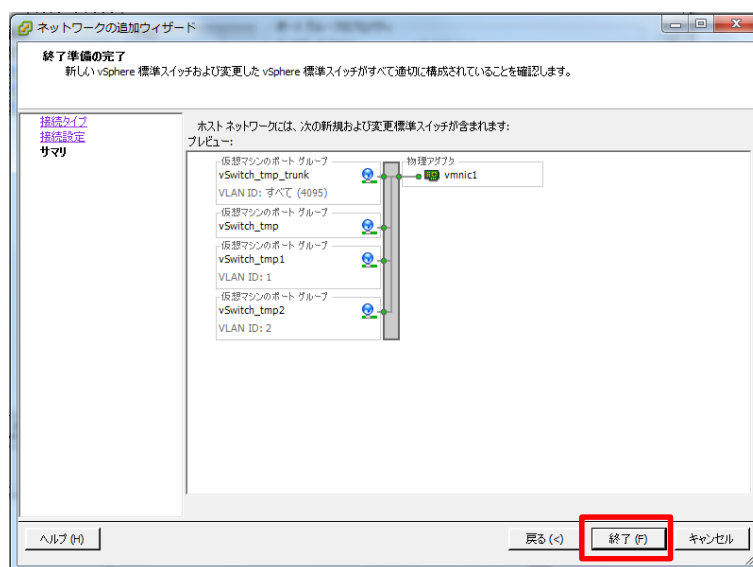
(11) [次へ]をクリックします。



(12) ネットワークラベルを入力し、VLAN ID に「すべて(4095)」を入力します。入力が終わりましたら、[次へ]をクリックします。



(13) 設定内容を確認し、[終了]をクリックします。

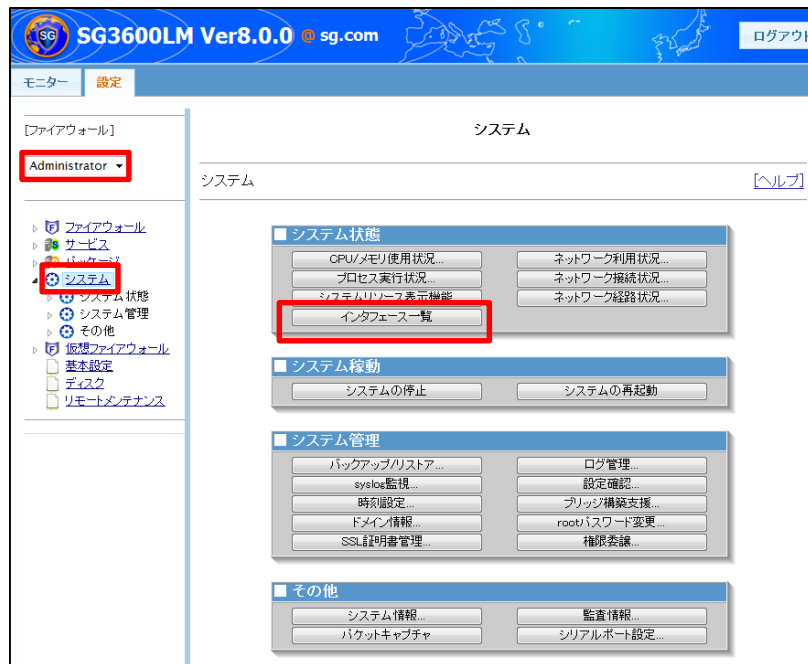


## 4. その他機能

### 4.1 インタフェース一覧

仮想ファイアウォール機能で使用しているネットワークインタフェースを Management Console から確認できます。

- (1) ツリーメニュー上部のプルダウンから[Administrator]を選択します。
- (2) ツリーメニューの[システム]のリンクをクリックします。
- (3) [システム状態]テーブルの[インタフェース一覧]ボタンをクリックします。



- (4) [インターフェース一覧]テーブルの[仮想ファイアウォール]の列で、ネットワークインターフェースが仮想ファイアウォールで現在使用中であるか、使用していない場合は使用できるかを確認できます。

インターフェース	状態	仮想ファイアウォール	リンクアグリゲーション	ポートミラーリング
eth0	UP	x	x	x
eth1	UP	x	x	x
eth2	UP	nec-SG-01	x	○
eth3	UP	nec-SG-01	x	○
eth4	UP	○(VLAN:x)	eth4_b	x
eth5	UP	○(VLAN:x)	eth4_b	x
eth6	UP	○	○	○
eth7	UP	○	○	○
eth8	UP	○	○	○
eth9	UP	nec-SG-02,nec-SG-03	x	x

共通 ○使用可能 ×使用不可  
ポートミラーリング: (ミラー)ミラーポート (監視)監視ポート

各項目の説明は表 4-1 の通りです。

表 4-1 インターフェース一覧の項目の概要

項目	説明
インターフェース	作成した物理ネットワークインターフェース、及び bonding インターフェースを表示します。
状態	ネットワークインターフェースが起動している場合は Up、停止している場合は Down、状態が不明な場合は UNKNOWN と表示します。
仮想ファイアウォール	ネットワークインターフェースを仮想ファイアウォールで使用している場合、対応する仮想ファイアウォール名を表示します。 1つのネットワークインターフェースを、VLAN を使用した複数の仮想ファイアウォールで使用している場合は、カンマ区切りで表示する。 VLAN を使用する仮想ファイアウォールでは使用できず、VLAN を使用しない仮想ファイアウォールでは使

	用できる場合は、「○(VLAN:x)」と表示する。
リンクアグリゲーション	ネットワークインタフェースを slave インタフェースとして登録している場合、対応する bonding インタフェース名を表示します。
ポートミラーリング	ネットワークインタフェースをポートミラーリング機能で使用している場合、対応する Open vSwitch 名を表示します。 監視ポートには(監視)、ミラーポートには(ミラー)が、Open vSwitch 名の後ろに付きます。

## 5. 注意事項

- 仮想ファイアウォールでは IPv6 アドレスを設定できません。
- 仮想ファイアウォールでは、メールサーバなどの各種サーバ機能を使用できません。
- 仮想ファイアウォールで使用しているインターフェースでは、ブリッジ接続は利用できません。
- Management Console を、ブラウザの複数のタブもしくはウィンドウで開かないでください。
- VLAN を使用している仮想ファイアウォールの通信速度は、500Mbps 程度となります。
- 「InterSecVM/SG for Hyper-v」では、VLAN を使用した仮想ファイアウォール機能は未サポートとなります。

以上