

SG3600LM、SG3600LG、SG3600LJ

SG v8.2

ポートミラーリング機能 説明書

NEC
2016 年 6 月 1 版

目次

1. はじめに.....	1
1.1 本書について	1
1.2 用語説明	1
1.3 機能概要	1
2. 使用方法.....	3
2.1 設定の流れ.....	3
2.2 画面での確認	3
3. 仕様.....	6
3.1 コマンド	6
4. 注意・制限事項.....	7

1. はじめに

1.1 本書について

本手順書は、SG シリーズのポートミラーリング機能の設定手順書です。

1.2 用語説明

本書で使用するポートミラーリング機能に関する用語を表 1.2-1 に示します。

表 1.2-1 ポートミラーリングの用語説明

用語	説明
監視ポート	監視対象であり、トラフィックのコピー元となるポート。
ミラーポート	トラフィックのコピー先となるポート。
標準ポート	監視ポートと通信を行うポート。監視ポートと標準ポートの間を流れるトラフィックを、ミラーポートにコピーすることができます。

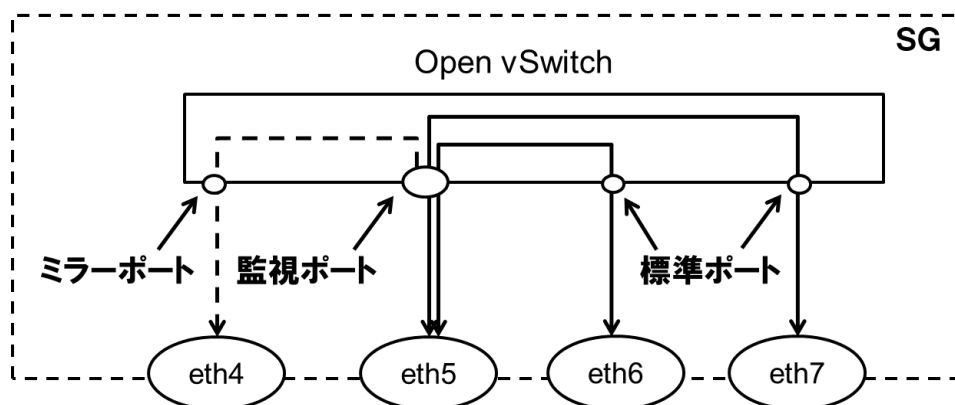


図 1.2-1 ポートミラーリング機能使用時のネットワーク構成

図 1.2-1 において、eth4 がミラーポート、eth5 が監視ポート、eth6 と eth7 が標準ポートです。そのため、eth5-eth6 間、eth5-eth7 間を流れるトラフィックを eth4 にコピーすることが可能です。

1.3 機能概要

ポートミラーリング機能は、あるインターフェースが送受信するトラフィックを、別のインターフェースにコピーする技術です。コピーしたトラフィックを、ミラーポートに接続した外部装置で受信することで、トラフィックの監視を行うことができます。本製品では、オープンソースの仮想スイッチソフトウェア「Open vSwitch」を用いてポートミラーリングを行います。仮想スイッチを用いてポートミラーリングを行うためには、通信を行う物理ネットワークインターフェース(標準ポート)とポートミラーリングしたトラフィックを流す物理ネットワークインターフェース(ミラーポート)を仮想スイッチのポートに登録し、ポートミラーリングの設定を行います。本製品では、監視ポートと標準ポート間を流れるトラフィックをミラーポートに対して出力することができます。図 1.3-1 は、本機能を使用した場合のネットワーク構成例を表しています。

※SG 宛に送信されたトラフィック、SG から送信されるトラフィックをミラーリングすることはできません。例えば、SG の Management Console にアクセスした際や、Web キャッシュサーバを介した通信を行った際のトラフィックをミラーリングすることはできません。

※ミラーポートに対して、IP アドレスを割り当てることはできません。

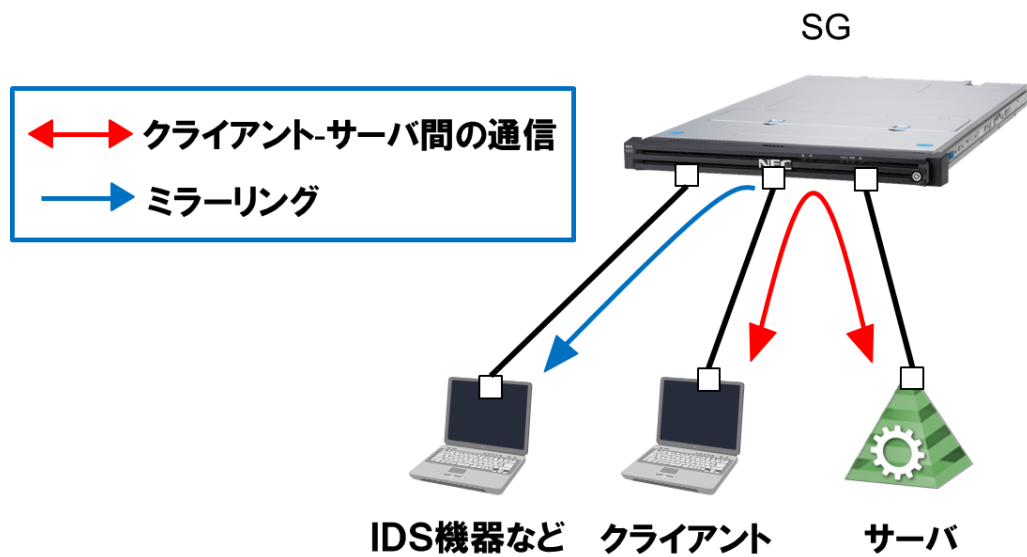


図 1.3-1 ポートミラーリング使用時のネットワーク構成例

2. 使用方法

2.1 設定の流れ

ポートミラーリング機能を利用するための設定方法について説明します。本機能はコマンドラインかつ root ユーザでのみ設定が可能です。以下の流れで設定を行います。

本機能では、1 つの監視ポートに対して、ミラーポートを 2 つまで設定することが可能です。ポートミラーリング設定は sg_mirror コマンドの --add オプションを使用します。eth0 以降の全てのネットワークインタフェースを監視ポート、標準ポートに指定できますが、eth0、eth1 をミラーポートに指定することはできません。sg_mirror コマンドの仕様は 3.1 章をご参照ください。

下記は、eth0、eth1 間で通信をする場合に、eth0 を監視ポート、eth2 をミラーポートに設定して、eth0 の通信を eth2 で監視する場合のコマンドの実行例です。

```
/opt/necfws/bin/sg_mirror --add --m=eth2 --s=eth0 --d=eth1
```

また、すでに 1 つの監視ポートに対してミラーポートを 1 つ設定している際に、同一の監視ポートに対して別のミラーポートを追加で設定することも可能です。下記は、eth0:監視ポート、eth1:標準ポート、eth2:ミラーポートというポートミラーリング設定をしている際に、追加で eth0 のトラフィックを eth3 にミラーリングする場合のコマンドの実行例です。

```
/opt/necfws/bin/sg_mirror --add --m=eth3 --s=eth0 --d=eth1
```

本機能は仮想ファイアウォール機能と併用することが可能です。すでに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に対して、本機能の設定を行う場合、--s オプションでは仮想ファイアウォールで使用しているインタフェースを指定し、--m オプションでは仮想ファイアウォールで使用していないインタフェースを指定してください。下記は、vsg1 という名前の仮想ファイアウォールが eth4 と eth5 を使用している際に、eth4 の通信を eth6 にミラーリングする場合のコマンドの例です。

```
/opt/necfws/bin/sg_mirror --add --m=eth6 --s=eth4
```

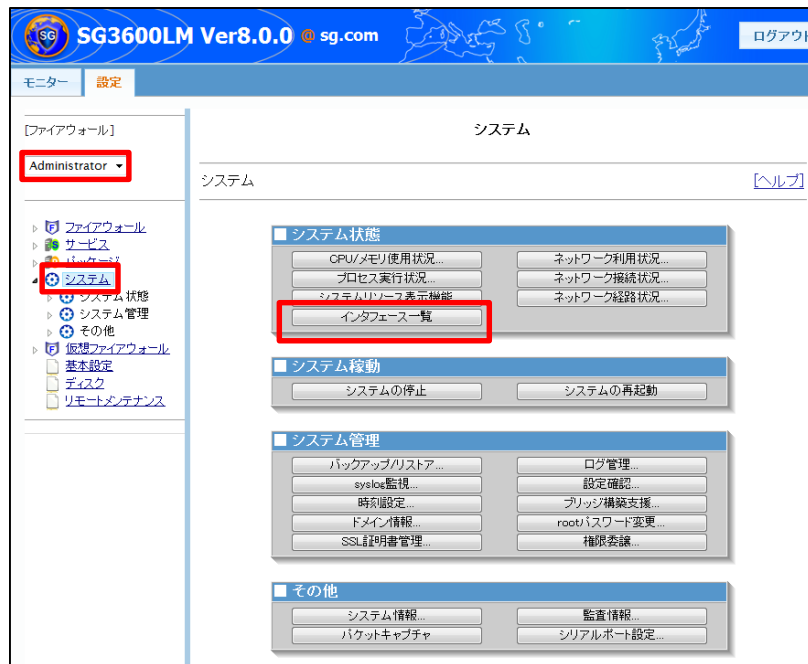
本機能では、下記の条件を満たすネットワークインタフェースを使用することができません。

- bonding インタフェースである
- slave インタフェースである
- 他のポートミラーリング機能で使用している
- VLAN ありの仮想ファイアウォールで使用している

2.2 画面での確認

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を Management Console から確認できます。

- (1) システム管理者で Management Console にログインします。
- (2) ツリーメニュー上部のプルダウンから[Administrator]を選択します。
- (3) ツリーメニューの[システム]のリンクをクリックします。
- (4) [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。



- (5) [インターフェース一覧]テーブルの[ポートミラーリング]の列で、ネットワークインタフェースがポートミラーリング機能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	o
eth3	UP	nec-SG-01	x	o
eth4	UP	o (VLAN: x)	eth4_b	x
eth5	UP	o (VLAN: x)	eth4_b	x
eth6	UP	o	o	o
eth7	UP	o	o	o
eth8	UP	o	o	o
eth9	UP	nec-SG-02,nec-SG-03	x	x

共通 o 使用可能 x 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 2.2-1 の通りです。

表 2.2-1 インターフェース一覧の項目の概要

項目	説明
インタフェース	作成した物理ネットワークインタフェース、及び bonding インタフェースを表示します。
状態	ネットワークインタ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します。 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)」と表示します。
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、対応する仮想スイッチ名を表示します。 監視ポートには(監視)、ミラーポートには(ミラー)が、仮想スイッチ名の後ろに付きます。

3. 仕様

3.1 コマンド

本機能では、表 3.1-1 に示すコマンドを提供します。

表 3.1-1 ポートミラーリング機能のコマンド仕様

コマンド名	sg_mirror		
格納場所	/opt/necfws/bin		
コマンド構文	sg_mirror --add --m=mirror_port1 [,mirror_port2] --s=src --d=dst1 ,dst2,dst3,... --del mirror_port --list mirror_port --restore --help		
独自引数	--add bridge --m=mirror1 [,mirror2] --s=src --d=dst1 ,dst2,dst3,... ※「=」は半角スペースで代用可能		仮想スイッチのポート(src と dst1,dst2,dst3...)間の通信において、src の入出力を別のポート(mirror_port1 [,mirror_port2])にミラーリングします。仮想スイッチ名は自動で「ovs_src」になる。すでに1つの監視ポートに対してミラーポートを1つ設定している際に、同一の監視ポートに対して別のミラーポートを追加で設定することも可能です。
	--m		ミラーポートとして登録する物理ネットワークインタフェース名を指定します。登録できるインタフェース数は最大で2つとします。仮想ファイアウォールで使用されているインタフェースを指定することはできない。2つ指定する場合はカンマ区切りで指定します。
	--s		監視ポートとして登録する物理ネットワークインタフェース名を指定します。本機能を仮想ファイアウォールで使用する場合は、仮想ファイアウォールで使用しているインタフェースを指定します。登録できるインタフェース数は1つとします。
	--d		標準ポートとして登録する物理ネットワークインタフェース名を指定します。1つ以上のネットワークインタフェースをカンマ区切りで指定します。仮想ファイアウォールで使用する場合は、本オプションを使用することができない。すでに本機能で使用しているインタフェースを指定する必要はありません。
	--del mirror_port		指定したミラーポートに関する設定を削除します。
	--list [mirror_port]		指定したネットワークインタフェースのポートミラーリング設定を表示します。ポートを指定しなかった場合は全てのネットワークインタフェースのポートミラーリング設定を表示します。
	--restore		バックアップファイルからポートミラーリング設定を復元します。
	--help		簡単なコマンドの使用方法 (usage) を標準出力に出力します。

4. 注意・制限事項

- ポートミラーリングで使用しているインタフェースでは、ブリッジ接続は利用できません。

以上