SG3600LM、SG3600LG、SG3600LJ
V8.0、V8.2、V8.3
InterSecVM/SG V4.0

ポートミラーリング機能
説明書

2019 年 10 月　5 版

目次

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
基本ファイアウォール	標準のファイアウォール。
仮想ファイアウォール	仮想ファイアウォール機能により実行された仮想のファイアウォール。
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。

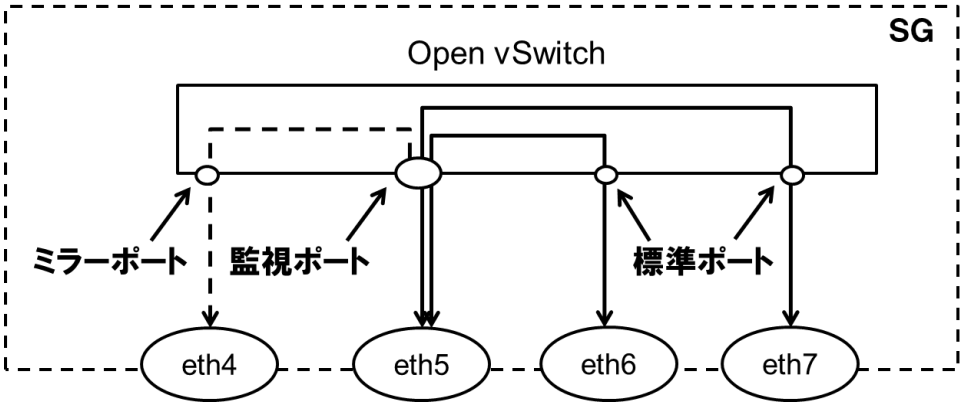


図 1.2-1 ポートミラーリング機能使用時のネットワーク構成

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、あるインタフェースが送受信するトラフィックを、別のインタ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。

※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。
※1 つの監視ポートに対して、複数のミラーポートと標準ポートを設定した場合、特定の監視ポート-標準ポート間のトラフィックのみを、特定のミラーポートにミラーリングすることはできません。全て

の監視ポート-標準ポート間のトラフィックが、全てのミラーポートにミラーリングされます。
※基本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を監視ポートとする場合、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。
※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を監視ポートとする場合、標準ポートを指定する必要はありません。監視ポートを流れる全てのトラフィックを、ミラーポートに出力することができます。

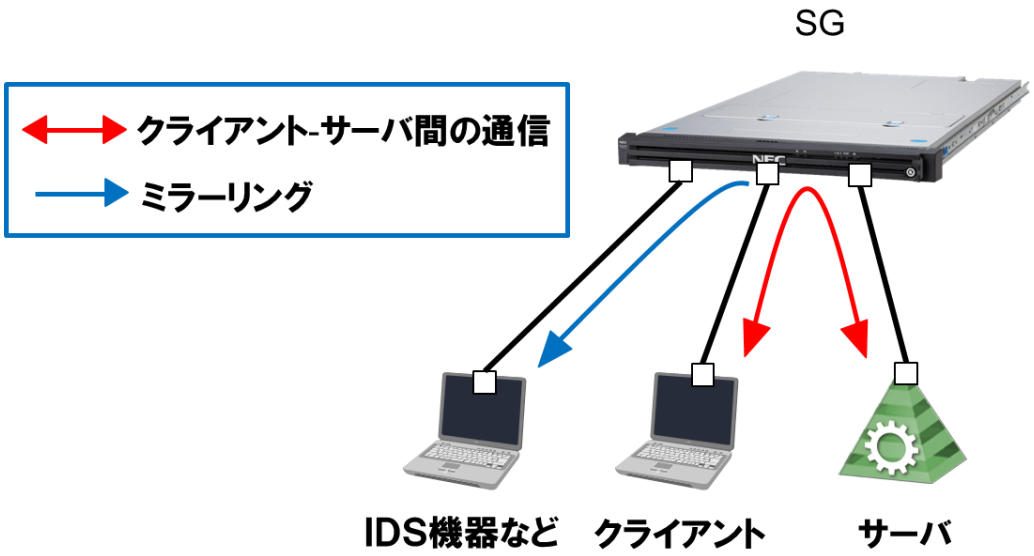


図 1.3-1 ポートミラーリング使用時のネットワーク構成例

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。

2.1.1 コマンドの実行

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。

- 新規にポートミラーリング設定を行う場合

  下記は、eth0 を監視ポート、eth2 をミラーポートに設定して、eth0-eth1 間のトラフィックを 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、1 つの監視ポートに対して、ミラーポートと標準ポートを複数設定することが可能です。下記は、eth0 を監視ポート、eth3、eth4 をミラーポートに設定して、eth0-eth1、eth0-eth2 間のトラフィックを eth3、eth4 で監視する場合のコマンドの事項例です。

  ```
  /opt/necfws/bin/sg_mirror --add --m=eth3,eth4 --s=eth0 --d=eth1,eth2
  ```

- ポートミラーリング設定を更新する場合

  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が可能です。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-eth1 間のトラフィックを 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
  ```

  この時、--d オプションで eth1 以外を指定した場合、標準ポートは指定したネットワークインタフェースに更新されます。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、eth3 をミラーポートとして追加し、標準ポートを eth1 から eth4 に変更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=eth4
  ```

- 仮想ファイアウォールでポートミラーリング設定を行う場合

  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 のトラフィックを 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
  ```

監視ポート、ミラーポート、標準ポートに指定できないネットワークインタフェースを、表 2.1-1 に示す。

表 2.1-1 使用できないネットワークインタフェース

ポート	使用できないネットワークインタフェース
全ポート共通	● bonding インタフェース ● slave インタフェース ● VLAN あり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
監視ポート	● 他のポートミラーリング機能で、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
標準ポート	● VLAN なし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 ● 他の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
ミラーポート	● eth0、eth1 ● VLAN なし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 ● 他の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

2.1.2　かんたん設定

(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[ファイアウォール]のリンクをクリックします。
(3)　[ルール設定]テーブルから、[かんたん設定]ボタンをクリックします。
(4)　画面の指示に従い、かんたん設定を行ってください(設定に変更がない場合も実行してください)。

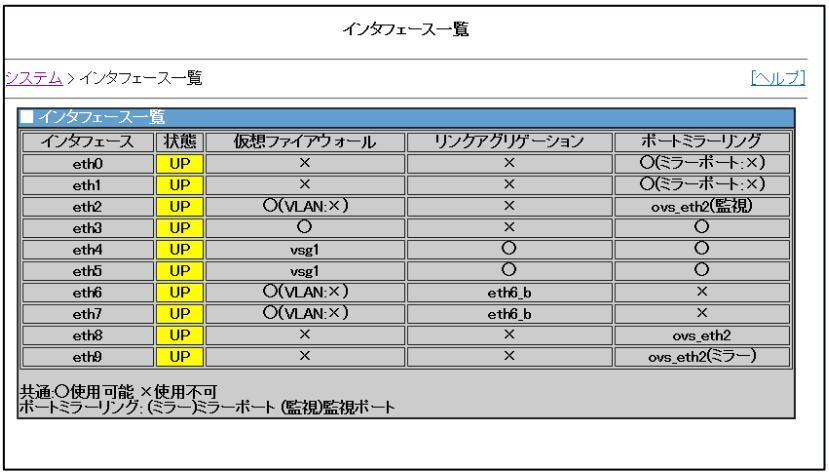
2.2　画面での確認

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。



各項目の説明は表 2.2-1 の通りです。

表 2.2-1 インタ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。

	仮想ファイアウォールで使用しておらず、新たに仮想ファイアウォールで使用可能な場合は○、使用不可能な場合は×と表示します。 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:×)」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。 bonding インタフェースとして登録しておらず、新たに bonding インタフェースとして登録可能な場合は○、登録不可能な場合は×と表示します。
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。 ポートミラーリング機能で使用しておらず、新たにポートミラーリング機能で使用可能な場合は○、使用不可能な場合は×と表示します。 監視ポートもしくは標準ポートとして登録できるが、ミラーポートとして登録できないインタフェースは、「○(ミラーポート:×)」と表示します。

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

<table>
<tr><td>コマンド名</td><td colspan="3">sg_mirror</td></tr>
<tr><td>格納場所</td><td colspan="3">/opt/necfws/bin</td></tr>
<tr><td>コマンド構文</td><td colspan="3">sg_mirror --add --m=mirror_port1 [,mirror_port2] --s=src --d=dst1 ,dst2,dst3,...
--del mirror_port
--list mirror_port
--help</td></tr>
<tr><td rowspan="5">独自引数</td><td rowspan="4">--add bridge
--m=mirror1 [,mirror2]
--s=src
--d=dst1 ,dst2,dst3,…

※「=」は半角スペースで代用可能</td><td colspan="2">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」になります。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。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。</td></tr>
<tr><td>--m</td><td>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ません。2 つ指定する場合はカンマ区切りで指定します。</td></tr>
<tr><td>--s</td><td>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。</td></tr>
<tr><td>--d</td><td>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ません。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。</td></tr>
<tr><td>--del mirror_port</td><td colspan="2">指定したミラーポートに関する設定を削除します。</td></tr>
<tr><td>--list [mirror_port]</td><td colspan="2">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。</td></tr>
<tr><td>--help</td><td colspan="2">簡単なコマンドの使用方法（usage）を標準出力に出力します。</td></tr>
</table>

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。
- 本機能と仮想ファイアウォール機能を併用する場合は、仮想ファイアウォール作成⇒ポートミラーリング設定の順に、設定を行ってください。
- ポートミラーリング設定を行っている仮想ファイアウォールを削除する場合は、先にポートミラーリング設定を削除してください。

以上