

Short Ver.

SSG to SRX Migration

ScreenOS から Junos OS へのマイグレーションガイド

2018年6月

ジュニパーネットワークス株式会社

JUNIPER
NETWORKS

Engineering
Simplicity

はじめに

本資料は、SSG (ScreenOS) と SRX シリーズ (Junos OS) の設定の違いおよび、基本的な Junos OS CLI の操作を説明していますので、SRX マイグレーションガイドとしてご利用ください。

各機能の詳細は、ユーザガイドなどをご参照ください。

* SRX300、Junos 15.1X49-D130 をベースに作成しております

目次

第1章: 設定の基礎	P. 4
第2章: 基本オペレーション	P. 15
第3章: 管理設定	P. 31
第4章: ゾーン / ルーティング	
第5章: オブジェクト	
第6章: IPsec	
第7章: HA (High Availability)	
第8章: IPsec	
第9章: HA (High Availability)	

Short Ver.

第1章：設定の基礎

Junos OS の操作

アジェンダ

- 1-1. Junos OS のモード
- 1-2. SSG と SRX 基本的なコマンドの違い
- 1-3. 設定ファイルの仕組み
- 1-4. 設定操作の基本コマンド

1-1. Junos OS のモード(1/2)

SRX(Junos OS)の CLI モードについて

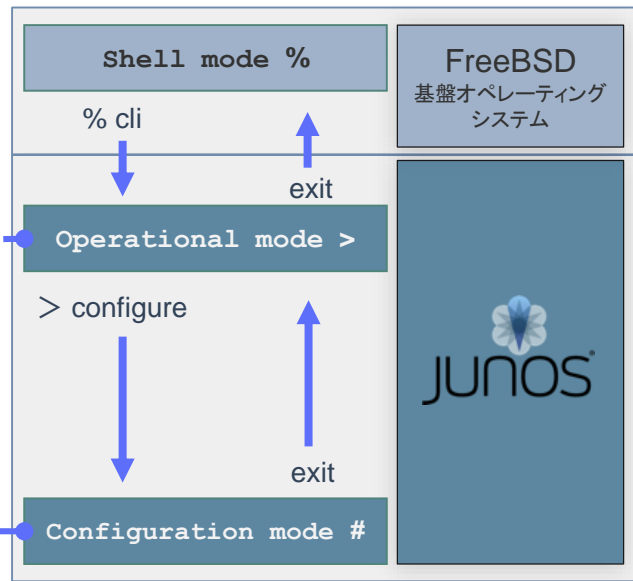
行う操作や設定によってモードを切り替えて利用

- シェルモード (※通常は使用しない)
基盤システムの操作を行うモード(Unix コマンド)
- Junos OS のオペレーショナルモード
機器動作のステータス確認や操作を行うモード
- Junos OS のコンフィグレーションモード
機器の設定を行うモード

• 各ステータスの表示
• ping、traceroute、telnet
• デバッグ
• OS アップグレード
• リポート、シャットダウン
• 時計の操作

• システム設定
• インタフェース設定
• ルーティング設定
• ポリシー設定
• セキュリティ設定など

Junos OS の CLI モードの遷移



1-1. Junos OS のモード (2/2)

root ユーザでログインした場合はシェルモードから開始

root ユーザ以外でログインした場合はオペレーショナルモードから開始

```
SRX300 (ttyu0)
login: root
Password: password

--- JUNOS 15.1X49-D130.6 built 2018-03-04 17:25:09 UTC

root@SRX300% ← シェルモード (root ユーザはこのモードにログイン)
root@SRX300% cli
root@SRX300> ← オペレーショナルモード (root ユーザ以外はこのモードにログイン)
root@SRX300> configure
Entering configuration mode
root@SRX300# ← コンフィグレーションモード
root@SRX300# exit
Exiting configuration mode
root@SRX300>
root@SRX300> exit
root@SRX300%
root@SRX300% exit
logout
```

1-2. SSG と SRX 基本的なコマンドの違い

SSG と SRX の基本的なコマンドの違い

操作	SSG (ScreenOS)	SRX (Junos OS)
設定	set	set
削除	unset	delete
設定の確定	即反映 *	commit
保存	save	commit
確認コマンド	get	show

* commit 相当のコマンド無し

1-3. 設定ファイルの仕組み(1/4)

SSG は設定後すぐコマンドが反映

SRX は設定後 commit を使用してコマンドを反映

- SSG

config の確認

- 設定コマンドによって設定を config に反映
- 稼働中の設定ファイル
- 機器の電源断時に消去

```
SSG5-> get config
```

saved config の確認

- save コマンドによって稼働中の設定ファイルをフラッシュ領域に保存
- 機器の電源断時においても保持

```
SSG5-> get config saved
```

1-3. 設定ファイルの仕組み(2/4)

SRX 設定の反映動作

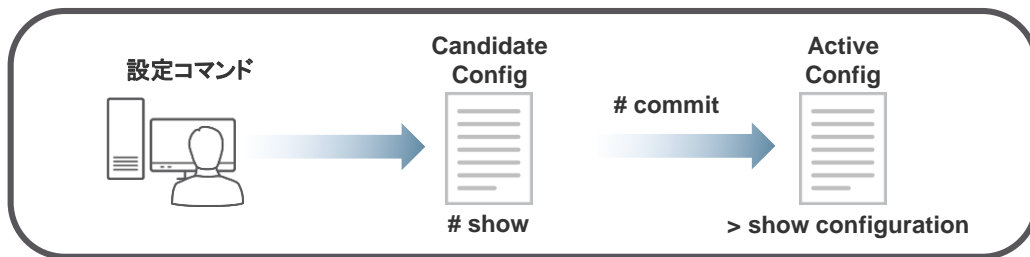
- SRX
- コンフィグレーションモードにて任意の設定を実行 (Candidate Config の編集)

```
root@SRX300# set configuration-command
```

- commit で設定を反映 (Active Config の確定)

```
root@SRX300# commit  
commit complete
```

← 反映処理後に出力



1-3. 設定ファイルの仕組み(3/4)

- SRX

Candidate Config (候補設定) の確認

- 編集中的設定ファイル
- 設定コマンドによって設定を Candidate Config に反映

```
root@SRX300# show
```

Active Config (稼働設定) の確認

- commit で確定された稼働中の設定

```
root@SRX300> show configuration
```

```
root@SRX300# run show configuration
```

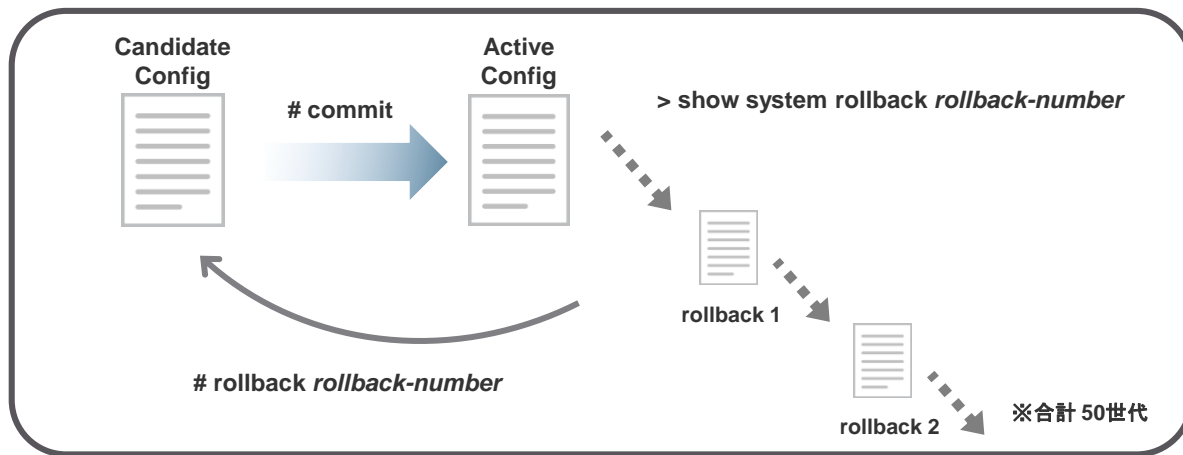
1-3. 設定ファイルの仕組み(4/4)

SRX は変更前のコンフィグが自動でバックアップ

設定を機器の再起動をせずにバックアップから復元することが可能

- SRX
- 設定の復元 (rollback)

```
root@SRX300# rollback rollback-number
root@SRX300# commit
```



1-4. 設定操作の基本コマンド(1/2)

SRX 設定の操作オプション

- SRX
- Active Config と Candidate Config の差分の確認 (compare)

```
root@SRX300# show | compare
```

- Candidate Config の構文エラーの確認 (check)

```
root@SRX300# commit check
```

- 設定ファイルを set 形式で表示 (display set)

```
root@SRX300# show | display set
```

```
root@SRX300> show configuration | display set
```

- 設定ファイルの連続表示 (no-more)

```
root@SRX300# show | no-more
```

1-4. 設定操作の基本コマンド(2/2)

SRX 設定 その他のコマンド

- SRX
- コンフィグレーションモードにおけるオペレーショナルモードのコマンドの実行 (run)

```
root@SRX300# run operational-mode-command
```

- 特定の設定の無効化 (deactivate)

```
root@SRX300# deactivate configuration-command
```

- 無効化された設定の有効化 (activate)

```
root@SRX300# activate configuration-command
```

第2章：基本オペレーション

デバイスのオペレーション操作

アジェンダ

- 2-1. 初期化・シャットダウン手順
- 2-2. 設定のバックアップ・リストア
- 2-3. レスキュー設定
- 2-4. OS アップグレード
- 2-5. パスワードリカバリー手順

2-1. 初期化・シャットダウン手順(1/3)

SSG はコンフィグを削除し再起動することで初期化

SRX はデフォルトのコンフィグを読み込むことで初期化

- SSG

```
SSG5-> unset all
Erase all system config, are you sure? y/[n]  y

SSG5-> reset
Configuration modified, save? [y]/n  n
System reset, are you sure? y/[n]  y
In reset ...
```

2-1. 初期化・シャットダウン手順(2/3)

- SRX

初期化は削除したいデータに応じて選択可能(3通り)

- 工場集荷時の設定をロード

```
root@SRX300# load factory-default
warning: activating factory configuration

[edit]
root@SRX300# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

- ユーザ作成データを削除

```
root@SRX300> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes
```

※コマンドを入力すると再起動が自動開始

- USB メモリやコンパクトフラッシュからフォーマット(全データ削除)

2-1. 初期化・シャットダウン手順(3/3)

SSG は電源オフで直接システムを停止(コマンドなし)

SRX はコマンドでシステムを停止

- SSG

- (SSG5 の場合)

電源ボタンがないため電源ケーブルを抜線することでシステムを停止

- SRX

- システム停止および電源オフ

```
root@SRX300> request system power-off
Power Off the system ? [yes,no] (no) yes
Shutdown NOW!
```

- システム停止

```
root@SRX300> request system halt
Halt the system ? [yes,no] (no) yes
--- snip ---
The operating system has halted.
Please press any key to reboot.
```

2-2. 設定のバックアップ・リストア (1/6)

SSG はターミナルにコンフィグを直接コピー & ペーストすることでロード

SRX は load コマンド実行後に直接コピー & ペーストすることでロード

ロードするコンフィグの形式によって選択が可能 (ツリー形式、set 形式)

- SRX

- ツリー形式

- ロード開始の準備

```
root@SRX300# load override terminal
[Type ^D at a new line to end input]
```

- コンフィグのロード (Ctrl + D で確定、Ctrl + C でキャンセル)
 - 設定を commit

```
root@SRX300# commit
commit complete
```

2-2. 設定のバックアップ・リストア (2/6)

- SRX

- set 形式

- コンフィグの削除

```
root@SRX300# delete
This will delete the entire configuration
Delete everything under this level? [yes,no] (no) yes
```

- ロード開始の準備

```
root@SRX300# load set terminal
[Type ^D at a new line to end input]
```

- コンフィグのロード (Ctrl + D で確定、Ctrl + C でキャンセル)

- 設定を commit

```
root@SRX300# commit
commit complete
```

2-2. 設定のバックアップ・リストア (3/6)

SRX は設定ファイルのローカル保存およびロードが可能

- SRX

- 設定ファイルの保存

```
root@SRX300# save filename
```

- 設定ファイルの確認

```
root@SRX300# run file list detail
/cf/root/:
total blocks: 36
-rw-r--r--  1 root  wheel           361 Mar  4  17:58 .cshrc
-rw-r--r--  1 root  wheel          1090 Mar  4  17:58 .login
-rw-r--r--  1 root  wheel           215 Mar  4  17:58 .profile
-rw-r--r--  1 root  wheel          6962 May 22  16:01 SRX300.cfg
total files: 4
```

- 設定ファイルのロード

```
root@SRX300# load override filename
root@SRX300# commit
```

2-2. 設定のバックアップ・リストア (4/6)

SSG は TFTP サーバへコンフィグをバックアップ

SRX は FTP サーバ等へコンフィグをバックアップ

- SSG

```
SSG5-> save config to tftp ip-address filename
```

- SRX

- ツリー形式のコンフィグバックアップ

```
root@SRX300# save ftp://user-name:password@ip-address/ filename
```

- set 形式のコンフィグバックアップ

```
root@SRX300# show | display set | save ftp://user-name:password@ip-address/ filename
```

2-2. 設定のバックアップ・リストア (5/6)

SSG は TFTP サーバからコンフィグを一旦コンパクトフラッシュに読み込み再起動することでリストア

SRX は FTP サーバ等から再起動せずリストア可能

- SSG

- TFTP サーバからのコピー

```
SSG5-> save config from tftp ip-address filename to flash
```

- 再起動

```
SSG5-> reset  
System reset, are you sure? y/[n] y  
In reset ...
```


2-2. 設定のバックアップ・リストア (6/6)

- SRX

- FTP サーバからのコピー

```
root@SRX300> ftp ip-address
220 3Com 3CDaemon FTP Server Version 2.0
Name (10.1.1.1:root): user-name
331 User name ok, need password
Password: password
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get filename
```

- コンフィグのリストア

- ツリー形式のコンフィグのリストア

```
root@SRX300# load override filename
root@SRX300# commit
```

- set 形式のコンフィグのリストア

```
root@SRX300# load set filename
root@SRX300# commit
```

2-3. レスキュー設定

SSG はレスキューコンフィグのリストア時に再起動が必要

SRX は再起動なしでリストア可能

- SSG

- レスキューコンフィグの作成

```
SSG5-> save config to last-known-good
```

- レスキューコンフィグの状態へリストア

```
SSG5-> exec config rollback
```

- SRX

- レスキューコンフィグの作成

```
root@SRX300> request system configuration rescue save
```

- レスキューコンフィグの状態へリストア

```
root@SRX300# rollback rescue  
root@SRX300# commit
```

2-4. OS アップグレード

SSG は TFTP サーバ経由で OS をアップグレード

SRX はローカルファイルや FTP サーバ経由で OS をアップグレード

- SSG

```
SSG5-> save software from tftp ip-address filename to flash
```

- SRX

- ローカルファイルでの OS アップグレード

```
root@SRX300> request system software add directory/filename
```

- FTP サーバより直接 OS アップグレード

```
root@SRX300> request system software add ftp://user-name:password@ip-address/filename
```

2-5. パスワードリカバリー手順(1/3)

SSG はパスワードのみのリカバリーが不可のためコンフィグ初期化が必要

SRX は root ユーザのパスワード初期化が可能

- SSG
 - 以下いずれかの方法でコンフィグ初期化
 - リカバリーピンホールを押しながら電源を入れる
 - ユーザ名、パスワード共にシリアル番号を入力

2-5. パスワードリカバリー手順(2/3)

- SRX
- 機器起動中に以下を実行

```
--- snip ---  
/kernel data=0xba0974+0x152ba4 syms=[0x4+0xa0810+0x4+0xf0441]  
  
Hit [Enter] to boot immediately, or space bar for command prompt.  
Booting [/kernel] in 1 second...  
  
Type '?' for a list of commands, 'help' for more detailed help.  
loader> boot -s  
Kernel entry at 0x801000c0 ...  
--- snip ---  
System watchdog timer disabled  
Enter full pathname of shell or 'recovery' for root password recovery or RETURN for /bin/sh:  
recovery  
Performing system setup ...
```

← スペースキーを押下

← シングルユーザモードでブート

← パスワードリカバリーを開始

2-5. パスワードリカバリー手順(3/3)

- SRX (続き)

```
--- snip ---
Starting CLI ...
root@SRX300> configure ← Configuration モードへ
Entering configuration mode

[edit]
root@SRX300> set system root-authentication plain-text-password
New password:
Retype new password: ← 新しいパスワードを 2回入力

[edit]
root# commit ← 設定を commit
commit complete

[edit]
root# exit
Exiting configuration mode

root> exit

Reboot the system? [y/n] y ← 再起動
Terminated
```

第3章：管理設定

Administration 設定

アジェンダ

3-1. 管理アカウントの設定

3-2. 初期設定

3-3. IP アドレス設定

3-4. ログ設定

3-5. NTP

3-6. SNMP

3-1. 管理アカウントの設定(1/2)

SSG と SRX は共に管理者アカウントとしてデフォルトのユーザが存在

- SSG
 - ユーザ名:netscreen パスワード:netscreen
 - 以下のコマンドでユーザ名、パスワードの変更が可能

```
SSG5-> set admin name user-name  
SSG5-> set admin password password
```

- SRX
 - ユーザ名:root パスワード:なし
 - 以下のコマンドでパスワードを設定

```
root@SRX300# set system root-authentication plain-text-password  
New password: password  
Retype new password: password
```

3-1. 管理アカウントの設定 (2/2)

SSG は 2つの権限が設定可能

SRX はクラスを使い権限の割り当てが可能

- SSG

```
SSG5-> set admin user user-name password password privilege [all | read-only]
```

- SRX

- デフォルトで 4つのクラス (operator、read-only、super-user、unauthorized)

```
root@SRX300# set system login user user-name class class-name authentication plain-text-  
password  
New password: password  
Retype new password: password
```

3-2. 初期設定(1/2)

SSG はホスト名、タイムゾーン、サマータイム、時間を設定

SRX はホスト名、タイムゾーン、時間を設定

- SSG

```
SSG5-> set hostname host-name  
SSG5-> set clock timezone 9  
SSG5-> set clock dst-off  
SSG5-> set clock mm/dd/yyyy hh:mm:ss
```

- SRX

```
root@SRX300# set system host-name host-name  
root@SRX300# set system time-zone Asia/Tokyo  
root@SRX300# run set date YYYYMMDDhhmm.ss
```

3-2. 初期設定(2/2)

時間設定の確認

- SSG

```
SSG5-> get clock
Date 11/21/2013 11:27:15, Daylight Saving Time disabled
The Network Time Protocol is Disabled
Up 14 hours 24 minutes 8 seconds Since 20Nov2013:21:03:07
1385033235.948425 seconds since 1/1/1970 0:0:0 GMT
GMT time zone area 9:00
GMT time zone offset -9:00
```

- SRX

```
root@SRX300> show system uptime
Current time: 2018-05-25 09:06:36 UTC
Time Source: LOCAL CLOCK
System booted: 2018-05-17 15:19:33 UTC (1w0d 17:47 ago)
Protocols started: 2018-05-17 15:19:33 UTC (1w0d 17:47 ago)
Last configured: 2018-05-21 17:24:04 UTC (3d 15:42 ago) by root
 9:06AM up 7 days, 17:47, 1 user, load averages: 0.12, 0.11, 0.08
```

3-3. IP アドレス設定 (1/3)

SRX のポートは L2 と L3 の 2種類

IP アドレスを設定するポートに L2 が設定されている場合は削除が必要
(SSG のブリッジグループに類似)

- SRX

- ポートの状態の確認

L2 設定

```
root@SRX300> show interfaces terse
Interface      Admin Link Proto   Local      Remote
ge-0/0/1       up    up
ge-0/0/1.0     up    up    eth-switch
ge-0/0/2       up    up
ge-0/0/2.0     up    up    inet      10.1.1.254/24
```

L3 設定

- L2 設定の削除

```
root@SRX300# delete interfaces ge-0/0/1 unit 0 family ethernet-switching
```

3-3. IP アドレス設定 (2/3)

SSG はインタフェースと IP アドレスを設定

SRX はインタフェースとロジカルユニット、アドレスファミリー、IP アドレスを設定

- SSG

```
SSG5-> set interface interface-name ip ip-address
```

- SRX

```
root@SRX300# set interfaces interface-name unit number family inet address ip-address
```

<設定例>

ge-0/0/1 の unit 0 に IPv4 のアドレス 10.1.1.1/24 を設定

```
root@SRX300# set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/24
```

3-3. IP アドレス設定 (3/3)

IP アドレスの確認

- SSG

```
SSG5-> get interface
A - Active, I - Inactive, U - Up, D - Down, R - Ready
Interfaces in vsys Root:
Name                IP Address          Zone      MAC           VLAN State VSD
bri0/0              0.0.0.0/0           Untrust   N/A           -   D   -
eth0/0              10.1.8.254/24      Trust     001b.c035.c980 -   U   -
```

- SRX

```
root@SRX300> show interfaces terse
Interface           Admin Link Proto  Local      Remote
ge-0/0/0            up    up
ge-0/0/0.0          up    up
  ~ 途中省略 ~
ge-0/0/1            up    up
ge-0/0/1.0          up    up  inet   10.1.1.1/24
```

ユニット番号

3-4. ログ設定(1/3)

SSG はイベントログやトラフィックログを機器に保存し get log で確認可能

SRX は設定のログを /var/log 配下のファイルとして保存し show log で確認可能

- SSG

```
SSG5-> get log event
Total event entries = 56
Date          Time          Module Level  Type Description
2013-11-22 10:44:30 system warn   00515 Admin user netscreen has logged on via
                                     the console
```

- SRX

```
root@SRX300> show log messages
Nov 21 11:39:31 SRX300 login[3055]: LOGIN_INFORMATION: User root logged in from host
[unknown] on device ttyu0
Nov 21 11:39:41 SRX300 login: Login attempt for user root from host [unknown]
```


3-4. ログ設定 (2/3)

SSG はログの保存先は固定

SRX はログの保存先をファイル名、ファシリティ、レベルで設定可能

- SRX
- ログ設定

```
root@SRX300# set system syslog file file-name facility level
```

- 文字列を指定することでフィルターが可能

```
root@SRX300# set system syslog file file-name match regular-expression
```

3-4. ログ設定 (3/3)

SSG はログの単位で syslog サーバへ転送するかを設定

SRX はファシリティ等で転送するログを指定

- SSG

```
SSG5-> set syslog config server-address log ( event | traffic | event )  
SSG5-> set syslog enable
```

- SRX

```
root@SRX300# set system syslog host server-address facility level
```

※SRX のトラフィックログに関しては、ログの収集モードによって設定が異なる

「第6章セキュリティポリシー」で別途詳細

3-5. NTP

SSG は NTP の有効化と NTP サーバを指定

SRX は NTP サーバを指定

- SSG

```
SSG5-> set clock ntp  
SSG5-> set ntp server server-address
```

- SRX

```
root@SRX300# set system ntp server server-address
```

3-6. SNMP

SSG は SNMP コミュニティと SNMP ホストを設定

SRX は SNMP コミュニティと SNMP トラップグループを設定

- SSG

- SNMP v1、v2c をサポート

```
SSG5-> set snmp community community-name ( Read-Write | Read-Only ) trap-off version v2c
SSG5-> set snmp host community-name manager-address trap v2
```

- SRX

- SNMP v1、v2c、v3 をサポート

```
root@SRX300# set snmp community community-name authorization ( read-write | read-only )
root@SRX300# set snmp trap-group group-name version v2
root@SRX300# set snmp trap-group group-name targets manager-address
root@SRX300# set snmp trap-group group-name categories category
```



JUNIPER[®]
NETWORKS

Engineering
Simplicity