Fortigate Firmware VersionUp 手順書

Ver.3.0MR7→ Ver.4.0MR2patch6

NVC

NETWORK VALUE COMPONENTS

改訂履歴

初版：2011/05/19

目次

はじめに

本マニュアルは Fortigate の OS バージョンを Version3.0MR7 から弊社推奨バージョン Version4.0MR2(Patch6)へアップグレードを行うための各種操作方法について記載しています。

アップグレード、ダウングレード方法について

FortiGate でのアップグレード・ダウングレードは WebUI と CLI の 2 通りが利用出来ます。

■アップグレード

・WebUI　　設定を引き継ぎつつアップグレードが可能です。*一部引き継がれない設定がございます。
・CLI　　工場出荷状態になります。

■ダウングレード　*ダウングレードは初期化を同時に行える、CLI からの実施をお勧め致します。

・WebUI　　ほぼ全ての設定が消えます。
・CLI　　工場出荷状態になります。

1. v3.0MR7 からのアップグレード

v3.0MR6未満からv4.0MR2Patch6以上へは直接アップグレードができません。

アップグレードパス

1.v3.0MR7patch8→v4.0MR1patch4にアップグレード
2.v4.0MR1patch4→v4.0MR2Patch6にアップグレード

現在使用しているバージョンがv3.0MR7patch8である場合は、一度v4.0MR1patch4にアップグレードを行なった後v4.0MR2Patch6へとアップグレードを行ないます。

バージョンがv3.0MR7patch8未満の場合は、一度v3.0MR7patch8にアップグレードを行います。

v3.0MR7patch8へのアップグレードは下記URLの資料にて実施願います。
http://gold.nvc.co.jp/supports/fortinet/tech/FAQ/folder.2008-11-04.2779728934/

2. 設定情報の引継ぎ(3.0MR7→4.0MR1)

注意：下記は3.0MR7から4.0MR1へアップグレードする際に発生する項目です。

- Log Settings Changes

FortiOSv4.0MR1 では config log trafficfilter はなくなりました。
よって FortiOSv3.0M6 から FortiOSv4.0MR1Patch4 へアップグレードの際設定は引き継がれません。

- System Settings

FortiOSv4.0MR1 では config system settings の配下の p2p-rate-limit がなくなりました。
よって MR6/MR7 から v4.0MR1Patch4 のアップデートの際に設定を引き継ぎません。

- Router Access-list

FortiOSMR6/MR7 から FortiOSv4.0MR1Patch4 のアップデートの際に、config router access-list の配下の設定に関して、失われる可能性があります。

- Identity Based Policy

ファイアウォールポリシー認証は FortiOSv4.0MR1 で変更されました。認証を要求するどんなファイアウォールポリシーも、現在は Identity Based ポリシーとして認識されています。以前に、異なるスケジュール、サービスおよびトラフィック・シェーピング・セッティングのために個別の認証ファイアウォールポリシーを作成しなければなりませんでした。しかし、FortiOSv4.0MR1 では、ファイアウォール認証セッティングはすべてファイアウォールポリシーの Identity Based ポリシーのセクション中で形成されます。トラフィックが Identity Based ポリシーのうちのどれとも一致しない場合、トラフィックは暗黙の DENY ALL となります。

- IPv6 Tunnel

FortiOSv3.0.MR7 から FortiOSv4.0MR1Patch4 へアップグレードの際、config system ipv6-tunnel の配下の設定は失われる可能性があります。

- User Group

FortiOSv3.0MRx では、protection profile は GUI から user group へ割り当てが可能でしたが、FortiOSv4.0MR1 からは CLI からのみ可能です。

- Zone Configuration

FortiOSv3.0MRx の Zone name の文字数は 32 文字以内でした。しかし、v4.0MR1 では 15 文字以内に変更になりました。よって、15 文字を超えるどんな Zone name も FortiOSv3.0 から FortiOSv4.0MR1Patch4 にアップデートした後に設定が失われます。

• IPv6 Vlan Interfaces

形成された ipv6 アドレスと Vlan インターフェースは、FortiOSv3.0MRx から FortiOSv4.0 MR1Patch 4 にアップグレードした後に設定が失われます。

• VIP Settings

VIP の設定 set http-ip-header は、FortiOSv3.0MR6/MR7 から FortiOSv4.0MR1Patch4 にアップデートした際に、disable になります。

• FDS Push-update Settings

config system autoupdate push-update の配下のアドレスとポート設定は、FortiOSv4.0MR1Patch4 にアップグレードした後に失われる可能性があります。

•Content Archive Summary

archive summary related configuration は FortiOSv4.0MR1Patch4 にアップグレードした後に失われます。

• RTM Interface Configuration

FortiOSv3.0MR6/MR7 から FortiOSv4.0MR1 にアップグレードする際、RTM オブジェクトを使用する配置の RTM インターフェースおよびいくつかの設定は保持されません。FortiOSv3.00MRx では、RTM オブジェクトは、大文字を使用していました。FortiOSv4.0MR1Patch4 は小文字を RTM オブジェクトに使用します。

•SSL-VPN Bookmarks

いくつかの SSLVPN bookmarks は、FortiOSv4.0MR1Patch4 にアップグレードした後に失われる可能性があります。

•Web Filter Exempt List

FortiOSv4.0MR1Patch4 は、ウェブ・コンテンツ・ブロックリストおよび除外リストが 1 つのリストに統合されました。v4.0 MR1MR1patch4 にアップグレードすることで、ウェブ・コンテンツ・ブロックリストのみが保持されます。

• IPS DoS Sensor Configuration

FortiOSv3.0MR7 から FortiOSv4.0 MR1 にアップグレードする場合、v3.0 の中の IPS DoS センサーの config は対応する DoSpolicy に変換されません。従って、DoS センサーに関連する設定は失われる可能性があります。

● Antivirus Service on Non-Standard Port

FortiOSv3.0MR7 から v4.0 MR1 にアップグレードすることで、non-standard-port でスキャンされる AntiVirus の設定は保持されません。

※回避策については、弊社 FAQ” non-standard-port で UTM 機能を利用できますか？ ”をご覧ください。

http://gold.nvc.co.jp/supports/fortinet/

3. Config の保存、リストア

3.1 準備

以下のものを準備する。

- [3.0MR7、4.0MR1]
  ネットワーク接続可能な PC(Internet Explorer 7.0 以上がインストールされていること)
- [4.0MR2]
  ネットワーク接続可能な PC (IE8 もしくは FireFox 3.5 以上がインストールされていること)
- アップグレードするファームウェア

3.2 PC の設定

WebUI では、ブラウザを利用して Config の保存を行います。
その為、作業は FortiGate に対してアクセス制限の無い PC で行います。

3.3 接続

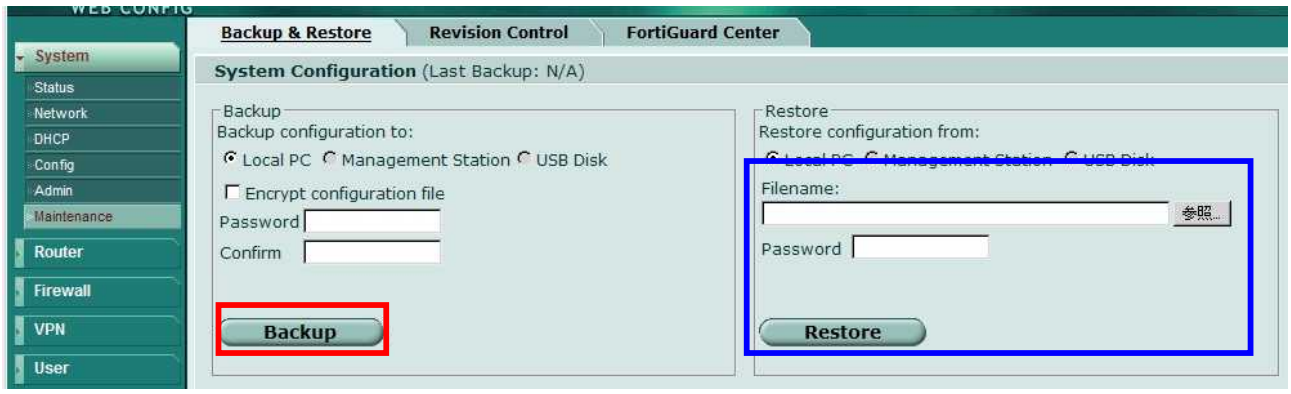
(1) FG の”Internal(Port1)”ポートに PC の LAN ケーブルを接続する。
(2) PC のブラウザより FortiGate にアクセスする。
(https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx x は FortiGate の IP を指定)
(3) ユーザ名・パスワードを入力してログインをします。

3.4 Config の保存 (OS v3.0) (赤枠)

(1) ブラウザ内の左側にある System >> Maintenance をクリックします。
(2) Backup and restore >> Backup をクリックするとファイルのダウンロード が開始されるので保存する。

＊Config のリストア (OS v3.0) (青枠)

(1) ブラウザ内の左側にある System >> Maintenance をクリックします。
(2) Backup and restore >> Filename: の右端にある“参照”をクリックしアップグレードするファイルを選択します。
(3) Restore をクリックし、コンフィグをリストアします。



（バックアップリストア画面 OSv3.0）

3.5 Config **の保存**　(OS v4.0) (**赤枠**)

(1)　**ブラウザ内にある”バックアップ”をクリックします。**

＊Config **のリストア**　(OS v4.0) (**青枠**)

(1)　**ブラウザ内にあるリストアをクリックします。**

（**バックアップリストア画面**　OSv4.0）

4. WebUI でのアップグレード

4.1 準備

以下のものを準備します。

- ネットワーク接続可能な PC　(IE8 もしくは FireFox 3.5 以上)
- Firmware　(*OS は http://gold.nvc.co.jp/supports/fortinet/OS/ からダウンロードしてください)

4.2 PC の設定

WebUI では、ブラウザを利用してアップグレードを行います。

その為、作業は FortiGate に対してアクセス制限の無い PC で行います。

4.3 接続

(1) PC のブラウザより FortiGate にアクセスをします。

(https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx それぞれ FortiGate の IP を指定)

(2) ユーザ名・パスワードを入力してログインをします。

4.4 アップグレード

(1) ブラウザ内の左側にある System をクリックします。

(2) System の下に現れた Status をクリックします。

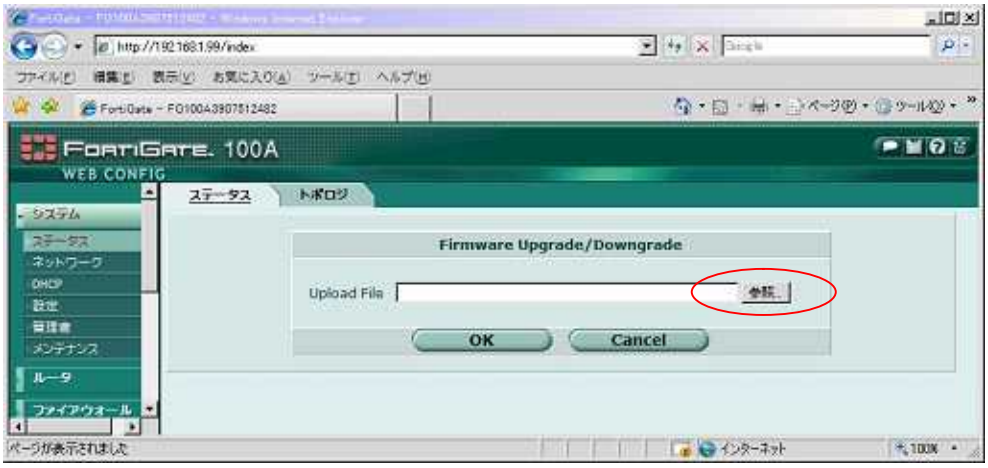
(3) ブラウザの中央にある Firmware Version で現在のバージョンを確認（図１参照）

（図１．バージョン情報確認画面）

(4) ファームウェアバージョン の右端にある更新ボタンをクリック。(図 2 参照)

(図２．アップデートボタン確認画面)

(5) 画面が切り替わった後 Upload File: の右端にある“参照”をクリックしアップグレードするファイルを選択します。(図 3 参照)



(図３．アップデートボタン確認画面)

(6) “OK”をクリックするとアップグレードが始まり、自動的にリブートします。

(7) リブート後、再ログインをしてファームウェアバージョンの確認を行います。
(Version4.0MR2(Patch6)まで繰り返し実行願います)

(8) Version4.0MR2(Patch6)までアップグレードが終わりますと管理画面が変更されます。
(図 4 参照)

（図 4. v4.0MR2 の画面）

(9) コンフィグをバックアップし作業は完了になります。

5. CLI でのアップグレード、ダウングレード

注意２: CLI でアップグレードの場合、Config やユーザー名、パスワードは工場出荷時状態になります。

5.1 準備

以下のものを準備する

- ネットワーク接続可能な PC(TeraTerm 等のターミナルソフト、TFTPServer がインストールされていること)
- クロス LAN ケーブル
- クロスシリアルケーブル (FortiGate に付属)
- アップグレードするファームウェア
- ダウングレードするファームウェア
- 適用するコンフィグ(ある場合)

5.2PC の設定

CLI では、TFTP サーバを利用してアップグレード行います。そのため、PC の設定は IP アドレスの設定とターミナルソフトの設定が必要になります。

(1) PC の IP アドレスを設定する(例:192.168.1.10/24)

(2) TeraTerm の設定を以下の通りに設定します。

- ボーレート：9600
- データ　　：8 ビット
- パリティ　：なし
- ストップ　：1
- フロー制御：なし

(3) TFTPServer ではファームウェアを保存してあるフォルダを指定します。

5.3 接続

(1) ターミナルソフトより FortiGate にアクセスします。

(2) ユーザ名・パスワードを入力してログインします。

5.4 アップグレード、ダウングレード

(1) 現在のバージョンを確認する。get sys status で確認します。

(2) exe reboot と入力し、リブートを行います。

(3) リブート後 Press Any Key To Download Boot Image.と表示されたら何かキーを押します。
Enter G,F,B,Q,or H： と表示されるので G を入力する。
※機体によっては何かキーを押した後、G を押さず(4)へ移行するものもあります。

＊次ページ実際のリブートしたときのプロンプト

FortiCLI 画面

```
Fortigate-800 # execute reboot

Please stand by while rebooting the system.

FGT800 (11:03-06.01.2005)

Ver:04000001

Serial number:FGT800260550****

RAM activation

Total RAM: 1024MB

Enabling cache...Done.

Scanning PCI bus...Done.

Allocating PCI resources...Done.

Enabling PCI resources...Done.

Zeroing IRQ settings...Done.

Verifying PIRQ tables...Done.

Boot up, boot device capacity: 61MB.

Press any key to display configuration menu...   ←ここで何かキーを押す

..

[G]:  Get firmware image from TFTP server.

[F]:  Format boot device.

[B]:  Boot with backup firmware and set as default.

[C]:  Configuration and information.

[Q]:  Quit menu and continue to boot with default firmware.

[H]:  Display this list of options.


Enter G,F,B,C,Q,or H:   ← G を入力する
```

(4) Enter tftp server address [192.168.1.168]: と表示されるので PC の IP アドレスを入力
(例: Enter tftp server address [192.168.1.168]: 192.168.1.10)

(5) Enter local address [192.168.1.188]: と表示されるので FG の IP アドレスを入力
(例: Enter local address [192.168.1.188]: 192.168.1.99)

(6) Enter firmware image file name [image.out]: と表示されるので Firmware のファイル名を入力
(例: Enter firmware image file name [image.out]: FGT_800-v300-build0400-FORTINET.out)

(7) その後、Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]? と確認メッセージが表示されるので D キーを押す
*モデルによっては”B”が表示されません。

(8) 自動的にリブートされるのでログイン後、アップグレードの確認を行います。
ダウングレードの場合は、保存していたコンフィグをリストアします。

6. HA 構成時でのアップグレード、ダウングレード

HA 構成時に通信断を少なくするアップグレード作業の流れについて解説いたします。

※注意：Active-Passive の HA 構成時の手順について解説いたします。Active-Active の HA 構成の場合は弊社サポートへご連絡下さい。

6.1 準備

以下のものを準備します。

- ネットワーク接続可能な PC(TeraTerm 等のターミナルソフトがインストールされていること)
- クロスシリアルケーブル

6.2 PC の設定

CLI では、ターミナルソフトを利用してコマンドを実行します。

(1) TeraTerm の設定を以下の通りに設定します。(コンソールから実施する場合)

- ボーレート：9600
- データ　　：8 ビット
- パリティ　：なし
- ストップ　：1
- フロー制御：なし

6.3 HA ステータスの確認

主系の FortiGate を FortiGate01、従系の FortiGate を FortiGate02 として解説致します。
FortiGate02 の HA ステータスが Master であった場合は作業対象の機器が逆となります。

(1) ターミナルソフトより FortiGate01 にアクセスします。
(2) ユーザ名・パスワードを入力してログインします。
(3) HA ステータスの確認。diagnose sys ha status により確認します。(注:P15 参照
(4) ターミナルソフトより FortiGate02 にアクセスします。
(5) ユーザ名・パスワードを入力してログインします。
(6) HA ステータスの確認。diagnose sys ha status により確認します。(注:P15 参照

6.4 FortiGate02 をネットワークから切り離し

(1) FortiGate02 の実通信を行っているケーブルを取り外します。
(2) FortiGate02 の HA の同期を行っているケーブルを取り外します。

6.5 FortiGate02 のアップグレード

別項のバージョンアップ手順を参照します。

「1. v3.0MR7からのアップグレード」を参照

*configの引継ぎが必要な場合はWebUIを利用したバージョンアップ手順にて実施願います。

*ダウングレードではCLIによる実施を推奨致します。

6.6 FortiGate02 と FortiGate01 の入れ替え

(1) FortiGate01 の実通信ケーブルと HA ケーブルを取り外します。
※通信断が発生いたします。

(2) FortiGate02 の実通信ケーブルと HA ケーブルを取り付けます。

(3) exe update-now コマンドにより自動アップデートを実行します。

(4) 実通信に問題が発生していないことを確認します。
バージョンアップによる問題の有無を確認します。問題が発生した場合は設定等を見直し問題を修正します。

6.7 FortiGate01 のアップグレード

別項のバージョンアップ手順を参照します。

「1. v3.0MR7からのアップグレード」を参照

*configの引継ぎが必要な場合はWebUIを利用したバージョンアップ手順にて実施願います。

*ダウングレードではCLIによる実施を推奨致します。

6.8 FortiGate01 のネットワークへの導入

(1) FortiGate01 の HA ケーブルを取り付けます。

(2) diagnose sys ha status によりネゴシエーションが行えていることを確認します。(注:P15 参照

(3) FortiGate01 の実通信ケーブルを取り付けます。

(4) 実通信に問題が発生していないことを確認します。

以下コマンドの実行例となります。

注：diagnose コマンドはメーカ開発コマンドであるため詳細にはお答え致しかねますので予めご了承頂きたくお願い致します。

▼FortiOS v3.0

FortiGate01 # diagnose sys ha status

```
HA information
Statistics
        traffic.local = s:208814 p:1890370 b:182008613
        traffic.total = s:208811 p:1890359 b:182008238
        activity.sess = c:0 u:0 d:0
        activity.fdb    = c:0 q:0

Model=500, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=0, load_balance=0, schedule=3.

HA group member information: is_manage_master=1.
FG500A39075XXXXX, 1. Master:200 FortiGate01
FG500A39085XXXXX, 0.    Slave:100 FortiGate02
```

出力結果一番下から二行に表示されている S/N、ホスト名、HA ステータスを確認します。
また、両機器の S/N が表示されていることでネゴシエーションが行えていることを確認します。

▼FortiOS v4.0

ForitGate01 # diagnose sys ha statsus

```
HA information
Statistics
        traffic.local = s:5478 p:191932 b:43865437
        traffic.total = s:5856 p:191933 b:43865497
        activity.fdb    = c:0 q:0

        Model=300, Mode=2 Group=0 Debug=0
        nvcluster=1, ses_pickup=1

        HA group member information: is_manage_master=1.
        FG500A3909601XXX, 0. Master:255 ForitGate01
        FG500A3909602XXX, 1.    Slave:128 ForitGate02

        vcluster 1, state=work, master_ip=169.254.0.1, master_id=0:
        FG500A3909601XXX, 0. Master:255 ForitGate01(prio=0, rev=0)
        FG500A3909602XXX, 1.    Slave:128 ForitGate02(prio=1, rev=1)
```

7 v4.0MR1 からのアップグレード

v4.0MR1patch4未満からv4.0MR2Patch6以上へは直接アップグレードができません。

現在使用しているバージョンがv4.0MR1を使用している中でpatch4未満の場合は、一度v4.0MR1patch4にアップグレードを行なった後v4.0MR2Patch6以上へとアップグレードを行ないます。

※なお、config の保存、リストア　WebUI でのアップグレード・ダウングレード方法は、項番 4～5 を参考に行ってください。

アップグレードパス

[v4.0の場合]

V4.0MR1patch4未満→v4.0MR1patch4にアップグレード

V4.0MR1patch4以上→v4.0MR2Patch6にアップグレード

8 設定情報の引継ぎ(v4.0MR1→v4.0MR2)

注意：下記は 4.0MR1 から 4.0MR2 へアップグレードする際に発生する項目です。

• DLP Rule

DLP 機能は FortiOSv4.0MR2Patch6 にアップグレードする際、sip simple sccp というサブプロトコルの設定が失われる可能性があります。

• System Autoupdate Settings

FortiOSv4.0MR2Patch6 にアップグレードした後、config system autoupdate schedule は、初期値にリセットされます。

以上