Fortigate Firmware VersionUp 手順書

Ver.4.0MR2Patch6→ Ver.4.0MR3Patch1

NVC

NETWORK VALUE COMPONENTS

改訂履歴

初版：2011 年 8 月 22 日

目次

はじめに

本マニュアルは Fortigate の OS バージョンを Version4.0MR2(Patch6)から弊社推奨バージョン Version4.0MR3(Patch1)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 通りが使用されます。

<<アップグレード>>

[WebUI]

設定を引き継ぎつつ OS の Version を上げる事が可能。*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>>

[WebUI]

ほぼ全ての設定が失われますので、ダウングレードはより確実な CLI から行うことをお勧め致します。

[CLI]

工場出荷状態になります。

1. v4.0MR2Patch6 からのアップグレード

v.4.0MR2Patch6未満からv4.0MR3Patch1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v4.0MR2Patch6未満である場合は、一度v4.0MR2Patch6にアップグレードを行なった後v4.0MR3atch1へとアップグレードを行ないます。

以下は、V4.0MR2Patch6へのアップグレード手順書のリンクです。

http://gold.nvc.co.jp/supports/fortinet/OS/FortiOSv4.0MR2p6_rev1.pdf

アップグレードパス

1.v4.0MR2Patch6未満→v4.0MR2Patch6にアップグレード

2.v4.0MR2Patch6→v4.0MR3Patch1 にアップグレード

2. 設定情報の引継ぎ (4.0MR2Patch6→4.0MR3Patch1)

注意：下記は4.0MR2patch6から4.0MR3patch1へアップグレードする際に発生する項目です。

- **DNS Server**

インタフェースの設定にある dns-query recursive/non-recursive オプションは、VDom ごとのシステム設定に移動します。また、FortiOSv4.0MR3Patch1 へのアップグレード後は、config system dns-server にて、このオプションの設定を行なうことが出来ます。(CLI からのみ設定可)

- **Ping Server**

インタフェース設定の Ping Server オプションにある gwdetect は、VDom ごとの router 設定に引き継がれます。FortiOSv4.0MR3Patch1 へのアップグレード後は、config router gwdetect にて、このオプションの設定を行なうことができます。(CLI からのみ設定可)

- **SNMP community**

FortiOSv4.0MR3Patch1 へのアップグレード後、SNMP ホストの IP アドレスをネットマスクで指定できます。

- **AMC slot settings**

FortiOSv4.0MR3Patch1 へのアップグレード後、config system amc-slot で設定されている ips-weight のデフォルト値が balanced から less-fw に変わります。

- **Web filter overrides**

FortiOS v4.0 MR2 Patch4 から FortiOS 4.0MR3Patch1 へアップグレード後、Web フィルタのオーバーライドのコンテンツがなくなります。

- **Firewall policy settings**

送信元インタフェースまたは宛先インタフェイスに、amc-XXX インタフェースを設定している場合、FortiOS 4.0MR3Patch1 へアップグレード後、config firewall poicy の ips センサーのデフォルト値が all_default から default に変わります。

- **URL Filter**

FortiOS 4.0MR3Patch1 へアップグレード後、URL フィルタの action 設定が、Allow、Pass、Expect、Block から Allow、Monitor、 Exempt、 Block に変わります。FortiOS 4.0MR3Patch1 の Allow はログの記録をしません。新しい設定の Monitor は Allow のアクションを行ない、ログを記録します。FortiOS 4.0MR2Patch6 の Pass は、FortiOS 4.0MR3Patch1 の Exempt に吸収されます。また、CLI コマンドが set action pass から set exempt pass に変更となります。

- **FortiGuard Log Filter**

FortiOS 4.0MR3Patch1 へアップグレード後、config log fortiguard filter の設定がなくなります。

- **FortiGurar Log Setting**

FortiOS 4.0MR3Patch1 へアップグレード後、config log fortiguard setting 上の Quotafull や use-hdd オプションがなくなります。

3. Config の保存、リストア

3.1 準備

以下のものを準備する。

- [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)

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 HTTP/HTTPS のアクセスを許可しているポートに、PC を直接またはネットワーク経由で接続する。

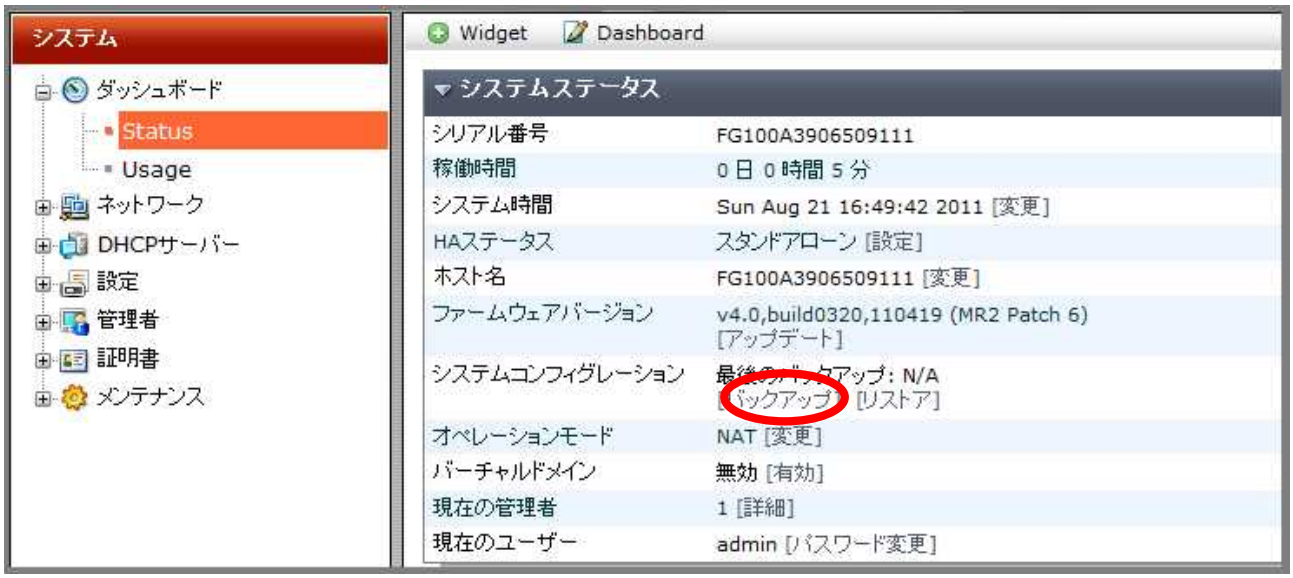
(2) PC のブラウザより FortiGate にアクセスする。

(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。

3.4Config の保存 (OS v4.2.6)

(1) 左上のシステム>>ダッシュボード>>Status にあるバックアップをクリックします。



（Dashboard の status 画面 OSv4.2.6）

(2)　バックアップ画面の”バックアップ”をクリックすると、バックアップがはじまります。

(バックアップ画面　OSv4.2.6)

＊Config のリストア　(OS v4.2.6)

(1)　左上のシステム>>ダッシュボード>>Status にあるリストアをクリックします。

(Dashboard の status 画面　OSv4.2.6)

(2)　ファイル名の右側にある参照をクリックし、リストアするファイルを選択します。

(3)　画面の” 復元”をクリックすると、リストアが始まります。

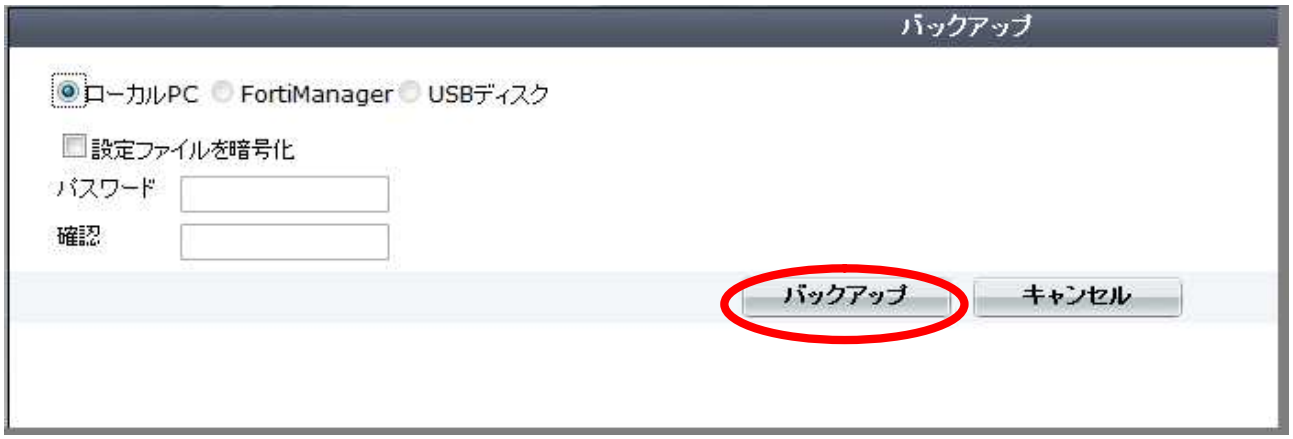
(リストア画面　OSv4.2.6)

3.5 Config **の保存**　(OS v4.3.1)

(3)　**左上のシステム>>ダッシュボード>>Status にあるバックアップをクリックします。**

(Dashboard **の** status **画面**　OSv4.3.1)

(4)　**バックアップ画面の"バックアップ"をクリックすると、バックアップがはじまります。**



(**バックアップ画面**　OSv4.3.1)

＊Config **のリストア**　(OS v4.3.1)

(4)　**左上のシステム>>ダッシュボード>>Status にあるリストアをクリックします。**

(Dashboard **の** status **画面**　OS v4.3.1)

(5)　ファイル名の右側にある参照をクリックし、リストアするファイルを選択します。

(6)　リストア画面の”復元”をクリックすると、リストアが始まります。

(リストア画面　OS v4.3.1)

4. WebUI でのアップグレード

4.1 準備

注意：WebUI でのアップグレードでは基本的に config は保持されますが、必ずバックアップは取得いただくようお願いいたします。
また、全角入力の設定がございますお客様は、別途資料を参照してください。

以下のものを準備します。

- [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

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) 左上のシステム>>ダッシュボード>>Status の中央にある ファームウェアヴァージョンで現在のバージョンを確認します。（図１参照）

(2) 現在の config のバックアップを取得します。(注:p.8 参照)

（図１．バージョン情報確認画面）

(3) ファームウェアバージョン の下にあるアップデートボタンをクリック。(図 2 参照)

(図２．アップデートボタン確認画面)

(4) 画面が切り替わった後アップグレードファイル: 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)

(5) “ 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。

(6) OS v4.0MR3Patch1 のアップグレード後、再ログインをしますと管理画面が変更されます。(図 4 参照)

(7) 手順(1)と同様にして、ファームウェアバージョンの確認を行います。

（図 4．v4.0MR3Patch1 の画面）

(8) **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: 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。
そのため必ずバックアップは取得いただくようお願いいたします。

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)

また、現在の Config の保存を行なう。(注:p.8 参照)

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) execute 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

```
FG100A2906506103 #    execute reboot
This operation will reboot the system !
Do you want to continue? (y/n)y
The system is going down NOW !!
System is rebooting...

FG100A2906506103 #
Please stand by while rebooting thFG100A (19:06-02.28.2006)
Ver:04000003
Serial number:FG100A2906506103
RAM activation
Total RAM: 256MB
Enabling cache...Done.
Scanning PCI bus...Done.
Allocating PCI resources...Done.
Enabling PCI resources...Done.
Zeroing IRQ settings...Done.
Verifying PIRQ tables...Done.
Disabling local APIC...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.
[I]:    Configuration and information.
[Q]:    Quit menu and continue to boot with default firmware.
[H]:    Display this list of options.

Enter G,F,B,I,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_100-v400-build0458-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. v4.0MR2Patch6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. v4.0MR2Patch6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 v4.0MR2Patch6

ForitGate01 # diagnose sys ha status

```
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)
```

出力結果一番下から五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 v4.0MR3Patch1

ForitGate01 # diagnose sys ha status

```
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

v4.0MR1patch9未満からv4.0MR3Patch1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patch9未満の場合は、一度
v4.0MR1patch9にアップグレードを行なった後v4.0MR3Patch1以上へ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

[v4.0MR1Patch9未満の場合]

V4.0MR1Patch9未満→v4.0MR1Patch9にアップグレード

V4.0MR1Patch9以上→v4.0MR3Patch1にアップグレード

8. 設定情報の引継ぎ(v4.0MR1→v4.0MR3)

注意：下記は 4.0MR1 から 4.0MR3 へアップグレードする際に発生する項目です。

• Network Interface Configuration

インタフェース設定で、ips-sniffer-mode が enable で、そのインタフェースが firewall policy に設定されていた場合、FortiOSv4.00 以降の OS から、v4.00MR3Patch1 へアップデートを行ないますと、ips-sniffer-mode の設定は disable に変わります。

• Traffic shaping

v4.00MR3Patch1 にアップデート後に、Traffic shaping の guaranteed-bandwidth,inbandwidth, outbandwidth そして maximum-bandwidth の単位が、kilo-bytes/sec から kilo-bits/sec に変わります。

• System Autoupdate Settings

v4.00MR3Patch1 にアップデート後、config system autoupdate schedule のデフォルト値が disable から enable に変わります。

• DHCP Server

v4.00MR3Patch1 にアップデート後、DHCP Server のホスト名が数字に変わります。また、IP アドレスの範囲を設定が“start-ip” と “end-ip”から“config ip-range”に変わります。

• DNS Server

インタフェースの設定にある dns-query recursive/non-recursive オプションは、VDom ごとのシステム設定に移動します。また、FortiOSv4.0MR3Patch1 へのアップグレード後は、config system dns-server にて、このオプションの設定を行なうことが出来ます。(CLI からのみ設定可)

• Ping Server

インタフェース設定の Ping Server オプションにある gwdetect は、VDom ごとの router 設定に引き継がれます。FortiOSv4.0MR3Patch1 へのアップグレード後は、config router gwdetect にて、このオプションの設定を行なうことができます。(CLI からのみ設定可)

•SNMP community

FortiOSv4.0MR3Patch1 へのアップグレード後、SNMP ホストの IP アドレスをネットマスクで指定できます。

• IPS DoS sensor log setting

v4.00MR3Patch1 の場合、IPS Dos センサーのデフォルトのログ設定のデフォルトが disable です。v4.00MR1 の Patch9 以降の OS で、IPS Dos センサーのログ設定が enable または disable の場合、v4.00MR3Patch1 にアップデート後は、IPS Dos センサーのログ設定は disable になります。

• IPS sensor log setting

v4.00MR3Patch1 の場合、IPS センサーのログ設定のデフォルトは enable です。4.00MR1 の Patch9 以降の OS で、IPS センサーのログ設定が disable の場合は、v4.00MR3Patch1 にアップデート後も disable のままです。v4.00MR1Patch9 または、それ以降の Patch の OS で、IPS センサーのログ設定が、enable または default の場合、v4.00MR3Patch1 にアップデート後は、その設定は enable になります。

• DLP Rule

sip simple sccp が設定されているサブプロトコルの DLP ルールは、v4.00MR3Patch1 にアップデート後に失われます。

• Web Filter & Spam Filter

config 上の FortiGuard の設定で、webfilter-status と spamfilter-status は webfilter-force-off と antispamforce-off に変わります。v4.00MR3Patch1 にアップデート後では、これらの設定のデフォルトの設定は enable です。web filter や spam filter を使用するため、CLI からこの 2 つのエントリーを disable に変更しなければなりません。

変更後の config

```
config system fortiguard
        set webfilter-force-off disable
        set antispam-force-off disable
end
```

• URL Filter

FortiOS 4.0MR3Patch1 へアップグレード後、URL フィルタの action 設定が、Allow、Pass、Expect、Block から Allow、Monitor、 Exempt、 Block に変わります。FortiOS 4.0MR3Patch1 の Allow はログの記録をしません。新しい設定の Monitor は Allow のアクションを行ない、ログを記録します。FortiOS 4.0MR2Patch6 の Pass は、FortiOS 4.0MR3Patch1 の Exempt に吸収されます。また、CLI コマンドが set action pass から set exempt pass に変更となります。

• FortiGuard Log Filter

FortiOS 4.0MR3Patch1 へアップグレード後、config log fortiguard filter の設定がなくなります。

• FortiGurar Log Setting

FortiOS 4.0MR3Patch1 へアップグレード後、config log fortiguard setting 上の Quotafull や use-hdd オプションがなくなります。

以上