Fortigate Ver.4.0MR3Patch12 Information

NVC
NETWORK VALUE COMPONENTS

改訂履歴

発行年月	版 数	改版内容
H25.4	第 1.0 版	初版発行
H25.4	第 1.1 版	OS バージョンの修正

目次

1. はじめに

本マニュアルは Fortigate の OS バージョンを弊社推奨バージョン Version4.0MR3Patch12 へアップグレードを行う際の注意事項について記載しています。

具体的なアップグレード手順については、以下のバージョンアップ手順書を参照ください。

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

Fortigate バージョンアップ手順書

2. アップグレードパス

現在ご利用の OS バージョンによっては、バージョンアップを段階的に行う必要がございます。下記のアップグレードパスをご参照いただき、ご利用バージョンに合わせたバージョンアップ手順を行ってください。

現在の利用バージョン	→	経由バージョン	→	最新バージョン
Version4.0MR3Patch11	→	なし	→	Version4.0MR3Patch12
Version4.0MR3Patch11 未満	→	Version4.0MR3Patch11	→	Version4.0MR3Patch12
Version4.0MR2Patch15	→	なし	→	Version4.0MR3Patch12*1
Version4.0MR2Patch15 未満	→	Version4.0MR2Patch15*2	→	Version4.0MR3Patch12*1
Version4.0MR1Patch9 以上	→	Version4.0MR2Patch15	→	Version4.0MR3Patch12*1

*1: Version4.0MR2 から MR3 にバージョンアップする場合は仕様変更に伴う変換手順が発生します。詳しくは「3.2 仕様の変更」をご参照ください。

*2:現在 Version4.0MR2Patch15 未満から Version4.0MR2Patch15 にバージョンアップを行う手順については、下記資料をご参照ください。

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

3. v4.0MR2 からのバージョンアップ注意事項

注意：下記はv4.0MR2patch15からv4.0MR3patch12へアップグレードする際に発生する項目です。

3.1 config の変更

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、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。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

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

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 フィルタリング overrides

FortiOS v4.0 MR2 Patch4 から FortiOS 4.0MR2Patch14 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ースに、amc-XXX インタフェースを設定している場合、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

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 以降の 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 4.0MR2 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

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

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。

3.2 仕様の変更

文字コードの変更

FortiOS4.0MR3 では FortiGate 内部で使用する文字コードが UTF-8 に統一されました。これに伴い FortiOS4.0MR2 でオブジェクト名に 2 バイト文字を利用している場合、バージョンアップ後に正常に変更されない場合がございます。

安全にアップグレードするために、**FortiOS4.0MR2 で 2 バイト文字をご利用のお客様は、すべての 2 バイト文字を半角英数字に変換してから、アップグレードをおこなってください。**なお、Web フィルタリングの禁止ワードは別途変換作業が発生するため半角英数字に変換する必要はございません。

Web フィルタリング設定方法の変更

FortiOS4.0MR3 では Web フィルタリングのコンテンツブロックが CLI からのみ設定可能となります。これに伴い FortiOS4.0MR2 で WebUI からコンテンツを設定されている場合、バージョンアップ前に config ファイルを取得して内容を修正し、バージョンアップ後に修正済みの config をリストアする作業が必要になります。詳しくは「5.Web フィルタリングコンテンツブロックの config 変換」をご参照ください。

3.3 Fortianalyzer サポートについて

FortiOSv4.0MR3Patch12 は FortiAnalyzerv4.0MR3Patch6 以上をサポートしています。もし、FortiAnalyzer の ver が FortiAnalyzerv4.0MR3 Patch6 未満の場合は、FortiAnalyzerv4.0MR3Patch6 へのアップグレードが必要になります。

アップグレード手順につきましては、下記資料をご参照ください。

http://gold.nvc.co.jp/supports/fortinet/OS/FortiAnalyzer%20VersionUp%20Manual_v436.pdf

4. v4.0MR3 からのバージョンアップ注意事項

注意：下記はv4.0MR3patchXからv4.0MR3Patch12へアップグレードする際に発生する項目です。

4.1 仕様の変更

Historical Report

以下の対象機器にてヒストリカルレポートを保存している場合は、バージョンアップ後にレポートが削除されてしまいます。そのため、バージョンアップ前にヒストリカルレポートをダウンロードして PC のローカルにバックアップしておく必要があります。

対象機器：FortiGate40C, FortiGate60C, FortiGate80C

FG300C Disk Logging

FG300C で v4.0MR3 から v4.0MR3Patch6 のバージョンをご利用の場合に、ディスクロギングに関連する不具合が確認されています。不具合を修正するために、該当機種・バージョンをご利用の場合は、v4.0MR3Patch7 以上のバージョンにアップグレードする際にディスクフォーマットが必要となります。詳しくは「6.FG300C ディスクフォーマット」をご参照ください。

また、FG300C では v4.0MR3Patch7 以上のバージョンにアップグレード後、SQL ロギングはデバイスの RAM サイズに依存します。ログは RAM の最大 10%までを使用し、それを超えると古いログを上書きしていきます。レポート作成もクエリ応答が可能な SQL ログに基づく影響を受けます。

Disk Logging

Fortigate のパフォーマンス最適化のため、FortiOSv4.0MR3Patch12 へのアップグレード後、disk ロギングが無効になります。extended ロギングやレポート機能を使用する場合は、メモリへのロギングまたは、FortiCloud へのロギングを有効にすることを推奨致します。

対象機器は以下の通りです。

- Fortigate40C
- Fortigate60C
- Fortigate80C
- Fortigate80CM
- Fortigate300C (PN: P09616-04 or earlier)
- Fortigate200B　オプションの HDD 非搭載機のみ

SQL logging upgreade limitation
FortiOS v4.0 MR3 Patch12 へアップグレード後、筐体上で利用できる全 RAM 量
容量を元に SQL ロギングを保持します。ログは、RAM の最大 10 パーセントを使用します。一度、閾値を超えた場合、古いログは新しいログに上書きされます。ヒストリカルレポートを生成する場合、クエリによって利用される SQL ログを元に影響を受けます。

対象機器：FG-100D、FG-300C

4.2 Fortianalyzer サポートについて

FortiOS v4.0MR3Patch12 は FortiAnalyzer v4.0MR3Patch6 以上をサポートしています。もし、FortiAnalyzer の ver が FortiAnalyzer v4.0MR3 Patch6 未満の場合は、FortiAnalyzer v4.0MR3Patch6 へのアップグレードが必要になります。

5. Web フィルタリングコンテンツブロックの config 変換

v4.0MR2 では Web フィルタリングのコンテンツブロックの禁止ワードを WebUI から設定した場合 CLI 上では実態参照という表記方法で記載されています。v4.0MR3 以降 Web フィルタリングのコンテンツブロックは仕様変更に伴い CLI からのみ設定可能となりました。そのため CLI 上で解読可能な表記に変更させる必要があります。本項目では、実体参照部分を日本語表記に変換し、設定に反映させる方法を示します。

5.1 準備

作業を行う前に必ず項番 7.4 の(8)で取得した config ファイルのコピーをバックアップとして保存してください。

5.2 config の変換

(1) 項番 7.4 の(8)で取得した config ファイルをテキストエディタを利用して開きます。

(2) 表示された config のテキスト文中の config webfilter content から config webfilter urlfilter の前の end までをコピーします。

```
config webfilter content
    edit 1
        config entries
            edit "&#x30c6;&#x30b9;&#x30c8;"
                set lang japanese
                set status enable
                (省略)
            next
        end
    set name "test"
    next
end
config webfilter urlfilter
```

(図 5-2-2.バックアップファイルの内容)

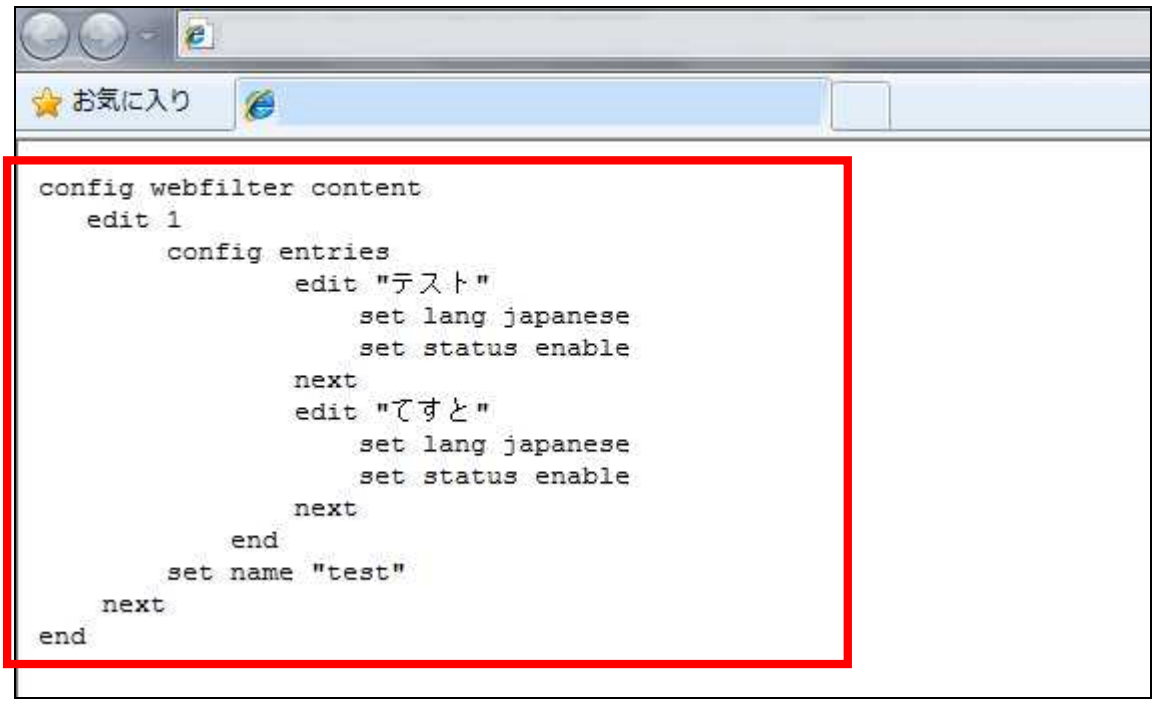
(3) テキストファイルを新規作成し、項番(2)でコピーした部分を貼り付けます。

(4) 項番(3)のファイルの最初の行に<html><body><pre>を、
最後の行に</pre></body></html>を入力します。(図 8-2-4.①、②参照)

```
<html><body><pre>                                    ①
config webfilter content
    edit 1
        config entries
            edit "&#x30c6;&#x30b9;&#x30c8;"
                set lang japanese
                set status enable
                (省略)
            next
        end
    set name "test"
    next
end
</pre></body></html>                                 ②
```

(図 5-2-4.テキストファイルの内容)

(5) 項番(4)で編集したファイルを html ファイルとして保存します。
(6) 項番(5)で保存した html ファイルを開き、表示された文章をコピーします。



(図 5-2-6.Web ブラウザの内容)

(7) 項番(1)の config ファイルの config webfilter content から end の部分を、項番(7)でコピーした部分に置き換えます。変更後は以下のようになります。

```
config webfilter content
    edit 1
        config entries
            edit "テスト"
                set lang japanese
                set status enable
                (省略)
            next
        end
        set name "test"
    next
end
config Web フィルタリング  urlfilter
```

(図 5-2-7.変換後の config ファイル)

(8) 項番(7)で置き換えた config ファイルを、文字コードを UTF-8 に指定して保存します。

(9) 項番(8)で保存した config ファイルを機器にリストアします。5.Config の保存、リストア参照

(10) リストア後に config をバックアップして作業終了です。5.Config の保存、リストア参照

6. FG300C ディスクフォーマット

FG300C で v4.0MR3 から v4.0MR3Patch6 のバージョンをご利用の場合に、ディスクロギングに関連する不具合が確認されています。不具合を修正するためには、該当機種・バージョンをご利用の場合は、v4.0MR3Patch7 以上のバージョンにアップグレードすることと、アップグレードする際にディスクフォーマットを実行することが必要となります。
本項目では、FG300C を v4.0MR3~v4.0MR3Patch6 から v4.0MR3Patch7 以上にバージョンアップする際の手順を示します。

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 (対応ブラウザ情報はアップグレードするバージョンの ReleaseNote をご確認ください。)
- アップグレードするファームウェアファイル
- シリアルケーブル (FortiGate に付属)

ディスクのフォーマットに伴い以下のものをバックアップします。

- config (Fortigate バージョンアップ手順書　3.コンフィグのバックアップ、リストア　を参照してください)
- 過去に作成したレポート
- ログファイル (「6.3 ログファイルのバックアップ」を参照してください。)

6.2 GUI 接続

(1) FG の HTTP/HTTPS のアクセスを許可しているインタフェースに、PC を直接またはネットワーク経由で接続します。

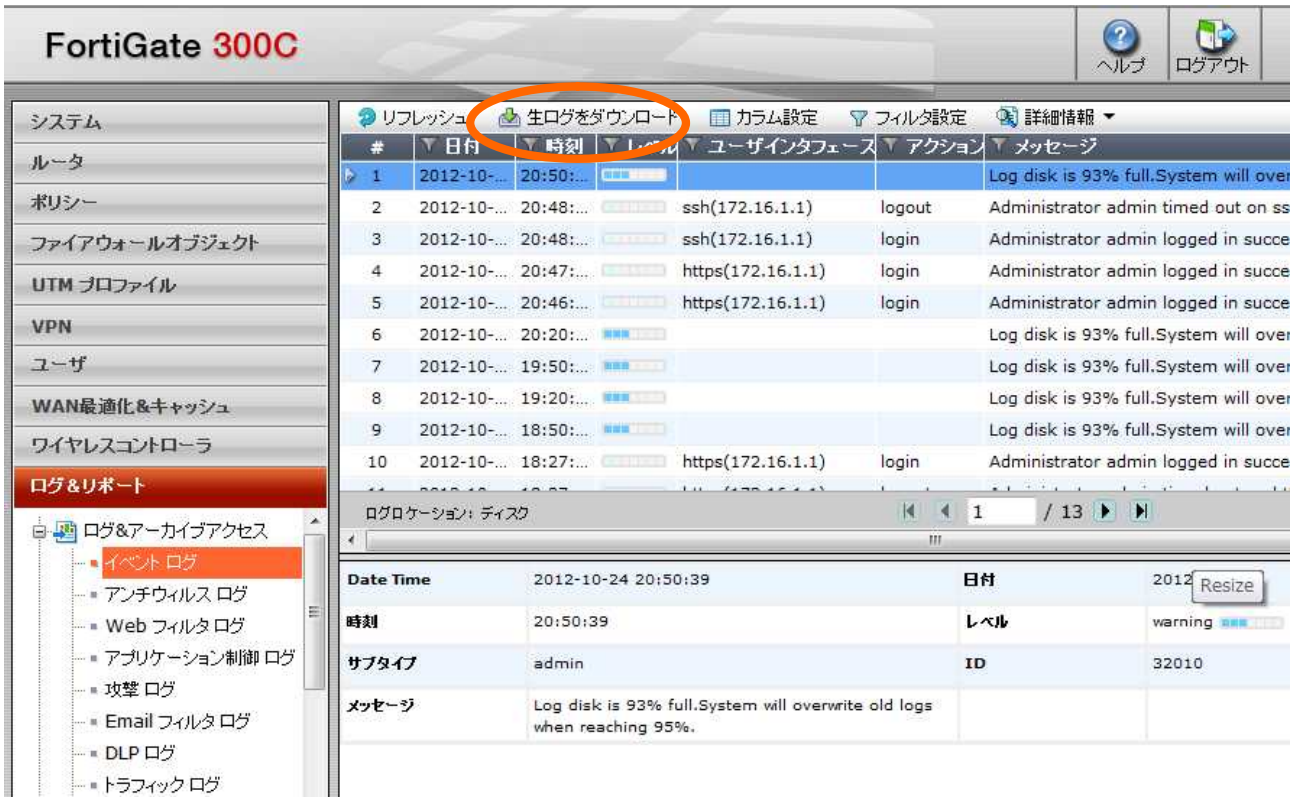
(2) PC のブラウザにて FortiGate にアクセスします。
(ブラウザに URL https://xxx.xxx.xxx.xxx もしくは http://xxx.xxx.xxx.xxx を指定します。x は FortiGate の IP アドレスを指定します。)

(3) ログイン画面が表示されるので、ユーザー名・パスワードを入力してログインをクリックします。

6.3 ログファイルのバックアップ

ディスクのフォーマットを行うとディスクに保存されているログが削除されるため、必要な場合はログファイルのバックアップを行います。

(1) ログ&リポート > ログ&アーカイブアクセス > イベントログを表示し、「生ログをダウンロード」をクリックして PC にログファイルを保存します。



(図 6-3-1.ログ画面)

(2) その他のログファイルに関しても、(1)と同様の手順で取得します。

6.4 ネットワークからの切り離し

ディスクフォーマット時に config も削除されるため、Fortigate をネットワークから切り離します。

6.5 WebUI でのアップグレード

Fortigate のインタフェースに PC を直接接続し、Fortigate バージョンアップ手順書の「4. WebUI でのアップグレード」を実行します。

6.6 config のバックアップ

Fortigate バージョンアップ手順書の「3. Config のバックアップ、リストア」を参照し、バックアップを実行します。

6.7 と 6.8 の作業は、Fortigate バージョンアップ手順書の「5. CLI でのアップグレード、ダウングレード」の手順の途中でフォーマットを実行する流れとなります。

6.7 ディスクフォーマット(OS 領域)

Fortigate バージョンアップ手順書の「5. CLI でのアップグレード、ダウングレード」から「5.4 アップグレード、ダウングレード」の(2)まで実行してから以下の手順を実行します。

(1) 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 F を入力し、
All data will be erased,continue:[Y/N]? と表示されるので Y を入力します。

```
Enter G,F,B,I,Q,or H: ←F を入力

All data will be erased,continue:[Y/N]? ←Y を入力
Formatting boot device...
.............................
Format boot device completed.
```

6.8 CLI でのアップグレード

Fortigate バージョンアップ手順書の「5.4 アップグレード、ダウングレード」の(3)~(8)を実行します。

6.9 ディスクフォーマット(Log 領域)

CLI でログインした状態で以下の手順を実行します。

(1) execute formatlogdisk コマンドを実行します。再起動が発生します。

```
FG300C3911602818 # execute formatlogdisk
Log disk is /dev/sda1.
Formatting this storage will erase all data on it, including
   logs, quarantine files;
and require the unit to reboot.
Do you want to continue? (y/n)y

Formatting the requested disk(s) and rebooting, please wait...
Formatting the disk...
- unmounting /data2 :   ok
- unmounting /var/log :   ok
- unmounting /var/storage/FLASH2-38AD707D21A52A84 :   ok
Formatting /dev/sda1 ... done

The system is going down NOW !!
```

6.10 config のリストア

Fortigate バージョンアップ手順書の「3. Config のバックアップ、リストア」を参照し、リストアの手順を実行します。

6.11 ネットワークへの接続

Fortigate をネットワークに接続します。

(1) 実通信に問題が発生していないことを確認します。
アップグレード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の修正または切り戻しを行います。

(2) アンチウィルス、IPS をご利用されている場合は、exe update-now コマンドにより最新シグネチャのアップデートを実行します。

補足：SQL ロギングの無効化

FG300C ではディスクロギングに関連する不具合の発生に伴い、Fortigate でのレポート作成機能をご利用されない場合は SQL ロギング設定を無効にすることを推奨しております。以下に手順を示します。

(1) GUI にログイン後、ログ＆リポート > ログ環境設定 > ログ設定 を表示し、Enable SQL Logging のチェックマークを外し、「適用」をクリックします。

(図 6-12-1.SQL ロギング設定画面)

(2) この設定変更を行うと、GUI へのログイン時に SQL ロギング設定を有効にするように促す警告画

面が表示されますが、「Go」をクリックするとSQLロギングが有効の設定に戻ってしまうので、クリックしないように注意してください。

（図 6-12-2.ログイン後警告画面）

以上