FortiGateVer.6.0 MR4 Patch5

Information 資料

株式会社ネットワークバリューコンポネンツ
NETWORK VALUE COMPONENTS

目次

1. はじめに

本マニュアルは FortiGate の OS バージョンを弊社提供バージョンの Ver6.0 MR4 Patch5 へアップグレードする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、以下の手順書を参照ください。
https://gold.nvc.co.jp/document/fortinet/tech/tech_doc/FortiGate アップグレード手順書.pdf

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サイトをご参照いただき、ご利用バージョンに合わせたアップグレード手順を行ってください。

https://docs.fortinet.com/upgrade-tool
※FortiOS 5.2.9 以前の OS からアップグレードする際は、一度 5.2.9 までアップグレード頂いた後、アップグレードパスに従いバージョンアップを実施ください。

3. サポート機種

FortiOS Ver6.0 MR4 Patch5 をサポートしている機種は下記の通りです。

機器シリーズ	機器
FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-101E, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG‑300D, FG-300E, FG-301E, FG‑400D, FG‑400E, FG‑401E, FG‑500D, FG‑500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG‑900D, FG-1000D, FG-1100E, FG-1101E, FG‑1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG‑3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG‑3810D, FG-3815D, FG-5001D, FG-3960E, FG‑3980E, FG-5001E, FG‑5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

3.1 Special branch supported models

以下のモデルは、FortiOS 6.0 MR4 Patch5 の特別ブランチでリリースされています。 正しいビルドを実行されていることを確認するには、CLI コマンド「get system status」を実行して、Branch point フィールドに該当のビルド番号が表示されていることを確認します。

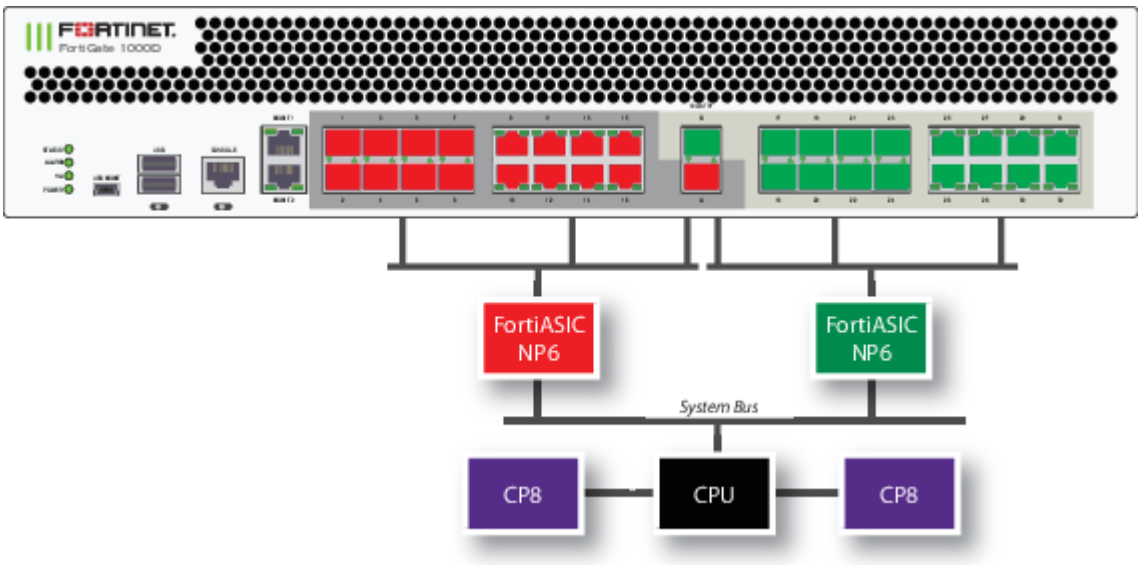
機種	ビルド番号
FG-80F	is released on build 5656.
FG-80F-BP	is released on build 5656.
FG-81F	is released on build 5656.
FG-100F	is released on build 5651.
FG-101F	is released on build 5651.
FG-200F	is released on build 5653.
FG-201F	is released on build 5653.
FGR-60F	is released on build 5654
FGR-60F-3G4G	is released on build 5654

4. アップグレード注意事項

4.1 CAPWAP traffic offloading

入力インタフェースと出力インタフェースが異なる NP6 チップ上にある場合、CAPWAP トラフィックは NP にオフロードされません。以下のモデルが影響を受ける可能性がございます。

機器シリーズ	対象機器
FortiGate シリーズ	FGT-900D, FGT-1000D, FGT-2000E, FGT-2500E



FortiGate-1000D の SPU 配置

4.2 FortiClient (Mac OS X) SSL VPN requirements

Mac OS X 10.8 で SSL VPN を使用するときは、FortiOS で SSLv3 を有効にする必要があります。

4.3 Use of dedicated management interfaces (mgmt1 and mgmt2)

最適な安定性を得るために、管理トラフィック専用の管理ポート（mgmt1 および mgmt2）を使用してください。 一般のトラフィック処理用途で管理ポートを使用しないでください。

4.4 Tags option removed from GUI

タグオプションは GUI から削除されます。これには次のものが含まれます。
・「システム > タグ」ページを削除
・「タグ」セクションがすべてのページから削除
・「タグ」カラムがあったすべてのページから削除

4.5 System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	・[システム]> [詳細]メニューを削除しました（ほとんどの機能を[システム]> [設定]ページに移動しました） ・構成スクリプトのアップロード機能をトップメニュー>構成>スクリプトページに移動しました。 ・自動スクリプト構成の GUI サポートを削除しました（この機能は引き続き CLI でサポートされます)。 ・すべてのコンプライアンステストをセキュリティレーティングテストに変換しました。

4.6 PCI passthrough ports

Bug ID	Description
605103	PCI パススルーポートの順序は、アップグレード後に変更される場合があります。 SR-IOV ポートはデフォルトで MAC オーダーであるため、これは VMXNET3 および SR-IOV ポートには影響しません。

4.7 FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.1 はバグ 570575 を解決し、ポートに電力を供給できない FortiGate を修正しました。 解決された問題のセクションを参照してください。ただし、PoE ハードウェアコントローラーでは、CLI を使用して実行する必要のある更新が必要になる場合があります。 このコマンドが正常に実行されると、PoE ハードウェアコントローラーのファームウェアが最新バージョン 2.18 に更新されます。

diagnose poe upgrade-firmware

4.8 AWS-On-Demand image

Bug ID	Description
589605	FortiOS 6.4.0 以降、FGT-VM64-AWSONDEMAND イメージは提供されなくなりました。 AWSPAYG モデルと AWSBYOL モデルの両方が、同じ FGT-VM64-AWS イメージを共有します。

4.9 Azure-On-Demand image

Bug ID	Description
657690	FortiOS 6.4.3 以降、FG-VM64-AZUREONDEMAND イメージは提供されなくなりました。Azure PAYG モデルと Azure BYOL モデルはどちらも、アップグレードと新しい展開のために同じ FG-VM64-AZURE イメージを共有します。アップグレードする前に、構成をバックアップしてください。

4.10 FortiClient EMS Cloud registration

FortiOS 6.4.3 は、FortiClient EMS クラウドサービスをサポートします。ユーザは 2020 年 12 月中旬にサービスを登録して使用できるようになります。

4.11 SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 および 6.4.3 は、strong-crypto で有効になっている場合、TLS1.0 のサポートを終了しました system global。この変更により、TLS 1.0 を介した SSL トラフィックはチェックされないため、デフォルトでバイパスされます。

TLS 1.0 トラフィックを調べたりブロックしたりするには、管理者は次のいずれかを実行できます。

config system global で strong-crypto を無効にします。FortiOS の 6.2.6 と 6.4.3 またはそれ以降のバージョンに適用されます。
config firewall ssl-ssh-profile：
FortiOS の 6.2.6 以降では、set unsupported-ssl を block にします。
FortiOS の 6.4.3 以降では、set unsupported-ssl-negotiation を block にします。

4.12 Policy routing enhancements in the reply direction

応答トラフィックが FortiGate に入り、ポリシールートまたは SD-WAN ルールが設定されている場合、出力インタフェースは次のように選択されます。
・構成システム設定で補助セッションが有効になっている場合
6.4.0 以降、応答トラフィックは、出力インタフェースとネクストホップを決定するためのポリシールートまたは SD-WAN ルールと一致しなくなります。
この変更の前は、応答トラフィックは、出力インタフェースとネクストホップを決定するためにポリシールートまたは SD-WAN ルールと一致します。
・構成システム設定で補助セッションが無効になっている場合
応答トラフィックは、元の着信インタフェースで出力されます。

5. Changes in CLI

以下の内容が変更されています。

Bug ID	Description
640488	ブロックリスト、許可リスト、外部リソースなどのリソースを処理するために、FortiGate のプロキシで最大メモリ使用量を設定するオプションが追加されます。 config system global set proxy-resource-mode {enable|disable} end
666855	FortiOS は、RSA-PSS シリーズの署名アルゴリズムを使用したクライアント証明書の検証がサポートされます。しかしながら特定のクライアントで問題が発生します。 クライアント認証に関連する署名アルゴリズムを制御するための属性が追加されます（TLS 1.2 にのみ影響します)。 config vpn ssl settings set client-sigalgs {no-rsa-pss | all} end
682561	get system instance-id コマンドが追加されます。

6. Change in default behavior

以下の内容が変更されています。

Bug ID	Description
598614	SSL VPN 認証ルールでグループと user-peer が指定されていて、同じグループが複数のルールに表示されている場合、各グループと user-peer の組み合わせを個別に照合できようになります。
669018	Web フィルターブロック/警告ページでのフォーティネット URL 評価送信のリンクが https://globalurl.fortinet.net に更新されます。
673609	auto-join fortiCloud リトライタイマーが 600 秒から 60 秒に変更されます。

7. Change in table size

以下の内容が変更されています。

Bug ID	Description
665668	IPIP トンネルテーブルのサイズを VDOM あたり 256 およびグローバルで 512 から VDOM あたり 1024 およびグローバルで 1024 に増やされます。 ・FG-3xxxE シリーズ: 400,000 に増加します。

8. New features or enhancements

以下の内容が変更されています。

Bug ID	Description
658206	新しい REST API POST /api/v2/monitor/vpn/ike/clear？mkey = <gateway_name>は、vpn ike ゲートウェイのクリアを診断するのと同じ方法で IKE SA トンネルを停止します。
660596	先行標準の POE デバイスは一般的ではないため、poe-pre-standard-detection はデフォルトで無効に設定されています。以前のビルドからアップグレードすると、構成された値が引き継がれます。
661105	session-sync-dev を使用してセッション同期処理をカーネルにオフロードすることにより（さまざまな最適化を使用）、4 メンバーの FGSP セッション同期をサポートして重い負荷を処理できます。
667285	NAC ポリシーを設定する場合、デバイスに一致する MAC アドレスを手動で指定すると便利な場合があります。 MAC アドレスのワイルドカードは、*文字を指定することでサポートされます。
673371	ローカルインターフェイスで ICMP タイプ 13 がサポートされます。
676484	汎用 DDNS サービスプロバイダーを DDNS サーバとして構成する場合、サーバータイプとアドレスタイプを IPv6 に設定できます。これにより、FortiGate は IPv6 DDNS サーバに接続し、更新用に FortiGate の IPv6 インターフェイスアドレスを提供できます。 config system ddns edit <name> set ddns-server genericDDNS set server-type {ipv4 | ipv6} set ddns-server-addr <address> set addr-type ipv6 {ipv4 | ipv6} set monitor-interface <port> next end
677334	SSL VPNOS チェックで MacOS Big Sur11.1 のサポートが追加されます。
677684	ADVPN を介して作成されたショートカットを持つハブアンドスポーク SD-WAN トポロジでは、ダウンまたはリカバリされたショートカットが、SD-WAN サービスストラテジーによって選択されるメンバーに影響を与える可能性があります。 SD-WAN hold-down-time により、ダウンしたショートカットトンネルが復旧し、ショートカットがサービスストラテジー式に追加されたときに、ホールドダウン時間が経過するまでショートカットが優先度低で保持されます。
680599	ICMP レート制限を上げて、FortiGate が 1 秒あたりにより多くの ICMP エラーメッセージを送信できるようになります。 ICMP レート制限が 1 秒（100 jiffies）から 10 ミリ秒（1 jiffy）に変更されます。
690179	ヘルスチェックと SLA ログ用の SD-WAN REST API は、結果に ADVPN ショートカット情報を公開するようになります。 child_intf 属性は、対応するショートカットの統計を返します。 ADVPN ショートカットのリアルタイム SLA 情報を表示する CLI コマンドも追加されます。

	# diagnose sys sdwan sla-log <health check name> <sequence number> <child name>
691411	Log & Report > Events > SDN Connector Events logs で、動的アドレス関連のイベントの EMS ログが記録されていることを確認します。 ・EMS タグを追加 ・EMS タグを更新 ・EMS タグを外す
697675	管理対象の FortiSwitch の最大数を 8 から 16 に増えます。

9. アップグレードに関して

9.1 Device detection changes

FortiOS 6.0 ではデバイス検知機能に以下の構成が含まれています。
・Visibility：検出された情報は、トポロジの可視性とロギングに利用できます。
・FortiClient endpoint compliance：FortiClient から学習した情報を使用して、これらのエンドポイントのコンプライアンスを実施できます。
・Mac-address-based device policies：検出されたデバイスは、カスタムデバイスとして定義し、デバイスベースのポリシーで使用できます。

FortiOS 6.2 では以下のように変更されます。
・Visibility：変更はありません。
・FortiClient endpoint compliance：新しいファブリックコネクタに置き換わります、動的ポリシーのために他のすべてのエンドポイントコネクタと整合します。（FortiClient EMS）
・Mac-address-based device policies：FW アドレスに Mac アドレス範囲が設定できるようになります。これにより、以前のデバイスポリシー機能は、通常のポリシーで実現できるようになります。
6.0.x でデバイスポリシーを使用していた場合は、アップグレード後にこれらのポリシーを通常のポリシーテーブルに手動で移行する必要があります。
6.2.0 にアップグレードした後：

1. デバイスごとに MAC ベースのファイアウォールアドレスを作成します。
2. アドレスを通常の IPv4 ポリシーテーブルに適用します。

6.4.0 では、デバイス検出に関連する GUI 機能が再配置されました。

1. デバイスセクションは、ユーザと認証（以前のユーザとデバイス）からダッシュボードのウィジェットに移動しました。
2. メールコレクションの監視ページが監視 からダッシュボードのウィジェットに移動しました。

6.4.4 では、デバイスを右クリックすると、新しいサブオプションである Delete が追加されました。このオプションは、デバイスがオンラインの場合、またはデバイスが FortiClient から取得されている場合は使用できません。

9.2 FortiClient Endpoint Telemetry license

FortiClient Endpoint Telemetry License が廃止され、FortiClient EMS に統合されます。

9.3 Security Fabric upgrade

Fortinet Security Fabric を構成している場合、以下の OS がサポート対象となります。

機器	OS
FortiAnalyzer	FortiAnalyzer 6.4.1
FortiManager	FortiManager 6.4.1
FortiClient	FortiClient 6.4.1
FortiClient EMS	FortiClient EMS 6.4.0
FortiAP	FortiAP 6.4.0 以降
FortiSwitch	FortiSwitch 6.4.1 以降

※複数の FortiGate で Security Fabric 構成されている場合、ファブリック内のすべての FortiGate デバイスは同一である必要がございます。

9.4 Minimum version of TLS services automatically changed

セキュリティを向上させるために、FortiOS 6.2.0 は ssl-min-proto-version オプション（config system global）を使用して、FortiGate とサードパーティの SSL および TLS サービス間の通信に使用される最小 SSL プロトコルバージョンを制御するようになっております。
FortiOS 6.0 MR4 Patch5 以降にアップグレードした場合、デフォルトの ssl-min-proto-version オプションは TLS v1.2 になります。
以下の SSL および TLS サービスは、デフォルトとして TLS v1.2 を使用するためにグローバル設定を継承します。 これらの設定は個別の設定で上書き可能です。

・Email server (config system email-server)
・Certificate (config vpn certificate setting)
・FortiSandbox (config system fortisandbox)
・FortiGuard (config log fortiguard setting)
・FortiAnalyzer (config log fortianalyzer setting)
・LDAP server (config user ldap)
・POP3 server (config user pop3)

9.5 Downgrading to previous firmware versions

以前のファームウェアバージョンにダウングレードすると、すべてのモデルで設定が失われます。 以下の設定のみ保持されます。

・operation mode
・interface IP/management IP
・static route table
・DNS settings
・admin user account
・session helpers
・system access profiles

9.6 Amazon AWS enhanced networking compatibility issue

この拡張機能では、5.6.2 以前のバージョンの AWS 用 FortiGate VM との互換性の問題があります。 FortiOS 6.0 MR4 Patch5 イメージを 5.6.2 以前のバージョンにダウングレードすると、ネットワーク接続が失われます。 AWS はコンソールアクセスを提供しないため、ダウングレードされたイメージを復元することはできません。
FortiOS 6.0 MR4 Patch5 から 5.6.2 以前のバージョンにダウングレードする場合、拡張 NIC ドライバーの実行は許可されません。 次の AWS インスタンスが影響を受けます。

C5 / C5d / C5n / F1 / G3 / G4 / H1 / I3 / I3en / Inf1 / m4.16xlarge / M5 / M5a / M5ad / M5d / M5dn / M5n / P2 / P3 / R4 / R5 / R5a / R5ad / R5d / R5dn / R5n / T3 / T3a / u-6tb1.metal / u-9tb1.metal / u-12tb1.metal / u-18tb1.metal / u-24tb1.metal / X1 / X1e / z1d

回避策は、インスタンスを停止し、タイプを非 ENA ドライバーNIC に変更することです。

9.7 FortiLink access-profile setting

新しい FortiLink ローカルアクセスプロファイルは、FortiGate によって管理される FortiSwitch の物理インタフェースへのアクセスを制御します。FortiGate を 6.4.0 にアップグレードすると、すべての管理対象 FortiSwitch のインタフェースの allowaccess の設定が、デフォルトの FortiGate ローカルアクセスプロファイルによって上書きされます。6.4.0 にアップグレードした後、ローカルアクセスプロファイルにプロトコルを手動で追加する必要があります。
■ローカルアクセスプロファイルを設定する場合

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
```

```
        set internal-allowaccess https ping ssh
    next
end
```

■ローカルアクセスプロファイルを管理対象の FortiSwitch に設定する場合

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

9.8 FortiGate VM with V-license

FortiOS6.2 から V ライセンスを備えた FortiGate-VM で Split-vdom が有効にできます。

■split-vm の有効方法

```
config system global
    set vdom-mode [no-vdom | split vdom]
end
```

※split-vdom の詳細については https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/744923/split-task-vdom-mode-support をご確認ください。

9.9 FortiGuard update-server-location setting

FortiGuard のシグネチャアップデート等で利用される FortiGuard サーバに接続する際に、update-server-location のデフォルト設定は、ハードウェアプラットフォームと VM で異なります。ハードウェアプラットフォームの場合、デフォルトは any です。 VM の場合、デフォルトは usa となります。
遅延を少なくするためには手動で「any」に設定頂く必要があります。

```
config system fortiguard
    set update-server-location [usa | any]
end
```

9.10 FortiView widgets

モニターウィジェットは、スタンドアロンのダッシュボードとして保存できます。
デフォルトのダッシュボード設定には、次の 2 つのタイプがあります。
Optimal：6.4.1 のデフォルトのダッシュボード設定

Comprehensive：6.4.1 より前のデフォルトのモニターおよび FortiView 設定

フィルタリングファセットは、フルスクリーンモードおよびスタンドアロンモードの FortiView ウィジェットで使用できます。

9.11 WanOpt configuration changes in 6.4.0

ポート設定はプロファイルプロトコルオプションで行われます。 HTTPS 設定は、ファイアウォールポリシーで certificate inspection の設定する必要があります。
FortiOS 6.4.0 では、set ssl-ssh-profilecertificate-inspection をファイアウォールポリシーに追加する必要があります。

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

9.12 WanOpt and web cache statistics

WanOpt と Web キャッシュの統計は、モニターからダッシュボードのウィジェットに移動しました。

9.13 IPsec interface MTU value

IPsec インタフェースは、6.2 からのアップグレード後に異なる MTU 値を計算する場合があります。
この変更により、アップグレード後に OSPF ネイバーが確立されなくなる可能性があります。 回避策は、OSPF インタフェースの設定で有効になるように mtu-ignore を設定することです。

Interface 設定：

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

9.14 HA role wording changes

マスターという用語はプライマリに変更され、スレーブはセカンダリに変更されました。この変更は、すべての HA 関連の CLI コマンドと出力に適用されます。唯一の例外は、VRRP に関連する出力であり、変更されません。

9.15 Virtual WAN link member lost

mgmt インタフェースがアップグレード前に dedicated-to management の設定されている場合、virtual-wan-link のメンバーはアップグレード後に失われます。

9.16 Enabling match-vip in firewall policies

FortiOS 6.4.3 以降 match-vip、アクションが受け入れに設定されている場合、ファイアウォールポリシーでは許可されません。

10. 各 Fortinet 製品とのサポートについて

10.1 FortiAnalyzer

FortiAnalyzerとFortiOSの互換性については、下記ページに最新情報がございます。
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/0955b58b-a143-11eb-b70b-00505692583a/fortianalyzer-compatibility_-_caveats.pdf

※FortiGate のアップグレード前に FortiAnalyzer のアップグレードを行う必要がございます。

10.2 FortiManager

FortiManagerとFortiOSの互換性については、下記ページに最新情報がございます。
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/61c2bba0-a142-11eb-b70b-00505692583a/fortimanager-compatibility_-_caveats.pdf
FortiOS 6.4.1は、FortiManager6.4.1以降で動作させる必要があります。

※FortiGate のアップグレード前に FortiManager のアップグレードを行う必要があります。

10.3 FortiClient

FortiClient と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiClient for Windows	FortiClient 6.4 FortiClient Endpoint Telemetry ライセンスおよびフォーティネットセキュリティファブリックのアップグレードの重要な互換性情報を参照してください。
FortiClient for MacOS X	FortiClient 6.4 FortiClient Endpoint Telemetry ライセンスおよびフォーティネットセキュリティファブリックのアップグレードの重要な互換性情報を参照してください。
FortiClient for Linux	FortiClient for Linux は、Ubuntu 16.04 以降、Red Hat 7.4 以降、および CentOS7.4 以降でサポートされています。 FortiClient を IPsecVPN または SSLVPN にのみ使用している場合は、FortiClient バージョン 6.0 以降がサポートされています。
FortiClient for iOS	FortiClient 6.4.0 以降
FortiClient for Android and VPN Android	FortiClient 6.4.0 以降

※FortiOS のリリース時点での情報ですので、FortiClient の Release Notes も合わせてご確認ください。

10.4 FortiSwitch

FortiSwitch (FortiLink モード)と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiSwitch (FortiLink)	3.6.9 以降

※FortiOS のリリース時点での情報ですので、FortiSwitch の Release Notes も合わせてご確認ください。

10.5 FortiAP/FortiAP-S

FortiAP および FortiAP-S と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiAP	5.4.2 以降
	5.6.0 以降
FortiAP-S	5.4.3 以降
	5.6.0 以降

※FortiOS のリリース時点での情報ですので、FortiAP/FortiAP-S の Release Notes も合わせてご確認ください。

10.6 FortiSandbox

FortiSandbox と FortiOS の互換性は以下の通りです。

プラットフォーム	OS バージョン
FortiSandbox	2.3.3 以降

※FortiOS のリリース時点での情報ですので、FortiSandbox の Release Notes も合わせてご確認ください。

11. 動作環境

11.1 推奨 Web ブラウザについて

FortiGate の WebUI を表示する際の推奨ブラウザとなります。

プラットフォーム	OS バージョン
Microsoft Edge	Version 88
Mozilla Firefox	Version 85
Google Chrome	Version 88

他の Web ブラウザは正しく機能する可能性がありますが、Fortinet ではサポートされていません。

11.2 Explicit Web Proxy のブラウザサポートについて

FortiGate の Explicit Proxy 機能を利用する際のサポートブラウザの一覧です。

プラットフォーム	OS バージョン
Microsoft Edge	Version 44
Mozilla Firefox	Version 74
Google Chrome	Version 80

他の Web ブラウザは正しく機能する可能性がありますが、Fortinet ではサポートされていません。

11.3 SSL-VPN (Web モード)のサポートについて

FortiGate の SSL-VPN(Web モード)でサポートされているブラウザの一覧です。

プラットフォーム	ブラウザバージョン
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 85 Google Chrome version 88
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 85 Google Chrome version 88
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 68
macOS Big Sur 11.0	Apple Safari version 13 Mozilla Firefox version 85 Google Chrome version 88
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

11.4 VM プラットフォーム

FortiGate-VM の動作可能なプラットフォームとなります。

プラットフォーム	ブラウザバージョン
Citrix	Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1(Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	Windows Server 2012R2 with Hyper-V role Windows Hyper-V Server 2019
Open Source	XenServer version 3.4.3 XenServer version 4.1 and later
VMware	ESX versions 4.0 and 4.1 ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0
VM Series - SR-IOV 次の NIC チップセットカードがサポートされています。	Intel 82599 Intel X540 Intel X710/XL710