DATA SHEET

FortiOS 無線 LAN コントローラ

今日の組織は、急速に普及している IoT デバイス、要求の厳しいモバイルやリモートワーカー、進化し続けるセキュリティの脅威などによって、ネットワーク環境の高度化が進み、多くの課題に直面しています。フォーティネットのセキュア無線 LAN コントローラには、FortiGate ネットワークセキュリティプラットフォームの基盤を形成する専用のネットワークセキュリティオペレーティングシステムである、FortiOS が統合されています。このソリューションにより、無線 LAN のセキュリティ ドリブン ネットワーキングが実現します。

セキュリティ ファブリック統合

フォーティネットのセキュア無線ソリューションがフォーティネット セキュリティ ファブリックの一部となることで、脆弱性が最も多く存在する有線 / 無線ネットワークのエッジまでの協調型のセキュリティポリシーによる保護が可能になります。

優れたパフォーマンス

最新の無線標準、FortiLink によるエッジでの統合セキュリティ、5 GHz 無線へのクライアントステアリング、アプリケーション制御のすべてのサービスの組み合わせにより、最高レベルのパフォーマンスとユーザーエクスペリエンスを実現します。

エンドツーエンドの無線 LAN セキュリティ

コントローラからアクセスポイントまでの統合セキュリティサービスにより、ネットワーク、クライアント、アプリケーションを保護します。

ハイライト

- Wi-Fi 6 FortiAP をサポート
- 1 ～ 8,000 台以上までアクセスポイントを拡張可能
- SD ブランチ、教育機関、医療機関、サービス業向けの柔軟な導入モデル
- セキュリティと管理を統合
- 小売業店舗向けの PCI コンプライアンス機能
- Web キャプティブポータルによるゲストアクセス統合管理
- BYOD デバイスのフィンガープリント認証と制御
- 無線 LAN IDS 機能と不正アクセスポイント管理を統合
- スペクトル分析

ハイライト

主な機能と特長

拡張性と耐障害性	高い拡張性を備え、一元的に管理されるエンタープライズ無線 LAN であり、無線リソースの統合管理により、無線チャネルの干渉を緩和し、一貫した無線 LAN パフォーマンスをもたらします。
統合セキュリティ機能	有線セキュリティ機能を無線 LAN に拡張し、1 つのコンソールで有線 / 無線両方の管理を一括で行えるようにして、「簡潔でわかりやすい」ネットワーク管理インタフェースをもたらします。
レイヤー 7 アプリケーションの可視化	SPU ベースの詳細なパケット検証テクノロジーを搭載し、市場をリードする機能を活用して、細部にわたるアプリケーションレベルの可視化と制御を実現します。

Intra-SSID Privacy 機能を備えたセキュア無線ネットワーク、第三者機関に認証された強固な認証セキュリティ、高度なネットワーク機能へのニーズは、かつてないほど重視されています。FortiOS エンタープライズクラス無線 LAN コントローラは、セキュリティ、無線、ネットワークの業界で最も包括的なサービススイートで、フォーティネットの専用 SPU（セキュリティプロセッシングユニット）が実現するハードウェアアクセラレーションと使いやすいエンタープライズ無線ソリューションを 1 つの統一プラットフォームで提供します。

卓越した柔軟性で、導入に関するすべてのニーズに対応

無線インフラストラクチャは高い柔軟性と拡張性を備えている必要があります。セキュリティ機能と無線ネットワーク機能を統合することで、フォーティネットのセキュアな無線 LAN コントローラは、ネットワークの複雑さを大幅に緩和し、結果的に TCO を削減します。VLAN を使用しないフォーティネットのアプローチは、複雑なレイヤー 2 の要件を緩和して、ネットワーク全体に VLAN 情報を伝達する必要をなくし、拡張性に優れた大規模な導入を簡素化して加速させます。どのようなネットワークの規模であっても、FortiGate の多様なモデルから最適な FortiGate ソリューションを選択できます。

集中セキュリティ管理

有線 / 無線のセキュリティ機能を統合して一元的に管理することで、マルチベンダーネットワークのトラブルシューティングにおける複雑さを回避し、マルチベンダー製品に伴う高コストのトレーニングと認定を不要にし、運用コストの削減と IT 担当者の作業負荷の軽減を実現します。運用コストの削減に加え、クライアント、アクセスポイント、スイッチ、セキュリティのサービスの一元的かつ完全な可視化を実現し、セキュリティと制御の一貫性あるポリシーの全社的な適用が可能になります。

高度なアプリケーション制御

無線帯域幅は、貴重な共有媒体であるため、無線 LAN でのビジネスアプリケーションの優先順位付けは非常に重要です。FortiOS アプリケーション制御機能が無線 LAN コントローラに組み込まれており、4,000 以上のアプリケーションシグニチャによる詳細なレイヤー 7 検証を使用して、重要なアプリケーションの帯域幅保証と優先順位付けを可能にします。業界をリードするこのアプリケーション制御機能により、無線 LAN を最適な状態で稼働し、目的のアプリケーションに利用されるようにするために必要とされる、きめ細かなアプリケーション制御が実現します。

業界をリードするセキュリティ

FortiOS は、統合脅威管理（UTM）から発展したものです。フォーティネットは業界規格の認定数で他ベンダーを圧倒しており、さまざまなセキュリティサービスが組み込まれたクラス最高の統合保護を提供します。アンチウイルスから、Web コンテンツのフィルタリング、アプリケーション制御、ネットワーク IPS、E メールフィルタリング、DLP に至るまで、有線ネットワークに適用していたものと同様のセキュリティ機能を、無線 LAN にも適用できるようになりました。標準実装された無線侵入検知システム機能により、次のような多数の無線周波数侵入手法を検知することで、無線 LAN の保護が強化されます。

- アソシエーション / 認証 / EAPOL フラッディング
- De-authentication ブロードキャスト
- 偽造された MAC
- アドホックネットワークの検知と阻止
- 無線ブリッジの検知
- 正しく構成されていないアクセスポイントの検知
- MAC OUI のチェック

自動化された不正アクセスポイントの検知と抑止

不正なアクセスポイントがあると、クレジットカード情報などの機密データが漏洩する脆弱性がネットワークに生じ、ネットワークセキュリティの深刻な脅威が引き起こされます。このため、PCI DSS を始めとするデータセキュリティ基準では、大抵、不正アクセスポイントのプロアクティブな監視と抑止が義務付けられています。FortiGate の不正アクセスポイントのオンワイヤ検知エンジンでは、さまざまな相関手法を使用して、不正アクセスポイントがネットワークに接続されているかどうかを判断します。この自動プロセスは、不明なアクセスポイントを継続的に監視し、承認されていないことが検知されたアクセスポイントがあった場合は、自動的に抑止します。

ハイライト

バンドステアリング

バンドステアリングは、クライアントを最も効率的にサービスを提供できる周波数帯に切り替えることで、利用可能な無線ネットワークの効率的な使用を可能にします。FortiOS では、周波数帯の能力に基づき、ユーザーが周波数帯をクライアントに割り当てることができます。バンドステアリングを利用しないと、デュアルバンドのクライアントが 2.4 GHz または 5 GHz のいずれかのチャンネルに割り当てられる可能性があり、デバイスがどちらを優先するかによって片方のチャンネルに割り当てが集中してしまう恐れがあります。バンドステアリングを利用すると、このトラフィックの一部をユーザーが選択した周波数帯に割り当てることができます。バンドステアリングのもう 1 つの例として、デバイスを重要度（またはネットワークで通過するトラフィックのタイプの重要度）によって分離することができます。優先度の低いプロファイルのクライアントをすべて 2.4 GHz チャンネルに残し（帯域幅が問題にならない場合）、クライアントを 5 GHz 帯に移動することで、高いデータレートを実現します。

無線リソースの自動プロビジョニング

FortiOS の DARRP（Distributed Automatic Radio Resource Provisioning）テクノロジーにより、無線インフラストラクチャは最大のパフォーマンスを発揮するよう常に最適化されます。この高度な機能が備わったフォーティネットのアクセスポイントは、近隣のアクセスポイントからの干渉、ノイズ、信号がないか無線周波数環境を継続的に監視し、ネットワーク上の各アクセスポイントについて、最適な無線周波数のパワーレベルを FortiGate 無線 LAN コントローラで判断できるようにします。新しいアクセスポイントがプロビジョニングされる際にも、管理者の手を煩わせることなく、DARRP によって最適なチャネルが選択されます。

キャプティブポータル

ゲストユーザー向けのブラウザベースの認証も、SSL 対応のキャプティブポータル経由でサポートされています。この組み込みのキャプティブポータルにより、HTML ログインページのカスタマイズのほか、統合ゲスト管理ポータルを使用したゲストアカウントのプロビジョニングや管理も可能になります。FortiOS は、ユニバーサルアクセスメソッド（UAM）もサポートしており、サードパーティの外部キャプティブポータルサーバーとの統合や、FortiToken ワンタイムパスワード（OTP）ソリューションによる二要素認証を可能にしています。

デバイスフィンガープリンティング

デバイスフィンガープリンティングは、ネットワークに接続するデバイスに関するさまざまな属性の収集を可能にします。収集された属性により、個々のデバイスのクライアントの OS、デバイスタイプ、使用しているブラウザーなどを完全または部分的に識別できるようになります。デバイスフィンガープリンティングで、より多くの情報をステーションに提供することができるため、システム管理者が利用されているデバイスのタイプを把握し、必要であれば対策を講じることができます。

スペクトル分析

既存の AP 無線を使用してスペクトル分析を実行することで、エリア内の干渉デバイスの把握に役立つ詳細な RF 情報を入手することができます。信号干渉、スペクトラグラム、干渉源リストなどのさまざまなグラフを表示することができます。

完成されたセキュアな無線 LAN アーキテクチャー

- Web キャプティブポータル、802.1x、一時的なゲストアクセス
- ユーザー / デバイスの識別、承認
- ユーザー / デバイスベースのポリシー、アプリケーション制御
- 不正アクセスポイントの排除、無線侵入検知
- ユーザー / アプリケーションベースの無線 QoS
- ネットワーク / 脅威の詳細な可視化、コンプライアンスレポート作成

技術仕様

無線 LAN コントローラ	
ネットワーキング	
Bonjour ゲートウェイ	アップルの Bonjour プロトコルの監視と制御が可能
DHCP	統合型 DHCP サーバー
VLAN	インタフェースおよびトランク
	SSID と VLAN のマッピング
	VLAN の動的なサポート
ルーティング	静的 / 動的 / ポリシーベースルーティング
	RIP、OSPF、BGP のサポート
マルチキャスト	PIM モード
	マルチキャストからユニキャストへの変換
データのフォワーディング	集中型 : FortiGate へのトンネリング、VLAN なし
	分散型 : ローカルでブリッジ
	分割ポリシーベース : リソース、ポリシーに基づく選択的フォワーディング
プロビジョニングと管理	
管理アクセス	Web ブラウザ経由の HTTPS
	SSH、Telnet、およびコンソール
	SNMP（V1 および V2）
管理の可用性	1+1 の高可用性（HA）のサポート
	HA モードでヒットレスフェイルオーバー
監視	アクセスポイント（周波数、チャネル）: ステータス、使用状況、使用率
	クライアントの監視 : 信号強度、SNR、ユーザー名、IP、デバイスタイプ、ファイアウォールポリシー、帯域幅の使用量、アプリケーションの可視化
	不正アクセスポイント
	階層化メッシュ接続
	無線状況の監視、クライアントのトレンド、オーバーロードのアクセスポイント、過剰無線周波数エラー
	API で位置情報の取得が可能
一元管理	有線 / 無線やセキュリティの構成 / 監視の一元管理
	FortiManager による数千ヵ所の拠点の一元管理
	FortiAnalyzerによる数千ヵ所の拠点の一元的なレポート作成や、ネットワークの分析およびトレンド
トラブルシューティング	リモート無線パケットのキャプチャ
リモートアクセスポイント	
リモートアクセスポイント（テレワーカー）のサポート	FAP の全モデルでサポート
	FortiGate 無線コントローラに FAP をリモートで導入可能（WAN リンク経由）
	オプションでデータトラフィックを暗号化
	分割ルーティング : ポリシーに基づく選択的フォワーディング（FortiOS 5.2）
WAN のサバイバビリティ	無線 LAN コントローラに接続できない場合でも、無線クライアントの接続を維持
トラブルシューティング	ローカル FAP 診断用 Web ポータル
メッシュおよびブリッジング	
トポロジ	マルチホップメッシュ
	マルチメッシュインスタンスのサポート
メッシュホップ	最大ホップ数を構成可能
ブリッジ	ポイントツーポイントのブリッジング
	無線 ISP アプリケーション向けのポイントツーマルチポイントのブリッジング
管理	FortiGate Web インタフェースを使用

無線 LAN コントローラ	
無線アクセスと認証	
アクセス：認証方法	IEEE 802.1X（EAP、Cisco-LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-SIM、EAP-AKA）
	RFC 2716（PPP EAP-TLS）
	RFC 2865（RADIUS 認証）
	RFC 3579（EAP の RADIUS サポート）
	RFC 3580（IEEE 802.1X RADIUS ガイドライン）
	RFC 3748（拡張認証プロトコル）
	WEP64 : 64 ビットの WEP
	WEP128 : 128 ビットの WEP
	WPA（Wi-Fi Protected Access）パーソナルおよびエンタープライズ（M-PSK（Multiple PreShared Keys）のサポートを含む）
	WPA2（パーソナルおよびエンタープライズ）: 802.11i 規格
	MAC アドレス認証
	RADIUS 経由の MAC アドレス認証
	BYOD 向けの証明書ベース認証
認証サーバー	内部データベース、RADIUS、LDAP、TACACS+
	外部認証サーバー : Microsoft Active Directory、Microsoft IAS RADIUS サーバー、Cisco ACS サーバー、FreeRADIUS、Interlink RADIUS サーバー、Steel Belted Radius
暗号化プロトコル	CCMP/AES
	TKIP
	TKIP+AES
	DTLS
	L2TP/IPSec（RFC 3193）
	XAUTH/IPSec
VPN	SSL
	IPSec
キャプティブポータル	内部または外部認証サーバーに対する認証
	ブランド、グラフィックス、言語など、フルカスタマイズ可能なルック & フィール
	免責事項ページ
	複数のキャプティブポータルページ
	外部キャプティブポータルにフォワード
	認証後に Web サイトにリダイレクト
ゲストユーザー管理	統合型レセプショニストゲストユーザーの管理ポータル
	使用期限を構成可能
	開始時刻を構成可能
	一括アカウント作成
	FortiAuthenticator との統合で、E メールベースのセルフサービスキャプティブポータル対応

技術仕様

無線 LAN コントローラ	
無線周波数およびパフォーマンスの管理	
DARRP（Distributed Automatic Radio Resource Provisioning）DARRP スケジューリング	一貫性のある最適なパフォーマンスを達成するための無線周波数チャネルの自動選択
	構成可能（有効 / 無効）
	オプションでタイムスロットを除いて有効化
バンドステアリング	インテリジェントなロードバランスで 5 GHz の無線周波数バンドにステアリングすることで、最適なパフォーマンスと干渉緩和を実現
アクセスポイントのロードバランシング	利用可能なチャネルでアクセスポイント全体にわたってクライアントを均等に分散
自己修復	障害が発生したアクセスポイントを補うために、自動的に TX パワーレベルを調整して無線到達範囲を拡大
スペクトル分析	環境の干渉要因を把握する
不正アクセスポイント管理	
バックグラウンドスキャン	不正アクセスポイントのバックグラウンドでのフルタイムスキャン
オンワイヤの相関手法	オンワイヤの相関手法で、ローカルネットワークに接続されている悪意のあるアクセスポイントを特定
不正の抑止	自動 / 手動の抑止機能向けの構成可能オプション
	有害なアクセスポイントの無線による抑止、および特定された不正アクセスポイントにクライアントが接続しないようにする対策
無線 IDS	複数の無線周波数侵入手法を検知してログに記録
イベントログ	不正アクセスポイントの全イベントの Syslog
監査	FortiAnalyzer で生成される、PCI-DSS コンプライアンス向けの事前構成済みレポート
BYOD およびモビリティ	
デバイスのアイデンティティ	会社の資産と従業員所有のデバイスを区別
	デバイスタイプ、ベンダー情報、OS タイプ、OS バージョンを特定して分類
アプリケーションの可視性	4,000 以上のシグニチャをサポートするレイヤー 7 のアプリケーション検知
	アプリケーションの検知、優先順位付け、抑止が可能
サービス品質（QoS）	エンドツーエンドの QoS
	アプリケーションのポリシーベースの再タグ付け
	有線 / 無線ネットワーク全体で QoS タグを維持
	無線を使用するビジネスクリティカルアプリケーションの送信を優先
ポリシー管理	デバイスおよびユーザー ID に基づくファイアウォールおよびトラフィックシェーピングのポリシーを管理および適用
802.11kvr のサポート	よりインテリジェントにローミングを判断することで高速ローミングを実現
	802.11i の高速ロームバック
	802.11i の事前の高速アソシエート
	PMK キャッシング
プレゼンス検知	プレゼンスアナリティクスのためのプレゼンス検知

無線 LAN コントローラ	
IPv6 のサポート	
クライアントのサポート	IPv6 クライアントをサポート
管理	IPv6 を使用した管理：IPv6 ノードとして動作するよう FortiGate をサポート
トラフィック	ルーティングプロトコル、ファイアウォール、UTM のサポート
ファイアウォール	ICSA ファイアウォールのエンタープライズ認定
	ICSA IPv6 対応ファイアウォール
	USGv6 対応ファイアウォール
業界標準	
Wi-Fi Alliance	WPA Personal、WPA Enterprise、WPA2 Personal、WPA2 Enterprise、WPA3-Enterprise、WPA3-Personal、WMM、WMM Power Save、Wi-Fi Agile Multiband、Wi-Fi CERTIFIED 6、Wi-Fi CERTIFIED ac、Wi-Fi CERTIFIED a/b/g/n、Wi-Fi Enhanced Open
IEEE 標準コンプライアンス	802.11ax、802.11a、802.11b、802.11d、802.11g、802.11k、802.11n、802.11r、802.11v、802.11w、802.11ac、802.1Q、802.3ad、802.3af、802.3at、802.3az、802.11ax、802.3bz
その他の RF テクノロジー	
	Bluetooth ビーコン対応
	Hanshow および SES-imagotag の ESL（電子棚札）システムのサポート

技術仕様

RFC	
BGP	
RFC 7911	Advertisement of Multiple Paths in BGP
RFC 4724	Graceful Restart Mechanism for BGP
RFC 4456	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC 4360	BGP Extended Communities Attribute
RFC 4271	A Border Gateway Protocol 4 (BGP-4)
RFC 2918	Route Refresh Capability for BGP-4
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2439	BGP Route Flap Damping
RFC 1997	BGP Communities Attribute
RFC 1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC 1772	Application of the Border Gateway Protocol in the Internet

RFC	
DHCP	
RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 2132	DHCP Options and BOOTP Vendor Extensions
RFC 2131	Dynamic Host Configuration Protocol
Diffserv	
RFC 3260	New Terminology and Clarifications for Diffserv
RFC 2597	Assured Forwarding PHB Group
RFC 2475	An Architecture for Differentiated Services
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

RFC	
暗号化	
RFC 6954	Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 8031	Curve25519 and Curve448 for the Internet Key Exchange Protocol Version 2 (IKEv2) Key Agreement
RFC 7634	ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec
RFC 7627	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension
RFC 7539	ChaCha20 and Poly1305 for IETF Protocols
RFC 7427	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
RFC 7383	Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 7027	Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)
RFC 6989	Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 6290	A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE)
RFC 6023	A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)
RFC 5723	Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption
RFC 5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
RFC 4635	HMAC SHA TSIG Algorithm Identifiers
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
RFC 4478	Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7
RFC 2845	Secret Key Transaction Authentication for DNS (TSIG)
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2085	HMAC-MD5 IP Authentication with Replay Prevention
RFC 1422	Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
RFC 1321	The MD5 Message-Digest Algorithm
PKCS #12	PKCS 12 v1: Personal Information Exchange Syntax

技術仕様

RFC	
DNS	
RFC 6895	Domain Name System (DNS) IANA Considerations
RFC 6604	xNAME RCODE and Status Bits Clarification
RFC 6147	DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
RFC 4592	The Role of Wildcards in the Domain Name System
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4033	DNS Security Introduction and Requirements
RFC 3597	Handling of Unknown DNS Resource Record (RR) Types
RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 3007	Secure Domain Name System (DNS) Dynamic Update
RFC 2308	Negative Caching of DNS Queries (DNS NCACHE)
RFC 2181	Clarifications to the DNS Specification
RFC 2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
RFC 1995	Incremental Zone Transfer in DNS
RFC 1982	Serial Number Arithmetic
RFC 1876	A Means for Expressing Location Information in the Domain Name System
RFC 1706	DNS NSAP Resource Records
RFC 1183	New DNS RR Definitions
RFC 1101	DNS Encoding of Network Names and Other Types
RFC 1035	Domain Names - Implementation and Specification
RFC 1034	Domain Names - Concepts and Facilities
ICMP	
RFC 6918	Formally Deprecating Some ICMPv4 Message Types
RFC 6633	Deprecation of ICMP Source Quench Messages
RFC 4884	Extended ICMP to Support Multi-Part Messages
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 1191	Path MTU Discovery
RFC 792	Internet Control Message Protocol IP
RFC 5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
RFC 4301	Security Architecture for the Internet Protocol
RFC 3272	Overview and Principles of Internet Traffic Engineering
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP
RFC 2072	Router Renumbering Guide
RFC 2071	Network Renumbering Overview: Why would I want it and what is it anyway?
RFC 1918	Address Allocation for Private Internets
RFC 1123	Requirements for Internet Hosts -- Application and Support
RFC 1122	Requirements for Internet Hosts -- Communication Layers
RFC 791	Internet Protocol
IP マルチキャスト	
RFC 4604	Using Internet Group Management Protocol Version 3 (IGMPv3 and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC 3973	Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)
RFC 3956	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
RFC 3306	Unicast-Prefix-based IPv6 Multicast Addresses
RFC 2365	Administratively Scoped IP Multicast
RFC 1112	Host Extensions for IP Multicasting
IPSec	
RFC 4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

RFC	
IPv4	
RFC 6864	Updated Specification of the IPv4 ID Field
RFC 5177	Network Mobility (NEMO) Extensions for Mobile IPv4
RFC 4632	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
RFC 3927	Dynamic Configuration of IPv4 Link-Local Addresses
RFC 3021	Using 31-Bit Prefixes on IPv4 Point-to-Point Links
RFC 1812	Requirements for IP Version 4 Routers
IPv6	
RFC 6343	Advisory Guidelines for 6to4 Deployment
RFC 5175	IPv6 Router Advertisement Flags Option
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 4862	IPv6 Stateless Address Autoconfiguration
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
RFC 4193	Unique Local IPv6 Unicast Addresses
RFC 4007	IPv6 Scoped Address Architecture
RFC 3971	SEcure Neighbor Discovery (SEND)
RFC 3596	DNS Extensions to Support IP Version 6
RFC 3587	IPv6 Global Unicast Address Format
RFC 3493	Basic Socket Interface Extensions for IPv6
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 3053	IPv6 Tunnel Broker
RFC 2894	Router Renumbering for IPv6
RFC 2675	IPv6 Jumbograms
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2185	Routing Aspects Of IPv6 Transition
RFC 1752	The Recommendation for the IP Next Generation Protocol IS-IS
RFC 5310	IS-IS Generic Cryptographic Authentication
RFC 5308	Routing IPv6 with IS-IS
RFC 3359	Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
LDAP	
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 3494	Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status
NAT	
RFC 7857	Updates to Network Address Translation (NAT) Behavioral Requirements
RFC 6888	Common Requirements for Carrier-Grade NATs (CGNs)
RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
RFC 5508	NAT Behavioral Requirements for ICMP
RFC 5382	NAT Behavioral Requirements for TCP
RFC 4966	Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status
RFC 4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
RFC 4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
RFC 3948	UDP Encapsulation of IPsec ESP Packets
RFC 3022	Traditional IP Network Address Translator (Traditional NAT)

技術仕様

RFC	
OSPF	
RFC 6860	Hiding Transit-Only Networks in OSPF
RFC 6845	OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type
RFC 5340	OSPF for IPv6
RFC 4812	OSPF Restart Signaling
RFC 4811	OSPF Out-of-Band Link State Database (LSDB) Resynchronization
RFC 4203	OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
RFC 3630	Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 3623	Graceful OSPF Restart
RFC 3509	Alternative Implementations of OSPF Area Border Routers
RFC 3101	The OSPF Not-So-Stubby Area (NSSA) Option
RFC 2328	OSPF Version 2
RFC 1765	OSPF Database Overflow
RFC 1370	Applicability Statement for OSPF
PPP	
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2364	PPP Over AAL5
RFC 1661	The Point-to-Point Protocol (PPP)
RADIUS	
RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2548	Microsoft Vendor-specific RADIUS Attributes
RIP	
RFC 4822	RIPv2 Cryptographic Authentication
RFC 2453	RIP Version 2
RFC 2080	RIPng for IPv6
RFC 1724	RIP Version 2 MIB Extension
RFC 1058	Routing Information Protocol
SIP	
RFC 3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3261	SIP: Session Initiation Protocol
SNMP	
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4273	Definitions of Managed Objects for BGP-4
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 2863	The Interfaces Group MIB
RFC 2578	Structure of Management Information Version 2 (SMIv2)

RFC	
SNMP	
RFC 1238	CLNS MIB for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)
RFC 1215	A Convention for Defining Traps for use with the SNMP
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1212	Concise MIB Definitions
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1156	Management Information Base for Network Management of TCP/IP-based internets
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets SSH
RFC 4254	The Secure Shell (SSH) Connection Protocol
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol
RFC 4252	The Secure Shell (SSH) Authentication Protocol
RFC 4251	The Secure Shell (SSH) Protocol Architecture
RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers SSL
RFC 6176	Prohibiting Secure Sockets Layer (SSL) Version 2.0
RFC 6101	The Secure Sockets Layer (SSL) Protocol Version 3.0 TCP
RFC 6691	TCP Options and Maximum Segment Size (MSS)
RFC 6298	Computing TCP's Retransmission Timer
RFC 6093	On the Implementation of the TCP Urgent Mechanism
RFC 793	Transmission Control Protocol
TLS	
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3
RFC 7858	Specification for DNS over Transport Layer Security (TLS)
RFC 6347	Datagram Transport Layer Security Version 1.2
RFC 6066	Transport Layer Security (TLS) Extensions: Extension Definitions
RFC 5746	Transport Layer Security (TLS) Renegotiation Indication Extension
RFC 5425	Transport Layer Security (TLS) Transport Mapping for Syslog
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 4681	TLS User Mapping Extension
RFC 4680	TLS Handshake Message for Supplemental Data VPN
RFC 4761	Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
RFC 4684	Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
RFC 4577	SPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements Wireless
RFC 5415	Control and Provisioning of Wireless Access Points (CAPWAP)
RFC 5416	Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
RFC 5417	CAPWAP Access Controller DHCP Option
RFC 8110	Opportunistic Wireless Encryption (OWE)

技術仕様

RFC	
その他のプロトコル	
RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2) For RFC 7540, only flow mode is supported; proxy mode is not yet supported.
RFC 5424	The Syslog Protocol
RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4960	Stream Control Transmission Protocol
RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
RFC 3376	Internet Group Management Protocol, Version 3
RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4960	Stream Control Transmission Protocol
RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
RFC 3376	Internet Group Management Protocol, Version 3
RFC 2890	Key and Sequence Number Extensions to GRE
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 2661	Layer Two Tunneling Protocol "L2TP"
RFC 2637	Point-to-Point Tunneling Protocol (PPTP)
RFC 2412	The OAKLEY Key Determination Protocol
RFC 2225	Classical IP and ARP over ATM
RFC 2033	Local Mail Transfer Protocol
RFC 1413	Identification Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
RFC 1011	Official Internet Protocols
RFC 959	File Transfer Protocol (FTP)
RFC 826	Echo Protocol
RFC 783	The TFTP Protocol (Revision 2)
RFC 768	User Datagram Protocol
-	The TACACS+ Protocol

RFC	
その他	
RFC 7348	Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
RFC 4784	Verizon Wireless Dynamic Mobile IP Key Update for cdma2000(R) Networks for cdma2000(R) Networks
RFC 4470	Minimally Covering NSEC Records and DNSSEC On-line Signing
RFC 3985	Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 2979	Behavior of and Requirements for Internet Firewalls
RFC 2827	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
RFC 2780	IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers
RFC 2647	Benchmarking Terminology for Firewall Performance
RFC 2644	Changing the Default for Directed Broadcasts in Routers
RFC 2231	MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations
RFC 1945	Hypertext Transfer Protocol -- HTTP/1.0
RFC 950	Internet Standard Subnetting Procedure
RFC 894	A Standard for the Transmission of IP Datagrams over Ethernet Networks

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ