

FortiAnalyzer

セキュリティファブリックのログ管理と相関分析

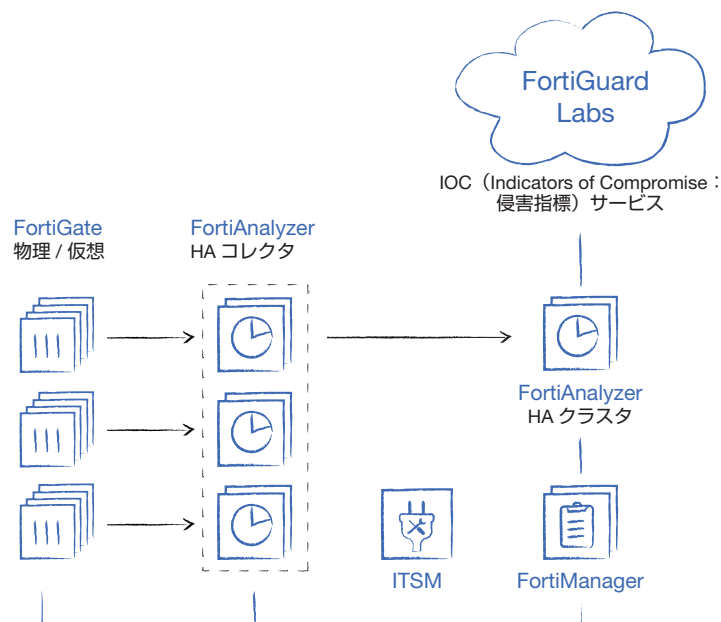
FortiAnalyzer は、**オーケストレーション、オートメーション、レスポンスの一元化**によって、攻撃対象領域全体のリスクを軽減し、組織全体のセキュリティを強化します。

フォーティネット セキュリティ ファブリックに FortiAnalyzer を統合することで、攻撃対象領域の拡大につながった新しいテクノロジーの分析や監視の複雑さが軽減され、**エンドツーエンドの可視性**によって脅威の特定と排除が容易になります。

高度な脅威の検知と相関付け：セキュリティやネットワークの担当者は、インフラストラクチャ全体のネットワークセキュリティの脅威を直ちに識別し、対応することができます。

ワークフローとコンプライアンスレポートの自動化：セキュリティとネットワーク両方の担当者がカスタマイズ可能なダッシュボード、レポート、高度ワークフローハンドラーを利用できるため、ワークフローの高速化と、法規制やコンプライアンスの監査が容易になります。

拡張性を備えたログ管理：FortiGate、FortiClient、FortiManager、FortiSandbox、FortiMail、FortiWeb、FortiAuthenticator、Syslog などからログを収集します。単体ユニットとして導入できるほか、特定のオペレーションや保持の要件に合わせて最適化することもできます。



主な機能と特長

セキュリティ ファブリックの分析

- すべてのログを網羅するイベントの相関付けとリアルタイムのアノマリ検知を実現するとともに、IOC (Indicators of Compromise : 侵害指標) サービスおよび脅威の検知を通じて脅威対策に要する時間を短縮

フォーティネット セキュリティ ファブリック統合

- FortiClient、FortiSandbox、FortiWeb、FortiMailのログを相関付けることで、ネットワークの細部まで可視化し、重要で実用的なインテリジェンスを提供

エンタープライズクラスの高可用性

- 地理的に分散するFortiAnalyzer DBの自動バックアップ (最大4ノードクラスター) によって、ディザスタリカバリに対応

セキュリティの自動化

- REST API、スクリプト、コネクタの自動化、さらにオートメーションステッチ (ワークフローの自動化) を活用して複雑さを解消し、迅速なセキュリティレスポンスを実現

マルチテナント / 管理ドメイン (ADOM)

- ADOMを活用して顧客データを分離し、ドメインを管理することで、コンプライアンスと効率的なオペレーションを実現

柔軟な導入オプションとアーカイブ用ストレージ

- アプライアンス、VM、ホスティング型、またはクラウドの導入オプションをサポートし、AWS、Azure、またはGoogleを2次ストレージとして使用し、ログをアーカイブ

ハイライト

セキュリティオペレーションセンター (SOC)

FortiAnalyzer の SOC は、実用的なビュー、通知、レポートの形でリアルタイムのログと脅威データを提供し、セキュリティチームによるネットワークの保護を支援します。一元的な監視、脅威やイベント、ネットワークのアクティビティの把握が可能となるため、アナリストはネットワーク、Web サイト、アプリケーション、データベース、データセンター、およびその他のテクノロジーの保護が容易になります。事前定義済み / カスタマイズされたダッシュボードを使用して一元管理が可能となり、セキュリティ ファブリックへの容易な統合が実現します。新しい FortiAnalyzer SOC サービス サブスクリプションは、ブレイックとコネクタによるインシデント管理ワークフローが組み込まれており、セキュリティの自動化とオーケストレーションの強化によってセキュリティアナリストによる作業を簡素化します。

インシデントの検知とレスポンス

FortiAnalyzer の自動化されたインシデントレスポンス機能を活用することで、セキュリティチームは単一のビューからインシデントのライフサイクル管理できます。アナリストは、デフォルトあるいはカスタマイズしたイベントハンドラーを利用して、迅速な検知や自動的な相関付け、接続されたフォーティネット製デバイスおよび syslog サーバーの修正が可能になると同時に、インシデント管理機能やブレイックによってインシデントを迅速に割り当てて分析できるため、イベント管理や侵害されたエンドポイントの特定に注力可能になります。監査履歴やインシデントレポートによってタイムラインやアーティファクトの追跡が可能になると同時に、ITSM プラットフォームとの効率的な統合を通じてお客様のセキュリティオペレーションセンターにおけるギャップが解消されるとともに、セキュリティ態勢が強化されます。

The screenshot displays the FortiAnalyzer interface for incident monitoring. On the left, there is a navigation pane with categories like 'All Security Events', 'Compromised Hosts', 'High Risk App Usage', and 'Malicious Domain/URL Access'. The main area shows a table of events with columns for ID, Event, Event Status, Event Type, Count, Severity, Last Update, Additional Info, and Handler. One event is highlighted: 'Rudy Dawson Laptop' with a severity of 'Critical' and a count of 152. Below the event list, details for the 'Rudy Dawson Laptop' are shown, including its IP address (172.16.100.92.10), MAC address (00:15:00:0a:0f:cb), and operating system (Linux LUBUNTU 16.04).

FortiAnalyzer ブレイック

FortiAnalyzer ブレイックは、セキュリティチームの作業を簡素化し、重要なタスクに注力することが可能になります。すぐに活用できるブレイックテンプレートが提供されているため、SOC アナリストは調査のユースケースを迅速にカスタマイズして自動化し、侵害されたホストや重大な不正侵入に対するレスポンス、C&C の IP のブロックなどを実行できます。また、ブレイックエディターを使用して、調査中のホストへのレスポンスを柔軟に変更できます。FortiAnalyzer では、アナリストがブレイックをドリルダウンしてタスク実行の詳細を確認したり、ブレイックを編集してカスタムプロセスやタスクを定義したりできます。また、FortiOS や EMS をはじめとするセキュリティファブリックの他のデバイスとの連携を可能にするブレイック用コネクタも組み込まれています。

IOC (Indicators of Compromise : 侵害指標)

IOC (Indicators of Compromise : 侵害指標) サービスは、ネットワークやオペレーティングシステムで観察される不審な使用や痕跡を特定し、コンピュータへの侵入を高い確度で判断します。FortiGuard の IOC サブスクリプションによって提供されるインテリジェンス情報を利用することで、セキュリティアナリストはこのような侵害の痕跡に基づいてリスクのあるデバイスやユーザーを特定できます。約 50 万件もの IOC で構成される IOC パッケージが毎日作成され、Fortinet Developers Network (FNDN) 経由で FortiSIEM、FortiAnalyzer、FortiCloud の各製品に配信されます。アナリストは、過去のログを再スキャンして脅威を追跡したり、新しいインテリジェンスに基づいて脅威を特定したりできるだけでなく、IP アドレス、ホスト名、グループ、OS、脅威の総合評価、ロケーションマップビュー、そして脅威の数を基準に集計された、ユーザーの脅威スコアを確認できます。

The screenshot shows the FortiAnalyzer dashboard with two circular gauges. The first gauge shows '787 Total Users' and the second shows '7131 Total Endpoints'. Below the gauges is a table with columns: Endpoint Name, Users, MAC Address, IP Address, Hardware/OS, Vulnerabilities, Network Location, and Last Update. The table lists several endpoints, including 'VAN-200427-NB', 'Addison Medina Laptop', 'Van-200739-NB', 'VAN-iPhone-7', and 'kevinwilliams', each with associated user names, MAC and IP addresses, and vulnerability counts.

アセットとアイデンティティ

セキュリティ ファブリックにおけるアセットとアイデンティティの監視と脆弱性の追跡機能により、SOC は完全な可視性と攻撃対象領域の分析が可能になります。アセットとアイデンティティが可視化され、NAC のテレメトリに基づいてアセットが分類されます。ログの収集、正規化、相関付けを自動化する SIEM モジュールを内蔵しているほか、FortiSOAR との統合によって、インシデントのさらなる調査と脅威の根絶が可能になります。FortiAnalyzer Connector や API Admin を利用した FortiSOAR のインシデントデータのエクスポートもサポートしています。

レポート

FortiAnalyzer には 39 以上のテンプレートが用意されており、サンプルレポートの中から最適なレポートをすばやく指定できます。レポート機能を利用することで、ログから独自のデータレポートを生成できます。オンデマンドのレポートだけでなく、スケジュールに基づく E メール通知やアップロードの自動化にも対応しており、カレンダー表示による容易な管理が可能です。700 以上のチャートとデータセットを内蔵しており、PDF、HTML、CSV、XML などのレポートフォーマットを柔軟に利用して、独自のカスタムレポートを作成できます。

ハイライト

SD-WAN の監視

SD-WAN ダッシュボードでは、イベントハンドラーによる SD-WAN アラートの検知によるリアルタイムの通知とアクションが可能になるため、お客様は複数の WAN インタフェースに SD-WAN を適用するメリットを直ちに実感できます。履歴グラフでは WAN リンクの状態を監視することが可能で、ジッター、遅延、およびパケットロスに関して、深刻度が「critical」と「high」の SD-WAN アラートを確認できます。セキュア SD-WAN の新しいレポートでは、SD-WAN の重要な指標の概要、アプリケーション別の SD-WAN リンク使用率、遅延、パケットロス、ジッターの変化、そして SD-WAN パフォーマンスの統計の詳細チャートと履歴グラフが表示されます。

サードパーティ製品との統合を可能にするログ転送機能

1 台の FortiAnalyzer ユニットのほか、別の FortiAnalyzer ユニットのほか、syslog サーバー、あるいは CEF サーバーにログを転送できます。クライアントとなる FortiAnalyzer が、サーバーとして機能する FortiAnalyzer ユニットのほか、syslog サーバー、または CEF サーバーにログを転送します。クライアントは、別のユニットやサーバーにログを転送するだけでなく、アーカイブされたログのデータポリシー設定に基づいてログのローカルコピーも保持します。クライアントで生成されたログは、リアルタイム、またはほぼリアルタイムで転送されます。

柔軟なクォータ管理機能によるマルチテナントのサポート

管理ドメイン (ADOM) 毎に、時間に基づくログデータのアーカイブおよび分析ポリシーを設定できるほか、定義済みポリシーに基づくクォータの自動管理が可能で、ポリシーの構成や使用状況の監視の指針となるトレンドグラフが提供されます。

仮想マシン

FortiAnalyzer VM-S

新しい FortiAnalyzer のサブスクリプション型ライセンスモデルでは、VM 製品の SKU と FortiCare サポートの SKU に加えて、IOC サービスと FortiAnalyzer SOC サービスも 1 つの SKU に統合されており、製品の購入、アップグレード、更新が簡素化されます。

FortiAnalyzer S シリーズ SKU は、1 日あたり 5 GB、50 GB、500 GB のログに対応する積み上げ方式のライセンスであるため、1 日あたりのログデータ量を増やす際に必要な SKU の単位数を指定して購入することができます。また、異なる単位の SKU を同時購入し、1 日あたりのログデータの総量を増やすこともできます。

FortiAnalyzer VM

FortiAnalyzer VM は、ネットワークのロギング、分析、レポートを単一システムに統合し、ネットワーク全体のセキュリティイベントに関するより高度な情報の把握を可能にします。仮想化テクノロジーを活用する FortiAnalyzer VM は、FortiAnalyzer ハードウェアアプライアンスのソフトウェアベースバージョンであり、多くの仮想化プラットフォームで動作するように設計されています。FortiAnalyzer VM では、FortiAnalyzer ハードウェアアプライアンスのすべての機能が提供されます。

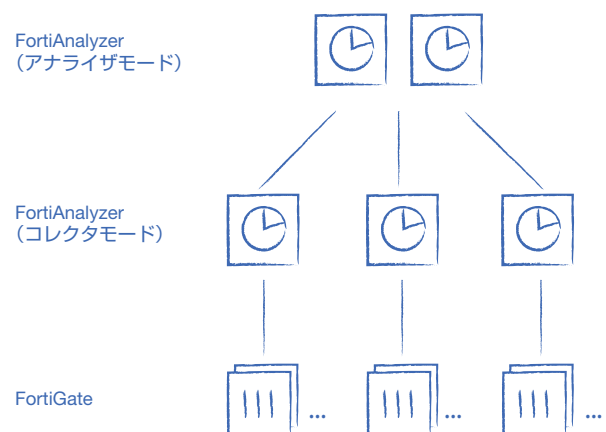
FortiAnalyzer VM を利用することで、組織が、セキュリティイベント分析、フォレンジック分析、レポート、コンテンツアーカイブ、データマイニング、悪意のあるファイルの隔離、脆弱性の評価などの機能を一元的に利用できるようになります。また、フォーティネットのアプライアンスやサードパーティ製デバイスからの地理的、時間的に異なるセキュリティデータの収集、相関付け、分析の一元化によって、セキュリティ対策の簡素化された統合ビューが提供されます。

FortiAnalyzer Cloud


フォーティネットが管理する FortiAnalyzer インフラストラクチャを活用したいお客様には、クラウドベースの分析およびレポートサービスである FortiAnalyzer Cloud を提供しています。FortiAnalyzer Cloud には、FortiCloud のポータルからシングルサインオンで簡単にアクセスいただけます。

アナライザモードとコレクタモード

アナライザモードとコレクタモードを異なる FortiAnalyzer ユニットに展開してユニットを連携させると、ログの受信、分析、レポートの総合的なパフォーマンスが向上します。コレクタモードでの FortiAnalyzer の主なタスクは、接続デバイスのログの FortiAnalyzer への転送とログのアーカイブです。ログ受信タスクがコレクタにオフロードされるため、アナライザがデータ分析とレポート生成に集中できるようになり、コレクタのログ受信パフォーマンスが向上します。



技術仕様

FortiAnalyzer 仮想アプライアンス	FortiAnalyzer VM BASE	FortiAnalyzer VM-GB1	FortiAnalyzer VM-GB5	FortiAnalyzer VM-GB25	FortiAnalyzer VM-GB100	FortiAnalyzer VM-GB500	FortiAnalyzer VM-GB2000
システム性能							
ログ処理 GB / 日	1 *	+1	+5	+25	+100	+500	+2,000
ストレージ	500 GB	+500 GB	+3 TB	+10 TB	+24 TB	+48 TB	+100 TB
管理可能なネットワークデバイス / 仮想 UTM (VDOM) サポート数 (最大)	10,000	10,000	10,000	10,000	10,000	10,000	10,000
オプション							
FortiGuard IOC (Indicators of Compromise : 侵害指標) サービス				☑			
SOC サブスクリプション				☑			
ハイパーバイザー要件							
サポートするハイパーバイザー	VMware ESX / ESXi 5.5 / 6.0 / 6.5 / 6.7 / 7.0、Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 / 2016、Citrix XenServer 6.0 以降および Open Source Xen 4.1 以降、Redhat 6.5 以降および Ubuntu 17.04 上の KVM、Nutanix AHV (AOS 5.10.5)、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud (GCP)、Oracle Cloud Infrastructure (OCI)、Alibaba Cloud (AliCloud)						
仮想 NIC 枚数 (最小 / 最大)	1 / 4						
仮想 CPU 数 (最小 / 最大)	4 / 無制限						
メモリ (最小 / 最大)	8 GB / 無制限						
* コレクタモードの場合は無制限							
							
FortiAnalyzer アプライアンス	FortiAnalyzer 150G	FortiAnalyzer 200F	FortiAnalyzer 300F	FortiAnalyzer 400E			
システム性能							
ログ処理 GB / 日	25	100	150	200			
分析用持続レート (ログ / 秒) *	500	3,000	4,500	6,000			
コレクタ用持続レート (ログ / 秒) *	750	4,500	6,750	9,000			
管理可能なネットワークデバイス仮想 UTM (VDOM) サポート数 (最大)	50	150	180	200			
最長分析日数 **	38	40	28	30			
オプション							
FortiGuard IOC (Indicators of Compromise : 侵害指標) サービス	☑	☑	☑	☑			
SOC サブスクリプション	—	—	☑	—			
Enterprise Protection バンドル	—	—	☑	—			
ハードウェア仕様							
形状 (EIA 規格およびその他の 19 インチラック適合)	デスクトップ	ラックマウント (1 RU)	ラックマウント (1 RU)	ラックマウント (1 RU)			
インタフェース	2 x GbE RJ45	2 x GbE RJ45	2 x GbE RJ45、2 x SFP	4 x GbE			
ストレージ	4 TB (2 x 2 TB)	4 TB (1 x 4 TB)	8 TB (2 x 4 TB)	12 TB (4 x 3 TB)			
利用可能なストレージ (デフォルト RAID 構成時)	2 TB	4 TB	4 TB	6 TB			
リムーバブル HDD	—	—	—	☑			
RAID ストレージ管理	○ (0、1)	—	○ (0、1)	○ (0、1、5、10)			
RAID タイプ	ソフトウェア	—	ソフトウェア	ソフトウェア			
デフォルト RAID レベル	1	—	1	10			
冗長電源 (ホットスワップ対応)	—	—	—	—			
サイズ							
高さ x 幅 x 奥行	241 x 89 x 205.5 mm	44 x 432 x 381 mm	44 x 432 x 380 mm	43 x 437 x 503 mm			
重量	4.24 kg	7.8 kg	8.6 kg	14.1 kg			
動作環境							
AC 電源	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz			
消費電力 (平均 / 最大)	36 W / 43 W	49 W / 114 W	65 W / 130 W	93 W / 133 W			
放熱	147.4 BTU/h	390 BTU/h	445 BTU/h	456 BTU/h			
動作温度	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	5 ~ 35 °C			
保管温度	-20 ~ 75 °C	-35 ~ 70 °C	-35 ~ 70 °C	-40 ~ 60 °C			
湿度	5 ~ 95 % (結露しないこと)	20 ~ 90 % (結露しないこと)	20 ~ 90 % (結露しないこと)	8 ~ 90 % (結露しないこと)			
動作高度	最高 2,250 m	最高 2,250 m	最高 2,250 m	最高 3,000 m			
準拠規格							
準拠規格	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、UL/cUL、CB			

* 持続レート：SQL データベースおよびシステムのパフォーマンスを低下させることなく、最小で 48 時間 FortiAnalyzer プラットフォームが維持可能なログメッセージレートの最大値。

** ログを分析用持続レートで継続的に受信する場合に保持できる最大日数。平均ログレートが低いと保持日数は長くなります。

技術仕様

FortiAnalyzer アプライアンス	FortiAnalyzer 800F	FortiAnalyzer 1000F	FortiAnalyzer 2000E
システム性能			
ログ処理 GB / 日	300	660	1,000
分析用持続レート (ログ / 秒) *	8,250	20,000	30,000
コレクタ用持続レート (ログ / 秒) *	12,000	30,000	45,000
管理可能なネットワークデバイス仮想 UTM (VDM) サポート数 (最大)	800	2,000	2,000
最長分析日数 **	30	34	30
オプション			
FortiGuard IOC (Indicators of Compromise : 侵害指標) サービス	✓	✓	✓
SOC サブスクリプション	✓	✓	—
Enterprise Protection バンドル	✓	✓	—
ハードウェア仕様			
形状 (EIA 規格およびその他の 19 インチラック適合)	ラックマウント (1 RU)	ラックマウント (2 RU)	ラックマウント (2 RU)
インタフェース	4 x GbE、2 x SFP	2 x 10 GbE RJ45、 2 x 10 GbE SFP+	4 x GbE、2 x SFP+
ストレージ	16 TB (4 x 4 TB)	32 TB (8 x 4 TB)	36 TB (12 x 3 TB)
利用可能なストレージ (デフォルト RAID 構成時)	8 TB	24 TB	30 TB
リムーバブル HDD	✓	✓	✓
RAID ストレージ管理	○ (0、1、1s、5s、10)	○ (0、1、1s、5s、5s、6s、6s、10、50、60)	○ (0、1、5s、6s、10、50、60)
RAID タイプ	ハードウェア (ホットスワップ対応)	ハードウェア (ホットスワップ対応)	ハードウェア (ホットスワップ対応)
デフォルト RAID レベル	10	50	50
冗長電源 (ホットスワップ対応)	(オプション)	✓	✓
サイズ			
高さ x 幅 x 奥行	44 x 443 x 563 mm	89 x 437 x 650 mm	89 x 437 x 648 mm
重量	13.0 kg	15.42 kg	26.3 kg
動作環境			
AC 電源	100 ~ 240 V AC、 50 ~ 60 Hz	100 ~ 240 V AC、 50 ~ 60 Hz	100 ~ 240 V AC、 50 ~ 60 Hz
消費電力 (平均 / 最大)	108 W / 186 W	192.5 W / 275 W	293.8 W / 354 W
放熱	634 BTU/h	920 BTU/h	1,840 BTU/h
動作温度	0 ~ 40 °C	10 ~ 35 °C	10 ~ 35 °C
保管温度	-35 ~ 70 °C	-40 ~ 60 °C	-40 ~ 70 °C
湿度	20 ~ 90% (結露しないこと)	8 ~ 90% (結露しないこと)	8 ~ 90% (結露しないこと)
動作高度	最高 2,250 m	最高 2,250 m	最高 2,250 m
準拠規格			
準拠規格	FCC Part 15 Class A、RCM、 VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、 VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、RCM、 CE、UL/cUL、CB

* 持続レート：SQL データベースおよびシステムのパフォーマンスを低下させることなく、最小で 48 時間 FortiAnalyzer プラットフォームが維持可能なログメッセージレートの最大値。

** ログを分析用持続レートで継続的に受信する場合に保持できる最大日数。平均ログレートが低いと保持日数は長くなります。

技術仕様



FortiAnalyzer アプライアンス	FortiAnalyzer 3000F	FortiAnalyzer 3000G	FortiAnalyzer 3500G	FortiAnalyzer 3700F
システム性能				
ログ処理 GB / 日	3,000	3,000	5,000	8,300
分析用持続レート (ログ / 秒) *	42,000	42,000	60,000	100,000
コレクタ用持続レート (ログ / 秒) *	60,000	60,000	90,000	150,000
管理可能なネットワークデバイス仮想 UTM (VDOM) サポート数 (最大)	4,000	4,000	10,000	10,000
最長分析日数 **	30	30	38	60
オプション				
FortiGuard IOC (Indicators of Compromise : 侵害指標) サービス	✓	✓	✓	✓
SOC サブスクリプション	✓	✓	✓	✓
Enterprise Protection バンドル	✓	✓	✓	✓
ハードウェア仕様				
形状 (EIA 規格およびその他の 19 インチラック適合)	ラックマウント (3 RU)	ラックマウント (3 RU)	ラックマウント (4 RU)	ラックマウント (4 RU)
インタフェース	4 x GbE, 2 x SFP+	2 x GbE RJ45, 2 x 25 GbE SFP28	2 x GbE RJ45, 2 x SFP28	2 x SFP+, 2 x 1 GbE
ストレージ	48 TB (16 x 3 TB – 最大 48 TB)	64 TB (16 x 4TB)	96 TB (24 x 4 TB)	240 TB (60 x 4 TB SAS HDD)
利用可能なストレージ (デフォルト RAID 構成時)	42 TB	56 TB	80 TB	216 TB
リムーバブル HDD	✓	✓	✓	✓
RAID ストレージ管理	○ (0、1、5、6、10、50、60)	○ (0、1、1s、5、5s、6、6s、10、50、60)	○ (0、1、1s、5、5s、6、6s、10、50、60)	○ (0、1、1s、5、5s、6、6s、10、50、60)
RAID タイプ	ハードウェア (ホットスワップ対応)	ハードウェア (ホットスワップ対応)	ハードウェア (ホットスワップ対応)	ハードウェア (ホットスワップ対応)
デフォルト RAID レベル	50	50	50	50
冗長電源 (ホットスワップ対応)	✓	✓	✓	✓***
サイズ				
高さ x 幅 x 奥行	132 x 437 x 648 mm	130 x 440 x 650 mm	178 x 437 x 660 mm	178 x 437 x 767 mm
重量	34.5 kg	30.15 kg	41.2 kg	53.5 kg
動作環境				
AC 電源	100 ~ 240 V AC, 50 ~ 60 Hz	100 ~ 127 V 以上 / 10 A, 200 ~ 240 V 以上 / 5 A	100 ~ 240 V AC, 50 ~ 60 Hz	2,000 W AC
消費電力 (平均 / 最大)	449 W / 541 W (12 HDD 搭載時)	385 W / 500 W	629.5 W / 677.3 W	850 W / 1,423.4 W
放熱	1,846.5 BTU/h	1,350 BTU/h	2345.07 BTU/h	4,858 BTU/h
動作温度	10 ~ 35 °C	0 ~ 40 °C	5 ~ 35 °C	10 ~ 35 °C
保管温度	-40 ~ 70 °C	-20 ~ 75 °C	-40 ~ 60 °C	-40 ~ 70 °C
湿度	8 ~ 90% (結露しないこと)	5 ~ 95% (結露しないこと)	8 ~ 90% (結露しないこと)	8 ~ 90% (結露しないこと)
動作高度	最高 2,250 m	最高 2,250 m	最高 2,250 m	最高 2,133 m
準拠規格				
準拠規格	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

* 持続レート：SQL データベースおよびシステムのパフォーマンスを低下させることなく、最小で 48 時間 FortiAnalyzer プラットフォームが維持可能なログメッセージレートの最大値。

** ログを分析用持続レートで継続的に受信する場合に保持できる最大日数。平均ログレートが低いと保持日数は長くなります。

*** 200 V ~ 240 V の電源に接続する必要があります。

FORTINET®

フォーティネットジャパン株式会社

〒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