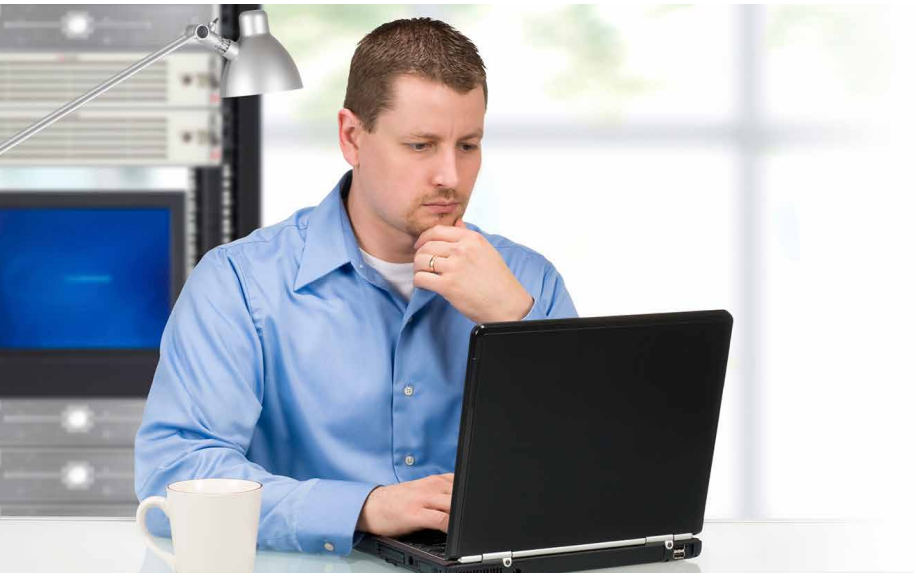
DATA SHEET

FortiAnalyzer
集中ロギング、分析、レポート



FortiAnalyzer

FortiAnalyzer 200D、400E、1000E、2000E、3000E、3000F、3500E、3500F、3900E、 FortiAnalyzer VM

集中ロギング、分析、レポート

ネットワークの包括的な可視化

FortiAnalyzer プラットフォームは、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。FortiAnalyzer を通じて、許容可能な使用ポリシーの監視および維持に必要な労力を最小化するとともに、攻撃パターンの特定に基づいてセキュリティポリシーを調整し、今後の攻撃阻止に備えることができます。また、あらゆる規模の組織が、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などの機能を一元的に利用できるようになります。

FortiAnalyzer の物理 / 仮想アプライアンスを導入することで、幅広い地域および時系列のセキュリティデータを集中的に収集し、相関性を分析し、総合的なセキュリティの状況を容易に把握できます。フォーティネットアプライアンスやサードパーティ製デバイスからアラートやログ情報が集約され、現在のセキュリティ体制をシンプルな 1 つのビューに表示します。さらに、詳細データを捕捉してフォレンジック分析に利用することで、プライバシーおよび情報セキュリティ侵害の公表に関する法令およびポリシーを厳格に遵守することが可能になります。

主な機能と特長

能率的なグラフィカルレポート	FortiGate やサードパーティ製デバイスで発生したイベント、アクティビティ、トレンドに関するネットワーク全体のレポートを提供
ネットワークイベント相関	IT 管理者がネットワーク全域でネットワークセキュリティ脅威をより迅速に発見および対処可能
スケーラブルなパフォーマンスとキャパシティ	数千台の FortiGate や FortiClient エージェントをサポートし、保持 / コンプライアンスの要件に応じてストレージの動的拡張が可能
スタンドアロン、コレクタまたはアナライザモードでの利用が可能	単体ユニットとして導入できるほか、ストア & フォワードや分析など特定のオペレーション向けに最適化も可能
フォーティネット製品ポートフォリオとのシームレスな統合	密接な統合によってパフォーマンスが最大化され、FortiAnalyzer を FortiGate または FortiManager ユーザーインタフェースで管理可能

広範な課題に対応するフォーティネットの管理ソリューション

新たな脅威の出現や企業の成長、あるいは新しい法規制やビジネス要件に対応するため、ネットワークは絶え間なく進化しています。従来の分析製品は、時間の経過とともにデータをロギング、分析、レポートし、企業全体における脅威を記録し特定することにフォーカスしていました。

FortiAnalyzer は、エンタープライズクラスの機能を利用してこのような脅威を特定できるほか、常に変化を続けるネットワークに合わせてその能力を柔軟に進化させていくことが可能です。FortiAnalyzer は、自社のビジネス要件に合わせて自由にカスタマイズしたレポートを生成できると同時に、階層的、段階的なロギングトポロジでログを集約させることができます。

多様な管理機能を提供するフォーティネット製品の基本理念：

- 多様なフォームファクタ
- アーキテクチャの柔軟性
- 自由自在なカスタマイズ
- シンプルなライセンスモデル

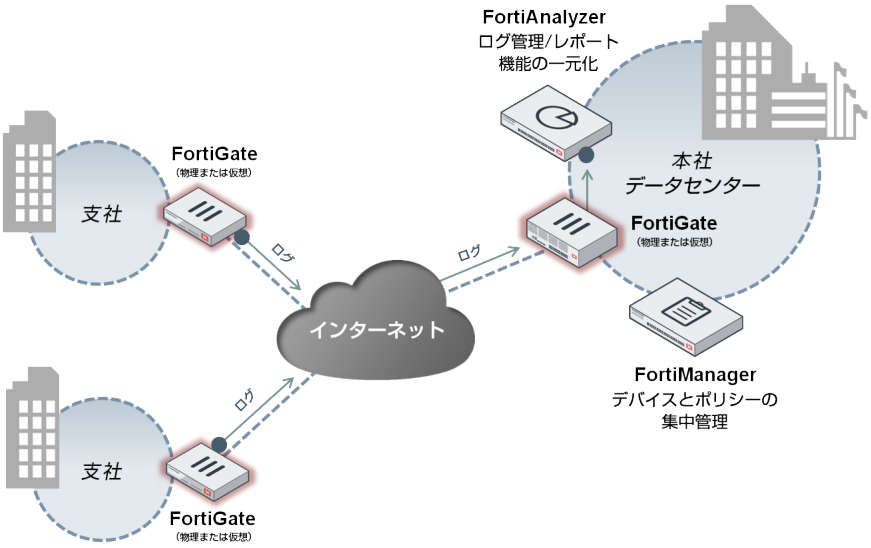
ハイライト

レポーティングおよび可視化ツール

- **FortiView サマリレポート**
  トップユーザー、アプリケーション、送信先、Web サイト、脅威、VPN の使用状況などをグラフィカルでフィルタリング可能なアドホックビューで表示します。
- **レポート用テンプレートを内蔵**
  カスタマイズ可能な PDF テンプレートを活用して、カラフルでグラフィカルなネットワークセキュリティと使用状況の総合レポートを表示できます。
- **UTM およびトラフィックサマリレポート**
  UTM/ トラフィックが統合された新しいレポートによって、セキュリティプロファイルおよびトラフィック / 帯域幅パターンを定期的に分析することができます。
- **イベント管理**
  重要なイベントを検出・監視し、異常な可能性のある挙動に関するこれまでにない詳細な情報を IT 管理者に提供します。
- **テンプレートのインポートとエクスポート**
  レポートを作成後、別の FortiAnalyzer や異なる仮想管理機能（ADOM）に構成をエクスポートし、変更することができます。

JSON および Web サービス（XML）API

- API をすべての FortiAnalyzer ハードウェアモデルと仮想マシンで使用できます。
- JSON API — MSSP/ 大規模エンタープライズが FortiAnalyzer のレポート、チャート / データセット、およびオブジェクトを操作できます。
- XML API — IT 管理者は FortiAnalyzer のプロビジョニング / 構成およびレポートの生成を迅速に実行できます。
- Fortinet Developer Network（FNDN）にご加入いただくと、ツール、サンプルコード、ドキュメントにアクセスし、フォーティネットの開発者コミュニティに参加できます。



ログビューアー

- リアルタイムログまたは履歴ログの表示
- トラフィック、イベント、全セキュリティログの選択
- デバイスや仮想管理機能（ADOM）別のログ、または集計したログの表示
- ログフィルタリングと検索機能
- ログ詳細画面での細密な調査
- 国やアプリケーションなどを直感的なアイコンで表示

イベント管理

- 包括的なアラートビルダー
- 深刻度のレベル、特定のイベント、アクション、および送信先によるトリガー設定
- 特定の時間内で発生したイベント数によって変化するしきい値を設定
- アラート履歴の表示と検索
- 電子メールや SNMP による通知、または Syslog イベントの作成

FortiManager との高度な連携

- エンタープライズクラスのデバイス管理
- 使い慣れた GUI を利用して完全にネットワークを制御可能
- FortiAnalyzer を組み込んだ統合ソリューションとして利用可能

DLP アーカイブ

- DLP コンテンツアーカイブの調査
- 電子メール、HTTP、FTP、IM などのアーカイブタイプをサポート
- アーカイブテキストやダウンロードファイルの表示

FortiAnalyzer のサポート対象デバイス

- FortiGate 統合脅威管理アプライアンス
- FortiMail 統合セキュアメールアプライアンス
- FortiClient エンドポイントセキュリティ
- FortiWeb Web アプリケーションファイアウォール
- FortiManager 集中セキュリティ管理
- FortiSandbox 脅威保護
- FortiCache Web キャッシング
- Syslog 互換のすべてのデバイス

技術仕様

	FortiAnalyzer 200D	FortiAnalyzer 400E	FortiAnalyzer 1000E
システム性能			
ログ処理 GB / 日	5	75	300
分析用持続レート（ログ / 秒）	120	500	4,000
コレクタ用持続レート（ログ / 秒）	350	725	6,000
管理可能なネットワークデバイス / 仮想管理（ADOM）/ 仮想 UTM（VDOM）サポート数（最大）	150	200	2,000
ハードウェア仕様			
形状	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（2 RU）
インタフェース	4 x GbE	4 x GbE	2 x GbE
ストレージ	1 TB（1 x 1 TB）	12 TB（4 x 3 TB）	24 TB（8 x 3 TB）
リムーバブル HDD	—	○	○
RAID ストレージ管理	—	○（0、1、5、10）	○（0、1、5、6、10、50、60）
デフォルト RAID レベル	—	10	50
冗長電源（ホットスワップ対応）	—	—	○
サイズ			
高さ x 幅 x 奥行	4.5 x 43.3 x 35.2 cm	4.3 x 43.7 x 50.3 cm	8.9 x 43.7 x 68.4 cm
重量	6.1 kg	14.1 kg	23.6 kg
動作環境			
AC 電源、消費電流	100 - 240 V AC、50 - 60 Hz、6 A（最大）	100 - 240 V AC、60 – 50 Hz	100 - 240 V AC、60 – 50 Hz
消費電力（平均）	60 W	93 W	192.5 W
放熱	205 BTU/h	456 BTU/h	920 BTU/h
動作温度	0 ～ 40 ℃	5 ～ 35 ℃	5 ～ 35 ℃
保管温度	-35 ～ 70 ℃	-40 ～ 60 ℃	-40 ～ 60 ℃
湿度	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
準拠規格			
準拠規格	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB

	FortiAnalyzer 2000E	FortiAnalyzer 3000E	FortiAnalyzer 3000F
システム性能			
ログ処理 GB / 日	500	800	1,600
分析用持続レート（ログ / 秒）	7,500	15,000	35,000
コレクタ用持続レート（ログ / 秒）	11,250	50,000	52,500
管理可能なネットワークデバイス / 仮想管理（ADOM）/ 仮想 UTM（VDOM）サポート数（最大）	2,000	4,000	4,000
ハードウェア仕様			
形状	ラックマウント（2 RU）	ラックマウント（2 RU）	ラックマウント（3 RU）
インタフェース	4 x GbE、2 x 10 GbE SFP+	4 x GbE、2 x GbE SFP	4 x GbE、2 x 10 GbE SFP+
ストレージ	36 TB（12 x 3 TB）	16 TB（8 x 2 TB）	48 TB（16 x 3 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、5、6、10、50、60）	○（0、1、5、6、10、50、60）
デフォルト RAID レベル	50	10	50
冗長電源（ホットスワップ対応）	○	○	○
サイズ			
高さ x 幅 x 奥行	8.9 x 43.7 x 64.8 cm	8.7 x 48.2 x 75.5 cm	13.2 x 43.7 x 64.8 cm
重量	26.3 kg	32.5 kg	34.5 kg
動作環境			
AC 電源、消費電流	100 - 240 V AC、60 – 60 Hz	100 - 240 V AC、50 - 60 Hz、10 A（最大）	100 - 240 V AC、60 – 50 Hz
消費電力（平均）	390 W	375.8 W	465 W
放熱	1840 BTU/h	1,947 BTU/h	1,904 BTU/h
動作温度	10 ～ 35 ℃	10 ～ 35 ℃	10 ～ 35 ℃
保管温度	-40 ～ 70 ℃	-40 ～ 65 ℃	-40 ～ 70 ℃
湿度	8 ～ 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
準拠規格			
準拠規格	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB

技術仕様

	FortiAnalyzer 3500E	FortiAnalyzer 3500F	FortiAnalyzer 3900E
システム性能			
ログ処理 GB / 日	3,000	5,000	4,000
分析用持続レート（ログ / 秒）	36,000	60,000	48,000
コレクタ用持続レート（ログ / 秒）	60,000	90,000	75,000
管理可能なネットワークデバイス / 仮想管理（ADOM）/ 仮想 UTM（VDOM）サポート数（最大）	10,000	10,000	10,000
ハードウェア仕様			
形状	ラックマウント（4 RU）	ラックマウント（4 RU）	ラックマウント（2 RU）
インタフェース	2 x GbE、2 x GbE SFP	2 x GbE、2 x GbE SFP	2 x GbE、2 x 10 GbE SFP+
ストレージ	24 TB（12 x 2 TB ～ 48 TB 最大）	72 TB（24 x 3TB）	15 TB SSD（15 x 1 TB SSD）
リムーバブル HDD	○	○	○
RAID ストレージ管理	○（0、1、5、6、10、50、60）	○（0、1、5、6、10、50、60）	○（0、1、5、6、10、50、60）
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）	○	○	○
サイズ			
高さ x 幅 x 奥行	17.5 x 48.2 x 69.0 cm	17.6 x 48.2 x 69.0 cm	8.9 x 43.7 x 68.4 cm
重量	34.9 kg	42.52 kg	23.6 kg
動作環境			
AC 電源、消費電流	100 - 240 V AC、50 - 60 Hz、11.5 A（最大）	100 - 240 V AC、60 – 50 Hz	100 - 240 V AC、50 - 60 Hz、11.5 A（最大）
消費電力（平均）	465 W（12 HDD 搭載時）	465 W	470 W（15 HDD 搭載時）
放熱	1,904 BTU/h	1,904 BTU/h	1,637 BTU/h
動作温度	0 ～ 40 ℃	0 ～ 40 ℃	10 ～ 35 ℃
保管温度	-25 ～ 70 ℃	-25 ～ 70 ℃	-40 ～ 60 ℃
湿度	10 ～ 90%（結露しないこと）	10 ～ 90%（結露しないこと）	5 ～ 95%（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、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB	FCC Part 15 Class A、C-Tick、VCCI、CE、UL/cUL、CB

	FortyAnalyzer VM-BASE	FortyAnalyzer VM-GB1	FortyAnalyzer VM-GB5	FortyAnalyzer VM-GB25	FortyAnalyzer VM-GB100	FortyAnalyzer VM-GB500	FortyAnalyzer 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	500GB	+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 / 仮想管理（ADOM）/ 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
ハイパーバイザ	VMware ESX/ESXi 4.0 / 4.1 / 5.0 / 5.1 / 5.5 / 6.0、Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2、Citrix XenServer 6.0+、Open Source Xen 4.1+、KVM、Amazon Web Services（AWS）						
仮想 NIC 枚数（最小 / 最大）	1 / 4						
仮想 CPU 数（最小 / 最大）	1 / 無制限						
メモリ（最小 / 最大）	1 GB / 無制限						

* Collector モードの場合は無制限

FORTINET®
フォーティネットジャパン株式会社

お問い合わせ

www.fortinet.co.jp/contact