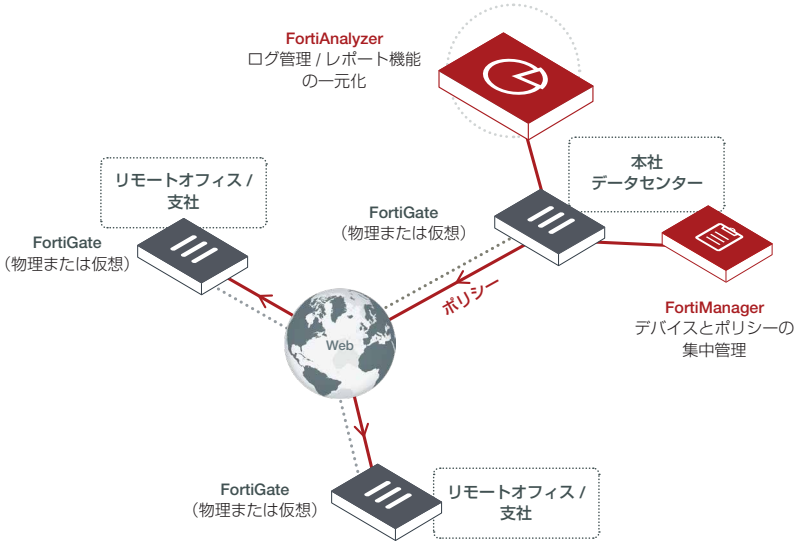
FortiAnalyzer

ダイナミックかつ急激に変化する今日のセキュリティ環境では、ネットワークの可視化が不十分であることが原因で、平均 100 日以上にわたって情報漏洩の検知が遅れ、データ侵害が見過ごされてしまう状況が続いています。脅威にさらされる期間が長期化すると、機密性の 高い顧客情報や社内情報が攻撃される可能性が日に日に高くなります。FortiAnalyzer は、あらゆる攻撃対象の脅威に関する重要な実用的インテリジェンスを提供し、瞬時の可視化、状況の認識、リアルタイムの 脅威インテリジェンス、そして実用的な分析を可能にすると同時に、フォーティネット セキュリティ ファブリック向けに、NOC-SOC セキュリティ分析や運用に役立つ全体像を提供します。



分析の一元化

イベント相関と高度な脅威検知機能：
IT管理者がネットワーク全体でネットワークセキュリティの脅威をより迅速に発見し、対処可能

強力な NOC-SOC ダッシュボード：
カスタマイズ可能な NOC-SOC ダッシュボードによる、ネットワークの管理、監視、制御を実現

スケーラブルなパフォーマンスと柔軟な導入：
数千台の FortiGate や FortiClient のエージェントをサポートし、保持の要件に応じたストレージの動的拡張が可能。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向けに最適化も可能

フォーティネット セキュリティ ファブリックでは、フォーティネットのエンタープライズファイアウォールの導入によって持続的な標的型攻撃に対抗するほか、FortiAnalyzer を追加することでセキュリティ ファブリックの可視性を強化し、実用的で確実なセキュリティアラート情報を自動的に提供することで、エンドツーエンドの統一された保護が可能になります。

FortiAnalyzer では、フォーティネットのエンタープライズファイアウォールの分散ネットワークからのログの収集、分析、相関付けが一元化されるため、単一コンソールからすべてのファイアウォールトラフィックを表示し、レポートを生成できます。FortiGuard IOC（Indicators of Compromise：侵害指標）サービスに加入すると、侵害されたホストの優先度順リストが提供されるため、すぐに対策を実行できます。

特長

- **検索およびレポートの一元化：** Google 検索のようにシンプルで直感的な機能を使って、ネットワークのアクティビティやトレンドを検索し、レポートを作成可能
- **IOC（Indicators of Compromise：侵害指標）を自動的に提供：** FortiGuard IOC のインテリジェンスを使用してセキュリティログをスキャンし、APT を検知
- **リアルタイムおよび過去のネットワークアクティビティを表示：** アプリケーション、送信元、送信先、Web サイト、セキュリティの脅威、管理情報の変更、システムイベントのサマリを表示
- **軽快なイベント管理：** 事前定義済みのセキュリティイベントを容易にカスタマイズし、自動アラートを設定可能
- **フォーティネット セキュリティ ファブリックとのシームレスな統合：** 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

ハイライト

インシデント対応

FortiAnalyzer の優れたインシデント対応機能によって、イベント管理やウイルス感染したエンドポイントの特定に注力可能となり、管理や分析の効率が改善されます。機能強化された標準および独自のイベントハンドラーを活用して、即座に悪意のある不審な挙動を検知できます。イベントが FortiOS の自動化フレームワークに統合されることで、エンドポイントは自動的に隔離されます。インシデントの検知と追跡、さらに痕跡の収集と分析は ITSM との統合によって効率化されており、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、セキュリティ対策が強化されます。

FortiView：ネットワークの詳細な可視化

FortiAnalyzer のカスタマイズ可能なインタラクティブダッシュボードでは、ネットワークトラフィック、脅威、アプリケーションなどの直感的なサマリビュー（図 1）を利用して、問題をすばやく特定できます。FortiView は、リアルタイムデータと過去データを単一ビューに統合できる包括的なネットワーク監視システムで、ネットワークに対する脅威のログや監視、複数レベルのデータのフィルタリング、管理アクティビティの追跡などの多くの機能を備えています。

図 1

IOC（Indicators of Compromise：侵害指標）

IOC（Indicators of Compromise：侵害指標）サマリには、Web の使用で感染が疑われるエンドユーザーが表示されます。エンドユーザーの IP アドレス、ホスト名、グループ、OS、総合脅威評価、マップビュー、脅威の数などの情報が提示され、ドリルダウンによって、脅威の詳細を表示できます。FortiAnalyzer は、IOC の生成にあたって、エンドユーザーごとの Web フィルタログを脅威データベースと照合してチェックします。一致する脅威が見つかると、脅威スコアがそのエンドユーザーに割り当てられます。FortiAnalyzer は、エンドユーザーの脅威のスコアを集計することで、そのエンドユーザーの総合的な IOC を判定します。IOC サマリが FortiGate デバイスの UTM Web フィルター経由で生成され、FortiGuard の FortiAnalyzer サブスクリプションによってローカルの脅威データベースが FortiGuard 脅威データベースと常に同期されます。

レポート

レポート機能を利用することで、カスタムデータレポートをログから生成できます。FortiAnalyzer には、30 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。オンデマンドに加えて、カレンダービューによるスケジュール指定も可能であるため、電子メールによる通知やアップロードの自動化によって管理が容易になります。300 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。

監視とアラート

イベントハンドラーでは、ログから抽出してイベント管理に表示するメッセージを定義します。イベントハンドラーを有効にして、イベントの生成を開始する必要があり、イベントハンドラーを構成することで、特定のデバイス、すべてのデバイス、またはローカルの FortiAnalyzer ユニットのイベントを生成するように指定できます。FortiGate、FortiCarrier、FortiCache、FortiMail、FortiManager、FortiWeb、FortiSandbox の各デバイス、および syslog サーバーのイベントハンドラーを作成できるほか、システムを構成することで電子メールアドレス、SNMP コミュニティ、または syslog サーバー経由で、イベントハンドラーのアラートが送信されるように指定できます。

ネットワークオペレーションセンター（NOC）と セキュリティオペレーションセンター（SOC）

管理センター内の FortiAnlyzers NOC-SOC は、実用的なログと脅威データを提供することでネットワーク全体の保護を支援します。SOC によって、脅威、イベント、ネットワークアクティビティの一元的な監視と把握が可能になり、定義済みの FAZ（FortiAnalyzer）ダッシュボードやウィジェットを使用して、ネットワーク、Web サイト、アプリケーション、データベース、サーバー、データセンターなどのテクノロジーを保護したり、カスタマイズ可能な単一インタフェースによって、セキュリティ ファブリックに簡単に統合したりできます（図 2）。

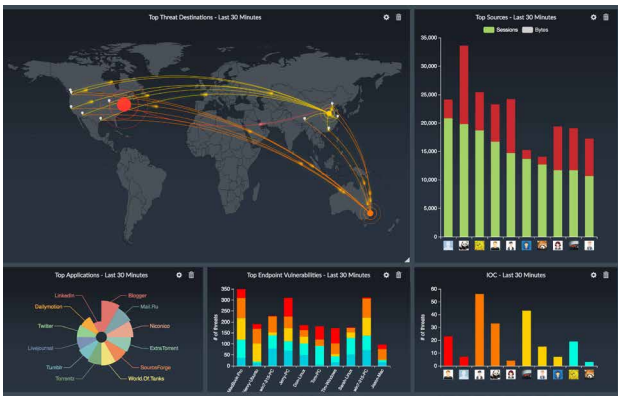


図 2

フォレンジック分析のためのログ取得

ログ取得を使用して、ある FortiAnalyzer デバイスからアーカイブされたログを、別の FortiAnalyzer デバイスで取得します。この方法を利用すると、管理者が過去のデータに対するクエリやレポートを実行し、フォレンジック分析に役立てることができます。FortiAnalyzer デバイスは、ログ取得のサーバーまたはクライアントのいずれかとして動作し、どちらの場合も、指定されたフィルターに基づき、指定されたデバイスと期間のログデータ取得の役割を実行します。取得されたデータにはインデックスが設定され、データ分析やレポートに使用できます。

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

ある FortiAnalyzer ユニットから、別の FortiAnalyzer ユニット、syslog サーバー、または CEF（共通イベント形式）サーバーにログを転送できます。この場合のクライアントとは、ログを別のデバイスに転送する FortiAnalyzer ユニットのことであり、サーバーとは、ログを受信する FortiAnalyzer ユニット、syslog サーバー、または CEF サーバーを指します。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、ログのローカルコピーを保持します。ログのローカルコピーは、アーカイブログのデータポリシーの設定に基づき作成され、受け取ったログがリアルタイム、またはほぼリアルタイムで転送されます。転送されるコンテンツファイルとしては、DLP ファイル、ウイルス対策隔離ファイル、IPS パケットキャプチャなどがあります。

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（図 3）。

柔軟なクォータ管理機能により、マルチテナントに対応

管理ドメイン（ADOM）別に、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、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監視の指針となるトレンドグラフが提供されます。

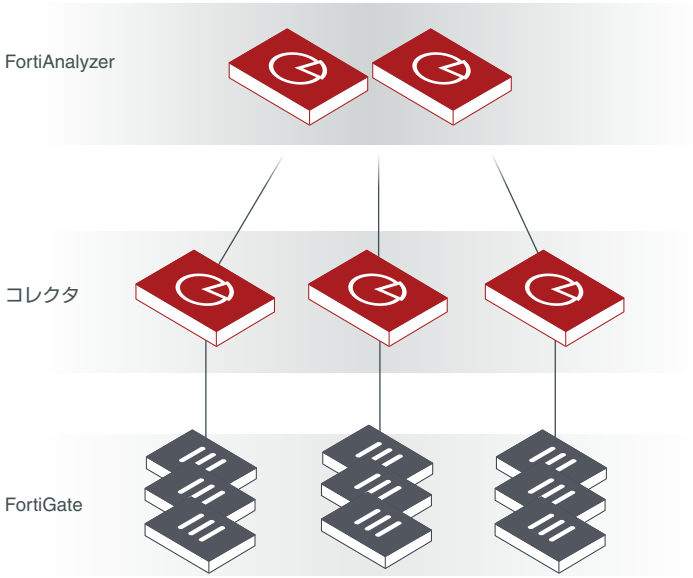


図 3

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、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、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。

技術仕様

	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
FortiGuard Indicators of Compromise（IOC：侵害指標）サービス	✓	✓	✓	✓	✓	✓	✓
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 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7、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、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud（GCP）、Oracle Cloud Infrastructure（OCI）						
仮想 NIC 枚数（最小 / 最大）	1 / 4						
仮想 CPU 数（最小 / 最大）	2 / 無制限						
メモリ（最小 / 最大）	4 GB / 無制限						

* コレクタモードの場合は無制限

技術仕様

	FortiAnalyzer 200F	FortiAnalyzer 300F	FortiAnalyzer 400E
システム性能			
ログ処理 GB / 日	100	150	200
分析用持続レート（ログ / 秒）	3,000	4,500	6,000
コレクタ用持続レート（ログ / 秒）	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）	150	180	200
最長分析日数	40	28	30
サポートするオプション			
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓	✓	✓
FortiManager 集中セキュリティ管理機能（最大 20 デバイス）	—	—	—
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（1 RU）
インタフェース	2 x GbE RJ45	2 x GbE RJ45、2 x SFP	4 x GbE
ストレージ	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（RAID 構成時）	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、5、10）
RAID タイプ	—	ソフトウェア	ソフトウェア
デフォルト RAID レベル	—	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	44 x 432 x 381 mm	44 x 432 x 380 mm	43 x 437 x 503 mm
重量	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
消費電力（平均 / 最大）	49 W / 114 W	65W / 130W	93 W / 133 W
放熱	390 BTU/h	445 BTU/h	456 BTU/h
動作温度	0 ～ 40 ℃	0 ～ 40 ℃	5 ～ 35 ℃
保管温度	-35 ～ 70 ℃	-35 ～ 70 ℃	-40 ～ 60 ℃
湿度	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 3,000 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 800F	 FortiAnalyzer 1000E	 FortiAnalyzer 2000E
システム性能			
ログ処理 GB / 日	300	600	1,000
分析用持続レート（ログ / 秒）	8,250	18,000	30,000
コレクタ用持続レート（ログ / 秒）	12,000	27,000	45,000
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）	800	2,000	2,000
最長分析日数	30	30	30
サポートするオプション			
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓	✓	✓
FortiManager 集中セキュリティ管理機能（最大 20 デバイス）	—	✓	✓
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（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 GbE	4 x GbE、2 x SFP+
ストレージ	16 TB（4 x 4 TB）	24 TB（8 x 3 TB）	36 TB（12 x 3 TB）
利用可能なストレージ（RAID 構成時）	8 TB	18 TB	30 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）	○（0、1、5、6、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）	—	✓	✓
サイズ			
高さ x 幅 x 奥行	44 x 443 x 563 mm	89 x 437 x 684 mm	89 x 437 x 648 mm
重量	13.0 kg	23.6 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）	108W / 186W	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 ℃	5 ～ 35 ℃	10 ～ 35 ℃
保管温度	-35 ～ 70 ℃	-40 ～ 60 ℃	-40 ～ 70 ℃
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、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 3000F	 FortiAnalyzer 3500F	 FortiAnalyzer 3700F
システム性能			
ログ処理 GB / 日	3,000	5,000	8,300
分析用持続レート（ログ / 秒）	42,000	63,000	100,000
コレクタ用持続レート（ログ / 秒）	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	10,000	10,000
最長分析日数	30	30	60
サポートするオプション			
FortiGuard IOC（Indicators of Compromise：侵害指標）サービス	✓	✓	✓
FortiManager 集中セキュリティ管理機能（最大 20 デバイス）	✓	✓	✓
ハードウェア仕様			
形状	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、2 x SFP インタフェース	2 x SFP+、2 x 1 GbE
ストレージ	48 TB（16 x 3 TB – 最大 48 TB）	72 TB（24 x 3 TB）	240 TB（60 x 4 TB SAS HDD）
利用可能なストレージ（RAID 構成時）	42 TB	63 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、5、6、10、50、60）	○（0、1、5、6、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	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	176 x 482 x 690 mm	178 x 437 x 767 mm
重量	34.5 kg	42.52 kg	53.5 kg
動作環境			
AC 電源	100 ～ 240 V AC、50 ～ 60 Hz、11.5 A（最大）	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
消費電力（平均 / 最大）	449 W / 541 W（12 HDD 搭載時）	465 W / 558 W	850 W / 1,423.4 W
放熱	1,846.5 BTU/h	1,904 BTU/h	4,858 BTU/h
動作温度	10 ～ 35 ℃	0 ～ 40 ℃	10 ～ 35 ℃
保管温度	-40 ～ 70 ℃	-25 ～ 70 ℃	-40 ～ 70 ℃
湿度	8 ～ 90%（結露しないこと）	10 ～ 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 2,133 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

* 3700F は、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.co.jp/contact

お問い合わせ