FortiAnalyzer

フォーティネット セキュリティ ファブリックにおいて、ネットワークの**瞬時の可視化**、リアルタイムの脅威インテリジェンス、実用的な分析を実現

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

ハードウェア：
400E、1000E、
2000E、3000F、
3500F、3700F、
3900E、
FortiAnalyzer VM

FortiCare Worldwide support
support.fortinet.com

FortiGuard Security Services
www.fortiguard.com

FortiAnalyzer

FortiAnalyzer 400E、1000E、2000E、3000F、3500F、3700F、3900E、FortiAnalyzer VM

エンタープライズネットワークは、組織の成長や法規制、あるいはビジネスの要件によって常に進化しており、その結果セキュリティアプライアンスから大量のデータが生成されています。しかしながら、時間の経過に沿ってこれらのデータを可視化する手段がなければ、常に変化する脅威を発見することはできません。脅威の環境が複雑化し、急速に変化する今日、このような脅威が検知されずに長期に渡って存在し続けることも少なくありません。

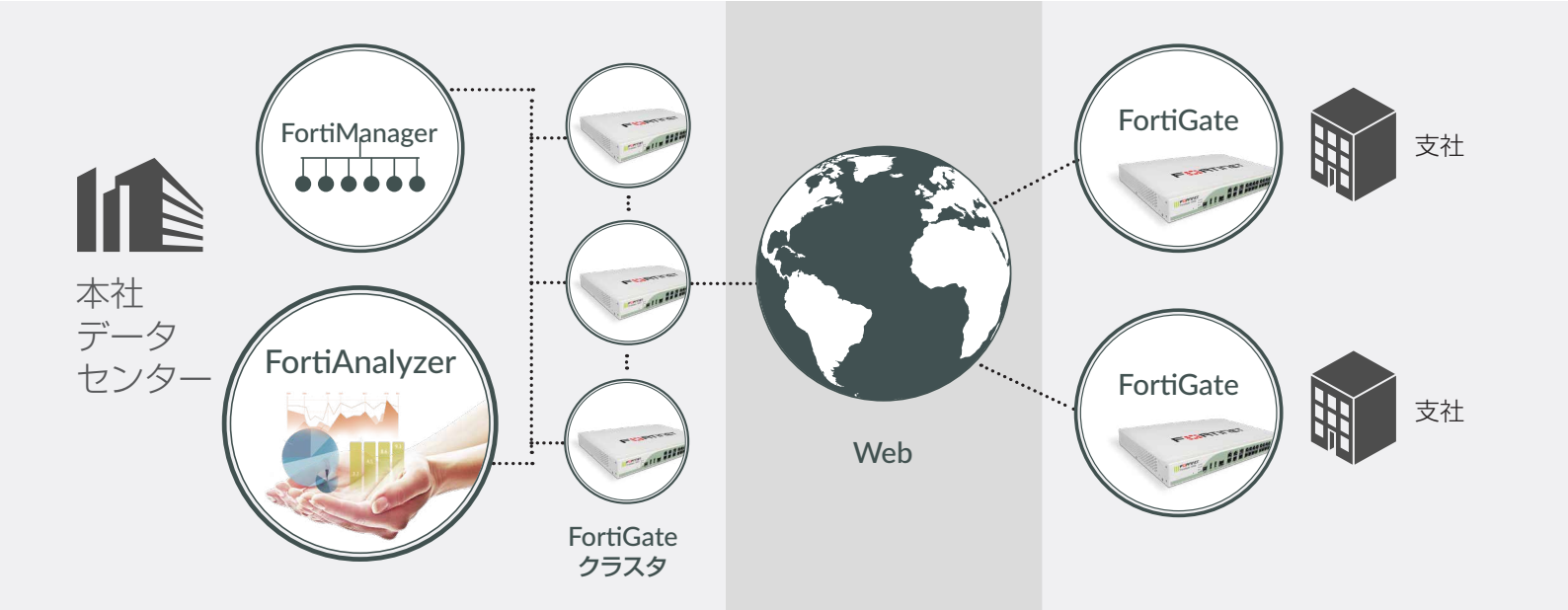
フォーティネット セキュリティ ファブリックでは、フォーティネットのエンタープライズファイアウォールの導入によって持続的な標的型攻撃に対抗するほか、FortiAnalyzer を追加することでセキュリティ ファブリックの可視性を強化し、実用的で確実なセキュリティアラート情報を自動的に提供することで、エンドツーエンドの統一された保護が可能になります。

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。

主な機能と特長

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

導入例



フォーティネット セキュリティ ファブリックは、IoT からクラウドまで企業ネットワークを包括的に保護します。
FortiAnalyzer によって収集、相関付けされた、ファブリックからのネットワークやセキュリティの情報を、単一管理コンソールから確認できます。

ハイライト

FortiView — ネットワークの詳細な可視化

- 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問題をすばやく特定
- 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）
- 無線ユーザー、不正アクセスポイント、およびエンドポイントの脆弱性の詳細ビュー
- グラフやマップによる可視化
- ドリルダウン分析により、攻撃の経路やトランザクションの追跡、新しい実用的なインテリジェンスの発見が可能

図1

IOC（Indicators of Compromise：侵害指標）— FortiGuard の脅威インテリジェンスを活用

- セキュリティログのスキャンによって、不審なトラフィックパターンを識別
- セキュリティ侵害の自動防御システムが、侵害の痕跡を常に監視
- セキュリティ侵害の恐れがあるホストのリストを優先度順に提示
- セキュリティの状態の的確な判断を可能にし、高度な脅威を検知することで組織全体を保護

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可能
- 定義済みポリシーに基づくクォータの自動管理
- 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

レポート

- サンプルレポートが付属する 28 以上のテンプレートを提供
- オンデマンドに加えて、電子メールによる自動通知やカレンダービューに基づくレポート実行のスケジュール指定も可能
- 柔軟なレポートフォーマット：HTML / CSV / XML / PDF
- カスタムレポート：カスタムレポートの作成に利用できる、300 以上のチャートを内蔵

フォレンジック分析のためのログ取得

- 過去のログを取得して、履歴データに対する分析を実行
- 柔軟な取得オプション：すべてのログの取得だけでなく、フィルターによる取得ログの選択も可能
- 容易な構成：クライアント / サーバー間のリモートによるログ取得を数回のクリックでセットアップ

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

- Syslog サーバー、CEF ログサーバー、FortiSIEM、または FortiAnalyzer にログを転送し、長期の保管、フォレンジック分析、法規制へのコンプライアンスに活用
- 柔軟な構成：すべてのログを転送、またはフィルターを使って転送するログを指定可能
- CEF サーバーの Syslog に送信するログフィールドを制御

監視とアラート

- ネットワークをリアルタイムでプロアクティブに監視して、攻撃を特定
- 20 以上のイベント定義をそのまま利用できるだけでなく、高度なカスタマイズも可能
- アラートの自動通知により迅速な対応が可能
- イベントの詳細へのドリルダウンによって、短時間での調査を実現

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）

- 脅威、イベント、ネットワークアクティビティの監視と識別を一元化。事前定義済みの FortiAnalyzer ダッシュボードを使用できるほか、独自にカスタマイズすることも可能（図 2）

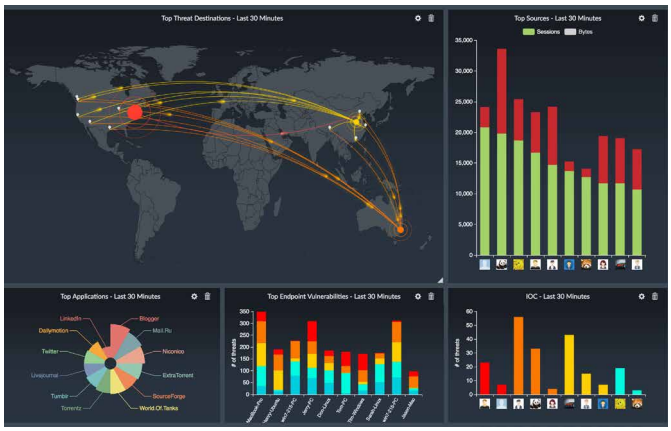


図2.

技術仕様

	FortiAnalyzer 400E	FortiAnalyzer 1000E	FortiAnalyzer 2000E
システム性能			
ログ処理 GB / 日	200	600	1,000
分析用持続レート(ログ / 秒)[1]	6,000	18,000	30,000
コレクタ用持続レート(ログ / 秒)[1]	9,000	27,000	45,000
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)	200	2,000	2,000
最長分析日数[2]	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 GbE	4 x GbE、2 x 10 GbE SFP+
ストレージ	12 TB(4 x 3 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)	6 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)
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	4.3 x 43.7 x 50.3 cm	8.9 x 43.7 x 68.4 cm	8.9 x 43.7 x 64.8 cm
重量	14.1 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)	93 W	192.5 W	293.8 W
放熱	456 BTU/h	920 BTU/h	1,840 BTU/h
動作温度	5 ～ 35 ℃	5 ～ 35 ℃	10 ～ 35 ℃
保管温度	-40 ～ 60 ℃	-40 ～ 60 ℃	-40 ～ 70 ℃
湿度	8 ～ 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 3,000 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

[1] 持続レート - SQLデータベースおよびシステムパフォーマンスの低下がなく、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。
[2] ログレートが低い場合、最長分析日数は増加します。

技術仕様

	FortiAnalyzer 3000F	FortiAnalyzer 3500F	FortiAnalyzer 3700F	FortiAnalyzer 3900E
システム性能				
ログ処理 GB / 日	3,000	5,000	8,300	4,000
分析用持続レート(ログ / 秒)	42,000	63,000	100,000	72,000
コレクタ用持続レート(ログ / 秒)	60,000	90,000	150,000	108,000
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)	4,000	10,000	10,000	10,000
最長分析日数	21	30	60	5
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)	ラックマウント(2 RU)
インタフェース	4 x GbE、2 x GbE SFP	2 x GbE、2 x GbE SFP	2 x SFP+、2 x 1 GbE	2 x GbE、2 x 10 GbE SFP+
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)	15 TB SSD(15 x 1 TB SSD)
利用可能なストレージ(RAID構成時)	42 TB	63 TB	216 TB	12 TB
リムーバブルHDD / 冗長電源(ホットスワップ対応)	✓	✓	✓	✓
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)	○(0、1、5、6、10、50、60)
デフォルトRAIDレベル	50	50	50	50
サイズ				
高さ x 幅 x 奥行	13.2 x 43.7 x 64.8 cm	17.6 x 48.2 x 69.0 cm	17.8 x 43.7 x 76.7 cm	8.9 x 43.7 x 68.4 cm
重量	34.5 kg	42.52 kg	53.5 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、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz、11.5 A(最大)
消費電力(平均)	449 W(12 HDD搭載時)	465 W	850 W	470 W(15 HDD搭載時)
放熱	1,846.5 BTU/h	1,904 BTU/h	4,858 BTU/h	1,351 BTU/h
動作温度	10 ～ 35 ℃	0 ～ 40 ℃	10 ～ 35 ℃	10 ～ 35 ℃
保管温度	-40 ～ 70 ℃	-25 ～ 70 ℃	-40 ～ 70 ℃	-40 ～ 60 ℃
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)	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 2,133.6 m(大気温度 35 ℃)	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	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	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
ハイパーバイザー要件							
サポートするハイパーバイザー	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)、Microsoft Azure						
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

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