

FortiSandbox

提供形態：



アプライアンス 仮想マシン PaaS クラウド

AI を活用した最高レベルのブリーチ防御



FortiSandbox は、フォーティネット セキュリティ ファブリックと統合されたフォーティネットのブリーチ防御ソリューションとして、幅広いデジタル攻撃に AI を活用することで、ランサムウェアやクリプトマルウェアを始め、急速に進化する標的型脅威からの保護を可能にします。第三者機関によるテストで常に最高評価を獲得しており、ゼロデイ、高度なマルウェアの検知とレスポンスの自動化によって、実用的なインテリジェンスをリアルタイムで提供します。



セキュリティ ファブリックで幅広い攻撃対象に対応

ネットワーク、メール、Web アプリケーション、エンドポイントをキャンパスからクラウドまで包括的に保護するほか、さらには、オペレーションテクノロジー（OT）環境で用いられる ICS（産業用制御システム）デバイスも保護対象とし、一体型の拡張可能なアーキテクチャによって、高度な標的型攻撃からの効果的な保護を実現します。



ゼロデイや高度なマルウェアの検知と減災を自動化

ネイティブ統合とオープン API によって、フォーティネットや他社の保護ポイントからのオブジェクトの送信を自動化し、脅威インテリジェンスをリアルタイムで共有することで、脅威への瞬時の対応と同時に制約のあるセキュリティリソースへの負荷の軽減を可能にします。



第三者機関による認定とトップクラスの評価

NSS Labs のブリーチ検知システム（BDS）やブリーチ防御システム（BPS）、ICSA Labs の高度な脅威防御（ATD）など、第三者機関による実環境での厳格なテストで、既知および未知の脅威の検知に関して常に最高評価を獲得しています。

ブリーチ防御

- リモートオフィス
- 支社
- キャンパス
- データセンター
- パブリッククラウド（AWS、Azure）

第三者機関の認定



FortiGuard
セキュリティサービス

www.fortiguard.com



FortiCare Worldwide
Support

support.fortinet.com

ハイライト

AI を活用したサンドボックスによるマルウェア分析

AI を活用した 2 段階のサンドボックスアプローチによって、今ある保護機能がさらに強固なものになります。不審なファイルや高リスクのファイルは、第 1 段階の FortiSandbox の AI を活用した静的分析にかけられ、既知および新たなマルウェアが迅速に特定されます。第 2 段階の分析は隔離された環境で実行され、AI による振る舞い分析をベースに攻撃のライフサイクル全体を明らかにします。AI が新たなマルウェアの手法を継続的に学習することでマルウェアの挙動指標を自動的に更新し、新しいゼロデイ脅威に対する FortiSandbox の動的分析検知エンジンの効率と効果を向上させます。図 1 に示すように、AI ベースの動的分析によって発見された新たな脅威がリアルタイムで表示されます。

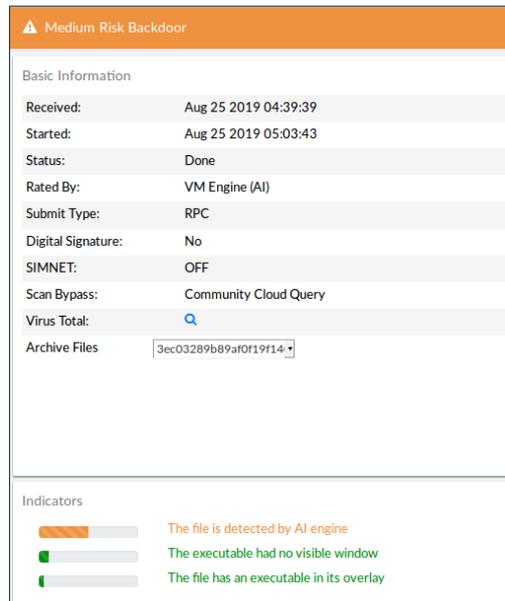


図 1 : AI ベースの動的分析

MITRE ATT&CK ベースのレポート / 調査ツール

FortiSandbox は詳細な分析レポートを提供し、発見されたマルウェアの手法は、組み込みの調査ツールによって MITRE ATT&CK フレームワークにマッピングされます。セキュリティオペレーション(SecOps)チームは、この高性能なツールを用いて、キャプチャしたパケット、オリジナルファイル、トレーサーのログ、マルウェアのスクリーンショット、および STIX 2.0 準拠の IOC をダウンロードし、ファイルの検証後に詳細な脅威インテリジェンスを取得して実効性の高い対策を実施できます (図 2 を参照)。

また、セキュリティオペレーションチームでは、マルウェアのすべてやり取りをビデオで記録する、あるいは仮想環境において手動でマルウェアとやり取りすることを選択できます。

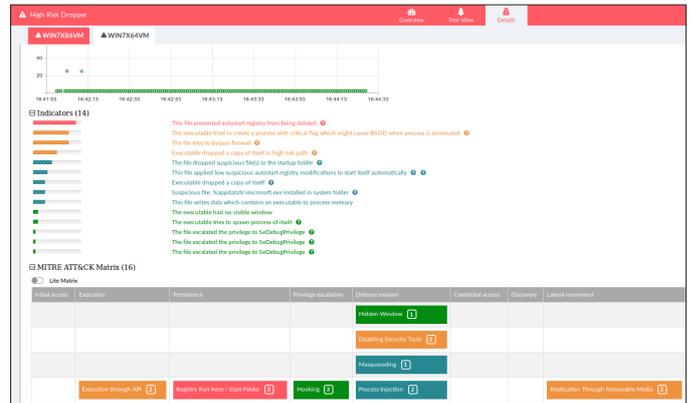


図 2 : MITRE ATT&CK マトリックスと組み込みツール

ブリーチ防御の自動化

FortiSandbox はフォーティネットの様々なセキュリティ製品との統合が可能で、極めてシンプルな設定でブリーチ防御対策の自動化を実現します。不正なコードが特定されると、FortiSandbox がリスク評価を返し、ローカルのインテリジェンスがフォーティネットや、フォーティネット ファブリック レディ パートナー、他社のセキュリティソリュー

ションとリアルタイムで共有されて、新しい高度な脅威に対する減災と予防措置に利用されます。ローカルインテリジェンスをフォーティネットの脅威研究チームである FortiGuard Labs と共有し、世界中の企業や組織の保護に活用することもできます (オプション)。図 3 に、自動減災プロセスのワークフローを示します。

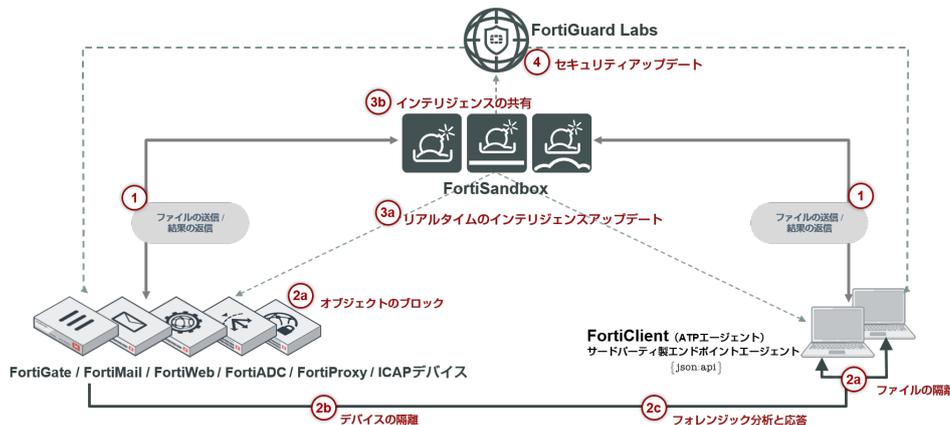


図 3 : FortiSandbox の脅威減災ワークフロー

- クエリ**
- ① 分析用にファイルを送信し、分析結果を受信
- 減災**
- ②a 送信デバイス上でオブジェクトをブロック / エンドポイント上でファイルを隔離
- ②b エンドポイントの隔離
- ②c より詳細な検査および応答
- アップデート**
- ③a 統合されたデバイスにセキュリティ侵害指標 (IOC) を共有
- ③b 分析結果をFortiGuardと共有 (オプション)
- ④ すべての顧客 / デバイスの保護を改善

導入オプション

容易な導入配備

FortiSandbox は、単体のアプライアンスで数多くのプロトコルの検証をサポートしているため、ネットワークとセキュリティのインフラストラクチャを簡素化し、容易な運用を実現して TCO を削減します。さらに、セキュリティ ファブリック プラットフォームに統合することで、高度な脅威保護のレイヤーが既存のセキュリティアーキテクチャに追加されます。

FortiSandbox は、市場で最も柔軟性の高い分析アプライアンスで、お客様固有の構成や要件に最適な導入オプションを選択することができます。さらに、企業や組織はこれらの導入オプションを組み合わせることで選択することが可能です。

フォーティネット製品との統合

FortiSandbox は、FortiGate、FortiMail、FortiWeb、FortiADC、FortiProxy、FortiClient (ATP エージェント)、ファブリック レディ パートナー 各社のソリューションとネイティブに統合され、サードパーティセキュリティベンダーとは JSON API または ICAP 経由で連携します。不審なコンテンツはインターセプトして FortiSandbox に送信できます。また、統合されているこのようなデバイスすべてにおいてタイムリーに保護対策が改善されるとともに、詳細なレポート機能も提供されます。

この方法では、他の FortiSandbox も統合されるため、リアルタイムのインテリジェンスを瞬時に共有でき、複数の FortiSandbox を地理的に離れた場所に導入する大企業にとって、大きなメリットとなります。このゼロタッチの自動化モデルは、国やタイムゾーンが異なる場所への包括的な保護に最適です。

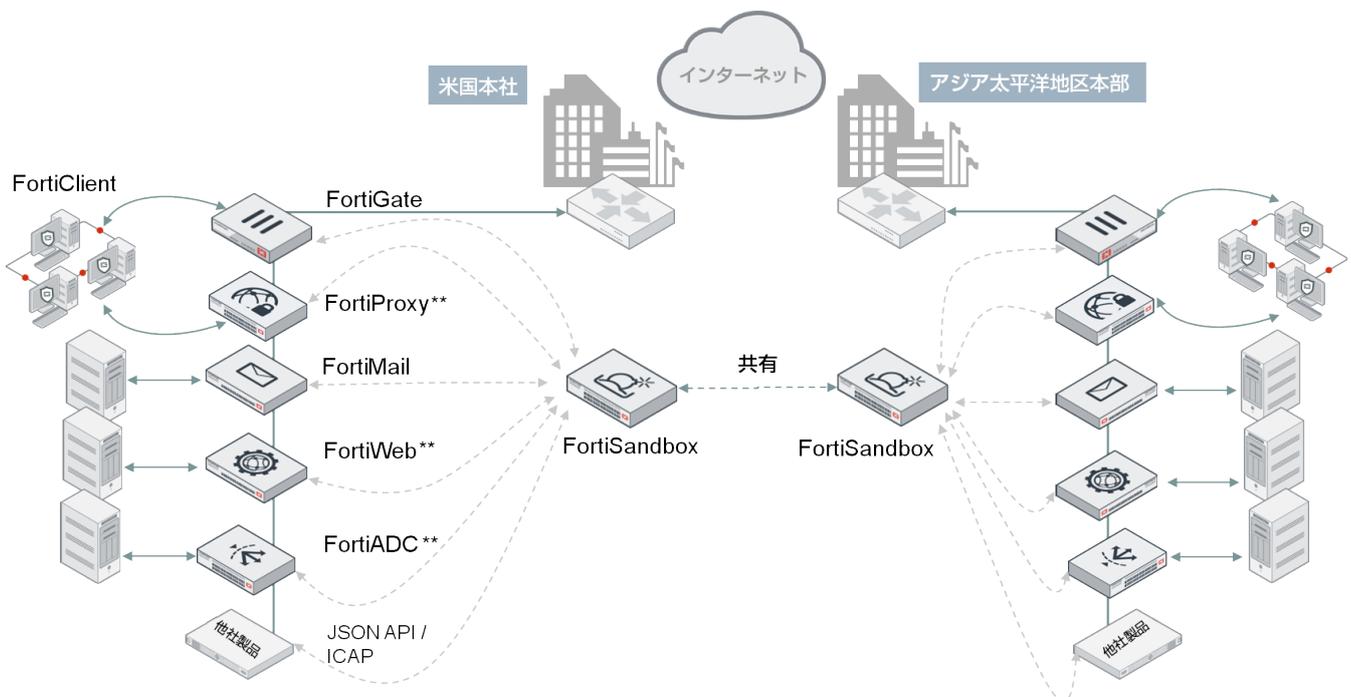


図 4：フォーティネット製品との統合導入モード

スタンドアロン

FortiSandbox のこの導入モードでは、ネットワークスイッチのスパン（ミラーリング）ポートまたはネットワークタップ、MTA または BCC モードの E メールからの入力を使用できます。また、SecOps の分析者が GUI を使用してオンデマンドでファイルをアップロードすることや、CIFS / NFS プロトコルや、AWS S3、Azure Blob 経由でファイルレポジトリをスキャンすることも可能で、複数ベンダーの製品による既存の脅威保護アプローチを強化する場合に理想的な選択肢となります。

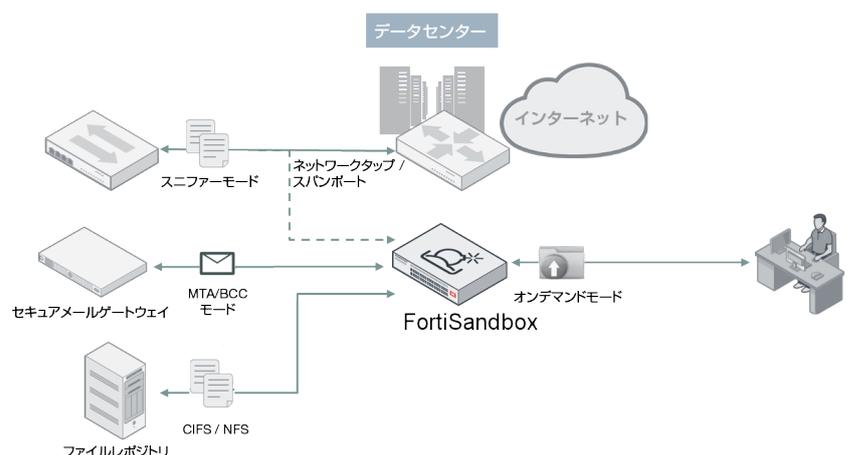


図 5：スタンドアロン導入モード

主な機能と特長

高度な脅威保護

ランサムウェアをはじめとする新たな脅威の検査、パスワード保護されたマルウェアの滅災
AI 活用による、実行されていないコード内に存在する可能性のある脅威を特定する静的コード分析

仮想 OS サンドボックス:

- AI による振る舞い分析により新しいマルウェアの手法を継続的に学習
- 複数インスタンスの同時処理に対応
- サポートする OS : Windows 10、Windows 8.1、Windows 7、macOS、Linux、Android、ICS システム
- 独自の Windows / Linux OS やアプリケーションで VM をカスタマイズ
- 侵入対策技術: スリープ状態のコール、プロセスおよびレジストリの照会ほか
- コールバックの検出: 活性化したマルウェアが実行する不審な URL へのアクセス、ポットネットによる C&C サーバとの通信および攻撃トラフィック
- キャプチャしたパケット、オリジナルファイル、トレーサのログおよびスクリーンショットのダウンロード
- サンドボックスインタラクティブモード
- マルウェアのやりとりのビデオ録画

ヒューリスティック / パターン / レピュテーションベースの分析

サポートするファイルタイプ:

.7z、.ace、.apk、.app、.arj、.bat、.bz2、.cab、.cmd、.dll、.dmg、.doc、.docm、.docx、.dot、.dotm、.dotx、.eml、.elf、.exe、.gz、.htm、.html、.iqy、.iso、.jar、.js、.kfg、.lnk、.lzh、.Mach-O、.msi、.pdf、.pot、.potm、.potx、.ppam、.pps、.ppsm、.ppsx、.ppt、.pptm、.pptx、.ps1、.rar、.rtf、.sldm、.sldx、.swf、.tar、.tgz、.upx、.rl、.vbs、.WEBLink、.wsf、.xlam、.xls、.xlsb、.xism、.xlsx、.xlt、.xltm、.xltx、.xz、.z、.zip

サポートするプロトコル / アプリケーション:

- FortiGate との統合モード: HTTP、SMTP、POP3、IMAP、MAPI、FTP、IM およびこれらの SSL 暗号化バージョン
- FortiMail との統合モード: SMTP、POP3、IMAP
- FortiClient EMS との統合モード: HTTP、FTP、SMB
- FortiWeb との統合モード: HTTP
- ICAP クライアントとの統合モード: HTTP
- スニファーモード: HTTP、FTP、POP3、IMAP、SMTP、SMB
- MTA / BCC モード SMTP

サポートする OT プロトコル: tftp、modbus、s7comm、http、snmp、bacnet、ipmi

VM イメージのトラフィックをシステムトラフィックから分離

スニファーモードでのネットワーク脅威検知: ポットネットの挙動やネットワーク攻撃、不審な URL へのアクセスの特定

SMB / NFS ネットワーク共有のスキャンおよび不審なファイルの隔離。
スキャンのスケジューリングが可能

ドキュメントファイルに埋め込まれた URL のスキャン

サードパーティ製 Yara ルールとの統合

オプションで不審なファイルをクラウドサービスに自動送信し、アナリストによる分析とシグネチャの作成が可能

サードパーティによる追加のスキャンングに対応するネットワーク共有へのファイル転送オプション

ファイル送信によるブラックリストおよびホワイトリスト作成

スキャンとクエリ用のメールやファイルからの URL 送信

システム統合

ファイル送信方式: FortiGate、FortiMail、FortiWeb、FortiADC、FortiProxy、FortiClient (ATP エージェント)

ファイルステータスのフィードバックとレポート: FortiGate、FortiMail、FortiWeb、FortiADC、FortiProxy、FortiClient (ATP エージェント)

動的な脅威 DB アップデート:

- FortiGate、FortiMail、FortiWeb、FortiADC、FortiProxy、FortiClient (ATP エージェント)
- 登録済エンティティ向けの定期的な動的 DB のプッシュ送信
- ファイルのチェックサムと不正 URL の DB

データベースプロキシの更新: FortiManager

リモートログ管理: FortiAnalyzer、FortiSIEM、Syslog Server

JSON API を使用することで、サンプルをアップロードし、実用的なマルウェアインジケータをダウンロードして修復するプロセスの自動化が可能

認定他社製品との統合: CarbonBlack、Ziften、SentinelOne

FortiSandbox 間での IOC (Indicators of Compromise: 侵害指標) の共有

ネットワーク / 導入

ファイル入力方式: 統合されたデバイスからのファイル送信、スニファーモード、オンデマンドのファイルアップロード

隔離されたネットワークのサポート

高可用性クラスタリングのサポート

ポート監視により、クラスタ内のフェイルオーバーをサポート

静的ルーティングのサポート

監視およびレポート

リアルタイムの監視用ウィジェット: スキャン結果の統計、スキャン実行情報 (経時的)、標的となったホスト上位リスト、検出されたマルウェア上位リスト、感染されている URL 上位リスト、コールバックドメイン上位リスト

イベントの詳細ビューアー: 挙動、マルウェア名、評価、種類、ソース、送信先、検出時刻およびダウンロード経路を動的にテーブル表示

レポートとログ: GUI での表示、PDF と RAW ログファイルのダウンロード

レポート生成: MITRE ATT&CK ベースのレポート: ファイルの変更、プロセスの挙動、レジストリの挙動、ネットワークの挙動

サンプルファイル、サンドボックストレーサのログ、PCAP キャプチャおよびインジケータ (STIX 2.0 フォーマット)

管理

GUI および CLI による設定が可能

複数の管理者アカウントを作成可能

設定ファイルのバックアップとリストア

不審なファイルが検出されると電子メールで通知

グローバルな電子メールのリストおよび管理者に毎週レポートを送信

一元化された検索ページでは、管理者による検索条件のカスタマイズが可能

高頻度なシグネチャの自動更新

新しい VM イメージの自動確認とダウンロード

仮想マシンの状態監視

管理者向けの Radius 認証



技術仕様

	FortiSandbox 500F	FortiSandbox 1000F/-DC	FortiSandbox 2000E	FortiSandbox 3000E	FortiSandbox 3000F
ハードウェア					
ネットワークインタフェース	4 x GbE RJ45 インタフェース	4 x GbE RJ45 インタフェース、4 x GbE SFP インタフェース	4 x GbE RJ45 インタフェース、2 x 10 GbE SFP+ インタフェース	4 x GbE RJ45 インタフェース、2 x 10 GbE SFP+ インタフェース	4 x GbE RJ45 インタフェース、2 x 10 GbE SFP+ インタフェース
ストレージ	1 x 1 TB	2 x 1 TB	2 x 2 TB	4 x 2 TB	4 x 2 TB
電源装置	1 x PSU	1 x PSU、2 台め PSU (オプション、ホットスワップ対応)	2 x 冗長 PSU (ホットスワップ対応)	2 x 冗長 PSU (ホットスワップ対応)	2 x 冗長 PSU (ホットスワップ対応)
システム性能					
VM 数	6*	14*	24*	56*	72*
サンドボックスのプリフィルタ処理 (ファイル数 / 時) ¹	4,500	7,500	12,000	15,000	18,000
VM のサンドボックス処理 (ファイル数 / 時)	120	280	480	1,120	1,340
実環境の処理効率 (ファイル数 / 時)	600 ²	1,400 ²	2,400 ²	5,600 ²	6,720 ²
スニファースループット	500 Mbps	1 Gbps	4 Gbps	8 Gbps	9.6 Gbps
MTA 性能	5,000 メール / 時	10,000 メール / 時	15,000 メール / 時	35,000 メール / 時	42,000 メール / 時
サイズ					
高さ x 幅 x 奥行	44 x 438 x 320 mm	44 x 438 x 580 mm	88 x 438 x 530 mm	89 x 437 x 738 mm	88 x 438 x 601 mm
重量	8.5 kg	11.34 kg	12.25 kg	19.52 kg	20 kg
形状	1 RU	1 RU	2 RU	2 RU	2 RU
電源装置 (AC / DC)	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz / -48 VDC	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz	100 ~ 240 V AC、50 ~ 60 Hz
最大電流 (AC / DC)	100 V / 8A、240 V / 4 A	100 V / 5 A、240 V / 3 A / -48 VDC / 9 A	100 V / 8 A、240 V / 4 A	100 V / 9.8 A、240 V / 5 A	100 V / 10 A、240 V / 5 A
消費電力 (平均 / 最大)	30.1 / 76.3 W	66.93 / 116.58 W	164.7 / 175.9 W	538.6 / 549.6 W	462.1 / 392.8 W
放熱	260.34 BTU/h	397.75 BTU/h	600.17 BTU/h	1,943.82 BTU/h	1,610.81 BTU/h
動作環境					
動作温度	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	10 ~ 35 °C	0 ~ 40 °C
保管温度	-20 ~ 70 °C	-40 ~ 70 °C	-20 ~ 70 °C	-40 ~ 70 °C	-40 ~ 70 °C
湿度	5 ~ 90% (結露しないこと)	5 ~ 90% (結露しないこと)	5 ~ 90% (結露しないこと)	8 ~ 90% (結露しないこと)	5 ~ 90% (結露しないこと)
準拠規格					
規格・認定	FCC Part 15 Class A、RCM、VCCI、CE、BSMI、KC、UL / cUL、CB、GOST				
FortiSandbox VM					
システム要件					
サポートするハイパーバイザー	VMware ESXi、Linux KVM CentOS、Microsoft Hyper-V、Nutanix、AWS、Azure				—
仮想 CPU 数 (最小 / 最大)	4 / 無制限 (仮想 CPU 数を Windows VM 数 + 4 と一致させることを推奨します)				4
メモリ (最小 / 最大)	8 GB / 無制限				8 GB
仮想ストレージ容量 (最小 / 最大)	30 GB / 16 TB				200 GB
仮想ネットワークインタフェース (最小)	6				—
システム性能					
スニファースループット	1 Gbps				N.A.
サンドボックスのプリフィルタ処理 (ファイル数 / 時) ¹	システム構成に依存				
ローカル VM					
VM 数	ノードあたり 8 VM、クラスターあたり最大 99 ノード				5 (最大 200 Windows Cloud VM)
VM のサンドボックス処理 (ファイル数 / 時)	システム構成に依存				100、最大 4,000
実環境の処理効率 (ファイル数 / 時) ²	システム構成に依存				500、最大 20,000
クラウド VM					
VM 数	1 (最大 200 VM)				
VM のサンドボックス処理 (ファイル数 / 時)	システム構成に依存				20、最大 4,000
実環境の処理効率 (ファイル数 / 時) ²	システム構成に依存				100、最大 20,000
準拠規格					
規格・認定	—				SOC2

注：数値はすべて「最大」の性能値であり、利用環境およびシステム構成に応じて異なります。

* デフォルトで Windows VM ライセンスがハードウェアに付属しています：FortiSandbox 500F (2 つ)、FortiSandbox 1000F/-DC (2 つ)、FortiSandbox 2000E (4 つ)、FortiSandbox 3000E (8 つ)、FortiSandbox 3000F (8 つ)。

VM 数の追加は、アップグレードライセンスとして販売されます。

¹ FortiSandbox では、FortiGuard インテリジェンスを利用してプリフィルタリングを実行します。

² プリフィルタおよび動的分析が連続的に実行される場合は、実環境の Web および電子メールのトラフィックに基づいて算出されます。



FortiSandbox 500F



FortiSandbox 1000F/-DC



FortiSandbox 2000E



FortiSandbox 3000F



インテグレーションマトリックス

	FortiGate	FortiClient	FortiMail	FortiWeb	FortiADC	FortiProxy
FortiSandbox アプライアンスと VM	FortiOS V5.6 以降	FortiClient for Windows OS V5.6 以降	FortiMail OS V5.4 以降	FortiWeb OS V5.6 以降	FortiADC OS V5.0 以降	FortiProxy OS V1.2.3 以降
FortiSandbox Cloud	FortiOS V6.4.2 以降、 6.2.5 以降	FortiClient for Windows OS V6.4.4 以降、7.0 以降	FortiMail V6.4.3 以降	—	—	—

オプションアクセサリ

Optional Accessories		
1 GE SFP SX Transceiver Module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FSA1000F-PS	AC power supply for FDC-1000F, FIS-1000F, FSA-1000F modules only.
DC Power Supply	SP-FSA1000F-DC-PS	DC power supply for FSA-1000F-DC module only.

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