SONICWALL製品ラインナップ：一覧

次世代ファイアウォール
ハイエンド：NS*sp* 15700
大規模分散企業、データセンター、MSP向けに設計されたマルチインスタンスファイアウォールであり、高速保護、高ポート密度、真のテナント分離を統一ポリシーで提供

ミッドレンジ：NS*a*シリーズ
NS*a* 9650/9450/9250/
6650/5650/4650/3650/2650
中規模のネットワーク、支店・支局、分散型企業向けに、業界で検証済みセキュリティの有効性とパフォーマンスを実現

エントリレベル：TZシリーズ
TZ670/TZ570/TZ400/TZ350
中小規模組織やSDブランチ導入組織向けの統合型の脅威防止およびSD-WANプラットフォーム

バーチャル：NSvシリーズ
柔軟性の高いライセンスモデルを備えた仮想ファイアウォールにより、パブリックおよびプライベートクラウドインフラストラクチャの重要なコンポーネントをすべて保護

Wireless Security
SonicWaveシリーズ
SonicWave 432e/432i/432o/
231c/224w/231o
次世代のワイヤレスデバイス向けに構築されたセキュリティとパフォーマンスをクラウドまたはファイアウォール経由で管理

Secure Mobile Access
SMA Series SMA 8200v/7210/
6210/500v/410/210
ネットワークおよびクラウドリソースへのシンプルでポリシーに準じた安全なアクセス

Access Switch
SWS12-8/SWS12-8POE/SWS12-10FPOE/
SWS14-24/SWS14-24FPOE/SWS14-48/
SWS14-48FPOE
SMBとSDブランチ導入にて次世代セキュア接続によるインテリジェントスイッチを実現

Eメールセキュリティシリーズ
ESA 9000/7000/5000/
VMソフトウェア/クラウドサービス
高度なメール脅威から保護する多層ソリューション

管理および分析
Capture Security Center
グローバル管理システム（GMS）
Network Security Manager
ネットワークの制御と知見がパワーとなる

Capture Security Appliance (CS*a*)
オンプレミスファイルのチェックとマルウェアの阻止。

Capture Client
高度なマルウェア保護、サンドボックス、アプリケーション脆弱性インテリジェンス、感染時のロールバックなど、複数のエンドポイント保護機能を提供する一体型クライアントプラットフォーム

Cloud App Security
Office 365やG Suiteなどの SaaSアプリケーションに次世代セキュリティを実現したCASBソリューション。クラウドでのコンプライアンスを確保しながら、高度な脅威からEメール、データ、ユーザー認証情報などを保護します

次世代のファイアウォールサブスクリプションサービス

Essential Protection Services Suiteは、あらゆる必須セキュリティサービスを提供して、既知の脅威や未知の脅威から保護します。これにより、RTDMIテクノロジーによるキャプチャ高度脅威保護、ゲートウェイ型アンチウイルス、侵入防止およびアプリケーション制御、コンテンツフィルタリングサービス、包括的なスパム対策サービス、ネットワーク可視性、24時間365日のサポートなどを提供。

Advanced Gateway Security Suite (AGSS)は、すべての物理的および仮想的SonicWallファイアウォールのアドオンサービスとしてご利用いただくことで、最も高度で未知の脅威から保護します。

Advanced Gateway Security Suite (AGSS) 以下サービスをバンドル。TotalSecure Advanced Editionでの次世代ファイアウォールと組合せてご利用いただけます。

- Capture Advanced Threat Protection (ATP) クラウドベースのマルチエンジンサンドボックス
- ゲートウェイウイルス対策およびスパイウェア対策
- 侵入防止サービス
- アプリケーションコントロール
- コンテンツ/Webフィルタリングサービス
- 24時間365日のサポート

Security-as-a-Service (SECaaS)
ターンキーソリューションでネットワークセキュリティをアウトソーシング

詳細は sonicwall.com をご覧ください

お客様に投げかけるべき質問集

次世代ファイアウォール

- マルチギガビットのパフォーマンスのニーズを満たす帯域幅の増加に対応できますか。
- 現在使用しているファイアウォールは、受信される脅威の割合で脅威を検証を実行できますか。
- パフォーマンス基準について教えてください。
- ファイアウォールの背後にあるユーザー/ネットワークの総数はどのくらいありますか。
- ピーク時のセッション/接続総数はどのくらいありますか。
- ファイアウォールに接続するリモートサイトとユーザーの数はどのくらいありますか。
- セキュリティコントロールの有効性をどのように評価していますか。
- インターネット接続はどのようなタイプですか。通信速度はどの程度ですか。
- ゼロデイ攻撃などの新しい脅威から保護するために、どのような対策を講じていますか。
- ご使用のサンドボックスは、ディープメモリに隠れた脅威を検出し、ブロックすることができますか。
- サンドボックスには、何個のエンジンが組み込まれていますか。
- サンドボックスは、検査が終わるまでゲートウェイでファイルを保持できますか。
- 組織で適用されているファイアウォールがHTTPSトラフィックを検査しているかどうかご存知ですか。
- HTTPSトラフィック検査のために、ネットワークサービスの中断やダウンタイムが発生したことがありますか。
- 適用されている仮想ファイアウォールの堅牢性は、物理ファイアウォールと同程度にありますか。
- パブリッククラウドまたはプライベートクラウド環境をどのように保護していますか。
- 仮想ネットワークには、適切なセキュリティゾーニングとマイクロセグメンテーションを実装できていますか。
- 仮想トラフィックに対し、可視性と制御が完全に得られていますか。
- MPLSをSD-WANに置き換えることで安全なプライベートネットワークを構築することにより、コストを削減することに関心はおありでしょうか。

Capture Client

- エンドポイントには、ランサムウェアや暗号化された脅威に対して一貫した高度な保護が必要ですか。
- エンドポイント全体に対し、ポリシーのコンプライアンスとライセンス管理をどの程度簡単に適用できますか。
- エンドポイントの可視性とセキュリティ体制の管理に苦労していますか。
- サンドボックス環境に、エンドポイントセキュリティー向けの製品が接続されていますか。
- エンドポイントにインストールされているアプリケーションを分類整理し、その範囲にどのくらいの脆弱性が存在するかご存知ですか。
- 現在利用されているソリューションは、システム状態を継続的に監視していますか。
- ランサムウェアによる被害を元のクリーンな状態に戻すことはできますか。
- 未知のデバイスや感染の可能性をもつデバイスがエンドポイントに接続されることを回避する機能を装備していますか。

Cloud App Security

- O 365かG Suiteを使用されていますか。
- O 365/G Suiteを保護するために、ProofpointまたはMimecastを使用されていますか。
- O 365の社内メールをスキャンしていますか。
- 許可されたSaaSアプリケーションは、組織内にていくつ使用されていますか。
- SaaSアプリケーションに保存されたデータのコンプライアンス管理に苦労していますか。
- ユーザーの資格情報が侵害されているかどうか、どのようにして確認していますか。
- 誰が、どこから、いつ、データにアクセスしているか、視覚的に確認できますか。(BYOD)

Inspect Deep Memory

特許出願中のシステムであるSonicWall Real-Time Deep Memory Inspection (RTDMI™) エンジンは、リアルタイムでメモリを精査し、未知の大量に出回っているマルウェアをプロアクティブに検出・ブロックします。このエンジンは、SonicWall Capture Advanced Threat Protection (ATP) クラウドサンドボックスサービスで利用可能となり、後々発生するメルトダウンによる悪意ある行為など、最も狡猾となる最新の脅威であっても特定・回避します。

Wireless Security

- 従業員/パートナー/お客様から、Wi-Fiの通信速度が遅いとのクレームがありますか。
- ワイヤレスユーザーの最大人数はどのくらいですか。
- セキュリティ保護されたワイヤレスソリューションをネットワークに追加する場合、そのコストが気になりますか。
- 802.11ac Wave 2ワイヤレス規格については、どの程度ご存知ですか。
- アクセスポイントの管理（クラウド管理とファイアウォール管理）に柔軟性が必要であると思いますか。
- WiFiネットワークを効果的に構築しましたか。
- APをファイアウォールから切り離す必要がありますか。
- WiFiネットワークで高度なセキュリティ機能を備えることに不安がありますか。
- お客様へのサービスは重要となりますか。
- 来訪者用にカスタマイズ出来るゲスト用ログインポータルが必要ですか。

Access Switch

- PoE対応デバイスに電力を供給するには、ギガビット対応のアクセススイッチが必要ですか。
- 統一された可視性と管理を備えた一体化セキュリティ体制は、あなたにとって重要はシステムでしょうか。
- SonicWallのエコシステムで作動するサードパーティ製スイッチを用いるソリューションに問題を抱えていますか。

Secure Mobile Access

- 現在、リモートワークフォースアクセスにどのような方法を用いていますか。
- ゼロトラストネットワークアクセスによるアプローチの採用について、どのようにお考えですか。
- オンプレミスやクラウドでホストされた企業のリソースやアプリケーションへの安全なアクセスをどのように確保していますか。
- ネットワークにアクセスするユーザーとデバイスをすべて把握していますか。
- 現在、ビジネスクリティカルとなるWebプロパティやWebサーバをどのように保護していますか。

電子メールセキュリティ

- ランサムウェア、スピアフィッシング、ビジネスメールの侵害など、高度なEメールの脅威に対して不安を抱えていますか。
- 現在のEメールセキュリティソリューションは、高度な脅威保護機能を備えていますか。
- 機密情報を含むメールが外部に漏れることが懸念されますか。
- GDPR、Sarbanes-Oxley、GLBA、HIPAAなどのレギュレーションをどのように順守していますか。
- お客様にマネージドメールセキュリティサービスを提供したいとお考えですか。(MSSP)

管理およびアナリティクス

- 単一の管理プラットフォームにセキュリティソリューションを一体化することで、どのような問題が解決できるでしょうか。
- セキュリティインフラストラクチャの管理に関して、どのような経済上および運用上の課題を抱えていますか。
- PCI、HIPPA、GDPRなどのサイバーセキュリティコンプライアンスを確実に準拠していることを示せますか。
- 脅威やリスクを迅速かつ正確に検出し、対応することができた場合、セキュリティ体制はどのように変化すると思われますか。
- サイバー脅威とビジネスに対するリスクを完全に可視化することで、自社とそのリーダーシップチームはどのような価値を享受できるでしょうか。

詳細は sonicwall.com をご覧ください