

# Advanced Gateway Security Suite

完全なネットワークセキュリティを1つの統合パッケージで実現

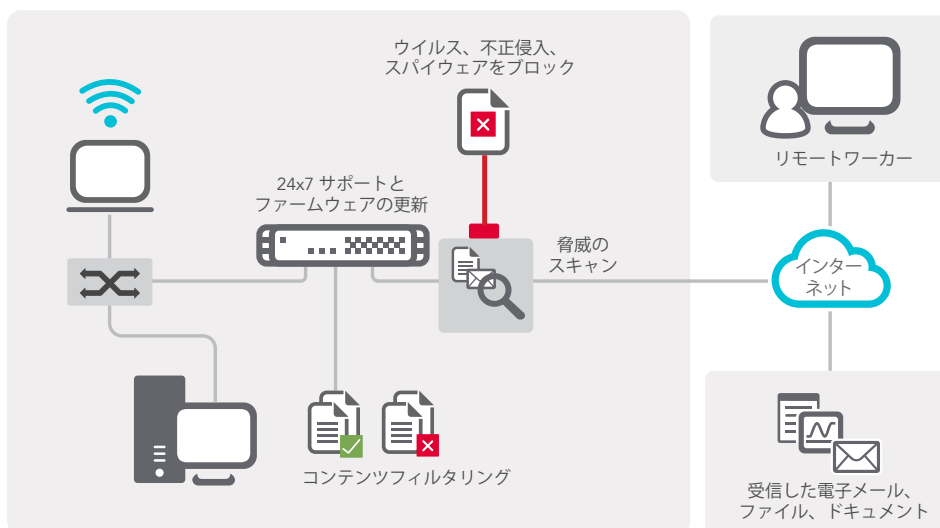
ネットワークセキュリティは複雑になりがちですが、既知および未知の悪意ある脅威からネットワークを保護するのに、こうした複雑さは不要な存在です。SonicWall Advanced Gateway Security Suite (AGSS) は、包括的な保護に必要なすべてのネットワークセキュリティサービスを、利便性に優れたお求めやすいパッケージに統合することで、アドオンセキュリティサービスのホスト選択に伴う複雑さを解消します。

NSa および NSv シリーズ、SuperMassive シリーズ、TZ シリーズなど、すべての物理 / 仮想ファイアウォールで利用可能な SonicWall AGSS は、ゼロデイ攻撃、ウイルス、不正侵入、ボットネット、スパイウェア、トロイの木馬、ワームなどの悪意のある攻撃からネットワークを保護します。クラウドベースの多層型サンドボックスインスペクションにより、疑わしいファイルをゲートウェイで検査し、未知の脅威からネットワークを保護します。新たな脅威が特定されると、その脅威を防御するシグネチャが SonicWall ファイア

ウォールと Capture Cloud データベースで即座に自動更新されます。多くの場合、これはソフトウェアベンダーがソフトウェアにパッチを適用する前に行われます。すべての SonicWall ファイアウォールは、さまざまなアプリケーションタイプとプロトコルのトラフィックをスキャンする、特許取得済みの Reassembly-Free Deep Packet Inspection® エンジンを搭載し、内部および外部の攻撃とアプリケーションの脆弱性から 24 時間体制でネットワークを保護します。SonicWall ソリューションは、インターネット使用ポリシーを適用して、不適切で非生産的かつ違法の疑いがある Web コンテンツへの内部アクセスを包括的なコンテンツフィルタリングで制御するツールも提供します。さらに、この多彩なサービスバンドルには、24 時間体制のテクニカルサポート、重要なファームウェア更新、ハードウェア交換も含まれています。

## 導入効果:

- 完全なネットワークセキュリティソリューション
- ICSA 認定のゲートウェイアンチウイルス / アンチスパイウェア対策
- 最先端の IPS テクノロジー
- アプリケーションインテリジェンスおよび制御
- コンテンツフィルタリング
- ファームウェア更新とハードウェア交換に対応する 24x7 サポート
- SonicWall RTDMI を備えたマルチエンジンネットワークサンドボックス



## Advanced Gateway Security Suite

SuperMassive 9800 (1 年間)  
01-SSC-1183

SuperMassive 9600 (1 年間)  
01-SSC-1590

SuperMassive 9400 (1 年間)  
01-SSC-1580

SuperMassive 9200 (1 年間)  
01-SSC-1570

NSA 6600 (1 年間)  
01-SSC-1560

NSa 5650 (1 年間)  
01-SSC-3674

NSa 4650 (1 年間)  
01-SSC-3493

NSa 3650 (1 年間)  
01-SSC-3451

NSa 2650 (1 年間)  
01-SSC-1783

TZ600 (1 年間)  
01-SSC-1460

TZ500 シリーズ (1 年間)  
01-SSC-1450

TZ400 シリーズ (1 年間)  
01-SSC-1440

TZ300 シリーズ (1 年間)  
01-SSC-1430

NSv 1600 (1 年間) 01-SSC- 5787

NSv 800 (1 年間) 01-SSC- 5737

NSv 400 (1 年間) 01-SSC- 5681

NSv 300 (1 年間) 01-SSC- 5584

NSv 200 (1 年間) 01-SSC- 5306

NSv 100 (1 年間) 01-SSC- 5219

NSv 50 (1 年間) 01-SSC- 5194

NSv 25 (1 年間) 01-SSC- 5165

NSv 10 (1 年間) 01-SSC- 5008

複数年の SKU を利用できます。

SonicWall ファイアウォールの全製品の SKU については、[www.sonicwall.com](http://www.sonicwall.com) をご覧ください。

SonicWall Advanced Gateway Security Suite は、以下の機能を備えています。

- ゲートウェイアンチウイルス、アンチスパイウェア、侵入防御、アプリケーションインテリジェンスおよび制御サービスのサブスクリプション
- コンテンツフィルタリングサービスのサブスクリプション
- 24x7 サポートのサブスクリプション
- Capture Advanced Threat Protection (ATP) サービスのサブスクリプション

### 特長と利点

この完全なネットワークセキュリティソリューションには、さまざまな脅威（ランサムウェア、ウイルス、スパイウェア、ワーム、トロイの木馬、アドウェア、キーロガー、悪意のあるモバイルコード (MMC)、その他の危険なアプリケーションと Web コンテンツ）に対する包括的な保護に必要なすべての要素が統合されています。

**Capture Advanced Threat Protection (ATP)** サービスは、未知の攻撃やゼロデイ攻撃をゲートウェイで阻止する、クラウドベースのマルチエンジンソリューションと自動修復機能により、高度な脅威の検出とサンドボックスに変革をもたらします。

Capture ATP には、悪意のある動作を示さないマルウェアや暗号化で武器を隠蔽しているマルウェアを検出してブロックする、SonicWall Real-Time Deep Memory Inspection (RTDMI) テクノロジーが実装されています。メモリー内で武器を示すようにマルウェアに強制することで、RTDMI エンジンは、大量に出回っているゼロデイ脅威や未知のマルウェアをプロアクティブに検出してブロックします。これは、メモリーベースのリアルタイムインスペクションの技術を正しく活用することで可能になります。

**ICSA 認定のゲートウェイアンチウイルス / アンチスパイウェア対策は、ネットワークベースのマルウェア対策と、数千万件のマルウェアシグネチャを登録したクラウドデータベースを組み合わせることで、高度な最新の脅威に対する強固なセキュリティ保護を実現します。**

**最先端の IPS テクノロジーは、すべてのネットワークトラフィックをスキャンし、不正なパターンや異常なパターンの有無を調べることで、ワーム、トロイの木馬、ソフトウェアの脆弱性、その他の不正侵入を防ぎ、ネットワークの信頼性とパフォーマンスを高めます。**

**アプリケーションインテリジェンスおよび制御**は、アプリケーション固有の一連のポリシーセットであり、アプリケーションの分類とポリシーの適用を通じて、業務用アプリケーションとそれ以外のアプリケーションのどちらも管理者が制御、管理できるよう支援します。

**コンテンツフィルタリング**は、安全性、セキュリティ、生産性の課題に対処します。これは、インターネット使用ポリシーの適用を制御し、有害で非生産的な Web コンテンツへのアクセスをブロックすることで可能になります。

**ファームウェア更新とハードウェア交換**に対応する 24x7 サポートでは、重要なファームウェア更新やアップグレード、業界トップクラスのテクニカルサポート、タイムリーなハードウェア交換、セルフヘルプの電子ツールの利用などにより、お客様のビジネスと SonicWall への投資を保護します。

### AGSS サービスの概要

マルチエンジンサンドボックス、ゲートウェイアンチウイルス / アンチスパイウェア、侵入防御、アプリケーションインテリジェンスおよび制御サービス

- リアルタイムのゲートウェイアンチウイルスエンジンにより、ウイルス、ワーム、トロイの木馬などのインターネットの脅威をリアルタイムでスキャンします。
- 動的なスパイウェア対策により、悪意のあるスパイウェアのインストールをブロックし、既存スパイウェアの通信を遮断します。
- 強力な侵入防御により、ワーム、トロイの木馬、その他の悪意のあるコードなど、ネットワーク関連のさまざまな脅威を防ぎます。
- アプリケーションインテリジェンスおよび制御により、アプリケーションの分類とポリシーの適用が可能になります。
- 動的に更新されるシグネチャデータベースにより、進化し続ける脅威に対応します。
- RTDMI を備えたマルチエンジンサンドボックスにより、ゼロデイ攻撃やランサムウェアなどの未知の脅威を防ぎます。

## Capture Advanced Threat Protection (Capture ATP)

- ネットワークに侵入する前にゼロデイ攻撃をブロックします。
- 修復シグネチャが、他のネットワークセキュリティアプライアンスへ迅速に配布されます。
- 脅威状況の変化に対応する高度な保護対策を確立します。
- さまざまなファイルタイプを分析します。

## コンテンツフィルタリングサービス (CFS)

- 包括的なコンテンツフィルタリングにより、不適切で非生産的かつ違法の疑いがある Web コンテンツへの内部アクセスをきめ細かく制御できます。
- Web サイトの評価を SonicWall ファイアウォールにローカルにキャッシュすることで、アクセス頻度の高いサイトの応答時間をほぼゼロにします。
- 動的に更新される評価アーキテクチャにより、要求されたすべての Web サイトを、数百万にのぼる URL、IP アドレス、ドメインを収録したクラウドのデータベースと相互参照し、各サイトの評価をローカルのポリシー設定と比較します。

## コンテンツフィルタリングクライアント

- Real-Time Deep Memory Inspection (RTDMI) を使用してマルウェアを迅速かつ正確に阻止します。
- SonicWall コンテンツフィルタリングクライアントにより、ファイアウォールの境界外にあるエンドポイントデバイスにインターネット使用ポリシーを適用してセキュリティと生産性を高めます。Windows、Mac OS、Chrome のエンドポイントに対応した個別のサブスクリプションサービスとして利用できます。

## 24x7 サポート

- ソフトウェアおよびファームウェアの更新とアップグレードにより、ネットワークセキュリティを維持し、ソリューションを常に最新の状態に保ちます。
- チャット、電話、電子メール、Web による 24 時間体制のサポートを利用でき、基本的な構成やトラブルシューティングについて相談できます。
- 障害の発生時には、Advance Exchange (良品先出しサービス) のハードウェア交換を利用できます。
- SonicWall のサービス広報の年間サブスクリプションを利用できるほか、電子サポートツールや適切に管理されたディスカッショングループにもアクセスできます。

SonicWall Advanced Gateway Security Suite の詳細については、[www.sonicwall.com](http://www.sonicwall.com) をご覧ください。

## 当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。