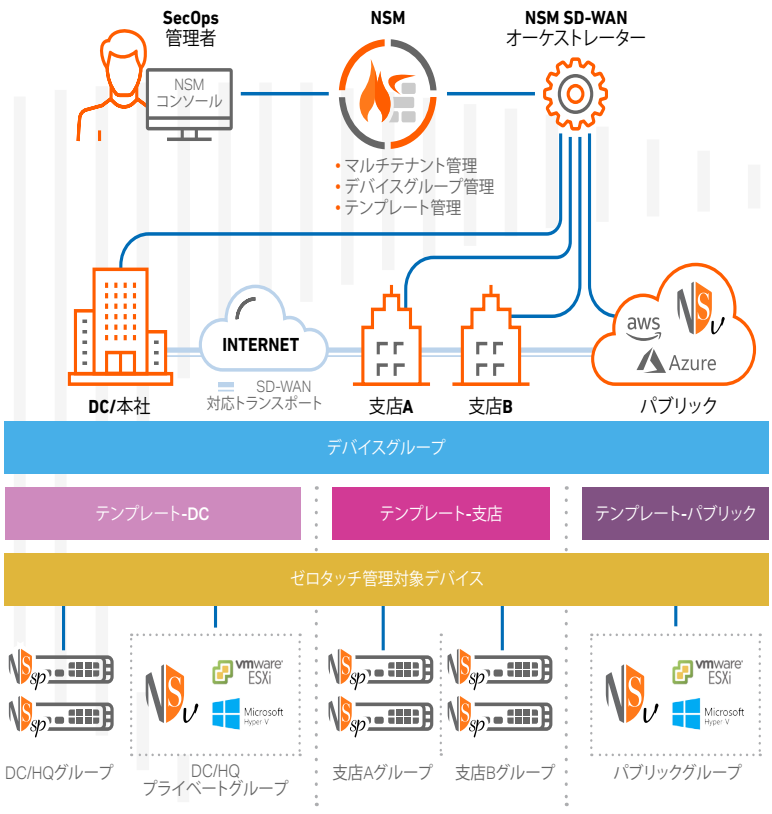
SONICWALL

# Network Security Manager

## あらゆる規模の環境に適した統合ファイアウォール管理システム

中小企業や分散型企業、複数の企業、閉鎖ネットワークなど保護対象に関係なく、ネットワークセキュリティは、運用上の障害や目に見えないリスク、規制上の要求に直面する可能性があります。これまでの効率的なファイアウォール管理の実践は、信頼できるシステムと運用管理手段に依存していました。ですがSecurity Operation Centers（SOC）が適切に運用されていても、頻繁なエラーや構成エラー、そしておそらくこうした規制への違反が課題であることに変わりはありません。




## ハイライト

### ビジネス

- セキュリティ管理にかかるオーバーヘッドを軽減
- 脅威環境とセキュリティ対策に関する知見
- IT組織の効率化と管理者の疲労の軽減を同時に実現
- ビジネスの中断による損失やセキュリティインシデントを回避

### 運用

- ファイアウォール管理サイロを排除
- リモートで簡単にいつくものファイアウォールを導入可能
- システムの重大な問題に対して迅速に対応し、最適なネットワークパフォーマンスを確保
- すべての管理対象デバイスで一貫性のある構成とポリシーを確立
- SD-WANネットワークの迅速な展開を促進

### セキュリティ

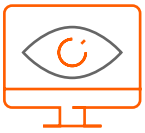
- すべての環境で一貫したセキュリティポリシーを監査、コミット、実施
- すべてのサイトで一貫性のあるSD-WAN構成を確立
- 脅威を発見し、問題やリスクに迅速に対処
- ポリシーに基づくアクションの結果をより明確に監視および追跡
- インサイダー脅威など、権限のないユーザーの認証を防止

集中管理。強化されたセキュリティ。

www.sonicwall.com/nsm

データシート

マルチテナント集中管理型ファイアウォールマネージャーであるSonicWall Network Security Manager（NSM）は、監査可能なワークフローを遵守することにより、すべてのファイアウォール操作をエラー無しに一元的に管理できます。レポート作成と分析[1、2]は、単一画面表示による可視性を提供し、すべてのファイアウォールログを統合して相互に関連付けることにより、脅威の監視と発見を可能にします。また、NSMはファイアウォール間で一貫したポリシーの適用が可能であり、すべての構成変更の詳細な監査証跡ときめ細かいレポートを提供するため、コンプライアンスの維持にも役立ちます。このソリューションは、複数のテナントや多数の場所に数百台のファイアウォールデバイスが展開されているネットワークを管理するようなあらゆる規模の組織に拡張できます。NSMは、より少ない労力と時間ですべてを実現します。



## 容易な管理：ファイアウォール操作の一元化

NSMは、統合されたファイアウォール管理システムに必要なものをすべて提供します。テナントレベルの可視性、グループベースのデバイス制御、無制限の拡張性により、SonicWallのネットワークセキュリティ操作の一元的な管理とプロビジョニングを実現します。これには、すべてのファイアウォールデバイスやデバイスグループ、テナントの展開と管理、柔軟なローカル制御による環境全体で、DNSフィルタリングやコンテンツフィルタリングなどの一貫したセキュリティポリシーの同期と実施、単一の動的ダッシュボードからの包括的な監視と詳細なレポート・分析機能が含まれます。また、NSMではAruba ClearPassとの統合によるネットワークアクセス制御も可能です。さらに、NSMなら、ブラウザ対応デバイスを使ってどこからでもアクセスできる単一のコンソールにより、すべての操作を管理することが可能です。

### マルチテナント管理

ファイアウォール環境を拡張する場合、その環境に応じて拡張できるファイアウォール管理システムが必要になります。NSMは、すべての管理対象テナントにおいて、完全なマルチテナント管理と独立したポリシー管理の分離を実現します。この分離には、各テナントにファイアウォール操作を指示するNSMの管理機能が含まれます。割り当てられたテナントアカウントの境界内でデバイスグループ管理やポリシーの調整、その他すべての管理タスクを実行するために、すべてのテナントに独自のユーザー、グループ、役割を設定できます。

### デバイスグループ管理

デバイスグループでは、ファイアウォールデバイスをグループまたは階層グループとして作成および管理し、ファイアウォールのグループに構成テンプレートをコミットし展開する効果的な方法を提供します。これにより、選択したファイアウォールグループ全体でポリシーやオブジェクト、要件を一貫性のある信頼性の高い方法で同期および実施できます。テンプレートにあるすべての承認済みポリシーへの変更は、そのテンプレートにリンクされているすべてのデバイスグループに自動的に適用されます。デバイスのグループ化は、管理や識別、関連付けを容易にするために、ネットワークタイプやロケーション、事業部、組織構造、属性の組み合わせといったあらゆる特性に基づいて細かく定義できます。

### テンプレートの管理、コミット、展開

NSMの簡略化されたワークフローにより、多くのロケーションで1台から数百台のファイアウォールデバイスを管理する構成テンプレートを容易かつ迅速に設計、検証、監査、承認、およびコミットできます。さまざまなファイアウォールポリシーや設定、関連オブジェクトを含むテンプレートは、デバイスから独立して定義されます。これらのテンプレートは、同様の構成を必要とするデバイスまたはデバイスグループに一元的かつ自動的にプッシュするためにNSMが使用します。

テンプレートとテンプレート変数を組み合わせることで、数百台のリモートファイアウォールを一元的に展開してプロビジョニングし、インターフェイスIP、DNS構成、ファイアウォールホスト名などのような、デバイスごとに固有の値を維持しながら、一貫性のある構成を確立できます。分散型企業の場合は、単一のテンプレートを使用して新しい支店やリモートサイトを簡単にオンボーディングして保護できるため、すべての場所でデバイスごとに個別に手動セットアップを行う必要がなくなります。

## SD-WANのオーケストレーションと監視

NSMは、直感的なセルフガイド型ワークフローにより、企業全体のSD-WANネットワークの展開を簡便化します。NSMは、支店や小売店など、数百か所のサイト全体およびサイト間で、アプリケーションベースのトラフィックやその他のトラフィックステアリング構成を一元的に確立および適用します。また、NSMでは、一貫した構成を確保し、最適なアプリケーションパフォーマンスを促進し、ネットワークインフラストラクチャ担当チームが問題のトラブルシューティングを迅速に行って解決できるように、SD-WAN環境全体の健全性とパフォーマンスを監視します。

## VPNのオーケストレーションと監視

NSMは、簡単なウィザードベースのステップバイステップのセットアッププロセスによってVPNの設定とポリシーを簡素化し、システム管理者が繰り返し使用できるセルフガイド型ワークフローを使ってサイト間の接続と通信を迅速にエラーなしで確立できるようにします。さらに、VPNの監視ではVPNの状態をアクティブに把握でき、VPN環境全体のアクティビティ、健全性、パフォーマンスを完全に可視化します。ネットワーク管理者は、この情報を活用して接続の状況、転送されたデータ、これらのVPNトンネルで使用された帯域幅を監視できます。また、アラートによって管理者はVPN接続の完全性をプロアクティブに維持し、サイト間の継続的な接続を確保できます。

### 効率性の向上：スマートに仕事をこなし、容易かつ迅速にセキュリティアクションを実行

NSMは、スマートに仕事をこなし、容易かつ迅速にセキュリティアクションを実行できる生産性管理ツールです。ビジネスプロセスを簡略化し、場合によっては、ワークフローを自動化してより優れたセキュリティ関連の調整を実現するという原則に基づきNSMは設計されています。また、セキュリティ運用と管理作業の実行における複雑さ・時間・オーバーヘッドの抑制も支援します。

## 手間いらずのゼロタッチ展開

NSMに統合されるゼロタッチ展開サービスは、遠隔拠点や支部・支店へのSonicWallファイアウォールやスイッチ、アクセスポイントの展開および運用を手間をかけずに実現します。プロセス全体に必要なユーザー介入は最小限で、完全に自動化されています。ゼロタッチ対応デバイスは、直接インストール先のサイトに出荷されます。登録して有線ネットワークにつなげば、接続されたすべてのデバイスは、即座に安全かつシームレスに操作できます。NSMで通信リンクが確立されると、あらかじめプロビジョニングされたデバイステンプレートが自動的にすべての接続されたデバイスにプッシュされます。これによって従来の現場での導入プロセスにおける時間やコスト、複雑さが排除されます。

## エラーのない変更管理

NSMは、ファイアウォールポリシーの変更管理およびSOCの監査要件に適う強力な自動化ワークフローへの即時アクセスを提供します。すなわち、一連の厳密なプロセスを適用することで、エラーフリーのポリシー管理を実現します。その対象となるのは、展開前の構成の比較、検証、承認です。承認グループには、さまざまな部門のチームが定める内部監査手順に準拠できる柔軟性があります。NSMは、強制的な承認ワークフロープロセスにより、運用効率の改善、リスク軽減、設定ミスやヒューマンエラーの排除を実現します。

## RESTful APIによる管理の自動化

NSM RESTful APIは、熟練したセキュリティ担当者がNSM独自の機能を管理するための標準的なアプローチを提供します。NSMとサードパーティの管理コンソール間の相互運用を容易にし、社内セキュリティチームの効率を高めることができます。APIサービスでは、管理対象デバイスのファイアウォール操作を自動化できます。これには、デバイスグループやテナントの管理、監査構成、システムの健全性の確認操作などの一般的な日常業務が含まれます。

### 認識の向上：隠れたリスクを調査するアクティブな監視、レポート作成、分析[1,2]

NSMのインタラクティブなダッシュボードには、リアルタイムのデータの監視、レポート作成、データ分析の機能があります。問題のトラブルシューティングやリスクの調査、高度な適応型セキュリティ対策の実施に向けたスマートなセキュリティポリシーのアクションの実行をサポートします。

管理者は、リアルタイムのアラートによって正確かつ迅速に行動して組織を最適に運営し続けることができます。その結果、組織がビジネスの中断による損失やセキュリティインシデントを回避することを支援できます。

## 優れた可視性

NSMは、Analytics[1,2]との連携により、テナント、グループ、デバイスの各レベルにおいて、SonicWallのセキュリティエコシステム全体を最長7日間、継続的に可視化します。また、ファイアウォールエコシステムを通過するすべてのネットワークトラフィックとデータ通信について、静的なほぼリアルタイムの分析を提供します。ログデータはすべて自動的に記録、集計、コンテキスト化され、有意義で実践的、かつ理解しやすい方法で表示されます。その後、データドリブンな洞察と状況認識に基づき、適切な防御・是正措置を発見、解釈、優先順位付けし、実施することができます。スケジュールレポートを使用すれば、トラフィックデータを任意に組み合わせてレポートをカスタマイズすることも可能です。履歴データによる分析や異常検出、セキュリティギャップの発見などを目的に、デバイス、デバイスグループ、またはテナントレベルで記録されたログを最長365日間表示するため、効果的なネットワークとセキュリティ操作を追跡、測定、実行できます。

### リスクの把握

ドリルダウン機能とピボット機能の追加により、データをより詳細に調査して関連付け、高度な正確性と確信をもって隠れた脅威や問題を徹底的に検証し、発見できるようになりました。履歴レポートと、ユーザーベースおよびアプリケーションベースの分析、エンドポイントの可視性を組み合わせることで、出入りのトラフィックやアプリケーションの使用状況、ユーザーおよびデバイスのアクセス、脅威アクションなどに関連する多様なパターンや傾向を徹底的に分析できます。これにより、セキュリティリスクの発見だけでなく、修復を一元化するための状況認識や重要なインサイトや知識を取得しながら、環境全体で一貫したセキュリティの実施を促進・推進する結果を監視および追跡できます。

### 労働生産性の最適化

User Analytics[1,2]は、従業員のウェブアプリケーションとインターネットの使用状況に関する幅広く透明性の高いビューを提供します。ドリルダウン機能によって、アナリストは、関心のあるデータポイントをユーザーレベルで簡単に素早くピボット分析と調査を行い、検出プロセスで明らかになるように、リスクの高いユーザーやアプリケーションに対して確証のあるポリシーによって制御された対策を確立できます。さらに、生産性レポート[1,2]は、指定した期間における従業員のインターネットの使用状況や行動に関する洞察を提供します。強力なスナップショットと、ユーザーのウェブアクティビティを生産的、非生産的、許容可能、許容不可、カスタム定義グループなどの生産性グループに分類したドリルダウンレポートを生成し、組織でインターネットの使用状況をより詳細に把握して制御することを支援します。

### 柔軟性の高い展開

お客様は、運用、規制、予算における各要件に最も適したさまざまな方法でNSMを展開できます。

メンテナンスを不要にするため、NSMはSonicWallがホストするSaaS製品としてインターネット経由でアクセスできます。NSM SaaSを使用すると、運用コストを削減して、オンデマンドで拡張できます。ハードウェアやソフトウェアの展開、メンテナンススケジュール、ソフトウェアのカスタマイズ、構成やアップグレード、ダウンタイム、減価償却や廃棄のコストなどが発生しません。これらの費用はすべて不要になり、予測可能な低額の年間サブスクリプションのコストのみに置き換えられます。

**全体的なシステムの制御とコンプライアンスのためには、NSMをMicrosoft Azureパブリッククラウドで展開するか、VMWare、Microsoft Hyper-V、KVM上のプライベートクラウドで仮想アプライアンスとして展開できます。このようにすることで、システムの拡張性と俊敏性、システムプロビジョニングの素早さ、管理の容易性、コストの削減などの、仮想化による運用上および経済上の利益をすべて得ることができます。**

### セキュリティ機能

政府、公的機関、医療機関、製薬会社、その他の大規模な組織では、多くの場合、ミッションクリティカルなアプリケーションや、機密文書システム、SCADA、研究施設などのきわめて機密性の高い情報システムのプライバシーと分離を維持するために、閉鎖ネットワークを展開します。NSMでは、SonicWallのラインセスマネージャーやMySonicWallに問い合わせなくても管理対象のNSMシステムやファイアウォールのオンボーディング、ライセンス管理、パッチ適用、およびアップグレードをオフラインで行える方法を管理者に提供することで、閉鎖ネットワーク環境をサポートしています。

セキュリティ機能を追加する場合は、NSMの管理インターフェイスへの不正アクセスを防止するための複数のアカウントアクセス制御対策をNSMで適用します。NSMは、ユーザーの役割に応じて特定の管理権限の制御を付与し、指定されたログイン試行失敗の回数に基づいてアカウントのロックアウトをトリガーします。また、ユーザーのアクセスは、許可された送信元IPアドレスの指定済みリストからログインして2要素認証（2FA）[3]によって保護されている場合にのみ許可されます。

## 機能の概要

### 管理

- Aruba ClearPassによるネットワークアクセス制御(NAC)
- テナントおよびデバイスグループレベルの管理
- 構成テンプレート
- デバイスのグループ化
- デバイス構成をテンプレートに変換
- コミットと展開のウィザード
- 構成の監査
- Config – Diff
- オフライン管理とスケジュール
- セキュリティファイアウォールポリシーの管理
- セキュリティVPNポリシーの管理
- SD-WANの管理
- セキュリティサービスの同期
- 高可用性
- 構成バックアップ
- RESTful API
- マルチデバイスのファームウェアアップグレード
- 役割ベースの管理
- アクセスポイントとスイッチの管理
- インテリジェントプラットフォーム監視(IPM)[3]
- マルチデバイスの証明書の管理

### 監視[1、2]

- デバイスの健全性とステータス
- ライセンスとサポートのステータス
- ネットワーク／脅威サマリー
- アラートおよび通知センター
- イベントログ
- トポロジ表示

### 分析[1、2]

- ユーザーベースのアクティビティ
- アプリケーションの使用状況
- Capture Clientによる製品間の可視性
- リアルタイムの動的な可視化
- ドリルダウン機能とピボット機能

### レポート作成[1、2]

- スケジュールされたPDFレポート – テナント／グループ／デバイスレベル
- カスタマイズ可能なレポート
- 集中型ロギング
- マルチ脅威レポート
- ユーザー中心のレポート
- アプリケーションの使用状況レポート
- 帯域幅とサービスのレポート
- ユーザーごとの帯域幅レポート
- 生産性レポート

### セキュリティ

- 閉鎖ネットワークのサポート
- アカウントのロックアウト
- アカウントのアクセス制御
- 2要素認証のサポート[3]
- 認証アプリによる2要素認証のサポート

## ライセンスおよびパッケージ

**管理**

| 特徴 | NSM SaaS Essential | NSM SaaS Advanced | NSM On-Premises[2] |
|---|---|---|---|
| テナント | あり | あり | あり |
| デバイスインベントリ | あり | あり | あり |
| グループレベルでのポリシーのプッシュ | あり | あり | あり |
| デバイスグループ | あり | あり | あり |
| テンプレート | あり | あり | あり |
| コミットと展開<br>(ワークフローの自動化) | あり | あり | あり |
| 構成の監査 | あり | あり | あり |
| Config Diff | あり | あり | あり |
| ワークフローの自動化 | あり | あり | あり |
| API | あり | あり | あり |
| ゼロタッチ導入 | あり | あり | あり |
| SD-WANのオーケストレーションと監視 | あり | あり | あり |
| VPNのオーケストレーションと監視 | あり | あり | あり |
| タスクのスケジューリング | あり | あり | あり |
| バックアップ／リストア | あり | あり | あり |
| ファームウェアアップグレード | あり | あり | あり |
| アクセスポイントとスイッチの管理 | あり | あり | あり |
| 高度なDNSフィルタリング | あり | あり | あり |
| Aruba ClearPassによるネットワークアクセス制御 | あり | あり | あり |
| レピュテーションベースのコンテンツフィルタリング | あり | あり | あり |

## ライセンスおよびパッケージ（続き）

| レポート作成 | | | |
|---|---|---|---|
| 特徴 | NSM SaaS Essential | NSM SaaS Advanced | NSM On-Premises[2] |
| グループ／テナントレベルのダッシュボード | あり | あり | なし |
| Capture ATP（デバイスレベル） | あり | あり | あり |
| Capture Threat Assessment（デバイスレベル） | あり | あり | あり |
| 生産性レポート[5] | なし | あり | なし |
| VPNレポート | なし | あり | なし |
| カスタムレポート | あり | あり | なし |
| スケジュールレポート（フロー、CTA、管理） | あり（フローレポートを除く） | あり | あり |
| データのレポート日数 | 7日 | 365日 | 365日 |

| 分析 | | | |
|---|---|---|---|
| 特徴 | NSM SaaS Essential | NSM SaaS Advanced | NSM On-Premises[2] |
| ユーザーベースの分析 | なし | あり | あり |
| アプリケーション分析 | なし | あり | あり |
| ドリルダウンとピボットを使用したネットワークのフォレンジックと脅威ハンティング | なし | あり | あり |
| Cloud App Security – シャドーITの特定 | あり | あり | なし |

## システム要件

### インターネットブラウザ

- Microsoft® Internet Explorer 11.0以降、最新バージョンのMicrosoft Edge、Mozilla Firefox、Google Chrome、Safari

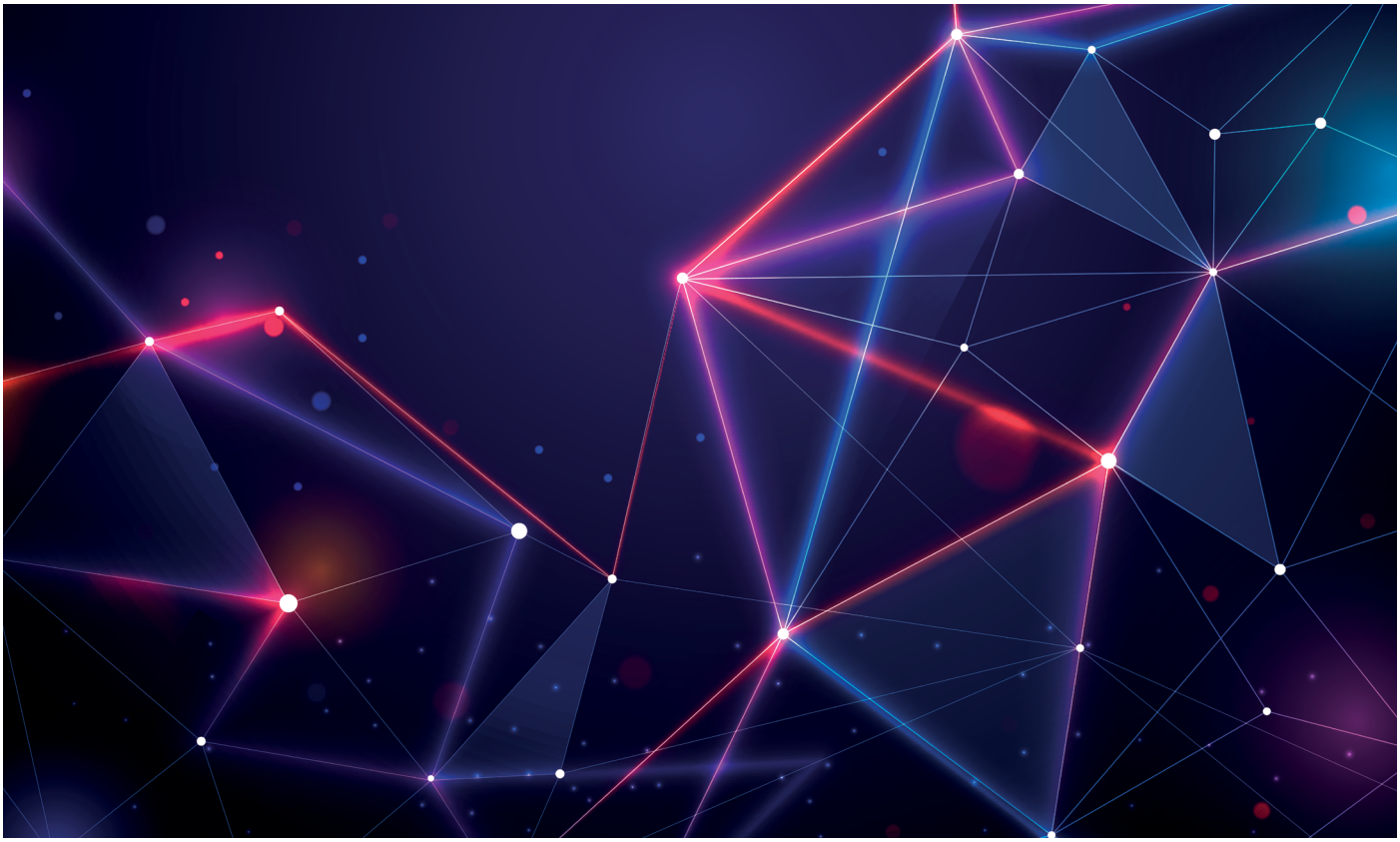
### NSM On-Premisesのシステム要件

- ハイパーバイザー：ESXi 7.0、6.7、Hyper-V 2016、2019、KVM
- パブリッククラウド：Azure
- 必要最低コンピューティングリソース：4 vCPU、24 GBのメモリ（1～500台のファイアウォールを管理する場合）、250GBのストレージ

### 管理対象デバイス

- NS*sp* 15700、NS*sp* 13700、NS*sp* 12000シリーズ[4]、SuperMassive 9000シリーズ[4]、NSAシリーズ、NS*a*シリーズ、TZシリーズ、SOHO-W、SOHO 250、SOHO 250W
- 第5世代アプライアンスおよびファームウェア（SonicOS 5.9を実行する非ワイヤレスSOHOデバイスなど）はサポートされていません。
- SonicWall Network Security Virtual Appliance：NS*v*シリーズ
- SonicWall SonicWave[6]、SonicPoint
- SonicWaveのサポートにはWi-Fi 6対応アクセスポイントが含まれています
- SonicWallスイッチ

[1] NSM SaaSにはレポート作成機能と分析機能が含まれています。
[2] NSM On-Premisesでレポート作成機能と分析機能を使用するには、SonicWall Analytics On-Premisesのインストールとライセンスが別途必要です。
[3] NSM On-Premisesのみで利用可能です。
[4] 365日のレポート作成および30日の分析機能はサポートされていません。
[5] 第6/6.5世代ファイアウォールではAGSS/CGSSのライセンスが有効化されている必要があります。第7世代ファイアウォールではEssential Protectionのライセンスが有効化されている必要があります。
[6] SonicWaveのサポートにはWi-Fi 6対応アクセスポイントが含まれています。



# ファイアウォール、接続されているスイッチ、アクセスポイントのすべての展開と管理を1つの使いやすいインターフェイスで

www.sonicwall.com/nsm

## SonicWallについて

SonicWallは、安定した、拡張可能で、シームレスなサイバーセキュリティを提供することにより、誰もがリモート/モバイルで危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、中小企業をサポートします。詳しくは www.sonicwall.comをご覧ください。

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細は当社ウェブサイトをご覧ください。
www.sonicwall.com

SONICWALL