SONICWALL®

2026 年 4 月 1 日

報道機関各位

ソニックウォール・ジャパン株式会社

SonicWall、年次調査を中小企業の保護の成果を軸に再構築
― 2026 年版サイバー保護レポートで「七つの大罪」を明らかに

新しいレポートでは、中小企業は精度をますます高めている AI 対応型の攻撃者からの脅威に直面しており、深刻度の高い実行可能な攻撃が 20%以上増加していることが判明

カリフォルニア州ミルピタス ―2026 年 3 月 31 日 ― SonicWall は本日、2026 年版 SonicWall サイバー保護レポートを発表しました。本レポートは、従来の脅威レポートから、ビジネスリーダーにとって非常に重要な事項である保護の成果を重視する内容へと大きく転換するものです。レポートの中心となっているのは、真剣な対応が求められる調査結果です。ほとんどの中小企業の失敗の理由は、巧妙な攻撃ではありません。失敗の理由は、SonicWall が「サイバーセキュリティの七つの大罪」と命名した、7 つの予測可能で予防できるギャップです。

2026 年版レポートは、SonicWall の 100 万を超えるセキュリティセンサーのグローバルネットワークからのデータを引き続き活用して、さらに精度を高め、執拗さを増す脅威の状況を明らかにしています。いくつかの重要な統計結果として、次のようなものがあります。

- 深刻度が高および中レベルの攻撃は 20.8%増加し、131 億 5,000 万件となっています。攻撃者は、攻撃の頻度を高めているのではなく、よりスマートに攻撃しています。
- 今日では、自動化されたボットが 1 秒あたり 36,000 を超える脆弱性スキャンを生成しており、すべてのインターネットトラフィックの半分以上を占めています。悪質なボットトラフィックだけで、全世界のインターネットトラフィックの 37%まで急増しています。
- IoT 攻撃は 11%増えて 6 億 990 万件に達しました。Log4j だけでも、公表されてから 4 年後である 2025 年に 8 億 2,490 万件の IPS（侵入防止システム）による検知が発生しています。
- アイデンティティ、クラウド、認証情報の侵害が、アクション可能なセキュリティアラートの 85%を占めています。攻撃者が選んでいる武器は、ゼロデイではなく、盗み出されたパスワードです。
- 中小企業はランサムウェアに対する備えが不十分です。2025 年の中小企業における侵害の 88%はランサムウェア関連であり、これは大企業で見られる確率の 2 倍以上です。

SonicWall の SVP 兼マネージドセキュリティサービス担当 GM であるマイケル・クリーンは次のように述べています。「SonicWall のデータは、攻撃が高速化していること、そして一部のケースでは攻撃がさらに少しずつ巧妙化していることを明らかにしています。しかし、私たちが目撃して調査している攻撃の大半は、見過ごされ続けている基本的なも

のです。危険なのは、AIが機能していないことではありません。私たちがすべきであるとすでにわかっていることを、AIを言い訳にしてやらないことです。」

2026 年版 SonicWall サイバー保護レポートは、当社の歴史において初めて、脅威に関する統計だけでなく、保護の成果に主眼を置きました。今年の調査において、SonicWall は「七つの大罪」と名付けた 7 つの繰り返し起きているパターンを特定し、中小企業の侵害の調査、セキュリティ評価、インシデントレビューにわたってレジリエンスとエクスポージャーの違いについて一貫した定義を明確にしています。

サイバーセキュリティの七つの大罪

2026 年版保護レポートは、例外的または新たな攻撃方法を侵害リスクの原因とするのではなく、調査において繰り返し見られ、その多くが予防可能である 7 つの運用上の失敗を特定しています。七つの大罪は以下の通りです。

1. **基本を無視している** — 脆弱な認証、パッチ未適用のシステム、過剰な管理者権限は、依然として主な攻撃対象領域となっています。
2. **過信** — 自社は小規模であるから標的にはならないと信じ込むこと、制御の効果を過大評価すること、テストを行わずにレジリエンスを想定することが危険な盲点を生み出します。
3. **非常に無防備なアクセス** — 過度に寛容なルール、フラットなネットワーク、認証後の暗黙的な信頼は、いったん侵入できれば妨げられることのない経路を攻撃者に提供します。
4. **受動的なセキュリティ体制** — 24 時間体制の監視やプロアクティブな脅威ハンティングが行われていない場合は、攻撃者がスケジュールを設定できます。平均的な侵害は 181 日間検出されません。
5. **コストに基づいたセキュリティに関する意思決定** — 短期的な予算のプレッシャーに基づいて投資を先延ばしにすることは、後からコストを発生させます。しかも投資額よりも高くつきます。ダウンタイムと復旧も含めると、中小企業における 1 件の侵害は 491 万ドルを超える可能性があります。
6. **レガシーアクセスモデルへの依存** — いったん認証すると広範囲のネットワークアクセスが許可される VPN は、依然として企業のセキュリティで最も悪用される侵入ポイントの 1 つとなっています。分析対象期間中に、VPN の CVE は 82.5%増えました。
7. **実行することよりもトレンドを追いかける** — 最新のツールを完全な形で導入せずに購入し、プロセスのギャップをテクノロジーが補ってくれると期待することは、それ自体が一種の脆弱性です。ツールは成果を生み出しません。実行することが成果を生み出します。

クリーンは次のように続けています。「大きな被害に遭う組織は、巧妙な攻撃が原因で失敗しているのではなく、予測可能で予防できるギャップが原因で失敗しています。中小企業は米国の経済を支える基盤であり、米国の全企業の 99%、民間部門の雇用の半分近くを占めています。このような企業を守ることが、コミュニティ全体を守ります。そのため、本レポートは単なる脅威の統計ではなく、保護の成果に主眼を置いたものになっています。」

パートナーファーストという SonicWall の使命に沿って、2026 年版サイバー保護レポートは、MSP や MSSP に中小企業の意思決定者と戦略的な対話を行うために必要なデータと手段を提供し、技術的な脅威インテリジェンスをリーダーにとって対応可能なビジネスリスクに変換できるようにすることを目的としています。

SONICWALL®

SonicWall 2026 年版サイバー保護レポートは 1 つのことを明確にしています。保護されていることとリスクにさらされていることの違いがテクノロジーであるケースはめったにありません。違いは、実行することです。本レポートは、中小企業および中小企業を守る MSP や MSSP 向けに、データ、明確さ、次に行うべきことのロードマップによってそのギャップを埋められるようにすることを目的としています。
SonicWall の詳細および 2026 年版 SonicWall サイバー保護レポートの全文は、
https://www.sonicwall.com/ja-jp/resources/white-papers/sonicwall-2026-cyber-protect-report
をご覧ください。

※本リリースは米国 SonicWall によるプレスリリースの翻訳版です。詳細につきましては、SonicWall Japan までお問い合わせください。

【 SonicWall について 】

30 年以上にわたり、SonicWall はパートナーファーストのモデルを推進しており、目的に合わせて構築したテクノロジー、クラウド提供型のセキュリティサービス、リアルタイムの脅威インテリジェンスを組み合わせて、企業が侵害を防ぎ、リスクを軽減し、進化し続ける最新の脅威に直面しながら事業を継続できるよう支援しています。当社は、他社が機能や特徴を提供する一方で、お客様に最善のセキュリティの成果を提供することに取り組んでいます。　統合されたサイバーセキュリティポートフォリオと、17,000 社を超えるパートナーで構成されるグローバルコミュニティを通じて、SonicWall はマネージドサービスプロバイダーがネットワーク、クラウド環境、エンドポイント、アプリケーションを積極的に管理し、継続的に最適化し、目に見える形で保護することを可能にします。当社は侵害防止、コンプライアンス達成、コスト効率、ヒューマンエラーの削減など、ビジネスリーダーにとって重要な成果に主眼を置いてサイバーセキュリティのあり方を再定義しています。その理由は、保護とは、製品で何ができるのかではなく、製品が実際に何を提供できるのかに関するものであるからです。

詳細は、以下よりご確認頂けます。
コーポレートサイト：　https://www.sonicwall.com/ja-jp
SonicWall Japan 情報サイト：　https://sonicwall-pub.snwl.jp

X(Twitter)、LinkedIn、Facebook、Instagram で当社をフォローしてください。
X:　https://x.com/SonicWall
LinkedIn:　https://www.linkedin.com/company/sonicwall/
Facebook:　https://www.facebook.com/SonicWall/
Instagram:　https://www.instagram.com/sonicwall_inc/

【報道関係者様からのお問い合わせ先】
ソニックウォール・ジャパン株式会社 PR 担当
Japan_SNWL@sonicwall.com