Press Release
2026 年 3 月 13 日（金）
ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガード、最新脅威レポートを発表：
新規かつユニークなマルウェアが 1500%以上増加し、セキュリティの複雑化が進行

事後対応型のセキュリティから、事前対応型の脅威インテリジェンスと統合プロテクションの活用が必要

2026 年 3 月 13 日（金） - 企業向け統合型サイバーセキュリティソリューション（ネットワークセキュリティ／セキュア Wi-Fi／多要素認証／エンドポイントセキュリティ）のグローバルリーダーである WatchGuard（R）Technologies の日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、代表執行役員社長 谷口 忠彦、以下ウォッチガード）は、**「インターネットセキュリティレポート」**の最新版を発表しました。本レポートでは、回避型および暗号化された脅威が急激に増加していることを明らかにしています。これにより MSP には、より積極的かつ統合的なセキュリティアプローチが求められています。

半年ごとに発行されているレポートでは、ウォッチガードの匿名化されたネットワークセキュリティ、エンドポイント、DNS フィルタリング製品から集約された脅威インテリジェンスを活用しており、攻撃者がマルウェアの量を増やし、巧妙化レベルも向上させていることを示しています。このことは組織のセキュリティ対策において、依然として一般的な反応型のシグネチャベースの防御が採用されており、その限界が露呈したままとなっています。

2025 年には新規マルウェアが四半期ごとに増加し、第 3 四半期から第 4 四半期だけで 1,548%の急増を記録しました。同時に、検知されたマルウェアの 23%が従来のシグネチャベース検知を回避しており、事実上ゼロデイ脅威に該当し、これにより、行動ベースの AI を活用した保護の必要性がさらに強まっています。

主な調査結果により、従来のセキュリティモデルの課題が浮き彫りに

- **回避型マルウェアが急増中：**エンドポイント上で過去 15 倍以上の未確認マルウェアが確認され、脅威アクターは静的検知手法を回避する新種かつ難読化された手法を優先的に利用しています。
- **暗号化配信が標準化：**ブロックされたマルウェアの 96%が TLS 経由で配信され、HTTPS 検査を実施していない組織には重大な可視性のギャップが生じています。
- **エンドポイント攻撃手法が進化：**悪意のあるスクリプトは過去 1 年で減少傾向にありますが、代わりに Windows バイナリや LotL（環境寄生型）ツールが主要な感染経路となり、信頼の置けるプロセスを悪用して検知を回避しています。
- **依然として根強いネットワークの脅威：**2025 年下半期にはネットワークベースの攻撃手法は減少したものの、検知件数の大半は特に最近の Web アプリケーションにおける長年の脆弱性を標的としており、侵入防止システム（IPS）などネットワークの多層防御の必要性を改めて浮き彫りにしています。

洗練された攻撃者による配信手法と収益化

調査では、攻撃者がマルウェアの配信方法と収益化手法を向上させていることも明らかになりました。2025 年後半、ウォッチガードは悪意のある PowerShell スクリプトを用いて、リモートアクセストロイの木馬（RAT）など、サービスとしてのマルウェア（MaaS）ツールを展開しつつ、自動ファイル分析を意図的に回避するフィッシングキャンペーンを観察しました。

ランサムウェア活動は前年比 68.42%減少したものの、公開された身代金支払額は過去最高を記録し、攻撃件数は減少する一方、単発の高額の攻撃へ移行していることを示唆しています。攻撃者がアクセス権を獲得した後の収益化手段としては、暗号通貨マイニングが依然として摩擦の少ない手法として幅を利かせています。

MSP にとって意味するところ

ウォッチガードのチーフセキュリティオフィサーである Corey Nachreiner（コリー・ナクライナー）は次のように述べています。「今日の脅威情勢は、単体ソリューションや事後対応型のセキュリティモデルでは対応しきれないほど拡大しています。MSP にとって、ビジネスリスクは特に高く、顧客の侵害はサポートコストの増加、信頼性に対するダメージ、そして明らかな競争上の不利をもたらします。2026 年以降も成功を収める MSP とは、顧客の環境全体にわたり、積極的な脅威インテリジェンスと統合された保護体制を明確に実証できる企業だと言えます。」

この調査結果は、高度なエンドポイント保護／検知／レスポンス（EPDR）、AI を活用した脅威検知、そして継続的監視を組み合わせた最先端の防御戦略の必要性を裏付けています。攻撃がより持続的かつ複雑化する中、MSP は 24 時間 365 日のマネージド検知／レスポンスサービスを提供することで差別化を図りつつ、リスクを低減し、長期的な顧客価値を創出する立場を強化しています。

ウォッチガードの調査結果の詳細については、「半期ごとに発行されるインターネットセキュリティレポート」の完全版をダウンロードしてください。
https://www.watchguard.com/wgrd-resource-center/security-report-h2-2025

*本資料は、本社が発表したプレスリリースの翻訳版です。

【WatchGuard Technologies について】

WatchGuard（R）Technologies, Inc.は、統合型サイバーセキュリティにおけるグローバルリーダーです。ウォッチガードの Unified Security Platform（R）（統合型セキュリティプラットフォーム）は、マネージドサービスプロバイダー向けに独自に設計されており、世界トップクラスのセキュリティを提供することで、ビジネスのスケールとスピード、および運用効率の向上に貢献しています。17,000 社を超えるセキュリティのリセラーやサービスプロバイダと提携しており、25 万社以上の顧客を保護しています。ウォッチガードの実績豊富な製品とサービスは、ネットワークセキュリティとインテリジェンス、高度なエンドポイント保護、多要素認証、セキュア Wi-Fi で構成されています。これらの製品では、包括的なセキュリティ、ナレッジの共有、明快さと制御、運用の整合性、自動化という、セキュリティプラットフォームに不可欠な 5 つの要素を提供しています。同社はワシントン州シアトルに本社を置き、北米、欧州、アジア太平洋地域、ラテンアメリカにオフィスを構えています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多彩なパートナーを通じて、国内で拡大する多様なセキュリティニーズに応えるソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向は X（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。
X： https://twitter.com/WatchGuardJapan
Facebook： https://www.facebook.com/watchguard.jp

また、最新の脅威に関するリアルタイム情報やその対策法は SecplicityJP までアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
マーケティング担当
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp