

ウォッチガード、2025 年第 1 四半期最新インターネットセキュリティレポートを発表： 攻撃者が従来の防御策をかいくぐり、総ユニークマルウェア数が 171%増加

AI の急成長により、メール経由のマルウェア脅威および ユニークで回避型のエンドポイント脅威が増加し、ランサムウェアが減少

2025 年 8 月 1 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、四半期毎に発行している「インターネットセキュリティレポート」の最新版（2025 年第 1 四半期）を発表しました。本レポートでは、第 1 四半期にウォッチガードの脅威ラボの研究者たちによって観測された、マルウェア、ネットワークセキュリティおよびエンドポイントセキュリティの脅威に関する主な傾向の詳細を報告しています。

本レポートの主要な調査結果によると、ユニークマルウェアの総検知数が前四半期比で 171%増加し、脅威ラボが記録した過去最高水準に達しました。これに加え、「ゼロデイマルウェア」の著しい増加が確認され、シグネチャベースの検知を回避するように設計された回避型脅威の急増を暗示しています。つまり、脅威をパターンに基づいて検知する従来のセキュリティシステムを標的としていることを示しています。特に注目すべきは、IntelligentAV (IAV) が提供するプロアクティブな機械学習 (ML) による検知が 323%急増したことにより、高度なマルウェア検知において重要な役割を果たしていることが浮き彫りになりました。また、Gateway AntiVirus (GAV) の検知数は 30%増加し、トランスポートレイヤセキュリティ (TLS) マルウェアが 11 ポイント増加したことから、暗号化チャネルが主要な攻撃ベクトルであることを示唆しています。IAV による検知数の急増と TLS マルウェアの増加は、攻撃者が難読化と暗号化に依存しており、従来の防御策の限界を浮き彫りにしています。これらの結果は、大規模の高度で潜在的な脅威に対抗するため、可視性の向上と適応型セキュリティの強化が急務であることを強調しています。

また、脅威ラボは、エンドポイントにおける新たなマルウェア脅威が 712%増加したことを確認しました。過去 3 四半期にわたって新たなマルウェア脅威は一貫して減少傾向にあったため、この数値は深刻だと言えます。エンドポイントにおいて最も出現したマルウェア脅威は、システムへのログイン、パスワード管理、アクセストークンの作成などを行う資格情報窃取ツールである LSASS ダンプでした。攻撃者は LSASS を悪用し、ユーザーモードを回避して直接カーネルモードの命令を実行することで、システムコンポーネントにアクセスします。

ウォッチガードの CSO（チーフセキュリティオフィサー）、Corey Nachreiner（コリー・ナクライナー）は次のように述べています。「2025 年第 1 四半期のインターネットセキュリティレポートにおける最新の調査結果は、サイバーセキュリティ業界全体の傾向を裏付けており、AI 戦争が現実のものとなっています。攻撃者は、AI ツールによって強化されたソーシャルエンジニアリングやフィッシング手法にますます依存するようになっており、自動化されたパイプラインを活用して大規模な標的型キャンペーンを実行する能力を獲得しています。これにより、組織は AI の進化と巧妙化するサイバースリスクに対抗するため、堅牢で正確かつ強力なセキュリティ対策を導入する必要性がさらに高まっています。」

以下に、ウォッチガードの最新インターネットセキュリティレポート（2025 年第 1 四半期版）における主な調査結果を紹介します：

- ランサムウェアは前四半期比で 85%減少しましたが、最も多く検知されたマルウェア脅威の第 2 位はランサムウェアのペイロードである「Termite（ターmite）ランサムウェア」でした。これは、ファイルを暗号化するマルウェアであるクリプトランサムウェアの減少という業界の傾向を裏付けるものです。攻撃者は、データバックアップと復旧の改善が進んだため、暗号化ではなくデータ窃取へと手法をシフトしています。
- スクリプト（スクリプトプログラミング言語から派生した、または使用するファイル）は、この四半期で約半減し、過去最低水準となりました。過去において、脅威ラボはエンドポイントにおけるマルウェア検知の主要な攻撃ベクトルとしてスクリプトを観察してきました。その他の Windows などに対する環境寄生型攻撃（LoTL）は、前四半期比で 18%と最も高い増加率を示し、スクリプトが占めていた部分に取って代わりました。
- 暗号化された接続で検知された最も深刻なマルウェアは、Trojan.Agent.FZPI という新しい悪意のある HTML ファイルであり、正当なものを装ったファイルと暗号化された通信を組み合わせています。この脅威は、過去数年間にわたり脅威アクターが使用してきた複数の技術を組み合わせた、超高度なフィッシング添付ファイルです。組織は、この脅威を検知し、無効化するため、堅固な TLS 調査、行動分析、そしてエンドポイント保護を行う必要があります。
- 2025 年第 1 四半期において、最も広く拡散したマルウェアは、新たに特定された脅威である Application.Cashback.B.0835E4A4 であり、記録上最も広範に拡散したマルウェアファミリーの一つとして、チリで 76%、続いてアイルランドで 65%と高い影響を受けました。Application.Cashback の変種が広範に拡散していることは、これらの高度な脅威に対処するため、地域別の防御策の必要性を示しています。
- ネットワークシグネチャのユニーク数、またはネットワークで検知された既知の攻撃数は、攻撃者がより狭い範囲の 익스プロイトに焦点を当てたため、前四半期比で 16%減少しました。ネットワーク攻撃の動向は、新たな 익스プロイトが出現する一方で、攻撃者がパッチ未適用の既存の脆弱性を大規模に悪用し続ける傾向が継続していることを示しています。これにより、組織は両方の脅威に対処する必要性に迫られています。
- マルウェアの脅威は、Web ではなくメール経由で継続的に出現しており、脅威アクターが AI の進化により信憑性の高い標的型フィッシングメッセージを作成しやすくなったため、伝統的なフィッシング手法でユーザーを標的としていることが示唆されています。ただし、2025 年第 1 四半期には、AI と機械学習を活用したツールにより、ネットワークとエンドポイントの境界で検知される脅威の数が大幅に増加しています。

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）アプローチやウォッチガードの脅威ラボのこれまでの四半期ごとのリサーチアップデートと同様、この四半期レポートで分析されているデータは、ウォッチガードのリサーチ活動に賛同するウォッチガードのネットワークおよびエンドポイント製品を利用するお客様から、匿名により収集した脅威インテリジェンスに基づいています。

インターネットセキュリティレポートの最新版（2025 年第 1 四半期）の全文は以下よりダウンロードできます。

<https://www.watchguard.com/wgrd-resource-center/security-report-q1-2025>（英語版）

*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>

WatchGuard は、WatchGuard Technologies, Inc.の登録商標です。その他の商標は各社に帰属します。

【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>