Press Release
2025 年 12 月 5 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、2025 年第 2 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：サイバー犯罪者がステルス戦術を採用し、暗号化接続経由の回避型マルウェアが 40%急増

ゼロデイマルウェアと新たな USB 感染経路を用いてシグネチャを回避

2025 年 12 月 5 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 2 四半期）を発表しました。本レポートでは、第 2 四半期（4 月-6 月）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、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。

本レポートの主な調査結果によると、回避能力の高い高度なマルウェアが 40%（前四半期比）増加したことが明らかになりました。収集されたデータは、ほとんどのセキュアな Web トラフィックを支える暗号化プロトコルである TLS（トランスポートレイヤセキュリティ）を利用した暗号化チャネルを、攻撃者が好んで攻撃ベクトルとして使用していることを示しています。TLS はユーザー保護に不可欠ですが、攻撃者は悪意のあるペイロードを偽装するために悪用するケースが増えています。

第 2 四半期のマルウェア検知件数は全体で 15%増加し、その内訳は Gateway AntiVirus（GAV）が 85%増、IntelligentAV（IAV）が 10%増となり、これは巧妙な脅威の検知において IAV の役割が拡大していることを示しています。現在、マルウェアの 70%が暗号化された接続を介して配信されていることから、攻撃者が難読化やステルス手法への依存度を高めている実態が浮き彫りとなり、組織が暗号化トラフィックの可視性を向上させ、柔軟な保護戦略を採用する必要性が示唆されています。

脅威ラボではまた、ネットワーク攻撃も 8.3%増の小幅な上昇を観測しました。同時に攻撃の多様性は縮小し、検知された固有シグネチャは前四半期の 412 件から 380 件に減少しています。特に注目すべきは、JavaScript を悪用した新たな「Web クライアント JavaScript 難読化技術を用いたエクスプロイトキット」が収集データに追加された点です。これは、難読化を回避技術として活用し、従来の制御をすり抜ける新たな脅威が急速に拡散し得ることを示しています。調査結果によれば、新たなエクスプロイトが出現する一方で、攻撃者は依然としてブラウザ、Web フレームワーク、オープンソースツールにおける古くから広く利用されている脆弱性に大きく依存し続けています。

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。「第 2 四半期を通じて、本レポートの調査結果は、攻撃者が検知を回避し、影響の最大化に注力する中で、暗号化チャネル経由の回避型マルウェアが増加していることを示しています。リソース制約のある MSP や小規模 IT チームにとって、この変化は強力

な対策で迅速に適応することが喫緊の課題であることを意味しています。一貫したパッチ適用、実績ある防御策、迅速な対応が可能な高度な検知／レスポンス技術が、これらの脅威を軽減する最も効果的な対策であり続けています。」

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 2 四半期版）における主な調査結果を紹介します：

- **新規かつ独自のマルウェア脅威が 26%増加し、**脅威アクターによるマルウェア回避手法である暗号化のパッキング普及が明らかになりました。これらのポリモーフィック脅威はシグネチャベースの検知を回避するため、APT Blocker（標的型攻撃対策）や IAV など、ウォッチガードの高度なサービスによる検知率が上昇しています。
- **脅威ラボは予期せず、リモートアクセスバックドア「PUMPBENCH」とローダー「HIGHREPS」といった 2 つの USB ベースのマルウェア脅威を特定しました。**両者ともコインマイナー「XMRig」を展開し、Monero（XMR）をマイニングしており、暗号資産保有者におけるハードウェアウォレットの使用と関連している可能性が高いと言えます。
- **ランサムウェアが 47%減少し、**標的を厳選して影響力の大きい組織を狙う攻撃へと移行しており、より深刻な結果をもたらす傾向を反映しています。特に、アクティブな恐喝グループの数が増加しており、Akira や Qilin が最も攻撃的なグループとして挙げられます。
- **ドロッパーがネットワークマルウェアの多くを占めていました。**検知上位 10 件のうち 7 件が第一段階のペイロードであり、トロイの木馬「Trojan.VBA.Agent.BIZ」や認証情報窃取マルウェア「PonyStealer」などが含まれ、初期侵害にユーザーが有効化したマクロを悪用しています。悪名高い Mirai ボットネットも 5 年ぶりに再出現し、主にアジア太平洋地域に集中しました。ドロッパーの増加は、攻撃者が多段階感染を好むことを示しています。
- **ゼロデイマルウェアが依然として主流であり、全検知件数の 76%以上、暗号化マルウェアのほぼ 90%を占めています。**これらの調査結果は、特に TLS トラフィック内に隠蔽された脅威に対して、シグネチャを超えた高度な検知能力の必要性を強調しています。
- **DNS ベースの脅威が続いており、**DarkGate リモートアクセストロイ（RAT）に関連するドメインや、RAT として機能するローダーマルウェアが含まれ、DNS フィルタリングが重要な防御層であることを裏付けています。

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 2 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-q2-2025（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

【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