

## ウォッチガード、2024 年第 3 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： 正規の Web サービスやドキュメントが標的とされ、 エンドポイントマルウェアが 300%増加

その他クリプトマイニング型マルウェアの復活、シグネチャベースの攻撃や  
ソーシャルエンジニアリング攻撃の増加、EMEA 全域におけるマルウェア攻撃の増加

**2025 年 4 月 18 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（2024 年第 3 四半期）を発表しました。本レポートでは、第 3 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。

本レポートの主な調査結果では、エンドポイントで検知されたマルウェアが前四半期比で 300%増加し、脅威アクターが攻撃の実行にソーシャルエンジニアリングの手法を多用するようになり、悪意のある目的のために正規の Web サイトやドキュメントを悪用する脅威が増加していることが浮き彫りになっています。Word や Excel のようなマイクロソフトのドキュメントは、ユーザーを欺いて悪意のあるソフトウェアをダウンロードさせる標的として長い間利用されてきましたが、Word、Excel、PowerPoint の Office ファイルに対する厳格なマクロ対策により、攻撃者は現在、OneNote ファイルを利用して Qbot（リモートアクセスのボットネット型トロイの木馬）を配信するようになっています。また、正規のサービスを悪用するもう 1 つの脅威として、WordPress プラグインの脆弱性を狙った新たな攻撃が台頭しています。脅威アクターはこのような脆弱性を悪用することで Web サイトを制御し、そのサイトの知名度を利用してブラウザのアップデートを促すためのプロンプトでユーザーを欺き、マルウェアを実行する SocGholish のような悪意のあるダウンロードをホストしています。WordPress は世界中で 4 億 8,860 万以上の Web サイトをホストしており、インターネット上の全 Web サイトの 43%を占めています。

脅威ラボでは、今四半期、クリプトマイナーを利用する脅威アクターの増加も観測しており、その多くはさらに悪質な行為を実行できる能力を有していました。クリプトマイニングとは、ユーザーの端末に潜伏し、その端末のコンピューティングリソースを窃取して、ビットコインなどのオンライン通貨をマイニングするマルウェアです。暗号通貨の価値と人気が再び高まるにつれ、クリプトマイニングを行うマルウェアの使用頻度も再び高まっています。

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。「2024 年第 3 四半期のインターネットセキュリティレポートの調査結果は、従来のマルウェア脅威と回避型マルウェア脅威の劇的な変化を示しています。これらの調査結果は、脅威の状況がいかに迅速に進化するかを示しています。したがって、古い脅威を迅速に捕捉し、新しい脅威にリアルタイムで適応できる、包括的できめ細かい防御機能を備えたサイバーセキュリティソリューションを活用することが重要です。あらゆる規模の組織は、予期せぬトラフィックパターンを発見し、滞留時間を短縮するために AI を活用

した脅威検知の採用を検討すべきであり、結果として侵害のコストを削減するだけでなく、従来のマルウェア対策も維持することができます。」

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（2024 年第 3 四半期版）における主な調査結果を紹介します：

- 今四半期は、シグネチャベースの検知数が 40%増加し、脅威アクターが攻撃の実行にソーシャルエンジニアリングの手法を多用し始めています。攻撃者は、レガシーシステムや広範な脆弱性を悪用する戦略を洗練させており、従来型のマルウェアの普及率が上昇していることを裏付けています。
- マルウェア攻撃の検知数では、欧州・中東・アフリカ（EMEA）が全体の 53%を占め、前四半期から倍増しました。一方、ネットワーク攻撃の検知で最も多かったのはアジア太平洋地域で、59%が同地域の標的となっていました。
- マルウェア攻撃は、前四半期から 15%減少しました。また、脅威ラボの調査結果によると、攻撃者が新たに作成したマルウェアや独自のマルウェアは前四半期に比べて減少していますが、その代わりに、より広範なマルウェアのテクニックを使用してデバイスを感染させています。
- 検知されたマルウェアのうち、シグネチャベースの検知手法を回避できたのはわずか 20%でした。これは、いわゆる「ゼロデイマルウェア」と呼ばれている、よりプロアクティブな手法で検知する必要のあるマルウェアの実態とは大きく異なる結果でした。
- ランサムウェアはここ数四半期減少傾向が続いていましたが、脅威ラボのデータによると、今四半期は 2024 年第 2 四半期よりもランサムウェアによる攻撃が増加しました。脅威アクターは、新たな攻撃手段を作り出すのではなく、ランサムウェアを配信するために既存の手口が幅広く使用されました。
- 今四半期のエンドポイントにおけるマルウェア検知数は、第 2 四半期と比較して 300%増と大幅に増加しました。この増加は、アクティブなマシン 10 万台あたりでブロックされた脅威が 74%減少したことと相まって、エンドポイントに届くスパムのような同種のマルウェアが氾濫し、同じペイロード（悪質なコード）を持つ別々のマルウェアキャンペーンである可能性が高いことを示唆しています。

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（2024 年第 3 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-q3-2024>（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 (TM) (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](mailto:jpnsales@watchguard.com)

URL : <https://www.watchguard.co.jp>