Press Release
2026 年 11 月 20 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：
2026 年上半期、AI の台頭により、マルウェアによる大量攻撃から精密攻撃へ移行

攻撃数の減少の裏で、広範な偵察活動、巧妙な回避行動、TLS の脆弱性を悪用

2026 年 11 月 20 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、日本法人社長 大野 欽司、以下ウォッチガード）は、最新の**「グローバル脅威レポート」**を発表しました。本レポートは年 2 回発行されており、脅威アクターが AI を活用したツールを駆使し、従来の雑多で大量のキャンペーンから、特定の被害者を標的としたマルウェアや、より広範囲にわたる目立たない低頻度の偵察行為（プロービング）、および認証情報に基づくアクセスといった攻撃手法に移行していることが明らかになりました。

本レポートは、ウォッチガードのネットワークセキュリティ製品およびエンドポイントセキュリティ製品より、匿名化された情報を収集して得られた脅威インテリジェンスに基づいており、ネットワーク上のエクスプロイト活動全体が減少する一方で、攻撃者がますます高度なマルウェアを使用していることが判明しました。ネットワーク攻撃の総件数は 79%減少したものの、エンドポイントにおける新規マルウェアは前年比で 2,000%以上増加し、分析期間中のエンドポイントの脅威のほぼ 96%が、わずか 1 台のマシンにのみ確認されました。こうした相反する兆候は、脅威アクターが「マルウェア・アズ・ア・サービス（MaaS）」、自動化、そして AI を活用して、さらに多くのネットワークにわたるより多くの脆弱性をテストし、特定の被害者向けに大規模に独自のペイロード（悪意のプログラム）を作成し、従来の防御策を迂回していることを示しています。

ウォッチガードの CISO（チーフ・インフォメーション・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）は次のように語っています。「アラートの総数が減少したからといって、攻撃者の危険性が低下したわけではありません。攻撃者は、手に入るあらゆるツールを駆使して、より選択的かつ精密な攻撃を仕掛けています。最近の調査結果によると、再利用可能なペイロードや大量スキャンから、個々のシステムに合わせてカスタマイズされたマルウェア、広範囲にわたる低強度／低頻度のプロービング、そして境界防御を迂回できる認証情報に基づくアクセスへと、攻撃の手口が移行していることが示されています。MSP にとって、広範に顧客を保護するためには、統合的な可視性、TLS インスペクション、AI を活用した検知、強力な ID 制御、そして継続的なレスポンスが不可欠となります。」

攻撃の件数と多様性の間にギャップが拡大していることに加え、本レポートの主な調査結果には以下の点も挙げられます：

- **初期侵入手法が変化している**：調査データによると、脅威アクターはセキュリティレイヤを突破するために、信頼の置けるアカウントやネイティブツールをますます多用していることが明らかになりました。PowerShell の検知件数は急激に減少した一方で、認証情報の取得、持続化、リモートアクセス、および防御回避が、今年上半期の脅威ハンティングにおいて最も顕著なテーマとして浮上しました。

- **攻撃件数が減っているものの、対象が広範囲になっている：**ネットワーク攻撃の平均件数は減少したものの、IPS シグネチャのユニーク数が増加し、上位 10 件の攻撃が占める割合は減少しました。汎用的な Web シェルシグネチャが世界で最も広範なネットワーク攻撃となり、ベルギーのマシンの 75%、イタリアと米国のマシンではそれぞれ 60%近くに達しました。
- **攻撃者は依然として古い脆弱性を悪用して利益を得ている：**本レポートで挙げられたネットワーク攻撃シグネチャの上位 50 件に関する脆弱性の中央値は 2014 年に公開されたものであり、CVE に関する 44 件のシグネチャのうち 31 件は、少なくとも 10 年以上前の脆弱性を標的としていました。SQL インジェクションだけでも、ネットワーク攻撃の検知件数の 17%以上を占めていました。
- **暗号化は依然としてデフォルトの配信経路となっている：**マルウェアの 95%は TLS 経由で届きましたが、デバイスのうち暗号化されたトラフィックを検査しているのはわずか 20%に過ぎません。回避型マルウェアは、検知件数全体の 3 分の 1 近くを占め、高度なマルウェア防御機能を備えたデバイスにおける TLS インスペクションを通じて確認された検知件数の 36%を占めました。
- **ランサムウェアは依然として活発かつ競争の激しい市場となっている：**ランサムウェアのエコシステムは、統合が進む一方で、新たな参入者も引き寄せています。公に確認された恐喝活動が過去最高水準に達したにもかかわらず、エンドポイントでの検知件数は前年同期比で 68%以上減少しました。ウォッチガードは 2026 年上半期に 41 の新たなランサムウェアグループを追跡しており、上位 8 つのグループが、約 5,000 件に上る公に確認された恐喝要求の半数以上を占めました。

この調査結果は、侵入防止、高度なエンドポイント保護、アイデンティティセキュリティ、そして継続的な監視を組み合わせた多層防御体制の必要性を改めて裏付けています。セキュリティチームや MSP は、古い脆弱性やサポート終了済みのエッジデバイスへの対応を優先するとともに、多要素認証（MFA）やゼロトラスト型のアクセス制御を導入し、アラートの総数だけでなく、攻撃の到達範囲や多様性も把握する必要があります。

ウォッチガードの「グローバル脅威レポート」（英語版）は以下よりダウンロードできます。
https://www.watchguard.com/wgrd-resource-center/security-report-h1-2026

*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】
ウォッチガードは、マネージドサービスプロバイダー（MSP）向けに設計された統合型サイバーセキュリティ分野におけるグローバルリーダーです。30 年以上にわたり、MSP が大規模なセキュリティ対策を提供する方法を確立し、脅威情勢のあらゆる大きな変化に先んじるべく、絶えず革新を続けてきました。AI を活用した「Unified Security Platform（R）」により、ゼロトラストに対応したネットワーク、エンドポイント、アイデンティティ保護機能を単一の統合プラットフォームで提供し、複雑な運用の軽減、対策成果の向上、ビジネスの効率的な成長を可能にします。世界中で 150 万社以上の顧客を保護する 25,000 社以上の MSP に利用されており、パートナーが世界中の顧客に対して、強力かつ測定可能なセキュリティの成果を提供できるよう支援しています。

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