Press Release
2023 年 12 月 12 日（火）
ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガードの脅威ラボが「2024 年度サイバーセキュリティ予測」を発表

LLM、AI ベースのボイスチャットボット、最新の VR/MR ヘッドセットなど、注目のハッキングを研究者たちが予測

2023 年 12 月 12 日（火）– 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、「2024 年度サイバーセキュリティ予測」を発表しました。「2024 年度サイバーセキュリティ予測」は、ウォッチガードが毎年発表しているセキュリティに関する最新の予測であり、大規模言語モデル（LLM）を標的とした悪意のあるプロンプトエンジニアリングの手口、マネージドサービスプロバイダー（MSP）による、自動化を徹底した統合型セキュリティプラットフォームの強化、AI を活用した音声チャットボットで悪意のある活動を拡大する「ビッシャー」、そして最新の VR/MR ヘッドセットでのハッキングなど、ウォッチガードの脅威ラボ調査チームが 2024 年に出現すると考えている、最も顕著な攻撃や情報セキュリティのトレンドが網羅されています。

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。「新種のテクノロジーが登場するたびに、サイバー犯罪者が利用できる攻撃ベクトルが新たに生まれています。2024 年では、企業や個人を標的とする新たな脅威は、さらに高度化、複雑化し、管理が困難になります。サイバーセキュリティのスキル不足が続く中、サイバーセキュリティを強化し、進化し続ける脅威情勢から組織を守るために、MSP、統合型セキュリティ、自動化プラットフォームの必要性はかつてないほど高まっています。」

以下にウォッチガードの脅威ラボチームによる、2024 年度の主なサイバーセキュリティ予測を紹介します：

- **大規模言語モデル（LLM）を標的とした悪意のあるプロンプトエンジニアリングの手口：**現在、企業や個人は、業務効率を高めるために LLM を試しています。しかし、攻撃者も LLM を不正な目的のために悪用する方法を学びつつあります。ウォッチガードの脅威ラボは、2024 年の間に、犯罪攻撃者であれ研究者であれ、賢明なプロンプトエンジニアがコードを解読し、LLM を操作して個人データを流出させるだろうと予測しています。
- **MSP が自動化プラットフォームでセキュリティサービスを強化：**サイバーセキュリティ関連の求人は約 340 万件に上り、有効な人材をめぐって熾烈な競争が繰り広げられているため、2024 年にはより多くの中小企業が、MSP や MSSP と呼ばれる信頼できるマネージドサービスプロバイダーやセキュリティサービスプロバイダーにセキュリティ保護を依存するようになると思われます。MSP や MSSP は、増大する需要と不足する人材リソースに対応するため、人工知能（AI）や機械学習（ML）を活用した高度な自動化機能を備えた統合型セキュリティプラットフォームをさらに強化すると予測されます。
- **ダークウェブで AI スピアフィッシングツールの販売が好調：**サイバー犯罪者はすでに、スパムメールを送信したり、説得力のある文章を自動的に作成したり、インターネットやソーシャルメディアから特定のターゲットの情報や人脈をかき集めたりするツールをアンダーグラウンドで購入することができますが、こうしたツールの多くはまだ手作業で、攻撃者は一度に 1 人のユーザーやグループを標的にする必要があります。このような整然とした手順のタスクは、人工知能や機械学

習による自動化に最適であり、2024 年には AI を搭載したツールがダークウェブのベストセラーになる可能性が高いと予測されます。

- **AI を活用したビッシングが 2024 年に本格化：**VoIP（ボイスオーバーインターネットプロトコル）と自動化技術により、膨大な数の番号に簡単にダイヤルできるようになりましたが、電話を受けた人間が被害に至るまでには、依然として人間の詐欺師が必要です。このような方法だと、ビッシング詐欺（インターネット電話などを使ってカード番号などを盗み出そうとするフィッシング詐欺の新たな手口）は簡単には成立しませんが、2024 年には変わる可能性があります。ウォッチガードは、説得力のあるディープフェイクオーディオと、電話を受取った人と会話を続けることができる LLM が組み合わさることで、ビッシングコールの規模と量が大幅に増加すると予測しています。しかも、人間の攻撃者が関与する必要すらなくなるかもしれません。
- **VR/MR ヘッドセットでユーザー環境を再現：**仮想現実と複合現実（VR/MR）のヘッドセットは、ようやく普及の兆しを見せています。しかし、新しく便利なテクノロジーが登場するところには、犯罪者や悪意のあるハッカーがつきまといます。2024 年には、研究者か悪意のあるハッカーが VR/MR ヘッドセットからセンサーデータの一部を収集し、ユーザーがプレイしている環境を再現するテクニックを見つけるだろうと脅威ラボの研究者は予測しています。
- **QR コードの利用急増によりハッキングが大量発生：**携帯電話などのデバイスでリンクをたどる便利な方法を提供するクイックレスポンス（QR）コードは、数十年前から存在していましたが、近年、あらゆる場所での利用が爆発的に増加しています。脅威ラボのアナリストは、2024 年に、従業員が QR コードをたどって悪意のある宛先に移動することによって引き起こされる大規模なハッキングが発生すると予想しています。

脅威ラボによる来年の予測についての詳細、および ウォッチガード CSO の Corey Nachreiner と セキュリティオペレーション担当ディレクタの Marc Laliberte による予測ビデオは、以下でご覧いただけます。
https://www.watchguard.com/wgrd-resource-center/cyber-security-predictions-2024

【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ーと提携しており、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 Twitter（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。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