Press Release

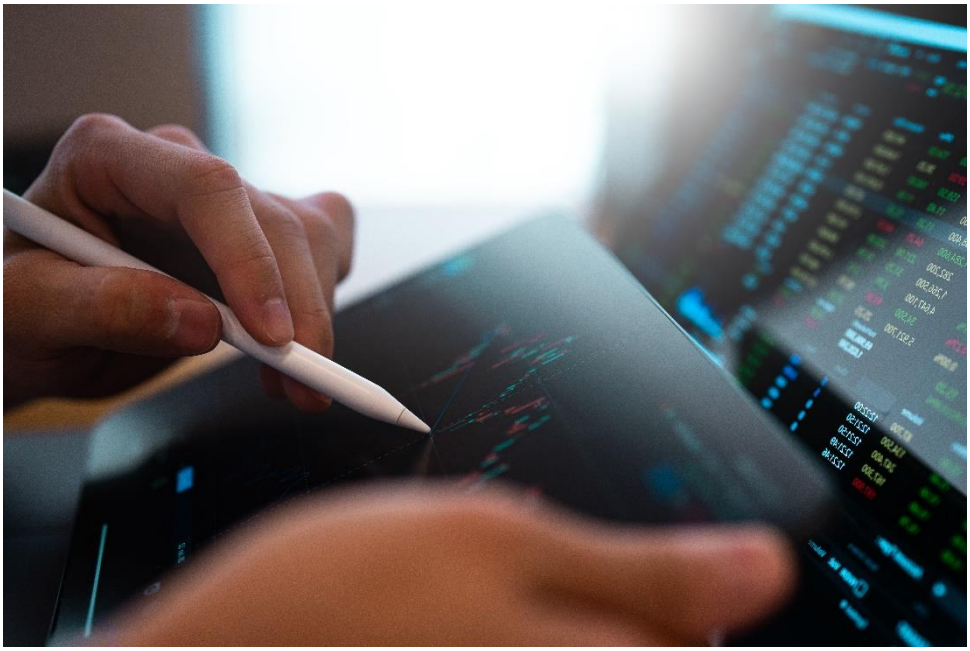
ノートン 広報部
2023 年 12 月 26 日

急速する AI 技術の進歩はサイバー犯罪の脅威にも
高度な AI により、脅威は個人と中小企業の双方に対してさらにパーソナライズ化へ

ノートン、2024 年のサイバーセキュリティ予測 5 選を発表

進化するサイバー犯罪の脅威から身を守るヒントを伝授

消費者向けサイバーセーフティブランド「ノートン™」は、2024 年に起こり得るサイバー犯罪の脅威についての予測 5 選を発表いたします。2024 年は、AI 技術の進歩により高度に個々へパーソナライズされた脅威に対して、警戒を強める必要があります。家族や同僚の声、外見を模倣するサイバー犯罪者がディープフェイクを使用し、信ぴょう性の高く見える広告やダイレクトメッセージを介して配信されるスパイウェア・アプリなど、見たり、聞いたり、読んだり、クリックしたりするものに対して、見た目通りの信頼できるものであるかどうかを再確認することが、これまで以上に重要となります。



2024 年 ノートンサイバーセキュリティ予測 5 選

1. AI の進歩がサイバー犯罪の急増に拍車をかける

ノートンの専門家は、2024 年は AI の能力が多様化する年と予測しており、サイバー犯罪はテキスト生成にとどまらず、テキストから動画やその他のマルチメディアを作成するツールを持つようになるだろうと述べています。このような進歩により、特に頻繁に広告が目に入るショート動画などの動画メディアの場合、本当の録画動画と生成された動画を見分けることがより難しくなるだろうと予測しています。

2. ソーシャル・エンジニアリングがより顕著になる

サイバー犯罪者は、人々の感情や脆弱性を操ることが、欲しい情報やものを手に入れる最善の方法だと認識しています。ノートンの専門家は、2024 年にサイバー犯罪者は AI が生成したコンテンツをソーシャルメディア上で利用し、フェイクニュースや欺瞞的な広告、公人のディープフェイク、信頼できる人脈から発信されたように見せかけたダイレクトメッセージを広める、などの手口が増えると指摘しています。上記のようなソーシャル・エンジニアリング攻撃は、ソーシャルメディアだけでなく、サイバー犯罪者が AI を使用して上級幹部の声や外見を模倣する BCC（Business Communication Compromise）攻撃（以前は BEC（Business Email Compromise）攻撃と呼ばれていた）の進化に伴い、企業においてもさらに深刻化するだろうと予測しています。

3. 個人および企業に向けたデジタル恐喝は、より標的を絞るようになる

2024 年には、ダークウェブ上でのデータの買い取りや、VPN インフラを悪用しデータを盗んだりする恐喝がより狡猾になると、ノートンの専門家は予測しています。さらに、クラウドインフラへの攻撃は大幅に増加し、リモートワークやクラウドベースの組織構造に大きな課題をもたらす可能性もあります。また、恐喝の手口も従来の暗号化だけでなく、犯罪者がセクストーションのような手法で人々や企業を恐喝するなどといった恐喝手法の進化が予測されます。

4. スパイや恐喝を行うモバイルアプリが増える

金融技術の進歩に伴い、即日融資のやり取りができるアプリ関連において悪質行為の増加が懸念されています。アプリでは迅速かつ、簡単に融資を受けられることができ、近年利用者からの人気が高まっています。一方で確実に返済を回収するために、非倫理的な手法をとる悪徳金融業者も登場してきています。このような背景から、ノートンの専門家は今後、モバイル機器をターゲットにした偽のチャットアプリ作成と配布が急増し、一見何の問題もないように見えるインターフェースの中に暗号を盗むモジュールや、スパイウェアのモジュールを隠す可能性があると述べています。

5. 暗号通貨における脅威の高まり

暗号通貨の急速な進化は、サイバー犯罪者にとっても新たな機会を生む可能性があります。暗号通貨の非中央集権的な性質により、詐欺の逆探知や詐欺の検出がほとんど不可能です。ノートンの専門家は、サイバー犯罪者は暗号通貨取引所や相互運用プロトコルへの侵入や、急速に発展している MaaS（Malware-as-a-Service）を使用したスマートコントラクトの悪用など、多くの手段を通じて暗号資産の所有者を標的にすると考えています。

進化するサイバー犯罪の脅威から身を守るために

2024 年、サイバー犯罪がより巧妙になり、標的が絞られ、発見が難しくなる中、ノートンは消費者が自分自身とデジタル・フリーダムを守るためのツールや知識、ヒントを提供し続けることを目指しています。進化するサイバー犯罪の脅威から身を守るために、以下 4 つのポイントをお伝えします。

- **クリックする前に懐疑的になりましょう**

サイバー犯罪者は、人気の企業や組織、人物に装うことがあります。誰が実際に連絡をしてきているのかよく調べずにボタンやリンクをクリックしないようにしましょう。

- **パスワードを管理しましょう**

パスワードを異なるアカウントで同じものを使用しないようにし、多様素認証を利用できる場合は利用しましょう。ノートン パスワードマネージャーなどのツールは、安全で複雑なパスワードを生成・管理し、各アカウントに固有のパスワードを設定することで、パスワードの再利用による複数アカウントへの侵入を防ぎます。

● **プライバシー、セキュリティ、アイデンティティの保護は徹底しましょう**

個人情報の盗難・流出が増加し、手口が巧妙化している中、データ漏洩を警告するツールは不可欠です。ノートン 360 では、Windows、Mac、スマートフォン、タブレットをオールインワンで保護し、Windows 向けクラウドバックアップ、インターネット閲覧をプライベートに保つ VPN を提供します。また、データが流出したことを検知するだけでなく、問題の修復をサポートします。

● **コンピュータのみならずモバイルセキュリティも忘れずに**

悪質なアプリが増加し、サイバー犯罪者が消費者をインターネット上であらゆる角度から追跡する手口も増えてきています。iOS および Android で利用可能なアバスト モバイルセキュリティなど、最新のモバイルセキュリティをスマートフォンにインストールしておきましょう。

ノートン製品情報

■パソコン、スマホをオールインワンで守るセキュリティソフト

ノートン™ 360：https://jp.norton.com/360

ノートン 360 デラックスは、パソコン、スマホ、タブレットなどのデバイスと Wi-Fi 通信等をオールインワンで守るセキュリティソフトです。詐欺サイトやウイルスなどサイバー攻撃の脅威を検知し、防御する他、インターネット利用時に通信内容を盗み見されないように暗号化する VPN 機能を搭載。その他、お子様を守るための保護者機能、個人情報流出を検知するダークウェブモニタリング機能、パスワードを安全に管理するパスワードマネージャー機能など、消費者の皆様が、より快適かつ安全にインターネットを利用できるようになる機能を多数搭載しています。

*ノートン 360 スタンダード版には、保護者機能とダークウェブモニタリング機能は搭載していません。

■個人情報の流出を検知し、メールとアプリで通知、被害時に 365 日電話でサポート！

ノートン™ ID アドバイザー：https://jp.norton.com/products/identity-advisor

ノートン™ 公式ストア：https://jp.norton.com/

流出した個人情報は、ダークウェブ等で売買され、不正利用される可能性があります。ノートンはインターネットをパトロールし、お客様の個人情報が流出した場合、メールとアプリでお知らせします。また、SNS アカウントの乗っ取り、フィード内の危険なリンクや不適切コンテンツを警告します。個人情報の不正利用被害にあった場合は、365 日復旧支援スペシャリスト(日本拠点）がトラブル解決をサポートします。関連機関と三者通話を行い、サポートさせていただく場合もございます。

*対象 SNS 等、機能の詳細は HP をご確認ください。

ノートンについて

ノートンは、サイバーセーフティのブランドである、Norton、Avast、LifeLock、Avira、AVG、ReputationDefender、CCleaner を通じて、デジタル化が進んだ世界においてもサイバー犯罪などの危険を心配せず、自由にデジタルを使いこなせる環境、「デジタルフリーダム」の実現に力を注ぐグローバル企業「ジェン (NASDAQ：GEN)」の主要サイバーセーフティブランドです。人々が安全に、プライバシーが保たれ、自信を持ってデジタルライフを送ることができるよう、これからの時代もサポートしてまいります。ジェンは、サイバーセキュリティ(インターネット利用の保護)、プライバシー保護、個人情報対策の分野で受賞歴のある製品とサービスを、150 カ国以上の 5 億人以上のユーザーに提供しています。詳しくは、Norton.com と GenDigital.com をご覧ください。