身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2023年12月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

■フィッシングによるインターネットバンキングへの不正送金被害が急増

2023年12月29日

・警察庁と金融庁は12月25日、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について、注意喚起を発表した。一般財団法人日本サイバー犯罪対策センター（JC3）でも12月25日に、同様の注意を呼びかけている。

・警察庁及び金融庁によると、2023年4月及び8月に、インターネットバンキングに係る不正送金事犯による被害急増に関する注意喚起を行うとともに、被害金融機関と連携し対策を講じているが、その後も被害は拡大し続け、12月8日時点で、2023年11月末における被害件数は5,147件、被害額は約80.1億円と、いずれも過去最多を更新しているという。

・警察庁及び金融庁では年末年始は特に、3メガバンクを騙るフィッシングと、「不正アクセス」、「個人情報の確認」、「取引の停止」等のワードに注意を呼びかけている。

デジタル化が進む現代社会で、フィッシング詐欺は毎年増加しています。年末年始は特に、メガバンクを騙るフィッシング詐欺には注意しましょう。

■画像：不正送金発生状況のグラフ

■出典：
https://scan.netsecurity.ne.jp/article/2023/12/29/50419.html?utm_source=newspass&utm_medium=delivered&utm_campain=syndication

■長野日報社 ランサムウェア攻撃で業務支障 朝刊ページ数半分で発行

2023年12月21日

・諏訪市に本社がある新聞社、「長野日報社」がサイバー攻撃を受け、記事などを作る端末の一部が使えなくなったとして、２１日の朝刊のページ数を通常の半分にして発行しました。

・会社によりますと、１９日夜、社内にある新聞を作るためのサーバーに、データを勝手に暗号化して身代金を要求する「ランサムウエア」と呼ばれるサイバー攻撃があったということです。この影響で、サーバーと接続していた記事などを作る端末の一部が使えなくなったとしています。このため、２１日の朝刊のページ数は通常の半分の８ページにして発行しました。

・会社によりますと、原因は調査中で今のところ復旧の見通しもたっていないため、２２日以降もページ数を減らして発行する可能性もあるとしています。

ランサムウェアの被害に遭うと、業務に支障や遅れが生じてしまいます。セキュリティ対策の強化が必要と感じる場合はすぐに専門家に相談してみましょう。

■画像：NHK NEWS

■出典：
https://www3.nhk.or.jp/lnews/nagano/20231221/1010029146.html

■QRコードから不正サイト誘導、被害相次ぐ「クイッシング」と呼ばれる手口も

2023年12月1日

・全国的に普及している二次元コード（QRコード）を巡り、不正なサイトの広告が表示されたり、クレジットカード情報の入力を求められるなどの被害が相次いでいる。従来の「フィッシング」詐欺は、メールやショートメールから不正サイトにリンクさせて個人情報を入力させる手口。一方で、メール内の不正サイトへのURLリンクをQRコードに置き換えたケースは「クイッシング」とも呼ばれ、情報セキュリティ会社は警戒を呼びかけている。

・情報セキュリティー会社トレンドマイクロは、QRコードが悪用される手口について「（QRコードを使うことで）見た目によるリンクへの違和感や、不正リンクであるという識別も難しくなる」と説明。また、「最近はQRコード決済サービスの普及により、ネット詐欺の中で金銭を受け取る方法としてQRコードを提示する手口も出てきた」として警戒を強める。

■画像：決済などで普及しているQRコード

■出典：https://www.itmedia.co.jp/news/articles/2311/30/news134.html

詐欺の手法は日々、変化し巧妙になっていきます。少しでも不審に思ったり不安を感じたりしたら、すぐに身近な人に相談してみましょう。

■日本航空電子、米子会社にサイバー攻撃　製品図面が流出

2023年12月4日

・日本航空電子工業は4日、米国子会社が外部からの不正アクセスを受け、社内管理用の資料やコネクター製品の図面を含む生産業務用のデータが一部流出したと発表した。攻撃を受けた米子会社のサーバー内の一部ファイルも暗号化され、みられなくなっているという。ランサムウエア（身代金要求型ウイルス）による攻撃で、電話やメールによる脅迫を受けているが一切対応しない方針だ。

・同社はJAEオレゴンの不正アクセスを11月2日に検知し、6日に公表していた。その後具体的な被害について調査し、本日内容を発表した。子会社のサーバー内には日本の顧客の情報が入っている可能性もあるという。今後、今回の攻撃による被害が確認された場合は、関係する顧客に順次報告する。

・同社は対策本部を設置し、外部専門家と一緒に被害状況の調査と復旧作業を進めている。

■画像：日本航空電子

■出典：
https://www.nikkei.com/article/DGXZQOUC0490D0U3A201C2000000/

近年、ランサムウェアの被害に遭ってしまう企業が増加しています。各拠点の従業員教育とセキュリティ対策の強化に努めましょう。

■政府、内閣サイバー職員倍増へ　次官級配置、指揮系統を強化

2023年12月30日

・政府は、政府機関へのサイバー攻撃や不正アクセスを監視し、安全確保を担う内閣サイバーセキュリティセンター（NISC）の人員を2024年度に倍増させる方針を決めた。

・NISCトップのセンター長は内閣官房副長官補が務めている。現在はその下に専任の局次長級の内閣審議官3人を配置している。24年度からは次官級1人、局長級2人、局次長級3人を充てる計画。関係者によると、常勤の人員は現在約90人で、85人増員させる。これとは別に、専門知識を持つ民間の非常勤職員も増やす予定。

・昨年12月に策定した国家安全保障戦略は「サイバー安保分野での対応能力を欧米主要国と同等以上に向上させる」と明記。政府機関システムを常時分析し、脅威対策やシステムの脆弱性を是正するための仕組みを構築するとしており、NISCの態勢強化で具体化を図る。

政府のNISCの人員を倍増させる方針から、現在のセキュリティ対策を強化する重要性が分かります。

■画像：内閣サイバーセキュリティセンター（NISC）態勢強化のイメージ

■出典：
https://news.yahoo.co.jp/articles/026fd253c474592de3e8f652d111cce698c664a1

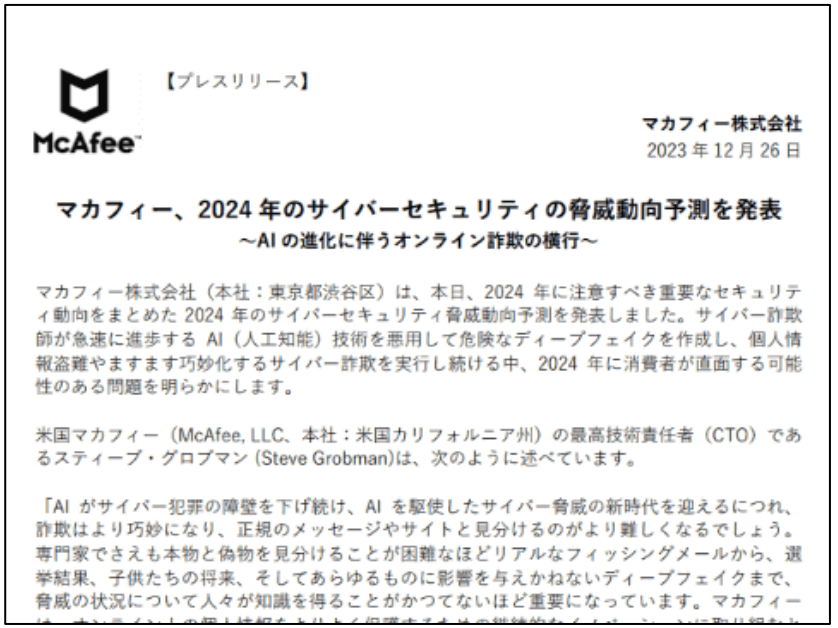
■マカフィー、2024年のサイバーセキュリティ脅威動向予測を発表 AIを悪用した詐欺などを警告

2023年12月28日

・マカフィー株式会社は12月26日、2024年の「サイバーセキュリティ脅威動向予測」を公開した。米McAfeeのCTOであるスティーブ・グロブマン氏は、発表にあたり「脅威の状況について人々が知識を得ることが、かつてないほど重要になっている」とコメント。AIにより、詐欺と正規のメッセージやウェブサイトとの見分けがより難しくなる中、脅威について知識を持つことが重要であるとした。

脅威動向予測の内容は、次の6項目。

・2024年選挙を妨害するディープフェイク
・ソーシャルメディア上にAI詐欺が横行
・子どもたちの間でのネットいじめが増加
・偽の寄付サイト
・新種のマルウェアや、声と映像のクローン詐欺がAIにより加速
・2024年パリ五輪に向け詐欺が急増



【プレスリリース】

マカフィー株式会社
2023 年 12 月 26 日

マカフィー、2024 年のサイバーセキュリティの脅威動向予測を発表
～AI の進化に伴うオンライン詐欺の横行～

マカフィー株式会社（本社：東京都渋谷区）は、本日、2024 年に注意すべき重要なセキュリティ動向をまとめた 2024 年のサイバーセキュリティ脅威動向予測を発表しました。サイバー詐欺師が急速に進歩する AI（人工知能）技術を悪用して危険なディープフェイクを作成し、個人情報盗難やますます巧妙化するサイバー詐欺を実行し続ける中、2024 年に消費者が直面する可能性のある問題を明らかにします。

米国マカフィー（McAfee, LLC、本社：米国カリフォルニア州）の最高技術責任者（CTO）であるスティーブ・グロブマン (Steve Grobman)は、次のように述べています。

「AI がサイバー犯罪の障壁を下げ続け、AI を駆使したサイバー脅威の新時代を迎えるにつれ、詐欺はより巧妙になり、正規のメッセージやサイトと見分けるのがより難しくなるでしょう。専門家でさえも本物と偽物を見分けることが困難なほどリアルなフィッシングメールから、選挙結果、子供たちの将来、そしてあらゆるものに影響を与えかねないディープフェイクまで、脅威の状況について人々が知識を得ることがかつてないほど重要になっています。マカフィー

■画像：マカフィー　サイバーセキュリティ脅威動向予測

■出典：https://internet.watch.impress.co.jp/docs/news/1558001.html

2024年にはAIの発達によって、サイバーセキュリティ脅威がさらに高まると予想されます。それらを回避するために脅威についての知識を持つことが大切です。

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。