BASIC
Confertas Office

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1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。

BASIC Confertas Office

■IPA 「情報セキュリティ10大脅威 2023」を決定

・IPA（独立行政法人情報処理推進機構）は、情報セキュリティにおける脅威のうち、2022年に社会的影響が大きかったトピックを「情報セキュリティ10大脅威 2023」として公表した。

・個人の順位では、「フィッシングによる個人情報等の詐取」が2年連続で1位。フィッシング対策協議会のフィッシング報告状況によると2022年の報告件数は約97万件と、2021年の約53万件から大幅に増加しており、一層の注意が必要。

・組織の順位では、3年連続で「ランサムウェアによる被害」が1位。2022年も脆弱性を悪用した事例やリモートデスクトップ経由での不正アクセスによる事例が発生。

・ランサムウェアの感染経路は多岐に渡るため、ウイルス対策、不正アクセス対策、脆弱性対策などの基本的な対策を、確実かつ多層的に適用することが重要。また、バックアップの取得や復旧計画を策定するといった、攻撃を受けることを想定した事前の準備が重要。

多岐に渡る脅威に対して、適切な対策を取ることが引き続き求められます。専門家に相談し、対策を施しましょう。

2023年1月25日

前年順位	「個人」向け脅威	順位	「組織」向け脅威	前年順位
1	フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害	1
2	ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃	3
3	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取	2
4	クレジットカード情報の不正利用	4	内部不正による情報漏えい	5
5	スマホ決済の不正利用	5	テレワーク等のニューノーマルな働き方を狙った攻撃	4
7	不正アプリによるスマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7
6	偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害	8
8	インターネット上のサービスからの個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加	6
10	インターネット上のサービスへの不正ログイン	9	不注意による情報漏えい等の被害	10
圏外	ワンクリック請求等の不当請求による金銭被害	10	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

■画像：IPA 「情報セキュリティ10大脅威 2023」の個人/組織向けランキング

■出典：IPA（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/about/press/20230125.html

■個人情報漏えい・紛失事故　2年連続最多を更新。流出・紛失情報は592万人分

2023年1月19日

・㈱東京商工リサーチが独自集計・調査を開始した2012年以降の11年間で、漏えい・紛失した可能性のある個人情報は累計1億2,572万人分で、日本の人口に匹敵するスケールに広がった。このほか、集計対象外だが非上場企業や海外企業、官公庁、学校など様々な組織でも事故は起きており、流出した個人情報は天文学的なボリュームにのぼるとの見方もある。

・2022年の情報漏えい・紛失事故の165件のうち、原因別では、「ウイルス感染・不正アクセス」の91件（構成比55.1%）が最多で、半数以上を占めた。次いで、「誤表示・誤送信」が43件（同26.0%）で、メールの送信間違いやシステムの設定ミスなど人為的な原因も上位に入った。

・被害の大きさや影響度合いが大きい「ウイルス感染・不正アクセス」は増加の一途をたどる。特に、2022年は2月以降、マルウェア「Emotet」による感染が急拡大した。

・情報漏えい・紛失事故165件のうち、原因となった媒体別では「社内システム・サーバー」が76件（構成比46.0%）で最多。1件あたりの情報漏えい・紛失人数の平均では、「社内システム・サーバー」を媒体とした事故が11万2,363人分と突出した。社内サーバーが不正アクセスを受け、顧客情報が流出したケースなどが多い。

情報セキュリティ対策は、いまや企業が経営を維持するためには不可欠な時代ですね。

■画像：東京商工リサーチ調べ　ウィルス感染・不正アクセスによる事故　発生推移
■出典：Yahoo!ニュース　東京商工リサーチ
https://news.yahoo.co.jp/articles/c28ca4ab4daae97d32f55da96d08135e559f5d83?page=1

BASIC Confertas Office

■世界で最も使われるパスワードは「password」「123456」解読しやすいパスワードは控えましょう！

2023年１月１日

・パスワードに関する調査が世界規模で実施され、まだ多くの人が脆弱なパスワードを使用し、パスワードの使い回しをしている事実が明らかになった。使い回しで問題なのは、「パスワードリスト攻撃」だが、同じくらいに危険なのが、分かりやすい（解読されやすい）パスワードの設定。日本での第1位は「123456」、次いで「password」「1234」「12345678」と、いずれもハッカーからすると1秒以内で解読できるものばかり。

・職場で使用するツールや文書のパスワード共有は、生産性がアップし、便利な協業を促進できるため日常業務に欠かせない。しかしながらそこには、パスワードの漏洩リスクがつきものであるとして、よくある方法ながらも避けるべき7つの習慣（右記）をあげている。

パスワードの設定内容だけでなく、管理方法も一度見直してみましょう。

■表：パスワード漏えいにつながりやすい7つの習慣

1. Eメール	メールはその内容が暗号化されず、コンテンツがプロバイダのバックアップデータなどに保存されるため
2. SMSショートメッセージ	メール同様、エンドツーエンドの暗号化がされておらず、情報はクラウドベースで保管される。SMSはパスワードを含め、機密情報を送信するのにふさわしくない
3. スプレッドシート	クラウドベースのスプレッドシートを共有してパスワードを共有することは、シェアしたい人たちだけでなく、外部からの侵入にもさらされやすい
4. 付箋	職場や家庭でパスワードのシェアに多く利用されているのが付箋という事実がある。言うまでもなく、様々な人の目に触れ、紛失したり、盗難したりする可能性は無限大
5. メモ機能のアプリ	メモ機能のアプリに、会員番号やパスワード、ログイン情報を記入している人も多い。こうしたアプリは、初期設定で暗号化されていないため、機密情報の入力は避けるのがベスト
6. 記憶	調査では55%がパスワードの保管場所を「記憶」に頼っていると回答。デジタル化が進む中で、ログインとパスワードを使用する機会は増える一方、数十もの強力で複雑なパスワードを記憶するのは、もはや難しい。特に記憶に頼っているうちは、「安易なパスワード」を「使いまわす」という2つのミスを同時に侵すことになりかねない。
7. ウェブサイトでのパスワードマネージャー	ウェブサイトを利用する際に、ログイン画面から「自動」でログイン名とパスワードが入力されることがある。この方法のリスクは、他のデバイスやスマホ、旅先などでログインしようとする際に、どちらも自動入力されないし、情報が自分の記憶に残っていない可能性もかなり高い

■出典：Yahoo!ニュース　AMP
https://news.yahoo.co.jp/articles/da94a0cb42c19c3a0a46941e8caaf4041d652835?page=1

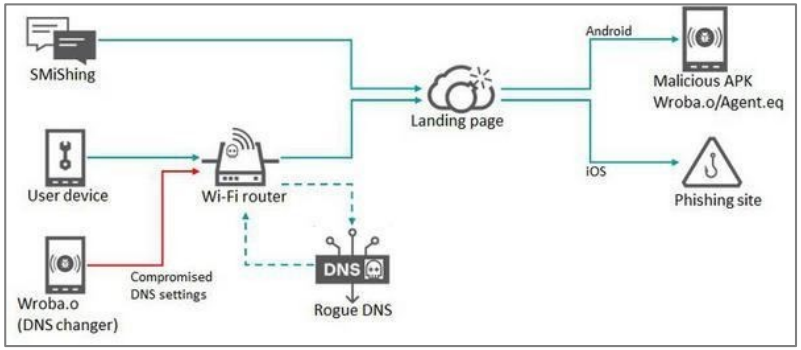
■Wi-Fiルータ乗っ取るマルウェア「Wroba」に注意

2023年1月24日

・セキュリティソフトメーカーのKaspersky Labは、Wi-Fiルータに侵入してドメインネームシステム(DNS: Domain Name System)をハイジャックする機能を備えた「Wroba」と呼ばれるDNS Changer型マルウェアに注意するよう呼びかけている。

・現状の主なターゲットは韓国とされているが、フランス、日本、ドイツ、米国、台湾、トルコなどの他の地域もターゲットにしていると分析されている。これらの地域ではスミッシング（携帯電話へのSMSを利用するフィッシングのこと）が主な初期感染手段とされ、今後DNS Changer機能が更新されて、これらの地域のWi-Fiルータが狙われる可能性があると予測されている。

・無料または公共のWi-Fiネットワークが脆弱な場合、感染したモバイルデバイスからルータが侵害され、さらに他のデバイスにこのマルウェアが拡散するリスクが指摘されている。



■画像：Wi-Fiルータを乗っ取る「Wroba」の感染フローとDNSハイジャック（Securelist）

無料または公共のWi-Fiネットワークへ接続するのは危険です。Wi-Fiルータのセキュリティ状況や、Wi-Fiへの接続時のルールを、社内で再確認しましょう。

■出典：マイナビニュース　TECH+
https://news.mynavi.jp/techplus/article/20230124-2572359/

■ヤマト運輸を装ったフィッシングメールやSMSに注意を呼びかけ

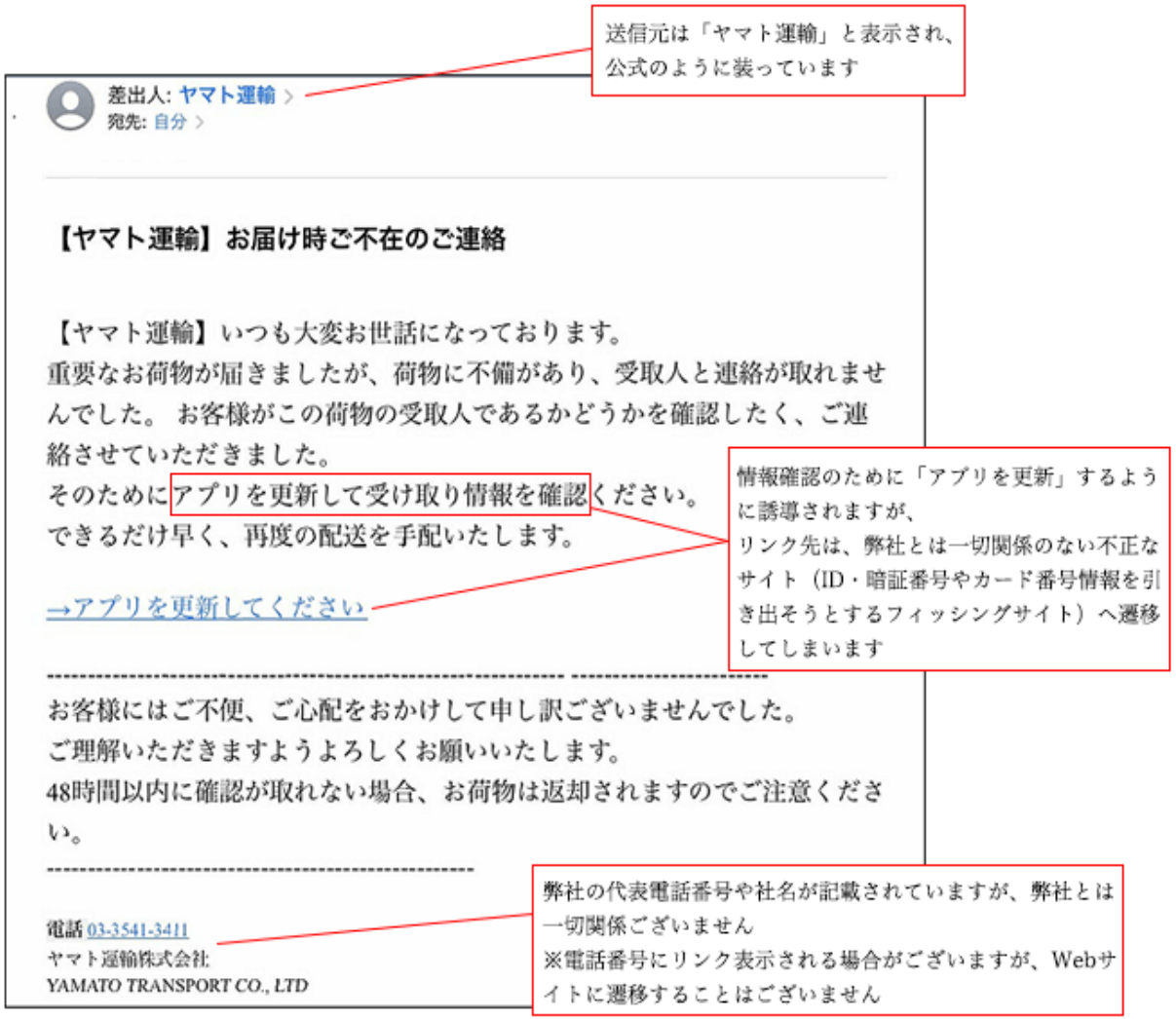
2023年1月5日

・ヤマト運輸は2023年1月5日、同社を装ったフィッシングメールやSMS等が報告されているとして注意を呼びかけ。メール文面のURLをクリックすると偽の詐欺サイトにつながる。

・荷物の配達時の不在連絡を装った内容となっており、URLをクリックしてアプリを更新するよう促す。

・リンク先はIDや暗証番号、クレジットカード情報等の入力を促す偽のサイトとなっており、誤って入力してしまうと第三者に情報が悪用される可能性があり、大変危険。

他にも新年早々、PayPayカードやビューカードをかたるフィッシングメールについての報告が見られました。引き続きフィッシング詐欺にも十分に注意する必要があります。



■画像：ヤマト運輸より Eメールの文面例 [1]

■出典：ヤマト運輸
https://www.yamato-hd.co.jp/important/info_181212.html

■日本独特のPPAPとEmotet被害

2023年1月3日

・国内での感染被害が深刻化しているエモテット（Emotet）は世界的に流行し、マルウェア脅威ランキングで世界1位にランキングされている。

・最近では攻撃メールの巧妙さが進化しており、添付ファイル名に実在する組織名を使ったり、メール本文に実在する組織名や署名などを掲載したりするケースも確認されている。

・暗号化ZIPファイルを添付し、本文に解凍パスワードを記載した攻撃メールが出現して以来、日本国内での被害が急拡大したといわれている。

・暗号化ZIPファイルをメールに添付し、その解凍パスワードを別メールで送付する方法は「PPAP」と呼ばれており、日本だけで普及した情報漏洩防止策であり、それが裏目に出た結果。

・内閣府がPPAPの廃止を宣言したことを受け、日立製作所やソフトバンクなどが相次いで利用廃止に踏み込む。日本国内ではPPAPを廃止する動きが加速している。

ZIPファイルの送信後にパスワード通知メールを送る、いわゆる「PPAP」は、セキュリティ対策としてはその有効性は以前から疑問視されています。Emotet被害を助長してしまう可能性がありますので、今一度ファイルの送信方法は検討しましょう。

■出典：NetIB-News
https://www.data-max.co.jp/article/61257

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。