事務所ニュース News
2023.4
K-044

発行 ： ふじわら税理士事務所　兵庫県高砂市神爪1丁目 12 番 18 号 高田ビル 2F　Tel.079(433)0030　Fax.079(433)0020

経営バイタルの強化書 KEIEI VITAL

脅威の内容を理解し、基本的な対策を身につけましょう!

情報セキュリティ10大脅威と対策

税務会計の業務においても電子帳簿保存法や電子インボイスの開始等が進み、電子データをどのように扱い、情報セキュリティをどう確保するかがますます重要になってきます。

情報セキュリティ10大脅威の内容と対策について理解しましょう!

1 情報セキュリティ10大脅威

IPA(独立行政法人情報処理推進機構)は、2023年1月25日「情報セキュリティ10大脅威 2023」を公開し、2月28日に組織編の解説書、情報セキュリティ10大脅威の活用法、情報セキュリティ10大脅威 2023 セキュリティ対策の基本と共通対策を公開しました。

「情報セキュリティ10大脅威」は情報セキュリティ対策の普及を目的として、2006年から前年に発生した情報セキュリティ事故や攻撃の状況等から脅威を選出し、上位10位までを公表しているものです。「個人」の立場と「組織」の立場でのランキングはそれぞれ【図1】のようになっています。

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位となりました。フィッシング詐欺は、実在の公的機関、有名企業を騙るショートメッセージサービス(SMS)等を送信し、偽物のウェブサイト(フィッシングサイト)へ誘導し、個人の認証情報(IDやPW等)や個人情報を入力させ詐取する手口です。

フィッシングに関する情報提供や動向分析を行っているフィッシング対策協議会※2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、フィッシングに対するより一層の注意が必要とされる状況になっています。詐取された認証情報による不正ログインを予防するためには、多要素認証を有効にする、被害を早期に発見するために利用サービスのログイン履歴やクレジットカード等の利用明細を日常的に確認する、といった取り組みが重要となります。

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位となりました。2022年も脆弱性(セキュリティの弱いところ)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しています。また、情報の暗号化のみならず窃取した情報を公開すると脅す「二重脅迫」に加え、DDoS攻撃(ウェブサイトやサーバーに対して過剰なアクセスやデータを送付するサイバー攻撃)を仕掛ける、被害者の顧客や利害関係者へ連絡するとさらに脅す「四重脅迫」が新たな手口として挙げられています。

ランサムウェアの感染経路は多岐にわたるため、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です。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をしておくことが重要です。

今年は個人、組織ともに10位の脅威が入れ替わるのみで、9位までの脅威の種類は昨年と同じとなりましたが、組織の10位に他の脅威を誘発しかねない「犯罪のビジネス化(アンダーグラウンドサービス)」が新たにランクインしたように、各脅威の手口を知り、脅威に対して適切な対策を取ることが求められています。

IPAでは従来の10大脅威の解説に加えて、今年新たに、多岐にわたる脅威に対して共通する対策をまとめて具体的に解説する「共通対策」を作成しています。そこでは、パスワードの適切な運用方法や、適切なインシデント対応方法などを7つの項目に分類して記載し、効率的な対策の支援が示されています。以下で情報セキュリティ対策の基本と共通対策について説明します。

【図1】情報セキュリティ10大脅威 2023※1

「個人」向け脅威	順位	「組織」向け脅威
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
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
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
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
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
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)
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
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
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
ワンクリック請求等の不当請求による金銭被害 圏外	10	犯罪のビジネス化(アンダーグラウンドサービス) 圏外

圏外 :昨年はランクインしなかった脅威

2 情報セキュリティ対策の基本と共通対策

① 情報セキュリティ対策の基本

世の中には「情報セキュリティ10大脅威」へランクインした脅威以外にも多数の脅威が存在しますが、攻撃者が利用する「攻撃の糸口(手口)」は類似したものが多く、脆弱性を悪用する、ウイルスを使う、ソーシャルエンジニアリングを使う等の古くから知

裏面へ続く→

られている手口が使われています。ここでは、【図2】に示すように「攻撃の糸口」を5つに分類し、それぞれに該当する対策を「情報セキュリテイ対策の基本」としています。脅威の内容は時代に応じて変わってきますが、「攻撃の糸口」に変化がない限り、「情報セキュリテイ対策の基本」を行うことでインシデントや被害に遭うリスクを低減することができるようになります。

【図2】情報セキュリティ対策の基本※3

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化 ※「共通対策」で詳細を解説	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視すべき対策を理解する

最近では、以前にも増してクラウドサービスの利用も一般的になってきています。クラウドサービスを利用する場合には、「情報セキュリテイ対策の基本」に加えてクラウドに特有な対策(責任範囲の明確化や、クラウドが停止した場合に備えた代替案の準備、設定不備への対応)を+αとして行うことで、被害に遭う可能性を少なくすることができます※3。

② 共通対策

脅威の種類は多岐にわたっていますがその対策に着目すると、共通しているものがあります。ここで説明する共通対策は、複数の脅威に対して同時に行うことができるため対策を効率的に進めることができます。

【図3】複数の脅威に有効な対策(共通対策)※3

対策	対象	
	個人	組織
パスワードを適切に運用する	○	○
情報リテラシー、モラルを向上させる	○	○
メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない	○	○
適切な報告/連絡/相談を行う	○	○
インシデント体制を整備し、対応を行う		○
サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う		○
適切なバックアップ運用を行う	○	○

「複数の脅威に有効な対策」として、誰もが知っておくべき3つの対策についてその概要を説明します。

対策1 パスワードを適切に運用する

個人や組織に関わらずパスワードの設定はオンラインショッピングやネットワークカメラ(見守りカメラ)等の様々な場面で必要になります。適切な設定・運用を行い、不正ログインされてしまった場合の下記の対策を行いましょう。

●適切な設定をする

・初期設定のままにしない
・以下を意識した推測されにくいパスワードを設定する
　①数字、アルファベット、記号等の複数の文字種を組み合わせる
　②生年月日や名前を使わない
　③連続した数字やアルファベットにしない
　④単純な単語一語だけにしない
・パスワードは使い回さない
　複数のサービスで同じパスワードを利用していると、どこかで漏れた時に軒並み不正ログインされてしまう

●適切な保管、運用を行う

・パスワードは他人に教えない
・IDとパスワードをセットで保管しない
・スマホやPCにパスワードのメモを貼らない
・複数人で使用する端末ではブラウザにパスワードを記憶させない

●不正ログインされてしまった時の対応

・パスワードを即時に変更する
・パスワードを使い回している場合、併せてパスワードを変更する

対策2 情報リテラシー、モラルを向上させる

世の中には意図せず情報モラルに反することを行ったり、故意に不正を行ったりする人がいます。組織においては業務で急いでいたり、緊急対応をしていたり等、精神的に追い込まれて、組織のためによかれと考えてルールに反してしまうこともあります。悪気があるかないかに関わらず自身の行為には責任が伴い、特に、組織においてはたとえ従業員の勝手な行動であったとしても組織への影響や責任が問われることが多くあります。「個人として」、「組織として」どのように対策すべきか理解しましょう。

●家族や組織従業員を教育する

情報リテラシーの向上が必要な者は気を付けるべきことに自身で気付けないことが多い。個人であれば、これからPCやスマホを使う子へ、使い慣れていない親へ、組織であれば従業員への教育を行います。例えば、下記のような教育を行うとよいでしょう。

【個人、組織共通】

①SNSの利用に関するケース
　・掲載されている情報が正しいとは限らない
　・安易に情報を拡散しない
　・情報発信は慎重に行う
②インターネット利用に関するケース
　・本物に似せた偽のウェブサイトがある
　・個人情報を盗もうとするウェブサイトがある

●継続的に取り組む

・定期的に、適切な時期に教育する

対策3 メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない

様々なサービスからの連絡がメールで行われたり、SMSでお知らせが届けられたりすることがあります。本物を騙った偽の連絡であるとそれを起因として個人情報を盗まれたり、金銭被害に繋がったりするおそれがあります。

●被害にあうタイミング

悪意があるメールやSMSを受信して、内容を閲覧した時点ではまだ情報を盗まれたり、端末がウイルス感染したりすることはありません。そのメールやSMSから誘導されたウェブサイトに情報を入力することで入力した情報が盗まれ、添付ファイルを開くことでウイルスに感染し、端末に保存されている情報が盗まれたり、端末が正常に動作しなくなったりしてしまいます。

●メールやSMS、SNSに関する注意事項

・安易にリンクやQRコードを開かない
・記載された電話番号に電話をかけない

●メール固有の注意事項

・画像をクリックやタップしない
　一見ただの画像であってもリンクになっていて、クリックやタップをすると偽のウェブサイトが開かれるおそれがあるので注意が必要です
・添付ファイルを開かない

●リンクやURLをクリックせずに確認する方法

メール内のリンクを疑い、リンク先について以下のようにして確認するとよいです。

①ウェブページを検索して開き、確認する
②あらかじめブックマーク(お気に入り)しておく
③あらかじめ正規のアプリをインストールしておき、そのアプリを使ってサービスを参照する

※1 情報セキュリティ10大脅威 2023 (IPA) (URL:https://www.ipa.go.jp/security/vuln/10threats2023.html)
※2 フィッシングの報告 (フィッシング対策協議会) (URL:https://www.antiphishing.jp/)
※3「情報セキュリティ対策の基本と共通対策 (PDF)」(URL:https://www.ipa.go.jp/files/000108841.pdf)