Ｐマークニュース

＜２０２３年新春号＞　Vol. ４２

株式会社トムソンネット　Ｐマークコンサルティンググループ

目 次 と 記 事 概 要

健康保険証機能を搭載したマイナンバーカード「マイナ保険証」に切り替える等、マイナンバーカードの利用に関する動きが活発化しつつあります。
前提となるマイナンバーカード（以下マイナカード）も、その普及策が奏功して申請ベースでは運転免許証を上回る約 8300 万枚、普及率 65.9%に達しています（2023.1.4 現在）。「マイナ保険証」は、健康保険証をマイナンバーで紐づけ、マイナカードの公的個人認証機能を利用します。以下では、利用拡大するマイナカードの公的個人認証機能の現状と課題について考察します。

先日(2023 年 1 月 25 日)に IPA(独立行政法人 情報処理推進機構)から「情報セキュリティ 10 大脅威 2023」が公表されました。この先 1 年間で特段に留意すべき脅威が挙げられています。その中で特に注目したいのは、「組織」の 10 位にランクインした「犯罪のビジネス化」です。闇サイト(ダークサイト)を使った事案で、被害者は企業に限りません。目下ホットな社会問題にもなっている広域強盗事件の“名簿”の情報源に、ダークサイト上の情報を利用している可能性が取り沙汰されています。
今回の事例に学ぶでは、「組織」の脅威を中心に俯瞰します。

昨年（2022 年）も個人情報漏えいに関する多くの事故が新聞紙面を賑わしました。個人情報漏えい事故の個々の内容を知ることも大切ですが、個人情報漏えいに対する注意喚起という側面からは、統計情報等により大勢を知ることが重要です。
斯かる観点から、東京商工リサーチが毎年公表している「個人情報漏えい・紛失事故」統計は大変有益です。調査対象が上場企業とその子会社に限定されてはいるものの、動向を知るうえで貴重な統計であり、記事ではその概要を採り上げました。併せて、2022 年に猛威を振るったサイバー攻撃事故状況にも触れました。

以上

１．マイナンバーカードによるオンライン個人認証
―　健康保険証の「マイナ保険証」への全面切り替え　―

2022.10.13 河野太郎デジタル相は、健康保険証を保険証機能搭載したマイナンバーカード「マイナ保険証」に切り替える旨を表明しました。全面的な実施は 2024 年秋が目途です。

一方、マイナンバーカード(以下マイナカードという)の普及も、その普及策が奏功して、運転免許証を上回る約 8300 万枚、普及率 65.9%に達しています(2023.1.4 現在)。

「マイナ保険証」は、健康保険証をマイナンバーで紐づけ、マイナカードの公的個人認証機能を利用しています。

以下では、利用拡大するマイナカードの公的個人認証機能の現状と課題について、「デジタルトラスト」にも触れながら、考察します。

（1）幅広いマイナカードの利用

マイナカードの利便性は下記のとおり、幅広いものがあります。

・マイナカード提示により、社会保障・税などの手続で、添付書類 が不要になり、マイナンバーの証明ができる。
・マイナカードにより、専用サイト「マイポータル」から子育てや介護等に係る行政手続きがオンラインで可能になる。
・確定申告も e-TAX を利用して簡素化が可能になる。
・コンビニで住民票の写しの受け取りが可能になる。
・マイナカードと交通系 IC カードを提携させた地方自治体による高齢者限定の運賃割引制度の導入も可能になる(前橋市の「マイタク」(2016.1.23 開始)など)。
・「アンドロイド」スマートフォンにカード機能を搭載(2023.5.11 開始)、 「アイフォン」への機能搭載についても協力を要請。(2022.12.25 岸田首相が米アップルのティム・クック CEO に)
・健康保険証として利用(2023 年秋目途に全面切り替え)。健診結果や予防接種歴、薬剤や医療費情報の確認が可能になる。
・運転免許証との一体化。(2024.年度末を目途に検討中)
・外国人の在留カードとの一体化。(2025 年度を目途に検討中)

これらの利用では、マイナカードの公的個人認証機能が使われています。

マイナカードによる公的個人認証は、簡単です。既に利用を開始している(2022.10.20 開始)「マイナ保険証」について、顔認証付カードリーダーを利用し、試してみました。

個人認証は、「顔認証」か「パスワード認証」(4 桁)かの選択になります。

「パスワード認証」ではマイナカード登録時に設定した「利用者証明用電子証明書」の 4 桁を入力します。「顔認証」の場合は、顔認証付カードリーダー画面の枠内に顔を近づけると、マイナカードに記憶された映像と照合され、認証されます。因みに、マスクをつけたまま、近づけてみると「マスクをはずしてもう一度・・・」のメッセージが表示されます。一連の認証は適切で、簡単且つスムーズに行われます。行政機関の窓口事務員が、運転免許証提示による認証で、運転免許証の顔写真と

「対面している本人」とを照合している場合より確実かもしれません。
「パスワード認証」では、パスワードを忘れてしまった場合や、記憶が不明確で入力ミスを3回連続するとパスワードロックが掛かり、当該電子証明が利用できなくなる場合があることを考えると、「顔認証」はかなり利用し易いものと言えます。

（2）マイナカードの公的個人認証機能

マイナカードでは、ICチップ内の**電子証明書**(信頼できる第三者（認証局）が間違いなく本人であることを電子的に証明するもので、書面取引における印鑑証明書に代わるもの)を用いて、個人の本人確認に必要な**「身元確認」と「本人確認(当人確認)」**を行っています。

マイナカードに記録されている電子証明書は、次の2種類です。

・**署名用電子証明書**（暗証番号が英数字6～16文字のもの）・・・インターネット等で電子文書を作成・送信する際に利用します（例　e-Tax等の電子申請）。「作成・送信した電子文書が、利用者が作成した真正なものであり、利用者が送信したものであること」を証明することができ、主体者(ランダム文字列＋受付窓口識別記号)、発行年月日、有効期間の満了日、発行者、シリアル番号が記憶されています。

・**利用者証明用電子証明書**（暗証番号が数字4桁のもの）・・・インターネットのウェブサイト等にログインする際に利用します（例　マイナポータルへのログイン、コンビニでの住民票の写し等の交付）。「ログインした者が、利用者本人であること」を証明することができ、氏名、生年月日、性別、住所、発行年月日、有効期間の満了日、発行者、シリアル番号が記憶されています。

利用者証明では、前述のとおり、「顔認証」か「パスワード認証」が選択できますが、使いやすいのは、「顔認証」です。顔認証では、「眼の周りが見えれば、顔の約7割の面積が隠れていても99.9%以上の精度で本人を見分ける」と言われています(2023.1.15日経報道)。

また、マイナカードによる「顔認証」のみが公的サービスでの「顔認証」として認められ、LINEアプリを使って住民票などの写しの交付を請求できるサービスについて、その適法確認請求は棄却されました（2022.12.8東京地裁)。判決では、ＬＩＮＥ申請では偽造された本人確認書類でも審査を通過する可能性があるとした上で、「不正の手段がひとたび確立されれば住民基本台帳制度の根幹への信頼が揺らぐことになりかねない」と指摘。厳格な本人確認は、行政のＩＴ化を推進するデジタル手続き法とも整合するとしました。

マイナカードを使ったeKYC(electronic Know Your Customerの略で、2018年の犯罪収益移転防止法の改正で認められた）は、国際基準に照らしても最高レベル(2022.12.8日経報道)だと言われています。

なお、総務省資料によれば、マイナカードは下記のとおり安全だと言っています。

・顔写真入りであり、対面での悪用は困難なため、「なりすまし」はできない。
・IC チップ部分には、プライバシーの高い個人情報は入っておらず、税や年金等の個人情報は記載

されていない。健康保険証として利用する場合でも、特定健診情報や薬剤情報などは入っていない。

・マイナンバーを見られても（マイナカードの裏面)、マイナカードを利用するには、顔写真付き本人確認書類(マイナカードの表面)などでの本人確認があり、個人情報の盗用等の悪用は困難である。

・紛失・盗難の場合は、24 時間 365 日体制で一時利用停止が可能である。

・アプリごとに暗証番号を設定し、一定回数間違うと機能がロックされる。

・不正に情報を読みだそうとすると、IC チップが壊れる仕組みとなっている。

（3）マイナカードの公的個人認証サービスの民間利用

デジタル取引では、①インターネット上における通信の相手が本人であり、なりすましをされていないことを確認できない。②またデジタルデータが改ざんされやすい。これを防ぐ「本人性の確認」と「電子署名、タイムスタンプ等による非改ざん性」を実現する**「デジタルトラスト」**が要請されます。

マイナカードの**公的個人認証サービス（JPKI）**は、この**「デジタルトラスト」**の一翼を担っています。マイナカードの「電子証明書」を利用することにより、オンラインによる本人確認のための公的サービスである**公的個人認証サービス（JPKI）**を利用することができ、公的個人認証サービスの民間利用が増加し、173 社(大臣認定事業者(プラットフォーム事業者)17 社、その事業者を利用している事業者は 156 社(2023.1.1 現在))となっています。その利用目的も多岐にわたっています。

オンラインでの金融口座開設、証券口座開設、生保本人確認、損保加入手続き(インターネット経由で加入できる一日単位の短期自動車保険、旅行保険、傷害保険など)、住宅ローンの契約手続きなど。

更にマイナカードの公的個人認証サービスを「電子署名法の認証業務を行う電子認証局」の電子証明書と紐づけた民間 ID の利活用があります。2022.10.21 にリリースされた**「めぶく ID」**(旧まえばし ID)です。「めぶく ID」は、前橋市の取組みで、マイナカードの本人確認を実施した上で、**スマートフォン上**に電子署名法の電子証明書を発行し、これをトラストポイント(インターネット上で行われる電子的な認証の手続きのために置かれる起点)とする仕組みです。

「スーパーシティ構想」(医療や交通、教育、行政手続きなど生活全般にまたがる複数の分野で、AI などを活用した最先端の技術を導入することで、便利で暮らしやすい街を実現しようとする構想)のために必要な個人の ID が「めぶく ID」であり、その活用によって、共助型未来都市をつくっていこうとするものです。

（4）マイナカードの課題と更なる期待

マイナカードは、デジタル社会に不可欠な**「デジタルトラスト」**の一翼を担う**公的個人認証サービス（JPKI）の提供手段として、またマイナ保険証**という全国民対象の業務に使用され、

「誰ひとりとして取り残されないデジタル化」の提供手段として期待されます。それゆえに課題も多くハードルは高いと言えます。

その普及である。マイナカードは、運転免許証を上回る約 8300 万枚、普及率 65.9%に達しているものの、医療機関・薬局での顔認証付カードリーダー(オンライン資格確認等システム)の導入は、9万６千台あまり(2023.1.15 現在)と対象の４割にすぎません。マイナ保険証対応の設備投資コストに耐えられない、診療所の構造を考えると改修不能だ、とごねる医師もいると言われますが、医療情報化支援基金による「顔認証カードリーダーの無償提供や、ネットワーク環境の整備などのそれ以外の費用の補助の拡充」もあります。

2023．4 までに全対象機関に原則として導入が義務付けられ、その導入が急がれます。一方、「普通の人々に保険証の切り替えを迫るのに行政の現場がのんびりしているように見える」という指摘があります(2022.11.18 日経)。厚生労働省がマイナンバーを使った情報照会システムの改定を行いましたが、2 割にあたる３７の自治体が他の機関への情報照会を全く行っていなかったという、会計検査院の調査結果からの指摘もあります。

また、全国民の利用を前提とした「使いやすさ」の課題も存在します。スマホによるマイナカード機能ができても、高齢者のスマホ利用には課題も多く、残念ながら、システムにとって、不可避の課題があります。

前述のようにマイナカードにかかわる技術的システム対応は、現在とりうる最善のものと言えるものの、運用面での想定外のヒューマンエラー、ワールドワイドで発生するセキュリティ犯罪等による「情報流失」などの課題がやはり残ります。

こうした課題を抱えながら、「マイナンバーカードを普及させ、その上にデジタル社会の夢を描かなければならない」(岸田首相 2022.12.26)。「デジタルを活用することは徹底してデジタルを活用することで、人間は人間が本来やるべきことに時間と力を使い、人が人に寄り添う、ぬくもりのある社会を実現する」(2022.12.1 河野デジタル相)ためにマイナカードへの期待は大きいものがあります。

現状は、マイナカードがもたらすデジタル社会の夢は「理解」しつつ、まだ「納得」にはかなりの距離があります。脳科学者は「理解」は理論・理性により導かれることが多く、「納得」は「わかった」と感じる経験・情緒により導かれることが多いと言います。

マイナ保険証の「納得」は、皆が利用して「にっこり」する当たり前の体験から得られることが予想されます。あるいは「納得」より「お得」からかも知れません。

「利用方法ごとに丁寧に説明して不安をきちんと払拭していく」為政者の努力と、我々の「理解」がなお一層必要と思われます。

２．事例に学ぶ：「情報セキュリティ 10 大脅威 2023」について

事例シリーズの第 18 弾です。

つい先日(2023 年 1 月 25 日)に IPA(独立行政法人 情報処理推進機構)から「情報セキュリティ 10 大脅威 2023」が公表されました。毎年の恒例ではありますが、この先 1 年間で特段に留意すべき脅威が挙げられています。

■「情報セキュリティ 10 大脅威 2023」

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

今回注目したいのは「組織」の 10 位にランクインした「犯罪のビジネス化」です。闇サイト(ダークサイト)を使った事案で、被害者は企業に限りません。目下ホットな社会問題にもなっている広域強盗事件の“名簿”の情報源に、ダークサイト上の情報を利用している可能性が取り沙汰されています。

それ以外で気が付くのは前年と順位に大差がないことではないでしょうか。とは言いながら、引き続く「Emotet」の蔓延等からマイクロソフト社を始め各社は懸命に対策を施しています。以下、「組織」の脅威を中心に俯瞰してみようと思います。

(1)脅威の因果関係

「脅威」は平板に列挙されていますが、一次事象→二次事象のように因果関係のあるものが見受けられます。

1 位の「ランサムウェアによる被害」は、3 位の「標的型攻撃による機密情報の窃取」から派生した事案が増えています。PC が使えなくなるだけでは済まず、情報の流出にも及び、被害(出費)が巨額に上ったケースもあります。今や世界で最も危険なマルウェアの 一つと言われる「Emotet」もランサムウェアを呼び込むこともあります。

2 位の「サプライチェーンの弱点を悪用した攻撃」の有名な事案に、2022 年 3 月に部品メーカのランサムウェア被害のため国内 14 工場が稼働停止になったトヨタの例があります。このこと自体問題ではありますが、発端は部品メーカの子会社へのサイバー攻撃との発表がありました。

取引先の情報セキュリティが脆弱な場合、侵入された PC からアドレス帳やメールそのものが搾取され本丸(標的)の企業や機関に“なりすまし”メールが送られます。受け取った側では差出人名、件名、本文がいかにも本物のメールに見えるため、添付ファイルや本文中の URL をついクリックして感染します。ダークサイトに個人や会社の情報が一旦アップされると、それを消すのはまず不可能です。消すことができないのであれば、それを悪用した手口に乗じないようにしましょう。

(2)マイクロソフト社の対応

マイクロソフト社(以下「MS」)は、1990 年代から Excel がウィルス蔓延の元になっていた関係で各種のマルウェア対策に取り組んできていますが、近年ではデフォルト(初期設定)として Office ソフト(Word、Excel 等)で以下のようしています。

①危険性のあるファイルを「保護ビュー」(読み取り専用)で開く

②インターネットからのファイル内のマクロ(VBA プログラム)の起動をブロックする

①②に該当するファイルを開いた際には黄色地の警告メッセージが表示されます。ここで、該当するのはメールの添付ファイルやサイトからのダウンロードファイル等です。

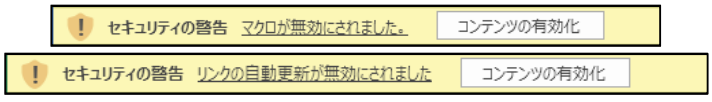
①のメッセージは以下のもので、既に目にしているでしょう。

「編集を有効にする」をクリックすると書き込みモードになります。痛し痒しですが、安全を期す余りこのままの状態にしておくと、インターネットからダウンロードする必要があるフォントが含まれていた場合に別のフォント(明朝体等)に置き換えます。結果、表示不能や文字化けが発生する可能性があります。

ファイルメニューの[オプション]から[トラストセンターの設定]で保護ビューの(後のマクロも同様)標準設定を変更できますが、お勧めする訳ではありません。

［トラストセンターの設定］

続いて、②のメッセージは以下の通りです。Emotet で有名になりました。



これらは Offce ファイルにマクロや外部参照が含まれていることを示しています。他の PC 等から複写して読み込んだファイルには以前からこのメッセージが表示されていましたが、インターネットからのファイルに対しては①のメッセージの後も表示され、広範囲にこの処置を行っています。

(3)Acrobat、ブラウザの対応

「PDF」の規格を開発したアドビ社は、「Acrobat」等がその脆弱性によりネットバンキングウイルス、ランサムウェアなどを蔓延させてきた経緯があり、頻繁にアップデート版がリリースされています。

先だっての 2023 年 1 月にも大きな更新がありました。PDF ファイルに添付ファイルを設定できることが主な要因となっており、Acrobat 及び Acrobat Reader での開封やダウンロードをブロックするブラックリストを更新した旨、アナウンスされています。

Google 社のブラウザ「Chrome」については、2022 年 6 月に警察庁から「Emotet の新機能として、Chrome に保存されたクレジットカード情報を盗み、外部に送信する機能が追加された」との発表があったり、2023 年 1 月に Imperva 社から「暗号資産のウォレットやクラウドプロバイダーの認証情報等の機密ファイルが盗まれる危険性がある」と警告される等、犯罪者の標的にされています。都度メジャーなアップデートを行っています。

MS は、Office 製品の他にもセキュリティ確保に注力しています。ブラウザの「Edge」では、怪しいサイトを開けないようやり過ぎと言えるくらいガードを堅くしていますが、2023 年 1 月に BSI 社から「電子メールで送信された添付ファイルを開かせることにより、攻撃者は Edge を介して悪意のある Web サイトをホストし、その Web サイトを閲覧するようにユーザを誘導する可能性がある」旨が公表され、急ぎバージョンアップを行いました。

イタチごっこの感が否めませんが、このように各社はサイバー攻撃への対応に注力しています。使用しているソフトの更新は大変重要です。

(4)まとめ

トヨタのケースでも見られるように、サイバー攻撃によるシステムの停止で複数の会社の実務に破綻を来す事案が目立ちます。元凶はダークサイトかもしれませんが、業務上で PC を利用している範囲(業務連絡が中心)では**大本を探ればメールに起因**すると言っても過言ではないでしょう。メール添付ファイルの開封、メールの誘導によるサイトの閲覧や識別情報(ID、パスワード)の入力には注意に注意を重ねる必要があります。

悪意のあるメールは差出人アドレスが不審な場合が多いのですが、この 2～3 ヶ月前から件名に「代理送信」の注釈があるものも出てきました。一見して差出人アドレスのドメインの不正を見破るのが難しくなり、本文にボタンが表示されているとついクリックしかねません。

しかし、受信した**メールを「テキスト形式」**(「HTML 形式」ではなく)で表示させることにより、ボタンの画像がジャンプ先の URL 文字列(http・・・)になります。文字列であれば、それをコピー&ペーストして「gred」等に安全性のチェックを委ねることができます。是非メーラー(メールソフト)の設定を見直していただければと念じて已みません。

また、Emotet は Office ファイルのみならず、Zip ファイルやショートカットファイルにも含まれるようになっています。Emotet の感染有無確認ツール**「Emocheck」によるチェック**と、併せて**各種ソフトの最新化**も定例的に実施・確認をしていただければ幸いです。

[参考例 1：HTML 形式表示]

[参考例 2：テキスト形式表示]

参考例 3：gred によるチェック結果]

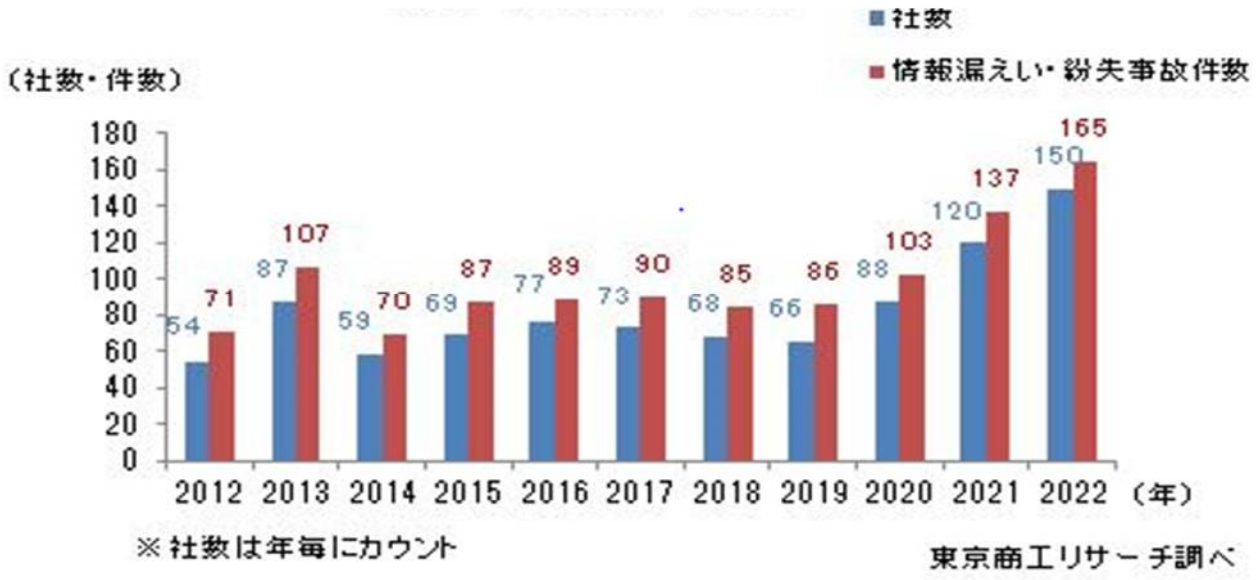
３．2022 年の個人情報漏洩事故状況について

（１）東京商工リサーチによる上場企業とその子会社における「個人情報漏えい・紛失事故」の 2022 年の実態統計から

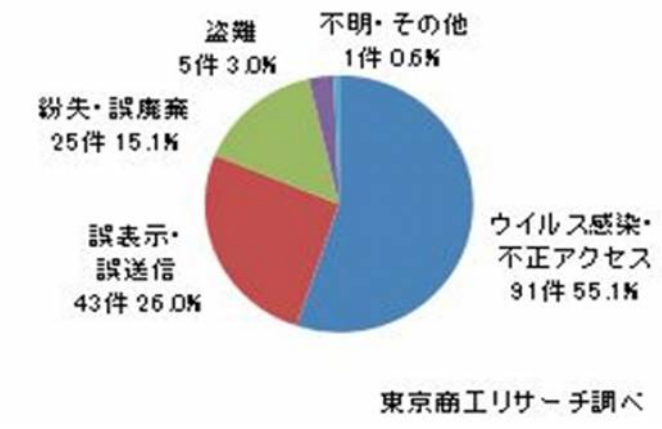
株式会社東京商工リサーチは、上場企業とその子会社における「個人情報漏えい・紛失事故」の集計調査を 2012 年から毎年行っており、今年も昨年（2022 年）の結果を公表しています。

昨年の事故件数は 165 件で、一昨年に続き 2 年連続して調査開始以来で最多になり、個人情報漏洩事故は増え続けています。以下では東京商工リサーチが公表した調査結果のポイントを見て行きます。

①2022 年の「個人情報漏えい・紛失事故状況」の概況



②情報漏えい・紛失事故の原因別割合について



情報漏えい・紛失事故 165 件を原因別に示したのが左図グラフです。

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、半数以上を占めました。

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ています。

このほか、保管しておくべき書類や取引記録の廃棄・紛失などの「紛失・誤廃棄」が 25 件（同 15.1%）、従業員が社内規定に反して個人情報を持ち出したりした「盗難」が 5 件（同 3.0%）となっています。

1 事故あたりの情報漏えい・紛失人数の平均は、「ウイルス感染・不正アクセス」が 8 万 9,978 人分と圧倒的に多くなっています。サイバー犯罪は、紙媒体が中心の「紛失・誤廃棄」（平均 1 万 1,922 人分）などに比べ規模が大きく、被害が広範囲に亘ることを示しています。

（2）2022 年で特筆すべきは「ウイルス感染・不正アクセスによる事故」の増勢

①東京商工リサーチの事故集計における、「ウイルス感染・不正アクセスによる事故」の状況

下図のグラフはウイルス感染・不正アクセスによる事故の年度推移です。グラフからも 2019 年以降の増勢振りが目につきます。

今回の東京商工リサーチの統計に於いては、「ウイルス感染・不正アクセスによる事故」の増加要因として 2022 年 2 月以降、マルウェア「Emotet」による感染が急拡大したことを挙げています。

【ウイルス感染・不正アクセスによる事故発生の年度別推移】

②増え続けるランサムウエア被害

また、昨年の「ウイルス感染・不正アクセスによる事故」を振り返るとき、前述の「Emotet」とともに猛威を振るったのが、「ランサムウェア」でした。

ランサムウェアに関する事故については、警察庁が被害集計を行っていますが、2022 年は 230 件の被害届が出されました。（2021 年は 146 件）警察庁は「ランサムウェアによる攻撃は引き続き活発に行われている」とのコメントを出しています。

昨年の「ランサムウェア」被害も企業や団体の規模を問わずでており、社外から社内のネットワークに接続する VPN 機器や、職場のパソコンを遠隔操作するリモートデスクトップから侵入されるケースが引き続き多く、警察庁ではパソコンの OS や VPN 機器を最新のものに更新するなど、システムの脆弱性を埋める対策をとることを呼びかけています。

４．お知らせ（トピックス）

（１）マイナンバーカード申請が１月上旬に約８３００万枚と運転免許証を超える

年初早々マイナンバーカードの発行申請件数が、運転免許証を超えたことが報道されました。

総務省が毎月発表しているマイナンバーカードの全国統計の交付枚数は、直近では下表の推移を辿っており、その急増振りが窺えます。

時期	交付枚数	交付枚数率	備考
2023/01/31	75,663,329 枚	６０．１％	
2022/11/30	67,846,028 枚	５３．９％	2022 年 10 月 18 日に 50%を超えました。
2022/09/30	61,657,397 枚	４９．０％	
2022/07/31	58,151,191 枚	４５．９％	
2021/12/31	51,871,720 枚	４１．０％	2022 年末の状況。

（２）2022 年の保険代理店における P マークの新規取得は 11 社

保険代理店の P マーク新規取得件数は、一時期（２、3 年前）低水準で推移しましたが、2021 年から持ち直し、昨年は、2021 年と並ぶ 11 社が新たに P マークを取得しました。

この結果、昨年末時点で P マークを取得している保険代理店数は 133 社になりました。

以上

Ｐマークをはじめとして各種ご相談は下記で承っています。ご気軽にどうぞ！

連絡先　　株式会社トムソンネット　（https://www.tmsn.net/）
〒101-0062 東京都千代田区神田駿河台４－６　御茶ノ水ソラシティ１３階
電話　03-3527-1666　　FAX03-5298-2556

担当:　岩原 秀雄（Mail：iwaharahi1017@tmsn.net）　　平泉 哲史（Mail：s.hiraizumi@tmsn.net）
　　本間 晋吾（Mail: s.honma@tmsn.net）