Ｐマークニュース

＜２０２３年盛夏号＞　Vol. ４４

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

健康保険証のマイナンバーカード「マイナ保険証」への全面的切替えを予定する2024年秋を前に、多くのマイナンバーカード・トラブルが報道され、2023.7.19個人情報保護委員会によるデジタル庁への立ち入り検査も実施されました。マイナンバーカード(以下マイナカードという)の普及は、運転免許証を上回る約9360万枚、普及率75.3%に達しています(2023.7.16総務省HP)。一方、マイナカード返納騒ぎもおこっています。マイナカード・トラブルについて、その投げかけた課題を考察します。

パスワードは、電子データの授受等における代表的セキュリティ手法であり、パスワードに関する種々の考え方や方法論が示されています。そこで今回の「事例に学ぶ」では、みなさまに適切なパスワード運用を図って戴くために、「パスワード窃取（が窃取される）方法」、「パスワード設定のヒント」、「パスワード更新の功罪の経緯」、「パスワードの(定期)更新は“悪手”か」といった切り口からそれぞれの問題を解説し、安全なパスワード作りを提案しています。記事では最後に、例え1文字だけの変更であっても、1年に1回はパスワードを更新することをお勧めしています。

昨今のランサムウェアに代表される不正アクセスの猛威は、未然に防ぐ事前対策の難しさとともに、セキュリティインシデントが発生してしまった場合の被害を最小限にとどめる対応を準備しておくことの必要性を痛感させられます。

被害を最小限にとどめ、企業の信用を保つために、セキュリティインシデント対応はすべての企業が準備しておくべき重要事項であり、経営課題といえます。本誌では、以前（2022年爽秋号）もセキュリティインシデント発生後の対応を採り上げましたが、改めて対応のポイントを整理しました。

以上

１．マイナンバーカード・トラブルの投げかけた課題
―「自分ごと」としての個人情報管理をー

健康保険証のマイナンバーカード「マイナ保険証」への全面的な切り替えが予定される、2024年秋を前に、多くのマイナンバーカード・トラブルが報道され、2023.7.19 個人情報保護委員会によるデジタル庁への立ち入り検査も実施されました。マイナンバーカード(以下マイナカードという)の普及は、運転免許証を上回る約9360万枚、普及率75.3%に達しています。(2023.7.16総務省HP)。半面、マイナカード返納騒ぎも一方で起こっています。そこで今回は、マイナカード・トラブルについて、その投げかけた課題を考察します。

（1）発生しているマイナカード・トラブルとその原因
(個人情報保護委員会 2023.7.19 資料から抜粋)

a）コンビニでの住民票等誤交付

・住民票の写し等の証明書を取得する「コンビニ交付サービス」において、別人の又は本人により廃止済みの証明書（特定個人情報又は保有個人情報を含む。）を誤交付した。（令和５年５月 30 日～31 日、地方公共団体４団体（横浜市、足立区、川崎市、徳島市)、令和５年７月３日、宗像市）

・原因は、 開発にあたった富士通関連会社のシステムミス(令和５年５月 30 日～31 日の事案）、またその後の修正システムの更新未実施(令和５年７月３日の事案)

b）－１ 各種サービスにおけるマイナンバーの紐付け誤り（健康保険証）

・複数の健康保険組合等（個人情報取扱事業者）において、被保険者とは別人のマイナンバーを誤登録し、マイナポータルやオンライン資格確認システムを通して別人に医療情報等（個人データを含む。）を漏えいした。

・原因は、地方職員共済組合が、年金支給対象者を個人番号管理システムに登録する際、基本４情報（氏名、生年月日、性別、住所）を確認してマイナンバーを特定することとなっていたが、その徹底を怠っていたため。

b）－２各種サービスにおけるマイナンバーの紐付け誤り（年金記録）

・地方職員共済組合（個人情報取扱事業者）において、年金請求の手続時に、請求者とは別人のマイナンバーを誤登録し、マイナポータルを通して別人に年金記録等（個人データを含む）を漏えいした。

・原因は、地方職員共済組合が、年金支給対象者を個人番号管理システムに登録する際、基本４情報（氏名、生年月日、性別、住所）を確認してマイナンバーを特定することとなっていたが、その徹底を怠っていたため。

b）－３各種サービスにおけるマイナンバーの紐付け誤り（障害者手帳）

・地方公共団体（静岡県、宮崎県、鳥取市）において、障害者手帳の情報とマイナンバーの紐付けを行う際に、対象者とは別人のマイナン バーを誤登録し、マイナポータルを通して別人に障害者手帳の情報（保有個人情報を含む）を漏えい又はそのおそれが発生した。

・原因は、静岡県が、障害者手帳の情報をマイナンバーと紐付けて障害者手帳管理システムに登録する際、基本４情報（氏名、生年月日、性別、住 所）の確認が不十分であった。
また、宮崎県及び鳥取市においては、誤登録を防止するために必要な確認手順又は運用に不備があったため。

ｃ）－１公金受取口座等の誤登録(公金受取口座（マイナポータル））

・各地方公共団体の支援窓口における本人又は手続支援員による操作ミス（ログアウトの失念）に起因する公金受取口座の誤登録等により、別人のマイナンバーと本人の銀行口座情報を誤って紐付けた結果、銀行口座情報（保有個人情報を含む）を漏えいした。

・原因は、デジタル庁が、公金受取口座の登録等に関する事務において各地方公共団体の支援窓口の共用端末を利用するに際して、正確な操作手順の徹底のほか、操作手順に伴うリスクの軽減等について、リスク管理及びその対策ができていなかったため。

ｃ）－２公金受取口座等の誤登録（国税庁 確定申告時）

・確定申告書の登録時に銀行口座情報を公金受取口座に登録を希望した者について、国税庁がデジタル庁に情報提供をした際、登録希望者のマイナンバーと別人の銀行口座情報を誤って紐付けた結果、銀行口座情報（保有個人情報を含む。）を漏えいした。

・原因は、国税庁が、デジタル庁に情報提供した銀行口座情報について、誤登録を防止するために必要な確認手順又は運用に不備があったため。

ｃ）－3公金受取口座等の誤登録(マイナポイント)

・各地方公共団体の支援窓口における本人又は手続支援員による操作ミス(ログアウトの失念)に起因するマイナポイントを受領する決済サービス情報（保有個人情報を含む）の誤登録等により、マイナポイントの誤交付又はそのおそれが発生した。

・原因は、デジタル庁が、公金受取口座の登録等に関する事務において各地方公共団体の支援窓口の共用端末を利用するに際して、正確な操作手順の徹底のほか、操作手順に伴うリスクの軽減等について、リスク管理及びその対策ができていなかった。

（２）共通する基本的な課題

①個人情報の分散管理　欧州各国の番号制度はナンバーによる一元管理が主流ですが、日本では一元管理を回避して分散管理しています。このため、「紐づけ」という作業が必要です。分散管理に至ったのは、住民基本台帳ネットワークでの「プライバシー権侵害違憲裁判」での最高裁判断による所が大きく、裁判は合憲としましたが、「行政事務で扱う個人情報を一元管理できる主体が存在しない」こととという条件がついているため、分散管理としたのは、妥当な判断と考えます。

②「紐づけ」の難しさ　何の個人情報をもとに、異なるファイルに記録された個人情報を同一人のものと判断する難しさがあります。氏名漢字とフリガナによる判断としても、マイナカード上にはフリガナの表記はありません。金融機関口座はカナ氏名のみで漢字の表記がありません。戸籍謄本は、2023 年の戸籍法改正によりフリガナを追加しましたが、これ以前は漢字表記のみでフリガナの表記はありません。その漢字にフリガナを付すのも難題です。例えば女子プロゴルファーの山下美夢有(みゆう）岩井双子姉妹千怜(ちさと)と明愛

(あきえ)など、興味のない人は即座に読めないと思われます。フリガナだけから漢字を探すのも難題です。「サイトウ」姓は、漢字では 50 種類あるのではと言われています。
されば、「漢字氏名＋フリガナ＋生年月日」では、どうか？　さすがにこの条件では、該当個人は特定される確率は高いのですが、最近の事故事例では、この 3 要素が同一の別人がいて、誤って「紐づけ」されたという事例も報告されています。

従来こうした判断は、他の種々「アナログ」情報を加味して、担当者が個別に判断し、処理されてきたと思われます。しかしながら、デジタルでの「紐づけ」は、設定されたルールでのみ処理され、随時に「アナログ情報」を加味することがありません。デジタライゼーションの進行する社会にあって、デジタルで個人を特定し識別していくためには、克服しなければならない関門であり、各人がデジタル社会に対する覚悟として、意識し取り組まなければならない難問でもあります。

③今回のトラブルでは、健康保険組合等（個人情報取扱事業者）地方職員共済組合（個人情報取扱事業者）地方公共団体　国税庁等の組織体におけるオペレーション・ミスが原因と思われるトラブルが多く発生しています。各組織体における正確な操作手順の徹底、誤登録を防止するために必要な確認手順又は運用の不備も指摘されています。各組織体における情報処理人財の不足も指摘される中、デジタルに対する組織体全体の「対応能力不足」の感も否めません。静岡県でのトラブルでは、担当者が 1 名であったとの情報もあります。

（3）公的個人認証機能を持つマイナカードへの期待

進む少子高齢化社会にあって、デジタルの利用による利便性の拡大・効率化は必須です。行政の利便性の拡大・効率化も然りです。調査報告では、世界の行政デジタル化ランクでは日本は、14 位(韓国は 3 位)と立ち遅れています。

こうした状況下にあって、マイナカードを安全に確実に利用していく運用は不可欠です。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。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)」**を行っている。こうした機能を持つマイナカードを安全に確実に利用し運用していく事が必要なのです。

この公的個人認証機能を利用してマイナカードは下記のとおり、幅広く拡大しています。

・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)、 「i-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 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)

（4）マイナカード・トラブルへの対応

デジタル社会における個人情報保護の施策として、「P マーク制度」が主として企業向けであるに対して、「マイナカード」の施策は、全国民向けと考えられます。デジタル社会で個人情報を保護し、施策を推進するために、マイナカードを安全に確実に運用していく努力・取組が必須となります。

政府は、相次ぐトラブルに対応するため、「マイナンバー情報総点検本部」を設置し、マイナポータルで個人が確認できる 29 項目の情報に対して誤登録かいなかを洗い出し、7 月末までに 3600 の行政機関に紐づけ作業の状況を聞き取り、誤りのおそれのある機関に今秋までに全データの調査や登録の修正を求めるといわれています。

また、個人情報保護委員会は、独立の監督官庁として、2023.7.19 にデジタル庁が管理する「公金受取口座登録制度に基づくシステム」に立ち入り検査し詳しく調べることとしていました。一方、マイナカード・トラブルの現象をとらえて、「マイナカード返納」を促す主張があります。

この主張では、デジタル社会の個人認証を何によって安全確実に確立するのでしょう。

マイナカードの機能をいかなる方法で、代替しょうと言うのだろうか。現象だけを捉えて手段の本旨を求めず、話題として仕立て上げる集団やジャーナリズムがあるのはさびしい思いです。個人認証を伴うこうした政策を展開する国々のなかで、「絶対に批判もできなく反対のできない権力国家」があります。一方で、わが国のように、多くの難点を指摘し、それらを暴いて自由に報道される社会は、民主的で健全だと思われます。ただ、その難点だけをとらえて「イチかゼロ」かの論理で排除しようとする主張には「危なさ」を感じます。

少子高齢化社会を迎え、デジタルで対応できる事は、デジタルへの転換が望まれます。しかしながら、いくつかの克服すべき難関があります。前述の「紐づけのむずかしさ」「デジタルに対する組織体全体の対応能力不足」は、そのなかでも極めて難関な課題と思われます。

この「アナログの壁」の克服には、**我々一人ひとりの努力と覚悟**も必要です。アナログ情報の幾つかをデジタルへ転換する努力と覚悟です。多くの人が、マイナカードで検索できる自分の個人情報を確認しているだろうか？　自分の個人情報が正しく登録されているか確認しなくて良い？　個人情報保護には、まず自分の個人情報の登録内容を把握しなくてはなりません。自分で確認することが基本です。行政が実施したことで、自分と関係ない？　自分の個人情報です。「他人ごと」ではありません。「マイナポータル」を利用して自分で確認するか？　市役所などでの本人による「確認」をサポートする手段も利用して確認するか？　マイナカードの安心・確実な運用を**「自分ごと」**として前進させたいものです。

２．事例に学ぶ：「パスワード」の設定について

事例シリーズの第 21 弾です。今回は『「パスワード」の設定』について検討してみたいと思います。前回紹介しました「情報セキュリティ 10 大脅威」では毎年のように標的型攻撃やランサムウェアが上位を占めます。いずれもアカウント情報・ログイン情報の窃取やフィッシングサイトへの識別情報の入力がトリガーになります。煎じ詰めればパスワードが窃取されたか、意識の有無に関わらず先方に通知してしまったか、です。

8 年前になりますが、同じテーマで検討したことがありました。その中では「パスワードは最長でも 6 カ月ごとに更新」するようお勧めしていますが(その後政府方針により撤回)、ここで見直しをしてみようと思います。

(1)パスワード窃取の方法

「情報セキュリティ読本(六訂版)」(IPA)でパスワードの窃取の方法が以下のように紹介されています。(筆者要約)

方法	説明
①ブルートフォース攻撃	特定の ID に対し、全ての文字を組み合わせて(いわゆる“総当たり”で)ログイン(解読)を試みる
②リバースブルートフォース攻撃	複数の ID に対し、全ての文字を組み合わせてログイン(解読)を試みる
③辞書攻撃	人名や辞書に載っている単語やよく使われそうな文字列を用いてログイン(解読)を試みる
④パスワードリスト攻撃	攻撃者が事前に入手してリスト化した ID とパスワードを組み合わせてログイン(解読)を試みる

これらの方法の中で文字数が極端に短い場合を除き①、②は現実的ではないと考えます。何故なら、英数字 6 桁で 21 億通り以上、8 桁で 2 兆 8000 億通り以上の組み合わせがあります。ログインを試みてパスワードが不一致とのレンスポンスを得るのに各回ある程度(ミリ秒レベルでしょうが)の時間を要し、それを何億回も繰り返すには年単位でかかるためです。

ブルートフォース攻撃のイメージ
引用：株式会社セキュアオンライン HP

③④は「説明」にあるように一般に使われている言葉や本人の公開されている固有情報を元にパスワードを生成しログインを試みます。上記のように、ブルートフォース攻撃では途方もない時間を要す可能性があるため、③④と①②の組み合わせることにより“リーズナブル”な時間内でログインに成功し窃取に至るものと推測します。

(2)パスワード設定のヒント

前項をベースにすれば、“ありふれている”や“簡単に推測される”、“単語を含んでいる”等のパスワードを避けることです。既にご存知のように、“123145678”等が“ありふれている”に該当し、氏名や生年月日、電話番号等本人の公開(或いは既知)情報の文字列を含んでいるのが“簡単に推測される”です。“単語”はずばりそのもので、“password”等もその部類です。

これらは覚えやすいことから使いたくなります。使用するのであれば**間に**(決して“前後”ではなく)**特殊文字をいくつか(1 文字でも)挿入して 10 文字以上に**する等のひと手間を加えまし

ょう。文字の挿入場所の候補は母音の前や連続した子音の間で、要は“読めない”ようにすることです。

(3)パスワード更新の功罪の経緯

パスワードの“定期更新”は数年前まで各企業において半ば義務とされていました。「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(2014 年)に“パスワードの有効期限の設定”があり、定期的な更新を促しています。プライバシーマーク審査のチェック項目の一つにも“パスワードの定期更新が行われていること”がありました。

所が、2017 年に米国 NIST が発表した「NIST Special Publication 800-63B」の中でパスワードについて“**サービスを提供する側がするべきでない**”としている事項に以下のようなものがあります。

・大文字、小文字や特殊文字、桁を一定数必要とするパスワードの複雑さの要件を設定
・パスワードに有効期限を設定

これを受けた総務省の方針や JIPDEC の「JIS Q 15001-2006 をベースにした個人情報マネジメントシステム実施のためのガイドラインー第 2 版」(2018 年)で“パスワードの有効期限を設定していること”が削除されました。NIST の提言は現在でも活きています。

(4)パスワードの(定期)更新は“悪手”か

重要なのは、パスワードを変更する行為(加えて定期的な更新)そのものが危険な訳ではないと言うことです。国民のための情報セキュリティサイト(総務省)では「**定期的な変更のみを(社員に)要求**することで、パスワードが単純化したり、ワンパターン化したり、サービス間で使い回しするようになることの方が問題となります。」と説明しています。要すれば、定期的な更新を義務化することによって“面倒だ”“煩わしい”と思わせることが問題なのです。

Windows 系の運用管理システム「Active Directory」でも標準を“42 日”としているように、パスワードの**“定期更新”はできる限り実施するべき**と思います。期間は 1 年が適当と考えます(半年ではやや厄介か)。Google Chrome にオートコンプリート用に保存されたクレジットカード情報が窃取された事案があるように、1 年もすると無意識の使い回しやブラウザへの登録が避けられないと考えるからです。

(5)まとめ

パスワードの設定は情報セキュリティの論を俟たない重要事項です。多要素認証を採用しているサイトも増えていますが、PC 利用の場合ログインの度にスマホの併用が必須になったりして利便性に問題があるため、引き続き ID とパスワードだけで利用している人が多いのではないでしょうか。類推されやすい文字列であってもひと味加えれば OK 等、ハードルを下げても 1 年に 1 回パスワードを更新することをお勧めします。

殆どの P マーク事業者さんではパスワードの定期更新をルール化していないと思われますが、従業者の皆さんが**“自発的に”更新**するのを禁止している訳ではないでしょう。セキュリティリテラシーの維持・向上のため、一人ひとりが意識を持って更新されることを期待します。

３．セキュリティインシデント対応再考

昨今のランサムウェアに代表される不正アクセスの猛威は、未然に防ぐ事前対策の難しさとともに、セキュリティインシデントが発生してしまった場合の被害を最小限にとどめる対応を準備しておくことの必要性を痛感させられます。

セキュリティインシデント対応とは、文字通りセキュリティインシデントが発生した際に行う、応急処置や調査、公表、恒久対応などのことです。セキュリティインシデントは、重大な問題に発展しうるセキュリティ上の事件や事故を意味する言葉で、外部からの攻撃や内部不正・不注意、自然災害などさまざまな要因で発生する可能性があります。

近年は急速な情報化の進展により、どの企業もセキュリティインシデントと無縁ではいられません。未然に防止する対策に加え、セキュリティインシデントが発生した場合に備えた準備や適切な対応ができるようにしておくことが非常に重要になっています。

（1）セキュリティインシデント対応の重要性

セキュリティインシデントに対して適切に対応することは、企業を守り、安定的な経営を進める上で欠かせません。セキュリティインシデントが発生してしまった場合に、迅速に適切な対応が行えるよう準備しておくことが、防止策と並んで非常に重要です。

迅速かつ適切にセキュリティインシデントに対応できなかった場合、社内外の被害拡大、問題の複雑化、企業の信用失墜、業績への影響などさまざまな部分で事態の悪化を招くことが懸念されます。被害を最小限にとどめ、企業の信用を保つために、セキュリティインシデント対応はすべての企業が準備しておくべき重要事項であり、経営課題といえます。

（2）セキュリティインシデントへの対応ステップとその内容

セキュリティインシデントが発生した場合に被害を最小限に留めるためには、手際よく対応することが必須です。そのためには、事前に対応手順（ステップ）とそのステップでの対応内容が詰められ、関係者がそれを共有していることがポイントです。

基本となる対応ステップと各ステップにおけるポイントは以下の通りです。

基本ステップ	各ステップにおける対応内容	備考（留意事項）
１．事前準備	インシデントの発生を想定して、発生時に備えて対応する組織、指揮する人、対応の流れなどを整備して、トップマネジメントの承認を得て社内に周知します。	システム部門だけでなく他部門も巻き込んで対応する必要がある場合は、準備段階から他部門に周知しておくことが重要です。 また、定期的にセキュリティインシデントを想定した対応訓練（例:バックアップの戻し訓練等）を実施することが、実際に発生した際の迅速な対応に繋がります。

２．検知・報告	セキュリティインシデントの兆候に気づき、報告するステップです。 インシデントを最初に検知する場面には次のようなものがあります。 ①システムで外部からの不正アクセスが検知された。 ②メールを誤送信してしまった顧客から個人情報流出を疑う相談があった。等々 インシデントが発覚した際には、速やかに定められた報告ルートに沿って、社内のみならず、委託先等の関係先にエスカレーションすることが大切です。	報告の遅れや事実の隠蔽は、適切な対応を妨げ、被害の拡大を招きます。 事前に報告ルートを定めておくことに加え、インシデントの発生を隠蔽しない、報告しやすい職場環境を築いておくことも重要です。
３．応急処置	セキュリティインシデントの発生が報告されたら、関係者による対策チームを組成し、被害の拡大を防ぐための応急処置にあたります。 応急処置はスピード感を持って対応することで、被害の拡大を防ぐことが重要です。	外部からの攻撃の場合は、ネットワーク遮断、マルウェアの駆除、ログ確保、情報流出有無の確認などです。 内部起因の場合には、当事者への事実確認、情報流出先の特定、二次被害を防ぐ対応などを行います。 上記のうち、ネットワーク遮断など予め手順を定めておくことが出来るものは、文書化しておくことがスピーディな対応に繋がります。
４．調査	被害の拡大を食い止める応急処置が済んだらより詳細な原因及び影響調査を行います。 ログの追跡や被害状況の確認、関係者への聞き取りなど、インシデントの内容に応じて必要な調査を行います。	外部攻撃の場合には、セキュリティ専門会社などを交えた調査も有効です。 インシデントに応じたセキュリティ専門会社のリストを整備し、調査内容を確認しておきます。
５．通知・公表	インシデントの影響が社外に及ぶ場合には、被害者や、二	インシデントの内容によっては、関係当局や警察、IPA（情報処理推進機構）

	次被害の可能性がある先に通知します。被害が広範囲に及ぶ場合には、ホームページへの情報掲載やマスコミへの公表も必要です。	などへの報告も必要です。 問い合わせ窓口の設定は、顧客や取引先の不安を和らげます。
６．恒久対応	応急処置では被害の拡大を防ぐための暫定的な対策を行いましたが、調査によってインシデントの全貌が判明したところで、本格的な対策を行います。	システム的な対応に加えて、外部への適切な情報公開により対応状況を周知することも重要です。 外部からの攻撃であれば、不正なアクセスの侵入経路を塞ぐ対応や、セキュリティ対策ソフトの導入などを行なった上で、遮断や停止していたシステムを再開します。
７．再発防止・事後対応	インシデント対応が一区切りしたあとは、再発防止策を整理します。 対策チームが中心となって、再び同様のインシデントが発生しないように、根本的な原因を追求して対策を打ちます。	再発防止策としては、例えば、セキュリティ対策ツールの導入や、情報持ち出しルール見直し、従業員へのセキュリティ教育の強化などが挙げられます。 また、インシデント対応フローの有効性についても振り返り、改善点があれば見直します。

上表に１．～７．までのポイント事項を記述しましたが、自社において「セキュリティインシデント対応」を本格的に取り纏める場合は、さらに実用性を高めるために、「対策チームのメンバー構成及び責任者」や「ネットワーク遮断、マルウェアの駆除、ログ確保、情報流出有無の確認の具体的手順と実施者」さらに「外部攻撃の場合には、セキュリティ専門会社のリスト」などを文書化し、それを必要性に応じてメインテナンスして行くことが需要です。

最後に、「セキュリティインシデント対応」を作成し、社内に周知することの重要性は、インシデント発生時の迅速な対応により被害を最小限にと止める効果の他に、全社にインシデントの発生は自社にとっては無縁といった考えを否定するもので、常にインシデント発生の可能性を意識することで、日常業務に対して緊張感をもって行うという最大のインシデント対策に繋がるものと考えます。改めて御社のインシデント対策をご確認ください。

４．お知らせ（トピックス）

（１）JIPDEC から 2022 年度の P マーク付与事業者における個人情報の取扱い事故報告集計が公表されました。

JIPDEC から 7 月下旬に 2022 年度における P マーク付与事業者からの「個人情報の取扱いにおける事故報告の集計」が公表されました。

2022 年度の事故報告は、保護法改正に伴う「速報」「確報」の義務化が施行された直後の集計であり注目されましたが、概要は下記のとおりです。

①事故報告件数

年度	報告事業者数（社）	事故報告件数	備考
2022 年度	1,460 社	7,009 件	内速報 1,878 件
2021 年度	1,045 社	3,038 件	

②うち「速報」事故報告件数と内訳

速報理由	件数
要配慮個人情報	983 件
財産的被害	478 件
不正の目的	300 件
1,000 人超	117 件
合計	1,878 件

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。お気軽にどうぞ！

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）