Ｐマークニュース

＜２０２４年爽秋号＞　Vol. ４９

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

今年度は、個人情報保護法の 3 年毎見直しが行われています。
令和 7 年(2025 年)改訂予定の直しの検討として、その検討中間整理が公表されました。中間整理では、特に、個人の権利救済手段の在り方(団体による差止請求制度や被害回復制度)、課徴金については、事業者、個人それぞれに与える影響が大きく、今後とも一層の意見集約作業が必要と考えられることから、令和 6 年（2024 年）末までを目途に議論を深めていくとしていますが、検討結果が未公表であるため、今回は、中間整理のなかで、興味深い「漏洩等報告・本人通知の在り方など」「こどもの個人情報に関する規律の在り方」について概観します。

今回は“持ち出し PC”の留意点がテーマです。背景は、警視庁が毎年のように更新し公表している「マルウェア『ランサムウェア』の脅威と対策（脅威編）」で“ランサムウェアの感染経路については、VPN 機器やリモートデスクトップ（NW 機器）からの侵入が全体の 83%を占めている”とされています。
対策として挙げられているのは PC やサーバの OS のアップデート等基本的な事柄で、至極当然のことです。NW 機器から侵入されただけでは自社としては問題なく、データやプログラムが格納されている PC 等が侵されて初めて被害になります。特に会社のセキュリティポリシーの管理下を離れた持ち出し PC に危惧を抱きますので、管理上の留意点を纏めました。

Windows 10 はバージョン「22H2」が最終バージョンになります。
Windows 10 は 2022 年 10 月 18 日に、バージョン 22H2 への更新が始まり、2023 年 4 月 27 日にこの 22H2 が最終バージョンとなることが発表されています。
今後は特別な事が無い限り新機能は追加されず、バグ修正やセキュリティ更新のみのサポートとなります。

１．漏洩等報告・本人通知の在り方など(個人情報保護法改訂／中間整理　その 2)

―あわせて「こどもの個人情報に関する規律の在り方」について―

今年度は、個人情報保護法の 3 年毎見直しが行われています。

令和 7 年(2025 年)改訂予定の直しの検討として、その検討中間整理が公表されました。

中間整理では、特に、個人の権利救済手段の在り方(団体による差止請求制度や被害回復制度)、課徴金については、事業者、個人それぞれに与える影響が大きく、今後とも一層の意見集約作業が必要と考えられることから、令和６年（2024 年）末までを目途に議論を深めていくとしていますが、検討結果が未公表であるため、今回は、中間整理のなかで、興味深い「漏洩等報告・本人通知の在り方など」「こどもの個人情報に関する規律の在り方」について概観します。

（１）「漏洩等報告・本人通知の在り方など」について（中間報告では、現状を下記としています）

・令和２年改正法の施行により、令和４年度（2022 年度）から漏えい等報告が義務化されたこと等により、漏えい等報告の件数は増加しており、令和５年度（2023 年度）は 12,120 件の報告がありました。

・個人データに係る本人の数が１人の事案としては、病院や薬局における要配慮個人情報を含む書類の誤交付又は紛失や、クレジットカードの誤送付などが多くなっています。

・要配慮個人情報を含む事案は、全体の 89.7%を占めています。

この現状をふまえての提言は下記となっています。

「漏えいした個人データに係る本人の数が１名である誤交付・誤送付案件が大半を占めているが、このようなケースは、当該本人にとっては深刻な事態になり得るものであり、本人通知の重要性は変わらないものの、本人通知が的確になされている限りにおいては、委員会に速報を提出する必要性が比較的小さい。また、漏えい等又はそのおそれを認識した場合における適切な対処（漏えい等が生じたか否かの確認、本人通知、原因究明など）を行うための体制・手順が整備されていると考えられる事業者については、一定程度自主的な取組に委ねることも考えられます。

そこで、例えば、体制・手順について認定個人情報保護団体などの第三者の確認を受けることを前提として、速報については、一定の範囲でこれを免除し、さらに「漏えいした個人データに係る本人の数が１名である誤交付・誤送付案件のようなケース」については確報について一定期間ごとの取りまとめ報告を許容することも考えられる。」

現状を踏まえての、妥当な歓迎すべき提言となっています。

（２）「こどもの個人情報等に関する規律の在り方」（中間報告では、現状を下記としています）

・ 現行法上こどもの個人情報の取扱い等に係る明文の規定は基本的にない。

・こどもの個人情報等に関する社会的反響が大きかった事例が見られる。全寮制の学校において、全生徒にウェアラブル端末を購入してもらい、心拍数、血圧、睡眠時間、入退室履歴等を把握し、生徒の健康管理に役立てる取組を実施することが報道された事例がありました。

・また・別の学校では、生徒の手首に装着した端末で脈拍を計測して、授業中の集中度を測定する実証研究を行い、教員がそのデータを基に授業の振り返り等に活用していた事例がありました。
・委員会においては、令和６年（2024 年）２月に、大手学習塾に対して、大量の児童の個人データを保有及び管理しているにもかかわらず、その管理が不十分であり、必要となる安全管理措置を講じるよう、指導を行いました。
・「個人情報保護法相談ダイ」では、事業者において第三者提供や目的外利用等本人の同意が必要な行為を行う予定がある際に、法の規定上は「本人の同意」が必要とあるが、本人が未成年である場合にはどう対応すればよいのか、といった事例が挙げられます。
・このほか、見知らぬ事業者によるこどもの個人情報等の利用を不安視する相談や、こどもの個人情報等の開示や削除の依頼をしているにもかかわらずこれに応じない事業者に関する相談もあります。　こうした現状認識のもと、下記を提言しています。

（１）主要各国においてこどもの個人情報等に係る規律が設けられており、執行事例も多数見られることも踏まえ、こどもの権利利益の保護という観点から、規律の在り方の検討を深める必要がある。

（２）a：法定代理人の関与　現行法上、原則として本人同意の取得が必要とされている場面において、こ どもを本人とする個人情報について、法定代理人の同意を取得すべきことを法令の規定上明確化することを検討する必要がある。また、本人に対する通知等が必要となる場面においても、こどもを本人とする個人情報について、法定代理人に対して情報提供すべきことを法令の規定上明文化することを検討する必要がある。

ｂ：利用停止等請求権の拡張 現行法上、利用停止等請求権を行使できる場面は、保有個人データについて違法行為があった場合等限定的であるが、こどもの要保護性を踏まえると、こどもを本人とする保有個人データについては、他の保有個人データ以上に柔軟に事後的な利用停止を認めることについて検討する必要がある。ただし、取得について法定代理人の同意を得ている場合等、一定の場合においてはその例外とすることも考えられる。

ｃ： 安全管理措置義務の強化 こどもの個人データについては、こどもの「安全」を守る等の観点から、特に取扱いに注意が必要であり、組織的、人的、物理的及び技術的という多角的な観点からリスクを検討し、必要かつ適切な安全管理措置を講ずる必要がある。そこで、こどもの個人データについて安全管理措置義務を強化することがあり得る。

ｄ： 責務規定 各事業者の自主的な取組の促進という観点からは、こどもの個人情報等の取扱いについては、こどもの最善の利益を優先し特別な配慮を行うべき等、事業者等が留意すべき責務を定める規定を設けることも検討する必要がある。

ｅ： 年齢基準 Q&A の記載や GDPR の規定の例などを踏まえ、16 歳未満とすることについて検討を行う。

「こどもの個人情報等に関する規律の在り方」については、 個人情報保護法として、はじめての提言であり、改訂を期待したい事項です。

２．事例に学ぶ：持ち出し PC について

事例シリーズの第 26 弾です(前回は 25 弾でした)。今回は“持ち出し PC”をテーマに挙げてみました。背景は、警視庁が毎年のように更新し公表している「マルウェア『ランサムウェア』の脅威と対策(脅威編)」で“**ランサムウェアの感染経路**については、**VPN 機器**や**リモートデスクトップ(NW 機器)からの侵入**が多くを占めている”としていることです。

対策として挙げられているのは PC やサーバの OS のアップデート等基本的な事柄です。NW 機器から侵入されただけであれば自社としては特段問題はなく(DoS 攻撃の踏み台になる可能性はあり)、データやプログラムが格納されている PC やサーバが侵されて初めて被害になります。特に会社の管理下を離れた持ち出し(テレワーク)PC が懸念されます。

（1）「マルウェア『ランサムウェア』の脅威と対策（脅威編）」の要旨

2024 年 3 月に IPA から発表された今年注意を要するサイバー空間における「情報セキュリティ 10 大脅威 2024」の法人部分で“ランサムウェア”がこの数年に引き続き首位を占めています。ランサムウェアは、その PC 内のデータを暗号化等によって利用できない状態にした上で、そのデータを利用できる状態に戻すことと引き換えに身代金(金銭)を要求します(「二重恐喝」)。

警察庁により公表されている企業・団体等におけるランサムウェア被害の件数は、令和 3 年より急増し、令和 6 年上期で 128 件発生しています。

ランサムウェアの感染経路については、**VPN 機器やリモートデスクトップからの侵入が全体の 83%**を占めており、これらのテレワーク等に利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めています。

同「対策編」では、“ランサムウェア感染を防ぐ対策としてまずは**基本ルールを定着させ、サイバーセキュリティ意識を高めていきましょう。**”と訴え、具体的には“OS やソフトウェアは常に最新の状態にしよう”“ウイルス対策ソフトを導入しよう”“パスワードを強化しよう”等が挙げられています。**NW 機器のセキュリティ強化だけでは不十分**であることを意味します。

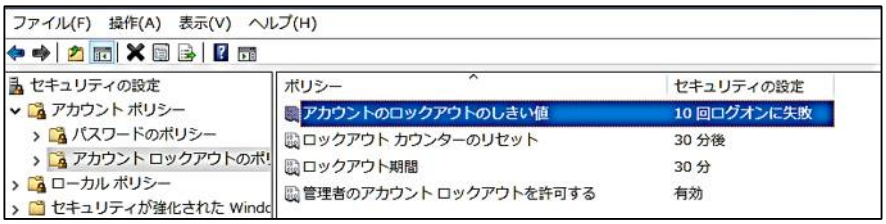
（2）持ち出し PC の設定

テレワークで使用する PC には、個人の私物と会社資産の持ち出しが考えられます。私物についてはプライバシーの問題等があり会社として詳細に立ち入ることは叶いませんので、ここでは会社資産の(つまり持ち出し)PC に着目します。

持ち出し PC は**“会社で設定したセキュリティポリシー(各種の設定)を変更していない”が大前提**ですが、その他に以下の事項も検討すべきです。(WindowsPC を前提に)

①起動時パスワードの回数制限設定

PC への悪意による使用を防ぐため起動する際のパスワードを設定していない人はいないと思いますが、〝誤入力回数制限〟についてはいかがかでしょうか。



パスワードを破ろうとした際には何度もログインを繰り返します。その際、連続して失敗した場合の回数(しき

い値)制限が設定でき、その**回数に達すると指定した時間が経たないと再びログイン画面にならない**ようにすることができます。このことによって“犯行”を諦めさせられます。「ローカルセキュリティポリシー」で回数やロックアウト期間(時間)の設定を行います。

https://www.aibsc.jp/joho/security/tada/01.html　などの説明が参考になります。

②ディスク類の暗号化

Windows を起動する際のパスワード(パスコード)や PIN コードの設定だけでは PC を盗まれた場合に内蔵の HDD や SSD を抜かれ、他の機器(PC 等)で会社の機密情報や各種のパスワード等を読み取られる恐れがあります。

そこに登場したのがディスク類の暗号化機能で、**「BitLocker」が Windows に付属**しています(Home 版では解除のみ)。“回復キー”を知らないとアクセスができませんが、その機器で利用している限りは暗号化していることを何ら意識することはありません。

③USB 媒体の自動再生の抑止

USB メモリー等を PC に挿し込んだ時、その中に収納されているコンテンツを自動起動させることができます。CD や DVD を装填した途端に映像や音楽が始まるのは便利ですが、マルウェア(ウィルス等)が起動された場合にはランサムウェアを呼び込むかもしれません。**コントロールパネルの「自動再生」**アイコンをクリックすると、媒体別に“装填した際にどうするか”の選択メニューが表示されます。**“何もしない”が無難**ですが、一度設定を確認してみましょう。

（3）テレワーク時のルール

数年前政府の肝いり政策「働き方改革」を機に、「P マークニュース」で**テレワークに伴うリスク対策**について検討しました。その半年後にコロナ禍でてれわが常態化したのは何の因果でしょうか。その稿では、トムソンネットがプライバシーマークの支援先各社さんに提供させていただいている規程(安全管理細則等)に、標準として**「携帯可能な PC、携帯電話、スマートフォン、タブレット端末等(モバイル機器)の利用」の項を設けてある**旨が述べられています。

例えば、　“モバイル機器の利用時には、安全なワイヤレスネットワークサービス(Wi-Fi)を利用する。”、等々です。この際再度目を通され自社として不足があればルールを追加されてはいかがかでしょうか。

（4）まとめ

企業の情報セキュリティ脅威のトップにランクされている「ランサムウェア」・・・その被害の多くは NW 機器の脆弱性を突破口に PC やサーバに侵入されたものです。特にテレワークの場合が要注意です。一方テレワークには PC の持ち出しが付いて回り、**窃取や盗難等の場合に備えた対策が必要ですが、ランサムウェア対策と共通する**ことが多くあります。

今回は“いつでもできる”事柄を 3 点挙げて検討してみました。できそうなことは直ぐにでも実行に移されるようお勧めします。

３．Windows10 のサポートが 2025 年 10 月 14 日に終了します

Windows 10 は**バージョン「22H2」**が最終バージョンになります。

Windows 10 は 2022 年 10 月 18 日に、バージョン 22H2 への更新が始まり、2023 年 4 月 27 日にこの 22H2 が最終バージョンとなることが発表されました。

今後は特別な事が無い限り新機能は追加されず、バグ修正やセキュリティ更新のみのサポートとなります。

（１）サポート期限は 2025 年 10 月 14 日

Windows 10 のサポート期限は、2025 年 10 月 14 日と発表されましたが、この期限とは、Windows 10 の最新のアップデートであるバージョン 22H2 であることが条件です。バージョン 21H2 以前のまま使用している人は、すでにサポート切れになっています。サポート切れの OS では､マルウェアや未知のウィルスといった脅威に対して脆弱性が発生しますので、早急な更新が必要です。

Windows 10 のサポート終了日は、2025 年 10 月 14 日と公式から発表されています。この日を過ぎると、マイクロソフトからセキュリティアップデートが提供されなくなるため、コンピューターウイルスや不正アクセスのリスクが高まります。サポート終了まではまだ時間がありますが、徐々に移行の準備を進めていくことが賢明です。特に企業では、計画的なアップグレードや移行が欠かせません。個人ユーザーの場合も、セキュリティを守るために新しい OS への移行を検討する必要があります。

（２）サポート終了がユーザーに与える影響

サポート終了後も Windows 10 を使い続けることは可能ですが、セキリティ面で大きなリスクを抱えることになります。マイクロソフトからのセキュリティアップデートが提供されなくなるため、新たに発見された脆弱性を狙ったサイバー攻撃に対して、無防備な状態になってしまうのです。たとえば、個人情報の流出や、ランサムウェアによるデータの暗号化など、深刻な被害に遭う可能性が高まります。特に、インターネットに接続するパソコンは常にセキュリティ脅威にさらされているため、注意が必要です。企業の場合、データ流出などを起こしてしまうと社会的な信頼性にも関わります。

（３）サポート終了後のセキュリティリスクと脆弱性

サポート終了後の Windows 10 は、まるで防火壁のないネットワークのようなものです。新たな脆弱性を突いた攻撃者は、自由にシステムに侵入し、大切なデータを盗み出すことができてしまいます。過去には、サポートが終了した Windows XP を狙った「WannaCry」により、世界中で大規模な被害が発生しました。

こうした危険と隣り合わせの状況を避けるためには､Windows 11 へのアップグレードや、他の OS への移行を検討する必要があります。セキュリティを守るためには、新しい環境への移行が不可欠です。

（4）Windows 10 サポート終了後のセキュリティ対策

Windows 10 のサポート終了後も安全に使い続けるための対策方法を次に解説します。

最も効果的なのは Windows 11 へのアップグレードですが、PC の互換性や動作環境を確認する必要があります。

仮想デスクトップやクラウドサービスの活用、Linux や macOS への移行も選択肢の一つです。自社に適した方法を選択し、セキュリティリスクに備えることが大切です。

（5）Windows 11 へのアップグレード

Windows 10 のサポート終了後も安全に使い続けるには、Windows 11 へのアップグレードが最もスムーズな対策です。アップグレードすることで、最新のセキュリティ更新プログラムを適用し、脆弱性を防ぐことができます。また、Windows 11 の新機能やパフォーマンスの向上も期待できます。アップグレードの手順は Microsoft の公式 Web サイトで詳しく解説されているので、それを参考にして実施して下さい。万が一、PC が Windows 11 の動作環境を満たさない場合は、他の対策を検討する必要があります。

アップデート作業をスムーズに進めるには、事前に十分な準備を整えることが必要です。

ここでは、事前にどのような準備を整えればよいかを解説します。実行中に何らかのトラブルが発生するリスクを減らすためにも、必要な準備をきちんと整えた上で作業を開始することが肝要です。

（6）アップグレード作業を実行するための環境を整備について

Windows 11 へのアップグレードを決断したら、必要な環境を整えましょう。

具体的な準備には、以下のようなものがあります。

・システムドライブ（C ドライブ）の空き容量を確保する。
・インストールメディアを用意する。
・安定したインターネット接続環境を用意する。（有線接続推奨）
・電源コードを確実に接続する。

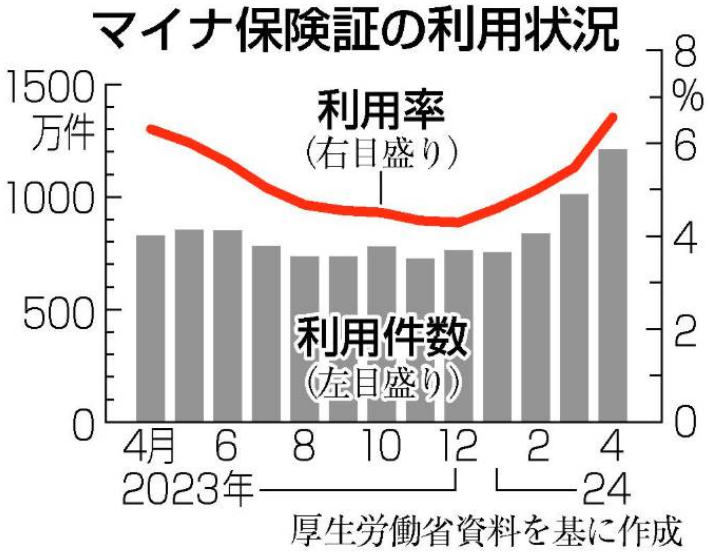
アップデート中にインターネット接続が切れたり電源コードが抜けて強制終了したりすると、トラブルの原因になりかねません。場合によっては Windows が起動しなくなり、クリーンインストールが必要になるケースもあります。

そのため、アップデート作業は安定した環境で作業を実行することが大切です。

４．トピックス

現行の健康保険証の新規発行を停止し、マイナンバーカードと一体化し「マイナ保険証」に本格移行する１２月２日まであとわずかに迫ってきました。

しかしながら、現状はまだマイナ保険証のメリットが十分に理解されておらず、利用率の低迷が下表の通り続いているようです。そのため、政府は活用が進むまでは、現行保険証との併用を最長１年間認めるといった移行措置を設定しています。



【図解】マイナ保険証の利用状況

現行保険証の新規発行が終わる１２月２日以降は、マイナ保険証以外の主な資格確認方法として、現行の保険証や、マイナカードを持っていない人などに発行される「資格確認書」も利用できることになっています。

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）