Ｐマークニュース

＜２０１７年陽春号＞　Ｖｏｌ．１９

（株）トムソンネット

Ｐマークコンサルティンググループ

２０１７年陽春号目次

１．改正個人情報保護法が施行されます(続)

ー　2017.5.30 から全ての事業者での遵守が義務づけられました　ー

改正個人情報保護法が、2017 年 5 月 30 日の施行と決定され(2016.12.20 閣議決定)、2016.10.5 付で「個人情報保護に関する法律施行規則」が公示され、2016.11.30 付で、「個人情報保護法ガイドライン」(全 4 編)が公表されました。ガイドラインのなかで「格別の措置」とされていた金融分野のガイドラインについても公表されました。(2017.2.28 個人情報保護委員会)　個人情報保護法の改正をうけて、P マークの認証基準である JIS 規格も、見直し検討に入っており、2017 年秋以降に改正・公表される見込みです。

こうした状況をうけて JIPDEC が「改正個人情報保護法へのプライバシーマーク制度の対応方針について」を公表しました。(2016.11.30)　2017 年は、10 年ぶりの個人情報保護法改正によって、中小事業者の特例はなくなり全ての事業者の遵守が義務づけられ、個人情報保護が大きく再認識される年となります。今号では、改正個人情報保護法の内容のうち「個人識別符号」「要配慮個人情報」ついて、詳述します。

（１）「個人識別符号」について

「個人識別符号」の含まれるものを「個人情報」として新規に追加定義(2 条 I 項 2 号)しました。

①「個人識別符号」とは次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものとしています。

ａ：特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの。

身体の一部の特徴をデジタル化した**符号(a)**とは、

- 細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列
- 顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌(顔貌)
- 虹彩の表面の起伏により形成される線状の模様(虹彩)
- 発声の際の声帯の振動、声門の開閉並びに声道の形状及びその変化(声紋)
- 歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様(歩容)
- 手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状(静脈)
- 指紋又は掌紋

ｂ：個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるものサービスの利用者個人に割り当てられる**符号(b)**とは

・旅券法（昭和 26 年法律第 267 号）第 6 条第 1 項第 1 号の旅券の番号
・国民年金法（昭和 34 年法律第 141 号）第 14 条に規定する基礎年金番号
・道路交通法（昭和 35 年法律第 105 号）第 93 条第 1 項第 1 号の免許証の番号
・住民基本台帳法（昭和 42 年法律第 81 号）第 7 条第 13 号に規定する住民票コード
・行政手続における特定の個人を識別するための番号の利用等に関する法律
（平成 25 年法律第 27 号）第 2 条第 5 項に規定する個人番号
・次に掲げる証明書にその発行を受ける者ごとに異なるものとなるように記載された個人情報保護委員会規則で定める文字、番号、記号その他の符号
〇国民健康保険法（昭和 33 年法律第 192 号）第 9 条第 2 項の被保険者証
〇高齢者の医療の確保に関する法律（昭和 57 年法律第 80 号）第 54 条第 3 項の被保険者証
〇介護保険法（平成 9 年法律第 123 号）第 12 条第 3 項の被保険者証
・その他前各号に準ずるものとして個人情報保護委員会規則で定める文字、番号、記号その他の符号

②今回改正では、下記の符号は含まないとしています。
a. 携帯端末 ID　携帯電話番号
b. クレジットカード番号
c. メールアドレス（ドメインから個人が識別できるものを除く）
d. SNS の会員 ID　等

③なお、ガイドラインからは、証券番号、銀行口座番号などは、含まないと解釈できますが、「容易照合性 」により、個人情報にあたる場合があることに注意が必要です。　例えば「〇〇代理店扱いの証券番号」を含む情報は「個人情報」に該当します。メールでの問い合わせではよくあるケースですが、留意が必要です。

（２）「要配慮個人情報」（2 条 3 項）について

①「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいいます。（ガイドラインで詳細に具体例を示しています。）

②保護法では、労働組合への加盟、門地、本籍地、性生活に関することが要配慮個人情報に含まれていません。しかしながら、JIS Q 15001 と同様に、「金融分野における個人情報保護に関するガイドライン」では、センシティブ情報として対象となっています。

③取得にあたっては本人同意が必要です。保険代理店は病歴などを記載した「告知書」を取得しますが、これは保険会社の募集委託をうけての取扱いですから、保険代理店が本人の同意書を取得するわけではありませんが、要配慮個人情報ですから、封筒に入れて扱う等その取扱いに留意が必要です。

④要配慮個人情報を第三者提供することは、本人から第三者提供に関する同意を取っていないかぎり禁止です。またオプトアウトの取扱いも禁止です。

今回ガイドラインは、全ての分野に共通の汎用的なガイドラインとして、個人情報保護委員会が作成し、「従来の各分野別のガイドラインを一元化したもの」と位置付けています。

ただし、一部の分野(医療関係、金融関係、情報通信関連など)については、「このガイドラインを基礎として、当該分野において必要となる別途の規律を定める」としています。この各分野固有の「格別の措置」に特化した「金融分野における個人情報保護に関するガイドライン(案)」が示されました。(2016.12.13 の個人情報保護委員会)

そのガイドラインによれば、「各分野固有の「格別の措置」については、行政の継続性の観点から、原則として現行の各分野ガイドラインの規制水準を維持するとともに、法改正に伴い新たに必要となる規定を盛り込む」ことを基本として、下記の「格別の措置」を盛り込んでいます。

ａ:「機微(センシティブ)情報」について

・現行ガイドラインの「機微(センシティブ)情報」(第５条)に、「要配慮個人情報」を合わせ、新たな「機微(センシティブ)情報」と定義する。

・新たな「機微(センシティブ)情報」についても、現行ガイドラインと同様に情報を取得等できる場合を限定する。とりわけ、その取扱いにおいて、「あらかじめ本人の同意を得る」ことに、留意すること。

・新たな「機微(センシティブ)情報」については、オプトアウト(提供にあたり、あらかじめ以下の情報を本人に通知し、または本人が容易に知りうる状態に置いておくとともに、本人の求めに応じて第三者への提供を停止すること)を用いないこと。

ｂ:「本人の同意」については、原則として書面によることとする。

ｃ:「オプトアウト」を「個人の支払い能力に関する情報を個人信用情報機関へ提供する」にあたっては、用いないこととする。

（３）認証されたＰマークとの関連　(JIPDEC の 2016.11.30 公表文及び Q&A から引用)

①現在取得しているプライバシーマークは、改正個人情報保護法の施行後においてもそのまま使用できるか?

⇒使用できます。

プライバシーマークの審査の基準となっている JIS には、現行でも法令遵守が要求規格として盛り込まれており、その要求事項を満たしたプライバシーマークの取得事業者は、法令等が改正されてもこれに適切に対応できるマネジメントシステムが構築され運用されているものと考えられます。従って改正個人情報保護法施行後もプライバシーマークは有効です。

②新たにプライバシーマークを取得する場合、または現在取得しているプライバシーマークを更新する場合、改正個人情報保護法施行後において、審査の基準は変るか?

⇒変りません。

従来通り、現行の JIS Q 15001:2006 を基準として適合性の審査・認証を行います。ただし、当然のことながら改正個人情報保護法の全面施行に伴い同法を遵守すべく必要な措置を講ずる必要があります。

③改正個人情報保護法施行後の審査において、改正個人情報保護法を遵守するための必要な措置を取っていなかった場合、審査は不適合となるか?

⇒現地審査において、何ら措置が講じられていない場合は、リスクに応じた措置を講じるよう是正を求めます。ただし、JISQ15001 の改正を踏まえた審査開始までの間は、今後講じる措置の計画を報告することも可とし、次回更新審査時に再度実施の有無を確認します。

改正個人情報保護法の施行によって、金融分野事業者の義務がより明確になりました。

改正法を遵守していく社内規程・同意文など雛型・様式、見直しのルール化などの具体的な方策が必要です。その方策のひとつはＰマーク取得です。ご相談ください。

２．「やさしい情報セキュリティ」その１０：ルータの脆弱性について

つい先日、国内の情報セキュリティに関する総本山とも言うべき IPA（(独）情報処理推進機構）から「情報セキュリティ 10 大脅威」の 2017 年版が公開されました。これは、2016 年度に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から IPA が脅威候補を選出し、「10 大脅威選考会」が審議・投票を行い、下表のように決定したものです。

「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングや クレジットカード情報の不正利用	1	標的型攻撃による情報流出
ランサムウェアによる被害	2	ランサムウェアによる被害
スマートフォンやスマートフォンアプリを 狙った攻撃	3	ウェブサービスからの個人情報の窃取
ウェブサービスへの不正ログイン	4	サービス妨害攻撃によるサービスの停止
ワンクリック請求等の不当請求	5	内部不正による情報漏えいと それに伴う業務停止
ウェブサービスからの個人情報の窃取	6	ウェブサイトの改ざん
ネット上の誹謗・中傷	7	ウェブサービスへの不正ログイン
情報モラル欠如に伴う犯罪の低年齢化	8	IoT 機器の脆弱性の顕在化
インターネット上のサービスを悪用した攻撃	9	攻撃のビジネス化 （アンダーグラウンドサービス）
IoT 機器の不適切な管理	10	インターネットバンキングや クレジットカード情報の不正利用

（１）注目すべき脅威は？

この中で注目されるのは、昨年ランク外だった“IoT 機器の脆弱性の顕在化”(「組織」向け脅威の 8 位）です。IPA は“IoT とは、モノのインターネット（Internet of Things)。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み”と説明しています。Iot 機器は、コンピュータの姿をしておらずにインターネットに繋がっている機器や装置のことになります。
昨年ウェブカメラがウィルス「Mirai」（ミライ）に感染し、長時間に亘って商用のネットワークやサーバを攻撃する事件が多発しました。ちなみに、「Mirai」のソースプログラムが容易に手に入るため、ちょっとした知識で“亜種”を作ることができることから大変に危険視されています。

（２）オフィス内に IoT 機器はあるか？

工場や病院などと異なり、一般にオフィスで IoT 機器が使われているとの認識が余りないと思われますが、実はいくつかあります。先ずはインターネット経由で遠隔サービスの対象となっている機器が該当します。防犯カメラ、センサー（侵入検知器)、複合機等々。
IoT 機器を支えるのが、社内 LAN や IoT 機器をインターネットに繋ぐ「ルータ」(無線 LAN（Wi-Fi）のアクセスポイントやファイアーウォールを兼ねている場合もあり）です。IoT 機器が攻撃をされても、“動きがおかしい”“繋がらない”の社内レベルの被害で済めばいいのですが、そこに棲みついたマルウェアが社内システムに留まらず、取引先のシステムを攻撃する可能性があります。そうなると、被害者のはずだった貴社が正に加害者になってしまいます。

（３）ルータの現況

ルータには社内側（無線アクセスポイント、LAN ポート）と外部側（WAN ポート）に接続口があります。内部側の無線アクセスポイントは、工場出荷時点で 10 文字以上のパスワードが設定され（SSID 別）侵入は難しく、有線 LAN なら尚更問題ないでしょう

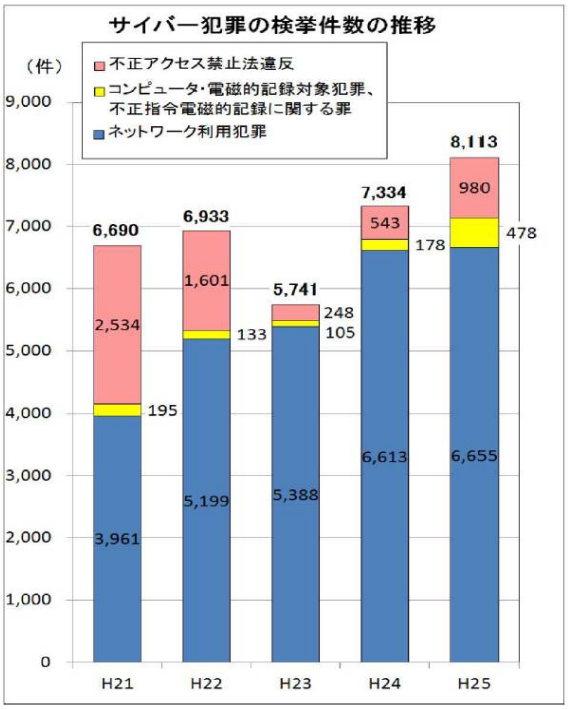
対して、外部側は（モデムに繋がっている場合）インターネットを経由して世界に門戸を広げており、マルウェアに侵入されるケースが急増しています。大手製造元であるシスコシステムズ、アイ・オー・データ機器、バッファロー社などが相次いでセキュリティの警告を公表しています。貴社で使用中のルータについてメーカーの HP をチェックしてみることを強くお勧めします。

なお、無線 LAN の保護策として“MAC アドレス制限”や“SSID ステルス化”が著名ですが、この場合はほぼ該当しません。何故ならマルウェアは外部側から侵入することが圧倒的に多いからです。

（４）防御策は何か？

貴社にとってブラックボックスと言えるセンサーなどと違い、ルータは自社でセキュリティレベルを高められます。代表的なのは“管理者のパスワード”です。工場出荷時の設定のままになっていないでしょうか。ID が“admin”、パスワードが“password”という具合です。これは誰もが知っており、パスワードを設定しているとは言えません。

ポイントの第一は、このパスワードを自社なりのものに変更することです。SSID のパスワードと異なり、PC やスマホ、Iot 機器の設定には影響がありません。次は、メーカーの HP を定期的に閲覧し、セキュリティ機能の更新をルーチン化することです。長くても半年に 1 回はパスワードの変更とソフトウェアの更新をしましょう。「IT 機器管理台帳」にルータを記載するなどによって、明示的に“管理対象”として認識し、セキュリティ対策に気を配りたいものです。



【警察庁：広報資料より】

３．「マイナポータル」、ご存知ですか？

個人番号カードはお持ちですか。

2017 年は個人番号カードを使った各種サービスがスタートします。以下では、個人番号カードを使ったサービス「マイナポータル」について紹介します。

（１）マイナポータルとは

自宅のパソコン等から、個人番号カードを利用して行政機関がマイナンバーの付いた自分の情報を「いつ」、「どこと」やりとりしたのか確認できるほか、行政機関が保有する自分に関する情報や、行政機関から自分に対しての必要なお知らせ情報等を確認できるようになります。

具体的には、下表に示すサービスが予定されています。

NO	機能区分	内容
1	情報提供等記録表示（やりとり履歴）	情報提供ネットワークシステムを通じた住民の情報のやり取りの記録を確認できる
2	自己情報表示（自分の情報）	行政機関などが持っている自分の特定個人情報が確認できる
3	お知らせ	行政機関などから個人に合ったきめ細かなお知らせを確認できる
4	民間送達サービスとの連携	行政機関や民間企業等からのお知らせなどを民間の送達サービスを活用して受け取ることができる
5	サービス検索・電子申請機能（ぴったりサービス）	地方公共団体の子育てに関するサービスの検索やオンライン申請（子育てワンストップサービス）ができる
6	公金決済サービス	マイナポータルのお知らせを使い、ネットバンキング（ペイジー）やクレジットカードでの公金決済ができる
7	もっとつながる（外部サイト連携）	外部サイトを登録することで、マイナポータルから外部サイトへのログインが可能になる

（２）マイナポータルの利用には、個人番号カードが必要です。

マイナポータルでは、なりすましにより特定個人情報を詐取されることのないように、利用の際は、情報セキュリティ及びプライバシー保護に配慮した厳格な本人認証が求められます。このため、個人番号カードのＩＣチップに搭載される公的個人認証を用いたログイン方法が採用され、マイナポータルにログインする際は、個人番号カードが必要となります。

（３）さらに個人番号カードを読み込むために IC カードリーダーが必要です。

自宅等のパソコンからマイナポータルへログインする際は、個人番号カードを読み込むためのカードリーダーが必要になります。カードリーダーの購入は利用者の負担となります。

なお、自宅にパソコン等の端末が無い人のために、公的機関にマイナポータルを利用可能な端末が設置される予定です。

（４）マイナポータルの利用は、平成 29 年 7 月から試行運用が開始される予定です。

平成 29 年 7 月から行政機関の間の情報連携の試行運用が開始される予定です。マイナンバーの付いた自分の情報のやりとりの確認もこれ以降可能になる予定です。

マイナポータルのその他のサービスについても平成 29 年以降順次開始することが予定されています。

上記の通り、今年（2017 年）は、個人番号カードを使った各種サービスが順次始まります。
まだ個人番号カードの申請をされていない方は、そろそろ発行の手続きを進められては如何でしょうか。
これまで個人番号カードの発行には時間が掛かるなどの指摘がありましたが、最近はカード申請から発行までの期間は、1 か月程度との自治体が増えています。

４．トムソンネットからのお知らせ

みなさまに季刊でお届けしているこの「P マークニュース」は、2012 年 10 月の発刊以来、みなさまから様々な形で温かいご支援を戴き、次号で 20 号を迎えます。

改めてこの間のみなさまのご支援に深く感謝するとともに、今後もみなさまの個人情報保護への取り組みや、P マーク取得、情報セキュリティの強化といった課題の解消のお役に立てる情報紙として、さらなる紙面の充実を図りたいと考えております。

就きましては、みなさまから本紙に対するご希望やご意見、あるいは個人情報保護法等の法や制度改正や情報セキュリティ等に関するご意見等がございましたら、是非、お寄せ戴きたく、お願い申し上げます。

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　（http://www.tmsn.net/）

〒101-0062 東京都千代田区内神田駿河台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）