Ｐマークニュース

＜２０１６年陽春号＞　Ｖｏｌ．１５

（株）トムソンネット

Ｐマークコンサルティンググループ

２０１６年陽春号目次

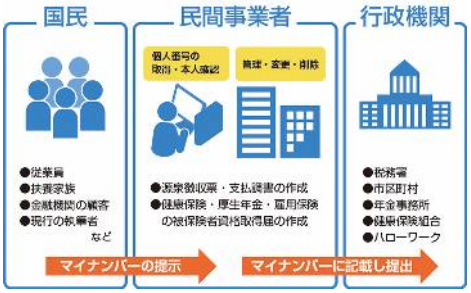
１．マイナンバー関連個人情報のＰＭＳへの対応

マイナンバーの通知がされ、その利用が 2016.1 から開始されています。マイナンバーを取扱っている事業者、これからの事業者もいるでしょうが、「特定個人情報」も「個人情報」であり、JIS Q15001:2006「個人情報保護マネジメントシステム(PMS)-要求事項」の適用を受けることは勿論、番号法に従い、かつ特定個人情報ガイドラインにも適合するように取扱わなくてはなりません。

その取扱いについて JIPDEC は、2016.2.12 に「特定個人情報の取扱いの対応について」を一部改訂し、公表しました。また、「個人番号への対応について」FAQ を追加しています。

それ等を中心に PMS への対応について整理しました。

（１）マイナンバー関連の個人情報とは？



多くの事業者で取扱うマイナンバー関連個人情報の主なものに下記があります。

①所得税、住民税関係の帳票
②健康保険・厚生年金保険関係の帳票
③雇用保険関係の帳票
④その他（報酬・料金・契約金及び賞金の支払調書、不動産関連支払調書など）
⑤特定個人情報の管理帳票（各種「個人番号」取得票、「個人番号」取扱記録など）

（２）「特定個人情報」と JIS Q15001：2006

「特定個人情報」については、慎重な取扱いと個人情報保護法、JIS 要求事項よりも厳格な保護措置が求められています。

①番号法では、個人番号を取扱う事務を限定し、その規定された範囲を超えて個人番号を利用することを禁じています。例えば、本人の同意を得たとしても、個人番号を社員番号として利用することは禁じています。

②罰則規程は、事業者が取扱う個人情報の量に関わらず、適用され、より厳重になっています。

前記の JIPDEC「特定個人情報の取扱いの対応について」では、「特定個人情報」について、①JIS Q15001:2006 の要求事項に基づいて対応を必要とする事項と、②番号法に基づき対応を必要とする事項とに分けて、各々の項目を下記としています。

ａ：JIS Q15001:2006 の要求事項に基づいて対応を必要とする事項
・個人情報の特定、リスク等の認識・分析及び対策（要求事項 3.3.1、3.3.3）
・法令・国が定める指針その他の規範（要求事項 3.3.2）
・資源、役割、責任及び権限（要求事項 3.3.4）
・緊急事態への準備（要求事項 3.3.7）

ｂ：番号法に基づき対応を必要とする事項

・取得、利用及び提供に関する原則(要求事項 3.4.2)
・正確性の確保(要求事項 3.4.3.1)
・安全管理措置(要求事項 3.4.3.2)
・委託先の監督(要求事項 3.4.3.4)

（３）プライバシーマークの審査基準はどう変わるか？

「特定個人情報」について、審査基準である「JIS Q 15001:2006」が変更されるわけではありませんので、JIPDEC では、「JIS に基づき付与事業者が対応すべき事項、留意すべき事項が加わる。と考えてください」としています。分かりにくい表現ですが、前記の（２）の②ａ：JIS Q15001:2006 の要求事項に基づいて対応を必要とする事項については、「PMS 従来規程への追加訂正」及びその運用を必要としています。また、同じく（２）の②ｂ：番号法に基づき対応を必要とする事項については、「PMS 従来規程への追加訂正」ないし「番号法に基づく新たな対応規程作成」及びその運用を必要としています。この対応基本に基づいて　従来どおり、文書審査(文書規程審査)と現地審査(その運用状況審査)がされるとしています。

（４）具体的な留意事項を 2 例だけ示すと(他にもありますが)

①個人情報保護方針について JIS 規格に適合していると認められれば変更や新規策定の必要はないのですが、例えば個人情報保護方針に下記のような宣言が含まれていれば、改訂が必要です。(JIPDEC の FAQ17-4-2)

・「本人の同意を取得した利用目的の範囲内のみで取扱う」と限定して宣言している。
（「特定個人情報」は「本人の同意」を必ずしも必要としていないので、この規定は適合しない）
・遵守する法令を個人情報保護法に限定して宣言している。

②「特定個人情報」の取扱いを収集から廃棄までの全てを「委託」するので、自社としては何らのマイナンバー対応も考えなくてよいか。(JIPDEC の FAQ17-10-8)

・個人番号関係事務の代行サービスの利用等により個人番号関係事務の全部を委託する場合、当該委託先に対し、要求事項 3.4.3.4 による委託先の監督が求められます。
・個人番号関係事務の全部を委託する場合も事務取扱担当者の役割、責任及び権限を明確に定め、文書化した上で、担当者を設置することが原則です。文書化にあたっては、個人番号関係事務の委託先の監督を役割、責任及び権限に含める必要があります。
・個人番号関係事務の全部を委託するために事務取扱担当者が設置しづらい場合であっても、当該事務委託先の監督を担当する者が明確である必要があります。(例：個人情報保護管理者の役割、責任及び権限として、個人情報の取扱いの委託先の監督が含まれ、文書化されていること)
・また、委託先の監督だけではなく、JIS Q 15001:2006 の各要求事項に対応する必要があります。自社内で特定個人情報を取り扱う作業を行わない(保管等が発生しない) 場合であっても、貴社が行う事務を委託している場合は、「JIS Q 15001:2006(個人情報保護マネジメントシステム―要求事項)」の管理対象となります。
・特定個人情報の保管等が発生しない場合も「閲覧」していると考えられます。この場合においても、「JIS Q 15001:2006(個人情報保護マネジメントシステム―要求事項)」においては個人情報の特定（要求事項 3.3.1）の対象となります。特定個人情報についても同様です。また「閲覧のみの個人情報について、リスクは存在するか」というリスク認識につなげることとなります。

（５）マイナンバー関連個人情報に関するトムソンネットでの対応

トムソンネットでは、前記の JIPDEC 基本対応原則に基づいて、弊社の提供した PMS 規程類への具体的な変更・追加訂正を行い、それ等の規程類を 2015.11 からリリースしています。また、前記ではその一部を例示した P マーク審査での具体対応につきましても、コンサルさせていただいています。お気軽に別記連絡先にお問い合わせください。

２．トムソンネットのＰマークコンサルを評価する（ユーザアンケートより）

弊社は、これまでに１２社（保険代理店１０社、システム会社２社）に対してＰマーク取得に関するコンサル業務を行って参りました。弊社のコンサルの基本方針は、個人情報保護マネジメントシステム（ＰＭＳ）の大きな柱である、

①マネジメントサイクル（ＰＤＣＡサイクル）を維持すること。

②個人情報にかかわる事故を起こさない体制を作り上げること。

③個人情報の取扱ルールを確立すること。

の実現です。そのために、継続性のあるＰＭＳ体制が保険代理店様に定着するよう、「丁寧に」「リーズナブルな価格」で、Ｐマークの取得支援をすることをモットーにしています。

そんな弊社のＰマーク取得支援業務が、実際に弊社の支援サービスをご利用された保険代理店様から、どのように評価されているかを、前号に続き、昨年の暮れに実施したユーザアンケート（６社様から回答）から探ってみました。

（１）Ｐマーク取得のためのコンサル会社として弊社が選ばれた理由

結果は以下の通りでした。

順位	選定理由	社数
１	保険業務の精通している	５社
２	有力者の紹介	３社
３	価格がリーズナブル	２社
４	コンサルティングのキャリアが豊富	１社

選定理由のトップに「保険業務に精通している」を挙げられているのは、極めて妥当と思われます。

保険代理店様の個人情報を保護するＰＭＳ体制を確立するためには、保険の業務知識なくしては不可能です。弊社は数多いＰマークコンサル業者の中でも保険業務への精通度はトップクラスと自負しております。また、弊社の本音として「コンサルティングのキャリアが豊富」をもっと評価して、選んで欲しかったと欲張っています。

（２）コンサル過程における説明および提供物件に対する評価

以下の結果を戴きました。

評価	良好	普通	物足りない
社数	６社	０社	０社

丁寧に、支援先に定着するＰＭＳ体制の確立を目指す弊社としては、大変うれしい評価ですが、保険代理店様に特化したコンサル会社として「良好」は当然であり、最低の義務と考えております。

（３）Ｐマークの付与適格性審査の申請に対する支援対応について

以下の３項目について、その支援状況を「良好」「普通」「物足りない」の３択で評価して戴きました。結果は３項目ともすべての保険代理店様から「良好」との評価を戴きました。

支援区分	評価	社数
①申請書類の準備	良好	６社
②現地審査への対応	良好	６社
③審査指摘事項への対応	良好	５社（＊）

（＊）回答を戴いた中の１社様は、大変周到な準備をされ、現地審査における審査の指摘事項がなかったため、「良好」回答が５社になりました。

弊社のＰマーク取得支援サービスの最大の強みは、Ｐマークの審査経験豊富なスタッフを揃えていることです。Ｐマーク審査に必要な対応事項を長年の審査経験に基づいて、懇切丁寧に説明、対応して行きます。このため、上記のユーザ評価の通り、一般的には苦労が多いと言われる現地審査でも大きな問題指摘を受けることなく、Ｐマーク資格を取得されています。

上記のアンケート結果は、回答された保険代理店様の弊社へのお気遣いが多少含まれているものと思われますが、弊社としては、保険代理店様に特化したＰマーク取得コンサル会社として、そのコンサル業務の内容に高評価を戴いたもの思っております。これからＰマークの取得をご検討の保険代理店様におかれましては、是非とも弊社にお声掛け戴きたくお願い申し上げます。

３．近時のセキュリティ動向を探る

個人情報保護と情報セキュリティは密接な関係にあります。

そこで、近時情報セキュリティ分野において、どのような事象が問題となっているのかを探るために、日本ネットワークセキュリティ協会が毎年発表している、その年の「情報セキュリティ十大ニュース」を参考に見てみました。下表は、日本ネットワークセキュリティ協会が発表した平成２７年と２６年の「情報セキュリティ１０大ニュース」です。下表の中に挙がっている項目については、みなさんの記憶に鮮明に残っているものも幾つかあることと思いますが、如何ですか。

順位	平成２７年	平成２６年
１位	（6 月 1 日）本年金機構で 125 万件の個人情報が流出	（9 月 25 日）ベネッセ個人情報漏えい事故の調査報告書を公表
２位	（1 月 9 日）サイバーセキュリティ基本法全面施行	（11 月 6 日）サイバーセキュリティ基本法が成立
３位	（9 月 25 日）米中サイバーセキュリティ合意はサイバー戦回避	（4 月 7 日）Heartbleed など脆弱性が多発（4、5 月）
４位	（2 月 2 日）解消されないセキュリティ人材不足	（8 月 1 日）オンラインバンキング不正送金の被害急増
５位	（9 月 11 日）国が CSIRT の実効ある体制強化を勧告	（11 月 13 日）日本サイバー犯罪対策センター（JC3）設立
６位	（7 月 28 日）9 億 5 千万台のスマホに影響をあたえる脆弱性が発覚	（4 月 4 日）警察庁、ビル管理システムの探索行為に注意を喚起
７位	（7 月 11 日）Flash Player に対する脆弱性攻撃の増加	（10 月 1 日）マイナンバー制度準備進む
８位	（10 月 26 日）標的型サイバー攻撃相談件数 6 倍に	（9 月 3 日）POS マルウェアによる 5600 万件のカード情報流出が発覚
９位	（10 月 5 日）マイナンバー制度施行、通知カードの送付も始まる。	（9 月 17 日）被害が止まらないパスワードリスト攻撃
10 位	（6 月 9 日）SECCON 2015 の開催概要を発表、CTF 盛況	（9 月 18 日）DDoS 攻撃業者を使ったオンラインゲームの業務妨害で高校生を書類送検

上表から読み取れる最近の情報セキュリティ事情について、ポイントを挙げてみたいと思います。

（１）ベネッセ事件（27 年）、年金機構事件（26 年）は、記憶に新しいところですが、個人情報の漏洩件数が１００万件を超す大型の個人情報漏えい事件が２年続けて発生しました。このように１００万件を超す情報漏えい事件は、セキュリティ問題を通り越して、大きな社会問題となりました。

（２）２年連続で第２位にランクされている「サイバーセキュリティ基本法」ですが、みなさまご存知ですか。今後は国家レベルでサイバーセキュリティを強化する体制を構築され、政府や関係省庁のサイバーセキュリティ対応が進められます。

（注）サイバーセキュリティ基本法…国による情報セキュリティ戦略の基盤となる法律で、国政に重要なウェイトを占める分野について国の制度、政策、対策に関する基本方針・原則・準則・大綱を明示したもの

（３）個人情報漏えいに直結する「Heartbleed」や「Flash Player」といった特定システムの脆弱性やオンラインバンキング不正送金やパスワードリスト攻撃は、近年の事故を傾向として目を引きます。その傾向は衰えることなく、個々の問題に対する迅速な対応が求められます。

（４）昨年１０月から通知カードの交付が始まった「マイナンバー制度」は、高い情報セキュリティ精度が求められている制度であり、重要なセキュリティ問題として考慮すべき事項です。

（５）今後の情報セキュリティを考えるとき、平成２７年度の４位にランクされた「解消されないセキュリティ人材不足」は、ＩＴ化が進展する中で深刻な問題です。セキュリティ人材の果たす役割は、今後益々、大きくなると思われ、この分野の人材が充実して行くことが望まれます。

４.「やさしい情報セキュリティ」その６：（ウィルスと標的型攻撃について）

今回は昨今世間を騒がせている「ウィルスと標的型攻撃」について述べてみたいと思います。（以下では、ウィルスのみならず不正な動作をするプログラムの総称・“マルウェア”を主に使わせていただきます）

“標的型攻撃”と言えば、平成 27 年の日本年金機構の情報漏洩事案で一躍話題になりましたが、更に高度化し脅威が増しています。今までは標的企業・機関のウェブサイトにあるデータベースを直接アタックする手口を用いていましたが、標的型攻撃は手口が間接的で、そのため防衛が大変難しくなっています。どうしたら防げるのでしょうか？　一緒に考えてみたいと思います。

大事なことは、もし PC やサーバに不審な挙動が発覚した場合、会社全体の LAN をインターネットから遮断し情報の流出を防ぐことです。当然業務に支障を来しますので、人的・組織的安全措置として日頃から社内での“報連相”を習慣付けることが欠かせません。

（１）標的型攻撃の現状

“標的型攻撃は大企業や著名な機関が受けるのであって中堅・中小企業には矛先が向かない”・・は間違いです。確かに数多ある中堅・中小企業が直接のターゲット（標的）として白羽の矢が立つことは稀でしょう。しかし、実際に中小企業が攻撃を受けた例があり、最終ターゲットの大企業を狙うときに取引先中小企業の PC を“踏み台”にする可能性もあります。もし自社の PC がマルウェアに侵され、結果的にお客さんに被害をもたらした場合、“被害者だったはずが加害者になった”ことになります。

（２）標的型攻撃のパターン

主な古典的な手口は、添付ファイルにウィルスを仕込んだメールを送るやり方でした。近年では、発信者を偽って（なりすまし）サイトを開かせるようなメールを送りつけるやり方が激増しています。サイトを開くとマルウェアがダウンロードされ、情報流出のバックドア（裏口）が作られる、というシナリオです。

ここで問題は、メールを受け取った人から見ていかにも信用できそうな発信者の名前をどうして知ることができたのでしょう。それは、前段として名前を使われた“発信者”の PC に侵入し、アドレス帳から“宛先”が取り出されたという他ありません。バックドアが仕掛けられたことを検出するのは中々難しいのですが、電機系のある大手会社によれば、感染後の挙動パターンは約 50 種類に分類され、そのパターンに合致した場合に“黒”と判定する方式を研究中とのことです。早期の実用化が待たれます。

（３）対策

標的型攻撃にはマルウェア感染を防ぐことから始めることになりますが、これを“入口対策”とすれば、情報を持ち出されるのを止める“出口対策”にも注目が集まっています。

①入口対策

マルウェア感染の原因はメールとホームページの閲覧による場合が大半ですが、メールは、この際是非“テキスト形式”にしましょう。メールソフトの設定で、デフォルト（初期設定）では“html”形式になっています。html 形式で表示すると、メール本文にウィルスが含まれる場合開いただけで感染します。“（受信した）メールをテキスト形式で表示する”に変更し、送信する側もテキスト形式に設定することが望まれます。Outlook などを提供している当のマイクロソフト社が、仕事で使うメールはテキスト形式を推奨すると公言しています。

メール本文そのものにウィルスを含んでいなくても、本文に“http://・・・”があってホームページに誘導する手口が流行しています。本文や添付ファイルが“黒”の場合と異なり、この場合は検知されません。大概のケースでは、送信者にいかにも信用できそうな会社名や銀行名などが書かれており、ついつい何だろうと開き勝ちです。そのようなメールは“なりすまし”ですから送信者を疑う必要があります。詳しい人にメールのヘッダ情報を見てもらえば判別がつきます。適切な入口対策を講ずることにより、自社の情報を防衛すると共に、“踏み台”にもなる可能性を減らしたいものです。

②出口対策

“ゼロデイ攻撃”といい、脆弱性が発見されてから修正プログラムが提供されるまでの間にその脆弱性を攻略するなど、どんな入口対策を採っても完璧な防衛策はないとの観点から、感染しても重要な情報が持ち出されないようにしようとするのが出口対策です。マルウェアが勝手に外部に情報を送出するのを遮断する方法です。UTM（統合脅威管理）装置、IPS（不正侵入検知・防御システム）など

によって防御を相当程度自動化できますが、数万円以上の予算を要し毎年の保守料も考慮しないといけません。

しかし、実際にマルウェアが動作を始めるまで日数が掛かることをヒントにして、マルウェア検出ソフトを使い（できれば週１回程度）PC の全体検査を行うことで発見することができます。日本年金機構でも、感染してから流出が始まる（バックドアが作動する）まで 20 日間を要しています。

③ログの点検

ログに関しては、“当社にはサーバがないから不要”とは言わず、上記の理由から各 PC のログ監視も定期的（最低月１回）に行うべきです。

PC には色々なログが取られており、「イベントビューアー」（Windows の場合）でログを見ることができますが、実際のところ生のままでは解読が難しいです。ログを見やすくする編集ソフトには安価なものもありますので、導入を検討されるようお勧めします。また、デフォルトでは設定されていませんが、（サーバだけでなく）各 PC にあるファイルのアクセスログを採取することも可能です。

５．トムソンネットからのお知らせ

（１）ご存知ですか。マイナンバーメールマガジンが便利です。

内閣府大臣官房番号制度担当室（内閣官房社会保障改革担当室）から、マイナンバー制度に関する関係省庁からの新着情報の発信を主とする「マイナンバーメールマガジン」が配信されています。

今年の１月から配信され、現在第８号までが配信されています。

マイナンバーの制度等の動向を知る上で便利は情報源であり、詳細については下記ＵＲＬをご覧ください。

http://www.cao.go.jp/bangouseido/mailmagazine/mailmagazine.html

（２）２８年４月末現在のＰマーク取得保険代理店数は、１２２社です。

ＪＩＰＤＥＣ公表の資料によれば、今年の１月～４月の保険代理店における新規Ｐマーク取得は、８社となっています。今後、業法改正等もあり、例年以上にＰマークを取得する代理店の増加が見込まれます。

時期	２８年１月	２８年２月	２８年３月	２８年４月
新規社数	５社	１社	１社	１社

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　(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　　℡　090-5528-1712　　平泉　哲史　　℡ 090-3691-5343
本間　晋吾　　℡　090-2762-4623