Ｐマークニュース ＜２０１５年新春号＞　Ｖｏｌ．１０	（株）トムソンネット Ｐマークコンサルティンググループ

２０１５年新春号目次

１．特集：マイナンバー取扱いガイドラインが公表されました
２．シリーズ：Ｐマーク取得のための勘どころ（その９：Ｐマークの取得申請）
３．「やさしい情報セキュリティ」その１：パスワードについて
４．ご存知ですか！　個人情報漏えい保険
５．トムソンネットからのお知らせ

１．特集：マイナンバー取扱いガイドラインが公表されました

―より一層求められる「特定個人情報」の保護―

マイナンバー(正式には個人番号)が 2015.10.1 から全国民に通知され、その利用開始が 2016.1 に迫ってきました。2016.1 からは「年金に関する相談照会」「申告書・法定調書等への記載」「被災者台帳の作成」等で利用が開始されます。これに先立ち「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」(2014.12.11)およびその別冊として「金融業務における特定個人情報の適正な取扱いに関するガイドライン」(2014.12.11)が公表されました。

同ガイドラインでは、「特定個人情報」が個人情報保護法(以下(法)という)の適用をうけることから、法の適用遵守を大前提として、個人情報保護に関する JIS 規格(JIS Q 15001　以下 JIS)規格という)に適合した規格項目を「望ましい」としています。従って JIS 規格の認定制度としてのＰマーク取得事業者は「望ましい個人番号利用事務実施者であり、望ましい個人情報関係事務実施者」であるといえます。

特定個人情報の取扱いは、「特定個人情報」の影響力が大きいこと、滅失・毀損・漏洩などの事故の被害が甚大であることが想定されること、利用目的が限定されることなどから、下記の点で、法・JIS 規格より厳密な措置が要求されています。

ガイドラインは、官公庁・地方公共団体・健保組合等の「個人番号利用事務実施者」と、民間の源泉徴収事務や金融機関の支払い調書事務に携わる「個人番号関係事務実施者」と分けています。
ここでは「個人番号関係事務実施者」の為のガイドラインについて紹介します。

①特定個人情報の利用制限

・個人番号を利用した「名寄せ」は禁止
・支払調書作成時に個人番号を記載する事務を対象
　(保険申込書に個人番号を記載するため、顧客から提供をうける)
・源泉徴収票(給与支払い報告書・退職所得の特別徴収票など)作成時に個人番号を記載する事務を対象
・激甚災害時に金銭の支払いを行う際に個人番号を記載する事務を対象
　(なお、激甚災害時に金銭の支払いを行うために個人番号を利用することは、番号法の認めた例外であり、個人番号利用事務または個人番号関係事務のどちらかににも該当しないため、当該事務を利用目的として、個人番号の提供をうけることはできない)

②特定個人情報の提供制限等

具体的には限定的に下記の提供が考えられます。
・本人又は代理人からの提供（本人は、給与の源泉徴収事務、健康保険・厚生年金保険届出事務等のために、個人番号関係事務実施者である事業者に対し、自己（又はその扶養親族）の個人番号を書類に記載して提出する）

・個人番号利用事務実施者からの提供
・個人番号関係事務実施者からの提供
・委託、合併に伴う提供
・情報提供ネットワークシステムを通じた提供
・委員会からの提供の求め
・各議院審査等その他公益上の必要があるときの提供
・人の生命、身体又は財産の保護のための提供

なお、法上の第三者提供とは下記の点で異なっています。

法は、個人情報取扱事業者に対し、個人データについて、本人の同意がある場合、法令の規定に基づく場合等(共同利用等ただし書きの 7 項目)には、第三者に提供することができることとしています。

一方、番号法においては、全ての事業者を対象に同法第 19 条で特定個人情報を提供できる場合を限定的に定めており(上記)、特定個人情報の提供については、法第 23 条は適用されません。なお、開示等の求めにおいて、本人から個人番号を付して求めが行われた場合や本人に対しその個人番号又は特定個人情報を提供する場合は、特定個人情報を提供することができます。

③特定個人情報の安全管理措置等

法は、個人情報取扱事業者に対して、個人データに関する安全管理措置を講ずることとし、従業者の監督義務及び委託先の監督義務を課しています。

番号法においては、これらに加え、全ての事業者に対して、個人番号(生存する個人のものだけでなく死者のものも含む。)について安全管理措置を講ずることとしています。(番号法第 12 条)

また、個人番号関係事務又は個人番号利用事務を再委託する場合には、委託者による再委託の許諾を要件とする(同法第 10 条)とともに、委託者の委託先に対する監督義務を課しています(同法第 11 条)。

＊法に加えて下記の監督義務が追加されています。
「個人番号を取り扱う事務の範囲の明確化」、「特定個人情報等の範囲の明確化」、「事務取扱担当者の明確化」、「個人番号の削除、機器及び電子媒体等の廃棄」

＊乗合代理店で、複数の保険会社にまたがる同一顧客の個人番号の提供を受ける場合であっても、複数の保険会社を連名にして、個人番号の提供を受けることはできません。

＊生損保にまたがる保険商品の場合、一方の保険会社が代表して個人番号の提供を受けることは、他方の保険会社からの委託があればできます。

④罰則の強化

法における個人情報取扱事業者に対する罰則の適用は、主務大臣からの是正命令に違反した場合、虚偽報告を行った場合等に限られています。一方、番号法においては、類似の刑の上限が引き上げられているほか、正当な理由なく特定個人情報ファイルを提供したとき(4 年以下の懲役 or200 万円以下の罰金 or 併科)、不正な利益を図る目的で個人番号を提供、盗用したとき(3 年以下の懲役 or150 万円以下の罰金 or 併科)、人を欺く等により個人番号を取得したとき(3 年以下の懲役 or150 万円以下の罰金)の罰則を新設する等、罰則が強化されています(番号法第 67 条から第 75 条まで)。なお、日本国外においてこれらの罪を犯した者にも適用されます(同法第 76 条)。

マイナンバーの利用拡大も論議されています。個人情報保護が、個人情報の取扱い、その安全管理対策の面できめ細かく規定され、留意が必要になっています。加えて、それらの措置を、PDCA を通じたマネジメントシステムとした「PMS」がますます重要になっています。今のうち、PMS の導入が必須でしょうか！！

２．シリーズ：Ｐマーク取得のための勘どころ（その９：Ｐマークの取得申請）

個人情報保護マネジメントシステム（ＰＭＳ）に則って作成した内部規定に従い、（仮）運用を行い、運用に対する監査および代表者見直しが完了すれば、Ｐマークの取得申請が可能になります。

以下では取得申請手続きのポイントを説明します。

（１）申請について

Ｐマーク付与適格性審査を申請できる事業者は、国内に活動拠点を持つ民間事業者で、Ｐマークの付与は法人単位になります。

Ｐマークの**付与機関は、一般財団法人日本情報経済社会推進協会（ＪＩＰＤＥＣ）**です。

また、**Ｐマーク審査は、ＪＩＰＤＥＣから審査機関としての指定を受けた団体**が、事業者からのＰマーク付与適格性審査申請の受付、申請内容の審査・調査等の業務を行います。

審査機関は、現在全国に１９機関あります。

申請事業者が審査機関の会員となっている場合は、当該審査機関に申請します。また保健・医療・福祉分野の事業者は、当該業種の専門審査機関であるＭＥＤＩＳ－ＤＣに申請します。その他の場合は、申請事業者の本社の登記上所在地に従い、地域毎に定められている審査機関に申請します。

（２）申請時に必要となる書類

（注）文書名の後に「＊」があるものは、所定の様式に記入する

以下の文書を整えて審査機関に提出します。
プライバシーマーク付与適格性審査申請チェック表（紙媒体で提出）＊
プライバシーマーク付与適格性審査申請書＊
会社概要＊／個人情報を取扱う業務の概要＊／すべての事業所の所在地及び業務内容＊
個人情報保護体制＊
個人情報保護マネジメントシステム（PMS）文書（内部規程・様式）の一覧＊
JIS Q 15001 要求事項との対応表＊
教育実施サマリー（全ての従業者に実施した教育実施状況）＊
監査実施サマリー（全ての部門に実施した監査実施状況）＊
事業者の代表者による見直し実施サマリー＊
登記事項証明書（「履歴事項全部証明書」あるいは「現在事項全部証明書」）等、申請事業者の実在を証する公的書類／定款、その他これに準ずる規程類／会社パンフレット（ある場合）
個人情報保護マネジメントシステム（PMS）文書一式（内部規程・様式全て）
個人情報管理台帳/リスク分析結果の記録された見本の、各１ページ分コピー

（３）申請費用について

種別	小規模	中規模	大規模
申請料	51,429 円	51,429 円	51,429 円
審査料	205,715 円	462,857 円	977,142 円
付与登録料	51,429 円	102,858 円	205,715 円
合計	308,573 円	617,144 円	1,234,286 円

・申請費用は左表の通り申請事業者の企業規模区分に従います。
・企業規模は下表の通り、業種と資本金、従業者数によって定まります。
・保険代理店の業種分類は、製造業・その他になります。

業種分類	小規模	中規模	大規模
	資本金の額又は出資の総額および従業者数		
製造業・その他	2～20 人	3 億円以下または 21～300 人	3 億円超かつ 301 人～
卸売業	2～5 人	1 億円以下または 6～100 人	1 億円超かつ 101～
小売業	2～5 人	5 千万円以下または 6～50 人	5 千万円超かつ 51 人～
サービス業	2～5 人	5 千万円以下または 6～50 人	5 千万円超かつ 51 人～

ちょっと一休み・・・

ＩＰＡ（情報処理推進機構）が毎年行っております**「ひろげよう情報モラル・セキュリティコンクール」**第１０回受賞作品が、昨年１２月１０日に決定し発表されましたので、その一部をご紹介します。
全国の小学生、中学生、高校生・高専生から作品を募集したこのコンクールは「標語」「ポスター」「４コマ漫画」の３部門について行われました。

受賞作品の詳細は、以下のＵＲＬにてご参照ください。

http://www.ipa.go.jp/security/event/hyogo/2014/index.html

標語部門とポスター部門の**最優秀賞作品**と、優秀賞作品の中から**弊社選んだお気に入り**を以下に示しましたので、ご覧ください。

１．標語部門

最優秀賞	**「Ｙｅｓ，ＯＫ　クリック前に　一呼吸」（中２）**
弊社のお気に入り	**「利便性　となり合わせの　危険性」（中３）** **「パスワード　英・数・記号で　複雑化」（高１）** **「おぼえよう　せかいとつながる　ぼくらのルール」（小２）** **「書き込み　一瞬　記録は一生」（高１）** **「（Ｓ）その情報　（Ｎ）流れているよ　（Ｓ）知らぬ間に」（高２）**

短い言葉の中に、システムを扱う際の注意すべきポイントが旨く表現されています。
最優秀作品が示す通り、メール送信時にはクリックをする前に、一呼吸おいてアドレス確認を行うことを習慣づけたいものです。

２．ポスター部門

最優秀賞	**弊社のお気に入り**
（小６作品）	（中２作品）
	

最優秀作品は、迷惑メールに困惑する様子が物語のように表現されている点が評価されました。

３.「やさしい情報セキュリティ」その１：パスワードについて

今回を皮切りに、計４回に亘り「やさしい情報セキュリティ」について述べさせていただきます。趣旨は、レベルが決して高くなくとも、会社全体できちんと運用できるルールを定めるためのヒントにしていただくことにあります。社内ルールがないのは大問題ですが、一方、ルールを完璧なものにしたがために運用が煩わしく、結果的に誰も守らない状態は何としても避けたいものです。

近年情報セキュリティに対する脅威がマスコミを賑わし、今やパスワードの重要性についての認識が国内全体に浸透してきました。以前のように、毎回パスワードを入力するのが面倒だからやらないという声が少なくなっていると感じています。ただ、忘れやすい、担当者が休んだ時に困るなどとして、パスワードに安易な（破られやすい）文字列を設定したり、従業員や部門の全員が同じものを使っているケースも目にします。

パスワードを破る“手口”で典型的な例は、ソフトウェアを駆使し、aaaaaaa、baaaaaa、caaaaaa・・・のように１文字ずつ変えて総当たりする方法です。この方法では膨大な回数を試行しなければならないため、いかにも単語らしい（辞書に載っている）ものを選んで回数を減らすやり方も採られます。それでも試行回数は大変な数になりますが。

ただ、このような方法でパスワードを破ろうとする対象は、インターネット上に公開されているサイト（情報）に限られます。社内で使用するパスワードであれば、攻撃者は当該のパソコンでキーボードから入力すると考え、少しレベルを下げてもいいでしょう。

次に、現実的なパスワードの運用についてポイントを数点述べてみます。

（１）アルファベットを子音のみとし数字との組み合わせに

アルファベットの単語や固有名詞は類推されやすいですが、aiueo の母音が混じる特性があります。日本語のローマ字表記では 100%。英語でも「y」を母音とすると、母音を含まない単語は「mm」（ふ～ん）などの間投詞に限られます。従って、単語から母音を抜くと他人に類推されず、自分には忘れ難いことになります。たとえば、「三四郎」→「snsr」、「吾輩は猫である」→「wghhnkdr」、「松田聖子」→「mtdsk」のようにです。文字数は「8」以上が望ましく、数字を「1964tokyo」のように前に配置するのがいいと言われています。特殊文字を混ぜると更に強固になります。

（２）パスワードの一覧表管理も

従業員が個別にパスワードを設定した場合、休んだ時にどうするかは確かに問題です。多くの企業では上長に伝えたり、隣の席同士で教え合うことが行われています。情報システム責任者が一括で管理している企業もありますが、その場合パスワードの一覧表を紙には書かず、Excel（パスワード付き）で管理する方法が採られています。

（３）パスワードの更新サイクル

パスワードは最長でも 6 カ月ごとに更新したいものです。長く同じパスワードを使い続けたため、他者に知られて“なりすまし”に遭った場合、潔白を信用してもらうのにどれだけの労力がかかるでしょう。退職者が侵入し、知っているパスワードを使ってデータを抜き取られたら大変なことになります。

（４）「試行回数」に制限を

パスワードを何度も入力・試行している内にいつかは破られるかもしれません。iPhone であれば間違ったパスコードを続けて 6 回入力すると一旦使えなくなります。同じように、Windows では「アカウントのロックアウトのしきい値」に試行回数の上限が設定できます。標準では「0」、即ち何度でも試行できるようになっていますので、ここには是非とも回数(10～20 程度か)を設定したいものです。

４．ご存知ですか！　個人情報漏えい保険

ベネッセホールディングスの顧客情報流出問題をきっかけに、損害保険大手が提供する個人情報漏えい保険への関心が高まっています。

（１）個人情報漏えい保険の概要

個人情報漏洩保険は、2005 年の個人情報保護法施行を機に各損保会社で商品化され、保険契約者を会社とする法人向け保険で、個人情報漏えい事件で被保険者である会社や会社従業員が被った損害を補償する損害保険です。

保険商品の内容は保険会社によって多少異なりますが、商品の基本的な枠組みは、賠償責任担保部分と費用損害担保部分のセット商品となっています。

①賠償責任担保部分

【保険対象となる主な損害】

損害賠償金／争訟費用／求償権の保全・行使等の損害防止軽減費用／.事故発生時の緊急措置費用

②費用損害担保部分

【保険対象となる主な損害】

謝罪広告・会見費用／お詫び状作成・送付費用／見舞金・見舞品購入費用／コンサルティング費用／弁護士への相談費用

国内の主要損保会社の取扱いは以下の通りです。

・東京海上日動「個人情報漏えい保険」
・三井住友海上火災保険「情報漏えいプロテクター」
・損保ジャパン「個人情報取扱事業者保険」
・日本商工会議所「個人情報漏えい賠償責任保険制度」
・東京商工会議所「個人情報漏えい共済制度」
・富士火災「みんなの情報ガード」

（２）個人情報漏えい保険を巡る最近の動向について

ベネッセの事件後、損保各社には中小企業などから問い合わせが急増し、大手を中心に保険加入ニーズの取り込みを強化する動きが相次いでいます。

東京海上日動では、本体部分の支払い上限を１０億円、費用部分の上限を１億円としていましたが、この費用部分の上限を数倍に引き上げました。

一方、三井住友海上火災保険は、日本商工会議所の会員企業に対して漏えい保険の加入料の割引を適用するなどして、企業への売り込みを強化しています。同社では、ベネッセの漏えい事件発覚後から「中小企業を中心に１日５０～１００件もの問い合わせが寄せられる」（広報担当）とのことです。

損害保険ジャパン日本興亜保険も４月から、情報漏れ対応のためのコールセンターの立ち上げをはじめとする支援サービスに乗り出しており、漏えい保険商品でも事後対応を手厚くして企業にアピールしています。

このように損保各社が力を入れ始めた個人情報漏えい保険ですが、まだ企業への浸透度は浅く、現状の加入率はせいぜい数%程度とみられています。しかしながら、中小企業を中心に潜在需要は大きく、経済産業省がベネッセの事件を受けて、先ごろ個人情報保護に関するガイドラインが改定され、対応強化が要求されていることから、今後は企業の対策意識が一段と高まるとみられ、同時に個人情報漏えい保険も従来以上に損保各社の販売競争も激しくなることが予想されます。

最後に、この個人情報漏えい保険は、個人情報保護態勢をしっかりとっていた、という前提で保険金が支払われるものです。個人情報保護態勢をなおざりにする代わりにはなりません。

まずはＰマークの取得等によって個人情報保護態勢をしっかり確立することが先決です。

５．トムソンネットからのお知らせ

（１）「図説：生命保険ビジネス」を発刊しました。

みなさまにご好評を戴いております「図説：保険ビジネス」シリーズの第３弾として、昨年１２月に「図説：生命保険ビジネス」を金融財政事情社より発行しました。

これまで生命保険を取り扱った本は数多く出版されていますが、その内容は、生保商品の仕組みやライフステージでどんな保険が必要か、あるいはどんな商品が有利かといったものが大半で、生命保険事業自体が扱われることは稀でした。

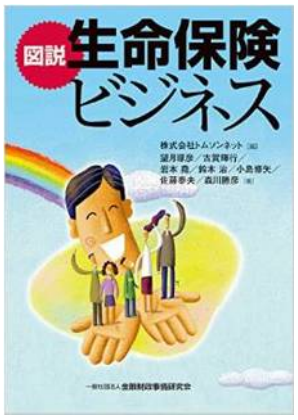
このため、今回の「図説：生命保険ビジネス」においては、国民一人当り契約金額世界ＮＯ１を誇る生命保険事業に照準を当て、個人マーケットが成熟するなか、商品・販売チャネルの多様化を進めてきた生命保険会社が直面する課題と、今後お客さまから求められる役割等を丁寧に説明しています。

本の構成は、見開き２ページで１テーマを採り上げ、左ページに文章、右に図説とわかりやすい構成になっていることも特徴です。

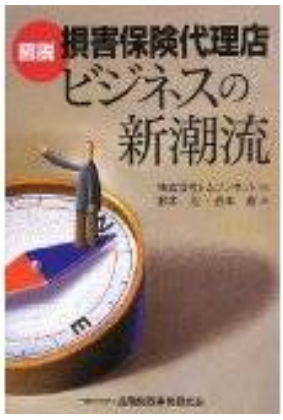
生保ビジネスに携わる新入社員から役員の方に至るまで、幅広くご利用戴けるものと確信しております。是非、ご購入をご検討下さい。

また、既刊の「図説：損害保険ビジネス」「図説：損害保険代理店の新潮流」も併せご購読をお願いします。

新発売



図説シリーズ既刊



以上

Ｐマークやシステムについての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　　本間　晋吾 ℡ 090-2762-4623