Pマークニュース ＜２０１８年新春号＞　Vol.　２２	（株）トムソンネット Pマークコンサルティンググループ

１．Pマークの遵守規格 JIS Q 15001：2017が公表されました
２．「やさしい情報セキュリティ」その１２：ビジネスメール詐欺
３．2017年の保険代理店におけるPマーク取得動向について
４．お知らせ

１．Pマークの遵守規格 JIS Q 15001:2017が公表されました

改正個人情報保護法が2017.5.30に施行されたことに伴って、個人情報保護に関するJIS Q 15001が改訂され、公表されました。前回の制定が2006年ですから、11年ぶりの改訂です。この規格はPマークの遵守規格ですから、Pマーク取得事業者の遵守規程も変わってきます。公表されたJIS Q 15001:2017を解説します。

（１）公表されたJIS Q 15001:2017

下記のように５編の構成になっています。

本文	マネジメントシステムに関する要求事項を記載	JISQ15001:2006の本文規程要素に該当
附属書A (規程)	管理目的及び管理策	JISQ15001:2006の本文規程要素に該当
附属書B	管理策に関する補足	参考　審査必須でない
附属書C	安全管理措置に関する管理目的及び管理策	参考　審査必須でない
附属書D	新旧対応表	参考

全体として、個人情報保護法ガイドラインと比肩できるような具体例示・丁寧な表示が多くなっており、「解説」では、改正に当たってこの規格が「民間部門の個人情報保護の促進及び消費者保護に重要な役割を果たしていることから，要求事項の基本的な考え方を変更せず，旧規格に基づいて構築された個人情報保護マネジメントシステムがこの規格の改正によって不適合を生じないことに配慮」したとしています。

しかしながら、この附属書A(規程)の各規格は一読して内容を把握するのは難しいものです。

例えば、本文の「１.用語及び定義」では、「この規格で用いる主な用語及び定義は，個人情報保護法による。その他の主な用語及び定義は，次による。」となっており、法が新たに定義した「個人情報」「要配慮個人情報」「匿名加工情報」などについては「個人情報保護法による」のみで、「その他の主な用語及び定義」が46項目規定されています。また、法に新たに明記された「オプトアウト」に関する条文(法２３条第２項から第４項、規則第７条から第８条、規則第１０条)は、「個人データの提供に関する措置」(附属書 A(規程)A3.4.2.8)のただし書き b)に「・・・・法令等が定める手続に基づいた上で，・・・」と規定しているだけで、オプトアウトの際には、個人情報保護委員会への届出が必要なことなどを

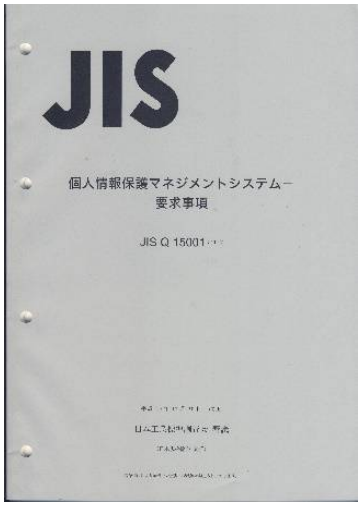
類推しなければなりません。JIS Q 15001:2017 は、当然に改訂個人情報保護法を踏まえた規格ですから、改正法を理解し遵守しなければならないことを考えると、ややこの辺の記述は不親切でわかりにくいと言えます。

一方で、附属書 C には「参考」ではありますが、「安全管理措置に関する管理目的及び管理策」として、14 項目にわたる管理目的及び管理策があります。これらは JIS Q 27002:2014 の箇条 5 から箇条 18 を基に作成されたものとしていますが、注目です。
JIS Q 27002 は、「情報セキュリティマネジメントのための実践規範」として「情報資産」を対象としているのに対し、JIS Q 15001 は「個人情報」という必ずしも資産性のないものも対象とした規格です。JIS Q 15001:2017 の規格「リスクアセスメント及びリスク対策」では「特定した個人情報の取扱いについて，個人情報保護リスクを特定し，分析し，必要な対策を講じる」(附属書 A(規程)A3.3.3)ことが求められ、「必要な対策を講じる」とは「分析した個人情報保護リスクに対し，その評価に相応し，組織の事業内容又は規模に応じ，経済的に実行可能な最良の技術の適用に配慮することである。」とされており、一律な安全管理措置を求めていません。

（２）公表されている今後のスケジュールについて

①改正 JIS の公表　　2017.12.20
②改正 JIS の審査基準の公表　　2018.1.12
③改正 JIS の実施ガイドラインの出版　　2018.の春頃
④移行準備期間　　2018.1.12 から 2018.7.31
⑤新規申請　現行の審査基準による新規審査の申請締切日　　2018.07.31
⑥新規申請　新基準による新規審査の申請受付開始日　　2018.08.01
⑦更新審査　現行の審査基準による更新審査の申請締切日　　2020.07.31
⑧更新審査　新基準による新規審査の申請受付開始日　　2018.08.01

（３）審査基準(2018.1.12 公表)はどうなるのでしょうか?



公表された主たる新審査基準は下記のようになります。
①次の事項に関する審査は原則として**文書審査で確認**する。
文書化された内部規程の有無
内部向け個人情報保護方針に定める事項
外部向け個人情報保護方針に定める事項
保有個人データの開示等の請求等に応じる手続きとして定める事項
②文書審査での PMS 文書の**用語**は規格と同一であることは必須ではない。
③3.3.3 リスクの認識、分析及び対策では大きな変更をしておりますが、**現行 JIS のもとでのリスク対応もそのまま受け入れられる**と思われます。**「現状で実施し得る対策を内部規定として文書化し、それが講じられていること」を審査基準としています。**
④付属書 C は、**参考であり、審査基準ではない。**
⑤匿名加工情報の取扱い方針については、文書化した情報でなく、トップマネジメントでの説明でもよい。
⑥2006 版規格は規格各項毎に承認手順を要求していたが、一括して規定することができるとしたため(付属書 A の A3.1.1)、審査項目数は現行の 1/3 くらいになるのではないかと推測されます。

弊社では、2017 年版 JIS 規格、その審査基準の公表内容にそって、「PMS 基本規程」をはじめとする規程類の改訂作業を続けています。2018 年夏頃といわれています「改正 JIS の実施ガイドライン」も参考に最終案を作成の予定です。

２．「やさしい情報セキュリティ」その１２：ビジネスメール詐欺

昨年４月、IPA（独立行政法人情報処理推進機構）から「サイバー攻撃の情報共有の枠組み、複数の企業から**“ビジネスメール詐欺”**に関する情報提供を受けました。

そこで、その事例を詳細に解説し、手口を明らかにするとともに、国内企業に潜行していると考えられる“ビジネスメール詐欺”について注意喚起を行います。」との公表がありました。その時分は標的型攻撃やランサムウェアほど話題にはなりませんでしたが、昨年暮れに JAL（日本航空）が前後数回に亘り総計３億 8,400 万円もの被害に遭ったことが発表され、俄然クローズアップされています。警視庁もホームページで警戒を呼びかけています。

以下、ビジネスメール詐欺（別名“外国送金詐欺”“企業版オレオレ詐欺”）について、状況と対策などを述べてみたいと思います。

（１）ビジネスメール詐欺の手口

ビジネスメール詐欺は、取引先とのメールのやり取りに割り込む形でニセのメールを送りつけ攻撃者の用意した口座へ送金させる詐欺の手口です。要は“なりすまし”です。

標的型攻撃以上にその企業の事情を知っているような内容のメールになっており、時には取引のある２社を相手にすることがあるため、取引内容や支払条件も本物と区別が付かない位ですが、“口座が変わった”“至急”がほぼ共通に含まれており、振込口座は海外のものです（JAL の場合は香港）。

“取引先”に限らず、社長や上司を語って担当者への振込みを要請するケースもあるようですから、特に経理・出納担当の人には注意や鋭い“直感”が望まれます。

（２）ビジネスメール詐欺の兆候

国内での実例ではメール本文が英語です。ただ、いつ日本語に堪能な悪人が頭をもたげるか・・時間の問題と思います。ともかくは、振込口座が海外、内容に、“口座の変更”“至急”に類するの言葉が含まれているものは絶対に要注意です。

併せて重要なことは、どこかでメールアカウントが盗まれていることがそもそもの原因です。他の脅威と同じく、怪しげなメールが届き始めると兆候が現れたと考えられます。

（３）詐欺メールの見分け方

IPA や警視庁の発表では、本物とよく似たアドレスでメールを送り付け、その返信がきっかけになっているケースが多いようです。

■本物のメールアドレス　allce@company.co.jp

■偽物のメールアドレス　①allce@compnay.co.jp

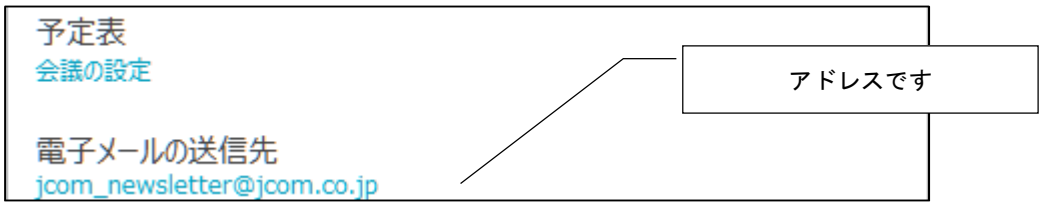
②allce@compny.co.jp

③aallce@company.co.jp

④allce.company.co.jp@freemail.com

①②③は、注意深く見るしかありません。④は、ドメイン（@の後）が企業のものではなく個人用ですから、取引先ではないとすぐ分かるでしょう。

上のような表示がでない場合、「差出人」（Outlook の場合）をクリックすると下のようなサブウィンドウが開くと思いますので、その［電子メールの送信先］でアドレスが表示されます。



（4）対策

ビジネスメール詐欺の被害に遭わないようにするには、まずこのような攻撃があるということを知るのが第一歩です。その他次のようなことが挙げられます。

①確認したい時は「To」に取引先の入力を（そのまま返信は禁物。偽ったアドレスに送信される）
②口座の変更など極めて重要な事柄には電話で確認を（メールでの確認は禁物）
③普段とは異なるメールに注意（突然英文になった、言い回しが丁寧/親しげになった等々）
④不審と感じた場合の組織内外での情報共有（支払いに係るメールには複数人での確認等々）
⑤ウイルス・不正アクセス対策（そもそものきっかけの可能性大。メールサーバへの不正侵入も）

JAL が被害者に陥ったのに対し、スカイマークは③で免れています。

最後に。ビジネスメール詐欺は「兆候」にもあるよう、メールアカウントが盗まれている可能性が大です。と言うことは、システム全体への侵入、ひいては個人情報を含む企業の秘密情報の流出も懸念されます。メールの脅威に対する基本的な動作がビジネスメール詐欺にも功を奏することを再認識したいものです。

＜ご参考＞タイミング良く、1 月 30 日に IPA(情報処理推進機構)が「情報セキュリティ 10 大脅威 2018」の順位を発表しました。その中で“ビジネスメール詐欺”が 3 位にランクインしています。詳細説明は 3 月に公開されることとしています。

■「情報セキュリティ 10 大脅威 2018」　NEW：初めてランクインした脅威

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	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 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォンアプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃によるサービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化（アンダーグラウンドサービス）	9 位

３．2017 年の保険代理店における P マーク取得動向について

（１） 伸びを欠いた新規取得

2017 年は、前年に施行された保険業法の改正、さらには同年 5 月に施行された個人情報保護法改正という大きな法制度の改訂があったため、保険代理店においても個人情報保護強化の重要性が高まり、従来以上に P マークを取得する保険代理店が増加することが予想された年でした。

しかしながら結果は、下表が示す通り予想とは裏腹に P マークを**新たに取得した保険代理店は 11 社に留まりました。**

保険代理店の P マーク取得は、年間 22 社が新規取得という飛躍な伸びがあった 2012 年を境に、その後はここ数年、保険代理店の P マークの年間新規取得社数は 15 社以上と着実に増加を続けていただけに意外な結果となりました。

2017 年末時点における P マーク取得保険代理店数は 132 社になっています。

前年（2016 年）末（128 社）比では、11 社の新規取得がありましたが、既取得先の 7 社が継続更新を行わなかったため、年間増加は 4 社と低い伸びとなりました。

年度	2013 年	2014 年	2015 年	2016 年	2017 年
新規取得数	17	16	15	15	11

2017 年に P マークを新規取取得した 11 社の取得時期は下表の通りです。

1 月	2 月	3 月	５月	７月	９月	12 月
１社	１社	3 社	１社	2 社	１社	2 社

① 2017 年の年間取得が 11 社と低調に推移したことは残念ですが、それ以上にショックなのは P マークの継続更新を行わなかった代理店が 7 社と多くを数えたことです。
P マーク取得の必要性が叫ばれるこの時期だけに看過できない問題であり、更新時の問題等の把握が必要と考えています。
2017 年新規取得の 11 社のうち、本社所在地「東京」が 6 社、後は埼玉、大阪、愛知、奈良、香川がそれぞれ 1 社ずつとなっています。
なお、奈良、香川においてはそれぞれの県における P マーク取得第一号の保険代理店の誕生です。

（２）2018 年の動向を予測する

今年（2018 年）の保険代理店における P マーク取得動向の予測ですが、以下の理由により昨年の低調を補う形で増加することが予想されます。

① 保険業法改正以降、保険代理店の経営者は金融庁等の動きから、顧客情報、特に個人情報の保護の必要性は感じており、漸く昨年で業法改正対応は一段落し、P マーク取得が経営課題に遡上してきたとの声を聞く機会が多くなっている。
② 個人情報保護法の改正を受けて JIS Q 15001 も昨年改正が公表されたが、旧制度による P マーク取得申請の受付が 2018 年 7 月末までとなるため、「P マークを取るなら今！」との駆け込み申請が増えることが見込まれる。

５．お知らせ

（１）「P マーク取得は今がチャンス！」

これまでにも本誌面において、JIS Q 15001 の改正を受けて、「P マークを取るなら今がチャンス！」と呼びかけて参りましたが、旧制度による取得申請が今年の 7 月末で終了することが明らかになりました。

P マークの取得は制度運用の固まっている旧制度で申請取得した方が、現時点では審査等がスムーズに運ぶ可能性が高く、弊社では P マーク取得を検討されている保険代理店様に早期申請を強くお勧めしております。

2 月中に検討を開始できれば、7 月末申請は十分可能です。

まずは、弊社（下記）にご連絡をお願い致します。

（２）4 月入社の新人教育は弊社の生損保公開講座にお任せください

新入社員の早期戦力化には、適正な業務知識教育が必須です。

日々お忙しい保険代理店のみなさまにおいては、自社内での教育・研修は負荷の高いものと、推察いたします。

就きましては、多くの保険関係の企業でご利用戴き好評を得ております弊社の生損保研修をご利用下さい。**公開講座の日程は弊社ホームページをご覧ください。**

Ｐマーク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）

以上