Ｐマークニュース ＜２０１９年新春号＞　Vol.　２６	（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．改訂 JIS(JIS Q 15001:2017)の運用（その２）

前号に引き続き、個人情報保護法(含むそのガイドライン)及び「実践ガイドブック」を参照しながら、改訂 JIS の補完をできればと思います。簡単なようで規程が複雑な**「第三者提供」**についてです。

この規程は、JIS 規格はあっさりしていますが、法とガイドラインはしっかりと規定していますので、JIS 規格・法・ガイドライン・実践ガイドラインを縦覧して整理します。(「実践ガイドブック」とは「JIS Q 15001:2017 対応　個人情報保護マネジメントシステム導入・実践ガイドブック」日本規格協会刊)

（１）「第三者提供」の取扱いの基本

「提供」とは「第三者が個人情報を利用可能な状態に置くこと」です。「提供」に関する個人情報の取扱い規程で必要とされるのは**「本人の同意」**を得ることです。また、この規程は個人情報保護法(以下「法」という)で定義されている**「個人データ」について適用**され、「個人情報」については適用されません。自分(自事業所)の個人情報が、自分(自事業所)の知らないうちに、第三者に利用されることを法で規制しているのです。

法と JIS Q 15001:2017(以下 JIS 規格という)は、「提供」を以下のように規定しています。

区分	規定している内容
法の「提供」に関する規定項目	①提供制限の原則（同意取得） ②オプトアウトによる第三者提供 ③第三者に該当しない場合 ④外国にある第三者への提供の制限 ⑤第三者提供に係わる記録の作成等 ⑥第三者提供を受ける際の確認等
JIS 規格における「提供」に関する規定項目	①個人データの提供に関する措置 ②外国にある第三者への提供の制限 ③第三者提供に係る記録の作成等 ④第三者提供を受ける際の確認等

（２）「第三者提供」規程適用の例外

①留意したいのは、「第三者」でなく、**「本人」又は「自事業所」へ「提供」**する個人情報の取扱いです。「第三者」に該当しませんから「提供の同意取得」あるいは「オプトアウトの手続」が「不要」で、「提供」ができます。

ａ）本人による提供個人情報(SNS 上で投稿者のプロフィール・投稿内容等の取得の場合)

ｂ）本人と一体と評価できる関係にある者への提供個人情報(本人の代理人又は家族など本人側への「提供」と見なされる場合)

ｃ）同一事業所内で他部門に提供する個人情報

ｄ）本人との関係において提供主体である事業者と一体のものとして取扱うことに合理性がある個人情報(**「委託」**に伴う個人情報、**「事業承継」**に伴う個人情報、**「共同利用」**に伴う個人情報)

保険代理店で取扱う保険申込一件書類は「委託」に伴う個人情報であり、上記ｄ）に該当します。

②法の規定する「第三者提供」規程は、「個人データ」について適用され、「個人情報」については適用されないとしていますが、JIS 規格では、「特定した『個人情報』については、『個人データ』と同様に扱わなければならない」と規定していますので、**Ｐマーク取得事業者では、特定しているすべての個人情報に適用となります。**

③「第三者提供」に該当しますが、法及び JIS 規格により、「提供の同意取得」が必要でない場合は下記です。

ａ）　法令に基づく場合

ｂ）　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

ｃ）公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

ｄ）国の機関若しくは地方公共団体又はその委託を受けた者が、法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれがあるとき

ｅ）既に「取得時」あるいは「連絡・接触時」に本人の同意を取得している場合

ｆ）オプトアウトの場合

ｇ）法人その他の団体の役員に関する場合

（３）「同意」の必要性について

SNS 上に投稿者本人がプロフィール・投稿内容等を提供することについては、「本人からの提供」ですから、上記のとおり「同意」は必要ありません。しかしながらこれには、留意が必要です。ネット上で、次々に拡散され、炎上するという本人が思いもよらない状況が起こることも想定されます。この際に「個人データ」を「消し去る権利」「取り戻す権利」は

現行法では、規定されていません。(EU では GDPR によって、これらの権利を法定しています)現行法の改定が待たれるところです。

「第三者提供」の同意取得については、できれば省略したいものですから、無理な解釈もみられます。例えば、**団体契約の際の「団体構成員の個人情報」の取扱い**について、「募集コンプライアンスガイド」(2017.4.25 日本損害保険協会)に掲載がありますが、やや無理があります。団体が保険料を試算するために個人データを代理店へ「提供」する場合は、同意は「不要」としています。その理由は法第 23 条第 1 項第 2 項に該当するからとしています。「人の生命、身体又は財産の保護のために必要がある場合であって、**本人の同意を得ることが困難であるとき**」ですが、団体がその構成員の同意を得ることは困難でしょうか？ 拡大解釈です。団体が福利厚生の一環としてその構成員の個人情報を利用することについては、やはり何らかの形で同意が必要と考えるべきでしょう。実態としてはほとんどの事業者が、利用目的の通知あるいは公表までは行っており、同意取得までには至っていないものの実態的な同意は得ていると考えられますが。

代理店が団体構成員の個人情報を取得することは、「委託」業務の利用目的範囲内の行為であり、代理店での同意取得は不要と考えます。

（4）ネットワーク上の「提供」について

個人情報が物理的に「提供」されていない場合であっても、第三者がネットワーク等を利用することにより個人情報を利用できる状態にあれば、「提供」にあたります。従って事業者がホームページなどに従業者の個人情報を掲載する際は、利用目的を特定の上、従業者本人の「提供に関する同意」が必要です。

ネットワーク上の個人情報を、記録せずに**単に「閲覧」する行為**については、「提供を受ける行為があるとは言えない」とガイドラインは解説しています。「提供を受ける」個人情報については、法もＪＩＳ規格も、「提供」の規程の続きとして、第三者提供を受ける際の確認等を規定しており、「提供を受ける」個人情報の「取得」についても規定していますが、「単に「閲覧」する個人情報」は、**法も JIS もその取扱いを何ら規制していません**。「閲覧」する本人の良識に従うということでしょうか。自覚したいものです。

２．事例に学ぶ：「危険メール」の防御策　～標的型攻撃、BEC 等に備えて～

事例シリーズの第 3 弾になります。今回は標的型攻撃や BEC（ビジネスメール詐欺）など諸悪の根源とも言うべき、「危険メール」について述べさせていただきます。

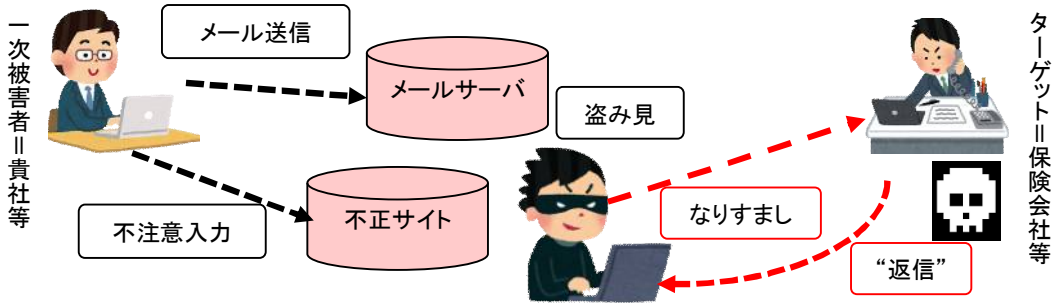
危険メールはウィルスを含むメールとは限りません。数年前からはウィルスを含み、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェア全体を「マルウェア」(Malware)と呼ぶようになりましたが、恐らく各社でお使いのウィルス対策ソフトは“マルウェア対策”まで行っていると思います。また、UTM(Unified Threat Management：統合脅威管理)やサンドボックスを導入して大変強固なセキュリティ対策を整えている会社さんもあるでしょう。

とは言いながら攻撃者は日々巧妙、且つ執拗になり最後のトリデは担当者の“目利き”に委ねられることになります。

（1）サイバー攻撃を受けると致命傷にも

被害に遭った場合、個人としてはクレジットカードの悪用、口座からの不正引落しが怖いでしょうが、企業としては“信用失墜”、特に取引先への被害波及でしょう。ある統計（HP 社）では、“サイバー攻撃を受けた中小企業の 60%は 6 ヶ月以内に業務停止まで追い込まれている”旨の報告がされています。

典型的な例が“なりすまし”に遭うことです。ある会社の人（一次被害者）のアドレスで顧客や取引先（ターゲット）の担当者にメールを送って信用させ、ターゲットの PC やサーバに不正ソフトを仕込ませるケースです。そもそもが一次被害者またはターゲット社員のメールアカウントが悪用されたことが原因です。ともかくは各社においてアカウントを盗まれない・乗っ取られないようにすることが先決です。



（2）差出人（送信者）アドレスのチェックを

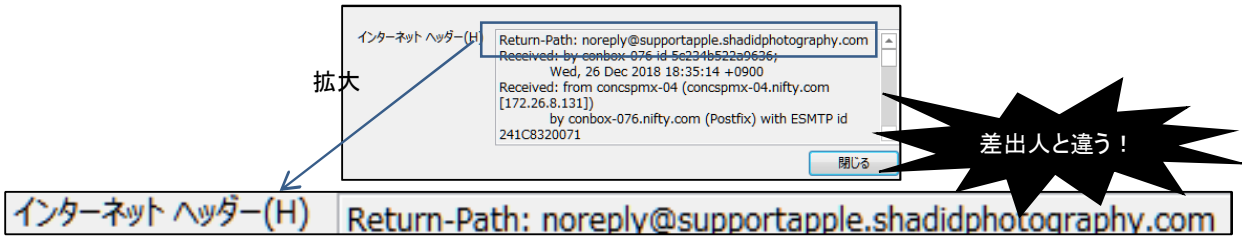
危険メールの見極めの第一歩は「差出人」です。一般に、メールソフト（メーラ。Outlook など）の受信メール一覧で見えるのは「(差出人の）表示名」で、アドレスではありません。下の例（実例です）受信フォルダには「Amazon」のみが見える筈です。

「表示名」はメーラの設定で簡単に変更できます。「アドレス」はメーラでは設定できませんが、メールサーバを構築できる技術力があれば何にでも設定できます。「アドレス」の“@”以下を「ドメイン」と呼びます。このドメインが実在する会社名を表しているかがポイントです。上記の例では“rakuten”の後の“mtv”が怪しいと気付くべきです。また、正規の“◍◍◍.co.jp”の後に更に“.cn”や“.uk”などが付いていたら完璧にアウトです。

（3）返信先のチェックを

なりすましメールは「差出人」に一次被害者のアドレスを使いますが、ターゲットからの返信を自分のアドレスに設定します。一次被害者を返信先にすると、一次被害者本人が返信メールを見て気付くからです。

返信先アドレスを調べるのは「(メールの) ヘッダー」です。Outlook の場合は、当該の受信メールを選択し、[オプション]をクリックすると受信したメールのプロパティが表示されます。ヘッダーの先頭に出てくる「Return-Path:」以下がそれです。通常送信アドレスと返信先アドレスは同じはずです。異なっている場合や返信先アドレスがない (空欄) というのは問題です。



（4）メールアカウントの乗っ取り対策はあるのか

結論としては“完全な対策はない”としか言わざるを得ません。Ｐマークで言えば“残留リスク”です。強固と言われた「WPA2」も心細くなっている程ですが、人間系としてできるだけの注意は払いたいものです。各種のガイドラインには①ID とパスワードの使い回し禁止、②パスワードには類推が困難な文字列を、③不用意にメールアカウントを入力しない、等々の注意喚起をしています。

加えて、“会社のアドレスを私用に使わない”を再徹底しませんか。特に通販の注文、SNS などの会員登録は絶対に禁止すべきです。一言で言えば、仕事上の必然性がない限り入力フォームに会社のアドレスをインプットするのは厳禁です。ましてや、“FacebookID でログイン”など、「OAuth」(オーオース) 認証には決して応じないよう周知徹底しましょう。

（5）まとめ

「働き方改革」の時流に乗り、社外での就業が普及することなどを背景として情報セキュリティ強化のツール類が一段と賑やかになっています。AI を活用し機能が充実するのは喜ばしいのですが、“人間の目”がどうしても残ります。乗っ取り防止のため、向後も適宜“目利き”と防御の参考にしていただけそうな事例を紹介していきたく思っています。

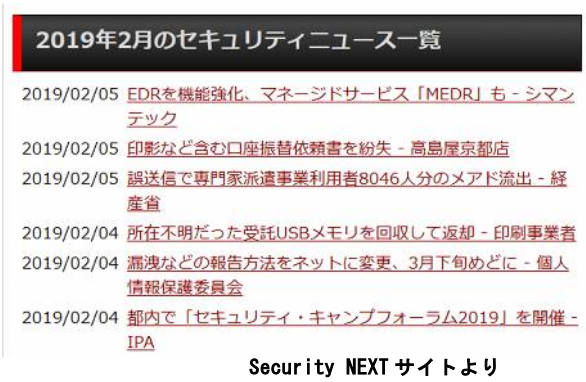
３．個人情報保護および情報セキュリティ対策は情報収集から

今年も年明けから個人情報に係わる様々なニュースが飛び交っています。こうした個人情報の事故やあるいは情報セキュリティの動向に関するニュースは、企業におけるシステムや個人情報保護の担当者はもちろんのこと、トップマネジメントにおいても情報を収集し、動向を把握することが肝要と思われます。しかしながら、情報収集といっても、常に数多くの新聞やテレビ等に接して、個人情報等のニュースを洩らさず収集することは、現実的ではありません。

そこで、日々お忙しいみなさんに、個人情報の保護や情報セキュリティに関するお勧めの情報収集方法をご案内します。

（１）個々の個人情報の漏えい事故の発生や情報セキュリティシステムの動向を把握する

個人情報の漏えい事故等は、通常は新聞等のマスメディアから情報入手することが一般的ですが、各種メディアに紹介されたセキュリティ事故やウイルス動向、さらにはセキュリティシステムに関するニュースをネット上で網羅的に掲載している便利なサイトがあります。



Security NEXT サイトより

ご存知の方も多いと思いますが「Security NEXT」の情報セキュリティニュースです。

（http://www.security-next.com/）

このサイトを毎週一回チェックすることで、前述の個人情報漏えい事故等は概ね入手することが出来るといっても過言ではありません。加えて過去の情報に関しても、10 年以上遡って調べることが可能な大変有用性の高いサイトです。

また、情報処理推進機構（IPA）が、前年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、年初に毎年発表している「情報セキュリティ 10 大脅威」、（https://www.ipa.go.jp/security/vuln/10threats2019.htm）もセキュリティ対策を講ずる上では、目を通したい情報です。

（２）個人情報の漏えい事故等に関する統計情報を知る

国内で発生した個人情報漏えい事故に関する（年間）統計情報は、事故の傾向等を知る上で有意です。この分野の統計情報では、以下のネット公開している資料が充実しています。

①日本ネットワークセキュリティ協会(JNSA)では、新聞等に発表された個人情報漏えい事故を集計し、年間レポートを作成し、公表（https://www.jnsa.org/result/incident/）しています。個人情報漏えい事故の発生件数に始まって事故に伴う推定損害額や、原因別、業種別、漏洩メディア別等様々な切り口から個人情報漏えい事故の分析を行っています。

②P マーク制度の元締めである日本情報経済社会推進協会（JIPDEC）では、P マーク取得事業者からの事故報告に基づき「個人情報の取扱いにおける事故報告にみる傾向と注意点」と題するレポートを毎年公表しています。事故の要因分析等の他に対策等に就いても触れており参考になります。因みに平成２９年度のレポートは以下に掲載されています。

（https://privacymark.jp/system/reference/pdf/H29JikoHoukoku_180831.pdf）

セキュリティ情報の収集・把握は、セキュリティ対策の第一歩として効果的と思われます。

４．お知らせ

トムソンネットが、代理店様の情報セキュリティへの取組状況等を監査します

弊社は、経済産業省が定める「情報セキュリティ監査制度」に則った監査を実施する「情報セキュリティ監査企業」として、「情報セキュリティ監査企業台帳」に登録されています。

IT 技術の進化に伴って、各業務のシステムへの依存度が高まっている現在、システムの問題は、経営の課題と言えます。

このため、各企業・組織においては、情報セキュリティリスク抑制や、顕在化した場合の影響最小化に向けて、「情報セキュリティマネジメト」をはじめとする種々の対策を講じられていますが、変化・進化する IT 技術や社会環境の下で、必要とされる情報セキュリティ対策も変化・進化し続けられることが求められ、その対応に追われている状況にあると思われます。一方、情報セキュリティ対策の充実には、それなりの労力・コストが必要となり、対策強化をどこまで行い続ければいいのか悩まれている保険代理店様も多いのではと、推察いたします。

斯かる状況下、トムソンネットでは、保険業務に精通したシステム経験豊富なスタッフが、「保険代理店、ブローカー、少額短期保険」を対象に、情報セキュリティリスク対策について、網羅性や妥当性、経済合理性を考慮した適切な対策が講じられているかを確認・評価を行うサービスを提供しています。

具体的には、代理店様の情報セキュリティ取組状況を評価し、業務特性・規模等踏まえた適切なセキュリティ管理態勢構築の提案や支援を行います。

就きましては、弊社の上記サービスにご興味やご関心をお持ちの方は、是非、下記にご一報戴きたくお願い申し上げます。

弊社へのご連絡・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