Ｐマークニュース

＜２０１８年陽春号＞　Ｖｏｌ．２３

（株）トムソンネット

Ｐマークコンサルティンググループ

２０１８年陽春号目次

１．更なる個人情報保護の強化へ

―EU 一般データ保護規制(GDPR)を読み解く―

2018.5.25 には EU 一般データ保護規制(GDPR)が施行されます。この GDPR を読み解き、これからの個人情報保護施策の方向性を探ります。

「個人情報保護」を基本的権利として認識し、その定義を厳格にして、その権利の保護、処理、移転、などについて規制した上で、「執行と制裁の強化」を明確にしています。日本では、2017.5.30 個人情報保護法が改正施行され、2017.12.20 には P マークの基準である JIS Q 15001 が改正公表されたばかりですが、グローバル化のなか再度の改正が必要でしょう。

EU 一般データ保護規制(GDPR)は、1995 年の EU データ保護指令に代わり適用されます。EU データ保護指令は OECD8 原則(1980 採択年)を踏まえて定められています。(なお、各国でも制定されており、日本でも 2005 年に初めて個人情報保護法が施行された経緯があります)

GDPR は 173 項目の前文とともに、99 条にわたる規制事項がきめ細かく定められています。おもな規制をその背景とともに考えます。

①**「EU 域外への持ち出し原則禁止」**です。メールアドレスやクレジットカード情報を域外にいる第三者が見られることにすることを原則禁止し、欧州市民との商売に係わる個人データ、出張や旅行で域内にいる日本人の個人データ、欧州の従業員の個人データを日本で管理する場合などの持ち出しが禁止されます。グローバル企業なら大抵が規制対象になります。ただし、十分な保護対策を講じている国である場合(日本はこの十分性認定を取り付けつつある)、データ主体者の明確な同意がある場合、所定の契約書(標準契約条項の締結あるいは拘束的企業準則の策定)のルールに従っている場合などは持ち出しができるとしています。

②**「データポータビリティの権利」**です。個人は自分が企業に提供した個人データを取戻し、他の企業に移す権利を明記しています。この背景にあるのは、**IT の巨人(グーグル、アップル、フェイスブック、アマゾンのいわゆる GAFA)による個人データ独占の新たな脅威です。**電子決済サービスの利便

性も AI による自動運転の性能も、この大量のデータ資源に左右されることを考えれば個人データの争奪はグローバルな新たな経済覇権争いです。また、こうした個人データの独占への対抗規制でもあります。

③**「忘れられる権利」**です。GAFA などのプラットフォーマーや SNS 等で取得された個人データは、本人の意思に関係なく保持され続けられ、プライバシーに関わる個人情報等は時にネット上の「炎上」問題を引き起こしています。「個人の権利の強化」を明記したものです。

④**「AI 等の自動処理のみによる評価・決定への拒否権」**です。この明記もまた「個人の権利の強化」です。AI で利用された個人データの正当性を確認することなどを踏まえています。

⑤**「執行と制裁の強化」**です。GDPR への違反企業は、全世界の年間売上高の４%若しくは 2000 万ユーロ(1 ユーロ 125 円とすると 25 億円)のどちらか高い方を上限とする制裁金を科すことを明記しています。2018.3.17 フェイスブックからの個人データ流失事故が報じられました。同社が学術調査の目的でケンブリッジ大の教授と正式に契約して提供した個人データが、契約に違反して横流しされ、流失したもの。8700 万件に及ぶ。同社は管理が及ばないこととして、責任を否定していましたが、2018.4.9 マーク・ザッカーバーグ最高経営責任者(CEO)は「悪用防止が十分でなく、我々の責任について十分見渡せていなかった。」として対応の不備を認めました。2012 年、グーグルが閲覧履歴の取得手法を問題視され 2250 万ドル(約 24 億円)の制裁金を命じられましたが、今回の対応策が遅れれば GDPR ルール違反の恐れも出てくると思われます。強力な規制の明記です。

「個人データ」の取扱いをめぐって起こる種々の課題は、どこか遠いところの**異世界の問題ではありません。**単一民族である日本は、欧米に比して「個人情報保護」に対する意識が低いと言われてきました。しかしながら、街頭で 10 人に 3 人は外国人に会うというグローバル化している時代に、日本だけの価値観は成り立ちません。先進国の自負として「個人情報保護」が本人の基本的価値であることをまず再確認する必要があります。

次に個人情報の取扱いです。我々は日常的に取り扱う個人情報に更なる留意が必要です。
我々が日常的に利用している GAFA のサービスが持つ個人情報の取扱いも留意すべき課題です。GAFA の提供するサービスに利便性と危うさの両面があるからです。

例えばパスワードなしの処理。「戸締まりなしの外出」とも言えます。セキュリティの心配のない田舎の生活ならともかく、そうでなければ必須です。あるいはセキュリティソフトを導入していない、あるいはその更新がされていない OS の利用。「雪道のスノータイヤなし運転」とも言えます。運転に自信がある自分への過信は、ひょっとすると他人への大事故に繋がります。ネット社会では一人の誤処理がたちまち全体に拡散しかねません。

しかしながら、現状は一向に進展をみていません。保険代理店の P マーク取得は 135 件前後にとどまっています。全業種では 15800 件近い P マーク取得事業者のなかで、1%にも満たない状況です。これは、保険会社が何とかしてくれるという伝統的（？）な保険代理店の体質からでしょうか？　それとも保険代理店を中心に P マーク取得を薦めている弊社の進め方が的を射ていないからでしょうか？　この取り組みを定年後の社会的貢献？？と思いあがっていた結果でしょうか？　自虐的な問いの答えは得られないまま、「個人情報保護」の欧米の流れは、次のステップへと進んでいます。

２．保険代理店様における個人情報保護への取り組み（３）

前々号に続き、保険代理店様における個人情報保護への取り組みをご紹介します。
今回は、株式会社ワイズメンコーポレーション様でＰマーク運営に携わっている取締役の安里様に弊社からのＰマーク関連の質問にお答え戴きました。

Ｑ１：標的型攻撃メールやランサムウエアといったネットワークを介した個人情報漏えい事故が脅威になっていますが、何か対策は講じられていますか。

Ａ⇒　ランサムウエアに対抗する最善策は、メール、Web、アプリケーション、ネットワークを包括的に保護する堅固なセキュリティです。弊社ではUTM（Unified Threat Management／「統合脅威管理」）を設置し外部から入る際に潜む脅威を検出するシステムを取り入れています。しっかり監視をするとともに自動的に悪意のあるコンテンツや挙動をブロックしています。その防御をもすり抜け攻撃を受けデータを失った場合であっても業務を復旧することができるデータバックアップシステムも取り入れています。ランサムウエア攻撃を受けた場合、必ず業務が止まってしまいます。
第一段階の防御の次は被害にあった際の復旧のスピードと考え対策としています。

Ｑ２：個人情報に囲まれて業務を行っている保険代理店のＰマーク取得が中々進まない現状があります。その原因は何であると思われますか。

Ａ⇒　弊社がプライバシーマークを取得したのが2012年4月です。
取得を目指して運用を始め、取得するまでは1年近く掛かりました。他代理店の中でも取得の方向へ進みつつ取得に至らなかったというケースも聞いております。
取得までの準備等の煩わしさが先行して進まなかった部分は感じられます。今、この保険業界においては体制整備が義務付けられております。
2016年5月29日改正保険業法施行以前は保険会社に対して体制整備義務が課されていました。
しかし、改正保険業法の施行によって、保険募集人自身にも体制整備が義務付けられるようになりました。体制の整備の方法は、保険代理店の規模よって分けられますがこの保険業界の扱う物ほとんどは個人情報です。個人情報の取り扱いについてはどの業界よりも慎重に厳しく取り扱わなければならない業種です。体制整備を整え高いレベルのルールのもと運用することになっている今、この流れの中においてプライバシーマークの取得は取り組まざるを得ないものになるのではないでしょうか。

Ｑ３：Ｐマークの運用局面においてもコンサル会社（トムソンネット）からは、十分な情報や支援がありますか。他社にトムソンネットを推薦するとすれば、そのよきところと悪いところは　なんであると感じておられますか。

Ａ⇒　弊社はＰマーク初回取得時からトムソンネットさんにコンサルをお願いしています。
トムソンネットの担当の皆様は保険会社のご出身の方々ということもあり保険代理店の業務についての知識を充分もってらっしゃいます。話が通じる！という言葉が分かりやすいと思うのですが取得であったり更新の対策についてのやりとりがスムーズに運ぶことは他とは違う部分だと思います。
規定の変更等の際も早急に知らせて頂いていますし対応が丁寧です。
今後も継続してコンサル業務をお願いしたいと思っております。

３．「やさしい情報セキュリティ」その 13：今年要注意のセキュリティ脅威

前回にもお知らせしましたように、1 月 30 日に IPA（情報処理推進機構）から「情報セキュリティ 10 大脅威 2018」が下図のように発表され、続いて 3 月 30 日に同題の解説がホームページに公開されました。今回はその中で主に「組織」について重要、あるいは興味深い事柄を抜き出して述べてみたいと思います。

■「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

（1）“順位”で注目されること

“脅威”の右に NEW のマークがあるのは昨年度ランクインしていなかったものです。注目すべきは「ビジネスメール詐欺」がいきなり 3 位に入っていることです。前回（2018 年新春号）の P マークニュースでご紹介したように、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。別名、“企業版オレオレ詐欺”“外国送金詐欺”とも呼ばれています。

攻撃手口に多いのが(JAL のケースも)取引先との請求書の偽装です。取引先と請求に係るやりとりをメール等で行っている所に割り込み、攻撃者が取引先になりすまし攻撃者の用意した口座を記入した偽の請求書等を送りつけ、振り込ませる。なお、攻撃者は取引のやりとりをなんらかの方法により盗み見し、取引や請求に関する情報や関係している従業員の情報を入手した上で攻撃を行なっています。

ポイントは“取引のやりとりを盗み見られた”ことです。それと、メールへの“返信”です。取引先との間に入り込んでメールのやり取りを行い信用させますから、正規の取引先に電話やメールを送れば（この場合宛先にアドレスを入力）、すぐに判明したはずですが、「表示名」にだまされて攻撃者のアドレスに送信したことではまってしまいました。

社長や上司になりすまし、従業員に攻撃者の用意した口座へ振り込ませると言う手口もあります。この時、攻撃者は事前に入手した経営者や関係している従業員等の情報を利用しています。

いずれも、どこかでメールアカウントが盗まれたことが原因です。パスワードを複雑にする、文字数を長くする、などメールアカウントの管理レベルを明日からでも上げることを検討いただければと思います。

（２）引き続き「標的型攻撃」が１位に

企業として被害の甚大さを考えると 2 年連続「標的型攻撃」がトップにあるのは頷けます。不特定多数に感染させる一般的なウィルスと異なり、攻撃対象（標的）を絞って不正ソフトを送りつけたり、不正ソフトをダウンロードさせたりします。日本年金機構の 130 万件の個人情報流出事件で一挙に有名になりました。

大手企業でないから標的にされない？　それは全くの誤りです。

最終ターゲットを保険会社として取り敢えず代理店に攻撃を試みるなど、標的企業の取引先やグループ子会社等を攻撃の踏み台にすること（ウイルスでメールアカウントを乗っ取る等）もあり、業種や会社規模に関係なく狙われるおそれがあります。

（３）「個人の 10 大脅威」は会社に関係ないか？

大いにあります！

特に、会社のメールアドレスを使ってネット通販の会員登録や SNS(Facebook、Twitter など)に ID 登録を行うのはすぐ止めていただきたいものです。ネット通販への注文や SNS への投稿が、不注意から意図しない業者への情報提供に繋がる危険があります。「5 位 ウェブサービスへの不正ログイン」「6 位 ウェブサービスからの個人情報の窃取」が典型例です。

特に SNS で安易に“いいね”をクリックしたり、各種の診断系アプリ（性格判断、深層心理分析など）へ申し込みをすることによって、氏名やメールアドレス、友人（取引）関係などの個人情報を奪われ、行く行くは“なりすまし”に使われる可能性があることは公知の事実です。或いは、不用意な投稿によって会社の名誉にキズを付けることになるかもしれません。

（４）“パスワードの更新”のこと

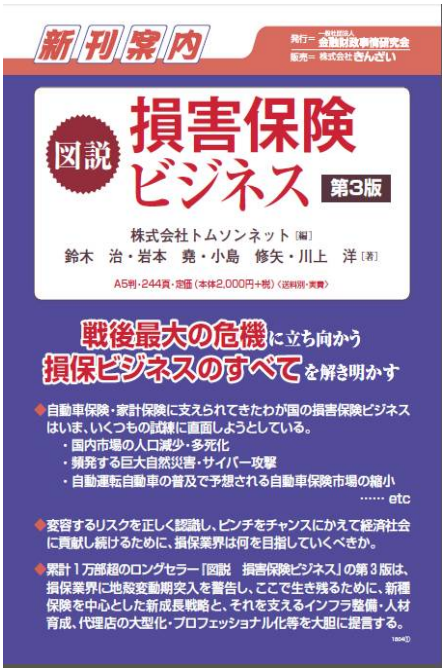
最後になりますが、「JIS Q 15001-2006 をベースにした個人情報マネジメントシステム実施のためのガイドライン－第 2 版」が 4 月 10 日に改定され、安全管理措置の中で望ましいとしていた“パスワードの有効期限を設定している”の項目が削除されました。

このため、パスワードを“定期的に更新する”が審査基準から除かれます。理由は、定期的な更新を義務づけたると形骸化し勝ちで、デメリットが多いためとしています。ある調査によると対象者（大学生）の 46%もの人が 1 文字だけの変更に留めているとの報告もあります。

LINE が 2017 年に実施した「セキュリティ実態把握調査」でも、「自分や家族、恋人や友だち、知人等自分の周りの人で、アカウントを乗っ取られたことがある人がいる」と回答した人は全体の約 4 割あり、サービス別では LINE が多く、次いで Twitter、Facebook メッセンジャーの順であったとのことです。定期的更新はさておき、“123456”や“qwerty”（キーボードの上段配列）などすぐに類推できるパスワードは今からでも変更しましょう。

４．トムソンネットからのお知らせ

「図説損害保険ビジネス（補訂版）」の改訂版（第３版）を出版します。



弊社が金融財政事情研究会から出版している「図説損害保険ビジネス」は、見開き２ページで１テーマを左ページに文章、右に図説と分かり易い構成で、特に保険代理店様においてはトップマネジメントから新入社員に至る幅広い層のみなさまからご好評を戴いておりますが、補訂版（第２版）の出版から約８年が経過し、損保ビジネスを取り巻く環境は大きく変わろうとしています。

とりわけ自動運転自動車の出現・実用化は、自動車保険を中心に進展してきたわが国損保ビジネスに対し大きな転換を迫っており、保険流通の仕組みを始めとして大きな変貌を遂げることが予想されます。

こうした損保業界の動向を解説し、損保ビジネスの方向性を読み解くべく前第２版から大幅に内容を刷新し、この度改訂版（第３版）を出版する運びとなりました。

改訂版（第３版）において採り上げた「損保保険とは何か」に始まり、「損保経営のガバナンスと ERM」に至る 10 のテーマは、みなさまの日々の業務に様々な形でお役に立てるものと確信しております。「図説損害保険ビジネス（第３版）」は、５月中旬頃には本屋さんの店頭に並ぶ予定です。是非ともお買い求め戴きたくご案内申し上げます。

なお、図説シリーズとして既刊の「図説生保ビジネス」、「図説損害保険代理店ビジネスの新潮流」もご利用戴きたく、併せご案内申し上げます。

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（Mail：iwaharahi1017@tmsn.net ） 平泉 哲史（Mail：s.hiraizumi@tmsn.net）
本間 晋吾（Mail: s.honma@tmsn.net）