Ｐマークニュース

＜２０１８年盛夏号＞　Ｖｏｌ．２４

（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年盛夏号目次

１．「個人情報」ってそんなに重要で価値あるもの？
－「個人情報・個人データ」を巡る最近の状況から－

「データエコノミー」と言われます。人の行動や企業の活動が生み出すデータを競争力向上に生かす新たな経済です。ヒト･モノ・カネが生み出す情報資源が爆発的に増え、経済から政治、社会、日常の生活にまで影響を及ぼしています。その中心は「個人情報・個人データ」です。**「個人データ銀行」創設**という新聞記事もあります。**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**の新たな脅威もあります。こんな中で 2018.5.25 には**EU 一般データ保護規制（GDPR）が施行**されました。

また、2018.7.17 には EU との経済連携協定から得られる利益を保管し拡大する**「欧州委員会による日本への十分性認定」**についての最終合意が公表されました。

「個人情報・個人データ」を巡って大きな流れが生じています。「個人情報・個人データ」の今までの理解はどう変わっているのでしょうか？ 私達はどう考えたら良いのでしょうか？

2018.7.18 の日経記事です。「三菱 UFJ 信託銀行は 2019 年にも、個人から購買履歴等のデータを預かり、民間企業に提供する『個人データ銀行』を始める方針を固めた」。個人がスマホなどから発信される購買履歴、健康情報、行動記録(旅行履歴、道路交通履歴など)を、それ等を管理記録するアプリ会社と個別にデータ提供の契約を結び、個人の同意を得て、データ提供を受ける。このデータを、健康食品会社、旅行会社、スポーツクラブ等に手数料をとって、提供する。個人には 1 企業ごとに毎月 500 円から 1000 円程度の報酬を支払う、というものです。個人が、毎日利用しているスマホから発信している情報が「信託ビジネス」と親和性が高いと見て、取引の対象となるのです。

「個人情報・個人データ」の保護が、「個人情報の漏えい、滅失又はき損を防止」するため、「合理的な対策を講じるとともに、必要な是正措置を講じる」ことに重きを置いていることと、全く異なる視点からの保護の考え方が必要でしょうか？「個人情報・個人データ」の**提供者の基本的権利(提供したものは取り戻せる？ 移転はできる？全てを消去することができる？など)を規定**したうえで保護をどうするかの視点です。

グローバルにおいては、前述の IT の巨人による個人データ独占の新たな脅威の一つとして、グーグルは世界中からデータを集め、2017 年 12 月期の売上高 12 兆円は、大半が「個人データ」をもとにした広告収入だといわれています。22 億人が使うフェイスブックとグーグルをあわせたネット広告の世界シェアーは 6 割を超すといわれます。

「個人情報・個人データ」が負った利便性の対価です。その大きさと影響力に世界は**「知の民主化」の危機**ととらえ始めています。また、個人情報を提供しているという意識のないままにグーグルが記録している「個人情報・個人データ」は、個人の種々の情報がプロファイルされ、「個人」が気が付かない間に把握されているという実情もあります。便利さの代償に**「個人の基本的な権利」が危ういのです。**

こうした状況に法制度として立ち向かったのが 2018.5.25 施行の **EU 一般データ保護規制（GDPR）**です。GDPR は改正個人情報保護法と同様にさまざまな「個人情報・個人データ」を企業や行政が処理する際のルールを定めていますが、改正個人情報保護法には定めていない規程も多くあります。自分の「個人情報・個人データ」がどのように処理されるかについての基本的な権利を個人に保障しています。改正個人情報保護法にはなく(開示等の請求権など一部規定されてはいますが)、GDPR に規定されている「個人の基本的権利」とは、下記の通りです。

①忘れられる権利 The Right to be forgotten	1. 本人(データ主体)は、当該本人(データ主体)に関する個人データについて管理者に不当に遅滞することなく消去させる権利を持つものとする。 管理者は、次に掲げる根拠(掲載略)のいずれかが適用される場合、個人データを不当に遅滞することなく消去する義務を負うものとする。 2. 管理者が個人データを公開しており、第 1 項による個人データを消去する義務を負う場合、その管理者は、利用可能な技術及び実施の費用を考慮し、当該個人データを取り扱っている管理者たちに本人（データ主体)が当該個人データの**あらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならない。** (第 17 条 1 及び 2)
②制限権 The Right to restriction of processing	本人(データ主体)は、管理者に対して一定の場合(個人データが正確でない、係争中で個人データの削除・廃棄の制限希望)に**個人データ保存以外の処理を制限する**権利を有する。(第 18 条)
③データポータビリティの権利 Right to data portability	本人(データ主体)は、当該本人(データ主体)が管理者に提供した当該本人(データ主体)に関する個人データについて、構造化され、一般的に利用され機械処理可読性のある形式で受け取る権利があり、当該データを、個人データが提供された管理者の妨害なしに、他の管理者に移行する権利がある。(第 20 条)
④異議を唱える権利 Right to object （プロファイリングに異議を唱える権利)	1. データ主体は、当該データ主体のそれぞれの状況に関する理由を根拠として、第 6 条第 1 項(e)号又は(f)号に基づくプロファイリングを含む当該条項を根拠とした自己に関する個人データの取扱いに対して、いつでも異議を唱える権利を有する。管理者は、データ主体の利益、権利及び自由に優先する取扱いのための、又は法的主張時の立証、行使若しくは抗弁のための差し迫った正当な

	根拠であることを示さない限り、もはや個人データを取り扱ってはならない。（なお、ただし書きの制限がある。） 2. 個人データがダイレクトマーケティングのために取り扱われるならば、本人（データ主体）は、当該マーケティングのための当該本人（データ主体）に関する個人データの取扱いに対して、いつでも異議を唱える権利を持つ。当該ダイレクトマーケティング範囲内のプロファイリングを含む。（第 21 条 2 項）
⑤自動的処理のみによる意思決定に服さない権利 Automated individual decision-making, including profiling	1. 本人（データ主体）は、当該本人（データ主体）に関する法的効果をもたらすか又は当該本人（データ主体）に同様の重大な影響をもたらすプロファイリングなどの自動化された取扱いのみに基づいた決定に服しない権利を持つ。（第 22 条 1 項） 第 2 項では適用されない場合を規定している。

この GDPR は、過剰規制であり、「個人情報・個人データ」を結果的に公開することで便利な生活を送っているのだから**過剰規制はするな**という意見もあります。日本では、「従業員や顧客などの個人データの EEA（欧州経済領域）域外への持出し禁止」規制で大騒ぎとなりました。これは「**欧州委員会による日本への十分性認定**」についての最終合意（2018.7.17）で解決し、GDPR に対する不満は少し和らいでいますが。

「便益のために個人情報を提供するか」という調査では、肯定的な中国、ロシアなどと違って日本は肯定する人が少なく、その割合は全世界平均以下という調査があるといわれます（2018.7.16 日経）。これは個人情報保護の意識レベルが高いということでしょうか？ Google 検索、Google MAP、などを使う時に自分の「プライバシーにつながる個人データ」を提供しているなんて意識が無いだけ？？ 大変残念なことに、「個人情報・個人データ」を事業の用に供する際のしくみルールである P マーク取得率では、保険代理店は他業種に比し著しく低い状況です。まして、「個人情報・個人データ」が「個人の基本的権利」であるとの意識は、EEA とは国民性の違いはあるでしょうが、極めて低いのではないでしょうか？ 「個人情報・個人データ」を巡って危うい超情報化社会が到来しつつあります。この状況を踏まえて、GDPR という法規制が施行されました。「個人情報・個人データ」は、大変に価値があり大切な情報であることを再認識したい最近の状況です。

【個人情報／個人データの定義比較】

国・地域	用語	定義
日本	「個人情報」 「個人データ」 「保有個人データ」 （出典：改正個人情報保護法 2016 年 1 月）	「個人情報」とは、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などにより特定の個人を識別できるもの（他の情報と容易に照合することが出来、それにより特定の個人を識別することができることとなるものを含む）又は個人識別情報が含まれるもの」をいう。 また、個人情報をデータベース化した場合、そのデータベースを構成する個人情報を特に「個人データ」といい、そのうち、事業者が開示などの権限を有し 6 か月以上にわたって保有する個人情報を、特に「保有個人データ」という。
欧州	「個人データ」 （出典：ＥＵ一般データ保護規則 2016 年 4 月）	「個人データ」とは、識別されたまたは識別され得る自然人（以下「データ主体」という）に関するあらゆる情報を意味する。識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、または当該自然人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的もしくは社会的アイデンティティに特有な一つもしくは複数の要素を参照することによって、直接的にまたは間接的に識別され得る者をいう。
米国	「個人データ」 （出典：米国プライバシー権利章典 2012 年 2 月）	プライバシー権利章典は、個人データの商業利用に適用される。この用語（個人データ）は、特定の個人に連結可能なすべてのデータをいい、集約されたデータを含む。個人データは特定のコンピュータその他のデバイスに連結するデータも含みうる。例えば、利用記録を作成するために使われるスマートフォンや家庭のコンピュータの識別子は個人データである。

２．保険代理店様における個人情報保護への取り組み（４）

引き続き、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、株式会社ヒューマン＆アソシエイツ様の生島代表取締役様ほか、Ｐマーク運営に携わっているみなさまに弊社からのＰマーク関連の質問にお答え戴きました。

（１）保険代理店として、Ｐマークを取得して良かったと思う点があればお教えください。

先ず、導入＆取得に向けて大変苦労しましたが、その後の保険会社や監督官庁の監査では、PMS の認定を受けているというだけで、それ以上の質問も無く簡単に済ますことができ、30 社以上の乗合がある弊社にとっては助かっています。

また、取得に向けて社員の個人情報に対する意識も随分改善されたと感じています。

PMS でも業界の体制整備義務においても、いずれにしても　やっていることを第三者に証明しなければいけなくなった時代において、認定制度は分かりやすく安心できる制度ではないかと思います。

また世界的に個人情報の取り扱いに注目があたりルールが厳しく変わっていく中、多くの個人情報を取り扱う代理店にとって必須になっていくと感じています。

（２）多くの保険代理店でメールや郵便物の誤送信に悩まされています。
御社における誤送信対策として取り組んでいる点があればお教えください。

弊社の業務の中で誤送信が考えられるものとして郵便、ＦＡＸ、メールが考えられます。

まずどれにも言えることですが宛先を入念にチェックすることを入社時や定期的に行う勉強会で徹底しています。その上で郵便、ＦＡＸについては別の者とダブルチェックを通して送付を行っています。またＦＡＸとメールについてはテスト送信を行った宛先でないと送ってはいけないというルールを作っています。さらに、メールについては送信頻度も高いため一定時間の間であればメールの送信を取り消せるシステムを導入して対応しています。これは、メール誤送信は送信直後に気付くことが多いという統計データをもとに導入しました。

（３）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。

ウィルス対策のソフトを全パソコンに導入していることは勿論ですが、ファイアウォールを導入し、パケットのフィルタリングと通信の監視を２４時間しています。このファイアウォールの導入によって月に６７件もの攻撃メールが届いていることが発覚しました。この通信結果を踏まえた上でランサムウエアやその他攻撃メールの実例を取り入れながら定期的な講習を社員全員に行っています。

悪意ある攻撃の手段というのは日進月歩なのでシステムを導入して終わりではなく、攻撃手段の把握と最新の知識を周知することが最大の対策だと考えています。

（４）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。その原因はなんであると思われますか。

個人情報保護法や PMS 規定の理解の難しさ、Ｐマーク取得に向けての自社が扱う個人情報の洗い出し、社員一人一人への意識改革への働き掛けや教育など準備業務の繁雑さ、二年毎の更新という多くのハードルが原因では無いでしょうか。

３．事例に学ぶ：技術的安全対策で十分か　～日本年金機構個人情報漏洩事案～

前号まで「やさしい情報セキュリティ」と題し、都合 13 回のシリーズで主に情報セキュリティの技術的安全対策について述べてきました。

今回以降、技術的なことに限らず個人情報の保護や情報セキュリティの維持・向上にお役に立ちそうな事柄をご紹介させていただきます。

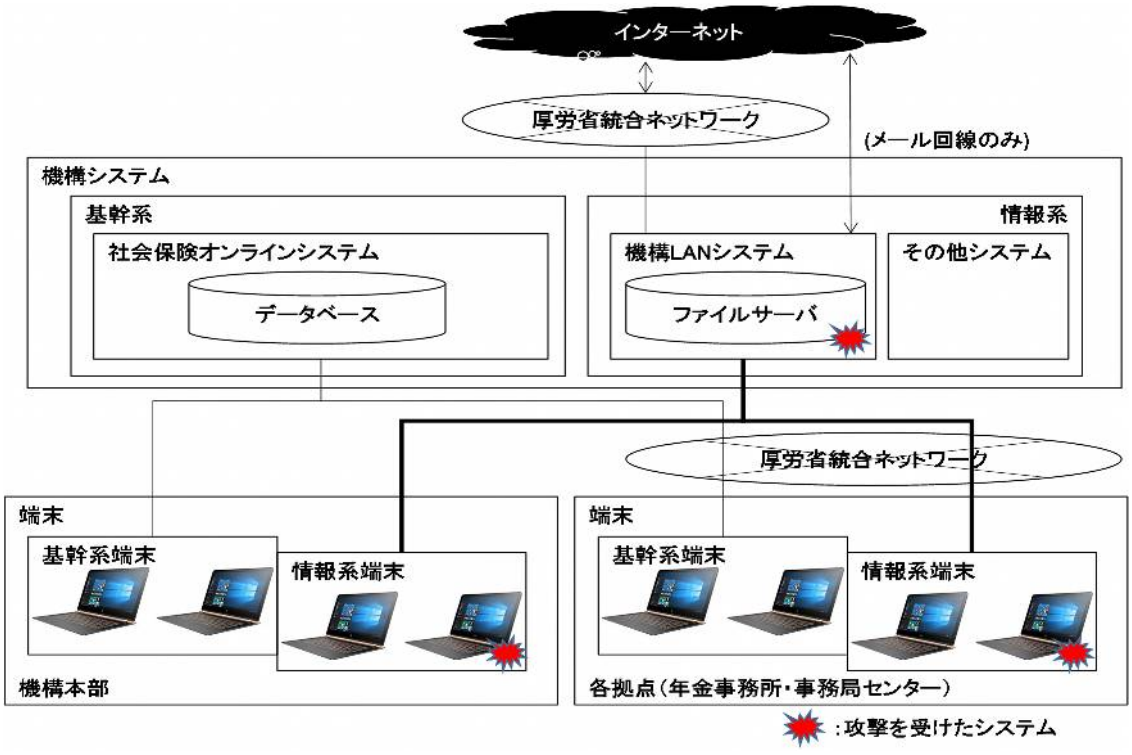
その第 1 回目。三年前に発生した日本年金機構（以下「機構」）における 125 万件に及ぶ個人情報の流出事案が、年月を経るに連れて風化しつつあるような気配を感じており、本質的なことを忘れてはいけないと思い採り上げました。当該事案のまとめは『検証報告書』として「日本年金機構における不正アクセスによる情報流出事案検証委員会」から公表されていますが、一般企業にも示唆となることがいくつか含まれています。機構はいわずもがな公的機関で、当該事案は“一般性がない”と受け止められる傾向があります。しかし、“なぜ、なぜ・・”と原因を突き詰めて行くと民間企業にも当てはまることが浮き彫りになります。それらを紹介し、他山の石としたく考えています。

（１）管理されていない個人情報が大量に存在していたこと

機構のシステム（ネットワーク）の概略は下図の通りで、最重要な社会保険オンラインシステムにアクセス可能な端末（PC）は一般の情報系端末と分けていました。「省庁ガイドライン」に則っています。個人情報は基幹系のデータベースのみに置くこととし、その端末からはインターネット（メール等）のアクセスができないよう意図している訳です。

ところが、基幹系のデータベースから担当者（一人ではありません）はデータをダウンロードしファイルサーバにコピーを持っていました。つまり、“個人情報がインターネットから隔離されていない”状態にあったのです。しかも、その運用を管理者が黙認していたと言うことです。Ｐマーク事業者で言えば、“同じ内容であっても、保管場所が違う場合は別の個人情報として特定しリスク対策を講じる”の原則に沿っていなかったことになります。

＜機構ネットワーク概念図＞　　出展：「検証報告書」



（２）攻撃される意識が希薄だったこと

機構は全ての社会保険加入者の情報を収集していますが、中央官庁そのものではありません。どうしても「ウチなんかターゲットに・・」の思いがあったことは否めないようです。

結果的に機構が被害者になりましたが、本丸は厚労省だったかもしれません。事実、数度に亘った執拗な攻撃の最初は厚労省の職員に送られた不正メールです。この時、機構職員の氏名とアドレス（公開していない）が盗まれて、以降の攻撃に利用され、ターゲットが機構に変わったのかもしれません。その後、実際に在籍する機構職員の氏名やアドレスを利用して“なりすまし”をしています。

ここで言えるのは、ターゲットの組織を狙う前に関係する組織に侵入し、ターゲットの社員が信用しそうな情報を得る流れがあると言うことです。取引先からターゲットの情報を入手する、などです。

（３）攻撃を軽く考えていたこと

攻撃の早期の段階で、ある職員は標的型攻撃の可能性があり追って本格的な攻撃の恐れがある旨を情報発信していました。しかし、機構内で正式に取り上げられることがなく、組織として判断し却下した形跡がありません。

全ての組織には脅威に対応する体制が整えられ、実際に顕在化（発現）した場合にはその機能を果たすことが求められるのは当然です。ここで“体制”とは、社内に専門技術者を必要とする意味ではなく、外部の支援者を含めてのことです。

（４）点検が不十分であったこと

前の(2)項で述べた通り、ファイルサーバに重要なデータは保管されていないことが建前になっている以上、その点について自己点検（運用の確認）や内部監査が行われていませんでした。また、攻撃が繰り返されている中で全端末の一斉点検を行っていますが、責任者から具体的なチェックポイントが示されなかったため見落としが発生し、更なる感染を防げませんでした。

結局は運用実態とかけ離れた机上の管理がなされていたと言っても過言ではないでしょう。

（５）まとめ

情報セキュリティにおいて、“完全な予防は不可能。被害の極小化が重要”との考え方が主流になっています。当該事案でも攻撃に使用されたマルウェア（ウィルス）の中に新型のものもあったように、多額の費用を投じた装備をしていても事前対策に漏れは避けられません。

企業としては経済的に可能な範囲で物理的・技術的安全対策を講じた上で、当該事案をヒントに人的・組織的措置によって被害を最小限に食い止める方策に傾注することが必要です。

【日本年金機構における 125 万件に及ぶ個人情報の流出事案】

漏洩は 2015 年 5 月日本年金機構の職員宛てに送られた標的型攻撃メールにより起こりました。
ヤフーのフリーアドレスから送られたこのメールは、「厚生年金制度見直しについて（試案）に関する意見」等の件名で送信されており、開封や添付ファイルのダウンロードを行う事で、端末がウィルスに感染してしまったのです。

この不審メールによる標的型攻撃は複数回行われました。攻撃が発覚した 2015 年 5 月 8 日以降「不審なメールに注意」との社内喚起が行われますが、具体的なメール内容については申し送りがなかった為、その後の度重なる攻撃により感染端末が増加、結果として 125 万件にも上る大規模な情報抜き取りが行われてしまいました。

４．お知らせ

（１）Ｐマークの新規取得申請は、8 月から改定 JIS Q 15001(2017)基準のみとなりました

Ｐマーク新規取得申請は 7 月末で旧 JIS 基準による申請受付は終了し、8 月 1 日から新基準による新規審査の申請のみとなりました。

なお、更新申請は、2020 年 7 月 31 日まで移行措置として旧基準による申請が認められます。

弊社では JIS 新基準による新規取得申請の対応を始めておりますので、従来同様、P マークの取得を検討されている保険代理店様につきましては、お気軽にご相談ください。

（２）2017 年の個人情報漏えい事故状況が発表されました

NPO 日本ネットワークセキュリティ協会（JNSA）から 2017 年の個人情報漏えいに係る調査・統計が速報版として 6 月半ばに発表されました。

2017 年については、事故発生を示すインシデント件数が、前年（2016 年）の 468 件から 100 件程減少して 381 件になっており、ここ数年の減少傾向が続いています。

①業種別発生状況（ワースト 3）

	2016 年	2017 年
1	教育・学習支援 107 件（22.9%）	公務 110 件（28.5%）
2	金融・保業 105 件（22.4%）	教育・学習支援 60 件（15.5%）
3	公務 68 件（14.5%）	卸売業・小売業 33 件（8.5%）

業種別の事故発生件数をみると、ここ数年は、「公務」、「金融・保険業」、「教育・学習支援業」がワースト 3 という形が固定されていましたが、2017 年は「金融・保険業」が 27 件と大幅改善され、ワースト 3 の座を譲ったことは特筆されます。この改善が今後も継続されることが期待されます。

②原因別漏えい件数

	2016 年	2017 年
1	管理ミス 159 件（34.0%）	誤操作 97 件（25.1%）
2	誤操作 73 件（15.6%）	紛失・置忘れ 84 件(21.8%)
3	不正アクセス 68 件（14.5%）	不正アクセス 67 件（17.4%）

前年初めてワースト 3 に登場した「不正アクセス」は、2017 年も発生件数 67 件と前年とほぼ同数の事故が発生していますが、全体の発生件数が減っている中で、その発生原因割合は 17%とアップしており、引き続きネットワークのセキュリティ管理の強化やセキュリティソフト最新版の適用の確行が求められます。

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）