Pマークニュース ＜２０１６年盛夏号＞　Ｖｏｌ．１６	（株）トムソンネット Ｐマークコンサルティンググループ

２０１６年盛夏号目次

１．コンプラは顧客重視なのか？

改正保険業法が 2016.5.29 から施行され、募集代理店における体制整備義務が課せられました。
法の定めるところであり、法定事項の遵守には取り組んでいる。ただ一方で遵守はするが、それは最低限の遵守で済ませ、面倒なことはできるだけやらないというのも実態ではないでしょうか？
「コンプラでは、飯が食えない。テンプラでなら食えるが」なんて。体制整備義務のひとつとして法定された「個人情報取扱いに関する社内規制の策定」（規則第 227 条の 9)なども、できるだけ簡単な保険会社の提供物があれば、それで「お茶を濁す」？

古老の代理店主曰く「契約者に寄りそった対応はパソコンではできないよ。俺は契約者に正月には毛筆手書きで賀状を送って、全ての契約者に信頼されている。」これこそが契約者の身近にいて寄り添うすばらしいこと!! ただ、「手書き毛筆」で「何を」伝えるかでしょうか？ 契約者のリスク把握に役立ち、ニーズの的確な把握が十分か？ も気掛かりです。
保険の募集の仕方に、最新の技術や仕組みを取り込んだ形が普及してきました。それはパソコンを利用したシステムであり、ネットワーク、SNS、スマホの利用であったり。これらは業容の拡大のために、より細かな顧客のニーズを記録でき、必要な時に伝えられ、その要望を処理できます。しかも早く多くの顧客に。しかしながら、顧客情報がデータとして取扱われ、顧客から離れた「名簿」として売買するという取扱いも現れて、「利便の拡大」と「その弊害の拡大」という両面がみられるようになりました。これには猛省が必要です。

保険業が経済社会のなかで、成長し、募集チャネルの多様化（銀行窓販、来店型ショップ、インターネットによる募集）、保険代理店の大型化が進んできました。とともに弊害を伴う法制度の未整備が指摘され、顧客ニーズの的確な把握（意向把握、情報提供、意向確認）と法令等の遵守の体制整備が、法定されたということでしょうか？ 新たな成長を求めて、最新の技術や仕組みを取り込んでいく。その行き過ぎには、法規制がある。と考えると新たな成長に前向きでなければ、法規制は重荷でしょうか？
コンプラはまさに重荷？ しかし、やがて最新の技術や仕組みを使った募集に淘汰されていく。そう割り切れればスキッとするかも知れません。今に生きている顧客は、利用できる最新の技術や仕組みを享受したい、だから法規制遵守のコンプラが必要とも考えられます。顧客の求めるものに対応できずには顧客の満足は得られません。
また、法規制の中には、社会規範の遵守を改めて求めていることもあります。個人情報保護と言いますが、「自分のことを見ず知らずの人が知っているって、厭ですよね。自分の個人情報を何の目的で利用するかを明確にしましょう。」ということがこの法令の基本です。これもコンプラです。

改正個人情報保護法施行細則の原案が提示され、その意見公募が８月末までされ、今秋末にも制定されるようです。改正個人情報保護法では、「匿名加工情報」などとして利用拡大がはかられる一方で、「第三者からの提供」については規制が強化されそうです。これもコンプラです。個人情報に係わるだけに目線は「顧客重視」です。（詳細は次号以降でお知らせします）

２．個人情報漏えい事故の状況（JNSA 2015 年度／速報版より）

ＮＰＯ日本ネットワークセキュリティ協会（ＪＮＳＡ）から 2015 年の個人情報漏えいに係る調査・統計が 6 月半ばに速報版として発表されましたので、2013 年度および 2014 年度の個人情報漏えい事件・事故（インシデント）の調査結果と対比しました。

①個人情報漏えいインシデント概要データ

項目	2013 年	2014 年	2015 年（速報）
漏えい人数	925 万 0065 人	4,999 万 9892 人	496 万 0063 人
インシデント件数	1,388 件	1,591 件	799 件
想定損害賠償総額	1,438 億 7,184 万円	1 兆 6,642 億 3,910 万円	2,541 億 3,663 万円
一件当たりの平均漏えい人数	7,031 人	3 万 2,616 人	6,578 人
一件当たり平均想定損害賠償額	1 億 926 万円	10 億 8,561 万円	3 億 3,705 万円
一人当たり平均想定損害賠償額	2 万 7701 円	5 万 2,625 円	2 万 8,020 円

2015 年については、事故発生を示すインシデント件数が、これまでの半数程度と 1 千件を下回りました。世間を騒がす大量の個人情報漏えい事故もときに発生していますが、企業の個人情報保護に関する意識は年々向上しており、今後もインシデント件数が 2015 年の水準からさらに減少して行くことが期待されます。また、ベネッセ事件が発生した 2014 年の数値は例外としても、一件当たり平均想定損害賠償額の水準は増加傾向にあり、個人情報の漏えい事故が企業に大きなダメージを与えることへの十分な認識が必要です。

②業種別

順位	2013 年	2014 年	2015 年（速報）
1	公務 587 件（42.3%）	公務 540 件（33.9%）	公務 222 件（27.8%）
2	金融・保業 294 件（21.2%）	金融・保業 503 件（31.6%）	教育・学習支援 142 件（17.8%）
3	教育・学習支援 158 件（11.4%）	教育・学習支援 190 件（11.9%）	金融・保業 102 件（12.8%）

業種別の事故発生件数は、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すが、3 業種の全体に占める割合は減少しています。

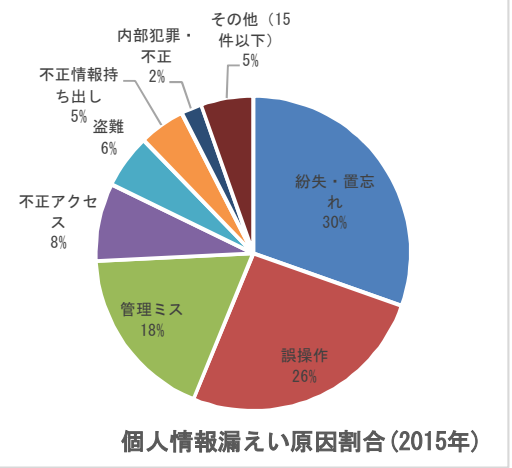
特に金融保険の減少振りが目を引きます。

③原因別漏えい件数

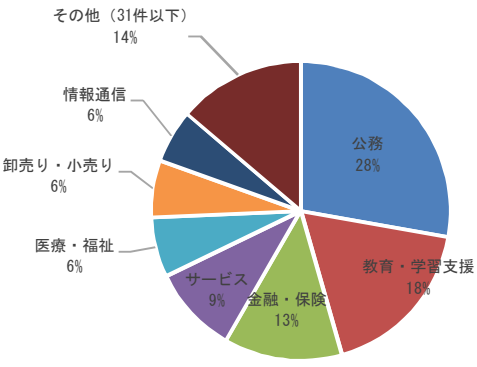
順位	2013 年	2014 年	2015 年（速報）
1	誤操作 485 件（34.9%）	管理ミス 696 件（43.7%）	紛失・置忘れ 243 件（30.4%）
2	管理ミス 449 件（32.3%）	誤操作 491 件（30.9%）	誤操作 206 件（25.8%）
3	紛失・置忘れ 199 件（14.3%）	紛失・置忘れ 200 件（12.6%）	管理ミス 144 件（18.0%）

個人情報漏えい原因においても「誤操作」・「管理ミス」・「紛失・置忘れ」のワースト 3 は、固定化している感があります。「管理ミス」が 15 年度には減少傾向をみせているのは、徐々に組織として個人情報に対する管理ルールが整備されてきたことが、減少傾向の一因と思われます。

その一方で、ヒューマンエラーの代表である「紛失・置忘れ」が増加しており、「気を付けましょう」だけでは解決せず、組織的な教育、予防対策が求められます。



個人情報漏えい原因割合(2015年)



個人情報漏えい事故業種別発生割合(2015年)

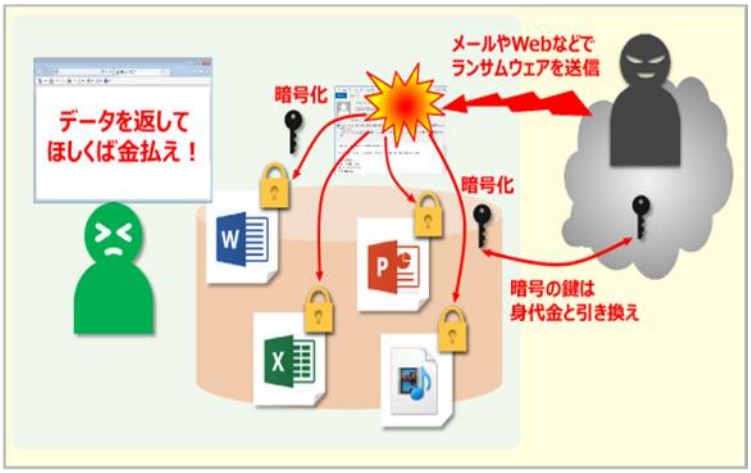
３.「やさしい情報セキュリティ」その７：ランサムウェアについて

数ある“マルウェア”の中で、お金に直結する悪玉が猛威を振るい始めています。称して“ランサムウェア”。感染したコンピュータは、ファイルやシステムへのアクセスを制限され、この制限を解除するためにマルウェアの作者（攻撃者）に ransom（身代金）を支払うよう要求されます。支払いの方法に匿名プリペイドキャッシュサービスを指定するなど、当然ですが攻撃者を秘匿しています。

（１）ランサムウェアに襲われると・・・

PC がランサムウェアに襲われた場合、特定のファイル（Word や Excel ファイル等）が暗号化されます。画面に突然ファイルが暗号化された、復号化するキーが欲しいか？の旨のメッセージが現れます。応答するとビットコイン等を使った振り込みを要求してきます。PC 上のファイルだけではなく、ネットワークに繋がっているファイルサーバのファイルも攻撃範囲です。WindowsPC だけではありません。Mac もターゲットになっています。

「ウィルスバスター」で著名なトレンドマイクロ社が発表（2016/8/1）した「企業におけるランサムウェア実態調査 2016」（以下「TM 調査」）には、被害に遭った企業の約 62%が攻撃者に“身代金”を払い、金額は 300 万円以上が過半数を占めていると報告されています。データやシステムの復旧、売上機会の損失の対応費用などを含めた総被害金額が 1 億円を超えた企業もあるようです。



（２）被害はどの程度広がっているか？

国内、海外とも被害程度は実のところよく分かっていませんが、「TM 調査」によれば、企業・組織において IT に関する意思決定者および関与者 534 名を対象にランサムウェアの攻撃にあったことがあるかを尋ねたところ、25.1%（134 名）が攻撃にあったことがあると回答しているとのことです。

大変なパーセンテージです。決して大企業や著名な会社だけではありません。

公的な統計が乏しい理由は、被害企業が“金で済むなら”と被害届を余り出したがらない風潮があるためと推測されます。被害届の提出先や相談先が知られていないのも一因と思われます。政府機関では「（独法）情報処理推進機構」（IPA）が担当になっていますが。

（３）どのようにして襲うのか？

ランサムウェアは第 6 回（前回）で触れた“標的型攻撃”の一種です。宅配便の再配達を偽った電子メールを発信する等、悪意のあるウェブサイトを閲覧させるタイプが多いようです。添付ファイルを使うものもありますが、いずれにしても“マルウェア”が発端です。

受信者にとって、発信者や件名に違和感を持たれないように巧妙な細工が施されているため、十二分に注意しながら受信メールを取り扱うことが必須です。

（４）そして対策は？

ファイルが流出する標的型攻撃に対する対策は前回述べていますが、ランサムウェアへの対抗策は暗号化される前のファイルに戻す“バックアップ”になります。但し、バックアップ先は外部ストレージか、“常時”仮想ドライブがあてがわれることのない装置や媒体が安全です。

また、「技術的安全措置」だけでは不十分で、「人的・組織的安全措置」の重要性を認識する必要があります。「TM 調査」では、34.8%の人が“自分の会社が攻撃されるとは思っていない”と答えています。この認識（の甘さ）が最も危険です。技術的な対策として高性能の IDS（不正侵入検知）、IPS（不正侵

入防御）を設置されている企業も多いと思われますが、どんな技術的防御策を装備していても完璧な対策は望めません。

防御策を活用し評価する組織の仕組みがなければ宝の持ち腐れです。情報セキュリティに関わる脅威・事案が発生した際には取引先との折衝が必要になる等、予算措置を含め企業として高度な経営判断をする体制・組織が必須になります。

（５）「CSIRT」（Computer Security Incident Response Team　“シーサート”）編成のお勧め

CSIRT は、情報セキュリティ担当役員（CISO）を中心に、コンピュータやインターネット上で、主にセキュリティ上の問題が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査を行い、経営陣に意見具申を行う組織のことです。“チーム”は情報システム担当みならず、営業、技術、財務、法務・・等々の各部門からメンバーをアサインします。毎日業務が発生することはないでしょうから、定期的な会合への参加と事案が起きた時にすぐ集合や相談ができるような仕組みがあれば十分です。現在 PMS 委員会、情報セキュリティ委員会等を運営されていれば、CSIRT にライドするのも容易でしょう。社外の有識者を加え、更に強固な体制にすることも考えられます。

【ご参考：コンピュータウイルス用語】

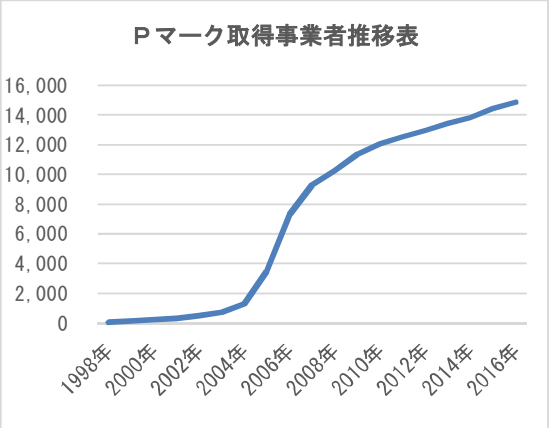
ウイルス用語	意味及び内容
クラッカー（Cracker）	犯罪行為を目的として、他人のコンピュータに侵入して、データやプログラムの改ざん・破壊等を行う者。
サイバーテロ Cyber Terrorism	WEB を通じ、政府機関、公的施設、企業等に対して、不正アクセスを行い、データの破壊や消去、Web 情報改ざん、情報漏洩、ウイルスの感染を行うことで、攻撃対象の中枢を麻痺させたりする行為のこと。
スニッフィング（sniffing）	ネットワークを流れるデータを傍受すること。パケット・スニッフィングと呼ばれることもある。
スパイウェア（Spyware）	インターネット利用者が気づかないうちにパソコンにスパイのように侵入し、個人情報を勝手に収集したり、パソコンに障害を引き起こしたりするプログラム。
スパムメール（迷惑メール） Spam Mail	受信者側が希望しないにもかかわらず一方的に送りつけられるメール（スパムメール等も含む）。受信者に不快感を与えたり、携帯電話のアドレス宛てに送信された迷惑メールは受信料金が発生する。
トロイの木馬 （Trojan horse）	ごく普通のプログラムのように装って実行させるプログラム。実行するとそのコンピュータのバックグランドで活動を開始し、ハッカー、クラッカー等が侵入するための裏口（バックドア）を開けたりする。
なりすましメール	メールの差出人を詐称して送信されるメールのこと。
ハッキング（hacking）	不正に他人のコンピュータに侵入して操作すること。
標的型攻撃メール	ウイルスを仕込まれたメールが送り付けられる、サイバー攻撃の一種です。添付ファイルを開いたり、URL をクリックするなどした場合に、コンピュータがウイルスに感染し、重要な情報を盗まれる危険性がある。
フィッシング詐欺 Phishing	フィッシング詐欺とは、実在の銀行やショッピングサイトなどにそっくりな偽のページに呼び込み、クレジットカード番号や暗証番号などを入力させてそれを入手してしまうという詐欺。
マルウェア（malware）	malicious software（悪意のあるソフトウェア）の短縮された語で、単一のコンピュータ、サーバー、コンピュータネットワークに、ウイルスまたはスパイウェアなどの被害を起こすように設計された悪意のあるプログラムの総称。
ランサムウェア （Ransomware）	ランサムウェアとは、感染した PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。身代金要求型不正プログラムとも呼ばれます。
ワーム（Worm）	電子メールなどを介してコンピュータに侵入後、データ改ざん・削除・破壊行為を行ったり・自己の分身を添付してばら撒き、自己増殖をするプログラム。
DoS 攻撃 Denial of Service Attack	攻撃対象となったサーバー等に対して、大量のデータや不正なデータを連続して送りつけることで、過剰な負荷がかかり、システム停止・ネットワークの麻痺等の障害に追い込まれる。
Winny（ウィニー）	匿名性を特徴とする和製ファイル共有ソフト。ファイル共有を行うにあたり、データはすべて暗号化されており、格子状のネットワーク構成になっている為、中心となるサーバーが存在しない。

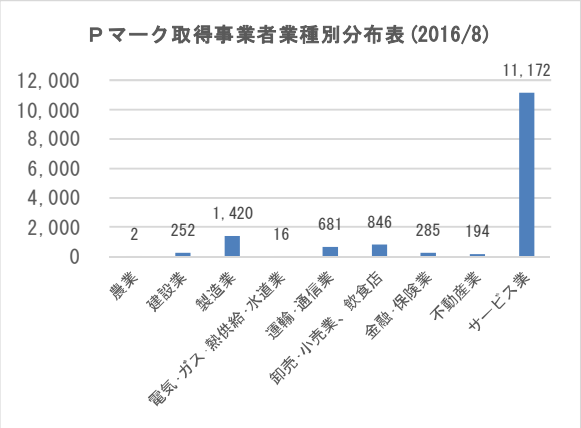
４．Ｐマーク雑記帳

（１）制度発足以来のＰマーク取得事業者数の推移

日本においてＰマーク制度が生まれたのは、1998 年でした。

Ｐマーク取得事業者数は、2006 年の個人情報保護法の施行で大きく伸び、昨年のマイナンバー制度の導入も増加要因になっています。**現在（2016 年 8 月 12 日）Ｐマーク所得事業者数**は、ＪＩＰＤＥＣ資料によれば **14,856 社**となっていますが、Ｐマーク制度の発足以降下図のような推移を辿っています。





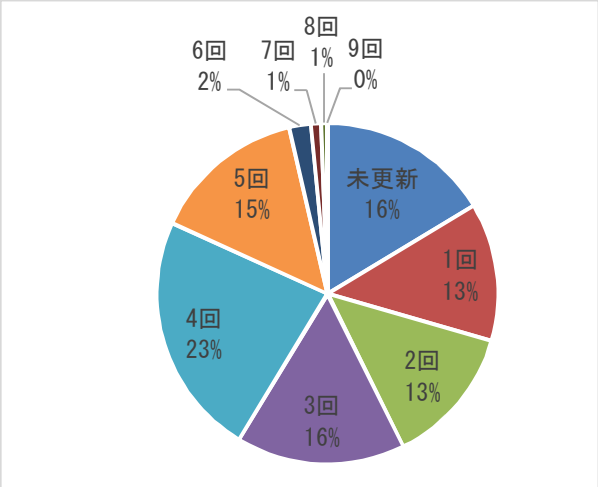
（２）Ｐマーク取得事業者数は幅広い業種で着実に増加中です。

直近の 5 年間（2011 年 9 月～2016 年 8 月）におけるＰマーク取得事業者の業種別伸び率をみると、以下となっています。

①全体の伸び率は 17%であり、情報サービス・調査業が含まれる「サービス業」が 18%、「金融・保険業」が 17%と平均的な伸びになっています。**こうした中で「保険媒介代理業」の 48%アップは、突出しており、保険代理店業界におけるＰマーク取得の本格化を読み取ることが出来ます。**

②この 5 年間で業界としてＰマーク取得を伸ばしたのは、建設業 41%増、運輸・通信業 24%増であり、Ｐマークが広範囲に亘ってビジネスに浸透しつつあると言えます。

（３）Ｐマーク事業者（14,856 社）の継続回数分布と業種別ランキング



順位	業種	事業者数
1	情報サービス・調査業	5,857
2	その他の事業サービス業	2,170
3	印刷業	1,074
4	労働者派遣業	334
5	広告代理業	291
6	その他の専門サービス業	286
7	広告業	237
8	土木建築サービス業	197
9	社会保険労務士事務所	178
10	一般貨物自動車運送業	161

①継続概数の分布をみると、継続回数 4 回（Ｐマーク取得後ほぼ 10 年前後が経過、個人情報保護法施行時に取得）がもっとも多くなっていますが、全体でみると継続回数 5 回以下では大きな差がなく分布しており、着実に取得事業者が増加していることが窺えます。

②Ｐマーク取得事業者の業種別ランキングをみると、ソフトウエアハウスが属する「情報サービス・調査業」がダントツです。2 位の「その他の事業サービス」には労働派遣業、建物サービス業、ビルメインテナンス業等が属します。上表ランキングのトップ 10 には洩れましたが、**保険媒介代理業（126 社）が漸く 13 位**まで上昇してきたことは注目されます。

５．トムソンネットからのお知らせ

今年の前半は多くの保険代理店様において、業法改正対応が代理店運営の重点課題であったことと思われます。

そして、今年の下期からは業法改正対応もほぼ一段落し、**次の一手として「Ｐマークの取得」をご検討**されている保険代理店様も増えているようです。(弊社でもいくつかの問い合わせを戴いております)

Ｐマーク取得支援について、Ｐマークニュースでお付き合い戴いている皆様からお声掛けを戴いた場合は、是非優先的に対応させて戴きたいと思っておりますが、ご承知の通りＰマークの取得には８か月前後を要しますので、場合によっては対応時期が相当先になってしまう可能性もあります。

就きましては、Ｐマーク取得をご検討されている場合は、**早めに弊社にお問い合わせ戴きたくお願い申し上げます。**

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)

以上