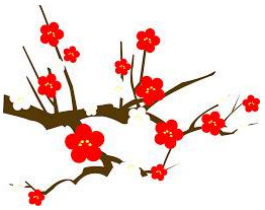
Pマークニュース ＜２０１７年新春号＞　Ｖｏｌ．１８	（株）トムソンネット Pマークコンサルティンググループ

２０１７年新春号目次



１．特集：改正個人情報保護法が施行されます

－2017.5.30 から全ての事業者での遵守が義務づけられましたー

改正個人情報保護法が、2017 年 5 月 30 日の施行と決定され(2016.12.20 閣議決定)、法令の整備、ガイドラインがほぼ整いました。2016.10.5 付で「個人情報保護に関する法律施行規則」が公示され、2016.11.30 付で、「個人情報保護法ガイドライン」(全 4 編)が公表されました。ガイドラインのなかで**「格別の措置」**とされていた金融分野のガイドラインについてもその案が示されています。(2016.12.13 の個人情報保護委員会)

個人情報保護法の改正をうけて、P マークの認証基準である JIS 規格も、見直し検討に入っており、改正個人情報保護法の全面施行後に改正・公表される見込みです。こうした状況をうけて JIPDEC が「改正個人情報保護法へのプライバシーマーク制度の対応方針について」を公表しました。(2016.11.30)

2017 年は、10 年ぶりの個人情報保護法改正によって、中小事業者の特例はなくなり全ての事業者の遵守が義務づけられ、個人情報保護が大きく再認識される年となります。

（１）主な改正点は下記ですが、詳細は順次に今後このニュースで取り上げて行きます

①) 個人情報の定義の追加と関連規定の整備
- ａ：「個人識別符号」を個人情報と明記。
- ｂ：「要配慮個人情報」定義の新設と関連規定の整備
- ｃ：「匿名加工情報」定義の新設と関連規定の整備
- ｄ：「個人情報取扱い事業者」定義の改正
- ｅ：「匿名加工情報取扱い事業者」の明記

②) 利用目的制限の緩和

③「提供」に関する規定の改訂
- ａ：第三者提供時の確認・記録義務の新設
  - ・確認・記録の適用対象　適用対象外の明定
  - ・確認義務　確認方法、複数回にわたる提供の際の確認方法
  - ・記録義務　記録の作成方法、記録事項(提供者、受領者)、保存期間(1 年、３年)
- ｂ：オプトアウト規定の見直し
- ｃ：提供罪の新設

④匿名加工情報の取扱いについて

⑤開示等請求権の明確化

⑥個人情報保護委員会の新設とその権限規定の整備
⑦個人情報の取扱いグローバル化への対応

（２）金融分野の「格別の措置」について

今回ガイドラインは、全ての分野に共通の汎用的なガイドラインとして、個人情報保護委員会が作成し、「従来の各分野別のガイドラインを一元化したもの」と位置付けています。ただし、一部の分野（医療関係、**金融関係**、情報通信関連など）については、「このガイドラインを基礎として、当該分野において必要となる**別途の規律**を定める」としています。この各分野固有の**「格別の措置」**に特化した「金融分野における個人情報保護に関するガイドライン（案）」が示されました。（2016.12.13 の個人情報保護委員会）そのガイドラインによれば、「各分野固有の『格別の措』』については、行政の継続性の観点から、**原則として現行の各分野ガイドラインの規制水準を維持するとともに、法改正に伴い新たに必要となる規定を盛り込む**」ことを基本として、下記の「格別の措置」を盛り込んでいます。

①「機微（センシティブ）情報」について
・現行ガイドラインの「機微（センシティブ）情報」（第５条）に、「要配慮個人情報」を合わせ、新たな「機微（センシティブ）情報」と定義する。
・新たな「機微（センシティブ）情報」についても、現行ガイドラインと同様に情報を取得等できる場合を限定する。とりわけ、その取扱いにおいて、「あらかじめ本人の同意を得る」ことに、留意すること。
・新たな「機微（センシティブ）情報」については、オプトアウト（提供にあたり、あらかじめ以下の情報を本人に通知し、または本人が容易に知りうる状態に置いておくとともに、本人の求めに応じて第三者への提供を停止すること）を用いないこと。
②「本人の同意」については、原則として書面によることとする。
③「オプトアウト」を「個人の支払い能力に関する情報を個人信用情報機関へ提供する」にあたっては、用いないこととする。

（３）認証されたＰマークとの関連　（JIPDEC の 2016.11.30 公表文及び Q&A から引用）

①現在取得しているプライバシーマークは、改正個人情報保護法の施行後においても**そのまま使用できるか?**
⇒使用できます。プライバシーマークの審査の基準となっている JIS には、現行でも法令遵守が要求規格として盛り込まれており、その要求事項を満たしたプライバシーマークの取得事業者は、法令等が改正されてもこれに適切に対応できるマネジメントシステムが構築され運用されているものと考えられます。従って改正個人情報保護法施行後もプライバシーマークは有効です。

②新たにプライバシーマークを取得する場合、または現在取得しているプライバシーマークを更新する場合、改正個人情報保護法施行後において、**審査の基準は変るか?**
⇒変りません。従来通り、現行の JIS Q 15001:2006 を基準として適合性の審査・認証を行います。ただし、当然のことながら改正個人情報保護法の全面施行に伴い同法を遵守すべく必要な措置を講ずる必要があります。

③改正個人情報保護法施行後の審査において、改正個人情報保護法を遵守するための**必要な措置を取っていなかった場合、審査は不適合となるか?**
⇒現地審査において、何ら措置が講じられていない場合は、リスクに応じた措置を講じるよう是正を求めます。ただし、JISQ15001 の改正を踏まえた審査開始までの間は、**今後講じる措置の計画を報告することも可**とし、次回更新審査時に再度実施の有無を確認します。

改正個人情報保護法の施行によって、金融分野事業者の義務がより明確になりました。改正法を遵守していく社内規程・同意文など雛型・様式、見直しのルール化などの具体的な方策が必要です。
その方策のひとつはＰマーク取得です。ご相談ください。

２．２０１６年に発生した個人情報漏えい事故を顧みる

昨年（2016 年）も残念ながら後を絶つことなく多くの個人情報漏えい事故が発生しました。
以下には、2016 年に発生した事故で、個人情報の流出件数が多かったものを中心に挙げてみました。

NO	発生時期	事故の表題	事故の概要
1	2016/3/7	江崎グリコ、不正アクセスで約 8 万 3 千件	同社の通販サイト「グリコネットショップ」からクレジットカード情報を含む最大約 8 万 3 千件の顧客情報が流出。サイトが使う外部サービスに脆弱性があり、不正アクセスを受けて流出した。
2	2016/4/21	日テレの WEB サイトに不正アクセスで約 43 万件	同社の Web サイトが不正アクセス攻撃を受け、保有する個人情報のうち約 43 万件が流出の恐れ。原因は、OS に対する不正な命令文を外部から紛れ込ませる「OS コマンドインジェクション」による攻撃であることがログ解析で判明した。
3	2016/4/23	J-WAVE、不正アクセスで約 64 万件	Web サイトへの不正アクセスにより、リスナーなどの個人情報約 64 万件が流出の可能性。原因はアイデアマンズ製「ケータイキット for Movable Type」の脆弱性による。
4	2016/4/30	エイベックス、不正アクセスで約 35 万件	同社サイトに不正アクセスがあり、アンケートやオーディションなどに応募した人の氏名や住所、電話番号、メールアドレスなどの個人情報約 35 万件が流出した可能性。契約アーティストの公式サイトなどで使用するソフトに脆弱性があった。
5	2016/6/14	JTB、不正アクセスで約 793 万件	海外からの不正アクセスによって、最大で約 793 万件の個人情報が流出した可能性があると発表した。取引先を装った標的型攻撃メールの添付ファイルを開き、ウイルスに感染したのが原因。
6	2016/6/22	講談社「ViVi」通販サイトに不正アクセスで約 1 万件	流出した個人情報は、同サイトで注文した会員分約 1 万件。原因は同サイトで利用している EC プラットフォーム「スパイラル EC」のシステムの脆弱性を突いたサイバー攻撃。
7	2016/7/27	クラッシュ・オブ・キングスでハッキング被害約 160 万件	攻撃者は同サイトのシステムへ不正侵入し、フォーラム登録者 159 万 7717 件のユーザー名、電子メールアドレスなどが流出。原因はラムアプリケーションソフトウェア「vBulletin」のセキュリティ脆弱性を突いて機密データにアクセスしたと推測される。
8	2016/11/10	カゴヤ・ジャパンで不正アクセス約 4 万 8 千件	同社のデータベースサーバが不正アクセスを受け、同社を利用した全ユーザー（解約済み顧客を含む）の個人情報約 4 万 8 千件が流出した可能性がある。公開サーバの脆弱性を突かれて「OS コマンドインジェクション攻撃」を受け、データベースサーバのデータが不正に操作されたという。
9	2016/11/10	「フラット 35」、不正アクセスで約 3 万 7 千件	「フラット 35」を扱う「優良住宅ローン」が、約 3 万 7 千件の顧客情報流出の恐れがあると発表。電子メールの管理サーバが不正アクセスを受けた。
10	2016/12/2	資生堂子会社、WEB サイトに不正アクセスで約 42 万件	同社の子会社で、化粧品を販売するイプサの公式オンラインショップがシステム上の脆弱性を突かれて不正アクセスを受け、約 42 万件の個人情報が流出した可能性がある。

上表の通り、大口の個人情報漏洩事故の多くは、システム対する不正アクセスによるものです。
日本を代表するような組織や団体が数多く含まれており、今やどんな企業であっても、「うちは大丈夫！」と胸を張って言えるところは、少ないのではないかとさえ思えます。

３.「やさしい情報セキュリティ」その９：内部不正

今回は“内部不正”について述べてみたいと思います。

よく紙誌上では“内部犯行”の言葉が賑わします。有名な通信教育事業者の事件を含め（委託先社員の不祥事も委託元の内部犯行に違いありません）、三菱 UFJ 証券システム部長代理の顧客情報持出しなど、世間の耳目を集めた大きな事件は両手でも余る程を数えます。ただ、今回敢えて“不正”としたのは、犯罪行為を指す“犯行”だけではなく、ハインリッヒの法則に従い犯行に至る前の社内規程違反に範囲を広め、どのように防ぐかに焦点を当てたいと考えたことによります。

IPA（独法情報処理推進機構）が毎年以下「10 大脅威」）を公表していますが、その中で“内部不正”のランクが 2014 年版では 11 位、2015 年版では 2 位です。2016 年版では 8 位と後退していますが、個人としての脅威と組織としての脅威を合わせた総合順位であって、組織順位ではやはり 2 位に位置づけされています。他に、調査会社が集計した統計でも、“情報漏洩事故の 80%が内部犯行による”と発表されています。

「情報セキュリティ10大脅威 2016」個人別・組織別　順位

（）内は総合順位、（−）は総合順位でのランク外です。

個人（カッコ内は総合順位）	順位	組織（カッコ内は総合順位）
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）	1 位	標的型攻撃による情報流出（2 位）
ランサムウェアを使った詐欺・恐喝（3 位）	2 位	内部不正による情報漏えい（8 位）
審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ（7 位）	3 位	ウェブサービスからの個人情報の窃取（4 位）
巧妙・悪質化するワンクリック請求（9 位）	4 位	サービス妨害攻撃によるサービス停止（−）
ウェブサービスへの不正ログイン（5 位）	5 位	ウェブサイトの改ざん（6 位）
匿名によるネット上の誹謗・中傷（−）	6 位	対策情報の公開に伴い公知となる脆弱性の悪用増加（10 位）
ウェブサービスからの個人情報の窃取（4 位）	7 位	ランサムウェアを使った詐欺・恐喝（3 位）
情報モラル不足によるサイバー犯罪の低年齢化（−）	8 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）
職業倫理欠如による不適切な情報公開（−）	9 位	ウェブサービスへの不正ログイン（5 位）
インターネットの広告機能を悪用した攻撃（−）	10 位	過失による情報漏えい（−）

１．不祥事の発生頻度

経産省（産業経済研究所）の資料によれば、従業員 300 人以上の大企業についてではありますが、2014 年にアンケート調査を行った結果として営業秘密窃取またはその疑い事例は

・外部からの具体的な危険性があったと感じた例がある　20.2%
・内部において具体的な危険性があったと感じた例がある　24.8%
・可能性はあるが、具体的な危険は感じたことがない　39.4%　（残りはその他）

となっています。話題の“標的型攻撃”を含む外部からの脅威よりも、内部の問題を重視すべきことが多くの企業で認識されています。

２．経営者の認識と性弱説

上記のような状況下で、経営者の皆さんはどのように感じておられるのか・・？　数百社を訪問させていただいた中で、どの代表者の方からも “社員を信用している”と言われています。当然のことと思います。つまり “性善説”と言うことでしょうか（一抹の不安を持ちつつも）。

しかし、 “社員性善説”に立つと、リスクの認識ひいては安全対策の発想やアイディアが止まってしまいます。一方では“性悪説は馴染まない”・・、そこで提案したいのは“性弱説”です。人間誰しも魔が差したり勘違いがあり、良かれと思ってしたことが結果的にルール違反になったり、などは極く普通にあることです。このような思いで“想定リスク”を考えてみてはいかがでしょうか。

３．実施している対策と従業員の意識

「2015 年版 内部不正の現状とその対策」（IPA）によれば、従業員の“内部不正への気持ちが低下する対策”と企業が“（重要だとして）実施している対策”にギャップがあります。多くの従業員は“社内システムの操作の証拠が残るのが最も有効”と思っているにも拘わらず、その対策が現状では 5 位に入っていません。“ID やパスワード”が最大の割合を占めています。おかしいですね。

対策の実施状況

順位	対策	割合
1	社内システムにログインするための**IDやパスワードの管理**が徹底されている	31.9%
2	開発物(ソースコード)や顧客情報などの重要情報は**特定の職員のみアクセス**できるようになっている	29.4%
3	**退職者のアカウント**は、即日、削除される	27.5%
4	職務上で作成・開発した成果物は、企業に帰属することを研修で周知徹底する	26.9%
5	情報システムの管理者以外に、**情報システムへのアクセス管理**を操作できない	24.4%

内部不正への気持ちが低下する対策

社員		内容	経営者・管理者の結果	
順位	割合		順位	割合
1位	54.2%	社内システムの操作の証拠が残る	19 位	0.0%
2位	37.5%	顧客情報などの重要な情報にアクセスした人が監視される(アクセスログの監視等含む)	5 位	7.3%
3位	36.2%	これまでに同僚が行ったルール違反が発覚し、処罰されたことがある	10位	2.7%
4位	31.6%	社内システムにログインするためのIDやパスワードの管理を徹底する	3位	11.8%
5位	31.4%	顧客情報などの重要な情報を持ち出した場合の罰則規定を強化する	10 位	2.7%

「2015 年版 内部不正の現状とその対策」抜粋

４．重要な対策

前掲の表などをヒントに採るべき重要な対策を 2 つ挙げます。いずれも大きな費用と業務負荷にはならないと考えます。「組織における内部不正防止ガイドライン」（IPA）に「内部不正チェックシート」が掲載されていますので、自社の状況を確認されることもお勧めします。

①技術面――ログの運用

操作の証拠である「ログ」について多く問合せを受けるのは“いつまで保存すればいいのか”です。この点に関しては警視庁が“指針”を出しています。2009 年に国内の主なプロバイダーなどに対し、ログを 3 カ月程度保存するよう要請しました。このことから、最低 90 日、願わくは 180 日分の容量を持ちたいものです。その際、ID が複数の従業員で共用されていると証拠の役目が果たせないことになります。ログを調べるのも大変ですが、ネットでは簡便なソフトウェアも紹介されています。

②組織面――職場環境

“気持ちが低下する対策”の 5 位に罰則のことが挙げられています。正に“悪意”を持たれないような職場環境作りです。昨年から具体的に始まった「ストレスチェック」もその一つになりますが、退職者による情報の持ち出しの事案も多数報告されていますので注意が必要です。

また、P マーク運用で義務づけされている「運用の確認」は“自制”“牽制”の効果が期待できます。欠かさず実施したいものです。

４．Ｐマークいろいろ調べてみました

（１）Ｐマーク制度の始まりについて

個人情報保護に関する制度及び法制化の動きは、1980(昭和 55)年に OECD 経済協力開発機構）から、個人情報保護に関するガイドライン(OECD プライバシーガイドライン)が発行されたことに始まります。わが国でも様々な検討がなされましたが、2005 年に「個人情報保護法」が制定されるまでは行政機関以外の個人情報保護に関する包括的な法律は存在せず、民間組織は旧通商産業省や所属団体のガイドラインを利用し、自主的に取り組んでいました。

そこで、積極的に「個人情報保護の取り組み」を実施している事業者に対し、何らかのインセンティブを提供しようと 1998 年に誕生したのが「プライバシーマーク制度」でした。

因みに、1998 年のＰマーク付与事業者数は 58 社でした。

（２）昨年（2016 年）末の業種別Ｐマーク取得事業者数（JIPDEC 公表資料より）

業種名	2015 年	2016 年	増減(同率)	業種名	2015 年	2016 年	増減（同率）
農業	2	1	-1 (-50%)	卸売・小売業・飲食店	837	851	14 (1.7%)
建設業	241	258	17 (3.3%)	金融・保険業	272	288	16 (5.8%)
製造業	1,402	1,425	23 (1.6%)	不動産業	184	201	17 (9.2%)
電気・ガス・熱供給・水道業	16	17	1 (6.2%)	サービス業	10,837	11,314	477 (4.4%)
運輸・通信業	654	688	34 (10.4%)	**合計**	**14,445**	**15,043**	**598 (4.1%)**

Ｐマーク取得事業者は、ほぼ全業種で着実に増加傾向を示しています。増加数は、ここ数年は 4～500 社／年で安定的に推移していましたが、昨年は約 600 社と増加数を伸ばしました。

（３）Ｐマークの更新と辞退数について

Ｐマークを取得しながら更新を辞退する事業者も少なくありません。辞退者については、Ｐマーク取得事業者数の累計と有効Ｐマーク取得事業者の関係で知ることが出来ます。2016 年 3 月末で見ると、取得累計 20,199 社に対して有効取得事業者は 14,755 社となっており､その差である約 5400 社が辞退していることになります。また、このことから**Ｐマークの継続率は、73%程度**ということになります。

（４）Ｐマークの取得・更新における審査費用

単位：円（消費税8%込）

	事業者規模					
	新規のとき			更新のとき		
種別	小規模	中規模	大規模	小規模	中規模	大規模
申請料	51,429	51,429	51,429	51,429	51,429	51,429
審査料	205,715	462,857	977,142	123,428	308,572	668,571
付与登録料	51,429	102,858	205,715	51,429	102,858	205,715
合計	308,573	617,144	1,234,286	226,286	462,859	925,715

Ｐマークの新規取得および更新においては、左表に示す審査費用が必要となります。
審査費用は、申請料／審査料／付与登録料で構成され、3 ランク（大／中／小）の事業者規模によってそれぞれの料金が定まっています。

（５）Ｐマーク取得を支援する自治体があります

ご存知でしたか、プライバシーマーク取得に伴う助成金制度を設けている自治体があります。東京都では港区、江東区、江戸川区に以下の通り助成金制度があります。

①港区　中小企業向け支援制度…補助金額：対象経費の 1/2 上限 500,000 円

②江東区　環境認証等取得費補助…補助金額：対象経費の 1/2 上限 200,000 円

③江戸川区　ISO 認証取得、エコアクション 21 認証取得、プライバシーマーク認定取得助成金…補助金額：対象経費の 1/2 上限 500,000 円

東京以外では、横須賀市、千葉市、ひたちなか市（茨城県）などが行っています。

５．トムソンネットからのお知らせ

（１）Ｐマーク取得に関する説明会を実施します

保険代理店のみなさまは、昨年は業法改正対応等、大変多忙な一年だったことと思います。しかしながら、今年は多くの保険代理店様においては、業法改正対応も一段落して、次の経営課題に取り組む準備をなさっていることと存じます。

恐らく「個人情報の保護対応」が経営課題の一つに挙がっている保険代理店様も少なくないと思われます。弊社では個人情報保護の切り札であるＰマーク取得に関する説明会を、みなさまのご希望に沿って実施しますので、下記連絡先に気軽にお声掛け下さい。

このＰマークニュースでも再三お伝えしていますが、新たなＰマークの取得は、法律改正の施行前やJIS規格の改訂前に当たる「現在」が得策と思われます。この機会に是非、ご検討ください。

（２）新人教育に弊社の生損保公開講座をご利用ください

好評を戴いております弊社の生損保研修（公開講座）は、4月までの日程をホームページにて発表し、参加者を募っております。

4月には新入社員を迎える保険代理店様も多いことと思われますが、弊社の生損保基本コースは、初めて保険業界に飛び込む方々にとって、保険の基礎を習得する格好の場であると思います。

是非、公開講座への参加をご検討ください。

以上

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）