Ｐマークニュース ＜２０１４年爽秋号＞　Vol.　９	（株）トムソンネット Ｐマークコンサルティンググループ

２０１４年爽秋号目次

１．Ｐマーク審査基準強化の方向か
２．シリーズ：Ｐマーク取得のための勘どころ（その８：運用その２）
３．２０１２年度個人情報漏えい事故調査報告書（日本ネットワークセキュリティ協会）の概要
４．ご存知ですか！　保護すべき「個人情報」とは
５．トムソンネットからのお知らせ

1. Ｐマーク審査基準強化の方向か

― 経産省個人情報保護法ガイドライン改訂(案)を公表（２０１４．９．２５）―

経産省は「経済産業分野を対象とするガイドライン」の改訂を 2014.9.26 公表し、10.28 までパブコメを実施し、その後改訂する予定です。

今回の改訂は、2014.7.9 に公表されたベネッセからの大量個人情報流失事故（漏洩個人情報 2260 万件　(保護者および子供の氏名、住所、電話番号、子どもの性別や生年月日などの情報が漏洩)からの教訓を受けた対応ですが、**ガイドラインの趣旨は、今までＰマーク審査基準に反映されてきており、 今後のＰマーク審査が、より厳格になることが想定されます。**

改訂ガイドラインに示された骨子は、下記の点です。

（１）人的安全管理措置として、「教育・訓練等を実施する対象である従業者には、派遣社員等の直接雇用関係にない者も含まれることを明確化する。

（２）組織的安全管理措置として、下記を例示している。

・個人データの安全管理の実施及び運用に関する責任及び権限を有する者である個人情報保護管理者（ＣＰＯ）については、原則として、役員を任命すること。また、事業の規模等に応じ、社内に個人データの取扱いを総括する部署を設ける、ＣＰＯが代表者となり個人データの取扱いを監督する「管理委員会」を設置するなど、必要かつ適切な体制を整備すること。
・個人情報保護対策及び最新の技術動向を踏まえた情報セキュリテイ対策に十分な知見を有する者が、社内の対応を確認する（必要に応じ、外部の知見を有する者を活用し確認することを含む）など、監査実施体制を構築すること。
・スマートフォン等の記録機能を有する機器の接続を制限し、機器の更新に対応するよう規程を整備すること。

（３）物理的あるいは技術的な安全管理措置として、下記を例示している。

・例えば、カメラによる撮影や作業への立ち会い等により、記録又はモニタリングを実施すること。

・入退室の際の業務上許可を得ていない記録機能を有する媒体・機器の持ち込み・持ち出しの禁止又は検査の実施。
・入退室の記録を保存すること。
・個人データの監視システムについて、定期的にその動作を確認すること。
・個人データへのアクセスやダウンロードに関するログについて、不正が疑われる異常な記録の存否を定期的に確認すること。

（４）委託先の選定にあたって、「委託先に係わる組織的、人的、物理的、技術的な安全管理措置が、委託する業務内容に沿って、確実に実施されることについて、必要に応じ、委託先の社内体制、規程等の点検、実地検査等を行った上で、その結果について、個人情報保護管理者（ＣＰＯ）等が適切に評価することが望ましい。

（５）委託業務の監査は、定期的に（少なくとも年１回）実施すること等により、委託契約に盛り込んだ内容の実施状況等を調査した上で、その結果について、個人情報保護管理者（ＣＰＯ）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

（６）委託契約に盛り込むことが望まれる事項として、以下を追加する。

・委託先で個人データを取り扱う者の役職又は氏名等（委託先で作業する委託先の従業者以外の者を含む。）に関する事項（契約書とは別のリスト等により、個人データを取り扱う者を把握する場合も考えられる。）。
・安全管理に関する事項が遵守されず、委託先から個人データが流失した場合の損害賠償責任。

（７）再委託先以降の監督

再委託を行う場合には、委託を行う場合と同様に、委託元は再委託先の監督を行うこと。

（８）適正取得のため、下記を確認・対処すること。

・第三者から個人情報を取得する場合において、提供元の選定に当たっては、その保護法の遵守状況（例えば、オプトアウト、利用目的、開示手続き、問い合わせ・苦情の受付窓口をＨＰに明記していることなど）を確認することが望ましい。
・ 第三者から個人情報を取得する場合には、その都度、当該個人情報の取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、適法に入手されていることを確認することが望ましい。
・第三者から個人情報を取得する場合において、当該個人情報が適法に入手されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

２．シリーズ：Ｐマーク取得のための勘どころ（その８：ＰＭＳ運用のポイント②）

ＰＭＳ運用として前号で、

①計画：運用準備（年度運用計画／教育計画／監査計画）

②実施：安全管理規程に基づくルール適用

安全管理実施記録(入退室管理記録、文書授受記録、文書廃棄記録など)

適正管理（従業者への必要な監督、委託先管理）

教育（教育実施）

について説明しました。

今回は、

③点検：運用確認(自主点検項目報告/ＰＭＳ文書見直し/監査チェックリスト点検/規格適合性監査/運用監査/対リスク分析監査/是正および予防措置)

見直し(代表者による見直し)

についてポイントを説明します。各項目の実施ポイントは下表の通りです。

区分	項目	具体的テーマ	実行担当者	作業のポイント
点検	運用確認	自主点検	部門管理者	・規定の手順に従い、社内の全部門においてＰＭＳが適切に運用されていることを、確認する。 ・自主点検項目としては、 －最終退出時の施錠確認等の社内点検 －入退館（室）の記録の定期的な確認 －アクセスログの定期的な確認 は、必須である。
		ＰＭＳ文書見直し	ＰＭＳ事務局	・文書は、制定日、改定日を含め管理する。 ・規定の手順に従い、毎年一回以上実施する。
	監査	監査チェックリスト点検	監査責任者	・作成された監査チェックリストが、業務状況等の変化により、その項目に過不足が生じていないかどうかを見直す。
		規格適合性監査	監査責任者	・事業環境の変化や法令等の改廃に伴って行われた、ＰＭＳ規定や社内規定の改定が、ＪＩＳ規定に適合したものか否かの確認を年１回以上行う。
		運用監査	監査責任者	・決められた手順に従い、運用点検を定期的に行う。 ・監査報告書は監査を実施した状況のほか、問題点や改善すべき事項を記述する。 ・監査員は自らが所属する部門を監査してはならない。
		リスク分析監査	監査責任者	・事業環境の変化や法令等の改廃、さらには新たなシステム機器等の導入等があった場合は、従来のリスク分析におけるリスク評価を見直し、必要であれば追加のリスク対応を行う。
是正予防	是正予防	是正処置および予防措置	部門管理者	・監査での指摘や緊急事態の発生で発見された不適合については、是正措置及び予防措置を講ずることが必要である。 ・立案された是正処置及び予防処置は、実施時期を含め代表者の承認を得て行う。 ・ＰＭＳ規定で定めた手順に従い、是正処置及び予防処置を実施し、是正措置・予防措置管理表等に記録する。
見直し	見直し	代表者による見直し	代表者	・見直しのインプットは、経営環境の変化／監査報告書／是正措置・予防措置管理表となる。 ・次年度のＰＭＳ運用が、現状よりよいマネジメントシステムとなるための方策を盛り込む。 ・規定の手順に従い、年一回以上行う。

３．２０１２年度個人情報漏えい事故調査報告書の概要

ＮＰＯ日本ネットワークセキュリティ協会（ＪＮＳＡ）から２０１２年の個人情報漏えいに係る調査報告書が２０１４年７月に発表されましたので、過去２年（２０１０年／２０１１年）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ながら、概要をみてみました。

（１）個人情報漏えいインシデント概要データ

項目	2010年	2011年	2012 年
漏えい人数	557 万 9316 人	628 万 4363 人	972 万 0065 人
インシデント件数	1679 件	1551 件	2357 件
想定損害賠償総額	1215 億 7600 万円	1899 億 7379 万円	2132億6405万円
一件当たりの平均漏えい人数	3468 人	4238 人	4245人
一件当たり平均損害賠償額	7556 万円	1 億 2810 万円	9313 万円
一人当たり平均損害賠償額	4 万 3306 円	4 万 8533 円	4万4628円

２０１２年については、**インシデント件数が大幅にアップ**したため、件数に比例して漏洩人数も前の２年を大きく上回りました。

また、インシデント一件当たりの規模（漏洩人数、推定損害賠償額額）も残念ながら減少傾向には至っていません。

（２）業種別発生状況（ワースト３）

順位	2010年	2011年	2012年
1	公務 555件（33．1%）	公務 516件（33．3%）	**金融･保険業** **1094件（46．4%）**
2	**金融･保険業** 423件（25．0%）	**金融･保険業** 332件（21．4%）	公務 486件（20．6%）
3	教育･学習支援業 191件（11．4%）	教育･学習支援業 216件（13．9%）	教育･学習支援業 302件（12．8%）

これまでも業種別発生状況では、常にワースト３に入っていた**金融・保険業**ですが、２０１２年は遂にダントツで**ワースト１位**になってしまいました。

実に事故の半数近く（４６%）が金融・保険業で発生しました。

（３）原因別漏えい件数

順位	2010年	2011年	2012年
1	管理ミス 609件（36．3%）	誤操作 539件（34．8%）	**管理ミス** **1391件（59。0%）**
2	誤操作 543件（32．3%）	管理ミス 497件（32．0%）	誤操作 494件（20．1%）
3	紛失･置忘れ 211件（12．6%）	紛失･置忘れ 213件（13．7%）	紛失･置忘れ 189件（8．0%）

個人情報漏えい原因としては、これまでは「管理ミス」と「操作ミス」がほぼ半々であったものが、２０１２年においては、事故の６割が「管理ミス」によって発生しています。

組織として個人情報の取扱いルールが未整備、若しくはルールが存在していても遵守されていないために、社内や主要な流通経路で発生するものであり、企業規模を問わず、組織的な対応が急務と思われます。

４．ご存知ですか！　保護すべき「個人情報」とは

個人情報の保護が重要性には、誰も異議を唱えないと思いますが、肝心の保護すべき「個人情報」とは何かを問われますと、ちょっと答に窮する方も多いと思われます。

そこで、Ｐマーク取得のためスタートである「保護すべき個人情報とは何か」について、説明をしたいと思います。

（１）個人情報の定義

個人情報保護マネジメントシステム（ＰＭＳ）では、『「個人情報」とは、**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等により特定の個人を識別することができるもの（**他の情報と容易に照合することができ**、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）』と定義しています。

すなわち、「個人に関する情報」と「他の情報と容易に照合することができ、…」であることが重要です。

ａ：「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限らず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。

ｂ：「他の情報と容易に照合することができ、…」とは、例えば通常の作業範囲において、個人情報データベース等にアクセスし、照合することができる状態をいい、他の事業者への照会を要する場合等であって照合が困難な状態を除く。

（２）具体的な事例について

区分	事例
個人情報に該当する事例	・本人の氏名 ・生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報 ・防犯カメラに記録された情報等本人が判別できる映像情報 ・特定の個人を識別できるメールアドレス情報(keizai.ichiro@meti.go.jp) 等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等) ・特定個人を識別できる情報が記述されていなくても、周知の情報を補って識別することにより特定の個人を識別できる情報 ・雇用管理情報(会社が従業員を評価した情報を含む。) ・個人情報を取得後に当該情報に付加された個人に関する情報(取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となる。) ・官報、電話帳、職員録等で公にされている情報（本人の氏名等） **(注）漏れになりがちな個人情報** ・携帯電話のアドレス帳／業務の中で二次的に発生する管理資料(データベース、加工情報など／ＰＭＳの運用において発生する記録類(同意書、誓約書、教育理解度把握のためのテスト、アンケートな／バックアップデータ／監視ビデオ／電話音声の録音記録／健康診断結果についての記録(機微情報)／生体認証を採用している場合の生体認証個人情報(静脈認証情報など)（機微情報）
個人情報に該当しない事例	・企業の財務情報等、法人等の団体そのものに関する情報（団体情報） ・記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@xyzisp.jp 但し、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。） ・特定の個人を識別することができない統計情報

（注）個人情報保護法においては、JIS 規程より狭く、生存する個人に関する情報に限定しています。

５．トムソンネットからのお知らせ

１．事務所を移転しました

弊社の事務所が神田から御茶ノ水に移転しました。
新しい事務所はＪＲお茶の水駅から徒歩２分の地で、連絡先は以下の通りです。

〒101-0062 東京都千代田区神田駿河台４－６
御茶ノ水ソラシティ１３Ｆ
電話 03-3527-1666・ＦＡＸ03-5298-2556

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　℡ 090-5528-1712　　平泉　哲史 ℡ 090-3691-5343
本間　晋吾　℡ 090-2762-4623

以上