

2010.07.15

情報セキュリティニュース <2010 No.2>

「2010年度上期における個人情報漏えい事故」 ～傾向と分析から導かれる企業にとって必要な対応～

2010年の年明けより、既に半年が経過しましたが、おりしも今年には個人情報保護法施行から5年となります。この5年間で多くの企業は個人情報保護法の遵守を中心とした「情報セキュリティの対策」に注力してきました。しかしながら、近年では大規模な漏えい事故事例は格段に少なくなっているとはいえ、個人情報漏えい事故はほぼ毎日のように何処かしらで発生しているのです。それは一体どうしてなのでしょう？この疑問に答えるためには、過去に発生した数々の個人情報漏えい事故をつぶさに分析するほかありません。

そこで本稿では、2010年度の1月から5月までに発生した個人情報漏えい事故（注1）についての分析結果、およびその分析結果から導き出される企業にとって必要な個人情報保護対策について解説します。

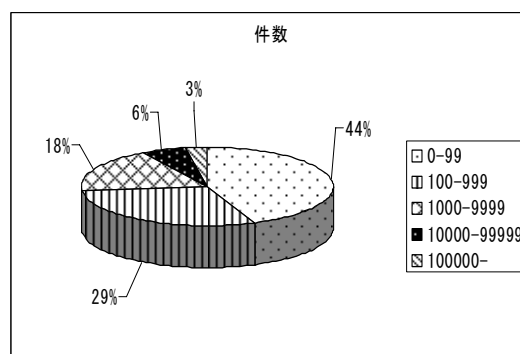
（注1：事故事例については、セキュリティネクストのHP（<http://www.security-next.com/>）にて公開されている情報から収集しています）

1. 個人情報漏えい事故の傾向と分析結果

(1) 漏えい規模の傾向

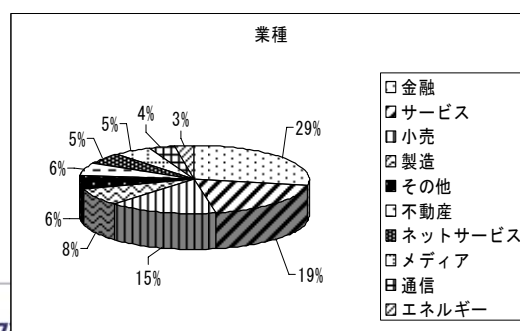
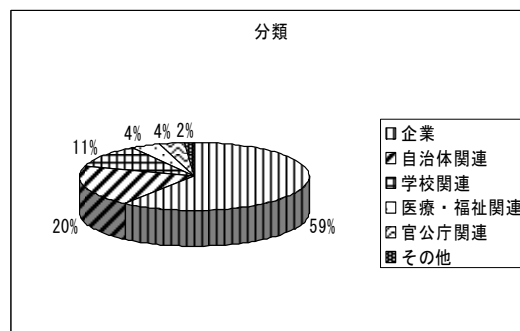
本稿で分析の対象とした事故事例は2010年度の1月から5月までに発生したもので、その総数は199件です。このうち漏えい規模（個人情報の漏えい件数）が公表されている事例は184件あり、漏えい件数の総数は約1,270,959件にのぼります。このうち最大漏えい件数は226,317件、最小件数は1件、1事故あたりの平均漏えい件数は約6,907件となっています。

2009年に発生したような数百万件単位の情報漏えい事故はなく、全体の約7割が1,000件以下の規模にとどまっているようです。



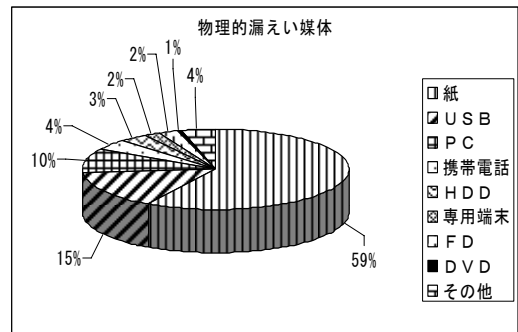
(2) 漏えい組織の傾向

漏えい主体となった組織の分類については、全体の約6割（120件）が民間企業でした。ついで自治体関連、学校関連があわせて約3割（自治体関連：39件、学校関連：22件）程度となっています。民間企業の業種別の内訳については、金融機関が最も多く、民間企業における事例の約3割（約29%）を占めています。ついでサービス業（約19%）、小売業（約15%）、製造業（約8%）といった順位になっています。



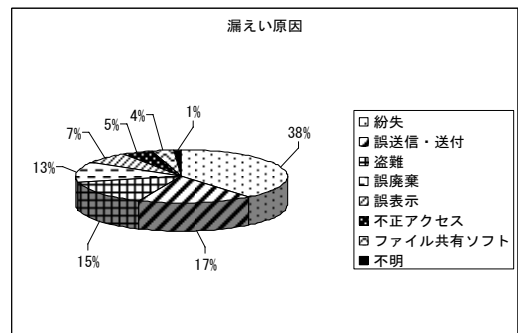
(3) 漏えい媒体と漏えい場所の傾向

事件事例のうち、物理的な漏えい媒体に個人情報が格納されていたケースは144件にのぼっています。このうち、紙媒体（書類、名簿、はがき、その他印刷物）が最も多く、全体の約6割を占めており、ついで、USB（約15%）、PC（約10%）と続いています。物理的な漏えい媒体以外の50件の事例は、電子メールの誤送信、WEBページ上での誤表示、サイバー攻撃によるデータ搾取などです。なお、漏えい発生場所は約7割が組織の内部で発生しており、持ち出しなどによる外出先での発生は約3割となっています。



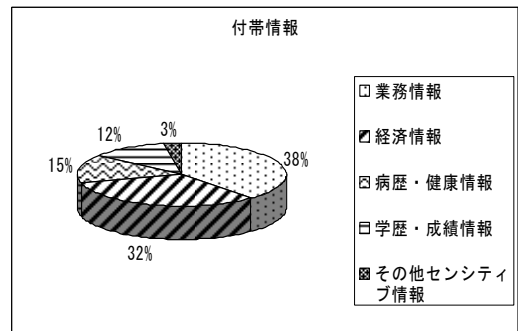
(4) 漏えい原因の傾向

漏えいの原因で最も多いケースは紛失で全体の約4割を占めています。ついで、誤送信・誤送付（約17%）、盗難（約15%）、誤廃棄（約13%）と続いています。なお、約4%にあたるファイル共有ソフトによる事故は6件発生しており、そのうち半分はWINNY利用による自宅PCのウィルス感染が原因となっています。



(5) 個人情報に付帯して漏えいした情報の傾向

個人情報が漏えいした際、住所、氏名、電話番号、メールアドレスなどの基本的な個人情報に付帯して様々な情報が漏えいしたケースは109件ありました。このうち、組織の業務に関連する情報（顧客との契約内容、顧客へのサービス内容など）が約4割を占めており、経済情報（口座番号、所得情報、クレジットカード情報など）、病歴・健康情報、学歴・成績情報と続いています。



(6) 分析結果

2010年度の1月から5月までに発生した199件の個人情報漏えい事故について上記の(1)～(5)を踏まえて分析してみると、注目すべきポイントが2点あります。1つ目は業種と個人情報に付帯して漏えいした情報との関係です。上記(5)の傾向からも半数以上のケースで基本的な個人情報以外の情報が付帯して漏えいしています。さらにその半数のケースが個人にとって大変「重要」な情報に該当しているのです。ここでいう「重要」な情報とは、二次的な被害に繋がるような経済情報（口座番号、所得情報、クレジットカード情報など）や身体的特徴・趣味・嗜好・思想・病歴といったセンシティブ情報などをいいます。

個人情報にも様々なものがありますが、その内容によって漏えいした際の重要度は大きく異なります。言い換えると、漏えい被害者の精神的な苦痛や経済被害の危険性の観点から漏えいした情報の内容及び影響（損害賠償）が異なるということです。日本ネットワークセキュリティ協会では「個人情報の価値」を、経済的損失レベルと精神的苦痛レベルという2つの軸で整理しています。

経済的損失レベルの最も高いカテゴリー（3段階中のレベル3）には、口座番号&暗証番号、クレジットカード番号&有効期限などが該当します。これらの情報は主に金融機関での事故が多く見られます。一般企業でも個人顧客と金銭的なやりとりがある業種では、同じようにこうした情報が漏えいする事故が散見されます。

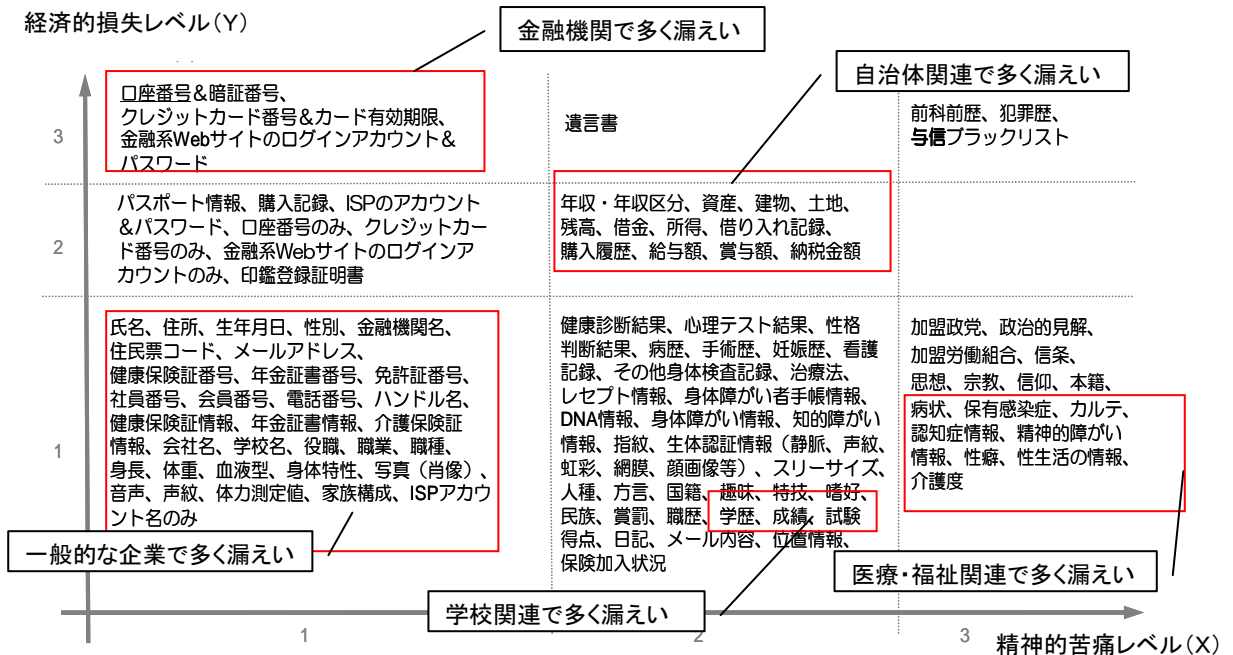
また、精神的苦痛レベル（3段階中のレベル3）の高いものには、病状、カルテ、介護状況などが該当します。医療・福祉関連については、ほとんどのケースで漏えいした情報には病状、病歴などのセンシティブ情報が含まれています。

年収・年収区分、納税情報、所得情報などは、経済的損失レベル、精神的苦痛レベルともに高いもの（3段階中のレベル2）になっています。これらの情報は主に納税関連の情報、所得に関する情報を取り扱っている自治体関連での事故が多く見られます。

成績関係（成績、試験、得点）も経済的損失レベルはレベル1ですが、精神的苦痛レベルはレベル2となっています。学校関係ではほぼ全てのケースで生徒に関する情報が漏えいしています。

こうした情報が基本的な個人情報に付帯して漏えいするケースが数多く見られる背景には、企業以外（自治体関連、学校関連、医療・福祉関連、官公庁関連）の組織が主体となった事例が4割にもものぼっているという点が挙げられます。こうした企業以外の組織に対しては、人々からの情報管理に関する信頼度が極めて高い傾向にあることから、情報漏えい事故の発生は、組織全体の信頼を大きく損ねてしまう危険性を含んでいます。あらためて情報漏えい事故防止への取り組みは、企業だけの問題ではないということを認識する必要があります。

また、一般的な企業であっても、業務内容によってはこうした重要な情報が基本的な個人情報に付帯して漏えいする危険性があるということに、留意が必要です。



※日本ネットワークセキュリティ協会「2008年度 情報セキュリティインシデントに関する調査報告書より

注目すべきポイントの2つ目は、漏えい媒体と漏えい原因の関係です。漏えい媒体として最も多かったケースが紙媒体（書類、名簿、はがき、その他印刷物）でした。これは漏えい原因とも密接に関係していると考えられます。漏えい原因に占める紛失、誤廃棄の割合は約5割をしめています。つまり、昨今の個人情報漏えい事故では、業務上の過失による紙媒体の紛失や誤廃棄がいまだにあとを絶たないということなのです。

また、USBが紙媒体について高い割合（約15%）を占めていることも留意する必要があります。近年ではUSBの記憶容量が格段に増えており、しかも安価のため今や、SDカードと並んで外部記憶媒体の主流といってもよいでしょう。ここで留意したいのは、USBには大量のデータが保管できること、また非常に持ち運びやすいということです。言い換えれば、大容量のデータを持ち運ぶことにより、社外で紛失したり、盗難の被害に遭う危険性があるということです。大変便利な反面、しっかりとした使用管理を行うことが求められるということになります。

USB同様に大量の情報を格納しているのが、PC、HDD、DVD/FDです。なかでも特に注意したいのがHDDです。USB以上にHDDは大容量です。このため、誤廃棄してしまった場合は、外部への漏えいの危険性はもちろん、組織の業務遂行上にも大きな影響を与える危険性があります。

携帯電話については、USB同様に紛失しやすい媒体であるということがいえます。最近では、スマートフォンが流行しており、業務で使用する上でも大変利便性の高い機能を有していることから、携帯電話の紛失による業務情報が付帯した個人情報漏えい事故の増加が懸念されます。

物理的な媒体以外では、メールでの誤送信、WEBページ上での誤表示による漏えいが数多く見受けられます。WEBページのセキュリティ管理について脆弱な企業が潜在的に多ければ、こうしたケースによる漏えい事故も今後増えていくことが懸念されます。また、ファイル共有ソフト（WINNY, SHARE）による漏えいもあとを絶ちません。物理的な媒体、もしくは電子メールなどにより自宅のPCへ個人情報を格納することがこのケースの温床になっているといえます。

	紛失	誤送信・送付	盗難	誤廃棄	誤表示	不正アクセス	ファイル共有ソフト
紙	◎	△	○	○	×	×	×
USB	◎	×	○	△	×	×	×
PC	◎	×	◎	×	×	×	×
携帯電話	◎	×	△	×	×	×	×
HDD	◎	×	×	◎	×	×	×
DVD/FD	◎	×	×	○	×	×	×
物理的な媒体以外 (電子データ)	×	◎	×	×	◎	○	○

注：凡例（◎：特に多くの事例が見られる、○：多くの事例がみられる、△：事例あり、×：事例なし）

2. 企業に必要な今後の対策

ここでは、先述の事故事例の分析結果より、今後、企業にとって必要な対策について2点紹介します。

(1) 対策1「情報資産の分類・整理と重要度に応じた管理施策の実施」

上記1の(6)のとおり、個人情報漏えい時における情報の内容は大変重要です。可能であれば個人情報については真に業務にとって必要な情報のみを保有・管理しておくことが望まれます。そのためには、社内で保有している情報資産を分類・整理することが必要です。その際には、個人情報に限らず、全ての情報資産を対象とされることをお勧めします。分類・

整理のポイントとしては、情報資産の概要、保管媒体、保管場所、管理部門、廃棄年月、委託先会社名、などを明確化して台帳を作成しておくことです。こうした情報資産が一覧化された台帳を作成することができれば、それ以降は台帳をメンテナンスしていくことで効率的かつ適切に情報資産を管理することが可能となります。

次のステップとして必要なことが情報資産ごとの重要度の設定とその重要度に応じた管理施策の実施です。社内で保有する情報については個人情報とそうでないものとあり、また各情報における重要度も様々です。ここでは、その重要度を数種類に分類（例：厳秘→秘→重要）し、情報ごとに設定し、重要度に応じた管理施策を実施していくことが求められます。管理施策については、情報の収集～保管～利用～廃棄までといった情報資産の各ライフサイクルに応じた施策を検討することが必要です。情報資産の重要度に応じて、利用可能者、利用手続を詳細に設定しておくことが望まれます。情報管理施策の検討に際しては、費用対効果にも留意する必要があります。重要な情報資産に関してはコストをかけても管理を徹底する必要がありますが、重要度の低い情報については業務効率を優先した柔軟な管理施策を施行することでもかまわないということです。

なお、こうした情報資産の分類・整理～重要度に応じた管理施策の実施までのプロセスは、情報資産管理ルールとして社内の正式文書（規定類）として策定しておくことが望まれます。

(2) 対策2「従業員への教育の徹底と現場管理実態の把握」

個人情報管理の両輪をなすのは、「システム」と「人」であるといえます。入退出管理、データアクセス管理などはシステムによってセキュリティレベルをある程度保持することができます。システムは定められた動きしかできませんから、対策のレベルとその効果も概ね予想とおりの結果が得られます。しかしながら、「人」の部分はそう簡単ではありません。時に予測不能なことが行われるのです。業務ルールを逸脱した情報持ち出し、管理ルールを無視した情報資産の廃棄、不注意による情報資産の紛失など、この「人」の部分をいかに管理するかが大変重要なのです。そのためには、個々人において徹底して管理ルールを遵守するような職場環境、意識レベルを醸成していくことが必要です。具体的な施策としては、定期的な社内教育や「ケーススタディ」での研修の実施が考えられます。eラーニング教育を活用されるのも良いでしょう。

また、従業員相互で、情報管理実態に関する「クロスチェック」を実施し、従業員相互で確認し合う習慣を促すこともお勧めします。社員への意識啓発施策としては、情報セキュリティハンドブックの交付や携帯カード配布などのツール類により平常時より社員に情報管理を意識付けすることが効果的です。なお、社内規則に情報管理ルールに違反した際の罰則規定を設けて社内によく告知をすることは、意識啓発だけではなく内部犯行抑止への効果が期待できます。

更に、こうした従業員への意識啓発が実際に浸透しているかどうかを把握するために実施することが望まれるのが、現場の個人情報管理実態の把握です。「人」の部分の管理実態は、目でみて把握することが何よりも確実なものです。これについては既存の内部監査の実施、職場の情報管理者による抜き打ちで調査の実施など、各会社に即したやり方を施行することで構いません。「現場を見て、リスクを知る」を是非、実践されることをお勧めします。

3. おわりに

今回の調査では、個人情報保護法施行後から5年経過した今でも、「毎日どこかで個人情報漏えい事故が起きている」という状況であることがわかりました。残念ながら個人情報漏えい事故を100%防止するためには、一切の個人情報を保有しないほかにありません。しかし、それでは企業活

動がままなりません。そこで大切なことは、個人情報漏えい事故の発生の可能性をできる限り低減し、万が一、事故が発生しても迅速な緊急時対応により大きな被害が出ないような、堅牢な情報管理体制を構築することです。そうした体制構築に向けては、平常時より情報管理実態を把握し、改善に向けた取り組みを地道に積み重ねていくことが重要です。本稿が貴社の情報管理対策の見直しの契機となれば幸甚です。

インターリスク総研 コンサルティング第二部 BCM 第二グループ
マネージャー・上席コンサルタント 江尻 明隆

株式会社インターリスク総研は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究およびコンサルティングに関する専門会社です。
情報セキュリティに関しても、コンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問い合わせ先、または、お近くのニッセイ同和損保、あいおい損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合わせ先

㈱インターリスク総研 コンサルティング第二部
TEL.03-5296-8918 <http://www.irric.co.jp/>

本誌は、マスコミ報道など公開されている情報に基づいて作成しております。
また、本誌は、読者の方々が企業の情報セキュリティへの取り組みを推進する際に、役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。

不許複製／Copyright 株式会社インターリスク総研 2010