個人情報漏洩事故と個人情報保護監査

個人情報保護監査研究会
会員 no.9　　蓮見　節夫

2007 年 3 月に、大きな個人情報漏洩事故が公表されています。

一つは、大日本印刷株式会社（以下、D社と略）によるもので「個人情報流出に関するお詫びとお知らせ」が 2007 年 3 月 12 日に同社のホームページに掲載されました。これについては、(財)日本情報処理開発協会プライバシーマーク推進センターより「認証取消しに次いで重い文書による「改善要請」の処分」を決定し、通知したとの発表が 2007 年 3 月 23 日に同協会のホームページに掲載され、さらに「大日本印刷株式会社からの個人情報漏洩事故について」とする公表文が 2007 年 3 月 27 日に同ホームページに掲載されました。

もう一つは、株式会社ソニーファイナンスインターナショナル（以下、S社と略）の「社員による個人信用情報機関情報の外部流出について」（2007 年 3 月 30 日)と、ＵＦＪニコス株式会社（4 月 1 日以降は三菱ＵＦＪニコス株式会社）（以下、M社と略）の「個人信用情報流出の可能性について」(2007 年 3 月 30 日)とが、それぞれのホームページで発表されています。これについては経済産業省より「クレジット会社２社に対する個人情報保護法 34 条に基づく勧告」が行われたと同省のホームページで公表されています(2007 年 3 月 30 日)。

このような漏洩事故に対して、システム監査人は、どのように受け止めたらよいのでしょうか。

1　D社個人情報漏洩事故の概要と対策

以下、ホームページ上に公表されている事故の概要です。

D社が業務委託している会社の元社員が、主に販促用 DM を取扱う電算処理室内で勤務しており、不正な記憶媒体によるデータ書き出しが行われ、外部に持ち出され、一部情報は詐欺にも使われたものです。持ち出されたデータは 2001 年～2004 年に集中しており、総数 7,976,790 件となっています。

その間は、監視カメラの設置、生体認証による入退室管理の強化を行っていたが、内部犯行は防げなかった、2004 年 10 月以降「ポケットのない作業服着用によるデータ等の持ち出し防止」「アクセスログの取得」を行った、としています。

個人情報流出の原因として「悪意を持った内部者による不正な記憶媒体によるデータ書き出し行為を防止する上で、結果として管理に不十分な面がありました」としています。

今後の対策として①データ記憶媒体取扱者の極小化と社員限定、また、記憶媒体への書き出しログのチェック頻度を高める、②記憶媒体の書き出し場所の分離と限定、③再発防止策の徹底教育、を行うとしています。

２　Ｓ社の事故の概要と対策

Ｓ社の発表文による概要と対策の要約です。

「弊社の社員（有期雇用）ならびに派遣社員が、個人信用情報機関の情報の一部を業務目的外で検索し外部に流出させていたことが判明しました」「これまでの調査により、複数の社員が業務時間中に弊社の情報端末を使って、前記個人情報機関から、不正に個人信用情報を取得し、これを外部の者に提供していたことが確認できました」「弊社は、改めて個人情報の管理体制を全社的に見直し、個人情報の取扱いをより厳格なものとし、社員の教育、監督を徹底してまいります。」

３　M社の事故の概要と対策

M社の発表文による概要と対策の要約です。

「弊社の元嘱託社員が、弊社の保有する個人信用情報、および個人信用情報機関から不正に照会して取得した個人信用情報の一部を特定の第三者に不正に提供していた事実が判明いたしました」「(調査結果) 元嘱託社員はアクセス権限の範囲外であるにもかかわらず、個人信用情報機関にアクセスし、不正に個人信用情報が照会、取得され、外部に流出していることが確認された」「(不正照会の数) 673 名様分」「(不正照会の期間) 2004 年 3 月から 2007 年 3 月まで」

「(発生原因) 弊社では、必要な範囲にアクセス権限を制限しています。また、指紋認証システムによる入退室管理、私物の持込・持出の禁止、監視カメラの設置、アクセスログの取得など、セキュリティ面の強化を図っており、個人信用情報機関への不正照会を防止する体制を整えておりました。しかし、今回の件については、事件発生時においては、日常業務に紛れた行動であったことから不審な行動の発見には至りませんでした。また、実際の照会業務と照会結果に不正がないか、事後的にチェックする体制が不十分でした」

「(再発防止への取り組み) 1.信用情報の取扱いに関する緊急の再教育を実施。2.アクセス権限者および照会業務可能端末を必要最低限になるよう絞込む。3.部署ごとに照会端末の利用記録をシステムに出力し、端末利用者の利用内容と突合させて不正利用がないか事後的にチェックする。」

４　経済産業省の勧告の内容（要約）

経済産業省は、Ｓ社及びM社に対し、個人情報の保護に関する法律に基づき、法違反状態を是正し法違反行為の再発を防止するよう勧告しました。特にＳ社については、７日以内に事実関係の追加的な調査結果等を報告するよう併せて勧告しました。認定した違反行為は、個人データの「安全管理措置義務違反」、「従業員の監督義務違反」、「利用目的による制限違反」、「適正な取得義務違反」、「取得に際しての利用目的の通知義務違反」及び「第三者提供の制限違反」です。

Ｓ社に対して

⑴規定に違反したものを特定し、現時点における類似の違反の有無を調査し、違反が行われている場合は、当該違反行為を中止し、当該違反の再発を防止するための必要な措置を講じること

⑵①従業者による個人データへのアクセス状況の監視の用に供することができる適切な方法により従業者による個人データへのアクセスの記録を行うこと、②個人データへのアクセス記録を確認する等の実効的な方法により従業者による個人データへのアクセス状況の監視を行うこと、③従業者の監督の具体的な実施状況を確認し、実施している安全管理措置及び従業者の監督の内容を改善すること

⑶ 勧告に対して取った措置を、平成 19 年 4 月 27 日までに報告すること

M社に対して

⑴ 従業者の監督の具体的な実施状況を確認し、実施している安全管理措置及び従業者の監督の内容を改善すること

⑵ 勧告に対して取った措置を、平成 19 年 4 月 27 日までに報告すること

５　プライバシーマーク推進センターによる「要請」処分

Ｄ社はプライバシーマークの認定を受けている業者です。Ｄ社に対して文書による「改善要請」処分が発表されました（2007 年 3 月 23 日）。その要約です。

以下の 6 項目に対して１ヶ月以内に改善し、その結果を報告すること。

⑴本件事故の関連部門について個人情報の取扱いに関する臨時監査を実施すること

⑵本件事故の原因を特定し、その原因に対して現状の対策が有効であるかの検証をすること

⑶上記⑴⑵の結果を踏まえて現状の措置が有効でないと判断できるリスクに対して、必要な対策を検討すること。この場合、従業者の個人情報の無断・不正持出を防止する措置については特に留意すること

⑷本件事故以外の個人情報の取扱いについて、リスク分析を実施して現状の管理の仕組みを点検し、不具合が認められたところについては、改善策を検討して講じること

⑸以上の事項に関する見直し結果については、個人情報保護マネジメントシステム文書に適切に反映し、関連する全従業者及び委託先事業者に周知・徹底すること

⑹マネジメントシステムの根幹である継続的改善が有効に機能するように対応策を検討し、環境変化に応じた適切な安全管理措置が講じられるようにすること

６　プライバシーマーク推進センターの対応

プライバシーマーク推進センターでは、2007 年 3 月 27 日の公表文において、以下の対応を発表しています。

制度の信頼確保に全力を尽くします：

- 公表される事故等の状況を踏まえ、注意喚起等手段を通じて情報提供を積極的に実施し、認定事業者に適切な対応を求めます
- 環境変化を踏まえた審査基準の在り方を随時検討し、その結果を審査業務に反映し、時代の要請に適切に対応した保護策の実現を図ります
- 審査員制度の下で審査員の質の向上を図り、更に審査員教育を充実する等審査能力の維持・向上に努め、審査結果の信頼性の確保を図ります
- IT 等の進展を踏まえた適切な対応を促すために、セミナー、研究会の実施等によって認定事業者の啓発活動を促進します
- 苦情処理活動を通じて認定事業者の指導・監督を充実し、個人情報保護活動の充実を図ります

制度の改革を検討します：

- 認定事業者の運用状況を定期的に監視・監督する制度
- 事故や事件を起こした事業者に対して、一定期間の後に現地審査によって改善措置の実行状況を確認する制度
- 大規模な個人情報取扱い事業者に対する適正な現地審査のあり方
- 内部監査担当者の監査知識・能力を客観的に評価する仕組

7　個人情報保護監査実施上の教訓

われわれシステム監査人は、個人情報保護監査に直接、間接にタッチすることが多い。また、プライバシーマーク推進センターの制度の改革の中で「内部監査担当者の監査知識・能力を客観的に評価する仕組」を挙げており、われわれシステム監査人に期待されている部分も多くあります。

この事故の中で、どのような教訓を得ることができるでしょうか。

JIS Q 15001 個人情報保護マネジメントシステムの中で、事故との関係で特に重要なところがあります。

(1)　目的外利用を行わないための仕組み

「事業者は、特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならない」ことを求めています。ここは、2006 年版になって追加された要求事項です。これを単なるお題目で終わらせないためには、更に具体化する必要があります。①個人情報の利用目的を特定し関係者に周知しておくこと。②目的外利用をさせないための技術的・物理的対策。たとえば、アクセス制限や入退室制限など。③従業者の監督。④制度的な面としては目的外利用かどうか曖昧な場合は、管理者と相談するなど。⑤事後的なチェックとしてはアクセスログの点検、入退室記録の点検などの日常点検。このとき、問題発見の感度の向上。問題かなと思ったときの報告制度な

ど

(2)　リスクなどの認識、分析及び対策の中のリスク分析の仕組み

「事業者は、特定した個人情報について、その取扱いの各局面におけるリスクを認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない」ことを求めています。これも形が整っていれば良いというものではありません。具体的に詳細に個人情報の取扱いの行われている全ての局面のリスクが洗い出される必要があります。担当者が直接タッチしていないところが抜けることがままあります。外注先、移動中、通信 or 通信の途上、アウトソースされたサーバの中、メールサーバの中、廃棄処理、出先の無人店舗、室、建物、周辺環境などです。

リスク分析は、コンサルタントなどの外部の者にまかせっきりというのはダメです。実際にその仕事にタッチしている人たちを巻き込んで行うことで、隠れたリスクを発見したり、取扱者の意識を高めることができます。

リスク分析をした結果は、リスク対策を行い、必要な規程に反映します。また、企業の体力との関係で 100%完全な対策はできませんから、残存リスクを認識しておくことも重要です。リスク対策は、経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(2007 年 3 月 30 日改正)、金融庁の「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」、厚労省「医療情報システムの安全管理に関するガイドライン」、日本工業標準調査会の「JIS Q 27001 情報セキュリティマネジメントシステム要求事項」の付属書A「管理目的及び管理策」などを参考にして、自社の実態に即した内容で定めます。

リスク分析は、公表された事故の情報なども、自社に当てはめて該当する問題はないか、見直すことも必要です。

(3)　安全管理措置

「事業者は、その取扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要、かつ、適切な措置を講じなければならない」としています。ここは、リスク分析の結果としてのリスク対策が反映されるところです。目的外利用をさせないための物理的、技術的な仕組みもこの中に組み込みます。

安全管理措置は、具体的に規程等に折り込み、関係する人たちに周知しておきます。また、その通りに実施されているかをチェックするための日常点検も組み込みます。

(4)　従業者の監督

「事業者は、その従事者に個人情報を取扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該事業者に対し必要、かつ、適切な監督を行われなければならない」としています。具体的には、誓約書もありますが、上司等との日常的な、報告、連絡、相談の仕組みがあり、かつ機能していることです。監査の点からはなじみにくいのですが、縦・横のコミュニケーションができており、目標に向かって協働できている職場では、内

部犯行は起きにくいものです。一人ひとりが孤立し、ぎすぎすした職場の雰囲気があるところは要注意です。

(5)　委託先の監督

個人情報の取扱いを委託する場合は、十分な個人情報の保護水準を満たしている者を選定する基準を確立すること、個人情報の安全管理が図られるよう委託先の監督を求めています。委託契約書においても、個人情報の取扱いについての条項を入れることを求めています。委託先での個人情報の取扱いについて、必要な頻度で監査・点検ができる仕組みも必要です。

委託先選定基準も、単に形式的に作成するだけではだめです。委託する業務内容や、個人情報の取扱い方によって、リスクが違いますから、取るべき安全対策も異なるものです。委託する側で、必要と思われるチェック項目を用意し、安心して個人情報の取扱いを任せられるかを判断します。プライバシーマークや ISMS の認定事業者であれば OK としてしまうのではなく、具体的に一つ一つの項目をチェックすることが必要です。

委託先に渡す個人情報は、必要な範囲に限定して渡します。

(6)　教育

教育では、a)個人情報保護マネジメントシステムに適合することの重要性及び利点、b)個人情報保護マネジメントシステムに適合するための役割及び責任、c)個人情報保護マネジメントシステムに違反した際に予想される結果、を行うことを求めています。

特に、取扱っている個人情報の利用目的を理解すること、定められた手順に従って取扱うこと、それが目的外利用を阻止する仕組みでもあること、日常活動の中で、“変だな”と思ったことはいつでも上司と相談すること、など、基本的な勤務動作に繋がっています。

(7)　運用の点検

個人情報保護マネジメントシステムが適切に運用されていることが各部門及び階層において定期的に確認されるための手順の確立を求めています。

具体的には、日常点検や、チェックリストに基づく自己点検などです。最終退出時の社内点検の記録と確認、最初に出社した人と最後に退社した人の記録と確認、情報システムへのアクセスログの取得と点検などです。

ここでも点検者は、“異常”、“問題”、“普段と異なる傾向”などへの感度を高める必要があります。何年にもわたって不正アクセスが行われていたにもかかわらず、外部から指摘されなければ気が付かないというのは、記録・点検が、お座なりにしか行われていなかったのではないでしょうか。

(8)　監査

内部監査も、何年にもわたって不正アクセスが行われていたにもかかわらず、気が付かないというのは、反省すべき点が多々あるのでしょう。

当然監査人は、以上に述べてきた事柄について、すべて監査項目として、問題点を指摘

できる能力を要求されています。そのためには、JIS の要求事項や、内部規程のみでなく、技術の進歩や、社会の事件･事故の教訓を自ら取り入れ、不適合や不正に対する感度を高める必要があります。もちろんのこと、経験の積み重ねも必要です。

以上、システム監査人として、事故の教訓を自ら取り込むべく、自分自身の反省も含めてまとめてみました。（記：平成 19 年 4 月 17 日）