⑧ 個人情報保護・情報セキュリティ事故・事件の発生状況と法的規制について

（松田治男委員：財団法人日本データ通信協会　Ｐマーク推進室長）

通信速度の飛躍的向上を実現するNGN時代を迎えて、中堅企業においてもクラウド・コンピューティング技術を活用した業務の効率化とニュービジネスの創造が可能となってきた。一方で、NGN＋クラウド・コンピューティング環境での情報セキュリティ・安定稼働について最も心配であるとの調査結果も出ており、NGN を活用しようとする中堅企業は、C・I・A（Confidentiality、Integrity、Availability）を満足したクラウドベンダーを選定する必要に迫られている。ここでは、総務省、日本情報処理開発協会（JIPDEC）の公表資料から、ネット系サービスに関係する最近の事故・事件発生状況を概括するとともに、個人情報保護・情報セキュリティに関する法的規制・自主規制について解説する。

1.平成 20 年度不正アクセス行為の発生状況

まず、総務省が発表した平成 20 年度（2008 年度）の「不正アクセス行為の発生状況」について整理する。

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/security.html

(1) 不正アクセス行為の発生状況

①認知件数

2289 件でそのうち「国内からのアクセス」が 1993 件を占める。

②被害を受けた特定電子計算機のアクセス管理者

プロバイダーが 1589 件と最も多い。

③認知の端緒

警察職員による被疑者の取り調べ等の警察活動によるものが最も多く（1567 件）、次いで利用権者（ISP 契約者等）からの届け出によるもの（656 件）の順になっている。

④不正アクセス行為後の行為

インターネットオークションの不正操作（他人になりすましての出品等）が最も多く（1559 件）、次いでオンラインゲームの不正操作（他人のアイテムの不正取得等）（457 件）、ホームページ（HP）の改ざん・消去（152 件）、情報の不正入手（E メールの盗み見等）（46 件）、インターネットバンキングの不正送金（37 件）、不正ファイルの蔵置（不正なプログラムやフィッシング用 HP の蔵置等）（5 件）の順になっている。

(2) 不正アクセス禁止法違反事件の検挙状況

検挙件数は 1740 件（助長行為 3 件を含む）。識別符号窃用型は 1736 件で、セキュリティホール攻撃型は 1 件であった。検挙人員は 138 名。

識別符号窃用型のうち、利用権者の管理の甘さにつけ込んだものが最も多く（1368 件）、次いで識別符号を知り得る立場にあった元従業員、知人等によるもの（163 件）、フィッシングサイトやスパイウェア等を使用して入手したもの（136 件）の順になっている。

動機では、不正に金を得るため（1498 件）、オンラインゲームで不正操作を行うため（120 件）、嫌がらせや仕返しのため（52 件）の順になっている。

(3) 不正アクセス防御上の留意事項

パスワードの適切な設定・管理、フィッシングサイトに対する注意、スパイウェア等の不正プログラムに対する注意を挙げている。また、国または民間企業等で実施しているアクセス制御機能の研究成果も公表されているので参考になる。

2.平成 20 年度個人情報の取扱いに関する事故の発生状況

次に、JIPDEC が発表した平成 20 年度（08 年度）の「個人情報の取扱いに関する事故の発生状況」だ。

http://privacymark.jp/news/2009/0707/H20JikoHoukoku_090707.pdf

(1) プライバシーマーク付与事業者の事故報告

件数は 587 社：1276 件で前年度より 213 件減少している。JIPDEC に報告があった 1245 件のうち、委託先において 363 件（29%）発生しているが、これは前年度の 39%から大幅に減少しており、個人情報保護法・JIS の要求事項である「委託先の監督」が適正に行われた結果と分析している。

(2) 事故の原因

JIPDEC に報告のあった 1245 件のうち、「漏えい」が 770 件、「紛失」が 307 件で全体の 87%を占めている。

原因について前年度と比較すると、「メールの誤送信」「盗難」「紛失」が増加している。

(3) 事故に関する注意事項

1) 携帯電話、ノート PC、USB メモリー等の紛失・盗難事故が依然として多い。暗号化・ロック等のセキュリティ対策を講じるとともに、持ち出しについての社内ルールを適正に守るため、従業員に対する意識付けが重要である。

2) 「Bcc:」で送信すべきところを「To:」で送信するなどの操作ミス、個人情報ファイルの添付ミス等の E メール配信に伴う事故が多い。送信前の再確認や添付ファイルの暗号化等の安全管理措置が重要であるが、最終的にはヒューマンエラーを回避するための継続的教育が基本である。

3) ファイル交換ソフトのウィルス感染による情報漏えい事故は依然としてなくならない。未然防止策を講じていると推測されるが、従業員がその対応策を遵守していることの継続的な確認と危機意識の共有がポイントである。

4) 上記の総務省報告にあるように、従業員の不正行為による個人情報の漏えい等が発生しており、一部、本人等への二次被害も発生している。アクセス権管理の見直し、アクセスログの定期的確認、内部報告体制の明確化等とともに、従業員対話や継続的教育の中で

個人情報保護の意識向上が望まれる。

3.個人情報保護・情報セキュリティに関する法的規制

(1)個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号)－個人情報保護法－

個人情報保護法および同施行令により、5000 件を超える個人情報を個人情報データベース等として所持し事業に用いている事業者は、個人情報取扱事業者とされた。主務大臣への報告やそれに伴う改善措置に従わない等の適切な対処を行わなかった場合は、事業者に対して刑事罰が科される。平成 21 年(09 年)9 月、個人情報保護法は内閣府から消費者庁に移管された。

また、事業分野別の「個人情報保護に関するガイドライン」が公表されているので、事業分野特有の個人情報の取り扱いについては該当するガイドラインを遵守する必要がある。

http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

日本データ通信協会(JADAC)は「認定個人情報保護団体」として、「電気通信個人情報保護推進センター」を運営している。

(2)特定電子メールの送信の適正化等に関する法律(平成 14 年 4 月 17 日法律第 26 号)

－特定電子メール法－

携帯電話あての迷惑メールが社会問題化したことなどを受けて、平成 14 年(02 年)に「特定電子メール法」が制定され、受信者から受信拒否通知があった場合に広告宣伝メールの送信が禁止される「オプトアウト方式」規制や「未承認広告」である旨の表示義務等が導入された。さらに平成 17 年(05 年)に法改正され、送信者情報を偽った送信が禁止され、違反の場合は直接刑事罰が科されることとなった。

この改正による一定の成果を上げたものの、依然として巧妙化・悪質化する迷惑メールや外国から送信される迷惑メールに対応するため、平成 20 年(08 年)にさらなる法改正が行われた。この改正により以下のような迷惑メールへの対応強化が図られた。

a)オプトイン方式による規制の導入(同意のない送信の原則禁止)

b)法の実効性の強化(法人の場合、罰金が 3000 万円以下に大幅に引き上げになったこと等)

c)外国から発信される迷惑メールへの対応強化

総務省は特定電子メール法を適用して、出会い系サイトの広告・宣伝メールを送信した個人事業者等に対して改善を命じる措置命令を行っている。

また、JADAC は「登録送信適正化機関」として、「迷惑メール相談センター」を運営している。

(3)不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)

－不正アクセス禁止法－

目的は、不正アクセス行為の禁止とともに、その罰則及びその再発防止のための都道府県公安委員会による援助措置等を定め、電気通信回線を通じて行われる電子計算機に係る犯

罪防止及びアクセス制御機能により実現される電気通信に関する秩序維持を図り、もって高度情報通信社会の健全な発展に寄与することである(1 条)。

最近では、M 証券の元部長代理が他人の ID で顧客データベースにアクセスし(不正アクセス禁止法違反)、会社の CD を無断で自宅に持ち帰り(窃盗罪)、約 5 万件の個人情報を名簿業者に売却するという事件が発生している。

(4)特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律
(平成 13 年法律 137 号)－プロバイダー責任制限法－

ネット掲示板上の誹謗中傷などについて、情報発信者と被害者との間で板ばさみになっていた特定電気通信役務提供者(プロバイダーやネット掲示板管理者など)の責任を軽減することを目的としている。具体的には、一定の条件の元であるならば、情報発信者が発信する情報が違法であるとの判断がなされた時、その情報の削除をした場合に、その情報発信者に対する法的な責任(債務不履行、不法行為による損害賠償責任等)が免除される。また、被害者からプロバイダー等に対して情報発信者の氏名や連絡先等の開示請求があった場合に、それが一定の要件を満たしていると判断されれば、その開示請求に応じることができる。

「プロバイダ責任制限法対応事業者協議会」で対応ガイドラインを公表・運用しているので参照していただきたい。

http://www.isplaw.jp/

・名誉毀損・プライバシー関係ガイドライン
・著作権関係ガイドライン
・商標権関係ガイドライン
・発信者情報開示ガイドライン

4.個人情報保護・情報セキュリティに関する自主規制

ISO/IEC 等における国際規格化、JISQ 規格化等を受けて、個人情報保護・情報セキュリティマネジメントがより効果的に活用できるように各種「管理基準」「認証制度」が告示・導入されているので、ISMS やプライバシーマークの認証取得・維持活動を通じて、自社の個人情報保護・情報セキュリティに関するマネジメントシステムを定着化させることが望まれる。

・情報セキュリティ管理基準
・電気通信分野における情報セキュリティ確保に係る安全基準
・ASP・SaaS における情報セキュリティ対策ガイドライン
・ISMS 認証基準 JIS Q 27001:2006(ISO/IEC 27001:2005)
・個人情報保護マネジメントシステム－要求事項(JISQ 15001:2006) 等

JADAC は情報通信分野におけるプライバシーマーク付与認定に係る「指定審査機関」業務を行っている(P マーク推進室)。