個人情報保護法に関する現状と対策とは？

Q

弊社では、インターネットを利用して顧客情報を収集し、CRM（Customer Relationship Management）を社内で構築しています。
新法に対応するための体制整備をしたいと思っていますので、現状と対策について教えてください。

A

二〇〇四年四月二日、政府は、「個人情報の保護に関する基本方針」を閣議決定しました。来年四年の全面施行に向けて、体制整備に取り組むよう求めています。

前回に続いて、現状と対策について説明します。

1 現状

一昨年、総務省（http://www.soumu.go.jp/）が民間企業・地方公共団体・病院・大学などを対象に行った「情報セキュリティ対策に関するアンケート調査」によると、現状は次のとおりとなっています。

① 大手民間企業のセキュリティ管理体制について、専門チームを設置しているのは全体の約二四％にとどまっており、欧米と比較して、体制面での取り組みが遅れていることが指摘されています。

② ウィルス対策は、病院を除き、おおむね対策が実施されています。

③ 外部からの不正アクセス対策は、「ファイヤーウォール」「ルータ」「プロキシーサーバー」等の基本的対策はとられているものの、「VPN」「IDS」「脆弱性アセスメント」「DOS攻撃回避ツール」などは、二〇％に満たない低い数字となっています。

④ セキュリティ・ポリシーの策定は、大手民間企業の約五〇％が「すでに策定済み」「策定作業中」と回答しています。しかし、中小企業は一〇％に満たない数字となっており、病院・学術研究機関では、約四〇％が「策定予定なし」と回答しています。「知識・ノウハウがない」「予算がない」といった理由に集約されます。

⑤ 今後の対策計画としては、「暗号化」「セキュリティ・ポリシーの策定」「社員教育」「IDS」「メール・Webフィルタリング」「VPN機器」「ログ解析」などの項目が高い数字となっています。

2 対策の指針

プライバシー・リスク・マネジメントや情報セキュリティシステムには、最高かつ唯一の方法というものはなく、各企業が重点を置くリスク項目を選択し、合理的判断と資源配分計画の中で実施していくべきものです。

個人情報保護法の規制原理は、①取得利用規制、②セキュリティの確保、③情報主体の権利行使への対応の三つです。

企業はまず、第四章に定められた法的要請を最低限満たす「情報システムとセキュリティ・ポリシー」を構築策定し、訴訟の場においても、これを主張立証できる仕組みを作ることが肝要です。

3 対策…個人情報取扱事業者の義務

(1) 情報の利用目的

個人情報の利用目的をできる限り特定しなければなりません。また、変更する場合には、変更前の利用目的と関連性を有する範囲を超えてはいけません（§15）。さらに、あらかじめ本人の同意を得ないで、特定された利用目的達成に必要な範囲を超えて、個人情報を取り扱ってはいけません。

なお、事業承継によって個人情報を取得した場合には、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはいけません（§16）。

(2) 情報の取得

偽りや不正の手段により個人情報を取得してはいけません（§17）。

また、個人情報を取得した場合、利用目的を変更した場合は、あらかじめその利用目的を公表している場合を除き、速やかにその利用目的を本人に通知し、または公表しなければなりません（§18）。

(3) データ内容の正確性の確保・安全管理措置

利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければなりません（§19）。

また、その取り扱う個人データの漏洩、滅失または毀損の防止、その他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りません（§20）。

(4) 従業者・委託先の監督

従業者および委託先に個人データを取り扱わせる際は、当該個人データの安全管理が図られるよう、必要かつ適切な監督を行わなければなりません（§21）（§22）。

(5) 第三者への提供に関する制限

原則として、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはいけません。ただし、一定の例外があります（§23）。

(6) 情報主体に関する事項

① 保有個人データに関する事項の公表等については、個人データに関し、取り扱い事業者の氏名または名称、個人データの利用目的、開示などの手数料、適正な取り扱いの確保に関して、本人の知りえる状態に置かなければなりません（§24）。

② 開示は、本人から、当該本人が識別される個人データの開示を求められた時は、原則として、遅滞なく個人データを開示しなければなりません。

なお、開示しない旨の決定をした時も通知を要します（§25）。

③ 訂正については、本人から、個人データの内容が事実でないという理由によって、データ内容の訂正、追加または削除を求められた場合には、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、個人データの内容の訂正を行わなければなりません。

なお、個人データの内容の全部もしくは一部について訂正等を行い、また訂正等を行わない旨の決定をした時は、本人に対し通知を要します（§26）。

④ 利用停止については、個人データが利用目的を超え、また、不適正な手段により取得され、本人からデータの利用停止または消去を求められた際は、その求めに理由があれば、個人データの利用停止等に多額の費用を要するなどの困難な事由がある場合を除き、違反を是正するために必要な限度で、利用停止を行わなければなりません（§27）。

⑤ 本人から求められた措置の全部または一部について、その措置をとらない旨を通知する場合、またはその措置と異なる措置を取る旨を通知する場合には、本人に対し、その理由を説明するよう努めなければなりません（§28）。

⑥ 開示等の求めを受け付ける方法を定めることができます。この場合、本人が容易かつ的確に開示等の求めをすることができるよう、個人データの特定に資する情報提供、その他本人の利便を考慮した適切な措置をとらなければなりません（§29）。

⑦ 開示を求められた時は、当該措置の実施に関し、実費を勘案して合理的であると認められる範囲内において、その手数料額を定め、手数料を徴収することができます（§30）。

⑧ 個人情報の取扱事業者に関する苦情は、適切かつ迅速な処理に努め、その目的を達成するために必要な体制の整備に努めなければなりません（§31）。