個人情報保護法と企業のセキュリティ管理

Personal Information Protection Law and Corporate Security Management

椎木　孝斉　　河井　宣之
■SHIIGI Takayoshi　■KAWAI Nobuyuki

「個人情報の保護に関する法律」（以下，個人情報保護法と略記）の全面施行を受け，多くの企業は，この法律に対応できるセキュリティ管理を行うことが必要となった。そのようなセキュリティ管理を行うには，企業は，コンプライアンス及びリスク管理活動の一環として，情報セキュリティ管理に取り組む必要がある。

情報セキュリティ マネジメントシステム（ISMS：Information Security Management System）を中心とした関連規格や制度を活用し，組織的かつ継続的にセキュリティ管理を維持，改善していくことで，積極的な対応を進めることが重要である。

Following the full enforcement of the Personal Information Protection Law, many corporations have found it necessary to implement information security management programs that meet the requirements of that law. To achieve this objective, these corporations are addressing their information security management needs as part of their general compliance and risk management activities.

It is important for such corporations to take proactive action by continuously maintaining their information security management activities on the corporate level utilizing the information security management system (ISMS) and other related standards and schemes.

1 まえがき

個人情報は，現在の高度情報通信社会で事業を展開する多くの企業にとって，非常に重要な意味を持つ情報である。すなわち，有効に利用することができれば，他社との差異化を図りビジネスを推進するための原動力とすることができる一方で，使い方や管理を誤り，個人情報漏えいといった事件を起こしてしまえば，たちまち企業の信用を失墜させ，ビジネスに重大な悪影響を及ぼしうる。

このようななか，個人情報の適正な取扱いを目的として，個人情報保護法が2003年5月に成立し一部施行され，2005年4月には，個人情報を取り扱う事業者への罰則規定を含めて全面施行された[(1)]。

ここでは，個人情報保護法の概要と，個人情報の保護で中心的な役割を果たす情報セキュリティ管理において，企業が組織的に取り組むべき対応について述べる。

2 個人情報保護法の背景

企業が事業を進めるうえで個人情報を取り扱うのは，最近になって始まったことではない。しかし，近年の情報の電子化やネットワーク化が進むなかで，その位置づけが急激に変化しており，それが今回の個人情報保護法の制定に大きな影響を与えた。

2.1 情報の電子化に伴うリスクの増大

電子情報は，大量の情報を蓄積して瞬時に処理することができるとともに，大量の情報をコピーしたり持ち出したりすることも非常に容易である。また，従来の紙文書であれば物理的なアクセスが必要であったものが，電子情報の場合，ネットワークでつながってさえいれば，物理的に移動することなく，どこからでも瞬時にアクセスすることができる。

更に，ネットワーク利用の拡大によって，外部からの不正アクセスのリスクも増大しており，いったん流出してしまった情報は，ネットワークを通じて，コストをかけずに瞬時に広めることができるようになってきている。

実際，近年の個人情報漏えい事件においても，このような電子情報の特性を反映した，大量の個人情報の漏えいが頻発している。

2.2 個人情報利用の増大

情報化社会においては，ユーザーのニーズを把握し，そのニーズに的確に応えていくためには，個人情報の利用は欠くことのできないものであると言える。なぜなら，個人情報を適切に利用することで，その個人に適したサービスを提供できるようになり，最終的な顧客満足が達成できると考えられるからである。このため，企業は多くの活動において，個人情報の収集を進めることになり，収集した情報を様々な企業活動に用いるようになってきている。近年多くの企業で進められてきたCRM（Customer Relationship Management）なども，そういった顧客サービスの向上を目指したも

のと考えることができる。

しかし，この状況は，個人情報を提供する側から見れば，本人が知らないところで，必ずしも本人の希望とは合致しない目的で，個人情報が利用されるのではないかという懸念につながる。そして，そのような目的外利用は，収集された個人情報が本人の知らないところで，ひとり歩きする危険性をもはらんでいる。

個人情報の有効利用を促進するためには，個人情報を提供する側と，収集及び利用する側との信頼関係がもっとも重要であり，安心して個人情報を提供できるようにするためにも，それの適切な保護が重要となる。

3 個人情報保護法の概要

3.1 法律の目的

個人情報保護法の目的及び基本理念は，第1条と第3条にそれぞれ述べられているが，その意味するところは，個人情報の有用性に配慮しつつ，個人情報の権利・権益を確保するところにある。すなわち，個人情報の有効活用を阻害するものではなく，逆に，個人情報を有効に活用するために，個人情報を正しく取り扱い正しく保護することを事業者に求めている，ということを理解する必要がある。

また，個人情報保護法は，いわゆるOECD（経済開発協力機構）プライバシーガイドライン[(2)]の8原則の意図をくみ入れて策定されており，8原則にそれぞれ対応する形で，個人情報取扱い事業者の義務規定が定められている[(3)]。

3.2 各種ガイドラインとの関連

個人情報保護法は，行政が民間の事業者を規制する法律という性格を考慮し，第8条において，国が，「事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定」を行うことを規定している。これを受け，各省庁で，所管する事業者を対象としたガイドラインが策定されている[(4)]。

違法かどうかを最終的に判断するのは裁判所であるとはいえ，該当するガイドラインには必須事項も含まれており，対象事業者は，それらが拘束力を持ちうるものとして対応する必要がある。

中でも，経済産業省による「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」（以下，経済産業省ガイドラインと略記）は，そのほかのガイドラインのベースとなるものである。したがって，各事業者においても，確実に内容を押さえておく必要がある。

3.3 情報セキュリティとの関連

個人情報保護法における安全保護，すなわち情報セキュリティに関連するのが，第20条～第22条の義務規定である。

第20条は安全管理措置すなわち情報セキュリティ対策の中心的な義務規定であり，「個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又は，き損の防止その他の個人データの安全化のために適切な措置を講じなければならない」とされている。

想定される脅威として，一般的に想定される情報の漏えいのほかに，滅失やき損が挙げられており，個人情報に関して，機密性，完全性，可用性それぞれの確保を行う必要性を述べていると考えることができる。法律においては，必要な対策について具体的には，述べられていないが，例えば経済産業省ガイドラインでは，「組織的」，「人的」，「物理的」，「技術的」のそれぞれの観点から必要な対策を実施することを求めており，個別のセキュリティ対策だけではなく，体制やルールを含めた組織としての包括的な対策を実施する必要がある。

第21条と第22条では，従業者及び委託先それぞれに対する個人情報の取扱いに関する監督について義務規定が定められている。昨今頻発している，内部の従業者や委託先からの個人情報の漏えい事件に対応する規定であり，人に関するセキュリティの重要性を踏まえたものと考えることができる。

企業は，内部の従業者及び委託先を単純に信じるのではなく，両者に起因するリスクを認識し，必要な対策を実施する必要がある。

4 これからの企業のセキュリティ管理

4.1 CSRとコンプライアンス・リスク管理

企業活動において，企業を取り巻くステークホルダーに積極的に貢献し，社会的責任を果たすCSR（Corporate Social Responsibility）の重要性が，大きくクローズアップされるようになってきている。そこでは，企業が守るべき事項を確実に遵守する（コンプライアンス）とともに，CSRにかかわる活動を企業が抱えるリスクとして認識し，それを積極的に管理していく，リスク管理としてのスタンスが非常に重要になってきている。

個人情報保護法対応などの法令遵守はもちろんのこと，企業のセキュリティ管理全般においても，このコンプライアンス及びリスク管理の活動として取り組む必要がある。

コンプライアンス・リスク管理の活動においては，それが永続的な活動であり，かつ法令の変更などの変化に対応できるようにする必要があるため，体制を含めて，組織全体として，包括的に対応を進めることが必要である。そのためには，企業はコンプライアンス・リスク管理のための方針を策定し，仕組みを確立し実施して，継続的に維持，改善していくことが重要である。これはいわゆるPlan－Do－Check－Actサイクルに基づくマネジメントシステムを構築し，維持改善を図っていくことにほかならない。

4.2 JIS Q15001 コンプライアンス プログラムとISMS

個人情報保護に関連するマネジメントシステムを構築する場合には，個人情報保護に特化するアプローチと，個人情報を企業の重要な情報資産の一部として考え，企業が取り扱うすべての重要な情報資産に対する，セキュリティ管理の仕組みを構築するアプローチがある。前者がJIS Q15001に基づくコンプライアンス プログラムの確立，後者が情報セキュリティ マネジメントシステム（ISMS：Information Security Management System）認証基準（英国規格BS7799-2：2002）に基づくISMSの確立に該当し，企業は個人情報保護法への対応を進めるうえでは，両規格及び，関連する認証制度を活用することができる（**表1**）。

表1．JIS Q15001とISMS認証基準の比較
Comparison of JIS Q15001 and ISMS certification standards

項　目	認証規格	
	JIS Q15001:1999	JIPDEC ISMS認証基準（Ver.2.0）（BS7799-2:2002）
目　的	個人情報保護	情報セキュリティ管理
第三者認証制度	プライバシーマーク制度	ISMS適合性評価制度（BS7799-2認証制度）
ガイドライン	－	ISO/IEC17799（JIS X5080）
対象とする情報	個人情報のみ	組織が取り扱うすべての情報 （個人情報以外の以下の情報を含む ・経営情報 ・技術情報 ・研究情報，など）
対象範囲	個人情報にかかわる取扱いすべて （安全管理以外の以下の範囲を含む ・利用目的の通知 ・開示，訂正，削除要求への対応 ・苦情処理，など）	情報セキュリティ（安全管理）にかかわる範囲のみ

JIPDEC：日本情報処理開発協会　　ISO：国際標準化機構
IEC：国際電気標準会議

企業の情報セキュリティ管理という観点から考えた場合，企業が守るべき情報資産は個人情報以外にも存在し，守るべき法律も個人情報保護法だけではない。したがって，多くの企業にとっては，組織的なセキュリティ管理の中心的基盤としてISMSを導入し，それに整合する形で，個人情報保護法など各法律の遵守の仕組みを構築し，必要に応じて，ISMSにも法律遵守に伴う修正を施していくというアプローチが有用であろう。

4.3 ISMSとコンプライアンス

ISMSは企業の法令遵守を保証するものではない。しかし，ISMSでは，法令，規制，契約といった事項は，対象組織において遵守が必要なものという形で，コンプライアンスの考え方が基盤として盛り込まれている。

具体的には，情報セキュリティ基本方針の内容やリスクアセスメントの体系において，「法令，規制及び契約上の要求事項」を考慮することが求められているほか，外部環境の変化として法令などが変化した場合には，適切にISMSを見直す必要性がある旨が要求事項として盛り込まれている。ISMSを確立する企業は，まず，情報セキュリティに関連する法律を識別することが必要である。そのうえで，識別された法律について，組織の仕組みとして，遵守するために必要なルールを策定する。なお，ISMS認証取得審査においては，識別された法律及び関連して組織が定めたルールを，実際にどのように守っているかをそのエビデンスとともに提示する必要がある。

また，個人情報保護に関しては，個別で管理策（データの保護及び個人情報の保護）が設けられており，組織として，個人情報に関連する法律を遵守するための対策を，ISMSを確立する場合においても示す必要がある。

4.4 ISMSと安全管理措置

前述のとおり，ISMSに取り組むだけで，個人情報保護法における個人情報を取り扱う事業者に求められるすべての義務規程に対応できるわけではない。個人情報保護法に全面的に対応するには，組織がISMSとは別に対応を考える必要がある。

ISMSが対応するのは，個人情報保護法の安全管理措置に関連する義務規程であり，更に，安全管理措置の中でも経済産業省ガイドラインでいうところの「組織的安全管理措置」に関連する部分である。

経済産業省ガイドラインでは，「組織的安全管理措置として講じなければならない事項」として，5項目が挙げられており，その各項目について，「講じることが望ましい事項」も詳細に述べられている。

そこで，ISMSの観点で見た場合の各項目の対策ポイントを述べると，次のようになる。

⑴　組織体制の整備　　経営層レベルから，各部門管理者，担当者に至るまでの，全社的な体制の構築。特に個人情報保護の体制と情報セキュリティの体制が別にある場合は，両者の整合性をとることが重要。

⑵　規程の整備と運用　　必須の対応を含みかつ，組織が実施可能なルールの整備と文書化。更に，法的要求事項も含めた記録の採取と定期的な検査。

⑶　取扱い状況を一覧できる手段の整備　　法的要求事項に関連する資産を識別できる資産台帳の整備と定期的な更新。

⑷　安全管理措置の評価，見直し及び改善　　ISMSの内部監査の計画と実施。マネジメント層による評価（マネジメントレビュー）の定期的な実施。

⑸　事故又は違反への対処　　既遂，未遂のものも含めた迅速な報告。過去の事件・事故事例の蓄積と活用。

5 当社のISMS関連サービス

5.1 ISMS認証取得コンサルティング

これまで述べたとおり，ISMSの確立は，これからの企業のセキュリティ管理に非常に有用である。しかし，それが組織の経営活動の一部であり，継続的な活動である以上，適切に導入しないとISMSの導入が逆に企業にとっての新たなリスクとなりうる。

当社のISMS認証取得コンサルティングでは，その点を踏まえ，認証取得の範囲や体制の決定，今後の認証範囲の拡大シナリオなど，初期の方針策定の段階から参画し，ユーザーが無理のないISMSの構築を進められるように，ユーザーのISMSのマスタープラン策定を支援するメニューを用意している。また，メインのサービスとなるISMS構築段階のコンサルティングにおいても，現状の業務プロセスや，現在のセキュリティ管理状況を十分考慮することで，企業が継続的，段階的にレベルアップし，企業文化として定着するまで継続的に実施するという，ISMSの基本を踏まえたコンサルティングに注力している(**図1**)。

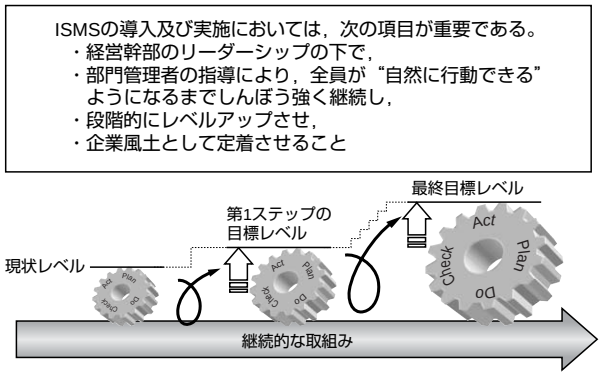

図1．ISMSの基本 ― 継続的な改善により，段階的にレベルアップさせ，定着させていくことが重要である。
Basis of ISMS

5.2 セキュリティ監査サービス

ISMSなどのマネジメントシステムにおいては，それが適切に実施されているかというCheck(確認)の活動が非常に重要である。セキュリティ監査サービスは，そのCheckの活動を支援するサービスとして実施しているものである。

当社のセキュリティ監査サービスは，監査によって企業みずからが現状のセキュリティ管理レベルを把握し，みずからがセキュリティの向上を進めていくための助言を行うサービス(情報セキュリティ監査制度[5]に基づく「助言型監査」)を中心として実施している。

また，監査にあたっては，関係者へのヒアリングや現場の確認といった一般的な監査方法に加えて，必要に応じて，情報システムの脆弱(ぜいじゃく)性を専用のツールを利用して詳細に診断するという，技術的な手法も組み合わせて実施している。これにより，ユーザーの目的及び監査の重点に対応して，様々な監査に利用してもらうことができると考えている。

6 あとがき

情報セキュリティは，個人情報保護の観点からも，企業にとってますます重要になってきている。当社は，今後もISMSを中心としたサービスを提供することで，企業がセキュリティ管理を組織的かつ継続的に維持，改善していくための支援を行っていく。

また今後は，セキュリティ監査サービスを更に充実させることに加え，情報セキュリティにかかわるコンプライアンス対応の支援や事業継続管理にかかわるサービスを確立し，企業の「情報セキュリティガバナンス」[6]の構築を，ソリューションの提供と合わせて，支援していく予定である。

文　献

(1) 内閣府．個人情報の保護に関する法律(平成15年第57号)．<http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html>，(参照 2005-04-04)．
(2) OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.<http://www1.oecd.org/publications/e-book/9302011E.pdf>, (参照2005-04-04)．
(3) 内閣府．OECD8原則と個人情報取扱事業者の義務規定の対応．<http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/pdfs/gensoku.pdf>，(参照 2005-04-04)．
(4) 内閣府．個人情報の保護に係る関係省庁の検討状況．<http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html>，(参照 2005-04-04)．
(5) 経済産業省．情報セキュリティ監査制度．<http://www.meti.go.jp/policy/netsecurity/audit.htm>，(参照 2005-04-04)．
(6) 経済産業省．企業における情報セキュリティガバナンスのあり方に関する研究会報告書．<http://www.meti.go.jp/report/data/g50331dj.html>，(参照 2005-04-13)．

椎木　孝斉　SHIIGI Takayoshi
東芝ソリューション(株) プラットフォームソリューション事業部 プラットフォームソリューション第三部主務。情報セキュリティサービスの開発に従事。情報処理学会会員。
Toshiba Solutions Corp.

河井　宣之　KAWAI Nobuyuki
東芝ソリューション(株) プラットフォームソリューション事業部 プラットフォームソリューション第三部参事。情報セキュリティ関連コンサルティング及び情報セキュリティシステムの構築に従事。
Toshiba Solutions Corp.