住友化学システムサービス株式会社における個人情報保護法への取り組みについて

住友化学システムサービス(株)
西川　浩
後藤俊則
里村敏子

Concerning Sumitomo Chemical Systems Service's Initiative on the Personal Information Protection Act

Sumitomo Chemical Systems Service Co., Ltd.
Hiroshi Nishikawa
Toshinori Goto
Toshiko Satomura

The Personal Information Protection Act, which implements the 8 Principles of the Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD), went into full effect in April 2005. The background and requirements of the Act are outlined. Then will be explained the direction with respect to the Act for this company, which is in the business of handling personal information; each process for dealing with the "Safety Management Measures" enacted by this company referring to the Ministry of Economy, Trade and Industry's guidelines; and the "Compliance Program".

はじめに

25年前、1980年9月23日のOECD（経済協力開発機構）理事会で「OECDプライバシーガイドライン」が採択された。この「プライバシー保護と個人データの国際流通についての勧告」の中に8つの原則が記述されており、Table 1で示すOECD8原則と呼ばれる。これが日本も含めて世界各国の個人情報の保護に関する考え方の基礎になっている。日本においてはその後幾多の取組を経て、2003年5月に「個人情報保護関連五法」が成立した。この時点で行政機関だけでなく、民間部門における個人情報保護に関する法整備が整ったといえる。関連五法の中で、民間事業者に関わる法律は「個人情報の保護に関する法律（平成15年法律第57号）」であり、これが通常「個人情報保護法」と呼ばれている。

個人情報保護法では、「個人情報取扱事業者」に対して、OECDの8原則を踏まえた義務を各条文で定めている。この義務の中で、用語の解釈や守るべき義務についての詳細な解釈及びその実現程度や方法に関しては、それぞれの事業分野毎に異なることを考慮し、所管省庁が別途ガイドラインを示すこととした。経済産業省では、平成16（2004）年10月に「経済産業分野を対象とするガイドライン」[1] を公表した。そして、個人情報保護法は、「個人情報の保護に関する基本方針」[2] の平成16（2004）年4月閣議決定を経て、平成17（2005）年4月1日に全面施行された。

住友化学㈱と住友化学システムサービス㈱（以下当社）は、個人情報保護法が定める、「個人情報」を体系的に構成した「個人情報データベース」を取扱っており、後述するように、法が定義するところの「個人情報取扱事業者」に該当する。また、当社は住友化学㈱の「個人情報」を顧客から委託されてシステム的に取扱っており、受託関係にある。個人情報保護法では、個人情報に関する委託先の監督義務が記載（第22条）されている。このため、当社は個人情報取扱事業者として法に対応することはもちろん、受託事業者として、住友化学㈱の監督を受けることになる。

当社は、2004年の10月頃から、半年後に控えた個人情報保護法の全面施行への対応検討を開始した。

個人情報保護法の第4章では、「個人情報取扱事業者が遵守すべき義務」を定めている。この義務はデータの安全に関する「安全管理措置」と、データ収集目的の明確化やデータ内容の正確さを企業として約束する「コンプライアンス・プログラム」とに大別できる。それぞれが経済産業省のガイドラインによって具体化されている。

Table 1 OECD 8 Principles
OECD8**原則**

Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
収集制限の原則	**個人データの収集には制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。**
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
データ内容の原則	**個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。**
Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
目的明確化の原則	**個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。**
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except : (a) with the consent of the data subject; or (b) by the authority of law.
利用制限の原則	**個人データは、目的明確化の原則により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。** **(a) データ主体の同意がある場合、又は、** **(b) 法律の規定による場合**
Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
安全保護の原則	**個人データは、その紛失もしくは不当なアクセス、破壊、使用、修正、開示等の危険に対し、合理的な安全保護措置により保護されなければならない。**
Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
公開の原則	**個人データに係わる開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。**
Individual Participation Principle	An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs
個人参加の原則	**個人は次の権利を有する。** **(a) データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること** **(b) 自己に関するデータを、** **(i) 合理的な期間内に、** **(ii) もし必要なら、過度にならない費用で、** **(iii) 合理的な方法で、かつ、** **(iv) 自己に分かりやすい形で、自己に知らしめられること。** **(c) 上記 (a) 及び (b) の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異議を申立てることができること。** **(d) 自己に関するデータに対して異議を申し立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。**
Accountability Principle	A data controller should be accountable for conforming with measures which give effect to the principles stated above.
責任の原則	**データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。**

このガイドラインでは「個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格」という項を設け、「個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを策定し、実施し、維持し及び改善を行うことが望ましい」と記載している。さらに「なお、その体制の整備に当たっては、日本工業規格 JIS Q 15001**「個人情報保護に関するコンプライアンス・プログラムの要求事項」**[3] **を、個人データの安全管理措置の実施に当たっては、**JIS X 5070**「セキュリティ技術 ― 情報技術セキュリティの評価基準」**[4] **及び**JIS X 5080**「情報セキュリティマネジメントの実践のための規範」**[5] **等を参考にすることができる」と記述している。**

JIS X 5080**は情報セキュリティマネジメントに関する国際標準**ISO 17799**をJIS化した規格である。つまり個人情報保護法が要求する「安全管理措置」を実現するには、**ISMS（Information Security management System）**の手法をベースにすることが合理的であると解釈できる。また、**JIS Q 15001**はいわゆる**

プライバシーマーク制度といわれるものであるが、そのマネジメントシステムはISO 9000やISO 14000と軌を一にするものである。当社は2001年にISO 9000に基づくQMS（Quality Management System）、2004年にはISO 17799に基づくISMSの認証を取得している。

本稿では、最初に個人情報保護法について概観する。次に、ガイドラインが要求する「安全管理措置」と「コンプライアンス・プログラム」への当社の対応について具体的に報告する。

個人情報保護

経済・社会の情報化の進展に伴い、コンピュータやネットワークを利用して大量の個人情報が収集され処理され保管されている。それに伴い、個人情報の取扱いは、今後もますます拡大していくが、個人情報の性質上、一度誤った取扱いがされると、個人に取り返しのつかない被害を及ぼす懸念がある。Table 2には最近発生した個人情報漏洩事件（出典：IT保険ドットコム等）の一部を掲げている。情報化社会においては、個人情報の流通は必要不可欠であることから、既にOECD加盟国の大多数が、前述したOECDガイドラインの原則を遵守した個人情報保護法制を有するに至っている。日本においても、個人情報保護法が平成15（2003）年5月に成立・公布された。法は、官民を通じた個人情報保護の基本理念等を定めた基本法に相当する部分と、民間事業者の遵守すべき義務等を定めた一般法に相当する部分から構成されており、平成17（2005）年4月1日より全面施行された。

Table 2 Personal Information Leak Incidents
個人情報漏洩事件

Discovered **発覚時期**	Organization **事業者名**	Records **件数**	Content **内容**	Cause **原因**	Compensation per person **1人当たりの支払額**
Jun.03 **H15年6月**	Lawson **ローソン**	560,000	Card member information **カード会員情報**	Internal crime? **内部犯？**	¥500
Jul.03 **H15年7月**	Ricoh **リコー**	60,000	Family registry information tape **戸籍情報** MT	Lost in transit by courier **宅配便で輸送中紛失**	?
Aug.03 **H15年8月**	A-Plus **アプラス**	80,000	Member information **会員情報**	Removed by contractor employee? **委託先社員の持ち出し？**	¥1,000
Oct.03 **H15年10月**	Family Mart **ファミリーマート**	180,000	E-mail newsletter subscribers **メルマガ購読者**	Removed by employee or contractor employee? **社員、委託先社員の持ち出し？**	¥1,000
Jan.04 **H16年1月**	Sanyo Shinpan **三洋信販**	1,160,000	Loan balance **貸付残高**	Employee participation? **社員関与？**	case-by-case **個別対応**
Feb.04 **H16年2月**	Yahoo! BB **ヤフー**BB	4,520,000	Subscriber information **契約者情報**	ID, password left out **ID、パスワードの放置⇒盗み見**	¥500
Mar.04 **H16年3月**	Japanet Takata **ジャパネットたかた**	300,000	Customer list **顧客名簿**	System development company? **システム開発会社？**	?
Apr.04 **H16年4月**	Cosmo Oil **コスモ石油**	2,200,000	Card member information **カード会員情報**	Leaked by insider? **社内から流出？**	?
May.04 **H16年5月**	Mitsubishi Materials **三菱マテリアル**	1,100	Online customer information **ネット販売顧客情報**	Inadequately protected web page **HPの対策不備**	?
Oct.04 **H16年10月**	Mie Prefectural Library **三重県立図書館**	133,000	User information **利用者情報**	Contractor employee removed without permission, stolen PC **委託社員無断持出⇒PC盗難**	?
Nov.04 **H16年11月**	Rihga Royal **リーガロイヤル**	12,000	Guest information (including credit card) **宿泊者情報（クレジットカード含む）**	Stolen PC **パソコン盗難**	?
Feb.05 **H17年2月**	NTT Docomo NTT**ドコモ**	25,000	Customer list **顧客名簿**	?	?
Mar.05 **H17年3月**	Club Tourism **クラブツーリズム**	90,000	Subscriber information **契約者情報**	Unauthorized access **不正アクセス**	?
Apr.05 **H17年4月**	Michinoku Bank **みちのく銀行**	1,310,000	Subscriber information (including bank account information) **契約者情報（口座情報含む）**	Incorrect disposal? **誤破棄？**	?
May.05 **H17年5月**	Kakaku.com **カカクコム**	22,000	E-mail addresses **メールアドレス**	Unauthorized access **不正アクセス**	?
Jul.05 **H17年7月**	Rakuten Ichiba **楽天市場**	36,000	Subscriber information **契約者情報**	?	?

1．個人情報保護法の構成

Table 3に示したように個人情報保護法は、6章から構成されている。法の目的は、個人情報の有効性に配慮しつつ、個人の権利利益を保護することである。そのために基本理念（第3条）及び政府による基本方針の作成（第7条）、その他の施策の基本となる事項を定め、国および地方公共団体の責務等（第2章）を明らかにし、さらに個人情報を取り扱う事業者の遵守すべき義務（第4章）を定めている。

個人情報取扱事業者の義務に関する規定は、公共部門が「行政機関個人情報保護法」[6]や「独立行政法人等個人情報保護法」[7]で定められているのに対して、民間部門に対する義務規定は「個人情報保護法」で定められている。

前述したように、各省庁の主務大臣が法を執行するための基準として各省庁が告示する省庁ガイドラインが制定されており、当社が個人情報保護に対する対策を検討する場合は、法本体と経済産業省ガイドラインがその枠組みとなる。

Table 3 Contents of the Personal Information Protection Act
個人情報保護法の構成

Chapter 1. General Rules
第1章　総則
— Purpose (Article 1)
目的（第1条）
— Definitions (Article 2)
定義（第2条）
Personal information
個人情報
Personal information database
個人情報データベース
Personal information-handling organization
個人情報取扱事業者
Personal data
個人データ
Own personal data
保有個人データ
— Basic philosophy (Article 3)
基本理念（第3条）
Chapter 2. Responsibilities, Duties, Etc. of National and Regional Public Bodies
第2章　国及び地方公共団体の責務等
Chapter 3. Measures, Etc. Relating to the Protection of Personal Information
第3章　個人情報の保護に関する施策等
— Basic policies (Article 7)
基本方針（第7条）
Chapter 4. Duties, Etc. of Personal Information-Handling Organizations
第4章　個人情報取扱事業者の義務等
Section 1. Duties of Personal Information-Handling Organizations
第1節　個人情報取扱事業者の義務
Section 2. Promotion of Personal Information Protection by Private Bodies
第2節　民間団体による個人情報の保護の推進
Chapter 5. Additional Rules
第5章　雑則
Chapter 6. Penalties
第6章　罰則

2．個人情報とは

個人情報保護法では、「個人情報」、「個人データ」及び「保有個人データ」の語を使い分けており、個人情報取扱事業者に課せられた義務はそれぞれ異なるので、注意を要する。経済産業省のガイドラインでは、それぞれについて事例を挙げて詳細な解説を行っている。

(1) 個人情報

「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問わない。

例えば、当社のメールシステムで採用しているアドレスはtarou.yamada@sc-sss.co.jpのような形式であるため、「SSS社の誰」、と特定できることから個人情報とみなされる。S100.01@sc-sss.co.jpの形式であれば別に対照表が存在しない場合には個人情報ではない。

(2) 個人情報データベース

「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合物、又はコンピュータを用いていない場合であっても、カルテや指導要録等、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものをいう。

(3) 個人情報取扱事業者

法では、「個人情報取扱事業者」とは、国の機関、地方公共団体、独立行政法人、地方独立行政法人等いわゆる「官」と、個人情報データベース等を事業の用に供している者いわゆる「民」とを定義している。ただし「民」に対しては、個人情報を取扱う事業者全てが「個人情報取扱事業者」とはせず、例外として、「規定並びにその取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが

少ない者を除く」としている。

例外に相当する判断基準としては、個人情報データベースの規模によるものとし、具体的には、政令第2条で、「その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6か月以内のいずれの日においても5,000人を超えない者とする。5,000人を超えるか否かは、当該事業者の管理するすべての個人情報データベース等を構成する個人情報によって識別される特定の個人の数の総和により判断する。ただし、同一個人の重複分は除くものとする。」と定めている。

また、「事業の用に供している」の「事業」とは、一定の目的を持って反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない、とも定めている。

住友化学㈱や当社は5,000人を超えるデータベースを取扱っており、当社は「個人情報取扱事業者」となる。

(4) 個人データ

「個人データ」とは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。

Table 4 Correspondence between OECD 8 Principles and the Personal Information Protection Act
OECD8原則と個人情報保護法との対応

	OECD 8 Principles OECD8原則	Duties of Personal Information-Handling Organizations 個人情報取扱事業者の義務
Purpose Specification Principle 目的明確化の原則	Purpose of collection must be made clear, and use of data must match purpose of collection. 収集目的を明確にし、データ利用は収集目的に合致するべき	ー Must specify as precisely as possible the purpose of use (Article 15) 利用目的をできる限り特定しなければならない。(第15条)
Use Limitation Principle 利用制限の原則	Must not use for other purposes without agreement of the data's subject and compliance with legal procedures. データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない	ー Must not handle beyond the scope necessary for achieving the purpose of use (Article 16) 利用目的の達成に必要な範囲を超えて取り扱ってはならない。(第16条) ー Must not divulge to third party without obtaining permission from person concerned (Article 23) 本人の同意を得ずに第三者に提供してはならない。(第23条)
Collection Limitation Principle 収集制限の原則	Should collect data by legal and fair methods after informing and obtaining agreement from the subject. 適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき	Must not collect data with deceitful or other unfair methods (Article 17) 偽りその他不正の手段により取得してはならない。(第17条)
Data Quality Principle データ内容の原則	Data should fit the purpose of use and be accurate, complete, and up-to-date. 利用目的に沿ったもので、かつ、正確、完全、最新であるべき	Must work to keep information accurate and up-to-date (Article 19) 正確かつ最新の内容に保つよう努めなければならない。(第19条)
Security Safeguards Principle 安全保護の原則	Data should be protected from loss, destruction, use, alteration, divulgence, etc. with reasonable measures to safeguard security. 合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき	Must take necessary measures to manage security. (Article 20) 安全管理のために必要な措置を講じなければならない。(第20条) Must perform necessary supervision of employees and contractors. (Articles 21, 22) 従業者・委託先に対し必要な監督を行わなければならない。(第21、22条)
Openness Principle 公開の原則 Individual Participation Principle 個人参加の原則	Should make public the intent to collect data, indicating clearly the data's existence, the purpose for which it is to be used, and the manager responsible. データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき	ー Must give notice or make public announcement of the purpose of use when collecting data. (Article 18) 取得したときは利用目的を通知又は公表しなければならない。(第18条) ー Must put the purpose of use, etc. in a state in which it can be known by the subject person. (Article 24) 利用目的等を本人の知り得る状態に置かなければならない。(第24条) ー Must disclose possessed personal data at the subject person's request. (Article 25) 本人の求めに応じて保有個人データを開示しなければならない。(第25条) ー Must perform corrections, etc. at the subject person's request (Article 26) 本人の求めに応じて訂正等を行わなければならない。(第26条) ー Must cease usage, etc. at the subject person's request. (Article 27) 本人の求めに応じて利用停止等を行わなければならない。(第27条)
Accountability Principle 責任の原則	Should permit persons to confirm the storage location and content of data about themselves, and guarantee a hearing for all complaints. 自己に関するデータの所在及び内容を確認させ、又は意義申立を保証するべき	Must work to process complaints appropriately and promptly. (Article 31) 苦情の適切かつ迅速な処理に努めなければならない。(第31条)

(5) 保有個人データ

「保有個人データ」とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する「個人データ」をいう。

3. 個人情報取扱事業者の義務

個人情報保護法第4章では個人情報取扱事業者の義務などについて、第15条から第36条までを定めている。これはOECD8原則を日本の実情に照らして具体化したものである。Table 4に8原則と法の各条文との対応関係を示した。これらの義務は、大きく安全管理措置に関するものと、コンプライアンス・プログラムの範疇に帰するものに分けられる。

4. 安全管理措置

個人情報取扱事業者の義務を定めている条文の中で、特に第20条では、「安全管理措置」として、「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。」とだけ定めている。

前述したように、必要かつ適切な措置の具体的な内容は事業分野毎に異なる。そこで経済産業省のガイドラインが一定の基準を示しているわけである。ガイドラインでは、まず「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管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。」としている。

つまり、安全管理措置は、組織的、人的、物理的及び技術的という四つの領域で講じるべしとしているわけである。

(1) 組織的安全管理措置

ガイドラインでは「組織的安全管理措置とは、安全管理について従業者（法第21条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。」としている。そして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Table 5に示す5項目を挙げている。

Table 5 Security Management Measures
安全管理措置

Organizational Measures **組織的安全管理措置**	1. Maintain an organization to enact personal data security measures **個人データの安全管理措置を講じるための組織体制の整備**	11
	2. Maintain and operate in accordance to rules established by personal data security measures **個人データの安全管理措置を定める規程等の整備と規程等に従った運用**	5
	3. Maintain a procedure for listing the handling status of personal data **個人データの取扱い状況を一覧できる手段の整備**	2
	4. Evaluate, revise, and improve personal data security measures **個人データの安全管理措置の評価、見直し及び改善**	3
	5. Deal with accidents and violations **事故又は違反への対処**	2
Human Measures **人的安全管理措置**	1. Conclude closed contracts for employment and commission contracts. **雇用契約時及び委託契約時における非開示契約の締結**	2
	2. Perform education and training for workers. **従業者に対する教育・訓練の実施**	3
Physical Measures **物理的安全管理措置**	1. Manage building (office) entries and exits. **入退館（室）管理の実施**	2
	2. Prevent theft, etc. **盗難等の防止**	5
	3. Physically protect machinery and equipment. **機器・装置等の物理的な保護**	1
Technical Measures **技術的安全管理措置**	1. Identification and authorization of access to personal data **個人データへのアクセスにおける識別と認証**	2
	2. Control of access to personal data **個人データへのアクセス制御**	8
	3. Manage permission to access personal data **個人データへのアクセス権限の管理**	2
	4. Log access to personal data **個人データのアクセスの記録**	2
	5. Measures against unauthorized software on information systems that handle personal data **個人データを取り扱う情報システムについての不正ソフトウェア対策**	3
	6. Measures for transport and transmission of personal data **個人データの移送・送信時の対策**	2
	7. Measures for regression testing of information systems that handle personal data **個人データを取り扱う情報システムの動作確認時の対策**	2
	8. Monitoring of information systems that handle personal data **個人データを取り扱う情報システムの監視**	2

(2) 人的安全管理措置

ガイドラインでは「人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。」とし、Table 5に示す2項目を指摘している。

(3) 物理的安全管理措置

ガイドラインでは「物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。」とし、Table 5に示す3項目を指摘している。

(4) 技術的安全管理措置

ガイドラインでは「技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。」とし、Table 5に示す8項目を指摘している。

(5) 講じなければならない事項の具体化

このように経済産業省のガイドラインでは安全管理措置として4つの領域で計18項目を「講じなければならない」としているが、その実現の仕方には当然のことながらいくつかの方法がある。ガイドラインでは、要求項目を実施する上で望まれる事項を列挙している。例えば、技術的安全管理措置の第2番目で要求している「個人データへのアクセス制御」を実現するには、「個人データへのアクセス制御を行う上で望まれる事項」として、

- 個人データへのアクセス権限を付与すべき従業者数の最小化
- 識別に基づいたアクセス制御
- 個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）

等8例を挙げている。

「個人データへのアクセス制御」は必ず講じなければいけないのだが、状況に応じて必要かつ適切な措置を講じることが求められるのであって、その具体的な方法としては、望ましいとして掲げた8項目のどれか（複数も可）、あるいはそれ以外で企業が定める方法で実現すればよい。なお、Table 5の右端の数字は、それぞれの「講じなければならない項目」に対して、列挙された「望ましい対策」の数を示している。

5. コンプライアンス・プログラム

次に、法が求める「コンプライアンス・プログラム」についてであるが、その作成にあたっては、経済産業省のガイドラインで述べている、JIS Q 15001が参考になる。JIS Q 15001では、Table 6に概要を示すとおり第4章で「コンプライアンス・プログラム要求事項」を定義している。要求事項として最初に求めているのは、「事業者の代表者は、個人情報保護方針を定めるとともに、これを実行し維持しなくてはならない」である。個人情報保護法の第4章で定めている義務の中で安全管理措置としてガイドラインが定めている項目を、JIS Q 15001と対比すると、ガイドラインであげている、物理的安全管理措置と技術的安全管理措置を除いたものが、コンプライアンス・プログラム要求事項に相当するといえる。

Table 6 Requirements for compliance program on personal information protection
個人情報保護に関するコンプライアンス・プログラムの要求事項

4.	Compliance Program Requirements Issues **コンプライアンス・プログラム要求事項**
4.1.	General Requirements Issues **一般要求事項**
4.2.	Personal Information Protection Policy **個人情報保護方針**
4.3.	Planning **計画**
4.3.1.	Specification of Personal Information **個人情報の特定**
4.3.2.	Legal and Other Criteria **法令及びその他の規範**
4.3.3.	Internal Regulations **内部規程**
4.3.4.	Planning Document **計画書**
4.4.	Implementation and Operation **実施及び運用**
4.4.1.	Organization and Operations **体制及び運用**
4.4.2.	Measures Concerning Collection of Personal Information **個人情報の収集に関する措置**
4.4.3.	Measures Concerning the Use and Disclosure of Personal Information **個人情報の利用及び提供に関する措置**
4.4.4.	Appropriate Management of Personal Information **個人情報の適正管理業務**
4.4.5.	Rights of Subjects Concerning Personal Information **個人情報に関する情報主体の権利**
4.4.6.	Education **教育**
4.4.7.	Complaints and Consultation **苦情及び相談**
4.4.8.	Compliance Program Document **コンプライアンス・プログラム文書**
4.4.9.	Document Management **文書管理**
4.5.	Audit **監査**
4.6.	Revision by Organization Representative **事業者の代表者による見直し**

6. 法違反の考え方

個人情報保護法第34条では、「主務大臣は、個人情報取扱事業者が第16条から第18条まで、第20条から第27条まで又は第30条第2項の規定に違反した場合

において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。」と定め、さらに、命令（第2項）、緊急命令（第3項）を規定している。この第2項、第3項の規定による命令に違反した者は、「6月以下の懲役又は30万円以下の罰金に処する。」という罰則規定が第56条で定められている。

違反であるか否かは、個人情報取扱事業者が、ガイドラインに沿って必要な措置等を講じたか否かにつき判断して行なわれる。すなわち、ガイドライン中、「しなければならない」と記載されている規定については、それに従わなかった場合は、規定違反と判断され得る。一方、ガイドライン中、「望ましい」と記載されている規定については、それに従わなかった場合でも、規定違反と判断されることはないが、個人情報保護の推進の観点から個人情報取扱事業者としては、できる限りの対応を取り組むことが肝要である。

さらに、法による罰則以外に注意すべきことは、情報漏えいなどを起こした場合に蒙る社会的信用の失墜や、巨額の損害賠償額の負担などである。

個人情報保護法への当社の対応

当社としての個人情報保護法への対応であるが、法の完全施行を半年後に控えた時点で、

- 体制整備、規定類整備、従業者への教育などのコンプライアンス・プログラムの作成及び実施は施行日（2005年4月1日）までに完了すること。
- 安全管理措置については、対象システムを洗い出し、実施している対策現状を早急に把握し、リスクアセスメントを実施する。
- 実施が必要とされる対策については、ITインフラ全体としてのセキュリティ対策を優先とし、個別対策は優先順位を付けて実施する。

という基本方針を定めた。

1．個人データと保有個人データ

個人情報取扱事業者の取扱うデータが、単なる個人データであるか、あるいは保有個人データであるかによって、法の定める義務の範囲が異なる。Table 7に示すように、保有個人データである場合には法第15条から第31条が関係する（Bで示す）のに対して、保有個人データでない場合は、法第15条から第23条が対象となる（Aで示す）。なお、Table 7には違反した場合の罰則規定の対象も示している。

当社の場合は、当社が単に住友化学㈱の個人情報の取扱を受託されている立場では、当社には「保有個人データ」は無いことになるが、当社は従業員情報等のように独自に保有個人データを有している。そのため全ての義務を対象に対応することとした。

また、住友化学㈱が保有する個人データの取扱いを当社が受託している場合は、住友化学㈱として必要な対応と、当社としての対応を整理・相談した上で分担を決定した。

Table 7 Act Enforcement and Penalties
法の適用および罰則の対象

Art. 条	Contents 内容	A	B	Penalty 罰則
15	Specification of purpose of use 利用目的の特定			
16	Limitations by purpose of use 利用目的による制限			
17	Appropriate collection 適正な取得			
18	Notification of purpose of use during collection 取得に際しての利用目的の通知等			
19	Preserving accuracy of data contents データ内容の正確性の確保			
20	Security management measures 安全管理措置			
21	Supervision of employees 従業者の監督			
22	Supervision of contractors 委託先の監督			
23	Restrict disclosure to third parties 第三者提供の制限			
24	Announcement of issues related to possessed personal data 保有個人データに関する事項の公表等			
25	Openness 開示			
26	Revision,etc. 訂正等			
27	Cessation of use, etc. 利用停止等			
28	Reason explanation 理由の説明			
29	Procedure to address requests for disclosure, etc. 開示等の求めに応じる手続			
30	Fees 手数料			
31	Personal information-handling organization complaint process 個人情報取扱事業者による苦情の処理			
32	Report retirement 報告の徴収			
33	Advice 助言			
34	Recommendations and instructions 勧告及び命令			
35	Restrictions on use of authority of competent minister 主務大臣の権限の行使の制限			
36	Competent minister 主務大臣			

2．安全管理措置への対応

前述したように、法が定める「義務」に対しては、安全管理措置とコンプライアンス・プログラムの二つの側面がある。まず最初にISMSをベースにした安全管理措置について述べる。

Fig. 1は安全管理措置対応へのプロセスを示している。当社が取扱う「個人情報データベース」を全て洗い出し、個々に実施管理策を策定していくに先立って、「データベースの重要度」と「実施管理策の選択標準」の2つの標準を策定した。

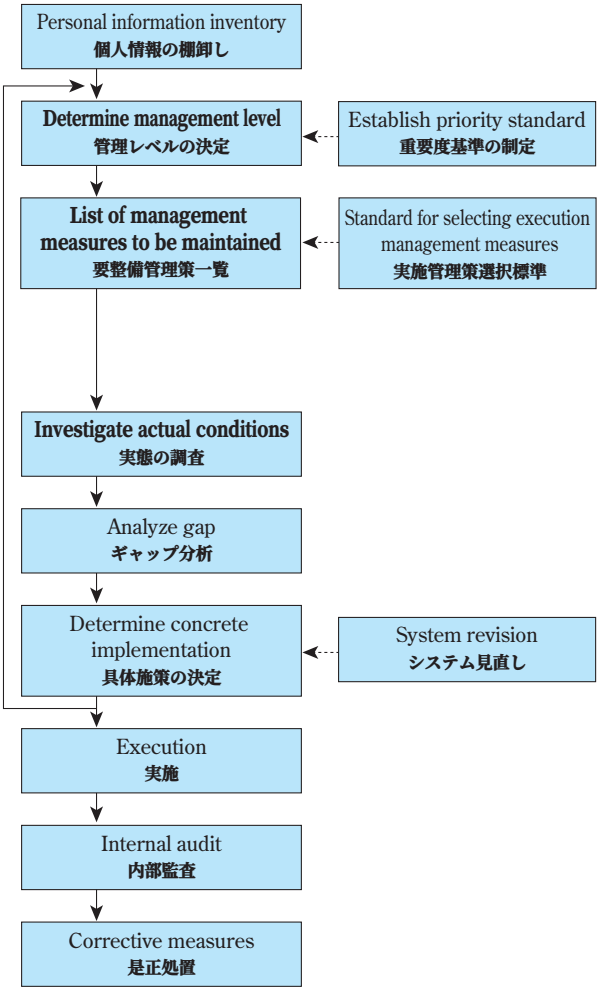

Fig. 1 Security Management Process
安全管理措置対応へのプロセス

(1) データベースの重要度 ― 重要度基準の導入

「個人情報」の定義については前述したが、通常「個人情報データベース」は、氏名等の個人を識別する情報と、その個人の身体、財産、職業、肩書き等の属性を保有するデータ項目とからレコードが構成されている。そこで、使用されている属性を列挙して属性集合（データ項目）を明確にし、個々の属性が持つ重要度を標準として定めた。（Table 8参照）

Table 8 Relation of Priority to Database, Attributes
重要度レベルとデータベース、属性の関係

Priority 重要度	Example Database データベース例	Example Attribute 属性例
3	Health and treatment information 保健医療情報	Physical exam results 健康診断結果
	Economic impact information 経済的影響ある情報	Bank account number 銀行口座番号
2	Information revealing individual characteristics of person 個人の私的特性を示す情報	Personnel evaluation, family structure, residence address 人事評価、家族構成、自宅住所
1	Information on persons outside the organization 組織外の個人に関する情報	Customer information, partner information 顧客情報、取引先情報
0	Information on persons inside the organization 組織内の個人に関する情報	Company e-mail address, telephone extension 社内メールアドレス、社内電話番号

重要度については、個人データが漏洩した場合に本人が被る権利利益の侵害度を考慮して決定することとし、当社では重要度として最上位を3とする、0から3までの4段階を定義した。

(2) 実施管理策の選択標準の決定

Table 5で示したとおり、経済産業省のガイドラインでは安全管理策を4つのカテゴリに分けた上で、各カテゴリ毎に実施しなければならない項目を18項目挙げている。したがって、個人情報取扱事業者は18の項目全てに対して対策を講じなければいけないが、具体的な方法については、ガイドラインが掲げる選択肢の中からひとつ以上を選択すればよいことになる。どの項目を選択するかは、その対策がもたらす効果と実施にあたっての技術的難易度や費用などを考慮することが必要である。そこで、データの持つ重要度に応じて、ガイドラインが示す「望ましい管理策」のどれを採用するかを標準として定めた。

ガイドラインでは「技術的対策」として講じなければならない事項を8項目列挙している。その第1番目が「個人データへのアクセスにおける識別と認識」であり、さらにこの事項に対して、Table 9に示すとおり具体的な方法を2つ示している。この両者を比較すると、前者（IDとパスワードによる識別）は、技術的にもコスト的にも容易に実現できる。後者（端末そのものの識別）は、技術上・運用上の複雑さがある。識別機能は後者の方が当然高い。当社の考え方として、まず全てのシステムは最低限の対策として前者を採用することとし、その中で非常に高い管理を要求される個人情報データベースを運用してい

Table 9 Personal Data Access Identification and Authorization: Measures by Level
個人データへのアクセスにおける識別と認証 レベル別対応策

Issues that must be addressed 講じなければならない事項	Desiable steps 望まれる事項	Management Level 管理レベル
Identification and authorization for access to personal data 個人データへのアクセスにおける識別と認識	In order to confirm access to personal data is justified, carry out identification and authorization (e.g. ID and password authorization, biometric authorization, etc.) that user is worker with access permission. 個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証（例えば、IDとパスワードによる認証、生体認証等）の実施	0
	Perform identification and authorization on terminal or addresses (e.g. MAC address, IP address, electronic certification, secret decentralization technology, etc.) usable by workers with permission to access personal data. 個人データへのアクセス権限を有する各従業者が使用できる端末又はアドレス等の識別と認証（例えば、MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施	3

るシステム（管理レベル3以上）は、後者の対策を併せて採用することとした。

(3) 個人情報の棚卸

基準と標準の策定の後、まず実施したことは、住友化学㈱及び当社に存在する個人情報を全て洗い出し、管理台帳を整備することであった。この管理台帳には、個人情報の内容と、保管運用しているシステム名称がまとめられている。

(4) システム管理レベルの決定

一つの個人情報データベースは複数のデータ項目から構成されている。各データ項目には「重要度レベル」が標準として定義されている。データベースを構成するデータ項目の中で、最大の重要度レベルを持つデータ項目の重要度を、そのデータベースの重要度とすることとした。また、一つのシステムには複数のデータベースが存在することから、そのシステムの中で、最大の重要度を持つデータベースの重要度を、システムの重要度とし、これを「システム管理レベル」と定義した。管理台帳で把握した全てのシステムに対して「管理レベル」を計算し整理した。

(5) 実施管理策の制定

対象としているシステムの管理レベルと、実施管理策の選択標準とから、そのシステムが装備しておくべき管理策一覧を定めた。

(6) 実施管理策作成

対象システムがその時点で、どのような管理策を実施しているかの実態調査を実施した。これと（5）で定めた「装備しておくべき管理策」との相違点（ギャップ）を整理した。

(7) ギャップ分析

装備しておくべきと定めた管理策全体と実態とにはギャップが存在した。このギャップは、個々の事項に関して次の三つのどれかになる。

① 装備しておくべき管理策と合致する（そのシステムのレベルにふさわしい対応策を既に実施している）
② 装備しておくべき管理策を満たしていない（レベルで要求されている対応策を実施していない）
③ 装備しておくべき管理策より高すぎる（ある意味でオーバースペック）

(8) 実施すべき施策の決定

ギャップ分析での結果である①及び③の項目については、その事項については新たに対策を実施する必要はない。②については、新規に実施する必要がある。しかしながら、もし、そのシステムの管理レベルを下げることができれば、この事項を実施する必要が無くなる。管理レベルを下げるには、データベースを構成している個人情報で、高い管理レベルを有する属性を無くせばよい。つまり、本当にその属性をデータベースとして保持すべきかどうかを検討し実施すべき施策を実施した。

(9) 実施、内部監査、是正処置

実施が決定した事項については、予算手当ての上、実行計画を作成し、実施するとともに、その後、進捗管理や内部監査を実施してフォローする。

3. 組織的安全管理措置と人的安全管理措置

ガイドラインが、組織的安全管理措置として講じなければならないとした項目は5項目であり、具体的に望ましい対策として列挙した事項は総数で23ある。また、人的安全管理措置については、2項目、総数5である。

組織的安全管理措置の中の5項目のうち、「個人データの安全管理措置を講じるための組織体制の整備」について望ましい事項としては11事項が挙げられている。例えば

・従業者の役割・責任の明確化
・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化

である。当社はQMSの枠組みの中で既にほとんどを実施していたことから、特段の対策を必要としなかった。

ただ、雇用契約時及び委託契約時におけるガイドラインの要求を考慮し、契約書の見直しを実施するとともに、教育に関しても、改めて全社員及び協力会社員に対しての教育を実施した。

4．コンプライアンス・プログラム

次にコンプライアンス・プログラムであるが、前述したように、個人情報保護法が、個人情報取扱事業者の義務として、第4章で定めた条項の中で、第20条安全管理措置の「物理的安全管理措置」と「技術的安全管理措置」を除いた部分と、第20条以外の要求事項は、JIS Q 15001の要求事項に相当している。当社は既にQMS及びISMSの取得において、「要求事項の文書化」について実績を有していたことから、JIS Q 15001の要求事項についても、QMSやISMSの枠組みの中で行った。QMSの「品質マニュアル」に相当しているコンプライアンス・プログラムはかなり整備されていると判断した。最終的には「個人情報保護規程」としてまとめた。また、個人情報保護法特有の要求事項以外は、ISMSのマネジメントシステムを原則採用することで対応した。ここでは紙面の都合上詳述しないが、情報処理開発協会が平成17(2005)年4月に公表した「法規適合性に関するISMSユーザーズガイド」[8]には、ISMSと個人情報保護法との関係が詳しく説明されている。

おわりに

本稿では、個人情報保護法を概観した上で、経済産業省のガイドラインを基にした安全管理措置への対応を中心に報告した。

1．国際的な動き

米国や欧州など海外の状況については割愛したが、EUではかなり厳しい要求をしており、適切な安全管理措置を怠ると、国際的な情報流通の世界から拒絶されることにもなる。これは電子商取引におけるセキュリティと同様に考えるべきである。

2．業界ガイドライン

経済産業省ガイドラインは産業界全般での基準を目指していることから、詳細な手続きなどについては示していない。電子商取引推進協議会（ECOM）が平成17(2005)年1月に定めた「民間部門における電子商取引に係る個人情報保護に関するガイドライン」[9]のように、業界に特化したガイドラインが出てきつつある。

3．全体把握と継続的見直しの必要性

個人情報は、その発生からデータベースへの登録がされた後、オンラインで参照されたり、印刷されたりと様々な利用形態が存在する。従って、法が求める安全管理措置を検討するには、単にデータベースを保管するサーバだけを対象にリスク評価を行うだけでは安全とはいえない。個人情報のリスク分析を実施する場合は、データあるいは情報のライフサイクルを明確にすることが重要である。いくらデータベースサーバ周りを強化しても、印刷物での漏洩や、ネットワーク上での漏洩を見落としては意味がない。ネットワークなどをはじめとするハードウェアはもちろん、全てのIT資産に関してITIL（Information Technology Infrastructure Library：ITサービス管理・運用規則に関するベストプラクティス）をベースにした構成管理や変更管理などのシステマチックな運用管理が必要である。個人情報はIT資産の一部分でしかない。セキュリティの3要素である、機密性、完全性、可用性を対象にしたISMSの手法が重要である。

また、IT資産の価値は当然時代とともに変化するし、ネットワークやサーバの構成変更などが、IT資産に対する新たなリスクをもたらしてくる。対応策についても、新しい技術が必ず出現してくる。資産の特定、脅威の洗い出し、脆弱性の特定、リスクの計算、対応策選択という流れは、個人情報でも全く同様であり、常にPDCAをまわしていくことが重要である。

引用文献

1) 経済産業省：平成16年10月，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.
2) 個人情報の保護に関する基本方針 平成16年4月2日閣議決定.
3) JIS Q 15001：1999 個人情報保護に関するコンプライアンス・プログラムの要求事項.
4) JIS X 5070：2000 セキュリティ技術 ― 情報技術セキュリティの評価基準.
5) JIS X 5080：2002 情報技術 ― 情報セキュリティマネジメントの実践のための規範.
6) 行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）.
7) 独立行政法人等の保有する個人情報の保護に関す

る法律（平成15年法律第59号）.
8) 財団法人日本情報処理開発協会，平成17年4月，法規適合性に関するISMSユーザーズガイド.
9) 電子商取引推進協議会（ECOM），平成17年1月「民間部門における電子商取引に係る個人情報保護に関するガイドライン」.

PROFILE

西川　浩
Hiroshi Nishikawa
住友化学システムサービス株式会社
顧問

里村　敏子
Toshiko Satomura
住友化学システムサービス株式会社
品質保証部

後藤　俊則
Toshinori Goto
住友化学システムサービス株式会社
品質保証部長