企業における個人情報保護対策の取り組み

Approach to Personal Information Protection Measures in Enterprises

寺田 由美子

要 約 個人情報保護法が2005年4月に完全施行しているため，企業は既に個人情報保護の義務がある．本稿では，個人情報保護法策定までの背景と，企業の個人情報保護対策に必要な取り組みとして，個人情報保護に関するガイドライン情報及び当社が奨める企業の個人情報保護対策の進め方を記述する．また企業における個人情報保護対策を推進していく上での課題と解決策や，短期間に企業の個人情報保護対策状況を明確にして，不足している安全管理対策を指摘するという，当社が開発した個人情報保護対策ソリューションの概要を記述する．

Abstract Since the Personal Information Protection Law （Japan） has been completely enforced starting April, 2005, the enterprises have the obligation of protecting the personal information.

This paper discusses first the background leading up to the legislation of this Law, then, the guideline information on the personal information protection and how to develop the protection measures for the personal information in the enterprises that our company recommends as a necessary approach to the protection measures.

Moreover, it describes the outline of “ Personal Information Protection Measures Solutions ” developed by Nihon Unisys, which clarifies the problems and their solutions in promoting the protection measures for the personal information in the enterprises, and the status of the company ’s protection measures in a short period of time, and points out the insufficient portion of protection measures.

1. はじめに

2005年4月から全面施行した個人情報保護法[1]は，6章，59条と附則から構成されており，1章から3章が公布された2003年5月に施行された．個人情報保護法では，目的に「この法律は，高度情報通信社会の進展に伴い個人情報*1の利用が著しく拡大していることにかんがみ，個人情報の適正な取り扱いに関し，基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め，国及び地方公共団体の責務等を明らかにするとともに，個人情報を取り扱う事業者の遵守すべき義務等を定めることにより，個人情報の有用性に配慮しつつ，個人の権利利益を保護することを目的とする」

と定義している．この法律では，IT化の進展に伴い個人情報の利用の扱いに対する社会的な不安感（個人情報漏洩事故など）の広がりが背景となって，個人情報取扱事業者*2（民間企業）に対して，情報セキュリティ対策を中心とした安全管理措置[2]が義務付けられている．

本稿では，個人情報保護法策定までの背景から，企業の個人情報保護対策として必要な取り組みを記述する．また，企業が個人情報保護対策を推進していく中での様々な課題に対する解決策の一例や，当社が開発した短期間に企業の個人情報保護対策状況を明確にして不足している対策を指摘する個人情報保護対策ソリューション[3]の概要を記述する．

2.　法制化の背景と個人情報保護法の構成

日本国内で個人情報保護法が制定された背景に，国際的な動きが関係している．

2.1　国際的な動き

個人情報保護に関する法制化の動きは，1980 年に OECD（経済協力開発機構）*3 から個人情報保護に関するガイドライン（OECD プライバシーガイドライン）[4][5]が発行されたことに始まる．OECD プライバシーガイドラインでは，個人情報保護に関して次の八つの原則（OECD 8 原則*4）が定められ，各国の取り組みを進展させた．

① 収集制限の原則
② データ内容の原則
③ 目的明確化の原則
④ 利用制限の原則
⑤ 安全保護の原則
⑥ 公開の原則
⑦ 個人参加の原則
⑧ 責任の原則

この原則が各国の国内法を整備する上での基本となっており，OECD 加盟国である日本の個人情報保護法も同様である．また，EU（ヨーロッパ連合）*5 は 1995 年に EU 指令（個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令）[6][7]を出し，EU 加盟国は加盟国外への個人データの移動は当該国が適切なレベルの保護を提供している場合に限られることと定めた．そのため，日本が EU 圏内で活動を行うために個人情報保護に関する法制化を行うことが必要となった．

2.2　日本国内の動き

日本国内における個人情報保護法成立の背景としては，1997 年に通商産業省（現経済産業省）が公表した民間部門における電子計算機に係わる個人情報の保護に関するガイドライン[8]があげられる．このガイドラインは，1999 年に JISQ 15001*6（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）として日本工業規格化された．

個人情報保護法策定の要因としては，昨今発生している個人情報漏洩事故，漏洩した個人情報を利用した詐欺事件が社会問題となっていること，2002 年に公的機関の中で稼働した住民基本台帳ネットワークシステム（住基ネット）*7 が考えられる．住基ネットの稼働に伴い各地方公共団体は，他の自治体管理の住民データにアクセスできるようになり，住民や自治体にとって利便性が向上した．反面その利便性によって，自治体では自組織の住民データだけでなく他の自治体管理であった個人データを含めて安全に管理することが必須となった．このような背景から個人情報の取扱が重要視され，民間企業を含めた個人情報の保護を義務付ける法律の制定が必要となった．法制化の背景として国際的な動きと日本の動きを図 1 示す．また，OECD 8 原則と個人情報保護法の関係を図 2 に示す．

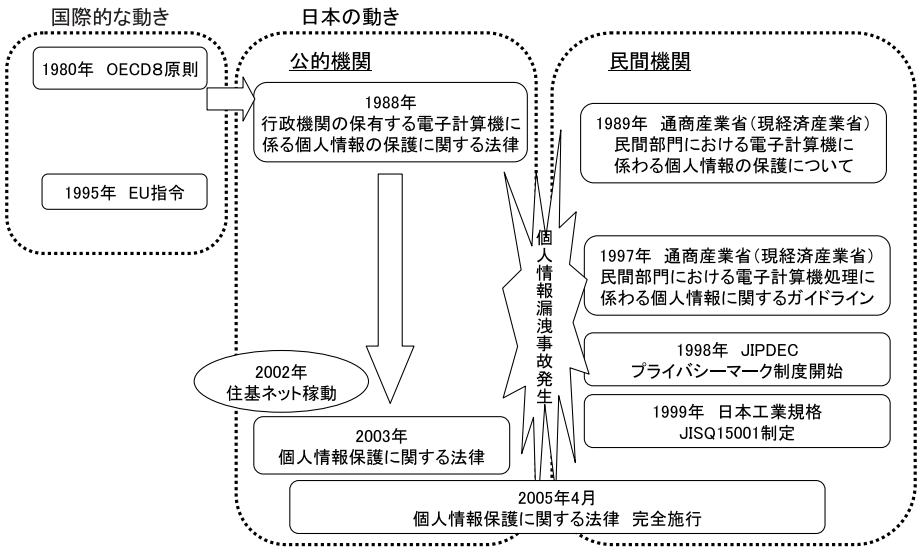


図 1　法制化の背景（国際的な動きと日本の動き）

OECD　8原則	内容
①収集制限の原則	個人データは、適法・公正な手段により、かつ情報主体に通知または同意を得て収集されるべきである。
②データ内容の原則	収集するデータは、利用目的に沿ったもので、かつ、正確・完全・最新であるべきである。
③目的明確化の原則	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である。
④利用制限の原則	データ主体の同意がある場合や法律の規定による場合を除いて、収集したデータを目的以外に利用してはならない。
⑤安全保護の原則	合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護すべきである。
⑥公開の原則	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である。
⑦個人参加の原則	データ主体に対して、自己に関するデータの所在及び内容を確認させ、または異議申立を保証するべきである。
⑧責任の原則	データの管理者は諸原則実施の責任を有する。

個人情報保護法（抜粋）
（利用目的の特定）　第十五条 利用の目的をできる限り特定しなければならない。 （利用目的による制限）　第十六条　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。 （第三者提供の制限）　第二十三条　あらかじめ本人の同意を得ないで第三者に提供してはならない。
（適正な取得）　第十七条　偽りその他不正の手段により取得してはならない。
（データ内容の正確性の確保）　第十九条　正確かつ最新の内容に保つよう努めなければならない。
（安全管理措置）　第二十条　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。 （従業者の監督）　第二十一条　従業者に対する必要かつ適切な監督を行わなければならない。 （委託先の監督）　第二十二条　委託を受けた者に対する必要かつ適切な監督を行わなければならない。
（取得に際しての利用目的の通知等）　第十八条　取得した場合は利用目的を通知又は公表しなければならない。 （保有個人データに関する事項の公表等）　第二十四条　保有個人データに関し本人の知り得る状態に置かなければならない。 （開示）　第二十五条　本人から保有個人データの開示を求められたときは遅滞なく開示しなければならない。 （訂正等）　第二十六条　本人から保有個人データの 訂正を求められた場合には内容の訂正等を行わなければならない。 （利用停止等）　第二十七条　本人から保有個人データの利用停止を求められた場合利用停止等を行わなければならない。
（個人情報取扱事業者による苦情の処理）　第三十一条　苦情の適切かつ迅速な処理に努めなければならない。

図 2　OECD 8 原則と個人情報保護法

2.3　個人情報保護法の構成

個人情報保護法は関連 5 法として構成している.

① 個人情報保護法
② 行政機関個人情報保護法[9]
③ 独立行政法人等個人情報保護法[10]
④ 情報公開・個人情報保護審査会設置法[11]
⑤ 整備法[12]

そのうち民間企業に直接関係するのは個人情報保護法である．その他4法は行政機関など公的分野における個人情報保護の法制となっている．

個人情報保護法では，国及び地方公共団体の責務と個人情報取扱事業者の義務等に分かれている．個人情報保護についての共通の一般規程を定めている第1章～第3章と，民間企業などに対する個人情報保護の規制を定めている第4章～第6章から構成されている．民間企業に関係する部分を表1に示す．

表 1　個人情報保護法の構成と個人情報取扱事業者の義務

個人情報保護法		個人情報取扱事業者の義務
第1章　総則	1　目的（1条） 2　定義（2条） 3　基本理念（3条）	○
第2章　国及び地方公共団体の責務等	1　国及び地方公共団体の責務（4条、5条） 2　法制上の措置等（6条）	―
第3章　個人情報の保護に関する施策等	第1節　個人情報の保護に関する基本方針（7条） 第2節　国の施策（8条～10条） 第3節　地方公共団体の施策（11条～13条） 第4節　国及び地方公共団体の協力（14条）	―
第4章　個人情報取扱事業者の義務等	第1節　個人情報取扱事業者の義務 (1)　利用目的の特定、利用目的による制限（15条, 16条） (2)　適正な取得、取得に際しての利用目的の通知等（17条, 18条） (3)　データ内容の正確性の確保（19条） (4)　安全管理措置、従業者・委託先の監督（20条～22条） (5)　第三者提供の制限（23条） (6)　公表等、開示、訂正等、利用停止等（24条～27条） (7)　苦情の処理（31条） (8)　主務大臣の関与（32条～35条） (9)　主務大臣（36条） 第2節　民間団体による個人情報の保護の推進 (1)　団体の認定（37条）、対象事業者（41条） (2)　個人情報保護指針（43条） (3)　主務大臣の関与（46条～48条） (4)　主務大臣（49条）	○
第5章　雑則	50条～55条	○
第6章　罰則	56条～59条	○

2.4　個人情報保護に関するガイドライン

事業分野ごとの措置として，各省庁では所管している事業分野向けに個人情報保護に関するガイドライン案を公表しパブリックコメントを募集した．その後各省庁は，2004年7月から2005年3月にかけて個人情報取扱事業者の義務等に対してガイドラインを策定している．主な事業分野における個人情報保護に関するガイドライン[13]を表2に示す．事業分野向けのガイドラインでは，個人情報保護法に対して事業分野において必須事項，努力事項としてまとめているが，具体的にどこまで対応をすればいいのか企業側で判断に迷う部分がある．また，各種協会団体も加盟団体向けにガイドライン[14]を策定している．主な協会団体におけるガイドラインを表3に示す．企業は，ガイドラインを参考にして自らの企業で個人情報保護対策を推進していくことが必要である．

3.　企業に求められる個人情報保護対策

企業に求められている個人情報保護対策とは，個人情報保護法及び自社の事業分野所管省庁の個人情報保護に関するガイドラインや所属協会団体のガイドラインに則って，以下のような対策を実施することである．

- 収集する個人情報の利用目的を特定し，特定した利用目的の範囲内で利用する

表 2　主な事業分野の所管省庁における個人情報保護に関するガイドライン

事業分野	所管省庁	ガイドライン名称	策定時期
事業全般	経済産業省	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[15]	2004年12月
金融・信用	金融庁	(1) 金融分野における個人情報保護に関するガイドライン[16]	2004年12月
		(2) 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[17]	2005年1月
雇用管理	厚生労働省	雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針[18]	2004年7月
国土交通	国土交通省	国土交通省所管分野における個人情報保護に関するガイドライン[19]	2004年12月

表 3　主な協会団体における個人情報保護に関するガイドライン

事業分野	協会団体名	ガイドライン名称
経済産業省所轄	社団法人　情報サービス産業協会	情報サービス産業　個人情報保護ガイドライン[20]
	電子商取引推進協議会(ECOM)	民間部門における電子商取引に係る個人情報の保護に関するガイドライン[21]
	日本情報処理開発協会(JIPDEC)	プライバシーマーク制度における監査ガイドライン[22]
	日本通信販売協会(JADMA)	通信販売における個人情報保護ガイドライン[23]
金融庁所轄	全国銀行協会(JBA)	個人情報の保護と利用に関する自主ルール[24]
		個人データの安全管理措置等に関する指針[25]
	全国信用金庫協会	個人情報の保護と利用に関する自主ルール[26]
		個人データの安全管理措置等に関する指針[27]
	日本証券業協会	個人情報の保護に関する指針[28]
		協会員における個人情報の適正な取扱いの確保について[29]
		インターネット取引において留意すべき事項について（ガイドライン）[30]

- 収集する個人情報の利用目的を通知または公表する
- 個人データを安全に管理する
- 第三者への提供時の対応をする
- 保有個人データに関して公表，開示・訂正・利用停止手続を整備する
- 苦情処理手続を整備する
- 個人情報保護への取り組みを表明するための方針を策定する

特に個人データの管理は，安全管理措置として，組織的，人的，物理的，技術的な観点から取り組む必要がある．組織的安全管理措置では，個人情報保護推進のための体制や規程類を整備し，個人データに関わる業務の委託先に対する基準等を作成する．人的安全管理措置では，従業者に対して個人情報保護に関する教育を実施する．物理的安全管理措置や技術的安全管理措置では，個人情報に関わる業務を安全な環境で実施するための対策を行う．

個人情報保護法が完全施行された現状では，対策を実施していない状態で漏洩事故等が発生した場合は企業にとって重大な問題となり得る．対策検討及び実施に時間が足りずに対策の実施を終えた企業は，現状の対策を見直し，改善することが必要である．個人情報保護ガイドライン要求事項に対して，「どこまで対策を行えば問題ないのか」という疑問があるが，セキュリティ対策はここまで実施すれば終わりということは決してありえない．それは，環境の変化，新たな脅威の発生，現状のセキュリティ対策を維持できているか等が関係しているためである．

企業が現状できることは，事業分野における情報や昨今の情報漏えい事故等の課題から企業の中での対策方針の決定，計画を立てて対策を実施，遵守状況の定期的な確認，問題があれば

改善していくことである．

3.1　企業における個人情報保護対策を推進する上での課題

個人情報保護に関して法律が制定されるまでの間は，その対応が企業に任されていた部分が多く，情報セキュリティ対策に取り組んできた企業であっても個人情報保護法対応が不十分な場合がある．個人情報を保護するための対策は，企業の中の組織構造，業務体系，企業に応じた個人情報保護対策基準が関係するために推進していくことが難しい傾向にある．以下に，企業が個人情報保護対策を推進する上での課題を整理した．

- 個人情報に関わる業務を行う部門が多岐に渡るため，今までに統一した対応が行われていない傾向にある．そのためガイドライン要求事項への対応を実施するときに，関連する部門との調整や検討に時間を要する．
- 個人情報保護対策を進めるための決まったプロセスが存在しない．プライバシーマーク制度[*8]や BS 7799/ISMS 適合性評価制度[*9]のような第三者基準を目指す企業であればそれらのプロセスを利用して個人情報保護対策を進めることが可能であるが，個人情報保護対策のみを進める（認証取得を目指さない）企業のための明確なプロセスがない．
- 個人データを安全に管理するための物理的・技術的対策の実装に明確な基準がない．そのために必要な予算確保が難しい．
- 個人情報保護に関する管理の専門家，技術の専門家を有していても，管理，技術両面を合わせた専門家が少ない傾向にある．

以上のような課題を踏まえて，当社が奨める個人情報保護対策の進め方を次の節に記述する．

3.2　当社が奨める個人情報保護対策の進め方

当社が奨める企業の個人情報保護対策の進め方の概要を図 3 に示す．1）個人情報保護対策を推進するための体制整備と概要計画の作成，2）個人情報保護方針の策定と公表，3）現状把握と対策検討，4）課題に対する個人情報保護対策の実施，5）遵守状況の確認，見直し及び改善を実施していくという流れである．実際の進め方は，企業に応じた段階を経て行くことになるが，期間は半年程度を要する場合が多い．

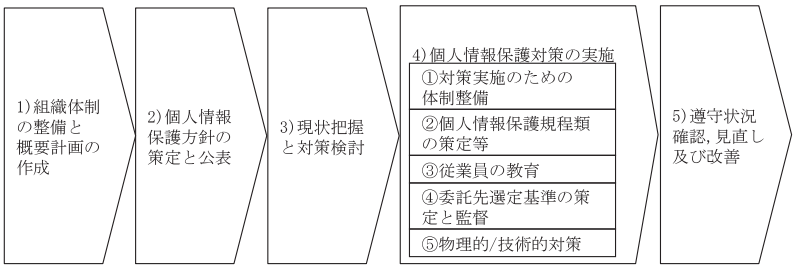


図 3　当社推奨個人情報保護対策の進め方

以下に当社が奨める個人情報保護対策の進め方を各作業段階ごとに説明する．

1）　組織体制の整備と概要計画の作成

個人情報保護対策は企業内の部門を跨って実施することが必要なために，個人情報保護対策を推進する組織体制（個人情報推進プロジェクト等）の整備を行う．個人情報推進プ

ロジェクトは，経営企画部門，営業部門，人事部門，総務部門，広報部門，情報システム部門，その他営業店など，個人情報取扱部門から一名以上を選任し構成する．各部門の代表は，それぞれ役割と責任を担う．プロジェクトの責任者は，企業の個人情報保護に関して責任を持つ担当役員 CPO （Chief Privacy Officer）とする．さらに，個人情報保護に関する専門家をプロジェクトメンバに加える．

概要計画は，いつまでにどのような個人情報保護推進を完了させるかという目標と関連部門に対して協力を要請するために必要である．

2） 個人情報保護方針の策定と公表

個人情報保護対策を推進することの必要性や個人情報保護を全社で推進するための個人情報保護方針を策定し，従業員に周知徹底する．また，社外に対して個人情報保護への取り組みを表明するために個人情報保護方針を公開する．公開に併せて個人情報保護に関する社外からの問い合わせ窓口を設置する．

3） 現状把握と対策の検討

個人情報保護対策として実施しなければならない課題を整理するために，企業内に存在する個人情報を洗い出し個人データ管理台帳にまとめる．また，個人情報を取り扱う業務を調査して業務の流れをまとめる．

個人情報保護対策として不足している事項を把握するために，現状の個人情報取扱業務がガイドラインの要求事項（安全管理措置など）を満たしているかどうか対策状況を調査する．対策が不足している事項には組織的，人的，物理的，技術的の側面から必要な対策を検討し，実施するための計画を作成する．

4） 個人情報保護対策の実施

上記 3）で抽出される個人情報保護対策としては以下の作業分類がある．

① 対策実施のための体制整備

個人情報保護対策を実際に運用していくための責任や役割を明確にするために，個人情報取扱部門における対策実施体制を整備する．実施体制として個人情報取扱管理者，担当者を設置して各々に責任と役割を与える．

② 個人情報保護規程類の策定

個人情報取扱に関してガイドライン要求事項を満たすための規程類を策定する．個人情報取扱に関する規程は，個人情報の入手，登録，加工，保管，削除など社内での取り扱いに関する規程，手順等を定めたものである．

また，策定した各種規程類が遵守されていることを監査するための規程や，各種規程類に違反したときの罰則について定める．その他に事故対応体制，事故報告手順，原因究明手順などを文書化する．

個人情報取扱に関する規程類が既存の文書と関連があるか，新たに策定が必要な文書か，既存の規定文書に改訂が必要かどうか調査する．既存の関連文書がある場合には，内容がガイドライン要求事項を満たしているか確認する．なお，新たに規程類を策定する際には既存の情報セキュリティ規程に準じたセキュリティ要件を確保し，企業内の既存文書体系に応じて策定する．

③ 従業員への教育

企業が決定した個人情報保護対策を従業員に周知徹底するために，従業員に対して教育

を実施する．教育を実施するために従業員への教育内容，対象者，教育期間，実施方法，実施記録，評価等についての計画を策定する．教育内容には，個人情報保護の必要性，個人情報保護のための一般的な概要教育，社内で策定した個人情報保護規程類の教育，個人情報に関わる問合せや苦情対応を想定した訓練を含む．

④　委託業者選定基準の策定と監督

個人データに関わる業務を外部委託する場合，企業の中で統一した対応を取る必要があるため，ガイドライン要求事項に則って委託先選定基準や委託先との契約に必要な内容を明文化する．また，委託先を監督する内容を定め，委託先を監督する．

⑤　物理的/技術的対策

現状把握よりガイドライン要求事項から不足している物理的，技術的安全管理措置を実施する．実施した対策を定期的に監査する．物理的対策例としては，入退室管理，個人データを保存した媒体の保護や情報システムの物理的保護がある．技術的対策は，4.2 節技術的な個人情報保護対策のポイントに記述する．

5)　遵守状況確認，見直し及び改善

4）で新たに実施した対策や企業が今までに取り組んできた対策が遵守されていることを確認するために，策定した監査規程に則り，個人情報保護の遵守状況を監査する．

策定した規程類が業務上の運用に問題がないか，実施体制に問題がないか，物理的，技術的対策に不足がないかなど遵守状況に応じた改善が必要なことを明確にする．要改善事項があれば対策を再検討し，改善を重ねていく．また，内部監査以外に，外部の監査を導入することの検討やセキュリティ認証制度（プライバシーマーク制度，BS 7799/ISMS 適合性評価制度など）の取得を視野に入れながら，今後の企業の取組方針を検討する．

本節では，一般企業において必要な個人情報保護対策を記述した．企業にとって個人情報保護対策に取り組むことは，個人情報保護法が施行された現状では必須となっているが，新たに実施した対策を運用し企業の中に浸透させていくことは，内部での役割分担や既存業務運用への追加作業が発生するため，難しいと考えられる．次の節では，個人情報保護対策推進の難しさを解決するための方法として一例を述べる．

3.3　企業における個人情報保護対策を推進するための解決策

企業における個人情報保護対策を推進していく中での様々な課題を解決するために，情報セキュリティ対策と個人情報保護対策を関連付けて実施することが効果的である．個人情報は，情報セキュリティの観点から見た場合には，機密性，完全性，可用性が非常に高い情報資産の一つである．

個人情報保護法第 20 条安全管理措置では，「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．」

とある．情報セキュリティ対策は，機密性，完全性，可用性の観点から情報資産を守るのに対して，個人情報保護法の安全管理措置は，個人データを組織的，人的，物理的，技術的観点から安全に管理することとなっている．どちらも情報資産を守るために対策を行うということには変わりはない．どのように守るかという観点が異なるだけで実際の対策を行うときには共通する内容が多い．個人情報保護対策と情報セキュリティ対策は，情報資産を守るための運用を

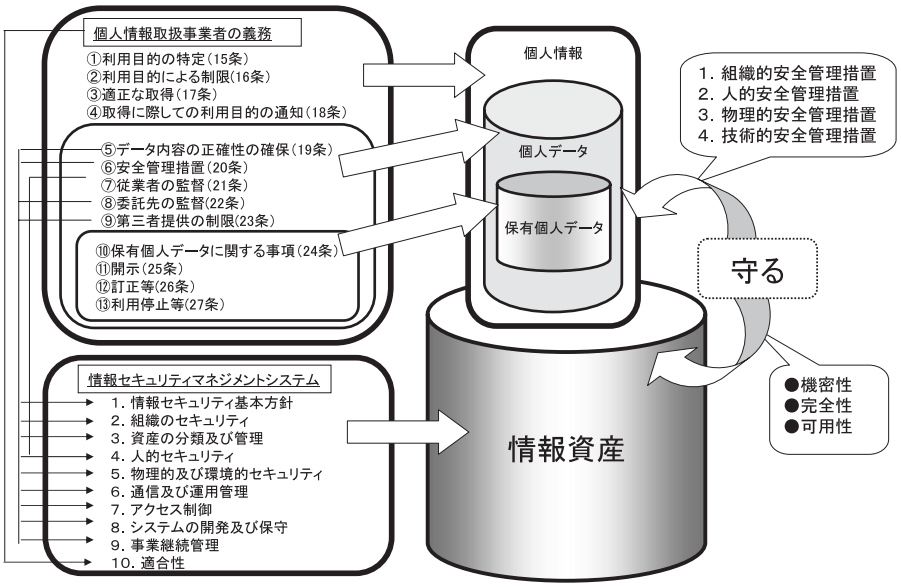


図 4　個人情報保護対策と情報セキュリティ対策の関係

行いながら，その運用を定期的に見直し，改善していくことである．個人情報保護と情報セキュリティの関係のイメージを図 4 に示す．

情報資産を守るための枠組みとして，情報セキュリティマネジメントシステム（ISMS）*10 がある．3.1 節に個人情報保護対策の課題を記述したが，情報セキュリティマネジメントシステムの枠組みに則って対策を実施し，さらに個人情報保護に特化した対応*11 を追加することによって解決が可能といえる．今までに情報セキュリティ対策を実施してきた企業は，個人情報保護対策に特化した部分への対応を追加するのみで対応可能と考えられる．

情報セキュリティ対策が進んでいる業界の一例として銀行を中心とした金融業界が挙げられる．金融業界では，金融庁から顧客情報管理についての取り組みが義務付けられており，金融庁の検査マニュアル[31]による検査が実施されている．また金融情報システムセンタ（FISC）*12 が策定した安全対策基準*13 に則った対応を実施しているため，一般企業と比較すると個人情報保護に関しては，現状のセキュリティ対策で不足している部分を補う程度という位置付けになる．図 5 に金融業界における個人情報保護対策の位置付けのイメージを示す．

4.　短期間で対策状況の現状把握が可能な個人情報保護対策ソリューション

4.1　個人情報保護対策ソリューションの概要

個人情報保護法が完全施行された現在となっては，企業は既に個人情報保護の義務がある．しかし，対策の検討や導入のための期間が足りなかった場合には不足している対応がないか再度確認する必要がある．その際に，外部の専門家の客観的な診断を利用することは有効な手段である．

当社が提供している個人情報保護対策ソリューションは，短期間に個人情報保護対策状況を分析し，対策ポイントや対策方法を明示することが特長である．フェーズ 1 短期セキュリティ診断とフェーズ 2 短期セキュリティ対策の二つのフェーズで構成している．

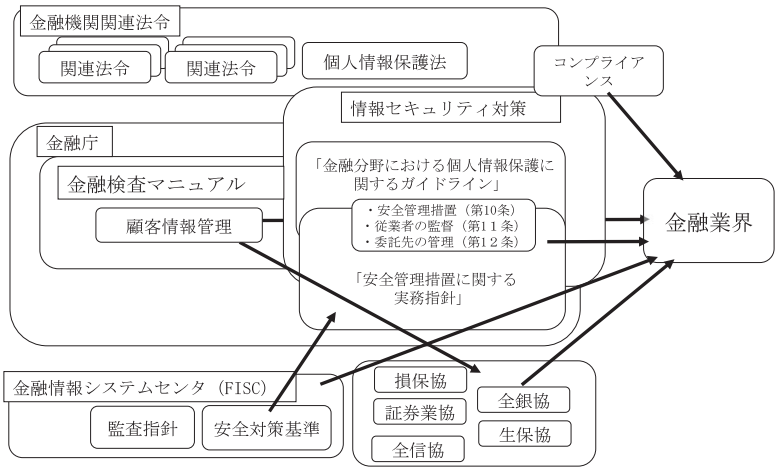


図 5　金融業界における個人情報保護対策の位置付け

フェーズ 1 短期セキュリティ診断では，事業分野のガイドラインを元に個人情報保護対策状況を短期間（2 週間から 1 か月程度）で診断し，短期診断報告書（以下，報告書と記述）としてまとめる．個人情報保護対策を進める中では個人データの洗い出しと台帳整備や個人データに関わる業務の流れをまとめリスク分析を実施する作業に時間を要する．短期診断では，対策のポイントとなる点や対策の優先度を短期間の診断で明示するため，対策方法を迷っている企業にとって内部の検討課題に参考となる情報を提供する．

また，フェーズ 2 短期セキュリティ対策では，フェーズ 1 のセキュリティ診断結果から必要な対策を実施する．この短期セキュリティ対策は，短期間に優先度の高い対策を実施することを目的としている．個人情報に関する規程類が現状策定されていない場合，規程の策定は優先度が高い対策の一つであるが，企業の既存の文書体系やセキュリティ文書との整合性を取る必要があるため，短期間での策定は困難である．このような場合は参加協会団体等の雛形文書を元に策定後，見直し時に企業に合った文書として改善していくという方法が考えられる．企業に応じた文書体系の整備は，当社では短期対策以外にコンサルティングサービスとして提供している．企業のニーズに応じて，短期対策やコンサルティングサービスなどを選択していただくことが可能である．

個人情報保護対策ソリューションの作業プロセスを図 6 に示す．また，個人情報保護対策ソリューションの作業プロセスが，3.2 節で説明した当社が奨める個人情報保護対策の進め方のどの部分に該当するかを図 7 に示す．

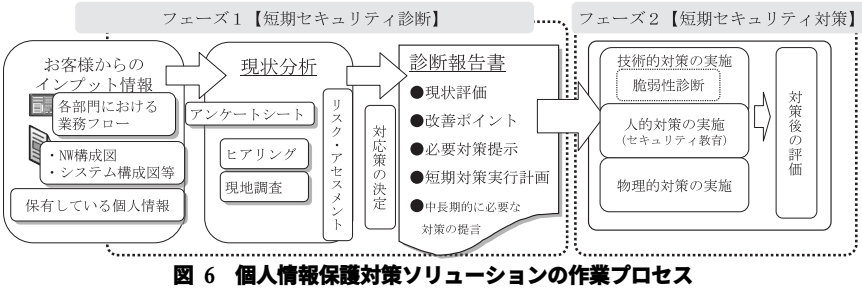


図 6　個人情報保護対策ソリューションの作業プロセス

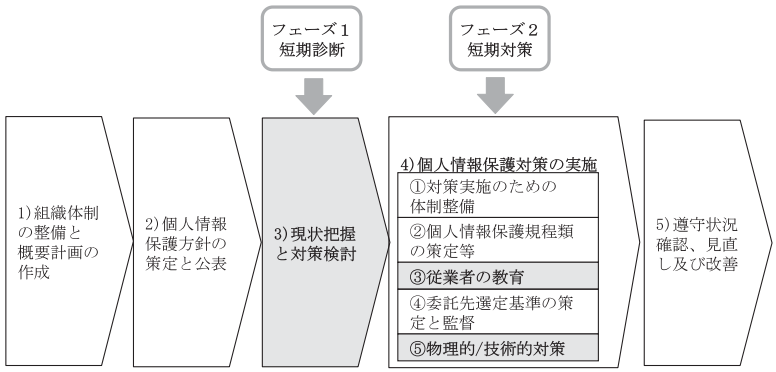
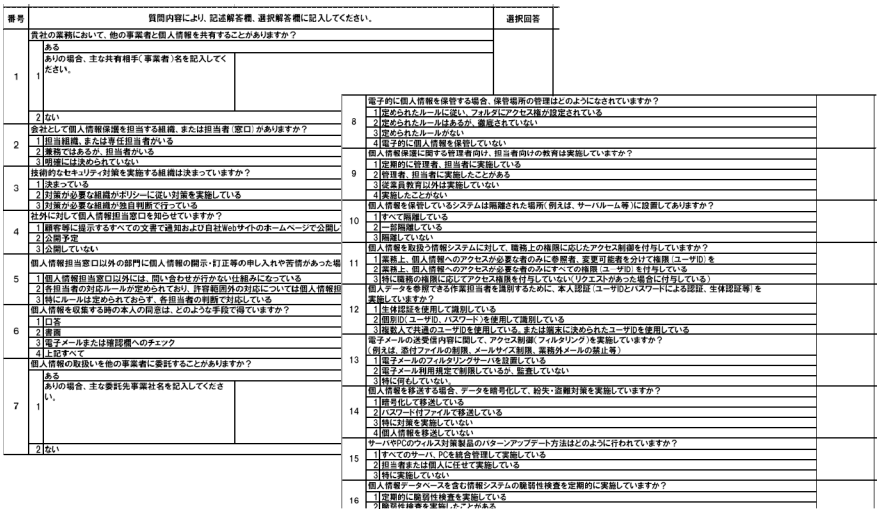


図 7　当社推奨個人情報保護対策の進め方と個人情報保護対策ソリューションの関係

フェーズ 1 短期セキュリティ診断では，事前に個人情報保護推進担当者の方に 150 問程度のアンケート（図 8 にイメージを示す）に回答していただく．アンケートは，個人情報保護のガイドライン要求事項及び情報セキュリティ対策についての状況を把握するための質問で構成され，回答は三つないし四つから選ぶ形式である．



番号	質問内容により、記述解答欄、選択解答欄に記入してください。	選択回答
1	貴社の業務において、他の事業者と個人情報を共有することがありますか？	
1-1	ある	
1-1	ありの場合、主な共有相手（事業者）名を記入してください。	
1-2	ない	
2	会社として個人情報保護を担当する組織、または担当者（窓口）がありますか？	
2-1	担当組織、または専任担当者がいる	
2-2	兼務ではあるが、担当者がいる	
2-3	明確には決められていない	
3	技術的なセキュリティ対策を実施する組織は決まっていますか？	
3-1	決まっている	
3-2	対策が必要な組織がポリシーに従い対策を実施している	
3-3	対策が必要な組織が独自判断で行っている	
4	社外に対して個人情報担当窓口を知らせていますか？	
4-1	顧客等に提示するすべての文書で通知および自社Webサイトのホームページで公開し	
4-2	公開予定	
4-3	公開していない	
5	個人情報担当窓口以外の部門に個人情報の開示・訂正等の申し入れや苦情があった場	
5-1	個人情報担当窓口以外には、問い合わせが行かない仕組みになっている	
5-2	各担当者の対応ルールが定められており、許容範囲外の対応については個人情報担	
5-3	特にルールは定められておらず、各担当者の判断で対応している	
6	個人情報を収集する時の本人の同意は、どのような手段で得ていますか？	
6-1	口全	
6-2	書面	
6-3	電子メールまたは確認欄へのチェック	
6-4	上記すべて	
7	個人情報の取扱いを他の事業者に委託することがありますか？	
7-1	ある	
7-1	ありの場合、主な委託先事業社名を記入してください。	
7-2	ない	
8	電子的に個人情報を保管する場合、保管場所の管理はどのようになされていますか？	
8-1	定められたルールに従い、フォルダにアクセス権が設定されている	
8-2	定められたルールはあるが、徹底されていない	
8-3	定められたルールがない	
8-4	電子的に個人情報を保管していない	
9	個人情報保護に関する管理者向け、担当者向けの教育は実施していますか？	
9-1	定期的に管理者、担当者に実施している	
9-2	管理者、担当者に実施したことがある	
9-3	従業員教育以外は実施していない	
9-4	実施したことがない	
10	個人情報を保管しているシステムは隔離された場所（例えば、サーバルーム等）に設置してありますか？	
10-1	すべて隔離している	
10-2	一部隔離している	
10-3	隔離していない	
11	個人情報を取扱う情報システムに対して、職務上の権限に応じたアクセス制御を付与していますか？	
11-1	業務上、個人情報へのアクセスが必要な者のみに参照者、変更可能者を分けて権限（ユーザID）を	
11-2	業務上、個人情報へのアクセスが必要な者のみにすべての権限（ユーザID）を付与している	
11-3	特に職務の権限に応じてアクセス権限を付与していない（リクエストがあった場合に付与している）	
12	個人データを参照できる作業担当者を識別するために、本人認証（ユーザIDとパスワードによる認証、生体認証等）を実施していますか？	
12-1	生体認証を使用して識別している	
12-2	個別ID、ユーザID、パスワード）を使用して識別している	
12-3	複数人で共通のユーザIDを使用している、または端末に決められたユーザIDを使用している	
13	電子メールの送受信内容に関して、アクセス制御、フィルタリング）を実施していますか？（例えば、添付ファイルの制限、メールサイズ制限、業務外メールの禁止等）	
13-1	電子メールのフィルタリングサーバを設置している	
13-2	電子メール利用規定で制限しているが、監査していない	
13-3	特に何もしていない	
14	個人情報を移送する場合、データを暗号化して、紛失・盗難対策を実施していますか？	
14-1	暗号化して移送している	
14-2	パスワード付ファイルで移送している	
14-3	特に対策を実施していない	
14-4	個人情報を移送していない	
15	サーバやPCのウィルス対策製品のパターンアップデート方法はどのように行われていますか？	
15-1	すべてのサーバ、PCを統合管理して実施している	
15-2	担当者または個人に任せて実施している	
15-3	特に実施していない	
16	個人情報データベースを含む情報システムの脆弱性検査を定期的に実施していますか？	
16-1	定期的に脆弱性検査を実施している	
16-2	引脆弱性検査を実施しておりかない	

図 8　短期診断アンケートのイメージ

アンケートの回答を元にヒアリングと現地調査を実施し，対策状況をさらに詳細に確認する．それらの情報からガイドラインに対してベースライン・アプローチで簡易的なリスク分析を実施し，50 ページ程度の報告書（図 9）としてまとめる．報告書では，ガイドライン要求事項への達成度を概要レーダチャートに表し，特に安全管理措置については詳細なレーダチャートを提示する．

報告書に記述するレーダチャートでは，ガイドライン要求事項に対して対策状況を 5 段階に評価する．個人情報保護対策は組織的な対応が必要なため，組織的に取り組んでいることが重要である．

概要レーダチャートは，個人情報保護ガイドラインを六つの観点に分け，それぞれの達成度を表す．安全管理措置詳細レーダチャートには，ガイドライン要求事項の安全管理措置の組織

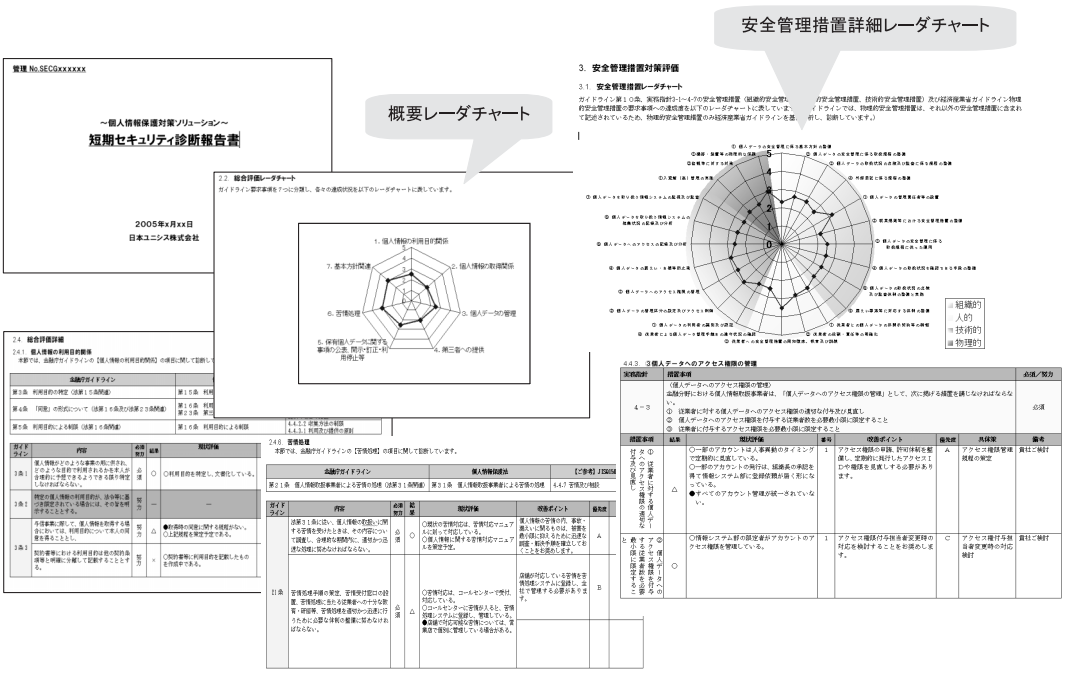


図 9　報告書のイメージ

的，人的，物理的，技術的な観点から詳細に達成度を表す．（図 9 報告書のイメージ内に例示）

情報セキュリティ対策をバランス良く行う必要があるのは周知のことであるが，個人情報保護対策についても同様である．対策が不足している部分を視覚的に表現することにより対策の優先度が明確になる．

4.2　技術的な個人情報保護対策のポイント

報告書では，ガイドライン要求事項全体に対して必須義務と努力義務の種別を記述している．ガイドライン要求事項の必須義務については，組織的に早急に対策を行う必要がある．本節では，技術的な個人情報保護対策のポイントとして経済産業省ガイドラインを例に説明する．経済産業省ガイドラインでは「技術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，次の①～⑧がある．

① 個人データへのアクセスにおける識別と認証
② 個人データへのアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データのアクセスの記録
⑤ 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
⑥ 個人データの移送・送信時の対策
⑦ 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
⑧ 個人データを取り扱う情報システムの監視

これら 8 項目に対して，実際の情報システムの中での対応として考えられることを以下に記述する．（以下に示す“経技①”は経済産業省ガイドライン技術的安全管理措置①を表している）

- 人事情報と連携可能な統合アカウントシステムの導入（経技①）
- 情報セキュリティ対策を導入しやすいネットワーク構成の整備及び対外接続及び内部重要サーバへの通信経路にファイアウォールと不正侵入防御装置の導入（経技②）
- 人事異動情報等に基づいた統合アカウントシステムの運用（経技③）
- アクセスログを保存，分析できる仕組みの導入及び正確なアクセスログを保存するための時刻同期システムの導入（経技④）
- サーバ，クライアントすべてを含めたセキュリティパッチ，ウイルス対策の導入（経技⑤）
- 重要ファイルの暗号化，持ち出し制御及びモバイル PC の紛失対策（経技⑥）
- 情報システムに対する定期的な脆弱性検査（経技⑦）
- サーバの稼働監視（経技⑧）

上記以外に，情報システムに関わる文書を整備していくことが重要である．文書の整備とは，情報セキュリティポリシに基づいた情報システムに関わる文書の体系化と，既存システムに不足している文書を洗い出し策定することである．情報システムに関わる文書の中で特に運用管理規程や情報システムの利用手順の整備が重要と考える．過去に発生した情報漏洩事故は組織の内部から発生する傾向がある．情報システムに関する規程類を策定し，策定した規程類を従業員へ教育・訓練することが，情報システムに対する誤操作等を未然に防止することに繋がる．

次の節では技術的な個人情報保護対策を実装する上でポイントとなる企業のネットワーク構成整備の必要性を記述する．

4.3　情報セキュリティ対策を導入しやすいネットワーク構成の整備

当社の過去の経験から企業の中のネットワークがどのように構成されているかによって，情報セキュリティ対策を行う上での費用対効果の高い対策を実装できるか，また導入が行いやすいかが判断できる．情報システムに対する技術的なセキュリティ対策を行う対象としては，ネットワーク，サーバ，アプリケーション，クライアントがある．これらの対象にセキュリティ対策を組み合わせて実装することで，より強固なセキュリティ対策を実現できる．

情報システムやサーバのネットワーク上の配置が利用目的や重要度に応じて構成されていると，サーバやアプリケーションへのセキュリティ対策に加えて，ネットワークにおける対策を効果的に実装することが可能になる．

また，ネットワークが業務の情報システム化に応じて随時拡張されてきたような場合には，開発期間や予算の面からネットワーク構成の見直しが後回しになる傾向がある．それにより新たに開発した情報システムに対してはセキュリティ対策を行うが，既存の情報システムに対してはネットワーク構成上の問題からセキュリティ対策を行えない場合がある．その結果，社内のネットワークに接続している情報システムが取り扱うデータの重要度が同等であってもセキュリティ対策のレベルに差が出る．

以下に，目的別ネットワークに対するセキュリティ対策例を示す．ネットワークに接続するサーバやネットワーク機器は，オペレーティングシステムの不要なサービスを停止する，ウイルス対策や最新セキュリティパッチを適用済み，不要なユーザ ID や脆弱なパスワードを設定していないものとする．また，機器は時刻を同期し，アクセスログを保存しているものとする．また，各ネットワークの接続境界にはファイアウォールを設置し，通信に必要なものだけを許

可するようにアクセス制御を実施する．

① インターネット接続ネットワーク

インターネット接続ネットワークは，インターネットからのアクセスを許可する公開用 Web サーバやインターネットを利用して社外と電子メールを交換するためのサーバを配置する．

インターネットとの接続は不特定多数からのアクセスがあるため，インターネットとの接続境界にファイアウォールを設置する．また不正アクセス検知防御対策，電子メールによるウイルス感染や内部からインターネット上の社外の Web サイト接続におけるウイルス感染を防御するためのゲートウェイ・ウイルス対策を実施する．日々脆弱性情報が更新されるため，定期的に脆弱性検査を実施して，発見されたサーバ等の脆弱性に対する対策を行う．

② 対外接続ネットワーク

業務上必要な取引先との接続を行う対外接続ネットワークでは，接続相手先や利用者を限定する．外部組織との接続であるため，外部との接続境界にファイアウォールを設置し，必要に応じて不正アクセス検知防御対策やゲートウェイ・ウイルス対策を実施する．

③ 内部向けサービス用ネットワーク

従業員向けの内部用 Web サーバやメールサーバ，従業員向けサービス提供サーバを配置する．内部向けサービス用ネットワークにおいては，利用者を従業員のみに限定し，サービスの利用の許可や制限を行うために統合認証システムを導入する．

④ 内部重要サーバ用ネットワーク

企業の業務システムに関わるサーバやデータベース・サーバを配置する内部重要サーバ用ネットワークでは，利用者は業務システム利用権限者や運用者のみに限定し，不正アクセス検知防御対策やデータベースに特化した不正アクセス検知を実施する．また，従業員の人事情報を扱う人事部門が管理するシステムは，業務システムとは別の内部重要サーバ用ネットワークに配置する．

⑤ 従業員用ネットワーク，支店/拠点ネットワーク

従業員用ネットワーク，支店/拠点ネットワークは，本社の執務エリアや支店/拠点執務エリアにおける従業員の OA 用パソコン（クライアント）を接続する．ネットワークは部門ごとに分け，部門によっては，部門共有ファイルサーバを配置する．

従業者用ネットワーク，支店/拠点ネットワークにおけるセキュリティ対策としては，不正持ち込み PC 防御やクライアントに保存した機密度の高い電子データの持出制御，媒体の利用制限や，外部と交換する電子ファイルの暗号化を実施する．また，社外に持ち出す PC についてはハードディスクの暗号化を実施する．

⑥ 運用管理ネットワーク

運用管理ネットワークは，業務システムやサービス提供サーバ（Web サーバやメールサーバなど），ネットワーク機器の稼働監視システム，各サーバに保存しているログを集中的に管理するための集中ログサーバやログ解析サーバ，不正アクセス検知防御対策やウイルス対策システムの管理サーバを配置する．運用管理ネットワークは企業の情報システム部門など運用管理部門のみの利用とする．

以上，目的別ネットワークのセキュリティ対策例として説明した内容を図 10 に示す．

目的別に構成していないネットワークの状態で，取扱うデータの重要度に応じてセキュリティ対策を実施すると，複数のネットワークに同一のセキュリティ対策が必要になる．目的別にネットワークを構成することにより，ネットワークの重要度に応じたセキュリティ対策製品を選定し実装することが可能となり，費用対効果の高いセキュリティ対策に繋がる．

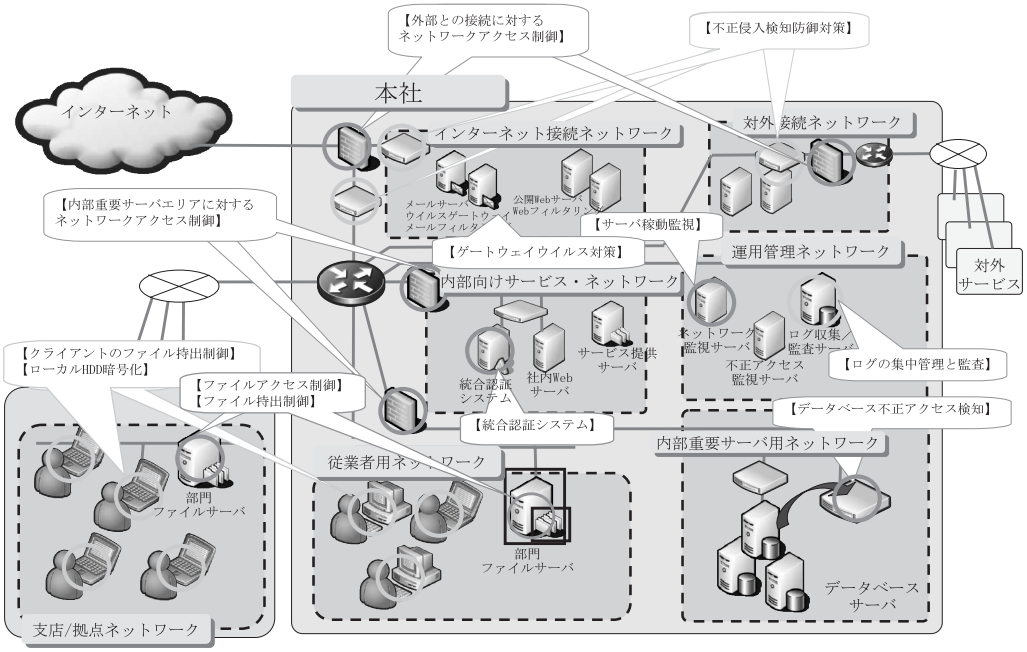


図 10　技術的な情報セキュリティ対策例

4.4　個人情報保護対策ソリューションにおける個人情報保護対策例

当社の個人情報保護対策ソリューションでは，技術的な対策については 4.3 節で説明した技術的対策のポイントと現状の企業の対策状況を勘案して対策案を提示する．現状の構成から一度に対策を実施することは困難であるため，段階を設けて実現可能な対策案とする．

表 4 に報告書に記述している対策案を例示する．（実際の報告書の対策案では，推奨製品名と概算価格を参考情報として記述している．）報告書では，安全管理措置の組織的対策，人的対策，物理的対策，技術的対策それぞれに対する対策案を優先度別に記述している．業務の特性や運用上の問題及び予算や具体的な対策方法を検討するに当たっての参考情報となる．

5.　お　わ　り　に

個人情報保護法が 2005 年 4 月に完全施行され，5 ヶ月が経過している．個人情報漏洩事故はいまだに毎日のように発生している．個人情報保護法では義務に違反した場合，義務違反となり主務大臣からの勧告・命令がある．その命令に違反した場合の罰則として，6 ヶ月以下の懲役または 30 万円以下の罰金がある．

個人情報漏洩事故では消費者である一般市民が被害者になるため，消費者側は漏洩事故を発生させた企業に対して不信感を抱くことになり，それが企業のイメージダウン，ブランド価値

表 4　報告書の対策案例

分類	説明	早急に対応が必要な対策	次期に推奨する対策
組織的対策	体制整備，規程策定，評価・見直し及び改善，事故等への対応整備　など	個人情報保護体制の整備 各管理段階における規程策定	個人情報保護コンサルティングサービス
人的対策	非開示契約の締結 教育・訓練の実施　など	非開示契約の締結 個人情報保護に関する集合研修	e-Learning
物理的対策	入退室管理 物理的保護（盗難対策）　など	訪問者と従業者の識別と訪問者の入退室記録，監視カメラ，媒体の施錠保管	IC カード入退室システム 媒体シュレッダー
技術的対策	① 個人データへのアクセスにおける識別と認証	統合アカウントシステム	IC カード認証
	② 個人データへのアクセス制御		内部ファイアウォール
	③ 個人データへのアクセス権限の管理		人事システムとの連携
	④ 個人データのアクセスの記録	時刻同期 サーバ別ログ保存	アクセスログ集中管理システム，ログ分析システム
	⑤ 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	サーバ，クライアントウイルス対策	アンチウイルス統合管理 ゲートウェイ・ウイルス対策
	⑥ 個人データの移送・送信時の対策	ファイル暗号化	媒体持出制御
	⑦ 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	脆弱性診断	テスト環境整備
	⑧ 個人データを取り扱う情報システムの監視	ネットワーク監視システム	不正アクセス検知システム

の低下や顧客離れになりかねない．万が一にも個人情報漏洩事故を発生させてしまった場合に，対応の遅れや不十分な漏洩防止策など事故後の対策が不適切ならば，消費者はさらに厳しい目で企業への信頼感や今後の取引について判断するであろう．

個人情報保護対策は情報セキュリティ対策と同様に，対策を実施した後にそれが継続的に遵守できているか，環境などの変化に応じて見直し改善しているか，これらの PDCA サイクルの運用が継続的に必要である．

個人情報保護対策や情報セキュリティ対策の導入当初は，その運用を実施していくことが企業やその従業員にとって厳しい対応と思われがちであるが，前向きに取り組む企業は，顧客からの信頼感が増し，それが業績向上に繋がる．業務や新たに開発する情報システムの中に，今やセキュリティ対策は必須の時代である．企業の中に個人情報保護や情報セキュリティをいかに浸透させることができるかが今後は企業価値判断の重要な要素の一つになると思われる．

当社の個人情報保護対策ソリューションは，2004 年 9 月に発表してから，金融，製造・流通，国土交通などの業種の企業にご利用頂いている．対策に取り組んでいるものの，「どこから行えばいいのか」と判断に困っている場合，「既に対策を実施しているが不足点はないか」と検討中の場合，担当者が経営層に対して予算の提示・確保をするために自社の対策状況の明確化に利用する場合があり，どの場合にも役立つ結果となったと考えている．今後も企業の情報セキュリティ対策の向上に役立つソリューションを提供していきたい．

本稿が個人情報保護対策の参考情報としてご活用いただければ幸いである．

＊1　個人情報：個人を識別できる氏名，生年月日などの情報のこと．
個人データ：個人情報保護法における，個人情報データベース等を構成する個人情報のこと．
保有個人データ：個人データの内開示や訂正などの権限を有するデータで，6 ヶ月以上保有されたデータのこと．

＊2　個人情報取扱事業者：過去 6 ヶ月以内に 5,000 件以上で構成される個人情報データベース等を事業の用に供する者．

＊3　OECD（経済協力開発機構）：欧米などの先進国を中心とする加盟国間の協力によって，経

済成長の促進，開発途上国への援助，世界貿易の拡大などを目指す国際機構．

＊4　OECD 8 原則：1980 年に OECD（経済協力開発機構）の理事会で採択された「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」の中に記述されている 8 つの原則．

＊5　EU（ヨーロッパ連合）：ヨーロッパの政治経済の統合を目指し，加盟国間の相互協力を強化することを目的として設立された超国家機構．

＊6　JISQ 15001：財団法人日本規格協会により 1999 年 3 月に発行された規格．規格の正式名称は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」

＊7　住民基本台帳ネットワークシステム：総務省，地方公共団体共同のシステムとして，居住関係を公証する住民基本台帳のネットワーク化を図り，全国共通の本人確認を可能とするシステムであり，電子政府・電子自治体の基盤．http：//www.soumu.go.jp/c-gyousei/daityo/

＊8　プライバシーマーク：JIPDEC（財団法人日本情報処理開発協会）が管理する個人情報取り扱いに関する認定制度．

＊9　BS 7799/ISMS 適合性評価制度は，組織の ISMS が適切に実施されていることを，第三者機関が審査・認証する制度．

＊10　情報セキュリティマネジメントシステム（ISMS）：ISMS（情報セキュリティマネジメントシステム）：Information Security Management System の略．組織が情報資産を適切に管理し守るための包括的な枠組みのこと．http：//www.isms.jipdec.jp/isms/index.html

＊11　個人情報保護に特化した対応：保有個人データに関する利用目的の通知や開示，苦情手続きなど．

＊12　金融情報システムセンタ（FISC）：FISC （The Center for Financial Industry Information Systems）は昭和 59 年に金融機関，保険会社，証券会社，コンピュータメーカー，情報処理会社等によって設立された財団．金融機関等における金融情報システムの活用や安全性確保等に関して指針の提示等を行っている機関．http：//www.fisc.or.jp/ippan.htm

＊13　安全対策基準：金融機関等コンピュータシステムの安全対策基準・解説書の略．http：//www.fisc.or.jp/ippan.htm

参考文献

［1］ 個人情報の保護に関する法律（平成十五年法律第五十七号），http：//www 5.cao.go.jp/seikatsu/kojin/houritsu/index.html

［2］ 個人情報保護法　第二十条（安全管理措置）

［3］ 当社が提供しているソリューション，http：//bdc.unisys.co.jp/eps/sec_sol/pdp_sol/index.htm

［4］ 1980 年に OECD（経済協力開発機構）の理事会で採択された「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」の中に記述されている 8 つの原則，http：//www 1.oecd.org/publications/e-book/9302011 E.pdf

［5］ 外務省　プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告（1980 年 9 月（仮訳），http：//www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html

［6］ EU,http：//europa.eu.int/comm/justice_home/fsj/privacy/

［7］ 電子商取引実証推進協議会 ECOM のプライバシー問題検討ワーキング・グループ，EU 指令「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（ECOM プライバシー問題検討 WG 訳），http：//www.isc.meiji.ac.jp/ ~ sumwel_h/doc/intnl/Direct-1995-EU.htm

［8］ 平成 9 年 3 月 4 日通商産業省告示第 98 号「民間部門における電子計算機に係わる個人情報の保護に関するガイドライン」，http：//www.gip.jipdec.or.jp/policy/infopoli/privacy.html［9］ 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）

［10］ 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）

［11］ 情報公開・個人情報保護審査会設置法（平成 15 年 5 月 30 日法律第 60 号）

［12］ 行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（平成 15 年法律第 61 号）

［13］ 国民生活局，個人情報の保護に関するガイドラインについて，http：//www 5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

［14］ 社団法人　情報サービス産業協会, http：//www.jisa.or.jp/pdguide/link 06 b-j.html

［15］ 経済産業省，「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」，平成 16 年 10 月，http：//www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf

［16］ 金融庁，「金融分野における個人情報の保護に関するガイドライン」，平成 16 年 12 月 6 日金融庁告示第 67 号，http：//www.fsa.go.jp/common/law/kj-hogo/01.pdf

[17] 金融庁,「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」, 平成 17 年 1 月 6 日金融庁告示第 1 号, http：//www.fsa.go.jp/common/law/kj-hogo/04.pdf
[18] 厚生労働省,「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」, 平成 16 年 7 月 1 日, http：//www 5.cao.go.jp/seikatsu/kojin/gaidorainkentou/koyou.pdf
[19] 国土交通省, 国土交通省告示第千五百号, 平成 16 年 12 月 2 日, http：//www 5.cao.go.jp/seikatsu/kojin/gaidorainkentou/kokudo.pdf
[20] 社団法人　情報サービス産業協会,「情報サービス産業　個人情報保護ガイドライン」(第三版), 改定 2000 年 (平成 12 年) 5 月 10 日, http：//www.jisa.or.jp/legal/privacy_protect_guideline.html
[21] 電子商取引推進協議会 (ECOM),「民間部門における電子商取引に係る個人情報の保護に関するガイドライン」(Ver.3.0), 平成 17 年 1 月 31 日, http：//www.ecom.or.jp/home/privacy_gl/GuideLineV 3.pdf
[22] 日本情報処理開発協会 (JIPDEC),「プライバシーマーク制度における監査ガイドライン」, http：//privacymark.jp/ref/pmaugl.html
[23] 日本通信販売協会 (JADMA),「通信販売における個人情報保護ガイドライン」, http：//www.jadma.org/index 2.html
[24] 全国銀行協会(JBA),「個人情報の保護と利用に関する自主ルール」, http：//www.zenginkyo.or.jp/news/16/pdf/news 161231.pdf
[25] 全国銀行協会(JBA),「個人データの安全管理措置等に関する指針」, http：//www.zenginkyo.or.jp/news/17/pdf/news 170232.pdf
[26] 全国信用金庫協会,「個人情報の保護と利用に関する自主ルール」, http：//www.shinkin.org/new/041224/3_21.pdf
[27] 全国信用金庫協会,「個人データの安全管理措置等に関する指針」, http：//www.shinkin.org/new/050318/3_26.pdf
[28] 日本証券業協会,「個人情報の保護に関する指針」, http：//www.jsda.or.jp/html/kisoku/pdf/c 021.pdf
[29] 日本証券業協会,「協会員における個人情報の適正な取扱いの確保について」, http：//www.jsda.or.jp/html/kisoku/pdf/c 022.pdf
[30] 日本証券業協会,「インターネット取引において留意すべき事項について (ガイドライン)」, http：//www.jsda.or.jp/html/oshirase/internetwg/guidline.pdf
[31] 金融庁, 金融持株会社に係る検査マニュアル, 平成 15 年 7 月, http：//www.fsa.go.jp/manual/manualj/motikabu.pdf
[32] KPMG エムエムシー(株), “ 図解実務入門よくわかる JISQ 15001 ”, 日本能率協会マネジメントセンター, 2004 年
[33] 岡村　久道, “ 個人情報保護法の知識 ”, 日本経済新聞社, 2005 年
[34] 社団法人日本能率協会, “ 個人情報保護法対応審査員が教える ISMS 実践導入マニュアル ”, 2005 年
[35] 藤谷　護人, “ e-Japan 時代の情報セキュリティと個人情報保護 ”, 2003 年

執筆者紹介　寺 田　由 美 子 (Yumiko Terada)

1986 年法政大学工学部電気工学科卒業. 同年日本ユニシス(株)入社. UNIX　CAD システムの開発, ネットワーク設計, 大規模インターネット接続環境, ネットワーク・セキュリティ環境構築業務を経て, 2003 年より情報セキュリティコンサルティング業務に従事. 現在日本ユニシス・ソリューション(株)ソリューションビジネス　情報セキュリティソリューションに所属し, IT と情報セキュリティ観点からのソリューション開発, コンサルティング業務を担当.