個人情報保護のためのソリューションフレームワーク

IT System Solution Framework for Personal Information Protection Law

北折　昌司
■KITAORI Shoji

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）では，個人情報取扱事業者は「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」（第20条）とされている。しかし，これには，IT（情報技術）システムに展開するための具体的な措置の内容については定められてない。

東芝ソリューション（株）は，経済産業省のガイドラインに基づいて具体的なセキュリティ機能の基準を作り，これを“個人情報保護対応基準（PDPS3：Personal Data Protection Standard for System Solutions）”とした。この基準により，特定の業種・業務向けシステムと情報セキュリティ基盤システムとの役割分担及び連携が可能となり，個人情報保護法に対応したコンサルテーションと組み合わせることで，個人情報保護のためのソリューションフレームワークが実現した。

The Personal Information Protection Law stipulates that holders of personal information must take sufficient measures to protect that information. However, the law does not specify concrete means by which this is to be achieved.

Toshiba Solutions Corp. has formulated an original detailed IT system specification called the personal data protection standard for system solutions (PDPS3), based on the guidelines of the Ministry of Economy, Trade and Industry (METI). The PDPS3 standard enables the cooperation of all application systems and security infrastructure systems. By combining PDPS3 with a consulting service, we have realized a system solution framework for personal data protection.

1　まえがき

2005年4月1日に完全施行となった個人情報保護法[(1)]では，「個人情報データベース等を事業の用に供しているもの」を個人情報取扱事業者と定め，個人情報の取扱いに関して様々な義務を課している（第2条）。ほとんどの企業がこの個人情報取扱事業者に該当し，法律で定められた個人情報の適正な取扱いを行わなくてはならない。なかでも，第20条の「安全管理のために必要かつ適切な措置」，いわゆる安全管理措置は，企業の情報セキュリティ管理を法律により義務化しているという点で重要である。

安全管理措置の具体的な内容については個人情報保護法には記述がなく，各省庁が所轄分野ごとにまとめるガイドラインで必要に応じて記述されることになっている。現在，各省庁から個人情報保護法施行のためのガイドラインが公開されているが，その中でも経済産業省のガイドライン[(2)]はもっとも詳細かつ具体的で，また，他の省庁に先んじて発表されたこともあり，ほかのガイドラインのベースとなる重要な位置を占めている。

経済産業省のガイドラインでは，安全管理措置を「組織的安全管理措置」，「人的安全管理措置」，「物理的安全管理措置」，「技術的安全管理措置」の四つの種類に分け，それぞれに「しなければならない」項目と，それを更に詳細に記述した「望ましい」項目を挙げている（**図1**）。望ましい項目は比較的詳細な実施内容を含んでいるため，安全管理措置の一つの実施標準になるものと思われる。

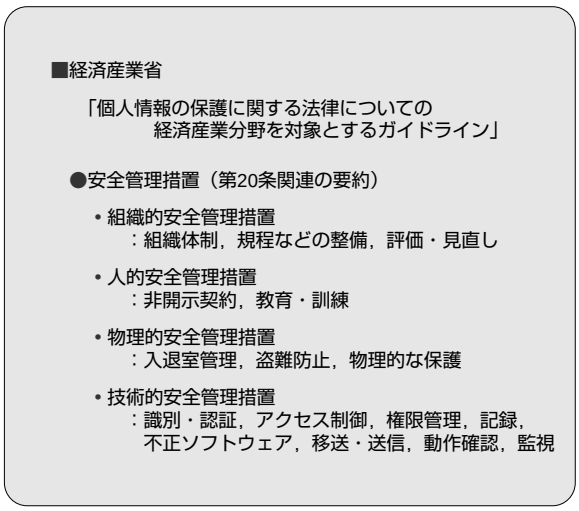

図1．経済産業省ガイドラインの安全管理措置[(2)] ― 安全管理措置を四つに分類して詳細を定めている。
Security management practices in METI guidelines

2 個人情報保護対応基準（PDPS3）

経済産業省のガイドラインは標準として有用なものであるが，実際のシステムを作り上げる立場から見ればあいまいな点が多く，システムを開発し構築する場合には更にブレークダウンすることが必要になる。また，実際のシステムがこのガイドラインに準拠しているかどうかを判断するうえでも，よりいっそうの具体化が必要になると考えられる。

そこで東芝ソリューション（株）は，経済産業省のガイドラインを基礎として，システムソリューションの開発及び構築のための“個人情報保護対応基準（PDPS3：Personal Data Protection Standard for System Solutions）”を策定した[(3)]。この基準を適用することによって，当社のシステムソリューションのセキュリティ機能を強化向上させることができるとともに，それを運用するユーザーが個人情報保護法への対応状況を的確に把握することができる。

例えば，経済産業省のガイドラインでは「個人データを取り扱うシステムの使用状況の定期的な監視」を行うことが望ましいと決められているが，使用状況とは何を示しているのか，定期的とは実際にどのような時間間隔を求めているのかあいまいである。しかし当社では，これについて具体的な基準を設けることで，一定の実現レベルを保つことができる。また，ユーザーに対しては，何をどのように監視しているのかを明確に説明することができるようになるため，ユーザー自身がそれで十分なのか，あるいは不足しているのかを容易に判断することができるようになる。

セキュリティを考えた場合，システムを利用するユーザーが常に適切な判断ができるかどうかがたいへんに重要となる。なぜなら，完全なセキュリティや絶対安全なシステムは存在しないことが明らかであり，その危険性を認識して使ってもらうことが安全性の基本と考えるからである。個人情報保護対応基準（PDPS3）の狙いもまさにそこにある。

3 組織的安全管理措置

経済産業省のガイドラインが求める安全管理措置の中で，組織的安全管理措置については個人情報保護対応基準（PDPS3）に含めることは適切ではないと考えられる。なぜなら，ここで求められていることは，システムを運用するユーザーの組織体制，規程類，リスク評価といった企業独自の判断や経営方針などに立ち入った内容だからである。これについて，第三者である当社が何かの基準を設けることは必ずしも妥当ではないであろう。

しかし，組織的安全管理措置についても，ユーザーの実施状況が不十分なため個人情報が流出したとされた場合，安全管理義務違反とみなされる可能性もある。そこで当社は，当社のシステムソリューションに関する組織的安全管理措置について，コンサルテーションサービスを用意した。

当社は，既に“情報セキュリティマネジメントシステム（ISMS）[(4)]認証取得コンサルティング”というコンサルテーションサービスを実施しており，多くの実績を上げている。組織的安全管理措置はISMS規格の要件にほぼ含まれるため，共通した手法を用いることができる。したがってユーザーは，当社のコンサルテーションサービスを受けることにより，組織的安全管理措置の要求に十分に備えられるとともに，更に，必要に応じてISMS認証を取得することもできる。

4 情報セキュリティ基盤システム

このように，当社では個人情報保護対応基準（PDPS3）を策定し，それに基づいたソリューション並びにコンサルテーションをユーザーに提供したいと考えている。しかし，個々のシステムソリューションごとに基準に適合させていくことは効率が良いとはいえない。また，セキュリティはユーザーのすべてのシステムにとって共通の課題であり，それを解決する一連の基盤システムとして実現したほうが高い投資効果を上げることができると考えられる。そこで当社は，様々な業種・業務システムと連携した情報セキュリティ基盤システムソリューションとして，“IT資産管理システムソリューション”，“ID（IDentification）管理／認証システムソリューション”，“ネットワークセキュリティソリューション”を用意した（**図2**）。

IT資産管理システムソリューションとは，様々なIT資産すなわち，パソコン（PC）などのハードウェア，そこに記録されているソフトウェアやデータといった価値ある資産を管理し，アクセス制御することで，不正利用や持出しを防止することができるシステムソリューションである。

ID管理／認証システムソリューションは，アクセスの主体となる人あるいは媒体となる機器などを確実に識別し認証するためのシステムソリューションである。例えば，ICカードを用いたユーザー認証や，PKI（Public Key Infrastructure）認証基盤といったシステムなどが挙げられる。

ネットワークセキュリティソリューションは，IT資産管理システムあるいはID管理／認証システムと連携してネットワークの適切な制御を行うシステムソリューションである。簡単なものではファイアウォールや侵入検知システムなどが挙げられるが，最近では資産管理や認証と更に密接に連携した，高度なネットワーク制御の仕組みとして“検疫ネットワーク”といったものも現実のものとなっている。

4.1 業種・業務システムとの連携

それでは，情報セキュリティ基盤システムが業種・業務システムとどのように連携し個人情報保護の機能を果たしていくかを，ID管理システムを例にとって説明する。

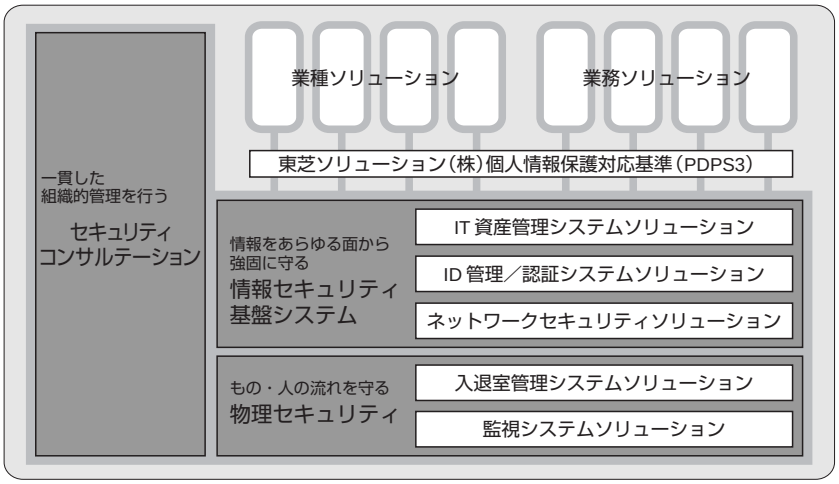

図2．個人情報保護対応ソリューション― 様々な業種・業務ソリューションと情報セキュリティ基盤システムソリューションが個人情報保護対応基準（PDPS3）によって連携している。

Architecture based on PDPS3 standard

ID管理システムとは，ユーザーを識別する固有情報であるID，及びその認証に用いる情報，例えばパスワードや電子証明書などを安全に保管・管理し，ユーザーの識別と認証を正しく行うためのシステムである。

現在でも比較的多くの場合，業種・業務システムが管理するデータベースにこうしたIDや認証情報が記録され，業種・業務システムが独自の方法で識別と認証を行っているケースがある。このときにはID管理システムというものは明示的には存在することはない。しかし，経済産業省のガイドラインによれば，ID管理及び認証に関する要求事項は少なくない。これを**図3**に示す。

これらの要求事項を満足するセキュリティ機能として，個人情報保護対応基準（PDPS3）はより詳細な実装基準を定めている。しかし，これを個々の業種・業務システムごとに実装する場合，それに掛かるコストも大きいが，なにより，それぞれの業種・業務システムが独自に実装を行うことによる一貫性の欠如が，セキュリティ上は非常に大きな問題になると推定される。そこで，これらの業種・業務システムとは独立したID管理システムが必要となるのである。

ID管理システムを用いた場合，すべての業種・業務システムが必要とするID及び認証情報を一元管理し，業種・業務システムから識別・認証にかかわる要求があった場合，統一したポリシーにより識別と認証が行われ，その結果が業種・業務システムへと返される（**図4**）。ID管理システムは，個人情報保護対応基準（PDPS3）の識別・認証にかかわる実装基準に基づいた，個人情報保護のための基本機能を備えている。したがって，個々の業種・業務システムはその実装を行う必要はなく，個人情報保護対応基準（PDPS3）のほかの実装基準に注力すればよい。また，識別と認証については厳密に一貫性が保たれると同時に，結果として1か所による認証制御，すなわちシングルサインオンの仕組みを構築することが可能となる。

■個人データへのアクセスにおける識別と認証を行ううえで望まれる事項

●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，生体認証など）の実施

※IDとパスワードを利用する場合,望ましい措置
- パスワードの有効期限の設定
- 同一又は類似パスワードの再利用の制限
- 最低パスワード文字数の設定
- 一定回数以上ログインに失敗したIDの停止，などの措置

●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などの識別と認証（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など）の実施

MAC：Media Access Control
IP　：Internet Protocol

図3．識別・認証に関する要求事項[2] ― 経済産業省のガイドラインでは，識別・認証に関する技術的安全管理措置について推奨基準を定めている。

Identification and authentication requirements in METI guidelines

4.2　個人情報保護対応ソリューション

個人情報保護対応基準（PDPS3）は，個人情報保護の観点から情報セキュリティ基盤システムと業種・業務システムとの役割分担及び連携を実現させるものである。また，この基準

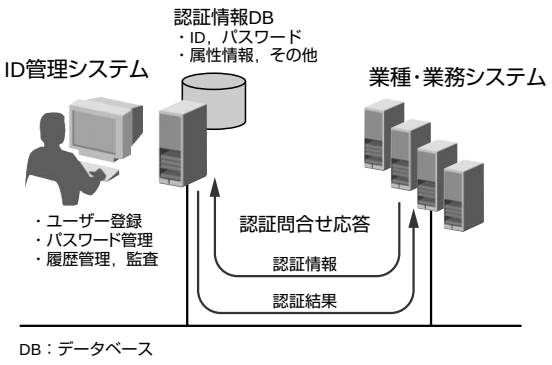

図 4．ID 管理システムと業種・業務システムとの連携 ― ID 管理システムはすべての業種・業務システムの識別と認証を統合する情報セキュリティ基盤システムとして機能する。

Cooperation of ID management system and application systems in authentication process

に含まれない組織的安全管理措置については，コンサルテーションサービスを用意して，これらのシステムを利用するユーザーがすべての安全管理措置を実現できるようにしている。こうしたフレームワークに従って提供される当社のシステムソリューション及びサービスを“個人情報保護対応ソリューション”と呼ぶ。前述の ID 管理システムも個人情報保護対応ソリューションの一つであると言うことができる。当社は今後，こうした個人情報保護対応ソリューションを順次リリースしていくことにしている。

5 あとがき

以上述べたように，東芝ソリューション（株）は，個人情報保護対応ソリューションを提供することで，ユーザーの個人情報保護法対応に向けて，ユーザーと共に企業セキュリティの実現を目指したいと考えている。

文　献

⑴ 首相官邸．個人情報の保護に関する法律．<http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/>，（参照 2005-02-28）．

⑵ 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．<http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf>，（参照 2005-02-28）．

⑶ 東芝ソリューション（株）．「個人情報保護法対応基準」を制定．<http://www.toshiba-sol.co.jp/ccc/news/detail/041019-2.htm>，（参照 2005-02-28）。

⑷ 日本情報処理開発協会（JIPDEC）．情報セキュリティマネージメントシステム（ISMS）。<http://www.isms.jipdec.jp/>，（参照 2005-02-28）。

北折　昌司　KITAORI Shoji

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。
セキュリティサービスの開発業務に従事。
Toshiba Solutions Corp.