解説 1

ITシステムによるプライバシー対策

さまざまな分野における急速なITシステムの普及により、個人情報が収集・蓄積される機会が昨今増えてきています。一方、2005年4月に個人情報保護法が施行されるに当たり、企業が保有する個人情報を適切に保護し、利用するための早急な対策が求められています。この対策は、マネジメント・システムおよびITシステムの両面から行う必要があります。セキュリティーに関連する体制・ポリシー策定・教育・マニュアル整備・運用確立・徹底といったマネジメント・システムでの対応も非常に重要ですが、ここではITシステムによる対策に焦点を当て、個人情報保護のためのセキュリティー対策、およびこれに加えて必要となる「自己の個人情報の取り扱いをコントロールする権利」（Alan Westin, Privacy and Freedom 1967）と定義されるプライバシーの権利を保護するための対策を解説します。

日本アイ・ビー・エム株式会社
セキュリティー&ネットワーク技術 担当
青木 美佐 Misa Aoki

［プロフィール］
1990年、日本アイ・ビー・エム入社。以来、流通ソリューション・センターに所属し、IT技術者として流通・サービス業のお客様のクライアント/サーバー・システム、Webシステムの構築プロジェクトに参画。2002年より技術 セキュリティー&ネットワーク技術のマネジャーとして、主にセキュリティー／プライバシー・エリアにおけるお客様・社内エンジニアへの技術支援に従事。

❶. 個人情報のライフ・サイクルとITシステムによる対策

2005年4月に個人情報保護法が施行されるに当たり、プライバシーを考慮したシステム構築が注目されています。プライバシーとは「自己の個人情報の取り扱いをコントロールする権利」（Alan Westin, Privacy and Freedom 1967）と定義されています。個人情報とは、特定個人を識別することが可能な情報すなわちPII（Personally Identifiable Information）を指します。詳細定義は、法令やガイドラインによる場合がありますが、一般には「氏名、住所、電話番号、メール・アドレス」などが該当します。

お読みくださっている皆さんの多くはインターネット・ショッピングを利用された経験があることでしょう。皆さんご自身のプライバシーの権利とは、そのサイトが利用・保持するご自身の「氏名、住所、電話番号、メール・アドレス」などの情報の取り扱い方法を自分で決める権利があるということを意味します。

IT（Information Technology：情報技術）システムでは、個人情報保護の観点でどのような対策を取るべきでしょうか？ 個人情報のライフ・サイクルである「収集」「利用」「保管」「廃棄」の四つの段階ごとに実施すべき主な対策を次に挙げます。

《収集》

●利用目的／利用範囲の明示

- 収集する個人情報の種類・利用目的・共有範囲・取り扱い基準を明示。
  －Webサイトでの収集の場合、プライバシー・ポリシーをページ上に記載するなど。

●適正な取得

- 業務遂行に必要最低限にとどめた情報収集。
- アンケートのような任意な情報提供の際は、その情報を提供する本人が得られる利益・利便性を明示。
  －提供された個人情報については「弊社からのご案内を差し上げるのに使用してもよろしいです

か?」など、確認するプロセス(画面など)を設け、情報提供した本人が意志表示可能とするなど。

《利用》

●収集時の合意範囲での利用

- 個人が特定できる形では、個人情報を収集時に合意を得た範囲に限定した業務でのみ使用する。
- データ・マイニングなど、本人が明示した以外の目的で使用する場合は、個人を特定しない程度に抽象化する。

●保有データの開示・訂正の仕組み

- 保有している個人情報データの開示/訂正要求に対応した機能・仕組みの作成。
  - ―本人が使用するためのアプリケーションを構築して対応、もしくは要求があった時点で企業側が個別に操作し対応。

●不用意な開示防止への方策

- 作業ファイルの残存、正規利用者からの悪意を持ったアクセスへの対策を講じる。
- 個人情報を扱う業務には、ユーザー認証機能を設ける。
- ユーザー認証の際に利用するユーザーIDの使い回しは禁止する。
- 詳細なアクセス制限/管理を行う。
  - ―情報利用者と本人との関連によるアクセス。
  - ―本人の同意の有無に対応した情報処理。
  - ―個人情報に関するアクセス・ログの取得など、説明責任を保つために必要な措置。

《保管》

●保有状況、利用方法の把握と適切な運用

- どのような個人情報をどの部門で保有し、どのように使用しているのかを以下の観点から把握し、その範囲で適切に運用する。必要に応じ、不正アクセス防止のためにデータを暗号化する。
  - ―入手目的・入手経路・入手方法・維持方法
  - ―取り扱い経路(情報のオーナー・利用者など)
  - ―保管場所(一時保管を含む)・保管形態・保管期間
  - ―流通経路(複製利用・委託・提供など)

《廃棄》

●廃棄方法の確定と適切な運用

- 個人情報ごとに保管期間後の廃棄方法を決め、運用する。
- メディア・機器を廃棄する際に個人情報を残したままにしない。

《全段階にわたり》

●正確性・安全性の確保

- 不正なアクセスを防止する。
  - ―操作の制限(複製禁止など)・暗号化・認証強化。
- 保有データの「最新」「正確」を保つように努める。
  - ―企業が「最新・正確である」と想定している状態に保つ。事実と相違しているという本人からの指摘があった時点で、対応・修正できる仕組みを用意する。
  - ―全社的に共通に扱うデータベースをアプリケーションごとに複製して使用する場合は、複製先での使用方法(再複製の有無を含む)を把握し、維持する仕組みを用意する。

❷. プライバシー保護を考慮したアクセス制御/管理の必要性

セキュリティー対策の強化および既存システムの改修、運用の見直しなどを通じて、前述の対策の多くは実現可能です。実際、個人情報漏えい事件が続発する中で、個人情報の利用に関しては、アクセス可能な利用者・目的・手段を最少限に限定し、アクセスを制限する対策を講じられている企業は多いことでしょう。

しかしながら、こうしたセキュリティー対策による制限のみで、プライバシー対策の観点からのアクセス制限は十分といえるでしょうか?

セキュリティー対策により、企業の機密情報としての個人情報の保護は実現しても、個々人に指示された個人情報の利用範囲が、同じ業務の中でも異なる際の対応は困難でしょう。セキュリティー対策に加えて、個人情報保護のルール(個々人により指示された利用範囲)に対応するアクセス制御の実装が必要とな

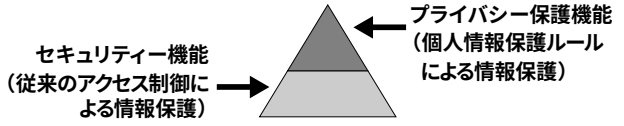

図1. プライバシー保護を実現するアクセス制御/管理

ります。これは、前述の個人情報利用時の対策としての「詳細なアクセス制限／管理」に該当します(**図1**)。

例えば、あるショッピング・サイトのお客様である山田花子さんは、自分の個人情報をショッピングに必要な配送などの業務以外では利用してほしくないという意志を持っているとします。一方、田中太郎さんはパーソナライズされた自分あてのセール情報などをEメールでタイムリーに知らせてほしいと希望しています。このショッピング・サイト上のデータベースを利用して、例えばマーケティング部門が購入傾向を分析するために購入履歴・年齢・性別を利用する場合は、どのように処理すればよいでしょうか? また、パーソナライズしたマーケティング活動を行う場合はどうでしょうか? 情報の利用者(配送部門やマーケティング部門の担当者)に対して、データベース上のデータ項目ごとに、利用目的に応じたアクセス制限／管理の必要があるでしょう。

❸. プライバシーを考慮したITシステムでの対策例

前述のようにプライバシー保護の観点からは、個人情報を扱うITシステムの利用者を、その人の役割(所属部署・役職など)や利用目的、アクセス対象となる情報との関係によってアクセス制御できることが求められます。

以下に、プライバシーを考慮したITシステムを実現するための三つの対応例を挙げます。

3.1. データベース設計

プライバシー保護の観点からは、個人情報を含むデータはできるだけほかのデータと分離し、PII(Personally Indetifable Information:個人を特定できる情報)のみを含んだデータベースやテーブルを構築することが有用です。PIIが必要な場合のみ、このデータベースやテーブルにアクセスすることで、利用範囲および利用者の制限、アプリケーションからの個人情報利用の制御が容易となります。

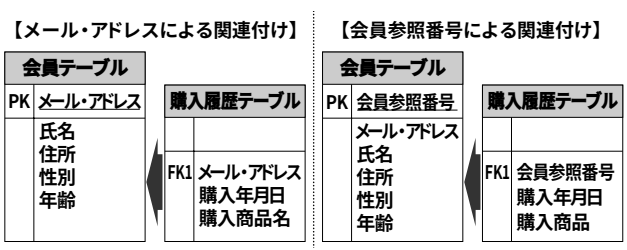

図2. データベース設計の例

例えば、**図2の左**に示したように、会員情報とその購入履歴を保持するために、PIIと見なされるメール・アドレスをキーに関連付けると、購入履歴テーブルも個人情報として慎重な扱いが必要となる可能性があります。一方、**図2の右**に示したように、二つのテーブルを関連付けるキーを、個人とは直接関係ないもの(会員参照番号)とした場合、会員参照番号自体はPIIではないため、購入履歴テーブルは個人情報として見なされなくなります。

3.2. プライバシーを考慮した処理

次に、個人情報の利用目的に合わせて処理することも有用です。例えば、購入傾向を分析処理するたびに、図2の右の会員テーブルと購入履歴テーブルに性別・年齢・購入商品名を問い合わせる場合、個人情報を扱う処理と見なされる可能性があります。そこで、両テーブルから購入傾向分析に必要な情報(性別・年齢・購入商品)のみを抽出した購入傾向テーブルをあらかじめ別途作成しておき、購入傾向分析処理ではこの購入傾向テーブルに問い合わせることで、個人情報を扱わずに分析処理が可能となります。

3.3. 利用目的によるアクセス制御

最後に、個人情報を含むデータベースへのアクセス制御をミドルウェアなどに任せ、アクセス・ポリシーに従って検査し、不正な要求の排除を行う例として、ISO/IEC 10181-3によるアクセス制御モデルを挙げ

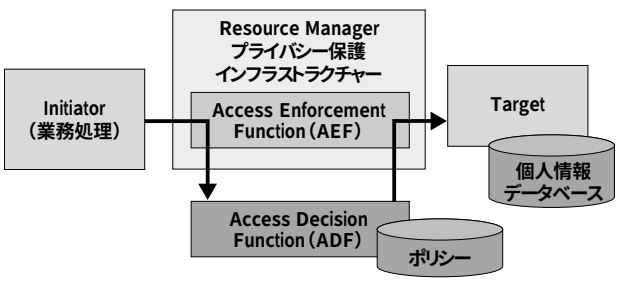

図3. ISO/IEC 10181-3によるアクセス制御モデル

ます(**図3**)。この方法は前の二つの例と比べ、業務アプリケーションの要件に依存する範囲を最小に抑え、かつプライバシーを保護することができます。

❹. Tivoli Privacy Manager for e-businessによるアクセス制御

前章で紹介したアクセス制御モデルは、IBM製品ではTivoli® Privacy Manager for e-business[1]が実装しています。Tivoli Privacy Manager for e-business利用時のポリシー作成から監査までの概要を以下にご紹介します。

4.1. ポリシー作成

Tivoli Privacy Manager for e-businessの一機能であるポリシー・エディターからプライバシー・ポリシーを定義します。プライバシー・ポリシーには、Webサイト内で収集する個人情報の種類や利用目的、共有範囲、業務固有の制約事項など、プライバシーへの考え方や個人情報の取り扱い基準を記述します。プライバシー・ポリシーを記述する際には、Webサイトで収集するすべての個人情報に関するデータ項目を洗い出し、以下の事柄を決めておくとよいでしょう。

- 企業の情報、コンタクト先
- 係争の解決先
- 収集する個人情報の種類・項目
- 個人情報の利用目的、利用する業務の範囲
- 個人情報収集時の同意の有無(オプトイン/オプトアウトなど)
- 個人情報の利用者
- 個人情報の保存期間

4.2. ポリシーの組み込み

定義されたプライバシー・ポリシーは、個人情報を取り扱う業務による処理に適用されます。また、このプライバシー・ポリシーを、P3P(Platform for Privacy Preferences)ポリシー文書に変換することも可能です。個人情報が処理されるとき、Tivoli Privacy Manager for e-businessが監視を行うことによって、プライバシー・ポリシーが順守されます。

- P3Pは、ユーザーがWebサイトでの自分の個人情報の取り扱いを、より簡単に自動で管理するために、W3C(World Wide Web Consortium)が定めた規格です。P3Pでは、Webサーバーが持つプライバシー・ポリシーをXML(Extensible Markup Language)で表現するための規約と、このプライバシー・ポリシーをユーザー側(Webブラウザー)に通知するためのプロトコルとを規定しています。Internet Explorer 6.0やNetscape Navigator 7.0といったブラウザーがP3Pを実装しています。

《参考》
「The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification」 http://www.w3.org/P3P/

4.3. 個人情報と同意情報の収集

個人が個人情報を企業に対し提供する際に、企業はプライバシー・ポリシーに基づいて、個人情報の取り扱い(収集・使用目的・使用方法)に関する趣旨を各個人に伝えます。個人情報取り扱いに対する承諾を得た後、承諾内容を個人別に記録し、各個人の承諾内容に基づくアクセス管理を行います。

4.4. アクセス制御

プライバシー・ポリシーに基づき、個人情報取り扱い目的別に定義されたアクセス制御を行うように、Privacy Managerサーバー(図3のADFに対応)とPrivacy Managerモニター(図3のAEFに対応)の機能によってアクセスを監視・制御します。Privacy Managerサーバーは、Privacy Managerモニターから受け取った個人情報へのアクセス情報により、プライバシー・ポリシーに適合するかどうかを判断して、アクセス可否を決定します。Privacy Managerモニターは、個人情報にアクセスするアプリケーション・プログラムに実装され、個人情報にアクセスが発生したときに、Privacy Managerサーバーへアクセス可否判断を問い合わせ、判断結果をアプリケーション・プログラムに返答します。そのアクセス・ログにより、従来のDBMS(Database Management System:データ

ベース管理システム）の機能だけでは困難であった、読み出しを含むデータベースへの問い合わせ結果を、本人の同意の有無、アクセス・ポリシーの検査結果、データの利用者情報とともに取得できます。

4.5. 監査レポートの作成

プライバシー・ポリシーが順守されているかどうかを判断するために、レポートを作成することができます。以下の監査レポートにより、個人情報が企業内部でどのように使用されているかを把握できます。

- 個人情報の管理に使用されているポリシーに関する、企業全体の視点でのレポート。
- 個人情報に対するアクセスについて、ポリシーへの適合／不適合についての監査証跡。
- 特定の個人情報にだれが何のためにアクセスしたのかに関するレポート。

このように、Tivoli Privacy Manager for e-businessを利用することにより、「だれが、どの情報を取り扱うか」のみを管理するだけでなく、企業の個人情報に対するアクセス・ポリシー（プライバシー・ポリシー）に基づき「だれが、何の目的で、だれの情報を取り扱うか」というプライバシー保護とその監査が可能になります。

❺. おわりに

個人情報を保護する上でのITシステムによる対応策とプライバシー保護の観点からの対応例をご紹介しました。

現時点の個人情報保護法では、データを収集・利用する場合にどうすればよいかをデータ保護の観点から定めており、プライバシー保護の域には達していないといわれています。しかしながら、「情報開示管理」[2]でも示したように、個人情報漏えい事故が頻繁に報道される状況下、個人情報保護法が施行されると、個人情報の適切な利用に個々人の関心がさらに高まると思われます。

セキュリティー対策を行い、ユーザーからお預かりしている個人情報の漏えいを防止することは、事故に伴う賠償金支払いなどの金銭的損失や、社会的な企業イメージの失墜を防ぐために不可欠です。これに加え、ユーザーごとの指示に従ったプライバシー対策を行うITシステムの構築が、企業の資産である個人情報を最大限に活用するオンデマンド企業の実現を導くことになるでしょう。

[参考文献]

[1] Tivoli Privacy Manager: http://www-6.ibm.com/jp/software/ tivoli/products/privacy.html

[2] 渡辺 芳明、情報開示管理ソリューション – 情報漏えい防止と情報有効活用の両立–、本誌51ページ