

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 -

大量の個人情報漏えい、お客様へのおわびやセキュリティ対策のために多額の支出が必要となる事件が続発しています。通常、対策として取られるのは、システム内で個人情報を扱う人間を限定する方法です。ただし、この対策だけでは、せっかく集積されている情報を死蔵することにもなりかねません。個人情報に代表される機密情報を有効に活用しつつ、機密情報の漏えいを防止できるシステムを構築することが、今求められています。

その実現のためには、機密情報の有効活用を行いながら、情報の不正使用・漏えいを防止するための情報開示管理という概念を提唱します。漏えいを防止しなければならない機密情報の中でも、個人情報は特に詳細なアクセス制御が必要になるなど、より強力な仕組みにより保護することが必要です。情報開示管理では、個人情報を保護できるような強力な情報保護の仕組みを構築し、この仕組みを、他の機密情報の保護にも適用することを考えます。



日本アイ・ピー・エム株式会社
テクニカル・サポート
IBM ディスティングイッシュト・エンジニア、
CISSP

渡辺 芳明 Yoshiaki Watanabe

[プロフィール]

日本アイ・ピー・エム(株)テクニカル・サポート所属。セキュリティおよびプライバシー担当のICP ITアーキテクトとして、

数多くのお客様で、セキュリティおよびプライバシー関連のシステムを設計・構築。IBM ディスティングイッシュト・エンジニア、技術士(情報工学部門)、CISSP(Certified Information System Security Professional)。
Eメール・アドレス: watanabe@jp.ibm.com

①. 情報漏えい事件の対策と情報開示管理

2003年以来、顧客情報が大量に漏えいする事件が続発しています。中には、おわびとして商品券を配ったり、システムのセキュリティ強化策を講じるために何十億円という費用が掛かってしまった例もあります。

情報漏えい事件に対応したシステムのセキュリティ強化策としては、重要情報へアクセスできる利用者を制限することが多いようです。

国内の企業では、伝統的に性善説に基づいた運用方式が取られることが多く、職務として情報へのアクセスが不要になった利用者のIDがそのまま残っていたり、個人単位の認証が行われていなかったりすることが、これらの事件の温床となったと考えられます。事件の共通点として、サーバー内に格納された機密情報が、運用管理担当者や外部委託者による不正行為で盗まれる場合が多かったことを考えると、機密情報にアクセスできる利用者の数を制限する方法は有効な対応策であると考えられます。

ただし、利用者の制限は、運用管理担当者の不正という単一の原因に特化した対策であり、それだけでは十分とはいえません。現在、多くの企業で運用されているシステムでは、それ以外にも多数の課題が存在し、運用管理担当者の不正以外の理由で機密情報が漏えいする可能性もたくさん残っているからです。そうした潜在的な課題が顕在化するたびに個々に特化した対応策を取っているのでは、根本的な完全な解決にはなりません。潜在的に存在する課題を網羅的に解決し、情報漏えいの可能性をなくす解決策を事前にとっておく必要があります。

また、機密情報にアクセスできる人間の数を極端に制限すると、保有する情報の有効活用を図れなくなり、所有している情報を死蔵してしまうことにもなりかねません。現在のようなオンデマンド時代にこそ、企業が持つ重要な情報を有効に活用することが要請

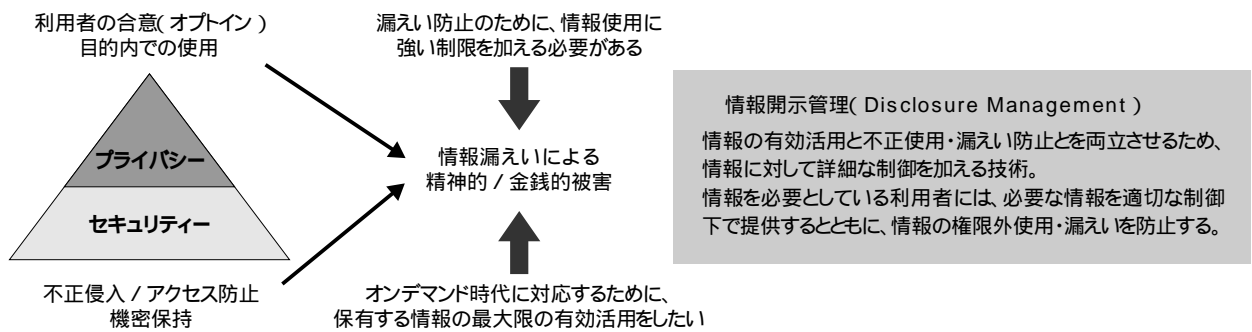


図1. 情報開示管理

されています。

所有する情報を有効に活用しながら、情報の不正使用を防止し、情報漏えいを防ぐためには、矛盾する二つの要件を同時に満たすことが必要になります。それには、情報開示管理という考え方に基づいたソリューションが有効です(図1)。

2. 個人情報処理の特性と、機密情報の情報開示管理への応用

図1には、セキュリティ機能の上にプライバシー機能を付加しています。これは次に挙げる例のように、個人情報については通常のアクセス制御機能だけでは対応し切れない部分があるためです。

- ・ 個々の個人情報の使用範囲は、その企業が消費者に提示したプライバシー・ポリシーによって示された範囲となります。社内ユーザーが業務を行うときに個人情報を使用できるか否かは、プライバシー・ポリシーにより許可された範囲に含まれる業務であるか否かにより決定されます。
- ・ 個々の消費者は、自分の個人情報の使用範囲に関して指示(合意)することができます。同じ業務であっても、その業務での使用に合意したお客様の情報は使用できますが、合意のなかったお客様の情報は使用できません。

個人情報の適正な使用範囲は、多くの要因によって変化します。2005年4月に個人情報保護法が施行されると、個人情報の適切な使用範囲についての消費者の関心もより高まると思われ、ここに述べたような詳細な処理が要求される場合が増えてきます。このように、情報開示管理の面から見たときに、個人情

報は、ほかの情報に比べて詳細な制御が必要となることが多く、それに伴い高度な管理が必要になるという特徴があります。

従来、情報の漏えい防止というと、Trusted OSで使用される強制アクセス制御機能、あるいはそれに類似したアクセス制限による漏えい防止方式での対応が検討されることが少なくありませんでした。現在、個人情報漏えいしたサイトで採用されている利用者の極端な制限も、この考え方に沿った対応策であるといえるでしょう。これらの方式を採用すると、確かに情報漏えいのリスクを削減できますが、反面、情報の使用方法が制限されるという課題が生じます。大量の個人情報漏えいという事件に対する緊急避難としては適切であっても、保有する情報の有効活用を図るといふ今日の要求から見たときには柔軟性に欠け、長期的な対策としては不十分であると考えられます。

一方、個人情報保護で使われる詳細なアクセス制御に基づく情報保護方式は、そのために使用される基礎技術が発展してきたこともあって、十分実用に耐える段階に達してきています[1]。個人情報保護に用いられる技術を応用して、機密情報の漏えい防止を行いながら、情報の有効活用を図る情報開示管理の考え方が現実味を帯びてきたのです。

3. 個人情報処理アーキテクチャー

機密情報の保護に対して、個人情報保護機能に基づく情報開示管理を実装するには、まず、個人情報処理とはどのようなものであるべきかを明確にしなければなりません[2]。そのためのアーキテクチャーを図2に示します。

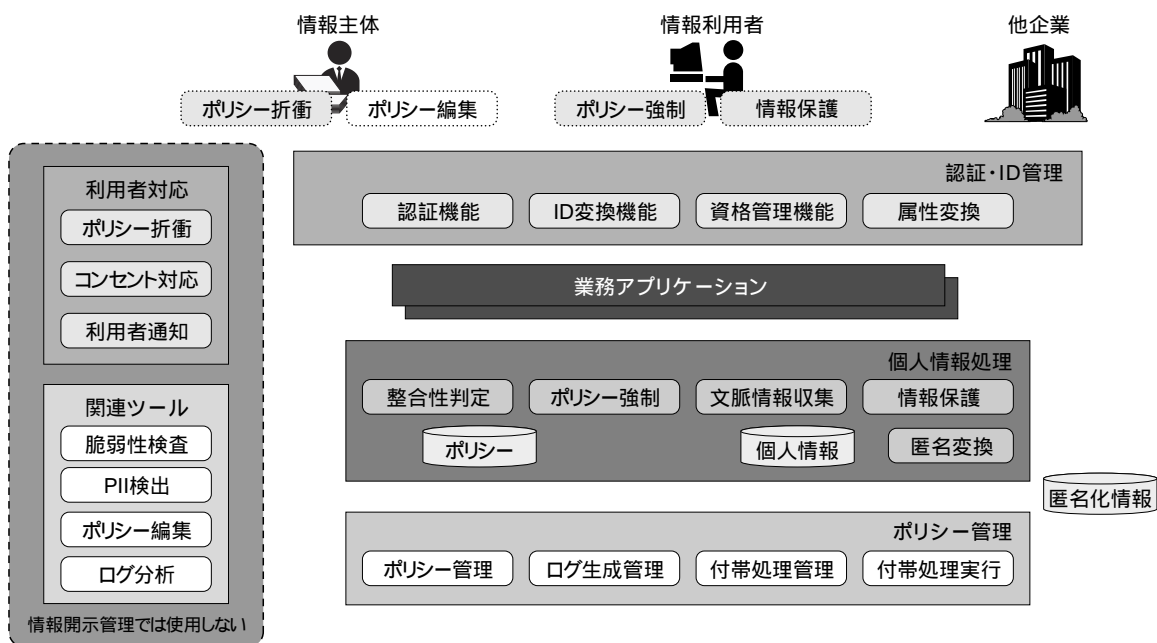


図2. 個人情報処理アーキテクチャー

このアーキテクチャーでは、個人情報を処理する業務アプリケーションの周りに、情報開示管理を実現する機能が配置されています。

・ **認証 / ID管理機能**

個人情報を扱う業務アプリケーションを使用するときに、利用者は、個人単位の認証を受けておく必要があります。これにより、個々の処理に関する説明責任を果たすことが可能となり、同時にアクセス制御に必要な情報を取得できます。

また、異なる情報保護ポリシーを持った企業へ個人情報を第三者提供するための情報の属性変換も必要となります。従来のようなファイル渡しによる第三者提供ではなく、Webサービスによる動的な個人情報の流通を可能とするには、このような機能が重要となります。

・ **個人情報処理機能**

この機能には、個人情報本体とポリシーが含まれています。情報を使用するときには、まず、ポリシーに照らし合わせて、このアクセス要求が正しいか否かを判定します。判定は、利用者識別や処理目的といった静的な情報だけではなく、処理の順序・環境などの動的な要素(情報アクセスが行われる文脈)も考慮する必要があります。判定の結果、ポリシーに適合していると判断されたアクセス要求だけが、処理を許可

されます。また、この機能には、格納 / 転送中の情報に対する漏えい防止のための機能も含まれています。

・ **ポリシー管理機能**

ポリシーの管理は、一つの大きな機能となります。この機能には、ポリシーの管理機能と、情報に対するアクセス・ログの管理機能が含まれています。

・ **利用者対応機能**

利用者の合意(オプトイン / オプトアウト)処理や、利用者に対するサイトからの個人情報に関連する通知機能などが含まれます(この部分は、個人情報処理固有のものであり、ここで考える情報開示管理においては使用しません)。

・ **関連ツール**

個人情報保護に関するサイトの脆弱性検査など、各種のツール類がここに含まれます(この部分も、個人情報処理固有のものであり、ここで考える情報開示管理では使用しません)。

この個人情報処理アーキテクチャーでは、格納 / 転送中の情報を適切に保護することにより、システム管理者や運用者による情報漏えいを阻止します。同時に、ポリシーに基づくアクセス制御機能で、エンド・ユーザーからの権限を超えたアクセス要求を防止し、正当な利用者からの正当な要求に対してのみ許可を与えることで、情報の有効活用を図ることが可能とな

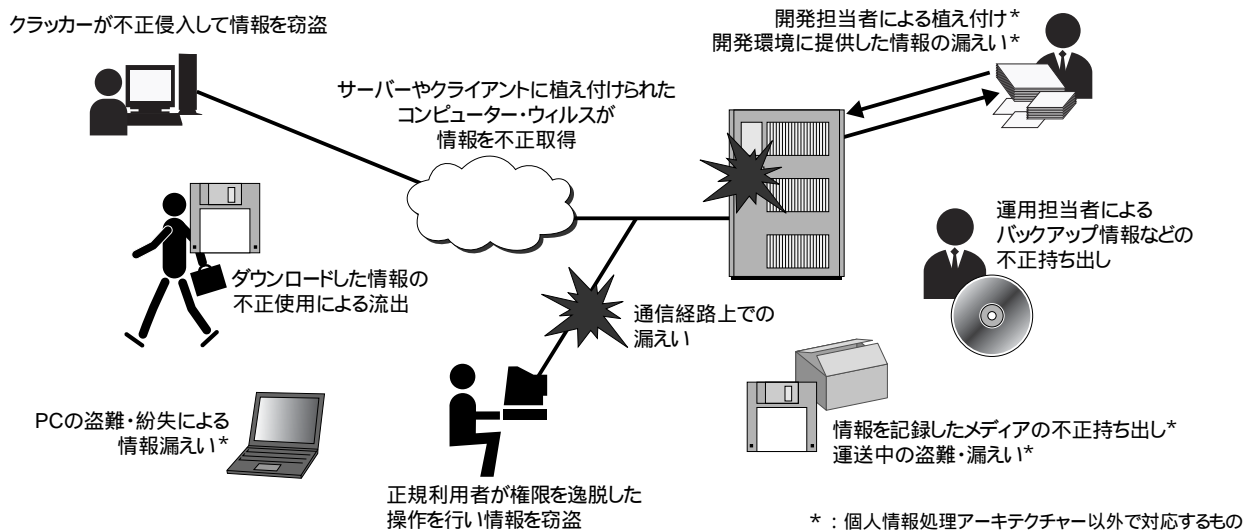


図3. 機密情報に対する漏えいの脅威

ります。

次に、この個人情報処理アーキテクチャーを機密情報の漏えい防止に適用するとどうなるかについて検討します。

4. 機密情報漏えいの脅威と対策

機密情報漏えいの脅威は、システムの各所に存在します。主な脅威を図3に示します。

ここに上げた脅威の多くは、個人情報保護アーキテクチャーを実装するテクノロジーで対抗することができます(図で*を付けた項目は、システム運用時以外の対策が必要となるため、個人情報保護アーキテクチャー以外の対応策により防御します)。

・ 正規利用者の権限逸脱行為による情報の盗盗

正規利用者への「なりすまし」は、認証機能で防御します。また、正規利用者が、与えられた権限以上の機密情報にアクセスしようとしたときは、ポリシー強制機能で対抗します。

・ 運用者による情報の不正持ち出し

サーバーに格納中の機密情報を、情報保護機能により(暗号化するなどの手段で)保護しておくことによって、機密情報の不正持ち出しが情報漏えいにつながるような対策を講じます。

・ 通信経路上での情報漏えい

通信途上の機密情報も、情報保護機能によって(暗

号化した通信経路を使用するなどの手段で)保護し、通信経路上の情報漏えいを防止します。

・ 情報を記録したメディアの不正持ち出し、運送中の盗難・漏えい

暗号化による保護を施せない印刷媒体などについては、物理的な媒体にRFID(Radio Frequency Identification)や万引き防止用のタグを付けて不正持ち出しを管理することにより、情報漏えいに対抗します。

・ PCにダウンロードした情報の不正使用

社内使用のPC(Personal Computer)は会社から支給されることが多いため、不正使用防止のための仕組みをPCに組み込むことが可能です。個人情報処理アーキテクチャーでは、情報利用者のPC側に情報保護機能とポリシー強制機能とを組み込むことにより、情報の有効活用と情報漏えい防止とを共存させます。PC側にダウンロードしたファイルは、情報保護機能で(通常は暗号化することによって)保護しておきます。PC利用者がファイルを読み出すときには、ポリシー強制機能がサーバー側のポリシーへ問い合わせ、それに従ってアクセス制限を強制します。モバイル利用者であっても、PHS(Personal Handyphone System)などを使用してサーバー側に接続できる場合が多いため、接続したサーバーの制御下にあるときだけ情報を使用できるように強制すると、強力な防御を行うことが可能となります。

・クラッカーが不正侵入して情報を窃盗

クラッカーによる不正侵入が仮にあったとしても、このアーキテクチャーを実装したシステムでは、格納 / 転送中のいずれにおいても、機密情報が保護されない状態で存在することはあり得ず、クラッカーによる情報の窃盗を防止できます。また、クラッカーが管理者権限などを不正に入手したとしても、機密情報のアクセスにはポリシーによる制限が掛かっていますから、通常の場合、クラッカーは機密情報を不正に入手することができません。

・サーバーなどに植えつけられたコンピューター・ウィルスによる情報の窃盗

クラッカーによる不正侵入の場合と同じく、機密情報は常に保護された状態で存在しますから、コンピューター・ウィルスによる情報の窃盗も防止できます。

・開発担当者によるバック・ドアの植え付け、および情報の窃盗

システム開発時に、開発担当者がバック・ドアや、情報漏えいのための仕組み(Covert Channel)をこっそりと植え付けていないかどうかを検査する仕組みが必要となります。これは、システム開発時のテストを十分に行うことと、本番環境への移行において不正な処理の植え付けの検査を十分に行うこと、および開発環境と本番環境を分離しておくことで実現できます。

・PCの盗難・紛失による情報漏えい

PC側の情報保護機能により、たとえ機密情報をダウンロードしたPCが盗難・紛失したとしても、PCの中に格納されている機密情報が漏えいすることはありません。

⑤. おわりに

以上、述べてきたように、個人情報処理アーキテクチャーを応用したシステムでは、機密情報の漏えいを防止しながら情報の有効活用を図ることが可能となり、機密情報に対する情報開示管理機能を実現できます。

個人情報処理アーキテクチャーを構成する個々の要素技術として使用できるテクノロジーは、各社から出荷されています。ただし、これらの要素技術を個々に導入しただけでは、整合性のあるシステムを構築することは難しく、機能的に穴の開いたシステムにならざるを得ません。

個人情報処理アーキテクチャーの中心となるものは、ポリシーと、ポリシーを強制する機能です。個人情報処理アーキテクチャーを構成するほかの構成要素は、ポリシー強制機能へ問い合わせ、ポリシー強制機能が下したアクセス可否の判断に従って処理を行うことが必要となります。

このような、中央制御の仕組みに従うことによって、整合性の取れた情報保護機能を実装することが可能となります。

[参考文献]

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

[2] 青木 美佐、ITシステムによるプライバシー対策、本誌46ページ