管理コスト削減とシステム向上を実現するID管理システム技術

ID Management Technology for Cost-Saving and Functional Reinforcement of Systems

能勢　健一朗　　池田　竜朗　　小林　智恵子
■NOSE Ken-ichiro　■IKEDA Tatsuro　■KOBAYASHI Chieko

複数のシステムでID（IDentification）を個別に管理している場合，追加や削除などセキュリティ管理業務が煩雑になり運用コストが高くなりがちである。また，2005年4月に完全施行された「個人情報の保護に関する法律」[1]（以下，個人情報保護法と略記）への対応や，増大する運用管理コストを削減するために，IDによるユーザー識別と認証の仕組みをどのように実現するかは重要な課題となっている。

東芝ソリューション（株）が開発したID管理システム技術は，個人情報保護法と経済産業省ガイドラインに準拠したセキュリティ機能を持ち，様々な業務システムのID管理を統合的に扱うことで，管理コスト削減とシステム向上を実現するとともに，個人情報保護法に対応したシステムの構築を容易にすることが可能である。

When managing IDs on multiple systems, ID management operations (addition, deletion, etc.) commonly become complex, resulting in a high management cost. Moreover, conformance with legislation such as the Personal Information Protection Law, which came into force in Japan on April 1, 2005, and the creation of mechanisms for user identification and recognition that can reduce the high cost of ID management, have also become important issues.

Toshiba Solutions Corp. has developed ID management technology incorporating a security function that conforms with both the Personal Information Protection Law and the guidelines of the Ministry of Economy, Trade and Industry (METI). By integrating the IDs of multiple enterprise systems, it is possible to develop a system that can reduce the management cost and enhance the system capabilities.

1 まえがき

インターネットに代表されるオープンなネットワークでのビジネスは，単一サービスから複数サービス間の連携へと移行し，新たなビジネスメリットをもたらしているが，その一方でIDが散在するリスクが発生し，各企業はリスク対策のために増大するコストに頭を抱えている。

また，2005年4月から個人情報保護法が完全施行されたのに伴い，個人にかかわる情報の取扱いがますます重要になっている。

複数のサービス（システム）において，利用者の識別情報と属性情報，及びセキュリティポリシーなどを個別に管理している場合，追加や削除などセキュリティ管理にかかわる業務が煩雑になり，運用コストが高くなる傾向にある。

個人情報保護法に対応しつつ，運用コストを削減するための仕組みをどのように実現するかが重要な課題となっている。

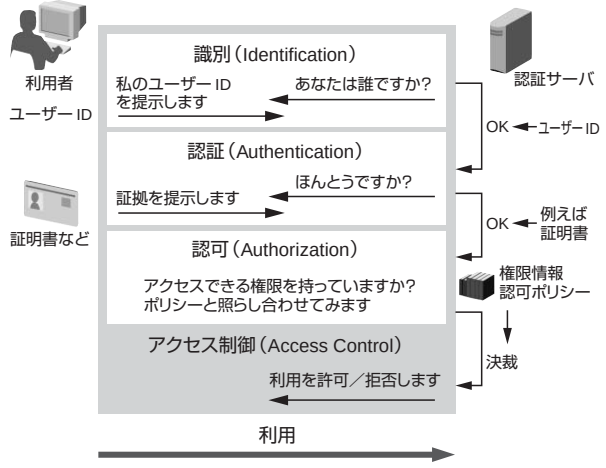

図1．認証と認可のフロー―本人のID情報の提示によって認証し，更に，本人である証拠の提示によってアクセス権限を確認し，利用を認可する。
Flow of authentication and authorization

2 個人情報保護法とID管理

経済産業省が発表した「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]（以下，経済産業省ガイドラインと略記）では，個人情報を取り扱う企業，すなわち個人情報取扱事業者の義務とされる安全管理措置を，詳細かつ具体的に規定している。

そのなかでも「個人データへの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の実施」は，もっとも重要な要件であると

いえる。なぜならば，“アクセス制御”，“権限の管理”，“アクセスの記録”などほかの多くの要件は，この“識別と認証”が正しく実施されたことを前提にしているためである。

したがって，“識別と認証”で利用されるID（ここでいうIDとは，単にユーザーIDといった識別情報だけではなく，属性情報などを含む利用者にかかわる情報全体のことを指す）をいかに安全に管理するかが，非常に重要な課題となっている（**図1**）。

更に，日常的に見られるIDの不適切な管理，例えば，退職した従業員のIDが残されている，不特定ユーザーであるゲスト用IDを使い続けている，といった運用が，重大な情報漏えい事件を起こす直接的な原因になることも多くなってきている。

3 ID管理／認証基盤システム

現在ほとんどの企業で行われているID管理は，システムごとに個別にIDを持ち，それぞれのシステムが独自に識別と認証を行うものが多く，このようなID管理ではシステム間の整合性をとることが難しいのが現状である。

例えば，一人の従業員が退職した場合，一個のIDが不要となるだけでなく，すべてのシステムの該当するIDを一つずつ削除する必要も生じてくる。しかし，このように管理が煩雑であれば，どこかで削除漏れが発生し，そのIDが不正アクセスに利用される可能性がある。

更に，経済産業省ガイドラインでも，利用者の認証に用いるパスワードは定期的に変更することが求められているが，そのため，パスワードをシステムごとに変更する状況となり，利用者はそれらのパスワードを正確に記憶し，使用するという負担を強いられることになる。

このような問題を解決するには，システムごとに個別に管理されていたIDに関する情報を一つにまとめることによって，IDの統合管理を実現する企業の基盤システムが必要となってくる。これを東芝ソリューション（株）では，ID管理／認証基盤システムと呼んでいる（**図2**）。

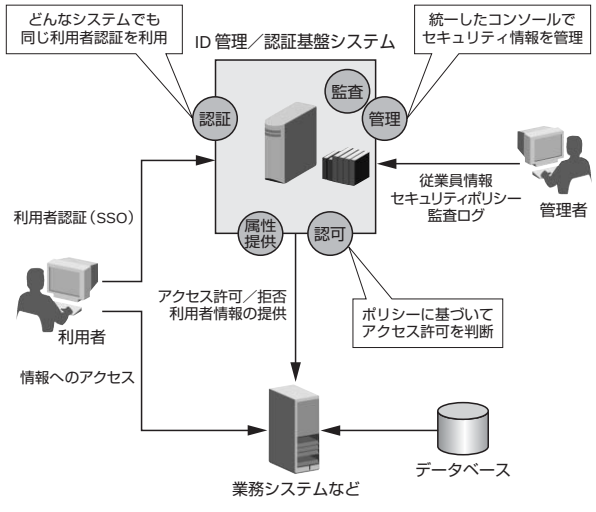

図2．ID管理／認証基盤システム ― システムごとに個別管理されていたIDの統合管理を実現する。

ID management authentication infrastructure system

4 IDの統合化を容易にするシステム技術

ID統合管理のポイントは，IDを利用する業務システムごとに適切な個別のカスタマイズを実現することにある。これは，IDは一つに統合されたとしても，それを利用して認証を行う業務システムは依然として独立して存在するためである。

ID統合のためのツールとして注目されているものに，プロビジョニングツールがある。このプロビジョニングツールは，マスタのデータベースを中心に，ほかのデータベースと連携してIDを管理する機能を持っているため，マスタのデータベースだけを管理することで，容易にID統合を実現できる。

しかし，実際の適用には適用先業務やツールのカスタマイズが必要であり，特にカスタマイズの内容がシステム及びツールの機能に依存するため，開発コストが高くなる傾向にある。また，このようなツールを使ったとしても，個人情報保護法に対応するという観点では十分な機能を備えているとはいえない。

当社ではこの点に着目し，様々な業務システムと連携できる標準インタフェースを用いた汎用的なID管理／認証基盤システムに，統合ID管理のために必須となる基本機能として5A（認証（Authentication），認可（Authorization），管理（Administration），監査（Audit），属性提供（Attribute Providing））機能を標準で実装した（**図3**）。

当社が提供するID管理／認証基盤システムには，以下の特長がある。

⑴ 利用者の使い勝手を向上
- ⓐ 何度も認証プロセスを行わない（シングルサインオン）
- ⓑ 複数の認証要素を持たない（パスワードなど）

⑵ 管理機能を一本化
- ⓐ セキュリティポリシーを一元管理
- ⓑ 管理者の負担を軽減
- ⓒ セキュリティ品質の維持
- ⓓ 開発期間やコストの圧縮
- ⓔ 法令遵守対応（個人情報保護法対応など）

⑶ 高度なセキュリティ機能に対応
- ⓐ クロスドメイン連携，ID連携など
- ⓑ より強力な認証方式に対応（電子証明書，生体認証など）

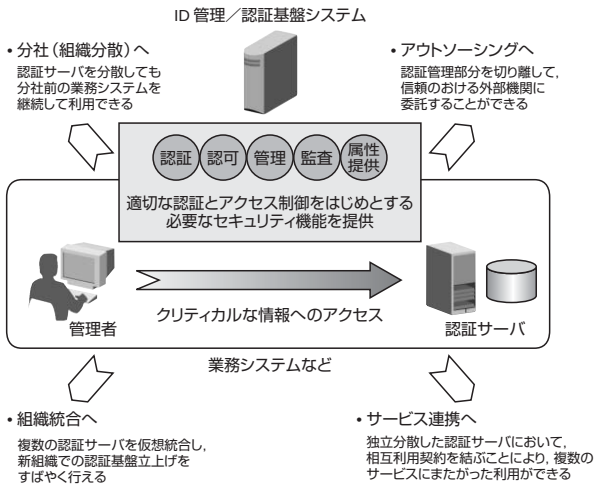

図 3．東芝ソリューション（株）の ID 管理／認証基盤システム — 5A 機能（認証，認可，管理，監査，属性提供）によって，適切な認証とアクセス制御をはじめとする必要なセキュリティ機能を提供する。

ID management authentication infrastructure system provided by Toshiba Solutions Corp.

5 ID活用技術

IDに関連するサービス領域としては，IDを安全に管理及び提供するもの（ID管理）と，管理されたIDを活用するもの（ID活用）とがある。一般に，前者はIDを活用するための基盤を提供するために利用され，後者はIDを活用した新しいサービスを構築するために利用される。前記のID管理／認証基盤システムは，ID管理をターゲットとしたものである。

当社は，このID管理だけでなく，ID活用にも注目している。ID活用技術では，複数のシステムに分散されているIDの情報を安全にやり取りすることで，連携されたIDを実現できることを目指している。

これにより，本来様々なサービスやシステムで保有していたIDを相互に利用しあうことができるが，ここで問題となってくるのが，IDの保護である。当然，誰もがIDを相互利用できるという完全なオープン利用は望ましくなく，ある程度の制約を持たせる必要がある。

これを解決するアプローチとして，Liberty AllianceではCircle of Trust（信頼の輪）という概念を提唱している[(3)]。Circle of Trustという信頼関係を構築した枠の中で，利用者主導のIDを相互利用することを実現している。

また，もう一つの問題としてトレーサビリティ（追跡性）がある。例えば，ユーザーが利用したサービスにかかわる情報（何を購入したのかなど）を収集することにより，ユーザーのプライバシーが損なわれる危険性がある。

この解決策として，Liberty AllianceではIDどうしを直接関連付けしないことにより，仮名（各サービス間で連携時の仮の名前）を実現している。これは，信頼できる第三者による保証に基づいて，ユーザーの保証と仮名とを両立している。

こうしたアプローチのうえで，必要な情報（主にユーザーの属性）だけ交換しあうことにより，リスクを軽減しつつ，様々なサービスへ活用できることが期待されている。例えば，一般的な認証やアクセス制御といったセキュリティサービスから，ユーザーの好みに基づいたコンシェルジェサービス，位置情報サービスなど様々な活用サービスが考えられている。

これらのサービスを実現するうえで重要となってくるものとして，IDの場所を検索するディスカバリサービスと，IDの属性情報を交換する属性交換サービスとが考えられる。

これらサービスの基本的な仕様は，Liberty Alliance仕様やOASIS SAML仕様[(4)]などで提供されており，上記標準インタフェースの基本的な仕様は，それらの標準仕様に基づいた機能を利用している。これにより，レガシーシステムや他社製品との相互接続性を確保することが期待できる。

更に，当社では，拡張した機能を提供するために，これら標準仕様をベースとした拡張機能を研究開発しており，より高度な5A機能の提供を目指している（**図4**）。

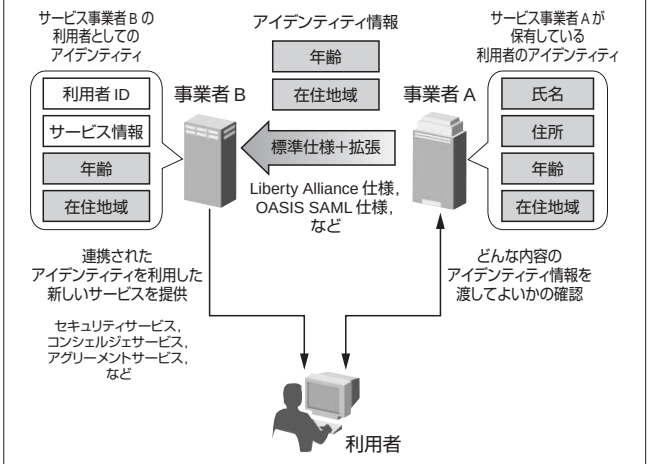

図 4．Liberty Alliance の概念 — 各サービス間において必要な情報だけを交換し合うことにより，様々なサービスへ活用できる。

Concept of Liberty Alliance

6 個人情報保護法への対応

当社では，経済産業省ガイドラインへの対応状況を確認するために，経済産業省ガイドラインに基づいて策定した個人情報保護対応基準に適合するようなシステムソリューションの開発を行っている。これにより，個人情報保護法の安全管理措置として求められる基本機能を実現したID管理／認証

基盤システムを提供することが可能となっている。

しかし，個人情報保護法に対応していくためには，ID管理／認証基盤システムだけでなく，システム全体として対応していく必要がある。そのため，顧客が確実な安全管理策を実施するために必要な各種マニュアルや運用ガイド，及び組織的安全管理策の実現に向けたコンサルテーションサービスを用意するとともに，個人情報保護法に準拠した適正なシステムの導入から構築及び運用管理までを実現できるような総合的なサービスも提供している。

当社が開発したID管理／認証基盤システムは，個人情報保護法と経済産業省ガイドラインに基づいた主要なセキュリティ機能を実現し，様々な業務システムのID管理を統合的に扱うことを目指しているため，個人情報保護法に対応するシステム環境の構築を容易にするとともに，運用における運用管理者の負担を軽減することができる(**図5**)。

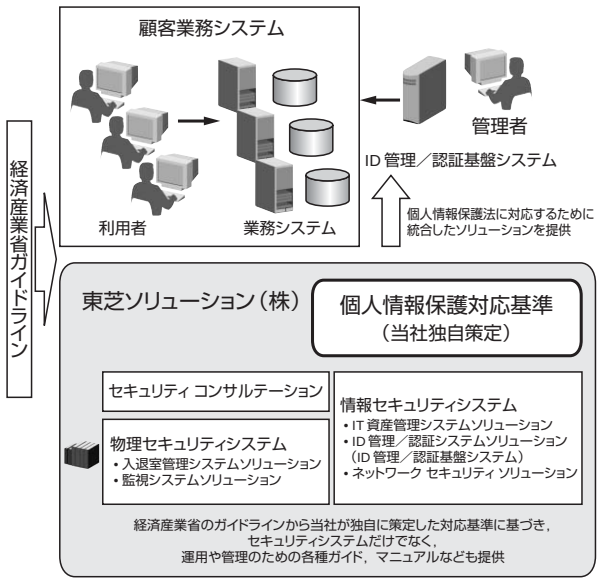

図5．個人情報保護対応ソリューション— ID管理／認証基盤だけでなく，運用管理などトータルで個人情報保護法に対応するため，統合したソリューションを提供する。

Solutions for Personal Information Protection Law

7 あとがき

当社は，個人情報保護法と経済産業省ガイドラインに準拠したセキュリティ機能を持ち，様々な業務システムのID管理を統合的に扱うことにより管理コストの削減とシステム向上を実現する，ID管理／認証基盤システムを開発した。これにより，個人情報保護法への対応や，運用管理コストの削減といった相反する課題を解決することができる。

今後は，ID管理／認証基盤システムを中核とし，人事情報システム，入退出などの物理セキュリティシステム，そして業務系システムを有機的に結び付け，セキュリティと利便性の向上をもたらすとともに，顧客にとって最適なIT(情報技術)基盤を実現していく。

文　献

(1) 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)．

(2) 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)．

(3) Liberty Alliance Project. Liberty Alliance.
＜http://www.projectliberty.org/＞，(参照 2005-02-28)．

(4) OASIS. Security Services (SAML) TC.
＜http://www.oasis-open.org/committees/security＞,(参照 2005-02-28)．

能勢　健一朗　NOSE Ken-ichiro

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 第三部主任。情報セキュリティ技術の開発に従事。
Toshiba Solutions Corp.

池田　竜朗　IKEDA Tatsuro

東芝ソリューション(株) SI技術開発センター SI技術担当。情報セキュリティ技術の開発に従事。情報処理学会会員。
Toshiba Solutions Corp.

小林　智恵子　KOBAYASHI Chieko

東芝ソリューション(株) SI技術開発センター SI技術担当主任。情報セキュリティ技術の開発に従事。
Toshiba Solutions Corp.