セキュリティと利便性を両立させる統合認証基盤

Construction of Unified Authentication Platform achieving Coexistence of Convenience and Security

大　竹　章　裕

要　約　企業内には数多くのシステムが存在し，その中には部門独自で管理しているシステムが見受けられる．これらのシステムには社外秘などの重要な情報が格納されており，適切な管理を要求される．さらにはネットワークの整備が進んでいることもあり，これらのシステムが容易にインターネットにさらされる環境にもなりえる．一方で 2005 年 4 月施行の個人情報保護法や内部統制などの外部要因により，情報セキュリティマネジメントが企業の経営にとって必須の条件となった．そのマネジメントを支える技術としてシステムのアクセスコントロールおよび ID 管理の基盤を整えることが急務である．また，セキュリティを意識するばかりでなく，利便性と両立する必要がある．

ネットマークスでは統合認証基盤として，ID の管理を行う仕組みである ID 管理基盤と，認証サービスを提供する仕組みである認証基盤を定義し，セキュリティと利便性を両立するシステムの構築に取り組んでいる．ID 管理基盤は，ID のライフサイクルを管理し，必要なときに必要なタイミングで ID を付与し，不要な ID はすぐに使用できないようにする．認証基盤は，確実な本人認証と利便性を高めるためのシングルサインオンやデバイス認証の環境を提供する仕組みである．さらに，近い将来に必ず訪れるクラウドコンピューティング時代を迎えるにあたっての統合認証基盤の構築についても取り組んでいる．

Abstract　There are many business systems in a company, and some of them are maintained by individual organizational units. They require the appropriate management because the important information such as “for internal use only” is stored in these systems. Besides, these systems can be exposed to the Internet easily by the fully-maintained network environment. At the same time, the information security management has become an essential requirement for the corporate management because of the external factors such as the Personal Information Protection Law and the internal control. In order to achieve this security management, the company should maintain their platform for access control and ID management urgently. In addition, it is necessary to be conscious of not only security but convenience.

Netmarks Inc defines the identity management system and the authentication system each as the platform for the unified authentication infrastructure. And the company works at construction of the unified authentication infrastructure that is consistent with security and convenience. An identity management platform manages the life cycle of identity. An identity management platform provides identity data as necessary, and revokes it if unnecessary. The authentication platform provides the environment of the reliable identity authentication, single sign-on for convenience, and devices authentication. Furthermore, we are working at constructing a unification authentication infrastructure for the cloud computing that is a near future system.

1. は じ め に

株式会社ネットマークス（以降，ネットマークス）では，セキュリティの分野で常に最先端の技術を取り入れ，ネットワークに接続された誰でもが安心して利用できるシステムの環境を顧客に提供してきた．2005 年の個人情報保護法施行からは，特に企業内部の情報セキュリティに対して注目し，ソリューションを提供している．本稿では，情報セキュリティの 3 大基本要素である CIA（Confidentiality：機密性，Integrity：完全性，Availability：可用性）の内，機密性と完全性に対して主にフォーカスのあたる統合認証基盤について，ネットマークスが考える機能要素を解説する．また統合認証基盤の構築経験を基に，実装にあたって注意すべき点について述べる．さらに統合認証基盤に関する今後の技術的な取り組みについても紹介する．

2. 統合認証基盤

統合認証基盤とは，情報システムやネットワーク，ファイルといった IT 資源に対して利用者がアクセスする際の本人確認や利用権限の範囲，レベルの限定（認証・認可）と，それらの基となる情報（ID：Identity 情報）の登録を統合して管理するものである．

個々のシステムでは，利用者に対して登録された正規のユーザであるか本人確認を行う機能は装備されているが，その設定はそれぞれのシステムで行う必要があり，システムが増加するに従って運用の負荷も増加するのは明らかである．そこでシステム毎に装備されていた認証機能を統合し，ID の集中管理を行うことで運用負荷の軽減を図り，同時にセキュリティを高めながら利便性も両立する統合認証基盤の必要性が増してきた．

2. 1 統合認証基盤の市場

IT の発展により，企業内では情報システムによるさまざまなサービスが充実してきた．しかしながら個々の情報システムが独自に認証機能を装備している限り，システムの利用者について認証や認可の情報を格納するデータベースが個々に存在することを意味する．その結果，システムが増えればそれらのデータベースも増えることとなる．また一方で情報セキュリティや企業内のコンプライアンスの意識の高まりから，システムの利用者の認証・認可のためのデータベースを適切に管理することが要求されるようになった．これは，多発する情報漏えい事件の主な原因が，削除もしくは無効化していなかった退職者などの本来不要な ID を利用した不正アクセスだったことによると考えられる．法律でも，2005 年 4 月に施行された個人情報保護法，さらには 2007 年 9 月に施行された金融商品取引法[*1] を中心として企業の内部統制が求められるようになった．内部統制のガイドラインとして金融庁企業会計審議会内部統制部会から発表された「財務報告に係る内部統制の評価及び監査の基準」には，IT 統制におけるアクセス制御についても記述されている．

最近では，PCI DSS（Payment Card Industry Data Security Standard）と呼ばれるクレジットカードビジネス関連事業者向けのデータセキュリティ基準が注目を集めている．PCI DSS は 12 項目の要件で構成されており，そのうち要件 7 と 8 でデータやコンピュータへのアクセスに関する基準を示している．

NPO 日本ネットワークセキュリティ協会（JNSA）の調査[2]において，「情報セキュリティツール」市場で六つに分類されているカテゴリー[*2] のうち「アイデンティティ・アクセス管理製品」は二番目に大きな規模となっている．特に 2007 年度以降は三番目のカテゴリーである

「ネットワーク脅威対策製品」を市場構成比において3ポイント以上離しており，情報セキュリティ対策としての重要性が増していることが分かる．富士キメラ総研の調査[3]では，内部脅威ソリューションのカテゴリーのうち，統合認証基盤に関係するデバイス認証ツール，シングルサインオン，統合ID管理ツール，RADIUS*3サーバ ソフトウェア/アプライアンスの市場に注目すると，デバイス認証ツールが一度落ち込む見込みだが，それ以外は堅調に伸びていく予測となっている．特に統合ID管理ツールに関しては，2009年見込みで約43億円，2010年予測で約46億円規模という予測になっている（表1，図1）．

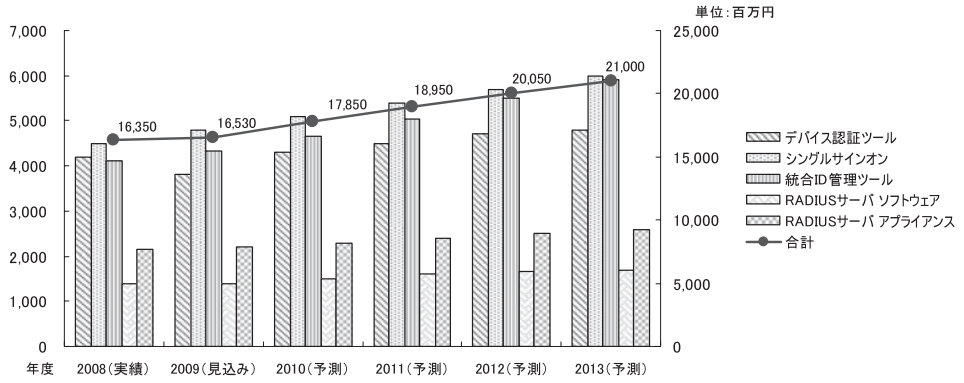
以上の調査データからも，統合認証基盤の重要性と注目度が高まっていることが伺える．

表1　統合認証基盤に関連する製品市場の実績と予測

単位：百万円

	2008年度（実績）	2009年度（見込み）	2010年度（予測）
デバイス認証ツール	4,200	3,800	4,300
シングルサインオン	4,500	4,800	5,100
統合ID管理ツール	4,100	4,330	4,650
RADIUSサーバ ソフトウェア	1,400	1,400	1,500
RADIUSサーバ アプライアンス	2,150	2,200	2,300
合計	16,350	16,530	17,850

富士キメラ総研「2009ネットワークセキュリティビジネス調査総覧」セキュリティ機器/ツール市場から抜粋



富士キメラ総研「2009ネットワークセキュリティビジネス調査総覧」セキュリティ機器/ツール市場から抜粋

図1　統合認証基盤に関連する製品市場の実績と予測

2.2　統合認証基盤の構成

ネットマークスでは，統合認証基盤をID管理基盤と認証基盤に分類し，提供する機能を切り口にそれぞれの機能要素として定義している（表2）．

ID管理基盤は，主にIDのライフサイクルを管理する役割を担う．ID情報用データベースを元帳として各認証用データベースに対して情報の整合性を保つためのプロビジョニングを行う仕組みである．詳細は2.3節にて述べる．

認証基盤は，認証用データベースにより各業務システムに対して認証サービスを提供する役割を担う．また，一回の認証で複数のシステムを利用できるシングルサインオン環境や，ICカード認証や指紋認証などのバイオメトリクス認証による認証方式を提供することも認証基盤に含まれる．詳細は2.4節にて述べる．

統合認証基盤の理想は，すべてのシステムから参照される一つの認証用データベースでID

表 2　統合認証基盤の機能要素

	機能	説明
ID管理基盤	ID情報用データベース	ID情報を一元的に格納するデータベース（ID管理基盤として管理者が操作を行うための各種機能を含む）
	パスワードマネジメント（変更/同期）機能	ユーザからのパスワード変更を受け付け，ID情報用データベース，認証用データベースへ更新内容を反映する
	プロビジョニング（/デプロビジョニング）機能	各ID管理対象となるシステムへID情報の配信，変更，削除を行う
	ワークフロー機能	ID情報の申請，承認を行う
認証基盤	認証用データベース	IDの認証情報を管理するデータベースであり，認証機能を有する（LDAPサーバ，Active Directoryなど）
	ネットワーク認証用ゲートウェイ（GW）機能	LDAPサーバと連携し，主にネットワーク認証機器（無線アクセスポイント，SSL-VPN，認証スイッチ）に認証機能を提供する
	デバイス認証機能	WindowsクライアントにICカード認証や指紋認証などのバイオメトリクス認証機能を提供する
	シングルサインオン（SSO）機能	一度システムへログインを行うとユーザが許可されているシステムへは再度認証をせずに利用可能にする環境を提供する
共通	ログ機能	監査のためのログをレポーティング情報として提供する

を管理し運用する構成である．実際には，既に構築/運用されている数々のシステムをすべて一つの認証用データベースには統合できないため，プロビジョニング機能により補完する．つまり，中心となる認証用データベースに統合できるシステムは統合し，それ以外のシステムに対してはプロビジョニングを行い ID の整合性を保つことによって統合管理を行うハイブリッドな構成となる（図 2）．

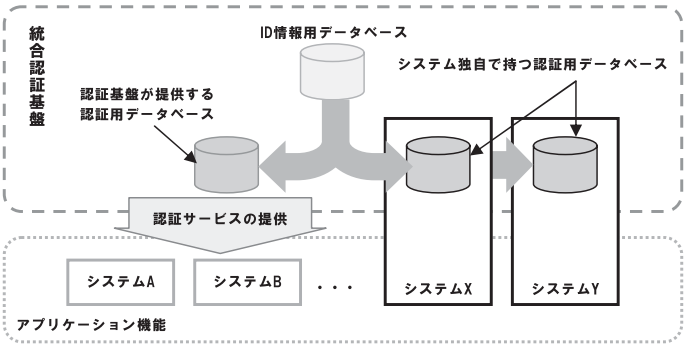


図 2　ID 情報用データベースと認証用データベースの位置付け

2. 3　ID 管理基盤

ID 管理基盤は，システムを利用する利用者の識別子である ID およびパスワードなどの認証情報を管理する仕組みとして，企業/組織内で発生する組織改編，ユーザ属性の更新，IT 環境の変更（新システムの追加，既存システムの改修/リプレース/バージョンアップ）などのイベ

ントに対して，ID のライフサイクルの管理を行う基盤である（図 3）．そして ID 情報用データベース，パスワードマネジメント機能，プロビジョニング/デプロビジョニング機能，ワークフロー機能および共通機能としてログ機能で構成される（表 2）．以下，各機能について説明する．

図 3　ID のライフサイクル

2. 3. 1　ID 情報用データベース

ID 情報用データベースは，利用者に対する各システムの ID やパスワード，属性情報などをメタデータとして格納するデータベースである．つまりユーザの属性情報を抽象化して格納し，配信先のシステムに対して意味のあるマッピングを行うための元帳の役割を担う．たとえばあるシステムは性別を“male/female”としてテキスト情報として持つが，別のシステムでは 0 と 1 で持つなどの違いを吸収する必要がある．また，ID 情報用データベースを設計する上で必要となるのが，ID 情報の基となるトラステッドリソースの決定，前述のメタデータと配信するデータのマッピング，アクセス制御の元情報となるロール情報の管理方針の決定である．

2. 3. 2　パスワードマネジメント機能

企業/組織内ではセキュリティポリシーにより，各システムのパスワードを定期的に変更するようにルール化されているところがほとんどである．そのため利用者は，利用を許可されているシステムに対してそれぞれパスワード変更作業が定期的に発生する．利用しているシステムが多ければ多いほど，利用者のパスワードの運用負荷が増えることになる．従って，利用者に対してパスワードを集中管理できるサービス環境を用意し，その環境でパスワードを変更すれば，関連するすべてのシステムのパスワードも同時に変更される機能が必要となる．一方で管理者側もシステムの利用者からパスワードの忘却などの理由によりパスワードリセットの依頼を受けた場合，対象となるすべてのシステムに対してリセット処理を行うことになり運用負荷が増えることになる．たとえば別の利用者のパスワードをリセットしてしまうなどの操作ミスを起さないような注意を求められる．従って，管理者に対しては一箇所でパスワードリセット処理を行えば，対象の利用者に関連するシステムのパスワードをすべてリセットできる機能が必要となる．

2. 3. 3　プロビジョニング/デプロビジョニング機能

プロビジョニング/デプロビジョニング機能は，統合認証基盤の対象となる各システムへ必要な ID 情報を配信する機能である．ID 情報用データベースでマッピングされたルールに従い

各システムに対してデータを配信する．またデータの加工が必要であれば，ルールに従い加工した後に配信する（プロビジョニング）．一方で利用者の退職などによりIDが不要になった場合は，直ちに無効化し，退職者がシステムに対して不正にアクセスできないようにする．またIDを無効化しても一定期間IDは残す運用を行っていた場合は，期限が来たら必ず削除する処理も必要となる（デプロビジョニング）．

2. 3. 4　ワークフロー機能

申請から承認，配信（登録）処理までの一連の業務フローをシステム化する機能である．最近では，内部統制のシステム要求により，登録の人為的ミスや個別の判断を排除するために必要な機能として位置づけられている．

2. 4　認証基盤

認証基盤は，利用者がネットワークやファイルを含む情報システムへアクセスする際に，システムに登録された正規のユーザであるかを確認・検証を行う仕組みとして，認証用データベース，ネットワーク認証用ゲートウェイ機能，デバイス認証機能，シングルサインオン（SSO）機能および共通機能としてログ機能により構成される（表2）．以下，各機能について説明する．

2. 4. 1　認証用データベース

統合認証基盤としては，一つの認証用データベースで構成されることが理想だが，各システムに認証用データベースが存在する場合もあり，プロビジョニングを行うことにより整合性を保つ．認証基盤としての中核となる認証用データベースと各システムに存在する認証用データベースがある．

2. 4. 2　ネットワーク認証用ゲートウェイ機能

ネットワークシステムを利用する際に認証を必要とするシステムとして，認証VLANや検疫ネットワーク，リモートアクセスなどがあげられる．ネットマークスはネットワークインテグレータであるため，あえてネットワーク認証用ゲートウェイ機能を強調して定義している．これらのネットワーク認証には，認証サーバとしてRADIUSが利用される．最近のネットワーク認証用の機器は，認証データベースがLDAPに対応していることが多いが，ネットマークスではRADIUSを経由した連携を推奨している．アクセスログやアカウンティングログ[*4]の取得機能がLDAPより充実していることがその理由である．

2. 4. 3　デバイス認証機能

現在では，指紋認証をはじめとするバイオメトリクス認証やICカード認証など，本人確認を行うためのさまざまな認証方式が実用化されている（表3）．これらは本人の持ち物や体の特徴，癖などを利用して本人確認を行う認証方式である．実際には，組み合わせて利用する場合が多く，たとえばワンタイムパスワードであればトークン＋PIN[*5]の所有と記憶の二要素認証となる．パスワードによる認証機能の実装は比較的容易だが，利用者が簡単なパスワードを設定してしまうことによりセキュリティレベルは下がってしまう．最近では「パスワードの文字列を複雑なものにする（文字数や文字の種類）」や「定期的に変更する」など，システムに

実装されているポリシーを活用していることがほとんどであり，一定のセキュリティレベルは保持されているが，利用者のパスワード管理に関する負担も少なくない．利便性を損なうことなく高いセキュリティレベルを保持するには，バイオメトリクス認証やICカード認証などのデバイス認証機能の提供も検討する必要がある．

表3　認証の種類と認証方式

認証の分類		主な認証方式
Something you are	個人の体の特徴を利用して本人を識別する	指紋，虹彩，静脈など
Something you do	個人の行動や動作の癖などの特徴を利用して本人を識別する	サイン，声紋，キーストローク
Something you have	個人の持ち物によって本人を識別する	トークン，ICカード
Something you know	個人の記憶によって本人を識別する	パスワード，PIN（暗証番号）

2.4.4　シングルサインオン（SSO）機能

シングルサインオン（SSO）機能は，利用者の利便性を高める機能である．利用者が一度認証を行えば，その利用者が許されているシステムをシームレスに利用できるようにする機能である．各システムにエージェントを導入するエージェント型，クライアントとサーバの間に設置するリバースプロキシ型，システムの認証画面で自動的に利用者のパスワードを入力するパスワード代行入力型などがある．一般的にはWebアプリケーションに対してシングルサインオンを実現する製品が多い．Webアプリケーションに対応する製品では，エージェント型，リバースプロキシ型，共にブラウザのcookie機能を利用しシングルサインオンを実現する．エージェント型は大規模ユーザが利用するシステムに対して負荷分散の構成が取りやすいが，各システムに対してエージェントと呼ばれるモジュールを組み込む必要がある．当然システムが利用しているWebサーバ（ApacheやIISなど）に対応している必要もある．リバースプロキシ型は，シングルサインオンの対象となるシステムに対して手を加える必要がなく比較的容易に導入することができる．しかしながらリバースプロキシという構成が，性能上ボトルネックとなりやすいため，大規模ユーザが利用するシステムへの実装は注意が必要である．また複数拠点にまたがったシングルサインオンを実現するには，ネットワークの構成にも見直しが必要になる場合もある．パスワード代行入力型は，システムに対して手を加える必要もなく，リバースプロキシのようなボトルネックになるポイントも発生しない．デメリットとしては，クライアントにパスワード代行入力用のモジュールを導入する必要があることなどがあげられる．以上のようにそれぞれの方式にはメリット/デメリットがあり，実際には複数方式を組み合わせたハイブリッド構成で実装することが多い．

2.5　共通

統合認証基盤の機能要素にはそれぞれログ機能が実装されている．ここでは，ID管理基盤と認証基盤のそれぞれで必要とされるログ機能について述べる．

2. 5. 1　ID 管理基盤におけるログ機能

ID 管理に関わる各操作の履歴を保管，保存し，監査証跡として利用する．ある利用者の ID を変更，削除した場合の日時，申請者，承認者，操作結果のログが記録されていることによって，正しい手続きによって更新操作が行われた証跡となる．

2. 5. 2　認証基盤におけるログ機能

認証時の成否やアクセス元などを保管，保存し，監査証跡として利用する．不正なユーザがアクセスしていないか，不正な大量のアクセスがないかなど，セキュリティの観点からの証跡の役割がある．当然，認証プロセスの集中による負荷などを確認するシステム的な役割もある．またバイオメトリクス認証を導入した際は，FAR（False Acceptance Rate：他人受入率）や FRR（False Rejection Rate：本人拒否率）といった認証のための閾値のチューニングにも利用される．

3.　セキュリティと利便性を両立させる実装

統合認証基盤は，IT 資源にアクセスする利用者が，そのシステムに登録された正規のユーザであるかを確認・検証し，IT 資源を利用する権限を正規に認められている範囲に限定することによりセキュリティを確保する技術である．一方で，導入することにより，利便性を向上させる側面もある．代表的な例としてシングルサインオン機能は一度の認証により，複数のアプリケーションを別のシステムであることを意識せず利用することができる．また，ID 管理基盤の中核であるプロビジョニング機能は，運用者に対し一度の処理で複数のシステムに対してユーザ追加/変更/削除の操作を可能にする．利用者と運用者に対する統合認証基盤の主な役割と利便性を図 4 に示す．

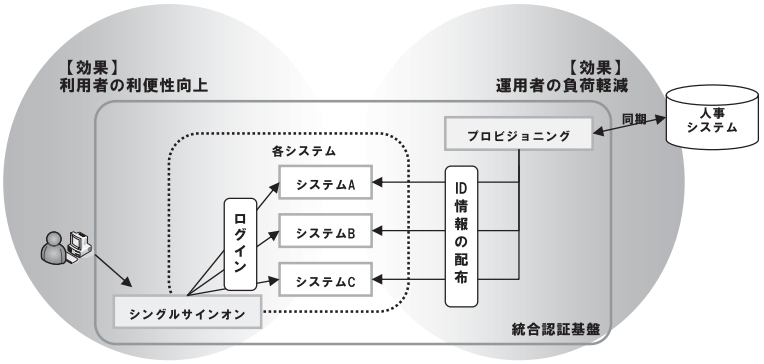


図 4　統合認証基盤と利便性

3. 1　ID 情報用データベースと認証用データベース

統合認証基盤には，ID 情報用データベースと認証用データベースの 2 種類の役割のデータベースがある．物理的に同一のデータベースである場合もあるが，役割が大きく異なるため分けて認識しておく必要がある．

3.1.1　トラステッドリソースの定義と連携

トラステッドリソースとは，ID 情報用データベースに格納するべき元のデータベースを指す．一般的には人事データベースを指すが，派遣社員やアルバイトの情報は人事データベースとは別に管理されていることが多く，通常は複数のデータベースから後述するデータクリーニングを行い ID 情報用データベースに格納する．

ネットマークスが構築に携わった事例では，ID 情報用データベースとトラステッドリソースをオンラインで接続させるケースは少ない．人事データベースには給与や家族構成などの個人情報が多数含まれており，人事担当部門のポリシーによりオンラインで接続できないなどの顧客側の事情が多く見られた．その場合，CSV 形式などのテキストデータによって，利用者の姓名や社員番号（多くの場合ログイン ID），属性情報（役職，職位，所属部署）などを出力し，ID 情報用データベースに投入する．

3.1.2　データクリーニングとデータマッピング

トラステッドリソースから ID 情報用データベースにデータを投入する際には，データクリーニングが必要となる．たとえば社員を管理している人事システムのデータベースでは，姓と名が別々のフィールドに格納されているが，派遣社員を管理しているデータベースは姓名が一つのフィールドに格納されていたり，名前のふりがなが，それぞれ“ひらがな”と“カタカナ”で格納されているなどのケースも考えられる．意味は同じだが格納の際のシステム的な実装方法が異なり，それらを ID 情報用データベースに投入する際に，どちらかに揃える必要がある．また，その逆で一見同じ意味を持つようなデータが実はシステム的には異なる意味のデータであることが考えられる．たとえば，人事システム上で使う退職者フラグは，決められた未来のタイミング（月末など）で処理されるためのフラグだが，別のデータベースでは，既に退職したユーザを識別するためのフラグであるという具合である．データクリーニングとは，複数のトラステッドリソースから流れてくるデータの持つ意味を認識し，メタデータとして同じ意味合いのものは同じフィールドに一定のルールに則った形式で格納できるようにする処理である．

次に，データクリーニングし ID 情報用データベースに格納した情報と，各システムへ配信する情報を対応させるためのマッピングを行う．単にメタデータをそのまま各システムのフィールドに対応させるだけでなく，複数のメタデータから結合処理や条件分岐処理を行ってデータを生成する．

3.1.3　アクセスコントロール情報（ACL）の取り扱い

アクセスコントロールは，システムに正規に認められた権限の範囲での利用を制御するために必要な機能であるが，統合認証基盤のシステム上には，個々のアプリケーションシステムに依存する個別のアクセスコントロール情報を格納せずにシステム構築を行う場合がほとんどである．これにはいくつかの理由があげられる．まず，認証基盤上で対象となるすべてのアプリケーションシステムのアクセスコントロール情報を格納すると，データベースが非常に大きなものになり，ID のライフサイクル管理が煩雑になってしまうなど現実の運用に適さない．さらに，新しいアプリケーションシステムが加わった際にデータベースへの影響範囲が大きくなる．以上を考慮すると，原則は，アクセスコントロール情報を格納しない仕組みが望ましい．

しかしID管理基盤側でアクセスコントロールのための元情報は必要になる．そこで考えられるのがロールによる管理である．ロールは以下の三種類に大別される．

1） ビジネスロール
2） ITロール
3） アプリケーションロール

ビジネスロールは，役職，部門といったビジネス上の位置付けや担当業務の職責などを分類し，職務分掌上齟齬が生じないように定義する．なお，兼任や人事異動時の引継ぎ期間などについても考慮が必要である．ITロールは，システム上で付与すべき権限の集合体として定義する．たとえば，あるITロールにはファイルサーバの読み取り権限とOracleデータベースの表やビューを検索する権限を付与し，そのITロールと利用者のIDの紐付けを行う．これは，個々のIDに対してそれぞれのシステム権限を付与し管理するのではなく，ロールベースでの管理を行うための定義である．アプリケーションロールは，ITロールでは管理しきれないシステム独自の詳細な権限を管理する際のロールである．パッケージソフトによっては詳細な権限をロールという形でまとめる機能を持っているものがあり，これがアプリケーションロールにあたる．以上のロールの大別もまだ検討の余地があるが，ロールによる管理（ロールマネジメント）の考え方は，アクセス権限を安全に効率良く管理するために必要となる．

3.2 IDのライフサイクルとプロビジョニング

ID管理基盤によるIDのライフサイクル管理は，利用者の入社から退社までの間，企業内で発生する組織改変やユーザ属性の更新，IT環境の変更に伴いプロビジョニング機能によりID情報を常に整合性を保ちながら最新に維持し，更新する仕組みである．

組織改編は，半年や一年に一度の大きな改編から日々発生する細かい改編まで，さまざまな規模が考えられる．それらを考慮し追随できるような基盤が必要である．ユーザ属性の更新は，利用者であるユーザの昇進，異動，結婚による姓の変更など，入社から退職までの利用者個人についての情報の変更である．特に，昇進や異動などは利用できるシステムや権限が変わることが考えられる．注意が必要なのは異動による引継ぎ期間の考慮である．引継ぎ期間が終わった後にはシステムの利用やアクセス権限の変更が必ず実施される仕組みを用意する必要がある．IT環境の変更には，前述したようにシステムの追加や更新，バージョンアップなどが考えられる．

プロビジョニング/デプロビジョニング機能については，ID管理ソフトウェア製品により処理方法が異なるので，導入の際には注意が必要である．ある製品は各システムに対してアクションを行う度に接続と切断を繰り返すため，オーバヘッドが大きく配信処理に時間がかかる．ただし，コミット情報を細かく取得しているので，障害時は復旧後すばやく処理を再開できるというメリットがある．一方，別の製品は，システム単位に一括処理でIDを作成し効率よく配信できるが，障害時は処理のロールバックと再実行が必要な場合がある．このようにそれぞれの製品には特徴があり，それらを捉えた上で製品を選択する必要がある．

3.3 パスワードマネジメント機能の実装

パスワードマネジメント機能は，システム利用者とシステム管理者の両方に対してサービスを提供することを考慮する必要がある．機能の要素としては，パスワード変更サービス，パス

ワード変更反映処理，パスワードポリシー制御がある．

3.3.1　パスワード変更サービス

パスワード変更サービスには管理者と利用者の二つの提供対象が存在する．管理者に対しては，利用者のパスワードリセットのための機能を，利用者に対しては，自らのパスワードを変更する機能を提供する必要がある．管理者へ提供するパスワードリセットの機能は，主に利用者のパスワード忘却時に利用するもので，あらかじめ規定された値へ強制的に上書きすることによって利用者が認識可能なパスワードへ変更する機能である．パスワードをリセットする機能は，各システムが持っていると考えられる機能であるが，ここで必要としているのは統合されたリセット機能である．各システムへそれぞれリセットを行うのではシステムを管理する側への運用負荷が高い．ID 管理基盤から集中管理されるパスワード変更サービスにより，利用者が許可されているシステムに対してすべてのパスワードがリセットされる機能が実装されることが望ましい．

一方で，システムの利用者のためのパスワード変更サービスには，パスワードの有効期限による定期的なパスワード変更とパスワード忘却時に自らパスワードをリセットするパスワードリマインダの機能が必要とされる．定期的なパスワード変更については，管理者向けのパスワードリセット機能と同様に集中管理された ID 管理基盤によって，一箇所で変更を行い各システムへ配信される機能が実装されることが望ましい．それによってパスワードを変更し忘れるという人為的ミスを防ぐことができる．パスワードリマインダ機能は，本人しか知りえない情報をあらかじめ複数セットしておき，パスワード忘却時にその情報を利用し本人確認を行い，自らパスワードリセットを行う機能である．たとえば親の出身地や旧姓，ペットの名前，血液型，趣味などを入力する．この機能は，システムの運用者の負荷を軽減させる方法として有効である．ただし，このパスワードリマインダ機能については，利用される環境によってはセキュリティ上効果がない場合があるので導入には注意が必要である．たとえば学校法人では，学生同士で個人的なつながりが強くプライバシー情報をお互いに知っていることが多いからである．

個別のシステムからのパスワード変更機能は停止させることが望ましい．個々のシステムでパスワードを変更できてしまうと，パスワードの不一致が起こり，利用者の混乱を招くからである．また後述するが全体のパスワードのポリシーと異なるパスワードを入力してしまった場合，全体での整合性が取れなくなり，不具合が発生する場合が考えられる．

3.3.2　パスワード変更反映処理

パスワード変更反映処理については，以下の点において注意が必要である．

1)　変更を反映させる順番
2)　失敗した場合のリカバリ方法
3)　どこで（どの処理で）失敗したのか把握する手段

変更を反映させる順番については，処理のスピードなどを検討して決定する必要がある．処理に時間がかかるシステムなどでは，すぐに反応がないためシステムがエラーとして判別してしまい，処理がストップしてしまう可能性もある．リカバリ方法については，再度はじめからパスワード変更処理を行ってパスワードの不整合を解消させるのか，失敗した箇所から処理を

再実施するのかなどの検討が必要になる．また，製品によってはパスワード変更受付だけを行い個々のシステムに対して変更処理が失敗しても利用者には把握できない仕様になっているものもある．これらのことから，処理の順番やそれぞれのシステムからのエラー情報の取得方法などについて考慮が必要となる．

3.3.3　パスワードポリシー

統合対象となるシステムで実装されているパスワードポリシーはそれぞれ異なることが多く，すべてのシステムでパスワードポリシーを揃えることが難しい．無理に揃えたとしても，共通に利用できるポリシーは，文字数制限（何文字以上）などの簡単なものであり，却ってパスワードの強度が落ちてしまうことになる．従って，それぞれのシステムではパスワードポリシーを管理せず，パスワード変更サービスを一箇所で行う仕組みを用意し，その仕組みの中で，入力されたパスワードのポリシーチェックを行うことにより，パスワードの強度を保つ方法が現実的である．

3.4　ワークフローの実装

ワークフローシステムは業務に直結するシステムであり，組織の運営に関わる問題のため，業務コンサルタントのノウハウが必要となる．承認経路の決定や権限委譲のルールなどシステムの視点からだけでは決定できない事項が数多く存在し，顧客側のシステム担当者だけでは決定できないからである．そのため，ワークフローシステムの設計は，他の機能の設計とは分けて進める方法が望ましい．業務コンサルティングを行った上でワークフローシステムが実現できる機能とすり合わせを行い，実装する方法を推奨する．特に現場の視点からのみでフローを検討すると例外フローが著しく増加してしまう．業務効率化の観点から例外フローは極力作成しない決断が必要となる．それは同時に運用負荷の軽減にもつながる．

3.5　シングルサインオンとデバイス認証

シングルサインオンはユーザの利便性を高めることができるが，一度の認証によって複数のシステムにシームレスにアクセスすることが可能になるため，より強固な本人確認の仕組みが必要となる．シングルサインオンの導入により利用者が記憶しておく必要のあるパスワードの数を減らすことができ，利用者のパスワード管理の負荷は低くなる．それにより，パスワードポリシーを厳しくしてセキュリティを保つという方法も考えられるが，利便性とセキュリティの両立という観点からバイオメトリクス認証やICカード認証などのデバイス認証の導入がより効果的である．

3.6　実装におけるプロジェクトの考慮点

統合認証基盤の構築プロジェクトを進めるにあたっては，技術的な側面だけでなく，プロジェクトマネジメントがプロジェクトの成否の重要な要素となる．基盤であるがゆえに関連するシステムの範囲が広く，連携対象の各システム担当者や担当業者での調整に時間がかかるなどの理由により，プロジェクトの意思決定が遅くなっていく傾向がある．プロジェクトを進める上では，経営的な判断と決定ができるエグゼクティブスポンサーをプロジェクトメンバーに参画させることがポイントとなる．

現場においても顧客側の担当者の作業工数などに考慮が必要である．これには統合認証基盤に対応させるシステムを構築した業者の工数も含まれる．統合認証基盤システムは，前述したように他システムとの連携が多いため，顧客側の担当者が他のシステムの担当者および業者と調整する事項も非常に多くなる．

また，移行作業についても注意が必要である．特にパスワードの移行は技術的に不可能な場合が多い．セキュリティの観点から各システムは，不可逆性の暗号化を行った上でパスワードを格納していることがほとんどであり，データベースからパスワードの平文を取得できないことが多い．したがってパスワードの初期化を伴うことを考慮に入れる必要がある．この場合，顧客側では利用者に対し準備期間を設けてアナウンスを行う必要がある．

4.　統合認証基盤に対する今後の取り組み

4.1　統合認証基盤の仮想化

サーバ機器の高性能化により，コンピュータ資源の有効活用の側面からサーバの仮想化が注目されている．機器の性能や容量が上がっていることにより，CPU やメモリの使用率は下がっているものの，一つの OS 上に複数のサービスを動作させた場合，障害発生時の問題切り分けが煩雑になったり，構成変更時の影響範囲が大きくなってしまうなどの問題点が考えられる．そこで仮想化技術により，物理的なレイヤと OS を切り離すことで，コンピュータ資源の有効活用と前述の問題点の解消を図ることができる．

特に統合認証基盤システムは，仮想化技術のデメリットの影響を受けにくいモデルであると考えている．その理由は仮想化を行った際のボトルネックとなりやすい物理的な I/O 部分への負荷が大きくないためである．統合認証基盤の内，ID 管理基盤は高度な即時性を要求されないシステムである．従って一括処理などはシステム的に負荷が低い夜間に行うなどの対応が可能である．個別処理なども秒以下の単位での処理能力を要求されることはきわめて少ない．また，認証基盤に関しては，即時性は要求されるものの処理するデータ量は少ないため，システムの CPU やメモリなどのリソースを長時間占有することがない．そのため統合認証基盤を構成するサーバ群を仮想化プラットホーム上へ構築することにより，システムの集約化が図れる．

4.2　クラウドコンピューティング環境への対応

「所有から利用へ」というコンピュータシステムのパラダイムシフトにより，利用者管理の基盤である統合認証基盤もクラウドコンピューティング環境への対応が迫られている．統合認証基盤のクラウドコンピューティング環境への対応方法としては，大きく二つの方法が考えられる．一つ目は，社内の統合認証基盤からプロビジョニングを行い，サービス提供業者へ ID 情報を配信する方法である．二つ目は，企業/組織内で管理している ID とサービス提供業者の ID に対して，ID を軸に紐付けを行うアイデンティティ・フェデレーションの技術を利用する方法である．

4.2.1　シームレスなプロビジョニング

ID 情報をプロビジョニングする方式のメリットは，社内で運用されている認証基盤システムがダウンした場合でも，クラウド環境上にあるシステムについては継続的に利用が可能であるという点である．一方でデメリットは，ID 情報という個人情報に近い機密性の高いデータ

を世界中で分散されているサーバのデータベースに配信してしまうことである．また，利用者の利便性を維持するためには，サービス提供業者が用意する認証画面に対して自動的に認証を行う仕組み（パスワード代行入力機能など）を別途用意する必要などが発生する．

4.2.2　アイデンティティ・フェデレーション機能による連携

最小限（ID のみで済むなど）の ID 情報をサービス提供業者へ渡すだけで良く，セキュリティを保った上で利用者の利便性を高められる．企業/組織内で管理している ID とサービス提供業者の ID との間でランダムな値を仲介させ，ID を直接紐付けないため，プライバシーを考慮した連携が可能になる．XML 関連の標準化団体 OASIS（Organization for the Advancement of Structured Information Standards）が策定している SAML（Security Assertion Markup Language）準拠の製品や OpenID Foundation の OpenID，マイクロソフト社の CardSpace などの方式が挙げられる．細かい仕様はそれぞれ異なるが，共通しているのは，認証情報を格納する認証用データベースを企業とサービス提供業者で互いに同期して保持する必要がないという点である．サービス提供業者がどの仕様に対応しているかによって，実装する方式を選択する必要があるが，サービスを相互に乗り入れる動きもあり，今後の動向に注目したい．

5. お　わ　り　に

本稿では，主に技術的な視点から統合認証基盤について述べたが，機会があれば，3.6 節「実装におけるプロジェクトの考慮点」で触れたように，技術だけでは解決できない側面に対してのノウハウについてもまとめていきたいと考えている．また，技術的側面においてはロールマネジメント機能が注目を集めており，ID 管理システムを販売している各社から次々とロールマネジメント製品がリリースされている．既存の ID 管理システムでは不足しているロールの管理機能をより強化するためである．統合認証基盤を充実させる新しいソリューションとして，ロールマネジメントについても取り組んでいく必要があると考えている．

最後に，執筆にあたり技術的な相談に乗っていただいたプロジェクト/グループのメンバー，市場調査や資料収集にご協力頂いた商品企画室及びセキュリティビジネス推進部の方々にこの場をお借りしてお礼を申し上げたい．

＊ 1　2007 年 7 月 31 日に公表された「金融商品取引法に関する政令・内閣府令等」を含む金融商品取引法が施行された日（2007 年 9 月 30 日）を施行日として記述している．

＊ 2　「統合型アプライアンス」「ネットワーク脅威対策製品」「コンテンツセキュリティ対策製品」「アイデンティティ・アクセス管理製品」「システムセキュリティ管理製品」「暗号製品」の 6 カテゴリー（大分類）に分類されている．

＊ 3　RADIUS（Remote Authentication Dial In User Service）は元々ダイヤルアップ・インターネット接続サービス向けに認証と利用事実の記録（アカウンティング）を目的に開発されたプロトコル．常時接続方式のインターネット接続サービス，無線 LAN，VLAN などのネットワークサービス向けにも幅広く利用されている．また，RADIUS プロトコルに対応した認証サーバを RADIUS サーバと呼ぶ．

＊ 4　RADIUS のアカウンティングログはセッションの開始時だけでなく終了時にも記録され，セッション中に使用されたリソースの量（時間，パケット，バイトなど）も含め詳細なログを残すことができる．

＊ 5　Personal Identification Number の頭文字．日本語では暗証番号と訳されるが数字だけでなく英字や記号も利用可能な場合が多い．

参考文献　［1］「内部統制におけるアイデンティティ管理解説書 第2版」，日本ネットワークセキュリティ協会，2009年6月
［2］「平成20年度 情報セキュリティ市場調査報告書」，日本ネットワークセキュリティ協会，2009年3月
［3］「2009ネットワークセキュリティビジネス調査総覧（上巻）」，株式会社富士キメラ総研，2009年7月，P17
［4］「導入前に知っておきたいバイオメトリクス認証」，アットマーク・アイティ，2003年11月，http://www.atmarkit.co.jp/fsecurity/special/44biomet/biometrics01.html（上記URL確認：2009年11月5日）

執筆者紹介　大　竹　章　裕（Akihiro Otake）
2000年㈱ネットマークス入社．指紋認証やICカード認証を統合管理するマルチデバイス認証ソリューション，ID管理ソリューションなどの企画，設計，構築業務に従事．その後，情報セキュリティのコンサルタント，ITアーキテクトとして活動．現在，統合認証基盤を中心としたセキュリティソリューションの構築を行うDC技術統括部に所属．JNSA標準化部会IDMワーキンググループなどで活動．CISSP．