企業向け多要素認証プラットフォームの設計

八木 哲志（NTT コミュニケーションズ株式会社）
山田 慈朗（NTT コミュニケーションズ株式会社）
上野 磯生（NTT コミュニケーションズ株式会社）
高杉 英利（NTT コミュニケーションズ株式会社）

概要　企業向けの認証サービスを対象とし，多彩な認証レベルを提供する多要素認証機能と多数の Web サイトへのログインを容易にする認証連携機能を実現する多要素認証プラットフォームを開発した．ここでは，その機能概要を報告する．本プラットフォームでは，個人，端末，回線を特定する認証方式において低コストで利用しやすいさまざまな認証方式を実装し，これらの認証方式の組み合わせにより，基本的な認証レベルから，強固な認証レベルまで，低コストに実現した．また，この認証方式の組み合わせは企業の管理者自身の操作によって，自由に設定可能とした．これにより企業のセキュリティポリシーに応じた様々な認証レベルを提供する柔軟性と，簡単かつ迅速に変更できる即応性を実現している．また，認証系のシステムにおいて重要となる，セキュリティ脆弱性対策の考え方についても述べる．

1. はじめに

企業向けのクラウドコンピューティングや SaaS(Software as a Service)の普及に伴い，さまざまなサービスを利用する際に認証を必要とする Web サイトが増加している．現在，その認証には，ユーザ ID とパスワードの組み合わせによる認証（パスワード認証）が広く用いられている．しかしながら，顧客情報や金融情報のようにセキュリティ上重要な情報を取り扱うサービスにおいては, パスワード認証のみによる認証方式ではなく，複数の認証方式を組み合わせることが推奨されている[1]-[3]. 例えば, 企業向け SaaS である Google Apps では，パスワード認証に加えて，電話を用いた確認コードによる認証も実施するように設定可能となっており，複数の認証方式を組み合わせることにより，認証の強度を確保している．このように，多要素認証導入の必要性が一段と高まってきている．

他方，多くの Web サイトから個別に認証を求められることになると, 多数の ID やパスワードが必要となる．それらの管理が煩雑となるため，結果的に各ユーザが ID およびパスワードの一覧をメモに記載しておいたり，複数の Web サイトのパスワードを同一のものに設定する等，ID およびパスワードが漏洩・流出するリスクが高まることとなる．また，各 Web サイトにログインする度に，それぞれの ID およびパスワードを入力することになり，ユーザにとっては不便でもある．上記を解決するための技術として，認証連携（シングルサインオン）技術があるが， ID およびパスワードが漏洩したときに複数のサイトに侵入されてしまうことから，シングルサインオンを安全に利用するためには通常用いられる認証レベルよりも強固な認証を採用することが必要不可欠である．

そこで筆者らは, 企業向けの認証サービスを対象とし，多段階の認証レベルを提供する多要素認証機能と多数の Web サイトへのログインを容易にする認証連携機能を実現する多要素認証プラットフォームを開発した[4]．これまでに多要素認証に関する検討が行われ[5][6], 関連するソフトウェアが開発されてきたが[7]-[12]，強固な認証レベルを得るために，生体認証やワンタイムパスワードトークン等のように専用機器が必要となる認証方式を基本としており，コストが高くなってしまう．また，多要素認証の設定を柔軟に変更ができないことが多く，様々なニーズに応えることが難しい．

そこで，本プラットフォームは，低コストで利用しやすいさまざまな認証方式を実装し，これらの認証方式の組み合わせにより，基本的な認証レベルから，強固な認証レベルまで，低コストに実現した．また，この認証方式の組み合わせは企業の管理者自身の操作によって，自由に設定可能とした．これにより企業のセキュリティポリシーに応じた様々な認証レベルを実現する柔軟性と，簡単かつ迅速に変更できる即応性を実現している．

本稿では，まず，第 2 章で多要素認証に関する従来技術における課題と対策を説明する．第 3 章では多要素認証プラットフォームで必要となる機能を整理し，要件を明らかにする．第 4 章では，提案する多要素認証プラットフォームの設計内容について示し，第 5 章で認証系のシステムにおいて重要となる，セキュリティ脆弱性に対する対策の考え方を示す．最後に，第 6 章でまとめと今

後に向けた課題を示す.

2. 従来技術の課題と解決手段

2.1 従来技術の課題

多要素認証関連の検討としては, [5][6]等が挙げられる. [5][6]は，生体認証を利用した多要素認証方式であり，専用の機器が必要となり，ある程度のコストがかかり，手軽に利用することは難しい．多要素認証機能およびシングルサインオン機能を実現するソフトウェアとしては，[7]-[12]等が挙げられる．これらのソフトウェアにおいても，前述の通り，複数の認証方式を組み合わせたり，専用の機器が必要となる等,認証には高いコストを要する．また，多要素認証の組み合わせを決めて認証の設定を行った後に，セキュリティポリシーの見直し等により他の認証方式に変更したい場合でも，設定変更作業には時間を要し，すぐには変更できない．さらに，多要素認証の組み合わせる場合，通常は指定された認証方式すべてが認証成功とならなければ認証が成功したとはならず，この点において柔軟な認証設定が必要となる.

2.2 課題の解決手段

上記の課題を解決する手段として，認証に要するコスト高については，個人・端末・回線を特定する認証に，低コストで利用しやすい認証方式を多数用意し，それらを組み合わせることにより，安価かつ強固な，利便性の高い多要素認証を実現する．認証方式の組み合わせの設定変更の迅速化と柔軟な認証設定方法については，企業毎に認証方式の組み合わせ条件を，論理積(AND)だけでなく，論理和(OR)を用いて記述する認証条件式を設定・変更できるようにすることで，即応性と柔軟性を実現する.

3. 企業向け多要素認証プラットフォームにおける要件

3.1 企業向け認証サービスの要件

企業向けに認証サービスを提供する場合に想定した主な要件を以下に列挙する.

・企業の社内ネットワーク環境および社外のリモート環境から，企業の社内システムおよびインターネット上の社外システムへのアクセス時にシングルサインオンを利用でき，認証時には多要素認証を利用できること.

・企業の管理者が認証条件を簡単かつ迅速に変更できること.

・アクセスする企業，アクセス元，Web アプリケーションの組み合わせ毎に認証条件を柔軟に変更できること.

3.2 多要素認証機能の要件

3.2.1 認証方式の分類

認証方式を分類する場合，一般的には，認証に利用する情報に基づき，記憶情報による認証，生体情報による認証，所有物情報による認証の３種類に分類することが多い．しかしながら，Web アプリケーションの認証は通常，ネットワーク経由で行うものであり，回線情報を比較的容易に入手でき，利便性の高い認証が実現できる．そのため，ここでは回線情報による認証も分類に加えることを検討した.

また,認証方式の組み合わせを考える場合には,個人,利用端末および利用回線の識別など，識別対象も重要となり，この対象も分類も加えている．例えば，ユーザを認証するためには，認証方式の組み合わせの中に個人を識別する認証方式が必須である．また，個人・端末・回線を識別する認証方式を組み合わせることで，利便性を維持しつつ，高いセキュリティを実現できる．このように，認証方式の組み合わせを考える際に識別対象による分類は有用となる.各分類に対する認証方式の例も含め，表 1 としてまとめた.

なお，認証方式の例として記載した携帯電話認証については，回線としての分類することも有り得る．しかしながら，本検討では，例えば，盗難・紛失するといった場合があるように，所有物としての側面を重視し，ここでは所有物として分類することとする.

表 1 認証方式の分類

識別対象による分類	利用情報による分類	認証方式の例
個人	記憶	パスワード認証 マトリクス認証
	生体	指紋・静脈認証、虹彩認証 顔認証、音声認証
	所有物	ICカード認証 ワンタイムパスワード認証
端末		機器認証 携帯電話認証
回線	回線	送信元IPアドレス認証 NGN回線認証

3.2.2 機能要件

多要素認証機能の主な要件を以下に列挙する.

要件 1 個人・端末・回線を特定する認証には，低コス

トで利用しやすい認証方式を複数用意すること．

要件 2 企業および Web アプリケーションの組み合わせには，多要素認証の組み合わせ条件を論理積(AND)と論理和(OR)を用いて記述する認証条件式の形で容易に設定・変更できること．

要件 3 アクセス元となる場所に対する認証条件の変更には，回線を認証することによりアクセス場所を特定できるため，認証条件式に回線認証を含めることで実現すること．

要件 4 端末の環境によっては利用できない認証方式が存在するケースが考えられるため，そのような認証方式を実施せず，認証失敗とし，その認証処理をスキップさせる機能を備えること．

要件 5 今後，新たな認証方式を開発した場合に，その方式を容易に追加できるようにするためのインタフェースを用意すること．

3.3 認証連携機能の要件

3.3.1 認証連携方式の分類

シングルサインオン方式は，エージェント型とリバースプロキシ型の２種類に分類することができる[13]．図 1 に示すとおり，エージェント型はサービスを提供する SP(Service Provider)側にエージェントソフトウェアを配置することにより，シングルサインオンを実現するものである．他方，リバースプロキシ型では，各 SP にアクセスする場合はリバースプロキシと呼ばれるサーバを必ず経由するようにしてシングルサインオンを実現するものである．エージェント型は各 SP へエージェントソフトウェアの導入やアプリケーションの改修が必要となることがデメリットであるが，アクセスの負荷は比較的分散しやすいというメリットがある．リバースプロキシ型はリバースプロキシサーバへの負荷が集中することがデメリットであり，各 SP ではエージェントソフトウェアの導入が不要で基本的にはアプリケーションの改修も不要であることがメリットである．

3.3.2 機能要件

認証連携機能の主な要件を以下に示す．

要件 6 アクセスの負荷集中を防ぐことを重視し，今回はエージェント型を開発の対象とすること．エージェント型とリバースプロキシ型には，それぞれ一長一短があるが，筆者らが検討する多要素認証プラットフォームは数百のオーダーの SP と，数百万のオーダーの同時ログインユーザに対するシングルサインオンを提供するプラットフォームを想定しており，また，それらの SP の中には，認証処理によるトラフィックと比較して支配的なトラフィックを発生させる動画ストリーミング再生のようなサービスも含まれる可能性もあることから，認証に関係するトラフィックのみを処理すればよいエージェント型が適切であると考えたためである．

要件 7 企業の社内ネットワーク環境および社外のリモート環境から，企業の社内システム，およびインターネット上の社外システムへのアクセス時にシングルサインオンを利用できること．

要件 8 シングルサインオン方式は１つに限定せず，用途に応じて幅広く対応できるように，複数のシングルサ

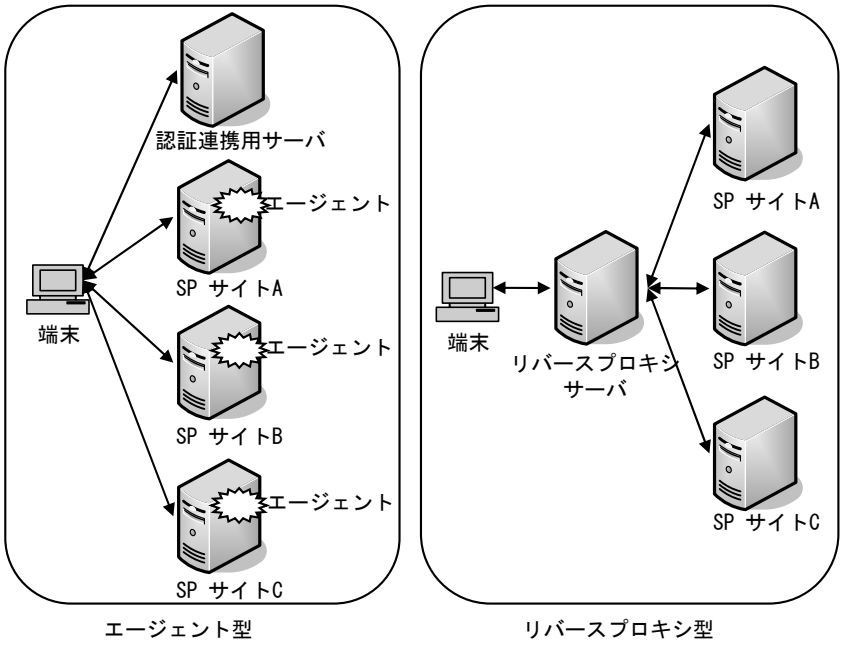

図 1 認証連携（シングルサインオン）方式の分類

インオン方式を実装すること.

要件 9 各 SP の認証条件式が異なる場合，実施済の認証方式はスキップし，未実施の認証方式のみ実施すること.

3.4 ID 管理機能の要件

多要素認証機能や認証連携機能を利用する上で必要となる ID 管理機能に関する主な機能要件を以下に示す.

要件 10 企業等のグループ情報やユーザ情報を管理できること.

要件 11 認証やシングルサインオンに必要な情報を管理できること.

要件 12 企業の管理者や一般ユーザ等の権限管理ができること.

4. 多要素認証プラットフォームの設計

第 3 章にて示した多要素認証機能，認証連携機能，ID 管理機能に関する要件にそれぞれ対応するモジュールとして，多要素認証エンジン，SSO (Single Sign On)マネージャ，ID マネージャの 3 つのモジュールを実装する．図 2 に開発した多要素認証プラットフォームの構成を示す.

4.1 多要素認証エンジン（多要素認証機能）

多要素認証エンジンモジュールは，複数の認証方式を組み合わせた認証を実現するものであり,現時点では 10 種類の認証方式に対応している.

本機能の主な仕様を以下に示す.

·SP から要求された認証要求を契機として，ユーザに関する認証を行ない，その結果を認証応答として SP へ返信する.

·表 2 に示すとおり，個人を特定する認証方式として 4 種類，端末を特定する認証方式として 4 種類，回線を特定する認証方式として2種類の計10種類の認証方式が利用可能である．そのほとんどの認証方式は専用装置が不要であり,低コストで利用しやすい認証方式である(**要件 1**)．人を特定する認証方式については，ほとんどの認証システムで利用されているパスワード認証に加えて,一種のワンタイムパスワード認証と解釈できるマトリクス認証とメールチャネル認証，およびカードの盗難や紛失のリスクを除外すれば強固なセキュリティを実現できる IC カード認証を実装した.端末を特定する認証方式としては，強固な認証レベルを実現する証明書ベースの機器認証，簡易な認証である MAC アドレスベースの機器認証，それらの中間的な認証レベルであるクッキーを用いた機器認証と，携帯電話用の認証方式を実装した．回線を特定する認証方式としては,適用範囲が広い IP アドレスベースの認証と,NGN 回線での強固なセキュリティ

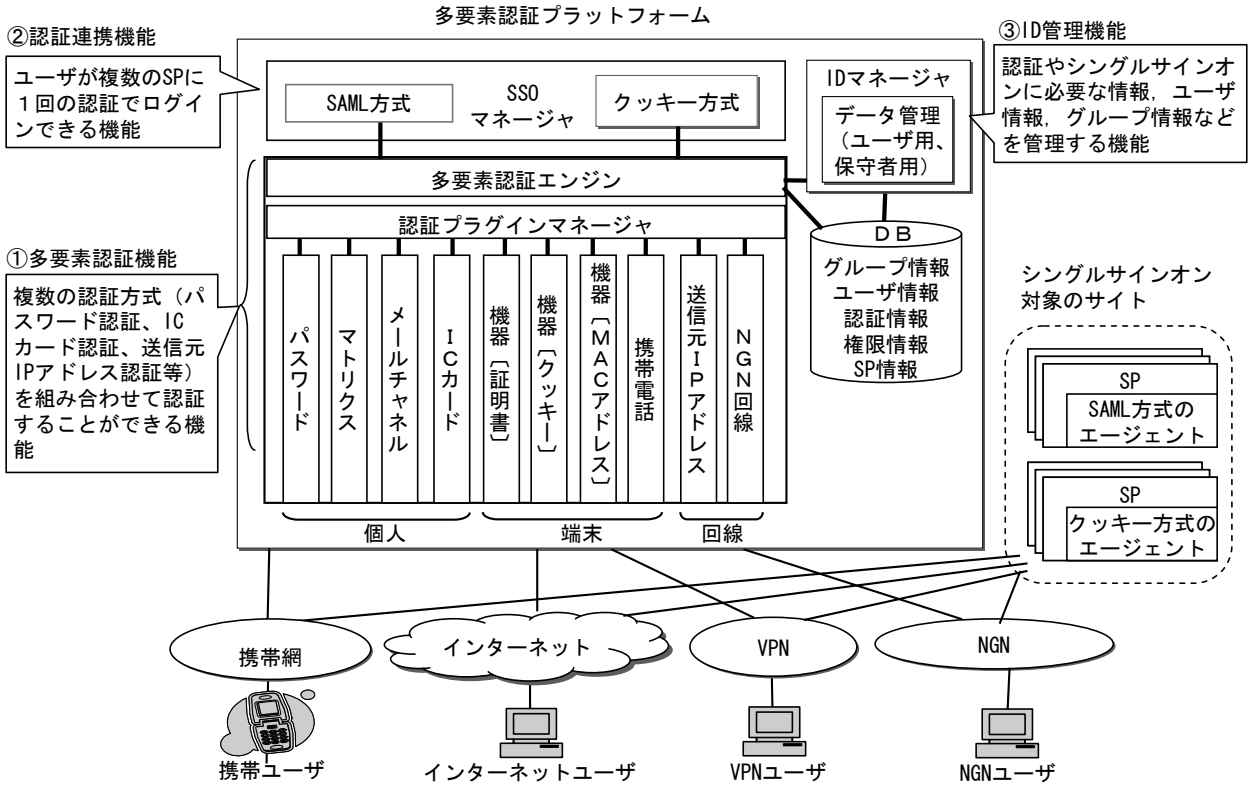

図 2 多要素認証プラットフォームの構成

表 2 多要素認証プラットフォームで利用可能な認証方式

識別対象	利用情報	認証方式	説明
個人	記憶	①パスワード認証	IDとパスワードによる認証
		②マトリクス認証	乱数表内の指定位置の乱数を入力することによる認証
	所有物	③メールチャネル認証	メールで別途送付されるワンタイムパスワードを入力することによる認証
		④ICカード認証	ICカード内の証明書情報に基づいた認証
端末		⑤機器認証（証明書）	端末内の証明書情報に基づいた認証
		⑥機器認証（クッキー）	端末内のクッキー情報に基づいた認証
		⑦機器認証（MACアドレス）	端末のMACアドレスに基づいた認証
		⑧携帯電話認証	携帯電話のID情報に基づいた認証
回線	回線	⑨送信元IPアドレス認証	端末の送信元IPアドレスに基づいた認証
		⑩NGN回線認証	NGNの回線IDに基づいた認証

を実現できる NGN 回線認証を実装した．生体認証およびワンタイムパスワードトークンによる認証については専用装置が必要になる等，手軽に利用することが難しいため，今回は実装していない．

・認証サービスを利用する企業の管理者は，SP が提供するサービス毎に認証条件式を割り当てることができる（**要件 2**）．SP が複数のサービスを提供する場合，それぞれ異なる認証条件式を設定できる．例えば，図 3 に示すように，○○SP が情報を参照するだけのサービスと更新も行うサービスを提供していたとき，通常参照よりも更新の方が重要な処理であるため，□□企業では参照サービスにはパスワード認証だけでよいが，更新サービスはパスワード認証に加え，IC カード認証も必要というように認証条件式を設定できる．

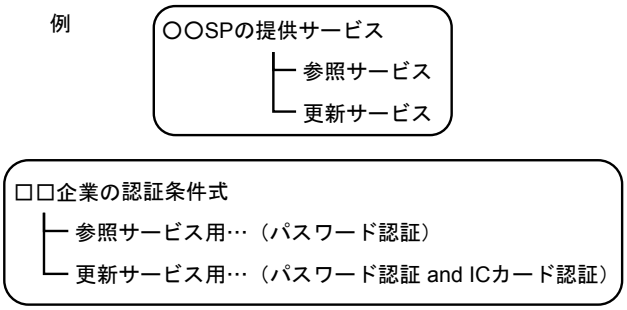

図 3 SP の提供サービスと企業の認証条件式

・認証条件式に論理積(AND) とともに論理和(OR)を導入することにより，ユーザの利用環境に合わせて容易に認証条件を切り替えることができる（**要件 2**）．

指定された IP アドレスの端末からは パスワード認証のみ実施するが，それ以外の端末では IC カード認証も実施する場合の例を図 4 に示す．

この例のように，企業内のイントラネット上の端末からアクセスする場合と，外部のインターネット上の端末からアクセスする場合で，認証レベルを変えることが可能である（**要件 3**）．

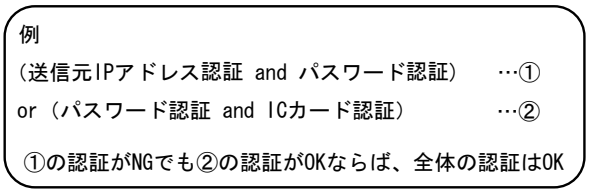

図 4 認証の組み合わせ設定例について

・ユーザの利用環境によっては認証条件式の中に利用できない認証方式が含まれる．例えば， IC カード認証が認証条件式に含まれているがユーザが利用する端末に IC カードリーダが設置されていない場合等である．このような場合が想定されるため，その認証時にはユーザが画面からスキップを指定し，次の認証方式に処理を進めることが可能である．（**要件 4**）．また，図 5 のような認証式で IC カード認証をユーザがスキップした場合, IC カード認証と論理積(AND)で結合されたパスワード認証は成功しても全体の認証に影響がないため，パスワード認証も自動的にスキップされ，次はメールチャネル認証の処理が実施される．

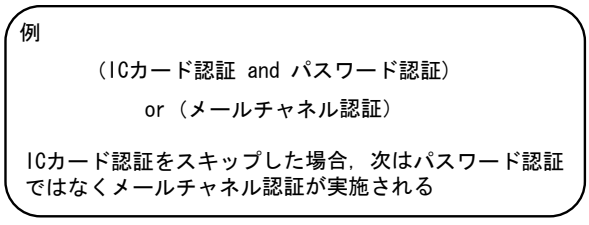

図 5 認証スキップ

・認証プラグインマネージャは，認証方式関連のインタフェースを共通化し，作成した各認証方式のモジュールをプラグインとして管理する．認証方式をプラグイン化することで, 今後, 新たな認証方式を追加する場合に, その方式を容易に組み込むことができるアーキテクチャとした（**要件 5**）．

4.2 SSO マネージャ（認証連携機能）

SSO マネージャモジュールは，複数の SP を一度の認証でログインできるようにするシングルサインオン機能を実現するものである. シングルサインオン方式として，エージェント型によるシングルサインオンを実装し（**要件 6**），エージェント型の中でも，企業内イントラネット向けとインターネット向けを想定した上で，以下の２つの方式に対応している（**要件 7**）.

・SAML 方式

SAML(Security Assertion Markup Language)は, 認証情報や属性情報等を Web アプリケーション間で安全に交換するために XML 関連の標準化団体である OASIS によって策定されたプロトコルである[14]. 強固なセキュリティを目指して設計されており，企業がインターネット上の Web アプリケーションを利用する場合に適している. SAML 方式を実現するミドルウェアとして，本プラットフォームでは，NTT ソフトウェア社の TrustBind/Federation Manager[15]を利用している.

・クッキー方式

認証成功後に発行される認証チケットを格納したクッキーの情報を用いて，シングルサインオンを実現する方式である. SP 側ではエージェントソフトウェアを導入し，Web アプリケーションではクッキーから認証チケット情報を読み出す処理を追加するだけでよいため，既存アプリケーションに対して比較的少ない修正を加えるだけで実現可能なシングルサインオン方式である．また，発行した認証チケットの有効期限内においては，認証プラットフォームに負荷をかけることなく，何度でもサービスへのログインが可能である．企業がイントラネット内の Web アプリケーションを利用する場合には，クッキー方式が適している．クッキー方式を実現するミドルウェアとして，本プラットフォームでは，NTT データ社の VANADIS SSO[16]を利用している.

認証連携機能の主な仕様は以下の通りである.

・シングルサインオン方式として，SAML 方式およびクッキー方式を利用できる（**要件 8**）.

・SAML 方式とクッキー方式が混在した複数の SP に対しても相互にシングルサインオンを可能とする（図 6 参照）.

・各 SP の認証条件式が異なる場合，実施済の認証方式はスキップし，未実施の認証方式のみ実施する（**要件 9**. 図 6 参照）.

4.3 ID マネージャ（ID 管理機能）

本プラットフォームは, SaaS での利用を想定しており，複数のユーザ企業（グループ）が本プラットフォームを利用し，それぞれが複数の SP のサービスを利用する形態を想定している.

ID マネージャモジュールでは，SP の登録・削除，グループの登録・削除，ユーザの登録・削除と，グループ毎に利用可能な認証方式，グループ毎に利用できる SP

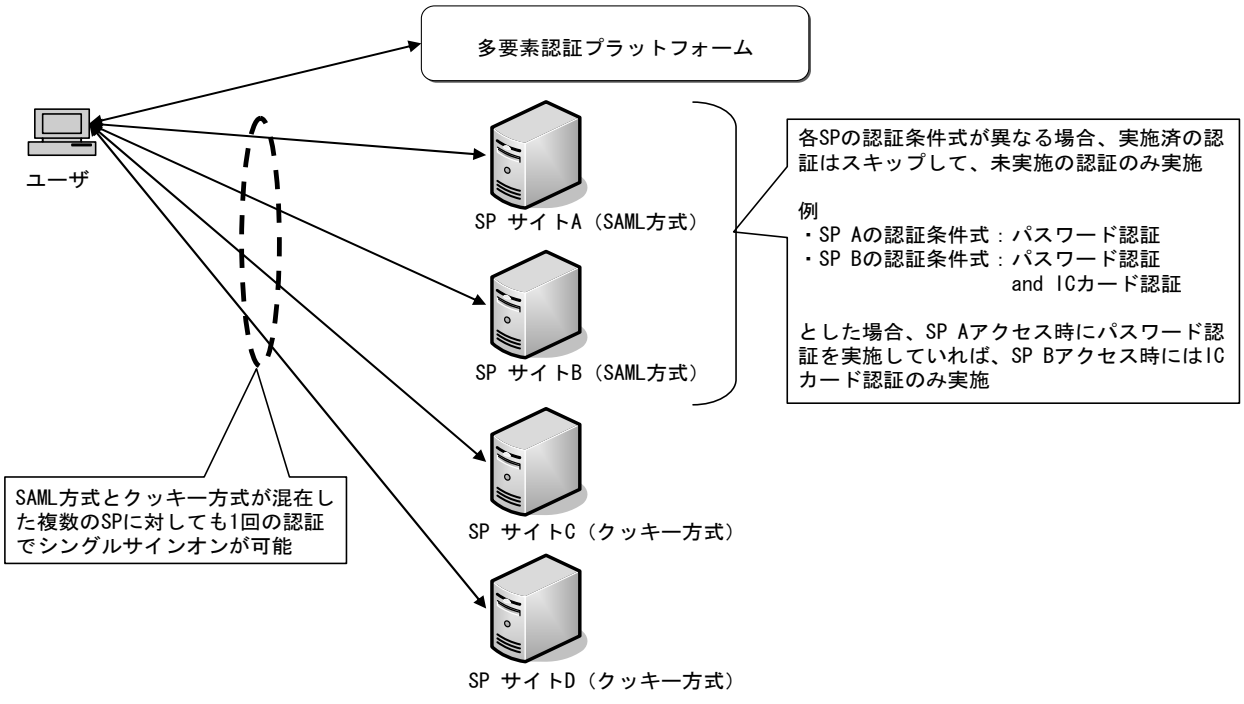

図 6 認証連携（シングルサインオン）機能について

とその認証条件式，グループに所属するユーザ，ユーザが利用できる SP, ユーザ毎の認証情報等の管理を実施する．

本機能の主な仕様は以下の通りである．

・利用者権限（システム管理者，グループ管理者，一般ユーザ等）により，利用できる機能を制限することができ，権限の付与，削除ができる（**要件 12**）．

・SP 情報（SP の識別番号，SP 名，シングルサインオン方式種別等）の登録，削除ができる（**要件 11**）．

・グループ情報（グループ ID，グループ名，利用可能 ID 上限数，利用可能な認証方式，利用可能な SP，認証条件式等）の登録，変更，削除ができる（**要件 10,11**）．

・ユーザ情報（ユーザ ID，氏名，所属，認証情報，SP 側のユーザ ID 等）の登録，変更，削除ができる（**要件 10,11**）．

4.4 多要素認証プラットフォームの特徴

本プラットフォームの特徴を，以下に示す．

・個人・端末・回線を特定する認証方式について，低コストで利用しやすい認証方式を多数用意し，それらを組み合わせることにより，安価かつ強固な，利便性が高い多要素認証を実現できる．

・認証サービスを利用する企業の管理者が認証方式の組み合わせを柔軟かつ迅速に設定・変更できる．

・2 種類のシングルサインオン方式に対応しており，双方においてシングルサインオンができる．

・サービス提供事業者である SP(Service Provider)は認証機能を開発する必要がなく, セキュリティリスクと SP 側の構築コストを削減できる．またプラットフォーム自体の設計には直接関わらないが，SAML の理解や実装は比較的難しいため，簡易に SP に認証機能を組み込むためのライブラリやドキュメントも用意した．また，組み込み機器のようなリソースに余裕の少ない環境での適用も事例としてあったため，当プラットフォームにおける SAML のプロトコルの個々のパラメータレベルでのインタフェース仕様書も用意することにより，ライブラリを用いずに必要最低限かつ十分な SP 側実装を可能とした．

5. セキュリティ脆弱性対策

本プラットフォームは，セキュリティの要となる認証機能を提供するものであり，他のシステムと比較して強固なセキュリティが要求されるため，徹底的に脆弱性対策を実施することが重要である．そのため，プログラム開発に対しては, IPA（独立行政法人 情報処理推進機構）のガイドライン[17]に記載の対策を講じるとともに，外部の脆弱性検査機関 3 社に本プラットフォームの脆弱性検査を依頼した．すべての脆弱性を検出できる検査会社は，現時点では存在せず，複数の検査会社において検査することにより，脆弱性の検出漏れを一掃するよう努めた．また，検出された脆弱性については，すべての対策を早急に講じることが理想ではあるが，改修期間や改修コストの関係で即座に実施できない項目も存在する．そこで，検査会社内におけるセキュリティの有識者と協議した上で，下記(A)～(D)に脆弱性を分類し，(A)については対策を確実に実施し，(C),(D)については優先順位をつけて対策を実施した．

(A) セキュリティリスクが大きく，緊急で対応が必要なもの

(B) 本プラットフォームを利用する環境下では脆弱性を攻撃できないか，または攻撃しても何らかの手段で防御できるため，対策の必要がないもの

(C) 暫定的に運用対処で回避できるもの

(D) その他のもの

6. おわりに

企業向けの認証サービスをターゲットとし，各企業のイントラネット内の社内システムやインターネット上の Web アプリケーションを利用する場合に，多段階の認証レベルを提供する多要素認証機能と多数の Web アプリケーションへのログインを容易にする認証連携機能を実現する多要素認証プラットフォームを開発した．

本プラットフォームでは，個人，端末，回線を特定する認証方式において低コストで利用しやすいさまざまな認証方式を実装し，これらの認証方式の組み合わせにより，基本的な認証レベルから，強固な認証レベルまで，低コストに実現した．また，この認証方式の組み合わせは企業の管理者自身の操作によって，自由に設定可能とした．これにより企業のセキュリティポリシーに応じた様々な認証レベルを提供する柔軟性と，簡単かつ迅速に変更できる即応性を実現している．また，認証系のシステムにおいて重要となるセキュリティ脆弱性対策の考え方を明らかにした．

今後の課題としては, スマートフォンやタブレット PC 等の新たな端末向けの認証機能の拡充や既存システムの認証機能との連携機能の実現，多要素認証利用時の認証方式の組み合わせを選ぶための評価方法[18][19]の確立等がある．また当プラットフォームを実用した結果，特に多要素認証機能について，Web システム以外でも用い

たいという要望がサービス開発者より複数挙がったため，その実現にも取り組んでいきたい．

参考文献

1) FFIEC, “Authentication in an Internet Banking Environment,” Oct. 2005.
2) PCI Security Standards Council, “Payment Card Industry （PCI） データセキュリティ基準 要件とセキュリティ評価手順 バージョン 2.0,” Oct. 2010.
3) 情報セキュリティ政策会議, “政府機関の情報セキュリティ対策のための統一基準(第 4 版),” Feb. 2009.
4) 山田慈朗，八木哲志，上野磯生，北川 毅，高杉 英利，“認証連携機能を兼ね備えた多要素認証プラットフォームの開発,” 信学技報, ICSS2010-52, pp.47-52, Nov. 2010.
5) Bhargav-Spantzel, A., Squicciarini, A., Bertino, E., "Privacy Preserving Multi-Factor Authentication with Biometrics", DIM'06, Nov. 2006.
6) Davar PISHVA, "Spectroscopically Enhanced Method and System for Multi-Factor Biometric Authentication," IEICE TRANS. on Inf. and Syst., Vol.E91-D, No.5, pp.1369-1379, May 2008.
7) IceWall SSO および EVE MA, http://h50146.www5.hp.com/products/software/security/icewall/sso/solution/eve_ma.html.
8) IdentityGuard, http://japan.entrust.com/products/identityguard/index.html.
9) GetAccess, http://japan.entrust.com/products/getaccess/index.html.
10) SecuMAP, http://www.secugen.co.jp/special/index.html.
11) NC7000-3A, http://www.nec.co.jp/netsoft/nc7000-3a/.
12) OepnAM, http://www.osstech.co.jp/product/openam.
13) 松永功,“アイデンティティ管理の実現に関する一考察,” INTEC TECHNICAL JOURNAL, no.2, pp.58-63, Oct. 2003.
14) OASIS, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,” 2005.
15) TrustBind/Federation Manager, http://www.ntts.co.jp/products/trustbind/index.html.
16) VANADIS SSO, http://bs.nttdata.co.jp/vim/relativesol/.
17) IPA, “安全なウェブサイトの作り方 改訂第 5 版,” April 2011.
18) 山田慈朗，八木哲志，上野磯生，北川 毅，高杉 英利，“多要素認証プラットフォームにおける認証技術組み合わせの評価方法について,” 情報処理学会研究報告, Vol.2010-CSEC-51, No.11, pp.1-5, Dec. 2010.
19) 上野磯生，八木哲志，山田慈朗，北川 毅，高杉 英利，“生体認証を含めた多要素認証の評価方法,” 信学技報, NS2010-142, pp.1-6, Jan. 2011.

八木 哲志（非会員）
2002 年早稲田大学大学院理工学研究科修了．同年日本電信電話（株）入社．以来，RFID，認証，認可等のプラットフォーム技術に関する研究開発に従事．現在，NTT コミュニケーションズ（株）にて，認証系システム開発に従事．

山田 慈朗（非会員）
1988 年北海道大学大学院工学研究科修了．同年日本電信電話（株）入社．以来，通信ネットワークの制御法，設計法，評価法の研究開発に従事．現在，NTT コミュニケーションズ（株）にて，認証系システム開発に従事．電子情報通信学会会員．

上野 磯生（非会員）
1992 年神戸大学大学院理学研究科修了．同年日本電信電話（株）入社．以来，分散協調処理に関する研究開発，Web ホスティングに関する基盤開発，およびその運用保守等を経て，現在，NTT コミュニケーションズ（株）にて，認証系システム開発に従事．

高杉 英利（非会員）
1987 年筑波大学大学院理工学研究科修了．同年日本電信電話（株）入社．以来，FTTH 関連アーキテクチャの開発，NTT 西日本（株）及び（株）NTT ネオメイトにて IP 技術者育成，113，116 等始めとするクラウド型 IP コールセンタシステムの開発，インキュベーションに従事．現在，NTT コミュニケーションズ（株）認証・セキュリティプロジェクト部長．博士（工学）・技術士（電気・電子）．

投稿受付：2011 年 7 月 30 日
採録決定：2011 年 12 月 6 日
編集担当：西 直樹（日本電気）