社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－GN－64（8）
2007／6／1

FACE技術と認証サービスの提案

斉藤典明、山崎哲朗、知加良盛、小林透、金井敦
NTT 情報流通プラットフォーム研究所
〒239-0847 神奈川県横須賀市光の丘1-1

様々な社会サービスがネットワーク上で利用可能となると同時にID盗難などの脅威も増加している。そのため、非常に多くのIDを安全に管理する必要性が増加してきている。このような問題を解決するために、ユーザの振る舞いと状況の情報の活用によりユーザを識別・認証する仕組みを実現することによって、ID・パスワードなしにユーザを認証できる新しい認証基盤の研究開発を行っている。その中で、ユーザの振る舞いと状況の情報をIDベース暗号を応用したディジタル証明書の活用によりユーザを識別する方式を検討した。本論文では、この方式の概要と、今回開発したIDベース証明書の発行と高速検証と実現する認証エンジンの概要を述べ、このエンジンを活用したネットワーク上の認証サービスを提案する。

The Fragment Aggregation Certification Method

SAITO Noriaki, YAMAZAKI Tetsuro, CHIKARA Sakae,
KOBAYASHI Toru, KANAI Atsushi
NTT Information-Sharing Labs.
1-1 Hikarinooka Yokosuka-shi, KANAGAWA 239-0847 JAPAN

A lot of threats like a ID theft are increasing though our daily life became convenient by using the Internet, and we will have to manage our many IDs to avoid these threats. To solve such problem, we are developing a new authentication platform which can authenticate users without IDs and passwords by using behavior and situation information of users. In this development, we considered a new approach that users are identified by using a digital certification technology which is an application of the ID-base encryption technology as behavior and situation information of users. In this paper, the outline of our new approach and the prototype certification engine which is developed as a core of our approach are described, then the authentication service on the network based on using this engine is proposed.

1. はじめに

様々な社会サービスがネットワーク上で利用可能となると同時にID盗難などの脅威も増加している現在、多くのネットワーク利用者が、非常に多くのIDを安全に管理することに翻弄されつつある。そこで、IDなしにユーザを識別・認証できる新しい認証基盤が実現できれば、現在のID管理に伴う多くの問題が解決できると仮定している。このIDなしにユーザを識別・認証するための仕組みの一つとして、ユーザの振る舞いと状況の情報を活用することによって実現することを考えている。そのためには、ユーザの振る舞いや状況の情報を確実に記録し第三者に提示できる必要があり、ここでディジタル証明書を活用する。特にここでは、ユーザの振る舞いや状況の情報という散発的に発生する情報をオンデマンドでディジタル証明書化できる仕組みとしてIDベース署名を活用したディジタル証明書による方式を提案し、ディジタル証明書を発行・高速検証するプロトタイプエンジンを開発した。また、ユーザにID不要な認証サービスを提供するためにはこのディジタル証明書を感じさせない（IDやディジタル証明書の管理の負担を感じさせない）ネットワークサービスの仕組みが必要となる。そこで本論文では、この開発したプロトタイプエンジンの

概要と、このエンジンを活用した認証サービスの実現方式を提案する。

2. 研究の背景

ネットワークサービスの生活環境でのかかわりの増加と、ネットワークを利用した盗難犯罪などの脅威の増加により、多くの利用者はネットワーク上の自分自身の識別コードであるIDを複数もち、IDの保護のためのパスワードを管理することのわずらわしさを体験している。ID・パスワード管理のわずらわしさから開放されるためのアプローチとして、現在はシングル・サイン・オン、バイオメトリクス、ICカード、ID管理ツールの利用が考えられる。しかしながら、多くの利用者は、実名性と匿名性を使い分けながら複数の立場や状況に応じて複数のIDを使い分けている。そのため、もし利用している多数のIDを、実名性の高い一つのIDに集約したとすれば、このIDを実名性の必要のないサービスへの利用には抵抗を感じる。そのため、実名性の高い一つのIDへの集約というアプローチには限界があると考えられる。

一方、サービス提供者においても実名性が必要な場合もあるが、実名性までは必要なくユーザ識別において同一性のみが識別できれば良い場合や、サービスを受ける正当な権利者であることが識別できれば良い場合がある。特に個人情報保護法の施行後、サービス提供者はユーザ情報の収集にはユーザの同意が必要があるなどの管理コストがかかるほか、情報漏えい事件に対する大きなリスクを抱えることになる。このため、サービス提供者にとっても、ユーザ情報を取得せずにユーザを識別管理できる方法が開発されることには大きなメリットがある。

そこで、実名性あるいは実名性に近い情報を用いてユーザを識別・認証するのではなく、実名性の低い、匿名性の高い情報を複数使うことによってユーザを識別・認証できる技術を実現することによって、ID不要な認証方式が確立できると仮定しこれまで研究してきた(図1)[1-3]。

このようなユーザの実名性は伏せたまま"ID不要な認証方式"を確立するために、次のように検討してきた(図2)。ユーザがすべてのID一つに統一できない理由の一つは、多くのユーザはIDを立場や役割で使い分けている(多様なアイデンティティ)からであり、ユーザは立場や役割に応じて振る舞いや状況が異なっている。そこで、ユーザの振る舞いやそのときの周囲の状況の情報を知ることによって、その時々のユーザのアイデンティティを識別することができる。そしてこのユーザの振る舞いや周囲の状況の情報によりユーザを特定する技術が必要になり、このユーザの振る舞いや周囲の状況を第三者に提示できる仕組みとして、ディジタル証明書の活用を考えた。ユーザの振る舞いや周囲の状況ごとにディジタル証明書を発行・NW内に蓄積し、必要に応じて組み合わせて活用(第三者提示など)することによってユーザの同一性や、ユーザのアイデンティティを識別できる仕組みの実現を検討してきた。

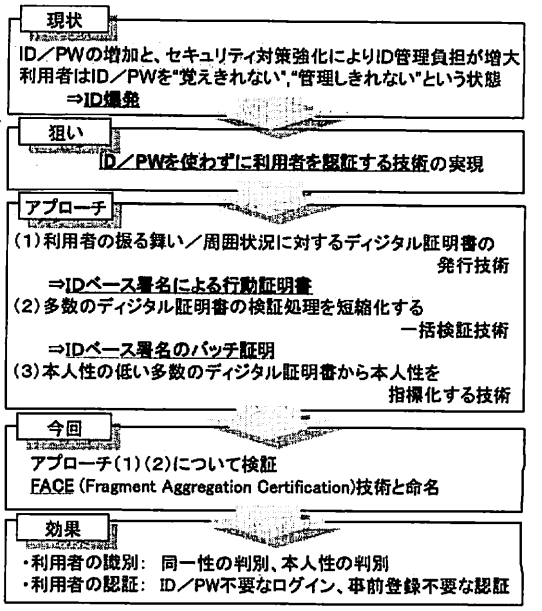

図1. 本研究の位置づけ

この検討の中において、この実名性を隠したままユーザの振る舞いや状況に対してディジタル証明書を発行

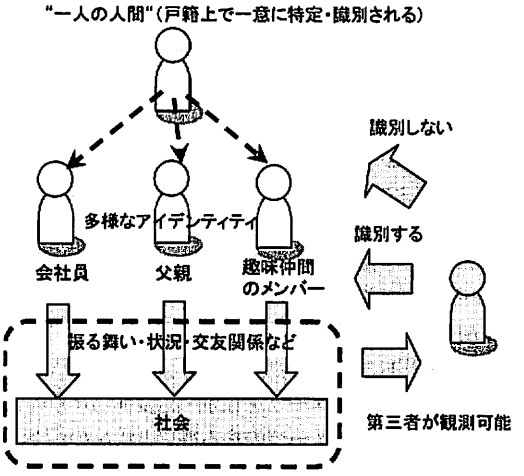

図2. ユーザ識別の考え方

する仕組みとしてIDベース署名(Identity-Based Signature Scheme)の活用を検討してきた。IDベース署名はIDベース暗号(Identity-Based Cryption)[4]によるディジタル証明であり、公開されているIDを公開鍵(可読性のある文字列を公開鍵にできる)とし、これに対応する秘密鍵を後から生成する。現在IDベース暗号のこの特徴が注目されており、PKI (Public Key Infrastructure)が不得意とする領域での活用が期待されている。そして、我々の研究では、PKIと比べて事前の公開鍵の交換が不要であり、実名性の高い身元情報の交換を不要にすることができることに着目している。このIDベース署名を使って、ユーザはネットワーク上で行動するつど行動証明書が発行され蓄積される。この蓄積された行動証明書を複数組み合わせて第三者に提示し、検証することによって、ユーザのアイデンティティを識別して認証することが可能になると仮定している。この検証の再に、IDベース証明書を一括化し検証する仕組みとしてバッチ証明(Batch Processing)の技術[5]を導入して開発した。今回、このIDベース証明書の発行、検証においてバッチ証明する一連の技術についてFACE(Fragment Aggregation Certification)技術と命名した。

このエンジンを用いて実際にユーザをアイデンティティごとに認証するための仕組みについては検討課題が残っており、今回このFACE技術を活用してネットワークサービス化するための仕組みについて検討したので報告する。

3.FACE技術の概要

ここで提案するFACE技術は、IDベース署名とバッチ証明を基本とする技術であり概要について述べる(図3)。IDベース署名は、楕円曲線暗号を用いた公開鍵暗号技術の応用の一つであり、公開されているIDを公開鍵とし、これに対応する秘密鍵をペアリング演算という楕円曲線上の双線形写像によって生成する。この秘密鍵を用いてディジタル署名にしたものがIDベース署名である。ディジタル署名の検証において、通常のPKIでは、署名情報と署名を生成したときに使われた秘密鍵に対応する公開鍵で検証するが、IDベース署名では、署名情報と、署名に用いられた秘密鍵に対応する公開鍵(公開ID)と、公開IDから秘密鍵を生成する際のパラメータの一部である検証鍵(これも公開情報)を用いて検証する。このとき、公開ID・秘密鍵とそれらによる署名情報が複数あった場合、署名を検証するためには複数の署名情報、複数の公開ID、検証鍵を使って逐次実施する。これに対してバッチ証明では、複数の秘

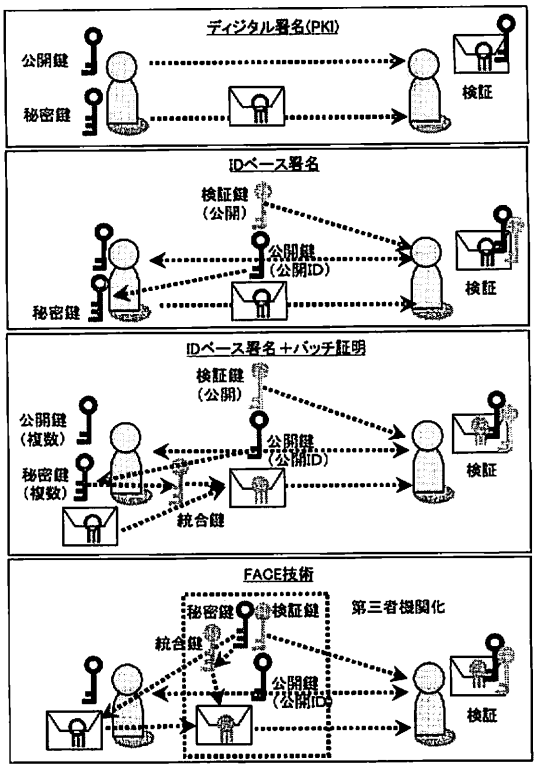

図3. FACE技術の概要

密鍵を統合した秘密鍵を生成し、この秘密鍵を用いて複数の署名情報を統合した一つの署名情報を生成し、一つの署名情報と署名に関係している公開ID(複数)と検証鍵(一つ)を用いて一括検証が可能である。ただし、この状態では、秘密鍵を持っているユーザが自由に署名できるが、公開IDとしてさまざまな事象(時刻や場所などのID)に対する証明書として活用するためにはユーザが自由に署名できることは好ましくない。そこで、公開IDから秘密鍵の生成を第三者機関化してコントロールすることによってIDベース署名を証明書として運用する仕組みにしたものがFACE技術である。これはPKIにおけるRA (Registration Authority) /CA (Certificate Authority)に相当するものとしてIDベース署名ではTA (Trusted Authority)が考えられており、このTAの機能の中で署名生成、秘密鍵の管理と

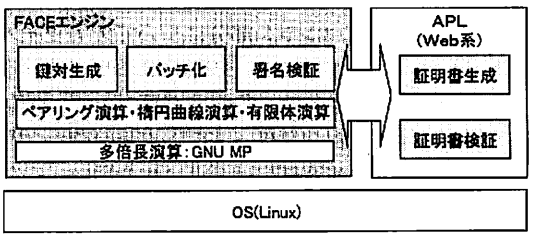

図4. FACEエンジンのモジュール構造

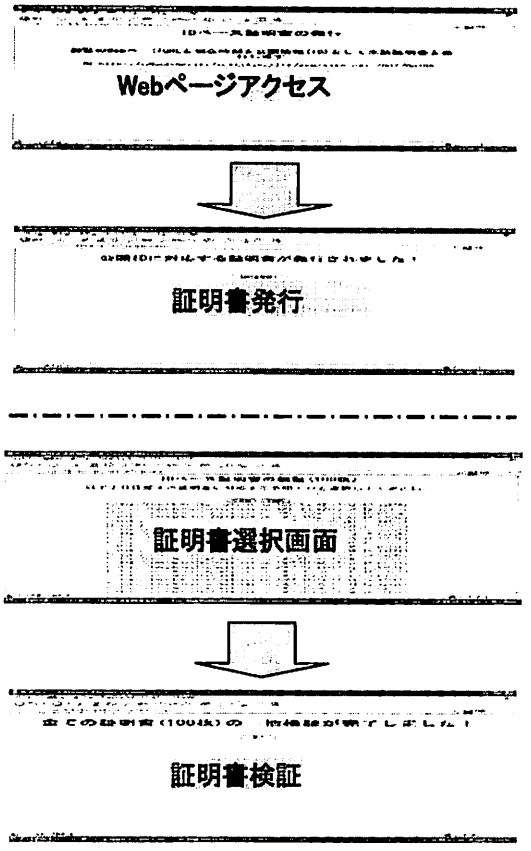

図5. FACEエンジンによる証明書発行検証例

バッチ証明を実現するものである。

既存のディジタル署名（PKI）と比べたFACE技術の特徴を整理する。

(1)証明書発行者の公開鍵を含むCA証明書が不要なため署名長が短くなる。

(2)公開鍵が証明したい内容そのものの文字列であるため可読性がある。

(3)複数の証明書を束ねて検証できる（バッチ化できる）ため、多数の証明書のやり取りが不要となり、それに伴う処理負荷を大幅に軽減できる（処理速度・問い合わせ回数・転送データ量）。

(4)利用者の本人情報を含まない証明書で運用ができる。

次にFACE技術のエンジン部分についてプロトタイプを開発したので、そのモジュール構成について述べる（図4）。IDベース署名は、多倍長演算の上に、有限体演算部、楕円曲線演算部、ペアリング演算部から構成される。多倍長演算部にはGNU MPを用い、その他のモジュールは独自開発である。この上で、IDベース署名を実現する基本モジュールとして、公開IDから

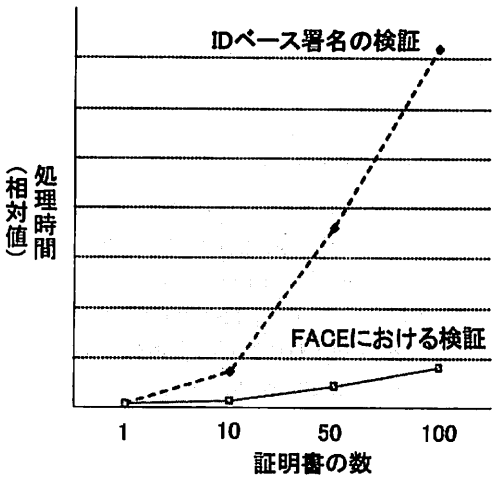

図6. FACEエンジンによるバッチ化と検証時間

秘密鍵を生成する鍵対生成部、バッチ証明のためのバッチ化部、バッチ証明を実施する署名検証部を構成した。実際の証明書の発行と検証は、これらのモジュールをWeb上のインタフェース（CGI）から呼び出す形で開発した。画面の流れとしては、証明書の発行は、参照したWebページのURLと時刻を公開IDとして証明書を発行し蓄積する。証明書の検証は、蓄積されている複数の証明書から対象となる証明書を選択することによって検証が実施される（図5）。

今回のエンジンはプロトタイプであるため処理性能についてはペアリング演算、楕円曲線演算、有限体演算に関しては改善の余地があるが、全体の処理傾向はつかめるので、性能の傾向を図6に示す。ここでは、すでにIDベース証明書が発行されており、蓄積されているIDベース証明書の中から検証したい証明書を複数選択した後、検証用の一枚のIDベース証明書に束ねて検証するまでの時間を相対値として計測した。IDベース証明書1枚のときは、バッチ化処理が伴わないため、通常のIDベース証明書の検証とFACE方式（IDベース署名＋バッチ証明）と差異はない。IDベース証明書が増えるにつれて、バッチ処理のないIDベース証明書の逐次検証と、バッチ処理を実施したFACE方式の差異が大きくなり、100枚のIDベース証明書の処理においては通常のIDベース証明書の検証時間にくらべFACE方式は約1/7の処理時間になった。このことからも大量のIDベース証明書を検証する際には非常に優位であることがわかる。

4.FACE技術による認証サービス

以上のようなIDベース署名を用いたFACE技術による

ID・パスワードが不要な認証サービスのイメージを図7に示す。ユーザは普段から自分の立場を意識せずに(匿名化された状態で)Webの参照やゲートの通過などをそのつど証跡としてディジタル証明書が発行され蓄積されてゆく。ネットワーク上のサービスでこれまでの行動の際に生じたディジタル証明書を用いて認証するイメージである。具体的な例として、最近はやりの友人の紹介によって参加するSNSに加入する場面において、既存会員の誰かの友人であることをメールのやり取り実績や一緒に遊びに行ったときの行動の実績を証明書化し提示することができれば友人であることが確実に立証できるようになるであろう。また、もう一つの例として、自分が成人であることをネットワーク上で立証したいシーンがあったとする。このとき、実世界での酒類の購買実績(お店で対面で購入するので)を証明書として蓄積し、これをネットワーク上で提示することができれば匿名性を保ちながら成人であることが容易に立証することができるであろう。

次に、このようなシーンに対して、これまで議論してきたFACE技術を当てはめる(図8)。ユーザは、普段からネットワーク上のどこかのサイトで(メールサービスやWebの閲覧を含めて)サービスを受けているとする。通常のこのサービス受益の事実を認知して(図8－①)その事実に対して証明書を発行する(図8－②)。この証明書をネットワーク行動証明書(Network Behavior Certificate)と呼ぶことにする。このようなユーザの振る舞いの事実を認知し証明書化するには中立的な第三者機関が必要になり、ここではTA相当が実施することになる。また、この証明書の中にはユーザを識別する情報は入れないため、証明書を所有していることがその行動をした証明になる(図8－③)。基本的なインプリメントでは、ネットワーク行動証明書はユーザサイドで蓄積・管理してゆくことになる。(もちろん、これを代行するインプリメント方法も考えられる。次にユーザが、ある別なサイトのサービスを受けるために複数枚の過去のネットワーク行動証明書を必要とする場合、ネットワーク行動証明書をバッチ処理し(本提案方式では、ネットワーク行動証明書が一枚でもバッチ処理を実行する)、その結果生じた証明書をサービス提供者に提示して自分の過去の行動を立証する(図8－④、⑤)。この立証のために提示される証明書は立証の要求が起こるつど生成され、その場限り有効なものである。また、立証においてこのバッチ処理によって生じた証明書を提示するため、ネットワーク行動証明書そのものが盗用されるのを防ぐことができる。

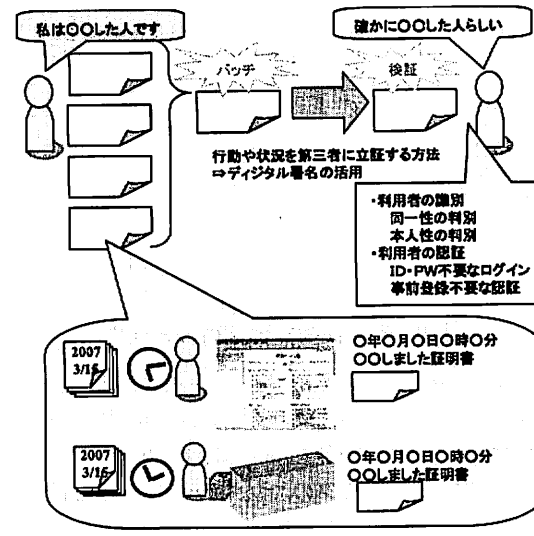

図7. 想定利用シーン

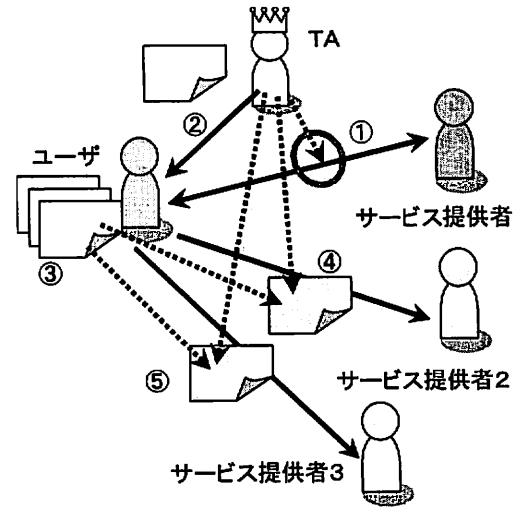

図8. FACE技術による実現モデル

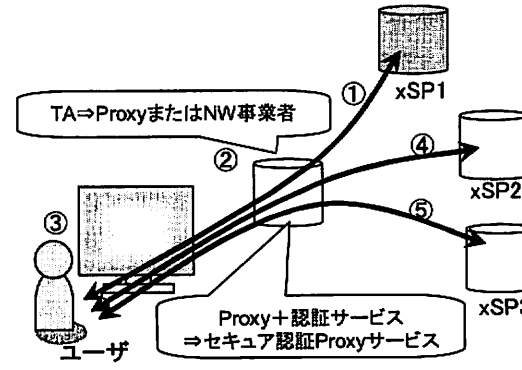

図9. NWサービス化モデル

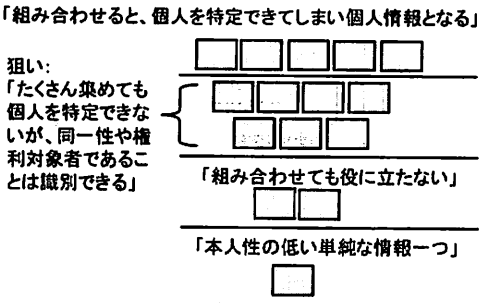

図10. 本人性指標化技術の方向性

さらに、このモデルをネットワークサービス化することを検討する。ネットワーク上のユーザの振る舞いを中立的な立場で認知することができるのは、アプリケーションレイヤではProxyサービスのようなものか、もう少し低いレイヤではネットワークサービスレベルでの認知となる。よってこのような機能の中にFACEエンジンを導入する方針で考えてゆく。このとき、上位レイヤで流れているユーザIDなどは認知せずに、セッションレベルでの識別でサービス利用の事実を認知し、その事実に対して証明書化することになる。このとき、IDベース署名におけるTAの機能、ネットワーク行動証明書の発行、秘密鍵の管理、ネットワーク行動証明書のバッチ処理を実施するネットワークの機能をセキュア認証プロキシ機能(Secure Authentication Proxy Function) と名づける。この機能では、先のFACEエンジンのうち、鍵対生成とバッチ化のモジュールが実装される。ユーザ側では、ネットワーク行動証明書の受領と蓄積、xSPの要求に応じてネットワーク行動証明書の選択が必要になるが、これらの一連の処理がユーザが意識することなく実施されることが望ましい。そのため、本来ユーザ側で実施する機能をセキュア認証プロキシ機能で代行することも考えられる。ユーザから提示された証明書を検証することによってユーザを識別・認証しその結果サービス提供を実施するxSPサイドでは、先のFACEエンジンのうち署名検証モジュールが実装される必要がある。

また、このときどのような条件やどの程度の確実性でユーザを識別・認証できるかを明らかにする必要がある。つまり、ユーザの過去の行動情報を組み合わせることによって本人性を特定するための指標化が必要になる。ここでは、単体の情報では本人性の薄い情報とし、大量に集めると本人を特定する情報にまでなるが、本人を特定するまでには至らないが、同一性や一定の条件を満たしているかどうかを判定できる程度まで集めることがポイントになる(図10)。また、このような認証サービスを実現するには、ユーザサイド、セキュア認証プロキシサイド、xSPサイドでのネットワーク行動証明書のやりとりによりユーザを認証するための安全で効率的なプロトコルを設計する必要がある。以上のことかあら、プロトコル化とユーザの指標化が直近の今後の課題である。また、さらなる課題として、このような認証サービスを実現するにあたってIDベース署名の特徴をさらに活かす方法や認証サーバの負荷を軽減する方法などの検討も残っている。

5. まとめ

多くのネットワーク利用者が、非常に多くのIDの安全な管理に翻弄されつつある。そこで、ID・パスワードなしにユーザを識別・認証できる新しい認証基盤が実現できれば、現在のID管理に伴う多くの問題が解決できると仮定し、ユーザの振る舞いと状況の情報を活用することによって実現することを考えている。そのために、散発的に発生するユーザの振る舞いや状況の情報を確実に記録し第三者に提示するためにIDベース署名を活用したディジタル証明書による方式を提案した。また、ディジタル証明書を発行・高速検証するプロトタイプエンジンを開発し、このエンジンを活用したネットワーク上の認証サービスの実現方式を提案した。今後の課題として、ユーザの振る舞いや状況によって発生するディジタル証明書を複数組み合わせて本人性を判定するための本人性の指標化と、ネットワークサービス化するためにユーザサイド、認証機能サイド、サービス提供者サイドで、ユーザを識別・認証するための安全で効率的なプロトコルの設計がある。

【参考文献】

[1]斉藤、櫛田、山崎、小林、金井,"ネットワーク社会におけるID氾濫の課題分析～ID爆発の問題提起～", 情報処理学会研究会報告,2006-GN-61-6,p.29-34,2006.

[2]斉藤、櫛田、山崎、小林、金井,"多様なアイデンティティを実現する認証方式の提案",情報処理学会研究会報告,2007-GN-62,p.131-136,2007.

[3]斉藤、山崎、櫛田、山本、知加良、小林、金井,"IDベース証明書を用いた"ゆるい認証"方式の提案",2007-GN-63,p.55-60,2007.

[5]A.Shamire,"Identity-based cryptosystems and signature schemes",In advences in Cryptology - CRYPTO'84,vol.196 of LNCS,p.47-53,Springer,1984.

[5]千田、山本,"対話証明のバッチ実行とその応用", 電子情報通信学会 SCIS 2007,1C2-2.