2007－GN－63 (10)
2007／3／22

IDベース証明書を用いた〝ゆるい認証〟方式の提案

斉藤典明、山崎哲朗、櫛田達也、
山本剛、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

ネットワーク上の様々な脅威が増加している現在、ユーザのID管理の負担が爆発的になるID爆発の状態になりつつある。これは、必ずしもIDの活用が重要ではないシーンにまでIDが活用されているためであり、ネットワーク上の多様なアイデンティティに基づいてユーザを識別・認証できる仕組みを実現することによって解消できると考えている。本論文では、ネットワーク上のアイデンティティに基づいてユーザを識別・認証するための仕組みの一部として、ユーザの行動や状況を確実に記録・活用するための機能をIDベース証明書とバッチ実行を用いてはじめて実装し、その性能検証を行った。その結果、理論どおりの実装ができたことを確認し今後のシステム化の見通しがついたので報告する。

The "Generous Authentication" based on The Identity-Based Certificate

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

In the present network society, several kind of threats on the network are increasing, we should have to spend many care for protecting many IDs, so in the near future our daily life will be annoyed by the ID explosion. One of the reason for such phenomenon is to use too many IDs regardless of suitable or not suitable, then we considered that the ID explosion will be able to be avoided by introducing a new function which is able to identify and certify the network user based on whose several identities (standpoint, role, personality ...) in the network. As the first step for the implementation of such function, we developed this function by using many ID-Based Certificates, which are generated based on the user's behavior in the network or his situation on the network, and the Batch Processing. In this paper, the outline of this function and the performance characteristic are shown.

1. はじめに

インターネットの普及およびブロードバンド環境の普及に伴い、様々なサービスがオンライン化され、生活に必要な様々な環境がネットワーク上に実現してきている。一方で、ネットワーク社会を背景にした様々な事件や脅威も増加している。そのため、ネットワーク上の権利を守るための手段としてIDを確実に守る必要性が増してきている。このような社会現象に対して先の論文では[1,2]、ユーザが管理するべきIDが爆発的に増加することにより利用者自身がこれに追随できなくなってくる状態をID爆発(ID Explosion)と定義し、ユーザがIDを〝覚えきれない〟、〝管理しきれない〟状況へ対処する必

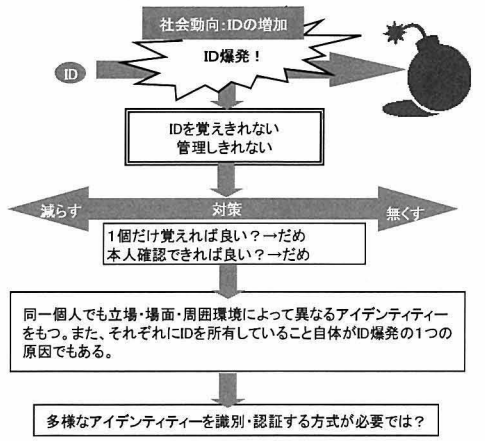


図1. ID爆発解決へのアプローチ

要性が急務であることを提言した。

このID爆発を解決するための既存の技術で容易に考えられるアプローチには大きく分けて2つがある。ユーザのID管理の負担を軽減するというアプローチと、ユーザがID管理をしなですむようにするというアプローチである。前者の具体的な例としては、シングルサインオンのように一つのID／PW(PW：パスワード)に関連付けて集約し、一つのID／PWをきっちり管理しする方法や、ID管理ツールのようなID管理の自動化を目指す方向が考えられる。後者のID管理をなくしてしまうアプローチの具体例としてバイオメトリクス認証がある。

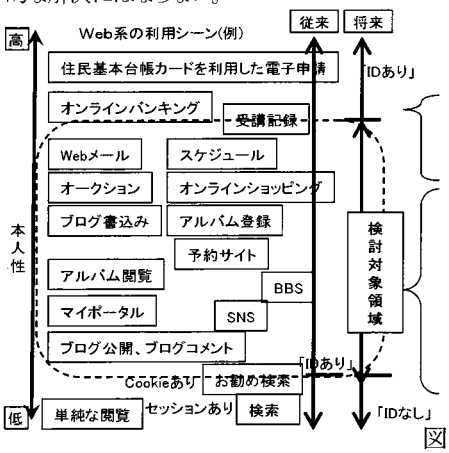
しかしながら、我々の通常のネットワークの利用では、様々な立場や用途に応じて様々なIDを使い分けている実情を考慮すると、すべてのIDを一つのIDで集約することはできない。バイオメトリクスのような確実な本人性まで必ずしも常に必要ない。また、ID管理ツールの利用は多少ユーザの負担を軽減することはできるものの抜本的な解決にはならない。

そこで本研究では、ID爆発を解決するための第三のアプローチとして、本人性は必ずしも問わず、様々な立場において使い分けを可能にするような、ネットワーク社会上のアイデンティティに応じてユーザを識別・認証する技術：ネットワークアイデンティティ認証(Network Identity Authentication)を提案している[3]。

本論文では、このネットワークアイデンティティ認証技術の実現の最初のステップとして、ネットワーク上のアイデンティティを表現するために、ユーザの行動や状況を認証・否認不可な情報として記録・活用するための機能を導入する。このユーザの行動や状況を確実な情報として記録・活用する手段としてディジタル署名(Digital Signature)の一つであるIDベース署名(Identity-Based Signature Schemes)のアルゴリズムに基づいたIDベース証明書(Identity-Based Certificate)を用いて実装し、性能検証を実施したので報告する。

2. ゆるい認証

まず我々の提案する技術の位置づけを図1に示す。図1左側において縦軸は、本人性の強弱を示しており、一番上は、現実の本人性とネットワーク上で確認できる本人性の同一視が必要となる部分である。ユーザ本人の存在証明や本人そのものに付帯する財産、権利を示すためのIDが必要となる領域であり、多様なアイデンティティという概念とは相容れない領域であり、我々の提案する技術の対象範囲外となる。図1左側の一番下の部分は、ユーザの識別は不要な領域であり、多様なアイデンティティという概念は不要な領域である。そのため、ここの領域についても我々の提案する技術の対象範囲外になる。よって我々の提案する技術の対象領域は、この中間の部分に相当し、この部分は図1右側に示すような特徴があると考えられる。



初回利用	通常利用	考え方	コスト	評価
きつい本人性確認でID発行	ID提示	本人とバンドルできる。突き詰めればバイオメトリクス、ICカード。	初回認証のコスト ＞ 通常利用とID管理のコスト	ID利用が適している
ゆるい本人性確認でID発行	ID提示	本人にバンドルする必要性が小さい(トラブル時に必要)。 トラブル解決技術の導入により対象が広がる。	初回認証のコスト ≦ 通常利用とID管理のコスト のときID管理の負担を感じる。	ID管理が負担になりID利用が適していない可能性がある
本人確認なしでID発行	ID提示・口頭可	トラブルがない又は小さい事が前提に適用。		

図2. ゆるい認証の適用領域

このような検討領域のサービスにおいても、現在は通常はIDが利用されており、ここでのIDは本人性の確認が薄い状態で付与される。容易にIDが発行され、様々なサービスが利用できるようになり非常に利便性が向上する。しかしながら、昨今の様々な脅威への対策としてこれらのIDの管理が重要となり、ID発行の容易さに比べ普段のID管理の手間が非常に増えていることが課題となっている。

この領域においては、現実の本人性よりもサービスを享受するための本人性(例えば、予約であれば予約した人と現実に来た人が同じであればよい、など)が確認できればよいはずである。しかしながら現実には、様々な悪用があるために、現実の本人性と結びつけることによって悪用を防止しようとしているのが実体である。一方で、魅力的ではあるがあまり重要ではないサービスのために現実の本人性を結びつけることに対するユーザの抵抗感は大きい。このため、匿名でサービスを提供することを許容するような仕組みや仲介サービスも登場している。

ここで、現実の本人性を不要とし、悪用を防止しつつ、自己申告型の本人性を許容する本人認証を"ゆるい認証"(Generous Authentication)と定義すると、この"ゆるい認証"が実現できればこのような領域のユーザ認証の課題を解決できると仮定し、この"ゆるい認証"を実現することが本研究のゴールとなる。

ただし、"ゆるい認証"の実現はシステム的なつくりだけでなく社会的な許容も必要となることから、現実の世界で"ゆるい認証"が馴染むシーンから適応され、次第に社会で許容されることによって適用領域が広がり、最後は現在は本人確認までしているが本来は必ずしも本人性を必要としないシーンまで広がっていくものであると考えられる。そのためには、本人性確認がないことによるトラブルが小さい場合への適応や、本人性確認をしないことによって生じるトラブルを解決できる代替技術(例えば、悪用の防止や抑止、検知の技術や悪用者の追跡技術など)の導入が必要となるであろう。このような本人性確認をしないことによるトラブルを解決する戦略の一例として、確実な部分に対してディジタル署名を適応する方法が考えられる。

3. IDベース証明書とバッチ実行技術

我々の検討ではゆるい認証を実現するためには、本人性を扱わずにネットワーク上で観測可能なユーザのアイデンティティを認証する技術の実現が必要であり、その要件は表1のとおりである。このような要件を満たすためには、ユーザを識別するために用いる情報についても本人性の薄い情報を活用する必要があり、ここでは本人性の薄い情報としてユーザのネットワーク上の振る舞いやそのときの状況などのネットワーク上で観測可能な情報を活用することとした(図3)。これらの情報を用いてユーザの特性を意味づけ、指標化することによって、本人性を扱わずにユーザを識別・認識できる技術を実現してゆく[4,5]。

表1. ネットワークアイデンティティ認証の要件

◎ネットワークアイデンティティ認証の要件
(1)一意に識別できる(確率的も可) (2)本人性は問わない(多様性の許容) (3)詐称は拒絶できる
◎多様性のバリエーション
(A)基本型: 1個人が立場や役割に応じて複数のアイデンティティを持つ (B)変化型: 1個人のもつアイデンティティが変化する (C)交代型: アイデンティティが別の個人に引き継がれる (D)集合型: 複数の個人が一つのアイデンティティをもつ
◎認証システムとしての要件
・本人性の薄い情報を活用する ・秘密情報を漏らすことなく検証できる

本論文では、まずこの実現における最初のステップとして、ネットワーク上で観測可能なユーザに関する状況や行動の記録を本人性を伏せたまま信頼できる情報として扱う方法を検討した。このような特性の情報を扱うには、従来から秘密情報を明かさずに検証する方法として、ゼロ知識証明(Zero Knowledge Interactive Proof)という方法が知られている[6]。これは公開鍵暗号を活用する方法で、その一つにディジタル署名が位置づけられる。

ただし、通常のディジタル署名では、あらかじめ本人性の確認されユーザ間で鍵交換を行い署名と検証を実施するため、本人性が明らかになり、本人性を隠蔽したい場合には不都合となる[7]。そこで、あらかじめの鍵交換が不要であり、署名者と検証者の間で公知の情報から秘密鍵を生成し検証することのできるIDベース署名[8]の活用が有効となる。このIDベース署名からメッセージ部分の取扱を省略したIDベース証明書によるユーザの識別・認証方法を検討する。

3.1 PKIとの違い

次に通常のPKI(Public Key Infrastructure)によるディジタル署名とIDベース署名の違いについて簡単に述べ

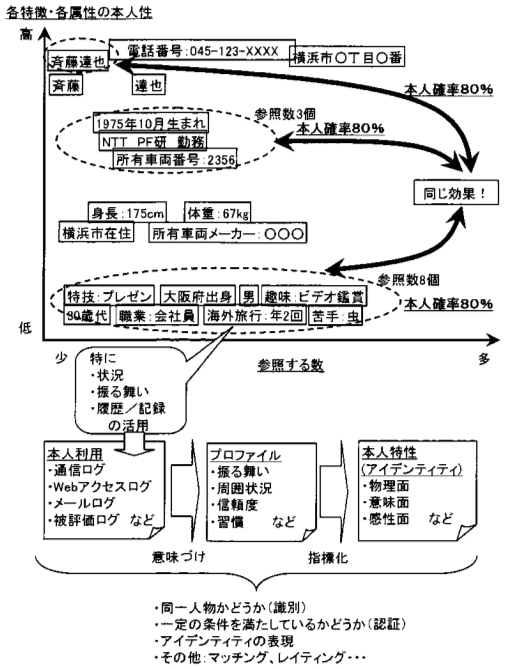


図3. 本人性の低い情報によるユーザ特定

る(図4)。通常のPKIのディジタル署名では（図4上段)、RA(Registration Authority)にて秘密鍵と公開鍵の鍵対を生成し、秘密鍵はユーザが厳重に管理し、公開鍵はCA(Certificate Authority)に公開鍵証明書として登録する。今、ユーザPからユーザVに、重要な情報を送信するとする。このときユーザPは重要な情報を秘密鍵を用いて署名をし、ユーザVに送信する。ユーザVはユーザPの公開鍵証明書から公開鍵を取得し、ユーザPから送られてきた署名付情報を検証し、検証が成功すればユーザPから正しく送信されてきた情報であることを確認できる。

IDベース署名では(図4下段)、この鍵対を生成するときに、すでに公になっている情報を公開鍵相当になるように秘密鍵を生成することが特徴である。例えば、現在参照しているWebページのURLと時刻情報をIDとして秘密鍵を生成する。ここで、ユーザPからユーザVに、重要な情報を送信するとする。このときユーザPはすでに公になっているIDから自分の秘密鍵を生成し、この秘密鍵を用いて重要な情報に署名をしてユーザVに送信する。ユーザVは、公になっているIDと第三者機関（TA : Trusted Authority）の公開鍵を使って検証用の鍵を生成し、ユーザPから送られてきた署名付情報を検証し、検証が成功すればユーザPから正しく送信されてきた情報であることを確認できる。この仕組みを活用することによって、例えば、ネットワーク上の参照行動に対する証明書を発行し、ユーザの本人性は確認しないがある時刻にあるWebページを参照したことをIDベース証明書を用いて立証することが可能になる。

3．2 IDベース証明書活用における課題

次にこの特徴を我々の検討の中で用いることを考える。我々の検討ではネットワーク上で観測可能な本人性の薄い情報として、ネットワーク上の振る舞いやその時のユーザを取り巻く状況に関する情報を複合的に活用してユーザを識別・認証しようとしている（図3)。このような情報の確実性を立証するにはIDベース証明書の利用が効果的である。一方で、このことは一人のユーザを特定するためには、複数の情報を活用することになり、それぞれの情報がディジタル証明書つきであるとすると、それぞれの証明書を検証する必要が出てくる。このため、ユーザを識別・認証するための情報が大量になると、大量の証明書を検証するために時間を要するというデメリットがある。このようなデメリットを解消する方法にバッチ実行(Batch Proceessing)という方法が提案されている[9]。これは、複数のIDベース証明書を一括して証明検証する方法である。

4．バッチ実行アルゴリズムと性能検証

本研究では、ユーザのWebページなどの参照動作に対してIDベース証明書を発行し証明検証をバッチ実行

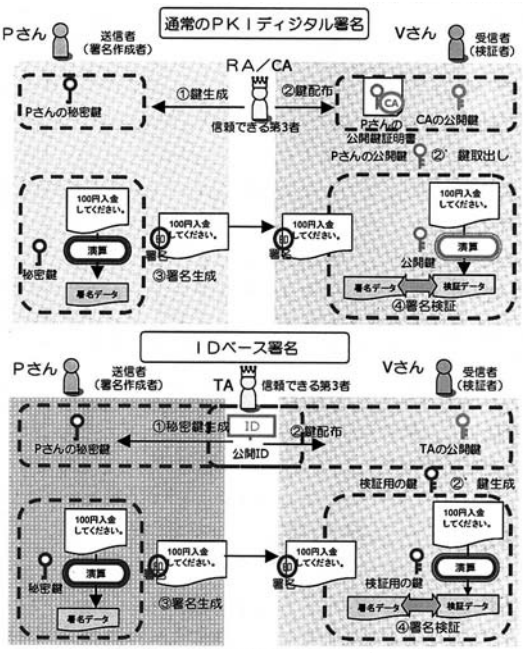


図4．PKIとIDベース署名

する部分について実装を行い性能検証を行っている。本論文では性能検証結果について速報レベルで報告する。(詳細な検証などは今後の論文で報告する。)

まず、複数のIDベース証明書を用いた検証の流れを図5を用いて説明する。さらに、この一連の処理を実装した結果については図6のとおりであった。ここで、公開IDとして、ユーザが参照したWebページの記録をIDベース証明書化するイメージで、URL、日時、整理番号にhash演算したものを公開IDとしIDベース証明書を生成し、一括検証するIDベース証明書の数として1、10、50、100の場合で性能測定を実施した。実装にあたってはLinux PC上にC言語を用いてプログラミングした。ソフトウェア構成は、多倍長演算部にgmp(GNU Multi Precision)[10]を用い、独自に作成した楕円曲線演算部、ペアリング演算部、IDベース証明書作成部、バッチ実行部から成る。

・バッチ実行なしの場合:証明書生成者は、対応する公開IDと秘密鍵からd個のIDベース証明書を作成し(性能検証結果は図6の①)、これらを検証者に送る。検証者は、それぞれの検証用の鍵を用いて逐次検証してゆく(性能検証結果は図6の②)。

・バッチ実行の場合:証明書生成者は、d個の秘密鍵を用いて合成した秘密鍵を生成する(図5の⑤)。次に、d個の公開IDを用いて合成したIDを生成する(図5の⑥)。この合成された秘密鍵を用いて、合成されたIDに署名を打ち証明書を生成し(図5の⑦、⑤～⑦の処理の性能検証結果は図6の③)、これを検証者に送る。検証者は、一つの証明書を検証用の鍵を用いて検証する(図5の⑧、性能検証結果は図6の④)。

また、図5の⑤～⑧の計算式は図7の⑤～⑧に対応している。

検証結果を参照してわかるとおり、証明書生成時間においてはバッチ実行なしがある程度優位である。しかしながら、検証時間においては、バッチ実行ではIDの数が増えてもほぼ一定値であるが、バッチ実行なしではIDの数に比例して検証時間がかかることがわかる。このことから理論どおりの実装ができていることが確認できた。

5. まとめ

生活に必要な様々なサービスや環境がネットワーク上に実現してきている一方で、様々な脅威も増しておりユーザが管理するべきIDの負担が爆発的に増加するID爆発の状態になってきている。このID爆発を解決するためには、IDの管理が負担となるような高い本人性

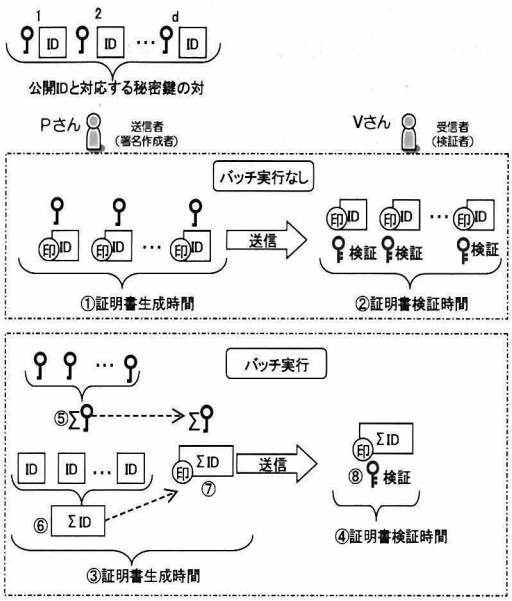


図5. IDベース証明書におけるバッチ実行

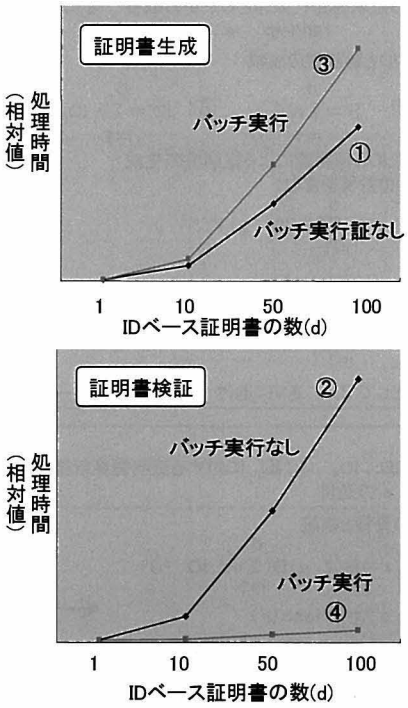


図6. 性能検証結果

を必要としない利用シーンにおいてIDの利用が不要になる方法が有効である。そのためには、様々な立場において使い分けを可能にするネットワーク社会上のアイデンティティに応じてユーザを識別・認証する技術が必

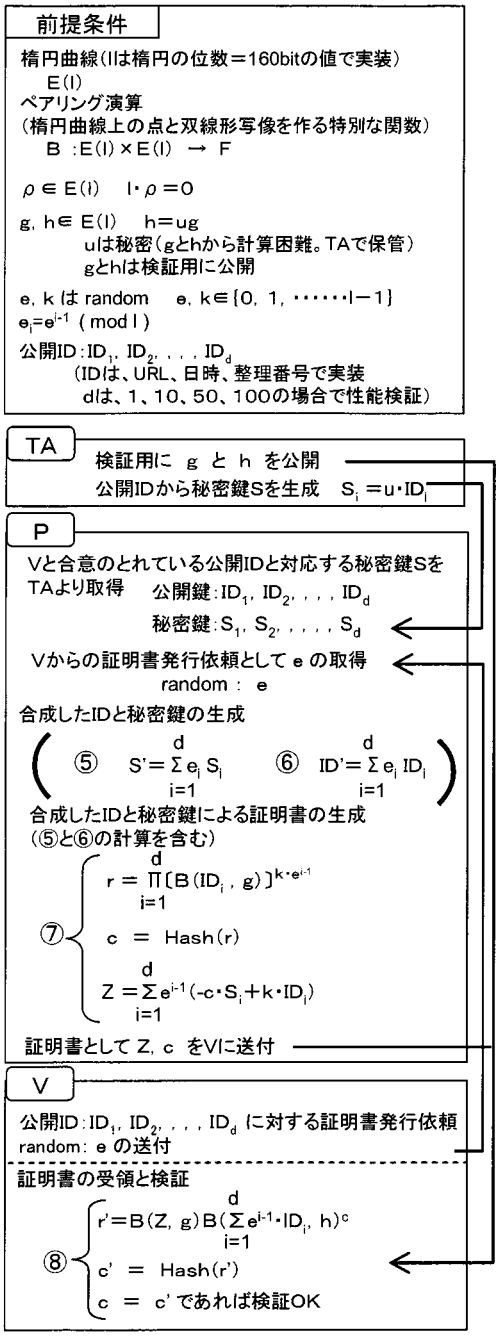


図7．演算アルゴリズム

要になる。そこで、本論文では、ユーザの行動や状況を認証・否認不可な情報として記録・活用するための手段としてIDベース証明書とバッチ実行を用いた実装と性能検証をおこない、理論どおりの実装ができていることを確認した。

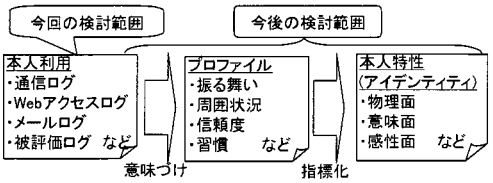


図8．今後の課題

今回の検討は、ネットワーク上のアイデンティティを認証するための一連の処理の中で、ネットワーク上のユーザ行動を確実な情報として記録・検証する部分についてのみの実装報告である。今後は、今回のIDベース証明書とバッチ実行を認証のエンジン部分として用い、ユーザの様々なネットワーク上の行動や状況をIDベース証明書化し、この証明書に基づいてユーザのネットワーク上のアイデンティティを実現する方式について検討を行っていく(図8)。

【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]櫛田、斉藤、山崎、小林、金井,"ID爆発における周辺技術調査及びID管理方法に関する一考察",情報処理学会研究会報告,2006-GN-61-7,p.35-40,2006.

[3]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.

[4]山崎、櫛田、斉藤、小林、金井,"IDベース署名を利用した利用者認証に関する一検討",電子情報通信学会2007総合大会,B-7-139.

[5]櫛田、山崎、斉藤、小林、金井,"ネットワーク行動証明書を利用した認証サービス",電子情報通信学会2007総合大会,B-7-138.

[6]佐古,米沢,古川,"セキュリティとプライバシを両立させる匿名認証技術について", 情報処理 Vol.47 No.4,pp.410-416,2006.

[7]太田,藤岡,"ゼロ知識証明の応用", 情報処理 Vol.32 No.6,pp.654-662,1991.

[8]Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, "Advances in Elliptic Curve Cryptography", "X.4.1. Identity-Based Signature Schemes",p.228-229, Cambridge University Press, 2005.

[9]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.

[10] http://www.swox.com/gmp/