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

2006－CSEC－34（60）
2006／7／21

IDベース暗号、バイオメトリック認証における失効問題についての比較

泉 昭年† 上繁 義史‡ 櫻井 幸一†‡

†九州大学 ‡財団法人 九州システム情報技術研究所

E-mail: †{izumi,sakurai}@itslab.csce.kyushu-u.ac.jp, ‡ueshige@isit.or.jp

あらまし IDベース暗号においては、IDそのものを公開鍵として扱うことで公開鍵とその所有者の関連付けを行い、バイオメトリック本人認証においては、登録されているテンプレートを抽出することの出来る生体情報を所有するのは本人だけであるという事実に基づいて本人認証を行う。このように本人の個人情報から抽出できる電子データは、本人との関連付けが比較的強いものであるが反面、盗難・紛失に際しての失効・再登録が困難である。個人情報から作成・抽出されるデータをどのようにして失効させるかという着眼から本論分ではIDベース暗号、バイオメトリック認証における失効問題の比較・考察を行う。

キーワード IDベース暗号,バイオメトリック,公開鍵基盤

1. まえがき

近年の急速なインターネットの発達により、我々はネットワークを介しての情報交換を容易に、高速に行えるようになった。今後もますます普及していくことが予想される。しかしながら、ネットワークを介しての情報交換には悪意の有る攻撃者による電子的なデータの盗聴、改竄および成りすましなどの攻撃が考えられ、それらに対するセキュリティリスクが常に存在する。

成りすましによる攻撃を防止するために、本人認証と呼ばれる技術を用いて、その本人の正当性を検証することが出来る。例えば、ユーザ名とパスワードの組み合わせを使って、コンピュータを利用しようとしている人にその権利があるかどうかや、その人が名乗っている本人かどうかの確認や、利用者を識別してユーザごとに異なるサービスを提供することが出来る。認証の際に用いられる情報(ユーザ名やパスワードなど)が他人に発覚すると不正利用が行われてしまう恐れがある。このため、認証データの機密性が要求される場合には、認証データを暗号化するなど、漏洩防止に細心の注意が払われているが、認証データの盗難・紛失が発覚した際には即座にその認証データの失効・再登録を行う必要がある。

現在はそのセキュリティリスクを回避するための技術として、主に公開鍵暗号を用いた公開鍵基盤（Public Key Infrastructure : PKI）が用いられている。

PKIが提供する機能の一つに、公開鍵証明書(以下、証明書と呼ぶ）の発行があり、これは公開鍵の持ち主が正しい相手であることを保証するための電子書類である。秘密鍵の盗難や紛失、または部署の変更などにより公開鍵の失効・再登録を行う際には、古い証明書を失効させ、新たな証明書を発行することで対応することが出来る。

近年IDベース暗号を用いた公開鍵暗号が注目されている。IDベース暗号とは、通信相手のID（メールアドレスなど）を直接公開鍵として用いる暗号方式であり、従来のPKIのように証明書を用いての公開鍵の保証を行う必要が無い。しかしながらIDベース暗号を用いた公開鍵暗号において、公開鍵を失効させる際には同時にその公開鍵に対応するIDをも失効させなければならないという失効問題が生じる。

また、近年注目されている本人認証方式に、バイオメトリック本人認証方式があり、本人の直接的な属性である指紋などの生体情報（バイオメトリック情報）から特徴点であるテンプレートと呼ばれる電子データを抽出する。事前に登録されて有るテンプレートと、認証時に抽出されるテンプレートを比較・評価することによって本人認証を行うことが出来る。近年の研究によると、テンプレートからバイオメトリック装置を詐称することのできる人工サンプルを作成することが出来ることが知られている。したがって、登録されているテンプレートの盗難・紛失などが発覚した際には即座に登録テンプレートの再登録が必要となる。しかしながら、一つのバイオメトリック情報から抽出することの出来るテンプレートは通常一つであるため、失効させたテンプレートに対応するバイオメトリック情報は二度と本人認証のために使うことが出来なくなってしまう。これは、バイオメトリック認証におけるテンプレートの失効問題であるといえる。

以上のように、IDベース暗号とバイオメトリック本人認証は、共に個人情報から電子データを抽出するシステムであり、その電子データを用いて暗号化・本人認証を行う。しかしながら、暗号化・本人認証システ

ムにおいては鍵・認証データの盗難および紛失に際しては、それらのデータの失効・再登録が不可欠であるが、個人情報から抽出された電子データの再登録は困難である。したがって、ID ベース暗号とバイオメトリック本人認証は個人情報から抽出される電子データを基礎として用いるシステムとして比較可能であると考えられる。

本論分の 2 章では ID ベース暗号における失効問題、3 章ではバイオメトリック本人認証における失効問題について述べ、そして 4 章では ID ベース暗号における失効問題とバイオメトリック認証における失効問題の比較を行う。

2. ID ベース暗号における失効問題

公開鍵暗号において、公開鍵が本当にその所有者のものであるかを保証するために従来の PKI が用いる証明書を用いた方式とは別に ID ベース暗号が提案されている。ID ベース暗号の概念は 1984 年に A.Shamia によって提案され[1]、具体的な方式が 2001 年に D.Boneh や M.Franklin らによって提案された[2]。本章では ID ベース暗号を用いた公開鍵暗号における失効問題について述べる。

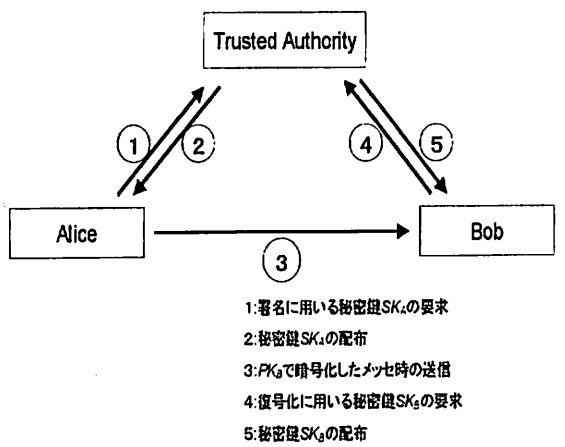

図 1 ID ベース暗号

2.1.ID ベース暗号による公開鍵の正当性の保証

公開鍵暗号を用いる暗号システムにおいて、公開鍵が本当にその所有者のものであることを保証することは極めて重要である。

例えば Alice が Bob へ公開鍵暗号を用いて通信を行うとする。この時、ボブの公開鍵は PK_B である。暗号化を伴う通信が行われる前に Alice は Bob の公開鍵 PK_B を入手しなければならない。しかしながら、悪意のある攻撃者 Charlie によって Bob の公開鍵 PK_B が Charlie の公開鍵 PK_C に置き換えられてしまうかもしれない。このことに Alice が気づかなければ Charlie の公開鍵 PK_C で暗号化されたメッセージの内容は攻撃者 Charlie によって読み取られてしまうだろう。

従来の公開鍵暗号を用いた PKI では、このような攻撃を防ぐために、認証局を設置している。この認証局が公開鍵に対して認証局自身のディジタル署名を付加させた証明書を発行することで公開鍵の正当性を保証するという方法を取っている。

ID ベース暗号を用いた PKI では、受信者のメールアドレスを直接公開鍵として用いることが出来るため、従来の公開鍵暗号を用いた PKI が使ってきたような証明書を用いることなく、公開鍵とその持ち主の関連を保証することが出来る。送信者 Alice と受信者 Bob が ID ベース暗号を用いた公開鍵暗号通信を行う場合を図 1 に示す。

ID ベース暗号を用いた公開鍵暗号基盤では、秘密鍵の管理や、秘密鍵取得の際に本人認証を行う第三者機関として Trusted Authority（TA）を設置する。秘密鍵 SK_A や秘密鍵 SK_B は一度入手すれば、失効されるまでは繰り返して使うことが出来るので図 1 において、手順①、②、④、⑤は一度だけしか行われる必要が無い。

2.2.ID ベース暗号における失効問題

公開鍵暗号において、復号化に用いる秘密鍵が悪意の有る攻撃者によって盗難されてしまうと、その秘密鍵に対応する公開鍵で暗号化されたメッセージが盗聴された場合、暗号化されたメッセージの内容は攻撃者によって読み取られてしまう。したがって、秘密鍵の盗難・紛失などが発覚した場合は、即座にその秘密鍵に対応する公開鍵を失効させ、新しい秘密鍵を作成した後に公開鍵の再登録を行わなければならないこれは ID ベース暗号を用いた公開鍵暗号においても同様である。

しかしながら、ID ベース暗号を用いた公開鍵暗号では、通常公開鍵は受信者の ID そのものであるため、その公開鍵を失効させてしまうと、対応する ID を用いての ID ベース暗号を二度と行うことが出来なくなってしまう。これが ID ベース暗号における公開鍵の失効問題である。

例えば、メールアドレス bob@b.com の ID を持つボブの公開鍵 PK_B に対応する秘密鍵 SK_B が盗難されてしまったため PK_B を失効させるとする。その後、メールアドレス bob@b.com へと送信されるメッセージは ID ベース暗号を用いて暗号化することは出来なくなって

しまう。

そこで、Bobのメールアドレスとして newbob@b.com が再登録されるとすると、これまで bob@b.com を用いて Bob と通信していたエンティティに対して、bob@b.com は失効され、newbob@b.com が再登録されたことを通知する必要がある。その後、ボブと通信を行う際には newbob@b.com のメールアドレスを用いなければならなくなってしまう。さらに、izumi@itslab.csce.kyushu-u.ac.jp のように、公的な立場で用いる ID を失効させなければならなくなった場合は、私的に用いている ID の場合とは異なった、データベースへのアクセス権限の書き換えなどの問題も生じてしまうだろう。

現在 ID ベース暗号における失効問題に対してとられている手法は、ID の末尾に有効期限などの付加情報 j_u を記載し、bob@b.com||j_u とするというものである。例えば、公開鍵を一ヶ月周期で更新する取り決めを行い、2006 年 7 月にメールアドレス bob@b.com を持つ Bob と ID ベース暗号を用いた公開鍵暗号で暗号化メッセージを送る際には、公開鍵を bob@b.com||2006.07 として暗号化を行うことになる。しかしながら、この手法は決められた周期で鍵の再登録を行う方式であるため、公開鍵の失効・再登録を即座に行うことが出来

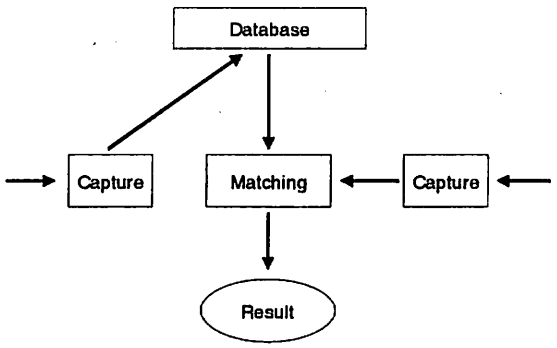

図 2　バイオメトリック個人認証

ないという欠点を持っている。即時性を高めるために、更新の周期を短くすることも考えられるが、対応する秘密鍵の作成、配布にかかるコストが増大してしまうと考えられる。

3. バイオメトリック認証における失効問題

本人認証を行う際に現在最も広く採用されている方式は、ID とパスワードの組み合わせによって本人認証を行うパスワード本人認証である。しかしながら、クレジットカードのスキミング、パスワードの盗難などの脅威によって、パスワード本人認証に変わる本人認証の必要性が叫ばれ始めている。バイオメトリック本人認証はその要求に応える本人認証技術の一つである。バイオメトリック本人認証では、身体的特徴（指紋や虹彩）、行動的特徴（声紋や署名）などの生体的特徴を抽出し、あらかじめ登録された特徴のデータベース（テンプレート）との間で類似性を評価し、十分に類似性が高ければ本人と認証する。ところが、バイオメトリック情報は一旦第三者に知られてしまった場合に、パスワードと違って新しいものと置き換えられないという点について致命的である。

3.1 バイオメトリック認証

バイオメトリック個人認証は、パスワードなどの代わりに本人の生体情報を用いて本人を認証するものである。バイオメトリック個人認証は、なりすましにくいという安全性と本人に常に備わっているという利便性が特徴である。現在、各銀行はパスワードの盗み見やカードスキミングの対応策として、ATM にバイオメトリック認証の取り入れを始めている。

バイオメトリック認証を用いた本人認証の手順を図 2 に示す。バイオメトリック認証は、登録フェーズと認証フェーズから成り立っている。まず、登録フェ

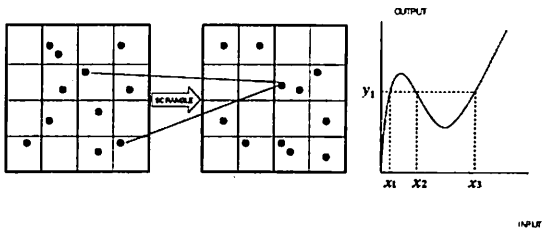

図 3：一方向関数によるテンプレートの付加逆変換の例

ーズでは本人認証に用いる本人の生体情報の特徴点をテンプレート情報として抽出しデータベースに格納する。次に、認証フェーズでは、認証時に抽出したテンプレート情報と、登録フェーズに抽出したテンプレート情報の比較を行う。この比較で双方のテンプレートの類似度を評価して、十分類似性が高ければ本人と認証する。テンプレートは、特殊な装置を用いなければ可視化することは困難であり、それを模倣したサンプルの製造、使用が困難であるため、パスワードや物証

を用いての認証よりも安全であると考えられてきた。

ところが、近年の研究によるとバイオメトリック個人認証に対して多くの危険性が指摘されるようになってきた。例えば、本人の協力や不注意によって生のバイオメトリック情報を得ることが出来れば、ある条件においては簡単にバイオメトリック認証装置を詐称する人工サンプルを製作したり、データを詐称される可能性が指摘され始めた。また、生のバイオメトリックサンプルが得られなくても、テンプレートから認証を可能にするバイオメトリックサンプルを復元する可能性も指摘されている。

したがって、データベースに登録されているテンプレートが万が一漏洩した際には、そのテンプレート情報から作られたバイオメトリックサンプルによって認証の成りすましが行われる可能性がある。

しかしながら、バイオメトリック情報から抽出されるテンプレートは通常一つであるため、テンプレートの再登録を行うことができない。これがバイオメトリック本人認証におけるテンプレートの失効問題である。

テンプレートの保護や、テンプレートを更新可能なものとする観点から、いくつかの研究開発事例が報告されている。バイオメトリックデータを多対1の対応を持つ一方向関数（図3）によって変形させ、元のデータの復元をできないようにする方法や、予測不可能な幾何学的変換を与えて、元のデータの復元をできないようにするというキャンセラブルバイオメトリックが IBM の Ratha らによって提案されている。図では、例えば二次元のデータをブロックごとにスクランブルして、複数のブロックから同じブロックへ特徴点を写像させると、元の特徴点配置は一意には復元不可能である。あるいは、連続値関数の場合には同図右のような関数を用いて変形させると、変換後の値 y から変換前の値 x を一意には復元不可能である。Ratha はこの概念の具体的な実現方法として予測不可能な幾何学的変換（図4）を与えて、元のデータが復元できないようにすることを提案した。図4左に示す変換では、ブロック単位で位置を入れ替えることにより元のテンプレートを予測することが困難になっている。また、同図右の変換では、ブロックの形状に幾何学的歪みが加えられ、それに合わせてもとの図形をゆがませている。他に、テンプレートにハッシュ関数を適用する匿名バイオメトリック[4]、バイオスクリプト[5]などの研究が行われている。

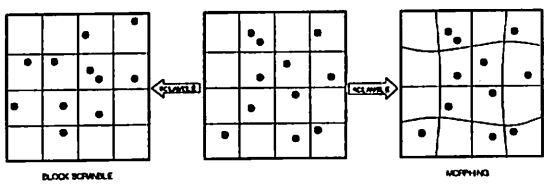

図4：テンプレートのブロックスクランブルとモーフィングの例

これらの方式では、幾何学的変換の関数やハッシュ関数を変更することによって一つの生体情報から複数のテンプレートを抽出することが出来る。テンプレートの再登録時には、以前と異なる幾何学的変換の関数、ハッシュ関数を用いることで対応する。

しかしながら、キャンセラブルバイオメトリックには、テンプレートの秘匿の性能の点では十分ではなく、照合関数の仕様が公開されていたり、不特定多数の認証機関へ配布するような用途では安全とは言えないという課題、匿名バイオメトリック、バイオスクリプトには登録・照合時に十分に多くのサンプルを得る必要があり、利便性にかけるとの課題が残されており、実装例は現在のところ報告されていない。

4. ID ベース暗号、バイオメトリック本人認証における失効問題の比較

本章まで、ID ベース暗号における公開鍵の失効問題、バイオメトリック本人認証におけるテンプレートの失効問題を個別に取り上げてきた。本章ではそれぞれの失効問題、及びそれに対する既存の対応策の比較を行い、最後に今後の課題を挙げる。

ID ベース暗号とバイオメトリック本人認証では、個人情報を元に公開鍵、テンプレートを作成する。したがって ID ベース暗号とバイオメトリック本人認証に生じる失効問題には失効、再登録させたいデータがそのデータと関連付けされる対象の個人情報から生成されるという共通点がある。通常の ID ベース暗号、バイオメトリック本人認証において公開鍵とその所有者の ID は1対1の関係であり、生体情報とその特徴点であるテンプレートも1対1の関係を持っている。これまでに挙げた失効問題に対しての解決策は一つの ID、生体情報から複数の公開鍵、テンプレートを作成可能とする、すなわち生体情報とそれから生成される電子データの関係を1対多とすることであると考えられる。

ID ベース暗号では ID に付加情報を付け、その付加情報に変化を持たせることで一つの ID から複数の公

開鍵を作成できる方式が考えられ、バイオメトリック本人認証では、生体情報から抽出したテンプレートに歪曲変換関数やハッシュ関数などの一方向間関数を適用させ、その一方向関数に変化をもたせることで、一つの生体情報から複数のテンプレートを作成できる方式が考えられている[3],[4],[5]

しかしながら、ID ベース暗号においては現在のところ ID に有効期限を付加情報として結合させる方式しか考えられておらず、有効期限内に秘密鍵の紛失や盗難が発覚した際、即座に公開鍵を更新させることの出来るシステムであるとは言いがたいと思われる。また、バイオメトリック本人認証においても実際の運用に向けては登録・照合時に十分多くのサンプルを得る必要があること、照合関数の仕様が公開されていたり、不特定多数の認証機関へ配布するような用途ではテンプレートの秘匿性の性能の点では不十分であるとの見解がある。[6]

	IDベース暗号	バイオメトリック本人認証
失効・再登録の対象	公開鍵(ID)	テンプレート
既存の対応策	公開鍵に情報付加	キャンセラブルバイオメトリック 匿名バイオメトリック バイオスクリプト

表 1 : ID ベース暗号とバイオメトリック本人認証の比較

また、ID ベース暗号、バイオメトリック本人認証における再登録にかかる演算不可などコストの比較なども興味深い内容であるように思われる。

今後、個人情報から作成されるデータを用いるシステムという観点から ID ベース暗号、バイオメトリック認証の失効問題に取り組む必要があると考えられる。

文　献

[1] A.Shamir:Identity-Based Cryptography and Signature Schemes, Proceedings of CRYPTO' 84, pp.4-53, 1984

[2] D.Boneh and M. Franklin: Identity-Based Encryption from the Weil Pairing, Proceedings of CRYPTO 2001, pp.213-229, 2001

[3] N.K.Ratha,J.H.Connell,R.M.Bolle,"EnhancingSecurity and Privacy in Biometric-based Authentication Systems" , IBM Systems Journal, Vol. 40, No. 3, pp.614-634, 2001.

[4] Tuyls P.,Goseling J., "Capacity and examples of template-protecting biometric authentication systems", ECCV Workshop BioAW, no.77, 2004

[5] Soutar C., Roberge D., Stoianov A., Gilroy R., KumarV.,"BimetricEncryption",http://www.bioscrypt.com/assets/Biometric_Encryption.pdf

[6] 鷲見和彦，松山隆司，，中嶋晴久，“バイオメトリクス認証テンプレート保護に関する検討”，2005 年暗号と情報セキュリティシンポジウム予稿集，pp. 535-540，2005.