A security for anonymity service on the Internet

匿名保証サービス

——個人情報保護の観点から——

芝　　勝徳

はじめに

本論は筆者が関係して特許願として請求された，発明の名称「認証システム」について，その発明の背景，経緯と応用の可能性と残る問題点について論じたものである。

・背景

匿名保証に関する本発明は，ネットワークを介して情報提供者端末から情報受容者端末(End to End)に所定の情報を暗号化して確実に伝送するための認証システムに関するものである。現在，ネットワークを介した通信において個人情報等の秘密をやりとりする場合，PKI(Public Key Infrastructure;公開鍵基盤)技術を利用したシステムが使用されている。PKIは，次の3点のサービスを提供する。

1. 認証(Authentication)

   相手が自分だと主張することを他者に保証すること

2. 完全性(Integrity)

   情報が場所を移動したり時間が経過したりする間に変更されなかったことを保証すること

3. 秘匿性(Confidentiality)

   意図した受信者以外は誰も情報を読み取ることができないことを保証する

こと

これらのサービスにより見知らぬ人同士(エンティティ)の間で安全な通信を可能とし，その上で本人保証や通信される情報の原本性保証をすることができる。

PKIには本人性と公開鍵を結合する行為を責任をもって行う認証機関(CA)が信頼できる第三者という立場で存在しなければならない。また，その運用において信頼できる時間源としてタイムスタンプ機関(TSA)が必要となる。*特許文献「参考」

このようにPKIを基盤とした通信は広く実際のネットワーク（＝インターネット）上で行われており，その最終利用者はほとんどPKIの知識を持たずに使用している。具体的にはブラウザに組み込まれた証明書を信頼できるものとし，氏名，生年月日，住所やクレジット番号等の個人情報等を通信相手先のWebページ上の書式に入力している。この場合，相手サーバは利用者に認証されたことになり暗号化によりやりとりされる情報の秘匿性が守られる。

これらの基盤技術の上でわが国においても電子政府，電子自治体のいわゆる電子申請のサービスではPKIである公的個人認証サービスを利用して行政側から申請者を認証することができるようになり，一部の行政事務から導入が本格化している。[1)]

・必要性

しかし，PKIには次のような機能は備わっていない。情報データが個人情報である場合は情報の発生源＝発信者である情報提供者個人のものであるが，いったん送信されてしまった後は情報受容者である個人情報取扱事業者[2)]により個人情報データベース等に入力されてしまい，システムにより運用されれば技術的には取扱事業者が個人情報をいつ，どのように見るかは自由に行えるものとなる。すなわち一般的には情報を提供した本人が管理できるようにはなっていない。

また，個々の要素が複合化された個人情報の場合，情報提供者は取扱事業者に対して情報の一部のみを開示したい，全体を開示したくないというような制御もできない。

つまり，情報受容者である取扱事業者が情報を適切に取り扱うかどうかはまったく保証されておらず個人情報の提供者は取扱事業者を信用するしかない状況である。

本発明はこれらの従来技術の運用上の問題点を解決すべくなされたもので，「情報提供者」が「情報受容者＝個人情報取扱事業者」に対して開示する情報の要素や使用目的を限定する定義を可能とし，かつ当該情報の秘密性を担保することができる認証システムを提供することを目的とする。

・技術の特徴と実現方法

詳細は特許申請書類の明細書によることになるが，概略としては以下のようなものである。

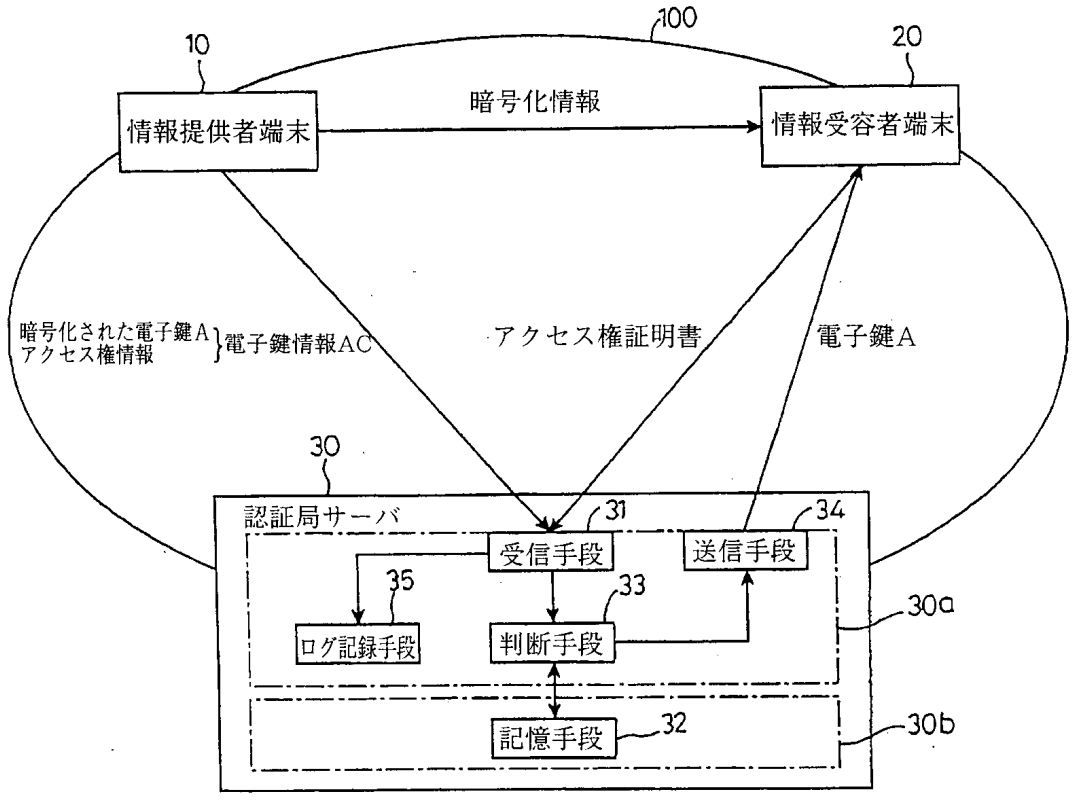

図1

情報提供者端末から個人情報等の所定の情報が電子鍵Aによって暗号化され，情報受容者端末へ送信される。暗号化に用いられた電子鍵Aは暗号化され，アクセス権情報とともに電子鍵情報ACとして認証局サーバへ送信され，電子鍵Aとアクセス権情報が関連づけられた状態で記憶される。その後認証局サーバが情報受容者からアクセス許諾証明書を受信した際，判断手段によりアクセス権情報とアクセス許諾証明書を照合すると共にログ記録手段により当該情報受容者端末からのアクセスログが記録される。（図1・図2・図3参照）

すなわち，PKI技術を背景とし個人情報提供者と取扱事業者の両者の間に立った信頼できる第三者の位置で，情報提供者が発行する電子鍵と個人情

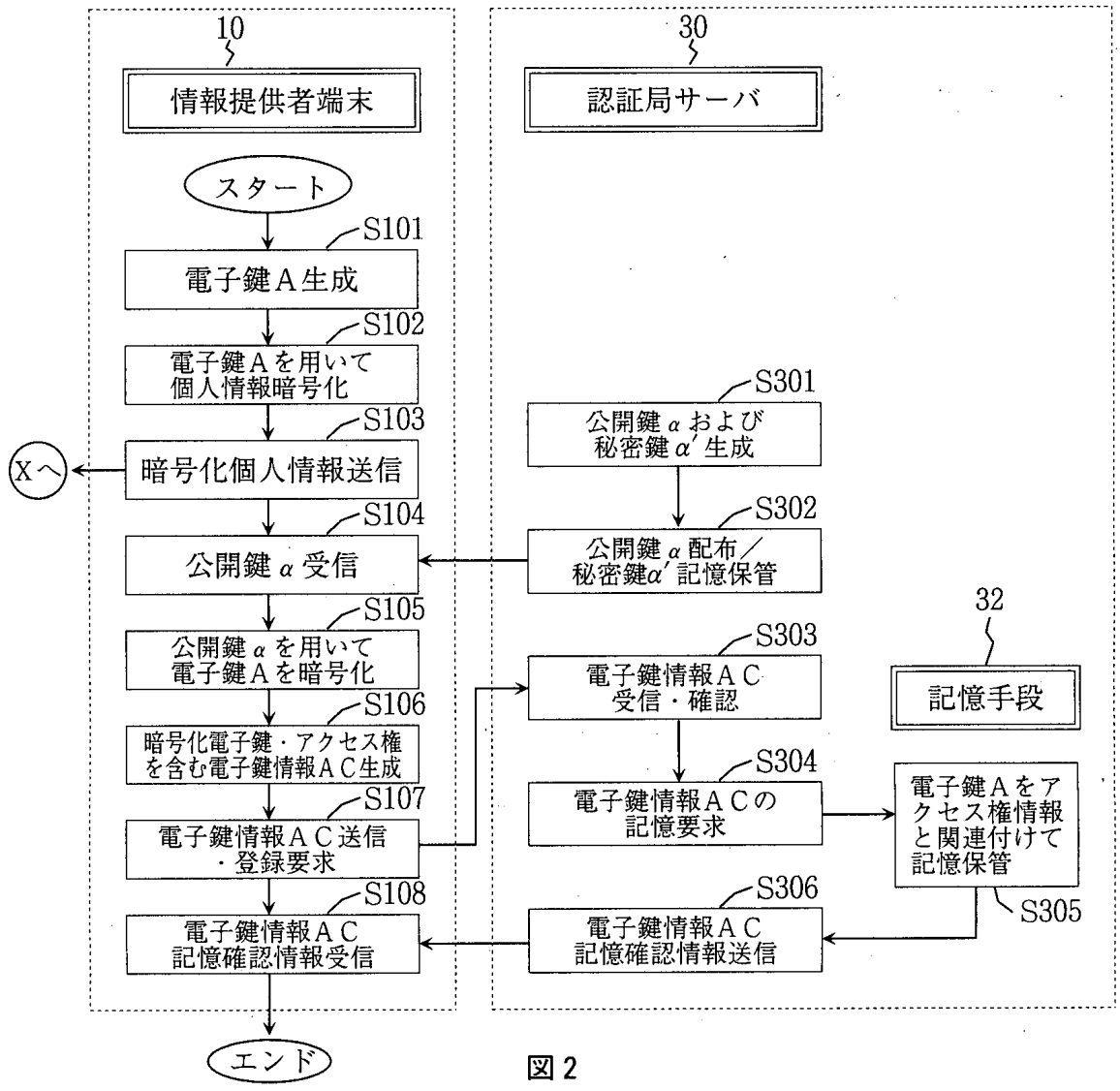

図2

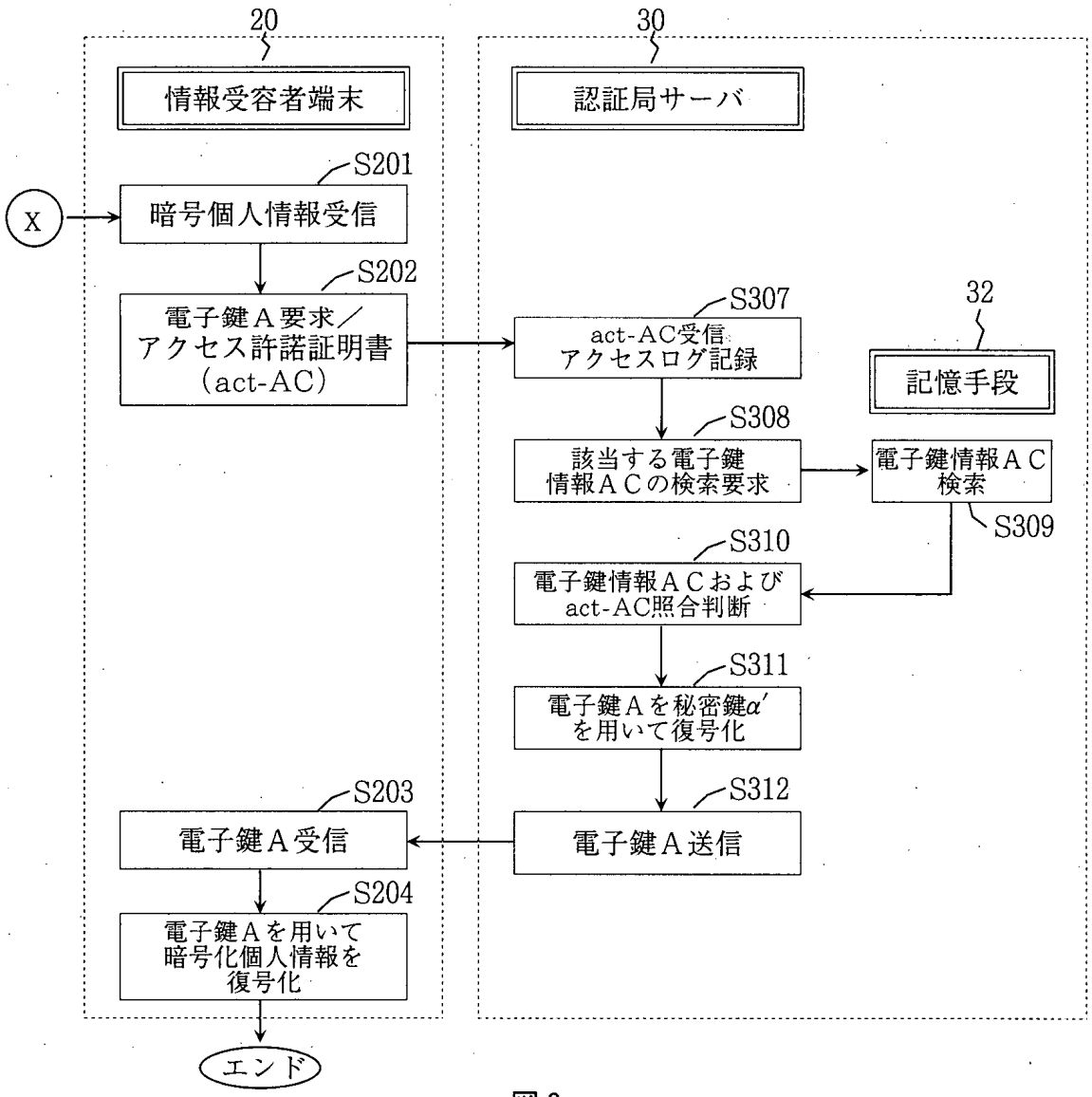

図3

報の要素単位（例えば氏名のみ）でアクセス権を設定したり，アクセスできる有効期限を限ることができる電子鍵情報を厳密に管理することにより，情報取扱事業者は情報の閲覧を含む取扱に際して電子鍵情報から得られる復合化の条件が必須となり，またその記録が第三者である認証システムに残ることになる。これにより結果的に情報提供者はその情報が匿名性をもって扱われることを制御することができる。DNA等の採取とその応用研究におけるデータベース作成等におけるいわゆる匿名化処理は取扱事業者側で行われることが前提であり，このような場合の匿名はその脆弱性が残存することは払拭できない。本発明の技術はPKIにより設定されたアクセス権の原本性＝真

正性もより確実に証明され，認証システムが記録するログによって取扱事業者における不正使用や漏洩が生じた場合においてその発生場所，時刻，経路を特定する賛助となり，人的セキュリティ対策における抑止効果としても期待できる。

・応用を期待するケースやシステム

国の社会保険システムにおいて，特定の有名人(テレビタレントや首相を含む議員関係者)の納付状況が漏洩した例を見れば，現在の行政の事務処理システムにおける内部職員からの個人情報の保護について十分に手段が講じられていると考える人は少ない。実際，端末装置は無造作に設置されていたり操作者の認証についても無いもしくは無いに等しいという状況を散見することができる。

数十年前からのいわゆるレガシーシステムといわれるベンダ固有の端末装置が集中的に情報処理する大型コンピュータに接続されている過去の状況から，どこにおいても市販され入手できるパーソナルコンピュータがベンダ非固有のオープンサーバに端末（クライアント）として接続されるようになった現状に至って，個人情報の不正利用（単純な興味本位の閲覧を含む）や漏洩の脅威は加速的に増大している。犯罪者にとっては手の平に隠れる記憶媒体で数万から数十万人の個人情報を手元のパソコンに接続して持ち出すことにさほどのコストとリスクはない。まして記録が残らないということになると組織内での情報や端末取扱規則などは実効的な抑止力にはなりにくい。

筆者が匿名保証にこだわる理由は，あらゆるシステムで個人情報が収集保存され，本人の意志に反して利用されるケースは量的にも質的にも拡大しており今後縮小することは考えられないという事実であり，不適切に処理される可能性があるのであればあらゆる手段を通じて匿名的に扱われることを本人の意志により制御できるべきと考えるからである。

もしこのような技術が応用されるとすれば，先ず行政関連のシステムから

ということが予想される。2004年現在，わが国は世界に先行する電子政府・電子自治体の構築をe-Japan戦略の一部として位置付けている。民間における保証に先んじて匿名保証を含む認証サービスが実装されることを強く期待する。質的にも例えば個人のDNAの情報等は病歴や家系と共に収集されることにより，本人のみならず未来の子孫にいたるまで重大かつ深刻な不利益を与えてしまう。より大きな責任を取扱事業者は持つことになり，この責任を各個人情報取扱事業者の組織単独で果たすことは困難になりつつある。

1. 行政分野(税，保険，教育等)
2. 医療分野[3)]

は本技術の応用を期待する分野である。

・実装する場合の課題

特許を申請する時点では，発明が必要とする前提の条件にPKIの存在をあげているが，本格的に実装して運用するとなるとさらに現実的にいくつかの課題が存在している。

1. タイムスタンプ機関の不在もしくはサービスの不十分さ

信頼できるタイムスタンプを発行する事業者が2004年末の現時点では十分に育成されていない。ネットワーク上で正確な時刻情報を配信するためには時源となる原子時計保有や一定量のアクセスに耐えるサーバを十分な帯域をもった回線に接続し，可用性（24時間，365日）を保って長期間運用するという条件を要求される。現在，タイムスタンプの単位あたりの料金などを含めてどのように事業者が育成され，業態として定着するのかが未だ不透明である。[4)]

2. PKI技術だけでは解決できない情報の長期保存問題

本発明における重要な要素は第三者における認証システムが情報へのアクセスログを記録することにある。そのログの原本性を長期にわたって確保する技術が未だ確定していない。PKIにおいて認証局(CA)が発行する

証明書には有効期限が設けられる。有効期限内において鍵情報を利用した電子署名はそれがこの当該ログの記録に対するものであった場合，有効期限内にその原本性＝完全性を保証することは可能であるが，有効期限後の署名検証は意味のないものになってしまい，数年という範囲での保証はできても10年以上の長期保存に対してはサービスが不能になるという問題が存在する。

上記の行政や医療に関する事故に対する不服申し立てや訴訟においてはPKIの有効期限を越えるものが存在し，長期保存という課題は実際のサービス実装において避けて通ることはできない。

3. 匿名保証サービスを提供する主体の人格

本発明において認証サービスを提供するものが情報提供者と情報受容者の間の第三者となることは述べたとおりであるが，双方から信頼される存在となるためにはいくつかの条件が発生する。

ひとつはPKIにおける認証局（CA）相当のセキュリティレベルやポリシーで設立・運用されなければならないのではないかという課題である。そうした場合詳細は割愛するが多額の投資を必要とし，ビジネスとしての成立を考えた場合，成立に困難が伴うということになる。

わが国における認証局の設立と運用に関しては特定のグループや範囲のみを対象とする認証局を除いて，個人が利用できるサービスの対価はまだ比較的高価である。唯一「公的個人認証サービス」のみは各地方公共団体単位で既に投資された大規模システムを背景として稼働していることもあり，24時間以内の個人の異動や死亡による失効等をサービスレベルとするという高いレベルに対して比較的安価に享受することができる。しかし，政府も民業圧迫を恐れて行政機関に限定した署名の検証範囲を定めるなど民業圧迫しないという方針が優先され，民間が同サービスを利用できないでいるなどの現状がある。

また，同認証サービスは税金が投入されたシステムであるため，見かけ

上の費用(個人が実費として支払う)は安価でも投入された税金による費用の総額から割出される発行された証明書1単位あたりの費用は2004年後半時点ではまだ高価なものである。

・課題に対する解決とその方向性

以上3つの課題をあげたが，その解決の見込みと方向性をまとめてみたい。タイムビジネスに関しては行政もその必要性を強く感じており，民間事業としての指針を示すなどして一定の方向性と安定した社会基盤としての定着が見込まれる。情報の長期保存問題については本発明だけではなく，すべての行政における電子公文書の保存や電子申請において受理した添付される電子文書の保存等，根本的に電子政府や自治体を支える基礎技術であるため，税の申告等が本格化している現状のなか何らかの方策がとられることは確実である。ただしこの2つの解決は個人単位でも支払い可能な費用を前提に構築されるべきであり，高価であるが故に普及が妨げられることがあってはならないと考える。

最後の課題である誰が匿名保証できる第三者になれるかについては，筆者は当初行政機関もしくは近い主体がその任にあたり，サービスを公共的なサービスとして提供することが望ましいと考えている。公共投資であるがために対費用効果を無視した無駄な計画・調達・構築・運用を行ってはならないのは当然であるが，既出の「公的個人認証サービス」の検証の民間開放と共に執行されるべき行政課題だと考えている。

・匿名保証における負の副作用

述べてきたとおり，本発明は個人情報を保護し，個人を不正な情報利用や漏洩といった脅威から守るという意図をもってなされたものであるが，匿名性それもインターネット上の匿名は誹謗中傷や犯罪の手段として利用されている事実は隠せない。本発明はPKI技術を応用し，個人を特定し認証できる

機能を論理的に反転させた結果であるので，記録が残る限り不正な目的で匿名を使用することは難しいが，匿名化を利用してその上に代理執行者等を積み重ねていくことにより，追跡しにくいシステムを構築することは可能である。 名前や住所を知られずにある商品を買いたいといったような応用において代理に購入するエージェントの出現がそれである。

しかし一方，大規模災害時における安否確認(特に生存情報)を安全に特定の範囲(例えば家族のみ)に配布する等のサービスはすぐにでも求められているものであり，携帯電話の高機能化や交通事業における乗車券・定期券に代わるICカードの普及など匿名保証の前提となる社会基盤システムは整えられつつある。

筆者においては，地域社会における情報システムの利用において特定のICカード等を応用し，通信だけではなく放送分野における連携においてこのテーマを掘り下げてみたいと考えている。

特許文献

特開2002-368737号広報

参考

1. 『電子政府・電子自治体推進プログラム』総務省 平成13年10月
2. 個人情報の保護に関する法律(平成15年５月30日法律第57号)
3. 『今後の医療情報ネットワーク基盤のありかたについて』
   医療情報ネットワーク基盤検討会最終報告書(案)厚生労働省 2004年８月30日
4. 『タイムビジネスに係る指針(ネットワークの安心な利用と電子データの安全な長期保存のために)』総務省 2004年11月５日