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

2003－DPS－114 (4)
2003－EIP－ 20 (4)
2003／8／28

個人情報の原本性と処理内容を保証するサービス
-- 匿名保証を中心に

神戸市外国語大学
芝 勝徳
株式会社 デジコム
川上 幸生

1. 概要

本稿における考察の対象はネットワーク上のサービスモデルである。サービスに関わる人格を

1) 個人
2) 情報処理組織
3) 本サービス提供者

の3者とし、サービスの内容の概要を

「個人が、本人の意志により自身に属する個有情報の情報提供者となるケースにおいてその情報を受領し処理する組織内で、情報が提供者おの意図した用途以外には利用されないことを第3者として保証するサービス。特に匿名性をもって処理される必要を満たすサービス」

とする。

2. 要件

サービスは以下のような要件を持つものとする。

1) 情報の原本性
情報が提供者本人の情報であることの保証

2) 処理資格/権限の限定
情報処理組織が、適切に情報を取扱える資格所有者であることの保証

3) 処理の保証
情報処理のおける取扱い行為において、取扱者、取扱日時等の情報を履歴管理し、行為の存在を保証

4) 情報提供者の許諾
情報提供者の許可した相手または行為に限って情報が取り扱われることの保証

5) 情報の漏洩防止
情報が情報処理組織外に漏洩しないことの保証

6) 第三者機関による認定
上記の保証が信頼できる第三者機関に定めるポリシー、ルールに適合していることの保証

3. 社会基盤としての個人情報の原本性と処理内容の保証

現在のネットワーク社会において情報を提供する場合、情報処理組織のアプリケーションサーバの証明、情報提供者の本人保証、提供した情報の原本性の保証など、これらはすでにPKI技術の確立により第三者機関の認証サービスとして実現されている。しかし、情報処理組織に届いた後、その情報が適切に取り扱われるかについては、何ら保証する技術もサービスも存在しておらず、提供者は、情報処理組織を信頼する以外にないのが現状である。

一方、情報処理組織である企業/行政機関に対し「情報取り扱いの適切性」を期待するニーズは高く、その保証は、電子技術的な基盤に基づいたものである必要があり、「第三者機関による保証/認定の仕組み」が社会基盤として必要となると考えられる。

本稿ではこれをネットワーク上で提供されるサービスとして実現することを仮定して考察を行った。基礎としたものはPKI技術基盤による「権限属性認証」である。CAによる個人認証、電子署名技術の応用では、本サービスが必要とする詳細な権限コントロールは困難である。そこで、本サービスでは属性認証（Attribute Authority)と属性証明書（Attribute Certificate)技術(RFC3281)を技術的基盤に置く。ただし、保証の程度については「情報提供者が十分な安心感を持つことが可能となるレベル」を実現することを目標に実装を考察することする。

4. 公開鍵証明書（PKC）を使った権限管理の問題点

属性認証／属性証明書を利用する上で、まず、通常の認証局（CA）が発行する公開鍵証明書を使って権限をコントロールした場合の問題を整理する。権限情報が変更されるたびにPKCを再発行しなくてはならない通常、PKCは1年～3年程度の有効期限にて運用されることが効率的とされているが、権限情報はそれより短いスパンで変更される事が多く、それに合わせPKCを発行した場合、工数が多く不効率となる。また、情報が公開されてしまうPKCは一般に公開される事が前提にあるので、公開したくない情報（この場合は権限）を記載できなくなってしまう。そこで、PKIの技術を前提にして、下記の特徴をもつ属性証明書(AC)が考案された。(RFC3281) 属性認証局（AA）自身も、認証局（CA）から発行されたPKCを用いて属性証明書（AC）に署名を行う

1) CAの存在が前提となっている
   ACを発行できる相手は、同じ認証ドメインのユーザに限定される
2) CAに比べて、運用形態がシンプルである
   PKCの存在が前提にあるので、AAはACの発行時に本人性の確認等の必要がない
3) ACには、公開鍵が格納されない
   属性の証明書という位置づけから、公開鍵は不要である

5. 属性証明書の利用

1) PULL モデル

CA は利用者に対し PKC を発行し、同時に、AA に対しても同じ PKC を発行する。

利用者がサービスの提供を要求すると、サービス提供者は、AA に対し利用者の AC 発行を要求する。この際、利用者の PKC を提示する。

AA は、あらかじめ登録されている権限情報より利用者の AC を発行する。

サービス提供者は、AC の権限情報に基づき、提供できるサービスを利用者に通知する。

2) PUSH モデル

AA は CA から AC 署名用の PKC を発行されている。 利用者も同じ CA から証明書を発行されている。利用者は、AA に AC の発行を要求する。

AA は、予め登録されている権限情報より AC を 発行して、利用者に返信する。利用者は, PKC と AC をサービス提供者に提示してサービスの利用を要求する。

サービス提供者は、AC から権限情報を取り出しその内容によって提供できるサービスを利用者に 通知する。

6. 情報の原本性

例えば匿名保証を行う上でも、情報提供者と個人証明ならびに情報自体の原本性は保証される必要がある。これらの保証は、すでに確立されている PKI 技術基盤による電子認証、電子署名にて行う。

7. 処理資格/権限の限定

情報提供者にとっては、情報が提供時に意図した用途（クレジットカード情報なら決済）に限って利用されることが保証されるとする。しかし、情報用途それ自体を電子的に管理する方向でのソリューションは、情報の電子化に伴う煩雑さや労力を考えると、非現実的なものになる。

そこで、本サービスでは、用途自体の管理の代替として、情報取扱い資格／権限を詳細に取り決められる仕組みと、それを職務従事者に多重化して付与した場合においても、権限属性認証により確実に管理を行える仕組みを提供し目的を達成する。

8. 処理の保証

情報の提供時から情報の取扱いにおいて、情報の参照者名、参照資格、参照形態、参照日時等を完全に監視し、取扱い行為の情報として蓄える。特に、情報へのアクセス日時については、TSA(Time Stamp Server)管理による時間証明も行う。

9. 情報提供者の許諾

もし、情報提供者が許可を与えた時に限って情報が参照されることを、文字通りシステムにて実現しようとすれば、提供者の許諾行為がその時々に求められるといった煩わしいシステムになってしまう。一方、通常、個人がなんらかの情報を提供する場合には、提供時に特定の目的が存在しており、そのケースにおいては情報の取り扱い許可を情報処理組織側に同時に与えていると解釈できる。

そこで、本サービスでは、提供者が情報を提供する際、「この目的において利用を許可する」といった意味を含んだ「属性証明書」をつけて、それを情報提供者の「取扱い許諾書」の意味として利用する。これにより、正規の情報取扱い資格者であっても、情報提供者側からの許諾書がなければ情報を取り扱えないということになる。更に、この「取扱い許諾書」に含む情報として、情報の参照回数の指定、情報の有効期限の指定等を盛り込み、より細かく提供者自身による情報のコントロールを実現させる。

10. 情報の漏洩防止

本サービスは、情報の電子的な漏洩（ファイルの持ち出しなど）を直接的に防止するものではない。また、情報受容者の人間系による漏洩（情報を口伝えする、或いは情報の印刷物を流す等）についても防止はできない。しかしながら、前述した「情報用途の限定」、「情報取扱い行為の保証」、加えて情報自体をPKI 技術により暗号化して保管することを併せた総合セキュリティー管理を行う方式にてよって、「情報漏洩防止」を実質的に実現する。

漏洩のケースとして、仮に情報漏洩を目論む人物が部外者であるならば、本サービスにより情報取扱い資格を与えられていないので、情報アクセスは一切できない。もし、情報受容機関内部の人間で、取扱い資格をもった人物が情報漏洩を目論んだ場合には、漏洩の行為が「取扱い行為の保証」により完全に履歴管理され追跡可能なシステムであることが、その人物に対して大きな抑止力を与えるだろう。更には、情報そのものもPKI 技術により暗号化されていて、万が一情報が外に持ち出せた場合においても、「取扱い資格書」と、「取扱い許諾書」の二つが整合性の取れた形で揃っていることが本サービスにて確認されないと参照できない仕組みとする。

11. 第三者機関による認定

本サービスは、保証における技術基盤を「権限属性認証」においている。この属性の具体的な例を考えると、商品購入の目的で送られてきた個人のクレジットカードの情報にアクセスできる権限属性は、そのサイト運営組織内の「ネットワーク販売担当者」であろう。ここで、その「ネットワーク販売担当者」にアクセス許可を与えるという行為を、サイト運営組織が行えるとしたらどうだろうか。それを許すということは、運営組織が自由に情報にアクセスできることに繋がり、結局は、その企業を社会的に信頼するという本サービスが存在しない状況と変わらないことになってしまう。そこで、本サービスでは、権限属性付与におけるポリシーとルール、並びにサイト運営機関が「匿名保証サイト」であり続けるためのポリーと運用規定を明確に定め、その基準に則り匿名保証の認定、監査を行う。また、権限属性（情報取扱い資格）の付与行為自体も、第三者機関として実施する。

12. サービスの適応分野

本サービスは、権限属性認証の技術基盤と、第三者機関としての匿名保証認定制度を基に構成されているため、扱う情報の種類や、業種の特異性に何ら制限を持たない。

例）ゲノム情報管理分野への適用

ゲノム解析における研究は、生命の基本を解明し、難病の克服を始めとし科学・産業・社会への莫大な波及効果が期待され、世界規模で進んでいる。この研究をより効率良く進める上では、ゲノム情報をネットワーク経由にて収集することが必須となるが、ヒトゲノム情報を集めた場合、そのゲノム情報はまさに取扱に大きな注意を要するものであり、その情報保護は、誰もが信頼できるシステムである必要がある。