e-Japan 認証基盤における認証方式とその統合化に関する一考察

道坂 修　春山 智　中山 亮　上島 康司　岩城 修

株式会社 NTT データ　技術開発本部

Email:{dousakao,haruyamas,nakayamar,ueshimay,iwakio}@nttdata.co.jp

1. はじめに

近年インターネットの普及により電子商取引や各種申請手続きや届け出等、インターネット上のサービスが発展しつつあるが、これらサービスにおける各種認証機能は不可欠となっている。

こうした背景にて、e-Japan 重点計画 [1]では各サービスに対する認証機能を社会インフラとして整備してゆく計画が進められてきた。中央官庁における官職を認証する府省庁認証基盤(GPKI)[2]や地方自治体の官職および組織を認証する地方自治体組織認証基盤(LGPKI)[3]、更には全国民を対象とする公的個人認証サービス[4]等、政府主導による PKI 本人認証基盤が整備されつつある。

また GPKI ブリッジ認証局と相互認証による接続を行う特定業務認証局が認められ、国土交通省の電子入札システムへの参加資格を認証する帝国データバンクによる認証局[5]など、本人認証の他に、主体に付帯する権限や資格等の属性の認証を行うニーズも高まっている。

一方では空港における入出国管理や物流にて本人認証にバイオメトリクス認証を導入していく動きも見られる。e-Airport[6]では搭乗券のチェックインとパスポートの本人確認を顔や虹彩といった生体的特徴を元に認証を行うバイオメトリクス認証の実証実験[7]が開始される他、米国では運転免許証やパスポートの IC カード化にあたり、生体特徴データ登録の義務化[8]やそのフォーマットの標準化[9]を行っており、本人認証方式にバイオメトリクスを用いるニーズも高まっている。

本稿では e-Japan の進展に伴い今後普及が予測される社会インフラとしての各種認証基盤の技術的課題を整理すると共に、これらの課題解決策とこれら複数の認証方式を統合する方式について考察する。

2. 各認証方式の特徴と課題

本節では、社会インフラとして見た場合の各認証方式の特徴と課題を考察する。

2.1 PKI による本人認証方式

(1)方式の特徴

当該方式は、ダイジェスト関数と公開鍵暗号の性質を利用し、電子署名とこれに対応する公開鍵証明書の有効性を検証することで、電子署名法で解釈される本人の実在性と本人の意思を認証するものである。当該方式のポイントは以下の通りである。

- 電子署名で用いる秘密鍵は IC カード等の耐タンパ装置内に管理され、秘密鍵に対応する EE 公開鍵証明書や信頼点証明書も適宜 IC カード内で管理される。またこれら情報に対するアクセスは PIN 等の IC カードへ認証を行うことで実現し、秘密鍵による署名演算や各種証明書の取得を行うことができる。**(特徴 2-1-1)**
- 用いる IC カードにおけるフォーマットやコマンド APDU やそのシーケンスは一般に標準化されておらず、認証局間で互換性がないことが多い。IC カードへのドライバ API は PKCS#11 等の規格があり、ドライバ API 間で互換性がとれる可能性がある。**(特徴 2-1-2)**
- 署名検証を行う場合、ハッシュの比較を行うだけでなく、署名に対応する鍵が有効であるかどうかを検証するため、公開鍵証明書の検証が必要である。公開鍵証明書の検証は、検証を行う者の信頼を置く信頼点証明書と当該証明書が認証関係でつながっていることを確認する認証パス構築と認証パスを構築する証明書間の各種検証（有効期間、失効確認、証明書の改竄、証明書間のポリシー制御、ポリシー制約、名前制約、鍵使用目的等）を行う必要がある。**(特徴 2-1-3)**

(2)課題

当該方式は秘密鍵の管理を厳重に行う必要があるが、特徴 2-1-1 により秘密鍵に対するアクセスは IC カードに設定される PIN を認証するケースがほとんどである。カード-端末間通信内容の傍受や、IC カードの PIN 照合が成功しカードの活性化が行われた時点で悪意のある別のプログラムがカードにアクセスした場合、なりすましが起こる可能性がある。またこれを防ぐ方法としてカード-端末間の相互認証やセキュア通信等があげられるが、いずれの場合にしても端末におけるセキュリティが十分に確保されている必要がある。**(課題 2-1-1)**

次に特徴 2-1-2 により IC カードへのアクセスはドライバ API のレベルで互換性がとれる現状であるため、複数の認証基盤の発行する IC カードを扱うためにはこれらドライバの切り替えが必要となる。また一般にドライバのインストールは IC カードとセットで行われるが、前述の理由によりこれらドライバの正当性を検証するための仕組みが必要となる。この際にコード署名検証による OS のドライバ認証機能を利用することとなるが、OS の信頼の置く認証局が必ずしも利用者の信頼の置く認証局とは限らないことやトロイの木馬等のウィルスにより OS のルート証明書ストア機能やドライバ署名検証モジュールが改竄されている等の OS そのものの正当性が信頼できないため、必ずしも安全とは言えない状況である。**(課題 2-1-2)**

また特徴 2-1-3 では検証対象証明書の信頼ドメインと検証を行う者の信頼ドメインが異なり、かつこれらドメインが相互認証関係にない場合、検証対象の信頼ドメインが検証者にとって信頼できるものであるか、その判断が難しい。**(課題 2-1-3)**

さらに両者が相互認証関係にある場合、認証パス構築と認証パス検証を行い当該証明書の検証を行うが、以下

の課題がある。**(課題 2-1-4)**

- 認証パス構築、認証パス検証に必要となる各種認証情報(認証局証明書、失効リスト等)の取得先が各認証局によって特定できない場合がある。また取得先のリポジトリは認証を行わないことが多く、リポジトリの成りすましによる認証妨害が起こる可能性がある。
- 失効確認は失効リスト(CRL)の取得か OCSP レスポンダへのオンライン失効問い合わせを行う二つの方法が用意されているが、CRL 取得の場合 CRL ダウンロードコストがかかる他、定期発行のための失効タイムラグが発生する可能性がある。
- 認証パス構築および認証パス検証を行う場合、検証者の信頼点証明書が信頼できるものであることが前提となる。IC カード等により検証者の信頼点が置き換えられていないことが保証されている必要がある他、更新を含め信頼点証明書が失効していないことを検証者は常に確認しておく必要がある。

2.2 属性認証方式

(1)方式の特徴

当該認証方式は現時点では標準がなく、属性を本人と見立て本人認証方式を流用するケースが多い。例えば、弁護士等の資格を認証する場合、PKI の本人認証を利用し、資格保有を記載した公開鍵証明書を発行、当該証明書による電子署名を検証することで資格認証を実現する方法が考えられる。

また近年では属性そのものを証明する属性証明書を利用した属性認証方式も検討されている[10]。属性証明書は属性を証明する属性認証局から発行され、本人の所有する公開鍵証明書とペアで使用される。属性証明書における属性の記述は基本的に自由であり資格等の属性を保有している旨の内容が記載される。属性の認証は PKI による本人認証とセットで行われ、属性証明書の有効性検証は PKI による公開鍵証明書の検証に準じる。

(2)課題

当該方式は、PKI による本人認証と類似するため基本的にはそれと同様の課題を持つ。当該方式を PKI による本人認証方式を流用している場合、属性毎に公開鍵証明書とこれに対応する秘密鍵を管理する必要があり、利用者にとって管理コストがかかる問題がある。また本人認証を兼ねる場合、属性のよりどころとなる情報が変わった場合、証明書が失効し、本人を認証する手段が一時的に失われる等の、利便性の問題がある。**(課題 2-2-1)**

また属性証明書を使用する認証方式の場合、上記課題は解決できる反面、属性証明書の表す属性の内容が冗長であることから、属性の内容確認が一意にできない可能性がある。**(課題 2-2-2)**

2.3 生体情報による本人認証方式

(1)方式の特徴

当該方式は、予め本人のものとして登録してある生体特徴データ(テンプレート)と認証時にスキャンした生体特徴を統計的手法等によりその類似性を比較することにより本人認証を行う方式である。PKI 等の方式では本人をその所有物や記憶に置き換え認証を行うのに対し、当該認証方式は本人しか持ち得ない生体的特徴を利用するため、非常に厳密な本人認証方式と言える。

当該方式は PKI と比較し、以下の特徴がある。

- 使用する生体的特徴が指紋、顔、虹彩等様々であり、かつ同じ種類の生体的特徴であってもそれを実装するベンダ毎に照合アルゴリズムや生体スキャナ・ドライバ等が異なり互換性が取れないこと。**(特徴 2-3-1)**
- 照合の結果として、本人であるのに拒絶・失敗するケース(本人拒否誤り)や本人であるのに誤って他人に照合してしまうケース(他人受入誤り)など、100%正しいとは限らないこと。またその精度が認証に用いる生体情報の種類やそのアルゴリズムや照合時の生体のコンディション(体調や慣れ、気候など)等の要素に依存することや、照合アルゴリズムに設定するしきい値などのパラメータにも依存すること。**(特徴 2-3-2)**
- 生体特徴は PKI による秘密鍵とは異なりその主体の生命が続く限り基本的に不変であることから、当該方式で使用するテンプレートは盗聴・漏洩されることのないよう厳重に管理しなければならないこと。**(特徴 2-3-3)**
- 上記性質により PKI による認証とは異なり認証を行うプレーヤと認証対象間で直に認証を行う必要があること。**(特徴 2-3-4)**

(2)課題

当該方式は、特徴 2-3-1・特徴 2-3-2 により、使用する生体的特徴やアルゴリズム、認証条件によってその信頼性が異なる。各アルゴリズムについては日本規格協会で精度評価の標準化を検討[11]されてきているが、使用するアルゴリズムや設定されるパラメータの組み合わせによる認証精度やその安全性について客観的証明を行う共に、認証そのもののフレームワークを標準化する必要があると考える。**(課題 2-3-1)**

次に特徴 2-3-1 により、課題 2-1-1 および 2-1-2 と同様の観点で生体スキャナやドライバに対する安全性も証明できる必要がある。**(課題 2-3-2)**

また特徴 2-3-3・特徴 2-3-4 により、認証を行う認証者と認証対象である被認証者の二者間で直接認証を行う必要があるが、第三者に対し当該方式で認証された事実を客観的に証明することができない。また照合に用いるテンプレートは IC カード等の耐タンパ装置で管理されるものであり、通常は認証を行う端末と IC カード間で照合を行うため、ネットワーク越しの第三者がこれによる認証を行うことが困難である。(**課題 2-3-3)**

2.4 その他課題

これら認証方式はそれぞれ独立しており、サービス提供者はどの認証方式による認証を使用するべきかまたそれをどのように組み合わせればよいか、その判断が難しい。また認証のフレームワークがサービス毎に異なるため、認証を必要とするサービス間の連結が困難である。**(課題 2-4-1)**

またサービスを連携させる場合、現状では各サービスで独立しており、連携するサービスの前後でどのような認

証が行われたのかを相関するサービス間で確認できる必要がある。**(課題 2-4-2)**

またそれぞれの認証方式を商取引に適用する場合、認証方式の欠陥や運用による事故に対する損害補填が必要になると考えられるが、認証基盤毎に損害補填に対する制度や考え方が異なる。これより求められるセキュリティレベルやそのリスクに応じた認証が必要となる。**(課題 2-4-3)**

3. 提案方式

3.1 解決のアプローチ

上記における課題に対し、以下の要件を満たす認証プラットフォームを提案する。

- **要件 1：**認証対象者の端末が信頼でき、同端末にて安全に認証を行うことができる。**(課題 2-1-1,2-1-2,2-3-2,2-3-3)**
- **要件 2：**認証方式に依存することなく第三者に認証結果を客観的に証明することができる。**(課題 2-4-2)**
- **要件 3：**サービス提供者の認証に関するコストを抑え、認証に求められるセキュリティレベルに応じた認証方式を選択できる。**(課題 2-4-1,2-4-3)**

要件 1 は、各認証方式に共通して見られる課題である端末のセキュリティを向上させるものである。利用者の認証環境（認証を行うソフトウェアやドライバ、IC カードや生体スキャナ等のハードウェア）の正当性を認証することで端末のセキュリティを向上させるアプローチである。本稿では各認証方式のドライバやハードウェアのセキュリティが万全であることを前提に認証を行うソフトウェアの正当性を認証する方式を提案する。

要件 2 は、認証を必要とするサービスが自ら認証を行うのではなく、要件 1 を条件として利用者の端末上で認証を実行しその結果をそのサービスおよび第三者に証明するものである。本稿では、サービスが信頼を置く認証代行者によって利用者端末上で認証を実行、その結果を認証代行者が証明する方式を提案する。

要件 3 は、前述の要件を加味し、サービスの求める認証条件を理解しこれに対応する適切な認証方式を認証代行者が選択し認証を行うことでサービス提供者の認証コストを低減させるものである。本稿では、認証に関わるプレーヤを整理し上記の目的を満たす認証モデルと認証手順を提案する。

3.2 認証モデル

提案方式では、利用者と認証代行者、サービス提供者、TTP の四者から構成され、以下のモデルによる認証を実現する。

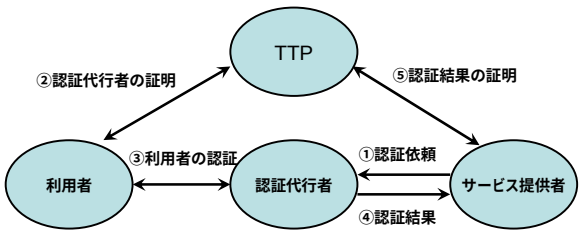

図 1 認証モデル

(1)サービス提供者

サービスの種類に応じて利用者に対して認証代行者を通じて認証を行う。本モデルにてサービス提供者は認証プラットフォームの提供する認証サービスに対してその運用を認証局に見られる CP/CPS 等の運用規定を十分に理解し、信頼を置く必要がある。

また認証代行者による認証結果を同プラットフォームの提供する TTP による証明を利用し正しく認証が行われたかどうかを検証する必要がある。

(2)利用者

サービスを利用する利用者はサービスへのアクセス時にサービス提供者から提示される認証条件に従い認証代行者からの認証を受ける。

また利用者は認証代行者の提供する認証エージェントのセットアップおよび実行に対し、認証エージェントが安全であるかどうかを検証する必要がある。

利用者もサービス提供者と同様に認証プラットフォームの運用規定を理解し信頼を置く必要がある。

(3)認証代行者

認証代行者は利用者の認証を代行する認証エージェントプログラムとサービス提供者からの認証条件に応じて認証エージェントを配布する認証センタから構成される。認証センタは認証条件に応じて適切な認証エージェントを配布する。

(4)TTP

TTP は認証エージェントそのものの存在性と認証エージェントの実行した認証条件とその結果に対し、これが正当であることを利用者およびサービス提供者に証明する。

3.3 認証条件

サービス提供者が提示する認証条件は SAML[12]等認証に必要となる各種パラメータの設定のほか、以下の条件を指定する。

(1)認証条件

認証を行う内容（本人の実在性の認証、本人に付帯する属性の認証等）を指定する。認証代行者はこの情報により認証方式を決定する。

(2)方式毎の個別認証条件

各認証方式で必要となる個別認証条件を指定する。PKI の場合は、信頼点証明書や認証パス検証の条件、属性認証の場合は、PKI の条件に加え認証を行う属性の内容、生体認証の場合は使用する生体的特徴、使用するアルゴリズム、アルゴリズムパラメータ等を指定する。

(3)認証保証条件

(1)(2)にて指定する認証条件において、損害補償が必要な場合、損害補償額を指定する。

3.4 認証手順

提案方式では以下の手順で認証を行う。

(1)認証条件の提示

利用者がサービス提供者のサービスにアクセスした際に認証が必要となった場合、サービス提供者は自身の署名を付与し認証条件を指定し、利用者の認証を依頼する。

(2)認証エージェントの選択、配信

認証代行者は認証センタにて(1)にて取得した認証条件の署名検証を行った後、内容に応じて最適な認証方式とそのパラメータの選択/加工を行い、最適化した認証エージェントを利用者に提供する。

(3)認証エージェントの認証

利用者は認証センタより配布される認証エージェントに対し、TCPA[13]等のハードウェアコード署名検証を実装した端末(以下セキュア PC)上で認証エージェントそのものの認証を行う。認証用エージェントに付与されるコード署名と TTP より発行されるアプリケーション証明書に対し、セキュア PC 上に設定される信頼点証明書との認証パス検証を行う。またアプリケーション証明書の有効性確認は当該証明書を発行する認証局へ自ら問い合わせを行う。

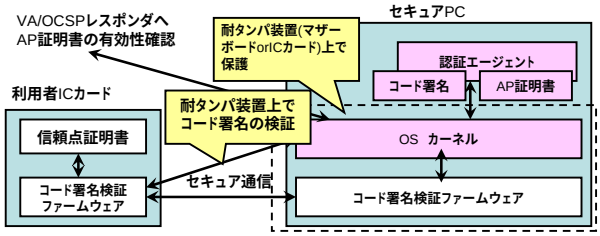

図 2 認証エージェントの認証

(4)認証エージェントによる認証

認証エージェントは認証センタから指示された認証条件に従い利用者を認証する。認証エージェントの実行においてもセキュア PC 上のコード署名検証を行い正当性を確認すると共に、認証エージェントの使用するドライバに対してもその正当性を同様の手法により検証する。ドライバにおいては IC カードや生体スキャナの正当性を検証するため相互認証を行う。

また利用者にて認証エージェントの要求する条件(認証方法に対応する IC カードや生体スキャナの有無等)を満たすことが出来ない場合は認証失敗とする。

(5)認証結果の返却

(4)にて認証した結果を認証エージェントおよび利用者による電子署名を付与し認証代行者を経由してサービス提供者に返却する。認証結果は成功/失敗の結果の他に、前述の認証条件や認証に使用したプログラム情報等を記述し、認証結果の客観性を確保する。

(6)認証結果の認証

サービス提供者は(5)にて返却された結果に対し認証エージェントおよび利用者の電子署名を検証する。

3.5 個別の認証方式についての考察

(1)PKI による本人認証方式

課題 2-1-3 は認証対象の認証ドメイン(信頼点証明書)をどのような基準で信頼するか、最終的には認証を行うサービスに委ねられる。このため、上記のようなケースの場合、サービスが認証代行者に対し予め信頼を置く認証局を複数登録しておく必要がある。また信頼を置く基準として認証条件に指定する保証条件を考慮し、保証条件を満たす認証ドメインを信頼する運用も考えられる。

(2)属性認証方式

課題 2-2-2 は属性証明書における属性表現の冗長性が課題となるが、属性認証局が単一属性のみを証明する場合、例えば弁護士属性認証局の発行する属性証明書は属性の記述を参照しなくても弁護士資格の保有を証明するものであるならば、その属性の認証にあたり属性証明書がその属性認証局により発行されたことを確認すればよい。属性認証局が複数の属性を証明したり、属性における数量や程度等を証明する場合、認証代行者にて認証局毎の属性表現のパターンを登録し、認証局毎にパターンに応じた属性内容の認証を行う必要がある。

(3)生体情報による本人認証方式

課題 2-3-1 に示す通り、各アルゴリズムの信頼性の評価と認証フレームワークの標準化が必要となるが、提案方式では各アルゴリズムで用いる環境(ドライバ、生体スキャナ、テンプレートの様式)や処理手順が公開され、その信頼性を客観的に評価できることを前提としている。認証フレームワークにおいては各アルゴリズムの識別と処理手順の切り替えが必要になると考えられる。

4. おわりに

本稿では、各認証方式の技術的課題とその解決策、そしてこれらを統合するための認証プラットフォームの仕組みを提案したが、クライアントにおける十分なセキュリティ確保と認証プラットフォーム全体の運用、そして TTP としての監査条件についてはさらなる十分な検討が必要である。今後はこれらの技術動向と法整備動向を留意し、同プラットフォームの検討を進めていく予定である。

またこれら認証を行う上で個人を識別するための個人情報を管理していく必要があるが、個人情報保護の観点でその取り使いについて十分な留意が必要である。

参考文献

[1]:高度情報通信ネットワーク社会推進戦略本部,e-Japan 重点計画, 2001 年 3 月
[2]:総務省行政管理局,政府認証基盤,
http://www.gpki.go.jp/
[3]: 総合行政ネットワーク運営協議会, 地方自治体における組織認証基盤,http://www.lgpki.jp/
[4]:総務省,「地方公共団体による公的個人認証サービス制度の創設について」,
http://www.soumu.go.jp/s-news/2002/020228_3.html
[5]:帝国データバンク,電子入札用電子認証サービス,
http://www.tdb.co.jp/ca/index.html
[6]:NAA, e-Airport,http://www.e-airport.jp/ja/
[7]:日本航空システム,プレスリリース(第 02013 JGN 号)
[8]:米国下院, “Enhanced Border Security and Visa Entry Reform Act of 2001”(国境警備強化・ビザ入国改正法案)
[9]:IBG, “Background on Biometrics Standards”,
http://www.biometricgroup.com/e/biometric_standard.htm
[10]:IETF, “An Internet Attribute Certificate Profile for Authorization”(RFC3281),
http://www.ietf.org/rfc/rfc3281.txt
[11]:日本規格協, JIS-TR X0053「指紋認証システムの精度評価方法」等
[12]:OASIS,” Security Assertion Markup Language (SAML)”,
http://xml.coverpages.org/saml.html
[13]:”Trusted Computer Platform Alliance”,
http://www.trustedpc.org/