中澤ゼミ

公的個人認証サービスにおける認証局の在り方

A1200309 大竹康雅

1 はじめに

インターネットの普及に伴い，電子データはビジネスや日常生活において不可欠な存在になっている．しかし，ネット上でのデータ通信では，配送経路上で第三者に盗聴あるいは改竄される可能性もある．それに加えて，データを渡したという証拠がなければ，事実や内容の事後否認が起きる危険性がある． このような危険を排除するためのシステムとして電子署名，電子証明書が利用されている[1][2].

本研究では，この電子署名，電子証明書のメカニズム，利用例，それに加えてＧＰＫＩ，ＬＧＰＫＩなどの公的認証基盤について調査し，これらを踏まえて個人による電子契約，電子申請などのオンラインサービスの利便性を高めるために，公的個人認証サービスにおける電子証明書の検証者範囲の拡大と，それに伴う民間認証局と公的認証局の新しい在り方を提案する.

2 電子署名システム

一般的に，重要な文書を扱う場合には文書に署名[1]を施す．署名の有無により，文書を閲覧する人はそれが署名された本人によって書かれたものであること，および署名されてから見るまでの間に内容が書き換えられていないことを確認できる.

ネット上で電子データを活用する場合にも，これと同じメカニズムが必要になってくる．そのための技術が電子署名である[2]．ネット上では改竄，なりすましという脅威が常に存在するために，電子署名により文書の真正な成立，つまり本人性[2]，非改竄性[3]，否認防止[4]の担保をしている．この技術は公開鍵暗号方式を利用することで実現されている.

2.1 公開鍵暗号方式[3]

公開鍵暗号方式は本人が秘密に持つ秘密鍵と，広く公開する公開鍵の鍵ペアによって実現されている．鍵ペアを構成している2本の鍵は互いに数学的に密接な関係があり，公開鍵と秘密鍵をそれぞれ個別に作ることはできない．このため，鍵ペアを構成する一方の鍵で暗号化したメッセージは，もう一方の鍵でしか復号化できないという特性を持っている.

2.2 電子署名の送受信[4]

ここでは公開鍵暗号方式を利用した，具体的な電子署名の送受信プロセスを説明する．電子署名の送受信プロセスは，送信する文書やメッセージを送信者が秘密鍵で暗号化することから始まる．ただし，元のデータをそのまま暗号化するのではない．送信者はハッシュ関数と呼ばれるプログラムを使い，文書やメッセージを圧縮した小さいデータを作成する．ハッシュ関数プログラムは，任意のビット長の情報を固定ビット長の情報に変換するプログラムである．このプログラムは，変換後の情報から変換前の情報を復元することが不可能な一方向の変換機能を持つ．圧縮したデータはメッセージダイジェストと呼ばれ，圧縮によってデータ量が小さくなっているため，元のデータをそのまま暗号化，復号化するよりも時間がかからない．送信者はメッセージダイジェストを自分の秘密鍵で暗号化する．この手順が電子署名の作成プロセスの送信者側の手順である．ここで暗号化したデータが電子署名であり，これを文書やメッセージに添付して送信する.

次に受信者側の手順を説明する．受信者は，送信者の公開鍵で受信した電子署名を複号化し，メッセージダイジェストを取り出す．また受信した文書からも自らメッセージダイジェストを生成する．そして，2つのメッセージダイジェストを比較し，一致すればその電子署名は公開鍵に対応する秘密鍵で暗号化されたものと確認できる．つまり，この秘密鍵は送信者本人だけが持つものであるため，間違いなく本人が送信したものであるという一連の手続きによって本人性が保たれる.

そのことに加えて，送信時と受信時に同じメッセージダイジェストが生成されたことを検証できれば，伝送途中で改竄されていないことが確認でき，受信者は電子署名を偽造できないので，受け取った文書を受信者自身が改竄することもできない．また，送信者，受信者ともに同じメッセージダイジェストを持っているため，後になって否認することもできない.

2.3 電子証明書[2]

電子署名システムでの受信者は，文書，電子署名と共に送られてきた送信者の公開鍵で電子署名を復号化する．しかし，送られてきた公開鍵自体が本人のものでない場合，電子署名の真正性は成り立たない．例えば，第三者が本来の送信者の名前だけを偽り，異なった秘密鍵，公開鍵を使った場合でも，受信側では送信者本人の電子署名であると判定されてしまう.

このような問題を防ぐためには，電子署名が確かに本人のものであるという証明が必要になる．しかし，扱う文書と電子署名は毎回異なるため，電子署名そのものを証明することはできない．そこで，代わりに1つしか存

---

[1] 日本では捺印,欧米などではサイン
[2] 確かに本人が書いたという性質
[3] 第3者に書き換えられていない性質
[4] 文書の通信後に，送信の否定ができない性質

在しない公開鍵を証明する．このような電子的な証明書が電子証明書である．例えて言えば，印鑑証明書に相当する．

3 認証局

3.1 認証局の業務[4]

3.1.1 個人認証と法人認証

電子証明書は認証局と呼ばれる機関が発行する．認証局は証明書発行依頼者(被証明者)を調査し，依頼者の身元と依頼内容に間違いないことを確認したら証明書を発行する．これは個人，法人に対して行う場合がある．

この認証局は電子証明書発行の他に，個人のための電子署名も作成している．電子署名の作成には秘密鍵と公開鍵の鍵ペアが必要となることは前述した．このように作成された秘密鍵は，個人により保管されることになり，もう一方の公開鍵は個人によって保管される場合やサーバに保管される場合がある．加えて，公開鍵には認証局により電子署名が施され，登録，電子証明書の発行がなされる．そして，ここで作成された電子署名により本人確認が行われ，電子証明書の発行により電子署名の証明がなされる．このような流れにより本人性の証明をすることが認証であり，それを個人に行うことが個人認証である．

さらに，認証局は一般の民間企業に対して電子署名システムを構築する業務も行っている．この業務は一般の民間企業が個人に電子署名，電子証明書を利用したサービスを円滑に提供できるようにするためである．例えば，一般の民間企業が個人に対して電子申請や電子契約などのサービスを提供したい場合，電子署名システムの構築が必要となる．具体的には電子署名により一般の民間企業と個人が相互認証するシステムや，電子申請書，電子契約書などに添付する電子署名の検証システムなどである．これらのシステムを構築する際に，認証局が一般の民間企業に対して電子署名と電子証明書を発行し，結果的に法人認証することになる．個人はその法人の電子証明書を確認することで，その民間企業が提供している電子申請や電子契約などのサービスを受けることができる．

3.1.2 失効情報

秘密鍵を盗まれたり，紛失した場合[5]や電子証明書の有効期限が切れた場合は，その電子証明書を無効にする必要がある．このような無効になった電子証明書の情報は失効情報と呼ばれ，その失効情報とサービスに利用された公開鍵の情報を照らし合わせ，電子証明書の有効性を確認する．この失効情報は認証局が管理している．

[5] 秘密鍵が盗まれると公開鍵の有効性が失われてしまうため

3.2 民間認証局と公的認証局

電子署名の作成や電子証明書の発行，管理などの業務は，民間企業が運営する民間認証局によって始められた．このような経緯から，現在でも基本的には民間認証局よりその業務が行われている．政府はこのような民間企業に比べて情報化が遅れていたこともあり，１９９４年より政府の情報化推進を始めた．この取り組みにより，政府や地方公共団体でも電子署名作成や電子証明書の発行，管理などの認証業務を行える基盤を構築してきた．現在では公的認証基盤により個人，法人ともに認証できるようになり，行政手続きなどがオンライン化されている[5]．しかし，現在の公的認証局の在り方は民間認証局との関係もあり，電子証明書を利用したサービスの利便性とサービス水準向上の足かせとなっている部分がある．

4 電子政府･電子自治体における認証局と認証基盤

基本的に電子証明書は民間認証局が発行，管理していると前述したが，ここでは公的認証局による電子証明書の発行，管理について詳しく説明する．

4.1 日本政府認証基盤[6]と地方公共団体組織認証基盤[7][5] [6] [7]

ＧＰＫＩでは各省庁が「府省認証局」と呼ばれる電子認証局を設置し，主として官職[8]に対して電子証明書を発行する．また，各府省認証局の間にブリッジ認証局[9]が介入し相互認証する．ＬＧＰＫＩでは都道府県及び市町村等の地方公共団体が「都道府県域認証局」と呼ばれる電子認証局を設置し，府省認証局の場合と同じく官職に対して電子証明書を発行する．これらのようなＧＰＫＩとＰＫＩは結合され，電子政府，電子自治体を実現する基礎となっている．

ＧＰＫＩとＬＧＰＫＩはインターネットとは別のネットワーク，総合行政ネットワーク[10]で接続されている．総合行政ネットワークとは国と地方公共団体間だけで接続され，インターネットとは直に接続されないので外部からのアクセスはできない．また，ＧＰＫＩの認証局とＧＰＫＩの認証局は，ブリッジ認証局が介することで相互認証されている．相互認証とは認証局同士が保証し合い，システム的にも相互に証明書を検証できる仕組みである．図１のブリッジ認証局と各府省認証局がそれぞれ異なる認証局から電子証明書の発行を受けている場合を考える．ブリッジ認証局は相互認証により各府省認証局を認

[6] GPKIともいう．GPKI：Government Public Key Infrastructureの略
[7] LGPKIともいう．LGPKI：Local Government Public Key Infrastructureの略
[8] 都道府県知事や市町村長などの職
[9] 相互認証するために各認証局の間に入る認証局
[10] ＬGWAN：Local Government Wide Area Networkともいう．

証しているので，各府省認証局が発行を受けている他の認証局の発行する電子証明書を，自らを認証する認証機関が発行した電子証明書と同じように信頼して扱うことができる．

図1を見ると分かるが，相互認証が行われなかった場合，最上層の認証局を設置しなければならない状況となる．簡単に言うと，最後に認証する認証局の認証ができないという問題点がある．その問題の解決策として相互認証がある．

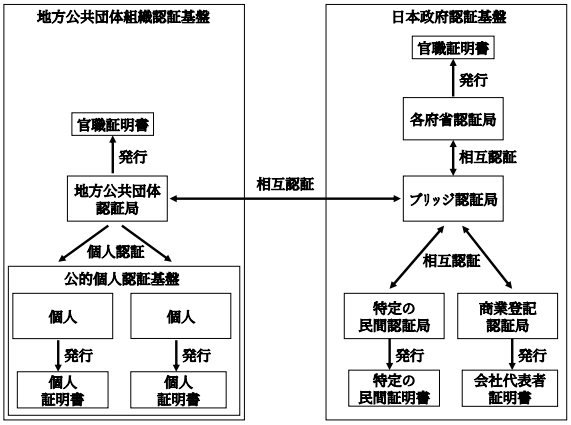

図1　公的認証基盤の関係

このように認証ＧＰＫＩとＬＧＰＫＩが相互認証により結ばれると，総合行政ネットワークで扱う情報に対して保証されていない情報は存在しないので，個人情報を安全にやり取りすることができる．

4.2 公的個人認証基盤[7][8]

行政手続のオンライン化に必要な電子認証サービスを，全国どこに住んでいる人に対しても安い費用で提供する基盤が公的個人認証基盤である．これにより，窓口に出向く必要があった行政手続が，家庭や職場からインターネットを介して可能となる．

この公的個人認証基盤の構築に大きな役割を果たすものとして住基ネット[11]があり，総合行政ネットワークでＧＰＫＩ，ＬＧＰＫＩと接続されている．この住基ネットにより個人に対して電子証明書を生成する流れができている．ここで生成された個人のための電子証明書は住基カード[12]という形で格納，配布される．なお，この基盤を利用した公的個人認証サービスは既に始まっており，個人の電子証明書（住基カード）を利用して電子申請を行える．

4.3 公的個人認証サービスと民間認証局によるサービスの棲み分けと検証者範囲

公的個人認証サービスは地方公共団体が提供するサービスで，必要な費用は電子証明書の発行手数料や税金で賄われている．ここで発行された電子証明書は行政手続きなどでしか利用できない．一方，民間で利用できる電子証明書は，既に多くの民間認証局により提供されている．このように現在では，電子証明書発行などの電子認証サービスの用途が分かれており，公的個人認証サービスが民間認証局の提供するサービスに参入することは，民間で処理可能な業務を公的機関が行う，いわゆる「民業圧迫」の事態を招きかねず好ましくない面があると考えられている[8]．

現在のサービスの棲み分けは，公的個人認証サービスにおける個人の電子証明書に関する失効情報の提供を受け，その有効性確認を行える署名検証者の範囲を限定することで実現している．その範囲は行政機関等，裁判所及び一定の条件を満たした民間認証局に限定されており，具体的には国の各府省，地方公共団体，独立行政法人や地方独立行政法人などである．これに対して一般の民間企業では，公的個人認証サービスにおける電子証明書が，本当に公的認証局が発行したかを確認できないため，この電子証明書を利用するサービスを提供することはできない．この理由は，一般の民間企業が公的認証局と相互認証しているわけではないからである．

現在では既に民間認証局が提供しているサービスと，公共団体が提供しているサービスの棲み分けを確保した制度となっている．それゆえ，現在のサービスにおいては法律の規定により，民間の業務に対して公的個人認証サービスで発行された電子証明書を利用することは認められていない．

5 新しい認証局の在り方

5.1 公的個人認証サービスにおける電子証明書の検証者範囲の拡大

ここでは民間認証局にも公的個人認証サービスにおける失効情報を与え，電子証明書の検証者範囲を拡大し，民間認証局が公的認証局と一般の民間企業との架け橋となる新しいシステムを提案する．

まず，公的認証局である都道府県認証局と民間認証局の仲介役として民間認証局を位置づけ，民間認証局と都道府県認証局とが相互認証できるようにする．これにより，お互いが電子署名した電子証明書の有効性を確認することが可能となる．次の段階として，一般の民間企業が個人に対し電子申請，電子契約などのサービスを提供する際に，民間認証局へ失効情報の問い合わせをすることになる．その問い合わせを受けた民間認証局は，一般の民間企業の代わりに公的個人認証サービスにおける失効情報を都道府県認証局に問い合わせ，電子証明書の有効性確認をする．

これに加えて，一般の企業に電子署名システムを提供するという従来の業務も続ける．しかも，提供価格を

[11] 住民基本台帳ネットワークシステムの略
[12] 住民基本台帳カードの略

安価にすることが可能となる．この理由は後ほど述べる．このような執行情報の提供と既存の電子署名システム構築が民間認証局における業務である．このことにより公的個人認証サービスによる電子証明書の検証者範囲は拡大し，個人は民間でも公的個人認証サービスによる電子証明書が利用できる．図1にその概要を示す．

図2を見ると総合行政ネットワークとインターネットの二つのネットワークが使用されていることが分かる．これは総合行政ネットワークと一般の民間企業が直接インターネットで接続されると，インターネット上で盗聴の危険やハッキング，ウィルスによる攻撃などが発生しセキュリティ面で弱い．そのため民間認証局がインターネットと総合行政ネットワークの緩衝地帯の役割を果たしている．それに加えて間に民間認証局を置き公的認証局と相互認証することで，公的認証局の規定した条件が適用され，失効情報管理を既存のシステムと同等のレベルで行うことができる．

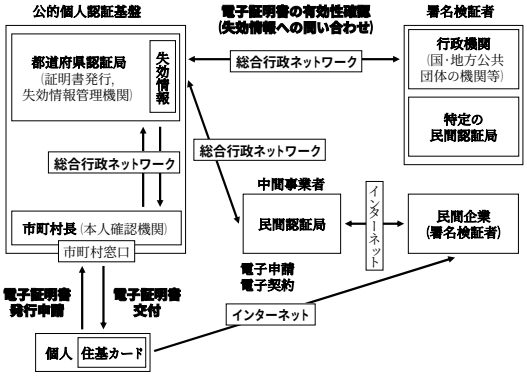

図2　公的個人認証サービスにおける電子証明書の検証者範囲を拡大した場合の認証局の位置と情報の流れ

5.2 公的個人認証サービスにおける電子証明書の検証者範囲を拡大する意義

現在，個人が受けることのできる電子証明書を利用したサービスは，公的なサービス以外に民間のサービスも存在する．この場合，個人により民間認証局に電子証明書を発行してもらう負担が大きい．この負担とは個人で初めて電子証明書を発行してもらう不安，調査･契約･維持にかかる費用の高さなどである．費用が高くなる理由として，電子証明書を発行するシステム構築の初期投資が大きいことや，利用者が少ないことがあげられる．初期投資におけるコストは，全てに関与する人件費，電子署名システム構築，電子署名の作成（秘密鍵と公開鍵の作成），電子証明書の発行，公開鍵の登録，管理，失効情報の管理などにより発生する．

本研究で提案した公的個人認証サービスにおける電子証明書の検証者範囲の拡大により，前述した問題が解決できる．民間認証局の初期コストの要因となる業務を公的個人認証サービスに任せることで，大幅にコストを下げることができる．そのコストを下げることができれば，一般の民間企業に対しての公的個人認証サービスにおける新しい電子署名システムの構築などのサービス提供，いわゆる法人認証などの提供価格を下げることができる．結果として電子署名システムを導入し，個人にサービスを提供する一般の民間企業も増加する．これにより民間認証局の利益増大，個人の電子証明書を利用したサービス水準の向上，公的個人認証サービス利用者の増加が期待でき，「民業圧迫」という懸念も解消される．

6 結び

本研究では公的個人認証サービスにおける電子証明書の検証者範囲の拡大と，それに伴う民間認証局と公的認証局の新しい在り方を提案した．この提案により電子証明書の敷居を下げ，その電子証明書を利用した個人による電子申請，電子契約などのオンラインサービスを，安価に受けることができる．このことに加えて，電子証明書を持つ個人が増加すれば，一般の民間企業がサービスを提供する意義も広がり，サービス水準も向上し，より便利になるだろう．しかし本研究で示した提案にも発展の余地や問題点がある．提案したシステムでは，民間認証局，公的認証局，一般の企業と連結しうる数，形態が多いので，ビジネスの可能性も大きいといえる.それに伴い，情報の流れなどが複雑化しそれぞれの業務内容，効率の面に問題が生じてくるだろう．加えて，公的な団体も関与していることもあり，ビジネス形態の変化などに対する法的対応の問題などを解決する必要がある．

参考文献

[1]谷口功，よくわかる暗号化技術，入門ビジュアルテクノロジー，pp.74-89，2000.9.

[2]熊谷誠治，誰も教えてくれなかったインターネットセキュリティのしくみ，日経インターネットテクノロジー，pp.95-97/128-150，1999.5.

[3]結城浩，暗号技術入門，ソフトバンク,2003.9.

[4]塚田孝則，企業システムのための PKI～公開鍵インフラストラクチャの構築･導入･運用～，日経 BP 社，2001.12.

[5]http://www.gpki.go.jp/，政府認証基盤(GPKI)，総務省 行政管理局.

[6]株式会社 NTT データ研究所，電子契約導入のすすめ，ソフト･リサーチ･センター，2004.4.

[7]インターネット電子申請，電子申請推進コンソーシアム，Ohmsha，2004.6.

[8]http://www.jpki.go.jp/，公的個人認証サービスポータルサイト，公的個人認証サービス都道府県協議会.