電子政府・電子行政

～セキュリティ向上を目指して～

藤田 佳久，荒久田 博士
Yoshihisa FUJITA，Hiroshi ARAKUTA

1　はじめに

近年，インターネットの普及を始めとする IT の急速な進歩によって，人々のライフスタイルのみならず社会の構造そのものが大きく変化している．社会全体の IT 化に付随して，高速インターネット回線の低価格化が急激に進んだ．また，企業のみならず一般家庭にも高速インターネット回線が普及し，様々なサービスがインターネット上で利用できるようになった．行政とのやり取りに関してもオンライン化が積極的に進められている．

行政のオンライン化として，行政情報を電子情報として国民に提供することにより，行政サービスの向上を目的とした電子行政がある．本発表では，現在行われている電子行政サービス，電子行政に関する問題点，基盤技術を説明し，次世代暗号技術に関して発表する．

2　電子政府・電子行政

2.1　目的

電子政府・電子行政は，コンピュータやネットワークなどの情報通信技術を行政のあらゆる分野に活用することを目的としている．それらにより，国民に対する各種行政サービスの利便性向上（24 時間行政サービス等），業務効率改善による行政コストの削減，行政 IT 化に伴う経済産業の復興が期待されている．

2.2　住民基本台帳ネットワークシステム

現在行われている電子政府・電子行政サービスとして，住民基本台帳ネットワークシステム（以下，住基ネット）がある．住基ネットは，氏名・住所・性別・生年月日の４情報と住民票コード[1]により本人確認ができるシステムである．このシステムにより，以下のサービスが受けられる．

- 住民票の写しを必要としない行政申請
- 住民票の写しを全国どこからでも受取可能
- 転入・転出届の一本化

住基ネットにおける本人確認方法は，住基ネット IC カードを用いる．現在，住基ネット IC カードは，行政機関のみで利用可能であり，民間企業間での利用はできない．

[1]住基法に基き住民に付与される 11 桁のコード情報

2.3　問題点

電子政府・電子行政には，以下のような問題がある．

- セキュリティの確保

  ユーザ端末と受付システムとの接続時の通信の安全が確保されなければならない．通信経路上でのデータに対しては，盗聴，改竄，なりすまし，事後否認といった問題に対する対処が必要となる．特に住基ネットにおいて，住民票コードを盗難・盗聴される事態に対処して，なりすましを防ぐ本人認証技術が必要である．

- 情報の標準化

  情報が電子化されて，相互利用可能な状況になるためには，情報の標準化が必要である．標準化が行われない状況で電子化が進行すると，相互に読み取り不可能な情報が多量に発生して，混乱が生じてしまう．

3　基盤技術

電子政府・電子行政の問題点を解決する技術として，以下のようなものがある．

3.1　PKI

PKI(Public Key Infrastructure：公開鍵基盤) とは，公開鍵暗号方式に基づいて構築された．電子化された申請書に対する脅威（盗聴，改竄，なりすまし，事後否認等）から守るインフラ技術である．公開鍵暗号方式により，盗聴や電子文書の改竄が行われていないことが証明される．また，認証局が発行する電子証明書により，通信相手 (公開鍵の持ち主) が本人であることが証明される．日本政府における認証機関を GPKI(Government PKI) という．PKI の主な構成要素として以下の３要素がある．Fig.1 に PKI の概要を示す．

- 認証局 (CA：Certification Authority)

  ユーザに対して，公開鍵と対応する秘密鍵の所有者を結びつける証明書を発行する．発行した証明書の信頼性が失われた場合は，その証明書を失効させ，証明書失効リスト (CRL:Certificate Revocation List) を発行する．証明書利用者が取得できるように，証明書と CRL をリポジトリに公開する．

- リポジトリ

  CA が発行した証明書や CRL を格納する．証明書や CRL を証明書利用者が検索して取得をできるようにする．

- アーカイブ

  電子署名の長期保存に適用するため，有効期限が切れた証明書や CRL を保持する．暗号目的で利用される秘密鍵のバックアップを行う．

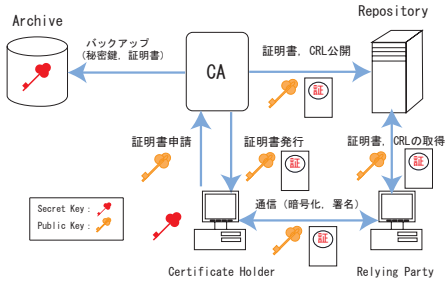

Fig. 1　PKI

4　次世代暗号技術

公開鍵暗号方式において，秘密鍵は厳重に保管する必要がある．秘密鍵が漏洩すると，その秘密鍵の所有者に対するなりすましが発生し，不正申請など電子認証システムの信頼が大きく損なわれてしまう．そこで，秘密鍵が漏洩して署名が偽造されても，署名偽装を検知可能にするなどの秘密鍵漏洩を前提とした署名偽造対策技術の研究が現在進められている．その次世代暗号技術のひとつとして「MAC(Message Authentication Code) 付きディジタル署名」がある．

4.1　MAC 付きディジタル署名

MAC 付きディジタル署名とは，ディジタル署名に加えて，MAC 値を用いて署名偽造の検知を行う技術である．MAC 値とは，MAC 生成用秘密鍵とデータを元に固定ビット長の出力を計算する関数である．MAC 生成用秘密鍵とは，ハードウェア製造時にハードウェア内に格納され，一度書込みが行われると二度と書込みができない鍵のことである．

4.2　MAC 付きディジタル署名を利用した暗号技術

MAC ディジタル署名を行うことで，署名対象データに対する MAC 値を検証して署名が生成されたハードウェアを確認できる．署名検証者からの MAC 値と署名生成者からの MAC 値が一致すれば，ディジタル署名が偽造されていないことを示すことができる．なぜなら，署名生成者のハードウェアを入手することは非常に困難であるからである．MAC 付きディジタル署名の概要を Fig.3 に示す．

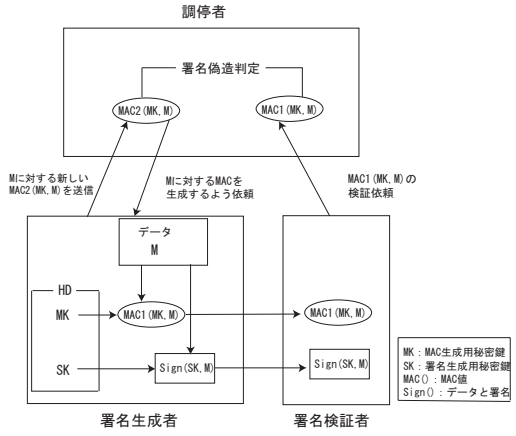

Fig. 2　MAC 付きディジタル署名

ここでの調停者とは，署名生成者と署名検証者から信頼される第三者機関であり，MAC 値の検証を行う．

5　今後の展望

現在，住基ネットに用いられている IC カードのメモリは 64Kbytes（文字情報で約 3 万 2000 文字）である．しかし，現在では 4 情報と住民票コードを読み出すだけで，これ程の高性能 IC カードは不要である．そこで将来，現在利用されていないメモリ領域を有効利用するために住基ネットは民間企業へ開放されると考えられる．住基ネットが民間企業へ開放されることで，住基ネット IC カードの中に，キャッシュカード・定期券・診察券・各種会員券・社員証などが組込まれる．また，IC カードが健康保険証や運転免許証に変わる個人証明書となる．そのことにより，キャッシュレス（電子マネー）時代が到来する．しかし，個人情報を守るセキュリティ技術が確立されていない為，実現は 20 年後ぐらいである．

電子政府構築にあたり，最も重要なことは情報管理である．今後の電子政府の発展には，セキュリティ技術の発展が不可欠となる．暗号技術が確立しなければ，電子政府は成立しない．今後の暗号技術として，量子暗号技術がある．量子暗号とは，光子の量子論的な性質を利用して通信方法で，盗聴した内容を不正確にすることができる，盗聴が受信者に判明するっといったことが可能となる暗号である．但し量子暗号技術は現在半径 100km 以内でしか通信できず，実用化のめどは立っていない．そこで，MAC 付きディジタル署名が認証技術に利用されると考えられる．

参考文献

1) デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策，日本銀行金融研究所 宇根正志，2003/6

2) PKI(公開鍵インフラストラクチャ)，エントラスジャパン 鈴木優一，2002/6