電子申請システムの概要
――電子申請システムにおける基盤技術の紹介

Summary of Electorical Application System for the Government
――Introduction of Generic Technology in Electronic Application System

飯 田 眞 弘, 城 代 優 二

要　約　政府は，高度情報通信ネットワーク社会の構築を目指して，官民共同体制にて電子政府・電子自治体の施策を積極的に進めている．その施策の重要な柱に位置付けられているのが電子申請システムの構築である．

本稿では，電子政府（e-Government）に関する様々な施策を紹介し，電子申請システムの位置付け・役割を明確にする．続いて，電子申請システムの概要を述べるとともに，システムの基盤と要素技術（インターネット・セキュリティ，電子認証，電子署名，XML 技術等）の適応について解説する．

Abstract　Japanese government is now promoting the joint government-industry program for the advanced information and telecommunications network society to establish the central and local electronic (or digital) government(e-Government). In this joint program, building of the Electronic Application System is positioned in the important strategic activities.

This paper introduces various measures for the e-Government, and defines the position and role of the electronic application system in one, and then outlines the electronic application system, as well as the infrastructures and technological elements of its system, such as Internet security, digital authentication, digital signature XML, and etc.

1. は じ め に

行政サービスの向上を目指し，政府では，2001 年の 1 月に打ち出された e-Japan 戦略[*1] に基づき，電子政府[*2] の実現に向けての動きが加速化している．日本ユニシス株式会社（以下，当社）ではこうした電子政府に向けた社会公共ソリューションとして，1999 年にコンセプト「OG 21」を発表し，官公庁向け文書管理システム「OG-DOCS」と電子申請向けソリューション「OG-APPS」を提供している．

電子政府の実現において重要な役割を担う電子申請に関しては，実証実験が積み重ねられ，その成果が財団法人ニューメディア開発協会より「インターネット電子申請システム」として公表されている．この「インターネット電子申請システム」は，インターネットによる電子申請システムの構築のための基本的なソフトウェア部品及び構築手続を体系化したものであり，当社はそのソフトウェア部品を用いて申請システムを開発し，その有効性を評価する実地検証に参画した．その適用技術を基に OG-APPS は開発されている．

本稿は，電子政府の施策について電子申請システムを中心に照会すると共に電子申請の仕組み及びそこで用いられている要素技術について説明するものである．

2. 電子政府施策の現状認識

最近「電子政府」という言葉に注目が集まっている．当社も 2001 年 10 月に開催された日本経済新聞社主催の電子政府戦略会議において特別協賛社として参画する等，積極的に電子政府対応を推進している．はじめに電子政府とは何かを紹介する．

2.1 電子政府とは

e-Japan 戦略において，電子政府について「電子政府は，行政内部や行政と国民・事業者との間で書類ベース，対面ベースで行われている業務をオンライン化し，情報ネットワークを通じて省庁横断的，国・地方一体的に情報を瞬時に共有・活用する新たな行政を実現するものである.」と述べている．具体的には，自宅や会社，サービス拠点のパソコンからインターネットの窓口を通じ，24 時間，国や地方公共団体の様々な行政情報を手に入れたり，電子的に行政手続ができるようになることを目指している．

これを推進するためには，IT 技術の活用が前提となっている．従って，電子政府の実現に向けての動きは，一言で言えば，「政府が推進する行政サービス向上を目指した IT 革命」と表現できる．政府が掲げている目標は「IT 立国の形成」であり，「IT 革命の恩恵をすべての国民が享受でき国際的な競争力を得る」としている．

2001 年 1 月には，IT 基本法に基づき，総理を本部長，全閣僚と民間等の有識者を本部員とし，官民を挙げて IT 施策を推進する IT 戦略本部が発足し，目標に「我が国が 5 年以内に世界最先端の IT 国家になる」を掲げた e-Japan 戦略を決定するとともに，具体的な行動計画を定めた「e-Japan 重点計画」[*4]，「e-Japan 2002 プログラム」[*5] を策定し，重点的かつ戦略的に IT 施策を積極的に実施している状況である．

2.2 電子政府の e-Japan 重点計画

e-Japan 2002 プログラムに至る行政の取り組みと法整備は次のように進んできている．

◇行政の取り組み

- 1999 年 10 月　ミレニアム・プロジェクト
- 2000 年 11 月　IT 基本戦略
- 2001 年 1 月　e-Japan 戦略
- 2001 年 3 月　e-Japan 重点計画
- 2001 年 6 月　e-Japan 2002 プログラム

◇法整備

- 1999 年 5 月成立　行政機関の保有する情報の公開に関する法律（2001/1 施行）
- 1999 年 8 月成立　住民基本台帳法一部改正（2002/8 施行予定）
- 1999 年 8 月成立　不正アクセス行為の禁止等に関する法律（2002/2 施行）
- 2000 年 5 月成立　電子署名および認証業務に関する法律（2001/4 施行）
- 2000 年 11 月成立　高度情報通信ネットワーク社会形成基本法（IT 基本法）（2001/1 施行）
- 2001 年成立　個人情報の保護に関する法律案（2001/12 までに成立予定）

e-Japan 重点計画では,「目指すべき高度情報通信ネットワーク社会の姿」として4項目をあげている.

① すべての国民が IT のメリットを享受できる社会
② 経済構造改革の推進と産業の国際競争力の強化が実現された社会
③ ゆとりと豊かさを実感できる国民生活と,個性豊かで活力に満ちた地域社会が実現された社会
④ 地球規模での高度情報通信ネットワーク社会の実現に向けた国際貢献が行われる社会

また,高度情報通信ネットワーク社会の実現のために特に重点的に施策を講ずべき五つの重点政策分野をあげている.

① 世界最高水準の高度情報通信ネットワークの形成
② 教育及び学習の振興並びに人材の育成
③ 電子商取引等の促進
④ 行政の情報化及び公共分野における情報通信技術の活用の推進
⑤ 高度情報通信ネットワークの安全性及び信頼性の確保

2.3 電子政府における申請システムの位置づけ

電子政府には,行政と国民,行政と企業,行政と行政という三つの区分けが考えられる.電子政府実現のイメージを図1に示す.

・G2C(Government to Citizen)
行政機関と国民
・G2B(Government to Business)
行政機関と民間企業
・G2G(Government to Government)
行政機関同士

図1は,電子政府における G2C, G2B 及び G2G の関係を示すものであるが,これについて簡単に説明する.

1) G2C

G2C は,電子申請に代表されるように,申請・届出などの行政手続のオンライン化や情報公開サービスなどが含まれ,主に住民サービスの向上を目指している.e-Japan 2002 プログラム(平成14年度重点施策に関する基本方針)では,IT 施策の柱として「電子政府・電子自治体の着実な推進」を掲げており,「申請・届出等の電子化に必要とされる地方公共団体による公的個人認証サービス等のシステムの整備等の基盤整備を着実に推進する」としている.

2) G2B

G2B の重要な柱として,G2C と同様に行政に対する申請・届出の電子化があげられる.また,電子申請以外の重要項目として電子調達(電子入札を含む)がある.電子調達の例としては,すでに旧建設省(現国土交通省)が進めている公共調達基盤システム(建設 CALS)がある.G2B での認証の対象は企業となり,公的法人認証サービスがすでに開始されている.

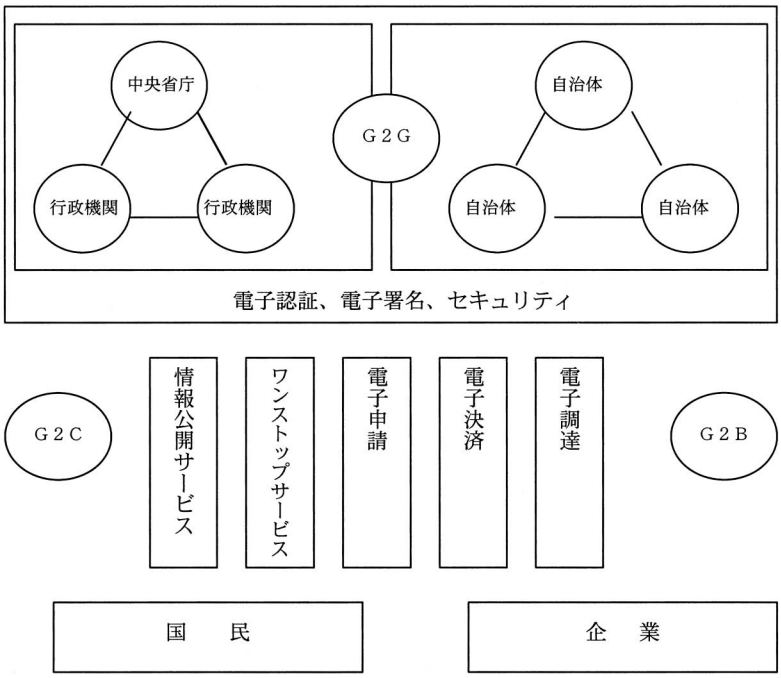


図 1　電子政府の実現イメージ

3）G2G

G2Gは，行政間における情報交換を目的としたものであり，申請手続きにおける行政間の連携業務があげられる．代表的なものとして，ワンストップサービスの実現がある．一つの目的行為に付随する申請が複数存在し，また窓口の行政機関が異なる場合，従来は，複数の申請手続きをそれぞれの窓口で行っていたが，これを一度の申請手続きで済ませようという考えである．このためには，行政間で申請情報を交換し，手続を連携させる仕組みが必要であり，行政文書の電子化が大前提となる．

上記G2C，G2Bにおいて共通しているのが，インターネットを介したIT技術の活用であり，中でも電子認証，電子署名および暗号化等のセキュリティ対策は，重要な要件となっている．

電子申請は，電子政府の実現にあたり，これらIT技術を活用する象徴的な位置づけとして存在しており，電子政府の実現に向けて整備される主要IT技術基盤が電子申請の実現のための必須要件となっている．e-Japan重点計画においては，重点項目「行政の情報化および公共分野における情報通信技術の活用の推進」の具体的な施策の一つとしてあげられている．計画では2001年度早期にアクションプランを策定し，2003年度までにオンライン化の実施及びこれを具体的に推進するための事項として，申請・届出手続の電子化に関わる共通的基盤システムを2002年度までに整備することが計画されている．ここでいう共通的基盤システムとは，府省認証システム，複数の手続の受付・結果通知等について汎用的に利用できるシステムと定義されている．

次章で汎用受付等システムについて述べる．

3. 電子申請システムの概要

3.1 基本的な仕様

ここでは，総務省の「申請・届出等手続のオンライン化に関わる汎用受付等システムの基本的仕様」（総務省）に記述された要点を簡潔にまとめ，電子申請システムに求められる要件を明らかにする．

総務省の仕様における電子申請は，複数の手続の受付・結果通知等について共通的に利用できる「汎用受付等システム」と申請システムの実現に伴う認証業務や手数料を取り扱う「その他共通システム等」の二つのシステムの整理において説明されている．

申請者とのインタフェース等，電子申請システムでの処理の流れを図 2 に示す．

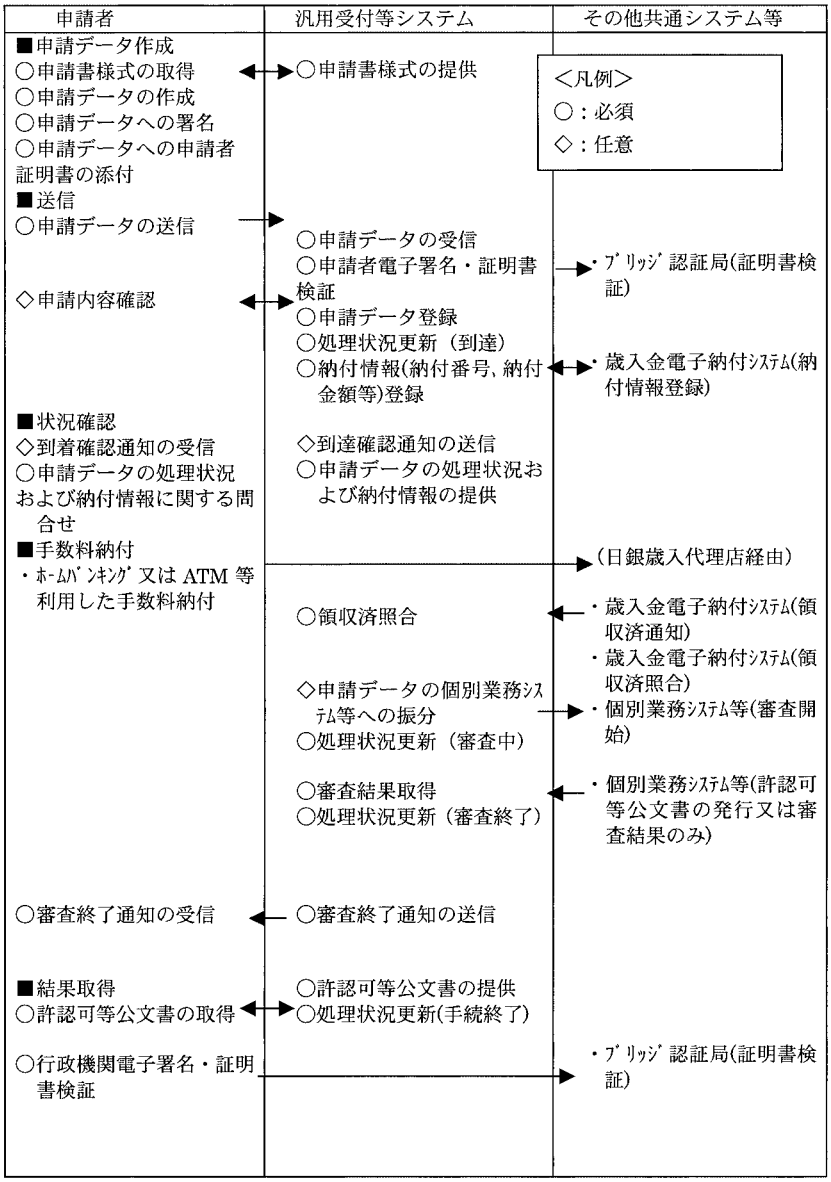


図 2　申請者とのインタフェース等

電子申請システムの最大の特徴は，インターネットを活用することである．これにより申請者への地理的および時間的格差を取り除き，会社および自宅の PC から申請・届出を行えるサービスを提供できることになる．

図 2 に示した申請者が行う処理手順を説明する．

①申請データ作成

・汎用受付等システムにインターネットにより接続し，申請書様式を取得する．

・申請書様式を利用して申請書を作成し，各手続に定められた書類を添付し申請データを作成する．

・ブリッジ認証局[*8] と相互認証[*15] している認証局[*11] の認証に基づき申請データに電子署名を付与する．

・申請者の電子署名[*16] を認証する認証局等が発行した公開鍵証明書[*10] を申請データに添付する．

②送　　信

・申請者端末から汎用受付等システムに申請データを送信する．

③状況確認

・汎用受付等システムに接続して，当該申請に係る処理状況，手数料の納付番号，納付金額等の納付情報を確認する．

・「到達」，「審査中」，「審査終了」，「手続終了」の区分で処理状況を確認する．

④結果取得

・汎用受付等システムに接続して，許認可等の公文書を取得する．

・行政機関が発行した許認可等の公文書に付与されている電子署名および官職証明書について官職証明書の有効性，電子署名の真偽，公文書の改変の有無を検証する．

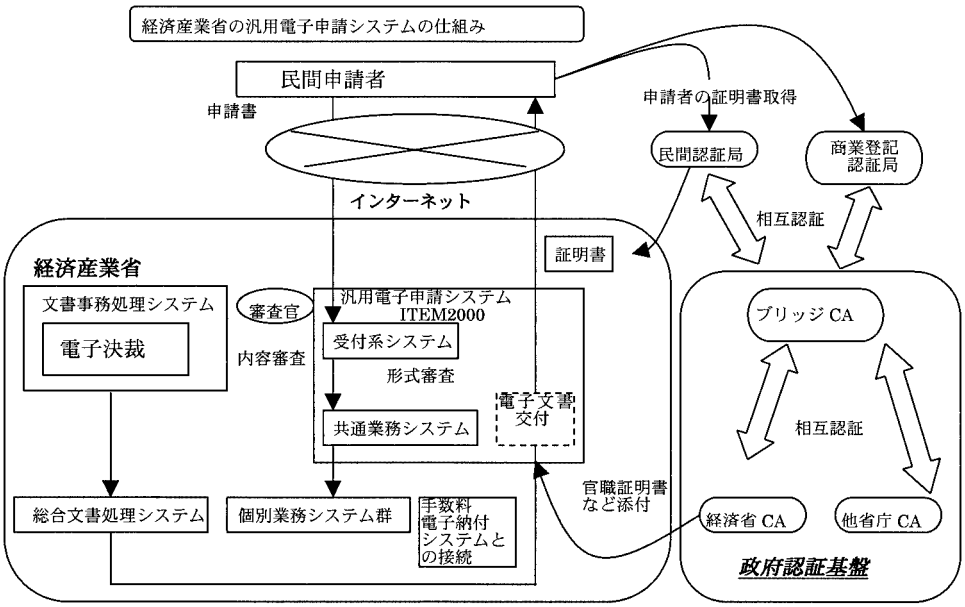
ここで重要な点は，申請者端末と汎用受付等システムとの接続（送信，状況確認，結果取得）時の通信の安全が確保されていなければならないということである．通信経路上でのデータに対しては，盗み見，改竄，他人のなりすましといった問題に対する対処が行われている必要がある．本項で登場した用語，「認証局」，「公開鍵」，「秘密鍵」，「公開鍵証明書」，「電子署名」等は，電子申請に於いて申請者情報および申請データを外部の脅威から守る上で必要不可欠な技術要素である．これらについては，第 4 章で詳しく説明することにする．

3.2 電子申請システムの概要

電子申請システムは，前述総務省の「申請・届出等手続のオンライン化に関わる汎用受付等システムの基本的仕様」（総務省）に記述された仕様に基づき，各省庁毎に独自要件を取り込みながら，別個にシステム構築を行なうことになっている．

図 3 は，経済産業省において，構築したシステムの概要である．

インターネットを介して民間申請者より提出された申請書を経済産業省の汎用電子申請システムにて受け付けている．次に申請者を認証するために政府認証基盤であるブリッジ認証局と連携をとっている．また，受付後の各申請書の審査手続は，個別業務システム群にて行われている．汎用電子申請システム業務フローにて説明されているように，申請から審査までの手続きが準備，受付，審査・決裁，公文書発行という



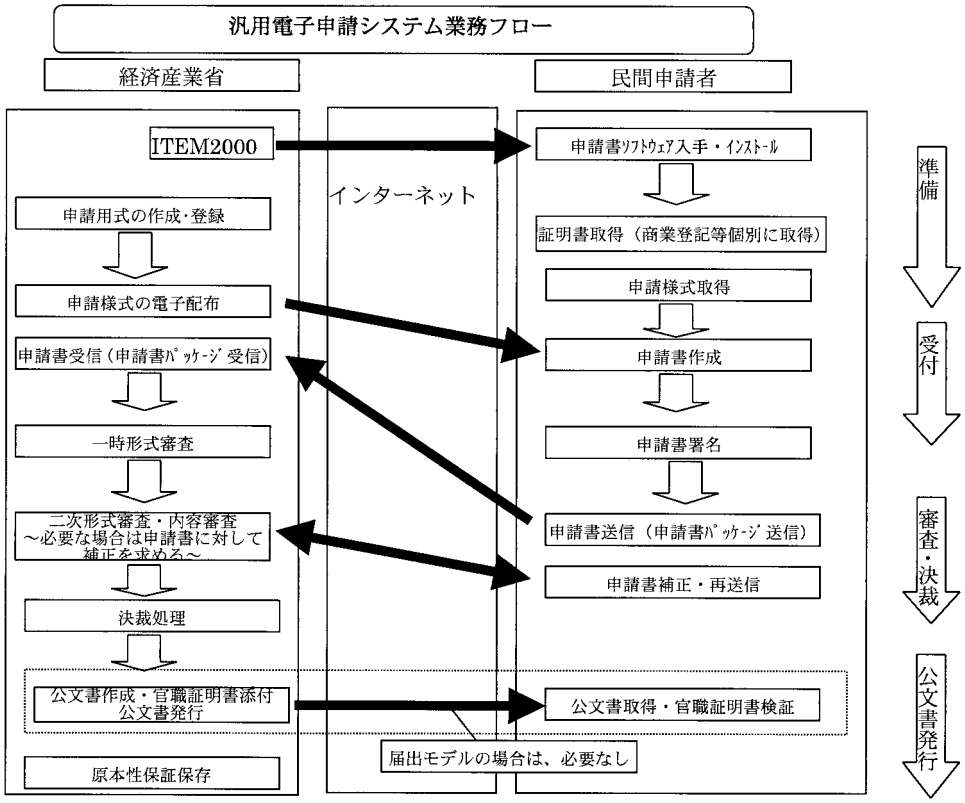


図 3　電子申請システムの概要（経済産業省の事例）

資料出展 http : //www.meti.go.jp/application/item 2000 exp/index.html
経済産業省（e-METI）推進本部ホームページより「経済産業省関連の申請・届出手続きに係る電子申請システム（ITEM 2000）」を参照

大きな区分けになっているのが特色である.

総務省の仕様にある申請書様式の取得作業は，この事例の通り，申請者が申請書を作成するソフトウェアの入手およびインストールまでの作業に対応している.従って，申請書様式という表現は，申請書を作成し，署名を付与し送信するまでの仕組み全体を意味している.

4. 電子申請システムを支える技術

インターネットによる電子申請を行う上で，従来書面において実現していた手続きをオンライン化するにあたって，全行政手続きに共通する課題として省庁間の横断的な組織である共通課題研究会があげた課題項目には，下記のものがある.

- 申請者等の認証
- 手数料等の納付方法
- 申請・届出等の到達時期等
- 電子文書の原本性確保

行政手続きにおける国民等と行政機関との情報のやり取りを整理すると以下の分類が考えられる。

・行政処分等に関するもの
　申請・届出・報告（許認可等)、不利益処分等
・契約に関連するもの
　競争契約参加資格審査への応募、入札および国有財産貸付の申し込み等
・上記以外のもの又は上記いずれにも関連するもの
　歳入歳出に関する手続、相談、教示・助言、広報・連絡　等

（資料出展　共通課題研究会「インターネットによる行政手続の実現のために」
平成十二年三月）

これらの手続をインターネットを用いたオンライン化をすることを前提として，問題の整理を行い，それに伴う技術的，および制度的な解決を図ることが必要となっている.

課題として取り上げられた問題の所在を要約すると，

1)　申請者等の認証

インターネットという公開されたネットワークを使用することにより，下記の点を仕組みおよび制度として保証する必要がある.

・送信された情報の名義人の同一性
・情報の改竄に対する防御
・情報の漏洩（盗み見）に対する防御

2)　手数料等の納付方法

申請手続きのオンライン化に伴い，従来書面手続においては，印紙または現金にて行っていた手数料の納付についてもオンライン化する必要がある．これに伴

う行政共通の仕組みの構築が求められる．

3)　申請・届出等の到達時期等

申請・届出や結果の通知等については，到達時期を起点として法律上の一定の効果が発生することから，オンラインにて申請を行った場合の到達時期を明確にする必要がある．

4)　電子文書の原本性確保

申請文書を電子化するに伴い，電子情報が容易に複製および改変を行えるため，行政が申請情報を保存管理するにあたり，原本をどのように確保するかを仕組みとして明確にする必要がある．

これらの共通課題については，すでに仕組みおよび制度面についての議論が終了し，結論がだされている．中央省庁においては，2002 年度中に総務省の共通仕様に基づいた汎用受付通知システムの構築を終了させ，電子申請の受け付けを開始することになっている．

ここでは，上記の内より申請者等の認証の仕組み及びセキュリティ確保をどのような形で実現できているのかを政府認証基盤（GPKI：Government Public Key Infrastructure）を中心に解説する．

続いて，申請システムの汎用化という観点で申請審査手続と受付処理の分離および申請手続きのパッケージ化について解説する．

4.1 PKI[*6] 技術に基づく政府認証基盤

政府認証基盤（以下 GPKI）は，公開鍵暗号方式[*7] に基礎をおく認証基盤技術（PKI）に基づいて構築されるものであり，電子化された申請書に対する本人性，真正性，事後否認防止を目的とした，電子署名に対する基盤であり，電子署名法と密接な関係がある．

電子署名法の成立によりインターネットにより送付された電子申請に電子署名の付与を行うことにより，上記の本人性，真正性，事後否認といったことに対する法的な根拠を持たせることを可能とした．

GPKI は，電子署名の検証，署名に対する証明を行うための基盤であり，省庁および民間のそれぞれの認証局をブリッジ認証局[*8] を介して相互認証させることにより複数の異なる認証局により証明された署名の正当性を評価することを可能としている．

4.1.1 電子署名の考え方

電子署名の方式の代表的なものにデジタル署名（図 4）がある．これは，公開鍵暗号方式による文書のハッシュトータルに対する暗号化，公開鍵暗号の性質を用いた，秘密鍵に対する公開鍵[*9] による復号機能による署名の本人性および認証局の証明書による本人性に対する認証，ハッシュトータルの比較による文書の真正性の確認を行う．手順を簡単に説明すると下記の通りとなる．

① 電子文書の作成者は，電子文書に数学的情報処理を施し固有の数字データを成生する．この数字データは，ハッシュ値と呼ばれ，電子文書毎に固有の値となる．ハッシュ値は，任意の長さのデータを固定のデータ長に圧縮するためのアルゴリズムであり，下記の性質を持つ．

・圧縮したデータから，圧縮前の状態のデータを逆算して求められない．

・同じ変換後のデータを生成する二つの元データを発見するのは困難

この一方向性のハッシュアルゴリズムを用いることによりメッセージの破損/改竄の検知が可能となる.

② ハッシュ値を電子文書作成者の秘密鍵で変換したもの（デジタル署名）を電子文書に添付する.

③ 電子文書とデジタル署名を送信先に送付する.

④ 送信先は，受信した電子文書からハッシュ値を生成し，受信したデジタル署名を送信者（電子文書作成者）の公開鍵を用いて復号し取り出したハッシュ値と比較検証する.

ここでの検証は，下記の二つが行われる.

・送信者の公開鍵により署名が復号できることにより，送信者が公開鍵に対応する秘密鍵の持ち主であることを検証する.

・ハッシュ値を比較することにより署名時以降に内容の変更（改竄）が行われていないことを検証する.

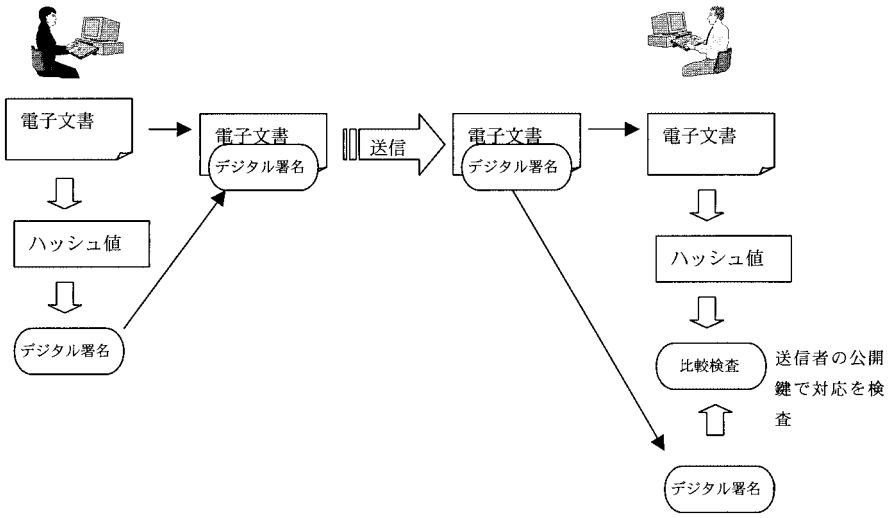


図 4　デジタル署名の仕組み

4.1.2　電子署名法について

申請書が電子化されている場合，申請書を作成した本人の確認が重要となる.

平成 12 年 5 月に制定された「電子署名法」は，電子署名の有功性を法的に明記したものである.

次に「電子署名及び認証業務に関する法律(平成十二年五月三十一日法律第百二号)」記載内容（抜粋）を照会する.

「電子署名及び認証業務に関する法律（平成十二年五月三十一日法律第百二号）」

（目的）

第一条　この法律は、電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的とする。

（定義）

第二条　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものを言う。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

2　この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

3　この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

第二章　電磁適記録の真正な成立の推定

電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

署名法の目的を要約すると，

・電磁的記録の真正な成立の推定

・特定認証業務に関する認定の制度

の 2 点をのべている．

1)　電磁的記録の真正な成立の推定

我々日本人の日常生活においては，書面の作成者の特定に印鑑の押印をもって行うことが通例である．

以下に電子文書に対する電子署名を書面における印鑑との比較において述べる．

真正な成立の推定とは，民法第 228 条第 4 項で「私文書は，本人またはその他の代理人の署名又は押印があるときは，真正に成立したものと推定する」という考え方にほぼ類するものと考えられる．

つまり，押印は，印鑑登録証明書の印影との照合において，検証が可能であり，また，登録された印鑑は，本人のみが保存管理しているはずであるということから，印鑑登録された印鑑による押印をもって，真正に成立したと推定している．

印鑑登録された印鑑の取り扱いが本人の厳密な管理の下で行われるのと同様に電子署名を行うために必要な符号及び物件が本人の管理化で厳密に行われていた

場合，署名の真正性が推定されるとしている．真正に成立したとは，本人の意思に基づいて署名が行われたことを意味している．

ここでいう本人のみの管理化の符号および物件とは，公開鍵暗号方式による署名を行う場合署名の基となる暗号処理に使用される秘密鍵を指している．

公開鍵暗号方式は，秘密鍵と公開鍵のペアーの鍵にて暗号および復号化を行うものであり，一方の鍵にて暗号化を行った場合，復号は，対になっている一方の鍵においてのみ可能となる性質を持っている．つまり，秘密鍵にて暗号化したものの復号は，相対する公開鍵のみにて可能であり，また公開鍵にて暗号化したものは，相対する秘密鍵においてのみ復号可能となる．

秘密鍵は，その名の通り鍵ペアを所有する本人が印鑑登録した印鑑と同様に厳重に管理保管を行い，他人が取り扱えないことを運用の前提とする．一方，公開鍵は，公開された鍵であり，自由に入手が可能である．

デジタル署名は，鍵の所有者本人のみが取り扱える秘密鍵にて暗号化したメッセージを相対する公開鍵にて復号できることをもって，署名が本人にて行われた真正性を推定できるとしている．

また，この場合，公開鍵が本人のものであることが前提となる．公開鍵が本人のものに間違いないことを第三機関による証明を取り付けることによりこの問題を解決する．即ち印鑑登録に対する公的機関の印鑑登録証書と同じ意味合いを持つ．

認証局と呼ばれる第三機関は，公開鍵が本人のものに間違いないことを証明するために公開鍵に対して認証局自身の秘密鍵にて署名を行い，また，その秘密鍵に対する公開鍵を一般に広く公開を行う．公開鍵に対する認証局が署名したものを電子証明書という．

2) 特定認証業務に関する認定の制度

特定認証業務とは，前述した電子証明書を発行する認証局業務を行う事業者の特定の業務に対する国の認定業務を指している．具体的には指定調査機関または承認調査機関が国を代表して認証局に対して認定審査を行う．

認証局業者は，調査機関に対して認定審査を行い，以下の認定基準に対する審査を受ける．

■認証業務を行う設備およびセキュリティ

認証業務を行う設備は，高いセキュリティが保たれており，設備に対する不正アクセスに対する防御，厳重な資格管理に基づく認証システムの操作がおこなわれる仕組みが設けられていること．また，火災，地震，停電，水害に対する対策が講じられていること等についての審査.

■証明書の利用者に対する真偽の確認方法

署名を行う利用者に証明書を発行する場合，本人であることをどのような方法にて行うことになっているかの審査であり，本人であることを証明するための資料の確認が前提となっている．具体的には，運転免許証，パスポート，年金手帳，保険証等がある．

また，認証局が発行する電子証明書は，申請者の公開鍵に認証局の電子署名を付与

することで作成されるが，この場合の署名に用いるアルゴリズムおよび鍵長についても以下のように規定されている．

（特定認証業務）
第二条　法第二条第三項の主務省令で定める基準は、電子署名の安全性が次のいずれかの有する困難性に基づくものであることとする。
一　ほぼ同じ大きさの二つの素数の積である千二十四ビット以上の整数の素因分解
二　大きさ千二十四ビット以上の有限体の乗法群における離散対数の計算
三　楕円曲線上の点がなす大きさ百六十ビット以上の群における離散対数の計算
四　第三号に掲げるものに相当する困難性を有するものとして主務大臣が認めもの

「電子署名及び認証業務に関する法律施行規則（平成十三年三月二十七日総務省・法務省・経済産業省令第二号）」抜粋

認証局が行う電子署名に関する規定に示された基準を満たす署名アルゴリズムとして，下記のものがあげられる．

RSA
ESIGN
ECDSA
DSA

従って，利用者が行う署名も上記のいずれかを用いることになる．

4.1.3　政府認証機関における認証の仕組み

電子申請を行う場合，申請書を受け付ける行政側は，申請者の付与した署名の有効性の検証を行う．

同様に申請者は，申請書に対する行政からの通知に付与された署名に対して同様に有効性の確認を行う必要がある．インターネットという不特定多数が共有するネットワークを介する故に署名の有効性の確認は，相互に必須となる．

署名の有効性の確認に於いては，下記の確認作業が行われる．

・認証パス[*17]の構築
・認証パスの検証
・署名検証

また，署名の検証においては，以下の処理が行われる．

・署名に付与された公開鍵による復号による署名自体の有効性の確認
・署名に付与された公開鍵証明書による署名者の認証
・公開鍵証明書が期限切れまたは，なんらかの理由による失効をしていないかどうかの確認
・署名の検証による改竄の検知.
・公開鍵証明書を発行した認証局の検証

図5は，電子申請において官側が申請書に付与された電子署名の有効性を検証する仕組みを説明したものである．

申請者は，政府の認定を受けた任意の認証局より認証書を取得し，それに基づいて申請書に電子署名を付与し，送信する．

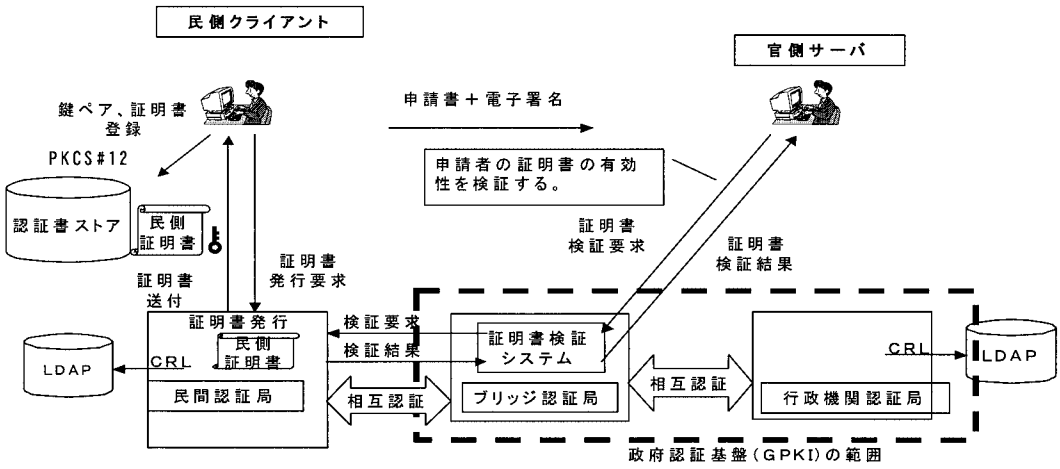


図 5　電子申請システムにおける署名の検証の仕組み

官側は，申請書を受け付けた時点で付与された電子証明書の検証を行なう．証明書の検証は，ブリッジ認証局の運営する証明書検証システムにより行われる．証明書検証システムは，申請者の署名を認証している認証局に証明書の有効性を照会し，その結果を応答する．

4.1.4　署名検証におけるブリッジ認証局の位置付け

電子申請に付与された電子署名の有効性の検証は，署名者に対する認証を行っている認証局の信頼に基礎をおいている．電子署名の認証を行う認証局が電子署名の検証者にとって信頼関係がない場合，認証局との信頼関係の構築が必要となる．電子署名の検証は，認証局の認証に基づいて行われることから，信頼関係の構築は，認証局間の相互認証という方法を用いて行われる．

相互認証は，認証局が相互に相手認証局に対して相互認証証明書[*18]を発行し，互いに相手の発行した相互認証書に対して電子署名を行うことにより実施される．これにより電子署名の検証者は，検証者が信頼をおく認証局が発行した相互認証証明書に基づいて，署名者の認証局の有効性を確認することが可能となる．

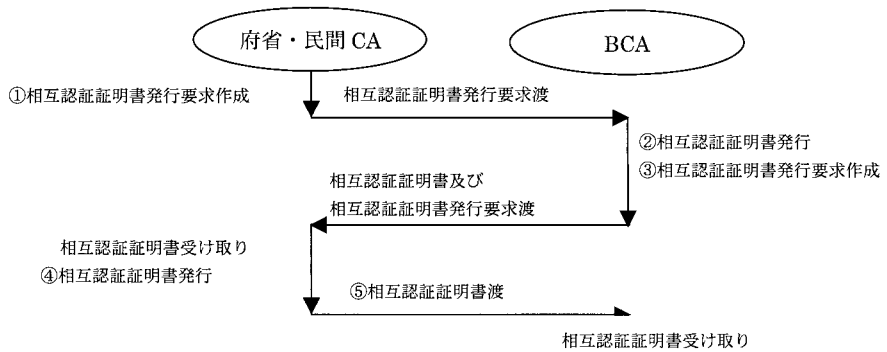


図 6　相互認証省及び発行要求の交換

（政府認証基盤相互運用性仕様書　平成 13 年 4 月 25 日参照）

電子申請においては，申請者は，特定認証業務の認定を受けた認証局の中から任意の認証局を選定し，その認証に基づき電子署名を行う．また，申請書を審査する側は，各省にて運用する認証局が認証する公開鍵証明書に基づいて通知，許可書等に電子署名を行なう．

政府認証基盤においては，民間の不特定多数認証局および官側の省庁認証局の相互認証を行う仕組として，ブリッジ認証局を設立し，全認証局がブリッジ認証局との相互認証を行うことにより，認証局の信頼性を確保する方式を取っている（図 6）．

4.1.5 証明書検証システム

電子申請システムにおける認証処理をブリッジ認証局との連携において説明する．

ブリッジ認証局は，政府の各府省が電子申請受け付け時に行う証明書の検証機能を簡便に実現するために証明書検証サーバ機能を提供している．

各府省は，電子申請に付与された署名の検証を証明書検証システムに検証依頼を行うことにより実現できる．

図 7 にあるように官側は，受付た申請書に付与された電子署名を検証するためにブリッジ認証局の証明書検証システムにアクセスしている．証明書検証システムへのアクセスは，OCSP（Online Certificate Status Protocol）（RFC 2560）のプロトコルを使用して行われる．

証明書検証システムは，下記の機能を提供する．

・証明書検証サーバ自身の証明書の発行要求，発行された証明書の受入
・署名検証者からの証明書検証要求受付

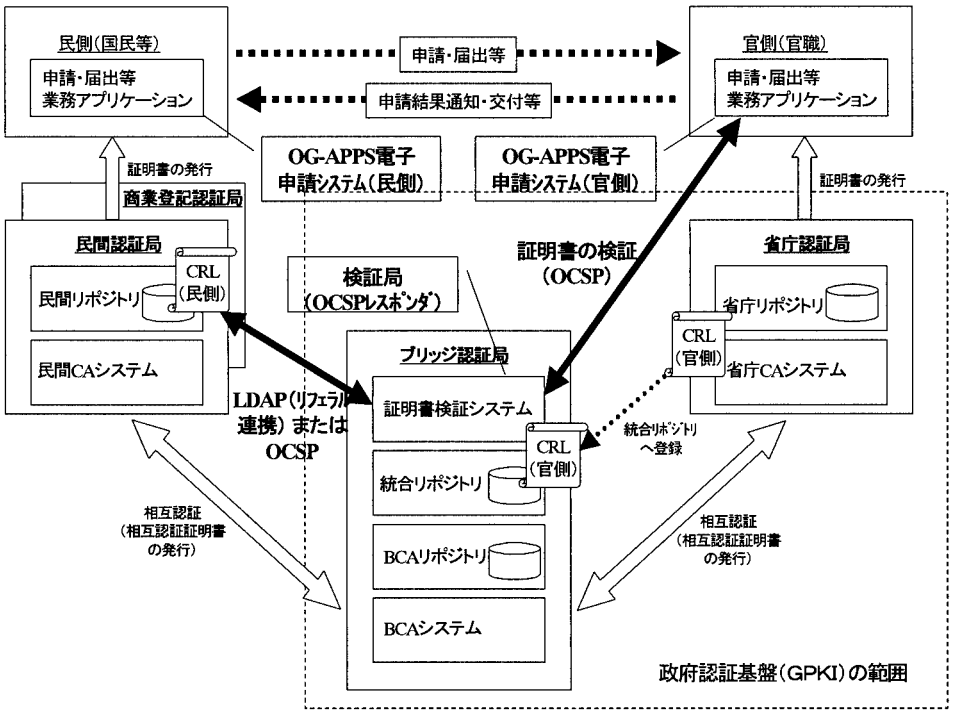


図 7　電子申請における認証処理の流れ

・各 CA（Certificate Authority：認証局）が発行した CRL[*12]/ARL[*13] の検証
・各 CA が提供する OCSP レスポンダ[*14] への検証要求送信とその応答の受信
・認証パス構築
・認証パス検証
・署名検証者への証明書検証結果の送信

4.2 セキュリティ

インターネット利用において，安心かつ信頼できる IT 環境を構築することが求められる．それは一般に言われるセキュリティ対策で，脅威と対策の対で記述できる．表 1 は，インターネット利用にて発生し得る脅威と対策をまとめたものである．

表 1 IT 環境での脅威と対策

脅　威	対　　策
覗き見	暗号化技術
侵入	ファイヤウォール、ウィルスチェック
なりすまし	本人確認・接続先確認
改変（改竄）	電子署名
複写	電子透かし（不正コピー検知の目的で原本の所有権の保証）

対策にあがっている暗号化技術，本人確認・接続先確認，電子署名，電子透かしのいずれも，公開鍵による認証基盤技術（PKI：Public Key Infrastructure）の応用であり，電子申請システム構築には公開鍵・秘密鍵の所有者および有効性を保証する電子認証基盤が不可欠である．電子認証基盤は，申請者(企業，個人)，審査者(官職)，サーバ，等毎にそれぞれが持つ公開鍵・秘密鍵に対して証明書を発行・登録管理し証明書を公証する役割を担う．

上記の内，なりすまし及び改竄に対しては，電子署名により解決が行われる．

4.2.1 メッセージの暗号処理

メッセージの覗き見に対する対策として，メッセージの暗号化を行う．

暗号化処理としては，共通鍵暗号方式と公開鍵暗号方式があるが，それぞれについて，下記の特色がある．

1） 公開鍵暗号方式

鍵長が電子申請においては，2048 ビットまで使用可能であり，最大の鍵長を使用した場合，安全性が極めて高い．

但し，暗号処理および復号処理に時間を要する．通常，共通鍵暗号方式の約 1000 倍の時間を要するといわれている．

代表的な暗号方式に RSA，DSA，楕円暗号方式等がある．

2） 共通鍵暗号方式

暗号鍵と復号鍵が同一の鍵を使用するため，暗号メッセージを送信するためには，相手が同一の復号鍵を所有していることが前提となる．

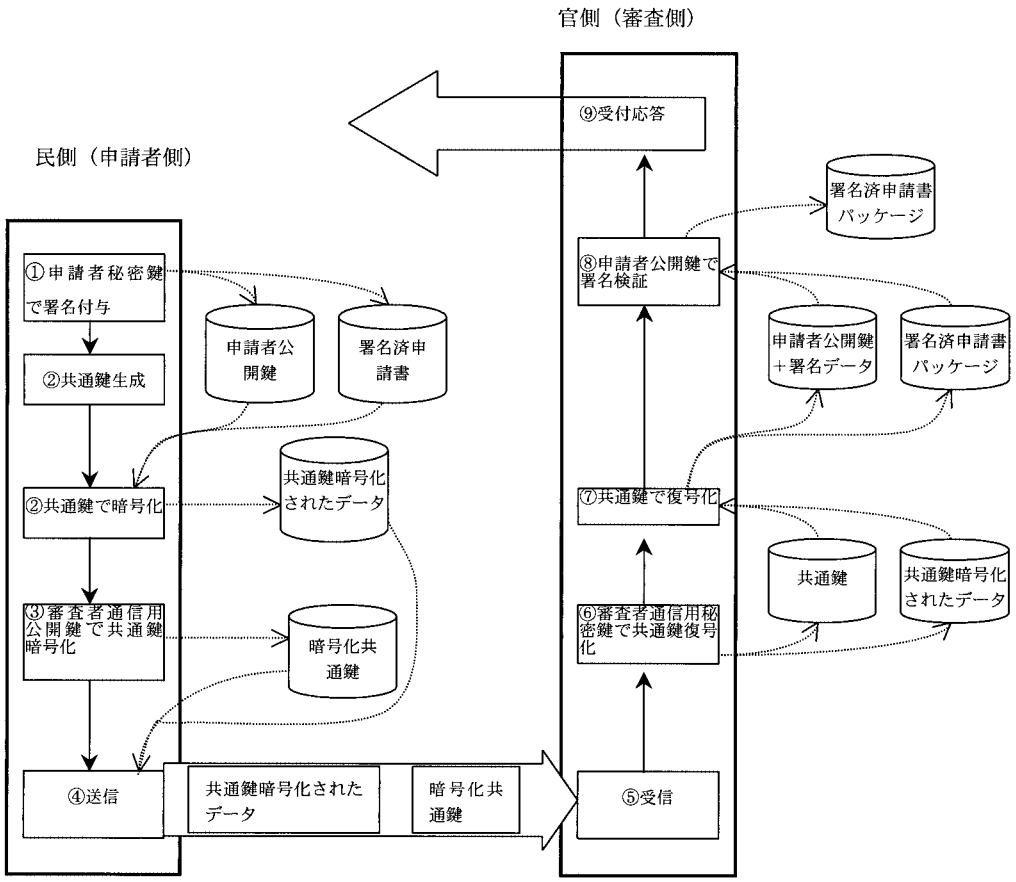
電子申請の場合，不特定の申請者より申請が行われる為，共通鍵を運用することは，極めて困難となる．

代表的な暗号方式として，DES，RC 2，RC 4，RC 5 等がある．

3)　申請書送付時に行われる暗号処理

前述のことから，処理効率と運用性を考え，電子申請の暗号処理として，共通鍵と公開鍵の併用の方式が一般的に用いられる．

図 8 に申請書送付時に行われる暗号処理の一例について説明する．



①申請者は，秘密鍵を用いて申請書に電子署名を行う．
②申請者環境にて共通鍵暗号に用いる共通鍵を生成し，署名を付与した申請書を暗号化する．
③予め入手しておいた官側の公開鍵にて暗号処理に用いた共通鍵を暗号化する．これにより共通鍵は，官側においてのみ復号可能となる．
④共通鍵で暗号化した申請書と公開鍵で暗号化した共通鍵を送信する．
⑤申請書を受信する．
⑥官側は，公開鍵にて暗号化された受信メッセージより共通鍵を取り出すために官側の秘密鍵にて復号する．
⑦復号化した共通鍵を用いて申請書を復号する．
⑧申請書に付与されている署名を申請者の公開鍵を用いて検証する．
⑨受付結果を申請者に応答する．

図 8　電子申請の暗号処理の説明図

4.2.2　侵入に対してのシステム上の考慮

インターネットにおけるメッセージ送受信は，通常通常 HTTP または，HTTPS プロトコルを用いて，実施される．

このため，暗号化されたメッセージを WWW サーバにおいて復号を行ってしまうと，公開性の高い WWW サーバであるため，メッセージの覗き見および改竄といった攻撃の危険が発生する．安全なメッセージの受け付けを行うためには，WWW サーバ内における攻撃に対する対策が必要である．

財団法人ニューメディア開発協会にて開発したセキュア通信方式においては，暗号メッセージの復号を WWW サーバのさらに内側にセキュア通信サーバを設置し，WWW サーバとセキュア通信サーバの間にファイアウォールを設置することにより実現している．

具体的には，WWW サーバとセキュア通信サーバの間に設置されたファイアウォールは，外部メッセージの入力を受け付けない設定になっており，ファイアウォールの内側のセキュア通信側からのみメッセージにアクセスできる方式を取っている．

セキュア通信サーバは，WWW サーバに到達した暗号化メッセージをファイアウォールの内側よりポーリングを行うことにより取得をし，復号化する．

これにより，暗号化メッセージは，安全な地点にて復号化が実現される（図 9）．

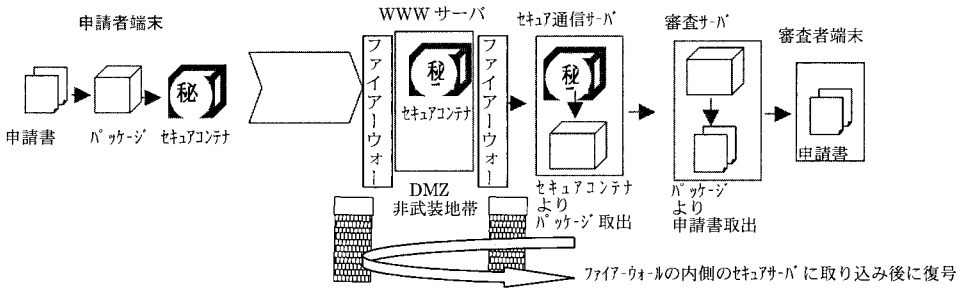


図 9　セキュア通信のメッセージの流れ

4.3　電子申請システムの汎用化について

4.3.1　申請審査手続と受け付け処理の分離

ここまで，電子申請システムの機能的観点で話を進めてきたが，もう一つ重要な検討課題がある．それは，申請・届出の手続が多いということである（1 省庁当たり約 2,000 手続）．

数多くの異なった特性を持つ手続をどのように電子申請システムで上手く処理するかが重要な課題としてあげられる．手続毎に申請・届出の書式は違うしその審査業務も異なっている．すなわち，フロントエンド（申請書類個々の作成）とバックエンド（申請内容の意味的審査：個別審査）はそれぞれ異なるが，その仲介を行う電子申請システムを汎用的かつ共通的に構築できるかが重要となる．電子申請システムの機能間を流れるデータが申請データとそれを管理するメタデータ（情報）である．これらデータの型が 1 省庁当たり約 2,000 種類存在し，それらに対して年間多いものであれば何万，少ないものであれば，数百といった申請・届出が行われている．

電子申請システムの開発を行う場合，これらの膨大な手続きにシステムが如何に影響を受けないかということが重要となる．

総務省「申請・届出等のオンライン化に関わる汎用受付等システムの基本仕様」では，申請者側と行政側とのインタフェースの部分を汎用化することをまず行うべきだとしている．その結果，個々の手続に依存する部分をバックエンドとし，申請書の送信から受け付けまでの部分との分離を図ることが求められる．前者を個別申請，審査システム後者を汎用受付システムと呼ぶ．

4.3.2　申請手続きのパッケージ化

現行の申請・届出は，窓口へ出向いて行うか，郵送により行われる．郵送の場合を分析すると電子申請システムが満たさなければならない要件が整理できる．実際に何千もの手続に対して，年間万の単位の申請・届出が行われている．

郵便封筒の機能を以下に記述する．

・封筒には，申請書本文および添付文書等何個でも入れることができる．
・申請本文等には，本人であることを保証するために捺印を付与する．かつ紙であるため改変が行われれば検知できる．
・封印すれば，格納した文書に対して覗き見も改変もできない．
・配達員により本人に直接封筒を配達できる．

電子申請システムでは，郵便封筒に当たるものをパッケージという概念で実現する．パッケージは XML 技術の RDF（Resource Description Framework）構造から成り，中には XML ファイル，ワープロファイル（WORD，一太郎，等），表示用ファイル（PDF，CAD，等）と鏡，本文，別紙，添付等に充てがい，自由な組合せで書類一式を決めることができる．また，中身のファイルには，本人であることの保証および改変検知のために電子署名を，覗き見防止のために暗号化を行えるように実装する．

下記の図 10 は，経済産業省において構築した汎用受付通知システムの文書パッケージの概念図である．

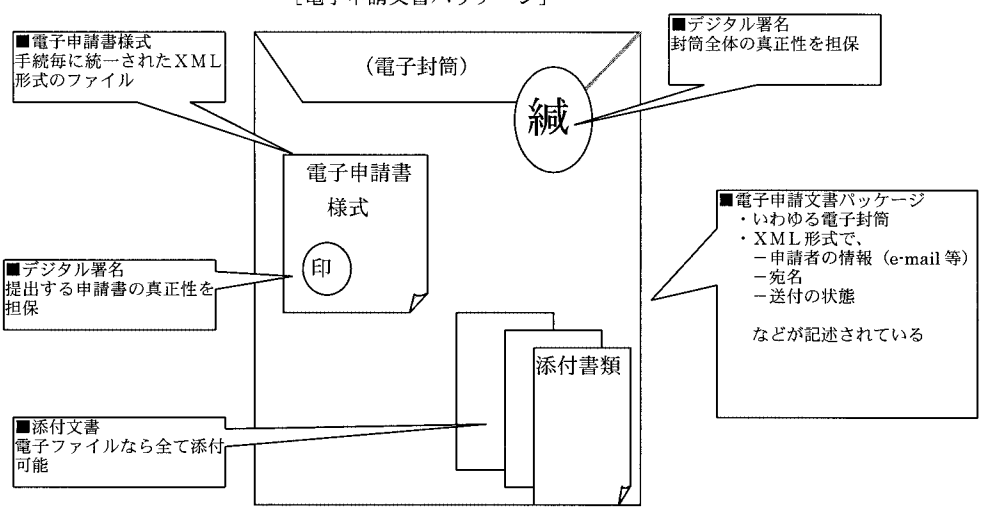


図 10　経済産業省における電子文書パッケージ概念図

資料出展 http : //www.meti.go.jp/application/item 2000 exp/index.html
経済産業省（e-METI）推進本部ホームページより「経済産業省関連の申請・届出手続きに係る電子申請システム（ITEM 2000）」を参照

図 11 は，申請書パッケージを中心とした申請，審査の手続の流れを概念的に説明している．

申請，審査の手続で取り扱う情報は，申請者が作成する申請書および添付文書の他に，官側にて作成する訂正指示書，認定書といった情報がある．これらをパッケージ化することによりシステムは，申請から審査までの流れを個々の情報の形式に依存せずに行うことが可能となる．

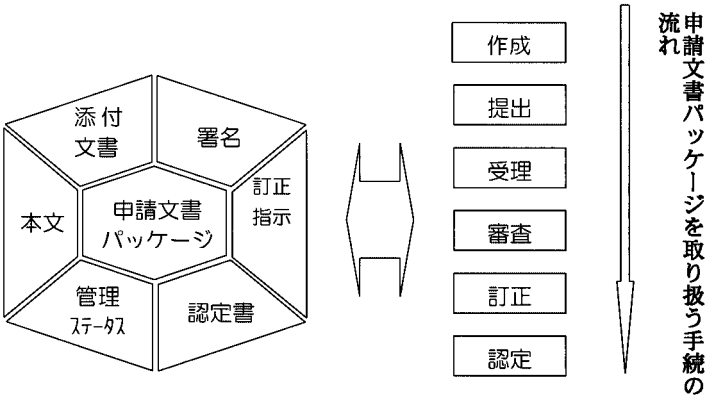


図 11　申請文書パッケージと申請審査業務

4.3.3　パッケージに用いられる XML 技術

電子申請システムで取り扱われる情報を整理すると下記の内容が存在する．

1）　申請者が作成する情報

　　申請書本文（構造化文書（XML），ワープロ文書，PDF 他）

　　添付文書（画像，ワープロ文書，PDF 他）

2）　審査側が作成する情報

　　訂正指示書（構造化文書（XML）

　　訂正指示（個別訂正指示情報テキスト）

　　証書（申請に対する許可，認定）

財団法人ニューメディア開発協会が開発した「インターネット電子申請システム」における「電子申請文書処理コンポーネント」においては，上記情報を構造化言語である XML（eXtensible Markup Language）を用いて，パッケージングする方式を提供している．

図 12，13 に「電子申請文書処理コンポーネント」を用いた申請書パッケージの事例を示す．

申請書を構成する各情報は，パッケージ情報管理ファイルの XML のタグにより結び付けられる．パッケージ情報管理ファイルを参照することによりすべての構成要素を管理することが可能となっている．

申請を行う場合は，申請文書パッケージに署名を付与し，パッケージ全体を暗号化し送信を行っている．

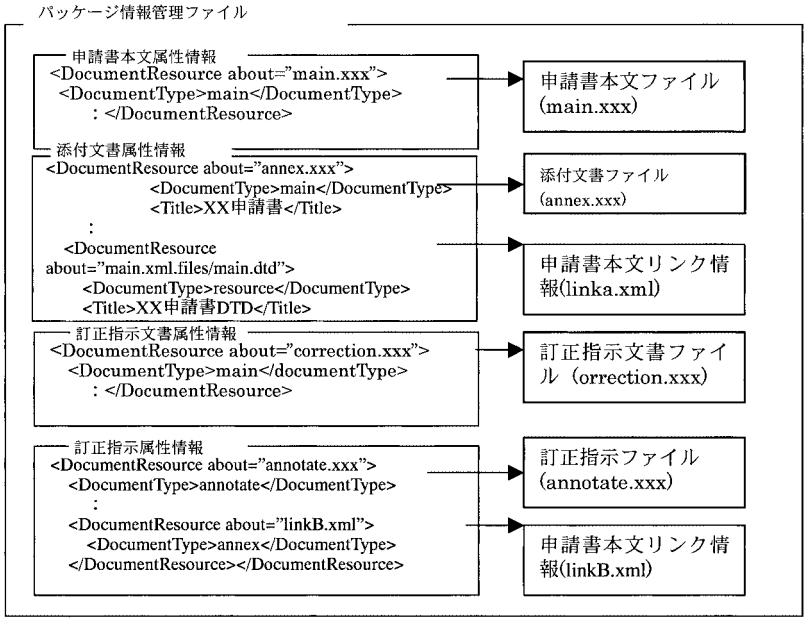


図 12　申請文書パッケージ

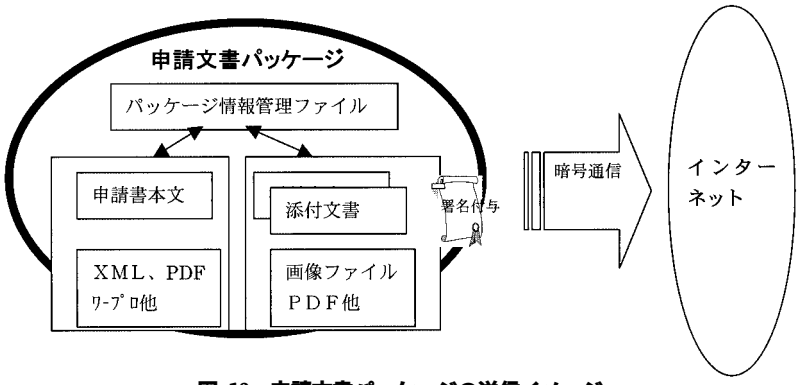


図 13　申請文書パッケージの送信イメージ

5. おわりに

電子申請システムの開発は，2003 年度までに中央省庁および地方公共団体（都道府県，市町村）における開発を終了させる計画で進められている．地方公共団体のシステム化のスケジュールは，中央省庁より 1 年程遅れて開始しており，平成 2002, 2003 年度に開発のピークを迎えようとしている．地方公共団体の場合，国に比べ，予算が潤沢でない場合が多く，システム開発は，財政的には大きな負担といえる．このため，中央省庁の開発の成果を活かし，コストおよび期間の効率性の高いシステム開発が望まれる．

用語説明

＊ 1　e-Japan 戦略
2001 年 1 月に IT 戦略本部により打ち出されたもので，2005 年までに世界最先端の IT 国家を目指すという国家戦略のこと．

＊ 2　電子政府
デジタル技術を活用して各種行政サービスの電子化を図り，行政サービスの効率的率向上を目指すもの．

＊ 3　ワンストップサービス
1 つの目的行為に要する行政側の申請手続き及び窓口が複数存在する場合，これを 1 つの窓口に申請を行うことにより関連する申請手続きを自動的に連携して行うこと．行政側の国民へのサービスの向上の一環として，申請者が行う手続の負担の軽減を目指したもの

＊ 4　e-Japan 重点計画
e-Japan 戦略（2001 年 1 月に IT 戦略本部によって打ち出されたもので，2005 年度までに世界最先端の IT 国家を目指すという国家戦略のこと．）を具体化するために政府が迅速かつ重点的に実施すべき施策．

＊ 5　e-Japan 2002 プログラム
「e-Japan 戦略」及び「e-Japan 重点計画」を各府省の 2002 年度の施策に反映する年次プログラムで下記五つの柱を重点項目としている．
①高速・超高速インターネットの普及促進
②教育の情報化・人材育成の強化
③ネットワークコンテンツの充実
④電子政府・電子自治体の着実な推進
⑤国際的な取組の強化

＊ 6　PKI（PublicKeyInfrastructure）
認証基盤．
公開鍵の正当性を保証する公開鍵証明書の発行・公開を行う枠組．
公開鍵証明書は公開鍵暗号やデジタル署名を利用する時に必須．

＊ 7　公開鍵暗号
暗号時と復号時に，鍵ペアのうちそれぞれ異なる鍵を用いる暗号方式．代表的なものに RSA 暗号がある．また，この原理を応用して署名時に秘密鍵，署名検証時に公開鍵を用いることにより電子署名の仕組みを実現することができる．

＊ 8　ブリッジ認証局（ブリッジ CA，BCA）
行政機関の CA，法人 CA，民間 CA との間に相互認証証明書を発行して，認証基盤の要としての役割を果す CA.

＊ 9　公開鍵
公開鍵暗号方式において用いられる鍵ペアの一方．秘密鍵に対応する，公開されている鍵．

＊10　公開鍵証明書
ある公開鍵を記載されたものが保有することを証明する電子的文書．認証局が記載内容を確認のうえ，認証局の署名を付与することで，その公開鍵の正当性を保証する．

＊11　CA（CertificateAuthority）
認証局
公開鍵証明書の発行，公開鍵証明書取得者の登録，失効，鍵管理を行う機関．

＊12　CRL（CertificateRevocationList：証明書失効リスト）
証明書の有効期間中に内容変更や秘密鍵の盗難，紛失，破壊などの理由で失効した公開鍵証明書リスト．

＊13　ARL（AuthorityRevocationList：認証局失効リスト）
証明書の有効期間中に証明書の内容変更，秘密鍵の盗難，紛失，破壊等の理由により失効した認証局の自己署名証明書や相互認証証明書のリスト．

＊14　OCSP レスポンダ
OCSP プロトコルを用いて公開鍵証明書の有効性についての問い合わせを行う場合の応答先のサーバ．公開鍵証明書が失効リストに存在するかどうかを主に確認し，応答を返す．

＊15　相互認証
二つの異なる認証ドメインの認証局がお互いに認証を行うことにより，それぞれの認証局が発行した認証書の有効性を保証する考え方．「4.1.4．署名検証におけるブリッジ認証局の位置付け」にて詳細説明．

＊16　電子署名電子的な署名．一つの方式として，デジタル署名がある．詳細「4.1.1 電子署名の考え方」にて記述．

＊17　認証パス
自己の CA から相手の公開鍵証明書を発行した CA までをたどる検証の道筋．

＊18　相互認証証明書
二つの異なる認証ドメインの CA がお互いを認証したことを示す為に，相互に発行する証明書．

参考文献
［1］ 総務省，申請・届出等手続のオンライン化に関わる汎用受付等システムの基本的な仕様，総務省ホームページ掲載 http : //www. soumu.go.jp/gyoukan/kanri/kanri_f.htm, 平成 13 年 8 月 6 日行政情報化推進各省庁連絡会議幹事了承
［2］ 経済産業省，電子署名及び認証業務に関する法律，経済産業省ホームページ掲載, http : //www.meti.go.jp/policy/netsecurity/digitalsign-law.htm，平成十二年五月三十一日法律第百二号
［3］ 首相官邸, IT 戦略本部(第 3 回)平成 13 年 3 月 29 日 資料 4, 首相官邸ホームページ掲載 http : //www.kantei.go.jp/jp/it/network/dai 3/3 gijisidai. html, e-Japan 重点計画(高度情報通信ネットワーク社会の形成に関する重点計画)
［4］ 総務省共通課題研究会，インターネットによる行政手続の実現のために，総務省ホームページ掲載 http : //www.soumu.go.jp/gyoukan/kanri/kanri_f. htm, 平成 12 年 3 月
［5］ 財団法人ニューメディア開発協会, NMDA 電子申請フレームワーク「システム構築ガイド第 1 版，ニューメディア開発協会ホームページ掲載，http : //www.nmda.or.jp/nmda/soc/sinsei 2 ki-press. html
［6］ 経済産業省，経済産業省関連の申請・届出手続きに係る電子申請システム(ITEM 2000)」，経済産業省ホームページ掲載 http : //www.meti.go.jp/application/item 2000 exp/item 2000 exp 03. html
［7］ 政府認証基盤(GPKI)政府認証基盤相互運用性仕様書，e-Gov ホームページ掲載 http : //www.gpki.go.jp/session/index. html, 平成 13 年 4 月 25 日 基本問題専門部会了承
［8］ 小松文子他，PKI ハンドブック，2000 年 11 月 25 日第 1 版，ソフト・リサーチ・センター
［9］ CIO Online : Special Report「電子政府の可能性を探る」, アイデージー社ホームページ掲載特集「電子政府の可能性を探る」e-Goverment http : //www.idg.co.jp/CIO/contents/special/special 7. html
［10］ 総務省電子政府・電子自治体推進プログラム 平成 13 年 10 月 16 日，総務省ホームページ掲載, http : //www.soumu.go.jp/s-news/2001/011016_3. html
［11］ 首相官邸，e-Japan 戦略 平成 13 年 1 月 22 日，首相官邸ホームページ掲載，http : //www.kantei.go.jp/jp/it/network/dai 1/1 siryou 05_2. html

執筆者紹介

飯　田　眞　弘（Masahiro Iida）

1977 慶応大学文学部卒業．1984 年日本ユニシス(株)入社．航空部品補給システム，医療オーダシステム，厚生労働省 FD 申請システム等の公共関連のシステム開発を担当．1999 年財団法人ニューメディア開発協会のコンソシアムにて「インターネット電子申請システム」実地検証システムの開発を担当．以降，電子申請システム OG-APPS の製品開発に従事．

城　代　優　二（Yuji Jodai）

1971 年東京農工大学工学部卒業．同年日本ユニシス(株)入社．シリーズ 2200/1100 のデータベース・プロダクトの開発・保守，三井物産 MISA プロジェクト，海上自衛隊人事システム開発，　建設 CALS のクリアリングハウス実証実験システム開発を経て，現在，社公システム一部官公システム二室所属し，電子申請システム開発に従事．