電子署名活用ポイントガイド

Ver.1.2

財団法人　日本情報処理開発協会

はじめに

このハンドブックは、電子署名の仕組みを理解して適切に導入推進する立場にある方々を対象に、電子署名の基礎から応用まで幅広く解説を試みたものです。

電子署名を利用する場合、電子署名や公開鍵暗号方式など聞きなれない多くの用語が使われ、利用を躊躇する場合もあるかと思います。そこで、関連する用語を一つ一つ理解ができるように説明を加えました。

本文は3章からなっています。

「第1章　電子署名とそのしくみ」では、電子署名の法的裏付けとなる、電子署名法やe文書法といった法律の紹介を通して、電子署名に求められる要件を整理すると共に、対応する電子署名技術を解説しています。

「第2章　電子署名の利用」では、電子政府や自治体における電子署名の利用について電子申請などの例を示しながら紹介を行っています。

「第3章　電子文書と長期保存」では、電子署名付きの文書を数十年にわたってその署名の有効性を検証可能にするための「長期署名フォーマット」や時刻情報をデータに付加するタイムスタンプについて解説をします。

できるだけわかりやすく、かつかなり専門的なところまで、解説を行ったつもりです。電子署名の理解の一助になれば幸いです。

2009年11月　財団法人日本情報処理開発協会

目　次

第1章　電子署名とそのしくみ

1.　電子署名とは

電子署名とは、デジタル文書の真正性を保証するために付けられる電子的な署名情報であり、文字や記号、マークなどを電子的に表現して署名行為を行うこと全般を指します。これは、紙面における「手書き署名」や「捺印」に相当しますが、署名や印影を単にデジタル化するという単純なものではありません。

「手書き署名」や「捺印」は、「手書き署名」のインクや「捺印」の朱肉が紙に染み込み、紙を媒体に本文と強固に結合しています。電子文書も、電子署名部分だけが離れないよう、本文の電子データと電子署名の電子データが強固に結合している必要があります。

電子署名のうち特に、公開鍵暗号方式（用語集参照）を応用して、秘密鍵（署名鍵）を所持している者だけが正しく署名でき、かつその文書が改ざんされていないことを証明できる署名方式のことを「デジタル署名」といいます。以下では、特に断りのない限り、電子署名はデジタル署名の意味で使っています。

デジタル署名の本質は、公開鍵暗号方式による文書の暗号化です。秘密鍵によって暗号化（署名）された文書は署名済み文書そのものなので、署名済み文書と署名が離れることはありません（図 1-1 の左図）。

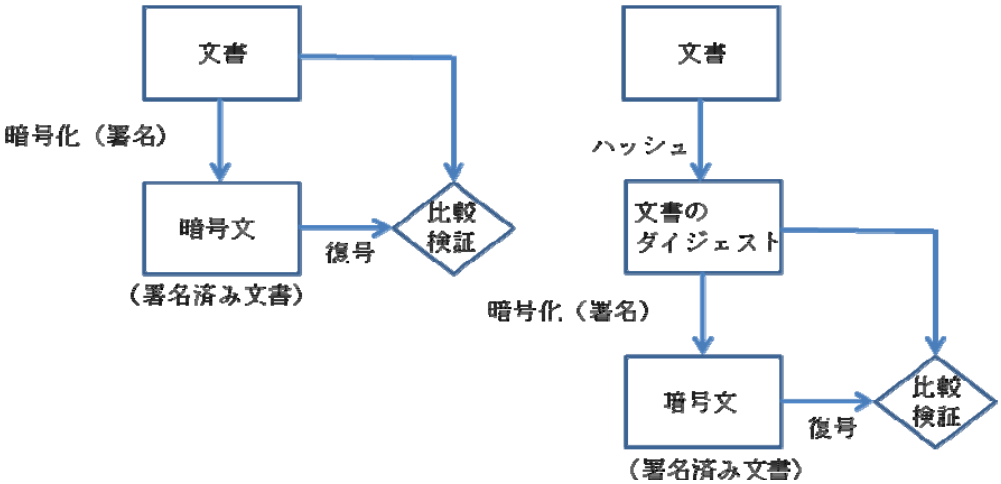


図 1-1 デジタル署名の原型

しかし、実際には、文書を直接秘密鍵（署名鍵）でもって暗号化し、署名済み文書を生成することはありません。理由は 3 つあります。

・公開鍵暗号システムの処理が遅い（共通暗号システム（用語集参照）より 2 桁から 3 桁遅い）
・平文（暗号前の文）と暗号文のペアを与えることにより解読されやすくなる
・署名が元の文書と同じかそれ以上の長さになる

従って、実際には図 1-1 の右図のようにハッシュ関数（用語集参照）を用いて文書のダイジェ

スト（160 ビット～512 ビット長のハッシュ値）を作成し、このダイジェストを秘密鍵でもって暗号化（署名）することで、上記の問題を解決しています。

図 1-2 は、図 1-1 の右図を署名者と検証者とに分けて描いた図です。

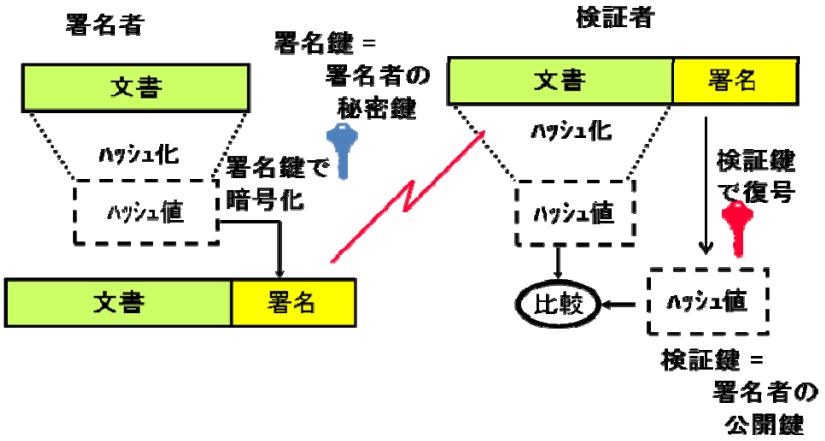


図 1-2 デジタル署名における署名と検証

2. 電子署名法

電子署名に法的効力を認めるかどうか、また、どの方式を電子署名として認めるかといった事項は、国によって異なります。電子署名法が最初に制定されたのは、米国のユタ州で、1995 年 2 月に制定されました（1995 年ユタ州法、1996 年改正）。米国の連邦法としては、2000 年 6 月に電子署名法（The Electronic Signatures in Global and National Commerce Act）が成立し、同年 10 月から発効しています。この法案にクリントン大統領は最初にペンとインクとで署名を行い、引き続き電子署名を行ったと伝えられています。欧州連合（EU）でも同年 12 月に電子署名指令が成立しました。

日本の電子署名は、電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号、最終改正：平成 18 年 3 月 31 日法律第 10 号）により具体的に定められています。

この電子署名法は、電子署名と特定認証局の認定の双方を定めており、このうちの「電子署名」については次のように定義しています。

> 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いう。
>
> 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。
>
> ＜電子署名及び認証業務に関する法律より抜粋＞

つまり、本人性の確認と非改ざん性の確認が電子署名の要件となっています。電子文書には手書き署名や捺印を行うことはできませんので、これに代わる本人性の確認と非改ざん性の確認を備えた電子署名技術を適用する必要があります。

また、電子文書（電磁的記録）の真正な成立の推定要件として、本人による署名に加えて署名鍵の適切な管理についても言及しています。

> 第三条　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。
>
> ＜電子署名及び認証業務に関する法律より抜粋＞

3.　公的な認証局における電子認証

電子署名は、現在のところデジタル署名技術が使われています。この技術では一対の公開鍵と秘密鍵をペアで生成し秘密鍵で署名すると、対応した公開鍵でのみ署名の検証ができるという原理を使っています。

公開鍵が確かに署名者本人の秘密鍵に対応した公開鍵であることの証明は、通常、信頼できる第三者機関によって行われます。その証明書が公開鍵証明書と言われるものです。この証明書を提示することによって、不特定多数の相手に、公開鍵が本人のものであることを証明することができます。このような、第三者が電子的にその本人性の証明を行うことを電子認証といいます。

「認証」という用語は、人、物、情報の真正性を確認する意味での認証（Authentication）もありますが、ここでは、ある権威者が人や物に対して、その資格や特性を証明するという意味での認証（Certification）という意味で用いています。

公的な公開鍵証明書には、電子署名法に基づいて発行される公開鍵証明書（特定認証業務）、商業登記に基づく公開鍵証明書、住民基本台帳に基づく公的個人認証サービスの証明書などがあります。

(1) 特定認証業務

電子署名法では、この法律に基づいた認証機関による証明書発行業務を「特定認証業務」と呼んでいます。認証機関が公開鍵登録時に行う本人確認手段と証明書記載内容については省令にしたがっています。

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。　＜電子署名及び認証業務に関する法律より抜粋＞

主務省令で定めるとなっている、認証局が証明に用いる電子署名については、電子署名及び認証業務に関する法律施行規則（平成13年3月27日）で次のように定められています。ここで、一項は現状、鍵長が1024ビット以上のRSA、二項は鍵超1024ビット以上のDSA、三項は鍵長160ビット以上のEC（楕円曲線暗号）を意味しています。

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数分解

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　前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るもの

＜電子署名及び認証業務に関する法律より抜粋＞

(2) 商業登記に基づく電子認証

法務省が提出した「商業登記法等の一部を改正する法律」が国会で成立し（2000年4月19日公布）、法人については商業登記情報に基づく認証システムが稼働しています。制度的には、法務局の登記官が法人代表者の公開鍵を証明することになります。法務大臣の指定する法務局に印鑑を提出した者は、登記官に対し、次の事項の証明を請求することができ、登記官はこの請求に対して電子証明書を発行します。

・法人代表者が用いる電子署名の公開鍵
・法人の商号、代表者の氏名・資格等の登記事項
・証明の有効期間

(3) 公的個人認証

住民基本台帳に記載されている15歳以上の希望者（日本国内に住所のある日本国民）に対して提供される電子認証で、2004年1月から公開鍵証明書の発行が開始されています。但し、用途は政府機関や各地方公共団体への各種届出・申請などに制限されています。発行者は申請者の住所がある都道府県の知事で、市区町村の窓口にて発行の申請が行えますが、原則として代理申請は認められていません。

申請に必要な費用は一般的に500円で有効期間は発行日より3年間です。証明書には、住所

情報が記載されているため、現在は住所変更に伴い、公開鍵証明書も失効します。

総務省自治行政局（2009 年 3 月 4 日発表）によると、公的個人認証サービスによって発行された公開鍵証明書の数は 2009 年 2 月末時点の累計発行件数は約 104 万枚となっています。

(4) 証明書記載事項と個人情報保護

署名の検証者は、検証時に表示される公開鍵証明書に記載された内容により署名者を疑いの余地なく特定できなければなりません。そのためには、署名者と検証者の双方によって合意された認証局から公開鍵証明書が発行されていること、公開鍵証明書には、署名者を特定することができる必要最小限の情報が記載されていることが必要です。

ただし、公開鍵証明書は、名称は“公開”ですが誰でも自由に他人の証明書を取得できるようにする必要はありません。必要な検証者だけに制限して開示できれば十分です。制限しないと、公開鍵証明書に記載された個人情報が必要以上に露出する恐れがあります。

公開鍵証明書と似ていると言われる印鑑登録証明書の場合も、取得できるのは本人に限られ、開示する相手は本人が選択できます。さらに、発行された印鑑登録証明書の開示先を本人が制限することが可能であり、また、印鑑登録証明書を使用する取引は、事実上重要な取引に限られています。

商業登記に基礎を置く電子認証の公開鍵証明書に記載される事項は、法人の商号や本店所在地などと代表者の氏名だけなので、個人情報は代表者の氏名だけです。また、特定認証業務による公開鍵証明書も、氏名や組織の情報あるいはメールアドレスなどです。

一方、公的個人認証による公開鍵証明書は、本人特定用に住所、氏名、生年月日、性別の 4 情報が表示されています。現在は、現在は検証者が政府機関や各地方公共団体で、用途が政府機関や各地方公共団体への各種届出・申請などに用途制限されていますが、今後民間での利用が認められることになると、何らかの個人情報保護対策が必要になることは必至です。

4. e 文書法

(1) e 文書法の構成

e 文書法は、税法や商法、労働法などの各種法令により、民間企業が作成・保存することを義務付けられている文書・帳票類の電磁化（電子的・磁気的）を、一部の例外を除いて一括して認める法律の通称で、電子文書法とも呼ばれています。通則法と整備法の 2 つの法律から構成され、2004 年 11 月 19 日に成立し、2005 年 4 月 1 日に施行されました。

通則法の正式名称は「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」といい、文書保存を義務付けている各法律に対して原則としてすべて電子保存を認める通則を示し、その目的や言葉の定義、条件などの共通事項を定めています。

一方の整備法は正式名称を「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」といい、通則法のみでは不足する規定整備を行うもので、個別の法律の部分改正を具体的に規定しています。

民間に文書の保存を義務付けている法律は、電子帳簿保存法のように電子データを認めるもの、紙媒体での保存でなければならないものなど個別の法律によって要件や内容が異なっていましたが、e-文書法はこれらに対して一括して電子保存を認め、251 の法律が実質的に改正されました。

e 文書法では、初めから電子文書として作成された文書（電子文書）の保存だけでなく、紙で作成された書類をスキャナで読み込んだイメージファイルなど（電子化文書）も一定の技術要件を満たせば原本と見なすことを認めています。ただし、緊急時に即座に確認する必要があるもの（船舶に備える安全手引書など）や現物性が極めて高いもの（免許証、許可証など）、適正公平な課税確保のための一部文書など約 50 の法令にかかわる文書は除外されています。

(2) e 文書法関連の政省令

e-文書法では、電子保存の具体的な方法や要件については規定せず、文書内容の重要性や消失・改ざん・漏えいなどが発生した場合の影響の大きさなどによって、各省庁が省令によって定めることになっています。

以下は、財務省令の抜粋です。ここでは、電子署名とタイムスタンプの双方が義務付けられています。

電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律施行規則の一部を改正する省令（平成 17 年財務省令第 1 号）

（省略）

二　前号の入力に当たっては、次に掲げる要件を満たす電子計算機処理システムを使用すること。

イ　（省略）

ロ　当該国税関係書類をスキャナで読み取る際に、一の入力単位ごとの電磁的記録の記録事項に、当該入力を行う者又はその者を直接監督する者の電子署名（認定認証事業者（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第四条第一項（認定）の認定を受けた者をいう。以下この号において同じ。）により同法第二条第三項（定義）に規定する特定認証業務が行われる同条第一項に規定する電子署名又は商業登記法（昭和三十八年法律第百二十五号）第十二条の二第一項第一号（電磁的記録の作成者を示す措置の確認に必要な事項等の証明）に規定する措置で次に掲げる要件を満たすものに限る。以下この号及び第八条において同じ。）を行うこと。

（省略）

ハ　当該国税関係書類をスキャナで読み取る際に、電子署名が行われている当該国税関係書類に係る電磁的記録の記録事項に財団法人日本データ通信協会（昭和四十八年十二月十日に財団法人日本データ通信協会という名称で設立された法人をいう。）が認定する業務に係るタイムスタンプ（次に掲げる要件を満たすものに限る。以下この号及び第八条において「タイムスタンプ」という。）を付すこと。

（以下省略）

＜財務省令抜粋＞

平成 17 年 2 月 28 日
国税庁長官

「電子帳簿保存法取扱通達の制定について」の一部改正について（法令解釈通達）

（省略）
（タイムスタンプの付し方）
4-28 規則第 3 条第 5 項第 2 号ハ（(タイムスタンプ)）の規定の適用に当たり、「電子署名が行われている当該国税関係書類に係る電磁的記録の記録事項」とは、電子署名を行うことにより作成された電磁的記録の記録事項（以下 4-28 において「電子署名データ」という。）及び国税関係書類に係る電磁的記録の記録事項（以下 4-28 において「画像データ」という。）の両方を指すのであるから、電子署名データと画像データの両方を対象として、一のタイムスタンプを付す必要があることに留意する。
（以下省略）

＜財務省令抜粋＞

(3) 文書の保存期間

以下に、文書の保存期間を参考のために列挙します。

A) 行政機関が保有する文書の保存期間

行政文書の管理方策に関するガイドライン」では、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）及び法律施行令（平成 12 年政令第 41 号）の制定に伴う、各行政機関における行政文書の管理方法に関する定めを行っています。

保存期間 30 年

・条約その他の国際約束の署名又は締結のための決裁文書、法律の制定・改廃の決裁文書、特殊法人の設立・廃止の決裁文書、基本的な計画の策定・変更・廃止の決裁文書、予算・組織・定員の基本的事項の決裁文書
・認可法人の設立・廃止の決裁文書
・関係閣僚会議付議のための決裁文書、政務次官会議付議のための決裁文書、事務次官等会議付議のための決裁文書
・府省令等の制定・改廃のための決裁文書、行政文書の管理に関する定め
・公益法人設立許可の決裁文書、事業免許、資格免許等の許認可の決裁文書
・判決書（正本）
・国有財産台帳
・決裁簿
・行政文書ファイル管理簿
・公印の制定、改正又は廃止を行うための決裁文書
・特殊法人又は認可法人の管理のための台帳

保存期間 10 年

・審議会等の答申、建議又は意見

・法令の解釈・運用基準の決裁文書、許認可等の審査基準、不利益処分の処分基準
・有効期間が 10 年以上の許認可等をするための決裁文書
・条約その他の国際約束の解釈・運用基準の決裁文書、所管行政に係る重要な政策の決定に係る決裁文書
・行政不服申立て、行政審判その他の争訟の裁決書、裁定書、決定書
・叙勲、褒章又は各種表彰の決裁文書
・政策決定の基礎となった国際会議等の決定、概算要求書

B) 法人が保有する文書の保存期間

株式会社、宗教、学校などの法人が法人活動を行う上で長期保存が義務付けられている文書について以下に示します（http://www.the-soumu.com/から引用）

永久保存

・定款、株主総会議事録、取締役会議事録、株主名簿、社債原簿
・登記済証（権利証）など登記・訴訟関係書類官公署に対する提出文書、官公署の許可書、認可書、命令書、通達などで重要な書類
・特許、実用新案、意匠、商標など工業所有権に関する特許料・登録料納付受領書や特許・登録証などの関係書類

保存期間 30 年

・特別管理物質の製造または取扱作業場において常時作業に従事する労働者に関する作業概要等の定期記録、およびその労働者の特定科学物質等健康診断個人票

保存期間 10 年

・商業帳簿および営業に関する重要書類…貸借対照表・損益計算書・営業報告書・利益処分案とそれぞれの付属明細書、総勘定元帳、各種補助簿、株式申込簿、株式割当帳、株式台帳、株主名義書換簿、配当簿、印鑑簿、倉庫証券簿、判取帳など

保存期間 7 年

・取引に関する帳簿…仕訳帳、現金出納帳、固定資産台帳、売掛帳、買掛帳、経費帳、帳簿代用書類など決算に関して成された書類…たな卸表など
・現金の収受・払出し、預貯金の預入れ・引出しに際して作成された取引証憑書類…領収証、預金通帳、借用証、小切手・手形控、振込通知書など
・有価証券の取引に際して作成された証憑書類…有価証券受渡計算書、有価証券預り証、売買報告書、社債申込書など
・たな卸資産の引渡し・受入れに際して作成された書類以外の取引証憑書類（資本金一億円超の大法人の場合）…請求書、注文書、契約書、見積書、仕入伝票など
・給与所得者の扶養控除等（異動）申告書、保険料控除申告書、源泉徴収簿（賃金台帳）、住宅取得控除申告書

5. PKI とデジタル署名

公開鍵を認証するしくみは公開鍵基盤（PKI）とよばれています。以下では、PKI とデジタル署名の関係を少し詳細に解説します。

(1) 公開鍵基盤

公開鍵基盤（PKI：Public Key Infrastructure）は、公開鍵暗号を用いて電子署名や電子認証（本人確認）を実現するための基盤です。公開鍵基盤の構成を図 1-3 公開鍵基盤に示します。通常は、これらの構成要素をひとまとめにして認証局と呼んでいます。

署名者が公開鍵基盤を利用するときは、先ず始めに、鍵生成ツールを使って「公開鍵」と「秘密鍵」の鍵ペアを生成します（①）。次に、署名者はこの鍵ペアが署名者のものであることを示す公開鍵証明書を発行してもらうために「登録局」に行き、本人確認を受けた後（②）、「認証局」に「公開鍵」を提出して公開鍵証明書を受け取ります（③）。一方、検証者は、「認証局」から検証に必要な公開鍵証明書や CRL を取得することができます（④）。

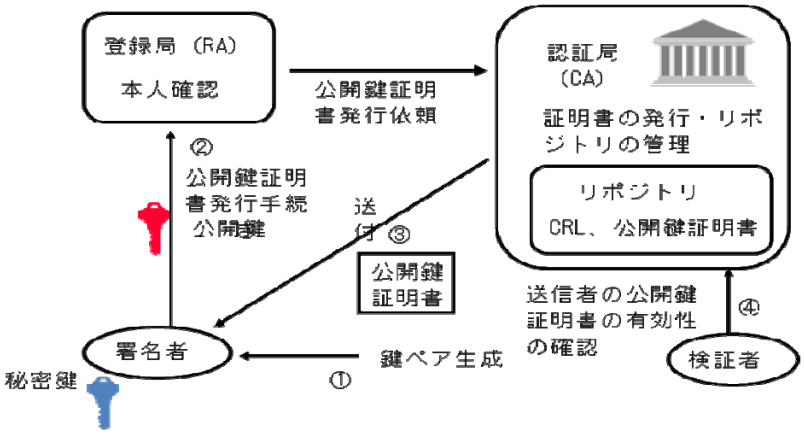


図 1-3 公開鍵基盤

公開鍵基盤の基本的な構成要素である、登録局、認証局及び認証局内のリポジトリの役割は次の通りです。

A) 登録局（RA：Registration Authority）

本人の申請を受け、本人確認を行い、本人に関する情報の登録を行ない、認証局に対して公開鍵証明書（Certificate）の発行依頼を行ないます。

また、公開鍵証明書の失効や更新の際にも公開鍵証明書所有者からの申請を受け、認証局に対して失効の依頼を行います。

B) 認証局（CA：Certification Authority）

登録局からの依頼を受け、証明書ポリシー（CP：Certificate Policy）に従って、公開鍵証明書（Certificate）を発行し、申請者に送付します。また、登録局の指示により、公開

鍵証明書の失効や有効期間がすぎた場合にリポジトリの失効情報の更新を行います。

認証局は、認証局運営規定（CPS：Certification Practice Statement）に従って運営されます。認証局運営規定は認証局を利用する人に対して認証局の信頼性・安全性を明示するための文書で、認証局の運用に関するセキュリティポリシーも含まれます。一方、証明書ポリシーは認証局が発行する証明書の記載事項や本人確認方法等を明記した文書を指します。

C) リポジトリ（Repository）

公開鍵証明書に関する情報を記憶するもので、認証局が管理します。公開鍵証明書や公開鍵証明書の失効リスト（CRL）が格納され、利用者は必要なときにリポジトリから最新の証明書や失効情報を得ることができます。

(2) 公開鍵証明書および失効情報

A) 公開鍵証明書（Certificate）

現在広く用いられている公開鍵証明書は ITU（国際電気通信連合）が 2000 年に勧告した X.509 第 3 版（X.509v3）です。X.509v3 の公開鍵証明書は図 1-4 のように、必須情報である基本領域と拡張領域及び発行者の署名から構成されます。

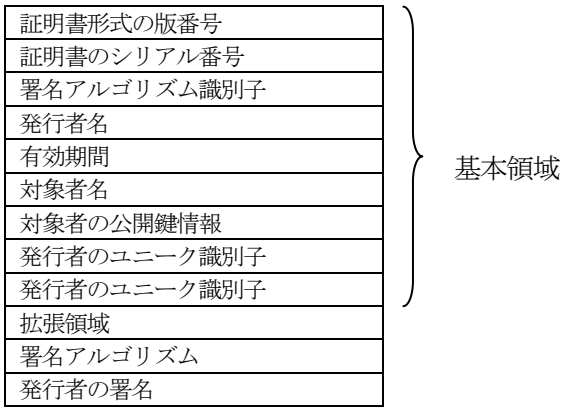


図 1-4 公開鍵証明書

拡張領域には、鍵用途、証明書ポリシー、CRL 配付元情報などを格納することができます。

鍵用途は、秘密鍵と公開鍵のペアをどのような用途に使うことができるかを表示します。表 1-1 は、鍵用途の一覧です。鍵用途は複数指定することも可能です。

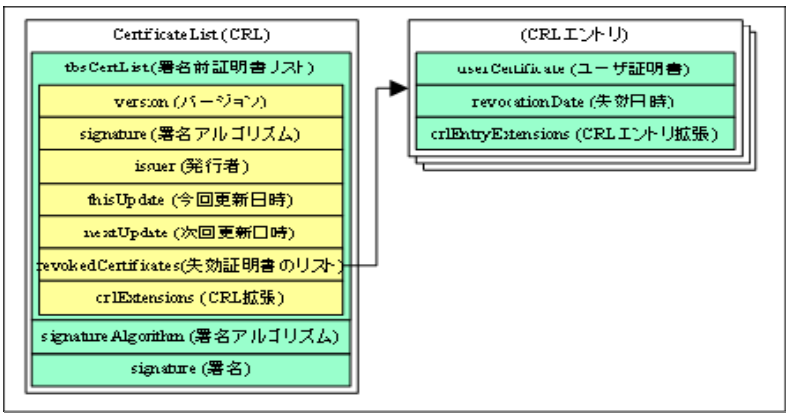
表 1-1 鍵用途

名称	鍵使用目的
digitalSignature	デジタル署名の検証に利用します。
nonRepudiation	否認防止を目的とした、デジタル署名の検証に利用します。
keyEnciperment	鍵配送を目的とした、共通鍵などの鍵の暗号化に利用します。
dataEncipherment	データの暗号化に利用します。
keyAgreement	DH アルゴリズムなどによる鍵合意(Key Agreement) に利用します。
keyCertSign	証明書の署名を検証するために利用します。CA 証明書のみ有効です。
cRLSign	証明書失効リスト(CRL)の署名を検証するために利用します。
encipherOnly	データの暗号化にのみ利用します。keyAgreement が指定されている場合のみ指定可能です。
decipherOnly	データの復号にのみ利用します。keyAgreement が指定されている場合のみ指定可能です。

http://www.ipa.go.jp/security/pki/033.html

B) 証明書失効リスト (CRL : Certificate Revocation List)

単に失効リストとも言い、失効した公開鍵証明書に関する情報リストです。公開鍵証明書の失効 (Revocation) とはその有効期間内に、秘密鍵の漏洩や技術の進歩により秘密鍵の秘匿性が失われたり、申請者の氏名変更など証明書記載事項に変更があった場合に公開鍵証明書そのものを無効にすることを云います。失効リストは、発行者名、発行時刻、次に発行を行う予定の時刻、及び失効した公開鍵証明書 (シリアル番号、失効日時、失効理由など) のリストから成ります (図 1-5)。失効理由は、利用者や認証局の秘密鍵の危殆化、記載事項変更、一時保留などが定義されています。



http://www.ipa.go.jp/security/pki/042.html

図 1-5 失効リスト

C) OCSP

OCSP (Online Certificate Status Protocol) は、証明書が有効か否かをオンラインで問い合わせるためのプロトコルです。証明書のシリアル番号を送り、その時点の証明書のステータスを受け取ります。ステータスは、有効 (good)、失効 (revoked)、不明 (unknown) のいずれかで、失効 (revoked) の場合は、失効日時と失効理由が示されます。

(3) 認証局の信頼性

公開鍵証明書が信頼できるものであるためには、その公開鍵証明書が、信頼する認証局（これをトラストアンカーという）から発行されたものであるか、あるいは信頼する認証局が直接あるいは間接的に認証した認証局から発行されたものである必要があります。認証局の信頼モデルとして「単一モデル」、「階層モデル」、「メッシュモデル」、「ブリッジモデル」などがあります（図 1-6）。

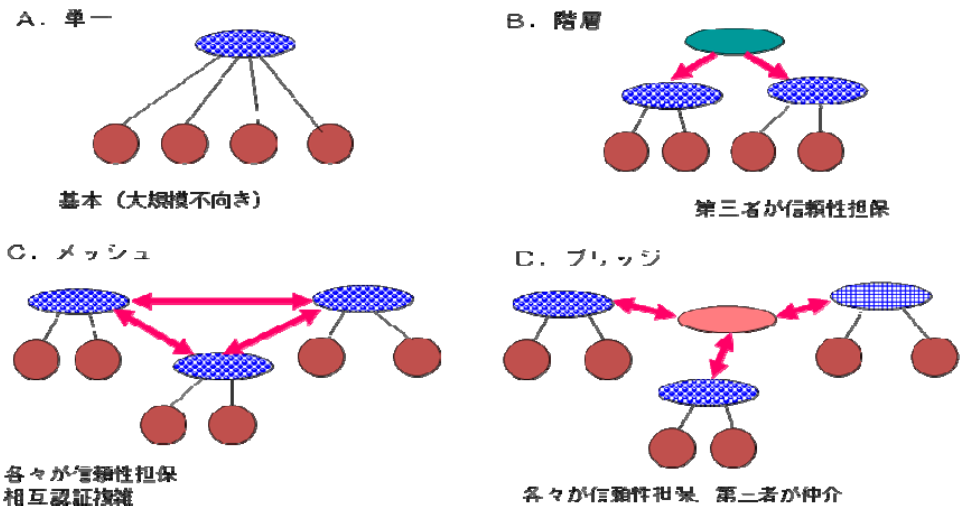


図 1-6 認証局の信頼モデル

A) 単一モデル

1 つの認証局（トラストアンカー）で構築される方式です。

B) 階層モデル

複数の認証局を階層型（ツリー構造）に構成する方式です。最上位の認証局をルート CA と呼び、このルート CA がトラストアンカーであれば、順次次の層の認証局を信頼することにより、認証局をルート CA の直接及び間接的な信頼関係で結ぶことができます。

C) メッシュモデル

複数の認証京同士で相互認証（Cross Certification：認証局同士が相互に相手の公開鍵に対する証明書（相互認証書）を発行しあうこと）により信頼関係を構築する方法です。

D) ブリッジモデル

複数の認証局がブリッジ CA と相互認証することにより間接的に信頼関係を構築する方法で、メッシュモデルに比べて構造を単純にすることがでます。

なお、このほかに、信頼性をブラウザに頼るモデルを「Web モデル」と呼んでいます。Web モデルは一般に広く利用されているブラウザ（Internet Explorer や Netscape Communicator）にプリインストールされているトラストアンカーを信頼するモデルですが、トラストアンカーを利用者が選択できるわけではありません。

(4) デジタル署名の生成と検証

図 1-7 に、デジタル署名の生成処理と検証処理の流れを示します。

ここでは、次の 3 つに分けて説明します。

・デジタル署名の生成

・デジタル署名の検証

・公開鍵証明書の有効性検証

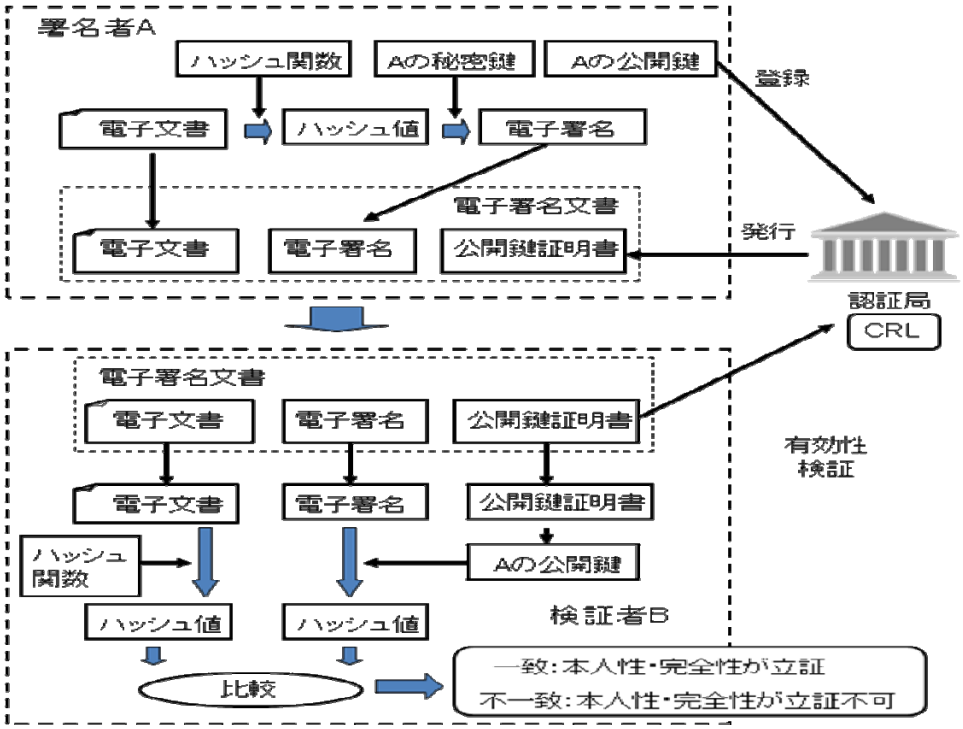


図 1-7 デジタル署名の生成と検証

A) デジタル署名の生成

署名者は次の手順でデジタル署名を行ないます。

①署名者は、ハッシュ関数を用いて署名する文書のハッシュ値を生成。

②次に、生成したハッシュ値を署名者の秘密鍵で暗号化（この暗号化されたデータを署名または署名値と言う）。

③公開鍵証明書を添付。

B) デジタル署名の検証

署名検証者の処理の流れは次の通りです。

①文書からハッシュ値を生成。

②添付されている公開鍵証明書の有効性を確認するために、公開鍵証明書を発行した認証局から失効情報を入手し、公開鍵証明書の有効性を確認。

③公開鍵証明書が有効であれば、署名者の公開鍵で署名を復号し、①で生成したハッシュ

値と比較。一致した場合、送信者の秘密鍵で電子署名が生成されたこと（本人性）及び電子文書が途中で第三者によって改ざんされていないこと(非改ざん性)が確認できる。

C) 公開鍵証明書の有効性検証

公開鍵証明書の有効性を調べるため、以下の検証を行います。

①検証したい公開鍵証明書から出発して、公開鍵証明書に格納された発行者識別（issuer）などによって信頼関係を順にたどり、自分が信頼している認証局（トラストアンカー）までたどれるかを確認。

②有効性を検証する時刻が、公開鍵証明書の有効期間内にあることを確認。

③公開鍵証明書が、検証時刻に失効していないことを、CRL または OCSP により確認。

④公開鍵証明書のポリシーと整合性があることを確認。

D) 署名フォーマット

現在、基本的な署名フォーマットとして、抽象構文記法（ASN.1）で記述された CMS 署名フォーマットと XML で記述された DSIG 署名フォーマットの 2 つの標準があります。

RFC5652：“Cryptographic Message Syntax (CMS)”

RFC3275：“(Extensible Markup Language) XML-Signature Syntax and Processing”

CMS 署名フォーマットは、電子メールや PDF の署名などに使われており、DSIOG 署名フォーマットは Office 文書（拡張子が.docx など）を含む XML 文書の署名に使われています。

図 1-8 は CMS 署名フォーマットの構造です。図の中のカプセル化コンテント情報と署名属性が署名対象です。カプセル化コンテント情報には署名対象のオブジェクト(文書)が格納され、署名属性には、署名者証明書の参照情報などが格納されます。

<table>
<tr><td colspan="2">版番号</td></tr>
<tr><td colspan="2">ダイジェストアルゴリズム</td></tr>
<tr><td colspan="2">カプセル化コンテント情報</td></tr>
<tr><td colspan="2">証明書</td></tr>
<tr><td colspan="2">失効情報</td></tr>
<tr><td rowspan="7">署名者情報</td><td>版番号</td></tr>
<tr><td>署名者識別子</td></tr>
<tr><td>ダイジェストアルゴリズム</td></tr>
<tr><td>署名属性</td></tr>
<tr><td>署名アルゴリズム</td></tr>
<tr><td>署名値</td></tr>
<tr><td>非署名属性</td></tr>
</table>

図 1-8 CMS 署名フォーマット

第2章　電子署名の利用

1.　電子署名の普及状況

ここでは、電子署名を利用するシステムの代表例として、省庁共通の電子申請システムである e-Gov 電子申請システム及び自治体が協同運営する eLTAX についてその普及状況、並びに、東京都を例にとり具体的なサービス内容を掲載します。

このほか、民間においては、電子契約、PL 法対応、先使用権保護、取締役会議議事録の電子化、医療分野での電子カルテや外部保存での利用など、戦略的な先行事例があります。これらの先行事例は、次の資料が参考になります。

電子認証局会議　電子署名活用ガイド

http://www.c-a-c.jp/pdf/digital_signature_guidebook_CAC.pdf

表 2-1 は e-Gov 電子申請システムで電子申請可能な府省別行政手続きの種類、表 2-2 は eLTAX の年度毎の利用状況です。

表 2-1 省庁別行政手続一覧

府省名(順不同)	手続き数
内閣官房	7
内閣府	223
公正取引委員会	64
国家公安委員会･警察庁	247
金融庁	1,475
総務省	928
財務省	235
国税庁	7
厚生労働省 (厚生労働省には、社会保険庁及び中央労働委員会を含んでいます。)	4,918
農林水産省	828
林野庁	114
水産庁	459
経済産業省 (経済産業省には、資源エネルギー庁、特許庁及び中小企業庁を含んでいます。)	3,114
環境省	257
合計	12,876

※ 平成 21 年 9 月 30 日現在の e-Gov で申請可能な手続き数（参照元の表記では件数）

http://www.e-gov.go.jp/shinsei/content-list.html

表 2-2 eLTAX の利用状況

（単位：件）

	申告						納付手続	申請・届出
	法人都道府県民税・事業税・地方法人特別税	法人市町村民税	個人住民税	固定資産税（償却資産）	事業所税	合計		
運用開始以降の累計	1,507,943	423,834	164,486	88,404	2,047	2,186,714	1,798	8,113
平成21年度（9月30日現在）	507,686	185,592	1,255	3,035	1,225	698,793	1,380	4,898
平成20年度	651,776	164,958	133,576	58,491	784	1,009,585	410	3,188
平成19年度	306,376	65,129	29,655	23,186	38	424,384	8	27
平成18年度	36,199	7,691	－	2,969	－	46,859	－	－
平成17年度	5,756	464	－	723	－	6,943	－	－
平成16年度	150	－	－	－	－	150	－	－

（注1）eLTAXの運用開始は、平成17年1月です。
（注2）年度の件数は、4月から翌年3月までの集計値です。

http://www.eltax.jp/outline/number_h21.html

表 2-3 は東京都の公的個人認証サービス対象手続きの導入状況です。自治体毎の手続き数の集計値を示しています。公的個人認証サービス対象手続きの数は市区町村によって差がありますが、住民票写し交付、軽自動車税納税証明書、納税証明書などが共通しています。

表 2-3 東京都の公的個人認証サービス対象手続きの導入状況

自治体	手続き数
東京都	73
荒川区	87
葛飾区	24
中野区	17
清瀬市	15
昭島市	14
足立区、目黒区、日野市	9
東村山市、板橋区、東大和市	8
台東区、墨田区、豊島区、八王子市、	7
港区、新宿区、練馬区、	6
府中市、町田市、羽村市	5
北区、立川市、調布市、小金井市、小平市、多摩市、日野で長	4
中野区、江戸川区、瑞穂町	3
江東区、青梅市、西東京市、武蔵村山市、西東京市	2
千代田区、文京区、品川区、世田谷区、渋谷区、杉並区、武蔵野市、三鷹市、国分寺市、国立市、福生市、狛江市、稲城市、あきるの市、檜原村、奥多摩町、大島町、利島村、新島村、神津島村、三宅村、御蔵島村、八丈町、青ヶ島村、小笠原村	なし

http://www.jpki.go.jp/jpkiguide/admin_proce/area/pdf/13_service_dounyuu.pdf

事例として表 2-5 に東京都港区におけるサービスを紹介します。

表 2-4 サービス事例

サービス	サービス開始日
児童手当額改定認定請求・額改定届	2005/01/25～
児童手当受給事由消滅届	2005/01/25～
児童手当振込口座変更届	2005/04/01～
住民票の写し交付申請	2005/01/25～
住民票記載事項証明書交付申請	2005/01/25～
乳幼児・子ども医療証再交付申請	2005/01/25～

2. 電子政府や自治体における電子署名の利用

以下では、電子申請システムを例に、利用者から見て電子署名がどのように使われているか、どのように使えばよいか概要を紹介します。

(1) e-Gov 電子申請システム

e-Gov 電子申請システムは各府省共通のシステムとなっており、表 2-5 の機能をもっています。これ以外に、各府省個別のシステムがあり、国税庁の国税電子申告・納税システム (e-Tax) や、社会保険庁の電子申請システムなどは個別対応になっています。

表 2-5 e-Gov 電子申請システムの主要機能

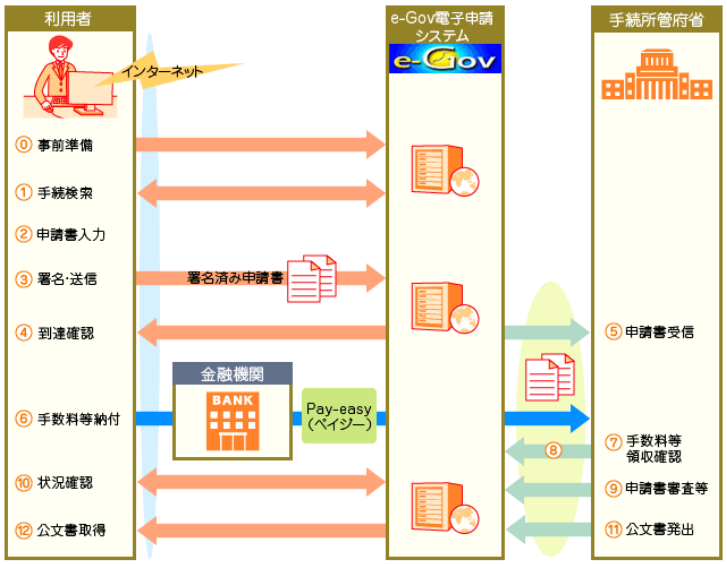
申請・届出	
申請(申請者・代理人)	申請や届出などの行政手続を、インターネットを利用して自宅や会社のパソコンを使って行います。
委任または委任情報の確認	
委任申請(申請者本人)	電子申請を代理人への委任するための手続を行います。
委任照会	発行済みの委任登録票発行番号と問合せ番号から委任状況の照会を行います。
委任検証	お手持ちの委任登録票の使用可否を検証します。
※手続によっては、代理人による申請、届出が認められる場合があります	
複数名で氏名を連ねて(連名して)申請・届出	
連名申請(連名代表者)	複数名で氏名を連ねて(連名して)申請・届出を行います。
署名追加	保存した申請データに署名を追加します。
連名申請提出	複数名で氏名を連ねて(連名して)申請・届出を行います。
個別ファイル署名で署名を追加	
署名追加	保存した申請データに署名を追加します。
複数の手続について、一括して申請・届出	
グループ申請	複数の申請・届出について、同一の記載項目の重複入力を省略した上で一括して申請します。
署名追加	保存した申請データに署名を追加します。
複数署名申請提出	グループ申請を行う際の複数署名済み申請データの提出を行います。
申請・届出等の状況照会	
状況照会	申請の状況を確認することができます。
通知照会	通知申請時に発行された通知発行番号と問合せ番号を確認できます。

公文書署名検証	電子公文書に付与された電子署名及び証明書を検証することにより、以下のことが確認できます。 電子公文書が、 ・改ざんされていないか 電子証明書が、 ・失効していないか ・有効期限が切れていないか ・政府認証基盤(GPKI)のブリッジ認証局(BCA)により相互認証された認証局から発行されているか
パーソナライズの利用	
パーソナライズの開設	利用者個人向けページを新規に開設し、ログインに必要な ID とパスワードを作成します。
パーソナライズの照会	パーソナライズに登録した手続情報、申請案件情報を確認できます。

http://www.e-gov.go.jp/shinsei/content.html

(2) 電子申請の手順

電子申請の手順を図 2-1 に示します。



http://www.e-gov.go.jp/shinsei/way.html

図 2-1 電子申請の手順

○事前準備

e-Gov 電子申請システムを使って電子申請をするためのパソコンの環境を整えます。

［申請書の作成・送信］

①手続検索

キーワードや所管府省を指定して行う行政手続を検索します。

また、検索後表示できる手続案内において署名の要否や記入要領を確認します。

②申請書入力

選択した行政手続の申請書入力様式に必要な事項を入力します。

また、選択した手続において必要とされている書類等を添付します。

③署名・送信

電子署名が必要とされている手続の場合、あらかじめ取得済みの電子証明書を利用して電子署名を行い、申請書を送信します。

電子署名が必要のない手続の場合は、そのまま送信します。

送信された申請書について、形式チェック、ウィルスチェック、証明書の有効性検証等を行った後、エラーが見つからない場合に到達番号と問合せ番号を払い出します。到達した申請書は、手続所管府省に転送されます。(図の⑤)

④送達確認

⑤所管府省が申請書受信

⑥手数料等納付

申請・届出を行う際に手数料等の納付を必要とする手続の場合、手数料等の納付を行います。利用金融機関がPay-Easyに対応している場合は、ATMやインターネットバンキングから手数料等の電子納付をすることができます。

⑦⑧手数料等領収確認

手数料等の払込み後、選択した行政手続を所管している府省において、当該手数料の領収確認を行います。領収確認後、納付済みであることがe-Govに通知されます。なお、手数料等の領収を確認できるまで、申請書等の審査が保留されることがあります。

[申請・届出の状況確認]

⑨所管府省が申請書審査

行政手続を所管する府省では、申請者が提出した申請書について必要な審査を行います。

申請書の記入内容に誤り等がある場合には、e-Gov の状況確認⑩を通じて申請者に対して申請書の訂正を求めます。

⑩申請・届出の状況確認

到達確認時に払い出される到達番号と問合せ番号により、行った申請・届出の処理状況を確認できます。

提出した申請書について訂正等の必要がある場合には、手続の所管府省が発する補正の求め等の内容を確認し、これに従って申請書を訂正します。

⑪所管府省が公文書発行

⑫公文書取得

行政手続の所管府省により公文書が発出された場合（図の⑪)、申請者は e-Gov の状況確認から当該公文書を取得することができます。

公文書に官職証明書による電子署名が付けられている場合、この官職証明書が有効なものであるかどうか確認することができます。

(3) 電子納付

インターネットで行政手数料などの支払いができるよう、国庫金取り扱い金融機関のインターネットバンキングやATMを利用して、電子納付ができるようになっています。国庫金の電子納付には、申請・届出等の都度、官公庁から発行された収納機関番号・納付番号・確認番号を

入力して払い込みます。

金融機関によって利用できる納付方法が異なります。利用可能な金融機関は、Pay-easy（ペイジー：税金・各種料金払込みサービス）に対応した金融機関で、銀行、信託銀行、信用金庫、信用組合、農協・漁協（農林中央金庫）、労働金庫となっています。

(4) 電子申請を行うにあたっての準備

以下では、電子申請を行う場合に必要となる準備作業の流れをご説明します（時々改定されていますので、実際の流れと異なる場合があります）。

A) パソコンの準備

電子申請を行うには、図 2-2 の準備が必要となります。

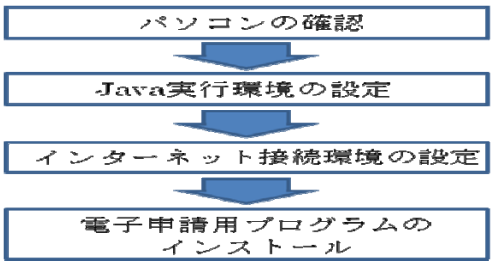


図 2-2 パソコンの準備

(a) パソコン環境

推奨が、CPU800MHz、メモリ 384MB、ハードディスク空き容量 100MB、OS は Windows 2000 SP4 以上または MAC OS X v10.4 以上となっていますので、ほとんどのパソコンはこの推奨環境をクリアしていると考えられます。

WindowsVista の場合は、e-Gov 電子申請システム（https://shinsei.e-gov.go.jp）を信頼済みサイトとして登録する必要があります。

(b) Java 実行環境の設定

最新の Java 実行環境（JRE）が推奨されています。JRE は、Java 言語で開発されたソフトウェアを実行するために必要なソフトウェアのセットです。Java を用いて開発されたソフトウェアは、プラットフォームに依存しない Java バイトコードで配布されるため、これを実行するための Java 仮想マシンなどのソフトウェアが必要です。

(c) インターネット接続環境の設定

公開鍵証明書の有効性を検証するために、認証局のレポジトリにある CRL にアクセスするための LDAP プロトコルが利用可能なことが必要です。

(d) 電子申請用プログラムのインストール

ダウンロードページからクライアントモジュールをダウンロードしインストールします。

安全な通信を行うためには、SSL のルート証明書の取り込みが必要です。正しいルート証明書が取り込まれたかどうかは、パソコンに取り込んだルート証明書のハッシュ値（フ

ィンガープリント）と、公開されている下記フィンガープリントとを比較することにより確認します。

ブリッジ認証局の自己証明書のフィンガープリント
SHA-1 615C B655 772A 67BB D4DD 2826 F5CD DEDD A616 F386
官職認証局の自己署名証明書のフィンガープリント
SHA-1 260D F56A 91EA B3BA E6F7 DA57 EC64 9D27 39D1 6A78
アプリケーション認証局の自己署名証明書のフィンガープリント
SHA-1 7F8A B0CF D051 876A 66F3 360F 47C8 8D8C D335 FC74

注：実際に比較する場合は、指定されたサイトをアクセスして確認してください。

B) 電子署名用公開鍵証明書の準備

e-Gov で電子申請する場合に利用できる電子証明書を発行している認証局（特定認証業務）は次の通りです（2009 年 2 月現在）。

・「商業登記に基礎を置く電子認証制度」を運営する電子認証登記所
・「AccreditedSign パブリックサービス 2」を提供する日本認証サービス株式会社
・「AOSign サービス」及び「法人認証カードサービス」を提供する日本電子認証株式会社
・「TOiNX 電子入札対応認証サービス」を提供する東北インフォメーション・システムズ株式会社
・「TDB 電子認証局サービス TypeA」を提供する株式会社帝国データバンク
・「セコムパスポート for G-ID サービス」を提供するセコムトラストシステムズ株式会社
・「電子入札コアシステム用電子認証サービス」を提供するジャパンネット株式会社
・「全国社会保険労務士会連合会認証サービス」を提供する全国社会保険労務士会連合会
・「ビジネス認証サービス　タイプ 1-E、1-A、1-G」を提供する日本商工会議所
・「よんでん電子入札対応認証サービス」を提供する四国電力株式会社
・「MJS 電子証明書サービス」を提供する株式会社ミロク情報サービス
・「公的個人認証サービス」を提供する地方公共団体
・「CTI 電子入札・申請届出対応電子認証サービス」を提供する株式会社中電シーティーアイ
・「税理士証明書発行サービス」を提供する日本税理士会連合会
・「日本司法書士会連合会認証サービス」を提供する日本司法書士会連合会
・「e-Probatio PS2 サービス」を提供する株式会社 NTT アプリエ
・「日本土地家屋調査士会連合会認証サービス」を提供する日本土地家屋調査士会連合会
・政府認証基盤（GPKI）の政府共用認証局（官職認証局）
・地方公共団体組織認証基盤（LGPKI）の組織認証局

なお、認証局から IC カードで電子署名用電子証明書の交付を受ける場合、その IC カードのドライバソフトウェアが CSP（注 1）及び PKCS#11（注 2）に対応しているものであれば、

e-Gov で電子申請を行う際に、IC カードを読み込んで電子署名をすることができます。

（注 1）CSP（Cryptographic Service Provider）は、Windows OS とともにインストールされている暗号化やハッシュ値の計算等の機能を受け持つソフトウェアエンジンです。

（注 2）e-Gov では、「PKCS#11 を利用する場合のインタフェース仕様」で定義されている仕様に対応しています。

なお、自治体の電子申請についても次のように同様の準備が必要となります。

図 2-3 公的個人認証サービスポータルサイト

(5) 文字コードの制限

e-Gov 電子申請システムにおいては、環境依存文字（JIS 第 3 水準漢字、第 4 水準漢字等）及び、下記の機種依存文字（代表的なもののみを記載）を正しく取り扱うことが出来ません。但し、添付書類の内容については対象外です。

- 囲み英数字（丸文字） ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳
- ローマ数字 Ⅰ Ⅱ Ⅲ Ⅳ Ⅴ Ⅵ Ⅶ Ⅷ Ⅸ Ⅹ
- 単位記号 ミリ キロ センチ メートル グラム トン アール ヘクタール リットル ワット カロリー ドル セント パーセント ミリバール ページ mm cm km mg kg cc m^2
- 年号 ㍾ ㍽ ㍼ ㍻
- 囲み文字 ㊤ ㊥ ㊦ ㊧ ㊨ ㈱ ㈲ ㈹
- 省略文字 №. ㏍ ℡
- 数学記号 ≒ ≡ ∫ ∮ Σ √ ⊥ ∠ ∟ ⊿ ∵ ∩ ∪
- 半角カタカナ 。「」、・ｦｧｨｩｪｫｬｭｮｯｰｱｲｳｴｵｶｷｸｹｺｻｼｽｾｿﾀﾁﾂﾃﾄﾅﾆﾇﾈﾉﾊﾋﾌﾍﾎﾏﾐﾑﾒﾓﾔﾕﾖﾗﾘﾙﾚﾛﾜﾝﾞﾟ
- その他 〝 〟

なお、漢字コードの JIS 改正に伴い一部の文字において、表示される字形が異なることがあります。表示が異なる文字については、「JIS 漢字コード表の変更について　―168 字の例示字形を変更―」（PDF）において確認することができます。
http://www.meti.go.jp/kohosys/press/0004964/0/040220jis.pdf

第3章　電子文書と長期保存

1.　デジタル署名の特徴

電子文書の真正性（本人性及び非改ざん性）は、デジタル署名を用いることによって確保することができますが、そのためには、デジタル署名に用いる秘密鍵に対応した有効な公開鍵証明書が必要です。

このため、公開鍵証明書は、次の点を考慮して利用する必要があります。

・公開鍵証明書には有効期間が必ず存在する。

・公開鍵証明書には失効が発生する可能性がある。

また、デジタル署名自体も次の点を考慮する必要があります。

・デジタル署名には信頼できる生成時刻を含んでいない。

・デジタル署名の基礎になる暗号技術は脆弱化して破られる可能性がある。

これら４つの考慮点はいずれも、長期保存を考える場合、デジタル署名の有効性の判断に大きな影響を与えます。

A)　公開鍵証明書の有効期間

公開鍵証明書には証明書の有効期間（開始日時～終了日時）が設定されています。有効期間の長さは認証局のポリシーによって決定されますが、数年が一般的です。図 3-1 に、公開鍵証明書の有効期間とデジタル署名生成時期による署名の有効性の関係を示します。デジタル署名の生成を公開鍵証明書の有効期間内に行い、且つ失効がなければ、公開鍵証明書の有効期間内の署名検証に対しては「有効」と判断されます。ところが、有効期間を過ぎた後に検証すると、通常、「無効」と判断されることになります。つまり、生成された当初は有効であったデジタル署名であっても、電子文書の真正性を確認できる期間は公開鍵証明書の有効期間内に制限されることになります。また、公開鍵証明書の有効期間外にその証明書に基づく署名を生成した場合も、有効なデジタル署名とは見なされません。これは、公開鍵証明書の有効期間外においては、秘密鍵が漏洩したことを通知する手段（CRL）がなく、漏洩した秘密鍵によってデジタル署名が生成されることを否定できないからです。

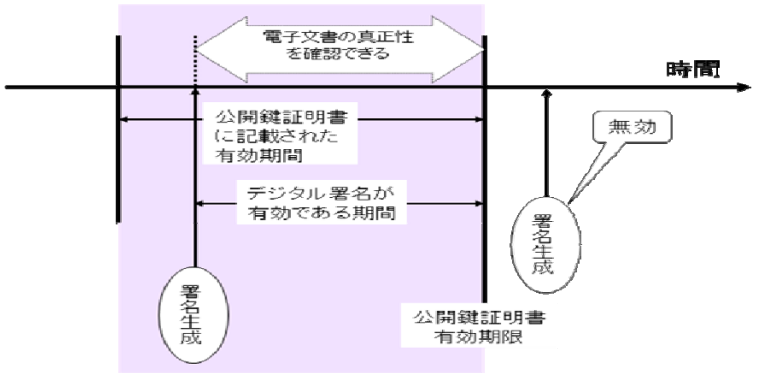


図 3-1 公開鍵証明書の有効期間と署名の有効性〔出典　文献 1〕

B)　公開鍵証明書の失効

公開鍵証明書の失効後とデジタル署名の有効性の関係を図示すると図 3-2 のようになります。公開鍵証明書の有効期間内であっても、失効後に生成されたデジタル署名は有効なデジタル署名とは見なされません。

公開鍵証明書の有効期間内であり、かつ失効前に生成されたデジタル署名であっても、一旦失効が発生するとそのデジタル署名の有効性は失われます。つまり、生成された当初は有効であったデジタル署名であっても、電子文書の真正性を確保できる期間は公開鍵証明書が失効するまでの期間に制限されることになります。

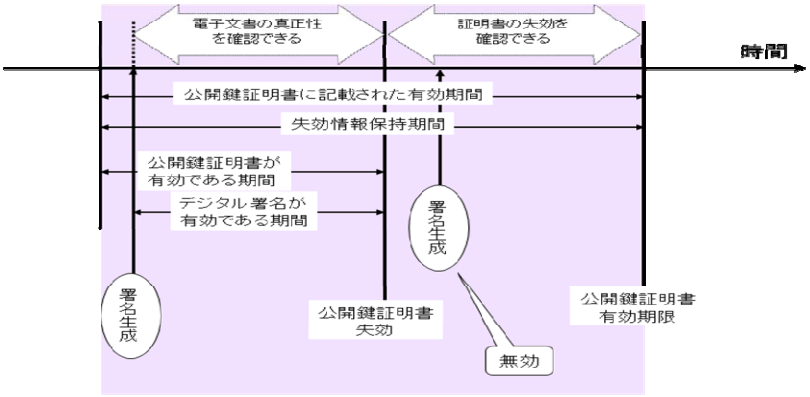


図 3-2 公開鍵証明書の失効と署名の有効性〔出典　文献 1〕

C)　デジタル署名が基礎とする暗号技術の脆弱化

現在のデジタル署名がよりどころとしているハッシュ関数や公開鍵暗号は、情報量的に安全性が保証されるものではなく、離散対数問題や素因数分解の計算量的な困難性に基づいています。従って、技術が進歩することによって、現在用いられているハッシュ関数や公開鍵暗号が脆弱化し、デジタル署名が容易に偽造されてしまう可能性があります。

一旦脆弱化した暗号技術に基づくデジタル署名は、偽造されたものと区別ができなくなるため、有効性を失うと考えなければなりません。公開鍵証明書は、技術動向を勘案して十分な安全性を保てるような有効期間を設定しているため、有効期間内に脆弱化して破られることは考えられません。しかし、証明書の有効期間を超えて電子署名文書を長期保存する場合には、脆弱化についても考慮しておく必要がでてきます。

SHA-1 の脆弱化

2005 年 2 月 15 日、世界的な暗号の権威である Bruce Schneier 氏のブログ「Schneier on Security」で「SHA-1 Broken」が公表された。中国・山東大学の Xiaoyun Wang 氏と Hongbo Yu 氏、セキュリティコンサルタントの Yiqun Lisa Yin 氏のチームが SHA-1 の攻撃に成功し、「2^{80}回の計算」をしなくても「2^{69}回の計算」で衝突するメッセージ組を見つけ出すことができというものであった。

2010 年問題

2006 年、NIST（米国立標準技術研究所）が、政府機関での使用を認める暗号アルゴリズムに関し、2010 年までは暗号強度（解読に要する計算量）を最小 80bit（2 の 80 乗）とし、2010 年以降は最小 112bit、2030 年以降は最小 128bit にする方針を打ち出した。2-key Triple DES、1024bit RSA, DSA、160bit ECDSA、SHA-1 が対象となる。

		等価安全性に相当する鍵長				
		80ビット安全性	112ビット安全性	128ビット安全性	192ビット安全性	256ビット安全性
共通鍵暗号		80	112	128	192	256
公開鍵暗号デジタル署名	素因数分解問題	1024	2048	3072	7680	15360
	離散対数問題	1024	2048	3072	7680	15360
	楕円曲線上の離散対数問題	160	224	256	384	512
ハッシュ関数		160	224	256	384	512

出典　SP 800-57　Recommendation on Key Management

2.　長期署名要件

電子文書の保存期間が公開鍵証明書の有効期間を越える場合もありますので、公開鍵証明書の有効期間後も、かつて署名が有効であったことを確認できる必要があります。このためには、次の要件を満たす必要があります。

・署名時刻を確定する
・再検証に必要な証拠情報を明確化する
・電子署名付文書と再検証に必要な情報を改ざん検知可能な状態にする
・電子署名文書や再検証に必要な証拠情報を改ざん検知可能な状態のままで保存する

これらの関係を図 3-3 に示します。

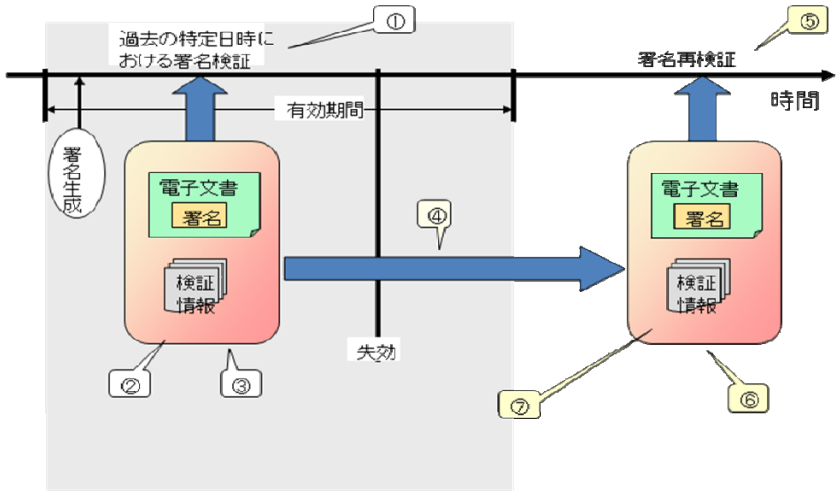


図 3-3 デジタル署名の有効性を長期にわたって維持するための要件〔出典　文献 1〕

①署名存在時刻を確定する

署名が証明書の有効期間内に存在したことを証明するために、信頼された時刻源から供給された時刻情報を用いて署名存在時刻を確定しておく必要があります。この手段としては、後述のタイムスタンプがあります。

②再検証に必要な証拠情報を明確化する

後日、署名の有効性を再確認可能にするためには、再確認に必要な情報をあらかじめ署名者と検証者の間の合意によって明確化しておき、署名検証時及び署名再検証時において、その情報をもとに署名の有効性を確認することが必要です。デジタル署名の有効性確認に必要な情報とは、署名検証において「有効な署名として成立」した事実を示す根拠となる情報であり、以下のようなものが挙げられます。

・署名者の公開鍵証明書、その署名者の公開鍵証明書が信頼する認証局までの公開鍵証明書、さらに、これらの公開鍵証明書が署名時点で失効していないことを示す情報（CRL など）。

・署名者と検証者が署名規則（署名ポリシー）合意したことの根拠となる情報

③電子署名付き文書と再検証に必要な証拠情報を改ざん検知可能な状態にする

「署名再検証に必要な証拠情報」に対しては、長時間経過した後でも改ざんされていないことを確認できる手段や情報が提供されていることが必要です。証明書や CRL をのまま保管した場合には、それらの情報に対して改ざんの有無を確認できる期間が、その公開鍵証明書の有効期間内に限定されてしまうことになります。従って、証拠情報内に含まれるデジタル署名の有効期間に依存することなく、長期にわたって収集した証拠情報すべての非改ざん性を確認可能とする技術が必要となります。

④電子署名文書や再検証に必要な証拠情報を改ざん検知可能な状態のままで保存する

必要な保存期間中、③のデータを改ざん検知可能な状態のままで保存します。

このように①～④の要件に沿った処置をほどこしておくことにより、長期経過後にデジタル署名を再検証する際に、⑤署名の存在時刻を確認し、⑥全ての証拠情報が改ざんされていないことを確認し、そして⑦確認された署名存在時刻を想定した上で証拠情報をもとに署名を検証するこ

とによって、もとのデジタル署名がその存在時刻においては有効であったことを確認することができます。

3. 長期署名フォーマット

(1) 長期署名フォーマットの構造

時間の経過と共に失われる可能性があるデジタル署名の有効性を維持すべく、第 1 章　図 1-8 の CMS 署名フォーマットや XML 署名フォーマットを拡張したフォーマットを長期署名フォーマットと言います。現在、以下のような長期署名フォーマット標準があります。

ETSI TS 101 733　“CMS Advanced Electronic Signatures (CAdES)”

ETSI TS 101 903　“XML Advanced Electronic Signatures (XAdES)”

ETSI TS 102 778　“PDF Advanced Electronic Signatures (PAdES)”

JIS X 5092 CMS 利用電子署名（CAdES）の長期署名プロファイル

JIS X 5093 XML 署名利用電子署名（XAdES）の長期署名プロファイル

CAdES、XAdES、PAdES を適用する代表的なアプリケーションとして、それぞれ、S/MIME 電子メール、オフィス文書（ODF や OOXML)、PDF などを挙げることができです。

長期署名フォーマットは、タイムスタンプ局やリポジトリ等の TTP を利用してデジタル署名の有効性を維持するための情報を生成する方法や、その情報をフォーマット内に格納する方法を規定しています。

図 3-4 は、デジタル署名の有効性を維持するために必要な情報を追加する様子を示しています。この図に基づき、どのような情報を追加していくのかについて説明します。

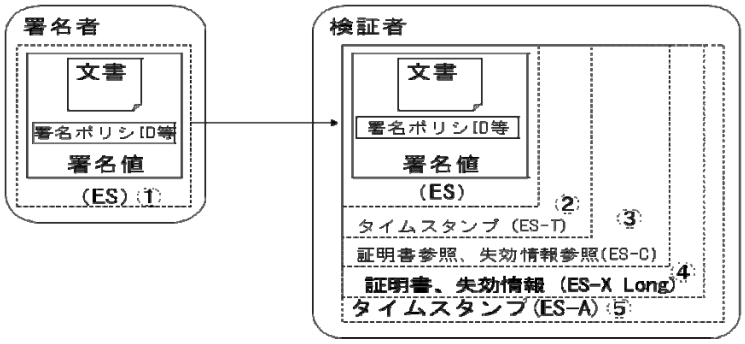


図 3-4 長期署名フォーマットの構造〔出典　文献 1〕

①ES（電子署名文書）

署名者は、デジタル署名を生成する時、以下の情報を含めたデジタル署名を生成することができます。これらの情報は署名フォーマット内の署名属性（署名の対象になる部分）に含まれるので改ざんを検知することができます。

・署名対象の文書

・署名ポリシーID

・署名者の証明書
・署名者の属性
・署名時刻
・署名値

②ES-T（ES に署名タイムスタンプを追加）

署名者もしくは検証者は、署名存在時刻を明確にするため、ES の署名値のハッシュ値をタイムスタンプ局に送付しタイムスタンプを取得します。そして、取得したタイムスタンプをデジタル署名に添付します。タイムスタンプは署名フォーマット内の非署名属性（署名値を計算する際に対象としない属性）に含まれます。

このタイムスタンプにより、デジタル署名の存在時刻を保証できます。従って、のタイムスタンプが示す時刻を基準として、デジタル署名の検証に必要となる情報を用いて再検証を実施することが可能となります。

③ES-C（ES-T に検証情報のリファレンスを追加）

検証者は、署名再検証に必要な情報を明確にするため、以下の情報をデジタル署名に追加します。これらの情報は署名フォーマット内の非署名属性に含めます。

・認証パス上の公開鍵証明書へのリファレンス
・公開鍵証明書の失効情報へのリファレンス

④ES-X Long（ES-C に検証情報を追加）

署名再検証に必要な情報を保存するため、以下の情報をデジタル署名に追加します。これらの情報は署名フォーマット内の非署名属性に含みます。

・認証パス上の公開鍵証明書
・公開鍵証明書の失効情報

⑤ES-A（電子署名文書の長期保存形式）

署名再検証に必要な情報を改ざん検出可能な状態にするため、デジタル署名とデジタル署名に追加した情報に対するタイムスタンプを取得し、これをデジタル署名に添付します。タイムスタンプは署名フォーマット内の非署名属性に含みます。

このタイムスタンプは、ES-C を生成したときに用いられたアルゴリズムや鍵が弱くなるか、漏洩した時や、前回取得したタイムスタンプが有効期限に到達する恐れがある場合に取得します。

これらの長期署名フォーマットによる長期保存方式は次の特長を持ちます。

(a) 第三者による検証が可能

長期署名フォーマットに従って構築された長期署名の有効性はシステムの安全性に依存するものではありません。つまり、文書保存システムの運用が正しく行われていたか否か、正しく動作していたか否かは長期署名の有効性に影響を与えることはありません。認証局及びタイムスタンプ局の信頼性を前提とし、構築された個々の長期署名データそのものを PKI で通常提供されている技術を利用して検証者が単独で検証を行うことができます。保存されているシステムとは関係なく、データ自体がある整合性を保ってさえいれば有効性を確認す

ることができるのです。つまり、長期署名データはポータビリティを持つといえます。

(b) 第三者が長期署名フォーマット構築を引き継ぐことが可能

延長処理（ES-T、ES-C、ES-X Long、ES-A などの構築）は、署名者、検証者、あるいは第三者の誰でもが実施することができます。更に、同一の組織やサーバが継続的に実施する必要は無く、他の組織やサーバが引き継ぐことができます。このことも上記で述べたポータビリティを持つことによるメリットであるといえます。

(c) 最新の署名技術によるカプセル化

タイムスタンプ局は常に最新の（その時点で安全性が確認されている）署名技術を用い、その技術で内側のデータを保護できる枠組みを与えるため、技術の陳腐化を懸念する必要がありません。特に、元の電子文書も常に新たなタイムスタンプの対象としているため、元のデジタル署名に係るアルゴリズムの脆弱化、私有鍵の漏洩、公開鍵証明書を発行した認証局の危殆化などが生じた場合でも、安全性は確保されます。

(d) TTP は認証局とタイムスタンプ局のみ

署名延長処理を実施する者やシステムの運用を信頼する必要はなく、また「電子公証局」のような新規の特別な TTP を仮定しなくてもかまいません。現状の PKI で存在するエンティティ、つまり TTP としての認証局やタイムスタンプ局のみで、長期署名に対する信頼の形成が可能です。

(e) 複数のタイムスタンプの重複による安全性強化

タイムスタンプを複数のタイムスタンプ局から同時期に取得することが可能です。異なる事業者、異なるアルゴリズムを利用したタイムスタンプを重複して利用することにより、予期せぬ失効や脆弱化が発生し、突然に有効性が失われたとしても、再検証時点に至るまでいずれかのアーカイブタイムスタンプが有効性を持続する期間に重なりを持てば、長期署名としての有効性は保持されます。

(2) 長期署名フォーマットの構築

長期署名フォーマットの構築は、署名者、検証者、それ以外の第三者の誰でも実施できます。ただし、タイムスタンプの取得や検証情報の取得タイミングには注意が必要です。

厳密な運用では、図 3-5 のように署名タイムスタンプを取得してから失効情報を得るまでに、猶予期間（失効要求があってから認証局による要求処理の期間と失効情報が発行される期間を加えた期間）を設けることを要求しています。

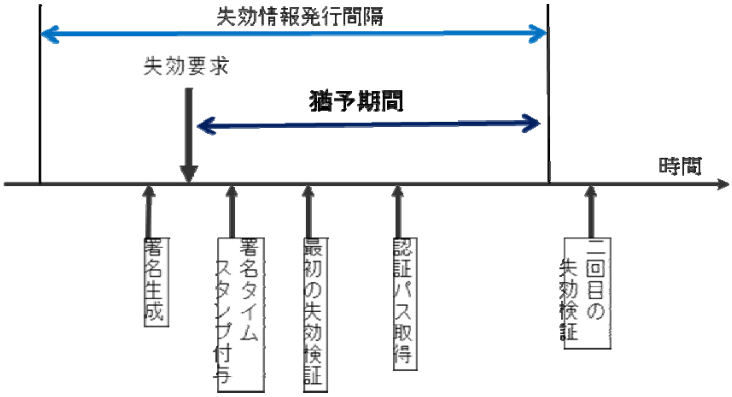


図 3-5 猶予期間〔出典　文献 1〕

猶予期間を設けないと、署名タイムスタンプ生成時における署名者公開鍵証明書の失効状態を正しく判断できないことがあるからです。つまり、失効直後に生成されたデジタル署名を、認証局が該当する公開鍵証明書の失効を反映する前の失効情報を参照してしまうことにより、誤って失効なしと判断してしまう可能性があるからです。

以下に、猶予期間を考慮して長期署名フォーマットを構築する手順を図 3-6 に従って説明します。

A)　デジタル署名生成
　-署名者がデジタル署名を生成（T0)。
B)　タイムスタンプ取得
　-署名者がデジタル署名を生成後あるいは検証者が電子署名文書入手後、デジタル署名が無効となる前（署名者の公開鍵証明書の有効期限切れや失効前かつデジタル署名に関連する暗号アルゴリズムの脆弱化前）に署名タイムスタンプを取得し、ES-T を生成（T1)。
C)　検証情報取得
　-T1 を基準とし、図 3-5 で示した猶予期間経過後に検証情報を取得し、ES-X Long を生成。
D)　初代アーカイブタイムスタンプ取得
　-署名タイムスタンプと検証情報が有効なうちにアーカイブタイムスタンプを取得し、ES-A を構築(T2)。署名タイムスタンプの検証情報を長期署名フォーマット内に格納する場合は、アーカイブタイムスタンプ取得前にそれらを収集して格納。
E)　次の世代のアーカイブタイムスタンプ取得
　-最初に取得した初代のアーカイブタイムスタンプが有効性を失う前(タイムスタンプトークンの公開鍵証明書の有効期限切れや失効前かつ関連する暗号アルゴリズム脆弱化前)に、次の世代のアーカイブタイムスタンプを取得 (T3)。初代アーカイブタイムスタンプの検証情報を長期署名フォーマット内に格納する場合、次の世代のアーカイブタイムスタンプ取得前に、それらを収集して格納。

最も新しいアーカイブタイムスタンプが有効性を失う前にE)と同様の処理を繰り返し、順次アーカイブタイムスタンプを取り続けることにより、論理的にはいつまでもデジタル署名の有効性を確認できることになります。

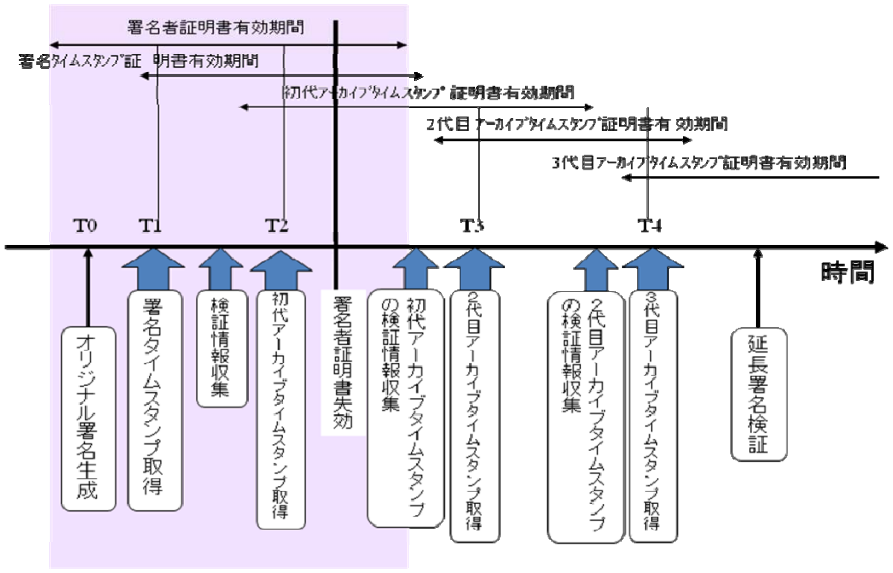


図 3-6 長期署名フォーマットの構築〔出典　文献1〕

(3) 長期署名フォーマットの検証

例えば数十年が経過し、元の電子署名文書に係わる公開鍵証明書の有効期限が切れてしまった後でも、正しく構築された長期署名フォーマットを検証することにより、署名タイムスタンプが示す時刻に電子署名文書が有効であったか否か（電子署名文書に添付されたデジタル署名が有効であったか否か）を確認することができます。長期署名フォーマットの検証は、構築の順にでも逆順にでも行うことができます。ここでは、逆順、つまり最新のアーカイブタイムスタンプから検証処理を進める場合について、図 3-7 に従って説明します。なお、図中の STS は署名タイムスタンプを、ATS はアーカイブタイムスタンプを表します。

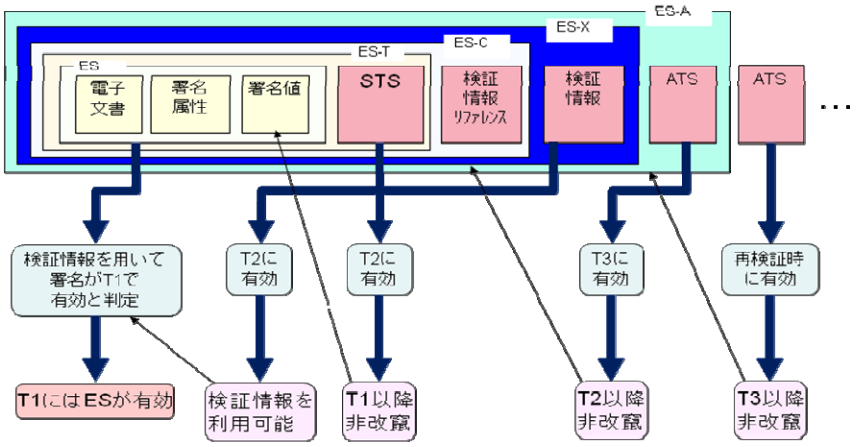


図 3-7 長期署名フォーマットの検証〔出典　文献1〕

A) 最新世代のアーカイブタイムスタンプの検証

-最新世代のアーカイブタイムスタンプのデジタル署名とハッシュ値を検証(タイムスタンプに付されたデジタル署名の検証、及び前世代の長期署名フォーマットの各要素を連結して得たハッシュ値との照合を実施し、改ざんされていないことを確認)。

注:この時点では最新のアーカイブタイムスタンプの公開鍵証明書は有効期間内にあり、認証パス上の証明書や失効情報は認証局のリポジトリから得ることができます。

B) 前世代のアーカイブタイムスタンプの検証

-前世代のアーカイブタイムスタンプのデジタル署名とハッシュ値を検証

-最新世代のアーカイブタイムスタンプの時刻 (T3) に遡って前世代のアーカイブタイムスタンプの公開鍵証明書を検証

注 : 前世代のアーカイブタイムスタンプは、最新のアーカイブタイムスタンプが添付された時刻 T3 には有効期間内にあり、かつ失効もしていなかったはずです。

C) 署名タイムスタンプの検証

-署名タイムスタンプのデジタル署名とハッシュ値を検証

-前世代の（ここでは説明上、最初の）アーカイブタイムスタンプの時刻（T2）に遡って、署名タイムスタンプの公開鍵証明書を検証。

注:署名タイムスタンプは、最初のアーカイブタイムスタンプが添付された時刻 T2 には有効期間内にあり、かつ失効もしていなかったはずです。

D) オリジナル署名の検証

-デジタル署名を検証

-署名タイムスタンプの時刻（T1）に遡って署名者の公開鍵証明書を検証

A)～D)の検証に成功した場合、元の署名の有効性が保たれていることが確認できます。なお、長期署名フォーマットに格納され保存された信頼点となる認証局の公開鍵証明書が、当時の公開鍵証明書であることを確認する必要があります。このためには、認証局は過去に利用した公開鍵証明書を長期にわたり保存しておくことが要求されます。

4. タイムスタンプ

(1) タイムスタンプの位置付けと効果

タイムスタンプは、電子データがタイムスタンプ生成時刻以前に確かに存在した事を証明（存在時刻証明）すると共に、その当時の状態を保持していることを証明（非改ざん性証明）することができます。電子署名文書（デジタル署名の付与された電子文書）の長期保存にとってタイムスタンプは必要不可欠な技術です。2004 年 11 月 5 日に総務省より「タイムビジネスに係る指針（ネットワークの安心な利用と電子データの安全な長期保存のために)」[総務省]が公表されました。この指針を踏まえて、2005 年 2 月に、(財) 日本データ通信協会は、同協会が定める基準を満たした技術・システム・運用体制によって、業務が厳正に実施されている

ことを認定する「タイムビジネス信頼・安心認定制度」の運用を開始しました。既に数社の事業者によりこの制度の認定を受けたタイムスタンプサービスが提供されています。

タイムスタンプは、その適用場面によりさまざまな効果を発揮します。

・文書等のデータへの適用

技術メモ、仕様書、図面、契約書、ログ、音声、マルチメディアなどのあらゆるデータの存在時刻と非改ざん性を証明するためにタイムスタンプを用いることができます。文書等のデータに対してタイムスタンプを取得し、そのデータとタイムスタンプを関連付けて保管しておき、必要なときに検証を行います。タイムスタンプの検証により、それらのデータがタイムスタンプの示す時刻以前に存在し、それ以降、内容に変更がないことを確認できます。

・デジタル署名への適用

デジタル署名の存在時刻を証明するためにタイムスタンプを用いることができます。電子文書等のデータではなく、電子文書等のデータから生成した署名データに対してタイムスタンプを取得します。署名者が署名生成時に署名生成直後にタイムスタンプを取得する場合、署名検証者が署名検証時にタイムスタンプを取得する場合などが考えられます。いずれの場合も署名生成時刻からタイムスタンプ取得時刻までの間が短い（有効期限切れや失効が発生する以前）ことが望まれます。取得したタイムスタンプは署名データ内に格納するなど、両者を関連付けて保管します。タイムスタンプの検証により、有効期限切れが発生した場合、デジタル署名が有効期限切れ以前に存在したことを確認でき、失効が発生した場合、失効情報が得られる限り、デジタル署名が失効以前に存在したことを確認できます。つまり、デジタル署名へのタイムスタンプの適用により、その存在時刻と非改ざん性を証明することだけでなく、デジタル署名の有効性判断の手がかりを与えることになります。

・電子署名文書の長期保存への適用

電子署名文書のデジタル署名を長期間再検証可能な状態で保存するためにタイムスタンプを用いることができます。この場合、署名データ及び検証用の各種データに対してタイムスタンプを取得し、それらを関連付けて保管します。署名データ及び検証用の各種データに加えてタイムスタンプを検証することにより、元のデジタル署名と関連付けられた公開鍵証明書の有効期限切れや失効の後であっても、当初デジタル署名が存在していた時点で、そのデジタル署名が有効であったことを確認できます。

(2) タイムスタンプのしくみと代表的な方式

タイムスタンプには、いくつか方式がありますが、実際に国内でサービスが提供されているものは、デジタル署名を用いた RFC3161 方式と、デジタル署名を用いないリンキング方式の 2 通りのみです。

A) タイムスタンプのしくみ

タイムスタンプしくみを図 3-8 にそって説明します。

a) 要求者が証明したい電子文書のハッシュ値を生成する。

b) それをタイムスタンプ局（TSA）に送る。
c) タイムスタンプ局（TSA）は時刻配信局（TA）からの時刻を定期的あるいは随時に受けて正確な時刻を保持している。
d) その時刻を含み、受け取ったハッシュ値との何らかの安全な関連付け（すり替えや偽造ができないような関連付け）を実施する。
e) その結果（データ）を要求者に返信する。

なお、タイムスタンプを検証する場合は、タイムスタンプが改ざんされていないことを確認し、電子文書のハッシュ値とタイムスタンプ内のハッシュ値とを比較します。

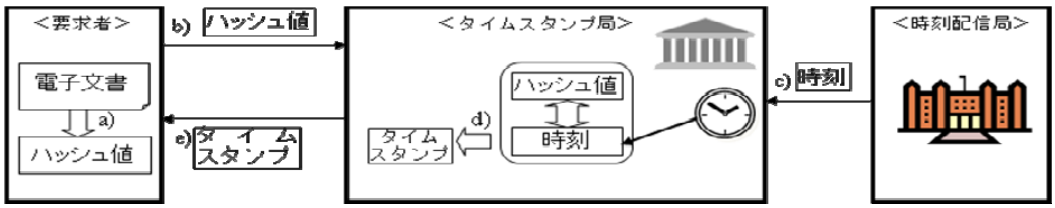


図 3-8 タイムスタンプのしくみ〔出典　文献 1〕

B)　RFC3161 方式のタイムスタンプ

この方式のタイムスタンプは、ハッシュ値や時刻情報にデジタル署名が付与されます。

①タイムスタンプ要求

RFC3161 で定めているタイムスタンプ要求は図 3-9 の構造をもち、TSA にハッシュ値を提供します。ノンスは、リプレーアタックを防ぐための乱数で、オプションですが指定することが推奨されています。また、証明書要求はタイムスタンプトークン内にタイムスタンプ署名検証用の公開鍵証明書を含めることを要求するためのもので、オプションでデフォルト“偽（含めない)”ですが“真（含める)”とすることが推奨されています。

版番号	
メッセージインプリント	ハッシュアルゴリズム
	ハッシュ値
要求ポリシー（op）	
ノンス（op）	
証明書要求（op）	
拡張（op）	

図 3-9 タイムスタンプ要求の構造

②タイムスタンプ応答

タイムスタンプ応答は図 3-10 に示すようにステータスとタイムスタンプトークン（TST）からなります。

ステータス
タイムスタンプトークン（TST）

図 3-10 タイムスタンプ応答の構造

タイムスタンプトークン（TST）は、図 3-11 のデータ構造（TSTInfo）に TSA の署名を付けたものです。文書に対する署名と同じ様に、CMS フォーマットのカプセル化されたコンテント情報に TSTInfo が入ります。

版番号
TSA ポリシー
メッセージインプリント
シリアル番号（TSA にユニーク）
時刻（UTC タイム）
時刻精度
オーダリング
ノンス（タイムスタンプ要求と同値）
TSA の名前
拡張

図 3-11 TSTInfo の構造

C) リンキング方式のタイムスタンプ

リンキング方式のタイムスタンプには対象となっている電子文書のハッシュ値、時刻情報に加え、タイムスタンプの正当性の検証を委託するための必要情報（タイムスタンプの ID 情報など）が含まれています。この方式の特徴として、全てのタイムスタンプはこれまで生成されたタイムスタンプに依存するようにリンクされて生成され、その過程で発生したリンク情報（ハッシュ値）を定期的に新聞等に公表することがあげられます。こうすることによって、リンク情報が公表された時点において、それまでに生成されたタイムスタンプの存在が保証されるため、システムの信頼性が確保されます（図 3-12）。

ただし、実際のサービスでは、エンドユーザが自分でその正当性を検証すること、つまり公開されたリンク情報と取得したタイムスタンプの関連性の確認はできず、検証はタイムスタンプ局に頼る必要があります。

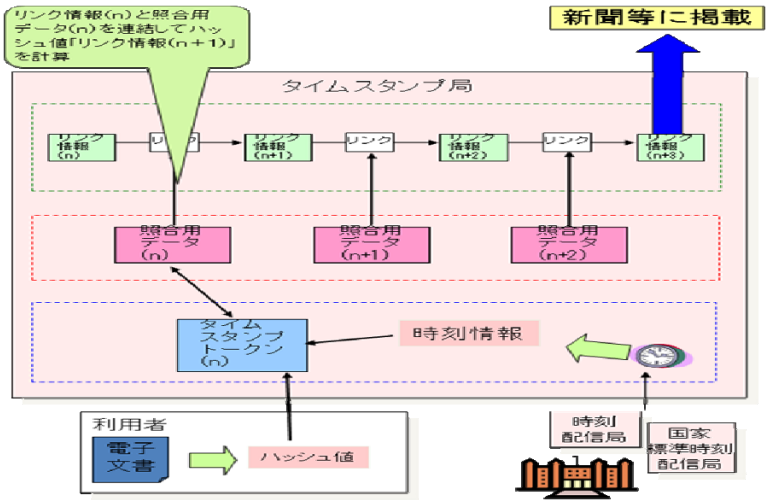


図 3-12 リンキング方式のタイムスタンプ〔出典　文献 1〕

(3) タイムスタンプポリシー

タイムスタンプトークン内には、TSA のサービスや運用に関する方針と規定がタイムスタンプポリシーとして表示されます（実際にはその OID が表示されます)。以下にその留意点を述べます。

A) 時刻及びその精度

標準時に対してトレーサブルな必要があります。

B) オーダリング（順序)

オーダリングが“真”の場合は、すべてのトークンが精度に関係無く時刻（genTime）の順序で発行されることを意味します。タイムスタンプ局がオーダリングを維持するのは通常難しく多くのタイムスタンプ局はオーダリングフラグを“偽”としています。

C) タイムスタンプ署名鍵のバックアップ

タイムスタンプ局の運用ではタイムスタンプトークンの署名鍵をバックアップする必要はありませんし、すべきでもありません。もしタイムスタンプトークンの署名鍵が漏洩したり危殆化したのではなく事故によって利用できなくなったのであれば、タイムスタンプ局は今までの公開鍵証明書を失効させず、新しい署名鍵を生成し以後新しいタイムスタンプ局の公開鍵証明書を用いれば良いからです。以前のタイムスタンプトークンは、以前の有効であった公開鍵証明書で検証できます。

D) タイムスタンプ署名鍵の安全性

タイムスタンプは公証機能を持っているので、タイムスタンプ局の公開鍵証明書の有効期間が短くてはその効用が限られます。RSA 換算で最低 1024 ビットの鍵長は必要です。長期署名フォーマットではもしアーカイブ目的のタイムスタンプに用いるのであれば更に強度の高い 2048 ビットの CA と同程度の強度を持つ鍵長を用い 10 年以上の有効期間を持つことが望まれます。

E) タイムスタンプ局の公開鍵証明書の発行周期

タイムスタンプ局の公開鍵証明書がその有効期間が残り少なくなった時点で発行された

タイムスタンプを用いた場合、タイムスタンプ自身の有効期間が短くなり、その可用性が損なわれます。従ってタイムスタンプ局は公開鍵証明書の有効期間の半分を経過した時点で次の公開鍵証明書を要求し以後タイムスタンプはこの新しい証明書をもちいて行うことが望まれます。このようにすれば最も有効性が短いタイムスタンプでも公開鍵証明書の有効期間の半分は保証されることになります。

現在提供されているタイムスタンプサービスには、10 年の有効期間を持つ公開鍵証明書及びそれに伴う鍵ペアを毎年更新するものがあります。こうすると、発行されるタイムスタンプトークンは常に 9 年以上の有効期間を持つこととなります。

F) タイムスタンプトークンとタイムスタンプ対象データとのリンク

タイムスタンプ要求者は取得したタイムスタンプトークンとタイムスタンプ要求時に用いたデータのハッシュ値との関連を明確にして保存しておかなければなりません。これは事後の検証を曖昧にしないために不可欠なことです。デジタル署名の長期保存に関しては、標準化された長期署名フォーマットを使うことができます。したがって、標準の長期署名フォーマットを使えばタイムスタンプ対象のデータとこれに対するタイムスタンプトークンとの対応付けを常に明確に保ったまま維持することができます。

〔参考文献〕

〔1〕木村道弘、前田陽二、宮崎一哉　著「電子文書保存のしくみと実務」中央経済社、2008 年 6 月

付録１　用語集

1. CA　→　認証局
2. CP　→　証明書ポリシー
3. CPS　→　認証局運用規定
4. CRL　→　失効リスト
5. OCSP（Online Certificate Status Protocol）
   認証局に対して証明書が有効であるか否かをオンラインで問い合わせるための通信手順。
6. PKI　→　公開鍵基盤
7. RA　→　登録局
8. TST　→タイムスタンプトークン
9. 鍵ペア（Key Pair）
   公開鍵暗号システムにおいて対となる公開鍵と秘密鍵。2 つの鍵は、公開鍵が与えられても、秘密鍵を導き出す事が計算上不可能な特性を持つ。
10. 危殆化（Compromise）
    秘密鍵が盗難、漏洩、解読によって機密性を失ったか、あるいはその可能性があること。
11. 共通鍵（Secret Key）
    暗号化と復号に同一の鍵を用いる共通鍵暗号方式における鍵。
12. 検証鍵（public key）
    公開鍵暗号システムにおける署名検証用の公開鍵。
13. 検証者（verifier）
    署名検証を行う人。
14. 公開鍵（Public Key）
    公開鍵暗号システムにおける鍵ペアのうち公開する方の鍵。
15. 公開鍵暗号システム（Public Key Cryptosystem）
    異なる 2 つの鍵（公開鍵と秘密鍵）を用いる暗号方式で、一方の鍵で暗号化したデータは他方の鍵でのみ復号できるようになっているシステム。
16. 公開鍵基盤（Public Key Infrastructure）
    公開鍵暗号システムを用いたサービスのための一連の技術や約束事。
17. 証明書（Certificate）
    認証対象者の識別情報と公開鍵とが対応していることを証明する文書で、認証局の署名を付与したもの。厳密には公開鍵証明書であるが、曖昧さがない限り単に証明書という。
18. 証明書の一時失効（Certificate Suspension）
    証明書の有効期間中に一時的に証明書を失効させる行為。
19. 証明書の失効（Certificate Revocation）
    証明書の有効期間内に、秘密鍵が危殆化したり氏名等の重要な属性情報に変更が生じて証明書を無効にする行為。

20. 証明書ポリシー（CP, Certificate Policy）
認証局が発行する証明書の記載事項や本人確認方法等を明記した文書。
21. 署名鍵（private key）
公開鍵暗号システムにおいて署名に用いる秘密鍵。
22. 署名検証（verification）
署名付き電子文書を、署名者証明書に含まれる署名者の公開鍵を用いて復号することにより、当該電子署名の正当性を検証する行為。
23. 署名者（signer）
署名生成を行う人。
24. 署名生成（signature generation）
電子文書を、署名者の秘密鍵を用いて暗号化し、所定のフォーマットに格納すること。
25. 失効リスト（CRL, Certificate Revocation List）
失効した証明書のリスト。通常認証局による署名が付される。
27. 信頼点（trust anchor）
利用者が信頼する認証局。通常は、ルート認証局であることが多い。検証者が署名者証明書の正当性を確認する際の拠り所となる。
28. タイムスタンピング機関（TSA, time-stamping authority）
あるデータが、ある時点より前に存在していた証拠を提供することを信託された、信頼できる第三者機関。
29. タイムスタンプ（time stamp）
作成または更新されたファイルにメタデータとして記録されているファイルの更新日時に関する情報。
30. タイムスタンプ局　→　タイムスタンピング機関
31. タイムスタンプトークン（time stamp token）
電子データのハッシュ値に時刻情報を連結し、署名を付与した時刻証明情報。
32. 長期署名（Long Term Signature）
署名時刻の特定を可能とし、かつ、署名対象及び検証情報を含む署名に関する情報の改ざん検知を可能とする措置を実施し、署名を長期にわたって検証可能にした署名。
33. デジタル署名（Digital Signature）
公開鍵暗号方式を応用して、秘密鍵（署名鍵）を所持している者だけが正しく署名でき、かつその文書が改ざんされていないことを証明できる署名方式.
34. 電子署名（Electronic Signature）
間違い無く本人である事を証明する電子的なデータ。デジタル署名と同義で使われる事が多いが、広義ではアナログ署名を電子データにしたものも含む。
35. 登録局（RA, Registration Authority）
証明書の発行や失効のプロセスにおいて、本人確認などの一部機能を認証局の承認を受けて行う機関。登録局は、証明書や失効リストの生成は行わない。
36. 認証（Certification）

個人、法人、装置等を対象として、証明書を生成するプロセス。

37. 認証局（CA, Certification Authority）
証明書の発行、開示、失効もしくは一時失効等のサービスを行う信頼された機関。

38. 認証局運用規定（CPS, Certification Practice Statement）
電子認証局による電子証明書の発行、失効、電子認証局の業務の運用管理の手続、電子認証局を運営する機関や利用者の責任と義務等について定めた文書。

39. 認証パス（certificate path）
署名者証明書から信頼点（トラストアンカー）の証明書までの証明書の連鎖。

40. ハッシュ関数（hash function）
電子文書に電子署名を施す際などに、その電子文書をある一定の大きさまで圧縮するための計算手順。ハッシュ関数の計算結果である圧縮データをハッシュ値、あるいはメッセージダイジェストと呼ぶ。

41. 否認防止（non-repudiation）
取引などを行った後に、当該取引に関与したことそのものを否定する不正行為（事後否認）を防止すること。

42. 秘密鍵（Private Key）
公開鍵暗号システムにおける鍵ペアのうちの一つで、他人には知られないように秘密にしておく鍵。

43. リポジトリ（Repository）
証明書やCRL等を保管しておき利用者からの要求に応じてそれら情報を提供する仕組み。

44. 猶予期間（grace period）
失効要求があってから失効情報が発行されるまでの期間。

付録 2　電子署名の理解に役に立つ Web サイト

(1) 電子署名・電子認証ホームページ

http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html

このページでは、電子署名や電子認証について、意義・必要性や関連制度を紹介しています。

○　電子署名・認証の必要性
○　電子署名及び認証業務に関する法律（電子署名法）
○　電子署名・認証の活用動向
○　電子署名を行う上での注意事項

(2) 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）

http://law.e-gov.go.jp/htmldata/H13/H13F11003006002.html

(3) 公的個人認証サービス ポータルサイト

http://www.jpki.go.jp/

(4) 電子政府の総合窓口

http://www.e-gov.go.jp/index.html

発行日　2009年11月

発行　財団法人日本情報処理開発協会

〒105-0011　東京都港区芝公園3丁目5番8号

機械振興会館内

Tel　03-3432-6597

Fax　03-3432-6201

この資料は、経済産業省委託事業「平成 21 年度電子署名・認証業務利用促進事業」の一環として作成しました。

平成 21 年 11 月発行