行政機関の電子化文書取扱ガイドライン（案）における電子認証・電子公証サービスの扱いに関する解説

（社）日本画像情報マネジメント協会
法務委員会

はじめに

電子化文書取扱ガイドライン（案）の中で、特に重要なことは電子化文書がその作成段階から廃棄に至る全プロセスの中で、正しく運用管理されて一切改ざんされていないことを、誰もが納得できる姿で証明できるということである。このことは、裏返せば、万が一改ざんがあった場合でも改ざんされていることを証明できるということである。

このような観点から、電子化文書取扱ガイドライン（案）では、電子化文書を作成する際に電子署名を行なうこと、及び保存する際に電子公証サービスを利用してタイムスタンプを取得することを推奨している。

５．システム管理者の責務

システム管理者は以下の責務を負う。

（中略）

5) 行政文書情報管理システムへの電子化文書の登録に際して、実務責任者と共に「電子署名」を行って、電子化文書が正しく作成されたことを明確にすること。

（以下省略）

７．実務責任者の責務

実務責任者は以下の責務を負う。

（中略）

3) 作成した電子化文書にシステム管理者と共に電子署名し、電子化文書が正しく作成されたことを明確にすること。

（以下省略）

８．システムの機能要件

行政文書情報管理システムは、次の機能を備えるものとする。

1）真正性の確保のための機能

① 作成した電子化文書にシステム管理者及び実務責任者が電子署名し、改ざん等の事実の有無が検証できる機能

② 電子署名された電子化文書の登録及びその更新に際し、その日時並びに実施者をこれらの情報に関連づけて記録する機能。

③ 重要度が高い電子化文書、長期にわたって保存する電子化文書については、信頼できる外部機関から提供される電子化文書証明サービス（電子公証サービス）を利用し、当該電子化文書の作成時期の証明及び改ざんなどの事実の有無を検証できる機能

（以下省略）

本解説書では、電子署名及び電子公証サービスの概要について説明を行い、行政文書の電子化保存においてこれらサービスがどのような役割を果たし、どのように利用されるべきかについて述べる。

1. 電子署名の概要

電子署名とは、簡単に言えば「紙文書における署名・印鑑と同等の役割を、電子記録に対して行うもの」である。文書に署名や押印がある場合と同様に、文書が電子的なものとして作成された場合は、電子署名が施されていれば真正に成立したものと見なされる。これは法律上認められていることであり、電子署名及び認証業務に関する法律（平成 13 年 4 月 1 日施行）でその取り扱いが定められている。この法律では、実際にどのような技術が電子署名に相当するのかということは、あえて定義していない。これは将来の技術革新を考慮した上でのことだが、本解説では現時点で最も有力な方式である公開鍵暗号方式を用いた電子署名について、その概要を記す。

単純な暗号アルゴリズム（暗号・復号処理における手順）では、データの暗号化と複合化において同じ鍵が使用される。鍵とはアルゴリズムで使用する変数のようなものであり、これが異なると生成される暗号文が異なる。これに対して、公開鍵暗号方式では暗号化と復号化に別々の鍵を用いる。それぞれの鍵を A、B とすると、

・A で暗号化したデータは B で復号できる
・B で暗号化したデータは A で復号できる

という特徴をこの方式は持っている。このうち鍵 A を利用者本人しか使えないよう厳

密に管理し、反対に鍵 B は本人以外にも公開する（この場合 A を秘密鍵、B を公開鍵と呼ぶ）。

公開鍵暗号方式を用いた電子署名は、電子文書（または電子化文書）からハッシュ値と呼ばれる値を生成し、そのハッシュ値を秘密鍵で暗号化することにより行われる。ハッシュ値とは、任意長のデータをある関数に入力し、その結果として出力される短い固定長のデータのことである。ハッシュ値は以下のような特徴を持つ。

・異なるデータから同じハッシュ値が生成される可能性がほとんどない（データが 1bit でも変われば、そこから生成されるハッシュ値も変わる）。この性質を利用して、データ改ざんの有無を検証できる。

・不可逆性、一方向性を持つ（ハッシュ値から元のデータを再現することができない）。

これらの技術を利用して、公開鍵暗号方式では次の手順で電子署名の作成と検証を行う。

【電子文書送信者 X による電子署名の作成】

1） 電子文書からハッシュ値を作成する。

2） ハッシュ値を X の秘密鍵で暗号化する（暗号化されたハッシュ値＝電子署名）。

3） 電子文書と電子署名を Y に送信する。

【電子文書受信者 Y による電子署名の検証】

1） X の公開鍵を用いて受信した電子署名を復号する。

2） 受信した電子文書からハッシュ値を作成する。

3） 1)で復号した値と 2)で作成した値が等しければ、電子文書は改ざんされておらず、かつそれが X によって作成されたものであることが分かる。

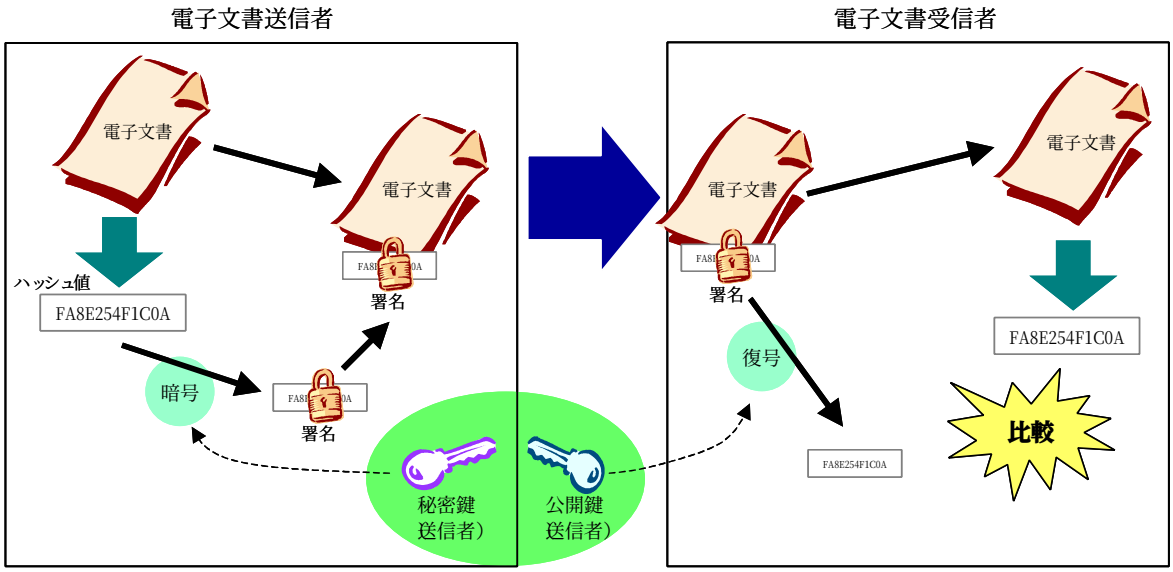

図 1．電子署名の作成と検証

2. 電子公証サービスの概要

電子公証とは、電子認証とならんで電子申請・企業間取引・電子文書長期保存等を支える基盤であり、一般的には「第三者（TTP: Trusted Third Party）による、電子的記録の原本性を保証するサービス」として捉えられている。電子公証という言葉が持つ意味にはいくつかの解釈が存在しているが、その共通部分のみを抽出すると以下のような要件が残る。

・電子的記録の真正性を保証し、証拠能力を担保するための一要素
・真正性の保証は、当事者ではなく第三者によって行われる。

この２つを満たすものが、広義の電子公証である。

電子公証のシステム構成は、第三者である電子公証センタと、それを利用するユーザから通常成り立っている。

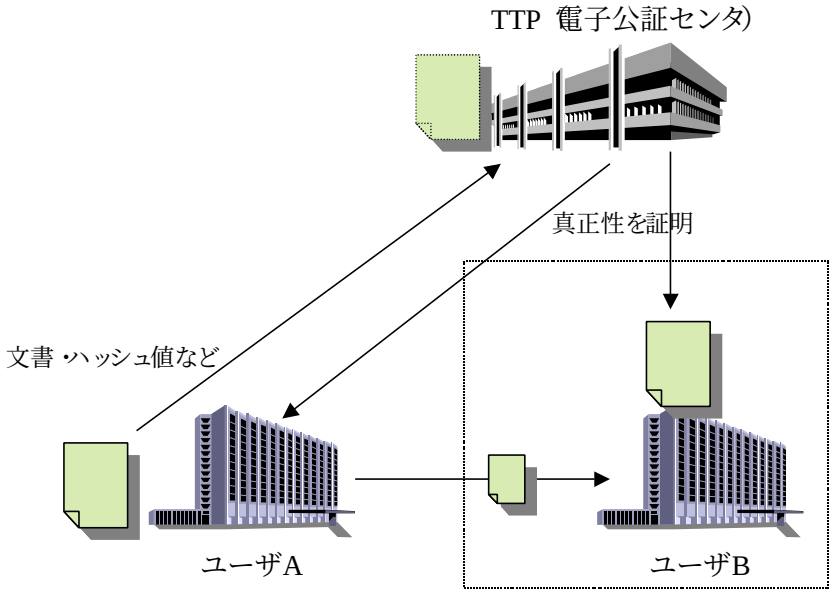

図 2. 電子公証サービスの基本構成

ユーザの手元にある電子的記録は、TTP によってその真正性が保証される。真正性を保証する方式はいくつかあるが、代表的な方式として

1） ユーザが TTP に電子的記録を預け、TTP でその記録を厳密に保管・管理する。
2） 電子的記録をユーザの手元に留めておき、TTP には真正性の保証に必要となるデータ（ハッシュ値など）のみを送信する。

という 2 種類が挙げられる。

3. 行政文書の電子化保存における電子署名・電子公証の役割

行政文書の電子化保存において、電子署名および電子公証サービスはそれぞれ以下のような役割を果たす。

1)　電子署名

電子化文書に実務責任者の電子署名を添付して保存することにより、その電子化文書が確かに有資格者（「文書情報管理士」の資格を有する者）によって作成されたものであることを、証明することができる。従って、元の紙文書から電子化文書が作成される際には有資格者により適切な手順に則った作業が行なわれており、電子化の過程で不適切な処理や意図的な文書改ざんなどは行なわれていないと推定できる。

また、実務責任者の電子署名を使用して、電子化文書が改ざんされていないかどうかを検証することができる。これにより電子化文書の真正性を確保することができるが、その期間は一般に比較的短い（3 年程度）。

2)　電子公証サービス

電子化文書に電子公証サービスから取得したタイムスタンプ等を添付して保存することにより、行政文書情報管理システムに保存されている電子化文書がいつ作成されたものであるか、客観的に証明することができる。また、電子公証サービスには「電子的記録が作成されて以降、改ざんが行なわれたかどうか」を検証する機能が通常備わっており、これにより電子化文書の真正性を確保することができる。その期間は、電子署名により実現される保証期間と比較した場合、一般に長期である。

以上のことを踏まえて、電子署名及び電子公証サービスは次のような形で利用されることが望ましい。

・電子化文書が作成以降改ざんされた、もしくは電子化の途中で改ざんされた場合の影響が大きいと判断される場合、実務責任者の電子署名が電子化文書に添付されるべきである。

・改ざんの影響が大きく、かつ対象となる電子化文書の保存期間が長期に渡る場合は、電子公証サービスを利用して電子化文書の真正性を保つことが望ましい。

以上