

電子署名について

第 1 電子署名の仕組み等

- 1 電子署名とは、電磁的記録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、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り、かつ、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をいう（電子署名及び認証業務に関する法律（電子署名法）第 2 条第 1 項）。
- 2 上記の電子署名の定義は、電子署名の機能に着眼した技術中立的なものとなっているが、現在の実務においては、公開鍵暗号方式と呼ばれる技術方式が用いられている。

公開鍵暗号方式とは、暗号化と復号とで異なる 2 つの鍵（秘密鍵と公開鍵）を使用する方式である。秘密鍵はその所有者が秘密に管理しなければならない鍵（プライベート鍵）であり、公開鍵は公開可能で、他の人に利用してもらい鍵である。片方の鍵で暗号化したものは、対になるもう一方の鍵でなければ復号できない。電子文書に電子署名を行う場合には、電子署名の対象となる電子文書について「ハッシュ関数」により「ハッシュ値」を算出し、そのハッシュ値を電子文書の所有者だけが持つ秘密鍵で暗号化することとなる。このハッシュ値を秘密鍵で暗号化した結果が、電子文書に対する電子署名となる。

なお、一对の秘密鍵及び公開鍵は、それに対応する電子証明書とともに発行されており、電子署名を検証する者は、認証局に対して電子証明書の有効性確認を行った上で、電子文書自体のハッシュ値と、公開鍵を用いて復号された電子署名のハッシュ値を比較することにより、電子文書が改ざんされていないことなどを確認することができる。

第 2 電子署名の種類

電子署名サービスには、ローカル型（本人が IC カード等に格納された本人から近接した環境にある秘密鍵を使用して署名するもの）、立会人型（本人の指示に基づき電子署名事業者がその秘密鍵を使用して署名するもの）、リモート型（本人の秘密鍵が電子署名事業者の管理するクラウド上など本人から遠隔した環境にあり、この秘密鍵を使用して署名するもの）などがある。

公的個人認証サービスによる電子証明書（JPKI、マイナンバー電子証明書）は、マイナンバーカード上のICチップに秘密鍵、公開鍵及び電子証明書を格納するローカル型のものに当たる。

第3 電磁的記録の真正な成立の推定（電子署名法第3条）

電磁的記録に記録された情報の内容を証拠として用いるためには、その成立の真正（当該内容が、挙証者の主張する特定人の意思に基づいて作成されたものであること。）を証明しなければならない。

電子署名法第3条は、民訴法第228条第4項と同趣旨の規定として、電磁的記録に記録された情報について一定の要件を満たす電子署名がされているときに、当該電磁的記録の成立の真正を推定することを規定している。同条の「これを行うために必要な符号」とは例えば秘密鍵が、「物件」とは例えばICカードがこれに該当する。

なお、電子署名法第3条は、公務員が職務上作成した電磁的記録を適用対象から除外している（民訴法第228条第3項参照）。

（参照条文）

○ 電子署名及び認証業務に関する法律（平成12年法律第102号）

（定義）

第2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。

2・3 （略）

第2章 電磁的記録の真正な成立の推定

第3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。