電子署名とは何か

弁護士　福間則博

（質問）最近よく耳にする「電子署名」とはどのようなものですか。

（回答）

電子署名とは、一言で言うと、電子情報に施される措置で、文書における署名あるいは記名押印と同じような役割を果たすためのものと言うことができます。

紙の文書の場合、署名あるいは記名押印により、本人が作成し又は本人が内容を変更したものであることを明らかにすることができます。署名においては、その筆跡によって本人が書いたか否かが判定することができますし、記名押印においても、本人の印鑑は他人に使わせる事は滅多にないと言う事情を背景として、その印が使われたときには本人が押したものと推定することができるからです。このように紙の文書においては、署名あるいは記名押印を施すことによってその文書が本人によって作成されまた本人の意思によって内容が変更されたものであることが明らかになります。

これに対し、パソコンによって作成される電子情報については、なりすましや改変・変造が容易であることから、これらを阻止するための方策が必要となり、その方策が「電子署名」に他なりません。

電子署名の法律上の定義は、電子情報に加えられた措置で、①本人によって作成されたことを示すもので、②改変されたか否かを確認することができるものです(電子署名及び認証業務に関する法律第 2 条)。この①②の要件から、電子署名は、紙の文書における署名あるいは記名押印の役割を果たそうとするものであることがお分かりいただけると思います。

では、その「措置」の内容はどのようなものであるかですが、これについては法律上特に制限はありませんが(技術的中立性)、実際利用されている措置は、公開鍵暗号方式によるものです。

公開鍵暗号方式においては、まず、対象となる電子情報について、その内容を簡略化(ダイジェスト化)するためにハッシュ関数を用いてハッシュ値を求めます。このハッシュ値は、対象となる電子情報がほんの僅かでも異なると全く違ったハッシュ値となることから、改変の有無を確認する手段となります。

次に、本人の保有している秘密鍵を使って、ハッシュ値を暗号化します。この暗号化された数値は、秘密鍵とペアになった公開鍵によってしか解読（復号）することができません。

このような公開鍵と暗号化された数値、そして、その公開鍵が本人のものであることを明らかにする証明書並びに通常の文章の形をとった電子情報(平文)を相手方に送付します。

相手方においては、公開鍵を用いて暗号化された数値を復号し、解読されたハッシュ値を確認します。そして送られてきた平文ついても自らハッシュ関数を用いてハッシュ値を求めます。そして 2 つのハッシュ値を比較して、一致すれば、それは本人によって作成された電子情報で、改変が行われていないことが明らかになります。なぜなら、公開鍵で復号できたということは、その暗号化された情報は秘密鍵によって作成されたものであり、秘密鍵は本人しか持ち得ないものだからであり、また、ハッシュ値が同一であるということは改変されていないことを示すものだからです。このようにして電子情報の作成の本人性と改変の有無を確認することができます。これが電子署名にほかなりません。