参考５

電子証明書と印鑑登録証明書との類似点・相違点

デジタル署名のＰＫＩは、日本の印鑑登録制度と非常によく似ているが、両者は、まったく別の制度である。印鑑登録は、慣習に基礎を置く制度で、日本では非常に重い役割を果たしており、不動産取引をはじめ、非常に重要な取引において利用されるが、一般の消費者取引や日常的に繰り返される企業間契約においては、いちいち実印と印鑑登録証明書は使わない。しかし、デジタル署名は、極めて危険なインターネットでの取引に、紙ベースの取引に匹敵するセキュリティを実現するための技術であって、その意味では、消費者取引を含めて、日常的に用いられることに意義がある。なお、両者の類似点・相違点は以下のとおりである。

◎　類似点

○　電子証明書

① 本人のみが発行申請をすることができる電子証明書に添付されている公開鍵によって、本人のみが有する秘密鍵によってなされたデジタル署名を検証することにより、成りすましを防止

② デジタル文書（平文）に秘密鍵でデジタル署名したもの（改ざん不能）を添付することにより、送信途上での文書の改ざんを防止

○　印鑑登録証明書

①　市町村に対し印鑑の登録または証明の申請をすることができる者を本人に限定していることから、本人が有する実印と印鑑登録証明書を所持する者は本人であるとする人格の同一性を確認（成りすましを防止）

②　実印の押捺された文書（改ざんしにくい）に印鑑登録証明書を添付することによって、その文書が真正に成立していることを担保

◎　相違点

１．存在形態

電子証明書は電磁的記録、印鑑登録証明書は紙の状態で存在する。実印の印影は複雑ではあるが、秘密ではない。一方、デジタル署名に用いる秘密鍵は、絶対に秘密でなければならない。印影の偽造により成りすましは可能である。しかし、一般に印鑑登録証明書が通用しているところをみると、実際に取引が行われることが、他の様々な不正への抑制要因となっているものと考えられる。一方、電磁的記録のコピーは自在にできるため、秘密鍵の数値は絶対に秘密にしたうえで、その秘密鍵に対応する公開鍵であることを第三者が常に証明できる仕組みが必要となる。

２．証明書の有効性の確認

○　電子証明書

・インターネット上だけでなく、実社会に申請者がいることを証明するための証明書として、当該証明書の行使の時点での有効性の確認が必要

・有効期限が存在し、更に、鍵ペアが格納されたＩＣカード等の紛失等により有効期限前に失効されることもあることから、受信者がその証明書の有効性を随時確認することが不可欠

○　印鑑登録証明書

・ 当該証明書を行使する必要がある場合ごとに交付を申請

・ 有効期限が定められていないこともあり、証明書を受領した側が、その証明書の真正性や有効性を確認することは稀

３．技術的側面

○　電子証明書

当該証明書の行使の時点での有効性確認に対応することができるよう、常に up to date な失効情報を管理することが必要

○　印鑑登録証明書

市町村長が、申請者の申請に応じて当該証明書を交付することができるよう、印鑑登録原票を当該市町村役場において保管すれば足りる。