전자서명법상의 인증제도에 관한 연구

2000.

연구책임자 : 유진식(초청연구원)

한국법제연구원

目 次

제 1 장 처음에

1. 컴퓨터네트워크의 리스크와 전자서명・인증

인터넷과 같은 이른바 사이버공간을 이용한 거래는 점점 증가하고 있으나 거기에는 해결해야 될 몇 가지 문제점이 있다. 첫째로는 인터넷상에서의 거래의 안전성의 문제이다. 사이버공간에서의 거래는 보통 상대방을 직접 상대하지 않기 때문에 상대방을 확인할 수 없는 경우가 많다. 그리고 거래의 내용에 대해서도 마찬가지이다. 그 내용은 컴퓨터라는 장치를 통해서 전자적인 형태로 전달되기 때문에 거기에는 서면에서 볼 수 있는 육필(肉筆)과 같은 개성이 없어서 그 전자메시지가 누구로부터 발신된 것인가 하는 것을 확인하는 일이란 쉽지 않다. 그 뿐만 아니라 전자메시지는 도중에 그 내용을 변경하여도 흔적이 남지 않기 때문에 그 내용의 동일성여부를 확인하기도 쉬운 일은 아니다.[1)]

거기서 위와 같은 어려움을 해결하기 위해서 전자메시지를 암호화하여 상대방에게 발신하는 방법을 생각할 수 있다. 즉, 거래의 당사자만이 해독할 수 있는 암호를 이용하여 전자메시지를 암호화하여 상대방에게 발신을 하는 방법이다. 그러나 이것으로 문제가 완전히 해결되는 것은 아니다. 첫째로 암호화하는 기술을 거래의 당사자 개개인이 소유하는 데에는 너무나 많은 비용이 소요된다는 점이다. 즉, 수준이 낮은 암호기술은 누구나 쉽게 이용할 수 있겠지만 이러한 기술은 그 만큼 쉽게 외부로부터 침해당하고 부인(否認)될 수 있기 때문이다. 따라서 외부로부터의 침해를 차단할 수 있는 비교적 안전한 암호기술을 이용하기 위해서는 많은 비용이 소요된다고 할 것이다. 이 때에 이러한 비용을 과연 거래당사자 개개인이 부담할 수 있는 능력이 있으며 또한 그렇게 거래를 했을 경우 생산성이 있는가 하는 문제이다.

그러나, 나아가, 설령 높은 기술을 이용한 암호기술을 구사할 수 있다고 하여도 문제는 여전히 남는다. 즉, 고도로 암호화한 전자메시지를 거래당

1) 內田 貴, 電子商取引と民法, 別冊 NBL NO. 51 “債權法改正の課題と展望”, 商事法務研究會, 285-286쪽.

사자간에 교환을 한다고 하여도 과연 전자메시지 속의 명의인이 실제로 존재하는 인물인지 또는 실재로 존재한다고 하여도 당해 전자메시지의 발신인이 명의인 본인인지 하는 등의 문제가 또 남아있는 것이다.

여기서 또 다시 이러한 문제점을 해결하기 위해서 또 한번의 연구가 필요하며 그 결과 생각할 수 있는 방법이 제3자를 개입시키는 것이다. 즉, 이 제3자는 전자메시지를 외부에서 쉽게 침해할 수 없는 고도의 기술을 이용하여 암호화 할 수 있는 능력을 지니고 있으며, 미리 전자메시지의 명의인이 누구인가를 파악하여 거래의 상대방에게 그 정보를 전달함으로써 전자메시지의 안고 있는 위험성을 어느 정도 줄일 수 있는 것이다. 이 때의 제3자가 제공한 기술을 이용하여 발신자가 전자메시지를 암호화하는 것을 이른바 '전자서명'이라고 하고, 이 제3자가 당해 전자서명과 관련된 정보를 확인하는 작업을 '전자인증'이라고 한다. 그리고 이 때에 이러한 역할을 하는 제3자를 '인증기관'이라고 한다.

2. 전자서명・인증과 법

이어서 문제가 되는 것은 위와 같은 전자서명・인증에 대하여 법적으로 어떻게 취급하며 그 때에 고려해야 할 사항은 무엇인가 하는 점이다. 이러한 문제는, 말할 것도 없이, 전자거래의 방식이 기존의 거래방식 즉, 서면과 서명・날인과 같은 방식과 다르다는 점에서 발생한다. 즉, 이것은, 바꾸어 말하면, 기존의 서면과 서명・날인 등이 수행했던 기능을 전자거래에서의 전자서명・인증 등이 대신 수행할 수 있는가 하는 점이다.

그런데 이러한 문제는 법해석학적인 방법에 의한 해결에는 한계가 있으며 어느 정도의 입법조치가 필요하다. 세계각국의 이른바 전자서명법, 디지털서명법 등의 법률은 바로 이러한 목적에서 제정되고 있는 것이다. 이 때에 어떠한 사항을 고려해야 하는가가 문제인데, 앞서 잠깐 언급하였지만, 지금까지의 입법례를 참고 하여보면, 대략 다음과 같은 점을 말할 수 있다.

첫째로 기존의 서면이나 서명・날인과 전자메시지, 전자서명 등과의 유형적인 차이에서 오는 점이다. 즉, 서면이나 서명・날인은 이미 확정된 상태로 존재하지만, 전자메시지나, 전자서명 등은 컴퓨터라는 장치 속에 존

재하고 있기 때문에 아직 유형적으로 확정되어 있지 않기 때문이다. 다시 말하면 이 양자의 유형적인 차이를 어떠한 연결고리를 이용하여 극복할 것인가 하는 점이다. 이 때의 입법론으로서는 두 가지 방법을 생각해 볼 수 있다. 먼저, 전자메시지, 전자서명 등을 서면이나 서명・날인과는 다르다는 점을 인정하여 새로운 제도를 창설하는 방법이다. 미국의 일부의 입법에서 볼 수 있는 예이다. 그리고 또 하나의 방법은 전자메시지, 전자서명 등을 서면이나 서명・날인과 유사 또는 동일하게 취급을 하는 방법이다. 이 방법은 이른바 「기능적 등가물(funtional equivalent) 어프로우치」라고 하는 것으로 기존의 서명・날인과 같은 아날로그방식이 수행해 왔던 것과 기능적으로 같은 역할을 수행할 수 있는 경우에는 전자메시지나 전자서명 등에 대해서도 같은 취급을 하는 방법이다.[2] 이 방법은 국제적으로도 폭넓게 지지를 얻어 유엔모델법을 비롯한 대부분의 나라의 전자서명법 내지 디지털서명법은 이 방법을 채택하고 있다.

둘째로 들 수 있는 것은 전자서명에 있어서 '기술'의 문제이다. 즉 어떠한 서명기술을 이용하여 메시지를 전자정보화하는 가의 문제이다. 이 점은 앞서 언급한 전자거래에 있어서의 전자메시지나 전자서명 등의 안전성에 대한 문제와 이들에게 어떠한 법적 효과를 부여할 것인가의 문제가 동시에 관련되어 있다. 왜냐 하면, 전자서명기술에는 다양한 종류가 있으며, 어떠한 기술을 이용하는가에 따라서 이에 대하여 부여하는 법적인 효과도 달라지기 때문이다. 다시 말하면 전자서명 등에 대해서 일정한 법적인 효과를 부여하기 위해서는 일정한 수준 이상의 기술이 전제가 되어야 하기 때문이다. 그리고 기술의 내용에 따라 규제의 정도가 달라지기도 한다.

마지막으로 전자서명에 대하여 어떠한 법적 효과를 부여할 것인가의 문제이다. 기존의 방식인 서면이나 서명・날인에 대해서는 거래와 관련하여 실체법 및 증거법상에서 일정한 법적 효과를 부여하고 있다. 예를 들면, 계약의 성립의 요건으로 의사표시뿐만 아니라 서면에 의할 것을 요구하고 있는 경우(영미법)라든가 증거법상에서 서명・날인이 있는 경우에 이른바 형식적 증거능력을 인정하는 경우(한국 민사소송법 제328조, 제329조) 등이 그

2) 內田 貴, 상게논문, 273쪽.

것이다. 이처럼 기존의 서면이나 서명・날인에 부여했던 법적인 효과 중에서 전자서명에 어떠한 효과를 인정하며, 또 나아가 그 효과의 정도를 동등하게 할 것인지 그렇지 않으면 그 이상으로 할 것인지 등이 문제가 된다. 이 경우에도 전자서명에 대해서 어떠한 법적 효과를 어느 정도까지 인정할 것인가 하는 점은 전자서명・인증제도의 규제의 내용과 직접적인 관련을 가진다.

결국 기본적인 고찰의 주요대상은 ①기존의 서면이나 서명・날인과 전자메시지, 전자서명 등과의 유형적인 차이를 어떻게 극복할 것인가 하는 점, ②전자서명에 있어서 기술의 의미, 그리고 ③전자서명에 대하여 어떠한 법적 효과를 부여할 것인가 이다. 그리고 이러한 사항에 대하여 어떠한 내용의 규정을 두느냐에 따라서 전자서명과・인증의 체계와 규제의 내용은 달라지게 된다. 이 세 가지의 요소는 전자서명・인증제도의 논의의 핵심을 이루는 사항으로 서로 유기적인 연관성을 가지며, 따라서 전자서명을 전제로한 인증제도의 구성의 기본이 된다. 즉, 이들 세 요소는 인증제도에 유기적으로 확산되어야 한다.

3. 연구의 목적과 범위

이상에서 살펴본 바와 같이 컴퓨터 네트워크를 이용한 거래에는 일정한 위험이 따르며 그러한 위험을 극복하기 위하여 고안된 것이 전자서명・인증제도라는 사실을 알았다. 그리고 이 전자서명・인증제도를 기능하도록 하기 위해서는 일정한 입법조치가 필요하며, 그 것은 위에서 언급한 세 가지요소로 수렴된다.

그런데 위와 같은 세 가지 요소를 고려하여 입법을 할 경우 한 가지 더 염두에 두어야 할 사항이 있다. 그것은 각국이 어떠한 법제를 취하고 있느냐에 따라서 위의 세 가지 요소에 대한 입법적인 대응이 달라진다는 점이다. 예를 들면 영미에서는 서명(署名)을 계약의 성립요건으로 하고 있지만 우리 나라에서는 이른바 낙성주의를 취하고 있기 때문에 반드시 그러한 형식을 요하지 않고 있다. 또 증거법상에서도 영미에서는 이른바 법정증거주의를 채택하여 이른바 최량증거법칙에 의해서 원본(原本)만을 증거로 하고

있지만 우리 나라의 경우에는 자유심증주의에 의해서 반드시 원본이 아니라고 하더라도 법관의 결정에 따라서 증거로 삼을 수 있다. 다만, 후술하는 경우처럼 법률이 서면이나 서명·날인을 요구하는 등의 경우에 제한적으로 연결고리를 마련하기 위한 입법이 의미를 갖는다고 할 수 있다.

그런데 현재 유엔모델법을 비롯하여 각국의 입법에 영향을 주고 있는 전자서명·인증에 관한 입법은 영미의 주도로 행해지고 있기 때문에 그 내용 역시 영미의 법제에 맞추어져 있다. 그럼에도 불구하고 현재의 우리 나라의 전자서명에 관한 내용은 위와 같은 점을 고려하지 않고 그대로 받아들여 입법을 하고 있는 실정이다.

그리고 또 한가지 전자서명·인증제도에 대한 규제도 결국은 위에서 언급한 요소 즉, 안전한 전자서명을 확보하는 데에 중점을 두고 행해져야 한다. 그러나 우리 나라의 법제는 반드시 이러한 균형을 이루고 있다고 할 수 없다. 특히 전자서명·인증제도와 관련한 규제에 있어서 전자서명 그 자체에 대한 실질적인 규제보다도 공인인증기관에 대한 외형적인 규제에 치중하고 있고 과징금과 같은 규제수단의 경우 그 내용이 변질된 형태로 운영되는 등 규제의 정도와 방법 그리고 그 수단에 있어서 검토되어야 할 사항이 많다. 그리고 상위인증기관에 해당하는 한국정보보호센터의 경우, 법규가 아닌 인증업무준칙을 근거로 하여 권한행사를 하고 있는 것도 법적으로 큰 문제라고 할 수 있다.

이상에서 살펴본 것처럼 전자서명·인증에 관한 법제는 민법과 증거법, 즉 민사소송법, 그리고 행정법에 관한 내용이 서로 유기적으로 관련되어 있음을 알 수 있다. 본고의 목적은 행정법적인 관점에서 전자서명·인증제도에 대한 규제의 내용을 분석하는 것이 목적이다. 그러나 앞서 살펴본 대로 규제의 내용 역시 전자서명을 어떠한 내용으로 구성하고 또 어떠한 법적 효과를 부여할 것인가에 따라서 규제의 내용도 달라지기 때문에 규제의 출발점이 되는 전자메시지의 법적인 취급, 전자서명에 있어서 기술의 의미 등에 대해서 살펴보고 이것을 기초로 하여 전자서명법상의 규제의 내용을 분석하기로 한다. 논의의 순서로서는 전자서명·인증제도의 분석을 위한 예비적 고찰로서 전자서명·인증의 구조 등을 먼저 살펴보고, 이어서 현행법인 전자서명법의 내용을 중심으로 고찰하고자 한다.

제 2 장 분석을 위한 예비적 고찰

제 1 절 전자서명・인증의 구조와 법

1. 아날로그와 디지털의 연결고리

앞서 언급한대로 사이버공간의 거래에서 먼저 문제가 되는 것은 기존의 서면이나 서명・날인과 전자메시지, 전자서명 등과의 유형적인 차이를 어떻게 극복할 것인가 하는 점이다. 바꾸어 말하면, 종이의 환경에서 전자적 환경으로 이행하는 데 필요한 연결고리를 마련하는 작업이다. 이 때에 연결고리로서 고려되는 요소는 서면, 서명・날인, 원본(原本) 등인데, 이들이 수행해 왔던 기능과 같은 기능을 수행할 수 있는 전자적 기술을 법률상에서 어떻게 표현할 것인가가 문제가 된다. 이 점은 실체법과 증거법에서 어떠한 법제를 취하고 있느냐에 따라서 전자적 기술의 법률상의 표현은 달라지게 된다. 즉, 영미법계에서는 계약법상에서 서명을 계약의 성립요건으로 하고, 또 증거법상 어떠한 사실을 재판에서 증거로 인정함에 있어서 법률로 정한 것에만 한정하는 법정증거주의를 채택하고 있는 경우와, 이와는 달리, 민법에서 계약의 성립요건으로 서명・날인을 요구하지 않는 이른바 낙성주의를 취하고, 민사소송법에서도 법관이 위와 같은 증거법칙의 제약을 받지 않고 변론의 전취지와 증거자료를 참작하여 형성된 자유로운 심증으로 행하는 자유심증주의[3]를 채택하고 있는가에 따라 마련해야 할 연결고리가 달라진다는 점이다. 전자 즉, 영미법계의 경우, 전자메시지 내지 전자서명은 종래의 서면, 서명・날인과 이질적이기 때문에 전자메시지, 전자서명에 의한 거래가 성립하고 재판상의 증거로서 채택되기 위해서는 양자를 연결시키기 위한 입법조치가 반드시 필요하다. 그 반면 후자의 경우에는 계약의 성립은 서명・날인을 요하지 않기 때문에 전자메시지로 충분히 가능하며, 증거법칙에 있어서도 자유심증주의를 취하고 있기 때문에 재판상의 증거로도 채택될 수 있다. 그러나 이 경우에도 국제적인 정합성과

3) 이시윤, 신정보판 민사소송법, 박영사(1996), 559-560쪽.

거래와 재판상의 효율, 그리고 법률에서 문서나 서명·날인을 요구하고 있는 경우[4]에는 연결고리를 위한 입법이 필요하다고 할 것이다.

그러면 이하에서 법제에 따라 연결고리에 대한 실정법상의 규정방식이 구체적으로 어떻게 달라질 수 있는가 살펴보기로 하자.

1) 서명주의와 법정증거주의의 경우[5]

이 점과 관련하여 먼저 이른바 최량증거준칙(best evidence rule)이 문제가 된다. 최량증거준칙이란 등본 등의 이차적 증거가 아니라 원본문서를 제출할 것을 요구하는 영미증거법상의 준칙이다. 이 준칙을 엄격하게 적용하면, 예를 들면, 서면으로 작성한 계약서를 디지털화해서 컴퓨터에 보존한 경우, 원래의 서면이 원본인 이상은 컴퓨터 데이터를 증거로 작성할 수 없게 된다. 혹은 처음부터 전자메시지의 형태로 거래의 데이터가 작성된 경우, 설령 전자메시지 자체를 원본으로 본다고 하여도 법정에 제출된 프린트물이나 법정에 설치된 단말기의 디스플레이에 표시된 화면은 컴퓨터에 보존되고 있는 데이터 그 자체가 아니라 그것을 인간이 읽을 수 있는 형태로 번역한 것이라고 할 수 있다. 그렇다면 과연 이것을 가지고 원본제출의 요건을 충족시켰다고 할 수 있는가가 문제이다.

영국에서는 1968년의 Civil Evidence Act, Section 5에서 컴퓨터문서의 복제에 대해서도 원본과 일치한다고 믿을 수 있는 한 증거로서 인정할 수 있다고 규정하여 약간의 처방을 하고 있지만, 데이터 메시지 그 자체의 증거능력을 일반적으로 인정하기 위한 규정은 존재하지 않는다.

미국의 경우에는 영국의 예와는 달리, 전자메시지는 많은 경우 최량증거준칙에 대한 예외를 인정한다고 하는 형식으로 전문증거배제원칙에 대한 예외인 업무기록의 준칙에 의해서 증거로서 인정되고 있다. 또한 최량증거준칙자체에 대해서도 FRE(연방증거규칙)은 많은 예외를 인정하고 있고(FRE 1003-1006), 나아가 컴퓨터기록을 서면이나 원본으로 인정하는 길을 열어 놓고 있다(FRE 1001(1), (3)).

---

4) 행정사무에서는 아직도 문서나 서명·날인을 요구하는 것이 보통이다.

5) 이 부분은 内田 貴, 電子商取引と法(4. 完), NBL. No. 603(1996. 10. 15)을 주로 참고하여 작성.

반면에 유엔모델법은 위와 같은 최량증거준칙에 대응하기 위한 규정을 마련해 놓고 있다. 즉 동모델법은 제8조(1)(a)(b)와 제9조(1)(b)에서 다음과 같이 규정하고 있다.

제 8 조 원본(原本)

(1) 정보가 원본의 형체로 제출되고 또는 보관될 것을 법으로 요구하고 있는 경우에, 그 요건은, 이하의 경우에, 데이터메시지에 의해서 충족된다.

(a) 데이터메시지로서인지 아닌지를 막론하고 정보가 처음으로 최종적인 형체로 작성된 때로부터 당해정보의 완전성에 관하여 신뢰할 수 있는 보증이 존재함과 동시에

(b) 정보의 제출이 요구되고 있는 경우에는 제출해야 할 자에 대하여 그 정보의 표시가 가능할 때

제 9 조 데이터메시지의 허용성 및 증거력

(1) 어떠한 법적 절차에 있어서도 이하의 경우에는 증거법칙을 적용함에 있어서 데이터 메시지를 증거로서 인정하는 것을 방해해서는 안 된다.

(b) 그것을 원용하는 자가 입수할 것을 합리적으로 기대할 수 있는 최량의 증거인 경우에, 그것이 원본의 형체가 아니라고 하는 것을 이유로 하는 경우

그런데 위와 같은 규정이 있다고 하여도 문제가 아직 남아 있는데 그것은 이 사문서가 전자메시지의 형태로 되어 있는 경우에 어떻게 하여 문서와 같은 증거력을 인정받을 수 있는가 하는 점이다. 먼저 생각할 수 있는 방법은 전자메시지를 프린트하여 그것을 원본문서 또는 등본으로서 제출하는 것이다. 그러나 이와 같은 방법은 일회적인 거래에서는 가능한 일이지만, 전자거래가 일반화하여 거래회수가 천문학적인 경우에는 이용하기 어려운 경우도 발생할 것이다. 이러한 경우에는 전자메시지 그 자체를 증거로서 제출할 필요성도 생기게 되는 것이다. 이러한 관점에서 전자메시지를 증거법상 어떻게 취급할 것인가에 관한 입법적인 처방이 필요한 것이다.

이 때에 입법론으로서, 앞서 잠깐 언급한대로, 두 가지 방법을 생각할 수 있다. 첫째로는 미국의 입법례에서 볼 수 있는 것처럼 전자메시지를 문서와는 다르다는 점을 인정하여 새로운 제도를 창설하는 것이다. 또 하나의 방법은 종래의 문서에 준해서 취급할 수 있도록 입법적인 방안을 강구하는 방법이다. 이른바 '기능적 등가물 접근방식'이 그것이다. 유엔모델법을 비롯하여 거의 대부분의 나라의 입법이 바로 이와 같은 입장을 취하고 있다. 유엔모델법 제6조는 전자메시지에 포함된 정보일지라도 후에 참고가 가능한 경우에는 문서로서의 조건을 충족시킨다고 규정하고 있다.

2) 낙성주의, 자유심증주의의 경우

그러나 위와 같은 규정은 계약의 성립요건에서 낙성주의를 취하고 증거법상 자유심증주의를 취하고 있는 나라와 미국처럼 입법상의 보완규정을 두고 있는 나라에서는 필요하지 않다. 오히려 전자메시지와 관련해서 문제가 되는 것은 사문서의 성립의 진정성(眞正性)의 여부 즉 이른바 형식적 증거력이 문제가 되는데 이것은 후술하는 전자서명에 어떠한 법적 효과를 부여할 것인가의 문제이다. 그러나 이 경우에도 다음과 같은 점에서 입법이 의미를 가질 수 있다고 생각할 수 있다. 첫째로 전자거래의 경우 국경의 의미가 약하기 때문에 외국과의 보조를 맞춘다는 측면에서 입법을 할 수도 있다는 점이다. 둘째로 전자메시지, 전자서명은 기존의 서면이나 서명·날인과 다르다는 것은 틀림없는 사실이기 때문에 거래와 재판의 효율이라는 측면에서 일정한 기준을 제시하고자 할 경우 입법을 고려할 수도 있다고 할 것이다. 그리고 마지막으로 민사상의 거래가 아니라 행정사무에서는 아직도 문서나 서명·날인을 통해서 의사표시를 하는 것이 보통이기 때문에 이 경우에도 의미가 있다고 할 것이다.

어쨌든, 실정법상에서 낙성주의, 자유심증주의를 취하고 있는 법제에서는 아날로그를 디지털에 연결하기 위한 입법조치는 제한적인 의미를 갖는다.

2. 전자서명에 있어서 기술의 의미

전자서명에 있어서 기술은 복합적인 의미를 가진다. 전자서명에 바탕한 전자인증제도는 전자거래에 있어서 교환되는 전자메시지의 '안전성'을 확보

하기 위하여 고안된 것이다. 이 때에 안전성의 핵심은 말할 것도 없이 기술이며, 전자서명에 어떠한 기술을 채용하느냐에 따라서 당해 서명에 대하여 부여하는 법적 효과와 그에 따른 규제의 내용이 달라진다. 즉, 안전성이 충분히 확보될 수 있는 높은 기술수준을 응용한 전자서명에 대해서는, 후술하는 바와 같이, 기존의 서면이나 서명・날인이 누렸던 것과 동등하거나 어느 경우에는 그 이상의 법적 효과를 부여할 수 있을 것이다. 그러나, 역으로, 만약 안전성이 보장되지 않는 낮은 기술수준의 전자서명에 대해서는 이러한 법적 효과를 부여할 수 없을 것이다. 그리고 전자서명・인증과 관련한 규제의 내용도 전자서명의 기술수준과 그에 대하여 부여된 법적 효과를 유지하고 보완하기 위한 관점에서 결정된다.

그러면 위와 같은 의미를 갖는 '기술'이 저자서명・인증에서 구체적으로 문제가 되는 것은 무엇인가? 그것은 입법으로 전자서명기술을 특정하느냐, 그렇지 않으면 기술중립적인 입장을 취하느냐의 문제이다.

여기에는 다음과 같은 의미가 있다. 기술을 특정하는 경우에는 전자서명・인증에 대하여 앞서 언급한 법적인 효과가 부여되기 때문에 재판상의 증거로 인정될 수 있다는 이른바 예견가능성이 확보된다. 즉, 거액의 거래를 하면서 분쟁이 발생할 경우, 그것이 법적으로 유효, 또는 증거로서 채용여부가 법원에 가지 않으면 알 수 없다고 해서는 아주 곤란한 일이며, 이렇게 될 경우 전자서명・인증제도의 많은 이용을 기대할 수 없을 것이다. 이처럼 예견가능성의 확보는 전자거래의 활성화를 위한 중요한 요소라고 할 수 있다. 그렇기 때문에 전자서명・인증제도에 대한 예견가능성을 확보하기 위해서는 어느 정도 기술을 특정할 수밖에 없는 것이다.[6)]

그러나 문제는 발전의 속도가 매우 빠른 IT산업의 속성에 있다. 이미 충분히 경험을 하고 있지만 IT산업이 개발・응용하는 기술의 발전의 속도는 놀랄만하다. 이러한 상황하에서 만일 기술을 특정할 경우, 거기에 맞추어서 만들어진 전자서명・인증에 관한 법제가 하루아침에 무용지물이 되는 경우도 상상할 수 있다. 여기에 전자서명・인증제도에 있어서의 기술문제를 둘러싼 고민이 있는 것이다.

---

6) 〔座談會〕電子取引法制整備の課題, ジュリスト No. 1183, 11-15WHr 참조.

이 점에 대해서 각국의 입법을 살펴보면 기술을 특정한 경우가 현재로서는 다수를 차지하고 있지만 기술중립적인 입장을 취하는 입법례도 늘고 있다. 입법에서 기술을 특정하는 경우 채택하는 기술은 현재 가장 높은 수준의 기술로서 평가되고 있는 이른바 디지털서명방식이다. 이하에서는, 먼저 디지털이란 어떠한 메카니즘의 서명기술인가를 간단히 살펴보기로 하자.

1) 디지털서명

전자인증에 가장 많이 이용되는 기술 중의 하나가 이른바 「디지털서명」이다. 이 디지털서명에 의해 적어도 서명·날인과 같은 정도의 인증면에서의 완전성(integrity)이 확보된다고 여겨지고 있다. 나아가 운용방법 여하에 따라서는 서명·날인보다 나은 완전성을 제공할 수도 있기 때문에 그 경우 그에 상응한 법적 효과를 부여할 수도 있다고 말해진다.[7]

디지털서명이란 정보(문장)를 특정한 지식을 이용하여 문장작성자의 동일성 또는 변경의 유무의 검사가 가능한 문장(인증문)으로 변환시키고(인증문의 생성), 이 인증문을 다시 문장으로 변환시키는 방법(검사·복원)을 말한다. 이 때에 인증문의 생성에 필요한 특정한 지식을 「인증문생성키」, 인증문의 검사 또는 복원을 위하여 필요한 지식을 「검사·복원키」라고 부르고 있다.[8][9]

현재 실용화되고 있는 암호방식으로서는 암호화키 또는 인증생성키와 복원키 또는 검사·복원키가 공통인 「공통키방식」과 암호화키 또는 인증생성키와 복원키 또는 검사·복원키가 다른 「공개키방식」이 있다. 후자의 경우 암호키와 복원키가 서로 다르기 때문에(비대칭), 양자를 합쳐서 「비대칭공개키방식」으로도 불리운다.[10]

「공통키방식」은 신속한 처리가 가능하다는 장점이 있지만 키를 공유하기 때문에 서명의 관점에서 보면 기능이 떨어진다고 할 수 있다. 반면에 「공개키방식」은 공통키 방식에 비하여 처리속도는 떨어지지만 이 방식에 의할

7) 內田 貴, 電子商取引と民法, 273쪽.
8) 電子取引法制に關する硏究會中間報告書, ジュリスト No.1114(1997. 6. 15), 145쪽.
9) 우리 나라 전자서명법에서는 전자를 전자서명생성키, 후자를 전자서명검증키라고 칭하고 있다(전자서명법 제2조 제3, 4호).
10) 內田 貴, 電子商取引と民法, 290쪽.

경우 상대방에 대하여 인증문생성키(비밀키)를 공개함이 없이 비밀키보유자가 아니면 작성할 수 없는 인증문을 작성할 수 있고, 또한 이렇게 작성된 인증문에 관하여 상대방은 누구에게나 공개되어 문제가 되지 않는 검사・복원키(공개키)로 검사・복원을 할 수 있다. 이처럼 문장에 대하여 작성자 이외에도 검사가 가능한 인증문을 첨부함으로써 작성자에게 고유한 서명과 같은 기능을 수행할 있기 때문에 전자서명에 적합한 방식으로 알려지고 있다.[11]

2) 외국의 입법례

먼저 유엔국제상거래법위원회의 유엔모델법의 예를 보기로 하자. 유엔모델법의 경우, '데이터 메시지'에 대하여 다음과 같이 규정하고 있다.

제 2 조 용어의 정의

(a) "데이터 메시지"란 전자문서교환(EDI), 전자우편, 전신(telegram), 텔렉스(telex) 또는 팩시밀리(telecopy)를 비롯한 전자적, 광학적(optical) 기타 유사한 수단으로 작성(generate), 발신, 수령 또는 저장된 정보를 말한다.

이처럼, 동모델법은 전자적으로 교환할 수 있는 모든 수단을 포괄적으로 규정하고 있을 뿐 전자서명에 특정한 기술을 이용할 것을 예정하고 있지 않다.

이에 대해서 유타주의 디지털서명법은 디지털서명은 '비대칭 암호체계(asymetric cryptosystem)를 사용한 메시지의 전송'(동법 제103조(10))이라고 규정하여 기술을 특정하고 있다.

한편 독일의 디지털서명법은 다음과 같이 규정하고 있는데, 표현은 다르지만 유타주처럼 기술을 특정하고 있다고 할 수 있다.

제 2 조 용어의 정의

(1) 이 법에서 "디지털서명"이라 함은 비밀서명키에 의하여 만들어진 전자문서상의 인장(印章)으로서 비밀서명키와 결합하여 인증기관 또는

11) 電子取引法制に關する研究會中間報告書, 145쪽.

제3조에 정하는 관청의 서명인증키와 함께 제공되는 공개키를 이용하여 서명키소유자의 진정여부와 전자문서의 변조여부를 확인할 수 있도록 하는 전자문서상의 인장을 말한다.

그런데 일본의 경우에는 중립적인 입장을 취하고 있다. 즉, 일본의 전자서명 및 인증업무에 관한 법률 제 2조는 다음과 같이 규정하고 있다.

제2조 이 법률에서 「전자서명」이란 전자적 기록(전자적 방식, 자기적 방식 그 밖의 사람의 지각으로는 인식할 수 없는 방식으로 만들어진 기록으로 전자계산기에 의한 정보처리용에 제공되는 것을 말한다. 이하 같음.)에 기록할 수 있는 정보에 관하여 행해지는 조치로 다음의 요건 모두에 해당하는 것을 말한다.

1. 당해 정보가 당해 조치를 행한 자가 작성한 것임을 나타내기 위한 것일 것.
2. 당해 정보에 관하여 개변(改變)이 행해졌는지의 여부를 확인할 수 있는 것일 것.

이처럼 일본의 경우 전자인증을 하기 위하여 전자적인 데이터에 가하는 일정한 정보처리의 결과를 총칭해서 「전자인증」이라고 하고 있다.[12] 일본법제의 특징은 다른 법제의 경우 공개키-암호방식을 이용하여 행하는 서명인 「디지털서명」이라고 명기하고 있는데 반하여 철저한 기술중립성을 견지하고 있다는 점이다.

3. 전자서명에 대한 법적 효과의 부여

1) 방식의 전환에 따른 고려의 요소

종래의 거래에서 서면과 서명·날인이 수행했던 기능을 전자문서에 의해서 행할 경우 실체법과 증거법상에서 고려해야 할 요소는 무엇인가? 이에 대한 논의를 하기 위해서는 먼저 서면과 서명·날인이 수행했던 기능이 무엇인지를 살펴보아야 할 것이다. 그런데 보통 이들 방식이 수행한 기능으로는 다음과 같은 9가지가 예시되고 있다.[13] 먼저 서면과 서명·날인 모두가 수

12) 전자거래법제에 관한 보고서, 15쪽.

13) 內田 貴, 電子商取引と民法, 278-285쪽, 참조.

행하는 기능으로는 ①의사전달기능, ②증거기능, 그리고 ③경고기능을 들 수 있다. 그리고 서면이 수행하는 기능에는 ④관리기능, ⑤완전성(integrity)유지기능, ⑥기록보존기능, 그리고 ⑦접근(access)용이(容易)화 기능이다. 마지막으로 서명・날인이 수행하는 기능으로는 ⑧귀속(atribution)기능과 ⑨명의인의 동일성확인(identification)기능을 들 수 있다.

여기서 다시 위의 9가지 기능 중 전자문서에서 고려해야 할 요소가 무엇인가가 문제가 된다. 이 점에 대해서는 앞서 언급한 아날로그방식의 디지털방식에의 연결의 문제와 컴퓨터 네트워크가 갖는 리스크의 속성이 고려된다. 그 결과 대체로 다음과 같은 세 가지 기능이 특히 문제가 되기 때문에 이들이 중점적으로 고려되어야 할 요소로서 지적되고 있다.[14]

첫째로 전자데이터의 귀속의 문제이다. 컴퓨터 네트워크라는 블랙박스를 통해서 거래를 할 경우 종이에 의해서 이루어지는 거래에서는 볼 수 없는 리스크를 동반하게 된다. 그 대표적인 것의 하나가 당해 전자메시지가 누구로부터 온 것인가가 확실하지 않다는 점이다. 그 결과 당해 전자메시지가 의사표시를 포함하고 있는 경우에 그 표의자가 정말로 메시지 속에서 주장하고 있는 인물인지 알 수가 없다. 그 인물이 실재하는 인물인지 설령 실재하고 있다고 하더라도 위조되었을 가능성이 얼마든지 있을 수 있다. 즉, 여기서 문제가 되는 것은 당해 전자메시지가 누구에게 귀속하는가 하는 점이다.

그런데 여기서 한가지 더 고려해야 할 점은 당해 전자메시지가 누구의 메시지의사에 의하여 작성되었는가를 확정하는 것도 귀속의 문제라는 점이다. 이것이 서면으로 거래가 이루어지는 경우 서명・날인이 수행하고 있는 귀속기능이며 민사소송법상의 형식적 증거능력의 문제이다. 이 때의 귀속의 대상이 되는 주체에는 최종적으로 효과가 귀속하는 본인 외에 권한 있는 대리인도 포함된다. 그리하여 전자메시지가 법률행위의 의사표시를 포함하는 경우, 여기서 귀속의 의미는, 전자메시지에 표시된 효과의사를 위의 작성명의인(본인과 대리인)이 가지고 있는 것이 되므로 처분증서에 관한 형식적 증거능력과 마찬가지로 귀속이 확정되면 법률행위의 사실이 증명되게 된다.

14) 內田, 상게논문, 285-289쪽.

둘째로 명의인의 동일성확인의 문제이다. 이것은 어느 전자메시지가 갑이라고 칭하는 인물의 의사에 의해서 작성되었다는 점이 증명이 된다고 하여도 그 인물이 실재의 갑 본인인지의 여부는 별도의 문제이다. 이 문제는 타인이 본인의 명의를 사용하여 법률행위를 하는 경우에 발생한다. 이것은 종래의 서면거래에서는 이른바 표현대리의 문제로서 등장한다. 이 점에 대한 종래의 주된 대응방식은 실인(實印)의 인감등록증명서를 첨부하는 것이었다. 전자거래에서 타인이 본인임을 주장하여 의사표시를 포함한 전자메시지를 송신하는 경우 기관방식의 대리와 똑같은 문제가 발생한다. 현행법상 표현대리가 성립하기 위해서는 권한부여의 표시나 기본대리권 혹은 과거의 대리권의 부여와 같은 사실이 필요하지만 오픈된 네트워크상에서, 특히 일회적인 거래에서 이러한 요건을 입증하기란 쉬운 일이 아닐 것이다. 이렇게 되면 상대방은 예상하지 못했던 손해를 입게 되기 때문에 어떻게 하면 상대방을 이 위험으로부터 보호할 것인가가 문제가 된다.

셋째로 전자메시지의 완전성의 문제이다. 전자거래에서 주고받는 데이터는 0과 1의 디지털신호이기 때문에 변경되어도 흔적이 남지 않는다. 따라서 전자데이터가 어느 기준시점 이후 변경되지 않았다는 점, 또한 인간의 개재(介在)의 유무와 관계없이 변화하지 않았다는 점, 즉 전자메시지의 완전성을 어떻게 확인할 것인가가 문제가 된다.

2) 법적 효과의 내용

위에서 살펴본 전자서명이 효과적으로 기능할 수 있도록 하기 위해서는 인증기관의 신뢰성을 확보함과 함께 전자서명에 대하여 법적으로 일정한 효과를 부여할 필요성이 있다. 이 때에 전자서명에 어떠한 법적 효과를 부여 할 것인가가 문제이다. 그러나 이 점에 대해서는 앞서 살펴본 귀속기능, 명의인의 동일성확인기능, 그리고 완전성유지기능의 세 가지가 중심이 된다.

(1) 귀속효과

이것은 앞서 살펴본 바와 같이 전자서명에 대하여 서명이나 날인의 경우와 같은 정도로 전자정보의 내용을 승인하고 그 내용에 구속될 의사가 전

자서명자에게 있다고 할 수 있는가 하는 문제이다. 만약 이것을 긍정한다면 전자서명에 이른바 『형식적 증거력』을 부여할 수도 있다. 그런데 여기서 문제가 되는 것은 귀속기능이란 단순한 기술적 확실성의 문제가 아니라, 서명이나 날인을 하는 경우의 명의인의 의식의 문제이다. 즉, 컴퓨터의 엔터・키를 한번 눌렀다고 해서 반드시 서명이나 날인을 하는 경우의 피구속의사・내용승인의사를 가지고 있었다고 할 수 없기 때문이다. 왜냐하면 귀속기능은 일정한 경고기능의 존재를 전제로 하고 있기 때문이다. 따라서 전자서명에 서명이나 날인에서 볼 수 있는 경고기능을 부여할 경우 귀속기능을 부여할 수 있을 것이다. 이를 위해서는 전자서명에 경고기능을 부여하기 위한 기술적인 방법[15]과 경우에 따라서는 법적인 조치가 필요할 것이다.

그리고 귀속기능과 관련하여 고려해야 할 사항은 이른바 표현대리의 문제이다. 이것은 전자서명의 법적 효과에 있어서 가장 문제가 되는 부분이다. 이 경우 본인의 귀책사유가 없는 경우에 표현대리를 인정하여 효과귀속을 인정하는 것은 무리이며, 본인의 귀책의 요소가 있다고 하여도 표현대리 이상의 보호를 부여할 필요성은 발견할 수 없다고 할 것이다. 만약 이러한 법적 효과를 부여하기 위해서는 그에 상응한 입법조치를 취해야만 할 것이다.

⑵ 명의인의 동일성확인 효과

명의인의 동일성확인에 관해서는 인증기관이 비밀키보유자의 본인확인을 확실하게 실시하면 그 기능은 달성된다. 그 확실성은 경우에 따라서는 손으로 한 서명이나 날인보다 앞설 것이다. 문제는 인증기관이 얼마나 확실한 확인절차를 밟고 있으며, 또한 그것을 어떻게 보증할 것인가의 문제이다. 이 점도 인증기관의 규제와 밀접한 관계가 있다.

---

15) 이와 관련하여 소개되고 있는 것이 PenOp이다. 이것은 패드위에 손으로 서명을 하여, 그 형체, 스피-드, 필압(筆壓) 등의 데이터를 디지털화해서 전자데이터(문서)와 일체화함과 동시에 손으로 한 서명을 디스플레이에 재현시키는 것이다. 內田, 상게논문, 293쪽.

⑶ 완전성유지효과

전자메시지의 완전성에 관하여 말하자면, 디지털서명의 경우 서명이나 날인 이상의 확실성을 확인할 수 있다. 만일 디지털서명된 전자메시지가 변경되면 공개키에 의한 복원이 불가능하게 되고 혹은 복원된 해쉬치(値)와 원래의 전자메시지의 해쉬치가 일치하지 않기 때문이다. 이러한 의미에서는 서면이나 서명 이상의 완전성유지기능이 있기 때문에 이에 대한 법적인 효과를 인정해도 좋을 것이다.

4. 안전한 전자서명의 요건

이상에서 전자서명에 의한 인증의 경우에 현단계에서 가장 기술성이 뛰어나다고 하는 디지털서명일지라도 인증기능에 있어서 완전하다고는 할 수 없다는 점을 알았다. 따라서 전자서명에 서명이나 날인과 동등한 또는 그 이상의 인증에 관한 법적 효과를 인정하기 위해서는 그에 상응한 수준의 전자서명에 한정할 필요가 있다고 할 것이다. 이 때에 안전성의 수준이 높고, 법적으로 강한 효과가 인정되는 전자서명을 「안전한 전자서명(secure electronic signature)」라고 부르기도 한다.[16] 바꾸어 말하면, 안전한 전자서명이 행해지는 경우에는 위에서 살펴보았던 법적 효과가 부여되게 된다. 그렇다면 과연 어떠한 전자서명이 안전한 전자서명인가가 문제가 된다. 이 점과 관련하여 안전한 전자서명과 관련하여 가장 주목을 받고 있는 미국 일리노이주의 The Electronic Commerce Security Act를 참고로 살펴보기로 하자.

동법은 「안전한 전자기록(a secure electronic record)」과 「안전한 전자서명(a secure electronic signature)」에 대해서 두 가지 법적 효과를 인정하고 있다. 첫째로 추정효이다. 안전한 전자기록에 대해서는 일정한 시점 이후 변경되지 않았다는 점이 추정되며(동법 Section 10-120(a)), 안전한 전자서명에 대해서는 명의인의 서명임이 추정된다(동법 Section 10-120(b)). 둘째로 안전한 전자서명에 대해서는 한가지 더 일정한 요건

16) 內田, 상게논문, 294쪽.

하에서 명의인에의 귀속효과를 인정하고 있다. 즉 이른바 표현대리와 관련된 문제이다. 그 요건으로는, ①명의인의 관리하에 있는 소스(source)로부터 서명을 창출하는데 필요한 서명장치나 다른 정보를 입수한 자의 행위에 의해서 전자서명이 이루어졌을 것(동법 Section 10-130(a)(1)), ②위와 같은 무권한의 액세스(access)나 사용이 명의인의 적절한 주의의무의 해태라는 상황 속에서 있었을 것(동법 Section 10-130(a)(2)), ③신뢰당사자(the relying party)가 전자기록의 외관를 합리적이고 선의(善意)로 신뢰하였을 것(동법 Section 10-130(a)(3))이다. 즉, 명의인과 전혀 관계없는 상태에서 위조된 전자서명은 포함되지 않지만, 대리권의 부여의 외관이나 기본대리권과 같은 요건은 요구하고 있지 않다.[17] 그러나 이 규정은 신분관계나 가사 혹은 소비자거래 등의 거래에는 적용되지 않는다(동법 Section 10-130(b)).

그러면 무엇이 안전한 전자기록, 안전한 전자서명인가? 이 점에 대해서 동법은 양자에 대해서 유사한 규정을 두고 있는데 여기서는 후자, 즉 안전한 전자서명에 대해서 살펴보기로 하자.

동법은 안전한 전자서명에 대해서 다음과 같이 규정하고 있다. 즉, 적격한 안전성확인절차(a qualified security procedure)를 이용하여 어느 전자서명이 특정인의 서명이라는 점이 검증될 수 있는 경우, 당해 전자서명은 검증시점에서 안전한 전자서명으로 간주된다(동법 Section 10-110(a)). 단 이 때에 신뢰당사자는 당해 적격한 안전성확인절차가, ①당시의 상황에서 거래상 합리적이었다는 점(동법 Section 10-110(a)(1)), ②자신에 의하여 신뢰할 수 있는 방법으로 이용되었다는 점(동법 Section 10-110(a)(2)), 그리고 ③자신이 합리적이고 선의(善意)로 당해 절차를 신뢰하였다는 점(동법 Section 10-110(a)(3))을 입증하여야 한다.

그리고 위의 검증에 이용되는 적격한 안전성확인절차(a qualified security procedure)는 당사자에 의해서 사전에 합의되었거나(동법 Section 10-110(b)(1)), the Secretary of State에 의해서 다음과 같은 네 가지의 요건을 갖춘 전자서명을 신뢰할 수 있는 방법으로 작성할

17) 內田, 상게논문, 295쪽.(동법 Section 10-120(a))

수 있는 절차로서 인정된(certified) 것이어야 한다(동법 Section 10-110(b)(2)). 그 요건이란, ①당해 절차가 이용된 전후관계(context) 속에서 살펴볼 때 서명자에게 고유한(unique) 것일 것(동법 Section 10-110(b)(2)(A)), ②당해 전자기록에 서명한 자를 객관적으로 특정하는(identify) 데 사용할 수 있으며(동법 Section 10-110(b)(2)(B)), ③당해 특정된 자에 의해서 신뢰할 수 있는 방법에 의해서 창출되고 동시에 용이하게 복제 또는 위조할 수 없고(동법 Section 10-110(b)(2)(C)), ④서명후 전자기록이나 서명이 변경된 경우에는 전자서명이 의도적이든 우연적이든 변경될 경우 무효로 되는 방법으로 창출되어, 전자기록에 연결되어 있을 것(동법 Section 10-110(b)(2)(D))이다.

1) the Secretary of State의 안전성 확인절차의 인정 (認定, certification)

위에서 살펴본 바와 같이, 일리노이주법에서는 안전한 전자기록과 안전한 전자서명에 대하여 추정효와 귀속효를 부여하고 있다. 이 때의 전자기록과 전자서명이 안전성을 갖추기 위해서는 적격한 안전성 확인절차에 의해서 안전성이 확인되어야 한다. 그리고 또 이 때에 이용되는 안전성 확인절차가 적격한 것인지의 여부는 the Secretary of State에 의해서 인정을 받아야 한다(동법 Section 10-135(a)). the Secretary of State가 인정을 하기 위하여 행하는 조사(investigation)나 심사(review)에서는 다음과 같은 요소를 고려해야 한다.

첫째로 당해 안전성 확인절차가 장기간에 걸쳐서 공중에게 완전하고 충분하게 정보가 공개되었는가 하는 점이다. 이것은 당해 안전성 확인절차가 적용할 수 있는 정보의 안전성(the applicable information security) 또는 과학계(scientific community)가 의도한 목적에 적합한가에 대한 포괄적인 심사와 평가를 하는데 편의를 제공하기 위함이다(동법 Section 10-135(a)(1)).

둘째로 당해 안전성 확인절차가, 성실한 방법으로 행해지고, 또 적용할 수 있는 정보의 안전성(the applicable information security)의 측면에서 또는 과학계(scientific community)에서 동법 Section 10-105

(안전한 전자기록) 또는 10-110(안전한 전자서명)에서 규정하고 있는 요건을 충족시킴과 동시에 적용할 수 있는 것으로 일반적으로 받아들여지고 있는가 하는 점이다(동법 Section 10-135(a)(2)). 이 경우 the Secretary of State가 당해 안전성확인 절차가 적용할 수 있는 정보의 안전성(the applicable information security)의 측면에서 또는 과학계(scientific community)에서 일반적으로 받아들여지고 있는지의 여부를 결정함에 있어서는 당해 분야에서 외부의 영향을 받지 않는 위치에 있는 전문가의 의견과 국제표준기구(ANSI(the American National Standard Institute), ISO(International Standard Organization), ITU(International Telecommunications Union), NIST(National Institute Standard and Technology)와 같은 단체에 의해서 발표된 내용을 고려하여야 한다(동법 Section 10-135(b)).

셋째로 the Secretary of State는 일리노이주 행정절차법의 규정에 따라서 인정을 행해야 한다. 이 과정에서 the Secretary of State은 당해 안전성 확인절차가 실행가능하고 적용가능한 것인지의 여부를 포함하여 동일성을 확인하기 위한 충분하고 완전한 절차인지를 규명하여야 한다(동법 Section 10-135(c)).

넷째로 the Secretary of State는 안전성 확인절차에 대한 인가(認可)를 일리노이주 행정절차법의 규정에 따라 적절한 조사와 심사를 통하여 취소할 수 있다. 이 때의 인가취소의 사유는 당해 안전성 확인절차가 의도된 목적과는 달리 성실하고 신뢰할 수 있게 행하여지지 않거나 그 밖의 인정의 요건에 위배되는 경우이다(동법 Section 10-135(d)).

2) 일리노이주 인정절차의 인증제도에의 시사점(示唆点)

위의 안전성 확인절차는 이른바 인증기관의 인증업무에 대한 상위인증기관의 관여와 감독에 관한 사항이라고 할 수 있다. 여기서 일리노이주법에서 제시된 요건과 절차를 정리해보면 첫째로 전자서명과 전자인증에 관한 공중에의 완전하고 충분한 정보공개, 둘째로 전자서명・인증에 응용하는 기술의 보편성과 전문성 그리고 인증절차의 적정성이다. 그런데 이와 같은

요건과 절차가 규정하는 내용은 단지 상위인증기관의 인증기관에 대한 규제에만 적용되는 것이 아니고 인증기관 자신도 인증업무와 운영에 도입하여야 할 것이다.

위와 같은 일리노이주 인정절차가 입법례로서 시사하는 가장 중요한 점은 그 내용이 매우 구체적이고 실질적이라는 점이다. 인증업무와 관련하여 발생할 수 있는 법적 문제는 역시 전자서명의 귀속효의 문제라고 할 수 있다. 그리고 이 문제를 해결하기 위한 하나의 방법으로서 안전한 서명을 확보하는 데에는 인증기관 그 자체에 대한 외형적인 규제도 중요하지만 전자서명 그 자체에 대한 구체적이고 실질적인 규제가 훨씬 더 생산적이라고 할 수 있기 때문이다. 어쨌든 이러한 요건과 절차는 전자서명·인증제도를 구성함에 있어서 많은 참고가 될 것이다.

제 2 절 인증제도

1. 사이버공간의 법의 세계에의 편입

컴퓨터 네트워크를 통한 의사전달과정에서 발생하는 위험성을 줄이기 위하여 고안된 전자서명 내지 전자인증은 사이버공간이라는 법적으로 불확정한 상태에 있는 공간을 법의 세계로 편입시키는 제도라고 할 수 있다. 이 때에 사이버공간을 어떠한 법의 세계로 편입시킬 것인가, 즉 인증제도의 내용을 어떻게 구성할 것인가가 문제가 된다. 이 점은 앞 절에서 살펴본 바와 같이 「전자서명·인증과 법」과 관련하여 고려하였던 세 요소, 즉 ① 아날로그와 디지털의 연결고리, ②전자서명에 이용하는 기술, 그리고 ③전자서명에 부여하는 법적 효과가 기본 방향을 정한다고 할 수 있다. 다시 말하면 이 세 요소의 유기적인 연결 속에서 인증제도는 구성되는 것이다.

그런데 인증제도의 구성과 관련하여 위와 같은 실질적인 요소 이외에도 누가 이러한 제도를 운영하는 주체가 될 것인가 하는 문제가 있다. 이 점과 관련해서는 두 가지 점이 논의의 대상이 된다. 첫째는 누가 위와 같은 인증을 할 수 있는가, 즉 인증기관(주체)의 문제이고 둘째는 이 인증기관의 신뢰성을 확보하기 위하여 상위인증기관을 인정할 것인가의 문제이다. 이하에서 이들에 대하여 간단히 살펴보기로 하자.

2. 인증기관

디지털서명의 경우 디지털서명이 첨부된 전자적인 데이터의 작성자가 누구인가는 그 디지털서명을 검증하기 위해서 이용되는 공개키가 어떠한 비밀키에 대응하는 가를 확인함으로써 알 수 있다. 이 때에 공개키와 특정한 자를 연결시켜 주는 정보를 취득하는 방법으로 여러 가지가 있을 수 있지만, 오픈된 네트워크에서 불특정한 자와의 사이에서 디지털서명을 이용한 통신을 행하는 때에, 위와 같은 정보를 제공하는 기관으로서의 인증기관의 존재가 필요하다.[18]

인증기관의 존재의의는 위와 같은 사실상의 기능 이외에도 제도적인 역할을 하고 있다. 먼저, 전자서명에 있어서 법적 효력이 인정되는 전자서명에 해당하는 가를 누구에게나 용이하게 판단하게 할 수 있게 하기 위해서는, 단지 법적 효력을 인정할 수 있는 전자서명의 요건을 정해야 할뿐만 아니라, 이와 함께 어떠한 서명이 법적인 효력이 부여된 전자서명인가를 미리 밝혀 두기 위한 제도를 만들어 둘 필요가 있는 데, 인증기관이 바로 이것에 해당한다. 그리고, 앞서 살펴본 대로, 일정한 디지털서명에 대하여 디지털서명 작성자가 전자증명서에 기재된 자라는 추정규정을 둔 경우에는 그 추정의 전제로서 전자증명서를 발행하는 인증기관에 관하여 그 전자증명서의 내용의 진정성를 담보하기 위한 일정한 틀을 설정해 둘 필요가 있다.[19] 이 때에 이 틀에 해당하는 것이 바로 인증기관이다.

인증기관이 제도적인 측면에서 가장 문제가 되는 것은 인증기관을 공공기관에 한정할 것인가 하는 점이다. 즉, 민간기업에 의한 인증업무를 허용할 것인가의 문제이다. 이 점에 대해서는 여러 입장이 있을 수 있으나, 인증이란 용도가 다양해서 언제나 공공기관에 의한 높은 신뢰성을 지닌 인증이 요구되는 것은 아니라는 점, 그리고 민간기업의 경우에도 암호기술 등을 이용함으로써 인증의 신뢰성을 담보할 수 있다는 점을 들어 민간의 참여를 인정해야 한다는 견해가 있는데 설득력 있다고 하겠다.[20] 특히 후술

18)電子取引法制に關する研究會(制度關係小委員會)報告書、ジュリストNo.1138(1998. 7. 15), 15쪽.
19) 상게 보고서, 29쪽.

하는 인증체계와 관련하여 상위인증기관이 존재할 경우, 민간기업에 의한 인증업무의 신뢰성은 한층 높아지게 될 것이기 때문이다.

3. 인증기관의 체계

공공기관이 독점적으로 인증업무를 행할 경우에는 특별히 공개키의 증명이 문제되는 일은 없을 것이다. 그러나 민간기업이 인증업무에 참여하게 되는 경우 인증업무의 신뢰성을 어떻게 확보할 것인가 하는 문제가 있다.

이 문제를 해결하기 위한 한가지 방법으로 인증기관의 전자서명에 대하여, 그 위에 상위인증기관을 설치하여 그 상위인증기관으로 하여금 하위인증기관의 공개키를 인증하는 방법을 생각해볼 수 있다. 이러한 계층구조형의 인증체계를 취하는 경우, 그 정점에 있는 인증기관은 하위인증기관의 인증만을 행하는 것이 아니라, 자격심사 등도 행하기 때문에 고도의 신뢰성을 충족시킬 수 있는 기관 즉 공공기관이 행하는 것이 타당하다고 할 것이다.[21]

4. 외국의 입법례

여기서는 위에서 살펴본 인증체계, 즉 인증기관과 계층구조형의 인증체계에 대하여 어떠한 규정을 하고 있는지 비교법적으로 살펴보기로 하자.

1) 유엔모델법

유엔모델법은 이 부분에 대하여 아무런 규정을 두고 있지 않다. 규제의 방식이 국가마다 다르다는 점을 염두에 두고 있다고 볼 수 있다.

2) 유타주

유타주의 경우 공인인증기관으로 활동을 하기 위해서는 주로부터 허가를 받아야 한다(동법 제103조 제16항, 제201조 등). 공인인증기관으로 허가를

---

20) 電子取引法制に關する研究會中間報告書, ジュリスト No.1114(1997. 6. 15), 147쪽.
21) 상게보고서, 147쪽.

받기 위해는 엄격한 요건과 자격을 갖추어야만 한다. 그리고 상업국은 공인인증기관의 역할을 함과 동시에 일반 공인인증기관의 상위인증기관으로서 역할을 겸하고 있다. 즉, 상업국은 인증기관의 허가권자이고(동법 제201조 제2항), 인증기관의 활동에 관한 행정입법의 제정(동 제104조 제3항 등), 인증기관의 동법의 규정의 준수여부에 대한 조사, 법규위반에 대한 인증기관의 허가의 제한, 정지 또는 취소 등의 권한(법 제203조 등)을 가지고 있다.

3) 독 일

독일의 경우에도 인증기관은 허가를 받도록 되어 있다(동법 제4조). 그리고 인증기관에 대한 상위인증기관의 역할은 주무관청이 맡고 있다. 즉, 주무관청은 인증서상의 디지털서명을 위하여 사용되는 서명키의 인증서를 발행한다(동 제4조 제5항). 또한 주무관청이 인증기관의 업무정지와 금지 및 허가의 취소 또는 철회의 권한을 가지고 있는 것도 물론이다(동 제13조 등)

4) 일 본

일본의 경우 인증업무의 규제에 있어서 독특한 체계를 취하고 있다. 먼저 인증업무를 주무성령(主務省令)이 정하는 기준에 따라서 행하는 『특정인증업무』와 그렇지 않은 『인증업무』로 나누고 있다.[22] 그리고 이 『특정인증업무』를 행하려고 하는 자는 주무대신의 인정(認定)을 받을 수 있도록 하고 있다(동법 제4조 제1항). 즉 일본법제의 경우 '업무'를 인증하는 방식

22) 이에 관한 조문을 소개하면 다음과 같다.

제 2 조제2항

이 법률에서 『인증업무』란 스스로 행하는 전자서명에 관하여 그 업무를 이용하는 자(이하 『이용자』라고 한다.) 그 밖의 자의 요구에 따라서 당해 이용자가 전자서명을 행했다는 것을 확인하기 위하여 이용되는 사항이 당해 이용자에 관한 것이라는 점을 증명하는 업무를 말한다.

동 제3항

이 법률에서 『특정인증업무』란 전자서명 중에서 그 방식에 따라서 본인만이 행할 수 있는 것으로서 주무성령에서 정하는 기준에 적합하게 행해지는 인증업무를 말한다.

을 채택하고 있는 것이다. 그리고 이 특정인증업무를 행할 수 있는 인정을 받은 자를『인정인증사업자』라고 한다(동법 제8조).

그리고 인증기관의 체계에 있어서도, 독일의 경우처럼, 인증기관의 인증을 행하는 이른바 최상위인증기관(root certification authority)제도는 두고 있지 않다. 다만, 주무관청이 인정기관의 인정에 대한 심사를 하는 과정에서 필요한 조사의 전부 또는 일부를 행하게 할 목적으로 일정한 자를 지정하는 제도를 두고 있다(동법 제4장). 이렇게 지정된 자를 지정조사기관이라고 한다(동 제17조). 이 점도 역시 다른 나라에서 볼 수 없는 독특한 제도이다.

제 3 절 인증업무에 관한 규제의 틀

전자서명에 있어서 가장 핵심적인 부분인 인증업무를 수행하는 공인인증기관에 대하여 어느 정도 규제를 가해야 할 필요성이 있다는 점에 대해서는 누구나 동의한다고 할 것이다. 문제는 어떠한 부분에 대해서 어느 정도까지 규제를 허용할 것인가가 문제가 된다. 규제의 정도와 내용은 각 나라의 사회구조나 정책에 따라서 달라지겠지만 공인인증기관에 대한 규제의 경우에는 인증의 범위가 국내에 그치지 않는 다는 점 그리고 기술적인 요소에 의해서 규제의 내용이 강하게 규율된다는 점을 들 수 있다. 이하에서 각국의 규제의 틀은 어떻게 되어 있는지 입법례를 간단히 살펴보기로 하자.

1. 유엔모델법

동모델법은 이 부분에 대하여 규정을 두고 있지 않다. 앞서 언급한 것처럼 규제에는 각국의 입장이 있고, 또 가능한 한 규제를 하지 않는 쪽에서 생각하기 때문일 것이다.

2. 유타주

유타주의 경우 비교적 엄격한 규제를 행하고 있다고 할 수 있다.

1) 인증기관의 허가제

앞서 살펴본 대로 유타주의 디지털서명법은 공인인증기관에 대해서 허가제를 채택하고 있다. 그리하여, 운영요원에 대한 능력요건, 담보제공의 의무, 운영체제의 안전성, 사업수행에 충분한 활동자금의 보유 그리고 기타 상업국이 규정하는 허가요건의 충족 등의 요건을 갖추고 있어야 한다(동법 제201조 제1항 등). 그리고 상업국은 동법이 규정하고 있는 사항을 준수하지 않거나 허가요건의 결하게 된 때에는 공인인증기관의 허가를 취소 또는 정지할 수 있다(동법 제201조 제4항).

2) 이행감사 및 조사

공인인증기관의 동법에 대한 규정의 준수여부를 평가하기 위하여 컴퓨터보안에 경험이 있는 공인회계사 또는 공인된 컴퓨터보안 전문가로 하여금 매년 1회 이상 감사를 하도록 하고 있다(동법 제202조). 그리고 상업국은 동법의 규정에 대한 준수여부를 확인하기 위해 공인인증기관의 활동을 조사할 수 있고 그 조사를 원할히 하고 동법의 준수를 확실히 하기 위하여 인증기관에 필요한 명령을 할 수 있다(동법 제203조).

3) 업무상의 규제

공인인증기관은 인증업무를 수행함에 있어서 법률이 정하고 있는 일정한 방식에 따라서 행해야 하는 것(제301조 내지 310조 등)과 반대로 금지되는 사항(동법 제204조)이 있다.

3. 독 일

1) 허가제

독일의 경우 인증기관에 대해서는 허가제를 취하고 있다(법 제4조 제1항). 허가의 요건으로서는 신청인의 인증기관을 영위함에 필요한 신뢰성과 전문성, 그리고 인증기관이 업무를 개시할 때에 이 법과 이 법 제16조[23]

에 의한 시행령에서 정하는 인증기관의 업무에 관한 기타의 요건에 대한 충족이다(동 제2항). 이 때에 신뢰성의 요건을 충족시키기 위해서는 신청인이 인증기관의 소유자로서 그 업무에 관하여 적용되는 법규를 준수할 것임을 보장할 수 있어야 하며, 전문지식에 대해서는 인증기관의 업무에 종사하는 자가 필요한 지식, 경험 및 기술을 가지고 있어야 한다. 그리고 인증기관의 업무에 관한 기타의 요건의 충족은 이 법과 이 법 제16조에 의한 시행령에서 정하는 안전성요건을 이행하기 위한 조치가 안전계획에 의하여 주무관청에 적절한 기간내에 통지되고 그 이행이 주무관청의 승인을 받은 기관에 의하여 조사・확인되는 경우이다(동 제3항).

2) 인증업무와 관련된 규제

먼저 주무관청은 인증서상의 디지털서명을 위하여 사용되는 서명키의 인증서를 발행한다(동 제5항 제1문). 즉, 인증기관은 주무관청으로부터 인증받은 서명키를 이용하여 인증업무를 수행하는 것이다. 그리고 인증서의 발행시 신청인의 확인의무 등(동법 제5조), 인증서의 내용(동 제7조), 신청인에 대한 디지털서명의 확인과 관련한 정보제공의무(동 제6조), 허위의 정보에 의하여 인증서가 발행 된 경우 등의 인증서의 접근차단(동 제8조), 시점증명(동 제9조), 안전조치 및 발행된 인증서의 문서화(동 제10조), 업무의 중지시의 의무(동 제11조), 그리고 개인적인 정보수집에 있어서 정보의 보호(동 제12조)에 관하여 구체적으로 규제를 가하고 있다. 그 외에

23) 동법 제16조(시행령)의 규정에 따라 동법 시행령 제1조는 다음과 같이 규정하고 있다.

제 1 조 허가의 부여, 취소 및 철회

(1) 디지털서명법 제4조 제1항의 규정에 의한 인증기관의 업무에 관한 허가는 주무관청에 서면으로 신청하여야 한다.

(2) 주무관청은 허가부여의 요건을 심사하기 위하여 필요한 사항을 확인한다. 주무관청은 필요한 근거서류, 특히 최근의 상업등기부초본과 인증기관의 법률상의 대표자에 관하여 연방중앙등록부법 제30조 제5항에 의한 최근의 품행증명서를 제출하도록 신청인에게 요구할 수 있다. 신청인은 필요한 전문지식을 증명하기 위하여 인증절차 또는 시점증명의 표시를 담당하는 직원이 필요한 직업상의 자격을 갖춘 사실을 상술하여야 한다.

(3) 주무관청은 허가의 거절, 취소 또는 철회를 하기 전에 신청인의 진술을 청문하고 허가의 거절, 취소 또는 철회의 이유에 대하여 이를 시정할 수 있는 기회를 주어야 한다.

서명키의 생성 및 저장과 디지털서명의 생성 및 확인을 위하여 사용하는 기술 부품, 그리고 디지털서명되는 문서의 표시를 위하여 사용하는 기술부품의 경우 안전조치를 행할 수 있는 것이어야 하고, 이들 기술부품에 관하여는 그 기술수준에 의하여 충분하게 검사되고 주무관청의 승인을 받은 기관에 의하여 그 요건의 이행을 확인하도록 되어 있다(동 제14조 제1항 내지 제4항).

3) 국가의 감독

주무관청은 위에서 언급한 사항을 인증기관이 준수하도록 하기 위하여 필요한 조치를 취할 수 있는 권한을 가지고 있다(동법 제13조 제1문).

먼저 주무관청은 부적합한 기술부품의 사용을 금지할 수 있고 인증기관의 전부 또는 일부의 업무를 일시적으로 금지할 수 있다. 또한 동법 제4조의 허가를 받지 아니하고 허가를 받은 것과 같은 외관을 야기하는 자에 대해서는 인증업무를 금지할 수 있다(동법 제13조 제2, 3문). 주무관청은 위와 같은 업무수행을 위하여 인증기관의 업무시간내에 인증기관을 출입할 수 있고, 인증기관에 대하여 장부 등의 자료제출을 요구할 수 있다.

그리고 주무장관은 인증기관이 의무를 이행하지 않을 경우에는 허가를 철회하여야 한다(동법 제13조 제3항). 이 때에 주무관청은 다른 인증기관에 의한 업무의 인수 또는 서명키소유자와의 계약의 청산을 확인하여야 한다(동법 제13조 제4항). 또한 주무관청은 인증서가 위조되었거나 위조로부터 충분하게 보호되지 않는 사실, 또는 서명키의 사용을 위하여 설치된 기술부품이 디지털서명의 위조 또는 디지털서명된 문서의 변조의 가능성이 있어 안전성에 하자가 있는 사실에 관하여 정당한 근거가 있는 때에는 인증서의 접근차단을 명할 수 있다(동법 제13조 제5항).

4. 일 본

1) 인정제도와 지정제도

일본의 경우 앞서 살펴본 것처럼 인증기관의 운영에 대해서 특정인증업무를 행하려는 자(이것을 인정인증사업자라 한다)에 대한 인정제도와 '인

정'시에 필요한 조사 등을 대행하는 지정조사기관제도 라는 독특한 시스템을 채용하고 있다. 일본은 인증업무를 인정을 받지 않고 행하는 인증업무와 인정을 받고 행하는 특정인증업무로 나누고 후자에 대해서는 일정한 요건을 갖춘 자에 대해서 인정을 해주고 있다(전자서명 및 인증업무에 관한 법률 제2조 제2항, 제3항). 동법은, 설비가 주무성령에서 정하는 기준에 적합할 것, 이용자의 진위(眞僞)의 확인이 주무성령에서 정하는 방법에 의해서 이루어질 것, 그리고 그 밖의 업무가 주무성령에서 정하는 기준에 적합한 방법에 의해서 이루어질 것을 인정기준으로 들고 있다(동법 제6조). 지정조사기관은 주무대신을 대신하여 인정인증사업자의 인정시 필요한 조사를 행하거나, 인정사업자가 설비 또는 업무를 변경하고자 하는 경우에 신청을 받는 등의 역할을 한다(동법 제17조).

동법은 지정기준으로 다음과 같이 네 가지 요건을 들고 있다. 즉, ㉠조사업무를 적확하고 원활하게 실시하는데 충분한 경리적 기초 및 기술적 능력을 갖출 것, ㉡법인의 경우에는 임원 또는 법인의 종류에 따라서 주무성령으로 정한 구성원의 구성이 조사의 공정한 실시에 지장을 초래할 염려가 없을 것, ㉢조사업무 이외의 업무를 행하고 있는 경우에는 그 업무를 행함으로 인하여 조사가 불공정하게 될 염려가 없을 것, 그리고 ㉣이 지정으로 인하여 신청에 관한 조사의 적확하고 원활한 실시를 저해하지 않을 것이다.

2) 인증업무와 관련된 규제

일본의 인증제도의 특징은 다른 나라의 규제에 비하여 그 정도가 약하다는 점이다. 즉, 인정인증사업자에게 부과되고 있는 의무에는 인정의 갱신, 업무의 설비, 업무의 실시방법에 변경이 있는 경우의 주무대신의 인정, 인정인증사업자의 신상에 변동이 생긴 경우와 업무의 폐지의 경우의 신고, 업무에 관한 장부 및 서류의 작성 및 보존의무 등에 그치고 있다(동법 제7조 내지 제12조).

지정조사기관의 경우에도, 역시 지정의 갱신(동법 제22조), 임원 또는 직원의 비밀유지의무(동 제23조), 조사의무(제24조), 조사업무규정의 작성과 주무대신의 인가(동 제25조), 장부의 기재 및 보존(동 제26조), 그리고 허가에 의한 조사업무의 폐지(동 제28조) 등에 그치고 있다.

이처럼 일본의 경우 인증업무 그 자체에 대한 규제는 거의 행하고 있지 아니하며 단지 인증제도의 외형을 유지하기 위한 규제에 그치고 있다는 점을 알 수 있다. 이러한 특징은 앞에서 잠깐 살펴본 인증에 대한 기술중립적 태도와 직접 관련이 있다고 할 수 있다. 즉 일본의 동법에서는 기술의 중립성을 전제로 규정을 하고 있기 때문에 그 만큼 규제에 있어서도 엄격성을 유지할 필요성이 적은 것이다.

3) 국가의 감독

동법에서의 국가의 주요한 감독수단은 보고의 요구 및 출입검사, 인정 및 지정의 취소, 그리고 벌칙이다.

주무대신은 동법의 시행에 필요한 한도내에서 인정인증사업자에 대해서 그 인정에 관한 업무에 관하여 보고하게 하며, 소속공무원으로 하여금, 인정인증사업자의 영업소, 사무소 그 밖의 사업장에 출입하여 그 인증에 관한 업무의 상황 혹은 설비, 장부서류 그 밖의 물건을 검사하게 하고, 혹은 관계자에게 질문하게 할 수 있다(동법 제35조 제1항).

주무대신은 인정인증사업자가 동법 제5조의 결격조항에 해당하게 되거나, 동 제6조의 인정기준을 결하게 된 때, 위에서 언급한 운영상의 의무위반, 그리고 부정한 수단에 의해서 인정을 받았거나 또는 변경에 대하여 인정을 받은 경우에는 인정을 취소할 수 있다(동법 제14조).

지정조사기관에 대해서는 주무대신은 당해 기관이 지정기준을 결하게 되었을 경우 이 기준을 다시 충족시키는 데 필요한 조치를 강구하도록 하는 적합명령을 내릴 수 있다(동법 제 27조). 또한 주무대신은, 인정인증사업자의 경우와 마찬가지로, 지정조사기관에 대해서도 보고의 요구 출입검사 권한을 행사할 수 있다(동법 제35조 제2항). 그리고 주무대신은, 인정인증사업자에 대해서와 마찬가지로, 지정조사기관에 부과되어 있는 업무상의 의무위반에 대하여 지정을 취소할 수 있다(동법 제29조).

그리고 또 한가지 국가의 감독수단으로서 벌칙조항을 들 수 있다. 즉 위에서 언급한 사항을 위반했을 경우, 인정인증업자와 지정조사기관은 벌금형과 징역형에 처해지도록 되어 있다(동법 제41조 내지 제47조).

제 4 절 그 밖의 문제

1. 국제적 정합성의 확보

국경의 의미가 약한 사이버공간의 특성상 서명과 관련된 인증제도의 법체계에서 염두에 두어야 할 중요한 사항 중의 하나가 국제적인 정합성의 확보의 문제이다. 이 점과 관련해서 먼저 문제가 되는 것은 법제상에서 채택하고 있는 기술과 전자서명에 대한 법적 효과의 문제이다. 즉 이것들은 국제상호인증의 문제와 밀접한 관련이 잇는데, 이들 문제를 해결하는 방법으로서는 기본적으로는 정부나 국제기관에서 협정이나 조약과 같은 형식으로 쉽게 서로 인증할 수 있는 틀을 마련하는 것도 생각해 볼 수 있을 것이다.

2. 인증기관의 책임

인증은 전자적인 기술을 사용하고 있는데 100% 완벽하다고 할 수 없다. 여기서 인증기관이 잘못하여 인증을 한 결과 상대방이 입은 손해를 어느 정도까지 배상해야 하는 문제가 있다. 이 문제가 생기는 이유는 만약 그 손해가 인증기관의 잘못과 상당인과관계가 있는 경우 배상해야 한다고 하면 인증기관의 경영은 성립할 수 없기 때문이다. 또 이것을 이용자의 요금에 전가시키면 요금이 너무 비싸진다는 문제가 있다. 이것을 보험으로 해결하는 방법도 있으나, 보험의 경우에도 리스크가 너무 크거나 나아가 그 리스크가 어느 정도인지 조차 알기 어려운 점이 있다. 결국 문제는 일정한 경우, 즉 불가항력에 의한 경우 등에 인증기관의 면책을 인정할 것인가 하는 점을 법률에 명기할 것인가가 문제가 된다.[24] 이에 대해서 각국의 입법례는 유타주의 디지털서명법에서 일정한 경우의 면책사유를 정해놓은 예 이외에는 규정하고 있지 않다(동법 제502조 제2항). 이러한 입법의 태도는 현재로서는 분쟁이 어떠한 형태로 발생할 것인지 분명하지 않기 때문에 앞으로의 분쟁의 사례를 지켜보면서 대응하고자 하는 입장이라고 볼 수 있다.[25]

24) 〔座談會〕電子取引法制整備の課題, ジュリスト No. 1183、18쪽, 요코야마의 발언.
25) 〔座談會〕電子取引法制整備の課題, ジュリスト No. 1183, 18쪽, 이나가키의 발언.

제 3 장 전자서명법상의 전자서명·인증에 관한 일반규정

제 1 절 처음에

이상에서는 전자서명법의 분석을 위한 예비작업으로 전자서명·인증을 둘러싼 법적인 문제를 기존의 서면이나 서명·날인과 비교하여 살펴보았다. 그 결과 법적인 논의의 출발점이 되는 기본논점은, 반복이 되지만, ① 아날로그와 디지털의 연결고리, ②전자서명에 있어서의 기술의 의미, 그리고 ③전자서명에 대한 법적 효과의 부여의 세 가지로 수렴된다는 사실을 알았다. 이들 세 가지 논점은, 이미 앞서 살펴본 대로, 서로 유기적인 연관성을 가지며, 전자서명법을 구성하는 기본을 이룬다. 그렇기 때문에 전자서명법의 기본요소 이외에 또 하나의 중요한 부분을 이루는 인증체계에 대한 법적 규율도 위의 세 가지 요소의 내용에 의하여 결정되게 된다. 즉, 다시 말하면 인증제도를 둘러싼 규제의 구조도 위의 세 가지 요소를 유기적으로 고려하여 결정하여야 한다.

이하에서는 위와 같은 점을 염두에 두고 현행 전자서명법의 체계와 구조에 대하여 고찰하기로 한다. 그리고 한가지 여기서 덧붙이고자 하는 사항은 우리 현행법은 전자서명과 전자인증에 대해서 전자서명법 뿐만 아니라 전자거래기본법에서도 규정을 두고 있다는 점이다. 따라서 필요한 경우에는 전자거래기본법의 규정에 대해서도 언급한다는 점이다.[26]

제 2 절 기능적 등가물 접근방식

위에서 살펴본 바와 같이 계약의 성립에 있어서 낙성주의를, 증거법에서 자유심증주의를 취하는 법제에서는 전자메시지, 전자서명을 기존의 서면이나 서명·날인과 연결시키기 위한 입법조치는 불필요하다. 다만 위에서 언

26) 이처럼 전자서명법과 전자거래기본법으로 분리하여 규정하는 것이 입법적으로 바람직한 가에 대해서는 논란은 차치하고라도 양법에서 규정하고 있는 용어의 정의조차도 서로 일치하지 않는 점은 문제라고 하지 않을 수 없다.

급한 것처럼, 국제적인 정합성이라든가, 거래나 재판의 효율을 위한 경우, 그리고 행정청에 전자메시지를 이용하여 허가신청을 하는 경우처럼 계약 이외에 서면이나 서명・날인이 요구되는 경우에는 앞서 언급한 연결고리가 필요할 것이다. 이처럼, 실정법상에서 낙성주의, 자유심증주의를 취하는 경우에는 이른바 아날로그를 디지털에 연결하기 위한 입법조치는 제한적인 의미를 갖는다. 그러나 위와 같은 제한적인 의미에서나마 전자메시지, 전자서명이 갖는 이질성을 극복하기 위한 입법조치가 필요하다고 할 것이다.

현행법은 전자메시지의 문서와 다른 점의 극복, 즉 본고의 표현에 의하면, 아날로그와 디지털을 연결하는 방법으로 유엔모델법의 방식, 즉 전자메시지를 문서에 준하는 방식을 취하고 있음을 알 수 있다. 즉, 이 점은 무엇보다도 전자거래기본법과 전자서명법이 정의(定義)규정에서 전자문서(전자거래기본법 제2조 제1호, 전자서명법 제2조 제1호) 또는 전자서명(전자거래기본법 제2조 제5호, 전자서명법 제2조 제2호)이라는 표현을 쓰고 있는 것으로부터도 알 수 있다.

먼저 현행법이 전자메시지를 어떠한 형태로 규정하여 문서로서의 법적 성격을 부여하고 있는지 살펴보기로 하자. 이에 대하여 전자거래기본법은 '전자문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 아니한다(제5조)'라고 규정하고 있다. 이 규정은 전자메시지도 문서로서 취급한다는 점을 직접 선언하고 있다. 그러나 이러한 규정방식은 논리적으로 비약되어 있다는 생각이 든다. 동법에서는 '전자문서'라는 표현을 쓰고 있지만 실제로 이것은 문서와는 전혀 다른 성격의 것이다. 즉 동법은 전자문서를 '컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적 형태로 작성되어, 송・수신 또는 저장되는 정보'라고 규정하고 있다. 따라서 이것을 단도직입적으로 문서라는 용어를 사용하기보다는 문서와 전자메시지를 공통적으로 연결하는 요소를 찾아내어 그 요소를 매개로 하여 규정을 하는 기능적인 방법을 취해야 할 것이다. 예를 들면, 양자의 공통성은 '메시지'라고 할 수 있으므로 이것을 확인할 수 있는 점에 포인트를 두는 것도 한가지 방법이 될 것이다.

제 3 절 기술의 중립성과 예견가능성

우리 나라의 경우 전자문서에 관한 규율은 전자거래기본법과 전자서명법의 양자에 의해서 이루어지고 있다. 그런데 문제는 똑같은 사안에 대하여 양자의 규정내용이 다르다는 점이다. 먼저 전자거래기본법은 전자문서와 전자서명에 대하여 각각 다음과 같이 규정하고 있다.

제 2 조(정의)

1. “전자문서”라 함은 컴퓨터 등 정보처리능력을 가진 장치(이하 “컴퓨터 등”이라 한다)에 의하여 전자적 형태로 작성되어, 송·수신 또는 저장되는 정보를 말한다.
5. “전자서명”이라 함은 전자문서를 작성한 작성자의 신원과 당해 전자문서가 그 작성자에 의하여 작성되었음을 나타내는 전자적 형태의 서명을 말한다.

이에 대하여 전자서명법은 다음과 같이 규정하고 있다.

제 2 조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “전자문서”라 함은 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성, 송·수신 또는 저장된 정보를 말한다.
2. “전자서명”이라 함은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 당해 전자문서에 고유한 것을 말한다.

전자거래기본법의 경우, 전자문서를 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적 형태로 작성된 정보라고 하고, 전자서명에 대해서도 단지 전자적 서명의 형태라고 규정하여 기술을 특정을 하고 있지 않다.[27]

---

27) 전자거래기본법의 경우에도 전자서명법상의 공인인증기관의 인증을 받은 전자서명에 대해서는 전자서명법의 경우와 마찬가지로 민사소송법상의 형식적 증거력과 본인 및 내용의 비변경성의 추정효를 인정하고 있다(동법 제6조). 그러나 전자서명법상에서 공인인증기관의 인증을 받을 수 있는 전자서명은 디지털방식을 이용한 서명에 한하기 때문에 전자거래기본법이 규정하고 있는 모든 전자서명이 전자서명법상의 공인인증기관에 의한 인증의 대상이 되는 것은 아니다. 그리고 전자거래기본법은 제5조에

그에 반해서 전자서명법은 기술을 특정하고 있다. 즉, 전자서명법은 전자문서에 대한 정의는 전자거래기본법과 같지만, 전자서명은 비대칭 암호화 방식을 이용하여 전자서명생성키로 생성한 정보라고 규정하고 있다. 여기에서 말하는 서명방식이 이른바 '디지털서명'으로 현단계에서 가장 뛰어난 기술방식으로 일컬어지고 있다. 따라서 전자서명법이 예정하고 있는 기술은 '디지털서명'[28]으로 모든 전자서명을 대상으로 하고 있는 것은 아니다. 즉, 수기(手記)서명을 스캐닝한 이미지, 키보드를 이용한 서명, 그리고 접근제어를 위한 비밀번호(password) 등의 기술은 동법의 적용대상에서 제외된다.[29]

이렇게 볼 때 양자는 규율의 대상과 범위가 다르다고 할 것이다. 즉, 전자거래기본법의 경우, 모든 형태의 전자문서, 전자서명을 규율대상으로 하고 있지만, 전자서명법의 경우에는 디지털방식에 의해서 서명된 전자문서만을 그 규율의 대상으로 하고 있는 것이다.

이러한 기술의 특정은 앞서 언급한 예견가능성 즉, 재판상의 증거능력과 서명의 효과와 규제 등의 내용을 규정하는 중요한 출발점이 된다. 즉, 후술하는 것처럼 우리 나라의 전자서명법은 서명의 법적 효과로서 본인의 추정성과 내용의 비변경성까지까지 인정하고 있다. 이것은 해외의 다른 어느 입법례에서도 볼 수 없는 규정이라고 할 수 있다. 그리고 규제와 관련해서는 역시 엄격한 규제가 뒤따르는 것이 보통이다. 즉, 법적 효과를 보장한

서 전자문서의 문서로서의 효력과 제7조에서 전자문서의 증거능력이 부인되지 않는다고 규정하고 있는데, 후술하는 바와 같이, 우리 나라의 법제에서는 자유심증주의(민사소송법 제187)를 채택하고 있기 때문에 이러한 조문은 제한적인 의미만을 갖는다.

28) 전자서명법에서 '디지털서명'이라는 용어 대신 '전자서명'이라는 용어를 사용한 것은 외국어는 가능한 한글로 표기한다는 정부의 어문정책, 법제처의 법률용어 사용방침에의 부응, 디지털서명에 대한 적절한 역어의 부재, 그리고 전자서명이라는 용어로 규정한다고 하더라도 정의 규정에서 디지털서명임을 명확하게 표현하였으므로 혼동은 없을 것이라는 이유가 있다고 한다. 신일순/김춘아/박민성, 〈연구보고〉 전자서명 및 인증제도, 정보통신정책연구원(1998.12), 90쪽.
그러나 위와 같은 용어의 사용은 엄격히 말하면 잘못된 것이라고 말할 수 밖에 없다. 왜냐 하면 디지털서명은 전자서명의 한 종류에 속하는 것으로 전자서명과 동의어가 아니기 때문이다. 다시 말하면 디지털서명은 전자서명의 서브-카테고리(sub-category)인 것이다. 그렇기 때문에 입법례에서 전자서명이라는 용어를 사용하고 있을 경우 기술의 중립성을 취하고 있는 것으로 받아들여지고 있다. 예를 들면, 일본의 입법례.

29) 상게보고서, 90쪽.

만큼, 거기에 걸맞는 규제가 필요하다는 논리도 성립하기 때문이다. 어쨌든 장을 바꾸어 자세히 살펴보겠지만 우리 나라의 전자서명법의 규제는 해외의 다른 입법에 비해서 규제의 정도가 강한 것으로 말해지고 있는데 위의 기술의 특정과 그에 따른 법적 효과의 인정 등이 강한 규제의 한 요인이 되고 있다는 점은 틀림없는 사실이라고 할 수 있을 것이다.

그러나 이러한 규정방식이 문제가 없는 것은 아니다. 먼저 기술의 특정과 관련한 점이다. 기술을 특정할 경우 그 방식을 이용한 전자문서에 대하여 그에 상응한 법적인 효과를 법률로 규정하는 것이 가능하기 때문에 앞서 언급한 예견가능성이라는 관점에서 볼 때 큰 강점을 지닌다고 볼 수 있다. 이러한 예견가능성이 보장될 때, 전자문서를 이용한 거래가 활발해져서 제도의 목적을 충분히 달성할 수 있다. 그러나, 이미 다 알고 있듯이, IT기술의 혁신은 그 내용과 속도에 있어서 상상을 초월하는 측면이 있기 때문에 특정한 기술의 지정은 이러한 기술개발을 저해하는 요소로 작용할 수 있다. 실제로 현재 전자서명법에서 규정하고 있는 디지털서명방식은 현 단계에서 가장 뛰어난 기술을 구사하고 있다고 하지만, 이 방식이 이용하고 있는 비대칭암호방식과 병행하여 공통키에 의한 서명방식의 이용도 검토되고 있다. 따라서 입법의 방식으로써 꼭 기술을 특정해야 하는가에 대해서는 검토의 여지가 있다고 하겠다.

그리고 기술의 특정과 관련하여 또 문제가 되는 것은 전자서명에 따른 법적 효과의 문제이다. 전자서명의 효과를 어디까지 인정할 것인가는, 이미 거듭해서 언급한 것처럼, 거기에서 이용되는 기술과도 밀접한 관련이 있다. 기술을 특정하게 되면 법원도 전자서명의 완전한 효과를 인정하는 데에 인색하지 않을 것이다. 거기서, 일정한 기술을 사용하면 완전성(integrity)에 관하여 재판소가 틀림없이 추정효를 인정한다고 하는 메시지를 입법이라고 하는 형태로 전하면, 한 발 앞선 형태의 안전성을 제공할 수도 있을 것이다. 이와 같은 제도의 구성이 이른바 예견가능성을 높여서 전자거래를 활성화에 직접 연결된다는 점은 두 말할 필요도 없을 것이다. 이러한 취지에서 우리 나라의 전자서명법은, 다음 항목에서 자세히 살펴보겠지만, 공인인증기관에 의해서 인증을 받은 전자서명의 법적 효과로서, 민사소송법상의 형식적 증거력(민사소송법 제328조, 제329조)은 물론

이고 본인 및 내용의 무변경성에 대한 추정효까지 인정하고 있다(전자서명법 제3조).

그러나 이처럼 전자서명의 법적 효과를 두텁게 인정하는 데에도 문제점은 내포되어 있다. 즉, 위와 같은 규정을 둘 경우, 실제로 전자서명이 첨부되어 있기만 하면 그것은 변경되어 있지 않다고 하는 것을 정의(定義)상 말하고 있는 것과 마찬가지 이야기가 된다. 그리고 전자서명의 효과에 비변경성까지 포함되게 되면 아주 사용하기 쉽게 되지만, 역시 기술(技術)이라고 하는 것은 어딘가에 허점이 있기 마련이므로, 개인의 권리가 아무런 귀책사유도 없는데 뺏기고 만다고 하는 것은 납득하기 어려운 일이라고 할 것이다.[30]

이점과 관련하여 현행법제의 경우, 본인의 추정효를 인정함으로써 발생할 수 있는 사안에 대하여 충분한 입법적인 대응이 되어 있다고는 볼 수 없다.

제 4 절 전자서명의 법적 효과

위에서 살펴본 바와 같이 전자서명에 대한 법적 효과와 관련해서 주로 문제가 되는 것은 귀속효과, 명의인의 동일성확인의 효과, 그리고 완전성유지효과였다. 이 중에서 완전성유자효과의 경우, 전자서명기술로써 디지털서명 이상의 기술을 사용하면 서명이나 날인 이상의 확실성을 보장할 수 있음을 알았다. 그리고 명의인의 동일성확인효과의 경우에도 인증기관이 확실한 확인절차의 수행 등 인증업무를 충실히 수행할 경우 인정을 할 수 있을 것이다. 즉, 명의인의 동일성확인효과의 인정여부는 인증기관의 기능과 역할이 그 관건이 된다. 이 점은 인증기관에 대한 국가의 규제의 강도와 밀접한 관계가 있다.

그러나 역시 제일 문제가 되는 것은 귀속효과이다. 이미 앞서 언급한 것처럼, 여기에는 두 가지 측면이 있다. 먼저 전자서명에 대한 서명자 본인의 승인의사를 인정할 것인가의 문제이다. 만약 이것을 긍정한다면 전자서명에 이른바 『형식적 증거력』을 부여할 수도 있다. 또 한가지는 이른바 표

30) 〔座談會〕電子取引法制整備の課題, ジュリスト No. 1183, 15쪽, 이나가키의 발언.

현대리의 문제이다. 즉, 전자서명의 명의인의 의사와 관계없이 타인이 서명을 한 경우 그 효과를 명의인에게 귀속시킬 수 있을 것인가 하는 점이다. 이하에서는 이러한 점을 염두에 두고 현행법상의 전자서명의 법적 효과에 대한 규정을 검토해 보기로 한다.

전자거래기본법 제6조와 전자서명법 제3조는 전자서명의 법적 효과에 대하여 각각 다음과 같이 규정하고 있다.

전자거래기본법

제 6 조(전자서명의 효력) ①제16조의 규정에 의한 공인인증기관이 인증한 전자서명은 다른 법률에 그 효력을 부인하는 규정이 있는 경우를 제외하고는 관계 법률이 정하는 서명 또는 기명날인으로 본다.

②제1항의 규정에 의한 전자서명이 있는 전자문서는 작성자가 서명한 후 그 내용이 변경되지 아니한 것으로 추정한다.

전자서명법

제 3 조 (전자서명의 효력) ①공인인증기관이 제15조의 규정에 의하여 발급한 인증서에 포함된 전자서명검증키에 합치하는 전자서명생성키로 생성한 전자서명은 법령이 정한 서명 또는 기명날인으로 본다.

②제1항의 규정에 의한 전자서명이 있는 경우에는 당해 전자서명이 당해 전자문서의 명의자의 서명 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다.

위의 전자거래기본법과 전자서명법의 규정을 보면, 먼저 양자 모두 귀속효과 중에서 명의인의 전자서명의 내용에 대한 구속의사를 인정하는 이른바 형식적 증거능력을 인정하고 있다. 즉 전자거래기본법 제6조 제1항과 전자거래기본법 제3조 제1항의 규정이 바로 그것이다. 그러나 이 형식적 증거능력을 인정함에 있어서 문제가 되었던 것이 종래의 서명이나 날인이 수행하는 이른바 경고기능이 전자서명의 경우에는 확보되기 어렵다는 점이었다. 따라서 이러한 문제점을 보완할 수 있는 법률의 규정이 있는 편이 바람직하다고 할 것이다. 그러나 현행법에는 이러한 조항이 존재하지 않는

다. 물론 이 문제점은 전자서명기술의 발달에 의해서 얼마든지 해결될 수 있는 문제이지만 현재의 기술수준에서는 역시 검토되어야 할 사항이라고 할 것이다.

이어서 전자거래기본법 제6조 제2항과 전자서명법 제3조 제2항의 문제이다. 여기서는 양자의 규정방식이 다르다. 즉 전자는 전자서명내용의 무변경성, 이른바 완전성유지효과를 인정하고 있는데 그치고 있는 반면 후자는 거기에 이른바 표현대리까지도 인정하고 있기 때문이다. 이것은 똑같은 전자서명에 대하여 서로 다른 법적 효과를 인정하고 있는 것이어서 법적인 정비가 요청된다. 그리고 완전성유지효과는 현재 전자서명법에서 전자서명기술로 디지털서명을 채용하고 있기 때문에 이 효과를 인정하는 데에는 큰 문제가 없을 것이다.

그런데 역시 문제는 타인이 명의인의 이름을 사칭하여 전자서명을 한 경우, 즉 표현대리를 인정할 것인가 하는 문제이다. 이 문제는 앞서 살펴본 대로 명의인에게 귀책사유가 없음에도 불구하고 언제나 책임을 지우게 하는 것은 불합리하다고 할 것이다. 따라서 어떠한 요건하에서 명의인이 책임을 져야 하는가 하는 점에 대해서 법률에 명시해 두어야 할 것이다. 그러나 현행법은 이 점에 대해서 침묵하고 있다. 이것은 중대한 입법의 불비로 시급히 개선되어야 할 것이다.

제 4 장 인증제도에 관한 현행법제

제 1 절 처음에

인증업무 관련기관으로서는 정보통신부, 한국정보보호센터, 공인인증기관, 국가정보원 등이 있지만 이 중에서 핵심이 되는 기관은 역시 공인인증기관과 한국정보보호센터(이하 보호센터라고 칭한다)이다. 즉 공인인증기관은 전자서명법에서 규정하고 있는 인증을 실제로 행하는 기관이기 때문이다. 그리고, 보호센터의 경우, 공인인증기관의 상위인증기관으로서의 기능을 수행하고 있을 뿐만 아니라, 정보통신부의 공인인증기관의 지정과 관련된 실질심사를 담당하는 등, 이른바 공인인증제도의 안전성과 신뢰성의 확보를 위한 제도의 중심에 있다고 할 수 있다. 이하에서는 공인인증기관과 보호센터를 중심으로 인증제도에 관한 현행법제를 분석하기로 한다.

제 2 절 공인인증기관

1. 공인인증기관의 법적 성질

전자서명이 법적으로 효력을 인정받기 위해서는 전자서명법(제3조) 및 전자거래기본법(제6조)이 정하고 있는 공인인증기관에 의해서 인증을 받아야만 한다. 이 공인인증기관은 정보통신부장관이 '인증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자'중에서 지정하도록 하고 있다(전자서명법 제4조 제2항). 그리고 '공인인증기관으로 지정 받을 수 있는 자는 국가기관·지방자치단체 또는 법인'에 한하도록 되어 있다(전자서명법 제4조 제2항).

여기서 이 공인인증기관의 법적 성질이 무엇인가가 문제가 된다. 그런데 현행법상 공인인증기관으로 지정될 수 있는 것은 국가기관·지방자치단체와 법인인데 이 때에 전자와 후자는 법적 성질이 같은 것인지 그렇지 않으면 달리 취급해야 할 것인지 논란의 여지가 있다. 그러나 현재 공인인증기관으로 지정된 기관은 모두 법인이라는 점 등을 감안하여, 편의상 본고에

서는 법인으로서 지정된 공인 인증기관에 한정해서 살펴보기로 한다.

국가 또는 지방자치단체는 행정사무를 자신이 스스로 처리하기도 하지만, 여러 가지 이유에서 외부의 기관, 특히 민간의 법인에게 맡겨서 처리하기도 한다. 이것을 이른바 『사인(私人)에 의한 행정』 라고 한다.[31] 이 경우 민간의 법인에게 맡겨지는 행정사무의 내용에 따라, 당해 법인을 지정기관, 지정법인 등으로 분류하여 법적인 성질을 논하기도 한다.[32] 전자의 지정기관은 지정에 의하여, 지정되기 전에는 소관장관 등이 행사하도록 되어 있던 '행정권한'이 위임되고, 그것을 행사하게 된다. 지정기관으로서 지정(보통 행정처분에 의해서 행해진다)되면, 행정권한이 사인에게 위임되고 위임된 권한에 행정처분을 발할 수 있는 권한이 포함되어 있는 경우에는, 위임 후 지정기관이 스스로 행정청으로서 당해 권한을 자신의 이름으로 행하게 된다.

그에 반해서 후자의 지정법인은 행정청으로부터 지정을 받아 일정한 공공적 업무를 행하는 법인을 말한다. 이 지정법인은, 지정기관이 권력적인 행정권한을 위임받아 업무를 수행하는 것과는 달리, 비권력적인 업무나 지도, 계발 등과 같은 활동을 하는 것이 보통이다.[33] 즉, 양자를 구분하는 기준은 수행하는 업무의 권력성의 유무에 있다고 할 수 있다.

이러한 지정기관, 지정법인에 대해서는 지정의 단계에서부터 엄격한 규제를 받는다. 즉, 지정요건과 업무상의 보고, 장부비치, 업무의 휴·폐지의 제한, 비밀유지업무, 그리고 위반할 경우 지정의 취소나 행정벌에 의한 제재 등이 가해지게 된다.

위와 같은 분류에 따를 경우 전자서명법상의 공인인증기관은 지정법인에 해당한다고 할 수 있다. 즉, 인증업무는 전자서명의 진정성을 확인하는 일로써 이것은 비권력적인 업무이기 때문이다. 그리고 이러한 인증업무는 원래 국가가 독점적으로 행하는 일이 아니기 때문에 이러한 지정행위는 사실상 사인의 활동을 규제하는 하나의 방식으로 이해할 수 있다.[34]

---

31) 米丸恒治, "私人による行政", 日本評論社(1999), 315쪽.
32) 米丸, 上揭書, 315쪽.
33) 이상은 米丸의 상게서 315-316쪽을 참고로 하여 작성.
34) 米丸, 上揭書, 344쪽 참조.

실제로 현행법상 인증제도에 대한 규제의 근간을 이루는 것이 바로 이 공인인증기관의 지정제도이다. 즉, 현행법은 전자서명에 대한 인증을 행할 수 있는 기관을 지정하여 인증 자체를 행할 수 있는 기관을 제한하고 있는 것이다. 이것은 시작의 단계에서부터 인증제도의 목적에 적합하지 않은 행위자를 배제하려는 것이다. 그렇기 때문에 이것은 규제의 기본이면서 또한 다음 단계에 대한 규제를 예정하고 있는 것이기 때문에 지정제도는 강력한 규제수단의 하나라고 말할 수 있다.

이하에서는 위와 같은 점을 염두에 두고 전자서명법상의 공인인증기관에 대한 규정을 고찰하고자 한다.

2. 공인인증기관의 지정요건

1) 안전성・신뢰성의 요건

지정제도는 '무엇이 법률상 효과를 갖는 전자서명인가를 명백히 하고, 또 공인인증기관의 전자증명서에 기재된 자가 디지털서명을 작성한 자라고 추정하기 위한 요건을 설정'하는 의미도 갖는다. 이러한 지정제도의 취지에서 볼 때, 공인인증기관의 요건은 추상적으로는 「인증기관으로서의 업무를 적정하고 확실하게 처리할 수 있을 것」이라고 말할 수 있다. 「인증기관으로서의 업무」의 구체적인 내용은 뒤에서 살펴보기로 하고 여기서 문제가 되는 것은 「적정하고 확실」하게 처리할 수 있다는 기준이 무엇인가 하는 점이다.[35]

전자서명법 제4조 제1항은 '정보통신부장관은 인증업무를 안전하고 신뢰성있게 수행할 능력이 있다고 인정되는 자를 공인인증기관으로 지정할 수 있다.'라고 규정하고 있다. 이 요건은 동법 제4조 제3항의 기술능력・재정능력 등과 직접적인 관계를 갖고 있다. 이 안전성과 신뢰성을 확보하기 위해서 고려해야 할 요소로서 다음과 같은 점을 고려해 볼 수 있다. 첫째로 인증업무는 암호방식을 이용하기 때문에 암호에 관한 전문지식을 갖추고 있는 관리자가 필요하다. 그리고 이 관리자는 고객에게 발행하는 공개키-

35) 電子取引法制に關する研究會報告書, ジュリスト(1998.7.15)、30쪽.

증명서에 안전성 높은 암호키를 사용하여 디지털서명을 하기 위해서도 필요하다고 할 것이다.

둘째로 인증시스템에의 불법적인 침입에 대한 방지조치의 필요성이다. 인증기관의 인증시스템은 이른바 해커- 등에 의한 외부로 부터의 불법적인 침입을 당할 염려가 있다. 인증기관은 이러한 불법적인 침입으로부터 시스템을 보호하기 위하여 신뢰성 높은 방어벽을 구축할 필요가 있다.

셋째로 설비의 안전성과 신뢰성의 확보이다. 인증기관이 안정적, 계속적으로 인증업무를 수행하기 위해서는 설비의 안전성과 신뢰성을 확보하는 일이 중요하다. 예를 들면, 사고에 대비한 설비의 다중화와 보관데이터 베이스의 백업 등의 조치가 그것이다. 또한 천재지변 등과 같은 자연재해에 대한 안전대책도 필요하다.

넷째로 관련시설내부에의 외부인의 부정침입을 방지하기 위한 조치의 필요성이다.

마지막으로 업무제공의 계속성·신속성의 확보이다. 인증기관이 제공하는 공개키-증명서의 발행이나 고객으로부터의 증명서를 건네 받은 제3자로부터의 조회 등의 서비스에 관해서는 이들 서비스의 이용자가 필요할 때에는 언제든지 이용할 수 있도록 하기 위한 계속성·신속성이 필요하며, 이를 위해서는 설비상·운영상의 체제를 갖출 필요가 있다. 특히 증명서가 실효된 경우 신속히 공시되지 않는다면 고객이나 이를 건네 받은 제3자가 불측의 손해를 입을 가능성이 있기 때문에 특히 신속성이 요청된다.

위와 같은 요소는 결국 기술능력·재정능력 등과 직접적인 관련이 있다. 현행법에서는 기술능력·재정능력 등에 관한 구체적인 기준은 대통령령에 위임하고 있다. 이 위임규정에 따라 전자서명법 제3조 제1항 제1호는 기술능력에 대하여 다음과 같이 규정하고 있다.

제 3 조 (지정기준) ①법 제4조제3항의 규정에 의한 공인인증기관의 지정기준은 다음 각호와 같다. 다만, 국가기관 또는 지방자치단체가 공인인증기관으로 지정 받는 경우에는 제2호의 재정능력을 적용하지 아니한다.

1. 기술능력 : 다음 각목의 요건을 갖춘 인증관리체계 운영인력 12인 이상

가. 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의

국가기술자격 또는 이와 동등 이상의 자격이 있다고 정보통신부장관이 인정하는 자격을 갖출 것

나. 정보통신부장관이 정하여 고시하는 정보보호 또는 정보통신운영·관리 분야에서 2년 이상 근무한 경력이 있을 것

다. 인증관리체계의 운영·비상복구대책 및 침해사고의 대응 등에 관하여 보호센터에서 실시하는 교육을 이수할 것

2. 재정능력 : 자본금 80억원 이상

3. 시설 및 장비 : 다음 각목의 설비

가. 가입자의 신원확인 및 관리를 위한 설비

나. 전자서명키 관리체계를 안전하게 유지하기 위한 설비

다. 인증서를 안전하고 신뢰성있게 관리하기 위한 설비

라. 전자서명 및 시점확인을 위한 설비

마. 인증관리체계를 안전하게 운영하기 위한 보호설비

②제1항제3호의 규정에 의한 시설 및 장비에 관한 세부사항은 정보통신부령으로 정한다.

2) 결격요건

이 요건은 법인이 공인인증기관으로 지정 받기 위한 소극요건으로 결국은 안전성과 신뢰성을 확보하기 위한 것이라고 말할 수 있다. 전자서명법은 다음과 같이 규정하여 법인의 임원이 여기에 해당하는 경우에는 당해 법인은 공인인증기관으로서 지정을 받을 수 없다고 규정하고 있다.

제 5 조 (결격사유) 다음 각 호의 1에 해당하는 자는 공인인증기관으로 지정 받을 수 없다.

1. 임원 중 다음 각목의 1에 해당하는 자가 있는 법인

가. 금치산자·한정치산자 또는 파산자로서 복권되지 아니한 자

나. 금고이상의 실형의 선고를 받고 그 집행이 종료(집행이 종료된 것으로 보는 경우를 포함한다)되거나 집행이 면제된 날부터 2년이 경과되지 아니한 자

다. 금고이상의 형의 집행유예의 선고를 받고 그 집행유예기간 중에

있는 자

라. 법원의 판결 또는 다른 법률에 의하여 자격이 상실 또는 정지된 자

마. 제12조의 규정에 의하여 지정이 취소된 법인의 취소당시의 임원이었던 자(취소된 날부터 2년이 경과되지 아니한 자에 한한다)

2. 제12조의 규정에 의하여 지정이 취소된 후 2년이 경과되지 아니한 법인

3) 지정의 대상

전자서명법은 '공인인증기관으로 지정 받을 수 있는 자는 국가기관·지방자치단체 또는 법인'에 한정하고 있다(동법 제4조 제2항). 공인인증기관이 수행하는 인증업무는 위에서 살펴본 것처럼 많은 자본과 높은 기술력을 필요로 한다. 그렇기 때문에 공신력 있는 기관이나 법인과 같은 형태의 기관으로 인증기관의 지정대상을 한정할 필요가 있는지도 모른다. 그러나 개인이라고 해서 위와 같은 자본과 기술력을 갖출 수 없는 것은 아니며, 인증기술의 혁신 등에 의해 개인에 의해서도 얼마든지 인증업무를 수행할 가능성이 있다고 할 것이다. 따라서 이처럼 공인인증기관의 지정대상을 한정하는 것은 검토의 여지가 있다.

4) 지정절차

공인인증기관의 지정절차는 대통령령과 시행규칙으로 규정하게 되어 있다(동법 제4조 제4항, 동법시행령 제2조 제1항, 동법시행규칙 제2조). 그러나 위의 법령에 규정된 내용은 지정을 신청하는데 필요한 서류 등에 관한 사항, 그리고 국가 또는 지방자치단체를 공인인증기관으로 지정하는 경우에는 미리 관계기관의 장과 협의하도록 규정하는데에 그치고 있다. 따라서, 지정은 행정처분이기 때문에 지정에 따른 실질적인 절차는 행정절차법의 규정에 의해서 진행되어야 한다(행정절차법 제3조 제1항). 따라서 행정절차법 제2장 처분에 관한 규정을 중심으로 처분절차에 적용되는 규정은 인증기관의 지정절차에도 그대로 적용된다.[36]

36) 여기서 인증기관의 지정의 경우, 인증기관의 지정을 받고자 하는 자(즉, 상대방)의

그리고 또 한가지 여기서 지적해야될 사실은 지정절차와 관련하여 시행령 제2조 제3항에 '정보통신부장관은 국가기관 또는 지방자치단체를 공인인증기관으로 지정하는 경우에는 미리 관계기관의 장과 협의하여야 한다.' 라고 규정하고 있는데 이 규정은 시행령에 규정할 사항이 아니라 법률, 즉 전자서명법에 규정하여야 한다. 왜냐하면 관계기관과의 협의는 권한행사의 주체를 제약하는 사항이기 때문이다. 법률에 규정이 없이 시행령에 바로 규정하는 것은 위임입법의 한계를 벗어난 일이라고 해야할 것이다.

위와 같은 절차를 통해서 정보통신부장관이 '공인인증기관을 지정하는 경우에 공인인증기관지정대장에 이에 관한 사항을 기재한 후 신청인에게 공인인증기관지정서를 교부하고, 보호센터로 하여금 전자서명법 제2조 제10호의 규정에 의한 인증관리체계에 의하여 누구든지 그 지정사실을 확인할 수 있도록 필요한 조치를 취하게 하여야 한다(시행령 제2조 제2항).

3. 공인인증기관의 의무

1) 인증업무준칙의 제정(법 제6조)

공인인증기관은 인증업무를 개시하기 전에 인증업무의 종류, 수행방법 및 절차, 인증역무의 이용조건 및 이용요금, 기타 인증업무의 수행에 관하여 필요한 사항이 포함된 인증업무준칙을 작성하여 정보통신부장관에게 신고하도록 되어 있다(법 제6조 제1항). 그리고 정보통신부장관은 신고한 인증업무준칙의 내용이 인증업무의 안전과 신뢰성의 확보에 지장을 초래하거나 가입자의 이익을 저해할 우려가 있다고 판단하는 경우에는 상당한 기간을 정하여 당해 공인인증기관에게 인증업무준칙의 변경을 명할 수 있다(법 제6조 제2항).

이 인증업무준칙은 공인인증기관이 업무를 적정하고 확실하게 행할 수 있도록 담보하기 위하여 공인인증기관으로 하여금 인증업무에 관한 기본적

신청에 의해서 절차가 진행되는 이른바 신청에 대한 처분이기 때문에 행정절차법 중 신청에 대한 처분에 관한 규정이 주로 적용된다. 즉 제17조의 처분의 신청, 제19조의 처리기간의 설정·공포, 제20조의 처분기준의 설정·공표, 제22조의 의견청취, 그리고 신청을 거부하는 경우에는 제23조 처분의 이유제시 등의 규정이 적용된다.

인 사항을 정한 것이다.[37] 업무준칙에 규정해야 할 사항에 대해서 법령으로 규정하는 방식과 공인인증기관의 임의에 맡기는 방식을 생각해 볼 수 있는데 현행법은 후자를 택하고 있다. 다만 이를 보완하는 방식으로 일정한 경우, 정보통신부장관이 변경명령권을 행사하도록 하고 있는 것이다.

2) 서비스제공과 관련된 의무

이른바 지정법인으로서의 공인인증기관의 인증업무는 공공적 성격을 띠기 때문에 서비스의 제공에 있어서 민사상의 그것과는 다른 법적인 제약을 받는다. 즉, 정당한 이유 없이 서-비스의 요청을 거부하거나 부당한 차별을 해서는 안된다(법 제7조). 그리고 서비스의 내용도 법령의 규정에 의해서 일정한 정도까지 정해진다. 즉, 전자서명법은 인증서에 포함되어야 할 사항, 인증서의 효력 등에 대하여 규정을 두고 있다. 이하 차례로 살펴보기로 한다.

(1) 인증서의 내용

제15조 제2항은 인증업무의 핵심인 인증서발급에 있어서 인증서의 내용에 다음과 같은 사항을 포함시키도록 규정하고 있다.

1. 가입자의 이름
2. 가입자의 전자서명검증키
3. 가입자와 공인인증기관이 이용하는 전자서명 방식
4. 인증서의 일련번호
5. 인증서의 유효기간
6. 공인인증기관의 명칭
7. 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 이에 관한 사항

그리고 인증서를 발급 받고자 하는 자의 신청이 있는 경우에는 인증서의 이용범위 또는 용도를 제한하는 인증서를 발급할 수 있고(법 제15조 제4항), 특히 유효기간을 정함에 있어서는 인증서의 이용범위 및 용도, 이용

37) 電子取引法制に關する硏究會報告書, 30쪽.

된 기술의 안전과 신뢰성 등을 고려하도록 규정하고 있다(법 제15조 제5항).

⑵ 인증서의 효력의 소멸, 효력의 정지, 폐지

정식으로 발급된 인증서일지라도 발급 후 법령에 규정된 일정한 사유의 발생에 의하여 인증서의 효력이 소멸, 정지되거나 인증서 그 자체가 폐지되기도 한다.

먼저 인증서의 효력은 다음과 같은 사유에 의하여 소멸된다(법 제16조). 즉, ①인증서의 유효기간이 경과한 경우, ②법 제12조 제1항의 규정(사위(詐僞) 기타 부정한 방법으로 공인인증기관을 지정 받은 경우 등)에 의하여 공인인증기관의 지정이 취소된 경우, ③가입자 또는 그 대리인의 신청에 의해(법 제17조) 인증서의 효력이 정지된 경우, ④법 제18조의 규정(가입자 또는 그 대리인이 인증서의 폐지를 신청한 경우 등)에 의하여 인증서가 폐지된 경우, 그리고 ⑤법 제21조 제4항의 규정(공인인증기관이 보관·관리 소호로 전자서명생성키가 분실·훼손 또는 도난·유출 된 때)에 의하여 보호센터가 공인인증기관에게 발급한 인증서가 폐지된 경우이다.

인증서의 효력의 정지에는 행정처분에 의한 정지와 가입자 등에 의한 정지의 두 가지 경우가 있다. 전자의 경우, 정보통신부장관이 '인증업무의 안전과 신뢰성 확보를 위하여 필요한 경우 제10조의 규정에 의하여 인증업무를 휴지 또는 폐지하였거나 제12조의 규정에 의하여 인증업무가 정지된 공인인증기관이 발급한 인증서의 효력을 정지'하는 경우이다. 이 경우 정보통신부장관은 보호센터로 하여금 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(법 제16조 제3항). 후자는 가입자 또는 그 대리인의 신청에 의하여 공인인증기관이 인증서의 효력을 정지하는 경우이다(법 제17조 제1항). 이 경우에도 공인인증기관은 인증서의 효력을 정지한 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(법 제17조 제2항).

마지막으로 인증서의 폐지이다. 이것은 가입자 등의 신청이나 법령의 규정에 의한 사유에 근거하여 공인인증기관이 인증서를 폐지하는 것으로 제

3자의 불측의 손해를 방지하는데 목적이 있다. 현행법상 규정된 폐지사유로는, ①가입자 또는 그 대리인이 인증서의 폐지를 신청한 경우, ②가입자가 사위 기타 부정한 방법으로 인증서를 발급 받은 사실을 인지한 경우, ③가입자의 사망·실종선고 또는 해산 사실을 인지한 경우, 그리고 ④가입자의 전자서명생성키가 분실·훼손 또는 도난·유출된 사실을 인지한 경우이다(법 제18조 제1항). 그리고, 이 때에 공인인증기관은 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(법 제18조 제2항).

3) 인증업무의 안전 및 신뢰성확보의 의무

(1) 전자서명키의 보관·관리의무

전자서명키에 대해서는 공인인증기관의 업무개시의 시점에서부터 엄격한 통제를 받게 되어 있다. 즉, 공인인증기관은 인증업무를 개시하기 전에 보호센터로부터 전자서명검증키를 인증받아 이 키에 합치하는 전자서명생성키를 이용하여 인증업무를 수행하여야 한다(법 제8조).

공인인증기관은 가입자의 신청이 있는 경우 이외에는 가입자의 전자서명생성키를 보관하여서는 아니 되며, 가입자의 신청에 의하여 그의 전자서명생성키를 보관하는 경우에도 당해 가입자의 승낙 없이 이를 이용하거나 유출하여서는 아니 된다(법 제18조 제2항). 또한 공인인증기관은 자신이 이용하는 전자서명생성키를 안전하게 보관·관리하여야 하며, 당해 전자서명생성키가 분실·훼손 또는 도난·유출된 때에는 보호센터에 지체없이 통보하고 인증업무의 안전과 신뢰성을 확보할 수 있는 대책을 강구하여야 한다(법 제18조 제3항). 공인인증기관으로부터 통보를 받은 보호센터는 당해 공인인증기관에게 발급한 인증서를 폐지하고 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(법 제18조 제4항).

그리고 가입자에게도 자신의 전자서명생성키를 안전하게 보관·관리하고, 또 이를 분실 또는 훼손한 때에는 공인인증기관에 통보하여야 하는 의무를 지고 있다(법 제18조 제1항).

⑵ 비밀유지의무

공인인증기관은 인증업무와 관련하여 가입자 등의 개인정보를 입수하게 되는데 이들 정보를 필요 이상으로 수집을 하거나 수집한 정보를 함부로 누설해서는 아니 된다. 현행법은 공인인증기관의 개인정보 수집단계에서부터 엄격한 규제를 하고 있다.

먼저 공인인증기관은 인증업무 수행에 필요한 최소한의 개인정보만을 수집하여야 하며, 본인의 동의없이 개인정보를 수집하여서는 아니 된다(법 제24조 제1항). 그리고, 공인인증기관은, 다른 법률에 특별한 규정이 있거나 본인의 동의가 있는 경우 이외에는, 수집된 개인정보를 인증업무 이외의 목적으로 이용하거나 유출하여서는 아니 된다(법 제24조 제1항). 나아가 공인인증기관 뿐만 아니라 인증업무에 종사하거나 종사하였던 자의 경우에도 직무상 알게 된 타인의 개인정보를 누설하거나 타인에게 제공하여서는 아니 된다(법 제24조 제4항). 그리고 만약 가입자가 자신의 개인정보에 대한 열람을 신청하거나 당해 개인정보의 오류에 대하여 정정을 요구하는 때에는 공인인증기관은 지체없이 필요한 조치를 취하여야 한다(법 제24조 제3항).

⑶ 인증업무의 휴지·폐지 및 양수 등에 따른 의무

공인인증기관이 인증업무를 휴지하거나 폐지하는 경우, 그 때까지 발행된 전자증명서의 유효성이 당해 공인인증기관에 의해 증명될 수 없게 되어 재판 등에서 당해 공인인증기관이 발행한 전자증명서의 유효성이 문제가 되는 경우에 그 입증이 곤란해지는 문제가 있다.[38] 따라서, 이에 대비하여 공인인증기관이 인증업무를 휴지·폐지할 경우에는 미리 신고를 하게 하고 휴지하는 경우에는 그 기간도 한정할 필요가 있다. 그리고 나아가, 인증업무를 폐지하는 경우에는 당해 공인인증기관이 발행한 전자증명서에 관한 기록을 다른 공인인증기관에 인수하도록 하는 등의 조치가 필요하다고 할 것이다.

---

38) 電子取引法制に關する研究會報告書, 30쪽.

현행법은 공인인증기관이 인증업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일전까지 이를 가입자에게 통보하고 정보통신부장관에게 신고하여야 하며, 이 경우 휴지기간은 6월을 초과할 수 없도록 되어 있다(법 제10조 제1항). 역시 공인인증기관이 인증업무를 폐지하고자 하는 때에도 폐지하고자 하는 날의 60일전까지 이를 가입자에게 통보하고 정보통신부장관에게 신고하여야 한다(법 제10조 제2항). 이 때에 공인인증기관은 가입자의 인증서와 인증서의 효력정지 및 폐지에 관한 기록(“가입자인증서등”)을 다른 공인인증기관에게 인계하여야 한다(법 제10조 제3항 본문). 다만, 부득이한 사유로 인하여 가입자인증서등을 인계할 수 없는 경우에는 정보통신부장관이 신고를 받아 보호센터에 대하여 당해 공인인증기관의 가입자인증서 등을 인수하도록 명할 수 있다(법 제10조 제3항 단서 및 제4항).

한편 공인인증기관이 다른 공인인증기관의 인증업무를 양수하거나 다른 공인인증기관인 법인을 합병하고자 하는 경우에는 정보통신부령이 정하는 바에 따라 정보통신부장관에게 신고하여야 한다(법 제9조 제1항). 그리고 다른 공인인증기관으로부터 인증업무를 양수한 공인인증기관 또는 합병한 경우의 합병후 존속하는 법인이나 합병으로 설립된 법인은 종전의 공인인증기관의 지위를 승계한다(법 제9조 제2항).

⑷ 기록보존의무

공인인증기관이 발행하는 전자서명서의 내용, 인증서의 효력의 소멸, 효력의 정지 및 인증서의 폐지 등의 사항에 대하여 다툼이 있을 수 있기 때문에 이와 관련된 기록을 일정한 기간 보존할 필요가 있다. 현행법은 공인인증기관은 가입자인증서 등을 당해 인증서의 효력이 소멸된 날로부터 10년 동안 보관하도록 규정하고 있다(법 제22조 제2항).

4) 손해배상의무

전자서명법 제26조는, ‘공인인증기관은 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상

하여야 한다. 다만, 그 손해가 불가항력이나 이용자의 고의 또는 과실로 인하여 발생한 경우에는 그 배상책임이 경감 또는 면제된다.'라고 규정하고 있다. 공인인증기관이 인증업무와 관련한 불법행위에 의하여 가입자 등에게 손해를 입힌 경우 손해를 배상하여야 하는 것은 이 조문을 기다리지 않아도 당연한 일이다. 이 조문의 의의는 오히려 단서조항에 있다고 할 것이다. 즉, 불가항력 등의 경우 공인인증기관이 책임을 면할 수 있도록 하고 있기 때문이다.

제 3 절 한국정보보호센터

1. 한국정보보호센터의 법적 성격

인증업무를 규율하는 전자서명법의 핵심을 이루는 것은 앞서 살펴본 공인인증기관에 관한 규정이지만 이에 못지 않게 중요한 역할을 하고 있는 것이 보호센터이다. 보호센터는 정보보호시책을 효율적으로 추진하기 위하여 설립된 기관이다(정보화촉진기본법 제14조의 2). 정보화촉진기본법 제14조의 2는, 정부는 “정보의 안전한 유통을 위하여 정보보호에 필요한 시책”을 강구함과 동시에 “암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치”를 강구하도록 규정하고 있다. 보호센터는 이 규정에 의거하여 설립된 것이다.

보호센터는 전자서명법 제8조(공인인증기관의 업무수행), 제10조(인증업무의 휴지·폐지 등), 제12조(인증업무의 정지 및 지정취소 등) 및 제25조(전자서명인증관리업무)의 규정에 의하여 전자서명 인증관리체계에서 최상위인증기관의 임무와 역할을 수행한다. 그런데 이 규정 중에서 보호센터의 중심적인 기능은 전자서명법 제25조에 근거해서 수행된다. 먼저, 전자서명법 제25조 제1항의 규정에 의하면 보호센터의 기능은, ①전자서명의 안전하고 신뢰성 있는 이용환경조성, ②공인인증기관의 전자서명검증키에 대한 인증, 그리고 ③전자서명인증기술의 개발 및 보급 기타 전자서명인증과 관련된 업무의 수행이다. 그러나 여기서 중요한 것은 ②와 ③, 즉 공인인증기관의 공인인증기관으로서의 기능(이른바 최상위인증기관의 기

능)과 전자서명인증기술의 개발 및 보급이라고 할 수 있다. 이 때에 보호센터의 최상위인증기관으로서의 기능에 대한 전자서명법의 규정은 매우 간단하다. 즉, 먼저 제8조에서 공인인증기관이 인증업무를 개시하기 전에 보호센터로부터 전자서명검증키를 인증받아 이 전자서명검증키에 합치하는 전자서명생성키를 이용하여 인증업무를 수행하여야 한다고 규정하고 있다. 그리고 공인인증기관이 인증업무를 폐지한 경우 다른 공인인증기관이 가입자인증서 등을 인계할 수 없는 경우 보호센터가 인수할 수 있다는 규정(법 제10조 제3, 4, 5항), 인증서효력에 관한 공시(법 제16조 제3항), 그리고 공인인증기관의 전자서명생성키의 분실·훼손 또는 도난·유출에 대한 조치(법 제21조 제3, 4, 5항) 등이다. 그러나 보호센터의 최상위인증기관으로서의 기능에 대한 가장 포괄적이고 핵심적인 조항은 전자서명법 제25조 제2항이다. 즉, 이 조항은 '제3조, 제6조, 제7조, 제15조 내지 제19조, 제22조 및 제28조의 규정은 제1항의 규정에 의한 공인인증기관의 전자서명검증키에 대한 인증에 관하여 이를 준용한다. 이 경우 "공인인증기관"은 "보호센터"로, "가입자"는 "공인인증기관"으로 본다.'라고 규정하고 있다. 즉, 다시 말하면, 보호센터와 공인인증기관과의 법률관계를 공인인증기관과 가입자와의 그것에 준해서 규율한다는 이야기이다.

위에서 살펴본 것처럼 보호센터의 전자서명법상의 기능은 크게 나누어 최상위 인증기관으로서의 기능과 전자서명인증기술의 개발 및 보급 등의 기능을 한다고 말할 수 있다. 그러나 보호센터의 실제로 수행하고 있는 기능은 여기에 그치지 않는다. 예를 들면, 전자서명법상의 규정에 의하면 정보통신부장관의 권한에 속하는 권한인 공인인증기관의 지정을 위한 실질심사 등(전자서명법 제4조 등)의 권한을 법률의 위임도 없이 보호센터가 이른바 행정규칙인 인증업무준칙(이하 '업무준칙'이라 한다)에 근거하여 행사하고 있는 것이다(한국정보보호센터 인증업무준칙 1.5.4). 이처럼 보호센터의 활동을 둘러싸고 법적으로 적지 않은 문제점이 있음을 알 수 있다. 이하에서는 이 점에 대해서 살펴보기로 한다. 논의의 순서로서는 먼저 보호센터의 행정조직법상의 법적 성격을 살펴본 후, 보호센터의 업무준칙을 소재로 하여 법적인 문제점을 파악해 보기로 한다.

2. 한국정보보호센터의 정부조직법상의 위치

보호센터는 정보통신부에 속해있는 행정기관인데 먼저 정부조직법상의 어떠한 규정에 근거해서 설치되었는가를 살펴보기로 하자. 정부조직법상의 주된 국가행정조직은 제2조 제2항의 부(部)·처(處)·청(廳)인 중앙행정기관을 중심으로[39] 제5조의 합의제행정기관[40], 제4조의 부속기관[41], 그리고 제3조의 특별지방행정기관[42]으로 이루어진다. 이 중에서 보호센터는 중앙행정기관은 아니기 때문에 자연히 나머지 세 종류의 기관 중 어느 하나에 속한다고 볼 수 있다. 그리고 보호센터는 행정위원회와 같은 합의제행정기관이나 특별지방행정기관이라고 할 수 없기 때문에 결국 제4조의 부속기관에 속한다고 볼 수밖에 없을 것이다.

그런데 정부조직법 제4조의 부속기관은 이른바 행정관청이 아니기 때문에 법률에 의해서 권한이 위임되지 않는 한 스스로 의사를 결정하여 외부에 의사표시를 할 수 없다. 즉, 보호센터는 법률에 의해서 정보통신부장관의 권한이 위임되지 않는 한 외부에 대하여 의사표시를 할 수 없다. 그러나 후술하는 것처럼 보호센터는 충분한 위임규정 없이 많은 권한을 행사하고 있다. 이하에서 이 점에 대하여 살펴보기로 하자.

3. 한국정보보호센터의 권한행사를 둘러싼 법적 문제점

그러면 여기서 먼저 보호센터가 어떠한 법적 근거에 의해서 업무를 수행하고 있는지 살펴보기로 하자.

---

39) 부, 처 및 청 이외에도 다른 법률에 특별한 규정을 두어 중앙행정기관을 설치 할 수 있다(정부조직법 제2조 제2항).

40) 합의제행정기관은 소관사무의 일부를 독립하여 수행할 필요가 있는 때에 법률이 정하는 바에 의하여 설치되는 행정위원회 등을 말한다.

41) 소관사무의 범위 안에서 필요한 경우 대통령령에 의하여 설치되는 시험연구기관, 교육훈련기관, 문화기관, 의료기관, 제조기관 및 자문기관 등을 말한다.

42) 중앙행정기관이 소관사무를 수행하는 과정에서 지역적인 편의성을 도모하기 위하여 법률 또는 대통령령에 의하여 일정한 지역의 중앙행정기관의 사무를 처리하기 위해서 설치되는 행정기관이다.

전자서명 및 인증과 관련하여 전자서명법상에 규정된 보호센터의 권한은 전자서명법 제8조에서 규정하고 있는 공인인증기관의 전자서명검증키를 인증할 수 있는 권한뿐이다. 전자서명법 제25조에서 위의 권한 이외에 전자서명인증기술의 개발 및 보급 기타 전자서명인증과 관련된 업무를 수행한다고 규정하고 있는데 이것은 너무 포괄적이어서 이 규정을 가지고 권한의 위임이 있었다고는 볼 수 없을 것이다. 그리고 전자서명법시행령이나 시행규칙에도 위와 같은 위임에 관한 사항은 존재하지 않는다.

그런데 문제는 보호센터가 자신이 정한 이른바 '인증업무준칙'에 의거해서 권한을 행사하고 있다는 점이다. 이 인증업무준칙은 전자서명법 제25조 제2항 및 제6조의 규정에 의해서 보호센터가 작성하여 정보통신부장관에게 신고하도록 되어 있다. 그리고 그 내용은 ①인증업무의 종류, ②인증업무의 수행방법 및 절차, ③인증역무의 이용조건 및 이용요금 그리고 ④기타 인증업무의 수행에 관하여 필요한 사항이다(전자서명법 제6조 제1항). 이 때에 정보통신부장관은 인증업무준칙의 내용이 인증업무의 안전과 신뢰성의 확보에 지장을 초래하거나 가입자의 이익을 저해할 우려가 있다고 판단하는 경우에는 상당한 기간을 정하여 당해 공인인증기관에게 인증업무준칙의 변경을 명할 수 있다(동 제2항). 이 인증업무준칙은 말 그대로 보호센터가 업무를 수행하는 지침에 불과한 것으로 새로운 권한을 창설할 수 없다.

그러나 실제로 보호센터의 인증업무준칙은 위의 규정을 훨씬 뛰어 넘어서 많은 새로운 권한을 규정하고 있다. 이하에서 주요한 것을 살펴보기로 하자.

1) 적용범위 및 인증서정책

업무준칙은 적용범위에 대하여 '보호센터의 전자서명 인증업무에 관하여 전자서명법, 동법시행령 및 시행규칙에서 정한 것을 제외하고는 이 인증업무준칙이 정하는 바에 의한다'(업무준칙 1.2)라고 규정하고 있다. 이 것은 마치 업무준칙이 전자서명법 등과 같은 위치에 있는 것처럼 규정하고 있는 것으로 문제라고 하지 않을 수 없다. 즉, 업무준칙은 이른바 법규가 아니기 때문에 전자서명법 등을 대신하여 상대방의 권리·의무를 규율하는 내

용을 규정할 수 없다.

인증서정책의 경우 전자서명법 제16조 제2항의 경우, 즉 공인인증기관이 인증업무를 휴지 또는 폐지하였거나 인증업무가 정지된 공인인증기관이 발급한 인증서의 효력의 정지는 정보통신부장관의 권한이기 때문에 이것을 보호센터의 권한으로 규정한 업무준칙 1.3의 규정도 검토되어야 할 것이다.

2) 전자서명생성키 및 알고리즘의 취약성에 대한 조치

업무준칙 2.1.1.3은 '보호센터는 공인인증기관으로부터 전자서명생성키에 대한 분실·훼손 또는 도난·유출, 취약성을 통보 받은 경우 당해 공인인증기관에게 발급한 인증서를 폐지한 후 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 공고한다. 국가기관·지방자치단체가 수행하는 공인인증기관으로부터 전자서명생성키에 대한 분실·훼손 또는 도난·유출, 취약성을 통보 받은 경우에는 지체없이 국가정보원장에게 통보한다.' 라고 규정하고 있다. 그리고 업무준칙 2.1.1.4의 전자서명 알고리즘 취약성에 대한 조치에 대해서도 위와 동일한 사항을 규정하고 있다.

이 경우 공인인증기관의 보호센터에 대한 통지에 대해서는 전자서명법 제21조 제3항에 규정되어 있는 반면 보호센터의 국가정보원장에 대한 통보에 대해서는 법률상의 근거가 없다. 그러나 보호센터의 국가정보원장에의 통보는 권한행사와 관련되는 사항이기 때문에 법률의 근거가 있어야 할 것이다. 따라서 위의 규정은 업무준칙에 규정될 사항이 아니라 전자서명법에 규정되어야 할 사항이라고 생각한다.

3) 공인인증기관지정 관련 실질심사

공인인증기관의 지정은 정보통신부장관에 속하는 권한이다(전자서명법 제4조 제1항). 이 때의 지정요건은 신청자가 인증업무를 안전하고 신뢰성 있게 수행할 수 있는가 하는 점이다(전자서명법 제4조 제1항). 그리고 신청자가 이러한 능력을 갖추고 있는가를 알아보기 위하여 신청자의 기술능력·재정능력·시설 및 장비 기타 필요한 사항을 구체적으로 심사하게 된다. 이것을 이른바 실질심사라고 한다. 그런데 이러한 실질심사는 기술적

인 면 등 전문성이 요구되기 때문에 행정청은 이러한 업무를 일정한 요건을 갖춘 제3자에게 위탁하여 처리하기도 한다.[43] 그러나 이러한 실질심사는 권한행사의 주요한 부분을 이루기 때문에 반드시 법률에 근거가 있어야 한다. 그런데 전자서명법상에는 이러한 내용이 규정되어 있지 않음에도 불구하고, 업무준칙 2.1.2.1의 규정을 보면 보호센터가 이 업무를 처리하고 있음을 알 수 있다.

그러나 이 실질심사에 관한 업무의 위탁처리에 관해서도 역시 전자서명법상에 그 근거를 명시하여야 할 것이다.

4) 보호센터의 책임

인증업무와 관련하여 인증기관에게 어느 정도까지 책임을 인정할 것인가는 전자인증제도를 구성하는 데 있어서 매우 중요한 사항의 하나라는 사실은 이미 앞에서 언급한 바 있다. 이 점에 대해서 공인인증기관에 대해서는 앞서 살펴본 것처럼 전자서명법 제26조에 규정을 두고 있는데 보호센터의 배상책임에 대해서는 그 규정이 없다(보호센터도 인증기관으로서의 역할도 하고 있기 때문에 배상책임을 져야할 경우가 있다). 그 대신에 업무준칙 2.2.2는 '보호센터는 전자서명법, 동법 시행령 및 시행규칙 또는 이 인증업무준칙의 각 규정에서 정한 사항 이외의 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리불능으로 인한 손해에 대하여는 책임을 지지 않는다.' 라는 면책사항을 규정하고 있다. 그러나 두말할 필요도 없이 배상책임은 한 나라의 법체계의 고유한 문제로서 법규가 아닌 업무준칙과 같은 규정으로 결정될 사항은 아니라고 할 것이다. 이 규정 역시 전자서명법에 근거를 두어야 한다.

5) 재판관할 및 분쟁조정

업무준칙 2.3.2는 재판 관할에 대하여, '보호센터와 공인인증기관 또는 신뢰당사자와의 인증업무와 관련한 분쟁해결을 위하여 서울지방법원을 관

43) 일본의 『전자서명 및 인증업무에 관한 법률』은 인정인증사업자(우리 나라의 공인인증기관에 해당)의 인정에 있어서 실질심사의 전부 또는 일부에 대해서 주무대신의 지정을 받은 지정조사기관이 행할 수 있다고 규정하고 있다(동법 제17조).

할 법원으로 정한다.'라고 규정하고 있다. 그러나 재판관할은 법률에 규정해야 할 사항으로 이 업무준칙의 규정은 효력이 없다고 할 것이다.

그리고 업무준칙 2.3.3은 분쟁 조정에 대하여 다음과 같이 규정하고 있다.

정보통신부장관은 보호센터와 공인인증기관 또는 신뢰당사자 간에 분쟁이 발생한 경우에 분쟁당사자의 요청에 따라 보호센터와 공인인증기관에게 관련 자료를 제출하도록 요구하고 전자서명법 및 인증업무준칙의 준수 여부 등을 조사하여 조정안을 제시함으로써 합의에 이르도록 유도하고 시정조치를 명할 수 있다.

재판 이외의 분쟁해결에 있어서도 그 과정이나 결과가 상대방에게 법적인 영향을 미치는 경우에는 역시 법률상의 근거가 있어야 한다. 그런데 위의 분쟁조정에 관한 내용은 관련자료의 제출, 전자서명법 및 인증업무준칙의 준수 여부 등의 조사, 조정안의 제시 그리고 시정조치를 명하고 있다. 따라서, 이 분쟁조정에 관한 사항도 업무준칙에 규정될 사항이 아니기 때문에 전자서명법에 규정되어야 할 것이다.

6) 보호센터의 인증기관으로서의 기능과 규제조항

보호센터는 공인인증기관의 전자서명검증키를 인증하는 상위 인증기관으로서 역할도 수행한다(전자서명법 제25조, 제8조 등). 그리고 전자서명법은 보호센터의 공인인증기관에 대한 인증업무와 관련하여 별도의 규정을 두지 않고 공인인증기관의 이용자에 대한 규정 중에서 몇 개의 조문을 준용하도록 하는데 그치고 있다(동법 제25조 제2항). 이 때에 준용되고 있는 사항은 전자서명법 제3조(전자서명의 효력), 제6조(인증업무준칙), 제7조(인증역무의 제공 등), 제15조(인증서의 발급 등), 제16조(인증서의 효력), 제17조(인증서의 효력정지 등), 제18조(인증서의 폐지), 제19조(인증관리체계의 운영), 제22조(인증업무에 관한 기록의 관리) 및 제28조(요금부과)이다. 그러나 공인인증기관과 가입자의 관계 그리고 보호센터와 공인인증기관의 관계가 서로 다르기 때문에 과연 위의 준용규정이 그대로 타당한지에 대해서는 검토를 요한다고 할 것이다. 특히 제3조의 전자서명의 효력에 관한 규정은 공인인증기관의 이용자에 대한 인증의 기능과 보호

센터의 공인인증기관에 대한 인증의 기능은 다르다. 즉, 전자의 경우에는 거래상의 상대방 및 거래내용의 동일성을 확인하려는 목적으로 인증이 행해지는 반면, 후자의 경우에는 공인인증기관의 인증의 신뢰성확보를 위한 목적으로 인증이 행해지기 때문이다.

제 4 절 공인인증기관에 대한 국가의 관여

정보통신부장관은 인증관리체계에 관한 정책수립과 함께 앞서 살펴본 공인인증기관의 의무가 당해 기관에 의해서 이행되지 않을 경우, 그에 대한 시정명령을 내릴 수 있고(법 제11조), 이 시정명령에 대한 불이행을 포함하여 일정한 경우에 인증업무의 정지 및 취소를 할 수 있다(법 제12조). 이 이외에도 과징금의 부과(법 제14조), 벌칙(법 제6장) 등에 의해서 공인인증기관의 업무의 적정성을 담보하고 있다. 이하 차례로 살펴보기로 한다.

1. 전자서명 인증관리체계에 관한 정책수립

정보통신부장관은 전자거래법 제20조(전자거래촉진계획의 수립·시행) 제2항 및 제1항 제6호의 규정에 의하여 전자서명, 인증, 암호화 등 전자거래의 안전성 및 신뢰성의 보호에 관한 사항에 대하여 부문계획을 수립하고 주요정책의 수립과 그 집행에 있어서 이를 고려하도록 되어 있다. 정보통신부장관은 전자문서의 안전성과 신뢰성을 확보에 있어서 가장 중요한 사항인 '인증'에 관하여 종합적인 정책을 수립하고 시행하는 주무관청인 것이다.

2. 시정명령

정보통신부장관은 공인인증기관의 법령상의 의무불이행에 대하여 빠짐없이 시정명령을 내릴 수 있다. 그러나 여기서 문제가 되는 것은 '공인인증기관의 업무수행방법이 부적합하여 전자서명의 안전과 신뢰성 확보에 지장을 줄 우려가 있는 경우'라고 규정하고 있는 법 제11조 제1호의 규정이다. 이 규정은 내용이 너무 추상적으로 되어 있어서 상대방의 권리를 침해할 염려가 크다고 할 것이다. 검토되어야 할 사항이다.

3. 인증업무의 정지 및 지정취소 등

정보통신부장관은 공인인증기관이 다음 각 호의 1에 해당하는 경우에는 6월이내의 기간을 정하여 인증업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 및 제2호의 경우에는 지정을 취소하여야 한다.

1. 사위 기타 부정한 방법으로 제4조의 규정에 의한 지정을 받은 경우
2. 인증업무의 정지명령을 받은 자가 그 명령에 위반하여 인증업무를 정지하지 아니한 경우
3. 제4조의 규정에 의한 지정을 받은 날부터 6월이내에 인증업무를 개시하지 아니하거나 6월이상 계속하여 인증업무를 휴지한 경우
4. 제6조제2항의 규정에 의한 인증업무준칙 변경명령에 위반한 경우
5. 제11조의 규정에 의한 시정명령을 정당한 사유 없이 이행하지 아니한 경우

4. 행정조사

행정조사는 감독기관이 공인인증기관이 인증업무를 안전하게 수행하고 있는지의 여부를 확인하고 또 의무이행확보를 위한 정보를 수집하기 위하여 필수적인 사항이다. 전자서명법은 행정조사에 대하여 다음과 같이 규정하고 있다.

제14조 (검사 등) ①정보통신부장관은 인증업무의 안전과 신뢰성 확보 및 가입자의 보호 등을 위하여 필요한 경우에는 공인인증기관에 대하여 자료를 제출하게 할 수 있으며, 관계 공무원으로 하여금 공인인증기관의 사무실·사업장 기타 필요한 장소에 출입하여 인증관리체계·장부·서류 기타 물건을 검사하게 할 수 있다.

②제1항의 규정에 의하여 출입·검사를 하는 공무원은 그 권한을 나타내는 증표를 관계인에게 내보여야 한다.

5. 의무이행확보수단

1) 과징금

행정상의 의무이행확보의 수단 중에서 상대방에게 금전적인 의무를 과하는 수법으로는 행정형벌인 벌금, 과료, 행정질서벌인 과태료, 가산세 그리고 과징금을 들 수 있다. 벌금과 과료는 상대방의 위법행위가 사회적 법익을 침해하는 정도에 이른 경우에 과해지는 금전적 제재이며, 과태료는 신고 등의 의무를 게을리 한 경우와 같이 그 위반행위가 사회적 법익의 침해에는 이르지 아니하고 경미한 정도에 그친 경우에 과해지는 금전적 제재이다. 그리고 가산세는 납세의무자가 납세신고, 납부 등의 법률상의 의무를 이행하지 않은 경우에 부과된다.

그에 반해서 과징금은 경제적 이득을 박탈하는 수법으로 이것은 두 가지 유형으로 나누어 볼 수 있다. 첫째로는 법을 위반하여 과다하게 이득을 취한 경우에 거기에 상응한 액수를 몰수하여 국고에 귀속시키는 방법이다. 독점규제 및 공정거래에 관한 법률 제22조의 부당한 공동행위에 의해서 부당이득을 취한 경우에 부과하는 경우가 그 예이다. 또 한 가지는 경제적인 동기에서 범한 범죄에 대한 것으로 그 행위로 인하여 취득한 이득을 몰수하는 경우이다. 예를 들면, 공해방지시설을 설치해야 함에도 불구하고 이를 설치하지 않거나 설치하였다 하더라도 가동을 하지 않는 경우이다. 대기환경보전법 제19조, 수질환경보전법 제20조, 제20조의 2, 그리고 구 자동차운수사업법 제31조의 2 등이 그것이다.

그러나 우리 나라의 법제에서는 이 과징금제도가 변형된 형태로 이용되고 있다. 즉, 상대방의 위법행위가 원래는 허가취소나 영업정지 등의 처분에 해당하지만 이에 갈음하여 과징금을 부과하는 것이 그 예이다. 전자서명법상의 과징금제도도 바로 이 유형에 속한다. 전자서명법 제13조는 '정보통신부장관은 제12조제1항 각 호의 1에 해당하는 경우로서 그 업무정지가 가입자 등에게 심한 불편을 주거나 기타 공익을 해할 우려가 있는 때에는 그 업무정지처분에 갈음하여 2천만원 이하의 과징금을 부과할 수 있다.'라고 규정하고 있다. 그러나 이와 같은 변형된 형태의 과징금제도의 운

영은 다음과 같은 두 가지 문제점을 안고 있다고 할 수 있다.

첫째로, 영업허가취소나 영업정지의 제재조치가 어떻게 금전적인 제재로 대체될 수 있는가 하는 점을 반드시 논리적으로 설명하기 어렵다는 점이다. 원래 영업허가는, 다시 설명할 것도 없지만, 사회의 안전과 질서의 유지를 위하여 일정한 행위에 대하여 일반적으로 금지를 하고, 일정한 요건을 갖춘 자에 한해서 이를 허가해 주는 규제제도 이다. 이렇게 허가를 받은 후에도 그 요건을 결하게 되면 다시 허가의 취소나 영업정지처분을 하게 되는 것이다. 그런데 이 경우 이들 허가취소나 영업정지를 대신한 금전적인 제재에 의해서 이러한 결여된 요건이 충족 될 수 있는가? 이점은 상대방이 위반한 내용이 무엇인지에 따라 그 결과가 달라질 것이다.

먼저 상대방의 위반한 내용이 단순히 영업방식 내지 행위양식이 문제가 된 경우에는 금전적 제재에 의해서도 그 요건이 충족되는 경우가 있을 것이다. 왜냐 하면 상대방이 그 영업방식이나 행위양식을 바꾸거나 중지하기만 하면 그 요건이 충족될 수도 있기 때문이다. 예를 들면 식품접객업소에서 식품위생법에 의해서 금지된 소재로 식품을 제조하여 판매한 경우 이에 대해서 영업허가취소나 영업정지처분 대신에 금전적 제재수단을 사용하여도 일정한 효과를 거둘 수 있을 것이다(식품위생법 제65조, 제4조 등 참조).

그러나 상대방의 위반 내용이 영업시스템 그 자체나 설비 등, 구조적인 부분과 관련 된 경우에는 단순히 금전적인 제재수단을 사용한다고 하여도 그 결여된 요건이 충족된다고는 볼 수 없을 것이다. 만약 이 경우 영업허가의 취소나 영업정지를 대신하여 금전적인 수단을 사용할 경우에는 상대방은 위반내용을 시정하지 않은 채 영업을 계속하는 위험성마저 존재한다. 여기서 전자서명법상의 규정을 예로 들어 살펴보기로 하자.

전자서명법 제13조의 규정에 의하여 공인인증기관의 인증업무의 정지 대신에 과징금을 부과할 수 있는 사항은 동법 제12조 제1항 제3, 4, 5호의 경우이다. 각 사항에 대하여 차례로 살펴보기로 하자.

먼저 제3호는 '공인인증기관이 지정을 받은 날부터 6월이내에 인증업무를 개시하지 아니하거나 6월 이상 계속하여 인증업무를 휴지한 경우'이다. 이 경우 어떠한 제재를 가하는 것이 적합한가를 고려하기 위해서는 먼저 왜 인증업무를 개시하지 않거나 휴지하고 있는가 그 원인을 조사해보아야

할 것이다. 공인인증기관이 인증업무를 개시하지 않거나 휴지한 데에는 자금이나 기술 인력 등 인증기관을 운영하는데 결정적인 요소가 아직 갖추어지지 않았기 때문일 가능성이 높다. 왜냐 하면, 공인인증기관을 운영하는 데에는 막대한 예산과 기회비용이 필요하기 때문에 위와 같은 이유가 없음에도 불구하고 인증업무를 개시하지 않거나 인증업무를 휴지하는 업자는 없을 것이기 때문이다. 이것은 공인인증기관으로 인증받기 위한 기술능력, 재정능력, 시설 및 장비 등의 요건이 얼마나 무겁게 되어있는가 하는 점을 상기하면 쉽게 납득할 수 있을 것이다(전자서명법 제4조, 동시행령 제3조 등 참조). 따라서 위와 같은 요건이 갖추어지지 않은 상태에서 단지 금전적인 제재수단을 가하게 된다면 상대방으로서는 요건이 결여된 상태에서 인증업무를 수행하는 결과를 낳을 수도 있다.

제4호는 전자서명법 제6조제2항의 규정에 의한 인증업무준칙 변경명령에 위반한 경우, 인증업무의 정지 대신에 과징금을 부과하는 경우이다. 여기서 먼저 인증업무준칙에 포함된 내용은 ①인증업무의 종류, ②인증업무의 수행방법 및 절차, ③인증역무의 이용조건 및 이용요금, 그리고 ④기타 인증업무의 수행에 관하여 필요한 사항이다. 이들의 경우에는 비교적 금전적 제재에 의해서 시정하기에 용이한 사항이 포함되어 있다고 할 수 있다. 그러나 ②와 ④의 경우 인증업무의 구조적 문제와 관련되어 있을 가능성을 배제할 수 없기 때문에 이들에 대한 제재수단으로서 과징금을 부과하는 것은 반드시 합리적이라고 할 수 없다.

제5호는 전자서명법 제11조규정에 의한 시정명령을 정당한 사유 없이 이행하지 아니한 경우이다. 그런데 전자서명법 제11조에 해당하는 사항은 자그마치 12항목에 이르고 있다. 이 중에서도 특히 금전적 제재수단에 의할 경우 문제가 되는 사안, 즉 인증업무의 구조적인 문제에 해당하는 것으로서 들 수 있는 것은 다음과 같다.

제11조(시정명령)

1. 공인인증기관의 업무수행방법이 부적합하여 전자서명의 안전과 신뢰성 확보에 지장을 줄 우려가 있는 경우
2. 공인인증기관으로 지정을 받은 후 제4조제3항의 규정에 의하여 공인

인증기관이 갖추어야 할 사항을 갖추지 아니한 경우

7. 제10조의 규정에 위반하여 인증업무휴지 또는 폐지의 통보나 신고를 하지 아니하거나 인증업무폐지시 가입자인증서등을 인계하지 아니한 경우
8. 제12조제2항의 규정에 위반하여 지정이 취소된 공인인증기관이 가입자인증서등을 인계하지 아니하거나 신고하지 아니한 경우
11. 제18조의 규정에 위반하여 인증서를 폐지하지 아니하거나 그 사실을 확인할 수 있는 조치를 취하지 아니한 경우

따라서 제5호의 경우에도 인증업무의 정지 대신에 과징금을 부과하는 것은 반드시 논리적으로 설명하기가 어렵다는 것을 알 수 있다.

따라서 위의 경우에는 변형된 과징금을 부과하기보다는 인증업무의 정지 사유에 해당하는 사안을 시정하고 개선하여 그 요건을 갖추게 하는 것이 문제의 핵심으로, 앞서 언급한 것처럼, 만일 이것을 변형된 과징금으로 대체하게 된다면 요건이 미비된 상태에서 인증업무를 계속하게 되는 결과를 낳고 말 것이다.

변형된 과징금제도의 또 하나의 문제점은 기존의 제도와의 정합성의 결여에서 유래한다. 즉 변형된 과징금제도가 위에서 살펴본 기존의 금전적 제재에 의한 행정법상의 의무이행확보제도와 어떠한 관계에 있는가하는 점이다. 즉, 이 변형된 과징금제도는 전혀 새로운 금전적 제재수단으로서 기존의 제도로서 포섭할 수 없는 새로운 제도인가 하는 점이다. 그러나 반드시 그렇다고 할 수 없다. 이 변형된 과징금제도는 어느 쪽이냐 하면 행정벌에 속하는 금전적 제재수단, 즉, 벌금, 과료 또는 과태료에 속하는 어느 것이라고 해도 무방할 것이다. 따라서 기존의 제도로 충분히 포섭할 수 있는 사안을 전혀 별개의 제도로 편입시키고 있는 오류를 범하고 있다고 할 수 있다. 이렇게 되면 제도 전체에 혼란을 가져와 당해 제도가 의도했던 목표를 달성하지 못하는 결과를 낳게 될 것이다.

2) 행정벌

행정벌이란 행정상의 의무위반에 대하여 벌(罰)로서 과해지는 제재이다. 행정벌에는 형벌과 질서벌의 두 가지가 있다. 전자는 사인(私人)의 행정상

의 의무위반의 정도가 중대하여 사회적 법익을 침해하는 정도에 이른 경우에 형법 제41조에 규정된 사형에서 몰수에 이르는 9가지의 형(刑)의 종류가 과해지는 벌이다. 그리고 후자는 이른바 과태료로서 신고의무의 위반 등과 같이 의무위반의 정도가 경미한 경우에 과해지는 벌이다.

전자인증제도에 있어서 어느 정도의 규제를 가할 것인가 하는 점은 인증제도에 있어서 채용하고 있는 기술, 인증의 효과 등에 의해서 결정되어야 한다는 점은 이미 앞서 언급한 바와 같다. 의무이행확보수단의 하나인 행정벌도 규제수단의 중요한 부분을 차지하고 있다는 점에서 이러한 기준의 적용을 받아야 한다는 점은 쉽게 이해할 수 있을 것이다.

앞서 살펴본 것처럼 전자서명법에서는 서명기술에 있어서도 디지털서명 방식으로 특정을 하고 있고 인증의 효과에 있어서도 형식적 증거능력 뿐만 아니라 본인과 내용의 무변경성의 추정효과도 인정하는 등 폭넓은 법적 효과를 인정하고 있다. 따라서 규제수단도 이에 상응할 정도로 비교적 엄격한 행정벌이 허용된다고 할 것이다. 이하에서 전자서명법상에 규정된 행정벌에 대해서 살펴보기로 하자.

(1) 행정형벌

행정형벌은 양형으로 분류해보면 3년이하의 징역 또는 3천만원 이하의 벌금에 처하는 경우와 1년이하의 징역 또는 1천만원 이하의 벌금에 처하는 경우의 두 카테고리로 나눌 수 있다.

먼저 전자에 속하는 사항은 다음과 같다.

전자서명법 제21조 제2항에 의하면 '공인인증기관은 가입자의 신청이 있는 경우외에는 가입자의 전자서명생성키를 보관하여서는 아니 되며, 가입자의 신청에 의하여 그의 전자서명생성키를 보관하는 경우에도 당해 가입자의 승낙 없이 이를 이용하거나 유출하여서는 아니 된다'라고 규정하고 있다. 디지털서명에 있어서 안전성의 유지라는 측면에서 볼 때 가입자의 전자서명생성키의 관리는 핵심적인 사항에 속한다고 할 것이다. 이러한 의미에서 본 규정의 위반에 대해서 무거운 형벌로서 규율을 하고 있다고 본다(전자서명법 제31조 제1호).

두 번째로 전자서명법 제23조 제1항의 위반, 즉 타인의 전자서명생성키를 도용 또는 누설한 경우에도 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하고 있다(전자서명법 제31조 제2호).

그리고 마지막으로 타인의 명의로 인증서를 발급받거나 발급받도록 한 경우에도 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 하고 있다(전자서명법 제31조 제2호). 전자서명법에서 인정하고 있는 인증의 효력의 핵심중의 하나가 본인의 동일성의 추정효라는 점을 고려할 경우, 처음부터 타인의 명의로 인증서를 발급받게 되면 인증제도의 근간이 흔들리기 때문에 엄격한 제재가 가해질 필요가 있을 것이다.

후자 즉, 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하는 경우는 다음과 같다.

먼저 공인인증기관과 보호센터는 가입자의 인증서와 인증업무에 관한 기록을, 당해 인증서의 효력이 소멸된 날로부터 10년간, 안전하게 보관·관리하여야 할 의무가 있다(전자서명법 제22조 제1, 2항, 제25조제2항). 이것은 전자인증을 둘러싼 분쟁이 발생했을 경우에 대비한 것으로 전자서명을 종래의 서면이나 서명·날인과 동일하게 취급하는 이른바 '기능적 등가물'로 인정하기 위한 조치이다. 이 규정을 위반하면 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하게 된다(전자서명법 제32조 제1호).

둘째로 개인정보보호에 관한 규정을 위반한 경우이다. 전자서명법 제24조 제2항은 공인인증기관이 본인의 동의 없이 수집된 개인정보를 인증업무외의 목적으로 이용하거나 유출하는 것을 금지하고 있다. 그리고 동조 제4항은 인증업무에 종사하거나 종사하고 있는 자가 직무상 알게된 타인의 정보를 누설해서는 않된다는 직무상 비밀유지의무를 규정하고 있다. 이들 규정을 위반한 자에 대해서도 역시 1년이하의 징역 또는 1천만원 이하의 벌금에 처해지고 있다.

그리고 전자서명법 제33조는 '법인의 대표자나 법인 또는 개인의 대리인·사용인 기타 종업원이 그 법인 또는 개인의 업무에 관하여 제31조 또는 제32조의 위반행위를 한 때에는 행위자를 벌하는 외에 그 법인 또는 개인에 대하여도 각 해당 조의 벌금형을 과한다'라는 양벌규정을 두고 있다.

⑵ 행정질서벌(과태료)

과태료의 액(額)은 500만원으로 되어 있는데 전자서명법에서는 9가지의 경우를 규정하고 있다.

먼저 신고 또는 통보의무 등을 게을리 한 경우이다. 즉, ①동법 제6조의 인증업무준칙의 작성과 변경시 정보통신부장관에의 신고를 하지 않은 경우이다(동법 제34조 제1항 제1호), ②인증업무의 양수 등에관한 신고를 게을리한 경우(동법 제34조 제1항 제3호, 제9조), ③인증업무의 휴지 또는 인증업무의 폐지 사실을 가입자에게 통보하지 아니하거나 정보통신부장관에게 신고하지 아니한 경우, ④인증업무의 휴지·폐지한 경우 공인인증기관은 가입자의 인증서와 인증서의 효력정지 및 폐지에 관한 기록의 인계 및 신고의무를 위반한 경우, 그리고 ⑤전자서명생성키의 분실·훼손 또는 도난·유출시 공인인증기관이 보호센터에 대한 통보의무를 게을리 한 경우(동법 제34조 제1항 제7호)이다.

둘째로 인증역무의 제공의 거부나 가입자 또는 인증역무 이용자를 부당하게 차별한 경우이다(동법 제34조 제1항 제2호). 인증역무는 공익성이 강한 사업으로 역무의 이용계약의 체결이나 계약의 내용 등은 부합계약의 성격을 띠기 때문에 정당한 이유 없이 이를 거부할 수 없을 뿐만 아니라 계약내용에 있어서도 차별을 해서는 안된다.

셋째로 행정조사 등에 관한 규정을 위반한 경우이다. 전자서명법 제14조 제1항은 '정보통신부장관은 인증업무의 안전과 신뢰성 확보 및 가입자의 보호 등을 위하여 필요한 경우에는 공인인증기관에 대하여 자료를 제출하게 할 수 있으며, 관계 공무원으로 하여금 공인인증기관의 사무실·사업장 기타 필요한 장소에 출입하여 인증관리체계·장부·서류 기타 물건을 검사하게 할 수 있다'라고 규정하고 있다. 이 때에 고인인증기관이 자료를 제출하지 아니하거나 허위의 자료를 제출한 자 또는 관계 공무원의 출입·검사를 거부·방해 또는 기피한 경우에는 500만원의 과태료에 처하도록 되어 있다(동법 제34조 제1항 제6호).

마지막으로 개인정보보호에 관한 경우이다. 공인인증기관이 본인의 동의 없이 개인정보를 수집하거나, 가입자의 개인정보열람을 거부 또는 개인정보의 오류를 정정하기 위하여 필요한 조치를 취하지 않은 경우이다(동법 제34조 제1항 제8, 9호).

제 4 장 인증제도에 관한 현행법제

제 5 장 맺음말

사이버공간을 이용한 거래는 꾸준히 증가하여 우리에게 새로운 가능성을 부여하고 있는 것은 사실이다. 그러나 이 공간을 이용한 의사의 교환은 기존의 법과 제도에서 경험하지 못한 것으로 몇 가지 해결하지 않으면 안될 문제를 제시한다.

첫째로 문제가 되는 것은 의사교환을 위하여 제공되는 사이버공간을 제공하고 있는 컴퓨터 네트워크가 안고 있는 리스크이다. 왜냐 하면 미지의 컴퓨터 네트워크상에서 무슨 일이 일어나고 있고 또 일어날 수 있는지를 확인할 수 있는 기술은 현재 확보되어 있지 않기 때문이다. 이러한 리스크를 감소시키기 위한 방법의 하나로 생각해낸 것이 이른바 전자서명이다. 전자서명은 메시지를 일정한 기술을 이용하여 암호화하여 상대방에게 전달함으로써 외부로부터의 침입을 방지하고 전자메시지의 내용의 안전성을 어느 정도 보장할 수 있게 된다. 그러나 컴퓨터 네트워크상의 리스크가 전자서명 그 자체만으로는 해소된다고는 할 수 없다. 전자서명을 이용하여 전자메시지를 발신했다 하더라도 그 발신자가 실재하는 인물인지 또는 설령 발신자가 실재한다고 해도 발신자가 바로 당해 전자메시지의 명의인인지 등의 문제는 여전히 남게된다. 여기서 이러한 문제를 해결하기 위하여 등장한 것이 제3자 기관으로서의 인증기관이다. 인증기관은 사전에 전자메시지의 발신자에 관한 정보를 확인하여(인증), 거래의 상대방에게 미리 전달함으로써 위와 같은 문제점을 어느 정도 해소하는 역할을 한다.

둘째로 문제가 되는 것은 이러한 전자서명・인증에 대해서 실체법상 그리고 증거법상 어떠한 법적 효과를 부여할 것인가의 문제이다. 이것은 기존의 서면이나 서명・날인과 같은 이른바 아날로그의 환경에서 전자서명과 같은 디지털환경으로의 변화에서 발생한다. 이 때에 고려할 사항은 ①아날로그환경과 디지털환경을 어떠한 고리로서 연결할 것인가, ②전자서명에 응용하는 기술을 입법적으로 특정할 것인가, 그리고 ③전자서명・인증에 어떠한 법적 효과를 부여할 것인가 하는 점이다. 그런데 이 세 가지는 서로 유기적인 연관성을 가지며 전자서명을 전제로 한 인증제도의 구성의 기

본이 된다. 즉, 인증제도는 위의 세 가지의 요소를 유기적으로 고려하여 구성되어야 한다. 그리고 인증제도는 전자서명법의 핵심을 이루기 때문에 전자서명법 역시 위와 같은 세 가지 요소를 고려한 인증제도의 내용에 따라서 규정되어야 한다.

위의 세 가지 요소를 염두에 두고서 현행 전자서명법을 살펴보면 다음과 같은 내용으로 되어 있음을 알 수 있다.

첫째로, 전자서명법은 아날로그와 디지털의 연결고리에 관해서는 이른바 기능적 등가물 접근방식을 취하고 있다. 그런데 이 점과 관련하여 한가지 논의해야 할 사항은 전자적 정보를 어떠한 형태로 변환시킨 것을 증거 등으로 삼을 것인가 하는 점이다. 즉, 전자서명한 내용, 즉 전자적 정보는 컴퓨터라는 장치를 전제로 하여 존재하기 때문에 그것을 어떠한 형태로 변환시킬 것인가를 법으로 특정하는 것이 바람직한가 하는 점이다. 우리 나라의 민사소송법은 앞서 살펴본 것처럼 증거법칙에 관하여 자유심증주의를 취하고 있기 때문에 변환형태를 특정하지 않고 상황에 따라서 당해 전자적 정보를 확인하는 방법도 생각해볼 수 있을 것이다. 즉, 다시 말하면 우리 나라의 경우에는 실정법에서 낙성주의와 자유심증주의를 취하고 있기 때문에 특별한 입법조치가 없어도 전자메시지와 전자서명에 의해서 계약이 성립하고 또 당해 전자메시지와 전자서명이 재판상의 증거로 채택되는 데에는 문제가 없다. 다만 본문에서 언급한 것처럼, 행정사무에서와 같이 법률에서 문서나 서명·날인을 요구하고 있거나, 국제적인 정합성, 그리고 거래나 재판상의 편의를 위하여 입법을 할 필요가 있을 것이다. 즉, 우리 나라에서 아날로그를 디지털로 연결하기 위한 입법조치는 제한적인 의미를 가지고 있다는 점이다.

둘째로, 전자서명기술에 있어서는 전자거래기본법에서는 기술의 중립성을, 전자서명법에서는 디지털서명으로 특정하고 있다.[44] 전자서명법에서 디지털서명으로 기술을 특정하고 있는 것은 기술의 중립성의 측면에서 검토의 여지가 있지만 예견가능성이라는 측면에서 보면 필요한 입법조치이기도 하다.

44) 전자서명법의 경우 용어는 전자서명이지만 실제로 공개키방식의 디지털서명기술을 채택하고 있음은 본문에서 살펴본 바와 같다.

마지막으로 전자서명에 대한 법적 효과에 대해서는 가장 문제가 되고 있는 귀속효를 인정하고 있다고 볼 수 있다. 그러나 이러한 귀속효를 인정하기 위해서는 일리노이주법에서 볼 수 있듯이 그에 상응한 실체적, 절차적 규정을 두어야 하는데 전자서명법의 경우 이러한 요건이 결여되어 있다. 시급한 검토가 요청되는 부분이라고 할 수 있다.

위와 같은 세 가지 요소를 전제로 하여 구성된 인증제도는 인증기관과 인증체계, 그리고 국가의 관여가 그 내용의 중심을 이룬다. 이들에 대한 규정에 관하여 고려할 때에 가장 핵심적인 사항은 인증의 법적 효과(명의인의 동일성, 내용의 무변경성, 그리고 귀속효)를 보장하기 위한 이른바 '안전한 전자서명'의 확보이다.

본문에서 살펴본 공인인증기관의 지정에서 업무의 수행 등에 이르기까지 엄격한 규제를 가하는 것도 바로 이 안전한 전자서명을 확보하기 위한 것임은 말할 필요도 없다. 문제는 규제의 내용이다. 즉, 규제가 위의 각 목표를 달성하기에 적합할 정도로 균형 있게 행해지고 있는가 하는 점이다. 이에 대한 판단자료의 하나로 삼을 수 있는 것이 일리노이주의 입법례이다. 이미 앞서 살펴본 것처럼, 동주(同州)의 인정절차가 인증제도에 시사하는 점으로는 다음과 같은 점을 들 수 있다. 첫째로 전자서명과 전자인증에 관한 공중에의 완전하고 충분한 정보공개, 둘째로 전자서명・인증에 응용하는 기술의 보편성과 전문성 그리고 인증절차의 적정성이다. 이 내용에 비추어 볼 때, 현행 전자서명법의 규제의 내용은 공인인증기관 그 자체를 규제하는 외형적인 규제는 매우 강하나 인증기관의 인증절차 등 전자서명과 관련한 실질적인 부분을 규제하는 측면은 매우 약하다는 사실이다. 즉, 전자서명과 인증에 관한 공중에의 정보공개도 관련 당사자에 관한 기본적인 사항의 공개는 어느 정도 이루어지고 있다고 볼 수 인지만, 전자서명・인증 그 자체에 대한 내용은 거의 공개되고 있지 않다. 그리고 전자서명에 이용되고 있는 기술에 있어서도 단지 보호센터가 인증하는 디지털서명방식을 채용한다는 것 이외에는 그 기술이 과연 보편성과 전문성이 있는 것인지의 여부에 대해서도 충분한 정보가 제공되고 있지 않다. 따라서 이러한 점에 대해서도 충분한 검토가 이루어져야 할 것이다.

그리고 현행 전자서명법이 부여하고 있는 전자인증에 대한 본인의 추정효, 그 중에서도 특히 이른바 표현대리와 관련하여 본인의 책임을 한정하는 입법조치가 필요하다고 할 것이다. 즉, 현행법의 경우에는 공인인증기관이 인증한 전자서명이 있기만 하면 본인임이 추정되고 있는데, 이렇게 되면 본인에게 아무런 책임이 없는 경우에도 책임을 져야 할뿐만 아니라, 악의의 상대방까지 보호하는 결과가 되기 때문이다.

그리고 그 이외에도 몇 가지 점을 지적하면 다음과 같다.

먼저 인증체계와 관련하여 전자서명법상의 권한에 대한 규정이 불분명하여 정보통신부장관과 보호센터 사이에 권한행사를 둘러싸고 혼선을 빚을 염려가 있다. 즉 권한행사에 관한 많은 부분이 법적 효력이 없는 보호센터의 인증업무준칙에 근거를 두고 있다는 점이 이것을 단적으로 말해준다. 권한행사의 주체가 누구인가 하는 점은 상대방의 권리에 직접적인 영향을 미치는 사항이기 때문에 반드시 법률에 근거에 의해서 확정되어야만 한다. 나아가 이 점과 관련하여 한 가지 더 덧붙일 사항은 전자인증에 관한 법제정비가 필요하다는 점이다. 전자서명, 전자인증에 대한 현행법상의 규율은 이미 앞서 언급한 바와 같이 전자거래기본법과 전자서명법에 의해서 행해지고 있다. 그러나 본문에서 지적한 것처럼 양법에서 규정하고 있는 전자서명, 전자인증에 대한 법적 효과가 서로 다른 것은 물론 용어의 정의조차 통일되어 있지 않다. 그 이외에도 전자서명에 응용하는 기술에 대한 입장 등에서도 차이를 보이고 있다. 따라서 이러한 양법에 규정되어 있는 내용상의 모순은 정비되어야 할 것이다. 그리고 나아가 입법론적으로도 과연 양자를 별도로 두는 것이 바람직한 것인지 검토의 여지가 있다고 할 것이다.[45]

이어서 공인인증기관의 지정절차규정이 불충분하다는 점이다. 전자서명법, 동법시행령 및 시행규칙에는 공인인증기관의 지정절차에 관하여 간단한 신청절차만을 규정하고 있을 뿐, 어떠한 심사절차를 거쳐서 지정을 하는지의 여부가 매우 불투명하게 되어 있다. 그러나 이러한 절차는 공인인

45) 이렇게 별도의 법률이 존재하게 된 데에는 부처간의 권한의 조정이 쉽지 않다는 점이 작용하고 있을지도 모른다. 참고로 전자거래기본법에 관한 권한은 산업자원부장관이, 전자서명법상의 권한은 정보통신부장관이 행사하고 있다.

증기관의 지정을 신청한 당사자의 권리보호를 위해서 뿐만 아니라 공중을 위해서도 투명하게 규정되어야만 한다.

그리고 의무이행확보수단의 하나인 과징금의 경우 현재 우리 나라에서 변형된 형태로 이용되고 있는데 전자서명법에서도 이것을 그대로 답습하고 있다. 이렇게 되면, 본문에서 지적한 대로, 금전적인 제재수단에 의한 의무이행확보수단의 체계에 혼란을 가져올 뿐만 아니라, 인증기관이 인증업무를 행하기에 부적합한 상태에서 다시 인증업무를 행할 가능성이 있다는 점에서 이것은 논리적으로나 인증업무의 안전성의 확보의 면에서나 문제가 있다고 할 것이다.

마지막으로 구제절차에 관한 점이다. 인증을 둘러싼 분쟁에 대한 구제절차는 전자서명법 제26조의 손해배상에 관한 규정과 정조보호센터의 인증업무준칙에 규정된 재판관할과 분쟁조정에 관한 규정이 전부이다. 그러나, 인증이란 특수한 분야에 대한 구제절차가 위와 같은 간단한 규정으로 충분한지는 검토의 여지가 있다. 더구나 인증업무준칙은 법규가 아니기 때문에 재판관할을 지정한다던가, 분쟁조정 등에 관한 규정을 할 수 없다.

그리고 인증업무는 전문적이며 대량적인 의미를 띠는 경우가 많을 것이므로 여기에 걸맞는 피해자 구제제도를 고려해야 할 것이다. 특히 공인인증기관의 경우 단지 검사 등에 한하는 이른바 지정법인이기 때문에 공인인증기관의 행위는 이른바 권력작용이 아니기 때문에 분쟁시 행정쟁송제도를 이용할 수 없다. 반면에 상위인증기관인 보호센터는 행정기관이기 때문에 당해 기관의 처분에 대해서는 행정쟁송으로 다툴 수 있다. 그러나 이 때에 발생하는 분쟁은 대개 전문적인 기술과 관련이 있기 때문에 특별한 이의신청제도 등을 창설하는 것도 하나의 방법이 될 것이다.

제 5 장 맺음말

<참고문헌>

1. 국내문헌

김은기, 전자인증과 법률문제, 정보법학 제2호(1998.12).

황희철, 전자서명과 법률문제, 정보법학 제2호(1998.12).

소재선, 전자인증의 법적 문제점, 경희법학 제33권 제2호(1998.12).

장경환, 전자서명의 범위와 효력, 경희법학 제33권 제2호(1998.12).

김용섭, 인터넷과 행정법상의 과제, 법제연구 제18호(2000.6).

배대헌, 인터넷과 민법상의 과제, 법제연구 제18호(2000.6).

손진화, 전자서명의 법적 과제, 비교사법 제8호(1998.6).

한웅길, 전자거래와 계약법, 비교사법 제9호(1998.12).

최준선, UNCITRAL 전자상거래모델법과 우리 나라의 전자거래기본법(안) 비교, 비교사법 제9호(1998.12).

전성배, 전자서명인증 정책, 통신정보보호학회지 제9권 제3호(1999.9).

양덕기, 사이버 증권거래와 전자서명 인증서비스체계, 통신정보보호학회지 제9권 제3호(1999.9).

김용준, 백석철, 정종윤, 박정식, 김재중, 전자상거래 인증서비스 체계, 통신정보보호학회지 제9권 제3호(1999.9).

최영철, 오경희, 이재일, 홍기융, 이홍섭, 전자서명 인증관리센터 구축 및 운영, 통신정보보호학회지 제9권 제3호(1999.9).

신용섭, 전자서명 인증관련 주요 정책방향, TTA저널 제63호(1999.6).

배대헌, 인증기관의 손해배상책임에 관한 소론, 인터넷법률 제3호(2000.11).

현대호, 인증기관의 감독과 규제, 인터넷법률 제3호(2000.11).

<참고문헌>

하강헌, 국제전자상거래의 발전과제에 관한 소고, 무역상무연구 제13호 (2000.2).

신홍식, 김창연, 전자상거래 보안과 전자인증, 정보산업 197(1999.6).

이시윤, 신정보판 민사소송법, 박영사(1996).

정영화, 남인석, 전자상거래법, 다산출판사(2000).

배대헌, 전자서명・인터넷 법, 세창출판사(2000).

정상조 엮음, 인터넷과 법률, 현암사(2000).

신일순/김춘아/박민성, 〈연구보고〉 전자서명 및 인증제도, 정보통신정책연구원(1998.12).

한국정보보호센터, 〈보고서〉 전자서명 인증관리센터 운영・관리 방법연구 (1999. 5).

한국전산원, 〈보고서〉 전자문서 이용 활성화의 법적 장애요인 분석 (1998. 6).

2. 일본문헌

内田 貴, 電子商取引と民法, 別冊 NBL NO. 51 “債權法改正の課題と展望”, 商事法務研究會.

内田 貴, 電子商取引と法(4. 完), NBL. No. 603(1996. 10. 15).

内田 貴, 電子認證・電子署名をめぐる法制度整備のあり方(上), NBL. No. 675(1999. 10. 15).

内田 貴, 電子認證・電子署名をめぐる法制度整備のあり方(下), NBL. No. 675(1999. 11. 1).

電子取引法制に關する研究會中間報告書, ジュリストNo.1114(1997. 6. 15).

電子取引法制に關する研究會(制度關係小委員會)報告書, ジュリストNo. 1138 (1998. 7. 15).

〔座談會〕電子取引法制整備の課題, ジュリスト No. 1183(2000. 8. 1・15合併號)

米丸恒治, “私人による行政”, 日本評論社(1999).

信森毅傳, 米國における電子取引法の檢討狀況(1), NBL. No. 663(1999. 4. 15).

〃 , 米國における電子取引法の檢討狀況(2), NBL. No. 665(1999. 5. 15).

〃 , 米國における電子取引法の檢討狀況(3), NBL. No. 669(1999. 7.15).

〃 , 米國における電子取引法の檢討狀況(4・完), NBL. No. 675 (1999. 10. 15).