’전자금융거래법’ 개정법률안 소개 및 개정 필요성

김기창 (고려대학교 법학전문대학원 교수)

1. 지난 10여년 간의 상황

금융위원회는 전자금융거래에 공인인증서 등을 사용하도록 강제해 왔습니다. 공인인증서는 90년대 후반에 각광을 받은 보안기술인 것은 사실이지만, 15년에 지난 요즈음에는 여러 한계가 노출된 낙후된 기술로 평가받습니다.

공인인증서는 액티브엑스 등으로 알려진 '별도 프로그램'을 설치해야 이용 가능한데, 바로 이것이 여러 문제를 불러 일으킵니다. 서비스 제공자(쇼핑몰, 결제서비스 제공자 등)는 고액의 비용을 지불하고 공인인증서 사용에 필요한 서버측 프로그램(server-side solution)을 구입하여 서버에 설치해야 하고, 서비스 이용자(소비자)들은 자신이 이해하지도 못하는 여러 추가 프로그램을 자신의 컴퓨터에 거듭 설치해야 합니다.

이로 인한 문제점은 지난 6월11일에 '인터넷기업협회'가 이번 개정법률안을 공식 지지하면서 발표한 성명서에 다음과 같이 요약 설명되어 있습니다.

> 그동안 액티브엑스를 기반으로 하는 공인인증서 의무사용은 많은 인터넷기업들의 시스템 구축·관리 비용을 증가시켰고, 신규사업자에게는 진입비용을 증대시켜 국내 인터넷산업 전반의 경쟁력 약화를 초래하였다.
> 또한 공인인증서 의무사용은 국내 이용자의 인터넷 이용환경을 불편하게 만들어 외국 서비스 이용을 확대시켰고, 외국 이용자들의 국내 인터넷서비스 이용을 어렵게 만들어 우리 인터넷기업의 글로벌 시장 진출에 걸림돌이 되고 있는 실정이다.

http://opennet.or.kr/wp-content/uploads/2013/06/kinternet-official-statement.pdf
(인터넷기업협회 성명서, 2013.6.11)

2. ’전자금융거래법’ 개정법률안 내용

개정안은 전자금융거래법 제21조 제3항을 아래와 같이 개정하는 것입니다:

> ③금융위원회는 [전자금융기술 및 전자금융업무에 관한] 기준을 정함에 있어서 보안기술과 인증기술의 공정한 경쟁을 저해하거나, 특정기술 또는 서비스의 사용을 강제하여서는 아니된다.

일반적으로, 정부가 특정 기술을 편파적으로 지원하거나, 강요하는 것은 다양한 기술들 간의 공정한 경쟁을 통한 기술 진보와 혁신의 가능성을 박탈하게 되므로 바람직하지 않습니다. 특히, 보안 기술은 나날이 진화하는 공격기법에 신속히 대처해야 하는 분야이고, 실제로 기술 변화 속도도 매우 빠르기 때문에 정부가 개입하여 특정 기술 사용을 강요할 경우, 신 기술의 시장 진입이

늦어지거나 불가능하게 됩니다.

더 심각한 문제는, 정부가 특정 보안 기술을 온 국민에게 강요할 경우, 그 기술이 뚫리면(어떤 보안 기술도 완벽할 수는 없습니다), 온국민이 '일거에' 대규모 피해를 입게 될 위험이 매우 높아진다는 것입니다. 지난 3.20에 발생한 방송사, 금융사의 대규모 보안 사고도 공인인증용 프로그램의 취약점을 악용하여 이루어진 측면도 있습니다.

은행 등 금융회사는 사고거래의 책임을 지도록 이미 법률이 정하고 있습니다(전자금융거래법 제9조). 금융회사가 책임을 져야하므로 보안 기술도 금융회사가 선택하도록 하는 것이 옳습니다. 미국, 영국, 유럽, 일본 등 세계 각국도 사고거래의 책임을 금융회사에 지우는 대신에, 금융회사로 하여금 현재의 기술 수준을 반영한 합리적인 보안 기술을 스스로 선택하도록 하고 있습니다. 이렇게 해야 보안 기술에 대한 활발한 투자와 새로운 기술의 경쟁적 발달이 가능해집니다.

이번 전자금융거래법 개정법률안 통과를 지지하는 전국 주요대학 컴퓨터 공학과, 정보보호학과, 과학기술정책학과, 경영학과 교수 등 300여명이 발표한 지지서명서에도 이점은 다음과 같이 표현되어 있습니다. http://bit.ly/11H4Zsy ("전자금융거래법 개정법률안에 대한 입장"):

> 전자금융거래법 제21조 제3항 개정법률안은 정부 정책의 '기술 중립성'을 확보함으로써 기술 발달과 서비스 품질 향상을 달성하는데 필요한 바람직한 제도 개선 방안이라고 판단하고, 이 법률안이 조속히 통과되기를 희망한다.

3. 한미FTA 제15.4조(전자인증 및 전자서명)

한미FTA 제15.4조는 다음과 같이 규정하고 있습니다:

> 1. 어떠한 당사국도 다음의 전자인증을 위한 법령을 채택하거나 유지할 수 없다.
> 가 . 전자거래의 당사자가 그 거래를 위하여 적절한 인증 방법을 상호 결정하는 것을 금지하는 법령
> 나. [이하 생략]

'공인인증서 등'의 사용을 강제하는 금융위 규제의 근거를 제공하는 현행 전자금융거래법 제21조 제3항은 인증방법의 ‘상호 결정’(거래의 쌍방이 자유롭게 합의하여 결정하는 것)을 보장하는 한미FTA 제15.4조에 어긋나므로, 이미 효력을 상실하였습니다(신법 우선 원칙; FTA가 신법임).

미국 정부는 자국의 인터넷 기업들이나 금융회사가 어떤 인증 방법을 선택하는지에 대하여 전혀 개입하지 않고 있습니다. 만일 미국 정부가 자국의 특정한 인증 기술의 사용을 미국내에서 강제함으로써 한국 기업이 제대로 미국 시장에 진입할 수 없도록 한다면, 미국 정부의 그러한 행위는 역시 한미FTA 위반입니다.

4. 은행감독에 관한 바젤위원회(BCBS)의 전자금융 위험관리 원칙

한국정부는 2009년 3월15일에 바젤위원회(BCBS) 회원국이 되었으므로, 동 위원회가 채택하는 은행감독 원칙을 준수할 국제법적 의무를 지고 있습니다. 바젤위원회는 “어떤 인증 기법을 사용할 것인지는 ... 은행경영진의 평가에 기초하여 은행이 결정하여야 한다“는 원칙을 채택하고 있습니다(Risk Management Principles for Electronic Banking, Principle 4).

'공인인증서 등'의 사용을 강제하는 금융위 규제의 근거를 제공하는 현행 전자금융거래법 제21조 제3항은 OECD회원국으로서 한국정부가 부담하는 국제법적인 의무에도 반합니다.

5. 미국 국립표준기술연구소(NIST) 연구 결과

2011년12월에 미국 국립표준기술연구소는 다양한 인증 기술을 면밀히 검토한 후 "전자인증 가이드라인"을 발간하였습니다(SP800-63-1). 이 연구 결과에 따르면, 전자파일 형태로 저장되고 소트프웨어로 이용하는 인증서(국내 보급된 공인인증서 99%이상이 이런 형태입니다)의 보안강도는 3등급에 불과한 반면, 잠금장치가 있는 OTP생성기는 그 보다 안전한 4등급에 해당한다고 설명하고 있습니다(등급이 높을수록 보안강도도 높습니다) (첨부파일 참조). 물론 더 강력한 OTP를 ‘강제’해야 한다는 뜻이 결코 아닙니다. 시장이 선택하게 하면 됩니다.

이미 15년이나 된 공인인증 보안 기술은 이처럼 열악할 수 밖에 없습니다. 그런데도, 한국 정부는 이런 낙후된 기술의 사용을 계속 강요함으로써 공인인증 관련 업체의 영업이익과 사업편의를 보장하는 한편, 인터넷 기반의 여러 국내의 소규모 스타트업 기업들이나 대규모 온라인 쇼핑몰 등이 전세계 고객을 상대로 경쟁력 있게 영업하지 못하도록 제약하는 것입니다.

6. 맺는 말

상상해 보십시오, 만일 아마존(amazon.com)이라는 온라인 쇼핑몰에서 물건을 구입하고 소비자가 돈을 지불하려 할때, 미국정부가 지정한 인증기관이 발행한 특정한 인증서를 반드시 제시해야 결제거래를 할 수 있도록 아마존이 규제 받았더라면, 과연 아마존이 전세계로 뻗어나갈 수 있었겠습니까?

다른 예를 들어보겠습니다. 코자자(kozaza.com)라는 소규모(직원 7-8명) 스타트업 기업이 있습니다. 북촌 일원의 한옥을 국내는 물론 전세계에 소개하면서, '한옥 스테이'를 예약할 수 있도록 해주는 웹사이트입니다. 외국인들에게는 물론이고, 아파트에서만 살아 온 우리 젊은 세대에게도 인기를 끄는 서비스입니다. 그러나, 막상 온라인으로 예약과 결제를 하려면 공인인증서 때문에 매우 번거롭고 까다로운 난관을 거쳐가야 합니다. 한국인들이야 이미 온라인 결제를 하려면 단단히 각오해야 한다는 사실을 익히 알고 있겠지만, 한국을 방문하는 기회에 한옥에서 하룻밤을 지내고 싶어하는 외국인들에게 국내의 전자금융거래는 한마디로 악몽입니다. 거래 자체를 아예 포기하게 만듭니다.

공인인증서, 안심클릭 등으로 이루어진 한국의 전자금융거래는 이처럼 인터넷 기반의 여러 기발한 서비스가 세계의 고객들을 상대로 뻗어나가지 못하도록 발목을 잡고 있습니다.

안전한 기술은 강제할 필요가 없습니다. 안전한 기술을 일부러 외면하는 금융회사는 없습니다. 안전한 기술을 선택해야 사고가 덜나고, 물어줘야할 배상 책임도 줄어들기 때문입니다. 정부가 억지로 강제해야 마지못해 쓰는 보안 기술은 이미 그 자체로 경쟁력이 없는 기술입니다.

전자금융거래법 제21조 제3항 개정 법안은 다양한 보안/인증 기술들이 공정하게 경쟁할 수 있도록 규제자가 시장을 제대로 감시하고, 기술 중립적 입장을 취해야 한다는 지극히 당연한 상식을 담고 있는 것입니다. 정부가 특정 기술의 판촉에 나서거나, 특정 기술의 사용을 강제해서는 안된다는 점을 분명히 하는 것입니다.

이 법안은 "단 한 조항"만을 개정하는 것이지만, 국내 주요 대학의 교수들과 한국 IT산업의 핵심 주체들로 구성된 인터넷기업협회가 공식 지지를 천명하고 있는 법률안 입니다. 이 법안이 통과되면 한국의 IT산업이 전세계를 상대로 뻗어나갈 수 있는 발판이 마련되며, IT분야의 일자리 창출, 한국 보안 산업과 인터넷 산업 도약의 기틀이 마련될 것입니다.

[참고 자료]

- 공인인증서는 이미 대규모로 유출되어 왔습니다. 보안업계에서는 공공연한 비밀입니다.
  - 2007년에 5000장 이상 유출됨 http://www.boannews.com/know_how/view.asp?page=40&gpage=31&idx=1539&numm=1211&search=title&find=&kind=03&order=ref
  - 2013년에도 700여장 유출됨 http://www.nocutnews.co.kr/show.asp?idx=2401707
  - 드러나지 않은 유출 규모는 알 수 없음.
- 공인인증서 탈취용 악성코드는 널리 퍼져 있고, 이용자에게 '주의'를 당부하는 것으로는 역부족임. http://www.ddaily.co.kr/news/news_view.php?uid=103122
- 공인인증 '프로그램'의 취약점도 계속 발견되고, 보고되고 있습니다:
  - 제큐어웹 ActiveX 원격코드 실행 취약점 보안 업데이트 권고 (http://www.krcert.or.kr/kor/data/secNoticeView.jsp?p_bulletin_writing_sequence=2311)

[첨부 자료]

1. 미국 국립표준기술연구소 발간, "전자인증 가이드라인" (2011)
2. 한미FTA 제15.4조 (전자인증 및 전자서명)
3. 은행감독에 관한 바젤위원회(BCBS), 전자금융위험관리원칙(2003)
4. 한국인터넷기업협회, 전자금융거래법 개정안 공식 지지성명

5. 전국 주요 대학 컴퓨터공학, 정보보호/보안학 전공 교수 등 300명, 전자금융거래법 개정안 지지서명

전자금융거래법 개정법안에 대한 전문위원 검토보고서 분석

이종걸 의원실

결론: 개정법안에 대한 "정확한 팩트에 근거한 의미있는 반대"는 없음

검토보고서에 소개된 금융위원회와 사단법인 금융결제원(공인인증 업체)의 견해는 다음과 같음.

1. 금융위원회 입장(보고서 제 7 면):

> "개정안에 대하여 금융위원회는 공인인증서와 동등한 안전성을 가진 인증기술이 없는 상황에서 13 년간 사용되어 온 공인인증제도를 당장에 철폐하는 경우 금융회사 및 이용자들의 혼란과 전자금융사고가 증가할 우려가 있고, 전자금융 인증체계 개편 관련 연구용역(6~9 月)을 실시 중이므로 금년 하반기까지 충분히 검토 후 법 개정의 추진여부가 결정될 필요가 있다는 의견을 제시함."

그러나,

- "공인인증서와 동등한 안전성을 가진 인증기술이 없는 상황"이라는 금융위 주장은 사실과 다름. 미국 국립표준기술연구소(NIST)가 2011 년에 발간한 "전자인증 가이드라인"은 공인인증서보다 더욱 안전한 인증수단들이 존재하고 있음을 확인.
- "공인인증제도를 당장에 철폐"하는 상황을 전제로 한 금융위 주장은, 이 법안 내용과는 무관함. 이 법안은 공인인증서 사용을 '강제'하지 말자는 것이지, 공인인증제도를 '철폐'하자는 것이 아님. 공인인증서를 계속 사용하기를 원하는 금융회사는 계속 사용할 수 있음.
- 금융위원회 용역(인증체계 개편 관련 연구 용역)은 이 법안 채택 후 자율적, 점진적 변화가 업계에서 서서히 진행되는 동안, 언제든지 상시로 수행되면 될 것임. 이 법안 처리가 금융위 연구 용역 일정에 종속되어야 할 이유는 없음.

전문위원 검토보고서도 이점을 지적하면서, 다음과 같이 결론짓고 있음(보고서, 7-8 면):

> "개정안의 취지는 해킹 등으로 인한 취약점이 노출된 공인인증서의 '존폐'여부가 아닌, 금융위가 공인인증서 사용을 강제하여서는 안된다는 것"

따라서, 금융위원회 입장은 사실과 다르거나, 이 법안과는 무관한 주장이거나, 이 법안 통과와 충분히 양립 가능한 주장이므로, 이 법안에 대하여 정부측의 "의미있는 반대"는 없는 상황임.

2. 공인인증 사업 수행 민간 업체(사단법인 금융결제원) 의견

- 금융위원회(정부) 입장은 공인인증 영업을 수익사업으로 하는 민간 업체(사단법인 금융결제원) 입장을 그대로 반복하는 것임. 따라서 공인인증 업체의 의견을 별도로 논할 필요는 없음.
- 민간 업체의 주장 중, (1)공인인증서가 창조 경제에 이바지했다, (2)인증수단을 다양화하면 더 많은 관리이슈와 해킹문제가 일어날 수 있다는 부분(보고서 각주 11)은 사실과 다름.
- 공인인증서 강요 때문에 오히려 국내의 여러 기발한 스타트업 기업들이 전세계를 상대로 영업할 길이 막혀있음. 한국에서만 강행되는 "국내 공인" 인증서를 사용해야 하므로, 외국 고객은 결제 불가능.
- 인증수단을 한가지로 강제, 통일할 경우, 그 수단이 뚫리면 온국민이 '일거에' 당하게 되므로 더욱 심각한 위험을 초래함.
- 인증수단 선택을 금융회사의 자율에 맡겨둔 선진 각국(미국, 영국, 유럽)의 경우, 그로 인한 혼란이나 불편이 생겼다는 사례는 없음. 오히려 한국보다 안전, 편리, 다양한 전자금융서비스가 이루어지고 있음.

전문위원 검토보고서도 이점을 지적하면서, 다음과 같이 결론 짓고 있음(보고서 제 8 면):

> "전 국민을 대상으로 하는 특정기술의 사용강제는 해킹 규모 등에 따라 국가 전체적인 문제를 야기하거나 보안산업의 발전을 저해할 수 있고, 은행·증권사 등 금융회사가 자율적으로 금융보안 수단을 결정하는 것이 바람직"

3. 금융위원회와 공인인증 사업 수행 민간 업체 간의 부적절한 관계

- 공인인증서 사용을 강제해주는 금융위원회 고위 관리(부이사관)는 퇴직 즉시 공인인증 사업 수행 민간 업체인 '사단법인 금융결제원' 감사로 취업하여 3 년간 10 억여원을 받는 상황임.

> "금융결제원 감사에 원중희씨 선임" - 중앙일보 2012.3.14 자 보도 http://bit.ly/108F5M1
>
> "정부의 '공인인증서' 집착은 '정경유착'과 '전관예우' 때문?" 미디어뉴스 2013.6.20 자 보도 http://bit.ly/13YWIPc

4. 개정안이 채택되도 금융위원회는 '인증방법에 관한 기준'을 정할 권한을 여전히 보유함

- 전문위원 검토보고서 본문 마지막 페이지(제 8 면)에 기재된 아래 내용은 오해의 소지가 일부 있음:

  "한편, 개정안에 따르면 금융위가 정보기술부문 및 전자금융업무에 대하여만 세부 기준을 정할 수 있고, 인증방법과 관련한 세부 기준은 정할 수 없다는 문제가 있는바, 금융회사를 이용하는 금융소비자보호와 관련하여 인증방법에 대한 기준설정이 없는 경우에도 문제가 없는 지에 대한 여부도 검토가 필요할 것으로 봄."

- 현행 제 21 조 제 2 항은 금융위원회에게 "전자적 전송이나 처리를 위한 인력, 시설, 전기적 장치, 소요경비 등의 정보기술부문 및 전자금융업무에 관하여" 기준을 제정할 권한을 이미 포괄적으로 부여하고 있음.

- '인증 방법'은 제 21 조 제 2 항이 말하는 "정보기술부문"에 당연히 포함되므로, '제 3 항'이 개정되어도 금융위원회는 '인증방법에 관한 기준'을 정할 권한을 여전히 '제 2 항'에 근거하여 보유함.

- 제 21 조 제 3 항 개정안은 금융위원회가 제 2 항에 의하여 포괄적으로 부여받은 기준 제정 권한을 행사함에 있어서 "공정한 기술 경쟁"을 저해해서는 안된다는 것 뿐임.

전자금융거래법 개정안 신·구 조문 대비표

현 행	개정안
제 21 조(안전성의 확보의무) ① 생략 ② 금융기관등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자금융거래의 종류별로 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다. ③ 금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 「전자서명법」 제 2 조 제 8 호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다.	제 21 조(안전성의 확보의무) ①(현행과 같음) ②(현행과 같음) ---------- ③ 금융위원회는 전 항의 기준을 정함에 있어서 보안기술과 인증기술의 공정한 경쟁을 저해하거나, 특정기술 또는 서비스의 사용을 강제하여서는 아니된다.

"금융회사가 접근 매체를 자율적으로 선택할 수 있어야 한다"

– 미래부 정보보호정책과 오승곤 과장(현행 공인인증제도 감독 관청 실무책임자)
(2013.6.13. 국회 유승희 미방위 간사 주최 공개토론회에서 발언)

한미 FTA 제 15.4 조 (전자인증 및 전자서명)

"거래 당사자가 그 거래를 위하여 적절한 인증방법을 상호 결정"할 수 있어야 함.

KAIST, 포항공대, 서울대 교수 등 300 여명, 지지서명

> 정부 정책의 '기술 중립성'을 확보함으로써 기술 발달과 서비스 품질 향상을 달성하는데 필요한 바람직한 제도 개선 방안이라고 판단하고, 이 법률안이 조속히 통과되기를 희망한다.

인터넷기업협회(네이버, 다음, SK 컴즈, 카카오 등 150 여개 국내 인터넷기업)도 공식지지성명

> 공인인증서 의무사용을 금지하는 이번 개정안이 한국 인터넷산업의 혁신과 발전을 가로막는 여러 가지 현행 규제들에 대해서도 전반적인 개선의 시발점이 되는 계기가 되었으면 한다.

미국 국립표준기술연구소(NIST), "전자인증 가이드라인"(2011.12 출간)

- 소프트웨어적 보안인증서(국내 공인인증서 99%에 해당) → Level 3 에 불과함
- 잠금장치 있는 OTP 생성기 → Level 4 (더 우수한 인증 수단)

개정법안은 특정 기술, 제품을 '강제'해서는 안된다는 내용.

- http://choice.opennet.or.kr/info.php 참조

미국 국립표준기술연구소 발간 '전자인증 가이드라인'

※등급이 높을수록 보안 수준 높음

자료:NIST

2등급 LEVEL 2

일반 OTP(일회용 비밀번호) 생성기, 스마트카드 리더기 등

일반 OTP
(일회용 비밀번호)
생성기

스마트카드
리더기

3등급 LEVEL 3

USB · PC · 스마트폰 등에 저장된 인증서(국내 보급 공인인증서의 99% 이상)

공인인증서

4등급 LEVEL 4

잠금장치 있는 OTP 생성기, 프로세서가 내장된 별도의 하드웨어(USB 저장장치 아님) 등

잠금장치 있는
OTP 생성기

프로세서 내장
하드웨어

전자서명법 개정법률안 설명

2013.6.13
고려대학교 법학전문대학원 교수
김기창

1. 개정안은 PKI 기반 전자인증서(X509 digital certificate) '기술 자체'를 논란하는 것이 아니다.

따라서, 인증서가 온라인상에서의 신원 확인(authentication) 수단이라느니, 인증서가 안전하다느니, 위험하다느니, 전자서명이 어떤 '기술적' 원리로 이루어지는지 등에 대한 논의는, 이 개정법안과는 전혀 무관한 논점이다.

개정안에 따르더라도 PKI 기반 전자인증서(X509 규격)가 여전히 사용되고, 이것으로 신원 확인을 하고, 전자서명을 하게 된다.

개정안 제 2 조에 정의된 '전자서명'과 현행법상 '공인전자서명'의 정의는 완벽하게 동일하다. 따라서 '공인전자서명'이 안전한 기술이라면, 개정안에 따른 '전자서명'도 같다.

2. 개정안은 전자인증서가 금융거래에 사용되는지 여부와 무관하다.

원래, 인증서는 금융거래 뿐 아니라 모든 전자거래에 사용될 수 있다. 한국에서만 인증서가 금융거래를 연상하게 하는 이유는 금융위원회가 인증서 사용을 금융거래에서 강제해 왔기 때문이다. 현행 전자서명법도 인증서의 용도를 금융거래 등으로 제한하지 않으며, 개정안도 같다.

인증서 '덕분에' 금융거래가 안전해졌는지 위험해 졌는지에 대한 논의는 이 개정법안과는 전혀 무관한 논점일 뿐 아니라, 그러한 주장 자체가 기술적 무지를 노출할 뿐이다. 왜냐하면 '실제로' 거래(금융거래건, 비금융거래건)가 '안전'하게 설계되어 있는지 여부는 '인증서'에 달려있는 것이 아니라, 그것을 '어떻게' 실제로 구현하는지에 달려있다. 허술하게 설계된 거래 솔루션이라면 인증서를 사용하건 안하거나 위험하고, 안전하게 설계된 솔루션이라면 인증서를 사용하건 안하건 안전하다.

전자인증서를 사용하기만 하면 마치 거래가 '안전'하게 되는 듯 주장하는 자는 자신의 무지함을 노출할 뿐이다.

3. 현행 전자서명법 제 3 조 제 1 항은 한미 FTA 제 15.4 조에 어긋나므로 이미 무효임.

한미 FTA 는 전자서명법보다 나중에 비준된 것이므로 전자서명법 규정이 한미 FTA 와 충돌할 경우, 신법 우선의 원칙에 따라 한미 FTA 가 우선한다. 한미 FTA 제 15.4 조는 다음과 같다(밑줄은 필자가 추가):

> 1. 어떠한 당사국도 다음의 전자인증을 위한 법령을 채택하거나 유지할 수 없다.
>
> 가 . 전자거래의 당사자가 그 거래를 위하여 적절한 인증 방법을 상호 결정하는 것을 금지하는 법령
>
> 나. [이하 생략]

현행법 제 3 조 제 1 항은 당사자 일방이 상대방 의사와 무관하게 '공인전자서명'을 그들 간의 거래에서 사용할 수 있도록 규정하고 있다. 이 점은 제 3 조 제 3 항과 비교해 보면 분명해 진다. 제 3 조 제 3 항은 "공인전자서명 외의 전자서명은 **당사자 간의 약정에 따른** 서명, 서명날인 또는 기명날인으로서의 효력을 가진다"고 규정함으로써, 인증서 및 전자서명을 사용할지 여부는 쌍방의 합의에 따른다는 점을 명시하고 있다.

그러나 동조 제 1 항은 그러한 언급이 전혀 없이 "다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다"고만 하고 있으므로, 일방이 상대방의 의사와 무관하게 공인인증서와 공인전자서명을 사용할 수 있게 되어, 인증방법의 '상호 결정'을 보장하는 한미 FTA 와는 양립할 수 없다.

전자서명은 인증서 사용을 당연히 전제하는 개념이고, 인증서를 사용하지 않고서는 전자서명을 할 수 없다.

4. 현행법 제 3 조 제 2 항은 법관의 자유심증주의에 반한다.

'육필 서명'이나 '인감 날인' 조차도 우리 법체제 하에서는 문서의 진정성립을 뒷받침하는 '증거자료'에 불과하다. 증거자료를 믿을 것인지 여부는 법관의 자유심증에 따르는 것이고, 육필 서명되거나 인감도장 또는 막도장이 날인된 문서라고 해서 그 기재내용 대로의 법적 효력을 언제나 인정받는 것

은 아니다.

육필 서명이나 인감 날인에 대해서 별도의 법규정 없이 법관의 자유 심증에 따른 판단을 통하여 문서의 진정성립이나 위조, 변조 여부를 판결하도록 하는 것이 한국법의 입장이므로, 전자서명에 대하여 육필 서명이나 인감 날인에도 부여하지 아니하는 '법정 추정력'을 부여하는 규정(제 3 조 제 2 항)을 둘 합리적 이유는 없다.

이 규정(현행법 제 3 조 제 2 항)은 90 년대 후반, '전자서명' 기술을 처음 접한 당시 법률가들이 실제로 인증서가 안고 있는 여러 기술적 한계를 제대로 이해하지 못하고 소박하게 품었던 과장된 환상에 기인한 규정일 뿐이고, 이제는 삭제되어 마땅하다.

5. 전자서명이 없는 이메일 등의 전자문서도 당연히 증거능력이 있다.

"전자문서 및 전자거래 기본법" 제 4 조 제 1 항은 "전자문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 아니한다"고 이미 규정하고 있다.

개정안 제 3 조 제 3 항도 같은 입장에서 "전자문서는 전자서명이 부착되어 있지 않다는 이유만으로 문서로서의 효력이 부인되지 아니한다"고 규정한다.

6. 루트인증기관은 반드시 독립적 제 3 자의 전문적, 정기적 검증을 받아야 한다.

현행 전자서명법은 루트인증기관 KISA 에 대한 독립적 제 3 자의 전문적, 정기적 검증에 관한 규정이 없고, 실제로 KISA 는 그러한 검증을 지금껏 받은 바 없다. 작년(2012)에 와서야 비로소 KISA 도 그 업무 수행의 안전성 여부를 제 3 자로부터 제대로 검증받기 위하여 준비 중이고, 조만간 만족스럽게 검증을 통과할 것으로 희망한다.

개정안 제 4 조는 루트인증기관에 대한 독립적 제 3 자의 전문적, 정기적 검증을 규정하고 있는 바, KISA 도 이러한 검증을 통과하기만 하면, 개정법하에서도 지금처럼 루트인증기관으로 인정받을 수 있게 된다.

개정법안 경과 규정 제 2 조는 "개정 전 전자서명법 제 4 조의 공인인증기관은 이 법 시행일로부터 1

년 동안 이 법 제 4 조 제 1 항의 인증업무수행기준을 충족하는 것으로 본다"고 규정함으로써 검증을 준비하고 통과하는데 필요한 충분한 시간적 여유를 제공하고 있다.

7. 개정안은 미래부 장관이 인증업무수행기준을 정하도록 규정하고 있다.

개정안은 인증서비스에 대한 '완전 방임'을 표방하지 않는다. 개정안 제 4 조 제 1 항은 인증업무수행기준을 미래부 장관이 정하도록 하고 있고, 국제적으로 이미 통용되는 인증업무수행기준(WebTrust, ETSI, ISO 기준 등)에 대해서도 미래부 장관이 이를 승인할지 여부를 종국적으로 결정할 권한을 여전히 보유하도록 규정하고 있다(개정안 제 4 조 제 2 항).

8. 개정안은 미래부장관이 정하는 기준을 충족하는 인증기관들 간의 공정한 경쟁을 보장한다.

미래부 장관이 스스로 정한 인증업무수행기준을 충족하는 인증기관이라면, 이를 미래부 장관이 차별적으로 대우할 이유가 없고, 그럴 근거도 없다.

원래, 루트인증기관은 복수로 존재하는 것이 당연한 것이다. 미국, 영국 등 세계 각국에서도 다 그렇게 하고 있다.

KISA 외에 루트인증기관이 하나라도 더 존재하게 되면 인증제도가 '혼란'에 빠지게 된다고 상상할 근거는 없다. 오히려, 루트인증기관의 '제도적 독점'을 보장할 경우, 그 서비스의 품질 및 경쟁력 저하가 우려된다. 예를 들어, 만일, 미국정부가 Verisign 만이 "유일한 루트인증기관"이라고 법으로 정하고 독점을 보장해 주고, 제 3 자의 전문적이고 정기적인 검증도 안받아도 되게 해두었다면, Verisign 이 과연 전세계로 성장할 수 있었겠는가? 여러 루트인증기관들 간의 공정한 경쟁을 통하여 기술력과 안전성이 증진되는 것이다.

9. 개정안은 국내 인증제도 및 인증기술의 글로벌화 및 선진화 토대를 제공한다.

현행 '공인인증 제도'는 그 정점에 위치한 루트인증기관 KISA 의 신뢰성을 '한국 정부'의 권위로부터 도출하려할 뿐, 전문적, 독립적, 정기적 검증에 기초한 신뢰성을 국제 무대에서 주장할 수 없도록 되어 있다. 이러한 고립적 인증제도는 한국에만 독특한 것이고, 이렇기 때문에 현행법 제 27 조의 2(상호인정)과 같은 규정을 아무리 둬 본들 외국정부가 한국의 고립된 인증체계를 인정할 이유가 없다.

13 년이 지난 지금에 이르기까지 한국 정부와 인증역무의 상호인정 협정을 체결한 외국 정부는 없다. 그도 그럴것이 외국 정부는 이미 인증 서비스를 글로벌 표준에 맞게 정비하고, 루트인증기관의 신뢰성을 특정 정부의 폐쇄적 권위에 의존하지 아니하고, 독립적 제 3 자의 전문적, 정기적 검증(국제적으로 승인된 감사기준에 따라 수행되는 검증)을 토대로 신뢰를 구축하고 있기 때문이다.

폐쇄적, 국가 단위의 고립된 인증제도(현행 '공인'인증제도)를 만들어 두고, 외국도 그런 식의 고립된 인증제도를 만들것이라고 막연히 전제한 다음, 그런 외국 정부와의 '협정'을 통해서 한국의 '공인인증역무'가 국외에서도 인정받을 수 있을 것이라는 순진한 상상은, 인증제도가 글로벌 무대에서 어떻게 작동하는지 그 근본 원리조차 이해하지 못했기 때문에 품었던 환상에 불과하다.

개정안은 이런 미개한 발상을 극복하고, 국내의 인증제도 자체를 '글로벌 표준'에 맞게 정비하는 것을 핵심 내용으로 한다.

10. 개정안은 박근혜 대통령의 대선 공약을 실현하는 것이다.

박근혜 대통령은 "글로벌 표준에 맞는 다양한 인증서비스 허용"을 대선 공약으로 걸었다. 개정안은 국내의 인증업체들도 글로벌 기준에 맞게 독립적 제 3 자의 전문적, 정기적 검증을 받도록 하고, 국제적으로 승인된 감사기준에 따라 검증받은 인증업체들 간에는 차별하지 않는 것을 핵심 내용으로 하고 있다.

개정안은 또한 미국 캘리포니아 주의 전자서명 규정을 참조하고 대폭 반영한 것이다. 캘리포니아 주의 전자서명 규정은 루트인증기관은 반드시 제 3 자의 검증을 받도록 규정하고, 미국 외의 글로벌 기준에 맞는 검증을 받은 루트인증기관들도 캘리포니아 주 정부가 루트인증기관으로 인정하는 것을 내용으로 하고 있다. 이렇게 하는 것이 "글로벌 표준에 맞는 다양한 인증서비스를 허용"하는 것이다.

<현행 전자서명법상 ’공인전자서명’, ‘일반전자서명’ 그리고 개정법안상 ‘전자서명’ 비교>

	현행 전자서명법		전자서명법 전부개정법률안
	공인전자서명	일반전자서명	전자서명(개정안 제 2 조 제 2 호)
목적	·법에서 서명 등을 요구하는 문서를 전자화할 때, 자필서명과 동일한 기능을 수행하는 전자적 수단을 제공	·당사자 간의 자유로운 합의에 의해 다양한 목적으로 사용 가능	·당사자 간의 자유로운 합의에 의해 다양한 목적으로 사용 가능(개정안 제 3 조)
효력	·전자서명법 제 3 조에 의해 서명 등과 동일한 효력을 가짐 ·전자문서의 진본성·무결성을 보장, 부인방지 기능을 수행	·당사자 간 약정에 따라 서명 등과 동일한 효력을 가짐	·당사자 간 약정에 따라 서명 등과 동일한 효력을 가짐(개정안 제 3 조 제 1 항) ·전자문서의 진본성·무결성을 보장, 부인방지 기능을 수행(개정안 제 2 조 제 2 호 전자서명의 당연한 기능)
요건	·전자서명 생성정보가 가입자에게 유일하게 속할 것 ·서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것 ·전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 ·전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것	·특별한 요건 없음	·전자서명 생성정보가 가입자에게 유일하게 속할 것 ·서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것 ·전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 ·전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것 (개정안 제 2 조 제 2 호)
이용 범위	·법에서 서명 등을 요하는 문서를 전자적으로 작성하는 경우 ·본인확인(전자서명법 제 18 조의 2)	당사자 간의 합의에 따름	· 당사자 간의 합의에 따름(개정안 제 3 조) · 다른 법이 제한하거나 배제하지 않으면, 당사자 간의 합의에 따라 본인확인 용도로 당연히 이용
발급 기관	·공인인증기관에 의해 발급	·일반인증기관에 의해 발급	· 미래부 장관이 정하는 업무수행기준을 충족하는 인증기관이 발급(개정안, 제 4 조 제 1 항, 제 2 항)
발급 기관 요건	·법에서 정한 기술적·재정적 요건을 갖추고, 국가기관의 관리·감독을 받음	·특별한 요건 없음	· 법에서 정한 기술적, 재정적 요건을 갖추고, 전문적, 독립적 제 3 자의 정기적 검증을 받아야 함. (개정안 제 4 조 제 4 항)

IT 보안 규제체제 및 법 제도의 재검토

2013.7.4.

김기창

고려대학교 법학전문대학원

1. '진흥책', '육성책'의 문제점

- WIPI(2005-2009)도 모바일 산업 "진흥책"이었음.
  - 기술 규격을 업계가 자율적으로 채택/불채택을 선택하는 '기술 표준(Technical Standard)'으로 유지하려 하지 않고, 정부가 행정력으로 채택을 강제하는 '기술 규정(Technical Regulation)'으로 만듦.
  - 개발 단계에서의 정부 지원 → 기술 개발 → 지원(강제) 요청 → 강제
  - 강제 규정화되는 순간, 기술 진보는 정체.
  - 기술 진보와 무관하게 기득권 자들의 이해관계의 역학구도 형성: 이통사, 기기 제작사, 콘텐트 공급사 등은 기존(기득권) 체제 수호 욕구
- '공인'인증서(1999-2013)도 암호기술, 전자상거래 '육성책' 이었음.
  - 고강도(128bit) 암호화 기술 필요 → 정부 지원 → 고강도 암호화 성공(1998)
  - 그러나 '보안'에 대한 기본적 이해는 결여:
    - 서버인증 안함 (http 접속 + 플러그인)
    - 유저 행태에 대한 고려 없음: 무조건 "예", ''설치"
    - Keystore, Keychain 이 뭔지도 몰랐음
    - 신뢰 체계가 형성되는 전체 메카니즘을 몰이해: 루트인증기관은 '무조건' 믿으라?
  - 보안, 온라인 신원(identity) 체계에 대한 '정부' 개입 욕망: 정부가 인증기관을 지정: '공인'

인증기관 제도

- 강제하기 시작하면, 기득권자 발생(사업적 기득권, 규제 기득권), 기술진보 정체
- ‘보안’이라는 미명으로, 정부가 인증업자, 특정 보안기술 판촉사원 행세...

2. Security Theatre (보안 ‘쑈’)

- False logic:
  - ‘보안’은 강제해야?
  - ‘보안’은 정부가 규제해야?
  - ‘보안’은 비공개 해야?
  - ‘보안’은 국내에 둬야?
- ‘공인’ 인증 제도(전자서명법)
  - 암호입력 쑈, ‘보안’플러그인 설치 쑈
  - 인증기관은 정부가 ‘지정’ 해야 안전? → “셀프 인증”하는 KISA 를 정점으로?
- 측량 정보 국외 반출 규제(측량 수로조사 및 지적에 관한 법률, 제 16 조)
  - 북한도 ‘공개된’ 지도 정보는 국외반출 허용
  - ‘공개된’ 지도 정보를 국내에만 둔다고 무슨 ‘보안’?
  - 외국인/적대세력은 네이버, 다음 지도 접속, 이용 못하나?
- 위치정보사업자 ‘허가제’, 위치기반 서비스사업자 ‘신고제’ (위치정보의 보호 및 이용 등에 관한 법률, 제 5 조, 제 9 조)
  - 개인의 security 나 privacy 침해에 대하여 제재하는 것으로는 부족한가?
  - ‘사전’ 규제가 가능하기나 한가?

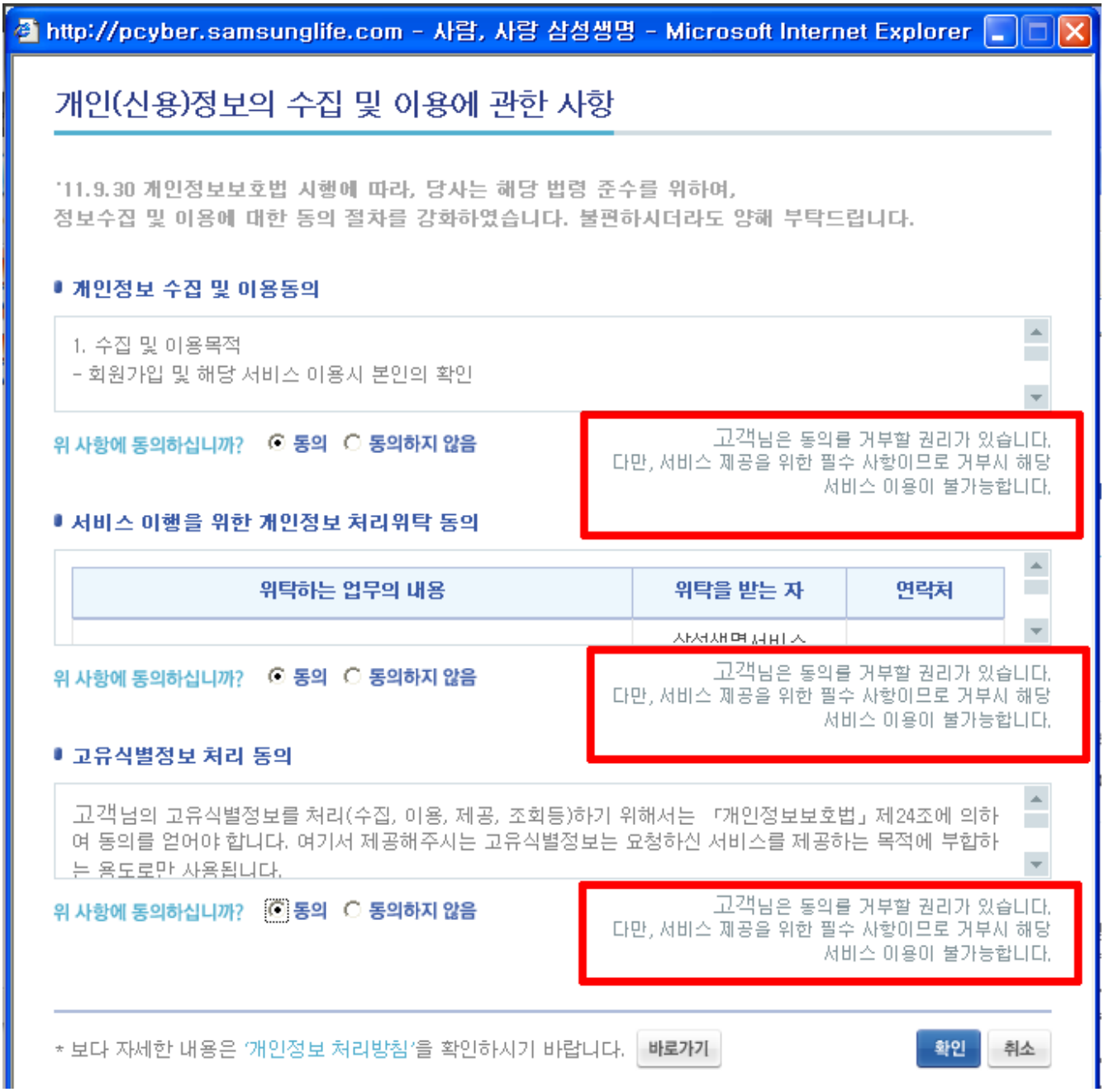
- 범법을 기획하는 자가 '허가' 신청, 사전 '신고' 할까?

- 금융회사의 정보처리 및 전산설비 위탁에 관한 규정[1] (금융위 고시; 입법예고 중 2013 년 4.17-5.26)
  - PCI DSS 기준 준수하는지를 전문 감사업체가 감사하면 충분할 것을...
  - 3.20 보안 참사, 농협 원장삭제 사건, 현대캐피탈, 한화보험 계정정보 유출...

3. 기술 인력, 정책 결정자가 저지르는 법률의 오해

- 공인인증서
  - 금융감독위원회를 동원하여 금융거래에 공인인증서 사용 강제:
    - 전자서명의 법적 효력(?) 오해
    - 금융실명법 왜곡: 본인확인 기술이 하나 뿐인가?
  - 이른바 '부인방지' (non-repudiation)
    - 개인키가 유저에게 유일하게 귀속, 서명시점에 배타적 지배, 관리가 입증되어야 가능
    - '서명자'는 부인 못하지만, 과연 누가 '서명자'였는지는 입증 불가능
    - "실제로 공격자를 붙잡으면", 그 공격자는 그런 거래를 했다는 점을 부인하지 못하게 할 수 있다는 뜻. 아무짝에 쓸모 없는 헛소리일 뿐.
    - 고객에게 책임을 떠넘기고, 고객에게 책임을 지울 수 있는 기술?
- 개인정보보호법 상 '동의' 형식 규제
  - 약관 법리의 원칙에 비추어, '동의'가 중요한가, '명시, 설명'이 중요한가?
  - 체크박스/라디오버튼(□ 동의 / ⦿ 동의) 오용의 폐해

1 http://www.ddaily.co.kr/news/news_view.php?uid=104280



4. 정부/규제자가 '기술 전문가' 행세, '기업가' 행세를 하는 문제

- 인증, 보안 기술 분야
  - WebTrust 기준, PCI DSS 기준을 흉내낸 '기준'도 정부가 제정, 제정 후 방치
  - 그 기준을 준수하는지 여부에 대한 '검사/감사' (security audit)도 정부가 수행하는 '시늉'

- 보안감사 전문업체를 정부가 '지정', '관리'하겠다는 태도.
- 민간 업자는 '못믿는다'? 그럼, 정부 공무원은 믿을 만 한가?

- 유망 사업 아이템, Buzz Word 를 찾아 헤메는 정부
  - 클라우드
  - 빅데이터 분석센터?
  - HTML5 시범사업?
  - "정부 R&D"의 존재 이유에 대한 몰이해

5. 규제자(政), 업체(經), 전문가(學)의 위험한 유착관계

- 정부의 강제에 기대어 사업하려는 유혹
- 공무원 앞에서 세일즈 하려는 부도덕한 자세
- 공무원의 '업적주의' 조급증, '정부주도' 산업 발전의 추억
- 학자, 전문가의 윤리성:
  - 용역 수주 가능성을 고려하여 비판 자제, 자기 검열
  - 발주자가 '원하는' 결과물 산출(공인인증제+금융실명제 = 공인인증서 강제)
  - 제자들의 입지, 업계 진출 전망 고려

6. 결론

- '기술 중립적' 규제
- 업계의 자율 존중, 전문가 단체의 역량 함양 기회 보장
- 사전적 행정 규제 강박증 탈피, 사후적이고 사법적인 제재
- 기초 과학, 기초적 인프라에 대한 장기적 안목의 '정부 R&D 철학' 수립 필요

- IT 기술 분야 정부 정책이 추구해야 할 근본 가치 수립, 공표, 준수
- 업무수행 '프로세스 혁신' 필요, Stakeholders 의 적절한 참여 보장
- transparency = power shift
- https://bugzilla.mozilla.org/

IT 보안 규제 , 정책 , 법률의 상관 관계

김기창

고려대학교 법학전문대학원

2013.7.4

1. ‘진흥책’, ‘육성책’의 문제점

- WIPI(2005-2009) 도 모바일 산업 ‘진흥책’이었음 .
  - ‘기술 표준 (Technical Standard)’ 과 ‘기술 규정 (Technical Regulation)’ 의 차이 무시 .
  - 기술 개발 단계에서부터 정부지원 → 기술 개발 → 지원 (강제) 요청 → 강제
  - 강제의 논리 , 기술의 논리
- ‘공인’인증서 (1999-2013) 도 암호기술 , 전자상거래 ‘육성책’ 이었음 .
  - 고강도 (128bit) 암호화 기술 필요 → 정부 지원 → 고강도 암호화 성공 (1998)
  - 그러나 ‘보안 기술’과 ‘신뢰의 제도적 얼개’ 대한 기본적 이해는 결여
  - 보안 , 온라인 신원 (identity) 체계에 대한 ‘정부’ 개입 욕망
  - ‘보안’이라는 미명으로 , 정부가 보안기술 판촉사원 행세 하면서 규제파워 누림 .
  - ‘보안 기술’ 이슈가 더이상 아니라 , ‘권력’과 ‘사업 이권’의 문제

2. Security Theatre (보안 '쑈')

False logic:

- ' 보안'은 강제해야 ?
- ' 보안'은 정부가 규제해야 ?
- ' 보안'은 비공개 해야 ?
- ' 보안'은 국내에 둬야 ?

‘보안 생쑈’ 사례 1, 2

- ‘공인’ 인증 제도 (전자서명법)
  - 암호입력 쑈 , ‘보안’플러그인 설치 쑈
  - 인증기관은 정부가 ‘지정’ 해야 안전 ? → “ 셀프 인증” 하는 KISA 를 정점으로 ?
- 측량 정보 국외 반출 규제 (측량법 , 제 16 조)
  - ‘공개된’ 지도 정보를 국내에만 둔다고 무슨 ‘보안’ ?
  - 외국인 / 적대세력은 네이버 , 다음 지도 접속 , 이용 못하나 ?

‘보안 생쑈’ 사례 3, 4

- 위치정보사업자 ‘허가제’, 위치기반 서비스사업자 ‘신고제’ (위치정보법, 제5조, 제9조)
  - 개인의 security 나 privacy 침해에 대하여 ‘사후’ 제재하는 것으로는 부족한가?
  - ‘사전’ 규제가 가능하기나 한가?
  - 범법을 기획하는 자가 ‘허가’ 신청, 사전 ‘신고’ 할까?
- 금융회사의 정보처리 및 전산설비 위탁에 관한 규정 1 (금융위 고시; 입법예고 중 2013년 4.17-5.26)
  - PCI DSS 기준 준수하는지를 전문 감사업체가 감사하면 충분할 것을 ...
  - 3.20 보안 참사, 농협 원장삭제 사건, 현대캐피탈, 한화보험 계정정보 유출 ...

3-1. 기술 인력의 법률 오해

- 공인인증서 사용 강제
  - ‘전자서명’의 법적 효력 (?)
  - 금융실명법 왜곡 : 본인확인 기술이 하나 뿐인가?
- 전자서명의 추정력? 이른바 ‘부인방지 (non-repudiation)’
  - 개인키 유일 귀속, 배타적 지배, 관리가 입증되어야 가능
  - ‘서명자’는 부인 못하지만, 과연 누가 ‘서명자’였는지는 입증 불가능
  - 고객이 부인하지 못하게 하는 ‘기술’?
  - 고객에게 책임을 지울 수 있는 기술?

3-2. 정책결정자들의 법률 오해

- 개인정보보호법 상 '동의' 형식 규제
  - 약관 법리에 대한 몰이해 / 오해
  - 약관 법리상 , ' 동의'가 중요한가 , ' 명시 , 설명'이 중요한가 ?
  - 예측가능 , 불이익 여부에 따라 '명시 , 설명의무' 결정
- 체크박스 / 라디오버튼 (□ 동의 / ◉ 동의) 오용의 폐해
  - 선택의 여지가 없는데 '체크박스' , ' 동의' ?
  - 유저를 '기망'하여 optional 동의를 받아내는 수법


http://pcyber.samsunglife.com - 사람, 사랑 삼성생명 - Microsoft Internet Explorer
개인(신용)정보의 수집 및 이용에 관한 사항
'11.9.30 개인정보보호법 시행에 따라, 당사는 해당 법령 준수를 위하여,
정보수집 및 이용에 대한 동의 절차를 강화하였습니다. 불편하시더라도 양해 부탁드립니다.
개인정보 수집 및 이용동의
1. 수집 및 이용목적
- 회원가입 및 해당 서비스 이용시 본인의 확인
위 사항에 동의하십니까? 동의 동의하지 않음
고객님은 동의를 거부할 권리가 있습니다.
다만, 서비스 제공을 위한 필수 사항이므로 거부시 해당
서비스 이용이 불가능합니다.
서비스 이행을 위한 개인정보 처리위탁 동의
위탁하는 업무의 내용
위탁을 받는 자
연락처
위 사항에 동의하십니까? 동의 동의하지 않음
고객님은 동의를 거부할 권리가 있습니다.
다만, 서비스 제공을 위한 필수 사항이므로 거부시 해당
서비스 이용이 불가능합니다.
고유식별정보 처리 동의
고객님의 고유식별정보를 처리(수집, 이용, 제공, 조회등)하기 위해서는 「개인정보보호법」 제24조에 의하
여 동의를 얻어야 합니다. 여기서 제공해주시는 고유식별정보는 요청하신 서비스를 제공하는 목적에 부합하
는 용도로만 사용됩니다.
위 사항에 동의하십니까? 동의 동의하지 않음
고객님은 동의를 거부할 권리가 있습니다.
다만, 서비스 제공을 위한 필수 사항이므로 거부시 해당
서비스 이용이 불가능합니다.
* 보다 자세한 내용은 '개인정보 처리방침'을 확인하시기 바랍니다.
바로가기
확인
취소

4. 정부 / 규제자가 '기술 전문가' 행세 , ' 기업가' 행세

- 인증 , 보안 기술 분야
  - WebTrust 기준 , PCI DSS 기준 흉내낸 '기준'도 정부가 제정 , 제정 후 방치
  - 그 기준을 준수하는지 여부에 대한 '검사 / 감사' (security audit) 도 정부가 수행하는 '시늉'
  - 보안감사 전문업체를 정부가 '지정' , ' 관리'하겠다는 태도 .
  - 민간 업자는 '못믿는다' ? 그럼 , 정부 공무원은 믿을 만 한가 ?
  - 정부 '지정' 업체와 민간 '인정 (accredition)' 업체 간에 자유 경쟁 허용하면 안되나 ?
- 유망 사업 아이템 , buzz word 을 쫓아다니는 정부
  - 클라우드
  - ' 빅데이터' 분석센터 ?
  - HTML5 시범사업 ?
- " 정부 R&D" 와 " 기업 R&D" 의 존재 이유와 차이에 대한 몰이해

5. 규제자 (政), 업체 (經), 전문가 (學) 위험한 유착관계

- 정부의 강제에 기대어 사업하려는 유혹
  - 공무원에게 세일즈 하려는 부도덕 / 비겁한 자세
- 공무원의 '업적주의' 조급증 , ' 정부주도' 산업 발전의 추억
- 학자 , 전문가의 윤리성 :
  - 용역 수주 가능성을 고려하여 비판 자제 , 자기 검열
  - 발주자가 '원하는' 결과물 산출 (공인인증제 + 금융실명제 = 공인인증서 강제)
  - 제자들의 입지 , 업계 진출 전망 고려

6. 결론

- ‘기술 중립적’ 규제
- 업계의 자율 존중, 전문가 단체의 역량 함양 기회 보장
- 사전적 행정 규제 강박증 탈피, 사후적이고 사법적인 제재 활용
- 기초 과학, 기초적 인프라에 대한 장기적 안목의 ‘정부 R&D 철학’ 수립 필요
- IT 기술 분야 정부 정책이 추구해야 할 근본 가치 수립, 공표, 준수
  - 업무 프로세스 자체의 혁신 필요
  - https://bugzilla.mozilla.org/