전자금융보안 규제정책의 실패 및 현실적 해법

가. 금융보안사고 현황 및 원인분석

1. 공인인증서에 편향된 “관치 보안”의 폐해

날짜	업체	사고 규모
2008 년 2 월	옥션	1863 만명 개인정보 유출
2010 년 3 월	신세계몰	820 만명 개인정보 유출
2011 년 4 월	현대캐피탈	175 만명 개인정보 유출
2011 년 4 월	농협은행	농협은행 서비스 수일 간 중단
2011 년 7 월	SK 컴즈	3500 만명(네이트 회원) 개인정보 유출
2011 년 11 월	넥슨	1320 만건 개인정보 유출
2013 년 3 월	방송사/금융회사/보험회사	이른바 “3.20 전산 대란”
2014 년 1 월	국민/롯데/NH 카드 등	고객정보 1 억여건 유출(내부자 공모, 관리부실)
2014 년 2 월	금융결제원	대규모 자동이체 사고(CMS 계좌이체 허점)

출처: http://goo.gl/fqQXp (대한민국의 정보 보안 사고 목록, 위키백과), 뉴스 보도 등

2. “정부 주도” 보안기술 정책 13 년의 결과와 한계

- 획일성: 계란을 ‘한 바구니’에 억지로 담아 두도록 강제하는 상황
- 무책임성, 투자 인센티브 감소, 면죄부 제공: “정부가 하라는 것 다 했으니, 우리는 책임 없다”
- 경쟁 회피, 카르텔 현상 유지, 수동적 대응: 새로운 보안기술 도입은 모두들 외면, 정부 눈치만
- 클라이언트쪽 보안(=공인인증서)에 집착, 서버쪽 보안은 무관심/무지: 둘 다 뚫린 최악 상황
- 국가안보 Risk 증가:
    - 적대세력이 공인인증 플러그인 취약점 악용할 경우, 전국민 PC 일거에 장악

나. 해법 및 개선 방향과 전략

1. “정부 주도” 강박증 탈피하고, 보안기술 다변화 및 경쟁 체제 도입 필요

- 정부가 보안 기술을 결정, 지정해줘야 한다는 전체주의적 발상에서 졸업할 때.
- 금융회사에게 보안 기술 선택 자율권을 부여하고, 사고거래에 대한 책임도 철저히 부과
- 고급 보안기술 경쟁 체제 도입 필요:
  - 현재는 ‘기술 경쟁’이 아니라, 노임 인하 경쟁, 납기 단축 경쟁, 하도급 경쟁이 창궐한 최악 상황(기술은 정부가 이미 ‘공인’이라는 이름을 붙여 획일적으로 ‘지정’해 둔 상황)
  - 정부가 특정 기술을 골라서 획일적으로 강제하는 행위를 중단하면, 다양한 앞선 기술, 고급 기술의 경쟁적 시장 진입이 촉진되고, 고급 보안인력이 제대로 성장할 수 있는 시장 여건이 마련될 것 (현재와는 전혀 다른, 바람직한 소프트웨어 인력 상황 및 시장 형성)

2. 규제자/정부의 역할 및 임무를 제대로 이해하고 재규정할 필요

- 해서는 안될 일 (잘못된 규제)
  - 기술에 개입하거나, 특정 기술 사용을 강요하는 행위는 금물
  - 서버측 보안에 대하여 “정부가 검증/점검해 주겠다”는 발상은 금물: 금융위/금감원이 형식적으로 수행하는 보안성 심의, 인증방법 평가위원회 제도 등은 폐지
    - 정부가 본격적 보안 점검을 해줄 역량이 사실은 없다는 점을 솔직히 직시할 필요
- 해야 할 일 (규제자의 정당한 역할과 임무)
  - 전자금융 사고거래 현황을 정확, 신속히 파악, 적절한 수준에서 공유/공표
    - 금융소비자 피해구제가 적정하게 되는지 모니터링하는데 필요
    - 공격에 대한 대응책 연구 개발에 필요
  - 금융회사들이 서버측 보안의 기술적, 관리적 측면에 대하여 전문성과 독립성이 있는 제 3 자(보안점검 전문 업체; audit practitioners)의 본격적인 보안 점검을 매년 받도록 지도
    - 현재와 같이 금감원이 형식적으로(서면에 근거하여) 수행하는 일회성 보안성 심의는 폐지하는 대신, 전문적인 민간 보안점검 서비스 시장이 활성화할 수 있도록 지원.

3. 집단 소송제 도입 필요

서버 관리 부실로 인하여 발생하는 개인정보 유출사고 피해에 관하여 집단소송제 도입

- 서버 보안 투자를 자연스럽게 유도하는 방안이 될 것임.
- 전문적, 독립적 업체로부터 보안 감사를 받지 아니하는 금융회사는 사고발생시 배상책임이 특히 높게 책정될 가능성이 높아질 것임.

다. 비용에 대한 고려

"그동안 잘 운영되어 오던 전자금융거래 인프라를 일거에 바꾸려면 막대한 비용이 든다"는 반론을 예상할 수 있는바,

- 거듭 발생하는 대형 보안 참사는 현재 사태가 심각한 보안 파탄 상황에 놓여 있음을 입증하는 것임. "그 동안 잘 운영되어 왔던 것"이 결코 아님.
- "일거에 바꾸라"는 것도 아님:
  - 정부가 규제 전략을 신속히 바꾸어주면,
  - 관련 업계의 인프라와 기술 상황이 점진적, 자발적으로 개선, 변화할 수 있다는 뜻임.
- "막대한 비용이 든다"는 것도 근거가 없음.
  - 지금까지는 정책의 실패로 인하여 보안투자 인센티브가 제거, 위축되어 있던 상태
  - 규제 전략의 변화로 인하여, 개별 금융회사들의 '자발적'인 보안 투자 활성화가 이루어진다면 관련 산업 및 시장의 성장, 발전, 일자리 창출을 뜻하는 것이므로 오히려 바람직.

1. 정부가 새로운 보안 기술을 공급하라는 것이 아님.
   - 정부주도의 관치 보안 정책 및 규제를 바꾸라는 것임. 이것은 비용이 드는 것이 아님.
   - 배상 책임을 지지도 않을 정부가, 금융회사들에게 "이 기술 쓰라"고 강요해 놓고 대형 사고가 나도 책임을 안지는 부당한 규제권 남용행위를 중단하라는 뜻.
   - (1)보안 기술 선택은 금융회사가 자신의 책임으로 하고, (2)사고 거래에 대한 책임은 금융회사에게 철저히 묻고, (3) 금융회사의 서버보안 상황에 대해서는 보안점검 전문업체로부터 본격적인 보안 감사를 매년 받도록 지도하라는 뜻.
2. 모든 금융회사들이 일거에 보안 기술을 바꾸어야 하는 것이 아님.
   - 공인인증서 위주의 현행 보안 솔루션을 그대로 유지하기를 원하는 금융회사는 자기책임으로 그렇게 하면 됨. 공인인증서를 금지하라는 뜻이 아님. 공인인증 관련 업체 '연착륙' 가능.
   - 다른 첨단 보안기술이 더 안전하고 효율적이라고 판단하는 금융회사는 그러한 기술을 채택하고, 공인인증서를 사용하지 않을 자유/자율을 부여하라는 뜻 ==> 고급기술 시장진입 가능
   - "공인인증서를 사용했으니, 책임 없다"는 식의 부당한 면죄부는 이제 그만하라는 뜻.
3. 규제 개선으로 보안 기술의 경쟁적 발달, 서버 보안 점검 서비스 시장 활성화를 통하여 전자상거래가 글로벌 수준으로 안전, 간편해지면, e-commerce 및 S/W 관련 산업의 폭발적 성장, 세계진출 가능.
   - 13 년간의 정책 실패를 교정함으로써 '창조 경제'가 무엇인지를 보여줄 수 있는 쇼케이스.

폐쇄적 “ IT 정책”의 구조

인증·보안 기술의 사례

김 기 창

고려대학교 법학전문대학원

2011.10.26

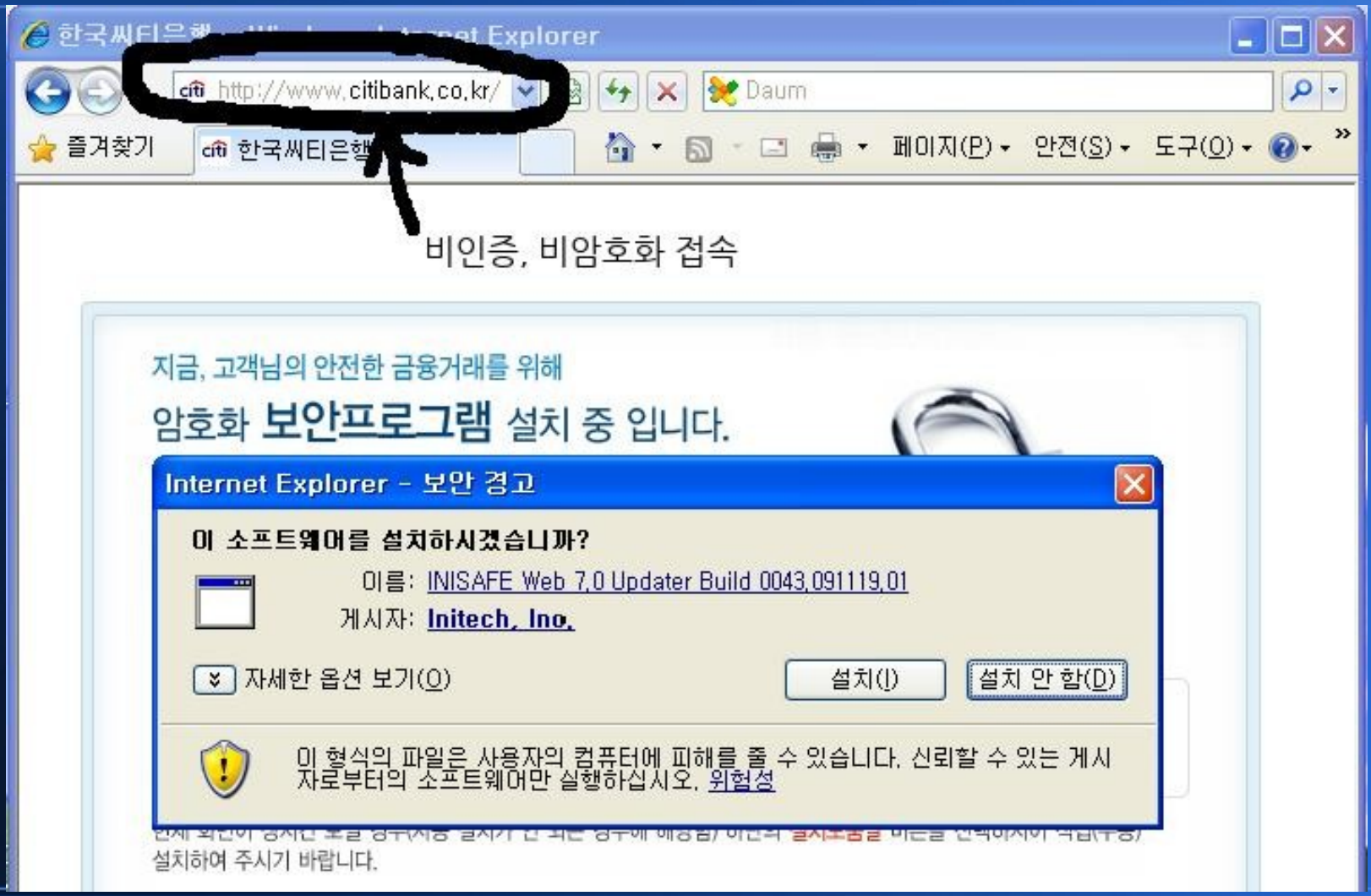
90 년대 말 상황

- 암호기술에 대한 정책적 오류 (세계 각국)
- 웹브라우저의 암호화 강도 문제점
  - 미국내 : 128bit
  - 미국외 : 40bit
- 1999 년 국내 기술진 (ETRI) SEED 알고리즘 개발 : 고강도 (128bit) 암호 교신 가능
- 1999 년말 경 미국 정부 암호기술 수출 허용 : 2000 초부터 웹브라우저도 128bit 암호 교신

국내용 인증·암호화 교신

- Trust 에 대한 이해 부족
- “Lab 환경”을 전제한 Proof of concept 수준
- Plugin 기반
- X509 인증서를 사용하되 ,
  - 개인키를 SEED 로 암호화 해서 보관
  - 대칭암호화 cypher 를 플러그인으로 배포
- 서버인증 개념 부재 / 몰이해
- 클라이언트 인증서 개인키 관리 문제 외면

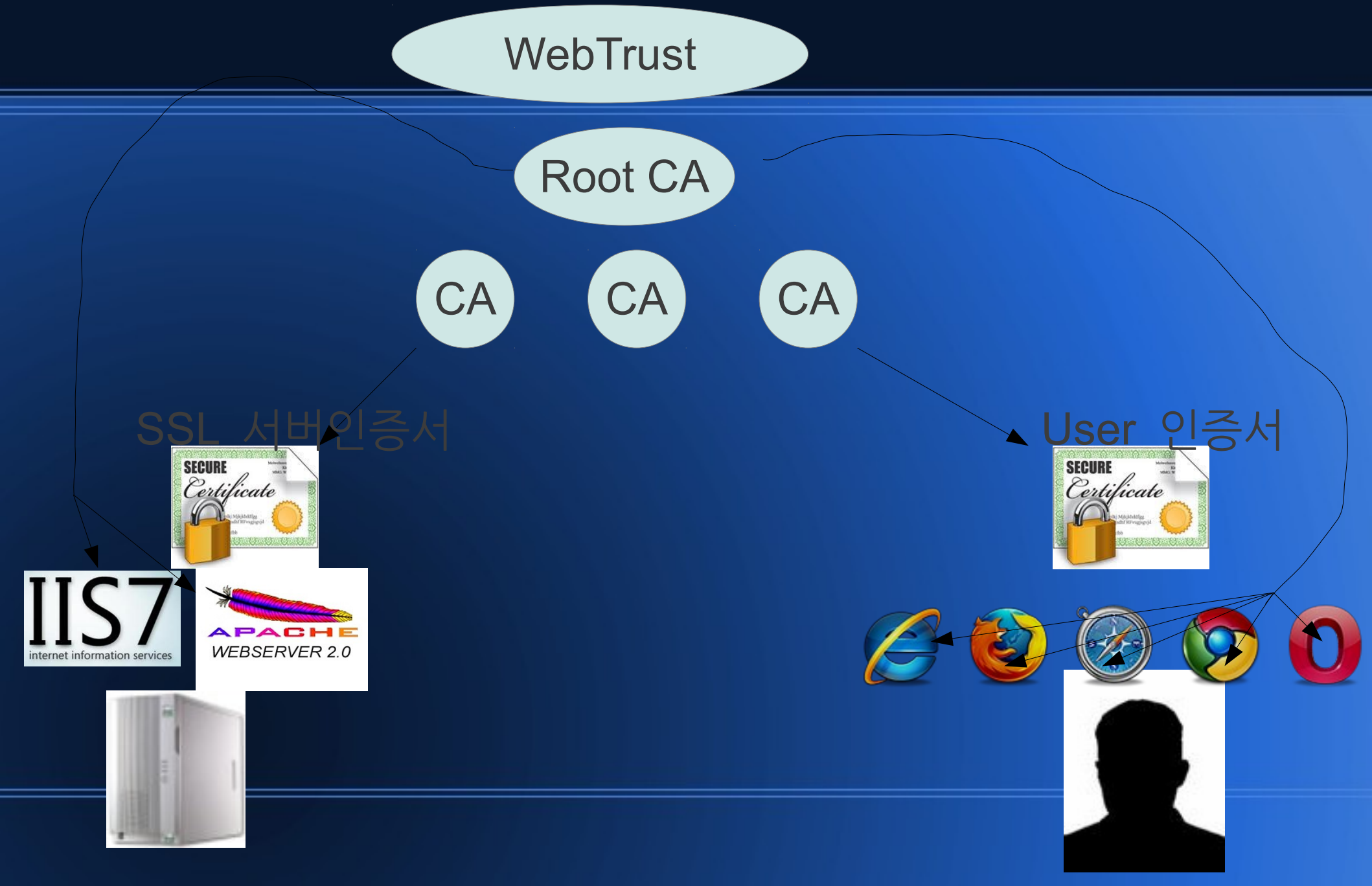
서버 인증 불가능


http://www.citibank.co.kr/
Daum
즐겨찾기
한국씨티은행
페이지(P)
안전(S)
도구(O)
비인증, 비암호화 접속
지금, 고객님의 안전한 금융거래를 위해
암호화 보안프로그램 설치 중 입니다.
Internet Explorer - 보안 경고
이 소프트웨어를 설치하시겠습니까?
이름: INISAFE Web 7.0 Updater Build 0043.091119.01
게시자: Initech, Inc.
자세한 옵션 보기(O)
설치(I)
설치 안 함(D)
이 형식의 파일은 사용자의 컴퓨터에 피해를 줄 수 있습니다. 신뢰할 수 있는 게시자로부터의 소프트웨어만 실행하십시오. 위험성
설치하여 주시기 바랍니다.

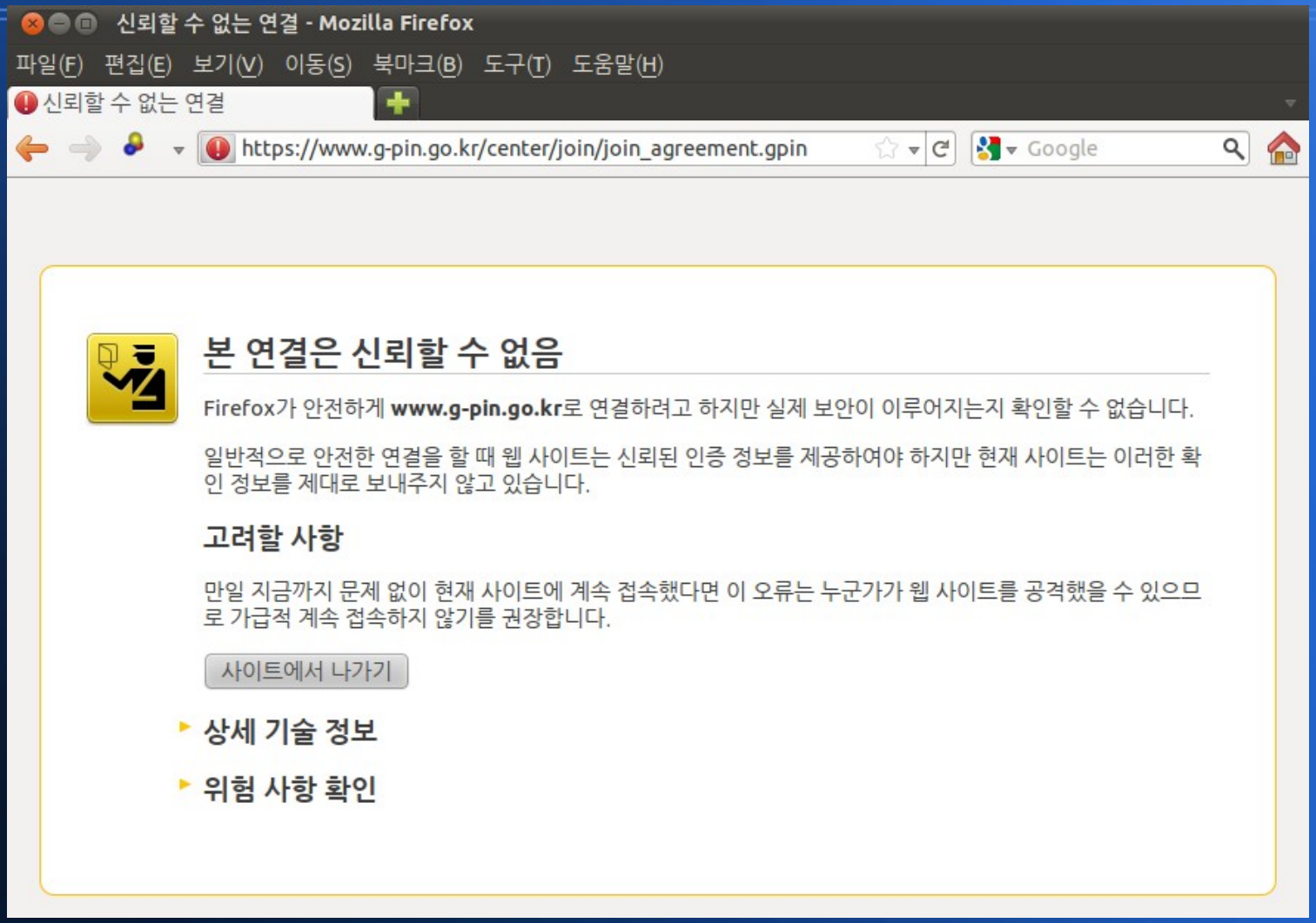
HTTP+Plugin 문제점

- 논리적 출발점 : HTTP 로 접속한 서버에 대한 '맹목적 신뢰' 강요 (플러그인 게시자 명칭 확인 ?)
- 플러그인 설치 단계에서의 proxy 공격 / 피싱 공격
- 서버 인증 불가능 : 플러그인 설치에 앞서서 (1) 유저가 서버를 맹목적으로 먼저 신뢰하고 (2) 플러그인을 설치하면 (3) 그 플러그인이 서버를 '뒤늦게' 인증하는 설계 구조
- 서버가 주는 플러그인이 그 서버의 위험성을 유저에게 알려줄 가능성은 없음 (100% OK).

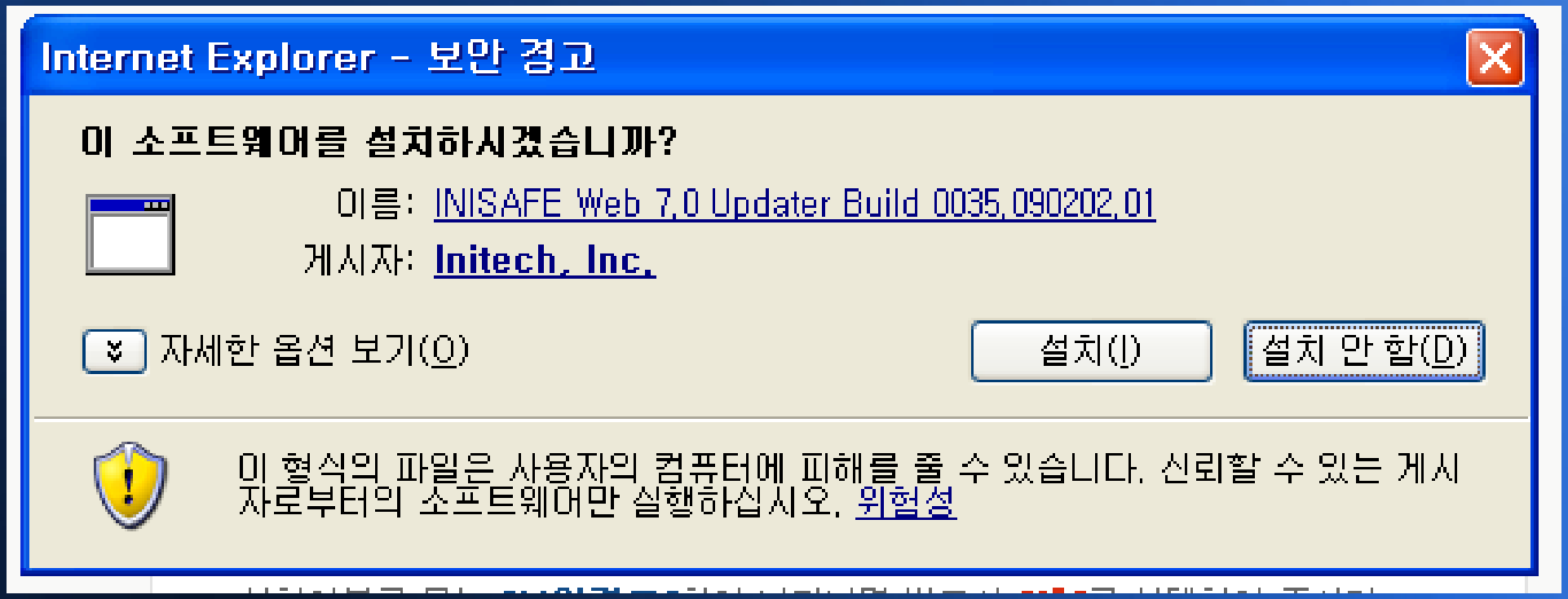
PKI 인증제도의 Trust 구조



국내용 인증의 한계 (서버인증 X)



국내용 인증의 문제 **(Client)**



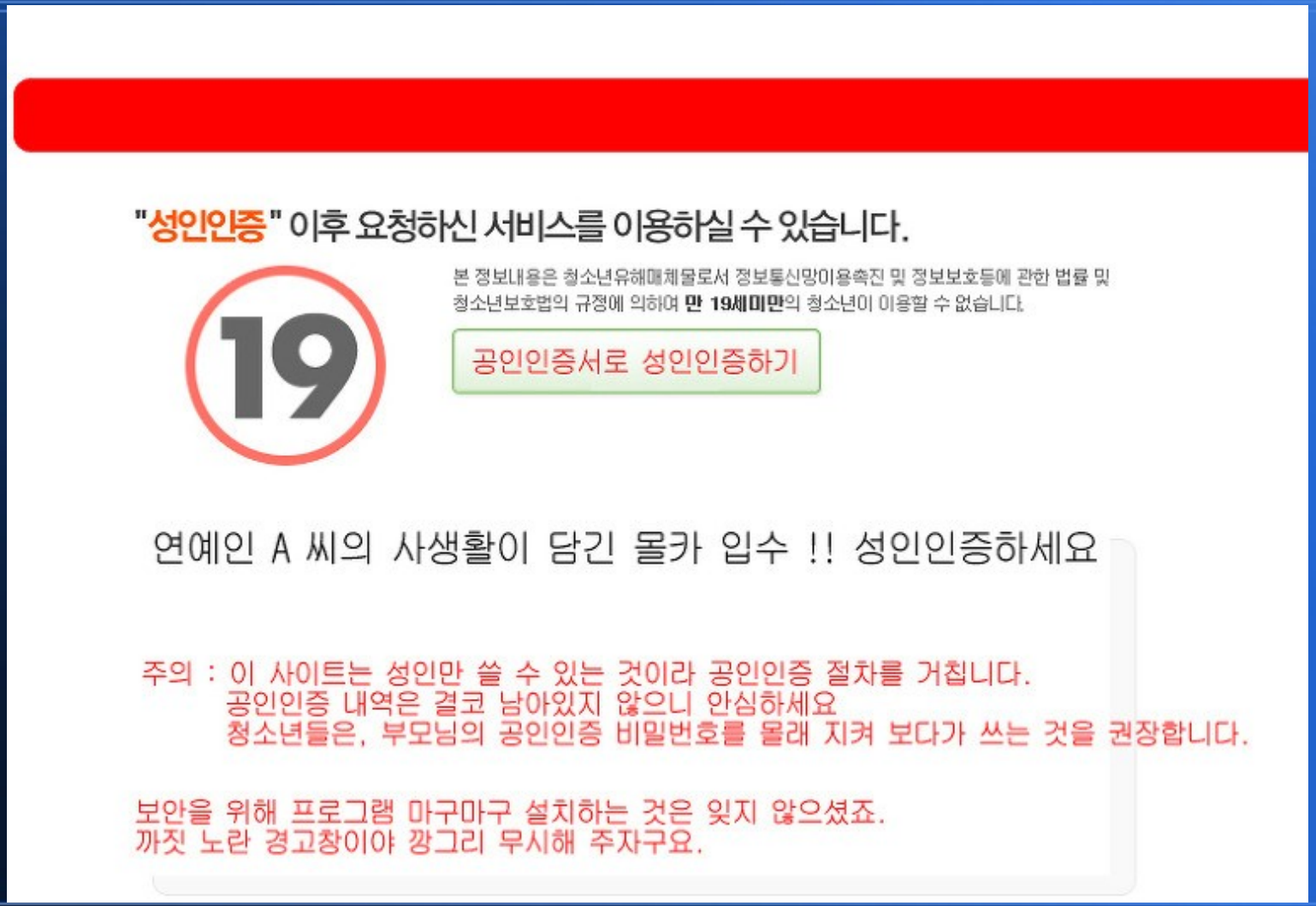
국내용 인증의 문제 **(Client)**

- 인증서 / 개인키 저장 : NPKI 폴더
  - 단순복사 가능 : 인증서 암호로만 보호
  - 해당 PC 를 이용하는 모든 유저에게 노출
  - 아이폰 / 안드로이드폰에서의 제약 / 취약점
- Plugin 필요 : 클라이언트 / 서버 플러그인
  - 비용 : 배포 / 설치 / 유지 / 관리 어려움
  - 유저행태 : “ 닥치고 OK”!
  - Plugin 안전성 검증 곤란 / 불가

“ 보안 프로그램” 설치 강요

- 금융감독원의 “보안 프로그램 3 종 세트”
- 고정 암호에 의존하는 인증서 개인키 파일 보호 ?
- Keystore 바깥에 존재하는 인증서 개인키 파일
- 개인키 파일 보호를 위한 여러 선진기술에 대한 이해 부재 / 구현 곤란 :
  - Gnome Keyring, iPhone Keychain
  - MS Crypto Keystore
  - Hardware SM

공인인증서 탈취 공격 : @blueori



HTML5 <keygen>

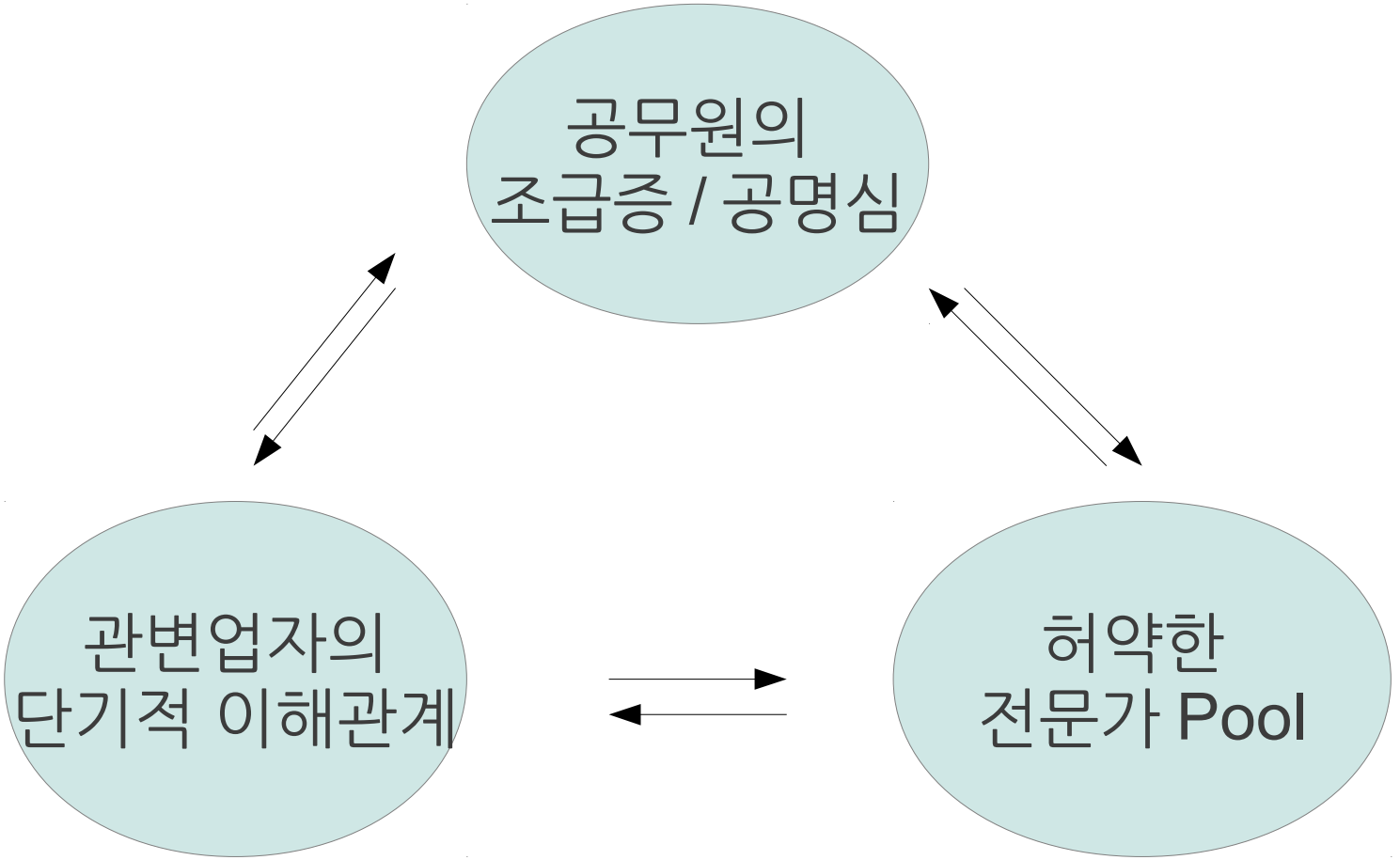
거래내역 전자서명

거래내역	A 는 B 에게 100 원을 송금합니다. 2010.4.15. 10:57:07
해쉬값	67e4efbfa58f778ca780e68c26281c369949260f
서명데이터	NzvMFxBwGFGIIKS7GI37AhWKCVvvP/kEuJc cHnrRZMbva/G4E2rRn4ULVX02qQFmuQ241U UGYRLvfpxCY/O1MJ4hla58qILSXByuscZnspA S7ra0VY2U03VHBUdGVJ8phXSicuqaseHJBN4 LNhqNbRqACogh6LwEKRjONbk59crv0XC0we ah+f9KGZJJowtIEDRp+Gv+SS2emXeJZKoJh2b vpf4/JD1dVQoBhgMRplOesGZtqimZutZMQGvf QN7amoJu5hQ5pHNpgfmRH7lnxECijua5WEOP syAkOd0mUU1l+c7NalCFXITBNDnND/Ijmnk9

“ 부인방지” : 법률과 기술의 차이

- 전자서명이 없어도
  - 문서로서의 효력 , 구속력 있음 (email, 문자메세지 등)
  - 전자서명 없어도 , 부인의 설득력이 없으면 부인 못함 .
- 전자서명이 있어도
  - ' 누가 ' 한 서명인지는 알 수 없음
  - 유저의 공인인증서 / 암호가 유출되어 공격자가 서명한 거래라는 주장이 설득력이 있으면 , 부인 가능
  - 금감원 " 명의도용 인터넷 불법대출 , 갚을 필요없다 "
  - 전자금융거래의 경우 : 개인고객의 중대한 과실 입증 필요

“ 진흥책”의 내막



- 정부개입 IT 환경 → 경쟁저해 , 기술혁신 말살

“ 진흥책”의 결과

- 누구를 위한 '공인' 인증제도인가 ?
  - 이익집단 형성
  - 국제기준 인증업체들 국내진입 장벽
  - 국내 보안 기술 시장의 고립 : red ocean
- 공인인증서 사용 강제 ?
  - 국내형 공인인증기술의 경쟁력 부재를 반증
  - 금융기관 / 이용자 / 인터넷사업자의 희생에 기반한 국내 보안업체의 영업모델
  - 규제 기관의 부처 이기주의 , 기득권 옹호 구조

SEED, PKI 강제 , 10 년 후 ...

보안의 뿌리 '암호'가 사라진다

(전자신문 , 2011.10.21 보도)

정부 무관심에 한국 제안 국제표준 퇴출 위기

“ 국내 암호 분야 연구가 정부와 학계의 관심 소홀로 뿌리가 흔들리고 있다 . 정부기관조차 암호연구팀을 줄이거나 폐쇄하는가 하면 , 우리나라가 제안해 국제표준화한 SEED 암호화 알고리즘은 무관심 속에 시장경쟁에서 밀려날 위기에 처했다 .”

은행감독에 관한 바젤 위원회

- 기술 중립성 / 다양성

... 구체적 위험에 대비한 특정 기술 해법을 강제하거나 전자금융 거래의 기술 표준을 정하려는 것이 아니다 . 기술적 사안은 금융기관들과 각종 표준화 기구들이 기술 진보에 상응하여 지속적으로 대처할 사안이다… 이런 이유로 , 본 위원회는 전자금융 위험 관리를 “획일적 해법으로 (one size fits all)” 대처하는 것이 적절하다고 믿지는 않는다 .

- 은행의 기술 선택권

은행은 PIN, 암호 , 스마트카드 , 생체정보 , 디지털인증서 등을 포함한 다양한 인증 기법을 사용할 수 있다 . … 어떤 인증 기법을 사용할 것인지는 전자금융 ... 위험에 대한 경영진의 평가에 기초하여 **은행이 결정하여야 한다** .

http://www.bis.org/publ/bcbs98.pdf

공인인증서의 보안 수준 ?

Table 2. Token Types Allowed at Each Assurance Level

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token (공인인증서)	√	√	√	
Passwords & PINs	√	√		

* 미국 국립 표준기술 연구소 (NIST), “Electronic Authentication Guideline”, p. 39

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/

전자금융감독규정 제 3 장 (현행 감독규정 제 7 조-제 41 조)의 개정 방향 [예시]

[금융위원회 고시]

제 3 장 전자금융거래의 안전성 확보 및 이용자 보호

제 1 절 규제자의 임무

제 7 조(금융소비자 보호) 금융위원회와 금융감독원은 전자금융 서비스가 기술 발전을 반영한 합리적 방법으로 안전하게 제공되고, 전자금융거래와 관련된 분쟁이 신속하고 정당하게 해결되도록 하여 금융소비자가 적절히 보호되는데 필요한 감독을 수행한다.

제 8 조(금융회사 등의 책임성 확보) 금융위원회와 금융감독원은 금융회사 등이 우월적 지위를 남용하거나 법령이 정한 책임을 부당하게 소비자 또는 다른 사업자에게 전가하거나 회피하지 않도록 하는데 필요한 감독을 수행한다.

제 9 조(기술 및 서비스의 자유로운 경쟁과 발전) 금융위원회와 금융감독원은 전자금융거래 서비스 제공에 사용되는 거래기술, 보안기술 및 보안감사 서비스가 활발하고 공정하게 경쟁하고 발전할 수 있는 시장 환경이 손상되지 않도록 감독을 수행한다.

제 10 조(규제의 투명성 및 형평성) 금융위원회와 금융감독원은 전자금융거래 서비스와 관련된 정보가 적절한 수준에서 투명하게 공개되고 규제의 형평성이 유지되도록 한다.

제 2 절 금융회사 최고 경영진의 책임

제 11 조(관리 감독 체계의 확립) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 관한 위험을 관리하고 책임소재를 분명히 하는데 필요한 관리 감독 체계를 자체적으로 확립하여야 한다.

제 12 조(일괄 위임의 금지) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업에 적용되는 보안 통제 절차의 핵심적 사항을 직접 검토하고 승인한다.

제 13 조(외주 계약 관계 등의 점검과 관리) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업이 외주 계약 관계 등 제 3 자에게 의존하는 부분에 대하여 적절히 점검하고 관리하는데 필요한 상시적 체계를 수립한다.

제 14 조(직원의 훈련 및 교육) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 수반되는 위험을 관리하는데 필요한 인력을 충분히 확보하고 그들에 대한 상시적이고 정기적인 훈련 및 교육 프로그램을 마련한다.

제 3 절 보안 통제 조치

제 15 조(적절한 인증기술의 채택) 금융회사 등은 거래의 성격과 해당 거래에 수반하는 위험의 수준을 고려하여 업계의 기술 수준을 반영한 합리적인 당사자 인증 기술을 채택하여야 한다.

제 16 조(분쟁 예방 및 대처) 금융회사 등은 거래 내용을 고객이 분명히 이해할 수 있도록 유저 인터페이스를 설계하고, 거래의 주체와 거래의 내역을 신뢰성 있는 방법으로 확인하고, 거래 데이터가 변조되지 않도록 하며, 변조 여부를 판별하는데 필요한 합리적 조치를 채택함으로써 전자금융거래와 관련된 분쟁을 예방하고, 분쟁에 대처하여야 한다.

제 17 조(업무 권한의 분할) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램의 운용에 있어서 각 직원의 임무가 적절히 분리, 분할되도록 하는데 필요한 조치를 취함으로써 자신의 전자금융 업무가 직원들 간에 상호 검증될 수 있도록 해야 한다.

제 18 조(접근, 출입 권한의 통제) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램에 대한 접근 권한 및 출입 권한 통제가 적절히 이루어지도록 함으로써 각 직원이 자기 권한을 스스로 변경할 수 없도록 하며, 업무권한의 분리, 분할을 통한 상호 검증 체계가 우회되지 않도록 해야 한다.

제 19 조(거래 기록 등의 보호) 금융회사 등은 전자금융거래 내역, 거래 기록 등의 정보가 변경되지 않고 보존될 수 있도록 하는데 필요한 조치를 마련하여야 한다.

제 20 조(검사 이력 및 증거 확보) 금융회사 등은 고객의 모든 전자금융거래에 대하여 감사/검사 이력(audit trails)이 남도록 하고, 법원에 제출될 수 있는 증거자료를 평소에 확보하고, 증거자료가 사후에 변조되지 않도록 하는데 필요한 적절한 조치들을 상시로 취해야 한다.

제 21 조(고객의 비밀 보호) 금융회사 등은 전자금융거래 내역의 비밀성을 유지하는데 필요한 적절한 조치를 마련하여야 한다.

제 4 절 법적 책임 및 평판에 관한 사항

제 22 조(고객에게 제공되어야 할 정보) 금융회사 등은 고객이 거래할지 여부를 제대로 판단하는데 필요한 정보(명칭, 규제상황 등)를 적절히 제공하여야 한다.

제 23 조(개인정보보호) 금융회사 등은 고객의 개인정보를 법령에 따라 준수하여야 한다.

제 24 조(사업지속에 필요한 대비책) 금융회사 등은 전자금융 서비스가 상시 제공될 수 있도록 사업규모, 사업지속 및 비상 대책에 관한 사전 기획 절차를 마련하여야 한다.

제 25 조(재난 회복 및 사고 대응책) 금융회사 등은 전자금융 서비스에 대한 내부자의 공격이나 외부자의 공격 등 불의의 사태를 관리하고 피해를 최소화 하는데 필요한 사고 대응책을 적절히 개발하여 시행한다.

제 26 조(사고 보고 및 분쟁절차 모니터링) 금융감독원은 전자금융 사고거래의 내용과 규모를 정확히 파악하고, 공평하고 신속한 분쟁해결을 위하여 다음 조치를 취한다:

1. 전자금융 서비스와 관련된 소비자의 불만, 이의, 환불신청 등을 통합적으로 접수할 수 있는 페이지(금융소비자 보호페이지)를 금융감독원이 관리하고, 각 금융회사는 이 페이지의 링크를 자신의 홈페이지에 게시한다.
2. 금융감독원은 금융소비자 보호페이지를 통하여 접수된 소비자의 불만, 이의, 환불신청을 해당 금융회사 등에 이첩하고, 분쟁해결 과정을 모니터링 한다.
3. 금융감독원은 각 금융회사 별 사고거래의 내용과 규모를 신뢰성 있는 방법으로 파악하여 보안기술의 연구 개발 및 서비스 품질 향상에 필요한 한도에서 적절한 수준과 방법으로 공표한다.

제 5 절 보안감사 서비스

제 27 조(정기적, 전문적, 독립적 보안감사) ① 금융회사 등은 다음 중 하나의 보안점검 기준에 따른 보안감사를 수행할 전문성과 독립성이 있는 보안감사 업체와 계약을 체결하고 보안감사를 년 1 회 이상 받아야 한다.

1. PCI DSS 등 국제적으로 인정받는 금융거래 보안 기준
2. 금융감독원이 공표하는 별지의 보안 기준(금융감독원 데이터 보안 기준; Korea Financial Supervisory Service Data Security Standards)(이하, FSS DSS 라 함)

② 금융감독원은 FSS DSS 의 지속적인 업데이트 및 국제화 작업, FSS DSS 기준에 따른 보안감사 서비스 제공자의 자격 요건 및 품질 관리에 필요한 업무를 지원한다.

제 28 조(신규 솔루션에 대한 제 3 자 검증) ① 금융회사 등이 전자금융 거래 솔루션을 신규로 채용할 경우에는 독립적이고 전문적인 보안감사 업체의 검증을 받고, 그 검증 보고서를 해당 서비스 개시 후 6 개월 이내에 금융감독원에 제출하여야 한다.
② 전항의 검증 보고서는 해당 금융회사의 웹사이트에도 공지하여야 한다.