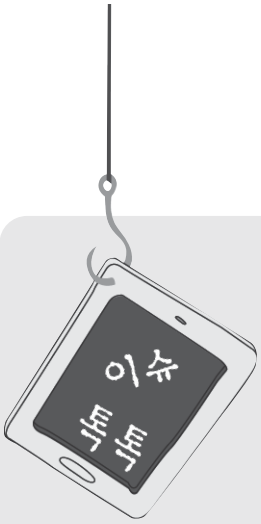


한국의 IT 보안은 새출발이 필요하다

김기창 • 고대 법대 교수, 오픈넷 이사

공인인증서, 어떻게 시작되었나

1990년대 말까지 미국 정부는 고강도 암호화 기술의 해외 수출을 금지하는 정책을 취했다. 따라서 미국 외에 배포되는 웹브라우저들은 저급한 수준(40bit)의 암호화 교신 기능만을 가지고 있었다. 당시 정보통신부와 한국전자통신연구원(ETRI)은 금융, 전자상거래 등 민감한 정보가 오가는 거래를 온라인으로 수행하기 위해서는 '고강도' 암호화 기술이 필요하고, '독자적' 암호 기술은 군사적 유용성도 있다고 판단하여 정부 차원의 암호화 기술 개발 지원이 이루어졌다. 이런 노력의 결과, 1999년 ETRI는 당시로는 높은 수준에 해당하는 128bit 길이의 키를 사용한 대칭 암호화 알고리즘(SEED) 개발에 성공했다.

그러나 독자 개발한 SEED 알고리즘을 이용한 고강도 암호화 접속은 웹브라우저와는 별도로 유저가 자신의 컴퓨터에 설치해야 하는 부가 프로그램(플러그인)에 의존해야 했다. 웹브라우저 자체에서

는 저강도 암호화만을 제공하고 있던 당시에는 이렇게 '별도 프로그램'을 유저들에게 나누어주고, 이것을 사용하여 고강도 암호화를 하면 된다는 식의 사고방식은 '간명한 해법'이라고 모두들 여겼다.

하지만 다음과 같은 두 가지 사정은 이런 해법을 당장 무의미하게 만들 뿐 아니라 매우 위험하게 만들었다.

첫째, 한국의 암호화 기술이 국제적으로 알려진 직후, 미국 정부는 암호 기술의 미국 외 수출 규제를 철폐했고 2000년 5월부터는 전 세계에 배포되는 웹브라우저 자체가 128bit 암호화 교신 기능을 구비하기 시작했다(지금은 그보다 훨씬 강력한 256bit 암호화를 웹브라우저가 기본으로 제공하고 있다). 정보통신부의 지원으로 ETRI가 1999년에 개발한 128bit 암호화 기술은 보안 강도 면에서도 이제 오히려 저급한 수준의 기술로 전락했다.

둘째, 1990년대 말의 기술 수준으로는 웹서버가 유저에게 '별도 프로그램'을 나누어주고 이것으로 암호화를 하면 된다고만 생각했을 뿐, 그것이 초래하는 보안 위험에 대하여는 별 문제의식이 없었다. 하지만 유저들에 대한 해킹 공격은 2000년대에 폭발적으로 증가했다. 따라서 유저들이 웹 서핑 과정에서 웹사이트가 내려주는 어떤 프로그램을 자신의 컴퓨터에 설치하는 행위 자체가 엄청난 보안 위험을 초래한다는 사실을 깨닫게 되었다. 악성코드가 바로 이런 방법으로 전파되기 시작한 것이다.

한국 기술진이 '독자적'으로 개발한 고강도 암호화 기술을 사용해야 할 기술적, 사업적 이유는 전 세계 모든 웹브라우저들이 이미

그와 같은 수준의 암호화 접속 기능을 '기본 탑재' 하기 시작한 2000년 5월부터는 없어졌고, '별도 프로그램' 을 유저의 컴퓨터에 설치해야 하는 기술은 매우 심각한 보안 위험을 초래하므로 오히려 사용하지 말아야 할 이유가 생겼지만, 한국 정부와 국내 최상위 공인인증기관인 한국인터넷진흥원(KISA)은 '별도 프로그램 설치' 가 필요한 한국형 공인인증 기술규격을 고집했다. 128bit 암호화를 위해서는 이미 쓸모도 없게 된 기술이지만, 암호화 기술에서 '한때' 세계 수준에 도달했었다는 헛된 자부심이 작용했고, 공인인증기관이라는 제도를 법으로 만들면서 생겨난 여러 기득권 구조가 기술의 변화를 따라잡기는커녕 기술 진전을 외면하면서 제도적 강제에 의존하기 시작한 것이다.

'한국형' 공인인증 기술의 특징

(1) '독특한' 저장 위치

공인인증서('한국형' 인증서)는 NPKI라는 이름의 폴더에 저장된다. USB 저장장치에 공인인증서를 저장한 사람은 USB 폴더 내에 NPKI라는 이름의 폴더가 보일 것이다. 컴퓨터 하드디스크에 저장할 경우, 그 위치는 C:\Program Files\NPKI 폴더거나(윈도우XP 운영체제의 경우), %UserProfile%\AppData\LocalLow\NPKI이다(윈도우 비스타 이후).

유저의 인증서를 이런 위치에, 이런 방법으로 저장하는 경우는 전 세계에 유례가 없다. 그로 인하여 다음과 같은 문제가 생긴다.

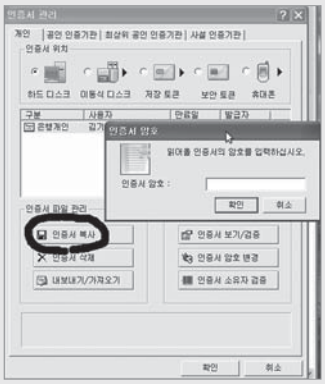
우선, 어떤 웹브라우저도 이렇게 저장된 유저 인증서를 인식할 수는 없다. 그렇기 때문에 '부가 프로그램'을 유저가 자신의 컴퓨터에 설치해야 하고, 웹서버 또한 서버 측의 부가 프로그램을 설치해야 한다.

둘째, 유저들이 공인인증서 사용에 필요한 부가 프로그램을 '구입' 해야 하는 것은 아니지만, 서버들(금융기관 등)은 이런 프로그램을 국내 보안업체들에서 구입해서 유저들에게 배포해야 한다. 웹브라우저가 인식할 수 있는 위치와 방법으로 유저의 공인인증서를 저장했더라면 유저들이 부가 프로그램을 자신의 컴퓨터에 설치해야 할 필요도 없고, 서버가 비싼 가격으로 공인인증 솔루션을 구입하지 않아도 되지만, 저장 위치를 독특하게 정해둠으로써 국내 보안업체들이 이 솔루션을 금융기관에 판매하고 영업할 수 있도록 해주고 있는 것이다.

셋째, 공인인증용 부가 프로그램의 안전성을 제대로 검증할 방법이 없다. 은행이 이 프로그램의 안전성을 검증할 역량이 있는 것도 아니고, 소스가 공개되지도 않기 때문에 국제 무대에서 검증받을 기회도 없다. 오로지 제작 업체의 기술력과 윤리성에만 전적으로 의존하여 온 국민이 자신의 컴퓨터에 이들 프로그램을 설치해야 하며, 이 프로그램이 유저의 컴퓨터에서 수행하는 작업이 정확히 무엇인지는 투명하게 공개되어 있지 않다. 요컨대, 보안업체를 무작정 믿으라는 것이다.

(2) 무단 복제가 쉽게 가능

보안 업체들과 금융기관들은 하드디스크에 있는 공인인증서를 USB로 복사하거나, USB에 저장된 인증서를 하드디스크에 복사할 때에는 (1) 은행이 운영하는 '공인인증센터'에 접속하여 공인인증용 부가 프로그램을 설치하고, (2) 그 웹사이트의 안내에 따라서 공인인증서를 '복사'하도록 안내하고 있다. 공인인증서를 복사하려는 유저는 이때 인증서 암호를 반드시 입력하도록 되어 있다(그림1 참조).



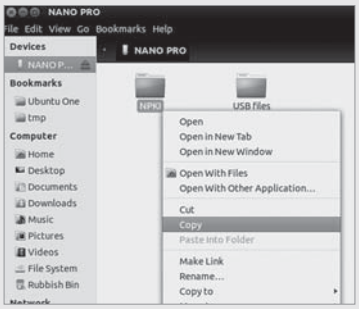
〈그림1〉 공인인증서를 복사하려면 인증서 암호가 필요한 것 같지만 실은 전혀 필요치 않다.

'인증서 암호를 모르면 나의 공인인증서를 다른 사람이 함부로 복사해갈 수 없으니 안전하겠구나"라고 생각할 이용자가 많을 것이지만, 실은 이런 절차를 거칠 필요도 없이 공인인증서는 쉽게 복사된다. 공인인증서가 저장된 NPKI 폴더를 단순히 복사해서 붙이기(copy+paste) 하면 아무 곳으로나 마구 복사되기 때문에 암호를 입력하라는 것은 순전히 '쇼'에 불과하다. 컴퓨터 지식이 전혀 없는 이용자라면 NPKI 폴더가 어디 있는지조차 모르기 때문에, 하라는 대로 부가 프로그램을 설치하고 암호를 입력하겠지만, 이런 이용자를 상대로 '암호 입력'을 하게 만들어서 거두는 효

과는 고작해야 컴맹들을 상대로 한 눈속임일 뿐, '보안'과는 무관하다.

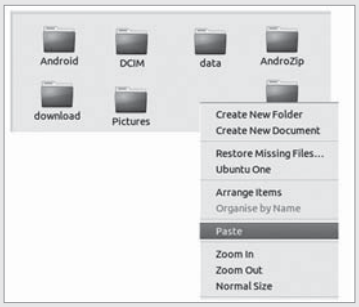
공인인증서를 스마트폰으로 이동하는 절차 역시 비슷한 문제가 있다. 국내 스마트폰 사용자 10명 중 7명이 사용하는 안드로이드 폰의 경우, 공인인증서를 스마트폰에 복사하는 "솔직한" 방법은 다음과 같다.

첫째, 인증서가 담긴 USB를 PC에 꽂는다. 거기에 있는 NPKI 폴더를 '오른 클릭'하여 복사한다.(그림2 참조)



〈그림2〉

둘째, 안드로이드 폰을 PC에 연결한다. 폰 화면 상단에 USB 아이콘이 뜨는데, 이것을 쓸어내려 스마트폰이 USB 대용량 저장장치로 인식되게 선택한다. 그러면 스마트폰 SD 카드 폴더들이 대충 '그림3'처럼 나타나는데, 그중 빈 공간에 마우스를 '오른 클릭'해서 조금 전에 복사해둔 NPKI 폴더를 붙여넣는다.



〈그림3〉

이렇게 하면 공인인증서가 스마트폰으로 복사된다. 이런

사실을 설명하기는커녕, ActiveX를 설치하라, 8자리 인증코드를 입력하라, 주민번호를 입력하라, 비밀번호를 입력하라, QR코드를 찍으라 등의 온갖 복잡한 과정을 거쳐가도록 이용자들을 '유도' 하는 이유가 무엇일까? 컴퓨터 지식이 전혀 없는 무지한 일반인들을 상대로 "공인인증서는 워낙 안전해서 복잡하고 까다로운 절차를 거쳐야 비로소 스마트폰으로 '이동' 할 수 있다"는 그릇된 환상을 유지하기 위해, 한마디로 "보안 코스프레"를 하는 것이다.

(3) 더 많은 부가 프로그램 설치 필요

공인인증서는 이처럼 무단 복제가 매우 쉽기 때문에 유저의 컴퓨터에 대한 침입 공격이 성공하게 되면 공격자는 당장에 유저의 공인인증서(개인키) 파일을 입수하게 된다. 따라서 인증서 개인키 암호를 어떻게 보호할 것이냐에 보안의 모든 것이 달려 있게 된다. 바로 이런 이유로 국내 금융기관들은 키보드 보안 프로그램 설치를 강제하고 있다.

하지만 인증서 암호는 유저가 정하는 것이고, 대부분의 유저들은 자신이 다른 여러 계정에서 사용하는 암호와 인증서 암호를 같이 정해두고 사용하고 있으며, 유저들이 다른 계정에서 입력하는 암호는 쉽게 유출되므로, 금융기관들이 아무리 키보드 보안 프로그램 설치를 강제해도 그 실효성은 기대할 것이 못 된다. 바로 이런 위험을 금융기관들도 스스로 인정하고, 유저들에게 인증서 암호는 다른 어떤 계정 암호와도 다르게 정해두고 사용하라고 계몽하긴 하

지만, 실제로 이런 권고를 실천하는 유저들의 비율이 높기를 기대할 수는 없다.

USB 저장장치에 공인인증서를 저장하면 마치 덜 위험해지는 듯 이야기하는 경우도 많으나, 이런 주장은 기술적 근거가 없다. 유저의 컴퓨터에 악성코드를 심는 데 성공한 공격자라면, 유저의 하드디스크에 NPKI 폴더가 없다고 해서 당장에 악성코드를 스스로 지우고 철수할 이유가 없다. 유저가 USB를 삽입하는 순간, 그 사실을 감지해서 NPKI 폴더가 복제되도록 악성코드를 작성하는 것이 그리 어려운 것도 아니다.

요컨대, 공인인증서는

- 공격자가 복제해 가기 매우 쉬운 위치와 방법으로 저장될 뿐 아니라,
- 그런 공인인증서를 사용하기 위해 유저가 부가 프로그램을 자신의 컴퓨터에 설치해야 하고,
- 인증서 개인키 파일이 무단 복제되어 유출될 위험이 높기 때문에 인증서 개인키 암호를 보호하기 위해 키보드 보안 프로그램 등 여러 추가적 프로그램의 설치도 강요하지만,
- 유저들이 인증서 암호와 다른 계정 암호를 같게 정해두고 쓸 경우(대부분의 경우) 인증서 암호의 유출을 막을 방법도 없다.

법률의 오해

공인인증서의 이러한 기술적 취약점에도 불구하고, 국내 보안 업계

는 전자서명의 '법적 효력'을 거론하면서 마치 공인인증서 사용이 보안기술 면으로는 별 소용이 없지만, 법적으로 불가피한 것처럼 주장하기도 한다. 즉, 공인 전자서명이 있으면 당사자가 서명 날인한 것과 같은 '법적 효력'이 인정될 뿐 아니라, 나중에 당사자가 그 거래를 부인할 수 없게 할 수 있다는 것이다(이른바 '부인 방지' 효력).

그러나 전자문서라는 이유만으로 그 문서의 효력이 부인되는 것도 아니고(즉, '전자서명'이 되어야 문서로서 효력을 인정받는다는 주장은 근거가 없고), 오프라인상에서 종이로 이루어지는 거래에 서명 날인을 한다고 해서, 온라인상에서도 반드시 전자서명이 필요하다는 법리도 없다. 세계 각국에서 무수히 많은 금융거래가 전자서명 없이 이루어지고 있으며 이것이 무슨 '법적' 문제를 불러일으키는 것도 아니다. 국내법 역시 전자금융거래에는 전자서명을 해야 한다는 법률 규정이 있는 것도 아니다. 전자서명이 없어도 전자문서의 효력을 함부로 부인해서는 안 된다는 것이 한국법이고 외국의 법제도 마찬가지다.

기술 인력이 내세우는 이른바 '부인 방지'라는 개념은 천박한 법률지식에 근거하고 있다. 그들은 전자서명이 되면, 그 거래는 서명자가 한 거래로 추정된다면서, 전자서명법 제3조 제2항을 거론하고 있다. 해당 조항은 다음과 같다.

② 공인 전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명

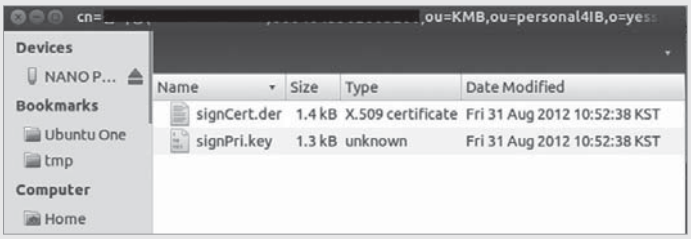
된 후 그 내용이 변경되지 아니하였다고 추정한다.

그러나 이 조항을 적용하려면 우선 '공인 전자서명'이 무슨 뜻인지를 알아야 한다. 전자서명법 제2조 제3호는 '공인 전자서명'으로 인정받으려면 다음 요건을 반드시 구비해야 한다고 정하고 있다.

가. 전자서명생성정보가 가입자에게 유일하게 속할 것
나. 서명 당시 가입자가 전자서명생성정보를 지배 · 관리하고 있을 것 [이하 생략]

여기서 '전자서명생성정보'란 인증서 '개인키'를 말하는 것이다. NPKI 폴더 하위에 자신의 공인인증서가 저장된 폴더 안을 열어보면 다음과 같은 두 개의 파일이 있음을 알 수 있다. 일반인이 '공인인증서'라고 부르는 것은 실제로는 이 두 개의 파일을 지칭하는 것이다. 그 중 'signPri.key'라는 이름의 파일이 바로 유저의 전자서명생성정보(개인키)이다.(그림4 참조)

유저의 개인키가 유저에게 "유일하게 속할 것", 그리고 유저가



〈그림4〉

"서명 당시 이 개인키를 지배 · 관리하고 있을 것"이라는 요건은 유저의 공인인증서가 무단 복제되어 공격자의 손에 놓이게 되면 애초에 충족될 수 없다. NPKI 폴더가 통채로 복사되고 인증서 암호가 유출된 상황이라면 그런 공인인증서로 아무리 전자서명을 해 본들 '공인전자서명'으로 인정받을 수는 없고, '공인전자서명'에 인정되는 '추정력'이라던가, '부인 방지' 효력이란 것은 아예 거론할 여지가 없게 된다.

상식적으로 보더라도, 나의 공인인증서를 공격자가 입수하여 그것으로 그자가 전자서명하여 거래한 경우, 내가 (1) 공인인증서를 고의로 유출시켰다거나 (2) 나의 공인인증서가 유출되는 과정에서 내가 매우 크게 잘못한 경우가 아니라면 그런 거래의 책임을 내가 져야 할 이유는 없다.

사고 거래는 고객의 공인인증서가 유출되었기 때문에 생기는 것이고, 이럴 경우(즉, 개인키의 배타적 지배가 더 이상 유지되지 않는 경우)에는 '공인전자서명'이라는 것이 아예 성립될 수가 없기 때문에 이른바 '부인 방지'니, 공인전자서명의 '추정력' 따위를 거론할 법적 근거가 없어지는 것이다. 공인인증서로 전자서명이 되어있기만 하면 고객이 책임을 져야 한다는 판례도 없고, 만일 그런 판례가 나온다면 그야말로 억울하기 그지 없을 것이다. 마구 복제되어 쉽게 유출되는 허술하고 위험한 공인인증서일망정, 그것으로 전자서명이 되기만 하면 무조건 본인이 책임을 져야 한다는 입장은 상식을 벗어난 것이다. 그것이 금융소비자를 보호하는 길도 아니고, 세계

어느 나라도 그런 법제도를 채택하지는 않는다.

공인인증서로 전자서명을 하게 하면 '부인 방지' 효과가 있다는 주장은 기술도 모르고 법도 모르는 사람의 무지한 환상일 뿐이다. 이런 주장은 결국 사고 거래의 책임을 금융 소비자에게 지우겠다는 해괴한 발상에 근거를 두고 있는데, 금융 소비자를 보호해야 할 금융감독 당국이 이런 입장을 고수하고 있다는 것은 아이러니의 극치라고 생각한다.

총체적 보안 난국을 극복하는 방안

부가 프로그램을 설치해야만 하는 공인인증서 때문에 한국의 유저들은 "보안경고창이 나타나면 반드시 '설치'를 눌러 진행하십시오"라는 안내를 받아왔다. 이것이야말로 한국을 해커들의 천국으로 만든 첩경이라고 생각한다. 악성코드를 퍼트리기 가장 좋은 환경을 보안 업체들이 앞장서서 조성해두는 셈이다. 한국 유저들의 좀비 PC 감염율이 세계에서 가장 높은 편에 속하게 되고, 전 세계 스팸메일 발송국을 조사하면 미국, 중국에 이어 한국이 3위를 차지하고 있으며, 유럽 지역 스팸메일의 경우, 한국이 발송국 1위를 차지한다는 사실은 한국 보안 업계에 대한 가장 신랄한 고발장에 다름 아니다. 국민 다수의 컴퓨터는 사실상 거덜난 것이다. 보안경고창을 가볍게 무시하고 "예"를 눌러 진행하도록 보안 업체가 전 국민을 '안내' 하면 이렇게 될 수밖에 없다.

오늘도 한국의 금융기관과 이동통신사는 이메일 첨부파일을 클

릭하면 ActiveX를 설치 또는 실행하라는 이른바 '보안 메일'을 고객들에게 보내고 있다. 악성코드를 전파하려는 공격자들이 쓰는 수법이 바로 이런 것이므로, '프로그램 설치/실행이 필요한 첨부 파일'을 이메일로 보내는 행위는 죄악에 가까운 짓인데도 이걸 '보안 솔루션'이라면서 납품하는 업체가 멀쩡히 영업을 하고 있다는 사실 자체가 바로 국내 보안 체계의 총체적 허술함과 윤리의식 부재를 입증하는 것이다. 물론 역설적으로 들리겠지만, 보안 업체는 바이러스로 영업하는 측면도 있다. 명색이 바이러스를 '치료'한다는 프로그램을, 바이러스 유포를 가장 많이 '조장'하는 배포 방식인 ActiveX 플러그인 형태로 배포하는 세계 초유, 전대 미문의 코미디가 지난 10여 년간 가능했던 이유는 단순히 기술적 '무지'로만 설명하기는 어렵다.

이런 총체적 보안 난국을 벗어날 해법은 없는가?

우선, 근본적인 원인은 정부의 잘못된 보안 규제에서 찾아야 한다. 공인인증서라는 낡고 허술한 기술을 지난 13년간 강제해오면서, 유저들에게 보안경고창이 뜨면 반드시 '예'를 누르라고 끈질기게 세뇌해온 것은 분명히 잘못된 것이다. 자신이 이해하지 못하는 프로그램을 함부로 설치하는 위험천만한 행위를 대수롭지 않게 여기도록 온 국민의 컴퓨터 이용 습관을 정부가 앞장서서 위험하게 만들고 나면, 어떠한 보안 해법도 소용이 없어진다.

유례가 없는 대형 사고가 거듭되는 국내 보안의 현 상황을 보면 더 이상 '예전 방식대로' 계속될 수는 없는 시점에 왔다고 생각한

다. 13년 넘게 계속된 공인인증/ActiveX에 의존한 국내 보안 체제의 소프트 랜딩(soft landing)을 고민해야 할 때다. 다음과 같은 해결 방향을 제시하고자 한다.

첫째, 공인인증서는 '선택(option) 사항'으로 전환되어야 한다. 더 이상 정부가 특정 보안 기술 사용을 '강요' 해서는 안 된다. 다양한 보안기술이 활발히 경쟁할 수 있어야 보안 기술이 발달한다.

둘째, 공인인증서 '저장 위치'는 NPKI 폴더가 아니라 웹브라우저가 인식할 수 있는 키 저장소(keystore)를 사용해야 한다. 그러면 부가 프로그램(ActiveX 등)을 설치 안하고 공인인증서를 이용할 수 있다.

셋째, 공인인증서 로그인은 유저가 원할 경우에 선택할 수 있도록 옵션(option)으로 제공한다. 하지만 '공인인증서만'으로 조회/이체거래 등을 할 수 있게 해서는 안 된다. 공인인증서는 이미 대량으로 유출되었다고 보아야 하며, 인증서는 유저의 'id를 확인' 하는 정도의 의미만을 부여하고, 계좌 조회, 이체 등에는 일회용 비밀번호가 사용되야 한다.

인증서 기술은, 비록 원리 자체는 이미 20년 전에 확립된 것이긴 하지만, 실제로 수많은 유저들에게 인증서 개인키를 어떻게 안전하게 배포하고, 어디에 어떤 방식으로 유저 인증서를 저장하는 것이 바람직한지에 대해서는 아직 무수히 많은 문제가 있는 미숙한 보안 기법이다. 하드웨어 보안토큰 형태로 유저 인증서를 배포하는 것도 많은 현실적 문제가 있다. 거래내역 전자서명에 대해서는 아직 아

무런 국제 표준도 없는 실정이다.

이러한 미숙 · 허술한 보안 기법을 1990년대 말의 기술 수준과 당시의 소박한 발상을 기반으로 '부가 프로그램'으로 대충 땜질하여 전 국민에게 지난 10여 년간 무식하게 강제한 결과 한국의 보안 상황은 더 이상 지탱하기 어려운 지경이 되었다고 생각한다. 공인인증서 사용을 강제하지 않고 '선택사항'으로 전환하는 것이 지금 우리에게 시급하게 필요한, 유일한 해결책이다.

보안 기술 분야에 정부가 개입하여 강제 규정을 만들 경우, 눈가림 보안, 규정 충족을 위한 보안, 타율적 · 억지춘향식 보안이 판을 치게 마련이다. 보안업체와 관련 기관은 진정으로 안전에 도움이 되는 조치를 상시로 취하는 것이 아니라, 규정이 요구하는 것만을, 규정상 요구되는 시점에만 조치한 다음(규정 충족에 필요한 최소한의 보안), 사고가 나면, "우리는 규정이 하라는 것은 모두 다 충족했다. 따라서 책임이 없다"는 발뺌이 통하게 되는 것이다.

공인인증서 사용이 강제되지 않으면 부가 프로그램을 설치하도록 강요되지도 않을 뿐 아니라, 다양한 웹브라우저와 운영체제가 국내에도 확산될 수 있게 된다. 지금처럼 국민 대다수가 동일한 웹브라우저를 사용하며 서너 개의 업체가 배포한 '보안 플러그인'이 온 국민의 컴퓨터에 깔려 있는 사태는 지극히 위험하다. 어떤 적대적인 세력이 마음만 먹는다면 특정 업체의 '보안 플러그인'을 통해 전 국민의 컴퓨터가 일거에 장악될 수 있다. 이런 위험한 여건을 정부가 스스로 초래해두고 있는 현 사태는 시급히 교정되어야 한다.