기 고

험난한 중국정보보안인증

'09.8.7 중국컴퓨터세계보 기자 : 王臻 (왕쩐)

정보보안인증의 험난한 길

얼마 전, 호주의 Rio Tinto社 상하이사무소 직원 4명이 중국 국가기밀을 훔친 혐의로 체포되었다. 이 4명은 중국 대외수출입철광석 협상기간에 정보를 유출했고 중국 철강업계에 7천억 위엔의 경제적 손실을 입혔다. 이 일은 중국의 기업정보 관리에 경종을 울렸고 인터넷안전 및 정보보안 문제를 전략적으로 접근할 필요성을 제시하였다.

정보산업의 빠른 발전과 정보화과정이 심화됨에 따라, 정보보안문제는 전 세계 공통의 관심사가 되고 있다. 정보보안 영역에서 통일된 인증제도로 정보시스템 안전을 보장하는 것은 각국에서 통용되는 방법이다. 중국도 예외가 아니다.
금년 4월 27일, 국가품질감독검험검역총국, 중화인민공화국 재정부, 중화인민공화국 국가인증인정감독관리위원회는 공동으로 〈정보보안제품 강제인증 실시에 관한 공고〉(2009년 제33호)를 발표하였다. 국가품질감독검험검역총국, 국가인증인정감독관리위원회는 〈일부정보보안제품 강제인증 실시에 관한 공고〉(2008년 제7호)에서 정보보안제품 강제인증의 실시를 2010년 5월 1일로 연기하며, 정부구매법 범위내에서만 실시한다고 발표했다. 인증제품의 범위는 방화벽, 인터넷 보안격리카드와 선로선택기, 보안격리와 정보교환, 보안라우터, 스마트 카드칩 운영체, 데이터백업 및 복구, 보안데이터베이스시스템, 스팸차단, 침입탐지시스템, 인터넷 해킹스캐너, 보안심사, 웹사이트 복구 등 13종 제품이다.

기자가 이해한 바로는, 〈일부정보보안제품 강제인증 실시에 관한 공고〉는 2008년 1월에 이미 발표되었으며, 1년 후 재정부와 공동으로 공고문을 조정 발표하였다. 원 공고문의 시행시기를 연기했을 뿐 아니라 정보보안제품 인증 대상도 정부구매법이 규정하는 범위로 한정한다고 했다.
세계적으로 정보보안의 중요성을 국가전략으로 제고시키고 있는 오늘날, 국가는 정보보안제품의 품질향상 및 국가정보의 보장을 위해 정보보안제품 및 정보네트워크 시스템의 보안에 대한 여러 가지 행정허가 및 인증 등 관리감독을 실시한다. 그러나 사실상, 중국 정보보안 인증의 길은 매우 험난하다.

"우방의 놀라움", 남의 이목을 현혹시켜 진위를 판단하지 못하게 하다

2008년 1월말, 〈일부정보보안제품 강제인증 실시에 관한 공고〉가 정식으로 발표되었다. 이 공고문에 따라서, 2009년 5월 1일부터 강제인증 목록에 있는 13종 정보보안제품 중 제품인증서를 취득하지 못하거나 중국 강제인증마크를 표시하지 않은 제품은 출고, 판매, 수입 또는 기타 경영활동을 할 수 없다.
이에 대해 수많은 외국의 질의와 보도가 이어졌고, 국제표준관련 조직과 산업협회에서 반대의 목소리도 높아져 관계부처는 매우 난감한 상황에 직면했다.

일부 미국의 주요매체는 다음과 같이 보도했다. '중국 정부는 외국정보산업체들이 정보보안기술제품에 대한 인증신청을 중국 관계기관에 할 것으로 여기며, 새로이 입안된 동 정책은 명백히 국가보안 뿐만 아니라 국내 정보기술 산업

두 측면을 고려한 것이다. ' 미국 싱크탱크전략 및 국제연구센터(CSIS)의 연구원은 심지어 이의 동기가 일부 무역적 측면 이외에도 산업스파이 문제를 포함하고 있으며, 중국 정부가 정보기술시장에서 자국회사를 지원하려는 계획을 포함한다고 했다. 그는 또한 '중국의 두 번째 동기가 명쾌하지 않다.' 고 했다.

〈일본 마이니찌신문〉은 '이러한 제도는 아마도 외국기업의 지적재산을 중국의 경쟁기업에게 제공할 우려가 있다.' '만일 중국 정부가 포기하지 않으면 장차 심각한 국제무역의 쟁점이 될 것이다.' 라고 했다.

이로 인해 2008년 9월 재미 중국상업무역연합위원회에서 미국정부 관계자는 동 정책에 대한 질의를 하였다. 주중 미국대사관의 대변인은 '미국은 중국이 계획하고 실시하는 새로운 규정이 무역관례상 적절하지 않다' 라고 지적했다. 이 질의에 대해, 국내 관계부처에서는 거듭 명확한 해명을 해야만 했다. '중국의 조치는 국가안보를 보장하고 정보기술 산업을 추진하기 위함이라고 했다.'

그러나 외국의 미디어들은 이 기회를 틈타 악의적인 보도를 하고, 심지어 사실왜곡까지 서슴치 않았으며, 중국의 관리제도까지 모함하였다. 정보보안 인증에 다년간 종사했던 전문가는 기자에게 '당시 관련된 외국보도에는 대대적인 허위보도로 가득했다' 고 말했다.

본 기자도 〈일본경제뉴스〉의 몇 백자분량의 원고에서 최소한 아래와 같은 허위사실을 발견했었다: '13종 강제인증제품의 목록' 을 '13개 컴퓨터 바이러스방지 강제인증표준' 으로 쓴 것, 또한 뜬금없이 '13개 규정 중 기반소프트웨어를 포함한다', '인증을 취득하려면 기업에게 소프트웨어 설계도의 소스코드를 공개하라고 할 것이다' 등 허위사실을 유포했다.

이러한 보도는 사람들로 하여금 판단을 흐리게 할 뿐 아니라 중국이 현재 확립하고 있는 정보보안제품 인증제도를 왜곡하는 것이다.

'우방을 놀라게 하는' 그리고 분명치 않는 말들로 인해 중국 관계부처는 번거로움을 마다않고 지속적으로 대화와 해명을 해왔다. 그 후 인증제도의 실시를 연기했다.

2008년 7호 공고문중 강제인증 실시대상 13종 정보보안제품을 명확히 밝혔으며 이는 많은 IT제품 중 극소수의 일부 정보보안 전용제품임에도 불구하고, 전혀 언급된 바 없는 디지털 가정용 전기제품, 디지털 복사기, 평판 TV 등 제품들이 외국의 보도에는 포함되어 있었다.

중국의 법률, 법규 및 인정제도 등에서 인증기관 및 시험기관은 반드시 고객의 비밀을 지켜야할 책임이 있다. 정보보안제품에 대한 인증 및 검사시 보안등급의 요건에 따라 이미 상응하는 보안조치를 제정하였다. 인증을 신청하는 기술 자료는 엄격히 인증 및 검사에만 쓰이며 기타 목적으로 사용되지 않는다.

이 13종 제품중 스마트카드 COS제품만 인증검사시 제조업체가 보안기능관련 소스코드를 제공해야 한다. 그밖에 6종 암호모듈을 지닌 제품은 암호실현 및 사용과 관련한 부분의 소스코드를 제공해야 하는데 소스코드 전체는 아니다. 그 밖에 제품은 인증시 어떠한 소스코드 제공도 없다. 주의해야 할 것은 국제적으로 통용되는 CC(정보기술보안성 통용평가기준) 인증인데, 스마트카드 COS를 검사시 마찬가지로 보안기능과 관련한 소스코드 제공을 요구한다. 암호모듈 검사시 소스코드 제공을 요구하는 것은 이미 미국정부가 발표한 표준 FIPS140-1(후에 FIPS140-2로 대체됨)에서 더욱 엄격한 요구사항을 제시하였는데, 즉 신청자는 반드시 소스코드에 대한 설명을 제공해야 하는 것이다. 중국 속담에 '자기가 하고 싶지 않은 일은 타인에게도 시키지 말라' 고 했다. 미국정부와 산업협회는 중국의 제품인증제도가 암호모듈관련 검사시 소스코드를 제공해야 한다는 똑같은 요구에 대해 명백히 반대하고 있다.

'이것을 과연 미국인의 건망증이라고 해야 할지 아니면 등잔 밑이 어둡다고 해야 할지?' 한 정보보안인증 전문가의 반문이다.

이 사람은 정보보안인증에 다년간 경험을 쌓은 전문가로 기자에게 말했다. '중국은 현재 정보보안제품 강제인증제도를 확립하고 있다. 이는 중국 정보보안제품 평가시 존재하는 중복검사, 인증서 중복발급 등의 문제를 해결하고자 하는 것이며, 국가안보, 공공이익과 국민권익, 합리적 관리체계, 시장규범, 산업발전촉진 및 실시에 대한 관리로 중국국가상황에 부합하고 또한 WTO/TBT 협정상 원칙에도 부합한다.'

'사실상, 외국매체의 진의는 부정확한 정보를 통해 여론을 조성하고 중국의 독창성에 압력을 가하는 것이다' 라고 익명의 중국표준화 전문가도 논평했다.

이는 지난 WAPI 사건을 떠오르게 한다. WAPI는 무관심에서 출발하여 모두가 관심을 갖는 상황을 거쳐, 무기한 연기되었으며 재차 국제표준 투표과정을 거쳐야하는 상황에 이르렀다. 이러한 과정에서 기술, 표준 및 시장에 대한 반성은 현재의 중국 정보보안제품 인증분야를 다시금 생각하게 하였다.

어쩔수 없이 천천히 간다

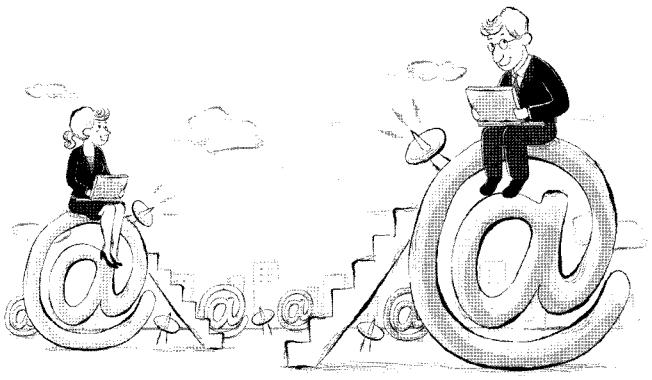
국제여론중, '무역장벽, 국내 정보기술산업 보호, 산업스파이' 등의 단어는 이미 중국에 대해 널리 쓰이는 '죄명'이 된 듯하다. 매번 중국이 독자적인 표준 정책을 내놓을 때마다 '국제무역 수구주의자'로 몰아세운다. 중국도 늘 피동적으로 '시행연기', '정부구매' 등의 방법으로 대응한다.

국가인증인정감독관리위원회가 발표한 2003년 제113호 공고문에서, 2004년 6월 1일부터 무선 네트워크제품에 대한 강제인증(WAPI)을 실시한다고 했지만, 미국의 강한 항의로 좌초되었다.

중국 자체표준에 관한 정책에 대하여, 외국의 일부 연구기관은 '중국정부가 최근 몇 년 동안 국내 정보산업을 보호하기 위해 채택한 유사조치들이 중국 정보기술 발전의 불균형을 가져왔다' 고 해석하였다.

이번 〈일부정보보안제품 강제인증실시에 관한 공고〉도 예외가 아니다. 사실상, 미국내 CC인증은 정부구매에서 강제적이다. 2002년 7월 1일부터 강제 시행되었다. 관련전문가의 소개에 의하면, 미국은 만일 정보보안제품이 국가비밀정보시스템에 사용된다면 규정상 미 국방부 국가보안국에서 검사를 실시하도록 되어있으며, 요구하는 수준도 상당히 높다. 그러나 미국은 오히려 이것을 중국이 강제인증을 실시하는 것에 대한 반대 이유로 삼고 있다.

1년여 동안 국내외에서 반복적인 협상을 거쳐, 세계금융위기상황을 고려해 국내관계부처는 최종적으로 실시를 조정하기로 결정했다. 기존방침에서 새로운 조정안을 내놓았다. 새 방안은 실시범위에서 큰 조정을 했는데, 오직 정부구매법의 범위에서 실시한다는 것이며 아울러 시행을 1년



연기하기로 했다.

가장 우려되는 점은 바로 내년 5월 1일 이후 강제인증이 순조롭게 실시될 것인가이다.

2009년 4월, 국가인증감독위원회는 〈정보보안제품 강제인증 지정인증기관 및 시험기관 업무범위에 관한 공고〉(2009년 제25호)를 발표하였는데, 정보보안제품 강제인증 실시 관련 지정인증기관 및 1차 7개 지정시험기관과 그 업무범위에 대해 명확히 하고 있다.

현재, 이미 몇 십 개의 제품이 관련기구에 인증신청을 했다. 향후 1년 내에 관련기관은 또 대량의 기초작업을 완료해야 하며 나아가 통일된 기술규범, 인증실시과정, 제도관철, 재정부에 종부구매목록 제공협조, 각 부처위원회 관련 업무연계과정추진 등을 포함한다. '이러한 작업은 모두 가속도를 내야하며 그래야 이 제도를 각처에서 실현시킬 수 있다' 고 한 전문가가 말했다.

한편, 우리는 결코 외국매체가 기대하는 세계적 정보기술회사로 부터 이 제도에 대한 반대를 받지 않았다. 중국은 세계 최대의 정보기술제품 시장중의 하나이며, 이 방대한 시장은 세계정보기술회사에게 굉장한 흡인력을 지니고 있다. 미국 레노버社의 데이터에 따르면 현재 중국의 정보보안기술 시장중 외국회사의 점유율은 약 70.5%이다.

사실상 MS社, CISCO社, SUN社 등 회사들도 아직 이 사항에 대한 입장 표명을 하지 않았다, 또한 칩 제조업체 인텔은 중국 법규를 지킬 것이라고 표명했으며, IBM社 대변인도 중국에 수출하는 제품이 동 규정의 영향을 받지 않을 것이라고 말했다. 인증관련 직원은 매일 많은 글로벌회사들이 관련기관에 인증제도에 대해 문의하고 있다고 말했다. WAPI제품 강제인증으로 말하자면 기자도 중국정보보안 인증센터 웹사이트에서 소식을 들은바 있다. 현재까지 인증신청을 한 외국기업이 국내기업보다 많다.

'편리'와 '내재적 위험'

현재, 국내 정보보안인증의 발전이 이렇게 험난한 것은 국내 산업환경이 아직 성숙되지 못했다는 객관적인 조건 외에, 주요 저지세력이 외국에서 온 것이기 때문이다. 외국 반대세력의 목적은 분명하다. 중국이 그들이 주도하는 CCRA협정에 가입하도록 하는 것이며 또한 이것으로 중국의 독자적인 표준을 억제하려는 것이다.

그러면, 이 CCRA는 도대체 어떤 협정인가? 이 국가들에게 어떠한 '편익'을 가져올 것인가?

현재, 국제사회에서 미국, 영국, 프랑스 등 26개 국가가 소위 통용준칙(CC)에 기초한 상호인정협정(CCRA)에 서명한 것으로, 그들은 줄곧 중국도 CC 상호인정체제에 가입하라고 요구해왔다. CCRA가 비록 중국표준의 참고 및 인용을 할 만한 점이 있긴 하지만 역시 많은 것들이 중국 국내사정에 부합하지 않는다.

'중국이 CCRA에 가입하면 가장 직접적인 장점은 바로 외국기업의 수천가지 제품이 중국시장에 진입할 수 있다는 것이고, 중국의 표준에 따라 더 이상 어떠한 인증을 진행할 필요가 없어진다. 또한 이 협정에 따라 중국 국내인증을 받은 제품은 2년의 준비기간 후에 직접 회원국에 진입할 수 있다!' 고 관련인사가 분석했다. 이는 회원국에게 '편익'을 주게 되지만, 중국제품에겐 보안상 내재적 위험성을 여전히 갖게 한다.

한 정보보안 산업계 최고 전문가가 기자에게 말했다. 특히 현재의 정부구매중 노트북, 핸드폰, 디지털카메라, 라우터, 교환기 등 최첨단 통신설비는 기본적으로 외국산 제품이 많다. 이로 인해, 정부의 구매영역에서 정보보안제품 강제인증실시는 매우 필요한 것이다.

'보안상 잠재위험에 대해 언급했는데 광범위하게 구매하는 다기능 일체형(복합기)이 바로 전형적인 예이다.' 라고 이 인사가 기자에게 말했다. 이러한 다기능 일체형은 스캐너, 팩스, 프린터 및 복사기 등이다. 다기능 일체기는 자체적으로 CPU, 저장기기, 디스플레이 설비, 입출력 설비를 지니고 있으며, 정보수집, 처리 및 전송 등의 기능을 한곳에 갖고 있다. 그 본질은 이미 한대의 컴퓨터와 같다. 이로 인해, 일반 컴퓨터와 같으며 다기능 일체기는 허점과 은폐점 등 보안상 잠재적인 위험이 높다.

특히 민감한 정보처리과정 중 정보가 노출되거나 악의적 도용 가능성이 존재한다. 비록 일부 제조자들이 그 제품이 신분인증, 비밀강화(저장비밀, 전송비밀), 잔류정보제거 등 조치로 안정성을 높인다고 선언하긴 했지만, 전문지식에서 악의적인 의도가 있는 경우, 여전히 다기능 일체기를 이용하여 민감한 정보를 훔쳐낼 가능성이 있다. 만일 우리가 CCRA에 가입한다면 이 외국제품들은 향후 중국의 정보보안 검사를 회피할 수 있고 그로 인한 보안위험과 내재적 위험은 잠재할 수 밖에 없다.

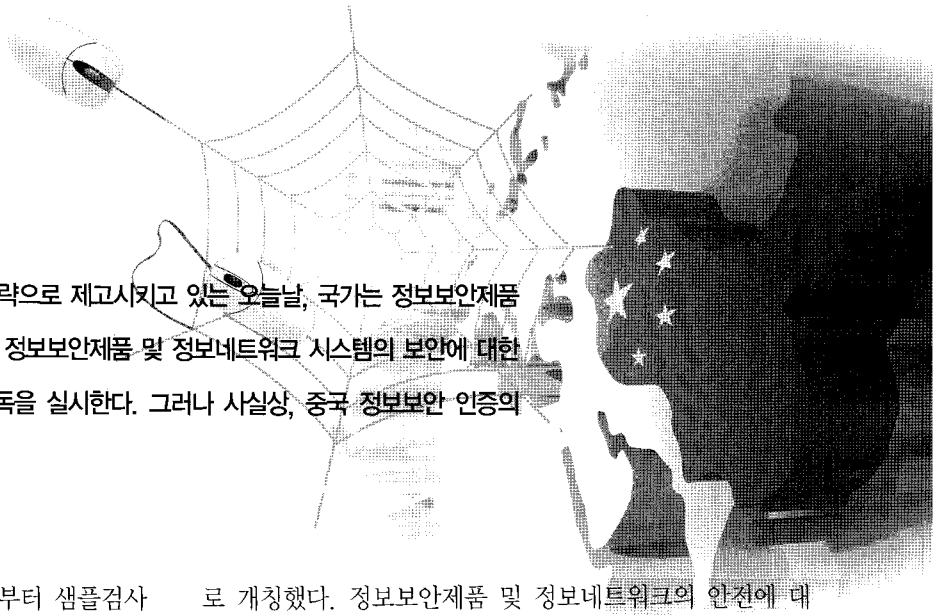
따라서 이러한 생각을 바탕으로 관련전문가들은 간언한다. CCRA에 가입할 것인가, 강제인증인가 아니면 자율인증인가에 대해 현재 중국은 여전히 심도있게 연구, 분석 중이다. 특히 정보보안분야에서 산업발전이든 업계관리이든 중국은 독자적인 기술표준을 완전히 포기해서는 안되며, 국제표준을 따라야 한다. 이 CCRA 가입은 중국 정보보안제품과 기술의 독창성에 절대적으로 불리할 것이다. 이로 인해 중국은 현재 CCRA 가입신청을 하지 않았다. 중국의 독자적인 정보보안제품 인증체계 확립을 어떻게 할 것 인가? '우리는 서방의 지휘봉에 따라 갈 수만은 없다, 독자적 표준을 유지해야 하며 자기에게 속한 정보보안제품 통일인증체계를 확립해야 한다.' 라고 관계자가 말했다.

중국강제인증 '누설을 막고 결점을 찾다'

국가는 강제인증 실시제품에 대해 반드시 '중국강제인증'(China Compulsory Certification) 즉 CCC 인증을 받아야 한다고 규정하고 있다. 강제인증제품 목록에 속하는 모든 제품은 반드시 국가가 지정하는 인증기관의 합격을 받아야 한다. 관련증서를 취득하고 인증마크를 부착한 후에야 출고, 판매, 수입 및 경영활동을 할 수 있다. 동시에 이 CCC 인증도 세계에서 통용되는 강제인증제도이다.

이로 인해, CCC 인증의 토대에서 정보보안제품 강제인증시 제품검사는 반드시 3가지 절차를 거쳐야한다: 형식시험, 공장검사 및 정부감독.

인증을 신청하는 기업에 대해 인증기관은 생산라인에서 현장실사를 한다. 또한 제품을 사진으로 촬영한다. 인증서 발



> 세계적으로 정보보안의 중요성을 국가전략으로 제고시키고 있는 오늘날, 국가는 정보보안제품의 품질향상 및 국가정보의 보장을 위해 정보보안제품 및 정보네트워크 시스템의 보안에 대한 여러 가지 행정허가 및 인증 등 관리감독을 실시한다. 그러나 사실상, 중국 정보보안 인증의 길은 매우 험난하다.

급 후 6개월에서 1년 내에 시장과 사용자로부터 샘플검사를 실시한다. 다년간 정보보안인증에 종사한 한 전문가는 중국상황에 따라 초기에는 관련인증부처는 형식시험에서 샘플시험을 위주로 했었다. 기업자체적으로 생산라인에서 2대의 샘플을 선정한다. 정보보안산업은 비교적 작기 때문에 신기술과 신제품은 여전히 샘플을 위주로 한다. 어떤 기업들은 이러한 허점을 이용하기도 한다.

예를 들면, 어떤 기업들은 제품설명에 더욱 많은 시험항목과 더욱 좋은 시험결과를 열거하기 위해 최상의 제품을 인증시험에 보내지만 시장에 판매하는 때는 최저의 제품을 판매한다. 이러한 방식은 과거부터 계속 금지되었지만 근절되지 않았다. 이에 대해 관련 인증기관은 현장실사를 강화하여 제품이 규정과 설명서대로 생산됐음을 보장한다. 이렇게 기업의 조작행위들을 규정지어 놓았다. 안전등급이 비교적 높은 제품에 대해 그 생산라인과 개발환경도 검사한다.

누가 정보보안의 책임자가 될 것인가?

10년 전과 비교해서 국내 정보보안인증 상황이 발전을 했지만 현재까지 중국은 정보보안제품 인증에서 아직 완전히 통일된 인증표준과 체계를 갖추지 못했고 강제인증은 더욱 어려운 상황이다. 이로 인해 정보보안인증은 가볍지 않은 사명을 띠고 있다.

2004년 국가품질검사총국 등 8개 부 위원회는 〈국가정보보안 인증인정체계에 관한 통지〉를 공동 발표하였고, 그 중 정보보안제품 검사와 인증기능은 분리하도록 요구하였다. 2006년 '중국정보보안 인증센터' 성립 후 (원래 '중국정보보안제품 평가인증센터') 정보보안제품의 인증사업을 새로 설립된 '중국정보보안 인증센터'로 이양했고 이어서 '중국정보보안 제품평가 인증센터'를 '중국정보보안 평가센터'로 개칭했다. 정보보안제품 및 정보네트워크의 안전에 대해 필수적인 인증과 관리감독은 반드시 이루어져야 한다. 왜냐면 이것은 정보보안제품 품질확보 및 국가정보보안에 매우 중요한 일이기 때문이다.

특히, 정부구매부분에서의 정보보안은 반드시 인증을 통해 보장되어야 한다. 인증검사를 통과한 제품의 절대적 안전은 보장하지 못하지만 최소한 중국표준에 부합하지 않는 제품의 품질이 불안전하다는 것을 의미하기 때문이다.

〈정보보안제품 강제인증 실시에 관한 공고〉에서 중국은 이미 강제인증을 받아야 할 13종 보안제품을 확정했다. 또한 이 13종 제품의 확정 및 그 인증실시규칙에 대해 토론할 때 각 부처의 많은 의견이 있었으며 많은 논쟁을 벌였었다. 예를 들면 제품목록을 어떻게 확정할 것인가, 각 제품은 어떤 표준에 근거할 것인가, 제품의 정의, 어떻게 검사하고 샘플을 보내며 인증단위는 어떻게 구분할 것인가 등 다각적인 노력을 통해 최종적으로 13종 제품의 인증실시 규칙과 통일된 신청서, 검사보고 양식 등을 확정했다. 이러한 내용들은 총 1천6백 항목이며 약 65만자 이다. 이렇게 많은 기초작업을 완성했기 때문에 이런 제도를 각처에 정말로 실현시킬 수 있는 것이다.

이미 관련기관에서 검사의 표준 요구사항, 검사의 표준 환경, 검사방법, 검사항목, 비용, 인증서 등 초보적인 통일을 이루었지만, 향후 검사기관, 전문가 훈련, 시험 및 기술교류 등을 규범화할 것이다. 그러나 정보기술은 발전하고 있고, 검사기술도 발전하고 있다. 이로 인해 표준도 발전해야 한다. 규범의 완전한 통일을 이루어야 하는데 이는 여전히 힘들고 먼 상황이다. 현재 일정한 기초업무를 완성하긴 했지만 관련 업무들이 더욱 통일되고 규범화되어야 한다.