TBT 중앙사무국 동정

중국 정보보안기기 강제인증제도 대응현황

기술규제대응과
02-509-7254

□ 중국 정보보안기기 강제인증제도 개요

중국은 품목별로 각각 운영되던 공산품에 대한 강제 검사제도를 통합하여 '03년부터 전자파 · 통신 · 안전 등과 관련된 132개 품목(자동차 · 냉장고 · 생활가전 · 전기제품 등)에 대해 CCC제도(China's Compulsory Certification)를 시행하고 있다. 특히, '07년 8월 WTO를 통해 자국내에서 유통되는 13개 정보보안제품(해외제품 포함)을 대상으로 '강제인증제도(ISCCC)'를 '09년 5월부터 시행할 계획이라고 각국에 통보하여 세계적으로 관심의 대상이 되고 있다.

이에 대해 세계 각국은 동 제도가 국제무역에 장애가 되는 불필요한 기술규제이며, 기업에 부담을 주고 기업의 기술정보 유출 등 우려가 있음을 들어 중국정부에게 철회를 요청하기 시작했다. 우리나라도 WTO의 TBT 위원회 및 중국과의 한중 적합성평가 소위원회를 통해서 국내 기업의 우려사항을 전달하고, 강력히 항의하여 왔다.

이에 따라 중국의 동 규제 기관인 중국국가인증인가감독관리국(CNCA)는 당초 제도의 시행 예정일인 '09년 5월 1일을 '10년 5월 1일로 1년 연기하고, 규제대상도 정부 조달품목으로 한정한다고 '09년 4월 29일 공식 발표하였다. 그러나 여전히 동 인증제도의 시행이 유효하며, 무역을 저해하는 비관세장벽으로 작용할 수 있어 적극적 대응책 마련이 필요하다.

중국정부는 국가정보의 보안성 확보를 제도 시행의 목적이라 발표하고 있으나, 중국의 전반적인 제도 시행에 있어 모호한 부분이 많이 남아있으며, 정부조달로 한정하겠다는 내용도 현재까지 명확한 시행방침이 없는 상태이다.

□ 국내업계 반응

LG, 삼성 등 국내 전자업계는 중국의 동 인증제도가 핸드폰, 디지털 카메라, 가전 등 퍼스널 디바이스 보다는 일반 대중이 사용하는 기기의 해킹 및 바이러스 대응 등을 위한 목적으로 추측하고 보안기능이 임베디드된 제품은 특별한 관련이 없을 것으로 판단하고 있다. 한편, 강제인증제도의 품목이 확대될 경우 문제가 발생할 것이라고 우려하는 목소리도 있다. 반면 DB 솔루션 업체와 보안업체에서는 마케팅 에이전시를 통해 수출 중인 DB 시스템이 정보보안제품에 해당되므로 강제인증제 시행시 문제 발생의 우려가 있다고 보고 있다.

국내 업계에서는 중국의 인증제도와 관련하여 '08년부터 지속적으로 예의주시하고 있으나, 아

적은 중국의 진의가 명확하지 않아 판단을 유보중인 것으로 파악된다. 다만, 동 제도가 향후 휴대폰·디지털 카메라·LCD TV·디지털 복사기 등으로 확대되는 경우 국내기업의 피해 정도는 상당히 클 것으로 우려하고 있다.

□ 세계 각국의 대응현황

미국은 중국의 인증제도 시행의 규제적용대상을 정부조달품목으로 한정한 것으로 평가하고, 여전히 남아있는 모호한 부분에 대해 양자채널, WTO/TBT 위원회 및 EU, 일본, 한국과 공조를 통해 대응할 방침인 것으로 파악되었다.

예를 들어 '09년 5월 1일 일본 정산성 대신의 방미시에는 USTR 대표와 공동으로 중국측의 제도 보류를 원한다는 내용의 공동성명을 발표한 바 있다.

일본은 동 제도의 부적절성을 지적하고 철회를 요구하는데 가장 적극적인 것으로 관찰되는데, 일본은 '09년 4월 29일 중일 정상회담시 동 인증제도의 재검토를 요청한 바 있으며, '09년 5월 4일 미국 무역대표부와의 공동성명 발표도 일본측이 주도했던 것으로 알려지고 있다.

또한 일본은 이번 중국의 인증제도 시행에 대하여, '09년 4월 24일 주요 일간지인 요미우리 신문이 크게 공론화시키는 한편 관방장관도 직접 언급을 하는 등의 대응을 통해 매우 강경한 자세를 보이고 있다.

□ 국내 대응현황

우리나라에서는 중국의 제도시행계획 발표 직후부터 동 사안과 관련하여 안철수 연구소 등 국내의 정보보안제품 관련업계 및 기관을 대상으로 대책회의를 총 4회 개최한 바 있으며 현재 전자정보통신산업진흥회 등을 통해 상시 협력 및 공조채널을 가동하고 있다.

국제공조를 통한 정보공유 및 공동대응은 지난해 12월 한미일 3국이 일본에서 공동 대응을 추진하기로 합의한 이후 긴밀한 협력관계를 유지하고 있다. 이와 관련하여 미국 무역대표부(USTR) TBT과장이 '09년 3월 방한하여 지식경제부 기술표준원 기술규제대응과장과 면담을 하였고, 이어 기술규제대응과장이 '09년 5월 미국을 방문하여 공조방안을 협의하였다.

또한 일본과의 공조는 지난해에 이어, '09년 3월 WTO/TBT 위원회 기간동안 관련 사항의 공조대응을 위한 회의를 하였고, 최근 '09년 5월 18일 지식경제부 무역투자실장이 일본 경산성 통상국장과 한일간 지속적인 공조방안을 논의하였다.

한편 기술표준원은 WTO/TBT 위원회에서 '08년 11월과 '09년 3월 두 차례에 걸쳐 중국의 정보보안제품 강제인증에 대한 국내 업계의 우려표명을 하였고, 지속적으로 세계 각국과 정보교환 및 공동 대응을 하여왔다.

중국과 직접적인 접촉을 통한 대응으로는 '08년 11월 한중 적합성평가 소위원회에서 중국 CNCA 측에 아국 업계의 우려사항과 동 인증제도의 부당함을 강하게 표명하고 중국 정부의 인증제도 연기를 약속받은 바 있다.

□ 향후 대응방안

우리나라는 동 인증제도에 대한 한미일 국제 공조를 계속해나가고 '09년 6월 WTO/TBT 위원회 회의시 미, 일, EU 등과 사전 실무회의를 추진하여 보다 구체적으로 중국의 인증제도에 대한 대응책을 마련할 계획이며 중국 규제당국과 양자협의 등을 지속 추진할 예정이다.

또한 '09년 7월 부산에서 개최될 예정인 한·중 적합성평가 소위원회에서는 동 사안을 주요 의제로 다루어 중국의 인증제도와 관련하여 모호한 부분에 대한 자세한 설명을 듣는 기업대상의 설명회도 개최할 계획이다.

기술표준원에서는 동 인증제도와 관련하여, 앞으로도 업계 관계자들과 수시 대책회의를 통해 지속적으로 업계 의견을 수렴할 계획으로 인증관련 내용 및 절차서 작성 배포, 인증대비 사전 준비, 수출 기업에 대한 맞춤형 교육 및 컨설팅 시행 등으로 국내 업계의 피해를 최소화하기 위한 국가차원의 체계적 대응방안을 수립할 계획이다.

또한, 중국측에서 정보보안 기능이 있는 디지털 기기로 대상품목 확대 여부 및 정부조달로 국한하겠다고 발표한 후에도 국영기업 등 적용범위를 확대할 가능성 여부 등에 대하여 예의 주시할 방침이다

중국의 강제인증 정보보안 제품의 적용범위

연번	동보문	통문상의 제품명	시행 규칙(안)	시행 규칙에 기재된 적용범위
1	CHN/278	웹사이트 복구	CNCA-1 1C-086	웹 사이트 내용의 비승인(unauthorized) 변경에 대해 실시간 자동 복구를 시키고, 웹 사이트에 대한 감시와 통제, 복구와 완전성의 보호를 실현시키는 시스템이다.
2	CHN/279	방화벽	CNCA-1 1C-074	서로 다른 보안 환경 사이에 복히 서로 다른 보안시스템을 갖는 통신망이나 도메인 사이에 집속하는 시스템. 방화벽 제품은 한 대의 전용 설비가 될 수 있고 여러 기존 부품의 기술의 조합도 될 수 있다. 방화벽 제품은 다음과 같은 특성을 갖고 있다: 통신망 환경 사이의 모든 통신은 방화벽을 직접 통과할 수 있다. 로컬 보안 시스템에 따라 권한이 있는 통신에 대하여 통과 할 수 있다.
3	CHN/280	네트워크 보안격리 카드, 선로선택	CNCA-1 1C-075	물리적 차단과 격리, 한 방면의 격리나 부분 격리 기능의 부품을 포함한다. 물리적 차단과 격리 부품은 정보를 물리적으로 차단하는 정보 보안 부품을 의미한다. 한 방면의 격리 부품은 판이서 제어 정보(access control information)를 교환하는 하드웨어 따터션에 의하여 정보가 다른 안전한 도메인에서 한 방면으로의 흐름을 실현하는 정보 보안 부품을 의미한다. 부분 격리 부품은 다른 도메인에서 부분 기리를 실현하는 정보 보안 부품을 의미한다. 그 중 정보 흐름은 일반적으로 선용 응용 게이트이다.
4	CHN/281	보안격리, 정보교환	CNCA-1 1C-076	보안격리 및 정보교환 제품은 내외부 네트워크간에 웹 프로토콜 층적(자단)의 기반하에 웹사이트간 정보 보안 교환 실현을 보장할 수 있는 제품 또는 두 개의 서로 다른 도메인사의 정보보안부품이 프로토콜 전환의 수단을 통한 정보 운송 방식으로 데이터 교환을 실현하며 시스템에서 명확히 요구된 전송의 성보만 통과할 수 있도록 한다. 그 정보흐름은 보통 공용 응용 서비스이다.
5	CHN/282	보안 라우터	CNCA-1 1C-077	보안전략에 의한 메커니즘과 알고리즘을 기반으로 웹 사이드를 중적하고 신분인증, 데이터기밀(데이터 암호화)과 보안 라우터 여부서를 통해 웹 사이트의 데이터 흐름을 제어하고 보호한다
6	CHN/283	IC 카드 칩운영체제(COS)	CNCA-1 1C-078	IC 카드 칩운영 체제(COS Chip Operating System)는 IC카드 칩에서 작장하고 작동한다. 이 소프트웨어는 비 휘발성의 메모리(MRAM)에 저장한 응용 데이터나 프로그램의 기밀성과 완전성을 보호하며 IC 카드 칩의 외부 정보 교환 및 통제를 목적으로 한다.
7	CHN/284	데이터백업, 복구	CNCA-1 1C-079	데이터 핵심 소프트웨어, 데이터 복시 소프트웨어, 지능 저장 장치에 제공한 데이터수집, 전송, 관리 능력을 이용하여 업무 시스템에서 백업이 필요한 데이터, 응용 데이터, 일시 데이터를 실시간이나 주기적으로 예비저장 장치에 저장하는 기능이다. 독립한 히이트 백업 및 복구관리 소프트웨어 제품; (2) 독립한 데이터 복사 및 복구 소프트웨어 제품.
8	CHN/285	보안운영시스템	CNCA-1 1C-080	시스템 설계, 구현, 사용 및 관리 등 각 단계에서 하나의 완전한 시스템 보안 전략에 의한 운영 시스템을 의미한다. 본 규칙에 적용되는 제품 범위 (1) 독립 보안 운영 시스템 소프트웨어 제품; (2) 설계하시나 보안 운영 시스템을 내장(embedded) 한 제품 (예를 들어서: PC, 노트북, PDA, 서버, 방화벽, 인코딩 기지 등 설비).
9	CHN/286	보안데이타베이스 시스템	CNCA-1 1C-081	시스템 설계, 구현, 사용 및 관리 등 모든 단계에서 하나의 완전한 시스템 보안전략에 따라 운영하는 시스템을 의미한다. 적용 제품 범위는 다음과 같다: (1) 독립 보안 데이터베이스 시스템 소프트웨어 제품, (2) 보안 데이터베이스 시스템을 집적하거나 내장(embedded) 한 제품 (예를 들어서: PC, 노트북, PDA, 서버, 방화벽, 인코딩 기계 등 설비).
10	CHN/287	스팸차단	CNCA-1 1C-082	SMTP 표준 프로토콜(Standard Protocol)에 따라 전자 메일 시스템에서 전송한 스팸 메일을 식별, 필터링하는 시스템을 의미한다. 이 시스템은 전자메일전송 경로에서 스팸 메일을 검출하여 식별하거나 메일을 스팸 메일로 인증한다. 스팸차단 기능을 제공하는 동시에 셀프 시스템의 안전을 보장해야 한다 본 규칙이 적용되는 제품 범위는: (1) 무인한 스팸차단 룬로(Gateway); (2) 메일 전달이 기반한 스팸차단 시스템; (3) 메일 시버와 하나로 본 스팸차단 메일 서버; (4) 메일 서버에 설치하는 스팸차단 소프트웨어.
11	CHN/288	침입탐지 시스템	CNCA-1 1C-083	컴퓨터 웹 사이트나 컴퓨터 시스템에서 여러 곳의 정보를 수집분석하여 웹 사이드나 시스템에시 보안규칙을 위반한 행위나 공격 받을 현상이 있는지 발견하는 시스템을 의미한다. 제품 범위는: (1) 웹 사이트형 침입 탐지 시스템; (2) 해인 엔진형 침입 탐지(감사 측정)시스템
12	CHN/289	네트워크 해커 스캐너	CNCA-1 1C-084	스스로 알고 있는 보안 룬내를 하나씩 검사하여 보안 관리 설계 피하 및 위히도를 확인하고 구체적인 해결 방안을 제시하다 본 규칙은 웹사이트를 통해 히스템 보안을 원격 평가하는 도구에 적용한다. 적용 되지 않는 제품 범위는: (1) 해당 시스템에 대해자(에이전트)가 있는 host based 형 보안 평가 도구; (2) 데이터베이스 전용 보안 평가 도구; (3) 웹(WEB) 전용 보안 평가 도구.
13	CHN/290	보안심사	CNCA-1 1C-085	(1) 컴퓨터, 서비, 웹 사이트, 데이터베이스 관리 시스템, 기타 응용 시스템 등을 객체 대상으로 한 종류의 보안감사를 하며 보안감사 사건에 대하여 분석과 반응을 진행하는 보안 감사 제품; (2) 종합형: 컴퓨터, 서비, 웹 사이트, 데이터베이스 관리 시스템, 기타 응용 시스템 등을 객체 대상으로 두 개 이상 종류에 대하여 보안 감사를 하며 보안 감사 사건에 대하여 동일한 분석과 반응을 진행하는 보안 심사 제품.