情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

국내 평가·인증 정책의 현황 및 향후 추진방향

이대섭*, 홍원순**

요 약

정보보호제품의 안전성 및 신뢰성이 검증된 제품의 공급 및 이용 촉진을 위해 운영되고 있는 정보보호제품 CC 인증제도, 암호제품에 대한 암호 검증제도, 공공기관 도입 정보보호제품에 대한 보안적합성 검증제도 등에 대한 현황 및 향후 추진방향을 살펴본다.

Ⅰ. 서 론

정보보호제품의 보안기능을 검증하여 국가 정보보호 수준을 향상시키고, 정보화 역기능으로부터 주요 자산을 보호할 수 있도록 공공기관 사용자에게 신뢰할 수 있는 정보보호제품을 선택할 수 있는 평가정책으로 우리나라는 'CC 인증제도', '암호 검증제도' 및 '보안적합성 검증제도'를 운영하고 있다. 본 고에서는 각 제도의 체계 및 절차 등의 현황과 향후 추진방향을 살펴본다.

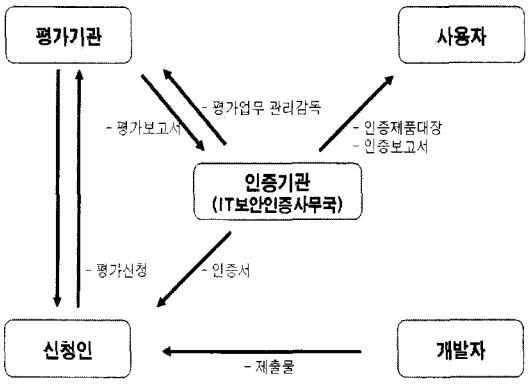
Ⅱ. CC 인증제도

정보보호시스템 평가·인증제도는 민간업체가 개발한 정보보호제품의 보안기능을 검증하여 국가차원에서 안전성과 신뢰성을 보증하기 위해 국제공통평가기준에 따라 평가·인증하는 제도이다. 우리나라는 1998년 2월부터 평가·인증제도를 시행하고 있으며, 2002년부터는 국제공통평가기준(Common Criteria)에 따라 정보보호제품을 평가·인증하고 있다. 평가·인증제도는 '정보화촉진기본법 제15조 및 동법 시행령 제16조'에 근거하여 시행하고 있으며 상세 내용은 '정보보호제품 평가·인증 수행규정'에서 규정하고 있다.

2.1. CC 평가·인증체계

현재 한국정보보호진흥원(KISA), 한국산업기술시험원(KTL) 및 한국시스템보증(KOSYAS)이 평가업무를 수행하고, IT보안인증사무국 IT보안인증사무국이 인증업무를 수행한다. [그림 1]은 평가·인증체계를 보여준다.

2006년 1월 IT보안인증사무국이 국가정보보안지침을 개정하여 평가·인증 대상을 확대하고, 같은 해 5월 국제상호인정협정(CCRA)에 가입함에 따라 국내 정보보호제품에 대한 평가 품질 향상 요구가 맞물리면서 평가수요가 급증하였다. 평가 대기기간 단축을 위해 IT보안인증사무국은 기존 KISA에서만 수행해 오던 평가업무를 민간에서도 할 수 있도록 개방하였다.



〔그림 1〕 평가·인증체계

* 고려대학교 (itscc@korea.ac.kr)
** 한국정보보호진흥원 보안성평가단 (wshong@kisa.or.kr)

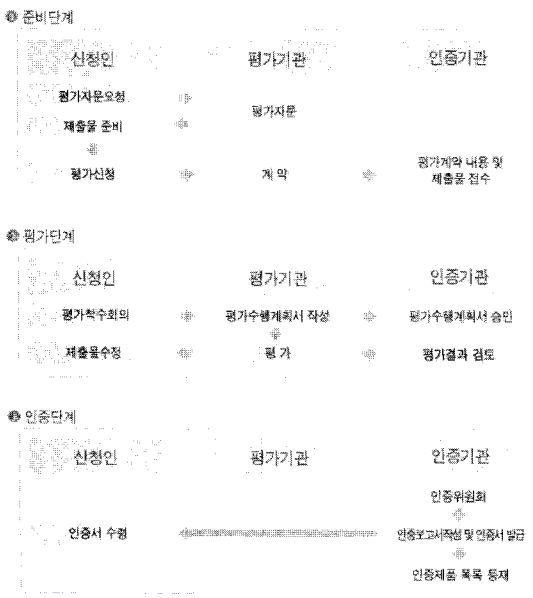
이에 맞추어 정보통신부에서도 2007년 8월 정보화촉진기본법 시행령을 개정, 민간 평가기관에 지정에 대한 근거가 마련되었으며 현재 KTL과 KOSYAS가 민간 평가기관으로서 평가업무를 수행 중에 있다.

또한 IT보안인증사무국은 평가적체 문제에 적극적으로 대응하기 위해 2007년 3월부터 국내용 정보보호제품 평가인증 및 유사제품 일괄평가인증을 실시하였다. 국내용 제품은 보안기능과 취약성 시험을 제외한 일부 평가항목을 표본 추출하여 적용하고 결과기록 등을 최소화함으로써, 국내용 평가기간을 4개월 정도 단축하였다.

2.2. 평가 · 인증절차

[그림 2]에서처럼 평가과정은 평가준비단계, 평가단계 및 인증단계로 진행한다. 평가준비단계는 평가신청인의 평가신청부터 계약까지의 과정이며, 평가단계는 평가기관에서 평가팀을 구성하여 평가제출물을 평가하고 평가보고서를 완료할 때까지의 과정이다.

인증단계에서는 인증위원회를 개최하여 평가 및 인증결과의 타당성 및 공정성에 대한 심의 · 의결 등을 통해 인증서 및 인증결과서를 교부하고 인증된 제품의 설명 및 인증서 인증번호 등을 인증제품대장에 등재한다. 사후관리단계에서는 인증서보유기관이 인증제품의 형상을 변경한 경우, 인증효력유지를 위하여 인증효력 유지신청서 및 보안영향분석서를 작성하여 인증기관에 신청하여야한다.[1]



〔그림 2〕 평가 · 인증절차

Ⅲ. 암호 검증제도

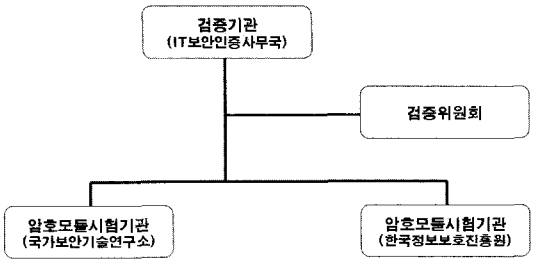
암호 검증제도는 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보보호의 보호를 위해 사용하는 암호제품에 대해 안전성과 구현 적합성을 검증하는 제도로서, '전자정부법 제27조(정보통신망 등의 보안대책 수립시행)' 및 '암호모듈시험 및 검증지침'에 근거하여 시행된다.

3.1. 암호 검증체계

[그림 3]에서와 같이, 암호모듈 시험기관은 국가기술보안연구소(NSRI)와 한국정보보호진흥원이며, IT보안인증사무국 IT보안인증사무국이 검증기관 업무를 수행하고 있다. 검증위원회는 관계기관, 학계 및 연구기관, 검증 · 시험기관 등의 산학연 전문가로 구성하며, 시험 · 검증결과의 타당성 · 공정성에 대한 심의 · 의결 및 신청인과 시험기관간 분쟁조정 등의 역할을 한다.[2]

3.2. 암호 검증절차

암호모듈 시험 및 검증을 수행하기 위해 시험기관의 장은 시험반을 구성하여 검증대상 암호모듈이 시험기준에 명시된 요구조건을 만족하는지 여부를 시험한다. 만일 시험과정에서 제출물이 미비하여 시험 수행이 불가한 경우 정해진 기한 내에 신청인에게 제출물의 보완을 요청할 수 있다. 시험기관은 암호모듈 시험이 완료된 후, 시험결과보고서를 검증기관에게 제출하며, 검증기



〔그림 3〕 암호검증체계

관은 시험결과에 대한 검토 후 검증위원회의를 개최, 위원회의 심의결과에 따라 검증서를 발급하고 암호모듈 검증목록에 등재한다.

Ⅳ. 보안적합성 검증제도

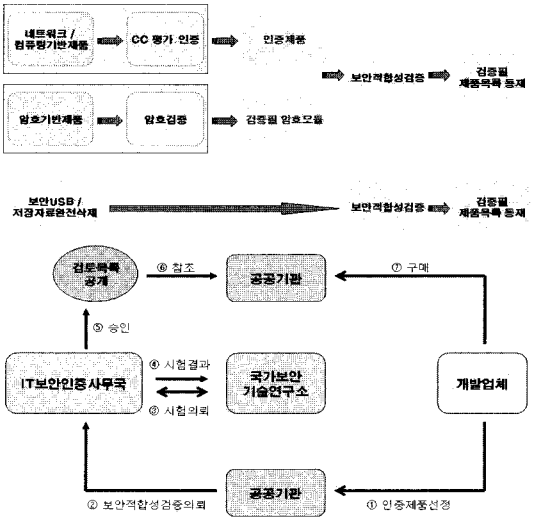
보안적합성 검증제도는 전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률 등 관계법규에 의거하여 공공기관에 도입하는 정보보호제품의 보안적합성과 안전성을 사전 검증함으로써 국가정보통신망의 보안수준을 제고하기 위해 시행하는 제도로, 전자정부법 제27조(정보통신망 등의 보안대책 수립시행) 및 국가정보보안 기본지침 제91조에 근거한다.

공공기관은 IT보안인증사무국 홈페이지에 등재된 '검증필 정보보호제품목록'과 '검증보고서'를 참조하여 해당기관에 적합한 정보보호제품을 사용해야 한다. 정보보호제품을 도입하고자 하는 기관은 도입 전 '검증필 정보보호제품 목록'을 참조하여 정보보호제품을 도입할 수 있으며, 목록에 등재된 제품은 별도의 보안적합성 검증 절차 없이 도입할 수 있다.[3]

4.1 보안적합성 검증체계

보안적합성 검증 신청의 주체는 정보보호제품 도입기관이며, 검증기관인 IT보안인증사무국이 검증대상 제품의 보안기능과 신청기관이 작성한 사용자 보안요구사항과의 일치성 여부를 검토한다. [그림 4]는 검증체계 및 검증제품의 등록절차를 보여준다.

공공기관에서 도입하려는 네트워크 및 컴퓨팅 기반의 정보보호제품인 경우, 보안 적합성 검증을 통과하여야 하며, 보안성 평가를 받은 인증제품이어야만 보안 적합성 검증을 신청할 수 있다. 다만, 라우터, 보안 USB, 저장자료 완전삭제 등 일반 IT 제품인 경우, CC 평가를 받지 않고 보안 적합성 검증을 신청할 수 있다. 암호기반 제품의 경우에는 암호검증제를 통과한 검증필 암호모듈이어야 보안 적합성 검증을 신청할 수 있다. IT보안인증사무국은 검증대상제품에 대한 시험이 필요하다고 판단할 경우, 시험기관인 국가보안기술연구소에 보안적합성 시험을 의뢰한다. IT보안인증사무국은 검증대상제품의 시험결과와 국가암호정책의 준수여부를 참고하여 신청기관이 의뢰한 보안등급의 적합여부를 판정하여 신청기관과 관계기관에 통보한다.

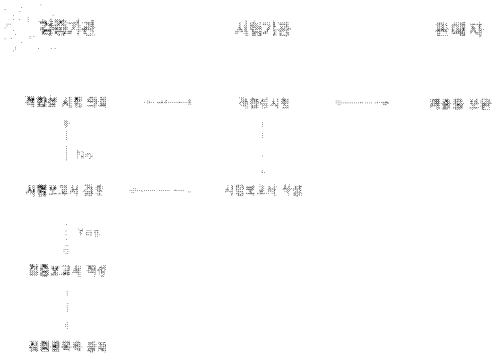


〔그림 4〕 보안적합성 검증체계 및 등록절차

4.2 검증절차

보안적합성 검증절차는 사전검토단계와 적합성시험단계로 구분되는데, 사전검토단계에서는 시험을 위한 제출물의 완성도를 검토하며 시험단계에서는 실제 사용환경에 기반한 제품을 검증한다. [그림 5]는 사전검토단계 절차를 보여준다. 신청기관에서 대상제품을 선정하여 신청서를 작성하여 제출하면, IT보안인증사무국에서 사전검토를 하여 적합한 경우에 시험여부를 판단한다. 시험이 필요한 경우에는 적합성 시험에 착수하고, 불필요한 경우에는 검증보고서를 작성하여 그 결과를 신청기관에 통보한다.

〔그림 5〕 사전검토단계



〔그림 6〕 보안적합성시험단계

[그림 6]에서는 적합성시험단계 절차를 보여준다. IT보안인증사무국은 시험기관에 적합성 시험을 의뢰하고, 시험기관은 적합성 시험을 수행한 결과를 시험보고서에 작성한다. IT보안인증사무국은 검증대상제품의 시험결과와 국가암호 정책의 준수 여부를 참고하여 신청기관이 의뢰한 보안등급의 적합 여부를 판정하여, 이를 신청기관과 관계기관에 통보한다.

V. 제도의 차이점 및 향후 추진방향

[표 1]은 3개 제도간의 주요 차이점을 요약한 것이다. 이 제도들은 국가 차원에서 정보보호제품의 신뢰성과 안전성을 보증하는 제도로 유사한 도입목적에서 시행되고 있다고 볼 수 있다. 한편으로는 상호보완적인 면과 제도별 적용대상이 확실히 구분되는 측면이 있다. 우선, CC 인증제도는 정보보호제품의 보안기능 에 대한 안전성 및 신뢰성을 검증하는 반면에, 보안적합성 검증제도는 CC 평가제도에서 평가한 보안기능 이외 부분에 대해 정확하게 구현되었으며 작동되는지를 시험한다. 추가적으로, 공공기관이 구축한 IT 환경에서 평가된 제품이 통합되어 운영될 경우, 기관 차원에서의 안전 · 신뢰성을 검증한다. 공공기관은 기관의 IT 구축 세부 내역을 보안적합성 검증 신청시 제출하여야 한다.

이처럼 유사한 도입 목적성을 갖는 각각의 평가 · 인증제도들은 상호보완적인 부분과 개별 제도만의 고유한 특성을 가지고 있다. 예컨대, 공공기관이 특정 정보보호제품을 도입하고자 하는 경우, 이 제품은 우선 CC 인증을 획득하여야 하며, 이후 보안적합성 검증 시에 CC 평가에서 수행되지 않은 제품의 범위 · 기능이 추가 시험되고 제품이 기관의 환경에 부합하는지 확인되어야 한다. 이를 통해 공공기관은 안정성과 신뢰성이 검증된 제품을 도입할 수 있는 것이다.

〔표 1〕 제도 비교

	CC 인증	암호검증	적합성검증
시행연도	1998년	2005년	2001년
지침개정	2007.8	2004.12	2007.5
적용대상	상용 정보보호제품	암호모듈제품	공공기관에 도입하는 정보보호제품
평가기준	공통평가기준 (CC)	암호검증기준 암호시험기준	미공개
신청인	정보보호제품 개발자 또는 사용자	정보보호제품 개발자 또는 사용자	공공기관
평가 · 시험기관	-KISA(보안성 평가단) - KTL - KOSYAS	- NSRI - KISA(암호 응용팀)	NSRI
인증 · 검증기관	IT보안인증 사무국	IT보안인증 사무국	IT보안인증 사무국
평가인증범위	제품의 보안기능	암호모듈	CC평가범위 이외 기능 및 제품사용환경

또한, 향후 2009년 1월부터는 보안적합성 검증시 CC 인증 외에도 암호검증이 필수요건으로 추가될 예정이다.[2] 현행 CC 평가체계에서는 제품의 암호모듈에 대한 안정성 확인은 평가범위에서 제외되어 있다. 이는 암호정책이 각 국가마다 달라 국제적으로 공통적으로 통용되는 CC에 암호 정책을 포함하는 것이 바람직하지 않기 때문이다. 그러므로 정보보호제품 내 구현되어 있는 암호모듈의 안정성에 대해서는 별도의 확인이 요구되며, 이를 위해 IT보안인증사무국은 향후 공공기관에 도입되는 정보보호제품에 대해 암호검증을 필하도록 조치하였다. 이로서 향후 CC 인증 및 암호검증은 개별적인 제도가 아닌 보안적합성 검증을 위한 유기적인 사전 자격요건으로 자리매김하게 될 예정이다.

Ⅵ. 결 론

앞서 살펴본 바와 같이, 현재 운영되고 있는 CC 인증제도, 암호 검증제도 및 보안적합성 검증제도는 상호보완적인 특성 및 차별성을 가지고 있다. 향후에도 민간업체가 개발한 정보보호제품의 경쟁력을 강화하고 안전성과 신뢰성을 보증함으로써, 궁극적으로는 공공기관이 안심하고 제품을 도입하여 사용할 수 있도록 지속적으로 상호보완적인 제도로서의 발전방향을 모색해가야 한다.

특히, IT보안인증사무국은 CCRA 인증서발행국으로서의 위상 제고를 위해 평가·인증제도를 국제수준에 맞도록 개선해 나아가야 하며, 이러한 제도 개선이 통해 우리나라 정보보호산업을 육성시키는 초석이 될 수 있도록 지속적인 연구·발전이 필요하다. 또한, 향후에도 지속적으로 신종 정보보호제품에 대한 보호프로파일을 지속적으로 개발·배급하여 민간업체에서 제품 개발시 이를 참조, 국가 정보통신망 보호에 적합하고 국제적으로도 경쟁력 있는 제품을 개발할 수 있도록 유도·지원하여야 한다.

참고문헌

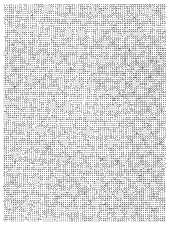
[1] IT보안인증사무국, "정보보호제품 평가인증 수행규정", 2007. 12

[2] IT보안인증사무국, "암호모듈 시험 및 검증지침", 2005. 1

[3] IT보안인증사무국, "정보보호제품 공공기관 도입 세부절차", 2007. 5

[4] http://www.kecs.go.kr

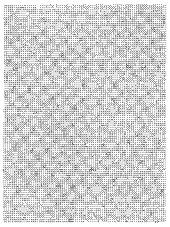
〈著者紹介〉



이 대 섭(Lee Dae Seob)

2007.1 ~ 현재 : 성균관대학교 컴퓨터 공학과 박사과정

관심분야 : 정보보호 평가인증



홍 원 순(Hong Won Soon)

2001 : 한국 정보통신대학교 IT경영학 석사

관심분야 : 정보보호 평가