情 報 保 護 學 會 誌
第19卷 第1號, 2009. 2

영국의 보안검증표시 스킴에 관한 분석

유 정 현*, 손 경 호**, 이 완 석**, 곽 진***

요 약

최근 정보보호의 중요성이 부각됨에 따라 보안성이 검증된 정보보호 제품/서비스에 대한 선호도가 높아지고 있다. 또한 보안성 평가로 검증된 정보보호 제품/서비스의 보안 기능에 대한 안전성과 신뢰성을 보증하기 위해서 보안검증표시 스킴의 필요성이 증대되고 있다. 이에 따라 본 고에서는 영국의 보안검증표시 스킴에서 규정하는 보안검증표시 스킴의 체계, 절차, 검증 제품에 대해서 분석하고자 한다.

Ⅰ. 서 론

IT 산업과 정보 기술의 급속한 발달로 인하여 행정, 국방, 교육, 산업 등 국가의 모든 영역에서 정보 시스템에 대한 의존도가 높아지고 있다. 하지만 정보 유출, DoS 공격, 해킹 등에 따른 역기능도 확산되고 있는 추세이다. 이에 따라 국내·외 정부기관에서는 이러한 역기능을 방지하기 위해 보안 기능이 강화된 다양한 정보보호 제품/서비스가 도입되어 운영되고 있다.

이에 따라, 정보보호 제품/서비스에 대한 정보보증의 중요성이 증대되고, 보안성 평가가 완료된 제품에 대한 보안검증표시 스킴이 요구되고 있다.

따라서 본 고에서는 영국의 통신전자보안그룹에서 시행하는 보안검증표시 스킴에 대해서 분석할 수 있도록 2장에서는 "보안검증표시 스킴의 정의"에 대해서 설명하고, 3장에서는 "보안검증표시 스킴의 체계"에 대해서 기술한다. 4장에서는 "보안검증표시 스킴의 절차"에 대해서 설명하고, 5장에서는 "보안검증표시 검증 제품"을 분석한 후 6장에서 결론을 맺는다.

Ⅱ. 보안검증표시 스킴의 정의

영국 내각 산하에서 정부기관의 정보보호 프로젝트에 대한 조정 역할을 수행하는 중앙정보보증기구(CSIA : Central Sponsor for Information Assurance)는 정보보증의 주요 고려 사항인 정보보호 제품/서비스의 보안 기능에 대한 타당성을 시험하기 위해 보안검증표시 스킴(CCTM : CSIA Claims Tested Mark)을 2005년 1월에 제정하였다. 그 후 2008년 4월 7일부터 중앙정보보증기구의 소유권이 통신전자보안그룹(CESG : Communication Electronics Security Group)으로 이전하면서 보안검증표시 스킴(CCTM : CESG Claims Tested Mark)으로 명칭이 변경 되었다[1].

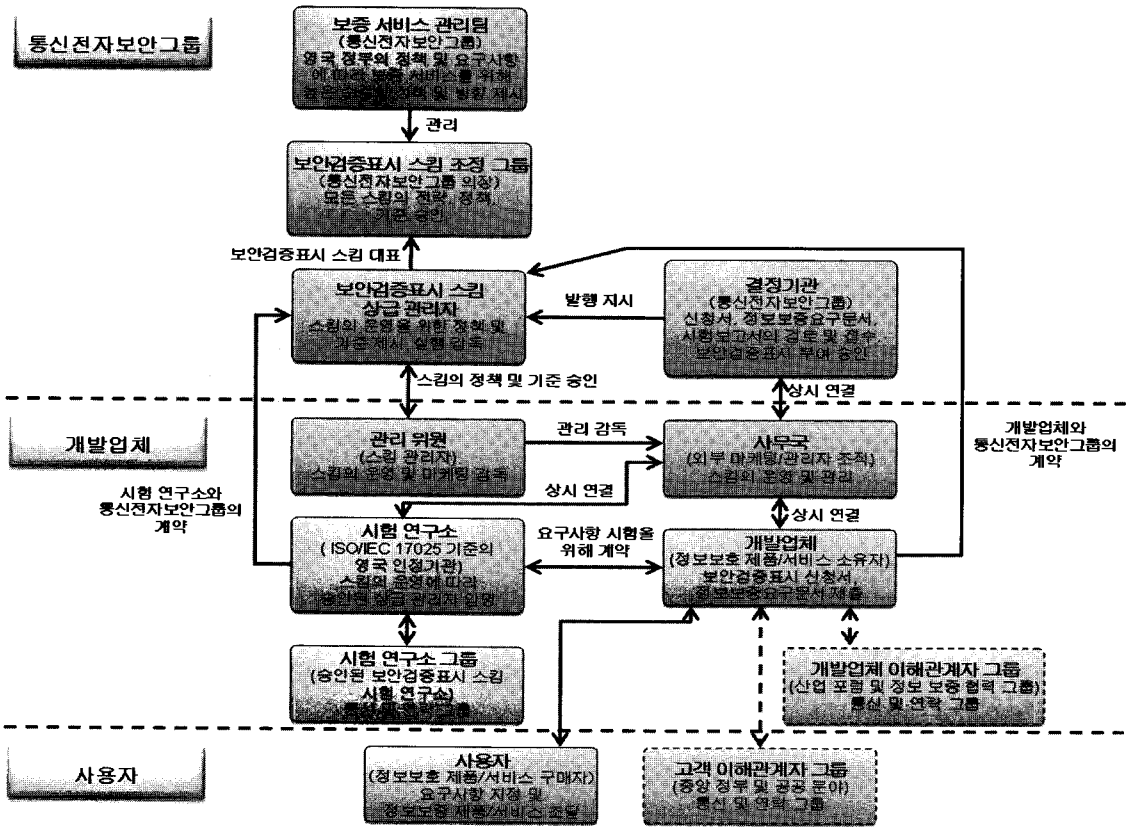
보안검증표시 스킴은 공공 및 개인을 위하여 보안 기능 요구사항의 유효성 증명을 위해 고안된 독립적 시험을 통하여 인가된 제품에 정부 보증 품질 마크를 제공한다. 이러한 시험보고서는 ISO/IEC 17025와 영국의 인정 기관(UKAS : United Kingdom Accreditation Service)에 의한 보안검증표시 스킴에 의거하여 인가를 받는다. 또한, 정보보호 제품/서비스의 비용-효과 창출 및 요구사항 시험(claims testing) 기능의 능률성에 대한 정부와 산업체의 요구를 충족시킨다. 따라서 보안검증표시 스킴은 정부 및 공공 기관, 지방자치 단체 등이 정보보증 요구사항을 만족하는 정보보호 제품/서비스 구매를 용이하게 한다[2][3].

Ⅲ. 보안검증표시 스킴의 체계

3.1 조직 및 역할

본 절에서는 요구사항 시험 및 승인 과정에서 주요

* 순천향대학교 정보보호학과 (jhyoo@sch.ac.kr)
** 성균관대학교 정보보호그룹 (khson@security.re.kr, wsyi@kisa.or.kr)
*** (교신저자) 순천향대학교 정보보호학과 교수 (jkwak@sch.ac.kr)



〔그림 1〕 보안검증표시 스킴의 조직 및 관리체계

관계자의 역할과 관련 정책 및 접근 방법에 대해서 설명한다. [그림 1]은 보안검증표시 스킴과 관련된 조직 및 관리체계를 나타낸다.

보안검증표시 스킴의 주요 관계자는 다음과 같다.

- ○보안검증표시 스킴 조정 그룹
- ○상급 관리자
- ○관리 위원
- ○결정기관
- ○시험 연구소
- ○개발업체 및 서비스 제공자
- ○사무국
- ○사용자

3.1.1 보안검증표시 스킴 조정 그룹

보안검증표시 스킴은 전자통신보안그룹에서 관리되고 있는 정보 보증 컨설팅 서비스에 대한 포트폴리오의 일부로서 운영된다. 보안검증표시 스킴 조정 그룹은 최상위 등급의 방침을 제공하고 정책을 검토하며 전반적인 스킴의 성과에 대하여 모니터링을 실시한다.

3.1.2 상급 관리자

상급 관리자는 통신전자보안그룹에서 임명한다. 상급 관리자는 개발업체, 사용자, 시험 연구소, 기타 관계자의 식별된 요구사항을 고려하여 스킴을 운영하기 위한 목표, 검토 방침, 기준을 확립한다.

상급 관리자는 다음과 같은 업무를 수행한다.

- ○결정기관 운영
- ○전반적인 스킴 운영
  - 스킴 관리 위원 임명
  - 결정기관, 사무국 선정
- ○스킴과 관련된 민원 관리

○스킴과 관련된 분쟁 중재 및 조정

3.1.3 관리 위원

관리 위원은 보안검증표시 스킴의 운영 관리를 위하여 상급 관리자로부터 지명되며, 다음과 같은 업무를 수행한다.

○스킴 운영 절차, 과정에 관한 조언 및 지침을 사무국에 제공
○작업 우선순위를 확립
○상급 관리자에게 스킴 운영에 관한 연례 보고서를 제출

3.1.4 결정기관

결정기관은 스킴 신청서 접수 및 보안검증표시를 부여하기 위하여 상급 관리자로부터 지정되며, 다음과 같은 업무를 수행한다.

○정보보호 제품/서비스의 요구사항 시험을 위한 정보보증요구문서를 검토
○신청서 승인 여부에 관한 결정을 사무국에 통지
○시험보고서, 추가 시험보고서, 시험보고서 요약문, 최종 정보보증요구문서를 검토 및 수용
○정보보호 제품/서비스의 보안검증표시를 부여
○상급 관리자, 사무국, 관리 위원을 통한 문의 사항이나 문제 발생 시, 지침과 조언을 제공

3.1.5 시험 연구소

시험 연구소는 스킴의 원활한 운영을 위하여 상급 관리자로부터 지정되며, 다음과 같은 업무를 수행한다.

○상급 관리자에 의하여 규정된 스킴을 준수
○ISO/IEC 17025, 요구사항 시험 방법론 준수
○스킴 인증서를 인정하고 유지
○상업적 기밀성을 최고 수준으로 유지

3.1.6 개발업체 및 서비스 제공자

개발업체는 개발자 또는 개발 조직이며, 서비스 제공자는 정보보호 서비스를 제공하는 정보보호 제품 또는 개발업체의 소유자이다.

개발업체 및 서비스 제공자의 역할은 다음과 같다.

○스킴 신청서 제출
○신청을 위한 추가 문서, 정보보증요구문서 준비
○최종 정보보증요구문서 준비
○시험 연구소와 계약 체결
○스킴의 조건 준수

3.1.7 사무국

사무국은 보고서를 작성하여 관리 위원에게 제출하며, 스킴의 운영을 지원하기 위해 다음과 같은 업무를 수행한다.

○스킴 등록 및 신청서 조회
○스킴 신청서에 관한 진행과정과 결과를 개발업체에게 통지
○스킴과 관련된 정보 제공 및 지원
○보안검증표시 스킴 웹사이트에 최종 정보보증요구문서와 시험보고서 요약문을 포함하여 세부사항을 게재
○보안검증표시 스킴 인증서 부여 준비
○보안검증표시 스킴 웹사이트에 모든 스킴 문서와 계약 유지 보수에 대한 정보 게재

3.1.8 사용자

사용자는 정보보호 제품/서비스를 구매 및 조달하는 사람이나 조직을 나타낸다. 사용자는 다음 사항을 통해 정보보호 제품/서비스의 정보를 얻을 수 있다.

○보안검증표시를 부여 받은 정보보호 제품/서비스의 정보는 웹사이트에 게재되어 있고, 추가 정보에 관해서는 개발업체에 연락하여 해당 업체를 통해 제공 받을 수 있다.

Ⅳ. 보안검증표시 스킴의 절차

4.1 보안검증표시 스킴의 신청

4.1.1 개요

본 절에서는 스킴 신청의 등록 및 접수에 관련된 개발업

체의 책임과 보안검증표시 부여에 관하여 설명한다[4].

4.1.2 정보보증요구문서

개발업체는 등록 신청서를 제출하기 전에, 정보보호 제품/서비스를 위한 정보보증요구문서를 준비해야 한다.

정보보증요구문서는 다음과 같은 사항을 제공하여야 한다.

- ㅇ스킴에 시험받을 정보보호 제품/서비스의 기능에 대하여 명백하고 정확한 서술 제공
- ㅇ보안검증표시가 부여 될 정보보호 제품/서비스의 기능 요구사항에 대한 요약문 포함(150글자 내외)
- ㅇ정보보증요구문서의 버전 표시
- ㅇ정보보호 제품의 버전과 플랫폼을 포함하여 명칭을 명시
- ㅇ정보보호 서비스의 평가기간을 포함하여 명칭을 명시

정보보증요구문서는 스킴 신청에 있어서 주요한 구성 요소이며, 다음과 같은 단계에서 사용된다.

- ㅇ등록 : 스킴 신청을 등록하기 위해서는 스킴 신청서와 제출물을 제출
- ㅇ신청 접수 : 정보보호 제품/서비스에 대한 정보보증요구문서의 스킴 시험 접수 결정을 결정기관에서 검토
- ㅇ요구사항 시험 : 정보보증요구문서에 명시된 정보보호 제품/서비스의 모든 요구사항 및 플랫폼 시험은 공인된 시험 연구소에 의해 수행
- ㅇ시험보고서 작성 : 시험 연구소는 정보보증요구문서에 명시될 모든 요구사항과 플랫폼을 위해 정보보호 제품/서비스의 시험보고서와 시험보고서 요약문을 준비
- ㅇ보안검증표시 부여 : 보안검증표시를 부여받은 정보보호 제품/서비스의 최종 정보보증요구문서는 시험보고서 요약문과 함께 웹사이트에 게재

개발업체는 사전에 보안검증표시 시험 연구소의 권고에 따라 정보보증요구문서를 작성해야 한다. 시험 연구소는 스킴에 정보보증요구문서를 제출하기 이전에 요구사항 시험의 가능 유·무를 판단하고, 시험에 대한 접근 및 기초적인 점검을 수행하는 것을 돕는다.

정보보호 서비스의 개발업체는 결정기관의 승인을 위해 5명의 고객이 응답한 설문조사를 고객의 회사명, 연락처와 함께 보안검증표시 사무국에 제출해야 한다. 개발업체는 리스트를 사무국에 제출하기 전에 선정된 고객의 연락처 및 시험 연구소와의 시험 계약서를 제출해야 한다.

시험 연구소는 정보보호 서비스를 이용한 고객들에게 요구사항에 대하여 인터뷰를 실시한다. 인터뷰 평가 기간은 요구사항 시험 시작 전에 12개월 동안 실시한다. 인터뷰는 보안검증표시 부여에 대한 유지 보수를 위해 필요하지만, 보안검증표시를 부여 후 6개월 이상 소요되지 않는다.

정보보호 제품/서비스의 개발업체는 다음 사항을 고려해야 한다.

- ㅇ정보보호 제품/서비스를 출시하기 위한 계획과 스킴 신청 시기를 고려해야 함
- ㅇ정보보호 제품/서비스의 차후 버전을 개발
- ㅇ요구사항 시험은 정보보증요구문서에 포함된 정확한 버전과 플랫폼을 보증
- ㅇ정보보호 제품/서비스가 시험된 이후에 구현된 새로운 버전 또는 추가적인 플랫폼은 보안검증표시에 따라 재제출하거나 유지 보수 신청 형태로 제출
- ㅇ시험 과정과 암호 검증의 통신전자보안그룹 지원 제품 서비스(CAPS : CESG Assisted Products Scheme), FIPS 140 평가 사이의 관계 및 의존도를 고려해야 함

4.1.3 등록

개발업체는 정보보호 제품/서비스의 시험을 신청하고, 보안검증표시를 부여받기 위해 정보보호 제품/서비스의 각 버전에 대한 신청서 및 정보보증요구문서를 구별하여 제출한다.

보안검증표시 스킴은 영국 외무 연방성과 개발업체와 계약을 체결한다. 계약서는 스킴에 참여하는 개발업체가 계약 내용을 준수할 것을 확약하고, 통신전자보안그룹의 역할에 대해서 명시하고 있다.

개발업체는 사무국의 신청 등록처에 다음 사항을 제출한다.

- ㅇ정보보호 제품/서비스를 등록하기 위한 보안검증

표시 신청서
- ㅇ정보보호 제품/서비스의 정확한 버전 및 플랫폼을 포함한 정보보증요구문서
- ㅇ정보보호 제품/서비스의 정확한 버전 및 플랫폼에 대한 사용자 또는 관리자 지침
- ㅇ정보보호 제품/서비스의 정확한 버전 및 플랫폼에 대한 마케팅 연구 보고서(웹사이트의 URL 포함)
- ㅇ개발업체 등록 수수료

사무국은 스킴의 요구 조건을 만족하는 신청서를 등록한다. 정보보호 제품/서비스의 스킴 신청서가 등록되면 개발업체는 신청 번호를 발급 받는다.

사무국은 다음 사항을 수행한다.
- ㅇ신청서의 정보를 바탕으로 개발업체의 계약서를 준비하고, 외무부 장관을 대신하여 통신전자보안그룹이 서명한 사본 2부를 준비
- ㅇ서명된 계약서 사본 2부를 개발업체에 보내고, 개발업체는 사본 2부에 서명을 한 뒤 사무국이 서명한 날로부터 10일 이내에 사본 1부를 사무국에 제출

4.1.4 신청 접수

사무국은 결정기관이 검토 및 승인할 신청서와 제출물을 준비한다.

결정기관에 의한 신청서와 제출물의 검토 및 승인은 개발업체에게 별도의 통보가 없는 한 일반적으로 5~10일 이내에 사무국에 의해 등록된다.

결정기관은 신청 접수/철회를 결정하여 사무국에 알린다. 사무국은 결정기관의 결정을 개발업체에게 통보하며, 신청 철회 시 그 이유를 개발업체에게 통보한다.

신청 접수 시 사무국은 개발업체의 계약서를 확인하고, 개발업체에게 신청 접수 확인을 통보한다. 스킴의 신청 접수에 정의된 조건들을 모두 만족하면 스킴 신청은 접수된다.

4.1.5 요구사항 시험

개발업체는 스킴에 명시된 문서에 따라 정보보증요구문서를 접수한 시험 연구소가 시험을 진행할 수 있도록 계약을 체결한다.

시험은 영국의 인정 기관에서 인증된 시험 연구소에서 진행되며 시험 연구소 지침에서 명시된 과정에 따라 실행된다.

요구사항 시험을 수행하는 시험 연구소의 목록은 스킴 웹사이트에 게재되어 있다. 사무국은 요구사항 시험에 사용될 스킴에 의거하여 승인된 정보보증요구문서의 개발업체를 확인하고, 개발업체는 시험에 대한 모든 권한을 시험 연구소에 위임한다.

모든 요구사항 시험은 사무국이 정보보증요구문서에 대한 접수 여부를 결정하기 전에 진행된다. 개발업체는 요구사항 시험을 수행하는 시험 연구소와 시험 시작 및 종료일에 대한 계획을 사무국에 보고한다.

개발업체는 시험 방법론, 계획, 스크립트 제작에 필요한 모든 기술 정보를 시험 연구소에 제공한다. 또한 시험 연구소의 요청이 있을 시에는 기술적 설명, 기술 문서, 개발업체의 기술 관리자 연락처를 제공한다. 시험 연구소는 이러한 정보를 시험 방법론 개발과 시험 환경 설정을 위하여 사용한다.

시험 연구소에 의한 요구사항 시험은 계약서에 명시한 날짜로부터 8주 이내에 시작하고, 요구사항 시험 기간은 20일 이내에 완료되어야 한다.

4.1.6 시험보고서 작성

시험 연구소는 기능성 시험의 결과, 기존의 보증 인증서 유효성, 시험 연구소 지침에 명시된 정보보호 서비스에 관한 형식과 절차에 의거한 유효성 검사, 감사, 인터뷰 결과를 문서화해야 한다.

정보보증요구문서에 대한 모든 시험이 완료되면 시험 연구소는 최종 버전의 시험보고서를 개발업체에게 배포한다. 또한 시험 연구소는 시험보고서와 시험보고서 요약문을 사무국에 제출한다.

개발업체는 최종 버전의 시험보고서를 검토한 후 관찰 결과와 권고사항을 포함하여 시험보고서와 시험보고서 요약문을 사무국에 제출한다.

개발업체는 시험보고서가 시험 연구소의 권고사항을 참고하여 정보보증요구문서를 수정하고 최종 정보보증요구문서를 작성한다. 개발업체는 정보보증요구문서의 기본적인 검토를 수행하기 위하여 시험 연구소에 정보보증요구문서를 제출한다. 시험 연구소는 최종 정보보증요구문서, 시험보고서와 시험보고서 요약문을 사무국에 제출한다.

시험보고서와 시험보고서 요약문은 개발업체가 사무국으로부터 정보보증요구문서가 요구사항 시험에 합격

하였다고 통보받은 날로부터 3개월 이내에 사무국에 제출해야 한다. 만약 사무국은 지정된 기한 내에 시험보고서를 제출받지 못하였을 경우, 사무국은 결정기관, 개발업체, 시험 연구소의 확인을 통해 신청을 취소할 수 있다.

4.1.7 보안검증표시 부여

사무국은 결정기관이 검토 할 시험보고서, 시험보고서의 요약문, 추가 시험보고서, 최종 정보보증요구문서와 보안검증표시 부여 결정 절차를 준비한다.

결정기관은 시험보고서 및 추가 시험보고서에서 다음 사항을 검토한다.

- ㅇ시험 연구소 지침에 명시된 절차에 따라 정보보증 요구문서가 시험 받았는지 확인
- ㅇ시험 연구소의 시험 결과 및 소견 검토
- ㅇ보안검증표시 부여 여부 결정

결정기관에 의한 신청서와 문서의 검토 및 승인은 개발업체에게 별도의 통보가 없는 한 일반적으로 5~10일 이내에 사무국에 의해 등록된다.

결정기관은 시험보고서를 검토하고 정보보호 제품/서비스에 대한 보안검증표시 부여 여부를 결정한다. 또한, 다음을 고려하여 시험보고서의 요약문과 최종 정보보증요구문서를 검토한다.

- ㅇ시험 연구소에 의해 권고된 정보보증요구문서의 변경사항과 결정기관에 의해 승인된 내용만 포함되어 있는지 확인
- ㅇ시험보고서의 요약문이 시험 연구소의 지침에 만족하는지 확인
- ㅇ정식으로 보안검증표시 부여 시, 웹사이트에 게재하기 위해 시험보고서 요약문과 최종 정보보증요구문서 승인

결정기관은 정보보호 제품/서비스의 보안검증표시 부여 여부를 확인하여 시험보고서의 요약문과 최종 정보보증요구문서를 웹사이트에 게재하는 것을 승인한다. 사무국은 결정기관의 결정을 개발업체에게 통보하고 보안검증표시 부여가 승인 되지 않으면 신청이 철회된다.

결정기관에 의해 보안검증표시 부여가 승인되면 사무국은 웹사이트에 정식 발표를 위한 준비를 하며, 최대 10일 정도의 기간이 소요된다.

정식 발표는 다음과 같은 사항을 포함한다.

- ㅇ스킴의 승인을 받은 최종 정보보증요구문서와 시험보고서의 요약문을 웹사이트에 게재
- ㅇ정보보호 제품/서비스 명칭 및 관련 마케팅 정책을 웹사이트의 보안검증표시 부여 목록에 게재
- ㅇ개발업체에게 배부되는 인증 번호와 보안검증표시 로고 발행
- ㅇ정보보호 제품/서비스의 정확한 버전 및 플랫폼에 사용될 보안검증표시 로고를 개발업체에 전달(보안검증표시 로고에 인증 번호 및 로고 사용 지침서 포함)
- ㅇ정보보호 제품/서비스의 보안검증표시 인증서에 상급 관리자의 서명을 기입하여 개발업체에게 발행

4.2 보안검증표시의 유지 보수

4.2.1 개요

본 절에서는 정보보호 제품/서비스를 위한 보안검증표시의 유지 보수 과정을 설명한다. 보안검증표시의 유지 보수 계약에 적용되는 사항은 다음과 같다.

- ㅇ제품명이나 소유권이 변경되었을 경우에도 정보보호 제품/서비스의 보안검증표시의 효력은 유지
- ㅇ서비스의 유지 관리 조건 확인을 통하여 보안검증표시 연장 가능(발급 후 2년차)

4.2.2 유지 보수를 위한 신청 준비

기존에 명시된 정보보호 제품/서비스의 명칭, 버전 및 소유권이 변경되더라도 개발업체는 정보보호 제품/서비스를 유지해야 한다.

다음의 경우, 보안검증표시 유지 보수 신청서를 사무국에 제출한다.

- ㅇ기존의 정보보호 제품/서비스에 부여되었던 인증서의 효력 지속 기간을 변경된 정보보호 제품/서비스명에 이전할 경우
- ㅇ보안검증표시 효력 기간 만료 이전에 정보보호 서비스 유지 보수를 위한 갱신 등록 시(2년 유지 보수)

정보보호 제품/서비스명과 소유권이 변경되었을 경우, 개발업체는 정보보증요구문서를 갱신하고 재제출한다. 시험 연구소는 이에 대한 기본적인 재시험을 요구하지 않는다.

4.2.3 유지 보수를 위한 등록

개발업체는 스킴에 정보보호 제품/서비스의 보안검증표시 유지 보수를 위해 신청서를 제출해야 한다. 개발업체는 사무국에 다음과 같은 사항을 제출하여야 한다.

- ㅇ정보보호 제품/서비스에 대해 보안검증표시 유지 보수를 기록하기 위한 보안검증표시 신청서
- ㅇ보안검증표시를 부여받은 정보보호 제품/서비스의 정확한 버전과 플랫폼을 위한 개정된 정보보증요구문서
- ㅇ보안검증표시 유지 보수를 위한 개발업체 수수료

정보보호 서비스를 위해서 개발업체는 12개월 동안 서비스를 사용하고 시험 연구소와 스킴 계약에 동의한 2~5명의 고객의 연락처 정보(이름, 조직명)를 보안검증표시 사무국에 제출해야 한다. 이러한 고객은 시험 연구소의 인터뷰를 결정기관에 의해 승인받고, 정보보호 서비스가 정보보증요구문서에서 정해진 요구에 따라 동일한 서비스를 제공하는 것을 검증한다.

신청서가 스킴의 조건을 만족하면 사무국은 신청서를 등록한다.

4.2.4 유지 보수를 위한 신청 접수

사무국은 결정기관의 결정을 다음 사항과 같이 개발업체에 통보한다.

- ㅇ결정기관의 신청 접수 여부
- ㅇ결정기관이 작성한 보안검증표시의 유지 보수 신청 접수의 취소사유서를 개발업체에 통보

4.2.5 유지 보수를 위한 요구사항 시험

요구사항 시험은 4.1.5와 동일하다.

4.2.6 유지 보수를 위한 시험보고서 작성

시험보고서의 작성은 4.1.6과 동일하다.

4.2.7 유지 보수를 위한 보안검증표시 부여

결정기관은 새로운 시험보고서에 대해서 다음과 같은 사항을 검토한다.

- ㅇ인터뷰/설문조사가 정확한지 확인하고 그 결과를 수용할 수 있는지 확인
- ㅇ보안검증표시 부여 여부를 결정

결정기관이 보안검증표시 유지 보수를 위하여 보안검증표시 부여를 승인하면, 사무국은 다음과 같은 사항을 준비한다.

- ㅇ개발업체에게 부여되는 새로운 인증서
- ㅇ개발업체에게 발행되는 새로운 인증서 번호와 보안검증표시 로고

새로운 인증서는 정보보호 제품/서비스를 위한 기존 인증서의 잔여기간 동안 유효하다.

4.3 결정기관의 검토 과정

4.3.1 결정기관의 책임

보안검증표시 스킴 결정기관의 역할은 다음과 같다[5].

- ㅇ스킴의 기술 및 절차에 대한 정보보증요구문서의 권고 및 지침을 기반으로 각 신청서에 적용하는 것을 보증
- ㅇ요구사항 시험 수행 및 보안검증표시를 부여하기 전에 정보보증요구문서의 요구사항과 마케팅 정책에 대한 유효성과 완전성을 보증
- ㅇ정보보증요구문서의 시험 방법론이 정보보증요구문서의 모든 요구사항과 잘 알려진 취약성을 다루며, 플랫폼의 조합이 관련 결함에 적합함을 보장
- ㅇ시험보고서(추가 보고서 포함)의 검토를 기반으로 보안검증표시 부여 최종 결정
- ㅇ상위 기관의 권고에 따른 기준 및 절차의 정기적인 검토 보증

4.3.2 결정기관의 검토 요구사항

정보보증요구문서, 시험보고서, 추가 시험보고서, 시험보고서 요약문은 개발업체와 시험 연구소의 지침을 따르며, 결정과 승인 절차에 따라 결정기관에서 검토한다.

정보보증요구문서와 관련된 결정기관의 검토 기록과 이에 요구되는 개발업체의 활동은 사무국이 개발업체의 활동 준수 사항을 위해 발행하는 정보보증요구문서의 결정기관 검토 양식에 따라 결정기관이 문서화를 실시한다. 시험보고서에 관련된 결정기관의 검토 기록, 추가 시험보고서, 시험보고서 요약문과 이에 따라 요구되는 시험 연구소 활동은 사무국이 시험 연구소의 활동 준수 사항을 위해 발행하는 시험보고서는 결정기관의 검토 양식에 따라 결정기관이 문서화를 실시한다.

정보보증요구문서 또는 시험보고서 컨퍼런스콜(Conference-Call)에서 협의한 결정기관의 결정 및 개발업체/시험 연구소 활동은 결정기관의 검토 양식에 기록한다.

결정기관은 사무국으로부터 전달받은 문서를 8일 이내에 결정기관 검토 과정을 완료시키고, 사무국에게 결정기관 검토 양식을 반송한다. 모든 결정기관 검토의 서면답변서는 사무국을 통해서 개발업체 또는 시험연구소에 의해 결정기관으로 전달된다.

4.4 결정기관의 평가 절차

4.4.1 1차 정보보증요구문서 검토

정보보증요구문서 검토의 목적은 정보보증요구문서가 개발업체, 시험 연구소 지침대로 스킴의 요구사항을 충족시키는 것을 보증한다.

1차 시험보고서는 검토하고, 정보보증요구문서의 요구사항을 고려해야 한다. 만약 정보보증요구문서의 요구사항을 충족시키지 못한다면 정보보증요구문서 결정기관의 검토 양식에 이를 기술한다.

또한 정보보증요구문서에서 사용자의 오해를 초래할 수 있는 문제점이 발생한다면 개발업체는 결정기관의 검토 양식을 이용하여 보고한다.

4.4.2 2차 정보보증요구문서 검토

결정기관은 정보보증요구문서의 변경 사항, 개발업체 또는 시험 연구소의 서면답변서에서 결정기관의 검토에 제시된 요점들을 재확인한다.

4.4.3 정보보증요구문서 컨퍼런스콜

2차 정보보증요구문서 검토 후에도 문제점이 남아 있다면, 결정기관, 시험 연구소, 개발업체 사이에 컨퍼런스콜을 준비한다. 컨퍼런스콜은 시험 전이나 시험 완료 후, 문제점들을 해결하고자 정보보증요구문서에 필요한 변경사항에 대해서 회의를 갖는 과정이다.

4.4.4 정보보증요구문서 승인

정보보증요구문서 검토에서 문제점이 발생하지 않았다면, 결정기관은 정보보증요구문서를 승인하고 요구시험을 수행한다. 만약 2차 정보보증요구문서 검토에서 문제점이 발생하게 되면, 결정 기관은 승인 조건을 제시한 조건부 승인을 통보하거나, 정보보증요구문서를 제출한 개발업체에게 잠정적 신청 철회를 통보한다.

이러한 조건부 승인은 정보보증요구문서 결정 기관의 검토에 기록된다.

- ㅇ요구사항 시험 완료 후 정보보증요구문서에 대한 결정 기관의 검토 또는 시험 연구소의 서면답변서에서 요구하는 변경사항을 수정한 시험보고서와 함께 제출된 정보보증요구문서의 사본을 제출해야 함
- ㅇ정보보증요구문서의 수정은 요구사항 시험 시작 전에 이메일 전송 또는 컨퍼런스콜에 제출하여 주어진 시간 내에 완료해야 함
- ㅇ요구시험 완료 후 정보보증요구문서의 간단한 변경 사항도 수정하여 시험보고서를 작성하고, 정보보증요구문서의 사본과 함께 제출해야 함

4.4.5 시험보고서 검토

시험보고서 검토의 목적은 시험 연구소의 권고와 관찰 보고를 검토 및 승인을 수행하는 과정이다. 또한 시험 연구소는 정보보증요구문서에서 제시된 시험 요구사항에 따라 시험을 수행한다.

1차 시험보고서에서 중요하지 않은 정보보증요구문서 요구사항의 일부분에 대한 삭제를 요청 시, 평가에 영향을 끼치지 않거나 정보보호 제품/서비스의 효율성에 필수적이지 않다면 결정기관은 이 요구사항을 제거

하는데 동의한다. 또한, 마케팅 정책은 관련 요구사항을 제거하기 위해 개정한다.

요구사항이 마케팅 요소가 정보보호 제품/정보보호 서비스 문서에서 개발업체가 촉진하고 있는 기능의 주요 부분과 관련이 있으면, 결정기관은 요구사항을 제거하는 것에 관하여 동의하지 않는다. 결정기관이 요구사항을 제거하는 것에 관하여 동의하지 않을 경우에, 개발업체는 확인된 이 문제를 해결하기 위해서 적절한 방안을 마련해야 한다.

요구사항 시험을 위해 지정된 플랫폼 조합에서 일부분의 기능이 동작하지 않는다면, 정보보증요구문서의 요구사항은 어떠한 플랫폼 조합에서 작동하지 않는지 수정하여 명시해야 된다.

또한 시험 연구소의 시험보고서에 있는 권고와 관찰 보고를 충족하여야 하며 만약 그렇지 않으면, 결정기관의 검토 기준을 충족시키기 위해서 개발업체와 시험 연구소는 적절한 방안을 마련한다.

4.4.6 추가 시험보고서 검토

결정기관에 의해 제안된 시험보고서의 설명들은 시험 연구소 또는 개발업체에 의해 명백히 언급되어야 한다. 이것은 기준에 의거하여 결정기관이 검토한다.

추가 시험보고서에서 시험 연구소 권고 및 관찰 보고를 충족하여야 하며 만약 그렇지 않으면, 결정기관의 검토 기준을 충족시키기 위해서 개발업체와 시험 연구소는 적절한 방안을 마련해야 한다.

4.4.7 시험보고서 컨퍼런스콜

추가 시험보고서 검토 후에 문제점이 남아있다면 결정기관, 시험 연구소, 개발업체 사이에 컨퍼런스콜을 준비한다. 이는 문제점을 해결하고 보안검증표시를 부여하기 전에 정보보증요구문서, 요구사항 시험, 시험보고서를 완료하는데 필수적인 요소이다.

4.4.8 보안검증표시 부여 결정

문제점들이 해결되고 결정기관의 검토에서 언급된 모든 조건을 충족시킨다면, 결정기관은 시험보고서 결정기관의 검토에서 보안검증표시를 부여한다.

시험보고서 또는 관련된 추가 시험보고서의 검토 후에 최종 정보보증요구문서 또는 시험보고서 요약문에 변경 사항이 있다면, 결정기관은 조건을 제시하여 보안검증표시를 부여한다. 이러한 조건은 보안검증표시 스킴 웹사이트에서 공식적으로 부여를 발표하기 전에 최종 정보보증요구문서와 시험보고서 요약문에 적용되는 변경사항이다.

만약 시험보고서 컨퍼런스콜 이후에도 문제점이 남아있다면, 결정기관은 보안검증표시 부여를 하지 않는다.

4.4.9 발행 검토

발행 검토는 시험보고서 요약과 최종 정보보증요구문서를 처리하고 결정기관에 의하여 검토되고 승인 받는다. 시험보고서를 검토 한 후에, 시험보고서 또는 추가 시험보고서의 결과물은 결정기관에 의해 승인되며, 보안검증표시 부여를 결정한다.

결정기관은 모든 중점들이 처리되는 것을 보증하기 위해 결정기관의 검토와 비교하여 최종 정보보증요구문서 및 시험보고서 요약문에 대한 변경사항을 점검한다. 또한, 결정기관은 마케팅 정책의 일관성을 위해 최종 정보보증요구문서 및 시험보고서 요약문을 점검하기도 한다.

최종 정보보증요구문서와 시험보고서 요약문에서 사용자의 오해를 초래할 수 있는 문제점이 발생한다면 개발업체 또는 시험연구소에서 결정기관의 검토양식을 이용하여 보고한다.

V. 보안검증표시 검증 제품

본 절에서는 위에서 분석한 자료를 토대로 영국의 보안검증표시 스킴의 검증을 받은 제품들의 명칭, 제품/서비스 버전, 개발업체, 검증 일자에 대한 정보를 기술한다. [표 1]~[표 7]은 보안검증표시 스킴의 검증을 받는 제품 목록의 사양을 나타낸다[6][7].

〔표 1〕 연결 보호 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
HP ProtectTools Email Release Manager	Product	5.0	Hewlett Packard	2006.05.17

〔표 2〕 미디어 및 장치 인증 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
Connect Protect	Product	2.0	BeCrypt	2006.04.26
Connect Protect	Product	1.6.2.6	BeCrypt	2007.09.08
DeviceWall	Product	4.01	Centennial Software	2006.09.05
Excelsior Security Manager	Product	1.0	CGI (Europe) Ltd	2007.09.27
Credant Mobile Guardian Enterprise Edition	Product	5.2.1	Credant Technologies	2008.02.18
Reflex Disknet Pro	Product	4.5.1	Reflex Magnetics	2007.11.07
Sanctuary Device Control	Product	2.8.7	SecureWave	2007.09.08
Secure Data Media Solutions Service	Service	1.0	SDMS Ltd	2008.12.19
Secure Data Media Solutions Service	Service	1.0	SDMS Ltd	2008.12.19
Trusted Client Platform	Product	1.2	BeCrypt	2007.09.27

〔표 3〕 미디어 및 정보보호 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
DESlock+	Product	3.2.7	Data Encryption Systems Ltd	2008.05.13
Disk Protect	Product	4.1	BeCrypt	2006.10.23
PDA Protect	Product	4.1	BeCrypt	2006.11.30
Pointsec for PC Enterprise Workplace Edition	Product	5.2.2	Pointsec Mobile Technologies Ltd	2006.04.26
Pointsec for Pocket PC	Product	2.3.10	Pointsec Mobile Technologies Ltd	2006.10.30
SafeBoot® Device EncryptionTM for PC/Laptop	Product	5.0	SafeBoot	2006.09.05
Syntaxis Shared Collaborative Working Environment Service	Service	2.7	Ultra Electronics Datel	2008.06.28
Virtual Infrastructure Access Services	Service	5.5b	IBM United Kingdom Ltd	2007.05.13

〔표 4〕 네트워크 링크 보호 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
AEP Netilla Security Platform	Product	5.2.3.7	AEP Networks	2006.11.30
Juniper Networks Secure Access Family	Product	5.4R2.1	Juniper Networks (UK) Ltd	2007.04.24
Whale Intelligent Application Gateway	Product	3.1	Whale Communications	2008.02.27

〔표 5〕 말소 및 폐기 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
Hard Disk Magnetic Crusher COMBO	Product	1.0	Future Technology Industry Limited	2007.06.13
Hard Disk Magnetic Crusher HC 3000	Product	1.0	Future Technology Industry Limited	2007.06.13
Hard Disk Magnetic Crusher HC 7800	Product	1.0	Future Technology Industry Limited	2007.08.06
Managed Service for Secure Destruction of Data on Magnetic Media Holding Protective Markings of up to & including (IL6) Top Secret	Service	1.0	Barron McCann Technology Ltd	2008.11.27
Managed Service for Secure Destruction of Data on Magnetic Media	Service	1.0	Barron McCann Technology Ltd	2008.11.28
Secure Destruction of Data on Magnetic Media	Service	1.0	R&R Data Managed Services Limited	2008.02.27
Secure Destruction of Data on Magnetic Media	Service	1.0	Ultratec Limited	2007.09.14
Secure Destruction of Data on Hard Drives and Magnetic Storage Media	Service	1.0	Data Eliminate Limited	2008.09.11

〔표 6〕 무결성 보호 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
eSafe	Product	5.2	Aladdin Knowledge Systems Limited	2007.03.07
Application Manager	Product	6.0	AppSense	2007.10.21
Digital Record Object Identification (DROID)	Product	3.0	The National Archives	2008.02.27
MessageLabs Anti-Virus Service	Service	5.1	MessageLabs	2006.04.26
MessageLabs Anti-Virus Service	Service	5.1	MessageLabs	2007.11.05
NI Enterprise Manager	Product	5.0	NetIntelligence Limited	2007.10.30
Sanctuary Standard Edition	Product	2.8.0	SecureWave	2007.09.08
TruSeal	Product	2.0	TruData Integrity	2007.11.08

〔표 7〕 검증 시설 분야의 검증 제품

제품명	제품/서비스	버전	개발업체	검증 일자
Health Check	Service	1.0	Digital Assurance Consulting Ltd	2008.12.04

Ⅵ. 결 론

본 고에서는 영국의 통신전자보안그룹에서 시행하는 보안검증표시 스킴에 대해서 분석하였다.

보안검증표시 스킴과 관련된 조직 및 역할에 대해서 알아보고, 보안검증표시 스킴의 신청 · 등록 · 요구사항 시험 · 시험보고서 작성 · 보안검증표시 부여 · 유지보수 등 평가 절차를 분석하였다. 또한 영국의 통신전자보안그룹의 홈페이지에 등록된 보안검증표시 검증 제품 목록을 분석하였다.

국내에는 정보보호 제품/서비스에 대한 효율적인 인식이 부족한 실정이다. 본 고에서 분석한 영국의 보안검증표시 스킴을 국내 실정에 맞춰 도입한다면 정부 및 공공기관의 정보보호 제품/서비스 도입에 필요한 비용과 시간의 효율성을 높일 수 있고, 보다 발전된 보안 평가 서비스로 향상 될 것으로 예상된다.

참고문헌

[1] CSIA, "Csia Claims Tested Mark Scheme Description of the Scheme", 27 February 2008.

[2] CESG, "Helping deliver confidence in information assurance", May 2008.

[3] CESG, "How to deliver confidence in assurance for your product and sevice claims", May 2008.

[4] CSIA, "Csia Claims Tested Mark Scheme Vendor Guide", 27 February 2008.

[5] CSIA "Csia Claims Tested Mark Scheme Decision Authority Guide", 27 February 2008.

[6] CESG, "Directory of CESG Claims Tested Mark (CCTM) Awards for Products and Services", January 2009.

[7] http://www.cctmark.gov.uk(CCTM 홈페이지).

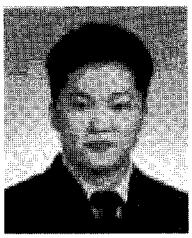
〈著者紹介〉

유 정 현 (Junghyun Yoo)

학생회원

2005년 3월~현재: 순천향대학교 정보보호학과 재학

<관심분야> 정보보호



손 경 호 (Kyungho Son)

특별회원

2001년 2월: 성균관대학교 전기전자컴퓨터공학과 학사

2004년~현재: 성균관대학교 컴퓨터공학과 석 · 박사과정 재학중

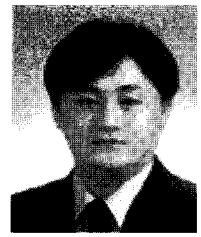
2001년 1월~현재: 한국정보보호진흥원(KISA) 선임연구원

<관심분야> 정보보호, 정보보호제품 및 시스템 보안성평가, 스마트카드 취약성

이 완 석 (Wan S. Yi)

정회원

1991년 5월: Va. Tech. 전산과학과 학사
2001년 2월: 동국대학교 정보보호학과 석사
2004년~현재: 성균관대학교 전자공학과 박사과정
1994년~1996년: 현대정보기술 CAD/CAM사업부 사원
1996년~현재: 한국정보보호진흥원 IT기반보호단 u-IT서비스 보호팀 팀장
<관심분야> 정보보증, 정보보호 제품 평가, 정보통신기반보호, 신규 IT서비스 보호



곽 진 (Jin Kwak)

종신회원

성균관대학교 학사, 석사, 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재: 순천향대학교 정보보호학과 교수
<관심분야> 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, u-City 정보보호 기술 등