情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

영국의 맞춤형 보증 서비스 제도 분석을 통한 국내 평가서비스 향후 발전방향

고 웅*, 곽 진**

요 약

정보화 사회가 추진됨에 따라 다양한 IT 제품 및 시스템의 개발이 증가되고 이를 통한 삶의 질적 향상 및 효율적인 생활을 이루게 되었다. 하지만 정보화 사회의 역기능 현상이 발생하게 되면서 IT 제품 및 시스템의 보안성 평가 서비스에 대한 관심이 증가하게 되었다. 이에 따라 다양한 보안성 평가 서비스가 개발되고 연구되고 있는 상황이다. 본 고에서는 이러한 보안성 평가 서비스 개발 및 연구에 필요한 선행연구로서 영국의 맞춤형 보증 서비스 제도의 절차 및 기준을 분석하고 이를 기반으로 국내 평가 서비스의 향후 발전 방향에 대해 제시하고자 한다.

Ⅰ. 서 론

최근 들어 사회의 각 분야에서 정보화가 추진됨으로써 정보사회가 가져다주는 긍정적인 효과를 위한 다양한 IT 제품 및 시스템의 개발이 증가하고 있다. 그러나 초기 정보화의 발전 속에서도 이슈가 되지 못했던 정보의 누출, 변조, 오용과 같은 정보화 역기능 현상의 발생이 빈번하게 늘어남으로써 최근 정보보호 문제가 중요한 이슈로서 다루어지게 되었다. 이러한 문제점을 위해서 선결되어야 할 주요 현안으로 IT 제품 및 시스템에 대한 검증된 보안성 평가 기술이 떠오르고 있다.

보안성 평가 기술은 기존의 암호기술과 함께 IT 제품 및 시스템 정보보호를 위한 핵심기술의 하나이며, 국내외에서 활발하게 그 연구가 진행되고 있다. 정보보호 제품의 보안성 검증과 효율성을 위하여 공통평가기준이 마련되었으며, 이를 통해 IT제품이 예상되는 모든 보안 위협요소들에 대해 어떻게 대응하고 있으며 보안성이 어느 정도 있는가를 평가할 수 있는 기준을 제공하여 준다.

하지만 공통평가기준이 가지고 있는 이점과 동시에 그에 따른 평가 검증 시간 및 비용 상의 단점도 부각되면서 이를 해결하기 위하여 세계 각국이 자국에 맞는 효율적인 보안성평가 서비스를 제안하고 시행하고 있다.

본 고에서는 IT 제품 및 시스템의 평가 보증을 위한 영국의 맞춤형 보증 서비스 제도(CESG Tailored Assurance Service)를 분석하고 이를 기반으로 국내 평가 서비스가 나아갈 방향을 제시하여 본다.

본 고의 구성은 다음과 같다. 2장에서는 영국의 전반적인 보안성 평가 서비스를 분석하고, 3장에서는 영국 내에서 시행 중인 맞춤형 보증 서비스 제도를 분석한다. 4장에서는 분석한 내용을 토대로 국내 평가서비스가 나아갈 방향을 제시하고 5장에서 결론을 맺는다.

Ⅱ. 영국 보안성 평가 서비스

2.1 정보 보증 및 컨설턴트 서비스

영국의 CESG(Communication Electronics Security Group)에서 보안성 평가 서비스에 관련된 모든 업무를 주관하고 있으며, 그 중 중앙 정부 및 지방 자치 기관에 제품 및 시스템을 제공하기 위한 평가로써 IACS (Information Assurance & Consultancy Services)를 제공하고 있다.

IACS는 국가 기관의 요구에 적합한 IT 제품 및 시스

* 순천향대학교 정보보호학과 정보보호응용및보증연구실 석사과정 (wgo@sch.ac.kr)
** (교신저자) 순천향대학교 정보보호학과 교수 (jkwak@sch.ac.kr)

템의 보안 기능 보증을 위하여 설계되었다. 이를 통해 발생 가능한 다양한 취약성 검증을 제공하며, 영국 내의 활용되는 제품 및 시스템 보안 기능을 객관적이고 독립적인 환경에서 보증하고 있다.

다음 [표 1]은 IACS에서 제공하고 있는 서비스를 정리한 것이다.

〔표 1〕 IACS 제공 서비스[1][4]

서비스	내용
CESG Listed Adviser Scheme (CLAS)	- 영국 정부 및 공공 기관에 정보 보증 컨설턴트 제공 - 위협, 취약성, 보안 대책의 공식적인 평가
CESG Assisted Products Service (CAPS)	- 암호 보안 기법을 사용하는 제품의 개발자 및 사업자에게 디자인 컨설턴트 업무 제공 - 제품들이 정부 기준에 부합하는지 검증
CESG Claims Tested Mark (CCTM)	- 독립 테스트 기반의 공공 및 개인 분야를 위한 정부 품질 마크 제공 - 사업자가 주장하는 보안 기능의 유효성을 검증하기 위하여 설계
CESG Tailored Assurance Service (CTAS)	- 보증 활동 툴박스 사용 - 정부 IT 시스템 보증 지원 서비스 - 취약성 탐지 기준 향상을 위한 방식으로 설계
IT Health Check Service (CHECK)	- 취약성으로부터 검증된 IT 시스템과 네트워크를 필요로 하는 정부와 CNI (Coalition for Networked Information) 편의를 위하여 설계
Common Criteria (CC)	- 정보 보안성의 보증을 요구하는 제품에 공식적인 인증 및 승인을 제공하는 국제 공통 평가 기준
Compliance Checking	- IS5, Manuals T, V, Y를 포함한 Infosec 표준에 의거한 검사 제공
Tempest	- Tempest 인증은 CESG의 공인된 테스트 설비를 통하여 실시

○ CESG Listed Adviser Scheme (CLAS)

- 본 서비스는 영국 정부 및 공공 기관에 유용한 IA(Information Assurance) 컨설턴트를 제공하며 이 서비스에서 위협, 취약성 및 보안 수칙의 유효성은 최신의 평가로 일관되게 제공되고 있다. 영국 정부 IT 시스템의 위협 및 취약성이 증가함에 따라 이와 같은 컨설턴트의 필요성이 증가하게 되었다.
- 서비스 지침서는 정책, 암호, 네트워크 보안 등 일반적인 IA의 모든 범위를 포함하는 프로젝트에 제공된다.
- CLAS 회원 신청은 필요한 자격과 IA 경험을 갖춰야 한다. 지원자는 다음 기준을 승인 받아야 한다.
  - 전문가 자격증, 전문 기관의 회원
  - Infosec과 적성 훈련(ITPC)에 의한 IA 경험
  - 이전 회원으로부터의 추천

○ CESG Assisted Products Service (CAPS)

- 디자인 컨설턴트는 암호 보안 기법을 사용하는 제품의 개발자 및 공급자에게 제안된다. 이러한 암호 평가 서비스는 정부 기준을 기반으로 검증을 실시하고 중앙 정부 및 공공 기관 등에 공식적인 사용을 승인한다.
- CESG에 의하여 승인된 제품은 암호 보안 등급을 선별하여 증명서를 발급하고 암호 테스트의 결과는 CC 평가로 통합될 수 있다.

○ CESG Claims Testes Mark (CCTM)

- CCT Mark는 공인된 독립적 테스트를 통하여 공공 및 민간 기관에게 정부 품질 보증 마크를 제공하고, 사업자가 주장하는 보안 기능을 검증하기 위하여 설계되었다.
- 정보 보안 제품의 보안 기능 요구에 유효성을 부여하기 위해 평가가 실행되며, CCTM 서비스는 절차에 따라 테스트 기관에 의해 착수된다. 이러한 테스트의 결과는 ISO/ IEC17025와 영국 인가 서비스에 의한 CCT Mark 요구 체계에 의거하여 인가 받는다.

○ CESG Tailored Assurance Service (CTAS)

- CTAS는 점점 더 복잡해지는 정부 IT 시스템의 보증을 취약성 확인에 더 집중된 새로운 접근 방식으로 이전 평가 계획 시 발생하는 비용보다 저비용으로 제공된다. 이러한 서비스는 취약성 탐지의 기준을 상향시키며, 간편하고 유연성을 제공하도록 설계되었다.
- CTAS의 평가는 일반적으로 4단계로 이루어진다.
  - 준비 : 보안목표명세서와 평가 작업 프로그램의 생성
  - 평가 : 제품이나 시스템의 평가
  - 보고 : 평가 보고서 생성 및 CESG로의 보고
  - 유지 : 보증 유지 계획의 실시
- 제품 보증 활동

- 기능 및 설계 평가
- 개발 과정 검사
- 보안 기능 테스트
- 소스 코드 분석
- 취약성 분석 및 테스트
- 제품 보증 유지 관리 재평가

- 시스템 보증 활동
  - 시스템 구조 및 설계 검토
  - 시스템 보안 테스트
  - 설치 및 수행 절차 검토
  - 시스템 보증 유지 관리 재평가

○ IT Health Check Service (CHECK)

- 보안 기능의 정확한 실행을 보증하고 시스템 또는 네트워크에 포함된 정보의 기밀성, 무결성, 가용성을 손상시킬 우려가 있는 취약성을 확인하는 서비스를 제공한다. 이러한 서비스는 인증된 시스템 및 네트워크의 취약성 및 공통 구성 결함에 근거를 둔 취약점이 있는지 확인하기 위한 분석으로 구성되어 있다.
- 본 서비스의 보고서는 어떠한 취약성인지 선별하고 효과적인 보안 대책을 추천하는 내용이다. 또한 HMG Infosec 표준 No.2에 의거하여 인가를 위한 최소한의 요구에 응하고 있다.

○ Common Criteria (CC)

- 국제적 상호 인증 평가인 CC는 정보 보증 요구사항에 응하는 제품에 정형적인 표준 승인을 제공한다. CC는 제품의 보안 특징에 관하여 개발자의 보안요구사항이 유효하고 인증 표준에 대한 보증을 제공한다.
- 상업적 평가 시설(CLEFs)로 알려진 독립적 테스트 기관이 평가를 수행하며 CESG에 근거한 인증기관은 영국 내에 있는 모든 CC 평가를 감독하고 인증한다. 이 평가 보고의 결과는 인증기관에 의해 제출된 인증 보고에서 확인되고 문서화된다.

○ Compliance Checking

- CESG는 HMG와 다른 공공 기관 조직에서 사용하기 위하여 상업적으로 이용 가능한 저장정보 분해 장비를 승인하며 이러한 장비는 Overwriting(오버라이팅)되거나 Degaussing(자장제거)된 제품이다.
- Overwriting 저장정보 분해 장비는 HMG Infosec 표준 No.5의 보안 지정된 정보 또는 주의해야 하는 정보의 안전 처리에서 기술된 Lower overwriting 과 Higher overwriting 기준에 따라 적합성 테스트를 받는다.
- Degaussing 장비는 IS5와 설명서 S를 통해 저 수준 또는 고 수준 설계를 승인받고 저 수준 제품 승인은 CCT Mark 계획을 통해 보증 받는다. CESG는 고 수준 요구사항이 있는 NSA Degaussing 평가 제품 목록에 있는 제품의 사용을 승인한다.

○ Tempest

- 영국에서 Tempest 인증은 CESG 공인 테스트 시설에 의해 수행된다. 이 시설로부터의 테스트 결과는 인증 표준에 의거하여 CESG에 의해 승인된다.
- Tempest는 보안 지정 데이터가 처리되는 장비나 시스템으로부터의 방사물의 방사를 연구, 측량하고 억제하는 것을 제공한다. 방사물은 모든 전기와 전자 장비가 수신기기에 전달될 때 의도하지 않는 도청을 말한다.

Ⅲ. 맞춤형 보증 서비스

3.1 서비스 배경

영국의 정보보호 제품은 ITSEC이나 CC와 같은 평가기준을 가지고 평가를 실시하고 있다. 정보보호 시스템의 경우 CC개념을 활용하면서도 보다 덜 제약적이며 빠르고, 저렴하게 제품을 평가하는 제도를 운영하고 있다. 이러한 제도는 평가기준의 EAL4 이하에 대해 평가하며 제품이나 응용시스템의 개발과정을 평가하고 있다. 이러한 서비스 중 CTAS는 특수한 IT 시스템 상에서 사용될 IT 시스템이나 IT 제품을 테스트할 필요가 있는 사업자를 위해 설계되었다[4].

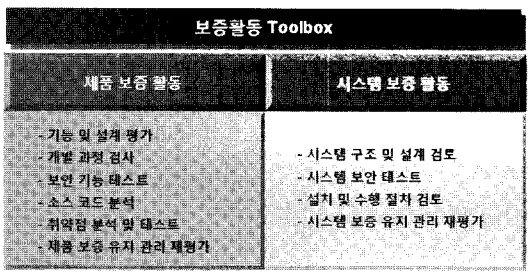
3.2 목적

영국의 CTAS 서비스는 신용제공자(Accreditor)의 필요에 맞게 조정된 유연하고 신속하며, 효율적으로 맞춰진 방법으로 CESG 승인 평가기관을 이용하기 위한 메커니

즘을 고객에게 제공하기 위해서 설계되었다. 따라서 CTAS는 기존의 평가 계획에 비해 IA(Information Assurance) 취약점을 찾는데 더 중점을 두고 있으며, 평가는 기술적 이슈와 보안 기술과 관련된 절차상에 중점을 두고 있다. 또한, 신용제공자는 리스크를 수용할 수 있는지 여부에 대해 최종적인 결정을 하고, 이를 통하여 보안의 모든 리스크를 보호하고 있다는 것을 보증하는 역할을 한다[4].

3.3 보증 활동

본 서비스는 간단한 소프트웨어 컴포넌트에서 국가 인프라 네트워크까지 여러 IT 제품과 시스템을 위해 사용되고 있으며, 이를 위하여 보증활동에 필요한 Toolbox를 생성하고 적절한 평가 서비스를 제공한다.



〔그림 1〕 보증 활동 툴박스[2]

3.3.1 제품 보증 활동

■ 기능 및 설계 평가

기능 및 설계 평가는 컴포넌트, 인터페이스, 보안 기능 및 의존 상태 등을 포함한 제품을 이해하기 위한 충분한 설계 정보를 입수할 수 있는지 여부를 분석한다. 그리고 설계의 범위를 사용 목적에 맞게 구성하여 효과적인 보안 테스트를 위해 제품을 분석하는 목적을 가지고 있다.

이러한 목적을 통하여 평가자는 제품 기능 설계를 검사하고 보안 요건에 합당한지 점검하며, 해당 제품에 보안 취약점이 존재하는지 확인하여야 한다. 또한, 제품이 보안 기능 정보 보안과 관련된 모든 구성요소와 인터페이스 등이 충분히 포함된 설계인지와 보안 요구사항을 만족하는지에 대하여 확인하여야 한다.

평가하는 동안 제품의 복잡성이 취약성을 찾기 어렵게 만들 경우, 그 한도를 규정하고 명백하거나 잠재적인 취약성에 상관없이 컴포넌트를 우회하거나 비활성화 할 수 있는 가능성도 포함하고 있는지를 확인하여야 한다.

■ 개발 과정 검사

개발 과정 검사는 보안 취약점을 통제하기 위하여 개발하는 동안에 사용된 도구와 과정의 효과에 대한 포괄적인 평가를 공식화한다는 목적을 가진다.

이를 위하여 평가를 시작하기 전에 평가자는 신용제공자와 평가 작업 프로그램(EWP)에게 이를 인정하는지 확인해야 한다. 예를 들면 개발자 사이트 방문 및 절차 적합성 감사 실시에 대한 확인을 들 수 있으며 또는 개발자가 제공한 절차문서의 표본 추출에 대한 확인일 수도 있다. 평가자는 개발자에 의해 사용되고 설계된 디자인, 적합성, 매니지먼트 구성들의 테스트를 위해서 사용된 모든 툴, 기준 및 절차 등을 확인하고, 보안 기능의 범위를 결정하여 개발자에 의해 취약한 인터페이스가 테스트 되었는지, 툴과 절차 그리고 소프트웨어 코딩 표준은 일반적인 보안 취약점들을 고려하여 사용되었는지 확인해야 한다. 만약, 이미 제품이 사용되고 있다면 최신 버전에 보고된 취약점들을 측정 결과의 증거로 제공할 수 있다.

■ 보안 기능 테스트

보안 기능 테스트는 제품에 흔히 알려진 보안 취약점들이 없는지 확인하고, 보안 기능을 테스트하는 목적을 가진다.

제품에 대하여 이미 알려진 취약점들이 존재하는지 전체적인 분석을 하며, 개발자가 발견했지만 아직 해결하지 못한 취약점이 존재하는지 알아봐야 한다. 평가자는 보안목표명세서에서 요구된 보안 기능을 테스트하여야 하며 테스트에서는 개발자의 반복적인 테스트와 평가자에 의해 만들어진 테스트 구성에 의해 실행된다. 테스트는 비슷한 보안 기능, 구성, 인터페이스로 확장되며 테스트 방법은 CESG에서 인정된 방법이어야 한다. 만약 테스트 중에 구성, 설치, 작업 등의 문제를 발견할 경우(잠재적인 보안 취약점), 평가자는 신용제공자, 개발자 그리고 CESG에 관찰 보고서를 통해 보고하여야 한다.

■ 소스 코드 분석

소스 코드 분석은 테스트 수행 시 발생할 수 있는 잠재적인 취약점 여부와 제품 구현 시 발생할 수 있는 문제점들을 유추하기 위한 목적을 가진다.

일반적인 취약점들이 존재하는 코드를 분석 할 때에는 자동화된 툴로 조사하고 위협적인 취약점들이 존재하는 것으로 보일 수 있는 것에 대해서는 수동적으로 분석을 한다. 또한, 그 외에 코드의 핵심 부분은 직접 수동적으로 확인하고 분석해야 한다. 외부 인터페이스들에 관한 수행, 중요 기능은 보안목표명세서에 포함한다. 평가자는 제품이 설계상의 취약점, 에러와 같은 문제점이 존재하는지, 잠재적인 취약성을 가지지 않게 코딩되었는지 기술하여야 한다.

■ 취약점 분석 및 테스트

취약점 분석 및 테스트는 제품에 대한 테스트 수행 시 잠재적인 취약점이 존재하는지 분석하는 목적을 가진다.

취약점 분석은 제품 설계와 소스 코드에 접근하여 분석하며, 블랙박스(시스템이나 시스템 컴포넌트 또는 프로그램 내부 구조에 대한 자세한 지식 없이 수행하는 테스트)와 같은 보증 서비스보다 빠르고 효율적으로 진행된다. 개발자들은 툴과 기술을 적용하여 테스트에서 취약점을 분석하며, 시스템 환경에서 제품에 대한 모든 위협을 고려하여야 한다.

■ 제품 보증 유지 관리 재평가

제품 보증 유지 관리 재평가에서는 제품의 지속적인 보증 유지 관리를 제공하기 위한 목적을 가지고 있다.

평가 완료 시 평가기관은 제품의 유지 관리 단계에 대하여 언급한다. 제품이 유지 관리 단계로 진행 되는 경우 그와 관련한 이유를 평가 보고서에 기록한다. 평가기관은 보증 유지 관리 계획(AMP) 템플릿을 사용하여 그 내용을 신용제공자, 개발자, CESG와 논의하여야 한다.

3.3.2 시스템 보증 활동

■ 시스템 구조 및 설계 검토

시스템 구조 및 설계 검토는 컴포넌트, 인터페이스, 보안 기능 및 의존 상태 등을 포함한 제품을 이해하기 위해 필요한 설계 정보를 입수 할 수 있는지를 확인하고, 설계의 범위를 사용 목적에 맞게 구성하는 목적을 가지고 있다.

평가자는 제품 기능 설계를 검사하고 보안 조건에 합당한지 분석하며, 보안 취약점들이 제품 내에 존재하는지를 확인한다.

또한, 제품이 다음과 같은 설계가 되도록 컨설턴트 한다.

- 보안 기능 정보와 모든 구성요소 및 인터페이스 등을 충분히 확인하고 설계에 포함
- 모든 보안 요구사항을 만족하는지 검토
- 보안 강도 또는 자체 보안의 유효성
- 평가하는 동안 제품의 복잡성이 취약성을 찾기 어렵게 만들 수 있는 경우에 그 한도 규정
- 명백하거나 잠재적인 취약성에 상관없이 컴포넌트를 우회하거나 비활성화 할 수 있는 가능을 포함하고 있는지 확인

■ 시스템 보안 테스트

시스템 보안 테스트에서는 제품에 흔히 알려진 보안 취약점이 존재하는지 확인하고, 요구된 보안 기능을 테스트하는 목적을 가진다.

보안목표명세서에서 요구된 보안 기능이 반드시 포함되어야 하며 테스트에서 개발자의 반복적인 테스트와 평가자에 의해 만들어진 테스트의 구성에 의해 실행되어야 한다. 테스트는 비슷한 보안 기능, 구성, 인터페이스로 확장되며 테스트 방법은 CESG에서 인정된 방법이어야 한다. 만약 테스트 중에 구성, 설치, 작업 등의 문제를 발견할 경우(잠재적인 보안 취약점) 평가자는 신용제공자, 개발자 그리고 CESG에 관찰 보고서를 통해 보고해야 한다.

보안 기능을 테스트함에 있어 평가자는 제품이나 시스템의 설계를 이해해야 하며, 비슷한 제품이나 시스템상에서 취약점에 대한 모든 지식을 활용하여 테스트를 진행해야 한다. 이러한 테스트들은 IT 보안 자체 검사에서 반복적으로 이루어진다.

■ 설치 및 조작 절차 검토

설치 및 조작 절차 검토에서는 문서화된 절차가 시스

템에서 가장 적합한 실행인지 확인하고, 실제 문서화된 절차를 실행 할 것인지 결정하는 목적을 가진다.

IT 보안 자체 검사는 평가 작업 프로그램에서 상세하게 제공되며 신용제공자의 요구를 중점으로 이루어지게 된다. 일반적으로 제품의 전달, 설치, 관리, 사용자 안내, 구성 통제, 기록 검사 등의 보완을 제공하며, 해당 범위 내에 백업의 절차와 장애 복구 계획이 포함되어 있다. 평가자는 일반적으로 가장 적합한 실행을 위한 문서화된 절차를 검토해야 하며, 시스템 감사에 의해 절차를 결정하고 있는지 확인 할 수 있다.

■ 시스템 보증 유지 관리 재평가

시스템 보증 유지 관리 재평가는 제품의 지속적인 보증 유지 관리를 제공하는 목적을 가지고 있다. 보증 유지 관리 계획에서는 제품 업데이트가 어떻게 평가되는지 제공한다.

주기적인 검토는 일반적으로 다음 내용을 포함하고 있다.

- 이전 검토에서 권고 사항 이상의 평가
- 이전 평가 또는 검토에서부터 확인한 새로운 취약점을 위한 검사
- 개정 역사 및 그 결과의 검토
- 보안 영향 분석에서 시스템 변화의 검토
- 관련 개발자 테스트의 검토
- 개발자의 테스트가 부적절할 경우, 구체적인 보안 기능 업데이트 테스트
- 신용제공자의 요구가 있을 경우, 운영 절차의 어플리케이션 감사
- 시스템 운영자와 관리자에 의해 사전 보고서 검토

보안 기능, 컴포넌트 및 인터페이스에서 중요한 변화가 있거나 추가할 사항이 있을 시에는 적절한 보증을 하기 위해서 재평가가 필요하다. 그리고 권고 사항은 유지 관리 보고서에 포함해야 한다.

3.4 평가 프로세스

평가는 일반적으로 4단계를 가지고 있다[3].

- 준비 : 보안목표명세서와 평가 작업 프로그램의 생성
- 평가 : IT 제품 또는 시스템의 평가
- 보고 : 평가 보고서와 CESG평가 보고서의 생성
- 유지보수 : 보증 유지보수 계획의 실행

■ 준비 단계

이 단계에서는 평가기관의 서브컨트랙터(Sub-Contractor), SSA, 개발자, CESG로부터 시작된다. CESG는 보안목표명세서와 평가 작업 프로그램에 정보를 제공하기 위해서 고객, 신용제공자 및 개발자와 함께 작업한다.

스폰서와 평가 업체 사이에서 다른 부분의 동의가 없으면, 스폰서는 신용제공자와 CESG에 의해 승인된 정보를 통하여 보안목표명세서를 작성한다. IT 시스템 또는 제품에서 운영되고 있는 고객의 IT 보안 요구사항과 환경에 정당한 평가가 이루어진다.

보안목표명세서는 IT 제품 또는 시스템의 보안 아키텍처를 설명하고, 이를 명확하게 전달하며 제품 또는 시스템을 상세히 기술한다. 평가 작업 프로그램의 목적을 위하여 정확한 유효범위를 포함하며, 이것은 위협, 가정, 중요 보안 기능을 기술하여야 한다. 활용 가능한 자원을 효과적으로 이용하기 위해서는 보안 목표는 주요 취약점에 대응하는 기능 및 인터페이스에 우선순위를 부여해야 한다.

평가 작업 프로그램은 평가 업체, CESG, 신용제공자, 고객 및 개발자에 의해 개발된다. 신용제공자는 평가 작업 프로그램의 콘텐츠를 승인하고, 활동 및 유지보수를 책임진다. 초기 버전은 평가 작업 프로그램을 최종적으로 완료할 평가 업체를 위하여 스폰서 또는 컨설턴트 제공자에 의해서 준비된다. 최종 버전은 일반적으로 보안명세서에 평가의 범위와 보증 요구사항이 정의된 후에 개발된다.

평가의 시작에 앞서, 스폰서는 CESG와 상담을 하고 신용제공자는 평가 업체와 평가 작업 프로그램에 대한 의견을 협의한다. 개발자가 IT 보안에 물질적으로 영향을 주는 시스템 설계에 변화를 주거나 시스템의 위협이 바뀌게 되면 평가 작업 프로그램을 변경하여야 한다.

평가 업체의 평가 작업 프로그램의 정의 단계에서의 결과물은 CESG, 신용제공자 및 스폰서와 공유해야 한다. 결과물이 보안목표명세서의 요구사항과 일치하지 않으면 평가자는 이를 CESG, 신용제공자 및 스폰서에게 통지한다. 평가자는 이 일에 관련된 이들에게 조언을

구하고, 변경 통제 절차를 통해서 정식으로 변경 계획을 신청한다.

평가 작업 프로그램은 중요 위협과 목적 및 보안목표 명세서의 중요 보안 기능과 인터페이스를 증명하는 것 뿐 아니라 다음 사항에 대해서도 증명한다.

- 낮은 우선순위를 포함하는 모든 보증 활동을 증명
- 평가 작업 프로그램에서의 여러 활동의 중요성을 증명

준비 단계를 완성하기 위해서, 보안목표명세서와 평가 작업 프로그램이 관련된 모든 것을 승인할 필요가 있으며, 평가자는 평가 작업 프로그램 내에 정의된 프로그램을 완성해야 한다. 추후에 평가 작업 프로그램이 업데이트 되려면 신용제공자와 CESG의 동의를 얻어야만 한다.

■ 평가 단계

○ 평가자의 역할

평가는 보안목표명세서와 평가 작업 프로그램에 근거하고 있으며, CTAS 방법론의 보증활동과 관련해 적절한 조치를 취하는 것이다. 평가자는 개발자와 일하면서 평가기간 동안에 추가적인 문제점을 찾고 수정을 제안할 수도 있다. 중요한 문제점들은 신용제공자, 스폰서 및 CESG에 위협 감시 보고서를 통해 보고되어야 하며 발생 가능한 문제의 해결 및 부수비용을 위한 권고 사항을 확인해야 한다.

○ CESG 역할

평가를 통해서 CESG는 평가 업체와 신용제공자에게 기술 지침서와 감사를 제공하기 위한 준비 상태에 놓여질 수 있다. 예를 들어, CESG가 침입 테스트에 관한 계획을 검토할 필요가 있고 그 결과를 통해 IT 제품 또는 시스템의 설계를 평가자가 상세히 이해하게 된다면, CESG와 평가 업체와의 계약에 이러한 활동을 포함시키게 된다.

○ 개발자 역할

평가 진행 동안, 평가 업체와 스폰서 간의 맞춤형 평가 작업 프로그램 계약을 통하여 다음 사항에 대하여 제공하게 된다.

- 설계와 실행을 이해하기 위한 컨설턴트
- 기능 설계와 설계 문서
- 소스 코드 접근
- 제품 및 시스템의 설정
- 테스트 기술 지원
- 개발 절차 감사를 위한 개발 환경 접근
- 잘 알려진 취약점 정보
- 설치 및 수행 절차와 증거

○ 고객과 신용제공자 역할

고객과 신용제공자는 평가 절차 도중 다음과 같은 활동 역할이 요구된다.

- 보안목표명세서와 평가 작업 프로그램의 일치
- 완성 날짜 또는 보증 목표 달성에 영향을 줄 수 있는 문제
- 검토될 필요가 있는 우선 사항
- 수행 환경에서의 테스트

■ 보고 단계

보고 단계에서는 일목요연하게 보고서를 요약하고, 보안 취약점 또는 주요 기능 오류의 리스트를 통해 추가적인 잔여 위협 및 업무 영향도를 기술하여야 한다. 또한, 시스템 환경에 있어서 관련성을 밝히고 있으며 세부적인 시스템 구성을 통해 제품에 대한 위협이 일반적인지 아닌지에 대해 검증한다. 이러한 보고서의 내용은 보증활동을 통하여 결론을 이끌어내며, 식별된 취약점의 완화를 위한 권고사항을 기술한다. 상세한 평가와 테스트 기록은 앞으로의 보증 유지보수 작업을 지원하며, 유지보수 지원을 제공하는 평가가 요구되어 질 때, 재사용될 수 있다.

평가 업체는 스폰서, 신용제공자 및 CESG에 평가 보고서의 사본을 제공해야 한다.

평가 보고서의 최종 초안의 수취에 있어서 CESG는 평가 검토를 평가 보고서에 포함시킬 수 있는 신용제공자와 고객에게 배부한다. 보고서에는 보안상의 위협 및 업무 영향도를 기술하고, 주요 결과물이 어떠한 범위에서 평가되었는지에 대해 입증하고 요약한다. 본 과정을 거치고 나면 맞춤형 보증 평가가 완료된다.

■ 유지보수 단계

각 기관에서 사용되고 있는 제품은 수정 및 패치가 이루어지고 시스템은 업데이트와 계속적인 재설정을 거치게 된다. 또한, 이전에 알려지지 않았던 취약점이 드러날 수도 있으며, 시간이 지남에 따라 설정에서 에러가 발생할 수도 있다. 따라서 대부분의 평가된 IT 제품과 시스템을 이용하는 동안 보증 유지보수를 받아야 한다.

제품 또는 시스템이 계속되는 보증을 유지하기 위한 방법으로 보증 유지보수 계획(AMP : Assurance Maintenance Plan)이 있다. 이 계획은 위협에 의해 IT 시스템 및 제품이 변경되거나 자체 내에서 변경되는 것을 고려하여 CESG에 의해 정기적으로 검토 받을 필요가 있다.

유지보수는 일반적으로 평가 완료 6~12개월 후에 변경에 대한 감사의 수행과 IT Health Check을 포함하여 진행한다. 또한 보안 영향력을 분석하기 위해서 1년 동안 주요 업데이트를 검토한다.

보안 기능, 인터페이스 및 컴포넌트의 중요 변경 및 추가의 경우에는 보증을 위한 재평가가 필요하다. 만약 재평가를 위한 요건이 신용제공자와 고객의 동의를 얻게 되면, 변경을 신청하게 되고 이전의 유지보수 또는 평가 결과를 재활용하게 된다.

Ⅳ. 국내 평가 서비스 향후 발전방향

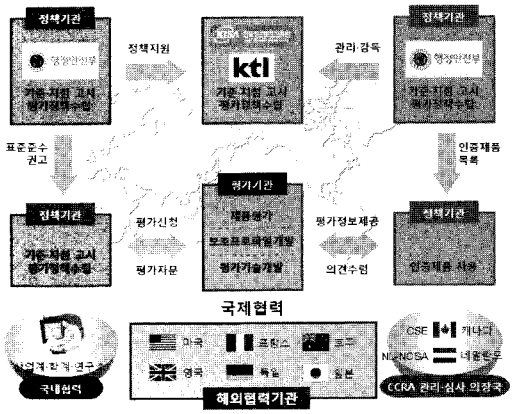
4.1 국내 평가 서비스 현황

국내 평가 서비스의 현황을 보면 아직까지 많은 서비스가 제공되거나 연구가 진행되고 있지 않다. 현재 서비스가 제공되고 있는 국내 평가 서비스 현황을 보면 다음과 같다[5][6].

- 정보보호시스템 평가·인증 제도
- 보안적합성검증제도
- 암호검증제도

■ 정보보호시스템 평가·인증 제도

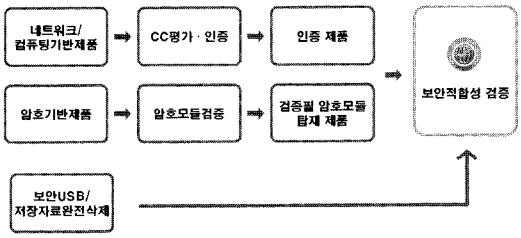
국내의 정보보호시스템 평가·인증 제도는 정보보호 제품의 보안기능을 검증하여 국가 정보보호 수준을 제고하고 정보보호제품의 객관적이고 공정한 평가·인증을 실시하여 제품의 경쟁력을 강화하는데 목적을 두고 있다.



〔그림 2〕 국내평가체계도

■ 보안적합성검증제도

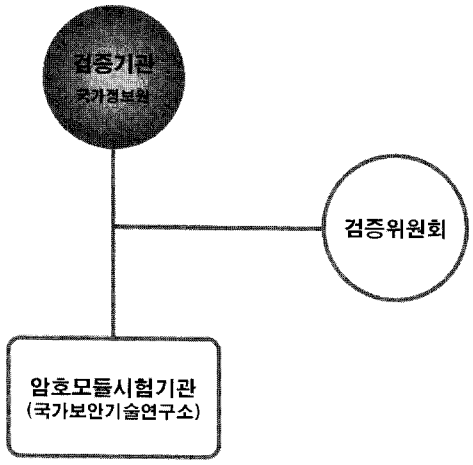
보안적합성검증제도는 전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률 등 관계법규에 의거하여 공공기관에 도입하는 정보보호제품의 보안적합성과 안전성을 사전 검증함으로써 국가정보통신망의 보안수준을 제고하기 위해 시행하는 제도이다.



〔그림 3〕 보안적합성검증 체계

■ 암호검증제도

암호검증제도는 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보보호의 보호를 위해 사용하는 암호제품에 대해 안전성과 구현 적합성을 검증하는 제도이다.



〔그림 4〕 암호검증체계

4.2 평가 서비스 비교

국내의 평가서비스 중 영국의 맞춤형 보증 서비스 제도와 흡사한 제도는 현재 존재하지 않는다. 따라서 이와 동일한 수준에서의 비교는 불가능 하지만 이를 통하여 국내 평가서비스의 현황을 분석할 수 있다.

다음 표는 국내의 평가서비스와 영국의 평가 서비스의 제품 평가 절차에 따른 비교 분석을 나타낸 것이다.

〔표 2〕 국내 평가서비스와 영국 CTAS 제도 비교 분석

	국내 CC 인증	보안적합성검증제도
평가 신청	사용자에 의한 신청	사용자에 의한 신청
적용 범위	암호모듈을 제한 모든 IT 제품	CC인증 제품과 암호검증필 제품
평가 기준	공통평가기준, CEM	보안적합성시험기준 (국보연)
보증 등급	EAL1~EAL7	-
관리 범위	완료된 제품의 검증	완료된 제품의 검증
평가 실시	모든 공통평가기준 문서의 작성 완료 후 평가 실시	- 네트워크/컴퓨팅기반 제품 - 암호기반 제품 - 보안USB/저장자료완전삭제
평가 실시 시기	제품 설계 완료 후	제품 설계 완료 후
관련기관	신청기관, 평가기관, 인증기관, 인정기관, 인증서보유기관, 공인시험기관	국가보안기술연구소, 국가정보원, 각급기관

	암호검증제도	영국 CTAS 제도
평가 신청	사용자에 의한 신청	사용자에 의한 신청
적용 범위	암호 모듈 및 알고리즘	암호모듈을 제한 모든 IT 제품 및 시스템
평가 기준	FIPS 140-1, 140-2	보증활동 툴박스
보증 등급	-	- 제품 등급 : EAL2/EAL3 정도의 수준 - 시스템 등급 : 없음
관리 범위	완료된 제품의 검증	완료된 제품의 검증 및 추후 유지보수
평가 실시	- 소프트웨어, 하드웨어 펌웨어 암호 모듈 및 알고리즘	- 준비 - 평가 - 보고 - 유지보수
평가 실시 시기	제품 설계 완료 후	제품 설계 완료 후
관련기관	검증 신청인, 검증기관, 검증위원회, 암호모듈시험기관	신청인, 정보제공자, 개발기관, 평가기관, CESG-IACS

4.3 향후 발전방향

국내 평가서비스는 영국의 맞춤형 보증 서비스를 포함한 IACS제도와 같이 다양한 평가 서비스를 제공하고 있지 못하다. 그리고 평가 서비스와 관련한 학술적, 기술적 연구 또한 그 분야가 다양하지 못하고 연구 결과물도 아직은 그리 많지 않다.

따라서 국내에서의 연구의 질적 향상과 연구 분야의 다양성을 위하여 선진 국외 평가서비스에 대한 선행 연구가 필요할 것으로 분석된다. 이러한 국외 평가서비스의 분석을 통하여 국내 환경에 적합한 서비스의 도출과 그에 따른 관련 기술의 연구 및 테스트가 활발하게 이루어져야 국내 평가 서비스가 보다 효율적이고 질적인 향상을 꾀할 수 있을 것이다.

앞서 분석한 영국의 맞춤형 보증 서비스의 절차 및 검증 범위를 보면 단순한 제품의 유효성 검증뿐만 아니라 제품의 추후 운영 단계에서의 유지보수까지의 서비스를 제공하고 있다. 이를 통하여 제품의 업데이트 및 변경에 따른 보안성 유효성을 검증하고 제품의 안전성 및 효율성에 대한 보증을 유지하게 된다. 이러한 지속적인 제품 및 시스템에 대한 보증을 통해 사용자의 신뢰를 지속적으로 유지해 나갈 수 있다.

국내의 평가를 보면 제품에 대한 안전성 및 효율성에

대한 평가를 통해 제품을 보증하지만, 이는 단순한 제품의 초기 단계의 검증을 이루고 있다. 제품의 추후 관리 및 운영환경에서의 검증을 통한 보증을 제공하고 있지는 못하다. 따라서 국내에서 제공하는 기존의 서비스에 추후 관리 서비스 및 운영환경에 따른 맞춤형 서비스를 제공하거나, 신규 서비스를 통한 평가 보증 서비스에 이와 관련한 절차적인 부분을 명시한다면 보다 효율적인 서비스를 제공 할 수 있을 것으로 기대된다.

V. 결 론

현재 정보화가 진행됨에 따라 다양한 IT 제품 및 서비스에 대한 평가 보증에 대한 기대가 증가하고 있다. 이에 맞추어 다양한 평가 보증 서비스가 요구되고 있으며, 이를 위한 연구가 진행되고 있다. 다양하고 많은 연구가 진행되기 위해서는 이를 위한 선진 국외 평가서비스에 대한 선행연구가 필요할 것으로 생각된다. 본 연구를 통하여 국내 환경에 적합한 평가서비스의 개발과 연구가 활발히 진행될 수 있을 것으로 기대된다.

이에 본 고에서는 영국의 맞춤형 보증 서비스의 평가 프로세스를 분석하여 국내 보안성 평가 제도가 나아가야할 방향을 제시해 보았다. 본 고에서 분석한 평가서비스를 통하여 국외 평가 보증 서비스의 분석을 위한 기본 틀과 국내 평가 서비스 개발 및 연구를 위한 초석으로 활용할 수 있을 것으로 기대된다. 또한 이를 통하여 국내에 추후 유지보수를 포함한 보증 서비스의 개발 및 발전을 기대해 본다.

참고문헌

[1] CESG, "IACS Information Assurance & Consultancy Services", 2007.

[2] CESG, "CESG Tailored Assurance Service Methodology Version 2.1", June 2007.

[3] CESG, "CESG Tailored Assurance Service Operating Procedure for Evaluations Version 1.0", June 2007.

[4] http://www.cesg.gov.uk/products_services/iacs/ctas/index.shtml.

[5] 한국정보보호진흥원, "평가·인증 가이드", 2006.

[6] 국가정보원 IT보안인증사무국, "정보보호제품 평가인증 수행규정", 2008.

〈著者紹介〉

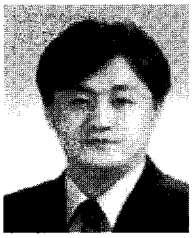
고 웅 (Woong Go)

학생회원

2008년 2월: 순천향대학교 정보보호학과 학사

2008년 3월~현재: 순천향대학교 정보보호학과 석사과정

<관심분야> 정보보호, 보안성 평가, 개인정보보호, 유비쿼터스 어플리케이션 보안 등



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