通信情報保護學會誌
第5卷 第1號, 1995. 3

외국의 정보보호 체계 분석(Ⅱ)

A Study on the Foreign Information Security Evaluation and Certification Scheme(Ⅱ)

강 창 구*, 윤 이 중**, 김 대 호*, 이 대 기***

요 약

본 논문에서는 국내 정보보호 체계를 수립하기 위하여 외국에서의 정보보호 체계분석의 일환으로 영국의 정보보호 시스템 평가승인 체계에 대하여 분석하였다. 먼저 영국에서의 정보기관 구조를 소개하고, 정보보호 체계와 관련한 조직의 구성 및 임무에 대하여 기술하였다. 또한 영국의 정보보호 시스템 평가승인 절차를 분석하였으며 영국의 암호 알고리즘과 평가 기준서인 ITSEC에 대해 분석하였다.

1. 개 요

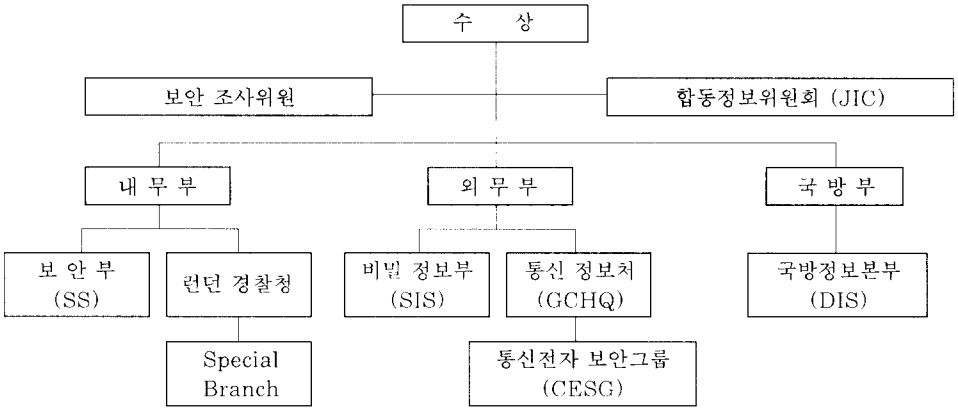
컴퓨터와 통신기술의 발전으로 정보화 사회가 도래함에 따라 정보와 통신의 결합, 정보 자원의 공유, 정보 서비스의 다양화로 인하여 정보 이용이 생활화되고 정보는 중요한 자산이 되고있다. 이러한 중요 정보를 이용하는 정보 이용자는 정보의 불법 도난, 교란, 훼손, 악용등의 위협으로부터 정보를 보호하기 위한 대책 수립이 요구된다. 이에 따라 영국 정부에서는 정보화 사회의 역기능을 방지하고 정보처리 업무를 보다 효율적으로 수행하며 또한 민간 부문으로부터의 정보보호 시스템에 대한 수요증가에 부응하기 위하여 1989년 12월에 IT(Information Technology)제품 및 시스템의 보안기능을 평가 승인하는 새로운 제도를 수립할 것을 상공부(DTI : Department of Trade and Industry)와 통신전자 보안그룹(CESG : Communications Electronics Security Group)에 지시하였다.

DTI와 CESG는 UK IT Security Evaluation and Certification Scheme(이하 "본 제도"라 한다)을 1991년 3월에 완성하여 공표하였으며 정보보호 시스템에 대한 평가승인에 적용하고 있다[1].

본 제도의 목적은 첫째 정부와 민간 부문에 사용될 정보보호 시스템에 대한 평가승인 체계를 확립하고, 둘째 유럽의 보안평가 기준서인 ITSEC (Information Technology Security Evaluation Criteria)[2]에 근거하여 평가를 수행함으로써 평가승인 결과에 대하여 국제적 상호 인증의 기반을 제공함에 있다[4, 7]. 특히 본 제도는 국가의 비밀정보를 저장, 가공, 처리하는데 있어서 사용되는 모든 정보보호 시스템에도 적용된다.

* ETRI 책임 연구원
** ETRI 선임 연구원
*** ETRI 책임 기술원, 한국통신정보보호학회 산학이사

2. 정보 기관 구조



JIC : Joint Intelligence Committee
SS : Security Service
SIS : Security Intelligence Service
GCHQ : Government Communications HeadQuarters
DIS : Defence Intelligence Staff

※ 참 고
〈 20 C 초 육군성내 〉
- MI 5(방첩, 안전 기능) → 1924년 내무부산하 보안부(SS)로 변경
  영국 본토의 방첩, 보안 활동
- MI 6(첩보 수집, 대외 공작 기능) → 1911년 외무부 산하 비밀 정보부(SIS)로 변경
  세계 각국 정보 수집
- MI 8(통신정보수집) → ?년 외무부 산하 통신정보처(GCHQ)로 변경
  세계 각국 통신 정보 수집

그림 1. 정보기관 구성도

본 논문에서는 국내 정보보호 체계를 수립하기 위한 기반 연구로서 영국에서의 정보기관 구조, 정보보호 체계 관련 조직, 평가승인 절차 및 평가 기준서에 대하여 분석하였다.

3. 평가 승인 관련 조직

3.1 통신전자 보안 그룹(CESG)

- 영국의 정보보호 분야의 기술적인 공식 기관
- 1985년 2개의 평가 기관(Evaluation Facilities : EF)을 설립하여 시스템 평가를 수행하게 함.
- 추가로 2개의 기관이 더 설립됨. 이 기관은 HMG 프로젝트만을 전담하여 평가하는 CAEF(CESG Approved Evaluation Facilities)다.
- 한편, 시스템을 구축해 가는 과정에서 보안 제품들이 평가 승인되어야 한다면 평가 작업에 드는 비용을 절감시키기 위하여 1987년 제품평가를 상용을 기반으로 일반 산업체가 평가 기관으로 인가받아 운영하도록 결정
- 1989년에는 두개의 회사가 Commercial Licensed Evaluation Facilities(CLEF)로 인가받았으며 일반 보안 제품 평가는 물론 HMG 시스템 평가의 대부분을 수행케 할 계획을 갖고 있었다[3].

- 암호 알고리즘 개발 및 암호 칩 개발 공급
- 알고리즘의 비도 평가

3.2 상공부(DTI)

- 영국의 상업, 산업 전반에 관련하는 기관
- 1987년 Commercial Computer Security Centre를 설립하여 산업 분야의 정보보호를 기술적으로 지원하게 되었음.
- 보안 제품들의 요구 증대와 시장 개발을 위해 1989년 "GreenBooks"이라 일컬어지는 제품 평가만을 위한 평가 기준서 및 일련의 사용지침서들을 발간하였다. 이 기준서는 1989년 동안 실제 상용 제품들을 대상으로 적용되었고 산업 전반에서 많은 자문을 받았다.
- 일반용 정보보호 시스템의 평가승인 체계 유지 운영
- 보안 제품 수출 허가통제

3.3 관리 위원회(Management Board)

가. 조직 구성

CESG와 상공부의 3급 공무원 2명이 공동의장이 되고 위원들은 CESG, 상공부, 국방부, 재무부 CCTA(Central Computer and Telecommunication Agency)의 5급 혹은 6급 공무원으로 구성된다. 상공부는 기업 및 민간을 대표하고, CCTA는 금융기관을 대표하며 국방부는 국방분야, CESG는 정부기관을 대표한다.

나. 임 무

- 본 제도의 운영 정책수립 및 목표 설정
- 다음에 관한 규정을 검토하고 승인한다.
  - 승인기관의 운영
  - 제도의 전반적 운영
  - CLEF의 승인
  - 제도허가 프로그램(Scheme Licensing Programme)
- 승인기관의 재정지원
- 승인기관의 보고서 검토
- 평가승인 대상물 및 평가 재원의 지속적 확보

3.4 승인기관(Certification Body)

가. 조직 구성

승인기관은 관리위원회의 지침에 따라 CESG와 상공부 공동으로 운영하고 있으며 CESG 내에 설치되어 있는 기구이다. CESG 의장이 승인기관의 장이 되고, CESG와 상공부의 관리자들로 구성 운영된다.

나. 임 무

- 평가기관(CLEF) 인가
  평가기관은 NAMAS(National Measurement Accreditation Service)의 인가를 받아야 함[5, 6].
- CLEF의 작업 수행상태 감독
- Scheme Licensing Programme 운영
- 평가기관에 대한 기술교육 및 지원
- 제도에 의해 수행된 평가결과의 승인
- 승인제품 목록(CPL : Certified Product List) 작성 및 공표
- 제도관련 문서 출판(UKSP : UK Scheme Publication)
- 다른 나라의 승인기관과 긴밀한 협조 체제 유지 및 승인 제품의 상호 인정
- 관리위원회에 주기적 보고

3.5 평가기관(CLEF)

가. 승인된 평가기관

- Admiral Management Services Ltd (CLEF)
- EDS-SCICON UK Ltd (CLEF)
- Logica Defence and Civil Government Ltd (CLEF)
- Secure Information Systems Ltd (CLEF)

나. 임 무

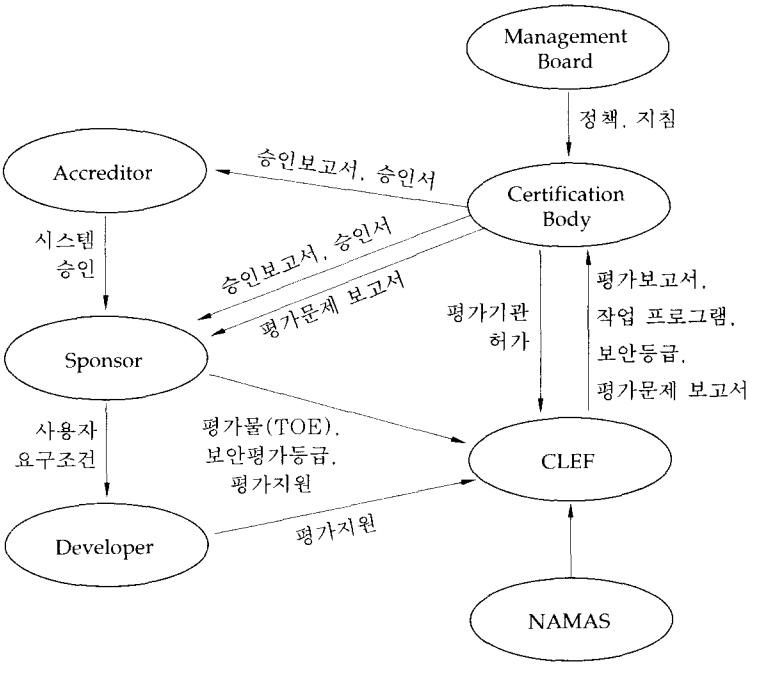
- 정보보호 시스템 평가 및 평가 결과 작성
- 평가 시스템의 승인 의뢰(승인기관)
- 평가 내용에 대한 보안유지 및 지적 재산권 보호
- 모든 수행 업무 내용을 승인기관에 보고
- 시스템 개발업체에 대한 기술 자문

3.6 기타 관련 조직

- 평가의 스폰서 : 스폰서는 평가를 의뢰한 조직으로서 제품의 개발자일 수도 있고 시스템 사용자일 수도 있다. 실제 평가를 위해 요구되는 품목들을 공급할 능력에 한계가 있다하더라도 스폰서가 되는 것에는 아무런 제약조건이 없다.
- 평가 대상물의 개발자 : 후원자와는 별도로 개발자가 분리되어 있을 수 있다.

4. 평가 승인 절차

4.1 평가 승인 체계



NAMAS : National Measurement Accreditation Service

그림 2. 평가승인 체계도

4.2 사전 평가 협의 단계

그림 3은 정보보호 시스템 사전평가 협의 절차도를 나타낸다. 그림에서 스폰서는 security traget을 준비하여야 하는데 이때 아래와 같은 내용이 포함되어야 한다.

- 시스템 보안 정책(System Security Policy) : 시스템에 대한 보안 목적, 위협요소, 대책 및 제품의 보안 특징, 사용방법, 사용환경이 기술되어 져야 한다.
- 보안 기능에 대한 보안 매카니즘
- 매카니즘의 최소 강도(비도)
- 평가 목표 등급(E1 ~ E6)
- 보안 기능 규격
- 기타 필요한 자료 첨부

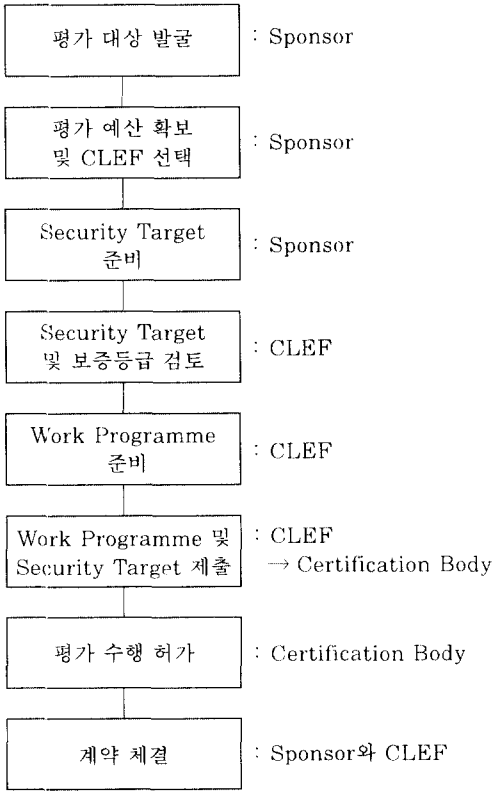


그림 3. 정보보호 시스템 사전평가 협의 절차도

또한 CLEF가 준비하는 work programme에는 ITSEC과 본 제도를 만족하기 위해서 평가해야 할 작업목록을 정의하고 있다.

4.3 공식 평가(Formal Evaluation)단계

스폰서는 평가하는데 필요한 모든 자료 및 개발품목을 평가기관에 제출하고 평가하는데 요구되는 기술을 지원한다. 평가기관은 평가 중 발생한 모든 문제점을 승인기관에 보고하여야 하며, 승인기관은 스폰서/개발자와 이 문제를 논의하고 해결책을 찾는다. 평가기관은 평가 시스템 혹은 제품에 대해서 비밀성, 무결성, 가용성을 평가한다.

4.4 승인(Certification)단계

승인기관은 평가기관으로부터 평가보고서를 검토하고 평가물이 보안 목표를 만족하는지를 결정한다. 여기서는 평가기관이 수행하지 못한 사항 즉, 알고리즘의 비도등을 평가하며 또한 최종 평가 등급을 결정하게 된다. 이때 스폰서는 승인기관에게 승인 비용을 지불하여야 한다.

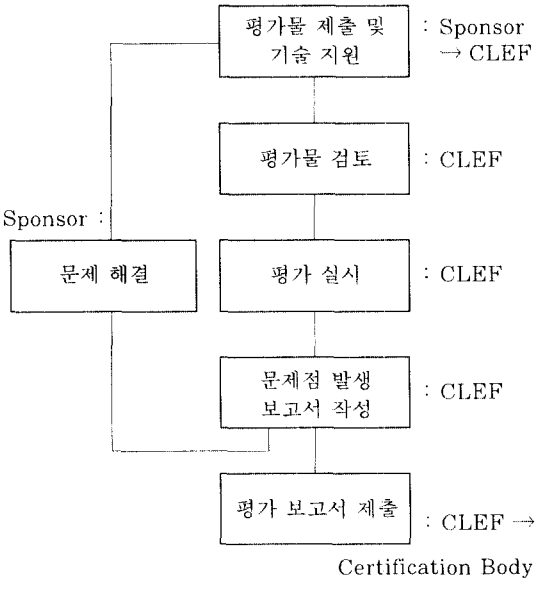


그림 4. 정보보호 시스템 공식 평가 절차도

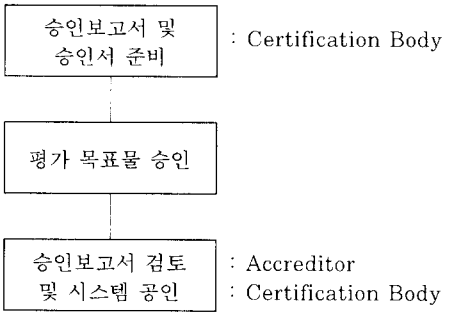


그림 5. 정보보호 시스템 승인 절차도

5. 스폰서의 임무

평가절차에 관련하여 스폰서가 해야할 일은 단계별로 다음과 같다.

5.1 평가 전단계

- 평가 목표물과 기타 평가제출물에 대한 법적 권리 설정, 평가기관 및 승인기관의 법적 보증 확보
- 요구 보안 등급 결정
- 평가기관과의 계약서 상에 다음 사항을 명시
  - 모든 평가 결과는 승인기관으로 보내져야 한다.
  - 평가기관은 승인기관의 요구에 적극 호응하여야 한다.
- 개발자와 개발기간 중 발생한 지적 재산권의 소유 제한 내용이 포함된 동의서를 작성하여야 한다.
- 평가결과에 대한 개발자의 권리 포기각서

5.2 평가 단계

- 평가기간 중 평가 대상물에 대한 모든 변경사항을 평가기관에 통보하여야 한다.
- 평가 대상물 개발에 사용된 컴퓨터를 액세스할 수 있게 허가한다.
- 평가자에 대한 각종 지원(훈련, 토의, 컴퓨터 제공, 사무실 제공 등)
- 평가기관으로 부터의 질의에 응답
- 평가기관에 평가 제출물의 적기 제공
  - 평가 대상물(소스 코드, 기능 규격, 설계 규격 및 구현 내용 포함)
  - 보안 목표 등급
  - 구성도
  - 보안성 증빙 자료 및 시험 결과서
  - 평가 대상물 개발과정에서 사용된 절차, 방법, 사용도구, 표준 등에 관련된 문서
  - 평가 대상물 사용 설명서

5.3 평가후 단계

- 평가 보고서의 비밀 유지
- 승인 보고서의 결정 수락
- 승인 비용 지불
- 승인 제품의 판매
- 비인가적 변조를 위한 형상관리

6. 평가 기준

6.1 평가 기준서

영국, 프랑스, 독일, 네덜란드는 각국의 보안성 표준을 조화롭게 통합조정하여 IT 시스템에 대한 국제보안 평가기준 설정에 주도적 역할 수행을 겨냥한 유럽의 보안 평가 기준서인 ITSEC(Information Technology Security Criteria)를 1991년에 발표하였다[1]. 따라서 영국에서는 ITSEC이 정보보호 시스템에 대한 평가 기준서이다. 이 ITSEC은 유럽 4개국의 공통된 보안기준과 보안 평가 과정에 대한 내용과 IT 시스템의 보안기능을 표현하는 방법으로 구성되어 있다. 평가등급은 7개 등급으로 구분하였으며 등급별로 여러

가지 정확한 요구사항을 제시하고 있으며, 각 등급에 적용될 수 있는 유효성 기준(effectiveness criteria)도 제시하고 있다.

ITSEC에서 IT Security는 다음과 같이 정의한다.

- 비밀성(Confidentiality) : 정보의 비허가된 노출의 방지
- 무결성(Integrity) : 정보의 비허가된 변조의 방지
- 가용성(Availability) : 정보나 자원들의 정상적인 사용을 불법적으로 방해하는 행위 금지

ITSEC에 대한 각 국들의 노력은 다음 사항을 목표로 하고 있다.

- 유럽 국가간 무역 장벽을 피하기 위한 공통 지침서
- 보안 평가 기준에 대한 기본적인 표준안과 시험에 관한 지침서
- 재평가 또는 새로운 버전에 대한 평가과정의 신뢰성 문제를 해결할 수 있는 지침서
- 새로운 보안 제품 또는 개선된 제품들 사이의 충돌을 최소화하고, 기대효과를 최대화할 수 있는 지침서
- 다국적 개발과 이질 시스템인 경우 평가과정에서의 중복된 노력을 최소화하는 지침서

이 ITSEC에 포함되어 있는 보안요소로는 비밀성, 무결성, 가용성을 모두 포함하고 있기 때문에 정보는 접근권한을 가진 사용자에게만 노출되며 수정할 수 있는 권한을 가진 사람만이 수정할 수 있고, 정보와 다른 기술적 자원을 적법한 사용자가 필요시에는 항상 접근할 수 있다. 이와같은 ITSEC은 보안기능(functionality), 보증(assurance) 기준에 따라 보안요구 사항을 분석하고, 평가등급을 제시하고 있다.

6.2 보안 기능(Fuctionality)

보안 평가의 목적은 평가시스템에 대해서 보안에 대한 보증 등급을 부여하는 것이다. 이 목적으로 달성하기 위해 평가자는 시스템이 보안 측면에 기여하는 기능을 정확하게 구분하고 정의할 수 있어야 한다. ITSEC에서는 보안 기능에 대하여 다음 3가지 추상화 수준을 제시하고 있다.

- 보안 목표 : 가장 추상화된 수준으로 시스템이 달성하려고 하는 보안에 대한 기여로서 왜 보안기능이 요구되는가를 정의한다.
- 보안 기능 : 보안에 기여하는 제품이나 서비스의 특성으로 실제 무엇이 수행되는가를 나타낸다.
- 보안 매카니즘 : 보안 기능을 구현한 논리 및 알고리즘으로 보안기능이 어떻게 수행되는지를 나타낸다.

또한 이 기준서는 보안기준의 가장 중요한 부분을 이루고 있는 보안 기능을 제시하고 있는데 보안기능은 다음과 같은 8개의 기본적인 기능으로 나누어진다.

1) 식별(Identification)과 인증(Authentication)

요구된 사용자의 신원을 식별하고 인증한다.

2) 접근 제어(Access Control)

사용자나 프로세서에 의한 객체에 대한 사용을 제어하고, 사용자나 프로세스간의 정보흐름을 제어하며, 접근 권한을 관리하고 검증한다.

3) 기록성(Accountability)

보안에 관련된 행위를 수행할 수 있는 권한의 변화를 기록한다.

4) 감사(Audit)

보안에 대한 위협이 될 수 있는 모든 사건을 추적하고 조사한다.

5) 객체 재사용(Object Reuse)

데이타 객체의 재사용을 제어한다.

6) 정확성(Accuracy)

보안에 관련된 정보의 정확성과 일치성을 보장한다.

7) 서비스의 신뢰성(Reliability)

보안 서비스의 가용성과 신뢰성을 보장한다.

8) 데이타 교환(Data Exchange)

통신 채널을 통한 전송중의 데이타 보안을 보장한다.

이러한 보안 기능에 근거를 두고 평가 등급을 F1 ~ F10의 10개 등급으로 분류하였으며 F1 ~ F5까지의 5개 등급은 미국의 TCSEC으로부터 유도되어 그 기능들을 포함하고 있고, F6 ~ F10까지의 5개 등급은 시스템의 운영 체계와는 별도로 다양한 형태의 제품 또는 시스템이 상기의 8개 보안기능으로 정의될 수 있음을 나타내고 있다. 따라서 시스템의 보안기능은 미리 정의되어 있는 등급과는 상관없이 발표된 표준기능으로 부터 유도될 수 있어서 특정 시스템의 보안 기능이 또 다른 표준을 나타내는 기준서가 될 수 있다.

6.3 보증(Assurance)

보증 기준은 2개의 상이한 내용으로 되어 있는데 첫번째는 시스템에서 규정된 보안기능의 정확한 구현에 대한 정확성(correctness)에 관한 모든 기준을 포함하고 있으며, 두번째는 시스템 평가과정에서 발견된 보안기능, 보안 매카니즘의 유효성(effectiveness)을 나타내는 기준을 포함하고 있다. 이와같이 보증에 관한 평가는 정확성과 유효성에 관한 기준이 만족되었다는 것을 증거로 제시해 준다.

1) 정확성(Correctness)

이 기준은 평가 시스템에 관한 신뢰에 따라 7개의 평가등급을 제시하고 있는데 E0가 가장 낮은 등급이고, E6가 가장 높은 등급이다. E1으로부터 E6에 이르는 평가등급은 점진적으로 요구사항이 증가하는데 개발과정, 개발환경, 운영 지침서, 평가를 위한 운영결과 등이 어떻게 만족되어야 하는지를 나타내고 있다.

2) 유효성(Effectiveness)

유효성이란 보안 제품이 사용될 가상적인 환경이나 실제 환경에서 일어날 수 있는 가정된 또는 실제 위협에 대응하는 능력을 말한다. 유효성 평가를 위한 지침은 평가 등급별로 구분되지 않고 전체로서 적용되도록 제시하고 있다. 유효성 평가는 시스템이 사용될 환경에서의 제안된 사용에 관한 사항으로 다음과 같은 기준을 포함하고 있다.

- 기능의 적합성(Suitability) : 시스템의 보안기능이 보안 목표에 규정된 위협에 대응할 수 있는지 여부
- 기능의 결합성(Binding) : 각각의 보안기능과 매카니즘이 함께 수행되어 통합될 수 있는지 여부
- 매카니즘의 강도(Strength) : 보안 매카니즘이 직접 공격에 견딜 수 있는지 여부
- 사용의 편리성(Ease) : 보안 기능과 매카니즘을 실제 운영시의 편리성
- 운영 침투에 대한 보호 : 시스템 운영시 보안 목표에 규정된 보안이 유지되지 않는 침투허점이 발견될 수 있는지 여부

이러한 기준에 근거하여 유효성 평가는 시스템의 보안 매카니즘에 대한 강도를 기본(basic), 중급(medium), 고급(high)으로 분류하고 있다. 기본 등급은 모든 중요한 매카니즘이 비록 시스템에 관한 정보를 알고 있는 공격자로부터는 침투당할

수는 있지만, 그 외의 우연한 침투 공격으로부터는 보호되는 수준이고, 중급 등급은 모든 중요한 매카니즘이 제한된 기회와 자원을 갖고 있는 공격자로부터 보호되는 수준이며, 고급 등급은 모든 중요한 매카니즘이 고급 수준의 기술, 기회, 자원을 갖고 있는 공격자에 의해서만 침투될 수 있는 수준이다.

6.4 종합 등급(Rating)

보안 평가후에 종합 등급은 유효성과 보증 기준을 제외한 보안기준과 정확성 기준에 의하여 보안 요구가 더 엄격한 순서로 다음과 같이 분류된다.

(E0), (F1, E1), (F2, E2), (F3, E3), (F4, E4), (F5, E5), (F5, E6)

정확성 기준을 만족하지 못하는 모든 시스템은 E0 등급인 부적절한 보증 등급을 부여 받으며, 정확성 기준을 만족하는 경우에도 유효성 측면에서 실패한 모든 시스템도 역시 E0 등급을 부여받는다. 유효성 기준에 대한 등급은 별도로 부여하지 않는다.

6.5 미국의 보안 평가기준과의 비교

표 1. ITSEC과 TCSEC간의 비교

ITSEC 기능 수준	ITSEC 정확성 수준	TCSEC 평가 등급
-	E0	D
F - C1	E1	C1
F - C2	E2	C2
F - B1	E3	B1
F - B2	E4	B2
F - B3	E5	B3
F - B3	E6	A1
F - IN Data Integrity F - AV System Availability F - DI Communication Integrity F - DC Communication Secrecy F - DX Network Security		

ITSEC에서 보안 기능 측면으로 분류된 F1 ~ F5 등급은 TCSEC의 5개 등급과 일치하도록 설계되었다. 그러나 ITSEC의 평가등급은 무결성과 가용성의 다양한 기준을 통합하려고 노력하여 TCSEC에는 없는 여러 요구사항을 포함하고 있다. ITSEC의 평가등급과 TCSEC의 평가등급 사이에는 직접적인 일치성은 존재하지 않으나 두 보안성 평가 기준서 사이의 동질성은 다음과 같다.

ITSEC에서 평가된 보안 제품이나 시스템은 해당 행의 TCSEC 요구조건을 충족하지만 그 반대는 성립하지 않는다. 왜냐하면 ITSEC의 요구사항들이 TCSEC의 요구사항보다 더 광범위하고 구체적이기 때문이다. ITSEC은 심지어 접근제어 정책을 갖고 있지 않는 시스템까지도 평가 범주에 포함시켜 그 평가대상이 광범위하기 때문에 TCSEC의 TCB(Trusted Computing Base)와 참조 모니터(Reference Monitor)의 개념을 포함하고 있지 않다.

7. 암호 알고리즘

7.1 HMG Application

본 제도하에 성공적으로 평가받은 제품은 모든 HMG 어플리케이션에(특히 암호 분야에서는) 적합한 것은 아니다는 사실을 주지해야 한다. 사용자들은 초기에 CSEG(사용자 요구와 조정 그룹의 장)에게 자문을 구해야 한다.

HMG confidentiality application에는 암호 알고리즘이 이미 발표되었거나 공공에 사용될 수 있는 것은 사용하지 않는 것이 HMG의 정책이다. 이는 HMG 정보에 대한 위협(the nature of threats)에 대비하기 위한 것이다.

HMG의 분류된 정보나 기타 기밀 자료를 보호하기 위해 사용되는 모든 암호 기술들은 CESG로부터 승인을 받아야 한다. 일반적으로 CESG가 지정한(CESG-specified) 알고리즘 사용을 요구하고 있다. 이러한 알고리즘들은 HMG 부서들과

정부기관에 준하는 기구 또 몇몇 영국 회사들(firms)에서만 사용 가능하다.

7.2 RAMBUTAN

CESG가 설계한 암호칩(cryptographic chip)으로서 허가를 받아야만 사용할 수 있다. HMG 통신 링크상에 사용될 때 RESTRICTED로 분류된 것(material)과 기밀 자료이나 분류되지 않은 것들을 보호하기 위해 승인되고 있다.

영국내에서 통신상에서의 비밀자료에 대한 보호를 요하는 응용들에 승인되어질 수 있다. 해외 통신 링크상에 비밀 자료들의 보호는 경우에 따라 승인되어질 수 있다.

또한 RAMBUTAN은 CESG 승인을 조건으로, 비밀성 뿐만 아니라 무결성을 위한 암호학적 처리(cryptseal), privacy compartmentation 혹은 패스워드 암호와 같은 COMPUSEC 응용들에서 정보를 보호하기 위해서 사용될 수 있다.

1994년 7월 30일부터 CONFIDENTIAL까지의 분류된 비밀자료에 대한 암호학적 보호에 있어서 새로운 HMG COMSEC 요구 조건은 CESG가 평가(assess)하고 승인한 하드웨어, 본 제도에 의해 적정한 레벨로 승인된 소프트웨어 혹은 RAMBUTAN 장비를 사용할 것을 권고하고 있다.

8. 결 론

본 연구에서는 국내 정보보호 체계를 수립하기 위하여 외국에서의 정보보호 체계분석의 일환으로 영국의 평가 승인 체계에 관해 분석하였다. 먼저 영국에서의 정보기관 구조를 소개하였으며, 정보보호 체계와 관련한 조직으로서 CESG, DTI, 관리 위원회, 평가기관, 승인기관에 대한 조직구성 및 임무에 대하여 기술하였다. 또한 영국의 정보보호 시스템 평가승인 제도를 분석하였으며 영국의 암호 알고리즘과 평가 기준서인 ITSEC에 대해 분석하였다.

영국에서는 국가 보안 업무를 통해 조정하는 외무부 산하의 CESG와 산업, 민간 분야의 정보보호 업무를 담당하는 상공부가 주축이 되어 정보보호 체계를 수립하여 운영하고 있다. 특히 정보보호 시스템에 대한 평가는 정부가 승인한 민간 업체(CLEF)에서 수행하고 있으며 최종승인은 CESG와 상공부가 운영하는 승인기관인 Certification Body에서 하며 승인된 제품은 Certified Product List에 게재되어 공표된다.

우리나라도 정보화 사회에서 자국의 정보를 보호하기 위해서는 국가 주요 정보 뿐만 아니라 기업 및 개인 정보를 보호할 수 있는 대책을 수립하여야 하고, 정보보호 시스템의 시장 개방화에 대비하기 위해서는 자주적인 정보보호 기술을 확보하고, 정보보호 시스템의 개발 보급을 보다 활성화하여야 할 것이다.

지금까지의 선진 외국에서의 정보보호 체계에 대한 분석을 토대로 하여 우리 실정에 적합하고 국가적 이익을 최대화할 수 있는 정보보호 시스템 평가 승인 체계를 시급히 구축하여 정보화 사회에 능동적으로 대처하여야 할 것이다.

참 고 문 헌

[1] CESG & DTI, Description of The Scheme, UKSP 01, Issue 1.0, March 1991.

[2] Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France-Germany-the Netherlands-the United Kingdom, June 1991.

[3] The Licensing of Commercial Licensed Evaluation Facilities, UK IT Security Evaluation and Certification Scheme, UKSP02, Version 1.0, March 1991.

[4] Handbook of Computer Security Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP03, Version 1.0, March 1991.

[5] NAMAS Accreditation Standard, General Criteria of Competence for Calibration and Testing Laboratories: M10, March 1989, NAMAS Executive, NPL, Teddington.

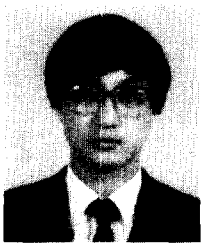
[6] NAMAS Regulations, Regulations to met by Calibration and Testing Laboratories: M11, April 1989, NAMAS Executive, NPL, Teddington.

[7] Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993.

□ 著者紹介

강 창 구

1979년 2월 : 한국항공대학 항공전자공학과 졸업 (공학사)
1986년 2월 : 충남대학교 대학원 전자공학과 (공학석사)
1993년 8월 : 충남대학교 대학원 전자공학과 (공학박사)
1979년 ~ 1982년 : 한국공군 기술장교
1987년 ~ 현재 : ETRI 책임 연구원



윤 이 중

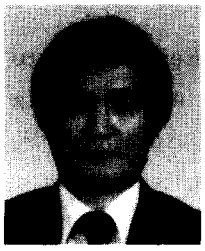
1988년 : 인하대학교 전산학과(학사)
1990년 : 인하대학교 전산학과(석사)
1990년 ~ 현재 : ETRI 선임연구원

※ 주관심분야 : 컴퓨터/네트워크 보안, DBMS

김 대 호

1977년 : 한양대학교 전자공학과(학사)
1984년 : 한양대학교 산업대학교 전자공학과(석사)
1993년 : Univ. of Maryland at College Park
Dept. of Computer Science Visiting Scholar
1977년 ~ 현재 : ETRI 책임연구원

※ 주관심분야 : 전송분야, 통신 및 컴퓨터 보안



이 대 기

1966년 : 한양대학교 전자공학과(학사)
1987년 : 한양대학교 전자공학과(석사)
1980년 ~ 1992년 : ETRI 산업기술개발부장, 지상시스템연구부장
1992년 ~ 현재 : ETRI 책임기술원
한국통신정보보호학회 산학이사