通信情報保護學會誌
第5卷 第1號, 1995. 3

외국의 정보보호 체계 분석(I)

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

강 창 구*, 윤 이 중**, 김 대 호*, 이 대 기***

요 약

본 연구에서는 국내 정보보호 체계를 수립하기 위하여 외국정보보호 체계분석의 일환으로 미국의 정보보호 체계를 분석하였다. 본 논문에서는 먼저 미국의 정보보호 체계의 주요 기구인 NCSC와 NIST의 역할을 알아보고, 미국의 컴퓨터 보안 프로그램으로서 TPEP, 네트워크 제품평가 및 DBMS 평가방법에 대해서 분석하였으며 또한 통신 보안 프로그램으로 CCEP, 정부 승인 DES 제품 프로그램, EFT 인증 프로그램, PNSL, OLSL 및 암호 제품의 판매 제한정책에 대하여 기술하였다.

1. 서 론

정보화 사회의 도래와 함께 정보와 통신의 결합, 정보 자원의 공유, 정보 서비스의 다양화로 인하여 정보 이용이 생활화되고 정보는 중요한 자산이 되고 있다. 이러한 중요 정보를 이용하는 정보 이용자는 정보의 불법 도난, 교란, 훼손, 악용 등의 위협으로부터 정보를 보호하기 위하여 노력할 것이다. 또한 국가 기간 전산망이 완료됨에 따라 중요한 정보 자산이 컴퓨터와 통신망을 통하여 오가게 될 것이며, 정보에 대한 보호대책을 강구하지 않으면 정보 자산의 손실은 피할 수 없으리라 판단되어 진다. 특히 유무선 통신을 이용한 정보의 송수신은 시간적, 공간적 한계를 극복하여 경제, 사회, 문화적 일대 변혁을 요구하고 있다. 특히 금융, 무역, 산업체 등의 여러분야에서 정보의 송수신은 자산의 이동이며 또한 비밀 또는 프라이버시의 이동으로 해석될 수 있다. 한편 정보화로 인하여 야기되는 역기능이 심각하게 대두되어 경제, 산업, 사회적으로 결정적인 손실을 끼칠 우려가 현실로 나타나고 있다.

이와 같은 역기능에 대한 실제 피해 상황은 정확히 공표되고 있지 않지만 정보에 대한 불법 액세스가 그 대부분으로 추정되고 있다. 이러한 불법 액세스는 송수신 양측의 단말부분에서도 발생할 수 있으나 통신로 상에서도 발생될 수 있으므로 통신로 양단에서 암호화 기법과 통신망 접근 액세스 기법에 의해서 정보보호가 이루어져야 한다.

정보보호 시스템에 대한 필요성은 처음에는 국가의 요구에 의해서 제기되어 국가용 정보보호 시스템이 개발 사용되기 사용하였으나 정보화 사회

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

로 접어듬에 따라 개인, 기업 등 민간 부문으로부터의 요구가 급증하게 되었다. 또한 선진외국의 일반용 정보보호 시스템 판매업체의 국내 시장 개방요구에 대처하기 위해서 국익 차원에서 그 필요성이 절실히 요구되고 있다.

이러한 상황에서 국내에서도 국가적으로 정보보호 체계를 수립하여 정보보호 시스템의 개발, 사용을 활성화하여 안전하고 건전한 정보화 사회의 건설에 능동적으로 대처하여야 한다.

따라서 본 연구는 국내 정보보호 체계를 수립하기 위한 기반연구로서 본 논문에서는 미국에서의 정보보호 체계를 분석하고자 한다.

2. NCSC와 NIST의 역할

2.1 NCSC(National Computer Security Center)

1981년 국방부는 Computer Security Initiative에 의해서 시작된 업무를 확장하기 위하여 NSA(National Security Agency)내에 CSC(Computer Security Center)를 설치하였다. 그후 CSC는 컴퓨터 보안을 모든 정부기관에 확장 적용하기 위하여 1985년 8월에 CSC를 NCSC로 명칭을 변경하였으며 NCSC의 주요 임무는 다음과 같다[4].

- trusted 컴퓨터 시스템의 보급확산
- commercial vendors에 의해서 개발된 보안 제품 평가
  trusted OS, compartmented mode workstation, system high workstation, network products, add-on security products, security subsystem, formal verification tools
- 컴퓨터 보안연구 개발에 관련하여 정부 및 기업체에 대한 기술 지원
- trusted 시스템과 응용에 통합될 수 있는 보안 기술에 관한 연구지원 및 연구결과 공표
- TCSEC(Orange book) 요구사항에 대한 기술지침서 개발 및 출판
- trusted 시스템 개발 평가에 따른 자문, 교육 및 tool 제공
- 설계 결함등의 시스템 보안 문제를 Computer Security Technical Vulnerability Reporting Program에 보고하는 체계 구성
  - 평가된 제품에 대해서 결함이 발생되면 제품의 등급이 조정된다.

NCSC는 NIST와 밀접한 관계를 유지하면서 업무를 수행하며, 특히 NIST의 CSL(Computer Systems Laboratory), DIA(Defense Intelligence Agency) 및 기타 컴퓨터 보안 관련 정부기관과 밀접한 관계를 유지하고 있다.

2.2 NIST(National Institute of Standards and Technology)

NIST의 CSL는 컴퓨터 보안의 표준제정, 연구업무 수행, 보안 제품 시험, 컴퓨터 보안 교육 및 기타 정부기관을 지원하며 다음과 같은 주요 업무를 수행한다.

- 컴퓨터 보안 표준 개발 및 표준화 연구 개발 지원
  - 표준화 기구인 ANSI, ISO, IEEE와 긴밀한 협조체제 유지
  - FIPS(Federal Information Processing Standard) 발간
- 연구 수행으로 보안 해결책 마련
  CSL은 자체 연구를 수행하고 연구 결과를 공표한다.
  또한 NSA와 협력하여 Open System 용으로 개발된 보안 표준이 국방부의 요구조건을 만족함으로 보증한다.

• 시험 방법 개발

CSL은 메세지 인증, 키관리 등 특정한 정보 표준(Federal Standard)에 대해서 업체에서 개발한 시스템의 적합성 시험을 수행하기 위한 시험용 시스템을 개발 제공하며 POSIX, OSI, NSA의 SDNS에 대한 test suites를 개발하고 있다[6,8].

3. 컴퓨터 보안 프로그램

3.1 TPEP(Trusted Product Evaluation Program)

NCSC의 주요 프로그램으로서 TPEP에 의해서 trusted OS와 기타 보안 제품들을 평가한다. 또한 TPEP는 TCSEC의 기준에 의하여 기술적 보호능력을 평가함으로써 상업용 컴퓨터 시스템의 보안 평가에 역점을 두고 있다.

trusted 시스템의 평가에 관한 세부내용은

- TCSEC(Orange book)
- Trusted Product Evaluations : A Guide for Vendors(Aqua book)

에 기술되어 있다.

trusted 시스템의 평가 절차는 그림 1과 같다.

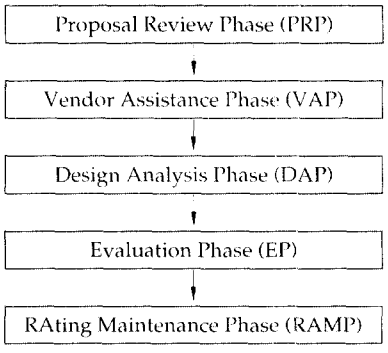


그림 1. trusted 시스템의 평가 절차

가. 제안서 검토 단계(Proposal Review Phase : PRP)

1) 초기 접촉(Initial Contact)

업체는 개발, 평가, 승인등 전체 계획에 대해서 토의하고, trusted 시스템을 제작 및 평가 처리 절차에 대해서 협의하기 위해서 NSA의 ISSO (Information System Security Organization)와 초기 접촉하여야 한다.

2) Certificate

제안서를 작성하기 전에 "Certificate Pertaining to Foreign Interests"에 서명하여야 한다. 이 문서에는 회사의 owner가 외국인이지 아니하며 외국인의 통제와 영향(FOCI : Foreign Ownership, Control, or Influence)을 받지 않고 운영되고 있다는 것이 명시되어 있어야 한다.

3) 제안서 검토(Proposal Package Review)

아래 내용을 포함한 제안서를 4부 제출하여야 한다.

• 회사 소개
  - 회사의 능력, 특히 trusted 제품 개발 능력
  - 연락 창구, 회사 규모, 생산 제품 혹은 서비스 실적, 최근 재정상태정보

• 시장 정보
  - 제안된 제품에 대한 시장성
  - 제품의 예상 사용자 현황 정보
  - 제품이 만족하는 정부 및 민간상의 요구사항

• 제품 제안서
  - 제품에 대한 기술 정보
  - 제품이 만족하는 보안 서비스
  - 목표 등급(B1, C1 등)
  - 개발 일정 계획
  - 기존 제품과의 차이점 및 특징

4) 프로그램 결정(Program Decision)

Office of Acquisition Policy and Business Development는 제안서를 검토하고 제안된 제품

의 NSA와 관련성 여부 및 평가 대상 품목 여부를 결정한다.

5) 사전 기술 검토(Preliminary Technical Review)

평가 전문가로 구성된 평가팀은 제품 제안업체의 전문가와 함께 제품의 개발 단계를 평가하고 사전 기술 검토 보고서(PTR : Preliminary Technical Report)를 작성한다.

6) 법적 합의(Legal Agreement)

제품 제안회사와 NSA는 법적 합의서에 서명한다. NSA는 제품 평가 수행에 필요한 보안 관련 정부를 제공할 것이며 모든 소유권 정보를 보호할 것에 서명한다.

공급자는 필요한 모든 기술정보를 제공할 것이고, 모든 필요 절차를 따를 것이며 NSA 혹은 기타 정보 프로그램을 근거로한 모든 제품 관련 문서를 NSA에 제출할 것이고 또한 RAMP 보고서를 준비할 것에 서명한다.

또한 쌍방은 법적합의서를 주기적으로 검토할 것에 동의한다.

7) 팀 선정(Team Assignment)

NCSC는 Trusted Products and Network Security Evaluation Division 부서로 부터 프로그램 관리자 및 기술 협력 창구를 선정한다. 업체는 기술적 결정 및 평가 기준의 적용 및 해석에 대해서 책임을 진다.

나. 업체 지원 단계(Vendor Assistance Phase : VAP)

이 단계에서 업체는 시스템을 개발하고, 보안시험절차를 수립하고 초안 문서를 작성한다. NCSC는 이 단계에서 시스템 설계 및 구현에 있어서 업체로부터의 문의에 응답함으로써 업체를 지원한다.

이 단계는 다음 두 단계로 구성된다.

1. 제품 개발 milestone 설정
2. 문서 작성 : 시스템 설계서, 시험계획서, RAMP 계획서 등

다. 설계 분석 단계(Design Analysis Phase : DAP)

이 단계에서는 설계서, 시험 계획서, 정형 검증(formal verification) 결과 및 기타 제공자료에 근거해서 설계 내용을 분석한다.

이 단계의 최대기간은 1년을 초과하지 않아야 하며 다음 세 단계로 구성된다.

1) 평가팀 검토

NCSC 평가팀은 제품설계에 대한 세밀한 심사를 수행한다.

평가팀 구성은 NSA section 71의 평가팀과 3개의 정부출연 연구 개발 센타 즉, Aerospace Corporation, Institute for Defense Analysis, Mitre Corporation로부터 선발된 사람들로 구성된다.

2) 초기 제품 평가 보고서(Initial Product Assessment Report : IPAR)

평가팀은 평가결과를 초기 제품 평가 보고서(IPAR)를 작성한다.

이 보고서에는 제품의 초기 평가 내용, 제품의 예상 등급, 평가 등급에 대한 기술적 요구사항 및 그 요구사항의 만족 방법등이 포함되어 있다.

3) 기술 검토 위원회(Technical Review Board : TRB)

NCSC는 기술검토위원회(TRB)를 소집하여 평가팀은 IPAR를 발표하고, 기술 검토를 받는다. 제품은 평가단계(Evaluation Phase)에 들어가기 전에 제품은 완성되어 판매 가능한 상태에 있어야 한다.

라. 평가 단계(Evaluation Phase)

이 단계에서 평가팀은 하드웨어, 소프트웨어 및 최종 문서들을 세밀히 분석하고, 시스템의 기능 시험을 수행한다. 또한 요구되는 등급에 대한 평가 요구사항에 대응하는 시스템의 보안 특징 및 보증내용이 기록된 문서를 작성한다.

1) 법적 합의서(Legal Agreement)

TRB의 승인이 나면 업체는 제품에 대한 평가 단계에 들어갈 수 있다.

만약 업체가 공식 평가(Formal Evaluation)를 요구하면 업체와 NCSC는 합의된 일정에 따라 공식 평가를 위하여 제품을 제출할 것을 법적 합의서에 서명한다.

2) 제품 게시(Product Bulletin)

제품이 공식평가에 들어오면 처리과정은 공개된다. NCSC는 Information Systems Security Products and Service Catalogue의 다음 분기호에 간단한 제품 소개를 한다. 이때 제품은 공식적으로 평가받고 있음과 업체의 요구등급을 나타내어야 한다.

3) 시험 준비(Evidence Review, Testing Preparation)

평가팀은 보안특성의 만족도, 설계서, 원천 부호, 질의에 응답할 업체의 창구인 등 시스템을 검사하고 시스템 시험을 준비한다.

4) 평가 보고서 초안(Draft Evaluation Report)

평가팀은 제품에 대한 최종 평가 보고서(Final Evaluation Report)의 초안을 IPAR를 근거로 하여 작성한다.

5) 시험 기술 검토 위원회(Test Technical Review Board)

NCSC는 공식 시험을 수행하기전에 시험 기술 검토 위원회를 소집하여 위원회로 하여금 초기 평가 결과를 검사하고, 제품이 모든 요구사항을 만족하는지를 검토 결정한다.

6) 시험(Testing)

평가팀은 공식 시험(formal testing)과 보안 시험(security testing)을 수행한다.

7) 최종 기술 검토 위원회(Final Technical Review Board)

시험이 성공적으로 끝나면 NCSC는 최종 기술 검토 위원회를 소집하여 평가팀의 제품 평가를 확인한다. 이 위원회는 평가팀이 작성한 FER (Final Evaluation Report)초안과 Information Systems Security Products and Services Catalogue에 나타날 EPL(Evaluated Products List)에 게재 자료를 검토한다.

8) 최종 평가 보고서(Final Evaluation Report)

NCSC는 수정된 최종 평가 보고서를 출판한다. 여기에는 평가과정, 제품개요, 평가등급의 요구사항 만족내용, 평가자의 comment, 평가 부품에 대한 요약 및 기타 기술 정보등이 포함되어 있다.

9) 평가제품 목록(Evaluated Products List : EPL)

NCSC는 평가가 완료된 제품을 Information Systems Security Products and Service Catalogue의 다음 분기호의 EPL section에 등록하여 발표한다.

마. RAMP(Rating Maintenance Phase)

제품이 공식적으로 평가받고 등급이 결정되면 등급은 공표되고 제품을 광고할 수 있다. RAMP는 EPL을 유지시키며 이 단계에서 제품에 새로운 기능을 추가할 수 있고 보증받은 제품의 새로운 version을 내놓을 수 있다.

3.2 네트워크 제품 평가(Evaluation of Network Product)

TPEP는 주로 trusted Operating System에 역점을 두고 있으나 네트워크 제품에도 적용된다. 네트워크 제품의 평가에 관련된 NCSC의 문서는 다음과 같다.

- TNI(red book)
  네트워크 제품에 대한 TCSEC의 요구사항을 기술하고 있으며, 또한 무결성, 부인봉쇄, 데이타 비익등 네트워크 환경에서 고려해야 할 대상들을 기술하고 있다.
- Trusted Network Interpretation Environments Guideline of the TNI of TCSEC
  trusted 컴퓨터 네트워크를 통합하고 운용 및 유지하는데 관련된 정보와 이기종 네트워크간에 요구되는 최소 보안 요구사항을 기술하고 있다.
- Trusted Product Evaluations : A Guide for vendors
  네트워크 제품을 평가 받기 위한 절차가 기술되어 있으며 이 절차는 Operating System에서와 유사하다.

3.3 데이타베이스 관리 시스템 평가(Evaluations of Database Management Systems)

- TPEP는 DBMS의 평가에도 적용된다.
- 데이타베이스 제품의 평가는 국방부 Trusted Database Management System Interpretation(TDI, Lavender book)에 따른다.
- TDI는 데이타베이스 관리 제품에 대해서 TCSEC을 설명한 것이다.
- 데이타 무결성, 데이타베이스 보호 권리 및 보안 라벨링(Security labeling)에 역점을 두고 있다.

4. 통신 보안 프로그램

미국정보는 암호와 통신보안 분야를 COMSEC이라 한다. 한편 COMPUSEC 프로그램은 정보가 처리되거나 저장되고 있는 동안에 정보에 대한 보호 대책이다.

COMSEC 프로그램의 목적은 통신매체가 무엇이든지간에 통신하는 중에 정보의 불법 액세스, 노출, 획득, 변조, 손실을 방지하기 위하여 설계된 보호 장치를 구현하는데 있다.

미국 정부의 COMSEC 프로그램은 NSA에 의해서 주로 관리되고 있다.

NIST와 재무부 (Treasury Department)는 통신보안 제품의 표준화를 추진하고 있다.

COMSEC 프로그램의 초점은 암호 제품이다. 비록 정부는 네트워크 전체 보안과 통신보안제품에 많은 관심을 가지고 있으나 이들 제품의 연구 및 평가는 주로 COMPUSEC 프로그램하에서 NCSC에서 수행되어 왔었다. 안전한 네트워크에 대한 관심이 증가함에 따라 많은 프로그램이 개발되고 있으며 예를들면 NIST에서는 OSI 기본 모델에 근거한 제품의 시험, 평가 및 승인 프로그램을 개발하고 있다.

COMSEC 프로그램으로는 다음과 같은 프로그램이 있다.

- Commercial Communications Security Endorsement Program
  : 고등급(high grade) 암호제품을 평가하는 프로그램
- Government Endorsed Data Encryption Standard Equipment
  : DES 알고리즘에 근거한 암호 제품을 평가하는 프로그램
- Electronic Funds Transfer Certification Program
  : 금융 거래에서 메세지 인증에 주로 사용되는 제품을 평가하는 프로그램

4.1 CCEP(Commercial COMSEC Endorsement Program)

1985년까지 NSA는 분류된 암호 알고리즘을 이용하여 고등급(high-grade) 암호제품의 개발자 역할을 하여왔다. 여기서 high-grade 암호제품이란 다음과 같은 것이 있다.

Type 1 : 분류된 데이타를 암호하는데 사용

예 STU(Secure Telephone Unit)
Trunk Encryption Device

Type 2 : 미분류된 sensitive 데이타를 암호하는데 사용

예 Authentication Devices
Transmission Security Device
Secure LAN

CCEP의 제정 목적은 업체의 설계개발 기술능력, 양산성과 NSA의 통신보안 개발 경험을 접목하여 미국 정부 및 민수 부분에 있어서 사용될 성능 좋고 값싼 통신보안 시스템을 개발하여 널리 보급하는데 있다.

이러한 목적으로 업체로 하여금 정부의 분류된 알고리즘을 업체의 통신보안 제품에 구현하고 이들 제품을 판매토록 유도하였다. 그러나 정부의 CCEP에 의한 승인 정책은 NSA가 승인한 암호제품 목록인 ECPL(Endorsed Cryptographic Products List)에 등록된 제품일지라도 사용자가 사용함에 있어서 제품의 효율성, 적합성에 대해서는 보증하지 않는다.

따라서 NSA는 기본 기능 규격에 따라 특정 제품을 개발하기 위해서 업체와 계약을 함으로써 암호 기술을 얻었다. 1985년 NSA는 개발 위험(development risk)을 업체로 넘기고, 제품의 시장성을 높히기 위하여 CCEP를 제정하였다. 이전의 계약 방식으로는 하나의 제품을 개발완료하는데 7년내지 10년이 소요되었으나 CCEP에 의해서는 거의 2년으로 cycle을 줄일 수 있었다. CCEP를 통하여 정부와 기업체 대표는 통신보안 제품, 특히 암호 장치를 개발, 시험, 승인하는데 사업 파트너가 되었으며 이것은 NSA의 암호 전문기술, 분류된 암호 알고리즘과 기업체의 사업 경험, 재정력을 조화시키는데 있었다. 그 결과 NSA의 희망데로 정부가 필요로하는 제품의 가격을 낮출 수 있었다.

NSA의 승인제품을 제작하기 전에 업체는 먼저 CCEP의 회원이 되어야 한다. 회원이 되기 위해서는 갖추어야 할 조건은 다음과 같다.

- 업체는 외국인 고용주 혹은 외국의 통제 및 영향을 받지 않아야 한다는 내용의 Certificate Pertaining to Foreign Interests에 서명하여야 한다.
- DIS(Defense Investigative Service)로부터 시설 및 인원에 대한 보안점검을 받아야 한다. 이것은 최종제품이 분류되지 않을지라도 알고리즘이 분류되어 있기 때문이다.
- 국무부의 군수통제국(OMC : Office of Munitions Control)에 등록되어야 한다.
- COMSEC 관련 자료를 배포받기 위한 COMSEC Material Control System을 갖추어야 한다.
- 공식적인 COMSEC 자료를 수발할 책임있는 COMSEC 관리자를 지명하여 NSA와 업체간의 창구 역할을 하며 자료 수발은 비밀 통신 채널을 이용하여야 한다.

CCEP에 등록되면 NSA는 해당업체에 대한 프로그램 관리자(Program Manager)를 지명한다. CCEP 프로그램 단계는 다음과 같다.

가. 초기 접촉(Initial Contact)

제작업체는 NSA와 접촉하고 다음 자료를 준비한다.

- 제품 제안서
  제품 설명서, 분류 등급, 보안 특징, 적용대상 시스템, 시장성, 경쟁성, 추진 일정계획
- 회사 소개서
  회사 소개, 전문 분야, 보안 상태
- 제품 보증서(Product Assurance Survey)
  회사의 경험, 제조 능력, product integrity, canfiguration, control, 제품 지원 능력

나. 프로그램 결정(Program Decision)

NSA는 업체의 제안서를 검토하고, 제안된 제품의 가치와 필요성을 판단하고, 업체의 보안성과 적합성(suitability)을 평가한다. NSA는 개발 제품이 시장성이 있고, 제품 개발 능력이 있는지를 판단하여야 한다. 또한 NSA는 COMSEC 제품의 개발 및 생산능력을 평가하기 위해 업체로 평가팀을 보낸다. 평가팀은 평가기준으로 NSA의 Objective Standards for Product Assurance를 이용하여 시설등을 평가하여 제안서를 승인한다.

다. MOU(Memorandum of Understanding)

NSA가 제작업체의 제안서를 승인하게 되면 NSA와 제작업체는 MOU에 서명하여야 한다. 이 MOU에는 NSA와 업체가 책임져야 할 사항이 기술되어 있다.

업체는 제품 평가에 필요한 모든 정보를 NSA에 제공할 것이며 모든 CCEP 요구조건을 준수할 것에 서약하고, NSA는 필요한 COMSEC 정보를 제공할 것이며 업체의 권리를 최대한 보호할 것임을 서약한다.

라. 제품 설계(Product Design)

업체는 MOU에 따라 제품을 설계하고 NSA 프로그램 관리자는 NSA의 모든 필요사항과 조치들을 제공하여야 한다.

마. MOA(Memorandum of Agreement)

MOU가 서명되면 NSA는 업체에게 만족되어야 할 특정된 보안사항과 제품 관련 요구조건을 통보한다. NSA는 다음 두개의 문서를 작성하고,

- TSRD(Telecommunication Security Requirements Document)
- ADRL(Agreement Data Requirements List)

업체는 많은 문서를 작성하여야 한다. 그 중 대표적인 것은 다음과 같다.

- TEO(Theory of Equipment Operation)
- TC(Theory of Compliance)

이들 자료는 MOA에 첨부된다.

이 MOA에는 업체와 NSA의 부가적인 책임 및 제품 개발, 평가에 대한 일정등이 명시되어 있다.

바. 제품 개발(Product Development)

업체는 MOA의 요구 사항에 따라 제품을 개발하고 시험한다. 이때 NSA 프로그램 관리자는 NSA의 모든 필요사항과 조치 사항을 제공하여야 한다.

사. 승인(Endorsement)

MOA의 모든 요구사항이 만족되면 업체는 개발한 제품과 평가에 필요한 ADRL에 기술된 모든 것을 제출하고, NSA는 제품을 평가하고 TSRD를 만족하면 MOA에 명시된 것과 같이 제품을 승인한다. 승인된 제품은 ECPL(Endorsed Cryptographic Products List)에 등록하고, 다음 분기의 Information Systems Security Products and Services Catalogue에 제품에 대한 소개를 한다.

아. 생산(Production)

업체는 승인된 제품을 판매하고 고객이 요구하는 현장에 설치한다. 이때 모든 판매는 판매 제한 조건에 따라야 하며 NSA는 제품이 회계 절차에 따라 생산되고, TSRD와 승인된 모든 항목에 일치하는지를 보증하여야 한다.

4.2 Government Endorsed DES Equipment Program

NSA는 1982년 DES를 이용한 제품의 일관성 있는 시험과 승인을 위하여 이 프로그램을 제정하였다. 이 프로그램에 의하여 업체들은 그들의 DES 제품을 NIST에 제출하였고, NSA와 NIST는 제출된 제품에 대하여 DES 알고리즘이 정확히 구현되었는지 또는 Federal Standard 1027와 국가 통신 보안 관련 요구사항을 만족하는지를 인증하였다.

1988년 NSA는 Government Endorsed DES Program을 점진적으로 폐지하기 시작하였으며 금융 응용 분야를 제외한 새로운 DES-based 제품에 대한 승인을 중지하였다.

DES 제품은 아직도 재무부에 의해서 승인되고 있으며 NSA Endorsed DES Products List (NEDESPL)는 기존 DES 제품에 대해서는 사용자들의 편의를 위해서 Information Systems Security Products and Services Catalogue에 공고되고 있다.

4.3 EFT Certification Program

재무부는 미국 정부의 금융거래에 있어서 메세지 인증에 주로 사용될 제품에 적용되는 승인 프로그램, 즉 EFT(Electronic Funds Transfer) Certification Program for Authentication Devices를 운용하고 있다. 이 프로그램에 의해서 평가되고 승인된 EFT Message Authentication Code 장비는 다음 정책 표준에 의하여 시험되고 있다.

- Federal Standard 1027-DES Encryption
- ANSI X9.17 - Optional Electronic Key Management

이 프로그램에 대한 상세한 내용은 Criteria and Procedures for Testing, Evaluating and Certifying Message Authentication Devices for Federal EFT Use에 기술되어 있다.

4.4 Protected Network Services List

정부는 NSA에 의해서 승인된 통신 서비스를 제공하는 common carrier의 목록을 유지하고 있다. 이 목록상에 서비스는 point-to-point로 전달되는 미분류 sensitive 정보를 보호하기 위해서 승인되었다. 이 PNSL 목록은 Information Systems Security Products and Services Catalogue에 포함되어 있다. 네트워크 보호 서비스는 다음 세 분류로 나눌 수 있다.

- PL(Private Line)
  전용회선으로서 승인된 PL은 암호를 사용하거나 보안 통신을 위한 조치가 취해져 있어야 한다.
- FDN(Flexibly Defined Network)
  Network of sequential links and no permanent physical circuit
- SPRS(Switched Protected Routing Service)
  공중(PSTN)통신망을 통해서 sensitive 정보를 보호해 주는 시스템

4.5 Off-Line Systems List

Off Line용 암호 제품으로서 Information

Systems Security Products and Services Catalogue에 OLSL이 포함되어 있다. 제품종류로는 다음과 같은 것이 있다.

- Manual Cryptosystems
  : operation codes, ciphers, authentication systems, one-time pad 등 대부분 고전적이며 오랜기간 동안 사용되어 왔다.
- KL-43
  : portable keyboard(card key...)
- Signals Operation Instructions(SOI)
  : 전시 또는 훈련 도중에 호출신호 및 레디오 주파수 변경 정보를 담고 있는 책자

4.6 보안장비의 판매 제약

보안장비는 미국 정부의 통제하에 개발되고 판매되고 있으며 암호 제품의 수출 제한은 아주 엄격하다. 암호 제품의 수출 규정은 미국 정보국이 적대국의 통신 내용을 분석하기 어렵게 하는 제품의 사용을 제한하기 위해서 제정되었다. TEMPEST 제품과 같이 암호제품은 미국무성의 OMC(Office of Munition Control)로부터 수출허가를 받아야만 외국 및 미국내의 외국인에게 판매할 수 있다. 암호장비의 형태에 따른 제약은 다음과 같다.

1) Type 1

원칙적으로 분류된 데이타 처리에 사용되며 미국 정부기관 및 정부 계약업체에게만 판매할 수 있다. NSA는 이들 제품의 사용을 NATO와 특정 외국 정부 즉, 캐나다, 오스트리아 등 우방국에게도 허가하고 있다.

2) Type 2

미분류된 sensitive 데이타 처리에 사용되며 미국 정부 기관과 미국내 기업체에 판매 가능하다. Type 1과 같이 NATO 등 특정 국가에게도 사용을 허가하고 있다.

3) DES 제품

미국내의 모든 기관, 미국인 소유의 모든 기관에도 제약없이 판매할 수 있다. 이들 제품은적절한 허가에 의해서 수출가능하나 최근에는 DES 제품을 무결성 서비스용으로는 수출가능하나 암호용으로는 수출되지 않는다.

4) 기타 보안 제품

업체의 고유 알고리즘에 의한 제품은 미국내의 모든 기관, 미국인 소유의 모든 기관에도 제약없이 판매할 수 있다. 이들 제품은 적절한 허가에 의해서 수출가능하다.

5. 결 론

본 연구에서는 국내 정보보호 체계를 수립하기 위하여 외국에서의 정보보호 체계분석의 일환으로 미국의 정보보호 체계를 분석하였다. 본 논문에서는 먼저 미국의 정보보호 체계의 주요 기구인 NCSC와 NIST의 역할을 알아보았으며, 미국의 컴퓨터 보안 프로그램으로서 TPEP, 네트워크 제품 평가, DBMS 평가 방법에 대해서 분석하였고, 또한 통신보안 프로그램으로 CCEP, 정부 승인 DES 제품 프로그램, EFT 인증 프로그램, PNSL, OLSL 및 보안장비의 판매 제한정책에 대하여 기술하였다.

우리나라도 국가 주요 정보 뿐만 아니라 기업 및 개인 정보를 보호하고 보안장비의 시장 개방화에 대비하기 위해서는 자주적인 정보보호 기술을 확보하고, 정보보호 시스템의 개발 보급을 보다 활성화하여야 할 것이다.

앞으로 선진 외국에서의 정보보호 체계에 대해서 보다 깊이 연구분석하여 우리환경에 적합하고 국가적 이익을 위한 정보보호 체계를 시급히 구축하여 정보화 사회에 능동적으로 대처하여야 할 것이다.

참 고 문 헌

[1] Datapro, Datapro reports on Information Security, Vol 1. 1990.

[2] Datapro, Datapro reports on Information Security, Vol 2. 1990.

[3] Datapro, Datapro reports on Information Security, Vol 3. 1990.

[4] D. Russell and G.T. Gangemi Sr., Computer Security Basics, O'Reilly & Associates, Inc. 1991.

[5] Eleen Frisch, Essential System Administration, OReilly & Associates, Inc. 1991.

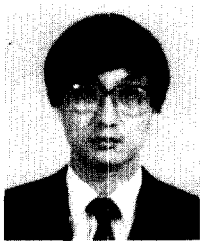
[6] NIST, CSL Annual Report 1992, NISTIR 5127, Feb. 1993.

[7] Manfred Reitenspiess, "Open System Security Standards," Computers & Security, Vol.12, No.4, pp.341-361, 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

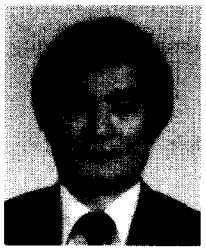
1988년 : 인하대학교 전산학과(학사)
1990년 : 인하대학교 전산학과(석사)
1990년 ~ 현재 : ETRI 선임연구원

※ 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