□특집□

미 국방부의 정보보호 관리체계 및 정책

김 기 윤† 나 관 식††

◈ 목 차 ◈

1. 서 론

미 국방부의 정보보호 관리체계 및 정책은 미 연방정부의 NSA, NIST에 의해 수립된 국가보안체계에 근거를 두고 있다. NSA는 "국가보안체계"라고 알려진 "워너 수정법안(Warner Amendment System)"에 따라 체계 및 통신의 보호에 대한 책임을 맡고 있다. 여기서 "국가보안체계"란 미 정부 및 정부조달업자들이 운용하는 통신 및 정보체계을 말한다. 여기에는 비밀정보도 포함되고, 국가보안과 관련된 암호행위도 포함되고, 군사력의 명령 및 통제도 포함되고, 무기 및 무기체계의 모든 장비도 포함되고, 군사 및 첩보행위를 수행하는데 필수적인 장비도 포함되고, 관례적인 상거래에서 이용되는 장비나 서비스도 포함된다. 또한, NIST는 연방정부의 전산체계에 대한 전산보안 표준 및 지침을 개발해서 보급하는 책임을 맡고 있다. 특히 NIST에 NCSL(National Computer Systems Laboratory)이 컴퓨터 보안 표준 및 지침을 개발하고, 컴퓨터 보호에 관한 FIPS(Federal Information Processing Standards)를 발행하고 있다.

1969년에 NSA(National Security Agency), DSB (Defense Science Board), 미 의회 등에서 정보보호 정책을 입안했다. 1970년 부터 정부, 학계, 산업계 등에서 정보보호정책에 대해서 연구하기 시작했고, 1977년 부터는 정부와 산업계에 적용하기 시작했다. 1983년에 미 국방부(DoD; Department of Defense)는 '70년대 부터 시작된 연구결과를 가지고, 정보보호 요구사항을 기술한 "Orange Book"을 발행하였다. 1984년에는 미 국방부의 CSEC(Computer Security Evaluation Center)를 모든 연방정부기관에 대한 전산보안평가에 대한 책임을 지도록 했다. 1985년에 NSA는 NCSC(National Computer Security Center)를 설립해서 안전한 전산시스템의 폭넓은 이용을 촉진시키고 있다. NCSC는 국가보안체계와 관련된 위험평가, 보안계획, 보안대책의 식별 및 운영 등에 관해서 연방정부의 모든 부서를 도와주고 있다. 1985년에 비밀정보를 취급하는 모든 연방정부기관이 정보보호를 위해서 개정된 "Orange Book"을 이용했다.

1987년에 제정된 전산보안법(Computer Security

† 정회원 : 광운대 경영학과 교수
†† 정회원 : 서원대 경영정보학과 전임강사

Act)에서 특히 중요한 것은, 제5항(Section)에서 모든 연방기관은 전산보안에 관해서 의무적으로 정기훈련을 받아야 한다는 것과, 제6항에서 모든 연방기관은 전산보안계획을 수립해야 한다는 것이다. 15000 여개가 넘는 연방기관의 전산보안계획들을 NSA와 NIST가 검토해오고 있다. 1992년에 NIST(National Institute of Standards and Technology)는 민간/상업용 위한 "Civil Orange Book"을 만들기 위해서 각 국에 초안을 배포해서 의견수렴을 하고 있다. 1993년에 미 연방정부의OMB (Office of Management and Budget)에서 발행한 Circular A-130에는 연방 정보자원관리에 관한 정책이 제시되어 있으며, 1996년에 부분적으로개정되었다. 국방부를 포함한 연방정부내 모든 행정부서가 전산보안 프로그램을 설치할 것을 요구하고 있다.

미 국방정보체계의 궁극적 목표인 C4IFTW(Command, Control, Communications, Computer, and Intelligence for the Warrior)의 개념은 언제, 어디서, 전투요원들에게 어떤 임무가 주어져도 승리할 수 있도록 필요한 모든 정보를 실시간 제공한다는 것이다. 이를 위해서 미 국방부는 전투요원의 요구에 부응하는 정보시스템을 적용시키기 위해서 미 국방정보기반구조(DII; Defense Information Infrastructure)를 구축하고자 국방 전체차원에서 노력하고 있다. 이를 위해서 DISA (Defense Information System Agency)는 C4I를 기획, 개발, 지원하고, DII의 대부분 중앙관리책임을 갖고, 특히 정보기술분야를 책임지고 있다. DISA는 DII의 정보보호를 위해서 CISS(Center for Information System Security)를 구축했으며, CISS는 DII와 C4I를 위한 정보의 가용성, 무결성, 비밀성 등을 보증하는 관리체계 및 정책에 대한 책임을 지고 있다.

미 국방부의 정보보호 관리체계 및 정책을 기술하기 위해서 제2장에서는 미 국방부의 정보보호 관리체계로서 DISA의 CISS 조직(보호 및 인증부서, 훈련부서, 평가부서 등)에 대해서 기술하고, 제3장에서는 미 국방부의 정보보호정책으로서, 미 국방부 훈령 5200.28-STD에 근거한 미 국방부의 정보보호에 관한 일반정책과 TCSEC에 근거한 미 국방부의 전산체계 평가기준에 대해서 기술하고자 한다.

2. 미 국방부의 정보보호 관리체계

DISA(Defense Information Systems Agency)는 1991년에 미 국방부 훈령((DoDD; Department of Defense Directive) 5105.19에 의거해서 1960년에 창설된 DCA (Defense Communications Agency)의 임무, 기능, 권한 등을 개편해서 설립되었으며, 정보화시대에 부응하는 미군의 첨단 정보체계구축을 목표로 하고 있다. DISA 조직은 미 국방부의 전투지원기관으로 설립되었으며, 국방부 C3I 차관의 지휘/통제를 받고 있다. DISA의 기본임무는 전평시 국방부, 각 군, 합참 등 군지휘기관의 요구에 부응하는 C3(Command, Control, Communication) 및 정보체계를 계획하고, 개발하고, 지원하는 것이다. 국방부 훈령 5105.19에는 31개의 임무 및 기능을 명시하고 있으며, 정보보호에 관련된 사항은 다음과 같다.

1) 국방부의 각 기관의 정보체계보호(통신보호 및 전산보호)의 상호운용성 요구사항의 조정한다.
2) NSA, DIA(Defense Intelligence Agency), 각 군 및 합참의 안전한(secure) 전술 C3 통신의 상호운용성 요구사항의 조정한다.
3) 전반적인 통합 기반구조의 일부로서 안전한 전술 통신 기반구조의 개발한다.

·DISA에 DISC(DISA Information Systems Center)의

임무는 DISA 기관장, DISA 본부, 그리고 전세계에 DISA 라인조직을 지원하는 정보관리 프로그램 및 시스템을 개발하고, 실행하고, 관리하는 것이다. 그리고, DISA 정보시스템의 하부구조를 기능적으로 지원하고, 운영 프로그램을 관리하는 것이다. 또한, 전세계 DISA 전산망, 전화, 비디오 원격회의, 기술적인 통제, 통신센터시설 등의 계획/설계/진화를 관리하는 것이다.

DISA에 CISS(Center for Information System Security)의 임무는 국방정보 전투프로그램(Defense Information Warfare Program)을 개발해서 실행하는 것이다. 즉 국방정보기반구조(DII; Defense Information Infrastructure)체계를 위한 통합된 정보체계보호 프로그램을 수립해서 관리하는 것이다. CISS는 INFORSEC 개발과 DoD 실행 간의 긴밀한 협의를 위해서 DISA와 NSA의 구성원들로 조직되어 있다. CISS는 국방정보전(INFOWAR; Defense Information Infrastructure) 프로그램을 개발하고, 국방정보체계보호 프로그램(DISSP; Defense Information System Security Program)을 수행하기 위해서, DISA의 야전운영국(FOA; Field Operating Agency)으로 설립되었다. CISS는 이러한 주요 임무을 수행하기 위한 기능은 다음과 같다.

1) 국방정보기반구조(DII)를 지원하기 위해서 운영을 보호하고, 검출하고, 대응책을 마련하고, 취약성을 분석한다.
2) 국방부의 요구사항에 따라 전산기, 체계, 네트워크의 보호 인가(accreditation)절차를 실행한다.
3) 국방부의 국방정보전(INFOWAR)에 대한 교육, 훈련, 인식 프로그램을 개발하고 조정하고, 실행한다.
4) 정보보호 기술지원계약(INFORSEC TSC; INFORSEC Technical Services Contract)과 국방부의 바이러스 대응 소프트웨어 사업(ASI; Antivirus Software Initiative)에 대해 관리한다.

CISS의 조직은 다음과 같이 3개 부서로 구성되어 있다.

(1) 보호 및 인증부서(Security and Certification Department)

1) DISA 국장 관할 하에 모든 프로그램 및 사업의 보호정책의 개발/지원/관리한다.
2) DISA의 활동, 프로그램, 직원 등을 위해서 위협 및 첩보에 관한 정보를 제공한다.
3) 인적/물적/정보 보안, 그리고 특수접근 프로그램관리(SAPM; Special Access Program Management), 통신보안(COMSEC; Communication Security), 누출전자파(TEMPEST; Transient Electronic Pulse Emanation Standard)관리, 위험관리, 운영보호(OPSEC; Operations Security), 작업장보호, 범죄예방, 특수보호실(SSO; Special Security Office)에 대해 지원한다.
4) DISA 프로그램에 대한 보호를 지원하고, 국가보안정책위원회에 DISA/DMNCS 대표가 되고, 감찰감(Inspector General)이 취급하지 않는 모든 첩보조사를 관리한다.
5) 전산기, 체계, 네트워크에 대한 인가를 위해서 국방부의 요구사항 및 절차를 실행하고, 정보체계보호의 설계 및 평가를 위한 지침을 제공하고, 그리고 보호요구사항과 표준의 준수여부를 확인하고 실행한다.

(2) 훈련부서(Training Department)

1) 국방부의 국방정보전(INFOWAR)에 대한 훈련 프로그램을 개발 및 실행 하고, 국방정보전 경력관리 프로그램(INFORWAR Career

Management Program)을 개발한다.

2) 국방정보전의 요구사항을 만족하는 정보보호제품의 식별과 보급 절차의 개발, 조정, 문서화, 실행에 대한 책임을 지고, 다수준 정보체계보호사업(MISSI; Multilevel Information System Security Initiative)의 실행을 위한 지침서를 갱신 및 배포한다.
3) 정보보호관련 정기간행물(DISSPATCH)을 출판한다.
4) 보호제품 데이터베이스를 관리한다.
5) 정보보호교육장(ITF; INFORSEC Training Facility)을 운영한다.

(3) 평가부서(Assessment Department)

1) 취약성 분석/평가 프로그램(VAAP; Vulnerability Analysis and Assessment Program)을 수행한다.
2) 취약성 평가를 위한 자동화 도구의 개발 및 관리, 그리고 침입자가 사용하는 도구에 대한 보안대책을 분석 및 개발한다.
3) 범죄 및 대첩보 조사활동에 대한 정보보호 분야 전문기술을 지원한다.
4) 정보보호 기술지원계약(INFORSEC TSC)을 관리한다.
5) ASSIST 프로그램을 관리한다.

DISA의 CISS 이외에 정보보호기술 관련 국방부 조직으로서 DARPA(Defense Advanced Research Projects Agency) 내에 ITO(Information Technology Office)에서는 국방정보체계 관련 기술을 자체 연구원 혹은 외부 연구소와 공동으로 개발한다. ITO의 임무는 국방력의 증강에 필수적인 하드웨어, 소프트웨어, 네트워크, 그리고 시스템관리 기술을 제공하는 것이다.

3. 미 국방부의 정보보호정책

3.1 미 국방부의 정보보호에 관한 일반정책

1970년에 미 국방부는 정보보호를 위한 정책을 제시하기 위해서 DSB(Defence Science Board)를 구성하여 최종보고서(Ware 보고서라고도 지칭)를 발간하였다. 1970년대 중반에는 ARPA (Advanced Research Projects Agency)와 미 공군이 컴퓨터 보안체계의 구성 및 평가 분야를 위주로 연구를 진행하였다. 1985년에 미 국방부 전산체계의 보안성 평가 및 인준기준인 국방부 훈령 5200.28-STD인 TCSEC(Trusted Computer System Evaluation Criteria)에서는 적절하게 인가받은 자만이 정보를 읽고, 쓰고, 생성하고, 삭제할 수 있도록 하는 정보에 대한 접근제어에 중점을 두고 있다 이와같이 국방분야에서는 비밀성을 무결성이나 가용성 보다 상대적으로 더 중요시하고 있다. 미 국방부는 1988년에 일반적인 전산보안에 관한 규정인 국방부 훈령 5200. 1-R (Information Security Program Regulation)에 근거를 두고 있는 전산보안 요구사항에 관한 정책지침서인 미 국방부 훈령 5200.28 (Security Requirement for Automated Information System)을 제시했는데, 그 내용은 다음과 같다.

(1) 전산체계 내의 비밀정보에 대한 보안대책

비밀정보 및 중요한 비밀 미분류정보는 전산체계 내에서 항상 보안대책에 의해서 보호되어야 한다. 이러한 정보에 대해서는 단지 허가받은자만이 접근할 수 있고, 의도된 목적을 위해서만 이용할 수 있고, 정보내용의 무결성이 유지되고, 필요한 비밀표시가 적절하게 되어있도록 보안대책이 마련되어 있어야 한다. 비밀정보에 대해서는, 미 국방부 훈령 DoD 5200. 1-R에 규정된 정보보호 요구사항이 충족되도록 해야 한다.

(2) 전산체계 내의 비밀 아닌 정보에 대한 보안대책

전산체계 내의 비밀이 아닌 미분류정보는 변조, 손실, 파괴로 부터 보호되도록 보안대책이 마련되어서, 필요한 경우에 항상 사용될 수 있어야 한다. 이러한 정보를 획득해서 이용하는데 소요되는 미 국방부의 투자는 보호될 필요가 있으며, 또한 이러한 정보에 대한 사기행위, 낭비, 남용 등은 예방될 필요가 있다. 비밀로 미분류된 정보를 위해서 제안된 보안대책은 OMB Circular No. A-130에 기술되어 있는데, 여기에는 적용가능한 인적, 물리적, 관리적, 기술적 통제방법들이 제시되어 있다.

(3) 정보 및 전산자원에 대한 보안대책

정보 및 전산자원을 (태업, 변조, 서비스 거부, 간첩행위, 사기행위, 횡령, 오용, 허가받지 않은 사람에 대한 노출 등으로 부터) 보호하기 위해서는 관리적, 절차적, 물리적, 환경적, 인적 보안, 그리고 통신보안, 전자파보안, 전산보안(예로써, 하드웨어, 방화벽, 소프트웨어 등)으로 구성된 보안대책들을 지속적으로 채택해서 실행시켜야 한다.

(4) 최소 보안요구사항의 만족

비밀정보 혹은 중요한 비밀 미분류정보를 처리하는 전산체계를 위한 보안대책들은 전산체계의 최소 요구사항이 충족되도록 선택되어야 한다. 이러한 최소 요구사항은 전산화와 수작업을 통해서 비용/효과적으로 그리고 통합적으로 충족되도록해야 한다

(5) 전산제품의 EPL 평가와 TCSEC 승인

상용제품 및 정부개발 혹은 정부지원 제품의 전산보안기능은 평가제품목록(EPL; Evaluated Products List)에 기재된 신뢰성있는 전산제품(trusted computer products)이란 명칭으로 평가되어질 수 있어야 한다. 평가된 제품은 미 국방부 훈령 5200.28-STD에 기술된 보안 구분, 등급, 기능(예로써, B, B1, 접근통제 등)에 따라서 정의되어야 하고, NSA의 NCSC에서 운용하고 있는 보안기준이 충족되어야 한다.

(6) 전산보안체계 구현을 위한 기한과 지정된 승인기관의 인가

전산보안과 관련된 다음과 같은 일정기한을 지켜야 한다.

1) 비밀정보 혹은 중요한 비밀 미분류정보를 처리 혹은 취급하고, 그리고 최소한 통제적인 접근보호(예로써, C2 등급 보안)를 요구하는 모든 전산체계는 위험평가절차를 근거로, 1992년 까지 요구되는 보안기능을 실행시켜야 한다.
2) 전산체계에 C2 등급 이상의 보안기능이 필요한 경우에는, 위험평가절차를 근거로, 보다 엄격한 요구사항을 충족시키는데 소요되는 일정기한을 개별적인 시스템 별로 결정해서 승인을 위해서 지정된 인가책임기관(DAA; Designated Approving Authority)에 제출해야 한다. 위에서 기술한 두가지 경우 중의 어느 경우에도, 적절한 보안대책이 전산체계에 설치/운영되었는지를 평가하기 위하여, DAA가 인가(accreditation)를 해야 한다.

(7) 전산기 중심의 보안기능의 구현이 불가능한 경우, 기타 보안대책의 수립

위 (6)항에 제시된 일정에 따라서, 기존 전산체계 혹은 개발 중인 전산체계에 대해서 추가적인 전산보안기능을 도입하는 것이 너무 비용과 시간이 많이 소요되거나, 기술적으로 힘들거나, 혹은 운영효과 측면에서 도저히 수용할 수 없을 정도로 부정적인 영향을 끼칠 경우가 있다. 이러한 경우에는 다음 사항을 적용시켜야 한다.

1) DAA에 의해 결정된 보안요구수준을 만족시

킬 수 있는 기타 보안대책들(예로써, 물리적 통제, 관리적 통제 등)로 대체할 수 있다.

2) 미 국방부의 부서장, 혹은 미 국방부 부서장이 지명한 DAA만이 위 (6)항의 예외규정을 인가 할 수 있다.

(8) 전산통신망 환경에서의 보안대책 책임규정

서로 다른 DAA가 관리하는 전산체계들이 상호연결되어 있을 경우에는, 개별적인 전산체계에 대한 인가요구사항이 기술된 동의서(MOA; Memorandum Of Agreement)가 필요하다. MOA에는 자료에 대한 설명과 비밀등급, 이용자들의 비밀취급등급, 여러 DAA 들 간의 마찰을 중재/해결하는 DAA의 지정, 전산체계들이 상호연결되기 전에 실행되었던 보안대책들 등이 기술되어야 한다. 어떤 국방부 부서의 전산체계와 동일한 국방부 부서 혹은 다른 국방부 부서의 전산체계가 상호연결 될 때, 그리고 계약자들의 전산체계와 국방부 부서 혹은 다른 국방부 부서 내의 전산체계가 상호연결 될 때, MOA가 반드시 필요하다.

(9) 전산체계 수명주기상의 보안정책 구현

보안정책은 초기 개념개발 부터 설계, 개발, 운영, 유지보수를 거쳐 대체 혹은 폐기 될 때 까지, 전산체계 수명주기 전반에 걸쳐 고려되어야 한다. 전산체계에 대한 모든 보안을 책임지는 DAA가 지명되어야 한다. 이를 위해서 전산체계 개발자의 책임 및 평가계획, 보안대책 요구사항에 대한 강제적인 규정, 비밀자료의 등급과 중요도를 표시, 전산체계에 대한 인가(accreditation), 보안대책들의 평가 프로그램 및 비상계획 수립 등에 대한 사항들이 마련되어야 한다.

(10) 외국인의 전산체계 접근통제

미국정부 소유 혹은 미국정부가 관리하는 전산체계에 대한 외국인의 접근은 국방부 부서장에 의해서만 허가될 수 있고, 그리고 이러한 접근은 미 국방부, 미 국무부(DoS; Department of State), 미 정보국(DCI; Director of Central Intelligence)의 정책과 일관성있게 부합되어야 한다.

(11) 중요한 정보(SCI)의 처리

중요한 정보(SCI; Sensitive Compartmented Information)를 처리하거나 저장하도록 승인된 전산체계에서, 중요하지는 않지만 비밀인 자료(classified non-SCI data)를 중요하지 않은 정보(non-SCI) 수준에서 이용되는 SCI 전산체계로 부터 추출하기 위해서 자동화된 방법(소프트웨어, 방화벽, 하드웨어)을 이용할 수 있다. 이러한 기능은 보안승인의 일부로서 간주되고, 그리고 이러한 전산체계가 최소한 B1 등급으로 운영되는 경우에만 가능하다.

3.2 미 국방부의 전산체계 평가기준

미 국방부에 의해서 1981년에 설립된 CSC(Computer Security Center, 1985년에 NCSC로 바뀜)는 안전한 전산시스템의 이용을 촉진시키기 위해서, 1983년에 전산체계 평가기준(TCSEC; Trusted Computer System Evaluation Criteria, 표지 색깔 때문에 "Orange Book"이라고도 함)을 제시했다. 이 기준은 전산시스템의 보안성을 효과적으로 평가하기 위한 기본적인 요구사항을 정하고, 그 요구사항에 따른 평가등급을 부여하고 있다. 또한, 이러한 기준이 사용되는 영역은 보안제품의 공급자, 이용자, 평가자 등이다. TCSEC은 접근제어방법에 근거해서 보안시스템이 접근하는 주체와 그 대상인 객체를 관련 데이터베이스 시스템을 통해서 제어한다는 관점에서 다음과 같은 요구사항을 갖고 있다.

1) 정책 - 강제적 보안정책(인가받지 않은 사람

은 비밀자료에 접근 할 수 없음)과 임의적 보안정책(선택된 사용자만이 자료에 접근 할 수 있음)이 있다.

2) 표시 - 접근대상이 되는 자료에 대한 보안등급을 식별하는 표지(label)를 표시할 수 있어야 한다.
3) 신분확인 - 누가 자료에 접근하고 어떤 자료가 허가되는지, 접근하는 주체와 객체에 대한 신분확인과 허가자료는 명확하게 식별되어야 한다.
4) 책임추적 - 보안관련 사건들의 발생이 기록되어서 감사자료로서, 추적이 가능하도록 유지/보호되어야 한다.
5) 보증 - 위 4가지 요구사항을 실행 및 평가할 수 있는 하드웨어/소프트웨어 기법이 운영되어야 한다.
6) 지속적 보호 - 이러한 기본적 요구사항들은 간섭 및 비허가된 변조로 부터 지속적으로 보호되어야 한다.

위 요구사항을 기반으로해서 원격접근 전산체계에서 처리되는 비밀정보에 대한 위협을 감소시키기위해서 다음과 같은 전산체계평가기준을 제시했다. 전산체계의 분류기준을 크게는 4가지(D, C, B, A)로 구분하고, C와 B는 각 각 C1, C2와 B1, B2, B3로 세분하고 있다. 각 분류기준 별로 보안정책, 책임추적, 보증, 문서화에 대한 내용을 기술하고 있다.

1) 등급 D (최소한의 보호) - 필요로 하는 보안적 특성은 없다. 이는 더 높은 평가등급에 대한 요구조건을 충족시키지 못한 시스템으로서 일반적인 운영체계가 여기에 속한다.
2) 등급 C (임의적인 보호) - 인지 필요성(need-to-know)을 위해서 자기 판단하에 선택적으로 보호한다.
   C1 (임의적인 보안보호) - 이용자와 자료를 분리하므로써, 선택적인 보안요구조건을 명목상으로 만족시킨다. 사용자 자신이 자료에 대한 제어가 적합한지, 어떤 사용자가 접근할 수 있는지 임의로 결정할 수 있는 권한을 갖게 된다. RACF(Resource Access Control Facility)를 탑재한 IBM MVS 운영체제가 이 등급으로 평가되고 있다.
   C2 (통제적인 접근보호) - 이용자들에게 로그인 절차, 보안관련 사항에 대한 감사, 자원분리 등을 통해서 자신의 행위에 대해 책임 추적 할 수 있도록 한다. 또한, 이전 사용자가 다루던 자료를 다음 사용자가 허가없이 취득하게 되는 사건을 막기 위한 제한을 요구하고 있다. RACF2를 탑재한 IBM MVS 운영체제 및 DEC사의 VAX 운영체제 VMS가 이 등급으로 평가되고 있다.
3) 등급 B (강제적인 보호) - 강제적인 접근통제규칙들을 실행시키기 위해서 비밀표시의 무결성을 유지하도록 한다.
   B1 (분류표시에 의한 보안보호) - C2의 모든 요구조건 이외에, 보안정책에 대한 비공식적인 설명, 자료의 등급표시, 지명된 주체와 객체에 대한 의무적인 접근통제 등이 요구된다.
   B2 (구조적인 보호) - 공식적인 보안정책을 문서화하고, 선택적 및 의무적인 접근통제를 전산체계 내에

모든 주체와 객체에 대해서 실행하고, 인증체계를 강화하고, 보호요소와 비보호요소를 구분관리하고, 엄격한 구성관리통제를 실행한다. 이 등급의 주요 개선점이 설계 측면인데, 시스템을 내부적으로 독립적인 모듈들로 구조화시킨다. Honeywell 사의 MULTICS가 이 등급으로 평가되고 있다.

B3 (보안영역) - 객체에 대한 주체의 모든 접근을 조정토록하고, 복잡성을 극소화 시키기 위해서 보안정책을 실행하는데 중요하지 않은 부호(Code)는 없애고, 시스템 회복절차를 마련하고, 외부 침투에 전산체계가 보호될 수 있도록 한다. 즉 설계가 개념적으로 간단하지만, 완벽에 가깝고 자격(capability)의 구현을 지원하는 주체 및 객체 영역이 있어야 한다. 보안에 대한 파괴규모가 아무리 크더라도 추적할 수 있는 강력한 감사기능을 요구한다

4) 등급 A1 (보증설계) - B3 등급과 기능적으로는 동등하지만, 특징은 정형화된 설계 규격서 및 검증기법, 보안기능의 정확한 구현에 대한 높은 신뢰성 등이다.

TCSEC은 비밀성, 무결성, 가용성 중에서 비밀성만을 강조해서 평가하고 있다. 미 연방지침인 FC(Federal Criteria)와 유럽의 정보기술 보안평가기준(ITSEC; Information Technology Security Evaluation Criteria)은 비밀성 뿐만아니라 무결성, 가용성을 포함하는 포괄적인 보안성 평가기준을 수립하고 있다. 또한, TCSEC은 전산시스템 자체를 위한 기준으로서 네트워크 혹은 데이터베이스 시스템에는 적용하기가 어려기 때문에, NIST에서는 1987년에 네트워크에 대해서 TNI(Trusted Network Interpretation)를, 1988년에 데이터베이스 시스템에 대해서 TDI(Trusted Database Interpretation)를 제시했다. 또한, 1993년에는 미 국방부는 정보체계를 총합화시켜서 정보자원의 관리능력을 증진시키기 위해서 TAFIM(Technical Architecture Framework for Information Management)을 제안했고, 1995년에 TAFIM Ver. 2.0이 나왔다.

4. 결 론

미 국방부의 정보보호 관리체계는 국방정보기반구조(DII)의 정보보호를 위해서 DISA의 CISS에서 국방정보체계 보호프로그램(DISSP; Defense Information System Security Program)에 의해서 수행되고, 이를 위해서 보호 및 인증부서, 훈련부서, 평가부서 등이 있다. (1) 보호 및 인증부서에서는 보안정책을 수립하고, 정보보호 프로그램 및 프로젝트를 감독한다. 정보시스템의 보호 설계 및 평가에 대한 지침을 제공하고, 국방부의 요구사항에 따라서 컴퓨터시스템 및 네트워크에 대한 인증을 수행하고, 표준을 검증한다. (2) 훈련부서에서는 정보전쟁에 대한 교육/훈련/인식 프로그램을 개발 및 훈련시키고, 정보전쟁 경력관리 프로그램을 수립하고, 또한, 정보전쟁의 요구사항에 만족하는 정보보호제품을 식별하여 문서화해서 배포하는 제반 절차를 개발한다. (3) 평가부서에서는 취약성 평가/분석 프로그램을 실행하고, 보안대책의 수립을 위한 자동화 도구의 개발 및 유지보수를 수행한다.

미 국방부의 정보보호정책 중에서 중요한 일반정책, 최소 보안요구사항, 전산체계 평가기준에 대해서 요약하면 다음과 같다.

첫째, 미 국방부 훈령 5200.28-STD에 근거한 미

국방부의 정보보호에 관한 일반정책으로는 (1) 전산체계 내의 비밀정보에 대한 보안대책, (2) 전산체계 내의 비밀아닌 정보에 대한 보안대책, (3) 정보 및 전산자원에 대한 보안대책, (4) 최소 보안요구사항의 만족, (5) 전산제품의 평가제품목록 평가와 TCSEC 인준, (6) 전산보안체계 구현을 위한 기한과 지정된 인준기관의 승인, (7) 전산기 중심의 보안기능의 구현이 불가능한 경우, 기타 보안대책의 수립, (8) 전산통신망 환경에서의 보안대책 책임규정, (9) 전산체계 수명주기상의 보안정책 구현, (10) 외국인의 전산체계 접근통제, (11) 중요한 정보의 처리 등이 있다.

둘째, TCSEC에 근거한 미 국방부의 전산체계 평가기준으로서 접근제어방법 요구사항으로는 (1) 정책, (2) 표시, (3) 신분확인, (4) 책임추적, (5) 보증, (6) 지속적 보호 등의 있고, 분류기준으로는 등급 D, C1, C2, B1, B2, B3, A1 등이 있다.

최근 미 국방부의 정보보호 관리체계 및 정책의 방향은 정보보호 관점에서 정보생존(information survivalbility) 관점으로 변화함에 따라, 정보보호에 실패해서 침입자의 공격이 성공했을 때 조차도 중요한 기능을 연속적으로 유지시키는 정보체계를 구축하려는 새로운 파라다임이 시작되고 있다. 정보에 대한 국방력의 의존도가 날로 증가됨에 따라, 정보보호(앞으로는 정보생존)에 대한 관리체계 및 정책의 중요성을 아무리 강조해도 지나치지 않게 될 것이다.

참고문헌

[1] Kowalski, Stewart, "Cybernetic Anaysis of National Computer Security," Jounal of Computers & Security, Vol.10, 1991, pp.217-227.

[2] _____ , "Cybernetic Anaysis of the 12th U.S. National Computer Security Conference," Jounal of Computers & Security, Vol.10, 1991, pp.228-235.

[3] U.S. Department of Defence, DoD 5200-28(D), Mar. 21, 1988.

[4] U.S. Department of Commerce, National Bureau of Standards, FIPS PUB 73; Guidelines for Security of Computer Applications, Jun. 30, 1980.

[5] U.S. Office of Management and Budget, OMB Circular A-130; Management of Federal Information Resources, Feb. 8, 1996.

[6] U.S. White House, Executive Order 12355, Apr. 1, 1982.

[7] beta.missilab.com:9000/

[8] csrc.ncsl.nist.gov/

[9] www.arpa.mil/

[10] www.disa.mil/

[11] www.ito.darpa.mil/

[12] www.jump.net/~snapp/papers/report.html

[13] www.les.mil/

김 기 윤

1976년 고려대학교 공과대학 토목/환경공학 (학사)
1979년 고려대학교 경영대학원 (석사)
1985년 고려대학교 경영학과 (박사)

1980년-현재 광운대학교 경영학과 교수
관심분야 : 정보시스템 보안/위험관리

나 관 식

1985년 광운대학교 경영학과 (학사)
1987년 광운대학교 경영학과 (석사)
1992년 광운대학교 경영학과 (박사)

1992년-1995년 경민전문대학 사무자동화과 전임강사
1996년-현재 서원대학교 경영정보학과 전임강사
관심분야 : 정보시스템 보안/위험관리