군사연구총서 40

정보전과 대응전략

김제영 신장균 김정헌

육군사관학교
화랑대연구소

발 간 사

컴퓨터와 네트워크 기술의 비약적인 발달은 개인, 기업, 정부 업무의 컴퓨터 의존도를 증대시키는 결과를 가져왔습니다. 이제 데이터의 보관 및 처리, 정보의 획득 및 교환에서 컴퓨터와 정보시스템의 역할은 핵심적인 요소입니다.

그러나 이의 역기능적인 측면 또한 관심을 가져야할 부분입니다. 컴퓨터 바이러스의 유포, 해킹, 사이버테러 등에 의한 국가 기반 구조의 침해 위협 등은 경계의 대상입니다. 정보통신, 전력, 급수, 금융체계 등 핵심적인 국가 기반 구조가 기능을 발휘하지 못하거나, 파괴된다면 안보와 경제에 치명적인 영향을 미치게 될 것입니다. 또한 국가 방위의 많은 부분이 점차 정보기술을 기반으로 하여 발전해 감에 따라 정보 보증에 대한 인식을 새롭게 해야 할 때입니다.

정보화 시대의 전쟁 양상은 적의 핵심기반체계를 공격하여 사상자의 수를 줄이면서 적의 전쟁 수행 능력을 마비시키는 개념으로의 변화가 예상됩니다. 미래의 전쟁은 정보전이 될 것이 명약관화(明若觀火)한 바, 각 국은 정보전에 대한 전략 수립 및 기술 개발에 노력을 집중하고 있습니다. 적에 비해 정보우위를 유지함으로써 아군의 정보활동을 원활하게 수행하고, 적의 정보활동을 역이용하거나, 거부할 수 있는 정보통신 기반구조, 컴퓨터 기술의 확장, 조직 및 전문인력의 양성은 정보작전을 위한 필수적인 요소입니다.

이런 맥락에서 볼 때 육군사관학교에서 실시하는 컴퓨터 교육은 미래전을 대비하는 사관생도들에게 정보전의 중요성을 인식하게 하고, 정보전 수행의 잠재적 능력을 배양하는 데 크게 도움이 되리라고 생각합니다.

정보전을 중심으로 미래전 양상에 대한 분석과 정보보안 대책, 정보보안 관리 모델, 암호와 침입탐지 시스템에 관해 체계적으로 정리하고, 정보전의 대응 전략을 제시한 이 책이 미래 전장 환경을 이해하는 데 많은 도움을 줄 것으로 기대하며, 우리 군의 발전에도 크게 기여하리라 확신합니다.

사관생도 교육의 바쁜 시간속에서도 '정보전과 대응전략'이라는 훌륭한 저술을 완성한 김제영, 신장균, 김정헌 교수와 화랑대연구소 관계관 여러분의 노고에 격려와 치하를 보내는 바입니다.

2002년 7월

육군사관학교장 **박 준 근**

목 차

제1장 정보전의 개념

정보화시대의 전쟁 양상은 종전의 대량 소모전에서 적의 핵심 기반체계를 공격, 파괴, 마비시킴으로써 사사상자를 최소화하면서 적의 전쟁 수행체계를 마비시키는 개념으로 변화가 예상되며, 미래전은 정보 기능과 체계가 통합된 정보작전(Information Operations) 중심의 정보전(IW; Information Warfare)이 될 것이다. 정보전에 대한 전략 수립 및 기술개발 노력은 세계 여러 나라에서 추진되고 있으나 미국을 제외한 대부분의 국가는 초보적인 단계를 벗어나지 못하고 있으며, 특히 정보기반구조의 가용성, 신뢰성, 지속성 등을 보장하는 정보보증 전략 및 기술개발은 매우 미흡한 실정이다. 미국 국방부의 정보전 대응 전략은 정보의 비밀성과 무결성을 강조하는 전통적인 정보보안(INFOSEC) 계획에서 국가의 주요 정보기반 체계를 보호하는 주요 기반구조 보호(CIP) 계획으로, 다시 주요 기반구조 보호 계획에서 정보 기반구조를 운영 및 통제하는 정보시스템에 대한 침해/공격에 대한 보호와 신뢰성 보장과 정보의 가용성을 보장하는 개념인 정보보증(IA) 계획으로 발전하고 있다.

1.1 정보전(IW)의 정의

정보전은 전쟁 목표를 달성, 진척시키기 위하여 전시 및 평시에 수행하는 정보작전이며 정보작전은 정보 및 정보시스템을 보호하는 동시에 적의 정보 및 정보시스템에 부정적인 영향력을 행사하기 위하여 수행되는 활동으로 정의할 수 있다. 미국 합참은 정보전이란 '정보우위를 확보하기 위하여 적이 보유 및 수행하고 있는 정보, 정보 처리, 정보 체계, 컴퓨터 기반의 네트워크에 부정적인 영

향을 미치고, 아군이 보유 및 수행하고 있는 정보, 정보 처리, 정보 체계, 컴퓨터 기반의 네트워크을 보호하는 행위'라고 정의하고 있다. 여기서 정보우위(Information Superiority)는 아군의 정보활동인 정보의 계속적인 수집, 처리, 생산, 전파하는 흐름을 원활히 수행하고, 적의 정보 활동을 이용하거나 거부하는 능력이며, 정보체계는 정보를 수집, 처리, 저장, 전송, 생산, 유포하는 정보활동을 수행하는 정보통신 기반구조, 컴퓨터, 조직 및 인력 등의 구성요소로 되어 있는 시스템을 말한다. 또한 미국의 DISA(Defense Information Systems Agency)는 정보전의 정의를 '국가의 군사전략에 따라서 적의 정보와 정보시스템에 영향을 주는 동시에, 자국의 정보와 정보시스템은 보호함으로써 정보우위를 차지하기 위한 행위'로 규정하고 정보전을 방어적 정보전(Defensive Information Warfare)과 공격적 정보전(Offensive Information Warfare)으로 구분하고 있다. 방어적 정보전은 아군의 정보나 정보 시스템에 대한 공격으로부터 보호하는 것으로 증가되는 공격 가능성, 감소되는 방어 가능성, 정보의 비밀성과 무결성 파괴에 대한 효율적인 대응을 강조하고 있는데 방어 비용이 해당 정보 자원의 손실에 의한 피해 비용보다 작아야 한다는 경제적 논리를 포함하고 있다. 공격적 정보전은 적군의 정보나 정보 시스템에 대한 공격으로 목표가 되는 정보나 정보 시스템의 가치를 공격자 측면에서는 향상시키고 방어자 측면에서는 감소시키는 것을 의미한다. 즉, 공격자는 해당 정보를 얻음으로써 원하는 정보 가치를 획득하거나, 적의 정보시스템 파괴 또는 마비로 인해 상대적인 정보 가치를 높이는 것이다.

한편 미국 국방대학교의 마틴 리비키(M. C. Libicki)교수는 정보전의 특성을 군사부분뿐만 아니라 민간부분까지 포함하여 정보와 정보기술이 적용될 수 있는 모든 종류의 전쟁 양상을 식별하였으며, 정보전의 범위를 지휘통제전(Command & Control Warfare), 심리전(Psychological Operations), 해커전(Hacker Warfare), 경제

정보전(Economic Information Warfare), 사이버전(Cyber Warfare)으로 분류하였다. 지휘통제전은 전쟁 지휘 및 통제 체계에 관련된 정보 보안 활동으로 가장 중요한 현대 정보전의 요소이고, 첩보기반 정보전은 전통적인 군사정보전의 구성요소이며, 전자전은 군사 전자장비 운영을 특성화한 정보전으로 일반적으로 전자기 스펙트럼에 대한 보호 및 억제와 관련 있다. 한편 심리전은 정보전의 인간 측면을 포함하고 있으며, 해커전은 컴퓨터 해커에 의해 아군의 정보를 보호하고 적군의 정보와 정보체계를 무력화시키기 위한 현대 정보전이고, 경제 정보전은 주식 및 금융 시장을 마비시키고 교란하는 등의 경제적 측면이며, 사이버전은 현재 실용화되어 있거나 또는 가상적인 정보전의 모든 요소를 포함하는 현대 정보전의 핵심 부분으로 넓은 의미로는 위에서 언급한 각종 형태의 정보전을 모두 포함하고 있다. 이와 같이 미래전의 핵심은 정보작전에 기반을 둔 정보전이 될 것이며, 특히 사이버 공간상에서 주요한 전략적 또는 전술적인 정보시스템을 마비, 파괴시킴으로써 전쟁 수행 능력을 무력화하는 사이버전이 정보전의 주축이 될 것이다.

정보전은 정보와 정보체계가 공격과 방어의 대상이 되기 때문에 전통적인 개념과는 다른 새로운 전쟁 특성을 갖고 있다. 첫째로, 정보전은 전통적인 전쟁 경계가 불분명해진다는 점으로 사이버 공간에서는 누가 공격하고 있는지, 어디서 공격하고 있는지, 누가 공격을 당하고 있는지 등의 식별이 어렵기 때문에 시간적 공간적 경계가 없어짐으로 사이버 공간을 통해 접근할 수 있는 곳이면 어디든지 전장이 될 수 있고 전쟁의 시기도 무의미하다. 둘째로, 전쟁 기만이 매우 용이하다는 점으로 사이버 공간에서는 디지털 기술의 발달로 사실 정보에 대한 조작을 쉽게 할 수 있으며 적은 비용과 노력으로 빈번하게 조작할 수도 있다. 셋째로, 정보전의 수준이 범죄 수준인지, 테러 수준인지, 전쟁 수준인지를 구별하기가 어렵다는 점으로 정보전에서는 정보 공격을 사고나 실수, 고장, 장난, 범죄 등

과 구별하기 어렵기 때문에 적절한 공격 경보시스템이나, 공격 평가 방법이 명확하지 않다. 넷째로, 정보전 수행 비용이 매우 저렴하다는 점으로 정보전은 고도의 정보기술에 대한 전문 지식만 필요한 전쟁이므로, 정보전 공격 및 방어 무기 개발이 전통적인 무기 개발에 비해 매우 경제적이다. 이와 같이 정보전은 적을 살상하지 않고 무형의 정보를 대상으로 하여 적의 전력을 무력화함으로써 적을 제압하는 전쟁 특성을 갖고 있다.

현재 정보전에 사용되는 정보 무기에는 EMP/T 폭탄, 컴퓨터 바이러스, 트로이 목마, 네트워크 웜, 컴퓨터 침입 등이 있다. EMP/T 폭탄(Electromagnetic Pulse Transformer Bomb)은 강력한 전자기 에너지를 방출하여 공격 목표의 기능을 마비시키거나 기능을 상실하게 하는 것으로 목표가 되는 컴퓨터나 네트워크 등의 정보 시스템에 대한 서비스 거부 공격을 가능케 하는데, 주요 공격 대상에는 전원 공급 장치, 컴퓨터, 네트워크 장비, 기타 반도체 소자를 포함하고 있는 장비 등이 있다. 컴퓨터 바이러스는 일종의 악성 프로그램으로 다른 프로그램들과 달리 사용자 몰래 자신을 다른 곳에 복사하는 자기 복제 능력을 가지고 있어서 컴퓨터를 느리게 하거나 파일에 손상을 주어 시스템 또는 정보를 사용하지 못하게 하는데, 부트 영역에 감염되는 부트 바이러스와 파일에 감염되는 파일 바이러스, 부트와 파일에 모두 감염되는 부트/파일 바이러스, 그리고 응용 프로그램에서 사용되는 매크로를 통하여 감염되는 매크로 바이러스가 있다. 트로이 목마(Trojan Horse)프로그램이란 자기 복사 능력은 없이 고의적인 부작용만 가지고 있는 프로그램을 말하며, 네트워크 웜(Worm)은 컴퓨터 네트워크에 자동으로 복제되어 전파되는 악성 프로그램으로 자동 복제 바이러스라고 할 수 있다. 컴퓨터 침입은 정보 시스템을 해킹하여 정보 접근, 정보 조작, 시스템 무력화 등의 정보전 공격을 말하는데 해킹 기법에는 시스템의 환경변수를 이용하거나, 사용자의 패스워드를 크래킹 하거나, 네트워크

프로토콜을 이용하거나, 응용 프로그램의 보안 오류를 이용하는 방법 등이 사용된다.

최근에 미국 국방부는 국방 정보체계의 상용체계 이용비율이 90% 이상으로 국가 핵심기반체계의 민간기술 의존도가 심화되고 국방부 정보체계에 대한 해커 침입 건수가 날로 증가하고 있어 국가 핵심 기반체계 보호에 대한 심각성이 대두되고 있는 정보화 사회의 특성을 분석하고, 미래의 정보전은 과거의 전쟁과는 달리 군사분야의 정보체계뿐만 아니라 민간 분야의 정보체계까지 공격과 방어의 대상이 됨을 분명히 하였다. 따라서 군사적 정보작전의 목표는 단순히 전술적, 작전적인 군사차원의 수준뿐만 아니라 국가의 전략적 수준까지도 포함하고 있으며 전략적 목표는 국가통수기구에 의해 정치, 외교 및 경제적 수단으로 전쟁을 억제하고 대량파괴무기의 개발을 저지하며 국가적인 정보통신 지휘통제체계를 보호하는 것으로 확대되었으며, 이러한 정보작전 목표하의 대상 표적도 종전에 운용되었던 군사작전과 관련된 군사시설이나 무기체계 뿐만 아니라 민간시설까지도 포함하는 광범위한 표적을 대상으로 하고 있다. 이에 따라 미국은 대통령 지시사항(PDD-63; Presidential Decision Directive)으로 국가 정보 기반구조를 보호하고 정보전 대응 능력을 배양하기 위해서 전통적인 정보보안(INFOSEC; Information Security)계획을 국가 차원의 정보보안 계획인 주요 기반구조 보호(CIP; Critical Infrastructure Protection) 계획으로 발전시켰으며 국가 주요 정보 네트워크에 대한 준비와 예방, 침해 탐지와 대응, 강력한 정보 기반구조 구축의 3단계 목표를 설정하였다. 한편 미국 국방부는 1996년부터 정보전 대비 계획으로 주요 기반구조 보호 계획에서 좀더 진보된 개념인 정보보증(IA; Information Assurance) 계획을 설정하고, DARPA(Defense Advanced Research Project Agency)를 통해 정보보안에서 정보의 가용성(Availability)과 정보체계의 생존성(Survivability)을 강조한 정보보증 프로젝트를 강력하

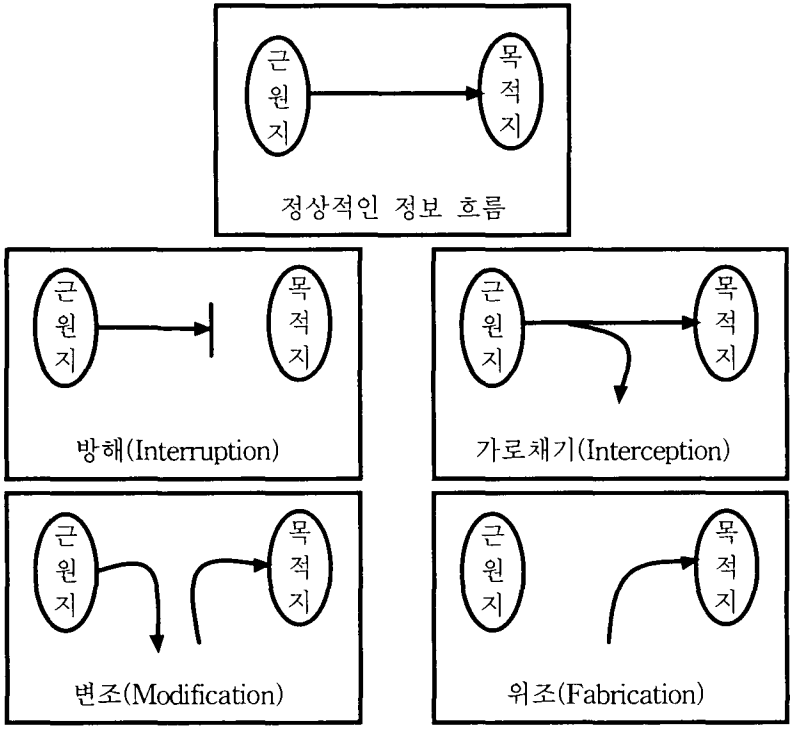
게 추진하고 있다. 정보보증은 정보전에 대한 미국 국방부의 인식이 변화하면서 대두된 개념으로 미국 국방부의 정보전 대응 전략이 정보보안(INFOSEC) 계획에서 주요 기반구조 보호(CIP) 계획으로, 다시 주요 기반구조 보호(CIP) 계획에서 정보보증(IA) 계획으로 변화하고 있음을 의미하며, 정보 기반구조를 운영 및 통제하는 정보 시스템에 대한 침해에 대한 보호와 신뢰성 보장과 정보의 가용성을 보장하는 개념으로 발전하고 있다.

1.2 정보보안(INFOSEC)

정보보안(INFOSEC; Information Security)은 '정보의 수집, 가공, 저장, 검색, 송신 중에 정보의 훼손, 변조, 유출을 방지하기 위한 관리적, 기술적 수단을 강구하는 것'(정보화촉진기본법 제2조)이라고 정의할 수 있다. 정보통신시스템에 의하여 전자적으로 처리되는 정보량이 증가함에 따라 주요 정보통신시스템에 대한 사회 전반의 의존도가 이에 상응하여 증대하고 있는 정보화 사회에서 정보보안의 필요성은 첫째로, 주요 정보통신시스템의 안전 운영에 문제가 발생할 경우 사회의 주요 기능이 마비되어 막대한 손실 및 혼란을 초래하기 때문에 사회 각 분야에서 구축 운영되는 정보통신시스템의 안정성을 확보해야 하며, 둘째로, 개방형 정보통신망은 사용이 편리하고 운영비용이 저렴한 장점이 있으나 정보시스템에 대한 비인가자의 접근이 용이하므로 비인가자에 의한 시스템 접근 및 사용 또는 파괴, 자료의 위조 및 변조 등의 보안 위협에 대한 대응 수단 확보가 필요하며, 셋째로, 정보통신시스템을 활용한 새로운 응용 서비스의 신뢰성 및 안정성을 확보하기 위해서는 사용자 식별 및 인증, 비밀보호 등의 응용 서비스 보안 대책이 필수적인 점을 들 수 있다.

일반적으로 정보보안에 대한 체계적인 접근 방법에는 보안 공격(Security Attack)을 분석하고, 보안 서비스(Security Service)를

정의하고 이를 구현할 보안 기법(Security Mechanism)을 구현하는 것이다. 보안 공격은 조직의 정보 보호를 저해하는 위협 행위로서, 정보 출처로부터 정보 목적지로 이동하는 정상적인 정보 흐름을 저해하는 공격에는 방해(Interruption), 가로채기(Interception), 변조(Modification), 위조(Fabrication) 등이 있다.



〔그림 1.1〕 정보 흐름과 보안 위협

방해는 불필요한 다량의 정보를 특정 시스템에 고의로 송신하거나, 통신회선을 절단하여 정보통신시스템의 장애를 유발하게 하거나, 시스템의 오작동을 유발하게 하는 등의 위협으로 정상적인 작동을 저

해하는 행위로서 정보의 가용성에 대한 공격이다. 가로채기는 정보 통신시스템을 통하여 전송되는 통신 내용을 불법적으로 가로채어 정보를 획득하는 행위로서 정보의 비밀성에 대한 공격이다. 변조와 위조는 타인에게 고의로 피해를 입히거나 자신의 이익을 위해 정보 통신시스템에 의하여 보관 또는 처리되는 정보의 내용을 부당하게 변경하거나 조작하는 행위로서 정보의 무결성에 대한 공격이다. 이 외에도 정당하게 처리된 정보에 대한 부인(denial) 위협로서 통신 메시지를 송신한 후 고의로 그 사실을 또는 내용을 부정하는 행위인 송신 부인과 통신 메시지를 수신한 후 고의로 그 사실을 또는 내용을 부정하는 행위인 수신 부인이 있다.

이러한 보안 위협은 수동적인 공격과 능동적인 공격으로 분류하기도 하는데 수동적인 공격이란 가로채기 위협으로 전송 정보에 대한 도청이나 감시를 말하며, 능동적 공격은 방해, 위변조 위협으로 정보의 불법 변조나 거짓 정보의 생성을 말한다. 수동적인 공격에는 정보 내용 공개와 트래픽 분석의 유형이 있는데 정보 내용 공개는 e-메일 메시지, 음성 통화, 전송 파일 등에 포함되어 있는 전송 내용을 공격자가 탐지하지 못하도록 하는 것이고, 트래픽 분석은 공격자가 정보 내용은 탐지하지 못하더라도 통신자의 장소와 실체, 메시지 교환 횟수와 길이 등의 트래픽 정보를 알아내는 위협이다. 이러한 소극적인 공격은 정보를 변경하지 않기 때문에 탐지하기가 매우 어렵지만 예방은 가능하므로 공격의 발견보다 예방을 더욱 강조하게 된다. 한편 정보의 위변조를 주로 하는 적극적 공격에는 신분 위장, 재전송, 불법 수정, 서비스 부인 등이 있다. 신분 위장(masquerade)은 하나의 개체가 다른 개체의 행세를 하는 것으로 예를 들어 사용자 인증 순위를 알아내어 정당한 진행 순서대로 진행한 후 그 순서대로 재전송하여 어떤 소수의 인증된 개체가 상위의 추가 특권을 가진 개체로 행세하는 것을 들 수 있다. 재전송(replay)은 특정한 정보를 수동적으로 획득한 후 다시 전송함으로써

비인가된 결과를 얻는 것을 말한다. 불법 수정(modification)은 단순히 정보의 일부를 고치거나 메시지 전송을 지연하고 순서를 변경함으로써 불법적인 결과를 얻는 것이다. 끝으로 서비스 부인(denial of service)는 정보통신시스템이 정상적으로 작동하지 못하게 방해하거나 정지시키는 위협으로 예를 들어 어느 개체가 특정한 시스템으로 향하는 메시지를 억류하는 경우나, 메시지의 과다 전송으로 네트워크를 무력화시키는 경우가 있다. 이러한 적극적인 공격은 소극적인 공격과는 달리 모든 정보통신 장비와 네트워크를 물리적으로 완벽하게 보호해야하기 때문에 완전한 예방은 어렵고 공격을 실시간 또는 근접시간에 탐지해 내고 공격 피해를 빠르게 복구하는데 초점을 두고 있다.

보안 서비스는 정보 및 정보시스템에 대한 보안을 강화하기 위하여 보안 체계가 제공하는 기능적인 서비스로서 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 부인봉쇄(Non-repudiation) 등이 있다. 인증은 정보의 송수신자 또는 정보시스템 이용자의 신원을 식별하여 거짓 사용자가 아님을 확인하는 서비스로서 정보통신의 경우에는 정보통신 당사자가 서로 상대방의 실체를 확인하여 시스템 및 사용자에 대한 신뢰성을 갖도록 보증해야 한다. 기밀성은 전송 또는 보관 중인 정보를 비인가자가 부정한 방법으로 획득하더라도 그 내용을 알 수 없도록 보호하는 서비스로서 소극적인 보안 공격으로부터 정보를 보호하는 것이다. 기밀성의 정보보호에는 송수신자 사이의 전송 정보를 일정 기간 동안 보호하는 것과 전송 정보의 출처와 목적지, 횟수, 길이, 송수신 시각 등의 통신 트래픽 특성을 공격자로부터 보호하는 트래픽 흐름정보 보호가 있다. 무결성은 전송 또는 보관 중인 정보를 인가되지 않은 방법으로 변조 또는 위조할 수 없도록 보호하는 서비스로서 정보 및 정보시스템이 인가된 사용자에 의해서만 수정될 수 있도록 통제하는 것으로 수정 기능에는 쓰기, 변경, 상태 변경, 삭제,

생성 및 전송 지연 그리고 재전송 등이 포함된다. 정보통신 환경에서의 무결성 서비스는 연결형 무결성 서비스(Connection-oriented Integrity Service)와 비연결형 무결성 서비스(Connectionless Integrity Service)로 구분되는데 연결형 서비스는 메시지 스트림을 대상으로 송신 메시지가 복사, 추가, 수정, 순서 변경 또는 재전송되지 않고 원래 송신한 상태 그대로 수신됐음을 보장하는 것으로 메시지 훼손에 대한 보호 서비스도 포함한다. 한편 비연결형 서비스는 정보통신 환경에 관계없이 단일 메시지를 대상으로 하여 메시지의 불법 변경으로부터 보호하는 것이다. 무결성 서비스는 적극적인 보안 공격에 대한 보안 서비스이므로 위협 예방보다는 공격 발견에 초점을 둔다. 무결성에 대한 침해가 발견되었을 때 서비스는 침해 사항을 시스템에 보고하게 되며 소프트웨어에 의하여 정보의 무결성 상실을 자동으로 복구하는 기능을 포함할 수도 있다. 가용성은 인가된 사용자가 필요로 할 때 정보 자원을 이용할 수 있도록 하는 서비스로서 다양한 공격 형태에 대한 보안 서비스가 필요하다. 어떤 공격은 인증이나 암호화와 같은 기법에 의해 보호될 수 있으나 또 다른 공격은 가용성의 손실을 사전에 예방하거나 피해로부터 복구하는 보안 기법을 필요로 한다. 부인 봉쇄는 사용자가 정보통신시스템을 통하여 정보를 송수신하거나 처리한 사실을 부정할 수 없게 부인을 방지하는 서비스로서 송신자 부인 봉쇄와 수신자 부인 봉쇄가 있는데 송신자 부인 봉쇄는 메시지가 송신되었을 때 수신자는 그 메시지가 실제로 송신자에 의해 송신되었음을 확인할 수 있어야 하며, 수신자 부인 봉쇄는 메시지가 수신되었을 때는 송신자는 그 메시지가 실제로 수신자에 의해 수신되었음을 확인할 수 있어야 한다.

보안 기법은 보안 서비스를 구현할 수 있는 정보 기술로서 엑세스 제어 기술, 암호 기술, 인증 및 서명 기술, 네트워크 보호 기술, 보안 기능 평가 기술 등이 있다. 엑세스 제어는 정보시스템내의 정

보를 누구에 의하여 또 어떻게 접근될 수 있는가를 통제하는 기술인데 임의적 엑세스 제어(DAC; Discretionary Access Control)와 강제적 엑세스 제어(MAC; Mandatory Access Control)가 있다. 임의적 엑세스 제어는 정보를 사용하려는 주체의 신원에 근거하여 정보자원인 객체에 대한 접근을 통제하는 것으로 ACL(Access Control List), 능력 리스트(Capability List), 열쇠/키 메카니즘 등이 있으며, 강제적 엑세스 제어는 정보자원인 객체에 비밀등급과 이 객체에 대해 사용자인 주체가 갖고 있는 비밀인가에 근거하여 접근을 강제적으로 통제하는 기법으로 판독(read)의 경우에는 주체의 비밀인가가 객체의 비밀등급보다 크거나 같아야 하고 기록(write)의 경우에는 주체의 비밀인가가 객체의 비밀 등급보다 낮거나 같아야 한다는 보안규칙에 따라 강제적으로 접근을 통제하게 된다. 암호기술은 정보의 내용을 의도된 사용자 외에는 알지 못하도록 정보를 변형하는 기법으로 암호 키와 복호 키의 어느 한 쪽으로부터 다른 쪽을 쉽게 구할 수 있는 대칭 암호시스템과 쉽게 구할 수 없는 비대칭 암호시스템이 있다. 대칭 암호시스템은 관용 암호시스템(Conventional Cryptosystem)이라고 하는데 미국의 DES, 유럽의 IDEA 등의 알고리즘이 있으며, 한편 비대칭 암호시스템은 공개키 암호시스템(Public Key Cryptosystem)이라고 하며 대표적인 알고리즘에는 RSA가 있다. 인증은 정보 자원을 사용하려는 주체의 신원을 확인하는 기술로서 패스워드와 같은 기본적인 방법과 사용자의 신원에 기반한 디지털 서명 인증 방법 그리고 키 서버를 이용하여 네트워크의 통합인증을 수행하는 커버로스(Kerberos) 등이 있는데 현재는 공개키 암호 알고리즘인 RSA를 이용한 서명 및 인증 기법이 사실상의 산업 표준으로 널리 사용되고 있다. 네트워크 보호 기술에는 침입차단시스템(Firewall)과 침입탐지시스템(Intrusion Detection System) 등이 있는데 침입차단시스템은 접속을 요청한 단말기의 네트워크 주소에 사용하여 접속 여부를 결정하는 시스템

으로부터 사용자 인증 및 접속, 암호화 기능 등이 추가된 일반적인 시스템까지 있으며, 침입탐지시스템은 정보시스템에 대한 엑세스를 기존의 해킹 수법과 비교하거나 사용자의 행위를 감시하여 통계적인 추론 방법으로 또는 인공지능 분야의 시스템 사용 규칙 기반의 전문가 시스템을 활용하여 침입을 실시간으로 경보할 수 있는 시스템이다. 보안 기능 평가 기술에는 상용 보안 제품의 보안 기능과 보증성을 평가할 수 있는 보안평가 기준과 평가 방법론이 개발되고 있는데 1985년 미국이 정보시스템 신뢰성 평가 기준인 TCSEC (Trusted Computer System Evaluation Criteria)을 제정한 이래 1991년 영국, 프랑스, 독일, 네덜란드가 정보기술 보안 평가 기준인 ITSEC(Information Technology Security Evaluation Criteria)를 제정하였으며 1997년부터 미국, 캐나다, 영국, 프랑스, 독일, 네덜란드가 공동으로 국제 공통 평가기준인 CC(Common Criteria)를 제정하고 있다. 이와 같이 정보보호 기술을 일반 사용자가 신뢰하며 안전하게 사용할 수 있도록 보증하는 정보보호시스템의 성능과 신뢰도에 대한 평가의 중요성을 인식한 선진국에서는 정보보호시스템의 성능과 신뢰도를 평가하기 위하여 국제 환경에 맞는 평가 기준을 제정하여 시행하고 있다. 국내에서는 정보화촉진기본법 제15조를 근거로 정보통신부에서 정보통신망 침입차단시스템과 침입탐지시스템의 평가기준 및 평가지침서를 고시하였으며 한국정보보호진흥원에서 1998년부터 침입차단시스템에 대한 평가제도를 시행하고 있으며, 2000년부터는 침입탐지시스템 에 대한 평가를 시행하고 있다.

1.3 기반구조 보호(CIP)

주요 기반구조는 그 기능을 발휘하지 못하거나 파괴될 경우 자국의 안보와 경제에 치명적인 영향을 미칠 수 있는 핵심적인 기반구조를 말하며 여기에는 정보통신 체계, 전력 체계, 급수 체계, 금

융 체계, 긴급 상황 체계 등이 포함된다. 미국은 2000년에 국가 차원에서 정보보안을 추진하기 위하여 대통령 지시사항(PDD-63)으로 정보기반 구조의 취약성을 제거하기 위한 주요 기반구조 보호(CIP; Critical Infrastructure Protection) 계획을 수립하여 2003년까지 국가 정보기반 구조의 보호 능력을 확보를 목표로 세부 프로그램을 추진하고 있다. 주요 기반구조 보호는 크게 3단계 목표로 구성되어 있는데 1단계 목표는 준비 및 예방(Prepare and Prevent)이고 2단계 목표는 탐지 및 대응(Detect and Respond)이며 3단계 목표는 강력한 기반 구축(Build Strong Foundations)이다. 1단계 목표인 준비 및 예방은 보호 대상을 파악하고 취약성을 평가하는 단계로 주요 네트워크 자산간의 상호 의존성과 취약성을 식별하는데 필요한 방법을 개발하고 실질적인 취약성 제거 프로그램을 개발하며 예산의 투자 우선 순위를 결정하는 단계이다. 2단계 목표인 탐지 및 대응에는 공격과 침입 탐지, 첩보 수집 능력 확보, 경보 및 정보 공유, 그리고 대응, 재구성 및 복구 능력 확보가 있는데 침입탐지 분야로는 고기능 방화벽, 침입탐지시스템, 비정상적인 행위 식별기, 악성코드 스캐너를 이용하여 다층 계층으로 보호하고 공격을 탐지하며, 첩보 수집 능력 확보 분야에는 국방부, FBI, NSA (National Security Agency) 등의 연방기관이 공동으로 공격 시점, 공격 범위 공격 근원지 등을 분석한다. 경보 및 정보 공유 분야에서는 공격 경보와 취약성 정보를 공유할 수 있는 시스템을 구축하는 것으로 정부와 민간 차원의 보안 정보센터와 국방 차원의 보안 정보센터사이의 정보 교류를 포함하고 있다. 그리고 대응, 재구성 및 복구 능력 확보 분야에는 주요 기반구조가 공격을 받는 동안에 다른 공격을 제한하기 위하여 대응, 재구성 및 복구 능력을 확보하는 것이 있다. 끝으로 3단계 강력한 기반 구축에는 연구 개발, 전문가 확보, 홍보, 법률적 지원 등이 있는데 연구 개발 대상에는 침입탐지 모니터, 운영체제 악성 코드를 식별하는 인공지능, 침입자

발견 및 제거, 기반구조 견고성 강화, 기반구조간 상호 의존성 식별 기술, 취약한 핵심 노드 발견 기술 등이 있으며, 전문가 확보 분야에는 정보 기술자가 갖추어야 할 기술 수준 파악, 전문 정보기술센터 설립, 사이버 군(Cyber Corps) 제도, 연방정부 보안 교육과정 설립 등이 포함되어 있다.

구분	목표	프로그램
1단계	준비 및 예방	1. 보호대상과 상호의존성 파악 및 취약성 평가
2단계	탐지 및 대응	2. 공격 및 침입 탐지
		3. 첩보/법적 대응 능력 확보
		4. 경보 및 정보 공유
		5. 대응, 재구성 및 복구 능력 확보
3단계	강력한 기반 구축	6. 연구 개발
		7. 전문가 확보
		8. 홍보
		9. 법률적 지원
		10. 개인의 권리 및 사생활 보호

〔표 1.1〕 미국 CIP의 목표와 추진 프로그램

주요 기반구조 보호의 목표를 구현하기 위하여 설정한 열 개의 세부프로그램을 살펴보면 다음과 같다. 첫 번째 프로그램인 보호대상과 상호 의존성 파악 및 취약성 평가는 연방정부 및 민간 영역의 주요 정보 네트워크 자산과 이들 사이의 상호 의존성 및 취약성을 식별하고 실제적인 보안 취약성을 제거할 수 있는 프로그램을 개발하는 것이다. 그 결과 연방정부가 주요 정보자원을 보호하기 위한 파일럿 프레임워크를 개발하고 보안 목록 데이터베이스를 구축하였고 3-5년을 주기로 외부 전문가 그룹에 의해 취약성을

재평가하고 있다.

두 번째 프로그램인 공격 및 침입 탐지는 고기능 방화벽, 침입탐지 모니터, 비정상적 행위 식별기, 기관차원의 관리시스템, 악성코드 스캐너 등을 주요 정보시스템을 다중 계층으로 보호하는 것으로 각 연방 기관에 산재해 있는 침입탐지 모니터를 네트워크로 연결하여 시스템의 비정상적인 행위를 분석하고 탐지하는 기능을 수행하는 것이다. 이 프로그램을 위해 크게 세 개의 침입탐지 네트워크를 구성하였는데 첫 번째 네트워크는 국방 정보시스템을 모니터하여 침입을 탐지하며, 침입이나 공격을 당한 후에 원래 상태로 복원하는 국방 JTF-CND(Joint Task Force-Computer Network Defense)이고, 두 번째 네트워크는 정부기관의 정보시스템을 모니터하여 침입을 탐지하며, 침입이나 공격을 당한 후에 원래 상태로 복원하는 FIDNet(Federal Intrusion Detection Network)이며 세 번째 네트워크는 JTF-CND와 FIDNet를 통합하여 국가 안보를 위협하는 비인가 침입과 공격을 격리하고 억제하며 사후에는 사고 조사와 취약성 평가를 수행하는 NSIRC(National Security Incident Response Center)이다. 이에 따라 미국 국방부는 1999년에 국방부와 육해공군에 설치되어 있는 약 500여 개의 침입탐지시스템을 네트워크로 연결하여 JTF-CND를 구축하였고, 연방정부는 2001년에 중앙집중형 침입탐지 및 대응 시스템을 GSA(General Service Administration)의 FedCIRC(Federal Computer Incident Response Capability)에 설치하고 이를 중심으로 FIDNet를 구축하여 비인가 침입 또는 공격 행위를 실시간으로 분석하고 있다. 각 침입탐지 시스템크에서 탐지하고 분석한 비인가 침입과 공격은 FedCIRC로 통합되어 국가 차원의 정보침해 대응 조치 및 평가를 수행하고 있다.

세 번째 프로그램인 첩보/법적 대응능력 확보는 정보통신시스템의 새로운 위협과 침해에 대응하기 위한 법 집행과 필요한 첩보를 수집하는 활동을 지원하는 것으로 국가 차원의 협의체인 NIPC(National

Infrastructure Protection Center)를 운영한다. NIPC는 FBI, 국방부, NSA, 첩보 기관 등의 연방기관의 전문가로 구성되며, 법 집행, 첩보 및 대첩보(counter-intelligent) 임무 수행에 필요한 권한을 부여받아, 공격 징후를 분석하여 사이버 공격 조기경보를 발령하고 침입과 공격에 대해서는 발발 시각, 근원지, 범위 및 형태, 침입/공격 주체 등을 파악한다.

네 번째 프로그램인 경보 및 정보 공유는 공격/침해 정보 및 경보를 국가차원에서 실시간으로 공유할 수 있는 효율적인 체계를 구축하는 것으로 NIPC를 중심으로 연방기관, 국방부, 주정부 등의 관련 기관이 연계되어 공격/침해 정보를 공유하고 조기경보 발령을 전파한다. 연방기관의 각 침입탐지시스템이 연결된 FIDNet에서 발견한 비정상적인 행위 데이터는 FedCIRC로 통합되어 분석되며, FedCIRC에서 판단된 불법적인 행위와 공격 징후는 NIPC로 보고되며, NIPC가 발령한 국가차원의 공격 조기 경보는 FIDNet을 통해 전파된다. 국방 분야에서는 JTF-CND가 침입/공격 징후를 종합하고 분석하여 NIPC로 보고하고 NIPC가 발령한 국가차원의 공격 조기 경보를 받아 전파한다. 또한 FIDNet와 JTF-CND의 침입탐지시스템간에 침입/공격 관련 데이터를 공유하는 네트워크 연동체계를 구축하며 침해 사고를 정밀하게 분석하고 평가하기 위해 침입/공격 관련 데이터를 NSIRC로 통합하여 분석한다.

다섯 번째 프로그램인 대응, 재구성 및 복구능력 확보는 정보 기반구조가 공격을 받는 동안에 그 공격을 제한하고 시스템 기능을 지속하며 침해 피해를 복구하는 계획을 수립하는 것이다. 공격이 발발하면 대응기관 들인 JTF-CND, FIDNet, FedCIRC, NIPC 등이 함께 공격의 특성 및 내용을 분석하고 NIPC의 주도로 법 집행기관을 통해 다음 절차에 따라 대응한다. 먼저 의심스러운 사용자가 정보 네트워크에 접근하는 것을 차단하고, 네트워크의 운영을 방어상태로 변경하여 예방조치를 취하며, 공격 기술을 제압할 수 있는

보안 소프트웨어 패치를 실행하고, 피해가 예상되는 네트워크 구성 요소를 격리하며, 더욱 악화된 상태에서는 네트워크 운영을 일시적으로 중지시키며, 비상 운영 시스템을 가동하여 정보 네트워크 기능을 지속한다.

여섯 번째 프로그램인 연구 개발은 국가차원의 보안계획을 추진하기 위하여 필요한 연구 개발 요구를 도출하고 각 연구 프로젝트의 연구 개발 우선순위를 설정하고 연구비를 지원하기 위한 것이다. 연구 전략을 수립하고 연구 지원을 수행하고 있는 CICG(Critical Infrastructure Coordination Group)에서 식별한 연구 개발 주제에는 대규모 네트워크에 대한 침입 탐지 모니터 기술, 운영체제에 설치되어 있는 트랩도어인 악성코드를 식별하기 위한 인공지능 기법, 공격이나 침해 발생시 침입자를 발견하고 추적하여 제거하며 공격 피해를 최소화하고 정보 서비스를 지속하기 위한 시스템 복구 기법, 주용 기반구조의 네트워크와 시스템의 신뢰성과 견고성 그리고 생존성을 향상시키기 위한 기술, 공격에 대한 기반구조 대응을 모델화하기 위한 기술, 기반구조간의 상호 의존성을 식별하고 취약한 구성 요소를 발견하기 위한 기술 등이 있다.

일곱 번째 프로그램인 전문가 확보는 국가 차원에서 필요한 정보 보안 전문가의 수와 보유해야할 기술 수준을 판단하고 부족한 전문 인력을 보충하고 현재 보안 인력을 훈련시키는 프로그램을 운영하여 정보 보안 전문가를 확보하는 것이다. 이를 위하여 다음과 같은 교육 프로그램을 통해 정보 보안 전문가 부족 문제를 해결한다.

① 정보 보안 직책 담당자가 갖추어야 할 핵심 능력을 식별하고, 이들에게 필요한 교육 훈련 프로그램 및 수료 후 자격 인증(certification)을 정립한다.

② 정보기술 교육훈련 기관인 CITE(Center for Information

Technology)를 설립하고 정보 보안 교육 프로그램을 개발하여, 현재 보직되어 있는 정보 보안 직책 담당자를 재교육하고 핵심 보안기술을 지속적으로 보유할 수 있게 한다.

③ 차세대 정보 보안 인력을 확보하기 위하여 대학과 대학원에 정보 보안 장학금 제도(SFS; Scholarship for Services)를 신설하고, 이를 위하여 대학과 대학원에 정보 보안 관련 과목의 개설과 정보보안 연구실의 설립을 지원한다. 또한 장학금을 수혜한 학생들은 졸업후 일정기간 동안 연방정부의 정보 보안 부서에 근무하도록 한다.

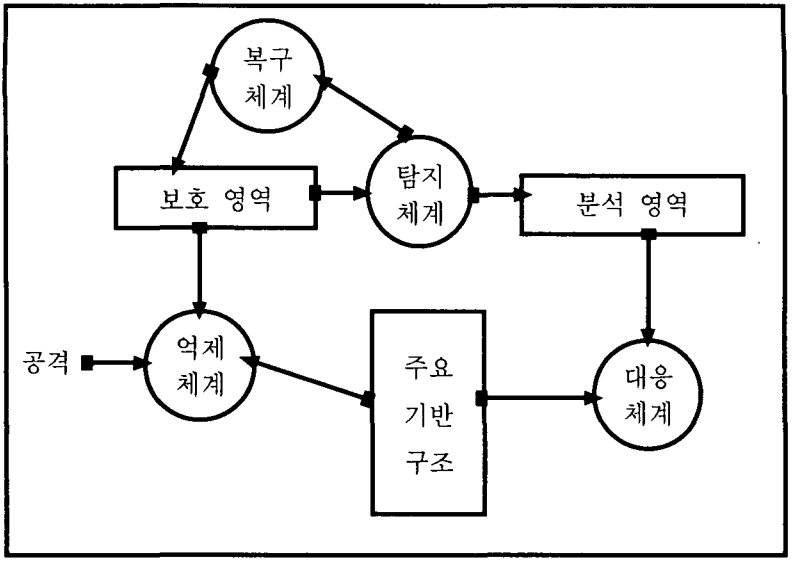
여덟 번째 프로그램인 홍보는 정보보안 사고가 발생하기 전에 사이버 공격에 대한 방어 능력을 향상시키기 위해서는 평상시에 대비하고 보안 활동을 수행해야 한다는 것을 홍보하고 이를 위한 국가의 CIP 정보보안 추진 계획을 다른 민간 조직과 공공 기관에도 홍보한다. 특히 미국 기업과 정보 보안 기술자들간의 연계를 강화하기 위한 주요 기반구조 보호 연계(Partnership for Critical Infrastructure Security) 프로그램을 운영하여 민간과 정부가 함께 국가의 정보보안 수준을 향상시키기 위한 노력을 기울인다.

아홉 번째 프로그램인 법률적 지원은 위에서 제시된 여덟 가지 프로그램들을 지원하기 위한 법적인 기반을 구축하는 것으로 필요한 법률 제정 및 예산 획득을 위하여 의회와 긴밀하게 협력한다.

열 번째 프로그램인 개인의 권리와 사생활 보호는 국가의 CIP 계획의 목표가 국가의 이익과 국민의 자유를 보장하는데 있으므로 개인의 권리와 사생활 보호를 강화시킬 수 있는 체계를 구축하는 것이다. 이를 위하여 대통령 명령으로 1999년에 설립된 국가 기반구조 보장회의(NAIC; National Infrastructure Assurance Council)가 주요 기반구조 보호 계획의 추진이 개인의 자유와 권리, 사생활보호 등에 어떠한 영향을 미치는지를 조사하고 분석한다.

1.4 정보보증(IA)

정보보증(IA; Information Assurance)이란 1996년에 미국 국방부가 작전 지침인 정보작전(DoD Directive S-3600.1, Information Operations)을 제정하고, 기존의 정보전에 대한 인식을 갱신하면서 새로 대두된 정보 보안 개념이다. 미국 국방부에서 정보전이란 개념을 폐지하고 정보보증이란 용어를 사용하게된 배경은 미국의 국가방위가 정보기술을 기반으로 하는 국가의 주요 기반구조에 의존한다는 사실을 인식하였기 때문이다. 즉, 해킹, 사이버테러 등 주요 기반구조의 침해위협을 방지하기 위해서는 주요 기반구조를 소유·운영 및 관리하는 국방부를 비롯한 연방정부, 공공기관 및 산업체의 보호 노력을 통합하고 조정하는데 그 성공의 열쇠가 있다고 인식한 결과이다. 따라서, 정보보증의 의미는 비밀로 분류된 정보 및 정보시스템을 보호하는 정보보안(INFOSEC)이라는 기존의 정보 및 정보시스템 보안보다 광의의 개념으로 기반구조를 구성·운영 및 통제하는 정보와 정보기술에 대한 침해와 공격에 대한 비밀성, 무결성, 인증, 부인 방지 및 가용성을 보장하는 것을 말한다. 이러한 정보보증 추진 계획은 크게 인력 분야, 기술 분야, 운용 분야로 구분되는데 이 분야들은 서로 상호 의존적인 관계를 갖고 있으며 인력 분야에는 교육, 훈련, 인증서, 인력 확보, 신뢰성 등이 포함되고, 기술 분야에는 암호, 침입 탐지, 방화벽, 네트워크 보호 등이 포함되며, 운용 분야에는 계획, 조직, 지휘 및 통제, 구성원간의 협조 등이 포함된다. 한편 주요 기반구조를 보호하기 위한 미국의 정보보증 모델은 그림 1.2와 같이 침해/공격에 대한 억제 체계, 침해/공격에 대한 탐지 체계, 기반구조에서 제공하는 서비스 복구 체계, 그리고 추후의 침입 혹은 위협에 대비하는 대응 체계로 구성된다.



〔그림 1.2〕 정보보증 모델

주요 기반구조를 보호하기 위한 다양한 형태의 정보보호 기술개발 노력이 세계 여러 나라에서 진행되고 있으나 미국을 제외한 대부분의 국가는 초보적인 단계를 벗어나지 못하고 있으며, 특히 기반구조의 가용성, 신뢰성, 지속성 등을 보장하는 정보보증 기술개발은 매우 미흡한 실정이다. 미국 국방부는 DARPA(Defense Advance Research Projects Agency)를 중심으로 전략적 사이버 방어(Strategic Cyber Defense)를 위한 정보보증과 생존성(IA & S; Information Assurance & Survivability) 연구개발 프로그램을 추진하고 있으며, NSA(National Security Agency)를 중심으로 정보보증 포럼을 구성하고 정보보증 기술 프레임워크(IATF; Information Assurance Technical Framework)를 개발하고 있다.

1996년에 DARPA/ITO(Information Technology Office)는 국방부 정보시스템에 대한 외부의 어떤 공격에 대해서도 시스템의 중요 서비

스 및 기능에 대한 최소한의 성능을 지속할 수 있는 정보 생존성에 대한 연구 프로젝트를 추진하였다. 정보 생존성이란 시스템이 공격을 받은 이후에도 중요 서비스 및 기능에 대하여 적절한 성능을 지속시킬 수 있는 시스템의 능력이라고 정의할 수 있는데, 기밀성, 인증, 부인방지 등과 같은 전통적인 보안개념보다는 신뢰성, 가용성, 안전성과 같은 보안특성에 의존하여 공격 피해의 파급 효과를 최소화하고, 시스템이 공격을 받은 이후에도 서비스 및 기능이 중단되지 않고 최소 기능을 유지해야 한다는 특징을 갖고 있다. 미국의 군사 정보 시스템들은 상용통신인 인터넷과 컴퓨터 기반구조에 의존하고 있으며 이들과 상호 연동되어 운영되고 있다. 전 세계적으로 연결된 인터넷은 미국 내에 있는 정보 시스템에 대한 공격이 세계 어느 곳에서든 이루어질 수 있다는 것을 의미한다. 이러한 주요 정보 시스템에 대한 다양한 공격, 정확히 예상할 수 없는 공격에 대하여 주요 정보 시스템이 적절한 기능을 유지할 수 있는 기술을 개발하는 것이 이 프로젝트의 목표이다. 이 목표를 달성하기 위하여 정보 생존성 프로젝트는 다음과 같은 네 가지 연구 분야로 나누어 핵심 기술을 개발하고 있다.

(1) 고신뢰 컴퓨팅 시스템(High Confidence Computing)

고신뢰 컴퓨팅은 기반구조의 주요 구성요소인 정보시스템 운영체제에 보안기능을 첨가한 차세대 운영체제를 개발하는 것이며, 이를 통하여 완전하고 보안성이 강한 방어벽을 만들며, 또한 특수한 침해 대응 환경으로의 변환을 용이하게 하기 위하여 시스템 환경을 재 설정할 수 있는 시스템을 개발한다.

(2) 고신뢰 네트워킹(High Confidence Networking)

고신뢰 네트워킹은 네트워크 서비스의 중단이나 침입과 같은 공격

에 대응하기 위한 강한 침입 차단 기능을 개발하고 현재 그리고 새로운 네트워크 기술에 보호 메커니즘을 추가하기 위한 기술을 개발한다.

(3) 래퍼와 구성(Wrappers and Compostion)

래퍼와 구성은 전통적인 시스템에 대한 공격을 막기 위하여 시스템에 방어벽을 쉽게 추가할 수 있는 래퍼 기술, 정형화 방법 및 구성 기법(Compositional Technique) 등을 개발하는 것으로 이러한 기술을 이용하여 강화된 시스템의 보호능력 및 생존력을 평가할 수 있는 기술도 개발한다.

(4) 대규모 시스템의 생존성(Survivability of Large Scale Systems)

대규모 시스템의 생존성은 침입과 의심스러운 사건에 대하여 신뢰성 있는 탐지를 하고, 기반구조가 탐지된 사건에 대응하며, 침해/공격에 의하여 피해를 입은 시스템들의 중요한 작업에 대하여 자원을 재 할당할 수 있게 한다. 또한 원래의 공격에 대하여 견딜 수 있도록 환경을 재 설정할 수 있는 능력을 갖추도록 시스템을 개발하고 있다.

한편 DARPA도 전략적 사이버 방어를 위한 정보보증 연구개발의 중요성을 인식하고, 연구 개발 대상 분야로 정보보증 과학 및 공학, 사이버 센서 및 활용, 사이버 상황 파악, 사이버 지휘 통제, 방어 메커니즘, 사이버 방어 전략을 설정하였다. DARPA의 기본적인 정보 보증 전략은 위험균형 최적화와 계층적 방어(Layered Defense)이다. 위험균형 최적화는 위험 요소 중 취약성이 심각한 부분부터 점차적으로 보완하여 일정 시간이 경과되면 보호되어야 할 주요

정보에 대하여 전체적으로 향상된 보안성을 갖게 하는 것이고, 계층적 방어는 침입을 단계적으로 즉, 예방, 탐지, 그리고 감내의 단계로 구분하여 방어하는 것이다. 이러한 전략적 사이버 방어를 위해 DARPA는 다음과 같은 여덟 가지의 연구개발 프로그램을 추진하고 있다.

첫 번째 프로그램은 전략적 침입 평가(Strategic Intrusion Assessment) 기술 개발로서 다양한 침입탐지 시스템들과 대응 시스템들을 함께 동작시키고 서로 정보를 공유할 수 있는 공통 침입 탐지 프레임워크(Common Intrusion Detection Framework)를 개발하는 것이다. 사이버 공격은 하나의 침입탐지시스템으로는 탐지하기가 어렵기 때문에 침입 행위를 효율적으로 탐지하고 평가하기 위해서 침입탐지스템이 서로 침입에 대한 정보를 교환할 수 있어야 하며 대응 시스템과도 통합되어 시스템 관리자들이 대응 방법과 복구 방법을 찾을 수 있어야 한다. 공통 침입 탐지 프레임워크는 침입 및 피해에 관련된 정보를 수집하기 위한 센서, 보고된 침입 정보의 타당성과 대응의 필요성을 판단하기 위한 분석 엔진, 그리고 침입에 대응하기 위한 대응 엔진으로 구성된다. 정보 수집 센서는 에이전트 기술을 기반으로 통계적 상관 관계 및 정성적 추론 기법을 사용하여, 수집된 정보를 여과하여 상위 계층에 보고하도록 개발하고 있다. 또한 분석엔진은 자동 패턴 감지, 이벤트 분류 및 상관 관계 분석, 모델기반 추론 등의 기법을 사용하여 공격자의 의도를 추측하고 미래의 행동을 예측한다.

두 번째 프로그램은 침입 감내 시스템(Intrusion Tolerant Systems) 기술 개발로서 침입과 결함이 발생한 상황에서도 데이터와 프로그램의 일관성을 유지하기 위한 기술과 서비스 거부 공격에 대응하는 기술과 높은 시스템 가용성을 유지하는 기술을 개발하는 것이다. 정보의 일관성을 유지하기 위하여 의심스러운 프로그램 코드와 데이터를 사용하기 전에 손상되지 않은 프로그램 코드 및 데이터

구분할 수 있는 메커니즘을 개발하며, 악성 코드가 피해를 입히기 전에 이를 제지하기 위한 모니터도 개발한다. 시스템의 가용성을 유지하기 위해서는 피해가 확산되지 않도록 하는 기술, 하드웨어와 소프트웨어 자원을 재구성하는 기술을 개발하며, 시스템 기능의 선별과 자원 재할당 기술도 개발한다.

세 번째 프로그램은 고장 감내 네트워크(Fault Tolerant Networks) 기술 개발로서 사이버 공격에 대한 고장 감내 능력을 네트워크 수준에서 가지도록 네트워크를 강화하기 위한 고장 감내 생존성 기술, 일관성과 가용성을 보장하도록 하는 서비스 거부 방지 기술, 서비스 거부 공격에 대한 잠재적 취약성을 감소시키는 기술, 그리고 액티브 네트워크 기술을 이용한 공격 대응 메커니즘을 개발한다. 먼저, 고장 감내 생존성 기술 개발은 고장 감내 시스템의 메커니즘을 이용하여 네트워크가 결함을 견디도록 하는 기술을 개발하는 것으로서 가상 자원의 중복 및 복제를 위하여 네트워크를 중첩시키고 관리하는 기술, 생존성있는 서비스를 제공하기 위한 네트워크 분할기술, 네트워크가 공격에 보다 잘 견디도록 네트워크 구조를 강화하는 기술, 네트워크 성능 저하를 감소시키는 기술, 분산 네트워크의 안정화 알고리즘, 고장 감내 네트워크의 파괴 모델 등을 개발한다. 다음으로 서비스 거부 방지 기술 개발은 공격자의 자원 소비를 제한함으로써 서비스 거부 공격을 방지하는 기술을 개발하는 것으로서 중요하지 않은 작업 처리에 의한 자원소모를 제한하는 기술인 시장기반 네트워크 할당 전략과 서비스 거부 공격의 가능성을 최소화하는 통신 프로토콜인 경과기반 프로토콜 기술로 구성된다. 마지막으로, 액티브 네트워크 대응 기술 개발에서는 이전에 개발되었던 액티브 네트워크와 침입탐지 메커니즘을 개선하여 공격 또는 고장의 경우에도 네트워크의 생존성을 보장하는 기술을 개발한다.

네 번째 프로그램은 동적 연립(Dynamic Coalitions) 기술 개발로

서 최소한의 운영을 위한 분산된 제휴 보안 정책을 수립하기 위하여 다차원, 보안 정책 관리, 안전한 그룹 관리, 그리고 연립 기반구조 서비스에 관련된 기술을 개발한다. 먼저, 다차원 보안 정책 관리 기술 개발은 정책 표현 및 정책 기술, 그리고 정책 발견 기술 등을 개발하는 것이다. 특히, 정책 표현 및 번역에 관련된 세부 기술로는 사람이 읽기 쉬운 형태로 표현된 정책을 컴퓨터가 해독할 수 있는 형태로 변경하는 기술, 보안 정책을 광범위하게 표현 할 수 있는 표현 언어 기술, 호스트와 네트워크 보안 정책을 정의하는데 있어서 사용자를 도와줄 수 있는 도구모음 등을 개발한다. 다음으로, 안전한 그룹 관리 기술 개발을 위해, 멤버가 그룹에 합류 또는 탈퇴할 때에도 관리 행위가 수행될 수 있게 하는 기술, 새로 합류한 멤버는 대화 이력에 접근하지 못하게 하는 기술, 재합류하는 멤버에게는 탈퇴 이전에 키를 부여하기 위한 기술, 다른 기관의 사용자들이 동적으로 그룹을 구성하는 경우 사용자와 조직의 보안 정책에 적합한 보안 제어를 수행하는 기술, 연립 내에서의 부인 방지 기술, 그리고 연립 내에서의 감사(auditing) 기술 등을 개발한다. 끝으로 연립기반구조 서비스 기술은 인증서와 인증기관에 관한 것으로서, 인증서의 온라인 확인 기술을 개발하고, 다중 인증서 기반구조에 대비한 다른 인증서 관리, 기반구조간의 상호 인증, 도메인 보안 정책, 주소 매핑 정책, 그리고 인증서 포맷 등도 연구한다.

다섯 번째 프로그램은 정보 보증 기술 개발로서 시스템 보안 관리, 공격 예방, 탐지 및 대응, 그리고 정보보증을 위한 구조와 통합 분야의 기술을 개발하기 위해서, 기존의 다양한 보안 관리를 통합된 환경에서 제공하기 위한 SSD(Security Service Desk)를 개방하고, 방화벽, 감사 기록 등의 다양한 보안 요소를 이용하는 보안 관리를 추상화하고, 이들을 정책 시스템과 연계시킬 수 있는 미들웨어 서비스인 SMART(Security Management and Administration of Remote Trusted Systems)를 개발한다. 예방 기술 개발을 위해

서는 네트워크 DNS(Domain Name Server)의 보안을 강화하여 이름과 주소 매핑을 인증하게 하고, DVPN(Dynamic Virtual Private Network)을 구축한다. 미들웨어 측면에서는 CORBA(Common Object Request Broker Architecture) 보안을 강화하여 CORBA 보안 서버를 구축하고, 역할 기반의 접근 통제 도구를 개발한다. 운영체제 측면에서는 내장 프로세스 개념을 도입하여 신뢰할 수 없는 응용 프로그램은 보안 매니저 프로세스가 실행시키도록 한다. 응용 프로그램 측면에서는 필터링, 모니터링, 암호화 기능을 갖는 래퍼(wrapper)를 사용하여 악성 코드에 대비한다.

여섯 번째 프로그램은 정보 보증 과학/공학 도구(Information Assurance Science & Engineering Tools) 개발로서 정보보증 기술 및 체계의 설계와 평가를 위한 통합된 환경과 도구를 개발하는 것이다. 정보보증 과학 측면에서는 사이버 과학, 정보보증 메트릭, 그리고 정보보증 모델을 개발한다. 먼저, 사이버 과학은 현존하는 정보보증 연구를 분석하여 누락된 영역을 찾아내고, 정보보증 연구를 보완하기 위한 사항을 연구한다. 정보보증 메트릭 개발은 정보보증 설계, 평가, 운영 및 시험에 활용할 메트릭들을 찾고, 이 메트릭들을 적용하기 위한 방법론을 개발하며, 정보보증 모델 개발에서는 논리, 추론, 의사결정 등에 사용하는 수리적 모델을 개발한다. 정보보증 공학에 관련되어서는 정보보증 설계, 정보보증 평가, 벤치마크에 사용하기 위해 정보보증 메트릭, 정보보증 모델, 사이버 과학 등을 적용하기 위한 과학적이고 신뢰성 있는 방법론을 개발하고, 정보보증을 설계 및 평가하기 위한 도구를 개발하며, 정보보증 설계 및 평가를 위한 통합 환경을 구축하기 위한 기술을 개발한다.

일곱 번째 프로그램은 자율적 정보 보증(Autonomic Information Assurance) 기술 개발로서 광범위하게 분산된 환경에서 발생하는 자동화된 사이버 공격에 대응하기 위해서 공격을 중단시키거나 그 피해를 최소화시키는 자동화된 대응 방법을 개발하는 프로그램이다. 개발

할 대상 기술에는 공격에 대하여 효과적으로 대응하기 위한 방법을 빠른 시간 내에 선택하기 위한 기술, 분산되어 있는 재귀적 방어 능력을 결집시킬 수 있는 통제 이론 및 게임 이론에 대한 연구 등이 있다. 또한, 방어 통제 시스템의 프로토타입을 개발하고, 모델링된 시스템, 위협 등에 시나리오를 적용할 수 있도록 확장된 모델을 제안한다. 또한, 운영체제, 방화벽, 응용, 데이터베이스 등의 시스템 요소 별로 적용할 수 있는 대응 방법과 기능을 정립하기 위한 연구도 수행한다.

여덟 번째 프로그램인 사이버 지휘 통제(Cyber Command & Control) 기술 개발은 상위 수준의 의사결정을 지원하기 위한 기술 개발 프로그램으로서 자동화된 공격에 대응하기 위한 사이버 OODA(Observe, Orient, Decide, Act)기술을 개발하는 것이다. 이 프로그램에서는 사람이 공격자의 행동과 목표를 조사하고, 공격자에게 대항하기 위한 가장 효과적인 행동을 결정하고 수행하게 도와주는 기술을 개발하는데, 주요 개발 대상은 상황 인식, 행동양식 개발 및 수행, 그리고 의사소통 및 피해 평가가 있다. 먼저, 상황 인식은 모니터 시스템이 붕괴되었는지, 공격 행동이 탐지되고 있는지, 또는 전략적 공격이 발생하고 있는지 등을 평가하는 평가 기능의 상태와 평가 진도 등의 정보를 취합하는 기술을 개발하는 것이다. 또한, 전략적 공격자가 앞으로 어떠한 행동을 취할 것인지도 결정하기 위한 기술도 개발하며, 공격이 발생되고 있는 상황을 이해하는데 도와주기 위한 시각화 기술도 개발한다. 행동양식 개발 및 수행에서는 현재 어떠한 방어 대책이 있고, 그 대책을 적용할 경우 공격을 얼마나 효과적으로 방어할 수 있으며, 대책 적용이 시스템에 어떠한 영향을 미칠 수 있는지 비교 판단하는 기술을 개발한다. 의사소통 및 피해 평가 기술은 사이버 공격으로 인하여 시스템의 어떠한 기능과 자료가 파손, 변조 또는 훼손당했는지 분석하고, 시스템의 성능과 임무 수행에 전반적으로 어떠한 영향을 미쳤는지 분석하는 기술을 개발한다.

제2장 정보보안 관리

정보보안 문제에는 '정보를 어떻게 통제하여 보호할 것인가'라는 보호 메커니즘의 설계와 구현뿐만 아니라 '설계된 보호 메커니즘을 어느 정도 신뢰할 수 있는가'라는 보안의 평가 및 검증도 중요한 이슈에 포함된다. 정보시스템의 보안평가는 사용자 및 개발자들에게 정보시스템이 갖고 있는 보안 기법에 대한 보편적인 기준을 확립하고 이 기준을 기반으로 시스템이 제공하는 보안기능 및 보증기능의 수준을 검증하는 것이다. 정보시스템의 보안성을 평가하기 위한 보안평가 기준은 1985년에 미국이 국방 표준인 정보시스템 신뢰성 평가 기준(TCSEC:DoD-5200.28-STD)을 제정한 이래, 1990년에 영국, 독일, 프랑스, 네덜란드 등 유럽 4개국이 공동으로 정보기술 보안평가 기준(ITSEC)을 제정하였으며, 이후에 미국, 캐나다 등에서 국가보안기관을 중심으로 자국의 실정에 맞는 정보시스템 보안평가 기준을 제정하여 시행하였다. 미국, 영국 등 선진 6개국은 국가별로 서로 다른 평가기준을 시행할 경우 비용과 시간의 과다 소모, 호환성 결여 등의 문제점이 발생할 수 있음을 인식하고, 1993년부터 국제 표준의 성격을 갖는 평가기준을 개발하기 시작하여 1998년에 국제공통평가기준(CC v2.0)을 제정하였고 현재는 이를 토대로 국제표준기구(ISO/IEC)에서 국제 표준화를 위한 노력을 경주하고 있다. 한편 정보보안 선진국에서는 조직의 보안관리에 대한 중요성을 인식하고 영국의 BSI(British Standard Institute)나 미국의 NIST(National Institute of Science & Technology)와 같은 정보보호 기관에서 국가 차원의 보안 관리 절차 및 방법론을 자체적으로 개발하여 적용하고 있으며, 국제적인 보안관리 표준으로 ISO/IEC JTC1/SC27에서 정보기술 보안관리 지침(GMITS; Guidelines of the Management of IT Security)이 개발되고 있다.

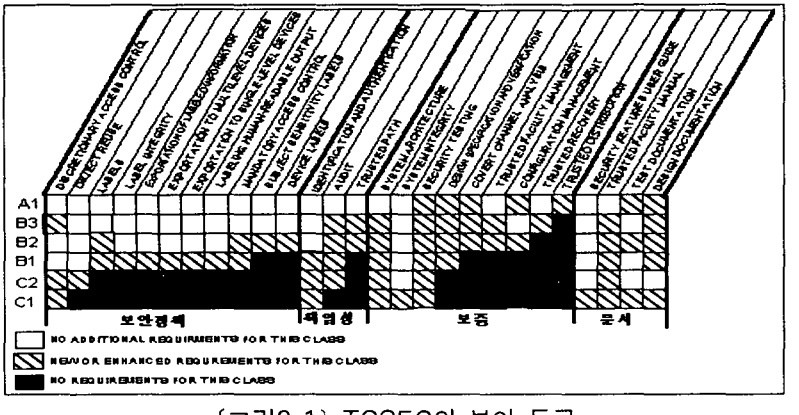
2.1 신뢰성 평가기준(TCSEC)

미국의 NCSC(National Computer Security Center)는 1985년에 안전한 정보시스템을 평가하기 위한 지침서인 TCSEC(Trusted Computer System Evaluation Criteria)를 발간하였다. 신뢰할 수 있는 정보시스템은 인가된 사용자나 사용자 그룹을 식별하고 정보에 대한 읽기, 쓰기, 삭제 등의 엑세스 요구를 통제하는데, 정보보안의 절대적인 보증을 요구하는 것은 비효율적이기 때문에 어떤 종류의 보안 기준들이 정보보안을 평가하는데 적절한가를 식별해야 한다. TCSEC은 정보시스템의 보안을 효과적으로 평가하기 위하여 여섯 개의 기본 요구사항을 정의하고 그 기본 요구사항을 만족시키는 수준에 따라 일곱 가지의 보안평가 등급을 제시하고 있다.

TCSEC의 기본적인 보안 요구사항에는 보안정책(Security Policy), 표시(Marking), 식별(Identification), 기록성(Accountability), 보증(Assurance), 지속적인 보호(Continuous Protection)가 있는데 보안정책, 표시, 식별, 기록성은 정보에 대한 엑세스를 통제하기 위한 요구사항이고, 보증과 지속적인 보호는 신뢰성 있는 정보시스템을 유지하기 위한 요구사항이다. 보안정책 요구사항은 정보시스템에는 명확하고 잘 정의된 보안정책이 존재해야 한다는 것으로 정보시스템에는 정보를 요구하는 주체와 정보 자원인 객체가 식별하고, 주체가 특정 객체에 대한 엑세스 요구를 인가할 것인지를 결정하기 위해 적용할 보안 규칙들의 집합이 있어야 한다. 표시 요구사항은 엑세스 통제를 위한 보안 레이블이 정보 객체와 결합되어야 한다는 것으로 강제적 보안정책 규칙에 따라 시스템에 저장된 정보에 대한 엑세스를 통제하기 위해 모든 객체에 대해 보안등급을 신뢰성 있게 식별하는 레이블을 표시할 수 있어야 하며, 이러한 레이블들은 정보에 대한 엑세스 요구 시에 보안 등급 비교를 위해 사용 가능해야 한다. 식별 요구사항은 모든 주체들이 유일하고 분명하게 식별되어야 한다는 것으로 엑세스 요구 시마다 엑세스하는 주체가 누구인지 식별이

가능해야 하고 이와 관련된 인증 정보는 안전하게 관리되어야 하며 시스템 내에서 보안 관련 행위를 수행하는 모든 작동중인 요소들과 관련이 있어야 한다. 기록성 요구사항은 감사 기록자료가 보안에 영향을 주는 행위가 책임질 수 있는 부문까지 추적될 수 있도록 선별적으로 유지되고 보호되어야 한다는 것으로 정보보호시스템은 감사 기록 내에 보안관련 사건들의 내용을 완벽하게 기록 할 수 있어야 한다. 보증 요구사항은 보안 정책, 표시, 식별, 기록성 등의 보안 요구사항이 시스템에 의해 적용되고 있다는 것을 보증하는 메커니즘이 있어야 한다는 것으로, 독립적인 하드웨어와 소프트웨어 메커니즘으로 존재하여야 하며 그 효율성을 평가할 수 있어야 한다. 지속적인 보호 요구사항은 위의 요구사항을 만족하는 보안 메커니즘은 공격 혹은 불법적인 변경 등으로부터 지속적으로 보호되어야 한다는 것이다.

TCSEC은 위와 같은 보안 요구사항을 만족하기 위하여 보안정책, 책임성, 보증 및 문서에 대한 기능 수준과 보증의 수준에 따라 크게 D분류, C분류, B분류, A분류로 구분하고, 각 분류를 다시 세분하여 그림 2.1과 같이 일곱 가지 보안 등급을 제시하였는데 낮은 보안 등급에서 높은 보안 등급 순으로 나열하면 D(평가 부적합), C1(최저), C2, B1, B2, B3 및 A1(최고) 등급이다.



〔그림2.1〕 TCSEC의 보안 등급

먼저 보안평가의 기본 분류인 D, C, B, A에 대한 분류의 정의를 살펴보면 다음과 같다.

- D분류: 최소 보호(Minimal Protection)
  기본 요구사항이 없는 보안수준으로 평가는 되었지만 상위 평가등급을 위한 요구사항들을 충족시키지 못한 시스템들이 여기에 포함된다.
- C분류: 임의적 보호(Discretionary Protection)
  임의적 보호에는 임의적 엑세스 제어 기능을 제공하며 감사기능을 수행하여 모든 주체들의 동작을 기록 유지하는 기록성을 포함하고 있다. 임의적 엑세스 제어는 주체의 식별에 근거하여 객체에 대한 엑세스 요구를 통제하는 기법으로 한 주체가 다른 주체에게 자신이 갖고 있는 엑세스 권한을 넘겨주는 것이 허용된다.
- B분류: 강제적 보호(Mandatory Protection)
  강제적 보호의 중심은 보안 레이블의 무결성을 유지하고 강제적 엑세스 제어를 수행하는 TCB(Trusted Computing Base) 개념이다. 강제적 엑세스 제어는 객체에 포함된 기밀 수준과 주체에게 부여된 보안인가에 근거하며, 수학적인 보안 모델을 사용하여 보안 정책을 적용함으로써 주체의 객체에 대한 엑세스를 강제로 통제하는 기법이다. 이 분류를 만족하는 정보시스템은 TCB를 기반으로 하는 보안 모델을 기반으로 조회 모니터(reference monitor) 개념이 구현되었다는 것을 제시해야 한다.
- A분류: 증명된 보호(Verified Protection)
  증명된 보호의 특징은 공식적인 보안 검증(formal security verification)으로 시스템의 보안 메커니즘이 모든 기밀 정보를 효과적으로 보호할 수 있는지를 증명하기 위하여 이론적으로 정형화된 검증 기법을 사용한다. 또한 TCB가 정보시스템의 설계와 구현 단계에서 제시된 보안 요구사항을 충족하는지를 증

명하는 확장된 문서가 요구된다.

이러한 분류에서 평가 등급은 다시 D, C1, C2, B1, B2, B3, A1으로 세분된다. 각 등급은 서로 독립적인 것이 아니고 서로 연관되어 있으며 상위 등급은 하위 등급에 보다 많은 보안 요구사항들을 추가시킨 것으로 정의된다. 실제로 이 등급들은 D, C, B, A의 4가지 분류와는 다른 4개의 집합으로 구분할 수 있다: 집합 D는 요구사항이 없는 등급이다; 집합 C1/C2/B1은 많은 상업적 운영체제에 대한 일반적인 보안 특성을 요구하는 등급들이다; 집합 B2는 사용하고 있는 모델의 보안에 대한 정확한 증명과 TCB의 서술적인 명세서를 요구하는 등급들이다; 집합 B3/A1은 TCB에 대해 더욱 정확하게 증명된 명세서와 공식 설계를 요구하는 등급들이다. 이와 같은 각 보안 등급에서 요구하는 보안 특성들은 다음과 같다.

1) 등급 D(Minimal Protection)

요구되는 보안특성이 없는 등급으로 보안평가가 실패한 시스템이 포함된다.

2) 등급 C1(Discretionary Security Protection)

C1 등급은 동일 수준의 기밀성을 갖는 데이터를 처리하는 사용자들의 환경을 위한 등급으로 시스템은 데이터로부터 사용자의 등의 격리(separation)를 제공한다. 사용자들이 그들 자신의 데이터를 보호할 수 있는 엑세스 제한을 구현하기에 충분한 엑세스 제어 메카니즘이 있어야 한다. C1 등급으로 분류되기 위해서는 시스템은 보안기능을 포함하는 보안 영역(domain)을 가져야 하는데 이 영역들은 비인가된 변경(tampering)으로부터 보호되어야 한다. C1 등급에서의 가장 중요한 개념은 DAC(Discretionary Access Control), 임의적 엑세스 제어이다. 모든 사용자 그룹은 확인되어야 하며, 각

사용자 그룹은 다른 사용자 그룹의 엑세스 요구를 허락 또는 거부할 수 있는 권한을 갖는다. 즉 사용자 그룹의 식별에 근거하여 객체에 대한 엑세스 요구를 통제하게 된다. 또한 시스템 보안을 보증하기 위해서는 침투시험(penetration testing)과 같은 방법을 수행하여 비인가 된 사용자 그룹이 보호 메카니즘을 우회하거나 파괴하는 방법이 없다는 것을 보여야 한다. 이러한 C1 등급에 요구되는 보안기준은 다음과 같다.

- 보안정책(security policy)
  - Discretionary 엑세스 제어
- 기록성(Accountability)
  - 식별(identification)과 인증(authentication)
- 보증(assurance)
  - 시스템 구조(system architecture)
  - 시스템 무결성(system integrity)
  - 시스템 시험(system testing)
- 문서화(Documentation)
  - 사용자 보안 가이드(security features user's guide)
  - 신뢰기능 매뉴얼(trusted facility manual)
  - 시험문서(testing documentation)
  - 설계문서(design documentation)

3) 등급 C2(Controlled Access Protection)

C2 등급은 보호기능이 개인 사용자 수준으로 구현되는 임의적(discretionary) 엑세스 제어를 제공한다. 시스템의 감사추적(audit trail)은 각 객체에 대한 각 개인들의 엑세스를 추적할 수 있어야 한다. C2 등급에 부과된 추가의 규제는 잔여정보(residue) 노출의 제거이다. 잔여정보란 한 프로세스가 실행이 종료된 후 레지스터,

메모리, 디스크에 남아 있는 데이터이다. 즉 프로세스 종료시에 기억장소에 남아있는 것 뿐 아니라 보조기억 장치에 쓰여진 데이터를 포함한다. C2 등급은 잔여정보인 한 객체(object)가 다른 사용자에 의해 다시 사용될 수 있기 전에 0으로 쓰기를 하는 등의 방법으로 제거되어야 하는 요구사항을 포함한다.

4) 등급 B1(Labeled Security Protection)

모든 B 등급은 비임의적 엑세스 제어 즉, 강제적인 엑세스 제어(MAC; Mandatory Access Control)를 포함한다. B1 등급에서 제어되는 모든 주체와 객체들은 각각 하나의 보안수준(security level)을 할당받아야 한다. 제어되는 각 객체는 개별적으로 보안 수준에 의해 레이블이 붙여지고 이 레이블들이 기본적으로 엑세스 제어 결정에 사용된다. 엑세스 제어는 계층적 등급(hierarchical levels)과 비계층적 범주(non hierarchical categories)를 모두 포함하는 보안 모델(security model)에 기초로 하고 있다. 계층적 등급을 갖는 시스템의 예로는 Unclassified, Classified, Secret, Top Secret의 계층적 등급을 갖는 군사적 모델을 들 수 있고 비계층적 범주는 최소 권한(need-to-know) 범주 집합을 의미한다. 이러한 강제적인 엑세스 제어 정책을 포함하고 있는 대표적인 보안 모델은 Bell-Lapadula 모델이다. Bell-Lapadula 모델은 보호시스템을 유한 상태 기계(finite state machine)로 나타내는데 현재 상태는 신원허가(clearance)를 갖는 주체들의 집합, 비밀등급(classification)을 갖는 주체들의 집합, 그리고 엑세스 행렬(access matrix)로 표현되며, DAC에 관해 다음과 같은 중요한 특성을 갖는 보호 모델이다.

① SS 특성(simple-security property): 주체 S는 자신의 신원허가보다 작거나 같은 비밀등급을 갖는 객체에 대해서만 판독을 수행할 수 있다.

② * 특성(star property): 주체 S는 자신의 신원허가 보다 크거나 같은 비밀등급을 갖는 객체에 대해서만 기록을 수행할 수 있다. 이 특성은 주체가 자신의 비밀수준 보다 더 낮은 비밀수준으로 정보를 복사하는 것을 금지한다.

5) 등급 B2(Structured Protection)

B2 등급의 주요한 개선은 설계 요구사항이다: B2 시스템의 설계와 구현은 더욱 철저한 테스트와 조사가 가능해야 한다. 검증 가능한 설계가 제시되어야 하며, 테스트는 시스템이 제시된 설계를 구현했음을 확인할 수 있어야 한다. 따라서 시스템의 모든 주체와 객체들에게 적용되는 DAC와 MAC 통제가 명확하게 정의되고 문서화된 공식적인 보안모델을 기초로 구성되어야 한다. B2 등급의 또 다른 특성은 Covert 채널의 분석이 요구되는 점이다. Covert 채널은 서로 통신 할 수 없는 프로세스들이 비정상적인 방법으로 정보를 누출시키는 채널이다. 즉 직접적으로 통신하는 것이 아니라 제3의 객체를 통해 간접적으로 통신을 하거나, 또는 한 프로세스의 실행동작으로부터 다른 프로세스가 정보를 획득하는 방법을 사용하는 가상적인 채널이다.

6) 등급 B3(Security Domains)

B3 등급은 주체의 객체에 대한 모든 엑세스를 통제하는 조회 모니터는 시스템의 모든 엑세스 메카니즘을 포함하고 있는 부분으로 엑세스 권한집합이 데이터 베이스로 구성되어 있으며, 활동중인 모든 주체가 객체에 대한 엑세스 권한을 변경하기 위해서는 반드시 조회 모니터에 요구하여 승인을 받아야 하는 규칙이 적용된다. 이러한 조회 모니터는 분석과 테스트가 용이하도록 충분히 작아야 하며, 침투로부터 완전히 보호(tamperproof) 되어야 한다. 이러한 침투로부터 완전히 보호되는 시스템은 침투에 대해 매우 민감하게 저항하는 시

스템이다. 따라서 시스템 보안에 과한 위반 사건이 발생했을 때 즉시 식별할 수 있는 감사(audit) 능력과 시스템 회복능력이 요구된다.

7) 등급 A1(Verified Design)

A1 등급은 공식적으로 검증된 시스템의 보안능력은 B3 등급의 능력과 같다. A1 등급은 trusted computing base가 정확하게 구현되었다는 높은 수준의 보증(assurance)을 요구하는데 A1 등급 검증(certification)을 위한 5가지 중요한 기준이 제시되고 있다.

① 보호 시스템의 공식적인 모델과 그 모델의 일관성 및 적절성에 대한 증명
② 보호 시스템의 공식적인 최상위 명세(top-level specification)
③ 최상위 명세가 보호 모델과 일치한다는 것을 증명
④ 명세와 일치하는 구현
⑤ Covert 채널의 공식적인 분석

이와 같은 정보시스템 신뢰성평가 기준인 TCSEC이 제정된 이후에 미국은 다양한 정보시스템을 평가하기 위하여 TCSEC을 컴퓨터 네트워크에 적용하는 평가기준인 TNI(Trusted Network Interpretation of TCSEC), TCSEC을 데이터베이스 시스템에 적용하는 평가기준인 TDI(Trusted DBMS Interpretation of TCSEC), 그리고 TCSEC 평가기준의 일부분만을 만족시키는 서브시스템을 위한 평가기준인 CSSI(Computer Security Subsystem Interpretation of TCSEC) 등을 제정하였으며, 1992년에는 NSA(National Security Agency)와 NIST(National Institute of Standards & Technology)가 공동으로 위의 평가기준들을 단일화하기 위하여 연방평가 기준(FC; Federal Criteria)을 제정하였는데 이러한 노력들은 모두 국제 표준화를 위한 노력으로 미국, 캐나다, 프랑스, 독일, 네덜란드 및 영국에 의해 공통 평가기준(CC; Common Criteria) 제정으로 통합되었다.

2.2 공통 평가기준(CC)

세계 각 국의 평가기준이 상이하여 평가에 소요되는 비용과 시간이 많이 소요되므로 TCSEC(Trusted Computer System Evaluation Criteria), ITSEC(Information Technology Security Evaluation Criteria), CTCPEC(Canadian Trusted Computer Product Evaluation Criteria), FC(Federal Criteria) 등의 평가기준 통합의 필요성을 절감한 미국(NIST, NSA), 캐나다(CSE), 프랑스(SCSSI), 독일(BSI), 네덜란드(NLNCSA) 및 영국(CESG) 등 6개국의 국가 보안기관들이 1993년에 공통 평가기준인 CC(Common Criteria)를 개발키로 합의하였다. 1999년 8월에 CC v2.1이 발표되었으며 현재 이것을 토대로 국제표준기구(ISO/IEC JTC1 SC27 WG3)에서 표준화를 위한 노력을 경주하고 있다. 이러한 공통 평가기준(CC)은 신뢰성 평가기준(TCSEC)처럼 한 등급에 대하여 기능과 보증의 요구사항이 규정되어 있는 것이 아니라 기능은 다양한 기능에 필요한 요구사항을 분류하여 기준으로 제시하되 이들은 부품처럼 필요한 기능만 선택하여 쓸 수 있도록 하고 가정된 위협에 대처하기 위해 필요한 기능을 모아 놓은 정보보호제품을 보증 등급에 따라 평가하게 된다. 공통 평가기준(CC)의 핵심은 3가지 부분(Part)으로 구성되어 있는데 제1부(Introduction and General Model)에서는 기본 개념과 일반모델을 제시하고 있고, 제2부(Security Functional Requirements)는 보안기능 요구사항을 기술하고 있으며, 제3부(Security Assurance Requirements)는 보안보증 요구사항을 기술하고 있다. 이 외에도 이미 정의된 보호 프로파일을 기술하며 보호 프로파일을 등록하는 절차를 명시하고 있다.

가. 기본 개념과 보안 모델

공통 평가기준(CC)은 정보보호시스템에서 요구되는 기능요구사

항 및 보증요구사항으로 이루어진다. 기능요구사항에서는 보안활동을 정의하며 보증요구사항은 정보보호시스템이 신청된 보안정도로 실제 정확하게 구현되었는지에 대한 신뢰도를 입증할 수 있는 기초가 된다. 보안평가의 일반 모델은 개발 과정, 평가 과정, 그리고 운영 과정으로 구성된다. 첫째로 개발 과정에서 개발자들은 정보보호시스템 개발 시 예상되는 보안기능을 설정하는데 공통평가 기준에서 정의하는 요구사항들을 유용하게 사용할 수 있다. 이는 공통평가 기준이 기존에 개발되어 사용해오던 정보보호시스템을 모델로 평가기준의 요구사항을 정의하고 있기 때문이다. 또한 정보보호시스템 이용자나 개발자가 그들의 요구를 만족하는 보안요구사항을 표준화된 방법으로 표현할 수 있게 보호프로파일(PP; Protection Profile)의 구조를 정의하고 있다. 평가대상이 되는 제품이나 시스템의 일부분 또는 전체를 TOE(Target of Evaluation)라고 하며 TOE가 제공하는 보안기능과 평가대상 범위를 설명하는 보안목표명세서(Security Target)는 TOE의 위협, 보안목적, 보안요구사항 및 보안기능과 보증기준의 요약 명세서 등을 기초로 하여 작성된다. 이렇게 작성된 보안목표명세서는 평가 기초자료로서 평가자가 활용할 수 있다. 둘째로 평가 과정에서 평가자료로 사용되는 문서는 보안목표명세서, TOE에 관한 증거, TOE 보안기능 등이 있으며 이 과정을 통해 얻을 수 있는 결과로 TOE가 보안목표명세서를 만족하는지 확인할 수 있다. 평가과정 중 한 개 이상의 평가보고서를 작성하게 된다. 끝으로 운영 과정에서는 평가를 마친 TOE를 운영하는 동안 취약성이 발견되는 경우나 설정된 운영환경의 개정이 요구되는 경우 개발자에게 TOE의 추가 변경 요구사항을 보고서로 제출하도록 요청한다. 변경된 부분에 대하여 재평가가 이루어진다.

한편 평가를 위해 제출되는 IT 제품이나 시스템인 TOE가 가지는 보안기능을 TSF(TOE Security Functions)이라 하며 이 TSF의 모든 부분은 TOE에서 요구되는 보안기능을 정의하는 규칙인 TOE 보

안정책(TSP; TOE Security Policy)에 따라서 정의된다. TOE 평가는 TOE 보안정책이 TOE 자원 전체에 대해 적용됨을 보장하는 것이다. TOE 보안정책은 다수의 보안기능 정책(SFP; Security Function Policies)들로 구성된다. 각 보안기능 정책은 통제 범위를 가지며, 보안기능 정책에 의하여 통제되는 주체, 객체 및 오퍼레이션으로 정의된다. 보안기능 정책은 보안기능(SF; Security Function)으로 구현되며 보안 메커니즘들은 정책을 시행하는데 필요한 수단들을 제공한다. TSF(TOE Security Functions)는 TOE 보안정책을 직접적으로 적용하거나 TOE 보안정책 적용에 기여하는 모든 하드웨어, 소프트웨어 및 펌웨어로 구성된다. TSP는 사용자나 주체가 TOE 자원(TOE가 제공하는 정보 및 서비스)을 요청할 경우 이들의 접근통제 규칙을 정의하는 것이며 보안기능 정책으로 이루어진다. 이러한 보안기능 정책들은 정책수행을 위해 요구되는 기능들을 제공하는 메커니즘에 의하여 구현될 수 있다. 정보기술(IT)제품 및 시스템을 분류하고 각 특성에 맞는 보안목표를 유용하고 효과적으로 표현하도록 기존의 보안기능 요구사항을 선택하여 보호 프로파일을 작성함으로써 같은 분류에 속하는 IT제품이나 시스템은 보호 프로파일을 새로 작성할 필요 없이 기존에 작성되어 있는 보호 프로파일을 활용할 수 있게 한다. 예를 들어 침입차단시스템(Firewall), 관계형 데이터베이스 제품의 보호 프로파일이 개발된 상태에 있다. 그리고 보안목표명세서(ST; Security Target)는 평가 활동의 기초 자료로서 TOE에서 요구되는 보안요구사항과 객체들을 포함하며 요구사항을 만족시키기 위하여 TOE가 제공하는 기능과 보증평가를 정의한다. ST 작성자는 한 개 이상의 보호 프로파일에 적합하도록 보안목표명세서를 작성하여야 한다.

나. 보안기능 요구사항

사용자 및 개발자가 시스템의 보안요구사항을 정의하는 과정에서

정보보호 환경에 위협이 될 수 있는 요소들을 고려하여야 한다. 보호 프로파일이나 보안목표명세서의 개발자가 안전한 정보보호시스템을 개발하기 위해 요구되는 보안요구사항을 정의할 수 있도록 공통 평가기준은 일반적으로 공통되는 컴포넌트(Component)들을 포함하고 있는데 이러한 컴포넌트들이 가지는 계층적 체계는 보안위협에 적절히 대처하는 컴포넌트를 정확하게 선택하여 요구사항을 서술할 수 있도록 사용자를 도와준다. 보안 요구사항은 TOE의 기능 요구사항을 표준화된 방법으로 표현한 것으로써 기능 컴포넌트들의 집합을 정하는데, 보안기능 컴포넌트 구성요소에는 공통내용을 가진 패밀리를 그룹화한 클래스(Class), 공통된 보안목적을 가지는 컴포넌트들을 그룹화한 패밀리(Family), 실제 보안요구사항을 정의한 컴포넌트, 부분 보안목적을 만족시키는 보안기능 및 보증 컴포넌트들의 혼합으로써 재사용이 가능한 집합인 패키지(Package)가 있다. 여기서, 패키지는 TOE에서 요구하는 보안 목적 중에서 같은 의도를 가진 보안목적을 만족시키는 요구사항들을 모은 것으로 이들 요구사항들은 특정 보안목적을 만족시키는데 아주 유용하고 효과적인 컴포넌트로 알려진 것들의 집합이다. 또한 컴포넌트 오퍼레이션(Component Operation)은 공통기준을 정의하고 있기 때문에 요구사항들은 모든 TOE에 적용될 수 있도록 포괄적으로 서술되어 있다. 보호 프로파일, 보안목표명세표의 작성자가 개발이나 평가를 목적으로 TOE의 보안요구사항을 작성할 경우 각각의 시스템에 적합한 보안기능을 수행하고 위협들을 막을 수 있도록 기존의 컴포넌트들을 적절히 적용할 수 있는 방법을 제공하고 있다. 한편 컴포넌트들의 관계에는 종속성이 존재한다. 하나의 컴포넌트로는 보안기능을 구현하기에 부족하여 다른 컴포넌트들이 요구되는 경우 종속성이 나타나게 된다. 이와 같은 보안기능 요구사항으로는 감사기록 및 추적, 송·수신 부인방지, 사용자 데이터 보호, 신분확인, 보안기능의 보호, 가용성, 사용자 세션 통제, 안전한 경로 등이 있는데 이를 요약하면 다음 표 2.1과 같다.

클래스	내 용
FAU (Security Audit)	보안활동과 관련된 정보를 감지, 기록, 저장
FCO (Communication)	데이터를 교환하는 주체의 신원을 감지
FCS (Cryptographic Support)	암호 운용 및 키관리
FDP (User Data Protection)	사용자 데이터의 보호
FIA (Identification & Authentication)	사용자의 신원확인 및 인증
FMT (Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR (Privacy)	허가되지 않은 사용자에 의한 정보 도용방지
FPT (Protection of Trusted Security Functions)	TSF 데이터의 보호 및 관리
FRU (Resource Utilization)	TOE의 가용자원을 확보
FTA (TOE Access)	TOE에 대한 사용자 세션의 보호
FTP (Trusted Path)	사용자와 TSF간 혹은 TSF 간의 안전한 통신채널 확보

〔표 2.1〕 보안기능 클래스

다. 보안보증 요구사항

보안보증 요구사항은 TOE의 보증요구사항을 표준화된 방법으로 표현한 것으로써 보증 컴포넌트들의 집합을 정한다. 보안보증의 분류는 보안기능 요구사항의 분류와 비슷하며 보호프로파일, 보안목표명세서 작성 시 보안기능 요구사항과 더불어 보안보증 요구사항을 선택하여야 한다. 보안 보증은 보증컴포넌트, 보증패밀리, 보증

클래스로 분류되는데 보호프로파일과 보안목표명세서에 대한 평가 기준을 정의하며 TOE 평가를 등급별로 나누어 7등급의 평가등급을 제시하고 있다. 보안보증 요구사항에는 형상관리, 배달절차 및 운영, 개발, 설명서, 생명주기 모델, 시험, 취약성 분석 등이 있는데 이를 요약하면 다음 표 2.2와 같다.

클래스	내용
ACM (Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO (Delivery and Operation)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD(Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC(Life Cycle Support)	TOE의 생명주기와 관련된 사항을 확인
ATE(Tests)	TOE가 기술요구사항을 만족하는 지를 확인
AVA(Vulnerability Analysis)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용 등 잠재적 취약성을 확인
APE (Protection Profile Evaluation)	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE (Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA (Maintenance of assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

〔표 2.2〕 보안보증 클래스

라. 보안평가 보증등급(EAL; Evaluation Assurance Levels)

공통 평가기준(CC)에서 정의하고 있는 등급체계는 EAL1, EAL2, EAL3, EAL4, EAL5, EAL6 및 EAL7로 구성되며 EAL0은 부적합 판정을 의미한다. EAL1부터 EAL4등급까지는 사용된 특별한 보안 기술을 소개하지 않고 일반적으로 기존에 있었던 제품과 시스템을 재정비하기 위한 관점에서 적용될 수 있다. EAL4이상의 등급은 응

용기술로 사용된 보안기술까지 평가대상 범위를 넓히고 있다.

보증 클래스	보증 패밀리	보증평가등급에 따른 보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상 관리	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
배포와 운영	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
개발	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
설명서	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
생명 주기 지원	ALC_DVS			1	1	1	2	2
	ALC_FLR				1	2	2	2
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

〔표 2.3〕 보안평가 보증등급

마. 보안평가 유형

공통 평가기준(CC) 기반의 보안 평가에는 보호 프로파일(Protection Profile) 평가, 보안목표명세서(Security Target) 평가, 그리고 TOE (Target of Evaluation) 평가가 있다. 보호 프로파일은 정보보호시스템을 사용하고자 하는 보안 환경 및 보안 목적을 정의하고, 이에 적합한 보안 요구사항을 공통 평가기준에서 도출하여 정의하는 것이다. 공통 평가기준의 보안 요구사항에는 실제 구현에 관련된 사항은 명시되지 않음으로 보호 프로파일에도 구현 방법이나 구현 기술은 포함되지 않는다. 구현 방법이나 구현 기술은 보안 목표명세서에 포함되며, 보호 프로파일이나 보안 목표명세서의 대상이 되는 정보보호제품이나 정보보호시스템을 TOE(Target of Evaluation)라고 한다. 보호 프로파일의 작성 목적은 정보보호시스템의 구현 기술을 서술하고자 하는 것이 아니라 보안 환경에 따라 도출된 보안 목적을 만족하도록 보안 대책을 체계적으로 세우고 이에 합당한 보안 요구사항을 도출하여 정보보호시스템 평가를 위한 논리적 기초를 마련하고자 하는 것이며, 보안 목표명세서는 보호 프로파일에 근거하여 실제 개발된 제품의 보안관련 사항을 구현 방법과 구현 기술을 포함하여 작성하는 것이다.

1) 보호 프로파일 평가

사용자 단체, 정보보호시스템 개발자, 요구사항의 공통집합 정의에 관심이 있는 기타 조직 등이 보호 프로파일을 개발할 수 있다. 보호프로파일은 사용자에게 보안 필요성 및 목적을 설명하는 수단을 제공하며 이러한 보안 필요성 및 목적에 대한 평가를 손쉽게 할 수 있다. 보호 프로파일 평가는 공통 평가기준(CC) 제3부(Security Assurance Requirements)에 있는 보호 프로파일을 위한 평가기준에 따라 평가를 수행한다. 보호 프로파일의 평가 목적은 평가를 위

해 TOE의 요구사항을 표현하는 보호 프로파일이 완전성, 일관성, 기술적 적합성을 가지고 있는지 증명하는 것이다.

2) 보안 목표명세서 평가

보안 요구사항의 집합을 포함하는 보안 목표명세서는 보호 프로파일을 참조하여 작성할 수 있고 공통평가기준의 기능 및 보증 컴포넌트를 직접 참조하여 작성할 수도 있다. TOE를 위한 보안 목표명세서 평가는 공통 평가기준(CC) 제3부(Security Assurance Requirements)에 있는 보안 목표명세서를 위한 평가기준에 따라 평가를 수행한다. 이 평가의 목적은 보안 목표명세서가 완전성, 일관성, 기술적 적합성을 가지고 있는지 증명하고자 하는 것과 보호 프로파일에 대한 보안 목표명세서의 일치성을 요청할 경우 보안 목표명세서의 요구사항이 보호 프로파일 요구사항을 적당하게 만족하는지를 증명하는 것이다.

3) TOE 평가

TOE 평가는 평가된 보안 목표명세서를 기초로 공통 평가기준(CC) 제3부(Security Assurance Requirements)에 포함된 평가기준에 따라 수행된다. 평가 목적은 TOE가 보안 목표명세서에 명시된 보안 요구사항을 만족하는지를 증명하는 것이다.

이와 같이 공통 평가기준을 수용하게 되면, 위에서 설명한 바와 같이 하나의 시스템에 대한 다양한 보호 프로파일을 통해 각각의 사용자 요구사항이 구별되어 제시될 수 있으며, 제품 혹은 시스템별 평가기준이 보호 프로파일로 대체됨에 따라 모든 정보보호시스템에 대한 평가가 가능하게 된다. 공통 평가기준(CC)기반의 평가는 CC v1.0 개발에 참여하였던 미국, 캐나다, 영국, 독일, 프랑스, 네델란드 5개국의 CCMEB(Common Evaluation Methodology Editorial

Board) 위원회가 개발한 CEM(Common Evaluation Methodology)에 의해 평가된다. CEM의 평가 절차는 크게 평가 준비, 평가 시행, 평가 결과 승인의 3단계를 걸친다. 평가 준비는 산업체가 평가받고자 하는 제품에 대한 일부 제출물을 제시하고, 평가자가 이를 조정. 보완함으로써 평가가 시행될 수 있도록 준비하는 단계가 된다. 평가 시행단계에서는 산업체가 제시한 제출물에 기초하여 평가를 수행하며, 평가조사보고서(OR; Observation Report)와 평가기술보고서(ETR; Evaluation Technical Report)를 작성하게 되는데, 이는 제품평가의 결과보고서로서 발견된 취약점 및 문제점들을 포함한다.

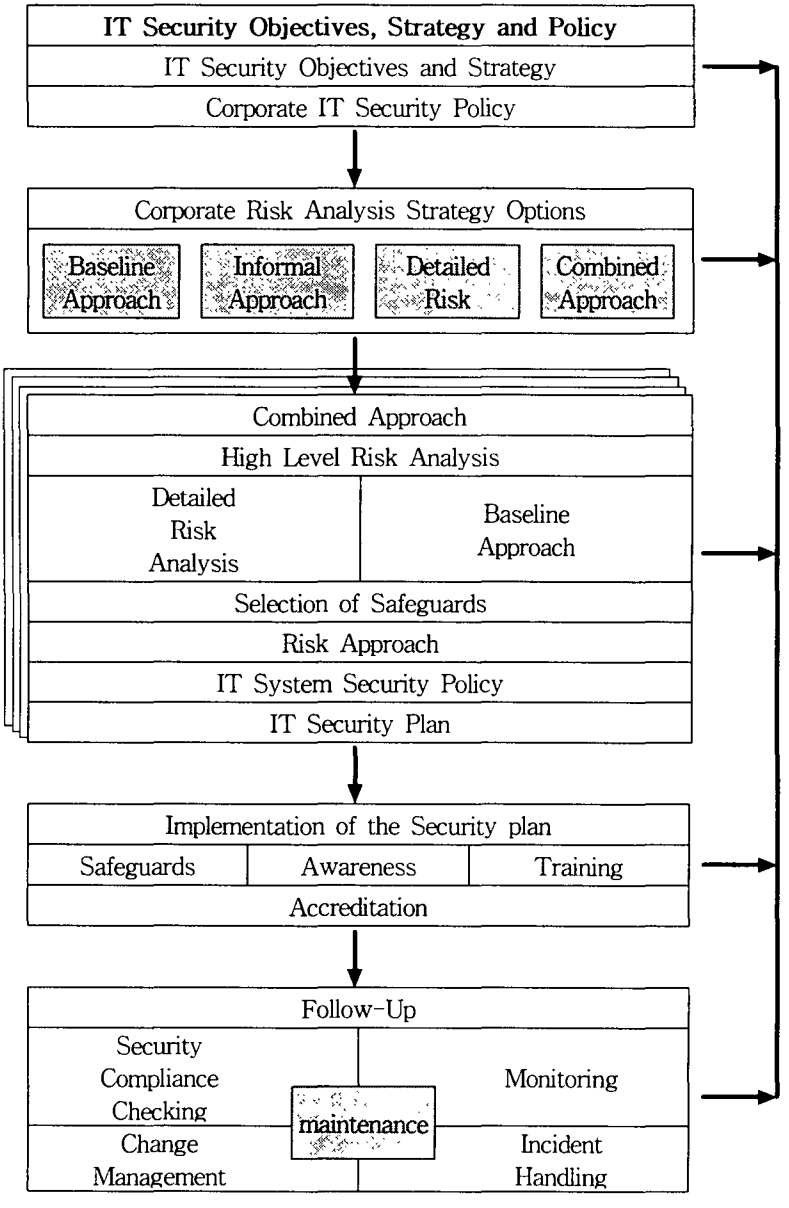
2.3 정보보안 관리 모델

정보보안 관리(Security Management)는 계획단계에서 보안정책을 수립하고 위험분석에 따른 시스템에 대한 보안계획이 작성되고, 실행단계에서 보안 시스템을 설치하여 운영하며, 평가단계에서는 보안 시스템의 평가와 보안감사를 하고, 다시 계획단계로 순환된다. 정보보안 선진국에서는 조직의 보안관리에 대한 중요성을 인식하고 영국의 BSI(British Standard Institute)나 미국의 NIST(National Institute of Science & Technology)와 같은 정보보호 기관에서 국가 차원의 보안 관리 절차 및 방법론을 자체적으로 개발하여 적용하고 있으며, 국제적인 보안관리 표준으로는 ISO/IEC, JTC1/SC27에서 정보기술보안관리지침(GMITS; Guidelines of the Management of IT Security)이 개발되고 있다. 정보기술보안관리지침(GMITS)은 총 5부로 구성되어 있는데 제1부(Concepts and Models of IT Security)는 보안관리의 개념과 보안 모델을 설명하고 있으며, 제2부(Managing and Planning IT Security)는 위험관리와 기획 프로세스에 대한 내용들을 포함하고 있다. 제3부(Techniques for the Management of IT Security)는 보안관리를 위한 구체적인 기법들을

제시하고 있으며, 제4부(Selection of Safeguards)에서는 보안요구사항과 조직의 특정환경에 따라 보안대책을 선정하는 과정을 기술하고 있다. 끝으로 제5부(Management Guidance on Network Security)에서는 인터넷과 같은 외부 네트워크와 연결된 상황에서 보안대책을 수립하는 방법을 기술하고 있다.

- ISO/IEC TR 13335-1: 1996, Guidelines for the management of IT Security
  - Part 1: Concepts and models for IT Security
- ISO/IEC TR 13335-2: 1997, Guidelines for the management of IT Security
  - Part 2: Managing and planning IT Security
- ISO/IEC TR 13335-3: 1998, Guidelines for the management of IT Security
  - Part 3: Techniques for the management of IT Security
- ISO/IEC TR 13335-4: 2000, Guidelines for the management of IT Security
  - Part 4: Selection of safeguards
- ISO/IEC TR13335-5: 1999, Guidelines for the management of IT Security
  - Part 5: Management guidance on network security

GMITS의 정보기술 보호관리의 모델은 정보보안 목적과 전략 및 정책을 수립하고 위험분석을 실시한 후 정보기술 보호계획을 수립한 다음 구현을 하며, 구현 후에는 철저한 사후관리를 실시하는 것으로 구성되어있다. 이러한 과정에 대하여 GMITS 제3부(Techniques for the Management of IT Security)에서 정보기술 보호를 위한 관리 프레임워크를 다음 그림과 같이 제시하고 있다.



〔그림2.2〕 GMITS 관리 프레임워크

정보기술보안관리지침(GMITS)에서 위험관리(Risk Management)는 보안관리의 가장 핵심적인 영역이다. 위험관리란 불확실한 사건의 피해를 식별, 통제, 최소화하는 전반적인 절차에 관계된 경영과학의 한 분야로서, 정보시스템의 위험관리는 측정/평가된 위험에 대한 보안대책을 일정 수준까지 유지하고 관리하는 것이다. 위험분석이란 정보시스템과 그 자산의 비밀성(confidentiality), 무결성(integrity), 가용성(availability), 기록성(accountability)에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템의 취약성을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것으로서, 위험분석의 3대 요소는 다음과 같은 자산, 위협, 취약성이다.

(1) 자산(asset)

보호해야 할 정보 자원들을 식별하고 체계적으로 분류하여, 소유하고 있는 자산들의 가치를 평가하는 기본적인 단계이다. 여기서 자산이란 하드웨어, 소프트웨어, 데이터 베이스, 사용자, 시스템 관련문서, 전산자료, 저장매체, 통신망 및 관련장비 등을 말한다.

(2) 위협(threat)

위협은 자산에 해를 줄 수 있는 위험의 원천이다. 이와 같은 위협을 식별하고 분류해서, 발생빈도와 손실크기를 측정하는 것을 말한다.

(3) 취약성(vulnerability)

취약성이란 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 뜻한다. 이와 같은 약점을 확인하고 분류하여 위협을 감소시키는 것이 취약성을 분석하는 목적이다.

정보기술보안관리지침(GMITS)에서는 위험분석(Risk Analysis) 방법으로 Baseline Approach, Informal Approach, Detailed Approach, Combined Approach의 4가지를 제시하고 있으며, 위험분석의 방법에 따라 통제사항을 선택하는 방법도 각각 상이하게 제시하고 있는데, 통제사항은 조직적 및 물리적 분야에서 7개의 세부 분야의 40개, 정보기술 시스템 분야에서 5개 세부 분야의 23개를 제시하여 다음 표 2.4와 같이 총 63개의 통제사항으로 구성되어있다.

구 분	세부분야	통제사항
조직적 및 물리적 통제사항 (40개)	IT Security Management and Policy	7
	Security Compliance Checking	2
	Incident Handling	4
	Personnel	4
	Operational Issues	12
	Business Continuity Planning	4
	Physical Security	7
IT 시스템 중심의 통제사항 (23개)	Identification and Authentication (I&A)	3
	Logical Access Control and Audit	5
	Protection against Malicious Code	4
	Network Management	6
	Cryptography	5

〔표 2.4〕 정보기술보안관리지침의 통제사항

정보기술보안관리지침은 이러한 통제사항을 선택하는 방법으로 3가지를 제시하고 있는데, 첫 번째 방법은 정보기술 시스템 별로 접근하여 통제사항을 선택하는 방법(Baseline Approach; Selection of Safeguards according to the System)으로 워크스테이션, 서버,

응용프로그램 등 유사 유형으로 분류하여 주제별로 통제사항을 선택하여 이를 구현하는 방법이다. 두 번째 방법은 위협에 따른 접근방법(Selection of Safeguards according to Security Concerns and Threats)으로 비밀성, 무결성, 가용성, 책임성, 인증성, 신뢰성에 영향을 줄 수 있는 위협으로 인한 위험을 최소화하기 위하여 필요한 통제사항을 선택 및 구현하는 방법이다. 끝으로 세 번째 방법은 상세분석에 따른 접근방법(Selection of Safeguards according to Detailed Assessment)으로 세부적인 위험분석을 통하여 위협과 취약성으로 인한 위험을 평가하여 해당되는 통제사항을 선택하는 방법이다.

끝으로 정보기술보안관리지침의 보안관리에 대한 구체적인 과정은 다음과 같이 요약 할 수 있다.

1) 보안정책의 수립

조직의 전체 수준에서 운영수준까지 계층구조별로 달성해야 할 보안 목적, 목적을 달성하기 위한 방법으로서 전략, 그리고 목적을 달성하기 위한 규칙으로서 정책을 정해야 한다. 이와 같은 보안정책에는 보안에 대한 요구사항(비밀성, 무결성, 가용성 등), 조직적 하부구조와 책임부여, 명령계통 및 절차, 정보분류를 위한 등급의 정의, 위험관리전략, 비상사태계획, 보안의식 및 훈련, 법적인 규제, 사고기록 등에 관한 사항들이 포함되어야 한다.

2) 보안조직의 역할과 책임 설정

보안에 관한 명령체계와 표준을 승인하는 보안위원회(security forum)와 조직 내에 보안문제를 관리하는 보안관리자(security officer)의 책임과 의무가 명확해야 한다. 이와 같은 보안위원회의역할은 보안정책을 세우고, 이를 보안프로그램으로 실행해서, 그 효과를 검토하며, 이에 필요한 인적/물적 자원을 마련하는 것이다. 보안관리자

의 책임은 보안프로그램의 실행을 감독하고, 보안에 관한 정책 및 명령체계, 보안의식 프로그램 등을 유지관리하고, 보안사고를 조사하고, 보안위원회에 제반사항을 보고하는 것이다.

3) 위험분석전략의 선택

위험분석에 대한 접근방법에는 다음과 같이 네 가지 접근방법으로 구분할 수 있다. 첫째, 기본적인 접근방법(baseline approach)은 모든 조직에 대해서 기본적인 보안요구사항을 충족시키는 표준적인 보안대책의 집합을 구축하는 것이다. 기본적인 통제의 장점은 시간과 비용을 많이 들이지 않고 모든 조직에서 기본적으로 필요한 보안대책을 선택할 수 있다는 것이다. 단점은 조직의 특성을 고려하지 않았기 때문에, 조직 내에 부서별로 적정 보안수준보다도 높게 혹은 낮게, 보안 통제가 적용된다는 것이다. 둘째, 비공식적인 접근방법(informal approach)은 조직 내부에 보안전문가가 없을 때, 외부 전문가의 지식과 경험을 이용하는 것이다. 장점은 별도의 기술을 습득할 필요가 없기 때문에, 작은 조직인 경우에는 비효과적이라는 것이다. 단점은 구조화된 접근방법이 없기 때문에, 위험을 제대로 평가하기 어렵고 보안대책의 선택 및 소요비용을 합리적으로 도출하기 어렵다. 또한, 계속적으로 반복되는 보안관리의 보안감사 및 사후관리가 어렵다는 것이다. 셋째, 세밀한 위험분석(detailed risk analysis)은 자산의 식별 및 평가, 자산에 대한 위협 및 취약성 평가를 근거로 위험의 발생확률과 손실크기를 곱해서 기대손실을 가능하면 계량적으로 계산하는 것이다. 손실 크기를 화폐가치로 계산할 수 없으면, 정성적인 위험분석법을 이용한다. 장점은 조직 내에 부서별로 적절한 보안수준을 마련할 수 있다는 것이다. 단점은 전문적인 지식과 시간과 노력이 많이 소요된다는 것이다. 넷째, 복합적인 접근방법(combined approach)은 기본적인 접근방법과 세밀한 위험분석의 장점을 이용하는 것이다. 즉 조직 내에 특정 부서가 높

은 위험에 직면해 있거나 매우 중요한 부서인 경우에는 세밀한 위험분석을 하고, 그렇지 않은 경우에는 기본적인 접근방법을 이용한다. 장점은 보안전략을 빠르게 구축할 수 있고, 상대적으로 시간과 노력을 효율적으로 활용할 수 있다는 것이다. 단점은 두 가지 방법의 적용대상을 명확하게 설정하지 못함으로써, 자원의 낭비가 발생될 수도 있다는 것이다.

4) 보안위험 평가

위험관리 방법에 따라서 위험통제(위험회피, 손실방지, 손실감소) 혹은 위험재무(위험인수와 위험이전)를 하게 된다. 보안관리자는 위험통제비용과 위험재무비용을 고려해서 적절한 조합을 구해야 한다. 위험재무는 경영학적 측면으로서 위험통제로도 통제가 불가능할 때 선택하는 방법이며, 비용이 너무 많이 드는 방법이다. 위험통제는 손실을 사전에 이루어져야 한다. 여기에는 위험평가과정에서 의사결정자의 위험인식태도에 따라서 비용 효과적으로 여러 가지 보안대책 중에서 최적 보안대책(safeguard)을 선택하는 단계이며, 여기서 선택해서 추진하는 비용까지 계산해야 한다.

5) 시스템보안 정책 및 계획 수립

정보시스템의 구성을 보여주는 구성 계획, 보안대책의 설치를 위한 설치계획, 시스템의 변경시 필요한 변경계획, 비상시를 대비한 비상계획 등을 작성한다. 여기서 구성계획에서는 시스템의 구성요소와 구성요소들간의 관계, 그리고 기존 보안대책의 설치현황 등이 작성되고, 설치계획에서는 새로운 보안대책의 설치에 필요한 자원, 일정 등이 작성된다. 또한, 변경계획에서는 시스템에 대한 확장, 새로운 시스템의 추가 등의 변경에 대한 계획이 작성되고, 비상계획에서는 비상사태를 대비한 계획이 작성된다.

6) 보안대책의 설치 및 보안 교육

보안대책은 안전대책, 혹은 통제, 혹은 대응책(safeguard, or control, or countermeasure)이라고도 불리고 있다. 보안대책은 위험을 감소시키기 위한 보호조치를 의미하며, 여기에는 장치, 절차, 기법, 행위 등이 포함된다. 새로운 보안대책을 기존 시스템에 설치하고, 효과적으로 운영하기 위해서 사용자와 관리자에 대한 보안교육을 실행하여 보안의식을 제고시킨다.

7) 보안감사 및 사후관리

보안감사는 구축된 시스템이 효과적으로 운영되고 있는지 점검하는 활동이다. 기존 시스템의 운영상태를 파악하여 문제점을 조사해서 감사지침서를 작성하며, 이를 보안방침의 수립이나 위험관리에 반영되도록 한다.

제3장 정보보증 기술

정보보증(IA; Information Assurance) 기술은 기반구조를 구성, 운영, 통제하는 정보 및 정보기술에 대한 침해와 공격으로부터 비밀성, 무결성, 인증, 부인방지 및 가용성을 보장하는 수단을 의미한다. 정보보증기술에는 암호시스템, 침입탐지 시스템, 방화벽, 네트워크 보호기술 등이 포함된다.

암호 시스템은 생성된 정보의 송수신 및 저장간에 요구되는 안전성을 확보하기 위한 도구이다. 대칭키 암호시스템은 네트워크 가입자의 수가 증가함에 따라 키 관리의 어려움이 발생하고 디지털 서명을 구현하기 어렵기 때문에 이들 문제를 효율적으로 해결할 수 있는 공개키 암호시스템이 널이 사용되는 추세이다.

암호화된 정보라 해도 시스템에 대한 불법적인 공격을 통한 정보의 조작이 가능하다면 암호화의 의미는 퇴색될 것이다. 시스템에 대한 불법적인 접근, 정보의 조작, 시스템을 무기력화하기 위한 시도에 대한 조기 발견 및 신속한 대응이 필요하다. 그러므로 보안관련 정보수집, 분석, 침입 여부에 대한 판정, 보고 및 대응행동을 기능으로 하는 침입탐지 시스템은 필수적 요구이다.

3.1 공개키 암호시스템

3.1.1 암호시스템

암호 시스템은 암호화에 사용되는 키의 형태에 따라 비밀키 암호시스템과 공개키 암호시스템으로 구별된다. 비밀키 암호시스템은 암호화와 복호화에 사용되는 키가 동일한 반면 공개키 암호시스템

에서는 암호화와 복호화에 서로 다른 키가 사용된다. 고전 암호시스템이나, 폐쇄성이 강한 집단에서는 비밀키 암호시스템을 사용하는 경우가 많으나, 인터넷과 같은 개방적인 시스템에서의 암호는 공개키 시스템을 사용하는 것이 사용자 입장에서 편리한 점이 많다. 비밀키 암호의 대표적인 예로는 미국의 NIST에서 채택한 DES, 우리나라에서 개발된 SEED와 스트림 암호를 들 수 있다. 공개키 암호의 예로는 RSA, 타원곡선 암호, 배낭암호 등을 들 수 있다.

비밀키 암호시스템이 갖는 가장 큰 문제점은 키의 분배 및 관리에 관한 것이다. Alice와 Bob이 비밀키 암호시스템을 이용하여 기밀사항을 주고받기 위해서는 먼저 비밀키를 공유해야 한다. 비밀키를 공유할 수 있는 방법은 보안성이 확보된 채널을 이용하거나 직접 만나서 전달하는 방법 등을 생각할 수 있다. 그러나 암호시스템에 가입한 사용자의 수가 많아지면 이는 매우 번거로운 일이 된다. 예를 들어 사용자의 수가 $n=1,000$이라면, 한 사용자는 다른 각각의 사용자와 서로 다른 비밀키를 공유해야 하므로 암호시스템 전체적으로는 총 $n(n-1)/2=499,500$ 개의 비밀키가 필요하다.

물론 비밀키 관리센터를 운영하면 사용자의 키관리 문제를 덜어줄 수 있다. 키관리 센터를 운영하는 경우 각 사용자는 자신의 비밀키만을 기억하며, 키관리 센터는 모든 사용자의 비밀키를 알고 있어야 한다. Alice가 Bob에게 비밀문서를 보내려면 Alice는 먼저 자신이 비밀키로 암호화한 문서를 키관리 센터로 보내고 키관리 센터에서는 이를 Alice의 비밀키로 복호화한 후, 다시 Bob의 비밀키로 암호화하여 Bob에게 보내는 방식이다. 그러나 이 경우 키관리 센터는 사용자들의 비밀 문서를 모두 볼 수 있다는 문제점이 있다. 또한 다양한 암호 서비스에 대한 사용자의 요구가 증가되면서 인증문제가 대두되었으나 대칭키 암호로는 이 문제를 해결할 수 없었다.

1976년 미국 스탠포드대학의 W. Diffie와 M. E. Hellmann이 연구논문 "New Directions in Cryptography"에서 비밀키 암호시스템

이 갖는 키관리와 인증문제를 동시에 해결할 수 있는 새로운 개념인 공개키 암호시스템(Public Key Cryptosystem)를 제안하였다. 비밀키 암호시스템에서는 암호화와 복호화에 사용된 키가 동일한 반면에 공개키 암호시스템에서는 암호화와 복호화에 사용되는 키가 서로 다른 비대칭형 암호시스템이다. 공개키 암호시스템의 각 사용자는 두 개의 키, 공개키(public key)와 비밀키(secret key, private key)를 갖는다.

3.1.2 공개키 알고리즘

모든 사용자의 공개키는 마치 전화번호부처럼 지정된 디렉토리에 공개되고 각 사용자는 자신의 비밀키만을 안전하게 관리하면 된다. 다른 사용자의 키를 기억하거나, 자신의 키를 다른 사용자에게 알릴 필요가 없으므로 사용자 개개인의 키관리 부담은 현격하게 감소될 수 된다.

Alice가 Bob에게 공개키 암호시스템을 이용하여 암호화된 문서를 보내기 위해서는 공개키 디렉토리에서 Bob의 공개키를 찾아 이를 이용하여 정해진 알고리즘에 따라 문서를 암호화하여 보낸다. 암호문을 수신한 Bob은 자신만이 알고 있는 자신의 비밀키를 이용하여 수신한 암호문을 복호화할 수 있다. 이를 함수를 이용하여 표현하면 다음과 같다. Bob의 비밀키와 공개키를 각각 S_{Bob}, P_{Bob} 라고 하면 메시지 M에 대한 암호화와 복호화는

$$C = E_{P_{Bob}}(M),$$

$$M = D_{S_{Bob}}(C) = D_{S_{Bob}}(E_{P_{Bob}}(M))$$

으로 계산된다. 여기서 E는 암호화(encryption), D는 복호화(decryption)를 의미한다.

공개키 암호알고리즘에서 암호화와 복호화에 사용되는 키가 다름에도 불구하고 알고리즘이 원활하게 작동되는 것은 공개키와 비밀키 사이에 수리적인 구조가 내재해 있기 때문이다. 외형상 전혀 관련이 없어 보이는 비밀키와 공개키는 수학적 규칙에 따른 가공과정을 거치기 전에는 마치 깨어진 거울의 양쪽과 같이 서로 잘 어울리는 형상을 지니고 있었다는 점을 기억해야 한다. 그러나 누구나 쉽게 접근할 수 있는 공개키로부터 비밀키를 유추할 수 있다면 문제는 심각해진다. 즉, Bob의 공개키 P_{Bob}으로부터 비밀키 S_{Bob}을 알아낼 수 있다면 Bob에게 전달되는 비밀 문건을 다른 사용자도 볼 수 있게 될 것이다. 이런 문제는 수학적 가공 과정을 통해 극복될 수 있다. 키의 생성에 관련된 수학적 가공과정은 비밀키와 공개키를 수리적 관련을 갖는 쌍으로 생성하고, 동시에 공개키로부터 비밀키를 유추하는 것은 현실적으로 불가능할 만큼의 긴 시간이 걸리도록 설계되어 있다.

3.1.3 공개키 암호시스템의 예

잘 알려진 공개키 암호알고리즘으로는 RSA암호, 타원곡선암호, 배낭암호 등이 있다. 여기서는 이들 알고리즘의 기본적인 개념을 기술하기로 한다.

1) RSA암호시스템

RSA암호시스템의 명칭은 이의 발견자인 R. L. Rivest, A. Shamir, L. Adleman의 이름에서 비롯되었다. RSA암호시스템의 안전성은 소인수 분해(prime factorization)의 어려움에 근거를 두고 있다. 두 개의 큰 소수 p, q로부터 이들의 곱 n을 구하는 것은 쉽지만 거꾸로 n을 알고 있다하여 n의 소인수 p, q를 구하는 것은 어렵다는 것이다. 실제로 n이 충분히 클 경우 소인수 p, q를 찾

아내는 방법을 누구도 제시하지 못하고 있다.

가) 키의 생성

한 사용자 Bob은 다른 사용자와는 독립적으로 충분히 큰 두 소수 p, q를 무작위로 선택한 후 곱 $n=pq$를 계산하고,

$$1<e<(p-1)(q-1) \text{이고 } \gcd(e,(p-1)(q-1))=1$$

인 수 e를 선택한다. 또한

$$1<d<(p-1)(q-1) \text{이고 } de\equiv 1 \bmod (p-1)(q-1)$$

인 수 d를 선택한다.

Bob의 공개키는 $P_{Bob}=(n, e)$이고, 비밀키는 $S_{Bob}=d$가 된다. Bob의 비밀키 d는 n의 소인수 p, q를 알고 있으면 e로부터 계산할 수 있다. 수 e는 공개키의 일부이므로 n을 소인수 분해 할 수 있다면 Bob의 비밀키는 쉽게 계산될 수 있다.

나) 암호화 및 복호화 알고리즘

Alice가 Bob에게 메시지 M을 암호화하여 보내기 위해서는 밥의 공개키 $P_{Bob}=(n, e)$를 이용하여 암호문

$$C=M^e \pmod n$$

을 작성한다. 여기서 M은 문서를 이진수로 표현한 후 이를 다시 십진수로 나타낸 것으로 n보다는 작은 수이다. 암호문 C를 수신한 Bob은 자신의 비밀키 d와 Fermat의 정리(p가 소수이고 a, p가 서로소이면 $a^{p-1}\equiv 1 \pmod p$이다.)를 이용하여 메시지

$$C^d=(M^e)^d\equiv M(\mathrm{mod}\,p)$$

를 복호화한다.

메시지의 복호화 과정은 다음과 같다. e, d는

$$ed\equiv 1 \mod (p-1)(q-1)$$

를 만족하므로

$$ed=1+k(p-1)(q-1)$$

인 양의 정수 k가 존재한다. 그러므로

$$C=(M^e)^d=M(M^{(p-1)(q-1)})^k$$

이다. 만일 p가 M의 약수가 아니면 Fermat의 정리에 의해

$$C=(M^e)^d=M(M^{(p-1)(q-1)})^k=M(M^{(p-1)})^{k(q-1)}=M\,(\mathrm{mod}\,p)$$

이다. 만일 p가 M의 약수이면 C와 M은 모두 p로 나누어지므로

$$C\equiv M(\mathrm{mod}\,p)$$

이다. 즉 어떤 경우이든 $C\equiv M(\mathrm{mod}\,p)$이다. 똑같은 논리로 $C\equiv M$ $(\mathrm{mod}\,q)$이다. 두 소수 p, q는 서로 다른 소수이므로

$$C=(M^e)^d\equiv M(\mathrm{mod}\,p)$$

이다.

2) 타원곡선 암호시스템

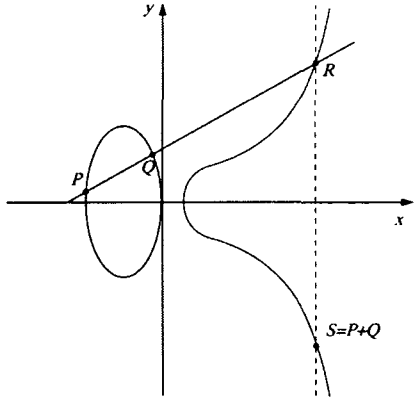
타원곡선(Elliptic curve)은 수학자들에 의해 오랫동안 연구되어 왔으며 최근에는 Andrew Wiles가 Fermat의 마지막 정리를 증명하는데 타원곡선이 중요한 역할을 한 것으로 알려져 있다. 타원곡선은 1985년 N. Koblitz와 V. Miller에 의해 암호학에 처음 응용된 이후 활발한 연구가 진행되고 있다. 유한체(finite field)에서 정의된 타원곡선군(群, group)에서의 이산대수 문제에 기초한 공개키 암호시시템을 타원곡선 암호시스템(ECC; Elliptic Curve Cryptosystem)이라고 한다.

타원곡선 암호시스템은 유한체의 곱셈군에 근거한 시스템으로 군(group)을 만들 수 있는 다양한 타원곡선을 활용할 수 있으므로 다양한 암호시스템을 설계할 수 있으며, 다른 공개키 암호시스템에 비해 작은 길이의 키로도 안전성을 확보할 수 있다. 예를 들어 ECC의 160비트 길이의 키는 RSA의 1024비트 길이의 키에 해당하는 안전도를 제공한다. 또한 RSA에서의 연산은 주로 곱셈의 연속인 반면, ECC에서의 연산은 주로 덧셈이기 때문에 연산 시간이 단축될 수 있을 뿐만 아니라 하드웨어, 소프트웨어적인 구현이 용이하다. 이러한 ECC의 장점은 휴대용 전화기와 같은 모바일(mobile) 시스템과 스마트 카드와 같은 작은 하드웨어에 적용 가능성을 높게 한다.

원곡선은 $Z_p = \{0, 1, \cdots, p-1\}$에서 정의된 방정식

$$y^2 = x^3 + ax + b$$

를 만족하는 점 (x, y)의 집합을 말한다. 타원곡선 위에서 두 점 P, Q의 덧셈 연산을 두 점을 잇는 직선과의 교점 R의 x축에 대한 대칭점 S로 정의하고 무한대 점을 덧셈의 항등원이 되도록 하면 타원곡선은 이 연산에 대해 군(group)이 된다.



〔그림 3.1〕 타원곡선에서의 연산

타원곡선에서 동일한 점 P를 α번 더한 값 $\alpha P = v$를 계산하는 것은 어렵지 않지만, 거꾸로 P, v가 알려져 있다해도 이로부터 α값을 구하는 것은 어렵다고 알려져 있다. 특히 타원곡선이 정의된 공간 Z_p에서 p가 2^{160}정도이면 α값의 계산은 현실적으로 불가능하다.

타원곡선을 이용한 암호시스템으로는 El-Gamal 암호시스템과 Menezes-Vanstone 암호시스템을 들 수 있다. 다음은 El-Gamal 암호시스템의 경우이다.

가) 키의 생성

키의 생성을 위해 적당한 크기의 소수 p와 Z_p위에서 타원곡선을 결정하고 이 타원곡선 위의 한 점 P를 선택한 후

$$Q = \alpha P$$

를 정한다. El-Gamal 암호시스템의 공개키는 (P, Q)이고 비밀키는 α이다. 위에서 말한 것처럼 공개키 (P, Q)로부터 비밀키 α를 구하는 것은 현실적으로 불가능하다.

나) 암호화 및 복호화 알고리즘
암호화할 메시지를

$$M=(u_1, u_2)$$

라고 하자. 이때 메시지 M은 타원곡선 상의 점이다. 암호문의 작성자는 임의의 수 k를 선택하여

$$v_1=kP, \quad v_2=M+kQ$$

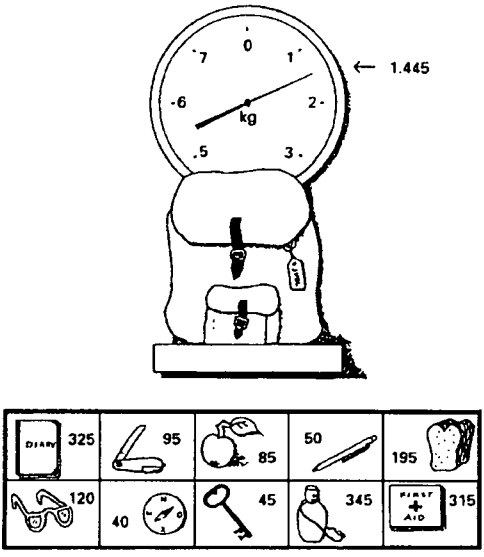
를 계산하여 이를 암호문 $C=(v_1, v_2)$으로 한다. 암호문 C를 수신한 수신자는

$$\begin{aligned} M=v_2-\alpha v_1 &= (M+kQ)-\alpha(kP) \\ &= (M+kQ)-k(\alpha P) \\ &= (M+kQ)-kQ \end{aligned}$$

로 원래의 메시지를 복호화할 수 있다.

3) 배낭 암호시스템

배낭 암호는 배낭 문제에 기반을 둔 암호시스템이다. 배낭 문제(knapsack problem)란 배낭 안에 들어 있는 물품의 종류는 비밀로 하고 단지 배낭에 들어는 물품들 무게의 합만이 알려져 있을 때 이로부터 배낭 안에 들어 있는 물건의 종류를 알아내는 문제이다. 배낭 안에 100개 정도의 물품이 들어 있는 경우 이들의 무게의 합을 알고 있다해도 배낭 안에 들어 있는 물품의 종류를 알아내는 것은 거의 불가능한 것으로 알려져 있다.



〔그림 3.2〕 배낭 문제

배낭 안에 들어있는 물품 각각의 무게의 집합을

$$A=\{a_1, a_2, \cdots, a_n\}, \quad a_i = \text{정수}$$

라고 하고,

$$X=\{x_1, x_2, \cdots, x_n\}$$

는 이진수들의 집합이라고 하자. 여기서 x_i는 a_i의 무게를 갖는 물품이 배낭 안에 들어 있으면 '1'이고 들어있지 안으면 '0'이다. 그러므로 두 집합 A, X가 주어지면 배낭 안에 들어 있는 물품들의 무게

$$S=\sum_{i=1}^{n} a_i x_i$$

는 쉽게 계산할 수 있다. 그러나 A, S가 주어진 상태에서 배낭 안에 들어 있는 물품의 종류 X를 구하는 것은 쉽지 않다.

1978년 Merkle과 Hellmann은 배낭무게 S로부터 들어있는 물품의 종류 X를 찾아내기 위해서는 물품들의 무게 A에 특정한 조건이 있어야 한다는 것을 알아냈다. 이들의 알아낸 조건은 A의 원소들을 크기 순으로 배열하였을 때 초월증가수열이 되어야 한다는 것이다. 초월증가수열이란 한 항의 크기는 이전 항 모두의 합보다 큰 수열을 말한다. 예를 들어

$$A=\{3,5,9,19\}$$

는 초월증가수열이다.

초월증가수열 A의 경우 물품들의 무게의 합이 $S=27$이다. 만일 $x_4=0$ 이면 나머지 물품들의 합이 19이하이므로 무게 a_4인 물품 없이는 27을 만들 수 없다. 그러므로 $x_4=1$ 이어야만 한다. 즉, 배낭 안에는 무게 19인 물품이 들어 있다. 나머지 물품의 무게는 27-19=8이므로 무게 9인 물품은 들어 있지 않으므로 $x_3=0$ 이다. 이런 방법으로 $x_1=x_2=1$ 임을 알 수 있다.

가) 키의 생성

암호문의 작성자는 임의로 초월증가수열

$$A=\{a_1, a_2, \cdots, a_n\}, \quad a_i=\text{정수}$$

와 서로소인 두 u, v를 선택한다. 이때

$$u > \sum_{i=0}^{n} a_i$$

이어야 한다. 이들 (A, u, v)는 배낭 암호의 비밀키가 된다. 공개키는 초월증가수열 A에 변형을 가하여 얻어진 새로운 수열

$$B=\{b_1, b_2, \cdots, b_n\}, \quad b_i = v a_i \bmod u$$

가 된다.

나) 암호화 및 복호화 알고리즘

암호화할 메시지의 이진수에 의한 표현을 X라 하면 암호문은 간단히

$$S = \sum_{i=1}^{n} b_i x_i$$

에 의해 작성된다. 새로운 수열 B는 초월증가수열이 아니므로 공개키 B와 암호문 S를 갖고 있다해도 부가적인 정보 없이는 이를 복호화할 수 없다.

암호문의 복호화는 비밀키 (A, u, v)를 알고 있을 때만 가능하다. 암호문 S가 수신되면 다음의 연산

$$\begin{aligned} v^{-1}S \bmod u &= v^{-1} \sum_{i=1}^{n} b_i x_i \bmod u \\ &= \sum_{i=1}^{n} v^{-1}(v\, a_i)\, x_i \bmod u \\ &= \sum_{i=1}^{n} a_i x_i \bmod u \end{aligned}$$

에 의해 복호화된다. 그런데 마지막 식에 나타난 a_i들은 초월증가수열의 합이므로 메시지의 이진 표현 X를 찾아낼 수 있다.

3.2 디지털 서명

3.2.1 디지털 서명의 필요성

종이 계약서에 계약 당사자 사이의 계약 내용을 확인하기 위해 인감도장을 찍거나 서명을 하는 것처럼 전자문서에도 전자상거래 등과 같이 데이터 파일의 내용에 영향을 미치는 모든 거래에는 서명이 필요하다. 컴퓨터와 통신망을 이용하여 송수신되는 전자문서에 암호기법을 이용하여 인감도장과 같은 기능을 할 수 있는 디지털로 표현된 일종의 암호문을 디지털 서명이라고 한다.

네트워크를 통하여 교환되는 디지털 메시지는 송수신후 송신자 또는 수신자에 의해 임의로 재편집될 수 있다. 예를 들어 송신자는 문서를 보낸 후에 자신에게 불리한 상황이 발생할 경우 문서의 송신 사실을 부인하거나, 메시지의 내용을 자신에게 유리하게 고친 후 오히려 수신자가 메시지의 내용으로 변경하였다고 주장할 수 있다. 이러한 문제는 수신자에 의해서도 야기될 수 있다. 그러나 이러한 분쟁이 생길 경우 제3자가 분쟁의 원인을 밝히는 것은 쉽지 않다. 이런 이유에서 전자문서의 경우 원본의 개념은 없고 사본으로 취급되어야 한다.

전자문서의 교환에서 야기될 수 있는 분쟁의 소지를 없애고 분쟁이 발생할 경우 송수신자가 수긍할 수 있는 분쟁의 원인을 밝힐 수 있는 근거를 제공할 수 있는 수단이 디지털 서명이다.

3.2.2 디지털 서명의 요구조건

디지털 서명된 전자문서는 메시지와 서명문으로 구성된다. 서명문은 메시지의 내용과 별개의 것이 아니라 메시지의 내용에 의존하는 것으로 메시지의 내용에 따라 서명문의 형태도 달아진다. 수기 서명, 인감, 지문 등을 그래픽 이미지로 저장하여 이를 전자문

서의 특정 부분에 복사하여 기록하는 것은 메시지의 내용에 영향을 받는 것이 아니기 때문에 디지털 서명이라고 할 수 없다. 그래픽 이미지를 서명으로 사용한다면 한 번 사용된 이미지는 다른 사용자에 의해 다시 복사되어 사용되는 등 불법적인 사용 가능성이 있기 때문이다.

위에서 말한 것처럼 디지털 서명은 송수신자 또는 제3자의 부정한 행위로 야기될 수 있는 분쟁을 억제하기 위한 것이므로 반드시 다음과 같은 기능을 가져야 한다.

(1) 서명자 인증

메시지에 첨부된 서명문을 통해 수신자가 메시지에 서명한 사용자가 누구인가를 식별할 수 있어야 한다. 만일 수신자가 서명 당사자를 확인할 수 없다면 제3자가 수신자에게 정당한 사용자로 위장할 수 있을 것이다. 그러므로 디지털 서명에서 서명자의 신원을 확인할 수 있는 기능은 필수적이다.

(2) 위조불가

메시지에 대한 서명자만이 서명문을 생성할 수 있어야 한다. 메시지의 작성자가 자신의 신분을 위장하여 다른 사람의 서명을 생성할 수 있다면 이는 다른 사람의 인감을 위조하는 것과 마찬가지이다. 그러므로 한 사용자가 부정한 방법으로 다른 사람의 서명을 생성할 수 없어야 한다.

(3) 재사용 불가

동일한 서명자라 해도 문서가 달라지면 서명문의 형태도 바뀌어야 한다. 그렇지 않다면 Alice의 디지털 서명 문서에서 Alice의 서명을 복사하여 다른 문서에 이를 첨부하여 Alice가 서명한 거처럼

위조할 수 있다. 그러므로 서명문의 서명은 다른 문서의 서명에 재사용될 수 없어야 한다.

(4) 변경불가

디지털 서명된 문서의 메시지 부분을 변경할 수 없어야 한다. 만약 메시지의 내용이 변경된 경우에는 변경사실을 사용자가 인지할 수 있는 기능을 포함해야 한다.

(5) 부인불가

메시지에 디지털 서명을 한 당사자가 본인에게 불리할 경우 서명 사실을 부인할 수 있다면 서명의 의미는 크게 축소될 것이다. 따라서 메시지에 서명을 한 서명자는 디지털 서명사실을 부인할 수 없어야 한다.

(6) 분쟁해결 기능

송수신자 사이에 디지털 서명에 관련된 분쟁이 발생했을 경우 제3자가 어느 쪽에 위법 사실이 있었는가를 판단할 수 있어야 한다.

3.2.3 해쉬함수와 메시지인증

메시지 인증이란 송신자가 보낸 메시지와 수신자가 받은 메시지와 일치하는가의 여부를 확인하는 기능이다. 만일 Alice가 Bob에게 보내는 메시지를 중간에 제3자가 가로채서 불법적으로 변조한 후 다시 Bob에게 보낸다면 송수신자 간에 원활한 정보교환이 이루어질 수 없을 뿐만 아니라 경우에 따라서는 심각한 문제가 야기될 수도 있다. 따라서 송수신자는 교환하려는 정보가 민감한 경우에는 송수신 정보의 일치여부를 확인해야 할 것이다. 이러한 기능을 갖는 함수로 해쉬(hash)함수를 들 수 있다.

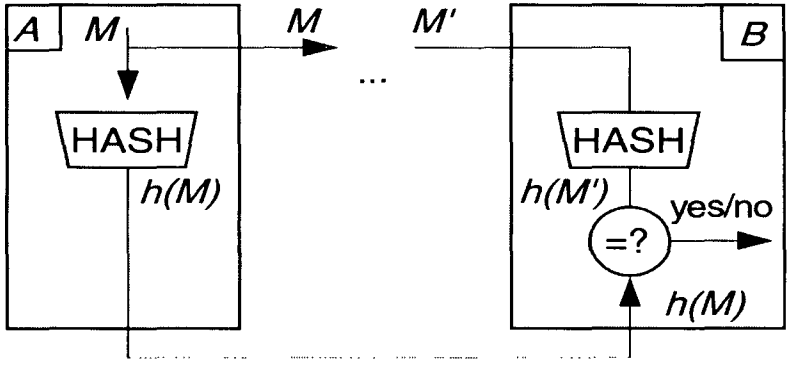
1) 해쉬함수

해쉬함수(hash function)란 임의의 길이를 갖는 이진법에 의한 메시지를 정해진 길이를 갖는 이진 부호로 바꾸는 기능을 갖는 함수이다. 예를 들어 우리 나라 표준 해쉬함수인 HAS-160과 미국의 NIST에서 개발한 전용해쉬함수 SHA-1은 모두 입력메시지의 길이에 관계 없이 항상 동일한 길이인 160비트의 출력을 낸다. 해쉬함수의 대표적인 암호학적인 특징은 일방향함수(one way function)로 충돌회피성(collision free)을 갖는 다는 점이다. 함수 h가 일방향성을 갖는다는 것은 입력 메시지 M에 대한 함수값 $h(M)$의 계산은 쉽게 할 수 있으나 주어진 함수값 v에 대해 $h(M)=v$를 만족하는 입력 메시지 M을 찾아내는 것은 계산상 불가능한 함수를 말한다. 또한 어떤 함수가 충돌회피성을 갖는다는 것은 함수값이 일치하는 서로 다른 입력쌍을 찾는 것이 현실적으로 매우 어려운 경우를 말한다. 함수 h에 대해 서로 다른 입력 메시지의 쌍 M_1, M_2가 $h(M_1)=h(M_2)$를 만족하면 M_1, M_2를 함수 h의 충돌 쌍(collision pair)이라고 한다. 함수 h가 충돌회피성을 갖는다는 것은 충돌 쌍을 찾는 것이 사실상 불가능함을 의미한다.

2) 해쉬함수를 이용한 메시지 인증

Alice가 평문 또는 이를 암호화한 전자 문서를 Bob에게 보내는 경우 해쉬함수를 이용하여 송수신 메시지의 일치 여부를 판단할 수 있다. 예를 들어 Alice가 Bob에게 메시지 M을 보내려고 한다고 하자. Alice와 Bob은 어떤 방법으로든 동일한 해쉬함수 h를 공유한다. Alice는 자신이 보내려하는 메시지 M에 대한 해쉬값 $h(M)$를 계산하여 메시지와는 별도로 Bob에게 보낸다. Bob이 받은 메시지를 M'이라고 하자. Bob은 Alice와 공유하고 있는 해쉬함수를

이용하여 자신이 받은 메시지에 대한 해쉬값 $h(M')$을 계산한 후 Alice가 별도의 채널을 통해 자신에게 보낸 해쉬값과 비교한다. 만일 중간에 불법적인 침입자가 Alice의 메시지를 가로채서 내용을 변경하였다면 M과 M'은 일치하지 않기 때문에 송수신 메시지에 때한 해쉬값은 서로 다르므로 즉, $h(M) \neq h(M')$이므로 Bob이 받은 메시지는 Alice가 보낸 것과 일치하지 않는다는 것을 알 수 있다. 반면에 $h(M) = h(M')$이면 Bob이 받은 메시지는 Alice가 보낸 것과 일치한다고 판단할 수 있다. Alice가 보낸 메시지 M과 Bob이 받은 메시지 M'이 일치하지 않는다면 M, M'은 해쉬함수의 충돌 쌍이 되므로 해쉬함수가 갖는 충돌회피성에 위배되기 때문이다.



〔그림 3.3〕 해쉬함수를 이용한 메시지 인증

3.2.4 공개키 알고리즘과 사용자 인증

위에서 언급한 것처럼 디지털 서명은 일종의 암호이고, 디지털 서명의 요구 조건을 만족하는 암호알고리즘은 공개키 암호이다. 일반적으로 공개키 알고리즘을 이용한 암호화는 암호문의 작성자가 수신자의 공개키를 이용하여 암호화하고 수신자는 이를 자신의 비밀키를 이용하여 복호화 한다. 그러나 이를 반대로 적용하면 암호문의 작성자의 신원을 확

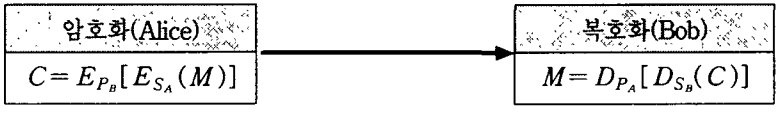
인할 수 있다. 즉 Alice가 자신의 비밀키 S_A를 이용하여 메시지 M을 암호화하여 Bob에게 보내면 Bob은 공개키 디렉토리에서 Alice의 공개키 P_A를 찾아 이를 복호화 할 수 있을 것이다.

〔그림 3.4〕 공개키 알고리즘을 이용한 사용자 인증

위의 프로토콜에서 암호화에 사용된 Alice의 비밀키 S_A는 Alice 자신만이 알고 있으므로 Alice는 자신이 메시지를 보내고 그 사실을 부인 할 수 없다. 그러나 이 방법은 누구나 암호문을 복호화 할 수 있다. 암호문을 푸는데 필요한 Alice의 공개키 P_A는 공개되어 있기 때문이다.

그러나 Alice가 메시지 M를 Bob에게 보내기 위해 자신의 비밀키 S_A를 이용하여 메시지 M을 암호화한 후 여기에 다시 Bob이 공개키 P_B로 암호화하여 Bob에게 보내면 Bob은 자신만이 알고있는 비밀키로 암호문을 일차 복호화한 후, 공개키 디렉토리에서 Alice의 공개키 P_A를 찾아 완전히 복호화할 수 있을 것이다.

이제 암호문 C를 풀기 위해서는 Bob의 비밀키가 필요하고 Bob의 비밀키는 Bob만이 갖고 있으므로 이 암호문을 해독할 수 있는 사람은 Bob뿐이다. 또한 이 암호문은 Alice만이 갖고 있는 Alice의 비밀키로 암호화되었으므로 수신자인 Bob은 송신자가 Alice임을 믿을 수 있다.



〔그림 3.5〕 공개키 알고리즘을 이용한 사용자 인증II

3.2.5 디지털서명

1) 공개키를 이용한 디지털서명

공개키 암호 알고리즘을 이용하여 Alice는 메시지 M에 디지털서명을 첨부하여 Bob에게 보낼 수 있다. 디지털서명을 위해서는 충돌회피성을 갖는 해쉬함수 h를 공유하고 있어야 한다. Alice는 메시지 M에 대한 해쉬값 $h(M)$을 계산한 결과에 자신의 비밀키 S_A를 이용하여 암호화한 값

$$s = E_{S_A}(h(M))$$

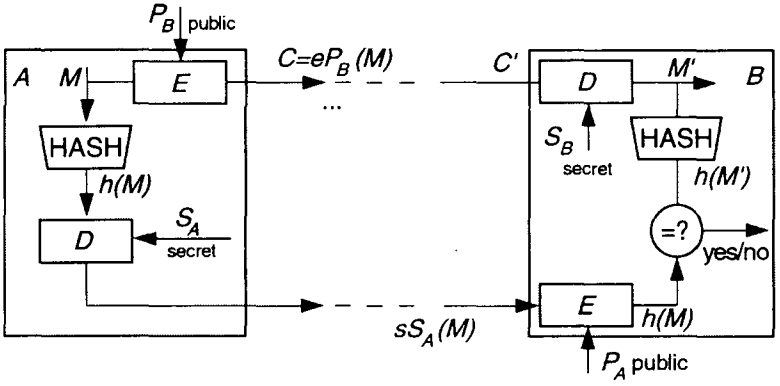
을 메시지 M의 디지털서명으로 하여 메시지 M에 디지털 서명 s를 첨부하여 Bob에게 보낸다.

Bob은 Alice의 공개키를 이용하여 수신한 디지털서명 s로부터 Alice가 보낸 해쉬값

$$h(M) = D_{P_A}(s)$$

을 찾아내고, 한편으로는 공유하고 있는 해쉬함수를 이용하여 수신한 메시지에 대한 해쉬값을 계산하여 서로 비교한다. 만일 두 값이 일치한다면 메시지 M은 손상되지 않았다고 판단할 수 있다. 이는 해쉬함수가 갖는 충돌회피성에 의해 보장된다. 또한 Alice의 비밀키는 자신만이 알고 있으므로 Alice의 비밀키에 의해 암호화된 디지털 서명은 Alice가 한 것이라고 판단할 수 있다.

전자서명의 대상이 되는 메시지는 평문 또는 암호화된 형태로 교환될 수 있다. 다음 그림은 암호화가 병행된 디지털서명의 경우이다.



〔그림 3.6〕 공개키를 이용한 디지털 서명

2) 디지털서명 알고리즘(DSA)

디지털서명 알고리즘, DSA(Digital Signature Algorithm)는 1991년 미국의 NIST(National Institute of Standards and Technology)에 의하여 제시되었고 현재는 DSS(Digital Signature Standard) 라는 이름으로 표준화되었다.

전자서명 알고리즘의 서명 생성자 Alice는 다음의 조건

$$2^{159} < q < 2^{160}$$

인 소수 q를 선택한다. 다음과 같은 계산으로 시작한다. 따라서 q는 2진수로는 160비트의 길이를 갖는다. 또 Alice는

$$2^{511+64t} < p < 2^{512+64t}, \quad t \in \{0,1,2,\cdots,8\}$$

이며, 동시에 위에서 선택한 소수 q가 $p-1$를 나누는 소수 p를 선택한다. 소수 p를 2진수로 표현하면 그 길이가 512~1024비트로 64의 배수가 된다.

이제 Alice는 mod p의 원시근(primitive root) x를 선택한 후

$$g = x^{(p-1)/q} \bmod p$$

를 계산하고 마지막으로 임의로 한 수 $a \in \{1,2,3,\cdots,q-1\}$를 선택한 후

$$A = g^a \bmod p$$

를 계산함으로써 키의 생성이 완료된다. Alice의 공개키는 (p, q, g, A)이고 비밀키는 a이다. 공개키로부터 비밀키 a를 찾아내는 것은 이산대수의 문제로 해결하기가 매우 어려운 것으로 알려져 있으며, DSS는 이러한 수학적인 어려움에 안전성의 근거를 두고 있다.

DSS 알고리즘에서도 메시지 인증과 처리속도 향상을 위해 해쉬함수

$$h: \{0,1\}^* \rightarrow \{1,2,\cdots,q-1\}$$

을 사용한다. 구체적으로 DSS에서는 SHA계열에 기초한 해쉬함수를 사용한다.

DSS에서 메시지 M에 서명을 가하는 과정은 다음가 같다. Alice는 임의의 수 $k \in \{1,2,3,\cdots,q-1\}$를 선택한 후, 자신의 비밀키와 공개키를 이용하여

$$r = (g^k \bmod p) \bmod q,$$
$$s = k^{-1}(h(M) + ar) \bmod q$$

를 계산하여 (r, s)를 메시지 M에 대한 전자서명으로 결정한다.

Bob은 메시지 M과 전자서명 (r, s)를 수신한 후

$$u_1 = s^{-1}h(M) \bmod q,$$

$$u_2 = s^{-1}r \bmod q,$$

$$v = (g^{u_1}y^{u_2} \bmod p) \bmod q$$

를 계산하여 $v = r$인지를 확인한다. 만일 Alice가 보낸 메시지가 원래대로 없이 Bob에게 전달되었다면

$$v = g^{u_1}y^{u_2} = g^{u_1}g^{au_2} = g^{h(M)/s}g^{rx/s} = g^k = r$$

이어야 하므로 $v = r$이다. 만일 위의 계산의 결과에서 $v = r$을 얻었다면 Bob은 Alice의 메시지는 송수신 도중에 손상되지 않았다는 결론을 내릴 수 있다. 메시지 M이 변조되었다면 이에 대한 해쉬값 $h(M)$도 달라졌을 것이고 따라서 Bob이 받은 디지털 서명의 구성 요소 s값은 Alice가 보냈던 값과도 다를 것이다. 따라서 Bob은 다른 u_1, u_2를 계산하게 되어 $v \neq r$라는 사실을 알게 된다.

최초의 메시지 송신자가 Alice인지의 여부는 비밀키 a를 알고 있는 것은 Alice뿐이라는 사실에 의해 판단된다. Alice의 공개키의 일부인 A와 g로부터 비밀키 a를 계산해 내는 것이 사실상 불가능하기 때문에 a를 알지 못한다면 정확한 s값을 알아내는 것 또한 불가능하다.

디지털서명의 확인이 가능하기 위해서는 $s \neq 0 (\bmod q)$이어야 한다. 만일에 s값이 영이 되는 전자서명이 만들어 졌다면, k값을 조정하여 새로운 전자서명을 만들어야 한다. 그러나 q값의 크기를 고려한다면 이러한 결과가 발생할 가능성은 2^{-160}의 위수를 갖기 때문에 실제상황에서는 이러한 경우가 자주 발생하지는 않는다.

3.3 공개키 기반 구조(PKI)

3.3.1 공개키 기반구조

통신과 컴퓨터 기술의 비약적인 발전으로 인터넷 사용자의 수는 급격히 증가하였다. 이에 따라 정부는 민원을 비롯한 행정업무를 점차로 인터넷을 통하여 처리하려 하고, 은행과 유통업을 비롯한 민간기업에서도 인터넷을 통한 거래 기법을 적용하며, 개인과 개인간의 인터넷을 통한 통신의 비중은 매우 높은 수준에 도달하게 되었다.

정해진 사용자와의 거래뿐만 아니라 필요에 따라 거래상대를 정하고 그 상대와 통신을 해야할 경우가 있다. 이때마다 상대방과 비밀키를 공유하고 이를 관리하는 것은 매우 번거로운 일이어서 현실적으로 적용이 불가능하다. 또한 비밀키 알고리즘으로는 디지털 서명이 어렵기 때문에 키관리 문제를 해결하고 동시에 디지털서명을 구현할 수 있는 공개키 암호 시스템의 출현은 자연스러운 것이라 할 수 있다.

공개키 암호 알고리즘의 경우 각 사용자는 비밀키와 공개키를 갖으며 각 사용자는 자신의 비밀키만을 관리하고 공개키는 다른 사용자의 공개키와 함께 게시판 또는 특정한 디렉토리에 저장되어 공개되므로 각 사용자에게 키관리는 더 이상 어려운 문제가 될 수 없다. 또한 각 사용자의 비밀키와 공개키는 각각 디지털서명의 생성키와 검증키의 역할을 하는 디지털서명을 구현할 수 있다.

그러나 모든 사용자에게 공개된 공개키는 이를 운영하는데 사용되는 메커니즘(게시판 또는 디렉토리)이 자체 안전성을 갖지 못하므로 이에 포함된 정보에 대한 공격(위조 또는 변조)이 행해질 가능성이 있다. 이러한 공격은 거래의 신뢰성과 안전성에 결정적인 타격을 주는 결과를 초래하게 된다. 예를 들어 Alice가 Bob에게 문서를 암호화하여 보내려한다고 하자. Alice는 공개키 디렉토리에서

Bob의 공개키를 찾아 이를 이용하여 문서를 암호화하여 정해진 통신경로를 이용하여 Bob에게 암호화된 문서를 보내게 될 것이다. 그런데 이에 앞서 Charles가 공개키 디렉토리에 침입하여 Bob의 공개키를 자신의 공개키로 변경시켜 놓고 전송되는 암호문을 중간에서 가로챈다면 지정된 수신자 Bob이 아닌 Charles가 Alice의 비밀 문서를 보게될 것이다.

앞의 예 외에도 공개키를 공개하고 나서 자신이 것이 아니라고 주장할 때 생기는 문제, 공개키의 취소 등에 관련된 문제 등은 공개키 알고리즘이 갖는 약점이라 할 수 있다. 공개키 알고리즘 운영에서 나타날 수 있는 문제 즉, 공개키의 무결성을 보장하기 위해 제시된 것이 공개키 기반구조(PKI; Public Key Infrastructure)이다.

사용자는 인터넷을 통해 민감한 사항을 전송하기 전에 전송내용이 안전하게 전송되며, 다른 사람에 의해 임의로 변경되지 않을 것이라는 확신을 갖기를 원하며, 거래의 상대방만이 전송 내용을 볼 수 있으며, 거래에 관련된 사용자가 거래 이후에 관련성을 부인 할 수 없다는 확신을 갖고 싶어한다. 캐나다의 재무성은 사용자의 이러한 욕구를 만족시킬 수 있는 해법을 공개키 기반구조로 정의하였다. 즉, PKI를 "사용자가 인터넷이나 다른 네트워크를 통하여 민감한 정보를 안전하게 전송할 수 있도록 사전에 확신을 주는 공개키 암호와 디지털서명에 기반을 둔 정책, 서비스, 정보보호 소프트웨어의 골격이다."로 정의하였다.

여기서는 공개키 암호 시스템에서 요구되는 공개키의 인증, 공개키의 관리, 공개키 인증서에 관해 기술한다.

3.3.2 PKI의 구성 요소

1) 인증기관

인증기관은 PKI를 구성하는 가장 핵심적인 기구로 그 역할과 기능

에 따라 정책승인기관(PAA; Policy Approving Authority), 정책인증기관(PCA; Policy Certification Authority), 인증기관(CA; Certification Authority)으로 구분되며 이들을 통틀어 인증기관이라고 한다. 인증기관의 가장 중요한 역할은 사용자의 공개키 인증서를 발행하는 것이다. 인증서(certificate)란 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 디지털 서명하여 생성되며, 인증서를 통해 사용자의 공개키가 사용자 자신의 것임이 틀림없음을 증명한다.

인증서(certificate)를 운전면허증에 비유한다면 인증기관은 경찰청의 운전면허 발급기관에 비유될 수 있다. 인증기관은 등록을 원하는 사용자에 대한 인증과 비밀키의 적절성을 확인한 후 인증된 정보에 디지털 서명을 실시한 후 사용자들에게 알리는 업무를 포함한 최종사용자(end user)들에 대한 인증서의 발급, 관리, 취소 등 일련의 업무를 수행한다.

이러한 서비스를 제공함에 있어 CA는 인증된 정보를 사용하게 될 신뢰할만한 기관뿐만 아니라 인증된 사용자들에게 자신의 공개키를 공개해야만 한다. 최종사용자와 마찬가지로 CA의 공개키도 디지털 서명된 인증서의 형태로 제공되어야 한다. 그러나 CA에 대한 인증서는 최종사용자의 인증서와는 달리 인증서 발급기관과 인증서 수신기관이 일치한다. 즉, CA에 대한 인증서는 자체 서명된 인증서이다.

2) 등록기관

공통적인 보안정책을 구현하거나 밀접하게 관련이 있는 그룹내의 사용자들에 대해 인증서를 발행해 주는 인증기관들이 논리적으로 그룹화되어 있는 집단인 도메인(domain) 내의 사용자의 수가 증가함에 따라 사용자들의 분포는 지리적으로 광범위하게 분산될

것이다. 또한 PKI사용자그룹의 사용자수가 증가할수록 CA가 처리해야할 업무의 양 또한 증가할 것이다. 등록기관(RA; Registration Authority)은 CA와 최종사용자 사이의 기관으로 새로운 가입자에 대한 등록, 키의 생성 및 취소 등의 CA의 인증 과정을 돕는 기능을 수행한다.

RA는 CA와 멀리 떨어져 있는 사용자들의 인증서 신청시 그들의 신분가 소속을 확인한 후, 인증서 요청서에 서명하고 인증기관에 제출한다. 이를 접수한 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행하여 등록기관을 통하거나, 직접 신청자에게 전달한다.

등록기관은 사용자의 편의를 위해 해당 지역에서 CA 역할을 대행하는 기관의 성격을 갖기도 한다.

3) 인증서 디렉토리

인증서가 만들어지면 차후 사용을 위해 저장되어야만 한다. 각 사용자들이 인증서를 저장해야 하는 불편을 덜기 위해 보통의 경우 CA는 인증서 디렉토리(Certificate Directory)를 사용한다. PKI의 중요한 구성요소인 인증서 디렉토리는 인증서를 관리하고 분배하는 기능을 제공한다.

4) 사용자

PKI 내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템을 포함한다. 사용자는 자신의 비밀키와 공개키를 생성할 수 있어야 하며, 공개키에 대한 인증서의 획득과 디지털 서명을 생성하고 검증할 수 있어야 한다. 또한 디렉토리를 토해 자신의 인증서를 다른 사용자에게 제공할 수 있어야 하며, 비밀키를 분실하거나 필요시 인증서의 취소를 요청할 수 있어야 한다.

5) 키 복구용 서버

PKI에 등록한 사용자의 수에 관계없이 사용자가 자신의 비밀키를 분실할 가능성이 있다. 이는 PKI에 관련된 모든 기관에 부담을 줄 수 있다. 예를 들면 CA는 분실한 키에 대한 공개키 인증서를 파기해야하고, 새로운 키 쌍(비밀키, 공개키)를 생성하고 이에 해당하는 공개키 인증서를 만들어야 한다. 결국 비밀키 분실 이전에 생성된 모든 암호화된 데이터는 복구가 불가능 해 진다.

이에 대한 해결책으로 키를 저장하고 복구할 수 있는 키 복구 서버(Key Recovery Server)를 두는 것이다. 키 복구 서버는 CA가 비밀키를 간직할 수 있는 간단한 방법을 제공한다.

6) 관리 프로토콜

관리 프로토콜(Management Protocol)은 PKI 안에서 사용자와 관리자 사이의 온라인 의사소통을 원활하게 하기 위한 것이다. 예를 들어 관리프로토콜은 등록기관과 사용자 또는 두 CA가 서로를 교차인증하기 위한 의사소통에 사용될 수 있다. PKI의 관리프로토콜로 CMP(Certificate Management Protocol), CMMF(Certificate Management Message Format) 등을 들 수 있다.

관리프로토콜은 다음의 기능을 제공할 수 있어야 한다.

- 등록 : 최초에 CA(직접 또는 RA를 통해)에 등록하는 과정
- 초기화 : 기반구조의 어딘가에 저장되어 있는 키와 가입자의 시스템이 정해진 관계에 따라 작동할 수 있도록 가입자의 시스템을 초기화한다. 예를 들어 사용자의 시스템은 CA의 공개키와 검증된 정보에 의해 안전하게 초기화되어야 하며, 사용자는 자신의 키에 의해 초기화되어야 한다.
- 인증 : 사용자의 공개키에 대한 인증서의 발급과 인증서를 해

당 사용자의 시스템으로 보내거나 게시판에 인증서를 공고하는 과정이다.

- 키 업데이트 : 모든 키의 쌍은 주기적으로 갱신되어야 하며 이에 따른 새로운 인증서가 발급되는 과정이다.
- 인증서의 취소 : 인증서의 취소는 일정한 자격을 갖춘 사람이 비정상적인 상황을 인지할 경우 CA에게 키의 취소를 건의할 수 있다.
- 교차인증(Cross Certification) : 교차 인증서는 한 CA가 다른 CA에게 발급한 인증서이다. 두 CA는 교차 인증서 발급에 필요한 정보를 교환한다.

3.3.2 PKI의 관리 대상

1) 공개키 인증서

공개키 인증서(public-key certificates)는 네트워크 내의 신뢰할 수 있는 사용자에게 공개키를 분배하는 안전한 수단이다. PKI에서 공개키 인증서의 발행 대상은 인증기관, 사용자 그리고 서버 등이다. 인증기관에게는 상위의 인증기관이 인증기관의 적법성을 인정하기 위해 발행하고, 사용자와 서버에 대해서는 사용자의 신원, 서버의 적법성을 증명하기 위해 인증기관이 발행한다.

공개키 인증서는 여러 면에서 자동차 운전면허증과 유사한 성격을 갖는다. 인증서와 면허증은 모두 신뢰할 수 있는 기관에 의해 발행되며, 사용자의 신분과 권리를 보장한다. 인증서에는 기본적으로 공개키에 관한 정보, 사용자가 속한 그룹에서의 사용자의 신분, 인증서에 포함된 내용을 검증한 기관의 이름 등이 포함되어 있다.

여러 가지 형태의 인증서가 이용되고 있다. 그 예로 Pretty Good Privacy(PGP), Internet Protocol Security(IPSec) 등을 들 수 있으나, 현재 가장 널리 사용되는 인증서는 국제통신연합(International

Telecommunication Union; ITU)의 X.509 v.3이다. ITU의 최초 인증서 X.509는 1988년 발표되었으며, 1993년, 1995년 두 차례에 걸쳐 수정되어 버전 2, 3이 발표되었다.

인증서 X.509는 다음의 내용을 포함한다.

Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer Name
Validity(Not Before/Not After)
Subject Name
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Signature

〔그림 3.7〕 인증서 X.509의 구조

- Version : 인증서 X.509의 버전 1, 2, 3을 나타낸다.
- Certificate Serial Number : 각각의 인증서에 유일하게 부여되는 정수의 일련번호로 인증기관이 생성한다.
- Signature Algorithm Identifier : 인증서에 서명하는데 사용된 알고리즘을 나타낸다.
- Issuer Name : 인증서를 생성하고 서명한 인증기관의 이름을 기록한다.
- Validity : 인증서가 사용될 수 있는 유효기간을 날자와 시간으로 표시한다.
- Subject Name : 인증서에 해당하는 비밀키의 소유자에 대한 식별 영역이다.

- Subject Public Key Information : 사용자의 공개키와 공개키가 사용될 수 있는 알고리즘과 변수에 대한 정보를 포함한다.
- Issuer Unique Identifier : 발행자의 부가 정보를 포함하는 영역으로 버전 2이상에 해당된다.
- Subject Unique Identifier : 사용자의 부가 정보를 포함하는 영역으로 버전 2이상에 해당된다.
- Extensions : 인증정책 등을 포함하는 영역으로 버전 3에 추가되었다.
- Signature : 인증서 내용 전반에 관한 서명 영역이다.

2) 상호인증서

PKI는 하나의 독립된 그룹 안에서 이루어지는 경우보다는 국가들, 정치단체들, 사업체들 사이에 연관을 갖고 구성된다. 그러나 각 PKI 그룹의 각 인증기관의 정책에 따라 독자적으로 운영되고, 독자적인 규정에 정하고 있다. 상호인증은 서로 다른 도메인에 가입된 인증기관과 사용자들이 상호 교류할 수 있는 여건을 제공한다.

상호 인증(cross certificate)이란 인증기관 사이에 상호인증협약에 따라 서로를 인증하므로써 신뢰를 형성하여 한 도메인의 사용자가 다른 도메인의 사용자를 신뢰할 수 있도록 하는 것이다.

3) 인증서 취소목록

인증서의 유효기간이 만료되기 전에 비밀키의 노출과 같은 상황이 발생하면 이 비밀키에 해당하는 공개키의 인증서는 효력이 상실된다. 인증기관은 효력이 상실된 인증서에 대한 목록을 작성하여 관리한다. 인증서 취소목록(CRL; Certificate Revocation List)에는 취소목록의 작성기관, 작성시점, 취소 사유, 인증기관의 서명 등을 포함한다.

3.4 침입탐지시스템

3.4.1 시스템 개요

침입탐지시스템(IDS; Intrusion Detection System)은 정보시스템 또는 네트워크로부터 보안 관련 정보들을 수집·분석해 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응행동을 수행하는 기능을 포함하고 있는 시스템으로 정의된다. 1980년에 미국의 Anderson은 침입에 대한 기본 개념으로 "비 인가된 정보로의 접근 및 정보 조작, 그리고 시스템 무기력화에 대한 고의적이고 불법적인 시도"라고 규정하였으며, 1987년 미국의 Denning은 실시간 침입탐지 모델을 발표하고 침입탐지전문가시스템(IDES; Intrusion Detection Expert System)을 "허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등의 불법적인 행위에 대한 예방이 실패하였을 경우 취하는 대응책으로, 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하여 실시간으로 대응 처리하는 시스템"으로 정의하고 있다.

침입탐지시스템에 대한 연구동향은 80년대 초에 호스트기반 침입탐지시스템이 주류를 이루고 있었으나 미국 데이비스대학에서 개발한 NSM(Network Security Monitor)으로부터 네트워크 기반의 침입탐지시스템이 개발되기 시작하였다. 데이비스대학은 미 공군 암호지원센터, 로렌스 리버모어 국립연구소, 헤이스택 연구소와의 공동연구를 통해 호스트 기반 및 네트워크 기반 침입탐지시스템을 통합 운용하기 위한 모델인 DIDS(Distributed Intrusion Detection System)의 개발에 참여했다. 1990년 이후 침입탐지시스템에 대한 연구는 더욱 가속화되어 분석모델에 대한 연구를 기반으로 기능적인 성장을 이루게 된다. 스탠포드대학에서는 침입탐지전문가시스템 모델을 확장한 NIDES(Next generation IDES)의 개발에 성공했고 분산환경

침입탐지시스템인 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Distribution)로 모델을 확장하고 있다. 또한 90년대 퍼듀대학에서는 Colored PetriNet 기술을 이용하여 IDIOT (Intrusion Detection In Out Time)를 개발했으며 미 산타바바라의 UCSB(University of California)에서는 상태전이 모델을 이용하여 STAT(State Transition Analysis Tool)과 Net-STAT를 개발했다. 현재 대표적인 상용제품에는 Intruder Alert(Axent), Real Secure(ISS), Stalker(TIS) 등이 있다.

3.4.2 침입 공격 형태

1) 전통적인 공격 기법

일반적인 공격절차는 가장먼저 공격대상에 대한 "정보수집 단계"이며, 그 다음 수집한 정보를 바탕으로 "시스템침입 단계"를 거치게 된다. 그리고 지속적인 침입 및 다른 시스템의 공격을 위한 "공격전이 단계"를 거치게 된다.

가) 정보수집 단계

정보수집은 공격의 첫 번째 단계로 공격대상 네트워크에 대한 정보를 파악하는 것이다. 주로 네트워크 토폴로지, 시스템 OS, 네트워크 장치의 종류, 그리고 WWW, FTP 등 공격대상 네트워크가 제공하는 서비스와 해당 버전에 대한 정보를 수집한다. 정보수집 방법은 스캔 공격도구를 이용하는 것에서부터, 다양한 네트워크 서버가 제공하는 정보를 수집하는 방법에 이르기까지 상당히 다양하며, 침입차단시스템을 우회할 수 있는 방법도 존재한다.

(1) 시스템 및 서비스 탐지

공격 대상 네트워크에 시스템이 있는지를 파악하기 위하여 일반

적으로 "PING"을 이용한 공격도구를 사용한다. 또한 DNS 서버를 조회하여 어떠한 시스템이 있는지를 파악할 수도 있다. 시스템의 존재여부에 대한 정보수집이 끝나면, 각 시스템이 어떠한 서비스를 제공하고 있는지를 점검하기 위해 열려진 포트를 점검한다. 특히 버그가 있는 서비스를 집중적으로 조사하게되며, 이러한 과정은 Sscan, Mscan, Vanilla scaner 등 "취약점 스캐너" 또는 "포트 스캐너"라는 자동화된 공격도구를 이용한다. 일반적으로 시스템의 존재여부와 서비스에 대한 스캔은 동시에 이루어진다.

(2) 운영체제(OS) 탐지

좀더 세밀한 공격을 위하여 해당 시스템의 OS 버전에 대한 정보수집을 한다. OS 버전을 탐지하는 기술은 "IP stack fingerprinting"이라는 특성을 이용한다. 시스템을 구별해내는 방법이다. 대표적인 도구로는 Queso, Nmap을 들 수 있다.

(3) 네트워크 토폴로지/방화벽 필터링 규칙 탐지

네트워크 토폴로지는 호스간의 거리를 나타내는 "Hop count"를 이용하여 알아낼 수 있으며, "Traceroute" 프로그램을 응용한 공격도구를 이용한다. 또한 방화벽에 의해 보호되는 시스템에 대한 정보를 수집하는 방법도 존재한다. 이러한 공격은 대부분의 방화벽이 필터링하지 않는 ICMP 패킷이나 Traceroute 패킷을 이용하며, 대표적인 공격도구로는 Firewalk, Hping 등이 있다.

(4) 네트워크 서버의 정보 수집

DNS, SNMP, Sendmail, NetBIOS 등 일반 네트워크 서버가 제공하는 정보를 수집하여 공격에 유용하게 사용할 수 있다. DNS의 경우 "Zone transfer" 또는 일반적인 Query를 이용하여 등록된 호스트의 정보를 알 수 있으며, 잘못 설정된 SNMP는 네트워크의 토

폴로지 및 각 종 네트워크 정보를 알려준다. 또한 라우터를 통하여 중요한 정보를 알아낼 수 있는 방법도 존재한다. "정보수집단계"는 공격대상 네트워크에 어떠한 호스트가 있으며, 해당 호스트가 어떠한 서비스를 제공하는가, 그리고 네트워크가 어떻게 구성되어 있는가를 파악하여 최종 공격 대상을 찾아내는 단계이다.

나) 시스템침입 단계

시스템침입 단계는 실제 개별 시스템에 침입하는 단계로 정보수집단계에서 수집한 정보를 바탕으로 가장 취약한 부분을 공격하게 된다. 일반적으로 버그가 있는 네트워크 서버를 공격하게 되는데 sadmind, amd, amountd, statd, POP, Imap 등 각종 서버의 원격 버퍼 오버로우(buffer overflow) 취약점을 공격한다. 그밖에 서버의 설정 오류를 이용하는 방법도 있으며, 패스워드 파일을 획득한 경우에는 "Crack"이라는 과정을 거쳐 패스워드를 해독하여 침입할 수도 있다. 시스템 침입단계에 사용되는 방법은 이미 잘 알려져 있고 많은 공격도구들이 공개되어 있으며 체계화되어 있다. 따라서 시스템/네트워크에 대해 깊은 지식이 없는 소위 "Script kiddies"라 불리는 해킹 관심자들도 누구나 손쉽게 시스템에 침입할 수 있다.

다) 공격전이 단계

"공격전이 단계"는 1차적인 시스템 침입 이후에 일어나는 침입을 말하는데, 1차적인 침입으로부터 얻은 정보 및 추가 작업을 통하여 시스템 침입을 확대하고 다른 시스템에 침입하는 단계이다. 일단 시스템 침입흔적을 제거하게 된다. 또한 정보수집단계로 인하여 남은 흔적도 제거하게 된다. 또한 일반계정으로 침입한 경우에는 충분한 권한(유닉스의 경우 Root 권한)을 갖기 위하여 로컬 시스템의 취약점을 공격하게 되는데, 대부분의 시스템에서 이러한 취약점을 갖고 있다. 또한 제 침입을 위하여 비인가된 접근을 제공해

주는 "백도어"를 설치하게 되는데 이러한 백도어는 데몬 서비스 형태, 또는 서비스의 비정상적인 설정 등을 이용하여 포트를 열어 놓게 된다.

이러한 작업을 손쉽게 해주는 툴킷이 존재하는데 흔히 "Rootkit"이라 부르며 시스템 종류별로 다양한 도구가 존재한다. 공격자는 시스템 침입에 성공한 시스템을 이용하여 보다 깊이 있는 공격을 수행하게 된다. 가장 전통적인 방법은 "Password Sniffer"로 자신이 침입한 시스템과 "신뢰관계"에 있는 시스템의 정보를 알아내어 별도의 공격을 하지 않고도 인가된 사용자로서 가른 시스템을 공격할 수도 있다. 가장 대표적인 예가 "r" 계열의 명령을 사용하는 경우이며, 이외에도 데이터베이스에 접근할 수 있는 경우도 있다. 공격전이의 또 다른 경우는 침입에 성공한 시스템을 다른 네트워크를 공격하기 위한 경유지로 사용하는 것이다. 이 경우 다시 정보수집단계부터 새로이 시작하게 된다. 경유지를 이용하는 이유는 공격자의 흔적을 추적하기 어렵게 하기 위함이며, 많은 경우에 있어 최소 2~3개 사이트 이상을 경유지로 사용한다.

2) 새로운 공격 기법

전통적인 공격모델의 변화는 미국에서 보안 시스템이 보편화되면서 이를 극복하고자 하는 공격자들의 노력에서 시작된다. 즉, 공격자와 방어자의 뚫고, 막는 경쟁으로 인한 것이다. 현재의 보안모델에서는 일반적으로 공격자가 항상 우세하며 방어자는 알려진 공격방법에만 대응하는 방식의 사이클을 가진다. 또한 인터넷이 실세계의 중요한 일부가 되면서 "사이버테러", "사이버범죄" 또한 구체화, 조직화되는 것도 전통적인 공격모델의 변화에 큰 영향을 주고 있다. 전통적인 공격기법 변화의 가장 큰 원동력은 방어자의 보안수준 향상이다. 침입차단시스템 및 침입탐지시스템의 보편화는 전

통적인 공격기법에 매우 효과적인 대응수단을 제공한다. 그리고 여러 국가의 CERT 간의 공조체계도 공격자의 활동범위를 좁혀가고 있다. 하지만 이러한 장벽을 극복하고 성공적으로 시스템에 침입하기 위한 기술 및 도구들이 최근 몇 년간 지속적으로 개발되고 있다. 대표적인 도구로는 hping, Firewalk, Loki Project, pcap, libent 등을 들 수 있다. 그리고 이러한 변화 중 주목을 끌만한 것은 1998년 중반에 공개된 백오리피스이다. 이러한 기술 및 도구들의 등장은 새로운 공격기법의 패러다임으로 가는 과도기이며, 기반 기술이 된다.

가) 백오리피스(Back Orifice)

백오리피스의 출현은 공격기법의 새로운 패러다임에서 큰 위치를 차지한다. 백오리피스는 새로운 네트워크 공격기법의 많은 특징을 내포하고 있으며, 가장 성공적인 공격과 명성을 이루었다. 다른 공격도구와 마찬가지로 백오리피스 또한 공격자에게 인가 받지 않는 접근 권한을 제공한다. 이와 더불어 새로운 기능으로는 패킷 릴레이 기능을 가지고 있으며, 새로운 공격 프로그램을 추가할 수 있는 기능을 가지고 있다. 이는 최근의 정보기술에서 나타나고 있는 에이전트 개념과 비슷한 개념으로 제품의 기능 및 버전업을 자동으로 하는 것과 비슷하다. 정보기술의 발전이 공격기술에도 적용되고 있는 것이다. 패킷 릴레이 기능은 공격자가 다시 시스템에 침입하지 않고 이미 침입에 성공한 시스템을 이용하여 다른 시스템을 공격하는데 이용할 수 있음을 의미한다. 물론 윈도우 시스템이라는 특성에서 연유된 것이기는 하지만 최근 이러한 형태의 공격도구들이 유닉스에서도 발견되고 있다.

백오리피스는 바이러스에 버금가는 전파력을 가졌다. 전파 매체가 전자메일, 웹을 통한 다운로드 등 보안시스템을 우회할 수 있는 수단을 이용하기 때문이기도 하지만, 언론에서 조장한 영향

이 적지 않다. 또한 제작자의 고의적인 의도가 있었는지는 모르겠지만 백오리피스의 재미있는 기능들은 해킹의 개념을 대중화하였고, 스크립트 키디(Script kidies)라 불리는 공격자보다도 수준이 낮은 "워너비"(Want to be, 해커가 되고 싶어하는 사람)들에게 해킹을 맛을 보여주고 도구를 제공함으로서 백오리피스를 널리 퍼지게 하였다. 이러한 면에서 백오리피스는 가장 성공적인 공격도구라고 말할 수 있다. 사실 백오리피스의 진정한 위협은 이러한 워너비들에 의한 공격이 아니다. 워너비의 호기심으로 인하여 이미 인터넷상의 수많은 시스템에 백오리피스를 비롯한 비슷한 종류의 공격도구들이 설치되었고, 이러한 시스템은 향후 더 강력한 공격을 수행할 수 있는 공격도구로 바뀔 수 있다는데서 그 위협이 존재한다. 예를 들면, 백오리피스가 설치된 1,000개의 시스템 정보를 가진 공격자가 새로운 분산서비스공격 도구를 만들고 이를 백오리피스를 이용하여 시스템에 인스톨한 뒤 공격을 수행한다고 가정할 수 있다.

백오리피스의 또 다른 특징으로는 일반 사용자를 공격 대상으로 했다는 점이다. 보안 인식이 확산되면서 서버 및 네트워크에 대한 보안이 향상되었고 결과적으로 공격자는 보안에 대한 인식이 없는 일반 사용자들을 공격대상으로 삼은 것이다. 그리고 일단 일반 사용자를 대상으로 일차적인 공격이 성공하고나면 공격전이 단계를 거쳐 서버에도 침입할 수 있는 기회를 갖게 된다. 백오리피스의 키스트로크 로깅기능을 이용하거나 PC에 저장된 패스워드 파일을 유출하여 서버에 침입할 수 있다.

나) 백도어

스캐닝 기술과 더불어 가장 빨리 변화하고 있는 공격 기술 분야가 백도어이다. 앞서 설명한 것처럼 백도어는 침입자가 아무런 인증이 없이도 로그기록을 남기지 않고 시스템에 다시 들어올 수 있도록

하는 수단을 말한다. 하지만 전통적인 백도어 기술은 이미 잘 아려져 있고 대부분의 모방 시스템에서 이를 탐지할 수 있어 공격자에게는 큰 위험부담을 안겨준다. 최근에 발견되는 백도어는 특정 포트를 열거나 네트워크 커넥션을 필요로 하지 않는다. Raw socket를 열어 특정 패킷이 오기를 기다린다. 그리고 조건에 맞는 패킷이 오면 그에 적절한 응답을 제공한다. 이러한 기술을 Tunneling 기술이라 하며 TCP, UDP, IP 등 다양한 프로토콜 계층에서 구현될 수 있으며, HTTP 등 응용프로그래밍 계층에서도 구현될 수 있어 방화벽을 우회할 수 있는 수단을 제공한다.

또한 침입탐지시스템을 우회하기 위하여 암호화 기능을 제공하기도 한다. 기존의 백도어와 같이 공격자가 접속해 오는 방식의 기술은 방화벽에 의하여 좌절될 수 있다. 이를 극복하기 위한 새로운 종류의 백도어 기술도 등장하고 있는데, 이는 백도어가 주기적으로 외부의 공격자에게 신호를 보내고 공격자는 이를 감지하여 커넥션을 맺는 방식으로 대부분의 사이트가 외부로 나가는 패킷에 대한 필터링을 하지 않는 보안모델의 취약점을 이용한 것이다. 네트워크 백도어 이외에도 시스템에서 특정 파일이나 프로세스를 숨기기 위한 기술도 발전하고 있다. 단순히 login, ps, ls, find 등과 같은 프로그램을 변조하는 것이 아니라 커널 레벨에서 이러한 은닉기능을 구현한다. 이미 Linux와 Solaris에 대한 커널 백도어가 공개되었다. 이러한 커널 백도어는 중요 시스템 파일에 대한 무결성을 검사하는 방법으로는 사실상 탐지하기가 불가능하다. 백도어의 형태 및 기능 또한 다양화되고 있다. 공격자가 백도어로 연결을 맺는 서버 개념의 백도어에서 벗어나 Revers Pimpage와 같이 클라이언트 형식의 백도어가 있으며, Tunneling 기술을 이용하여 모듈 업그레이드, 원격 공격명령 수행 등을 수행하는 에이전트 형태의 백도어도 존재한다. 이러한 기능이 추가되고 있다는 사실은 공격자가 지속적으로 백도어를 이용하겠다는 의미이며, 수 천대의 호스트가 공격에 사용되었던 최근의 DDOS 공

격에서처럼 향후의 공격을 준비한다는 의미로 받아들일 수 있다.

다) 네트워크 스캐닝

방화벽의 도입은 전통적인 네트워크 스캐닝 공격을 효율적으로 차단해 주는 보안 수단이 된다. 하지만 방화벽을 우회할 수 있는 공격기술 또한 많이 발전하였다. 대부분의 시스템에서 네트워크 패킷을 스니핑할 수 있도록 해주는 pcap 라이브러리, 임의의 패킷을 만들어 보낼 수 있도록 해주는 libnet 라이브러리의 공개는 방화벽을 공격하기 위한 공격도구의 기반기술이 되며, Firewalk, hping, nmap 등과 같은 고도의 스캐닝 도구에 사용된다. 공격자의 시스템에서 직접 스캔을 시도하는 전통적인 공격기법과 달리 제3의 서버를 이용하여 공격대상의 네트워크를 스캐닝할 수 있는 FTP bounce attack, DNS Bounce attack 등의 기술이 많이 사용되고 있으며, hping과 같이 소스 주소를 속여 스캔공격을 할 수 있는 방법도 존재한다. 그리고 Wingate, 백오리피스 등의 패킷 릴레이 기능을 제공하는 시스템을 이용함으로서 공격자의 위치를 노출시키지 않는다. 또한 공격자가 심어놓은 백도어 형의 공격 에이전트는 자동 또는 원격 명령으로 분산 네트워크 스캐닝 및 공격을 수행하고 그 결과를 공격자에게 실시간으로 전달하거나, 공격 경로를 따라 공격자에게 전달할 수도 있다. 이는 최근 발견된 Millennium Internet Worm, DDOS tools, VBS/NetLog 웜 등에서 그 가능성을 확인할 수 있다.

라) 인터넷 웜(Internet Worm)

인터넷에서 많은 사이트들의 네트워크 구조가 획일화되고 그리고 몇몇 시스템 및 솔루션이 대다수의 시장을 차지하게 되면서 이러한 시스템 및 솔루션의 새로운 취약점은 그 파급효과가 커지고 있다. 예를 들면, Solaris는 현재 워크스테이션 분야에서 가장 많은 시장을 확보하고 있다. 그리고 최근에 지속적으로 발견되고 있는 RPC

관련 취약점은 수많은 Solaris 시스템을 공격하는데 매우 효과적이었다. 이러한 획일화는 결국 인터넷 웜과 같은 자동화된 공격도구의 출현을 야기 시키고 있다. 1998년에 ADM Interner worm(ADMworm)이 발견되었으며, 1999년에는 ADMworm과 유사한 Millennium Internet Worm이 발견되었다. 이는 Imap4 v10.x, Qualcomm poper, Cind with iquery, 그리고 rpc.mountd services 등 최근의 원격 해킹 취약점에 대한 공격 기능과 다양한 추가 기능이 포함된 진보된 웜으로 국내 침해사고에서도 발견된 적이 있다. 이러한 인터넷 웜은 자동으로 임의의 공격 목표를 정하고 공격이 성공하고 나면 그 지점부터 또 다른 공격을 시작하므로 위의 취약점을 가진 많은 사이트가 공격을 당할 수 있다. Trin00, TFN 등 DDOS 공격도구 또한 위와 비슷한 종류의 인터넷 웜을 통하여 서버에 설치될 수 있는데, 실제로 몇 몇 침해사고에서 인터넷 웜과 비슷한 기능의 스크립트들이 발견되었다.

마) 윈도우용 공격도구

윈도우 시스템 기반의 공격도구가 증가하고 있다. 앞서 설명한 바와 같이 보안인식이 없는 일반 사용자를 대상으로 공격함으로서 보안시스템을 우회할 수 있기 때문이다. 그리고 윈도우 시스템의 성능 향상 또한 공격자로 하여금 윈도우 시스템을 매력적인 공격 목표로 만들고 있다. 많은 유닉스 시스템 기반의 공격 프로그램이 윈도우용으로 제공되고 있으며, Tfin00의 윈도우 버전인 Wintrin00가 발견되기도 했다. 백오리피스와 유사한 종류의 공격도구는 그 수가 수백 가지에 이르며, 최근 많이 발견되고 있는 E-mail을 전파 매체로 사용하는 매크로 바이러스 관련 침해사고에서 Trojan Horse와 매크로 바이러스 관련 사고가 가장 큰 부분을 차지하고 있다. 이러한 흐름은 공격도구들이 자동화되고 있음을 의미하며, 향후 패키지로 발전할 수도 있음을 보여준다.

3.4.3 침입탐지시스템 기능

침입탐지시스템의 기본기능은 보안관련 정보수집, 수집된 정보의 분석 및 침입 판정, 보고 및 대응행동으로 요약할 수 있는데 이러한 기능 구현을 위한 침입탐지시스템의 일반적인 구조는 감사정보 수집 및 축약, 패턴생성, 사건분석 및 침입 판정 그리고 사건보고 및 대응행동 모듈로 구성되어 있다. 감사정보수집 기능은 감시대상 시스템 또는 네트워크로부터 보안 분석을 위한 감사정보를 수집하며, 정보 제공원에 따라 시스템의 로그파일, 시스템 호출 함수 등으로부터 정보를 수집하는 호스트기반 침입탐지시스템과 네트워크 패킷으로부터 감사정보를 수집하는 네트워크기반 침입탐지시스템으로 분류한다. 감사축약 기능은 방대한 감사정보의 분석으로 인한 탐지효율의 저하 및 시스템 성능 저하를 미연에 방지하고 중복된 감사정보를 제거함으로써 보안 분석을 위해 수행되는 기능을 말한다. 이때 축약된 감사정보는 일반적으로 침입탐지시스템이 정의하고 있는 정형화된 감사 기록으로 변형되어 추후 분석을 위하여 감사 데이터베이스에 저장된다. 이렇게 축약된 감사정보는 사건분석 및 침입 판정 모듈에 의해 감사분석이 수행되며 이러한 과정이 침입탐지시스템의 핵심이라고 볼 수 있다. 침입 판정을 위한 분석 기술은 오용탐지(Misuse Detection) 기법과 비정상행위탐지(Anomaly Detection)기법으로 구분된다. 오용탐지기법은 일반적으로 침입으로 알려져 있는 행위 또는 비정상적인 행위를 패턴으로 정의하고 수집된 감사사건이 미리 정의된 패턴과 일치하는 경우에 이를 침입(또는 오용)으로 판정한다. 일반적으로 오용탐지기법은 패턴비교(Pattern Matching) 기술을 사용하며 현재 많은 상용제품들이 오용탐지기법을 사용하고 있다. 비정상행위탐지기법은 정상적인 행위에 대한 프로파일을 생성하고 실제 수집되는 감사정보를 프로파일과 비교해 정상행위로부터 벗어나는 비정상행위를 탐지하는 기법이다. 새로운

침입 또는 오용의 탐지에 효율적이라는 장점이 있는 반면, 탐지비용이 높고 악의적인 목적으로 자신의 행위패턴을 서서히 학습시키는 사용자에게는 취약하다. 또한 데이터베이스의 정확도에 따라 정상행위를 침입으로 분류하는 폴스 포지티브 탐지(False Positive Detection) 오류를 범할 수도 있다. 비정상행위탐지 모델은 데닝의 침입탐지모델이 기반을 이루고 있는데 현재 많이 적용되고 있는 탐지모델로는 수량적 분석, 통계적 분석 그리고 신경망 기반 모델 등이 있다. 수량적 분석 모델은 탐지 규칙 또는 속성값에 수치적인 값을 사용하여 침입 또는 오용을 탐지하는 방식으로서 대표적인 수량적 분석 모델로는 임계값에 기초한 탐지방식이 있으며 현재 많은 침입탐지시스템이 임계값을 통한 침입탐지방식을 사용하고 있다. 그러나 임계값 기반 비정상행위탐지 방식은 침입 판정을 위한 정확한 임계값 설정에 난점으로 인해 폴스 포지티브 탐지가 증가한다는 문제점이 있다. 사건보고 및 대응행동 모듈은 침입으로 판정된 사건을 보안 관리자에게 보고하고 이에 대한 대응행동을 자동 혹은 수동적으로 수행하며 통계적 보고 기능을 수행한다. 대응행동 방식은 일반적으로 수동적 대응과 능동적 대응으로 구분된다. 사건 발생과 행동 수행 사이의 시간적인 차이가 시스템에 큰 보안위협을 초래할 수 있으므로 대응에 관한 실시간적인 요소가 고려돼야 한다. 또한 침입탐지시스템은 감시대상 시스템 또는 네트워크로부터 발생하는 침입사건들에 대한 통계적인 보고서 작성 기능을 제공하여 보안 관리자의 보안상황과 향후 분석을 지원한다.

3.4.4 침입탐지시스템 전망

전통적인 공격기법들은 정보수집 단계에서는 하나의 시스템에서 단일의 공격대상 시스템이나 또는 대규모의 광범위한 네트워크를

대상으로 스캔공격을 수행하게 된다. 취약점 스캔공격 도구를 분류해보면 단일 취약점을 스캔하는 도구와 다수의 취약점을 스캔하는 도구로 구분될 수 있으며, 이들 도구는 하나의 시스템 또는 네트워크 블록 단위로 스캔하는 기능을 가지고 있다. 또 다른 특징은 서버 중심의 공격기법이다. 대부분의 공격도구(실제 시스템 침입에 사용되는 공격용 스크립트로 소위 "Exploits"라고 불리 운다.)는 서버의 취약점을 공격하며, 백도어나 트로이 목마도 공격하고자 하는 시스템에 서버를 설치하여 공격자의 클라이언트에서 침입하는 방식을 사용한다. 전통적인 공격모델에서의 침입경로는 다단계의 경로를 거치게 된다. 공격자는 자신의 흔적을 감추기 위해 2~3개 이상의 시스템에 차례로 침입하여 최종 공격 대상 시스템을 공격한다. 결국 침입을 당한 호스간에 체인을 이루고 마지막의 피해 시스템은 바로 전 단계의 시스템에 대한 정보만을 가지게 된다. 물론 전 단계의 시스템에서는 이미 공격자가 자신의 흔적을 제거하기 때문에 역추적은 거의 불가능하게 된다. 이러한 체인 모델에서 공격자는 각각의 시스템에 침입할 때마다 취약점 스캐너 등을 사용하게 되는데, 이 경우 상당한 시간을 필요로 하기 때문에 공격자는 백도어 등을 통하여 나중에 다시 시스템에 들어와서 정보를 가져가야 하는 위험이 존재한다.

한편 최근에 발견되는 새로운 공격기법들은 에이전트화, 분산화, 자동화, 은닉화의 특징을 갖고있다. 먼저 에이전트화는 공격자가 침입한 시스템에 다시 로그인하거나 또는 백도어를 통하여 재침입하고 다른 시스템을 공격하는 공격전이 단계를 거치지 않고 원격으로 조정 가능한 에이전트(agent)형의 백도어를 설치하여 다른 시스템을 공격하는 방법을 말한다. 이는 공격자가 매번 로그파일에서 침입 흔적을 지워야 하는 번거로움을 없애주며, 많은 시스템을 이용하여 분산 공격을 수행할 때 매우 효과적인 방법이다. 다음으로 분산화는 침입탐지시스템 등의 보안 시스템을 우회하기 위하여 많

은 수의 시스템에서 단일 시스템 또는 다수의 시스템을 공격하는 방법을 말한다. 분산 공격은 원격 명령으로 공격을 수행하거나 또는 패킷을 릴레이 해주는 에이전트화 된 공격도구를 이용함으로서 공격자의 위치를 감출 수 있으며, 보다 빠르게 공격대상 시스템에 대한 정보를 수집할 수 있다. 그리고 자동화는 인터넷 웜 및 윈도우용 공격도구, 그리고 최근 침해사고에서 발견되는 자동 공격 스크립트의 증가는 공격도구들이 자동화되고 있음을 의미한다. 그리고 이러한 자동화는 분산 네트워크 공격을 가능하게 한다. 끝으로 은닉성은 공격자의 위치를 은닉시킬 수 있는 공격기법으로 에이전트와 공격자간의 통신은 암호화 및 Tunneling 기법을 사용하여 탐지하기 어렵도록 한다. 이와 같이 침입의 형태는 점점 다변화되고 침입 도구의 고도화로 인해 보안위협을 날로 증가할 것이다. 따라서 침입탐지시스템은 정보시스템 보호의 핵심적인 역할을 수행할 것으로 예상된다.

이러한 침입 형태에 대응하기 위한 탐지시스템의 발전 전망은 첫째로 다양한 침입에 대한 탐지효율을 향상시키는 기술의 발전, 둘째로 보안 시스템들과의 연계를 통한 통합 보안관리 인프라의 구축을 들 수 있다. 먼저 침입탐지 효율을 높이기 위해서 현재 침입탐지시스템의 고속성, 확장성, 연동성에 관한 연구가 활발히 진행되고 있다. 침입탐지시스템의 고속성은 자료의 분산처리 및 감사정보 통신의 고속화 등의 방향으로 연구되고 있으며 대규모 네트워크에서 침입탐지를 적용하기 위한 확장성은 방대한 양의 정보처리 효율을 높이기 위해 분산 구조로 감사정보를 수집하며, 계층적인 구조로 분석 처리를 수행하는 모델로 연구되고 있다. 침입탐지시스템들 간에 정보와 처리 자원을 공유하고 협력 처리를 함으로써 탐지효율을 극대화하려는 연동성에 대한 연구는 감사정보의 정형화, 프로토콜의 표준화, 시스템 구조의 일반화 등의 방향으로 추진되고 있다. 한편 다른 보안 컴포넌트들과의 연계를 통한 통합 보

안관리 인프라를 구축하여 네트워크의 보안 수준을 높이려는 노력은 침입탐지시스템과 방화벽(firewall) 시스템과의 연동을 들 수 있는데, 침입탐지시스템과 방화벽 시스템을 일체형으로 하나의 시스템으로 통합하는 접근방식과 각각의 시스템을 연계하여 통합하는 접근방식이 시도되고 있다.

제4장 정보전 대응전략

시스템에 대한 외부 또는 내부로부터의 공격에 대한 방어, 탐지, 반응의 방법을 제공하고, 방해로 인해 작동이 멈춘 중요 서비스들을 가능한 효과적으로 되살리는 해결책을 제시하는 것을 내용으로 하는 정보 보증은 그 중요성이 크게 부각되고 있는 상황이다.

인터넷을 중심으로 한 정보통신기술의 발전과 더불어 정보공격 또는 사이버테러의 기술도 함께 발전하고 있으며, 최근의 정보공격 또는 사이버 테러의 형태는 매우 다양하고 그 수준도 심각한 상황에 이르게 되었다. 이에 미국과 영국을 주축으로 한 선진 각 국은 정보보증의 중요성을 심각하게 인식하고 이에 대한 대응 전략의 마련에 박차를 가하고 있다. 우리 나라에서도 정보통신부를 중심으로 대책을 마련하고 있으며, 군에서도 이를 위한 전문 인력을 양성하고 상시 대비체계를 구축해야 할 것이다.

4.1 미국의 정보보증 전략

미국 국방부는 적시 적소에 허가된 인원에게 유효 적절한 정보를 주기 위해 정보 네트워크 시스템을 사용한다. 그러나 빠른 네트워크 기술의 진보와 상업망과의 의존성이 커짐에 따라 미국 국방부의 정보 네트워크 시스템은 여러 가지 공격에 대해 위태롭게 되었다. 미국의 안보를 결정짓는 귀중한 정보를 어떻게 보호하는가가 중요한 문제가 된다. 정보 보증은 침입, 외부로부터 또는 내부로부터의 공격에 대한 방어, 탐지, 반응의 방법을 제공하고, 방해로 인해 작동이 멈춘 중요 서비스들을 가능한 효과적으로 되살리는 해결책을 제시해 준다. 5가지 보안 목표로 알려진 신뢰성(confidentiality),

완전성(integrity), 무결성(availability), 부인 방지(non-repudiation), 그리고 인증(authentication)을 달성하기 위한 목적으로 정보 보증은 현재 큰 주목을 받고 있다. 미국 국방부는 정보 보증을 다음과 같이 정의하였다: "정보 보증은 5가지 보안 목표를 확실히 지키면서 정보 시스템을 보호해 주는 정보-작전(information operation)이다. 외부, 내부의 공격으로부터 보호, 탐지, 대처하는 능력을 이용하여 정보 시스템을 복원할 수 있도록 해주는 것이다." 정보 보증은 시스템 보호와 전투 지원에 방해받지 않는다는 확신을 넘어, 갈수록 취약해지는 미국의 상호 연결된 기반 구조에 대한 안전성 구현에 필수적인 요소이다. 일반적으로 정보보증의 정의를 내리면, 기반 구조를 구성, 운영 및 통제하는 정보와 정보기술에 대한 침해에 대한 보호(protection), 신뢰성(confidentiality), 가용성(availability)을 보장하는 것을 말한다. 주요 기반 구조를 보호하기 위한 정보보증은 침해에 대한 방어, 기반 구조 파괴-침입-침해에 대한 탐지, 서비스의 복구, 추후의 침입 혹은 위협에 대응하는 대응 체계 등 4가지 큰 축으로 구성된다. IATF(Information Assurance Technical Framework)는 정보보증을 이루기 위해 필요한 여러 기술들을 구현한 프레임워크이다. NSA(National Security Agency)에서 후원하는 웹 사이트(http://www.iatf.net)에서는 IATFF(Information Assurance Technical Framework Forum)라는 포럼을 개최하여, 정보보증과 관련된 사용자 요구 사항, 문제점 등을 반영하여 IATF를 계속 유지, 발전시키고 있다.

4.1.1 정보보증 구조

가. 정보 기반 구조의 정의

IATF는 정보 기반 구조상에서의 정보 보증을 다룬다. 여기서 정보 기반 구조란 통신망, 컴퓨터, 데이터베이스, 시스템 관리, 응용

프로그램, 단말기기 등을 일컫는 말이며, 전 세계, 국가, 또는 특정 영역 등, 어떤 지역 수준에서 존재하게 된다. 전 세계 수준의 정보 기반 구조는 특정한 개인이나 조직에 의하여 제어, 관리가 이루어 질 수 없고, 기업, 학교, 정부와 같은 많은 조직들에 의해 공유되어야 한다. 인터넷과 전화망이 바로 전 세계 수준의 정보 기반 구조라 할 수 있다. 외부와 통신을 하는 대부분의 조직들은 전 세계 수준의 정보 기반 구조에 의존하게 되는데, 이 때 가상망, 전용망, WAN, 주문 방식의 정보망(customized network)등을 사용한다. 국가 수준의 정보 기반 구조는 국가가 정부 업무나 상업적 업무를 위해 사용하는 정보 기반 구조 모두를 포함한다. 국가 수준 정보 기반 구조의 가장 대표적인 예가 미국의 PDD(Presidential Decision Directive)-63에 정의되어 있는 중대 기반 구조(critical infrastructure)이다. 다국적 기업이 성장하기 전이나 인터넷이 출현하기 전에 국가 수준의 정보 기반 구조를 정의하는 것은 매우 간단하였으나, 최근 10년 전부터 전 세계 수준과 국가 수준 정보 기반 구조를 구분 짓는 것은 쉽지 않은 일이 되었다. 만일 둘 사이를 구분 지어야 할 경우에는, 각 국가는 그 나름대로의 판단 기준을 법령으로 제정하여 사용해 왔다. 마지막으로 특정 지역 수준의 정보 기반 구조는 특정 조직만을 위해서 작동하는 정보 기반 구조이다. 이들은 주로 상업 정보 시스템, 네트워크 기술, 응용프로그램들로 구성된다. 지역 정보 기반 구조의 소유자 및 관리자는 자신들만의 보안 기법을 적용하고 있다.

나. 정보 기반 구조의 분류

정보 기반 구조상에서 처리된 정보는 그 정보의 기능과 내용에 따라 공개될 수 있고, 어떤 경우는 허가된 특정 인원에게만 접근이 허용되어야 한다. 특정 인원에게만 사용되어야 하는 정보에도 많은

타입이 있다. 예를 들어, 기업은 여러 종류의 비밀 정보를 가지고 있고, 정부 조직은 법률 시행, 비밀, 1급 비밀 등의 여러 단계의 비밀 정보를 가지고 있다. 정보를 사용함에 있어서 이와 같이 분류된 정보를 흔히 정보 도메인이라고 한다.

모든 조직들은 업무를 수행하면서 중요한 기능을 보호하기 위하여, 공용(public) 정보와 비밀(private) 정보를 구분한다. 특정 정보를 어떻게, 어떤 범위로 보호해야 하는지는 업무 환경에 따라 다르다. 어떤 조직에는 공용으로 간주되는 정보가 다른 조직에서는 비밀 정보가 되고, 그 반대가 될 수도 있다. 정부는 비밀 정보에 "classified information"라는 머리말을 두어 특별히 분류한다. 예를 들어, 미국의 정부는 4단계 비밀 분류 체계를 사용한다: unclassified, confidential, secret, top secret. 이들 4가지 분류 단계 안에는 특정 부서에 적합한 세부적인 단계가 있을 수 있다. 보통 confidential, secret, top secret은 비밀 정보에 해당한다. Unclassified 문서는 공용 문서와 일부의 비밀 문서(sensitive 또는 Privacy Act Information)에 해당한다. 어떤 타입의 문서들은 비밀로 간주될 수 있다. 한 예가 법률 시행 정보로서, 잘못 다루어지거나 보호되지 않으면 치명적인 문제를 일으킬 수 있다. 저작권과 관련된 정보는 기업 조직에서는 비밀 정보이다. 이런 정보가 공개되는 경우, 기업에게 악영향을 끼칠 수 있기 때문이다. 개인의 금융, 의료 정보들도 비밀 정보에 포함된다. 정부는 연구, 공학, 병참, 행정을 지원하는 다양한 종류의 민감한 비밀의 문서를 다룬다.

대부분의 조직들은 비밀 정보를 보호하는데 있어서 공용 정보보다 더 엄격한 요구 조건을 제시한다. 예를 들어 한 조직에서, 인사 관리나 회계를 담당하는 관리자는 인사, 급여와 관련한 데이터베이스 파일과 서버에 완전히 접근 가능해야 한다. 그러나 이 관리자에게 비밀 프로젝트의 연구, 개발 정보 등을 접근하도록 할 필요는 없을 것이다.

접근 제어와 더불어 보호 수준에 따른 정보의 분할은 정보의 카테고리를 생성한다. 이 정보의 카테고리를 종종 "정보 도메인"이라고 부른다. 조직은 정보 도메인 사이에서 정보 분할과 정보 흐름이 엄격히 이루어지도록 특정 메카니즘을 적용한다. 공동 작업 환경에서 정보를 보호하는 것은 어려운 문제이다. 정보를 공유하는 조직들끼리는 정보의 비밀 수준과 그 정보를 보호하는 방법 등에 동의할 필요가 있다. 예를 들어, S라는 정보를 공유하는 A, B 조직에 있어서, A는 S를 상당한 비밀 정보로 간주하는 반면, B는 S를 공용 정보 수준으로 생각한다면 문제가 발생하게 된다. 각 조직의 보안 관련 대표자가 상호 동의하여 해결책을 찾아야 할 것이다. 이런 공유상의 보안 문제는 정부나 기업의 합동 프로젝트에서 쉽게 발생한다.

다. 보안 경계선과 정보 기반 구조

보안 경계선(boundaries)은 정보 기반 구조의 보안을 고려해야 할 때 꼭 필요하다. 보안 경계선은 정보가 존재하는 물리적 또는 논리적인 위치에 표시된다. 외부로부터 어떤 정보를 보호해야 할지를 이해하면, 가장 적절한 보호 대책을 가장 효과적으로 적용하는 데 도움이 된다. 그러나 실세계의 예를 분석하다 보면, 이 경계가 확실히 구분되어지기 어렵다는 것을 알 수 있다. 어떤 경우에는 사람, 정보, 정보 시스템의 경계선이 물리적인 위치에 의해 결정될 수 있다. 그러나 이러한 물리적 구분은 특정 위치에 여러 가지 보안 정책이 사용될 수 있고, 공용 정보와 비밀 정보가 공존할 수 있다는 사실을 고려하지 않는다. 다른 방법으로는, 특정 위치의 정보와 시스템을 관리하는 정책에 따라서 경계선을 긋는 방법이 있다. 그러나 이 방법은 동일한 정책이 물리적으로 멀리 떨어진 위치에 넓게 퍼져 있을 수 있다는 사실을 망각한 것이다. 그런데 문제를 더 복잡하게 하는 것은, 많은 경우에 한 컴퓨터 또는 서버에 공용 정보

와 비밀 정보가 공존하고 있다는 점이다. 그림 4.1(마. 미국 국방부의 컴퓨팅 환경 참조)은 경계선 정의와 관련된 문제의 복잡성을 나타내고 있다. 그림상의 조직은 두 개의 다른 위치에 있는 컴퓨터 환경을 가지는데 각자가 정보에 어떤 수준을 두어 분류, 관리하고 있다. 이 그림을 보면, 사설망(private network)이 인터넷에도 연결되어 있는데, 이런 경우 물리적인 위치가 경계선을 정의할 수도 있고, 정보의 서로 다른 수준에 의해 생긴 논리적 경계선도 존재한다.

라. 정보보증 프레임워크 영역(IA Framework Areas)

정보 시스템의 복잡도가 결정되면, 공통된 프레임워크가 적용되지 않는 한, 어떻게 시스템을 보호할 것인가 하는 문제가 대두될 것이다. IATF 문서에서 채택한 프레임워크는 정보 시스템의 정보보증 기술이 이용되는 국면에 따라 다음의 4 영역으로 분할한다.

- 로컬 컴퓨팅 환경
- 고립(Enclave) 경계선
- 네트워크와 기반구조
- 기반구조의 지원

이 네 가지 영역으로 분할함으로써, 정보 보증 기술은 좀더 명확하고, 특정 영역에 집중될 수 있다. 그러나 이렇게 분할된 영역은 상호 연관되는 부분이 존재하므로, 실제의 구현에 있어서는 이 중첩된 부분의 상호 작용에 특별히 유의해야 한다. 이 네 영역에 대하여 좀 더 자세히 알아보자.

1) 로컬 컴퓨팅 환경 프레임워크 영역

로컬 사용자 컴퓨팅 환경에는 서버, 클라이언트, 응용프로그램으로 구성된다. 응용프로그램에는 스케줄링이나 시간 관리, 프린팅,

워드 프로세싱, 디렉토리 관리 등이 있다. 로컬 컴퓨팅 환경은 많은 시간에 걸쳐 정부의 임무나 기업의 목적에 적합하도록 유지, 발전된 응용프로그램 또는 정보 시스템이다. 새로운 응용 프로그램을 이 시스템에 설치하려면, 시스템에서 지원하는 기반구조에 맞추는 노력이 필요하다. 이 기존 시스템은 많은 응용 영역에서 정보보증 솔루션이 필요하며, 서버와 클라이언트(응용프로그램, 운영체제, 호스트 기반 모니터링 프로그램 등등)가 보안의 대상이 된다. 정보보증 솔루션을 필요로 하는 응용 영역에는 다음과 같은 것이 있다.

- 메세징 시스템(예: e-mail)
- 운영체제
- 웹 브라우저
- 전자 상거래
- 무선 통신
- 공동 작업 컴퓨팅
- 데이터베이스

2) 고립된 경계선 프레임워크 영역

여러 로컬 컴퓨팅 환경들을 LAN으로 연결하고, 단일 보안 정책에 의해 이들을 관리한다면, 로컬 컴퓨팅 환경의 물리적 위치에 상관없이 "고립되었다(enclave)"라고 간주할 수 있다. 그런데, 보안 정책은 특정 타입, 수준, 처리되는 정보에 따라 유일하게 결정되므로, 단일 물리적 시스템도 한 개 이상의 고립 영역(enclave)을 가질 수 있다. 고립 영역 안에 있는 리소스를 접근하려면 그 영역만의 보안 정책을 따라야 한다. 하나의 고립 영역은 T-1, T-3, ISDN등과 같은 point-to-point 통신망에 의해 지리적으로 분산되어 존재할 수 있다. 고립 영역 내부와 고립 영역 외부 사이에 정보의 유입, 유출이 이루어지는 접근 지점을 고립 경계선이라고 한다. 고립 경계

선과 연결되는 네트워크 연결의 종류에는 다음과 같은 것들이 있다.

- 다른 고립 영역과의 정보 교환, 접근을 위한 인터넷과 같은 외부 네트워크 연결
- 원격 사용자 연결 : 전화망을 이용한 다이얼업 접근, 케이블 모뎀등을 이용한 ISP(인터넷 서비스 제공업체)의 직접 연결, TSP를 통한 전용연결
- 다른 LAN과의 연결

3) 네트워크와 기반 구조

여기서는 고립 영역들 사이의 연결이 이루어진다. OAN(Operational Area Network), MAN(Metropolitan Area Network), CAN(Campus Area Network), LAN 등이 이 범위에 속한다. 이 트랜스포트 망은 인공위성, 마이크로웨이브, RF 스펙트럼, 광섬유 등과 같은 정보 전송 매체를 가지고 있어, 라우터, 스위치와 같은 네트워크 노드들 간의 정보 전달을 돕는다. 정부와 기업에서 현재 사용하고 있고, 앞으로도 사용할 트랜스포트 망 서비스는 논리적으로 다음 세 가지 영역으로 분류되어질 수 있다.

- 공용망/상업망과 네트워크 기술 : 인터넷, 전화망, 무선 네트워크 등이 있다. 특히, 무선 네트워크에는 셀룰라, 인공위성, 무선 LAN, 페이징 네트워크가 있다. TSP(Telecommunication Service Provider)가 이 네트워크의 접근이 통제하고, 소유 및 관리한다.
- 전용망 서버스 : Federal Wireless Service와 FTS2000가 대표적인 예이다.
- 정부 소유 및 관리 : 정부 기관에서 소유, 관리하는 네트워크를 말한다. DoD의 SIPRNET 등이 있다.

4) 기반구조의 지원

안전한 관리와 서비스를 위해 정보 보증 메커니즘을 사용하려는 모든 네트워크, 고립 영역, 컴퓨팅 환경에서 기반구조의 지원은 가장 기본이다. 기반구조의 지원이 있어야만 단말 워크스테이션, DNS, 고수준 디렉토리 서비스와 같은 네트워크 서비스에서 안전을 기대할 수 있다. IATF에서는 기반구조의 지원을 위해, 공개키기반구조(PKI)를 지원하는 키 관리 기반구조(KMI)와 외부 공격으로부터의 탐지-반응 기반구조를 주로 사용한다.

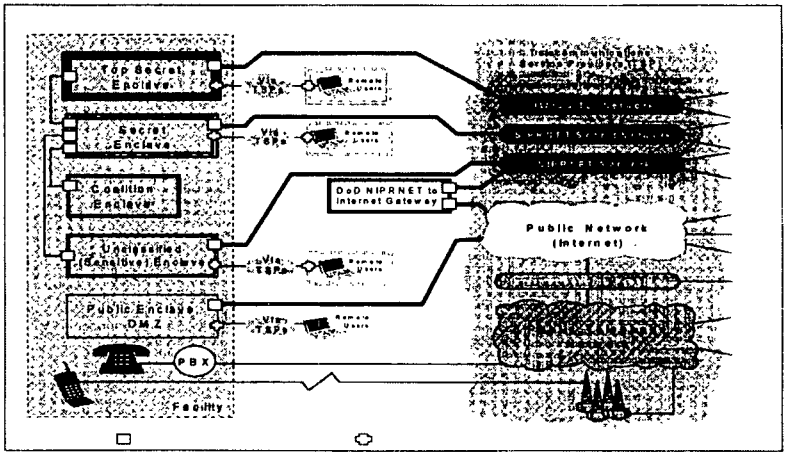
- KMI(키관리 인프라) : KMI에서는 안전한 공용키와 인증서의 생성, 분배 및 관리 뿐 아니라 대칭키 암호 서비스도 제공해 준다. KMI를 통하여 메시지의 송신자와 수신자는 신원이 증명되고 범죄자의 메시지 노출이나 변경과 같은 공격으로부터 안전하게 보호받을 수 있다.
- 탐지-반응: 외부 침입이 있을 때 신속한 탐지와 반응이 이루어지도록 한다. 특히, "융합"(fusion)이라는 기능을 제공하는데, 어떤 한 사건이 발생했을 때, 그 사건을 다른 사건들과 관련지어 분석하는 것을 말한다. 융합을 사용함으로써, 잠재된 공격 패턴을 파악할 수 있으므로 보안 면에서 향상된 시스템을 기대할 수 있게 된다. 이 탐지-반응 인프라는 침입 탐지 시스템과 모니터링 시스템을 이용한다. CERT라고 불리는 전문 요원의 관리가 필요하다.

마. 미국 국방부의 컴퓨팅 환경

국방 정보 기반구조(DII) 환경은 미국 정부의 가장 크고 가장 복잡한 정보 기반구조의 예이다. DII는 2백만 이상의 주요 사용자를 지원한다. DII 안에는 약 200개의 지휘소와 국방 메가센터라고 불리는 16개의 큰 데이터센터가 포함된다. 기본적 사용자 환경은 enclave(물리

적으로 보호된 시설과 구성요소)와 20,000개 이상의 지역 네트워크들, 백본 네트워크에 연결된 약 4,000개의 접속들의 혼합이다. 또한 DII는 300,000명 이상의 보안 전화 이용자들을 지원한다.

DII는 JWICS와 전세계적 연결을 위한 SIPRNET같은 WAN을 사용하여 임무 기능, 기타 군수, 정보 등의 범주를 지원하는 거대한 전세계적 가상 네트워크를 구성한다. 과거에는 이 정보 기반구조가 지정된 네트워크와 정형화된 정보 시스템을 이용하여 구축되었었다. 오늘날 DoD는 NII와 더 넓은 세계적 정보 기반구조 안에서 전반적으로 거의 상용 서비스에 의존한다.



〔그림 4.1〕 미 국방성의 컴퓨팅환경의 예

그림 4.1은 전형적인 사용자 사이트 또는 시설에 대한 시스템 배경 다이어그램이며, DII 구조의 더 넓은 확장을 보여준다. 전형적인 사용자 시설은 임무 기능 분야를 지원하는 많은 LAN을 가지고 있다. 오늘날 물리적 고립은 주로 트래픽의 상이한 분류 레벨의 비밀성과 무결성을 유지하는데 이용된다. 이들 고립된 LAN 가운데 가상 네트워크들은 고립지역 안에서 다양한 임무에 알맞는 기능을

지원하도록 구성된다. 경계가 요구될 때 네트워크들의 상이한 분류 사이에 엄밀하게 통제된 접속이 제공된다. 예를 들면 DoD 조직들은 비밀이 아닌 트래픽의 중요한 레벨을 수행하는 TS-SCI에서 작동하는 월드와이드 정보 시스템을 든든하게 보유하고 있다. 이것은 정보 커뮤니티 안에서 다른 사람들과 의사소통하기 위한 요구를 지원한다. 같은 TS-SCI 고립지역 안에서도 고객은 비 정보 사용자들과의 연결보다는 덜 굳건하지만 비밀/공개 시스템을 가지고 있다. 사용자들의 혼성 커뮤니티에 도달하기 위하여 비밀이 아닌 정보는 분리된 공개정보, 비빌, TS-SCI 시스템을 거쳐 흐른다. 이들 시스템들 사이에서 이동하는 정보는 개방을 고려한 정책이 이어져야 한다는 요구 때문에 복잡하다.

바. 사이버 공격의 실체

정보 시스템이나 네트워크는 항상 사이버 공격의 목표가 될 수 있다. 정보 네트워크 시스템은 모든 영역의 공격에 대해 안전해야 하고, 공격이 이루어지더라도 피해를 최소화하며 빠른 복구가 요구된다. IATF에서는 임의의 공격을 다음 다섯 가지 중 하나로 분류하고 있다.

1) 수동적 공격

수동적(Passive) 공격에는 네트워크 트래픽 분석, 암호화 되지 않은 메시지의 모니터링, 암호화 정도가 약한 메시지의 복호화, 패스워드 같은 인증 정보 훔치기 등이 있다. 수동적 공격은 허가되지 않은 사용자에 의한 정보의 유출, 노출 등을 말한다. 개인 신용카드 정보나 의료 정보 등의 노출도 역시 이 범주 안에 속한다.

2) 능동적 공격

능동적(Active) 공격에는 보호 시스템의 파괴, 악성 코드의 삽입,

정보의 절도 및 변경 등이 있다. 네트워크 망의 과다 사용으로 정상적인 서비스를 방해하거나, 허가된 외부 사용자의 고립 영역 접근 방해와 같은 서비스 거부 공격, 정보의 유출, 변경, 공개 등도 능동적 공격에 해당한다.

3) 인접 공격

인접(Close-In)공격은 허가 받지 않은 공격자가 정보 시스템으로부터 물리적으로 가까운 거리에 있어서, 물리적인 방법으로의 정보의 수집, 변경, 방해 등을 하는 공격이다. 주로, 정보 시스템이 있는 건물이나 방에 은밀히 침입하여 공격이 이루어진다.

4) 내부 공격

내부공격은 내부 인원(Insider)에 의한 공격으로 악의 있는 공격과 악의 없는 공격의 두 종류가 있다. 악의 있는 공격에는 부정 수단에 사용할 목적의 정보의 절도, 손상, 악용 등이 있다. 악의 없는 공격은 부주의나 보안 의식 부족, 무의식적인 보안 방해 등이 있다.

5) 배포시 공격

배포(Distribution)시 공격은 소프트웨어나 하드웨어를 제작할 당시, 제조 공장에서 악성 코드나 기능을 삽입한 것으로서, 차후의 정보 유출을 위한 백도어를 설치한 제품이 그 예이다.

4.1.2 종심 방어체계

미국 국방성은 효과적인 정보 보증 수행을 위하여 "종심 방어(Defense in Depth)체계"라는 전략을 내세웠다. 이 전략의 기본 원리는 어떤 조직인가에 상관없이 다른 정보 시스템이나 네트워크에 적용될 수 있다. 한 조직은 어떤 특정 기술의 지원을 받아서 어떤 작업을 수행할 조직 구성원에게 정보 보증이 필요하다는 것을 알려주어야 한다.

종심 방어체계의 기본 구성인 사람(people), 기술(technology), 작전(operation)의 요건은 다음과 같다.

- 사람(people): 훈련, 지각, 물리적 보안, 개인적 보안, 시스템 보안 관리
- 기술(technology): 기술 체제 영역, 보안기준, IT/IA 획득, 위험 사정, 신뢰증명서
- 작전(operations): 사정, 감시, 침입 탐지, 경고, 대응, 재구성

종심 방어체계의 세 가지 기본 요건 중에서 IATF는 기술(technology)에 초점을 맞추고, 사이버 공격을 막을 수 있도록 하는 공통 영역(네트워크와 기반구조의 방어, 고립 경계선의 방어 등등)에 초점을 맞춘다. 이런 방식을 씀으로써 어떤 특정 레이어나 특정 타입에 대한 공격으로부터 전체 시스템이 위협받는 것을 막을 수 있다. IATF 이외의 정책이나 절차, 기반 구조는 사람(people)과 작전(operations)에 집중하게 된다.

가. 종심 방어체계 계층

정보 기반 구조는 매우 복잡한 시스템으로 많은 곳에서 취약성을 가질 수 있다. 이점을 지적하기 위해, 정보보증 기술 포럼(IATF)은 "종심 방어체계" 전략 안에 다중의(또는 여러 계층의) 정보 보증 기술 해결책을 제시하고 있다. 따라서, 하나의 방어 메카니즘이 공격당하더라도, 그 뒤의 추가적인 방어 메카니즘이 보호를 해주게 된다. 계층적 보호 전략이라 하더라도 네트워크 구조상의 모든 가능한 포인트에 정보 보증 메카니즘이 요구되는 것은 아니다. 주요 영역에 적절한 보호 체계를 구현함으로써, 각 조직들만의 요구를 만족시키는 효율적인 보호 영역 세트가 맞추어지게 된다. 더욱이 계층화된 전략은 어떤 경우에는 저 수준의 보증 해결책만 사용하여 비용을 절감할

수도 있지만, 중요한 영역(예를 들면 네트워크 경계)에는 고수준 보증 해법을 사용하므로 보다 현명한 응용 시스템이라 할 수 있다.

나. 종심 방어체계 전략

효과적이고 견고한 정보보증(IA) 능력을 수행하고 정보보증에 대한 종심 방어체계 전략을 채택하는데 있어서 다음 사항을 고려해야한다.

- 조직에서 정보의 가치에 기초하여 요구되는 정보보호의 효율성과 정보의 손실 또는 압축 등의 잠재적 충격은 조직의 임무와 사업에 달려있다. 정보보증 결정은 위험분석에 기초하고 조직의 운영 목표에 맞추어져야 한다.
- 비용, 실행, 작업 충격, 오늘과 내일의 작업과 환경에 기초한다. 스스로 작업으로 변화할 수 있는 균형잡힌 보호 능력에 기초한 혼합된 접근
- 사람, 작업, 기술 등 세 가지 측면을 기술하는 혼성의 방법. 기술적 전이는 그것을 사용하도록 훈련된 사람들과 응용프로그램을 인도해주는 작동 과정 없이는 가치가 없다.
- 교육, 훈련, 실용적인 경험 그리고 인식에 대한 포괄적인 프로그램이 필요하다. 전문성과 자격증은 가치입증과 인식, 시스템 관리자들의 전문뼈대를 제공한다.
- 규격화된 상업제품의 추구
- 끊임없는 전이는 기능 및 보안이 연관된 네트워크와 정보처리 능력을 진화시키는 이점과 조직의 요구와 작동 환경들을 바꾸기 위한 적응성을 보장하는데 근접하도록 계획하고 실행해야 한다.
- 정기적인 정보 기반 구조의 IA 태세 평가. 네트워크에서 자동화된 스캐너들과 같은 기술 도구들이 취약성 평가에 도움을 줄 수 있다.
- 적대적 의도를 가진 자들의 움직임뿐만이 아니라 부주의하거나 비의도적인 사고, 자연 발생적 사고

- 공유, 표준화, 과정 , 정책 그리고 상호운용에 대한 집착.
- 증가하는 위험에 대해 균형을 유지하는 능력이나 첨단 신기술의 현명한 이용.
- 단일 장벽의 실패나 손실과는 다르게 전반적 정보 기반구조를 위태롭게 하지 않도록 하는 다양한 완화와 중첩된 보호의 채택
- 기대하거나 예기치 않은 사건에 대처할 수 있는 튼튼한 IA 태세를 실현 및 고수
- 오직 믿을만한 인원만이 물리적 접근을 한다는 확신. 어떤 방법들은 배경 조사, 신원 조사, 신임장, 뱃지 등이 적합하다.
- 취약성 리스트, 구현 도구를 감시하고 보안 매커니즘이 상호 작동되는지를 확신하고, 보안 상황과 매커니즘을 지속적으로 감시하고, 도구와 기술을 적절하게 채택하고 향상시켜라. 그리고 현안문제들을 신속하고 효과적으로 다루어라.
- 침입 탐지 시부터 사건 정보는 정해진 절차를 통해 권한을 갖는 책임자와 특수 분석 대응 센터에 보고되어야 한다.

사용자 커뮤니티의 지배적 요구사항은 그들의 운영 목표를 지원해줄 수 있는 정보와 정보 기반 구조로의 접근이다. 이것은 확고한 정보처리 기술과 신뢰성 있는 상호통신능력의 이용을 요구한다. IA는 조직들에게 그들의 정보에 대해 적절히 보호를 유지하기 위한 능력을 제공함으로써 이러한 요구사항을 만족시킬 수 있다. 프레임워크 문서는 종심 방어체계의 기술 관점에 초점을 맞춘다. 효과적인 IA 태세를 개발 중일 때는 종심 방어체계 전략의 세 가지 구성요소 즉, 사람, 기술, 운영이 먼저 체크되어야 한다.

다. 종심 방어체계 기술

정보 기반구조에 대한 IA 기술 목표와 접근의 표현은 네 가지의 종심 방어체계 기술 중점 분야로 구성된다: 컴퓨터 환경 방어, 고

립 경계 방어, 네트워크와 기반구조 방어, 기반구조 지원.

1) 컴퓨터 환경 객체 방어

사용자들은 내부 시스템 응용프로그램과 서버를 보호하기 위한 요구사항이 있다. 시스템이 상위 환경에서 다양한 유산과 혼합한 응용프로그램에 대한 인증(I&A), 접근 통제, 비밀성, 데이터 무결성, 부인방지 보안 서비스 등을 포함한다. 이러한 요구사항은 다음과 같다.

- 클라이언트, 서버, 응용프로그램이 서비스의 거부, 비인가 폭로, 자료의 수정에 대해 적절하게 방어되는지 확인
- 내부나 외부 모두 고립지역에 대해(enclave) 클라이언트, 서버 혹은 응용프로그램에 의해 처리된 자료들의 비밀성과 무결성을 확인
- 클라이언트, 서버, 응용프로그램의 무단사용에 대해 방어
- 클라이언트, 서버들이 안전한 구성 가이드라인들을 따르고 모든 적합한 패치들이 적용되도록 확인
- 패치와 시스템 구성 변화들을 추적하기 위하여 모든 클라이언트, 서버들의 구성 관리를 유지
- 응용프로그램의 변화는 보안 측면에서 무감축으로 통합될 수 있다는 것을 확인
- 내부이던 외부이던 믿을만한 사람 또는 시스템의 파괴적인 행동에 대해 충분한 방어를 확인

2) 고립지역 객체 방어

이러한 네트워크들로부터 정보와 서비스를 얻을 목적으로 개인, 또는 공공의 네트워크들에 연결된 정보 기반구조들을 보호하기 위한 요구사항이 있다. 이것은 그들이 지역적 컴퓨팅 환경과 같은 그들의 기반구조를 침입으로부터 보호해야 한다는 것을 의미한다. 성공적인 침입은 가용성, 무결성 또는 비밀성에 대한 절충을 초래할

수 있었다. 이러한 요구사항은 다음과 같다.

- 물리적이고 논리적인 고립 지역들이 적절하게 보호되도록 할 것
- 변화하는 위협들에 대응하는 서비스의 동적인 저지가 가능하도록 할 것
- 보호된 고립지역 안에 있는 시스템과 네트워크들이 수용 가능한 가용성을 유지하고 서비스 침입 거부에 대해 적절하게 방어되도록 할 것
- 고립지역들간의 자료 변화 또는 원격접근이 부적절한 폭로로부터 보호되도록 할 것
- 기술적인 문제 또는 구성적 문제들로 인해 자신을 방어할 수 없는 고립지역 안에 있는 시스템들을 위한 경계 방어를 제공
- 고립지역 경계를 가로질러 흐르도록 하기 위해 핵심적 정보를 선택적으로 허락하는 위험관리 수단 제공
- 외부 시스템에 의해 또는 강제적으로 침식당하고 있는 보호된 고립지역 안에서 시스템과 데이터에 대한 보호 제공
- 사용자가 고립 지역 바깥으로부터 정보를 받거나 보내는 것에 대한 인증 접근통제를 통한 강력한 인증 제공

3) 네트워크와 기반구조 객체 방어

정보 서비스가 유지되고 개인적, 공공, 비밀 등의 정보가 비의도적으로 폭로되거나 대체되지 않도록 하는 그들의 네트워크와 기반구조를 보호하기 위한 요구가 있다. 이러한 요구 사항은 다음과 같다.

- WAN을 통해 교환되는 모든 데이타가 비인가된 인원이 네트워크에 접근하여 자료를 폭로하는 것으로부터 보호되도록 할 것
- 임무를 지원하는 WAN과 임무지원 자료들이 서비스 공격 거부에 대해 적절한 보호를 제공하도록 할 것

- 적절히 보호된 정보가 아닌데 잘못 배달되거나 배달되지 않거나 지연되는 것에 대해 보호
- 트래픽 흐름 분석으로부터 보호
  - 사용자 트래픽
  - 네트워크 기반구조 제어 정보.
- 보호 매커니즘들은 다른 허가된 백본과 독립지역 네트워크들을 가진 순수한 작동에 간섭받지 않도록 할 것

4) 기반구조 객체 지원

기반 구조 지원은 다른 종심 방어체계 분야를 가능하게 하는 기술이다. 이 분야는 키 관리를 제공하고 종심 방어체계의 양상들을 탐지하고 대응한다. 그런 기반구조 지원 요소들은 침입탐지 시스템, 시스템 구성 검사 또는 조사에 필요한 자료 수집 등에 대해 탐지 및 대응할 수 있는 능력이 필요하다. 이러한 요구 사항은 다음과 같다.

- 키, 특정한 권한, 신분확인 관리 및 개인의 네트워크 이용에 대해 긍정적 증명을 해주는 암호화된 기반구조를 제공
- 침입이나 다른 알려지지 않은 사건의 신속한 탐지 및 대응이 가능하고, 작동간 상황 경고를 할 수 있도록 기반구조의 침입탐지, 보고, 분석, 평가를 제공
- 예비 및 재구성에 대한 요구사항을 실행하고 보고하도록 계획

이와 같이 주요 기반 구조를 보호하기 위한 정보보증은 침해에 대한 방어, 기반 구조 파괴-침입-침해에 대한 탐지, 서비스의 복구, 추후의 침입 혹은 위협에 대응하는 대응 체계 등 4가지 큰 축으로 구성되며, 정보보증 기술 프레임워크(IATF; Information Assurance Technical Framework)는 정보보증을 이루기 위해 필요한 여러 기술들을 구현한 프레임워크이다.

4.2 북한의 정보전 전략

4.2.1 북한의 정보기술

북한정보기술(IT)산업은 소프트웨어(SW) 분야는 상당히 높은 수준이지만 하드웨어(HW)는 단순 조립단계에 머물러 있는 것으로 평가된다. 통일부 조사에 따르면 북한은 80년대부터 HW 분야에서 SW 분야로 방향을 바꿔 SW개발에 적극 나서고 있다. 그 결과 SW 기술은 우리 나라와 3~5년 정도밖에 차이가 나지 않는 것으로 전해지고 있다. 북한에서 SW 개발을 주도하는 기관은 과학원, 김책공대의 전자계산연구소, 평양프로그램센터, 조선컴퓨터센터, 은별컴퓨터기술무역센터 등이다. 이들 기관은 매년 '전국프로그램 경연 및 전시회'를 개최한다. 김정일 국방위원장은 93년부터 이들 컴퓨터 관련기관을 수시로 방문, 프로그램 개발을 독려하고 있다. '윈도'용 워드프로세서로는 현재 '창덕 5.0'과 '단군'이 개발돼 널리 사용되고 있다. '단군'은 윈도환경에서 한글 처리가 가능함은 물론 한국의 KS코드도 지원한다. '창덕'은 유선인터넷언어(HTML) 문서작성 및 읽기 기능까지 포함돼 있어 한국 수준과 엇비슷하다는 평가까지 받고 있다. 북한은 군사용 SW 및 사회간접자본과 관련된 SW를 집중적으로 개발했다. 조선컴퓨터센터에서 개발한 해상교통지휘시스템(MTCS-21A) 자동항해지휘시스템(ANCS-4) 교통관제시스템 등이 대표적이다. 평양프로그램센터에서는 '창덕'과 '단군' 등 워드프로세서 외에도 다국어 편집프로그램 '평필', 표계산 프로그램 '용마', 전자출판 프로그램 '청류', 건축설계 프로그램 '백두산'등의 프로그램을 개발하기도 했다. 과학원은 음성인식 프로그램 '칠보산'을 개발할 정도로 기술력이 뛰어나다.

한편 HW는 매우 낙후되어 있다. 북한은 60년대 말 '전진-5500'이란 1세대 디지털 컴퓨터를 완성할 정도로 남한에 비해 우수한 수준이었으나 이후 기술력이 크게 낙후됐다. 82년 8비트 PC인 '봉

화4-1'을 생산하기 시작했으며 현재는 32비트 PC를 생산하는 수준이다. 평양컴퓨터조립공장은 연간 3만 여대의 생산능력을 갖추고 주로 국방 및 공공기관용으로 보급하고 있다. 조선과학원 산하 전자공학연구소는 집적회로(IC) 시험공장을 설립, 반도체 부문의 기술개발에도 나서고 있다. 현재 평양집적회로공장, 단천영예군인 반도체공장 등이 인쇄회로기판(PCB) 및 기초 반도체를 생산하고 있는 정도이다. 북한은 특히 정보화 촉진의 근간이 되는 통신시설이 상당히 취약하다. 따라서 정보통신 인터넷 등이 생산 기술력에서 모두 낙후될 수밖에 없는 실정이다. 전화선의 경우 93년까지 130만 회선에 불과했으며 공중전화도 2720대에 그쳤다. 95년 2단계 통신망 개발계획을 수립했으나 악화된 경제환경으로 지지부진한 상태이다. 이 계획대로라면 수동식 교환 4만 회선과 이동통신설비 1200회선, 무선호출 통신설비 1500회선을 수용했어야 했다. 97년에는 평양의 근거리통신망(LAN)과 각 기업소의 컴퓨터 등을 연결하는 북한 최초의 광역전산망을 개통했다. 북한은 이 시스템에 접속하기 위해 국가기관과 주요 기업소 등 극히 일부에 펜티엄급 PC를 보급했다. 최근에는 정부조직으로 전자공업성을 신설, HW 기술 개발에 주력하고 있다. 특히 '2000년 과학기술전망 목표'에서는 기초과학분야 이외에 컴퓨터와 원자력 이용 등 첨단과학기술 부문과 전자기계 등 분야에 연간 국민소득의 5%를 투자한다는 계획을 제시하고 있다.

4.2.2 북한의 정보전 능력

북한은 1990년대 초부터 전방부대와 인민무력부를 연결하는 광케이블을 설치하고, 인민무력부 산하의 지휘자동화대학(미림대학)을 중심으로 C3I(지휘, 통제, 통신, 정보)체계에 대한 연구를 추진하여 왔으며 특히 군 지휘 자동화, 사이버 테러 기술, 전자전 분야의 전문 인력을 양성하여 기술 개발을 추진하고 있다. 최근 들어 북한은 1999년을 과학의 해로 설정하고 과학기술 발전 특히

정보기술 발전 정책을 강력하게 추진하고 있다. 정보기술 분야에서 하드웨어 분야는 자본 부족, 외자 유치문제 등으로 상당히 위축되어 있으나, 부가가치가 높고 적은 자본으로 개발이 가능한 소프트웨어 분야는 괄목할만한 성과를 거둔 것으로 알려졌다. 군사분야에서도 해킹 및 바이러스 등의 정보전 기술을 상당한 수준으로 개발하였으며 향후 세계 첨단 수준의 잠재능력을 보유한 것으로 판단하고 있다.

4.3 정보보증 전략 제안

4.3.1 정책적 제안(정보보안 관리체계 정립)

정보보안 관리(Information Security Management)는 조직의 보안 위험을 식별하고 정보보안 위험을 효과적으로 관리할 수 있는 체계적인 대책을 수립하여 수행함으로써 조직의 관리정보에 대한 비밀성, 무결성, 가용성을 보장하는 것이다. 국제적으로 가장 중요한 동향으로는 영국의 BSI(British Standard Institute)를 중심으로 정보보안 관리체계 표준화를 들 수 있는데, BSI의 정보보안 관리체계 수립 지침인 BS7799-Part 1(Code of practice for Information Security Management)를 국제표준화 기구(ISO)에 상정하여 국제표준인 ISO/IEC 17799(2000년 12월)로 제정하였으며, 정보보안 관리체계 규격인 BS7799-Part 2(Specification for Information Security Management Systems)도 현재 국제표준화를 추진하고 있다. 특히 영국을 중심으로 BS 7799-Part 2를 기반으로 한 정보보안 관리체계 인증제도를 시행하고 있는데, 정보보안 관리체계 인증제도란 특정한 조직이 수립하여 운영하고 있는 정보보안 관리체계가 일정한 심사기준에 적합한지 여부를 공적인 제3의 인증기관이 객관적으로 평가하여 특정한 조직의 정보보안 관리체계를 보증해 주는 제도이다.

한편, 정보통신부는 민간 분야 정보보호 수준을 높이기 위해 정보통신 서비스 제공자들을 대상으로 해당 조직의 정보보호 관리체계를 심사·인증해 주는 정보보호 관리체계 인증제도를 2002년 5월부터 시행하고 있다. 정보보호 관리체계 인증제란 각 기관이 자사 정보보호 환경에 맞춰 정보자산을 효율적으로 보호하기 위해 수립·운영하고 있는 정보보호 관리체계가 정통부에서 제정·고시한 인증 심사기준에 적합한지를 심사·인증해 주는 제도로, 인증심사는 한국정보보호진흥원이 맡는다. 인증심사 내용은 신청기관의 정보보호 환경을 감안한 물리(출입통제·인적보안)·기술(정보시스템 보호)·관리적(정보보호정책·정보자산 식별·위험분석 평가 등) 보호 조치로 구분할 수 있는데, 신청기관이 5단계의 정보보호 관리과정(정보보호 정책 수립, 관리체계의 범위 설정, 위험관리, 구현, 사후관리)에 따라 해당기관이 처해 있는 정보보호 환경에 적합한 정보보호 관리체계가 구축되어 있는지, 정보보호 관리체계가 충실히 구현되어 있는지, 구축된 계획이 실제 실효성 있게 사후관리가 이루어지고 있는지를 심사하게 된다. 인증심사는 조직의 정보보호 관리체계가 처해진 정보보호 환경에 적절하게 수립·운영되고 있는지에 대하여, 관련문서 및 절차 등의 검토와 문서의 내용 등에 대한 실제 현장 점검을 통해 실시하고, 심사결과 부적합한 사항이 발견될 경우 30일의 기한을 정해 신청기관에 보완을 요청하고, 보완된 뒤 재심사를 실시한다. 또한 인증의 유효기간은 3년으로 하였으며, 유효기간 내 정보보호관리체계와 관련된 중대한 변경이 있을 경우 갱신심사를 할 수 있도록 규정하고 있다.

정보통신부의 정보보호 관리과정은 정보보호 관리체계를 수립하고 운영하기 위하여 유지 관리하여야 할 5단계의 활동으로 1단계 정보보호 정책 수립, 2단계 정보보호 관리체계 범위 설정, 3단계 위험관리, 4단계 구현, 5단계 사후관리로 구성되어 있다. 또한, 정

보보안 관리과정의 각 단계별 주요 인증 심사 요소를 다음과 같이 규정하고 있다.

- 정보보호 정책 수립 : 적합한 정보보호 정책의 수립 여부, 정보보호 조직의 구성, 운영, 책임성의 명확한 설정 여부
- 정보보호 관리체계 범위 설정 : 정보보호 관리체계 운영을 위한 관리 범위 설정 및 정보 자산의 현황 조사 여부
- 위험관리 : 위험관리 전략 및 계획 수립의 적절성, 위험 분석 및 위험 평가의 적절성, 채택한 정보보호 대책의 적절성
- 구현 : 정보보호 대책의 구현 적절성, 정보보호 교육 훈련의 효과성
- 사후 관리 : 정보보호 관리체계의 재검토 여부, 모니터링 및 개선 대책, 내부 감사활동의 적절성 여부

이러한 정보통신부의 정보보호 관리체계를 보안 수준이 매우 높게 요구되는 국방조직에 그대로 적용할 수 있는지 여부는 구체적인 검증이 필요하다. 특히 국제 표준과 정통부 지침에 부합하면서 사후 관리보다는 사전에 보안 위험에 대해 강화된 관리를 수행하게 하는 국방 정보보안 관리 기준의 제정이 필요하다. 국방 정보보안 관리 기준에는 정보보호 정책, 정보보호 조직, 정보자산 분류와 접근 통제, 인적 보안과 교육/훈련, 엑세스 제어와 암호, 운영 관리, 물리적인 보안, 보안사고 대응 및 복구 등의 측면에서 세부적인 통제가 강화되어야 한다. 국방 정보보안 관리 기준을 제정할 때 다음과 같은 정보보안 관리 통제 분야를 설정하고 각 분야 별로 적절한 보안 기준과 대책을 제시해야 한다.

- 정보보호 정책 : 보안 정책의 수립, 승인, 공표 및 유지관리 체계
- 정보보호 조직 : 보안 조직의 구성 및 운영 체계

- 정보자산 관리 : 정보자산의 분류와 취급 체계
- 시스템 보안 : 엑세스 제어, 암호체계, 데이터베이스 보안, 네트워크 보안
- 운영 관리 : 운영 절차와 통제, 시스템 관리, 보안사고 대응, 사후 관리

4.3.2 기술적 제안(정보 공격무기 개발)

유무선 인터넷을 중심으로 한 정보통신기술의 발전과 더불어 정보공격 또는 사이버테러의 기술도 함께 발전하고 있는데, 최근의 정보공격 또는 사이버 테러의 형태는 네트워크를 통한 동시 다발적인 공격, 직접공격보다는 우회공격, 서버 컴퓨터는 물론 개인용 컴퓨터에 대한 공격, 바이러스 기술과 해킹 기술의 통합, 지능형 분산 은닉된 공격 기술 등의 경향을 보이고 있으며, 다양한 정보공격 기술 중에서 가장 고도화된 기법은 해킹과 바이러스가 통합된 기술에 첨단 인공지능을 활용한 기법이라고 할 수 있다.

한국정보보호진흥원(http://www.kisa.or.kr/)에 접수된 국내 해킹사고는2000년 1,943건에서 2001년 5,333건으로 174% 증가하였으며, 바이러스 피해도 2001년 한 해 동안 무려 65,033건이 접수되어 해킹 및 바이러스로 인한 피해가 급격히 증가하고 있는데, 특히, 2001년에는 사이버테러의 해라고 할 수 있을 정도로 대규모 피해를 입힐 수 있는 공격들이 동시 다발적으로 발생하였다. 또한 공격 대상이 되는 컴퓨터가 유닉스, 윈도우 서버에서 개인용 PC로 확대되는 경향이 있으며 강력한 컴퓨팅 능력을 갖춘 개인용 컴퓨터를 이용한 인터넷 웜(Worm)이 급격하게 증가하고 있다. 이러한 바이러스 및 해킹의 공격기법은 매우 고도화되어 가고 있는데, Nimda 웜, Badtrans 바이러스와 같이 단순히 E메일을 열기만 하여도 감염이 되기도 하고, NakedWife 바이러스와 같이 선정적인 문구로 사용자들을 현혹시키기도 한다. 최근 출현하는 웜 중에는

바이러스와 해킹의 기능을 동시에 사용하여 더욱 지능적인 수법을 이용하고 있다. 해킹기법을 이용해 취약한 시스템을 검색해 불법으로 침입한 후, 바이러스처럼 내부시스템을 감염시켜 트로이 목마와 같은 악성프로그램을 심어 놓거나 서비스 거부 공격에 이용하기도 한다. 인터넷 웜의 대표적인 사례로는 2001년 4월 경 중국 항공기와 미국 정찰기 사이에 충돌 사건 후의 정보 공격을 들 수 있다. 미국 정찰기 반환과정에서 미국의 불평등한 요구 때문에 분개한 중국 해커들이 Sadmin/IIS Worm이라는 Internet Worm을 만들어 전 세계적으로 확산시켜 많은 피해를 입힌 경우인데. 여기에 사용된 공격 기법은 SUN Solaris의 sadmind 루트권한 버퍼 오버플로우 취약점 및 Microsoft IIS 서버의 Unicode 취약점을 이용하였다. 최근에 탐지된 주요한 인터넷 웜과 공격기법을 요약하면 다음 표와 같다.

Worm 종류	운영체제	공격 기법	발견일
Ramen Worm	Linux	ftp, lprng, rpc.statd 취약점	2001-01
Li0n Worm	Unix, Linux	bind 취약점	2001-03
Carko Worm	Solaris	Solaris snmpXdmid 취약점	2001-04
Sadmin / IIS Worm	Solaris, Windows	Solaris Sadmin, IIS Unicode 취약점	2001-05
Cheese Worm	Linux	Li0n 백도어	2001-05
Red Worm	Linux	bind, LPRng	2001-06
CodeRed Worm	Windows	ISAPI ida.dll 버퍼 오버플로우 취약점	2001-07
CodeBlue Worm	Windows	IIS Unicode Traversal 취약점	2001-09
Nimda Worm	Windows	IIS Unicode Traversal, MIME자동실행 취약점	2001-09

〔표 4.1〕 인터넷 공격의 예

첨단 정보통신기술은 시간적 공간적 차이의 개념이 없으므로 정보공격 또는 사이버테러도 전후방의 개념이 없다. 국가의 모든 기반구조는 상호 연동되어 사이버 공간에서 운영되기 때문에 전방과 후방의 개념이 없어지고 네트워크를 통해 접근할 수 있는 곳이면 어디든지 잠재적인 정보전 전장이 되는 것이다. 또한 정보공격 또는 사이버테러는 공격징후를 파악하여 사전에 경보할 수 있는 체계가 미약하기 때문에 기습 공격을 당하기 매우 쉽기 때문에 철저한 사이버 경계 및 침입 탐지 그리고 방어 기술, 복구 기술이 필요하다. 그러나 최선의 방어는 공격이므로 정보전에서 승리하기 위해서는 공격무기에 대한 연구 나아가 공격무기를 개발하는 연구가 필수적이다. 특히 다양한 해킹 기술 개발, 지능형 바이러스 제작, 해킹과 바이러스가 통합된 공격 기법 개발 등이 필요하다.

4.3.3 인력양성 제안(정보전 훈련장 구축)

가. 정보전 훈련장의 필요성

지난 20여 년간에 걸친 컴퓨터와 관련된 기술의 비약적인 발전과 개인용 컴퓨터의 보급은 급기야 현대인들의 삶을 컴퓨터와 분리하여 생각할 수 없을 만큼 그 의존도를 증가시켰다. 이는 개인의 생활뿐만 아니라, 기업, 정부기관, 군사적인 목적에 이르기까지 어느 한 부분 예외가 없을 정도이다. 그러나 컴퓨터와 네트워크에 사용된 기술이 완벽한 것은 아니다. 직관적이지 못한 사용자 인터페이스, 사용중 정지 현상과 운영체계 및 응용프로그램에서 발견되는 결함 등에 대한 경험이 그 예이다.

해커(hacker)란 컴퓨터가 갖고 있는 원래의 기능을 확장시킬 수 있을 정도의 재능을 갖춘 사람을 일컫는 긍정적인 의미의 말로 컴퓨터 시스템에 악의적인 공격을 가하는 크래커(cracker)와는 구별된다.

여기서는 컴퓨터 시스템를 공격하는 사람들을 공격자(attacker)라고 부르기로 한다. 공격자는 위에서 말한 컴퓨터와 네트워크 기술의 결함을 알아냄으로써 데이터를 빼내거나, 변경시키고, 시스템을 자신의 의도대로 조정함으로써 상대방에게 막대한 피해를 주거나 심지어는 대혼란을 야기할 수도 있다. 특히 공격의 대상이 군사적인 통제와 관련된 컴퓨터 시스템이라면 공격이 성공할 경우 이에 따르는 피해는 상상을 초월하는 것일 수도 있다. 컴퓨터와 네트워크에 의해 제어되고 무기체계와 명령체계에 심각한 혼란을 줄 수도 있기 때문이다. 이는 소수의 전문가에 의한 행해질 수 있으며, 외형적으로는 소리 없이 적을 무기력하게 만들 수 있는 심각한 공격의 유형이다.

이에 대한 대비는 필수적이기 때문에 이 분야만을 연구하는 전문가 집단이 출현하게 되었고 이는 군사 조직에서도 예외가 아니다. 군에서도 이 분야의 전문가를 양성하거나, 전문가들을 군조직에 포함시켜 공격적인 대비태세를 유지해야 할 것이다. 무엇보다도 중요한 것은 군의 중요 직위에 있는 장교들이 컴퓨터와 네트워크에 대한 공격의 중요성을 인식하고 이에 대한 기본적인 지식을 갖추어야 한다는 것이다.

한 분야에 대한 관심은 그 분야의 전문가로 발전하기 위한 가장 중요한 요건이다. 종종 미디어를 통해 보도되는 국내와 기업 또는 정부기관의 컴퓨터에 대한 해킹 사건, 컴퓨터 바이러스의 감염 등의 보도를 접하면서 이에 대해 관심을 갖는 사람이 많아 졌다. 인터넷에서 쉽게 구할 수 있는 해킹 툴(hacking tool)을 다운로드하고 싶은 충동을 느끼는 경우도 있을 것이다. 그러나 해킹을 실행에 옮기는 것은 쉽지 않다. 해킹 자체의 어려움보다는 해킹 사실이 밝혀졌을 경우에 대한 도덕적인 책임 문제가 해킹의 시도를 어렵게 만드는 것도 사실이다.

군조직에는 다른 조직에 비해 많은 수의 월등한 수준을 갖춘 해

킹 전문가가 필요하다. 군의 조직이 과학화되고 무기체계가 현대화될수록 컴퓨터에 대한 의존도가 높아지게 될 것이고 이에 따른 공격의 수준도 높아지게 될 것이다. 따라서 군조직 내에 컴퓨터와 네트워크에 대한 공격과 방어를 자유롭게 시험할 수 있는 공간을 만들어 이 분야에 대한 전반적인 관심을 유도하고 재능이 있는 해커를 발굴하여 전문가로 양성하는 것은 매우 의미 있는 일이다.

나. 정보전 훈련장의 구성

정보전 훈련장은 서버와 클라이언트를 연결하는 네트워크를 구성되며 이 시스템은 외부의 다른 네트워크와는 완전히 분리되어 통제되도록 구성하여 정보전 훈련장 안에서 클라이언트와 서버, 클라이언트와 클라이언트 사이의 공격이 행해질 수 있도록 설계되어야 한다. 최초에는 군내의 교육기관에 정보전 훈련장을 설치하여 운영에 관한 노하우를 축적하고 시설을 보강한 후 군내 인트라넷을 통해 정보전 훈련장을 구성하는 시스템에 자유롭게 접근하는 방식으로 확장하는 것이 바람직하다.

정보전 훈련장의 운영과 교육을 위한 전문적인 지식을 가진 관리자가 필요하며, 정보전 훈련장의 설치에 필요한 기본적인 시스템의 구성요소는 다음과 같다.

- 서버 및 단말기: 실제 실무에서의 사용 정도 및 설치 상의 문제점을 고려하여 두 가지의 운영체계 윈도우즈와 리눅스를 독립적으로 설치할 수 있는 구 대의 서버가 필요하다. 서버는 정보전 훈련 전용으로 사용할 경우 펜티엄III 수준이면 운용에 문제점이 없을 것으로 판단된다. 단말기의 수는 사용자의 수 및 관리 능력에 의존하나 20대 정도면 훈련장의 기능을 유지할 수 있으며, 단말기는 서버 또는 이보다 낮은 수준이라도 문제가 없다.
- 네트워크 구성: 서버와 단말기 사이의 네트워크 구성을 위해

허브 및 라우터의 설치가 필요하다. 네트워크의 구성은 외부의 실제 네트워크의 축소된 형태로 서버의 공격에 대한 침입탐지, 침입경로 등에 관한 분석 및 추적 실습이 가능하도록 구성되어야 한다.

부록: 정보통신기반보호법안

· 개요

정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터바이러스 등을 이용한 전자적 침해행위가 21세기 지식기반국가의 건설을 저해하고 국가안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설(主要情報通信基盤施設)을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하려는 것임.

· 주요골자

가. 주요정보통신기반시설의 보호를 위한 범정부적 대응체제를 구축하기 위하여 국무총리 소속 하에 정보통신기반보호위원회를 설치함(제3조).

나. 주요정보통신기반시설을 관리하는 기관의 장은 정기적으로 소관 시설에 대한 취약점을 분석·평가하여 이에 따른 보호대책을 수립·시행하고 주요정보통신기반시설을 관장하는 중앙행정기관의 장은 소관분야별 주요정보통신기반시설보호계획을 수립·시행하도록 함(제5조 및 제6조).

다. 중앙행정기관의 장은 정보통신기반보호위원회의 심의를 거쳐 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하도록 함(제8조).

라. 주요정보통신기반시설을 관리하는 기관의 장은 소관 시설이 침해사고로 인하여 교란·마비 또는 파괴된 사실을 인지한 때에는

이를 관계기관 등에 통지하고 피해복구 및 피해확산 방지를 위한 조치를 취하도록 함(안 제13조 및 제14조).

마. 정보통신부장관은 주요정보통신기반시설을 관리하는 기관의 동 시설에 대한 취약점 분석·평가 및 보호대책의 수립을 지원하기 위하여 정보보호전문업체를 지정하도록 함(제17조).

바. 해킹·컴퓨터바이러스 등 전자적 침해행위에 의하여 주요정보통신기반시설을 교란·마비·파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처하도록 함(제28조).

정보통신기반보호법

〔제정 2001.1.26 법률 제6383호〕

제1장 총칙

제1조(목적) 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망이용촉진및정보보호등에관한법률 제2조제1항제1호의 규정에 의한 정보통신망을 말한다.
2. "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
3. "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다.

제2장 주요정보통신기반시설의 보호체계

제3조(정보통신기반보호위원회) ①제8조의 규정에 의하여 지정된 주요정보통신기반시설(이하 "주요정보통신기반시설"이라 한다)의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하

에 정보통신기반보호위원회(이하 "위원회"라 한다)를 둔다.

② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③ 위원회의 위원장은 국무총리가 되고, 위원회의 위원은 대통령령이 정하는 중앙행정기관의 장과 위원장이 위촉하는 자로 한다.

④ 위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둔다.

⑤ 위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제4조(위원회의 기능) 위원회는 다음 각호의 사항을 심의한다.

1. 주요정보통신기반시설 보호정책의 조정에 관한 사항
2. 제6조제1항의 규정에 의한 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항
3. 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항
4. 그밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항

제5조(주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행하여야 한다.

② 관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

③ 지방자치단체의 장이 관리·감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정자치부장관에게 제출하여야 한다.

④ 관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

⑤ 정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제6조(주요정보통신기반시설보호계획의 수립 등) ①관계중앙행정기관의 장은 제5조제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립·시행하여야 한다.

② 관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.

③ 주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다.

1. 주요정보통신기반시설의 취약점 분석·평가에 관한 사항
2. 주요정보통신기반시설의 침해사고에 대한 예방 및 복구대책에 관한 사항
3. 그밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항

④ 정보통신부장관은 주요정보통신기반시설보호계획의 작성지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다.

⑤ 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다.

⑥ 주요정보통신기반시설보호계획의 수립·시행에 관한 사항과 정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제7조(주요정보통신기반시설의 보호지원) ①국가기관 또는 지방자치단체의 장인 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 국가기관 또는 지방자치단체의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 국가보안업무를 수행하는 기관의 장 등 대통령령이 정하는 국가기관의 장 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각호의 업무에 대한 기술적 지원을 요청할 수 있다.

1. 주요정보통신기반시설보호대책의 수립
2. 주요정보통신기반시설의 침해사고 예방 및 복구

② 국가안전보장에 중대한 영향을 미치는 다음 각호의 주요정보통신기반시설에 대한 관리기관의 장이 필요하다고 인정하여 제1항 각호의 기술적 지원을 요청하는 경우 국가보안업무를 수행하는 기관의 장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가보안업무를 수행하는 기관의 장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다.

1. 도로·지하철·공항 시설
2. 전력, 가스, 석유 등 에너지·수자원 시설

3. 방송중계·국가지도통신망 시설
4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

③ 국가보안업무를 수행하는 기관의 장은 제1항 및 제2항의 규정에 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다.

제3장 주요정보통신기반시설의 지정 및 취약점 분석

제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

② 중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.

③ 관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정자치부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

⑤ 중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.

⑥ 중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.

⑦ 주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

제9조(취약점의 분석·평가) ①관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

② 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.

1. 정보통신망이용촉진및정보보호등에관한법률 제52조의 규정에

의한 한국정보보호진흥원(이하 "보호진흥원"이라 한다)

2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다)
3. 제17조의 규정에 의하여 지정된 정보보호전문업체
4. 정부출연연구기관등의설립·운영및육성에관한법률 제8조의 규정에 의한 한국전자통신연구원

④ 정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.

⑤ 주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제4장 주요정보통신기반시설의 보호 및 침해사고의 대응

제10조(보호지침) ①관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당 분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.

② 관계중앙행정기관의 장은 기술의 발전 등을 감안하여 제1항의 규정에 의한 보호지침을 주기적으로 수정·보완하여야 한다.

제11조(보호조치 명령 등) ①관계중앙행정기관의 장은 제5조제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 분석하여 필요하다고 인정하는 때에는 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.

② 정보통신부장관은 제1항의 규정에 의한 명령 또는 권고를 받은 해당 관리기관의 장이 보호조치를 시행하는데 필요한 기술적 지원을 할 수 있다. 다만, 제7조제2항의 규정에 해당하

는 경우에는 그러하지 아니하다.

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

제13조(침해사고의 통지) ①관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.

② 정부는 제1항의 규정에 의하여 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위안에서 복구비 등 재정적 지원을 할 수 있다.

제14조(복구조치) ①관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

② 관리기관의 장은 제1항의 규정에 의한 복구 및 보호조치를

위하여 필요한 경우 관계중앙행정기관의 장 또는 보호진흥원의 장에게 지원을 요청할 수 있다. 다만, 제7조제2항의 규정에 해당하는 경우에는 그러하지 아니하다.

③ 관계중앙행정기관의 장 또는 보호진흥원의 장은 제2항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다.

제15조(대책본부의 구성 등) ①위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)를 둘 수 있다.

② 위원회의 위원장은 대책본부의 업무와 관련 있는 공무원의 파견을 관계 행정기관의 장에게 요청할 수 있다.

③ 위원회의 위원장은 침해사고가 발생한 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 대책본부장을 임명한다.

④ 대책본부장은 관계 행정기관의 장, 관리기관의 장 및 보호진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있다.

⑤ 제4항의 규정에 의하여 협력과 지원을 요청받은 관계 행정기관의 장 등은 특별한 사유가 없는 한 이에 응하여야 한다.

⑥ 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제16조(정보공유·분석센터) ①금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각호의 업무를 수행하고자

하는 자는 정보공유·분석센터를 구축·운영할 수 있다.

1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
2. 침해사고가 발생하는 경우 실시간 경보·분석체계 운영

② 제1항의 규정에 의한 정보공유·분석센터의 장은 업무종사자의 인적 사항 등 대통령령이 정하는 사항을 관계중앙행정기관의 장에게 통지하여야 한다. 통지한 사항을 변경한 경우에도 또한 같다.

③ 관계중앙행정기관의 장은 제2항의 규정에 의하여 통지받은 사항을 정보통신부장관에게 통보하여야 한다.

④ 정부는 제1항 각호의 업무를 수행하는 정보공유·분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다.

⑤ 제2항의 규정에 의한 통지의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제5장 정보보호전문업체의 지정 등

제17조(정보보호전문업체의 지정) ①정보통신부장관은 다음 각호의 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 정보보호전문업체로 지정할 수 있다.

1. 주요정보통신기반시설의 취약점 분석·평가 업무
2. 주요정보통신기반시설보호대책의 수립 업무

② 정보보호전문업체로 지정받을 수 있는 자는 법인에 한한다.

③ 정보통신부장관은 제1항의 규정에 의하여 정보보호전문업체를 지정하는 때에는 정보통신부령이 정하는 바에 따라 유효기간을 정하여 지정할 수 있으며, 그 유효기간이 만료한 때에는 재지정을 할 수 있다.

④ 제1항의 규정에 의한 지정과 제3항의 규정에 의한 재지정의 기준·절차 및 방법 등에 관하여 필요한 사항은 정보통신부

령으로 정한다.

제18조(결격사유) 다음 각호의 1에 해당하는 자는 정보보호전문업체로 지정받을 수 없다.

1. 임원중 다음 각목의 1에 해당하는 자가 있는 법인
   가. 미성년자·금치산자 또는 한정치산자
   나. 파산자로서 복권되지 아니한 자
   다. 금고 이상의 실형의 선고를 받고 그 집행이 종료(집행이 종료된 것으로 보는 경우를 포함한다)되거나 집행이 면제된 날부터 2년이 지나지 아니한 자
   라. 금고 이상의 형의 집행유예의 선고를 받고 그 집행유예기간중에 있는 자
   마. 제21조제1호 또는 제3호 내지 제5호의 규정에 의하여 지정이 취소된 법인의 취소당시의 임원이었던 자(취소된 날부터 2년이 지나지 아니한 자에 한한다)
2. 제21조제1호 또는 제3호 내지 제5호의 규정에 의하여 지정이 취소된 후 2년이 지나지 아니한 법인

제19조(정보보호전문업체의 양도·합병 등) ①정보보호전문업체는 다음 각호의 1에 해당하는 경우에는 정보통신부령이 정하는 바에 의하여 정보통신부장관에게 신고하여야 한다.

1. 제17조제1항 각호의 업무를 양도하는 경우
2. 정보보호전문업체인 법인간의 합병이 있는 경우

② 제1항의 규정에 의한 신고를 한 경우의 양수인 또는 합병에 의하여 설립되거나 존속하는 법인은 그 정보보호전문업체의 지위를 승계한다.

③ 제17조제4항(지정기준에 한한다) 및 제18조의 규정은 제1항의 규정에 의한 신고에 관하여 이를 준용한다.

제20조(업무의 휴지·폐지·재개) 정보보호전문업체가 업무를 휴지·폐지 또는 재개하고자 하는 때에는 휴지·폐지 또는 재개하고자 하는 날의 30일전까지 정보통신부령이 정하는 바에 따라 정보통신부장관에게 신고하여야 한다.

제21조(정보보호전문업체의 지정취소 등) 정보통신부장관은 정보보호전문업체가 다음 각호의 1에 해당하는 때에는 정보통신부령이 정하는 바에 따라 정보보호전문업체의 지정을 취소하거나 3월 이내의 기간을 정하여 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호 내지 제3호에 해당하는 때에는 정보보호전문업체의 지정을 취소하여야 한다.

1. 속임수 그 밖의 부정한 방법으로 지정을 받은 때
2. 제17조제4항의 규정에 의한 지정기준에 미달한 때
3. 제18조의 규정에 의한 결격사유에 해당된 때(임원이 결격사유에 해당된 날부터 3월 이내에 당해 임원을 개임한 때를 제외한다)
4. 업무를 수행하면서 알게 된 정보를 오용 또는 남용하여 주요정보통신기반시설의 운영에 장애를 가져온 때
5. 그밖에 이 법 또는 이 법에 의한 명령을 위반한 때

제22조(보고 등) ①정보통신부장관은 주요정보통신기반시설의 정보보호를 위하여 특히 필요하다고 인정하는 경우에는 정보보호전문업체에게 관련 서류 또는 자료를 제출하게 할 수 있다.

② 정보보호전문업체는 제1항의 규정에 의하여 관련서류 또는 자료의 제출을 요구받은 때에는 특별한 사유가 없는 한 이에 응하여야 한다.

제23조(기록·자료의 보존 등) ①정보보호전문업체는 제17조제

1항제1호의 규정에 의한 주요정보통신기반시설의 취약점 분석·평가업무와 관련하여 작성한 기록 및 자료를 안전하게 보존하여야 한다.

② 정보보호전문업체는 제21조의 규정에 의하여 지정이 취소되거나 업무를 폐지한 때에는 제1항의 규정에 의한 기록 및 자료를 관리기관의 장에게 반환하거나 이를 폐기하여야 한다.

③ 제2항의 규정에 의한 관련기록 및 자료의 폐기에 관하여 필요한 사항은 정보통신부령으로 정한다.

제6장 기술지원 및 민간협력 등

제24조(기술개발 등) ①정부는 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다.

② 정부는 정보통신기반시설의 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다. 이 경우 이에 소요되는 비용의 전부 또는 일부를 지원할 수 있다.

제25조(관리기관에 대한 지원) 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 지원을 할 수 있다.

제26조(국제협력) ①정부는 정보통신기반시설의 보호에 관한 국제적 동향을 파악하고 국제협력을 추진하여야 한다.

② 정부는 정보통신기반시설의 보호에 관한 국제협력을 촉진하기 위하여 관련기술 및 인력의 국제교류와 국제표준화 및 국

제공동연구개발 등에 관한 사업을 지원할 수 있다.

제27조(비밀유지의무) 다음 각호의 1에 해당하는 기관에 종사하는 자 또는 종사하였던 자는 그 직무상 알게된 비밀을 누설하여서는 아니된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

1. 제9조제3항의 규정에 의하여 주요정보통신기반시설에 대한 취약점 분석·평가업무를 하는 기관
2. 제13조의 규정에 의하여 침해사고의 통지 접수 및 복구조치와 관련한 업무를 하는 관계기관 등
3. 제16조제1항 각호의 업무를 수행하는 정보공유·분석센터

제7장 벌칙

제28조(벌칙) ①제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

② 제1항의 미수범은 처벌한다.

제29조(벌칙) 제27조의 규정을 위반하여 비밀을 누설한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

제30조(과태료) ①다음 각호의 1에 해당하는 자는 1천만원 이하의 과태료에 처한다.

1. 제11조제1항의 규정에 의한 보호조치 명령을 위반한 자
2. 제16조제2항의 규정에 의한 통지를 하지 아니한 자
3. 제20조의 규정에 의한 신고를 하지 아니한 자

4. 제22조제2항의 규정을 위반하여 관련서류 또는 자료를 제출하지 아니하거나 허위로 제출한 자
5. 제23조제2항의 규정을 위반하여 기록 및 자료를 반환하거나 폐기하지 아니한 자

② 제1항의 규정에 의한 과태료는 대통령령이 정하는 바에 따라 관계중앙행정기관의 장 또는 정보통신부장관(이하 "부과권자"라 한다)이 부과·징수한다.

③ 제2항의 규정에 의한 과태료처분에 불복이 있는 자는 그 처분의 고지를 받은 날부터 30일 이내에 부과권자에게 이의를 제기할 수 있다.

④ 제2항의 규정에 의한 과태료처분을 받은 자가 제3항의 규정에 의하여 이의를 제기한 때에는 부과권자는 지체없이 관할법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할법원은 비송사건절차법에 의한 과태료의 재판을 한다.

⑤ 제3항의 규정에 의한 기간 내에 이의를 제기하지 아니하고 과태료를 납부하지 아니한 때에는 국세체납처분의 예에 의하여 이를 징수한다.

부 칙

<제6383호, 2001.1.26>

이 법은 2001년 7월 1일부터 시행한다.

참고문헌

[1] 김제영 외, 암호학 개론, 경문사, 2000.

[2] 박상서, 이진석, 박춘식, "정보전 개념과 대응 기술", 정보과학회지, 제18권 제12호(2000), pp. 8-19.

[3] 백용기, "국방정보보호 정책방향 연구", 한국국방연구원, 2001.

[4] 서동일, 윤이중, 조현숙, "정보전 대비 실시간 침입자 감지 및 경보네트워크 구성방안", 정보과학회지, 제18권 제12호(2000), pp. 36-44.

[5] 신건영, "정보전 현황과 대응방안", 제1회 사이버 테러 정보전 컨퍼런스, 2002.

[6] 신장균, "UNIX 네트워크의 보안평가기준 및 검증방법 연구", 한국전자통신연구소, 1993.

[7] 이강신, 김학범, 이홍섭, "국내외 정보보호관리 모델에 관한 고찰", 정보보호학회지, 제11권 제3호(2001). pp. 24-37.

[8] Burnett, Paine, RSA Security's Official Guide to Cryptography, McGwraw-Hill, 2001.

[9] Buchmann, Introduction to Cryptography, Springer, 2001.

[10] Mel, Baker, Cryptography Decrypted, Addison-Wesley, 2001.

[11] http://www.kias.or.kr/ (한국사이버테러정보전학회)

[12] http://www.iatf.net/(Information Assurance Technical Framework Forum)

[13] http://www.iwar.org.uk/(IWS - The Information Warfare Site)

[14] http://www.nps.navy.mil/iwag/(Information Warfare Academic Group; Naval Postgraduate School)

[15] http://www.terrorism.com/iwdb/(the Information Warfare Database;

Georgetown University)

[16] Libicki, Martin, "What is Information Warfare?" National Defense University, ACIS Paper 3, August 1995.

[17] Schneider, Applied Cryptography, John wiley & sons, Inc, 1996.

[18] US DoD Chief Information Officer, Annual Information Assurance Report, 2000.

[19] US DoD, FM 3-13 Information Operations, 1998.

[20] US DoD, MCTL(Militarily Critical Technologies List) Section 10: Information Systems Technology, March 2002.

[21] Whitehead, Yulin G., "Information as a weapon," Master Thesis, Air University, 1999.

[22] Waltz, Edward, Information Warfare-Principles & Operations, Artech house. 1998.

저자소개

김제영

서울대학교 계산통계학과 졸업
미시간대학교 대학원 졸업(박사, 통계학)
현재 육군사관학교 수학과 교수

신장균

서울대학교 산업공학과 졸업
고려대학교 대학원 졸업(박사, 전산학)
현재 육군사관학교 전산학과 교수

김정헌

서울대학교 수학과 졸업
일리노이대학교 대학원 졸업(박사, 수학)
현재 육군사관학교 수학과 교수

軍事硏究叢書 第40集

2002. 8월

저 자 : 김제영(수학교수) / 신장균(전산학교수)
김정헌(수학교수)

2002년 8월 27일 초판 1쇄 인쇄

2002년 8월 28일 초판 1쇄 발행

발행처/ 육군사관학교 화랑대연구소

인쇄/제본 경희정보인쇄(주) Tel : 02)2263-7534