정보보증: 컴퓨터 보안의 새로운 패러다임

한국정보보호센터 이철원* · 김홍근*

1. 서 론

1970년대 초반 미국은 국방부를 중심으로 수작업으로 진행하여 왔던 주요 문서작업을 컴퓨터를 이용한 자동화된 문서처리시스템으로 전환하면서 컴퓨터 보안에 커다란 관심을 쏟아 왔다. 이와 더불어, 컴퓨터를 이용한 통신기술이 발전함에 따라, 통신보안, 네트워크 보안기술도 함께 발전하였으며, 많은 안전한 컴퓨터시스템이 개발되어 왔고, 현재도 컴퓨터 및 네트워크 보안기술이 개발되고 있다. 이러한 컴퓨터, 네트워크, 통신 관련 보안은 전통적으로 ComSec (Communication Security), CompuSec(Computer Security), NetSec(Network Security)으로 분류하여 왔으며, 이 세 가지 분야의 정보보호 목표는 정보의 비밀성, 무결성, 가용성을 보장하는 것이었으며, 특히 정보의 비밀성 보장에 주초점을 맞추고 암호, 접근통제 등 관련 기술이 개발되어 왔다.

한편, IT 기술의 발달과 함께 도로, 항만, 댐, 통신, 금융, 전력 등 기존 사회간접자본이 IT 기술을 이용한 정보화를 진행하고 있으며 날이 가면 갈수록 IT기술의 의존도가 높아지고 있다. 소위 정보기반구조(Information Infrastructure)가 국가적 및 전세계적으로 구축되어 가고 있으며, 우리나라도 초고속정보통신망의 구축이라는 범국가적인 사업을 추진하고 있다. 이러한 정보기반구조에는 기능을 발휘하지 못하거나 파괴될 경우 자국의 방위 및 경제안보에 치명적인 영향을 미칠 수 있는 국가의 일부 핵심적인 기반구조가 포함되며 이를 주요 기반구조(Critical Infrastructure)라 한다. 주요 기반구조에는 통신, 전력, 가스 및 유류의 저장 및 운송, 금융과 재정, 급수시스템, 긴급상황서비스(의료, 경찰, 소방 및 응급구조 포함) 및 정부서비스의 지속 등이 포함된다[1].

그러나, IT 기술의 발달과 더불어 주요 기반구조에 대한 각종 해킹, 바이러스, 사이버 테러의 가능성이 높아지면서, 침해 발생시 예상되는 피해 파급효과는 국가안보는 물론 국가경제의 경쟁력을 악화시키고 국민 개개인의 프라이버시에까지 심각한 피해를 줄 수 있다. 미 대통령령 13010에 의하여 설립된 주요기반구조 보호 대통령위원회(PCCIP, President's Commission on Critical Infrastructure Protection)에서 작성한 다음의 침해 시나리오는 주요 기반구조에 대한 침해가능성 및 침해로 인한 피해가 어느 정도인지를 충분히 예측할 수 있게 해준다. "미국에서 약 1만6천㎞ 떨어진 곳에서 해커가 컴퓨터와 모뎀을 조작, 미국 전역을 관장하는 전화교환센터에 침투한다. 이 센터는 전국 전화회선을 통제할 뿐만 아니라 전국 배전망, 철도, 심지어 항공망도 통제한다. 해커는 전화교환센터 침투를 통하여 국가기간시설들을 하나씩 마비시켜 나간다. 처음에는 지역 전력망을 무너뜨린뒤 항공교통시스템을 교란시킨다. 다음의 목표는 경찰비상연락망이다[2]." 실제로, 미국의 국가보안국(NSA, National Security Agency)에서는 '97년 컴퓨터 전문가를 북한의 해커로 위장하여 미 태평양사령부 지휘통제소에 대한 해킹을 감행하여 미 병력

* 정회원

을 완전히 마비시키기도 하였으며, '98년에는 해커를 동원한 훈련에서 간단히 전력공급망을 차단시킬 수 있음을 확인한 것으로 전해지고 있다[3].

또한, IT 기술이 발전함에 따라, 기반구조간의 상호 의존성이 증가하게 되었다. 금융기반구조는 통신 및 전력기반구조에 의존하며, 전력기반구조는 통신기반구조에 의존하게 되며, 통신기반구조는 전력기반구조에 의존하게 된다 따라서, 한 기반구조의 피해는 다른 기반구조에까지 영향을 미치므로 특정 기반구조 하나만의 보호가 아니라 관련된 모든 기반구조를 보호하려는 노력이 조화되어야 한다. 따라서, 세계 각국에서는 자국의 주요 기반구조를 보호하기 위한 범 정부적 정책개발, 각 기반구조별 보호기술개발 및 각 기반구조의 보호 노력을 조정하여 국가적인 기술개발 계획을 수립하고 있다. 특이할 만한 점은 기반구조를 보호하기 위하여, 전통적으로 강조되어 왔던 정보의 비밀성 혹은 무결성보다는 정보의 가용성 측면을 고려한 정보보호 기술개발을 강조한다는 점이다. 즉, 기반구조의 신뢰성과 지속성을 확보하는데 필요한 기술개발에 초점을 맞추고 막대한 예산 및 인력을 투입하고 있다.

본 고에서는, 주요 기반구조를 보호하기 위한 국외 기술개발 사례를 분석하여 정보보호 기술의 개념 변화를 고찰하고 이를 기반으로 국내 주요 기반구조를 보호하기 위한 기술개발 방향을 제시한다.

2. 정보보증이란?

2.1 주요 기반구조의 취약성

지난 10년간 개인용 컴퓨터, 워크스테이션, 데이터베이스 및 메인프레임은 분산 환경의 네트워크 지향 및 다양한 정보에 대한 신속한 수집 등을 위하여 상호 연결되고 있으며, 이러한 상호간의 연결 양상은 아주 빠르게 확산되고 있다. 인터넷이나 기타 데이터 네트워크에 정부용 네트워크, 금융 네트워크, 전기 공급을 통제하는 네트워크, 심지어 군용 네트워크까지 접속되어 가고 있다. 이와 같이 네트워크가 광범위하게 확장되어 복잡한 형태를 구성하고, 경제적인 측면에서도 기업간 경쟁 과열로 인한 생산성 제고 노력 등이 날이 갈수록 주요 기반구조의 운영, 유지 및 감시에 필요한 정보 시스템에 대한 의존도를 증가시켰다. 이러한 H/W, S/W적 복잡도는 그 자체로써 커다란 취약성이 될 뿐 아니라, 주요 기반구조를 구성하는 네트워크 구성요소가 검증이 안된 상용의 IT 제품을 사용함에 따라 기반구조는 외부의 공격에 취약성을 띠게 되었다. 또한, 기반구조 자체의 정보 시스템간 또는 기반구조 상호간 연결되는 특성으로 인하여 주요 기반구조에 대한 위협 범위와 위협의 잠재성이 커지게 되었다. 즉, 과거에는 인식할 필요도 없었던 분야의 취약성이 새롭게 나타나게 되었다. 실제로 지난 수년동안 다양한 신종의 해킹기법을 이용하여 통신망을 이용한 침입자들이 주요 통신업체, 인터넷 서비스 제공업체 및 다양한 최종 사용자 시스템에 침입하였다. 침입자 중에는 외국의 정보 기관, 산업 스파이, 조직화된 범죄 집단, 해커, 내부 침입자 등이 포함되어 있다. 주요 기반구조에 나타날 수 있는 주요 취약성으로는 다음과 같은 것이 있다.

- 컴퓨터 등 정보통신시스템의 보급 확대로 인한 정보통신시스템 자체의 버그 및 프로그램 오류, mis-coding, malfunction, 시스템의 복잡화에 따른 조작오류 등
- 정보통신프로토콜의 개방화 및 표준화에 따른 취약요소 증가
- 통신망 제어를 위한 망관리시스템의 접근 용이성
- 미국, 일본, 호주 등 전세계적인 인터넷 구축을 위한 국내 접속점 증가로 인하여 다양한 접근경로 제공
- 국내 인터넷 사업자간의 연동을 위한 연동센터 증가 및 연동센터 침해로 인한 인터넷 마비 가능성 존재
- 각 ISP가 유지하는 DNS 서버에 대한 침해 위협 증가

상기와 같은 취약성을 이용하여, 주요 기반구조를 침해하는 침입자에 대한 정보를 입수하거나, 침입자의 신원을 밝히는 것은 매우 어려운 일이다. 침입자는 상호 연결된 다른 시스템 속으로 숨어 버릴 수 있으며, 또 이전에 침입한 시스템에서 다른 시스템으로 침입을 시도하는 간접공격을 사용하기도 한다. 침입자는 침해하고자 하는

대상 시스템이 사이버 공간에 위치하여 있기 때문에 지리적, 공간적, 정치적 경계가 없기 때문에 익명성을 가지며, 법적인 중재도 불가능하여 이전의 국가적 성역도 무력화된다. 또한 주요 기반구조를 침해하는 기술은 상대적으로 개발비용이 적게 들어 적은 투자에 비하여 아주 높은 타격을 상대방에게 끼칠 수 있다. 더욱 위험한 것은 이러한 침해 기술이 상대적으로 간단하며 조금만 노력하면 어디에서나 쉽게 구할 수 있다는 것이다. 법적인 측면에서도 현재 주요 기반구조를 대상으로 행해지고 있는 침해행위에 대한 처벌이 매우 모호하게 다루어지고 있다.

상기와 같은 여러 가지 특성으로 인하여 주요 기반구조 침해를 막기 위한 법·제도·기술적 대응 방안 마련에 상당한 어려움이 수반한다. 이와 같은 상황에도 불구하고, 주요 기반구조 침해에 대응하기 위한 법·조직·제도 및 기술적인 보호 대책을 서둘러 정비하지 않으면 향후 주요 기반구조 침해에 따른 개인의 프라이버시 침해, 국가경제 피폐, 국가안보 위협에 이르기까지 상당 부분 우리의 현실로 나타나게 될 것이다. 본 고에서는 기술적 대책의 일환으로 기존의 전통적인 정보보호 관점이 아닌 주요 기반구조의 생존성을 제고하기 위한 기술개발 방향을 제시하고자 한다.

2.2 정보보증의 정의

정보보증이란 1996년 12월 미 국방차관 White가 미 국방부 지침 S-3600.1 정보작전(DoD Directive S-3600.1, Information Operations)에 서명함으로써, 기존의 정보전에 대한 미 국방부의 인식이 갱신되면서 대두된 개념이다[4]. 물론, 정보보증의 개념자체가 이때 새롭게 부각된 것은 아니지만, 국방부지침 S-3600.1로 인하여 정보보증은 국방부, 연방정부부처, 공공기관 및 산업체와의 협력체제를 강화시켜 주는 기틀을 제공하였다. 미 국방부에서 정보전이란 개념을 폐지하고 정보보증이란 용어를 사용하게된 배경은 미국의 국가방위가 IT 기술을 기반으로 하는 국가의 주요 기반구조에 의존한다는 사실을 인식하였기 때문이다. 즉, 해킹, 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서는 주요 기반구조를 소유·운영 및 관리하는 국방부를 비롯한 연방정부, 공공기관 및 산업체의 보호노력을 통합하고 조정하는데 그 성공의 열쇠가 있다고 인식한 결과이다. 따라서, 정보보증이란 용어자체가 함축하고 있는 의미는 비밀로 분류된 국가정보 및 정보시스템을 보호하는 소위 INFOSEC이라는 기존의 정보 및 정보시스템 보안보다 광의의 개념이다.

정보보증이란 기반구조를 구성·운영 및 통제하는 정보와 정보기술에 대한 침해에 대한 보호, 신뢰성 및 가용성을 보장하는 것을 말한다. 이미, 미 국방부에서는 '97년 8월 합참의장훈령(Chairman, Joints Chiefs of Staff Instruction) 6510.01B를 공포하여 다음의 (그림 1)과 같은 보증모델을 제시한 바 있다[5].

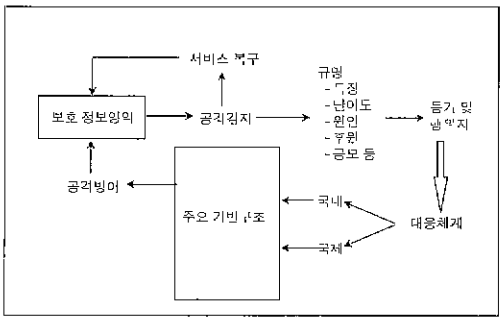

그림 1 정보보증 모델

그림 1에서 보는 바와 같이 주요 기반구조를 보호하기 위한 정보보증은 침해에 대한 방어, 기반구조 파괴, 침입 및 침해에 대한 탐지, 기반구조에서 제공하는 서비스 복구, 그리고 추후의 침입 혹은 위협에 대응하기 위하여 일련의 대응체계 등 4개의 큰 축으로 구성된다

3. 정보보증 관련 연구

주요 기반구조를 보호하기 위한 다양한 형태의 정보보호 기술개발 노력이 세계 여러 나라에서 진행되고 있다. 그러나, 미국을 제외한 대부분의 국가는 초보적인 단계를 벗어나지 못하고 있으며, 기술개발의 초점 또한 공격적인 침해수단 개발에 치중하고 있다. 본 장에서는 주요 기반구조의 가용성, 신뢰성, 지속성 등을 보장하기 위한 미 국방부 DARPA(Defense Advance Research Projects Agency)의 정보 생존성(Information Survivability), NRC(National Research

Council)의 정보시스템 신뢰성(Information System Trustworthiness)을 분석하였다.

3.1 정보 생존성(Information Survivability)

1996년 DARPA/ITO(Information Technology Office)에서는 국방부 시스템에 대한 외부의 어떤 공격에 대해서도 군 정보시스템의 중요 서비스 및 기능에 대한 최소한의 성능을 지속시키기 위하여 정보 생존성 프로그램을 시작하였다. DARPA의 정보 생존성 프로그램 매니저인 Hoiwe Shrobe에 의하면 생존성이란 "시스템이 공격을 받은 이후에도 중요 서비스 및 기능에 대하여 적당한 성능을 지속시킬 수 있는 시스템의 능력"이라고 정의하고 있다. 일반적으로 정보 생존성 프로그램은 다음과 같은 특징을 가지고 있다[6].

- 물리적 공격, 정보 공격, 내부 침입 등의 가능성을 가정하고 공격의 파급 효과 최소화 또는 정보통신시스템에 내재된 결함전파의 최소화 관련 보안 이슈에 주안점을 둔다.
- 시스템이 공격을 받은 이후에도 서비스 및 기능이 중단되지 않고 최소기능을 유지해야 한다는 점에서 전통적인 보안의 관점과 다르다.
- 기밀성, 인증, 부인방지 등과 같은 전형적인 보안개념보다는 신뢰성, 가용성, 안전성(safety)과 같은 보안특성에 의존한다.
- 인공지능 기술과 결합, 생물학적 모델의 체택 등 몇 가지 파격적인 관점을 가지고 있다.

이 프로그램의 목적은 고도로 통합되고 복잡한 주요 기반구조 특히, 군 정보시스템이 신뢰를 가지게 하는 것이다. 미국의 군 시스템들은 상용 통신과 컴퓨터 기반구조에 의존하고 있으며 이들과 상호연동되어 운영되고 있다. 전세계적으로 연결된 인터넷은 미국 내에 있는 정보 시스템에 대한 공격이 세계 어느 곳에서든 이루어질 수 있다는 것을 의미한다. 이러한 중요 정보 시스템에 대한 다양한 공격, 정확히 예상되지 않는 공격에 대하여 중요 정보 시스템이 적절한 기능을 유지할 수 있는 기술을 개발하는 것이 이 프로그램의 목표이다. 이 목표를 달성하기 위하여 정보생존성 프로그램은 다음과 같이 4가지 연구 분야로 나누어 진다.

- 고신뢰 네트워킹(High Confidence Networking)
- 고신뢰 컴퓨팅 시스템(High Confidence Computing)
- 래퍼와 구성(Wrappers and Composition)
- 대규모 시스템의 생존성(Survivability of Large Scale Systems)

상기의 4가지 기술은 다음의 그림 2와 같이 공격에 대한 강한 차단막을 생성하고 악의 또는 의심스러운 행위를 탐지하며, 그러한 행위를 격리시키거나 쫓아버림으로써 정보 공격에 대하여 중요 시스템 기능을 지속시키는 최소한의 요건을 보장하기 위하여 사용된다[7].

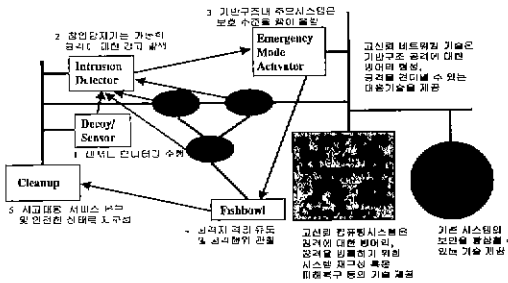

그림 2 정보 생존성

상기 4가지 기술 분야 중 "래퍼와 구성"은 전통적인 시스템에 대한 공격을 막기 위하여 시스템에 방어벽을 쉽게 추가할 수 있는 래퍼 기술, 정형화 방법 및 구성 기법(compositional technique) 등을 개발하는 것이다. 또한 이러한 기술을 이용하여 강화된 시스템의 보호능력 및 생존력을 평가할 수 있는 기술을 개발한다.

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

고신뢰 네트워킹은 네트워크 서비스의 중단이나 침입과 같은 공격에 대응하기 위한 강한 침입

차단 기능을 개발하고, 현재 그리고 새로운 네트워크 기술에 보호 메커니즘을 추가하기 위한 기술을 개발한다.

표 1 래퍼 및 구성에 대한 기술개발 필요성 및 관련기술

필요성	접근방법
COTS 제품들은 신뢰성이 없으며 보안 위험성을 가지고 있음	· 전통적 시스템 및 COTS 구성요소들의 보안 및 생존기능을 증대하기 위한 래퍼 기술 개발
시스템 구성요소들과 래퍼 기술의 통합에 따른 신뢰성 보장	· 생존력있는 구성요소에 대한 엔지니어링 규칙 개발 · 시스템 구성요소 및 래퍼 기술의 통합에 따른 보안 및 생존 특성을 예측할 수 있는 도구 개발
제품 또는 시스템의 취약성/보안 내구성 평가	· 코드 및 실행파일에서 취약성을 알아내기 위한 기술 · 보안 취약성의 알려진 분류에 기초한 공격 모델:보안 평가 도구를 개발하기 위하여 이를 사용

표 2 고신뢰 컴퓨팅에 대한 기술개발 필요성 및 관련기술

필요성	접근방법
전통적인 OS 보안 개념은 오늘날과 같이 복잡한 보안정책을 사용하는 네트워크 환경에 적합하지 않음	· 접근통제 및 보안정책 컴파일러를 위한 DTE(Domain-Type Enforcement) 개발
현재 보안 OS 기술은 시장 규모가 적으며 특수 목적의 OS만 이용할 수 있는 보안 기능을 가지고 있음	· 프로세스 네스팅(nestmg) 및 보안 확장과 같은 기술을 사용하여 차세대 통신 기반 OS에 보안 및 지원 소비 제어 결합
여러 중요 특성을 만족하는 분산된 시스템 구축 필요	· 안전성, 실시간, 결함 허용성간의 적당한 tradeoff를 허용하는 프레임워크를 제공하는 미들웨어 서비스 개발
기타	· 신뢰성, 정책 및 메커니즘을 협상하기 위하여 역할, 작업 흐름 모델 및 프로토콜에 기반한 권한부여 · 접근통제 및 메카니즘을 미들웨어 서비스(CORBA)로 통합

대규모 시스템의 생존성은 침입과 의심스러운 사건에 대하여 신뢰성 있는 탐지를 하고, 기반구조가 탐지된 사건에 대응하며, 침입자에 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.

다음의 표 1에서 표 4는 각 기술개발 분야의 필요성 및 주요 기술개발 내용을 보여주고 있으

표 3 고신뢰 네트워크에 대한 기술개발 필요성 및 관련기술

필요성	접근방법
공동 이용이 가능하고 접근할 수 있는 정보보호 서비스 창출	· 개방형 정보보호 구조 및 다중 계층 정보보호 협상 프로토콜 개발
서비스의 성능이 저하되는 동안에도 좋은 결과를 산출할 수 있는 성능유지	· 침입 내성 기술 개발 및 비밀 공유
악의있는 공격에 대한 생존	· 피해 컴포넌트의 식별 및 분리를 위한 침입탐지 API와 메커니즘에 대한 인터페이스 개발
응용 및 기반구조에 대한 생존력있는 변화 기술	· 경매, 다중 에이전시 계약 및 다른 전자적인 트랜잭션을 지원하는 정보보호 서비스
다른 정책을 가진 그룹간의 안전한 통신	· 새로운 알고리즘 및 정책 언어 개발
생존력있는 기반구조	· 안전하고 변경가능한 기본 에이전트, 노드 및 라우팅 개발

표 4 대규모시스템의 생존에 대한 기술개발 필요성 및 관련기술

필요성	접근방법
침입탐지 기술은 증명되지 않고 신뢰성이 없으며 잘 알려진 이벤트의 작은 부분만을 탐지하고 있으며, 확장성이 부족하고 빠른 대응과 피해 복구를 지원하지 않음	· 현재의 침입탐지 기술을 확장 · 침입탐지 시스템간 연동 기술 연구 · 평가 및 자동적인 대응에 대한 기술 연구
국가 비상사태 또는 IW 공격 때 중대국면(위기) 모드 운영을 제공하지 않음	· 의심스러운 공격이 있는 동안 중요 작업에 신뢰성있는 자원을 할당하기 위한 기술 개발
대규모 DoD 시스템의 생존을 예견하기 어려움	· 대규모 시스템에 응용할 수 있는 분석 모델 및 red team 운영

며, 참고적으로 DARPA에서는 104가지의 프로젝트가 종료되었거나 진행중에 있다.

국방부는 이 프로그램에 의하여 개발되는 기술들을 이용한 COST 제품 사용을 통하여 비용을 절감하고, 국방부에서 요구하는 보안성을 다양한 고객에 제공하기 위하여 기술 이전 전략을 세우고 있다. DARPA는 이를 위하여 국방정보체계국(DISA, Defense Information System Agency), 국가보안국(NSA)과 JTO(Joint Technology Office)를 설립하였으며 각 분야별로 표준화 기구, 산업체, 대학 등과의 협력을 통한 기술이전 계획을 세우고 있다.

3.2 정보시스템 신뢰성(Information System Trustworthiness)

정보시스템 신뢰성에 대한 연구는 DARPA와 ISSR(Information System Security Research) JTO의 요청에 의하여 NRC(National Research Council) 산하의 컴퓨터 과학 및 통신위원회(Computer Science and Telecommunications Board)에서 연구를 시작하였다[8]. 이 연구에서는 주요 기반구조를 구성하는 하부 개념으로써, 네트워크화된 정보시스템(Networked Information System)이란 용어를 사용하는데, 네트워크화된 정보시스템은 컴퓨터, 통신시스템 및 이를 사용하고 운용하는 사람의 통합체로 정의하고 있다. 네트워크화된 정보시스템은 기존의 시스템과 비교하여 다른 시스템과 많은 인터페이스를 가지고 있고, 시스템을 제어하기 위한 알고리즘을 사용하며, 상용의 제품(COTS S/W and H/W)을 많이 사용하고 있으며, 시스템 구성요소에 대한 확장성을 가지고 있다고 특성화하였다. 또한 네트워크화된 정보시스템의 신뢰성을 "환경요인으로 인한 붕괴, 사람의 실수, 악의적인 공격, 설계 및 구현시의 결함에도 불구하고 올바르게 동작하는 시스템"으로 정의하였다. 이 연구에서 정보시스템의 신뢰성을 구성하고 있는 요소를 크게 S/W, H/W 설계 및 구현시 결함을 제거할 수 있는 소프트웨어 공학적 측면의 보증, 시스템 보안 및 결함허용 등의 3가지로 나누었다. 실질적인 연구의 수행을 위하여, 공중전화망과 인터넷의 신뢰성(Public Telephone Network and Internet Trustworthiness), 네트워크화된 정보시스템을 위한 소프트웨어(S/W for Networked Information System) 개발, 보안기술의 새로운 개발 방향 제시(Reinventing Security), 기존의 시스템에 신뢰성을 부여하는 방법(Trustworthy Systems from Untrustworthy Components), 경제적 및 공공정책 측면, 신뢰성 구현을 위한 연구개발 등의 6가지 세부 분야로 나누어서 연구를 진행하여 '99년 1월 "Trust in Cyberspace"란 제목으로 최종 보고서를 발간하였다. 각 분야별 대표적인 발견사항(Findings) 및 위원회 권고사항은 다음과 같다[9].

3.2.1 공중전화망과 인터넷 보호

- 공중전화망은 새로운 취약점을 가지고 있는 소프트웨어와 데이터베이스에 더욱더 의존하고 있으며, 망 사업자의 새로운 사업 개시로 인하여 새로운 취약점이 발생하며, 이에 대한 보호대책이 개발되고 구현되어야 한다.
- 어떤 측면에서 보면, 인터넷의 프로토콜이 향상됨에 따라, 프로토콜 스택의 상위계층에서 보호 대책이 많이 사용됨에 따라 인터넷은 더욱더 안전해지고 있다. 그러나, 증가되는 인터넷 기반구조의 복잡성은 취약성을 더욱 증가시키며, 인터넷의 종단점(호스트)도 매우 취약하다. 인터넷은 공격과 기능정지에 너무 민감해서 인터넷을 통하여 주요 기반구조를 통제하기 위한 기본수단이 될 수 없다.
- 운영상의 오류는 공중망 및 인터넷 기능 정지의 주요 원인이다. 이 오류의 일부는 알려진 기술을 구현함으로서 방지될 수 있지만, 다른 오류들의 방지대책을 개발하기 위한 연구가 요구된다.

3.2.2 신뢰성 증진을 위한 S/W

- 신뢰성있는 네트워크화된 정보시스템의 설계는 시스템 구조와 프로젝트 계획 측면의 관점에서 새롭게 부각되는 연구분야이다.
- 네트워크화된 정보시스템을 개발하기 위하여 네트워크화된 정보시스템을 구성하는 하부시스템을 신뢰성있게 통합해야 하지만, 이러한 방법에 대해서는 거의 알려져 있지 않다.
- 최근의 프로그래밍 언어는 신뢰성을 증진시키는 특성을 포함하고 있으며, 신뢰성 증진

에 대한 프로그래밍 언어적 접근방법은 최근의 관련 연구에서 볼 수 있듯이 그 가능성이 더욱 증가될 것이다.

- 정형화 방법은 하드웨어 개발 및 요구사항 분석을 위하여 상업 및 산업 환경에서 성공적으로 사용되었고 소프트웨어 개발을 위해서는 일부가 성공적으로 사용되었다. 정형화 방법에 대한 기초연구에 대하여 지원을 계속하여야 한다.

3.2.3 보안기술의 새로운 방향 제시

- 지난 몇 십년 동안 보안에 관한 연구는 어떠한 사용자가 데이터나 다른 시스템 객체에 접근할 수 있는지를 기술함으로서 비인가된 접근으로부터 정보를 보호하는데 초점을 맞추는 접근통제 정형화 정책 모델에 기반을 두었다. 이와 같은 모델은 현재의 정보환경에 적합치 않으며, "위험은 존재한다, 위험은 제거될 수 없다, 위험은 전파가 가능하다"라는 속성을 고려한 보안모델 개발을 하여야 한다.
- 암호 인증 및 하드웨어 토큰의 사용은 인증을 구현하는데 있어서 가장 좋은 방법이다.
- 키 관리 기술을 좀더 널리 보급하기에는 아직까지 어려움이 존재하며, 공개키 기반구조, 특히 대규모 기반구조에서의 경험은 거의 없으므로, 이에 대한 연구 및 개발을 지속적으로 추진하여야 한다.
- 네트워크화된 정보시스템이 분산 시스템이기 때문에 네트워크 접근 통제 메커니즘은 네트워크화된 정보시스템의 보안에 중요한 역할을 한다. 가상사설망(VPN, Virtual Private Networks)과 침입차단시스템(Firewall)은 유망한 기술이라는 것이 증명되었으며 미래에는 더욱 주의를 끌 것으로 예상된다.
- 이동코드의 사용이 급속하게 증가하고 있다. 따라서, 악성 이동코드를 방지하기 위한 기술이 개발되어야 한다.
- 서비스 거부 공격에 대한 방어는 가용성이 시스템의 중요 특성이므로 네트워크화된 정보시스템의 보안을 위해 매우 중요하다. 서비스 거부 공격을 방지하기 위한 일반적 기법의 연구가 시급히 요구된다.

이 외에도 신뢰성 구현을 위한 연구 및 개발 측면에서 NRC는 민간부분과의 연구개발 협력을 강화하고, 장기간의 연구노력을 기울이고 홍보·전문인력 양성에 힘쓸 것을 권고하였다. 자세한 권고사항은 참고문헌 [9]를 참조하기 바란다.

4. 정보기반구조 보호 기술 개발 방향

정보화의 급속한 진전에 따라, 우리나라의 주요 기반구조도 정보시스템 및 정보통신망에 대한 의존도가 나날이 높아가고 있다. 이러한 시점에서, 그 동안의 비밀성 위주의 정보보호 기술 개발관점에서 벗어나, 어떠한 경우라도 주요 기반구조가 제공하는 서비스의 지속성을 보장하여 줄 수 있는 새로운 기술개발 방향을 정립하여 보는 것도 큰 의의가 있으리라 생각된다.

국내에서 현재 구축되어 운영되는 주요 기반구조로는 금융, 운송(항공, 항만, 도로), 통신, 급수 및 용수, 에너지, 전자정부를 포함하는 정부서비스 등이 있다. 이러한 주요 기반구조를 보호하기 위해서는 기존의 비밀성에 입각한 정보보호도 중요하지만, 기반구조에 대한 침해가 발생하였을 시 기반구조의 최소기능이 동작하도록 하여 그 피해 파급효과를 최소화할 수 있는 가용성에 대한 보장이 더 중요하다고 할 수 있다. 기반구조에 가해지는 위협은 물리적 위협과 사이버 위협이 있을 수 있으며, 기반구조 보호기술은 전자적인 무기, 무선주파수를 이용한 공격, 컴퓨터를 기반으로 하는 공격 등을 모두 고려하여야 한다. 본 고에서는 다음과 같은 4가지 분야의 새로운 기반구조 보호기술을 제안하고자 한다.

- 주요 기반구조 생존성 강화 사업 : 주요 기반구조에 대한 사이버 침해로부터 주요기반구조의 서비스 지속성을 보장할 수 있는 다양한 기술 개발
  - 취약성 정보, 침해사고 사례, 다양한 위협 정보를 공유할 수 있는 Clearing House 구축
  - 정보기반구조의 최소필수 구성요소 지정 방법론 개발
  - 취약성 분석 및 평가기술 개발
  - 침입탐지기술 개발
  - 트랩도어 탐지기술 개발
  - 악성 이동코드 탐지기술 개발
  - 침해대응기술 개발

- 침해복구 및 기반구조 재구성 방법 개발

· 사이버공간 신뢰성 고도화 사업 : 기반구조의 주요 구성요소인 정보시스템에 대한 완전하고 보안성이 강한 방어벽을 만들며, 침해영향 평가를 위한 환경을 구축하고, 새로운 네트워크 기술에 보호 메커니즘을 추가하기 위한 기술 개발

- 우선적으로 리눅스 등 공개된 운영체제를 대상으로 하는 정보시스템 운영체제 보안기술(Secure OS) 개발
- 데이터베이스관리시스템 보안기술(Secure DBMS) 개발
- 대규모 정보기반구조의 위험을 분석하고 이에 대한 대책을 제시할 수 있는 위험분석 기술 개발
- 정보기반구조를 모델링하고, 정보기반구조에 대한 다양한 위협영향 평가, 현재의 보안대책 평가 및 대안을 제시하는 시뮬레이션 기술 개발
- 인터넷 확장을 대비하고, 궁극적으로 정보기반구조의 인터넷 의존도가 심화될 것에 대비한 차세대 인터넷 보안기술 개발
- 정보기반구조 주요 구성요소의 고장시에도 제기능을 발휘할 수 있는 고장감내(Fault Tolerance) 기술 개발
- 보안기술의 확장 및 상호 호환을 대비한 표준화 및 평가기준 개발

· 소프트웨어 고도화 사업 : 주요기반구조 보호를 위한 하부구조로써 보안 소프트웨어의 품질 향상 및 선진국과의 소프트웨어 개발 능력 차이를 극복할 수 있는 소프트웨어 공학 관련 기술 개발

- 보안을 고려한 소프트웨어 개발 방법론 개발
- 주요 보안기술을 재사용 가능하며, 보안기술 자체를 하나의 부품화하여 필요시 사용 할 수 있도록 하는 부품 라이브러리 개발
- 정형화 방법론 개발

· INFOSEC 고도화 사업 : 기존의 전통적인 정보보호 분야인 통신보안(COMSEC), 컴퓨터 보안(COMPUSEC), 네트워크 보안(NETSEC)의 고도화

- 유·무선 통신 보안기술 개발
- 데이터 복구기술 및 실시간 통신 데이터 복구기술 등 키 복구기술 개발
- 공개키 기반구조와의 통합을 고려한 키 관리기술 개발
- 차세대 암호시스템 개발
- 생체인증, 하드웨어 기반의 고기능 인증기술 개발
- 하드웨어 기반의 고성능 침입차단시스템 개발
- 전자문서 공증, 전자입찰, 전자화폐 등 전자상거래 보안기술 개발
- 전자선거, 정보은닉 등 암호 프로토콜 개발
- 보안서비스 API 개발
- 전자파 차폐기술

이 밖에도 기반구조를 보호하기 위한 기술개발에서 간과해서는 안 될 중요한 고려요소는 기반구조간의 상호의존성이며, 특히 기반구조의 생존성 강화 및 사이버공간 신뢰성 고도화 부분에서는 상호의존도를 고려한 연구개발을 진행하여야 한다.

5. 결 론

정보화의 진전에 따라 산업시대의 사회간접시설이 IT기술을 이용하여 자동화되고, 점점 더 정보시스템 및 정보통신망에 의존하고 있으며, 이러한 기반시설들이 국가의 경제 및 안보에 막대한 영향을 미치고 있다. 현재 미국, 일본 등 선진외국에서는 국가 주요기반구조의 지속적인 서비스 보장을 통한 국가사회의 안정적인 기능 수행을 위하여 기반구조를 외부의 침해로부터 보호하여 기반구조의 가용성을 보장하기 위한 노력을 꾸준하게 진행하고 있다.

본 고에서는 미국 등 선진외국에서 불고있는 정보보호의 새로운 전형인 정보보증에 대하여 분석하였으며, 이 결과 기반구조를 보호하기 위해서는 기존의 전통적인 정보의 비밀성 보장 측면보다는 정보의 무결성, 가용성, 신뢰성 등 서비스의 지속성 보장에 더 초점을 두고 있다는 사실을 알 수 있었다. 이와 같은 분석을 바탕으로 하여, 국내의 주요 기반구조를 보호하기 위한 새로운

기술개발 방향을 제시하였다. 이러한 방향제시가 올바르다고는 말할 수는 없지만, 분명한 것은 과거 많은 보안 전문가들이 주장한 전통적 정보보호의 강조는 변화하는 정보환경을 완전하게 반영할 수 없다는 것이다. 무엇보다도 물리적이나 사이버 공간을 이용한 공격시에도 기반구조가 가지고 있는 고유의 핵심기능을 지속적으로 수행할 수 있는 기술개발이 중요하다는 것을 강조하고 싶으며, 이러한 기술개발에는 보안관련 연구자뿐 아니라, 인공지능, 네트워크, 운영체제 등 다양한 컴퓨터 분야 전문가가 필요하다는 것을 강조하고 싶다.

참고문헌

[1] The Joint Staff, Information Assurance : Legal, Regulatory, Policy and Organizational Considerations, 3rd Ed., Sep. 1997.

[2] 한국정보보호센터, 통신망 정보보호 대책 연구, 1998. 12.

[3] 국방정보체계연구소, 정보전 대응체계 건설을 위한 종합발전계획연구, 1998. 12.

[4] DoD, Department of Defense Directive(DoDD) S-3600.1 Information Operations(IO), 9 Dec. 1996.

[5] DoD, Chairman of Joint Chiefs of Staff, Chairman, Joints Chiefs of Staff Instruction 6510.01B Defensive Information Operations, Draft, June 1997.

[6] DARPA/ITO, Information Survivability, http://www.darpa.mil/ito/research/is/index.html

[7] DARPA/ITO, Survivability Briefing, presented at the ARPATech '96 Systems and Technology Symposium, May 22-24, 1996.

[8] National Research Council, Information System Trustworthiness, Interim Report, Committee on Information Systems Trustworhiness, National Academy Press, 1997.

[9] National Research Council, Trust in Cyberspace, Committee on Information Systems Trustworthiness, National Academy Press, 1999.

이 철 원

1987 중남대학교 수학괴(이학사)
1989 중앙대학교 전자계산학과(이학석사)
1989~1996 한국전자통신연구원 선임연구원
1996~현재 한국정보보호센터 시스템기술팀 선임연구원
관심분야 컴퓨터 및 네트워크 보안, 주요기반구조 보호, 정보보호 시스템 평가기준
E-mail : leecw@kisa.or.kr

김 홍 근

1985 서울대학교 컴퓨터공학과(공학사)
1987 서울대학교 컴퓨터공학과(공학석사)
1994 서울대학교 컴퓨터공학과(공학박사)
1994~1996 한국전산원 선임연구원
1996~현재 한국정보보호센터 시스템기술팀장
관심분야 컴퓨터 및 네트워크 보안, 병렬처리
E-mail hgkim@kisa.or.kr