通信情報保護學會誌
第9券 第2號 1999. 06

정보통신기반구조 보호 현황

이 철원*, 이 병각*, 김 현주*, 김 홍근*

요 약

국가 정보통신기반구조는 국방과 같은 전통적인 군사적 목적이외에 정보통신시스템, 전력 및 가스 등과 같은 에너지시스템, 금융 및 재정시스템, 영공관리시스템을 포함하는 교통시스템, 급수체계 등과 같이 핵심적인 응용분야에까지 매우 다양하게 적용되고 있다. 이러한 정보통신기반구조가 인터넷 등을 이용하여 상호 접속이 됨으로써 하나의 정보통신기반구조의 붕괴, 마비 혹은 피해는 다른 정보통신기반구조에까지 지대한 영향을 끼치게 되며 심지어는 국가안보에 까지 지대한 영향을 미치게 된다.

본 논문에서는 국가 정보통신기반구조와 관련한 정보전(Information Warfare)에 대한 개념을 정립하고 정보전에 대응하기 위한 국외 사례를 분석하여 다양한 보호대책을 제시하여 국내 정보통신기반구조 보호대책 수립에 도움을 주고자 한다.

I. 서 론

최근 우리나라를 비롯한 미국, 캐나다, 유럽 등의 선진국은 국가 정보통신기반구조(NII, National Information Infrastructure) 구축을 위하여 초고속정보통신망을 확충하는 등 고도의 정보화 사회 진입을 위하여 노력하고 있다. 정보통신기반구조란 "정보통신기술을 활용하여 정보유통 및 처리에 활용되는 관련 설비를 관리·통제하기 위한 정보시스템 및 정보통신망"을 의미한다. 이러한 국가 정보통신기반구조는 국방과 같은 전통적인 군사적 목적이외에 정보통신시스템, 전력 및 가스 등과 같은 에너지시스템, 금융 및 재정시스템, 영공관리시스템을 포함하는 교통시스템, 급수체계 등과 같이 핵심적인 응용분야에까지 매우 다양하게 적용되고 있다. 지금까지의 전통적인 정보보호체계는 국방, 외교 등과 같은 특수한 분야에서의 보안에 초점을 두고 이에 대한 위협분석 및 대책마련에 많은 연구 및 개발을 수행하여 왔다. 그러나, 국가 정보통신기반구조가 정보통신, 에너지, 재정시스템 등 사회 전 분야에 걸쳐 확대됨으로써 정보보호의 관점은 변화하게 되었다. 즉, 국방 및 외교안보분야에서 사용되는 비밀로 분류되는 데이터에 대한 정보보호와 더불어 정보통신 및 재정시스템 등에서 사용되는 비밀로 분류되지는 않았지만 중요한 데이터(SBU, Sensitive But Unclassified)를 취급하는 분야에 대한 정보보호의 중요성도 비밀 데이터 보안에 못지 않게 증가되었다[1]. SBU 데이터를 처리하는 정보통신기반구조는 비밀 데이터를 처리하는 국방 등과 같은 정보통신기반구조보다 개방적 환경(Open Computing Environment)이며 상대적으로 접근하기가 용이하므로 해커의 주요 활동대상이 되었다. 또한 정보기술(IT, Information Technology)이 발전함에 따라 비밀 데이터 처리에도 상용제품이 많이 사용됨으로써 상용 정보보호 기술에 대한 많은 지식을 축적하고 있는 해커의 활동영역도 동시에 확대되었다. 또한 다양한 정보통신기반구조가 인터넷 등을 이용하여 상호 접속이 됨으로써 하나의 정보통신기반구조의 붕괴, 마비 혹은 피해는 다른 정보통신기반구조에까지 지대한 영향을 끼치게 되었다. 따라서, 이

*한국정보보호센터 ({leecw, bklee, kimhj, hgkim}@kisa.or.kr)

러한 기반구조들을 물리적 혹은 전자적인 공격으로부터 보호하여 사용자에게 가용성(Availability)을 보장한다는 것은 매우 어려운 일로서 이와 같은 불법적인 공격사례는 재정적으로 막대한 피해를 초래하며 심지어는 국가안보에까지 지대한 영향을 미치게 된다 [2].

최근 국내에서도 공공기관 비밀번호 파일의 불법 유출, 홈뱅킹 및 폰뱅킹 사고, 국제적 해킹 사고 등 국가 또는 개인 정보 누출 등과 같은 정보화 역기능 현상이 국가사회 전반에 걸쳐서 심각한 문제로 대두되고 있다. 이러한 정보화 역기능 현상은 전통적으로 분류된 컴퓨터 및 네트워크에 대한 위협에 새로운 형태의 위협이 가미된 형태로 나타나게 되었다. 컴퓨터 바이러스, 웜(Worms), 트로이 목마(Trojan Horses), 논리폭탄(Logic Bombs), 트랩도어(Trap Doors), 하드웨어 칩(Chip)에 이상기능(Malfunction)을 첨가하는 행위, 컴퓨터 하드웨어의 고장을 야기시키는 소위 나노머신(Nano Machine)으로 분류되는 초소형의 로봇, 전파방해 및 전자적 목표물의 기능을 마비시키는 고출력의 무선주파수 총(High Energy Radio Frequency Gun) 등 우리의 상상을 초월하는 새로운 형태의 위협들이 기술의 진화에 발맞추어 등장하고 있다 [2].

미국, 유럽 등의 선진 각국들은 자국의 국가 정보통신기반구조 구축과정에서 급증하고 있는 각종 해킹으로부터 정보를 안전하게 보호하기 위한 범정부 차원의 여러 가지 정책 및 정보보호 기술의 연구 개발을 통하여 보다 효율적인 정보 체계를 구축하고 있는 중이다.

본 논문에서는 국가 정보통신기반구조에 막대한 피해를 끼치는 정보전의 위협으로부터 국가 중요 정보통신기반구조를 보호하기 위한 국외 사례를 분석하고 다양한 보호대책을 제시하여 국내 정보통신기반구조 보호대책 수립에 도움을 주고자 한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 정보통신기반구조에 대한 새로운 형태의 위협인 정보전에 대하여 기술하였고 제 3장에서는 미국에서 추진하고 있는 정보통신기반구조 보호대책에 대하여 기술하였다. 제 4장에서는 정보통신기반구조 보호를 위한 미 대통령 위원회의 R&D 권고 및 국방 정보통신기반 보호를 위한 미국의 대표적 기술개발 체계인 MISSI(Multilevel Information System Security Initiative) 프로젝트를 고찰하고 결론 및 향후 연구방향을 제 5장에서 기술하였다.

II. 정보전(Information Warfare)

산업사회를 거쳐 고도의 정보화 사회로 진입하면서 자동화되고 컴퓨터화된 각종 통신수단 및 각국마다 경쟁적으로 구축하고 있는 국가 정보통신기반구조 즉, 군사적 목적을 위한 국방정보통신기반구조를 비롯하여 전력시스템, 가스/유류의 저장 및 수송 시스템, 금융 및 재정 시스템, 급수시스템, 긴급구호시스템 등이 새로운 위협에 노출되기 시작하였다. 즉, 종래의 물리적인 무기체계를 이용한 전쟁이란 위협으로부터 해킹, 사이버테러를 포함하는 정보전이란 위협으로 위협의 개념이 변화되었다. 정보전은 일반적으로 저렴한 개발비용, 실행의 용이성, 실행시 미치는 거대한 파급효과 등과 같은 속성을 지니고 있으며 잠재적인 공격자들에게 익명이란 장막을 제공해 준다. 따라서, 정보전에 대한 위협은 21세기 정보통신 고도화사회에서 반드시 극복하여야 하는 과제이다.

본 장에서는 21세기 정보화시대에 나타날 수 있는 위협의 형태, 정보전의 개념 및 종류에 대하여 논의하고자 한다.

1. 새로운 위협

21세기 정보화 사회의 진입에 따라 기존의 위협형태와는 다르게 첨단기법을 이용한 새로운 형태의 위협이 나타나고 있다. 이러한 새로운 위협에는 다음과 같은 것이 있다 [3].

- 컴퓨터 바이러스

컴퓨터 바이러스는 물론 새로운 형태의 위협은 아니다. 다만, 컴퓨터 바이러스에 의한 피해 정도가 더욱 막대할 것으로 예상되기 때문에 컴퓨터 바이러스를 새로운 형태의 위협으로 분류하였다. 이 바이러스는 크기가 아주 작고 다양한 기능을 가지고 있으며 강력한 전염성을 가지고 감염 대상물에 치명적인 영향(데이터, 프로그램, 운영체제의 손상)을 끼칠 수 있다.

- Chipping

소프트웨어에 원하지 않는 기능을 삽입시킬 수 있는 것과 마찬가지로 하드웨어내에도 원하지 않는 기능을 삽입시킬 수 있다. 오늘날의 반도체 칩은 수백만개의 집적회로를 포함하고 있으며 반도체 칩을 제조할 시 칩 내부에 이상기능을 의도적으로 삽입할 수 있다. 특정 시간후에 칩의 고장을 야기시키거나 특정 주파수의 신호를 받으면 칩을 손상케하는 등의

표 2. 위협의 변화형태

위협행위	전통적 형태	변화 형태
해킹(Hacking) -Hacker, Cracker -Intruder,Penetrator -Phracker	- 정보유출 - 변조/위조 및 파괴 - 위장 - 비인가 접근 및 사용	- 범죄화 - 지능화 - 글로발화 - 시공간 추적 어려움 증대
바이러스(Virus)	- 불특정 대상 감염 - 피해 확산	- Cruise Virus(Smart Weapon) - 목적지향 감염 및 피해 유발
테러(Terror)	- Hijacking - Bomb 등	- Cyber Terror
전쟁(War)	- 무기(Weapon)	- InfoWar/CyberWar - 무기와 유사기능 보유 Software

이상기능이 삽입되어 사용자에게 피해를 줄 수 있다.

• Nano Machine

Nano Machine은 소프트웨어를 대상으로 하는 바이러스와는 달리 하드웨어를 목표로 한다. Nano Machine은 개미보다 작은 로봇으로서 목표하는 곳의 정보시스템 센터에 배포되어 목표로 하는 컴퓨터를 찾아 컴퓨터 내부에 침투하여 전자회로기판을 작동 불능케 함으로써 컴퓨터를 불능상태에 이르게 한다.

• Microbes

Microbes는 컴퓨터 주요 구성 부품인 실리콘을 파괴할 수 있으며, 컴퓨터가 많은 곳에 살포되어 집적회로를 파괴시켜 컴퓨터에 막대한 피해를 끼친다.

• High Energy Radio Frequency Gun

고출력의 무선 주파수를 전자적 목표물에 발사하여 그 기능을 마비시킬 수 있다. 이로 인한 피해는 보통의 정도(예, 시스템의 작동을 중지시키나 재시동은 가능)에서 막대한 피해(예, 시스템 하드웨어를 물리적으로 파괴)에 이르기까지 피해 형태가 다양하게 나타난다.

• Electro-Magnetic Pulse Bombs

EMP Bomb는 특수 임무를 가지고 적진에 잠입한 팀이 전자적인 장치를 파괴하는 데 사용한다. EMP Bomb는 상당히 넓은 면적내의 모든 컴퓨터 및 통신시스템을 파괴한다. EMP Bomb는 전형적으로 단일의 목표물이 아닌 Bomb 주변의 모든 장비에 타격을 주는데 사용한다.

• 전파방해(Electronic Jamming)

정보전에서 전파방해는 통신 트래픽을 막는데 사용하는 것이 아니라 잘못된 정보를 전달하여 상대방에게 타격을 주는 형태로 사용된다.

위에서 열거한 것과 같은 정보화시대에 악영향을 미칠 수 있는 위협형태의 변화 양상은 표 1과 같다.

2. 정보전의 개념

정보전이란 자신의 모든 중요 정보자원 및 정보시스템에 대해서는 적들로부터 보호하는 반면 적의 중요 정보자원 및 시스템에서의 우위를 차지하기 위해 취하는 행동으로 정보전은 정보의 파괴, 정보흐름의 변경, 정보의 내용에 대한 신뢰성 감소, 서비스 부인공격 등이 포함된다. 정보전 전문가 Winn Schwartau는 다음과 같이 정보전을 정의하였다.

"정보전은 산업계, 정치적 영향권, 국제 경제, 심지어는 모든 국가들에 대하여 수행된다. 정보전은 상대방의 위협에 대응하여 자신의 정보자산을 보호하기 위한 기술이며 자신의 국가 정보통신기반구조에 대한 비밀을 보장함과 동시에 상대방의 비밀을 절취하는 기술이다. 정보전은 정보를 소유하고 있는 자로부터 정보를 얻어내는 기술이며 상대방의 기술과 정보를 사용하지 못하도록 하는 것이다."

최근 들어 정보전은 국가 안보 및 국가 경제 보호 차원에서 새롭고 흥미있는 분야로 떠 오르고 있다. 정보화시대의 주된 혼란은 전력시스템, 전자송금시스템, 전화망, 영공관리시스템 같은 민감하지만 비밀로 분류되지 않은 데이터를 공격함으로써 야기되어질 것으로 예상되기 때문이다. 이러한 공격에 대한 결과는 아직 알려지지 않았지만 종래의 핵전쟁과 비교하여 저렴한 가격, 쉬운 접근성, 감시/감지/추적 등의 어려움으로 인하여 정보전의 효과는 적어도 핵전쟁시의 파괴력에 버금갈 것으로 예상된다.

일반적으로 정보전은 다음과 같은 속성을 지닌다[4].

- 익명성 제공으로 인한 공격행위 용이
- 침입하고자 하는 목표시스템이 다수 존재
- 지역적, 공간적 및 정치적인 경계가 존재하지 않음
- 저투자비용에 비해 고도의 기술 획득이 용이
- 정보사용에 대한 요구의 폭발적 증가
- 정보전 공격에 대한 확실한 처벌법(특히 국제법) 부재
- 정보전 공격에 대한 보호대책 미비

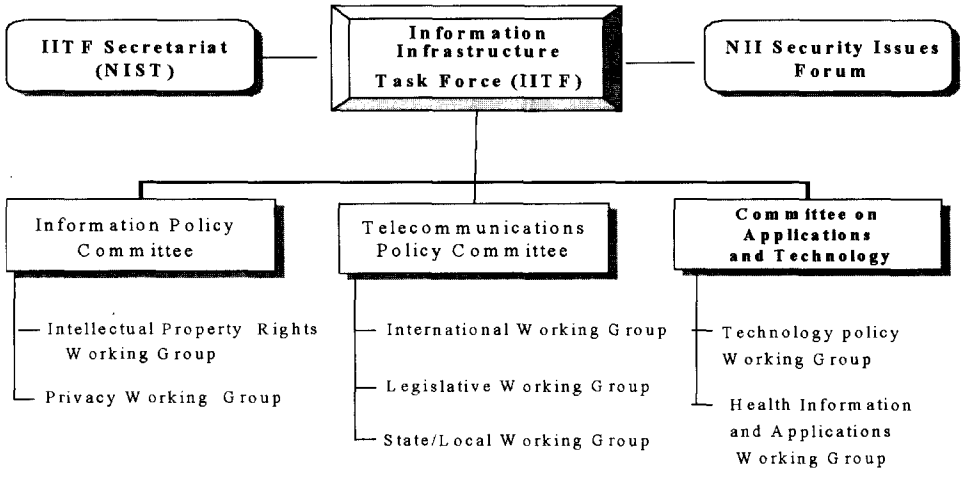


그림 1. IITF의 구성

3. 정보전의 형태

Winn Schwartau는 그의 저서 "Information Warfare"에서 몇가지 방법으로 정보전을 설명하고 있다. 그는 정보전을 다음과 같은 세 개의 부류로 나누어 정의하였다[5].

- Class 1 : 개인적 정보전

정보전의 첫 번째 종류는 개인의 프라이버시 특히 전자적으로 기록된 프라이버시를 침해하려는 시도 및 이에 대한 대응책에 관련된 개인적 정보전이다. 개인적 정보전은 개인의 정보가 저장된 시스템내의 전자기록과 데이터베이스 내용의 누출을 의미한다. 정보화 시대 각 개인의 프라이버시 정보를 불법적인 노출과 변조로부터 보호하고자 하는 것이 바로 Class 1 전쟁 즉, 개인적 정보전이다.

- Class 2 : 조직의 정보전

조직의 정보전은 세계 곳곳의 조직(회사,법인)들 간의 경쟁으로서의 정보전을 의미한다. 한 회사가 경쟁사의 데이터베이스를 침입하고 천오백만달러의 가치가 있는 연구결과를 복사할 수 있도록 해주는 시스템을 개발하는데 백만달러를 투자하는 것은 쉽게 상상할 수 있다. 경쟁사가 새로운 상품과 함께 시장을 선점하지 못하게 하기 위해서, 가동중인 진짜 데이터베이스를 파괴하고 메인프레임상에서의 바이러스로 인한 우연한 사고처럼 보이게 만들 수 있다.

Class 2 정보전은 정보의 취득에 대한 것 뿐만 아니라, 진짜 또는 가짜 정보를 유포하는 것도 가능하다.

- Class 3 : 광역적 정보전

이 정보전의 형태는 산업계와 국제 경제력 혹은 전체 국가에 대응하여 수행되어 진다. 경쟁자의 연구 자료를 절취하는 것이 아니라 비밀자료를 절취하여 이 정보를 정보의 원 소유자에 대응하기 위한 정보로 만드는 것이다. 광역적 정보전이란 국가의사결정시스템, 핵 또는 중요 군사시설 관리시스템, 은행망 등 경제 및 군사활동에 필수적인 네트워크를 파괴하여 적국의 군사적, 경제적 대응 능력을 마비시키는 정보전쟁을 의미한다.

III. 국외 정보전 대응체계

1. 미국의 정보전 대응체계

1993년 9월 15일, 미국에서는 "The National Information Infrastructure : Agenda for Action"을 발표하여 정보고속도로(Information Superhighway)로 불리는 국가 정보통신기반구조(National Information Infrastructure, NII)의 개발을 선언하였다 [6]. 이는 독립적으로 존재하던 기반구조들의 통합을 통하여 각종 서비스와 정보에 대한 접근 지원을 추구하고자 하는 것이다.

이에 따라, IITF(Information Infrastructure Task Force)를 설립하였고, IITF에서는 NII의 개발 비전 제시와 구현체계 확립을 위한 임무를 수행하게 되었다 [7]. 그림 1에서 보여지는 것과 같이 IITF는 정보정책위원회(Information Policy Committee), 통신정책위원회(Telecommunication Policy Committee), 응용 및 기술 위원회(Committee on Application and Technology)로 구성되어 있으며, 통신정책위원회 산하의 신뢰성 및 취약성 작업반(Reliability and Vulnerability Working Group, RVWG)에서는 NII의 보안 특성을 정의하는 과정에서 위협, 취약성, 신뢰성 등을 평가하여 이에 대한 보고서를 발표하였다 [8].

IITF의 세 위원회 및 그 산하의 작업반의 보안관련 활동을 조정하기 위해 NII Security Issues Forum이 설립되었으며 NII Security Forum은 IITF산하 위원회 및 위원회 산하 Working Group 의 보안관련 활동 조정을 주목적으로 하며 이후 Security Issues Forum에서 중요정보기반구조 보호대책의 필요성이 제시되었다. 이를 기반으로 1996년 7월 15일 대통령 행정명령(Executive Order) 13010을 공표함으로서 대통령 산하에 중요 정보통신기반구조 보호위원회(PCCIP, President's Commission on Critical Infrastructure Protection)를 설립하였으며 이후 Security Issues Forum의 임무를 PCCIP에서 수행하게 되었다 [9].

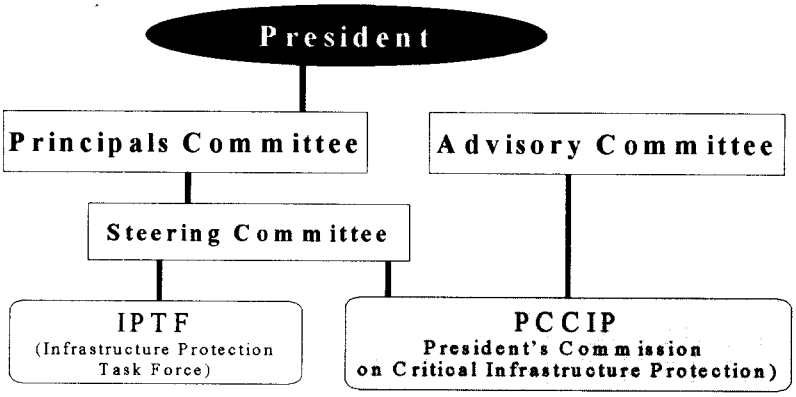


그림 2. 미국의 기반구조 보호 체계도

PCCIP는 중요 정보통신기반구조를 보호하고 위원회의 지속적인 업무 수행을 보장하기 위한 포괄적인 검토를 수행하고 국가 정책을 마련하기 위해서 구성되었다.

그림 2는 대통령령 13010에서 제시하는 미국의 정보통신기반구조 보호 체계도이다. Principal Committee는 정부부처 관리, 기관장 및 백악관 참모로 구성되며 대통령에게 보고될 보고서 등을 검토하여 대통령에게 보고하는 역할을 수행한다 [10].

Steering Committee는 위원장과 4명의 최고급 정부 인사로 구성되며, Principal Committee를 대신하여 PCCIP 및 IPTF의 업무를 감독하는 역할을 한다. 자문위원회(Advisory Committee)는 대통령에 의해 지명된 산업계 대표자로 구성되며 PCCIP에 정보통신기반구조 소유자 및 운영자의 기술적 조언과 전망을 제공한다. IPTF는 연방수사국(FBI), 국방부, 국가보안국(NSA)을 비롯한 다른 부처 및 기관들의 일부 인사로 구성되며 정보전 등과 같은 위협으로부터 중요 정보통신기반구조를 보호하고 지속적인 운영을 보장하기 위하여 정부 및 민간 분야의 노력을 식별하고 조정하는 역할을 수행한다.

1997년 10월, PCCIP는 중요 정보통신기반구조 보호 대책 마련을 위하여 PCCIP 보고서 "Critical Foundations"를 발간하였다 [11]. 이 보고서에서 PCCIP 위원회는 미국의 정보통신기반구조들이 직

면한 취약성과 이에 대한 위협을 검토, 평가하고 수많은 전문가와의 자문을 거쳐 향후 수십 년간 국가의 핵심적 근간이 되는 정보통신기반구조 보호에 대한 최선책을 찾기 위한 목표를 기술하였다. 위원회는 각 정보통신기반구조의 기능에 있어서 장애가 발생할 경우 국가 보안 또는 국가 경제에 영향을 미치는 정보통신기반구조를 정보통신, 전력, 가스 및 유류 저장, 전송, 금융, 운송, 상수도, 응급서비스 및 정부서비스의 8개로 정의하고 에너지, 금융, 정보통신, 물리적 분배, 인간필수서비스의 다섯 분야에서의 정보통신기반구조 특성 및 취약성을 연구하였다.

위원회에서 제시한 다섯 가지 정보통신기반구조의 특성 및 분석된 취약성은 다음과 같다.

- 정보통신 분야
  - 중요 정보통신기반구조가 정보통신기술에 의하여 상호 접속되고 의존함에 따라 다양한 취약성 및 공격기회 증가
  - 대표적 사례 : Y2K 문제
- 금융 분야
  - 취약성의 대부분을 물리적 보안 영역으로 분류
  - 백업의 중요성 강조
  - 정보통신 및 전력 기반구조와의 연계에 따른 취약성 강조
- 전력, 기름, 가스를 포함한 에너지 분야
  - 에너지 공급 혼란에 따른 타 기반구조의 영향 강조
  - SCADA(Supervisory Control And Data Acquisition)의 사이버 위협에 대한 위험 강조
- 물리적 분배(Physical distribution)
  - 교통문제 해결을 위하여 정보통신망 의존도가 심화됨에 따른 취약성 발생 지적
  - 물리적 분배를 위한 정보통신기반구조에 대한 위협증가에 따른 국가영공시스템(NAS, National Airspace System) 및 GPS(Global Positioning System)의 심각한 영향 지적
- 필수인간서비스(Vital human services)
  - 개인정보를 유지하는 대규모 DB의 취약성 경고
  - 급수시설의 유통제어나 수압조절시스템의 취약성 경고
  - 911 시스템의 취약성 지적

PCCIP 위원회는 국가 중요 정보통신기반구조를 보호하기 위한 구현전략을 다음과 같이 제시하였다.

- 목표 1 : 협력 체제 수립(Establishing)
  정부와 정보통신기반구조 사용자와 운영자간의 협력을 증진시켜서 정보통신기반구조 위협, 취약성, 상호 의존도와 관련된 정보의 공유를 증대시켜 나간다.
- 목표 2 : 협력 체제 확립(Building)
  정보통신기반구조 소유자 및 운영자, 그리고 주와 지역 정부가 그들의 정보통신기반구조 보호 역할을 수행하기 위해 충분히 알고 지원되도록 보장한다.
- 목표 3 : 협력 체제 구축
  연방 정부, 주 정부, 그리고 정보통신기반구조 소유자 및 운영자간의 효과적 협력 체제를 용이하게 하여 국가 정보통신기반구조 안전 보장 정책, 계획 및 프로그램을 수행하게 하는 국가 구조를 설립한다.
- 목표 4 : 인식과 교육
  교육 및 다른 적절한 프로그램을 통하여 정보통신기반구조 위협, 취약성, 상호의존성 보장 문제에서 국가적 인식을 향상시킨다.
- 목표 5 : 예시(Example)를 통한 선도
  정부 지도력을 보여주는 일련의 정보보호 관리 지침과 관련 프로그램을 제안한다.
- 목표 6 : 법적 주도권(Legal initiative)
  연방 정보통신기반구조 안전성 보장 및 보호 노력을 증대시키는 법령을 후원한다.
- 목표 7 : 연구개발
  정보통신기반구조의 안전성을 보장하기 위하여 2004년까지 10억 달러를 투자하고 1999년에 2억 5천만 달러에서 5억 달러로 연구개발비를 증가시켜 투자한다.

이와 같은 PCCIP 위원회의 연구결과에 고무된 미 정부는 1998년 5월 테러리스트와 새로운 형태의 사이버 공격에 대한 전쟁을 선포하면서, 고의적인 파괴 행위로부터 국가 중요 기반구조를 보호하기 위한 대통령 지시 PDD(Presidential Decision Directives)62, 63을 발표하였다. PDD 62/63은 미국의 핵심 정보통신기반구조에 대한 물리적 및 사이버 공격 취약성의 신속한 제거를 취지로 발표되었다. 이 지시사항의 목표는 미국이 2000년 이전에 정보전 관련 초기 대응 능력을 갖추고, 5년 이내에 국가의 중요 정보통신기반구조들을 고의적인 행위로부터 보호할 수 있는 능력을 향상시키는 것이다.

PDD63에서는 중요 정보통신기반구조를 보호하기 위한 국가적 노력에 관한 요구로서, 위험을 평가

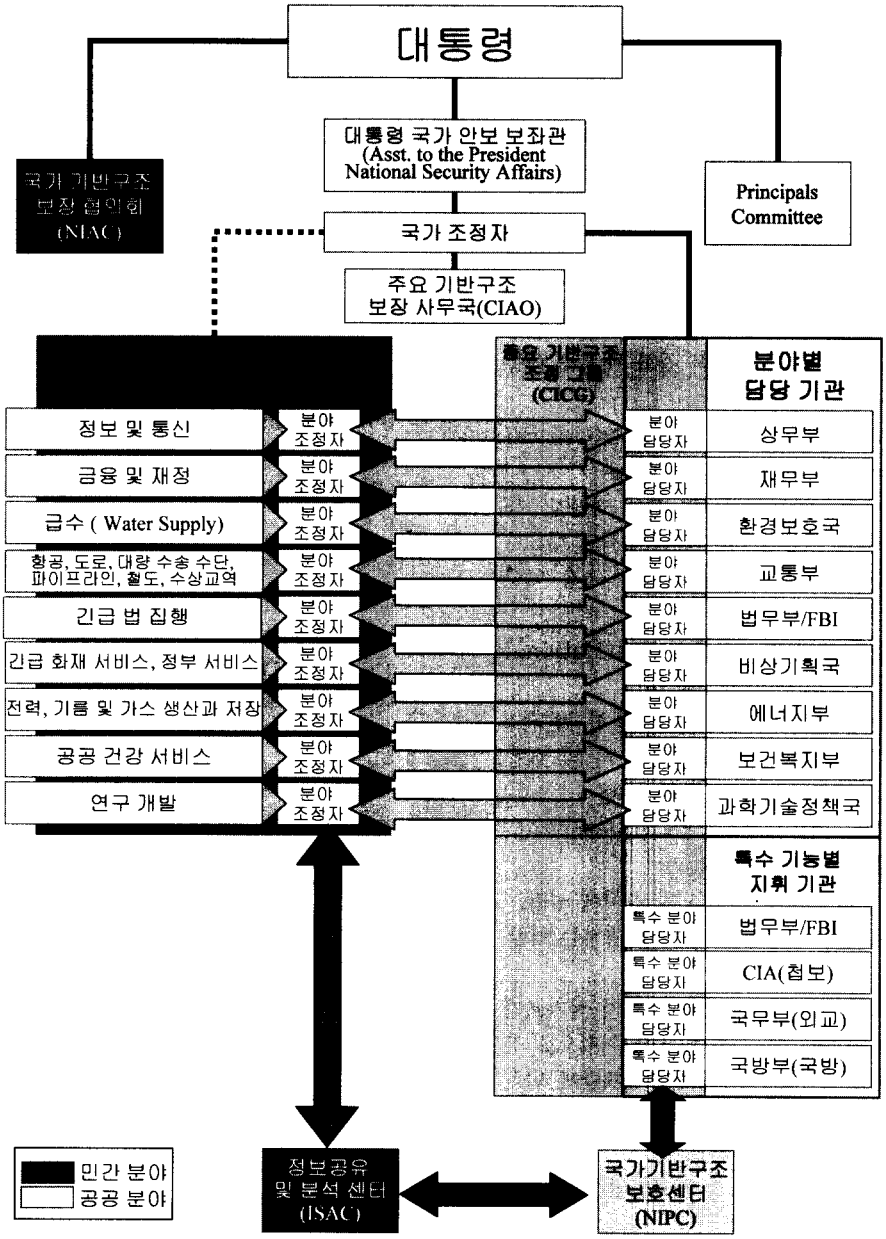


그림 3. PDD63에서 제시한 국가 구조

하고 공격에 대한 노출을 감소시키기 위한 연방 정부의 대책 수립이 지시되었다. 또한, 이 지시 사항에서는 민간 분야 대표자들과 정부 특수 기관들의 연결책을 마련하여 정부와 민간 분야가 서로 협력할 것이 강조되었다.

PDD63에 따라 PCCIP는 중요 기반구조 보장 사무국(CIAO : Critical Infrastructure Assurance Office)으로 개편되었으며 PDD63에서 제시한 정보통신기반구조를 보호하기 위한 주요 국가구조는 다음과 같다(그림 3 참조) [11].

- 국가 조정자(National Coordinator)
  - PDD의 구현을 조정하며 신설된 CICG (Critical Infrastructure Coordination Group)의 의장으로서 국가 기반구조 보장 계획의 개발을 감독하는 역할 수행
- 중요 정보통신기반구조 보장국(CIAO)

- 국가 조정자 지원
- 다양한 분야 계획들을 국가 정보통신기반구조 안전성 보장 계획으로 통합
- 국가 교육 및 인식 프로그램, 입법적 업무 및 공무를 조정

● 국가 정보통신기반구조 보장협의회(National Infrastructure Assurance Council)
- 중요 정보통신기반구조 제공자, 주 및 지역 정부 관리로 구성
- 정기적으로 소집되어 중요 정보통신기반구조 보호에 관한 정부와 민간의 협력 강화 대책을 대통령에게 자문해주는 역할 수행

● 중요 정보통신기반구조 조정그룹(Critical Infrastructure Coordination Group)
- 정보통신기반구조 담당기관의 분야 담당자, 특수분야 담당자를 포함한 기타 관련 부처의 대표자로 구성되어 PDD 63 구현과정에서 조정 역할 수행

● 국가 정보기반구조 보호 센터(National Infrastructure Protection Center)
- FBI에 설립하였으며, 중요 정보통신기반구조 위협 평가, 경고, 취약성, 법 집행 수사 및 대응체(response entity)로서의 역할 수행

● 정보 공유 및 분석 센터(Information Sharing and Analysis Center)
- 연방 정부와의 협력을 위해 민간 분야에 설립
- 민간 분야 정보를 수집, 분석 및 보급하는 역할

이와 같이 미국에서는 정보전을 21세기 국가보안 및 국가경제를 위협할 수 있는 중요한 위협으로 간주하여 관련 대응체계를 정비하고 기술개발에 박차를 가하고 있는 실정이다. 정보전에 대비한 미국의 기술개발 체계는 4장에서 제시하였다.

이외에도 일본에서는 진보된 정보통신기반구조의 발전을 위하여 정보통신기반구조 프로그램(ICI, Info- Communication Infrastructure)에 착수함으로써 미국의 NII 정책에 대응하고 있으며 일본 정부 차원에서 통상산업성(MITI, Ministry of International Trade & Industry)은 ICI 프로그램을 위해 정보시스템의 보안과 신뢰성 개선 대책 구현을 추진 중에 있다 [12].

IV. 정보전 대비 기술개발 현황

미국의 정보전 대비 기술개발 현황은 두 가지로 분류할 수 있다. 하나는 PCCIP 위원회를 중심으로 한 정보통신기반구조 보호를 위한 R&D 권고이며 다른 하나는 국방 정보통신기반구조를 보호하기 위한 MISSI 프로젝트이다. 본 장에서는 PCCIP 위원회의 R&D 권고안, MISSI 프로젝트의 개괄적인 개요를 기술하여 국내 정보전 관련 기술개발 계획에 도움을 주고자 한다.

1. PCCIP R&D 권고안

PCCIP R&D 권고안의 목표는 중요한 국가 보안, 경제, 그리고/또는 사회적 영향을 야기할 수 있는 8가지의 정보통신기반구조 분야에 대한 위협에 대처하고 취약성을 감소시킬 수 있는 기술 개발에 대한 로드맵을 제공하는 것이다 [13]. 고려된 구체적 기술들은 정보통신기반구조의 보호, 취약성 감소, 침입 탐지 및 경고, 침해시 피해 경감, 사고 관리 지원 및 복구를 촉진하는 기술이다. 이러한 기술은 PCCIP 자체에서 연구한 결과 및 외부 연구결과를 종합하여 정리한 것이다 (그림 4 참조).

PCCIP R&D 권고안에서는 장기간 정부 투자를 요구하는 기초연구를 강조하였으며 이 연구는 민간 분야 내의 기술 개발을 수반해야 한다고 강조하고 있다. 이러한 기술개발에는 프로세스, 시스템, 모델 및 모의실험, 하드웨어, 그리고 소프트웨어를 포함한다. 또한 R&D 권고안에서는 유용하고 쓰기에 편리한 제품 개발과 획득을 보장하기 위하여 정보통신기반구조 소유자 및 운영자간의 강한 연계를 강조하였다. PCCIP R&D 권고안은 다음과 같이 요약될 수 있다.

첫째, 정보 보증(Information Assurance), 모니터링 및 위협 탐지, 취약성 평가 및 시스템 분석, 위험 관리 및 의사결정 지원, 보호 및 피해 경감, 사고 대응 및 복구의 여섯 분야에서 연구 개발을 수행할 것을 권고하였다.

둘째, 정보통신기반구조 보증을 위한 연구에 1999년에는 5억 달러를 투자하고 이 후 5년 동안 투자를 점점 늘려서 2004년에는 10억 달러를 투자한다.

셋째, 국가 정보통신기반구조 보증을 위한 R&D 노력에 대한 촛점을 설정하고 기술개발 및 기술이전을 육성하기 위한 공공/민간 분야 협력을 확립한다.

PCCIP R&D 권고안에서 제시하는 여섯 가지 중점 연구개발 분야의 필요성은 다음과 같다.

● 정보보증 분야 : 침해사고율이 증가하고 알려진

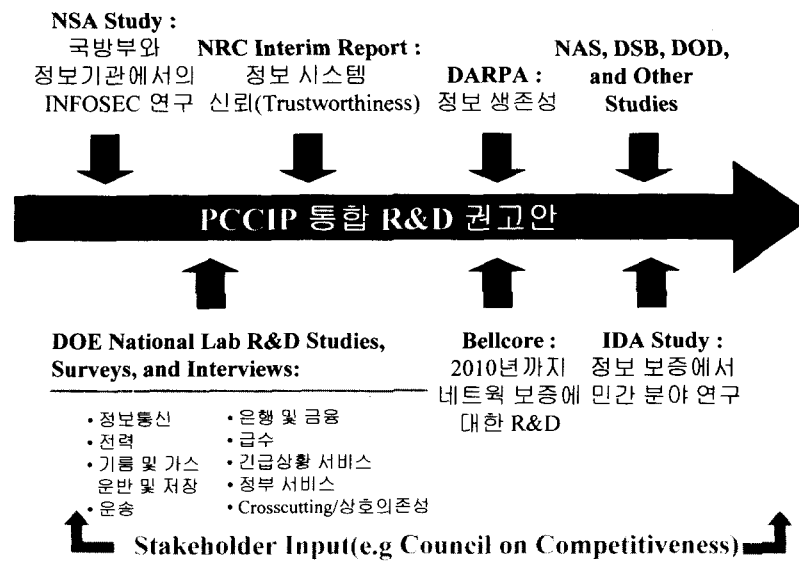


그림 4. PCCIP R&D 권고안의 중요 자료 소스

취약성이 점점 증가하고 활용 가능한 보안제품이 부적절한 현 상황에서 정보통신기반구조를 보호하기에 알맞는 새로운 보호수단을 개발해야 하는 이유는 명백하다. 정보통신기반구조와 이것을 이용하여 생성, 저장, 처리 및 전송되는 정보를 효과적으로 보호하기 위해 R&D 분야에 투자 및 노력이 요구된다. 이러한 분야의 연구개발 시급성은 시스템 통합율 증가와 행동특성을 예측할 수 없는 정보통신기반구조의 복잡도에 의하여 더욱 강조되어야 한다.

● 모니터링 및 위협 탐지 분야 : 신뢰적인 자동 모니터링 및 탐지 시스템, 시기적절하고 효과적인 정보 수집 기술, 그리고 효율적인 데이터 축약 및 분석 도구는 정보통신기반구조에 대한 지역적이거나 다른 공격과 조화된 대규모 공격을 식별하고 특성화하는데 필요하다. 이와 같은 기술은 정부 및 민간분야 정보통신기반구조 소유자 및 운영자에게 초기에 위협을 경고하고, 이에 의해 국가 안보, 경제, 삶의 질에 심각한 결과를 초래할 수 있는 광범위한 정보통신기반구조 붕괴를 예방한다.

● 취약성 평가 및 시스템 분석 : 취약성 평가 및 시스템 분석에 대한 진보된 방법 및 도구는 정보통신기반구조내의 중요 노드를 식별하고 정보통신기반구조 상호의존도를 조사하며 복잡한 시스템의 행동(behavior) 특성을 이해하기 위해 필요하다. 이러한 방법 및 도구는 물리적 및 사이버 보안같은 문제를 해결하기 위하여 보통 통합된 형태로 제공된다. 정보통신기반구조 관련 문제를 연구하기 위한 모델링과 시뮬레이션 도구 및 테스트베드(test bed)는 상당한 규모를 가진 실제 환경에서 수행될 수 없는 실험을 위해 중요하다. 뿐만 아니라 방법론 및 도구를 검증하고 타당화시킬 수 있는 기술도 필요하다

● 위험 관리 및 의사결정 지원 : 위험 관리 및 의사결정 지원 시스템 방법론과 도구는 정부와 민간분야 의사결정자가 위험을 감소시키기 위하여, 한정된 자원의 이용을 효과적으로 우선 순위를 정하는데 필요하다. 이러한 방법론과 도구는 자연재해, 물리적 공격과 같은 친숙한 위협과 사이버 시스템에 대한 신뢰와 상호의존성 증가로부터 야기되는 새로운 위협 및 미래의 위협 양자에 대한 위험을 다룬다.

● 보호 및 피해경감 : 실시간 시스템 제어, 정보통신기반구조 경화(hardening), 봉쇄 및 격리 기술은 전체 위협 스펙트럼에 대하여 정보통신기반구조 시스템을 보호하는데 필요하다. 다른 진보된 생존성, 신뢰성, 또는 보증 강화 수단이 연구되고 개발되어야 한다.

● 사고 대응 및 복구 : 지역적이거나 국가적인 정보통신기반구조에 영향을 미치는 자연재해, 물리적 및 사이버 공격과 같은 사고에 대해 효과적으로 계획하고 대응하며 복구하기 위하여 침해사고 대응 및

표 2 구체적 R&D 영역 및 주제

R&D 영역	R&D 주제
정보 보증	· 시스템 수준 보안 · 정보 보호에 대한 진보된 개념 및 이론 · 정보보호 관리 · 암호 기술
모니터링 및 위협 탐지	· 자동 모니터링 및 탐지 · 기반구조 정보 시스템
취약성 평가 및 시스템 분석	· 취약성 평가 툴 · 복잡한 시스템 모델링 · 테스트베드 · 검증 기술
위험 관리 및 의사결정 지원	· 위험 관리 · 의사결정 지원 시스템
보호 및 경감	· 실시간 분산 시스템 통제 · 기반구조 경화(Hardening) · 봉쇄 및 격리
사고 대응 및 복구	· 대응 기술 · 복구 기술

복구와 관련된 광범위한 새로운 기술 및 도구가 필요하다.

PCCIP 위원회에서 제시하는 각 분야별 구체적 R&D 주제는 표 2와 같다.

2. 미 국방부의 MISSI 프로젝트

국가 정보통신기반구조 중에서 국가안보와 직접적으로 관련이 되는 국방 정보통신기반구조에 대한 미국의 대표적 보안대책으로는 MISSI를 들 수 있다. MISSI는 MISSI를 구성하고 있는 제품과 공통의 보안관리 기반으로 구성된 통합적이고 응집력 있는 구조를 통하여, 국방 정보통신기반구조 구성요소를 위한 혁신적이고, 상호 운용성이 있는 보안 해결책을 제공한다. MISSI에서 제공하는 보안서비스로는 무결성, 신분확인, 부인봉쇄, 비밀성 및 가용성 등이 있으며 이와 같은 보안 서비스를 만족하기 위하여 다음의 그림 5에서와 같이 체계적이며 종합적인 보안 해결책을 제시하고 있다 [14].

그림 5에서 DMS는 국방메시지시스템(Defense Message System), GCCS는 광역명령통제시스템(Global Command and Control System), GCSS는 전투지원시스템(Global Combat Support System)을 DFAS는 국방부 재정·회계 서비스시스템(Defense Finance and Accounting Service)을 의미한다.

미국은 국방 정보통신기반구조에 대한 정보전 방어 능력을 배양하기 위하여 90년대 초반부터 NIST와 공동으로 추진하던 SDNS(Secure Data Network System) 프로젝트와 연계성을 지닌 MISSI 프로젝트를 NSA(National Security Agency), 정보보호산업체 등과 공동으로 추진하고 있다. 미 국방부는 MISSI 프로젝트를 통하여 전자메시지(Electronic messaging), 월드 와이드 웹, 접근통제 및 강한 인증, 파일과 미디어 암호기, 원격의 DB 액세스(Remote DataBase Access), 전자상거래/전자문서교환(EC/EDI) 및 국방부 메시지시스템 등 국방 정보통신기반구조 상에서 사용되는 다양한 응용에 나타날 수 있는 정보전 위협에 대비하고 있다.

V. 결 론

미국, 일본, 유럽 등 세계의 여러 국가에서는 국가정보기반구축을 위한 초고속정보통신망을 확충하는 등 고도의 정보화 사회 진입을 위하여 노력하고 있다. 그러나, 보안 기술보다 항상 앞서가는 정보기술로 인하여 국가의 중요 정보통신기반구조는 많은 취약성을 내포하게 되었으며 악의적 사용자 또는 집단에 의해 심각하게 위협받고 있는 실정이다. 정보통신기반구조의 붕괴는 국가적, 사회적, 경제적 기능 마비를 의미하므로, 각 나라마다 이를 예방, 완화, 복구하는데 많은 노력을 기울이고 있으며 다양한 대응책을 제시하고 있다. 이러한 국가 정보통

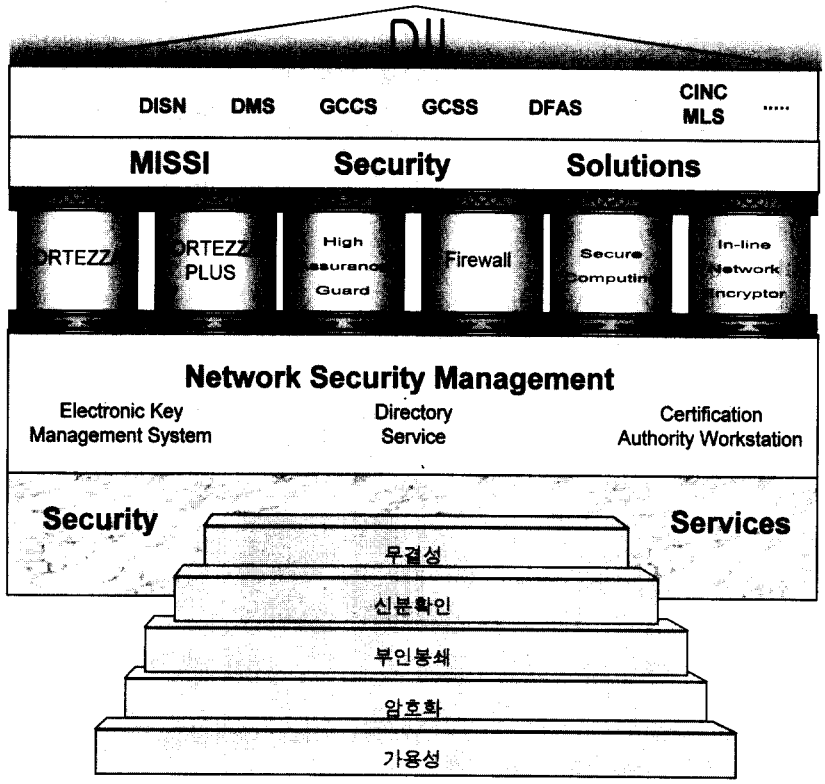


그림 5. MISSI의 보안구조

신기반구조는 국방과 같은 전통적인 군사적 목적이외에 정보통신시스템, 전력시스템, 금융 및 재정시스템, 교통시스템, 급수체계 등과 같이 핵심적인 응용분야에까지 매우 다양하게 적용되고 있다.

본 논문에서는 21세기 정보화시대에서 새롭게 도입되는 정보전의 위협을 고찰하고 21세기 정보전 관련 종합 대응대책을 효과적으로 도입 확산시키기 위하여 정보통신기반구조 보호에 있어서 국제적 주도권을 가지고 있는 미국의 정보전 대응 방안을 분석하였다.

미국은 1993년 NII 구축을 선언한 이래로 NII의 위험을 평가하고 중요 정보통신기반구조에 대한 위협 및 취약성을 분석하는데 많은 정부 예산을 투자해 왔으며 중요 정보통신기반구조 보호를 위하여 정부 및 민간 분야간의 협력이 구축되고 책임을 공유해야 한다고 주장하였다. 또한 정보통신기반구조에 대한 취약성 정보를 공유하고 법·제도적인 대책을 포함하는 국가적 대응 체제를 구축을 제안하였다. 또한 정보통신기반구조 보호를 위한 대통령 위원회를 중심으로 장기적인 R&D 개발계획을 작성하여 이를 실천하고 있다.

현재 우리나라는 국외의 정보통신기반구조 보호 대책을 검토하고 있으나 아직까지는 초보적 수준에 불과하다. 국가 중요 정보통신기반구조를 보호하여 국가적 보안체계 확립 및 튼튼한 자립경제기반을 구축하기 위해서는 정보통신기반구조 보호에 필요한 기술개발, 관련 법·제도 정비, 과감한 투자, 인력양성 및 관련 산업육성에 정진하여야 할 것으로 사료된다.

참고문헌

[1] Defense Science Board, Report of the Defense Science Board Task Force on Information Wafare - Defense, 1996.

[2] http://www.ndu.edu/ndu/inss/books/diw/intro.html, Defensive Information Warfare, National Defense University, Aug., 1996.

[3] Department of National Defense,

Information Warfare and the Canadian Forces, Document No. 1350-004-D001 Ver.1, 1996.
[4] Matthew G. Devost, "National Security in the Information Age", MS Thesis of The University of Vermont, 1995.
[5] Winn Schwartau, Information Warfare : Chaos on the Electronic Superhighway: Thunder's Mouth Press, 1994.
[6] http://sunsite.unc.edu/nii/NII-Agenda-for-Action.html
[7] http://www.iitf.nist.gov/about.html
[8] http://www.ncs.gov/n5_hp/N5_IA_HP/HTML/RVWG.HTM
[9] http://www.pccip.gov/eo13010.html
[10] http://www.pccip.gov/organization.html, The Steering Committee.
[11] http://www.pccip.gov/report_index.html, Critical Foundations.
[12] http://www.miti.go.jp/report-e/g316001e.html
[13] Research and Development Recommendations for Protecting and Assuring Critical National Infrastructures, Report of PCCIP, 1997.
[14] 이철원외 4인, "국가전산망을 위한 MISSI 분석", 통신정보보호학회지 제7권 제2호, 1997. 6.

이 철 원(Cheol Won Lee)

1987.2 : 충남대학교 수학과(학사)
1989.8 : 중앙대학교 대학원 전산학과(석사)
1989.9 ~ 1996.6 : 한국전자통신연구소 선임연구원
1996.6 ~ 현재 : 한국정보보호센터 선임연구원

<관심분야> 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호기술표준화

이 병 각(Byung Kak Lee)

1995.2 : 연세대학교 전산과학과(학사)
1997.8 : 연세대학교 컴퓨터과학과(석사)
1997년 ~ 현재 : 한국정보보호센터 연구원

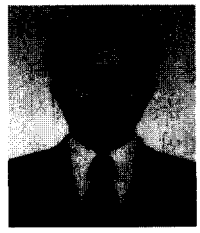
<관심분야> 컴퓨터 · 네트워크 보안, 운영체제 보안

김 현 주(Hyun Ju Kim)

1996.2 : 대구대학교 전산정보학과(학사)
1997.8 : 경북대학교 컴퓨터과학과(석사)
1997년 ~ 현재 : 한국정보보호센터 위촉연구원

<관심분야> 컴퓨터 · 네트워크 보안, 분산 컴퓨팅

김 홍 근(Hong Geun Kim)



1985.2 : 서울대학교 컴퓨터공학과(학사)
1987.2 : 서울대학교 컴퓨터공학과(석사)
1994.2 : 서울대학교 컴퓨터공학과(박사)
1994.5 ~ 1996.5 : 한국전산원 선임연구원
1996.5 ~ 현재 : 한국정보보호센터 시스템기술팀장

<관심분야> 컴퓨터 · 네트워크 보안, 병렬처리