□정보산업동향□

미국의 주요 기반구조 보호동향 분석

이 철 원[†] 박 용[††] 이 홍 섭[†††]

◈ 목 차 ◈

1. 서 론

최근 십여 년 동안, 우리 나라는 커다란 변화를 경험하였다. 사회 전 부분에 걸친 정보 혁명과 컴퓨터 도입은 경제활동, 국가안보 및 사람들의 일상 생활을 크게 변화시켜왔다. 정보화가 추진되어감에 따라 이전과 다른 새로운 산업들이 다양하게 창출되었으며, 국가의 부(富)를 증대시키는 새로운 방안으로 정보산업에 대한 인식이 전환되었다. 컴퓨터관련 기술은 인류에게 창조에 대한 무한한 가능성과 함께 가족 및 지역사회의 안전에 대한 새로운 위협을 가중시키고 있다. 이와 더불어 과거의 인습에서 벗어나 새로운 번영의 시대를 건설할 수 있는 기회를 계속해서 열어줄 것이라고 많은 사람이 믿고 있다. 그러나, 전술하다시피 이 새로운 시대를 열어가는 핵심시스템인 컴퓨터에는 많은 위협이 존재하고 있다. 전화를 하거나, 은행에서 돈을 송금하거나, 비행기를 탈 때에도 하나 이상의 정교한 컴퓨터 시스템이 운영하는 제어시스템에 의존하고 있다. 국가의 안전보장을 위한 국방시스템 또한 컴퓨터에 의해 제어되는 전력, 통신, 운송 등의 기반시설에 깊이 의존하고 있다. 컴퓨터에 의하여 제어되는 이 모든 시스템은 침입과 파괴에 취약하며, 핵심 경제분야와 정부기관일부의 컴퓨터에 이러한 침입이 발생할 경우, 우리는 상상하기 어려운 피해를 입을 것이다.

통신, 금융, 운송, 전력, 정부서비스 등 국가사회를 운영하고 유지하기 위한 핵심시스템에 대한 물리적 및 사이버 위협은 실제로 존재하고 있으며, 향후 국가의 위기상황 또는 타국과의 분쟁 시 종래의 재래식 무기를 이용한 대규모 인명살상보다는 컴퓨터에 의해 통제되는 주요 기반구조를 대상으로 공격이 집중될 것으로 예상된다.

"핵심 기능의 어떠한 중단이나 조작은 단순하고, 드물며, 처리하기 쉽고, 지리적으로 고립되며, 미국의 복지(welfare)에 미비하게 해를 입히는 것이어야 한다"라고 클린턴 대통령이 PDD(Presidential Decision Directive) 63에서 지적한 바와 같이, 미국을 비롯한 호주, 일본, 영국, 캐나다 등에서는 자국의 주요 기반구조를 보호하기 위한 노력을 범 국가적 차원에서 추진하고 있다[1]. PDD 63은 컴퓨터 기반 시스템들의 취약성을 평가하고 내재되어 있는 결함을 개선할 것과 연방정부에게 주요 기반구조를 보호하고 정보전에 대응하여 미국을 방어하기 위한 세부 계획을 만들 것을 요구하였다. 이에 따라, '99년 6월 국가계획 초안이 발

† 정회원 : 한국정보보호센터 통신모델링 과제책임자
†† 정회원 : 한국정보보호센터 인증관리팀 연구원
††† 정회원 : 한국정보보호센터 연구개발부장

표되었으며, 이에 대한 각계의 의견을 수렴하여 2000년 1월 7일 국가계획의 첫 번째 버전을 정식으로 발표하였다. 물론, 미국의 주요기반보호 국가계획의 프라이버시 침해에 대한 우려로 시민단체의 반발도 만만치는 않지만, 주요 기반구조 보호를 위한 범 국가적인 보호골격을 제시하는 등 국가의 주요 기반시설을 해킹·사이버 테러 등의 위협으로부터 보호하기 위한 초석을 마련한 것으로 평가되고 있다. 본 논문은 국내 주요 기반구조 보호골격 구축에 도움을 주고자 2000년 1월 7일 발표된 국가계획을 분석한 것으로, 미국의 연방정부, 주, 지방정부가 국가안보, 공중보건, 안전에 대한 책임을 보장하기 위하여 수행하여야 하는 것에 대한 종합적인 비전 및 주요 기반구조 분야의 붕괴에 대응하기 위해 필요시 되는 보호수단 구축방향에 대하여 분석하였다.

2. 국가계획

국가계획의 목표는 2000년 12월까지 주요기반구조 보호관련 초기 운영 능력을 확보하고 2003년 5월까지 완벽한 운영 능력을 확보하여 주요 정보 시스템에 대한 보호대책을 구축하는 것이다. 이 국가계획은 미국의 주요 기반구조를 보호하기 위한 골격으로써, 10개의 프로그램을 제시하고 있다. 각 프로그램별 세부 항목 및 개발 일정이 제시되어 있으며 총무처(GSA), 상무부(DoC), 법무부(DoJ) 등 각 기반구조에 대한 담당 부처에서는 이 일정에 따라 해당 세부계획을 작성하여야 한다[2][3].

이 계획은 세 개의 광범위한 목적을 위해 제시되었다.

- 준비 및 예방 : 주요 정보 네트워크에 대한 심각한 공격의 성공가능성을 최소화하고, 공격이 가해졌을 때에도 효과적인 기능을 지속할 수 있는 기반구조를 구축하기 위한 단계
- 탐지 및 대응 : 적시에 공격을 확인하고 평가하여 공격을 억제하고, 이러한 공격으로부터 신속히 복구하여 영향을 입은 시스템을 재구성하기 위한 조치
- 튼튼한 기반구축 : 미국의 중요한 정보 네트워크에 대한 공격에 보다 효과적으로 대비하고 예방하며 탐지하고 대응할 수 있게 하는 인력, 기관, 법률 및 전통을 국가가 창출하고 양성하기 위한 활동

국가계획에서는 이러한 목표를 달성하기 위해 다음과 같은 10가지 프로그램을 제안한다.

- 프로그램 1 : 주요 기반구조 자산 및 공유된 상호의존성을 파악하고 취약점을 다룬다.
- 프로그램 2 : 공격 및 침입을 탐지한다.
- 프로그램 3 : 강력한 정보 및 법 집행 능력을 개발하여 법률과 일관되도록 주요 정보 시스템을 보호한다.
- 프로그램 4 : 공격에 대한 경고 및 정보를 시기 적절한 방식으로 공유한다.
- 프로그램 5 : 대응, 재구성 및 복구 능력을 창출한다.
- 프로그램 6 : 프로그램 1-5를 지원하는 연구 및 개발을 촉진한다.
- 프로그램 7 : 적절한 수의 정보 보안 전문가를 훈련시키고 고용한다.
- 프로그램 8 : 사이버 보안의 개선이 필요함을 인식시킨다.
- 프로그램 9 : 프로그램 1-8을 지원하는 법령과 정부 예산을 지원한다.
- 프로그램 10 : 보호책의 모든 단계 및 구성요소에 있어서 미국 시민들의 시민적 자유, 프라이버시 및 사유 데이터 보호권을 충분히 보호할 수 있도록 한다.

이 국가계획에서는, 연방정부(국방 및 비국방 기관)와 민간분야(산업 및 협회)가 함께 협력하여 전술한 3가지 목적을 달성하도록 촉구하고 있으나, 민간분야보다는 정부 내에서 수행되었던 일과 장차 가까운 미래에 수행되어야할 일에 대해 더욱 구체적으로 기술하였다. 현재 발표된 국가계획에서는 민간 소유의 기반구조를 보호하기 위해 산업계와 주 정부 및 지방 정부가 맡게 될 구체적인 역할(개별적인 역할 및 연방 정부와 협력해서 맡게 될 역할), 고의적인 공격으로부터 물리적 기반구조와 사이버 기반구조를 보호해야 할 필요성, 주요 기반구조의 보호에 대한 국제적 동향의 검토 등에 초점을 맞추고 있으며, 국가계획에 대한 산업계, 의회, 주 정부와 지방 정부 및 일반 대중의 의견은 추후의 버전에 반영할 예정이다.

국가계획에서 주목할 만한 점은 국민의 프라이버시 보호 노력이다. 연방 정부는 정보와 시스템의 보호를 위한 기술을 신중하게 이용하지 못하면 원래의 의도와는 반대로 시민적 자유를 손상시킬 수 있다는 사실을 인정하고 있으며, 아무리 의도가 좋더라도 침입을 막는 조치가 너무 광범위하게 시행되면 선량한 활동에 피해를 줄 수 있음을 인식하고, 현존하는 법률 및 헌법이 보장하는 사생활 기대치와 충분히 일치하도록 보호대책을 개발했다[3].

2.1 프로그램 1 : 주요 기반구조 자산, 상호의존성 파악 및 취약성 분석

"프로그램 1은 정부 및 민간 부문이 공격받을 수 있는 주요 정보 네트워크의 취약성, 상호의존성 및 주요 자산을 파악하고, 취약성을 개선할 수 있는 현실적인 프로그램을 개발하고 실행하며, 평가 및 개선 활동을 지속적으로 수행한다."

주요 정보시스템 및 컴퓨터 네트워크의 보호태세를 갖추는데 필요한 초기단계는 잠재적인 취약성을 평가하는 것이다. 정보기관은 잠재적 적군의 능력을 쉽게 식별할 수 없기 때문에, 주요기반구조를 보호하기 위한 능력 평가는 가능한 적군의 힘을 예측하는 것 보다 우리가 가지고 있는 주요 정보시스템 및 컴퓨터 네트워크의 취약성을 평가하는데 좀더 비중을 두어야 한다고 지적하였다.

국가계획에서, 컴퓨터 네트워크의 악용여지가 있는 영역을 파악하는 주요 요소를 다음과 같이 대별하였다[3].

- 가장 중요한 자산의 파악 : 이것은 기관/부처의 업무중 국가 안보와 일상적인 임무 기준을 명백히 구별하는 것을 바탕으로 한다.
- 기관 내부 또는 기관과 민간 부문 사이의 공유된 상호의존성 분석
- 시스템 관리자, 운영자, 보안 전문가 및 정보화담당관(CIO: Chief Information Officer)에 의한 네트워크 취약점 평가 : 이것은 주요 자산 및 공유된 상호의존성의 파악을 바탕으로 한다.
- 완화 노력(mitigation efforts)의 성공을 확인하도록 훈련된 외부 전문가에 의한 평가

국가계획에서는, 정보시스템 보안을 위한 최상의 지침(best practice)과 표준이 취약성을 식별하고 처리하기 위하여 조직에 도움을 줄 수 있다고 판단하고 있으며, 연방정부, 민간분야, 표준단체들 간의 밀접한 협력을 통하여 취약성을 식별하고, 이 식별된 취약성을 제거하기 위한 조치를 우선순위화 하기 위한 지침을 제정할 것을 권고하였다. 또한, 연방정부 스스로도 연방정부 소유 시스템의 정보보안에 대한 최상의 지침 및 표준을 강화하기 위하여 지침(guideline)의 사용확대에 앞장설 것을 권고하고 있다.

모든 취약성은 재정상의 문제로 인하여 즉시 개선되어질 수 없다는 사실을 인식하고, 정부조직과 민간분야단체는 3-5년간에 걸친 개선노력을

우선 순위화 할 것을 요구하고 있다. 또한, 네트워크가 변화함에 따라 새로운 취약성이 소개되고 있으므로, 새로운 취약성과 이에 걸맞는 새로운 보호개념, 그리고 이를 위하여 활용할 수 있는 표준과 최상의 지침을 재검토할 수 있는 꾸준한 절차가 필요함을 주장하였다. 취약성 평가는 적군에게 공격법의 청사진을 제공할 수 있기 때문에, 평가는 반드시 그들 스스로 해야함을 강조하였다.

프로그램 1을 위한 주요 세부 항목은 다음과 같다.

- 연방부처들은 초기 취약점 평가를 수행하고 개선 계획을 개발한다. 전문가 분석팀이 보고서를 분석한다(완료).
- CIO 위원회는 연방 정보 시스템 보안 권고 규정에 대한 관계 부처간의 작업단을 구성하여 지속적인 정부 내의 보안에 관한 권고 규정의 실행상황을 확인하고 조정하며 이를 강화시키는 것에 주안점을 둔다(완료).
- 연방 정부는 주요 정보 자산의 보호 규정을 마련하기 위한 파일럿 구조와 데이터베이스를 범례와 아울러 개발해야 한다(완료).
- 공개키 기반구조를 위한 MISPC ver.2를 간행함으로써 MISPC를 통해 연방 공개키 기반구조(PKI) 사용자와 외부 PKI 구성원이 핵심적인 관리 업무를 다루기 위해 사용하는 인증서와 CRL 프로파일을 개선한다(2000년 2월)
- 연방 정부는 주요 물리적 기반구조 보호책의 첫 번째 버전을 완성한다(진행).
- 연방 정부는 주요 기반구조 자산 및 공유된 상호의존성을 파악하기 위한 방법을 개발한다(진행).
- 연방 부처와 기관들은 컴퓨터 시스템 취약점에 적절한 소프트웨어 패치와 기타 보완물을 적시에 설치할 수 있음을 보증한다(진행).
- 민간 부문의 정보 공유 및 분석 센터(Information Sharing and Analysis Center)는 회원사가 평가 및 개선 프로그램을 수행할 수 있도록 지침을 개발할 수 있다(진행).
- 민간 부문의 정보 공유 및 분석 센터에서는 부문 차원 또는 산업계 차원으로 공유된 취약점을 평가할 수 있다(진행).
- 연방 PKI 및 대중적인 검토를 위해 발행된 인증서 발급을 위한 보안 요구사항과 관리 구성요소를 활용하여 전자 우편과 같은 PKI 응용프로그램의 상호 운영성을 실증한다(진행).
- 모든 전자 우편은 서명되어야 한다. 국방성 전체에서 전자 우편의 암호화를 장려한다(진행).
- 취약성 개선 계획에서는 정부 기관과 핵심 기업의 주요 정보 시스템 네트워크에서 가장 심각하다고 알려진 취약성을 제거해야 한다. 지속적인 취약성 평가와 개선 작업을 수행한다(진행).

2.2 프로그램 2 : 공격 및 침입을 탐지한다.

"프로그램 2는 중요한 컴퓨터 시스템에 진보된 침입차단시스템, 침입탐지 모니터, 비정상행위 식별기, 전사적(enterprise-wide) 관리시스템, 악성코드 스캐너를 포함하는 다단계 보호장치를 설치하는 것이다."

프로그램 2에서는 현재 적용되고 있는 보안대책의 포괄적인 문제점을 다음과 같이 지적하였다. 첫째, 일부 침입차단시스템은 기능적으로 한계가 있거나 주기적으로 기능 향상이 되지 않으며, 침입차단시스템을 우회하는 기술도 존재한다. 둘째, 사용자는 복잡한 패스워드를 사용하지 않거나 패스워드를 주기적으로 변경하지도 않는다. 셋째, 일반적으로 획득 및 활용가능한 소프트웨어 프로그램을 통하여 패스워드를 간파할 수 있다. 넷째,

활 동	목 표 일
공군, 해군, 육군 및 국방부 기관에 침입 탐지 시스템을 연계하는 분석 및 대응 센터를 수립한다. 국가 안보관련침해대응센터(NSIRC)를 수립한다.	완료
주요 국방성 시스템에 초기 500개의 침입 탐지 모니터를 설치한다.	완료
침입 탐지를 위한 국방성 차원의 허브인 JTF-CND를 설립한다.	완료
연방 시스템에 있는 악성 코드의 검색을 시행한다.	FY 2000
연방 기관에 대한 침입 탐지 네트워크(FIDNet)를 시범 설시하고, 2000년 8월까지 22개의 주요 연방 사이트를 연결한다.	FY 2000
연방 시스템에 적절한 경우, 접근/활동 감시장치를 갱신하고 전사적 관리 시스템을 설치한다.	FY 2000
탐지 시스템을 개발하고 정기적으로 갱신한다.	2000년 10월
연방 정부에서 필요한 경우 침입차단시스템과 침입 탐지 모니터를 갱신한다.	2001년 1월

사용자가 순진하게 해커가 배포한 소프트웨어를 사용하거나, 전체 시스템에 트랩도어가 은밀하게 설치될 가능성도 있다. 다섯째, 사용자는 규칙을 위반하고, 집에서 일하기 위하여 비인가된 모뎀을 설치하기도 하며, 이로 인해 네트워크에 다른 사람이 진입하는 것을 의도하지 않더라도 허용하게 될 가능성이 있다. 또한, 일반적으로 사용되는 소프트웨어는 의도적이지 않은 취약성을 가지고 있음을 지적하였으며, 다른 기종의 소프트웨어와 하드웨어의 상호작용은 보안상의 결함을 야기한다고 지적하였다. 이와 같은 결함을 이용한, 네트워크상의 비인가된 침입이나 행위를 탐지하기 위해서 다음의 네 가지 유형의 방어적 탐지 시스템을 포함하는 고(高)자동화 프로그램 개발을 촉구했다.

- 정기적으로 갱신되는 고수준 침입차단시스템이나 침입탐지 모니터
- 인가된 사용자를 위한 접근과 행위규칙 그리고 인가된 사용자에 의한 비정상적인 행위를 식별하는 프로그램
- 네트워크상의 시스템이 무엇인지 식별하고, 시스템이 하는 일을 결정하고, 접근 규칙 및 행동규칙의 시행, 보안 향상(upgrade)을 적용할 수 있는 전사적 (enterprise-wide)차원의 관리 프로그램
- 운영체제 코드를 분석하는 기술 및 악성 코드(트랩도어나 논리 폭탄)가 설치되어 있는지를 판단하는 소프트웨어 기술

국가계획에서는 중요 정보시스템 네트워크상의 적절한 곳에 네 가지 유형의 탐지시스템의 각각에 대하여, "최상의(best of breed)" 프로그램을 설치할 것을 요구한다. 정부 내에서 이러한 프로그램의 설치가 강제될 것이며 정부는 정보공유 및 분석센터(Information Sharing and Analysis Center)를 통해 이러한 시스템의 평가 작업을 공유할 수도 있어야 한다. 프로그램 2를 위한 주요 세부 항목은 다음과 같다[3].

2.3 프로그램 3 : 법률과 일관성을 유지하면서 주요 정보 시스템을 보호하기 위한 강력한 첩보 및 법 집행 능력을 개발한다.

"프로그램 3은 미국의 법 집행과 정보 기관들을 지원하고 변형시키며 강화하여 컴퓨터 네트워크에 대한 새로운 종류의 위협과 범죄자들을 다룰 수 있도록 한다."

과거와 달리 기반구조에 대한 국외로부터의 위협은 쉽게 발견되고 접근될 수 없는 컴퓨터 기반 공격이 포함되고 있으며 미국 정보기관들은 외국의 정보전 능력과 이를 수행하고자 하는 의지에 대한 정보수집에 보다 우선 순위를 두고 있다. 특

활 동	목표일
연방법 집행 및 정보 기관이 사이버 위협과 주요 정보 시스템의 취약점에 대한 정보를 수집, 추적 및 분석하는 활동을 더욱 강화한다.	1999. 9.
정보 기관, 국방성 및 연방법 집행 기관은 사이버 공격의 위협을 다룰 수 있도록 정보를 수집하고 분석할 수 있는 신기술 개발 워크숍을 후원한다.	2000. 1. 및 이후

히, 물리적 또는 사이버적인 컴퓨터 네트워크에 대한 공격은 일반적으로 각 주의 법 및 연방법에 위배되는 것이므로 공격 발생의 증명, 공격행위자 발견, 그리고 범죄 입증을 위한 새로운 기술 개발 개발 등이 필요하게 된다. 따라서, 국방부, 정보기관, 다른 연방기관의 대표자와 공동으로 구성되는 FBI의 NIPC(National Infrastructure protection Center)에게 언제 공격이 발생했는지를 알아내고 그 공격의 범위와 시작점을 분석하며 그 침입자를 찾아내는 탐지 능력을 개발하고 향상시키는 임무가 부여되었다. 또한 다른 나라의 법 집행부와 함께 강화된 국제 협력 시스템을 구축하고, 주요 사이버 시스템에 대한 비인가된 침입과 공격을 법률로 금하는 일반적인 접근방법을 개발할 것을 제시하였다. 프로그램 3의 주요 세부 항목은 다음과 같다[3].

2.4 프로그램4 : 적절한 방법을 통한 공격 경고와 정보의 공유

미 공군 컴퓨터에 대한 "Solar Sunrise" 공격이 1998년 2월 처음 인지되었을 때, 이러한 공격이 다른 국방 시스템이나 주요 연방 네트워크, 또는 주요한 민간분야 시스템에 대해서도 진행 중인지를 알 수 있는 절차나 방법이 없었다. 따라서, 공격정보를 실시간으로 전달할 수 있는 더욱 효과적인 국가 차원의 시스템이 필요하게 되었으며 이에 관한 내용이 프로그램 4에 포함되었으며, 다음과 같은 목적을 위하여 프로그램 4가 계획되었다.

- 연방의 정보공유 향상 : 연방시스템 관리자는 FIDNet 체계를 이용하여 연방침해사고 대응팀(FedCIRC)에 시스템 이상에 대한 데이터를 전송하며 FedCIRC는 불법행위 및 침입징후 분석을 위하여 이 정보를 NIPC에 제공한다. 이를 통하여 불규칙하고 상호 무관한 공격들간에 침입의 연관성을 파악한다. 국방부의 경우, JTF-CND(Joint Task Force-Computer Network Defense)가 국방 부문의 침입관련 정보를 수집, 정리 및 평가하여 국방부 내의 침입징후를 발견하고 이를 NIPC에 보고하며 국방부 경보를 발령한다.
- 정보공유 및 분석센터 : 민간부문과 주 및 지방 정부의 경우, 정보공유를 위하여 연방정부로부터 경고 정보를 받아서 전파하는 정보공유 및 분석센터의 설립을 장려한다. NIPC는 위협, 취약점 및 관련 사태에 대한 정보를 정보공유 및 분석센터에 제공한다.

상기와 같은 목적 달성을 위해서는 미국의 기반구조를 운영하는 기업이 정부 전문가와 시스템 취약점 등에 관한 논의를 추진하는 것이 필수적이나, 정보공개법에 의거 정부에 제공된 자신들의 기업비밀이 공개될 수 있다는 점, 미 국민의 프라이버시를 침해할 수 있다는 점 등 정보공유를 위한 장벽이 현실적으로 존재할 수도 있다. 따라서, 미 정부에서는 이와 같은 장벽을 제거하기 위한 작업도 착수하고 있다. 프로그램 4의 세부 내용은 다음과 같다[3].

- 법무부와 주요기반구조보증사무국(CIAO, Critical Infrastructure Assurance Office)는 정보의 자유법 및 주요 시스템 취약점 정보의 보호에

관한 백악관 회의를 주최한다(완료).

- NIPC의 24시간 침입 통보 체제를 구축한다(완료).
- 연방정부가 소유한 위협, 취약점 및 경고 데이터를 민간 부문의 ISAC와 정기적으로 공유할 수 있는 메커니즘을 구축한다(2000년).
- CIA와 GSA는 연방 침해사고대응팀과 민간의 침해사고대응팀이 더욱 협력하고 공통 운영시스템을 개발하기 위한 백악관 회의를 후원한다(2000년).
- 필요한 경우 정보공유 및 분석센터의 형성을 지원하기 위한 법률 개정안을 제출한다(2000년).
- 민간 부문의 단체와 협력하여 핵심적인 분야의 정보공유 및 분석센터를 설립한다(2000년 및 이후 지속).

2.5 프로그램 5 : 대응, 재구성, 그리고 복구를 위한 능력 창출

"프로그램 5의 목표는 공격이 진행중인 동안 공격을 제한하고, 산업체와 기관 내에 정보공격과 관련한 비상 및 복구계획을 구축하여 정보공격을 다룰 수 있는 능력을 배양하는 것이다."

정보전 공격은 고립된 침해사고의 영역내로 제한되지 않으며, 전체회사 혹은 전체 기관, 모든 경제 분야, 국가의 한 지역, 혹은 국가 그 자체를 대상으로 할 수 있다. 프로그램 5에서는 상기와 같은 점을 고려하여, 일단 광범위한 공격이 식별되면, 프로그램 3에서 명시한 센터들이 법 집행기관 및 다른 기관들과 제휴하여 다음과 같은 대응을 시작하도록 하고 있다.

- 의심되는 사용자들에 의한 네트워크 접근 봉쇄
- 평상시에는 사용되지 않는 "방어 상태(defense condition)" 경계 착수
- 사용되어지고 있는 공격기술에 대한 새로운 보안 소프트웨어 패치 적용
- 네트워크 요소들의 격리
- 네트워크의 일정 부분 운영 중지
- 긴급운영시스템의 운영 개시

이와 동시에 법 집행 기관 및 기타 기관은 공격의 근원을 파악하고 이를 차단하기 위한 적절한 조치를 취하게 된다. 특히 비상계획과 관련하여 PDD 67을 통하여 미국 대통령은 모든 연방 부처와 기관들이 회계연도 1999년까지 새로운 비상계획을 제출하도록 하였으며 이 계획에는 PDD 63의 비상계획 부분이 포함될 예정이다. 프로그램 5의 세부 항목은 다음과 같다[3].

- 기반구조 보호관련 연방 부처 및 기관들은 비상계획을 포함한 기반구조 운영의 지속성을 보장하기 위한 계획을 수립한다(완료).
- 주요기반구조 보증사무국은 주요기반구조 보호활동과 관련하여 감사분야의 발전방향을 정립할 것이다(2000년).
- 침해에 대한 경고가 있을 때 연방 정부 네트워크에 취할 추가적인 방어 조치를 위한 프로토콜과 권고 사항을 개발한다(2000년).
- 연방비상관리청(FEMA, Federal Emergency Management Agency)은 비상 통신 시스템의 현대화를 실시한다(2003년).

2.6 프로그램 6 : 프로그램 1-5의 지원을 위한 연구개발 촉진

프로그램 6은 보호대책을 실행하는데 필요한 연구개발의 요구사항과 이에 대한 우선순위를 규정하고 기금 마련 등을 통하여 미국의 정보보호 기술이 변화하는 위협 및 전반적인 정보시스템의 발전에 뒤쳐지지 않는 시스템을 구현하는 것이 목적이다.

프로그램 6에서는, 현재의 기술로 국가계획의 처음 5단계에서 요구되는 많은 작업이 수행되는

데 많은 난관이 있음을 인식하고, 주요기반구조 보호관련 기관간 협의회 성격을 가진 CICG(Critical Infrastructure Coordination Group)의 연구개발 소그룹에서 국가계획을 지원하기 위하여 필요한 기술을 정의하고 있으며, 민간분야와 함께 다음과 같은 작업을 수행한다.

- 정보보안 연구 및 개발에 대한 요구사항과 우선 순위 조정
- 연구개발 요구사항의 예산확보 방안 및 부처간 연구개발 과제 조정
- 이미 수행된 연구에 연방자금이 사용되는 것을 방지하기 위한 의견 교환
- 필요기술이나 시장성 부족으로 인한 연구개발 미개척 분야 식별

이 과정은 이미 1998년에 시작되었으며, 여기에서 식별된 연구개발 우선 순위에는 다음과 같은 것들이 있다.

- 대규모 네트워크의 침입탐지 모니터링을 지원하는 기술
- 운영체제 코드내의 악성 코드(트랩도어)를 식별할 수 있는 인공지능 및 기타 기술
- 침입자를 억제, 중지 및 퇴출시키고 공격 또는 재난이 발생했을 때 손상을 완화하거나 정보처리 서비스를 복구하기 위한 방법
- 네트워크 신뢰성, 시스템 생존력 및 주요 기반구조의 구성요소와 시스템의 견고성을 향상시키기 위한 기술
- 공격 또는 고장에 대한 기반구조의 대응을 모델링하고, 상호의존성 및 핵심적인 취약한 노드, 구성요소 또는 시스템을 파악하기 위한 기술

프로그램 6의 주요 세부 항목은 다음과 같다[3].

- FY 2000 예산 및 추후의 예산을 위한 연방 주요 기반구조 보호를 위한 R&D를 조정한다(완료).
- 과학기술정책청(OSTP, Office of Science Technology Policy)은 민간 부문 및 학계와 협력하여 매년 연방 정부의 주요 기반구조 보호 R&D 우선순위를 조정한다(계속).
- 산업계, 학계 및 정부의 전문가들과 회의를 개최하여 보호책을 지원하는 주요 R&D 우선 순위에 대해 논의하고, 주요 기반구조 보호에 있어서 연방 및 민간분야의 R&D를 조정하기 위해서 공공-민간 협의 메커니즘을 수립한다(계속).
- 연구개발 성과의 활용을 위하여 주요 프로젝트의 목표일을 확인한다(완료).
- 주요기반구조 공통의 프로젝트를 지원하고, 2002회계년도의 공공-민간의 연구개발을 조정한다(2001년 3월).
- 정보기반구조보호연구소(I3P, Institute for Information Infrastructure Protection)를 설립하고 다수의 연구 프로젝트에 기금을 제공한다(2001년).

2.7 프로그램 7 : 적절한 수의 정보보안 전문가 채용 및 훈련

프로그램 7은 연방정부와 국가 전반에 걸쳐 필요한 정보보안 전문가와 기술을 조사하고 추가 인원을 훈련시키고 채용하기 위한 조치를 취하는 것이 목적이다. 주요기반구조를 보호하기 위하여 기본적인 요구사항은 잘 훈련된 인력이며, 미 정부에서는 대학의 학부 및 대학원 정보보호 프로그램을 통하여 인력부족 문제를 해결하려 하고 있다. 이 프로그램의 주요골자는 다음과 같다.

- 연방인사처(Office of Personnel Management)를 통한 연방 정부의 IT 직책의 수, 이러한 직책에 필요한 핵심적인 자격 및 교육훈련과 인증 업무를 파악

활 동	목 표 일
사이버 시민 프로그램을 구축하여 미국의 아동들에게 컴퓨터 시스템 사용에 대한 적절한 행동 및 윤리를 가르친다.	완료 (1999년 5월)
민간-공공 주요 기반구조 보안 협력관계를 구축하여 주요 정보 시스템 및 컴퓨터 네트워크의 위협에 대한 기업 및 정부의 의식을 높인다.	2000년 2월

- 정보기술 우수센터(CITE: Center for Information Technology Excellence) 지정을 통한 연방 IT 직원 교육, 기술 수준을 유지를 위한 교육제공
- SFS(Scholarship for Service) 프로그램을 통한 차세대 연방 IT 종사자와 보안 관리자들을 모집하고 교육. 이를 위하여, 매년 정보보호 분야의 학부 또는 대학원 학위를 취득하려는 300명의 학생들에게 장학금을 제공하고, 이의 대가로 학생들은 졸업 후 일정 기간동안 연방 IT 직원으로 근무
- 유망한 고교생을 선발하고 여름방학때 인턴 프로그램에 참가한 후 연방 IT 직원 표준 인증을 받도록 유도하여, 미래에 연방정부에 고용. 또한 중·고등학교에서 컴퓨터 보안 의식 제고 프로그램 개발
- 전체 연방 직원의 컴퓨터 보안 의식 제고를 위한 프로그램 개발

프로그램 7의 주요 세부 항목은 다음과 같다[3].

- SFS 프로그램 홍보 및 SFS 후보자의 인증 절차를 개발한다(완료).
- 연방 차원의 정보 시스템 보안 교육훈련 프로그램의 검토를 완료하여 현존하는 프로그램 및 부족하거나 중복되는 부분을 파악한다(2000년 3월).
- 대학의 SFS 프로그램 지원 및 참가 선정을 위한 표준 및 지침을 수립한다(2000년 4월).
- 시스템 관리자 및 정보보호책임자를 위한 연방 IT 보안종사자 인증 프로그램을 개발하고, 인증 목표를 달성하기 위한 교육훈련 프로그램을 개발한다(2000년 5월).
- INFOSEC 인식제고 커리큘럼을 개발하고 배포한다(2000년 5월).
- CITE 지정 표준을 수립한다(2000년 6월).
- 중·고등학교 홍보 프로그램을 개발한다(2000년 7월).
- SFS 프로그램 참가 대학을 선정한다(2000년 여름).
- 연방 정부 내의 정보 시스템 보안업무 수요를 조사하여, 연방 IT 직원 모집, 보수 및 자격 개발에 대한 신뢰성 있는 데이터를 확보한다.(2000년 여름).
- 2001년 1월부터 1년간 SFS 학부생 및 대학원생을 모집하고, 이후 매년 300명의 학생들을 모집한다(2000년 가을).

2.8 프로그램 8 : 향상된 사이버 보안 필요성을 미국인이 인식하도록 홍보

미국은 자국의 사이버공간 보호가 정부 단독의 일이 아닌 사업가, 정부, 그리고 평범한 시민까지 모든 미국인의 동참이 필요하다고 깨닫고, 정보시스템에 놓여진 새로운 위협 및 이를 방지하기 위한 행동의 필요성에 대한 이해 및 인식제고를 위하여 많은 노력을 기울이고 있다. 프로그램 8에서는 광범위한 인식제고 노력의 일환으로 다음과 같은 세부 실행계획을 수립하였다[3].

2.9 프로그램 9 : 프로그램 1-8을 지원하는 정부예산과 법령의 채택

프로그램 9는 다른 프로그램에서 제안된 추진전략을 지원하는 데에 필요한 법적 체계를 개발

하기 위함이다. 클린턴 대통령은 미국의 주요 기반구조를 보호하기 위하여 PDD 63을 제안했으며, 연방 부처 및 기관에게 그들의 중요시스템을 안전운영과 국가의 기반구조를 보호하기 위해 민간분야와의 협력구축을 PDD 63에서 언급하였고, 이에 부응하여 미국 의회는 FY 2000 예산으로 17억 3천7백만 달러를 책정하였다.

2.10 프로그램10 : 미국시민의 시민자유권의 완전한 보호, 시민의 사생활 권리, 그리고 시민 소유의 데이터 보호권리 보장

프로그램 10은 프로그램 1에서 부터 프로그램 9를 통하여 주요한 사이버 시스템들을 보호하는데 있어서 헌법과 다른 법률적 권리를 보호하기 위해 수행해야 할 작업들을 명시하고 있다. 미 정부는 주요 기반구조를 안전하게 하는 것도 중요하지만, 무엇보다도 시민의 자유를 보호하는 것이 우선하여야 한다고 인식하고 있다. 프로그램 10은 시민자유를 보장하기 위하여 매년 사이버 보안, 시민 자유, 그리고 시민권에 관한 공동토의를 개최하고 산업계 인사들로 구성된 국가기반구조 보증자문위원회(NIAC, National Infrastructure Assurance Council)에서 시민자유와 사생활권리, 그리고 개인소유 데이터 보호와 관련하여 국가계획 구현에 대한 검토 등을 매년 수행할 것을 규정하고 있다.

3. 결 론

정보기술의 발전에 따라 전세계 거의 모든 국가가 자국의 경제활동 보장, 국가안보 유지를 위한 핵심기능을 컴퓨터 시스템을 포함하는 제어시스템에 의존하게 될 것이며 이와 같은 추세는 앞으로 계속 지속될 것이다. 특히, 정보기술이 발전하면 할수록 이러한 현상은 더욱 심화될 것이다. 따라서, 컴퓨터 시스템을 포함하는 제어시스템에 의존하고 있는 전력과 전화망, 운송시스템, 그리고 금융기관 등에 대한 사이버 공격은 해당 기관의 네트워크 파괴뿐 아니라 국가경제, 심지어 국가안보에까지 영향을 미칠 개연성이 농후해졌다고 할 수 있다. 분명한 것은 다음 세대의 전쟁에서 목표는 국가의 주요 기반구조가 될 것이며, 이미 기반구조를 공격하기 위한 새로운 무기가 각국마다 비밀스럽게 개발되고 있다는 사실이다.

본 논문에서는 주요 기반구조를 보호하기 위한 미국의 노력인 국가계획을 분석하였다. 미국에서 제시하는 국가계획은 준비 및 예방, 탐지 및 대응, 튼튼한 기반구축의 3가지 목적을 가진 10개의 프로그램으로 구성되어 있으며, 각 프로그램마다 세부 실행계획을 포함하고 있다.

현재 우리나라의 경우에도, 정보통신부 등 일부 정부부처 및 한국정보보호센터를 중심으로 주요기반구조를 보호하기 위한 노력을 다각적으로 기울이고 있다. 미국의 국가계획에서 알 수 있듯이, 국가의 주요 기반구조를 효과적으로 보호하기 위하여서는 미국의 국가계획과 같이 주요기반보호를 위한 국가차원의 보호대책을 우리의 실정에 맞게 현실화할 필요성이 있으며 이를 적극적으로 추진하고자 하는 각계의 노력이 병행되어야 할 것이다.

참고문헌

[1] http://www.ciao.ncr.gov/63factsheet.html, Protecting America's Critical Infrastructures, 1998. 5.

[2] http://www.cdt.org/policy/terrorism/fidnet, National Plan for Information Systems Protection, 1999. 6.

[3] http://www.ciao.ncr.gov, National Plan for Information System Protection Ver. 1.0, Jan. 2000.

이 철 원

1987년 충남대학교 수학과(이학사)
1989년 중앙대학교 전자계산학과 (이학석사)
1989년-1996년 한국전자통신연구원 선임연구원
1996년-현재 한국정보보호센터 통신모델링 과제책임자
관심분야 : 컴퓨터 및 네트워크 보안, 주요기반구조 보호, 정보보호시스템 평가기준

박 용

1998년 서울대학교 사회학과 졸업
1998년-1999년 한국정보보호센터 기술정책팀 연구원
현재 한국정보보호센터 인증관리팀 연구원
관심분야 : 정보보호 정책, 주요기반보호 정책, 전자상거래 보안 및 전자서명 인증

이 홍 섭

1979년 한양대학교 전자공학 (공학사)
1985년 한양대학교 전자공학 (공학석사)
1999년 대전대학교 컴퓨터공학 (공학박사)
1980년-1996년한국전자통신연구원 책임연구원, 실장
1996년-현재 한국정보보호센터 연구개발부장, 기술본부장. 현 개발부장
1996년-현재 한국통신정보보호학회 상임이사
1997년-현재 정보통신기술협회 정보보호기술위원회 의장
관심분야 : 네트워크 및 시스템 보안, 전자상거래 보안 및 전자서명 인증