정보통신의 보안 강화 방안

박 훤 일 (경희대 법대 교수)

차 례

우리나라는 '정보화'를 국가적인 사업으로 추진한 결과 세계 최고수준의 초고속 인터넷 통신망이 전국에 가설되었으며 주요기반시설도 네트워크로 연결되어 있다. 그러나 우리나라의 정보통신망은 2003년 초의 1·25 인터넷 대란 때 경험하였듯이 사이버 공격에 매우 취약한 실정이다.

OECD에서는 정보통신의 보안은 제도나 기술만으로는 지키기 어렵고 하나의 문화(culture of security)로 고양되어야 한다고 말한다. 여기서는 전호(No.114)에 소개한 "9·11 사건 이후 미국 국토안보법제의 변화" 중에서 미국의 「사이버공간 안전을 위한 국가전략」과 비교하였을 때 우리나라에서는 정보통신망의 안전성을 강화하기 위하여 법제와 실제면에서 어떻게 대비하고 있는지 살펴보기로 한다.

---

1. 머리말

오늘날 사이버 공간에서의 침해사고(incident)는 해킹, 악성 코드의 유포, 서비스거부 공격 등 다양한 형태로 이루어지고 있다. 그러나 이러한 전자적 침해행위는 누가 하였는지도 모르게 신속하게 이루어지고 사고가 발생한 후에야 대처가 가능하므로 사전에 사이버 공간의 취약점을 보강하고 사후에는 신속한 대응 및 복구를 통하여 피해를 최소화할 필요가 있다.

현재 우리나라에는 전기통신기본법, 정보통신망이용촉진및정보보호등에관한법률, 정보통신기반보호법, 전자거래기본법 등 여러 가지 정보통신의 안전에 관한 법률이 시행되고 있으나 사이버공간에서의 정보통신망에 대한 공격 가능성에 대비하고 사고발생 시의 효과적인 대응 및 책임소재 규명에 충분치 못한 실정이다.

따라서 본고에서는 사이버공간의 안전성을 도모하기 위한 우리나라 현행 법제상의 문제점과 그 개선방안을 검토하고자 한다.

우리나라의 정보보호 관련법률 현황

목 적	법률의 내역
① 정보 자체의 기밀성 보호(암호)	- 국가보안법, 국가정보원법, 군사비밀보호법, 형법 - 정보화촉진기본법, 전자거래기본법, 전자서명법
② 정보의 수집·이용에 관한 시스템, 네트워크의 보호	- 정보화촉진기본법, 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률 - 전자정부구현을위한행정업무등의전자화촉진에관한법률, 전자거래기본법, 전자서명법 - 형법, 통신비밀보호법 - 화물유통촉진법, 산업기술기반조성에관한법률, 무역업무자동화촉진등에관한법률
③ 개인정보의 보호	- 공공기관의개인정보보호에관한법률, 정보통신망이용촉진및정보보호등에관한법률 - 신용정보의이용및보호에관한법률, 금융실명거래및비밀보장에관한법률 - 통신비밀보호법
④ 정보보호산업의 육성	- 정보화촉진기본법, 전자거래기본법, 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한법률

2. 정보통신의 안전성에 대한 위협

오늘날 정보통신의 안전성이 요구되는 이유는 경제·사회의 주요 기반 시스템이 개방 네트워크인 인터넷 기반의 정보통신에 크게 의존하고 있기 때문이다. 다시 말해서 국가안보, 행정, 치안, 금융, 통신, 운송, 에너지 등 주요 시스템의 어느 하나도 인터넷을 통하여 전자적으로 제어·관리되지 않는 것이 없을 정도로 점점 더 정보통신에 의존하는 경향이 심화되고 있다. 더욱이 우리나라는 전자정부(e-Government)를 구현하기 위하여 정부가 관련법률을 개정하고 정보기반구조(information infrastructure)를 구축하는 일에 앞장서 왔기 때문에 세계 어느 나라보다도 정보화의 속도가 매우 빠르다.

그러나 이에 비례하여 국내·외의 컴퓨터 전문가들이 컴퓨터와 인터넷을 이용하여 범죄를 자행하는 사례가 늘고 지역 분쟁이 빈번히 발생하면서 사이버戰(cyber war)이 벌어질 가능성도 커지고 있다. 이러한 사태는 정보통신기반시설을 대상으로 해킹, 컴퓨터 바이러스, 논리·메일폭탄, 서비스거부(denial of service: DoS), 고출력 전자기파 등 다양한 방법으로 일어날 수 있으므로(정보통신기반보호법 2조2호 참조) 정보통신시스템이 안정적으로 가동하기 위해서는 이러한 전자적 침해행위가 일어나지 않도록 사전에 예방을 하고 사후에는 신속히 피해를 복구하는 것이 중요하다.

요컨대 정보통신의 '안전성' 내지 '보안'이란 정보통신망에 대한 전자적 침해행위를 사전에 예방하거나 사후에 피해를 복구하는 등 정보통신 시스템이 정상적으로 가동하도록 보장(assurance)하고 정보통신기반시설을 보호(protection)하는 것을 말한다. 그러나 정보기술의 발달에 따라 전자적 침해행위도 고도화되고 있으므로 이에 관한 국제적 동향을 파악하고 국제협력을 추진하는 것이 중요하다(정보통신기반보호법 26조). 예컨대 OECD가 2002년 7월 채택한 「정보 시스템 및 네트워크의 안전을 위한 지침」[1] 이나 미국이 2003년 2월에 공표한 「사이버공간 보안전략」[2]이 좋은 기준이 될 것이다.

여기서 전자적 침해행위란 정보시스템의 취약점을 공격하여 시스템 내에 침투하거나 시스템을 마비·파괴하는 등의 사고를 유발하게 하는 것을 말한다. 좁게는 정보통신기반보호법 제2조제2호에 정의되어 있는 행위유형을 의미하지만, 넓게는 시스템이 당초 설계된 기능을 발휘할 수 없는 하드웨어·소프트웨어의 사기 및 절도, 산업스파이 활동, 데이터 조작상의 오류·사보타지, 풍·수해, 지진, 화재, 정전 등의 사고를 포함한다. 미국에서는 '사이버 공격'(cyber attack) 또는 '사이버 위협'(cyber threat)이라 하여 "컴퓨터 시스템을 이용하여 악의적인 목적을 갖고 컴퓨터 시스템 및 네트워크로 구성된 사이버공간에 대하여 불법적·악의적으로 국가의 정상적인 기능수행에 악영향을 미치고자 하는 일체의 과정과 행위"로 정의하고 있다.

정보통신의 보안이 추구하고 있는 기밀성(confidentiality), 가용성(availability), 무결성(integrity), 진정성(authenticity)의 관점에서 본다면 실시간으로 정보를 가로채 내용을 알아보는 감청(interception), 정보의 전송과정을 침해하는 방해(interruption), 권한 없이 정보의 내용을 수정하는 변작(modification), 권한 없이 없는 정보를 만들어내는 위작(fabrication)이 각각의 침해행위에 해당한다.

이러한 전자적 침해행위에는 해킹, 컴퓨터 바이러스, 웜, 트로이 목마, 논리폭탄, 전자우편폭탄 및 스팸메일 등이 있다. 이 중에서 웜, 논리폭탄, 전자우편폭탄 등이 사이버테러 수법으로 흔히 이용되는데 이를 간단히 설명하면 다음과 같다.

---

1) OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. <http://www.oecd.org/pdf/M00034000/M00034292.pdf>

2) The White House, *The National Strategy to Secure Cyberspace*, February 2003.

o 해킹(hacking): 악의적인 의도로 컴퓨터 시스템이나 네트워크에 존재하는 취약점을 이용하여 시스템과 네트워크의 정상적인 작동을 방해함으로써 사용자에게 위해를 가하는 행위

o 컴퓨터 바이러스(computer virus): 프로그램에 잠입하여 컴퓨터로 하여금 본래 목적 이외의 처리를 하도록 하는 프로그램을 말하며 종류에 따라서는 컴퓨터 시스템에 치명적인 해를 끼칠 수도 있다. 1970년대 미 국방부 알파-네트(Alpha-Net)에서 최초로 발견된 이래 최근에는 하루에 수십 개의 새로운 바이러스가 생겨나고 더욱 빠르게 확산되고 있다.

o 웜(worm): 컴퓨터 바이러스와 같은 악성 프로그램의 일종으로 바이러스와는 달리 컴퓨터 시스템의 다른 프로그램을 감염시키는 것이 아니라 자신을 스스로 복제하는 것이 특징이다. 그리하여 네트워크를 통해 널리 전파시킴으로써 네트워크에 치명적인 피해를 입히게 된다.

o 트로이 목마(Trojan horse): 운영체제(OS)에 대한 일반적인 침투유형의 하나로 마치 정상적으로 보이는 프로그램 내부에 숨겨 놓은 프로그램을 말한다. 계속적인 불법 침투가 가능하도록 시스템 내부에 부호를 생성하여 영구적으로 시스템 내부에 상주하다가 소기의 목적을 달성한 후에는 그 자취를 지워버리기도 한다.

o 논리폭탄(logic bomb): 트로이 목마의 일종으로 독립적인 형태 또는 시스템 개발자나 프로그래머가 의도적으로 프로그램에 오류를 발생시키는 프로그램 루틴을 무단 삽입한 것을 말한다. 특정 조건의 성취 또는 특정 데이터의 입력을 계기로 하여 프로그램이 전혀 예상치 못한 파국적인 오류를 범하도록 컴퓨터 시스템을 실행시키는 악성 코드이다.

o 전자우편폭탄(mail bomb): 수신인의 컴퓨터 시스템을 마비시키거나 파괴할 의도로 발송된 전자우편. 제어문자의 특수한 배열로 단말기를 폐쇄하기도 하며, 첨부파일에 바이러스나 트로이 목마를 포함시키거나 우편의 용량을 지나치게 크게 함으로써 전자우편함의 한계용량을 초과시켜 결국 시스템을 마비시킨다.

o 서비스 거부(denial of service: DoS): 정상적인 정보통신서비스를 방해하거나 정지시키기 위해 짧은 시간에 대량의 데이터를 대상 시스템에 전송하는 것. 악의를 가진 집단이 대상 서버에 엄청나게 많은 접속시도를 함으로써 서버의 자원을 소모시키고, 정상적인 사용자에 의한 접속을 불가능하게 만든다. 분산서비스거부(distributed DoS)란 해커에 의해 공격 프로그램이 설치된 수십, 수백 대의 컴퓨터에서 대상 서버를 행해 일제히 공격이 시도되는 것을 말한다.

o 스파이웨어(spyware): 어떤 사람이나 조직에 관한 정보를 수집하는 도구. 특정 사용

자에 관한 정보를 수집하여 광고업체나 관심 있는 사람에게 제공할 목적으로 사용된다.

o 전자기적 위협(electro-magnetic threat): 최근 들어 Chipping, Nano machine, HERF gun, EMPBombs, Electronic Jamming 등의 수단이 하드웨어를 마비・파괴하기 위해 많이 사용되고 있다.

3. 정보통신의 보안을 위한 현행 법제도

정보통신의 보안을 정보 시스템 및 네트워크에 관한 것에 국한시켜 본다면 현재 형법 및 정보통신망이용촉진및정보보호등에관한법률(이하 "정보통신망법"이라 함), 정보통신기반보호법의 다음 규정들이 그러한 목적을 위해 시행되고 있다.

첫째, 형법은 1995년 개정 시 정보기술의 발달에 따른 새로운 범죄유형에 대응하기 위하여 제314조의 업무방해죄에 컴퓨터등 장애에 의한 업무방해죄가 추가되었다. 컴퓨터등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해하는 행위이다. 해킹, 바이러스 유포로 인하여 컴퓨터 시스템의 작동에 이상을 일으킨 경우가 이에 해당한다.

둘째, 정보통신망법은 정보통신서비스제공자에 대하여 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하도록 의무화(동법 45조1항)하는 한편 정보통신망 침해행위 등에 대하여 벌칙을 적용하고 있다(동법 62, 63조).

처벌대상은 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 정보통신망 부정침입행위(동법 48조1항), 정보통신시스템, 데이터 또는 프로그램 등을 훼손・멸실・변경・위조 또는 그 운용을 방해할 수 있는 악성 프로그램의 전달・유포행위(동법 48조2항), 대량의 신호・데이터를 보내거나 부정한 명령을 처리하게 하는 등 정보통신망에 장애를 유발하는 행위(동법 48조3항), 정보통신망으로 처리・전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해・도용・누설하는 행위(동법 49조) 등이다.

셋째, 정보통신기반보호법에 의하면 다음의 행위를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

- 접근권한을 가지지 않은 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작・파괴・은닉 또는 유출하는 행위
- 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 등의 프로그램을 투입하는 행위

- 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위(예: 웜, 논리폭탄, 전자우편폭탄 등에 의한 서비스 거부(DoS 또는 DDoS) 등)
- 이상의 행위는 앞에서 살펴본 정보통신망법상의 행위가 주요정보통신기반시설에 대해 행해질 경우 한층 가중처벌하도록 한 규정이다.

4. 정보통신 보안 강화를 위한 대책

가. 원 칙

우리나라 정보시스템의 안전성을 제고하려면 법제도 면의 개선 이전에 정보보안에 대한 정부, 기업, 개인의 인식(awareness)을 획기적으로 제고할 필요가 있다. 현재 우리나라에서 많이 이용되고 있는 정보보안 기술에는 사전예방적 기술로서 침입차단기술(방화벽)과 암호기술이 있고, 사후방지적 기술로서 바이러스 백신 및 침입탐지 시스템이 있다. 우리나라의 정보보호업체들은 세계적으로 상당한 기술 수준을 인정받고 있으며, 직접 또는 외국 기업과 제휴하여 수요처에 제공하고 있다.

정부 차원에서도 정보화 못지 않게 정보보안을 위한 교육훈련 및 제품구입, 외주용역(outsourcing)에도 예산배정을 대폭 늘려야 한다. 일단 정보보호시장이 협소한 우리나라에서 외형적인 시장규모를 키워놓아야 정보보안 산업이 기술개발투자에 힘을 쏟고 내수 및 수출확대에 노력할 수 있을 것이다. 정보보안 산업의 발전을 위해서는 보안제품의 혁신 및 수요 창출, 가격경쟁력 제고, 정보보안제품의 필요성에 대한 인식의 확대가 시급히 요청된다.

구체적인 실천에 있어서는 개인(가정)과 중소기업, 대기업, 공공기관, 국가적 기반구조(national infrastructure), 국제협력의 단계별로 현황을 파악하고 그에 따른 개별 또는 공동으로 일률적 또는 단계적인 개선방안을 모색하는 것이 합리적일 것이다.[3]

정보보안의 강화를 위해서는 세 가지 측면을 함께 고려하여야 한다.[4] 그것은 정부가 주도적으로 정보보안에 관한 법률제도를 정비하는 것도 중요하지만 그 못지 않게 市場에서도 정보보안 관련업체들 상호간 그리고 정보통신망 이용자들과의 사이에 정보보안에 관한 모범적인 관행(best practices)이 정립되는 기능(market forces)이 작동하여야 한다는 것을 의미한다. 아울러 정보보안 기술에 있어서도 최적의 해결방법(solution)[5]이 모색되어야 한다.

---

3) 미국의 「사이버공간 보안강화전략」에서는 이러한 단계별로 실천계획 및 권고사항(Actions and Recommendations)을 제시하고 있다.

4) 정보보호에 있어서 세 가지의 접근방법을 강조한 것은 Joel R. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation", pp.1-2. 참조.

5) 기술적인 해결방법에는 기술법(*Lex Informatica*)의 형식으로 네트워크 구조에 기술표준, 프로토콜, 디

다시 말해서 정보통신의 보안은 기술적으로만 해결할 수 있는 것이 아니다. 정부가 법률제도 상으로 정책목표 및 정보보안의 기준을 설정하고 정부기관이 정보통신의 안전성에 대한 일차적인 책무를 부담하는 동시에 정보보안 관련기업 및 이용자들이 이에 협조하여야 하는 것이다. 또한 정보통신의 보안은 개인의 프라이버시 보호와 대립관계에 있기 때문에 양자의 균형을 도모하는 것도 중요하다. 뿐만 아니라 정보보안 관련업체, 보안관리담당자, 이용자들이 정보보안의 중요성을 인식하고 스스로 이를 지켜나가는 자율적인 행동규범(codes of conduct)이 마련되어야 한다.

그러나 이것만으로는 부족하다. 정보통신의 안전을 침해하는 기술이 발달하는 만큼 이에 대응하는 정보보호 기술의 진보를 위해서는 안정적인 시장이 확보되어야 하는 것이다. 다시 말해서 정보보안 기술의 제일 큰 수요자인 정부기관들이 선도적으로 구매를 함으로써 기술의 발달을 촉진하고 이 과정에서 개발된 신기술이 주변 영역으로, 다른 나라로 파급되도록 하는 선순환이 이루어져야 한다.

이를 위해서는 다음과 같은 행동계획(Action Plan)을 실천에 옮길 필요가 있다.

첫째, 정부는 정보통신의 보안을 위한 법제를 정비한다. 정부의 정보보호 조직은 특정 기구를 중심으로 개편하기보다 운영의 묘를 살려 현행 조직을 보다 유기적으로 연결하는 것이 바람직하다. 사이버 공격을 처벌하는 실체법은 가급적 기본법으로 일원화한다.[6] 사이버 공격을 수사하기 위한 절차는 인권 및 프라이버시의 존중을 위해 법원의 심사를 받도록 하되 비상사태 발생 시에는 사태가 해소될 때까지 한시적으로 미국 애국법(USA Patriot Act)과 유사한 제도를 도입한다.

둘째, 주요정보통신기반시설의 보호를 위하여 정부는 하드웨어, 소프트웨어를 포함한 정보보안 시스템 기타 제품을 우선적으로 구매하도록 한다. 정부가 앞장서서 구매할 때 정보통신 보안관련 업체는 시장의 확대에 따라 기술개발투자의 여력이 생기고 내수와 수출도 증가하게 될 것이다.

셋째, 우리나라가 비교우위를 가진 바이러스 백신, PKI 암호기술, 가상사설망 등 전략적인 정보보호산업을 육성한다.

넷째, 기업과 개인의 정보보안의식을 제고함으로써 국내 정보보안시장을 확장될 수 있는 풍토를 조성한다.

다섯째, 정보보호산업의 국제표준화 및 수출을 지원한다.

폴트 환경설정을 심어놓는(embedded in network architecture) 방안 등이 있다.

6) 형사처벌에 관한 법률은 가능한 한 일원화하여 단순·명료하게 규정하여야 예측가능성과 실효성을 높일 수 있다. 특별법상의 벌칙은 일반법으로 처리할 수 없는 특별한 경우에 예외적으로 인정되는 것이 타당하다. 미국의 사이버 공격에 대한 처벌 규정을 보면 1984년 컴퓨터사기및오용방지법(Computer Fraud and Abuse Act of 1984, 18 U.S.C. §1030)을 기본으로 기술의 발달, 시대상황 등을 고려하여 조문을 손질함으로써 사이버공간에서의 각종 범죄에 대응하고 있다.

나. 구체적인 실천방안

정보통신망의 보안대책은 유기적인 민·관 협력을 강화하되 정부가 이니셔티브를 갖고 개입할 분야와 민간부문을 지원할 분야를 구분할 필요가 있다. 주요 기반시설방어 종합계획 수립 및 사이버 공격의 탐지·경고·위기관리체제 구축, 조직적인 피해복구는 국가적 차원에서 수행하고, 민간부문의 자원이 부족한 분야는 정부가 주도적 역할을 담당하며, 국제성·범죄성을 띠는 경우에는 정부가 즉각 개입하도록 한다. 반면 민간부문의 기술력이 뛰어난 부문은 정부가 각종 인센티브를 제공하는 등 협력을 강화하여야 할 것이다.

정부방침이나 행정지도만으로 당장 시행할 수 있는 사항은 첫째, 국가적 대응체계의 원칙을 제시하고 민·관 협력체계를 강조하는 「사이버보안 기본전략」을 수립하는 일이다. 민·관 협력에 의한 사이버보안 연구개발과제를 선정하고, 사이버공간의 취약점 분석, 솔루션 개발 등 민·관·산·학의 협력과 역할분담을 통한 다양하고 구체적인 모델을 수립하도록 한다.

그리고 정부 또는 공기업의 정보화 추진 시 예산의 일정 비율은 사이버보안 진단을 받고 정보보호 솔루션을 구입하도록 의무화할 필요가 있다. 이 경우 중소기업에 속하는 정보보안업체가 개발한 정보보안 기술개발제품을 우선구매하는 등 필요한 지원시책이 마련되어야 할 것이다.

법률의 개정을 요하는 사항으로서 정보통신기반보호법의 법체계상의 문제점을 시정하고, 형법, 정보통신기반보호법, 정보통신망법 상의 사이버보안 침해행위유형을 정비하도록 한다. 또한 사이버보안 침해행위를 수사하는 절차법의 정비함에 있어서는 사이버 프라이버시권과 조화를 이루는 범위에서 절차상의 특례를 인정하는 것이 좋을 것이다.

이와 관련하여 국제적인 형사사법공조제도를 도입하여 유럽회의의 사이버범죄협약(CoE Convention on Cybercrime)에 조속히 가입하는 것이 바람직하다고 본다.

그밖에 예산조치를 요하는 사항은 주요 기관 및 일반의 사이버보안 인식의 제고를 위한 각종 캠페인을 전개하는 것, 초·중·고교 학생 및 공무원, 직장인을 대상으로 한 사이버보안 교육·훈련 프로그램을 실시하는 것, 주요정보통신기반시설의 사이버보안상태를 모의훈련을 통해 분석하는 시뮬레이션분석 센터를 설립하는 것, 주요정보통신기반시설에 대한 사이버보안 상태를 점검하는 실제 훈련을 정기 또는 수시로 실시하는 일 등이 있다. 중소기업의 사이버보안 취약점 평가 및 개선방안을 지도한다면 국가 전체적으로 사이버보안 수준이 한층 강화될 것이다.

여기서 정보보호의 로드맵은 장·단기에 걸쳐 여러 방향으로 전개되어야 한다. 우선 정부는 사이버보안이라는 큰 틀 속에서 구체적인 행동계획을 제시하고 정부가 앞

장서서 정보보호 솔루션을 채용함으로써 우리나라의 정보보호산업이 육성되는 선순환 구조를 만들어 나가는 것이 중요하다. 이 과정에서 정부와 민간부문이 긴밀한 협력관계를 이루어나가면서 정부, 기업, 개인 참여자들이 사이버보안에 대한 인식을 제고하여 일종의 '보안 문화'로서 발전시키는 것이 바람직하다. 그러므로 정부가 강제성을 띤 법률을 제정하고 이를 시행하기보다는 시장의 기능이 최대한 발휘될 수 있도록 하는 가이드라인 형태로 사이버보안 시책을 추진하는 것이 좋을 것이다.

<출처: 한국경영법무연구소,「경영법무」N0.115 (2003. 10)>