사이버정보보호의 경제적 효과에 관한 연구

- 경제적 효과 추정방법론 수립을 중심으로 -

신진*

*단국대학교

A Study on Economic Effects on Cyber Protection

Jin Shin*

*Dankook University

E-mail : korjin@empal.com

요 약

사이버 공간의 중요성이 커지고 그에 대한 의존성이 높아지면서 부수적으로 산업기밀유출, 사이버 테러, 개인정보유출의 문제 뿐 아니라 국가 간의 사이버 전쟁의 우려가 커지는 등 사이버 공간의 잠재적 위험성과 그에 따른 피해범위와 규모도 커지고 있는 실정이다. 그러므로 이에 대한 대비는 국가의 안보와 직결될 만큼 중요성이 커지고 있다. 따라서 정보보호체계의 확립이 시급하며 사이버 피해에 대한 체계적 이해가 필요하다. 이를 위하여 피해규모 및 피해액 추정 방법을 정리하고 이를 바탕으로 사이버 보호 대책을 수립해야 한다. 사이버보호의 경제적 효과는 사이버 보호 정책을 수립하는 기초적인 자료가 될 것이다.

본 연구에서는 사이버 피해의 체계적 이해를 바탕으로 사이버 보호의 경제적 효과에 대한 합리적인 추정방안을 연구하고자 한다.

ABSTRACT

Cyberspace is becoming increasingly important. Incidentally, there exist possibilities of the industrial secrets leaked, cyber attacks, privacy protection problems. In addition, there are growing concern of cyber war between nations. Thus potential hazards in cyberspace and the extent of damage are getting bigger. Therefore, a systematic understanding of cyber damage and damage scale is very important and damage estimation method should be developed to establish solid cyber protection system.

In this study, current and potential damage types are understood and damage scales are surveyed based on the analysis of existing studies and try to develop a reasonable methods to estimate economic effects of cyber protection.

키워드

Cyber Protection, Economic Effects, Cyberspace, Cyber Attacks, Privacy Protection

Ⅰ. 서 론

최근 정보기술과 네트워크의 비약적 발전으로 국가, 기업 및 개개인의 활동은 인터넷을 기반으로 한 사이버 공간으로 확장되고 있으며 그 절대적 중요성은 날로 커지고 있다.

정치, 경제, 사회 및 문화의 거의 모든 부문이 사이버 공간화 되고 있으며 사이버공간은 행정, 국방, 산업, 정보통신, 에너지, 금융 등 국가 기반시설 신경망의 핵심이 되고 있다.

사이버 공간의 중요성이 커지고 그에 대한 의존성이 높아지면서 부수적으로 산업기밀유출, 사이버 테러, 개인정보유출의 문제 뿐 아니라 국가가의 사이버 전쟁의 우려가 커지는 등 사이버 공간의 잠재적 위험성과 피해범위와 규모도 커지고 있는 실정이다.

그러므로 이에 대한 대비는 국가의 안전과 직결될 만큼 중요성이 커지고 있다. 따라서 사전에 잠재적인 사이버 위험을 체계적으로 파악하고 그 규모를 추정하며 이에 대응한 체계를 갖추는 것은 필수적이라 할 수 있다. 어차피 체계의 수립에는 그에 상응한 투자가 수반되므로 피해내용과 피해액의 추정을 기반으로 그 규모와 체계를 수립해 나가야 할 것이다.

따라서 우선 사이버 피해에 대한 체계적 이해와 피해규모 및 피해액 추정 방법을 정리하고 합리적으로 추정해나가는 것이 중요하다 할 것이다.

본 연구에서는 구체적인 산정의 전단계로 피해의 체계적 이해와 기존 연구에 대한 분석을 바탕으로 합리적인 추정방안을 모색해 보고자 한다.

Ⅱ. 사이버 시스템의 경제적 위상 및 피해형태

2.1 사이버 시스템 보호대상의 구분

보호되어야 할 사이버 시스템은 크게 시스템 자체, 기록된 정보와 그 시스템의 운용과 관련된 인력으로 나누어 볼 수 있다. 정보 시스템은 컴퓨터, 소프트웨어, 기록 매체, 통신기기 및 네트워크, 그리고 시스템 구성도 등으로 나누어 볼 수 있을 것이다. 특히 네트워크는 정보기간네트워크와 단위 네트워크, 공공성 네트워크와 민간 네트워크로 분류해 볼 수 있을 것이다.

정보시스템에 기록된 정보중 보호대상이 되는 것은 접속 기록, 문서 및 도면 등의 전자적 기록으로 나누어 볼 수 있다. 접속기록은 프라이버시 보호, 해킹방지, 사이버 범죄예방 등과 관련 하여 중요하다. 기업의 고객정보는 기업의 주요자산이며 정부나 민간의 기밀문건은 노출될 경우 큰 피해를 초래할 수 있다[1].

표 1. 일본정부의 정보보호정책 대상 범위

대상	주요내용
정보시스템	컴퓨터, 기본소프트웨어, 응용소프트웨어, 네트워크, 통신기기, 기록매체, 시스템 구성도
정보시스템에 기록된 정보	접속 기록, 문서 및 도면 등의 전자적 기록
이들 정보에 접속하는 자	상근, 비상근 및 임시직을 포함한 직원, 위탁사무자등

2.2 사이버 범죄의 형태

표 2. 사이버 범죄형태 별 피해자

사이버 범죄 형태	피해자		
	개인	기업	정부
온라인 사기행위 online fraud	○	○	
사기성 소프트웨어 scareware	○		
명의도용 identity theft	○		
지적재산권 침해 IP theft		○	
스파이 행위 espionage		○	
고객정보 손실 customer data loss		○	
온라인 절도 online theft from business	○	○	
온라인 강탈 extortion		○	
재정적 사기 fiscal fraud		○	○
접속방해 access interruption		○	○

사이버 범죄 형태는 피해자가 정부나 기업인가 또는 개인인가에 따라 얼마간의 다른 양상을 보인다.

개인의 경우는 명의도용에 의한 피해가 크며, 온라인 사기와 사기성 또는 가짜 백신 등 사기성 소프트웨어에 의한 피해가 주종을 이루고 있다.

우리나라에서는 개인의 경우 특히 보이스 피싱(voice fishing)의 피해가 최근 크게 증가하고 있다. 경찰청 자료에 의하면 2011년의 보이스 피싱 발생건수는 8,244건으로 5년 전인 2006년에 비하여 5.5배로 증가하였으며, 피해액은 1,019억 원으로 동기간 9.6배로 증가하였다.

표 3. 경찰청의 보이스 피싱 피해 통계

구분	2006년	2007년	2008년
발생건수 (증감률)	1488건 ·	3981건 (167%↑)	8454건 (112%↑)
피해액 (증감률)	106억 원 ·	434억 원 (309%↑)	877억 원 (102%↑)
구분	2009년	2010년	2011년
발생건수 (증감률)	6720건 (20%↓)	5455건 (19%↓)	8244건 (51%↑)
피해액 (증감률)	612억 원 (29%↓)	553억 원 (11%↓)	1019억 원 (84%↑)

기업의 경우는 지적 재산권의 침해가 가장 두드러지는 사이버 피해이다. 그리고 사이버 수단을 활용한 산업스파이 행위, 온라인 강탈 및 명의 및 암호 도용 등을 통한 온라인 절도 및 사기 피해가 크며 고객정보의 손실과 절도도 중요한 문제이다[2].

온라인 강탈은 기업 또는 개인을 대상으로 웜이나 바이러스를 메일에 실어 보내거나 실제 범죄에 활용하는 등 여러 가지 모습으로 나타난다. 최근에는 분산서비스거부(DDos) 공격의 형태를 보이기도 하며 특성상 보고되지 않는 경우가 많다.

정부의 경우는 세금과 복지지출관련 사기피해가 많다. 이런 종류의 피해는 중앙정부 및 지자체뿐 아니라 의료보험이나 연금의 경우에도 빈번하다.

에너지, 금융, 안보, 교통, 통신망 등 국가적인 주요 기간망에 대한 공격에 의한 교란 및 마비도 발생하고 있으며 잠재적인 위험은 경우에 따라 국가의 일부 기능을 마비시킬 정도로 그 크기를 가늠하기 어렵다.

Ⅲ. 사이버정보보호와 보호 가치

사이버정보보호의 가치는 사이버시스템이 침해되었을 때 발생할 가능성이 있는 피해의 현재가치라 할 수 있다. 또한 정보보호에 투자하지 않고 다른 분야에 동일한 자원을 투자하였을 경우 얻을 수 있는 최대의 효과는 즉 정보보호투자의 기회비용이라고도 할 수 있다. 그렇다면 어느 정도의 규모로 어떠한 분야에 어떤 방식으로 정보보호체계를 구축하고 그것은 어느 정도의 투자규모를 요구하는 것일까? 이것이 우리나라와 전 세계의 각국 정부, 공공기관 그리고 민간이 당면한 시급한 과제이다. 정부는 국가적 체계를 수립하고 공공기관 및 민간에게 가이드라인을 효과적으로 제시하고 적절한 방법과 자원을 확보하고 필요한 자원을 유 무료로 공급해야 할 것이다.

사이버보안은 네트워크, 컴퓨터, 프로그램과 자료를 공격, 손상 혹은 무단 접속으로부터 보호하도록 고안된 기술, 프로세스와 수행방법을 통칭한다.

사이버보안을 위해서는 정보체계 전반적으로 통합된 노력이 필요하다. 사이버보안의 주요요소는 컴퓨터응용 보안(application security), 정보 보안(information security), 네트워크 보안(network security), 재난복구(disaster recovery) 및 업무지속계획(business continuity planning) 그리고 최종사용자 교육 등이다.

사이버보안에서의 어려움은 보안위험이 매우 빠르게 지속적으로 전개된다는 특성에 기인한다. 전통적으로 가장 결정적인 문제에만 자원을 집중하고 상대적으로 덜 중요한 요소는 무시하거나 방치하였다. 이러한 방식은 지금은 통하지 않는다. 왜냐하면 지속적으로 예상한 것보다 더 많은 새로운 위험요소들이 등장하기 때문이다.

이러한 환경에 대응하기 위해서는 사전적이고 현장형의 접근이 필요하다. 즉, 지속적인 모니터링과 실시간의 판단이 필요하고 즉각적인 대응이 이루어져야 한다는 것이다.

이를 위하여 미국연방정부는 2010년 말 지출분석에 따르면 향후 5년간 연간 130억 달러를 배정하고 있다.

Ⅳ. 사이버 보호 효과의 합리적 추정방안

4.1 기존의 추정관련 연구

미국, 영국 등 선진국 등을 중심으로 사이버피해 규모에 대한 연구가 다수 이루어져 왔다. Detica report에 의하면 영국의 경우 사이버 피해규모는 최근 연간 270억 파운드에 이르는 것으로 보고되고 있다. 개인이 입은 피해가 31억 파운드이고 기업과 정부는 각각 22억 파운드, 210억 파운드로 나타났다.

4.2 사이버 보호 효과의 추정 방안

사이버 보호의 경제적 효과를 측정하기 위해서는 현존하는 사이버 피해와 잠재적인 피해를 구체적으로 파악하여야 한다. 우선 개념적 이해를 위하여 시험적으로 추정하는 방법으로는 각국을 대상으로 기존의 연구들이 분석한 방법을 근거로 국민소득, 산업분야별 생산액 또는 매출액 등을 비교하여 산출하는 방법을 생각할 수 있다. 또 하나는 기존 연구 대상국가와 우리나라의 측정대상별 특성을 비교하여 적절한 방법으로 파라메터를 수정하여 추정하는 방법이 있을 것이다.

향후 정밀한 추정을 위해서는 우리나라 자체의 원 데이터를 체계적으로 수집하고 그것을 바탕으로 실제 피해액에 가깝게 산정하는 모델을 수립해야 한다. 피해액을 산정한 후 그 피해를 방지하기 위한 대책이 마련되고 추진될 경우 얻을 수 있는 경제적 편익을 추정하기 위한 모델이 마련될 수 있을 것이다.

Ⅴ. 결론

사이버 시스템에 대한 공격의 형태는 날로 새로워지고 있으며 그 피해가능성 및 피해규모 도 급속히 증가할 것으로 보인다. 따라서 정보보호를 위한 대비는 항상 즉각적으로 이루어져야 하며 국가정책의 최우선적 과제라 할 것이다. 사이버 시스템의 주요 요소만 보호하면 되는 것이 아니라 사이버시스템 체계를 보호해야 한다. 따라서 그에 필요한 자원을 적절하게 배분하는 것이 필요하다 할 것이다. 향후 적절한 자원배분에 관한

연구가 치밀하게 진행되어야 할 것으로 사료된다.

참고문헌

[1] 정보보안대책추진회의결정(情報セキュリティ対策推進会議決定), 情報セキュリティポリシーに関するガイドライン, 2000.

[2] THE COST OF CYBER CRIME, A Detica report in partnership with the Office of cyber security and information assurance in the cabinet office, 2011.