情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

사이버정보보호의 경제적 효과분석: 국가적 피해액 산정을 중심으로*

신 진†‡
단국대학교

Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation of National Loss*

Jin Shin†‡
Dankook University

요 약

최근 여러 차례의 DDoS공격 및 정보유출사태에서 보듯이 사이버공간에 대한 의존성이 높아지고 있다. 산업기밀 유출, 사이버 테러, 개인정보유출의 문제 뿐 아니라 국가 간의 사이버 전쟁의 우려가 커지는 등 잠재적 피해범위와 규모도 커지고 있다. 그러므로 이에 대한 대비는 개인과 기업의 이익뿐만 아니라 국가의 안보, 나아가 세계평화와 직결될 만큼 중요성이 커지고 있다. 따라서 사이버정보보호체계의 확립이 시급하며 이를 위하여 사이버피해에 대한 체계적 이해가 필요하다. 따라서 사이버공간의 피해액 추정 방법을 정리하고 이를 바탕으로 정보 보호 대책을 수립하는 것은 중요한 국가적 과제라 할 수 있다. 정보보호의 경제적 효과에 대한 분석은 국가 정보보호 정책을 수립하는 기초적인 자료가 될 것이다. 우리나라의 사이버범죄에 의한 잠재적 피해액은 산정기준에 따라 큰 폭의 차이를 보이지만 대략 10조원에서 40조원 정도의 범위에 있다고 추정해 볼 수 있다.

ABSTRACT

Recent DDoS attacks and private informations leaked show that everyday life is interwoven with cyberspace and we are becoming more vulnerable to cyber attacks. Therefore, a systematic understanding of cyber damage structure is very important and damage loss estimation method should be developed to establish solid cyber security protection system. In this study, economic loss caused by cyber attacks are surveyed based on the analysis of existing studies and try to develop a reasonable methods to estimate economic effects of cyber security protection in Korea. Potential economic loss of Korea by cyber attacks may be situated between 10 billion and 40 billion dollars. But more sophisticated system should be established to estimate economic effects of cyber protection for proper policy decision making.

Keywords: Cyberspace, Cyber Attacks, Cyber Security, Economic Effect, Economic Loss

접수일(2012년 8월 14일), 수정일(1차: 2012년 11월 12일, 2차: 2013년 2월 13일), 게재확정일(2013년 2월 13일)
* 본 연구는 단국대학교의 지원으로 수행하였습니다.

† 주저자, korjin@dankook.ac.kr
‡ 교신저자, korjin@dankook.ac.kr

I. 서 론

최근 정보기술과 네트워크의 비약적 발전으로 국가, 기업 및 개개인의 활동은 인터넷을 기반으로 한 사이버공간으로 확장되고 있으며 그 중요성은 날로 커지고 있다. 오늘날 정치, 경제, 사회 및 문화의 거의 모든 부문이 사이버공간화 되고 있으며 사이버공간은 개인생활과 기업 활동 나아가 행정, 국방, 산업, 정보통신, 에너지, 금융 등 국가 기반시설 신경망의 핵심이 되고 있다.

그런데 이처럼 사이버공간의 중요성이 커지고 그에 대한 의존성이 높아지면서 산업기밀유출, 사이버 테러, 개인정보유출의 문제가 발생하고 국가간 사이버 전쟁의 우려가 커지는 등 사이버공간의 잠재적 위험성이 현실화되고 그 피해범위와 규모도 커지고 있는 실정이다. 따라서 이에 대한 대비는 국가의 안전과 직결될 만큼 중요한 사안으로 사전에 잠재적인 사이버 위험을 체계적으로 파악하고 그 규모를 추정하며 이에 대응한 보안체계를 갖추는 것은 필수적이라 할 수 있다. 또한 보안체계의 수립에는 그에 상응한 투자가 수반되므로 피해내용과 피해액의 추정을 기반으로 그 규모와 체계를 수립해 나가는 것이 필요하다고 하겠다.

사이버보안의 경제적 효과를 정밀하게 추정하기 위해서는 피해범주 및 규모에 대한 구체적인 자료수집과 분석체계의 구축이 전제되어야 한다. 그러나 우리나라의 경우 아직 사이버피해에 대한 정확하고 포괄적인 데이터가 마련되어 있지 않다. 이에 본고는 외국의 자료에 비추어 우리의 경우를 추정해보고자 한다.

II. 사이버 시스템의 경제적 위상 및 피해형태

2.1. 보호대상 사이버시스템

사이버 시스템은 〔표 1〕과 같이 크게 시스템 자체, 기록된 정보, 시스템의 운용 인력으로 나누어 볼 수 있다. 정보 시스템은 컴퓨터, 소프트웨어, 기록 매체, 통신기기 및 네트워크, 그리고 시스템 구성도 등으로 구성되어 있다. 네트워크는 정보기간네트워크와 단위네트워크, 공공성 네트워크와 민간 네트워크로 분류할 수 있다〔1〕.

정보시스템에 기록된 정보 중 보호대상이 되는 것은 접속 기록, 문서 및 도면 등의 전자적 기록으로 나누어 볼 수 있다. 접속기록은 프라이버시 보호, 해킹방지, 사이버 범죄예방 등과 관련하여 중요하다. 기업의 고객정보는 기업의 주요자산이며 정부나 민간의 기밀문건은 노출될 경우 큰 피해를 초래할 수 있기에 중요한 보호대상이 된다.

〔표 1〕 사이버정보보호의 대상

대상	주요내용
정보시스템	컴퓨터, 통신기기, 기록매체, 기본 및 응용소프트웨어, 네트워크, 시스템 구성도
정보시스템 기록 정보	접속기록, 문서 및 도면 등 전자적 기록
정보 접속자	상근, 비상근 및 임시직 직원, 위탁사무자 등

2.2. 사이버 범죄의 형태

사이버 범죄 형태는 피해자가 정부나 기업인가 또는 개인인가에 따라 얼마간 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 phishing)의 피해가 최근 크게 증가하고 있다. 경찰청 자료에 의하면 2011년의 보이스 피싱 발생건수는 8,244건으로 5년 전인 2006년에 비하여

〔표 2〕 사이버 범죄형태별 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		○	○

5.5배 증가하였으며, 피해액은 1,019억 원으로 같은 기간 동안 9.6배 증가하였다.

기업의 경우 가장 두드러지는 사이버피해는 지적재산권의 침해이다. 그리고 사이버 수단을 활용한 산업스파이 행위, 온라인 강탈, 명의 및 암호 도용 등을 통한 온라인 절도와 사기 피해가 크며 고객정보의 손실과 절도도 중요한 문제이다. 최근 우리나라에서는 2012년 2월부터 5개월간 가장 큰 통신사인 KT 고객 800만 명에 대한 정보가 유출되어 상업적으로 악용된 사례도 있다. 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 지자체 뿐 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.

실제로 미국, 러시아 등 여러 국가에서 피해사례가 나타나고 있으며 모의해킹을 통한 점검에서 사이버 모의공격에 의하여 주요시설의 제어시스템이 마비되는 것을 확인한 바 있다[2].

우리나라의 경우에도 사이버 공격의 피해를 체감하게 하는 여러 가지 사건이 발생한 바 있다. 우리나라는 특히 분단국가로서 비대칭전력으로 활용하고자 하는 북한의 사이버 공격이 현실로 나타나고 있으며 이는 직접적인 피해에 더하여 국가위험(country risk)을 악화시키는 요인으로도 작용하고 있다.

〔표 3〕 보이스 피싱 피해

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

〔표 4〕 해외 전자제어시스템 사이버 공격 피해사례

시기	발생국	피해내역
2003.1	미국	• 오하이오주소재 원자력발전소 네트워크에 슬래머웜 침투 • 안전감시시스템 5시간 정지
2003.8	미국	• 동부지역 철도신호시스템에 소빅-F 웜 감염 • 철도 수시간 운행 중단
2008.1	폴란드	• 14세 소년 TV리모컨 개조 트램교차로 불법조작 • 트램 4대 탈선 및 12명 부상
2009.8	러시아	• 수력발전소의 터빈제어시스템 장애 • 발전기 터빈 폭발 및 75명 사망
2010.7	이란	• 원자력발전소 제어시스템에 스턱스넷 바이러스침투 • 나탄즈 원심분리기의 일부 기능마비
2011.11	미국	• 일리노이주 상수도 시스템 침투 • 펌프 작동시스템 파괴

〔표 5〕 우리나라의 대규모 사이버피해사례

사건	시기	피해규모 (억원)	비고
1.25 대란	2003.1.25	1,600	KISA
7.7 DDoS 공격	2009.7.7	363~544	현대경제연
3.4 DDoS 공격	2011.3.4		청와대 등 40개기관
4.12 NH사태	2011.4.12	수백억원	한국경제
GPS 교란	2012.3.6		항공운항

III. 사이버정보보호의 경제적 효과

사이버정보보호의 경제적 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 정보보호투자의 기회비용이라고도 할 수 있다. 그렇다면 어느 정도의 규모로 어떠한 분야에 어떤 방식으로 정보보호체계를 구축해야하며, 그것은 어느 정도의 투자규모를 요구하는 것일까? 이것은 우리나라와 전 세계의 각국 정부, 공공기관 그리고 민간이 당면한 시급한 과제이다. 정부는 국가적 체계를 수립하고 공공기관 및 민간에 가이드라인을 효과적으로 제시하고 적절한 방법과 자원을 확보하여 필요한 자원을 공급해야 할 것이다.

사이버 정보보호 또는 사이버보안은 네트워크, 컴퓨터, 프로그램과 자료를 공격, 손상 혹은 무단 접속으로부터 보호하도록 고안된 기술, 프로세스와 수행방법을 통칭한다. 사이버보안을 위해서는 정보체계 전반적으로 통합된 노력이 필요하다. 사이버보안의 주요요소로는 컴퓨터응용 보안(application security), 정보 보안(information security), 네트워크 보안(network security), 재난 복구(disaster recovery) 및 업무지속계획(business continuity planning) 그리고 최종사용자 교육 등을 들 수 있다.

사이버보안에서의 어려움은 보안위험이 매우 빠르게 지속적으로 전개된다는 특성에 기인한다. 이전에는 가장 결정적인 문제에만 자원을 집중하고 상대적으로 덜 중요한 요소는 무시하거나 방치하는 경향이 있었으나, 이러한 방식은 지금은 통하지 않는다. 왜냐하면 언제나 예상한 것보다 더 많은 새로운 위험요소들이 지속적으로 등장하고 있기 때문이다.

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

IV. 사이버 정보보호 효과의 합리적 추정방안

4.1. 기존의 추정관련 연구

미국, 영국 등 선진국을 중심으로 사이버피해 규모에 대한 연구가 다수 이루어져 왔다. 영국의 사이버안전정보보장국(OCSIA)과 Detica는 지적자산도용과 산업스파이가 영국경제에 초래하는 비용에 대해 가늠하기 위하여 영국의 사이버범죄비용을 분석하였다. 여기서 '사이버범죄(cyber crime)'의 범위는 '금전적인 이익을 위하여 행하는 불법행위'로 인터넷이나 전자시스템을 사용하여 개인, 기업, 정부가 사용하는 정보와 서비스에 무단 접속하거나 공격하는 행위를 의미한다. 이 연구에서는 이제까지 이해가 부족했던 영국의 개인들에 대한 명의도용과 온라인 사기, 기업에 대한 지적재산침해, 산업스파이 및 강탈(extortion), 정부에 대한 재정적 사기(fiscal fraud)를 포함한 범죄행위에 초점을 맞추었다. 사이버범죄 행위자는 외국의 정보관련 기관, 대규모범죄조직에서 기업, 개인 및 소규모 기회주의자 그룹에 이른다.

Detica report에 의하면 영국의 경우 사이버피해 규모는 최근 년간 270억 파운드(약 48조원)에 이르는 것으로 보고되고 있다. 개인이 입은 피해가 31억 파운드이고 기업과 정부는 각각 22억 파운드, 210억 파운드로 나타났다[3].

미국의 Ponemon연구소는 사이버공격의 경제적 효과를 분석하고 그 추이를 관찰하기 위하여 2011년 미국 내 다국적기업을 포함한 여러 산업분야의 종업원 수 700인 이상인 50개 조직(기관과 기업)을 대표 표본으로 분석하였다. 이 연구보고서(2011)에 따르면 50개 조직에 미치는 사이버범죄의 효과는 매우 심각하여 연간 최저 150만 달러에서 최고 3,650만 달러에 이르는 것으로 나타나고 있다. 중간에 위치한 기업의 피해비용이 590만 달러에 이르는데 이는 전년에 비하여 56% 증가된 규모이다. 이 기업들은 매주 72번의 사이버 공격 피해를 입었고 이는 각 기업이 평균 1회 이상 공격에 의한 손실을 입었다는 의미가 된다. 이는 공격이 성공한 회수도 전년대비 44% 증가한 결과이다. 가장 손실이 큰 사이버 범죄는 악성코드, 서비스 거부, 분실장비와 웹기반 공격에 의하여 초래된 것으로 나타나고 있다[4].

한편 노턴사이버범죄보고서(2011)는 2011년 2월 6일부터 3월 14일까지 StrategyOne이 24개국의 성인 12,704명을 포함한 19,636명을 대상으로 인터뷰를 수행하여 [표 6]과 같은 결과를 보고하고 있다[5].

[표 6] 사이버범죄 추정피해액(백만달러)

	직접비용	시간손실 비용	계
미국	32,000	107,600	139,600
일본	7,900	10,100	18,000
호주	1,800	2,900	4,700
24개국	114,000	274,000	388,000

조사대상 성인의 수는 동일한 대표성을 확보하기 위하여 각국에 500명 기준으로 가중치가 배정되었다. 조사대상 24개국은 호주, 브라질, 캐나다, 중국, 프랑스, 독일, 인도, 이탈리아, 일본, 뉴질랜드, 스페인, 스웨덴, 영국, 미국, 벨기에, 덴마크, 네덜란드, 홍콩, 멕시코, 남아공, 싱가포르, 폴란드, 스위스, 아랍에미레이트연방으로 한국은 포함되지 않았다[6].

이 보고서에서는 주요 사이버범죄유형으로는 컴퓨터바이러스 및 악성코드(54%), 신용카드 등과 관련한 온라인 신용사기(11%), 피싱(10%)이 전체의 3/4을 차지하고 있다. 2010년도의 사이버 범죄의 경제적 비용은 약 1,140억 달러로 추정되었다. 이는 각국별로

'지난 12개월의 피해자 수 × 1인당 평균 사이버 범죄의 경제적 비용'의 산식을 활용하여 계산되었다.

동 기간의 사이버 범죄에 의한 손실시간의 가치는 각국별로 '지난 12개월의 피해자 수 × 1인당 평균 사이버 범죄의 손실시간의 경제적 비용'의 산식으로 계산되었다. 24개국의 피해자 수는 도합 431백만 명으로 나타났는데 이는 노턴의 최근 연구에 따르면 조사대상 24개국의 성인 중 69%가 지금까지 사이버 범죄에 노출되었으며 이중 65%가 지난 12개월간 사이버 범죄의 희생양이 되었다는 것을 전제한다.

또한 CIA Fact Book에 따르면 24개국 각국의 온라인 인구는 도합 8억 287만 명이며 이를 바탕으로 계산하면 2010년의 24개국 피해자 수는 4억 3,150만 명이 된다. 이들의 손실 시간비용은 2,740억 달러로 계산된다. 따라서 사이버 범죄의 시간비용을 포함한 총비용은 1,140 + 2,740 = 3,880억 달러(약 443조원)로 추산된다는 것이다.

유진호 등(2008)은 2005년의 우리나라 인터넷 침해사고 피해액을 매출이익 손실, 생산효율저하 손실, 복구비용, 피해 데이터 재생산비용 등 네 분야로 나누어 산정하여 일본의 IPA에서 산정한 일본의 피해액과 비교하였는데 한일간 GDP의 비율과 피해액의 비율이 유사함을 확인하였다. GDP는 일본이 한국의 6.1배였는데 피해액은 5.3배로 약간 낮았다. 이는 우리의 인터넷 활용율이 GDP에 비하여 높은 데 기인하는 것으로 보인다. 2003년 1월 25일 발생한 슬래머웜에 의한 인터넷 침해사고는 국내뿐 아니라 MS SQL서버 2000 등을 사용하는 국제적인 인터넷망의 접속장애에서 비롯되었다. 이 때 발생한 세계적 손실을 영국의 Mi2g는 9억 5천만~12억 달러, 미국의 CE는 10억 달러로 추산한 바 있다. 한편 KISA는 한국의 피해액을 1,055억~1,675억원으로 추산한 바 있다. 이는 우리나라의 피해액이 전세계 피해액의 12% 정도에 이르는 것으로 GDP비중에 비하여 월등히 높은 것은 피해 서버 기종의 점유율이 상대적으로 높은 데서 비롯된 것으로 보인다[7][8].

4.2. 사이버보호의 경제적 효과 추정 방안

사이버보호의 경제적 효과를 측정하기 위해서는 현존하는 사이버피해와 잠재적인 피해를 구체적으로 파악하여야 한다. 피해액 추정방법은 간접적인 방법과 현장중심의 직접적인 방법으로 나누어 볼 수 있을 것이다.

간접적으로 추정하는 방법으로는 가치추정방법으로 많이 사용되는 사례비교법을 들 수 있다. 각국을 대상으로 기존의 연구들이 분석한 방법을 근거로 국민소득, 산업분야별 생산액 또는 매출액 등을 비교하여 산출하는 방법을 생각할 수 있다. 또 하나는 유진호 등(2008)과 같이 기존 연구 대상국가와 우리나라의 측정대상별 특성을 비교하여 적절한 방법으로 파라메터를 수정하여 추정하는 방법이 있을 것이다.

직접적인 추정방법으로는 비용접근법과 소득접근법을 병용해볼 수 있을 것이다. 이를 위해서는 사이버범죄에 따라 발생하는 비용을 추정하기 위하여 필요한 피해분야별 상세자료를 확보해야 하는데 현재는 정확한 데이터를 얻기 어려운 상황이다. 정확한 자료를 수집하기 위해서는 실제 사이버범죄 사고에 관한 상세내용을 수집하는 체계의 확립이 필수적이다. 자료의 정밀성을 확보하기 위하여 업무담당 고위직원 인터뷰와 현장기반연구가 요구된다. 현장연구를 통하여 정보의 손실, 절도, 기업 활동 방해, 수익손실, 자산, 공장 및 장비의 파괴로 인한 직간접비용과 사이버보호를 위한 투자의 기회비용을 알아내야 한다. 이에 더하여 탐지와 조사, 감염, 회복 및 사후대응에 소요되는 비용도 파악할 필요가 있다.

사이버피해가 발생하는 경우 정보보호의 3대요소인 비밀성(confidentiality), 가용성(availability), 무결성(integrity) 중 어떤 것의 상실에서 손실이 발생하게 된다. Gorden & Loeb(2006)은 정보보호 침해사고를 비용/편익분석 방법을 통하여 연구하였고

〔표 7〕 사이버범죄 피해액 및 경제적 효과 추정방법

	활용특성
사례비교법	• 국민소득, 산업분야별 생산액, 매출액, 산업별 공격빈도 등을 비교하여 피해액 산출 가능 • 해외 기존연구의 응용 가능 • 추정비용이 적음 • 사이버범죄 피해액과 경제적 효과추정에 활용 가능
비용접근법	• 피해액 산정을 위하여 상세하고 포괄적인 자료수집 필요 • 비용이 많이 소요 • 피해액 산정에 유용
수익접근법	• 피해방지를 위하여 수행한 투자의 연차별 효과, 할인율의 산정을 바탕으로 경제적 효과의 현재가치 산정 • 피해액 산정 보다는 피해방지를 위한 투자효과 산정에 유용

비용을 직접비용과 간접비용, 명시적 비용과 잠재적 비용의 네 가지로 구분하여 피해액을 분석하였다. 이들의 분석을 따르면 피해액은 〔표 8〕과 같은 구조를 갖고 있고 이를 바탕으로 피해액을 산정할 수 있다. 즉 명시적인 직접비용은 매출이익의 감소, 생산효율의 저하 등의 기대이익 감소부분과 복구비용, 복구불능자산의 가치 등의 추가발생 비용으로 구성되며 이들이 각각 합산된다. 명시적인 간접비용은 사고예방을 위한 투자액으로 볼 수 있다. 한편 잠재적 직접비용은 현재 발생하지는 않았으나 발생할 가능성이 있는 보상책임 관련 비용을 들 수 있으며 잠재적 간접비용은 피해방지를 못하여 발생하는 이미지 손상과 그에 따른 기업가치 또는 주가의 하락을 들 수 있다. 여기서 매출이익의 감소, 생산효율의 저하 등은 미래가치의 현가화를 통한 일종의 수익접근법적 분석을 하게 될 것이다. 웜바이러스 공격에 의한 피해액 측정을 위해 Weaver & Paxson(2004)는 피해를 생산성 손실, 복구시간, 데이터 손실, 시스템 손상 등 네 가지 요소로 구분하고 피해액을 산정하였다〔9〕〔10〕.

〔표 8〕 사이버피해액의 구조

		명시적 비용		잠재적 비용
직접비용	기대이익 감소	매출이익 감소액	생산효율저하손실	잠재적 책임 비용
	추가비용 발생	복구비용	복구불능정보자산가치	
간접비용		예방 투자액		이미지손상 주가하락

본 연구에서는 데이터 수집상의 현실적인 제약을 인정하고 미국이 사이버보안법(Cybersecurity Act)이나 사이버정보공유 및 보호법(CISPA)의 제정 등과 관련하여 주요 근거로 자주 언급하고 있는 노턴사 이버범죄보고서(2011)의 계산방식을 원용하여 우리나라 사이버범죄의 경제적 피해를 추정해보고자 한다. 그런데 아쉽게도 우리나라의 경우는 노턴 보고서에 포함되어 있지 않고 또한 각국의 개별적 데이터도 제공되지 않고 있으므로, 우선 24개국의 경제규모와 우리나라의 경제규모를 비교하고 인터넷 사용자수를 비교하여 우리나라 사이버범죄의 경제적 피해를 시험적으로 계산해보고자 한다.

여기서 사이버범죄의 피해액은 국내총생산액(GDP)과 인터넷사용자수에 비례한다고 가정한다. 각국의 사이버 범죄 피해양상은 얼마간 다를 수밖에 없으나 충분한 데이터가 확보되지 않은 상황에서 경제규모와 사이버범죄의 피해 사이에는 정비례관계가 존재한다고 가정하여도 큰 무리가 없을 것으로 판단된다. 그리고 인터넷사용자수도 사이버 범죄피해건수 또는 피해액과 비례한다고 가정하여도 무방할 것으로 보인다.

〔표 9〕 24개국의 GDP와 인터넷사용자수

GDP (10억달러, 2010년)		인터넷사용자수 (천명, 2009년)	
한국	24개국	한국	24개국
1,014	49,340	39,400	1,247,591

〔표 10〕 사이버 범죄 피해액 추정(억달러)

	GDP 기준 추정 피해액 (2010년)		인터넷사용자수 기준 추정 피해액 (2009년)	
	한국	24개국	한국	24개국
직접피해	23.4	1,140	36.0	1,140
시간피해	56.3	2,740	86.5	2,740
합계	79.7	3,880	122.5	3,880

〔표 9〕와 같이 2010년 기준으로 조사대상 24개국의 GDP는 49조 3,400억 달러이고 우리나라의 GDP는 1조 140억 달러이다. 우리나라의 GDP는 조사대상 24개국의 2.06%이다. 한편 인터넷 사용자수는 우리나라가 3, 940만 명으로 조사대상 24개국의 12억 4,759만명에 비하여 3.16%에 이른다. 우리나라의 초고속 인터넷 보급수준이 세계적으로 최고수준에 이르고 있어 인터넷사용자수는 소득에 대비하여 24개국 평균보다 1.54배에 달하고 있다. 따라서 사이버 범죄의 피해 추정액도 인터넷사용자수를 기준으로 할 때 소득을 기준으로 계산한 수치와 비교하면 같은 비율로 크게 나타나게 된다. 우리나라의 인터넷의존도가 높으므로 사이버 범죄의 피해액도 경제규모로만 비교 추정한 경우보다는 클 것으로 판단되나 인터넷 사용자수로 비교한 것 보다는 어느 정도 낮은 수준에 있을 것으로 예측하는 것이 합리적일 것이다. 국내총생산액은 세계은행(World Bank)의 2010년 경상가격 기준을 사용하였으며 인터넷사용자수는 미국 중앙정보국(CIA)의 World Fact Book(2009년 기준)을 따랐는데 이는 최신의 수치이다. 따라서 노턴보고서의 추정치를 기준으로 비교해본다면 〔표 10〕과 같이 우리나라의 사이버 범죄 피해액은 년간 80억 달러에서

122억 달러 사이에 있다고 볼 수 있을 것이다. 이는 우리 원화로 환산한다면 9조 원에서 13조원 사이가 될 것이다[11] .

그런데 노턴보고서(2011)의 분석은 현재 일어나고 있는 피해를 대상으로 추정한 것이다. 따라서 피해의 가능성이 상존하고 있는 전력, 통신, 교통, 금융 등 국가기간망에 대한 공격에 따른 잠재적인 위험과 관련한 비용은 충분히 감안되지 않은 것으로 볼 수 있다. 이러한 분야의 잠재적 위험에 대한 기회비용을 포함하여 추산한다면 경제적 비용규모는 크게 증가할 것이며 따라서 사이버정보보호의 경제적 가치도 더욱 커질 수밖에 없다.

〔표 11〕 한국과 영국의 GDP 및 인터넷사용자수

GDP (10억달러, 2010년)		인터넷사용자수 (천명, 2009년)	
한국	영국	한국	영국
1,014	2,262	39,400	51,444

〔표 12〕 한국과 영국의 사이버 범죄 추정 피해액

	GDP기준 추정 피해액 (2010년)		인터넷사용자수 기준 추정 피해액 (2009년)	
	한국	영국	한국	영국
피해액	22조원	48조원	37조원	48조원

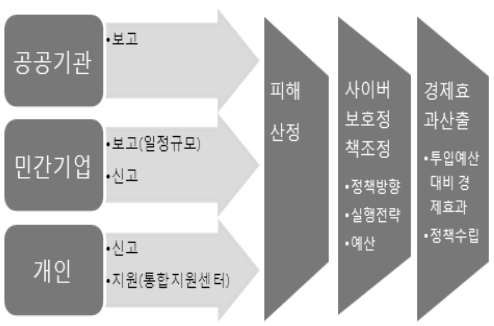
앞에서 살펴본 영국의 사이버피해규모를 바탕으로 〔표 11〕과 같이 국민소득과 인터넷이용자수를 기준으로 비교분석해보는 것도 의미가 있을 것이다. 우리나라의 사이버범죄피해규모를 Detica보고서의 수치를 기반으로 어림잡아 비교 산출하면 〔표 12〕와 같이 22조와 37조 사이 어딘가에 위치할 것으로 볼 수 있다. 이는 노턴보고서를 기준으로 계산한 것보다 2배가 넘는 수치이다. 이와 같이 차이를 보이는 것은 영국의 Detica 보고서의 경우 정부부문의 비중이 큰 것처럼 주로 산출범위의 차이에서 기인하는 것이다. 따라서 우리나라의 사이버범죄에 의한 잠재적 피해액은 산정기준에 따라 큰 폭의 차이를 보이지만 대략 10조에서 40조원 정도의 범위에 있다고 추정해 볼 수 있을 것이다.

사이버보안사고의 피해규모는 사고를 당하기까지는 잘 알 수 없으므로 사이버정보보호의 편익도 간과하기 쉽다. 그러나 정보보호정책의 수립을 위해서는 잠재적인 피해를 포함하여 피해가능영역과 피해규모를 사전에 파악하고 대비하여야하며 정보보호를 위한 투자전략도 수립해야 한다.

향후 정밀한 추정을 위해서는 우리나라 자체의 기초 데이터를 체계적으로 수집하고 그것을 바탕으로 실제 피해액과 잠재적 피해액을 정확하게 산정하는 모델을 수립해야 한다. 우리나라에서도 국가사이버안전관리규정에 의하여 중앙행정기관, 지방자치단체 및 공공기관은 소관 정보통신망에 대한 사이버공격정보를 수집, 분석 및 대응할 수 있는 자체 보안관제센터를 운영하도록 하고 있다. 또한 정보통신기반보호법에 의하여 공공기관의 장은 사이버공격정보를 수집할 경우 피해유무를 파악하고 공격 IP차단, 로그자료 보존 등 조치를 신속하게 취하도록 하고 있다[12][13].

공공기관의 피해산정은 이들 기관이 파악한 사이버공격관련 피해정보를 피해산정기관에 보고하도록 하면 공공부문의 피해규모를 산정하는데 문제가 없을 것이다. 그런데 민간의 경우는 관련 정보의 수집체계가 체계적으로 마련되어야 할 것으로 보인다. 일정규모 이상의 기업의 경우에는 제도적으로 보고하도록 의무를 부과하고 소규모 기업 또는 개인의 경우 일정한 패널을 구축하여 정기적으로 피해규모를 추계할 필요가 있다. 피해액을 산정한 후 그 피해를 방지하기 위한 대책이 마련되고 추진될 경우 얻을 수 있는 경제적 편익을 추정하기 위한 모델이 마련될 수 있을 것이다.

민간기업과 개인들의 신고접수 및 피해규모 파악과 피해최소화 및 복구를 지원하기 위한 '사이버피해 통합지원센터(통합지원센터)'의 설치가 필요하다. 물론 소관분야별 신고접수와 지원도 필요하나 신속한 대응을 위한 원스톱서비스체제의 구축을 통하여 민간기업과 개인이 신속히 대응할 수 있도록 지원하고 통합지원센터가 관련기관을 연계하여 피해를 최소화하는 체계의 구축이 필요하다. 사이버피해액 산정과 경제효과



〔그림 1〕 사이버보호 경제효과 분석모델

의 산출은 KISA 등 기존의 기관에서 법령의 규정을 통하여 수행하여도 무방할 것으로 보인다. 그런데 사이버보호정책을 총괄하는 기구의 구성과 역할은 심도 있는 논의를 진행하되 신속하게 구축하는 것이 필요하며 잠재적 피해를 사전에 예방하기 위하여 관련 예산 규모도 현실화하여야 할 것이다.

V. 결 론

우리나라의 사이버피해의 잠재적 규모는 대략 10조원 이상이 될 것으로 보인다. 그런데 사이버 시스템에 대한 공격의 형태는 날로 새로워지고 있으며 그 피해 가능성 및 피해규모도 급속히 증가할 것으로 보인다. 특히 분단국가인 우리나라는 북한이 사이버전력의 활용을 현실화하는 상황에서 그 위험성이 더욱 크다 할 것이다 따라서 정보보호를 위한 대비는 항상 즉각적으로 이루어져야 하며 이를 위한 체계의 확립과 예산의 확보는 국가자원을 배분하는 데 있어 국가정책의 최우선적 과제라 할 것이다. 사이버보안을 위해서는 사이버 시스템의 주요 요소만 보호하면 되는 것이 아니라 사이버시스템 체계를 보호해야 한다. 따라서 그에 필요한 자원을 적절하게 배분하는 것이 필요하다 할 것이다. 사이버정보보호의 구체적인 편익은 사태가 발생한 후에야 그 크기를 알 수 있다. 그러나 당하고 나면 너무 늦은 것이니 사전에 대책을 마련하는 것이 무엇보다 절실하다 할 것이다. 이번 연구를 바탕으로 향후 사이버보안의 경제적 효과와 적절한 자원배분에 관한 연구가 치밀하게 진행되어야 할 것으로 사료된다.

참고문헌

〔1〕 정보보안대책추진회의결정(情報セキュリティ對策推進會議決定), 情報セキュリティポリシーに關するガイドライン, 2000.

〔2〕 2012 국가정보보호백서, 방송통신위원회·행정안전부·지식경제부, 2012년 5월.

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

〔4〕 Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies, Ponemon Institute© Research Report, August 2011

〔5〕 Norton Cybercrime Report 2011, http://www.symantec.com

〔6〕 http://data.worldbank.org/indicator/NY.GDP.MKTP.CD, World Bank,

〔7〕 정보보호의 경제적 분석 연구 동향, 정보보호 이슈보고서 2008-8호, 한국정보보호진흥원, 2008년 10월.

〔8〕 유진호, 지상호, 송혜인, 정경호, 임종인, 인터넷 침해사고에 의한 피해손실 측정, 정보화정책 제15권 제1호, pp. 3-18, 2008년 봄.

〔9〕 Lawrence A. Gorden and Martin P. Loeb, Managing Cybersecurity Resources: A Cost-Benefit Analysis, McGraw-Hill, 2006.

〔10〕 Weaver N. and Paxson, V. , ″A Worst-Case Worm,″ Third Annual Workshop on Economics and Information Security, May 2004.

〔11〕 World Fact Book 2011, CIA

〔12〕 국가정보원, “국가사이버안전관리규정,” 대통령훈령 제291호, 2012.1..2, 일부개정

〔13〕 행정안전부, “정보통신기반보호법,” 법률 제9708호, 2009.8.23 시행

〈著者紹介〉

신 진 (Jin Shin) 종신회원
1983년 2월: 서울대학교 사회과학대학 무역학과 졸업
1989년 4월: Florida State University 대학원 경제학과(경제학석사)
1991년 4월: Florida State University 대학원 경제학과(경제학박사)
2008년~2011년: 호서대학교 벤처전문대학원 교수
2012년~현재: 단국대학교 교수
2012년~현재: 한국산업기술평가관리원 이사
〈관심분야〉 정보통신정책, 과학기술정책, 산업정책