DOI: 10.3745/KIPSTC.2008.15-C.3.191

인터넷 침해사고로 인한 기업의 경제적인 피해 산출 모델 및 케이스 연구

장 종 호[†] · 정 기 현[††] · 최 경 희[†††]

요 약

최근 우리 사회는 인터넷과 네트워크의 발전에 따라 자유롭게 정보를 공유하거나 습득하게 되었다. 그러나 인터넷의 발전으로 인해서 그에 대한 역기능도 나타나게 되었다. 대표적인 역기능이 바로 인터넷 공격이다. 인터넷 공격은 여러 분야에서 많은 피해를 주는데, 특히 경제적인 측면에서의 그 피해는 어마어마하다. 특히 기업의 경우는 이런 경제적인 피해에 민감하다. 그러나 국내에서는 이런 인터넷 공격으로 인한 경제적인 피해를 산정하는 모델에 관한 연구가 미비하다. 따라서 본 논문에서는 인터넷 공격으로 인한 경제적인 측면의 피해를 산출하는 하나의 모델을 제시하고 그 모델의 기준에 따라 가상적인 인터넷 공격의 경제적인 피해를 산정할 것이다.

키워드 : 인터넷 웜, 인터넷 공격, 인터넷 보안, 경제적인 피해

Economic Damage Model on Industries due to Internet Attack and A Case Study

Jong-Ho Jang[†] · Ki-Hyun Chung[††] · Kyung-Hee Choi[†††]

ABSTRACT

Because of the internet development, most of people can acquire the information freely. But it have the disadvantages. A remarkable thing among the disadvantages is the internet attack. Internet attacks were given damages to several fields. Specially, the damage is terrible to the economic side. Specially, company is susceptive to economic damage side. But it didn't execute a research about model that estimates damage to the economic side due to internet attacks. This paper presents a model that estimates the damage to economic side due to internet attacks.

Key Words : Internet Worm, Internet Attack, Internet Security, Economic Damage

1. 서 론

인터넷은 정보가 시간과 공간을 넘어 실시간으로 전달되는 것을 가능하게 해 준다. 이런 인터넷과 네트워크 환경의 발달로 인해서 모든 업무 처리 및 일상 생활이 더욱 편리해졌다. 그러나 네트워크가 발전함에 따라 이에 대한 부정적인 면도 나타나고 있는데 가장 대표적인 것으로 인터넷 침해사고를 꼽을 수 있다. 이런 침해사고는 인터넷 웜 및 분산 서비스 거부 공격(DDoS) 등 여러 가지 형태로 나타나고 있다[3]. 이 중 분산 서비스 거부 공격(DDoS)은 인터넷상에서 다수의 시스템이 협력하여 하나의 표적 시스템을 공격함으로써 시스템을 마비시키는 공격을 말한다. 그리고 인터넷 웜은 자기 복제 능력을 가진 것으로써 자동으로 취약성이 있는 시스템을 찾아서 공격하는 메커니즘을 가지고 있는 악성 코드의 일종이다[4]. 인터넷 웜은 1990년대 초반 Moris 웜이 출현한 이후 다양한 종류의 웜이 지속적으로 나타나고 있었지만 그 피해가 적어 잘 알려지지 않고 있었다.

인터넷은 누구든지 정보의 위치와 관계없이 어디에서나 정보를 얻을 수 있다는 점 때문에 이에 대한 여러 가지 공격이 더욱 파괴적이며 광범위하다. 이런 공격들은 네트워크를 사용하는 사용자들에게 악영향을 끼칠 뿐만 아니라 그 피해 또한 측정할 수 없을 만큼 엄청나다. 이러한 부정적인 면에 대처하기 위해서 방화벽이나 침입 탐지 시스템(IDS) 등과 같은 많은 연구가 이루어지고 있다. 특히 경제적인 이익을 목적으로 하는 기업들이 이런 인터넷 보안에 많은 관심을 가지고 있다.

그러나 인터넷 침해사고는 워낙 광범위하고 다양한 분야로 전파되기 때문에 이로 인한 피해를 사전에 100% 예방하

※ 본 연구는 사이버기술연구소 학술연구사업의 연구 결과로 수행되었음.
† 준 회 원 : 아주대학교 전자공학과 석사
†† 정 회 원 : 아주대학교 전자공학부 교수
††† 정 회 원 : 아주대학교 정보통신전문대학원 교수
논문접수 : 2006년 12월 13일, 심사완료 : 2007년 2월 1일

<표 1> 인터넷 공격으로 인한 경제적인 피해 통계[5]

인터넷 침해사고의 경제적인 영향(2000-2005)	
2006	133억불
2005	142억불
2004	175억불
2003	130억불
2002	111억불
2001	132억불
2000	171억불

는 것은 어렵다. 따라서 침해사고가 발생했을 때 실질적인 피해액을 산출하는 방법에 대한 연구가 필요하다. 이런 결과는 기업체로 하여금 인터넷 침해사고에 대한 예비 방어 비용과 피해액 그리고 사고 처리시 발생되는 처리 비용에 대한 비교, 검토를 가능하게 할 것이다.

컴퓨터 이코노믹스가 전세계의 약 150여 개의 대형 IT 보안 기구들과의 인터뷰를 기준으로 매년 발표하여 많은 기관들이 인터넷 바이러스나 해킹 방지의 계획으로 삼고 있는 통계에 따르면, 인터넷의 발달과 웜 등의 인터넷 보안을 위하는 코드들로 인한 피해가 매우 커다. <표 1>에서는 컴퓨터 이코노믹스가 발표한 최근 통계를 담고 있다. 이 통계값들은 인터넷으로 감염된 시스템의 분석, 수리 및 복원에 필요한 인건비, 감염된 동안 시스템 성능 저하에 따른 손실 그리고 하드웨어 및 소프트웨어 피해에 따른 직접적인 손실 등을 포함 하고 있다.

많은 선진국에서는 이런 피해에 대한 연구를 다각도에서 수행하고 있으나 아직까지 국내에서는 이런 인터넷 침해사고에 대한 피해액을 산출하는 연구에 대해서 소극적이다. 이는 인터넷 침해사고에 의한 피해액을 외부에 공개하는 것을 기업들이 꺼려하고 있기 때문이다. 그러나 이 피해 연구는 아주 중요한 의미를 지니고 있다. 인터넷 침해사고에 의한 피해는 소프트웨어에도 심각한 영향을 끼치므로 피해액을 수치화 시킨다는 것은 쉬운 일이 아니다. 그러나 피해액의 수치화는 각 피해를 비교 분석할 수 있는 도구로서 의미를 가질 뿐 아니라 피해에 대한 대응책을 마련하는 기준을 제시한다는 점에서도 중요한 의미를 가지고 있다.

인터넷 침해사고에 의한 경제적인 피해를 산출하는 방법이 크게 두 가지의 모델로 연구되고 있다. 첫 번째는 선형적인 모델로 경제적인 피해를 산출하는 모델인데, 이 모델에서는 인터넷 침해사고로 인한 전체적인 피해(D_{total})는 피해를 입은 시스템의 평균 피해액 (D_{system})과 피해를 입은 시스템의 수($N_{\inf}$)의 곱($D_{total} = N_{\inf} \times D_{system}$)으로 계산하고 있다[1]. 이 모델은 인터넷 침해사고에 의한 직접적인 피해만 산출할 뿐 간접적인 피해를 산출하는 방법을 제시하지 못하는 단점을 지니고 있다.

두 번째 모델은 인터넷 침해사고에 의해서 기업들이 입은 경제적인 피해를 산출하기 위한 모델이다. 이 모델은 직접적인 피해뿐만 아니라 간접적인 피해까지 포함한다[2]. 또한 이 모델은 경제적인 피해를 시간의 관점에서도 파악했다. 다시 말해 모두 같은 시간에 똑같이 발생하는 것이 아니고 시간에 따라 다르게 혹은 시간이 지남에 따라 점점 증가하는 식으로 피해가 발생한다는 것이다. 이는 직접적인 피해보다는 간접적인 피해와 밀접한 연관을 가지고 있다. 간접적인 피해의 경우는 시간이 지날수록 그 피해 소비자 및 피해 금액이 증가하기 때문에 시간이 지날수록 그 피해액도 증가한다. 그러나 이 모델은 인터넷 침해사고로 인해서 일반적으로 기업이 입은 경제적인 피해를 산출하기에는 적합한 방법이나 네트워크의 피해 정도나 소비자 피해 정도 같은 인자를 전혀 고려하지 않고 피해액을 산출했기 때문에 계산된 피해액이 정확한 값보다 훨씬 크게 산출된다는 단점을 지니고 있다. 본 논문에서는 위 두 가지 모델의 단점을 보완한 하나의 모델을 제시할 것이다.

본 논문의 3장에서는 인터넷 침해사고로 인한 경제적인 피해를 산출하는 모델을 제시할 것이다. 그리고 4장에서는 제시한 모델을 기초로 하여 실제 기업이 입은 경제적인 피해 예상액을 산출하고 5장에서는 결론을 기술한다.

2. 경제적인 피해 산출 모델

이번 장에서는 인터넷 침해사고로 인한 경제적인 피해를 산출하는 새로운 모델을 제시할 것이다. 제시될 피해 산출 모델은 여러 분야에서 활용 가능한 피해 모델로써 특히 기업의 경제적인 피해를 산출하는데 적합한 산출 모델이다. 이 피해 산출 모델에서 전체적인 피해는 직접적인 피해(D_{dam})와 간접적인 피해(IND_{dam})의 합($D_{total} = D_{dam} + IND_{dam}$)으로 나타낼 수 있다. 직접적인 피해는 인터넷 침해사고로 인해서 발생하는 물질적인 피해를 말하고 간접적인 피해는 그 외의 모든 피해를 지칭하는 것이다.

2.1 직접적인 피해모델

인터넷 침해사고로 인한 경제적인 피해 산출 모델에서 직접적인 피해는 기업이 입은 물질적인 피해를 말한다. 이는 공격으로 인한 피해를 복구하기 위한 비용 및 시간 등이 있으며, 시스템 복구비용(D_{system}), 생산성 손실비용(D_{pro}), 매출 손실비용(D_{rev})의 합으로 나타낼 수 있다.

$$D_{dam} = D_{system} + D_{pro} + D_{rev}$$

2.1.1 시스템 복구비용

시스템 복구비용(D_{system})은 인터넷 침해사고로 인해서 피해를 입은 시스템을 사고 이전의 상태로 되돌리는데 소요되는 총 비용을 말한다. 이는 하나의 시스템의 피해 복구비용과 피해 시스템의 수($N_{\inf}$)에 의해서 결정된다. 여기서 시스템의 피해는 크게 하드웨어와 소프트웨어로 구분된다. 이 중 하드웨어 복구비용($M_c = P_{hw} \times C_{hw}$)은 침해사고로 인해서

하드웨어가 손상되었을 경우 이를 수리하거나 교체하는데 소용되는 물리적인 비용으로 하드웨어 손상률(P_{hw})과 하드웨어 평균 교체 비용(C_{hw})으로 구할 수 있다.

반면에 소프트웨어 복구비용(D_{sw})은 침해사고로 피해를 입은 시스템내의 자료를 복구하는데 사용되는 총 비용을 말한다. 피해 자료는 복구가 가능한 자료와 불가능한 자료로 구분되는데 복구가 가능한 자료의 복구비용보다 불가능한 자료의 복구비용이 훨씬 더 크다. 이는 자료의 복구가 불가능한 경우 피해 복구비용은 공격 시에 잃게 되는 자산의 가치를 의미하기 때문이다. 복구가 가능한 피해 자료의 경우는 자료 복구비용을 적용하며, 복구가 불가능한 피해 자료는 파괴된 자료에 대한 재생산 비용을 적용한다. 이 소프트웨어 복구비용은 다음의 식과 같이 나타낼 수 있다. P_{idata}는 복구 불가능한 데이터의 비율, D_{data}는 복구 가능한 데이터의 복구 비용이며, D_{idata}는 복구 불가능한 데이터의 재생산 비용이다.

$$D_{sw} = (1 - P_{idata}) \times D_{data} + P_{idata} \times D_{idata}$$

시스템 복구비용은 위의 2가지의 피해액 외에도 시스템을 복구하는 관리자의 관리비용도 포함되는데 이는 복구시간(d_r)과 복구 관리자의 생산성(E_{ad})의 곱으로 나타낼 수 있다. 따라서 시스템의 복구 비용은 아래와 같이 나타낼 수 있다.

$$D_{system} = \{M_c + D_{sw} + (d_r \times E_{ad})\} \times N_{\inf}$$

2.1.2 생산성 손실비용

생산성 손실비용(D_{pro})는 인터넷 침해사고를 당함으로써 그 공격 및 복구시간 동안 기업이 생산활동을 하지 못함으로 인해서 발생하는 손실을 말한다. 이는 노동 가치와 시스템 불능시간 그리고 네트워크 손실률에 의존한다. 여기서 노동 가치(D_{time})는 근로자 1인당 시간 생산성을 의미하는데 이는 근로자의 생산성(E_{ca})과 1인당 년간 근로 시간(d_a)으로 구할 수 있다.

그리고 시스템 불능시간(d_o)은 인터넷 침해사고의 공격시간과 시스템 복구시간의 합으로 계산된다. 그리고 네트워크 손실률(P_{net})은 피해 기업의 전체 시스템 중 피해를 입은 시스템의 비율을 말한다. 이 네트워크 손실률이 얼마인가에 따라서 그 손실액이 달라지고 간접적인 피해에도 영향을 미치게 된다. 위의 인자들을 고려한 생산성 손실액의 전체 식은 다음과 같다.

$$D_{pro} = d_o \times D_{time} \times E_{no} \times P_{net}$$

2.1.3 매출 손실비용

매출 손실비용(D_{rev})는 인터넷 침해사고를 당함으로써 기업의 시스템이 제대로 동작을 하지 못하기 때문에 이로 인한 서비스 불능시간 동안 발생하는 기업의 매출 손실액을 말한다. 이는 서비스 불능시간(ds_o)과 시간당 기업의 매출액($\frac{R_a}{ds_a}$) 그리고 침해사고 영향도($P_{\inf}$)에 따라서 그 손실액이 달라진다. 여기서 시간당 기업의 매출액은 전체 매출액(R_a)과 기업의 서비스 시간(ds_a)으로 구할 수 있다. 매출 손실액의 전체 식은 다음과 같다.

$$D_{rev} = ds_o \times \frac{R_a}{ds_a} \times P_{\inf}$$

위의 식에서 침해사고 영향도는 사용불능으로 인해서 영향을 입은 매출의 확률을 말한다.

2.2 간접적인 피해모델

인터넷 침해사고로 인한 경제적인 피해 산출 모델에서 간접적인 피해는 앞서 설명한 직접적인 피해를 제외한 모든 피해를 말한다. 이 간접적인 피해는 시간의존적이고 특히 기업과 밀접한 관련이 있으나 각 기업이나 산업군마다 정확한 피해 보상 자료를 공개하고 있지 않기 때문에 이 피해를 정확하게 산출하는 일은 어려운 일이다. 식은 다음과 같다.

$$IND_{dam} = D_{lia} + D_{customer}$$

2.2.1 피해 배상 비용

기업들은 자사의 서비스를 이용하는 소비자들과 계약을 하는데 이 때 기업이 불안정한 서비스를 제공하거나 혹은 다른 이유로 소비자들에게 피해를 줄 경우 위약금을 지불하도록 하고 있다[6][16][17]. 피해 배상 비용(D_{lia})은 소비자들에 대한 이런 계약상의 위약금(C_c) 지불에 대한 손실액을 말한다. 특히 인터넷 의존도가 큰 기업일 경우 이에 대한 손실액도 크다. 또한 서비스 불능시간(d_o)과 피해 소비자의 수(N_{cus})에 따라서 이 손실액은 큰 차이를 보인다. 식은 다음과 같다.

$$D_{lia} = N_{cus} \times C_c \times d_o \times P_{claim}$$

위의 식에서 P_{claim}는 피해 비율을 의미하는데 이는 전체 소비자와 피해를 입은 소비자의 비로 구할 수 있다.

2.2.2 소비자 기회비용

소비자 기회비용($D_{customer}$)은 침해사고로 인한 피해 때문

〈표 2〉 인터넷 공격 피해 비용 모델 식 정리

피해 비용				식
총피해액				$D_{total} = D_{dam} + IND_{dam}$
	직접비용(D_{dam})			$D_{dam} = D_{system} + D_{pro} + D_{rev}$
		시스템 복구비용(D_{system})		$D_{system} = \{M_c + D_{sw} + (d_r \times E_{ad})\} \times N_{\inf}$
			하드웨어 복구비용(M_c)	$M_c = P_{hw} \times C_{hw}$
			소프트웨어 복구비용(D_{sw})	$D_{sw} = (1 - P_{idata}) \times D_{data} + P_{idata} \times D_{idata}$
			시스템 복구 관리비용	$(d_r \times E_{ad})\} \times N_{\inf}$
		생산성 손실 비용 (D_{pro})		$D_{pro} = d_o \times D_{time} \times E_{no} \times P_{net}$
		매출 손실 비용		$D_{rev} = ds_o \times \frac{R_a}{ds_a} \times P_{\inf}$
	간접비용(IND_{dam})			$IND_{dam} = D_{lia} + D_{customer}$
		피해배상비용(D_{lia})		$D_{lia} = N_{cus} \times C_c \times d_o \times P_{claim}$
		소비자기회비용($D_{customer}$)		$D_{customer} = \{C_A + C_P\} \times R_C$

〈표 3〉 식에서 사용한 변수들

변수	의 미	변수	의 미
D_{total}	경제적인 총 피해.	E_{no}	피해 기업의 임직원 수.
D_{system}	시스템 복구 총 비용.	E_{ca}	직원 1인당 생산성.
D_{pro}	생산성 손실 비용.	d_a	직원 1인당 근무 시간.
D_{rev}	기업의 매출 손실.	d_o	근무 불능 시간.
D_{lia}	소비자 피해 배상 비용.	P_{net}	피해 기업의 네트워크의 손실률.
$D_{customer}$	소비자 기회 비용.	ds_o	서비스 불능 시간.
D_{sw}	소프트웨어 복구 비용.	R_a	기업의 전체 매출.
M_c	하드웨어 복구 비용.	ds_a	기업의 서비스 시간.
d_r	시스템 복구 시간.	$P_{\inf}$	침해사고 영향도.
E_{ad}	시스템 복구 관리자 급여.	N_{cus}	서비스 가입 소비자 수.
$N_{\inf}$	피해 시스템 수	C_c	소비자 1인당 피해 보상금.
P_{idata}	복구 불가능한 자료 비율	P_{claim}	소비자 피해 비율.
D_{data}	복구 가능한 자료 비용.	C_A	실제 계약 해지 소비자 수.
D_{idata}	복구 불가능한 자료 비용.	C_P	계약 보류 소비자 수.
P_{hw}	하드웨어 손실률.	R_C	소비자 평균 매출액.
C_{hw}	하드웨어 복구비용.		

에 기업의 신뢰도가 떨어져서 소비자들이 실제 계약을 해지한 경우(C_A)와 계약을 하려고 했던 잠재적인 소비자(C_P)들이 계약을 포기한 경우의 기회비용으로 산출할 수 있다. 이는 시간이 지남에 따라 그 수가 증가하기 때문에 이 손실액은 시간이 지남에 따라 증가한다. 식은 다음과 같다. R_C는 소비자당 시간에 따른 평균 매출액을 의미한다.

$$D_{customer} = \{C_A(\Delta t) + C_P(\Delta t)\} \times R_C(\Delta t)$$

앞에서 언급한 직접 및 간접 피해액을 다시 정리하면 <표 2>과 같다. <표 3>에는 식에서 사용한 변수들을 정리하고 있다.

3. 인터넷 침해사고로 인한 경제적인 피해 산출

이번 장에서는 3장에서 제시한 모델에 기초하여 가상적인 인터넷 공격의 상황에서의 그 피해액을 산출할 것이다. 여러 종류의 서비스를 제공하는 기업들이 있지만 본 논문에서는 인터넷과 가장 관련이 깊은 ISP에 대한 경제적인 피해를 산출할 것이다.

3.1 직접적인 피해액 산출

3.1.1 시스템 복구비용 산출

시스템 복구비용에는 하드웨어 복구비용과 소프트웨어 복구비용 그리고 복구관리자 비용이 포함된다. 이 중 하드웨어 복구 비용은 하드웨어 손상율과 하드웨어 평균 복구비용으로 구할 수 있다. 인터넷 공격의 유형 중에는 하드웨어만 중점적으로 손상을 주는 공격이 있는데 이런 유형의 공격은 전체 인터넷 공격의 유형 중에서 극히 일부분에 지나지 않기 때문에 본 논문에서는 하드웨어 손상율을 0.1로 가정해서 사용했다. 그리고 하드웨어 평균 복구비용은 2005년 8월의 PC 부품별 소매시장 가격의 자료를 토대로 하드웨어의 주요소인 메모리, CPU, 메인보드 등의 평균값을 계산하여 40만원으로 책정했다[7].

소프트웨어 복구비용은 복구 가능한 자료와 불가능한 자료의 복구비용으로 나눌 수 있다. 이때 복구 가능 및 불가능한 비율은 국내 자료 복구업체 중 하나인 ㈜명정보기술의 자료 복구율을 토대로 구했다. ㈜명정보기술의 자료 복구율을 살펴보면 소프트웨어 복구율이 77.73%이다[8]. 이를 바탕으로 복구 가능 비율을 0.78로 정했고 불가능한 비율을 0.22로 정했다.

또한 국내 자료 복구업체들의 평균 자료 복구비용을 나타낸 <표 4>를 보면 알 수 있듯이 복구 가능한 자료의 복구비용은 평균 15만원인데 반해서 불가능한 자료의 복구비용은 David. M. Smith가 작성한 보고서인 “The Cost of Lost Data”의 내용을 참조해서 약 2000만원으로 책정했다 [9]. 또한 복구관리자 비용은 복구관리자의 생산성과 복구시간으로 구할 수 있다. 이 중 복구시간은 인터넷 공격에 대한 패치 프로그램을 개발하는 시간을 8시간으로 그리고 시스템을 복구하는 시간을 8시간으로 가정해서 총 복구시간을 16시간으로 선택했다. 그리고 복구관리자의 생산성은 노동부가 통계를 낸 국내 정보통신업계 근로자의 평균 연봉을 바탕으로 계산했다[10]. 그리고 피해를 입은 시스템의 수는 네트워크 손실률을 참고로 해서 산출했다.

〈표 4〉 자료 복구 업체들의 평균 자료 복구비용

자료 복구 업체	Win98/ME/NT/2000/XP
자료 맥	15만원
자료 올	15만원
㈜명 정보기술	15만원
㈜자료 복구 센터	15만원
제이네	15만원

3.1.2 생산성 손실비용 산출

생산성 손실비용에는 기업의 시간당 생산성과 근무 불능시간 그리고 네트워크 손실률이 포함된다. 기업의 시간당 생산성은 각 기업의 근로자 1인당 시간당 생산성과 전 임직원수의 곱으로 구할 수 있다. 그리고 인터넷 침해사고로 인한 근무 불능시간은 ICSA Labs에서 2004년도에 발표한 보고서의 내용을 기초로 하여 평균 시스템 불능시간을 23시간으로 선택했다[11]. 그리고 네트워크 손실률은 지난 2003년 1월 25일 Slammer 웜으로 인해서 일어난 인터넷 대란 때 국내 MS SQL 서버가 약 40%정도 피해를 입은 것을 기초로 하여 0.4로 선택했다[12].

3.1.3 매출 손실비용 산출

매출 손실비용에는 기업의 서비스 불능시간과 시간당 매출액 그리고 인터넷 공격의 영향도가 포함된다. 본 논문에서는 기업의 서비스 불능시간을 시스템 불능시간과 같이 놓았다[11]. 그리고 시간당 매출액은 전체 매출액을 서비스 시간으로 나눈 값을 선택했다. 그리고 침해사고 영향도는 정확하게 측정하는 기관이 없어서 본 논문에서는 [2]에서 선택한 값인 0을 사용했다.

3.2 간접적인 피해액 산출

3.2.1 피해 배상 비용 산출

피해 배상 비용은 기업의 서비스를 이용하는 소비자의 수와 피해 보상금 그리고 소비자 피해 비율로 구할 수 있다. 본 논문에서는 2003년 1월 25일 Slammer 웜으로 인한 인터넷 불능 사태 때의 네트워크 손실률을 바탕으로 소비자 피해 비율을 0.4로 추정했다[12]. 이 때 각 소비자에 대한 계약상의 위약금은 각 기업의 계약 약관에 명시되어 있다[6][16][17]. 따라서 소비자 1인당 계약상 위약금은 서비스 불능시간과 이 금액의 곱으로 산출할 수 있다.

3.2.2 소비자 기회비용 산출

소비자 기회비용은 실제 계약을 해지한 소비자의 수와 잠재적인 소비자의 수 그리고 소비자 당 평균 매출로 구할 수 있다. 또한 이 손실액은 시간이 지남에 따라서 증가하기 때문에 시간의존적이다. 본 논문에서는 이 시간을 1년으로 설정하고 실제 피해액을 산출했다. 실제 계약을 해지한 소비자의 수와 잠재적인 소비자의 수는 인터넷 리서치 기관의 ‘인터넷 서비스 교체 의향에 관한 집계 조사’의 자료를 바탕

<표 6> 실제 자료를 토대로 기업의 경제적인 피해액 분석

인 자			P_{hw}	d_r	ds_o	d_o
값			0.1	16시간	23시간	23시간
인 자			P_{net}	$P_{\inf}$	P_{claim}	Δt
값			0.4	0	0.4	1년
인 자			K사	H사	L사	
D_{system}	D_{sw}	P_{idata}	0.22	0.22	0.22	
		D_{data}	15만원	15만원	15만원	
		D_{idata}	2000만원	2000만원	2000만원	
	M_c	C_{hw}	40만원	40만원	40만원	
	E_{ad}		14,500원	14,500원	14,500원	
	$N_{\inf}$		16000대	640대	320대	
$\sum D_{system}$			766억 2400만원	30억 6496만원	15억 3248만원	
D_{pro}	E_{no}		37,957명	1,565명	734명	
	D_{time}		35,720원	10,532원	99,587원	
$\sum D_{pro}$			124억 7358만원	1억 5164만원	6억 7250만원	
D_{rev}	$\frac{R_a}{ds_a}$		13억 5000만원	1억 6500만원	7300만원	
$\sum D_{rev}$			0원	0원	0원	
D_{lia}	N_{cus}		6,241,789명	3,609,838	261,916	
	C_c		1,455원	1,404원	1,404원	
$\sum D_{lia}$			835억 5258만원	466억 2755만원	33억 8311만원	
$D_{customer}$	C_A		630,420명	364,593명	71,714명	
	C_P		10,958명	2,943명	45,260명	
	R_C		336,000원	324,000원	324,000원	
$\sum D_{customer}$			2155억 300만원	1190억 8166만원	378억 9957만원	
D_{total}			3881억 4516만원	1689억 2581만원	434억 8766만원	

으로 구했다[13][14][18].

이 집계 조사에 의하면 약 45.5%가 서비스 교체 의향이 있다고 답을 했고 교체 이유는 <표 5>에서 보는 것과 같이 집계되었다. <표 5>의 교체 이유 중에서 '안정성이 떨어져서'가 약 22.1%로 집계되었다. 따라서 45.5%의 교체 의향비율과 22.1%의 교체 이유 비율을 통해서 인터넷 침해사고로 인한 전체적인 서비스 교체 비율을 구할 수 있다. 45.5%중에서 인터넷 침해사고로 인한 서비스 교체를 원하는 비율이 22.1%이므로 전체적으로 인터넷 침해사고로 인해서 서비스를 교체할 비율은 약 10.1%정도임을 알 수 있다. 그리고 이 10.1%의 서비스 교체 비율과 각 기업의 서비스를 이용하는 소비자의 수를 통해서 계약 해지 소비자의 수를 구할 수 있다. 이렇게 산출된 전체 계약 해지 소비자 수에 소비자당 평균 매출액을 곱하면 소비자 기회비용을 산출할 수 있다. 소비자당 평균 매출액은 2005년도 각 기업의 자료를 바탕으로 구했다[15].

〈표 5〉 인터넷 서비스 교체 이유

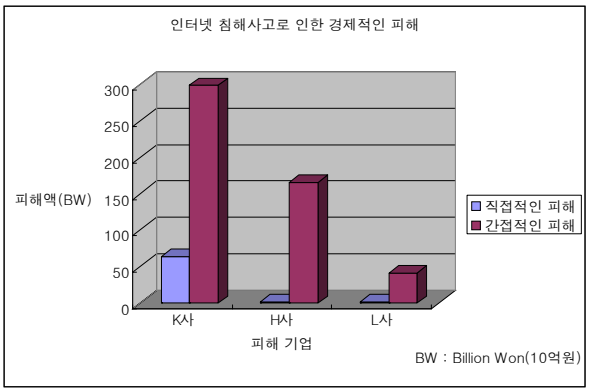
서비스 교체 이유	비율(%)
속도가 느려서	40.0
가격이 비싸서	24.1
안정성이 떨어져서	22.1
기타	13.8

3.3 실제 기업의 경제적인 피해 산출

지금까지 구한 자료를 바탕으로 국내 대형 ISP 3사에 대한 인터넷 침해사고의 경제적인 피해액을 산출해서 다음 <표 6>에 나타내었다.

다음 (그림 1)를 살펴보면 간접적인 피해의 비율이 훨씬 더 큰 것을 알 수 있는데 이는 소비자 기회비용이 전체에서 차지하는 비율이 가장 높기 때문이다.

각 기업의 전체적인 매출에 대비한 경제적인 피해액의 비율을 살펴보면 K사가 약 3.3%, H사가 약 11.7%, L사가 약



(그림 1) 각 기업의 피해 비율

6.8%로 각 기업마다 기업의 특성에 따라서 경제적인 피해의 비율이 서로 다르나 전체 매출에 대비한 경제적인 피해의 손실은 어느 기업이나 무시하지 못할 정도로 크다는 것을 알 수 있다.

4. 결론 및 향후 연구 방향

본 논문에서는 인터넷 침해사고에 의한 경제적인 피해를 산출하는 하나의 기준 모델을 제시했다. 제시한 피해 산출 모델은 인터넷 침해사고로 인한 직접, 간접적인 피해를 효과적으로 산출할 수 있는 기준을 제시하고 있다. 이 피해 산출 모델은 인터넷 침해사고로 인해서 기업이 입은 피해를 좀 더 정확하게 산출하는데 많은 도움을 줄 뿐만 아니라 이 피해 모델에 근거해서 산출된 피해액을 기준으로 이 후에 입게 되는 피해에 관한 하나의 기준점을 정하는데도 많은 도움을 줄 것이다.

그러나 본 논문에서 제시한 피해 산출 모델도 아직까지는 부족한 점이 많다. 여러 가지 인자들을 제시했으나 그 중 몇 가지 인자들은 정확한 값을 아직 알지 못해서 가정해서 경제적인 피해를 산출해냈다. 따라서 향후 연구 방향은 본 논문에서 가정한 여러 가지 인자들의 정확한 값을 알아내는 방법에 관한 연구가 수행되어야 할 것이고 이 연구에 바탕을 두어서 좀 더 정확한 경제적인 피해를 산출하는 기준 모델을 제시해야 할 것이다.

참 고 문 헌

[1] Nicholas Weaver, Vern Paxson, “A Worst-Case Worm,” Workshop on Economics and Information Security, June 2004.

[2] Thomas Dubendorfer, Arno Wagner, Bernhard Plattner, “An Economic Damage Model for Large-Scale Internet Attacks,” WET ICE 2004. 13th IEEE International Workshop, pp.223-228, June 2004.

[3] Jelena Mirkovic, Janice Martin, Peter Reiher, “A Taxonomy of DDoS Attacks and DDoS Defense Mechanims,” Computer Science Department University of California, Los Angeles, Technical Report No.020018, pp.39-53.

[4] Jose Nazario, Jeremy Anderson, Rick Wash, Chris Connelly, “The Future of Internet Worms,” Blackhat Briefings on Las Vegas, July 2001.

[5] http://www.computereconomics.com/article.cfm?id=1225, 2005 Malware Report: Executive Summary.

[6] http://www.kt.co.kr, 한국 통신 이용약관.

[7] http://www.etnews.co.kr/chart/chartdetail.html?chart_code=20050811094756, ‘각 PC 부품별 소매시장 가격’, 2005년 8월 기준.

[8] http://www.myung.co.kr/dr/menu02_01.php, 소프트웨어 복구율, (주)명정보기술, 2006년 12월 기준.

[9] David M. Smith, “The Cost of Lost Data,” Gaziadio business report in 2003.

[10] www.molab.go.kr, 정책정보자료 간행물 2005 노동 통계연감, pp.2, 4, 10, 338, 2006년 3월 기준.

[11] ICSA Labs 10th Annual, “Computer virus prevalence Survey,” 2004.

[12] http://www.secureosforum.org/news/security_read.htm?id=411&start=845, 보안뉴스, 정통부 ‘1.25 인터넷대란’ 조사결과 발표.

[13] http://www.etnews.co.kr/chart/chartdetail.html?chart_code=20060417094947, ‘분기별 초고속 인터넷 가입자 추이’, 2006년 4월 기준.

[14] http://www.embrain.com/pr/embrainPR_test.asp?page=8, ‘e리서치-초고속인터넷관련조사,’ 2006년 5월 기준.

[15] http://www.etnews.co.kr/chart/chartdetail.html?chart_code=20060306095234, ‘초고속 인터넷 사업자 2005년 ARPU 현황’, 2006년 3월 기준.

[16] http://service.hanaro.com/other/policy/stip.asp, 하나로 통신 인터넷서비스약관.

[17] http://www.powercomm.co.kr/index.jsp, LG 텔레콤 서비스 이용약관.

[18] http://www.etnews.co.kr/chart/chartdetail.html?chart_code=20060724101630, ‘초고속 인터넷 가입자 현황’, 2006년 7월 기준.

장 종 호

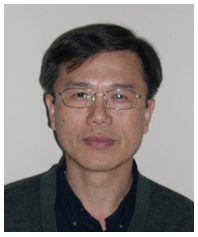
e-mail : toy3901@hotmail.com

2005년 아주대학교 정보통신대학 전자공학부(학사)

2007년 아주대학교 정보통신대학 전자공학과(석사)

2007년~현 재 삼성전자

관심분야 : 인터넷보안



정 기 현

e-mail : khchung@ajou.ac.kr

1984년 서강대학교 공과대학 전자공학과 (학사)

1988년 미국일리노이대학 EECS(석사)

1990년 미국퍼듀대학교 EE(박사)

1991년~1992년 현대전자반도체연구소

1992년~현 재 아주대학교 전자공학부 교수

관심분야 : 인터넷보안, 임베디드 시스템

최 경 희

e-mail : khchoi@ajou.ac.kr

1984년 서울대학교 사범대학 수학교육과 (학사)

1988년 프랑스 그랑데꼴 Enseeiht 정보과학과 (석사)

1990년 프랑스 Paul Sabatier 정보과학과 (박사)

1982년~현 재 아주대학교 정보통신전문대학원 교수

관심분야 : 운영체제 임베디드 시스템, 실시간 시스템