현안참고자료

사이버 테러의 상시 감시 체제를 구축하자!

- 디도스 사이버 테러의 피해와 대책 -

2009. 7. 23.

現代經濟硏究院
HYUNDAI RESEARCH INSTITUTE

목 차

1. 문제 제기: 심각해지고 있는 사이버 테러 문제

이제 인터넷은 경제와 사회 전반에 걸쳐 필수 불가결한 삶의 일부가 되고 있다. 인터넷 이용자수는 2001년 2,438만명에서 2008년 3,536만명으로, 전자상거래액은 2001년 119조원에서 2008년 630조원으로, 인터넷 뱅킹은 2001년 1,364조원에서 2008년 8,298조원으로 급증하고 있다. 반면에 인터넷 이용이 확대될수록 역기능으로서 **사이버 테러(인터넷 침해)에 의한 인터넷 피해 또한 기하급수적으로 증가한다.** 인터넷 해킹, 바이러스 침해에 의한 사이버 테러가 2004년 13만 7,103건였던 것이 보안 의식과 기술이 강화되면서 2008년에 2만 4,409건으로 매년 감소세를 보였다. 하지만 사이버 테러로 인한 피해액은 인터넷 이용 확대와 맞물려 더욱 늘어났을 것으로 판단된다.
사이버 테러에 대한 대비는 인터넷 기반의 경제·사회 체제가 가져야 할 필수 기능의 하나이다. **하지만 2009년 7월 7일 발생된 DDoS 사이버 테러 사태에서 나타났듯이 아직 일사분란한 대응 체제가 갖추어져 있지 못했으며, 사태의 심각성을 인식하는 사회적 분위기도 미흡하다. 사이버 테러의 대응책을 시급히 강구해야 한다.**

2. 7·7 DDoS 사이버 테러의 사례 : 경제적 피해액 추정

○ 개요

7월 7일부터 10일까지 3일간에 걸쳐 분산서비스거부(DDoS) 공격으로 청와대와 백악관 등 한미 주요 정부기관, 민간의 홈페이지를 이용하지 못하는 사건이 발생하였다.

* 분산서비스거부(DDoS : Distributed Denial of Service)란 다수의 컴퓨터를 이용해 특정 서버에 대량의 트래픽을 전송해 그 서버에 과부하를 발생시켜 정상적인 서비스 이용을 방해하는 사이버 공격법임

금번 DDoS 사이버 테러는 기존 컴퓨터 바이러스 침해에 따른 사태와 다른 몇 가지 특징을 보여주고 있다. **첫째, DDoS 공격을 받은 사이트라 하더라**

도 전혀 서비스 제공이 불가능한 것은 아니라는 점이다. DDoS 공격을 받은 서버라 하더라도 완전히 서비스 불능 상태에 빠진 것이 아니라 처리 능력에 따라 서비스 제공이 가능한 경우도 있어 침해시간 산정에 어려움이 있다. **둘째, 금번 DDoS 사태는 매일 공격 사이트를 지정해 옮겨 다닌 것이 특징이다.** 따라서 공격받은 사이트별로 피해를 입은 시간이 차이가 나므로, 피해액 산출시 필요한 피해업체의 비중 산정시 중요히 감안해야 한다.

○ 7·7 DDoS 사이버 테러의 경제적 피해 규모 추정

시간당 GDP에서 인터넷이 기여하는 부분을 간접 추정하여 손실액을 산출하는 방법을 활용하였다. 하지만 정확한 피해 현황을 조사하지 않고 추정하는 관계로, 금번 사태의 특징과 가정을 고려하여 아래와 같은 피해액 추정 산식을 정하였다.

(산식)

7·7 DDoS 사이버 테러 피해액

= Σ {(피해 기관·업체 관련 부문의 2009년 추정 GDP × 피해 기관·업체의 비중) / 연간근무시간} × 10.9% × 피해 시간

(산정 결과)

피해 시간을 최소 24시간, 최대 72시간으로 보았을 경우, 금번 DDoS 사태로 인한 경제적 피해액은 **최소 363억원에서 최대 544억원으로 산출되었다.**

7·7 DDoS 사이버 테러의 경제적 피해액 :

< 최소 363억원 ~ 최대 544억원 >

*참고: 작년 풍수해 피해액 580억원

(가정 및 유의사항)

1. 본 피해액 산정 산식은 개별 업체·기관의 정확한 피해 파악을 근거로 산출하는 것은 아니며, 또

한 통일된 기준 적용으로 개별 업체의 특성을 제대로 반영하지 않은 관계로 산정된 피해액에 오차가 존재함에 유의

2. 피해액 산정 방법으로는 한국정보보호진흥원 (2008)의 방법인 시간당 GDP에서 인터넷이 기여하는 부분을 간접 추정하여 손실액을 산출한 방법을 원용. 다만 전산업이 아닌 피해 업체만 고려하는 관계로 상기와 같이 산식을 변경하였고, 복구비용은 추정 어려움으로 산정에서 제외
3. "피해 업체·기관 소속 부문의 2009년 추정 GDP"에서 당 연구원(HRI)의 2009년 추정 GDP를 활용하였으며, 피해 업체·기관이 소속된 부문(국가기관, 신문, IT서비스업, 소매업, 은행)의 GDP내 비중은 산업연관표(2006년도)에 기초해 전산업 부가가치에서 차지하는 각 부문의 비중과 동일하다고 가정
4. "피해 업체·기관의 비중"은 소속 부문의 GDP에서 피해 업체·기관이 차지하는 비중으로서, 여기서 비중 계산시 고려된 매출(민간업체)과 예산(국가기관) 규모는 GDP에 비례한다고 가정
5. "10.9%"는 한국정보보호진흥원(2008)이 인터넷의 GDP 기여도로서 적용한 수치로서, 본 피해액 산출에서도 10.9%의 기여도가 있다고 가정
6. "피해 시간"은 DDoS 공격 시간 중에서 업체·기관이 피해를 본 시간을 의미하는 것임. 피해 업체·기관별 정확한 피해 시간 추정이 어려워 총 72시간 공격 중에서 1차 공격 시간인 24시간을 최소 피해 시간으로, 그리고 72시간 중의 절반인 36시간을 최대 피해 시간으로 가정하였음. 그러므로 피해시간 24시간~36시간이 과대 추정되었을 가능성도 존재

금번 DDoS 사이버 테러는 과거 1.25 인터넷 대란과는 달리 일부 사이트의 접속 지연이라는 특징으로 피해 시간은 길었으나 피해 금액은 크지 않은 것으로 판단된다. 하지만 참고로 최대 544억원은 작년의 풍수해 피해액인 580억원에 거의 근접한 수치여서 피해 정도는 심각하다고 할 수 있다.

3. 사이버 테러 대응책

DDoS, 바이러스에 의한 사이버 테러로 인한 피해는 유비쿼터스 사회 등 IT 네트워크가 대규모화하는 사회로 진전될수록 더욱 대형화하므로 이에 대하여 정부, 민간기업, 일반인이 공조하여 국가 차원에서 대응책을 시급히 강구해야 한다.

첫째, 고도의 통제 수준을 갖추기 위한 국가 차원의 사이버 대응 체제를 구축해야 한다. 사이버 테러는 국지적 공격이 아닌 글로벌 차원에서 행정, 민간, 가계 등 다양한 분야에 걸쳐 전면적으로 전개되는 속성을 지닌다. 그

러므로 사전 예방과 사태 발생시 필요한 자원의 신속한 동원 및 대응을 위해 국가 차원에서 이루어지는 고도의 통제 수준이 요청된다. 국가 차원의 CSO(Chief Security Officer: 최고 보안 책임자)를 임명하고 유관기간, 그리고 ISP, 보안 관련 민간기업이 참여하는 합동 통제 체제를 구축하고, 인터넷 침해 여부를 신속히 탐지하고, 공격 유형을 분석, 대응하는 통합 관제 체제를 구축, 운영해야 한다.

둘째, 사이버 테러 방지를 위한 국가 기관, 민간 기업내 '사이버 테러 신속대응 팀'을 조직해야 한다. 사이버 테러는 일반적으로 동시 다발적, 대규모적으로 진행되기 때문에 더 이상 피해 확산을 방지하기 위해서는 조기 대응이 절대 중요하다. 국가 기관과 민간 기업 내부에 '사이버 테러 신속대응팀'을 조직하여 다양한 분야의 전문 인력이 모여 상황 파악과 대응 방법을 강구하고, 단위 조직별 바이러스 퇴치 활동 체제를 구축한다.

셋째, 국가 차원에서 민간업체의 기술 개발 및 인력 양성을 지원해야 한다. 바이러스와 같은 악성 코드의 기술 개발 또한 컴퓨터 발달에 따라 빠르게 변하기 때문에 사전적으로 진화된 대응 기술을 개발하고 필요한 인력을 양성하는 노력이 필요하다. 국가 차원에서 민간업체의 바이러스 백신 개발 및 배포, 그리고 인력 양성을 지원하는 방안을 마련해야 한다.

넷째, '바이러스 색출의 날'을 정해 매달 전국적으로 바이러스 검사를 실시해야 한다. 사이버 테러의 핵심 수단은 자신은 알지 못하는 사이에 불법적인 행동에 사용되고 있는 PC이다. 일반인들은 금번 7·7 사태로 알 수 있듯이 개인 자신의 PC가 '나'만의 PC가 아니라 테러에 동원된 '무기'가 되고 있음을 심각하게 인식해야 한다. 인터넷에 연결된 PC라면 이런 불법적인 데에 이용될 가능성이 항상 존재하기 때문에 개인 스스로의 사전 예방이 무엇보다 중요하다. 정부는 일반 국민 대상의 보안 의식 강화 및 사전 예방 활동을 전개해야 한다. 과거 있었던 '쥐잡기 날' 같이 한달에 한번씩 컴퓨터 바이러스 검사를 행하는 '바이러스 색출의 날'을 정해 시행하는 것도 바람직하다.

1. 문제 제기: 심각해지고 있는 사이버 테러 문제

- 인터넷 이용 인구가 확산되면서 인터넷은 경제와 사회 전반에 걸쳐 필수 불가결한 삶의 일부가 되고 있음

< 인터넷 이용 현황 >

구분		2001년	2003년	2005년	2008년
인터넷 이용률	(%)	56.6%	65.5%	72.8%	77.1%
인터넷 이용자수	(천명)	24,380	29,220	33,010	35,360
전자상거래 거래액	(조원)	119	235	358	630
인터넷 뱅킹 이용	(조원)	1,364	2,844	4,490	8,298

자료: 한국인터넷진흥원 인터넷통계정보시스템, 통계청 국가통계포털, 한국은행 경제통계시스템
주: 1) '인터넷 이용률'과 '인터넷 이용자수'는 6세 이상 기준
2) '인터넷 뱅킹 이용'은 자금이체와 대출신청을 합한 금액

- 반면에 인터넷 이용의 역기능인 컴퓨터 바이러스, 스팸메일 등에 의한 사이버 테러(인터넷 침해) 사고는 대량으로 발생하고 있음[1)]
  - 2005년부터 인터넷 공격에 대한 보안 의식이 확대되면서 사이버 테러 건수는 매년 줄어드는 추세에 있음
  - 하지만 사고로 인해 피해액은 인터넷 이용 증대와 맞물려 더욱 증가하였을 것으로 판단됨

< 우리나라 인터넷 해킹, 바이러스 침해에 의한 사이버 테러 건수 >

(단위: 건)

구분	2004	2005	2006	2007	2008	2009 1~5
웜·바이러스	107,994	16,093	7,789	5,996	8,469	3,662
해킹신고처리	29,109	33,633	26,808	21,732	15,940	7,428
합계	137,103	49,726	34,597	27,728	24,409	11,090

자료: 한국정보보호진흥원, 「해킹 바이러스 통계 및 분석 월보」 각호

1) 본 보고서에서는 인터넷 침해를 '사이버 테러'로 규정

- **그 이유는 인터넷을 이용하는 사람이 늘어날수록 그 피해 규모는 기하급수적으로 증가하기 때문임[2)]**
  - 이는 2003년에 발생하였던 '1.25 인터넷 대란'을 통해 컴퓨터 웜 바이러스가 네트워크로 연결되지 않은 이전 컴퓨팅 시대보다 훨씬 빠른 속도로 전파되고, 그리고 훨씬 커다란 피해를 초래하고 있음을 피부로 느끼게 되었음

< 국내 주요 사이버 테러 >

날 짜	내 용	피해액
2003. 1. 25	일명 1.25인터넷 대란, 마이크로소프트 윈도우즈 서버(MS SQL서버)의 취약점을 이용한 슬래머 웜 바이러스로 인해 국내 8,800여대(11.8%) 컴퓨터 감염	1,055억원 ~ 1,675억원[1)]
2004. 7. 13	중국에서 유입된 악성 프로그램으로 국회와 한국국방연구원, 원자력연구소 등 10개 국가 전산망 피해	-
2008. 2. 5	사이버 쇼핑몰 옥션에서 이용자 1,081명의 개인 정보와 100만명의 계좌번호가 유출	-
2009. 7. 7	DDoS 공격에 의한 주요 정부기관, 민간의 인터넷 사이트 이용에 장애	363억원 ~ 544억원[2)]

주: 1) 한국정보보호진흥원 추정치 (2008)
2) 현대경제연구원 추정치 (* 추후에 상세한 산출 방식 설명)
3) DDoS 사례는 "첨부 1: 과거 DDoS 공격에 의한 피해 사례" 참조

- **그러므로 사이버 테러 대책은 인터넷 기반의 경제·사회 체제가 가져야 할 필수 기능의 하나로서 인식 확산과 체계화된 대응책이 시급히 요청됨**

- **하지만 2009년 7월 7일 발생된 DDoS 사이버 테러 사태에서 나타났듯이 아직 일사분란한 대응 체제가 갖추어져 있지 못했으며, 사태의 심각성을 인식하는 사회적 분위기도 미흡**
  - 이에 따라 금번 DDoS 사이버 테러 사태에 대한 경제적 피해 규모를 파악해 문제의 심각성을 살펴보고,
  - 향후 사이버 테러에 대한 정책적 대응을 제시함

2) 이를 '멧 칼프 법칙'이라 함. 네트워크에 n명이 참여하고 있다면, 이 네트워크의 가치는 참여자의 수에 비례하는 법칙임

2. '7·7 DDoS 사이버 테러' 사례 : 경제적 피해액 추정

○ '7·7 DDoS 사이버 테러'의 개요

- **(경과) 7월 7일부터 7월 10일까지 3일간에 걸쳐 DDoS (분산 서비스 거부) 공격으로 청와대와 백악관 등 한미 주요 정부기관, 민간의 인터넷 사이트가 마비되는 사건이 발생[3)]**
  - DDoS (Distributed Denial of Service : 분산 서비스 거부)란 특정 인터넷 서버에 대량의 트래픽(서비스 요청 신호)을 전송해 그 서버의 정상적인 서비스 이용을 방해하는 사이버 공격법임
  - 7월 7일(화) 18시 이후 공격이 시작되었으며, 7월 10(금) 18시를 지나 DDoS 공격 트래픽이 이전 대비 1/10 수준으로 급격히 감소하면서 접속 불능 사태가 종결 (방통위 발표 기준)
  - 7월 10(금) 자정이 지나면서는 악성 코드에 감염된 PC 파일이 삭제되거나 부팅 에러가 발생하는 피해를 발생

< 7·7 DDoS 사이버 테러 진행 경과 >

- 7일 오후 6시	DDoS 1차 공격 개시
- 8일 오전 2시	방송통신위원회 '주의' 경보령 발령
오후 6시	DDoS 2차 공격 개시
- 9일 오후 6시	DDoS 3차 공격 개시
- 10일 0시	PC 하드디스크 데이터 파괴
오후 6시	DDoS 공격 트래픽이 이전 대비 1/10 수준으로 감소하면서 피해 사이트들의 정상 접속하고, DDoS 공격 종료
- 11일 ~	PC 손상 방지 및 대처 방법 공지
- 13일 오전 8시	총 1,075건의 DDoS 악성코드 피해 신고 접수

3) 언론, 유관기관(방송통신위원회, 한국정보보호진흥원)의 발표 내용을 참조

< 공격 대상 기관 >

기관유형	공격 진행 시간 (7월 7일 18시 ~ 7월 10일 18시)		
	24시간	48시간	72시간
공공기관	국회	청와대	
	한나라당	국방부	
	외교통상부	한미연합사령부	
	국가정보원		
	행정안전부		
언론			조선닷컴
기업	안철수연구소	다음 메일	네이버 메일
	이스트소프트	파란 메일	옥션
은행	외환은행	국민은행	
	신한은행		
	농협		
	우리은행		
	하나은행		
	기업은행		

자료: 연합뉴스 2009. 7. 9일자 발표 기준

- '7·7 DDoS 사이버 테러'의 특징

① DDoS 공격을 받은 사이트라 하더라도 전혀 서비스 제공이 불가능한 것은 아님

- 과거 '1.25 인터넷 대란'시와 같은 컴퓨터 바이러스 공격시에는 바이러스에 감염된 인터넷 서버가 작동 불능 상태가 되어 인터넷 접속 서비스를 전혀 제공할 수 없는 상태에 빠짐
- 하지만 금번 DDoS 공격을 받은 서버는 계속되는 공격으로 정상적인 서비스 요구를 평소보다 더디게 제공하거나 심한 경우 불가능한 지경에 다다르게 됨

· 아울러 특정 웹사이트에 대한 총 DDoS 공격 시간이 접속 불능 시간을 가리키는 것은 아님
· 따라서 DDoS 공격을 받은 서버라 하더라도 완전히 서비스 불능 상태에 빠진 것이 아니라 처리 능력에 따라 서비스 제공이 가능한 경우도 있어 침해 시간 산정에 어려움이 있음

② 금번 DDoS 사태는 매일 공격 사이트를 지정해 옮겨 다닌 것이 특징

· 7월 7일부터 9일까지 매일 오후 6시에 사전에 지정된 인터넷 사이트로 공격 대상을 옮겨다녔음
· 3일간 계속 공격을 받은 사이트도 있지만 1일로 그친 사이트도 있음
· 따라서 공격받은 사이트별로 피해를 입은 시간이 차이가 나므로, 피해액 산출을 위해 피해 비중 산정시 중요히 고려

○ '7·7 DDoS 사이버 테러'의 경제적 피해 규모 추정

- 금번 7·7 DDoS 사이버 테러의 경제적 피해액 추정에는 "별첨 2: 경제적 피해 규모 추정에 관한 연구 방법"에 설명한 한국정보보호진흥원 (2008)의 방법 2를 원용[4)]

· 한국정보보호진흥원의 방법2는 피해 데이터 확보가 불가능한 부문(가계, 정부기관) 등을 고려하기 위해 시간당 GDP에서 인터넷이 기여하는 부분을 간접 추정하여 손실액 산출
· 즉 인터넷을 사용하는 생산주체들의 영업 및 생산 활동이 저하됨으로써 받게 된 피해를 GDP의 손실분으로 설명될 수 있다고 가정하고, 이때 손실액은 GDP에 'IT 자본의 총부가가치 기여도' 10.9%로 추정[5)]

4) 기존 인터넷 침해 사고에 대한 연구 방법에 대해서는 "첨부 2: 경제적 피해 규모 추정에 관한 연구 방법" 참조
5) 정보보호진흥원(2008) 방법 2에서 기대손실액 추정시 적용하였던 수치로서, 이는 신일순("IT 혁명과 기업활동의 변화", 「21세기 한국 메가트렌드 시리즈 II」, 2005)의 연구에서 원용

· 이러한 방법으로 한국정보보호진흥원은 2003년 발생된 1.25 인터넷 대란의 침해 비용을 GDP손실, 복구비용을 합한 1,675억원으로 추정
· 금번 7·7 사이버 테러의 경우에도 개별 업체의 피해 파악이 불가능하고, 정부 등의 공공 기관이 관련되어 있기 때문에 이 방법을 원용하였음
· 다만 전산업이 아닌 피해 업체만 고려하는 관계로 산정 방식을 변경하였고, 복구비용은 추정 어려움으로 산정에서 제외

- 금번 7·7 사이버 테러의 정확한 피해 현황이 아직 조사되지 않은 관계로 아래의 몇 가지 피해액 추정에 필요한 전제 조건을 설정

· 모든 업종·기관이 아닌 일부 피해 업체·기관만 고려해야 하는 관계로 피해 업체·기관이 관련된 부문에서 이들이 차지하는 비중(2006년도 매출, 예산 비중)으로 피해액 기여도를 감안
· 피해 시간은 총 DDoS 공격시간 72시간 중에서 1차 공격 시간인 24시간을 최소 피해 시간으로, 그리고 72시간 중의 절반인 36시간을 최대 피해 시간으로 추정

- 최종적으로 가정을 고려하여 결정된 7·7 사이버 테러의 피해액 추정 산식과 추정 도출에 필요한 파라미터와 자료원은 아래와 같음

< 피해액 산정 방식 >

(산식)

피해액 = Σ {(피해 업체·기관 소속 부문의 2009년 추정 GDP
× 피해 업체·기관의 비중) / 연간근무시간}
× 10.9%
× 피해 시간

(가정 및 유의사항)

1. 본 피해액 산정 산식은 개별 업체·기관의 정확한 피해 파악을 근거로 산출하는 것은 아니며, 또한 통일된 기준 적용으로 개별 업체의 특성을 제대로 반영하지 않은 관계로 산정된 피해액에 오차가 존재함에 유의
2. 피해액 산정 방법으로는 한국정보보호진흥원 (2008)의 방법인 시간당 GDP에서 인터넷이 기여하는 부분을 간접 추정하여 손실액을 산출한 방법을 원용. 다만 전산업이 아닌 피해 업체만 고려하는 관계로 상기와 같이 산식을 변경하였고, 복구비용은 추정 어려움으로 산정에서 제외
3. "피해 업체·기관 소속 부문의 2009년 추정 GDP"에서 당 연구원(HRI)의 2009년 추정 GDP를 활용하였으며, 피해 업체·기관이 소속된 부문(국가기관, 신문, IT서비스업, 소매업, 은행)의 GDP내 비중은 산업연관표(2006년도)에 기초해 전산업 부가가치에서 차지하는 각 부문의 비중과 동일하다고 가정
4. "피해 업체·기관의 비중"은 소속 부문의 GDP에서 피해 업체·기관이 차지하는 비중으로서, 여기서 비중 계산시 고려된 매출(민간업체)과 예산(국가기관) 규모는 GDP에 비례한다고 가정
5. "10.9%"는 한국정보보호진흥원(2008)이 인터넷의 GDP 기여도로서 적용한 수치로서, 본 피해액 산출에서도 10.9%의 기여도가 있다고 가정
6. "피해 시간"은 DDoS 공격 시간 중에서 업체·기관이 피해를 본 시간을 의미하는 것임. 업체별 정확한 피해 시간 추정이 어려워 총 72시간 공격 중에서 1차 공격 시간인 24시간을 최소 피해 시간으로, 그리고 72시간 중의 절반인 36시간을 최대 피해 시간으로 가정하였음. 그러므로 피해시간 24시간~36시간이 과대 추정되었을 가능성도 존재

< 피해액 산출에 사용된 파라미터와 자료원 >

파라미터		자료원
피해 부문(기관, 업체)별 GDP 비중		- 2006년 산업연관표 (한국은행)
해당 부문에서 피해 기관, 업체의 비중	피해 공공기관	- 2006년 예산 (기획재정부)
	피해 신문사	- 국가통계포털(통계청) - 전자공시시스템(금융감독원)
	피해 IT서비스 업체	- 부가통신서비스 매출액 (지식경제부 정보통신산업 통계연보)
	피해 전자상거래 업체	- 소매업태별 판매액 (통계청 국가통계포털)
	피해 은행	- 금융감독원 금융통계정보시스템
근로시간		- 국가통계포털(통계청)

- 피해액 산출

· 앞서 제시한 산식에 의해 피해시간을 최소 24시간에서 최대 36시간으로 보았을 경우, 피해액은 최소 363억원에서 최대 544억원으로 산출

· 금번 DDoS 사태는 과거 1.25 인터넷 대란과는 달리 일부 사이트의 접속 지연이라는 특징으로 피해 시간은 길었으나 피해 금액은 절반 정도에 지나지 않음

· 하지만 최대 544억원은 작년의 풍수해 피해액인 580억원에 거의 근접하고 있어 7·7 DDoS 테러의 피해 정도가 적지 않았음을 알 수 있음

(자료: 행정안전부(2008.12), 2008 각종 재난발생 현황)

3. 사이버 테러 대응책

- 유비쿼터스 사회 등 IT 네트워크가 대규모화하는 사회로 진전될수록 인터넷 역기능에 의한 피해 또한 대규모화하므로 이에 대한 국가 차원의 대응이 요청됨

· 금번 DDoS 사태에서도 개인들의 컴퓨터 작동은 가능하지만 특정 사이트에의 인터넷 접속만이 어렵다는 상황이었음에도 불구하고 피해 규모가 컸음

· 어느 한 주체만의 노력으로는 미흡하고, 정부, 민간기업, 일반인이 공조하여 국가 차원에서 대응하는 노력이 요청

- 고도의 통제 수준을 갖추기 위한 국가 차원의 사이버 대응 체제를 구축

· 인터넷 침해는 멧칼프 법칙에 의해 신속하면서도 기하급수적으로 확대되기 때문에 필요한 자원의 신속한 동원과 대응을 위해 국가 차원에서 이루어지는 고도의 통제 대응 수준이 요청됨

· 국가 차원의 CSO(Chief Security Officer: 최고 보안 책임자)를 임명하고 정부내 유관기간, 그리고 ISP, 보안 관련 민간기업 등이 참여하는 정부와 민간의 합동 통제 체제를 구축

· 인터넷 침해 여부를 신속히 탐지하고, 공격 유형을 분석, 대응하는 통합 관제 체제를 운영

- 사이버 테러 방지를 위한 국가 기관, 민간 기업내 '사이버 테러 신속대응팀'을 구축하여 위기 비상시 공격 차단, 클린 PC 유지 등의 활동 전개

· 사이버 테러는 일반적으로 동시 다발적, 대규모적으로 진행되기 때문에 더 이상 피해 확산을 방지하기 위해서는 조기 대응이 절대 중요

· 국가 기관과 민간 기업 내부에 '사이버 테러 신속대응팀'을 구축하여 다양한 분야의 전문 인력이 모여 상황 파악과 대응 방법을 강구하고, 단위 조직별 바이러스 퇴치 활동 체제를 구축

- 국가 차원에서 민간업체의 기술 개발 및 보안 전문 인력 양성 지원

- 바이러스와 같은 악성 코드의 기술 개발 또한 컴퓨터 발달에 따라 빠르게 변하기 때문에 사전적으로 진화된 대응 기술을 개발하는 노력이 필요
- 국가 차원에서 민간업체의 바이러스 백신 개발 및 배포, 그리고 인력 양성을 지원하는 방안도 마련

- '바이러스 색출의 날'을 정해 매달 전국적으로 바이러스 검사를 실시

- 인터넷 침해의 주요 수단이 자신은 알지 못하는 사이에 불법적인 행동에 사용되고 있는 개인 PC임
- 일반 국민들은 금번 사태로 알 수 있듯이 개인 자신의 PC가 '나'만의 PC가 아니라 테러에 동원된 '무기'가 되고 있음을 심각하게 인식해야 함
- 그러므로 인터넷으로 연결된 PC라면 이런 불법적인 데에 이용될 가능성이 항상 개재되어 있기 때문에 개인들이 주기적으로 사전 예방 활동을 갖는 게 무엇보다 중요
- 정부는 일반 국민 대상의 보안 의식 강화 및 사전 예방 활동을 적극 전개해야 함
- 과거 있었던 '쥐잡기 날' 같이 한달에 한번씩 컴퓨터 바이러스 검사를 행하는 날을 가져보는 '바이러스 색출의 날'을 정하는 것도 필요
- 즉 국가는 민간 업체를 지원하여 '국가 공인 무료 백신 스타트-업' 프로그램을 개발하여 유포하고, '바이러스 색출의 날'에 컴퓨터를 키면 이 '스타트-업' 프로그램이 자동 진행되면서 최신 백신 버전으로의 업데이트, 검사 등을 진행HRI

이장균 수석연구위원 (02-3669-4119, johnlee@hri.co.kr)

첨부 1: 과거 DDoS 공격에 의한 피해 사례

구분	일시	피해자	세부 내용	비고
국내	'06.11월	국내 화상채팅 업체	- 업체 서비스 중단 - ISP 백본, 국제회선 부하 증가	금품요구
	'07.10월	게임아이템 거래업체	- 홈페이지 접속장애(수~15Gbps 트래픽)	금품요구
	'08.2월	게임 업체	- 동남아 쪽으로부터 공격을 받아 사이트 일시적 폐쇄	국외→국내
	'08.3월	증권 사이트	- 중국해커로부터 협박성 DDoS 공격 - 해당 사이트 접속장애 발생	금품요구
	'08.6월	국내 O당 홈페이지	- 홈페이지 접속장애	
	'08.7월	국내 포털사이트 카페	- 카페에서 탈퇴당한 10대 내국인이 중국 사이트에서 공격툴을 구입 후 보복공격	보복성
	'08.12월	반크 홈페이지 공격	- 일본 네티즌의 공격으로 홈페이지 접속 장애	국외→국내
	'09.3월	디카 커뮤니티 O	- 홈페이지 접속장애	금품요구
해외	'06.12월	폴란드 특정서버 공격	- 전체 ISP에 걸쳐 산발적으로 발생하고 국내 인터넷에도 지연현상 발생	국내→국외
	'07.2월	Root DNS 서버	- 13개 루트DNS 중 6개가 공격 받음	
	'07.4월	에스토니아 정부, 의회 등 주요 사이트	- 러시아 해커에 의해 약 2주간의 공격으로 피해 사이트 접속불능	국가 사이버전
	'07.9월	전자지불홈페이지 www.e-gold.com(미국)	- Virut 바이러스 감염 PC가 C&C로부터 악성코드 다운로드후 공격	
	'08.8월	그루지아 국방부, 외교부 등 주요 정부 사이트	- 러시아 해커들에 의해 그루지아 국방부, 외교부 등 사이트가 공격을 받음	국가 사이버전
	'09.1월	키르기즈스탄 ISP	- 러시아 해커에 의해 해당국의 인터넷 마비	국가 사이버전

자료: 방송통신위 (2009. 7)

첨부 2: 경제적 피해 규모 추정에 관한 연구 방법[6]

- **Farahmad, Navathe, Sharp, & Enslow (2005)**[7] : 인터넷 침해사고를 위협의 주체, 위협의 종류, 대응조치 세 가지 요소로 분석하는 일반적인 틀을 제시

- **Gordon & Loeb (2006)**[8] : 정보보호 침해사고와 관계된 비용과 편익을 분석하는 방법론 제시
  - 비용을 직접비용과 간접비용 - 명시적비용과 잠재적 비용으로 구분
  - 직접 비용: 특정 침해사고에 명확하게 연계될 수 있는 비용 (인력손실, H/W손실, S/W손실 등)
  - 간접 비용: 특정 침해사고에 직접적으로 연계되어지지 않는 비용 (보안장비 구입비 등)
  - 명시적 비용: 특정 침해사고에 예방, 탐지, 복구하기 위해 침해사고 기간 동안 발생한 명백한 비용 (복구인력비용, 매출손실비용 등)
  - 잠재적 비용: 기회 손실과 관련된 묵시적 비용을 의미하는 것으로 침해사고에 의한 기업 이미지 손실, 잠재적 법적책임 비용 등으로 계량화에 어려움 존재하는 비용

- **Weaver & Paxson (2004)**[9] : 인터넷 공격에 의한 경제적 피해를 선형적인 방법으로 산출하는 모델
  - 인터넷 침해 사고로 인한 전체 피해를 각 시스템의 피해와 피해를 입은 시스템의 수의 곱으로 계산

---

6) 내용은 유진호 등("인터넷 침해 사고에 의한 피해손실 추정", 「정보화정책」, 2008년 봄, 한국정보보호진흥원)의 자료를 참조

7) Farahmand, F., Navathe, S.B., Sharp, G.P., Enslow, P.H. (2005), "Assessing Damages of Inforamtion Security Incidents and Selecting control Measures, A Case Study Approach", *Workshop on the Economics of Information Security.*

8) Gordon, L.A and Loeb, M.P. (2006), *Managing Cybersecurity Resources: A Cost-Benefit Analysis.*

9) Weaver, N. & Paxson, V. (2004), "A Worst-Case Worm", *Third Annual Workshop on Economics and Information Security.*

· 여기서 시스템의 피해는 하드웨어와 소프트웨어 복구비, 시스템 복구 관리비, 생산성 손실액 등으로 측정

- 정보보호진흥원 (2008)[10] :

① 방법 1: Gordon & Loeb (2006) 연구를 활용해 직접비용과 명시적 비용에 해당하는 4가지 비용으로 침해액 추정

· 4가지 침해 비용: 매출이익손실, 생산효율 저하로 인한 손실, 복구비용, 복구 불가능한 데이터의 가치

· 매출이익 손실: 침해 사고로 인해 정상 상태에서 얻게 될 매출이익이 상실된 부분으로서 인터넷 시간당 이익 x 피해시간 x 침해사고 영향도로 산출
(*인터넷 시간당 이익 = (연간매출 x 매출영업이익률 x 인터넷의존도) ÷ 연간 인터넷 영업시간)

· 이러한 방식으로 2003년 발생된 1.25 인터넷 대란의 침해 비용은 매출이익손실, 생산효율저하로 인한 손실, 복구비용을 합한 1,055억원으로 추정

② 방법 2: 방법 1이 피해 데이터 확보가 불가능한 부문(가계, 정부기관) 등을 고려에서 배제하는 한계를 극복하기 위해 시간당 GDP에서 인터넷이 기여하는 부분을 간접 추정하여 손실액 산출

· 방법 1에서 매출이익 손실과 생산효율 저하로 인한 손실은 국내에서 인터넷을 사용하는 생산주체들의 영업 및 생산 활동이 저하됨으로써 받게 된 피해로서 GDP의 손실분으로 설명될 수 있다고 가정

· 따라서 손실액은 GDP에 'IT 자본의 총부가가치 기여도' 10.9%로 추정[11]

· 이러한 방식으로 2003년 발생된 1.25 인터넷 대란의 침해 비용은 GDP손실, 복구비용을 합한 1,675억원으로 추정

이장균 수석연구위원 (02-3669-4119, johnlee@hri.co.kr)

10) 유진호 등, "인터넷 침해 사고에 의한 피해손실 추정", 「정보화정책」, 2008년 봄, 한국정보보호진흥원.

11) 정보보호진흥원(2008) 방법 2에서 기대손실액 추정시 적용하였던 수치로서, 이는 신일순("IT 혁명과 기업활동의 변화", 「21세기 한국 메가트렌드 시리즈 II」, 2005)의 연구에서 원용