주 제

인터넷침해사고대응지원센터 구축 및 운영

한국정보보호진흥원 노명선

차 례

우리나라는 정보통신 인프라 구축등 정보화에 대한 적극적인 정책추진으로 국가경제의 발전은 물론 실질적인 삶의 질 향상을 이루게 되었고, 이제는 사이버공간이 모든 분야에서 일상생활의 필수적인 요소로 자리잡게 되었다

그러나 정보화의 가속화로 인터넷이 모든 통신수단의 근간이 됨에 따라 인터넷에 대한 의존도 및 영향력의 증가와 함께 정보화의 역기능인 사이버 침해사고 및 해킹은 갈수록 늘어나고 해킹 수법 또한 전문화, 고도화 되어가고 있다. 우리는 지난 2003년1월 25일 슬래머웜으로 인해 전세계적으로 유례 없었던 인터넷대란을 겪은바 있는데, 이로 인해 사이버침해사고에 대한 적절한 예방과 대응을 위한 전문조직의 필요성이 절실히 대두되었고 마침내 인터넷침해사고대응지원센터가 2003년 12월에 설립되었다. 본 기고에서는 인터넷침해사고대응지원센터의 역할 및 대응체계등에 대해서 소개 하고자 한다.

I. 인터넷침해사고대응지원센터 구축 배경

1. 국내 정보화의 성숙

우리나라는 1990년대부터 초고속국가망, 주민등록등의 각종 전산망 구축등 본격적으로 정보화를 추진한 결과, 정보통신인프라를 통해 국가의 핵심 기반구조가 운영되고 사이버공간은 경제 · 사회활동을 위한 필수 생활공간으로 발전하게 되었다. 통계수치 상으로도 2006년 1월 현재 국내 인터넷 사용자수 3,257만명, 초고속 인터넷 가입자수 1,214만명으로 전국민의 71.9%가 인터넷을 이용하고 있으며[1], 국

1) 한국인터넷진흥원 인터넷통계정보시스템(http://isis.nida.or.kr)에서 인용

내 전자상거래 규모는 2004년 300조원 규모로 추정되고, 2005년 9월말에는 인터넷뱅킹 고객수 2,543만명에 인터넷뱅킹 업무처리 비중이 창구텔러 처리 비중을 앞지르는 등 인터넷이 이미 우리생활의 근간을 이루고 있음을 실감할 수 있다. 이러한 세계 최고 수준의 IT 인프라를 바탕으로 우리나라는 언제 · 어디서나 인터넷에 접속하여 정보를 신속하게 소통할 수 있는 유비쿼터스 사회로의 진입을 눈앞에 두고 있으며, 지구촌 유비쿼터스 사회의 도래를 선도하고 있다.

2. 정보화 역기능의 심화

국내 정보화가 도입기(1980~1996년), 성장기(1997~2000년)를 지나 성숙기(2001년~)로 진입하면서, 사이버 위협이 갈수록 다양화 · 지능화되고 있으며 사이버공격에 의한 피해도 점차 증가하고 있다. 국내 정보화 도입기에는 인터넷이 보편화되지 않아 사이버 공격으로 인한 피해가 대부분 개별시스템으로 한정되어 있었고, 바이러스의 주요 감염경로는 플로피디스크를 통해 개별 시스템을 감염시키는 것이 주류를 이루고 있었다. 성장기에는 PC 통신가입자수 300만명, 인터넷 사용자 수 1,000만명, 초고속 인터넷가입가구 수 400만을 돌파하는 등 정보화가 활성화 되면서 사이버 공격에 의한 피해도 폭발적으로 증가하였다. 국내 해킹피해건수가 1997년 64건, 1998년 158건, 1999년 572건, 2000년 1,943건으로 해마다 3배 가까이 증가하였고, 컴퓨터바이러스는 PC 통신이나 인터넷 등 통신망을 통해 급속히 전파되었다. 특히, 1999년 발생한 CIH 바이러스는 통신망 및 감염된 CD를 통해 확산되어 국내 30만대의 PC가 감염되는 엄청난 피해를 입혔다. 그리고, 초고속통신망 1,000만 가구 보급, 전 국민의 70%인 3,000만명이 인터넷을 이용하는 등 정보화 성숙단계로 진입되면서 우리나라는 세계최고수준의 초고속 정보통신 인프라의 구축으로 인터넷에 대한 접근성은 향상되었으나, 개별시스템 및 네트워크 보안미비와 사이버 공격에 대한 노출 증가로 웜 · 바이러스에 의한 공격이 증가하였다. 2001년 아웃룩주소로 자동발송되는 Nimda의 경우 국내에 유입 · 확산되는데 약 8시간이 소요되었으나, 2003년 1월 슬래머웜의 경우 8.5초마다 감염 컴퓨터 수가 2배로 증가하여 수십분 안에 전 세계에 확산되었다, 이에 따라 사이버 공격은 개별 국가 내의 문제로 국한되지 않고 국제적 이슈로 대두되고 있다.

3. 1.25 인터넷 침해사고

2003년 1월 25일 발생한 인터넷 침해사고는 "Microsoft SQL 서버 2000 및 MSDE 2000 시스템의 버퍼오버플로우 취약점"을 이용하여 전파되는 슬래머웜이 사상 유례없는 국내외 인터넷통신망의 접속장애를 유발시켜 2004년 국내에서 인터넷 상용서비스가 개시된 이후 가장 큰 피해와 파장을 불러일으켰다. 이로인해 국내에서는 전세계 감염시스템(약 7만5천개)의 11.8%인 8천8백여개가 감염되는 피해를 준바 있다. 125 인터넷대란 직후 MS SQL 서버의 취약점을 악용한 슬래머 웜은 개별 시스템을 공격하던 이전의 바이러스나 해킹사고와는 달리 네트워크를 직접 공격하여 인터넷을 사용하는 모든 활동을 정지시켜 버렸다. 이를 계기로 정보통신망의 안정성 문제가 사회적인 이슈로 대두되었고, 인터넷의 취약성과 제도적인 문제점을 분석하여 근본적인 대책마련이 요구되었다. 이에 따라, 대형 인터넷 침해사고를 예방하고 그 피해를 최소화하기 위하여 신고에 의존하던 수동적 침해사고 대응활동에서 인터넷 트래픽을 감시하여 인터넷 기반의 안정성을 모니터링하고 이상징후에 대응하는 능동적 침해사고 대응체제로의

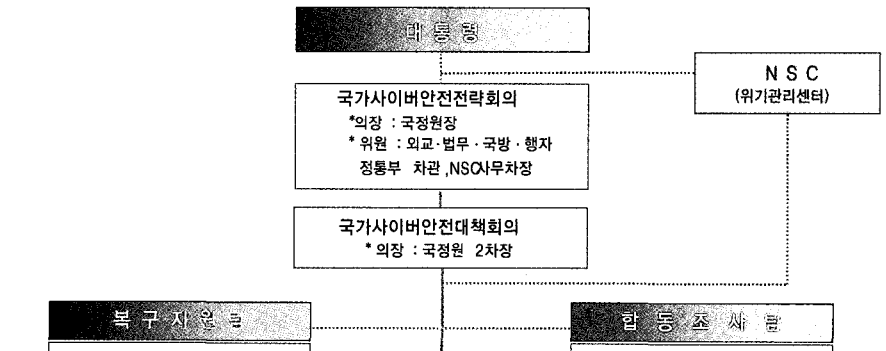
변화가 필요하게 되었다. 또한, 주요 통신사업자와 관제업체, 백신업체 등과의 상시적 정보공유와 협조체계를 통한 신속한 대응 요구가 높아지게 되었다. 그리하여 2003년 12월 한국정보보호진흥원 내에 '인터넷침해사고대응지원센터'를 구축하게 되었다.

II. 국내 인터넷침해사고 대응 체계

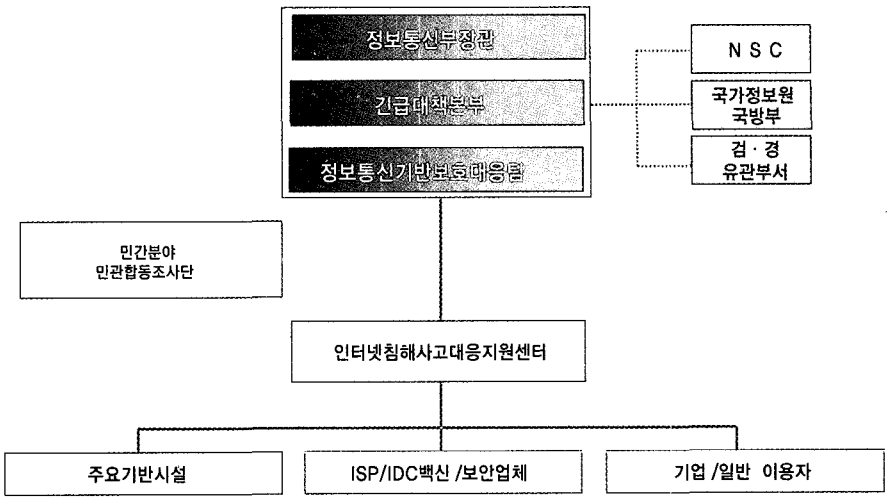
인터넷침해사고대응지원센터는 민간분야의 인터넷 침해사고에 대응하는 조직이나, 인터넷 침해사고는 네트워크를 통해 공공과 민간을 구분하지 않고 확산되므로 국가 인터넷 침해사고 대응체계에 대해 먼저 살펴볼 필요가 있다.

1. 국가 인터넷 침해사고 대응 체계 정비

인터넷 침해사고의 피해 범위가 네트워크로 확대되어 침해사고 발생 시 국가적인 비상상황으로 확산될 가능성이 커짐에 따라 인터넷 침해사고를 국가적인 차원에서 체계적으로 관리하여야 할 필요성이 대두되었다. 이에 따라 2004년에 제정된 국가위기관리 기본지침(대통령훈령 제124호)에 사이버안전이 국가핵심기반분야에 포함되었으며, 2004년 9월에 국가안전보장회의(NSC)를 중심으로 '사이버안전분야' 위기관리표준매뉴얼이 제작되었고, 2005년 7월에는 '사이버안전분야' 위기대응실무매뉴얼이 각 분야별로 작성되어 국가적인 차원의 큰 틀을 갖추게 되었다. 구체적으로 살펴보면, 인터넷 침해사고의 영역은 국가안전보장회의를 중심으로 국가사이버안전전략회의를 정점에 두고, 정보통신부를 중심으로 하는 민간분야와 국가정보원의 공공분야, 국방부의 국방분야로 나뉘어 침해사고 대응체계를 구축하였다. 분야별로 침해사고에 대응하기 위해 침해사고의 위험성을 판단하기 위한 기준과 침해사고 대응 절차를 수립하는 등 대응방안을 마련하였고, 각 주관부처들은



(그림 1) 국가 사이버안전분야 위기관리 체계



(그림 2) 민간 사이버안전분야 위기관리 체계

산하에 침해사고 대응을 위한 조직을 설립하고 이들을 통하여 침해사고 대응 업무를 수행하고 있다. 또한 각 기관들이 판단기준을 공유하고 협의하여 2005년 1월부터는 사이버 위기경보발령체계를 관심(Blue), 주의(Yellow), 경계(Orange), 심각(red) 4단계로, 그리고 위기 경보 이전단계는 정상(Green) 수준으로 일원화 하였다.

2. 민간분야 인터넷 침해사고 대응 체계

민간분야의 인터넷 침해사고 예방 및 대응업무를 효율적으로 수행하기 위하여 2003년 12월에 한국정보보호진흥원내에 인터넷침해사고대응지원센터를 설립하게 되었는데, 「정보통신망 이용촉진 및 정보보호등에 관한 법률」에 따라 주요 통신사업자(ISP), 인터넷데이터센터(IDC), 보안관제, 백신업체등으로부터 침해사고 관련 정보수집과 공유 및 신속한 대응협력체제를 구축하게 되었다. 또한, 특별한 사고가 발생할 경우 정보통신부는 원인파악 및 대책수립을 위해 각 분야의 보안전문가로 구성된 민관합동조사단을 운영할 수 있게 되어 있다. 이 사항은 2005년 7월에 작성된 '민간 사이버안전분야' 위기대응 실무매뉴얼에서 재정비되었고 민간 사이버분야의 위기경보중 '경계'와 '심각' 경보는 정보통신부에서 발령하고, '관심'과 '주의' 경보는 인터넷침해사고대응지원센터에서 발령하도록 정하고 있다. 또한 한국정보보호진흥원에서는 2004년 8월 인터넷 일반 사용자, ISP/IDC 담당자, 기업 정보보호 담당자 및 PC방 운용자등을 위해 경보 단계별 대응조치와 침해사고별 대응방법 등을 포함한 '민간 사이버안전 매뉴얼'을 발간 · 배포하였다.

III. 인터넷침해사고대응지원센터 역할

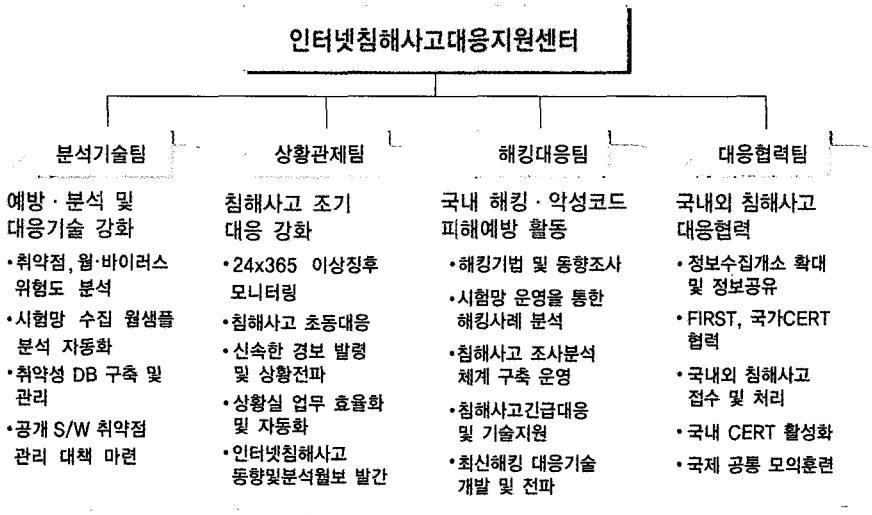
1. 인터넷침해사고대응지원센터 조직

민간분야 인터넷 침해사고 예방 및 대응을 하는 인터넷침해사고대응지원센터는 ISP/IDC 및 보안관련 업체등 인터넷 관련기관 등과 상시 정보공유 및 체계

화된 협조체계를 구축하고, 국제적 침해사고 대응창구의 역할을 수행하고 있다. 이를 위해 센터 내 각 팀에서 수행하는 주요업무는 다음과 같다. 인터넷 침해사고 예방분석 및 대응 기술 개발 업무를 담당하는 분석기술팀은 주요 취약점과 웜 · 바이러스에 대한 상세분석과 시험망 운영을 통한 웜 샘플 수집 및 분석 자동화, 웜샘플의 백신업체 제공, 시스템 및 네트워크 분야의 마이크로소프트 · 시스코 등과 협력체계 구축을 통한 대응체계 강화, 공개 소프트웨어 취약점 관리 대책 마련 등의 업무를 수행하고 있다. 침해사고 조기대응 강화를 위해 상황실을 운영하는 상황관제팀은 24시간 365일 국내 인터넷 트래픽의 실시간 모니터링과 취약점, 웜 · 바이러스에 대한 정보 수집 · 분석 등 사이버 위협에 대한 종합분석을 통하여 침해사고 심각성 수준에 따른 민간분야 위기경보 발령 및 상황전파 등의 업무를 수행하며, 홈페이지변조 및 악성코드 유포 웹사이트등을 조기에 탐지, 해당 기관/업체에게 실시간 통보하여 피해를 최소화 하는등의 초동대응 역할을 담당한다. 국내 해킹 및 악성코드 피해예방 활동을 위한 해킹대응팀은 악성 Bot, 감염 감축과 홈페이지변조 피해 예방 및 대응활동 그리고 주요 해킹사고 현장 출동 조사 및 지원활동, 해킹 방어대회 개최 등의 업무를 수행한다. 마지막으로 국내 · 외 침해사고 대응 및 협력을 위한 대응협력팀은 KrCERT 이메일등을 통해 침해사고에 대한 접수 · 처리 및 국내 침해사고대응팀(CERT)의 활성화, 중국 · 일본 등 APCERT등이 참여하는 해외유관기관과의 국제공동모의 훈련, APEC 개도국 정보보호 지원활동 등을 수행한다.

2. 인터넷 침해사고 대응 활동

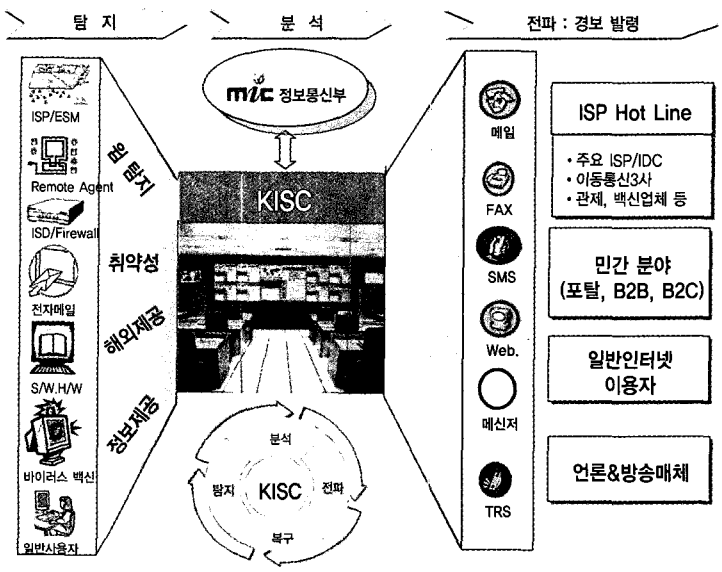
인터넷 침해사고에 효과적으로 대응하기 위해 인터넷침해사고대응지원센터는 웜 · 바이러스, 해킹기법 등의 확산 가능성, 영향력등 위험도를 객관적인 지표로 평가하여, 평가 결과 심각한 피해가 예상되면 침



(그림 3) 인터넷침해사고대응지원센터 조직도

해사고에 대한 예방차원에서 침해사고 규모 및 위협 정도에 따른 경보를 발령하게 된다. 경보는 국내 · 외에서 실제 사이버 공격등의 침해사고가 발생하여 각 급기관 및 업체로부터 이상 징후 또는 피해상황이 접수될 경우 상황을 종합적으로 분석하여 관심, 주의, 경계, 심각 등의 4단계로 발령한다. 경보 발령 시에는 평소 관심이 적은 개인 이용자들이 경보를 신속하고 편리하게 확인할 수 있도록 하기 위해 온라인 메신저(secure messenger), 메일링 리스트(sec-info), 휴대폰 문자메시지(SMS) 및 홈페이지 등 다양한 안내 수단을 통하여 전파하고 있다.

인터넷침해사고대응지원센터는 현재 전세계 177개국이 회원으로 가입되어 있는 국제침해사고대응팀협의회(FIRST)에 우리나라를 대표하여 KrCERT/CC라는 명칭으로 활동하고 있으며, 2003년에는 아시아 최초로 운영위원으로 선임되어 2005년에는 교육위원장으로 재선임되는 등 주도적인 활동을 하고 있다. 또한 아시아 태평양지역의 국제적 협력증진, 정보공유 촉진 및 기술교류를 위하여 2003년 2월 구축된 APCERT에서도 운영위원으로 활동하고 있는데, 이러한 해외 유관기관과의 활발한활동에 따라, 국외의 많은 기관들이 침해사고를 신고하여 침해사고처리에 대한 도움을 요



〈그림 4〉 인터넷침해사고대응지원센터 업무 흐름도

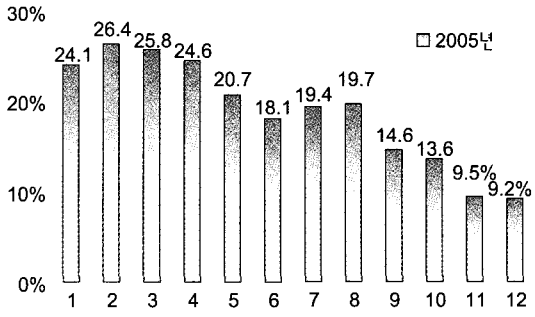
〈표 4〉 인터넷 침해사고 경보 단계

구 분	판 단 기 준	비 고
관 심 (Blue)	o 위험도가 높은 웜·바이러스, 취약점, 해킹기법 및 공격코드 출현으로 인해 피해 가능성 증대 o 해외에서 침해사고 확산 또는 일부 국내유입 및 확산 가능성 증대 o 국내 인터넷 이상 트래픽 발생 가능성 증대	징후 활동 감시 / 초기대응
주 의 (Yellow)	o 웜·바이러스, 해킹 등으로 국지적 피해발생 o 국지적인 인터넷 소통장애, 인터넷 관련 서비스에 장애가 발생 되거나 매우 우려되는 경우 o ISP/IDC, 일반 사용자, 기업 등의 긴급대응 및 보안태세 강화가 필요	협조 체제 가동 / 대응 및 복구
경 계 (Orange)	o 복수 ISP 망 또는 주요 정보통신 기반시설의 피해 발생 o 해킹 및 신종위협 으로 주요기업 및 포털, 연구소 등 민간부문에 중대한 피해 발생 o 웜·바이러스, 해킹 등 침해사고로 민간부문에 대규모 피해 발생 o 상황 해결을 위해 민관 각 분야의 협조 및 공동 대응이 필요한 상황	대비 계획 점검 / 긴급대응 및 복구
심 각 (Red)	o 국내 인터넷 전 분야에 소통장애 발생 o 주요 정보통신기반시설의 피해로 인하여 대국민 서비스 지장 발생 o 민간부분 전반에 인터넷 사용 불가능 o 국가적 차원에서 공동 대처해야 할 필요성이 있는 상황	즉각 대응 태세 돌입

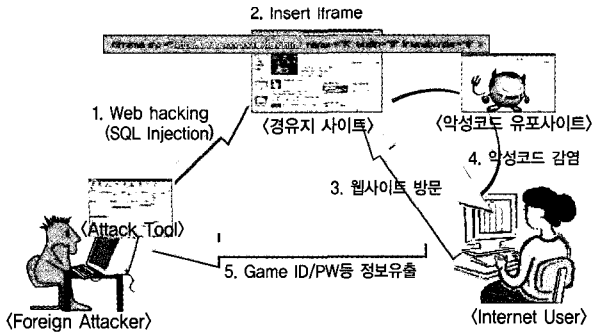
청해오고 있다. 침해사고가 접수되면 해당 업체 및 기관 등에 침해행위 중지와 시스템 점검을 요청하고 자체적으로 조치가 불가능하여 센터에 분석 및 대책을 요청할 경우 사고분석에 대한 기술지원을 하고 있다. 또한, 국내 시스템이 침해사고를 당하였을 경우에도 마찬가지로 사고대응을 위해 광역전화번호인 118로 전화 상담 및 기술지원을 제공하고 있다.

특정한 인터넷 침해사고가 다수 발생할 경우, 직접적인 피해를 당한 대상을 지원할 뿐만 아니라 잠재적으로 침해사고를 당할 수 있는 곳을 대상으로 예방을 위한 서비스를 상시적으로 운영하고 있다. 일례로, 최근 문제가 많이 되고 있는 웹해킹을 통한 악성코드 유포 사고를 대응하기 위해 '웹 취약점 점검 서비스'를 상시체제로 운영하여 2005년 1월 현재 약 500개의 사이트를 점검하는 등 적극적으로 대응해 나가고 있다.

인터넷 침해사고는 갈수록 다양화되고 지능화되기 때문에 새로운 기술을 빠르게 적용시켜 대응하여야 한다. 최근 가장 큰 문제가 되었던 2가지 유형의 침해사고에 대해 살펴보면, 스팸 발송, 피싱, 개인정보 유출등에 악용되는 악성봇은 도메인네임서버 싱크홀(DNS sinkhole) 기술[2]을 이용하여 ISP와 공동으로 해결해 나가고 있고, 악성코드 자동탐지 시스템을 센터에서 자체적으로 개발하여 악성코드를 유포하는 웹사이트를 찾아 제2, 3의 피해를 예방하기 위한 조치 및 기술지원 등의 대응업무를 해 나가고 있다. 이와 같은 새로운 기술의 적용으로 국내 악성봇 감염비율은 2005년 1월 24.1%에서 2005년 12월 9.2%로 62%나 크게 감소하는 성과를 거두었고, 악성코드 자동탐지 시스템을 개발하여 약 7만개의 국내 주요 사이트에 대해 자동 점검하여 2005년에는 국내 · 외 2천여 개의 이상의 악성코드 유포사이트를 탐지하여 조치한바 있다.



(그림 5) 2005년 월별 국내 악성봇 감염비율



(그림 6) 웹해킹을 통한 악성코드 유포 개념도

또한, 인터넷을 통해 특정 사이트에 대한 사이버공격을 국가간의 정치적인 목적을 가진 의사표현 수단으로 악용하는 사례가 자주발생하고 있다. 특히 한 · 중 · 일 3국간에는 영토 영유권 문제, 교과서 문제와 같은 역사 왜곡 등의 국가간 마찰로 인한 사이버 공격이 발생하고 있는데, 지난 2005년에 일어난 '8 · 15 중국 · 일본간 사이버전'과 '일본측의 국내 사이버외

2) 악성봇 관리 서버의 도메인명에 실제 IP 주소가 아닌 특정 IP 주소를 부여함으로써 악성봇에 감염된 PC가 실제 악성봇 관리 서버에 연결되는 것을 차단하는 기술

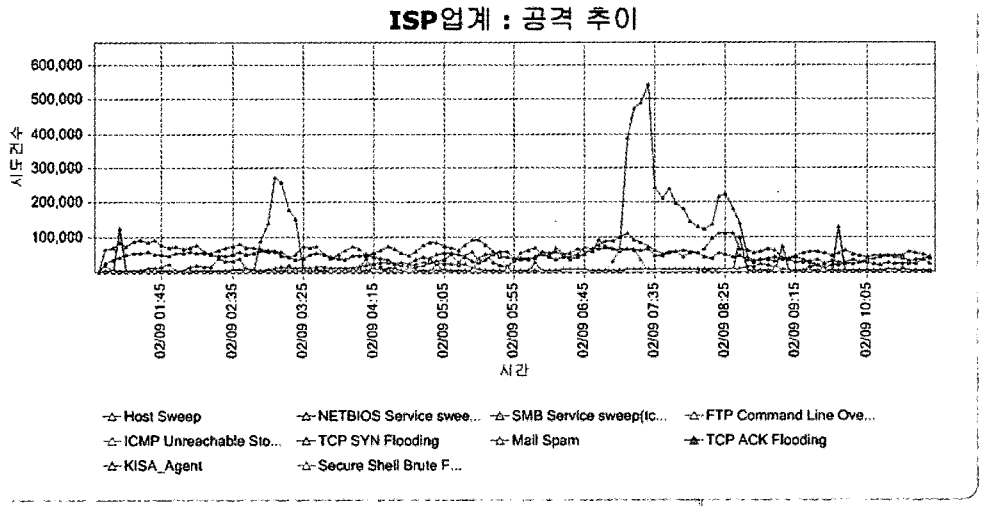
교사절단(VANK) 사이버공격[3]'의 경우 특정 사안에 대한 항의의 표현으로 사이버 공격을 감행하여 문제가 발생하였으나, 한중일 및 국내 유관기관과 확고한 공조체제를 통해 신속하고 적절한 대응조치를 취함으로써 사이버 공격에 대한 방어 및 사태의 확산을 미연에 막은 좋은 사례로 볼 수 있다.

3. 인터넷 침해사고 예방 활동

주요 통신사업자 및 보안관제, 백신업체와의 정보제공 구축을 통해 국내 네트워크 정보를 실시간으로 제공받아 24시간 365일 모니터링을 실시하고, 수시로 발생하는 소프트웨어 및 하드웨어의 취약성과 신종 웜 · 바이러스의 영향력에 대한 위험도를 평가함으로써 침해사고 발생 가능성을 조기에 탐지할 수 있도록 최선을 다하고 있다.

또한 최신 해킹 · 바이러스 동향 파악과 해킹 기법 연구 · 분석을 통해 침해사고에 대한 적절한 대응방안을 수립하고 관련 정보를 제공하여 인터넷 침해사고를 예방하고 있다. 특히, 국내에 새로운 유형의 침해사고가 발생할 경우, 해당 침해사고의 원인을 파악하기 위해 긴급 출동반을 편성하여 현장조사를 실시하고 분석 및 대책 보고서를 작성 · 제공하여 유사한 사고를 예방하도록 하고 있으며, 해킹 방어와 관련된 최신동향 파악 및 정보보호실무자의 침해사고 대응 능력 향상을 위해 2004년부터 해킹방어대회를 개최하고 있다.

인터넷망은 전세계적으로 오픈네트워크로 연결되어 지역과 국가의 경계가 없으므로 인터넷 침해사고에 대한 효율적인 대응을 위해서는 각 기관 및 국가들의 공동대응은 필수적이라 할 수 있다. 이를 위해 인터넷침해사고대응지원센터는 2004년부터 정기적으



(그림 7) 실시간 네트워크 트래픽 모니터링 시스템

3) 반크(VANK) : 우리나라의 민간 사이버외교사절단으로 2005년 8월에 인터넷 검색사이트인 구글이 반크측의 정정요구를 받고 독도표기를 변경한후 일본 네티즌으로부터 사이버 공격을 받음

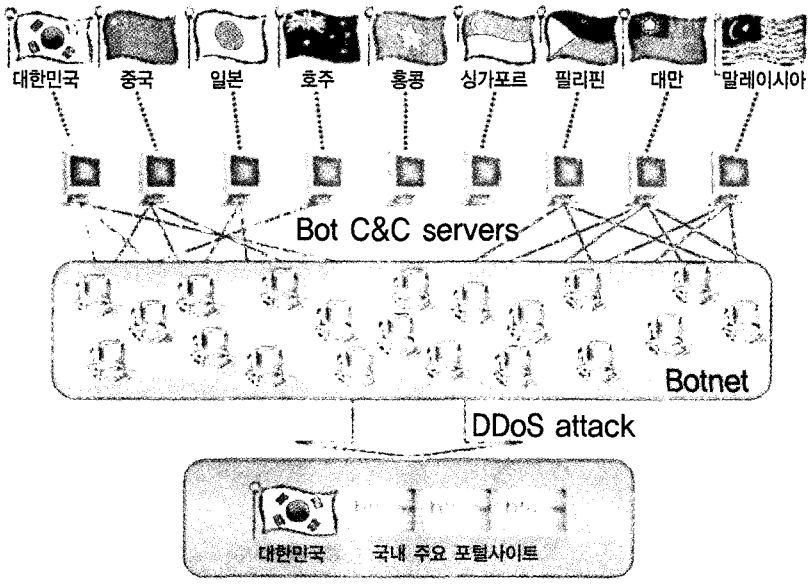
로 국내 통신사업자와 외국 침해사고대응기관이 참여하는 국제 공동대응 모의훈련을 실시하고 있다. 2004년에는 한 · 중 · 일 3개국이 참여하였고 2005년에는 아 · 태 침해사고대응팀협의회(APCERT) 9개 회원국이 참여하는 공동 모의훈련을 주최 하였다. 또한, 2005년에는 국제기구차원의 침해사고 대응능력 향상을 위한 2005 ASEM 사이버보안워크샵 및 개발도상국가의 침해사고 대응 역량 강화를 위한 아태지역 정보보호센터(APISC) 정보보호교육 실시 등 국제 대응 노력에 기여하고 있다.

향후 발생 가능한 침해사고에 대응하기 위하여 2004년에 해외 정보보호 선진기관인 미국 카네기멜론 대학(CMU)과 국제공동연구 협약을 체결하여 '차세대 침해사고 대응 및 예방기술 개발' 등 침해사고에 능동적이고 지능적으로 대응할 수 있는 정보보호기술 개발에 매진하고 있다.

인터넷 침해사고 예방 활동에 활용할 수 있도록 각종 통계 지표와 월별 동향 및 이슈에 대한 분석 정보를 제공하기 위하여 월별 인터넷 침해사고 현황 및 분석 보고서를 인터넷침해사고대응지원센터 홈페이지에 게시하여 제공하고 있다.

IV. 맺음말

IT839 정책에 따라 광대역통합망(BcN), u-센터 네트워크(USN)등의 정보통신 인프라 구축과 WiBro 서비스, DMB 서비스 등 신규 IT 서비스가 제공/활성화되는 등 유비쿼터스 환경이 한층 다가오고 있다. 또한 다양한 모바일 디바이스(Windows CE 기반의 스마트폰, PDA)의 보급, 모바일 플랫폼 표준 규격으로서 WIPI(Wireless Internet Platform for Interoperability)가 탑재된 휴대폰이 많이 보급됨에 따라 더욱 편리하고 풍부한 컨텐츠를 이용한 인



(그림 8) 2005년도 국제 공동 모의훈련 체계도

터넷 생활이 기대되며, 유무선 및 방송망, 음성통신망 등도 인터넷망으로의 통합이 점점 가속화될 것이다. 이러한 환경변화는 침해사고의 영역이 생활의 모든 영역으로 확대될 수 있음을 의미하는데, 인터넷침해사고대응지원센터에서는 휴대폰 바이러스 대응 기술, BcN 환경에 대비한 네트워크 모니터링 시스템 개발 등을 추진하여 환경변화에 적극 대비하고 있다.

최근의 인터넷 침해사고는 특정정보 유출, 금전적 이득은 물론 정치적 목적으로 하는 국가간의 사이버 공격 및 해킹이 자주 발생하고 있는데, 이럴 경우 기술적으로 훨씬 정교화 되고 조직화되어 탐지 및 대응이 점점 어려워 질 것으로 예상된다. 특히 지난해 악명을 떨친 웹해킹을 통한 악성코드 유포나 악성봇 등이 확대될 것이므로 현재의 악성코드 탐지 시스템과 악성봇 대응 시스템을 고도화해 가고 있다.

인터넷침해사고대응지원센터는 침해사고 신고전화로 광역번호 118을 운영하여 일반이용자 및 기업 등에 기술지원을 하고 있다. 그러나 컴퓨터에 익숙하지 않은 일반이용자의 경우 전화상의 설명만으로는 침해사고 대응에 어려움이 많을 수밖에 없다. 이러한 불편을 해결하기 위해 올해부터 일반 인터넷이용자에게 PC 원격점검 서비스를 통한 기술지원을 제공할 예정이다.

인터넷 침해사고는 국경에 국한되지 않고 발생하므로 침해사고 발생 시 범국가적으로 신속하고 효과적인 대응을 위해 해외 유관기간과의 신속한 공동대응이 필수적이다. 이를 위해 국제 공동 대응 능력을 제고하기 위해 2004년부터 한국,중국,일본등이 포함된 APCERT 회원국과 실시해온 공동모의훈련의 참가국을 계속 확대해 나갈 예정이다.

인터넷침해사고대응지원센터는 위와 같이 급변하는 인프라 환경과 해킹 기술에 적극 대응하기 위해 변화를 예측하고 미리 준비하여 민간 사이버 안전을 위해 모든 노력을 기울일 것이다. 또한 일반이용자들이 인터넷 침해사고를 당했을 경우, 적극적으로 지원할 수 있는 시스템을 개발하고 서비스를 운영하여 고객을 감동시킬 수 있는 기관으로 거듭날 수 있도록 최선을 다할 것이다.

끝으로, 다양한 양상으로 전개되는 인터넷침해사고를 사전에 예방하고 신속하게 대응하기 위해서 정부, 기업, 일반이용자 공동의 노력이 필수적이다. 아직도 국내에는 보안을 고려하지 않고 구축한 웹 서버 많거나 또한 무관심속에 방치된 휴면 홈페이지, PC도 많을 것으로 보인다. 이러한 잠재적인 위협요소들은 결국 피싱 경유지, 악성코드 유포 사이트로 악용되거나 악성봇에 감염되어 타인에게 피해를 주는 결과를 초래할 수 있다. 해킹에 가장 쉽게 이용되는 홈페이지 운용자의 경우 보안을 고려한 홈페이지 구축이 필요하고, 정보보호에 대한 깊은 지식이 없더라도 주기적인 보안 패치, 백업 및 복구계획의 수립, 백신 S/W의 사용만으로도 많은 부분 침해사고의 피해를 예방할 수 있으므로 올해에는 정보보호에 대한 더욱 지속적인 관심과 주의를 기울여 진정한 인터넷 인프라 강국을 자부하는 한국이 될 수 있기를 기대해 본다.

[참 고 자 료]

[1] 민간부문 정보보호 정책 연혁, 정보통신부, 한국정보보호진흥원, 2004. 12

[2] 2005 국가정보보호백서, 국가정보원, 정보통신부, 2005. 6

[3] 2005년 12월 인터넷 침해사고 동향 및 분석월보, 한국정보보호진흥원, 2006. 1

[4] 2003 정보시스템 해킹 · 바이러스 현황 및 대응, 한국정보보호진흥원, 2003. 12

[5] 2005 e-비즈니스백서, 한국전자거래진흥원,

2005. 3
[6] 한국인터넷진흥원 인터넷통계정보시스템 (http://isis.nida.or.kr)
[7] 인터넷침해사고대응지원센터 홈페이지 (http://www.krcert.or.kr)
[8] 정보통신망 침해사고 조사결과(MIC, 2003.2.18)

노명선

1990년 건국대학교 전자공학과 졸업
1990년 ~ 2000년 ㈜데이콤 통신망계획팀장
2000년 ~ 2004년 ㈜두루넷 인터넷망팀장
2004년 ~ 현재 한국정보보호진흥원 인터넷침해사고대응지원센터 상황관제팀장