IT839전략에서 정보통신 인프라 정보보호정책

정보통신부 정보보호정책과 김기권

차 례

I. 서 론

정보통신 기술의 발전은 개인 및 조직에 많은 변화를 주도해 오고 있다. 현재까지의 변화는 정보시스템, 가전, 유·무선 통신설비 등 기기 및 네트워크가 서로 다른 환경에서 개별적으로 개발·활용되어 왔다. 하지만 향후 변화의 핵심은 어느 곳에서나 시간에 상관없이 정보를 얻고 활용할 수 있는 하나로 통합된 생활로서의 유비쿼터스 컴퓨팅 사회(ubiquitous computing society)로 전환되고 있다는 것이다. 유비터쿼터스 사회로의 전환을 주도하기 위하여 정보통신부에서는 8대 신규 서비스(휴대인터넷, DMB, 홈네트워크, 텔레메틱스, RFID, W-CDMA, 지상파 DTV, 인터넷전화), 3대 첨단 인프라(BcN, USN, IPv6), 9대 신성장 디바이스(차세대 이동통신, 디지털 TV, 홈네트워크, IT SoC, 차세대 PC, 임베디드 S/W, 디지털 콘텐츠, 텔레메틱스, 지능형 로봇)의 IT839 전략을 구체화하였다. IT839전략의 추진에 따라서 2005년부터 휴대인터넷 등 다양한 서비스 도입, S/W, 부품, 기기 등의 개발에 따라서 IT 생산이 2007년까지 380조원의 생산유발효과가 나타날 것이고 IT부분의 국내총생산 비중이 3천불로 늘어나고 IT 고용인력이 150만명으로 증가할 것이다[1]. IT839 전략은 미래에 청사진을 제시하고 있지만, IT839 전략 달성에 있어서 간과하지 말아야 할 부분이 정보보호(information security)이다. 8대 신규 서비스, 3대 인프라, 9대 신성장 디바이스에 대한 적절한 정보보호의 대안이 마련되지 못할 경우, 앞에서 열거한 미래의 모습이 사이버 공격, 개인정보 유출, 불법복제·유통 등 사이버 공간 내의 불법행위의 온상으로 전락

할 수 있다. 이로 인해 심각한 경제적 피해로 사회전반에 엄청난 비용이 발생할 수 있다.

II. IT839 전략의 정보보호 위협요인 및 추진전략

1. 8대 신규서비스 위협 및 대응

8대 신규서비스의 위협은 개인정보 유출, 유통정보의 도·감청, 사이버공간 위험의 현실세계 위험으로의 전이 등이다.

개인정보의 유출은 보호되어야 하는 개인의 프라이버시(Privacy)가 침해되는 것이다. 텔레메틱스 서비스가 일반화되는 경우, 개인의 이동경로 및 현재위치와 같은 위치정보가 유출될 수 있다. 또한 개인의 RFID칩과 연결된 의료 데이터베이스내의 개인 진료 기록이 해킹이나 불법적인 수단을 통해서 유출될 경우 개인의 프라이버시가 크게 침해될 수 있다.

유통정보의 도·감청은 휴대인터넷을 포함한 이동통신 서비스와 인터넷전화(VoIP) 등을 통해서 전송되는 정보가 도·감청을 통해서 유출될 수 있는 위험이 높아질 수 있다. 현재 널리 활용되고 있는 무선 LAN의 경우도 도·감청의 위험에 노출되어 있으며, 이를 해결하기 위하여 최근 새로운 보안표준(IEEE 802.11i)이 발표되었다[2].

사이버공간의 위험이 현실세계의 위험으로의 전이될 가능성이 높아져, 사이버 공간 상의 기기들의 오류로 인한 오작동 및 고장으로 인한 문제가 금융, 항공, 교통, 에너지 등 주요정보통신기반시설과 같은 실제 물리적 공간상에서 대형 사고를 발생시켜 사회전반으로 문제가 확산될 수 있다.

8대 신규 서비스 위협에 대응하기 위해 위치, 의료, 상황정보 등 개인정보의 종합적인 보호체계를 정립하고 이동통신 서비스의 보안 기밀성을 강화하기 위한 핵심기술을 개발하며, 서비스 장애로 인한 피해 및 안전위협을 최소화하기 위한 안전 관리 체계의 수립한다. 이를 통해 안전하고 신뢰할 수 있는 신규 서비스를 보급할 수 있다.

2. 3대 인프라의 위협 및 대응

3대 인프라의 위협은 네트워크 융합에 따른 보안위협 확산, 사이버 공격의 지능화 및 고도화, USN 무선 환경의 내재적 취약성 등이다.

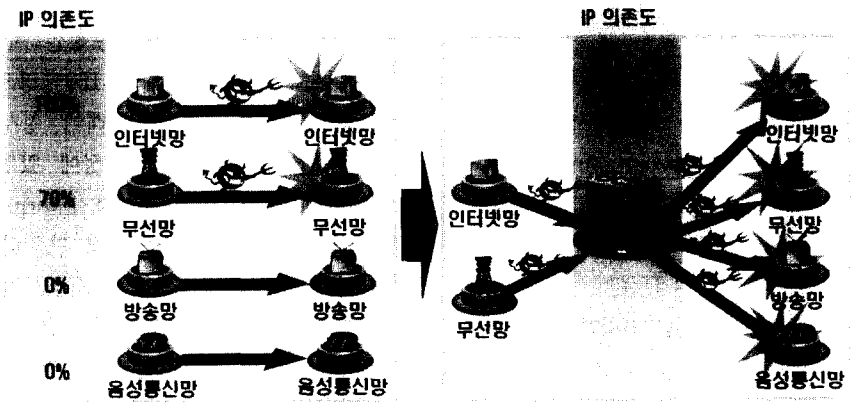


그림 1. 광대역 통합망의 위협

광대역통합망으(BcN)로 전활될 경우, 개별적으로 운영되고 있는 유·무선 통신망, 인터넷망, 방송망이 하나의 네트워크로 통합되고, 개별 통신망 내의 정보가 자유롭게 이동하게 된다. 융·복합화된 통합 네트워크는 다양한 요구사항을 수용하면서 매우 복잡하게 구성되어 네트워크의 내재적인 취약점이 증가하게 된다. 또한 금융, 항공, 물류, 에너지 등 국가기반구조의 정보통신 기반구조의 의존도가 심화되고 있다. 기반구조의 정보통신 침해사고 발생시 기반구조 전반에 장애를 초래할 수 있다.

사이버공격이 인터넷 확산에 따라서 일반화되고 있으며, 개별적으로 존재하던 해킹, 웜, 바이러스 등이 하나로 통합되면서 지능화·고도화되고 있다. 향후 광대역통합망으로 전환될 경우, 현재 유선 중심에서 유·무선으로 통합된 사이버공격이 확산될 수 있다.

USN 무선 환경은 내재적인 취약점이 존재한다. 무선환경은 폐쇄적인 유선 환경과 달리 개방된 환경으로 악의적인 공격자의 접근이 쉬우며, 무선 단말기기의 처리, 저장 능력 등의 한계로 인해 보안 기능을 추가하기 힘들어 사이버 공격에 취약하다.

3대 인프라의 위협에 대응하기 위하여 개별망 및 BcN의 보안성을 강화하기 위한 기술을 개발하고 적용하며, 네트워크의 침해 탐지 및 대응체제를 고도화하고, USN 무선환경의 안전성을 확보하기 위한 정보보호 기술 및 초경량 암호기술을 개발이 필요하며, 이를 통해 QoS 서비스를 제공하는 첨단인프라를 구축하게 될 것이다.

3. 9대 신성장 디바이스 위협 및 대응

9대 신성장 디바이스 도입에 따른 위협은 광범위하게 보급된 단말기기를 통한 개인정보의 다량수집 및 유출위험 증가, 무선단말기기의 보안 취약성 내재, 디지털 컨텐츠 불법복제 및 유통 증가 등이다.

모든 개인들이 이동통신 단말기기를 소유하고 모바일 웜·바이러스가 일반화되면서 단말기기에 내장된 개인정보가 무단 유출되는 위협이 증가하게 된다. 이와 함께 무선 단말기기들은 이동성을 보장하지만, 처리 및 저장능력이 PC와 같은 기기에 비해 부족하여 내재적인 보안취약성이 존재한다.

영화, 음악 등 콘텐츠들이 아날로그 형식에서 디지털 형식으로 전환되면서 제작부터 유통·소비까지의 모든 과정이 디지털화되었다. 디지털 컨텐츠의 특성은 통신망을 통한 자유로운 배포가 가능하며, 복사비용이 거의 들지 않아 적절한 보호조치가 되지 않으면 무제한적으로 확산될 수 있다.

9대 신성장 디바이스의 위협에 대응하기 위하여 개인정보 활용을 제한할 수 있는 능동형 프라이버시 보호기술을 개발하고, 임베디드 보안 SW 기술과 보안기능을 내장한 디바이스를 개발하며, DRM 요소기술 및 기반구조의 개발 및 적용을 통한 안전 컨텐츠 유통환경을 구축한다. 이를 통해서, 언제, 어디서나 모두가 신뢰할 수 있는 디바이스를 개발한다.

4. IT839 정보보호 전략의 비전과 추진과제

그림2에서와 같이 안전하고 신뢰할 수 있는 건전한 지능기반 사회 구축의 비전을 실현하기 위하여, QoS를 보장하는 최첨단 인프라 구축, 안전한 USN 이용환경 구축, 신규 IT 서비스와 디바이스의 안정성 확보, 정보보호산업 육성 및 정보보호문화 활성화를 추진할 것이다[3].

QoS를 보장하는 최첨단 인프라 구축을 위한 추진 과제는 사이버공격 예방 및 대응체계 고도화와 통합네트워크의 안전 및 신뢰성 개선이다. 안전한 USN 이용환경 구축을 위한 추진 과제는

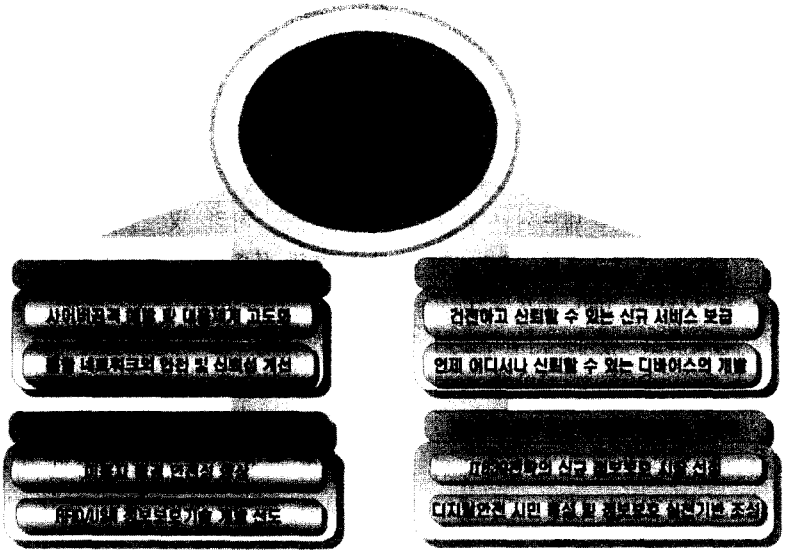


그림 2. IT839 정보보호 전략의 비전과 추진과제

이용자 환경 안전성 향상과 RFID/USN 정보보호기술 개발 선도이다. 신규 IT서비스와 디바이스의 안전성 확보를 위한 추진 과제는 건전하고 신뢰할 수 있는 신규 서비스 보급과 언제 어디서나 신뢰할 수 있는 디바이스의 개발이다. 정보보호산업 육성 및 정보보호 문화 활성화를 위한 추진 과제는 IT839전략의 신규 정보보호 시장 선점과 디지털안전 시민육성 및 정보보호 실천기반 조성이다.

III. 사이버 공격예방 및 대응체계 고도화

1. 사이버 공격 동향

최근 사이버공격은 패러다임이 변화하고 있다. 사이버 공격이 지능화·고도화되고 있으며, 공격의 간격이 짧아지고 있다.

사이버 공격은 해킹과 웜·바이러스 등의 형태로 나타나고 있으며, 최근 추세는 S/W 및 네

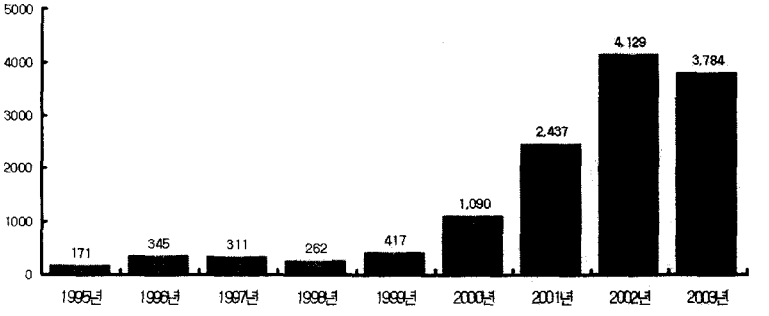


그림 3. CERT/CC에서 발표한 취약점 수

트워크 취약점의 급속한 증가, 해킹의 지능화·고도화와 웜·바이러스의 급속한 확산, 해킹 및 웜·바이러스의 융·복합화에 따른 피해의 급속한 증가로 요약할 수 있다[5].

S/W 및 네트워크 취약점의 급속한 증가는 PC 및 서버를 포함한 모든 컴퓨팅 자원이 고성능화되고, 인터넷으로 대별되는 네트워크에 연결되고, 이기종 기기들이 융·복합화되고 있어 S/W 및 네트워크의 복잡성 및 규모가 급속히 커지면서, 관련 취약점들이 빠른 속도로 증가하고 있다.

인터넷이 확산되면서 시간과 공간의 장벽을 허물고 다양한 정보를 자유롭게 나눌 수 있게 되었지만, 인터넷 확산으로 인해 해킹의 지능화 고도화 및 웜·바이러스가 급속히 확산되고 있다. 2000년 이후 자유롭게 인터넷에 접근하고 이용하게 되면서 자동화된 해킹 프로그램과 프로그램의 소스코드가 공개되면서 해킹에 대한 전문 지식이 없는 일반인도 해킹을 할 수 있게 되었고, 인터넷에 공개된 해킹 프로그램 소스코드를 활용하여 악성화되고 다양한 변종해킹 프로그램들이 양산되고 있다. 웜·바이러스도 공격코드 및 소스코드가 인터넷을 통해 확산되면서 수많은 악성화된 변종 웜·바이러스가 확대·재생산되고 있다. 2003년 하반기에 발생후 최근 급속도로 확산되고 있는 Bot의 경우도 소스코드가 공개된 이후 악성화와 2000여종 이상의 다양한 변종이 발생하였다.

사이버 공격의 추세가 취약점 발견 후 웜·바이러스로 발전하는 속도가 빨라지고 있으며, 수십초 내에 전세계의 네트워크에 전파될 수 있는 슈퍼웜에 대한 우려도 커지고 있다[5]. 최근 윈도우즈 운영체제의 취약점을 악용한 웜·바이러스는 경우가 증가하고 있다. PC 및 서버 등 컴퓨팅 자원의 고성능화와 초고속 인터넷의 보편화로 웜·바이러스가 초고속으로 전파되는 수단으로 악용되고 있다. 2003년 1월에 발생한 슬래머 웜의 경우도 인터넷 기반이 잘 구축된 우리나라에서 많은 피해가 났다. 슬래머 웜은 전세계 네트워크를 수십분 내에 감염시켰지만, 최근 수십 초 내에 감염시킬 수 있는 슈퍼웜인 warhol, flashflood 등에 대한 우려가 커지고 있다. 또한 취약점 발표 후 개인과 기업이 관련 패치를 설치하지 못한 상태에서 24시간 이내에 공격이 발생하게 되는 Zero-Day 초단기 공격이 출현할 것으로 예상된다.

2. 사이버 공격 대응체계 고도화

사이버 공격에 의한 인터넷 침해사고 대응체계 고도화를 위해서 (그림 4)과 같이 개인, 민간, 국가, 글로벌 4단계 방어체계 구축을 통한 안전

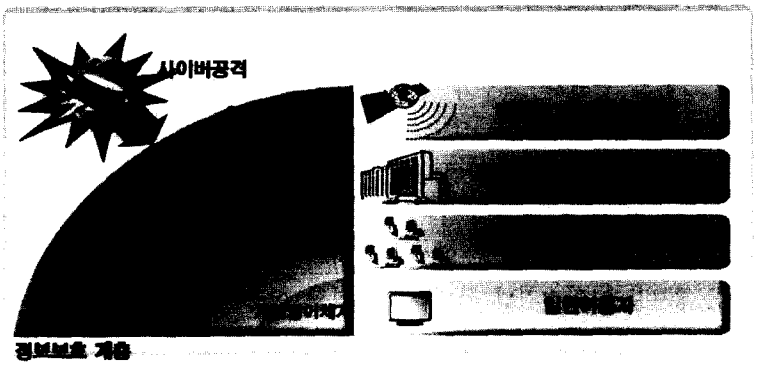


그림 4. 사이버공격 방어체계의 계층적 구조

한 IT 환경을 조성한다.

가. 글로벌 방어체계 구축

해킹 및 웜·바이러스 등에 의한 사이버 공격은 한 국가나 지역에 한정된 것이 아니라, 전세계적인 현상으로 동시다발적으로 발생하므로, 사이버 공격이 국내에 유입되기 전에 조기 탐지를 위한 글로벌 조기탐지체제를 구축해야 한다. 한·중·일 3국간의 Hot-Line을 구축하고 미국, 호주 등 APEC 지역으로 확대를 추진하며, 기타 아시아 지역 국가 간의 정보를 상시적으로 교환할 수 있도록 국가별 침해사고대응팀(CERT) 간의 네트워크를 구축한다. 이를 통해 침해사고 발생시 FIRST, APCERT 등 회원국간 대응 협력체계를 확보하여 국가간 침해사고 공동 대응 협력을 강화하고 상시 연락체계를 구축한다.

나. 국가 방어체계 구축

해킹과 결합된 초고속 슈퍼 웜에 대규모 침해사고에 대비한 국가차원의 대응을 강화하기 위해서 한국정보보호진흥원의 침해사고대응지원센터를 고도화하고, 해외 우수 연구센터와의 공동연구를 통해 침해사고 대응시간을 단축할 수 있는 기술을 개발한다. 침해사고대응지원센터의 고도화를 위해서, ISP, IDC, SO 등의 정보수집대상을 확대하고 소형사업자 및 해외NSP의 모니터링을 추진하며 최종적으로 광대역 통합망과의 연동을 추진한다. 대응약량 강화를 위해서, 전문가 분석 시스템, 대응지식 기반시스템, 인공지능 기능시스템 및 웜·바이러스/해킹 방지기술을 개발한다.

사이버공격으로부터 국가 주요정보통신기반시설의 보호를 위한 안정성 강화를 위해 주요기반시설 안전체계 강화, 정보보호 안전진단 확대, 정보보호관리체계인증 제도 고도화를 추진한다. 주요기반시설 안전체계 강화는 실시간 취약점 점검 및 모니터링 기술을 개발, 시스템 구축/운영을 통해 추진하며, 주요정보통신기반시설에 대한 취약점 분석·평가를 수행하는 정보보호컨설팅전문업체의 심사기준을 강화하고 제도 정비 및 사후관리를 강화할 예정이다. 정보보호 안전진단의 확대를 위해서 ISP, IDC, 인터넷상거래 업체로 한정되어 있는 안전진단의 대상을 확대하고, 디지털미디어센터(DMC) 등 BcN 환경에 맞는 안전기준을 개발해 2008년부터 BcN 안전진단 수행을 추진할 예정이다. 관리체계인증제도의 고도화를 위해, 제도 개선과 인증심사 대상을 확대하고 인증제도의 국제상호인정을 추진할 예정이다.

다. 기업 방어체계 구축

정보보호에 취약한 중소기업을 포함한 한 민간기업의 안전체계 강화를 위해서 민간분야 침해사고 공동대응체계와 중소기업 정보보호 지원체계를 구축할 예정이다.[6] 민간분야 침해사고 공동대응체계 구축을 위해서 정보보호 정책위원회를 설치하고 정보보호 주체별 태스크포스팀을 구성하여 정보보호 정책에 대한 방향 및 의견을 수렴하고 CERT 구축기준 및 성공사례(best practice) 등을 개발 보급한다. 중소기업 정보보호 지원체계 구축은 5인 이상의 300만여개의 업체를 대상으로 대한상공회의소, 중소기업중앙회 등 유관기관과 정보보호 학과, 정보보호 동아리 등의 대학과 학계 및 보안업체가 참여하는 중소기업 정보보호 협의체 등이 정보기업 취약점 검검, 지원사업 등 분야별 지원사업을 진행할 예정이다.

라. 개인 방어체계 구축

개인을 위한 사이버방역체제 구축을 위해서 사이버방역센터 설립과 클린넷(clean net)을 활성화할 예정이다. 사이버방역서비스는 대규모 인터넷 침해사고 발생시 패치파일과 전용백신을 제공받아 일반 개인들이 사이버방역센터에 접속하여 쉽게 설치할 수 있도록 할 예정이다. 이와 함께

표 1. ISP별 인터넷교환노드 보유현황

	한국전산원	KT	데이콤	케이아이엔엑스
인터넷교환노드명 (장소)	KIX (종로)	KTIX (혜화)	DIX (논현)	KINX (강남)

인터넷서비스제공업체(ISP)와 협력하여 개인이용자들에게 침입차단, 침입탐지, 백신 등의 보안서비스를 기본항목으로 제공하는 클린넷 서비스를 활성화할 예정이다. 이를 통해 개인 인터넷 이용자의 안전한 인터넷 사용을 보장하며, 향후 BcN 차세대 네트워크로 고도화할 예정이다.

IV. 네트워크 안전 및 신뢰성 개선

1. 인터넷망의 구조적 취약성 및 개선 방안

국내 인터넷망의 구조적 취약성은 인터넷망의 핵심 시설인 인터넷교환노드(IX), 국제관문국(IGO), 집적정보통신시설(IDC) 등이 서울 지역에 집중되어 발생하는 것으로 요약할 수 있다[7]. 국내 인터넷망은 94년 국내 인터넷 도입 후 서울을 포함한 수도권을 중심으로 증가한 폭발적인 수요를 충족시키고 효율적인 투자를 위해서 서울 중심으로 인터넷망이 구성되었다. 일부 지역의 집중형 인터넷망 구성은 지역내 주요 시설에 재난, 재해 및 대규모 침해사고가 발생할 경우 전국 인터넷망에 피해가 급속도록 확산될 수 있는 취약한 구조를 가지는 한계점이 있다. 구조적인 취약점을 인터넷교환노드, 국제관문국, 집적정보통신시설 차원에서 살펴보도록 하겠다.

인터넷교환노드는 인터넷서비스제공업체(ISP) 간의 트래픽을 상호연동해 주는 인터넷 기반구조의 최상위 노드이며, 국내 4대 인터넷교환노드가 모두 서울에 집중되어 있는 실정(표1)으로 국내 거의 모든 트래픽이 서울의 인터넷교환노드를 통한 연동이 되어 지역 하위노드에서 이상 트래픽이 발생할 경우 상위노드를 경유할 때마다 트래픽이 기하급수적으로 증가하여 인터넷교환노드로 집중되게 된다. 인터넷교환노드로의 집중현상이 더욱 심화되고 있는 추세이다.

하나의 인터넷교환노드에서 과부하가 발생하는 경우, 인터넷교환노드에 연결된 ISP도 영향을 받아 연동 ISP간의 트래픽의 교환이 곤란해진다. 서울지역의 인터넷교환노드 침해사고 발생시 서울지역에서 소통되는 ISP 간의 인터넷 트래픽에 대한 우회체계가 부족하여 전체 인터넷 소통장애로 확대될 우려가 있다. 2003년 5월부터 부산 인터넷교환노드를 구축·운영하면서 부산·경남 지

표 2. 인터넷 교환노드별 연동 현황

지역	종류	연동 ISP 수	총수용용량	피크 트래픽양 (2003)
서울	KIX	10	30.5Gbps	5.5Gbps
	KTIX	21	130Gbps	45Gbps
	DIX	39	92Gbps	35Gbps
	KINX	35	44Gbps	19Gbps
부산	BIX	13	5Gbps	904Mbps

※ 자료: 한국전산원, 2004 한국인터넷 백서

역의 인터넷 트래픽은 서울의 인터넷교환노드를 통하지 않고 처리가 가능하지만, 연동 ISP수, 총 접속용량 등 설비 규모가 미흡하여 서울지역의 대규모 트래픽을 우회시키지는 못한다.

국제관문국(IGO, International Gateway Office)은 국제 인터넷 서비스의 연동을 위하여 국가간 인터넷 서비스를 전달해주는 노드로, KT, 데이콤, 하나로 등 ISP의 국제관문국이 서울에 집중되어 있다. 이상 트래픽 폭주로 인한 국제관문국의 침해사고 발생시 국가간 인터넷 서비스의 연동이 곤란하여 국제적으로 고립될 수 있다. 슬래머 웜, 블래스터 웜 등 불특정 다수 또는 국외 특성 사이트를 대상으로 한 사이버 공격이 발생하는 경우 대다수의 트래픽이 국제관문국으로 집중되어 병목현상을 야기시킬 수 있다. 1.25 인터넷침해사고 원인분석 결과에 따르면, 슬래머 웜이 무작위로 발생시킨 유해 트래픽이 국제관문국으로 집중되었다. 국제 인터넷주소할당 분포를 고려할 때 이상 트래픽의 흐름은 한국에 할당된 주소가 0.7%로 확률적으로 99.3% 트래픽이 국제관문국으로 집중되어 해외로의 접속이 곤란하였다.

집적정보통신시설(IDC, Internet Data Center)은 대규모 정보통신 서비스를 제공하는 사업자의 위탁을 받아, 서버, 네트워크 장비 등의 정보시스템 장비를 일정한 공간에 집중하여 관리하는 시설로서, 포털, 커뮤니티, 게임, 등 대용량 인터넷 컨텐츠를 제공한다. 집적정보통신의 규모 측면에서 살펴보면, 95%이상 시설이 수도권에 집중되어 있다. 웜·바이러스 등 사이버 공격으로 인한 침해사고 발생시 피해가 대형화되어 ISP망까지 피해가 확산될 수 있다.

PC방, 가정용 xDSL의 대역폭 증가 등 초고속 가입자는 급속히 증가했지만 가입자 라우터 수용용량의 한계로 가입자망의 마비가능성이 높아지고 있다. 대역폭이 25메가인 VDSL 사용자의 1 2%만 슬래머 웜에 감염되어도 10 기가급 액세스 라우터의 수용능력을 초과하여 해당지역 가입자망을 마비시킬 수 있다.

표 3. 국내 IDC 지역별 현황

지역	IDC 수	규모(평)	단위규모(평/시설)
수도권	26(72.2%)	58,016(95.5%)	2,231
충 청	3(8.6%)	1,038(1.5%)	346
영 남	2(5.7%)	910(1%)	303
호 남	3(8.6%)	581(1.7%)	291
강 원	1(2.9%)	165(0.3%)	165

※ 자료 : 한국정보보호진흥원, 2003. 12

서울 및 수도권에 집중된 인터넷망의 구조적 취약성을 해결하기 위해, 인터넷 주요시설을 지방으로의 분산 구축을 유도한다. 행정수도 이전과 연계한 정책을 개발하고 지역 정보통신기술 산업기반 환경을 조성할 수 있도록 세제혜택 지원을 포함한 지원방안을 마련할 것이다. 세부적으로 살펴보면 2006년까지 인터넷교환노드의 지방 우회루트와 클린 가입자 인증제도의 도입을 추진하고, 2008년까지 집적정보통신시설(IDC)의 지역별 분산을 추진하며, 2008년 이후 국제 관문국의 이원화를 유도한다.

2. 관리적 취약성 및 개선방안

국내 인터넷망에 침해사고 발생시 인터넷망을 안전하게 통제·운영하기 위해 서비스망과 구분된 네트워크 관리체계 구축이 필요하다. 하나의 물리적 통신망에 인터넷 사용자 대상의 서비스를 위한 서비스망, 일괄적인 네트워크 장비 통제를 위한 관리망, 네트워크 장비 간의 필수정보를 상호교환하기 위한 정보교환망이 함께 혼재되어 있는 실정이다. 망이 혼재된 경우, 이상 트래픽 폭

주시에 스위치, 라우터 등 네트워크 장비에 대한 제어신호 등 비상신호의 전달이 곤란하다. 2003년 1.25 인터넷 침해사고 후, KT, 데이콤, 하나로 등 주요 ISP 들은 네트워크 장비 일괄 통제를 위한 관리망 분리에 대한 필요성을 인식하고 주요 거점노드 장비에 대한 별도 관리망 구축을 추진하고 있으나 전체적으로 미흡한 상태이다. 또한 침해사고 발생시에도 트래픽의 경로 설정을 필수적인 라우팅 테이블 등 네트워크 필수 정보의 생존성을 보장하기 위해 서비스망과 분리된 정보교환망 구축이 필요하다.

인터넷망의 관리적 취약성을 개선하기 위해서, 재난, 재해에 대응할 수 있는 DRP(disaster recovery planning) 구축을 통한 서비스 연속성을 확보 및 재난대비 표준관리절차를 적용하도록 한다. 사이버공격에 대비하여, 서비스망과 분리된 관리망/정보교환망을 구축하고, ISP 간의 정보공유를 위한 정보공유분석센터의 운영을 활성화하며, 상시로그 수집 및 분석기술을 개발한다.

3. 기술적 취약성 및 개선방안

네트워크 인프라가 대규모화, 고속화되면서 기존 보안기술을 적용에는 한계가 존재한다. 최근 라우터 장비의 처리속도가 기가(Giga)급에서 테라(Tera)급으로 발전해 가고 있지만[8], 방화벽의 처리속도는 아직 10기가 수준에 머물러 있는 실정으로, 침임탐지 및 방화벽 등 전통적인 보안장비를 인프라 보호에 적용하는 것은 부적합하다. 이와 함께 망구성의 대형화·복잡화되면서 인프라 내에 다수의 출입지점이 존재하여 유해 트래픽의 원천 차단이 곤란하다. 인프라 보호를 보안기능의 통·융합 및 효과적인 보안정책 적용기술이 미흡하다.

기술적 취약성을 개선하기 위하여, 트래픽 감시를 통한 사이버 공격조기 탐지, 보안정책 자동설정 및 통합 보안관리를 추진한다. 이와 함께 인프라의 최소 생존성을 보장하도록 망구조를 개선하고 가입자에 대한 사이버 방역 및 원천차단 체제를 구축한다. 2006년까지 조기탐지 및 자동차단 기술을 개발하고, 2007년까지 보안정책 자동설정 등 자동제어 기술을 개발하고 보안기능 통합형 망장비를 개발하며, 2008년까지 인프라 생존성 보장을 위한 망구조를 개선하고 가입자 사이버 방역 및 원천차단 체제를 구축할 것이다.

향후 광대역 통합망으로 전환될 경우, 인터넷망, 무선망, 방송망, 음성통신망으로 분리되었던 통신망이 하나의 통합망으로 수렴하게 된다. 광대역 통합망의 개별망에서 발생한 침해사고가 전체 통합망으로 빠르게 확대될 수 있다. 광대역 통합망의 취약성을 개선하기 위해서, 통합망의 침해 확산방지 대책을 수립하고, 보안 위험발생 수준에 따라서 단계적 분리, 운영을 추진하고 통합 통신망의 생존성과 안전성 향상을 위한 정보보호 기술을 개발한다. 2006년까지 침해사고 발생시 광대역 통합망에서 개별망을 분리하는 메카니즘 개발과 망의 우선순위에 따른 광대역 통합망의 분리계획을 추진한다. 이와 함께 침해유형별 대응방안을 연구하고 BcN 통신망 간의 연동 및 이동환경에서의 보안기술과 BcN 환경하에서의 정보보호 표준모델을 개발한다. 2008년까지 네트워크 안정성 향상을 위한 정보보호 기술 개발을 추진한다.

V. 맺음말

IT839 전략 추진은 개인, 기업 등 모든 사회구성원을 포함한 사회전반을 유비쿼터스 지식정보화 사회로 변모시킬 것이다. IT839 전략 추진에서 반드시 고려해야 할 사항이 정보보호이다. 서비스, 인프라, 신성장 디바이스에 대한 적절한 정보보호 투자와 노력이 이루어지지 않는다면, 지식정보화 사회를 한 순간에 무너뜨릴 수 있는

재앙이 닦칠 수도 있다. 그러므로, 유비쿼터스 사회로의 전환은 유비쿼터스 보안(ubiquitous security)이 함께 수반됨으로써 보장될 수 있다는 것을 앞에서 살펴보았다. 정보보호의 시간과 노력을 수익없는 비용 차원에서 접근하기 보다는 미래 기대손실을 줄이기 위한 투자로 인식하고 개인, 기업, 정부 등 모든 사회 구성원의 노력이 필요하다. IT839 전략 추진에 있어서 개별 기술 개발 뿐만 아니라, 정보보호 기술개발, 정책 시행, 문화창출 등 체계적이고 종합적인 노력이 모두 함께 이루어질 때 안전하고 신뢰할 수 있는 건전한 지능기반 사회로 전환할 수 있다.

참고 문헌

[1] 정보통신부, 국민소득 2만불로 가는길 IT839 전략, 2004

[2] Infosync, IEEE approves 802.11i security spec, 2004. 6

[3] 정보통신부, IT839전략 구현을 위한 중장기 정보보호 기본계획(안), 2004

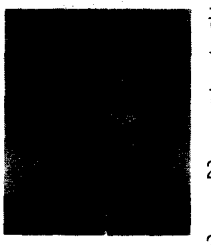
[4] 정보통신부, 민간부문의 해킹현황과 방지대책, 2004

[5] Don Marti, How Can You Defend Against a Superworm?, Linux Journal, 2003. 5

[6] 정보통신부, 중소기업 정보보호 현황과 대책, 2004

[7] 한국전산원, 2004년 한국인터넷 백서, 2004

[8] Nick McKeown, Growth in Router Capacity, 2003



김 기 권

1980년 : 동국대학교 사학과

1992년 : 미국 위스콘신주립대 정책학 석사

2001년 : 정보통신부 정보통신정책국 산업기술과장

2003년 : 정보통신부 정보화기획실 정보이용과장

현재 : 정보통신부 정보화기획실 정보보호정책과장