CHIEF INFORMATION OFFICER

CIO REPORT

| Vol. 15 2009. 08 |

NIA 한국정보화진흥원

CHIEF INFORMATION OFFICER

CONTENTS

Vol. 15 2009. 08

FOCUS

주요국의 사이버 보안 추진전략과 시사점

작성 : **유은재** 한국인터넷진흥원 주임연구원
윤미영 한국정보화진흥원 선임연구원

요약

- 최근 발생한 「7.7 사이버침해사고」의 피해에 따른 사회적 파장이 커지면서 사이버보안의 중요성 및 사이버 테러 대응이 주요 이슈로 부상

- 미국, 영국, 일본 등 전 세계적으로 인터넷 활용 범위 확대와 정보통신기술에 대한 의존도 증대 등으로 사이버보안 및 정보보호의 중요성에 대한 인식 확산
  - 사이버보안 정책의 중요성이 증대되면서 사이버보안의 위상이 점진적으로 격상

- 해외 주요국은 강력한 정부 리더십을 강조하면서 종합적인 사이버보안 국가 전략을 수립
  - 사이버보안 전담 조직인 사이버컨트롤타워 신설, 사이버보안 법률 체계 정비, 연구개발 역량 강화, 보안문화 확산 등을 통해 사이버공간의 신뢰도 제고 및 복원력 확보 등 미래의 안전한 디지털프라자 구축을 위해 노력

<주요국의 사이버 보안 추진 전략>

국가 총괄 조정기능 강화	미국	• 사이버보안을 **국가 핵심 아젠다**로 설정하고 **사이버보안정책관** 신설
	영국	• **사이버보안실(OCS), 사이버보안운영센터(CSOC)** 설립 추진
	일본	• 내각관방의 **정보보호센터(NISC)** 설립
법제도 개선	미국	• 정보통신 네트워크 관련 **법률의 통합** 및 **체계 확립** 검토
	영국	• 기관간 제휴를 통한 **법령 프레임워크** 개발
기술혁신 및 연구개발 고도화	미국	• 연구개발 **프레임워크 설계**
	영국	• 안전한 사이버공간 이용을 위한 **R&D 체계 구축**
	일본	• 「**그랜드챌린지**」형 연구개발 추진
보안문화 확산	미국	• **전국민 사이버보안 인식** 향상 추진
	영국	• 사이버보안 **인식 전환 촉구**
	일본	• **정부주도**의 정보보호교육 **역량** 확대

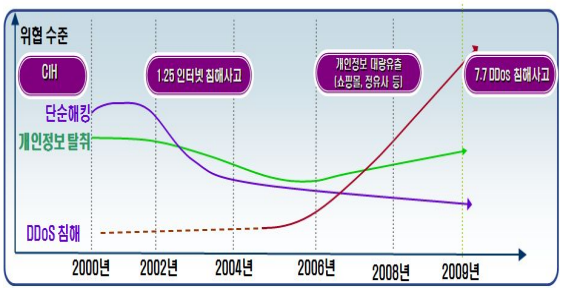
- 우리나라는 미래 사이버 위협에 대비하기 위한 사이버보안 전략의 전면적 재검토 및 선제적 대응 체계 마련 필요
  - 조직적·전문적 사이버보안을 위해 국가차원의 법규로 설립근거를 갖는 하나의 기관이 컨트롤타워가 되어 일원화된 보안체계 구축
  - 사이버보안 통합 법률 마련을 통해 부문간 업무의 융합 및 조정 필요
  - 사이버보안에 대한 연구개발 전략 강화 및 예산 지원 확대
  - 보안문화 확산을 위한 적극적인 인식제고 및 인력양성 프로그램 마련 시급

1. 사이버 공간의 중요성과 보안 위협의 증가

◎ 우리나라에서는 최근 발생한 **「7.7 사이버침해사고」**의 피해에 따른 사회적 파장이 커지면서 사이버 보안의 중요성 및 사이버 테러 대응이 주요 이슈로 부상

– 이번 공격은 해커가 공격대상으로 삼은 웹 사이트 뿐만 아니라 인터넷 서비스를 제공하는 인터넷 사업자 및 인터넷 사업자의 백본망[1]에 심각한 영향을 주어 사회적 혼란을 가져 온 점에서 주의 필요[2]

◎ **사이버 침해유형**이 점차 **복합화, 지능화, 대형화**되고 그 주기도 **일상화**되고 있으며, 사이버 위협 대상도 국가 전체로 확대



< 국내외 주요 사이버 침해사고 사례 >

일 자	주 요 현 황
2003년 1월 25일	• 「1·25 인터넷 대란」으로 윈도우 서버의 취약점을 이용한 '슬래머 웜' 바이러스에 의해 전 세계 7만 5천대 및 국내 8천 800여대 컴퓨터가 감염
2007년 6월 30일	• 에스토니아의 증권거래위원회 등 공공기관과 민간회사 등 약 300여개의 웹 사이트가 러시아세력으로 추종되는 해커들의 공격에 의해 마비
2008년 8월	• 러시아가 그루지아 공격 전 정보 관련 웹 사이트를 해킹
2009년 2월 5일	• 해킹에 의해 옥션 이용자 1천 81만 명의 개인정보 유출
2009년 7월 7일	• 청와대, 백악관 등 한미 주요 기관 웹 사이트와 일부 포털 등이 해커들의 DDoS 공격을 받아 다운되거나 접속 장애 사태 발생

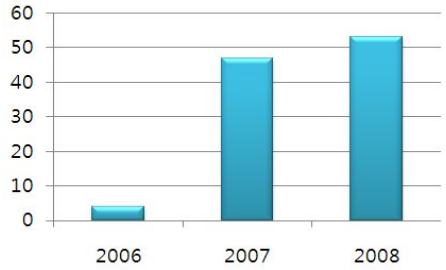
◎ 미국, 영국, 일본 등 주요국은 **사이버 보안**을 국가의 **핵심 아젠다**로 설정

– 해외 주요국들은 사이버침해유형의 변화에 따른 기존 사이버 보안 체계의 한계를 인식하고 종합적인 **국가 사이버 보안 전략 수립** 및 **기능 강화**

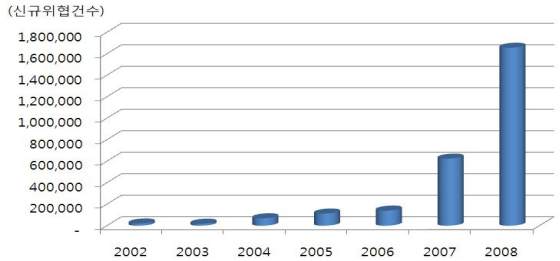
1) 백본망(backbone network) : 서로 연결되어 있는 소형 회선들로부터 데이터를 수집해 빠르게 전송할 수 있는 대규모 전송회선을 지칭
2) 국내 22개 사이트(청와대, 국방부, 행안부, 국회, 한나라당, 네이버 등), 미국 14개 사이트(백악관, 국무부, 국토안보부, 재무부, 워싱턴포스트 등) 등이 대상

◎ 우리나라도 사이버 보안 **전략의 전면적인 재검토** 및 **선제적 대응** 체계 마련 필요

< DDos 공격[3] 현황 >



< 신종 악성코드 현황 >



※ 출처 : Simantec, 「Global Internet Security Threat Report Trends for 2008」, 2009.4.

▌참고▌7.7 사이버침해사고 일지

□ 침해현황

○ 3차에 걸친 국내외 사이트 공격으로 **인터넷 접속 장애**

- 1차(7/7, 18시) : 청와대, 국회 등 국내 12개, 백악관 등 미국 14개 사이트 대상
- 2차(7/8, 18시) : 국정원, 안철수연구소 등 국내외 16개 사이트(미국 1개) 공격
- 3차(7/9, 18시) : 행안부 전자정부, 조선일보, 국민은행 등 국내 7개 사이트 공격

※ 7/10 0시부터 악성코드에 감염된 개인 PC 파괴기능 추가

○ KT 등 주요 ISP에서 파악한 **악성코드 감염 IP**는 11만여대로 확인됨

○ 악성코드에 의한 PC손상 피해 접수는 총 1,353건으로 파악됨(7/13)

□ 조치경과

○ DDoS 공격 탐지 후 대국민 **'주의' 경보 발령**, 보도자료, 인터뷰

○ **방통위** 차원의 **비상대응체제 구축** 및 적극 대응

- 네트워크국장을 반장으로 한 비상대응반 구성·운영(7.7~)

○ DDoS 관련 **범정부 차원**의 사이버위기 **대응** 공조

- 국무총리실장 주재 사이버테러 관련 관계부처 차관회의(7. 9. 15시)
- 국무총리 주재 국가정책조정회의(7.10. 8시)
- 국정원장 주재 제4차 사이버안전전략회의(7.10. 15시)

○ ISP/IDC, 통신사업자, 백신/보안업체 등 **민간**과 **긴급 협력 대응**

- 악성코드 유포 사이트로 추정되는 101개 사이트 차단('09.7.8. ~)

○ **KISA-ISP-백신업체간 협력**으로 감염 PC **추적** 및 **백신 처방**

- KISA는 악성코드 채집 · 분석 후 백신업체에 제공
- 백신업체는 악성코드 채집 · 분석 및 백신 신속 개발 및 배포
- ISP는 감염 PC의 악성코드 지속 제거 추진

3) DDoS(Distributed Denial of Service, 분산서비스 거부) : 공격자(해커)가 악성코드에 감염된 다수의 PC를 이용한 대량의 유해 트래픽 전송으로 네트워크와 시스템 과부하를 야기하는 정상적인 서비스를 방해

2. 해외 주요국의 사이버보안 추진 전략

◎ 사이버보안 문제가 국가경쟁력, 국가안보 등과 직결되어 있음을 인식하여, 해외 주요 선진국들은 사이버 공간의 신뢰도 향상 및 복원력 확보 등 미래의 안전한 사회를 위한 전략 추진

< 주요국의 사이버보안 추진 전략 >

국가 총괄 조정기능 강화	미국	• 사이버보안을 **국가 핵심 아젠다**로 설정하고 **사이버보안정책관** 신설
	영국	• **사이버보안실(OCS), 사이버보안운영센터(CSOC)** 설립 추진
	일본	• 내각관방의 **정보보호센터(NISC)** 설립
법제도 개선	미국	• 정보통신 네트워크 관련 **법률의 통합** 및 **체계 확립** 검토
	영국	• 기관간 제휴를 통한 **법령 프레임워크** 개발
기술혁신 및 연구개발 고도화	미국	• 연구개발 **프레임워크 설계**
	영국	• 안전한 사이버공간 이용을 위한 **R&D 체계 구축**
	일본	• 「**그랜드챌린지**」형 연구개발 추진
보안문화 확산	미국	• **전국민 사이버보안 인식** 향상 추진
	영국	• 사이버보안 **인식 전환 촉구**
	일본	• **정부주도**의 정보보호교육 **역량** 확대

1 국가 총괄 조정기능 강화 : 사이버컨트롤타워 신설

● 미국 : 대통령직속 사이버보안정책관 신설

◎ 디지털인프라를 국가의 주요 전략적 자산으로 인식하여 대통령 등 최상위 수준에서부터 사이버보안에 대한 적극적 참여의 필요성 인식

– 경제성장, 시민의 자유와 사생활 보호, 국가안보, 민주제의 지속적 개선 등을 위해 **사이버보안**을 **국가 핵심 아젠다**로 설정

◎ 국정 우선과제로써 국가 사이버보안 전략을 수립하고, 국가 최상위 수준의 사이버보안 리더십 발휘 및 총괄조정 기능 강화를 위한 **'사이버보안정책관(CPO)[4]'** 임명 추진 중

4) 사이버보안정책관(CPO) : Cybersecurity Policy Official

– CPO는 대통령이 직접 임명하며, 정부의 모든 사이버 보안 정책을 조정하고 통합하는 역할 수행

– 예산관리국(OMB)과의 긴밀한 협력을 통해 정부의 사이버보안 정책 통합 및 침해사고 대응 등이 효과적으로 실행될 수 있도록 관리

– 국방부(DoD), 국가안전보장국(NSA), 국토안전부(DHS) 등과 협력하여 사이버 테러에 대응하고 대규모 침해사고 발생시 총지휘관 역할 수행

< 미국 사이버보안 체계 위상 강화 >

※ 2001년 9.11 테러를 계기로 국토안전 및 사이버보안 주무부처로 국토안보부(DHS)를 신설하여, 국토안보부 준비국 산하의 국가사이버보안처(NCSD)와 국가사이버보안센터(NCSC)에서 범정부 차원의 사이버 보안 업무 총괄

❖ 사이버보안 정책관(CPO)은 연방정부 전체에 걸친 사이버보안 역할 조정 및 협력을 보다 원활히 하기 위해 CTO, CIO와 긴밀한 협력이 필요[5)]

• **CTO (Chief Technology Officer, 최고기술책임자)**
  – 애니쉬 초프라(Aneesh Paul Chopra)
  – 현 버지니아주 기술장관
  – 오바마 대통령은 내각에 CTO 직책을 신설
  – 에너지, 과학, 의료 등 다양한 분야의 IT관련 업무 총괄
  – 각료급으로 미국의 의료개혁 등 정책 현안을 해결하기 위해 IT 등 기술을 적극 활용

• **CIO (Chief Information Officer, 최고정보책임자)**
  – 비벡 쿤드라(Vivek Kundra)
  – 전 워싱턴 D.C 최고기술책임자
  – 연방정부 차원의 CIO 임명은 최초 미 정부의 정보화 부문을 관할하는 핵심 직책
  – 연방정부의 정보관리 업무는 물론, 기술정책 수립 업무를 맡아 CTO와 긴밀하게 협력

5) 이응용, 한정화 외, 「오바마 정부의 정보보호 정책방향」, 한국정보보호진흥원, 2009.6.

● 영국 : 사이버보안실 및 사이버보안운영센터 설립

◎ 급변하는 정보통신 환경 변화를 반영한 범정부 차원의 포괄적이고 종합적인 「**사이버보안전략(Cyber Security Strategy)**」을 발표('09.6.25)

– 본 전략은 사이버 공간의 신뢰도 향상 및 복원력 확보 등 미래의 안전한 디지털 인프라 구축을 위한 전략적 목표설정 및 정책실현 방법론 제시

– 1) 사이버공간 이용에 있어서 위험 요소 감소를 통한 2) 사이버범죄 대응 기회 포착 3) 사이버보안 지식 및 대응력, 의사결정 체계 강화 등을 중점 목표로 제시

◎ 사이버보안의 전략적 목표 및 정책실현을 위한 새로운 추진 체계 마련

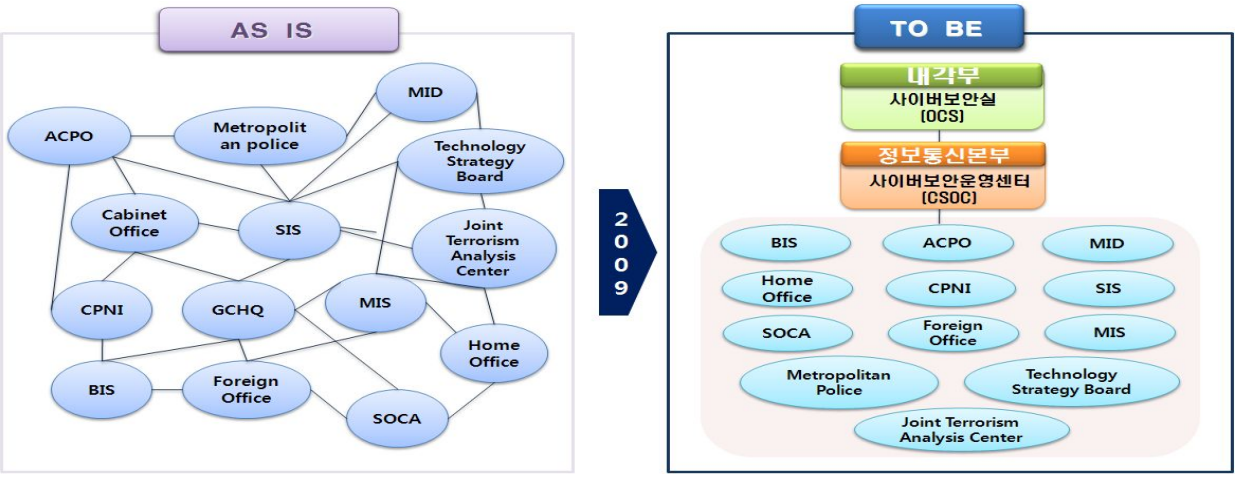
– **사이버보안실(OCS)**[6]**과 사이버보안운영센터(CSOC)**[7] **신설**을 통한 사이버보안 체계 강화

– 사이버보안실은 사이버보안 정책에 대한 **통합 조정 기관**으로 일관성 있는 정책을 각 부문에 공급하는 역할 담당

※ 사이버보안실 및 사이버보안담당관은 2009년 말 경에 신설 예정

– 사이버보안운영센터는 외부의 사이버 공격, 조직화된 사이버 범죄 및 테러로부터 각 부처 및 기업들을 보호, 침해사고에 대한 **효과적 대응** 및 **모니터링** 담당

< 영국의 사이버보안 체계 변화 >[8]



6) 사이버보안실(OCS) : Office of Cyber Security
7) 사이버보안운영센터(CSOC) : Cyber Security Operation Centre
8) VeyondStrategy 참조

일본 : 정보보호센터(NISC) 중심의 공공·민간 협력모델 구축

◎ 정보보호정책회의를 중심으로 국가 전반의 정보보호 문제를 다룬 「**제2차 정보보호 기본 계획**」을 발표

– 국가차원의 정보보호 기본 이념과 중점 정책 방향성을 제시

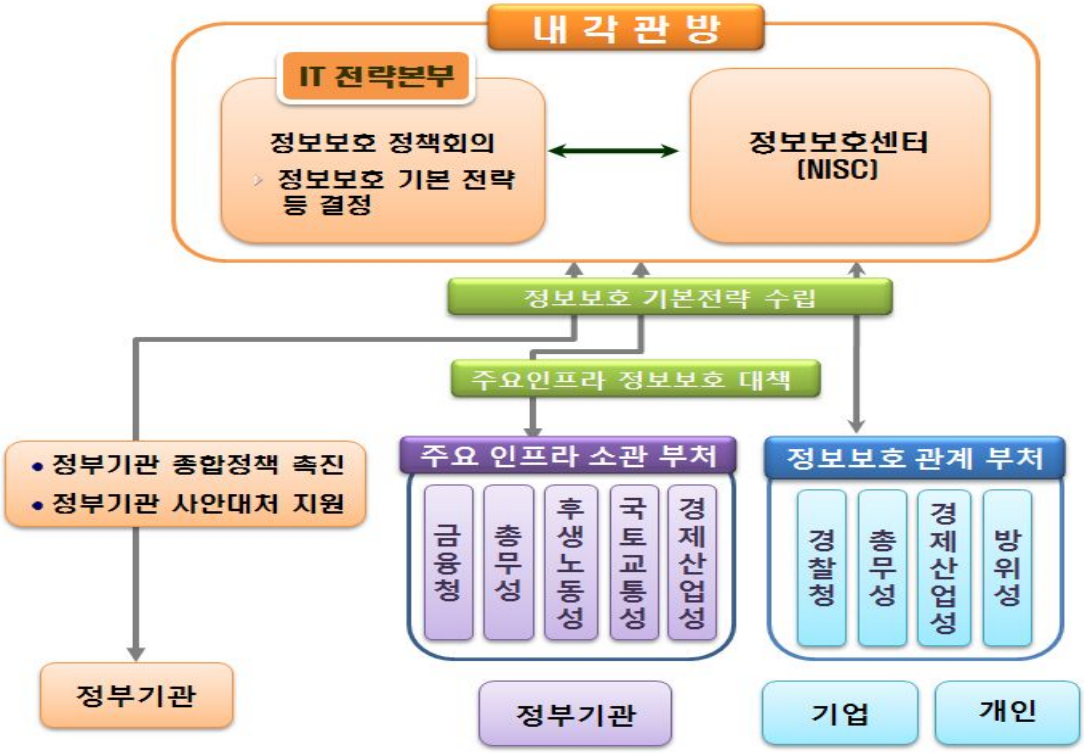
◎ 세계 2위의 경제대국에 걸맞는 정보보호 선진국을 실현하고 정보보호 분야의 **일본형 정책모델** 구현 추진

– 내각관방의 **정보보호센터(NISC)**[9]을 중심으로 공공·민간 각 주체별 역할분담을 위한 새로운 협력모델 구축

– 기본 정보보호 전략 입안, 정부기관의 종합적인 대책 추진, 침해사고 대응지원 등 **주요 기반시설 보호**와 **정부영역 정보보안 강화**의 2개 축으로 정보보호 활동 추진

– 정부기관의 정보보호 거버넌스 확립을 위한 조직 체계 및 사후 대응력 강화

< 일본의 사이버보안 체계 >[10]



9) 정보보호센터(NISC) : National Information Security Center
10) http://www.nisc.go.jp 참조

< 주요국 사이버 보안 추진체계 현황 및 비교 >

국가	기관명	소속	업무 및 기능	우리나라 유사기관 및 업무
미국	국가사이버보안센터(NCSC)	국토안보부(DHS)	• 연방정부 통신망 보호 • 국가안전보장국(NSA)과 FBI 통신 시스템의 정부 수집·공유 및 모니터링	• 국가사이버안전센터(NCSC) • 방통위, 국정원, 행안부, 국방부 등 정부기관이 민·관·군으로 분담, 소관 분야 정보수집 및 공유
	국가사이버보안처(NCSD)		• 사이버테러 대응전략수립 및 총괄 조정 • 취약점 확인 및 분석, 경보 발령 • 민관 협력 및 훈련, 교육 홍보	• 국가사이버안전센터(NCSC) • 한국인터넷진흥원((舊)한국정보보호진흥원) • 방통위, 국정원, 행안부, 국방부
	국가기반보호센터(NIPC)	연방수사국(FBI)	• 민간 해킹사고 조사, 모니터링 • 사이버위협 경향 분석 및 배포	• 한국인터넷진흥원((舊)한국정보보호진흥원) 및 통신, 은행, CERT 등
영국	국가기반보호센터(CPNI)	내각부	• 경보, 정부침해사고 대응기구 관할 • NISCC, NASC, CESG 등 합동근무, 물리적·사이버보안 융합 업무 수행	• 국가사이버안전센터(NCSC)
	정보보증중앙지원국(CSIA)	내무부	• 네트워크 및 정보보호 정책개발·발굴	• 방통위, 행안부 등
일본	정보보호센터(NISC)	내각관방	• 기본 정보보호 전략 입안, 정부기관의 종합 대책 추진 및 침해사고 대응 지원 등	• 방통위, 행안부, 국정원 등

2 사이버보안 법제도 개선

● 미국 : 정보통신 네트워크 관련 법률 통합 및 체계 확립 검토

◎ 헌법, 국내법, 국제법 등 산발적으로 발전되어온 정보통신 관련 **법률의 통합 및 체계 정리** 필요성 인식

- 사이버보안의 성공적 실현을 위한 법·정책의 효율적 수립 및 추진을 위해 의회와의 공고한 협력 관계 유지

◎ 미국 오바마 행정부는 사이버 보안 강화에 대한 강력한 정책 의지를 바탕으로 범정부 차원의 정책 수립에 기반이 될 전략 보고서[11] 발표('09.5.29)

- 기존의 사이버 보안 관련 정책의 면밀한 검토를 거쳐, 공공·민간 부문 등 다양한 분야의 국내·외 전문가 자문을 반영한 전략과 실행 계획 제안
- 사이버 보안 정책(Cyber security policy)의 개념을 사이버 공간에서의 보안과 운영에 관한 전략·정책·표준 등을 넘어, 국내외적 ICT 인프라를 위협하는 다양한 요인들을 다루는 것까지 포괄하는 것으로 정의

◎ 연방정보보호관리법(FISMA)[12]을 개정하고 강화할 예정

- 연방의 운용을 지원하는 주요 정보자원에 대한 보호 및 통제를 위한 포괄적 프로그램 제공
- 고도로 네트워크화된 국가기반 환경의 보호를 위해 민간·국가안보 관련 기관, 법집행 기관간 역할 조정을 통한 사이버위협에 대해 효과적 대응을 목적

11) Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure
12) FISMA(Federal Information Security Management Act of 2002) : 전자정부법규인 'The E-Government Act of 2002' 중 정보보호에 관한 연방법으로서 2002년부터 시행되었으며, FISMA는 연방정부의 정보보호를 확보하기 위한 체계를 규정하고, 연방 운용 및 자산을 지원하는 정보 자원에 대한 정보보호 통제 효과를 보장하기 위한 포괄적 프레임워크 제공

영국 : 기관간 제휴를 통한 법령 프레임워크 개발

◎ 영국 정부는 사이버보안전략 보고서를 기반으로 범정부차원 프로그램 구축 일환으로 사이버보안 관련 법률 해석, 정책 실행 등에 대한 부처간 불일치 해소를 위한 프로세스 개선을 진행할 계획

- 사이버전략의 효율적 실행을 위해 사이버보안실을 주축으로 현존하는 국내법 및 국제 정책, 법령, 규제 등을 사전 고찰
- 각 기관들과의 제휴를 통해 안전하고 복원력있는 사이버공간 형성을 지지할 수 있는 **법령 프레임워크** 개발

< 사이버 보안 전략을 위한 세부 정책 방안 >

정책방안	주 요 현 황
범정부차원 프로그램 구축	• 네트워크 안전성 및 복원력 확보, 사이버 보안 기술 개발 • 사이버 보안에 대한 정부부처 인식 제고 및 국제사회 협력체계 구축 • 사이버 보안 분야에 대한 인력 양성 및 사이버 범죄 · 테러에 대응하기 위한 핵심 역량 개발 • 정부의 사이버 보안에 대한 리더십 강화 및 책임 부여
정부-민간 간 협력체계 구축	• 공공 및 민간부문 핵심 시스템 장애 복구를 위한 협력체계 강화 • 정부와 산업간 기술 격차 해소를 위한 사이버 보안 기술 공유

일본 : 네트워크 안전성 확보를 위한 법 제정

◎ 국민이 안심하고 네트워크를 사용하기 위한 네트워크 안전성 및 신뢰성 확보에 주력

◎ '06년에 개정된 '정보통신사업법'을 근간으로 정보통신사업의 공공성을 강조하고, 합리적인 운영을 통해 정보통신서비스의 원활한 제공을 확보

- 이를 통해 이용자의 이익을 보호하는 한편, 정보통신의 건전한 발달 및 국민 편의 도모하여 공공복리 증진

3 사이버보안 기술혁신 및 연구개발 고도화[13]

● 미국 : 연구개발 프레임워크 설계

◎ 투명하고 책임감 있는 디지털 인프라 구축을 위해 개방과 혁신을 강조

- 연방정부는 **연구개발 전략 프레임워크**를 제공하며, 산업계와 학계의 중복된 연구를 피하고 전략적 연구과제 조정 역할을 확대
- 또한 연방정부는 민간부문 관계자들과 협력하여 국제 및 국내 표준화 기구들이 목표 설정시, 연구개발 프레임워크를 활용할 수 있도록 지원

● 영국 : 안전한 네트워크 구현을 위한 민·관 R&D 협력체계 구축

◎ 사이버보안 기술 **기술력 증진**을 위한 연구개발 정책 추진 예정

- 산업차원의 전략 개발 및 실행을 위한 민·관 협력과제 확대 및 예산 지원
- 사이버범죄 및 테러에 대응하기 위한 **핵심 역량을 개발**하는 등 사이버보안 기술 개발 및 R&D 체계 구축
- 정부와 기업이 필요로 하는 사이버보안 전문 지식, 차세대 네트워크 서비스 보안 등 미래융합적 기술 개발을 위한 인적 자원을 양성 하는 등 **기술교육 시스템** 확립

● 일본 : '그랜드챌린지형' 연구개발 추진

◎ 세계적 수준의 정보보호 관련 연구개발이 효율적·효과적으로 추진될 수 있도록 체계를 정비

- 시장성이 없으나 기술선점의 필요성이 있는 **정보보호 연구개발 분야**의 **중점화** 및 **다양성** 유지
- 선도적 정보보호 기술 개발을 위한 '**그랜드챌린지형**'[14] 연구개발 및 기술개발 추진

13) 미국, 영국, 일본 등 주요국은 사이버 보안을 위한 연구개발의 중요성을 인식하여 추진계획을 수립중임에 따라 구체적인 세부계획 미 존재

14) 미래사회의 기술 수요 및 환경을 예측하여 기반 기술을 개발

4 사이버보안 문화 확산

● 미국 : 전 국민 사이버보안 인식 제고 및 교육체계 개선

◎ 연방정부는 사이버보안에 대한 범국민 인식제고 활동 및 사이버교육 확대를 위해 교육 관계자 및 산업계와 연계를 통해 효율적인 방안 모색

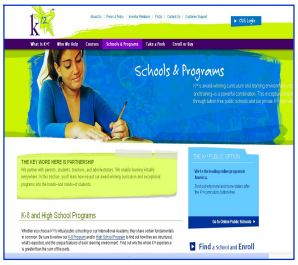
– 인터넷 사용에 대한 책임감, 인터넷상의 사기·ID 오남용·사이버 절도 대응, 사이버 윤리 등에 대한 인식향상을 주 목적으로 한 캠페인 시행

※ K-12 사이버보안교육프로그램(디지털 안전, 윤리, 보안) 추진 및 Smokey Bear(불조심), Click It or Ticket(안전벨트) 등과 같은 과거 성공적인 캠페인들을 벤치마킹하여 사이버보안 중요성에 대한 인식 확산

K-12 Education

❖ K-12는 인터넷으로 학생들을 연결하여 교육할 정보교육 프로젝트에서 유래하였으며, 미국내 약 14만개 학교들을 인터넷으로 연결하여 범국민적 교육정보화를 이루고자 하는 '넷데이(Net Day) 96' 운동과 같은 맥락에서 추진

※ K-12 : 유치원(Kindergarden)에서부터 고등학교를 졸업(12학년)까지 무상으로 교육받을 수 있는 13년간을 지칭



◎ 또한, 정보화 시대에 지속적인 경쟁력 강화를 위한 교육 프로그램과 연구개발 지원 확대 등 사이버 보안 교육 체계를 개선

– 사이버 공격, 취약성에 대한 정책 및 정보의 공유를 활성화하고, 정부와 산업계의 다양한 계층을 대상으로 폭넓은 훈련 실시

– 정부기관 및 민간기업 간의 인력 네트워크를 구축하여 다양한 분야의 근무기회를 제공하고, 사이버 보안 종사자들의 직무역량 향상 지원

● 영국 : 사이버보안에 대한 인식 전환 촉구

◎ 정부차원의 사이버보안 문제에 대한 인식 전환 노력

– 정부부처들 및 공무원들의 사이버보안에 대한 인식 제고

– ITPC(Infosec Training Paths and Competencies Scheme)를 두고 사이버 침해에 대한 인지수준 향상을 위한 교육 및 훈련 지원

– 대중과 이해관계자의 사이버보안 문제 인식 및 정보보호 윤리 교육 강화
※ 학교에서 수용 가능한 정보보호 내용 포함한 Becta schools 사이트의 “e-안전 교육” 커리큘럼 및 “Get Safe Online” 캠페인 실시 등

Get Safe Online 캠페인

❖ 안전하고 깨끗한 인터넷 이용환경 조성을 위해 영국 정부 및 SOCA(Serious Organized Crime Agency), HSBC, MS社 등이 공동으로 “Get Safe Online" 캠페인 실시
– 개인 이용자들에게 안전한 PC 사용법 및 사이버사기, ID 도용 문제 해결 방법 등을 이해하기 쉽게 전달

일본 : 정부주도의 정보보호교육 역량 확대

◎ 개인이 IT를 안전하게 사용할 수 있는 사회를 구축하기 위한 정부차원의 대책 마련
– 관계부처의 협력하에 개인의 정보보호 수준 제고 방안 마련
– 유아, 아동, 학부모 대상의 정보보호 교육 및 교재 개발 강화
※ 일본은 최근 OECD, APEC의 정보보호 관련 회의에서 온라인상의 아동보호를 위한 국제 공조 추진

◎ 민관 협력 및 자격시험을 활용한 인재육성의 지속적인 추진
– 정보보호 인재개발계획 마련하는 등 전문가 지원을 통한 기업에서 필요로 하는 인력 교육 및 확보 지원

일본 정부가 운영중인 정보보호 교육 웹사이트

< 총무성 “국민을위한 정보보호” 사이트 >

< 경제산업성 JNSA “인터넷 안전교실” 사이트 >

▌참고▌주요국의 사이버보안 정책 현황

1 미국 : 사이버보안에 대한 선도적 대응

○ 정보화 기술을 사용하는 사이버테러 등에 **선도적**으로 대처

– 사이버보안 국가전략 수립, 법제도 정비, 사고대응체계 정비, 공공·민간 협력 강화 및 정보보호문화운동 추진 등 **5개 주요 영역**을 중심으로 정보보호 정책 추진

○ 주요 사이버보안 정책

– 「국가 사이버공간 보호 전략」('03.3)

• 국가 사이버보안의 비전을 설정을 위한 공공·민간 파트너쉽 구축, 사이버보안 연속성 확보, 범국가적 정보보호인식 프로그램 등 5개 분야 30대 과제 추진

– 「국토안보 전략 계획」('08.9)

• 정보보호 관련 국가 주요 인프라와 자원 보호를 강화, 정부 통신시스템의 연속성 확보 및 사이버보안 역량 강화 전략 등

2 영국 : 정보보호 환경변화에 적극적으로 대처

○ 영국은 정보통신 환경변화에 따른 정보보호 환경변화에도 적극적으로 대처

– 이에 따라 정보보호와 관련된 입법 활동도 비교적 활발히 진행하는 등 미국·EU 등 타 국가들이 주도적으로 추진하는 **사이버보안 정책 수용**에 적극적임

○ 주요 사이버보안 정책

– 「국가 정보보증 전략」('07)

• 각 기관간 효율적인 위협정보 관리를 위해 관리자급의 책임과 의무를 강조

• 전문 기술 인력 양성 및 홍보 등을 통한 정보보호 신뢰도 제고

※ 국가 정보보증 전략은 '03년에 최초로 공표된 이후, '07년에 개정됨

– 영국의 보안정책 프레임워크」('08.12)

• 정부부처의 보안정책을 확산시키기 위해 「HMG Security Policy Framework」발표

• 거버넌스, 정부의 정보자산을 관리 및 보호, 개인정보보호, 정보보증, 물리적 보안, 對테러리즘 전략, 보안 위협 및 리스크 관리를 위한 업무연속성관리(BCM)[15] 등 7개 부문의 주요 보안전략 제시

3 일본 : 국가 발전 기본 전략으로서 정보보호 정책 추진

○ 정보보호의 국가 모델 정립을 위해 노력

– 일본의 정보보호 정책 목표는 "세계 일류 정보보호 立國"으로 高품질, 高신뢰, 안전을 바탕으로 한 **정보보호**의 **"Japan Model"**을 확립

○ 주요 사이버보안 정책

– 「제1차 정보보호 기본 계획」('06.2) 및 「제2차 정보보호 기본계획」('09.2) 수립

• 정부, 주요 인프라, 민간을 대상으로 정보보호 기본 계획에 대한 연간 전략 수립

※ 제1차 계획은 '06년~'08년, 제2차 계획은 '09년~'11년

• 공공(중앙/지방)·민간부문(기업/개인), 주요 인프라 영역으로 구분하여 매년 「**Secure Japan 200X**」를 수립하고 실행성과를 평가

15) 업무연속성관리(BCM, Business Continuity Management): 위기관리능력의 지표로 테러, 화재 등에도 주요 자산 보호 및 서비스 제공 가능

3. 시사점

◎ 사이버 보안 및 정보보호 강국 구현을 위해 국정과제로서 미래지향적인 사이버 보안 추진 전략 체계 확립 필요

- 사이버 보안을 국정우선과제로 선정하여 정부차원의 리더십 발휘와 성과평가를 통한 지속적인 개선을 기반으로 총괄조정 기능 강화
- 부처별로 분산되어 있는 사이버 보안 역할을 조정하고, 국가 차원의 비전 및 전략 수립
- 지속적이고 안정적인 사이버 보안관리와 사이버위기 적시 대응을 위해 **통합기구(사이버컨트롤타워)** 신설 등 **조직적 일관성** 및 **효율성** 제공

우리나라 사이버 보안 추진 체계

○ 우리나라의 경우, 주요 정보통신기반 보호는 행정안전부가 주관, 그 외의 공공부문은 국정원, 민간부문은 방송통신위원회가 각각 주관하여 **정보보호 기능**이 **부처별**로 **분산**되어 있음

◎ 국가 주도의 강력한 정보보호정책 및 사이버 보안 체계 수립을 위한 **법률 마련**을 통해 **사이버보안업무**의 **융합** 및 **조정** 필요

- 국가 전략수립 및 정보공유, 관리감독 등 사이버보안을 명시적으로 규정하여 유관기관간 정보공유 등 실질적인 협조 네트워크 구축을 위해 법제도 정비가 필수

우리나라 사이버 보안 법제도

○ 우리나라의 경우 사이버 보안 규정은 '사이버안전관리규정'과 '정보통신기반 보호법', '정보통신망이용촉진 및 정보보호 등에 관한 법률' 등 **여러 개별 법령**에 **분산**

◎ IT 강국이라는 입지를 유지하기 위한 지속적 사이버보안 연구개발 및 예산확대를 통해 인터넷 안전 및 신뢰 분야에서 선도적 역할 수행

- 사이버 보안 연구개발 및 전략 강화를 위해 산업체와의 유기적인 협력을 통해 연구개발 전략 프레임워크 구축

– 스마트그리드, 클라우드 서비스 등 새로운 IT 미래융합기술에 대한 선제적 정보보호 대응체계 마련 및 국제사회 선도

– 개방형 환경에서 자유롭게 사이버 공격·방어 신기술을 습득할 수 있는 장을 제공하여 **보안 전문 인력 양성과 일자리 창출**

◎ 범정부 차원에서의 사이버 보안인식 제고 및 디지털 역량을 강화하여 사이버 공간의 취약성 해결

– 경제성장, 국가안보, 미래경쟁력 향상을 위한 정보보호의 중요성을 인식하여 **범정부 차원**에서의 **인식제고** 및 **인력양성 프로그램** 마련

– 아동, 노약자, 주부 등 정보보호 취약계층 대상으로 정보보호·윤리 등 인식향상을 위한 교육 프로그램 마련 및 전국민 대상 정보보호 리터러시 향상

– 국민이 쉽게 접근할 수 있고 활용할 수 있는 TV, 포털, 블로그 등 뉴미디어를 통해 전 국민 대상의 정보보호 홍보 및 캠페인 확대

우리나라 정보보호교육

○ 행정안전부 : 정부정보화 교육센터 운영, 공무원 대상으로 교육 실시

○ 국가정보원 : 국가·공공기관 보안담당자와 주요 정보통신기반시설 관리기관의 보호책임자 등을 대상으로 사이버테러대응 교육 실시

○ 방송통신위원회(한국인터넷진흥원(舊 한국정보보호진흥원)) : 민간 대상으로 정보보호 인식제고를 위한 일반 교육과 정보보호 지식 전파를 위한 전문 교육 실시

▌참고▌우리나라의 「정보보호 중기 종합계획」

○ 우리나라는 국가차원의 정보보호 전략 및 종합적인 대책 마련을 위해 「정보보호 중기 종합계획」 발표('08.7)

– 종합적인 정보보호 대책 시행을 통해 취약한 정보보호 환경을 개선하고 정보보호 사회적 요구 충족을 위해 **6대 아젠다 18개 추진과제 73개 세부 과제**로 나누어 추진

아젠다	추진과제	목표
사이버침해 대응력 제고	1 사이버침해 예방체계 강화 2 사이버침해 대응체계 강화 3 국제 협력체계 강화	U-Gov의 안전성 확보
국가기반시설 보호 강화	4 국가기반시설 보호체계 강화 5 통합전산센터 보호체계 강화	
개인정보 보호체계 강화	6 개인정보보호 법·제도 개선 7 개인정보보호 관리체계 강화 8 개인정보보호 기술대책 강화	U-Society의 국민불안 해소
정보보호 기술기반 확충	9 국가 정보보호 수준 제고 10 전자인증 체계 개선 11 정보시스템 평가체계 개선 12 정보보호 기술개발 및 표준화	
정보보호 산업·인력 육성	13 정보보호산업 국가지원 확대 14 정보보호산업 해외수출 지원 15 정보보호 인력 양성	U-Biz의 신뢰성 제고
정보보호 문화조성	16 정보보호 교육 강화 17 정보보호 문화운동 전개 18 불건전 정보 유통 차단	

참고문헌

국내 문헌

1 국가정보원, 방송통신위원회, 행정안전부, 지식경제, 『2009 국가정보보호백서』, 2009.4.

2 민경식, 「일본의 최근 정보보호정책 현황 및 시사점」, 한국정보보호진흥원, 2008.6.

3 이연수, 이수연 외, 「주요국의 사이버안전관련 법 · 조직체계 비교 및 발전방안 연구」, 국가정보연구 제1권 2호, 2009.2.

4 이응용, 한정화 외, 「오바마 정부의 정보보호 정책방향」, 한국정보보호진흥원 2009.

5 황성원, 민경식, 「미국 · 일본의 정보보호정책 동향」, 한국정보보호진흥원, 2009.5.

6 임종인, 「사이버 보안 정책 및 법제도 현황」, TTA Journal No.118, 2008.7/8월호.

7 한국정보보호진흥원, 『미국 · 독일 · 일본의 정보보호법 체계에 관한 연구』, 2006.12.

국외 문헌

1 내각관방 정보보호센터, http:www.nisc.go.jp

2 정보보호센터, 「제1차 정보보호 기본계획」, 2005.12.

3 정보보호센터, 「제2차 정보보호 기본계획」, 2009.1.

4 총무성, 『정보통신백서』, 2008.

5 CSIS, 「Securing Cyberspace for the 44th Presidency」, 2008.12.8.

6 「Cyber Security Strategy of United Kingdom」, http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf, 2009.7.14.

7 White House, 「Cyberspace Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure」, 2009.5.28. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

8 「National Security Strategy of United Kingdom」, 2009.6.25. http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

9 http://www.dhs.gov/xlibrary/assets/DHS_OrgChart.pdf

CHIEF INFORMATION OFFICER

EXPERT INSIGHT

사이버 컨트롤타워의 중요성 및 협력 강화

ⓘ **정태명 교수** (성균관대학교 정보통신공학부)

ⓘ **조시행 상무** (안철수연구소)

기획 / 작성 : **윤미영** 한국정보화진흥원 선임연구원

"안전한 사이버 한국을 위해서는 어떠한 사이버 공격에도 초기 대응할 수 있는 **사이버 보안 체계 재정비, 전문가를 양성**해야 하며, **사이버 보안 조정관제도 및 정보보호를 위한 컨트롤타워** 필요"

정태명 교수 (성균관대학교 정보통신공학부)

- 전문분야 : 네트워크 관리, 정보보안, 실시간시스템
- 저서
  - 인터넷 시큐리티(2002)
  - 2020 미래한국(2005)
  - 사이버 공격과 보안 기술(2009)
- 주요활동
  - 2004년~2008년 : OECD WPISP 부의장
  - 2000년~현재 : 한국침해사고 대응팀 협의회 회장
  - 2003년~현재 : 한국정보처리학회 부회장
  - 2009년~현재 : 한국인터넷진흥원(KISA) 이사

단순한 인터넷 보호가 아닌 국가 안보 측면의 사이버 보안 정책 변화

◎ 해외 주요국은 사이버 보안을 단순한 인터넷 보호 차원이 아닌 국민의 재산과 국가의 안위를 보호하기 위한 국가 안보 차원에서 사이버 보안 정책을 추진

◎ 과거에는 방어 중심으로 사이버 보안 정책을 실시해왔으나, 현재는 국가 차원에서 사이버 부대 및 해커를 양성하여 공격 중심으로 보안 정책 변화

– 이러한 사이버 공격으로는 해킹, 바이러스, 스파이웨어 등을 통해 정보를 유출시키거나 경쟁사 무력화, 상대방의 정보 변형 등이 존재

◎ 영국, 일본, 미국 등 해외 주요국은 사이버 보안에 대한 당위성을 인지하고 전담조직과 체계를 정비하는 정책을 추진 중

– 특히 미국 오바마 정부는 홈랜드 시큐리티의 일환으로 사이버 보안을 강조하고 있으며, 이를 위해 사이버 정책을 대통령이 직접 관장

– 이에, 2009년 5월에 60일간 사이버보안 전문가들이 모여 집중 검토한 사이버공간에 관한 정책(Assuring a Trusted and Resilient Information and Communication Infrastructure)을 발표

사이버보안 조정관제도 및 컨트롤타워 구축을 통한 효율적이고 일관성 있는 사이버 보안 정비 체계 강화 필요

◎ 해외 주요국은 분산된 사이버 보안 업무를 중앙에서 통제할 필요성을 절감하고 사이버 보안 정책관제를 도입하기 위한 조직 신설 및 법 제도 개정 등을 추진

◎ 현재, 우리나라 정부 조직은 기능별 통합보다는 영역별 통합을 전제로 개편됨에 따라 여러 부처가 사이버 보안에 직·간접적으로 관여

- 국가정보원은 공공기관의 사이버 보안, 행정안전부는 전자정부 보안 및 개인정보보호, 지식경제부는 보안 산업 육성, 문화관광체육부는 콘텐츠 보안, 방송통신위원회는 인터넷 관련 사이버 보안을 담당

◎ 이러한 우리나라 정부정책은 7.7 DDoS 사태에서 볼 수 있듯이 대응단계에서의 정보공유 미흡으로 인해 정보 분석이 지연되었으며, 궁극적으로 즉각적인 대응체계 지연

- 또한, 법·제도 역시 7.7 DDoS 사태 발생시 공격자의 형태로 이동되는 당사자와 인터넷 격리 조치 등에 대한 법적 근거의 부족

◎ 이에 사이버 보안 조정관제도 및 컨트롤타워를 도입하여 효율적이고 일관성 있는 사이버 보안 체계 구축 및 향후 발생할 사이버 테러에 대한 대응체계 강화 필요

◎ 특히, 사이버 보안을 위한 컨트롤타워(사이버정책조정관)는 각 부처에 산재한 기능을 재검토하여 역할 재분배, 각 부처간 정보 공유를 위한 매개자 역할 등을 수행하여 미래 사이버 전쟁에 적극적인 대응체계 마련

- 컨트롤타워는 사이버 테러 발생시 각 부처의 보안 정책을 총체적으로 대응할 수 있는 정책을 정비해야 하며, 사건 해결 후에도 종합적인 분석 결과를 도출하는 역할 필요
- 사이버정책조정관의 설치는 단순한 직제신설이 아니라 우리나라의 사이버 보안을 위한 구심점이라는 인식 확산이 필요

“ 해외 기술 수입업체에 대한 의존도가 증대됨에 따라 사이버 보안에 대한 대응기술 및 인력이 부족하며, 이를 해결하기 위해서는 **정부와 민간의 사이버 보안 공조 체계 강화** 필요 ”

조시행 상무 [안철수연구소]

▸ 주요 경력
- 1995~1996 : 한글과컴퓨터
- 1996~2005 : 안철수연구소 엔진유닛 이사
- 2003~현재 : AVAR(아시아안티바이러스협회) 이사
- 2005~현재 : 안철수연구소 상무(CTO)

▸ 수상 경력
- 정보통신부 신소프트웨어상품대상(1996)
- 과학기술처 장영실상(1998)
- 국회 과학기술상(2000)
- 국제와일드리스트협회 “와일드리스트 올해의 리포터상 (2005.11)

DDoS 사건에 대한 대응과정 미흡 및 선의의 민간경쟁 부족

◎ DDoS 대응과정에서 정보가 한 곳으로 집중되지 못하여 대응체계에 있어서 혼란이 가중되었다는 점에서 향후 대책 마련 필요

– 경쟁적으로 보도에 치중하느라 100% 확인된 정보를 보도한 것이 아니라, 확인 중에 있는 정보들이 보도되는 경우가 많아서 피해 대책에 대한 정확한 인지 부족

◎ 중복된 정보 확인으로 인한 시간 소요, 선의의 역할 분담, 자체 분석 인력의 부족, 과거 대응 경험의 부족 등으로 선의의 민간경쟁 부족

– 과거 CIH 사건이나 1.25 인터넷 대란의 경우는 민간업체들끼리 대책 방안을 마련해 피해를 줄일 수 있는 방안을 강구했으나, 이번 7.7 DDoS 사태에서는 이러한 노력 부족

– 이는 우리나라 자체 기술을 가진 보안업체의 부족과 국내 보안 산업의 침체, 해외 기술 수입업체에 의존도 증대 등으로 인한 사이버 보안 강화에 대한 대응기술 및 인력 부족인 것으로 나타남

사이버 컨트롤타워의 중요성

◎ 정보 수집 및 분석, 기관별·업체별 장단점을 파악하고 역할 분담을 시킬 수 있어야 하며, 우리나라 보안 산업 전 분야에 대한 이해도가 높은 전문가 및 기관 설립 필요

◎ 단기적인 대응책이 아닌 장기적인 로드맵을 통해 꾸준한 투자 확보 필요하며, 사이버 보안 등 정보보호 관련 법안 등 최소한으로 규제할 수 있는 수단 필요

◎ 또한, 국민을 사이버 보안의 중요한 요소로 인식하고 전 국민을 전략적으로 사이버 보안 대응을 위한 참여자로 활용

- DDoS 공격에 사용된 좀비 PC는 가해자이며 피해자로써, 국민이 피해자가 되기 시작한 때부터 관심 증대

  ※ DDoS 초기 공격 시 전용백신을 다운로드한 수는 약 10만 명 정도였으나, 피해가 확산되자 하루 약 70만 명이 전용백신을 다운로드

사이버 보안 공조 체계 강화를 위한 협력 강화

◎ 이번 DDoS 공격으로 인해 정부와 민간의 협력이 더욱 중요해졌으며, 향후 점차 거세질 것으로 예상되는 사이버 공격에 대비하기 위해서는 민간부분의 적극적인 협조가 필요

◎ 이를 위해서는 사이버 보안에 대한 다양한 전문가를 확보해야 하며, 민간업체의 역할에 대한 존중 필요

◎ 이러한 민간의 역할도 중요하지만, 정부는 민간에서 할 수 없는 업무를 수행함에 따라 정부와 민간부문의 상호보안적인 역할 분담 필요

- 1.25 인터넷 대란 이후 오히려 우리나라 보안 업체가 쇠퇴한 경우처럼, 우리나라 보안 산업의 발전 없이는 국가적 사이버 재난 대응이 어려울 것으로 예상

- 특히, 정부는 투자 규모가 크거나 실패 가능성은 높지만 필요한 연구개발, 정부간의 공조가 필요한 수사, 사이버 보안 관련 법제도 정비, 보안인력 육성 및 교육, 보안의식 제고 등을 위한 정책 시행

CHIEF INFORMATION OFFICER

INFORMATION

이 달의 IT 용어 / 주요 이슈 및 행사

조사 / 작성 : **윤미영** 한국정보화진흥원 선임연구원

침입차단시스템 (IPS, Intrusion Prevention System)

- 인터넷에 연결되는 네트워크를 보호하기 위해 가장 기본적으로 사용되고 있는 방법으로 방화벽이라는 용어로 사용
  - 내부 네트워크와 인터넷간에 전송되는 문서들을 선별해서 수용, 거부, 수정하는 시스템으로 내부 네트워크와 인터넷의 경계 지역에 설치
- 침입차단시스템은 외부로 문서가 유출되는 것을 방지하는 것과 외부에서 들어오는 특정 정보를 차단하는 두 가지 방법 존재

침입탐지시스템 (IDS, Intrusion Detection System)

- 방화벽과 같이 단순히 네트워크를 통한 외부 침입을 차단하는 단계를 넘어 외부 침입에 의해 방화벽이 해킹된 후 침입 사실을 탐지해 이에 대해 대응하기 위한 솔루션
- 인터넷 등 외부망과의 접속시 일정 요건을 갖추지 않은 사람이나 데이터의 침입을 사전방지하기 위한 방화벽과는 달리 각종 해킹수법을 이미 자체적으로 내장, 침입행동을 실시간으로 감지, 제어할 수 있는 기능 제공

인증서 폐기 목록 (CRL, Certificate Revocation List)

- 네트워크 상 서버 접근 제어에 공개키를 적용할 때 쓰는 일반적인 방식 중 하나로, CRL은 가입자 이름과 인증서 현재 상태로 구성된 목록인데, 폐기 사유와 인증서 발급일, 발급기관 등의 정보를 포함
- 이 외에도, 각 목록에는 다음 폐기 목록 예정 일자를 포함하며, 사용자가 서버에 접근을 시도할 경우, 서버는 그 사용자에 관한 CRL 정보에 기반을 두고 접근 허용 여부 판단

8/6~8/7 IPTV 기술-서비스-정책 워크샵

▸ **주요 내용**

– IPTV의 서비스 활성화를 위해 관련 기술의 효율적인 연구 개발, 국내 관련 기술 및 서비스의 국제 경쟁력 강화, 국제적인 개방형 환경에 효과적 대처방안 등에 대한 논의

▸ 장소 : 천안 상록리조트

▸ 주최 : IPTV포럼 코리아

▸ http://www.iptvforum.or.kr/

8/11~8/12 21세기 지구환경전망 및 지속가능발전을 향한 저탄소녹색성장

▸ **주요 내용**

– 저탄소 녹색성장을 위해 현재 직면하고 있는 최근 상황을 공유하고, 향후 추진방향을 위한 핵심 이슈들에 대한 대응방안 논의

– 중장기적 미래 지구환경전망, 저탄소 사회를 건립하기 위한 지역정부의 노력과 미래계획, 국가차원 그린뉴딜의 주요 내용 및 저탄소 녹색성장 전략, 기업의 역할 및 시민사회의 역할 등에 대해 제시

▸ 장소 : 송도 컨벤시아(인천)

▸ 주최 : 인천광역시, 조선일보, 인천세계도시축전, 기후변화센터

▸ http://www.globalef.org/

8/19~8/22 '09년 UCN 하계 워크샵

▶ **주요 내용**

- 사업단 u-지능공간 개념의 소개와 제주지식산업진흥원 참여기관의 공동 전시회 개최를 통해 관련 기술에 대한 정보를 교류하고, 각 워킹그룹별 토의를 통해 u 지능공간 구조/규격 완성을 추진
- UCN 기술결과물 확산을 위한 u-지능공간 개념 소개, 커뮤니티 컴퓨팅 솔루션, 상황인지 프레임워크, 인덱스 모델 및 프레임워크, u-지능공간 통합 테스트베드 및 오브젝트 소개

▶ 장소 : 제주도 그랜드 호텔

▶ 주최 : 재)유비쿼터스컴퓨팅사업단

▶ http://www.osia.or.kr

8/25~8/26 모바일월드 2009 (The New Wave of Smartphones)

▶ **주요 내용**

- 국내 모바일 산업의 활성화와 글로벌 모바일 사업자간 비즈니스 기회 창출을 위해 '스마트폰의 새로운 물결'이라는 부제로 스마트폰의 진화와 발전방향 제시
- 모바일 기기, 네트워크, 애플리케이션, 소프트웨어, 모바일라이프 혁신 등의 주제에 대한 논의

▶ 장소 : JW 메리어트호텔 그랜드볼룸(서울)

▶ 주최 : 한국IDG

▶ http://www.conference.idg.co.kr/mobileworld2009

CIO 리포트 과월호 목록

2008	Vol. 1	어린이 안전과 IT
	Vol. 2	정보화 역기능 현황과 과제
	Vol. 3	재난관리와 IT
	Vol. 4	먹거리 안전과 IT
	Vol. 5	국가사이버테러 현황 및 대응동향
	Vol. 6	그린 IT 이슈와 대응동향
	Vol. 7	해외신간도서로 보는 미래 정보사회
	Vol. 8	2008년 주요 이슈와 IT
2009	Vol. 9	2009년 국내 10대 이슈 전망
	Vol.10	범죄 해결과 ICT
	Vol.11	고령화 문제와 ICT
	Vol.12	소셜네트워크와 공공서비스
	Vol.13	그린 Security
	Vol.14	주요 선진국의'소통형 디지털 정부'추진 현황과 시사점
	Vol.15	**주요국의 사이버 보안 추진 전략과 시사점**

1. “CIO 리포트”는 정보통신진흥기금으로 수행한「정보화 통계조사 및 동향분석」 사업 결과의 일부로 산출된 것입니다.

2. “CIO 리포트”는 매월 정부 정책입안자 및 일반 국민에게 국내외 주요 IT 이슈 분석과 동향 정보를 제공할 목적으로 발간됩니다.

3. 본 자료의 내용을 인용할 경우 출처를 명시하여 주시기 바랍니다.

4. 본 자료는 한국정보화진흥원의 공식 견해가 아니며, 본 내용에 대한 문의나 제안 사항이 있으시면 한국정보화진흥원 미래전략기획부로 연락하여 주시기 바랍니다.

■ 기획 · 구성

— 한국정보화진흥원 미래전략기획부 박선주 선임연구원(sjpark@nia.or.kr)

— 한국정보화진흥원 미래전략기획부 윤미영 선임연구원(yoonmy@nia.or.kr)

— 한국정보화진흥원 미래전략기획부 이윤희 선임연구원(unistar@nia.or.kr)

■ 문의 : 한국정보화진흥원 국가정보화기획단 미래전략기획부 윤미영 선임연구원

■ 보고서 온라인 서비스 : www.itglobal.or.kr