1 사이버 보안의 개요

1 사이버 보안의 생성 배경

- 2003년 1월 25일, 전국의 인터넷망이 마비되는 사상 초유의 사건이 발생(sql 취약점)

- 2007년 4월 27일, 에스토니아의 인프라 시설 및 관공서, 은행, 포털 사이트 등이 동시다발적으로 사이버 공격을 당함(사이버 공격)

1 사이버 보안의 생성 배경

- 2009년 7월 7일, 우리나라와 미국의 주요 정부 기관, 은행, 포털 사이트 등이 DDoS 공격을 당하여 일시적으로 서비스가 마비되는 사건이 발생 (DDoS)

- 2013년 3월 20일, 우리나라의 방송사와 금융권이 공격 당함

2 사이버 보안이란?

- 사이버상에서 네트워크를 통해 연결된 조직 및 사용자의 자산을 보호하기 위해 사용하는 기술적 수단, 정책, 개념, 가이드라인, 위기 관리 방법, 교육 및 훈련, 보안 보증 등을 뜻함(Total solution)

3 사이버 범죄(Cyber crime)

[사이버범죄의 유형]

범죄 유형	세부 유형	설명
사이버 테러형 범죄	해킹	다른 사람의 컴퓨터 시스템에 무단으로 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해 행위이다. 해킹에 사용된 기술 침해의 정도에 따라 단순 침입, 사용자 도용, 파일의 삭제 또는 변경, 자료 유출, 폭탄 스팸메일, 서비스 거부 공격 등으로 구분한다.
	악성 프로그램	정보 시스템의 정상적인 작동을 방해하기 위해 고의로 제작 · 유포하는 실행 가능한 모든 컴퓨터 프로그램을 말한다. 리소스의 감염 여부나 전파력 및 기능적 특징에 따라 바이러스, 웜, 스파이웨어 등으로 구분한다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 사이버 범죄(Cyber crime)

[사이버범죄의 유형]

범죄 유형	세부 유형	설명
일반 사이버 범죄	사기	인터넷에서 물건을 사고파는 과정에서 발생하는 범죄를 전자상거래 사기라고 하며, 인터넷 보급이 확대됨에 따라 규모가 커지고 있다.
	불법 복제	저작권법, 컴퓨터프로그램보호법 등에 따른 창작물에 대한 저작권 침해 행위를 말한다.
	불법 · 유해 사이트	공공의 안녕과 질서, 미풍양속을 해치는 반사회적 내용을 담고 있는 사이트로, 개설 목적 자체가 법률에 위반되거나 범죄 수단으로 사용되는 위법 사이트를 포함한다.
	사이버 명예훼손	인터넷 게시판에 타인의 명예를 훼손하는 글, 사진 등을 게시하거나 이메일 등으로 유포하는 행위를 말한다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 사이버 범죄(Cyber crime)

[사이버범죄의 유형]

범죄 유형	세부 유형	설명
일반 사이버 범죄	개인 정보 침해	쇼핑, 오락, 교육, 행정, 금융 등의 생활 전반이 온라인을 통해 이루어짐에 따라 개인 정보 침해도 늘어나고 있다. 개인 정보 침해 범죄의 심각성은 유출된 개인 정보가 다른 범죄에 이용될 수 있다는 것이다.
	사이버 스토킹	인터넷 게시판, 대화방, 이메일 등의 정보통신망을 통해 상대방이 원하지 않는 접속을 지속적으로 시도하거나 욕설 또는 협박 내용이 담긴 이메일의 송신 행위를 지속하는 것을 말한다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 사이버 범죄(Cyber crime)

- 사이버 범죄(Cyber crime) 또는 컴퓨터 범죄 (Computer crime)는 컴퓨터, 통신, 인터넷 등을 악용하여 사이버 공간에서 행하는 범죄로, 범행 목적에 따라 사이버 테러형과 일반 범죄형으로 분류

- 정보통신망으로 연결되는 컴퓨터 시스템이나 사이버 공간을 이용해 다른 사람한테 피해를 주고 건전한 사이버 문화에 해를 끼치는 행위

3 사이버 범죄(Cyber crime)

- 일반 범죄와 달리 빠른 시간 안에 불특정 다수에게 많은 악영향을 미치며, 사이버 공간 특성상 정보 발신자의 특정이 어렵고, 전자 정보의 증거 인멸 및 수정이 간단(불특정 다수, 전자 정보)

- 속성에 따라 정보통신망침해범죄, 정보통신망이용범죄, 불법컨텐츠범죄로 나뉨

4 사이버 스파이(Cyber espionage)

- 인터넷 등의 사이버 공간에서 특정 회사나 국가의 정보를 빼내어 그것을 필요로 하는 회사나 국가에 팔아 넘기는 활동(사이버 + 스파이)

- 사이버 스파이의 첫 사례는 1985년 독일의 '데이터 여행자 사건', 마르쿠스 헤스를 포함한 5명의 해커가 유럽우주기구(ESA), 미국항공우주국, 버지니아 주 군수 산업체, 일본 쓰쿠바 연구소 등에서 4년에 걸쳐 빼낸 산업·과학 정보를 구소련의 KGB에 팔아 넘긴 사건

4 사이버 스파이(Cyber espionage)

[마르쿠스헤스]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 사이버 스파이(Cyber espionage)

- ‘Red October’ 라는 작전명을 가진 대규모 사이버 스파이는 각국 정부 및 외교 기관, 연구 기관 등에 악성 프로그램을 유포하여 정보를 빼냄 (붉은 10월)

[대규모 사이버 스파이의 활동 중 하나인 Red October]

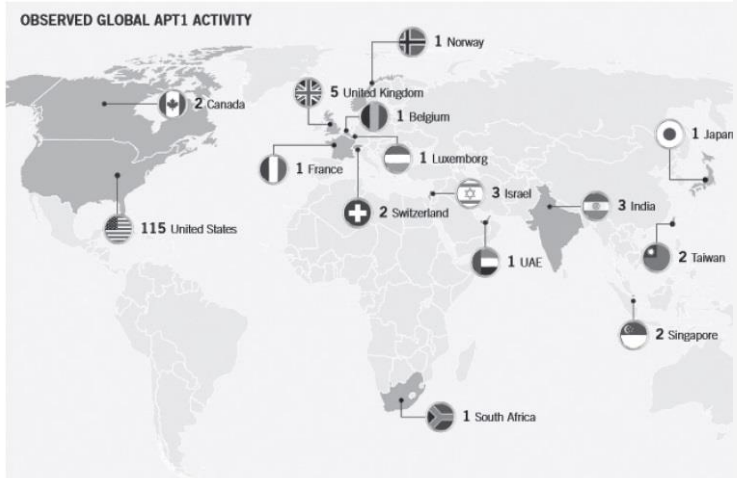
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 사이버 스파이(Cyber espionage)

- 1000여 명에 달하는 전문 직업 해커로 구성된 '중국 인민해방군 제3국 제2청 61398 해커 부대'는 2006년 무렵부터 최소 150건 이상의 기밀 정보 유출 공격을 감행(국가전)

4 사이버 스파이(Cyber espionage)

[중국 61398 부대가
사용한 것으로 추정되는 건물]



[중국 61398의 사이버 스파이
공격을 받은 국가]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 사이버 스파이(Cyber espionage)

- 사이버 스파이(Cyber spy)는 정보통신망에서 회사의 정보를 빼내 다른 회사로 팔아 넘기는 활동을 하는 컴퓨터 산업 스파이를 일컬음
- 일반 산업 스파이와는 다르게 고도의 기술이 필요하지 않아 컴퓨터를 잘 다루는 사람이라면 손쉽게 자료를 획득할 수 있음(기술 필요 없음)
- 또 다른 의미로는 안티 카페 회원 혹은 그와 반대되는 회원으로 위장 가입하여 안 좋은 글을 캡처한 뒤 이를 명예훼손, 모욕 등으로 협박을 하는 행위를 말함(인강)

5 사이버 전쟁(Cyber warfare)

- 2009년 유엔(UN)에서는 만약 3차 세계대전이 시작된다면 사이버 전쟁(분쟁)이 될 것이라고 예측

- 대표적인 사이버 전쟁
  : 2007년 에스토니아 사이버 분쟁,
  2008년 러시아와 조지아 간의 사이버 전쟁,
  2010년 미국과 이란의 사이버 분쟁 등

5 사이버 전쟁(Cyber warfare)

[사이버 전쟁 및 사이버 공격의 주요 사례 1]

연도	대상국	설명
1991	미국 → 이라크	• 미국이 이라크에 수출할 프린터 장치에 컴퓨터 바이러스를 이식하여 1991년 걸프전 당시 이라크 방공망 완전 마비 • 미군에 의한 이라크 정보망 교란 및 사이버 심리전 전개
1999	코소보 사태	• 북대서양조약기구(NATO)의 유고 공중 폭격에 반발한 해커들이 NATO 군사령부 홈페이지를 변조하고 이메일을 대량 발송하여 서버 운영 방해 • 미군이 사이버 부대를 동원하여 주요 기간 시설과 군 지휘 통신망을 무력화한 후 보병 진격
2007	에스토니아전	• 대통령궁, 의회, 정부, 은행, 언론사 등 주요 기관의 홈페이지와 전산망에 DDoS 공격으로 인한 피해 발생 • 약 3주간 지속적인 공격
2008	러시아 → 조지아	• 러시아가 조지아와의 영토 분쟁에 앞서 대규모 사이버 공격 감행 • 3일 동안 조지아 정부, 군 정보 시스템, 금융 기관, 언론사, 포털 사이트 등에 DDoS 공격

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 사이버 전쟁(Cyber warfare)

[사이버 전쟁 및 사이버 공격의 주요 사례 2]

연도	대상국	설명
2010	미국 → 이란(추정)	• 국가 기반 시설을 대상으로 제작된 새로운 유형의 바이러스인 스턱스넷(Stuxnet) 개발 • 미국 또는 이스라엘의 지원을 받아 이란 브세르 핵발전소 원격 감시 제어 시스템을 공격하기 위해 제작된 것으로 추정
2010	중국 → 미국(추정)	• 백악관을 해킹하여 핵무기 발사 암호를 유출하려고 시도 • 뉴욕타임스, 워싱턴포스트 등 주요 언론 기관 및 애플, 페이스북 등 민간 기관의 정보 해킹
2011	북한 → 한국(추정)	• 농협, 중앙일보, KBS, MBC, YTN 등을 공격하여 전산망 마비
2012	이란 → 미국 및 중동 친미 국가	• 미국 내 금융 기관의 데이터 센터 공격, 카타르 가스 회사에 악성 코드 공격
2013	시리아 친정부 단체 → 서방 국가	• 영국 BBC 방송, 인권 단체 휴먼라이트워치 등을 공격하여 시리아 정부를 옹호하는 메시지 게시
2013	러시아 → 조지아, 동유럽	• 조지아 내무부를 대상으로 피싱 메일 발송 • 미국 방위 산업체 공격
2016	러시아 → 미국	• 미국 민주당 등 주요 정부 요인의 메일 해킹

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 각국의 사이버 보안 동향

2 | 각국의 사이버 보안 동향

1 미국

- 1998년
  - 클린턴 정부는 '대통령령 제63호'를 공표하여 주요 기반 시설에 대한 범정부적 보호 체계를 마련
- 2001년
  - 9.11 테러를 계기로 부시 정부는 주요 기반 시설의 보호를 국토 안보 차원에서 다룸
- 2002년
  - 사이버 보안을 총괄 책임지는 국토안보부를 설립

1 미국

- 2009년
  - 1월에 출범한 오바마 정부는 사이버 보안 정책을 최우선 과제로 삼았으며, 같은 해 5월 '사이버 공간 정책 리뷰'를 발표
  - 사이버 보안 정책을 추진하기 위한 10가지 실행 과제 제시
  - 국가안보회의 내에 사이버 보안 조정관을 최고 책임자로 하는 '사이버 보안국'을 설립

2 | 각국의 사이버 보안 동향

1 미국

2009년

[사이버 공간 정책 리뷰의 단기 실행 과제]

어젠다	단기 실행 과제
최상위 리더십 발휘	① 국가 사이버 보안 정책 추진을 총괄 · 지휘하는 사이버 보안 조정관 임명 및 국가안보회의 담당 국으로서 사이버보안국 신설
	② 정보통신 기반을 안전하게 보호하기 위한 새로운 국가 전략 마련
	③ 대통령의 국정 핵심 과제로 사이버 보안 책정 및 성과 관리
	④ 국가안보회의 내 사이버보안국에 프라이버시 및 인권 담당관 임명
	⑤ 사이버 보안 관련 관계 부처 통합 지침 마련 및 협력 체계 구축
디지털 국가 역량 구축	⑥ 사이버 보안 촉진을 위한 범국가 차원의 인식 제고 및 교육 캠페인 실시
사이버 보안 책임 공유	⑦ 국제 사이버 보안 정책을 위한 미국의 역할을 확립하고 국제 파트너십 관련 역량 강화
효과적인 정보 공유 및 사고 대응 체계 구축	⑧ 사이버 침해 사고 대응 계획 수립 및 민 · 관 파트너십 향상을 위한 대화 촉진
혁신 촉진	⑨ 연구 개발 전략 프레임워크 구축 및 연구 촉진을 위한 침해 사고 정보 대응
	⑩ 프라이버시와 인권을 배려한 사이버 보안에 기반을 둔 ID 관리 비전 및 전략 수립

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 | 각국의 사이버 보안 동향

1 미국

- 2010년
  - 국방 검토 보고서에서 사이버 공간을 육·해·공·우주 외의 다섯 번째 전장으로 추가
  - 육군· 해군·공군의 사이버 전쟁을 총괄할 사이버사령부 지휘관을 국가안보국 국장으로 임명하여 사이버 조직의 골격을 완성
  - 육군·해군·공군·해병대가 개별적으로 운영하던 사이버 부대를 통합하여 사이버전에 대응하는 사이버 사령부를 전략사령부 내에 창설

1 미국

- 2010년
  - 국립표준기술연구소에서 사이버 보안 전문가를 육성하고 활용하기 위해 '국가 사이버 보안 교육 계획'을 발표

[미국 사이버 사령부의 로고]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

1 미국

2010년

[미국 국가 사이버 보안 교육 계획의 주요 내용]

목적	내용
국가의 정보 보호를 강화하기 위해 건전하고 지속 가능한 사이버 보안 교육 프로그램을 개발한다. 교육 프로그램은 다음 네 가지 측면으로 구성한다.	① Awareness: 국토부 주도의 국가 사이버 보안 인식 향상 'Stop. Think. Connect.' 캠페인, 정보 보호의 달(10월) 제정 등 일반인을 위한 안전한 인터넷 이용 환경을 조성한다.
	② Education: 교육부 및 전미과학재단(NSF) 주도의 공적인 사이버 보안 교육 유치원부터 고등교육, 직업 프로그램 등을 대상으로 사이버 보안 교육을 실시하여 민간 또는 정부 기관에 기능 인력을 공급한다.
	③ Federal Workforce Structure: 국토부 주도의 사이버 보안 전문 인력 양성 사이버 보안에 관한 업무와 취업, 커리어패스 등을 정의한다.
	④ Training and Professional Development: 국토부, 국방부 주도의 사이버 보안 전문 인력 교육과 전문 능력 개발 산업체와 학교, 연구소 등의 협력 아래 기존 연방정부의 전문 인력 강화 훈련 및 전문 능력 개발을 실시한다. 분야는 일반 IT 이용, IT 인프라, 관리, 보호, 법 집행 및 대응 활동 보고, 사이버 보안 운용의 영역을 포함한다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 | 각국의 사이버 보안 동향

1 미국

- 2011년
  - 기본적 자유권, 프라이버시, 정보의 자유로운 흐름이라는 3대 핵심 원칙을 바탕으로 '사이버 공간을 위한 국제 전략'을 수립, 발표
  - 12월에는 국가과학기술회의에서 2년 넘게 검토한 '사이버 보안 연구 개발 전략'을 발표

1 미국

- 2012년
  - 실전 투입용 사이버 무기 개발을 위한 대규모 프로젝트인 'Plan X'의 추진 계획을 발표
  - 2012년 10월에는 오바마 대통령이 '대통령령 20호'로 알려진 사이버전 교전 규칙 마련을 위한 기밀 지침에 서명

2 | 각국의 사이버 보안 동향

1 미국

- 2013년
  - 회계연도 국방수권법에 서명하여 국가 안보를 위한 사이버 역량 강화 의지 확고히 함(의지)
  - 2013년 2월 오바마 행정명령과 행정 지침을 발표하여 주요 기반 시설의 사이버 보안 체계에 대한 정비 실시(정비)

2 | 각국의 사이버 보안 동향

1 미국

- 2014년
  - 오바마 정부 2기에 '행정명령'에 따라 국가 기반 보호 계획 2013, 사이버 보안 프레임워크 등이 수립되는 등 민간과 정부의 협력에 따른 사이버 보안 강화 정책이 진행

1 미국

2015년

- 2월 백악관에서는 '국가 안보 전략'에 사이버 위협 대응을 주요 과제로 인식하고 대응 방안 제시
- 4월에는 'US DoD Cyber Strategy'를 발표하여 기존 전략에서 더욱 적극적인 기조로 변경된 전략을 공개
- 10월에는 'Cyber Threat Sharing Act of 2015' 법안이 통과되어 공공과 민간의 사이버 위협 정보 공유의 기반이 마련됨(공유)

1 미국

- 2016년
  - 2016년 2월 '사이버 보안 국가 행동 계획'을 발표

2 영국

- 정보보안 분야의 환경 변화에 적극적으로 대처하고 정보보안 관련 활동도 매우 활발하게 진행
- 1995년 영국표준기관은 기업의 보안 관리 수준을 향상하기 위해 '정보보안 관리에 대한 표준'을 제정

2 영국

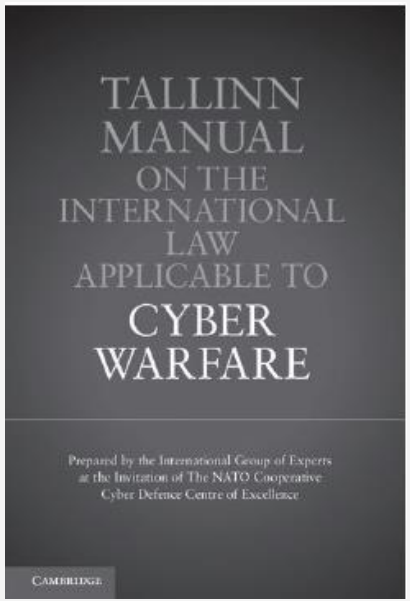
- 영국 사이버 안전 체계
  - 정보보증중앙지원국
    : 네트워크 및 정보보호 정책 총괄
  - 정보통신총국, 국가기반보호센터
    : 국가 전반에 걸친 정보보호 기관 역할 수행
  - 국가기반보호센터
    : 국가보안자문센터와 국가기반보안조정센터, CESG 등을 통합하여 2007년에 새롭게 창설

3 NATO(North Atlantic Treaty Organization)

- 2010년 신전략 개념에서 사이버 공격을 동맹국의 정보 네트워크에 대한 위협으로 선언(Treat)
- 2011년 NATO 국방장관 회의에서 동맹국 간 상호 협력을 바탕으로 한 사이버 방위 정책을 승인
- 2012년 10월부터는 NATO 최고 의사결정 기구인 북대서양이사회 차원에서 사이버 안보 분야에 대한 논의 본격화

3 NATO(North Atlantic Treaty Organization)

- 2013년 3월, NATO의 협력 기구인 사이버방어협력센터 (CCDCOE)는 사이버 공간에 대한 기존 국제법을 적용하여 사이버전에 대한 지침인 '탈린 매뉴얼' 발표



[탈린 매뉴얼]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 NATO(North Atlantic Treaty Organization)

[탈린 매뉴얼의 주요 내용]

조항	내용
Rule 05	모든 국가는 자국의 영토에 위치한 사이버 인프라가 다른 국가에 대한 적대 행위에 사용되도록 허용해서는 안 된다.
Rule 06	국제 의무를 위반한 사이버 작전을 수행한 국가는 국제법적 책임을 져야 한다.
Rule 09	국제 위법 행위의 피해국은 가해국에 대해 사이버 대응 조치 등과 같은 적절한 대응 조치를 할 수 있다.
Rule 13	무장 공격에 상응하는 사이버 공격을 받은 국가는 자위권을 행사할 수 있다.
Rule 15	사이버 무장 공격이 발생했거나 임박한 경우 자위권 행사를 위해 무력을 사용할 수 있다.
Rule 29	사이버 공격에 직접 가담한 민간인은 공격 가담 시점에 국제법상의 보호를 받지 못한다.
Rule 30	사이버 공격은 사람을 다치거나 죽게 하거나 물자를 파괴할 것으로 합리적으로 예상되는 사이버 공격 및 방어 작전을 말한다.
Rule 42	불필요한 부상이나 고통을 가져오는 속성을 가진 사이버전의 수단과 방법의 채택은 금지된다.
Rule 43	무차별적인 속성을 가진 사이버전의 수단과 방법의 채택은 금지된다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 EU(European Union)

- 2002년 3월 7일, 개인 정보와 프라이버시를 안전하게 보호하고 통신 네트워크의 안전성을 확보하기 위한 '정보보호기본법'으로 '프레임워크 지침'을 제정
- 2004년 4월에는 '유럽 네트워크 및 정보보안 기구' 설립
- 2009년 3월 CIP 사이버 보안 대책 발표

4 EU(European Union)

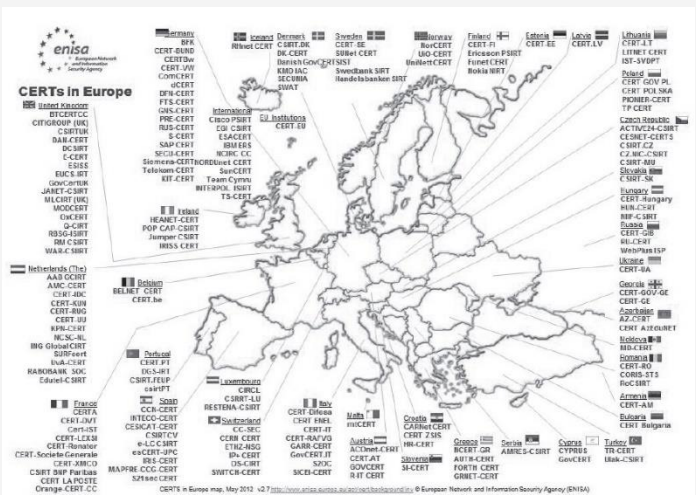
- 2010년 5월에는 유럽의 ICT 정책인 Digital Agenda 에서 사이버 공격에 대한 대책 마련의 중요성 강조

[벨기에의 수도 브뤼셀 에 위치한 EU 본부]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 EU(European Union)

- 사이버 공격에 대한 대응을 담당하는 CERT의 설립과 활동 계획 등이 마련(CERT)



[EU CERT 맵]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 EU(European Union)

- 2013년 'An Open, Safe and Secure Cyberspace' 사이버 보안 전략을 발표
- EU의 사이버 보안 전략
  - 사이버 복원력 확보
  - 사이버 범죄의 획기적인 감소
  - 사이버 방어 정책과 능력 개발
  - 사이버 보안을 위한 산업과 기술적 자원 개발
  - 사이버 공간에 대한 일관성 있는 정책 수립 및 EU의 핵심 가치 증진

5 일본

- 1994년에 내각 총리대신을 본부장으로 하는 '고도정보통신사회추진본부'를 설치하고, 2000년 7월에 이를 'IT전략본부'로 재편

- 2000년 1월에는 '정보 기관과 민간 주요 기반 시설의 안전 대책'을 추진하고 '해커 대책 등의 기반 정비에 관한 행동 계획' 마련

- 같은 해 3월에는 내각관방의 내각안전보장·위기관리실 아래에 '정보보안대책 추진실'을 설치하여 체계를 확립

5 일본

- 2001년에는
  '전자정부의 정보보안 확보를 위한 행동 계획' 마련

- 2002년 4월에는 각 성청에서 정보보안
  대책의 입안을 위해 정보보호 전문가로
  구성된 '긴급 대응지원팀'을 내각관방에 설치

- 2003년 10월 경제산업성은 '정보보호 종합 전략'을
  마련하고 주요 기반 시설에 대한 위협 정보 수집 및
  분석 능력 향상, 사이버 범죄에 대한 대책 수립,
  정보보호 관련 국제 협력 업무 등을 추진

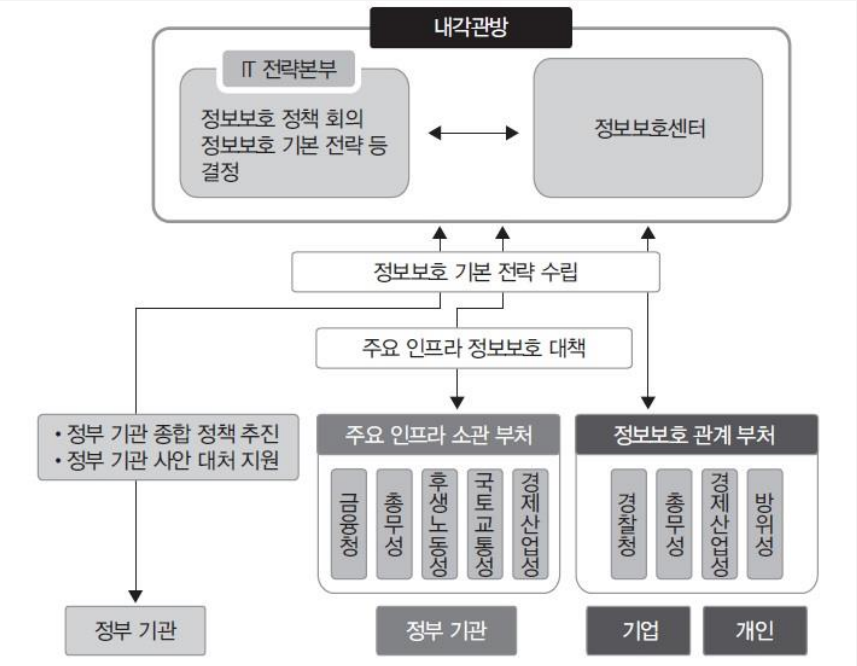
5 일본

- 2005년 4월에 내각관방의 '정보보호대책추진실'을 발족·강화하는 형태로 '내각관방정보보안센터'를 신규 설치

- 2015년 8월에는 새로운 사이버 보안 전략을 발표

5 일본

[일본의
사이버 보안체계]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 중국

- 1990년대부터 시작된 중국의 인터넷은 정부 주도로 상당히 강력한 사이버 보안 체계를 유지하고 있음(거대한 국가 인트라넷 형태)

- 인민해방군은 산하 기관인 군사과학협회에서 1991년부터 해커 양성(공격이 최선의 방어)

6 중국

- 중국의 사이버 안전 관련 기관
  - 국가안전부 : 국가 암호 관리 및 컴퓨터 보안 정책 수립 등 사이버 안전 업무 총괄
  - 국가보밀국 : 국가 공공기관의 보안 업무, 보안 감사, 보안 정책 시달 및 토제 감독 등을 담당
  - 공안부 : 국가 기밀을 보호하는 데 핵심 역할 수행

7 우리나라

- 2003년 1.25 인터넷 대란 이후
  '국가 사이버 테러 대응 체계 구축 기본 계획'을 마련
  (sql 취약점)

- 2004년 2월 '국가 사이버안전센터' 설립

- 2011년 7월, 국가 사이버 안전 대책 회의의 심의와 의결을 거쳐 8월에 50개 세부 추진 과제가 도출되어 현재 시행되고 있음

7 우리나라

- 2013년 사이버 테러 공격을 계기로 정부는
  국가 사이버 위기 관리 체계 구축

- 2016년 민간 싱크 탱크인 사이버보안정책센터 설립

7 우리나라

우리나라의 국가 사이버 보안체계

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 1.25 인터넷 대란

- 1·25 인터넷 대란은 2003년 1월 25일 대한민국 인터넷 망이 마비된 사건으로 마이크로소프트사의 SQL 서버의 허점을 이용하는 슬래머 웜이 이 사건을 일으킴(sql 취약점 → 슬래머 웜)

8 1.25 인터넷 대란

- 이 사건은 슬래머 웜에 감염된 PC들이 대량의 데이터를 생성해 KT 혜화전화국에 있는 DNS 서버에 인터넷 트래픽을 집중시키면서 시작 됨, KT 혜화전화국이 공격에 의해 마비되자, 전국적인 인터넷 트래픽이 다른 백본망으로 우회하기 시작했고, 다른 DNS 서버도 순차적으로 마비되어 감 (슬래머 웜 → DNS 서버 마비)

8 1.25 인터넷 대란

- 한편, 대기업의 인터넷 회선이 아닌 백본망을 빌리는 형태로 서비스를 제공하는 중소업체의 인터넷 회선은 대기업의 회선에 비해 마비의 정도가 덜 했음(대기업 vs. 중소업체)

- 이 사건으로 피해를 입은 인터넷 사용자들은 KT를 상대로 피해보상소송을 제기하기도 함

9 KISA

- 한국인터넷진흥원(Korea Internet & Security Agency, KISA)은 대한민국의 인터넷 진흥, 인터넷 정보보호 및 그에 대한 국제 협력 업무를 수행하는 과학기술정보통신부 산하 위탁집행형 준정부기관 임

- 한국인터넷진흥원의 설립 근거 법률은 정통망법 제52조, 2009년 7월 정부의 공공기관 선진화 정책에 따라 방송통신위원회 산하 3개 기관인 한국정보보호진흥원(KISA), 한국인터넷진흥원(NIDA), 정보통신국제협력진흥원(KIICA)이 통합되어 출범함

9 KISA

- 2018년 2월 기준으로 5본부 2실 10단 7센터 55팀으로 조직되어 있음, 또한 2016년부터 국가 간 협력 및 국내 정보보호기업의 해외진출 지원을 목적으로 해외 거점 사무소도 운영 중

- 해외 거점은 각각 중동지역은 오만, 동남아시아 지역은 인도네시아, 중남미 지역은 코스타리카, 아프리카 지역은 탄자니아에 위치하여 운영하고 있음

9 KISA

- 주요 기능은 다음과 같음(정보보호)
  - 사이버침해사고 대응·예방 및 민관 협력체계 운영
  - 미래 인터넷·정보보호 산업의 성장기반 조성
  - 국제협력 및 정보보호산업 해외진출 지원