전문가가 진단한 정보화법제도 쟁점과 과제- 2009-⑩

국가 정보보호 추진체계 관련법제 분석

김재광(선문대학교 법학과 교수)

목 차

표 목차

제1장 연구의 목적

전세계적으로 사이버공격의 지능화, 다양화로 인해 기존의 법적·기술적 대응만으로는 한계가 있으므로 새로운 유형의 악성코드,[1] 봇넷[2] 및 피싱[3]과 같은 사이버위협의 사전적 예방을 위한 법적 대응이 요구되고 있다.

---

1) 악성코드(惡性-) 또는 멀웨어(Malware)는 컴퓨터에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭이다. 예전에는 단순히 컴퓨터 바이러스만이 활동하였으나, 1990년대 말들어서 감염 방법과 증상들이 다양해지면서 자세히 분류를 나누기 시작했다. ① 컴퓨터 바이러스 : 프로그램을 통해 감염되는 악성코드, ② 웜 : 컴퓨터의 취약점을 찾아 네트워크를 통해 스스로 감염되는 악성코드, ③ 웜 바이러스 : 웜과 바이러스의 감염 방법을 동시에 갖춘 악성코드, ④ 트로이 목마 : 자가 복제능력이 없는 악성코드, ⑤ 스파이웨어 : 사용자의 정보를 빼내는 악성코드, ⑥ 애드웨어 : 컴퓨터 사용시 자동적으로 광고가 표시되게 하는 악성코드, ⑦ Hoax : 악성코드에 대한 잘못된 정보로 악영향을 끼치는 소문 등으로 분류할 수 있다. 위키백과사전 참조

2) 최근 봇넷(BotNet)이 보안 위협의 중심이 되고 있다. 봇넷이란 봇 악성코드에 감염된 PC들의 집합이다. 대표적인 것이 고전적인 인터넷 채팅 소프트웨어인 IRC(Internet Relay Chat) 기반의 봇넷이다. 봇 악성코드들은 PC를 감염시킨 뒤 봇 제어 서버에서 오는 봇 조종자의 명령에 따라 움직인다. 이렇게 감염된 PC들은 봇 제어 서버를 정점으로 하는 봇넷을 이뤄 봇 조종자의 명령에 따라 다른 컴퓨터를 공격한다. 안철수연구소 자료 참조

3) 'Phishing'은 영어의 'fishing' 이라는 단어와 조합된 것으로 정보를 얻기 위해 낚시질을 한다는 의미로 만들어졌다. 피싱에서의 전형적인 사기성 이메일은 친숙한 은행이나 전자상거래 사이트를 모방한 웹 사이트로 잠재적 희생자들의 방문을 유도한다. 사이트 방문 후에 사람들은 자신의 계정을 업데이트하거나 확인하라고 요구받는다. 그 과정에서 사이트 방문자들이 알지 못하는 사이 주민등록번호나 신용카드 번호와 같은 비밀정보가 누출된다. 피해자를 직접적으로 속이거나 직접적인 피해를 입히지는 않더라도, 이러한 정보들은 개인정보 도용 범죄에 이용되기도 한다. 피해자는 여러 해 동안 개인정보 도용 사실을 알지 못할 수도 있다. 미국의 IT 분야 리서치 전문 회사인 가트너에 따르면, 2007년에 매월 세계적으로 85억 개의 피싱 이메일이 보내졌고, 전체 피해자가 약 320만 명에 달했으며, 피해액은 36억 달러를 넘었다고 한다. 세계 안티피싱워킹그룹에 따르면, 2007년과 2008년에 피싱 웹 사이트의 수가 2배로 늘어났으며, 그 숫자는 6,500개 이상이라고 한다. 브리태니커백과사전 참조

우리나라의 경우에도 2009년 7월 7일에 발생한 인터넷상의 DDoS[4] 사태는 사이버 위험이 현실화됨으로써 사회에 미칠 수 있는 파국적 영향력과 금융거래 중단 등으로 이어지는 네트워크 도미노 현상을 보여줌으로써 사이버 세상의 위험성을 각인시켰다.[5] '7.7사이버테러'[6]라 불릴 만큼 충격을 안겨주었는데, 누가 어떤 목적을 가지고 이런 공격을 해왔는지 명확하게 밝혀지지 않다가 최근에 일부가 드러나고 있어 비상한 관심을 끌고 있다.[7]

한편 '7.7사이버테러'와 관련하여 세계적 보안업체인 맥아피(McAfee)의 크리스토퍼 조던 회장은 이번 공격이 끝이 아니라 "더 큰 공격의 시작"이라고 밝히면서 특히 이번 사이버테러가 '정치·사회적 목적을 가진 해킹'을 의미하는 핵티비즘(Hactivism)이라고 정의하였다.[8]

---

4) DDoS : 한 사이트에 인터넷망으로 동시에 수백만 대의 컴퓨터를 접속시켜 비정상적으로 트래픽을 늘림으로써 해당 사이트를 마비시키는 해킹 방법. 이를 위해 해커들은 불특정 다수의 일반인 PC에 DDoS 공격지시가 담긴 악성코드를 몰래 깔아 '공격용 숙주'로 활용한다.

5) 2009년 7월 7일. 한국과 미국의 주요 사이트에 사이버 공격이 감행되었는데, 청와대·국회·국방부, 미국의 백악관·국무부 등이 공격대상이었다.

6) 미국 실리콘밸리에 본사를 둔 세계적 보안업체 맥아피(McAfee)의 크리스토퍼 조던 부회장은 중앙일보와의 인터뷰에서 "사이버테러는 7월 7일이 아닌 5월 29일부터 시작됐다"고 말했다. 중앙일보 2009. 8. 10. 1면 참조.

7) 국가정보원장은 10월 29일 국회 정보위 국정감사에서 지난 7월 청와대와 국방부 홈페이지 등에 대한 사이버 테러의 진원지와 관련하여, 북한 체신청이 사용해온 인터넷 주소가 당시 사이버 테러에 사용됐다고 보고하였다. 이 인터넷 주소는 중국에서 선을 임대해 쓰고 있었으며, 지난 7월 당시 발생했던 한국과 미국의 26개 인터넷 사이트에 대한 공격 경로를 추적해서 이같은 내용을 확인한 것으로 밝혔다. 국정원은 그동안 당시 사이버 테러가 북한의 소행이라고 추정해왔지만 구체적인 북한 관계기관의 인터넷 주소를 밝힌 건 이번이 처음으로, 이에 따라 북한 정부가 당시 사이버 테러에 조직적이고 의도적으로 개입했을 가능성이 커진 것으로 분석되고 있다. 2009년 10월 30일 KBS 뉴스기사 참조

8) 핵티비즘(Hactivism) : 경제적 이득을 취하려는 해킹이 아닌 정치·사회적 목적을 가지고 이뤄지는 사이버공격. 해커(hacker)와 행동주의(activism)의 합성어다. 인터넷이 일반화되면서 나타난 '사이버 세계의 정치·사회적 운동'을 의미한다. 2002년 포르투갈의 해커들이 '동티모르를 독립시키라'는 구호를 내걸고 인도네시아 정부의 사이트를 마비시킨 사건은 핵티비즘의 전형적 사례다. 중앙일보 2009. 8. 10. 1면, 4면 및 5면 참조.

사이버테러 또는 사이버공격이 증가하는 이유로는 첫째, TCP/IP 네트워크 구조[9]와 MS 윈도우 운영체제로 대표되는 획일화된 인터넷환경, 둘째, 초고속 정보통신 인프라의 고도화로 네트워크와 서버의 성능이 향상되었으며 이에 따른 웜·바이러스[10] 전파속도의 가속화, 셋째, 사이버공격의 자동화로 피해자가 또 다른 가해자가 되어 본인도 모르는 사이에 다른 시스템을 공격함으로써 기하급수적으로 피해시스템이 증가한다는 것 등을 들 수 있다.[11]

해킹,[12] 바이러스 유포 등 사이버 침해행위로 인하여 국가 및 민간의 정

---

9) TCP/IP(Transmission Control Protocol/Internet Protocol의 약어) : 컴퓨터와 데이터통신장치를 통신망에 접목시키기 위하여 사용되는 100가지가 넘는 데이터 통신 프로토콜 집합에 대한 일반적인 이름이다.

10)컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성 프로그램을 일반적으로 컴퓨터 바이러스라고 말한다. 컴퓨터 바이러스는 성격이 조금 다른 3가지 종류, 즉 바이러스, 웜, 트로이목마로 나눌 수 있다. 컴퓨터 바이러스는 감염 대상을 가지고 있어 파일에 기생하면서 다른 사용자에게로 옮겨다니는, 말 그대로 바이러스이다. 반면, 웜이 컴퓨터 바이러스와 다른 점은 자기 복제를 한다는 것이다. 즉, 웜은 감염 대상을 갖지 않는다. 한편 트로이목마는 사용자의 정보를 빼가는 악성 프로그램이다. 따라서 엄격히 구분하자면 웜과 트로이목마는 바이러스에 포함되지 않는다. 하지만 넓은 의미에서 이 3가지를 모두 컴퓨터 바이러스로 일컫기도 한다. 웜은 보통 인터넷 전자우편의 첨부파일 형태로 퍼져나가고, 일단 파일이 실행되어 웜에 감염되면 자기복제를 통해 급속도로 퍼진다. 대표적인 웜바이러스에는 '프리티 팍'과 '콜레라'가 있다. 프리티 팍 바이러스는 프랑스에서 만들어진 것으로 추정되는데, 먼저 감염된 PC의 사용자가 등록해 둔 전자우편 주소록을 읽어 다른 PC로 옮겨가면서 PC에 들어 있는 중요 정보들을 유출시키는 것이 특징이다. 콜레라 바이러스는 독일의 해커 사이트에서 발견된 것인데, 자동으로 전자우편의 주소를 찾아 메시지를 전송하면서 전자우편 서버를 정지시키는 데다, 감염된 디렉터리에 있는 모든 실행파일의 실행을 방해해 프로그램을 무력화시킨다. 웜은 이렇게 첨부된 메일을 보내 인터넷 속도나 시스템에 무리를 줄 뿐만 아니라, 하드디스크를 포맷하거나 사용자 정보를 빼가는 등 특별한 증상을 가져오는 경우도 있다. 또한 최근에 발견된 웜은 전자우편을 보낼 때마다 이름을 달리하여, 사용자가 쉽게 알아채지 못하는 등 피해가 점점 커지고 있다. 한국에서는 2003년 1월 25일 웜바이러스에 감염되어 주요 서버가 다운되어 전국적으로 인터넷망이 정지되는 바람에 엄청난 피해를 입은 사례가 있다. 브리태니커 백과사전 참조

11) 이종환,「사이버상에서의 정보보호를 위한 정부역할 연구 - 민간부문을 중심으로」중앙대 박사학위논문(2006), 30면.

12) 해킹(hacking)은 컴퓨터 네트워크의 보안 취약점을 찾아내어 그 문제를 해결하고 이를 불법적인 목적으로 이용되는 것을 방지하고자 하는 행위이다. 하지만 대한민국에서

보통신망과 정보시스템에 대한 위협이 증가함에 따라 국가 차원의 체계적인 정보보호조치가 필요하게 되었다.

현재까지 각국의 상황을 살펴보면, '물리적 테러'에 대해서는 관련 법령 및 조직들의 정비가 상당히 진척되어 있는 반면, 사이버상에서 발생하는 '논리적 테러'에 대해서는 체계적인 법령과 조직의 정비가 불완전하다는 것이 일반적인 견해이다.[13] 이는 사이버테러가 발생한 경우에도 가시적인 피해가 발생하기 전까지는 자신이 공격당했는지의 여부에 대해서도 불확실하고, 피해규모를 산정하기가 어려우며, 관련기관 역시 확실하게 확정할 수 없기 때문인 것으로 보인다. 그럼에도 불구하고 사이버테러가 발생하여 주요 국가기관의 정보시스템을 파괴하여 국가기능을 마비시키는 경우에는 헤아릴 수 없는 전국적인 대규모의 인적·물적 피해가 예상된다.

그런 측면에서 사이버상에서 일어나는 여러 가지 사안 중에서 국가적 차원에서 접근해야 한다고 생각하고 있는 것이 사이버테러이다. 따라서 사이버테러의 의미와 특징에 대한 정확한 이해가 필요하다. 이러한 사이버테러를 포함한 사이버위협에 대한 유럽연합(EU), 독일, 일본 및 미국 등의 정보보호 관련법제 및 추진체계를 살펴본 뒤, 우리나라의 정보보호 관련법제 및 추진체계에 대한 분석을 하고자 한다.

는 해킹에 대한 잘못된 인식으로 인해 '적법한 권한을 갖지 않고 다른 사람의 데이터 정보에 접근하여 이를 가져가거나 수정하는 것'으로 종종 오해되기도 한다. 그러한 의미를 갖는 단어는 해킹이 아니라 크래킹이다. 한편, 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서도 "침해사고"를 정의하면서, ""침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다."(제2조 7호)고 하고 있다. 위키백과사전 참조

13) 지성우, "독일의 사이버위기 관련 법제의 현황과 전망"「사이버위기관련 법제의 현황과 전망」(단국대 법학연구소, 2009. 5. 29), 35면 참조

제2장 사이버테러와 정보보호의 의의

제1절 사이버테러의 의의

Ⅰ. 사이버테러의 의의

사이버테러(Cyber Terror)가 무엇인가에 대해서는 여러 가지 개념을 혼용하여 사용하고 있으며 국가마다 미묘한 차이를 보여주고 있다.
먼저 사전적으로는 "주요기관의 정보시스템을 파괴하여 국가 기능을 마비시키는 신종 테러로서 정보화시대의 산물로서 컴퓨터망을 이용하여 데이터베이스화되어 있는 군사, 행정, 인적자원 등 국가적인 주요 정보를 파괴하는 것"을 의미한다.

미국에서 사이버테러라는 개념은 "정치적·사회적 목적을 달성하기 위하여 특정 국가 또는 그 국민을 위협하거나 협박하고자 할 때 컴퓨터 네트워크 및 그 속에 저장된 정보를 파괴하겠다고 위협하거나 파괴하는 불법행위 또는 법적으로 승인된 권한없이 사이버시스템에 침입하여 폭력, 파괴 또는 방해를 고의적으로 사용하거나 사용하겠다고 위협하는 행위"라고 정의한다. 이것은 정부에 관한 것 뿐만 아니라 개인에 대해서도 적용하는 개념으로 이해되고 있다.

일본에서 사이버테러라는 개념은 "일반적으로 컴퓨터나 네트워크를 통해서 각국의 국방, 치안 등과 관련되는 컴퓨터 시스템에 침입하여 데이터를 파괴하는 등의 수단으로 국가 또는 사회의 중요한 기반을 기능부전

에 빠뜨리는 행위"[14]이다. 일선 경찰은 시행실시 대상을 명확히 한다는 측면에서 "중요인프라의 기간시스템에 대한 전자적 공격 또는 중요 인프라의 기간시스템에 중요한 장해, 전자적 공격에 의한 가능성이 높은 것[15]"이라 정의하고 있다. 여기서 중요 인프라란 정보통신, 금융, 항공, 철도, 전력, 가스, 정부・행정서비스(지방공공단체 포함) 등 각 분야의 사회기반을 의미한다. 또한 기간시스템이란 국민생활 또는 사회경제활동에 불가결한 역무의 안정적 공급, 공공안전확보 등에 중요한 역할을 하는 컴퓨터시스템을 지칭한다. 따라서 중요인프라의 기간시스템이란 은행의 주요 시스템, 철도회사의 열차운행관리 시스템, 전기회사의 발전 및 변전・송배전 시스템 등이라 할 것이다. 한편 전자적 공격이란 인터넷 등의 전기통신회선을 경유한 전기신호에 의해서 기능부전 또는 파괴하는 공격을 말한다. 전형적인 예로서는 과부하에 의해 시스템의 기능 이상이 오도록 하는 DoS 공격이나 표적시스템에 부정 액세스를 통해 중요한 내부 데이터를 개찬, 소거하도록 하여 기능 이상이 오도록 하는 행위 등이다. 요컨대 일본사회에서 보통의 시민생활을 영위하는데 불가결한 인터넷 등에서 일어난 공격이나 그 공격으로 인하여 발생한 장해를 사이버테러라고 개념짓고 있는 것으로 판단된다.

한편 "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄(logic bomb)·[16] 메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신

14) 양근원, "사이버테러 대응과 현행 절차법 검토"「인터넷법연구」제3권 제1호, 2004, 183면

15) 大泉 雅昭, "警察のサイバーテロ對策"「電氣通信」68(通卷697), 2005, 38項

16) 보통의 프로그램에 오류를 발생시키는 프로그램 루틴을 무단으로 삽입하여, 특정한 조건의 발생이나 특정한 데이터의 입력을 기폭제로 컴퓨터에 부정한 행위를 실행시키는 것. 프로그램이 전혀 예상하지 못한 파국적인 오류를 범하게 한다. 주로 이메일폭탄, 전자편지폭탄, 컴퓨터 바이러스 등과 같이 인터넷 등 컴퓨터 통신망을 이용한 범죄나 사이버 테러리즘의 수법으로 사용된다. 오류를 발생시키는 부호의 삽입에는 보통 트로이 목마를 응용한다. Daum백과사전 참조

망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말하며(국가사이버안전관리규정 제2조제2호) "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다(동조제3호).

Ⅱ. 사이버테러의 특징

사이버테러를 일으키기 위해 필요한 최소한의 것은 인터넷에 연결되는 컴퓨터 1대면 충분하다. 시·공간적으로 제한받았던 고전적인 테러에 비교하면 엄청난 차이를 보인다. 그 차이는 먼저 ① 지리적, 시간적 제한이 없다는 것이다. 전 세계 어디든 접속되는 전기통신회선을 경유하면 거리나 장소, 시간의 제한없이 공격을 감행할 수 있다. ② 익명성이 유지된다는 것이다. 물론 IP 어드레스나 아이디 패스워드 등의 식별기호가 필요하다고 하지만, 도용이나 해킹, 복수의 서버를 사용한다든가, 복수의 국가에 소재하는 서버를 경유한다든가 하는 방법으로 추적이 곤란하다. ③ 흔적이 남지 않는다는 것이다. 증거로서 남아야 할 전자적 기록이라는 것은 바꾸거나 소거가 용이하기 때문이다. ④ 공격이 소요되는 비용이 적다는 것이다. 인터넷으로 접속하는데 필요한 회선비용, 단말기 등은 일반적인 테러에 비교할 것이 아니다.

제2절 정보보호의 의의

Ⅰ. 정보보호의 의의

정보보호(Information Security, 정보보안)는 정보를 여러 가지 위협으로부터 보호하는 것을 뜻한다. 정보보호란 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미하며 정보를 제공하는 공급자 측면과 사용자 측면에서 이해할 수 있다. 먼저 공급자 측면에서는 내•외부의 위협요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호•운영하기 위한 일련의 행위를 의미하며 사용자 측면에서는 개인정보 유출, 남용을 방지하기 위한 일련의 행위를 의미한다.[17]

Ⅱ. 정보보호의 주요목표

정보에 대한 위협이란 허락되지 않은 접근, 수정, 노출, 훼손 및 파괴 등이다. 정보에 대한 위협은 나날이 늘어가고 있기 때문에 모든 위협을 나열할 수는 없으나, 전통적으로 다음의 세 가지가 정보보호의 주요한 목표이다(때로는 정보보호(정보보안)만이 아닌 보다 넓은 보안의 목표로 이야기되기도 한다).

첫째가 기밀성(機密性, confidentiality)이다. 이는 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 비밀보장이라고

17) 위키백과 참조

할 수도 있다. 원치않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다. 둘째는 무결성(無缺性, integrity)이다. 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다. 다시 말하면, 수신자가 정보를 수신했을 때, 또는 보관돼 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 첨삭되지 않았음을 확인할 수 있도록 하는 것이다. 셋째는 가용성(可用性, availability)이다. 허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것이다. 최근에 네트웍의 고도화로 대중에 많이 알려진 서비스 거부 공격(DoS 공격, Denial of Service Attack)이 이러한 가용성을 해치는 공격이다.[18]

18) 위키백과 참조

제3장 주요국가의 정보보호 관련법제 및 추진체계

제1절 서언

현재까지 세계 각국의 상황을 살펴보면, '물리적 테러'에 대해서는 정보보호 관련 법령 및 추진체계의 정비가 상당히 진척되어 있는 반면, 사이버상에서 발생하는 '논리적 테러'에 대해서는 체계적인 법령과 조직의 정비가 불완전하다는 것이 일반적인 견해이다. 이는 사이버테러가 발생한 경우에도 가시적인 피해가 발생하기 전까지는 자신이 공격당했는지의 여부에 대해서도 불확실하고, 피해규모를 산정하기가 어려우며, 관련기관 역시 확실하게 확정할 수 없기 때문인 것으로 보인다. 그럼에도 불구하고 사이버테러가 발생하여 주요 국가기관의 정보시스템을 파괴하여 국가기능을 마비시키는 경우에는 헤아릴 수 없는 전국적인 대규모의 인적·물적 피해가 예상된다. 그런 측면에서 사이버상에서 일어나는 여러 가지 사안 중에서 국가적 차원에서 접근해야 한다고 생각하고 있는 것이 사이버테러이다.

이러한 사이버테러를 포함한 사이버위협에 대한 유럽연합(EU), 독일, 일본 및 미국 등의 정보보호 관련법제 및 추진체계에 대해 살펴보고자 한다.

제2절 유럽연합

Ⅰ. 유럽연합의 정보보호 인식제고활동

유럽의 일반적인 정보보호 정비움직임을 이해하기 위해서는 유럽연합(EU)의 사이버위협에 대한 정보보호에 대한 이해가 선결적이라고 할 수 있다.

유럽연합은 집행위원회 산하 정보사회와 미디어 이사회(Information Society and Media Directorate and General, INFSO DG)와 유럽네트워크정보보안청(European Network and Information Security Agency, ENISA)의 정보화 및 정보보안정책을 통해 사이버위협에 대응하고 있다. 즉, INFSO DG의 관련 정책으로 “eEurope”, “안전한 정보사회를 위한 전략”, “미디어 리터러시”, “안전한 인터넷 플러스 프로그램” 등이 있으며, ENISA는 “ENISA의 역할과 비전” 및 각종 가이드라인을 통해 활발한 정보보호 인식을 제고하며 활동을 수행하고 있다.

EU의 정보보호 인식제고 활동은 첫째, 정보보안 인식제고를 위한 프로세스의 마련 및 효과성 측정을 위한 핵심성과지표 개발 등 체계화된 정보보안 인식제고 프로그램의 마련, 둘째, 정부와 다양한 분야의 민간기업 간 긴밀한 협조체계를 구축함으로서 효율적이고 효과적인 정보보호 인식제고 업무수행, 셋째, 각종 멀티플라이어(multiplier)를 활용한 대상별, 수준별 정보보호 교육 및 훈련의 중요성 강조 등과 같은 특징을 가진다.[19]

Ⅱ. 정보보호 추진체계

그리고 사이버위협에 대응한 유럽연합의 정보보호 추진체계로는 유럽네트워크정보보안청(ENISA), 컴퓨터비상대응팀(CERT), 사이버방어센터

19) 최철호, “독일의 정보통신망 정부규제 및 자율규제 현황”「정보통신망 안전성 및 신뢰성 확보방안」(2009. 8. 10), 29-30면 참조

(The Cooperative Cyber Defence Centre of Excellence), 조기경보시스템(EWIS : European Warning and Information System) 등이 있다. 이 중에 ENISA는 정보보안에 대한 유럽 각국의 초국가적 협력을 위해 2004년에 설립되었는데, 보안사고 처리를 위한 데이터 수집, 프레임워크 및 신뢰지수 측정방안 개발, 보안정보 공유 및 경고시스템의 실행가능성 검토 등을 수행한다. 또한 ENISA는 유럽 각국에 컴퓨터비상대응팀(CERT) 구축을 지원하고 있는데 2005년 9개국에서 2008년 6월 현재 15개국에 CERT 설립을 지원하였다. 또한 각국의 수준에 맞는 컨설팅을 실시하며 우수 CERT 활동 사례 등도 전파하는 것을 주 임무로 하고 있다.

제3절 독일

Ⅰ. 정보보호 관련법제

독일에서는 1970년대까지 테러방지를 위한 별도의 입법을 하지 않고 경찰법과 형법에 의해 테러방지를 수행하여 왔다.

독일의 안보관련 형법규정의 특징은 국가안보관련 조문이 형법전상 독립된 장으로 구성되어 있지 않고 각 개별 장마다 해당부분에서 헌법위반행위 또는 조직, 공익에 반하는 행위 또는 조직 등에 대하여 개별적으로 처벌규정을 두고 있다는 점이다. 형법각칙의 총 30개 장 중 제1장 평화교란, 내란죄, 민주적 법치국가의 위험(제80조-92b조), 제2장 국가반역죄, 외적 안전의 위험(제93조-제101a조), 제5장 국가방위에 대한 범죄(109조-109k조) 등에 테러에 대한 규정들이 산재되어 있다.

이와 같이 독일에서는 현재까지도 테러 또는 사이버테러 예방이나 처벌을 위한 특별한 법률을 제정하고 있지는 않으나, 각 개별 형벌법규를 통하여 테러와 사이버테러 방지에 대비하기 위한 규정을 두고 있다.[20]

독일의 정보보호 관련법제로는 정보통신법(Telekommunikationsgesetz: TKG), 통신서비스법(Teledienstegesetz, TDK), 연방데이터보호법(Federal Data Protection Acts, BDSG), 정보통신서비스정보보호법(Teledienstdatenschutzgesetz, TDDSG), 전자서명법(Act on Online Conditions for Electronic signatures), 통신법, 형법, 연방정보기술안전청 설치에 관한 법률, 연방의 정보기술의 보안강화를 위한 법률 등이 있다.[21]

먼저 2004년 제정된 정보통신법은 정보기관의 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷서비스제공자 등 정보통신서비스를 제공하는 모든 책임자에게 고객정보를 정부에서 접근 가능한 상태로 유지할 의무를 규정하고 있으며, 그러한 데이터는 정부의 감시기관이 직접 접근할 수 있어야 한다고 규정하고 있다.

2004년의 정보통신법은 상업적인 인터넷서비스제공자뿐만 아니라 비상업적인 서비스제공자나 전자게시판 운영자에 대해서도 적용된다. 만일 정보통신서비스제공자가 이러한 조치를 실행하지 않을 경우 그 운영을 중지시킬 수 있도록 규정하고 있다.

다음으로 통신서비스법은 인터넷서비스제공자의 정보차단의무에 대해

20) 지성우, 앞의 논문, 44면 참조
21) 최철호, 앞의 논문, 30-33면 참조

규정하고 있다. 일정한 요건 하에서 위법한 정보를 인지한 경우의 인터넷서비스제공자의 정보차단의무를 규정하고 있으며 의무를 이행하지 않은 경우에는 면책되지 않는다고 규정하고 있다.

그리고 연방데이터보호법은 개인정보를 보호하기 위한 기본법이다. 개인정보의 정의에서부터 정보주체의 권리와 정보처리자의 각종 의무, 제3국으로의 정보이전, 비디오감시, 익명성, 스마트카드, 민감한 정보의 수집 등에 대한 내용을 담고 있다. 특히 2003년에는 비디오감시에 관한 규정(제6b조)을 신설하였다. 비디오감시는 ① 공공기관의 임무수행의 경우, ② 주거권의 실현을 위한 경우, ③ 구체적으로 확립된 목적을 위해 권리있는 이익의 실현을 위하여 필요하고 관계당사자의 보호받을 이익이 우월하지 않은 경우에 한해 허용된다(동조제1항). 수집된 데이터의 처리와 이용은 그 데이터가 달성하려는 목적을 위하여 필요하고 당사자의 보호법익이 우월하지 않을 때에만 인정된다(동조제2항). 다른 목적을 위한 개인정보의 처리와 이용은 위험의 방지와 국가와 공익의 안전을 위하여 그리고 범죄행위의 추적을 위하여 필요한 경우에 한하여 허용된다(동조제3항). 비디오감시를 통하여 수집된 데이터가 특정한 개인과 연결될 경우에는 그 처리와 이용에 관하여 이를 당사자에게 통지하여야 한다(동조제4항). 비디오감시를 통하여 수집된 데이터가 목적달성을 위해 더 이상 필요하지 않을 경우 또는 지속적인 저장이 당사자의 보호법익에 상충될 때에는 지체없이 삭제되어야 한다(동조5제항).

또한 정보통신서비스정보보호법은 정보통신서비스 이용관계에서의 개인정보의 수집·처리에 관하여 규율하여 인터넷 포털사이트 운영자, 이메일서비스제공자, 온라인 게임서비스제공자 등의 정보통신서비스제공자가 고객정보를 이용·처리하는 행위에 직접적으로 적용된다. 동법은 정

보보안 범위, 서비스제공자의 사용자의 개념 정의, 정보보안 원칙, 서비스제공자의 의무, 보호되는 정보의 내용, 연방정보보안감독관의 역할 등에 대해서 규정하고 있다.

그리고 전자서명법은 EU에서 1999년 12월에 채택한 전자서명 지침에 따라 제정되었는데 주로 온라인상의 안전성 확보를 위한 인프라 관련 조항이 중심내용으로 되어 있다.

통신법은 제113a조에서 “데이타 저장의무”를 규정하고 있다. 그리고 제113b조는 “제113a조에 의해 저장된 데이타의 사용”에 대해 규정하고 있다.

형법은 제202a조에서 “데이타 탐지”를, 제202b조에서 “데이타 불법취득”을, 제202c조에서 “데이터의 탐지 및 취득의 예비”를, 제303b조에서 “컴퓨터 사보타지”를 규정하고 있다.

연방정보기술안전청 설치에 관한 법률은 연방내무부장관 직속으로 연방정보기술안전청의 설치를 목적으로 하면서, 연방행정청의 과제에 대해 구체적으로 규정하고 있다(제3조).

연방의 정보기술의 보안강화를 위한 법률은 연방정보기술안전청의 권한을 확대하고 연방의 정보기술 인프라에 대한 공격을 방지하기 위한 여러 가지 수단을 연방정보기술안전청에 부여하고 있다. 무엇보다도 다른 기관의 공식적인 요청이 없더라도 연방행정에서의 정보기술보안을 높이고 연방의 정보기술에 대한 위험을 방지하기 위하여 독자적으로 활동하는 권한을 연방정보기술안전청에 부여하고 있다. 이 법률은 보안을 위한

일반적인 기술적 지침에 관한 규정, 개별적으로 정보기술의 설정을 위한 규정, 구체적인 위험의 방지를 위한 조치에 관한 규정을 포함하고 있다.

Ⅱ. 정보보호 추진체계

독일의 정보보호 추진체계로는 먼저 독일연방 수상의 직속기관으로서 연방정보기관(BUndesnachrichterdienst, BND)이 있다. 다음으로 국내 치안유지 및 안전에 관한 사항은 연방내무부(Bundesministerum des Innern, BMI)가 담당하고 있다. 이러한 업무를 수행하기 위하여 연방내무부에는 다양한 산하기관을 운영하고 있는데, 그 중 하나가 연방정보기관과 유사한 기능을 하고 있는 연방헌법보호청(BfV)이다. 다만, 연방헌법보호청은 국내의 마약, 테러범 등에 대한 정보수집을 담당하는데 반하여,[22] 연방정보기관(BND)은 주로 국제관계에서의 대외적 첩보업무를 수행하는 점에서 업무의 성격에 차이가 있다. 또한 연방내무부 산하기관 중 경찰업무국은 치안유지와 범죄예방 및 마약업무를 담당하고 있다. 또한 연방국경의 수비를 위하여 내무부 산하에 연방국경수비대가 설치되어 있으며, 암보담당국은 독일 국내안보 및 질서유지에 관한 업무를 담당하는 부서로서 그 주요임무는 마약범, 스파이, 극우세력 및 기타 정치적·비정치적 테러를 검거하는데 있다. 또한 연방국방부 산하에 군관련 정보 및 첩보를 수집하는 군정보기관(AMA) 역시 군 내부에서의 정보활동을 수행하고 있다.[23] 독일에서의 정보기관들의 임무와 권한의 특징은 국내

22) 연방헌법보호청은 국내안보 분야라 할지라도 경찰이 정치에 개입할 수 있는 여지가 있는 분야를 담당함으로써 비밀경찰의 출현을 방지하는 역할을 수행한다. 연방헌법보호청은 자유민주적 기본질서를 해하는 행위, 연방이나 주의 안전을 해하는 행위로부터의 보호, 폭력의 사용 또는 이로 인해 발생하는 독일 연방공화국에 대한 위해행위, 국민의 생명·신체에 대한 위협적인 사상(기본법 제9조제2항) 특히 국민의 평화적인 공동생활을 저해하는 행위, 내국에서의 간첩행위에 대한 비밀 첩보공작 등의 업무를 수행한다.

안보에 있어서의 군대의 역할이 배제되어 있고, 국내안보의 주요담당기관으로서의 경찰의 지위확립과 독자적인 연방헌법보호청이 설치되어 있어 정치경찰이 인정되지 않는다는 데 있다.[24] 특히 국내안보에 대해서는 군대의 권한이나 연방정보기관의 권한이 배제되고 경찰이 중심적인 역할을 수행한다. 다만 경찰조직에 대해서는 연방정부가 구성을 담당하며 업무활동에도 관여한다고 한다.[25] 문제는 향후 테러의 국제화·보편화가 진행됨으로써 연방경찰, 연방헌법보호청, 연방정보기관(BND), 군정보기관(MAD) 등에서의 업무영역을 명확히 구분할 수 없는 경우가 다수 발생할 것이라는 점이다. 이에 따라 가령 연방헌법보호청의 경우 수집된 정보를 수사기관에 통보하도록 규정(제20조, 제21조)하고 있는 등 독일 내 대테러 유관기관 간 협조체제의 유기적 구축을 통해 해결하고 있다.

제4절 일본

Ⅰ. 정보보호 관련법제

일본은 이미 과학·기술 선진국으로서 첨단 정보통신기술 능력을 갖추었지만 사이버공격 대비능력은 막강한 경제력과 첨단기술력에 비추어 다소 뒤떨어져 있는 것으로 알려지고 있다.[26] 오늘날 일본은 사이버공격에 대응하기 위한 다양한 대책을 마련해 나가고 있다. 일본에서는 아직까지

---

23) 김일환, "독일 기본법상 대테러관련기관과 법제도들에 관한 고찰"「성균관법학」제15권제1호(2003), 82-83면 참조.
24) 지성우, 앞의 논문, 45면 참조
25) 지성우, 앞의 논문, 45면 참조
26) 일본의 정보보안법제에 대해서는 김재광·김정임, "일본의 사이버위기 관련 법제의 현황과 전망"「법학논총」제33권제1호(2009. 6, 단국대 법학연구소), 41면 이하 참조

심각한 사이버테러리즘은 발생하지 않고 있으나, 최근 들어 부정 액세스 사례와 컴퓨터범죄가 급증하고 있다.[27] 일본은 9.11테러 이후 국가차원의 사이버 안보를 위한 다각적인 노력을 기울이고 있는데, 경찰청에서 2004년에 발표한「테러대책추진요강」[28], 내각에 설치된 범죄대책각료회의에서 2003년 12월에 책정한「범죄에 강한 사회실현을 위한 행동계획」[29] 등등이 그에 해당이 된다. 또한 최근 정보 시큐리티 정책회의 의장(관방장관)은 각 부처가 운영하고 있는 서버의 수를 삭감하는 방침을 결정[30]하기도 하였다. 이는 중앙부처의 홈페이지가 개찬되는 사이버 테러 피해에 따른 결정이라고 하며, 서버의 총량을 줄이는 것이 곧 공격대상을 좁히는 것이라는 판단일 것이다.[31] 그러나 사이버테러를 안보적 측면에서 이해하면 그것을 정부와 민간으로 양분하기 어려운 측면이 있다고 하겠다.

2000년 11월에 일본은 IT기본법인「고도정보통신네트워크사회형성기본법」을 제정하고 2001-2005년에 이르는 동안 e-Japan 전략을 통해 국민을 대상으로 하는 인터넷 보급을 적극 추진하는 등 국가정보화를 지속적으로 추진해 왔다. 그 동안 추진한 성과로서 2006년 1월 IT신개혁전략을 발표하였다. IT신개혁전략의 중심은 정보보호라고 할 수 있다. 정부기관

---

27) 하옥현,「국가사이버안보체계 구축전략」(고려대 박사학위논문, 2005), 168면 참조

28) 사이버테러에 관한 정보수집, 수사체계 및 긴급조치능력의 강화, 조사원의 교육훈련충실, 주요 인프라 사업자나 해외관계기관과의 제휴강화 도모 등을 내용으로 한다.

29) 사이버 범죄대책추진 시책이 포함되어 있다.

30) 2009/05/08 産経新聞

31) 우리나라의 경우에도 사이버보안, 산업보안 등으로 불리는 정보통신 인프라를 통한 다양한 형태의 침해사고가 발생하고 있고 한 조사자료에 따르면 일일 평균 1만7000여 건의 사이버공격 시도가 이루어지고 있는 것이 현실이다. 특히 정부기관의 수많은 대국민 서비스가 전자정부 형태로 집적, 관리되고 있기 때문에 사이버공격은 더 이상 개인이나 기업을 위협하는데 그치지 않고 국가 시스템을 전복시킬 수 있는 위협으로 인식되고 있다.

통일기준에 따른 정부기관 및 지방공공단체의 정보보호대책 강화, 안전기준을 정비하는 시도를 통한 주요 인프라에 대한 정보보호대책 마련, 기업 정보보호수준 강화를 위한 대책 마련, 개인의 IT 이용에 대한 불안감 해소를 위한 교육 및 환경구축, 정보보호백서의 발간, 사이버범죄 방어를 위한 정보보호 기반의 형성, 청소년유해정보의 차단 등 인터넷 이용환경 개선, 정보윤리교육 추진 등이 그 내용이다.

최근 일본은 e-Japan 이후에 이를 계승하여 발전하는 한편으로 2006년에 계획한 ICT(Information Communication Technology) 기술력을 주축으로, 2010년부터는 유비쿼터스에 기반한 u-Japan 시대를 주창하고 있다[32]. 이것은 미국에서의 성공사례를 참고한 것으로 국제경쟁력을 높이고 지속적인 경제성장을 도모하려는 것으로 인구감소 및 새로운 국제 트렌드에 발맞추기 위한 기획이다. 이를 통해 컴퓨터와 인간과의 결합이 가속화되는 유비쿼터스 환경이 준비되는 것이다. 이처럼 하이엔드 기술이 현실로 유입되는 것은 일본에서도 마찬가지이다. 현재의 단순 사이버테러와 공격은 아직 국가적 차원의 위기를 초래할 만큼은 아니라는 의견이 있으나, 유비쿼터스 시대가 도래하게 되면 기존의 단순한 컴퓨터 네트워크 시대와는 다른 가공할 파괴력을 발휘할 수도 있다[33]. 그만큼 보안문제는 더 강화되어야 할 필요가 있게 되었다.

u-Japan 전략은 순기능과 동시에 일어나는 역기능을 해소하기 위해 정보보안을 포함하는「안심안전 21전략」은 총 100대 과제를 선정하고 있는데 그 중 21분야는 다음과 같다. 의료분야의 프라이버시를 보호하고,

---

32) 총무성 http://www.soumu.go.jp/menu_seisaku/ict/u-japan/index.html

33) 허태회 외, "세계 주요 강대국들의 정보전 준비와 대응체계"「국방연구」(제49권 제1호, 2006년), 38면

공적 기관 및 사업자가 보유하고 있는 개인정보보호, 일반사용자의 정보보호의식 향상, 정보네트워크의 취약성 극복방안 마련, 컴퓨터 바이러스에 대한 대응, 전자결제의 안전성 확보, 네트워크를 이용한 악질 상거래 수법에 대한 대응, 스팸메일에 대한 대응, 지적재산권 보호방안 마련, 디지털재화의 저작권보호, 컨텐츠의 2차적 활용 부족문제 해소, 정보기술 연구개발에 있어서 과학기술 윤리문제, 교육분야의 ICT 이용촉진, ICT 인재부족문제 해소, 교통통신망 이용서비스의 지역격차해소, 전자정부의 격차해소 등.

사이버 범죄인 부정액세스의 경우 2008년도에 전국 도도부현 경찰서가 경찰청에 보고한 부정액세스 행위를 대상으로 한 통계로 전년도에 비해 471건이 증가한 2,289건[34]이다. 이중 해외에서 유래한 액세스는 214건, 국내에서 발생한 액세스는 1,993건, 출처를 알 수 없는 경우가 82건이었다. 해외에서 유래한 액세스 건은 그 이전 연도인 2004년 37건, 2005년 53건, 2006년 37건, 2007년 79건에 비하면 급격하게 증가하였음이 눈에 띈다. 이 때문에 국제적 제휴에 대한 의견에 힘이 실리고 있는 것으로 판단된다. 피해자는 일반기업체가 685건, 대학 연구기관 등이 5건, 기타 10건(행정기관 6건 포함)이며, 부정액세스 피의자는 10대가 48명, 20대 42명, 30대 35명, 40대 11명 그 외 연령대가 소수를 차지한다. 부정액세스 행위를 한 피의자의 연령대는 정보시대를 이해하는 젊은 층에 집중되어 있음을 알 수 있다.

그러나 국가의 인프라를 위협하는 국가차원의 사이버테러는 이와는 구분될 필요가 있다. 일본의 국가적 차원의 사이버테러는 2000년 1월 말부

34) 총무성 부정액세스 행위 발생상황 2008,
http://www.soumu.go.jp/menu_news/s-news/090226_3.html

터 2월 중순에 걸쳐 중앙관청 등의 홈페이지가 부정액세스 당하는 사건이 있었다. 개찬(改ざん)내용은 홈페이지를 모두 파괴하는 것은 아니었다. 일부분이 중국어로 일본을 비판하는 내용으로 변환되었다거나, 미국의 성인 홈페이지로 연결되도록 되어 있었다.

한편 정보보호 관련법제로는「부정액세스행위금지등에 관한 법률」,「무력공격 사태 등에서의 국가의 평화와 독립 및 국가 및 국민의 안전확보에 관한 법률」,「무력공격 사태 등에서의 국민보호를 위한 조치에 관한 법률」그리고 가이드라인 등이 있다.

먼저 고도정보화네트워크의 안전성 및 신뢰성 확보를 위해서「부정액세스행위금지등에 관한 법률」을 두고 있다. 권한없는 자가 액세스하거나 컴퓨터에 침입하거나 이를 조장하는 행위에 대해서는 침입한 후에는 업무방해가 되어 형법이 적용될 수 있다. 그러나 바이러스자체를 규제하는 법률은 현재 존재하지 않으므로 바이러스를 통해서 업무방해나 파괴행위가 있었다면 형법을 적용하여 처벌할 수 있겠지만, 현행법에는 바이러스 작성 등의 행위에 대해서는 처벌이 어렵다고 볼 수 있다.[35]

다음으로「무력공격 사태 등에서의 국가의 평화와 독립 및 국가 및 국민의 안전확보에 관한 법률」은 2001년에 발생한 미국에서의 동시다발테러 등으로 국민에게 불안감을 주는 새로운 위험에 대비해야 할 필요성을 재인식하면서 국가의 긴급사태에 대처할 수 있는 시스템 정비에 돌입했다. 이에 따라 무력공격사태에 대처하기 위해「무력공격 사태 등에서의 국가의 평화와 독립 및 국가 및 국민의 안전확보에 관한 법률」[36]을 제

35) 横内 律子, “情報セキュティの現狀と課題”「立法と調査」第443號(國立國會圖書館, 2004) 참조

정・시행하게 되었다.

그리고 유사법제[37]인「무력공격 사태 등에서의 국민보호를 위한 조치에 관한 법률」(국민보호법)[38]은 무력공격으로부터 국민의 생명, 신체 및 재산을 보호하고, 무력공격이 국민생활 및 국민경제에 주는 영향을 최소화하기 위해, 국가, 도도부현 및 시읍면의 역할분담, 지정 공공기관의 역할, 국민보호를 위한 조치실시 체제 등에 대해서 정하도록 하고 있으며, 총무성과 소방청은 법률의 위임으로 이 법에 있어서 중추적 역할을 수행하며 두 기관에서 이에 관한 계획[39]을 수립하고 있다. 국민보호법은 무력공격에 대해서 대비하고 있다. 그러나 국가의 안전보장에 관계되는 긴급사태라는 것이 단순히 무력공격 사태만이 아니라, 식량, 에너지, 정보통신기술을 이용한 최신의 사이버 테러까지도 포함하여 새로운 위험이 되어 국가와 국민의 존립을 위협하고 불안감을 줄 수 있다는 것까지도 포함시키는 것에 대해 고려할 수 있는 여지가 있는 것으로 생각된다.

그리고 가이드라인으로 중요한 것은「정부기관의 정보시큐리티 대책을 위한 통일기준」이다. 정보시큐리티 정책회의는 정부기관의 정보시큐리티 대책과 관련하여 2005년 9월에「정부기관의 정보시큐리티 대책강화에 관한 기본방침」등을, 동년 12월에는「정부기관의 정보시큐리티 대책을

---

36) 제정 2003년 6월13일 법률 제79호, 최근 개정2006년 12월 22일 법률 제118호

37) 무력공격 사태 등에서 국민보호를 위한 조치에 관한 법률(국민보호법), 무력공격 사태 등에서 미국의 군대행동에 수반하는 우리나라가 실시할 조치에 관한법률(미군행동원활화법), 무력공격 사태 등에서 특정 공공시설 등의 이용에 관한 법률(특정공공시설이용법), 국제인도법의 중대한 위반행위의 처벌에 관한 법률(국제인도법위반처벌법), 무력공격 사태에서 외국군용품 등의 해상운송 규제에 관한 법률(외국군용품해상운송규제법), 무력공격 사태에서 포로 등의 취급에 관한 법률(포로취급법), 자위대법의 일부개정에 관한 법률(개정 자위대법)

38) 2004년6월18일 법률 제112호, 최근 개정 2006년 12월 22일 법률 제118호

39) 총무성국민보호계획(2005) 총무성훈령 제56호, 소방청국민보호계획(2005)

위한 통일기준」(이하 “정부기관 통일기준”이라 한다)을 결정하였다. 정부기관 통일기준에 관해서는 기술이나 환경의 변화에 입각하여 재검토하며, 2007년 6월에는 개정 제2판, 2008년 2월에는 개정 제3판, 2009년 2월에는 개정 제4판안이 결정되었다. 정부기관통일기준 제4판은 제2차 정보보안기준계획안(2009-2011)에 대응하는데 초점을 맞춰 주요 3개의 방향을 설정하고 있다. 먼저 ① 정부기관에 대해서 PDSC 프로세스를 적용하여 운영측면에서 효율을 강화하며 또한 최고정보보안 어드바이저 설치를 의무화하고, 전문가의 지시나 어드바이스가 조직전체에 신속하고 확실하게 반영되도록 대응한다. ② 기술환경의 변화에 따라 웹열람 및 통신시의 위험성에 대응할 수 있도록 웹클라이언트의 보안을 설정하고, 웹사이트 송신시의 안전확보와 관련된 대책을 추가한다. 그러기 위해서 전자메일의 포트 피해가 갖는 위험성에 대응하여 전자메일송신시 인증을 기본적으로 준수하는 것으로 변경한다. 또한 무선랜 환경이 갖는 위약성에 대비하기 위해서 기밀을 요하는 정보가 취급되는 무선랜 환경에서는 통신내용을 암호화하는 것을 추가한다. ③ 실무측면에서 준수되어야 할 항목으로는 기본편과 정보시스템편을 분할하여 성부(省府)대책기준에서 결재하는 수위를 나누어(대책레벨이라고 한다) 용이하게 하여, 기동성있는 운용을 가능하게 한다는 것이다. 그 외에도 ASP(Application Service Provider)・SaaS(Software as a Service)에 필요한 보안가이드라인, 각종 지침으로 가이드라인이 제시되고 있다.

Ⅱ. 정보보호 추진체계

일본의 정보보호 추진체계로는 내각관방성 정보시큐리티센터(NISC: National Information Security Center)[40], 사이버포스[41], 사이버클린센터[42], 국민을 위한 정보보호 사이트[43] 등이 있다.

1. 내각관방성 정보시큐리티센터

2005년 4월 정보보안 대책을 위한 핵심조직이 필요함을 인식한 일본정부는 정보 시큐리티 정책의 기본전략을 결정하는 “정보시큐리티 정책회의”와 그 수행 기관인 「내각관방 정보 시큐리티 센터[44]」를 설치했다. 2006년 2월에 발표된 “제1차 정보 시큐리티 기본계획”은 일본의 정보보안 문제에 관한 국가 전략이다. 이 기본계획은 기초하고 안전하고 안심할 수 있는 IT사회 구현이 목적이다.

가. 조직 및 업무

---

40) http://www.nisc.go.jp/index.html

41) http://www.cyberpolice.go.jp/cyberforce/cyberforce03_01.html 경찰청에서 운영하는 사이버 포스란 발생 사이버 테러 등에 직접 대처함과 동시에 사안대처 활동 지원을 하는 전국에 배치된 정보시큐리티에 관한 기동적 기술부대의 총칭이다. 사이버 포스는 1999년 하이테크 범죄대책에 관하여 도도부현 경찰을 기술적으로 리드하는 국가적 센터로 정보통신국에 기술대책과(현:정보기술 해석과)를 설치하였고, 그 기술적 중핵으로서 동과에 경찰청 기술센터를 설치하는 등 사이버 범죄 대책을 지원하는 체제를 유지하고 있다. 도도부현 경찰간에도 사이버 범죄수사에 필요한 태세를 정비하고, 각 도도부현 경찰들이 신속하게 제휴하도록 하고 있다. 사이버 테러가 일단 발생하면 사회적 영향이 지대하므로 그것을 사전에 방지하고 피해 확대를 방지하기 위해 2001년에 경찰청에 사이버 테러 대책 기술실(통칭:사이버 포스 센터, 경찰법시행규칙 제48조)을 설치하여, 각 관구 경국 등의 사이버 포스(기동적 기술부대)를 배치하는 등 감시・긴급 대처를 위한 체제를 만들었다.

42) https://www.ccc.go.jp 경제산업성과 총무성의 공동사업으로 운영되는 사이버클린 센터는 해당 사이버클린 운영회를 중심으로 IPA, JPCERT, Telecom-ISAC가 실무를 담당한다. 최근 급증하고 있는 악성코드 등 역기능을 방지 예방하기 위한 활동을 목적으로 하며, 일반국민을 대상으로 인터넷 운영과 관련된 각종 정보를 제공한다.

43) http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm 국민을 위한 정보보호 사이트는 총무성이 개인정보보호, 통신인프라의 정보보호 확보, 전자정부 및 지방자치단체의 정보보호 등 공공부문과 대국민 정보보호에 중점을 두고 정보통신정책국에서 정보보호 정책을 시행한다.

44) http://www.nisc.go.jp/index.html

센터장은 안전보장・위기관리담당부 장관보를 보하며, 부센터장(내각심의관), 정보시큐리티보좌관을 둔다. 개별 팀으로는 정보 시큐리티 정책에 관한 중장기 계획이나 연도계획을 입안하는 기본전략책정팀, 정보보안정책에 관한 국제제휴 창구역할을 하는 국제전략팀, 정부기관의 정보 시큐리티 대책을 추진하기 위한 통일적인 기준의 책정과 운용을 추진하는 정부기관총합대책촉진, 취약한 정보나 사안정보 등을 수집・분석・판단하는 한편 정부기관 등에 지원을 하는 중요인프라대책팀, 중요 인프라 행동 계획에 기초하는 정보 시큐리티 대책 및 관민이 제휴하는 사안처리지원팀으로 구성된다.

나. 정보 시큐리티 정책 회의

정보 시큐리티 정책 회의(고도정보통신네트워크사회추진전략본부령 제4조에 근거)[45]는 관민의 통일적・횡단적 정보보안 대책을 추진하기 위한 조직으로 2005년 5월에 내각 관방장관을 의장으로 하여 국가공안위원회 위원장, 방위청장관, 총무대신, 경제산업대신, 정보시큐리티대책에 관하여 우수한 식견을 가진 자로서 고도정보통신네트워사회추진전략본부장으로부터 정책회의에서 심의에 참가하도록 위촉받은 자로 구성된다.

(1) 제1차 기본계획

정보보안과 관련하여 각종 지침과 상황을 발표하고 제안하고 있는 이

45) 2000년 IT기본법으로서 고도정보화통신네트워크사회형성기본법이 제정되었고, 총리부속으로 정보통신기술전략본부(IT전략본부)가 설치되었으며, 그 부속 부회로서 개인정보보호법제전문위원회, 개인정보보호검토부회, 정보시큐리티부회, 전자상거래등검토부회가 설치되었다. 이 중 정보시큐리티부회에는 사이버테러 대책 워킹그룹이 설치되는 안이 검토되기도 하였다.

정책회의는 '시큐어 재팬 2006, 2007, 2008에 이어 2009년도에도 정보보안 안인 '시큐리티 재팬 2009'(SJ 2009: 2009년 5월 5일)에 대해 설명하고 있다[46]. 제1차기본계획(2006-2008년)을 통해 관계자의 의식이 높아졌다는 점(P to P 소프트로 정보유출이 높은 경우, 사이버공격에 정보를 도둑맞을 위험성, 시스템 장해로 사업이 정지되는 위험성 등에서), 우선적 정책추진 대응 구도를 구축했다는 점(정부기관의 통일적 기준에 기초한 대책과 평가, 중요인프라사업자간에 정보공유체제가 구축되었다는 점, 일본과 미국, 일본과 ASEAN간 정보교환), 문제예방을 위한 사전대책에 착수하는 정도의 진전 등을 그 성과로 정리하고 있다.

(2) 제2차 기본계획

제2차 기본계획(2009-2011년)에서는 정책계속과 변화하는 발전을 모토로 사전대책은 발생하기 전에, 문제가 발생해도 냉정하고 신속하게, 사후대응 복구활동추진을 목표로 하고 있다. 또한 사고를 전제로 한 사회 대응력강화를 위한 기반구축, 합리성에 근거한 접근 실현 착수개시, 현재의 경제정세에 대응한 지원착수추진을 중요방향으로 선정하였다. 이처럼 '사고를 전제로 한 사회'를 전제로 하여 2009년도에는 중요인프라 서비스의 유지 및 IT 장해시 신속하게 복구 등을 확보하는 것을 위해 관민 각주체의 공통인식을 형성·정착할 수 있도록 환경을 정비하며, 전자정부를 편리하고 안심하고 사용할 수 있는 적절한 정보보안대책을 강화하고, 정보보안을 위한 인적기반을 강화, 국경을 초월하여 발생하는 IT장해에 효과적으로 대처하기 위한 국제제휴 및 협조를 지속적으로 추진, IT를 안심하고 사용할 수 있는 기술전략을 적극적으로 추진하는 것을 핵심정책으로 한다.

---

46) http://www.nisc.go.jp/conference/seisaku/index.html

2. 사이버포스

경찰청에서 운영하는 사이버 포스[47]란 발생 사이버 테러 등에 직접 대처함과 동시에 사안대처 활동 지원을 하는 전국에 배치된 정보시큐리티에 관한 기동적 기술부대의 총칭이다. 사이버 포스는 1999년 하이테크 범죄대책에 관하여 도도부현 경찰을 기술적으로 리드하는 국가적 센터로 정보통신국에 기술대책과(현:정보기술 해석과)를 설치하였고, 그 기술적 중핵으로서 동과에 경찰청 기술센터를 설치하는 등 사이버 범죄 대책을 지원하는 체제를 유지하고 있다.

도도부현 경찰간에도 사이버 범죄수사에 필요한 태세를 정비하고, 각 도도부현 경찰들이 신속하게 제휴하도록 하고 있다. 사이버 테러가 일단 발생하면 사회적 영향이 지대하므로 그것을 사전에 방지하고 피해 확대를 방지하기 위해 2001년에 경찰청에 사이버 테러 대책 기술실(통칭 : 사이버 포스 센터, 경찰법시행규칙 제48조)을 설치하여, 각 관구 경국 등의 사이버 포스(기동적 기술부대)를 배치하는 등 감시·긴급 대처를 위한 체제를 만들었다.

3. 사이버클린센터, 국민을 위한 정보보호 사이트

경제산업성과 총무성의 공동사업으로 운영되는 사이버클린 센터[48]는 해당 사이버클린 운영회를 중심으로 IPA, JPCERT, Telecom-ISAC가 실무를 담당한다. 최근 급증하고 있는 악성코드 등 역기능을 방지 예방하

47) http://www.cyberpolice.go.jp/cyberforce/cyberforce03_01.html
48) https://www.ccc.go.jp

기 위한 활동을 목적으로 하며, 일반국민을 대상으로 인터넷 운영과 관련된 각종 정보를 제공한다.

국민을 위한 정보보호 사이트[49]는 총무성이 개인정보보호, 통신인프라의 정보보호 확보, 전자정부 및 지방자치단체의 정보보호 등 공공부문과 대국민 정보보호에 중점을 두고 정보통신정책국에서 정보보호 정책을 시행한다.

제5절 미국

Ⅰ. 정보보호 관련법제

미국의 정보보호정책은 1980년대부터 나타나기 시작하였고, 초기에는 국방이나 연방정보시스템을 주된 보호대상으로 삼았으며, 1990년 이후에는 중요기반시설로 확대되었다.[50] 이와 관련하여 연방법은 1950년 방위생산법(The Defence Production Act of 1950),[51] 1980년 프라이버시보호법,[52] 1986년 전자통신프라이버시법[53]이 적용되고 있다.

사이버위기관리는 1987년 컴퓨터보안법(Computer Security Act of 1987)[54]의 제정을 시작으로 나타났고, 1990년대에 이르러 1995년 문서사

---

49) http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm
50) 이창범 외,「미국, 독일, 일본의 정보보호법 체계에 관한 연구」(한국정보보호진흥원, 2006. 12), 18면 참조
51) 50 U.S.C, App. 2061 et seq.
52) 42 U.S.C. 2000aa
53) 18 U.S.C. 2510note.
54) 15 U.S.C. 271 et seq; 40 U.S.C. 759 컴퓨터보안법은 각 부처의 기밀정보에 관계되는 보안이나 프라이버시에 관계되는 계획을 수립할 것을 규정하고 있고, 연방컴퓨터시스

무감축법(Paperwork Reduction Act of 1995)에서는 각 부처에 대하여 컴퓨터보안법을 준수할 것을 요구하고 축적된 데이터에 대하여 중요도에 따라 보안대책을 마련하도록 하였다. 1996년에는 클링거 코헨법이 제정되어 정보시스템이 정상적으로 가능하도록 감시하는 정보화책임관(Chief Information Officer, CIO)을 각 부처에 배치할 것과 상무부에 대하여 국가표준기술연구소의 기준을 활용하여 연방정보시스템의 보안지침을 마련하도록 요구하였지만, 정보시스템 보호와 중요기반시설 보호에 대하여는 언급이 없었다. 2000년 정부정보보안개혁법, 2002년 전자정부법, 사이버보안강화법(Cyber Security Enhancement Act of 2002, CSEA)[55] 및 그 밖에 사이버에 관련한 연방법이 제·개정되었다. 특히 지난 9.11테러 이후 국토안보부 창설을 위한 국토안보법이 제정되어 시행되고 있으며, 전자정부법과 국토안보법에 연방정보보안관리법[56]을 편입시키는 등 관련 법규

템에 있는 기밀정보의 보안 및 개인정보의 보호를 위하여 기존의 보안 조치 내에서 최소한의 보안기준을 확립하기 위하여 제정되었다(CSA 2(a)).

55) 미국은 9.11 테러 이후 국토안보부 창설을 위한 국토안보법을 제정하면서 사이버보안에 관한 입법인 2002년 사이버보안강화법을 을 이 법에 삽입하여 제정·시행하고 있다. 이 법은 양형위원회로 하여금 특정한 컴퓨터 범죄와 관련된 판결 지침을 개정하고 형벌을 강화하며, 컴퓨터 범죄와 관련된 판결 지침을 개정하고 형벌을 강화하며, 컴퓨터 범죄에 대한 연구·보고를 하도록 하며, 긴급공개의 예외를 인정하는 것 등을 주요 내용으로 한다.

56) 2002년 11월 29일에 정부정보보안개혁법의 폐지에 따라 연방정보보안관리법이 제정되었고, 2002년 전자정부법의 제3절에 포함되었다. 이 법의 입법목적은 연방업무 및 자산을 지원하는 정보자원에 대한 정보보안통제의 효과를 높이기 위한 종합적인 틀을 제공하고, 고도로 네크워크화된 연방컴퓨팅 환경을 인식하고, 국민과 국가의 보안 및 관할지역 내 정보보완활동을 조정하는 등 관련 정보보안위험에 대한 효과적인 범정부 차원의 관리 및 감독을 시시하고, 연방정보 및 정보시스템의 보호에 필요한 최소한의 통제수단을 개발 및 유지하며, 연방기관의 장보보안 프로그램에 대한 감독을 강화하기 위한 메카니즘을 제공하고 상업적 목적으로 개발된 정보보안상품은 품질이 우수하고 역동적이며 강력하고 효과적인 정보보안 솔루션을 제공한다는 사실을 인정하고, 국방 및 경제안정에 필요한 주요 정보인프라를 보호하기 위하여 민간이 개발, 구축 및 운영하는 솔루션을 도입하고, 상업적 목적으로 개발된 상품 가운데 특정한 기술 하드웨어 및 소프트웨어 정보보안 솔루션을 선정하는 사항은 개별 기관에 맡겨져야 한다는 사실을 인식하는 것을 그 목적으로 한다(FISMA §3541). 동법은 관리예산처장

를 정비하였고, 또한 애국자법(The Patriot of 2001)[57]이 제·개정되었다. 이들 법률의 집행을 위하여 대통령의 행정명령과 각 부처의 지침 등이 마련되어 관련 법규의 시행을 구체화하고 있다.[58]

전자정부법은 정보보안에 대해 상세히 규정하고 있다. ① 입법목적 : 동 절은 정보자원에 대한 정보보안 통제의 효과를 조장하기 위한 총체적인 틀을 제공하고, 정보보안 위험에 대한 범정부 차원의 효과적인 관리 및 감독을 실시하며, 연방 정보 및 정보시스템의 보호에 필요한 최소한의 통제수단을 개발 및 유지하고, 연방기관의 정보보안 시스템에 대한 감독 강화를 위한 메카니즘을 제공하는 것 등을 목적으로 한다(제3541조). ② 정보보안 및 국가보안시스템의 의미 : 정보보안은 ㉮ 부적절한 정보변경 또는 파괴로부터 보호한다는 의미로서 정보청구의 보장 및 진정성 확보 등을 위한 보전, ㉯ 개인 프라이버시 및 재산적 가치있는 정보의 보호를 위한 수단을 포함하여 접속 및 공개에 대한 권한있는 제한을 유지한다는 의미의 비밀성, ㉰ 적절한 시기에 신뢰할 수 있는 방법으로 정보에 접속 및 이용할 수 있다는 의미의 이용가능성을 목적으로 권한없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다. 그리고 국가보안시스템은 기관 또는 기관과 계약을 맺은 자 또는 그 밖의 기관을 대신하는 조직에 의하여 이용 또는 운영되는 (여하한 정보통신시스템을 포함하여) 여하한 정보시스템을 말

이 연방정보보안사고센터를 운영하도록 하고 있으며(FISMA §3545), 연방정보시스템의 표준화에 대해서 규정하고 있다(FISMA §3546).

57) 이 법은 9.11사태 이후 테러 및 범죄수사에 있어 수사의 편의를 위하여 국민의 기본권을 제약하기 위하여 제정되었다. 이 법은 케이블텔레비전·사생활보호법 및 연방형법을 개정하여 수사당국에 의한 도청의 권한을 대폭 확대하는 등 수사를 위하여 정부에 강력한 권한을 부여하였다.

58) 현대호, "미국의 사이버위기 관련 법제의 현황과 전망"「법학논총」제33권제1호(2009. 6, 단국대 법학연구소), 14-15면 참조

한다(제3542조). ③ 적용범위 : 연방 행정기관의 모든 정보시스템에 적용된다. 다만 국가보안시스템, 국방성 및 중앙정보국시스템의 경우에는 일반 정보시스템과는 달리 일정한 예외를 두고 있다(제3543조). ④ 주요내용 :관리예산처장은 ㉮ 정보보안 정책, 원칙, 표준 및 지침의 개발 및 시행 감독, ㉯ 행정기관 등이 이용 또는 운영하는 정보 또는 정보시스템에 대한 정보보안 조치의 확인 및 제공, ㉰ 이 법에 대한 기관의 준수 여부 감독, ㉱ 최소 1년마다 기관의 정보보안 프로그램 검토 및 승인, ㉲ 정보보안 정책 및 절차와 정보자원관리 정책 및 절차의 조정, ㉳ 연방 정보보안사고센터의 운영감독, ㉴ 의회보고 등의 방법으로 각 기관의 정보보안 정책 및 업무를 감독한다. 이외에도 관리예산처장은 ㉵ 국가표준기술연구원법상의 표준 및 지침의 개발과 관련하여 국가보안시스템을 운용하거나 통제하는 기관 및 사무국과의 조정작업을 거침으로서 가능한 최대한의 범위에서 그러한 표준 및 지침이 국가보안시스템용으로 개발된 표준 및 지침을 보충할 수 있도록 하여야 한다(제3543조). 각 기관의 장은 정보보안에 관한 정책, 절차, 표준, 지침 등을 준수하여 기관의 전략적 목표에 따라 정보 및 정보시스템에 대한 정보보안 조치를 강구하여야 한다. 기관의 장은 이와 관련된 권한을 당해 기관의 정보화책임관에게 위임할 수 있다. 그리고 각 기관은 정보 및 정보시스템에 대한 정보보안을 위하여 기관단위의 정보보안 프로그램을 개발 및 시행하여야 한다. 동 프로그램은 ㉮ 정보 및 정보시스템의 보안상의 위험에 대한 주기적인 평가, ㉯ 정보보안 위험의 감소 및 정보시스템의 수명주기에 맞춘 정보보안 유지 등을 위한 정책 및 절차, ㉰ 보안교육, ㉱ 정보보안에 관한 정책, 절차 및 업무상의 어떠한 결점에 대한 평가 및 이에 따른 구제조치를 계획, 시행, 평가 및 기록하기 위한 과정, ㉲ 보안사고에 따른 탐지, 보고 및 대응을 위한 절차, ㉳ 정보시스템에 대한 영속적 운영을 위한 계획 및 절차 등이 포함되어야 한다(제3544조).

미국은 1980년대 초 컴퓨터 범죄가 급증하고 기존의 연방 형사법 규정으로는 이들을 모두 규율할 수 없게 됨에 따라 연방법전 제 18편 제 1030조(18U.S.C.§1030)를 개정하여 컴퓨터 관련 범죄를 일괄적으로 규정한 「컴퓨터 사기 및 오용법(Computer Fraud and Abuse Act : CFAA)」[59] 을 제정하여 1986년부터 컴퓨터 정보처리에 대한 범죄적 행위를 규제하고 있다. 동법은 컴퓨터 범죄가 나날이 지능화·정교화 해짐에 따라 그동안 7차례의 개정(1988, 1989, 1990, 1994, 1996, 2001, 2002, 2008)을 한 바 있다.

연방법전 제18편 제1030조(18U.S.C.§1030) 이외에도 18U.S.C.§2701(저장된 통신에 대한 불법접근), 18U.S.C.§1028(a)(7)(ID도용), 18U.S.C.§1028A(가중된 ID 도용), 18U.S.C.§1029(접근장치사기), 18U.S.C.§1037(CAN-SPAM법), 18U.S.C.§1343(유선사기), 18U.S.C.§1362(통신방해) 등에서 컴퓨터 네트워크 관련 범죄를 규정하고 있다.[60] 즉, 「컴퓨터 사기 및 오용법」은 컴퓨터[61]를 통한 국가안보정보, 금융정보,

---

59) 18U.S.C.§1030 이 법은 2001년 애국자법과 2008년「동일성 절취 집행 및 회복에 관한 법률(Identity Theft Enhencement and Restitution Act, ITERA)에 의하여 개정되었는데, 컴퓨터시스템의 해킹을 방지하고 연방컴퓨터 관련 범죄를 해결하기 위하여 제정되어 연방형법에 포함되어 있다(18 U.S.C. §1030).

60) http://www.usdoj.gov/criminal/cybercrime/ccmanual/03ccma.html

61) "컴퓨터"라 함은 전자적, 전기적, 광학적, 전기화학적, 또는 기타 고속처리장치로서 논리적, 산술적, 또는 저장의 기능을 수행하는 것을 의미하며, 이런 장치에 직접 관련되어 있거나, 이런 장치와 맞물려 작동하는 자료 저장 장치나, 통신 장치를 말한다. 그러나 자동화된 타자기나 식자기, 휴대용 소형 계산기 또는 이와 유사한 장치들은 포함되지 않는다(18U.S.C.§1030(e)(1)). "보호되는 컴퓨터"라 함은 ① 금융기관 또는 미국 정부가 전용하는 컴퓨터를 의미하며, 그렇게 전용하지 않는 경우에는, 금융기관이나 미국 정부에 의하여 사용되거나 금융기관이나 미국 정부를 위하여 사용되는 컴퓨터로서, 범죄를 구성하는 행위가 금융기관이나 미국정부에 의한, 또는 금융기관이나 미국정부를 위한 사용에 영향을 미치는 경우나 ②이러한 컴퓨터가 주간(州間) 또는 외국과의 통상이나 통신에 사용되는 경우를 말하는데, 미국과의 주간(州間) 또는 외국과의 통상이나 통신에 영향을 미치는 방식으로 사용되는 경우 미국 외에 있는 컴퓨터를 포함한다(18U.S.C.§1030(e)(2)).

행정정보 등에 대한 불법 접근과 취득 및 사용, 보호되는 컴퓨터를 이용한 사기, 보호되는 컴퓨터에 대한 손상 등을 범죄로 규정하고 이에 따른 처벌을 규정하고 있다.

컴퓨터 네트워크 범죄 관련 다른 연방법전 규정[62]으로는 18U.S.C.§2701(저장된 통신에 대한 불법 접근)[63], 18U.S.C.§1028(a)(7)(ID 도용)와 18U.S.C.§1028A(가중된 ID 도용),[64] 18U.S.C.§1029(접근장치 사기),[65] 18U.S.C.§1037(CAN-SPAM법)[66] 등이 있다.

한편 2009사이버보안법안(Cybersecurity Act of 2009)은 2009. 4. 1일 민주당 상원의원 제이 록펠러(Jay Rockefeller)와 빌 넬슨(Bill Nelson), 그리고 공화당 상원의원 올림피아 스노위(Olympia Snowe) 등의 발의로 백악관 내 국가사이버보안자문국설치법안과 함께 미국 상원에 제출되어 현재 논의 중인 법안이다. 동 법안의 목적은 미국 내에서의 상거래의 자유로운 흐름의 보장, 사이버상의 통신 보안 확립을 통하여 국제 교역 파트너들과의 자유로운 거래 보장, 상기 목적을 위한 인터넷과 인트라넷 통신의 지속적인 개발과 이용 제공, 사이버위협에 대한 효과적인 사이버

---

62) http://www.usdoj.gov/criminal/cybercrime/ccmanual/03ccma.html

63) 고의로 정당한 권한 없이 전기통신서비스가 제공되는 설비에 접근하거나, 고의로 설비에 대한 인가된 접근권한을 초과하여 시스템 내 전기적 저장 상태에 있는 유선 또는 전기통신에 대한 접근권을 얻거나 변경하거나 방해하는 경우에 범죄를 구성한다.

64) 법적 권한 없이 연방법 위반을 구성하거나 중죄를 구성하는 불법행위를 범하거나, 조장하거나 공모할 의도를 가지고 다른 사람의 신분인식 수단을 이전, 소지, 또는 사용하는 경우에 범죄를 구성하며, 특정한 경우에는 가중 처벌한다.

65) 권한 없는 접근장치 또는 위조접근장치의 생산, 사용, 소지, 또는 매매행위 등은 범죄를 구성한다.

66) 주간(州間) 또는 외국과의 통상에 있어서, 또는 이들에 영향을 미치는 경우에, 접근권한 없이 보호되는 컴퓨터에 접근하여 그 컴퓨터로부터 또는 그 컴퓨터를 통하여 다량의 상업적 전자 메일의 전송을 시도하는 경우 등 불법 스팸메일 관련 범죄를 규정한다.

방어를 유지하고 증진시키기 위한 정보기술 전문가 양성 등이다. 동 법안은 인터넷 망이 사이버 공격을 받을 위험에 처할 경우, 인터넷으로부터 연방 주요기반 시설의 망을 인터넷으로부터 차단할 수 있는 권한을 국가사이버보안자문관(National Cybersecurity Advisor)[67]에게 부여하는 등 미국의 주요 기반 시설을 사이버공격으로부터 보호하기 위한 보다 강화된 조치들을 담고 있다. 동시에, 민간과 유기적인 협력관계를 통하여 사이버보안이 보다 효율적으로 달성될 수 있다는 인식하에, 국립표준기술원(NIST)이 제정한 표준들을 민간에 홍보, 전파, 교육시키기 위한 구체적인 방안을 규정하고 있다. 또한 국립표준기술원(NIST)은 동 법이 제정된 날로부터 1년 이내에 모든 연방정부 및 연방정부와 계약을 맺은 자, 그리고 주요기반 시설들을 보유하고 있는 민간 사업자 등이 운영하는 주요 기반 시설의 정보 시스템과 망들을 감사할 수 있는 사이버 보안 표준을 개발해야 한다고 규정하고 있다. 국립표준기술원(NIST)은 현실에 부합하는 망의 지정과 표준을 마련하기 위하여 기존의 법, 집행명령(Executive Order), 규칙(Rule), 규정(Regulation), 가이드라인(Guideine)의 규정과는 별도로, 비밀 정보(Classified or Confidential information)와 위험수준(risk prfiles)에 근거하여 국가보안시스템으로서의 정보시스템이나 망을 지정하고 표준을 마련하도록 규정하고 있다.[68]

그리고 국가과학재단(National Science Foundation)은 연방차원의 사이버보안 연구개발에 있어서 안전하고 신뢰할 수 있는 소프트웨어의 개발 및 시험 등에 있어서 우선적으로 지원하여야 한다고 규정하고 있다(CA

67) 자문관은 국가시이버보안 프로그램과 전략에 관련된 문제에 대해 대통령에게 자문하고, 사이버보안 연구 및 개발에 관한 동향 및 개발내용 등에 관하여 평가하며, 그 결과를 2년마다 대통령에게 보고하도록 하고 있다.

68) 양지연, "미국의 정보통신망 정부규제 및 자율규제 현황"「정보통신망 안전성 및 신뢰성 확보방안」(2009. 8. 10), 79-86면 참조

§11). 그리고 국가과학재단은 연방차원의 정보기술자와 보안관리자를 양성하기 위하여 연방장학금 지원프로그램을 마련하여 제공하여야 한다고 규정하고 있다(CA §12).[69]

Ⅱ. 정보보호 추진체계

사이버보안에 대한 미국정부의 인식이 본격적으로 전환된 것은 2001년의 9.11사태를 겪고 난 뒤부터이다. 당시 부시대통령은 2001년 10월 행정명령 제13228호(Executive Order 13228, EO-13228)를 통해 국토안보국(Office of Homeland Security, OHS)과 국토안보위원회(Homeland Security Council, HSC)를 설치하였으며 2002년에 와서 국토안보법의 제정으로 국토안보부(Department of Homeland Security, DHS)가 설치되었다. 국토안보부에 의해 국가사이버보안센터(National Cyber Division, NCSD)가 운영되고 있다. 그리고 2004년에는 국가사이버보안센터를 통하여 국가사이버경보체제(National Cyber Alert System, NCAS)가 확립되어 정부차원의 사이버보안체제가 구축되었다.[70] 아울러 국토안보부는 좀 더 안전하고 안정적이며 여러 종류의 외부 위협에 유연하게 대처하여 미

---

69) 우리의 경우 한국연구재단법(제5조)상 한국연구재단(1. 학술 및 연구개발 활동의 지원, 2. 학술 및 연구개발 인력의 양성과 활용의 지원, 3. 학술 및 연구개발 활동의 국제협력 촉진 지원, 4. 제1호부터 제3호까지의 사업 수행에 필요한 자료 및 정보의 조사·수집·분석·평가·관리·활용과 정책개발 지원, 5. 학술 및 연구개발 관련 기관·단체의 연구·운영 지원, 6. 국내외 학술 및 연구개발 관련 기관·단체 간의 교류협력 지원, 7. 그 밖에 학술 및 연구개발에 필요한 사항)이나 과학기술기본법(제30조제5항)상 한국과학창의재단(1. 과학기술문화 창달 및 창의적 인재육성 지원을 위한 조사 연구 및 정책 개발, 2. 국민의 과학기술 이해 증진 및 확산사업, 3. 과학교육과정 및 창의적 인재육성 프로그램 개발, 4. 창의적 인재 교육 전문가 육성·연수 지원, 5. 과학기술 창달 및 창의적 인재육성과 관련된 과학문화·예술 융합프로그램 개발 지원, 6. 그 밖에 교육과학기술부장관이 지정 또는 위탁하는 사업)은 순수한 활동을 수행하고 있어 미국의 국가과학재단과 확연히 비교된다.

70) 현대호, 앞의 글, 5-7면 참조

국의 중요한 인프라와 중요한 자원(critical infrastructure and key resources, CIKR)을 보호하기 위한 통합적인 계획으로 2009 National Infrastructure Protection Plan(NIPP)보고서[71]를 발표하였다. 이 보고서에는 위험관리를 통한 예방과 보호, 정확한 상황분석, 미국의 정보기술인프라에 대한 위협에 대한 대응, 복구를 통해 자국의 보호를 강화하는 내용을 담고 있다.

최근 오바마 행정부는 국가 사이버 보안관련 정책과 활동을 총괄 조정하는 사이버보안정책관(cybersecurity policy official)을 백악관에 신설하는 등 사이버스페이스 보안 강화를 위한 강력한 정책의지를 반영한 범정부 차원의 전략보고서[72]를 발표(2009. 5. 29) 하였다. 이와는 별도로 현재 상원에서는 국가 사이버 보안 강화를 위해 사이버보안 위기시 대통령에게 인터넷의 사용을 일부 정지시키는 것을 허용하는 등 강력한 조치를 담고 있는 2009사이버보안법안(Cybersecurity Act of 2009)이 논의 중에 있다.[73]

제6절 소결

유럽연합은 사이버 공격의 지능화, 다양화로 인해 기존의 기술적 대응만으로는 한계가 있으므로 새로운 유형의 악성코드, 봇넷 및 피싱과 같은 사회공학적 공격의 사전적 예방을 위해 정보보안 인식제고에 지속적인

71) National Infrastructure Protection Plan by Office of Homeland Security, Sector Specific Plans on IT http://www.dhs.gov/files/progran\ms/editorial_0827.shtm
72) CYBERSPACE POLICY REVIEW : Assuring a Trusted and Resilient Information and Communications Infrastructure.
73) 양지연, 앞의 글, 79면 참조

노력 및 투자를 행하고 있으며 최근 정보보호 인식 실태조사 및 가이드라인 개발 등 활발한 연구를 수행하고 있다.

독일에서는 현재까지도 테러 또는 사이버테러 예방이나 처벌을 위한 특별한 법률을 제정하고 있지는 않으나, 각 개별 형벌법규를 통하여 테러와 사이버테러 방지에 대비하기 위한 규정을 두고 있다. 그리고 정보통신법, 통신서비스법, 연방데이터보호법, 정보통신서비스정보보호법, 전자서명법, 통신법, 형법, 연방정보기술안전청 설치에 관한 법률, 연방의 정보기술의 보안강화를 위한 법률 등 정보보호법제의 정비를 통해 사이버 위기에 적극 대응하고 있다. 그리고 독일에서의 정보기관들의 임무와 권한의 특징은 국내안보에 있어서의 군대의 역할이 배제되어 있고, 국내안보의 주요담당기관으로서의 경찰의 지위확립과 독자적인 헌법보호청이 설치되어 있어 정치경찰이 인정되지 않는다는 데 있다. 향후 테러의 국제화·보편화가 진행됨으로써 연방경찰, 연방헌법보호청, 연방정보기관(BND), 군정보기관(MAD) 등에서의 업무영역을 명확히 구분할 수 없는 경우가 다수 발생할 것에 대비하여 가령 연방헌법보호청의 경우 수집된 정보를 수사기관에 통보하도록 규정(제20조, 제21조)하고 있는 등 독일 내 대테러 유관기관 간 협조체제의 유기적 구축을 통해 미묘한 문제를 해결하고 있다.

일본은 정부가 사이버위기를 대응함에 있어서 법률로서 규율하는 외에 각종 지침과 가이드라인을 통해 사전에 예방할 수 있는 것과 사고발생시의 피해확대를 방지하는 것, 사건에 대한 검토 등을 위해 노력하고 있다. 물론 시간과 공간을 초월하고 그 징후를 알 수 없어 예측하기 어려운 사이버테러의 특성으로 인하여 완벽한 사전예방이라는 것은 쉽지 않은 일이나, 최대한 효과적으로 대응하기 위해서는 정부와 민간 공히 정보보안

이 국가정보보안의 중요한 부분[74]이라는 것을 보여주는 시스템을 갖추고 있다. 현재까지 치명적인 사건이 일어난 것은 아니나 향후 정말 심각한 테러가 이루어질 것을 상정하여, 국가위기 관련법제의 정밀한 검토를 하고 있는 것으로 보인다. 즉, 2004년 이후부터 무력공격사태법과 국민보호법 등의 개별법을 통괄하는 기본법으로서의 역할을 하는 긴급사태법(가칭)의 제정이 주장되고 있다. 그런데 재해대책기본법이나 국민보호법과의 정합성을 이유로 필요하지 않다는 의견이 강력하게 제기됨으로써 아직까지는 법제정이 되지 않고 있다. 이에 덧붙여 궁극적으로는 정보보호 관계법까지 결합하여 정보통신망 상의 위기 곧 사이버테러에 대한 부분까지도 대응하는 것을 고려하고 있다. 또한 하드웨어적인 정보처리장치나 정보통신망에 대한 관리, 기술적인 안전장치 및 하드웨어적인 시스템에 정통하고 사업자간, 사업자 행정부서간 보안대책을 연계할 수 있는 인재육성 및 사용자의 보안의식을 강화하는 데에도 노력을 기울이고 있다.[75]

미국의 경우 관련기관 간 기능에 따른 권한과 책임을 분산하고, 이러한 기관들의 수평적 협업을 통하여 사이버위기관리에 대응하고 있다. 대통령 직속의 관리예산처가 전자정부에 대한 책임을 맡고 있으며, 공공부문의 정보보안에 있어서도 원칙적으로 관리예산처가 추진체계의 중심에 있다고 있다. 그렇지만 국가안보시스템의 경우 국토안보부와 국방부 등을 중심으로 추진체계를 정비하였다. 이는 사이버공간에서 공공분야와 민간분야를 포괄하는 사이버위기관리는 국가안전보장과 직결된다는 인식하에서 국토안보부가 이에 관한 업무를 수행한다. 정보보안 관련법제도 이를 제도적으로 뒷받침하기 지속적으로 정비되고 있다.

---

74) 허태회 외, “세계 주요 강대국들의 정보전 준비와 대응체계”, 35면
75) 김재광・김정임, 앞의 논문, 59-60면 참조

제4장 우리나라의 정보보호 관련법제 및 추진체계 분석

제1절 서언

본격적으로 사이버위협에 대응하기 위한 정보보호에 관한 중요성이 논의되고 관련 제도가 정비되고 강화된 것은 2000년대에 접어들면서부터이다. 2001년에는 금융·통신·에너지 등 주요 정보통신기반시설을 특별히 보호하기 위하여「정보통신기반 보호법」을 제정·공포하였고,「정보통신망 이용촉진 등에 관한 법률」도 명칭을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하고 정보보호 등에 관한 규정을 대폭 보완하였다. 2005년에는 국가안보를 위협하는 해킹·컴퓨터바이러스 등 사이버 공격으로부터 국가정보통신망을 보호하기 위하여 사이버안전에 관한 조직 및 운영에 대한 사항을 체계적으로 정립한「국가사이버안전관리규정」이 대통령 훈령으로 발령되었다. 2006년에는 국가 핵심기술의 수출이 국가안보에 심각한 영향을 줄 수 있는 경우 또는 신고하지 아니하거나 허위로 신고하여 국가 핵심기술을 수출한 경우에는 그 국가 핵심기술의 수출중지·금지·원상복귀 등의 조치를 위할 수 있도록 하는 내용을 담은 「산업기술의 유출 방지 및 보호에 관한 법률」이 제정되었다.[76]

최근에는 초고속통신망 및 정보시스템의 활용이 확산되면서, 물류, 발전, 에너지 분야 등 국가 주요기반구조들의 정보시스템 의존도가 높아짐

76) 국가정보원·방송통신위원회·행정안전부·지식경제부, 2009 국가정보보호백서

에 따라 사이버테러를 비롯한 인터넷의 재해가 단순한 가상세계의 피해로 한정되는 것이 아니라, 현실 세계로 피해가 파급되어가고 있는 실정이다. 이러한 기반구조들의 연계성으로 하나의 기반구조가 피해를 입었을 경우, 다른 기반구조가 연쇄적으로 피해를 입을 가능성이 증가한다. 네트워크가 융합되는 환경이 도래할 경우 사이버공격에 취약한 무선망, 인터넷망에서 발생된 위협이, 음성통신망, 방송망까지 피해가 확산될 수 있다.

참고로 해킹사고의 접수·처리건수에 대한 통계를 살펴보면, 2009년 1월부터 6월까지의 통계로만도 9,747건에 이르고 있다. 77)

우리나라의 정보보호 추진체계는 국가정보원, 행정안전부, 지식경제부, 방송통신위원회, 민간사업자 등 다양한 기관으로 분산되어 있어 효율적이고 신속한 대응이 어려운 측면이 있다는 지적이 일반적으로 제기되고 있다. 정보보호 정책은 어느 부처에 컨트롤 타워기능을 부여하느냐가 핵심문제가 아니다. 정보보호 수준을 높이기 위해서는 정보보호 법·제도 수립과 문화운동, 기술개발 등을 따로 떼놓고 할 수는 없는 일이며, 정보보호체계가 분립되어 기능하는 현실을 무시하고 단순하게 기능을 통합하거나 분리하는 정보보호 추진체계 개편은 본질을 무시하는 것으로 타당하지 않다.

제2절 정보보호 관련법제의 유형별 분류

국내의 정보보호 법제는 각각 제정목적 및 기능별로 정보보호 추진체

77) 한국정보보호진흥원, 2009 June 인터넷 침해사고 동향 및 분석 월보

계 관련법제, 국가기밀 보호 관련법제, 중요정보의 국외유출방지 관련법제, 전자서명 및 인증 관련법제, 정보통신망과 정보시스템의 보호조치 관련법제, 정보통신망 침해행위 처벌 관련법제 등으로 분류할 수 있다.[78]

Ⅰ. 정보보호 추진체계 관련법제

국내 정보보호 추진체계는 국가사이버 안전체계, 전자정부 보호체계, 정보통신기반 보호체계 및 개인정보 보호체계로 나누어 볼 수 있다.

국가사이버 안전체계와 관련해서는 2005년 1월 대통령 훈령으로 발령된「국가사이버 안전 관리규정」에서 국가사이버안전전략회의, 국가사이버 안전센터 등 사이버 안전 관련조직에 대한 법적 근거, 임무, 관련 기관간 협력사항 등에 관한 사항을 규정하고 있다.

전자정부 보호체계와 관련하여서는 2007년 1월 개정된「전자정부법」에서 전자정부의 정보보호를 위해 대민서비스와 관련된 보안대책의 수립•조정 및 제도개선, 보안사고 발생시 대응 조치 등을 심의하기 위한 전자정부서비스보안위원회를 설치하도록 하였다. 행정기관의 장에 대하여는 국가정보원장이 안정성을 보장한 보안조치를 취하도록 하고 국가정보원장은 보안 조치의 이행여부를 확인할 책무를 각각 규정하였다.

정보통신기반보호체계에 대하여는 2000년 12월에 제정된「정보통신기반보호법」에서 정보통신기반보호위원회, 침해사고대책본부 및 각 중앙행정기관의 역할에 관한 사항을 규정하고 있다.

---

78) 이 분류는「2008 정보보호백서」를 참조하였다.

끝으로, 개인정보 보호체계와 관련된 법령으로는 공공부문에서「공공기관의 개인정보 보호에 관한 법률」,「전자정부법」및「주민등록법」등이 있으며, 민간부문에서는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「신용정보의 이용 및 보호에 관한 법률」등의 개별법이 존재하고 있다.

Ⅱ. 국가기밀 관련법제

국가기밀보호 관련법제에는 침해나 유출될 경우 국가의 존립•안전과 민주적 기본질서 유지를 위태롭게 할 정보 내지 국가 기밀에 대한 침해 금지와 처벌, 비밀의 분류, 국가기밀에 속하는 문서•자재•시설 및 지역에 대한 보안업무 등에 관하여 규정하고 있는 법령 등이 포함 된다. 예를 들면,「국가정보원법」제3조 중 국가기밀에 속하는 문서•자재•시설 및 지역에 대한 보안업무와 정보 및 보안업무의 기획조정 규정,「국가보안법」제8조 회합•통신,「보안업무 규정」제3조 보안책임 및 제2장 비밀보호(제5조 내지 제30조),「군사기밀보호법」제3조 군사 기밀의 구분, 제5조 군사기밀의 보호조치, 제12조 내지 제15조 군사기밀 누설 관련 조항 등이 이에 해당하며, 형법에는 간첩죄, 일반이적죄, 외교상 비밀누설죄, 공무상 비밀누설죄 등 다양한 규정들이 존재한다. 한편 종래에 주로 국가의 비밀보호 수단으로 사용되어 온 암호는 정보통신망상의 통신수단 및 전자상거래 등의 발전으로 민간분야에서도 사용이 늘고 있고, 이에 대한 법령정비가 이루어져 왔다. 암호의 사용과 관련된 법령으로는「보안업무규정」,「국가정보화기본법」,「전자거래기본법」등이 있으며, 암호의 부정사용과 관련된 법령으로는「국가정보원법」,「군형법」등이 있다.

Ⅲ. 중요정보의 국외유출방지 관련법제

국가안전보장과 관련된 보안정보나 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보 등 국내의 산업•경제 및 과학기술 등에 관한 중요정보가 정보통신망을 통해 국외로 유출되는 것을 방지하기 위한 대표적인 법령으로는 2006년에 제정된「산업기술의 유출방지 및 보호에 관한 법률」이 있다. 이 법률에서는 국내외 시장에서 차지하는 기술적•경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 국가핵심기술의 지정•변경(제9조)과 보호조치(제11조) 및 수출승인 등 국가핵심기술의 무단유출과 침해행위의 금지(제14조) 등을 정하고 있다. 공공연구기관에서 개발된 기술이 민간부문으로 이전되어 사업화되는 것을 촉진하고, 민간부문에서 개발된 기술이 원활히 거래되고 사업화될 수 있도록 관련 시책을 수립•추진함으로써 산업 전반의 기술경쟁력을 강화하여 국가경제의 발전에 이바지함을 목적으로 하는「기술의 이전 및 사업화 촉진에 관한 법률」에서는 기술이전•사업화 촉진에 참여한 자는 기술이전•사업화 촉진에 참여하면서 알게 된 공공연구기관 및 기업의 비밀누설을 금지(제38조)하고 이를 어길 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌하도록 규정하고 있다(제41조). 민•군겸용기술의 연구개발을 촉진하고, 군사 부문과 비군사 부문 간의 기술이전을 확대하며 규격을 통일함으로써 산업경쟁력과 국방력을 강화하는 데에 이바지함을 목적으로 2007년 12월에 개정된「민•군겸용기술사업 촉진법」제25조에서는 민•군겸용기술사업에 참여한 자에 대해 참여과정에서 알게 된 비밀유지의무를 부여하는 한편 제26조에서는 이를 위반한 자에 대하여는 3년 이하의 징역 또는 3천만원 이하의 벌금으로 처벌하도록 규정하고 있다. 그밖에 부정경쟁방지 및 영업비밀보호에 관한 법률 제18조는

부정한 이익을 얻거나 기업에 손해를 입힐 목적으로 그 기업에 유용한 영업비밀을 외국에서 사용하거나 외국에서 사용될 것임을 알면서 제3자에게 누설한 자는 10년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금에 처할 뿐 아니라 이러한 죄를 범할 목적으로 예비 또는 음모한 자에 대해서도 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 하여 중요정보가 외국에 유출될 우려가 있는 경우까지 엄격하게 통제하여 국부의 해외유출을 방지하고 있다.

Ⅳ. 전자서명 및 인증 관련법제

정보시스템과 정보통신망의 발전으로 인한 원격지간의 거래 및 업무가 활성화됨에 따라 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보인 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위해 전자서명 및 인증관련 법적 정비가 이루어졌다. 전자서명 및 인증과 관련된 법령에는 공인전자서명과 인증을 규정하고 있는「전자정부법」과 공인인증시장의 균형적 발전과 공정한 경쟁환경을 조성하기 위해 비영리 법인 등에 대한 공인인증 제공역무 영역을 설립목적에 맞게 구분하여 지정할 수 있도록 한「전자서명법」등이 있다.

Ⅴ. 정보통신망과 정보시스템의 보호조치 관련법제

해킹, 바이러스유포 등 사이버 침해행위로 인하여 국가 및 민간분야의 정보통신망과 정보시스템에 대한 위협이 증가함에 따라 국가차원의 체계적인 보호조치가 필요하게 되었다. 정보통신망과 정보시스템의 보호조치와 관련한 법령으로는「국가정보화기본법」,「정보통신기반보호법」,「정

보통신망 이용촉진 및 정보보호 등에 관한 법률」,「전자거래기본법」,「무역업무 자동화촉진에 관한 법률」,「산업기반 조성에 관한 법률」및「물류정책기본법」등이 있다.

Ⅵ. 정보통신망 침해행위의 처벌 관련법제

침해행위의 처벌 관련 법제는 해킹, 바이러스, 서비스 거부공격 등 정보시스템과 정보통신망에 대한 침해 등으로 피해를 야기하고 정보의 탈취, 위•변조 등으로 인한 국가•사회적 피해방지를 위해 이들 행위에 대하여 벌칙규정을 마련하고 있다.「정보통신기반보호법」제28조의 주요정보통신기반시설 침해행위에 대한 벌칙,「정보 통신망 이용촉진 및 정보보호 등에 관한 법률」제62조의 정보통신망 침해행위와 비밀 등의 보호의무 위반에 대한 벌칙규정이 대표적이다. 또한「전자무역촉진에 관한 법률」제30조의 무역유관기관의 컴퓨터파일에 기록된 전자무역문서 또는 데이터베이스에 입력된 무역정보에 대한 위조 또는 변조 등의 처벌,「물류정책기본법」제71조의 전자문서를 위작 또는 변작하거나 그 사정을 알면서 위작 또는 변작된 전자문서를 행사한 자 및 종합물류정보망 또는 국가물류 통합데이터베이스에 의하여 처리•보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해•도용 또는 누설한 자, 종합물류정보망 또는 국가물류통합데이터베이스의 보호조치를 침해하거나 훼손한 자 등에 대한 처벌 등의 벌칙규정이 있다. 그밖에 형법에서는 컴퓨터 사기죄를 도입하여 이에 대한 처벌규정을 두고 있다.

Ⅶ. 개인정보보호 관련법제

최근 정보통신기술의 발달에 의해 개인정보보호에 대한 침해가 증가하고 있어 이에 대한 관심이 증가하면서 관련법령의 정비가 지속적으로 이루어지고 있다. 개인정보 보호에 관한 기본적인 법령으로는 공공부문의 경우에는「공공기관의 개인정보보호 등에 관한 법률」이, 민간부문의 경우에는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 있는바,「전자서명법」이나「인터넷주소자원에 관한 법률」상 개인정보보호에 대하여는 모두「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 규정을 준용하도록 되어 있다. 그 밖에 개인정보보호에 관련된 법령으로는「전자정부법」,「통신비밀보호법」,「신용정보의 이용 및 보호에 관한 법률」,「금융실명거래 및 비밀보장에 관한 법률」등이 있다.

제3절 현행 정보보호 추진체계 관련법제 분석

현행법상 정보보호 추진체계는 국가사이버 안전체계, 전자정부 보호체계, 정보통신기반 보호체계 및 개인정보 보호체계로 나누어 볼 수 있다.

Ⅰ. 국가사이버 안전체계

국가사이버 안전체계와 관련해서는 2005년 1월 대통령 훈령으로 발령된「국가사이버 안전 관리규정」에서 국가사이버안전전략회의, 국가사이버 안전센터 등 사이버 안전 관련조직에 대한 법적 근거, 임무, 관련 기관간 협력사항 등에 관한 사항을 규정하고 있다.

그 외에 정부조직법, 국가안전보장회의법, 국가정보원법, 정보및보안업무기획·조정규정, 경찰법 등이 사이버안전 관련사항을 규율하고 있다. 그리고「국가 사이버 위기 관리법안」도 검토하였다.

1. 국가사이버안전관리규정

가. 입법목적

국가사이버안전관리규정(훈령)은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다(제1조).

나. 사이버공격과 사이버안전

"사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다(제2조제2호). "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다(제2조제3호).

다. 국가사이버안전관리 체계

(1) 국가사이버안전정책 및 관리

국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다(제5조).

(2) 국가사이버안전전략회의

국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다(제6조제1항). 전략회의의 의장은 국가정보원장이 된다(제6조제2항). 전략회의의 위원은 교육과학기술부차관·외교통상부차관·법무부차관·국방부차관·행정안전부차관·지식경제부차관·보건복지가족부차관·국토해양부차관·대통령실 외교안보수석비서관·방송통신위원회 상임위원·금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 한다(제6조제3항). 전략회의는 다음 각호의 사항(1. 국가사이버안전체계의 수립 및 개선에 관한 사항, 2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항 3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안 4. 그 밖에 전략회의 의장이 부의하는 사항)을 심의한다(제6조제4항). 전략회의의 구성·운영 등에 관하여 필요한 사항은 전략회의의 의장이 따로 정한다(제6조제5항).

(3) 국가사이버안전센터

사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다(제8조제1항). 사이버안전센터는 다음 각호의 업무(1. 국가사이버안전정책의 수립 2. 전략회의 및 대책회의의 운영에 대한 지원 3. 사이버위협 관련 정보의 수집·분석·전파 4. 국가정보통신망의 안전성 확인 5. 국

가사이버안전메뉴얼의 작성·배포 6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원 7. 외국과의 사이버위협 관련 정보의 협력)를 수행한다(제8조제2항). 국가정보원장은 사이버안전센터의 업무 수행과 관련하여 필요하다고 인정하는 경우에는 관계 중앙행정기관의 장에게 소속 공무원 및 전문요원의 파견을 요청할 수 있다(제8조제3항).

2. 정부조직법

가. 입법목적

정부조직법은 국가행정사무의 체계적이고 능률적인 수행을 위하여 국가행정기관의 설치·조직과 직무범위의 대강을 정함을 목적으로 한다(제1조).

나. 국가정보원

국가안전보장에 관련되는 정보·보안 및 범죄수사에 관한 사무를 담당하기 위하여 대통령소속으로 국가정보원을 둔다(제15조제1항). 국가정보원의 조직·직무범위 그 밖에 필요한 사항은 따로 법률로 정한다(제15조제2항).

다. 국방부

국방부장관은 국방에 관련된 군정 및 군령과 그 밖에 군사에 관한 사무를 관장한다(제28조).

라. 행정안전부

행정안전부장관은 국무회의의 서무, 법령 및 조약의 공포, 정부조직과 정원, 공무원의 인사·윤리·복무·연금, 상훈, 정부혁신, 행정능률, 전자정부 및 정보보호, 정부청사의 관리, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 낙후지역 등 지원, 지방자치단체간 분쟁조정, 선거, 국민투표, 안전관리정책 및 비상대비·민방위·재난관리 제도에 관한 사무를 관장한다(제29조제1항).

마. 지식경제부

지식경제부장관은 상업·무역·공업, 외국인 투자, 정보통신산업, 산업기술연구개발정책, 에너지·지하자원, 우편·우편환 및 우편대체에 관한 사무를 관장한다(제32조). 지식경제부는 정보통신산업과 관련한 업무를 담당하기 때문에 정보보안과 관련해서는 간접적인 지위를 가진다고 볼 수 있다.

3. 국가안전보장회의법

가. 입법목적

국가안전보장회의법은 헌법 제91조의 규정에 의하여 국가안전보장회의의 구성·직무범위 기타 필요한 사항을 규정함을 목적으로 한다(제1조).

나. 구성

국가안전보장회의(이하 "회의"라 한다)는 대통령·국무총리·외교통상부

장관·통일부장관·국방부장관 및 국가정보원장과 대통령령이 정하는 약간의 위원으로 구성한다(제2조제1항). 대통령은 회의의 의장이 된다(제2조제2항).

다. 직능

회의는 국가안전보장에 관련되는 대외정책·군사정책과 국내정책의 수립에 관하여 대통령의 자문에 응한다(제3조).

라. 국가정보원과의 관계

국가정보원장은 국가안전보장에 관련된 국내외정보를 수집·평가하여 이를 회의에 보고하여 심의에 자하여야 한다(제10조).

4. 국가정보원법

가. 입법목적

국가정보원법은 국가정보원(이하 "국정원"이라 한다)의 조직 및 직무범위와 국가안전보장업무의 효율적인 수행을 위하여 필요한 사항을 규정함을 목적으로 한다(제1조).

나. 조직

국정원의 조직은 국가정보원장(이하 "원장"이라 한다)이 대통령의 승인을 얻어 정한다(제4조제1항). 국정원은 직무수행상 특히 필요한 경우에는

대통령의 승인을 얻어 특별시·광역시·도에 지부를 둘 수 있다(제2항).

다. 직원

국정원에 원장·차장 및 기획조정실장과 기타 필요한 직원을 둔다. 다만, 특히 필요한 경우에는 차장 2인 이상을 둘 수 있다(제5조제1항). 직원의 정원은 예산의 범위 안에서 대통령의 승인을 얻어 원장이 정한다(제2항).

라. 조직 등의 비공개

국정원의 조직·소재지 및 정원은 국가안전보장을 위하여 필요한 경우에는 이를 공개하지 아니할 수 있다(제6조).

마. 원장·차장·기획조정실장

원장은 국회의 인사청문을 거쳐 대통령이 임명하며, 차장 및 기획조정실장은 원장의 제청에 의하여 대통령이 임명한다(제7조제1항). 원장은 정무직으로 하며, 국정원의 업무를 통할하고 소속직원을 지휘·감독한다(제2항). 차장은 정무직으로 하고 원장을 보좌하며, 원장이 사고가 있을 때에는 그 직무를 대행한다(제3항). 기획조정실장은 별정직으로 하고 원장과 차장을 보좌하며, 위임된 사무를 처리한다(제4항). 원장·차장 및 기획조정실장 이외의 직원의 인사에 관하여는 따로 법률로 정한다(제5항).

바. 겸직직원

원장은 현역군인 또는 필요한 공무원의 파견근무를 관계기관의 장에게

요청할 수 있다(제10조제1항). 겸직직원의 원소속기관의 장은 겸직직원의 모든 신분상의 권익과 보수를 보장하여야 하며, 겸직직원을 전보발령하고자 할 때에는 미리 원장의 동의를 얻어야 한다(제2항). 겸직직원은 겸직기간 중 원소속기관의 장의 지시 또는 감독을 받지 아니한다(제3항). 겸직직원의 정원은 관계기관의 장과 협의하여 대통령의 승인을 얻어 원장이 정한다(제4항).

사. 직권남용의 금지

원장·차장 및 기타 직원은 그 직권을 남용하여 법률에 의한 절차에 의하지 아니하고 사람을 체포 또는 감금하거나 다른 기관·단체 또는 사람으로 하여금 의무없는 일을 하게 하거나 사람의 권리행사를 방해하여서는 아니된다(제11조제1항). 국정원직원으로서 제16조의 규정에 의하여 사법경찰관리(군사법경찰관리를 포함한다)의 직무를 행하는 자는 그 직무를 수행함에 있어서 형사소송법 제34조(피고인·피의자와의 접견, 교통, 수진) 및 제209조에 의하여 수사에 준용되는 제87조(구속의 통지), 제89조(구속된 피고인과의 접견, 수진), 제90조(변호인의 의뢰)와 군사법원법의 관계규정(제63조·제127조·제129조 및 제130조)등 범죄수사에 관한 적법절차를 준수하여야 한다(제2항).

아. 국가기관 등에 관한 협조요청

원장은 이 법이 정하는 직무를 수행함에 있어서 필요한 협조와 지원을 관계 국가기관 및 공공단체의 장에게 요청할 수 있다(제15조).

5. 정보및보안업무기획·조정규정

가. 입법목적

정보및보안업무기획·조정규정(대통령령)은 국가정보원법 제3조제2항의 규정에 의하여 정보 및 보안업무의 기획·조정에 관하여 필요한 사항을 규정함을 목적으로 한다.

나. 정보 및 보안업무의 기획·조정

국가정보원장(이하 "국정원장"이라 한다)은 국가정보 및 보안업무에 관한 정책의 수립 등 기획업무를 수행하며, 동 정보 및 보안업무의 통합기능수행을 위하여 필요한 합리적 범위 내에서 각 정보수사기관의 업무와 행정기관의 정보 및 보안업무를 조정한다(제3조).

다. 기획업무의 범위

국정원장이 정보 및 보안업무에 관하여 행하는 기획업무의 범위로는 1. 국가 기본정보정책의 수립, 2. 국가 정보의 중·장기 판단, 3. 국가 정보목표 우선순위의 작성, 4. 국가 보안방책의 수립, 5. 정보예산의 편성, 6. 정보 및 보안업무의 기본지침 수립 등이 있다(제4조).

라. 조정업무의 범위

국정원장이 정보 및 보안업무에 관하여 행하는 조정 대상기관과 업무의 범위는 다음과 같다(제5조).

통일부는 통일에 관한 국내외 정세의 조사·분석 및 평가에 관한 사항, 남북대화에 관한 사항, 이북5도의 실정에 관한 조사·분석 및 평가에 관한 사항, 통일교육에 관한 사항 등이다.

외교통상부는 국외정보의 수집에 관한 사항, 출입국자의 보안에 관한 사항, 재외국민의 실태에 관한 사항, 통신보안에 관한 사항 등이다.

행정안전부는 국내 보안정보(외사정보 포함)의 수집·작성에 관한 사항, 정보사범 등의 내사·수사 및 시찰에 관한 사항, 신원조사업무에 관한 사항, 통신정보 및 통신보안업무에 관한 사항 등이다.

법무부는 국내 보안정보의 수집·작성에 관한 사항, 정보사범 등에 대한 검찰정보의 처리에 관한 사항, 공소보류된 자의 신병처리에 관한 사항, 적성압수금품 등의 처리에 관한 사항, 정보사범 등의 보도 및 교도에 관한 사항, 출입국자의 보안에 관한 사항, 통신보안에 관한 사항 등이다.

국방부는 국외정보·국내보안정보·통신정보 및 통신보안업무에 관한 사항, 제4호나목 내지 마목에 규정된 사항, 군인 및 군무원의 신원조사업무지침에 관한 사항, 정보사범 등의 내사·수사 및 시찰에 관한 사항 등이다.

문화체육관광부는 공연물 및 영화의 검열·조사·분석 및 평가에 관한 사항, 신문·통신 그 밖의 정기간행물과 방송 등 대중전달매체의 활동 조사·분석 및 평가에 관한 사항, 대공심리전에 관한 사항, 대공민간활동에 관한 사항 등이다.

지식경제부는 우편검열 및 정보자료의 수집에 관한 사항 등이다.

방송통신위원회는 전파감시에 관한 사항, 그 밖에 통신정보 및 통신보안업무에 관한 사항 등이다.

국토해양부는 국내 보안정보(외사정보 포함)의 수집·작성에 관한 사항, 정보사범 등의 내사·수사 및 시찰에 관한 사항, 통신정보 및 통신보안 업무에 관한 사항 등이다.

과학기술부는 북한 및 공산국가의 과학기술 정보 및 자료의 수집관리와 활용에 관한 사항 등이다.

기타 정보 및 보안업무 관련 기관은 정보 및 보안관련업무에 관한 사항 등이다.

6. 경찰법

가. 입법목적

경찰법은 국가경찰의 민주적인 관리·운영과 효율적인 임무수행을 위하여 국가경찰의 기본조직 및 직무범위 기타 필요한 사항을 규정함을 목적으로 한다(제1조).

나. 국가경찰의 임무

국가경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압

및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다(제3조).

다. 비상조치시의 특별조치 체계

경찰청장은 전시·사변, 천재·지변 그 밖에 이에 준하는 국가비상사태, 대규모의 테러 또는 소요사태가 발생하였거나 발생할 우려가 있어 전국적인 치안유지를 위하여 긴급한 조치가 필요하다고 인정할 만한 충분한 사유가 있는 경우에는 제2항의 규정에 따라 제주특별자치도의 자치경찰공무원(이하 "자치경찰공무원"이라 한다)을 직접 지휘·명령할 수 있다. 다만, 제주특별자치도 지역 단위의 치안유지를 위한 경우에는 제주특별자치도지방경찰청장이 지휘·명령할 수 있다(제25조제1항). 경찰청장 또는 제주특별자치도지방경찰청장은 제1항의 규정에 따른 조치가 필요한 경우에는 미리 제주특별자치도지사에게 자치경찰공무원을 직접 지휘·명령하고자 하는 사유 및 내용 등을 적시하여 통보하여야 한다. 이 경우 제주특별자치도지사는 정당한 사유가 없는 한, 즉시 소속 자치경찰공무원에 대하여 경찰청장 또는 제주특별자치도지방경찰청장의 지휘·명령을 받을 것을 명하여야 한다(제25조제2항). 경찰청장 또는 제주특별자치도지방경찰청장이 제1항의 규정에 따라 지휘·명령권을 인수한 경우에는 경찰청장은 경찰위원회에 즉시 보고하여야 하고, 제주특별자치도지방경찰청장은「제주특별자치도 설치 및 국제자유도시 조성을 위한 특별법」 제113조의 규정에 따른 관할 치안행정위원회에 즉시 통보하여야 한다(제25조제3항). 제3항의 규정에 따라 자치경찰공무원에 대한 지휘·명령권자의 변동사실을 보고받은 경찰위원회는 제1항에 규정된 사유에 해당되지 아니한다고 인정하는 때에는 그 지휘·명령권을 반환할 것을 의결할 수 있으며, 같은 사실을 통보받은 치안행정위원회는 제1항에 규정된 사유에

해당되지 아니한다고 인정하는 때에는 경찰청장 또는 제주특별자치도지방경찰청장에게 그 지휘·명령권의 반환을 건의할 수 있다(제25조제4항). 경찰청장 또는 제주특별자치도지방경찰청장은 제1항의 규정에 따라 경찰청장 또는 제주특별자치도지방경찰청장이 자치경찰공무원을 지휘·명령할 수 있는 사유가 해소된 때에는 자치경찰공무원에 대한 지휘·명령권을 즉시 제주특별자치도지사에게 반환하여야 한다(제25조제5항). 제1항 및 제2항의 규정에 따라 제주특별자치도의 자치경찰공무원이 경찰청장 또는 제주특별자치도지방경찰청장의 지휘·명령을 받는 경우 그 지휘·명령의 범위 안에서는 국가경찰공무원으로 본다(제25조제6항).

라. 경찰청 사이버테러대응센터

경찰청 사이버테러대응센터(Cyber Terror Response Center, 약칭 네탄)는 해킹, 바이러스제작 및 유포 등 각종 컴퓨터 범죄의 포착과 수사를 담당하는 대한민국 경찰청의 사이버범죄 전담 수사기관을 말한다.
1995년 해커수사대를 시작으로 1997년 8월 컴퓨터범죄수사대, 99년 사이버범죄수사대로 확대되었고, 2000년 7월 현 체제인 사이버테러대응센터를 창설하였다. 협력운영팀, 수사1팀, 기획수사2팀, 기술지원팀 등 3개팀으로 구성되어 있으며, 사이버테러 종합대책 수립시행, 전국 사이버수사요원 교육, 국제공조수사활동, 24시간 사이버순찰을 통한 초동조치 및 대국민 경보발령, 주요 사이버 테러사건 수사, 사이버테러 수사기법 개발 및 기술지원 등의 업무를 수행한다.

7. 「국가 사이버 위기 관리법안」

가. 법안의 제안이유

법안의 제안이유를 보면 다음과 같다. ① 사이버공간은 정보통신기술의 비약적인 발전과 더불어 정보기기와 컴퓨터 그리고 인터넷 등의 네트워크로 연결된 가상의 공간으로 이미 국민 생활의 보편적인 영역으로 자리매김하였고, 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있다. ② 이러한 특수성으로 말미암아 복잡·고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있다. ③ 사이버공격으로 초래되는 사이버위기는 현실세계의 물리적 질서혼란과 달리 특정개인에 대한 것일지라도 국가전체의 위기로 확대될 수 있다. ④ 과거 1·25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터 조직적인 사이버공격으로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있다. ⑤ 그러나 우리나라는 아직 국가차원에서 사이버위기를 체계적으로 관리할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있다. ⑥ 따라서 이 법에서는 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 한다.

나. 법안의 주요내용

법안의 주요내용은 ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제4조). ② 국가정보원장은 사이버위기를 효율적으로

관리하고 사이버공격 관련정보를 상호 공유하기 위하여 민·관 협의체를 구성·운영할 수 있음(안 제5조). ③ 국가정보원장은 국가사이버위기관리 종합계획을 수립하고 이에 따라 위기관리기본지침을 작성하여 책임기관의 장에게 배포하고, 책임기관의 장은 세부지침을 수립·시행하여야 함(안 제6조). ④ 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조). ⑤ 책임기관의 장은 사이버공격을 탐지하여 사이버위기 발생 가능성을 조기에 차단·예방하는 등 피해를 최소화하기 위하여 신속한 대응조치를 취하여야 함(안 제9조). ⑥ 책임기관의 장은 사이버공격으로 인해 피해가 발생한 경우에는 자체 사고조사를 실시하고, 그 결과를 관계 중앙행정기관의 장 및 국가정보원장에게 통보하여야 하며, 국가정보원장은 필요한 경우에 직접 사고조사를 실시할 수 있음(안 제10조). ⑦ 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버위기경보를 발령할 수 있으며, 책임기관의 장은 피해발생을 최소화하거나 피해복구 조치를 취해야 함(안 제12조). ⑧ 정부는 심각단계의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등을 위하여 관계 기관 및 전문인력이 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제13조). ⑨ 관계 중앙행정기관의 장 및 국가정보원장은 사이버위기관리에 필요한 기술개발·국제협력 등 필요한 시책을 추진할 수 있음(안 제14조 및 제16조). ⑩ 정부는 사이버공격 기도에 관한 정보를 제공하거나 사이버공격을 가한 자를 신고한 자에 대하여 포상금을 지급할 수 있음(안 제18조). ⑪ 직무상 비밀을 누설한 경우에는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 보안관제센터를 구축하지 아니한 경우에는 2천만원 이하의 과태료에 처할 수 있음(안 제19조 및 제20조) 등이다. 법안의 주요내용을 요약하면, 사이버 공격에 대한 국가차원의 종합적이고 체계

적인 대응과 사이버 위기 관리를 위해 국가정보원장 소속으로 국가사이버안전센터를 두고, 국가정보원장은 사이버 위기를 효율적으로 관리하고 사이버 공격 관련 정보를 상호 공유하기 위해 민·관 협의체를 구성·운영할 수 있으며, 국가정보원장은 국가사이버위기관리종합계획을 수립하고 이에 따라 위기관리기본지침을 작성해 책임기관의 장에게 배포하고, 책임기관의 장은 세부지침을 수립·시행해야 함 등이다.

다. 평가

「국가 사이버 위기 관리법안」은 개별 부처 차원의 입법적 대응보다는 국가전체 차원의 입법이 필요하다는 입장에서 제출된 것이다.

주요 국가 기반 시설 등에 대한 사이버 위기 예방 및 대응 조치를 의무화하고, 위기 발발시 국가정보원장이 대책본부를 구성할 수 있도록 한다는 것을 법안의 주요 골자로 하고 있다.[79]

그러나 "국민의 기본권을 침해할 수 있는 악법(惡法)"이라는 야당의 반대에 부딪혀 좌절된 바 있다.

이 법안은 대통령훈령인「국가사이버안전관리규정」을 구체화한 것으로 볼 수 있다.

Ⅱ. 전자정부 보호체계

전자정부 보호체계와 관련하여서는 2007년 1월 개정된「전자정부법」에서 전자정부의 정보보호를 위해 대민서비스와 관련된 보안대책

79) 제282회 국회(임시회) 제2차 전체회의에 상정・제안설명되었다(2009. 4. 23)

의 수립·조정 및 제도개선, 보안사고 발생시 대응 조치 등을 심의하기 위한 전자정부서비스보안위원회를 설치하도록 하였다. 행정기관의 장에 대하여는 국가정보원장이 안정성을 보장한 보안조치를 취하도록 하고 국가정보원장은 보안 조치의 이행여부를 확인할 책무를 각각 규정하였다.

그 외에 국가정보화기본법이 전자정부 보호체계 관련사항을 규율하고 있다.

1. 전자정부법

가. 입법목적

전자정부법은 행정업무의 전자적 처리를 위한 기본원칙·절차 및 추진방법 등을 규정함으로써 전자정부의 구현을 위한 사업을 촉진시키고, 행정기관의 생산성·투명성 및 민주성을 높여 지식정보화시대의 국민의 삶의 질을 향상시키는 것을 목적으로 한다(제1조).

나. 전자정부와 정보통신망

"전자정부"라 함은 정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다(제2조제1호). "정보통신망"이라 함은 전기통신기본법 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다(제2조제7호).

다. 정보통신망의 보호체계

전자정부법상 정보통신망의 보호체계는 ① 국회·법원·헌법재판소·중앙선거관리위원회 및 행정부, ② 행정안전부장관 등으로 구성되어 있다.

국회·법원·헌법재판소·중앙선거관리위원회 및 행정부는 정보통신망 등의 보안대책 수립·시행(제27조)의 임무를 수행한다.

행정안전부장관은 전자적 대민서비스 보안대책(제39조의2), 전자정부서비스보안위원회(제39조의3)의 임무를 수행한다.

(1) 국회·법원·헌법재판소·중앙선거관리위원회 및 행정부

정보통신망 등의 보안대책 수립·시행(제27조)의 임무를 수행한다.

(2) 행정안전부장관

전자적 대민서비스 보안대책(제39조의2), 전자정부서비스보안위원회(제39조의3)의 임무를 수행한다.

행정안전부장관은 전자적 대민서비스와 관련된 보안대책을 국가정보원장과 사전협의를 거쳐 마련하여야 한다(제39조의2제1항). 중앙행정기관과 그 소속기관 및 지방자치단체의 장은 제1항의 보안대책에 따라 당해 기관의 보안대책을 수립·시행하여야 한다(동조제2항).

제39조의2제1항의 규정에 따른 보안대책과 관련한 다음 각 호의 사항(1. 보안대책의 수립·조정 및 제도개선 2. 보안사고 발생시 대응조치 3. 제1호 또는 제2호에 해당하는 업무의 소관 중앙행정기관과 그 소속 기관

및 지방자치단체 간 공조 방안에 관한 사항 4. 그 밖에 전자정부대민서비스의 보안대책과 관련된 주요 정책사항으로서 위원장이 부의하는 사항)을 심의하기 위하여 행정안전부장관 소속하에 전자정부서비스보안위원회(이하 이 조에서 "위원회"라 한다)를 둔다(제39조의3제1항). 위원회는 위원장 1인을 포함한 20인 이내의 위원으로 구성한다(동조제2항). 위원장은 행정안전부장관이 되고, 위원은 대통령령이 정하는 관계 중앙행정기관 및 지방자치단체의 공무원과 위원장이 위촉하는 자로 한다(동조제3항). 위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둘 수 있다(동조제4항). 위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다(동조제5항).

2. 국가정보화기본법

가. 입법목적

국가정보화기본법은 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적으로 한다(제1조).

나. 정보보호, 정보통신망 및 정보통신기반

"정보보호"란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다(제2조제6호). "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여

정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체제를 말한다(제11호). “정보통신기반”이란 정보통신망과 이에 접속하여 이용되는 정보통신기기, 소프트웨어 및 데이터베이스 등을 말한다(법률 제2조 제12호).

다. 국가정보화 추진체계

국가정보화 추진체계는 정부, 국가기관과 지방자치단체, 행정안전부장관, 방송통신위원회 등으로 구성되어 있다. 정부는 국가정보화 기본계획의 수립(제6조)을 임무로 한다. 국가기관과 지방자치단체는 정보보호 시책의 마련(제37조), 개인정보 보호 시책의 마련(제39조), 건전한 정보통신윤리의 확립(제40조), 이용자의 권익 보호 등(제41조)을 임무로 한다. 행정안전부장관은 정보보호시스템에 관한 기준 고시 등(제38조)을 임무로 한다. 방송통신위원회는 전담기관의 지정 등(제48조), 초고속국가망의 관리 등(제49조), 광대역통합연구개발망의 구축・관리 등(제50조)을 임무로 한다.

(1) 정부

정부는 국가정보화의 효율적, 체계적 추진을 위하여 5년마다 국가정보화 기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다(제6조제1항). 기본계획은 행정안전부장관이 국가와 지방자치단체의 부문계획을 종합하여 수립하며, 제9조에 따른 국가정보화전략위원회(이하 “위원회”라 한다)의 심의를 거쳐 확정한다. 기본계획 중 대통령령으로 정하는 중요한 사항을 변경하는 경우에도 또한 같다(제6조제2항). 기본계획에는 다음 각 호의 사항(1. 국가정보화 정책의 기본 방향 및 중장기 발전방향, 2. 행정,

보건, 사회복지, 교육, 문화, 환경, 과학기술 등 공공 분야의 정보화, 3. 제16조에 따른 지역정보화, 4. 산업·금융 등 민간 분야 정보화의 지원, 5. 제2호부터 제4호까지의 사항과 관련된 분야별 정보보호, 국가정보화 기반의 조성 및 고도화, 6. 정보문화의 창달 및 정보격차의 해소, 7. 개인정보 보호, 건전한 정보통신 윤리 확립, 이용자의 권익보호 및 지적재산권의 보호, 8. 정보의 공동활용 및 표준화, 9. 국가정보화와 관련된 법령·제도의 개선, 10. 국가정보화와 관련된 국제협력의 활성화, 11. 국가정보화와 관련된 재원의 조달 및 운용, 12. 그 밖에 국가정보화 추진을 위하여 필요한 사항)이 포함되어야 한다(제6조제3항). 행정안전부장관은 위원회의 심의를 거쳐 국가와 지방자치단체의 부문계획의 작성지침을 정하고 이를 관계 기관에 통보할 수 있다(제6조제4항). 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장과 지방자치단체의 장은 소관 주요 정책을 수립하고 집행을 할 때 제3항 각 호의 사항을 우선적으로 고려하여야 한다(제6조제5항).

(2) 국가기관과 지방자치단체

국가기관과 지방자치단체는 정보보호 시책의 마련(제37조), 개인정보보호 시책의 마련(제39조), 건전한 정보통신 윤리의 확립(제40조), 이용자의 권익 보호 등(제41조)을 임무로 한다.

ⅰ) 정보보호 시책의 마련

국가기관과 지방자치단체는 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호를 위한 시책을 마련하여야 한다(제37조제1항). 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 마련하여야 한다(제37조

제2항).

ⅱ) 개인정보 보호 시책의 마련

국가기관과 지방자치단체는 국가정보화를 추진할 때 인간의 존엄과 가치가 보장될 수 있도록 개인정보 보호를 위한 시책을 마련하여야 한다(제39조).

ⅲ) 건전한 정보통신 윤리의 확립

국가기관과 지방자치단체는 건전한 정보통신 윤리를 확립하기 위하여 미풍양속을 해치는 불건전한 정보의 유통을 방지하고 건강한 국민정서를 함양하며, 불건전한 정보로부터 청소년을 보호하기 위하여 필요한 시책을 마련하여야 한다(제40조).

ⅳ) 이용자의 권익 보호 등

국가기관과 지방자치단체는 국가정보화를 추진할 때 이용자의 권익보호를 위하여 다음 각 호(1. 이용자의 권익보호를 위한 홍보·교육 및 연구, 2. 이용자의 권익보호를 위한 조직 활동의 지원 및 육성, 3. 이용자의 명예·생명·신체 및 재산상의 위해 방지, 4. 이용자의 불만 및 피해에 대한 신속·공정한 구제조치, 5. 그 밖에 이용자 보호와 관련된 사항)의 시책을 마련하여야 한다(제41조제1항). 정보통신서비스 제공자는 사업을 할 때 이용자를 보호하기 위하여 필요한 조치를 마련하여야 한다(제41조제2항).

(3) 행정안전부장관

행정안전부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거

나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다(제38조제1항). 행정안전부장관은 유통 중인 정보보호시스템이 제1항에 따른 기준에 미치지 못할 경우에 정보보호시스템의 보완 및 그 밖에 필요한 사항을 권고할 수 있다(제38조제2항). 제1항에 따른 기준을 정하기 위한 절차와 제2항에 따른 권고에 관한 사항 및 그 밖에 필요한 사항은 대통령령으로 정한다(제38조제3항).

(4) 방송통신위원회

방송통신위원회는 전담기관의 지정 등(제48조), 초고속국가망의 관리 등(제49조), 광대역통합연구개발망의 구축・관리 등(제50조)을 임무로 한다.

ⅰ) 전담기관의 지정 등

방송통신위원회는 광대역통합정보통신기반의 원활한 구축과 이용촉진을 위하여 필요한 때에는 홍보, 국제협력, 기술개발 등 그 업무를 전담할 기관(이하 “전담기관”이라 한다)을 분야별로 지정할 수 있다(제48조제1항). 정부는 광대역통합정보통신기반의 구축 및 이용촉진과 관련된 업무를 수행하는데 소요되는 자금을 전담기관에 출연하거나 융자 등을 할 수 있다(제48조제2항). 전담기관은 제2항에 따른 자금을 별도로 관리하여야 한다(제48조제3항). 전담기관의 지정 및 운영 등에 관하여 필요한 사항은 대통령령으로 정한다(제48조제4항).

ⅱ) 초고속국가망의 관리 등

방송통신위원회는 국가재정으로 공공기관과 대통령령으로 정하는 비영리기관(이하 “비영리기관등”이라 한다)이 이용하는 초고속정보통신망

(이하 “초고속국가망”이라 한다)을 구축·관리하거나 제48조에 따라 지정된 전담기관으로 하여금 구축·관리하게 할 수 있다(제49조제1항). 방송통신위원회는 비영리기관등이 초고속국가망을 최소의 비용으로 이용할 수 있도록 필요한 시책을 강구하여야 한다(제49조제2항). 초고속국가망의 구축·관리에 관하여 필요한 사항은 대통령령으로 정한다(제49조제3항).

ⅲ) 광대역통합연구개발망의 구축·관리 등

방송통신위원회는 광대역통합정보통신망의 구축을 촉진하기 위하여 국가재정으로 광대역통합연구개발망을 구축·관리·운영하거나 제48조에 따라 지정된 전담기관으로 하여금 구축·관리·운영하게 할 수 있다(제50조제1항). 방송통신위원회는 광대역통합정보통신망의 품질관리를 위하여 필요한 시책을 강구하여야 한다(제50조제2항).

Ⅲ. 정보통신기반 보호체계

정보통신기반보호체계에 대하여는 2000년 12월에 제정된「정보통신기반보호법」에서 정보통신기반보호위원회, 침해사고대책본부 및 각 중앙행정기관의 역할에 관한 사항을 규정하고 있다.

그 외에 방송통신위원회의 설치 및 운영에 관한 법률, 전기통신기본법 등이 전보통신기반 보호문제를 규율하고 있다.

1. 정보통신기반 보호법

가. 입법목적

정보통신기반 보호법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

나. 정보통신기반시설과 전자적 침해행위

"정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 말한다(제2조제1호). "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다(제2조제2호). "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다(제2조제3호).

다. 주요정보통신기반시설의 보호체계

주요정보통신기반시설의 보호체계는 정보통신기반보호위원회, 주요정보통신기반시설을 관리하는 기관의 장(관리기관의 장), 행정안전부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장, 관계중앙행정기관의 장 등으로 구성되어 있다.

정보통신기반보호위원회는 지정된 주요정보통신기반시설의 보호에 관한 사항 심의(법률 제3조), 대책본부의 구성등(법률 제15조) 에 관한 임무를 수행한다.

주요정보통신기반시설을 관리하는 기관의 장(관리기관의 장)은 주요정보통신기반시설보호대책의 수립(법률 제5조), 취약점의 분석·평가(법률 제9조), 침해사고의 통지(법률 제13조), 복구조치(법률 제14조) 에 관한 임무를 수행한다.

행정안전부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장은 주요정보통신기반시설보호대책 이행 여부의 확인(법률 제5조의2), 주요정보통신기반시설의 지정 권고(법률 제8조의2), 관계중앙행정기관의 장은 주요정보통신기반시설보호계획의 수립(법률 제6조), 주요정보통신기반시설의 지정(법률 제8조), 보호지침 제정(법률 제10조), 보호조치 명령(법률 제11조) 등의 임무를 수행한다.

(1) 정보통신기반보호위원회

주요정보통신기반시설(이하 "주요정보통신기반시설"이라 한다)의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 "위원회"라 한다)를 둔다(제3조제1항). 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다(동조제2항). 위원회의 위원장은 국무총리실장이 되고, 위원회의 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다(동조제3항). 정보통신기반보호위원회의 위원이 되는 중앙행정기관의 장은 기획재정부장관·법무부장관·국방부장관·행정안전부장관·교육과학기술부장관·지

식경제부장관·국토해양부장관·국가정보원장·금융위원회위원장 및 위원회의 위원장이 지명하는 중앙행정기관의 장으로 한다(동법시행령 제2조). 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다(동조 제4항). 법 제3조제4항의 규정에 의하여 위원회에 두는 실무위원회의 위원은 다음 각호의 자(1. 위원회의 위원이 속하는 중앙행정기관의 차관급 공무원, 2. 행정기관의 차관급 공무원 중 실무위원회의 위원장이 지명하는 자, 3. 법 제5조제1항의 규정에 의한 주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다), 정부투자기관 또는 정부출연기관의 장중 실무위원회의 위원장이 위촉하는 자)로 한다(동법시행령 제5조제1항). 실무위원회는 위원장 1인을 포함한 25인 이내의 위원으로 구성한다(동법시행령 제5조제2항). 실무위원회의 위원장은 행정안전부장관이 되며, 위원장은 회의를 소집하고, 그 의장이 된다(동법시행령 제5조제3항). 실무위원회의 간사는 실무위원회의 서무에 관한 사항을 총괄한다(동법시행령 제5조제4항). 실무위원회 간사는 행정안전부의 정보통신기반보호업무를 관장하는 고위공무원단에 속하는 공무원이 된다. 다만, 법 제7조제1항의 규정에 의한 경우는 행정안전부와 국가정보원의 정보통신기반보호업무를 관장하는 1급 또는 1급상당 공무원(고위공무원단에 속하는 공무원을 포함한다)이 공동으로 간사가 되고, 법 제7조제2항의 규정에 의한 경우는 국가정보원의 정보통신기반보호업무를 관장하는 1급 또는 1급 상당 공무원이 간사가 된다(동법시행령 제5조제5항). 실무위원회는 위원회에 제출된 안건과 위원회로부터 위임되거나 위원회의 위원장으로부터 지시받은 사항을 검토·심의한다(동법시행령 제5조제6항).

위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다(동법동조제5항). 정보통신기반보호위원회(이하 "위원회"

라 한다)의 위원장은 회의를 소집하고, 그 의장이 된다(동법시행령 제3조제1항). 위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 위원장이 지명하는 위원의 순으로 그 직무를 대행한다(동법시행령 동조제2항). 위원회의 사무를 처리하기 위하여 위원회에 간사 1인을 두되, 간사는 국무총리실장이 된다(동법시행령 동조제3항). 위원회의 회의를 소집하고자 하는 때에는 회의 일시·장소 및 부의사항을 회의개최 7일전까지 각 위원에게 서면 또는 전자문서로 통지하여야 한다. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다(동법시행령 동조제4항). 위원장은 법 제4조 각호의 규정에 의한 사항의 심의를 위하여 필요하다고 인정되는 경우에는 관련 전문가 또는 전문기관의 장으로 하여금 그에 관한 검토보고를 하게 할 수 있다(동법시행령 동조제5항).

위원회는 주요정보통신기반시설 보호정책의 조정에 관한 사항(법률 제4조제1호), 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항(법률 제4조제2호), 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항(법률 제4조제3호), 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항(법률 제4조제4호), 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항(법률 제4조제5호) 등을 심의한다.

한편 위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)를 둘 수 있다(법률 제15조제1항). 위원회의 위원장은 대책본부의 업무와 관련 있는 공무원의 파견을 관계 행정기관의 장에게 요청할 수 있다(법률 제15조제2항). 위원회의 위원장은 침해사

고가 발생한 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 대책본부장을 임명한다(법률 제15조제3항). 대책본부장은 관계 행정기관의 장, 관리기관의 장 및 보호진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있다(법률 제15조제4항). 제4항의 규정에 의하여 협력과 지원을 요청받은 관계 행정기관의 장 등은 특별한 사유가 없는 한 이에 응하여야 한다(법률 제15조제5항). 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다(법률 제15조제6항). 법 제15조제1항의 규정에 의한 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)는 정보통신기반보호와 직접 관련이 있는 중앙행정기관 소속 공무원 중에서 대책본부장이 지명하는 자 및 법 제15조제2항의 규정에 의하여 파견된 자로 구성한다(법률시행령 제22조제1항). 대책본부장을 보좌하기 위하여 차장 2인을 두되, 차장은 제1항의 규정에 의한 대책본부의 구성원 중에서 대책본부장이 임명한다(법률시행령 제22조제2항). 대책본부장은 침해사고에 적절히 대응하기 위하여 필요한 기능별로 실무반을 설치·운영할 수 있다(법률시행령 제22조제3항). 대책본부장은 대책본부를 대표하고, 그 업무를 총괄한다(법률시행령 제23조제1항). 대책본부장은 침해사고 피해의 효율적인 수습을 위하여 필요하다고 인정할 때에는 제22조제1항의 규정에 의한 대책본부의 구성원이 참여하는 회의(이하 "대책본부회의"라 한다. 이하 이 조에서 같다)를 소집할 수 있다. 다만, 다음 각호의 사항(1. 피해시설에 대한 복구조치, 2. 피해확산 방지에 필요한 조치, 3. 피해액 산정의 기준, 4. 유사한 침해사고의 방지를 위한 예방대책)에 관하여는 반드시 대책본부 회의를 거쳐야 한다(법률시행령 제23조제2항). 이 영에서 규정한 것 외에 대책본부의 운영, 대책본부회의 및 제22조제3항의 규정에 의한 기능별 실무반의 구성·운영 등에 관하여 필요한 사항은 대책본부장이 정한다(법률시행령 제23조제3항).

(2) 주요정보통신기반시설을 관리하는 기관의 장

주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행하여야 한다(법률 제5조제1항). 관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다(법률 제5조제2항). 지방자치단체의 장이 관리·감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정안전부장관에게 제출하여야 한다(법률 제5조제3항). 관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다(법률 제5조제4항). 정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다(법률 제5조제5항). 법 제5조제4항 본문의 규정에 의하여 관리기관의 장은 소관 주요정보통신기반시설의 4급·4급상당 공무원, 5급·5급 상당 공무원, 영관급장교 또는 임원급 관리·운영자를 정보보호책임자로 지정하여야 한다(법률시행령 제9조제1항). 제1항의 규정에 의한 정보보호책임자가 총괄하는 업무는 각호(1. 법 제5조제1항의 규정에 의한 주요정보통신기반시설보호대책의 수립·시행, 2. 법 제7조제1항 및 제2항 본문의 규정에 의한 기술적 지원의 요청, 3. 법 제9조의 규정에 의한 취약점 분석·평가 및 전담반 구성, 4. 법 제11조제1항의 규정에 의한 주요정보통신기반시설의 보호에 필요한 조치 명령 또는 권고의 이행, 5.

법 제13조제1항 전단의 규정에 의한 침해사고의 통지, 6. 법 제14조제1항의 규정에 의한 해당 주요정보통신기반시설의 복구 및 보호에 필요한 조치, 7. 기타 다른 법령에 규정된 주요정보통신기반시설의 보호업무에 관한 사항)와 같다(법률시행령 제9조제2항). 관리기관의 장이 정보보호책임자를 지정한 때에는 이를 관할 중앙행정기관의 장에게 통지하여야 한다(법률시행령 제9조제3항).

한편 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다(법률 제9조제1항). 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다(법률 제9조제2항). 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관(1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국정보보호진흥원(이하 "보호진흥원"이라 한다), 2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다), 3. 「정보통신산업 진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체, 4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원)으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다(법률 제9조제3항). 행정안전부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다(법률 제9조제4항). 주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다

(법률 제9조제5항).

한편 ①관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다(법률 제13조제1항). 정부는 제1항의 규정에 의하여 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위 안에서 복구비 등 재정적 지원을 할 수 있다(법률 제13조제2항).

한편 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다(법률 제14조제1항). 관리기관의 장은 제1항의 규정에 의한 복구 및 보호조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 보호진흥원의 장에게 지원을 요청할 수 있다. 다만, 제7조제2항의 규정에 해당하는 경우에는 그러하지 아니하다(법률 제14조제2항). 관계중앙행정기관의 장 또는 보호진흥원의 장은 제2항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다(법률 제14조제3항).

관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 행정안전부장관과 국가정보원장등 또는 필요한 경우 대

통령령이 정하는 전문기관의 장에게 다음 각 호의 업무(1. 주요정보통신기반시설보호대책의 수립, 2. 주요정보통신기반시설의 침해사고 예방 및 복구, 3. 제11조에 따른 보호조치 명령·권고의 이행)에 대한 기술적 지원을 요청할 수 있다(법률 제7조제1항). 국가안전보장에 중대한 영향을 미치는 다음 각 호(1. 도로·철도·지하철·공항·항만 등 주요 교통시설, 2. 전력, 가스, 석유 등 에너지·수자원 시설, 3. 방송중계·국가지도통신망 시설, 4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설)의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다(법률 제7조제2항). 국가정보원장은 제1항 및 제2항에 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다(법률 제7조제3항).

(3) 행정안전부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장

행정안전부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장(이하 "국가정보원장등" 이라 한다)은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다(법률 제5조의2 제1항). 행정안전부장관과 국가정보원장등은 제1항에 따른 확인을 위하여 필요한 경우 관계중앙행정기관의 장에게 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책 등의 자료 제출을 요청할 수 있다(법률 제5조의2 제2항). 행정안전부장관과 국가정보원장등은 제1항에 따라 확인한 주요정

보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있다(법률 제5조의2 제3항). 제1항에 따른 주요정보통신기반시설보호대책 이행 여부의 확인절차 등에 관하여 필요한 사항은 대통령령으로 정한다(법률 제5조의2 제4항).

한편 행정안전부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다(법률 제8조의2 제1항). 행정안전부장관과 국가정보원장등은 제1항에 따른 권고를 위하여 필요한 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다(법률 제8조의2 제2항). 제1항에 따른 주요정보통신기반시설의 지정 권고 절차, 그 밖에 필요한 사항은 대통령령으로 정한다(법률 제8조의2 제3항).

(4) 관계중앙행정기관의 장

관계중앙행정기관의 장 제5조제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립·시행하여야 한다(법률제6조제1항). 관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다(법률제6조제2항). 주요정보통신기반시설보호계획에는 다음 각호의 사항(1. 주요정보통신기반시설의 취약점 분석·평가에 관한 사항, 2. 주요정보통신기반시설의 침해사고에 대한 예방 및 복구대책

에 관한 사항, 3. 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항)이 포함되어야 한다(법률제6조제3항). 행정안전부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다(법률제6조제4항). 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다(법률제6조제5항). 주요정보통신기반시설보호계획의 수립·시행에 관한 사항과 정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다(법률제6조제6항).

한편 중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항(1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성, 2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도, 3. 다른 정보통신기반시설과의 상호연계성, 4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, 5. 침해사고의 발생가능성 또는 그 복구의 용이성)을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다(봅률 제8조제1항). 중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다(법률 제8조제2항). 관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다(법률 제8조제3항). 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다(법률 제8조제4항). 중앙행정기관의 장이

제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다(법률 제8조제5항). 중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다(법률 제8조제6항). 주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다(법률 제8조제7항).

한편 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다(법률 제10조제1항). 관계중앙행정기관의 장은 기술의 발전 등을 감안하여 제1항의 규정에 의한 보호지침을 주기적으로 수정·보완하여야 한다(법률 제10조제2항).

한편 관계중앙행정기관의 장은 다음 각 호(1. 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우, 2. 제5조의2제3항에 따라 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우)의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다(법률 제11조).

2. 방송통신위원회의 설치 및 운영에 관한 법률

가. 입법목적

방송통신위원회의 설치 및 운영에 관한 법률은 방송과 통신의 융합환경에 능동적으로 대응하여 방송의 자유와 공공성 및 공익성을 높이고 방송·통신의 국제경쟁력을 강화하며 방송통신위원회의 독립적 운영을 보장함으로써 국민의 권익보호와 공공복리의 증진에 이바지함을 목적으로 한다(제1조).

나. 위원회의 소관사무

방송에 관한 사항, 통신에 관한 사항, 전파 연구 및 관리에 관한 사항, 그 밖에 이 법 또는 다른 법률에서 위원회의 사무로 정한 사항 등이다(제11조).

다. 위원회의 심의·의결사항

위원회는 소관사무 중 다음 각 호의 사항(1. 방송·통신 기본계획에 관한 사항, 2. 방송사업자의 허가·재허가·승인·등록·취소 등에 관한 사항, 3. 전기통신사업자의 허가·취소 등에 관한 사항, 4. 주파수의 효율적 사용에 관한 사항, 5. 방송·통신 관련 기술정책의 수립에 관한 사항, 6. 방송프로그램의 유통상 공정거래 질서의 확립에 관한 사항, 7. 방송·통신서비스의 고도화 및 보편적 서비스에 관한 사항, 8. 방송·통신사업자 상호 간의 공동사업이나 분쟁의 조정 또는 사업자와 이용자 간의 분쟁의 조정, 9. 전기통신설비의 제공·공동이용·상호접속 또는 공동사용 등이

나 정보제공에 관한 협정의 인가 등에 관한 사항, 10. 방송사업자·통신사업자의 금지행위에 대한 조치 및 과징금 부과에 관한 사항, 11. 방송프로그램 및 방송광고의 운용·편성에 관한 사항, 12. 방송·통신에 관한 연구·조사 및 지원에 관한 사항, 13. 시청자 불만처리 및 방송·정보통신 이용자 보호·복지에 관한 사항, 14. 방송·통신 관련 기금의 조성 및 관리·운용에 관한 사항, 15. 방송·통신 관련 국제협력 및 통상에 관한 사항, 16. 방송·통신 관련 남북 교류·협력에 관한 사항, 17. 위원회의 예산 편성 및 집행에 관한 사항, 18. 소관 법령 및 위원회 규칙의 제·개정 및 폐지에 관한 사항, 19. 이 법 또는 다른 법률에 따라 위원회의 심의·의결 사항으로 정한 사항)을 심의·의결한다(제12조).

3. 전기통신기본법

가. 입법목적

전기통신기본법은 전기통신에 관한 기본적인 사항을 정하여 전기통신을 효율적으로 관리하고 그 발전을 촉진함으로써 공공복리의 증진에 이바지함을 목적으로 한다(제1조).

나. 비상시 통신체계

(1) 방송통신위원회

ⅰ) 비상시 통신 확보

방송통신위원회는 전시·사변·천재·지변 기타 이에 준하는 국가비상사태가 발생하거나 발생할 우려가 있는 경우에는 자가전기통신설비를 설

치한 자로 하여금 전기통신업무 기타 중요한 통신업무를 취급하게 하거나 당해 설비를 다른 전기통신설비에 접속할 것을 명할 수 있다. 이 경우에는 전기통신사업법의 전기통신업무에 관한 규정을 준용한다(제22조제1항). 방송통신위원회는 제1항의 경우에 필요하다고 인정하는 경우에는 기간통신사업자로 하여금 그 업무를 취급하게 할 수 있다(제22조제2항). 제1항의 경우에 그 업무의 취급 또는 설비의 접속에 소요되는 비용은 정부가 이를 부담한다. 다만, 자가전기통신설비가 전기통신역무에 제공되는 경우에는 당해 설비를 제공받는 기간통신사업자가 이를 부담한다(제22조제3항).

ii) 기술기준(제25조)

방송통신위원회는 전기통신설비가 기술기준에 적합하게 설치·운영되는지를 확인하기 위하여 다음 각 호(1. 전기통신설비 시책수립을 위한 경우, 2. 국가비상사태를 대비하기 위한 경우, 3. 재해·재난 예방을 위한 경우 및 재해·재난 발생시, 4. 전기통신설비의 이상으로 광범위한 통신장애가 발생할 우려가 있는 경우)의 어느 하나에 해당하는 경우에는 소속공무원으로 하여금 전기통신설비를 설치·운영하는 자의 설비를 조사 또는 시험하게 할 수 있다(제25조제5항). 제5항의 규정에 따른 조사 또는 시험을 하는 경우에는 조사일 또는 시험일 7일 전까지 그 일시·이유 및 내용 등에 대한 조사·시험계획을 전기통신설비를 설치·운용하는 자에게 통지하여야 한다. 다만, 긴급을 요하거나 사전통지의 경우 증거인멸 등으로 조사·시험목적을 달성 할 수 없다고 인정하는 경우에는 그러하지 아니하다(제25조제6항). 제5항의 규정에 의하여 조사 또는 시험을 하는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 하며, 출입시 성명·출입시간·출입목적 등이 표시된 문서를 관계인에게 주어야 한다(제25조제7항).

ⅲ) 통신재난관리기본계획의 수립(제44조의3)

방송통신위원회는 대통령령이 정하는 기간통신사업자(이하 "주요기간통신사업자"라 한다)의 전기통신역무에 관하여 재난및안전관리기본법에 의한 재난·자연재해대책법에 의한 재해 그 밖에 물리적·기능적 결함 등(이하 "통신재난"이라 한다)의 발생을 예방하고, 통신재난을 신속히 수습·복구하기 위한 통신재난관리기본계획(이하 "기본계획"이라 한다)을 수립하여야 한다. 이 경우 기본계획은 재난및안전관리기본법 제22조의 규정에 의한 국가안전관리계획 및 자연재해대책법 제16조의 규정에 의한 방재집행계획중 통신분야의 계획으로 본다(제44조의3 제1항). 기본계획에는 다음 각호의 사항(1. 통신재난이 발생할 위험이 높거나 통신재난의 예방을 위하여 계속적으로 관리할 필요가 있는 전기통신설비·그 설치지역 등의 지정 및 관리에 관한 사항, 2. 통신재난에 대비하기 위하여 필요한 다음 각목에 관한 사항, 가. 우회통신경로의 확보, 나. 전기통신회선설비의 연계운용을 위한 정보체계의 구성, 다. 피해복구물자의 확보, 3. 그 밖에 통신재난관리에 필요하다고 인정되는 사항)이 포함되어야 한다(제44조의3 제2항). 방송통신위원회는 제1항의 규정에 의한 기본계획을 수립하고자 할 때에 기본계획의 수립지침을 작성하여 이를 주요기간통신사업자에게 통보하여야 한다(제44조의3 제3항). 주요기간통신사업자는 제3항의 규정에 의한 수립지침에 따라 통신재난관리계획을 작성하여 방송통신위원회에 제출하여야 한다(제44조의3 제4항). 방송통신위원회는 제4항의 규정에 의하여 주요기간통신사업자가 제출한 통신재난 관리계획을 종합하여 기본계획을 작성한다(제44조의3 제5항). 방송통신위원회는 제5항의 규정에 의하여 확정된 기본계획중 주요기간통신사업자와 관련된 사항을 해당 주요기간통신사업자에게 통보하여야 한다(제44조의3 제6항). 기본계획의 수립에 관하여 필요한 세부사항은 대통령령으로 정한다(제44조의3 제7항).

ⅳ) 통신재난의 대비(제44조의4)

방송통신위원회는 통신재난이 발생하거나 발생할 것이 명백한 경우에 해당지역의 통신소통과 긴급복구를 위하여 기간통신사업자로 하여금 그 기간통신사업자의 전기통신설비와 다른 기간통신사업자 또는 자가전기통신설비보유자의 전기통신설비를 통합운용하게 할 수 있다(제44조의4 제1항). 제22조제3항의 규정은 제1항의 규정에 의하여 전기통신설비를 통합운용함에 소요된 실비를 보상하는 경우에 이를 준용한다(제44조의4 제2항). 제1항의 규정에 의한 전기통신설비의 통합운용에 관하여 필요한 사항은 대통령령으로 정한다(제44조의4 제3항).

ⅴ) 통신재난대책본부(제44조의8)

방송통신위원회는 통신재난의 피해가 광범위하여 정부차원의 종합적인 대처가 필요한 경우에 통신재난대책본부(이하 "대책본부"라 한다)를 설치·운영할 수 있다(제44조의8 제1항). 대책본부의 장은 방송통신위원회위원장이 된다(제44조의8 제2항). 대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다(제44조의8 제3항). 주요기간통신사업자는 대통령령이 정하는 바에 따라 통신재난에 대한 피해복구의 진행상황 등을 대책본부에 보고하여야 한다(제44조의8 제4항).

(2) 기간통신사업자

주요기간통신사업자는 그 소관에 속하는 전기통신역무에 관하여 통신재난이 발생한 때에 그 현황·원인·응급조치 내용 및 복구대책 등을 지체없이 방송통신위원회에 보고하여야 한다(제44조의7).

Ⅳ. 개인정보 보호체계

개인정보 보호체계와 관련된 법령으로는 공공부문에서「공공기관의 개인정보 보호에 관한 법률」,「전자정부법」및「주민등록법」등이 있으며, 민간부문에서는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「신용정보의 이용 및 보호에 관한 법률」등의 개별법이 존재하고 있다.

1. 공공기관의 개인정보 보호에 관한 법률

(1) 현행 개인정보보호법제 현황

종래 우리나라의 개인정보보호법제는 공공부문과 민간부문으로 이원화되어 있었고 그 법적 근거 및 추진체계를 달리하고 있었으며, 공공부문을 비롯한 정보통신, 금융, 의료부문 등에서 부처별·영역별로 산재해 있었다.[80] 공공부문에 있어서 개인정보보호를 위한 일반법으로 공공기관의개인정보보호에관한법률이 제정되었으며 이 밖에 주민등록법, 통계법, 공공기관의정보공개에관한법률, 전자정부법 등이 각각 공공부문에서 개인정보보호와 관련된 조항을 담고 있다. 특히 교육부문에 있어서는 원칙적으로 공공기관의개인정보보호에관한법률이 적용되나, 그 밖에 교육기본법, 초중등교육법, 학교보건법 및 각종 지침 등에 교육정보 보호에 관한 조항들이 개별적으로 나열되어 있다. 정보통신영역에 있어서는 가장 대표적인 개인정보보호 법률로서 정보통신망이용촉진및정보보호등에관한법률(이하 "정보통신망법"이라 한다)이 있으며, 그 밖에 전기통신기

80) 홍준형, "유비쿼터스 환경에서의 개인정보 보호"「공법연구」제32집 제5호, 204면

본법, 전파법, 통신비밀보호법 등이 있다. 그 밖에 금융분야의 개인정보보호 관련법률로는 신용정보의보호및이용에관한법률, 금융실명거래및비밀보장에관한법률 등이 있으며, 의료분야에는 보건의료기본법, 의료법, 전염병예방법, 후천성면역결핍증예방법, 생명윤리및안전에관한법률 등이 있다.

현행 개별분야 개인정보보호법제들은 특정한 조건을 두어 적용범위를 한정시키고 있을 뿐 아니라, 이들 법제 상호간에도 일관성이 없다. 엄격한 의미에서 개인정보보호법이라고 하기 위해서는 입법목적이 개인정보보호와 관련이 있어야 하고 해당 영역에서 개인정보를 취급하는 자가 어떠한 방법으로 무엇을 기준으로 삼아 개인정보를 처리하여야 하는지를 규정하고 있어야 할 것이나, 이러한 기준에 부합된다고 볼 수 있는 법률로는 공공기관의개인정보보호에관한법률이나 정보통신망법, 신용정보의이용및보호에관한법률 등을 언급할 수 있을 뿐이며 의료법, 변호사법, 보험업법 등의 법률들은 개인정보취급자 또는 이용자가 업무상 지득한 정보의 '비밀누설의무' 조항을 두고 있을 뿐 엄밀한 의미에서 개인정보보호법이라 말하기 곤란하다. 따라서 그렇지 않은 영역에서는 일반적인 의미에서 개인정보 또는 타인의 비밀을 누설하지 않아야 한다는 정도의 금지규정만 두고 있을 뿐 실질적으로 법이 그 기준이나 대안을 제시하고 있지 않고 있다. 그리고 대부분 개인정보의 침해에 관하여 사후적인 구제에 치중하고 있다는 비판을 받고 있다.

<표 1> 현행 개인정보보호 입법체계

구 분	관련 법규	규 제 내 용
공공부문	공공기관의개인정보보호에관한법률	○국가·공공기관 보유의 개인정보 보호 ○수집·처리·이용 과정상의 정보주체와 공공기관의 권리·의무 규율
	공공기관의정보공개에관한법률	○개인정보의 비공개, 부분공개
	주민등록법	○주민등록의 열람 또는 등·초본의 교부, 주민등록 전산정보자료의 이용 등
	통계법	○ 통계 작성 과정시 개인, 단체 법인의 비밀보호
	국정감사및조사에관한법률	○ 사생활 침해목적의 감사, 조사 제한
	국가공무원법	○ 업무상 지득한 비밀의 보호
통신부문	정보통신망이용촉진및정보보호등에관한법률	○정보통신서비스제공자에 의한 개인정보 수집, 처리 규제 ○여행업, 호텔업, 항공운송사업, 학원등 사업자의 개인정보보호
	통신비밀보호법	○우편물의 검열, 전기통신의 감청 등 통신관련 사생활의 보호
	통신제한조치의허가절차및비밀유지에관한규칙	○범죄수사·국가안보를 위한 통신제한조치의 허가절차
	전기통신사업법	○개별이용자에 관한 정보의 공개 및 유용금지 등
	위치정보의이용및보호등에관한법률	○위치정보의 수집·제공의 범위, 오·남용 방지
의료부분	보건의료기본법	○보건의료 관련 사생활의 보호
	의료법, 전염병예방법, 후천성면역결핍증예방법	○업무상 비밀 누설 금지
	생명윤리및안전에관한법률	○유전자정보의 보호 등
금융부문	신용정보의이용및보호에관한법률	○민간부문에 의한 개인신용정보 처리의 규제 ○신용정보주체의 열람 및 정정 청구 등
	금융실명거래및비밀보장에관한법률	○금융거래의 비밀보장
	증권거래법	○정보의 제공, 누설 금지
기타	변호사법, 외국환거래법, 법무사법, 공증인법 등	○업무상 지득한 비밀의 보호

출처: 김재광, "개인정보보호법 제정 후 주요 정책과제에 관한 고찰"「2008 미래정보사회 입법정책포럼 발제문」(2009. 1. 21) 참조>

이러한 현행법상의 문제점을 개선하고자 공공부문·민간부문을 모두 아우르는 개인정보보호법(안) - 이혜훈의원안, 변재일의원안 및 정부안 - 이 국회에 상정되어 있다.

통일적이고 체계적인 적용을 가능하게 하는 일반적 대원칙의 수용, 전문성이 요구되는 경우에만 특별법 또는 개별법을 제정하여 기본법의 원칙은 특별한 경우에만 그 적용의 예외를 인정, 기본법의 원칙이 보장되고 개별법에 산재되어 있는 예외규정을 최소화함으로써 법적 안정성과 법집행의 실효성 확보 등이 가능하도록 하여야 할 것이다.

(2) 개인정보보호기본법제정법률안의 주요내용

ⅰ) 입법동기

개인정보보호기본법제정법률안은 정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있으나, 국가사회 전반을 규율하는 개인정보 보호원칙과 개인정보 처리기준이 마련되지 못해 개인정보 보호의 사각지대가 발생할 뿐만 아니라, 최근 개인정보의 유출·오용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있는 바, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하려는 것이다.

ii) 3개 제정안의 주요사항 비교검토

<표 2>는 3개 제정안의 주요사항을 비교검토한 것이다.[표-2]을 보면 3개 제정안의 차이점과 공통점을 찾을 수 있고 추후 공청회에서 조정해야 할 쟁점에 대해서도 일정한 답을 제시할 수 있을 것이다.

<표 2> 제정안의 주요내용 비교

	이혜훈의원안	변재일의원안	정부안
추진체계	○ 국무총리소속 개인정보위원회 -정책 수립·집행기능 수행 ※ 조사, 시정명령 등 규제권 행사	○ 대통령소속 개인정보보호위원회 -정책 수립·집행기능 수행 ※ 조사, 시정명령 등 규제권 행사	○ 국무총리소속 개인정보보호위원회 -정책 심의·자문기능 수행 ※ 정책수립·집행은 행안부 및 관계부처 담당
피해구제	○ 개인정보위원회 內 개인정보분쟁조정위원회 설치	○ 개인정보보호위원회 內 개인정보분쟁조정위원회 설치	○ 개인정보분쟁조정위원회 별도 설치
	○ 조정결정에 재판상 화해 효력 부여(제58조)	○ 조정결정에 재판상 화해 효력 부여(제62조)	○ 조정결정에 민사상 합의 효력 부여(제44조)
	○ 집단분쟁조정 도입(제60조)	○ 집단분쟁조정 도입(제64조)	○ 집단분쟁조정 미도입
	○ 단체소송 미도입	○ 단체소송 도입(제67조~제73조)	○ 단체소송 미도입
처리기준	○ 개인정보 수집 및 처리시 동의원칙 명시 - 예외 사유 규정(제8조)	○ 개인정보 수집, 이용, 제공 등 처리기준 동일(제7조) ※ 정보주체 이외로부터 수집한 개인정보 처리시 고지의무 부과	○ 개인정보 수집·이용(제15조),제공(제17조) 기준 차등화 -제공시 더욱 엄격히 보호 ※ 계약이행, 개인정보처리자의 정당한 이익을 위해서는 정보주체 동의없이 제공 불가
	○ 공공부문은 - 법령상 소관사무 수	○ 공공기관은 법률에서 정하는 업무수행을 위해 불가	○ 공공기관은 법령 등에서 정하는 소관 업무수행

	이혜훈의원안	변재일의원안	정부안
	행 등 예외 인정(제30조)	피한 경우로 대통령령이 정하는 경우 등 처리	을 위해 불가피한 경우 수집·이용
업무위탁	○공개 또는 고지의무 없음 -수탁자 관리·감독, 손해배상책임 등만 규정(제15조)	○공개 또는 고지의무 없음 -수탁자 관리·감독, 손해배상책임 등만 규정(제23조)	○업무위탁시 정보주체에 대한 공개 또는 고지의무(제25조)
CCTV 등	○개인정보처리장치 설치·운영시 게시, 고지 등(제14조)	○자동정보처리장치 설치·운영시 고지 등(제18조)	○영상정보처리기기 설치·운영 기준 및 관리책임(제24조)
DB마케팅	○DB마케팅 사업 위원회 등록 및 관리·감독(제17조) -제3자 제공시 고지의무 완화	○DB마케팅사업 위원회 등록 및 관리·감독(제17조) - 제3자 제공시 고지의무 완화	○미도입
유출통지	○개인정보 누출·공개·도용(누출등) 통지 및 신고(제20조)	○개인정보 누출·공개·도용(누출등) 통지 및 신고(제25조)	○개인정보 유출시 통지(제32조)
개인정보영향평가등	○개인정보파일 등록(제31조) ○개인정보영향평가(제32조) ○파일 연계·연동시 협의(제33조)	○개인정보파일 등록(제13조) ○개인정보영향평가(제36조) ○파일 연계·연동시 협의(제14조)	○개인정보파일 등록(제30조) ○개인정보영향평가(제31조)
그밖의내용	○표준개인정보처리방침 등록(제7조) ○평가·인증기관 지정(제52조)	○표준개인정보처리방침 등록(제33조) ○평가·인증기관 지정(제38조)	○미도입

ⅲ) 개인정보처리(수집・이용・제공 등)의 기준 및 요건

<표 3>에서 보듯이 제정안은 모두 OECD 개인정보보호 8원칙(수집제한의 원칙(제1원칙), 정보의 질 확보의 원칙(제2원칙), 목적 명시의 원칙(제3원칙), 이용제한의 원칙(제4원칙), 안전성 확보의 원칙(제5원칙), 공개의 원칙(제6원칙), 개인참여의 원칙(제7원칙), 책임의 원칙(제8원칙) 등 국제적으로 정립된 개인정보보호 원칙을 비교적 충실히 반영하여 개인정보보호 및 수집・처리 원칙을 규정하고 있다(이혜훈의원안 제5조, 변재일의원안 및 정부안 제3조).

<표 3> 개인정보 수집・이용・제공 등 처리에 관한 기준 및 요건

구 분	이혜훈의원안	변재일의원안	정부안
수집・이용 요건	1정보주체의 동의 2법령상 허용 또는 법령상 의무 준수 3.계약체결・이행 4.급박한 생명・신체・재산상 이익 보호 5.정보처리자의 정당한 이익으로 정보주체 권리보다 명백히 우선하는 경우 (이상 안 제8조) 6.공공기관이 정보주체 동의, 급박한 생명・신체・재산상 이익 보호, 범죄수사 및 공소제기・유지, 법원 재판업무수행, 국제법상 의무이행, 기타 법률에서 정하는 업무수행을 위해 불가피한 경우(안 제30조)	1. 좌 동 2. 좌 동 3. 좌 동 4. 좌 동 5. 좌 동 6. 공공기관이 범죄수사, 공소제기·유지, 법원 재판업무수행, 국제법상 의무이행, 기타 법률에서 정하는 업무수행을 위해 불가피한 경우 (안 제7조)	1. 좌 동 2. 법률상 허용 또는 법령상 의무 준수 3. 좌 동 4. 좌 동 5. 좌 동 6. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 (안 제15조)

제3자 제공 요건	상동(별도동의 필요)	상동(별도동의 필요)	1. 별도 동의 2.법률 규정 또는 법령상 의무준수, 공공기관의 소관 업수행, 급박한 생명·신체·재산상 이익 보호를 위해 수집한 목적범위 내 제공 가능(안 제17조)
목적외 이용·제공	상기의 요건에 해당하는 경우외 목적외 이용 및 제공 금지 (안 제11조)	1. 별도 명시적 동의 2. 상기 2호부터 6호까지 해당할 경우를 제외하고는 목적외 이용 및 제공 금지 (안 제16조)	1.별도 동의 2 법률에 특별 규정 3.급박한 생명, 신체, 재산상 이익 4.통계 및 학술연구목적 5.소관업무 수행을 위해 개인정보보호위원회 심의를 거친 경우 6.조약, 국제협정 등의 이행을 위한 경우 7.범죄수사, 공소제기·유지 8.법원 재판업무 수행 9.형 및 감호, 보호처분의 집행(안 제18조) 단, 제5호부터 제9호까지는 공공기관만 적용

정부안은 개인정보의 수집·이용·제3자 제공 등 처리 단계별로 그 기준 및 요건을 차등화하여 별도로 규정하고 있는 반면, 의원안은 단계별로 구분하지 않고 수집시의 기준 및 요건을 모든 단계에 적용하도록 규

정하고 있다. 개인정보 보호의 강화라는 측면에서 볼 때, 정부안이 비교적 바람직한 입법방향으로 볼 수 있다.[81] 다만 개인정보의 처리기준 및 요건의 적절성 및 타당성 여부는 개인정보보호에 대한 인식 수준, 우리의 사회적·역사적·문화적 상황 등을 종합적으로 비교·검토하여 결정될 필요가 있으며, 예외사유 중 일부 불명확한 표현은 법률의 명확성 제고 차원에서 보다 구체화할 필요가 있다.

ⅳ) 정보주체 이외로부터 개인정보 수집시 고지의무

이혜훈의원안과 정부안은 정보주체의 동의를 받아 개인정보를 수집하는 경우, 정보주체에게 수집·이용 목적 등 필요사항을 고지하도록 하고 있으나, 동의 외의 경로를 통해 적법하게 개인정보를 수집하는 경우에 대한 고지 규정은 없다. 변재일의원안은 언론사·인터넷 포털 등을 통해 적법하게 공시·공개된 개인정보 또는 정보주체 이외의 다른 사람으로부터 수집한 개인정보를 처리하는 경우에도 정보주체의 요구가 있으면 수집 출처 및 처리목적·동의거부권 등을 고지하도록 하고 있다(안 제11조). 다만, 변재일의원안은 이 경우 고지의무의 예외사유를 규정하고 있으나, 그 요건이 일정 부분 불명확하고 포괄적이라 보여 이를 보다 구체화할 필요가 있다.[82]

ⅴ) 개인정보보호 추진체계

<표 4>에서 알 수 있듯이 제정안은 모두 개인정보보호 업무를 담당할 추진체계를 설치하도록 하고 있다(이혜훈의원안 제34조~제41조, 변재일의원안 제40조~제47조, 정부안 제9조·제10조). 의원안은 독립기구인 상

81) 행정안전위원회 검토보고서 42면 참조

82) 변재일의원안의 고지의무의 예외사유(안 제11조)를 보면, 고지로 인하여 공공안전·공중위생 등 공공의 안전과 이익에 중대한 위험을 초래할 우려가 있는 경우, 고지로 인하여 다른 사람의 권리·이익을 침해할 상당한 위험이 있는 경우이다.

설행정위원회를 두도록 하고 있는 반면, 정부안은 심의기구인 위원회와 집행기구로 분리하고 있다.

<표 4> 제정안별 개인정보보호 추진체계 비교

구 분	이혜훈의원안	변재일의원안	정부안
형 태	· 국무총리소속 개인정보위원회 및 사무처	· 대통령소속 개인정보보호위원회 및 사무처	· 국무총리소속 위원회(심의) · 행정안전부
기 능	· 개인정보 보호 및 이용에 관한 시책 수립 및 집행, 법령·제도 개선, 권리침해 조사 및 분쟁 조정, 피해구제 등 개인정보 정책 수립 및 집행 업무	좌 동	· 개인정보보호 기본계획 및 시행계획, 제도 개선 등에 관한 심의 및 의견제시 등 (개인정보보호위원회)
위원회 구성	· 9인 (위원장 및 상임위원 1인) · 위원장과 상임위원은 대통령이 임명, 비상임위원은 위원장이 추천한 자 중 국무총리가 임명	· 9인 (위원장 및 상임위원 1인) · 국회선출 3인 (상임위원 1인 포함) · 대통령 지명 3인 · 대법원장 지명 3인 · 위원장은 대통령이 임명	· 15인 이내 · 관련 고위공무원단에 속하는 공무원 · 시민사회단체 또는 소비자단체에서 추천받은 자 · 사업자단체에서 추천받은 자 · 개인정보 업무에 관한 학식과 경험이 풍부한 자 중 국무총리가 임명 또는 위촉

의원안의 경우 독립성 및 중립성을 강조하고 있는 반면, 정부안은 업무의 효율성 및 신속성을 강조하고 있는 것이 특징으로, 집행부로부터의 독립성이라는 기준에서 볼 때, 변재일의원안이 가장 독립성이 높고, 이혜훈의원안이 중간, 정부안이 독립성은 가장 낮다.

참고로 세계 각국은 유럽연합 개인정보보호지침의 주도적인 영향 하에서 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구

를 설치·운영하는 추세를 보이고 있다. 영미법계 국가 중 미국을 제외한 영국, 호주, 캐나다 등이 통합형 감독기구를 설치·운영하고 있고 미국만이 분산형 감독기구를 두고 있다.[83] 영미법계의 개인정보감독기구는 대체로 독립기구형식을 띄고 있다. 독립기구형으로 갈수록 독립성과 자율성이 실질적으로 확보된다고 하겠다. 독립기구형 개인정보감독기구는 일반적으로 ① 기관장의 임명이 행정부 수반 이외의 국왕이나 총독 등에 의해 이루어지고, ② 위원의 자격이 사법부나 입법부 등 행정부 이외의 기관에서 일하고 있거나 이들 기관의 추천을 받은 자로 제한되고, ③ 사무국이 개인정보감독기구에서 직접 운영하는 형식을 띠고 있다.[84] 한편 대륙법계 국가 중 프랑스는 국가정보자유위원회(CNIL)가 사인 및 공법인에 의한 법률의 준수를 감독·통제한다. 국가정보자유위원회는 독립된 행정위원회(une autorité administrative indépendante)의 법적 지위를 갖는다.[85] 독일에서는 개인정보보호를 위한 감독기구는 다소 복잡한 구조를 가지고 있는데, 연방개인정보보호청은 연방의 모든 공공기관에서의 개인정보처리와, 본래 연방관할에 속하는 통신서비스 및 우편서비스 부문에서의 개인정보처리에 대해서만 감독책임을 지고 통신과 우편을 제외한 민간부문의 개인정보처리에 대해서는 각 주가 지정하는 "정보감독청"이 감독책임을 지고 있다.[86]

개인정보보호의 오랜 역사를 지닌 유럽 각국이 얻은 결론은 개인정보

---

83) 개인정보처리의 기본원칙에 있어서는 미국이 시장중심적 접근방법을 채택하여 부문별 입법형식으로 나아간데 비하여, 영국 등은 권리중심적 접근방법을 채택하여 포괄적인 입법형식으로 나아가고 있다. 이러한 개인정보보호와 관련한 입법방식의 상이함은 입법배경에 미국은 자유주의적 정치전통이, 영국 등은 사회계약이론의 정치전통이 있는 것으로 파악되고 있다.

84) 김재광, "영미법계 국가의 개인정보보호법제 동향 및 함의"「공법학연구」제6권 제1호(한국비교공법학회, 2005) 참조.

85) 박균성,「프랑스의 전자정부법제」, 한국법제연구원, 2001, 85면.

86) 김재광, "개인정보보호법 제정 후 주요 정책과제에 관한 고찰"「2008 미래정보사회 입법정책포럼 발제문」(2009. 1. 21) 참조

보호의 성패는 효율적인 감독기관에 달렸다는 것이다. 감독기관은 상대적으로 열세에 있는 정보주체의 권리를 보호하기 위한 책임을 지며, 감시기능을 통해 분쟁의 소지를 사전에 제거할 수 있다. 이러한 개인정보보호전담기구제도는 공공 또는 민간부문의 개인정보 처리에 대한 지속적인 감시 및 조정기능과 정보보호 수준의 향상을 위한 관리적·기술적 대처방안을 연구하고 정보통신이용자의 권리를 보호하는 상담기능 이외에 새로운 정보기술 형태의 잠재적 영향력과 효과를 판단하여서 정보기술의 적용이 계획단계에서 개인정보보호와 조화될 수 있도록 권고하는 기능도 수행하는 것이 바람직하다.[87]

다만 <표 5>에서 보는 바와 같이 주요 외국의 경우 개인정보 보호기구가 다양한 형태로 존재하고 있으므로, 집행부로부터 독립적인 감독기구의 설치가 개인정보 침해를 예방하기 위한 필요충분요소는 아니라고 할 것이나, 현재 공공기관에서의 개인정보 침해사례가 증가하고 있는 현실과, 정보보호의 역사 역시 일천한 우리나라의 특성을 감안해 볼 때, 개인정보보호 업무의 전문성·객관성·투명성을 강화하기 위한 독립적인 위원회 형태의 조직설치가 필요하다는 학계의 일반적인 지적을 수용할 필요가 있을 것이다. 즉, 개인정보보호 추진체계 형태의 적합성 여부는 우리나라의 사회·경제적 환경과 법적 전통, 개인정보보호 수준 및 주요 외국의 사례 등을 종합적으로 고려하여 입법정책적으로 결정되어야 할 것으로 본다. 그런 측면에서 정부안의 심의기구에 불과한「개인정보보호위원회」의 소속(국무총리 → 대통령) 및 권한을 보다 강화하고, 위원 구성의 독립성을 제고하는 등 실질적인 기능상의 독립성을 강화하는 방안을 검토할 필요가 있다.[88]

---

87) 한국전산원,「국외 개인정보보호법제 분석 및 시사점」, 2004, 116면 참조
88) 행정안전위원회 검토보고서 51면 참조

<표 5> 주요 외국의 개인정보보호 추진체계

구분		근거법률	형 태	비고
일본		개인정보보호법 행정기관개인정보보호법	내각부 소속 「정보공개·개인정보보호 심사회」 설치 (공공) 총무성 장관 (민간) 각 부처	전담기구 없음
미국		(공공) 프라이버시법 (민간) 전자통신 프라이버시법 등 분야별 다수	(공공) 예산관리국(OMB) (민간) 연방거래위원회(FTC), 통신위원회(FCC) 등 ※ 자율규제 원칙	
유럽	영국	정보보호법	정보커미셔너 (국왕 임명, 별도 통합기금)	행정부로부터독립, 별도기구
	프랑스	정보처리축적및자유에 관한법률	정보자유위원회 (17인 구성, 법무부 예산)	
	독일	연방정보보호법	연방정보보호청 (대통령 임명, 연방내무부소속) 정보감독청(민간부문, 州별)	행정부소속형
	스웨덴	정보보호법	정보조사원 (재정부장관 임명, 인력·예산 지원)	
	덴마크	개인정보처리에관한법률	개인정보보호원 (법무부장관 임명, 예산 지원)	
	그리스	개인정보의처리및보호에 관한법률	정보보호원 (대통령 임명, 행정부소속)	
아시아	싱가포르	없음(입법 논의 중)	보호기구 없으나, 재정부에서 일부 기능 수행	전담기구 없음
	대만	컴퓨터에 의해 처리되는 개인정보보호에 관한 법률	(공공) 법무부 (민간) 각 부처	
	인도	없음	통신규제국, 금융감독기구 등에서 일부 기능 수행	
그 밖의 국가	캐나다	(공공)프라이버시법 (민간)개인정보보호및전자문서에관한법	연방프라이버시커미셔너 (추밀원장 임명, 예산·인사 독립)	행정부로부터독립, 별도 기구
	멕시코	없음(소비자보호법 등)	각 부처	전담기구 없음
	칠레	개인정보보호법	각 부처	

출처 : 행정안전부

vi) 개인정보 침해에 대한 분쟁해결 : 집단분쟁조정제도

제정안은 모두 개인정보에 관한 분쟁 조정, 침해행위의 중지, 원상회복 및 손해배상 등 개인정보 침해행위에 대한 분쟁해결을 위해「개인정보분쟁조정위원회」를 설치하도록 하고 있다(이혜훈의원안 제55조~제61조, 변재일의원안 제59조~제66조, 정부안 제38조~제47조). 다만, 그 소속을 의원안은 개인정보보호 추진체계(개인정보보호위원회 등) 산하에, 정부안은 현행 정보통신망법의 예에 따라 별도 기구로 설치하도록 하고 있으며, 조정의 효력에 대해 의원안은 분쟁조정에 대해 당사자가 15일 이내에 이의를 제기하지 아니할 경우 재판상 화해[89]가 있는 것으로, 정부안은 민사상 합의가 있는 것으로 보도록 규정하고 있다. 개인정보 피해는 특성상 소액피해가 대부분이고, 소액피해를 이유로 개별적으로 재판을 청구하는 사례는 거의 없다는 현실을 고려할 때 재판청구권을 과도하게 침해하지는 않을 것으로 보여, 소송에 따른 비용 및 시간절감 등을 위해 당사자의 적극적인 수용의사가 있는 경우에는 재판상 화해의 효력을 부여하는 방안을 검토할 필요가 있다.

한편, 의원안은 정부안과 달리 소비자기본법상의 집단분쟁조정제도를 도입하고 있다.[90] 집단분쟁조정제도란 피해가 다수의 소비자에게 같거나 비슷한 유형으로 발생하는 경우, 국가·지방자치단체·소비자단체 등 특정주체가 조정위원회에 일괄적인 분쟁조정을 의뢰(변재일의원안은 위원회의 직권으로 회부 가능)하는 것으로, 개인정보 피해는 다수에 걸친 소액 피해가 대부분이고, 최근 하나로텔레콤, 옥션 등 민간업체의 개인정보 유출에 대한 집단분쟁조정 절차가 개시되는 등 사회적 수요가 증가하고

89) 재판상 화해란 확정판결과 같은 효력이 부여됨에 따라 기판력이 인정되며, 화해에 재심사유가 있는 경우에만 재심의 소로 취소를 구할 수 있다.

90) 집단분쟁조정제도는 「소비자기본법」제68조에 규정되어 있으며, 2006년 9월부터 도입되어 있다.

있다는 점에서 도입할 필요성이 있다.

vii) 개인정보 영향평가

개인정보영향평가제도(Privacy Impact Assessment : PIA)는 개인정보 침해로 인한 피해는 원상회복 등 사후 권리구제가 어려우므로 영향평가의 실시로 미리 위험요인을 분석하고 이를 조기에 제거하여 개인정보 유출 및 오·남용 등의 피해를 효과적으로 예방할 수 있는 제도이다(.「사전예방의 원칙」). 즉, 개인정보영향평가제도는 새로운 정보시스템의 도입과 개인정보의 수집에 앞서 계획하고 있는 시스템이 구축·운영될 경우 프라이버시에 미칠 영향에 대하여 미리 조사·예측·검토하는 체계적인 절차를 의미한다.[91]

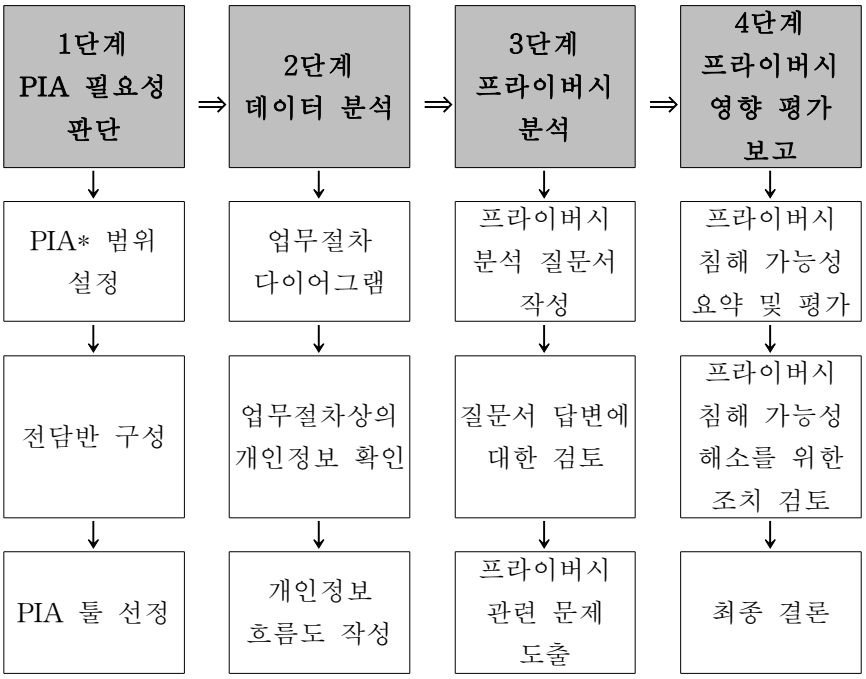
참고로 캐나다의 개인정보영향평가 절차도는 다음의[표-6]과 같다.[92]

---

91) 개인정보영향평가는 1989년에 David Flaherty의 "감시사회에서의 프라이버시보호(Protecting Privacy in Surveillance Societies)"란 저서에 그 개념이 제시된 후 1991년에 "개인정보영향평가를 위한 공식 가이드라인"이 미국 뉴욕 주 공공서비스 위원회의 "통신상의 프라이버시에 대한 정책(State of New York Public Service Commission, "Statement of Policy on Privacy in Telecommunications)"에서 제시되었고 1999년 이후에야 개인정보영향평가제도가 캐나다를 비롯한 몇몇 국가에서 의무적으로 시행되기 시작했다.

92) 캐나다의 경우 프라이버시 영향평가를 실시한 기관은 최종결과를 Privacy Commissioner에게 고지해야만 하며 이러한 고지는 평가의 대상이 된 프로그램이나 서비스가 실행되기 전 단계에서 이루어져야 한다. 이러한 사전고지는 Privacy Commissioner가 그러한 이슈를 검토하여 시행기관에게 적절한 프라이버시 보호조치를 하도록 조언할 수 있는 기회를 제공하도록 하기 위해 고안되어진 절차이다. 프라이버시 관련 이슈가 관련 프로그램과 서비스에 어떻게 관계되는지에 대하여 이해를 넓히기 위해 프라이버시영향평가를 실시한 기관은 PIA결과 요약본을 만들어 적절한 방법으로 일반에게 공개하여야 한다. 평가결과 요약본의 유포에는 인터넷과 기타 전통적인 출판방법이 사용되어 질 수 있으며 기타 관련된 문서나 참고자료도 함께 연계하여 공개할 수 있다.

<표 6> 캐나다 프라이버시 영향평가 절차도



* 출처 : 한국정보사회진흥원,「개인정보보호제도 시행을 위한 사례연구」, 37면

<표 2>]에서 보듯이 제정안은 모두 개인정보 영향평가제도를 도입하고 있다(이혜훈의원안 제32조, 변재일의원안 제36조·제37조, 정부안 제31조). 다만, 공공기관에 대해서는 일부 영향평가 대상 개인정보파일의 범위에서 차이가 있으나 의무적으로 도입하도록 한 반면, 민간부분에 대해서는 변재일의원안 및 정부안은 권고 또는 자율 실시를 원칙으로 하고 있고, 이혜훈의원안은 이에 대한 규정이 없다.

개인정보 영향평가제도는 정보시스템을 구축하기 전에 개인의 프라이버시에 영향을 미칠만한 요인을 사전에 발견하여 개선하고자 하는 것으

로, 공공·민간 구별 없이 모든 개인정보처리자에게 도입하는 것이 바람직하다는 의견도 있다.

그러나 민간부문은 원칙적으로 당사자 간 계약에 의하여 다양한 형태로 개인정보가 수집되는 경우가 많아 평가가 용이하지 않다는 점과 주요 외국의 경우도 공공기관만 의무화하고 있다는 점에서 제정안의 영향평가 실시 범위는 현실적인 측면을 고려한 규정이라 이해된다.[93]

한편, 의원안은 정부안과 달리 개인정보보호 추진체계(개인정보보호위원회 등)가 개인정보 영향평가 또는 개인정보 처리체계 평가 및 인증 등을 수행할 만한 적격기관을 평가·인증기관으로 지정하고, 관리·감독할 수 있도록 하고 있다(이혜훈 의원안 제52조·제53조, 변재일 의원안 제38조·제39조).

개인정보 영향평가 등 개인정보와 관련된 각종 평가 및 인증에 필요한 기술·시설·인력 등의 기준을 정하고, 이를 충족하는 기관만이 평가 및 인증 업무를 수행할 수 있도록 하는 것은 평가의 공정성과 전문성을 확보할 수 있다는 점에서, 의원안의 내용은 긍정적인 취지를 갖고 있다.

2. 주민등록법

가. 문제의 소재

1968년 주민통제 목적으로 만들어진 주민등록번호제도는 행정편의 제

93) 미국과 캐나다는 행정기관에 대해서만 프라이버시 영향평가를 의무적으로 시행하고 있고, 뉴질랜드·홍콩·호주 등에서는 공공·민간부문에 대해 시행을 권고하고 있는 정도라 파악되고 있다.

고에는 기여하였으나 개인식별번호로서 꼭 필요하지 않은 생년월일, 성별, 출생지역 정보를 담고 있고, 민간부문은 물론이고 공공기관에서도 주민등록번호 수집의 남용에 따른 개인정보유출이 심각한 수준에 이르고 있다.[94]

나. 주민등록제도의 연혁

일제강점기 때인 1942년 조선기류령(朝鮮寄留令)에 의해 지금과 유사한 형태의 거주자등록제도가 처음 실시 되었으며, 1950년 한국전쟁 중에 주민의 신분을 확인하기 위하여 시·도민증을 발급하였다. 1962년 5월 국민들의 거주관계, 상시 인구 동태파악 등을 목적으로 주민등록법이 제정되었는 바, 동법에 의해 모든 국민은 이름, 생년월일, 주소, 본적, 전출입사항 등을 시·읍·면에 등록하도록 의무화하였다. 1968년 9월,. 주민등록법 시행령 제3조와 동법 시행규칙 제1조에 따라, 최초로 주민등록번호가 도입되었다.

다. 주민등록번호제도의 문제점[95]

(1) 민감한 개인정보의 직접적 노출 - 개인정보자기결정권의 침해

주민등록번호 자체에 생년월일, 성별, 출생지역 등 개인의 민감한 정보를 담고 있어, 정보주체 본인의 의사와는 무관하게 이러한 개인정보가 그대로 노출되고 있다. 또한 주민등록번호는 그 사람을 대표하는 고유하

94) 김민호, "주민등록번호체계의 개편과 본인확인제도"「정보사회 신분확인제도의 법적 쟁점」(미래정보사회 입법정책포럼, 2009. 10. 16), 2면
95) 문제점에 대해서는 김민호, 앞의 글, 4-6면

고 유일한 번호로 평생 변경되지 않으므로 그 사람을 대체하는 표식이기도 하므로 인간의 존엄성을 훼손하다는 비판이 제기될 수 있다.

주민등록정보는 대부분의 행정행위에 기본적인 정보가 되고 있는데, 주민등록법과 관련된 개인정보의 등록제도는 총 400여개가 넘는 법령이 있다. 주민등록제도에 의하여 수집되는 정보는 개인정보를 침해할 위험성이 있는 민감한 정보가 포함되고 있다. 주민등록법시행령의 별지 1호 서식에서 혈액형, 직업, 혼인관계, 학력, 동원보류, 동원면제사유 등은 개인에 따라서 매우 민감한 정보로 인지될 수 있다. 인구이동상황을 파악하는데 주민편의와 혈액형, 직업, 혼인관계, 학력 등이 어떠한 연관성이 있는지 명확하지 않다. 또한 우리의 주민등록제도에서는 수집되는 개인정보의 유형을 법률이 아닌 시행령에 의하여 규정하고 있어서 그것이 법률사항이라는 측면에서 합법성의 논란이 있을 수 있다.[96]

둘째, 주민등록정보는 제도적으로 400여개가 넘는 법령에서 공동으로 이용되고, G4C시스템 및 전자정부의 이름으로 공동이용을 확대하고 있다. 이러한 개인정보의 공동이용은 수집목적의 이용을 제한하는 정당한 정보활동의 원칙을 위반하는 측면이 있다. 주민등록법이 “주민의 주거관계 등 인구의 동태를 상시로 명확히 파악”하는 것을 목적으로 하는 수단적인 성격의 법률이라고 할 때에 법의 기본목적을 유월하는 것으로 이해될 수 있다.[97]

(2) 포괄적 위임금지 원칙 위반

개인의 민감정보가 그대로 노출되는 , 즉 개인정보자기결정권이 침해

96) 박홍윤・변종화・임동욱, 전게논문 참조.
97) 박홍윤・변종화・임동욱, 전게논문 참조.

되는 주민등록번호 부여체계를 현행과 같이 13자리로 정하고 있는 것은 「주민등록법 시행규칙」인데, 「주민등록법」이나 「주민등록법 시행령」은 이와 관련하여 포괄적으로 위임하고 있다는 문제점이 지적되고 있다. 주민등록법 제7조제4항은 “주민등록번호를 부여하는 방법”을 대통령령으로 정하도록 위임하고 있으며, 「주민등록법 시행령」 제7조제4항은 “주민등록번호의 부여에 필요한 사항은 행정안전부장관이 정한다”고 규정하고 있을 뿐이다.

(3) 주민등록번호의 과다 수집

인터넷상에서는 회원가입・서비스이용 시 주민등록번호가 본인확인 및 성인인증 등을 위한 수단으로 널리 이용되고 있고, 따라서 주민등록번호의 유출 및 도용사고가 빈번하게 발생하고 있다. 이같은 주민등록번호의 유출 및 도용사고는 개인정보침해 상담・피해 접수건수의 거의 반에 가까운 건수를 기록하는 등 그 피해가 심각하다.

라. 선진 각국의 주민등록제도

이탈리아는 원칙적으로 개인신분번호가 없으나, 유사한 기능을 가진 세무번호(Codice Fiscale)가 존재한다. 일본은 원칙적으로 개인신분번호가 없으며, 주민기본대장법상의 ‘주민코드’가 유사한 역할을 담당하고 있다. 네델란드는 2007년 11월부터 시민서비스번호(BSN: Burger Service Number)를 도입, 기존의 사회보장번호(SoFi: Social Fiscal Number)를 대체하였다. 스페인은 우리 주민등록증과 유사한 국가신분증(DNI: Documento Nacional de Identidad)제도를 운영하고 있다. 스웨덴은 우리 주민등록번호 제도와 유사한 개인식별번호(PIN: Personal Identify

Number)제도를 운영하고 있다. 미국은 원칙적으로 개인신분번호가 없으나, 사실상의 신분번호로서 사회보장번호(SSN: Social Security Number)가 있다.[98]

마. 주민등록번호제도의 개선방안

첫째, 주민등록번호(관리번호, Source PIN)와 개인식별번호(신분번호, Sector Specific)의 분리하는 방안이다. 주민등록번호제도의 개편에 따른 사회적 혼란을 최소화하고 보다 저비용 고효율의 개선방안을 토출하기 위해서는 현행 주민등록번호(관리번호, Source PIN)는 그대로 두고, 행정청이 주민등록증을 발급할 때 별도의 시스템에 의하여 개인별 식별번호(신분번호, Sector Specific)를 부여하는 방안이 있다. 둘째, 개인식별번호의 체계의 개편하는 방안이다. 개인식별번호를 부여할 때에는 번호체계가 개인의 연령, 성별 및 출생지를 알 수 없는 무작위 번호(Meaningless Number)가 되어야 한다. 또한 번호체계의 내용 및 조합의 비공개가 확보되어야 한다.[99]

3. 전자서명법

1999년에 제정된 '전자서명법'은 전자적 환경에서 전자서명의 규범적 기초 위에 공인전자서명체계를 세워 전자문서의 안전성·신뢰성을 확보하고 다양한 분야에 공인인증서의 이용확산을 이끌어내었다. 이러한 공인전자서명은 실거래계에서 거래당사자의 신원을 확인하는 전자신분증의 역할로 확대하여 이용되면서 1,500만 명 이상이 사용하는 전자적 거래의

98) 김민호, 앞의 글, 7-12면
99) 김민호, 앞의 글, 12-13면

매체가 되었다. 아울러, 2001년 전자정부법은 전자정부의 구현에 필요한 전자문서의 이용에 따라 행정관인에 터 잡아 전자관인에 행정기관의 형식성을 담아 전자서명을 사용하는 법적 근거를 마련하였다. 이처럼 전자정부법상의 "행정전자서명"은 행정처분시 권한 있는 행정기관임을 대외적으로 표시하는 비인격적인(non-individual) 권한표시 제공 수단으로서, Off-line상 관인(청인과 직인)과 동일한 기능과 법적 효력을 갖는다. 처음에 꾸려낸 전자관인은 후에 행정전자서명으로 탈바꿈하면서 그 적용범위를 확대하였고, 행정기관 또는 공무원이 아닌 외부 공공기관의 업무담당자에게도 발급할 수 있게 되었다. 행정행위라는 제한된 안목에서 행정전자서명을 사용하기 시작하였지만, 점차 행정기관의 전자적 거래 외에 행정정보의 공유라는 차원에서 행정전자서명 뿐만 아니라, 공인전자서명도 호환할 수 있도록 하는 법제도로 확대를 논의하여 왔다. 이렇듯 전자서명법과 전자정부법에 규정한 전자서명은 전자문서의 안전성·신뢰성을 확보할 목적으로 마련한 정보사회의 기반에 해당한다. 공인전자서명과 행정전자서명은 공통의 기술적 특징을 가지고 있지만, 개별법의 목적·적용범위 및 운용체계의 상이함으로 각각 독립된 체계로 운용되고 있으며, 행정전자서명의 사용범위의 확대는 전자서명법상 공인전자서명체계와 일정 영역에서 체계상 혼란을 야기하기도 하였다.[100] 그러나 공인전자서명체계는 주로 전자거래에 사용되는 적용범위를 상정하고 이의 전자문서의 안전성·신뢰성을 확보하기 위하여 구축되었지만, 정부전자서명체계는 행정관인의 기능을 띤 것으로 행정기관 내부에 한정하여 그 적용범위를 상정하였다는 점에서 기본적인 차이를 드러낸다.

정부조직개편(2008.2.29)으로 공인전자서명체계와 행정전자서명체계의

100) 배대헌, 성장한 전자서명, 어떻게 성숙하나 - 전자서명 관련법제 및 이의 발전방향 모색, 인터넷법학회(2008.5.9) 발표논문 참조

최상위인증기관이 모두 행정안전부의 감독을 받는 현실적 사정 하에서 행정상 통합을 이루었고, 이를 기술과 정책에 있어서 하나의 체제를 구축하느냐에 관한 논의로 남게 되었다. 향후 이에 대한 입법정책적 논의는 두 가지 전자서명체계를 하나로 담아내는 형식을 먼저 정하되, 기술과 정책으로 이를 연장할 것인지에 대한 정책적 판단에 따라 규정을 정비하는지 여부를 최종적으로 결정할 수 있을 것이다.[101]

<표 7> 행정전자서명인증과 공인전자서명인증의 비교

구 분	공인전자서명인증(NPKI) (National Public Key Infrastructure)	행정전자서명인증(GPKI) (Government Public Key nfrastructure)
근거법령	전자서명법	전자정부법
발급대상	자연인 또는 법인(대리인)	행정기관(organ)
행사효과	권리의무주체의 신원확인	기관의 권한표시
처벌대상	발급대상자	공무원(행정기관이 아님)
발급성격	공증적 행위	권한 위임적 행위
가입탈퇴	임의신청주의	강제주의
용도	사적계약	행정행위
공무원	사인의 지위에서 사용	직무상 행위시 사용
수수료	유료	무료

101) 배대헌, 앞의논문, 2008

4. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

가. 입법목적

정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다(법률 제1조).

나. 정보통신망과 침해사고

"정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다(법률 제2조제1호). "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다(법률 제2조제7호).

다. 정보통신망의 보호체계

정보통신망의 보호체계는 ① 행정안전부장관, 지식경제부장관 또는 방송통신위원회, ② 행정안전부장관 또는 방송통신위원회, ③ 지식경제부장관, ④ 정보통신서비스 제공자, ⑤ 방송통신위원회, ⑥ 집적정보통신시설 사업자, ⑦ 안전진단 수행기관 등으로 구성되어 있다.

먼저, 행정안전부장관, 지식경제부장관 또는 방송통신위원회는 정보통신망 이용촉진 및 정보보호 등에 관한 시책의 마련(제4조)의 임무를 수행한다.

행정안전부장관 또는 방송통신위원회는 자료 등의 보호 및 폐기(제64조의2)의 임무를 수행한다.

지식경제부장관은 기술개발의 추진 등(제6조), 기술관련 정보의 관리 및 보급(제7조), 정보통신망의 표준화 및 인증(제8조), 인증기관의 지정 등(제9조), 정보통신망의 이용촉진 등에 관한 사업(제13조), 인터넷 서비스의 품질 개선(제15조)의 임무를 수행한다.

정보통신서비스 제공자는 개인정보의 수집·이용 동의 등(22조), 개인정보의 수집 제한 등(제23조), 주민등록번호 외의 회원가입 방법(제23조의2), 개인정보의 이용 제한(제24조), 개인정보의 제공 동의 등(제24조의2), 개인정보의 취급위탁(제25조), 영업의 양수 등에 따른 개인정보의 이전(제26조), 개인정보 관리책임자의 지정(제27조), 개인정보 취급방침의 공개(제27조의2), 개인정보의 보호조치(제28조), 개인정보의 파기(제29조), 청소년 보호 책임자의 지정 등(제42조의3), 임의의 임시조치(제44조의3), 자율규제(제44조의4), 정보통신망의 안정성 확보 등(제45조), 침해사고의 원인 분석 등(제48조의4), 정보 전송 역무 제공 등의 제한(제50조의4), 영리목적의 광고성 프로그램 등의 설치(제50조의5), 국외 이전 개인정보의 보호(제63조)의 임무를 수행한다.

방송통신위원회는 청소년 보호를 위한 시책의 마련 등(제41조), 정보보호 관리체계의 인증(제47조), 정보보호 관리체계 인증기관의 지정취소 등(제47조의2), 침해사고의 대응 등(제48조의2), 영리목적의 광고성 정보 전

송차단 소프트웨어의 보급 등(제50조의6), 과징금의 부과 등(제64조의3)의 임무를 수행한다.

집적정보통신시설 사업자는 집적된 정보통신시설의 보호(제46조), 집적정보통신시설 사업자의 긴급대응(제46조의2)의 임무를 수행한다.

안전진단 수행기관은 정보보호 안전진단(제46조의3)의 임무를 수행한다.

(1) 행정안전부장관, 지식경제부장관 또는 방송통신위원회

행정안전부장관, 지식경제부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다(법률 제4조제1항). 제1항에 따른 시책에는 다음 각 호의 사항(1. 정보통신망에 관련된 기술의 개발·보급, 2. 정보통신망의 표준화, 3. 정보내용물 및 제11조에 따른 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화, 4. 정보통신망을 이용한 정보의 공동활용 촉진, 5. 인터넷 이용의 활성화, 6. 정보통신망을 통하여 수집·처리·보관·이용되는 개인정보의 보호 및 그와 관련된 기술의 개발·보급, 7. 정보통신망에서의 청소년 보호, 8. 정보통신망의 안전성 및 신뢰성 제고, 9. 그 밖에 정보통신망 이용촉진 및 정보보호등을 위하여 필요한 사항)이 포함되어야 한다(법률 제4조제2항). 행정안전부장관, 지식경제부장관 또는 방송통신위원회는 제1항에 따른 시책을 마련할 때에는 「정보화촉진기본법」 제5조에 따른 정보화촉진기본계획과 연계되도록 하여야 한다(법률 제4조제3항).

(2) 행정안전부장관 또는 방송통신위원회

행정안전부장관 또는 방송통신위원회는 자료 등의 보호 및 폐기(제64조의2)의 임무를 수행한다. 행정안전부장관 또는 방송통신위원회는 정보통신서비스 제공자등으로부터 제64조에 따라 제출되거나 수집된 서류·자료 등에 대한 보호 요구를 받으면 이를 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다(법률 제64조의2 제1항). 행정안전부장관 또는 방송통신위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보안조치를 하여야 한다(법률 제64조의2 제2항). 행정안전부장관 또는 방송통신위원회는 다른 법률에 특별한 규정이 있는 경우 외에 다음 각 호(1. 제64조에 따른 자료제출 요구, 출입검사, 시정명령 등의 목적이 달성된 경우, 2. 제64조제4항에 따른 시정조치명령에 불복하여 행정심판이 청구되거나 행정소송이 제기된 경우에는 해당 행정쟁송절차가 끝난 경우, 3. 제76조제4항에 따른 과태료 처분이 있고 이에 대한 이의제기가 없는 경우에는 같은 조 제5항에 따른 이의제기기간이 끝난 경우, 4. 제76조제4항에 따른 과태료 처분에 대하여 이의제기가 있는 경우에는 해당 관할 법원에 의한 비송사건절차가 끝난 경우)의 어느 하나에 해당하는 사유가 발생하면 제64조에 따라 제출되거나 수집된 서류·자료 등을 즉시 폐기하여야 한다. 제65조에 따라 행정안전부장관, 지식경제부장관 또는 방송통신위원회의 권한의 전부 또는 일부를 위임 또는 위탁받은 자도 또한 같다(법률 제64조의2 제3항).

(3) 지식경제부장관

기술개발의 추진 등(제6조), 기술관련 정보의 관리 및 보급(제7조), 정

보통신망의 표준화 및 인증(제8조), 인증기관의 지정 등(제9조), 정보통신망의 이용촉진 등에 관한 사업(제13조), 인터넷 서비스의 품질 개선(제15조)의 임무를 수행한다.

ⅰ) 기술개발의 추진 등

지식경제부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 연구기관으로 하여금 연구개발·기술협력·기술이전 또는 기술지도 등의 사업을 하게 할 수 있다(법률 제6조제1항). 정부는 제1항에 따라 연구개발 등의 사업을 하는 연구기관에는 그 사업에 드는 비용의 전부 또는 일부를 지원할 수 있다(법률 제6조제2항). 제2항에 따른 비용의 지급 및 관리 등에 필요한 사항은 대통령령으로 정한다(법률 제6조제3항).

ⅱ) 기술관련 정보의 관리 및 보급

지식경제부장관은 정보통신망과 관련된 기술 및 기기에 관한 정보(이하 이 조에서 "기술관련 정보"라 한다)를 체계적이고 종합적으로 관리하여야 한다(법률 제7조제1항). 지식경제부장관은 기술관련 정보를 체계적이고 종합적으로 관리하기 위하여 필요하면 관계 행정기관 및 국공립 연구기관 등에 대하여 기술관련 정보와 관련된 자료를 요구할 수 있다. 이 경우 요구를 받은 기관의 장은 특별한 사유가 없으면 그 요구에 따라야 한다(법률 제7조제2항). 지식경제부장관은 기술관련 정보를 신속하고 편리하게 이용할 수 있도록 그 보급을 위한 사업을 하여야 한다(법률 제7조제3항). 제3항에 따라 보급하려는 정보통신망과 관련된 기술 및 기기의 범위에 관하여 필요한 사항은 대통령령으로 정한다(법률 제7조제4항).

ⅲ) 정보통신망의 표준화 및 인증

지식경제부장관은 정보통신망의 이용을 촉진하기 위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신서비스 제공자 또는 정보통신망과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다. 다만, 「산업표준화법」 제12조에 따른 한국산업표준이 제정되어 있는 사항에 대하여는 그 표준에 따른다(법률 제8조제1항). 제1항에 따라 고시된 표준에 적합한 정보통신과 관련된 제품을 제조하거나 공급하는 자는 제9조제1항에 따른 인증기관의 인증을 받아 그 제품이 표준에 적합한 것임을 나타내는 표시를 할 수 있다(법률 제8조제2항). 제1항 단서에 해당하는 경우로서 「산업표준화법」 제15조에 따라 인증을 받은 경우에는 제2항에 따른 인증을 받은 것으로 본다(법률 제8조제3항). 제2항에 따른 인증을 받은 자가 아니면 그 제품이 표준에 적합한 것임을 나타내는 표시를 하거나 이와 비슷한 표시를 하여서는 아니 되며, 이와 비슷한 표시를 한 제품을 판매하거나 판매할 목적으로 진열하여서는 아니 된다(법률 제8조제4항). 지식경제부장관은 제4항을 위반하여 제품을 판매하거나 판매할 목적으로 진열한 자에게 그 제품을 수거·반품하도록 하거나 인증을 받아 그 표시를 하도록 하는 등 필요한 시정조치를 명할 수 있다(법률 제8조제5항). 제1항부터 제3항까지의 규정에 따른 표준화의 대상·방법·절차 및 인증표시, 제5항에 따른 수거·반품·시정 등에 필요한 사항은 지식경제부령으로 정한다(법률 제8조제6항).

ⅳ) 인증기관의 지정 등

지식경제부장관은 정보통신망과 관련된 제품을 제조하거나 공급하는 자의 제품이 제8조제1항 본문에 따라 고시된 표준에 적합한 제품임을 인증하는 기관(이하 "인증기관"이라 한다)을 지정할 수 있다(법률 제9조제1항). 지식경제부장관은 인증기관이 다음 각 호(1. 속임수나 그 밖의 부정

한 방법으로 지정을 받은 경우, 2. 정당한 사유 없이 1년 이상 계속하여 인증업무를 하지 아니한 경우, 3. 제3항에 따른 지정기준에 미달한 경우)의 어느 하나에 해당하면 그 지정을 취소하거나 6개월 이내의 기간을 정하여 업무의 정지를 명할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다(법률 제9조제2항). 제1항 및 제2항에 따른 인증기관의 지정기준·지정절차, 지정취소·업무정지의 기준 등에 필요한 사항은 지식경제부령으로 정한다(법률 제9조제3항).

ⅴ) 정보통신망의 이용촉진 등에 관한 사업

지식경제부장관은 공공, 지역, 산업, 생활 및 사회적 복지 등 각 분야의 정보통신망의 이용촉진과 정보격차의 해소를 위하여 관련 기술·기기 및 응용서비스의 효율적인 활용·보급을 촉진하기 위한 사업을 대통령령으로 정하는 바에 따라 실시할 수 있다(법률 제13조제1항). 정부는 제1항에 따른 사업에 참여하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다(법률 제13조제2항).

ⅵ) 인터넷 서비스의 품질 개선

지식경제부장관은 인터넷 서비스 이용자의 권익을 보호하고 인터넷 서비스의 품질 향상 및 안정적 제공을 보장하기 위한 시책을 마련하여야 한다(법률 제15조제1항). 지식경제부장관은 제1항에 따른 시책을 추진하기 위하여 필요하면 정보통신서비스 제공자단체 및 이용자단체 등의 의견을 들어 인터넷 서비스 품질의 측정·평가에 관한 기준을 정하여 고시할 수 있다(법률 제15조제2항). 정보통신서비스 제공자는 제2항에 따른 기준에 따라 자율적으로 인터넷 서비스의 품질 현황을 평가하여 그 결과를 이용자에게 알려줄 수 있다(법률 제15조제3항).

(4) 정보통신서비스 제공자

개인정보의 수집·이용 동의 등(22조), 개인정보의 수집 제한 등(제23조), 개인정보의 이용 제한(제24조), 개인정보의 제공 동의 등(제24조의2), 개인정보의 취급위탁(제25조), 영업의 양수 등에 따른 개인정보의 이전(제26조), 개인정보 관리책임자의 지정(제27조), 개인정보 취급방침의 공개(제27조의2), 개인정보의 보호조치(제28조), 개인정보의 파기(제29조), 청소년 보호 책임자의 지정 등(제42조의3), 임의의 임시조치(제44조의3), 자율규제(제44조의4), 정보통신망의 안정성 확보 등(제45조), 침해사고의 원인 분석 등(제48조의4), 정보 전송 역무 제공 등의 제한(제50조의4), 영리목적의 광고성 프로그램 등의 설치(제50조의5), 국외 이전 개인정보의 보호(제63조)의 임무를 수행한다.

ⅰ) 개인정보의 수집·이용 동의 등

정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호(1. 개인정보의 수집·이용 목적, 2. 수집하는 개인정보의 항목, 3. 개인정보의 보유·이용 기간)의 어느 하나의 사항을 변경하려는 경우에도 또한 같다(제22조제1항). 정보통신서비스 제공자는 다음 각 호(1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우, 3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우)의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다(제22조제2항).

ii) 개인정보의 수집 제한 등

정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다(제23조제1항). 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다(제23조제2항).

iii) 개인정보의 이용 제한

정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다(제24조).

iv) 개인정보의 제공 동의 등

정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호(1. 개인정보를 제공받는 자, 2. 개인정보를 제공받는 자의 개인정보 이용 목적, 3. 제공하는 개인정보의 항목, 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간)의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다(제24조의2 제1항). 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적

외의 용도로 이용하여서는 아니 된다(제24조의2 제2항).

ⅴ) 개인정보의 취급위탁

정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호(1. 개인정보 취급위탁을 받는 자(이하 "수탁자"라 한다), 2. 개인정보 취급위탁을 하는 업무의 내용)의 어느 하나의 사항이 변경되는 경우에도 또한 같다(제25조제1항). 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다(제25조제2항). 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다(제25조제3항). 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다(제25조제4항). 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다(제25조제5항).

vi) 영업의 양수 등에 따른 개인정보의 이전

정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항(1. 개인정보를 이전하려는 사실, 2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다)·주소·전화번호 및 그 밖의 연락처, 3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차) 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다(제26조제1항). 영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실을 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다. 다만, 정보통신서비스 제공자등이 제1항에 따라 그 이전사실을 이미 알린 경우에는 그러하지 아니하다(제26조제2항). 영업양수자등은 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초 목적의 범위에서만 개인정보를 이용하거나 제공할 수 있다. 다만, 이용자로부터 별도의 동의를 받은 경우에는 그러하지 아니하다(제26조제3항).

vii) 개인정보 관리책임자의 지정

정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다(제27조제1항). 제1항 단서에 따른 정보통신서비스 제공자등이 개인정보 관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 관리책임자가 된다(제27조제2항). 개인정보 관리책임자의 자

격요건과 그 밖의 지정에 필요한 사항은 대통령령으로 정한다(제27조제3항).

viii) 개인정보 취급방침의 공개

정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다(제27조의2 제1항). 제1항에 따른 개인정보 취급방침에는 다음 각 호의 사항(1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법, 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목, 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다), 4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 취급방침에 포함한다), 5. 이용자 및 법정대리인의 권리와 그 행사방법, 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항, 7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처)이 모두 포함되어야 한다(제27조의2 제2항). 정보통신서비스 제공자등은 제1항에 따른 개인정보 취급방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다(제27조의2 제3항).

ix) 개인정보의 보호조치

정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호(1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행, 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영, 3. 접속기록의 위조·변조 방지를 위한 조치, 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치, 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치, 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치)의 기술적·관리적 조치를 하여야 한다(제28조제1항). 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다(제28조제2항).

x) 개인정보의 파기

정보통신서비스 제공자등은 다음 각 호(1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우, 2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우, 3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우, 4. 사업을 폐업하는 경우)의 어느 하나에 해당하는 경우에는 해당 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다(제29조).

xi) 청소년 보호 책임자의 지정 등

정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 정보통신망의 청소년유해정보로부터 청소년을 보호하기 위하여 청소년 보호 책임자를 지정하여야 한다(제42조의3 제1항). 청소년 보호 책임자는 해당 사업자의 임원 또는 청소년 보호와 관련된 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 지정한다(제42조의3 제2항). 청소년 보호 책임자는 정보통신망의 청소년유해정보를 차단·관리하고, 청소년유해정보로부터의 청소년 보호계획을 수립하는 등 청소년 보호업무를 하여야 한다(제42조의3 제3항). 제1항에 따른 청소년 보호 책임자의 지정에 필요한 사항은 대통령령으로 정한다(제42조의3 제4항).

xii) 임의의 임시조치

정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다(제44조의3 제1항). 제1항에 따른 임시조치에 관하여는 제44조의2제2항 후단, 제4항 후단 및 제5항을 준용한다(제44조의3 제1항).

xiii) 자율규제

정보통신서비스 제공자단체는 이용자를 보호하고 안전하며 신뢰할 수 있는 정보통신서비스를 제공하기 위하여 정보통신서비스 제공자 행동강령을 정하여 시행할 수 있다(제44조의4).

xiv) 정보통신망의 안정성 확보 등

정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신

망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다(제45조제1항). 방송통신위원회는 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치 및 안전진단의 방법·절차·수수료에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다(제45조제2항). 정보보호지침에는 다음 각 호의 사항(1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치, 2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치, 3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치, 4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치)이 포함되어야 한다(제45조제3항).

xv) 침해사고의 원인 분석 등

정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다(제48조의4 제1항). 방송통신위원회는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다(제48조의4 제2항).방송통신위원회는 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다(제48조의4 제3항). 방송통신위원회는 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장

에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다(제48조의4 제4항). 방송통신위원회나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다(제48조의4 제5항). 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다(제48조의4 제6항).

xvi) 정보 전송 역무 제공 등의 제한

정보통신서비스 제공자는 다음 각 호(1. 광고성 정보의 전송 또는 수신으로 역무의 제공에 장애가 일어나거나 일어날 우려가 있는 경우, 2. 이용자가 광고성 정보의 수신을 원하지 아니하는 경우, 3. 이용계약을 통하여 해당 정보통신서비스 제공자가 이용자에게 제공하는 서비스가 불법 광고성 정보 전송에 이용되고 있는 경우)의 어느 하나에 해당하는 경우에 해당 역무의 제공을 거부하는 조치를 할 수 있다(제50조의4 제1항). 정보통신서비스 제공자는 제1항에 따른 거부조치를 하려면 해당 역무 제공의 거부에 관한 사항을 그 역무의 이용자와 체결하는 정보통신서비스 이용계약의 내용에 포함하여야 한다(제50조의4 제2항). 정보통신서비스 제공자는 제1항에 따라 거부조치를 하려면 그 역무를 제공받는 이용자 등 이해관계인에게 그 사실을 알려야 한다. 다만, 미리 알리는 것이 곤란한 경우에는 거부조치를 한 후 지체 없이 알려야 한다(제50조의4 제3항).

xvii) 영리목적의 광고성 프로그램 등의 설치

정보통신서비스 제공자는 영리목적의 광고성 정보가 보이도록 하거나

개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 대통령령으로 정하는 정보처리장치에 설치하려면 이용자의 동의를 받아야 한다. 이 경우 해당 프로그램의 용도와 삭제방법을 고지하여야 한다(제50조의5).

xviii) 국외 이전 개인정보의 보호

정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다(제63조제1항). 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다(제63조제2항). 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항(1. 이전되는 개인정보 항목, 2. 개인정보가 이전되는 국가, 이전일시 및 이전방법, 3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다), 4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간) 모두를 이용자에게 고지하여야 한다(제63조제3항). 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다(제63조제4항).

마. 방송통신위원회

청소년 보호를 위한 시책의 마련 등(제41조), 정보보호 관리체계의 인증(제47조), 정보보호 관리체계 인증기관의 지정취소 등(제47조의2), 침해사고의 대응 등(제48조의2), 영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등(제50조의6), 과징금의 부과 등(제64조의3)의 임무를 수행한다.

(1) 청소년 보호를 위한 시책의 마련 등

방송통신위원회는 정보통신망을 통하여 유통되는 음란·폭력정보 등 청소년에게 해로운 정보(이하 "청소년유해정보"라 한다)로부터 청소년을 보호하기 위하여 다음 각 호(1. 내용 선별 소프트웨어의 개발 및 보급, 2. 청소년 보호를 위한 기술의 개발 및 보급, 3. 청소년 보호를 위한 교육 및 홍보, 4. 그 밖에 청소년 보호를 위하여 대통령령으로 정하는 사항)의 시책을 마련하여야 한다(제41조제1항). 방송통신위원회는 제1항에 따른 시책을 추진할 때에는 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조에 따른 방송통신심의위원회(이하 "심의위원회"라 한다), 정보통신서비스 제공자단체·이용자단체, 그 밖의 관련 전문기관이 실시하는 청소년 보호를 위한 활동을 지원할 수 있다(제41조제2항).

(2) 정보보호 관리체계의 인증

정보통신망의 안정성 및 신뢰성을 확보하기 위하여 기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자는 정보보호 관리체계가 제2항에 따라 방송통신위원회가 고시한 기준에 적합한지에 관하여 방송통신위원회나 한국인터넷진흥원이 지정하는 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로부터 인증을 받을 수 있다(제47조제1항). 방송통신위원회는 제1항에 따른 인증에 관한 정보보호 관리기준 등 필요한 기준을 정하여 고시할 수 있다(제47조제2항). 제1항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다(제47조제3항). 제1항에 따른 인증의 방법·절차와 그 밖에 필요한 사항은 대통령령으로 정한다(제47조제4항). 정보보호 관리체계 인증기

관 지정의 기준・절차・유효기간 등에 필요한 사항은 대통령령으로 정한다(제47조제5항).

(3) 정보보호 관리체계 인증기관의 지정취소 등

방송통신위원회는 제47조에 따라 정보보호 관리체계 인증기관으로 지정받은 법인 또는 단체가 다음 각 호(1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증기관의 지정을 받은 경우, 2. 업무정지기간 중에 인증을 한 경우, 3. 정당한 사유 없이 인증을 하지 아니한 경우, 4. 제47조제4항을 위반하여 인증을 한 경우, 5. 제47조제5항에 따른 지정기준에 적합하지 아니하게 된 경우)의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다(제47조의2 제1항). 제1항에 따른 지정취소 및 업무정지 등에 필요한 사항은 대통령령으로 정한다(제47조의2 제2항).

(4) 침해사고의 대응 등(제48조의2)

방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무(1. 침해사고에 관한 정보의 수집・전파, 2. 침해사고의 예보・경보, 3. 침해사고에 대한 긴급조치, 4. 그 밖에 대통령령으로 정하는 침해사고 대응조치)를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다(제48조의2 제1항). 다음 각 호(1. 주요정보통신서비스 제공자, 2. 집적정보통신시설 사업자, 3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자)의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정

보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하여야 한다(제48조의2 제2항). 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 방송통신위원회에 보고하여야 한다(제48조의2 제3항). 방송통신위원회는 제2항에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다(제48조의2 제4항). 방송통신위원회나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다(제48조의2 제5항). 방송통신위원회나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 제2항 각 호의 어느 하나에 해당하는 자에게 인력지원을 요청할 수 있다(제48조의2 제6항).

(5) 영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등

방송통신위원회는 수신자가 제50조를 위반하여 전송되는 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수 있는 소프트웨어나 컴퓨터프로그램을 개발하여 보급할 수 있다(제50조의6 제1항). 방송통신위원회는 제1항에 따른 전송차단, 신고 소프트웨어 또는 컴퓨터프로그램의 개발과 보급을 촉진하기 위하여 관련 공공기관·법인·단체 등에 필요한 지원을 할 수 있다(제50조의6 제2항). 방송통신위원회는 정보통신서비스 제공자의 전기통신역무가 제50조를 위반하여 발송되는 영리목적의 광고성 정보 전송에 이용되면 수신자 보호를 위하여 기술개발·교육·홍보 등 필요한 조치를 할 것을 정보통신서비스 제공자에게 권고할 수 있다(제50조의6 제3항). 제1항에 따른 개발·보급의 방법과 제2항에 따른 지원에 필요한 사항은 대통령령으로 정한다(제50조의6 제4항).

바. 집적정보통신시설 사업자

집적정보통신시설 사업자는 집적된 정보통신시설의 보호(제46조), 집적정보통신시설 사업자의 긴급대응(제46조의2)의 임무를 수행한다.

(1) 집적된 정보통신시설의 보호

타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설 사업자"라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다(제46조제1항). 집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다(제46조제1항).

(2) 집적정보통신시설 사업자의 긴급대응

집적정보통신시설 사업자는 다음 각 호(1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우, 2. 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우, 3. 중대한 침해사고가 발생하여 방송통신위원회나 한국인터넷진흥원이 요청하는 경우)의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다(제46조의2 제1항). 집적정보통신시설 사업자는 제1항에

따라 해당 서비스의 제공을 중단하는 경우에는 중단사유, 발생일시, 기간 및 내용 등을 구체적으로 밝혀 시설이용자에게 즉시 알려야 한다(제46조의2 제2항). 집적정보통신시설 사업자는 중단사유가 없어지면 즉시 해당 서비스의 제공을 재개하여야 한다(제46조의2 제3항).

사. 안전진단 수행기관

안전진단 수행기관은 정보보호 안전진단(제46조의3)의 임무를 수행한다.

다음 각 호(1. 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다), 2. 집적정보통신시설 사업자, 3. 정보통신서비스 제공자로서 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자)의 어느 하나에 해당하는 자는 방송통신위원회가 안전진단을 수행할 수 있다고 인정한 자(이하 "안전진단 수행기관"이라 한다)로부터 자신의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 받아야 한다. 이 경우 안전진단 수행기관은 15명 이상의 정보보호 기술인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인이어야 한다(제46조의3 제1항). 제1항에 따라 정보보호 안전진단을 받는 사업자는 관련 정보의 제공 및 시설·장소에의 출입 허용 등 안전진단 수행기관의 정보보호 안전진단 업무에 협력하고, 대통령령으로 정하는 바에 따라 정보보호 안전진단의 결과를 방송통신위원회에 제출하여야 한다(제46조의3 제2항). 제1항에 따라 정보보호 안전진단을 받아야 하는 사업자가 「정보통신기반 보호법」 제9조에 따라 취약점의 분석·평가를 받거나 제47조에 따른 정보보호 관리

체계의 인증을 받으면 그 분석·평가를 받거나 인증을 받은 해당 연도에는 제1항에 따른 정보보호 안전진단을 받은 것으로 본다(제46조의3 제3항). 안전진단 수행기관은 제1항에 따른 정보보호 안전진단을 받은 사업자에게 안전진단의 결과에 따라 정보보호조치의 개선을 권고할 수 있다(제46조의3 제4항). 안전진단 수행기관은 제4항에 따라 정보보호조치의 개선을 권고하였으면 그 권고내용 및 처리 결과를 방송통신위원회에 통보하여야 한다(제46조의3 제5항). 방송통신위원회는 제2항에 따라 제출된 정보보호 안전진단의 결과와 제5항에 따른 통보내용에 따라 필요하면 정보보호 안전진단을 받은 사업자에게 정보보호조치에 관한 개선명령을 할 수 있다(제46조의3 제6항). 제1항에 따른 정보보호 안전진단의 방법·절차·수수료, 안전진단 수행기관의 인정절차, 정보보호 기술인력의 자격기준, 정보보호컨설팅 수행실적, 그 밖에 필요한 사항은 대통령령으로 정한다(제46조의3 제7항). 방송통신위원회는 제1항제3호의 요건에 해당하는지를 확인하기 위하여 필요하면 관계 행정기관, 관련 자료 보유기관 또는 정보통신서비스 제공자에 대하여 필요한 자료의 제공 또는 사실의 확인을 요청할 수 있다(제46조의3 제8항).

제4절 소결

국내의 정보보호 법제는 각각 제정목적 및 기능별로 정보보호 추진체계 관련 법령, 국가기밀 보호 관련 법령, 중요정보의 국외유출방지에 관한 법령, 전자서명 및 인증 관련 법령, 정보통신망과 정보시스템의 보호조치 관련 법령, 정보통신망 침해행위의 처벌에 관한 법령 등으로 분류할 수 있다.

이 중 국내 정보보호 추진체계는 국가사이버 안전체계, 전자정부 보호체

계, 정보통신기반 보호체계 및 개인정보 보호체계로 나누어 볼 수 있다.

국가사이버 안전체계와 관련해서는 2005년 1월 대통령 훈령으로 발령된「국가사이버 안전 관리규정」에서 국가사이버안전전략회의, 국가사이버 안전센터 등 사이버 안전 관련조직에 대한 법적 근거, 임무, 관련 기관간 협력사항 등에 관한 사항을 규정하고 있다. 그 외에 정부조직법, 국가안전보장회의법, 국가정보원법, 정보및보안업무기획·조정규정, 경찰법 등이 사이버안전 관련사항을 규율하고 있다. 그리고「국가 사이버 위기 관리법안」도 검토하였다.

전자정부 보호체계와 관련하여서는 2007년 1월 개정된「전자정부법」에서 전자정부의 정보보호를 위해 대민서비스와 관련된 보안대책의 수립•조정 및 제도개선, 보안사고 발생시 대응 조치 등을 심의하기 위한 전자정부서비스보안위원회를 설치하도록 하였다. 행정기관의 장에 대하여는 국가정보원장이 안정성을 보장한 보안조치를 취하도록 하고 국가정보원장은 보안 조치의 이행여부를 확인할 책무를 각각 규정하였다. 그 외에 국가정보화기본법이 전자정부 보호체계 관련사항을 규율하고 있다.

정보통신기반보호체계에 대하여는 2000년 12월에 제정된「정보통신기반보호법」에서 정보통신기반보호위원회, 침해사고대책본부 및 각 중앙행정기관의 역할에 관한 사항을 규정하고 있다. 그 외에 방송통신위원회의 설치 및 운영에 관한 법률, 전기통신기본법 등이 전보통신기반 보호문제를 규율하고 있다.

끝으로, 개인정보 보호체계와 관련된 법령으로는 공공부문에서「공공기관의 개인정보 보호에 관한 법률」,「전자정부법」및「주민등록법」,「전자서명법」등이 있으며, 민간부문에서는「정보통신망 이용촉진 및

정보보호 등에 관한 법률」,「신용정보의 이용 및 보호에 관한 법률」등의 개별법이 존재하고 있다.

앞에서 살펴본 바와 같이 우리나라의 정보보호 추진체계는 국가사이버안전체계의 경우에는 국가정보원, 전자정부 보호체계의 경우에는 행정안전부, 정보통신기반 보호체계의 경우에는 정보통신기반보호위원회, 개인정보 보호체계의 경우에는 공공은 행정안전부장관이, 민간은 행정안전부장관, 지식경제부장관, 방송통신위원회, 민간사업자 등 다양한 기관으로 분산되어 있는 것이 특징이다.

정보보호 추진체계의 정비에 있어서는 현행법상의 분업적 협력시스템을 무시하고 특정부처에 독점한 권한을 부여하는 방식으로 가는 것은 옳지 않다. 그것은 정보보호 수준을 높이기 위해서는 정보보호 법·제도 수립과 문화운동, 기술개발 등을 따로 떼놓고 할 수는 없는 일이며, 분업적 협력시스템을 기본으로 하는 현행 법체계를 무시하고 단순하게 기능을 통합하는 정보보호 추진체계 개편은 타당하지 않기 때문이다.

제5장 결 론

유럽연합은 사이버 공격의 지능화, 다양화로 인해 기존의 기술적 대응만으로는 한계가 있으므로 새로운 유형의 악성코드 및 봇넷, 피싱과 같은 사회공학적 공격의 사전적 예방을 위해 정보보안 인식제고에 지속적인 노력 및 투자를 행하고 있으며 최근 정보보안 인식 실태조사 및 가이드라인 개발 등 활발한 연구를 수행하고 있다.

독일에서는 현재까지도 테러 또는 사이버테러 예방이나 처벌을 위한 특별한 법률을 제정하고 있지는 않으나, 각 개별 형벌법규를 통하여 테러와 사이버테러 방지에 대비하기 위한 규정을 두고 있다. 그리고 정보통신법, 통신서비스법, 연방데이터보호법, 정보통신서비스정보보호법, 전자서명법, 통신법, 형법, 연방정보기술안전청 설치에 관한 법률, 연방의 정보기술의 보안강화를 위한 법률 등 정보보안법제의 정비를 통해 사이버 위기에 적극 대응하고 있다. 그리고 독일에서의 정보기관들의 임무와 권한의 특징은 국내안보에 있어서의 군대의 역할이 배제되어 있고, 국내안보의 주요담당기관으로서의 경찰의 지위확립과 독자적인 헌법보호청이 설치되어 있어 정치경찰이 인정되지 않는다는 데 있다. 향후 테러의 국제화·보편화가 진행됨으로써 연방경찰, 연방헌법보호청, 연방정보기관(BND), 군정보기관(MAD) 등에서의 업무영역을 명확히 구분할 수 없는 경우가 다수 발생할 것에 대비하여 가령 연방헌법보호청의 경우 수집된 정보를 수사기관에 통보하도록 규정(제20조, 제21조)하고 있는 등 독일 내 대테러 유관기관 간 협조체제의 유기적 구축을 통해 미묘한 문제를 해결하고 있다.

일본은 정부가 사이버위기를 대응함에 있어서 법률로서 규율하는 외에 각종 지침과 가이드라인을 통해 사전에 예방할 수 있는 것과 사고발생시의 피해확대를 방지하는 것, 사건에 대한 검토 등을 위해 노력하고 있다. 물론 시간과 공간을 초월하고 그 징후를 알 수 없어 예측하기 어려운 사이버테러의 특성으로 인하여 완벽한 사전예방이라는 것은 쉽지 않은 일이나, 최대한 효과적으로 대응하기 위해서는 정부와 민간 공히 정보보안이 국가정보보안의 중요한 부분[102]이라는 것을 보여주는 시스템을 갖추고 있다. 현재까지 치명적인 사건이 일어난 것은 아니나 향후 정말 심각한 테러가 이루어 질 것을 상정하여, 국가위기 관련법제의 정밀한 검토를 하고 있는 것으로 보인다. 즉, 2004년 이후부터 무력공격사태법과 국민보호법 등의 개별법을 통괄하는 기본법으로서의 역할을 하는 긴급사태법(가칭)의 제정이 주장되고 있다. 그런데 재해대책기본법이나 국민보호법과의 정합성을 이유로 필요하지 않다는 의견이 강력하게 제기됨으로써 아직까지는 법제정이 되지 않고 있다. 이에 덧붙여 궁극적으로는 정보보안 관계법까지 결합하여 정보통신망 상의 위기 곧 사이버테러에 대한 부분까지도 대응하는 것을 고려하고 있다. 또한 하드웨어적인 정보처리장치나 정보통신망에 대한 관리, 기술적인 안전장치 및 하드웨어적인 시스템에 정통하고 사업자간, 사업자 행정부서간 보안대책을 연계할 수 있는 인재육성 및 사용자의 보안의식을 강화하는 데에도 노력을 기울이고 있다.[103]

미국의 경우 관련기관 간 기능에 따른 권한과 책임을 분산하고, 이러한 기관들의 수평적 협업을 통하여 사이버위기관리에 대응하고 있다. 대통령 직속의 관리예산처가 전자정부에 대한 책임을 맡고 있으며, 공공부문의

---

102) 허태회 외, “세계 주요 강대국들의 정보전 준비와 대응체계”, 35면
103) 김재광・김정임, 앞의 논문, 59-60면 참조

정보보안에 있어서도 원칙적으로 관리예산처가 추진체계의 중심에 있다고 있다. 그렇지만 국가안보시스템의 경우 국토안보부와 국방부 등을 중심으로 추진체계를 정비하였다. 이는 사이버공간에서 공공분야와 민간분야를 포괄하는 사이버위기관리는 국가안전보장과 직결된다는 인식하에서 국토안보부가 이에 관한 업무를 수행한다. 정보보안 관련법제도 이를 제도적으로 뒷받침하기 위해 지속적으로 정비되고 있다.

우리나라의 정보보호 추진체계는 국가사이버 안전체계의 경우에는 국가정보원, 전자정부 보호체계의 경우에는 행정안전부, 정보통신기반 보호체계의 경우에는 정보통신기반보호위원회, 개인정보 보호체계의 경우에는 공공은 행정안전부장관이, 민간은 행정안전부장관, 지식경제부장관, 방송통신위원회, 민간사업자 등 다양한 기관으로 분산되어 있는 것이 특징이다.

정보보호 추진체계의 정비에 있어서는 현행법상의 분업적 협력시스템을 무시하고 특정부처에 독점한 권한을 부여하는 방식으로 가는 것은 옳지 않다. 그것은 정보보호 수준을 높이기 위해서는 정보보호 법·제도 수립과 문화운동, 기술개발 등을 따로 떼놓고 할 수는 없는 일이며, 분업적 협력시스템을 기본으로 하는 현행 법체계를 무시하고 단순하게 기능을 통합하는 정보보호 추진체계 개편은 타당하지 않기 때문이다.

지금까지 알려진 정부방침은 외국사례들의 경우처럼 사이버테러와 관련한 정부부처간·정보기관간 분업과 협력의 유기적 조정을 통해 문제해결을 하겠다는 의지의 표명인지 여부가 분명하지 않지만 향후 테러의 국제화·보편화가 진행됨으로써 각 정보기관간 업무영역을 명확히 구분할 수 없는 경우가 다수 발생할 것에 대비하여 정보보호 추진체계간 협조체

제의 유기적 구축을 통해 신속한 문제해결을 도모하는데 한층 더 노력을 경주하여야 할 것이다. 다시 말해서 정보보호 추진체계의 정비가 컨트롤 타워의 '권력화'에 초점이 맞춰져서 민간사찰, 과잉수사 등 인권 침해 시비로 인한 소모적 논쟁을 피하여야 할 것이며(정치경찰의 방지), 정보보호라는 본래적이고 순수한 취지에 입각하여 정비되어져야 할 것이다. 다만, 2009년 7월 7일에 발생한 인터넷상의 DDoS 사태는 사이버 위험이 현실화됨으로써 사회에 미칠 수 있는 파국적 영향력과 금융거래 중단 등으로 이어지는 네트워크 도미노 현상을 보여줌으로써 '7.7사이버테러'라 불릴만큼 충격을 안겨주었는데, 최근에 국정원의 국회보고에 의하면 이러한 소행이 북한 체신청으로 드러난 점은 향후 정보보호 법제개선에 있어 일정한 방향성을 시사한다고 볼 수 있으나, 정부부처간·정보기관간 분업을 통한 협력의 유기적 조정을 통해 문제해결을 한다는 정보보호 추진체계 관련법제의 기본적인 정신은 지켜져야 할 것이다.

<참고문헌>

국내 문헌

김민호, “주민등록번호체계의 개편과 본인확인제도”「정보사회 신분확인 제도의 법적 쟁점」, 미래정보사회 입법정책포럼자료집, 2009. 10. 16

김민호・김현정, 전자정부와 법률유보, 「토지공법연구」제37집, 2007

김성태,「전자정부론」, 법문사, 2004

김일환, “정보화촉진기본법에 관한 토론문”「정보화촉진기본법, 전자정부법, 정보통신기반보호법 개정 공청회」, 2008. 9. 5

김일환, “전자정부와 개인정보보호”「민주, 법치국가의 발전과 사회통합」, 2008. 6. 28 한국공법학회 세미나 자료

김일환,「개인정보보호법제의 정비방안에 연구」,한국법제연구원, 1997

김일환, “독일 기본법상 대테러관련기관과 법제도들에 관한 고찰”「성균관법학」제15권제1호(2003)

김재광, “전자정부 관련법제의 개선방안”「선진국가정보화법 체계모색」-전자정부와 정보보호, 한국인터넷법학회 세미나, 2008. 5. 9

김재광, “온라인행정서비스의 역기능방지 관련법제의 문제점과 개선방안” 「인터넷법률」제33호, 2006.1, 법무부

김재광, “미국의 전자정부법에 관한 고찰”「전자정부법제연구」제1집, 2006. 6, 행정자치부

김재광, “영미법계 국가의 개인정보보호법제 동향 및 함의”「공법학연구」제6권 제1호, 한국비교공법학회, 2005

김재광・김정임, “일본의 사이버위기 관련 법제의 현황과 전망”「법학논총」제33권제1호(2009. 6, 단국대 법학연구소)

김종철, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론” 「인터넷법률」제4호, 법무부, 2001. 1

이규정・구병문,「미국 전자정부법 분석 및 시사점」, 한국전산원, 2003
이창범 외,「미국, 독일, 일본의 정보보호법 체계에 관한 연구」, 한국정보보호진흥원, 2006. 12
정완용, “행정전자서명에 관한 법적 고찰”「경희법학」제39권제3호, 2005. 2
지성우, “독일의 사이버위기 관련 법제의 현황과 전망”「사이버위기관련 법제의 현황과 전망」, 단국대 법학연구소, 2009. 5. 29
황병천・ 이자성・김재광 외,「지역정보화 관련 법제화 연구」, 자치정보화조합, 2006. 7
홍준형, “유비쿼터스 환경에서의 개인정보 보호”「공법연구」제32집 제5호
한국전산원,「국외 개인정보보호법제 분석 및 시사점」, 2004
Lawrence Lessig,「Code and Other Laws of Cyberspace」, Basic Books, 1999
양근원, “사이버테러 대응과 현행 절차법 검토”, 「인터넷법연구」제3권 제1호, 2004
양지연, “미국의 정보통신망 정부규제 및 자율규제 현황”「정보통신망 안전성 및 신뢰성 확보방안」, 2009. 8. 10
이영준 외,「사이버범죄방지조약에 관한 연구」, 한국형사정책연구원, 2001. 12
이종환,「사이버상에서의 정보보호를 위한 정부역할 연구 - 민간부문을 중심으로」중앙대 박사학위논문, 2006
정회근, 전자적 침해행위로 인한 주요정보통신 기반시설의 법적보호에 관한 연구, 단국대학교 박사학위논문, 2002
최철호, “독일의 정보통신망 정부규제 및 자율규제 현황”「정보통신망 안전성 및 신뢰성 확보방안」, 2009. 8. 10
하옥현,「국가사이버안보체계 구축전략」, 고려대 박사학위논문, 2005
허태회 외, “세계 주요 강대국들의 정보전 준비와 대응체계”「국방연구」제49권 제1호, 2006년

현대호, “미국의 사이버위기 관련 법제의 현황과 전망”「법학논총」제33권제1호, 단국대 법학연구소, 2009. 6
국가정보원・방송통신위원회・행정안전부・지식경제부, 2009 국가정보보호백서
한국정보보호진흥원, 2009 June 인터넷 침해사고 동향 및 분석 월보

국외 문헌

大泉 雅昭, “警察のサイバーテロ對策”「電氣通信」68(通卷697), 2005
內 律子, “情報セキュティの現狀と課題”「立法と調査」第443號, 國立國會圖書館, 2004
2009/05/08 産経新聞
총무성 http://www.soumu.go.jp/menu_seisaku/ict/u-japan/index.html
총무성 부정액세스 행위 발생상황 2008http://www.soumu.go.jp/menu_news/s-news/090226_3.html
http://www.nisc.go.jp/index.html
http://www.nisc.go.jp/conference/seisaku/index.html
http://www.cyberpolice.go.jp/cyberforce/cyberforce03_01.html
https://www.ccc.go.jp
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm
http://www.ipa.go.jp/
俊也＝日経SYSTEMS）[2007/11/15], http://itpro.nikkeibp.co.jp/article/NEWS/20071115/287263/

국가 정보보호 추진체계 관련법제 분석

2009년 12월 인쇄
2009년 12월 발행

발행인 : 김 성 태
발행처 : 한국정보화진흥원
서울시 중구 무교동 77번지
전화 : (02) 2131-0114
인쇄처 : 호정씨앤피
전 화 : (02) 2277-4718

<비매품>

· 본 보고서의 내용은 한국정보화진흥원의 공식 견해와 다를 수 있습니다.
· 본 보고서 내용에 대해 무단전재(無斷轉載)를 금하며, 가공·인용할 때에는 반드시 「한국정보화진흥원」이라고 출처를 밝혀 주시기 바랍니다.