콘텐츠산업법제지원사업(Ⅲ)

정보보안 관련법제의 문제점과 개선방안

- The Problem and Improvement of Information Security Law -

연구책임자 : 현대호 부연구위원
Hyeon, Dae-Ho

2007. 9.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

국 문 요 약

현행 정보보안 관련법제의 문제점을 분석하고, 그 개선방안을 도출하여 보았으며, 이를 요약 정리하면 다음과 같다.

첫째, 정보보호와 정보보안을 구별하였으며, 정보보안은 정보의 무결성, 비밀성 및 이용가능성을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것으로 파악하였다.

둘째, 미국의 정보보안에 관한 연방정보보안법을 중심으로 우리 나라 현행법제의 개선방안을 고찰하였다.

셋째, 인터넷 등을 통하여 정보시스템이 상호 연계되어 있어서 정보보안은 공공분야만의 문제가 아니라 민간분야에서도 직면하는 공통된 문제에 해당된다. 따라서 범정부차원에서 대응할 수 있는 통일된 집행체계를 마련하는 것이 중요하며 그 개선방안을 제시하였다.

넷째 , '(가칭)정보보안관리법'의 제정 필요성과 그 구체적인 법제화 방안에 대한 기본적인 틀을 제안하였다.

※ 검색어 : 정보보안, 정보보호, 정보시스템, 사이버, 해킹, 개인정보

Abstract

This paper analyzes problems current information security law, and deduces alternative proposals which are described below.

First, This paper separated information protection and information security. ‘Information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, availability.

Second, I inquire into information security law of United State, and deduce improvements of current information security law.

Third, because Information Systems are connected through the internet, Information Security is a common problem of governmental and civilian spheres. Therefore a single executive system is needed. This paper proposes a new single executive system.

Fourth, I propose a new bill which is given a name as ‘The Information Security Management Act’ in this paper

※ Key Word : Information Security, Information Protection, Information System, Cyberspace, Hacking, Personal Data

목 차

제 1 장 서 론

1. 연구의 목적

종래 오프라인에서 종이문서의 보안은 해당기관을 벗어나 이용・제공되는 경우가 드물고 이용・제공된다고 하여도 유형물이어서 독립된 입법의 필요성이 낮아 내부적인 업무규정(업무지침) 등으로 대응할 수 있었다.[1] 그렇지만 종이문서에 의한 업무가 전산화되어 디지털화된 정보(이하 '정보'[2]라 한다)가 정보시스템과 정보통신망을 통해 처리, 이용되는 환경에서 정보보안은 정보화 이전의 정보보안과는 질적인 측면에서 변모하였다. 즉 새로운 정보환경에서는 물리적 보안만으로는 그 목적을 달성할 수 없으며, 기술적 보안과 관리적 보안 등 다각적인 대응이 요구된다.[3]

2006년 현재 UN 전자정부준비지수 세계 제5위[4], 미국 브라운대학 전자정부평가 세계 제1위, IDC 정보사회지수 세계 제10위, 국제전기통신연합(ITU; International Telecommunication Union) 디지털기회지수(DOI) 세계 제1위로 상징되는 정보통신 선진국인 우리나라는 일찍이 이러한 정보통신영역에서 정보보안의 중요성을 깨닫고, 국가적 차원에서 정

1) 형법은 제20장에서 문서의 관한 죄를 규정하고 있는데(제225조 내지 제237조의2), 문서의 위조・변작에 대한 처벌규정과 전자문서의 대한 처벌규정을 두고 있으며, 비밀문서를 무단으로 개봉한 자에 대하여 제316조에서 비밀침해죄로 처벌하고 있다.

2) 정보라는 용어는 다양한 방면에서 너무나 광범위하게 사용되고 있어서 정확한 개념 정의를 한다는 것은 불가능하다. 그렇지만 정보라는 용어가 일반적으로 해당 영역에서 어떠한 의미로 사용되고 있는가에 대한 정의는 필요하다. 여기서는 정보라는 용어를 저작권법으로 보호되지 아니하는 사실과 사고(idea)에 한정하지 아니하고 정보시스템으로 처리되는 모든 내용물을 포함하는 넓은 개념으로 사용한다.

3) 정보보안의 중요성에 관해서는 Parker, Donn B., Computer Security Management, Reston Publishing Co. Inc., 1981, pp.7-13; 김일환, 情報保安關聯法制整備의 基準과 內容에 관한 硏究, 土地公法硏究(제26집), 韓國土地公法學會, 2005, 234-235쪽 참고.

4) UN, *Global e-Government Readiness Report 2005*.

책을 마련하고 이러한 정책을 뒷받침하기 위한 각종 입법을 추진하였다. 그러나 현행 정보보안 관련법제에 관해서는 사용자가 컴퓨터나 네트워크를 의식하지 않고 언제 어디서나 자유롭게 네트워크에 접속할 수 있는 정보통신기술을 의미하는 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경에 적합하지 않고, 지나치게 많은 법률에 관련 규정이 산재하여 복잡하고 산만하며, 민간영역과 공공영역을 나누고 공공영역도 다시 관할영역을 나누어 여러 기관이 분산하여 업무를 수행하면서도 이를 전체적으로 조정할 수 있는 권한있는 기관이 없어 통일적·체계적으로 대응을 하고 있지 못하다는 등 여러 문제점이 나타나고 있다.

따라서 이 연구에서는 정보사회에 진입에 필수적인 정보보안의 필요성과 새로운 입법의 필요성을 살펴보고, 아울러 정보보안에 관련된 현행 법체계의 문제점과 개선방안을 고찰하고자 한다.

2. 연구의 범위

연구의 범위는 우선적으로 정보보안을 정의하고 그 특징과 정보보안을 위협하는 침해요소에 관해 살펴보고, 현행 정보보안 관련법제를 개관하고자 한다(제2장). 그리고 국제적 보안관리기준을 제시한 OECD 지침과 정보보안 선진국인 미국 정보보안 관련법제의 현황과 내용을 살펴보며, 우리에게 주는 시사점을 도출하고자 한다(제3장). 이어서 제4장에서는 현행 정보보안 관련법제의 문제점을 분석하고 개선방안을 살펴보고, 제5장에서는 새로운 정보보안 관련법제를 구상하여 제시하고자 한다. 마지막으로 위의 논의를 정리하고 결론을 제시한다(제6장).

제 2 장 정보보안의 의의 및 현행 법제의 개관

제 1 절 정보보안의 의의

1. 정보보안의 개념

정보보안(information security)이란 정보의 무결성(integrity), 비밀성(confidentiality) 및 이용가능성(availability)을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다.[5)]

무결성이란, 저장, 소통되는 정보가 비인가자에 의해 무단 변경되지 않도록 정확성, 안전성이 보장되어야 한다는 원칙이다. 즉 정보는 의도적이든, 우발적이든 간에 허가 없이 변경되어서는 안된다. 비밀성이란 정보시스템에 의해 처리, 저장, 소통되는 정보가 비인가자에게 유출되지 않도록 하는 것과 유출되더라도 그 정보를 확인할 수 없도록

---

5) 미국 연방정보보안관리법(Federal Information Security Management Act of 2002) 제3542조 참조.

"Sec. 3542. Definitions

"(a) In General.--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) Additional Definitions.--As used in this subchapter:

"(1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-

"(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

"(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

"(C) availability, which means ensuring timely and reliable access to and use of information.

정보보안의 다양한 정의에 관해서는 Parker, Donn B., Computer Security Management, Reston Publishing Co. Inc., 1981, 39쪽 이하 참고.

하는 것이다. 기밀자료는 인가된 자에 의해서만 접근이 가능해야 하며 기밀성을 보장하기 위한 매커니즘에는 접근통제와 암호화 등이 있다. 이용가능성은 인가자가 필요할 때 언제든지 정보시스템을 사용할 수 있도록 정상상태로 유지하는 것이며 정당한 방법으로 권한이 주어진 사용자에게 정보서비스를 거부하여서는 안 된다는 것이다.[6)]

2. 정보보안과 정보보호의 구별

우리 실무계에서는 정보보호(information protection)라는 용어를 사용하며, 개인정보보호(personal data protection)와 정보보안(information security)을 포괄하여 사용하는 것이 일반적이며, '정보통신망 이용촉진 및 정보보호에 관한 법률', '정보통신기반보호법'과 같은 실정법에서도 정보보안이라는 용어대신 정보보호라는 용어로 정보보안을 가리키고 있다.

그러나 정보보호라는 말로 개인정보보호와 정보보안을 포괄하여 논하는 것은 바람직하지 않다. 왜냐하면 개인정보보호와 정보보안은 구분되며, 적용되는 기술이나 법리가 다른, 상대적으로 별개의 영역을 차지하는 개념이기 때문이다. 따라서 정보보호를 정보보안을 가리키는 용어로 사용하는 것은 바람직하지 않다.

정보시스템의 발달은 정보의 수집・이용・공개 및 저장하는 능력을 급격히 개선하여 왔고, 정보시스템에 의존하는 작업방식은 인터넷을 통하여 무수히 많은 다른 정보시스템과 상호 연결되어 있다. 이와 같은 환경의 변화에 따라 정보가 가지는 재산적 가치와 인격적 가치도 급격히 상승하는 변화가 나타났다. 정보보호는 통상 개인정보의 보호[7)] 또는 영업비밀에 대한 보호라는 문제로 귀결되고, 관련법률도 개

6) 마크 스탬프 저, 안태남, 손용락, 이광석 공역, □□정보보안 이론과 실제□□, 한빛미디어, 2006, 24쪽 참고; 한국정보보호진흥원, 정보보호 개론, 2000. 4~6쪽.

7) 개인정보의 보호는 종래 주로 형사법과 민사법에서 다른 법익의 보호에 부수하여 제한적으로만 보호되었다. 형법은 명예훼손죄(제307조～제312조)・비밀침해죄(제316조～제318조)・주거침해죄(제319조～제322조) 등을 통하여 인격의 왜곡이나 개인의

인정보의 보호에 관한 법률(정보통신망법, 공공기관개인정보보호법, 신용정보보호법 등)과 영업비밀의 보호에 관한 법률(부정경쟁방지법 및 산업기술의 유출방지 및 보호에 관한 법률 등)로 구별되어 발달하고 있다.

이와 같이 정보가 가지는 보호가치(법익)에 따른 정보자체의 보호법리와 여기서 다루고자 하는 정보보안(information security)은 구별된다. 정보보안은 미국의 경우도 개인정보의 보호나 영업비밀의 보호와 분리되어 독립된 입법('2002년 미국의 연방정보보안관리법')이 이루어졌으며 공공분야에서 연방정부 차원의 정보보안에 대한 효과적인 통제를 위한 총체적인 틀을 마련하는 것을 의도하였는데, 공공분야의 정보보안 관리체계가 중심을 차지하고 있다. 우리 나라의 경우에는 정보통신부와 국가정보원을 중심으로 한 민간분야와 공공분야의 정보보안에 대한 대응시책 등이 마련되어 정보보안의 중요성이 강조되어 왔

사적인 영역을 보호하였다. 이들 법익에 부수하여 개인정보는 보호되었고 그 자체만을 독립된 보호 대상으로 다루지는 않았다. 즉 형법 제319조제1항에서 『사람의 주거, 관리하는 건조물, 선박이나 항공기 또는 점유하는 방실(房室)에 침입한 자는 3년이하의 징역 또는 500만원이하의 벌금에 처한다』라고 하여 주거 등에 대한 물리적 침해를, 그리고 형법 제320조에서 『사람의 신체, 주거, 관리하는 건조물, 자동차, 선박이나 항공기 또는 점유하는 방실을 수색한 자는 3년이하의 징역에 처한다』라고 하여 신체 등의 물리적 수색으로부터의 자유를 보호하고 있다. 형법 제317조 제1항에서 『의사, 한의사, 치과의사, 약제사, 약종상, 조산사, 변호사, 변리사, 공인회계사, 공증인, 대서업자나 그 직무상 보조자 또는 차등(此等)의 직에 있던 자가 그 업무처리중 지득한 타인의 비밀을 누설한 때에는 3년이하의 징역이나 금고, 10년이하의 자격정지 또는 700만원이하의 벌금에 처한다』라고 하여 일정한 직업에 종사하는 자에게 업무상 취득한 개인정보를 타인에게 공개하는 것을 금지하고 있다. 개인정보에 대한 민사법의 보호도 다른 법익에 부수하여 보호하는 것으로 다루었고 독립된 법익으로 보지 않았다. 즉 인격적 이익에 대한 불법행위도 전통적으로 생명·신체 및 자유에 대한 물리적 침해에 중심을 두고 있었고 점차적으로 개인의 명예라는 사회적 평가에도 그 보호를 허용하였다. 20세기 초에는 '사생활의 비밀'과 '인격의 부당한 이용 또는 왜곡'에 관련한 개인의 감정을 보호하는 프라이버시권이 나타났고, 개인의 순수한 감정만을 침해한 경우 소위 '감정침해'라는 새로운 불법행위의 유형이 제기되고 있다. 최근에는 정보주체에게 자신의 정보에 대한 일정한 참여권을 행사할 수 있도록 새로운 '정보프라이버시(information privacy)' 또는 '개인정보자기결정권'을 도입하고 있다.

지만, 이원화 된 정보보안관리와 집행체계가 마련되어 왔고(민간분야는 정보통신부, 공공분야는 국가정보원) 최근에는 행정자치부가 전자정부사업을 총괄하면서 공공분야의 정보보안관리에 대한 역할이 강조되고 있다.

3. 정보보안의 분류

정보보안에 관한 분류는 다양하다. 여기서는 정보보안을 물리적 보안, 기술적 보안, 관리적 보안으로 분류하여 살펴보고자 한다.[8)]

먼저 물리적 보안은 건물과 같이 정보시스템을 설치하는 환경에 대한 침해에 대비하여 물리적 수단으로 보호하는 것을 말한다. 예를 들어 지진 또는 방화, 폭격, 물리적 침입 등에 대비하여 건물에 방진·방재설비를 갖추거나 지하에 설치하고 특수벽을 설치하는 것, 정해진 사람 이외의 출입을 통제하기 위한 제어시스템을 설치하는 것 등이 그 예이다.

기술적 보안이란 하드웨어나 소프트웨어와 같이 정보시스템을 통한 침해에 대비하여 기술적 수단으로 보호하는 것을 말한다. 예를 들어 암호화, 정보시스템의 백업체제 구축, 기술적 보호조치를 하는 것 등이 그 예이다.

관리적 보안이란 정보보안에 대비하여 인력, 조직, 경비를 확보하고 계획을 수립하는 것 등을 말한다.[9)] 정보보안을 효율적으로 추진하기 위한 추진체계, 사전적·사후적 절차, 정보보안 인력·조직·예산의 배정과 집행, 관리, 정보시스템운용 인력·조직의 관리 등이 그 예이다.

---

8) 필자와 동일한 분류로는 홍승필·고제욱, 정보보안 기술과 구현, 파워북, 1998, 18-21쪽. 김일환, 앞의 글, 237-238쪽,은 정보보안을 물리적 보안, 시스템 보안, 관리보안, 인적 보안으로 분류하고 있다. 시스템 보안은 필자가 사용하는 기술적 보안에 대응하는 것으로 판단된다. 관리적 보안과 인적 보안을 다르게 분류한 것에는 동의할 수 없다. 인적 보안은 관리적 보안의 하나의 항목으로 파악되어야 한다.

9) 홍승필, 유비쿼터스 컴퓨팅 보안, 한티미디어, 2006, 198쪽 참고.

4. 정보통신의 위협요소

정보보안의 종류에 대응하여 정보통신에 대한 위협을 분류하여 보면, 폭격과 같은 물리적 위협, 해킹, 바이러스 유포와 같은 기술적 위협, 추진체계의 혼란, 정보시스템 운용자의 사고와 같은 관리적 위협 등으로 분류할 수 있다. 전통적으로 이러한 정보통신에 대한 위협요소를 사이버테러, 컴퓨터범죄, 사이버범죄 등의 용어로 지칭하였다. 그러나 모든 정보통신에 대한 위협요소가 사이버테러 또는 컴퓨터범죄, 사이버범죄는 아니므로, 정보보안과 관련하여서는 정보통신에 대한 위협요소라는 용어를 사용하는 것이 타당하다고 생각한다.[10]

해킹이란 '컴퓨터를 이용하여 다른 사람의 정보처리장치 또는 정보처리시스템에 침입하여 그 정보처리장치가 수행하는 기능이나 전자기록에 부당하게 간섭하는 일체의 행위'를 말한다.[11] 이러한 해킹은 정보시스템의 취약점을 이용하여 불법적으로 접근한 후 자료의 유출, 위·변조 및 삭제, 시스템 장애 및 마비를 일으키기 때문에 정보통신에 대한 위협요소로 간주된다.

해킹은 초기에는 개인적인 호기심과 암호를 해독하는 경쟁심에서 시작되어 범죄로 간주되지 않았다. 그러나 최근 해킹은 단순히 비밀번호를 찾는 것에 멈추지 않고, 상대방의 컴퓨터에 저장된 중요한 데이터를 탐색하거나, 컴퓨터이용을 방해하는 것을 목적으로 해킹을 수단으로 하여 상대방의 컴퓨터에 침입하고 있다. 이에 따라 컴퓨터 정보보호의 필요성에 따라 해킹을 차단하려는 움직임으로부터 해킹을

---

10) Parker, Donn B., Computer Security Management, Reston Publishing Co. Inc., 1981, pp.43-44, pp.125-140. '정보통신망 이용촉진 및 정보보호에 관한 법률'에서는 '해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태'(법 제2조 제7호)라고 지칭하고 있다.

11) 강동범, 사이버범죄와 형사법적 대책, 형사정책연구 제11권 제2호, 78-79면.

범죄로 취급하기 시작하였다.

바이러스 유포는 프로그램 스스로 복제하여 다른 시스템에 자동 설치되어 시스템의 정상적인 작동을 방해하고 이상작동을 하도록 하거나, 특정날짜나 시간이 되면 프로그램이 스스로 작동하여 컴퓨터의 정보를 삭제하거나 시스템의 정상적인 작동을 방해하는 악성프로그램을 유포하는 것을 말한다. 컴퓨터사용자에게 막대한 피해를 일으킨 바이러스의 수는 헤아릴 수 없을 정도로 많으나, 대표적인 예로서는 1999년 초에 출현한 해피바이러스를 비롯하여 멜리사, Win95CIH, 러브레터, 코드레드, 오파서브, 펀러브, 클레즈, 해피타임 등이 있다.

이러한 해킹, 바이러스 유포 등을 일컫는 사이버테러는 국제안보협력센터(Center for International Security and Cooperation)에서 입안한 '사이버범죄와 테러리즘에 대한 국제조약 안(Proposal for an International Convention on Cyber Crime and Terrorism)에 규정되어 있는데, 이에 따르면 "법적으로 승인된 권한 없이 사이버시스템에 대하여 폭력, 파괴 또는 방해를 고의적으로 사용하거나 사용하겠다고 위협하는 행위를 말하며, 그러한 사용은 사람이나 사람들의 사망이나 상해, 실제적인 재산에 대한 실질적 피해, 사회적인 혼란 또는 중대한 경제적 피해를 가져오는 경우가 있을 수 있다"[12]고 규정하고 있다.

스팸메일(Spam mail)이란, 이용자가 원치 않는 정보를 불필요하게 반복적으로 전송하는 메일을 말한다. 정크 메일(Junk mail) 또는 벌크 메일(Bulk mail)이라고 하며, 원하지 않는 상업적 이메일(UCE, Unsolicited Commercial E-mail)이라고도 부른다. 이러한 스팸메일은 기존 현실세계에서의 광고전단지와 비슷한 기능을 하는데, 전자우편(e-mail)을 통해서 특정 상품을 광고하거나, 자신의 홈페이지 사이트를 홍보하기

12) Cyber terrorism means intentional use or thret of use, without legally recognized authority, of violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of a person or person, substantial damage to physical property, civil disorder, or significant economic harm.

위함이다. 스팸 메일은 그 비윤리성과 불법성 때문에 일반 상업용 광고 메일과 확실하게 구분된다. 일반 상업용 광고 메일은 사전에 메일 수신 서비스를 신청한 사람들을 대상으로 발송되는 메일로서, 수신자는 해당 메일 수신에 대해 어느 정도 예상을 하고 있을 뿐만 아니라, 수신자의 요청에 따라 언제든지 메일 수신이 중단될 수도 있는 계약적 성격을 갖는다. 반면에 스팸 메일은 수신자의 의사는 완전히 무시한 채 무차별적으로 발송되는 광고성 메일(전자게시물 포함)을 가리킨다. 더 나아가 폭탄메일을 통한 스팸메일은 정보시스템에 과부하를 주어 시스템을 마비시키기도 한다. 이것은 정보통신망의 안정적 운영을 방해하는 행위라고 할 수 있다.

제 2 절 현행 정보보안 관련법제의 개관

1. 개 요

정보보안 관련법제를 개관하기 위해서는 우선 정보보안 관련법제를 확정하는 작업이 선행되어야 한다. 우리나라에서는 아직 어느 범위까지 정보보안 관련법제로 볼 것인지에 관한 일반적 합의가 존재한다고 보기 어렵기 때문이다. 이렇게 정보보안 관련법제를 확정하기 위해서는 '정보보안'이라는 개념을 확정하여야 한다.

이미 설명한 것처럼 정보보안(information security)이란 정보의 무결성(integrity), 비밀성(confidentiality) 및 이용가능성(availability)을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다.[13]

따라서 정보보안에는 개인정보보호와 영업비밀보호와 같은 정보의 내용의 보호는 제외되는 것이 타당하다. 그러나 사람의 신원과 문서의 변

13) 미국 연방정보보안관리법(Federal Information Security Management Act of 2002) 제3542조 참조.

경 여부를 확인할 수 있도록 암호화 방식을 이용하여 인정하고 증명하는 것을 말하는 전자인증(Electronic Authentication)은 그것이 곧 정보보안을 위한 것만은 아니지만, 정보보안의 범위의 하나인 접근제어의 핵심이므로, 정보보안의 범주 안에서 다루어주는 것이 타당하다.[14] 그리고 정보보안은 이미 서술한 것처럼 물리적 보안, 기술적 보안, 관리적 보안을 내포하고 있다고 할 수 있다.

이렇게 보았을 때, 정보보안 관련법제에는 일련의 개인정보보호법과 영업비밀보호법이 포함되지 않는다. 그러나 인증을 규율하고 있는 '전자서명법'과 '전자정부법'은 포함된다. 그리고 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호에 관한 법률」, 「전기통신사업법」, 「정보화촉진기본법」, 「전파법」 등과 같은 정보통신부 소관법률과, 「국가정보원법」, 「국가사이버안전관리규정」, 「정보 및 보안업무 기획조정규정」과 같은 국가정보원의 담당법령, 「전자정부법」과 같은 행정자치부 소관법률, '형법'과 같은 법무부 소관법률 등이 포함될 것이다.

2. 정보화촉진기본법

정보화촉진기본법 제5조 제1항 제7호에서는 정보화촉진기본계획의 한 내용으로 각 분야별 정보보안에 관한 사항이 포함되어야 한다고 명시하고, 제14조 제1항에서는 "정부는 정보의 안전한 유통을 위하여 정보보호에 필요한 시책을 강구하여야 한다"고 규정하고, 제2항에서는 "정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구하여야 한다"고 규정하고 있다. 나아가 제15조[15]에서는 정보통신부장관이 정보보호시

14) 이에 관해서는 마크 스탬프 저, 앞의 책, 27쪽 참조; 인증의 필요성에 관해서는 이만영 외 공저, 인터넷 정보보안, 생능출판사, 2002, 17쪽 이하 참조.

15) 제15조 (정보보호시스템에 관한 기준고시등) ①정보통신부장관은 관계기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 정보보호시스템을 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고할 수 있다.

스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 이를 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고할 수 있다는 세부적인 내용도 규정하고 있다.

3. 형 법

형법에서는 보안과 관련된 조항으로, 1995년 개정으로 컴퓨터자료의 부정조작, 컴퓨터 파괴, 컴퓨터 비밀침해 행위와 컴퓨터 등 사용사기죄를 신설하였으며, 2001년 개정에서는 컴퓨터의 권한 없는 사용, 즉 타인의 신용카드를 이용하여 현금을 무단 인출하는 행위와 같이 진실한 자료를 부정하게 사용한 행위를 처벌하도록 추가하여 정하고 있다.

그 중 컴퓨터 바이러스와 관련해서는 형법 제314조 제2항의 업무방해죄를 들 수 있겠다. 동 조항은 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 사람은 5년 이하의 징역 또는 1,500만원 이하의 벌금에 처하도록 되어 있다. 그러나 이 조항에 의할 경우 컴퓨터 바이러스를 만든 것만으로는 충분하지 않고 적어도 업무용 컴퓨터 등 정보처리장치에 장애를 발생케 하여야 한다. 따라서 바이러스를 제작, 유포한 행위 자체는 현행 형법상으로는 규율의 대상이 되지 않으며, 정보통신망법에 의하여는 처벌할 수 있다.

해킹과 관련한 형법규정으로는 비밀침해죄 및 컴퓨터등사용사기죄의 성립여부가 문제될 수 있다. 형법 제316조 제2항에서는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자는 3년 이하의 징역 또는 500만원 이하의 벌금에 처한다고 규정하고 있

---

②정보통신부장관은 유통중인 정보보호시스템이 제1항의 규정에 의한 기준에 미치지 못할 경우에 정보보호시스템의 보완 기타 필요한 사항을 권고할 수 있다.

③제1항의 규정에 의한 기준고시와 제2항의 규정에 의한 권고 기타 필요한 사항은 대통령령으로 정한다.

다. 그러나 본 조문에서 전자기록의 의미는 데이터가 일정한 저장매체에 기록되어 있는 상태를 의미하므로 전송중인 데이터에 대하여는 대처할 수 없고, 일한 전송중인 데이터의 침해 역시 형법이 아니라 정보통신망법에 의해 규율될 수 있겠다.

한편 제347조의2에서는 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력 변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다고 규정하고 있다. 이 조문은 2001년 형법 개정으로 권한 없이 컴퓨터 시스템에 접근하는 행위에 대하여 대처할 수 있도록 하고 있다. 원래는 현금인출기에서 현금카드나 신용카드를 이용하여 현금을 인출하거나 계좌이체 시키는 행위에 대처하기 위한 것이었으나, 전자상거래에 있어서 비밀번호를 입력하는 행위뿐만 아니라 넓게 해킹 등을 통하여 권한 없이 컴퓨터 네트워크에 침입하는 행위도 포섭할 수 있게 되었다. 그러나 본 조문 자체가 이러한 무권한 접속으로 인하여 재산상 이득을 취득하여야 하기 때문에 재산상 취득 없는 단순한 해킹에 대하여는 여전히 형법상 처벌의 대상이 되지 않는다.

이러한 의미에서 정보보안에 대처할 수 있는 형법 적용의 범위는 정보통신의 현실에 비추어 보면 상당히 제한적이라고 할 수 밖에 없다.

4. 정보통신망 이용촉진 및 정보보호에 관한 법률

‘정보통신망 이용촉진 및 정보보호에 관한 법률(이하 ’정보통신망법‘으로 줄인다)’은 그 명칭에서 알 수 있듯이 정보통신망이용촉진과 개인정보보호라는 2개의 상이한 내용을 담고 있고, 이외에도 제3장에서 ‘전자문서중계자를 통한 전자문서의 활용’이라고 하여 전자문서에 관한 사항을 두고 있으며, 더 나아가서 제5장에서 ‘정보통신망에서의 청소년보호 등’이라고 하여 청소년보호에 관한 사항을 두고 있다.

이와 같이 상호 상이한 내용을 하나의 입법에서 규율하는 입법형식은 정보통신기술의 도입 초기에 적합한 형태이고 정보통신기술의 발달과 활용이 넓혀지고 규율하는 입법사항이 보다 복잡하고 다양화됨에 따라 분법화가 요구된다. 다시 말해서 현행 정보통신망법은 우리나라가 고도화되고 선진화된 정보사회로 진입함에 따라 분법화가 필요하다.

법의 주요내용은 다음과 같다. 해킹과 관련하여 정보통신망법에서는 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침하여서는 안 된다고 규정하고 있으며(동법 제48조 제1항), 이러한 행위를 한 자는 무단침입죄에 해당하여 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다(동법 제63조 제1호)고 규정하고 있다.

또한 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하지 못하도록 규정하고 있으며(동법 제48조 제3항), 누구든지 정보통신망의 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 안된다(동법 제49조)고 규정하고 있다. 이러한 행위는 정보통신망 비밀침해죄 및 정보훼손죄에 해당하고, 이를 위반한 자에게는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 하고 있다(동법 제62조 제5호, 제6호).

바이러스와 관련해서는 누구든지 정당한 사유없이 정보통신 시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”)을 전달 또는 유포하지 못하도록 정하고 있으며(동법 제48조 제2항), 이러한 행위는 악성프로그램 전달·유포죄에 해당하고, 이를 위반한 자에게는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(동법 제 62조 제4호)고 규정하고 있다.

5. 정보통신기반보호법

(1) 개 요

이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행하는 것을 목적으로 한다. 따라서 국무총리 소속으로 정보통신기반보호위원회를 설치하여 주요정보통신기반시설 보호정책의 조정, 주요정보통신기반시설의 보호계획의 종합·조정, 그리고 주요정보통신기반시설 보호와 관련된 제도의 개선 등에 대하여 규율하고 있다.

(2) 범정부적 보호체계 구축

'정보통신기반보호법'에 의하며, 범정부 차원의 정보보호체계 구축을 위해 정보통신기반보호위원회[16]를 설치·운영하도록 하고 있다.

정보통신기반보호위원회(위원장 : 국무총리)는 관계중앙행정기관의 장을 중심으로 구성되어 주요정보통신기반보호시설 지정, 보호계획 및 정책 등의 심의를 수행하며, 간사는 국무조정실이 담당하고 있다. 관계중앙행정기관은 소관 분야의 주요정보통신기반시설을 지정하고 보호계획을 수립하는 등의 업무를 수행한다. 주요정보통신기반시설의 관리기관은 소관시설에 대하여 취약점을 분석·평가하고, 이를 통한 정보보호 대책을 수립·추진하는 역할을 맡게 된다. 기타 중앙행정기관 및 관리기관은 정보보호책임관 및 정보보호책임자를 지정하여 해당 업무를 수행토록 하고 있다.

16) 2001년 7월 정보통신기반보호법이 시행됨에 따라 주요 정보통신기반시설의 보호정책을 심의하기 위한 정보통신기반보호위원회 및 실무위원회를 구성·운영하게 되었다.

(3) 주요 정보통신 기반시설 보호지원

국가기관 및 지방자치단체 소관 주요 정보통신기반시설을 보호하기 위하여 필요한 경우 관리기관 등에서는 전문기술 지원을 요청할 수 있도록 하고 있다. 본 요청 대상기관으로서 국가기관은 국가정보원·국군기무사, 전문기관은 한국정보보호진흥원·정보보호전문업체·한국전자통신연구원의 국가보안기술연구를 전담하는 부설연구소가 있다. 지원요청분야로는 보호대책의 수립 및 검토, 침해사고의 예방 및 복구를 위한 기술적 지원 등이 있다.

다만, 개인정보보호 등을 위하여 금융정보통신기반시설 등 개인 정보가 저장된 모든 정보통신기반시설에 대해서는 지원할 수 없도록 하고 있다.

(4) 주요 정보통신 기반시설의 지정

정보통신기반보호위원회 심의를 거쳐 중앙행정기관의 장이 고시함으로써 주요정보통신기반시설이 지정되며, 2001년 12월 20일에 1차 정보통신기반보호위원회가 개최되어 4개 부처의 23개 시설이 심의 통과되었다. 지정된 시설은 외교통상부 1개, 행정자치부 2개, 보건복지부 3개, 정보통신부의 통신망, 인터넷, 우정 분야 등 17개 이다.

또한, 2002년 9월 2차 지정심의에서는 5개 부처의 66개 시설이 심의 통과 되었다. 지정된 시설은 재정경제부 19개, 금융감독위원회 39개, 산업자원부 3개, 건설교통부 4개, 국회사무처 1개이다. 이후에도 지속적으로 기반시설 지정에 대하여 심의할 계획이다.

(5) 취약점 분석평가

지정된 시설의 관리기관은 최초 지정 후 6개월 이내에 취약점 분석 및 평가를 실시하되, 특별한 사유가 있는 경우에는 관계 중앙행정기

관의 장의 승인을 얻어 9개월로 할 수 있다. 그리고 매 2년마다 취약점 분석 평가를 실시하고, 실시하지 않은 연도에는 간이 취약점 분석 평가를 실시하도록 하고 있는데, 필요시에는 정보보호전문업체 및 한국정보보호진흥원, 한국전자통신연구원 등에 위탁하여 추진할 수 있다.

취약점 분석·평가 수행지원을 위하여 정보통신부에서는 '주요정보통신기반시설 취약점 분석·평가 기준'을 제시하였으며, 한국정보보호진흥원에서는 '취약점 분석·평가모델'을 개발하여 제공하고 있다.

2002년 12월 현재까지 기 지정된 89개의 주요 정보통신기반시설들은 정보보호전문업체에 위탁하여 추진되었거나 추진되고 있다.

(6) 침해사고 예방조치 및 대응

관계중앙행정기관의 장은 정보보호관리체계의 관리 및 운영, 취약점 분석·평가, 침해사고 예방 및 대응·복구 등에 관하여 소관분야의 시설에 대한 보호 지침을 제정하여 명령 또는 권고 할 수 있다. 이와 관련하여 필요한 경우 정보통신부에 지원을 요청할 수 있도록 하고 있다. 그리고 침해사고가 발생되었을 경우 관계중앙행정기관, 수사기관, 한국정보보호진흥원에 통지하고 신속한 복구조치를 위하여 관리기관의 장은 노력하되, 필요한 지원을 관계중앙행정기관 또는 한국정보보호진흥원에 요청할 수 있도록 하고 있다. 그리고 분야별로 중요한 상황이 발생될 경우에는 기반보호위원회의 위원장을 중심으로 침해사고대책본부를 구성하여 운영하며, 필요한 지원은 관계 중앙행정기관, 관리기관, 한국정보보호진흥원에 요청할 수 있도록 하고 있다.

(7) 정보공유분석센터

침해사고 관련 정보 등의 공유를 통하여 피해 확산을 최소화하기 위해 정보공유분석센터를 분야별로 설립·운영할 수 있으며, 이 경우 관할 중앙행정기관에 신고하도록 하고 있다. 현재까지 국내설립현황

으로 통신분야는 한국통신사업자연합회에서, 금융분야는 금융결재원과 한국증권전산에서, 순수 민간 부문의 경우 삼성SDS 및 기타 정보보호업체들이 현재 설립하여 운영중이다.

6. 전자거래기본법

전자거래기본법에서는 전자거래의 안전성 및 신뢰성을 확보하기 위하여 전자거래사업자에게 암호제품을 사용할 수 있도록 정하고 있으며(동법 제14조 제1항), 정부는 국가안전보장을 위하여 필요하다고 인정하는 경우에는 암호제품의 사용을 제한하고, 암호화된 정보의 원문 또는 암호기술에의 접근에 필요한 조치를 할 수 있도록 정하고 있다(동법 제14조 제2항).

7. 전자서명법

전자서명법에서 보안과 관련한 부분은 공인인증기과의 안정성 문제와 밀접한 관련이 있다. 따라서 전자서명법에서는 전자서명의 인증과 관련하여 공인인증기관은 인증 업무에 관한 시설의 안전성 확보를 위하여 정보통신부령이 정하는 보호조치를 취하여야 한다(동법 제18조의 3)고 규정하고 있으며, 공인인증기관은 자신이 발급한 공인인증서가 유효한지의 여부를 누구든지 항상 확인 할 수 있도록 하는 설비 등 인증업무에 관한 시설 및 장비를 안전하게 운영하여야 하고, 이러한 시설 및 장비의 안전운영 여부를 보호진흥원으로부터 정기적으로 점검받도록 정하고 있다(동법 제19조 제1항, 제2항).

공인인증기관은 자신이 이용하는 전자서명생성정보를 안전하게 보관·관리하여야 한다. 이 경우 당해 전자서명생성정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 보호진흥원에 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하도록 정하고 있으며(동법 제21조 제

1항), 또한 공인인증기관은 가입자의 공인인증서와 인증업무에 관한 기록을 안전하게 보관·관리하여야 할 뿐만 아니라 가입자인증서등을 당해 공인인증서의 효력이 소멸된 날부터 10년동안 보관하여야 한다(동법 제22조)고 규정하고 있다.

한편 공인인증기관은 인증업무 수행과 관련하여 가입자 또는 공인인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상하여야 하나(동법 제26조), 다만 그 손해가 불가항력으로 인하여 발생한 경우에는 그 배상책임이 경감되고, 공인인증기관이 과실없음을 입증한 경우에는 그 배상책임이 면제됨을 규정하고 있다.

8. 전자정부법

우리나라 전자정부는 2001년 3월에 제정된 '전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률'에 근거하고 있다. 우리나라는 1986년 5월 제정된 "전산망보급확장과이용촉진에관한법률"을 근거로 국가기간전산망사업을 추진하였으며, 1995년에 제정된 "정보화촉진기본법"을 근거로 정보화를 국정의 주요과제로 삼고 정보화정책을 추진하였다. 전자정부법은 이러한 정보화입법을 모법으로 하여 행정전자화를 통한 정부혁신을 달성하기 위한 기본법이라고 평가할 수 있고 이에 걸맞게 전자정부의 정보보안에 관한 기본적인 내용을 담고 있다. 하지만 종합적 관점에서 전자정부에서 정보보안의 정책의 수립·조정·실행을 위해서는 좀 더 구체적인 입법이 필요하다는 지적을 받고 있다.

전자정부법은 2007년 1월에 개정되었는데, 정보보안과 관련해서는 법률차원에서 3개의 조항이 신설되었다는 점에서 중요한 의미가 있다. 즉 공공분야에 대한 행정자치부의 역할과 정부부처의 임무를 법률차원에서 다룬 점에서 그 의미가 크다고 볼 수 있다. 구체적으로 전자정부법은 제27조제1항에서 "국회·법원·헌법재판소·중앙선거관리위원회 및 행정부는 전자정부의 구현에 요구되는 정보통신망과 행정정

보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다”고 규정하고 있으며, 제4항에서 “제3항의 규정을 적용함에 있어서 국회・법원・헌법재판소・중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 당해 기관의 장이 필요하다고 인정하는 경우에 한한다. 다만, 필요하지 아니하다고 인정하는 경우에는 당해 기관의 장은 제3항의 규정에 준하는 보안조치를 강구하여야 한다”라고 규정하였다. 동법 제39조의2에서는 전자적 대민서비스 보안대책을 행정자치부장관이 국가정보원장과 사전협의를 통하여 마련하도록 하였고 중앙행정기관과 그 소속기관 및 지방자치단체의 장은 이에 따라 보안대책을 수립・시행하도록 하였다.

한편, 전자정부법 제39조의3에서는 전자정부서비스보안위원회를 행정자치부장관 소속하에 설치하여 보안정책의 수립, 보안사고 발생시 대응조치 등을 심의하도록 하였으며 관련된 세부적인 사항과 실무위원회 등에 관련해서는 시행령에서 규정하도록 하였다.

9. 국가사이버안전관리규정

국가사이버안전관리규정은 대통령훈령(제141호)이라는 법규형식으로 규정되어 있지만 그 규율하고 있는 내용은 대부분 법률차원에서 규율되어야 할 사항으로 볼 수 있다. 이 규정의 내용을 살펴보면, 다음과 같다.

첫째, 이 규정은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 있으며, 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호하는 것을 목적으로 한다(동법 제1조 참조). 이 규정에서 국가사이버안전은 사실상 범정부차원의 정보보안에 관련된 것이고, 국가안보도 실질적으로는(국가사이버안전관리규정의 내용상으로는) 모든 정보보안에 관련된 것에 해당된다. 따라서 이 규정은 중앙행

정기관, 지방자치단체 및 공공기관에 적용된다(동 규정 제3조 전단). 다만, 정보통신기반보호법에 의하여 주요정보통신기반시설로 지정된 것에 대하여 적용되지 아니한다(동 규정 제3조 후단).

둘째, 이 규정은 중앙행정기관의 장이 소관 정보통신망에 대한 안정성 확보의 책임을 부과하고 있고 사이버안전업무를 전담하는 전문인력을 확보하도록 하였다(동 규정 제4조).

셋째, 이 규정은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 국가사이버안전과 관련된 정책 및 관리를 총괄·조정하도록 하였다(동 규정 제5조).

넷째, 이 규정은 국가사이버안전전략회의를 국가정보원장 소속하에 두고서 국가사이버안전에 관한 중요사항을 심의하도록 하고 전략회의의 위원등 세부적인 사항을 정하도록 하였다(동 규정 제6조).

다섯째, 이 규정은 전략회의의 효율적인 운영을 위하여 국가사이버안전대책회의를 두고 있다(동 규정 제7조).

여섯째, 이 규정은 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터를 두고서 사이버안전정책의 수립, 전략회의 및 대책회의의 운영에 대한 지원 등을 하도록 하고 있다(동 규정 제8조).

일곱째, 이 규정은 중앙행정기관의 장이 소관 정보통신망을 보호하기 위한 사이버안전대책을 수립, 시행하고 지도·감독하도록 하였으며, 국가정보원장은 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼을 작성 배포할 수 있도록 하였다(동 규정 제9조).

여덟째, 이 규정은 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장에게 국가정보통신망에 대한 사이버공격 등에 대하여 그 사실을 국가정보원장에게 통지하도록 하였다(동 규정 제10조).

아홉째, 이 규정은 국가정보원장에게 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려

하여 관심·주의·경계·심각등 수준별 경보를 발령할 수 있도록 하였고 관련기관의 장에게 적절한 조치를 하도록 하였다(동 규정 제11조).

열 번째, 이 규정은 중앙행정기관의 장 등이 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에 피해를 최소화하는 조치를 하고 그 사실을 국가정보원장에게 통보하도록 하였으며 국가정보원장은 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있도록 하였다(동 규정 제12조).

열한번째, 이 규정은 국가정보원장이 사이버공격으로 인하여 발생한 사고에 대하여 조사할 수 있도록 하였고, 범죄혐의나 피해가 심각하다고 판단한 경우에는 관련조치(수사요청 등)를 할 수 있도록 하였다.

10. 소 결

우리나라의 정보보안 관련법제는 많은 법률에 산재한 여러 규정을 가지고 있고, 정보보안을 위한 정책의 수립과 조정, 집행을 위해서 정부와 민간이 어떻게 협업을 하고, 정부의 여러 부처가 어떻게 권한과 의무를 분배하며, 이렇게 분배된 권한과 의무를 어느 조직이 조정·통합할 것인지에 대한 원칙에 대한 합의가 없이 단편적으로 입안되고 시행되고 있다고 할 수 있다. 따라서 법제의 개선을 위해서는 우선 이러한 기본적 사항에 대한 원칙적인 합의를 도출하고 이에 근거한 체계적인 법의 제·개정이 필요하다.

제 3 장 OECD 및 미국의 정보보안 관련법제

제 1 절 OECD의 지침

OECD는 1992년에 정보시스템의 개발과 이용에 있어서 통일된 규범을 형성하기 위하여 '정보시스템의 보안을 위한 지침'에서 9개의 기본원칙을 채택하였는데, 그 주요내용은 다음과 같다(번역문은 부록 1 참조).

(ⅰ) 책임의 원칙 : 정보시스템의 소유자, 제공자 및 이용자 그리고 기타 정보시스템의 안전성에 관련된 자의 책임과 의무를 명백히 해야 한다.

(ⅱ) 주지의 원칙 : 정보시스템에서 신뢰성을 높이기 위하여 정보시스템의 소유자, 제공자 및 이용자 그리고 기타 자가 쉽게 적절한 지식을 얻을 수 있는 안전성 유지에 일관성을 유지하고 정보시스템의 안전성을 위한 일반적인 조치, 관행 및 절차의 존재와 범위를 알려주어야 한다.

(ⅲ) 윤리의 원칙 : 정보시스템과 정보시스템의 안전성은 타인의 권리나 정당한 이익을 존중하는 방법으로 제공되고 이용되어야 한다.

(ⅳ) 분야별 협력의 원칙 : 정보시스템의 안전성을 위한 조치, 관행 및 절차는 기술적, 행정적, 조직적, 운영적, 상업적, 교육적 및 법적인 것을 포함하는 모든 관련된 배려와 관점을 고려해야 한다.

(ⅴ) 비례의 원칙 : 안전성의 수준, 비용, 조치, 관행 및 절차는 정보시스템에 의존하는 가치와 정도에 비례해야 하고, 특별한 정보시스템에 의존하는 안전성의 정도는 잠재적인 위험의 심각성, 개연성 및 범위에 비례해야 한다.

(ⅵ) 통합의 원칙 : 정보시스템의 안전성을 위한 조치, 관행 및 절차는 일치된 안전성시스템을 형성하기 위하여 조직 상호간에 조

치, 관행 및 절차에 협력해야 한다.

(vii) 적절성의 원칙 : 국내・외적인 관점에서 공공분야와 민간분야의 참여자들은 정보시스템의 안전성 침해를 예방하고 대응하기 위하여 적시에 협력적인 조치를 취하여야 한다.

(viii) 재평가의 원칙 : 정보시스템의 안전성은 시간이 경과함에 따라 정보시스템의 안전성을 위한 필요조건에 맞추기 위해 정기적인 재평가를 받아야 한다.

(ix) 민주주의의 원칙 : 정보시스템의 안전성은 민주사회의 합법적인 정보의 이용과 유통에 부합하여야 한다.

이 지침은 공공분야와 민간분야 모두를 위하여 제정되었고 모든 정보시스템에 적용된다. 위의 지침의 원칙에 따라서 공공분야와 민간분야는 정보시스템의 보호와 안전성의 제공을 위한 조치를 하고, 안전성 목적의 달성과 이들 원칙의 구현은 정보시스템의 보안을 위해 필요한 법적・행정적・자기규제적 그리고 기타의 조치・관행・절차와 기구의 설립을 촉진하고 지원할 것을 강조하고 있다. 구체적으로 이 지침은 다음을 목적으로 하고 있다. 첫째 정보시스템의 위험과 이러한 위험에 대처할 보안장치에 대한 인식을 증진시키고, 둘째 공공분야와 민간분야에서 정보시스템의 보안을 위하여 통일된 조치・관행 및 절차의 개발과 구현을 위한 책임을 지우는 일반적인 기반을 구축하며, 셋째 이러한 조치・관행 및 절차의 개발과 구현에 있어서 공공분야와 민간분야사이에 협력을 촉진시킨다. 넷째 정보시스템과 이용되는 수단에 대한 신뢰성을 높이고, 다섯째 국내・외적으로 정보시스템의 개발과 이용을 자극하며, 여섯째 정보시스템의 보안을 확보하기 위하여 국제적인 협력을 촉진시킨다.

제 2 절 미국 정보보안법제

1. 개 요

정보통신기술의 발전에 따라 국가의 모든 기능이 정보통신시스템에 의해 수행되고, 인터넷으로 세계가 하나로 연결되면서 정보통신시스템에 대한 침해행위와 그에 따르는 결과는 국가의 안전을 위협하는 수준에 이르고 있다.[17] 이러한 위험에 대처하고자 미국 연방 정부는 1987년 컴퓨터보안법(Computer Security Act of 1987), 1990년 OMB Circular A-130, 2000년 정부정보보안개혁법(Government Information Security Management Act of 2002)을 제정하였다.

나아가 국가 핵심 정보시스템이 테러와 전쟁에 있어 중요한 공격목표가 됨에 따라 정보보안 정책과 제도를 수립하고 국가적 전략을 마련하면서 각종 법제를 정비하고 있다. 특히 지난 9.11 테러 이후 국토안보부 창설을 위한 국토안보법을 통과하여 시행하고 있으며, 정부정보보안관리법(the Federal Information Security Management Act 0f 2002)을 전자정부법과 국토안보법에 삽입하여 통과시키는 등 정보보안 관련 법률을 정비하고, 애국자법을 제·개정하였으며, 대통령 행정명령과 각 부처의 지침 등을 통하여 이러한 법률의 시행을 구체화하고 있다.

한편 미국은 정보보안의 차원에서 과거에는 국내외에서 암호제품의 생산과 유통을 규제하여 왔는데, 현재는 이러한 규제가 상당히 완화된 상태이다. 이 보고서에서는 위에서 언급된 법령을 중심으로 미국 연방정부의 정보보안법제를 개관하고자 한다.

---

17) 한국정보보호진흥원, □□미국, 독일, 일본의 정보보호법 체계에 관한 연구□□, 한국정보보호진흥원, 2006. 12., 9-10쪽.

2. 관련법제의 내용

(1) 컴퓨터보안법(Computer Security Act of 1987, Public Law 100-235)

컴퓨터보안법은 연방 컴퓨터 시스템에 있는 기밀정보(sensitive information)의 보안 및 개인정보 보호를 위하여 기존의 보안 조치 내에서 최소한의 보안기준(security practices)을 확립하기 위하여 제정되었다(제2조 (a)항).

이 법은 국가표준국(National Bureau of Standard)에 연방컴퓨터시스템에 대한 표준 및 지침의 개발, 연방컴퓨터시스템 제기밀정보의 보안 및 프라이버시의 비용효율 보장에 필요한 표준 및 지침의 개발과 국가보안처의 기술적 조언 및 지원(작업생산품 포함)을 작성하도록 책임을 부과하고 있다(제2조 (b)항 (1)호). 그리고 기밀정보를 담고 있는 연방컴퓨터시스템의 운용관 전원에게 보안계획을 수립하도록 요구하고 있으며(제2조 (c)항 (3)호), 기밀정보를 담고 있는 연방컴퓨터시스템 관련자에게 정기적인 위탁교육에 관한 사항을 규정하고 있다(제2조 (c항) (4)호).

상무부내에 컴퓨터시스템보안 및 프라이버시자문위원회를 설치하며(제21조 (a)항), 위원회는 ⅰ) 컴퓨터시스템의 보안 및 프라이버시에 관하여 제기되는 운영, 기술, 관리 및 기계의 안전유지문제의 승인, ⅱ) 규격표준국 및 상무부에 연방컴퓨터시스템에 관련된 보안 및 프라이버시문제에 관한 자문, ⅲ) 사실개요서를 상무부장관, 관리예산처장, 국가안전처장 및 연방의회의 소관위원회에 보고 등의 권한이 있다.

(2) 관리예산처 회람 A-130(OMB Circular A-130)[18)]

미국의 전자정부 추진체계에서 가장 중심적인 기관은 관리예산처(OMB)이다. 동 기관은 정보보안과 관련해서도 중심적인 역할을 수행

18) 이에 관해서는 국가보안기술연구소, 미국 연방정보보안관리법 체계 및 동향, 『Security Issue』, 제5권 제3호, 2005. 10, 4-5쪽 참고.

하고 있다. 관리예산처는 전자정부 구축 관련법률에 의하여 관리예산처 회람 A-130(OMB Circular A-130)을 제정하여 정보자원의 관리와 정보보안에 있어 요구되는 의무의 수행에 필요한 사항들을 규정하고 있다.

1) 주요내용

①회람의 부록Ⅲ 연방정보자원보안(Security of Federal Automated Information Resources)은 연방 정보보안정책에 필요한 최소한의 통제장치들을 수립하고 있으며, 관련기관들에게 정보보안에 대한 책임을 지도록 하면서 각 기관들의 정보보안프로그램과 기관관리통제시스템을 상호 연계시키고 있다.

②회람은 정보가 손실, 남용, 비인가접근 및 비인가수정될 수 있는 위험을 제거하여 각 기관의 시스템 및 응용프로그램의 효과적인 운영과 정보의 기밀성, 무결성 및 이용가능성을 확보하려고 하였다. 이를 위하여 정보자원을 일반지원시스템(General Support System)과 주요응용자원(Major Application)으로 구분하고 각각에 대하여 각 기관들로 하여금 정보보안 담당 지정, 보안계획수립 및 보안통제평가 등을 수행하도록 하고 있다.

③회람은 관련기관의 권한과 의무를 규정하고 있다. 이 회람에 따르면 관리예산처는 연방정보자원 보안정책을 총괄하고 감독하며, 상무부 특히 국립기술표준원(National Institute of Standard and Technology : NIST)은 보안관련 표준 및 지침을 개발하고, 인사관리처(Office of Personnel Management : OPM)와의 협력 하에 연방공무원에 대한 정보보안 교육・훈련을 위한 지침을 검토・개정할 권한이 있으며, 연방기관들의 보안계획 수립에 필요한 지침과 지원을 제공하고, 각 기관의 침해사고 대응 및 취약성 정보 공유 및 조정을 담당하며 국방부, 국가보안국(NSA)의 기술적 지원을 받아 새로운 정보기술의 보안 취약성 평

가와 공표를 할 권한을 갖는다. 국방부, 특히 국가보안국(National Security Agency : NSA)은 상무부에 적정한 기술 자문 및 지원을 제공하고 새로운 정보기술의 취약성 평가와 관련하여 상무부를 지원할 의무가 있으며, 법무부는 보안침해사고가 일어날 경우 적절한 법적 조치를 하여야 한다. 총무처(General Services Administration : GSA)은 연방기관들이 정보처리장치 관련 장비 조달시 고려해야 할 보안지침을 제공하고 연방 기관들이 필요로 하는 적절한 보안서비스를 제공할 의무가 있다. 보안정책위원회(Security Policy Board)는 정보기술보안 관련 연방정부의 활동을 조정하는 역할을 담당한다.

2) 평 가

회람은 컴퓨터보안법에 비하면 정보보안에 관련한 추진체계를 보다 정교하게 체계화하였다. 그러나 시간이 흐름에 따라 전자정부 구축과 운영과 관련하여 회람 제정을 중심으로 한 현재까지의 대처가 국가안전보장시스템의 특수성을 살리지 못한다는 지적과 양적・질적으로 급격히 증가・변화하고 있는 새로운 침해행위에 대하여 효율적이지 못하다는 인식이 확산되고, 국가 주요기반보호에 대한 강도 높은 정책추진에 대한 요구가 일어나면서 미국 연방정부는 2000년 10월 30일 정부정보보안개혁법을 제정하게 되었다.

(3) 정부정보보안개혁법(Government Information Security Reform Act 0f 2000)[19]

1) 총 론

정부정보보안개혁법(Government Information Security Reform Act of 2000)은 ⅰ) 비기밀(unclassified)시스템과 ⅱ) 국가안보(national security)시

19) 이에 관해서는 김대호・오일석, “미국 전자정부 정보보안 법제 동향”, 『한국정보보호학회지』, 제13권 제3호, 2003.6, 18-20쪽 참고.

스템에 적용된다. ⅰ) 비기밀시스템인 경우, 1995년 정부문서감축법(Government Paperwork Reduction Act of 1995)과 1996년 정보기술관리개혁법(Information Technology Management Reform Act of 1996)에 의하여 관리예산처가 부여받은 권한과 책임을 유지하도록 하고 각 기관의 정보보안프로그램에 대한 감사관의 평가 역할을 제외하고는 기존 OMB Circular A-130을 법률의 내용으로 격상한 것으로 볼 수 있다. 그러나 ⅱ) 국가안보시스템의 경우, 정보보안과 관련한 관리예산처의 권한을 국방부, 중앙정보국 및 대통령이 지정한 다른 기관에 위임하도록 하고 있으며 국방부의 비기밀시스템에 대한 관리예산처의 권한도 국방부장관에게 일부 위임하도록 하고 있다.

요컨대 비기밀시스템의 경우 관리예산처를 중심으로, 국가안보시스템의 경우 국방부 등 국가안보관련부처를 중심으로 추진체계를 정리하였다고 할 수 있다.

2) 목 적

정부정보보안개혁법은 ⅰ) 연방정부가 가진 정보자원을 효과적으로 통제하기 위한 종합적인 틀을 제공하고, ⅱ) 고도로 네트워크화되어 있는 연방정부의 컴퓨팅환경을 인식하여 연방정부 정보처리의 상호운용성(interoperability)의 필요성과 철저한 보안관리의 필요성을 인식하며, ⅲ) 연방정부의 정보보안 위험성을 점검하여 정부차원에서 효과적인 수단을 제공하고, ⅳ) 연방정부의 정보나 정보시스템을 보호하기 위한 최소한의 통제수단을 제공하며, ⅴ) 연방정부의 정보보안프로그램을 효과적으로 통제하기 위한 체계를 제공하는 것을 목적으로 하고 있다.

3) 각 기관의 권한과 책임

①관리예산처장은 범정부차원의 정보보안 정책을 수립하여야 한다. 즉 관리예산처장은 ⅰ) 연방정보시스템의 비용효과적인 보안, ⅱ) 1996

년 정보기술관리개혁법(Information Technology Management Reform Act of 1996)에 제시된 정보기술아키텍쳐, iii) 정보시스템 위험의 확인 및 평가를 통한 위험관리주기 구축, iv) 위험의 적절한 통제, v) 정보보안 위험에 대한 인식 제고 및, vi) 정보보안 절차의 효과성 감시 평가 등을 포함하는 것을 내용으로 하는 정책을 수립하여야 한다. 관리예산처장은 연방정부의 정보나 정보자원을 효과적으로 관리하기 위한 정책, 원칙, 표준 및 지침을 개발하고 감독할 뿐만 아니라 수집된 정보의 분실, 오·남용, 불법접근·변조 등에 따라 발생되는 손실과 위험에 대비한 정보보안 대책을 강구할 것을 연방 정부기관들에게 요구할 수 있다.

관리예산처장은 연방정부기관의 장에 대하여 적절한 보안 대책의 수립, 사용 및 공유와 범부처 차원의 정보보안 계획 수립, 정보시스템의 생명주기에 적합한 정보보안 원칙 및 절차의 마련 등을 지시할 수 있다. 또한 1996년 정보기술관리개혁법(Information Technology Management Reform Act of 1996)과 국가표준기술원법(National Institute of Standards and Technology Act)에 근거하여 연방컴퓨터시스템의 보안과 관련한 상무부의 표준과 지침의 개발과 집행을 감독한다.

②상무부 장관은 연방정부시스템의 보안을 위한 표준과 지침을 개발하고 보급 검토하며 개정할 책임을 부담하며, 정보보안 훈련을 위한 표준과 지침의 개발, 각 정부 부처의 정보보안 정책 수립 지원 및 정보보안 위협 기술 평가 등에 대한 책임을 부담한다.

③국방부 장관과 중앙정보국장은 정보시스템의 보안정책, 표준 및 지침의 개발과 보급 및 그 수행을 점검하여야 하며 국방부 장관과 중앙정보국장이 마련한 정책, 원칙, 표준 및 지침의 모든 내용이 공개되도록 하여야 한다.

④법무부 장관은 정보보안 사고와 관련한 법적인 조치 및 보고 지침 등을 검토하고 개정해야 한다.

⑤총무처는 연방 정부 부처들이 새로운 정보기술을 도입하는 경우 발생되는 정보보안 문제를 검토하고 개선해야 하며, 각 부서의 보안 제품 확보를 위한 지원과 정보보안 기술의 도입에 있어서 비용 효과적인 제품과 서비스 등이 도입되도록 하여야 한다.

⑥인사관리국은 연방 공무원을 대상으로 컴퓨터 보안 교육과 관련한 법규를 재검토하고 개선하여야 하며, 컴퓨터 보안 교육 지침에 대해서는 상무부와 협력하여야 한다. 또한 정보보안 교육의 내용 및 교육 강사와 관련하여 국립과학재단(National Science Foundation) 및 기타 다른 기관들과 협력하여야 한다.

요약하면 비기밀시스템의 경우 관리예산처를 중심으로, 국가안보시스템의 경우 국방부 등 국가안보관련부처를 중심으로 정보보안을 관리한다. 연방 각 정부 부처는 관리예산처와 상무국이 작성한 정보보안 정책, 원칙, 표준 및 지침의 범위 내에서 각자의 정보보안 정책, 원칙, 표준 및 지침을 작성하고 채택한다.

4) 연방 부처의 정보보안 정책에 대한 평가

연방정부의 모든 부처는 ⅰ) 정보시스템의 안전성과 위협에 대비한 정기적인 위험평가, ⅱ) 관리예산처장이 지시한 내용을 수용하며 정책 대상 집단이 순응할 수 있는 비용 효과적이며, ⅲ) 정보보안 위험이나 책임의식 고취와 관련한 정보보안 의식의 제고 및 ⅳ) 심각한 취약점이 발견된 경우의 대처를 위한 제반 과정과 정보보안 사고 발생시 발견, 보고 및 대응절차 등을 포함한 정보보안 정책을 개발하고 수행하여야 한다.

또한 연방 정부 부처의 이러한 정보보안 정책은 ⅰ) 연간 예산, ⅱ) 정보자원관리정책, ⅲ) 1996년 정보기술관리개혁법에 의한 정보보안 성과 및 결과, ⅳ) 재정관리 정책 및 ⅴ) 정책관련 중요한 개선사항 등을 포함하여야 한다.

이러한 연방 각 부처의 정보보안 정책들은 정보화책임관협의회를 거쳐 정책담당관에 의해 최소한 1년에 1회 검토 받아야 하며 관리예산처장의 승인을 받아야 한다.

연방정부의 모든 부처는 매년 자신들의 정보보안 정책을 평가하여야 한다. 이 경우 정보시스템의 정보보안 통제기법의 효과성, 관련된 정보보안 프로그램 및 관련 정책과의 일치성에 대한 평가 등이 포함되어야 한다. 각 부처의 정보보안 정책에 대하여 관련 평가기관이나 감사관(inspector general)의 감사, 평가를 받아야 한다.

연방정부 각 부처는 정부정보보안개혁법에 제시된 정보보안 평가결과 및 정보보안 감사결과를 동 법 발효 후 1년 이내에 관리예산처장에게 보고하여야 하며 관리예산처장은 이러한 제반 보고를 요약하여 의회에 제출하여야 한다.

5) 정부정보보안개혁법에 대한 평가

미국 연방정부는 정부정보보안개혁법을 통하여 연방기관들의 정보보안 관련 업무에 대한 철저한 추진체계를 구축하고자 하였다. 구체적으로 살펴보면 각 연방기관에게 그 기관의 기능과 관련한 정보보안에 관한 명확한 권한과 책임을 부여하고, 각 부처의 내부에서도 행정기관의 장, 정보화책임관(CIO) 등의 업무와 책임을 명확히 하고, 각 연방기관이 관리예산처, 국립표준기술원이 법에 따라 제시한 지침에 따라 자체적으로 수행한 정보보안업무에 대하여 감사관의 감사 및 관리예산처와 의회에 대한 보고절차를 명확히 규정하여 각 부처의 정보보안정책을 철저히 감독하고 추진을 독려하는 제도를 확립하였다. 특히 관리예산처로 하여금 각 부처의 정보보안 정책에 대한 총괄감독을 수행하도록 하고, 각 부처의 자체 정보보안 평가 및 감사관의 보고서 등을 종합적으로 검토하여 기관의 성과평가에 반영되도록 하여 각 부처의 정보보안 정책 및 프로그램의 실행을 강화하는 절차를 확립하였다.

이러한 정부정보보안개혁법은 각 연방기관의 정보보안에 대한 인식과 관행을 바꾸는데 획기적인 역할을 한 법률로 평가된다. 그러나 정부정보보안개혁법은 2002년 11월 29일에 그 기한이 만료되는 한시법으로 규정되어 있었다. 이에 따라 미국 연방정부는 정부정보보안개혁법의 틀을 유지하면서도, 그동안의 정보보안과 관련된 문제점을 파악하여 개선한 법률의 제정을 준비하여 마침내 2002년 연방정보보안법을 제정하였다.

(4) 연방정보보안관리법(Federal Information Security Management Act of 2002)

1) 총 론

미국정부는 2002년 11월 29일 만료 폐기되는 정부정보보안개혁법(Government Information Security Reform Act 0f 2000)을 대체하는 연방정보보안관리법(Federal Information Security Management Act of 2002)을 성안하고, 2002년 전자정부법의 제3절에 이 법안을 포함하여 국회에 제출하고 의회는 이 법안을 통과시켰다.

본 법의 입법목적은 ⅰ) 연방 업무 및 자산을 지원하는 정보자원에 대한 정보보안통제의 효과를 높이기 위한 종합적인 틀을 제공하고, ⅱ) 고도로 네트워크화된 연방 컴퓨팅 환경을 인식하고, 국민과 국가의 보안 및 관할지역 내 정보보안활동을 조정하는 등 관련 정보보안위험에 대한 효과적인 범정부 차원의 관리 및 감독을 실시하고, ⅲ) 연방 정보 및 정보시스템의 보호에 필요한 최소한의 통제수단을 개발 및 유지하며, ⅳ) 연방기관의 정보보안 프로그램에 대한 감독을 강화하기 위한 메카니즘을 제공하고, ⅴ) 상업적 목적으로 개발된 정보보안상품은 품질이 우수하고 역동적이며 강력하고 효과적인 정보보안 솔루션을 제공한다는 사실을 인정하고, 국방 및 경제안정에 필요한 주요 정보 인프라를

보호하기 위하여 민간이 개발, 구축 및 운영하는 솔루션을 도입하고, vi) 상업적 목적으로 개발된 상품 가운데 특정한 기술 하드웨어 및 소프트웨어 정보보안 솔루션을 선정하는 사항은 개별 기관에 맡겨져야 한다는 사실을 인식하는 것을 그 목적으로 한다(제3541조).

본 법에서 '정보보안'이라 함은 정보의 무결성(integrity), 비밀성(confidentiality) 및 이용가능성(availability)을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다. 본 법은 연방 행정기관의 모든 정보시스템에 적용되며 다만 국가보안시스템, 국방부 및 중앙정보국시스템의 경우에는 일반 정보시스템과는 달리 일정한 예외를 두고 있다(제3542조).

2) 주요내용

①관리예산처장의 권한 및 역할(제3543조)

관리예산처장은 ⅰ) 정보보안 정책, 원칙, 표준 및 지침의 개발 및 시행 감독 ⅱ) 행정기관 등이 이용 또는 운영하는 정보 또는 정보시스템에 대한 정보보안 조치의 확인 및 제공 ⅲ) 이 법에 대한 기관의 준수 여부 감독 ⅳ) 최소 1년마다 기관의 정보보안 프로그램 검토 및 승인 ⅴ) 정보보안 정책 및 절차와 정보자원관리 정책 및 절차의 조정 ⅵ) 연방 정보보안사고센터의 운영감독 ⅶ) 의회보고 등의 방법으로 각 기관의 정보보안 정책 및 업무를 감독한다. 이외에도 관리예산처장은 ⅷ) 국가표준기술연구원법상의 표준 및 지침의 개발과 관련하여 국가보안시스템을 운영하거나 통제하는 기관 및 사무국과의 조정 작업을 거침으로써 가능한 최대한의 범위에서 그러한 표준 및 지침이 국가보안시스템용으로 개발된 표준 및 지침을 보충할 수 있도록 하여야 한다.

②연방기관의 권한 및 역할(제3544조)

A) 기관장의 책임

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.

B) 정보보안 프로그램

각 기관은 정보 및 정보시스템에 대한 정보보안을 위하여 기관 단위의 정보보안 프로그램을 개발 및 시행하여야 한다. 동 프로그램은 ⅰ) 정보 및 정보시스템의 보안상의 위험에 대한 주기적인 평가 ⅱ) 정보보안 위험의 감소 및 정보시스템의 수명주기에 맞춘 정보보안 유지 등을 위한 정책 및 절차 ⅲ) 보안교육 ⅳ) 정보보안에 관한 정책, 절차 및 업무상의 여하한 결점에 대한 평가 및 이에 따른 구제조치를 계획, 시행, 평가 및 기록하기 위한 과정 ⅴ) 보안사고에 대한 탐지, 보고 및 대응을 위한 절차 ⅵ) 정보시스템에 대한 영속적 운영을 위한 계획 및 절차 등이 포함되어야 한다.

C) 보고의무

각 기관은 매년 관리예산처장, 의회 관련위원회, 감사원 등에 대하여 정보보안에 관한 정책, 절차, 업무의 적절성 및 효과 등에 관하여 보고하여야 한다. 또한, 각 기관은 연간 예산, 정보자원관리, 정보기술관리 프로그램의 성과, 재무관리, 재무관리 시스템, 내부 회계 및 행정통제에 관하여 계획하고 보고함에 있어 정보보안에 관한 정책, 절차 및 업무의 적절성 및 효과를 포함하여야 한다. 각 기관은 이러한 보고 과정에서 확인된 정책, 절차 또는 업무상의 여하한 중대한 결함에 대해서도 보고하여야 한다.

D) 시행계획

각 기관은 관리예산처장과의 협의를 거쳐 정보보안 프로그램 관련 소요예산 및 기간, 인력 및 교육 등에 관한 사항을 시행계획에 반영하여야 한다.

E) 공고 및 의견수렴

각 기관은 적절한 시기에 정보보안에 관한 정책안 및 절차안을 국민과의 관계에 영향을 미치는 범위 내에서 국민에 대하여 공고함으로써 의견개진의 기회를 제공하여야 한다.

③독자적 연간평가

각 기관은 정보보안 프로그램 및 업무의 효과를 파악하기 위하여 이에 대한 독자적인 평가를 실시하여야 한다. 각 기관의 장은 관리예산처장이 정한 날까지 그 평가 결과를 제출하여야 하며, 관리예산처장은 평가결과를 요약하여 의회보고서에 포함시켜야 한다. 이와 관련하여 감사원장도 연방기관의 정보보안 정책, 업무의 적절성과 효과, 본 법의 요건준수를 주기적으로 평가하여 의회에 보고하여야 한다.

④연방 정보보안 사고센터(제3545조)

관리예산처장은 연방 정보보안 사고센터를 운영하여야 한다. 동 센터는 ⅰ) 보안사고와 관련하여 기관의 정보시스템 운영자에 대하여 정보보안 사고의 탐지 및 수습에 관한 지침 등 기술적 지원을 제공하고 ⅱ) 정보보안을 위협하는 사고에 대한 정보를 수집하고 분석하며 ⅲ) 정보시스템 운영자에 대하여 현존 및 잠재적 정보보안 위협과 취약부분에 관한 정보를 제공하고 ⅳ) 정보보안 사고 및 관련 문제를 국가표준기술연구원, 국가보안시스템을 운영 또는 통제하는 기관(또는 사무국) 및 법률에 따라 대통령령으로 정한 기타 기관(또는 사무국)과 협의하여야 한다. 국

가보안시스템을 운영 또는 통제하는 각 기관은 국가보안시스템에 대한 표준 및 지침과 일치하는 범위 내에서 정보보안사고, 위협 및 취약부분에 관한 정보를 연방 정보보안 사고센터와 공유하여야 한다.

⑤연방 정보시스템 표준(제3546조)

A) 표준 및 지침의 제정

상무부장관은 국가표준기술연구원에서 개발한 표준 및 지침을 기초로 연방 정보시스템에 관한 표준 및 지침을 제정하여야 한다. 다만, 국가보안시스템에 대한 표준 및 지침은 기타 법률 및 대통령령에 따라 개발, 제정, 집행 및 감독하여야 한다.

B) 강제요건

상무부장관은 연방 정보시스템의 운영 또는 보안의 효율성을 개선하기 위하여 장관이 필요하다고 결정하는 범위 내에서 제정된 표준을 강제력 및 구속력을 가지도록 하여야 한다. 제정된 표준은 강제력 및 구속력이 있는 정보보안 표준을 포함하여야 한다.

C) 대통령의 불승인 또는 변경권

대통령은 불승인 또는 변경하는 것이 공익을 위한 것이라고 판단한 경우에는 표준 및 지침을 불승인 또는 변경할 수 있다.

D) 기관장의 표준 강화

각 기관의 장은 당해 기관의 감독범위 내에 있거나 감독을 받는 정보시스템에 대한 비용절감적인 정보보안을 위하여 장관이 제정한 표준보다 더 엄격한 표준을 활용할 수 있다. 다만, 보다 엄격한 표준은 최소한 장관에 의하여 강제력과 구속력을 가지는 것으로 된 적용 가능한 표준을 포함하여야 하고, 정책 및 지침과 합치되어야 한다.

⑥국가표준기술연구원(제303조)

이 법은 국가기술표준연구원법을 다음과 같이 개정하였다. ①연구원은 정보시스템에 관한 표준, 지침 및 관련 방법 및 기술을 개발할 임무가 있다. ②국가보안시스템을 제외한 기관, 기관과 계약을 맺은 자 또는 기관을 대신하는 다른 조직에 의하여 이용되거나 운영되는 정보시스템과 관련하여 최소 요건을 포함하는 표준 및 지침을 개발하여야 한다. ③기관의 모든 업무 및 자산에 대하여 적절한 정보보안을 제공하기 위한 최소요건을 포함하는 표준 및 지침을 개발하여야 한다. 단, 그러한 표준 및 지침은 국가보안시스템에 적용되지 아니한다.

⑦정보보안 및 프라이버시 자문위원회(제304조)

이 법에 따라 국가표준기술연구원법은 '컴퓨터 시스템 보안 및 프라이버시 자문위원회'를 '정보보안 및 프라이버시 자문위원회'로 변경하고, 동 위원회는 개발된 표준 및 지침안의 검토를 포함하여 연방정부 정보시스템에 관한 정보보안 및 프라이버시 문제에 대하여 동 연구원, 상무부 장관 및 관리예산처장에게 조언하도록 개정되었다.

(5) 사이버보안강화법(CYBER SECURITY ENHANCEMENT ACT OF 2002)

1) 총 론

국가 핵심 정보시스템이 테러와 전쟁에 있어 중요한 공격목표가 되면서 국가안보와 정보보안이 점차 같은 체계 아래 일관된 정책추진이 필요하게 되고 있다. 특히 미국은 지난 9.11 테러 이후 국토안보부[20]

20) 국토안보부의 조직구성에 관해 자세한 것은 한국정보보호진흥원, □□미국, 독일, 일본의 정보보호법 체계에 관한 연구□□, 한국정보보호진흥원, 2006. 12., 85쪽 이하 참고.

창설을 위한 국토안보법을 제정하면서 사이버보안에 관한 입법인 2002년 사이버보안강화법(Cyber Security Enhancement Act of 2002)을 이 법에 삽입하여 제정・시행하고 있다.[21]

이 법은 양형위원회로 하여금 특정 컴퓨터 범죄와 관련된 판결 지침을 개정하고 형벌을 강화하며, 컴퓨터 범죄에 대한 연구・보고를 하도록 하며, 긴급공개의 예외를 인정하는 것 등을 주요 내용으로 한다.

2) 주요내용

①특정 컴퓨터 범죄와 관련된 판결 지침의 개정

이 법은 미국 양형위원회(SENTENCING COMMISSION)에 특정 컴퓨터 범죄를 저지른 피고인에게 적용할 지침 및 정책문을 검토 및 개정하도록 하면서, 그 검토・개정에 반드시 고려하여야 할 요구사항을 담고 있다(제225조 (b)항).

첫째, 판결 지침 및 정책문이 당해 공격을 방지하기 위하여 공격의 심각성, 당해 공격의 증가하는 발생률, 효과적인 억제 및 적절한 처벌에 대한 필요성을 반영하여야 한다. 둘째, ⅰ) 공격에 기인한 잠재적인 손실과 실제 손실, ⅱ) 공격에 수반된 정교함 및 계획의 수준, ⅲ) 공격이 상업적 이익이나 개인적인 재정상의 이익을 목적으로 이루어졌는가의 여부, ⅳ) 피고가 공격을 범하는 데 있어서 위해를 가하고자 하는 악의적인 의도를 가지고 있었는지의 여부, ⅴ) 공격이 위해를 당한 개인의 프라이버시권을 침해한 범위, ⅵ) 공격이 국방부, 국가안보부, 또는 법무부의 촉진에 있어서 정부가 사용하는 컴퓨터를 수반하였는지 여부, ⅶ) 위반 행위가 주요 기반에 대한 상당한 간섭 또는 붕괴를 의도하였거나 그렇게 하였는지의 여부, ⅷ) 위반행위가 공중 보건이나 공공 안전에 대한 위협 또는 어떤 사람에 대한 상해를 발생시킬 의도

21) HOMELAND SECURITY ACT OF 2002, SEC. 225 : PUBLIC LAW 107-296

를 가졌거나 발생시켰는지의 여부 등의 요소를 고려할지와 고려한다면 얼마나 고려할지에 대한 내용을 담고 있어야 한다.

②컴퓨터 범죄에 대한 연구 및 보고

양형위원회는 2003년 5월 1일 이전에 본 조에 따라 양형위원회가 취한 모든 조치를 설명하고, 위원회가 특정 컴퓨터 범죄에 대한 법정형의 권고를 포함하는 요약보고서를 의회에 제출하여야 한다(제225조 (c)항).

③긴급공개 예외

일정한 경우 긴급공개제도의 예외를 인정하고, 이에 따라 긴급공개한 경우 일정한 요건 아래 이를 법무부장관에게 제출하도록 하고 있다(제225조 (d)항).

④특정 컴퓨터 범죄에 대한 형벌 강화

이 법은 특정 컴퓨터 범죄에 대한 형벌을 강화하고 있다(제225조 (g)항).

(6) 일명 애국자법과 그 개정법[22)]

1) 개 요

9・11 테러이후 미국 정부와 의회는 초당파적인 '테러와의 전쟁'을 선포하고, 이를 입법화하였다. 하원과 상원이 Patriot Act (H.R.2975)와 USA Act (S.1510)를 각각 가결 후, 양원의 조정을 통해 상원과 하원을 통과하고 2001년 10월 26일 부시 대통령의 서명을 얻은 Patriot Act[23)]이 공표되었다.

22) 애국자법과 그 개정법에 관해서 자세한 것은 고영국, "미국의 정보보안법제에 관한 고찰", □□전자정부법제연구□□ 제2권 제1호, 2007, 71쪽 이하를 참고.

23) 입법과정이 보여주듯이 이 법을 상원의 "Uniting and Strengthening America Act"와 하원의 "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act"를 합친 것으로 약칭 "USA Patriot Act" 또는 「애국자법」으로 불린다.

발효 당시에 동법은 2005년 12월 31일까지만 효력을 가지는 한시법(sunset law)이었는데, 미국 애국자법 개선 및 재승인법이라는 개정법은 애국자법의 한시법 규정 16개중 14개를 영구화하고, 제206조 및 제215조에 대해서는 그 유효기간을 2009년 12월 31일까지 연장하였다.

이 법률은 주로 감청, 전자메일의 감시 등 전자적 감시와 관련된 것으로 정보보안과는 다소 거리가 있지만, 정보보안과 밀접한 관련이 있는 내용도 있다. 여기서는 정보보안과 밀접한 관련이 있는 내용에 국한하여 살펴보기로 한다.

2) 주요 내용

①컴퓨터 침입자의 통신내용 감청(제217조)

컴퓨터 시스템 관리자가 시스템에 무단침입자(computer trespasser)를 감시하기 위하여 법집행기관의 지원을 받을 수 있도록 하였다. 가장 효과적인 방법은 법집행기관이 대상 컴퓨터 시스템에 전송되는 무단침입자의 통신을 감청하는 것이다. 이를 위해 법집행기관에 소속된 조사관은 컴퓨터 관리자로부터 통신감청에 대한 동의를 얻어 감청하는 내용이 조사와 관련이 있다는 합리적인 근거를 가지고 침입자가 보내거나 수신하는 통신을 감청할 수 있다.[24]

②사이버테러의 억제와 방지(제814조)

컴퓨터 사기 및 오용방지법(CFAA)에서 보호되는 컴퓨터에 불법 침입한 자에 대한 형벌을 최고 10년(초범의 경우)과 20년(상습범의 경우)으로 강화하고, 이러한 불법침입자는 특정 유형의 침해행위를 요하지 않고 침해행위의 고의만 있으면 되도록 하였다. 국가안전보장 또는 사법절차에 사용되는 컴퓨터에 대한 침해행위는 피해액이 5천 달러 미만이어도 범죄로서 규정하였다. 이 법에 의하여 보호를 받는 컴

24) 고영국, 앞의 논문, 75쪽.

퓨터(protected computer)의 범위를 외국에 있더라도 미국에서의 주간(interstate) 또는 대외(foreign) 통상거래에 사용되는 컴퓨터까지 확대하였으며, 해외에서 범행을 하였더라도 미국 내에서 형사소추할 수 있도록 관할범위를 확장했다. 그리고 주법에서 컴퓨터 불법침입죄로 처벌받은 것도 전과(prior offenses)로서 취급한다.[25]

③사이버보안 포렌식기술의 개발 및 지원(제816조)

법무부장관이 적절하다고 인정하는 곳에 컴퓨터포렌식연구소(computer forensic laboratory)를 설치할 수 있게 하고, 기존 컴퓨터포렌식연구소에 대하여는 지원을 강화하고 특정 포렌식[26]와 훈련능력을 제공하도록 하였다.[27]

(7) 사이버보안법 등 암호관련법률

미국은 현재 암호제품의 수출입에 대한 통제는 상당부분 완화시킨 상태다. 또한 미 행정부는 미국내에서의 범죄수사등을 위해 CESA (Cyberspace Electronic Security Act)법안을 제정하여 미국 내에서는 암호의 개발, 사용, 판매에 대한 어떤 규제도 없앴다. 특히 2000년 제정된 E-PRIVACY(Encryption Protects the Right of Individuals from Violation and Abuse in Cyberspace) Act에서 암호사용에 제한이 없음을 선언하고 있다.

제 3 절 시사점

위와 같은 미국 정보보안 관련법제를 정리하고 그 시사점을 도출하면 다음과 같다.

25) 고영국, 앞의 논문, 75쪽.
26) 컴퓨터 포렌식 또는 디지털 포렌식(forensics)이란 컴퓨터 관련증거를 법정증거로 제출하기 위한 과학적인 증거수집 절차 또는 방법을 말한다.
27) 고영국, 앞의 논문, 76쪽.

첫째, 미국 정보보안 관련법제의 첫 번째 특징은 관련기관간 기능에 따른 권한과 책임을 분산하고, 이러한 기관들의 수평적 협업을 통하여 철저한 정보보안이라는 목표를 달성하고 있다는 점이다.

원칙적으로 비기밀시스템의 경우 관리예산처를 중심으로, 국가안보시스템의 경우 국토안보부와 국방부 등 국가안전보장관련부처를 중심으로 추진체계를 정리하였다.

미국은 대통령 직속의 관리예산처(OMB)가 전자정부에 대한 책임을 맡아 왔다. 공공부문의 정보보안에 있어서도 원칙적으로 관리예산처가 추진체계의 중심에 자리잡고 있다. 따라서 정보보안에 관해 실질적 실무를 담담하고 있는 연방 정보보안 사고센터도 관리예산처가 운영하고 있다. 그러나 다른 개별분야와 마찬가지로 전문성을 보충하고 협력적 목표달성을 위해 관련기관과 유기적으로 협력하는 추진체계를 갖추고 있다. 상무부장관은 보안을 위한 표준과 지침을 개발하고 보급할 책임이 있고, 법무부장관은 정보보안사고와 관련된 법적 조치를 취할 책임이 있으며, 총무처는 정보기술도입시 정보보안문제를 검토하고 개선하며, 각 부처의 보안제품 확보를 위한 지원을 할 책임이 있고, 인사관리국은 보안교육과 보완관련법규를 검토・개선할 책임이 있다. 이러한 정부조직을 전문적으로 뒷받침하기 위해 국가표준기술연구원과 정보보안 및 프라이버시 자문위원회라는 조직도 운영하고 있다. 공공과 민간영역을 포괄하는 사이버공간에서 정보보안은 국가안전보장과 직결된다는 인식하에 국토안보부가 이에 관한 임무를 수행한다.

이처럼 미국 정보보안 관련 추진체계는 관련기관의 기능에 따른 권한과 책임의 분산, 이러한 기관들의 수평적 협업을 통한 목표의 달성이라는 특징을 도출할 수 있다. 연결된 정보통신망과 같이 관련기관들 간의 협업도 정보통신망과 같이 촘촘히 연결되어 있다. 따라서 정보보안법제의 상당부분도 관련기관의 권한과 책임, 수평적 협업의 의

무, 방법, 절차 등을 규정하고 있다. 이러한 추진체계는 다른 어느 개별분야보다도 예방이 중요한 정보보안분야의 특성을 감안하여 이에 맞도록 체계화된 것이라고 추측할 수 있다.

둘째, 미국 전자정부법은 전자정부기금의 조성을 통해 전자정부가 연방차원에서 통합적으로 추진될 수 있도록 관련 재원의 안정적 지원을 보장하고 있으며, 정보보안분야에 있어서도 이러한 전자정부기금을 이용하여 정책을 견고하게 추진하고 있다. 우리나라는 별도의 기금조성 없이 현행 전자정부법이 제49조에서 정보화촉진기금으로 전자정부 구현을 지원할 수 있도록 되어 있으며, 그나마 2006년 12월 8일 국회를 통과한 개정 전자정부법에서는 이 조항마저 삭제하여 기금의 지원을 받을 수 있는 근거조차 없어졌다. 지금까지의 정보화사업이 괄목할 만한 성장을 거둔 이유 중 하나가 바로 정보화촉진기금의 안정적 지원이라는 사실에 비추어 볼 때 향후 전자정부의 효율적인 구현을 위해서는 안정적인 재원 확보가 중요하다.

셋째, 정보보안은 편리성과 안전성이라는 가치가 고려된다. 정보보안을 강화하면 서비스가 좀 더 불편해 질 수 밖에 없고, 서비스의 편리성을 강화하면 정보보안은 좀 더 약화될 수밖에 없다. 따라서 전자정부 서비스에서 양 가치의 조화에 대한 합의와 그에 바탕한 입법이 필요하다. 이러한 측면에서 보았을 때, 미국은 양 가치 중에서 정보보안에 좀 더 치중하는 합의를 이루고 그에 바탕한 입법을 하였다고 할 수 있다. 우리는 전자정부추진에서 이 양 자에 관해 국민적 합의를 도출하려는 노력이 상대적으로 미미하였다고 판단된다.

2005년 국회에서 지적된 전자정부서비스 보안대책 미비 지적 사건이 일어난 후 2006년 전자정부법 개정에서는 전자정부서비스 보안강화에 관련 규정이 대폭 강화되었다. 이러한 입법 전에 이에 관한 국민적 합의를 도출하고 이에 바탕하여 입법추진을 하였다면 절차적 정당성을 강화하였을 뿐 아니라, 법의 실효성을 증진시키는데 도움이

되었을 것이다. 국가기관은 앞으로 이에 관한 국민적 합의점을 도출하는데 좀 더 노력할 필요가 있다.

넷째, 미국에서도 암호의 개발, 사용, 판매, 수출입에 관해서 초기에는 국가안전보장과 관련이 있다는 인식하에 상당한 규제를 하였다. 그러나 이미 살펴본 것처럼 이러한 규제는 상당부분 완화되는 방향으로 나아갔고, 현재는 이에 관한 어떠한 규제도 없는 상태이다. 우리나라는 이에 관하여 어떠한 규제도 없다가 최근에 와서 이러한 규제를 시도하고 있다. 그러나 미국의 입법의 흐름에 비추어 신중한 판단을 요한다고 생각한다.

제 4 장 현행 정보보안 관련법제의 문제점과 개선방안

제 1 절 정보보안 집행체계

1. 개 요

인터넷으로 연결된 정보시스템의 보안은 공공분야와 민간분야 모두에서 상호간 직접적으로 영향을 받고 있다는 점, 정보보안은 국가안보정보(국방정보를 포함)를 넘어서 모든 분야에서 문제된다는 점, 그리고 국민의 일상생활에 직접적으로 영향을 미칠 수 있다 라는 점 등이 주목된다. 따라서 정보보안은 해당 기관에만 맡겨둘 사안이 아니라 범정부차원의 총괄기관이 필요하다. 이와 관련해서 우리 나라의 정부조직법에서는 다름대로 국가기관의 역할과 권한을 부여하고 있는데,[28] 정보보안에 관련해서는 명문화된 조항이 없으며 현행법에 의하

28) [도표 1] 행정자치부・국가정보원・정보통신부의 역할과 업무관련 법령등 비교

	행정자치부	국가정보원	정보통신부
정부조직법	제34조(행정자치부) ①행정자치부장관은 …… 전자정부 … 지방자치제도, 지방자치단체의 사무지원・재정・세제, 지방자치단체간 분쟁조정, 선거, 국민투표, 민방위・재난관리 제도에 관한 사무를 관장한다. ②~⑦ 생략	제16조(국가정보원) ①국가안전보장에 관련되는 정보・보안 및 범죄수사에 관한 사무를 담당하기 위하여 대통령소속하에 국가정보원을 둔다. ②국가정보원의 조직・직무범위 기타 필요한 사항은 따로 법률로 정한다. [참조] 국가정보원법 제3조(직무) ①국정원은 다음 각호의 직무를 수행한다. 1.~4.(생략) 5. 정보 및 보안업무의 기획・조정 ②(생략)	제38조(정보통신부) 정보통신부장관은 정보통신・전파관리・우편・우편환 및 우편대체에 관한 사무를 관장한다.

면 정보통신부, 행정자치부 및 국가정보원 등이 각자 해당 정보의 보안업무를 수행할 수 있다. 물론 정보보안에 대한 총괄기구의 지정과 그 역할 및 업무부여는 아래에서 살펴보겠지만 정부조직법 외에 개별법의 제·개정을 통하여서도 가능하다.

2. 집행체계의 현황과 문제점

(1) 정보통신부

정보통신부는 민간분야에 대한 정보보안과 주요정보통신기반시설과 관련된 분야에 대한 정보보안을 담당하고 있다. 즉 정보통신망법에 따라 정부통신부 장관은 정보보호지침을 마련하여 정보통신서비스제공자에게 권고할 수 있으며 집적정보통신시설사업자에게 정보통신시설의 안정적 운영을 하도록 보호조치를 하게 할 수 있다. 또한 정보보호안전진단을 주요정보통신서비스제공자 등에게 받도록 하여 정보통신망 또는 정보보호를 강화하고 있고 정보보호관리체계의 인증제도도 마련하여 정보통신망의 안정성 및 신뢰성 확보를 하고 있다. 더 나아가서 정보통신부는 정보통신기반보호법에 따라 주요정보통신시설의 보호체계를 수립·집행함에 있어서 총괄기관으로 역할을 하고 정보통신기반보호위원회를 지원하고 있으며 주요정보통신기반시설의 보호 및 침해사고의 대응에 관련해서도 기술적 지원을 한다.

(2) 행정자치부

행정자치부는 전자정부사업을 총괄하고 있지만 공공분야의 정보보안관리에 대하여는 실질적으로 국가정보원이 주로 역할을 하고 있다. 그렇지만 미국의 연방정보보안관리법에서 볼 수 있듯이 공공분야에서의

정보보안관리에 대한 체계적이고 총괄적인 정보보안집행체계와 행정기관의 역할 및 임무 등에 관련해서는 미흡한 점이 있다. 2007년 1월에 개정된 전자정부법에서는 공공분야의 정보보안과 관련해서 행정자치부의 역할이 강화되었고 전자정부서비스보안위원회를 설치하여 보안대책의 수립·조정 및 제도개선 그리고 보안사고 발생시 대응조치를 신속히 할 수 있도록 하였다.[29)]

---

29) 제27조 (정보통신망 등의 보안대책 수립·시행) ①국회·법원·헌법재판소·중앙선거관리위원회 및 행정부는 전자정부의 구현에 요구되는 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안대책을 마련하여야 한다.
②행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 보안대책을 수립·시행하여야 한다.
③행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통함에 있어서 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.
④제3항의 규정을 적용함에 있어서 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 당해 기관의 장이 필요하다고 인정하는 경우에 한한다. 다만, 필요하지 아니하다고 인정하는 경우에는 당해 기관의 장은 제3항의 규정에 준하는 보안조치를 강구하여야 한다.

제39조의2 (전자적 대민서비스 보안대책) ①행정자치부장관은 전자적 대민서비스와 관련된 보안대책을 국가정보원장과 사전협의를 거쳐 마련하여야 한다.
②중앙행정기관과 그 소속기관 및 지방자치단체의 장은 제1항의 보안대책에 따라 당해 기관의 보안대책을 수립·시행하여야 한다.

제39조의3 (전자정부서비스보안위원회) ①제39조의2제1항의 규정에 따른 보안대책과 관련한 다음 각 호의 사항을 심의하기 위하여 행정자치부장관 소속하에 전자정부서비스보안위원회(이하 이 조에서 “위원회”라 한다)를 둔다.
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
②위원회는 위원장 1인을 포함한 20인 이내의 위원으로 구성한다.
③위원장은 행정자치부장관이 되고, 위원은 대통령령이 정하는 관계 중앙행정기관 및 지방자치단체의 공무원과 위원장이 위촉하는 자로 한다.
④위원회의 효율적인 운영을 위하여 위원회에 실무위원회를 둘 수 있다.
⑤위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

(3) 국가정보원

국가정보원은 국가사이버안전관리규정 등에 따라 범정부차원에서 국가사이버안전에 관한 조직체계 및 운영에 대한 업무와 사이버보안에 관련하여 국가안보를 위협하는 사이버공격행위로부터 국가정보통신망을 보호하고 있으며, 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대한 사이버공격의 대응을 총괄·조정하는 역할을 하고 있다. 이와 같은 역할을 수행하기 위하여 국가사이버안전전략회의 및 국가사이버안전대책회의 그리고 국가사이버안전센터를 두고 있다. 국가사이버안전센터는 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 하기 위하여 국가사이버안전정책의 수립, 사이버위협 관련정보의 수집·분석·전파, 국가정보통신망의 안정성 확인, 국가사이버안전 매뉴얼의 작성·배포, 사이버공격으로 인하여 발생한 사고의 조사 및 복구지원, 그리고 외국과의 사이버 위협 관련 정보의 협력을 그 업무로 하고 있다.

(4) 소 결

앞에서 살펴본 것처럼 각국에 있어서도 향후 지속적으로 종이문서에 의한 업무처리가 정보시스템을 이용하는 업무로 대체됨에 따라 정보시스템으로 처리되는 정보에 대한 보안은 중요하다.[30] 우리 나라에서는 정보시스템을 이용한 업무처리가 일반화됨에 따라 공공기관 상호간 또는 공공기관과 민간기업 상호간에 정보의 이용·제공 등이 활발하게 이루어지고 있다. 따라서 정보시스템으로 처리되는 정보보안은 공공분야에 국한되어 다룰 문제가 아니라 정보시스템을 이용하는 모든 영역

30) OECD는 1992년 정보시스템 보안지침(Guidelines for the Security of Information Systems)을 마련하여 회원국에게 정보화사회의 대비하여 정보시스템에 관련하여 정보보안을 강화하도록 권고하였다.

에서 직면하는 공통된 문제이다. 따라서 정보보안은 범정부차원에서 대응할 수 있는 집행체계를 마련되어야 하며, 국가차원의 정보보안관리를 총괄할 기관이 요구된다. 미국의 경우처럼 우선적으로 공공분야에서의 정보보안이 체계화되어야 하지만 최근 우리 나라의 환경변화에서도 알 수 있듯이 행정정보 등이 민간분야에도 광범위하게 이용·제공되고 있고 상호간에 개방된 통신망으로 연결되고 있어서 공공분야와 민간분야 모두를 포섭하는 정보보안의 도입이 요구된다.

현재 우리 나라에서 정보시스템으로 처리되는 정보에 대한 보안관리체계는 국가정보원을 중심으로 하는 공공분야의 정보보안과 정보통신부를 중심으로 하는 민간분야의 정보보안으로 이원화되어 있다. 물론 국방부는 국방분야와 관련하여 정보시스템의 정보보안에 대한 국방정보대응센터 등의 집행체계를 마련하고 있으며 다른 중앙행정기관 등도 자체적으로 운영·관리하는 정보시스템의 정보보안에 대한 물리적·관리적 차원의 보안조치를 하고 있다. 이를 도표화하면 다음과 같다.

[도표 2] 국가정보보안관리체계

제 2 절 집행체계의 개선방안

우리 나라의 경우 국가적으로 정보보안에 중대한 위기가 발생할 경우에 대비하여 국가주요정보통신기반시설의 보호 및 적극적 대응을 위해 「정보통신기반보호법」 및 「국가사이버안전관리규정」등이 마련되어 있는데, 업무영역이 민간분야와 공공분야로 구분되어 있어 기관간 상호협력은 물론 사고 초기 신속한 대응이 곤란할 뿐만 아니라 사고가 발생할 경우 책임 소재 또한 불분명하다. 따라서 다음과 같은 개선이 요구된다.

첫째, 범정부차원에서 정보보안을 컨트롤할 수 있는 총괄 책임기관을 지정하고 국가차원의 정보보안 업무의 역할과 책임을 부여하며 정보보안의 수립 및 추진할 필요가 있다. 현재 우리 나라의 정부조직에 비추어 새로운 기구를 만들지 아니하는 한 국가차원의 정보보안은 정보통신부의 업무와 가장 유사하다(국가정보원은 수사기관이라는 특수성이 있고, 행정자치부는 지방자치단체 등을 감독하는 지위에서 있지만 민간분야에 대하여는 관여하기가 어렵다 라는 특수성이 인정된다). 따라서 정보통신부를 총괄기관으로 하고 국가차원에서 공공분야와 민간분야를 총괄하는 역할을 부여할 수도 있다.

둘째, 각 부처 및 주요시설의 정보보안 담당전문기관 간 각종 정보보안을 위협하는 정보의 공유・협력을 의무화하고, 국가기관・지자체・공공기관이 기관별 정보보안대책을 수립함은 물론, 총괄책임기관이 각급 기관들에서의 이행여부 및 안정성을 확인하여 시정조치를 권고할 필요가 있다.

셋째, 침해행위 발생시 피해기관은 관련 책임기관에 신고를 의무화하고 책임기관은 피해확산 방지를 위한 조치를 병행 피해에 따른 사고 복구는 물론, 사고조사와 동시에 정보보안업무 전반에 대한 책임감을 갖게 해야 한다.

1. 정보통신부

정보통신부는 현재 민간분야의 정보보안을 총괄하는 지위에 있으며 주요정보통신기반시설의 보안에 관하여서도 실무상 총괄기관으로 지위를 차지하고 있다. 차후에 공공분야에 대하여 행정자치부(또는 현재처럼 국가정보원)의 총괄적인 지위가 인정된다고 하여도 정보통신보안기술이나 정책 및 보안집행체계상으로는 정보통신부가 국가차원에서 정보시스템으로 처리되는 정보보안을 총괄할 수 있다. 만약 이와 같은 역할이 주어진다면, 정보통신부 산하에 국가정보보안관리센터, 통신정보・공유분석센터, 정보보안기술연구원 등도 설치할 수 있다.

2. 행정자치부

행정자치부는 전자정부사업을 총괄하고 있는데, 성공적인 전자정부의 실현을 위해서 정보시스템의 정보보안은 필수적이다. 따라서 행정자치부가 지휘・감독하는 행정기관 및 지방자치단체 등에 관련하여 정보보안을 총괄적으로 감독하는 역할이 인정된다. 따라서 현재 국가정보원이 수행하고 있는 공공분야의 정보보안업무는 상당부분 행정자치부로 이관하는 것이 요구되고 관련법제도도 정비되는 것이 요구된다(전자정부법의 보안 관련조항에 대한 강화가 필요하다).

3. 국가정보원

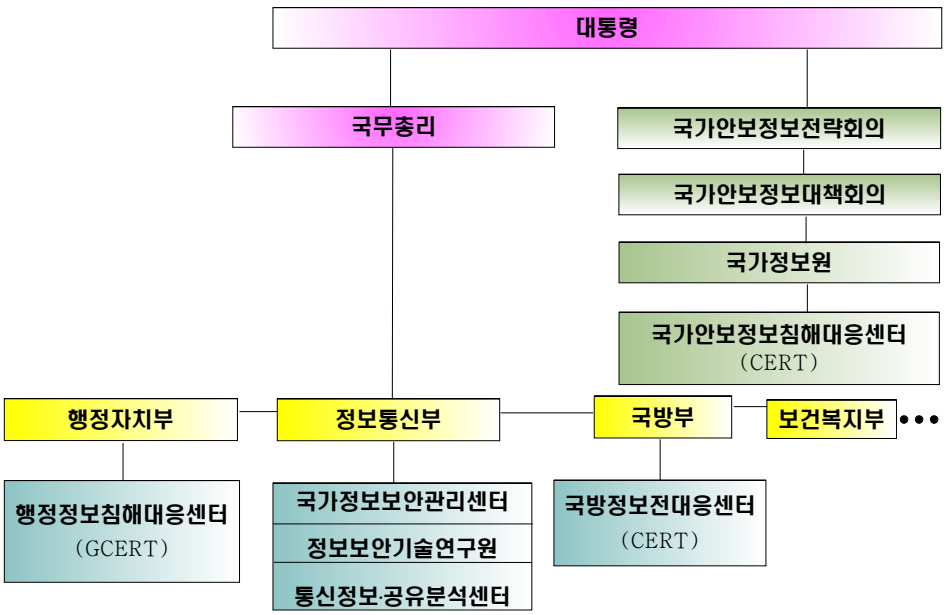
국가정보원은 국가사이버안전관리규정에 따라 공공분야의 정보보안관리에 대하여 중요한 역할을 수행하고 있는데, 해당 보안관리업무는 행정기관 등이 처리하는 통상적 업무처리에 해당되므로 정보통신부와 행정자치부로 이관하고, 국가정보원은 국가안보와 관련된 정보를 총괄하는 지위를 부여하는 것이 타당할 것으로 사료된다. 즉 국가차원의 정보보안을 정보통신부(공공분야는 행정자치부)가 총괄한다고 하여

국가안위에 관련해서 국가정보원의 법적 권한(예컨대, 정보보안의 침해행위가 국가안위에 영향을 줄 수 있는 경우에 공공분야와 민간분야의 기관으로부터 관련된 정보를 제공받거나 조사할 수 있는 권한 등)을 부여하지 않을 수 있다.

4. 소 결

이상에서 알 수 있듯이 정보시스템상의 정보보안은 국가안보나 국가안위에만 한정되는 것이 아니라 공공분야와 민간분야에서 공통적으로 직면하는 문제에 해당된다. 그러므로 국무총리가 범정부차원에서 정보통신부의 총괄하에 정보보안에 관련하여 각 중앙행정기관 등을 지휘·감독권을 행사하는 것을 고려할 수 있다. 물론 국가안보와 국가안전에 관련된 정보보안 등에 대하여는 국가정보원의 역할을 인정하지 않을 수 없다. 이상에서 살펴본 집행체계의 개선방안을 도식화하면, 다음과 같다.

[도표 3] 국가정보보안 관리체계



제 3 절 정보보안 관련법규

1. 관련법규의 현황

이미 고찰한 것처럼 정보보안 관련법제에는 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호에 관한 법률」, 「전기통신사업법」, 「정보화촉진기본법」, 「전파법」 등과 같은 정보통신부 소관법률과, 「국가정보원법」, 「국가사이버안전관리규정」, 「정보 및 보안업무 기획조정 규정」과 같은 국가정보원의 담당법령, 「전자정부법」과 같은 행정자치부 소관법률, '형법'과 같은 법무부 소관법률 등이 포함된다.

우리나라의 정보보안 관련법제는 많은 법률에 산재한 여러 규정을 가지고 있고, 정보보안을 위한 정책의 수립과 조정, 집행을 위해서 정부와 민간이 어떻게 협업을 하고, 정부의 여러 부처가 어떻게 권한과 의무를 분배하며, 이렇게 분배된 권한과 의무를 어느 조직이 조정·통합할 것인지에 대한 원칙에 대한 합의가 없이 단편적으로 입안되고 시행되고 있다고 할 수 있다. 따라서 우선 법제의 개선을 위해서는 이러한 기본적 사항에 대한 원칙적인 합의를 도출하고 이에 근거한 체계적인 법의 제·개정이 필요하다.

현재 범정부차원에서 정보보안은 실질적으로는 국가정보원과 정보통신부가 하고 있다. 그런데 공공분야와 민간분야의 역할구분은 정보통신부의 경우에는 관련 보안업무에 관한 독립된 법령을 마련하고 있어서 법형식상 적절한 것으로 볼 수 있지만, 국가정보원의 경우에는 법률차원에서 관련된 공공분야 정보보안의 업무처리에 대하여 그 근거가 희박하고 실질적으로는 국가사이버안전관리규정이라는 대통령훈령에서 규율하고 있다. 후자는 아래에서 다루겠지만 규율하고 있는 내용에 비추어 대부분 법률차원에서 규율하는 것이 바람직하고 관련 행정기관 및 공공기관 등의 적극적 협조를 이끌어 내기 위해서도 법률차원에서 규율되어야 할 내용이라고 사료된다.

2. 관련법규의 문제점과 개선방안

(1) 관련법규의 문제점

앞에서 살펴본 법규들은 나름대로의 필요에 따라 해당 집행기관을 중심으로 소관업무를 확대하는 방식으로 정보보안관리를 수행하고 있다. 그런데 이와 같은 보안관리체계는 개방된 망을 통하여 상호 연계되어 있는 환경에 적절히 대응하기가 곤란하다. 즉 범정부차원에서 정보보안의 문제는 통일적이고 체계적인 총괄기관에 의하여 관리될 필요가 있다. 이와 관련해서 실무상으로 주로 문제되는 것은 다음과 같다.

첫째, 우리나라의 정보보안 대응법률은 여러 가지의 관련법규에 분산되어 있으므로 일관성을 유지하기 어렵다. 정보보안 관련 법령이 여러 곳에 분산되어 법적용에서 중복과 책임의 한계가 불분명하고 일관성 있는 통제에 어려움이 있으므로 단일한 법제정의 필요성이 문제된다. 이와 관련해서 공성진의원 대표발의로 「사이버위기 예방 및 대응에 관한 법률안」이 국회에 제출되어 있지만 여기서 다루고자 하는 (가칭)정보보안관리법과는 구별된다.

둘째, 집행기관 간에 협조체계가 미흡하다. 예컨대, 정보통신기반보호법상 주요정보통신기반시설에 대한 지정은 기본적으로 각 부처가 지정하는 것으로 되어 있기 때문에 그 부작용으로 나타난 현상이 2003년 정보통신부와 한국정보보호진흥원(KISA)의 자체 조사결과에 따른 제3차 주요정보통신기반시설의 지정이 부처간의 협의 지연을 이유로 미루어진 바 있다. 주요기반시설에 대한 침해행위가 발생한 경우 엄청난 피해가 발생할 가능성이 있다는 점에 비추어 보면 법 개정을 통해 주요정보통신기반시설의 보호에 대해 모든 사항을 책임지고 통합하는 기구의 마련이 요구된다. 또한 2003년 1・25 인터넷 대란을

겪으면서 이러한 문제를 해결키 위해 국가정보원에 국가사이버보안의 실질적인 총괄기구라고 할 수 있는 국가사이버안전센터를 두었지만 주요정보통신기반시설은 제외하고 있으므로 유사시 혼선이 우려된다. 국가사이버안전센터가 총괄기구로서 역할을 하려면 인터넷침해사고대응지원센터와 국방정보전대응센터를 비롯해 각종 정보공유분석센터와 일반기업의 컴퓨터침해사고대응팀(CERT)까지 아우르는 정보공유체제가 구축돼야 하는데 현재는 이에 대한 명확한 법적 근거가 없는 것이 문제이다.

셋째, 침해사고 대응센터의 협조체계가 미흡하다. 정보통신망법은 제52조에서 “정부는 정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위하여 한국정보보호진흥원을 설립한다”라고 하여 한국정보보호진흥원을 1996년 4월에 설립하였고, 2003년에는 진흥원내에 인터넷침해사고대응센터를 운영 중에 있다. 또 국가사이버안전관리규정은 제8조제1항에서 국가사이버안전센터를 설치하고 있다. 공공부문에 대한 보안은 주로 국가정보원에서 책임지도록 규정하고 있고, 민간부문의 안전은 정보통신부가 맡도록 규정하고 있다. 그러나 이러한 권한 분산은 공공부문과 민간부문의 모든 정보시스템이 유기적으로 연결되어 있는 사이버환경에서 국가차원의 정보보안에 대한 대응체계가 이원화되어 불합리한 측면이 있다. 더욱이 유사한 업무를 국가차원에서 통합·지휘할 수 있는 기관이 불분명하여 일관성 있는 대응이 어렵다는 점, 평시·위기시 및 정책결정에 있어 실무집행 주관기관이 상이하여 혼란을 주고 있다는 점, 각 센터 간 정보공유 및 협조체제가 미미하고 유관기관 간 협조유지 규범이 부재하여 기관 간 공조가 혼선을 초래하고 있다는 점이 문제로 제기될 수 있다.

넷째, 위험수준 단계별로 경보발령 및 대응요령의 제도화가 미흡하다. 긴급사태 발생시 신속하고 체계적으로 대응하기 위한 예·경보체계 구축과 연계하여 정보보안의 위험수준을 평가하여 적정등급을 발

령하고 등급에 맞도록 대응하는 위험단계 및 대응요령 등의 대처방안이 수립되어야 할 것이다. 현재 국가사이버안전관리규정에 의하여 정상, 관심, 주의, 경계, 심각의 5단계로 구분하여 이에 대한 대처요령이 마련되어 있으며 경보협의회를 운영하도록 되어 있으나 대통령 훈령으로 되어있는 규정으로만 규제하고 통제하기에는 미흡하다. 따라서 평시와 긴급상황에서의 침해행위로부터 효율적으로 대처하기 위해서는 국가안보차원의 대응체계 식별과 기관별 역할, 경보 발령 및 행동요령 등이 관련법으로 명시되어야 할 것이다. 이러한 경보 발령 및 단계별 대응은 범국가적으로 적용되어야 하고, 위험수준을 판단하고 발령하는 최고의 판단기관과 이에 따른 경보발령을 접수・전파하는 부문 기관의 유기적 협조체제가 조성되도록 하여야 한다.

다섯째, 국제적 협력체제가 미흡하다. 사이버공간에서 발생하는 각종 침해행위는 국내에만 국한되는 문제가 아니며, 인터넷을 비롯한 정보시스템의 특성으로 말미암아 미국에서 발생한 웜이나 바이러스가 국내에 즉시 유입되고 있으며 특히 해킹사고는 대부분 중간경유지를 통과하여 일어나기 때문에 다른 어떤 분야보다도 침해의 예방과 사후처리를 위하여 국제간의 협력 증진은 중요한 과제라고 할 수 있다. 우리 정부도 정보보안 분야에서 국제적 협력의 중요성을 인식하고 많은 노력을 기울이고 있으나 아직도 미흡한 것이 사실이며, 침해행위에 관한 신속한 정보공유를 위한 국가 간 합의와 구체적인 실천 방안이 아직 충분히 마련되어 있지 못하다.

(2) 관련법제의 체계화와 (가칭)정보보안관리법의 제정 필요성

1) 정보통신기반보호법과 국가사이버보안관리규정의 통합

위에서 살펴본 정보보안과 관련된 문제는 법체계의 개선과 관련된 내용의 개정을 통하여 이루어질 수밖에 없다. 무엇보다도 정보보안관리 집행체계의 체계화는 정보통신부와 국가정보원이 수행하고 있는 보안

관리업무의 체계화와 관련법제의 체계화가 선행된 이후에 관련기관의 통합화 내지는 단일화를 논의할 수 있다. 따라서 정보통신부 소관의 정보통신기반보호법과 국가정보원의 국가사이버안전관리규정은 상호 규율하고 있는 대상을 구분하고 있지만 그 내용상으로는 상호 유사하다. 따라서 정보보안관리의 효율성을 위해서 이를 통합하는 것이 타당하다.

2) 정보통신망법의 분법화와 개선방안

①분법화 방안

정보통신망법은 앞에서 지적했듯이 상호 상이한 내용을 하나의 입법에서 규율하는 입법형식은 정보통신기술의 도입 초기에 적합한 형태이고 정보통신기술의 발달과 활용이 넓혀지고 규율하는 입법사항이 보다 복잡하고 다양화됨에 따라 분법화가 요구된다. 다시 말해서 현행 정보통신망법은 우리 나라가 고도화되고 선진화된 정보사회로 진입함에 따라 분법화가 필요하다. 정보보안과 관련하여 정보통신망법의 분법화은 첫째, 정보통신망법은 분법화하는 것이 바람직한데, 구체적으로 제2장 '정보통신망의 이용촉진'은 정보화촉진기본법으로, 제6장 '정보통신망의 안정성 확보(제49조의2 내지 제50조의8은 제외)'는 (가칭)정보보안관리법으로, 제4장 '개인정보의 보호'는 별도의 입법((가칭) 정보통신망상의개인정보보호에관한법률)에 포함시킬 수 있다(정보통신망법 제3장은 『전자거래기본법』에 '전자문서보관소제도'가 도입됨으로서 그 실효성을 상실되었으므로 이를 삭제해도 특별한 문제가 없다고 판단된다).[31] 제5장 '청소년보호'는 청소년보호법의 정보통신서비스와 관련된 청소년 보호조항과 통합하여 하나의 새로운 입법의 형태('(가칭)정보통신망상의청소년보호에관한법률)로 추진하거나 청소년보호법에서 통신망

31) 또한 시행이 이루어지고 있지 아니한 조항의 보완이 요구된다. 즉 정보통신망법 제8조(정보통신망의 표준화 및 인증) 및 제9조(인증기관의 지정 등)는 지금까지 시행이 보류된 상태인데, 이와 관련하여 정보시스템의 표준화 및 인증 등으로 개선하는 것이 요구된다.

상의 청소년보호를 모두 편입하여 정보통신망법의 청소년보호를 삭제하는 방법도 가능하다.

둘째, 또한 정보통신망법의 분법화한다면, 정보화촉진기본법으로 이관이 필요한 사항은 제2장인데, 그 중에서도 제12조 (정보의 공동활용체제 구축), 제13조 (정보통신망의 이용촉진 등에 관한 사업), 제14조 (인터넷이용의 확산), 제15조 (인터넷서비스의 품질개선) 등을 들 수 있다. 반대로 정보화촉진기본법에서 (가칭)정보보안관리법으로 이관이 요구되는 사항으로 제14조(정보보호등)와 제15조(정보보보시스템에 관한 기준고시 등)가 있다. 즉 정보화촉진기본법은 기본법으로서의 성격에 맞게 정보보안에 관한 기본적인 사항만을 규율하고, 보안과 관련된 실체적인 내용은 (가칭)정보보안관리법에서 규율할 수 있다.[32)]

②개선방안

정보통신망법은 다음과 같은 개선이 요구된다.

첫째, 안전진단 수행기관의 사후관리 강화방안의 마련(예컨대, 일정규모 이상의 집적정보통신시설사업자만 안전진단을 받도록 함)이 요구된다. 이를 위하여 정보보호시스템에 관한 기준고시 등이 필요하다.

둘째, 침해사고 예방 및 대응과 관련하여 이용자에 대해 정보통신서비스제공자가 취할 조치사항의 개선이 요구된다. 즉 침해사고에 대한

32) 제14조 (정보보호등) ①정부는 정보의 안전한 유통을 위하여 정보보호에 필요한 시책을 강구하여야 한다.
②정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구하여야 한다.

제15조 (정보보호시스템에 관한 기준고시등) ①정보통신부장관은 관계기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 이를 고시하고, 정보보호시스템을 제조하거나 수입하는 자에 대하여 이 기준의 준수를 권고할 수 있다.
②정보통신부장관은 유통중인 정보보호시스템이 제1항의 규정에 의한 기준에 미치지 못할 경우에 정보보호시스템의 보완 기타 필요한 사항을 권고할 수 있다.
③제1항의 규정에 의한 기준고시와 제2항의 규정에 의한 권고 기타 필요한 사항은 대통령령으로 정한다.

민·관 공동대응시스템의 구축이 요구된다.

셋째, 안전진단 수행기관 관리·감독규정 신설 등 안전진단 수행기관 사후관리 강화를 통한 안전진단제도의 실효성 확보가 요구된다. 정보보호관리체계 인증 또는 취약점 분석·평가 수검 사업자에 대한 안전진단 면제요건의 명확화가 필요하다. 즉 평가항목 등을 조정하여 중복점검의 최소화가 요구된다. 그리고 안전진단 의무대상 사업자의 범위를 명확히 하여 사업자간 형평성 제고가 요구된다.

넷째, 인증심사 수행기관을 한국정보보호진흥원에서 정보보호컨설팅 전문업체로 확대하는 정보통신망법 개정안이 국회 통과('06.12.22)에 따라서 인증심사의 부실방지 및 품질 제고를 위해 정보보호컨설팅전문업체에 대한 관리·감독 규정의 신설이 요구된다.

다섯째, 정보보호 안전진단, 정보보호 관리체계인증, 정보보호시스템 평가·인증 등의 분야에서 점차 한국정보보호진흥원와 정보보호업체간 차별성이 희소되고 있어서 한국정보보호진흥원의 역할을 정보보호업체에 대한 관리·감독 대행기구로 특화가 요구된다.

여섯째, 인터넷 침해사고 고도화에 대응이 요구된다. 구체적으로 ⅰ) 해킹수법, 침해사고 등의 다양화·고도화에 대한 대응능력의 제고가 요구된다. 즉 침해사고, 악성프로그램 등의 유형과 판단기준을 구체화할 수 있는 법적 근거를 마련하여 법률 집행의 투명성과 명확성 확보가 요구된다. ⅱ) 한국정보보호진흥원의 침해사고 예방활동 강화 및 법적근거 마련이 요구된다. 즉 자동화 장치에 의한 취약점 원격점검·분석 등 한국정보보호진흥원의 침해사고 예방활동에 대한 법적 근거의 마련이 필요하다. ⅲ) 정보통신서비스제공자의 정보보호에 대한 협력의무의 강화가 요구된다. 즉 정보보호 최저기준의 준수 의무화 검토가 요구되고, 침해사고 예방활동에 필요한 회선용량, 회선사용율, 공격정보 등에 관한 자료제공 의무화가 요구되며, 침해사고에 대한 긴급 대응조치에 필요한 가입자의 연락처정보 등 제공의무화(악성

코드 유포사이트, 홈페이지 변조, 악성봇 감염 IP 등)가 요구된다. 또한 사이버 침해사고에 대한 민·관 공동대응시스템을 구축하기 위하여 정통부(한국정보보호진흥원)와 국가정보원간 상호 협력 네트워크의 제도화하는 것이 논의되고 있는데 근본적으로는 (가칭)정보보안관리법에 의한 통합도 고려할 수 있다.

일곱째, 법률 적용 사업자와 면제 사업자의 명확화, 각종 원칙·기준 등의 구체화 등을 통해 법률의 투명성과 명확성을 확보가 필요하다.

(3) (가칭)정보보안관리법의 제정 필요성

위에서 살펴본 바와 같이 국가차원에서 정보보안관리체계를 마련하고 집행과정에서 나타나는 문제점 등을 개선하기 위해서는 근본적으로 (가칭)정보보안관리법의 제정을 통하여 범국가차원의 집행체계를 마련하는 것이 요구된다. 여기서 (가칭)정보보안관리법은 순수한 정보의 보호에 관한 법률이 아니라 업무(사무)가 전산화되어 전자적으로 처리되는 보안관리를 그 내용으로 하고, 그 규율하는 대상은 정보시스템으로 처리되는 모든 정보이다. 따라서 이 법은 개인정보의 보호를 그 규율대상으로 하는 것이 아니라 정보의 보호가치에 상관없이 (인격적 이익 또는 재산적 이익에 관련된 것인지와 상관없이) 정보의 무결성·비밀성·이용가능성을 보호한다. 이 법에서 규율하는 내용은 아래에서 살펴보겠지만 근본적으로 정보통신기반보호법, 정보통신망법과 정보화촉진기본법 및 국가사이버안전관리규정 등을 통합 내지는 일부 발췌하여 새로운 입법을 하므로 현행법상 개정이 필요한 사항은 당연히 (가칭)정보보보안관리법에서 문제된다. 다시 말해서 현행 정보통신망법상의 보안관리에 관련된 조항의 개선문제와 정보통신기반보호법 및 국가사이버안전관리규정 자체에 대한 개선문제도 (가칭)정보보안관리법의 제정에 포함된다.

제 5 장 새로운 정보보안 관련법제 구상

제 1 절 개 요

위에서 서술한 것처럼 이 보고서에서는 정보보안 관련법제의 개선방안으로 정보통신기반보호법과 국가사이버보안관리규정을 통합하고, 정보통신망 이용촉진 및 정보보호에 관한 법률을 분법화하는 것을 살펴보았다. 그리고 도처에 산재하여 있고 때론 중복되어 있는 정보보안에 관한 규범내용 중 범국가차원의 집행체계에 관한 내용과 정보보안에 관한 기본적인 내용을 하나의 법규범으로 성안하여 '(가칭) 정보보안관리법'을 제정할 것을 주장하였다.

여기서는 '(가칭)정보보안관리법'의 제정을 함에 있어, 기존의 현행법이 규율하고 있는 내용은 다루지 아니하고 새로 추가되어야 할 내용과 전체적인 구성체계(정보통신망법의 보안관리에 관한 조항, 정보통신기반보호법, 정보화촉진기본법과 국가사이버안전관리규정의 보안관리에 관한 조항 등)를 마련하는 것을 중심으로 서술하고자 한다.

제 2 절 (가칭) 정보보안관리법의 제정방안

1. 목적 및 적용범위

(1) 목 적

(가칭)정보보안관리법의 제정은 정보자원에 대한 정보보안 통제의 효과를 보장하기 위한 총체적인 틀을 제공하고, 정보보안 위험에 대한 범정부 차원의 효과적인 관리 및 감독을 가능하게 하는 것을 의도한다. 또한 정보 및 정보시스템의 보호에 필요한 최소한의 통제수단을 개발 및 유지하며 정보보안 프로그램의 이용에 대한 감독체계를 마련하는 것을 목적으로 한다.

여기서 정보시스템으로 처리되는 정보의 보안은 관리적·물리적·기술적 수단을 강구하는 일체의 행위를 말하며, 정보보안이라 함은 정보의 무결성, 비밀성 및 이용가능성을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것을 의미한다.[33]

(2) 적용범위

(가칭)정보보안관리법은 공공분야와 정보보안관리 집행체계를 통합하는 법이다. 따라서 현행 정보통신기반보호법과 국가사이버안전관리규정의 통합이 필요하다. 따라서 현행 정보통신기반보호법이 정의하고 있는 주요정보통신기반시설과 국가사이버안전관리규정이 적용되는 대상이 다소 상이하므로 중앙행정기관, 지방자치단체 및 공공기관의 정보시스템을 포함하여 주요 민간기업의 정보시스템과 사설 인터넷망 전체로 적용범위를 확대할 필요가 있다. 따라서 (가칭)정보보안관리법은 모든 정보시스템의 정보보안관리에 적용된다. 다만, 국방부 및 국가정보원에서 구축·운영하는 정보시스템의 경우에는 일정한 예외가 필요하다.

2. 정보통신부의 권한 및 역할

(가칭)정보보안관리법에서는 정보통신부가 국가차원의 정보보안을 총괄하는 기구로 지정할 수 있다. 따라서 정보통신부 장관은 ①정보보안 정책, 원칙, 표준 및 지침의 개발과 시행을 감독하고 ②행정기관 등이 이용 또는 운영하는 정보 또는 정보시스템에 대한 정보보안 조치를 인증 및 제공한다. ③일정한 기간(예컨대, 최소 1년마다) 사용하고 있는 정보보안 프로그램 검사 및 승인 등을 하고 ④정보보안과 정보자원 관리정책 및 절차를 조정할 수 있다. 또한 ⑤국가정보보안관

33) 미국의 연방정보보안관리법 제3542조 참조

리센터를 두고서 운영을 감독하고 ⑥국회 등에 정보보안 정책 및 업무를 보고하는 것이 요구된다. 이외에도 정보통신부 장관은 ⑦정보보안기술연구원을 두고서 표준 및 지침의 개발과 관련하여 국가보안시스템을 운영하거나 통제하는 기관 등의 업무를 조정하여 가능한 최대한의 범위에서 표준 및 지침이 국가보안시스템용으로 개발된 표준 및 지침을 보충할 수 있도록 하여야 하는 역할을 인정할 수 있다.

3. 집행기관의 임무 등

(1) 기관장의 책임

(가칭)정보보안관리법은 정보통신기반보호법을 통합하는 방식으로 입법할 수 있다. 따라서 각 기관의 장은 정보보안에 관한 정책, 절차, 표준, 지침 등을 준수하여 기관의 전략적 목표에 따라 정보 및 정보시스템에 대한 정보보안 조치를 강구하도록 하고, 기관의 장은 이 권한을 당해 기관의 책임자에게 위임할 수 있도록 하는 것이 필요하다.

(2) 정보보안 프로그램

(가칭)정보보안관리법에서 각 기관은 정보 및 정보시스템에 대한 보안을 위하여 기관단위의 정보보안 프로그램을 개발 및 시행하도록 함이 타당하다. 따라서 동 프로그램은 ①정보 및 정보시스템의 보안상 위험에 대한 주기적인 평가 ②정보보안 위험의 감소 및 정보시스템의 수명주기에 맞는 정보보안 유지 등을 위한 정책 및 절차 ③보안교육 ④정보보안에 관한 정책, 절차 및 업무상의 여하한 결점에 대한 평가 및 이에 따른 구제조치를 계획, 시행, 평가 및 기록하기 위한 과정 ⑤보안사고에 대한 탐지, 보고 및 대응을 위한 절차 ⑥정보시스템에 대한 영속적 운영을 위한 계획 및 절차 등이 포함되는 것이 필요하다.

(3) 보고의무

(가칭)정보보안관리법에서 각 기관은 정보보안에 관한 정책, 절차, 업무의 적절성 및 효과 등에 관하여 보고하도록 하는 것이 요구된다. 또한 각 기관은 정보통신부장관에게 정보보안 과정에서 확인된 정책, 절차 또는 업무상의 여하한 중대한 결함에 대해서도 보고할 필요가 있다.

4. 지원기관의 설치 및 운영

(1) 국가정보보안관리센터

정보통신부장관은 국가정보보안관리센터를 운영하는 것이 필요하다. 따라서 동 센터는 ①보안사고와 관련하여 기관의 정보시스템 운영자에 대하여 정보보안사고의 탐지 및 수습에 관한 지침 등 기술적 지원을 제공하고 ②정보보안을 위협하는 사고에 대한 정보를 수집하고 분석한다. 또한 ③정보시스템 운영자에 대하여 현존 및 잠재적 정보보안 위협과 취약부분에 관한 정보를 제공하고 ④정보보안 사고 및 관련문제를 정보보안기술연구원, 국가보안시스템을 운영 또는 통제하는 기관 및 법령에 따라 다른 기관과 협의하도록 한다. 국가보안시스템을 운영 또는 통제하는 각 기관은 국가보안시스템에 대한 표준 및 지침과 일치하는 범위 내에서 정보보안사고, 위협 및 취약부분에 관한 정보를 국가정보보안관리센터와 공유하도록 하는 것이 요구된다. 또한 ①정보보안에의 위험에 관한 정보를 수집, 분석하여 정보통신부장관에게 제공 ②행정기관등 유관기관에 대한 자문 및 지원 ③산·학·관·연간 정보보안에 관한 협력 증진 ④정보보안에 관한 국민인식과 보안위험경고와 우수사례 제공을 통한 정보문화 확산 ⑤보안제품과 서비스의 기준개발에 참여하고 위험측정 장려 ⑥정보보안과 관련한 국제협력 등을 수행하도록 한다.

한편, 현행 정보통신망법상 한국정보보호진흥원이 (가칭)국가정보보안관리센터와 유사한 역할을 하고 있는데, (가칭)정보보안관리법의 제정이 이루어진다면 한국정보보호진흥원의 역할[34]이 대폭적으로 조정되는 것은 불가피하다.

(2) 정보보안기술연구원

(가칭)정보보안기술연구원은 현재 국가보안기술연구소의 보안기술과 관련된 업무와 다른 국가기술표준화기관에서 수행하고 있는 정보통신 보안 표준화 기술정책과 관련된 업무를 통합하여 수행하는 것이 요구된다. 따라서 첫째, (가칭)정보보안기술연구원은 정보시스템에 관한 표준, 지침 및 관련방법 및 기술을 개발할 임무가 있다. 둘째, 국가보안시스템을 제외한 기관, 기관과 계약을 맺은 자, 또는 기관을 대신하는 다른 조직에 의하여 이용되거나 운영되는 정보시스템과 관련하여 최소요건을 포함하는 표준 및 지침을 개발하여야 한다. 셋째, 기관의 모든 업무 및 자산에 대하여 적절한 정보보안을 제공하기 위한 최소요

34) 한국정보보호진흥원은 정보통신망법 제52조제3항에 의하여 다음과 같은 업무를 수행하고 있다.
①정보보호를 위한 정책 및 제도의 조사・연구
②정보화 역기능 분석 및 대책 연구
③정보보호에 관한 홍보 및 교육・훈련
④정보보호시스템의 연구·개발 및 시험・평가
⑤정보보호시스템의 성능과 신뢰도에 관한 기준 제정 및 표준화 지원
⑥정보통신서비스제공자등에 대한 정보보호 안전진단의 지원
⑦정보보호를 위한 암호기술 개발
⑧개인정보보호를 위한 대책의 연구 및 보호기술의 개발・보급의 지원
⑨분쟁조정위원회의 운영지원 및 개인정보침해신고센터의 운영
⑩불법전송광고와 관련된 고충의 상담·처리
⑪정보시스템 침해사고 처리 및 대응체계 운영
⑫침해사고의 원인분석 지원
⑬『전자서명법』 제25조제1항의 규정에 의한 전자서명 인증관리
⑭제1호 내지 제10호의 사업에 부수되는 사업
⑮그 밖에 이 법 또는 다른 법령에 의하여 보호진흥원의 업무로 정하거나 위탁한 사업 또는 정보통신부장관으로부터 위탁받은 사업

건을 포함하는 표준 및 지침을 개발하도록 한다. 다만, 이와 같은 표준 및 지침은 예외적으로 국가정보원이나 국방부 등의 국가보안시스템에는 적용되지 아니하는 예외를 허용한다.

(3) 정보공유・분석센터

정보보안의 위협은 날이 갈수록 급격히 증가하고 있는 실정이어서 침해행위를 신속히 탐지하여 분석하고 관련정보를 공유하여 사고를 미연에 방지하는 것이 중요하다. 다시 말해서 점점 첨단화・지능화되고 있는 해킹이나 웜바이러스의 보안 위해요인 및 공격유형 등을 신속하게 탐지하고 종합적으로 분석하기 위해서는 우선 보안관제 활동이 필요하며 이를 통하여 획득한 통신망의 트래픽 정보 또한 외부로부터의 사이버공격을 차단하는데 매우 유용하다. 그래서 정보통신기반보호법은 제16조제1항에서 금융・통신 등 분야별 정보통신기반시설을 보호하기 위하여 정보공유・분석센터를 구축・운영할 수 있도록 하였으며, 이 센터는 취약점 및 침해요인과 그 대응방안에 관한 정보제공, 침해사고가 발생하는 경우 실시간 경보・분석체계 운영을 그 업무로 하였다.

그러나 국내 인터넷 네트워크에 대한 모니터링 자체는 현행 '통신비밀보호법' 제3조[35]에 위배될 소지가 있어 법리적 시비의 요소가 있는 것이 현실이다. 현재 정보통신부의 정부통합전산센터나 국가기간통신사업자가 운영하는 통신정보공유분석센터(일명 통신 ISAC), 금융기관에서 운영하는 금융정보공유분석센터(일명 금융 ISAC) 등에서 수행하고 있는 보안관제 활동의 중요성에 비추어 이러한 업무를 보장해주는 법적인 근거를 보다 강화할 필요가 있다. 이와 관련해서 정보통

35) 통신비밀보호법 제3조(통신 및 대화비밀의 보호) ①누구든지 이법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열, 전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.

신기반보호법에서는 정보공유·분석센터의 업무를 취약점 및 침해요인과 그 대응방안에 관한 정보 제공 및 침해사고가 발생하는 경우 실시간 경보·분석체계 운영을 주 내용으로 한다. 그렇지만 실제적으로는 자사 및 회원사들의 정보나 취약점이 노출될 것을 우려하여 상호 정보교류가 형식적인 수준에 머무르고 있다는 비판을 받고 있다. 정부가 현재 정보공유분석센터의 구축을 장려하고 그에 대한 기술지원을 강화하는 가운데 이를 더 강력히 추진하고 지원하면서 필요한 정보를 상호 협조할 수 있도록 하기 위해 주요 업무를 좀 더 구체적으로 명시할 필요가 있다.

5. 국가정보보안시스템의 표준 제정 및 이행

(1) 표준 및 지침의 제정

정보통신부장관은 (가칭)정보보안기술연구원에서 개발한 표준 및 지침을 기초로 국가정보보안시스템에 대한 표준 및 지침을 제정하는 것이 필요하고, 국가정보보안시스템에 대한 표준 및 지침은 법령 등에 따라 개발, 제정, 집행 및 감독하는 것이 요구된다.

(2) 강제요건

정보통신부 장관은 국가정보보안시스템의 운영 또는 보안의 효율성을 개선하기 위하여 필요하다고 인정되는 범위 내에서 제정된 표준을 강제력 및 구속력을 가지도록 할 필요성이 있다.

(3) 정보통신부 장관의 불승인 또는 변경권

정보통신부장관은 국가정보시스템의 표준 및 지침의 불승인 또는 변경하는 것이 공익을 위한 것이라고 판단한 경우에는 불승인 또는 변경할 수 있다. 이 경우 각 기관의 장은 당해 기관의 감독 범위 내

에 있거나 감독을 받는 정보시스템에 관련하여 정보통신부 장관이 제정한 표준보다 더 엄격한 표준을 활용할 수 있다. 다만, 보다 엄격한 표준은 최소한 정보통신부 장관에 의하여 강제력과 구속력을 가지는 적용가능한 표준을 포함하여야 하며, 관련 정책 및 지침과 합치하도록 함이 바람직하다.

제 6 장 결 론

2006년 현재 UN 전자정부준비지수 세계 제5위, 미국 브라운대학 전자정부평가 세계 제1위, IDC 정보사회지수 세계 제10위, 국제전기통신연합(ITU) 디지털기회지수(DOI) 세계 제1위로 상징되는 정보통신 선진국인 우리나라의 정보통신분야를 규율하는 정보통신관련법제는 정보화 추진체계와 인프라구축, 신뢰성·안전성 확보기반에서 정보통신서비스에 관련된 법제로 확대되고 있다. 그러나 여전히 신뢰성·안전성 확보기반이라고 불리우는 개인정보보호·정보보안·정보격차해소영역의 법제는 여전히 충분히 정비되어 있지 못하다. 그 중에서도 정보보안영역은 관련법제의 범위에 관해서도 진지한 고민이 없을 정도로 이론과 실무 양 측면에 있어서 저발전되어 있다. 이 보고서에서는 현행 정보보안 관련법제의 문제점을 분석하고 그 개선방안을 도출하는 것을 목적으로 정보보안을 정의하고 그 특징과 정보보안을 위협하는 침해요소에 관해 살펴보고, 현행 정보보안 관련법제를 개관하였다. 그리고 정보보안 선진국인 미국 정보보안 관련법제의 현황과 내용을 살펴보며, 우리에게 주는 시사점을 도출하였다. 이어서 현행 정보보안 관련법제의 문제점을 분석하고, 정보보안 관련법제의 개선방안을 도출하였다. 이상의 논의를 정리하면 다음과 같다.

첫째, 정보보안이란 정보의 무결성, 비밀성 및 이용가능성을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다. 우리 실무계에서는 정보보호라는 용어를 사용하는 경우도 있으나, 정보보호는 정보보안과 다른 용어이다. 이 보고서는 정보보안을 물리적 보안, 기술적 보안, 관리적 보안으로 분류하였으며, 해킹, 바이러스 유포 등 정보통신에 대한 위협도 이러한 분류에 따라 분류할 수 있다.

둘째, 우리나라에서는 아직까지 정보보안 관련법제의 범위에 대한 일반적인 합의가 존재하지 않는다. 이 보고서는 정보보안의 개념론을 전개하며, 이를 제시하는 방법을 사용하였다. 이에 따라 확정된 정보보안 관련법제에는 개인정보보호와 영업비밀보호와 같은 정보의 내용의 보호와 관련된 법제는 제외하고, 전자인증관련법제는 포함하였다. 결론적으로 현행 정보보안 관련법제는 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호에 관한 법률」, 「전기통신사업법」, 「정보화촉진기본법」, 「전파법」 등과 같은 정보통신부 소관법률과, 「국가정보원법」, 「국가사이버안전관리규정」, 「정보 및 보안업무 기획조정규정」과 같은 국가정보원의 담당법령, 「전자정부법」과 같은 행정자치부 소관법률, 「형법」과 같은 법무부 소관법률, 그리고 인증을 규율하고 있는 「전자서명법」과 「전자정부법」 등을 그 내용으로 한다.

셋째, 올바른 문제의식과 처방을 제시하기 위해 정보보안 선진국인 미국의 정보보안 관련법제를 고찰하였다. 미국은 1987년 컴퓨터보안법(Computer Security Act of 1987), 1990년 OMB Circular A-130, 2000년 정부정보보안개혁법(Government Information Security Management Act of 2002), 국토안보법, 정부정보보안관리법(the Federal Information Security Management Act 0f 2002), 애국자법과 그 개정법 등을 제정하였다. 이러한 미국 정보보안 관련법제의 특징은 (ⅰ) 추진체계에 있어서 관련기관의 기능에 따른 권한과 책임의 분산, 이러한 기관들의 수평적 협업을 통한 목표의 달성, (ⅱ) 전자정부기금의 조성을 통해 관련 재원을 안정적으로 확보하고 지원, (ⅲ) 정보보안과 그 대척점에 서 있는 편리성의 조화점을 합의하고 그에 바탕한 입법을 한다는 점 등을 꼽을 수 있다.

넷째, 정보통신이 발전하면서 정보시스템의 보안에 대한 관심이 점차 커질 것이다. 정보보안은 공공분야만의 문제가 아니라 모든 영역에서 직면하는 공통된 문제이다. 따라서 정보보안은 범정부차원에서

대응할 수 있는 집행체계를 마련되어야 한다. 현재 우리나라의 정보보안관리체계는 공공분야는 국가정보원이, 민간분야는 정보통신부가 총괄기관으로 기능하고 있다. 그러나 필자는 이러한 이원적 체제는 개방된 망을 통하여 상호 연계되어 있는 환경에서 보안을 유지해야하는 현재의 정보보안의 성격상 사고예방과 사고처리 모두에서 문제가 있다고 생각한다. 따라서 미국과 유사하게, 정보통신부를 총괄기관으로 하고, 유관기관 협력시스템을 갖추는 추진체계를 제안하였다.

다섯째, 현행 정보보안 관련법제를 살펴보면 그 내용이 여러 법규에 산재하여 있고 때론 중복되어 있어, 법적용 단계에서 문제가 있다. 그리고 유관기관간 협력시스템이 제대로 갖춰져 있지 않아 효율적이지 못하다. 이에 따라 침해사고 발생시 신속하고 효율적인 대응이 이루어지지 못하고 있으며, 위험수준 단계별로 경보발령 및 대응요령 등의 제도화, 국제적 협력체제의 제도화가 미흡하다. 따라서 이 보고서에서는 이러한 현행 법제의 문제점을 개선하기 위하여, 현행 정보통신기반보호법과 국가사이버보안관리규정을 통합하고, 정보통신망 이용촉진 및 정보보호에 관한 법률을 분법할 것을 주장하였고, 도처에 산재하여 있고 때론 중복되어 있는 정보보안에 관한 규범내용 중 범국가차원의 집행체계에 관한 내용과 정보보안에 관한 기본적인 내용을 하나의 법규범으로 성안하여 '(가칭)정보보안관리법'을 제정할 것을 주장하였다.

여섯째, 이 보고서에서는 '(가칭)정보보안관리법'의 제정을 함에 있어, 정보통신망법의 보안관리에 관한 조항, 정보통신기반보호법, 정보화촉진기본법과 국가사이버안전관리규정의 보안관리에 관한 조항 등과 같은 전체적인 구성과 현행 법제에서 개선해야 할 내용을 중심으로 서술하였다.

이상과 같이 오늘날 사용자가 컴퓨터나 네트워크를 의식하지 않고 언제 어디서나 자유롭게 네트워크에 접속할 수 있는 정보환경에서 정

보의 유출과 침해에 따른 피해는 상상을 초월한 중대한 결과를 초래한다. 따라서 정보시스템을 신뢰하고 사용할 수 있도록 정보보안의 위협요소에 대하여 대처하는 정보보안이 중요하다는 사실은 아무리 역설해도 지나치지 않는다. 인터넷으로 연결된 정보시스템의 정보보안은 보장되어야 하며, 우리나라가 세계에서 일류 정보환경을 구축하고 있는 것처럼, 일류 정보보안환경을 구축하기 위하여 정치하고 세련된 정보보안 관련법제를 하루 빨리 갖추어야 한다.

[부록 1] OECD 정보시스템 및 네트워크 보안지침

보안문화의 정착을 향하여

경제협력개발기구(OECD)

경제협력개발기구

1960년 12월 24일 파리에서 서명하여 1961년 9월 30일자로 발효하게 된 협약 제1조에 따라, 경제협력개발기구는 다음의 목적으로 수립된 정책들을 증진하기로 한다:

- 경제적 안정을 유지하고 이로써 세계경제 개발에 기여하는 동시에 회원국에서의 최고의 지속가능한 경제성장과 고용 그리고 생계기준의 향상을 이룩할 것;
- 경제개발의 과정에서 회원국 및 비회원국에서의 공고한 경제신장에 기여하는 것; 그리고
- 국제적 의무에 따른 다자적, 비차별적 원칙에 기하여 세계무역 신장에 기여하는 것.

OECD의 초기 회원국들은 오스트리아, 벨기에, 캐나다, 덴마크, 프랑스, 독일, 그리스, 아이슬란드, 아일랜드, 이태리, 룩셈부르크, 네덜란드, 노르웨이, 포르투갈, 스페인, 스웨덴, 스위스, 터키, 대영제국 및 미합중국이다. 그 이후로 다음의 국가들이 이하 기술하는 날짜에 가입하여 회원국이 되었다: 일본(1964년 4월 28일), 핀란드(1969년 1월 28일), 호주(1971년 6월 7일), 뉴질랜드(1973년 5월 29일), 멕시코(1994년 5월 18일), 체코 공화국(1995년 12월 21일), 헝가리(1996년 5월 7일), 폴란드(1006년 11월 22일), 대한민국(1996년 12월 12일) 그리고 슬로바키아 공화국(2000년 12월 14일). 유럽공동체 위원회(Commission of the European Communities)는 OECD 업무에 협력한다(OECD협약 제13조).

서 문

본 OECD 정보시스템 및 네트워크 보안지침: 보안문화의 정착을 향하여 는 2002년 7월 25일 OECD 이사회 제1037차 회기에서 권고안으로 채택되었다.

목 차

OECD 정보시스템 및 네트워크 보안지침

보안문화의 정착을 향하여

서 문

OECD가 1992년 정보시스템 보안지침(Guidelines for the Security of Information Systems)을 처음 제안한 이래로 정보시스템 및 네트워크의 이용 및 정보기술환경 전체가 극적인 변화를 겪었다. 이와 같은 지속적인 변화는 많은 이점을 제공하기도 하지만 정보시스템과 네트워크의 개발, 소유, 제공, 서비스관리 및 이용하는 정부, 기업, 기타 조직과 개인사용자(“참여자”)들로부터 보안에 관한 중요성이 보다 강하게 요구되기도 한다.

어느 때보다도 강력한 개인 컴퓨터, 집중되는 기술과 보편화된 인터넷 사용은 주로 폐쇄 네트워크였던 소규모, 고립 형 시스템을 대체하게 되었다. 오늘날, 참여자들은 갈수록 상호관련성이 높아지고 그 관계가 국경을 넘나든다. 더 나아가, 인터넷은 에너지, 교통 및 경제와 같은 주요한 하부구조를 지원하고 기업체들이 업무를 수행하고, 정부가 시민과 기업들에 대해 서비스를 제공하며 또한 시민 개개인이 정보를 전달 및 교환하는 데에 있어 주요한 역할을 차지한다. 커뮤니케이션과 정보의 하부구조를 구성하는 기술의 본질과 유형 또한 크게 변하였다. 하부구조에 접근하기 위한 장치들의 숫자와 본질은 배가되었는데, 여기에는 고정, 무선 및 이동 장치가 포함되었으며 “상시 동작 전원(always on)”을 통해 하부구조에 대한 접근율이 증가세를 보이고 있다. 이에 따라, 교환되는 정보의 본질, 규모와 민감성은 상당히 확장되었다.

상호연결성(interconnectivity)의 증가로, 이제 정보시스템 및 네트워크는 보다 빈번하고 광범위한 종류의 위협과 취약점에 노출되어 있다. 이로써 보안에 관한 새로운 문제점들이 제기된다. 이와 같은 이유로, 본 지침들은 새로운 정보사회의 모든 참여자들에게 적용되며, 보안문제에 관한 자각과 이해를 제고해야 할 필요성과 “보안문화”를 개발해야 할 필요성을 제안하고 있다.

Ⅰ. 보안문화의 정착을 향하여

본 지침은 보안문화 - 즉, 정보시스템 및 네트워크의 개발과 정보시스템 및 네트워크의 이용과 시스템 내에서의 상호작용시 사고하고 반응하는 방식을 채택할 때에 보안에 중점을 두는 문화 - 의 개발을 장려함으로써 끊임없이 변화하는 보안환경에 대응하는 바이다. 본 지침은 네트워크와 시스템의 안전한 설계와 이용에 관하여 종종 사후 재고가 이루어지던 때와는 확연히 구분되는 시점임을 암시해주기도 한다. 참여자들은 신뢰할 수 있고 안전성이 요구되는 정보시스템, 네트워크 및 관련 서비스에 보다 의존적이 되어가고 있다. 모든 참여자들의 이해관계와 시스템, 네트워크 및 관련 서비스의 특성을 고려하는 접근방식만이 효율적인 보안을 마련할 수 있을 것이다.

참여자 개개인은 보안을 확보하는 중요한 주체들이다. 참여자들은 이러한 자신들의 역할에 알맞게 관련 보안위험과 예방조치들을 자각하여 그에 관한 책임을 상정하여 정보시스템 및 네트워크의 보안을 강화하기 위한 조치들을 취해야 할 것이다.

보안문화의 장려를 위해서는 리더쉽과 광범위한 참여가 요구되며, 보안문화의 장려로 인하여 모든 참여자들 사이에서 보안의 필요성에 대한 공통의 이해뿐 아니라 보안계획 및 관리에 대한 우선적 고려성향이 강화되어야 할 것이다. 보안관련 쟁점들은 정부와 기업, 그리고

모든 참여자들의 차원에서 주요 관심과 책임의 대상이 되어야 할 것이다. 본 지침은 사회 전반의 보안문화 정착을 향한 작업의 기초를 이루게 될 것이다. 이는 참여자들이 모든 정보시스템 및 네트워크의 설계와 이용에 있어서 보안을 고려할 수 있도록 해줄 것이다. 본 지침은 모든 참여자들이 정보시스템 및 네트워크 운영에 관하여 사고하고, 평가하며, 영향을 주는 수단으로서 보안문화를 채택 및 장려할 것을 제안한다.

Ⅱ. 목 표

본 지침은 다음을 목표로 한다:

- 정보시스템 및 네트워크를 보호하는 수단으로서 모든 참여자들 사이에 보안문화 정착을 장려한다.
- 정보시스템 및 네트워크의 위험에 관한 인식을 제고; 그와 같은 위험에 대처하는 정책, 관행, 조치 및 절차에 관한 인식을 제고; 또한 그와 같은 정책, 관행, 조치 및 절차들을 채택 및 실행해야 할 필요성에 관한 인식을 제고한다.
- 모든 참여자들 사이에 정보시스템 및 네트워크 그 자체뿐만 아니라 이들이 제공 및 이용되는 방식에 대한 신뢰도를 향상시킨다.
- 모든 참여자들이 보안관련 쟁점들을 이해하고, 정보시스템 및 네트워크의 보안을 위한 관련 정책, 관행, 조치 및 절차를 개발·이행하는데 있어 윤리적 가치를 존중하도록 도와주는 종합적인 참고의 틀을 제정한다.
- 보안을 위한 정책, 관행, 조치 및 절차를 개발·이행하는데 있어 모든 참여자들 사이에 적절한 협력과 정보공유를 증진한다.
- 표준을 개발하거나 이행하는 데 관련된 모든 참여자들에게 보안이 중요한 목표로서 고려되도록 장려한다.

Ⅲ. 원 칙

다음의 9개 정보보안원칙은 상호보완적이기 때문에 전체적으로 이해되어야 한다. 이들 원칙은 정책결정계층뿐만 아니라 운영계층을 포함한 모든 참여자를 대상으로 고려한다. 본 지침에 의하면, 모든 참여자들의 정보보안책임이 각자의 역할에 따라 상이하다. 모든 참여자들은 인식, 교육, 정보공유 및 훈련을 통하여 정보보안에 관한 보다 높은 이해와 관행을 갖추게 될 것이다. 정보시스템 및 네트워크의 보안을 증진시키기 위한 모든 노력은 민주사회의 다양한 가치, 특히 자유로운 정보유통과 사생활 보호에 대한 기본원칙과 합치되어야 한다.[36]

1) 인 식

참여자들은 정보시스템 및 네트워크 보안의 필요성과 그 보안을 강화하기 위하여 무엇을 할 수 있는지를 알고 있어야 한다.

위험과 위험에 대처하기 위한 보호수단을 잘 알고 있는 것은 정보시스템 및 네트워크의 보안을 위한 일차적인 방어선이다. 정보시스템 및 네트워크는 내부 뿐 아니라 외부에 의한 위험요인으로부터 영향을 받을 수 있다. 참여자들은 보안의 실패로 인하여 자신들이 관리하는 시스템과 네트워크가 심각하게 손상될 수 있다는 것을 알아야 한다. 참여자들은 또한 상호연계성과 상호의존성으로 인해서 타인·타조직에게 가할 수 있는 잠재적인 위해에 관하여 인지하고 있어야 한다. 참여자들은 자신들의 시스템 구성배치와 업데이트, 네트워크상 위치, 보안을 강화하기 위해 실행할 수 있는 좋은 관행들과 다른 참여자들의 요구사항들을 인지하고 있어야 한다.

---

36) OECD는 본 지침 뿐만 아니라 세계정보사회에 중요한 다른 사안에 대한 지침을 제시하여 이를 보완할 수 있도록 하였다. 1980년 사생활보호와 개인 데이터의 국경간 유통에 대한 OECD 지침이 있다. 본 지침은 이 지침들과 연계해서 이해되어야 한다.

2) 책 임

모든 참여자들은 정보시스템 및 네트워크 보안에 책임이 있다.

참여자들은 상호연결된 지역적 그리고 세계적 정보시스템 및 네트워크에 의존하며, 그러한 정보시스템 및 네트워크의 보안에 대한 자신들의 책임을 알고 있어야 한다. 참여자들은 자신들의 역할에 알맞은 보안책임을 져야 한다. 참여자들은 정보보안을 위한 정책, 관행, 조치 및 절차를 정기적으로 검토하고 그것이 참여자들이 속한 환경에 적합한 것인지의 여부를 평가해야 한다. 제품과 서비스를 개발·구상 그리고 공급하는 참여자들은 시스템 및 네트워크 보안에 관한 사항들을 진지하게 검토하고, 업데이트를 포함한 적절한 정보를 적기에 배포하여 이용자들이 제품과 서비스의 정보보안 기능과 정보보안과 관련한 자신들의 책임을 보다 잘 이해할 수 있도록 해야 한다.

3) 대 응

참여자들은 정보보안사고를 예방, 탐지, 대응하기 위해 협력적인 자세로 적기에 행동을 취해야 한다.

참여자들은 정보시스템 및 네트워크의 상호연계성과 신속하고 광범위하게 확산되는 피해의 잠재적 발생 가능성을 인지하여 정보보안사고에 대처하기 위하여 협력적인 자세로 적기에 행동을 취해야 한다. 참여자들은 정보보안에 관한 위협 및 취약성에 대한 정보를 적절히 공유해야 하며, 정보보안사고를 예방·탐지·대응하기 위한 신속하고 효율적인 협력 절차를 시행하여야 한다. 허용이 되는 경우, 이는 국가간 정보공유 및 협력을 포함할 수 있다.

4) 윤 리

참여자들은 타인의 적법한 이익을 존중해야 한다.

정보시스템 및 네트워크가 우리 사회 전반에 널리 분포되어 있다는 점을 고려하여 참여자들은 그들의 작위나 부작위가 타인에게 위해를 가할 수 있다는 것을 인식하여야 한다. 따라서, 윤리적인 행동은 매우 중요한 것이므로, 참여자들은 최선의 업무관행을 개발·도입하도록 노력해야 하며, 정보보안에 대한 필요성을 인정하고, 타인의 적법한 이익을 존중하는 행동을 장려할 수 있도록 노력하여야 한다.

5) 민주성

정보시스템 및 네트워크의 보안은 민주주의사회의 근본적인 가치들에 부합하여야 한다.

사상과 발상(idea)의 자유로운 교환, 정보의 자유로운 유통, 정보와 통신의 비밀보장, 개인정보의 적절한 보호, 개방성 및 투명성을 포함하여, 민주주의 사회에서 인정되는 가치에 부합하는 방식으로 정보보안이 실행되어야 한다.

6) 위험평가

참여자들은 위험평가를 시행해야 한다.

위험평가는 정보보안에 관한 위협과 취약성을 확인하는 것이며, 기술, 물리적·인적 요인, 정책, 정보보안과 관련되는 제3자 서비스와 같은 주요 내·외적 요인을 모두 포함할 수 있도록 충분히 포괄적이어야 한다. 위험평가는 보호되어야 할 정보의 특성과 중요성을 고려하여 수용 가능한 위험수준을 결정하며 정보시스템 및 네트워크에 잠재적인 위해를 가져올 수 있는 위험을 관리하기 위한 적절한 통제수

단을 선택할 수 있게 하는 것이다. 정보시스템의 상호연계성이 지속적으로 증가하고 있으므로 위험평가는 타인에 의해서 발생하는 위해뿐만 아니라 타인에게 가해질 수 있는 잠재적 위험에 대해서도 고려하여야 한다.

7) 정보보안의 설계와 이행

참여자들은 정보보안을 정보시스템 및 네트워크의 핵심요소로 수용하여야 한다.

정보시스템, 네트워크 및 정책은 정보보안을 최적화 할 수 있도록 적절하게 설계·집행·조율되어야 한다. 이러한 노력의 중점은 주요한 것이지만 유일한 것은 아닌 이미 알려진 정보보안에 관한 위협과 취약성에 의해 야기되는 잠재적 위해를 방지하거나 제한하기 위한 적절한 안전장치와 해결책을 설계하고 도입하는데 있다. 기술적·비기술적 안전장치와 해결책이 모두 필요하며, 이들은 조직의 시스템 및 네트워크상의 정보가치에 상응하여야 한다. 정보보안은 모든 제품, 서비스, 시스템 및 네트워크의 기본적인 요소이며, 시스템의 설계와 구조의 필수적인 부분이 되어야 한다. 최종 사용자들에 있어, '정보보안의 설계와 이행'이라고 함은 대체로 자신들의 시스템에 필요한 제품과 서비스를 선택하고 배치하는 것을 의미한다.

8) 정보보안 관리

참여자들은 정보보안 관리에 대해 포괄적인 접근방식을 채택해야 한다.

정보보안 관리는 위험평가에 입각하여 이루어져야 하며, 참여자에 의한 활동의 모든 수준과 운영의 모든 측면을 포괄하는 것으로서 동태적이어야 한다. 정보보안 관리는 새로운 위협에 대한 전향적인 대

응책을 포함하여야 하며, 보안사고의 방지・탐지・대응과 함께 시스템 복구・지속적인 유지관리・검토 및 감사 등을 다루어야 한다. 정보시스템 및 네트워크의 보안을 위한 정책, 관행, 조치, 절차는 일관적인 정보보안체계가 이루어질 수 있도록 조정・통합되어야 한다. 정보보안 관리에 요구되는 사항은 참여자의 참여 수준・역할, 관련 위험 및 시스템 요건에 의해서 결정된다.

9) 재평가

참여자들은 정보시스템 및 네트워크의 보안을 검토하고 재평가하여 정보보안 정책, 관행, 조치, 절차를 적절히 수정해야 한다.

새롭고 변화하는 위협과 취약성이 계속해서 나타나고 있다. 참여자들은 정보보안의 모든 측면을 지속적으로 검토・재평가・수정하여 이와 같이 진화하는 위험에 대처하여야 한다.

정보시스템 및 네트워크의 보안지침에 관한 이사회 권고

보안문화의 정착을 향하여

이사회는 아래 사항들을 고려하고,

1960년 12월 14일 경제협력개발기구에 대한 협정, 특히, 1 b), 1 c), 3 a) 조항;

1980년 9월 23일 프라이버시보호 및 개인정보의 국경간 유통에 대한 가이드라인과 관련한 위원회 권고사항[C(80)58(Final)];

1985년 4월 11일 OECD회원국에 의해서 채택된 국경간 정보유통에 대한 선언[Annex to C(85)139];

1997년 3월 27일 암호정책 가이드라인과 관련한 위원회 권고 [C(97)62/FINAL];

1998 12월 7일～9일 글로벌 네트워크에서의 프라이버시보호에 관한 각료선언 [Annex to C(98)177/FINAL];

1998년 12월 7일～9일 전자상거래를 위한 인증에 관한 각료선언 [Annex to C(98)177/FINAL];

이사회는 아래 사항들을 인지하고,

정부, 기업, 조직 그리고 개인 사용자에게 정보시스템과 네트워크의 유용성과 가치는 계속 증가하고 있다;

정보시스템 및 네트워크가 갖는 기능적 중요성이 계속 높아지고, 국가경제와 국제무역뿐만 아니라 사회문화 및 정치적 삶에 있어서 안정성과 효율성을 확보하기 위하여 정보시스템 및 네트워크에 대한 의존

도가 증가하고 있기 때문에 이에 대한 신뢰성을 지키고 증진하기 위한 특별한 노력이 요구된다;

정보시스템 및 네트워크의 등장과 전세계적인 확산은 지속적으로 증가하는 새로운 위험을 가져왔다;

정보시스템 및 네트워크에 의해 저장되고 전달되는 데이터와 정보는 비인가 접근 및 사용·오용·변조·악성코드 전송·서비스 거부 또는 시스템 파괴와 같은 다양한 수단에 의한 위험에 노출되어 있으며, 이에 대한 적절한 정보보안대책이 요구된다;

정보시스템 및 네트워크에 대한 위험과 이에 대처하기 위한 정책, 관행, 조치, 절차에 대한 인식을 제고하고, 정보보안문화를 발전시키기 위한 핵심적인 방법으로서 정보보안에 적절한 행동을 장려하는 것이 필요하다;

현재의 정책, 관행, 조치 그리고 절차를 재검토하여 이로써 정보시스템 및 네트워크에 가해지는 위협으로부터 야기되어 전개되는 난제들에 적절히 대처할 수 있는지를 확인할 필요가 있다;

정보보안의 실패로 인하여 국가경제, 국제무역, 사회적·문화적·정치적 생활참여에 가해지는 잠재적 위해로부터 야기되는 난제에 대처하기 위하여 국제적인 조정과 협력을 증진하는 정보보안문화를 확립함으로써 정보시스템 및 네트워크의 보안을 증진하려는 공통의 관심사가 존재한다;

나아가 아래 사항들을 인지하고,

본 권고의 부속문서에 기술된 '정보시스템 및 네트워크 보안지침 : 보안문화의 정착을 향하여'는 자발적인 것이며 개별 국가의 주권에 영향을 미치지 않는다;

본 지침은 정보보안을 위한 유일한 해결책이 존재하거나 특정 상황에 어떠한 정책, 관행, 조치, 절차가 적절한지를 제안하는 것은 아니며, 정보보안문화의 발전으로 참여자들이 이익을 얻고, 정보보안문화 발전에 참여자들이 기여할 수 있는 방법에 대한 이해를 높일 수 있는 원칙의 준거틀을 제공하고자 한다;

이사회는 '정보시스템 및 네트워크 보안지침 : 보안문화의 정착을 향하여'를 정보시스템 및 네트워크를 개발・소유・공급・관리・서비스하고 사용하는 정부기관, 기업, 여타 조직 및 개인 이용자들에게 권고한다;

이사회는 회원국들에게 아래 사항들을 권고한다 :

본 지침에 제시된 정보보안문화를 채택・촉진하고 본 지침의 내용을 반영·참고하여 새로운 정보보안정책, 관행, 조치, 절차를 수립하거나 기존의 정보보안정책, 관행, 조치, 절차를 보완할 것;

본 지침을 실행하기 위하여 국내 및 국제적 차원에서 상호 협의, 조정, 협력할 것;

정보보안문화를 촉진하고 관련된 모든 단체들이 각자의 역할에 적합한 방식으로 본 지침을 실행하는데 책임감을 갖고 필요한 조치를 취할 수 있도록 본 지침을 정부, 기업, 사회조직 및 개인 이용자를 포함한 공공부문 및 민간부문에 홍보할 것;

OECD 비회원국들에게 적기에 적절한 방식으로 본 지침을 활용 가능하게 할 것;

정보시스템 및 네트워크의 보안과 관련된 관심사와 문제점에 대한 국제적인 협력을 촉진하기 위하여 매 5년마다 본 지침을 재검토 할 것;

이사회는 OECD 정보통신정책위원회(ICCP)에 본 지침의 실행을 장려할 것을 **지시한다.**

본 권고는 1992년 11월 26일 '정보시스템 보안지침에 관한 이사회 권고[C(920188/FINL)'를 대체한다.

경 과

정보보안지침은 1992년 최초로 마련되었으며, 1997년 재검토되었다. 이번에 이루어진 지침에 대한 검토는 '정보통신정책위원회(ICCP)'의 지시에 따라 '정보보안 및 프라이버시보호 실무반(WPISP)'에 의해 2001년 개시되었으며, 9월 11일 테러참사의 영향으로 작업이 가속화되었다.

초안작성은 2001년 12월 10～11일 워싱턴, 2002년 2월 12～13일 시드니, 2002년 3월 4～6일 파리에서 회의를 가졌던 WPISP의 전문가그룹에 의해 착수되었다. '정보보안 및 프라이버시보호 실무반(WPISP)'은 2002년 3월 5～6일, 2002년 4월 22～23일, 2002년 6월 25～26일 파리에서 회의를 가졌다.

본 *'OECD 정보시스템 및 네트워크 보안지침: 보안문화의 정착을 향하여'*는 2002년 7월 25일 제1037차 회기에서 OECD 이사회의 권고로서 채택되었다.

[부록 2] 미국의 연방정보보안관리법

제301조 정보보안

(a) 법명 - 본 절은 “2002년 연방정보보안관리법”이라 한다.

(b) 정보보안

(1) 총칙 - 연방법전 제44편 제35장은 말미에 다음의 신규 절을 추가하는 것으로 수정한다.

“제3절 정보보안”

“제3541조 목적

“본절의 목적은

“(1) 연방 업무 및 자산을 지원하는 정보자원에 대한 정보보안 통제의 효과를 보장하기 위한 총체적인 틀을 제공하는 데 있다.

“(2) 고도로 네트워크화 되어 있는 현재의 연방 컴퓨터환경을 인식하고, 국민과 국가의 보안 및 관할지역 내 정보보안 활동을 조정하는 등 관련 정보보안 위험에 대한 효과적인 범정부 차원의 관리 및 감독을 실시하는 데 있다.

“(3) 연방정보 및 정보시스템의 보호에 필요한 최소한의 통제수단을 개발 및 유지하는 데 있다.

“(4) 연방기관의 정보보안 프로그램에 대한 감독을 강화하기 위한 메카니즘을 제공하는 데 있다.

“(5) 상업적 목적으로 개발된 정보보안 상품은 품질이 우수하고 역동적이며 강력하고 효과적인 정보보안 솔루션을 제공한다는 사실을 인식하고, 국방 및 경제안정에 필요한 주요정보 인프라를 보호하기 위하여 민간이 개발, 구축 및 운영하는 마켓 솔루션을 반영하는 데 있다.

“(6) 상업적 목적으로 개발된 상품 가운데 특정한 기술적 하드웨어 및 소프트웨어 정보보안 솔루션을 선정하는 사항은 개별

기관에 맡겨져야 한다는 사실을 인식하는 데 있다.

"제3542조 정의

"(a) 총칙 - 제(b)항에서 정한 경우를 제외하고 제3502조의 정의 규정은 본 절에 적용된다.

"(b) 추가적 정의규정 - 본 절에서는 다음과 같이 사용된다.

"(1) '정보보안'이라 함은 다음을 목적으로 권한없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 정보 및 정보시스템을 보호하는 것을 말한다.

"(A) 부적절한 정보 변경 또는 파괴로부터 보호한다는 의미로서 정보청구의 보장 및 진정성 확보 등을 위한 보전

"(B) 부적절한 정보 변경 또는 파괴로부터 보호한다는 의미로서 정보청구의 보장 및 진정성 확보 등을 위한 보전

"(C) 적절한 시기에 신뢰할 수 있는 방법으로 정보에 접속 및 이용할 수 있다는 의미의 비밀성

"(2)(A) '국가보안시스템'이라 함은 기관 또는 기관과 계약을 맺은 자 또는 기타 기관을 대신하는 조직에 의하여 이용 또는 운영되는 (여하한 정보통신시스템을 포함하여) 여하한 정보시스템을 말한다.

"(ⅰ) 이러한 시스템의 기능, 운영 또는 이용은

"(Ⅰ) 정보활동과 관계가 있다.

"(Ⅱ) 국가보안에 관한 암호해독 활동과 관계가 있다.

"(Ⅲ) 군의 지휘 및 통제와 관계가 있다.

"(Ⅳ) 군비시스템의 필수설비와 관계가 있다.

"(Ⅴ) (B)목에 따른 군 또는 정보임무의 직접 수행에 중요하다.

"(ⅱ) 국방 또는 외교적 관점에서 행정명령 또는 의회법에 의하여 설정된 분류기준에 따라 구체적으로 권한이 부여된 정보에 관한 절차에 따라 항상 보호된다.

(B) (A)목 (ⅰ)(Ⅴ)는 (임금, 재무, 관재 및 인사관리운영을 포함하여) 일반적인 행정 및 사업운용을 위하여 이용되는 시스템을 포함하지 아니한다.

"(3) '정보기술'은 제40편 제11101조에서 규정된 의미에 따른다.

"제3543조 처장의 권한 및 역할

"(a) 총칙 - 처장은 다음을 포함하여 기관의 정보보안정책 및 업무를 감독하여야 한다.

"(1) 기관이 적절한 시기에 제40편 제11331조에 따라 공포된 표준을 채택 및 준수하도록 하는 것을 포함하여 정보보안에 관한 정책, 원칙, 표준 및 지침의 시행을 개발하고 감독함

"(2) 기관이 동 제11331조 및 본 절의 요건에 따라 공포된 표준과 일치하는 범위 내에서 다음에 해당하는 정보에 대한 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 야기되는 위험 및 해약의 정도와 상응하는 수준의 정보보안에 관한 보호조치를 확인하고 제공하도록 함

"(A) 기관에 의하거나 기관을 대신하여 수집되거나 보존되는 정보 또는

"(B) 기관 또는 기관과 계약을 맺은 자 또는 기관을 대신하는 다른 조직에 의해 이용되거나 운영되는 정보시스템

"(3) 국가표준기술연구원법(15U.S.C. 278g-3) 제20조에 따른 표준 및 지침의 개발에 대하여(국가보안국 등) 국가보안시스템을 운영하거나 통제하는 기관 및 사무국과 조정 작업을 거침으로써 가능한 한 최대한의 범위 내에서 그러한 표준 및 지침이 국가보안시스템용으로 개발된 표준 및 지침을 보충하도록 함

"(4) 제40편 제11303조에 따른 여하한 권한 있는 조치 등을 포함하여 본 절의 요건에 대한 기관의 준수여부를 감독함으로써 그러한 요건의 준수여부에 대한 책임을 부담토록 함

"(5) 최소 1년마다 제3544조 제(b)항에 따른 기관의 정보보안 프로그램을 검토하고 이를 승인하거나 부인함

"(6) 정보보안에 관한 정책과 절차를 관련 정보자원관리 정책 및 절차와 조정함

"(7) 제3536조에 따른 연방 정보보안사고센터의 운영을 감독함

"(8) 매년 3월 1일 이전에 다음을 포함하여 본 절의 요건에 대한 기관의 준수여부를 의회에 보고함

"(A) 제3545조에 따른 평가 자료의 요약

"(B) 국가표준기술연구원법 제20조에 따라 개발되고 제40편 제11331조에 따라 공포된 표준의 개발, 공포, 채택 및 준수여부에 대한 평가

"(C) 기관의 정보보안업무에 있어서의 중요한 결점

"(D) 그러한 결점에 대한 구제조치계획

"(E) 국가표준기술연구원법 제20조제(d)항(제10)호에 따라 국가표준기술연구원이 작성한 보고서에 대한 요약 및 처장의 검토의견

"(b) 국가보안시스템 - 제(a)항 제(4)호 내지 제(8)에서 규정된 권한있는 경우를 제외하고 본 조에 따른 처장의 권한은 국가보안시스템에 적용되지 아니한다.

"(c) 국방성 및 중앙정보국 시스템 -

"(1) 제(a)항 제(1)호 및 제(2)호에서 규정된 처장의 권한은 제(2)호에 규정된 시스템의 경우에는 국방장관에게 위임되며 제(3)호에 규정된 시스템의 경우 중앙정보국장에게 위임된다.

"(2) 본 호에 규정된 시스템은 국방성, 국방성과 계약을 맺은 자 또는 국방성을 대신하는 자로서 권한없는 접속, 이용, 공개, 방해, 변경 또는 파괴가 국방성의 임무에 지대한 영향을 미치는 여하한 정보를 보유하고 있는 여하한 주체에 의하여 운영되는 시스템을 말한다.

"(3) 본 호에 규정된 시스템은 중앙정보국, 중앙정보국과 계약을 맺은 자 또는 중앙정보국을 대신하는 자로서 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴가 중앙정보국의 임무에 지대한 영향을 미치는 여하한 정보를 보유하고 있는 여하한 주체에 의하여 운영되는 시스템을 말한다.

"제3544조 연방기관의 책임

"(a) 총칙 - 각 기관의 장은

"(1) 다음에 대하여 책임이 있다.

"(A) 다음에 해당되는 정보에 대한 권한없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 야기되는 위험 및 해악의 정도와 상응하는 수준의 정보보안에 관한 보호조치를 제공함

"(ⅰ) 당해 기관에 의하거나 당해 기관을 대신하여 수집되거나 보존되는 정보 및

"(ⅱ) 기관 또는 기관과 계약을 맺은 자 또는 기관을 대신하는 다른 조직에 의하여 이용되거나 운영되는 정보시스템

"(B) 다음을 포함하여 본 절의 요건 및 관련 정책, 절차, 표준 및 지침을 준수함

"(ⅰ) 제40편 제11331편에 따라 공포된 정보보안에 관한 표준 및

"(ⅱ) 법률에 따라 대통령령으로 정하는 국가보안시스템에 대한 정보보안표준 및 지침

"(C) 정보보안 관리절차가 기관의 전략 및 운용계획 절차와 통합하도록 함

"(2) 다음의 방법 등을 통해 기관의 고위공무원이 자신의 통제를 받은 업무 및 자산을 지원하는 정보 및 정보시스템에 대한 정보보안을 유지하도록 함

"(A) 그러한 정보 또는 정보시스템의 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 야기될 수 있는 위험 및 해

악의 정도를 평가함

"(B) 제40편 제11331조에 따라 공포된 표준에 일치하는 범위 내에서 그러한 정보 및 정보시스템을 보호하는 데 적절하도록 정보보안의 분류기준 및 관련 요건 등에 대한 정보보안의 수준을 결정함

"(C) 저렴한 비용으로 위험을 수용 가능한 수준으로 감소시키기 위한 정책 및 절차를 시행함

"(D) 정보보안의 통제 및 기술이 효과적으로 시행될 수 있도록 정보보안의 통제 및 기술을 주기적으로 시험하고 평가함

"(3) 제3506조에 따라 설치된 기관의 정보화책임관(또는 동 조의 적용을 받지 아니하는 기관에 있어서의 동등한 자격을 가진 자)에 대하여 요건을 당해 기관이 준수하도록 할 수 있는 권한을 위임함

"(A) 다음을 내용으로 하는 기관의 고위급 정보보안관리자를 임명함

"(ⅰ) 본 조에 따라 정보화책임관의 임무를 수행함

"(ⅱ) 본 조에 규정된 역할을 수행함에 있어 필요한 교육 및 경험 등 전문자격요건을 갖춤

"(ⅲ) 정보보안에 관한 임무를 당해 직책의 최우선 임무로 하는 자

"(ⅳ) 기관이 본 조의 내용을 준수하도록 지원하는 임무와 자원을 갖고 사무국을 운영하는 자

"(B) 제(b)항에서 요구하는 범기관적인 정보보안 프로그램을 개발하고 유지함

"(C) 본 편의 제3543조 및 제40편 제11331편에 따른 것을 포함하여 모든 적용 가능한 요건들을 내용으로 하는 정보보안에 관한 정책, 절차 및 통제기술을 개발하고 유지함

"(D) 그러한 책임과 관련하여 정보보안에 대해 중대한 책임을 지는 자를 교육하고 감독함

"(E) 제(2)호에 따른 책임에 대하여 기관의 고위급 공무원을 지원함

(4) 당해 기관이 본절의 요건 및 관련 정책, 절차, 표준 및 지침을 준수하도록 지원할 수 있는 충분한 전문 인력을 보유할 수 있도록 함

(5) 매년 당해 기관의 정보화책임관이 기관의 다른 고위급 공무원과 협력하여 당해 기관의 장에게 구제조치절차 등 당해 기관의 정보보안 프로그램의 효과에 대하여 보고하도록 함

(b) 기관 프로그램 - 각 기관은 다음을 포함하여 또 다른 기관, 계약자 또는 다른 관계자에 의하여 제공되거나 관리되는 것을 포함한 당해 기관의 업무 및 자산을 지원하는 정보 및 정보시스템에 대한 정보보안을 유지하기 위하여 제3543조 제(a)항 제(5)호에 따라 처장이 승인한 범기관적 정보보안 프로그램을 개발하고 구성하며 시행하여야 한다.

"(1) 당해 기관의 업무 및 자산을 지원하는 정보 및 정보시스템의 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 야기되는 위험 및 해악의 정도에 대한 주기적인 평가

"(2) 다음을 내용으로 하는 정책 및 절차

"(A) 제(1)호에서 요구하는 위험평가를 기초로 함

"(B) 비용절감을 통하여 정보보안에 대한 위험을 수용 가능한 수준으로 감소시킴

"(C) 각 기관의 정보시스템의 수명주기에 맞추어 정보보안이 유지될 수 있도록 함

"(D) 다음을 준수하도록 함

"(ⅰ) 본 절의 요건

"(ii) 처장이 정하는 정책 및 절차와 제40편 제11331조에 따라 공포된 정보보안표준

"(iii) 당해 기관에 의하여 결정된 것으로 수용 가능한 최소한의 시스템 사양 요건

"(iv) 법률에 따라 대통령령으로 정하는 국가보안시스템에 대한 표준 및 지침을 포함한 기타 적용 가능한 여하한 요건

"(3) 적절한 범위 내에서 네트워크, 설비 및 시스템 또는 일련의 정보시스템에 적당한 정보보안을 유지하기 위한 하위계획

"(4) 당해 기관의 업무 및 자산을 지원하는 계약자 및 기타 정보시스템을 이용하는 자를 포함하여 개인에 대하여 다음에 관한 정보를 알려주는 보안인식훈련

"(A) 자신의 활동과 연계된 정보보안에 대한 위험

"(B) 당해 위험을 감소시키기 위하여 고안된 기관의 정책 및 절차에 대한 준수책임

"(5) 1년을 넘지 않는 범위 내에서 위험정도에 따라 빈번하게 실시되는 정보보안에 관한 정책, 절차 및 업무 효과에 대한 주기적인 시험 및 평가로서 그러한 시험은

"(A) 제3505조 제(c)항에서 정한 목록상 확인되는 모든 정보시스템의 관리, 운영 및 기술통제에 대한 시험을 포함하여야 한다.

"(B) 제3545조에 따른 평가의 기초가 되는 시험을 포함할 수 있다.

"(6) 당해 기관의 정보보안에 관한 정책, 절차 및 업무상의 여하한 결점에 대한 구제조치를 계획, 시행, 평가 및 기록하기 위한 절차

"(7) 다음을 포함하여 제3546조 제(b)항에 의한 표준 및 지침에 따른 보안사고에 대한 탐지, 보고 및 대응을 위한 절차

"(A) 중대한 해악이 있기 전에 그러한 사고에 관한 위험을 경감시킴

"(B) 제3546조에서 규정하고 있는 연방 정보보안사고센터에 대한 통지 및 자문을 구함

"(C) 적절한 범위 내에서

"(ⅰ) 행정기관 및 관련 감사기관

"(ⅱ) 국가보안시스템에 관한 여하한 사고에 대비하여 대통령이 지명한 기관

"(ⅲ) 법률 또는 대통령령에 의한 기타 여하한 기관 및 사무국

"(8) 당해 기관의 업무 및 자산을 지원하는 정보시스템에 대한 영속적 운영을 확보하기 위한 계획 및 절차

"(c) 기관 보고 - 각 기관은

"(1) 매년 처장, 하위 정부개혁 및 과학위원회, 상원 정무 및 상공, 과학 및 교통위원회, 기타 권한 있고 적절하다고 판단되는 의회 위원회 및 감사원에 대하여 정보보안에 관한 정책, 절차, 업무의 효과 및 제(b)항의 각 요건에 대한 준수여부를 포함하여 본 절의 요건에 대한 준수여부를 보고하여야 한다.

"(2) 다음에 관하여 계획하고 보고함에 있어 정보보안에 관한 정책, 절차 및 업무의 적절성 및 효과를 그 내용으로 하여야 한다.

"(A) 기관의 연간 예산

"(B) 본 장 제1절에 따른 정보자원관리

"(C) 제40편 제3절에 정보기술관리

"(D) 제31편 제1105조 및 제1115조 내지 제1119조와 제39편 제2801조 및 제2805조에 따른 프로그램의 시행

"(E) 제31편 제1105조 및 제1115조 내지 제1119조와 제39편 제2801조 및 제2905조에 따른 프로그램의 시행

"(F) 연방재무관리개선법(31 U.S.C. 3512 note)에 따른 재무관리 시스템

"(G) 제31편 제3512조(통칭 '연방관리자재무통합법')에 따른 내부 회계 및 행정통제

"(3) 제(1)호 또는 제(2)호에 따라 확인된 다음과 같은 정책, 절차 또는 업무상의 여하한 중대한 결함을 보고하여야 한다.

"(A) 제31편 제3512조에 따른 보고에 있어 중대한 결점에 해당되는 경우

"(B) 재무관리시스템과 관련하여 연방재무관리개선법의 준수에 중대한 결함을 보고하여야 한다.

"(d) 시행계획 - (1) 제(c)항의 요건 외에 각 기관은 처장과 협의하여 제31편 제1115조에 따른 시행계획의 일부로서 다음을 기술하여야 한다.

"(A) 기간 및

"(B) 제(b)항에 따른 프로그램을 시행함에 있어 필요한 예산, 직원 및 교육 등을 포함한 자원

"(2) 제(1)호에 따른 기술은 제(b)항 제(2)호 제(1)목에 따른 위험평가를 기초로 하여야 한다.

"(e) 공고 및 의견수렴 - 각 기관은 적절한 시기에 국민과의 관계에 영향을 미치는 범위 내에서 정보보안에 관한 정책안 및 절차안을 국민에 대하여 공고함으로써 의견개진의 기회를 제공하여야 한다.

"제3545조 독자적 연간평가

"(a) 총칙 - (1) 매년 각 기관은 당해 기관의 정보보안 프로그램 및 업무의 효과를 파악하기 위하여 당해 프로그램 및 업무에 대한 독자적 평가를 실시하여야 한다.

"(2) 본 조에 따른 각 평가는 다음을 포함하여야 한다.

"(A) 당해 기관의 정보시스템을 대표할 수 있는 부분에 대한 정보보안 정책, 절차 및 업무의 효과에 대한 시험

"(B) (동 시험결과를 기초로 한) 다음에 대한 준수여부의 평가

"(ⅰ) 본 절의 요건 및

"(ii) 관련 정보보안 정책, 절차, 표준 및 지침

"(C) 적절한 범위 내에서 국가보안시스템과 관련된 정보보안에 관한 별도의 설명

"(b) 독자적 감사 - 제(c)항에 따라

"(1) 1978년 감사역법에 따라 임명된 감사역이 있는 각 기관의 경우 본 조에 따른 연간 평가는 당해 감사역 또는 당해 기관의 감사역이 정한 독립된 외부 감사에 의하여 실시되어야 한다.

"(2) 제(1)호가 적용되지 아니하는 각 기관의 경우 당해 기관의 장은 당해 평가를 실시함에 있어 독립된 외부 감사를 관련시켜야 한다.

"(C) 국가보안시스템 - 국가보안시스템을 운영 또는 통제하는 각 기관의 경우 본 조에 따른 평가에 있어 국가보안시스템과 직접적으로 관계가 있는 부분은 다음과 같은 방법으로 실시되어야 한다.

"(1) 당해 기관의 장이 지명한 자에 의해서만

"(2) 그러한 시스템에 있는 여하한 정보보안상의 취약성과 관련된 정보에 대하여 모든 관련 법률에 따라 당해 위험에 상응하는 수준에서 적절한 보호를 보장하는 방식으로

"(d) 현행 평가 - 본 조에 따른 평가는 그 전부 또는 일부에 대하여 당해 적용 기관의 프로그램 또는 업무와 관련된 감사, 평가 또는 보고를 기초로 실시할 수 있다.

"(e) 기관 보고 - (1) 매년 각 기관의 장은 처장이 정한 날 이전까지 처장에 대하여 본 조에 따른 평가결과를 제출하여야 한다.

"(2) 본 조에 따른 평가가 국가보안시스템과 직접적으로 관계가 있는 경우 처장에 대하여 제출된 평가 결과는 국가보안시스템과 직접적으로 관계가 있는 평가 부분에 대한 요약 및 평가만을 포함하여야 한다.

“(f) 정보의 보호 - 기관 및 평가자는 공개되는 경우 정보보안에 역효과를 미칠 수 있는 정보를 보호하기 위하여 적절한 조치를 취하여야 한다. 그러한 보호조치는 모든 적용 가능한 법률을 준수하고, 당해 위험에 상응하는 수준이어야 한다.

“(g) 관리예산처의 의회보고 - (1) 처장은 본 조에 따라 실시된 평가 결과를 요약하여 제3543조 제(a) 제(8)호에 따른 의회보고서에 포함시켜야 한다.

“(2) 본 조에 따른 처장의 의회보고는 그러한 시스템에 있는 여하한 정보보안상의 취약성과 관련된 정보에 대하여 모든 적용 가능한 법률에 따라 당해 위험에 상응하는 수준에서 적절한 보호를 보장하는 방식으로 국가보안시스템과 관계가 있는 정보보안에 관한 정보를 요약하여야 한다.

“(3) 중앙정보국장의 권한 및 통제를 받는 정보시스템 또는 국방장관의 권한 및 통제를 받는 국내외 정보프로그램 시스템에 대한 평가 및 기타 여하한 기술은 준거법에 따라 적당한 의회 감독위원회를 통해서만 의회에 제출되어야 한다.

“(h) 감사원장 - 감사원장은 다음에 관하여 주기적으로 평가하여 이를 의회에 보고하여야 한다.

“(1) 기관 정보보안 정책 및 업무의 적절성 및 효과

“(2) 본 절의 요건 준수

“제3546조 연방정보보안 사고센터

“(a) 총칙 - 처장은 중앙정보보안 사고센터를 운영함으로써

“(1) 보안사고와 관련하여 기관의 정보시스템 운영자에 대하여 정보보안사고의 탐지 및 수습에 관한 지침을 포함한 기술적 지원을 시기 적절하게 제공하여야 한다.

“(2) 정보보안을 위협하는 사고에 대한 정보를 수집하고 분석하여야 한다.

"(3) 기관의 정보시스템 운영자에 대하여 현존 및 잠재적 정보보안 위협과 취약부분에 관한 정보를 제공하여야 한다.

"(4) 정보보안 사고 및 관련 문제를 국가표준기술연구원, (국가보안국을 포함한) 국가보안시스템을 운영하거나 통제하는 기관 또는 사무국 및 법률에 따라 대통령령으로 정한 기타 그와 같은 기관 또는 사무국과 협의하여야 한다.

"(b) 국가보안시스템 - 국가보안시스템을 운영 또는 통제하는 각 기관은 법률에 따라 대통령령이 정하는 국가보안시스템에 대한 표준 및 지침과 일치하는 범위 내에서 정보보안사고, 위협 및 취약부분에 관한 정보를 연방정보보보안 사고센터와 공유하여야 한다.

제3547조 국가보안시스템

"국가보안시스템을 운영 또는 통제하는 각 기관의 장은 당해 기관이

"(1) 그러한 시스템에 포함된 정보의 권한 없는 접속, 이용, 공개, 방해, 변경 또는 파괴로부터 야기되는 위험 및 해악의 정도에 상응하는 수준으로 정보보안 보호조치를 제공하도록 할 책임이 있다.

"(2) 법률에 따라 대통령령이 정하는 국가보안시스템에 관한 표준 및 지침에 따른 정보보안 정책 및 업무를 시행하도록 할 책임이 있다.

"(3) 본 절의 요건을 준수하도록 할 책임이 있다.

제3548조 예산권한

"본 절의 내용을 이행하기 위하여 2003년부터 2007년까지 매 회계연도마다 필요한 만큼의 예산을 집행할 수 있는 권한이 있다.

제3549조 현행법에 대한 효과

"본 절, 제40편 제11331조 또는 국가표준기술법(15 U.S.C. 278g-3)

제20조의 어떠한 규정도 제5편 제552a조의 개인 프라이버시 보호에 관한 것을 포함하여 정보의 권한 없는 이용 또는 공개, 제5편 제552조의 정보공개, 제44편 제29장, 제31장 또는 제33장의 기록의 관리 및 처분, 본 편 제35장 제1절 정보자원의 관리 또는 미국 의회 또는 감사원장에 대한 정보공개 등과 관련하여 대통령, 관리예산처 또는 관리예산처장, 국가표준기술연구원 또는 여하한 기관의 장의 권한에 대하여 영향을 미치는 것으로 해석되지 아니한다. 본 절이 효력을 발하는 경우 본 장의 제2절은 적용되지 아니한다."

"(2) 기술적 보조 수정 - 동 제35장 초두의 조문 목차는 말미에 다음을 추가함으로써 수정된다.

"제3절 - 정보보안

"제3541조 목적

"제3542조 정의

"제3543조 처장의 권한 및 역할

"제3544조 연방기관의 책임

"제3545조 독자적 연간평가

"제3546조 연방정보보안사고센터

"제3547조 국가보안시스템

"제3548조 예산권한

"제3549조 현행법에 대한 효력"

(c) 일부 기관의 정보보안책임

(1) 국가보안책임 - (A) (본 법에 의한 여하한 수정안을 포함하여) 본 법의 여하한 규정도 미합중국법 제44편 제3542조 제(b)항 제(2)호에서 정하고 있는 국가보안시스템의 운영, 통제 또는 관리에 관하여 법률에 따라 대통령령이 정하는 국방장관, 중앙정보국장 또는 기타 기관장의 여하한 권한을 중지시키지 아니한다.

(B) 미합중국법 제10편 제2224조는 다음과 같이 수정된다.

(ⅰ) 제(b)항의 “(b) 목적 및 최소 요건 - (1)”을 삭제하고, “(b) 프로그램의 목적 - ”을 삽입함

(ⅱ) 제(b)항의 제(2)호를 삭제함

(ⅲ) 제(c)항의 제1)호 전단과 관련하여 “인프라” 뒤에 “제44편 제35장 제3절을 준수하는 것을 포함하여”를 삽입함

(2) 1954년 원자에너지법 - 본 법의 여하한 규정도 1954년 원자에너지법(42 U.S.C.2011 등)에 의하거나 이에 따른 여하한 요건의 효력을 중지시키지 아니한다. 제한된 정보 또는 이전에 제한되었던 정보는 1954년 원자에너지법에 따라 처리되고, 보호되며, 분류되고, 등급 하향 조정되며, 비밀취급이 해제된다.

제302조 정보기술관리

(a) 총칙 - 연방법전 제40편 제11331조는 다음과 같이 수정된다.

“제11331조 연방정보시스템 표준에 관한 책임

“(a) 표준 및 지침

“(1) 제정권 - 제(2)호에서 정한 경우를 제외하고 상무부장관은 국가표준기술연구원에서 국가표준기술연구원법(15 U.S.C. 278g-3(a) 제20조 제(a)항 제(2)호 및 제(3)호에 따라 개발한 표준 및 지침을 기초로 연방정보시스템에 관한 표준 및 지침을 제정하여야 한다.

“(2) 국가보안시스템 - (본 조에서 규정하고 있는) 국가보안시스템에 대한 표준 및 지침은 기타 법률에 따라 대통령령으로 개발하고, 제정하며, 집행하고, 감독하여야 한다.

“(b) 강제요건

“(1) 강제권한 - 제(2)호에서 정한 경우를 제외하고, 장관은 연방정보시스템의 운영 또는 보안의 효율성을 개선하기 위하여 장관이 필요하다고 결정하는 범위 내에서 제(a)항 제(1)호에 따라 제정된 표준을 강제하고 구속력을 가지도록 하여야 한다.

"(2) 강제표준의 내용 - (A) 제(a)항 제(1호)에 따라 제정된 표준은 다음과 같은 정보보안 표준을 포함하여야 한다.

"(ⅰ) 국가표준기술연구원법(15 U.S.C 278g03(b)) 제20조 제(b)항이 정한 최소한의 정보보안 요건을 제공함

"(ⅱ) 기타 연방 정보 및 정보시스템의 보안을 개선하는 데 필요함

"(B) 제(A)목에 기술된 정보보안 표준은 강제력과 구속력을 가져야 한다.

"(c) 불승인 또는 변경할 수 있는 권한 - 대통령은 불승인 또는 변경하는 것이 공익을 위한 것이라고 판단한 경우에는 제(a)조 제(1)항에 따른 표준 및 지침을 불승인 또는 변경할 수 있는 대통령의 권한은 위임될 수 없다. 그러한 불승인 또는 변경에 관한 통지는 연방관보에 즉시 발표되어야 한다. 상무부장관은 그러한 불승인 또는 변경의 통지를 받는 즉시 대통령의 지시에 따라 그러한 표준 또는 지침을 폐지하거나 변경하여야 한다.

"(d) 권한의 행사 - 회계 및 정책의 일관성을 유지하기 위하여 상무부 장관은 대통령의 지시에 따라 관리예산처장과 협력하여 본 조에서 규정한 권한을 행사하여야 한다.

"(e) 보다 엄격한 표준의 적용 - 행정기관의 장은 당해 기관의 감독범위 내에 있거나 감독을 받는 정보시스템에 대한 비용절감적인 정보보안을 위하여 본 조에 따라 장관이 제정한 표준보다 더 엄격한 표준을 활용할 수 있다. 단 보다 엄격한 표준은

"(1) 최소한 장관에 의하여 강제력과 구속력을 가지는 적용 가능한 표준을 포함하여야 한다.

"(2) 기타 제44편 제3543조에 의한 정책 및 지침에 따라야 한다.

"(f) 표준공표의 결정 - 본 조에 따른 여하한 표준의 공포에 관한 장관의 결정은 국가표준기술연구원법(15U.S.C. 278g-3) 제20조에서

규정한 국가표준기술연구원이 장관에 대하여 표준안을 제출한 후 6개월 이내에 이루어져야 한다.

"(g) 정의 - 본 조에서

"(1) 연방정보시스템 - '연방정보시스템'이라 함은 행정기관, 행정기관과 계약을 맺은 자 또는 행정기관을 대신하는 또 다른 조직에 의하여 이용되거나 운영되는 정보시스템을 말한다.

"(2) 정보보안 - '정보보안'이라 함은 제44편 제3542조 제(b)항 제(1)호에 규정된 용어의 의미와 동일하다.

"(3) 국가보안시스템 - '국가보안시스템'이라 함은 제44편 제3542조 제(b)항 제(2)호에 규정된 용어의 의미와 동일하다.

(b) 기술적 보조수정 - 동 편 제113장 초두의 조문 목차 중 제11331조에 해당하는 항목은 다음과 같이 수정한다.

"제11331조 연방정보시스템 표준에 대한 책임"

제303조 국가표준기술연구원

국가표준기술연구원법(15 U.S.C 278 g-3) 제20조는 본문을 삭제하고 다음을 삽입하여 수정한다.

"(a) 총칙 - 연구원은

"(1) 정보시스템에 관한 표준, 지침 및 관련 방법을 개발할 의무가 있다.

"(2) (연방법전 제44편 제3542조 제(b)항 제(2)호에 규정된) 국가보안시스템을 제외한 기관, 기관과 계약을 맺은 자 또는 기관을 대신하는 다른 조직에 의하여 이용되거나 운영되는 정보시스템과 관련하여 최소 요건을 포함한 표준 및 지침을 개발하여야 한다.

"(3) 기관의 모든 업무 및 자산에 대하여 적절한 정보보안을 제공하기 위한 최소 요건을 포함한 표준 및 지침을 개발하여야 한다. 단, 그러한 표준 및 지침은 국가보안시스템에 적용되지 아니한다.

"(b) 표준 및 지침에 관한 최소 요건 - 제(a)항에 의한 표준 및 지침은 최소한 다음을 포함하여야 한다.

"(1)(A) 위험수준의 정도에 따라 적절한 수준의 정보보안을 제공하기 위한 목적으로 각 기관에 의하여 또는 각 기관을 대신하여 수집되거나 보존되는 모든 정보 및 정보시스템을 분류하기 위하여 모든 기관이 이용하는 표준

"(B) 그러한 각 분류에 포함되는 정보 및 정보시스템의 유형에 대한 권고를 내용으로 하는 지침

"(C) 그러한 각 분류에 포함되는 정보 및 정보시스템에 대한 최소한의 정보보안요건

"(2) 정보보안사고의 탐지 및 수습에 관한 정의 및 지침

"(3) 정보시스템이 국가보안시스템으로서 법률에 따라 대통령령으로 정한 국가보안시스템에 관한 적용요건과 일치하는지를 확인하기 위하여 국가안전국을 포함한 국방성과 협력하여 개발한 지침

"(c) 표준 및 지침의 개발 - 제(a)항 및 제(b)항에 따른 표준 및 지침 개발에 있어 동 연구원은

"(1) 다음을 보장하기 위하여 (관리예산처장, 국방 및 에너지성, 국가안보국, GAO 및 치안국장을 포함한) 다른 기관 및 사무국과 민간부분에 대하여 자문을 구하여야 한다.

"(A) 정보보안을 개선하고 불필요하고 소모적인 중복노력을 피하기 위한 적절한 정보보안 정책, 절차 및 기술 이용

"(B) 그러한 표준 및 지침이 국가보안시스템 및 그러한 시스템에 포함된 정보를 보호하기 위한 표준 및 지침을 보충함

"(2) 국민에 대하여 표준 및 지침안에 대한 의견개진 기회를 제공하여야 한다.

"(3) 상무부 장관에 대하여 연방법전 제40편 제11331조에 따른 공표를 위하여 다음의 내용을 제출하여야 한다.

"(A) 본 조의 발효일로부터 12월 이내에 제(b)항 제(1)호 제(A)목에 따른 표준

"(B) 본 조의 발효일로부터 36월 이내에 제(b) 제(1)호 제(B)목에 따른 각 분류별 최소한의 정보보안 요건

"(4) 본 조의 발효일로부터 18월 이내에 제(b)항 제(1)호 제(B)목에 따른 지침을 발하여야 한다.

"(5) 가능한 최대한의 범위 내에서 그러한 표준 및 지침이 여하한 특정 하드웨어 또는 소프트웨어를 포함한 특정 상품의 이용 또는 획득을 요하지 않도록 하여야 한다.

"(6) 가능한 최대한의 범위 내에서 그러한 표준 및 지침이 확인된 정보보안 위험에 상응하는 수준의 보호를 제공하는 대안적 솔루션을 허용하는 충분한 유연성을 제공하도록 하여야 한다.

"(7) 가능한 최대한의 범위 내에서 상업적으로 기성 정보보안 상품의 이용을 허용하는 유연하고 시행 중심의 표준 및 지침을 이용하여야 한다.

"(d) 정보보안기능 - 동 연구원은

"(1) 연방법전 제40편 제11331조에 따른 공포를 목적으로 상무부장관에 대하여 제(a)항에 따라 개발된 표준을, 그러한 표준이 강제력 및 구속력을 가져야 하는 범위 내에서 권고안과 함께 제출하여야 한다.

"(2) 요구가 있는 기관에 대하여 다음에 관한 기술적 지원을 제공하여야 한다.

"(A) 제(a)항에 따라 개발된 표준 및 지침의 준수

"(B) 정보보안 사고의 탐지 및 수습

"(C) 정보보안에 관한 정책, 절차 및 업무

"(3) 필요한 범위 내에서 정보보안상의 취약부분과 비용 효율적인 정보보안을 제공하는 기술의 성격 및 범위를 결정하기 위한

연구를 수행하여야 한다.

“(4) 기관의 정보보안에 관한 정책 및 업무에 관한 시행지표 및 수단을 개발하고 주기적으로 개정하여야 한다.

“(5) 정보보안을 강화하기 위한 기관의 잠재적 적용 가능성을 판단하기 위하여 민간부문의 정보보안 정책 및 업무와 상업적으로 이용 가능한 정보기술을 평가하여야 한다.

“(6) 요구가 있는 경우 본 조에 따른 활동결과를 이용하고 적용하는 데 있어 민간부문을 지원하여야 한다.

“(7) 정보보안을 강화하기 위한 기관의 잠재적 적용 가능성을 판단하기 위하여 국가보안시스템을 대상으로 개발된 보안정책 및 업무를 평가하여야 한다.

“(8) 본 조에 따라 개발된 표준 및 지침의 효과를 주기적으로 평가하여 적절한 범위 내에서 개정하여야 한다.

“(9) 제21조에 따라 설치된 정보보안 및 프라이버시 자문위원회의 제(a)항에 따라 개발된 표준 및 지침에 관한 권고안을 권유하고 고려하여야 하며, 동 장관에 대하여 제출된 그러한 표준과 함께 그러한 권고안을 상무부 장관에 대하여 제출하여야 한다.

“(10) 본 조에 의한 책임을 완수하기 위하여 이전 년도에 수행되었고 차기 년도를 대비해 계획을 수립한 활동에 대한 대국민 연차보고서를 준비하여야 한다.

“(e) 정의 - 본 조에서 사용되는

“(1) ‘기관’은 연방법전 제44편 제3502조 제(1)호에서 규정하고 있는 의미와 동일하다.

“(2) ‘정보보안’은 동 편 제3542조 제(b)항 제(1)호에서 규정하고 있는 의미와 동일하다.

“(3) ‘정보시스템’은 동 편 제3502조 제(8)호에서 규정하고 있는 의미와 동일하다.

"(4) '정보기술'은 연방법전 제40편 제11101편에서 규정하고 있는 의미와 동일하다.

"(5) '정보보안시스템'은 연방법전 제44편 제3542조 제(b)항 제(2)호에서 규정하고 있는 의미와 동일하다.

"(f) 예산권한 - 상무부 장관은 국가표준기술연구원이 본 조의 내용을 수행하도록 함에 있어 2003년, 2004년, 2005년, 2006년 및 2007년 각 회계 연도마다 2천만 달러를 집행할 수 있는 권한이 있다.

제304조 정보보안 및 프라이버시 자문위원회

국가표준기술연구원법 제21조는 다음과 같이 수정한다.

(1) 제(a)항에서 "컴퓨터 시스템 보안 및 프라이버시 자문위원회"를 삭제하고 "정보보안 및 프라이버시 자문위워회"를 삽입함

(2) 제(a)항 제(1)호에서 "컴퓨터 또는 통신"을 삭제하고, "정보기술"을 삽입함

(3) 제(a)항 제(2)호에서

(A) "컴퓨터 또는 통신기술"을 삭제하고, "정보기술"을 삽입함

(B) "컴퓨터 또는 통신설비"를 삭제하고, "정보기술"을 삽입함

(4) 제(a)항 제(3)호에서

(A) "컴퓨터 시스템"을 삭제하고, "정보기술"을 삽입함

(B) "컴퓨터 시스템 보안"을 삭제하고, "정보보안"을 삽입함

(5) 제(b)항 제(1)호에서 "컴퓨터 시스템 보안"을 삭제하고, "정보보안"을 삽입함

(6) 제(b)항에서 제(2)호를 삭제하고 다음을 삽입함

"(2) 제20조에 따라 개발된 표준 및 지침안의 검토를 포함하여 연방정부 정보시스템에 관한 정보보안 및 프라이버시 문제에 대하여 동 연구원, 상무부장관 및 관리예산처장에게 조언한다."

(7) 제(b)항 제(3)호에서 "보고"뒤에 "매년"을 삽입함

(8) 제(e)항 뒤에 다음의 신규 항을 삽입함

"(f) 동 위원회는 동 위원회의 대다수가 정하는 지역과 시간 및 장소에서 회의를 개최하여야 한다."

(9) 제(f)항 및 제(g)항을 제(h)항으로 각각 재명명함

(10) 제(9)호에 따라 재명명된 제(h)항을 삭제하고, 다음을 삽입함

"(h) 본 조에서 사용되는 '정보시스템' 및 '정보기술'의 의미는 제20조에서의 의미와 동일하다.

제305조 기술적 보조수정

(a) 컴퓨터보안법 - 연방법전 제40편 제11332조 및 동편 제113장에 관한 조문 목차상 동 조문과 관련된 항목은 폐지된다.

(b) 플로이드 D. 스펜서 2001 회계연도 국방권한법 - 플로이드 D. 스펜서 2001 회계연도 국방권한법(Public Law 106-398)은 제1062조(44 U.S.C. 3531 note)를 삭제함으로써 수정된다.

(c) 문서업무감축법 - (1) 연방법전 제44편 제3504조 제(g)항은 다음과 같이 수정된다.

(A) 제(1)호 말미에 "및"을 추가함

(B) 제(2)호에서

(ⅰ) "제40편 제11331조 및 제11332조 제(b)호 및 제(c)호"를 삭제하고, "제40편 제11331조 및 본 장 제2절"을 삽입함

(ⅱ) "및"을 삭제하고, 마침표를 삽입함

(C) 제(3)호를 삭제함

(2) 동 편 제3505조는 말미에 다음을 추가함으로써 수정된다.

"(c) 주요 정보시스템의 목록 - (1) 각 기관의 장은 (주요 국가보안시스템을 포함하여) 동 기관이 운영하거나 동 기관의 통제를 받는 주요 정보시스템의 목록을 개발하고 보존하여야 한다.

"(2) 본 항에 따른 목록에 등재된 정보시스템의 확인에는 당해 기관이 운용하지 아니하거나 당해 기관의 통제를 받지 아니하는 것을 포함하여 각 시스템과 다른 모든 시스템 또는 네트워크

간의 인터페이스에 대한 확인이 포함된다.

"(3) 동 목록은

"(A) 최소 매년 업데이트를 하여야 한다.

"(B) 감사원장이 이용 가능하여야 한다.

"(C) 다음을 포함하여 정보자원관리를 지원하기 위하여 이용되어야 한다.

"(ⅰ) 제3506조 제(b)항 제(4)호에 따른 정보자원의 목록의 준비 및 유지

"(ⅱ) 제3506조 제(h)항 제40편 제3절 및 관련 법률과 지침에 따른 정보기술의 계획, 예산, 획득 및 관리

"(ⅲ) 제2절에 따른 정보보안통제의 감시, 시험 및 평가

"(ⅳ) 연방법전 제5편 제552조 제(g)항에 따른 주요 정보시스템 색인의 준비

"(ⅴ) 제21장, 제29장, 제31장 및 제33장에 따른 기록관리에 필요한 정보시스템 목록의 준비

"(4) 처장은 본 항의 요건을 시행하기 위한 지침을 발하고 감독하여야 한다.

(3) 동 편 제3506조 제(g)항은 다음과 같이 수정된다.

(A) 제(1)호 말미에 "및"을 삽입함

(B) 제(2)호에서

(ⅰ) "제40편 제11332조"를 삭제하고 "본 장 제2절"을 삽입함

(ⅱ) "및"을 삭제하고, 마침표를 삽입함

(C) 제(3)호를 삭제함

제 4 절 지출승인과 시행일

제401조 지출승인

제1절 또는 제2절에서 규정하고 있는 수정사항을 포함하여 당해 절

에서 구체적으로 규정된 기금전용에 관한 권한부여를 위한 목적을 제외하고는 2003 회계 연도부터 2007 회계 연도까지 매 회계 연도마다 제1절과 제2절의 내용을 이행하는 데 필요한 만큼의 금액의 지출을 승인한다.

제402조 시행일

(a) 제1절 및 제2절

(1) 총칙 - (2)항에서 규정한 경우를 제외하고, 제1절, 제2절 및 그에 따른 수정사항들은 이 법의 입법일로부터 120일 후에 시행한다.

(2) 즉시 시행 - 제207조, 제214조 및 제215조는 이 법의 입법일로부터 시행한다.

(b) 제3절 및 제4절 - 제3절과 본 절은 이 법의 제정일로부터 시행한다.

참 고 문 헌

한국정보보호진흥원, 민간부문 정보보호 정책 연혁, 2004.

국회 과학기술정보통신위원회 [편] 국회과학기술정보통신위원회, 정보통신 유·무선 서비스 관련 보안 강화를 위한 법제 연구, 2003.

과학기술부 과학기술부, 과학기술정보 보호체제 강화방안 연구, 2002

최영곤·도상호, 디지털정보의 보안, 博英社, 2000.

홍경효, 정보 보안과 정보 보호 정책. 技術士(통권185호), 韓國技術士會, 2006.

김일환, 情報保安關聯法制整備의 基準과 內容에 관한 硏究, 土地公法硏究(제26집), 韓國土地公法學會, 2005.

강경근, 情報保護의 憲法規範的 接近과 展望, 공법학연구(제6권 제2호), 한국비교공법학회, 2005.

이만영 외 공저, 인터넷 정보보안, 생능출판사, 2002.

한승오·김영대, 정보시스템의 정보보호를 위한 보안체제에 관한 연구, 논문집 제4집, 호남대학교대학원, 2004.

최창학, 한국의 전자정부 정책의 현재와 미래, 정보과학회지(제22권 제11호 통권 제186호), 한국정보과학회, 2004.

김대호·오일석, 미국 전자정부 정보보안 법제 동향, 情報保護學會誌 제13권 제3호, 韓國情報保護學會, 2003.

홍승필·고제욱, 정보보안 기술과 구현, 파워북, 1998.

松田貴典, ビジネス情報の法とセキュリティ : 情報システムの脆弱性と情報資産保護, 白桃書房, 2005.

山崎文明, 情報セキュリティと個人情報保護完全對策:完全對策, 日經BP社 2004.

Allison, Coleman, “Protecting Confidential Information”, computer law, Blackstone Press Limited, 1996.

Chris Reed, Computer Law, 3ed, Blackstone Press Limited, 1996.

Delta, Matsuura, Law of the Internet, Aspen Law, 1999.

John D. Zelezny, Communications Law, Wadsworth Publishing Co., 1997.

Kent D. Stuckey, Internet and Law, Law Journal Seminar-Press, 2000.

Bullesbach, “Das neue Bundesdatenschutzgesetz”, NJW 1991, 2593ff..

Diethelm Klippel, “Deliksrechtliche Probleme des Datenschutzes”, Betriebs-Berater 1983. 407ff..

Ernst, “Internet and Recht”, JuS 1997, 776ff..

Geis, “Internet und Datenschutzrecht”, NJW 1997, 288ff..

Hoeren, “Internet und Recht -Neue Paradigmen des Informationsrechts”, NJW 1998, 2849ff..

Kuong, J.F., Computer Auditing, Security, and Internal Control Manual, Prentice-Hall, Inc., 1987.

Mayer, “Recht und Cyberspace”, NJW 1996, 1782ff..

Parker, Donn B., Computer Security Management, Reston Publishing Co. Inc., 1981.

Schneider, “Datenschutz und Neue Medien”, NJW 1984, 390ff..

Schack, “Neue Techniken und Geistiges Eigentum”, JZ 1998, 753ff..

Spindler, “Haftungsrechtliche Grudprobleme der neuen Medien”, NJW 1997, 3193ff.