워크샵 2007 -

콘텐츠산업법제지원사업(III)

정보보안정책과 입법동향

2007. 4. 6.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

워크샵 일정

◈ 주 제 : 정보보안정책과 입법동향

◈ 일 정 : 2007년 4월 6일(금요일) 15:00 ~ 18:00

◈ 장 소 : 한국법제연구원 1층 대회의실

◈ 구 성

◇ 사 회

이관희 (경찰대학교 교수)

◇ 주제발표

제 1주제 : 공공분야의 정보보안정책과 입법현황

발 표 자 : 송경주 서기관, 김완평 사무관 (행정자치부 전자정부본부)

토 론 자 : 이인호 교수 (중앙대학교 법학과)

현대호 박사 (한국법제연구원 부연구위원)

제 2주제 : 정보통신분야의 정보보안정책과 입법현황

발 표 자 : 오상균 서기관 (정보통신부 정보보호기획단 정보보호정책팀)

토 론 자 : 이화실 입법조사관 (국회 과학기술정보통신위원회)

이철원 정책실장 (국가보안기술연구소)

제 3주제 : 국가의 정보보안정책과 입법현황

발 표 자 : 국가사이버안전센터

토 론 자 : 고낙훈 법제관 (법제처)

김충섭 입법조사관 (국회 정보위원회)

◇ 종 합 토 론

목 차

◎ 제 3 주제 국가의 정보보안정책과 입법현황 (국가사이버안전센터)

개 회 사

이 관 희
(경찰대학교 교수)

오늘날 인터넷은 일상생활에서 경제활동에 이르기까지 중요한 통신수단이자 정보전달수단으로 지위를 차지하고 있으며, 정치·경제·사회 및 문화 등 모든 영역에 엄청난 변화를 가져오고 있다. 따라서 개인은 인터넷상에서 인격권·재산권 및 행동자유를 누리게 됨에 따라 현행법의 개정이나 새로운 입법의 제정이 나타났다.

공공분야에서도 고도화된 정보시스템과 초고속정보통신망의 활용은 종이문서에 의한 행정정보의 관리·처리에 대한 용이성과 그 보관에 편리성을 가져온 것에 그치지 아니하고, 전자화 된 파일형태로 행정정보를 이용·제공할 수 있도록 하였다. 또한 전자적 형태로 이용·제공되는 행정정보의 범위도 급속히 확대되고 있고, 이용·제공의 방식도 다양화되고 있으며, 이용기관도 행정기관에서 공공기관 및 금융기관으로 넓혀지고 있다.

이상과 같은 사회 각 분야의 정보화 현상에 따라 정보시스템과 정보보안이 중요한 사회현안으로 등장하고 있으며 이와 같은 현실을 인식하여 한국법제연구원에서 관련 정부부처(국가정보원, 행정자치부 및 정보통신부 등), 입법관련기관(법제처, 국회 등) 및 연구기관(국가보안기술연구원, 한국정보보호진흥원 등)이 참여하여 공동으로 정보보안에 대한 국가정책과 입법개선 방안을 논의하는 것은 중요한 의미가 있다.

제 1 주제

공공분야의 정보보안정책과 입법현황

발 표 : 송경주 (행정자치부 전자정부본부 서기관)
김완평 (행정자치부 전자정부본부 사무관)

토 론 : 이인호 (중앙대학교 법학과 교수)
현대호 (한국법제연구원 부연구위원)

전자정부 안전관리 대책과 입법현황

송경주 서기관 · 김완평 사무관
(행정자치부 전자정부본부)

I 전자정부 안전관리체계 확립

□□ 정부보안관제센터를 통해 해킹, 바이러스 등 사이버위협 상황을 실시간으로 모니터링하여 적시 대응할 수 있게 하고,

□□ 전자정부침해사고대응팀(G-CERT)을 구성하여, 관련 기관간에 보안정보공유 및 공동대응 등 상호 협력체계 구축

❑ 전자정부 종합보안관제센터 설치 · 운영

❍ 인터넷망을 통해 유입되는 바이러스 차단 및 예방활동 강화
- e-메일을 통한 바이러스 유포 차단, 광고성 e-메일폭탄 차단, 바이러스 감염 치료 등

❍ 각종 사이버공격 징후탐지 및 유해트래픽 차단
- 해킹시도 등 사이버침입 탐지 및 조치, 공격 발신지 차단 등

❍ 전자정부 정보자원에 대한 침해사고 발생시 국가사이버안전센터, 인터넷침해사고대응센터 등 관련 기관과 공동 대응

❍ 전자정부보안 정기웹진(월간) 발간 · 배포(331개 기관)

❍ 앞으로, 사이버공격 감시·탐지·차단 뿐만아니라 사이버위협 상황에 대한 추적기능을 보강하여 사이버안전관리 강화

❑ 전자정부 대민서비스 침해사고대응팀(G-CERT) 구성·운영

❍ 중앙행정기관, 지방자치단체 등 각 행정기관간에 전자정부 정보보안정보 공유 및 상호 협력체계 구축

❍ 전자정부 대민서비스 분야에 대한 침해사고 예방, 침해사고처리 공동 지원

- 보안침해사고 예방 및 사고처리는 국정원과 합동조사 및 복구 지원팀을 구성하여 지원

❍ 각종 사이버위협 및 침해사고 대응 기술력 강화를 위한 교육 및 세미나 개최

❑ 정부원격근무서비스(GVPN) 제공

❍ 공무원이 재택·출장 등 원격지에서도 인터넷을 통해 안전하게 정부내부망에 접속하여 업무를 수행할 수 있도록 GVPN서비스 지원 강화

GVPN(Government Virtual Private Network) 서비스

전자업무관리시스템 등 공무원의 행정내부 업무수행을 위해 필요한 시스템은 보안성이 강화되어 있는 정부내부망에 연결되어 있으며, 퇴근 후 또는 출장중에 원격지에서 인터넷망을 통해 정부내부망에 접속할 수 있도록 해주는 서비스

❍ 정부원격근무(GVPN)서비스 활용 주요업무

- '07. 2월 현재, 전자결재, 정부 e-메일시스템, e-전자감사시스템 등 180개 기관 206개 업무에서 32,000여 공무원이 활용 중

Ⅱ 행정전자서명 인증관리 및 암호이용체계 확립

□□ 유무선 사이버행정 환경에서 공무원과 각 행정기관에 대한 신원 확인 및 전자문서의 위변조 방지를 위해, 행정전자서명 인증서 발급 및 인증서비스 제공

□□ 중요 전자문서 및 행정정보의 기관간 안전한 유통을 위해 전자정부 암호이용체계 구축·운영

❑ 행정전자서명인증체계(GPKI) 구축·운영

❍ 정부의 행정전자서명인증체계(GPKI)

- 최상위인증기관(Root CA)인 행정자치부가 정부의 행정전자서명 인증관리 전반에 대해 총괄·조정 역할을 담당하고,
- 6개 인증기관(CA)과 29개 등록기관(RA)을 두어 인증서 발급·관리, 인증서 사용자 등록업무를 수행

❍ 행정전자서명 인증서 등록 및 발급현황

- 행정전자서명은 공무원 개인용과 기관용으로 구분하고, 각 기관에게는 전자관인용과 서버장비 인증용으로 구분하여 발급
- '07. 2월 현재 공무원 개인용 338,418건, 기관용으로 4,926건 발급

❍ 행정전자서명인증 활용업무 현황

- ’07. 2월 현재 중앙행정기관, 지방자치단체 등 57개 기관의 195개 업무에서 행정전자서명 인증서를 적용
- 행정전자서명은 행정정보공유, 기관간 전자문서유통 등 주요 전자정부 시스템에서 신원확인, 주요문서정보의 암호화 유통 용도로 사용
- 핸드폰, PDA를 이용한 전자결재시에는 무선 인증서비스 제공

❍ 앞으로의 확대 추진계획

- 전자정부법 개정에 따라 행정전자서명 인증서 발급서비스 확대

※ 전자정부법 개정(’07.1.3)에 따른 인증서 발급 확대범위

- 「행정기관 및 공무원」→ 행정기관과 잔자문서를 유통하거나 행정정보를 공동이용하는 기관 및 그 기관의 직원

❑ 전자정부 정보시스템에 대한 접근권한관리

❍ 각급 행정기관 공무원의 업무별 역할과 담당업무에 따라, 전자정부 정보자원에 대한 접근제어관리를 통해 보안성 강화

- ’07. 2월 현재 행정정보공동이용시스템, 전자민원G4C 등의 전자정부시스템에서 적용 中

❑ 전자정부 암호이용체계 확립

❍ 중요 전자문서 및 행정정보를 암호화하여 유통할 수 있는 전자정부 암호이용기반체계 구축・운영

❍ 중요 전자문서의 암호화 유통시 필요한 암호키를 분산 보관·관리하고, 분실 또는 훼손시에는 암호키 복구서비스 제공

Ⅲ 공공기관의 개인정보보호 강화

□□ 온라인을 통한 공공서비스 제공이 증가하고, 국민들의 개인정보보호에 대한 인식이 높아짐에 따라, 공공기관의 개인정보보호에 대한 관리 강화

❑ 개인정보보호 관련 법제도 개선 추진

❍ 주민등록번호를 단순 도용하는 경우에도 3년 이하의 징역 또는 1천만원 이하의 벌금에 처할 수 있도록 주민등록법 개정('06.9월 시행)

❍ 개인 프라이버시 보호를 위해 CCTV 설치·이용 법적 규제 추진

- 국회에 CCTV와 관련하여 "공공기관의 폐쇄회로 설치에 관한 법률(안)" 등 4종의 법률안 계류 중
- 2.26(월) 국회에서 「공공기관의 개인정보보호에 관한 법률」을 포함, 국회 계류중인 의원발의 법안들의 입법 추진

❑ 공공기관 홈페이지를 통한 개인정보노출 방지 대책 추진

❍ 한국정보사회진흥원 내 전담인력 확보하고 점검 프로그램을 활용한 상시모니터링 체계 구축

❍ 홈페이지 개발시 개인정보 노출을 방지할 수 있는 기술적 가이드라인 적용 강화

- ❍ 공공기관별 개인정보 노출 수시점검 및 홈페이지 자료게재 프로세스 개선
- ❍ 공공기관별 개인정보 게재 방지프로그램 설치 권장
- ❍ 사이버 신원확인 과정에서의 주민번호 노출·도용 방지시스템 구축
- ❍ 행자부에서 개인정보 노출여부를 모니터링하여, 언론매체 및 홈페이지 등에 공개추진
- ❍ 보안서버(행정전자서명 SSL 인증서) 보급 확대

❑ 개인정보보호 교육 및 홍보 강화

- ❍ 행정·공공기관을 대상으로 개인정보보호 교육 실시
- ❍ 기관별 자체 교육용 영상홍보물, 교육교재 등 제작·배포
- ❍ 개인정보보호 인식과 사회적 관심의 제고를 위해 매달 1일을 '개인정보보호의날'로 지정·운영하며, 권역별로 순회하며 공청회·토론회·컨퍼런스 등을 개최

❑ 공공기관의 개인정보처리 실태점검 및 지도 강화

- ❍ 정기적으로 개인정보 노출 실태점검 및 지도

  ※ '07.5월까지 공공기관 27,000여 홈페이지를 대상으로 정밀 재점검을 실시, 개인정보 취약점을 일제 정비

- ❍ 개인정보보호 취약기관을 대상으로 보안컨설팅 수행
- ❍ 특히, 개인정보노출 등으로 언론에 보도된 기관 또는 대민서비스 기관에 대해서는 연 2회 이상 집중적인 실태점검 실시

붙임	전자정부 보안정책 관련 입법현황

< 총 평 >

○ 전자정부 보안정책과 관련한 별도의 독립법은 없는 상황

- 전자정부법에 일부 관련 조항

※ '07.1.3 개정안에 의해 전자문서 보안조치, 전자적 대민서비스 보안대책 등 보안관련 규정 강화

- 개인정보보호분야와 관련하여 「공공기관의개인정보보호에관한법률」이 있음

1. 전자정부 보안정책 일반 : 전자정부법

□ 전자정부법 개요

○ 연 혁

- 제정 : '01. 3. 28(시행 : '01. 7. 1)
- 개정 : '01. 12. 31 / '03. 5. 15 / '06. 10. 4 / '07. 1 .3

○ 입법취지

- 행정업무의 전자적 처리를 위한 기본원칙·절차·추진방법 규정
- 전자정부 사업 촉진
- 행정기관의 생산성·투명성·민주성 제고 및 국민의 삶의 질 향상

○ 적용범위

- 행정기관 업무의 전자적 처리

※ 행정기관의 범위

- 국회・법원・헌법재판소・중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관 포함) 및 그 소속기관, 지방자치단체

□ 전자정부법상 보안관련 규정

○ 개인정보보호 원칙(제2조)

- 행정기관이 보유・관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니됨

○ 행정전자서명 인증

- 정의(제2조제6호) : 행정전자서명은 전자문서를 작성한 행정기관, 행정기관과 전자문서를 유통하거나 행정정보를 공동이용하는 법인・기관 및 단체 내지 업무 담당자의 신원과 전자문서의 변경여부를 확인할 수 있는 정보로서 그 문서에 고유한 것

※ 행정전자서명 발급범위 확대 : (기존) 행정기관, 공무원 → (신규) 행정기관과 전자문서를 유통하거나 행정정보를 공동이용하는 기관 및 업무 담당자

- 행정전자서명의 효력, 중앙사무관장기관의 인증업무(제18조, 제20조, 제22조의2)
  ・전자공문서, 전자문서 유통, 행정정보 공동이용시 행정전자서명 사용

※ (기존) 전자공문서에 사용 → (신규) 전자문서 유통, 행정정보 공동이용시에도 사용

· 전자문서상 행정전자서명은 해당기관의 관인·공인, 담당자의 서명이 있는 것으로 보며, 행정전자서명이 된 후에 당해 전자문서는 내용이 변경되지 않은 것으로 추정
· 중앙사무관장기관의 장이 행정전자서명에 대한 인증업무 수행
· 중앙사무관장기관의 장은 행정전자서명과 공인전자서명의 연계방안을 마련해야 함

○ 정보통신망 등의 보안대책 수립·시행(제27조)

- 정보통신망과 행정정보에 대한 보안대책 수립 의무 : 국회·법원·헌법재판소·중앙선거관리위원회·행정부는 정보통신망과 행정정보 등에 대한 보안대책을 마련해야 하고, 각 행정기관의 장은 소관 보안대책을 수립·시행해야 함
- 정보통신망을 이용한 전자문서 보관·유통 관련 보안조치 의무(신규) : 행정기관의 장은 정보통신망을 이용한 전자문서 보관·유통시 국가정보원장이 안전성을 확인한 보안조치를 하여야 하고, 국가정보원장은 그 이행여부를 확인할 수 있음(행정부 이외는 임의사항. 단, 국회·법원·헌법재판소·중앙선거관리위원회의 경우는 이에 준하는 보안조치를 강구해야 함)

○ 전자적 대민서비스 보안대책(제39조의2)(신규)

- 행정자치부장관이 국가정보원장과 사전협의를 거쳐 마련해야 함
- 행정부 내 각 행정기관은 기관별 보안대책을 수립·시행해야 함

○ 전자정부서비스보안위원회 설치·운영(제39조의3)(신규)

- 전자적 대민서비스와 관련된 보안대책을 심의하기 위하여 행정자치부 소속하에 설치(위원장 : 행정자치부장관)

2. 공공기관 개인정보보호 분야
: 공공기관의개인정보보호에관한법률

□ 공공기관의개인정보보호에관한법률 개요

○ 연 혁

- 제정 : ’94. 1. 17
- 개정 : ’99. 1. 29

※ 현재, 개정안 국회 계류 중

○ 입법취지

- 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위해 그 취급시 필요한 사항 규정
- 공공업무의 적정한 수행을 도모하고 국민의 권리와 이익을 보호

○ 적용대상 및 범위

- 컴퓨터 처리정보(생존하는 개인에 관한 정보)
- 공공기관(국가행정기관, 지방자치단체, 기타 공공단체)

○ 구 성 : 본문 5장 25조, 부칙

□ 주요 내용

○ 개인정보의 취급관리

- 수집범위 : 정보주체의 동의 또는 법률에 근거하여 적법·공정한 방법으로
- 보유범위 : 소관업무 수행의 명확한 목적과 필요 최소한의 범위 내

- 사전통보 : 개인정보파일 보유기관은 행정자치부 장관, 중앙행정기관의 장에 반드시 사전통보
- 개인정보 파일의 공고 : 수집목적, 존재 등을 국민들이 알 수 있도록 연 1회
- 처리정보의 이용 및 제공 제한 : 법령이 정하는 경우 외 정보주체 의사에 반하여 사용되어서는 아니됨
- 취급자의 의무 : 누설·권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적 사용 금지

○ 정보주체의 권익보장

- 열람·정정·불복 청구

○ 지도·감독체계

- 개인정보보호심의위원회 : 국무총리 소속 자문위원회(위원장 : 행정자치부차관), 개인정보보호 관련 정책·제도개선, 의견조정 등
- 행정자치부 : 실태조사, 자료제출요구, 의견제시 및 권고
- 중앙행정기관의 장 : 소속·산하기관 등에 대한 지도·감독

□ 관련 입법동향

○ CCTV 관련 법안

- 공공부문의 CCTV 설치·관리와 관련된 3개 의원발의안과 공공기관의개인정보보호에관한법률안을 통합, 대안을 마련하여 국회 심의 중

○ 개인정보보호 기본법(3개 의원발의안) 등 개인정보보호 관련 6개 법안 국회 계류 중

○「행정정보공동이용법」제정 추진

- 행정기관과 공공·금융기관간 행정정보공동이용시 개인정보보호를 위한 원칙과 절차 규정(국회 계류 중)

토 론 문

이 인 호
(중앙대학교 법과대학 부교수・헌법학)

1. 전자정부의 이념에서 "개인정보의 공동이용"이라는 요소를 삭제하여야 한다.

2001년 3월 28일 제정된 「전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률」("전자정부법")은 전자정부의 운영원칙의 하나로서 행정정보공동이용의 원칙과 개인정보보호의 원칙을 선언하고 있다. 즉, 제11조(행정정보공동이용의 원칙)는 "행정기관은 수집・보유하고 있는 행정정보[1]를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다."고 규정하고 있고, 제12조(개인정보보호의 원칙)는 "행정기관이 보유・관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니된다."고 선언하고 있다.

그러나 이 법상의 개인정보보호의 원칙은 선언에 불과할 뿐 이를 구체화하는 규정은 존재하지 않으며, 대신 행정정보공동이용의 원칙에 보다 초점을 맞추고 있다. 동법 제21조는 행정기관 간에 행정정보를 공동이용하도록 의무지우고 있고, 특히 "공공기관의개인정보보호에관한법률 제10조 제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보"를 공동이용 대상정보의 하나로 규정하고 있다. 그리고 동법

1) "행정정보"라 함은 "행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호・문자・음성・음향・영상 등으로 표현된 것"을 말한다(법 제2조 제4호). 따라서 개인정보도 여기의 행정정보의 개념에 속한다.

제22조는 행정정보공동이용의 절차를 규정하고 있으나, 이 규정은 공동이용의 활성화를 위한 일반적 절차를 규정한 것일 뿐 달리 개인정보보호를 위한 절차적 제한을 가하고 있는 규율은 아니다.

요컨대, 현행 우리의 전자정부법제는 효율성 관점에 입각하여 “개인정보의 공동이용”이라는 요소를 너무나 당연한 전제로 삼고 있다. 공공부문의 개인정보보호법제가 미흡한 상황에서 개인정보의 공동이용을 강조하는 것은 위험한 일일 수 있다.

2. 개인정보DB는 각각 그 목적별로 분리되어 존재하여야 한다. 예외적으로만 computer matching이 허용되어야 한다.

개인정보분리의 원칙은 특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지되어야 한다는 요청이다.

그런데 현행의 「공공기관의 개인정보 보호에 관한 법률」(“공공기관 개인정보보호법”)은 그 입법목적이 “컴퓨터에 의하여 처리되는 개인정보의 보호”에 있음에도 불구하고, 디지털화된 개인정보의 특성을 충분히 고려하지 못한 채 개인정보화일을 마치 종이 문서인 양 취급하고 있는 것이 아닌가 생각된다. 컴퓨터 데이터베이스는 그 전부 또는 일부가 다른 데이터베이스의 일부 또는 전부와 매우 용이하게 결합되어 새로운 데이터베이스를 형성할 수 있다. 특히 우리나라의 경우 표준 개인식별자인 주민등록번호를 중심으로 하여 모든 개인정보화일을 구축하고 있기 때문에, 개인정보화일간의 정보통합은 매우 용이하다. 이는 포괄적인 개인정보통합관리시스템의 구축을 용이하게 하고, 그 결과 국가는 개인의 총체적인 인격상을 손쉽게 파악할 수 있는 위험성을 드러낸다. 이것은 개인정보자기결정권의 헌법정신과 양립하기 어렵다. 개인정보자기결정권은 타인의 수중에서 총체적인 인격상이 형

성되는 것 자체를 거부하는 개인의 기본권이기 때문이다.

그럼에도 공공기관개인정보보호법에는 컴퓨터결합 등에 의한 정보통합을 효과적으로 규율하는 장치가 대단히 미흡하고, 심지어 전자정부법은 컴퓨터결합을 통한 공동이용을 오히려 의무화하고 있다. 보유목적 외의 이용 및 제공이 정보주체의 동의나 인식 없이 폭넓게 허용되고 있는 반면에, 이러한 이용 및 제공의 결과 컴퓨터결합 등에 의한 새로운 개인정보화일의 생성을 명시적으로 금지하는 규정을 두고 있지 않다.

다만, 법 제10조 제3항은 보유목적 외 제3자 제공의 경우 보유기관의 장이 그 수령기관에 대하여 "사용목적·사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 강구하도록 요청하여야 한다."고 규정하고 있고, 시행령은 그 정보제공이 "통신망을 이용하여" 이루어지는 것일 때 만약 수령기관이 위 제한이나 요청사항을 이행하지 않는 경우에는, 보유기관의 장은 "즉시 처리정보의 제공을 중지"하도록 하고 있을 뿐이다(시행령 제12조 제2항). 그러나 이들 규정만으로는 개인정보의 통합에 따르는 위험성을 차단하기에는 역부족이다.

3. 현행의 공공기관개인정보보호법을 실질적인 '개인정보보호법'으로 개정하여야 한다.

목적구속의 원칙이란 '개인정보를 수집하는 목적은 (i) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ii) 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다(목적일치성)'는 요청이다. 이 원칙은 개인정보 수집기관 내부의 이용을 제한함과 동시에 특히 수집기관 이외의 제3자 제공을 통제하기 위한 것이다. 물론 이 원칙이 절대적일 수는 없고, 법률이 명시적으로 허용하는 예외가 있을 수 있다. 다만, 제3자 제공의 경우에도 위 수집제한의 원칙이 적용되기 때문에 제공목적의 정당성, 제공범위의 필요최소성, 제공방식의 합리성, 정보

주체의 인식명확성이 요구된다.

공공기관개인정보보호법 제10조는 사전에 공시된 개인정보화일의 보유목적이 아닌 다른 목적으로 처리정보를 이용하거나 제공하는 것을 금지하는 이른바 목적구속의 원칙을 규정하고 있다.

그러나 여기에는 매우 광범위한 예외가 인정되고 있다. 첫째, 다른 법률이 보유목적 이외의 목적으로 보유기관의 내부에서 이용하는 것을 허용하거나 또는 제3자 제공을 허용하는 경우에는 그에 따른다(제10조 제1항 전단). 따라서 공공기관개인정보보호법이 선언하는 목적구속의 원칙은 다른 법률에 의하여 얼마든지 훼손될 수 있다. 즉 위 법상의 목적구속의 원칙은 다른 법률에서 보유목적 외의 이용 및 제공을 규정하고 있지 않는 한도 내에서만 적용되는 원칙일 뿐이다. 이러한 규범적 태도는 공공기관개인정보보호법이 기본법으로서의 성격을 가지는 것이 아니라 단순한 일반법으로서의 성격을 가질 뿐이라는 것을 의미한다. 다시 말해서, 다른 법률의 규정에도 불구하고 동법상의 목적구속의 원칙이 적용되는 것이 아니라, 언제든지 다른 법률의 규정에 의하여 목적구속의 원칙이 배제될 수 있는 것이다. 이러한 규범적 성격은 이미 동법 제3조 제1항에서 선언되고 있다.

둘째, 이 법 자체에서도 8가지 광범위한 예외[2]를 인정하고 있다. 이러한 예외의 경우에는 사전에 공시된 보유목적에 구속되지 않고 얼마

2) "1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우
3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우
4. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우
6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
7. 법원의 재판업무수행을 위하여 필요한 경우
8. 기타 대통령령이 정하는 특별한 사유가 있는 경우" (법 제10조 제2항 본문 각호)

든지 다른 용도로 수집기관 내부에서 활용할 수 있으며, 또 정보주체의 동의를 받거나 통지함이 없이 임의로 제3자에게 제공할 수 있다(법 제10조 제2항 본문). 이에 따라 각 공공기관이 자신이 보유하는 개인정보화일과 다른 기관이 보유하는 개인정보화일을 상호 연결시키는 것(computer matching)이 법적으로 허용되어 있는 셈이다.

여기서 특히 제2호, 6호, 7호, 8호의 예외사유가 문제된다. 이처럼 광범위한 예외는 목적구속의 원칙을 무의미하게 만들 가능성을 지니고 있기 때문이다. 그 중에서도 특히 제2호의 사유는 행정기관 상호간에 거의 무제한적으로 개인정보를 공동이용할 수 있도록 하는 포괄적인 조항이다. 각 행정기관의 활동 중 "법률에서 정하는 소관업무의 수행"이 아닌 것이 없기 때문이다. 더 나아가, 제8호는 소관업무의 수행과 관련이 없는 보유목적 이외의 이용과 제3자 제공(예컨대, 상거래의 활성화를 위한 이용 및 민간기업에의 제공 등)을 포괄적이고 무제한적으로 대통령령에 위임하고 있다. 현행 시행령은 이러한 특별사유를 별도로 정하고 있지 않지만, 언제든지 대통령령에 의해 목적구속의 원칙이 파기될 수 있는 규범상태라고 하겠다. 다만, 법은 이 같은 보유목적 이외의 이용 및 제3자 제공에 대해 몇 가지 실체적 및 절차적 제한을 두고 있다.

4. 정보보안의 문제는 정부 내부의 문제만이 아니며 민간기관과 partnership 체제를 구축하지 않으면 해결하기 어렵다.

사이버테러 대응업무를 효율적으로 수행하기 위해서는 국가기관과 공기업, 민간의 기간통신사업자, 연구기관, 학계, 민간의 보안업체 등이 총망라돼 국가 정보보안정책을 도출해야 한다. 현재 분산 운영되고 있는 민·관의 침해사고대응센터(CERT)와 정보공유분석센터(ISAC)

를 연계해 범국가적 차원의 조기경보・대응체계를 구축하고, 해외 대응기구와의 협조를 강화해야 할 필요가 있다.

또한 민간분야와의 정보공유가 원활하게 이루어져야 한다. 세계 각국은 민간분야의 사이버 테러 징후를 분석하고 공유하는 정보공유분석센터(ISAC) 구축을 추진하고 있는데, 기업비밀 보호를 위해 민간 자율로 운영하면서 정부기관과 사이버테러 정보를 공유하는 방식을 취하고 있다. 정보보안은 정보통신부뿐만 아니라 군과 경찰・국가정보원과 관련되는 사안으로 민・관・군의 합동 협조체제 구축이 필요하다. 현재 운영되고 있는 정보통신기반보호위원회를 민・관・군 합동기구로 확대 개편하는 것을 검토할 필요가 있다.

토 론 문

현 대 호
(한국법제연구원 부연구위원, 법학박사)

1. 행정자치부의 향후 추진보안 정책과 관련하여

행정자치부는 공공분야의 전자정부사업을 총괄하고 있으며, 정부조직법 제34조제1항에서 전자정부사업을 명문화하고 있다. 더 나아가서는 전자정부법을 소관법률로 하고 있고, 동법 제27조와 제39조의2 및 제39조의3에서는 전자정부와 관련된 보안대책의 수립 등에 대한 행정기관의 의무 등을 규율하고 있다.

사이버공간에서의 정보 등에 대한 구체적인 보안책임은 오프라인에서와 마찬가지로 각각 해당기관의 장이 책임을 진다. 따라서 사이버공간에서 각각 해당기관이 수행하고 있는 행위 등에 관련된 보안도 해당기관이 책임을 지고 수행하는 것이 적절하다. 대체적으로 이와 같은 방식으로 현행법령이 입법화되어 있는 것으로 판단되며, 행정자치부가 2007년 01월에 전자정부법을 개정하여 제39조의2와 제39조의3을 신설한 것은 중요한 의미가 있다고 사료된다.[1)]

---

1) **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 인정

그런데 이들 조항의 신설과 관련하여 구체적으로 공공분야의 정보보안과 관련하여 행정자치부의 업무와 향후의 역할이 어떻게 세분화되고 집행의 실효성을 담보될 것인지에 대한 정책 등이 마련되어 있는가에 대한 의문이 제기된다.

2. 행정자치부의 향후 행정전자서명(GPKI)과 공인전자서명(NPKI)의 활용범위에 관련하여

2007년 01월 개정된 전자정부법은 제20조제1항에서 “전자공문서에는 행정전자서명을 사용한다. 다만, 행정기관은 「전자거래기본법」 제2조제5호의 규정에 의한 전자거래를 효율적으로 운영하기 위하여 공인전자서명을 사용할 수 있다”고 규정하고 있으며, 신설된 제22조의2에서 행정전자서명을 행정기관 이외에 행정정보를 공동이용하는 공공기관 및 금융기관 등에게 발급하고, 이용기관의 경우 행정전자서명을

하는 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.

이용하여 공동이용하도록 강제하고 있다.[2] 행정전자서명과 공인전자서명의 법적효력은 관련법률(전자정부법과 전자서명법)에 의하여 차이가 없고, 단지 공공분야(전자공문서와 행정정보공동이용에 관련된 분야)에 행정전자서명을 이용하는 것을 강제하는 것에 차이가 발견된다.

그러면 향후 계속적인 민원서비스의 전자화 등에 따라 행정전자서명과 공인전자서명이 중첩적으로 활용될 수도 있는 영역이 나타날 수도 있는데, 이와 관련하여 행정자치부의 입장은 무엇인가? 다시 말해서 2007년에 개정된 전자정부법처럼 행정전자서명의 활용을 행정기관 이외의 이용자(민원인)에게까지 확대할 것인가가 문제된다.

3. 범정부차원의 보안대책 실효성 확보와 집행조직의 효율성에 관련하여

사이버공간에서 정보 등에 대한 보안문제는 오프라인과 달리 각각 해당기관의 고유한 문제로 한정되지 아니하고, 해당기관과 연계된 다른 행정기관은 물론 이용자 등에게도 직접적으로 영향을 미칠 수 있으며, 사안(예컨대, 바이러스의 유포 등)에 따라서는 전자정부 전영역(민간분야를 포함한 사이버공간)에 영향을 미칠 수도 있다. 따라서 해당기관만으로는 독자적으로 이와 같은 문제를 해결할 수 없는 경우도 발생한다. 또 사이버공간에서의 보안문제는 오프라인보다도 훨씬 급

2) 제22조의2 (공공기관등의 행정정보 공동이용) ①행정기관은 그 기관이 보유하고 있는 행정정보를 공공기관과 『은행법』 제8조제1항의 규정에 따라 인가를 받은 기관 등 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 또는 대통령령이 정하는 법인·기관 및 단체(이하 이 조에서 "공공기관등"이라 한다)로 하여금 제22조제4항의 규정에 따른 행정정보공동이용센터를 통하여 공동이용하게 할 수 있다.
②제1항의 규정에 따라 행정정보를 공동이용하는 경우에는 행정전자서명을 사용하여야 한다.
③제21조제1항 및 제2항의 규정은 제1항 및 제2항의 규정에 따른 행정정보의 공동이용에 관하여 이를 준용한다. 이 경우 "행정기관"은 "공공기관등"으로, "행정정보를 공동이용하여야 한다"를 "행정정보를 공동이용할 수 있다"로 본다.

격하고 신속하게 이용자 등에게 영향을 미칠 수 있다. 그러므로 국가안보에 직접적으로 관련성이 없다고 하여도 국가차원(범정부 차원)에서 신속하고 체계적이며 실효성 있는 보안대책의 수립과 집행을 위한 조직체계를 마련하여야 한다.

이와 관련해서 행정자치부는 현재의 보안관련 조직체계로 적절히 대처할 수 있는가? 다시 말해서 향후 보안관련 조직체계를 보다 효율적이고 실효성이 있는 조직을 강구하고 있는가? 그리고 범정부차원에서 바람직한 정보 등의 보안집행체계에 대한 정책이 어떠한 방향으로 나아가야 함이 적절한 것인가에 대한 검토가 있어야 한다.

3. 정보보안 관련업무와 입법형식에 관하여

아래의 도식화에서 알 수 있듯이 정보보안과 관련된 업무는 행정자치부, 국가정보원 및 정보통신부가 주축을 이루고 있으며 관련법규를 마련하고 있는데, 이들 법규 중에서 법률차원에서 규율함이 타당한 것도 발견된다(예컨대, 국가사이버안전관리규정 등). 또한 정보시스템과 관련하여 정보보안은 온라인을 통하여 상호 연계되어 있으며 공통된 사항도 발견되어 이를 체계화하는 독립입법도 고려할 수 있을 것으로 사료된다(예컨대, (가칭)정보보안관리법의 제정 등).

[참조 : 행정자치부·국가정보원·정보통신부의 역할과 업무관련 법령등 비교]

	행정자치부	국가정보원	정보통신부
정부조직법	제34조 (행정자치부) ① 행정자치부장관은 …… 전자정부 … 지방자치제도, 지방자치단체의 사무지원·재정·세제, 지방자치단체간 분쟁조정,	제16조 (국가정보원) ① 국가안전보장에 관련되는 정보·보안 및 범죄수사에 관한 사무를 담당하기 위하여 대통령소속하에 국가정보원을 둔다.	제38조 (정보통신부) 정보통신부장관은 정보통신·전파관리·우편·우편환 및 우편대체에 관한 사무를 관장한다.

	선거, 국민투표, 민방위·재난관리 제도에 관한 사무를 관장한다. ②국가의 행정사무로서 다른 중앙행정기관의 소관에 속하지 아니하는 사무는 행정자치부장관이 이를 처리한다. ③ -⑦ 생략	②국가정보원의 조직·직무범위 기타 필요한 사항은 따로 법률로 정한다. **[참조]** 국가정보원법 제 3 조 (직무) ①국정원은 다음 각호의 직무를 수행한다. 1. 국외정보 및 국내보안정보(대공·대정부전복·방첩·대테러 및 국제범죄조직)의 수집·작성 및 배포 2. 국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무. 다만, 각급기관에 대한 보안감사는 제외한다. 3. 형법중 내란의 죄, 외환의 죄, 군형법중 반란의 죄, 암호부정사용죄, 군사기밀보호법에 규정된 죄, 국가보안법에 규정된 죄에 대한 수사 4. 국정원직원의 직무와 관련된 범죄에 대한 수사 5. 정보 및 보안업	

		무의 기획·조정 ②제1항제1호 및 제2호의 직무수행을 위하여 필요한 사항과 제5호에 정하는 기획·조정의 범위와 대상기관 및 절차 등에 관한 사항은 대통령령으로 정한다.	
소관법령 등	○전자정부법 ○공공기관의개언정보보호에관한법률 등	○국가정보원법 ○국가사이버안전관리규정 ○정보 및 보안업무 기획조정규정 등	○정보통신기반보호법 ○정보통신망 이용촉진 및 정보보호 등에 관한 법률 ○전자서명법 ○전기통신사업법 ○정보화촉진기본법 ○전파법 등

제 2 주제

정보통신분야의 정보보안정책과 입법현황

발 표 : 오상균 (정보통신부 정보보호기획단
정보보호정책팀 서기관)

토 론 : 이화실 (국회 과학기술정보통신위원회 입법조사관)

이철원 (국가보안기술연구소 정책실장)

정보통신분야의 정보보호정책과 입법현황

오 상 균
(정보통신부 정보보호정책팀)

Ⅰ. '07년 정책방향

가. 개인정보 보호 강화

개인정보에 대한 이용자의 권익보호를 위해 개인정보영향평가제와 주민번호대체수단(i-PIN) 도입을 확대하고, CCTV · RFID 등 새로운 매체에서의 개인정보를 규율할 수 있는 법적 근거를 마련하고, 이용자 동의 획득방법, 개인정보취급방침 공개방법의 구체화 등 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 하위법령을 정비를 추진할 계획이다.

민간분야 서비스가입시 주민등록번호 기재를 생략하고 생년월일로 대체 하는 등 주민등록번호 수집 최소화를 제도화하고 사업자의 개인정보 취급절차변경, 신규 시스템 도입 등의 경우 개인정보 위험도를 사전에 평가하여 스스로 보완할 수 있는 개인정보 영향평가제 도입과 인터넷 이용시 ID, 패스워드 등 개인정보를 암호화하여 보안성을 강화하는 보안서버 보급을 확대해 나갈 것이다.

웹사이트의 개인정보취급방침을 쉽게 공개하고 평가하는 수단인 P3P S/W를 개발 · 보급하여 웹사이트 선택과 이용의 편의성을 제고하고, 사회 전반의 개인정보보호 실태, 수준 등을 측정할 수 있는 지수인 개인정보보호신뢰지수를 개발할 계획이다.

또한 인터넷이 노출된 주민번호 등 개인정보에 대한 삭제를 지속적으로 추진하고 관계부처와 협조하여 중국, 대만 등 국외 사이트에 노출된 개인정보를 정기 점검하여 국제공조를 통한 삭제 등 협조체계를 강화하고, 위치정보사업자의 위치정보 이용실태를 점검하여 위반행위가 있을 경우 행정조치를 해나갈 예정이다.

나. 건전한 인터넷 이용질서 정립

인터넷상 불법·유해정보에 대한 내용심의기능을 강화하기 위해 상임위원 확대, 심의위원회 상설화 등 정보통신윤리위원회 심의기능을 강화하고 심의단계 축소를 통한 신속한 심의체계 마련뿐만 아니라 사이버상 명예훼손의 피해자 구제를 확대하기 위한 대체적 분쟁해결수단(ADR)으로 명예훼손분쟁조정부 신설 등을 추진함으로써 불법·유해정보 유통방지 및 피해구제 기능을 강화해 나갈 예정이다.

특히, 공공기관 및 일정기준에 해당되는 정보통신서비스제공자(포털, 미디어, UCC사이트)가 게시판을 운영할 경우 본인확인의무를 부여함으로써 네티즌의 자기책임의식을 제고하고 일정부분 사업자에게 의무를 부과함으로써 자정활동을 강화하도록 하겠다.

불법스팸의 유통을 제한하기 위해서 스팸발송 IP와 전화번호를 24시간내 즉시 차단토록하고 스팸의 절대 수신량과 이용자가 느끼는 불편을 함께 반영하는 『스팸체감지수』를 개발하여 그 결과를 정책에 반영시켜 나가겠다.

또한 전국교육청으로부터 신청을 받아 실시하는 건전한 인터넷이용을 위한 윤리교육 지원을 확대하고 인터넷 과다사용자에 대한 상담과 전문기관과 연계한 치료기능을 강화하여 인터넷 역기능에 적극 대처할 계획이다.

다. 안전한 사이버환경 구축

’03년 1.25대란이후 인터넷 침해사고에 대한 사후적 모니터링 및 대처능력은 강화되었으나 첨단화, 복잡화되는 다양한 침해유형에 대해 적극적으로 대처하기 위해서는 사전적 대응체계 마련이 필요하다. 이를 위해 차세대 침해사고 예측 및 대응기술을 개발하고, 지능형 센서, 전문가시스템을 적용하여 침해사고 대응시간을 단축(30분→20분)할 계획이다. 또한 공격자 정보 역추적 기능을 포함한 가상기업환경을 구축하여 새로운 해킹 기법 유형을 수집·분석함으로써 관련 기업 및 기관에 실시간으로 정보를 제공할 것이다.

기업의 정보보호 대응능력 강화를 위해 2천개의 중소기업에 웹방화벽을 보급하고 악성코드자동탐지 프로그램을 활용하여 방문자가 많은 10만개 주요 홈페이지를 대상으로 악성코드 탐지여부 일일점검과 1천개의 기업 홈페이지의 취약점 점검을 실시 및 정보보호 수준 자가 측정서비스를 제공하고 서버관리자를 대상으로 정보보호교육을 강화해 나갈 계획이다.

교육, 금융, 전자거래 등 분야별 암호이용 가이드라인을 보급하고 안전진단인증대상을 확대하여 민간기업의 정보보호 투자 확대를 유도해 나갈 계획이다.

라. 디지털 기회 확대

’05, ’06년 연속으로 우리나라의 디지털 기회지수는 세계1위를 자치할 정도로 정보인프라의 확충과 활용은 세계최고수준이다. 이를 계속 유지하기 위해 전국 모든 농어촌 지역에 초고속인터넷망 구축을 완료할 계획이다. 또한 노인, 장애인 등 소외계층이 손쉽게 정보통신기기에

접근할 수 있도록 중고PC와 보조기기도 계속 보급해 나갈 예정이다.

소외계층의 정보통신 접근성과 활용능력을 제고하기 위해 공공기관의 웹 접근성 준수를 제도화하고 실태조사 대상을 확대하고, 청각이나 언어장애인을 위해 중개사를 통해 수화, 문자 등을 이용하여 전화통화를 할 수 있도록 지원해주는 통신중계서비스(TRS)의 제공근거 및 운영기준 등을 마련하여 제도화를 추진할 계획이다. 그리고 북한 이탈주민과 결혼이민자 정보화교육기관을 확대하여 자격증 및 취업관련 교육을 강화하여 자활기반마련을 확대할 것이다.

Ⅱ. 입법현황

1. 국내 정보보호 법·제도 발전 현황

가. 정보보호 법·제도 발전 연혁

우리나라의 정보보호 법률은 초기 「국가정보원법」, 「국가정보원법」 제3조제2항에 근거한 「보안업무규정」 및 「정보 및 보안업무 기획·조정규정」, 「국가보안법」, 「군사기밀보호법」 등 국가기밀에 대한 보안업무를 규정한데서 시작되었다고 할 수 있다. 이후 1980년대부터 추진되어 온 국가차원의 정보화 발전과 동시에 이에 따른 역기능이 부상하면서 정보보호 관련법령이 새로이 정비되기 시작하였다.

1986년에 제정된 「전산망 보급확장과 이용촉진에 관한 법률」은 우리나라 최초의 정보화에 관한 법률로 정보화에 국가적 시책과 제도를 규정하였다. 동 법은 전산망의 보호를 위한 일부규정을 포함하고 있으나 정보보호의 중요성을 인식하고 이에 초점을 맞춘 법률은 아니었다. 민간부문에서 정보보호에 대한 중요성이 부각되고 정보보호시책의 강구 및 정보보호시스템에 대한 기준고시 등 관련 제도가 마련되기 시작한 것은 「정보화 촉진 기본법」이라고 할 수 있다. 1995년에

제정된 「정보화 촉진 기본법」은 정보화 촉진에 관한 내용과 더불어 정보보호에 관한 기본적인 규정도 마련되었다. 또한 1995년에는 형법이 개정되어 전자기록 위작·변작죄 및 전자기록에 대한 비밀침해죄 등이 규정되었다.

1999년에는 개인 및 기업의 정보유통과 중요정보를 보호하기 위하여 「전자서명법」이 제정되었다. 이와 함께 「전산망 보급확장과 이용촉진에 관한 법률」도 전면 개정되어 「정보통신망 이용촉진 등에 관한 법률」로 명칭이 변경됨은 물론 정보화 역기능에 대한 규정을 보완하고 재정비하였다.

한편 2000년대에 들어서면서 사회의 안정과 번영을 위해서는 이들 정보통신인프라를 각종 위협으로부터 보호하는 것이 국가의 중대한 과제로 인식됨에 따라 이에 대한 대책을 수립하고 그 법률적 근거로서 2001년 「정보통신기반보호법」이 제정·공포되었으며, 컴퓨터 등 정보처리장치에 허위정보나 부정한 명령을 입력하여 타인의 재산을 빼앗는 온라인 사기행위를 벌하는 형법규정이 신설되었고, 「정보통신망 이용촉진 등에 관한 법률」도 명칭을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하면서 정보보호와 관련된 규정을 대폭 강화하였다. 동법은 2003년에 1·25인터넷 대란을 계기로 침해사고 대응 관련 규정을 보완하였으며, 2004년과 2005년에 개인정보 침해 및 광고성 정보전송으로 인한 이용자 피해를 해소하기 위해 처벌규정을 강화하는 등 관련규정을 정비하였다.

2005년에는 지식정보화사회로의 발전에 따라 다양한 정보시스템이 도입·운영되고 있으나 이를 체계적으로 관리할 수 있는 체제가 마련되지 못하여 발생하는 중복투자 및 시스템간 연계 미흡 등의 문제점을 해소하고 정보시스템을 효율적으로 구성하기 위하여 정보기술아키텍처의 활용을 촉진하고, 정보시스템 감리제도를 확립함으로써 공공기관 등에 정보시스템이 효율적으로 도입·운영될 수 있는 기반구축

을 목적으로 하는 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」을 제정하였다.

나. 정보보호 법·제도 현황

국내의 정보보호 법·제도는 각각 제정목적 및 기능별로 정보보호 추진체계 관련 법령, 국가기밀 보호 관련 법령, 중요정보의 국외유출 방지에 관한 법령, 전자서명 및 인증 관련 법령, 정보통신망과 정보시스템의 보호추진 관련 법령, 침해행위의 처벌에 관한 법령으로 분류할 수 있다.

① 정보보호추진체계 관련 법령

국내정보보호 추진체계는 국가사이버 안전체계, 전자정부보호체계, 정보통신기반 보호체계, 개인정보 보호체계로 나누어 볼 수 있다.

국가사이버 안전체계와 관련해서는 2005년 1월31일 대통령 훈령으로 발령된 「국가사이버 안전 관리규정」에서 국가사이버안전전략회의, 국가사이버 안전센터 등 사이버 안전 관련조직에 대한 법적 근거, 임무, 관련 기관간 협력사항 등에 관한 사항을 규정하고 있다. 한편, 전자정보 보호체계에서는 2001년 2월26일 제정된 「전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률」을 기준으로 전자정부 추진과 더불어 정보보호에 관한 사항도 규정하고 있다. 또한 정보통신기반보호체계는 2000년 12월에 제정된 「정보통신기반보호법」에서 정보통신기반보호위원회, 침해사고대책본부 및 각 중앙행정기관의 역할에 관한 사항을 규정하고 있다. 개인정보 보호체계와 관련된 법령으로는 공공부문에서 「공공기관의 개인정보보호에 관한 법률」, 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」 및 「주민등록법」등이 있으며, 민간부문에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」등 개별법

이 존재하고 있다.

② 국가기밀관련 법령

국가기밀보호 관련 법령에는 침해나 유출될 경우 국가의 존립·안전과 민주적 기본질서 유지를 위태롭게 할 정보 내지 국가 기밀에 대한 침해금지와 처벌, 비밀의 분류, 국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무 등에 관하여 규정하고 있는 법령들이 해당한다.

예를 들면, 「국가정보원법」제3조 중 국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무와 정보 및 보안업무의 기획조정 규정, 「국가보안법」제8조 회합·통신, 「보안업무규정」제3조 보안책임 및 제2장 비밀보호(제5조 내지 제30조), 「군사기밀보호법」제3조 군사기밀의 구분, 제5조 군사기밀의 보호조치, 제12조 내지 제15조 군사기밀 누설 관련 조항 등이 이에 해당하며, 형법에는 간첩죄, 일반이적죄, 외교상 비밀누설죄, 공무상 비밀누설죄 등 다양한 규정들이 존재한다.

한편 종래에 주로 국가의 비밀보호 수단으로 사용되어 온 암호는 정보통신망상의 통신수단 및 전자상거래 등의 발전으로 민간분야에서도 사용이 늘고 있으며, 이에 대한 법령정비가 이루어져 왔다. 암호의 사용과 관련된 법령으로는 「보안업무규정」, 「정보화촉진기본법」, 「전자거래기본법」 등이 있으며, 암호의 부정사용과 관련된 법령으로는 「국가정보원법」, 「군형법」 등이 있다.

③ 중요정보의 국외유출방지에 관한 법령

국가안전보장과 관련된 보안정보나 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보 등 국내의 산업·경제 및 과학기술 등에 관한 중요정보가 정보통신망을 통하여 국외로 유출되는 것을 방지

하기 법령으로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제51조가 있고, 2006년에 제정된 「산업기술의 유출방지 및 보호에 관한 법률」은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 국가핵심기술의 지정·변경(제9조)과 보호조치(제11조) 및 수출승인 등 국가핵심기술의 무단유출과 침해행위를 금지하고 있다(제14조).

④ 전자서명 및 인증 관련 법령

정보시스템과 정보통신망의 발전으로 인한 원격지간의 거래 및 업무가 활성화됨에 따라 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보인 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명 및 인증관련 법적 정비가 이루어졌다. 전자서명 및 인증과 관련된 법령에는 공인전자서명을 규정하고 있는 「전자정부법」(구 「전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률」)이 있다. 공인인증시장의 균형적 발전과 공정한 경쟁환경을 조성하기 위하여 비영리법인 등에 대한 공인인증 제공역무 영역을 설립목적에 맞게 구분하여 지정할 수 있도록 「전자서명법」이 2005년12월30일 개정되어 2006년 7월부터 시행돼 오고 있다.

⑤ 정보통신망과 정보시스템의 보호조치 관련 법령

해킹, 바이러스유포 등 사이버 침해행위로 인하여 국가 및 민간의 정보통신망과 정보시스템에 대한 위협이 증가함에 따라 국가차원의 체계적인 보호조치가 필요하게 되었다. 정보통신망과 정보시스템의 보호조치와 관련한 법령으로는 「정보화촉진기본법」, 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「전자

거래기본법』, 「전자무역 촉진에 관한 법률』, 「산업기반 조성에 관한 법률』 및 「화물유통촉진법』등이 있다.

⑥ 침해행위의 처벌에 관한 법령

해킹, 바이러스, 서비스 거부공격 등 정보시스템과 정보통신망에 대한 침해 등으로 피해를 야기하고 정보의 탈취, 위·변조 등으로 인한 국가·사회적 피해방지를 위하여 이들 행위에 대하여 벌칙규정을 두고 시행하고 있다.

「정보통신기반보호법』제28조의 주요 정보통신 기반시설 침해행위에 대한 벌칙, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률』제62조의 정보통신망 침해행위와 비밀 등의 보호의무 위반에 대한 벌칙규정이 대표적이다. 또한 「무역업무자동화촉진법』제25조, 「화물유통촉진법』제54조의2 내지 제54조의4 벌칙규정 등이 있다. 또한 형법은 컴퓨터 사기죄를 도입하여 이에 대한 처벌규정을 마련하였다.

⑦ 개인정보보호 관련 법령

보호되어야 할 정보 중에서 개인정보 또한 중요한 부분을 차지하고 있다. 최근 정보통신기술의 발달에 의하여 개인정보보호에 대한 침해가 증가하고 있어 이에 대한 관심이 증가하면서 관련법령의 정비가 이루어지고 있다.

개인정보보호와 관련된 법령으로는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률』, 「공공기관의 개인정보보호 등에 관한 법률』, 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률』, 「통신비밀보호법』, 「신용정보의 이용 및 보호에 관한 법률』, 「금융실명거래 및 비밀보장에 관한 법률』등이 있으며, 최근 대형의료기관들을 중심으로 IT기술과 인력을 의료영역에 접목하여 정보화를 추진하는 등 개인의 건강정보가 데이터베이스화되고 네트워크를 통한 정보의 교류 및 활

용도가 높아짐에 따라 개인의 건강정보를 체계적으로 보호하기 위한 대책마련의 시급성과 기존의 치료위주의 서비스에서 예방/건강증진 등 삶의 질에 중심을 둔 포괄적 보건의료서비스 제공에 대한 국민 욕구의 증대를 충족하기 위한 방안으로서 보건복지부에 의해 「건강정보보호 및 운영에 관한 법률(안)」이 입법 예고되어 국회의 의결을 기다리고 있다(2006. 10. 24. 보건복지부 공고 제2006 - 226호).

그밖에, 개인정보보호의 중요성이 갈수록 강조되면서 사회 각 분야를 포괄하는 개인정보보호 일반원칙과 기준으로서의 역할을 담당하게 될 「개인정보보호법」의 제정이 추진되고 있으며, 이와 병행하여 정보통신부는 개인정보가 대량으로 취급되는 정보통신분야의 특성을 반영하고 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 시행 과정에서 나타난 미비점을 개선하기 위해 지속적인 노력을 경주하고 있다.

2. 주요 제·개정 법령

가. 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」(법률 제7816호 2006. 7. 1. 시행) 및 동법 시행령(대통령령 제19598호 2006.6.30.)의 제정

지식정보화사회로의 발전에 따라 다양한 정보시스템이 도입·운영되고 있으나 이를 체계적으로 관리할 수 있는 체제가 마련되지 못하여 중복투자 및 시스템간 연계 미흡 등 일부 문제점이 나타나고 있어 정보시스템을 효율적으로 구성하기 위한 체제 및 방법인 정보기술아키텍처(Information Technology Architecture)의 활용을 촉진하고, 정보시스템 감리제도를 확립함으로써 공공기관 등에 정보시스템이 효율적으로 도입·운영될 수 있는 기반을 마련하였다.

① 정보기술아키텍처 도입·확산 기본계획의 수립 등(법률 제4조)

공공기관에 정보기술아키텍처를 체계적으로 도입·확산시키기 위하여 정보통신부장관 및 행정자치부장관은 관계기관의 장과 협의하여 정보기술아키텍처 도입·확산을 위한 기본방향, 도입·운영 현황 및 성과분석에 관한 사항을 포함한 기본계획을 수립하여 정보화추진위원회에 보고하도록 규정하고 있다.

② 공공기관에 정보기술아키텍처 도입 의무화 및 운영 촉진(법률 제5조, 제6조)

정보화투자의 효율성을 제고하고 전자정부서비스의 품질 향상을 도모하기 위하여 대통령령이 정하는 공공기관의 장은 정보기술아키텍처 도입계획을 수립하고, 그에 따른 정보기술아키텍처를 도입·운영하도록 하는 한편, 정부는 정보기술아키텍처의 도입·운영을 촉진하기 위하여 공공기관에서 활용할 수 있는 참조모형을 개발·보급할 수 있도록 하고, 정보기술아키텍처를 도입·운영하고자 하는 공공기관에 대하여 기술 제공, 교육·훈련 지원 등을 할 수 있도록 하며, 공공부문과 밀접한 관련이 있는 민간부문에 대하여 정보기술아키텍처의 도입·운영을 권고할 수 있도록 하였다.

나. 전자금융거래법의 제정(법률 제7929호 2006. 4. 28.)

인터넷뱅킹 등 전자금융거래가 확산되고 전자화폐 등 새로운 전자지급수단이 출현함에 따라 비대면성 등과 같은 전자금융거래의 특성을 반영하여 거래당사자의 권리·의무 등 법률관계를 명확히 하는 한편, 전자금융업무를 영위하는 자에 대한 허가·등록 및 감독에 관한 사항을 체계적으로 정비함으로써 전자금융거래의 안전성과 신뢰성을 확보하였다.

다.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」및 시행령의 개정

① 2006년 3월 24일 개정법률의 이유 및 주요내용

청소년 유해 매체물로부터 청소년을 보호하기 위하여 청소년 접근을 제한하는 조치 등이 없이 인터넷 홈페이지 게시판에 게재된 청소년 유해 매체물을 정보통신서비스제공자로 하여금 삭제하게 하고(제44조제3항), 안전진단 수행기관을 15인 이상의 정보보호 기술인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인으로 확대하여 정보통신서비스제공자 등 안전진단 수행기관의 선택권을 확대하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하였다(제46조의3 제1·2·4·5·7항).

② 2006년 10월 4일 개정법률의 이유 및 주요내용

종전의 법률은 사업자의 규모 및 제공하는 서비스의 특성 등을 고려하지 아니하고 모든 정보통신서비스제공자 등에게 개인정보관리책임자를 지정하도록 하고 있으나, 종업원이 없거나 서너 명에 불과한 소규모 사업자에게까지 개인정보관리책임자를 지정하도록 하는 것은 과도한 의무부과라 할 수 있으므로 종업원 수·정보통신서비스 이용자 수 등이 정보통신부령으로 정하는 기준 이하인 정보통신서비스제공자 등은 개인정보관리책임자를 지정하지 아니할 수 있도록 하고(제27조 제1항 내지 제3항), 정보통신서비스제공자 등이 해당 이용자로부터 개인정보에 대한 오류의 정정 요구를 받은 경우 그 오류를 정정할 때까지 해당 개인정보를 제공 또는 이용하여서는 아니 된다는 현행 규정은 수용하기 어려운 부당한 정정요구에도 요구받은 대로 정정하지 아니하면 해당 개인정보를 제공 또는 이용하지 못하게 되는 모순이 있으므로 오류를 정정하지 아니하더라도 정정하지 못하는 사유를

이용자에게 통지하는 등 필요한 조치를 취한 경우에는 해당 개인정보를 제공 또는 이용할 수 있도록 하였다(제30조제5항).

③「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」의 개정(대통령령 제19424호 2006. 3. 29.)

앞의 개정법률(법률 제7812호, 2005. 12. 30. 공포, 2006. 3. 31. 시행)에 의하여 정보통신서비스제공자에 대하여 불법 광고성정보 전송자의 신원정보를 요청할 수 있는 법적 근거가 신설됨에 따라 동법 시행령의 관련 조항을 정비하고, 영리목적의 광고성 전자우편의 수신을 동의한 경우 종전에는 동의를 얻은 시기 및 내용까지 명시하도록 하던 것을 앞으로는 발송일 현재 수신자의 동의가 있었는지 여부만 명시하면 되도록 규제를 완화하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선・보완하였다(제26조, 제27조).

라. 전자서명법 시행령・시행규칙의 개정 (2006. 6. 30. 공포 2006. 7. 1. 시행)

2005년 12월말 개정을 마친 전자서명법은 공인인증기관간 공정경쟁체제 확립을 저해하는 행위에 대해 규제할 수 있는 법적장치의 마련과 공인인증서 이용자보호 강화를 주요골자로 하고 있는데 2006년 중반 시행령・시행규칙의 개정으로 전자서명법의 실효성을 확보하였다. 개정된 전자서명법에 의하면 공인인증기관은 공인인증서와 관련한 사고가 발생한 경우에 대비하여 보험에 가입하여야 하고, 공인인증서를 발급받은 일반 이용자들도 공인인증서의 이용범위나 용도를 벗어나 부정사용하거나, 타인에게 함부로 양도・대여하지 못하도록 하는 의무규정이 신설되었다. 만일 이를 위반하는 경우 징역이나 벌금 등의 처벌을 받게 된다.

마.「위치정보의 보호 및 이용 등에 관한 법률」의 개정(법률 제8002호 2006. 9. 27.)

긴급구조를 위한 개인위치정보 이용을 요구할 수 있는 자는 개인위치정보주체, 개인위치정보주체의 배우자 또는 직계 존·비속으로만 규정되어 있어 형제·자매가 긴급구조를 위한 개인위치정보를 이용하지 못하게 되어 있고, 친권자가 없는 미성년자의 경우 자살기도 등의 긴박한 경우에 그 위치추적을 요구할 수 있는 자가 없게 되므로 앞으로는 형제·자매도 위치추적을 요구할 수 있도록 개선하고, 친권자가 없는 미성년자의 경우 「민법」 제928조에 따른 후견인이 위치추적을 요청할 수 있도록 하였다(제29조).

바.「인터넷 주소자원에 관한 법률」의 개정(법률 제8088호 2006. 12. 26.)

최근 온라인 경매업체의 인터넷 광고 내용이 청소년들에게 악영향을 미치고 있어 불법, 청소년유해정보에 대한 대책이 시급한 실정임. 한편 불법통신 및 청소년유해정보에 대한 심사와 시정요구업무를 담당하는 정보통신윤리위원회가 청소년유해정보를 게재한 인터넷 업체에게 도메인 사용에 대한 제재를 할 경우, 현행법상에는 인터넷주소관리준칙 조항에 인터넷주소의 사용폐지와 등록말소에 관한 사항만 있기 때문에 과도하게 규정하고 있는 실정을 감안하여 너무 과도한 집행이 되지 않는 중간단계 조치인 “사용정지”에 대한 현실적 필요성을 추가 보완하여 한국인터넷진흥원에 도메인 이름을 일정기간 ‘사용정지’ 조항도 두어 단계별 제재절차를 확보할 수 있도록 근거를 마련하였다(제13조제1항제4호).

사. 「신용정보의 이용 및 보호에 관한 법률」의 개정(법률 제7883호 2006. 3. 24.)

채무자의 권리보호 강화를 위하여 채권추심업체의 부당한 채권추심 행위에 대한 규제를 강화하고, 채권추심규제의 일관성을 확보하기 위하여 「신용정보의 이용 및 보호에 관한 법률」에 따른 채권추심 관련 규제를 「대부업의 등록 및 금융이용자 보호에 관한 법률」의 채권추심 관련 규제와 통일시키는 한편(제26조의2), 범죄 피해를 예방하기 위하여 긴급한 경우에는 영장의 발부 전에도 검사 또는 사법경찰관이 개인신용정보를 금융기관 등으로부터 제공받을 수 있도록 하는(제24조 제1항) 등 신용정보 관련제도를 개선하였다.

아. 「금융실명거래 및 비밀보장에 관한 법률」의 개정(법률 제7886호 2006. 3. 24.)

한국증권선물거래소가 이상거래의 심리 및 회원의 감리업무 수행과 그에 상당하는 업무를 수행하는 외국거래소와 정보 등의 교환 및 이상거래 심리 등의 업무협조를 위하여 필요한 경우에는 금융기관의 종사자에게 금융거래정보를 요구할 수 있도록 하고, 그 금융거래정보를 외국거래소에 제공할 수 있도록 하였다

3. 정책 방향

가. 정보보호 법제 관련 현황 및 문제점

정보화 진전과 인터넷 보급 확산에 따라 정보화 역기능 방지 및 정보보호 시책수립을 위한 관련 법률들이 계속적으로 등장하고 있다. 그러나 현 법체계에서 목적 및 이해주체가 다른 대상이 하나의 법에서 규율되고, 같은 목적의 규정이 여러 법률에 분산 또는 중복되는

현상이 발생되었다. 예를 들어 현행 「정보통신망 이용촉진 및 정보보호등에 관한 법률」은 '86년 제정되어 '99년 전문 개정 이래, 20여 차례 크고 작은 개정을 거치며 규율 영역이 크게 확대되었는데, 당초 전산망의 보급 및 이용 확대를 목적으로 제정되었으나 점차 정보통신망보호, 전자문서, 개인정보보호, 청소년보호, 사이버윤리, 스팸규제 등이 차례로 추가되었다.

그 결과로 법체계상의 일관성 상실, 타 법률과의 중복규율, 규제 영역 및 범위의 불명확성 등을 이유로 학계, 산업계 등에서 정보통신망법의 정체성에 대해 의문을 제기하기에 이르렀다.

정보화 촉진, 정보격차 해소, 인터넷품질 관리 등의 분야는 이미 별도의 법률로 확대·발전되었다. 따라서 급변하는 IT환경에서 법의 실효성을 강화하고 투명성과 명확성을 확보하기 위해 관련 법률간의 정리와 전문 개정이 필요할 수 있을 것이다

두 번째로, 전자감시로 인한 개인의 기본권 침해 방지를 위한 법제가 필요한 상황이라 하겠다. 유비쿼터스 환경 도래에 따라 RFID/USN 등의 이용이 증대될 것으로 예상되고 범죄예방을 목적으로 한 CCTV 설치가 늘어가면서 감시기술을 이용한 개인의 공적·사적인 삶에 대한 추적이 증가하면 개인 인격의 주체성 및 자유의 훼손 초래가 발생되고 있다.

세 번째 정책으로는 융합서비스 환경에 적합한 개인정보보호 법제의 정비라 하겠다. 광대역통합망 기반의 홈네트워킹 등 다양한 융합서비스 환경에서 예상되는 개인정보침해에 대비하기 위해서는 포괄적인 법제도가 마련되어야 할 것이다.

네 번째로는 신 미디어에서의 불건전 정보 유통 방지를 위한 법제 개선이 요구된다. Wibro, DMB, IPTV 등 신규 미디어에서 발생할 수 있는 명예훼손, 스팸메일 등의 역기능 예방을 위한 법제도가 그것이다.

나. 입법 정책방향

우선 u-사이버 위협에 대한 예방능력 및 대응능력 제고를 위해 분산된 정보보호 법제의 체계화가 필요하다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보화촉진기본법, 정보통신기반 보호법, 정보시스템도입·운영등에 관한 법률 등에 분산된 규정을 하나의 법체계 내에서 통합하고 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 비롯하여 정보화촉진법, 전자서명법, 전자거래기본법 등에서 중복해서 규정하고 있는 법제의 재정비가 진행되어야 할 것이다.

또한 BcN 등 차세대 인프라 환경에서의 침해사고 예방 및 대응을 위한 체계의 마련, RFID/USN, 홈네트워크 디바이스 및 서비스에 필요한 인증제도 및 생체인식 등 다양한 첨단 인증기술을 이용한 인증제도 마련 및 전자감시장비 설치와 이용에 관한 적절한 법적 규율 방안 마련을 위해 프라이버시 영향평가제도(PIA : Privacy Impact Assessment)를 통해 정보시스템 도입이나 변경시 개인의 프라이버시에 미칠 영향을 사전에 평가하여 개인정보침해를 사전에 방지할 수 있도록 하는 제도 도입도 고려된다.

참 고 자 료

o 국가정보원・정보통신부, 2006국가정보보호백서, 2006

o 위치정보 관련 법·제도 개선방안, 한국정보보호진흥원, 2006

o 김인식, 電子金融과 정보보호에 관한 연구, 정보통신정책연구원, 2006

토 론 문

이 화 실
(과학기술정보통신위원회 입법조사관)

Ⅰ. 총론적 검토

토론문은 우리나라 정보보호 법·제도의 연혁과 현황을 소개하면서 특히 정보통신분야의 정보보호정책과 관련된 2006년 주요 제·개정 법령을 소개하고 있음. 또한, 2007년 정부의 정책 방향을 개인정보 보호 강화, 건전한 인터넷 이용질서 정립, 안전한 사이버환경 구축, 디지털 기회의 확대 등으로 구분하여 소개하고 있음. 마지막으로 현재 정보보호 법체계가 타법률과의 중복규율, 규제 영역 및 범위의 불명확성 등의 한계가 있다는 문제를 지적하면서 RFID/USN, 광대역통합망 기반의 다양한 융합서비스, 신 미디어에서의 불건전 정보 유통방지 등을 위한 법제 정비 필요성을 제시하고 있음.

발표문의 기본 법제 정비 방향에 동의하면서 아래에서는 몇 가지 주제에 대하여 토론하고자 함.

Ⅱ. 쟁점별 토론

1. 개인정보보호 법체계에 대한 검토

개인정보보호와 관련된 법령으로는 공공부문에 「공공기관의 개인정보보호 등에 관한 법률」, 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」과 민간분야에 「정보통신망 이용촉진 및 정보보

호 등에 관한 법률(정보통신망법)』, 「신용정보의 이용 및 보호에 관한 법률(신용정보이용법)』, 「금융실명거래 및 비밀보장에 관한 법률』등이 있음.

각 법률마다 개인정보와 관련하여 보호하고 있는 수준에 차이가 있음. 이에 따라 규제의 형평성 문제 등이 발생하고 있고 규제의 적용을 받지 않는 제3의 영역도 존재하고 있음. 이에 개인정보보호에 관한 기본법인 개인정보보호법안의 제정 논의가 있으나 확실한 추진 주체가 없음.

또한, 기본법과 별개로 공공부문과 정보통신망 분야에 대한 개별법을 두는 방향으로 논의가 진행 중임. 공공부문과 정보통신망 분야의 개인정보가 유출될 경우의 위험 등이 더 높다는 점을 고려하여 개별법을 두는 방향으로 논의가 진행되는 것은 바람직하나 개인정보 유출시의 책임 문제(형사적, 민사적)에 있어 사업자와 공공부문이 부당하게 다른 취급을 받는 것은 바람직하지 않을 것임.

행정자치부나 정보통신부에서 각각 「공공기관의 개인정보보호 등에 관한 법률』이나 「정보통신망법』의 정비를 준비 중일 것 같은데 이 부분에 대하여는 어느 정도 논의가 진행 중인지 알고 싶음.

또한, 이와 별도로 정보의 활용을 높여서 국가 전체의 생산성을 높인다는 차원에서 행정정보 공동이용 법(안)의 제정논의가 진행중이고 「신용정보이용법』도 개인신용정보의 합법적 유통을 열어 놓았다는 점에서 개인정보의 활용과 보호를 어떻게 조화시킬 것인가에 대하여도 논의가 필요할 것임.

2. 사이버 안전 법체계에 대한 검토

국가사이버 안전체계와 관련해서는 「정보통신기반보호법」에서 관리기관이 수행하는 업무의 국가사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 다른 시설과의 상호연계성, 침해사고 발생시 국가안전보장과 경제사회에 미치는 피해규모 및 범위 등을 고려하여 각 중앙행정기관에서 주요정보통신기반시설을 지정하도록 하고 있고 여기서 지정된 주요정보통신기반시설에 대하여 각 중앙행정기관의 장은 시설 관리기관이 수립한 보호대책을 총괄하여 주요정보통신기반시설보호계획을 수립하도록 하고 있음. 다만, 보호체계의 총괄은 공공부문은 국가정보원이, 민간부문은 정보통신부장관이 각각 수행하도록 하고 있음.

민간 영역에 대하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 전국적으로 정보통신망접속서비스를 제공하는 자, 정보통신서비스부문 전년도 매출액이 100억원 이상인 자, 전년도말 기준 3월간의 일일평균이용자가 100만명 이상인 자는 매년 정보보호안전진단을 받도록 하고 도출된 안전진단결과에 대한 처리 내용을 정보통신부장관에게 통보하도록 하고 있음.

또한, 최근에 제정된 「전자금융거래법」에서는 금융기관들이 전자금융을 시행할 때 발생할 수 있는 위험을 최소화하기 위하여 인력부문(인력 및 조직관리, 외부주문 관리 등에 관한 기준), 시설부문(건물, 전원·공조 등 설비, 전산실 등에 관한 기준), 정보기술부문 내부통제(정보화계획 수립·운영, 정보시스템 구축, 정보시스템 감리, 비상대책 수립·운용, 정보시스템 성능관리, 직부의 분리, 프로그램 통제 등)에 대한 안전성 기준을 준수하도록 하고 있음.

공공영역에 대하여는 대통령 훈령인 「국가사이버 안전 관리규정」에서는 주요정보통신기반시설로 지정된 시설 외의 모든 공공부문의 정보

통신망에 대하여 사이버 안전대책의 수립·시행 등을 규정하고 있음.

「국가사이버 안전관리 규정」과 「정보통신기반보호법」의 관계 및 주요정보통신기반시설로 지정되었을 때와 지정되지 않았을 때 공공부문에서 정보통신시설과 관련된 안전대책을 수립하고 시행하는데 어떠한 차이가 있는지 등에 대하여 토론했으면 함.

또한, 주요 정보통신기반시설로 지정되지 않은 민간부문의 정보통신서비스제공자의 시설과 공공부문에서 운영하고 있는 시설의 보호대책 수립에 있어 어떤 차이가 있고 만약 차이가 있다면 그러한 차이는 타당한 것인지에 대하여 설명을 부탁함.

그리고 금융기관은 현재 주요정보통신기반시설로 지정되어 있는데 전자금융거래법에서 설정된 안전성 기준과 정보통신기반보호법에서 주요정보통신기반시설이 2년에 한번 수행하여야 하는 취약점 분석·평가가 전자금융시설 보호 정도에 있어 어느 정도 차이가 있는지 또 이러한 보호체계는 어떻게 연계되고 있는지 알고 싶음.

마지막으로 올 해 1월에 사이버위기예방법(안)이 국회에 제출되어 어떤 상임위원회로 회부되어야 하는지가 논란이 된 적이 있음. 국가정보원에서 이와 관련된 법안을 계속 준비 중이라고 들었는데 어느 정도 논의가 진행되고 있는지 알고 싶음. 또, 지난번에 제출된 법안은 국민의 통신비밀 자유권의 침해 위험성이 높아 보였는데 그러한 부분에 대한 보완은 어떻게 하실 생각인지 알고 싶음.

3. 정보보호 법체계의 범위

발표문에서는 정보보호 법체계의 범위에 대하여 정보화 관련 역기능에 관한 법률을 포괄하여 정의한 것으로 보임. 그런데 정보보호 법

체계를 그렇게 넓게 볼 필요가 있는지 의문임.

사이버 안전에 대한 위험이나 침해시 사회에 미치는 영향 등에 대하여 중점을 두고 볼 필요가 있다는 생각이 듦. 따라서 발표문에서 밝히고 있는 바와 같이 현재 너무 광범위한 분야를 규율하고 있는 「정보통신망법」의 개정이 필요하다는 데에 동의함.

토 론 문

이 철 원
(국가보안기술연구소 정책실장)

1. 개인정보보호 강화

o 주민등록번호 기재 생략 등 개인정보 수집 최소화를 위한 법제적 노력은 상당부분 진척이 되었다.

그러나, 이미 유포되어 있는 특히, 중국 등에서 악의적으로 사용 및 판매되고 있는 개인정보의 삭제 등에 대한 강력한 정책이 필요하다. 이미, '04년 중국발 해킹사고에서 경험한 바와 같이 중국당국의 협조를 얻는 것은 어려운 일이 될 것으로 예측된다. 따라서, 이 부분에 대한 정부의 협상력이 요구된다.

o 최근 개인정보를 보호하기 위한 하나의 방법으로 정보통신망을 이용한 정보의 송수신시 보안서버를 사용할 것을 권고하고 있다. 보안서버를 활용하면 정보통신망을 이용한 정보의 송수신되는 개인정보가 암호화되므로 개인정보보호에는 상당한 효과를 거둘 수 있으리라 판단된다.

그러나, 공공기관 등에서 보안서버 확충을 위한 예산 확보가 어려운 실정이므로 정보보호 예산 확보를 위한 정보보호 예산 제도화 추진 노력이 필요하다.

2. 안전한 사이버환경 구축

o 사이버 침해사고의 사전적 대응체계 구축의 핵심은 정보공유이다. 다양한 기관에서 침해관련 정보를 수집하고 있으나, 사고 징후를 탐지 및 대응할 수 있는 실질적 정보의 교환이 아닌, 가공된 정보의 사후 통보적 공유형태를 가지고 있다.

이와 같은 정보공유 형태로는 침해사고의 사전방지 및 피해확산 방지에 한계를 가질 수 있다. 따라서, 침해사고에 대한 효율적 사전·사후 대응을 위하여 현재 유관기관에서 수집·분석되는 정보의 공유를 강제할 수 있는 법적 근거 마련이 필요하다.

o 교육, 금융, 전자거래 등 민간부분의 암호이용 가이드라인을 작성하여 보급하는 것은 매우 시의 적절하다 할 수 있다. 그러나, 민간부분의 암호이용 정책은 국가차원의 암호이용정책과 일맥상통하여야 한다. 따라서, 민간분야 암호이용 가이드라인 작성시에는 국가정보원과 협의하여 국가 암호이용정책에 상치하지 않도록 하여야 한다.

3. 정책방향

o 전자정부법, 정보통신기반보호법, 정보통신망 이용 촉진 및 정보보호 등에 관한 법률, 사이버안전관리규정 등 동일 목적에 대하여 다양한 법률로 규율하고 있다. 이 경우, 정보보호업무의 총괄기관 부재, 침해사고 발생시 책임소재 불명확 등 여러 가지 부작용을 초래할 수 있다.

따라서, 모든 영역을 아우를 수 있는 「정보보안기본법(가칭)」 제정이 필요하다고 판단된다.

「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」, 「국가사이버안전관리규정」 등에 명시된 중복 규정을 단일화할 필요가 있다. “취약점 분석·평가”, “정보보호관리체계 인증”, “정보보호안전진단”, “정보보안수준평가” 등이 유사 내용이므로 이러한 규정을 단일화하기 위해서도 가칭 「정보보안기본법」의 제정은 필요하다고 판단된다.

- o 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」은 초기 동법의 제정목적에 맞도록 범위를 축소하고 정보보호로 분류하기에는 애매한 사이버 윤리, 유해정보 차단 등 인터넷 역기능 방지에 중점을 둔 법률로 정체성을 갖도록 개정을 추진하는 것이 바람직하다고 판단된다.

- o 「정보통신기반보호법」중 주요정보통신기반시설 지정에 대한 고민이 필요하다고 판단된다. 정보통신기반시설은 국가사회를 운영·유지를 위한 필수시설로 정보통신기반시설 자체가 중요한 것이지 정보통신기반시설내의 일부가 중요한 것(주요정보통신기반시설)은 아니며, 정보통신기반시설의 구성요소가 이미 상호연동되므로 정보통신기반시설내 일부 구성요소를 주요정보통신기반시설로 지정하는 것은 무리가 따른다고 판단된다.

- o 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」에 따른 보안 아키텍처 관리는 국가정보원의 업무영역으로 판단된다. 그러나 동법에는 보안 관련 영역의 책임과 역할이 명시되어 있지 않으므로 차후 법 개정시 이를 반영하는 것이 필요하다.

또한 정보보호 촉진 측면에서 보안 아키텍처를 정보보호 성과분석에 활용할 필요가 있으며 동 성과분석 결과를 차후 공공기관의 예산

책정에 반영하는 등 정보보호 수준 강화를 위한 방안 마련도 필요할 것으로 판단된다.

- o 전자감시로 인한 개인의 기본권 침해 방지라는 명제는 헌법에서도 보장하는 바이므로 이를 추구하는 것에는 매우 적절하다 할 수 있다.

그러나, 신기술 출현시마다 이를 규제하는 법이 제정될 때까지 신기술을 이용한 정보의 악용 및 오용 가능성은 언제나 존재하므로, 이를 방지하기 위한 근본적인 대책 마련을 고심해야 할 때라고 판단된다.

제 3 주제

국가의 정보보안정책과 입법현황

발 표 : 국가사이버안전센터

토 론 : 고낙훈 (법제처 법제관)

김충섭 (국회 정보위원회 입법조사관)

국가사이버안전 정책과 입법현황

국가사이버안전센터

Ⅰ. 서 론

2003년 1.25 인터넷 대란, 2004년 국가 주요기관 중국發 해킹사고 등과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터의 조직적인 사이버공격으로 인한 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대되고 있다.

[표1] 연도별 사이버 침해사고 발생 건수

분 야	2003년	2004년	2005년	2006년
공 공	1,323	3,970	4,492	4,286
민 간	26,179	24,297	49,726	34,597
합 계	27,502	28,267	54,218	38,883

이처럼 정보통신 인프라를 이용한 해킹·사이버테러 등의 사이버위협에 대비하기 위해 정부는 2004년 '국가사이버안전센터' 설립과 함께 「국가사이버안전 관리규정(대통령 훈령 제141호, '05.1.31)」을 제정 시행해 오고 있다. 그러나 각급기관 및 民·軍 분야의 위협정보 공유는 물론, 국가 공공기관간의 협력 부족 및 他법률과의 상충시 효력이 제한되는 등 사이버안전업무 수행에 한계를 드러내고 있다. 따라서 국가안보

를 위협하는 외부로부터의 사이버위협에 효율적으로 대처하기 위해서는 民·官·軍 사이버안전 정책을 종합 기획·조정하고 지휘 체계를 일원화하는 등 국가사이버안전업무 추진체계를 보강할 필요가 있다.

Ⅱ. 국내·외 사이버안전관리체계

1. 주요국가 동향

미국은 9.11테러 발생이후 테러대응 대책을 강화하기 위하여 연방차원의 중심기관 설치 필요성을 인식하고, 조직정비를 단행하여 국토안보국, 사이버안보담당 대통령특별보좌관, 국토안보회의, 대통령주요기반보호위원회 등이 신설되었으며 2002년 11월 국토안보법(Homeland Security Act of 2002) 제정을 계기로 국토안보부(DHS: Departmentof Homeland Security)를 창설하였다. 사이버안전업무는 국토안보부내 국가 사이버보안국(NCSD)산하 US-CERT(Computer Emergency Readiness Team)가 담당하며, US- CERT는 美 전역에서 발생하는 사이버공격 방어를 기본 임무로 하면서 사이버위협 분석 및 취약점 보강, 사이버위협 경고 전파, 사이버공격 대응활동 조정 등의 임무를 수행한다. 또한, US-CERT는 연방정부, 산업계, 주/지방 정부 및 일반대중들을 대상으로 한 “국토안보부(DHS)-민관합동(Public-Private Sectors Partnership)” 체제를 구축, 사이버위협에 대응하고 있다.

영국은 1999년 전자공격으로부터 국가주요기반시설을 안전하게 보호하고자 정부부처와 민간부문에서 시행하고 있는 각종 활동들을 조정·발전시키기 위한 부처간 협력조직으로 국가기반보안조정센터(NISCC : National Infras-tructure Security Coordination Center)를 설립 운영하고 있다. NISCC는 내각장관을 의장으로 7개 유관부처 대표로 구성된 운영위원회에 의해 운영되는데 운영위원회는 내각사무처, 통신정보부(GCHQ)

의 전자통신보안국(CESG:Communication Electronics Security Group), 보안정보국(SS:Security Service), 내무부, 국방부, 경찰 등 관련부처로 구성되어 있으며, 실무부서는 사이버 위협정보 분석 및 평가, 침해사고 발생시 위기대응, 민간을 포함한 국가기관 대상 보안 및 정책자문과 정보보안 기술개발 등의 업무를 담당하고 있다. NISCC 주요업무는 전자적 침해사고로부터 국가 주요기반시설의 방어를 위한 보안조정 센터의 역할과 사이버위협 관련 기술연구, 전문가 보안권고 및 전문기술 제공하고 있으며 패치관리, 보안훈련 등의 민간분야 정보보호 서비스를 제공하고 있다.

일본의 사이버위협 대응조직은 내각관방 정보시큐리티대책추진실, 내각 고도정보통신네트워크사회추진 전략본부, 경찰청, 총무성, 경제산업성 및 일본컴퓨터긴급대응센터 등 민간기관으로 구성되어 있으며, 2000년 2월 내각관방청 산하에 내각관방 정보시큐리티대책추진실을 설치 인터넷의 급속한 이용확대 등 국민생활의 IT발전에 따른 부정엑세스(해킹), 컴퓨터 웜바이러스 확산 등에 대처하고 있다. 내각관방 정보시큐리티대책추진실은 각 정부부처와의 협력을 도모하고 민관 전문가로 구성된 비상근팀의 조언을 받아 전자정부의 정보보호 확보 및 중요 인프라 사이버테러 대책 등 민・관의 정보보호 확보를 위한 정책추진을 총괄・전담하고 있다.

또한, 내각총리대신 산하 내각 '고도정보통신네트워크사회추진 전략본부(IT전략본부)'에 설치된 정보시큐리티대책추진회의와 민간전문가로 구성된 정보시큐리티전문조사회의 사무국을 담당하면서 각 부처 업무조정을 하고 있다.

사이버공격 등으로 전자정부・중요인프라사업자 등의 정보시스템에 관한 장애가 발생하거나 장애 발생이 예상되어 정부차원의 위기관리

대응이 필요한 정보시큐리티 관련 사안에 대한 대응활동은 긴급대응지원팀(NIRT)에서 수행하며, 정보보호시책의 시행에 대하여 중장기적 관점에서 조언을 하고 중요 인프라 방호를 위한 사이버테러 대책 강구는 전문조사팀에서 수행한다.

2. 국내 사이버안전관리체계의 발전

우리나라의 사이버안전관리체계는 정보보호에서 시작되었다. 처음에는 주로 기밀보호를 위한 국가·공공기관 위주의 통신보안체계로 유지되어 오다가 1995년 정부가 정보화를 본격적으로 추진하면서 「전산망보급확장과이용촉진에관한법률」과 민간분야의 정보보호 수요증가에 따른 「정보화촉진기본법」을 제정, 이를 근거로 한국정보보호진흥원 신설 등 정보보호체계로 운영되어 오던 중 사이버 침해행위로부터 국가와 국민생활의 안전을 보장하기 위해 지난 2001년 「정보통신기반보호법」을 제정, 시행하여 왔지만 2003년 1.25 인터넷 대란이 발생, 전국적으로 8시간 인터넷이 중단되어 은행거래는 물론, 대부분의 전산망이 마비되는 대 혼란을 야기하는 등 국가적 차원의 신속한 대응에 한계를 보였다.

1.25 인터넷 대란을 계기로 정부에서는 국가 인터넷망의 전자적 침해사고 조기탐지 및 피해확산 방지와 관련기관 정보공유를 통한 신속한 공동대응체제 구축을 위해 2003년 12월 정통부산하 한국정보보호진흥원에 인터넷침해사고대응지원센터를 설치, 민간분야 정보보호를 담당토록 한데 이어 2004년 2월 국가 안보차원에서 대응이 필요하다고 판단, 국가안전보장회의(NSC)사무처 주관하에 국방부·정보통신부·국가정보원이 합동으로 국가정보원 산하에 사이버안전센터(NCSC, National Cyber Security Center)를 신설하는 등 범정부적인 사이버안전관리체계를 구축하였다.

또한 사이버공간의 위기를 전쟁, 재해·재난 등과 함께 국가위기관리차원에서 다루어야 한다는데 공감하고, '핵심기반분야'에 사이버안전을 포함하여 「국가위기관리기본지침(대통령훈령 제124호, 2004.7월)」을 제정하였으며 이를 근거로 「사이버안전분야 위기관리표준매뉴얼(2004.9월)」도 마련하였다.

그럼에도 불구하고 2004년도 상반기 주요 국가기관 해킹사고가 발생함에 따라 NSC 중심의 비상시 사이버위기관리업무와 보안기관으로서 국가정보원이 평상시 수행하는 사이버안전업무를 일원화할 필요성이 대두되었으며, 특히 이와 같은 해킹사고의 공간인 인터넷이 민·관·군 영역을 구분할 수 없을 뿐만 아니라 사전 예방활동을 강화하여 피해를 미연에 방지하는 것이 중요한 문제로 제기되면서 각각의 분야와 기관을 막론하고 정보공유 등 업무협조 강화가 절실히 요구되었다.

이러한 배경에서 대통령은 '국가차원에서 사이버안전업무를 총괄하는 기관을 정하고 이를 규범화 할 것'을 지시하였으며, 이에 국가정보원장을 의장으로 외교통상부, 법무부, 국방부, 행정자치부, 정보통신부, 국가안전보장회의 사무처 등의 차관급을 위원으로 하는 '국가사이버안전전략회의'의 설치, 유관기관간 정보공유 및 업무협조 강화 등을 명시한 「국가사이버안전관리규정(대통령훈련 제141호, 2005.1.31)」을 제정 시행하였다.

3. 국가사이버안전 관리체계

우리의 국가사이버안전 체계는 국가사이버안전관리규정(대통령훈령 제141호)을 기반으로 범국가 사이버안전체계의 수립 및 개선, 기관간 역할 조정 등 국가사이버안전에 관한 중요 사항을 심의하기 위한 '국

가사이버안전전략회의'와 전략회의의 효율적 운영을 위한 '국가사이버안전대책회의'를 설치하여, 사이버안전업무를 수행하고 있다.

[그림1] 국가사이버안전 관리체계

국가사이버안전전략회의는 국가사이버안전에 관한 중요사항을 심의하며, 전략회의의 의장은 국가정보원장으로 하고 위원은 외교통상부차관·법무부차관·국방부차관·행정자치부차관·정보통신부차관·국가안전보장회의 사무처의 사무차장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 구성되어 있다.

전략회의는 첫째 국가사이버안전체계의 수립 및 개선에 관한사항, 둘째 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, 셋째, 국가사이버안전관련 대통령 지시사항에 대한 조치방안, 넷째 그 밖에 전략회의 의장이 부의하는 사항 등에 대해 심의한다. 이는 우리나라 최고의 사이버안전 기구이며 이를 보좌하기 위하여 국가정보원 차장을 위원장으로 하고 관련부처의 실·국장을 위원으로 하는 국가사이버안전대책회의를 구성하였다.

4. 국가사이버안전 전담기구

국가사이버안전을 담당하는 기구로 국가정보원 국가사이버안전센터, 정보통신부 인터넷침해사고대응지원센터, 국방부 국방정보전대응센터를 설립하여 각각 국가공공・민간・국방분야를 담당케 하고 있다.

국가사이버안전센터(National Cyber Security Center:NCSC)는 사이버공격에 대한 국가차원의 종합적이고 체계적 대응을 위해 2004년 2월 국가정보원 산하에 설치되었으며 이 기관에서는 정보통신망에 대한 24시간 사이버위협정보를 수집・분석・전파하는 국가 종합상황실 운영과 각종 사이버공격에 대한 예방・대응활동과 피해확산을 방지함으로써 국가 주요 전산망에 대한 안전성 확보를 목표로 하고 있다.

국가사이버안전센터는 공공분야(국가・공공기관) 전산망 사이버위협에 대한 수준별 경보 발령 등 사이버공격에 대하여 체계적으로 대응하고 24시간 보안관제를 통해 사이버위협 정보를 수집・분석, 대책을 전파하는 한편 심각수준에 따라 경보를 발령하며, 또한 침해사고 발생시 긴급대응・조사 및 복구를 지원하고 국방부, 정보통신부 등 관계기관은 물론 해외 유관기관과의 협력을 강화하는 등 범국가적 차원에서 업무를 수행하고 있다.

정보통신부 한국정보보호진흥원 인터넷침해사고대응지원센터(Korea Emergency Response Team Coordination Center:KrCERT)는 2003년 1.25 인터넷 대란 이후 인터넷망의 전자적 침해사고 조기탐지, 분석, 예・경보를 통한 피해확산 방지와 관련 기관과의 상시적인 정보공유, 신속한 공동대응체제 구축을 통하여 인터넷망의 안전성・신뢰성 확보를 목적으로 2003년 12월에 설치되었다.

인터넷침해사고대응지원센터는 민간분야에서의 해킹, 웜·바이러스 등 인터넷 이상징후 수집·분석·평가와 해킹·바이러스의 위협경보를 ISP, IDC 사용자들에게 전파·발령하고 각 기관·사용자들의 피해복구지원 및 침해사고 상담 접수·처리, 홈페이지 은닉 악성코드 자동탐지 및 제거, 분기별 침해사고 모의훈련 등을 실시하고 있다.

국군기무사령부 국방정보전대응센터는 국방 주요 정보체계에 대한 보호지원을 목적으로 2003년 11월 설치되었다. 군사기밀에 대한 보안업무와, 보안사고를 예방하여 최상의 전투력 유지, 국방정보통신시설에 대한 보호대책, 국방 사이버침해사고 예방 및 복구 등의 기술지원 업무를 수행한다.

국방정보전대응센터는 국방전산망 24시간 침해정보 탐지·분석, 국방 주요 정보체계 취약성 진단·탐지·분석, 사고예방 및 사고조사·수사와 각급부대 CERT 조정통제, 원격·현장 피해복구 지원과 각 부대 정보보호 신기술·동향 전파 및 정보보호 관련 정보 제공 등을 수행하고 있다.

5. 사이버안전 예방활동

사이버위협으로 부터 사이버공간의 안전을 확보하기 위해서는 사전예방활동이 우선되어야 한다. 먼저 국정원은 중앙행정기관과 소속 및 산하기관에서 활용가능하도록 보안관리 기준을 포함한 '국가사이버안전매뉴얼'을 작성하여 배포하고 중앙행정기관은 국가사이버안전 매뉴얼을 바탕으로 해 기관의 실정에 맞게 정보보안 관련내규 또는 지침에 반영하거나 소관분야 안전대책을 수립하고 이를 소속 및 산하기관에 배포하여 사용토록 한다. 중앙행정기관은 국가사이버안전매뉴얼상의 보안관리 기준과 자체 수립한 안전대책에 따라 소관분야 정보통신

망에 대한 안전성과 안전대책 이행여부에 대해 정기점검을 실시하고 국정원은 관계 중앙행정기관과 협의하여 현장방문 또는 원격측정을 통하여 사이버안전대책 이행여부와 정보통신망의 안전성을 확인한다. 또한, 각급기관은 정보통신망 신·증설 등 정보화사업을 추진하는 경우 자체적으로 보안대책을 수립하고 그 적절성 여부에 대해 국정원에 보안성 검토를 요청하며 국정원은 적합한 보안대책을 제시한다.

둘째, 국정원은 국가차원의 사이버위협을 총괄 수집·분석·전파하는 체계를 구축 운영하며 각급기관은 국가차원의 사이버위협 정보가 종합 수집·분석될 수 있도록 사이버위협 정보수집의 보안관제망 연동을 지원한다. 국가사이버안전센터는 사이버위협 정보 또는 이상징후 정보 등과 같은 다양한 위협정보를 수집하기 위해 국가 주요전산망을 대상으로 24시간 사이버공격 및 위협징후를 모니터링 한다. 보안관제를 통한 위협감시와 함께 국내외 다양한 경로를 통해 오프라인상의 사이버위협에 대한 정보를 파악한다. 이와 함께 각급기관은 보안관제시스템 또는 오프라인 등을 통해 사이버위협 정보를 인지한 경우에는 초동조치 후 국가사이버안전센터에 신속히 통보하고 국가사이버안전센터와 위협정보 전파 및 사고신고 연락체계를 구성 유지해야 하며 사고 발생시에는 즉시 통보한다. 국가 기밀문서가 저정된 정보시스템에 해킹사고가 발생했을 경우에는 의무적으로 신고를 하여야 한다.

셋째, 각급기관은 사이버위협에 대비하여 정기적인 교육 및 훈련을 통해 소속 직원의 보안의식 제고와 보안관리 요령을 전파하고 국정원은 각급기관 정보보안담당자를 대상으로 국가 정보보안 설명회를 실시하며 사이버안전관련 전문기술 전수를 위해 국가정보대학원에 사이버테러 대응 관련 교육과정을 개설·운영한다

넷째, 각급기관은 소관분야 정보통신망을 보호하기 위해 사이버안전 기술 연구 개발의 소요를 국정원에 제기할 수 있고 국정원은 이를 바탕으로 연간 또는 중장기 연구개발 계획을 수립 시행할 수 있다

마지막으로 사이버위협으로 인해 사고가 발생하거나 피해발생 가능성이 있을 경우에는 사이버위협 수준에 따라 관심・주의・경계・심각의 4단계 경보를 발령하여 사이버안전을 확보하기 위한 대응체제를 갖추고 있다. 그리고 국정원은 사이버공격 발생시 효율적으로 대응하기 위해 사이버안전업무 전반을 대상으로 비상기획위원회, 국가안전보장회사무처, 국방・정통부 등과 협의하여 범국가차원의 사이버전 모의훈련을 실시하고 각급기관은 이 훈련을 통해 발견되지 않았던 새로운 취약점이나 관리가 허술했던 부분을 찾아내고 이를 보완하기 위하여 적극 협조한다

6. 사고조사 및 피해복구

사고조사라 함은 사이버공격으로 인해 발생한 정보통신망 보안사고 또는 침해사고에 대해 공격기법과 사고원인을 분석하는 일체의 행위라 하겠으며 피해확산 차단 및 유사사고 재발방지를 위한 보안대책을 수립하는데 그 목적이 있다.

중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국정원장에게 통보하여야 한다.

국정원장은 국가・공공기관에 대한 사이버공격으로 인하여 발생한 사고에 대해 그 원인분석을 위한 조사를 실시할 수 있고 관계 중앙행

정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있다. 경미한 사고의 경우에는 해당기관의 장이 자체적으로 조사하게 할 수 있다.

심각수준의 사이버위협 경보가 발령된 경우와 경보가 발령되지 않더라도 침해사고가 광범위하게 발생했거나 피해확산으로 범국가차원의 대응이 필요한 경우 또는 대규모 피해가 발생한 기관이 국정원에 피해확산방지 등의 대처를 위하여 정부차원의 조사 및 복구지원을 요청한 경우에는 국정원장이 관계 중앙행정기관의 장과 협의하여 범정부적 합동조사 및 복구지원팀을 구성·운영한다.

Ⅲ. 사이버안전 관련 법·제도 현황

국내 사이버안전 관련 법·제도는 각각 제정 목적 및 기능별로 정보보호 추진체계 관련법규, 정보통신망과 정보시스템의 보호조치 관련법규, 침해행위의 처벌에 관한 법규, 개인정보보호 관련 법규가 있다.

[표2] 사이버안전 관련 법·제도 현황

구 분	주요 내용 및 관련 법
정보보호 추진체계 관련 법규	o 국가사이버안전 체계 관련 법 :『국가사이버안전관리규정』 o 전자정부보호 체계 관련 법 :『전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률』 o 정보통신기반보호 체계 관련 법 :『정보통신기반보호법』 o 개인정보보호 체계 관련 법 :『공공기관의 개인정보보호에 관한법률』,『전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한법률』,『정보통신망 이용촉진 및 정보보호등에 관한 법률』 등

정보통신망과 정보시스템의 보호조치관련 법규	정보통신망과 정보시스템의 보호조치와 관련된 법규 o『정보화촉진 기본법』,『정보통신기반보호법』,『정보통신망 이용촉진 및 정보보호 등에 관한법률』,『전자거래기본법』,『전자정부법』,『무역업무 자동화 촉진에 관한 법률』,『산업기반조성에 관한법률』,『화물유통 촉진법』
침해행위의 처벌에 관한 법규	해킹, 바이러스, 서비스 거부 공격 등 정보시스템과 정보통신망에 대한 침해 등으로 피해를 야기하고 정보의 탈취, 위·변조 등으로 인한 국가·사회적 피해 방지를 위한 벌칙 규정 o『정보통신기반보호법』제28조의 주요정보통신기반시설 침해행위에 대한 벌칙,『정보통신망 이용촉진 및 정보보호 등에 관한법률』 제62조의 정보통신망 침해행위와 비밀 등의 보호 의무 위반에 대한 벌칙 규정
개인정보보호 관련 법규	『정보통신망 이용촉진 및 정보보호등에 관한법률』,『공공기관의 개인정보보호 등에 관한 법률』,『전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률』,『통신비밀보호법』,『신용정보의 이용 및 보호에 관한 법률』,『금융 실명거래 및 비밀보장에 관한 법률』

Ⅳ. 국가사이버안전 법체계 미비점 및 보강 방안

1. 사이버공격 정보의 탐지 및 분석·전파활동 보장

외국은 물론, 국내의 사이버위협이 날이 갈수록 급격히 증가하고 있는 실정이어서 사이버 위협 정보를 신속히 탐지하고 분석하여 정보를 공유하고 미리 대처함으로써 사고를 미연에 방지하는 것이 중요하다.

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 유용한 것이다.

그러나 이러한 보안관제활동은 국내 인터넷 네트워크에 대한 모니터링에서 비롯되고 있는데 이러한 모니터링 자체가 현행 '통신비밀보호법' 제3조에 위배될 소지가 있어 법리적 시비의 요소가 있는 것이 현실이다.[1)]

현재 정보통신부의 정부통합전산센터나 국가기간통신사업자가 운영하는 통신정보공유분석센터(일명 통신 ISAC), 금융기관에서 운영하는 금융정보공유분석센터(일명 금융 ISAC) 등에서 수행하고 있는 보안관제 활동의 중요성에 비추어 이러한 업무를 보장해 주는 법적 장치는 없다.

따라서 통신비밀보호법 제3조에서 혼신제거를 위한 전파감시를 허용하듯이 인터넷의 안전한 유통을 보장하고 역기능제거를 위한 모니터링을 할 수 있는 규정을 마련하고 유관기관간 사이버위협을 탐지하고 그 정보를 공유함으로써 신속히 대응할 수 있도록 통신비밀보호법을 개정하거나 타법률로 이를 뒷받침하는 것이 필요하다.

2. 국가사이버위기 대응체계 보강

국가적으로 사이버안전에 중대한 위기가 발생할 경우에 대비하여 국가 주요정보통신기반시설 보호 및 적극적 대응을 위해 「정보통신기

1) 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.

반보호법』및 「국가사이버안전관리규정』등이 마련되었다고 하나 업무 영역이 민간, 국가・공공영역으로 구분되어 있어 기관간 상호협력은 물론 사고 초기 신속한 대응이 곤란할 뿐만 아니라 사고가 발생할 경우, 책임 소재 또한 불분명하다.

국가적 비상시에는 책임지고 국가사이버안전을 컨트롤할 수 있는 총괄 책임기관을 지정하고 국가사이버안전업무의 역할과 책임을 부여하며 전체적인 사이버안전 정책을 수립 및 추진할 수 있도록 해야 한다. 아울러 사이버안전 담당 전문기관 간 각종 사이버위협 정보의 공유・협력을 의무화하고 국가기관・지자체・공공기관이 기관별 사이버안전대책을 수립함은 물론, 총괄 책임기관이 각급 기관들에서의 이행여부 및 안정성을 확인하여 시정조치를 권고할 수 있도록 해야 한다.

또한, 사이버공격 발생시 피해기관은 관련 책임기관에 신고를 의무화하고 책임기관은 피해확산 방지를 위한 조치를 병행 피해에 따른 사고 복구는 물론, 사고조사와 동시에 사이버안전업무 전반에 대한 책임감을 갖게 해야한다. 특히 보안대책이 부실하여 피해가 발생한 기관에 대해서는 징벌적 처벌이 수반되게 하는 등 각급기관이 상호 연계성을 갖고 사이버안전업무를 수행할 수 있도록 기관별 역할을 명확히 재정립해야 한다.

3. 입법 동향

사이버위기에 대해 국가차원의 일원화되고 체계적인 대응을 위해 06.12.28 한나라당 공성진 의원이 ‘사이버위기 예방 및 대응에 관한 법률안’ 을 국회에 발의하여 현재 계류중이고 국정원도 정부입법으로 ‘사이버위기 대응에 관한 법률안’ 을 마련하여 관계기관과 협의를 진행중에 있다.

공성진 의원이 발의한 법률안의 주요 내용을 살펴보면 다음과 같다.

첫째, 정부는 사이버위기에 관한 국가차원의 대책 등을 심의·조정하기 위하여 대통령 소속하에 국가사이버안전위원회를 두고 위원회는 위원장 1인과 부위원장 1인을 포함한 15인 이내의 위원으로 구성하며 위원장은 국무총리가 되고 부위원장은 위원중 국무총리가 지명한 자로 한다.

둘째, 국가사이버안전위원회는 사이버위기사태 선포 및 해제, 긴급안전조치 등 대책 수립, 기관간의 역할 조정, 사이버위기사태대책본부 구성·운영 등에 관한 사항을 심의한다.

셋째, 헌법, 정부조직법, 기타 법령에 의하여 설치된 국가기관과 지방자치단체 및 공공기관, 주요정보통신기반시설 관리기관, 주요정보통신서비스제공자 등은 소관 정보통신망에 대하여 사이버위기를 예방하고 사이버위기가 발생하였을 경우에 피해를 최소화하기 위한 제반 안전활동을 수행하여야 한다.

넷째, 국가사이버안전위원회의 위원장은 국가차원에서 사이버공격정보를 탐지·분석·전파할 수 있는 체계를 구축하고 이를 위하여 국가정보원장은 책임기관의 장으로부터 소관 정보통신망에 대한 사이버공격 정보를 수집·분석하여 대책을 강구·지원하여야 하며 그 활동결과를 보고서로 작성하여 국회에 제출하여야 한다.

다섯째, 국가사이버안전위원회의 위원장은 사이버위기가 발생하거나 발생할 가능성이 현저하여 국가·사회 전반에 미치는 중대한 영향 또는 피해를 최소화하기 위하여 국가차원의 긴급한 대응조치가 필요한 경우에는 위원회의 심의를 거쳐 사이버위기사태를 선포할 수 있고 선포시에는 국회에 통고하여야 하고 국회의 의결에 따라 사이버위기사태 해제를 요구시 위원장은 위원회의 심의를 거쳐 사이버위기사태를

즉시 해제하여야 한다.

여섯째, 국가사이버안전위원회의 위원장은 사이버위기사태시 책임기관의 장에게 사이버공격 감시활동, 긴급 복구대책 수립·시행, 사이버공격에 이용되는 정보통신망의 접속경로 차단 등 긴급 안전조치를 취하게 할 수 있다.

일곱째, 국가사이버안전위원회의 위원장은 사이버위기사태시 원인분석, 긴급대응, 피해복구 등을 위하여 관계기관 및 전문인력이 참여하는 사이버위기사태대책본부를 구성·운영하며 관계기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다.

여덟째, 책임기관의 장은 소관 정보통신망에 대한 사이버공격 사실을 발견한 경우에는 자체 조사를 실시하고 그 결과를 대책본부장에게 통보하여야 하며, 대책본부의 장은 필요할 경우에 직접 사고조사를 실시할 수 있다는 것 등이다.

Ⅴ. 결 론

정보통신기술의 비약적 발전으로 컴퓨터와 인터넷 등으로 이루어진 사이버공간이 국민생활과 국가안보의 중요한 영역으로 대두되었으나 사이버공간은 범지구적이며 국내적으로는 정부와 민간부분이 상호 연계되어 있어 사이버공간에서 발생하는 공격은 국경을 초월할 뿐만 아니라 정부 단독으로는 복잡하고 고도화되는 공격을 모두 차단하기에는 한계가 있다.

또한 1·25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터의 조직적인 사이버공격으로 인한 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을

미칠 수 있는 사이버위기 발생 가능성이 날로 증대되고 있으나 국가차원에서 체계적으로 대응할 수 있는 구체적 방법과 절차가 정립되어 있지 않아 사이버위기 발생시 국가안보와 국익에 중대하고 명백한 위험이 초래될 우려가 있다.

이에 따라 정부와 민간부분을 포함한 국가차원에서 사이버공격을 사전 탐지하고 정보를 공유할 수 있는 체계를 구축함으로써 사이버위기 발생을 예방하고 사이버위기가 발생하였을 경우에는 국가의 역량을 결집하여 효율적으로 대처할 수 있는 체계의 구축 및 대응활동 등을 명확히 규정하는 법률제정이 조속히 이루어 져야 할 것이다.

토 론 문

고 낙 훈
(법제처 법제관)

□ 사이버 안전 정책에 관한 법제의 정비 필요

○ 급속히 진전되는 정보화 사회로의 진입에 부응하여 이에 따른 정보화 역기능의 방지, 정보 및 시설의 보호와 피해 발생시 효율적인 보완 및 복구 등을 강구할 필요성은 절실함.
- 다양한 발제 주제 중 사이버 안전관리체계 및 이에 따른 법제적 측면에 중점을 두고자 함.

○ 현행 사이버 안전관리 체계에 관한 법제는 정보화촉진기본법을 비롯하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보시스템의 효율적 도입 및 운영등에 관한 법률」, 「전자정부법」등이 있고, 직접적으로는 「정보통신 기반보호법」이 마련되어 있으나,
- 각각의 법률은 제정된 이래 새로운 정보화 영역이 출현할 때마다 그때 그때의 필요에 따라 추가하는데 급급하였던 실정임.
- 목적의 혼재, 규율대상의 중복, 정부기관 또는 위원회의 권한 중복 및 과다설치 등의 문제가 상존

○ 관련 법령간의 체계화 및 통일이 절실, 예를 들면
- 민간 및 공공분야
- 축적된 정보의 보호

- 기반 시설, 인프라의 보호, 분야 등으로 구분,
- 국가사이버안전규정 만으로는 미흡한 실정

○ 기본법 성격의 법률의 마련하고, 여기에 근거하여 분야별 규율 영역을 명확히 할 필요가 있음

□ 국가사이버 안전 정책에 관한 제언

○ 국가정보원, 군, 사법기관 등의 기능 분담이 필요
- 사이버 침해 사고에 대하여는 국가안보차원에서 대처할 필요성이 증대, 다만 권력기관의 역할에 대하여는 그 간의 역사적 경험에 비추어 국민적 공감대를 넓히는 방안을 강구
  · 권력기관이 전면에 나서는 것을 기피하는 감이 있는데 이것이 타당한 것인지
- 최근 비밀의 보호에 관하여는 국가정보원 주관으로 기본법이 마련되어 국회에 제출된 바 있음
- 통계에 나타난 사이버 침해사고의 분류기준은 무엇인지?
  · 예상을 초월하는 사고건수에 대한 대국민홍보의 여건은 마련되지 않았는지?

○ 국가사이버 안전관리규정 만으로 민·관·군 간의 사이버 위협정보의 공유, 공공기관의 협력부족, 법률 규정 상호간의 상충시 권한의 제약 등을 극복하기 위하여 사이버 안전정책을 종합·조정하고, 대응체계를 일원화하는 국가사이버 안전업무 추진체계의 보강이 필요하다는 의견에 공감함.

○ 전문 인력의 체계적인 양성이 필요
- 직접적 위협인 북한, 잠재적 적성국인 중국의 최근 동향을 둘러싼 분석을 보면 전문 사이버 조직(부대)를 대량 양성하고

있는 것으로 보임

- 사이버 침해에 대한 공세적 안전 정책의 필요성은 없는지, 필요할 경우 우리도 전문 인력의 양성을 심각하게 고려하여야 함.

○ 국제협력증진

- 해외 사이버 공간을 통한 우회 침해사고, 해외 단체 또는 다수 외국인의 악의적인 합의에 의한 사이버 인프라 침투 등에 대비한 강제성 있는 국가간 협력등도 모색되어야 할 것으로 보임.

□ 국가사이버 안전 전담기구

○ 현행 국가사이버 안전담당기구인 국가사이버안전센터, 한국정보보호진흥원, 국방정보전대응센터가 공공기관·민간·국방분야로 분담하여 수행하고 있는 기능은 초기단계의 긴급사태에 대응한 체제로서 이해할 수 있고 그 간에 많은 기여를 한 사실을 인정할 수 있으나, 사이버 사고의 공간인 인터넷이 민·관·군 영역을 구분할 수 없는 추세를 감안하면

- 이 기관들의 설립근거를 법제 측면에서 뒷받침하고,
- 이들 기관을 통합·조정할 수 있는 단일기구 설치를 검토할 필요가 있음

□ 사이버 안전 예방활동

○ 국가정보원·중앙행정기관·소속 산하기관 간의 사이버안전 활동의 협조는 실제로 어느 정도 이루어지고 있는지

○ 상당부분이 강제성이 없는 협조·요청 등의 요건으로 되어 있을 경우 그 실효성은 어떻게 담보할 것인지 검토가 필요

□ 보안 관제 활동

○ 사이버 보안 관제 활동의 필요성은 수긍할 수 있으나 이를 법제화하는 데는 상당한 어려움이 예상됨.

- 우선 명백히 우려할 만한 정보에 근거할 경우 엄격한 절차를 걸쳐 사이버 공간에 대한 보안 관제 활동을 허용할 수 있는 방안은 강구하여야 할 것임.
- 추후 이러한 건설적인 실적이 축적되고 사이버 침해 사고의 치명성에 대한 국민적 공감대가 확산될 경우 점차 효율적인 사이버 보안 관제 활동방안을 마련할 수 있는 여건이 조성되리라 봄.

□ 실효성 있는 사이버위기 대응체계의 필요

○ 역할·책임소재의 단일화

○ 정보의 공유·협력·시정의 권고 보다는 좀더 실효성 있는 조치를 취할 수 있는 체계가 마련되어야 할 것임.

토 론 문

김 충 섭
(국회 정보위원회 입법조사관)

1. 적용범위의 조정

현행 정보통신기반보호법이 정의하고 있는 주요정보통신기반시설과 국가사이버안전관리규정이 적용되는 대상이 다소 상이하므로 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 포함하여 주요 민간기업의 정보시스템과 사설 인터넷망 전체로 적용범위를 확대할 필요 있음.

2. 대응법률 분산의 문제점

우리나라의 사이버테러 대응법률은 여러 가지의 관련법과 규정에 분산되어 있음으로 일관성을 유지하기 어려운 실정임. 사이버테러 관련 법령이 여러 곳에 분산되어 법 적용에서 중복과 책임의 한계가 불분명하고 일관성 있는 통제가 어려움. 따라서 사이버테러 분야를 총괄할 수 있는 단일한 법[1] 제정 필요성 있음.

3. 부서간의 협조체제 미흡

정보통신기반보호법상 주요정보통신기반시설에 대한 지정은 기본적으로 각 부처가 지정하는 것으로 되어 있기 때문에 그 부작용으로 나

1) 현재 공성진의원 대표발의로 『사이버위기 예방 및 대응에 관한 법률안』이 '06년 12월28일에 국회사무처로 제출되었으나, 소관문제로 인하여 '07년 1월 18일 국회의 안소관조정위원회 조정을 거쳐 국회법 제81조제2항에 따라 국회운영위원회에 협의 요청된 상태임. '07년 4월 중 국회 과학기술정보통신위원회 또는 국회 정보위원회로 회부될 예정임.

타난 현상이 2003년 정보통신부와 한국정보보호진흥원(KISA)의 자체 조사결과에 따른 제3차 주요정보통신기반시설의 지정이 부처간의 협의 지연을 이유로 미루어진 바 있음. 주요기반시설에 대한 사이버테러 시 상상할 수 없는 엄청난 피해가 발생할 가능성이 있다는 점에 비추어 보면 법 개정을 통해 주요정보통신기반시설의 보호에 대해 모든 사항을 책임지고 통합하는 기구의 제정이 시급하다고 볼 수 있음.

또한 2003년 1·25 인터넷 대란을 겪으면서 이러한 문제를 해결키 위해 국가정보원에 국가 사이버보안의 실질적인 총괄기구라고 할 수 있는 국가사이버안전센터를 두었지만 주요정보통신기반시설은 제외하고 있으므로 유사시 혼선이 우려됨. 국가사이버안전센터가 총괄기구로서 역할을 하려면 인터넷침해사고대응지원센터와 국방정보전대응센터를 비롯해 각종 정보공유분석센터와 일반기업의 컴퓨터 침해사고대응팀(CERT)까지 아우르는 정보공유체제가 구축돼야 하는데 현재는 이에 대한 명확한 법적 근거가 없는 것이 문제임.

4. 정보공유분석센터의 운영

정보통신기반보호법은 정보공유분석센터를 금융·통신 등 분야별 정보통신기반 시설을 보호하기 위해 구축·운영할 수 있도록 함. 정보통신기반보호법에서는 정보공유분석센터의 업무를 취약점 및 침해요인과 그 대응방안에 관한 정보 제공 및 침해사고가 발생하는 경우 실시간 경보·분석체계 운영을 주 내용으로 함. 그러나 실제적으로는 자사 및 회원사들의 정보나 취약점이 노출될 것을 우려하여 상호 정보교류가 형식적인 수준에 머무르고 있다는 비판을 받고 있음. 정부가 현재 정보공유분석센터의 구축을 장려하고 그에 대한 기술적 지원을 강화하는 가운데 이를 더 강력히 추진하고 지원하면서 필요한 정보를 상호 협조할 수 있도록 하기 위해 주요 업무를 좀 더 구체적으

로 명시할 필요가 있음.

5. 침해사고 대응센터의 협조미흡

정보통신망이용촉진및정보보호등에관한법률 제52조의 “정부는 정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위하여 한국정보보호진흥원을 설립한다.”는 조항에 의해 한국정보보호진흥원을 1996년 4월에 설립하였고, 2003년에는 진흥원내에 인터넷침해사고대응센터를 운영 중에 있음.

동일한 사이버테러 정책을 두고 이를 집행하는 기관이 이처럼 나뉜 것은 국가정보원법 및 정보통신기반보호법 등과 같은 현행법에서 공공부문에 대한 보안은 국가정보원에서 책임지도록 규정하고 있고, 민간부문의 안전은 정보통신부가 맡도록 규정하고 있기 때문임. 그러나 이러한 권한 분산은 오프라인에서의 보안문제를 해결하는 데는 별다른 어려움이 없겠으나, 사이버환경에서의 공공부문과 민간부문의 모든 정보시스템이 유기적으로 연결되어 있는 상태에서는 사이버테러에 대한 대응체계가 이처럼 이원화되어 있는 것은 불합리한 측면이 있음.

더욱이 유사한 업무를 국가차원에서 통합·지휘할 수 있는 실무 리더(Leader) 기관이 불분명하여 일관성 있는 대응이 어렵다는 점, 평시·위기 시 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 있음.

6. 위험수준 단계별 경보발령 및 대응요령 제도화 미흡

긴급사태 발생시 신속하고 체계적으로 대응하기 위한 예·경보체계 구축과 연계하여 사이버테러의 위험수준을 평가하여 적정등급을 발령

하고 등급에 맞도록 대응하는 위험단계 및 대응요령 등의 대처방안이 수립되어야 할 것임. 현재 국가사이버안전관리규정에 의하여 정상, 관심, 주의, 경계, 심각의 5단계로 구분하여 이에 대한 대처요령이 마련되어 있으며 경보협의회를 운영하도록 되어있으나 대통령 훈령으로 되어있는 규정으로만 규제하고 통제하기에는 미흡하다고 볼 수 있음.

따라서 평시와 긴급상황에서의 사이버테러로부터 효율적으로 대처하기 위해서는 국가안보차원의 대응체계 식별과 기관별 역할, 경보 발령 및 행동요령 등이 관련법으로 명시되어야 할 것임. 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 할 것임.

7. 국제적 협력체제 미흡

사이버공간에서 발생하는 각종 테러행위는 국내에만 국한되는 문제가 아니며, 인터넷을 비롯한 정보통신망의 특성으로 말미암아 미국에서 발생한 웜이나 바이러스가 국내에 즉시 유입되고 있으며 특히 해킹사고는 대부분 중간경유지를 통과하여 일어나기 때문에 다른 어떤 분야보다도 사이버테러의 예방과 사후 처리를 위하여 국제간의 협력 증진은 중요한 과제라고 할 수 있음.

우리 정부도 사이버테러 분야에서 국제적 협력의 중요성을 인식하고 많은 노력을 기울이고 있으나 아직도 미흡한 것이 사실이며, 먼저 사이버테러에 관한 신속한 정보공유를 위한 국가 간 합의와 구체적인 실천 방안이 아직 충분히 마련되어 있지 못하다는 점을 지적할 수 있음.

둘째, 신속한 정보공유와 수집을 위한 다양한 채널이 마련되어 있지 않은 문제가 있음.

셋째, 우수한 정보보호기술을 보유하고 있는 글로벌 IT기업 등과의 기술교류가 부족한 문제가 있음.

<정보통신기반보호법과 국가사이버안전관리규정 비교>

구분	정보통신기반보호법	국가사이버안전관리규정	비 고
목적	전자적 침해행위에 대비한 주요정보통신기반시설의 보호에 관한 대책수립 및 시행	국가사이버안전에 관한 조직체계 및 운영에 대한 사항 규정과 수행 기관과의 협력 강화 및 사이버공격에 대한 국가정보통신망의 보호	보호하는 대상의 차이에서 목적이 다소 상이
정의	정보통신기반시설, 전자적 침해행위, 침해사고에 대한 정의	정보통신망, 사이버공격, 사이버안전, 공공기관에 대한 정의	사이버테러의 정의 없음
적용범위	중앙행정기관의 장이 주요정보통신기반시설을 지정	중앙행정기관, 지방자치단체 및 공공기관의 정보통신망으로 제한하며 정보통신기반 보호법에서 정의한 주요정보통신기반시설에 대하여는 적용하지 않음	서로 적용 대상이 다름
책임	국무총리 산하에 정보통신기반보호위원회가 주요정보통신기반시설의 보호에 관한 사항을 심의	중앙행정기관의 장은 소관 정보통신망에 대하여 사이버안전을 위한 필요한 조치를 취할 책임을 명시	모든 사항을 책임지고 통합하는 기구 없이 해당 부처 책임하에 관리
조직	국무총리 소속하에 정보통신기반보호위원회 운영	국가정보원장 소속하에 국가사이버안전전략회의 및 국가사이버안전대책회의를 운영하고 국가사이버안전센터 운영	

기능	위원회는 보호정책의 조정, 보호계획의 종합, 보호와 관련된 제도의 개선 및 주요 정책사항 심의 각부 부처가 주요정보통신기반시설에 대한 지정 수행	전략회의는 국가사이버안전체계의 수립 및 개선, 사이버안전 관련 정책 및 기관 간 역할 조정 및 대통령 지시사항에 대한 조치방안 심의 국가사이버안전센터는 정책의 수립, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배포, 사고의 조사 및 복구지원, 외국과의 사이버위협 관련 정보의 협력을 수행	주요정보통신기반시설에 대한 원활한 지정 미흡
	주요정보통신기반시설은 취약점 분석·평가를 위한 전담반 구성	국가사이버안전매뉴얼 작성	취약점 분석·평가의 방법 및 절차는 별도의 대통령령으로 정함
보호지침	관계중앙행정기관의 장이 소관분야의 주요정보통신기반시설에 대한 보호지침을 제정	별도의 보호지침은 없으나 국가사이버안전메뉴얼의 작성 및 배포 업무를 명시	
보호조치명	관리기관은 보호대책을 제출하고 관계중앙행정기관은 이를 분석하여 필요한 조치를 명령 또는 권고한다.	보호조치 명령에 대한 명시 없음	대응요령의 명시 없음

령			
복구조치	관리기관의 장은 침해사고에 대한 복구시 관계중앙행정기관 또는 보호진흥원의 장에게 지원을 요청할 수 있으며 관리기관의 예산의 범위안에서 복구비 등 재정적 지원이 가능하다.	복구시 관계중앙행정기관의 장에게 요청 할 수 있으며, 재정적 지원에 대한 명시가 없다. 발생한 사고는 그 원인을 분석하기 위한 조사를 할 수 있다.	
대책본부	대책, 기술지원 및 피해복구를 위한 정보통신기반침해사고대책본부를 둘 수 있다.	대책본부의 명시 없음	