主題

정보유출에 따른 대응현황과 과제

한국정보보호센터 박광진, 주덕규

차 례

요 약

본 고는 급격한 정보통신환경 변화와 국가사회의 정보기반에 대한 의존성 증가에 따른 정보유출 위험성과 정보유출 및 대응현황을 조사·분석하고, 이러한 조사·분석 결과 나타난 현행 법·제도적 미비점들을 개선하기 위하여 정보의 등급별 보호제도의 개선, 국가 PKI의 조기 구현 및 정보주체의 권익 향상과 주요 기반구조 보호를 위한 민관 협력체계의 구축 등 새로운 질서 확립을 위한 효율적인 법·제도적 과제를 도출하였다.

ABSTRACT

This study surveyed the risks of unauthorized disclosures of information and analyzed the current status of legal correspondence. And assignments introduced for the establishment of new order in Cyberspace. This involved the improvement of rated information protection system, the building PKI, the progress of user's right and industry and government to work together for critical infrastructure protection from destructive Cyber attacks.

I. 서 언

최근 우리 나라를 비롯한 주요 선진국은 21세기 국가경쟁력 제고의 극대화를 위하여 정보사회를 기반으로 하는 지식기반(knowledgr-based)국가의 구현에 박차를 가하고 있다. 지식기반국가의 구현으로 가치있는 지식정보를 효율적으로 창출, 배분하고 활용함으로써 정치, 경제 및 사회 각 분야의 경쟁력을 극대화시키고 나아가 대국민 행정서비스 향상과

고도 경제성장 등을 실현할 수 있다. 그러나 이는 지식정보의 안전한 유통체계의 구축과 정보주체의 권리보호의 확대를 선결요건으로 작용하고 있다.

정보기술의 급속한 발전에 따른 컴퓨터 범죄와 정보보호에 대한 침해행위의 증가는 국가의 경쟁력과 가상공간에서의 법의 지배(the rule of law)에 대한 명백한 위협이 되고 있다. 국가사회 주요 정보의 정보시스템에 대한 의존도가 높아지고, 개방성의 특징을 지니고 있는 가상공간에서의 유통이 증가함에 따라 해킹(Hacking)과 컴퓨터바이러스 유포 등 정보화 역기능으로 인한 정보침해와 정보시스템 장애 유발 등 각종 위협에 대한 대응의 중요성은 더욱 증대되고 있다. 이는 현실적으로 전자정부의 구현과 전자상거래의 활성화에 큰 걸림돌로 작용하고 있다. 또한 프라이버시 및 지적재산보호 등 정보주체의 권리의식이 높아짐에 따라 정보주체의 자기정보통제권 및 정보보호 수단의 자유이용권 등 새로운 권리가 대두되고 있다.

이에 각국은 고성능 정보보호기술의 보급확대와 더불어 새로운 사회환경에 부합하는 법규범 마련 등 다양한 대책을 강구함으로써 가상공간에서의 새로운 질서의 형성을 도모하고 있다. 그러나 아직 당면한 수많은 문제점을 해소하기에는 충분한 여건이 마련되지 못하고 있는 실정이다.

따라서 본 고에서는 지식정보의 유출방지 현황과 정책적 과제를 살펴봄으로써 창조적 지식기반국가 건설에 필수적인 정보보호 논의의 기본방향을 제시하고자 한다.

Ⅱ. 정보의 이용과 유출 현황

1. 정보의 개념

국내 정보 관련 법령에서는 각 법의 목적에 따라 "정보"에 대하여 달리 정의하고 있다. 정보화에 관한 일반법인 「정보화촉진기본법」(개정 99.1.21, 법률 제5669호)에서는 "정보"를 "자연인 또는 법인이 특정목적을 위하여 광 또는 전자적 방식으로 처리하여 부호·문자·음성·음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식"으로 정의하고 있으며, 「공공기관의정보공개에관한법률」(제정 96.12.31, 법률 제5242호)에서 "정보"라 함은 "공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서·도면·사진·필름·테이프·슬라이드 및 컴퓨터에 의하여 처리되는 매체 등에 기록된 사항"으로, 특히 「행정정보공동이용에관한규정」(제정 98.3.28, 대통령령 제15745호) 에서는 "행정정보"라 함은 "행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 광 또는 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것"으로 정의하고 있다.

결국 정보는 "광 또는 전자적 방식으로 처리"되어 "부호·문자·음성·음향·영상 등으로 표현된" "자료나 지식"으로 정의할 수 있으며, 정보의 형태와 보안요구수준 및 보유주체와 처리목적 등에 따라 다양한 종류로 분류할 수 있다. 보안요구 수준에 따라 국가안보를 위하여 지정되는 비밀정보(classified information)와 비밀로 지정되지 아니하였지만 민감한 정보(sensitive but unclassified information), 처리목적에 따라 행정정보와 민간정보로 그리고 정보형태에 따라 개인정보, 신용정보 등으로 구별할 수 있다. 한편, 정보의 일종인 지식(knowledge)이란 보다 정확한 정보를 지칭한다. 우리가 현재 생산하고 입수할 수 있는 수많은 정보를 모두 지식이라고 할 수는 없다. 서적이나 인터넷상에서 입수할 수 있는 정보는 가독(read)되어지고 이해할 수 있어야만 지식으로 이용할 수 있다. 정보가 어떻게 해석되고 활용되어지느냐는 상이한 독자의 사전 경험이나 전문지식 및 필요성에 따라 달라지기 때문이다.

2. 정보의 이용

(1) 정보의 종류

지식정보사회의 구현은 각 조직에 다양하게 소재하고 있는 유용한 정보가 안전하게 관리되고, 필요한 자에게 적시 제공되는 기반환경 조성이 선행되어야 한다. 특히 다양한 지식정보를 방대하게 보유하고 있는 행정내부의 효율적인 정보공동 활용체계를 구축하여 행정능률의 향상을 도모함으로써 사회 각 분야의 지식정보화를 선도하고 나아가 국가 경쟁력 극대화에 크게 기여하게 되는 것이다.

행정기관이 보유·관리하는 행정정보는 문서자료의 감축을 통한 자원절감과 정보활용도 제고를 통한 업무의 능률적인 수행을 도모하기 위하여 기관간 공동으로 이용할 수 있도록 하여야 한다. 행정정보의 공동활용은 궁극적으로 대민 행정서비스의 질을 향상시킴으로써 국민의 삶의 질 향상과 국가경쟁력 제고를 통한 경제성장의 밑거름으로 작용할 수 있다. 정보사회에서 행정기관은 국방·외교 등 국가안보에 관한 국가비밀정보뿐 아니라 국가이익과 행정업무수행 및 개인 프라이버시에 영향을 미치는 민감정보 그리고 의료, 과학기술, 건설, 공업 및 유통정보 등 각종 일반정보를 보유·관리하고 있다.

국가비밀정보는 "그 내용이 누설되는 경우 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가기밀"로서 법령에 의하여 비밀로 분류된 것을 말한다. 「보안업무규정」(개정 81.10.7, 대통령령 제10478호)에서는 그 중요성과 가치의 정도에 따라 ①누설되는 경우 대한민국과 외교관계가 단절되고 전쟁을 유발하며, 국가의 방위계획·정보활동 및 국가방위상 필요불가결한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀을 Ⅰ급비밀, ②누설되는 경우 국가안전보장에 막대한 지장을 초래할 우려가 있는 비밀을 Ⅱ급비밀, ③누설되는 경우 국가안전보장에 손해를 끼칠 우려가 있는 비밀은 이를 Ⅲ급비밀로 구분하여 보호하고 있다.

민감정보는 국가안보 및 국방·외교 등 국가이익을 위하여 비밀을 유지하도록 법령에 의하여 특별히 지정되지 아니하였으나 "당해 정보의 손실, 오남용 및 무단접근과 위·변작이 국가이익이나 정부업무수행" 또는 "개인정보보호법상의 개인의 프라이버시"에 현저히 위해를 미칠 수 있는 정보를 말한다. 「공공기관의정보공개에관한법률」(제정 96.12.31, 법률 제5242호)에서는 공공기관이 직무상 작성 또는 취득하여 관리하고 있는 정보의 공개에 대하여 규정하고 있으나 제7조에 다음과 같은 비공개대상정보를 열거하여 공개대상에서 제외하고 있다.

1. 다른 법률 또는 법률에 의한 명령에 의하여 비밀로 유지되거나 비공개사항으로 규정된 정보

2. 공개될 경우 국가안전보장·국방·통일·외교관계등 국가의 중대한 이익을 해할 우려가 있다고 인정되는 정보

3. 공개될 경우 국민의 생명·신체 및 재산의 보호 기타 공공의 안전과 이익을 현저히 해할 우려가 있다고 인정되는 정보

4. 진행중인 재판에 관련된 정보와 범죄의 예방, 수사, 공소의 제기 및 유지, 형의 집행, 교정, 보안처분에 관한 사항으로서 공개될 경우 그 직무 수행을 현저히 곤란하게 하거나 형사피고인의 공정한 재판을 받을 권리를 침해한다고 인정할 만한 상당한 이유가 있는 정보

5. 감사·감독·검사·시험·규제·입찰계약·기술개발·인사관리·의사결정과정 또는 내부검토과정에 있는 사항 등으로서 공개될 경우 업무의 공정한 수행이나 연구·개발에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는 정보

6. 당해 정보에 포함되어 있는 이름·주민등록번호 등에 의하여 특정인을 식별할 수 있는 개인에 관한 정보. 다만, 다음에 열거한 개인에 관한 정보를 제외한다.

가. 법령 등이 정하는 바에 의하여 열람할 수 있는 정보

나. 공공기관이 작성하거나 취득한 정보로서 공표를 목적으로 하는 정보

다. 공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보

7. 법인·단체 또는 개인의 영업상 비밀에 관한 사항으로서 공개될 경우 법인 등의 정당한 이익을 현저히 해할 우려가 있다고 인정되는 정보. 다만, 다음에 열거한 정보를 제외한다.

가. 사업활동에 의하여 발생하는 위해로부터 사람의 생명·신체 또는 건강을 보호하기 위하여 공개할 필요가 있는 정보

나. 위법·부당한 사업활동으로부터 국민의 재산 또는 생활을 보호하기 위하여 공개할 필요가 있는 정보

8. 공개될 경우 부동산투기·매점매석 등으로 특정인에게 이익 또는 불이익을 줄 우려가 있다고 인정되는 정보

그렇지만 본 조 제2항에서 공공기관에 대하여 위 각 호에 해당하는 정보가 기간의 경과 등으로 인하여 비공개의 필요성이 없어진 경우에는 당해 정보를 공개대상으로 하도록 요구함으로써 행정기관에 의한 자의적인 비공개를 못하도록 하고 있다.

이러한 행정정보의 효율적인 공동이용을 위한 체계를 구축하기 위하여는 안전한 정보관리와 명확한 이용방법 및 절차에 관한 명확한 기준이 마련되어야 한다. 특히 정보제공 목적외 사용 등 부정한 정보이용과 정보통신망을 통한 정보의 유출 등을 방지하기 위한 정보보호 조치가 필수적으로 강구되어야 한다.

(2) 정보의 공동이용

정보의 공동이용을 활성화하기 위하여는 행정내부의 공동이용체계뿐만 아니라 행정과 다른 공공기관 및 일반인과의 정보 접수·제공체계가 확립되어야 한다. 또한 공동이용체계는 정보의 이용촉진·보호 및 경제성을 고려하여 가장 효율적인 방법으로 하여야 한다.

현재 「행정정보공동이용에관한규정」에서는 중앙행정기관(대통령직속기관 및 국무총리 직속기관을 포함) 및 그 소속기관과 지방자치단체의 기관에 한정하는 행정기관이 보유·관리하고 있는 행정정보를 다른 행정기관이 정보통신망에 의하거나 디스켓·테이프 기타 이와 유사한 매체에 의하여 제공받아 이용하는 공동이용에 관하여 규정하고 있으며, 다른 공공기관 및 일반인과의 공동이용에 관하여는 규정하고 있지 아니하다. 다만 「공공기관의정보공개에관한법률」에 의하여 공개청구가 가능하다.

행정기관간 공동이용의 대상이 되는 행정정보는 ①「공공기관의개인정보보호에관한법률」 제10조 제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보, ②각종 민원서류의 내용을 이루는 행정정보, ③통계정보·문헌정보·업무정보 등 행정업무의 수행에 참고가 되는 행정정보, ④일반적으로 공개가능한 행정정보, ⑤「정보화촉진기본법」 제8조의 규정에 의한 정보화추진위원회(이하 "위원회"라 한다)가 행정기관간 공동이용이 필요하다고 인정하는 행정정보로써(영 제5조), 행정기관의 장은 그 소관업무를 수행함에 있어서 다른 행정기관이 보유·관리하는 행정정보를 이용할 필요가 있는 경우에는 그 보유기관에 대하여 이용목적을 밝혀 당해 행정정보의 제공을 요청할 수 있으며(영 제11조), 행정정보의 제공요청을 받은 행정기관의 장은 정당한 사유가 없는 한 당해 행정정보를 제공하여야 한다(영 제12조).

다른 기관으로부터 제공받은 행정정보에 관하여 ①이용목적 외의 목적으로 이용하는 행위, ②수정·가공 등 변형시키는 행위, ③제공받은 행정정보 또는 그 변형된 행정정보를 스스로 구축한 행정정보인 것처럼 취급하는 행위, ④다른 기관에 다시 제공하는 행위 등을 제한하고 있으며(영 제13조), ①행정정보를 제공하는 경우에 행정정보의 이용·관리 등에 필요한 조건을 제시할 수 있으며 필요한 관계자

료의 제출을 요구할 수 있도록 하고 있는 제12조제2항의 규정에 의한 조건을 행정정보를 제공받은 기관이 이행하지 아니함으로써 행정정보의 관리 기타 소관업무의 수행에 지장을 초래한 경우, ②행정정보를 제공받은 기관이 제13조의 규정을 위반한 경우, ③기타 행정정보의 제공을 중단하거나 이미 제공한 행정정보를 회수하고 그 이용을 금지하여야 할 불가피한 사유가 생긴 경우에는 해당기관에 대하여 행정정보의 제공을 중단하거나 이미 제공한 행정정보의 반환 및 그 이용의 금지를 요구할 수 있도록 하고 있다(영 제14조).

3. 정보의 유출현황

(1) 위험성

정보와 통신의 결합으로 탄생된 새로운 가상공간(Cyberspace)은 더 이상 과학적 허구로 존재하지 아니한다. 수백만의 인구가 일상적으로 주요 업무를 네트워크화된 정보시스템을 이용하고 있다. 컴퓨터 시스템, 통신시스템 및 인간(이용자와 운영자 등)으로 구성된 네트워크화된 정보시스템에 대한 의존이 증가함에 따라 이에 대한 안전 · 신뢰성이 확보되지 아니하게 되면 정보화 촉진은 요원하게 된다. 유출된 정보는 그 자체로 국익저해 및 개인의 사생활 침해이지만, 타인의 개인정보를 이용하여 금전적 이득을 취하는 등 2차적인 범죄에 악용되고 있다.

오늘날 국가안보, 경제적 경쟁력 및 국민의 건강과 복지 등이 통신, 금융 및 운송 등 기반에 대부분 의존하고 있으며, 이들은 네트워크화된 정보시스템에 대한 의존이 증가하고 있다. 특히 전자정부의 구현은 개방 정보통신망을 기반으로 하고 있기 때문에 해킹 및 내부자에 의한 정보유출 등 위험성이 상존하게 된다.

대표적인 침해위험인 해킹은 타인의 정보시스템 취약점을 이용하여 불법접근 후 자료의 유출, 위 · 변조, 삭제 및 과부하로 시스템을 정지시키는 행위이며, 불법접근은 해킹을 위한 기본으로서 "가택무단침입"과 같은 행위로서 ID를 도용하거나 시스템 허점을 이용하여 접근한다.

자료 유출행위는 도청프로그램을 설치하여 ID와 비밀번호를 알아내거나 사용자 및 시스템의 중요정보를 유출하며, 자료 위 · 변조는 사용자 및 시스템의 주요 파일을 변조하여 오동작을 유발하거나 잘못된 정보를 제공한다. 자료 삭제 · 파괴는 디스크의 모든 자료를 삭제하는 경우가 많아 백업을 하지 않을 경우 막대한 손실을 입게 된다. 과부하정지는 시스템이나 네트워크에 업무와 트래픽을 가중시켜 정지시키거나 정상동작을 방해한다.

최근 국내 · 외 해커들이 개발한 신종 해킹프로그램들이 인터넷을 통해 널리 유포됨에 따라 이를 이용한 해킹사고가 급속하게 증가하고 있으며 대규모 네트워크 대상 침투와 파괴목적의 공격방법들이 등장하고 있다. mscan, sscan(해킹을 위한 취약성 자동 검색도구, 해킹사고의 70% 차지), smurf, (네트워크 부하를 주어 마비시키는 공격), Back Oriffice(원격지에서 윈도우PC 자료열람/삭제 공격) 등 신종 해킹기법을 이용한 해킹공격이 증가하고 있다.

(2) 현황

1998년 '월간인터넷 · 정보공동체포럼'이 일반인 응답자 104명을 대상으로 조사한 결과에 따르면, 응답자 60%가 개인정보유출 등 Privacy 침해문제를, 17%가 국가 중요문서의 유출 및 보안문제를 전자정부 구현시 우려되는 문제로 답변한 것으로 나타났다.

실제로 한국정보보호센터의 『정보화 역기능 현황 · 분석 및 대응방안 연구』(1998)에 의하면 1997년도 자료유출 발생건수는 총 22건이 발생하여 '96년 15건에 비하여 약 45%이상의 증가를 보였다. 특히 개인정보 등 민감정보의 유출이 70%이상을 차지하여 이에 대한 대비가 절실히 요구되고

있다. 공공기관의 자료유출은 '95년도 7건에서 '96년도 4건으로 줄어들었으며 '97년도에도 같은 수준을 유지하고 있다. 자료유출의 대부분을 차지하고 있는 해킹발생건수는 '97년 64건, '98년 158건, '99. 5 현재 156건으로 지속적으로 증가하고 있다.

컴퓨터범죄 단속실적으로는 '96년, 17건 37명을 입건하여 9명 구속, '97년, 133건 233명을 입건하여 71명 구속, '98년 196건 625명을 입건하여 163명을 구속하였다(검찰청, http://dci.sppo.go.kr).

또한, 현행 법령으로 보호되도록 하고 있는 공문서를 제외한 지식정보사회에서 특히 요구되는 유용한 정보가 입법미비로 제대로 보호되지 못하고 있는 실정이다. 담당 공무원들의 책임회피를 위하여 파기되거나 금전적 이득 등을 위하여 국외로 유출되는 경우에는 사실상 현황파악이 되지 못할 뿐 아니라 실효적으로 대응할 수 없게 된다.

최근 미국 CSI/FBI에 의하여 미국 기업, 정부기관, 금융기관 및 대학의 보안실무자 521명의 설문응답을 기초로 작성한 「1999년 컴퓨터범죄 관련 연례 조사보고서」에서 컴퓨터 범죄 및 기타 정보보호침해가 국내 경제 경쟁력 및 사이버스페이스에서의 법의 지배(the rule of law)에 심각한 위협을 주고 있음을 보여주고 있다.

외부자에 의한 시스템 침입(system penetration)이 3년간 지속적으로 증가하고('99년 응답자중 30%가 침입을 보고), 내부자에 의한 비인가 접근도 3년간 매년 증가하였다('99년 응답자중 55%가 침해사고를 보고). 또한 컴퓨터안전침해로 인한 금전적 손실은 3년간 약 1억 달러를 상회하였으며, '99년 보고서에는 총163개 기관에서 약 123백만 달러의 손실을 입은 것으로 나타나고 있다. 특히 법 집행기관에 대한 중대한 침해사고가 예년 17%대에서 '99년 32%로 급격히 증가하고 있는 것으로 나타나고 있다.

Ⅲ. 정보유출의 대응현황과 과제

1. 대응현황

우리 나라는 국가비밀정보와 기타 행정정보를 구분하여 보호하고 있다. 국가비밀에 대하여는 헌법과 보안업무규정 등 개별 실정법상 비공개규정을 두는 경우, 정보공개제도의 예외로서 국익정보를 규정하고 이를 비공개대상으로 하는 경우, 침해행위에 대하여 형사적으로 처벌하거나 행정상 비밀준수의무 등을 통하여 엄격히 보호하고 있다.

그러나 국가비밀이 아닌 공공기관이 보유하고 있는 민감정보 등의 고의적인 파기와 국외 유출로 인하여 행정의 낭비 및 국가 경쟁력 약화의 요인으로 작용함에 따라 이에 대한 대비책이 시급히 요구되고 있다.

'99년 7월 1일부터 시행되는 개정 「정보화촉진기본법」(개정 99.1.21, 법률 제5669호)에서는 정부에 대하여 공공기관이 보유하고 있는 정보의 독점방지와 정보에 대한 자유로운 접근을 보장하기 위하여 공공기관 보유정보의 제공을 확대하고 그 유통을 촉진하기 위한 시책을 강구하도록 하고(법 제13조), 정보의 안전한 유통을 위하여 정보보호에 필요한 시책과 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구하도록 하고 있다(제14조).

「정보통신망이용촉진등에관한법률」('99.2.8, 법률 제5835호) 에서는 정보통신부장관에 대하여 국내의 산업·경제 및 과학기술 등에 관한 중요정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스제공자 또는 이용자에 대하여 필요한 조치를 강구토록 하고 있으며, 중요정보의 범위 및 그 보호를 위한 조치의 내용 등에 관하여 필요한 사항은 대통령령으로 정하도록 하고 있다(제21조).

정부기관이 생산 또는 취득하고 있는 공문서와 자료의 관리에 대하여는 「사무관리규정」(개정 98.7.1, 대통령령 제15823호)에 의하고 있다. 여기서 공문서는 "행정기관 내부 또는 상호간이나 대외적으로 공무상 작성 또는 시행되는 문서(도면·사진·디스크·테이프·필름·슬라이드·전자문서 등의 특수매체기록을 포함) 및 행정기관이 접수한 모든 문서"로, 자료는 "행정기관이 생산 또는 취득하는 각종 기록물(공문서를 제외한다)중 행정기관에서 상당기간에 걸쳐 이를 보존 또는 활용할 가치가 있는 도서·사진· 디스크·테이프·필름·슬라이드 기타 각종 형태의 기록물"로 정의하고 있다.

이 규정에서는 공문서를 '법규문서·지시문서·공고문서·비치문서·민원문서 및 일반문서'로, 자료는 행정간행물·행정자료 및 일반자료로 구분하고 있으며, 보안업무규정 제4조의 규정에 의하여 비밀로 분류된 문서(이하 "비밀문서"라 한다)중 영구적인 보존가치가 있다고 판단되는 문서에 대하여는 당해 문서의 비밀보호기간이 만료되는 즉시 그 원본을 정부기록보존소에 이관하도록 하고, 전산망을 활용하여 작성·시행 또는 접수·처리되는 전자문서를 보존·관리함에 있어서 멸실·분실·도난·유출·변조 또는 훼손되지 아니하도록 필요한 안전장치를 하도록 하고 있다.

행정기관간 행정정보의 공동이용의 경우에는 행정정보공동이용규정에 의하여 행정정보공동이용센터로 하여금 행정기관간 행정정보의 공동이용을 위한 정보통신망 및 중계시스템을 설치·운영하도록 하고, 정보화일 보호대책을 수립·운영하도록 하고 있다. 행정기관은 다른 기관이 보유·관리하는 행정정보를 정보통신망을 통하여 제공받거나 이용할 수 있는 바, 정보통신망을 연계·이용함에 있어서 정부가 이미 구축한 정보통신망·정보시스템·정보보호시스템을 우선적으로 이용하도록 의무화하고 있다.

또한, 행정기관의 장은 전산시스템을 도입 구축 또는 변경함에 있어서 행정정보의 원활한 공동이용과 충분한 보호가 이루어질 수 있도록 필요한 조치를 하도록 하고, 유출될 경우 국가의 안전보장, 국민의 권리 기타 공공의 안전과 이익을 해할 우려가 있는 행정정보와 일반적으로 공개될 수 있는 행정정보를 구분하여 관리하도록 각 행정기관에 요구함으로써 정보의 구분관리를 통한 효율적인 정보보호를 도모하고 있다. 한편, 행정기관의 장에 대하여 보유·관리하는 행정정보 또는 다른 기관으로부터 제공받아 이용하는 행정정보가 유출되지 아니하도록 적절한 보호대책을 강구하도록 하고 있다.

최근 정부는 공무원에 의한 정부자료의 파기 및 유출위험성이 용이해짐으로써 공공기관의 기록물관리에 관한 기본법인 「공공기관의기록물관리에관한 법률」(제정 99.1.29, 법률 제5709호) 제정하여 대응책을 마련하였다.

이 법에 의하여 모든 공무원은 공공기관의 기록물을 보호할 의무를 진다. 여기서 보호되는 기록물은 "공공기관이 업무와 관련하여 생산 또는 접수한 문서·도서·대장·카드·도면·시청각물·전자문서 등 모든 형태의 기록정보자료"이다.

기록물관리기관은 기록물의 공개청구에 신속하게 응하기 위하여 보존하는 기록물의 공개여부를 미리 분류하여야 하며, 기록물관리기관이 대통령령이 정한 기준과 절차에 따라 보존매체에 수록한 기록물은 원본과 동일한 것으로 추정한다.

이 법에서는 기록물을 무단으로 파기한 자와 무단으로 국외로 반출한 자에 대하여 7년이하의 징역 또는 1천만원이하의 벌금에 처하도록 하고, 기록물을 무단으로 은닉 또는 유출한 자, 기록물을 중과실로 멸실시킨 자 및 기록물을 고의 또는 중과실로 일부 내용이 파악되지 못하도록 손상시킨 자에 대하여도 3년이하의 징역 또는 5백만원이하의 벌금에 처하도록 하여 실효성을 담보하고 있다. 이 법의 시행일은 2000년 1월 1일이다.

전산보안 관련 지침에서도 개인정보는 가급 자료로 분류하여 보호하도록 요구하고 있다.

정보의 유출에 따른 정보주체의 보호에 대하여는 「공공기관의개인정보보호에관한법률」 등 에 규정하고 있다.

2. 과 제

가. 정보관리제도의 개선

행정기관이 보유하고 있는 정보는 국가안보 등을 이유로 비인가 유출로부터 보호되도록 법령에 의하여 비밀로 지정한 비밀정보와 기타 행정정보로 구분할 수 있다. 여기서 비인가 유출이란 비인가 수신인에게 비밀지정 정보를 통신 또는 물리적으로 이전시키는 것을 말한다. 비밀정보에 대하여 미국은 「국가비밀정보규정」('95. 4. 17 대통령령 제12958호)에 의하여 "Top Secret", "Secret" 및 "Confidential"로 수준을 구분하고 있으며, 「비밀정보에대한접근규정」('95. 8. 4 대통령령 제12968호)에 의하여 엄격한 접근절차를 규정하고 있다.

우리 나라는 「보안업무규정」에 의하여 국가비밀을 중요성과 가치에 따라 Ⅰ, Ⅱ, Ⅲ급비밀로 구분하여 엄격히 관리하고 있다. 또한 관련 규칙에서는 직무수행상 특별히 보호를 요하는 사항에 대하여 '대외비'로 구분하고 이를 비밀에 준하여 관리하도록 요구하고 있다.

민감정보를 비롯한 기타 행정자료는 자료의 중요도에 따라 가급, 나급, 다급 및 기타 자료로 분류기준을 정하고 있으며, 이 기준에 따라 각급 기관의 장이 자체 분류하여 보호등급을 부여하고 체계적으로 보호 관리하도록 하고 있다.

이와 같이 각급 행정기관별로 정보를 자체 분류하고 보호등급을 부여하게 됨으로써 기관간 정보보호 체계가 상이하여 체계적인 정보관리와 효율적인 정보공유에 걸림돌로 작용하게 될 우려가 있다. 따라서 정보의 분류를 표준화하고 보호등급에 적합한 보호수단을 채택함으로써 정보관리의 효율성과 비용절감 효과를 기대할 수 있다. 또한 정보등급별 정보접근기준을 제시함으로써 정보공개의 활성화에도 기여할 수 있게 된다.

나. PKI(Public Key Infrastructure)의 구축

민주주의 체제하에서 정부는 시민과 그들의 기구에 대하여 봉사하고 보호하기 위하여 존재한다. 최근 환경변화로 각국 정부는 업무능률 향상과 비용절감 차원에서 시민과 기업에 대한 통신과 상호접촉에 전자적 수단을 활용하는 이른바 전자정부(electronic government)의 구축에 박차를 가하고 있다. 성공적인 전자정부의 구현은 정부시스템에 대하여 시민이 적절한 보호조치와 프라이버시 보호가 확보될 수 있다고 신뢰할 수 있어야 한다. 따라서 인터넷과 같은 개방 네트워크 환경하에서 안전한 상호작용을 위하여 공개키 기술을 이용한 PKI의 구축의 필요성이 대두되고 있다. PKI는 이용자 인증과 비밀통신을 위한 제품과 서비스, 장비 및 정책, 절차와 약정 등으로 구성되는 기반구조이다.

정부는 ① 정부서비스와 정보에 대한 일반인의 접근 향상, ② 정부의 상이한 지위, 부서 및 기관의 내부 및 상호간의 정보소통 향상, ③ 서비스 질의 향상과 정부 운영비용의 절감, ④ 비밀로 지정되지 아니한 정부 정보시스템의 안전성 향상 등을 위하여 PKI를 이용할 수 있다.

PKI는 정보의 송수신인간의 신원확인과 전송정보의 위·변조 여부를 신뢰할 수 있는 환경을 조성하여야 하며 이를 고려한 인증체계와 암호이용에 관한 법·제도적 정비 및 활용기술의 채택 등 종합적인 PKI 구현전략이 수립되어야 한다.

미국에서는 연방 PKI 추진위원회를 구성하여 활동중이며, 각 연방기관별로 PKI 파일럿 프로젝트를 수행하고 있다. 동 추진위원회는 PKI가 지원하게 되는 적용분야와 이용자 요구사항을 연계시켜 구체화시키는 업무작업반(BWG), 기술, 설계, 표준 및 상호운영 관련 쟁점을 취급하는 기술작업반(TWG),

정책, 법규범 및 책임문제를 취급하는 법규범 및 정책작업반(LPWG)을 설치·운영하고 있다.

우리 나라는 '99년 전자인증에 관한 기본법인 「전자서명법」을 제정하여 시행하게 됨으로써 국가 PKI 구축을 위한 법적 기반환경은 마련하였다. 그러나 PKI제도의 조기 정착을 위하여 범정부적 차원의 PKI 구현전략 수립과 실천을 위한 정책이 추진되어야 한다.

다. 정보주체의 권익보호의 확대

비밀로 지정되지 아니하였지만 이에 준하는 보안이 필요한 민감정보(Sensitive But Unclassified)에는 정보주체의 권리보호가 특히 요구되고 있는 개인정보가 포함된다. 국민의 사생활 보호는 우리 헌법상 국민의 기본권으로 보장되고 있으며, 국가나 어떠한 사인에 의하여서도 개인정보를 침해받지 않도록 하고 있다. 특히 고도 정보사회에서 개인정보는 그 효용성이 증대됨에 따라 이를 이용하는 분야가 증대되고 있다. 이에 따라 정보주체가 공개를 원하지 아니하는 개인정보가 유출 또는 제공되고, 원하지 아니하는 정보가 제공되거나 제공목적외 이용되는 등 오남용에 대한 대책이 요구됨에 따라 각 개인이 정부 등에 의한 정보수집, 보유, 확산 등의 제반사항에 대하여 알 권리를 가지면서 자기에 관한 정보에 타인이 액세스하는 것을 배제하는 권리 및 자기에 관하여 틀린 정보에 대한 정정청구권 등이 인정되는 정보프라이버시 개념으로 변화되고 있다.

이와 같은 「공공기관의개인정보보호에관한법률」의 제정이후 개인정보를 취급하는 분야별로 관련 입법이 마련되고 있지만, 체계적인 감독체계의 부재와 자기정보에 대한 신속한 열람 및 정정신청 절차의 미비로 실효를 거두지 못하고 있는 실정이다. 따라서 공공과 민간부문을 포괄하는 감독체계의 마련과 더불어 전자서명법의 본격 시행에 따라 전자인증제도를 활용한 신속한 자기정보의 열람 및 정정신청과 처리절차 등을 위한 제도개선이 마련되어져야 하겠다. 다만 민간영역에 적용되는 개정 「정보통신망이용촉진등에관한법률」(개정 1999.2.8, 법률 제5835호)에서는 정보주체가 자기정보에 대한 열람 및 정정청구를 하는 경우 정보통신서비스제공자에 대하여 '지체없이 필요한 조치'를 취하도록 함으로써 이용자의 권익향상을 크게 도모하고 있다.

라. 민간 산업체와 사법당국과의 협력 강화 문제

국가사회의 주요 기반구조가 개방 네트워크 환경에 의존하게 되고 주요 정보가 가상공간에서 유통됨으로써 그만큼 정보보호의 필요성이 더욱 높아지고 있다. 이러한 정보통신 환경 변화에 따라 효과적인 정보보호를 위하여 미국 클린턴 행정부는 국가기반구조보호를 위한 대통령위원회(PCCIP)를 설치하고, '98년 5월 22일 기반구조보호 관련 대통령령(PDD 63)을 발표하는 등 일련의 대응조치를 강구하고 있다. 미국 국가기반구조보호센터(NIPC) 의장인 Michael A. Vatis는 "증가하고 있는 일반적인 사이버 범죄와 컴퓨터 침해문제에 산업체와 사법당국이 공동으로 대처할 필요가 있다"고 하면서, "침해사고, 위협 및 취약성에 대한 정보공유만이 네트워크상의 불법행위 퇴치와 파괴적인 사이버 공격으로부터 국가 주요 기반구조를 보호할 수 있다"고 한다. NIPC는 통신과 에너지, 운수, 금융과 응급서비스 및 정부운영을 포함한 국가 기반구조상의 사이버 공격의 예방 및 대응을 위하여 정부주도 메카니즘으로서 지원하기 위한 연방정부와 민간 산업체와의 공동 협력체이다. 현재 정보전 등 사이버 위협에 대응하기 위한 체계 확립을 위하여 법·제도적 연구와 기반구조 분야별 현황과 대응기술 분석 등 사전 연구가 활발히 진행되고 있다. 그러나 CDT 등 주요 시민단체에서는 민간 기업에 대한 정부의 부당한 간섭우려와 감시 등에 따른 폐해를 지적하고 있어 향후 귀추가 주목된다.

Ⅳ. 결 어

이상에서 지식정보사회에서는 유용한 정보에 대한 의존도가 증가함에 따라 정보의 안전한 관리 및 유통과 정보주체의 권리 확대가 중요하며 이에 대한 실효적인 법제도의 정비가 필요함을 살펴보았다. 이에 따라 본 고에서는 정부 및 공공기관이 보유하고 있는 민감정보의 분류 표준화 및 보호등급별 보호수단의 적용을 통한 효율적인 정보관리 및 정보접근 보장, 국가 PKI의 조기 구현을 통한 안전한 정보유통 보호, 정보프라이버시의 원칙에 따른 개인정보의 보호를 통한 정보주체의 권리확대 및 정부와 민간의 협력을 통한 사이버 공격에 대한 대응으로 국가사회 주요 기반구조의 효과적인 보호가 제시되었다.

국내 정보유출 위험증가에 따른 법제도적 대응은 즉흥적이고 통일성이 결여된 입법만으로 대응하여서는 그 실효성을 담보하기 어려우며, 가장 효과적이고 경제적인 정보보호 수단을 사용한 범정부적인 정보보호 체계의 구축이 요망된다.

※ 참고문헌

1. 손상영, "지식기반국가 건설을 위한 정부개혁", 「지식기반국가 건설을 위한 정책토론회 자료집」, 정보통신정책연구원, 1999. 2.
2. 총무처, 『개인정보보호제도』, 1998.
3. 통신개발연구원, 『정보사회에 대비한 일반법 연구(Ⅱ)』, 1998.
4. 한국정보보호센터, 『국내외 정보화 부작용 사례 및 통계분석』, 1998.
5. 한국정보보호센터, 『정보화 역기능 현황·분석 및 대응방안 연구』, 1998.
6. 한국정보보호센터, 『국가기관 전산망별 보안등급기준(안) 연구』, 1999.
7. A. Michael Froomkin, "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution", 1995.
8. CABINET OFFICE, "Encryption and Law Enforcement", A Performance and Innovation Unit Report, May 1999.
9. Department of Justice CANADA, "A SURVEY OF LEGAL ISSUES RELATING TO THE SECURITY OF ELECTRONIC INFORMATION", 1996.
10. DTI UK, "Our Competitive Future: Building the Knowledge Driven Economy"(Analytical Report), 1998.
11. Federal Public Key Infrastructure Steering Committee, "Access with Trust", U.S. OMB, 1998.
12. Fred B, Schneider, "Trust in Cyberspace", National Academy Press, 1998.
13. NRC, "Fostering Research on the Economic and Social Impacts of Information Technology", National Academy Press, 1998.
14. OGIT Australia, "GATEKEEPER, A Strategy for public key technology use in the Government", 1998.
15. U.S. PCCIP, "Legal Foundations" Report, 1997.
16. U.S. PCCIP, "Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures", July 1998.
17. Richard Power, "1999 CSI/FBI Computer Crime and Security Survey", Computer Security Journal, SPRING 1999.
18. U.S. Congress, Office of Technology Assessment, "Information Security

and Privacy in Network Environments", September 1994.
19. Wayne Madsen, "Critical Infrastructure Protection Gathering at the Supreme Court', Computer Fraud & Security, September 1998.

주 덕 규

1990년 2월 숭실대학교 대학원 법학과(법학석사)
1999년 2월 숭실대학교 대학원 법학과(법학박사)
1996년 9월~현재 숭실대학교 법대 강사
1997년 10월~현재 한국정보보호센터 기술정책팀 위촉연구원
※주관심분야 : 정보통신법, 정보보호정책

박 광 진

1982년 2월 동국대학교 전자계산학과(경영학사)
1988년 2월 한양대학교 대학원 전자계산학과 (공학석사)
1998년 9월~현재 광운대학교 대학원 전자계산학과 박사과정
1983년 7월~1988년 3월 한국전기통신공사
1988년 4월~1996년 5월 통신개발연구원 책임연구원
1995년 9월~1996년 5월 정통부 초고속기획단 파견
1996년 6월~현재 한국정보보호센터 기술정책팀장
※주관심분야 : 정보보호정책, 네트워크 보안