通信情報保護學會誌
第6卷 第3號, 1996. 9

OECD, 프라이버시 그리고 시큐리티

OECD, Privacy and Security

박 춘 식*

요 약

시큐리티에 관한 국제적인 움직임은 ISO/IEC, OSI 등의 국제적인 표준 활동외에도 OECD를 통하여 활발히 전개되고 있다. 본 고에서는 OECD와 정보 보호와의 관계 그리고 OECD와 프라이버시, OECD와 시큐리티와 관련된 사항만을 집중적으로 발췌하여 소개하고자 한다. 특히 OECD의 ICCP의 활동, OECD Privacy 8원칙, OECD 시큐리티 9원칙, 그리고 각국의 대응 등을 중심으로 살펴보고자 한다.

1. 서 론

OECD(Organization for Economy Cooperation and Development: 경제개발협력기구)라는 용어가 메스컴에 자주 등장하고 있어 한번쯤은 들어본 적이 있을 것이다. 우리나라가 OECD에 가입 신청을 내고 난 이후 더욱 더 많은 관심을 끌게 되었으며 마치 OECD 가입이 선진국가들과 어깨를 나란히 할 수 있는 기회로 생각하여 더욱 더 큰 관심의 대상이 되고 있다.

1948년 유럽에서 마샬 플랜 기금 관리를 위해 발족된 OEEC(Organization for European Economic Cooperation)가 OECD의 전신이며, 1960년 마샬 플랜이 완료된 후 미국과 캐나다가 새로운 가맹국이 되어 서구 산업 국가들 사이의 정책 조정을 위해 발족된 국제 기구다. 이후 1964년에는 일본, 1969년에는, 핀란드, 1971년에는 오스트라일리아, 1973년에는 뉴질란드, 1994년에는 멕시코, 1995년에는 체코, 1996년 헝가리, 폴란드가 각각 가맹국이 되었으며 1996년 7월 현재 한국과 슬로바키아가 가입 심사중에 있다.

OECD 내에는 21개 분야별 위원회가 있으나 OECD는 작년 3월 가입신청서를 제출한 우리나라가 가입에 앞서 심사를 통과해야 할 위원회로 7개 위원회를 선정했다. 우리나라는 7개 위원회 가운데 1995년 말 해운위원회와 보험위원회를 통과했고 금융시장위원회, 자본이동 및 무역외거래위원회, 국제투자 및 다국적기업위원회, 환경위원회, 재정위원회 등 5개 위원회중 대부분 심사 또는 통과 단계에 놓여 있다. 현재 우리나라는 OECD 가입을 위한 최종 단계에 있는 것으로 알려지고 있으며 위원회에서 좋은 판정이 있을 경우 1996년 9월경에

* 한국전자통신연구소

는 이사회의 최종 결정을 거쳐 체코, 헝가리, 폴란드에 이어 29번째 가맹국이 되게 된다. 가입 신청을 하여 위원회를 통과한 국가중 이사회에서 부결된 경우가 없었던 경우를 생각해 볼때 우리나라의 OECD 가입은 낙관적이라고 생각된다. 그러나 이러한 OECD 가입이 무역, 노동, 환경, 금융, 시장 개방 등의 경제적인 문제에만 관심이 집중되어 있다. 즉 시장 개방 그중에서도 통신 시장 개방 등에 따른 시큐리티 문제는 전혀 거론되지 않고 있다. 물론 국가적으로 경제나 노동, 환경 문제가 더욱 주요한 사항임에 틀림없다. 그러나 국가의 안보나 공공 또는 개인 정보의 안전에 관련된 시큐리티나 프라이버시 문제도 간과해서는 안된다.

우리나라가 가입하기를 원하는 OECD의 권고는 법적 구속력은 없지만 정치적 또는 도덕적으로 커다란 영향력을 갖고 있다. OECD 권고안중 시큐리티에 관련되어 있는 대표적인 것으로는 OECD 개인정보에 관한 가이드라인과 OECD 정보 시스템의 시큐리티를 위한 가이드라인이 유명하다. 각국에서는 전기통신사업법, 금융관련법 등의 개인 정보에 관한 것이나 전자계산기나 정보시스템의 안전대책 기준의 가이드라인으로 이들 가이드라인인 OECD 프라이버시 8원칙과 OECD 시큐리티 9원칙 등을 기본으로 하여 작성하기 때문에 더욱더 큰 영향력을 가지게 된다. 더욱더 관심이 고조되고 있는 것은 1995년 12월의 모임에서는 미국이 자기나라의 시큐리티 정책인 Key Escrow 정책을 OECD를 통해서 각국과 의견 조정을 거쳐 실현시키려 하고 있는 점이며, 이러한 움직임은 계속되리라 예상되므로 이에 대한 우리나라의 대응도 서서히 준비하여야 할 단계라고 생각한다.

이러한 시큐리티에 관한 국제적인 움직임은 ISO/IEC, OSI 등의 국제적인 표준 활동외에도 OECD를 통하여 활발히 전개되고 있다. OECD는 G7 정상들간에 협의된 내용들을 구체적으로 검토하여 추진하는 실무회의며 가맹국간의 의견 조정을 거쳐 각국의 국내법에 영향을 크게 미치는 탓으로 정치적인 비중이 큰 회의다. OECD의 가입을 눈앞에 둔 우리나라는 OECD내의 각 위원회의 활발한 움직임을 지켜보아야 하며, 특히 시큐리티에 관련이 있는 정보·컴퓨터·통신정책 위원회인 ICCP(Committee for Information, Computer and Communication on Policy)의 활동에 관련 전문가들의 관심이 있어야 할 것이다. 가입이 확정된 후에는 가맹국으로써 의견 제시와 각국의 제안에 대한 우리나라의 실익과 여러가지 제반문제 등을 깊이 고찰해보는 시큐리티 전담반의 구성이, 정부는 물론이고 학계 연구계를 중심으로 시급히 이루어져야 할 것이다.

본 고에서는 OECD의 전문적인 내용은 경제 전문가나 통상 전문가의 몫으로 돌리고 OECD와 프라이버시, OECD와 시큐리티와 관련된 사항만을 집중적으로 발췌하여 소개하고자 한다. 특히 OECD의 ICCP의 활동, OECD Privacy 8원칙, OECD 시큐리티 9원칙을 중심으로 살펴보고자 한다.

본 논문은 7개장으로 구성되어 진행된다.

제2장에서는 OECD의 ICCP위원회의 동향을 다루고, 제3장에서는 OECD 시큐리티 관련 관심 사항이 되고 있는 OECD 시큐리티 전문가 회의에서 미국이 발표한 미국의 최근 시큐리티 정책 동향을 원문 그대로 소개한다. OECD의 프라이버시에 관련된 권고에 대해서는 제4장에서, 그리고 제5장에서는 OECD의 Privacy 8원칙을, 제6장에서는 프라이버시 권고에 대한 각국의 대응 방안을 살펴보기로 한다. 제7장에서는 정보 시스템의 시큐리티에 관련이 있는 OECD의 시큐리티 9원칙을 소개하고자 한다. 마지막으로 제8장에 결론부를 둔다.

2. OECD/ICCP 위원회의 동향[5]

경제협력개발기구(OECD)의 정보·컴퓨터·통신정책(ICCP)위원회는 21개 분야별 위원회 중 시큐리티 분야와 가장 밀접한 위원회다. 이 위원회에서는 정보·컴퓨터·통신에 관한 시스

템 및 서비스 분야에 관해서 기술정책과 그 응용에 관한 정책 문제와 경제적 사회적 영향에 관한 검토를 행하며 OECD 가맹국간의 정책 조정을 추진하고 있다.

OECD에서는 1994년 3월 G7 정상회담에서 논의된 내용을 실무 추진 차원에서, "기술, 생산성 및 고용"을 주제로 다음과 같은 5개의 활동에 관해서 연구 분석을 추진하고 있다.

- 기술·생산성과 고용
- 기술정책의 유효성
- 기술적이며 구조적인 변화와 노동 수요
- 정보 인프라 구축
- 새로운 성장 산업

이 가운데에서 ICCP 위원회에서는 정보 인프라 구축을 담당하고 검토를 추진하고 있다. 또한 OECD는 1995년 2월에 개최된 정보사회에 관한 관계 장관 회의에서 거론된 제반 과제에 대해서도 ICCP 위원회가 중심적 역할을 담당하며, 다른 관련 국제기관과의 협조를 통해서 업무를 추진해 나갈 것으로 기대되고 있다.

표 1은 1994년 OECD의 ICCP 위원회가 한 햇동안 활동한 주요 활동 상황을 정리한 것으로 ICCP 위원회의 성격을 이해하는데 참고가 될 것이다. 표 1에서 알 수 있듯이 1994년 11월 30일 부터 12월 2일까지 개최된 정보 인프라에 있어서 시스템 안전성 및 개인 데이터 프라이버시 보호에 관한 전문가 회의는 정보 시스템 시큐리티 및 개인 데이터·프라이버시, 지적 재산권 보호를 정보 인프라 운용시점에서 검토하고 암호화의 효용과 정부의 역할 등을 논의한 회의로 이 분야에서의 OECD 가맹국의 의견 조정을 하는 것으로 시큐리티와 직접적인 관계가 있는 회의다.

1995년에는 OECD가 처음으로 Security Policy를 주제로 선정하는 등 국제 사회에 있어서의 시큐리티 관심도를 더욱 높였다. 1995년 2월에 개최된 정보사회에 관한 관계장관회의에서 논의된 내용을 ICCP가 주도적으로 처리하는 활동외에도 시큐리티와 프라이버시에 관한 영향력이 큰 모임이 1995년 12월 18일부터 19일에 걸쳐 개최된 Ad hoc Meeting of Experts on Cryptography Policy OECD가 있었다. 이 모임에서는 미국의 Key Escrow 정책과 암호 관련 수출입 통제에 대한 내용이 주된 관심사가 되었다. 이 모임에서 미국 대표가 발표한 내용을 다음장에 소개하기로 한다.

3. OECD에 대한 미국의 최근 시큐리티 정책

1995년 12월 18일 부터 19일 양일간에 걸쳐 개최된 암호전문가회의인 Ad hoc Meeting of Experts on Cryptography Policy에서 미국의 대표로 참석한 대통령 특별 보좌관인 M. Nelson이 발표한 내용을 원문 그대로 소개한다. 이 모임에서 미국 대표는 개인의 프라이버시를 제공하는 암호 대책을 제공하기 위해서라는 목적으로 미국의 암호에 관한 기본정책, 암호 정책 그리고 Key Escrow 정책에 대한 내용들을 소개하였다. 미국은 Key Escrow 정책을 국제 사회에 통용시키려 하는 의도가 다분히 내재되어있는 내용으로 이 모임의 주된 관심사가 되고 있다. 그러나 유럽은 미국의 이러한 정책과는 다소 다른 T.T.P(Trusted Third Party) Certificate 정책을 추진하여 미국의 비밀 분산 정책과는 다소 상반된 중앙 집중 형태를 고려하고 있다. 그러나 미국은 그들의 정책을 유럽에 대해서도 계속해서 주입시키려 할 것으로 보인다. 이에 반해 최근에 이 모임에 참여하게 된 일본은 국내의 정책이 마련되지 않아 현재 정책 수립을 위한 대책을 서두르고 있는 실정이다. 비공식적인 내용이지만 일본은 미국의 Key Escrow 정책을 검토하여 이를 수용한 것으로 추정된다. 다음은 미국 대표가 발표한 원문 내용 그대로이다.

The Goal

To provide users with global encryption solutions they can trust to protect their privacy and corporate secrets

The Challenge

To find encryption solutions that do not unnecessarily hinder the ability of law enforcement and intelligence agencies to do their jobs

Interested Parties

Individuals(who want privacy protction), Law enforcement, Intelligence agencies, Corporate users, Computer hardware and software vendors, Government agencies (as users)

Fundamental of U.S. encryption policy

- No controls on domestic use of import of encryption products
- Mass market encryption software with key length of up to 40 bits can be easily exported
- Other products may be exported depending on strength of the algorithm and end users

How does the U.S. Develop Cryptographic Policy?

- Prior to 1993, policy was developed by ad hoc groups, normally through the National Security Council mechanisms.
- In 1993, a working group was informally established to study cryptographic policy and telephony access issues. It recommended the formation of a standing organization to address these issues, and provide government representation from national security, law enforcement, user and industry focused agencies.
- In 1994, the informal group was renamed and formalized as the U.S. Interagency Working Group on Encryption and Telecommunications.

Who's involved?

- Department of Commerce(NIST, BXA)
- Department of Defense(NSA)
- Department of Justice
- Department of State
- Department of Treasury
- Federal Bureau of Investigation
- Central Intelligence Agency
- National Economic Council
- National Security Council
- Office of Management and Budget
- Office of Science and Technology Policy

History of U.S. encryption policy

- 〈1983 All cryptography products required State Dept. licenses
- 1983 Commerce Dept. licenses for certain cryptography products
- 1992 Commerce Department licenses for 40 bit encryption
- 1993 Clipper Chip standard announced for telephone encryption
- 1995 Key escrow encryption initiative

A U.S. Historical Perspective on Key Escrow

- 1980s Growing commercial pressure for exportability of encryption products
- Growing recognition among government officials of the potential threat to national security and law enforcement of encryption.
- (1992 40 bit RC2/4 w/512 bit modules areement for export)
- 1993 April 16, 1993-Key Escrow Chip unveiled.(Clipper/Capstone)
- Government stresses voluntary nature of chip use and offers to work with industry on developing alternative approaches.
- Criticized-hardware, classfied algorithm, government agents, will be made mandatory
- Public discussion.

- 1994 Vice President Gore states goal of developing a system that would be implementable in software, not rely upon a classified algorithm, would be voluntary, and be exportable.(7/20/95)
- Open NIST meetings held with industry on developing alternatives. Key question raised: Would wide exportability be permitted for key escrow with strong encryption? Need for international solution identified.
- Industry develops other approaches, specifically focusing on commercial key recovery

표 1 OECD의 ICCP 위원회의 1994년도 주요 활동 상황

회 의 명	기 간	개 요
중동에 있어서의 상호접속 및 Equal Access에 관한 작업	1994. 1.27 - 1.28	중동의 전기통신 현황 및 경쟁 도입의 시비, OECD 가맹선진국의 현황 소개
ICCP 제 25회 회의	3.14 - 3.16	전기통신정책의 새로운 전개에 관한 각국의 보고, 1995 - 1996년 작업 계획 책정, 정보기술관련 활동이나 TISP 활동 수반
DSTI(과학기술산업국)/3 위원회 합동회의	3.17 - 3.18	산업위원회(IND), 과학기술정책위원회(CSTP), ICCP 합동으로 G7협의 내용을 긍정적으로 추진
TISP(전기통신 및 정보 서비스 정책 관련 작업) 제13회 회의	6.13 - 6.14	국제통신에 있어서 인프라 경제에 관한 각국의 의견을 청취하고, 경쟁 이익 등에 관해서 검토
국제계산요금제2회 전문가 회의	6.15 - 6.16	대체통화수단, 국제단순재판등에 대한 계산 요금 및 수납요금에의 영향을 각국 보고 검토
기술, 생산성 및 고용에 관한 제1회 3위원회 전문가 회의	6.28 - 6.29	생산성 향상, 고용 창출과 기술(특히 정보기술)관련, G7 고용정상회담으로 검토 요청을 받고 OECD 검토 결정
전기통신인프라경쟁에 관한 작업	9.19 - 9.20	전기통신시장에 있어서 인프라 경쟁의 성과에 대한 이해를 구하고 인프라 경쟁도입시 정책 유의점을 검토
EDI의 경제적 의미에 관한 회의	9.28 - 9.29	EDI에 관해서 유익한 점과 문제점 파악, OECD 및 각국의 금후 대응검토
ICCP 제26회 회의	10.24 - 10.26	1995년 4월의 정보인프라 특별세션 개최 제안, 위원회 조직 변경제안 등 검토
지식집약화경제에 있어서 고용과 성장회의	11.7 - 11.8	정보기술로 대표되는 신기술의 경제의 영향분석, 정보 인프라를 포함 4개의 작업 검토
기술, 생산성 및 고용에 관한 2회 3위원회 합동전문가회의	11.7 - 11.9	G7 고용서미트의 요청을 받은 각 활동의 진도 보고 및 금후의 작업 예정 토의
정보인프라에 있어서 시스템 안전성 및 개인 데이터 프라이버시 보호에 관한 전문가회의	11.30 - 12.2	정보 시스템 시큐리티 및 개인 데이터, 프라이버시, 지적 재산권 보호를 정보 인프라 운용시점서 검토, 암호화의 효용, 정부 역할 논의
TISP 제14회 회의	12.6 - 12.7	전기통신분야에 있어서 고용문제에 대한 각국의 보고를 검토 · 변호정책과 광대역 통신망 논의

4. OECD의 프라이버시 권고[4]

유럽에 있어서는 1970년대에 프라이버시법·데이터법이 계속해서 제정되어 왔지만 이들 중에는 개인 데이터의 국외처리를 제한하는 조항들이 있다. 이러한 조항들은 자국민의 프라이버시 보호에는 도움이 되지만 다른 측면에 있어서는 국가간의 정보의 자유로운 흐름을 방해하는 요인이 된다. 또한, 제한조항이 없다할 지라도 프라이버시 보호 내지 데이터 보호를 목적으로 하는 법률은 데이터의 국외처리를 저해하는 요인이 될 것이다. 그럴지라도 제한조항을 둔 법률의 제정국이 유럽에 집중되어 있다.

이러한 사실은 정보 산업에서 압도적인 우세를 점하고 있는 미국에 있어서는 커다란 위협이 되어 왔다. 미국에서는 전세계적인 규모의 통신 네트워크이 존재하며 그 소유주인 기업은 네트워크를 통해서 유럽 시장을 석권하려 하고 있다. 이때문에 프라이버시 보호법은 거꾸로 미국의 경제적 이익을 침해하는 위험성을 갖고 있어 미국과 유럽간의 이해관계가 대립되게 되었다.

이러한 이해 대립의 조정에 나선 곳이 OECD다. OECD는 1978년 처음으로 "국제 데이터 장해와 프라이버시 보호 전문가 그룹"이라는 새로운 Ad hoc 그룹을 설치하여 개인 데이터의 국제 유통과 개인 데이터 및 프라이버시 보호에 관한 기본적인 규칙에 관한 가이드라인을 작성하도록 지시하였다.

OECD는 이 전문가 그룹의 작업을 기본으로 1980년 9월 23일에 "프라이버시 보호와 개인 데이터의 국제 유통에 대한 가이드 라인에 관한 이사회 권고"(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)를 채택했다. 또한 이사회는 가맹국간의 정보의 자유로운 유통을 촉진하고 가맹국간의 경제적 사회적 관계의 발전에 대한 부당한 장해의 창설을 회피하도록 한다라는 내용을 결의하고 다음과 같이 권고하였다.

- 가맹국은 본 권고의 주요 부분인 권고 부속 문서의 가이드 라인에 열거되어 있는 프라이버시와 개인의 자유 보호에 관한 원칙을 자국의 국내법에 반영한다.
- 가맹국은 프라이버시 보호의 명목으로 개인 데이터의 국제 유통에 관한 부당한 장해를 만드는 것을 제거 또는 회피하도록 노력한다.
- 가맹국은 권고 부속 문서에 열거된 가이드 라인의 이행에 협력한다.
- 가맹국은 이 가이드 라인을 적용하기 위해 특별한 협의나 협력의 절차에 대해서 가능한 한 빨리 동의한다.

또한 이 기본 원칙인 8원칙은 OECD의 개인 정보 보호에 관한 유명한 원칙이 되었다.

5. OECD Privacy 8원칙[1]

통신 기술과 컴퓨터 기술의 발전을 배경으로서, 1970년대 부터 유럽을 중심으로 프라이버시 보호 문제가 거론되어, 1973년 국가레벨에서는 개인 정보 보호에 관한 법률인 데이터법이 스웨덴에서 제정되었다. 그후 각국에서 법제정화가 진행되고 있던 중, 개인 데이터의 자유로운 국제 유통과 개인 정보 보호 사이의 조정을 도모하기 위하여, OECD는 1978년에 개인 데이터와 프라이버시 보호와 국제 유통을 조정하는 기본 룰에 관한 검토를 시작하여 1980년 9월, "프라이버시 보호와 개인 데이터의 국제 유통에 관한 가이드 라인에 관한 이사회 권고"를 채택하였다. 이사회 권고인 이 문서는 제1부 총칙, 제2부 국내 적용에 있어서의 기본 원칙, 제3부 국제 적용에 있어서 기본

원칙, 제4부 국내 실시 그리고 제5부 국제 협력으로 구성되어 있다. 이중에서 제2부인 국내 적용에 있어서의 기본 원칙이 각국에 있어서의 프라이버시 보호를 고려하는데 중요하며 8개의 프라이버시 보호 원칙으로 되어 있다. 이 OECD 프라이버시 8원칙은 그후 각국의 개인 정보나 프라이버시 관련 법제도, 가이드 라인 등의 모델이 되었으며 각국의 공공 부문이나 민간 부문에 광범위하게 받아들여지게 되었다.

개인 정보에 관한 국제적인 움직임인 OECD 개인 정보에 관한 이사회 권고중의 국내 적용에 관한 8원칙은 수집 제한의 원칙, 정보 내용의 원칙, 목적 명확화의 원칙, 이용 제한의 원칙, 안전 보호의 원칙, 공개의 원칙, 개인 참가의 원칙, 책임의 원칙으로 되어 있으며 그 자세한 내용은 표 2와 같다.

표 2 OECD 프라이버시 8원칙

원 칙	개 요
수집제한의 원칙 (Collection Limitation Principle)	개인데이터의 수집에 제한을 두어야 하며 개인 데이터 수집 방법은 적법하며 공정한 수단에 의해 행하도록 하여야 한다. 경우에 따라서는 정보주체에 알리거나 동의를 구하여야 한다.
정보내용의 원칙 (Data Quality Principle)	개인데이터는 그 이용목적에 따라야 하며 이용 목적에 필요한 범위내에서 정확, 안전 그리고 최신의 것을 가져야만 한다.
목적 명확화의 원칙 (Purpose Specification Principle)	개인데이터의 수집 목적은 수집시 보다 늦지 않는 시점에서 명확화되어야 하며 그후의 데이터 이용은 해당 수집 목적의 달성 또는 수집 목적에 모순되지 않도록 하며 목적의 변경시에 명확화된 다른 목적의 달성에 한정해야만 한다.
이용제한의 원칙 (Use Limitation Principle)	개인데이터는 명확화된 목적이외의 목적을 위해서는 데이터 주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 공개나 이용 그외의 사용에 대해서는 금지되어야 한다.
안전보호의 원칙 (Security Safeguards Principle)	데이터는 분실 또는 부당한 접근, 파괴, 사용, 수정, 공개의 위험에 대해서 합리적인 안전보장 조치에 의해 보호되지 않으면 안된다.
공개의 원칙 (Openness Principle)	개인데이터에 관한 개발, 운용 및 정책에 관해서는 일반적인 공개 정책이 취하여지지 않으면 안된다. 개인데이터의 존재, 성질 및 주요목적과 함께 데이터 관리자의 식별, 통상의 주소를 분명히 하기 위한 수단이 쉽게 이용될 수 있도록 하여야 한다.
개인참가의 원칙 (Individual Participation Principle)	개인은 다음 4가지 권리를 가진다. 1. 데이터 관리자는 자기 데이터 유무를 확인할 수 있다. 2. 자기 데이터를 알 수 있다. 3. 1또는 2가 거부되었을 경우는 사유를 들을 수 있다. 4. 자기 데이터에 관한 이의 신청이 인정될 경우는 데이터를 소거, 수정, 완전화, 교정할 수 있다.
책임의 원칙 (Accountability Principle)	전기통신분야에 있어서 고용문제에 대한 데이터 관리자는 상기의 원칙을 실시하기 위한 조치에 책임을 가진다.

6. OECD 프라이버시 권고에 대한 각국의 대응[4]

OECD의 프라이버시에 관한 가이드 라인에 대해서 각국은 어떻게 대응하고 있을까. 결론적으로 가맹국들은 대부분 가이드라인을 기준으로 국내법에 반영하고 있는 것 같다. 여기서는 미국, 유럽 그리고 일본을 중심으로 이사회 권고에 대한 각국의 대응을 살펴 보기로 한다.

6.1 미국의 대응[3][4]

미국에 있어서는 연방 행정 기관에 대해서는 1974년에 제정된 프라이버시법에 의한 규제가 행하여 지고 있지만, 민간 부문에 대해서는 개인의 신용 정보 보호법 등에 의해 개별적으로 법적인 조치가 갖추어져 있다.

또한, NII의 구축에 있어서 개인 프라이버시를 보호하기 위한 정책의 존재나 사용자의 정당한 권리와 모순되지 않는 NII의 운영을 위해서 정보 기반 Task Force(IITF) 내의 정보 정책 위원회의 3개 Working Group 중의 하나로 설정된 프라이버시 Working Group이 1995년에 가이드 라인을 발표했다. 이 가이드 라인은 "프라이버시와 NII : 개인 정보의 제공 및 이용 원칙"으로 최종 정리되어 있다. 이것의 특징은 NII상의 정보 프라이버시와 정보 프라이버시 보호를 위해, 개인 정보의 기밀성(Confidentiality) 및 무결성(Integrity) 또는 경우에 따라서는 익명성(Anonymity)을 목적으로 암호화 등의 기술적 조치를 취한다는 점이다. 물론 이 가이드 라인의 내용은 OECD 프라이버시 8원칙을 근거로 하고 있다.

6.2 유럽의 대응

유럽에 있어서는 1970년대부터 각국에 있어서 개인 정보 보호를 위한 입법 조치가 되어 왔지만 대부분은 공공 부문이나 민간 부문 양쪽을 대상으로 하는 입법 조치가 되어 있다. 또 민간 부문에 있어서 개인 정보의 축적에 관해서 벌칙 등에 의한 강제력이 있는 등록 제도 등을 두어 개인 정보 보호를 담당하는 전문부국이 운용하는 것이 통례가 되고 있다.

1990년에 "개인 데이터 처리에 관한 개인의 보호에 관한 이사회 지령 제안"을 제출하였으며, 1992년에는 수정안이 제출된 후 최종안의 조정을 거쳐서 EU(European Union) 이사회는 1995년 EU 개인 보호 지령을 최종적으로 채택하였으며 전기통신 분야에 특유한 전기통신 프라이버시 지령 제안도 별도로 이사회에 제출되어 1994년 수정안이 제출되어 있는 단계다. 유럽에서는 개인 정보의 충분한 레벨의 보호를 위한 의도가 많이 내포되어 있으며 역시 OECD의 이사회 권고를 고려하고 있다.

6.3 일본의 대응

일본의 대응은 민간 부문, 행정기관 그리고 지방 공공 단체마다의 대책이 있다. 먼저 민간 부문에서는 1987년 금융 정보 시스템 센터(FISC)가 OECD 가이드라인을 받아들여 "금융기관 등에 있어서 개인 데이터 보호를 위한 취급 지침"을 정하였고 1988년에는 일본정보처리개발협회(JIPDEC)가 "민간 부문에 있어서 개인 정보 보호를 위한 가이드 라인"을 책정하고 있다. 이들 가이드 라인은 모두 OECD의 가이드 라인에 대응하여 만들어져 있다. 국가의 행정 기관이 보유하고 있는 개인 정보에 대해서는 OECD 가이드 라인 등을 따라서 "행정 기관 보유 전자계산기처리에 관한 개인 정보의 보호에 관한 법률"을 1988년 제정하였다. 1994년에는 지방 공공 단체가 개인 정보에 관한 조례를 제정하고 있다.

7. OECD 시큐리티 9원칙[4]

주로 본 논문에서는 OECD와 프라이버시에 대해서만 논하였지만 마지막장에 OECD의 정보 시스템의 시큐리티에 관한 이사회 권고를 첨부하였다. 1988년 OECD의 ICCP 위원회는 OECD 사무국이 정보 시스템의 시큐리티에 관한 보고서를 작성하는 것을 승인했다. 정보네트워크 시큐리티로 명명된 이 보고서는 1989년 10월에 ICCP 위원회에 제출되었다. 이 위원회 문서의 재검토에 따라, ICCP 위원회는 전문가를 소집해서 회의를 열어, 보고서에서 제기된 문제점을 찾아내도록 지시했다. 전문가들의 보고에 따라 ICCP 위원회는 1990년 3월에 전문가 그룹에 의한 정보 시스템 시큐리티에 관한 가이드 라인 초고 작성을 승인했다. 이 회의에 참가한 사람은 정부 대표자, 법률, 수학 및 컴퓨터 과학 연구자, 게다가 컴퓨터나 통신에 관련된 제품이나 서비스 제공자 및 사용자를 포함한 민간 부문의 대표 등으로 되어 있다. 전문가 그룹은 시큐리티에 관한 기본적인 생각을 국제적으로 통일하고 각국에 있어서의 시큐리티 관련시책의 실시나 시큐리티에 관한 국제 협력 등을 촉진하기 위한 목적으로 1991년 1월부터 1992년 9월까지 6회의 회의를 거쳐 1992년에 "정보시스템의 시큐리티를 위한 가이드라인"을 채택하였다.

OECD 시큐리티 가이드라인은 각국의 공적기관 및 사기업을 대상으로하며, 정보시스템의 시큐리티를 확보하기 위한 법률, 행정, 규칙, 수속 기타의 대책의 실시에 관한 원칙을 9개항으로 나누어 정리하고 있으며 강제력은 갖고 있지 않다. 표 3은 9개항에 대한 내용을 정리한 것이다.

표 3 OECD 시큐리티 9원칙

원 칙	개 요
책임원칙 (Accountability Principle)	정보시스템의 소유자, 제공자, 이용자 그외 정보 시스템 시큐리티에 관한 자의 임무 및 책임을 명확히 하여야 한다.
주지원칙 (Awareness Principle)	정보시스템의 신뢰를 높이기 위해 정보 시스템의 소유자 제공자, 이용자 그외 관계자는 시큐리티 유지와 모순이 없도록 정보시스템 시큐리티를 위한 수단, 관행 및 수속의 존재 그리고 범위에 관해서 쉽고 적절한 지식을 얻을 수 있도록 하여야 하며 알려주어야 한다.
윤리원칙 (Ethics Principle)	정보시스템 및 정보 시스템 시큐리티는 다른 자의 권리와 합법적인 이익을 존중하여 제공되어 이용될 수 있도록 하여야 한다.
다면적사고원칙 (Multidisciplinary Principle)	정보시스템 시큐리티를 위한 수단, 관행 및 수속은 기술, 행정, 조직, 운영, 영업, 교육 및 법률을 포함 그 문제에 관련된 여러가지 생각이나 시점을 고려하여야 한다.
비례원칙 (Proportionality Principle)	데이터는 분실 또는 부당한 접근, 파괴, 사용, 시큐리티의 요구는 개개의 정보시스템마다 다르므로 시큐리티의 레벨, 비용, 수단, 관행 및 수속은 적정하며 정보시스템의 가치가 요구되는 신뢰도, 시큐리티가 파괴되었을 경우의 피해의 심각도, 발생의 가능성, 범위에 비례하는 것이어야 한다.
통합성원칙 (Integration Principle)	정보시스템 시큐리티를 위한 수단, 관행, 수속은 일관되게 시스템 시큐리티 창출을 위해 상호간에 그리고 조직내의 다른 수단, 관행 및 구속과 조화있게 통합적으로 행하여져야 한다.

즉시성원칙 (Timeliness Principle)	정보시스템의 시큐리티에 대한 침해를 방지하고 동시에 그것에 대응하기 위한 공공부문 및 민간 부분은 국내 국제 레벨에 불구하고 시의 적절히 협조적으로 행동하여야 한다.
재평가원칙 (Reassessment Principle)	정보시스템 및 그것에 대한 시큐리티 요구는 시간에 따라 변하기 때문에 정보시스템 시큐리티는 정기적으로 재평가되어야 한다.
민주제 원칙 (Democracy Principle)	정보시스템 시큐리티는 민주주의 사회에 있어서 데이터와 정보의 합법적인 이용 및 유통과 정합을 취한 것이어야 한다.

8. 결 론

우리나라의 OECD 가입 신청을 계기로 프라이버시와 시큐리티 분야에 있어서의 국제적인 움직임을 잘 파악하여 국내 대응 방안을 마련하고 이 분야 관련 전문가들의 관심을 높이고자 본 자료를 정리하여 보았다. 우리나라에도 공공 기관의 개인 정보 보호에 관한 법률이 최근 제정되었으며 개인 정보 보호에 대한 많은 연구도 이루어지고 있다. 그러나 무역 개방과 함께 쏟아져 들어올 시큐리티 산업, 그리고 OECD 가입에 따른 국제적인 움직임 등을 미리 파악하여 국내 규정 제정 및 적절한 조치를 통해서 국내 정책에 반영시키거나 국제 정책 수립 협력을 위해 정부, 연구계, 학계, 산업계 등의 관심과 참여가 필요하다고 생각된다.

참 고 문 헌

[1] M. Horibe, 프라이버시와 고도 정보화 사회(in Japanese), 판암신서, 1995.

[2] 이선화, 박기식, 신범철, "우리나라 정보 보호 관련법규의 현황과 개선 방향", 통신정보보호학회 학회지, 제5권, 제2호, pp.5-25, 1995.

[3] The Office of Technology Assessment, Information Security and Privacy in Network Environments, 1994.

[4] 일본정보처리개발협회(JIPDEC), 시큐리티·프라이버시 문제 검토 중간 결과 보고서(in Japanese), 1995.

[5] 일본 우정성, 통신백서'95, 1996.

□ 著者紹介

박 춘 식(정회원)

광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구소 책임연구원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론