情 報 保 護 學 會 誌
第 15 卷 第 2 號, 2005. 4

국내외 암호관련 법제도 현황

권 현 조*, 전 길 수*, 이 재 일*

요 약

정보통신환경발달과 함께 지식사회에서 암호의 역할이 증대됨에 따라 OECD의 암호정책가이드라인 공표를 시점으로 각 국은 자국의 실정에 맞는 새로운 암호정책을 세우고 이에 따른 법·제도를 정비하기 위해 본격적인 노력을 기울여오고 있다. 하지만 암호는 개인의 프라이버시를 보호할 수 있는 가장 유용한 수단인데 반해 암호의 범죄이용 등으로 인한 국가의 안녕과 법질서 혼란을 초래할 수 있다는 역기능도 상존하고 있다. 각 국의 정부는 이러한 우려 때문에 암호이용을 제한적으로 규제하려는 정책을 시도하여 왔으나 시민단체의 반대에 부딪쳐 암호의 자율이용 원칙과 국가의 합법적 통제제도의 균형을 맞출 수 있는 암호정책을 세우는데 고심하고 있다. 본 고에서는 미국, 영국, 프랑스, 중국 등 주요 국가를 중심으로 암호이용을 활성화하고 암호의 역기능을 방지하기 위해 세운 암호정책 및 암호이용 관련 법제도 현황을 살펴보았다.

Ⅰ. 서 론

암호는 인터넷 및 이동통신 서비스의 보급으로 이에 기반한 경제 활동이 증가하면서 전자거래의 안전성·신뢰성 및 프라이버시보호를 위한 핵심기술로 자리잡고 있다. 현재 암호는 전자금융거래, 사이버증권거래, 전자입찰, 전자화폐, 위성방송 등에서 광범위하게 활용되고 있으며 또한 지적재산권 보호를 위한 심층암호방식(Steganography), 개인정보보호를 위한 익명성 보장기술 등을 통해 그 활용분야가 한층 더 확대되고 있다. 인터넷 쇼핑몰 등에서 신용카드 결제시, 고객의 신용카드 번호와 비밀번호 등 주요 금융정보가 전송될 때 SSL 암호통신 프로토콜이 사용되고 있다. 또한 최근 금융권과 이동통신사가 연계하여 서비스 중인 모바일 금융서비스에서도 휴대폰에 SEED나 3-DES 등이 내장된 암호칩을 탑재하여 금융거래 암호통신을 지원할 수 있도록 하고 있다. 이외에도 디지털 컨텐츠 산업이 발달하면서 디지털 컨텐츠 유료서비스 사업자들은 디지털 컨텐츠를 암호화함으로써 대가를 지불한 고객만이 디지털 컨텐츠를 열람할 수 있도록 하고 있다. 실제로 EBS 영어 교육방송와 연계 하고 있는 에듀엔피쓰리닷컴은 "넷싱크 브라우저라"는 학습용 교육 프로그램을 제작하여 배포하고 있다. 서비스 이용자는 넷싱크 브라우저를 먼저 설치하고 mp3파일을 다운받고자 하는 mp3 플레이어를 등록한다. 이러한 사전준비 과정이 끝나면 원하는 EB$ 강좌를 신청하고 대가를 지불하고 나면 해당 EBS 강좌의 암호화된 mp3 파일을 넷싱크 브라우저를 통해 다운받게 된다.

이와 같이 암호는 우리가 생각하는 것보다도 훨씬 우리 실생활에 가깝게 다가와 있는 것이 현실이다. 하지만 암호서비스나 제품의 취약성에 대응할 수 있는 체계가 미흡하여 일반인이 취약한 암호서비스 및 제품 사용으로 인한 피해에 효과적인 대처가 어렵다. 암호서비스 및 제품 제공자들의 책임과 역할을 제고하고 암호 이용자가 암호제품 및 서비스를 안전하게 이용할 수 있는 제도적 방안마련이 필요한 시점이다.

미국 등 선진 암호기술력을 갖춘 나라들은 암호기술·산업을 한 나라의 정보주권 확립에 필요한 전략산업으로 인식하고 암호기술 개발 및 암호산업 육성에 총력을 기울이기 위해 국가차원의 총체적인 암호정책

* 한국정보보호진흥원 ({hckwon, kschun, jilee}@kisa.or.kr)

을 수립하고 있다.

본 고에서는 미국을 비롯한 영국, 프랑스, 중국 등 주요국가의 암호관련 법제도 및 정책 현황에 대해 살펴보고 우리나라 암호정책의 현황을 파악하여 각국의 암호관련 법제도 현황을 비교해 보고자한다.

II. 암호관련 국제정책

암호는 국가기밀 유지차원에서 이용하는 형태였기 때문에 국제적인 논의나 통일적인 정책방향이라는 것이 없었으며 오히려 암호와 관련된 모든 사항 자체가 국가기밀로 다루어졌었다. 하지만 정보통신환경의 발달로 암호의 이용이 민간영역으로 확대됨에 따라 1990년대 중반 이후부터 암호와 관련된 국제적 논의가 이루어지기 시작하였다. 암호이용에 관한 국제적 논의의 시작은 암호기술의 수출통제와 관련하여 암호개발 업체와 정부의 상호갈등에서 출발하였고 특히, 암호의 선진기술력을 갖춘 미국에서 의무적 키복구제도 도입을 시도하면서 그 논의가 더욱 활발해지는 계기가 되었다. 의무적 키복구제도란 암호문의 생성 및 복호를 위해 필요한 암호키를 소유한 자는 국가기관 또는 국가가 지정한 기관에게 무조건 위탁하여 관리토록 하는 제도를 뜻한다.

본 절에서는 OECD 암호정책 가이드라인과 바세나르 협정의 주요내용에 대해 기술한다.

2.1 OECD 암호정책

1997년에 OECD는 암호정책의 기본방향인 암호이용의 신뢰도 제고, 암호의 자율적 선택보장, 시장주도형 암호개발 등 다음과 같이 8가지 원칙을 가이드라인으로 제정하였다[1].

① 암호이용의 신뢰도 제고 : 암호이용활성화제도, 암호평가제도 등 암호의 신뢰도 제고를 위한 국가정책 마련

② 암호의 자율적 선택 보장 : 이용자의 정보보호 수준에 따라 자유로이 암호를 선택하여 이용할 수 있는 암호 자율이용 원칙

③ 시장주도형 암호개발 : 국가통제가 아닌 시장의 수요와 공급의 원칙에 따른 암호개발 보장과 민간의 암호개발을 위한 정부의 지원체계 마련

④ 암호기술의 표준화 : 암호의 기술표준, 평가기준 등을 개발하여 제정하고 표준적합성, 안전성 평가 등의 결과를 활용을 촉진할 수 있는 제도 마련

⑤ 개인정보 및 프라이버시 보호 : 암호는 프라이버시 보호를 위한 기술적 중요수단이므로, OECD의 "프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침"을 준수하여 국가 암호정책을 수립

⑥ 정부의 합법적 접근권 보장 : 암호가 범죄에 악용되었을 경우 암호문에 해당하는 평문 또는 암호키에 대한 정부의 합법적 수사권을 부여하는 것은 각국의 현황을 고려하여 정할 것을 권고

⑦ 암호서비스 사업자의 책임규정 : 암호서비스 사업자와 가입자 모두가 키를 안전하게 관리할 의무가 있으며 정부의 합법적 접근권을 인정하며 따라야 함

⑧ 국제협력 증진 : 암호제품수출규제가 무역장벽이 되지 않도록 암호수출 정책 수립

이는 과거 군사기밀의 위한 암호에서 민간의 전자정보 보호를 위한 암호로 그 가치가 변화되었음을 공식적으로 천명함으로써 민간 주도형 암호기술을 연구개발 하여 자유로이 상품화할 수 있는 여건을 조성하였다고 평가받고 있다.

2.2 바세나르 협정

전략물자 및 암호품목/기술이 위험국가로 수출되는 것을 금지하기 위하여 대(對)공산권 수출통제를 담당하던 다자간 수출통제 조정위원회인 COCOM (Coordination Committee for Multilateral Export Controls)이 1991년 동서냉전의 종식에 따라 1994년 3월에 해체되었다. COCOM의 대부분 회원국들은 새로운 조약문에 서명하면서 암호품목을 계속적으로 수출통제목록에 포함시키자는 원칙에 합의하였다. 이것이 1996년에 제정된 바세나르 협정이다.

바세나르 협정은 상용무기와 이중용도품목의 수출을 통제하기 위한 다자간 국제수출통제체제이다. 바세나르 협정은 상용무기와 이중용도품목 및 기술의 불법축적 방지를 위해 그 이전에 대한 투명성과 책임을 강화함으로써 국제안보 및 지역안정에 기여하기 위해 성립되었다. 여기서 이중용도품목이란 군사목적과 일반시민을 위한 목적으로 모두 사용할 수 있는 품목으로 암호제품 및 기술도 이중용도품목에 속한다. 바세나르 협정에서 암호품목에 관해서는 GSN(General S/W Note)의 Category 5 Part 2에 명시되어 있다. 한국, 미국, 캐나다, 영국, 프랑스 등 33개국이 회원국으로 가입하였다. 통제품목의 이전 또는 거부의 결정은 각 회원국의 고유권한이며, 동 협정을 통해 규정된 조항은 자국내 법체제에 따라 자국의 상황에 맞도록

이행되게 된다 [2].

우리나라의 경우 대외무역법률 및 시행령에 근거하여 산업자원부가 지침으로 제정한 "전략물자수출입공고"에 바세나르 협정의 조약내용이 포함되어 있다 [3].

정보통신기술의 발전에 따라 바세나르 협정의 내용에 반영하여 이중용도품목에 대한 수출제도를 유연하게 운영할 수 있게 하였다. 이를 위해 2년마다 회원국간의 회의를 통해 바세나르 협정을 개정하기로 하였다. 1998년과 2000년에 암호에 관한 사항이 개정된 바 있다. 1998년에는 설계/변형이 불가능하며 제조업체의 기술지원 없이 구매자 스스로 설치 및 사용이 가능한 암호품목(대량 판매용 암호품목)에 한해 64비트 이하 S/W 및 H/W(암호관련 시스템 장비, 모듈, IC, 전용부품 등)의 수출이 자유화되었다. 또한 암호기능이 있는 스마트카드, 유료 TV 수신료 지불에 관련된 정보송수신 목적으로 전용 설계된 암호품목, 저작권 보호를 위해 복사방지 목적의 암호, 은행업무와 금전거래에만 한정된 전용 암호장비 등에 대한 수출은 더 이상 통제하지 않기로 하였다. 이외에도 기밀성을 위한 암호를 이용하기 위하여 설계 또는 개조된 것 중에서 대칭키 암호알고리즘으로 키길이가 56비트 이하인 것, 비대칭키 암호알고리즘으로 키길이가 512비트 이하인 것도 수출이 자유화되었다. 하지만 이들의 키길이를 초과하는 것들은 이때까지도 수출통제 대상이었으며, 이외에도 암호분석 장비, 도청을 탐지하기 위해 설계되거나 변형된 통신케이블 시스템 등 국가 안보에 민감한 사항들은 수출통제 대상으로 남아 있었다.

2000년에는 대량 판매용 암호품목에 한해 64비트 이상의 암호통제에 관한 조항을 삭제함으로써 대량 판매용 암호품목에 대한 수출은 키길이에 상관없이 완전히 자유화되었다. 즉, 다음의 조건에 모두 해당하는 것이 암호품목은 키길이에 상관없이 수출규제 대상에서 제외된다.

① 다음 중 어느 하나에 의해서 규제없이 대중적으로 소매상에서 구입가능한 것
: 상점(소매상)에서 소비자가 직접 구입할 수 있는 것, 일반우편판매 물품, 전자우편판매 물품, 전화판매 물품

② 암호기능들이 사용자에 의해 쉽게 변경될 수 없는 것

③ 사용자가 제품공급자의 추가 도움 없이 설치할 수 있는 것

④ 제품이 상기 ①~③에 해당되는 것을 증명하기 위하여 수출국 해당기관에 제품에 대한 구체적 자료가 제출될 수 있는 것

Ⅲ. 주요국가의 암호정책 및 법제도 추진 현황

본 절에서 기술한 주요국가의 암호정책 및 법제도 추진현황은 2002년에 발간된 OECD 보고서와 암호학자인 Koop가 조사하여 웹에 게시하는 나라별 암호정책 동향의 내용을 중심으로 한 것이다 [4,5].

3.1 미국

3.1.1 암호정책 기본방향

미국은 지금까지의 세계경제에서의 미국의 위상을 확고히 하기 위해서는 암호기술의 발전을 선도하는 미국 기업이 세계시장에서 암호기술의 경쟁력 우위를 지속할 수 있도록 정부의 정책이 필요하다고 판단하고 있다. 이에 따라 1999년 9월 국방부, 재무부, 법무부 및 상무부가 공동으로 작성하여 클린턴 대통령에게 제출한 "Preserving America's Privacy and Security in the Next Century" 보고서를 통해 암호정책의 기본방향을 제시하였다 [6].

이 보고서에 따르면 첫째 "정보보호 및 프라이버시 보호 수단으로 암호이용을 촉진" 정책에서 정부는 상용 암호제품의 개발을 장려하고, 암호기술 중립주의를 채택함으로써 공공 및 민간 부문이 공조하여 암호기술을 개발하도록 하고 우수한 기술은 서로 공유할 수 있는 제도를 마련하고 암호이용 선택에 있어 암호수요기관의 위험평가 결과에 따라 자유로이 선택할 수 있도록 보장하는 정책방안을 제안하였다.

둘째 "국제수준에 맞도록 암호수출통제제도 완화" 정책에서는 판매이전에 상용 암호제품에 대한 기술검토 실시, 암호제품의 수출국 관리를 위한 수출보고체계 제도 마련, 암호수출 허가절차 및 암호제품 판매 금지권한을 정부에 합법적으로 부여하는 등의 정책적 방안을 제시하였다.

셋째 "정부의 합법적 접근권 보장을 위한 법체제 정비" 정책에서는 암호의 역기능에 대비하기 위한 암호해독기술지원센터 설립, 키복구정보에 대한 정부의 합법적 접근권 보장, 기업과 정부의 공유정보에 대해 정부와 동일한 기밀보장 수준을 유지하는 등의 정책적 방안을 제시하였다.

3.1.2 암호수출통제제도

미국의 경쟁력 있는 암호기술이 외국으로 유출되는 것을 걱정하여 그동안 강한 규제를 해오던 암호수출통제 제도를 국제수준에 맞도록 완화하고자 하는 산업계

의견을 받아 들어 암호수출통제제도의 변화하기에 이르렀다. 현재 상무부 산하의 산업보호국(BIS, Bureau of Industry and Security)에서 상용 암호제품의 수출을 관리하고 있다. 대통령 명령에 따라 1996년 12월에 미국 수출관리규칙(EAR, Export Administration Regulation)의 Part 742를 개정하였다. 암호수출에 관한 사항은 EAR 15 C.F.R Parts 730-774, Section 740.13, 740.17 및 740.15에 규정되어 있다[7]. 개정의 주요내용은 미국 군수전략물자목록(U.S Munition List)에 속해있던 이중용도품목인 암호품목을 일반산업용품목 통제대상목록(CCL, Commerce Control List)으로 이관하여 수출을 통제하기로 한 것이다. 또한 1995년 이전에 키위탁 암호제품에 대해 국무부가 군수전략물자로 취급하여 수출시 엄격히 통제하였으나 키위탁 암호제품의 수출규제를 완화하기 위해서 키위탁 암호제품도 CCL로 이관하면서 상무부가 이에 대한 수출을 관리하기로 하였다. 따라서 상무부는 캐나다를 제외한 모든 전 지역으로 키위탁 암호제품을 수출하는 경우 이에 대한 수출허가를 받도록 하였다. 단, 국무부 장관이 지정한 쿠바, 이란, 이라크, 북한, 리비아, 수단 및 시리아 등 7개국으로의 수출은 금지되어 있다. 1998년 12월에 키위탁 암호제품의 수출제도를 합리적으로 변화시키기 위하여 BIS의 기술검토를 마친 키위탁 암호제품에 한해 수출허가를 면제하는 규정을 추가하였다. 이에 따라 BIS는 신청한 키위탁 암호제품이 "키위탁 또는 키복구 제품 기준"을 만족하는 지에 대해 기술검토를 실시한다. 이 기준의 2번째 조항에 따르면 정당한 법적 권한을 가진 정부기관이 이용자의 지식 또는 도움 없이도 암호 복구정보 또는 복구키를 복구할 수 있어야만 제품의 암호기능을 실행할 수 있다[8]. 2000년 개정에서는 EAR Part 740.17의 규정에 따라 EU 회원국, 호주, 체코, 헝가리, 일본, 뉴질랜드, 노르웨이, 폴란드 및 스위스 등으로 일부 암호품목을 수출하는 경우 BIS의 기술검토를 1회 마친 품목에 한해 수출허가를 별도로 받지 않도록 하였다. 2002년 상무부는 바세나르 협정의 조약내용을 반영하여 EAR을 개정하였다. 64비트를 초과하는 대량판매용 암호제품에 대해 수출 및 재수출을 자유화하기로 하였다. 다음 표에서는 EAR의 개정이력에 따라 미국 암호수출정책의 주요변화를 요약하였다.

미국은 암호의 가치변화에 따른 암호의 중요성을 인지하고 암호산업에 있어서도 자국의 경제적·기술적 우위를 유지하기 위한 암호정책을 펴오고 있다. 특히, 암호제품 및 기술의 수출규제 정책을 통하여 미국내 암호이용정책에 간접적으로 영향력을 행사해 왔다.

3.1.3 암호이용 관련 법제정 추진현황

미국 정부는 암호이용의 자율권을 보장하고 국가안보 및 사회질서 유지를 위한 암호통제의 법집행 수단을 개선하기 위하여 암호관련 법안을 여러 차례 제안한 바 있다.

1997년 2월 105회 국회에서는 암호이용 및 판매의 자유화, 의무적 키위탁제도 금지, 암호부정사용 금지 등의 내용을 주요골자로 하는 SAFE(Security and Freedom Through Encryption Act)의 입법화를 추진하였으나 법제정에 실패하였다. 이후 1999년 106회 국회에서 SAFE 법안을 수정하여 상정하였으나 현재 계류중인 법안으로 남아 있다. 또한 1998년 5월 105회 국회에서는 통신 및 전자정보에 대한 프라이버시 보호, 해독기술지원 및 수사지원을 위한 NET(National Electronic Technologies) 센터 설립, 암호제품의 수출에 관한 규제 등의 사항을 규정한 법안을 제안하기도 하였다. 이는 상원 소위원회까지 상정되었으나 이후 법제정 작업이 진행되지 못하였다. 1999년 9월 106회 국회는 미국시민의 프라이버시 보호를 위한 키복원기관에 관한 사항, 강제공개등에 관한 사항, FBI 산하 기술지원센터 기금조성에 관한 사항 등을 주요내용으로 하는 CESA(Cyberspace Electronic Security Act) 법안을 제안하여 2000년까지 미국 상·하원에서 몇 번의 수정작업을 진행하기도 하였으나 입법화되지 못하였다. 그리고 최근 2003년 1월 DSEA(Domestic Security Enhancement Act)(안)의 비공개 버전에서 암호를 범죄에 악용한 경우 초범인 경우 5년 이하의 징역, 재범인 경우 10년 이하의 징역 등 처벌조항을 규정하여 Patriot Act의 개정 법(안)에 삽입하려 했으나 결실을 맺지 못하였다[9].

이외에 암호를 포함한 정보보호업무에 대한 영역을 정의한 법이 있다. 2000년에 제정된 GISRA 2000 (Government Information Security Reform Act of 2000)에서는 각 행정기관이 소관기관의 정보보호정책을 수립하고 집행하도록 자율권을 부여하고 다만, 대통령령(Executive Order 13292, 2003.3.25)에 의해 비밀로 분류된 정보와 국가안보시스템에 대한 정보보호 기술·표준·지침 개발은 국방부, 중앙정보부 및 대통령이 지정한 기관에서 담당하고 이외의 연방정보 및 정부의 정보시스템에 관한 정보보호 기술·

〔표 1〕 미국의 암호수출정책 주요 변화

개정일	주요내용
96.12.13	**〔61 FR 65462 : 키위탁 암호장비 및 소프트웨어에 대한 수출허가제도〕** ·키위탁 암호제품에 대한 국가통제 의무를 부과 ·키위탁 암호제품을 최소규제원칙규정 및 대량판매용 대상품목에서 제외 ·공개가능한 키위탁 소프트웨어를 암호수출규제 대상으로 지정
96.12.30	**〔61 FR 68572 : 암호품목을 CCL로 이관〕** ·1996년 11월 15일 대통령령(E.O 13026)에 따라 군수전략물자목록에 있던 암호품목을 CCL로 이관 ·향후 2년간 56비트 DES 및 이와 동등한 수준의 암호알고리즘을 탑재한 암호품목의 수출허용. ※단 이러한 암호품목은 키위탁 및 키복구 기능을 갖는 암호품목의 사용 및 키관리기반구조 구축을 위해 사용되어야 함
98.09.22	**〔63 FR 50516 : 수출허가 대상의 암호품목〕** ·은행업무 및 금융거래 목적의 일반 암호상품 및 소프트웨어인 경우, 키복구 기능이 없어도 수출하는 것을 허용
98.12.31	**〔63 FR 72156 : 수출허가 대상의 암호품목〕** ·미국 기업의 해외지사, 보험회사, 건강의료 최종사용자에게 암호품목을 수출하는 것을 허용
00.01.14	**〔65 FR 2492 : 수출허가 대상의 암호품목 개정〕** ·1999년 9월 16일 미국정부의 새로운 암호정책 발표에 따라 테러지원국을 제외한 모든 지역에 있는 개인, 기업 및 민간부문의 최종사용자에게로 암호품목을 수출하는 것을 허용 ·수출사후 보고체계를 갖추어 수출현황을 관리
00.10.19	**〔65 FR 62600 : 수출허가 암호품목 재개정〕** ·2000년 7월 17일 미국정부의 암호수출규제완화 정책 발표에 따라 EU 회원국을 비롯한 23개국으로 기술검토를 받은 암호품목에 한해 별도의 수출허가 없이 수출하는 것을 허가 ·테러지원국 7개국에 대한 수출금지규정은 유지
02.06.06	**〔67 FR 38855 바세나르협정의 수준으로 완화〕** ·64비트를 초과하는 대량판매용 암호품목에 대해 1회 기술검토후 별도의 수출허가없이 수출허용 ·ECCN 5B002에 해당하는 암호품목도 수출허가예외규정에 적용
03.06.17	**〔68 FR 35783 : 기술검토신청 안내지침 제공〕** ·개인사용 용도로 개인이 해외여행시 수반하는 암호제품의 경우 수출이 가능하나 테러지원국 7개국에 대해서는 금지 ·암호기능을 내장한 스마트카드를 수출허가대상에서 제외, 따라서 별도의 수출허가가 필요 없이 기술검토 후 수출이 가능 ·암호기능을 내장한 단거리 무선장비로 소매용 또는 대량판매용인 경우 최소규제원칙을 적용 ·수출업자가 기술검토 신청시 필요한 정보를 정확히 제공할 수 있도록 지침마련

표준·지침 개발은 NIST를 통해 상무부가 담당하도록 규정하였다.

3.2 영국

3.2.1 암호정책 기본방향

1996년 6월 영국 상무부(DTI)는 "정보통신망에서의 암호이용에 관한 정부규제의 취지"라는 정책보고서를 통해 영국 암호정책의 기본방향을 발표하였다. 이 보고서에 따르면 정부는 암호키에 대한 합법적 접근권을 보존하기 위한 목적으로 제3의 신뢰기관을 승인 및 관리하는 법안을 도입할 예정이며 이러한 기관은 기관가입자 대상으로 암호키를 제출하도록 요청할 수 있다. 이로써 정부가 간접적으로 의무적 키복구제도를 도입함을 시사하였다.

상무부는 1997년 3월에 "암호서비스를 제공하는 TTP 승인제도에 관한 보고서"를 통해 암호이용에 관한 구체적 방안을 제시하였고 이에 대한 의견수렴을 실시하였다. 의견수렴 결과, 보고서내용에 전적으로 동의하는 의견은 소수의견이 불과하였으며 신뢰성 보장을 위한 TTP 승인제도를 찬성하지만 TTP 승인과정에서 키위탁에 대한 조건을 의무화하는 것에 대해 우려를 표명하였다. 이에 따라 상무부는 의견을 반영하여 수정된 보고서를 1998년에 다시 발표하기에 이르렀다. TTP 승인에 관한 사항은 강제규정은 아니며, 따라서 암호서비스 제공자는 정부의 승인 여부를 스스로 선택할 수 있다. 다만 승인 받은 TTP에 대해서는 키복구 기능을 갖추도록 하였다.

이 보고서 또한 의견수렴 과정을 통해 1999년 영국의 암호정책의 기본방향을 제시한 "전자상거래 신뢰기반 구축" 정책보고서를 발표하였다. 영국의 암호정책 기본방향으로 첫째, 평문 또는 해독키를 제출하도록 명령할 수 있는 권한을 법으로 제정하며, 둘째, 키위탁 및 키복구 제도를 장려하고, 셋째, 암호의 범죄악용 방지를 위한 산·학·연·관 공조체제를 구축한다. 이 보고서에 따르면 암호문에 해당하는 평문 또는 해독 키 제출명령 통지서 발부 권한은 유선감청 또는 수색·압류 수사권의 일부로서, 평문 또는 해독 키의 제출의무는 암호서비스 사업자와 이용자 모두에게 해당된다는 것이 정부의 입장이다. 단, 전자서명키는 수사권에서 제외된다. 암호서비스 제공자는 키위탁 또는 키복구에 대한 의무를 갖지 않아도 되며 키위탁 또는 키복구에 대한 사항을 권고사항으로 규정하고자 하였다. 다만 정부의 승인을 얻고자 하는 TTP는 수사권을 가진 정부기관이 암호문 수사에 필요한 정보를 요

청할 경우 키복구정보를 제출할 수 있음을 증명하여야 한다 [10]

3.2.2 암호이용관련 법제 추진 현황

1999년 전자상거래 신뢰기반 구축 보고서의 암호정책 방향에 따라 여러 가지 법안들이 제안되었었다. 이의 일환으로 1999년 7월 영국정부는 전자통신법(안)을 발표하였다. 법(안)에서는 해독명령 요청 권한에 대한 사항을 다루고 있었다. 법(안)에 따르면 합법적으로 암호문을 획득한 경우 해당 암호키를 소유하거나 암호문에 접근하여 이해할 수 있는 형태로 변환할 수 있는 자에게 해독명령 요청 통지서를 제시할 수 있다. 또는 암호키 제출 명령을 내릴 수도 있다. 다만 전자서명생성키를 공개하도록 요청할 수는 없다. 해독명령 요청 통지서에 대해 해당 암호 자료를 획득한 경우 관계기관의 주무부처(국무부 장관, 판사, 고위 경찰 등)의 승인을 얻어야 한다. 해독명령에 응하지 않는 자에 대해 최고 2년 이하의 징역에 처할 수 있는 처벌규정도 마련하였다. 또한 해독명령 요청을 통해 획득한 암호키의 사용을 제한키 위해 다양한 안전조항을 규정하기 위해 권한집행에 대한 시행령을 제정하고 이를 관장하는 감독감을 임명할 수 있도록 하였다. 정부는 해독권한을 가진 기관이 암호키에 접근할 수 있는 기술지원을 요청할 수 있는 기술지원센터 설립을 본 법(안)을 통해 제안하였다. 키위탁에 관한 사항이 법 조항에 명시되지 않았으나 암호서비스 기관 승인제도를 법조항으로 제시함으로써 키위탁 제도의 여지를 남겨두었다. 하지만 암호관련 조항에 대해 시민의 비판적인 반응으로 인하여 해독명령 권한에 관한 조항은 법(안)에서 삭제되었다. 따라서 2000년에 제정된 전자통신법(Electronic Communication Act)에서는 암호에 관한 조항이 일부만 포함되었다. 암호서비스의 신뢰성을 확보하기 위하여 영국정부가 정한 요구사항을 만족하는 자를 암호서비스 제공자로 승인하는 사항 등을 규정하였으며, 의무적 키위탁 금지조항도 마련하였다. 다만 키위탁을 하지 않음으로써 발생할 수 있는 손실에 대해서는 암호서비스 제공자와 가입자 사이에 합의하는 것에 대해 금지할 수 없다고 규정함으로써 키위탁 제도를 간접적으로 장려하고 있다고 판단된다.

2000년 2월 수사권 규제에 관한 법률(안)을 영국 하원에 제출하였다. 전자통신법(안)에서 삭제된 해독명령 권한에 관한 몇 개의 일부 조항을 수정하여 본 법률(안)에 포함시켰다. 이 법률(안)은 같은 해에 수사권규제에 관한 법률(RIPA, Regulation of Investigatory Power Act of 2000)로 제정되었는데 암호해독에 관한 수사권한 부여할 수 있는 조건을 다음과 같이 상세하게 규정하였다.

- 국가정보기관, 경찰, 서관 등이 암호문을 합법적으로 습득한 경우
- 국가안보, 범죄예방 및 경제안정의 목적을 위한 경우 또는 암호해독만이 수사해결에 유일하고 현실적인 수단인 경우
- 용의자가 암호해독에 필요한 키를 소유하고 있음을 확신하는 경우
- 수사에 필요한 암호문을 해독할 수 있는 키를 소유한 자에게 해당 평문 또는 해당 키를 제출토록 수사협조를 요청하는 경우
- 회사나 법인 등의 종사자에게 해독키를 요청하는 경우 또는 키를 더 이상 소유하고 있지 않지만 보관된 해당 키의 검색에 필요한 정보를 가지고 있는 경우 이를 제출토록 요청하는 경우

이외에도 고의로 암호해독 수사명령을 따르지 않는 자에 대해 처벌규정을 두고 있다. 처벌규정을 적용하기 위해 키의 소유여부를 입증하여야 하는데 이에 관한 사항은 매우 복잡하다. 해독명령 통지 이전에 키를 소유하고 있었음을 증명할 수 있었다면 통지시점 이후에 키를 소유하지 않더라도 키를 소유하고 있는 것으로 간주한다. 또한 용의자는 자신의 무죄를 입증하기 위해서는 해독능력이 없음을 증명하거나 과거 사건 발생시점에 키를 소유하고 있지 않았음을 증명하여야 한다.

ECA법을 통해 TTP 승인제도에 대한 법적 근거를 마련하였으나 tScheme의 민간 승인제도를 운영하고 있어 영국 정부는 민간의 승인제도가 원활히 운영될 경우 ECA법의 TTP 승인제도에 대한 규정의 효력을 발생시키지 않을 것이라는 단서 조항을 달았다. 현재 tScheme은 전자서명을 제공하는 서비스 기관과 온라인 Identity 관리를 위한 사용자 인증 서비스를 제공하는 기관에 승인제도를 운영하고 있으나 기밀성을 위한 암호화 서비스를 제공하는 기관에 대한 승인제도는 알려진 바가 없다 [11].

3.3 프랑스

3.3.1 수출통제제도

프랑스의 암호정책 담당 기관은 국가안보이사회(the Secretary General fo National Defense) 산하의 SCSSI(Service Central de La Securite

des Systemes d'Information)이다. 암호제품 수출입에 대한 기본법은 1996년에 개정된 제96-648호 통신기본법이며, 수출에 관한 상세 조항을 규정한 시행령으로는 제 98-101호(1998.2.24) 및 제 99-199호(1993.3.17)가 있다. 1996년 통신기본법을 개정하면서 암호제품에 수출입에 관한 사항을 규정하였다. 개정된 내용에 따르면 유럽연합 회원국 이외의 나라를 대상으로 암호장치 또는 서비스를 수출입하고자 하는 자는 해당 암호장치 또는 서비스의 목적이 기밀성을 위한 것이라면 정부의 허가를 받아야 한다. 프랑스는 바세나르 협정의 회원국임에도 불구하고 이때까지도 바세나르 협정에서 규정한 수출통제 제외 암호품목 목록을 적용하지 않았었다.

1999년 시행령이 공표된 이후 암호제품의 수입은 완전 자율화가 되었다. 이에 따른 암호수출입 및 이용에 관한 규제현황은 다음 표2와 같다.

3.3.2 암호이용관련 법제 현황

1996년 암호이용규제에 관한 법률이 제정되기 이전까지 프랑스내에서 암호의 공급과 이용에 대해 오랜 기간 규제가 있어왔다. 동법 및 시행령의 제정을 통해 제3의 신뢰기관을 통한 의무적 키복구 제도가 도입되면서 암호이용에 관한 규제가 다소 완화되었다. 40비트 이하의 암호이용에 대해서는 자율화하였고 40비트 이상의 고비도 암호를 이용하고자 하는 자는 신뢰기관인 키위탁 기관을 이용하도록 하였다. 제98-102호 키위탁 기관 승인조건에 관한 시행령에 따라 SCSSI의 승인을 받아야 한다. 다만, 암호문에 대한 프랑스 정부의 접근권을 보장하기 위해 신뢰기관의 가입자 암호키 제출을 의무화하도록 하고 있다. 신뢰기관은 가입자의 서비스 계약 체결시 이러한 사항에 대해 서면동의를 받도록 하고 있다. 이로써 40비트 이상의 고비도의 암호를 이용하고자 하는 자는 신뢰기관에게 키를 위탁하여야 한다. 프랑스 정부는 범죄수사에 필요한 경우 별도의 가이자 동의 없이 신뢰기관으로 하여금 가입자의 키를 제출토록 명령할 수 있게 되었다. 하지만 40비트 이하의 비도가 낮은 암호라도 이를 공급하는 자는 정부에 신고하여야 한다.

〔표 2〕 프랑스 암호규제 현황(1999년)

대상 범위	자율	사전신고	허가
인증기능	이용	수출입, 공급	
40비트 이하의 비밀성 기능	이용, 수입	공급, 이용, 수입	수출
40비트 이상, 128비트 이하의 비밀성 기능	이용, 수입 ※개인용도	공급	수출
아날로그 형태의 암호(예, 팩스)	이용, 수입		수출
이용자 접근이 불가능하게 설계한 암호응용프로그램	공급, 이용, 수출입		
외교관이 수반한 암호장비	이용, 수출입		
기타			공급, 이용

이와 같이 1999년 이전까지 의무적 키복구제도를 시행하는 등 암호이용에 대한 강한 규제를 해오다가 프랑스 수상의 암호자율화 정책을 발표함에 따라 128비트 이하의 암호이용을 허용하였으며 키위탁 기관을 통하 의무적 키복구 제도를 폐지하였다.

2001년 "일상생활의 보안에 관한 법률" 제정을 통해 암호이용 자유화 및 암호해독에 관한 사항을 일부 규정하면서 암호규제를 완화하였다. 이 법에서는 암호문에 관한 수사가 필요한 경우 해독능력을 가진 자 또는 해독키를 가진 자에게 해독을 요청할 수 있으며 최고 2년형에 달하는 범죄를 수사하는 경우 경찰이 국가 안보기관에게 해독지원을 요청할 수 있도록 규정하였다.

해독명령으로 인한 키위탁기관의 해독지원의 의무 및 위반시 2년 이상의 징역에 처하는 처벌조항과 해독명령 위반에 대한 최고 3년의 징역에 처하는 처벌조항을 규정하였다. 특히, 해독으로 인한 범죄 예방 및 피해경감의 효과를 거둘 수 있었으나 해독에 응하지 않아 범죄가 발생한 경우 해독명령 불복종에 대해 최고 5년의 징역에 처할 수 있도록 강한 처벌 규정을 두었다. 이외에도 동법 시행령(제2002-1709호, '02.8.7)에 따라 내무부 산하의 암호해독 기술지원센터를 설립하였으며 기술지원센터의 활동은 기밀사항이다.

3.4 중 국

중국의 경우 1999년에 제정된 "상업용 패스워드관리에 관한 법령"에 따라 자국내 암호제품 제조 및 이용을 엄격히 규제해 오고 있다. 중국공식지정 암호제조업체는 국가암호관리위원회의 승인을 얻어 암호제품을 제조하여 중국내 암호이용자들은 승인된 암호제품만을 이용하여야 한다. 개인이 해외에서 가져온 암호제품이나 스스로 개발한 암호제품을 사용할 경우 국가암호관리위원회의 별도 승인을 받아야 한다. 다만, 영사관내

에서 사용하거나 외교관이 사용하는 암호제품에 대해 승인을 받지 않아도 되는 예외규정을 두고 있다.

또한 2003년에 암호기능을 탑재한 수입 무선 단말기의 경우 중국에서 지정한 중국 알고리즘(WAPI, WLAN Authentication and Privacy Information)을 탑재하여야 하며 AES와 WEP(Wired Equivalent Privacy)를 비활성화시키도록 하는 정책을 발표하는 등 암호이용에 대해 강력히 규제를 하고 있다.

3.5 한 국

우리나라의 경우 국가정보원법, 보안업무규정, 군형법 등 국가 암호에 관한 기본 법률이 존재하여 암호자재에 대한 제작·공급·관리 등에 관한 사항을 정하고 있어 국가 암호이용에 있어 혼란이 없었으나, 민간 부분의 암호이용에 관한 사항을 정한 법률이 존재하지 않아 암호이용에 대한 여러 가지 논란이 제기 되어왔다. 이에 따라 1999년 민간부분의 암호이용에 관한 사항을 법제화하기 위하여 정통부와 국정원주도로 '암호이용촉진법'에 대한 법안을 마련하였으나 키복구제도에 대한 부처간 이견과 인권침해 우려의 위협이 제기되면서 입법화가 무산된 바 있다. 국외에서 의무적 키복구 제도로 인한 프라이버시 침해 논란이 국내로까지 전해졌기 때문에 실질적인 피해보다는 우려감으로 인해 법제화가 이루어지지 않았다. 의무적 키복구 제도는 암호이용자로 하여금 암호문 생성 및 복호에 필요한 암호키를 국가기관 또는 국가가 지정한 기관에게 의무적으로 위탁·관리토록 하고 암호가 범죄에 악용된 경우 합법적 수사에 따라 국가기관이 암호키를 사용할 수 있도록 보장하는 제도로 수사권 오·남용시에 암호이용자의 인권침해 우려가 있다.

현재 민간의 암호이용에 관하여 정보화촉진기본법, 전자거래기본법, 전자서명법 등에 암호 관련 조항이 일부 포함되어 있으나 전자거래 또는 정보유통의 안전성 및 신뢰성을 위해 암호를 이용할 수 있다는 선언적인 규정에 그치고 있어 암호이용에 관한 구체적인 사항이 규정되어 있지 않다.

암호기술은 전자정보의 누출을 방지하고 개인의 프라이버시를 보호해 주는 등 많은 장점을 가지고 있다. 실제로 OECD 암호정책가이드라인의 암호원칙에서 암호가 개인정보 및 프라이버시보호를 위한 가장 소중한 수단이라고 언급하고 있다. 하지만 암호화에 사용된 키가 분실되거나 손상되는 경우 자신의 정보에 접근할 수 없어 막대한 손실을 초래할 수 있다.

이러한 역기능에 대처하기 위하여 각 국에서는 1990년대 중반에 의무적 키복구제도를 도입하고자 하였으나 프라이버시 침해의 논란이 생겨 이를 대신하여 자발적 키복구제도 도입을 추진하고 있다. 이는 프라이버시를 최대한 보장하기 위해 이용자의 선택에 따라 암호키의 위탁 여부를 결정할 수 있도록 하는 제도이다.

행정자치부는 전자민원행정서비스에서 중요 민원서류를 신청인에게 전송할 때 중요정보의 노출방지를 위해 암호서비스를 적용하기로 하고 이에 필요한 암호키분배용인증서발급정책을 정보통신부와 수립하기로 협의하였다. 이에 따라 정보통신부와 한국정보보호진흥원은 2002년 8월, 암호키 분실에 따른 복원기능을 탑재한 정보보호제품의 경우 암호제품이 이용자의 프라이버시를 침해하지 않도록 하는 "암호키분배인증서및키의안전한관리를위한지침"을 마련하였다. 그리고 민원인 대상의 암호키분배인증서 발급서비스를 수행할 공인인증기관이 지침에 따른 안전한 시스템을 구축할 수 있도록 지원하였다.

"암호키분배인증서및키의안전한관리를위한지침"에서는 암호서비스에 필요한 암호키를 이용자의 시스템에서 생성하도록 하고 이용자가 키복구 서비스를 이용할 것인지 여부를 스스로 선택할 수 있도록 하여 이용자의 e-Privacy를 최대한 보장할 수 있도록 하였다. 또한 키를 관리하는 기관의 시스템이 해킹을 당하더라도 공격자가 쉽게 이용자의 키를 알아낼 수 없도록 보안조치를 강화하였다.

그러나 "암호키분배인증서및키의안전한관리를위한지침"은 법적 근거가 없어 정보통신부 지침으로 고시되지 못하였다. 이로 인해 민원인에게 암호키분배용인증서를 발급하는 공인인증기관을 대상으로 지침을 준수하도록 권고하였을 뿐, 그 외 암호키분배용인증서를 발급하는 사업자에 대해서는 적절한 조치를 취할 수 없었다. 따라서 모든 국민의 e-Privacy를 보장하는데 한계가 있어 지침의 실효성을 확보하기 위하여 제도적 보완이 필요하다.

2002년 기준 각국의 보안서버 활용현황을 조사한 2003년 OECD 정책 보고서(DSTI/ICCP/ E(2003)9)에 따르면 국내 인터넷 가입자 수의 비율은 30개 가입국 중 최고 수준이나 보안서버의 사용률은 25위로 저조한 것으로 조사되었다. 이에 대한 현황을 파악하기 위해 정보통신부 중심으로 국내 전문가들이 조사한 바에 따르면 OECD의 보안서버의 정의가 불명확하고 자료 수집상 객관성이 부족하여 실제 국내 보안서버 활용 비율보다 낮게 조사된 것으로 알려졌다. OECD의 조사대상 보안서버 수는 특정회사(VeriSign)의 인

〔표 3〕 암호관련 법 규정 주요내용

항목	법명(국가)	규정내용
국가 정보보호 정책 영역의 구분	GISRA '00(미국)	대통령령에 의해 비밀로 분류된 정보 및 국가보안시스템(National Security System)에 대한 기술·표준·지침에 대한 개발은 국방부(DoD), 중앙정보부(CIA) 및 대통령이 지정한 기관에서 담당 이외의 연방정보 및 정부시스템에 대한 기술·표준·지침에 대한 개발은 NIST를 통해 상무부(DoC)가 담당
암호이용 안전성 신뢰성 확보	ECA '00(영국)	암호서비스의 신뢰성을 확보하기 위하여 영국정부가 정한 요구사항을 만족하는 자를 암호서비스제공자로 승인하는 제도에 관한 사항을 규정
	Decree 98-206, Decree 98-207 (프랑스)	40비트 이상의 강한 암호의 이용 및 공급의 경우 프랑스 정부의 허가를 받아야 하며, 40비트 이하의 약한 암호라도 공급의 경우 프랑스 정부에 신고하여야 함 다만, 암호 공급자가 암호의 개발, 검증, 시험운영에 대한 사실을 2주전까지 프랑스의 정보시스템보안센터(SCSSI)에 미리 알리는 경우 신고 또는 허가를 받지 않아도 됨
	정보사회법 (안) (프랑스)	암호서비스사업자의 신고제, 의무조항, 처벌규칙 등에 관한 사항을 규정
	정부암호 정책지침 '97 (핀란드)	암호서비스 및 인증서비스의 안전성을 확보하기 위해 핀란드 정부는 서비스 제공기관에 대한 허가제도 및 승인제도에 관한 사항을 핀란드 암호정책 가이드라인에서 규정
암호의 역기능 방지 및 해독기술 지원 연구센터 설립	E-Privacy 법(안) '98(미국)	해독업무 기술지원을 위한 NET (National Electronic Technologies) Center를 법무부 산하에 설립하는 사항을 규정하였으며, 전 클린턴 행정부는 NET 설립을 위해 $20억 달러를 요청한바 있음
	AEDPA법 '96(미국)	AEDPA 법률에 따라 FBI는 해독기술을 지원하는 "Technical Support Center"를 설립
	CESA 법(안) '99(미국)	Technical Support Center의 4년간 운영예산 $8천만 달러의 추가지원을 요청한바 있음
	Daily Security 법 '01 및 동법 시행령 '02(프랑스)	해독업무 기술지원을 임무로 하는 내무부 산하의 기술지원센터를 설립 - 기술지원센터의 활동은 기밀사항임

〔표 3〕 암호관련 법 규정 주요내용(계속)

항목	법명(국가)	규정내용
암호기술의 관리	CSRDA 법 '02 (미국)	컴퓨터 및 네트워크 보안관련 연구·개발을 위한 연구기금지원, 공동연구센터 설립 등에 관한 사항을 규정 상무부 산하의 "컴퓨터보안·프라이버시 위원회"가 암호 및 프라이버시 등에 관련한 연구의 필요성을 조사토록 NIST가 연구기금을 지원 (2003년 : 약 12억, 2004년 : 약 13억)
키위탁 기관의 설립	Decree 98-102 (프랑스)	키위탁기관 승인조건에 관한 사항을 규정
암호해독 명령	Daily Security 법 '01 (프랑스)	해독명령으로 인한 키위탁기관의 해독지원의 의무 및 위반시 2년 이상의 실형 처벌 규정 해독 명령 위반에 대한 최고 3년의 실형 및 해독으로 인한 범죄예방 또는 피해경감의 효과를 거둘 수 있었던 경우 해독명령 불복종에 대한 최고 5년 실형 처벌 규정 암호문에 관한 수사가 필요한 경우 해독능력을 가진 자 또는 해독키를 가진 자에게 해독을 요청할 수 있는 권한 최고 2년형에 달하는 범죄 수사에 경찰이 국가안보기관에게 해독지원 요청
	Cybercrime Act '01 (호주)	치안판사는 증거자료를 담고 있는 컴퓨터의 주인 또는 임차인으로 암호관련 지식을 소유하고 있는 자에게 자료제출 명령을 내릴 수 있음 해당 명령을 이행하지 않을 경우 6개월의 구형에 처할 수 있음
	ISCA 법 '01 (벨기에)	수사판사의 해독명령에 대한 권한 부여 암호서비스에 관한 기술적 사항, 접근방법, 수행절차 또는 해독방법 등 수사에 필요한 정보를 제공할 수 있을 것으로 판단되는 자에게 합법적으로 해독명령을 내릴 수 있음
	PTIA 법, CCIMA법 (핀란드)	수사기관은 범죄수사에 필요한 암호생성정보를 소유하고 있는 사업자 또는 해당정보를 담고있는 컴퓨터 관리자에게 해당정보를 제출토록 명령할 수 있음
	ISSA 법 '02 (네덜란드)	해독명령권을 국가안보국에 부여 이에 해독의 전문지식을 소유한 자는 국가안보국의 관리·감독하에 컴퓨터를 해킹하거나 통신정보를 가로채기 하여 정보를 해독할 수 있음 이를 위반한 경우 6개월의 구형에 처할 수 있음

증서를 이용하는 보안서버만을 기준으로 통계에 반영하였으며, 국내에서 자체 발급한 인증서는 조사대상에서 제외되었다. OECD의 보안서버의 정의는 VeriSign사의 인증서를 사용하는 서버로 정의하였으나, 실제 보안서버는 웹서버와 웹브라우저 간의 안전한 통신기능(기밀성, 무결성, 신원확인)을 제공하는 서버로 정의하는 것이 일반적이다. 향후 보안서버 개념과 범위 결정, 인증기관 파악 등을 통해 국내 보안 서버의 수를 정확히 산정하고 OECD 등에 IT 지수 통계자료 통보시 자체 조사한 보안서버 수를 통보하여 지표가 상향 반영될 수 있도록 국제기구 활동에도 적극 참여하여야 할 것이다. 또한 OECD, ITU 등 국제기구의 지수관련 회의에 적극 참여하여 우리나라 입장 제시를 통해 집계방식을 개선할 수 있도록 하여야 한다. 조사결과를 보면, '2001년 하반기 ~ 2002년 상반기'의 우리나라 보안서버 수는 1,382개로 추정되었으며, 상기 보안서버 수를 우리나라 인구 4천7백만을 적용해 10만명 당 서버 수를 산출하면 2.94개로 추정되었다. 이는 인터넷 사용으로 인한 정보보호 위협이 증대되는 상황에서 매우 낮은 수라고 할 수 있다. 따라서 인터넷서비스를 제공하는 자로 하여금 기본적으로 보안서버의 사용을 하도록 하는 방안을 마련하고 이에 대한 홍보도 적극적으로 추진하여야 할 것이다.

Ⅳ. 국내외 암호이용관련 법제도 현황 비교

1997년 OECD가 암호정책가이드라인을 통해 암호정책의 기본원칙을 제시한 이래로 1997년부터 1999년 사시에 미국, 캐나다, 영국, 독일 등은 암호수출입통제제도, 암호관련 수사에 관한 제도, 암호해독기술 연구 등의 주제로 자국의 실정에 맞는 정책방안을 세우기 위한 연구를 진행하고 이의 결과를 암호정책 보고서로 발간하였다. 또한 이러한 보고서의 암호정책의 기본방향을 기반으로 이에 따른 법체제를 정비하기 위해 암호에 관련 조항을 일부 마련한 법안을 작성하여 입법화를 추진하였다. 미국의 경우 수차례 입법화를 시도하였으나 암호에 관한 독립법으로써 입법화 된 법안은 없다. 영국의 경우 ECA, RIPA 법에서는 암호에 관한 일부 조항을 포함하고 있으며 프랑스도 암호해독 및 수사에 관한 사항을 법에서 일부 규정하고 있다.

결론으로 국가 정보보호정책 업무 영역, 암호의 안전성·신뢰성 기반, 암호의 역기능 방지, 암호해독 및 수사에 관한 주제로 법 규정 및 법안의 규정을 나라별로 정리 요약하였다.

참 고 문 헌

[1] OECD, "GUIDELINES FOR CRYPTOGRAPHY POLICY", 1997

[2] http://www.wassenaar.org, "The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies", 1996

[3] 산업자원부, "전략물자수출입공고", *산업자원부 고시 제2002-123호*, 2002

[4] http://rechten.uvt.nl/koops/cryptolaw, "Crypto Law Suvey", 2002

[5] OECD, "Draft Revised Inventory of Controls on Cryptography Technologies", 2002

[6] http://www.fas.org/irp/news/1999/09/990916-crypto-wh.htm, "Preserving America's Privacy and Security in the Next Century", THE WHITE HOUSE, 1999

[7] BIS, "Export Administration Regulations", Jun, 2003

[8] BIS, "Key Escrow or Key Recovery Products Criteria", Supplement No.4 to Part 742, June, 2003

[9] http://www.cdt.org

[10] DTI, "Building Confidence in Electronic Commerce", May, 1999

[11] http://www.tscheme.org

〔붙임〕 암호관련 수출통제체제 및 법제 현황 비교

		호주	벨기에	캐나다	체코	중국	덴마크
바세나르 협정 가입		○	○	○	○	×	○
유럽연합 회원국		×	○	×	×	×	○
수출통제제도	수출통제	○	○	○	○	○	○
	관계 법령	소비자법령	군수전략물자 및 관련 기술의 수출입·이전에 관한 왕실법령('98)	수출입허가법률	국제수출통제체제에 적용되는 품목 및 기술의 수출입 규제에 관한 법률 및 시행령('97)	상업용 패스워드 관리법('99)	이중용도 품목 등에 관한 대통령령
	수출허가기관	국방부 산하의 국방신호이사회(DSD)	외교통상부	외교통상부	산업무역부	국가암호관리위원회	무역산업기관
	GSN 적용[1]	×	-	○	-	-	○
	수출규제 적용 운송수단 형태	미결정	유형	유·무형	유형	-	유·무형
	수입통제	×	×	×	×	○	×
암호이용 관계 법령		×	법률 제1997-19호('97) : 암호이용 자유원칙 선언	×	×	상업용 패스워드 관리법('99)	암호이용·판매에 관한 법률 제정 실패
자국내 암호이용 규제		×	○ (BIPT[2]) 정부기관의 사전동의 요구)	×	×	○ (국가암호관리위원회가 승인한 암호제품만 사용가능)	×
키복구 정책		정부용 암호제품에 키복구 기능 탑재 의무화('00)	의무적 키복구 정책	키복구 기술 사용 권장	-	-	키복구 정책의 필요성 논의
수사기관의 해독명령 관계 법령		사이버범죄법 ('01)	정보과학에 관한 법률('00)	근거 규정 마련 추진	-	-	-

※ '-' : 관련 정보 없음

1) GSN : General Software Note (이중용도품목에 대한 국제 수출통제체제인 바세나르 협정에서 규정한 수출규제대상품목 목록)

2) BIPT : Belgian Institute for Posts and Telecommunications

		오스트리아	핀란드	프랑스	독일	그리스	홍콩
바세나르 협정 가입		○	○	○	○	○	×
유럽연합 회원국		○	○	○	○	○	×
수출통제 제도	수출통제	○	○	○	○	○	○
	관계 법령	BGBI Nr.172/1995	이중용도품목 수출통제에 관한 법령('96), 이중용도품목 수출허가제도규칙('97)	암호수출통제법, 이중용도품목 수출통제 시행령 등	수출통제 관련 개정법('99)	-	수출입법령
	수출허가기관	경제연방부	통상산업부	SCSSI	경제기술부, 독일연방 수출관리청	-	-
	GSN 적용	○	○	×	-	○	×
	수출규제 적용 운송수단 형태	유형	유·무형	유·무형	-	-	유형
	수입통제	×	×	○	-	×	○
암호이용 관계 법령		×	×	암호이용규제에 관한 법률('96), 정보사회법(안)('01)	× ('99 암호정책 기본방향 제시)	×	×[3]
자국내 암호이용 규제		○ (라디오 주파수 암호규제)	×	○	×	×	×
키복구 정책		×	자발적 키복구 유도 정책	키위탁기관 승인제도('98), TTP를 통한 의무적 키복구 제도 폐지('99)	정부 부처간 의견대립으로 논의가 계속됨	-	-
수사기관의 해독명령 관계 법령		×	사전수색수사법, 범죄수사 강제수단에 관한 법	일상생활의 보안에 관한 법률('01), 제2002-1703호 시행령('02)	정부 부처간 의견대립으로 논의가 계속됨	-	해독명령에 관한 법률 제정의 필요성 제기('00)

3) 홍콩은 전화망에 연결되어 동작하는 암호제품의 경우 "네트워크연결규칙"을 준수하여야 함

		헝가리	아일랜드	이스라엘	이탈리아	일본	룩셈브르크
바세나르 협정 가입		○	○	×	○	○	○
유럽연합 회원국		×	○	×	○	×	○
수출통제 제도	수출통제	○	○	○	○	○	○
	관계 법령	-	수출통제법('83), 수출통제법령('96)	-('99 상업용 암호품목 수출규제정책)	수출허가 관련 법 No.89('97)	외국교역법('49) 및 시행령('80), 국제무역행정부 통보('92)	-
	수출허가기관	경제부	기업노동무역부 (수출허가부서)	국방부(IMOD)	외교통상부	외교통상산업부	-
	GSN 적용	-	○	×	○	○	○
	수출규제 적용 운송수단 형태	-	-	-	-	유형[5]	-
	수입통제	○	×	○	×	×	×
암호이용 관계 법령		×[4]	×('98, 암호정책의 기본원칙 제시)	상품 및 서비스 규제에 관한 시행령 개정('98)	이탈리아법 No.801('77) (국가기밀 보호용 암호의 이용 금지조항)	×	×
자국내 암호이용 규제		×	×	○ (암호허가제도)	×	×	×
키복구 정책			-	-		키위탁 및 키복구 제도 채택 여부 검토	-
수사기관의 해독명령 관계 법령		-	전자상거래법 ('00)	-	-	감청법 (암호통신 기록 기재)	전자상거래법 (안)('99)

4) 헝가리 전자서명법('01)에서 전자서명생성키를 전자서명 이외의 다른 목적으로 사용하는 것을 금지. 즉, 암호문 생성시 전자서명생성키를 사용하지 못하도록 법에서 규정

5) 2000년까지 유·무형 수단에 대해 수출규정을 모두 적용하여 왔으나, 2000년 7월에 외교통상산업부는 인터넷을 통한 암호소프트웨어의 수출규제를 완화하기로 함

		멕시코	네덜란드	뉴질랜드	노르웨이	폴란드	포르투갈
바세나르 협정 가입		×	○	○	○	○	○
유럽연합 회원국		×	○	×	×	○	○
수출통제 제도	수출통제	×	○	○	○	○	○
	관계 법령	-	수출입에 관한 법률 ('62), 전략물자수출시 행령	소비자법('96), 소비자세법('96), 수출금지법령 ('53)	전략물자·서비스·기술등에 관한 수출법률('87) 및 시행령('89)	-	-
	수출허가기관	-	수출입중앙기관 (CDIU)	외교통상부 산하 국제안보무기통제과(ISAC)	외교부	-	통상이사회
	GSN 적용	-	○	×	○	-	○
	수출규제 적용 운송수단 형태	-	유형	유형	유·무형	-	-
	수입통제	×	×	○	×	○[8]	×
암호이용 관계 법령		×[6] (소비자보호연 방법에서 암호이용 언급)	통신서비스 감청 시행령[7], TTP 제도 법률적 근거마련 프로젝트 추진	× (국가암호정책 위원회가 암호정책 수립)	×	×	×
자국내 암호이용 규제		×	×	×	×	×	×
키복구 정책		-	자발적 키위탁 제도 도입 추진('96)	-	-	-	-
수사기관의 해독명령 관계 법령		-	감청및국가안보 국에관한법률 ('02)	-	-	-	-

6) 2000년에 제정된 소비자보호연방법 제76B조의 규정에 따라 전자/광통신 사업자는 이용자의 프라이버시 보장수단으로 암호를 이용할 수 있으며 이 경우 소비자에게 사용한 암호기술을 공지하여야 함

7) 통신서비스감청시행령 제2조 규정에 따라 통신사업자는 자사가 조치한 암호기능을 취하하도록 정부기관으로부터 요청받을 수 있다.

8) 폴란드는 관계 법령('93) 규정에 의거 수입 암호제품을 구입하는 경우 수입 허가·인증을 받아야 함

		러시아	싱가포르	남아프리카	스페인	스웨덴	스위스
바세나르 협정 가입		○	×	×	○	○	○
유럽연합 회원국		×	×	×	○	○	×
수출통제 제도	수출통제	○	×	○(군사용)	○	○	○
	관계 법령	-	×	군사무기개발및 보호에관한법률	이중용도품목 수출통제 관련법률('98)	이중용도품목 및 기술지원 규제에관한법률 및 시행령('00)	수출통제품목에 관한법('97)
	수출허가기관	무역부	×	-	내무장관위원회	국가전략물자검사단	대외경제부의연방국
	GSN 적용	×	×	×	○	○	○
	수출규제 적용 운송수단 형태	-	×	-	유·무형	유·무형	유·무형
	수입통제	○	×[9]	○(군사용)	○[11]	×	×
암호이용 관계 법령		암호이용금지에 관한 대통령령('95)	×	전자통신 거래법('02)	통신일반법[12]	해독장비제작금지법('93)	VFKV('95) (라디오 암호통신 규제)
자국내 암호이용 규제		○ (FAPSI 암호허가기관)	○ (통신장비 허가제도)	×[10]	×	×	호환성보장을 위한 표준 적합성 검증필
키복구 정책		-	키복구기능을 탑재한 암호제품 이용 장려정책 ('00)	-	-	정부용 키관리제품에 키복구기능탑재 의무화	-
수사기관의 해독명령 관계 법령		-	컴퓨터오용 방지법('99)	전자통신 거래법('02)	통신일반법	-	-

9) 싱가포르는 수출에 대한 규제는 없었으며, 2000년 이전까지 수입에 대한 규제가 있었으나 2000.1.21 폐지

10) 원칙적으로 기업이나 민간에서 암호를 이용하는 것은 자유이나 암호사업자는 암호등록기관(상무부 국장)의 장에게 등록하여야 하며 등록된 사업자는 정부의 자료제출 명령에 응하여야 함

11) 개인용도의 암호기술 수입은 자유이나 국가안보에 연관되는 암호제품 또는 시스템의 수입은 국방부의 CESID 통제를 받음

12) 스페인의 통신일반법 제52조에 따라 암호통신을 위해 암호제품 또는 프로그램을 사용하는 것은 자유이나 정부용 제품에 사용한 암호알고리즘 또는 암호처리방법에 대한 정보제공의 의무를 개발자, 망관리자, 서비스 제공자 및 이용자에게 부과

		터키	우크라이나	영국	미국	한국
바세나르 협정 가입		○	○	○	○	○
유럽연합 회원국		×	×	○	×	×
수출통제 제도	수출통제	○[13]	○	○	○	○
	관계 법령	수출체제 시행령('95)	-	군사무기개발 및 보호에관한법률	수출관리규정 (ERA)[15]	대외무역법률 및 시행령, 전략물자수출입공고
	수출허가기관	외교통상과	-	상무부의 수출관리국	상무부의 산업보호국	산자부, 국방부
	GSN 적용	○	○	○	○	○
	수출규제 적용 운송수단 형태	유형	-	유형	유·무형	유·무형
	수입통제	×	×	×	×	×
암호이용 관계 법령		-	-	수사권규제에관한법률 (RIPA, '00), 전자통신거래법 (ECA, '00)	×[16] (암호정책기본방향 제시 '97)	×
자국내 암호이용 규제		-	-	×	×	×
키복구 정책		-	-	의무적 키위탁 금지[14]	의무적 키위탁 제도 도입 실패[17]	자발적 키복구 제도 도입 추진[18]
수사기관의 해독명령 관계 법령		-	-	수사권규제에관한법률 (RIPA, '00), 전자통신거래법 (ECA, '00)	×	×

13) 터키는 암호제품을 포함한 민감한 품목, 기술 및 이중용도품목의 재료 등을 이스탄불 금광물수출 연합에 등록하도록 하고 있음. 또한 군사용 암호제품을 수출하는 경우 국방부의 허가승인 필요

14) 전자통신법 제14조 규정에 따라 키위탁 의무를 금지조항으로 두고 있으나, 키위탁을 하지 않음으로써 발생할 수 있는 손실위험에 대해 알려 이용자에게 합의를 얻는 것을 허용

15) 미국은 상용암호 제품/기술을 수출하기 위해서 수출업자로 하여금 수출대상품목의 형태 및 최종 사용자의 유형에 따라 기술검토, 수출현황보고, 수출허가 등 단계적으로 수출규제를 적용

16) 미국은 CESA(안), SAFE(안), E-Privacy(안) 등 암호이용 관련 법제정 추진을 '97년부터 계속적으로 시도하고 있으나, 현재까지 법으로 제정된 법안은 없음

17) 미국은 '93년부터 NIST의 EES 표준 발표를 시작으로 키복구 기능을 탑재한 클리퍼칩을 정부용 제품에 탑재하도록 하는 클리퍼 정책을 추진하면서 의무적 키위탁 제도도입을 시도하였으나, 시민단체에 반대에 부딪쳐 클리퍼 정책을 계속 수정해오다 NSA는 정부기관 및 국방부에서 사용한 키복구 제품 평가기준을 '98년에 발표하고, NIST는 민간에서 개발한 정부용 키복구 제품을 위한 요구사항을 '98년에 제시하면서 더 이상의 키위탁에 대한 정책을 발표하고 있지 않고 있음

18) 정보통신부와 정보보호진흥원은 2002년 암호서비스 신뢰성을 제고하기 위한 암호서비스 사업자가 갖추어야 할 시설 및 장비에 대한 요구사항을 제시한 "암호키분배인증서및키의안전하관리를위한지침"을 마련하였으나, 법적 근거가 없어 실효성 확보에 어려움이 있음

〈著者紹介〉

권 현 조 (Hyun Joe Kwon)
정회원

1997년 2월 : 성균관대학교 정보공학과 학사
2000년 8월 : 성균관대학교 정보통신대학원 석사
1997년 1월~1997년 7월 : (주)나라계전기술연구소 연구원
1997년 7월~현재 : 한국정보보호진흥원 선임연구원
〈관심분야〉 키관리, 암호프로토콜, 공통평가방법론, 정보보호시스템평가

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호응용팀장
〈관심분야〉 암호학, 정보보호, RFID/USN 정보보호

이 재 일 (Jae-il Lee)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국IBM
1996년 7월~현재 : 한국정보보호진흥원 인프라보호단장
〈관심분야〉 : 유·무선PKI, 유비쿼터스 보안, 주요정보통신기반구조보호, 네트워크보안