韓國IT서비스學會誌
第11卷 第2號
2012年 6月

글로벌 기업의 암호해독명령 대응 방안

손상일* · 손유승* · 김영권* · 고승철***

A Crypto Control Guideline for Global Enterprises in Order to Respond the Decryption Order

Sang Il Son* · Yu Seung Son* · Young Kyon Kim* · Sung Cheol Goh**

■ Abstract ■

Nowadays, encryption is core technology widely used in IT industry to protect private information of individuals and important intellectual assets of companies. However, when criminals and terror suspects abuse such technology, national security can be threatened and law enforcement can be disturbed. To prevent such adverse effects of cryptography, some nations have enacted legislations that allow legally obtained encrypted data to be decrypted by certain law enforcement agencies. Hence it is imperative that firms having international presence understand and comply by each nation's regulations on decryption order. This paper explains circumstances under which legislations on decryption order were established, organizes countries with regulations and punishment, explores what global enterprises need to consider in making policies to effectively respond to decryption orders, and suggests that technological methods and managerial guidelines for control of encryption be established.

Keyword : Decryption Order, Global Enterprises, Crypto Control Guideline

논문투고일 : 2012년 04월 26일 논문수정완료일 : 2012년 06월 14일 논문게재확정일 : 2012년 06월 20일

* 수원대학교 IT 대학 컴퓨터공학과 박사과정
** 수원대학교 IT 대학 정보보호학과 교수, 교신저자

1. 서 론

오늘날 정보통신 분야의 기술 발전은 정보를 전달하고 교환하는 방식을 급진적으로 변화시키고 있다. 디지털 혁명으로 인해 커뮤니케이션의 속도, 효율 그리고 비용 절감 효과와 함께 국제적으로 커뮤니케이션 기반 시설의 정보보호, 사생활 보호에 관한 새로운 문제가 발생하고 있다[1]. 이러한 문제를 해결하기 위해 암호기술이 사용되고 있다.

전통적으로 암호기술은 국가보안 기술로 간주되어 개인이나 기업이 사용하는 것은 적극적으로 통제되었다. 그러나 OECD의 암호정책 지침에 따라, 국가들은 암호기술과 제품 사용에 대한 통제를 완화하였고, 오늘날 암호기술은 스마트폰, 디지털 TV, 유료 디지털 컨텐츠 등 IT 제품의 핵심 요소기술로 활용되고 있다. 또한 암호기술은 개인의 프라이버시와 의료정보, 재정정보, 이메일과 같은 개인정보보호와 기업의 중요한 정보자산을 보호하기 위해 널리 사용되고 있다. 그러나 범죄 또는 테러 용의자가 이러한 암호기술을 악용할 수도 있어 국가안보가 위협받거나 법집행에 상당한 어려움을 줄 수도 있다. 이러한 암호사용의 역기능을 방지하기 위해 일부 국가에서는 법집행 기관이 적법하게 획득한 암호화된 데이터에 대한 강제 암호해독 명령을 지시할 수 있도록 법률을 제정하고 있다.

최근 캐나다의 RIM 회사와 인도 정부 사이의 블랙베리 통신에 대한 접근권한 논쟁에서 나타났듯이, 암호통제는 여전히 중요한 쟁점사항이며, 단순히 논의 주제가 변했을 뿐이다[2].

2011년 UAE, 사우디아라비아, 인도, 레바논과 알제리 등의 일부 아랍 국가에서는 블랙베리를 통해 제공되는 e메일과 메신저, 웹브라우징 등 일부 보안서비스가 국가안보를 위협한다는 이유로 서비스 중단 가능성을 내비쳤다. 캐나다 RIM사의 블랙베리를 통해 e메일이나 메시지를 교환할 경우 이동통신사 서버를 거치지 않고 캐나다에 있는 통신센터로 전송되어 암호화하여 전달된다. 이러한 보안서비스 때문에 테러 혐의 등 범죄사건이 발생하더라도 정부는 해당 통신내용을 알 수 없는 문제가 발생한다는 것이다[3, 4]. 테러리스트의 위협이 심각한 아랍 국가들은 이러한 블랙베리의 보안서비스가 골칫거리일 수 밖에 없다. 그러나 범죄와 관련이 없는 선의의 사용자가 이런 서비스를 사용하는 경우, 전혀 인지하지 못한 상태에서 해당국가의 암호해독명령을 받았을 때 이를 준수하지 못해 범법자로 처벌받을 수 있는 위험이 있다.

이러한 상황에서 해외 여러 나라에서 사업을 수행하는 글로벌 기업의 직원이 앞에서 언급한 나라에서 블랙베리와 같은 암호기능을 제공하는 소프트웨어 또는 하드웨어 도구를 사용할 경우 해당 국가의 암호해독명령을 받았을 때 의도하지 않게 법을 위반할 위험이 있을 수 있다. 따라서 글로벌 기업의 보안 관리자들은 먼저 국가별 암호통제 정책을 이해하고, 소속 직원들이 거주 국가의 현행 암호법률에 위반하지 않도록 적절한 암호 수단 제공 및 암호통제관리 지침을 마련할 필요가 있다.

본 논문에서는 먼저 암호통제의 변화과정을 살펴보고, 현행 국가별 암호통제 정책 중 암호화된 형태로 전송되거나 저장된 데이터에 대한 법 집행기관의 합법적인 접근권한을 부여하는 암호해독명령의 개요와 이에 관한 법률 제정 배경을 살펴본다. 또한 암호해독명령과 관련한 법률과 처벌조항을 해당 국가별로 정리하고 이들 국가의 경제 규모를 비교 분석하여 글로벌 기업이 암호해독명령 관련 법률을 간과할 수 없는 이유를 제시하였다.

본 논문에서는 마지막으로 해외 여러 나라에 걸쳐 사업을 수행하는 글로벌 기업의 특성상 경제규모가 비교적 큰 해당 국가별 암호통제 관련 법률과 규제를 이해할 필요성에 대해 언급하고, 암호해독명령에 대해 효율적으로 대응하기 위해 글로벌 기업이 암호정책을 수립하는데 필요한 사항을 고찰하며, 암호통제의 기술적 수단과 관리적 지침의 수립에 대한 필요성을 제안하였다.

2. 암호통제 정책 현황

암호는 국가안보를 위한 중요 기술로 분류되어

암호가 기업 시스템에서 사용되는 것을 대부분의 국가에서 적극적으로 통제하였다. 그러나 통신 시스템이 기업들의 사업 운영에 필수 수단으로 활용되어, 1990년 초, 기업 시스템에서의 암호 사용 통제정책에 대한 격렬한 논쟁이 진행되었다. 이러한 논쟁의 결과, 1997년 초반 OECD가 「Guidelines on Cryptography Policy」를 발표하였고 이 가이드라인은 국가 암호정책에 대한 일반적인 원칙을 제안하였고 기업과 개인들이 자신의 이익을 보호하기 위해 적절한 암호 도구를 선택할 수 있는 권리와 정부의 암호에 대한 합법적 접근을 지원하는 정부의 권리를 모두 인정하며, 양측의 권리 행사에서 균형을 강조하였다.

이 가이드라인을 기반으로 각 국가에서는 암호 수출입 통제 제도, 암호관련 수사에 관한 제도, 암호해독기술 연구 등의 주제로 자국의 실정에 맞는 정책방안을 수립하기 위한 연구를 진행하여 암호정책의 기본방향을 정하고, 이를 기반으로 암호통제 관련 법률 제정을 추진하고 있다[5]. 또한 암호통제 관련 법률은 크게 암호기술의 수출입 통제정책과 암호화된 형태로 저장된 데이터에 대한 법집행기관의 합법적인 접근권한으로 구성된다.

현재 대부분의 국가들이 COCOM을 대체한 Wassenaar 협정에서 기술된 암호통제 규정을 준수한다. 여러 국가에서 특정 형태 또는 특정 국가로의 암호 수출을 통제하고 있으나, 중국과 러시아 등의 특정 국가들은 암호 수출 및 수입을 통제할 뿐 아니라, 자국 내부에서 암호기술을 사용 및 제공하는 것을 통제한다[2]. 그러나 암호는 데이터 보호 목적뿐만 아니라, 전자서명 또는 데이터의 무결성 검증 용도로 사용된다. 하지만 현 제도는 암호 용도의 무단 전환을 제어할 방법은 없는 실정이다.

3. 암호해독명령 개요와 제정 배경

암호해독명령은 범죄 또는 국가 안보를 위협하는 테러 용의자에게 암호화된 정보를 평문과 같이 이해 가능한 형식으로 제공할 수 있도록 명령할 수 있는 권한이다. 암호해독명령은 암호문에 대한 복호화를 요청할 수 있는 권리(demanding decryption)와 암호문을 복호화할 수 있는 키를 제공하도록 요청할 수 있는 권리(key delivery)로 나눌 수 있다. 또한 용의자 개인에게 복호화 명령을 내리는 경우와 용의자가 기업인 경우, 용의자 이외의 개인, 단체에게 복호화 명령을 내리는 경우로 구분할 수 있다. 국가에서 어떠한 암호통제정책을 수립하는지에 따라 암호화된 디지털 자료에 대한 접근 가능성이 차이가 날 수 있다. 만일 강력한 암호이용 통제정책을 가지고 있는 경우 암호화된 디지털 자료에 대해 쉽게 접근할 수 있어 범죄 예방이나 테러와 같은 국가안보를 위협하는 것에 대비할 수 있는 반면, 개인이나 기업들은 자신의 개인정보나 기업의 중요한 정보자산에 대한 기밀성을 보장할 수 없게 될 가능성이 높다[6].

저장된 데이터 또는 전송 도중의 데이터에 접근하는 것은 국가 보안기관 또는 경찰의 핵심 활동 요소로 간주되고 있다. 그 결과 합법적으로 전송되는 데이터를 가로채거나 저장된 데이터를 압수하며, 암호문으로부터 평문을 복원하는 다양한 형태의 법과 제도를 마련하였다.

암호는 통상적으로 기업 내부 또는 응용계층에서 적용된다. 따라서 네트워크 사업자는 암호를 해독할 수 없으며, 법 집행기관은 네트워크 사업자의 협조를 통한 암호 감청을 더 이상 할 수 없게 되었다. 그 결과 일부 국가들은 법적 절차에 따라 획득한 암호의 합법적 감청을 목적으로 법 집행기관의 암호 키 접근에 대한 관계자들의 지원을 의무화하는 법률을 제정하였다.

특히 정부가 암호에 대한 합법적 접근이 필요시 암호화된 디지털 데이터의 복호화를 위해 기술적 코드 또는 법을 이용한 방법이 있다. 먼저 기술적 코드를 이용하는 방식은 암호시스템에 법집행기관이 필요시에 쉽게 접근할 수 있도록 일종의 백도어를 설치하는 것으로, 대표적으로 미국의 Clipper Chip 시스템을 예로 들 수 있다[6]. Clipper Chip 시스템은 비공개 암호 알고리즘과 특수 마이크로프

로세서로 구성되며, 키 위탁(key escrow) 목적의 스페어 키(spare key) 기술을 지원한다. 따라서 정부는 필요시 스페어 키와 허가장(warrant)을 사용하여, 전자 정보(electronic information)의 암호를 해독할 수 있다[7]. 그리고 법을 이용하는 방식은 용의자에게 복호화를 강제할 수 있는 권한을 법으로 규정하는 것이다. 대표적인 예로는 영국의 RIPA (Regulation of Investigatory Powers Act) Part III를 들 수 있다[6].

통신 데이터는 여러 국가의 네트워크를 통해 전송될 수 있기 때문에, 사법적 감청절차는 당해 국가들 사이의 협조가 필수적이다. 그러나 암호를 사용하는 기업과 개인은 그러한 요청의 정당성과 진행 절차 및 대응 조치에 대한 기본 지식이 부족한 실정이다.

최근 주요 국가들은 프라이버시와 관련된 사회단체의 반발 때문에, 기술적 코드에 의한 강제 키 복구 정책을 포기하는 대신 암호해독명령 제도를 도입하고 있는 추세이다. 따라서 일부 국가들은 법적 절차에 따라 획득한 암호의 합법적 감청을 목적으로 법 집행기관의 암호 키 접근에 대한 관계자들의 지원을 의무화하는 법률을 제정하여 규제하고 있다.

4. 암호해독명령 관련 법률과 사례

본 논문에서는 나라별 암호통제 관련 법률 중 암호해독명령에 관한 법률이 이미 제정되어 시행되고 이에 대한 처벌 조항이 있는 법률을 중심으로 정리하였다. 일부 나라에서는 해독명령에 관한 법률 제정 문제가 아직 논의 중에 있으며 일부 국가에서는 해독명령에 관한 법률 제정 필요성이 제기되고 있고 근거 규정 마련이 추진 중이다.

프라이버시 또는 통신자유 등의 개인의 기본권 침해 논란에도 불구하고, 영국과 프랑스 그리고 싱가포르 등 전세계 10여개 국가에서 암호해독 명령 제도를 실시하고 있다. 또한 암호해독명령을 준수하지 않았을 경우 평균 2~3년의 징역형과 벌금 등 처벌 조항이 가볍지 않다. 다음은 암호해독명령에 관한 법률의 국가별 현황과 제정 배경 등을 정리한 것이다[5, 8].


Bert-Jaap Koops homepage

Crypto Law Survey

Version 26.0, July 2010

:: Bert-Jaap Koops

All rights reserved. Please credit if quoting.

Next update December 2011.

- Address list for crypto export licenses
- Mailing list announcing updates
- Maps summarizing the import, export, and domestic crypto controls around the world. Test your geographic knowledge!
- For background information, see my Ph.D. thesis, *The Crypto Controversy: A Key Conflict in the Information Society*, which is now full-text available. How can and should governments address the law-enforcement problems of cryptography?

home | related research | digital signature law survey | crypto and self-incrimination FAQ

FAQ | What's new | Sources | Table of Contents

[그림 1] Bert-Jaas Koops's Web Site[8]

4.1 프랑스

□ 관련 법률
- Law 2001-1062

□ 주요 내용
- 수사과정에 암호화된 데이터가 있으면 자격있는 사람에게 복호화 또는 복호화 키를 제공하도록 요청할 수 있다.
- 처벌 조항이 최소 2년의 징역형인 범죄 조사 과정에 필요하다면, 경찰은 암호화된 데이터에 대한 복호화를 요청할 수 있다.
- 2002년 8월 7일 제정된 Decree 2002-1073에 근거하여 내무부에 기술 지원센터(Technical Assistance Center)가 설립됨.

□ 처벌
- 최대 3년 징역형 또는 최대 45,000유로 벌금형
- 암호해독이 범죄를 예방하거나 피해를 줄일 수 있는 효과를 거둘 수 있었으나 암호해독 명령에 응하지 않아 범죄가 발생한 경우에는 최고 5년 징역형과 75,000유로 벌금형

※ 프랑스는 식민지이었던 아프리카 나라들과 국가안보 관련 소통이 많은 이유로 전통적으로 강력한 암호통제 정책을 펴오고 있다. 프랑스는 바세나르 협정의 회원국임에도 불구하고 협정에서 규정한 수출통제 제외 암호품목 목록을 적용하지 않

았었다. 그러나 1999년 이후 암호제품의 수입은 완전 자율화가 되었다. 하지만, 여전히 암호해독명령과 관련해서는 국가에서 강력하게 통제하고 있으며 처벌조항도 다른 나라에 비해 무겁다.

4.2 인도

□ 관련 법률
- The Information Technology Act 2000

□ 주요 내용
- 국가 안보나 범죄 예방의 목적으로 정부 기관은 컴퓨터 자원을 통해 전송되는 정보에 대해 획득을 지시할 수 있다.
- 법에서 지정한 기관의 요청이 있을 때, 컴퓨터 자원에 대한 책임을 지고 있는 등록자 또는 사용자는 정보를 복호화하기 위한 모든 설비와 기술적인 도움을 받을 수 있다.

□ 처벌
- 최대 7년 징역형

4.3 남아프리카공화국

□ 관련 법률
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act

□ 주요 내용
- 경찰은 암호화 통신에 대해 복호화를 요구할 권한이 있다.
- 경찰은 지정된 판사에게 암호해독 지시를 요청하는 권한을 갖는다(art. 21).
- 통신 감청 이전 또는 도중에 암호해독지시가 가능하다.
- 수신인은 복호화 키를 제공하거나 복호화에 도움을 주어야 한다(art. 29).
- 복호화 비용은 보상될 수 있다(art. 31).

□ 처벌
- 자연인과 피고용인에 대해서는 최대 2백만 Rand 벌금 또는 최대 10년 징역형
- 법인에 대해서는 5백만 Rand 벌금

4.4 아일랜드

□ 관련 법률
- The Electronic Commerce Act 2000(nr. 27)

□ 주요 내용
- 만약 범죄로 의심할 상당한 이유가 있으면, 판사는 수색영장을 발부할 수 있다.
- 영장을 통해 수사관은 압수한 자료에 쉽게 접근할 수 없거나 이해할 수 없는 형태의 정보 또는 전자 통신 정보를 포함되어 있으면, 정보 또는 전자통신 정보를 이해할 수 있는 형태로 요청하는 권한을 갖는다.
- 수사관은 사용자에게 복호화만 요청할 수 있고, 키 또는 패스워드를 넘기도록 요청할 수 없다. 그리고 수사과정에서 압수한 자료와 관련한 것에 대해서만 권한을 행사할 수 있다.

□ 처벌
- 유죄[1)]

4.5 호주

□ 관련 법률
- The Cybercrime Act, No. 161, 2001

□ 주요 내용
- 치안판사의 명령에 따라 암호키 제출 또는 암호화된 데이터의 복호화를 요구할 수 있다.
- 컴퓨터에 저장되어 있거나 컴퓨터로 접근가능한 증거 자료를 의심하는 상당한 이유가 있고 명시된 사람이 암호와 관련된 지식을 가진 용의자이거나 컴퓨터 소유자 또는 임차인일 때 암호해독명령을 내릴 수 있다.

□ 처벌
- 최대 6개월 징역형

1) 본 논문에서는 Bert-Jaas Koops 웹사이트를 참조하였는데, 아일랜드의 경우, 처벌 항목에 “What is the penalty for this?”란 질문만 명시하고 있어 자세한 처벌 조항은 알 수 없음.

4.6 벨기에

□ 관련 법률
- Information-science crime

□ 주요 내용
- 수사판사는 암호화 서비스에 대한 특별한 지식이 있다고 의심하는 사람에게 작업에 대한 정보를 제공하거나 서비스에 대한 접근 또는 복호화 방법을 제공하도록 명령할 수 있다.
- 수사판사는 적정한 사람에게 가능한 범위 내에서 복호화하도록 명령할 수 있다(판사가 명령한 형식으로 데이터에 접근가능하게 함).
- 비공개 권리를 갖고 있는 용의자 또는 사람에게는 복호화에 대한 이 명령을 내릴 수 없다.
- Article 12에는 감청한 암호화된 통신에 대 해 유사한 조항이 있다. 그러나 여기에는 비공개 권리를 가진 사람에 대한 예외도 없고 국가에 대한 민사적인 법적 책임 조항도 없다.

□ 처벌
- 6~12개월 징역형 그리고/혹은 BEF20k~BEF26 벌금

4.7 말레이시아

□ 관련 법률
- Computer Crimes Act 1997
- Digital Signature Act 1997
- Communications and Multimedia Act

□ 주요 내용
- 조사과정 중에 컴퓨터 운영 또는 자료와 관계가 있는 사용자와 사람에게 위법 행위와 관련되어 사용되었다는 상당히 의심되는 프로그램 또는 데이터 또는 자료에 접근하도록 충분한 도움을 제공하도록 요청할 수 있다.
- 조사과정 중에 컴퓨터 또는 다른 것에 저장되어 있는 컴퓨터 데이터에 대해 접근할 수 있도록 명령한다. 이 접근에는 컴퓨터 데이터를 이해할 수 있는데 요구되는 필요한 패스워드, 암호 코드, 해독 코드, 소프트웨어 또는 하드웨어를 제공하는 것도 포함된다.

□ 처벌
- 100,000링깃(Ringgit) 그리고/혹은 2년 징역형

4.8 네델란드

□ 관련 법률
- Dutch Code of Criminal Procedure(DCCP)
- Wiretapping of Public Telecommunicationsv Networks and Services Decree

□ 주요 내용
- 압수 수색시 컴퓨터에서 암호화된 정보가 발견 되면, 경찰은 암호 방법을 알 것으로 판단되는 사람에게 정보를 복호화하도록 명령할 수 있다.
- 자료 제출 명령에 의하여 경찰에 제출된 데이터에서 암호화된 정보가 발견되면, 경찰은 암호 방법을 알 것으로 판단되는 사람에게 정보를 복호화 하도록 명령할 수 있다.
- 만약 암호화된 통신이 감청에 통해 탐지되면, 경찰은 암호 방법을 알 것으로 판단되는 사람에게 정보를 복호화 하도록 명령할 수 있다.
- 적법한 감청의 경우, 통신제공자는 아래 법에 의해 그들이 적용한 암호를 해제하도록 요청받는다.

□ 처벌
- 최대 3개월 징역형

4.9 태국

□ 관련 법률
- The Thailand Computer Crime Act, B.E. 2550 of 2007

□ 주요 내용
- 컴퓨터 범죄를 수사하면서 법원의 허가를 받은 수사관은 컴퓨터 데이터를 디코딩하는 것이 가능하고 컴퓨터 데이터의 암호와 관련이

있는 사람에게 컴퓨터 데이터를 디코딩하도록 명령할 수 있거나 관련 전문가와 협업할 수 있다.

□ 처벌

- 벌금 200,000바트 그리고 해독 명령을 수행할 때까지 추가적으로 최대 5,000바트의 일일 벌금을 지불하도록 할 수 있다.

4.10 싱가포르

□ 관련 법률

- The Computer Misuse Act, 1999

□ 주요 내용

- 검사의 동의를 얻은 경찰은 범죄 조사 목적으로 언제든지 해독 정보, 코드, 기술에 접근할 수 있다.
- 경찰은 범죄와 연관된 가능성이 있는 컴퓨터의 운영과 관련이 있는 사용자에게 타당한 기술적 지원 또는 기타 지원을 제공하도록 요청할 권한이 있다.
- 해독 정보를 소유한 사람에게 범죄 조사의 목적에 필요한 데이터를 복호화하기 위해 필요한 해독 정보에 대한 접근을 요청할 수 있다.

□ 처벌

- 최대 S$10,000벌금 또는 3년 징역형

4.11 영국

□ 관련 법률

- Regulation of Investigatory Powers Act 2000

□ 주요 내용

아래의 경우에 해독 명령 권한이 주어짐

- 정보기관, 경찰, 세무국 등이 암호화된 데이터를 적법하게 획득한 경우
- 암호 해독이 국가 안보, 범죄 예방, 수사, 또는 영국의 경제적 이익에 필요한 경우
- 법에 정한 권한 또는 의무의 효과적인 행사 또는 적정한 성능을 위해 필요한 경우
- 해독 요구가 유일한 방법이거나 이에 준하는 경우
- 용의자가 복호화 키를 소유하고 있다고 확신되는 경우
- 회사에 근무하는 사람에 대해 적용하는 특별한 경우
- 복호화하는데 여러 키가 사용되는 경우
- 복호화를 요청받은 사람이 키를 가지고 있지 않으면, 키를 복구하는데 필요한 모든 정보를 제공해야 한다.
- 전자 서명키로만 사용되는 키는 제외

□ 처벌

- 최대 2년 징역형

※ 영국은 최근 암호 사용 비율이 증가하였고 급진주의적 아일랜드 공화국군(PIRA)가 무장해제한 반면 영국의 이라크전쟁 개입 이후 아랍권에 의한 테러가 증가했으며, 테러에 암호 사용 사실이 공개되면서 테러 및 범죄용의자에 대한 암호해독명령 실시를 위한 법제정 분위기가 조성되었기 때문이다[6].

이상 11개국에 대한 암호해독명령 관련 법률에 대해 정리하였다. 트리니다드 토바고, 안티구아와 바브다 등 일부 국가에 대한 법률은 지면의 제한상 생략하였다.

프랑스, 영국 등 이 장에서 기술한 국가들의 암호해독명령 법률 제정 배경에 대한 고찰로서 정보사회지수를 통해 분석해보면 다음과 같다.

세계 50여개 국가를 대상으로 컴퓨터(가정 내 PC 보급대수, 전체 IT 지출 중 소프트웨어 지출(%), GDP 대비 IT서비스 지출(%), GDP 대비 IT 지출(%) 등), 인터넷(인터넷 이용자 규모, 가구 인터넷 접속 비율(%), 모바일인터넷 이용자 규모, 전자상거래 지출 규모 등), 통신(초고속인터넷 도입현황, 무선통신 서비스 현황, 모바일 장비 현황 등), 사회적 측면(교육수준, 시민자유권, 정부 부패정도 등)을 포함한 국가별 정보화 수준을 종합적으로 측정하는 정보사회지수(Information Society Index)

를 보면 네델란드(6위), 영국(10위), 호주(12위), 싱카포르(13위), 벨기에(16위), 프랑스(18위)이다[9].

따라서 암호해독명령 관련 법률을 제정한 국가는 정보화 수준이 높아 비교적으로 일반사용자들의 암호기술 사용 비율이 높다고 판단된다. 이에 따라 암호기술 사용의 역기능을 방지하기 하기 위해 암호해독명령 관련 법률 제정이 필요했을 것이라 판단된다.

4.12 암호해독명령 법률 제정국가의 경제 규모 분석

다음은 세계은행(World Bank)에서 세계 200개가 넘는 국가별 GDP를 종합해 발표한 순위자료를 참조하여 앞에서 기술한 암호해독명령 관련 법률을 제정한 국가의 2010년 세계 GDP 기준 순위이다[9].

〈표 1〉 2010년 세계 GDP 기준 순위별 정리

국가	GDP($)	순위
프랑스	2,560,002,000,000	5위
영국	2,248,831,038,714	6위
인도	1,727,111,096,363	9위
호주	924,843,128,521	15위
네델란드	779,356,291,391	16위
벨기에	469,374,172,185	21위
남아공	363,703,902,727	28위
태국	318,522,264,429	30위
말레이시아	237,796,914,597	36위
아일랜드	211,389,968,514	42위
싱가포르	208,765,019,308	43위

<표 1>에 따르면, GDP 순위가 높은, 즉 경제규모가 비교적 큰 선진국에서 암호해독명령 관련 법률을 제정하여 시행하고 있다는 점을 알 수 있다. 이런 상황을 고려할 때 전 세계 여러 나라에서 사업을 하는 글로벌 기업들은 해당 국가의 암호해독명령에 관한 법률을 고려할 필요성이 있다고 판단된다.

4.13 암호해독명령 집행 사례

다음은 최근 영국과 미국에서 암호해독명령 집행 사례이다[8].

영국의 최고 감독 위원회에서 작성한 연간보고서에 따르면, 2008년 4월부터 2009년 3월까지, NTAC (National Technical Assistance Centre)는 27개의 암호해독명령에 대한 요청을 받았다. 이중 15개가 법원의 승인을 받았다. 하지만 11명이 해독명령 준수를 하지 못하였고, 이중 7명이 기소되었고 2명이 유죄선고를 받았다. 2009년 4월에서 2010년 3월까지는 NTAC가 38개의 암호해독명령에 대한 요청을 받았고, 이중 22개가 법원의 승인을 받았다. 17개의 암호해독명령이 집행되어 6개의 암호해독명령은 준수된 반면, 7개는 준수되지 못하였다(나머지는 연기됨). 암호해독명령을 준수하지 못한 5명은 기소되었으며 이중 1명은 유죄선고를 받았다. 하지만 이 보고서에는 해독명령을 준수하지 못한 것에 대한 자세한 처벌 정보는 없다.

2009년 미국 세관은 Boucher라는 사람의 입국을 저지하면서 노트북을 조사했다. 그의 노트북에서 “2yo getting raped during diaper change”라는 이름의 파일을 발견했으나 파일을 열수가 없었다. 세관 직원은 Boucher에게 노트북에 저장되어 있는 모든 이미지 파일을 보여줄 것을 요청했다. 이 요청에 따라 ‘Z’ 드라이브를 탐색했고 어린이 포르노 파일처럼 보이는 것이 발견되었다. 이 노트북은 압수되었으나 ‘Z’ 드라이브는 비밀번호 없이 열람이 되지 않아 Boucher에게 비밀번호 제출 명령이 내려졌다.

5. 글로벌 기업의 대응 방안

오늘날 글로벌 기업들은 여러 국가에 걸쳐 사업 시스템을 운영하고 있으며, 다른 나라에서 근무하거나 해외로 출장 가는 직원들은 원격지에서 암호 솔루션을 이용해 해당 기업의 국내 시스템을 사용할 수 있다. 이들 기업들은 시스템 내부에서 운용

되는 암호 기술과 관련하여 앞에서 언급한 암호해독명령 관련 법률을 제정하고 규제하는 나라의 통제를 간과하거나 암호사용 자체를 직원들에게 고지하지 않는 경향이 있다. 이로 인해 직원들은 시스템을 이용하는 도중에 전혀 인지하지 못한 상태에서 해당국가의 암호해독명령을 받았을 때 이를 준수하지 못해 범법자로 처벌받을 수 있는 위험이 있다.

따라서 글로벌 기업에서는 시스템이 이용되는 국가의 법제도적 통제를 충분히 고려하여 시스템을 구축하여야한다. 특히 IT서비스 회사의 시스템을 활용하거나 클라우드 서비스를 활용하는 기업은 국가의 암호사용 통제제도를 충분히 인식하고, 직원들에게도 암호통제 정책에 따른 법 위반 가능성을 고지해야한다. 또한, 글로벌 기업은 암호해독명령과 관련하여 법 집행기관들이 암호화된 데이터에 대해 해독 명령을 내린 경우 어떠한 위험이 있을 수 있는지 먼저 분석할 필요가 있다. 아래는 암호해독명령을 받았을 때 발생할 수 있는 취약점들이다.

- 사용자가 파일 등 암호화 시 사용했던 비밀번호를 기억하지 못하는 경우
- 암호화에 사용된 키 정보를 분실한 경우
- 암호화 자체가 네트워크 단계에서 처리되어 암호 사용자 또는 기업들은 복호화 지원이 원천적으로 불가능한 경우
- 기업에서 사용하는 암호 기술이 포함된 상용제품의 경우 키관리 및 키복구 기능 미인지 경우
- 이동형 컴퓨팅 장치(노트북, 태블릿 PC 등)에 기업이 더 이상 사용하지 않아 복호화 지원이 불가능한 암호화 솔루션으로 암호화된 데이터가 저장된 경우
- 'perfect-forwad secrecy'[2] 프로토콜을 사용하는 통신 장비를 사용한 경우[8]

2) 세션이 종료된 후 사용되었던 세션 키를 없애는 프로토콜로서 세션 키를 복구할 방법이 없다.

실수에 의해 암호해독 명령을 위반한 경우에도 처벌받을 가능성이 존재한다.

최근 기업에서 정보보호관리체계를 구현하여 적용하고 있다. 하지만 일반적인 정보보호관리체계의 암호통제 관련 정책은 포괄적인 내용을 기술하고 있기 때문에 암호해독명령 준수를 위해서는 세부 관리 지침 수립을 수립이 필요하다. 다음은 한국인터넷진흥원에서 시행하고 있는 정보보호관리체계(ISMS, Information Security Management System)의 암호 통제 분야 요구사항이다[11].

[암호 정책]

암호사용에 대한 정책을 수립하여야 한다.

- 문서화된 암호 정책이 있는가?
- 암호 정책에는 다음 사항을 포함하고 있는가?
  - 암호를 사용해야 하는 경우
  - 경우에 따른 암호화 방법 또는 필요한 신뢰 정도
  - 안전한 암호 프로그램의 배포관리
  - 전자서명 또는 부인봉쇄 서비스의 신뢰 정도

[암호 사용]

암호 정책에 따른 암호 사용시 적절한 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.

- 암호 정책에 따라 암호화가 필요한 경우, 적절 한 알고리즘과 키 길이를 결정하여 사용하고 있는가?
- 암호 정책에는 전자서명 또는 부인봉쇄 서비스시 암호화 적용에 대한 내용을 포함하고 있고, 이에 따라 이행하고 있는가?

[키관리]

암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구 방안을 마련하여야 한다.

- 암호 키에 대한 관리지침과 절차 및 방법이 마련되어 있고, 이에 따라 관리되고 있는가?
- 암호 키 복구 방안을 마련하여 이에 따라 키가 복구되는가?

암호통제 정책 수립시 더 세부적으로 고려해야 할 사항으로 Chris Sundt의 논문에서 제안한 사항을 살펴보면 다음과 같다[2].

- 암호 사용과 관련된 전반적인 접근방식 설정
- 조직 내부와 제 3자와의 협력과정에서 암호 사용 위치를 결정하는 절차 정의
- 규제와 법적 문제점 그리고 암호 설정과 관리 책임자와 관련된 정책 정의
- 키 관리 정책과 키 생성 및 유지 책임자 정의
- 정책 구현의 책임자 정의
- 정책 준수와 정책 유지 방법 정의

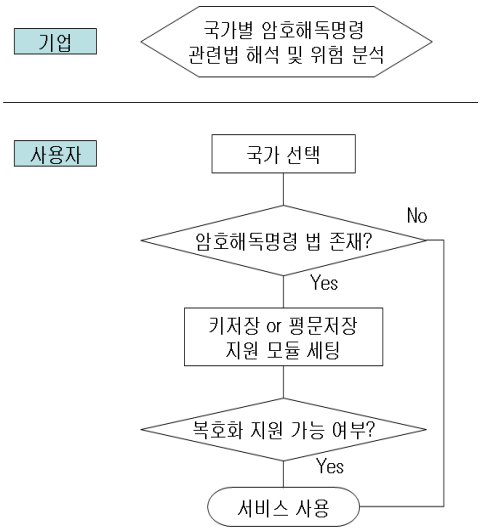
따라서 글로벌 기업의 정보보호책임자는 각 나라별 암호해독명령 관련 법률을 위반하지 않도록 해당 국가의 관련 법률을 충분히 숙지하여 암호해독명령 불복종에 따른 기업의 손실 위험을 분석하고, 앞에서 언급한 한국인터넷진흥원의 정보보호 관리체계와 Chris Sundt의 논문에서 제안한 암호통제 정책 수립 시 고려해야하는 사항들을 충분히 반영해서 세부 관리 지침을 수립하고, 사용자에게 이에 대한 사항을 고지하고 교육할 필요성이 있다.

세부 관리 지침의 예를 들면 기업의 즉각적인 통제를 벗어날 수 있는 장치, 즉 이동형 컴퓨팅 장치(노트북, 태블릿 PC 등), 이동형 저장장치(USB 저장장치, 외장형 하드 등)에 대한 암호솔루션에 대한 키 관리와 암호해독명령 준수에 대한 사항도 고려할 필요성이 있다. 그리고 기업이 현재 사용하지 않는 암호솔루션으로 암호화된 데이터의 저장여부를 확인하는 절차도 고려해야 한다. 왜냐하면 암호해독명령을 받았을 때 복호화 지원이 불가능하기 때문이다.

다음은 글로벌 기업에서 상용 암호장비를 구입할 때 암호해독명령 관련 법률에 대응하기 위해 고려해야하는 사항을 VPN 장비 도입의 예를 들어 설명한다.

기업 환경에서 VPN의 도입은 보안과 네트워크 인프라에 많은 변화가 수반되므로 도입 사유와 요구사항을 정의하고, 제안요청서(Request For Proposal : RFP) 발송과 접수된 제안서 평가 후, 시범 서비스나 벤치마크 테스트(Bench Mark Test : BMT)를 통해 세부 기능 평가를 진행한 후 결과를 취합하여 최종 제품을 선정하는 것이 일반적인 절차이다[12]. 하지만 이러한 도입과정에서 암호해독명령에 대응하기 위한 키 관리와 키 복구에 대한 부분을 명세서에 명확히 언급하고 관리할 필요가 있다.

또한, 기업들은 자체 개발한 암호 지원 제품 및 서비스를 활용할 수 있다. 하지만, 다양한 암호기술이 내장된 다양한 상용제품도 사용하기 때문에, 암호가 사용되는 위치를 결정하는 것과 마찬가지로 암호가 사용되는 제품과 서비스를 정확히 파악하는 것도 중요하다. 그리고 암호해독명령을 받았을 경우 사용자 및 관리자들은 키 관리 지침 및 절차에 따라 해당국가의 해독요청을 준수할 필요성이 있다.



[그림 2] 암호해독명령 준수에 필요한 어플리케이션 흐름도

암호해독명령 준수를 위한 기술적 수단으로서 필요한 어플리케이션에 관한 제안은 다음과 같다.

사용자 편의성을 고려하여 사용자 측에서는 근무할 또는 출장갈 국가만 선정하면, 해당 국가의

암호해독명령 관련 법률의 유·무 확인과 암호해독명령을 준수하는데 필요한 키복구 또는 평문 제출과 같은 요구사항을 이행할 수 있는 모듈을 자동으로 설정할 수 있다. 그리고 현재 기업의 시스템에서 사용하지 않는 암호솔루션으로 암호화된 데이터의 저장여부를 자동으로 확인하는 과정을 지원하는 어플리케이션을 개발하여 제공할 필요가 있다. [그림 2]는 앞에서 언급한 어플리케이션에 대한 간략한 흐름도이다.

6. 결론과 향후 연구과제

해외 여러 나라에서 사업을 하는 글로벌 기업들은 암호해독명령과 관련한 국가별 통제를 충분히 인식하고, 이를 준수해야 한다. 그러나 암호통제 제도는 국가별로 서로 다르며, 한 국가 내부에서도 법과 제도에 대한 해석이 불분명할 수 있는 환경에서, 기업들은 적절한 위험관리 절차를 통해 암호 사용과 관련된 위험에 대처해야 한다.

본 논문에서는 암호관련 여러 법률 중 암호해독명령 관련 법률을 제정하고 이에 대한 규제를 실시하는 국가를 구분하여 해당 법률과 처벌 조항을 정리하고 해당 국가의 경제 규모를 비교분석하여 글로벌 기업이 암호해독명령 관련 법률을 간과할 수 없는 이유를 제시하였다. 이에 따라 글로벌 기업이 암호해독명령에 대해 효율적으로 대응할 수 있도록 암호정책 수립 시 필요한 사항을 살펴보았고 암호통제의 기술적 수단과 관리적 세부 지침 수립의 필요성을 제안하였다.

향후 국내에서 영업활동을 하는 글로벌 기업에 대한 암호해독명령 적용에 관한 문제에 대해 연구가 필요하다. 국내에는 아직 암호해독명령 관련 법률이 제정되지 않았기 때문에 향후 법 제정 추진시 지금까지 제기된 국가의 통제와 프라이버시 및 기업 비밀 보호간의 논쟁 문제를 해결할 수 있는 방법인 신뢰할 수 있는 제 3의 기관(TTP, Trusted Third Party) 설립에 대한 논의가 필요할 것이다.

참 고 문 헌

[1] Nehaluddin Ahmad, “Restrictions on cryptography in India-A case study of encryption and privacy”, *Computer Law and Security Review*, Vol.25(2009), pp.173-180.

[2] Chris Sundt, “Cryptography in the real world”, *Information Security Technical Report*, Vol. 15, No.1(2010), pp.2-7.

[3] http://www.guardian.co.uk/technology/2011/apr/18/uae-blackberry-emails-secure.

[4] http://www.nytimes.com/2010/08/02/business/global/02berry.html?_r = 1&pagewanted = all.

[5] 권현조, 전길수, 이재일, “국내외 암호관련 법제도 현황”, 「정보보호학회지」, 제15권, 제2호(2005), pp.37-53.

[6] 백승조, 임종인, “피의자 개인의 암호이용 통제정책에 대한 연구”, 「정보보호학회논문지」, 제20권, 제6호(2010), pp.271-288.

[7] Zelezny, J. D., Communications Law, p.493.

[8] Bert-Jaas Koops’s web site, http://rechten.uvt.nl/koops/cryptolaw.

[9] http://www.idc.com/groups/isi/main.html.

[10] http://data.worldbank.org/data-catalog/GDP-ranking-table.

[11] http://isms.kisa.or.kr, “정보보호관리체계 인증심사 기준”, 2007.

[12] 박광청, 이규호, 조은영, “기업 환경 VPN 실전 구축 가이드”, 「시사컴퓨터」, 2004.

◈ 저 자 소 개 ◈

손 상 일 (ssidsc@nate.com)

현재 국방부에 재직 중이며, 국방정보전대응센터장을 역임하였고, 수원대학교 컴퓨터학 박사과정에서 암호통제 및 암호키 관리에 대해 연구하고 있으며, 주요 관심분야는 암호키, 네트워크 보안, 침입탐지 및 차단시스템, 정보전, 사이버테러, 침해사고 조사이다.

손 유 승 (useung@daum.net)

현재 국방부에서 정보보호 업무를 수행하고 있으며, 수원대학교 컴퓨터학과 박사과정에서 암호기술 및 정책, 사이버전, 침해사고 대응기술, 웹 응용프로그램 관련 정보보호 분야를 심도 있게 연구하고 있다.

김 영 권 (shark13659@naver.com)

현재 국방부에서 정보보호 업무를 수행하고 있고, 정보보호 교관을 역임하였으며, 수원대학교 컴퓨터학과 박사과정에 재학 중에 있다. 주요 관심분야는 정보보호관리체계, 정보전, 사이버테러, 침해사고 조사이다.

고 승 철 (goh5703@hanmail.net)

현재 수원대학교 IT 대학 정보보호학과 교수로 재직 중이다. 연세대학교 수학과 및 동 대학원를 졸업하고, 포항공대에서 전산수학 전공으로 이학박사 학위를 취득하였다. Pattern Recognition Letters, Lectures notes in computer science 등에 논문을 게재하였으며, 국내 학술지 및 국내외 컨퍼런스에도 20여편의 연구 결과를 발표하였다. 주요 관심분야 정보보호, 알고리즘, computational complexity 등이다.