Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1549

개인정보보호 관련 법령의 내용과 보안제품 분포간의 연관성 분석

김 민 정,[1†] 이 정 원,[1] 유 진 호[2‡]
[1]펜타시큐리티시스템(주), [2]상명대학교

Study on the Association between Personal Information Protection Legislation and Information Security Product

Min-Jeong Kim,[1†] Jung Won Lee,[1] Jinho Yoo[2‡]
[1]Penta Security Systems Inc., [2]Sangmyung Univ.

요 약

최근 몇 년간 크고 작은 개인정보 유출 사고가 끊이지 않고 있다. 그에 따라 개인정보보호 관련 법령이 지속적으로 제·개정 되고 있으며, 정보보호 제품도 발전하고 있다. 또한 보안 적합성 검증인 CC인증, 국정원 검증 암호모듈(KCMVP) 등 정보보호 제품에 대한 인증체계도 엄격히 이뤄지고 있다. 본 논문에서는 개인정보보호 관련 법령인 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률과 신용정보의 이용 및 보호에 관한 법률, 전자금융거래법의 5개 법령의 물리적, 기술적, 관리적 보호조치 중 기술적 보호조치의 키워드를 분석 및 분류하였다. 그리고 법령상 기술적 보호조치와 CC인증 및 KCMVP 제품군과 지식정보보안산업협회(KISIA) 회원사의 정보보호 제품 분포와의 연관성을 분석하였다.

ABSTRACT

For the past few years, personal information breach incidents, great and small, occurred constantly. Accordingly, the Personal Information Protection related Ordinances are enacted and amended persistently, and the information security products also keep advancing and developing in the same way. There are the certification systems such as Common Criteria Evaluation and Validation(CC) and Korea Cryptographic Module Validation Program(KCMVP) for the information security products. These are also strictly carried out. This paper analyzes and categorizes the 5 Personal Information Protection related Ordinances in the aspects of technical protection measures by using key words. Here are the 5 related ordinances; 'the Personal Information Protection Act', 'the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc', 'the Act on the Protection, Use, Etc, of Location Information', 'the Use and Protection of Credit Information Act', and 'the Electronic Financial Transactions Act.' Moreover, this study analyzes the association between the technical protection measures in the 5 relevant laws and the information security products that are obtaining the CC Evaluation & Validation(CC) and the products that are now produced at KISIA's member companies.
Keywords: Personal Information Protection, CC, KCMVP, KISIA

I. 서 론

2008년 옥션과 GS칼텍스를 시작으로 2010년 신세계몰, 아이러브 스쿨, 대명리조트, 러시앤캐시, 2011년 농협, 현대캐피탈, 네이트, 싸이월드, 넥스, 2012년 KT, EBS, 2013년 IBK캐피탈, 한화손해

Received(07. 08. 2015), Modified(09. 25. 2015), Accepted(09. 25. 2015)

† 주저자, korea.minjeong@gmail.com
‡ 교신저자, jhyoo@smu.ac.kr(Corresponding author)

보험, 메리츠 화재, SC은행, 씨티은행, 2014년 국민·롯데·농협 카드, KT, 호텔엔조이, 대한의사협회, 대한치과의사협회, 한의사 협회, 티몬, 통신 3사[1]에 이르기까지 지난 몇 년간 기업과 기관의 크고 작은 개인정보와 중요 정보의 유출 사고가 지속적으로 일어나고 있다. 중국의 한 검색 사이트에서는 우리나라 국민 수의 몇 배가 되는 개인정보가 돌아다니고 있다고 하니, 결국 피해를 입지 않은 국민이 없을 정도인 것이다.

이러한 사고를 예방하기 위해 국가에서는 개인정보의 보호를 위하여 관련 법령을 마련하고 지속적으로 개정·시행하고 있다. 정보보호 제품 역시 개인정보 유출 사고를 예방하기 위해 발전 하고 있으며 이러한 정보보호 제품의 보안 적합성 검증인 CC인증, 국정원 검증 암호모듈(Korea Cryptographic Module Validation Process, 이하 KCMVP) 등의 인증체계도 엄격히 이뤄지고 있다.

본 논문에서는 개인정보보호 관련 법령에 명시되어 있는 관리적, 물리적, 기술적 보호 조치 중 기술적 보호 조치에 초점을 맞추어 CC인증 제품 및 지식정보보안산업협회(이하 KISIA) 회원사의 정보보호 제품이 개인정보보호 관련 법령이나 규제에 많이 언급되어 있는 제품 중심으로 활성화 되었을 것이라 판단하고 이를 검증하고자 한다.

II. 기존 논문 및 개인정보보호 관련 법령 분석

신영진[2]은 개인정보를 보호하기 위한 기술적 보호 조치의 개선점을 제도적, 기술적, 인증제적 측면으로 정리하였다. 그 중 기술적 측면으로는 빅데이터를 활용한 보안 분석, 데이터 누출방지 솔루션, 디지털 포렌식, 추적금지, 지능형 보안, 융·복합 보안, 2채널 인증 등의 신기술 활용, 기술지원을 위한 컨설팅 활성화 등의 개선점을 도출했다.

김영희, 국광호[3]는 법률에서 밝힌 안전성 확보조치 기준 및 개선 연구의 경우 기준 항목을 평가한 전문가 집단의 업무 영역, 전문도 등의 특성에 대한 분류가 되지 않고 동일한 관점에서 평가되어, 개인정보 취급기관에서 기준적용을 위한 의사결정 방향에 대한 신뢰성을 주지 못하고 있다고 지적하였다. 이에 연구를 통해 개인정보의 안전성 확보조치 기준에 대해 전문가와 실무자 대상으로 가중치를 부여하였다. 전문가 집단은 내부관리계획, 접근 권한의 관리 순으로 우선순위가 높았다. 반면 실무자 대상의 경우 개인정보의 암호화 저장, 비밀번호 관리, 내부관리계획 순으로 우선순위가 높았다.

홍영란, 김동수[4]는 CC인증 도입이 10년 이상이 지나면서 실무자의 CC인증에 대한 긍정적 인식에 대해 실증적으로 증명하였다. 연구에 따르면 CC인증을 해본 경험이 있는 회사들은 CC인증이 보안성 강화의 중요한 요소임을 인정하고 있었고, 개발벤더에 근무하는 CC인증 담당자들은 제품 기획 등에 CC인증의 기본원칙을 반영시키고 있었다.

2.1 개인정보보호법(Act1)

개인정보보호법 제24조 제3항에 따르면 개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다고 명시되어 있다[5].

또한 법 제29조에는 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적·물리적 조치를 하여야 한다고 명시되어 있다[5].

2.1.1 개인정보의 안전성 확보조치 기준

행정자치부의 행정규칙인 개인정보의 안전성 확보조치 기준에는 개인정보처리시스템에 접속할 수 있는 개인정보 취급자 별로 사용자 계정을 발급하도록 하고 있으며, 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 IP주소 등으로 접속 권한 제한 및 불법 개인정보 유출 탐지를 하도록 하고 있다. 또한 가상사설망(VPN, Virtual Private Network) 또는 전용선 사용, 인터넷 홈페이지의 취약점 점검, 모바일 기기의 보호조치, 개인정보를 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우 암호화, 접속기록 보관 및 관리, 보안 프로그램의 주기적 업데이트 및 백신소프트웨어 설치 등의 조치를 하도록 하고 있다[6].

2.1.2 표준 개인정보보호 지침

행정자치부의 표준 개인정보보호 지침에는 개인영상정보의 안전성 확보를 위한 조치가 포함되어 있다.

제51조에 따르면 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 접근 통제 및 접근 권한의 제한조치를 해야 한다. 또한 개인영상정보를 안전하게 저장·전송할 수 있도록 네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치를 해야 하며 영상 저장 시 비밀번호 설정 등을 하도록 하고 있다. 또 처리기록의 보관 및 위변조 방지를 위한 조치를 하도록 하고 있다[7].

2.2 정보통신망 이용촉진 및 정보보호 등에 관한 법률(Act2)

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조에 따르면 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 기술적·관리적 조치를 하도록 하고 있다. 여기에는 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단 시스템 등의 접근 통제장치와 접속기록의 위변조 방지를 위한 조치, 개인정보를 안전하게 저장·전송할 수 있는 암호화기술, 백신소프트웨어의 설치 등이 명시되어 있다[8].

2.2.1 시행령

시행령 제15조에 따르면 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행과 침입차단시스템 및 침입탐지시스템을 설치·운영, 외부인터넷망을 차단하도록 명시하고 있다. 또한 개인정보처리시스템에 대한 접속기록의 위변조 방지를 위한 조치와 개인정보가 안전하게 저장·전송될 수 있도록 비밀번호의 일방향 암호화, 개인정보의 암호화 저장, 보안 서버 구축 등의 조치를 하고, 백신소프트웨어를 설치 후 주기적으로 갱신, 점검하도록 하고 있다[9].

2.2.2 정보보호조치에 관한 지침

미래창조과학부의 정보보호조치에 관한 지침의 기술적 보호조치는 네트워크 보안, 정보통신설비 보안으로 분류되어 있다.

네트워크 보안으로는 모니터링 도구를 이용한 트래픽 모니터링, 무선 서비스 시 사용자 인증과 데이터 암호화, 침입차단 시스템, 침입탐지시스템의 설치 운영 등이 있다.

정보통신 설비 보안을 위해서는 웹서버의 단독 운영, DNS 서버의 설정파일 백업, DHCP 서버의 로그기록 유지·관리, DB 서버의 망 분리, 로그기록 유지·관리 등을 하도록 하고 있으며, 접근제어기능, 주기적 취약점 점검 실시, 시스템 접근통제, 주기적 보안패치, 중요정보의 암호화 저장 등의 내용이 명시되어 있다[10].

2.2.3 개인정보의 기술적·관리적 보호조치 기준

방송통신위원회의 개인정보의 기술적·관리적 보호조치 기준에 따르면, 개인정보처리시스템에 대한 접근권한 설정과 접속 시 공인인증서 등의 안전한 인증수단을 적용하도록 하고 있다. 또한 개인정보처리시스템에 대한 접속권한을 IP주소로 제한하고 분석하여 불법적인 개인정보 유출 시도를 탐지하도록 하고 있으며, 물리적·논리적 망분리를 하도록 하고 있다.

개인정보처리시스템에 접속한 기록은 보존·관리하도록 하고 있다. 그리고 개인정보는 암호화 하여 저장하고, 송·수신 할 때에는 보안서버로 SSL을 설치하거나, 암호화 응용프로그램을 설치하도록 하고 있다. 또 백신 소프트웨어를 설치하여 주기적으로 갱신·점검하도록 하고 있으며 개인정보의 조회, 출력 시 마스킹하여 표시하도록 하고 있다[11].

2.3 위치정보의 보호 및 이용 등에 관한 법률(Act3)

위치정보의 보호 및 이용 등에 관한 법률 제16조에 따르면 위치정보의 누출, 변조, 훼손 등을 방지하기 위하여 방화벽의 설치나 암호화 소프트웨어의 활용 등의 기술적 조치를 하여야 한다고 명시되어 있다[12].

2.3.1 시행령

시행령 제20조 제2항에 기술적 보호조치가 언급되어 있다. 여기에는 위치정보 및 위치정보시스템의 접근권한을 확인할 수 있는 식별 및 인증 실시, 암호화·방화벽 설치 등의 조치, 접근사실의 전자적 자동기록·보존 장치의 운영, 보안프로그램 설치 및 운영 등이 명시되어 있다[13].

2.3.2 위치정보의 관리적·기술적 보호조치 권고 해설서

방송통신위원회의 위치정보의 관리적·기술적 보호조치 권고 해설서에 따르면 위치정보시스템에 대한

정당한 접근여부 확인을 위한 인증수단으로 ID/PW, 공인인증서, 일회용 패스워드 등을 명시하고 있으며, 외부로부터 접근 차단을 위해 방화벽, 어플리케이션, PKI 기반 인증, 생체(바이오) 인식 등을 하도록 하고 있다. 또한 권한 없는 접근 차단을 위해 접근통제 장치로 방화벽, 침입탐지시스템을 사용하도록 하고 있으며, 위치정보를 안전하게 저장 및 전송할 수 있는 암호화 기술을 사용하도록 명시했다[14].

위치정보시스템의 접근사실을 실시간 자동 기록 및 보존 관리 하도록 하고 있으며, 침해사고 방지를 위한 OS 보안패치 설치와 백신프로그램을 설치하도록 하고 있다.

2.4 신용정보의 이용 및 보호에 관한 법률(Act4)

신용정보의 이용 및 보호에 관한 법률 제19조 제1항에 신용정보전산시스템에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 세워야 한다고 명시하고 있다[15].

2.4.1 시행령

시행령 제16조에 침입차단시스템 등의 접근통제장치 설치·운영, 정보의 변경·훼손 및 파괴를 방지하기 위한 대책과 신용정보 취급·조회 권한을 직급별·업무별로 차등 부여와 신용정보 조회기록의 주기적인 점검을 하도록 하고 있다[16].

2.4.2 신용정보업감독규정

금융위원회의 신용정보업감독규정에 따르면 개인신용정보처리시스템을 침입차단시스템과 침입탐지시스템을 설치하여 보호하도록 하고 있으며, 접속기록의 백업, 개인정보의 암호화 저장, 송·수신 시 SSL 및 암호화 응용프로그램설치로 보안서버 구축, 악성프로그램의 침투여부 점검 및 치료를 위한 백신 소프트웨어 설치를 하도록 하고 있다[17].

2.5 전자금융거래법(Act5)

전자금융거래법 제21조 제2항에 따르면, 금융회사 등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준을 준수하여야 한다고 명시되어 있다[18].

2.5.1 전자금융감독규정

금융위원회의 전자금융감독규정운영에 따르면, 단말기 인증, 중요단말기의 외부 반출, 인터넷 접속 금지, 보조기억매체접근 통제 등의 단말기 보호대책과 개인별 계정 부여, 업무별 접근권한 통제, 접근기록 자동 기록 및 유지, 모니터링 등의 전산자료 보호대책이 명시되어 있다. 또한 해킹 등의 사고 방지를 위한 정보보호시스템 설치와 패치, 망분리, 무선 통신망의 사용자 인증, 암호화, 모니터링 등을 명시하였으며, 악성코드 검색·치료프로그램, 멀티 인증, 업무와 무관한 프로그램 및 인터넷 사이트 접근 통제, 개인별, 업무 특성별 내부 IP 주소부여 등을 명시하고 있다[19].

2.5.2 전자금융감독규정시행세칙

전자금융감독규정시행세칙 제7조의2에 전자금융기반시설의 취약점 분석·평가의 내용이 명시되어 있다. 중요 단말기의 외부반출, 인터넷접속, 그룹웨어 접속금지와 보조기억매체, 휴대용 전산장비의 접근통제 등을 하도록 하고 있다. 또한 사용자 인증과 개인별 사용자 계정 및 비밀번호의 부여, 이용자 정보 등 주요정보 보관 금지, 단말기 공유 금지, 내부 통신망의 비인가 장비의 무선 통신 접속 통제, 무선 통신망 이용 업무에 대한 승인 등이 명시되어 있다. 그리고 악성코드 검색 및 치료프로그램의 최신 상태 유지 및 점검 여부, 멀티 인증사용, 이용자 비밀번호의 암호화 등을 하도록 명시하였다[20].

2.6 개인정보보호 관련 법령상의 기술적 보호조치

본 논문에서는 한국인터넷진흥원(KISA)에서 구분한 법령 구분을 참고하였다. 개인정보보호 관계법령인 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률과 그 외 개인정보 활용이 많은 신용정보의 이용 및 보호에 관한 법률, 전자금융거래법의 총 5개 법령의 기술적 보호조치를 조사한 결과 기술적 보호

조치는 주요 정보 암호화, 접근 통제, 악성프로그램 방지, 가용성 확보의 4개로 구분 할 수 있다. 여기서 접근 통제는 다시 인증, 접근 권한 관리, 접속 기록 보관/관리, 모니터링, 매체관리, 모바일·무선보안, 가상사설망, 네트워크 접근통제, 망분리의 9개로 구분할 수 있다. 각각의 기술적 보호조치의 세부 내용을 30개로 구분한 내용은 다음 〔Table 1〕과 같다.

Table 1. Technical Protection Measures on Legislation

Technical Protection Measures		Contents	Act1	Act2	Act3	Act4	Act5	Total
Major information encryption		Transmitted and received (security servers)	∨	∨	∨	∨		4
		Video transmission	∨					1
		Wireless data		∨				1
		Storage	∨	∨	∨	∨	∨	5
		Portable memory device storage/ transmission	∨	∨				2
		Storage in PC for work, mobile device	∨	∨			∨	3
		Personal information printout, copy		∨				1
Access control	Authentication	Certification(PKI)		∨	∨		∨	3
		Biometric			∨			1
	Access right management	Level differentiation for system access right	∨	∨	∨	∨	∨	5
		Issuing account by personal information handlers	∨				∨	2
		DB access right management		∨				1
		Video information access control/ access management	∨					1
	Access record storage /management	Log management	∨	∨	∨	∨		4
	Monitoring	Monitoring		∨			∨	2
	Device management	Portable memory device , portable computation equipment access control					∨	1
	Mobile·wireless security	Mobile device access control	∨					1
		Mobile device password setup	∨					1
		Wireless LAN authentication		∨			∨	2
	Virtual private network	Virtual private network(VPN)	∨					1
	Network access control	System for blocking intrusion		∨	∨	∨		3
		Systems for detecting intrusions		∨	∨	∨		3
		Detection illegal breach to IP address analysis	∨	∨				2
		Limit access right to IP address	∨	∨	∨		∨	4
	Network separation	Blockade of external Internet networks		∨			∨	2
Malicious program prevention		Vaccine software	∨	∨	∨	∨	∨	5
		Automatic patch update	∨	∨	∨	∨	∨	5
		Delete program or function any purpose other than the purpose of work					∨	1
		Vulnerability inspection	∨	∨				2
Ensure availability		Load balancing measure, DDoS defense		∨			∨	2
Total								71

※ Act1 : Personal Information Protection Act
※ Act2 : Act on Promotion of Information and Communications Network Utilization and Information Protection, etc
※ Act3 : Act on the Protection, Use, Etc, of Location Information
※ Act4 : Use and Protection of Credit Information Act
※ Act5 : Electronic Financial Transactions Act

5개의 법령은 주요 정보의 저장 시 암호화, 시스템 접근 권한의 차등부여, 백신 소프트웨어 설치와 자동 업데이트가 모두 명시되어 있음을 알 수 있다.

영상정보의 전송 암호화, 접근통제/접근권한 관리와 모바일기기 접근통제, 비밀번호 설정 그리고 가상사설망은 개인정보보호법에만 명시되어 있다. 또한 무선데이터 암호화, 개인정보 출력, 복사물 관리, DB 접근권한 관리는 정보통신망법에만 명시되어 있다. 바이오 인식은 위치정보법에만, 보조기억매체 및 휴대용 전산장비 등의 매체관리, 업무 목적 외 기능/프로그램 제거는 전자금융거래법에만 명시되어있어 법률에 따른 차이를 볼 수 있다.

III. 법령과 CC인증 제품군 비교

본 논문에서는 5개의 개인정보보호 관련 법령에 따른 기술적 보호조치와 CC인증 제품을 비교하였다.

3.1 CC인증 제품

CC인증(보안적합성 검증)은 전자정부법 제56조, 공공기록물 관리에 관한 법률 시행령 제5조에 의거

하여 국가·공공기관에 도입하는 정보보호시스템에 대해 안전성을 검증하는 제도이다[21].

1998년 2월부터 정보보호제품 평가·인증제도를 실시하고 있으며, 2002년부터 국제공통평가기준(CC, Common Criteria)에 따라 정보보호제품을 평가·인증하고 있다[22]. 국내에서는 한국 인터넷진흥원(KISA), 한국산업기술시험원(KTL), 한국시스템보증(KoSyAs), 한국아이티평가원(KSEL), 한국정보통신기술협회(TTA), 한국정보보안 기술원(KOIST), 한국기계전기전자시험연구원(KTC)에서 평가하고 있다[23].

CC인증 제품군은 2014년 6월 기준 28종이 있으며 제품은 다음과 같다[21].

Table 2. CC Products Group

Products (Module)	Use
DB Access Control	DB access control and data loss prevention
DDoS defense equipment	DDoS attack detection and automatic prevention
PC Virtualization	Strict separation of PC for acture and virtual
PC Intrusion Prevention	Installed on PC, inflows and outflows traffic control to PC
Virtual Private network	VPN (IPSec or SSL)
Network data loss Prevention	Critical data loss prevention by control a traffic transmitted over the network
Network Access Control	Allow network access only the PC, install a security program
Data Transfer between different Network	Data and information flow control between different security level
Device Control	Device control and data loss prevention to USB, CD-ROM etc.
Wireless Lan Authentication	Allow wireless LAN access only authenticated users
Wireless Intrusion Prevention System	Threat intrusion detection and intrusion prevention in the wireless LAN environment
Digital Multiunction Printer	Remove module for built-in HDD in MFP
Server Virtualization	Strict separation for acture and virtual of server
Server Access Control	Server access right control and critical file security setting
Source code Vulnerability Weakness Analysis Tool	SW source code analysis and security weaknesses identification
Software-based Secure USB	USB memory access control and automatic deletion when lost
Smart Card	Smart card chip and operation system
SmartPhone Security management	Managed smartphone for business central control and security management
Anti-spam Mail System	Spam mail inflow detection and prevention
Anti-virus	Malicious code detection and removal in PC
Web Application Firewall	Harmful traffic based on WEB intrusion detection and automatic prevention
VoIP Security	Harmful traffic related VoIP detection and intrusion prevention
Intrusion Prevention System	Network harmful traffic intrusion detection and automatic prevention
Firewall	Inflow and outflow traffic control in network
Intrusion Detection System	Network harmful traffic automatic detection
Enterprise Security Management	Central control a multiple managed target system, security event monitoring and analysis
Patch Management System	Automatic perform a security patch from central server to PC
Host data loss Prevention	Critical data loss prevention to device control installed on the host

3.2 법령상 기술적 보호조치와 CC인증 제품의 비교

앞서 조사했던 5개 법령의 기술적 보호조치에 따라 CC인증 제품군 28개를 매칭하였다.

Table 3. Matching of Personal Information Protection Legislation - CC Products

Personal Information Protection Legislation			CC Products
Technical Protection Measures		Contents	
Major information encryption		Transmitted and received (security servers)	-
		-	VoIP Security
		Video transmission	-
		Wireless data	-
		Storage	-
		Portable memory device storage/transmission	Software-based Secure USB
		Storage in PC for work, mobile device	Host data loss Prevention
		Personal information printout, copy	
		-	Digital Multifunction Printer
Access control	Authentication	Certification(PKI)	-
		Biometric	-
		-	Smart Card
	Access right management	Level differentiation for system access right	Server Access Control
		Issuing account by personal information handlers	
		DB access right management	DB Access Control
		Video information access control/ access management	-
	Access record	Log management	Enterprise Security

	storage/management		Management
	Monitoring	Monitoring	
	Device management	Portable memory device , portable computation equipment access control	Device Control
	Mobile·wireless security	Mobile device access control	SmartPhone Security management
		Mobile device password setup	
		Wireless LAN authentication	Wireless Lan Authentication
	Virtual private network	Virtual private network(VPN)	Virtual Private network
	Network access control	System for blocking intrusion	Firewall
			Intrusion Prevention System
			Wireless Intrusion Prevention System
			Anti-spam Mail System
		Systems for detecting intrusions	Intrusion Detection System
		Detection illegal breach to IP address analysis	Network Access Control
		Limit access right to IP address	Network data loss Prevention
	Network separation	Blockade of external Internet networks	Data Transfer between different Network
Malicious program prevention		Vaccine software	Anti-virus
		Automatic patch update	Patch Management System
		Delete program or function any purpose other than the purpose of work	Web Application Firewall
		Vulnerability inspection	Source code Vulnerability Weakness Analysis Tool
		-	PC Intrusion Prevention
Ensure availability		Load balancing measure, DDoS defense	DDoS defense equipment
Virtualization		-	Server Virtualization
			PC Virtualization

조사 결과 법령에 명시된 세부 내용과 CC인증 제품이 일대일로 매칭되지 않았으며 법령에 따른 CC 인증 제품이 없거나 중복으로 매칭되는 경우도 있었다. 법령의 주요 정보와 영상정보의 송·수신과 저장 시 암호화, 공인인증서, 바이오 인식, 영상정보의 접근통제/접근 권한 관리 등에 해당하는 CC인증제품은 아직 없는 것으로 나타났다. 그러나 〔Table 4〕와 같이 국정원에서 암호화 모듈(KCMVP) 검증을 따로 실시하고 있어 매칭되지 않은 암호화에 대한 항목은 따로 인증 받을 것으로 보인다.

Table 4. KCMVP Products〔21〕

Products	CC level	KCMVP
Mail Encryption Module	N/A	Requirement
Section Encryption Module		
PKI Products		
SSO Products		
Disk·File Encryption Products		
Document Encryption Products (DRM), etc		
Keyboard Encryption Module		
HW Security Token		
DB Encryption Products		
Etc. Encryption Products		

법령에 뚜렷하게 명시되지 않은 인터넷 전화보안, 복합기 완전 삭제, 스마트카드, PC 침입차단, 서버 가상화, PC 가상화 등이 CC제품군에는 존재했다.

IV. 법령과 정보보호제품 비교

개인정보보호 법령과 CC제품의 비교를 바탕으로 실제 정보보호 업체의 제품 분포를 조사하였다. 정보보호 업체는 지식정보보안산업협회(KISIA)의 회원사 189개(2015.5.14. 기준)〔24〕를 조사하였다. 그 중 컨설팅과 출입통제, 총판, 연구기관, 공공기업 등을 제외한 회원사의 제품을 분석하였다. 회원사의 제품은 해당 회원사의 홈페이지를 통해 확인 하였으므로 홈페이지가 운영 중이지 않는 경우 분석에서 제외하였고, 합병한 기업은 하나의 기업으로 보아 총 187개 중 117개의 회원사를 분석하였다.

4.1 KISIA 회원사의 제품군 분포

117개의 회원사의 제품 중 법령과 CC인증 제품의 분류테이블에 적용 가능한 제품은 총 463개로 접속기록 보관/관리, 모니터링 관련 제품이 각각 37개, 36개로 약 30%의 업체가 생산하고 있었다. 또한, 침입차단시스템이 24개로 그 다음을 차지하였고, 침입차단, 침입탐지, 침입방지 시스템을 UTM으로 묶어 생각해본다면 총 62개로 약 13%를 차지하고 있다.

반면 법령에 명시되지 않고 CC인증에만 있는 제품은 10개미만의 업체만이 생산하고 있어 법령과 제품 간의 연관성이 있음을 추정할 수 있다.

Table 5. KISIA Member Company's Distribution

Personal Information Protection Legislation			CC Products	KISIA
Technical Protection Measures		Contents		
Major information encryption		Transmitted and received (security servers)	-	16
		-	VoIP Security	2
		Video transmission	-	1
		Wireless data	-	4
		Storage	-	16
		Portable memory device storage/transmission	Software-based Secure USB	8
		Storage in PC for work, mobile device	Host data loss Prevention	19
		Personal information printout, copy		20
		-	Digital Multifunction Printer	2
Access control	Authentication	Certification(PKI)	-	17
		Biometric	-	9
		-	Smart Card	4
	Access right management	Level differentiation for system access right	Server Access Control	15
		Issuing account by personal information handlers		7
		DB access right management	DB Access Control	9
		Video information access control/ access management	-	2
	Access record storage/management	Log management	Enterprise Security Management	37
	Monitoring	Monitoring		36
	Device management	Portable memory device , portable computation equipment access control	Device Control	12
	Mobile·wireless security	Mobile device access control	SmartPhone Security management	20
		Mobile device password setup		3
		Wireless LAN authentication	Wireless Lan Authentication	8
	Virtual private network	Virtual private network(VPN)	Virtual Private network	11
	Network access control	System for blocking intrusion	Firewall	24
			Intrusion Prevention System	10
			Wireless Intrusion Preventio n System	5
				Anti-spam Mail System	7
		Systems for detecting intrusions	Intrusion Detection System	16
		Detection illegal breach to IP address analysis	Network Access Control	18
		Limit access right to IP address	Network data loss Prevention	19
	Network separation	Blockade of external Internet networks	Data Transfer between different Network	8
Malicious program prevention		Vaccine software	Anti-virus	18
		Automatic patch update	Patch Management System	8
		Delete program or function any purpose other than the purpose of work	Web Application Firewall	20
		Vulnerability inspection	Source code Vulnerability Weakness Analysis Tool	9
		-	PC Intrusion Prevention	9
Ensure availability		Load balancing measure, DDoS defense	DDoS defense equipment	9
Virtualization		-	Server Virtualization	3
			PC Virtualization	2
Total				**463**

4.2 가설 설정 및 통계 분석

개인정보보호 관련 법령과 인증제품 수, 개발된 정보보호 제품 수간의 연관성에 대한 통계검증을 위해 테이블을 단순화시켰다. 또 CC인증 제품에 KCMVP 9개 제품을 추가하여 37개로 분석하였고, 접근통제는 사람, 접속기록관리 및 모니터링, 장비, 네트워크로 구분하였다. 그리고 각각의 키워드와 제품군의 수를 세어 통계분석을 위한 표로 나타내었다.

Table 6. List of Personal Information Protection Legislation - CC and KCMVP

Personal Information Protection Legislation				CC & KCMVP
Technical Protection Measures			Contents	
Major information encryption			• Transmitted and received(security servers) • Video transmission • Wireless data • Storage • Portable memory device storage /transmission • Storage in PC for work, mobile device • Personal information printout, copy	• VoIP Security • Software-based Secure USB • Host data loss Prevention • Digital Multifunction Printer • Mail Encryption Module • Disk·File Encryption Products • Document Encryption Products (DRM), etc • DB Encryption Products
Access control	Human	Authentication, Access right management	• Certification(PKI) • Biometric • Level differentiation for system access right • Issuing account by personal information handlers • DB access right management • Video information access control/ access management	• Smart Card • PKI Products • SSO Products • HW Security Token • Server Access Control • DB Access Control
	Access record Management and Monitoring	Access record storage/management, Monitoring	• Log management • Monitoring	• Enterprise Security Management
	Device	Device management, Mobile·wireless security	• Portable memory device , portable computation equipment access control • Mobile device access control • Mobile device password setup • Wireless LAN authentication	• Device Control • SmartPhone Security management • Wireless Lan Authentication
	Network	Virtual private network, Network access control, Network separation	• Virtual private network(VPN) • System for blocking intrusion • Systems for detecting intrusions • Detection illegal breach to IP address analysis • Limit access right to IP address • Blockade of external Internet networks	• Virtual Private network • Section Encryption Module • Firewall • Intrusion Prevention System • Wireless Intrusion Prevention System • Anti-spam Mail System • Intrusion Detection System • Network Access Control • Network • data loss Prevention • Data Transfer between different Network
Malicious program prevention			• Vaccine software • Automatic patch update • Delete program or function any purpose other than the purpose of work • Vulnerability inspection	• Anti-virus • Patch Management System • Web Application Firewall • Source code Vulnerability Weakness Analysis Tool • PC Intrusion Prevention • Keyboard Encryption Module
Ensure availability			• Load balancing measure, DDoS defense	• DDoS • defense equipment
Virtualization			-	• Server Virtualization • PC Virtualization

여기서 가상화는 법령에 키워드로 나타나있지 않고 제품빈도 역시 크지 않으므로 기타로 가용성 확보와 묶어 분석하였다.

Table 7. Analysis of Personal Information Protection Legislation - CC and KCMVP - KISIA

Technical Protection Measures		Personal Information Protection Legislation		CC & KCMVP		KISIA	
		freq.	%	freq.	%	freq.	%
Major information encryption		17	23.9	8	21.6	88	19.0
Access control	Human	13	18.3	6	16.2	63	13.6
	Access record Management and Monitoring	6	8.5	1	2.7	73	15.8
	Device	5	7.0	3	8.1	43	9.3
	Network	15	21.1	10	27.0	118	25.5
Malicious program prevention		13	18.3	6	16.2	64	13.8
Ensure availability, etc.		2	2.8	3	8.1	14	3.0
Total		**71**	**100**	**37**	**100**	**463**	**100**

4.2.1 가설 설정

〔Fig. 1〕은 〔Table 7〕의 기술적 보호조치에 해당하는 개인정보보호법령, CC인증 및 KCMVP 제

품, KISIA 각각의 비율을 그래프로 나타낸 것이다.

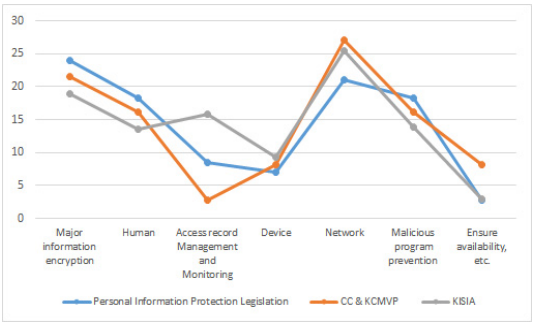

Fig. 1. Linearizer Graph of Personal Information Protection Legislation - CC and KCMVP Products - KISIA

그래프 모양이 비슷하게 나타남을 확인 할 수 있으며, 이것은 법령과 관련 CC인증 및 KCMVP 제품과 KISIA 회원사의 제조 제품은 관련성이 있다고 추측 할 수 있다. 이에 다음과 같은 가설을 설정하였다.

〔가설 1〕 법령에 기술적 보호조치 관련 키워드가 많이 나타날수록 관련된 CC인증 및 KCMVP 제품군이 많을 것이다.

〔가설 2〕 법령에 기술적 보호조치 관련 키워드가 많이 나타날수록 관련된 국내 제품 수가 많을 것이다.

4.2.2 통계 분석

가설검증을 위해 SAS를 이용하여 카이제곱(χ^2) 동질성 검증을 통해 연관성을 확인하였다. 카이제곱(χ^2)의 동질성 검증은 서로 다른 집단이 동일한 분포를 따르는지를 알아보기 위하여 사용하는 분석방법이다.

〔가설 1〕 법령에 기술적 보호조치 관련 키워드가 많이 나타날수록 관련된 CC인증 및 KCMVP 제품군이 많을 것이다.

카이제곱 검증결과 p-value는 0.7714 이므로 귀무가설을 채택하였다. 즉, 분포는 동질적이며, 법령에 키워드가 많이 나타날수록 관련된 인증제품(CC 인증+KCMVP) 도 많다는 것이 확인되었다.

Table 8. Chi-Square Test Results of Personal Information Protection Legislation - CC and KCMVP Products

	DF	Value	Prob
Chi-Square	6	3.2919	0.7714
Likelihood Ratio Chi-Square	6	3.3833	0.7594
Mantel-Haenszel Chi-Square	1	0.7073	0.4003
Phi Coefficient		0.1746	
Contingency Coefficient		0.1720	
Cramer's V		0.1746	
Sample Size	108		

※ WARNING: 36% of the cells have expected counts less than 5. Chi-Square may not be a valid test.

기대 도수가 5미만인 칸이 36%로 전체의 20%를 초과하여, 카이제곱 통계량 보다는 피셔의 정확 검정법(Fisher's Exact Test)이 더 정확하기 때문에 별도로 정확도 검정을 수행하였다.

Table 9. Fisher's Exact Test of Personal Information Protection Legislation - CC and KCMVP Products

	Table Probability (P)	Pr <= P
Fisher's Exact Test	9.016E-05	0.7988

피셔의 정확 검정법에서도 p-value는 0.7988 이므로 귀무가설을 채택하였다. 즉, 분포가 동질적이며, 법령에 키워드가 많이 나타날수록 관련된 인증제품(CC 인증+KCMVP) 도 많다는 것이 다시 한 번 입증되었다.

〔가설 2〕 법령에 기술적 보호조치 관련 키워드가 많이 나타날수록 관련된 국내 제품 수가 많을 것이다.

카이제곱 검증결과 p-value는 0.4659 이므로 귀무가설을 채택하였다. 즉, 분포가 동질적이며, 법령에 키워드가 많이 나타날수록 관련된 국내 제품수도 많다는 것이 입증되었다.

Table 10. Chi-Square Test Results of Personal Information Protection Legislation - KISIA

	DF	Value	Prob
Chi-Square	6	5.6302	0.4659
Likelihood Ratio Chi-Square	6	5.8590	0.4392
Mantel-Haenszel Chi-Square	1	0.2988	0.5847
Phi Coefficient		0.1027	
Contingency Coefficient		0.1021	
Cramer's V		0.1027	
Sample Size	534		

V. 결 론

본 논문은 개인정보보호 관련 법령에 명시되어있는 기술적 보호조치에 따라 CC인증 및 KCMVP 제품, 정보보호업체의 제조 제품에 연관성이 있을 것이라 가정하고 가설을 세웠다. 그리고 개인정보보호 관련 5개 법령(개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률과 신용정보의 이용 및 보호에 관한 법률, 전자금융거래법)과 KISIA 회원사인 정보보호 업체의 제조 제품을 조사하였다.

검증 결과 법령에 기술적 보호조치 관련 키워드가 많이 나타날수록 관련 CC인증 및 KCMVP 제품군이 많았으며, 관련 정보보호 제품 역시 많았다. 이를 통해 CC인증 및 KCMVP 제품과 정보보호 제품 생산 및 개발은 법령과 국가의 정책에 크게 영향을 받는다는 결론에 도달하였다.

향후에는 영상과 음성 정보 등 다양한 형태의 개.인정보의 중요성이 높아지고, 클라우드컴퓨팅, IoT 등 새로운 기술의 발전으로 법령의 제·개정이 이루어질것으로 예상됨에 따라 CC인증의 영역과 정보보호 제품도 확장될 것으로 기대된다.

본 연구는 법령의 내용과 관련 제품의 수를 단순 비교한 결과이기 때문에 법령의 제·개정 시점에 따른 직접적인 영향을 분석하기에는 한계가 존재한다. 따라서 향후에는 법령의 제·개정된 시점까지 넣어서 다각도로 분석할 예정이며, 법령의 제·개정에 따른 CC인증 및 KCMVP 제품과 정보보호 제품의 변화 추이를 지속적으로 추적 연구할 예정이다.

References

[1] Kim Seungjoo, "Actual condition of cyber warfare and latest hacking trend," Korea Univ., June. 2013, available : http://www.slideshare.net/skim71/ss-23039901

[2] Shin Young Jin, "A study on the improvement of technological protection measures for responding to privacy breaches," Proceeding of Autumn Annual Conference of The Korean Association for Policy Studies, pp. 465-488, Sep. 2013.

[3] Young Hee Kim and Kwang Ho Kook, "A Study on the Relative Importance of the Administrative and Technical Measures for the Personal Information Protection," The Journal of Society for e-Business Studies, 19(4), pp. 135-150, Nov. 2014.

[4] Young Ran Hong and Dongsoo Kim, "Analysis of the Effects of Common Criteria Certification on the Information Security Solutions," Journal of Society for e-Business Studies, 17(4), pp. 57-68, Nov. 2012

[5] Personal Information Protection Act

[6] Standards on Measures for Securing the Safety of Personal Information

[7] Standard Personal Information Guide

[8] Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

[9] Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

[10] Guidelines for Information Security Measures

[11] Standards on Technical and Administrative Protection Measures for Personal Information

[12] Act on the Protection, Use, Etc, of Location Information

〔13〕 Enforcement Decree of the Act on Protection & Utilization of Location Information, etc.
〔14〕 Manual on Administrative and Technical Protection Measures Recommendation of Location Information
〔15〕 Use and Protection of Credit Information Act
〔16〕 Enforcement Decree of Use and Protection of Credit Information Act
〔17〕 Regulation of Credit Information Business Supervision
〔18〕 Electronic Financial Transactions Act
〔19〕 Regulation of Electronic Financial Supervision
〔20〕 Rules for Regulation of Electronic Financial Supervision
〔21〕 National Cyber Security Center, availabl e: http://service1.nis.go.kr/certify/con venanceSummary.jsp
〔22〕 Ji Sun Kim, "A Study of CC for Privacy Management System," Master Thesis, Sungkyunkwan Univ., June. 2011.
〔23〕 IT Security Certification Center, http:// www.itscc.kr/appraisal_2.asp
〔24〕 KISIA, available: http://www.kisia.or.kr/

〈저 자 소 개〉

김 민 정 (Min-Jeong Kim) 정회원
2015년 2월: 상명대학교 지식보안경영학과 석사
2015년 2월~현재: 펜타시큐리티시스템(주)
〈관심분야〉 정보보호 정책, 개인정보보호, 산업보안

이 정 원 (Jung Won Lee) 정회원
현재: 펜타시큐리티시스템(주) 이사
〈관심분야〉 정보보호, 암호화, 보안정책

유 진 호 (Jinho Yoo) 종신회원
1992년 2월: 고려대학교 수학과 졸업
1994년 2월: 고려대학교 통계학과 석사
2010년 2월: 고려대학교 정보보호 박사
1993년 11월~1999년 12월: 한국전자통신연구원 연구원
2000년 1월~2004년 9월: IBM KOREA 전문차장
2004년 10월~2012년: KISA 인터넷문화진흥단장
2013년 ~ 현재: 상명대학교 경영학과 교수
〈관심분야〉 정보보호, 개인정보보호, MIS, 인터넷윤리