개인정보보호에 관한 IT컴플라이언스 적용방안에 대한 고찰

이홍석*
*고려대학교 컴퓨터정보통신대학원
redst77@korea.ac.kr

Research of apply IT Compliance about Personal Information Protection

Lee Hong Seok*
*Graduate School of Computer Information & Communication, Korea University

요 약

최근 전 세계적으로 스마트, 모바일, 클라우드 등 새로운 형태의 컴퓨팅 환경속에서 정보의 집적화, 대량화가 점차 확대됨에 따라 개인 정보의 유출 가능성은 날로 높아지고 있다. 오늘날 개인정보는 개인의 권익에 관한 문제로 국한되는 것이 아닌 기업의 사활을 좌지우지하는 비즈니스 이슈이다. 특히 국내 개인정보보호법의 전면적인 법 시행 후 규제대상이 아니던 기업 종업원의 개인정보는 물론 문서 형태의 개인정보까지를 규제대상으로 삼고 있어 개인정보보호 시장이 크게 확대될 것으로 전망된다. 본 논문에서는 개인정보보호와 관련하여 국내외 컴플라이언스를 비교분석하여 기업이 보다 효과적으로 IT컴플라이언스를 준수할 수 있는 방안을 제안한다.

1. 서론

정보통신 기술의 발전으로 사회는 다양한 형태로 변화를 겪고 있으며, 정보시스템의 의존도가 높아짐에 따라 정보시스템 보안 사고에 대한 위험이 점차 증가하고 있다.

특히, 최근에 개인정보 유출사고는 기존의 해킹, 바이러스, DDoS공격 사고에 비해서 그 심각성이 극대화 되고 있는 상황에서 개인정보보호는 단순히 개인의 권익에 관한 문제로 국한되지 않고, 기업의 존속여부까지 좌지우지하는 이슈로 대두되고 있다.

현대의 기업들은 고객 맞춤형 서비스에 대한 요구 증가로 취급하는 개인정보가 다양해지고 활용 범위도 복합, 융합되는 등 범위가 증가되고 있는 추세이다. 이러한 이유로 최근 빈번하게 발생하는 금융회사, 쇼핑몰, 유통업체 등의 대량 개인정보 침해사고는 법률소송, 배상 등과 연계되어 기업의 생존에 영향을 미치는 중요한 위험요소로 등장하였고 기존의 보호체계로는 전사적 차원으로 활용되고 있는 개인정보를 보호하는데 어려움이 발생되고 있다.

정보보호를 체계적으로 운영·관리하기 위하여 많은 기업들이 많은 예산 등을 투입하여 정보보호관리 체계를 수립하여 지속적으로 관리체계를 유지·관리할 수 있도록 많은 노력을 하고 있다.

기업이 대외적인 측면에서 개인정보보호 수준에 대한 신뢰도를 높이기 위해서는 전문적이고 객관적이고 공신력이 있는 제3자에 의한 평가가 필요하다. 본 논문에서는 최근 가장 이슈가 되고 있는 고객의 금융정보와 기타 개인정보를 취급하는 기업들이 준수해야하는 지불카드결제산업 데이터보안표준(PCI DSS)[1] 과 개인정보보호관리체계(PIMS)[2] 인증제도의 통제항목의 연관성을 분석하여 기업이 개인정보보호를 위한 IT컴플라이언스 적용 및 관련 정보보호활동의 중복노력을 감소하는데 효율적인 가이드로써 활용되었으면 하는 바램이다.

---

1) PCI DSS(Payment Card Industry Data Security Standard, 이하 PCI DSS) 신용카드 및 직불카드 회사들의 연합체인 PCI(Payment Card Industry)는 2004년 가정이나 소매상과 같은 소규모 환경에서 고객들의 금융 정보 유출을 방지하기 위한 목적으로 설립된 단체이며, PCI DSS는 2006년 7월, 아메리칸 익스프레스(American Express), JCB, 마스터카드(MasterCard), 비자카드(Visa International)등 세계적인 카드회사들이 모여 공식적으로 만든 PCI 보안 표준 협의회에서 출범

2) PIMS(Personal Information Management System) 방송통신위원회와 한국인터넷진흥원은 기업이 체계적이고 지속적인 개인정보 보호활동을 위한 관리체계를 제공하여 개인정보 침해 가능성 최소화 하고 기업의 자율적인 개인정보 보호 활동을 유도하고 국민들이 개인정보를 안전하게 관리하는 기업을 식별할 수 있는 기준을 제공하여 기업 스스로 개인정보 침해사고에 대한 사전적 예방을 유도하고 정보 주체인 개인들에게 구체적이고 믿을 수 있는 판단의 근거를 제공하기 위하여 개이정보보호관리체계 인증제도를 제정

2. IT 컴플라이언스

2.1 지불카드결제산업 데이터보안표준(PCI DSS)

고객의 카드 정보 노출 사고가 급증하고 카드정보보호에 대한 중용성이 인식되면서 2004년 주요카드회사들이 협력하여 PCI DSS라는 카드보안 표준을 만들었다. PCI DSS는 지불카드결제산업 보안표준위원회(PCI SSC)에서 관리한다. 이 표준은 카드사용자정보를 취급하는 모든 가맹점과 서비스 사업자들의 정보처리 업무환경과 보안정책 및 정보보호 환경의 보안수준을 평가하는 것이며, 또한 표준에 대한 준수 의무를 갖는다. <표 1>은 PCI DSS 의 통제분야와 통제 항목수를 분류하였다.[1,2]

<표 1> PCI DSS 통제항목

통제분야	통제 항목수
1. 데이터보호를 위한 침입차단시스템 설치 및 유지관리	4
2. 벤더가 제공한 디폴트 시스템 패스워드 및 기타 보안 파라미터 값 사용금지	4
3. 저장 데이터 보호	6
4. 카드 소유자 정보 및 민감한 정보 암호화 전송	2
5. 바이러스 백신 소프트웨어 설치 및 정기적 업데이트	2
6. 안전한 시스템과 어플리케이션 개발 및 유지관리	6
7. 알 필요 원칙에 따른 접근 통제	2
8. 시스템 사용자별 고유ID 부여	5
9. 카드 소유자 정보에 대한 물리적 접근 통제	10
10. 네트워크 자원과 카드 소유자 정보에 대한 접근 추적 및 모니터링	7
11. 보안 시스템 및 프로세스 정기적 테스트	5
12. 직원과 계약자들의 정보보호를 위한 정책 유지관리	9

2.2 개인정보보호관리체계 인증(PIMS)

기업이 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로 기업이 체계적이고 지속적인 개인정보보호 활동을 수행할 수 있는 방법론을 제공하여, 개인정보 취급자 부주의·관리소홀 등으로 인한 개인정보 침해 가능성 최소화 국민들에게 개인정보를 안전하게 관리하는 기업을 식별할 수 있는 기준 제공 할 수 있다.[3,4]

또한 방송통신위원회에서는 개인정보보호 관리체계의 국제 표준화 추진을 한국에서 세계 최초로 제안하여 ITU-T와 ISO/IEC [3] 에서 표준화 논의를 시작했다.[5]

3) ITU-T(International Telecommunication Union Telecommunication standardization Sector:국제전기통신연합 전기통신표준화부문), ISO(International Organization for Standardization: 국제표준화 기구), IEC(International Electrotechnical Commission:국제전기표준회

<표 2>는 PIMS 의 통제분야와 통제 항목수를 분류하였다.[5]

<표 2> PIMS 통제항목

통제분야		통제 항목수
개인정보보호 관리과정	1. 개인정보 정책수립	3
	2. 관리체계 범위설정	2
	3. 위험관리	3
	4. 구현	1
	5. 사후관리	2
개인정보 보호대책	1. 개인정보보호 정책	6
	2. 개인정보보호 조직	5
	3. 개인정보 분류	4
	4. 교육 및 훈련	4
	5. 인적보안	3
	6. 침해사고 처리 및 대응절차	7
	7. 기술적 보호조치	36
	8. 물리적 보호조치	5
	9. 내부검토 및 감사	9
생명주기 준거	1. 개인정보 수집	7
	2. 개인정보 이용 및 제공	16
	3. 개인정보 관리 및 파기	5

3. IT 컴플라이언스 통제항목 통합 방안

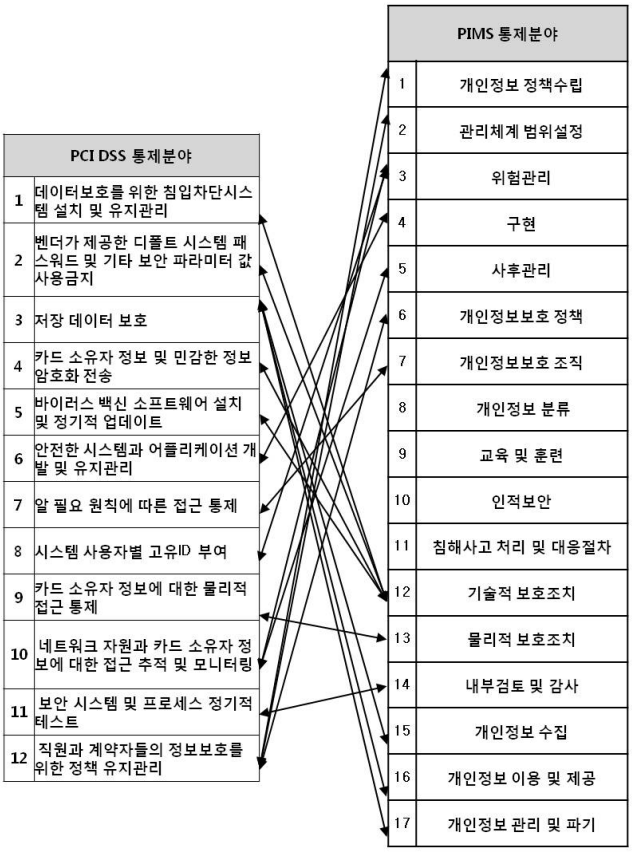
PCI DSS와 PIMS를 서로 비교하면 다음<표 3>과 같다. <표 3>에서 통제 분야를 보면 PIMS는 개괄적인 정보보호 범위를 포함하고 있으며 PCI DSS의 통제분야는 개인정보를 외부 해킹 등 범죄로부터 보호하기 위해 세부 기준을 제시한다. 결과적으로 중복되는 부분도 많이 있고 상호보완적인 관계를 가지기도 한다. 또한 PIMS는 가능한 범위를 지정하고 범위 내에서 준수를 하지만 PCI DSS는 100% 준수 의무를 갖는다.

<표 3> PCI DSS와 PIMS 비교

특징	PCI DSS	PIMS
통제 구현 방법	필수	위험관리 기반
구현 상세 내용 정의	높음	낮음
유연성	낮음	높음
주관기관	PCI SSC	KISA
대분류 수	12	17
통제항목 수 및 세부 통제항목	62개의 통제항목과 175개의 세부통제 내용 정의	118개의 통제항목과 325개의 세부 통제내용 정의
보호 및 처리 범위	고객카드 정보보호, 안전한 네트워크 유지관리, 취약점 관리, 네트워크 모니터링 및 정보보호정책 유지관리	개인정보 정책수립, 관리체계 범위설정, 기술적 물리적 보호, 기타 인증신청기관 사업모델에 따라 선택적으로 적용가능

특징	PCI DSS	PIMS
대상기관	카드정보를 이용한 거래업체	정보통신망과 연동하여 정보통신망을 운영하는 민간사업자로 인터넷과 연동된 정보통신망을 운영하는 사업자 대부분
혜택 및 벌칙	미준수시 카드거래 제약 카드정보 노출 사고 발생시 벌금부과	개인정보 사고 발생시 과징금 경감, 국내 경영평가 신용평가시 우대, 정보보호관련보험 요금할인 등
기간	유효기간 1년 네트워크 취약점 점검은 분기별 점검	유효기간 3년

따라서 PCI DSS를 준수하는 기업이 PIMS 인증을 위해 IT컴플라이언스간 공통항목에 대한 중복 노력을 줄이고 해당 통제항목를 상시 관리할 수 있도록 통제항목간 연관을 매핑한다. PCI DSS와 PIMS의 통제항목은 컴플라이언스 특성상 1:1 관계는 불가능하다. 그래서 본 논문에서는 항목간에 유사성과 키워드를 정의하여 객관적으로 분류하고 상호간에 매핑하는 방안을 이용하였다.



(그림 1) 통제항목 연관성

5. 결론 및 향후 연구방향

최근 개인정보보호법이 제정되고 시행되는등 우리나라의 개인정보보호의 수준제고를 위한 노력은 계속되고 있다. 하지만 기업이 고객정보를 수집·이용하는 과정에서 지속적으로 대량의 개인정보 유출사고가 발생하면서 기업의 인식제고가 필요한 시점에 와 있다.

100만 명이 넘는 대량의 고객 정보를 다루는 ISP, 인터넷 쇼핑몰, 포털 회사들을 중심으로 개인정보보호관리체계(PIMS) 인증에 대한 관심과 수요가 급증하고 있다. 이러한 정보보호관리체계를 위한 IT컴플라이언스들을 통합하여 관리할 수 있다면 정보보호관리체계를 보다 거시적 관점에서 볼수 있고 보다 효율적인 운영이 가능하다.

본 논문에서는 PCI DSS와 PIMS의 통제항목을 매핑하여 관리중복 또는 이중투자의 낭비를 지양하고 효율적인 통합관리 가능성을 제시하였다.

향후 국내외 정보보호관리체계를 위한 IT컴플라이언스의 세부 통제항목을 코드화 하여 정보보호 체계를 통합관리할수 있는 시스템이 개발되어야 할 것이며 이에 대한 연구가 필요하다.

참고문헌

[1] 김동국, 장성용, “결제카드산업 데이터보안표준(PCI DSS) 적용방안에 대한 고찰,” 정보보호학회지, 18(4), pp. 66-75, 2008년 8월.

[2] PCI Security Standard Council, “Payment card industry(PCI) data security standard – requirements and security assessment procedures,” Version 2.0, PCI Security Standard Council, Oct. 2010.

[3] 한국인터넷진흥원, “개인정보보호관리체계 인증 준비 안내서”, 2011

[4] http://isms.kisa.or.kr/

[5] 방송통신위원회 보도자료, ”개인정보보호 관리체계(PIMS) 국제 표준화 추진” Oct. 2011.