핀테크 산업의 지불카드산업 데이터보안표준(PCI-DSS)과 국내·외 정보보호인증제도 비교 연구

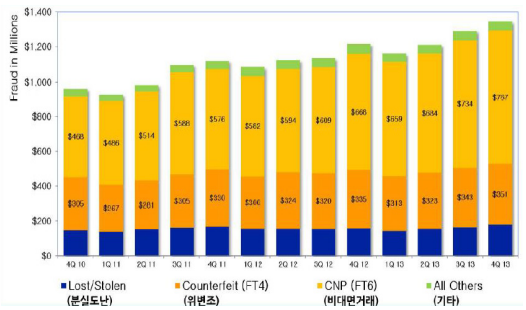
장 진 섭[1)]

목 차

1. 서 론

국내·외 대형 보안사고 발생으로 IT컴플라이언스(Compliance)가 강화되면서 관련 법령이 개정되고, 정보보호 관련 인증의 대상이 확대되고 있다. 국내는 2014년 대량 카드정보 유출 사고 이후 금융관련 보안대책이 수립되었고, 최근 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법)이 개정되어 ISMS(정보보호관리체계) 인증의무 대상이 확대되었으며, 개인정보보호 관련 인증제도로는 PIMS(개인정보보호관리체계)가 정보통신망법에 근거해서 운영되고 있다[1]. 미국은 [2)]HIPAA를 통해 개인 의료정보와 건강보험의 정보보호와 책임추적성에 대한 규제를 정하고 있고, 신용카드 정보를 보호하기 위하여 2006년부터 PCI-DSS(Payment Card Industry Data Security Standard)라는 지불카드관련 보안 표준이 제정되어 가맹점과 처리업체에 적용되고 있다[2][3]. 2013년에 정보보호관리체계 국제표준인 ISO/IEC의 ISO27001는 8년만에 전면 개정되었다[4].

최근 전자상거래와 핀테크(Fin-Tech)가 발전되고 있으며, 결제산업이 핀테크 분야의 핵심 인프라가 예상되어 지불카드 정보 보호의 중요성은 더욱 커지고 있다. VISA에 따르면 (그림 1)과 같이 개인정보(ID와 패스워드 등) 및 신용카드정보(카드번호, 유효기간, CVV 코드 등)의 유출로 인한 비대면거래시(CNP: Credit-Not-Present, 전화, 인터넷, 우편주문 등) 부정사용 규모는 전 세계적으로 연간 7천억 원 규모로 카드 부정사용 중 가장 큰 비중을 차지하고 있으며, 2008년 40% 에서 2013년 57%로 증가하는 추세이다[6][7]. 더 나아가 유출된 카드정보를 토대로 불법카드복제와 결제도 가능할 것으로 판단되어 핀테크 확산을 앞두고 더욱 우려가 커질 것으로 예상된다[5].



(그림 1) 신용카드 부정사용 유형별 트랜드[7]

국내도 카드 정보 유출로 인한 피해를 예방하기 위하여 지불카드 산업 관련 보안표준인 PCI-DSS (Payment Card Industry Data Security Standard)의 관심이 커지고 있다[5]. 여신금융협회 및 카드업계는 2014년 10월에 금융당국의 '전자상거래 결제 간편화 방안'의 후속조치 일환으로 온라인 구매 편의성 제고를 위해 간편 결제 방식 활성화를 위해 결제대행업체(PG

1) ㈜안랩 컨설팅본부 선임컨설턴트
2) HIPAA : The Health Insurance Portability and Accountability Act(미국의 의료정보보호법)

사)에 카드정보 저장을 위한 보안 및 재무적 기준을 마련하였다. 보안기준으로 PCI-DSS인증 취득, 결제대행업체 자체 부정사용 예방 시스템(Fraud Detection System, FDS) 및 재해복구센터 구축 등이 요구되고 있다[8].

간편결제서비스와 같은 핀테크 사업의 활성으로 인해 PCI-DSS의 관심과 인증의 필요성이 증가하고 있어, 본 논문 2장에서 지불결제 PCI-DSS 인증 적용 대상이 되는 신용카드 구조와 최근에 출시된 주요 간편결제서비스를 설명하고, 3장에서 PCI-DSS의 주요 구성 요소를 정리하여 프레임워크 형태로 제시한다.

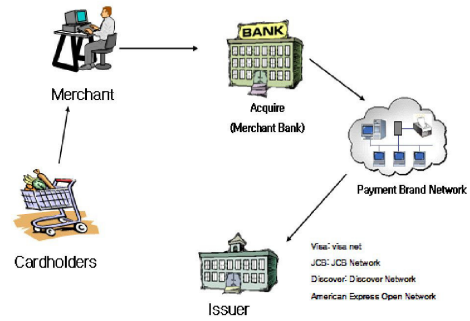
PCI-DSS 인증과 정보보호 인증체계를 중복으로 유지하는 기업은 인증 유지 및 운영에 부담으로 작용하고 있어, 4장과 5장에서 국내·외 정보보호 관련 인증과 PCI-DSS를 비교 분석한다.

2. 신용카드 결제체계와 간편결제 서비스

2.1 개요

지불결제 관련 보안표준을 이해하기 위해서는 카드산업 비즈니스의 이해가 필요하다. 지불카드 중 가장 많이 사용 되는 신용카드의 결제 구조(Scheme)는 국가 및 신용카드 브랜드 등 따라 다양하며, 결제흐름이 복잡하다. 신용카드 결제 흐름에 포함되는 당사자(Party)는 카드소유자(Cardholders), 가맹점(Merchant), 서비스제공자(Service Provider), 매입사(Acquire), 발행사(Issuer)이며, 신용카드 결제 절차를 간단히 정리하면 아래와 같다.

신용카드 소지자는 대형마켓이나 소매점과 같은 가맹점을 통하여 물품을 구매하면서 상점에서 카드를 사용하게 된다. 사용된 카드내역은 개인정보와 함께 신용카드결제 트랜잭션이 발생하며 이러한 트랜잭션은 가맹점 혹은 PG사나 VAN사와 같은 서비스 제공자의 결제정보 처리시스템을 통하여 은행과 같은 매입사와 발행사로 전송되게 된다. 이러한 카드결제 트랜잭션 흐름의 일부분을 담당하고 있는 기업은 카드결제정보 조회 및 승인 취소 등의 연계서비스를 위하여 정보시스템에 카드결제 정보를 저장하게 된다. 이상의 절차를 기본적인 흐름으로 도식화하면 (그림11)의 결제 카드 사업 흐름과 같다[9].



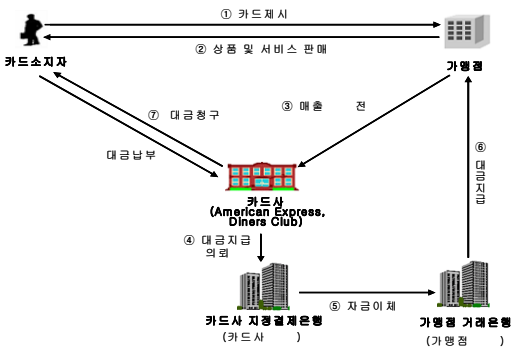
(그림 2) 결제 카드 사업 흐름[9]

2.2 신용카드 거래구조

신용카드 거래구조는 신용카드 발급사와 가맹점전표 매입사의 동일 여부에 따라 폐쇄형인 3당사자 구조(three party scheme)와 개방형인 4당사자 구조(four party scheme)로 구분된다[10][11].

2.2.1 3당사자 구조(Three Party Scheme)

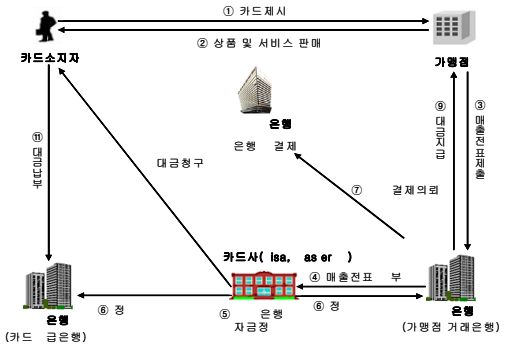
3당사자 거래구조는 카드소지자, 가맹점, 카드사업자 3개의 당사자가 거래에 참여하는 신용카드 거래가 이루어지는 구조이다. 신용카드사가 카드발행과 전표매입을 동시에 수행한다. 3당사 구조를 채택하고 있는 신용카드사는 외국의 Amex(American Express)와 Diners Club카드 등이다. (그림 3)과 같이 카드소지자가 가맹점에서 신용카드로 상품 등을 구매하면 가맹점은 매출내역을 카드사에 전송하고 카드사가 대금지급을 청구한다[10][11][13].



(그림 3) 3당사자 구조의 결제 흐름도[13]

2.2.2 4당사자 구조(Four Party Scheme)

4당사자 거래구조는 카드회원, 가맹점, 카드발급사, 전표매입사의 4개 당사자와 카드브랜드사를 중심으로 신용카드 거래가 이루어지는 구조이다. VISA, MASTER CARD가 4당사자 구조의 카드에 해당된다. (그림 4)와 같이 카드소지자가 가맹점에서 신용카드로 상품 등을 구매하면 가맹점은 거래은행으로, 거래은행은 카드사에 매출내역을 전송하고 카드사는 다자간 차액을 산출하여 가맹점거래은행에 통보한다[10][11][13].



(그림 4) 4당사자 구조의 결제 흐름도[13]

2.3 국내 신용카드 거래 구조

2.3.1 국내 신용카드 거래 구조 특징

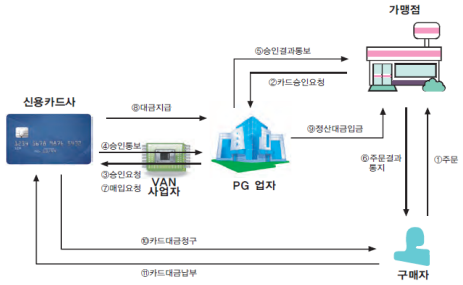
우리나라의 신용카드는 1969년 백화점 상점카드(store card) 형태로 도입되기 시작하였으며 다른 가맹점에서도 사용할 수 있는 신용카드는 1978년부터 은행들이 도입하기 시작하였다. 2014년 6월 기준으로 신용카드 사업자 현황은 총 23개이며, 전업카드사가 비씨, 신한, 하나, 롯데, 삼성 등 9개(은행계 6개, 기업계 3개)이고 겸영 은행이 NH농협, 전북은행, 기업은행 등 11개, 유통계 겸영 신용카드사업자가 현대백화점 등 3개이다[12]. 우리나라 신용카드 산업의 구조적 특징은 3당사자 거래구조와 4당사자형 거래구조가 혼재되어 있으나, 대부분의 국가와 달리 3당사자 거래 구조 비중이 현저히 높다. 비씨카드를 제외한 대부분의 전업카드사는 동일 신용카드업자가 회원업무와 매입업무를 동시에 수행하는 3당사자 거래 구조를 채택하고 있다[10][11][14].

2.3.2 신용카드 부가통신사업자(VAN사)

신용카드 부가통신사업자(value added network : VAN사)는 신용카드사와 가맹점간 통신망 구축 및 단말기 설치, 신용카드 거래의 전송 및 조회, 매출전표 수집 및 청구 대행 등 신용카드 지급결제와 관련한 다양한 부수업무를 한다. VAN사는 전자금융거래법 제2조 및 전자금융감독규정 제3조1호의 '전자금융보조업자'에 해당한다. 신용카드 소지자가 가맹점에서 거래대금을 신용카드로 결제하면 거래내역이 해당 카드사로 전송되고 카드사는 승인여부를 가맹점에 전송한다. 가맹점은 카드사에 매출전표를 제시하고 매입요청을 하게 되면 카드사는 매출전표를 매입한다. 한편, 이 과정에서 VAN사는 카드사를 대신하여 가맹점에 단말기를 설치, 관리하고 전표 매입 등을 대행하는데 VAN사는 이를 대가로 카드사 및 가맹점으로부터 수수료를 받는다. 카드사가 거래은행에 지급의뢰를 하면, 거래은행은 카드사의 계좌에서 가맹점의 계좌로 대금을 이체해준다. 카드사는 고객별로 정해진 대금 결제일에 맞추어 대금을 청구하고 고객이 이를 결제하면 거래가 종료된다[14][15]. 2015년 12월 기준 신용카드 VAN사는 한국정보통신, 케이에스넷, 나이스정보통신 등 17개 업체가 등록되어 있다[16].

2.3.3 결제대행업체(PG사)

구매자가 인터넷 쇼핑몰 등에서 신용카드로 대금을 결제하는 경우 신용카드 결제대행업체를 통해 지급결제절차가 수행된다. 결제대행업체는 신용카드회사와 계약에 따라, 신용카드회원에게 물품을 판매하거나 용역을 제공하는 자를 위하여 신용카드에 의한 거래를 대행하는 자를 의미한다. 보통 PG(Payment Gateway)업체라는 용어로 사용된다. PG사의 법적 지위는 전자금융거래법 제28조의 전자금융업자에 해당된다. 온라인 전자상거래의 경우 온라인쇼핑몰(가맹점)이 직접 신용카드사나 VAN사업자와 계약을 체결하고 신용카드거래를 발생시킬 수 있는 인프라를 갖추기 어렵다. 신용카드 PG업체는 해당 쇼핑몰과 VAN사업자나 신용카드사 사이에서 거래 및 승인 정보를 중계하고 정산을 대행한다. 결제진행 절차는 오프라인에서의 VAN사업자와 신용카드사간 지급결제절차와 동일하다[14][15].



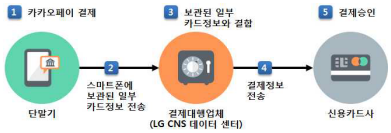
(그림 5) 신용카드 PG업체 결제흐름 절차[14]

2.4 주요 간편결제 서비스

최근 모바일 기기를 통한 간편결제 서비스가 출시되고 있으며 서비스에 따라 호환성(온/오프라인), 인증방식, 보안성 등 차별이 존재한다. 간편결제서비스는 디지털 결제서비스라고도 하며 주요 간편 결제 서비스는 카카오페이, 애플페이, 페이코, 삼성페이 등이 있다[17].

2.4.1 카카오 페이

카카오 페이는 모바일 메신저 기반의 서비스로 결제모듈(엠페이)을 내장함으로써, S/W기반(앱)의 편의성·보안성을 제공한다. 카카오 페이를 통해 온라인만 결제가 가능하며, 결제방식은 PIN 번호 입력 후 단말기에 저장된 일부 결제정보를 결제대행업체에 전송하여 결제정보를 결합시킨 후 결제정보를 신용카드사로 전송한다[17].



(그림 6) 카카오 페이 결제방식[17]

2.4.2 애플 페이

애플 페이는 스마트폰 단말 및 운영체제 공급을 지원함으로써, S/W 및 H/W기반의 호환성·편의성·보안성을 제공하며, 웨어러블 디바이스(애플워치)와의 연계를 통해 추가적인 기능을 제공한다. 근거리 무선통신(NFC, Near Field Communication)을 이용한 오프라인 결제 기능이 있다. 결제방식은 지문인증을 통해 본인 확인 과정을 거쳐 토큰화된 결제 정보가 가맹점을 통해 매입사에 전달되고, 매입사에서 토큰 정보를 검증한 후 승인 여부를 결정하여 카드발행사에 결제를 요청한다[17].

(그림 7) 애플 페이 결제방식[17]

2.4.3 페이코

페이코는 다수의 온·오프라인 가맹점을 확보하여 결제정보를 서버에 저장함으로써, S/W 기반(앱)의 편의성·보안성을 제공한다. [3]NFC를 터치하거나, 제품 택(TAG)에 부착된 QR코드를 스마트폰으로 촬영하여 상품결제가 가능하지만, 오프라인 결제의 경우는 티머니 가맹점에 한하여 이용이 가능한다. 결제방식은 사전에 등록한 PIN 번호를 입력하면, 서버에 저장된 결제정보를 신용카드사로 전송한다[17].

(그림 8) 페이코 결제방식[17]

2.4.4 삼성페이

삼성페이는 스마트폰 단말 공급 제조사로써 H/W기반(기기내장형)의 호환성·편의성·보안성을 제공한다. 특히 NFC, 마그네틱방식(MST : Magnetic Secure Transmission) 결제를 모두 지원하여 호환성이 높다. 결제정보가 토큰형태로 가맹점으로 전송, 토큰은 카드발급사로 전달되어 검증 후 승인 처리된다[17].

(그림 9) 삼성페이 결제방식[17]

3) NFC : Near Field Communication(근거리무선통신)

2.4.5 간편결제서비스 출시 후 카드구조 변화

간편결제 서비스가 온라인 결제 뿐 아니라 오프라인결제까지 가능해지면서, 카드 결제 프로세스에 전자전표매입과 같은 VAN사의 역할이 축소되고 있다[18].

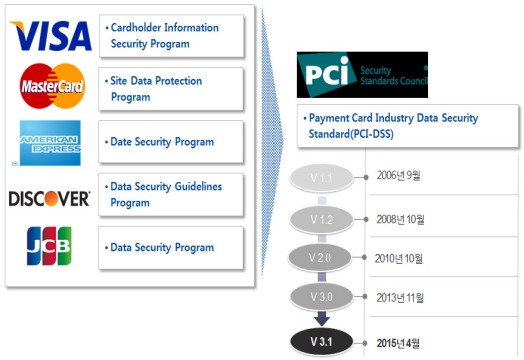
2015년 11월에 인터넷은행 설립 예비인가를 받은 카카오뱅크는 카드사·VAN사·PG사 없는 간편결제 서비스를 핵심제공 서비스로 계획하는 등 향후 신규 간편결제 서비스를 통해 결제 구조체계 변화가 예상된다[19].

3. PCI-DSS 프레임워크

3.1 개요

카드 정보 노출 사고 급증과 정보보호의 중요성이 인식되면서 2004년에 VISA, MASTER와 같은 주요카드회사들이 협력하여 PCI-SSC(Payment Card Industry Security Standards Council)을 설립하였다. (그림10)과 같이 PCI-DSS가 발효되기 전에는 VISA, MASTER CARD, AMERICA EXPRESS, DISCOVER, JCB 각 카드 브랜드별로 보안프로그램을 운영하고 있었으나, 2006년 9에 PCI-SSC에서 PCI-DSS(Payment Card Industry Data Security Standards) V1.1을 제정하였다[3]. 그 후 4번의 개정이 진행이 되었고, 최신 버전은 2015년 4월부터 발효된 PCI-DSS V3.1이다[2].

PCI-DSS는 주요 구성요소인 평가기준, 보호 정보, 적용 대상 시스템(인증범위), 준수대상, 평가 방법 및 절차를 기준으로 (그림2)와 같이 프레임워크로 표현할 수 있다.



(그림 10) PCI-DSS 발전 과정

3.2 PCI-DSS 평가 기준

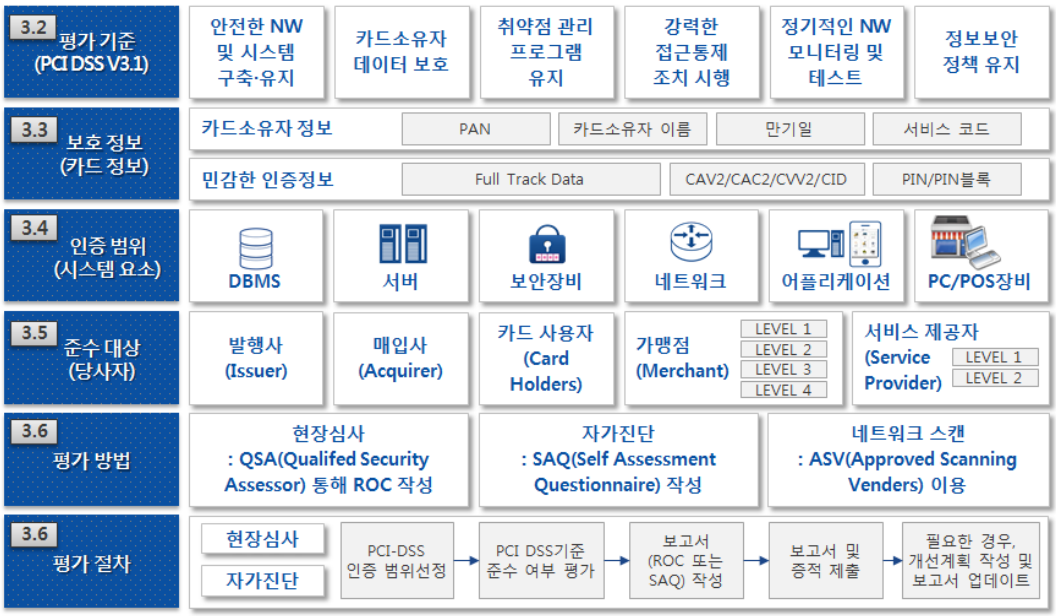
PCI-DSS는 카드소유자 정보의 보안을 강화하고 국제적으로 일관된 보안 평가기준을 적용하기 위해 개발되었다. PCI-DSS는 계정 데이터를 보호하기 위한 기술적, 관리적, 물리적 영역 보안기준을 제공한다. 기술적 영역은 안전한 네트워크와 시스템 구축 및 유지, 카드 소유자 데이터 보호, 취약점 관리 프로그램 유지, 카드정보 및 시스템 접근통제, 정기적 보안테스트 영역이며, 물리적 영역은 카드소유자 데이터에 대한 물리적 접근제한이 해당되고, 관리적 영역은 모든 직원에 대해 정보보안정책 유지 영역이다. PCI-DSS 평가 기준은 (표 2)와 같이 6개 부문, 12개 영역, 77개 항목, 244개 세부항목으로 구성되어 있고 부록에 호스팅업체에 대한 통제 관련 내용이 포함되어 있다.

3.3 PCI-DSS 보호 대상 정보

PCI-DSS의 보호 대상 정보는 (표 1)과 같이 지불카드정보(Account Data)이다. 지불카드정보는 카드소유자 정보(Cardholder Data)와 민감한 인증정보(Sensitive Authentication Data)로 구분된다. 카드소유자 정보는 카드번호에 해당되는 기본 계정정보(Primary Account Number : PAN), 카드 소유자 이름(Cardholder Name), 만기일(Expiration Data), 서비스코드(Service Code)이고, 민감한 인증정보는 Full track data(마그네틱선 데이터나 그에 준하는 칩상의 데이터), CAV2/CAC2/ CVV2/ CID,PIN/PIN블록이다. 카드번호(Primary Account Number : PAN)는 카드정보를 식별할 수 있는 유일한 요소이다[2].

(표 1) 지불카드정보(Account data) 유형

구분	정보 내용
카드소유자 정보 (Cardholder Data)	- 기본 계정 번호 (Primary Account Number) - 카드 소유자 이름 (Cardholder Name) - 만기일(Expiration Data) - 서비스 코드(Service Code)
민감한 인증정보 (Sensitive Authentication Data)	- Full Track data (maganetic-stripe data or equivalent on a chip) - CAV2/CAC2/CVV2/CID - PIN/PIN블록



(그림 11) PCI-DSS 프레임워크

(표 2) PCI-DSS 평가기준

구분	내용	항목수	세부 항목수
안전한 네트워크와 시스템 구축 및 유지	1. 카드 소유자 데이터를 보호하기 위한 방화벽 설치 및 유지한다. (방화벽 운영)	5	23
	2. 공급자가 제공한 기본 설정값을 시스템 패스워드와 기타 보안 파라미터에 사용하지 않는다.(기본 설정 변경)	6	12
카드 소유자 데이터 보호	3. 저장된 카드 소유자 데이터 보호한다.(저장된 카드정보 보호)	7	21
	4. 공개된 공공 네트워크를 통해 카드 소유자 데이터를 전송하는 경우 암호 전송한다.(카드정보 전송 보안)	3	4
취약점 관리 프로그램의 유지	5. 악성코드로부터 모든 시스템을 보호하고 안티 바이러스 소프트웨어 또는 프로그램을 정기적으로 업데이트한다.(안티 바이러스)	4	6
	6. 안전한 시스템과 어플리케이션을 개발하고 유지한다.(개발 및 운영)	7	28
강력한 접근통제 조치의 시행	7. 사업상 알 필요가 있는지에 따라 카드 소유자 데이터의 접근 제한한다.(카드정보 접근통제)	3	10
	8. 시스템 구성요소에 대한 접근을 식별하고 인증한다.(시스템 접근통제)	8	23
	9. 카드 소유자 데이터에 대한 물리적 접근 제한한다.(물리적 접근 제한)	10	27
정기적인 네트워크 모니터링과 테스트	10. 네트워크 자원이나 카드 소유자 데이터에의 접근 추적 및 모니터링한다. (접근추적 및 모니터링)	8	32
	11. 정기적으로 보안 시스템과 보안 프로세스를 테스트한다.(정기적 보안테스트)	6	19
정보 보안 정책의 유지	12. 모든 직원에 대한 정보 보안과 관련된 정책을 유지한다.(정보보안 정책)	10	39
부록	A. 호스팅 업체에 대한 추가 요구사항	4	5
소 계		81	249

3.4 PCI-DSS 인증 범위(Scope)

PCI-DSS 평가의 첫 단계는 인증 범위를 정하는 것이다. PCI-DSS의 인증 범위는 카드소유자 정보 환경(Cardholder data Environment : CDE)을 포함하거나 연결되는 모든 시스템 요소(System Components)이다. 카드소유자 정보 환경(CDE)은 카드소유자 정보나 민감한 인증정보가 저장, 처리, 전송되는 사람, 절차, 기술로 구성된다. 시스템 요소는 네트워크 장비, 보안시스템, 서버, 컴퓨터 장비, 응용프로그램 등을 포함한다. 인증 대상 기관은 인증범위 설정을 위해서 카드소유자 정보 환경을 식별하고 정의해야 된다. 그리고 목록이나 다이어그램을 통해 인증범위 대상이 정리가 되어야 된다. 인증대상 자산이 외주업체를 통해 아웃소싱이 될 경우, 인증 대상 기관은 카드정보가 처리되는 시스템 요소를 식별하고 매년 자체 평가 또는 교차평가를 통해 PCI-DSS 준거성을 증명해야 한다[2].

3.5 PCI-DSS 준수 대상(당사자)

본 논문 2장의 신용카드 결제 구조에서 살펴본 것과 같이 신용카드 결제 절차의 당사자는 카드소유자, 가맹점, 서비스 제공업체(카드정보를 저장·처리·전송하는 VAN사, PG사, 간편결제 서비스 등), 매입사, 발행사이다. 발행사와 매입사는 PCI-DSS를 준수하고, 가맹점과 서비스 제공업체가 카드소유자의 카드정보를 보호하고 PCI-DSS를 준수할 수 있도록 통제하는 역할을 수행한다. VISA의 경우 일정규모 이상 카드정보를 처리하는 가맹점과 서비스 제공업체를 PCI-DSS 인증 의무 대상으로 보고 있다. VISA는 인증 의무 대상을 매년 카드 트랜잭션 처리수와 사고발생 위험에 따라 (표 3)과 (표 4)와 같이 등급(level)을 나누고, 등급별로 인증 유지방법을 다르게 정하고 있다[21]. Level 1이 가장 상위 등급이다.

우리나라는 결제대행업체(PG사)가 카드정보를 저장하는 경우 보안기준으로 PCI-DSS인증 취득이 권고되고 있다[8].

(표 3) 트랜잭션 처리기준 서비스 제공업체 레벨

서비스 제공업체 등급		PCI-DSS 인증 방법		
구분	연간 처리 트랜잭션	현장심사 (QSA)	자가 진단(SAQ)	네트워크 스캔(ASV)
Level 1	30만 건 이상	매년 필수	선택	분기별 필수
Level 2	30만 건 미만	선택	매년 필수	분기별 필수

(표 4) 트랜잭션 처리기준 가맹점 레벨

가맹점 등급		PCI-DSS 인증 방법		
구분	연간 처리 트랜잭션	현장 심사 (QSA)	자가 진단(SAQ)	네트워크 스캔(ASV)
Level 1	6백만 건 이상	매년 필수	선택	분기별 필수
Level 2	1백만 ~ 6백만 건	선택	매년 필수	분기별 필수
Level 3	2만 ~ 1백만 건	선택	매년 필수	분기별 필수
Level 4	2만 건 이하	선택	매년 권고	분기별 필수

3.6 PCI-DSS 평가 방법 및 절차

PCI-DSS 준수 대상은 등급에 따라 매년 현장 보안심사(on-site Security Assessment) 또는 자가진단(Self-Assessment)을 수행하고, 분기별로 네트워크 스캔(Network Scan)을 해야 한다.

VISA의 PCI-DSS 기준으로 Level1에 해당하는 가맹점과 서비스제공업체는 매년 필수적으로 현장 보안심사를 받아야 하고, Level1에 해당하지 않는 대상은 매년 자가진단을 수행해야 한다. 현장보안심사는 PCI-SSC에서 인정한 QSA(Qualified Security Assessor)를 통해서 진행되며, QSA는 PCI-DSS요구사항 준수여부를 평가한다. QSA는 현장보안심사 진행 후 ROC(Report on Compliance)를 작성한다. ROC의 템플릿은 PCI-SSC에서 제공하며, 세부 내용과 요구사항은 카드 브랜드별로 일부 다를 수 있다[2][22]. 자가 진단은 PCI-DSS기준으로 준수대상 기업이 자체적으로 평가하고 SAQ(Self-Assessment Questionnaire)를 작성하여 관련 증적과 함께 매입사나 발행사에 보고한다.

PCI-DSS 준수 대상은 연간 트랜잭션 처리규모에 관계없이 분기별로 네트워크 스캔을 수행해야 한다. 네

트워크 스캔은 PCI-DSS에서 인정한 ASV(Approved Scanning Vendors)의 취약점 진단 서비스나 툴을 통해서 수행된다[2][23].

PCI-DSS 평가절차는 PCI-DSS 인증범위를 확정하고, 현장심사나 자가진단을 통해 PCI-DSS 기준 준수여부를 평가한다. 현장심사의 경우 QSA는 평가 완료 후 ROC를 작성하고, 자가진단의 경우 준수기관은 SAQ를 작성한다. 그리고 보고서(ROC나 SAQ)를 분기별로 진행된 네트워크 진단 결과와 같은 증적을 매입사나 발행사에 제출한다. 필요한 경우, 개선계획을 작성하거나 보고서를 수정해서 제출한다[2].

4. 국내·외 정보보호 및 개인정보보호 인증제도

정보보호 인증제도로 국제 표준인 ISO27001:2013과 KISA에서 운영하는 ISMS가 있고, 개인정보보호 인증으로 KISA에서 운영하는 PIMS와 NIA에서 운영하는 PIA가 있다.

4.1 KISA ISMS 인증 제도

ISMS(Information Security Management System)인증제도는 정보보호 관리체계를 구축·운영하고 있는 조직에 대해 정보보호 관리체계의 인증기준에 적합한지를 인증기관이 객관적이고 독립적으로 평가하여 적합성 여부를 판단해 주는 제도이다.

국내 기업이 스스로 정보보호 관리체계를 구축·운영하는데 활용할 수 있도록 관리체계 모델을 개발하고, 정보통신망법 개정을 통하여 정보보호 관리체계인증 제도를 2001년 7월에 도입하였다. 국내 기업의 실정을 반영한 관리체계를 도입하였으며, 이를 통해 기업 정보보호 수준을 제고하고자 하였다.

2012년 정보통신망법 개정으로 종전의 정보보호 안전진단제도가 폐지되고 정보보호 관리체계 인증 제도로 일원화 되었다. 또한, 주요정보통신서비스제공자를 정보보호 관리체계 인증 제도의 인증 의무대상자로 지정하여 운영하게 되었다. 2015년 12월 기준으로 ISMS 인증 유지 기업은 396개이며, 2015년 12월 정보통신망법 개정으로 2016년 6월부터 ISMS인증 의무대상자가 대폭 확대 적용된다. ISMS 의무대상자가 인증을 받지 않은 경우 과태료도 1천만원에서 3천만원으로 증액되었다[1]. ISMS 인증기준은 2013년에 ISMS 인증기준이 IT현황에 맞게 전면 개정되었으며 정보보호관리과정과 정보보호대책으로 구분이 된다. 정보보호관리과정은 5개 영역, 22개 항목으로 구성되어 있고, 정보보호대책은 (표 5)와 같이 9개 영역 92개 통제항목으로 되어 있다[24].

(표 5) KISA ISMS 인증 기준(정보보호대책)

영역	보호대책	항목수	세부 항목수
1. 정보보호 정책	정책의 승인 및 공표, 정책의 체계, 정책의 유지관리	6	13
2. 정보보호 조직	조직의 체계, 책임과 역할	4	7
3. 외부자 보안	보안요구사항 정의, 외부자 보안	3	4
4. 정보자산 분류	정보자산의 조사 및 책임할당, 정보자산의 분류 및 취급	3	7
5. 정보보호 교육	교육 프로그램 수립, 교육의 시행 및 평가	4	10
6. 인적보안	책임할당 및 규정화, 직원의 적격 심사, 주요직무 담당자 관리, 비밀유지	5	11
7. 물리적 보안	물리적 보호구역, 접근통제, 데이터 센터 보안, 장비보호, 사무실 보호	9	21
8. 시스템개발 보안	분석 및 설계, 구현 및 이행, 변경관리	10	22
9. 암호통제	암호정책, 암호사용, 키 관리	2	8
10. 접근통제	접근통제 정책, 사용자 접근 관리, 접근통제 영역	14	46
11. 운영보안	운영절차와 책임, 시스템, 네트워크 운영, 악성소프트웨어 통제, 원격 통제	22	56
12. 침해사고 관리	대응계획 및 체계, 대응 및 복구, 사후관리	7	14
13. IT 재해 복구	업무연속성 관리체계 수립, 업무연속성 계획, 시험 및 유지관리	3	6
소계		92	225

(표 6) ISO27001:2013 통제항목

영역	영역별 항목	항목 수
A.5 보안정책	정보보호에 대한 관리	2
A.6 정보보호에 대한 조직	내부 조직, 모바일 장치 및 원격근무	7
A.7 인적자원 보안	고용 전 보안, 고용 중 보안, 고용의 종료 및 변경	6
A.8 자산관리	자산의 책임, 정보의 등급화, 미디어 취급	10
A.9 접근 통제	접근통제에 대한 비즈니스 요구사항, 사용자 접근 관리, 사용자 책임.시스템 및 응용프로그램 접근 통제	14
A.10 암호화	암호화 통제	2
A.11 물리적 환경적 보호	물리적 환경적 보호, 장비 보호	15
A.12 운영 보안	문서화된 운영절차, 악성소프트웨어 보호, 백업, 로깅과 모니터링, 소프트웨어 통제, 기술적 취약점 관리, 정보 시스템 감사 고려사항	14
A.13 통신 보안	네트워크 보안 관리, 정보 전송	7
A.14 시스템 인수/개발/유지보수	시스템 인수 및 개발 그리고 유지보수, 개발 보안 및 지원 프로세스, 테스트 데이터	13
A.15 공급자 관계	공급자 관계내의 정보보호, 공급자 서비스 제고 관리	5
A.16 정보보호 사고 관리	정보보호 사고에 대한 관리 및 개선	7
A.17 업무 연속성 관리	정보보호 연속성, 이중화	4
A.18 준수	법 및 계약적 요구사항에 대한 준수, 정보보호 리뷰	8
소계		114

(표 7) PIMS 통제항목

영역	영역별 인증 내용	항목 수
1. 관리체계 수립	정책 및 범위, 조직, 경영진의 책임	9
2. 실행 및 운영	개인정보 식별, 위험관리	5
3. 검토 및 모니터링	개인정보 보호체계의 검토	3
4. 교정 및 개선	교정 및 개선 활동, 내부 공유 및 교육	2
5. 개인정보 생명주기 관리	개인정보 수집 시 보호조치, 개인정보 이용 및 제공 시 보호조치, 개인정보 보유 시 보호조치, 개인정보 파기 시 보호조치	15
6. 정보주체 권리보장	권리보장	3
7. 관리적 보호조치	교육 및 훈련, 개인정보 취급자 관리, 위탁업무 관리, 침해사고 관리	11
8. 기술적 보호조치	접근권한 관리, 접속기록 관리, 운영보안, 암호화 통제, 개발보안	23
9. 물리적 보호조치	영상정보처리기기 관리, 물리적 보안관리, 매체 및 출력물 관리	9
소 계		86

(표 8) PIA 평가항목

영역	분야	항목 수
I. 대상기관의 개인정보 보호 관리체계	1. 대상기관 개인정보 보호조직	4
	2. 개인정보 보호계획	2
	3. 개인정보 처리방침	7
	4. 개인정보파일 관리	6
	5. 개인정보 위탁 및 제공 시 안전조치	2
	6. 개인정보 침해 대응	4
	7. 정보주체 권익 보호	3
	8. 개인정보 처리구역 보호	3
II. 대상시스템의 개인정보보호 관리체계	1. 대상시스템의 개인정보관리	2
	2. 개인정보 취급내용 공개	6

영역	분야	항목 수
III. 개인정보 처리단계별 보호	1. 수집·이용 단계	12
	2. 저장·보유 단계	4
	3. 연계·제공 단계	40
	4. 파기 단계	3
IV. 특정IT기술 활용 시 개인정보 보호	1. CCTV 활용	5
	2. RFID 활용	7
	3. 바이오정보 활용	2
	4. 위치정보 활용	2
소계		114

4.2 ISO27001:2013 인증 제도

ISO27001은 국제표준 정보보호 인증으로, 영국표준(BS, British Standard)인 BS7799에서 2005년 11월에 ISO 표준이 되었다. 2005년 최초 제정 이후 8년 만에 개정된 ISO 27001:2013은 클라우드 컴퓨팅 등 최신 IT 내용이 반영되었으며, 다른 ISO 경영시스템과 같이 High Level Structure라는 공통된 프레임워크가 반영되었다[4]. 2015년 12월 정보통신망법 개정으로 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 ISMS 인증의무 대상 기관은 인증 심사의 일부를 생략할 수 있다고 규정되어 있다[1]. ISMS인증 심사의 세부 생략 범위에 대한 고시가 아직 정해지지 않았지만, ISO27001이 국제표준 정보보호 인증에 해당 되것으로 보인다. ISO27001:2013은 (표 6)과 같이 13개 영역에 대해 114개 항목으로 구성되어 있다.

4.3 PIMS(개인정보보호관리체계) 인증 제도

PIMS(Personal Information security Management System)는 개인정보보호관리체계를 수립운영하고 있는 조직에 대하여 인증심사를 기준으로 적합한지 여부를 인증기관이 평가하여 인증을 부여하는 제도이다.

방송통신위원회 심의·의결 '개인정보보호 관리체계 인증제 동비에 관한건'(제2010-66-273)으로 2010년부터 도입되었고, 2013년에 정보통신망법이 개정되어 법률에 의해 시행되었다. PIMS와 유사한 인증제도로 PIPL이 있었으나 2015년 정보통신망법 개정으로 2016년부터 PIPL과 PIMS가 PIMS로 통합되어 운영된다. PIMS는 ISMS와 달리 인증의무 대상자가 지정되어 있지 않고, 기업 및 기관은 자율적으로 PIMS 인증을 유지하고 있다. 2015년 12월 기준으로 PIMS 인증 유지 기관은 40개이고, PIPL 인증 유지 기관은 16개이다. 개인정보 유출 사고의 지속적인 발생과 대형 정보통신서비스 제공자의 경우에도 개인정보보호 관리체계 인증 획득의 경우가 많지 않아서 2015년11월에 PIMS인증의무 대상자 지정에 관해 정보통신망법 일부개정법률안이 의안 발의되었고, 2015년 12월 기준으로 소관위원회(미래창조과학방송통신위원회)에서 심사가 진행되고 있다[27].

PIMS 인증심사 기준은 (표 7)과 같이 9개 영역, 86개 항목으로 구성되어 있으며, 신청기관(공공기관/대기업/중소기업/소상공인)유형에 따라 심사항목이 차등 적용된다[25].

4.4 PIA(개인정보영향평가) 제도

PIA(Privacy Impact Assessment)란, 개인정보를 활용하는 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경 시 동 시스템의 구축·운영·변경 등이 개인정보에 미치는 영향(impact)에 대하여 사전에 조사·예측·검토하여 개선 방안을 도출하는 체계적인 절차이다.

2011년 개인정보보호법 제정으로 일정규모이상 개인정보파일 운영 공공기관은 의무 대상이다. 기존에 운용중인 시스템에 대한 영향평가는 개인정보 보호법 시행령 제35조에 따라 2016년 9월 30일 이전까지 개인정보 영향평가를 실시해야 된다. 개인정보 침해요인 분석을 위한 평가항목은 (표 8)과 같이 4개 평가영역, 18개 평가분야에 대하여 총 114개의 기준으로 구성되어 있다[26].

5. PCI-DSS와 정보보호 및 개인정보 보호 인증제도 비교

PCI-DSS와 정보보호인증(ISO27001, ISMS) 및 개인정보보호 인증(PIMS, PIA)을 제도적 측면과 평가/통제 영역 기준으로 비교할 수 있다.

5.1 제도적 측면

각 인증별 제도적 관점에서 비교는 (표 9)와 같이 보호 대상, 통제구현 방법, 의무 여부, 인증 유효 기간 등으로 구분할 수 있다.

보호 대상 정보/자산 기준으로 PCI-DSS의 통제목적은 카드정보 보호이고, PIMS, PIA의 목적은 개인정보 보호이다. ISMS와 ISO27001은 정보자산의 보호를 목적으로 한다. PCI-DSS는 카드정보 분야에 특화된 인증체계로, PCI-DSS는 보호 대상 정보(Account data)가 인증기관에 의해 확정되어 있기 때문에 다른 인증제도보다 인증범위와 통제 대상(시스템) 식별이 용이하다.

통제구현 방법을 기준으로 ISO27001과 ISMS는 위험관리 기반으로 위험평가를 통해 평가/보호대책 항목의 준수 여부를 선택 할 수 있다. 그러나 PCI-DSS는 평가 기준을 모두 준수해야만 인증이 유지된다[3]. PIMS와 PIA는 기본적으로 위험관리 기반이지만 개인정보보호법이나 정보통신망법에서 요구하는 내용은 필수적으로 준수해야 인증을 획득 할 수 있다. PIMS와 PIA의 대부분의 항목이 개인정보보호 관련 법령에 근거해서 만들어져서 실질적으로는 통제항목을 준수해야 한다고 볼 수 있다.

인증의무 대상 기준으로 PCI-DSS, ISMS, PIA는 일정 규모(기준) 이상의 기업 및 기관은 의무 대상자가 되지만, ISO27001과 PIMS는 의무 대상이 없이 자율적으로 운영된다. 정보보호 사고 발생과 개인정보보호 중요성

(표 9) 정보보호 인증 제도 비교

구분	PCI-DSS	KSIA ISMS	ISO27001:2013	PIMS	PIA
국내외	국제	국내	국제	국내	국내
분야	개인정보(지불카드) 정보보호	정보보호	정보보호	개인정보보호	개인정보보호
통제 구현방법	필수	위험관리 기반	위험관리 기반	위험관리 기반	필수
심사/평가 기관	QSA, ASV	KISA, TTA, 금융보안원, KAIT	BSI, DNV 등	KISA	개인정보영향평가 전문업체
인증기관	PCI SSC	KISA, 금융보안원	BSI, DNV 등	KISA	NIA
국내 관련법령	-	정보통신망법 제47조의2	-	정보통신망법 제47조의3 개인정보보호법 제13조	개인정보보호법 제33조
의무여부	의무	의무	자율	자율	의무
인증 대상기관	일정 규모(기준) 이상 가맹점, 서비스제공자 등 카드정보 처리자	일정 규모(기준) 이상 정보통신서비스 제공자, IDC사업자, 기간통신사업자	국내외 모든 기관(기업)	개인정보처리자	일정 규모(기준) 이상 개인정보파일을 운영하는 공공기관
인증/평가 기준	6개 분야 12개 영역 77개 평가기준 245개 세부 기준	14개 영역 104개 통제항목 253개 세부 점검사항	13개 영역 114개 통제항목	9개 영역 86개 점검항목	4개 분야 18개 영역 114개 평가기준
유효기간	1년 (분기별 네트워크 진단)	3년 (매년 사후심사)	3년 (매년 사후심사)	3년 (매년 사후심사)	평가 후 변경 없으면 유효

이 커지면서 인증 의무 대상이 확대되는 추세에 있다.

평가/심사기관은 PCI-DSS, ISMS, ISO27001, PIMS, PIA 공통적으로 인증제도가 독립적인 심사기관을 통해서 인증 준수 여부에 대해 심사 및 평가를 진행하고 있다.

인증 유효기간을 기준으로 ISMS, ISO27001, PIMS는 인증 획득 후 3년간 유효하며 매년 사후심사, 3년 후에는 갱신심사가 진행이 된다. 반면 PCI-DSS는 매년 인증유지를 위해서 QSA를 통한 현장보안심사를 받거나 자가진단을 수행해야 하고, 매분기 별로 네트워크 진단을 수행해야 한다. PIA의 경우 개인정보처리시스템 대상으로 평가가 완료 된 후 신규 도입이나 변경이 없으면 인증이 유지된다. 즉 개인정보처리시스템 변경이 발생된 경우에 다시 PIA 평가를 받는다.

(표 10) PCI-DSS와 정보보호인증 평가/통제 영역 매핑

KSIA ISMS(2013.5)														ISO27001:2013												
1. 정보보호정책	2. 정보보호조직	3. 외부자보안	4. 정보자산분류	5. 정보보호교육	6. 인적보안	7. 물리적보안	8. 시스템개발보안	9. 암호통제	10. 접근통제	11. 운영보안	12. 침해사고관리	13. IT재해복구	PCI-DSS V3.1	A.5 보안정책	A.6 정보보호조직	A.7 인적자원보안	A.8 자산관리	A.9 접근통제	A.10 암호화	A.11 물리적보호	A.12 운영보안	A.13 통신보안	A.14 시스템인수,개발,유지보수	A.15 공급자관계	A.16 정보보호사고관리	A.17 업무연속성	A.18 준수
									√	√			1. 방화벽 운영					√			√						
			√				√			√			2. 기본 설정 변경				√				√		√				
								√					3. 저장된 카드정보 보호						√			√					
								√					4. 카드정보 전송 보안									√					
										√			5. 안티 바이러스								√						
							√			√			6. 개발 및 운영 보안								√		√				
							√		√				7. 카드정보 접근통제					√					√				
			√						√				8. 시스템 응용프로그램 접근통제				√	√									
		√				√							9. 물리적 접근 제한							√							
										√	√		10. 접근 추적 및 모니터링					√			√						
							√			√			11.정기적인 보안테스트								√		√				
√		√		√	√						√	√	12. 정보 보안정책	√		√									√	√	√
		√							√	√			A.호스팅 업체 카드 정보 보호					√			√			√			

(표 11) PCI-DSS와 개인정보보호 인증 평가/통제 영역 매핑

PIMS(2016.1)										PIA(2014.11)																			
											Ⅰ.대상기관 개인정보관리체계								Ⅱ.대상시스템		Ⅲ. 처리단계별 개인정보 보호				Ⅳ. 특정IT기술 활용 개인정보			
1.관리체계수립	2.실행및운영	3.검토및모니터링	4.교정및개선	5.개인정보생명주기관리	6.정보주체권리보장	7.관리적보호조치	8.기술적보호조치	9.물리적보호조치	PCI-DSS V3.1	1.대상기관개인정보보호조직	2.개인정보보호계획	3.개인정보처리방침	4.개인정보파일관리	5.위탁및제공시안전조치	6.개인정보침해대응	7.정보주체권익보호	8.개인정보처리구역보호	1.대상시스템의개인정보관리	2.개인정보취급내용공개	1.수집·이용단계	2.저장·보유단계	3.연계·제공단계	4.파기단계	1.CCV활용	2.RFID활용	3.바이오정보활용	4.위치정보활용
							√		1. 방화벽 운영													√						
							√		2. 기본 설정 변경													√						
							√		3. 저장된 카드정보 보호												√							
							√		4. 카드정보 전송 보안													√						
							√		5. 안티 바이러스													√						
							√		6. 개발 및 운영 보안											√	√	√	√					
						√			7. 카드정보 접근통제									√		√	√	√	√					
							√		8. 시스템 응용프로그램 접근통제											√	√	√	√					
								√	9. 물리적 접근 제한								√											
		√				√	√		10. 접근 추적 및 모니터링												√	√						
		√							11.정기적인 보안테스트													√						
√	√			√	√	√			12. 정보 보안정책		√	√	√		√	√		√	√					√	√	√	√
						√	√		A.호스팅 업체 카드 정보 보호					√						√	√	√	√					

5.2 평가/통제 영역 기준

평가/통제 영역(대분류) 기준으로 PCI-DSS는 12개, ISO27001는 14개, ISMS는 13개, PIMS는 9개, PIA는 18개로 구성되어 있다. 본 논문에서는 (표 10),(표 11)과 같이 PCI-DSS를 기준으로 정보보호인증(ISO27001, ISMS)과개인정보보호 인증(PIMS, PIA)의 공통 영역을 매핑하였다. PCI-DSS 평가 기준과 ISMS, ISO27001의 영역은 비슷하게 연결이 된다. 하지만 PIMS와 PIA의 경우 개인정보 라이프 사이클(수집, 이용, 저장, 제공, 파기)의 법적 준거성 부분과 같이 개인정보보호법의 내용이 있는 영역은 매핑이 되기 어렵다. 정보보호 실

무에서는 여러 인증 평가 기준으로 진단(Gap 분석)과 적용할 경우 세부 점검 항목까지 매핑을 하지만 유효성 부분에서는 검증이 필요하여 세부 점검항목 간 비교는 향후 연구 과제로 남긴다.

6. 결 론

간편결제서비스와 같은 핀테크 사업의 활성으로 인해 카드정보보호에 특화된 PCI-DSS의 관심이 증대되고 있어서, 지불결제 PCI-DSS 인증 적용 대상이 되는 결제관련 비즈니스와 PCI-DSS의 주요 구성요소를 프레임워크 형태로 살펴보았다. 그리고 PCI-DSS 인증과 정보보호관리체계(ISMS, ISO27001:2013) 및 개인정보보호관리체계(PIMS, PIA)를 비교했다.

PCI-DSS를 비롯한 정보보호 관련체계를 준수해야 하는 기업의 입장에서 컴플라이언스에 대한 부담이 발생한다. 일본의 경우 일본 기업표준 정보보호관리체계인 ISMS인증을 PCI-DSS인증을 받은 경우 중복항목을 면제 해주고 있다[3]. 국내에서 최근 정보통신망법 개정으로 ISMS 인증시 국제인증을 받거나 정보보호 조치를 취한 경우 인증심사 일부 생략을 인정 근거가 생겼다. 세부 고시가 아직 발표되지 않았지만 PCI-DSS 인증도 ISMS 일부를 면제 범위에 포함 되어 인증대상 기업의 부담을 줄일 수 있을 것이라고 생각된다.

PCI-DSS, ISO 27001, ISMS, PIMS, PIA 통제 요구사항(보호대책)은 전체적으로 매핑이 되며 조직에게 적용되는 법률, 비지니스 상황, 보안 요구사항 목표 및 목적에 따라 유연하게 선택하거나 추가하여 적용하는 게 효과적이다. 국내외 정보보호 관련 인증체계의 요구사항(보호대책)은 포괄적이므로 조직의 보안 수준, 보안 목표 수준에 따라 선택하거나 추가하여 적용 하는 것을 고려하여야 한다. 또한, 보안 사고 측면에서 통제 항목을 모두 적용하더라도 보안 사고가 발생 가능하므로 통제 수준을 지속적으로 보장하는 것이 필요하다.

PCI-DSS는 카드정보 보호를 위하여 카드정보가 처리되는 모든 시스템의 보안통제를 위하여 기술적, 관리적 기준으로 최근 기술 동향이 반영되고 있다. 따라서 PCI-DSS 의 의무 대상이 아닌 기관의 경우에도 기관이 보호해야할 중요정보를 정의하고, 정보유출 위험을 감소시키기 위하여 PCI-DSS에서 요구하는 보안통제 항목을 기관의 현황에 맞게 적용할 수 있다.

향후에 PCI-DSS와 정보보호 및 개인정보보호 인증의 세부항목에 대한 연결 및 비교와 PCI-DSS와 전자금융거래법, 신용정보보호법, 개인정보보호법, 정보통신망법 등 국내 정보보호 관련 법령과 비교 및 적용에 관한 연구가 필요 할 것이다.

참 고 문 헌

[1] “정보통신망 이용 및 촉진에 관한 법률[법률 제13520호]” 2015.12.1.

[2] “Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures”, PCI-SSC, Version 3.1, 2015.4

[3] 최대수, ″효과적인 지불카드산업(PCI DSS) 컴플라이언스 구현 방안 연구“, 정보보호학회지 제18호, 2008.10.

[4] “Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 The new international standardfor information security management systems’, BSI, 2013.

[5] 박종선외, “보안에서 본 핀테크, 결제에서 본 핀테크”, 유진투자증권, 2015.4.7.

[6] NIA, “2015 개인정보보호 트랜드 전망”, 24쪽, 2015.

[7] VISA Korea “TC40 client fraud reporting and operating certificate ssubmission”, 2014.

[8] 여신금융협회, “결제대행업체 카드정보 저장 가능해진다”, 여신금융협회 보도자료, 2014.10.1.

[9] 김동국외, “PCI-DSS 적용방안에 대한 고찰”, 정보보호학회, 제18권4호, 2008.8

[10] 한국금융연구원, “우리나라 신용카드 거래구조의 문제점 및 개선 방안”, 2010.10.28.

[11] 길재욱 외, “우리나라 신용카드 현황과 발전방안”, 한국금융학회 동계 정책심포지움, 2012.11.21.

[12] 여신금융협회, “신용카드 업계현황”, 2014.9.

[13] 한국은행, “지급결제정보 제2006-6호”, 2~4쪽, 2006.8.24.

[14] 한국은행, “한국의 지급결제제도”, 2014.12.

[15] 한국은행, “2015년 지급결제총람”, 2015.2.

[16] 금융감독원, “VAN사 등록 현황”, 2015.12.18.

[17] 금융보안연구원, “주요 간편 결제 서비스의 보안성 비교 분석”, 금융보안연구원 보안연구부-2015-022, 1~8쪽, 2014.10.6.
[18] “사면초가 신용카드업계…수수료 강제인하·경쟁자 난입 한숨만”, 매일이코노미 제1836호, 2015.12.7.
[19] “인터넷전문은행 예비인가 결과”, 금융위원회/ 금융감독원 보도자료, 7쪽, 2015.11.29.
[21] “Visa Data Security Program Keeping Cardholder Datasafe VOL 02.06.13”, Visa, 2013.
[22] “PCI DSS v3.1 ROC Reporting Template”, PCI-SSC, 2015.4.
[23] “Payment Card Industry (PCI) Data Security Standard Approved Scanning Vendors Program Guide Version 2.0”, PCI-SSC, 2013.5.
[24] “정보보호 관리체계(ISMS) 인증 제도 안내서”, 미래창조과학부, KISA, 2013.6
[25] “개인정보보호 관리체계 인증 등에 관한 고시 전부개정안 행정예고“, 방송통신위원회 공고 제2015-58호, 2015.11.11.
[26] “개인정보 영향평가 수행안내서”, 행정자치부/NIA, 2015.3.
[27] “정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안(황주홍의원 대표발의)”, 의안번호 1917640, http://likms.assembly.go.kr/bill, 2015.11.6.

◐ 저 자 소 개 ◑

장 진 섭
2003년 전북대학교 법학과 학사
2008년 전북대학교 법학과 석사
2008년 ~ 2011년 해군 군수사령부 보안업무담당
2012년 ~ 현재 ㈜안랩 컨설팅본부 선임컨설턴트
2015년 ~ 현재 한국정보보호심사원협회 이사
관심분야 : Compliance, ISMS, Security Risk Management, Fin-tech, Cloud Computing Security