情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

안전한 지급결제 어플리케이션 개발을 위한 PCI PA-DSS 준수 방안 연구

허 성 무*

요 약

정보통신 기술 및 전자상거래의 발전으로 지급결제 서비스는 성장을 거듭하고 있으나, 그 중심에 있는 전자지급결제의 위험 역시 계속해서 발견되고 있다. 지급결제카드산업의 정보보호를 위해 설립된 PCI SSC에서는 지급결제 어플리케이션 개발에 대한 보안 표준인 PCI PA-DSS를 통해서 소프트웨어 벤더가 안전한 개발을 수행하도록 요구하고 있으나, 준수 대상인 기업 관점에서 참조 가능한 정보가 절대적으로 부족한 상황이다. 본 논문에서는 관련 보안 표준과의 연계 및 소프트웨어 개발 생명 주기를 통한 개발 절차 관리 방안을 통해, 소프트웨어 벤더가 PCI PA-DSS를 효과적으로 준수할 수 있는 방안을 제안한다.

Ⅰ. 서 론

1.1 연구 배경 및 목적

정보통신 기술의 발전으로 사회는 다양한 모습의 성장과 변화를 겪고 있으며, 전자상거래의 지속적인 발달 역시 그 모습 중 하나라 할 수 있다. 그 결과 은행의 고유 업무였던 지급결제 서비스에 소매유통업체, 제조업체 등 일반 기업들의 참여가 확산되고 있으며, 이들은 전자지급결제와 관련된 솔루션, 금융서비스 판매 채널을 제공하는 등 다양한 경제 행위를 보이고 있다.

지급결제는 경제주체들이 지급수단을 이용하여 실물 및 금융거래에 따라 발생하는 채권채무 관계를 화폐적 가치의 이전을 통해 청산하는 행위를 의미한다. 이러한 지급결제를 처리하기 위한 제반 계약과 그 운영시설을 지급결제시스템이라 총칭하며, 지급결제시스템은 이와 관련된 정보를 전달하는 메커니즘을 포함한다. 지급결제시스템은 금융의 하부구조로서 금융산업, 금융시장과 함께 금융시스템의 핵심적인 요소 가운데 하나로, 지급결제제도에 대한 충격은 금융제도 전체로 확산되어 경제 전반이 마비될 수 있다는 것에서 지급결제시스템의 안정성이 특히 강조되고 있다 [4,5].

지급결제시스템의 안정성은 다양한 리스크를 통해 위협될 수 있으나, 특히 지급결제 서비스를 성장하게 한 전자지급결제에서 끊임없는 위험이 발견되고 있다. 2009년 미국에서 발생한 신용카드처리업체 'Heartland Payment Systems'의 해킹 사고는 고객 정보의 유출로 인해 천문학적인 피해액이 발생한 대표적인 사례다 [2]. 전자지급결제와 관련된 보안 사고는 비단 해외에서만 발생하는 것이 아니라 IT 기술이 발달한 국내에서도 꾸준히 발생하고 있으며, 올해 초에는 카드 결제와 판매내역, 재고 등을 실시간 관리하는 POS(Point of Sales) 시스템의 해킹을 통해 고객 정보를 유출, 이를 악용하여 복제카드를 생성하는 방법으로 수백 건의 부정한 결제가 발생한 사고가 있었다 [14]. 또한, 보안 사고로 볼 수는 없으나 외국의 보안 컨퍼런스에서는 현금 자동 입출금기(ATM: Automated Teller Machine)의 해킹 시연을 통해 전자지급결제 시스템의 취약성을 확인한 사례가 있다 [15].

이와 같은 침해 사고 위험의 지속적인 증가로 인해 지급결제카드산업의 정보보호가 요구되고 있으며, 이를 위한 보안 표준을 마련하고 있는 곳이 바로 지급결제카드산업 보안 표준 위원회(PCI SSC: Payment Card

* (주)에이쓰리시큐리티 컨설팅사업본부 (hsm@a3security.com)

Industry Security Standard Council)이다. Visa, MasterCard 등 주요 카드 회사들이 모여 설립한 PCI SSC는 데이터 보안 표준(DSS: Data Security Standard)[1], 지급결제 어플리케이션 데이터 보안 표준(PA-DSS: Payment Application Data Security Standard), PIN[2] 처리 보안 표준(PTS: PIN Transaction Security)[3]과 같은 일련의 보안 표준의 개발, 관리 및 평가, 교육을 수행하고 있다. 해당 표준들은 지급결제카드산업 관련 보안 표준으로는 유일하여, 국가에서 제정한 규정이 아님에도 불구하고 일부 국가에서는 관련 조직의 해당 표준의 준수를 엄격히 규제하고 있다. 각 표준에 대해 많은 기업들이 각자의 조직 및 제품에 대해 표준 인증을 획득하고 있으며, 앞서 사례로 든 Heartland Payment Systems 역시 사고 이후 자사의 지급결제 어플리케이션에 대해 PA-DSS 인증을 획득하였다[11].

본 논문에서는 PCI SSC에서 마련한 표준 중 지급결제 어플리케이션에 대한 보안 표준인 PA-DSS에 대해서 알아보고, 이를 통해 안전한 지급결제 어플리케이션을 개발하도록 하는 방안에 대해 연구하였다. 본 논문을 통해 소프트웨어 벤더와 같은 지급결제 어플리케이션 관련 대상자들의 표준 준수 촉진을 통한 보안 수준 향상이 가능하며, 기타 관계자들의 PCI 보안 표준에 대한 전반적인 이해 향상 역시 기대할 수 있다.

1.2 연구 방법 및 구성

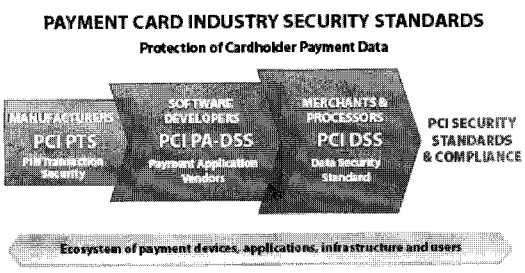
일반적으로 PCI 보안 표준들에 대한 연구는 그 수가 절대적으로 부족하며, 특히 PA-DSS 관련 연구는 전무한 편이다. 따라서 본 논문에서는 기존의 PCI DSS 관련 연구를 참조하여 PA-DSS와 비교, 분석하고자 한다. 또한, PCI SSC에서 제공되는 PA-DSS 관련 자료들의 경우 주로 PA-DSS 인증 평가를 수행하는 보안평가사를 위한 내용이 주로 기술되어 있어 PA-DSS를 준수해야 하는 관련 조직들에 대해서는 상대적으로 적은 정보를 제공하고 있다. 본 논문에서는 해당 내용을 분석하여, 지급결제 어플리케이션을 개발하는 소프트웨어 벤더가 PA-DSS를 준수할 수 있도록 하는 방안을 연구, 제시하고자 한다.

본 논문은 총 4장으로 구성되어 있다. 서론인 1장에서는 연구 배경, 목적, 방법 및 구성을 밝히고, 2장에서는 지급결제카드산업의 보안 표준을 관리하는 PCI SSC을 간략히 알아본 다음, 보안 표준인 PCI DSS, PCI PA-DSS의 개요를 확인하여 두 표준을 비교 분석한다. 3장은 PCI PA-DSS 준수 방안에 대해서 제시하고 있으며, PCI DSS 및 ISMS 표준과의 연계를 통한 표준 준수 촉진 방안과 지급결제 소프트웨어 개발 절차 관리 방안을 각각 포함하고 있다. 마지막으로 4장은 결론으로서 연구 결과의 요약과 연구의 한계점 및 향후 연구 방안을 밝히며, 끝으로 본 연구의 기대 효과를 서술하고 있다.

Ⅱ. PCI DSS 및 PCI PA-DSS 비교 분석

2.1 PCI SSC 및 PCI 보안 표준

지급카드결제산업 보안 표준 위원회(PCI SSC: Payment Card Industry Security Standard Council)는 2006년도, 카드회원 정보보호의 촉진을 위해 주요 카드 회사가 모여서 설립한 단체다. PCI SSC를 구성하는 다섯 개의 주요 카드 회사는 American Express, Discover Financial Services, JCB International, MasterCard WorldWide, Visa로, PCI DSS를 포함하는 일련의 지급결제카드산업 관련 보안 표준들을 수립하였으며, 그 중 PCI DSS를 각 회사들이 보유, 운영하고 있는 각각의 데이터 보안 표준 준수 프로그램에 기술적 요구사항으로 포함할 것을 동의하였다. 또한 표준 준수 대상 조직의 PCI DSS 및 PCI PA-DSS 준수 여부를 검토하는 보



〔그림 1〕 PCI 보안 표준 개요

1) 기존 연구 및 실제 산업에서는 'PCI'라는 용어를 주로 'PCI DSS'와 혼용하여 사용하고 있으나, 본 논문에서는 엄격히 구분하여 '지급결제카드산업(Payment Card Industry)'로 사용하였다.

2) Personal Identification Number, 카드의 개인 식별 번호

3) 초기에는 'PED(PIN Entry Device)' 보안 표준이었으나, 2009년 4월에 관련 보안 요구사항을 추가하면서 'PTS'라는 프레임워크를 새롭게 발표하고 해당 명칭으로 변경하였다.

안평가사인 QSA(Qualified Security Assessor) 및 PA-QSA를 교육, 자격을 부여하고 역할 역시 수행하고 있다. QSA 자격은 QSA 회사로 등록된 회사에 재직 중인 임직원이 SSC에서 주관하는 교육 과정 및 시험을 통과해야 취득할 수 있으며, 매년 갱신이 요구된다. 이 외에도 SSC에서는 각각의 QSA가 작성한 보고서의 검토를 통해 QSA 회사 및 개별 QSA의 자격을 검토하는 QA(Quality Assurance) 프로그램을 운영하는 등 다양한 활동을 수행하고 있다. PCI SSC에서 수립, 운영 및 관리하고 있는 보안 표준들에 대한 개요를 도식화 하면 [그림 1]과 같다 [11].

2.2 PCI DSS 및 PCI PA-DSS 비교

2.2.1 PCI DSS

PCI SSC를 통해 수립, 관리되는 대표적인 표준인 지급결제 데이터 보안 표준(DSS: Data Security Standard)은 카드회원 정보를 취급하는 모든 가맹점과 서비스 사업자들의 정보보호 정책과 정보처리 업무 환경 및 정보보호 환경의 보안 수준을 평가한다. 모든 가맹점과 서비스 사업자는 PCI DSS 준수 의무를 가지며, 회원사는 카드회원 데이터를 저장, 처리 혹은 전송하는 소속 가맹점 및 서비스 사업자들로 하여금 프로그램을 준수하게 할 책임이 있다. 즉, 카드 정보를 입력받고 재화 및 서비스를 판매하는 모든 매입사가 표준 준수 대상이 되며, 연간 카드 거래 규모에 따라 평가 기준이 [표 1]과 같이 달라진다 [1,6,7].

PCI DSS 평가는 VISA와 같은 글로벌 카드브랜드의 회원사로 등록되어 있는 매입사들이 자신들의 서비스를 이용하는 가맹점 및 서비스 제공자들에게 보안 평가를 이행하도록 요구하며, 이러한 요구를 접수한 보안 평가 대상 기업들은 PCI QSA를 보유한 독립된 평가기관, 즉 QSA 회사에 보안 평가를 신청하고 적합여부를 평가받게 된다. 보안 평가는 문서 검토, 인터뷰, 현장 실사 등으로 이루어지며, 보안평가사는 [표 2]와 같은 PCI DSS 요구사항에 대해 보안 평가를 실시한다 [1,6,7].

PCI DSS 평가에 대한 결과는 '표준 준수 보고서(RoC: Report on Compliance)'로 작성되어 대상 기업에게 전달된다. 그리고 평가 결과에 대한 대상 기업의 확인을 통해, 미 이행으로 나타난 통제항목에 대해서 향후 보완계획인 '개선 계획 보고서(Remediation Plan)'를 작성하도록 한다. 대상 기업은 개선 계획 보고서를 통해 미 이행 항목에 대해 개선하고 필요한 조치가 이루어지도록 계획하여, 결과적으로 PCI DSS의 모든 보안 요구사항을 만족할 수 있도록 한다.

보안평가사는 평가 대상 기업이 제출한 개선 계획 보고서를 검토 후, PCI DSS 평가에 대한 요약본인 'Summary of Findings'를 작성하여 대상 기업에 전달한다. 이후 대상 기업은 회원사(매입사)의 PCI DSS 평가 결과 요청 시 보안평가사로부터 전달받은 3개의 결과 보고서(Report on Compliance, Remediation Plan, Summary of Findings)를 전달하게 된다. 또한, 대상 기업에게는 PCI DSS 보안 평가를 실시한 보안평가사에 대한 평가 설문지인 'QSA Feedback Form'을 PCI SSC 담당자의 메일 주소로 발송하는 절차가 필요하다. 이와 같은 일련의 절차를 통한 PCI DSS 인증은 1년간 유효하며, 따라서 매년마다 갱신이 요구되고 있다 [1,12].

〔표 1〕 PCI DSS 평가 대상 기준

가맹점 레벨	선택 기준	검증실행 사항	검증실행자
1	• 연간 6,000,000건 이상의 거래 처리 • 고객 데이터 침해사고로 이어진 해킹, 공격을 받은 모든 가맹점 • 카드 협회에 의해 레벨 1로 분류된 모든 가맹점	• 매년 현장 보안감사 • 분기별 네트워크 스캔	• 독립된 보안 평가기관 (QSA) • 내부감사 (회사 임원 승인 시) • 공인된 독립스캔벤더 (ASV)
2	• 연간 1,000,000건 ~ 6,000,000건의 거래 처리	• 매년 PCI 자체 평가서 • 분기별 네트워크 스캔	• 가맹점 • 공인된 독립스캔벤더 (ASV)
3	• 연간 20,000건 ~ 1,000,000건의 거래 처리	• 매년 PCI 자체 평가서 • 분기별 네트워크 스캔	• 가맹점 • 공인된 독립스캔벤더 (ASV)
4	• 그 외 모든 가맹점 (승인 채널 불문)	• 매년 PCI 자체 평가서 작성 권장 • 매년 네트워크 스캔 권장	• 가맹점 • 공인된 독립스캔벤더 (ASV) • 규정준수(필수), 검증(선택)

〔표 2〕 PCI DSS 요구사항

통제 목표 / 요구사항			통제 항목 수[4]
안전한 네트워크 구축 및 유지	1	카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다	21
	2	시스템 패스워드 및 기타 보안 파라미터에 벤더가 제공한 디폴트 값을 사용하지 않는다	9
카드회원 데이터 보호	3	저장된 카드회원 데이터를 보호한다	20
	4	공중망을 통한 카드회원 데이터를 암호화하여 전송한다	3
취약점 관리 프로그램 유지관리	5	안티바이러스 소프트웨어를 사용하고 정기적으로 갱신한다	3
	6	안전한 시스템과 어플리케이션을 개발하고 유지한다	32
강력한 접근 통제 방안 수립	7	업무상 알 필요가 있는지에 따라 카드회원 데이터에 대한 접근을 제한한다	9
	8	컴퓨터에 접근하는 사용자별로 고유 ID를 부여한다	21
	9	카드회원 데이터에 대한 물리적 접근을 제한한다	21
네트워크 정기적 모니터링 및 테스트	10	네트워크 자원과 카드회원 데이터에 대한 모든 접근을 추적하고 감시한다	25
	11	보안시스템 및 프로세스를 정기적으로 시험한다	7
정보보호 정책 유지관리	12	직원과 계약자들의 정보보호를 위한 정책을 유지한다	39
공유 호스팅 제공업자를 위한 추가 요구사항[5]	A	공유 호스팅 제공업자는 카드회원 데이터 환경을 보호한다	5
합계			215

〔표 3〕 지급결제 어플리케이션 유형

유형	기능	설명
01	POS 묶음 (POS Suite)	대면 방식(face-to-face), 메일 주문/전화 주문(MOTO, 콜 센터 포함), 대화형 음성 응답(IVR), 웹(수동으로 입력되는 전자거래, MOTO 등의 거래) 및 EFT[6]/확인 인증을 포함하는 다양한 지급결제 채널을 위해서 가맹점에 의해 사용될 수 있는 Point of sale 소프트웨어
02	지급결제 미들웨어 (Payment Middleware)	가맹점 POS로부터 기타 가맹점 시스템 또는 처리업체로의 지급결제 승인 및 정산의 전송이나 처리를 용이하게 하는 지급결제 소프트웨어
03	지급결제 게이트웨이/스위치 (Payment Gateway/Switch)	가맹점 시스템 및 처리업체 간 지급결제 승인 및 정산의 전송이나 처리를 용이하게 하도록 제3자에게 판매 또는 배포된 지급결제 소프트웨어
04	지급결제 백 오피스 (Payment Back Office)	"백 오피스" 장소, 예를 들어 사기(fraud) 보고, 마케팅, 호텔 건물 관리, 또는 수익 관리 및 보고를 위해 지급결제 데이터가 사용되는 것을 가능하게 하는 소프트웨어. 해당 어플리케이션이 승인 및 정산의 일부가 아닐 수 있음에도 불구하고, 종종 소프트웨어 묶음으로서 지급결제 어플리케이션이 추가로 제공되며, 그렇게 되도록 요구되지는 않으나, PA-DSS 평가의 일부로 인증될 수 있음
05	POS 관리자 (POS Admin)	POS 어플리케이션을 운영하거나 관리하는 소프트웨어
06	특수 POS (POS Specialized)	블루투스(Bluetooth), 모바일, 휴대폰, VOIP 등과 같이 특화된 전송 방법을 위해서 가맹점에 의해 사용될 수 있는 Point of sale 소프트웨어
07	POS 키오스크 (POS Kiosk)	소유자가 지켜보고 있거나 그렇지 않은 키오스크, 예를 들어 주차장 같은 곳에서 발생할 수 있는 지급결제 카드 거래를 위한 Point of sale 소프트웨어
08	대면 방식 POS (POS Face-to-Face)	대면 방식(face-to-face) 지급결제 카드 거래를 위해서 가맹점에 의해 단독으로 사용되는 Point of sale 소프트웨어. 해당 어플리케이션은 미들웨어, 프론트 오피스 혹은 백오피스 소프트웨어, 매장 관리 소프트웨어 등을 포함할 수 있음
09	쇼핑 카트 & 온라인 상점 (Shopping Cart & Store Front)	소비자가 온라인 상점(Store Front)로부터 구매를 선택하고, 쇼핑 카트(Shopping Cart) 내 카드회원 데이터를 입력한 다음, 쇼핑 카트가 승인 및 정산을 위해 해당 카드회원 데이터를 전달하는, 전자거래 가맹점을 위한 지급결제 소프트웨어. POS 묶음(POS Suite)에서 언급된, 승인 및 정산을 위해 가맹점이 "가상의" POS에 데이터를 수동으로 입력하는 "Web"과는 차이가 있음

〔표 4〕 PCI PA-DSS 요구사항

통제 목표 / 요구사항		통제 항목 수[7]
1	전체 마그네틱 선, 카드 인증 코드나 값(CAV2, CID, CVC2, CVV2), 또는 PIN 블록 데이터를 보관하지 않는다	6
2	저장된 카드회원 데이터를 보호한다	7
3	안전한 인증 방법을 제공한다	3
4	지급결제 어플리케이션 활동의 로그를 기록한다	2
5	안전한 지급결제 어플리케이션을 개발한다	30
6	무선 전송을 보호한다	2
7	취약점을 다루기 위해 지급결제 어플리케이션을 테스트한다	2
8	안전한 네트워크 구현을 용이하게 한다	1
9	카드회원 데이터는 절대로 인터넷에 연결된 서버에 저장되지 않아야한다	1
10	안전한 원격 소프트웨어 업데이트를 용이하게 한다	1
11	지급결제 어플리케이션으로의 안전한 원격 접근을 용이하게 한다	3
12	공중망 상에서의 민감한 트래픽을 암호화한다	2
13	모든 비-콘솔 관리자 접근을 암호화한다	1
14	고객, 재판매자 및 통합업체를 위한 교육용 문서 및 교육 프로그램을 유지한다	5
합계		66

2.2.2 PCI PA-DSS

지급결제 어플리케이션 데이터 보안 표준(PA-DSS: Payment Application Data Security Standard)은 판매, 배포되거나 제3자에게 허가된 곳에서 인증 또는 정산의 일부로 카드회원 데이터가 저장, 처리, 전송되는, 지급결제 어플리케이션을 개발하는 소프트웨어 벤더 및 기타 관계자들에게 적용된다. 수행되는 지급결제 기능에 따라 지급결제 어플리케이션의 유형은 [표 3]과 같이 분류할 수 있다[8,9].

소프트웨어 벤더는 PA-QSA를 보유한 PA-QSA 회사를 통해 지급결제 어플리케이션의 PA-DSS 준수 여부를 평가받을 수 있다. PA-QSA 회사는 소프트웨어 벤더와 기밀 유지 협약서(NDA: Non Disclosure Agreement)를 작성한 다음 소프트웨어 벤더로부터 전달받은 해당 지급결제 어플리케이션과 PA-DSS 이행 가이드(Implementation Guide), 소프트웨어 설치 지침 등을 통해 PA-DSS의 모든 보안 요구사항을 만족하는지 평가하여 '검증 보고서(ROV: Report on Validation)'를 작성한다. PA-QSA가 평가를 실시하는 PA-DSS의 보안 요구사항은 아래 [표 4]와 같다.

모든 보안 요구사항이 만족될 경우 PA-QSA 회사의 PA-QSA는 기밀 유지 협약서 및 공개 동의서(Release Agreement)의 서명을 확인하고, PCI SSC로 검증 보고서를 전달한다. 보고서를 전달받은 SSC는 QA-DSS 인증 어플리케이션 목록에 해당 지급결제 어플리케이션을 등록하기 위한 비용(Listing Fee)을 소프트웨어 벤더에 청구하며, 비용 지불이 완료되면 PCI SSC 홈페이지에 매월 갱신되는 PA-DSS 준수 지급결제 어플리케이션 목록에 해당 어플리케이션 목록을 추가한다.

각각의 지급결제 어플리케이션은 매년 갱신 평가를 받아야 함은 물론이며 기존에 인증된 어플리케이션에 변경이 일어났을 경우에도 새로 평가를 받아야 한다. 한편 Visa에서 운영해 온 PABP(Payment Application Best Practices) 프로그램을 준수하고 있는 지급결제 어플리케이션의 경우, PABP 준수 현황에 따라[8] PA-QSA의 평가 절차 없이 승계 및 전환(Grandfathering and Transitioning) 절차를 통해 PA-DSS 인증을 획득 할 수도 있다[8,9].

---

4) 통제항목의 특성에 따라 실제로 평가가 일어나지 않을 수 있는 항목까지 모두 고려한 숫자임

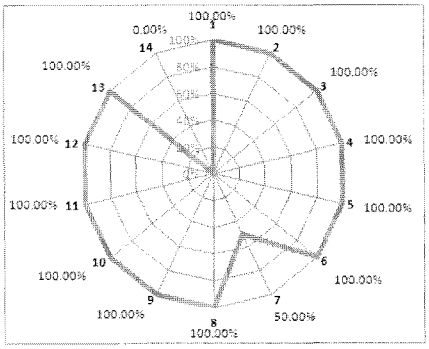
5) 준수 대상 업체가 공유 호스팅 제공업자(Shared Hosting Provider)일 경우, 기본적으로 제공되는 보안 요구사항 외에도 추가적인 요구사항을 준수해야 함

6) Electronic Funds Transfer (System), 전자식 자금 이동 (시스템)

7) 통제항목의 특성에 따라 실제로 평가가 일어나지 않을 수 있는 항목까지 모두 고려한 숫자임

8) PABP 버전 1.3 이전에 검토된 어플리케이션의 경우 12개월간, 버전 1.3의 경우 18개월간, 버전 1.4의 경우 24개월간 PA-DSS 인증을 유지할 수 있으며, PABP 검토 현황 등에 따라 PA-QSA가 참여할 수도 있다.

	PCI PA-DSS 요구사항 - 상위 수준	PCI PA-DSS 요구사항	PCI DSS 참조 가능 항목	비율
1.	전체 마그네틱 선, 카드 인증 코드나 값(CAV2, CID, CVC2, CVV2) 또는 PIN 블록 데이터를 보관하지 않는다	6	6	100.00%
2.	저장된 카드회원 데이터를 보호한다	7	7	100.00%
3.	안전한 인증 방법을 제공한다	8	8	100.00%
4.	지급결제 어플리케이션 활동의 로그를 기록한다	2	2	100.00%
5.	안전한 지급결제 어플리케이션을 개발한다	30	30	100.00%
6.	무선 전송을 보호한다	2	2	100.00%
7.	취약점을 악용하기 위해 지급결제 어플리케이션을 테스트한다	2	1	50.00%
8.	안전한 네트워크 구현을 용이하게 한다	1	1	100.00%
9.	카드회원 데이터는 절대로 인터넷에 연결된 서버에 저장되지 않아야한다	1	1	100.00%
10.	안전한 원격 소프트웨어 업데이트를 용이하게 한다	2	2	100.00%
11.	지급결제 어플리케이션으로의 안전한 원격 접근을 용이하게 한다	3	3	100.00%
12.	공급망 상에서의 민감한 트랜잭션을 암호화한다	2	2	100.00%
13.	모든 비-콘솔 관리자 접근을 암호화한다	1	1	100.00%
14.	고객, 제판매자 및 통합업체를 위한 교육을 돕서 및 그들 프로그램을 유지한다	5	0	0.00%
	합계	66	60	90.91%



〔그림 2〕 PCI PA-DSS 요구사항의 PCI DSS 연계 가능 수준

2.2.3 PCI DSS 및 PCI PA-DSS 비교

PCI PA-DSS는 PCI DSS에서 파생된 보안 표준으로, PCI PTS와는 달리[9] 많은 부분에서 유사한 형식과 내용을 갖는다. PA-DSS에는 DSS의 많은 요구사항이 반영되어 있으나 두 표준 간에는 분명한 차이점들이 존재하며, 그 중 대표적인 차이점을 살펴보면 다음과 같다.

첫째, PA-DSS와 DSS는 적용 대상에서 큰 차이가 있다. DSS는 카드회원 정보를 취급하는 모든 가맹점과 서비스 사업자를 대상으로 적용되는 반면에, PA-DSS는 지급결제 어플리케이션을 개발하는 소프트웨어 벤더 및 기타 관계자들에게 적용된다. 소프트웨어 벤더가 준수하는 보안 표준인 PA-DSS는 지급결제 어플리케이션을 사용하는 가맹점 및 서비스 사업자의 DSS 준수를 용이하도록 하나, PA-DSS를 준수하는 지급결제 어플리케이션을 사용하는 것만으로는 DSS의 준수를 보장할 수 없다. 즉, 하나의 표준이 다른 표준에 종속되는 것이 아니라, 지급결제 서비스의 정보보호라는 동일한 목표를 가진, 별개의 표준인 것이다.

둘째, 보안 표준 준수를 인증 받는 방법에 있어 PA-DSS는 DSS보다 유연하다는 장점이 있다. 각각의 QSA로부터 평가를 받은 후, 모든 보안 요구사항을 충족할 경우 1년간 유효한 인증을 획득할 수 있다는 점에서는 두 표준 모두 동일한 절차를 갖는다. 하지만 PA-DSS의 경우 QSA로부터의 인증 획득 절차 외에도 승계 및 전환(Grandfathering and Transitioning) 절차를 통한 인증 획득이 가능하다는 점에서, DSS보다 다양한 인증 획득 절차를 제공한다고 볼 수 있다.

셋째, PA-DSS를 평가하는 PA-QSA 회사는, QSA 보유는 물론 SSC에서 요구하는 환경에 부합하는 검사 연구실(Testing Laboratory) 역시 보유해야 한다. PA-QSA 회사는 소프트웨어 벤더로부터 지급결제 어플리케이션과 관련 문서들을 제공받아 표준 준수 여부에 대한 평가를 진행하는데, 보안 요구사항 및 평가 절차에 대한 검증 보고서(ROV) 뿐만 아니라 평가에 사용된 검사 연구실의 상세 환경에 대한 보고서도 함께 작성하여 PCI SSC로 전달해야 한다.

Ⅲ. PCI PA-DSS 준수 방안

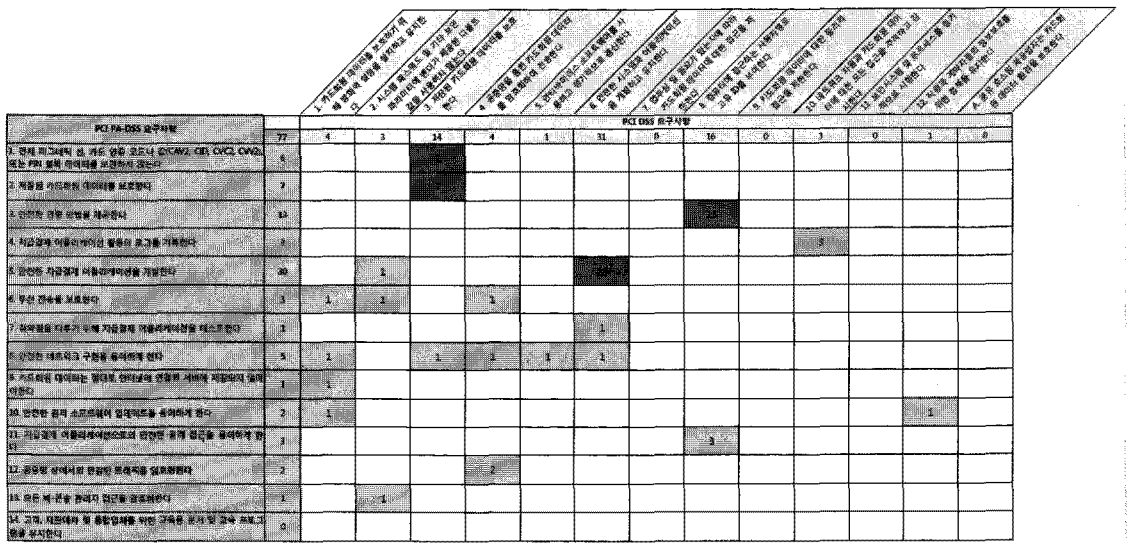
3.1 PCI DSS 및 ISMS 표준과의 연계를 통한 표준 준수 촉진 방안

3.1.1 PCI DSS와의 연계

PA-DSS의 준수를 위해 참조할 수 있는 정보는 그 수가 절대적으로 부족한 반면, DSS의 경우 PCI SSC에서 제공하는 자료[10] 등 사용 가능한 정보 및 연구 사례가 PA-DSS에 비해 상대적으로 다양한 편이다. 즉, DSS의 준수 방안과 관련된 정보를 참조하여 PA-DSS에 대한 보안 요구사항을 이해하고, 이를 준수할 수 있는 다양한 방안에 대해 고려해볼 수 있다. 단, 이와 같은 접근 방법은 PA-DSS의 보안 요구사항이 DSS와 많은 부분에서 유사하다는 것을 전제로 하기 때문에, 각각

9) PCI PTS는 PCI DSS의 '암호화된 PIN 블록의 저장 금지'와 관련된 표준이나, 내용 상 유사점은 거의 없다.

10) 대표적인 것으로는 자체 평가 설문지(Self-Assessment Questionnaire)가 있으며, 최근에는 소규모 회사의 PCI DSS 준수를 위해서 BBB(Better Business Bureau)를 통해 'Data Security - Made Simpler'라는 보안 가이드를 내놓기도 했다.



[그림 3] PCI DSS / PCI PA-DSS 보안 요구사항 비교 (Heat Map)

의 보안 표준이 실제로 얼마나 유사한지 사전에 파악할 필요가 있다.

PA-DSS와 DSS의 유사한 정도를 확인하기 위해, 보안 요구사항 별로 비교하여 정리한 결과는 [그림 2] 및 [그림 3]과 같다.

검토 결과를 통해 일부 항목을 제외한 PA-DSS 보안 요구사항의 대부분의 DSS와 직접적으로 연계 가능하다는 것을 확인할 수 있다. 연계가 어려운 일부 항목은 패치 및 업그레이드의 전달 및 배포, 교육용 문서 및 교육 프로그램의 유지에 해당되는 항목들로, 이는 소프트웨어 벤더에 적용되는 PA-DSS 특유의 보안 요구사항이며 대상 등 상세 내용의 차이로 인해 직접적으로는 연계시키기가 어려워 추가로 고려될 필요가 있다.

3.1.2 ISO 27001 및 K-ISMS[11]와의 연계

조직에서 정보보호 관리체계를 수립, 관리하여 준수하고 있는 ISMS 표준과 PCI DSS의 연계를 통해 상호적으로 활용하려는 방안이 다양하게 연구되어 업계에 나타나고 있다. 특히 다수의 기업에서 어려운 경제 상황에도 불구하고 보안 목표를 달성하기 위한 전략으로 GRC[12] 프로그램을 강화하는 추세를 보이고 있어, 컴플라이언스 준수를 위한 중복적인 노력을 감소할 수 있는 연계 방안의 중요성은 점점 증가하고 있다고 볼 수 있다. 또한 외국의 경우에는 PCI DSS 인증을 획득한 기업의 ISMS 인증 심사 시 중복 영역의 검사를 면제해 주거나, 두 표준의 인증 심사를 동시에 진행하여 감사 공정을 삭감하는 등의 혜택을 제공하고 있다 [6,10,13,16].

국내에 적용되고 있는 ISMS 인증 표준으로는 국제 표준기구인 ISO(International Organization for Standardization)의 ISO 27001과 한국인터넷진흥원의 K-ISMS가 있다. PCI PA-DSS를 기준으로 하여 관련된 PCI DSS, ISO 27001, K-ISMS의 보안 요구사항 및 통제 사항, 점검 항목 등을 나열, 참조할 수 있도록 한 점검표의 구현 예는 [그림 4]와 같다.

3.2 PCI PA-DSS 준수를 위한 지급결제 소프트웨어 개발 절차 관리 방안

안전한 지급결제 소프트웨어를 개발하기 위해서 PCI PA-DSS 보안 요구사항을 준수하도록 하는 개발 절차의 수립 및 운영이 필요하다. 하지만 PA-DSS를 포함하

11) 'ISMS(Information Security Management System, 정보보호 관리체계)는 일반적으로 정보자산의 기밀성 · 무결성 · 가용성을 실현하기 위한 과정을 체계적으로 수립 · 문서화 하고 지속적으로 관리 · 운영하는 것을 지칭하는데 쓰여, ISO 27001을 포함하는 의미로 해석될 수 있다. 따라서 본 논문에서는 한국인터넷진흥원의 정보보호관리체계 인증제도를 지칭하는 단어로 'K-ISMS'라는 표현을 사용하였다.

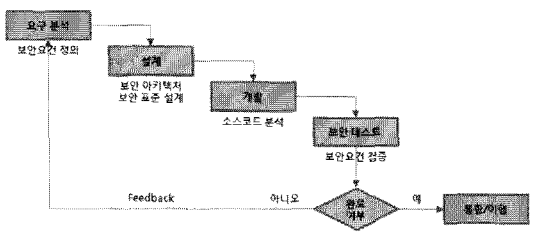
12) Governance, Risk, Compliance. 기업/조직의 위험 및 규제에 대응하는 전사적이고 통합적인 체계

PCI PA-DSS 요구사항	PCI PA-DSS 평가절차	적용	미적용	특이사항 / 비고	PCI DSS / ISMS 참조
3.2 지급결제 어플리케이션이 있는 PC, 서버 및 데이터베이스로의 접근은 반드시 고유의 사용자 ID 및 안전한 인증을 요구해야 한다.	3.2 벤더에 의해 작성된 *PA-DSS 이행 가이드*를 점검하여 고객 및 재판매자/통합업체가 지급결제 어플리케이션 및 카드회원 데이터가 있는 모든 PC, 서버 및 데이터베이스로의 접근에 고유의 사용자 ID 및 PCI DSS를 준수하는 안전한 인증을 통해서 통제되도록 강력하게 권고되고 있는지 검증한다.	O		- 준비한 표본을 점사한 결과 시스템별로 고유의 ID를 할당하고 있음을 확인함 - (사용자 관리 지침) 2장 1조에 사용자 계정은 사용자 별로 하나의 계정을 사용해야 하며, 계정의 등록 변경 관계 요청은 공식적인 문서 및 승인 절차로 이루어지도록 명시함 - 인터뷰를 통해서 서버/데이터베이스 담당자가 시스템별로 고유의 ID를 할당하고 있음을 확인함 - (시스템별 계정 목록) 확인 결과 모든 사용자는 고유의 사용자 이름을 사용하고 있음을 확인함	**PCI DSS 요구사항** 8.1 모든 사용자에게 시스템 구성요소 또는 카드회원 데이터로의 접근을 허용하기 전에 고유의 ID를 할당해야 한다. 8.2 고유의 ID를 할당하는 것에 추가로, 모든 사용자를 인증하기 위해 다음 중 최소한 하나 이상의 방법을 사용해야 한다: ■ 패스워드 또는 패스프레이즈 ■ 이중 요소 인증 (예를 들어 토큰 장비, 스마트 카드, 생체 인증, 또는 공개 키) **ISO 27001 통제사항 및 설명** A.11.5.2 사용자 식별 및 인증 모든 사용자들은 그들 개인적으로만 사용하는 고유의 식별자 (사용자 ID)를 가져야 하며, 사용자의 식별 요구를 입증하기 위해 적절한 인증 기법이 선택되어야 한다. **K-ISMS 통제사항 및 점검항목** 10.2.1 사용자 등록 사용자는 유일한 식별자를 가지고 그룹명은 적절한 명명규칙을 따르고 있는가?

〔그림 4〕 PCI PA-DSS 및 관련 보안 표준들을 연계한 점검표(예)

는 PCI 보안 표준은 주로 평가자의 입장에서 해당 표준의 보안 요구사항을 서술하고 있으며, 이를 준수하기 위한 지침은 상대적으로 부족한 편이다. 따라서 해당 보안 표준의 준수를 위한 방안이 추가로 고려될 필요가 있다.

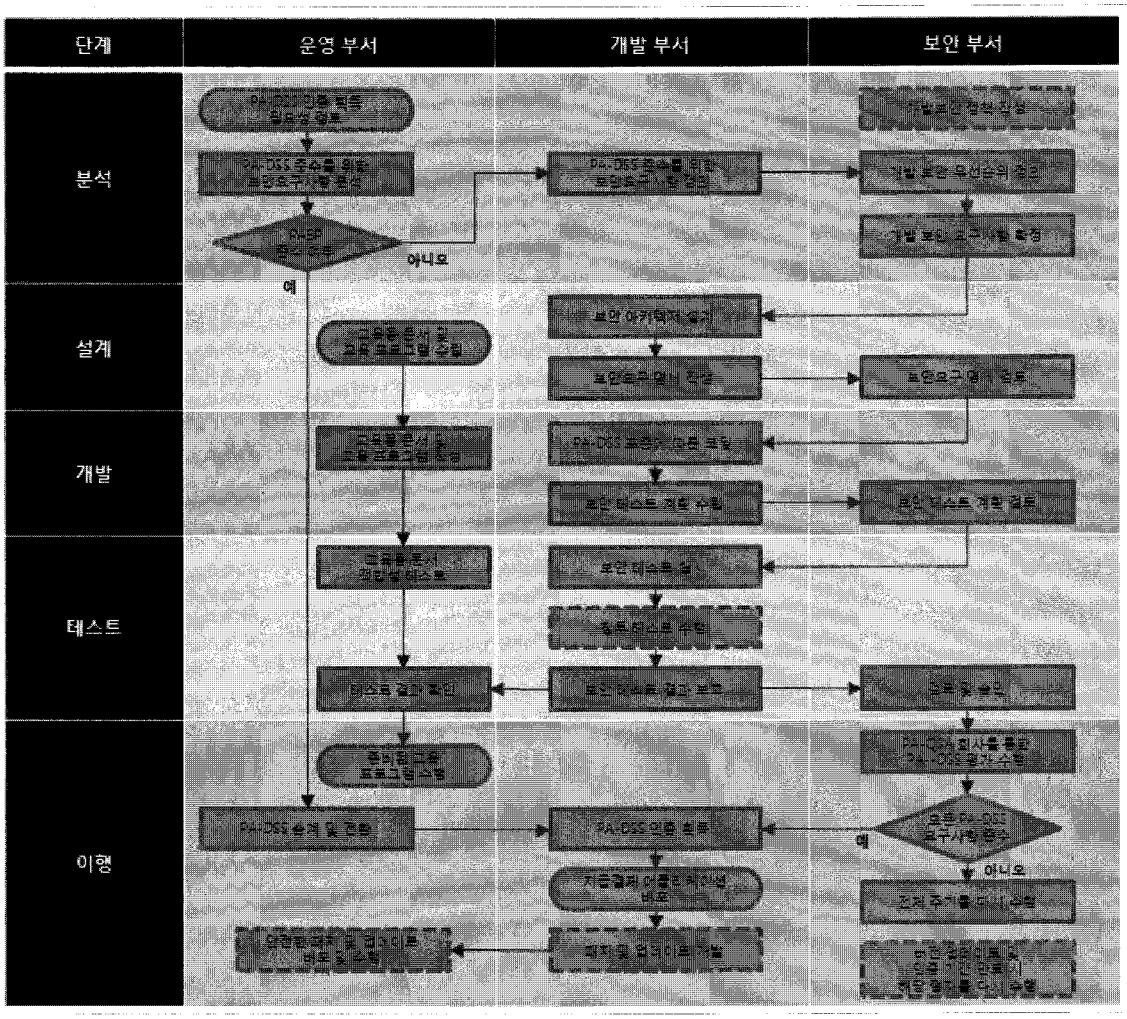
지급결제 소프트웨어를 개발하는 소프트웨어 벤더를 위해서는 SDLC에 따른 보안 절차를 제시할 수 있다. SDLC(Software Development Life Cycle, 소프트웨어 개발 생명 주기)란 소프트웨어 개발 과정에서 변화해가는 소프트웨어의 형상을 가시화하기 위하여 구분해 놓은 작업 공정을 의미한다. 이에 덧붙여 SDLC 보안이란, 소프트웨어 개발 과정에서 정보보호와 관련한 요구사항을 분석, 정의하고 설계 단계에 시스템 구조와 프로그램과 관련한 보안 설계를 적용하여 보안설계서에 따라 개발하여 새로 구축되는 시스템에 보안 요구사항을 적용하기 위한 절차로 정의할 수 있다. 일반적인 SDLC에 보안 테스트 등 정보보호를 위한 요소를 추가로 결합한 SDLC 보안 프로세스를 도식화 하면 [그림 5]와 같다 [3].



〔그림 5〕 SDLC 보안 프로세스

PA-DSS를 준수하기 위해서는 일반적인 보안 프로세스로 구성된 SDLC 외에도 구체적인 절차를 추가하는 것이 효과적이다. PA-DSS를 포함하는 PCI 보안 표준은 인증을 위해 보안 요구사항의 100% 준수를 요구한다는 특징이 있으며, 특히 PA-DSS의 경우에는 Visa의 PABP 프로그램 준수로도 인증을 획득할 수 있는 등 PA-DSS 특유의 고려사항이 존재하기 때문이다. 상세한 절차를 정의하기 위해 SDLC의 분석, 설계, 개발, 테스트, 이행 단계별 보안활동을 참여 조직별 역할로 정의할 필요가 있다. 조직의 구성 및 환경에 따라 다소 차이가 발생할 수 있지만, 일반적인 소프트웨어 벤더를 가정하고 회사 내의 운영 부서, 개발 부서, 보안 부서가 PA-DSS 준수 프로그램 개발 및 인증 획득 프로젝트에 참여하는 것으로 하여 각각의 역할 및 절차를 간략히 표현해보면 [그림 6]과 같다.

분석 단계에서 운영 부서는 지급결제 소프트웨어의 판매를 위한 PA-DSS 인증 획득 필요성 여부를 검토하고, PA-DSS 준수를 위한 보안 요구사항을 검토한다. 해당 단계에서 Visa의 PABP 프로그램 준수 여부를 우선적으로 확인하여, 준수하고 있을 경우에는 PA-DSS 승계 및 전환 절차를 통해 PA-DSS 인증을 바로 획득할 수 있다. 해당 사항이 없을 경우에는 PCI DSS 및 ISMS 표준을 참조, PCI PA-DSS 점검표를 작성하고, 보안 요구사항을 도출한 다음 개발 부서에 제시한다. 개발 부서에서는 분석된 결과를 통해 보안 요구사항을 정



〔그림 6〕 SDLC 단계에 따른 부서별 수행 역할 및 절차 흐름도

의하며, 보안 부서는 보안성 검토를 통해 이를 검증한다. 검증 시 사전에 정의된 개발 보안 정책을 참조하며, 필요에 따라서는 개발 보안 정책을 수정할 수 있다.

설계 단계에서는 개발 부서의 보안 아키텍처 설계 및 보안 요구 명세 작성 절차가 이어지게 되며, 보안 부서에서는 관련 법규 및 규정에 부합하는지 다시 한 번 검토하게 된다. 해당 단계에서 운영 부서는 이와 별개로 교육용 문서 및 교육 프로그램을 수립하며, 이는 고객, 재판매자 및 통합업체를 위한 교육용 문서 및 교육 프로그램의 유지에 대해 규정하고 있는 PA-DSS 요구사항을 기준으로 한다.

개발 단계에서 운영 부서는 PA-DSS 요구사항 및 소프트웨어 벤더의 지급결제 어플리케이션에 따라 PA-DSS 이행 가이드와 같은 교육용 문서 및 교육 프로그램을 작성한다. 개발 부서에서는 PA-DSS 요구사항에 따라 지급결제 어플리케이션을 개발하고, 보안 테스트 계획을 수립하여 보안 부서의 검토를 받도록 한다.

테스트 단계에서는 보안 테스트 계획에 따라 실제 테스트를 수행하며, 분석 단계에서 작성된 점검표의 활용이 가능함은 물론, 필요에 따라서는 외부 전문가 등을 통해 침투 테스트를 수행할 수도 있다. 운영 부서에서는 앞서 작성한 교육용 문서가 PA-DSS 요구사항을 만족하는지 검토하는 적합성 테스트를 수행하게 되며, 개발 부서의 테스트 결과와 종합하여 테스트 결과를 확인한다. 보안 부서에서는 개발 부서에서 보고한 테스트 결과를 검토하고, 결함이 발견 될 경우에는 해당 취약점을

조치하도록 하여 조치 완료 여부까지를 검토한 다음 이를 승인해야 한다.

마지막으로 이행 단계에서 운영 부서는 준비된 교육용 문서 및 교육 프로그램을 통해 실제 교육을 수행하도록 하며, 보안 부서에서는 PA-QSA 회사를 통해서 개발된 지급결제 어플리케이션에 대한 PA-DSS 평가를 수행하도록 한다. 모든 PA-DSS 요구사항을 준수할 경우 인증 획득이 가능하며, 추가적인 절차를 통해 PCI SSC의 QA-DSS 인증 어플리케이션 목록에 해당 지급결제 어플리케이션을 등록할 수 있다. 만약 모든 PA-DSS 요구사항을 만족하지 못할 경우, 전체 주기를 다시 수행하여 PA-DSS를 준수하는 지급결제 어플리케이션을 개발할 수 있도록 한다. 인증 획득 후에는 해당 지급결제 어플리케이션을 판매 및 배포하며, 패치 및 업데이트가 추가적으로 개발 될 경우 이를 안전하게 수행할 필요가 있다. 지급결제 어플리케이션이 업데이트 되거나 획득한 인증이 만료될 경우 각각 해당되는 절차를 다시 수행할 필요가 있으며, PA-QSA의 평가를 통해 획득한 인증과 PABP 준수 프로그램의 승계 및 전환 절차를 통한 인증의 경우 유효한 기간이 다르기 때문에 이를 사전에 인지하고 적절히 갱신해야 한다.

Ⅵ. 결 론

안전한 지급결제 서비스를 위해 설립된 PCI SSC에서는 지급결제 어플리케이션을 개발하는 소프트웨어 벤더를 위해 PCI PA-DSS를 수립하여 이를 준수할 수 있도록 관리하고 있다. PCI SSC의 보안 표준 중 하나인 PCI DSS로부터 파생된 PCI PA-DSS는 QSA 회사를 통해 준수 여부를 평가받아 모든 요구사항을 만족할 경우 인증을 획득할 수 있으며, Visa의 PABP 프로그램을 준수하고 있을 경우에도 이를 통해 인증 획득이 가능하다는 특징이 있다.

하지만 PA-DSS를 포함하는 PCI 보안 표준은 주로 보안 요구사항에 대한 평가자 관점의 내용을 서술하고 있으며, 해당 표준을 준수하기 위한 기업 중심의 지침이 상대적으로 부족한 편이다. 그 중에도 특히 PA-DSS의 경우 해당 표준의 준수를 위해 참조할 수 있는 정보는 DSS에 비해 절대적으로 부족하여, 해당 연구에 어려움이 있는 것이 사실이다. 따라서 본 연구에서는 DSS를 포함하여 PCI SSC에서 제공되는 문서를 주로 참조하였으나, 향후 관련 분야에 대한 연구가 지속적으로 발표된다면 보다 향상된 연구 결과를 획득할 수 있을 것이라 예상한다. 또한 본문에서 다룬 기타 표준과의 연계 및 SDLC 개발 절차 관리 방안의 경우, 관련 연구 및 업계 동향 등을 적극적으로 반영한다면 보다 실무적인 결론을 도출할 수 있을 것으로 본다.

본 논문을 통해 PCI PA-DSS 준수 대상인 소프트웨어 벤더는 표준 간 연계를 고려하여 중복되는 컴플라이언스 준수 노력을 효율적으로 감소시킬 수 있다. 또한 PA-DSS 준수를 위해 특화된 소프트웨어 개발 생명 주기에 따라 주체별로 명확한 역할 및 책임을 부여하여 효과적인 PA-DSS 준수 활동이 가능할 것으로 기대한다. 본 연구를 통해 소프트웨어 벤더는 보안 표준을 준수하여 보다 안전한 지급결제 어플리케이션을 개발하고, 기타 관계자들은 PCI 보안 표준에 대해 폭넓게 이해함으로써, 해당 시장의 확대는 물론 보다 안전한 지급결제 서비스가 실현될 수 있기를 바란다.

참고문헌

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

[2] 김범수, "미국의 개인정보 유출 통지 제도의 현황과 시사점," 人,@Internet, 1(2), pp. 50, 2009년 9월.

[3] 김인석, 김태호, 강형우, 이정호, 홍기석, 전자금융 이러면 안전할까?, 디비바다 미디어, 2010년 4월.

[4] 김자봉, 홍정훈, "최근 지급결제 환경변화에 대응한 감시체계 및 제도 개편 방향에 관한 연구," 지급결제학회지, 1(1), pp. 39-70, 2007년 12월.

[5] 김재필, "비금융기관의 지급결제서비스 현황 및 전망," 지급결제학회지, 2(1), pp. 1-26, 2008년 6월.

[6] 최대수, "효과적인 지불카드산업(PCI DSS) 컴플라이언스 구현 방안 연구," 정보보호학회지, 18(5), pp. 21-32, 2008년 10월.

[7] PCI Security Standard Council, "Payment card industry(PCI) data security standard - requirements and security assessment procedures," Version 1.2.1, PCI Security Standard Council, Jul. 2009.

[8] PCI Security Standard Council, "Payment card industry(PCI) payment application data security standard - program guide," Version 1.2.1, PCI

Security Standard Council, Jul. 2009.

[9] PCI Security Standard Council, "Payment card industry(PCI) payment application data security standard - requirements and security assessment procedures," Version 1.2.1, PCI Security Standard Council, Jul. 2009.

[10] "올해부턴 보안기준 한층 강화된다," 자동인식&보안, 14(1), pp. 36-39, 2009년 1월.

[11] PCI Security Standards Council Home Page, <http://www.pcisecuritystandards.org/>

[12] PCI DSS 보안감사에서부터 솔루션에 대한 모든 것! PCI DSS, (주)에이쓰리시큐리티, 2008년 7월.

[13] Trial by fire, PricewaterhouseCoopers, 2009

[14] "카드 고객정보 대량 유출..부정사용 피해도 속출," 연합뉴스, 2010년 1월 24일, <http://www.yonhapnews.co.kr/>

[15] "ATM hack gives cash on demand," IDG Communications, Jul. 29, 2010. <http://www.pcworld.idg.com.au/>

[16] "How to apply ISO 27002 to PCI DSS compliance," TechTarget, Jan. 28, 2008. <http://searchsecurity.techtarget.com/>

〈著者紹介〉

허 성 무 (Seongmoo Heo)
정회원

2009년 2월 : 중앙대학교 경영학과 졸업
2008년 11월~현재 : (주)에이쓰리시큐리티 컨설팅사업본부 컨설턴트
관심분야 : 정보보호, IT 감사, 내부 감사, GRC