情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

결제카드산업 데이터보안표준(PCI DSS) 적용방안에 대한 고찰

김 동 국*, 장 성 용**

요 약

신용카드 및 직불카드 회사들의 연합체인 PCI SSC(PCI Security Standards Council)는 2004년 가정이나 소매상과 같은 소규모 환경에서 고객들의 금융 정보 유출을 방지하기 위한 목적으로 PCI DSS가 제정되었다. 국내에서는 2007년부터 PCI DSS 보안감사제도가 시행되었으며 유일하게 PCI DSS 보안감사자를 보유한 ㈜에이쓰리시큐리티사가 가맹점[1] 및 PG/VAN社를 대상으로 PCI DSS 보안감사를 실시하였다. 본 연구에서는 2007년 한 해 동안 국내의 PCI DSS 보안감사를 수행하면서 요구사항에 만족하지 못하는 항목들에 대한 사례를 분석함으로써 국내 PCI DSS 보안감사 도입의 현 주소를 파악하고 이에 대한 개선안을 도출하여 보안감사에 보다 유연하게 대처할 수 있도록 하고자 한다.

2007년 한해 국내 보안감사 실시 결과 PCI DSS 보안감사 대상자의 요구사항 준수율은 평균 81%로 측정되었으며, 전체 233개의 요구사항 중 미적용으로 평가된 항목은 평균 38.7개로 나타났다. 전체적인 평균으로 따져봤을 경우 어느 정도 양호한 수준으로 판단할 수도 있으나 피감사 기업의 업태나 사전준비의 유무에 따라 많은 격차가 있었다. 특히, 기반이 튼튼한 PG사나 VAN사에 비해 신규로 등록되어 사업규모가 작거나 타사에 비해 카드결제산업이 차지하는 사업비중이 작은 곳은 PCI DSS 보안감사의 요구사항을 준수하는데 어려움을 겪고 있는 것으로 나타났다.

따라서, 본 연구에서는 PCI DSS 보안감사를 통해 도출된 미적용 사항 중 가장 많은 미적용율을 나타낸 10가지 항목에 대하여 분석하고 이에 대한 대안을 제시함으로써 향후, PCI DSS의 요구사항을 기업환경에 맞게 적용하기 위해 효율적인 가이드로써 활용되었으면 하는 바램이다.

Ⅰ. 서 론

정보시스템의 의존도가 높아짐에 따라 정보시스템보안 사고에 대한 위험이 매년 증가하고 있는 시점에서 정보보호는 단순한 정보시스템이나 정보기술에 국한된 문제가 아니라 국가적으로 광범위하게 시급하게 대처해야 하는 문제로 대두되고 있다.

특히, 우리나라 경우 지난 2008년 2월에 국내 대표적인 전자상거래 업체의 개인 정보가 유출되는 초유의 사태가 발생함으로써 이제는 개인정보보호에 대한 예방 및 통제 수준은 선택이 아닌 필수적인 부분으로 회사의 존속여부까지 미치는 파장이 되어버린 현실이다[1].

또한, 좀비 PC를 이용한 유해 트래픽을 동시에 유입시켜 서비스를 마비시키는 중국발 DDoS공격으로 인한 피해는 날로 증가하여 정부기관, 금융기관 등을 대상으로 하는 바이러스, 해킹등 사이버 테러에 의한 국가 안보가 위협을 받게 되었다. 이러한 상황에 대처하고자 공공기관뿐만 아니라 기업 차원에서는 정보보호관리체계의 수준을 평가하고 취약점을 파악, 대처함으로써 정보보호관리수준을 한 단계 진전시키고자 하는 노력을 기울이고 있는 실정이다.

정보보호를 위한 관심은 금융분야 중 카드소유자정보를 다루고 있는 카드업계에서도 주요 이슈로 부각되었으며, 이러한 정보보호관리 준수요건의 하나로 PCI DSS

* 서울산업대학교 IT정책전문대학원 박사과정 (share21@a3sc.com)
** 서울산업대학교 산업정보시스템학과 교수 (syjang@snut.ac.kr)

1) 전자상거래에 카드소유자정보를 취급하는 상점 : 옥션, 인터파크 등

(지불 카드산업 데이터표준)[2]가 제정되었다. 기존에는 대형 카드브랜드사 마다 고객정보 유출 방지를 위한 방법으로 각각의 보안감사 표준을 적용하고 있었으나 보다 통일된 보안감사 기준을 개발하기 위하여 PCI SSC (Security Standard Council)가 발족됨으로써 이러한 개별적인 보안감사에서 통합된 보안감사 기준인 PCI DSS를 개발하고 결제카드산업에 적용하기 시작하였으며 국내에서는 2007년부터 보안컨설팅 전문업체인 ㈜에이쓰리시큐리티가 QSA(Qualified Security Assessor)를 보유한 업체로 PCI SSC에 등록되어 지난해부터 단독으로 평가를 수행하고 있다.

국내의 보안감사 대상자는 연간 신용카드 결제 트랜잭션 중 VISA 트랜잭션이 600만 건 이상인 가맹점과 VISA의 AIS 프로그램에 적용받으며 연간 VISA 트랜잭션이 60만 건 이상인 PG社와 VAN社들이 PCI DSS 보안감사 적용 대상이다. 앞으로 PCI DSS를 적용받을 사업자들은 더 늘어날 것으로 예상된다.

PCI DSS 보안감사는 2006년 9월 PCI SSC의 설립과 동시에 PCI DSS v1.1이 발표되어 효력을 발효하게 되었으며, 오는 2008년 11월 30일까지 모든 PCI DSS 보안감사 대상 기업에 대하여 강제 적용할 방침으로 주요 이슈가 되고 있다. 보안감사 통과 기준은 PCI DSS 요구사항의 100%를 만족하는 것이며, 데드라인까지 요구사항을 적용하지 못하였을 경우 별도의 패널티를 적용받게 될 예정이다.

본 논문에서는 먼저 PCI DSS 보안감사제도에 대한 개요, PCI QSA소개, PCI DSS 보안감사 절차 등을 살펴보고, 실제 카드소유자정보를 취급하는 기업들이 고객 데이터를 처리하는 과정에서 발견되는 미이행 항목에 대한 적절한 대안을 살펴보고 분석함으로써, 향후 증가될 보안감사 대상 기업들이 중점적으로 고려해야 할 요구사항이 무엇인지에 대해서도 살펴보고자 한다.

〔표1〕 PCI DSS보안감사 대상 기준[7]

가맹점 레벨	선택기준	검증실행 사항	검증실행자
1	• 연간 6,000,000건 이상의 거래를 처리하는 모든 가맹점(승인 채널 불문) • 고객 데이터 침해사고로 이어진 해킹, 공격을 받은 모든 가맹점 • 카드 협회에 의해 레벨 1으로 분류된 모든 가맹점	• 매년 현장 보안감사 • 분기별 네트워크 스캔	• 독립된 보안 평가기관(QSA) • 내부감사(회사 임원 승인 시) • 공인된 독립스캔벤더(ASV)
2	• 연간 1,000,000 ~ 6,000,000건의 거래를 처리하는 모든 전자상거래 가맹점	• 매년 PCI 자체 평가서 • 분기별 네트워크 스캔	• 가맹점 • 공인된 독립스캔벤더(ASV)
3	• 연간 20,000 ~ 1,000,000건의 거래를 처리하는 모든 전자상거래 가맹점	• 매년 PCI 자체 평가서 작성 권장 • 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)

Ⅱ. PCI DSS(결제카드산업 데이타보안표준) 제도

2.1 개 요

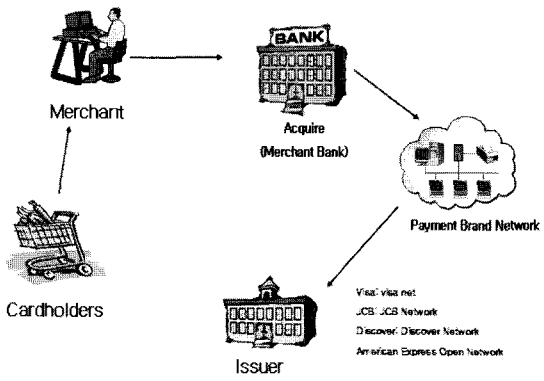
PCI DSS는 기존에 VISA, MASTER Card 등이 각자 운영해온 보안감사 프로그램을 통합해 하나의 통일된 보안감사 기준으로 제정한 표준으로서 신용카드 데이터 보호와 네트워크 보안을 위해 자가진단, 취약점 분석, 보안 실사등을 실시하도록 권고하고 있다.

카드브랜드의 보안프로그램으로는 비자카드의 CISP (Card Information Security Program), 마스터카드의 SDP(Site Data Protection Program) 등의 프로그램이 존재하였지만 다른 보안 표준간의 불일치, 보안요구사항의 중복 등으로 인한 불편함으로 인해 각자 운영해온 보안 프로그램을 통합하여 보안감사 프로그램을 준수해야하는 모든 가맹점 및 서비스 제공업체들을 대상으로 일관된 보안감사를 적용하기 위한 프로그램으로써 PCI DSS를 제정하게 되었다.

이 표준은 카드사용자정보를 취급하는 VAN社, PG社, 가맹점들의 정보처리-업무환경과 보안정책 및 정보보호 환경의 보안수준을 평가하는 것이며, 가장 중점적인 요구사항은 카드소유자정보를 불필요하게 저장하거나 보안에 취약하게 보관하는 것에 대하여 엄격한 통제를 요구하고 있다. 대표적인 요구사항으로 카드번호를 내부에 보관 시 암호화, 마스킹처리, 일방향 해쉬함수등을 적용하여 안전한 방법으로 저장하도록 요구하고 있으며 마그네틱 데이터, CVC/CVV[3], 비밀번호 등은 반드시 저장을 금하도록 규정하고 있다[2].

2) 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

3) CVC : Card Verification Code(Master)
CVV : Card Verification Value(VISA)
안전한 암호화 과정을 사용하는 카드의 마그네틱선에 기록된 데이터로서 데이터의 무결성을 보호하고 데이터의 위조/변조를 막는다.



〔그림1〕 결제 카드 사업 흐름 〔6〕

2.2 결제 카드 산업 흐름

신용카드 사용자(Cardholders)는 대형마켓이나 소매점을 통하여 물품을 구매하면서 상점에서 카드를 사용하게 된다. 사용된 카드내역은 개인정보와 함께 신용카드결제 트랜잭션이 발생하며 이러한 트랜잭션은 가맹점 혹은 PG社나 VAN社의 결제정보 처리시스템을 통하여 매입사나 은행으로 전송되게 된다. 이러한 카드결제 트랜잭션 흐름의 일부분은 담당하고 있는 기업들은 카드결제정보 조회 및 승인 취소 등의 연계 서비스를 위하여 기업내 정보시스템에 카드사용자의 결제 정보를 저장하게 된다.

이상의 절차를 기본적인 흐름으로 도식화 하면 [그림 1] 결제 카드 사업 흐름과 같다.

2.3 PCI QSA 소개

PCI DSS 보안감사를 수행하게 되는 보안감사자는 QSA 자격을 취득한 자만이 보안감사를 수행할 수 있으며 승인된 보안감사자인 QSA(Qualified Security Assessor)는 다음과 같은 요건을 통하여 매년 공정한 검증을 거쳐 갱신되고 있다.

■PCI QSA의 요구조건

QSA(Qualified Security Assessor)는 보안감사 대상 기업들의 PCI DSS 요구사항 준수여부를 현장에서 검토하는 감사자를 의미하며 매년 4~5회 PCI SSC (Security Standard Council)에서 주최하는 QSA 자격시험을 통하여 선발하고 있다. QSA 자격시험에 참가하기 위해서는 QSA가 근무하는 회사가 PCI SSC 보안감사 인증 기관으로 등록되어 있어야 한다.

■PCI DSS 보안감사 평가기관 등록

PCI DSS 보안감사를 수행할 수 있는 평가기관으로 등록되기 위한 요구조건으로는 첫째, 비즈니스 적법성, 독립성, 보장범위, QSA비용, QSA Agreement와 같은 경영요건을 갖추어야 하고 둘째, 다양한 보안 경험으로 얻은 기술과 Know-how를 가진 임직원과 기밀성 및 민감한 정보의 보호, 품질 보증 및 증거 보존을 위한 PCI 절차 엄수등과 같은 관리요건을 포함한 주요 조건을 충족하여야 한다[3].

2.4 PCI DSS 보안감사 절차

PCI DSS 보안감사는 VISA와 같은 글로벌 카드브랜드의 회원사로 등록되어 있는 매입사들이 자신들의 서비스를 이용하는 PG社, VAN社, 가맹점들에게 보안감사를 이행하도록 요구하며, 이러한 요구를 접수한 보안감사 대상 기업들은 QSA를 보유한 독립된 평가기관에 보안감사를 신청하고 적합여부를 평가받게 된다.

먼저, 첫 번째로 시작되는 문서자료 검토는 PCI DSS 요구사항에 포함되는 모든 평가범위의 사내 정보보호 정책/지침서, 주기적인 정보보호 교육 시행 여부, 침해사고 대응 계획, 시스템관리 및 데이터백업 업무의 적절성, 시스템 사용자 계정관리 절차, 네트워크 구성의 적절성, 접근차단 정책의 적절성, 정기적으로 수행된 보안점검기록 등에 관하여 문서화된 증적으로써 증빙할 수 있는 자료를 검토한다. 문서자료 검토 후 각 담당자와의 인터뷰를 통해 카드소유자정보통제현황을 파악하며, 전산실 물리 실사와 주요 시스템 보안설정 확인 등의 현장실사를 진행한다.

인터뷰 진행시 감사인은 [표 2] PCI DSS 보안감사의 12가지 요구사항에 해당되는 233개 세부항목의 감사를 통해 통제사항이 적합한지 여부를 감사 기록 체크리스트에 기록한다. 기록되어진 PCI DSS 보안감사에 대한 결과는 '보안감사 결과 보고서'로 작성되어 피감사자에게 전달하여 보안감사 결과에 대한 고객확인 및 수정사항 발생 시 보완하고 미이행으로 나타난 통제항목에 대하여 향후 보완계획인 "개선계획 보고서(Remediation Plan)"를 작성하여 미이행 항목에 대하여 개선하고 필요한 조치가 이루어지도록 계획한다.

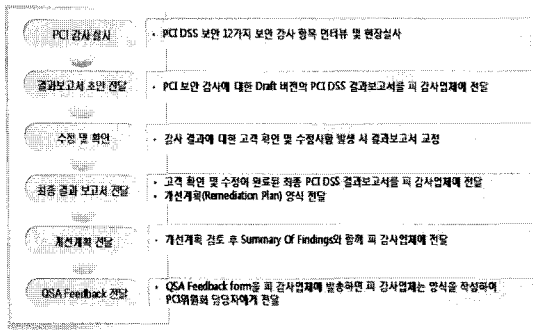
QSA는 피감사 업체가 제출한 Remediation Plan을

〔표 2〕 PCI DSS 보안감사의 12가지 요구사항[5]

항목	요구사항	세부항목
1	데이터보호를 위한 침입차단시스템의 설치 및 유지관리	25
2	제조사가 제공하는 시스템 기본 패스워드 및 기타 보안 설정 값의 사용 금지	13
3	저장 데이터의 보호	30
4	카드 소유자 정보 및 민감한 정보의 암호화 전송	6
5	바이러스 백신 소프트웨어 설치 및 정기적 업데이트	3
6	안전한 시스템과 어플리케이션 개발 및 유지관리	32
7	알 필요성(Need-to-Know) 원칙에 따른 접근통제	2
8	시스템사용자 별 고유 ID부여	26
9	카드 소유자 정보에 대한 물리적 접근통제	24
10	자원과 카드 소유자 정보에 대한 접근추적 및 모니터링	31
11	보안시스템 및 프로세스의 정기적 테스트	11
12	정보보호 정책 유지관리	44

검토 후, PCI DSS 보안감사에 대한 요약본인 'Summary Of Findings'을 작성하여 피감사 업체에 전달한다. 이후 피감사 업체는 회원사(매입사)의 PCI DSS 보안감사 결과 요청시 QSA로부터 전달받은 3개의 결과 보고서 (RoC[4], Remediation Plan, Summary Of Findings)를 전달하게 된다. 또한, 피감사인은 PCI DSS 보안감사를 실시한 QSA에 대한 평가 설문지인 "QSA Feedback form"을 작성하여 설문지에 기재된 PCI SSC 담당자의 메일주소로 발송하면 된다[4].

이상의 보안감사 절차에 대한 기본적인 흐름을 도식화 하면 다음과 같다.



〔그림 2〕 PCI DSS 보안감사 절차

2.5 표준 준수 보고서 내용

PCI DSS 보안감사를 수행한 감사인은 피감사 기업의 카드소유자정보처리 환경에 RoC 를 다음과 같은 보고서 양식에 따라 작성하여 피감자에게 전달한다.

1) 연락 정보 및 보고일자
- 가맹점/서비스 제공업체 및 감사인 연락 정보
- 보고일자

2) Executive Summary
- 피감사 기업의 사업에 대한 설명
- 회사가 카드소유자정보를 공유하는 서비스 제공업체 등의 관련 당사자들의 목록
- 정보 처리업체(processor)와의 관계 목록
- 해당 당사자가 카드회사와 직접 연결되어 있는지 여부
- 가맹점의 경우 사용하는 POS 제품
- PCI 정보보안 표준을 준수해야 하는 모든 자회사 법인 및 국제법인
- 카드소유자 정보 환경에 연결된 모든 무선 LAN 및/혹은 무선 POS 단말기

3) 감사 활동 및 접근법에 대한 기술
- 해당 보안감사 수행을 위해 사용된 보안감사 절차 버전
- 보안감사 수행기간
- 보안감사 시 중점을 둔 환경 (예: 고객의 인터넷 접근 지점, 회사 내부 네트워크, 매입사에 대한 처리 지점 등)
- 보안감사에서 제외된 분야
- 개략적인 네트워크 토폴로지 및 통제구성도
- 인터뷰 대상자 및 검토 대상 목록
- 하드웨어 및 중요 소프트웨어 목록

4) 분기별 스캔 결과
- 요구사항 11.2에 최근 4회의 분기별 스캔 결과 요약
- 감사 대상 업체에 존재하는 모든 (인터넷을 통해) 외부에서 접근하는 IP Address가 스캔 대상에 포함

4) RoC(Report on Compliance) : 표준 준수 보고서

5) 감사 결과 및 분석

- 모든 감사자는 각각의 보안 요구사항에 대해 상세한 내용을 기록하고 파악된 사항을 고려하기 위해 보고양식을 활용해야 함[5].

Ⅲ. 미이행 사항 분석

3.1 개요

PCI DSS 보안감사제도가 국내에서 처음 시행된 2007년에 PCI DSS 보안감사를 받은 가맹점, PG社, VAN社를 대상으로 보안감사를 통해 도출된 주요 미이행 항목들을 분석하고 세부통제 항목별 특징을 살펴보고자 한다.

3.2 세부 통제항목별 주요 미이행 항목

보안감사를 수검한 기업의 결과를 바탕으로 미이행으로 반영된 항목을 분석해 보면 총 233개의 세부통제 항목 중 141 개의 미이행 항목이 있었으며, 그중 가장 많은 수의 미이행 항목으로 나타난 10가지 세부통제 항목에 대하여 분석하였다. 보안감사 결과 가장 많은 미이행 항목으로 나타난 세부통제 항목은 PCI DSS 3.4항목으로 카드소유자정보는 어떤 형태로든 데이터를 저장 시 안전한 방법을 통하여 보관하도록 요구하는 사항이다. 또한 두 번째로 많은 미적용 세부통제 항목은 PCI DSS 3.3 항목으로 대부분의 피감사 기업은 카드번호의 온라인 출력 서비스 제공시 마스킹 처리를 하지 않거나 PCI DSS에서 요구하는 마스킹 처리기준에 미달한 것으로 나타났다.

상위 10가지 주요 미이행 항목에 대한 내용을 [표 3]를 통하여 확인할 수 있으며, 다음으로 세부통제항목의 요구사항과 미적용 사유 및 이에 대한 대응 방안에 대하여 분석하였다.

3.2.1 3.4 카드소유자정보의 안전한 저장

카드소유자정보는 고객의 개인정보가 기록되어있는 만큼 어떤 형태로든 읽을 수 없어야 하며 무선 네트워크, DB서버, 백업테이프와 같은 매체를 통해 고객 정보의 유출 가능성을 미연에 방지하여야 한다. 카드 소유자 정보의 유출 방지와 관련하여 주로 발견되는 미이행을 살펴보면 다음과 같다.

〔표 3〕 상위 10개의 미이행 항목

순위	세부통제	요구 사항	미이행수
1	3.4	민감한 카드소유자 정보는 어떤 곳에 저장되어 있더라도 다음과 같은 방법을 이용하여 읽을 수 없는 형태로 되어야 함 (이동식 매체, 로그, 무선네트워크를 통해 송수신되는 데이터를 포함) • SHA-1과 같은 단방향 Hash • Truncation (일부 정보 생략) • Index token과 PAD (PAD는 안전한 곳에 저장됨) • 3-DES 128-bit 혹은 AES 256-bit와 같은 강력한 암호화 (key 관리 절차 포함) 최소한 신용카드 번호만큼은 반드시 읽을 수 없도록 암호화되어야 함.	36
2	3.3	카드번호에 대한 masking (첫 6자리 혹은 마지막 4자리 숫자만 display될 수 있음) 단 특별히 카드번호를 모두 봐야 하는 직원에게는 적용되지 않음	15
3	11.2	최소 분기당 한 번 혹은 네트워크에 중대한 변화가 생겼을 경우 내부 및 외부 네트워크에 대한 네트워크 취약점 스캐닝 수행	15
4	6.1	모든 시스템과 소프트웨어는 벤더가 제공하는 최신의 보안 패치를 유지해야 함	13
5	8.5.8	그룹/공유/일반적인 계정/패스워드 허용 금지.	13
6	11.5	중요 시스템 및 파일의 비인가된 변경을 감시하고 경고하기 위한 파일 무결성 점검을 수행해야 함. 중요한 파일에 대해서는 최소 매일 수행해야 함	12
7	2.3	콘솔상에서의 접근이 아닌 경우 암호화. 웹기반 관리 및 콘솔 이외의 관리 접근에 대해 SSH, VPN 또는 SSL/TLS 등의 기술 사용	11
8	8.5.12	새로운 패스워드는 직전 사용한 4개의 패스워드와 동일한 것을 허용하지 않음	11
9	9.7.1	카드소지자 데이터를 담고 있는 매체의 등급을 분류하여 '기밀'로 분류된 정보를 식별하기 위한 라벨링	11
10	10.4	모든 주요 시스템의 시간 동기화	11

- 카드소유자정보를 DB에 보관하고 있으며, 데이터를 보호하기 위한 암호화는 적용하지 않음
- DB 서버 실사결과, 카드소유자정보가 평문 혹은 미흡하게 마스킹 처리되어 저장됨
- 어플리케이션에서 생성되는 카드결제 승인 로그(전문)를 확인한 결과 카드번호 등이 로그에 기록됨

미이행 항목에 관한 적절한 대안으로는 카드소유자 정보의 재사용이 불필요한 경우SHA-1 과 같은 단방향 Hash와 Truncation 혹은 Masking 을 적용할 수 있다. 단, Truncation 혹은 Masking 적용 시 PCI DSS 3.3에서 요구하는 6자리를 Masking 처리를 해야 한다. Index token 및 PAD를 사용할 경우 OTP방식의 암호화를 이용하여 카드소유자정보를 암호화하고 암호화에 사용된 OTP PAD를 일반 사용자로부터 접근통제가 이루어진 안전한 저장소에 저장해야 한다. 또한 DB암호화 솔루션을 사용하여 3-DES 128-bit 혹은 AES 256-bit와 같은 강력한 암호화를 이용하여 카드소유자정보를 암호화하고 DB암호화 키에 대한 문서화된 키 관리 절차를 보유해야 한다.

3.2.1 3.3 신용카드번호 마스킹 처리

신용카드번호가 온라인상에 출력될 경우 PCI DSS에서 요구하는 자릿수에 맞는 마스킹 처리가 되어야 하며, 특별히 카드번호를 모두 봐야하는 직원에게는 적용되지 않고 POS 영수증과 같이 카드소유자 정보가 출력되는 경우 PCI DSS보다 엄격한 상위 규정이 존재한다면 필수 요구사항으로 대체되지 않는다.

신용카드 마스킹과 관련하여 주로 발견되는 미이행을 살펴보면 다음과 같다.

- PCI에서는 카드번호를 온라인상에 출력 시 3rd Range와 3rd Range 앞의 2자리를 마스킹 처리 하도록 요구하고 있으나 마스킹 처리가 미흡함

미이행 항목에 관한 적절한 대안으로는 신용카드번호가 온라인으로 출력되는 서비스를 제공하는 경우 PCI DSS에서 요구하는 6자리를 마스킹 처리하도록 한다. 단, 임직원 및 이해관계자를 위한 일반 사용자의 접근통제가 이루어지는 온라인 출력은 Masking처리 예외사항으로 본다.

3.2.3 11.2 분기별 취약점 스캐닝

서버/네트워크/어플리케이션 취약점 스캔과 관련된 산출물을 점검하여 카드소지자 데이터를 관리하고 있는 환경에 대한 정기적인 보안 점검이 수행되고 있는지 확인이 필요하다.

서버/네트워크/어플리케이션 상에서 네트워크 구성도 변화 및 신규 시스템의 설치로 인한 변경과 관련하여 주로 발견되는 미이행을 살펴보면 다음과 같다.

- 분기마다 1회 이상 정기적으로 내부취약점 스캐닝과 ASV에 의한 외부취약점 스캐닝을 수행하지 않음

미이행 항목에 관한 적절한 대안으로는 첫째, 11.2.a의 요구사항을 만족하기 위해서는 내부에 존재하는 네트워크/서버/어플리케이션에 대하여 분기별 취약점 스캔을 실시하고 이에 대한 스캐닝 결과를 보유하여야 한다. 스캐닝 결과에는 카드소유자정보를 처리하는 환경과 연관되는 시스템에 대한 스캐닝 결과가 반드시 포함되어 있어야 한다.

둘째, 11.2.b에서 요구하는 외부 취약점 스캐닝은 승인된 스캐닝 벤더들 (Approved Scanning Vendors - 이하 ASV)에 의하여 분기마다 실시하여야 한다. 현재 전 세계적으로 130개 이상의 ASV가 존재하고 ASV 목록은 PCI CSS 웹 사이트에[5] 기재되어 있으며 이중 하나의 ASV를 선택하여 분기마다 스캐닝을 실시하고 스캐닝 결과를 감사자에게 제출하면 된다.

3.2.4 6.1 시스템 보안 패치

각 시스템에 적용된 보안 패치 리스트와 최신 벤더가 제공한 보안 패치 리스트는 보안 패치와 관련된 정책을 점검하여 새로운 보안 패치가 발표된 지 30일 이내에 적용되어야 한다는 규정이 있는지 점검해야 하며 패치와 관련하여 주로 발견되는 미이행을 살펴보면 다음과 같다.

- 서버 보안 정책서에 서버 각 기종별 최신의 패치를 설치하고 이를 주기적으로 감사 하 도록 명시하고 있지만 최근 버전에 대한 적용은 이루어지지 않음
- 보안 패치는 발표 후 30일안에 적용토록 하는 요구

5) https://www.pcisecuritystandards.org/pdfs/asv_report.html

에 대하여 해당 지침 반영이 미흡함

미이행 항목에 대한 적절한 대안으로는 보안감사자는 정보보호정책서에 최신 보안패치 발표 후 1개월 이내에 적용하도록 요구하는 항목을 신설하고, 완벽한 테스트를 거쳐 보안패치를 적용해야한다.

3.2.5 8.5.8 공용 그룹/패스워드 사용 금지

시스템 관리 혹은 다른 중요한 작업을 위한 공유 계정이 존재하여 접근 통제와 관련되어 주로 발견되는 미이행은 다음과 같다.

- 업무처리를 위한 통합계정 사용에 따른 그룹/공유 패스워드 사용의 위험성 존재
- 개발자나 실무자가 업무상 필요시 공유계정을 발급하여 사용하다 반납 시 그대로 방치되는 공유계정이 존재하는 위험

미이행 항목에 관한 적절한 대안으로는 사내 정보보호정책서에 그룹/공유 패스워드에 대한 사용금지 조항과 요청을 거부토록 하는 요구가 필요하며, 시스템 운영을 위한 계정의 사용이 필요할 경우 개인 개정으로의 로그인 후 SU와 같은 명령으로 계정 변경을 통하여 시스템을 운영하거나 운용에 필요한 사용자만을 관리운용 그룹에 포함시켜 운영하여야 한다.

이러한 계정 전환 절차를 통하여 이력을 남김으로써 차후 장애발생시 책임소재를 분명히 할 수 있으며, 비인가자에 의한 관리자 계정으로의 직접적인 무차별공격(Brute-Force Attacks)으로 인한 위험을을 예방할 수 있다.

3.2.6 11.5 중요 파일 무결성 점검

파일 무결성에 대한 점검을 수행하기 위하여 모니터링 된 파일들을 검사 및 결과물에 대한 검토를 통해 File integrity monitoring products (파일 무결성 감시 제품)를 사용하고 있는지를 점검하며 파일 무결성과 관련하여 주로 발견되는 미이행 항목을 살펴보면 다음과 같다.

- OS와 관련된 중요 시스템 설정파일에 대하여 무결성 검사 도구가 설치되어 있지 않음

미이행 항목에 관한 적절한 대안으로는 파일 무결성 모니터링 소프트웨어를 구축하여, 중요한 시스템 파일 또는 콘텐츠 파일의 무단 수정 발생 시, 해당 임직원에게 알리고 중요한 파일에 대해서는 최소 주 1회 이상 파일 비교 작업을 수행한다. 중요한 파일이란 시스템에서 사용하는 중요 명령어 파일을 가리킨다. (ls, pwd, cd, mkdir, rm 등) 이러한 중요 시스템 파일이 비인가자에 의해 변경되었을 경우, 관리자가 중요 명령어를 실행함과 동시에 악의적인 사용자가 중요파일에 심어놓은 스크립트가 같이 실행되며, 중요 시스템은 비인가된 작업을 수행하게 된다. 이러한 변경을 탐지하기 위하여 무결성 점검 도구를 이용하여 중요파일에 대한 수시점검과 변경 시 경고 메시지를 통해 파일 무결성을 유지할 수 있다.

3.2.7 2.3 원격 접속 시 안전한 기술사용

시스템 구성요소, 중요 서버, 무선 AP를 콘솔이 아닌 곳에서 관리상 접속 시 SSH등에 의해 암호화되어 있는지 점검하며 시스템의 서비스와 파라미터를 검토하여 내부적으로 Telnet 및 기타 원격 로그인 명령어의 사용이 금지되고 있는지 확인이 필요하다. 또한, 무선 관리 인터페이스에 대한 관리자 접근이 SSL/TLS로 암호화되는지 확인도 필요하며 콘솔상에 접속 시 주로 발견되는 미이행은 다음과 같다.

- 암호화되지 않은 평문 접속인telnet 등의 원격 접속 방법을 사용하여 주요 데이터의 유출 위험이 존재

미이행에 관한 적절한 대안으로는 PCI DSS 보안감사에서는 콘솔 이외의 모든 관리자 접근(Non-console administrative access)시 암호화된 접근 기술을 이용하도록 요구하고 있으며, 웹 기반 관리 및 기타 콘솔 이외의 관리자 접근에 SSH, VPN, 또는 SSL/TLS 등의 기술을 활용하도록 요구하고 있다. 이에 따라 콘솔 이외의 별도의 원격 접근 방식을 이용하여 주요 시스템을 관리할 경우 암호화된 프로토콜을 이용한 접근기술을 사용하여야 한다.

3.2.8 8.5.12 동일한 패스워드 사용금지

시스템 구성 요소, 중요 서버, 무선 AP의 샘플링을 통해 현재 시스템 구성 설정을 점검하여 패스워드 파라미터가 새로운 패스워드는 이전에 사용한 4개의 패스워

드와 똑같이 사용할 수 없도록 설정을 요구하는지 점검해야 하며 주로 발견되는 미이행은 다음과 같다.

- 정보보호정책서에 사용자 계정이나 패스워드 관리에 순환 패스워드의 주기적인 변경 요구 미흡
- 최초 패스워드는 사용자별로 고유하게 할당 되지만 사용자에 의한 즉각적인 변경 미흡

미이행 항목에 관한 적절한 대안으로는 새로운 패스워드는 사용된 마지막 4개 중 어떠한 패스워드의 중복 사용을 허용하지 않아야 한다. PCI DSS는 신규 패스워드 등록 시, 과거에 사용 했던 4 개의 패스워드와 동일하게 설정할 수 없도록 요구하고 있다. 이는 이전에 사용한 패스워드를 반복하여 사용할 경우 비인가자에게 노출로 인한 시스템 불법 로그인으로 이어질 수 있기 때문이다. 따라서 이전에 사용했던 4개의 패스워드를 기억하고 동일한 패스워드로 변경을 시도할 경우 변경되지 않도록 시스템의 보안파라미터를 수정하여야 한다.

3.2.9 9.7.1 기밀 정보 라벨링

카드소지자 데이터를 담고 있는 모든 매체의 등급을 구분하여 '기밀' 정보로 식별되고 있는지 확인이 필요하며 주로 발견되는 미이행 내용은 다음과 같다.

- 보안정책에 비밀정보를 SSL1등급으로 분류하고 있으나 저장매체의 등급 표기 부재

미이행 항목에 대한 적절한 대안으로는 카드소지자 데이터를 담고 있는 매체의 등급을 구분하여 기밀자료로 식별해야 한다. PCI DSS는 카드소유자정보를 포함하는 모든 매체를 기밀정보로 식별할 수 있도록, 등급표기를 하도록 요구하고 있다. 매체라 함은 카드소유자정보를 저장하기 위하여 사용되는 CD, DVD, 백업테이프, 백업라이브러리 등을 가리키는데 이러한 데이터 저장 매체에 '기밀' 혹은 'SL1'등을 라벨링하여 중요 정보가 담긴 매체를 식별 가능토록 처리하여 관리하여야 한다.

3.2.10 10.4 NTP를 이용한 시간 동기화

시간 동기화를 위해 회사 내의 정확한 시간을 확인하여 배포하는 프로세스를 검토하고 시스템 구성요소, 중요 서버, 무선 AP등 시간 관련 시스템의 변수들을 점검해야 하며 주요 시스템의 시간동기화에서 발견되는 미이행은 다음과 같다.

- NTP(Network Time Protocol) 기술을 이용한 시스템간 시간의 동기화 미흡
- 최신 NTP(Network Time Protocol) 버전 사용 미흡
- 내부 NTP(Network Time Protocol) 서버의 구성이 PCI DSS에서 요구하는 구성 조건에 미달

미이행 항목에 관한 적절한 대안으로는 중요 시스템의 시간 동기화가 필요하다. PCI DSS는 모든 중요 시스템의 시간을 동기화 하도록 요구하고 있다. NTP (Netime Time Protocol)서버를 이용하여 내부 중요 시스템들의 시간을 동기화함으로써 결제정보의 무결성을 유지하기 위함이다. 이를 위해 조직 내부의 둘 또는 세 대의 중심이 되는 타임 서버들이 외부 소스 [특별한 무선 라디오, GPS 위성으로부터 직접 받거나, 또는 국제원자시(IAT)와 UTC(과거 GMT) 에 근거한 외부 소스]로부터 타임 신호를 받아서 서로 비교함으로써 정확한 시간을 맞추고, 다른 내부의 서버들과 시간을 공유하여 시간을 동기화해야 한다. 또한 가장 최신 버전의 NTP를 사용하여 구버전 사용으로 인한 보안 취약점을 예방하고, 공격자에 의한 시각 변경 공격을 방지하기 위한 방안으로 타임서버가 NTP 업데이트를 제공받을 수 있는 특정 외부 호스트를 지정하여 시각정보를 받아오도록 하는 설정이 필요하다.

3.3 세부 통제항목별 주요 개선 항목

PCI DSS를 준수하기 위해서는 여러 가지 방법을 통하여 준비가 가능하다. 이에 대한 한 가지 대안으로써 솔루션을 도입할 경우 어떠한 항목에 대하여 만족할 수 있는지 [표 4]를 통하여 분석하여 보았다.

단, 각 벤더사의 솔루션별로 해당 항목에 대한 준수 기능에 차이가 있을 수 있다.

Ⅳ. 결 론

2007년에 PCI DSS 보안감사를 받은 기업을 대상으로 보안감사 시 발견된 미이행 항목을 분석하였고 이중 미이행률이 가장 높은 주요 세부통제 항목 10가지를 세

〔표 4〕 솔루션별 적용가능 항목

솔루션	요구항목
로그관리 솔루션	10.1 시스템 구성요소에 대한 모든 접근 시도를 개개의 사용자와 연관 지을 수 있는 프로세스 수립
	10.2 7가지 감사로그들(카드소유자 정보에 접근하는 모든 개인 사용자, 루트 또는 관리자 권한이 부여된 사용자에 의한 모든 행위, 모든 감사 증적에 대한 접근, 잘못된 접근시도, 식별 및 인증 메커니즘 사용, 감사로그 초기화, 시스템레벨 객체 생성 및 삭제)을을 기록
	10.3 10.2에서 언급된 감사 대상 이벤트에서 다음의 6가지 사항을 기록(사용자 신원, 이벤트 종류, 날짜와 시간, 성공 혹은 실패 표시, 이벤트의 발생지점, 영향을 받는 데이터 이름
	10.5.1 직무 상 필요시에만 감사 증적을 볼 수 있도록 제한
	10.5.2 비인가된 수정이 발생하지 않도록 감사 증적 파일을 보호
	10.5.3 중앙 로그 서버나 변경이 용이하지 않은 매체에 감사 증적 파일을 신속히 백업
	10.5.4 내부 LAN 로그 서버에 무선 네트워크 로그를 복사
	10.5.5 파일 무결성 모니터링 및 변경 추적 소프트웨어를 사용하여 기존 로그 데이터 변경 시 경고 발생
	10.6.b 모든 시스템에 대한 정기적인 로그 점검이 수행되고 있는지 확인
	10.7 감사 증적 히스토리를 최소 일년간 보관하고 온라인상에서는 최소 3 개월간 이용 가능하도록 보관
키 관리 솔루션 (키 관리에 대한 정책/지침이 구비되어 있어야 함)	3.5.1 암호화 키에 대한 접근을 필요한 최소한의 관리자로 제한
	3.5.2 암호화 키를 안전한 저장소에 안전한 형태로 보관
	3.6 3.6.1~3.6.10 에서 요구하는 10가지 항목에 대하여 카드소유자 정보 암호화에 사용되는 모든 키 관리 프로세스 및 절차를 문서화하며 이를 준수
DB암호화 솔루션	3.4 카드소시자 정보 보호
	3.5.1 암호화 키에 대한 접근을 필요한 최소한의 관리자로 제한
	8.5.16.a DB로의 모든 접근에 대한 인증
모의해킹	6.5 OWASP를 기준으로 웹 반 어플리케이션에 대한 취약점 점검
	6.6 정기적인 웹 반 어플리케이션 코드에 대한 점검
	11.3.2 어플리케이션 계층의 모의해킹 테스트
Email 암호화 솔루션	4.2 암호화되지 않은 e-mail을 통한 PAN 전송 금지
2 Factor 인증 솔루션	8.3 직원, 관리자 혹은 제3자에 의한 원격 접속의 인증을 위해 두 가지 인증 조치를 구현(RADIUS, TACAS, VPN)
무결성 점검 솔루션	10.5.5 파일 무결성 모니터링 및 변경 추적 소프트웨어를 사용하여 기존 로그 데이터 변경 시 경고 발생 11.5 파일 무결성 모니터링 소프트웨어를 구축하여, 주요한 시스템 또는 컨텐츠 파일의 무단 수정 발생 시, 경고 발생
취약점 분석 스캐너	11.2.a 최소 분기마다 또는 네트워크 상 중요한 변경 발생 시 네트워크/서버/어플리케이션 취약점 스캔에 대하여 취약점 스캔
침입탐지 솔루션	11.4 모든 네트워크 트래픽을 감시하고 침해 시도를 탐지하기 위해 NIDS, HIDS 혹은 IPS를 운영해야 함.

부감사통제항목으로 선정하여 요구사항과 미이행 사례 및 대안에 대하여 서술하여 보았다.

현재, 카드 결제 시 발생하는 개인정보에 대한 중요성은 기업뿐만 아니라 개인 모두가 점점 더 중요성을 인식하고 있으며 각종 개인정보 유출사고를 통하여 사회적 이슈로 부각되고 있다. PCI DSS는 국내에서는 처음으로 시행되는 보안감사인 만큼 해당 기업은 많은 미이행 항목의 도출에 따른 정보보호정책의 개선과 기술적으로 보완해야 할 부분을 고려해야 한다.

마지막으로 피감사 기업이 감사요건을 준수하기 위한 환경구축 시 다소 어려워하는 부분들에 대하여 고찰해 보았다.

첫째, PCI DSS 보안 감사가 글로벌 스탠다드를 기준으로 만들어진 요구사항이기에 국내의 사업규모가 작은 PG나 VAN사에게도 유연하게 적용할 수 있도록 고려되었으면 하는 바램이다.

둘째, 사업 규모에 비해서 PCI DSS 요건 준수를 위한 부가적인 사업예산이 추가로 투입되어 예상외의 사업예산 확보가 발생할 수 있겠다. 특히, 국내 금융감독원 전자금융거래법의 요구사항과 PCI DSS에서의 유사

한 요구사항으로 인하여 중복투자가 발생할 경우 규모가 작은 피 감사업체는 경제적 부담이 가중될 수 있겠다. 향후 이러한 규정의 중복에 대해서는 기준을 명확히 하고 규정의 조율을 통하여 비용대비 효과적인 보안감사 제도가 정착되었으면 한다.

셋째, 현재 PCI DSS에서는 요구사항 3.4에 대하여 보완 통제(Compensation Control)를 두어 보완통제 준수 시 요구사항 적용으로 보고 있으나 여타 항목에 대해서도 PCI DSS 보안감사실시에 따른 조건부 이행 항목을 추가하는 것도 유연하게 PCI DSS를 적용하기위한 방안이라고 본다. 현재, 감사 항목은 이행, 미이행에 따른 부분이지만 이행의 증적 활동으로 일부를 만족한다는 입장에서는 부분적인 조건부 이행에 해당되는 부분도 고려할 수 있으므로 조건부 이행 항목을 신설하는 것도 하나의 방안이 될 수 있겠다.

본 연구는 PCI DSS를 기업에 적용 시 가장 많이 나타난 미적용 사례를 분석하고 이에 대한 대응방안을 제시함으로써, 향후 PCI DSS 보안감사를 수검하기위해 준비하고자 할 때 미리 이행 증적 활동의 차원으로 도움이 될 것이라고 판단된다.

또한, PCI DSS의 모범사례를 발굴하여 활용, 적용함으로써 궁극적으로는 개인정보의 보안 강화로 인하여 기업의 정보보호 운영환경의 신뢰성이 증대되고 대외적으로는 결제카드산업의 대외신뢰도를 기여하는데 역할이 되었으면 한다.

참고문헌

[1] 디지털타임스, "가입자 개인 정보 유출 비상" Feb 2008.

[2] PCI Security Standard Council, Glossary, Abbreviations and Acronyms, p3, Sep 2006.

[3] PCI Security Standard Council, Validation Requirements for Qualified Security Assessors, pp. 33-35, Sep 2006.

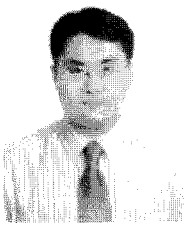
[4] PCI Security Standard Council, Validation Requirements for Qualified Security Assessors, pp. 36-39, Sep 2006.

[5] PCI Security Standard Council, Payment Card Industry Data Security Standard Security Audit Procedures v1.1, pp. 8-46, Sep 2006.

[6] PCI Security Standards Council, Qualified Security Assessor Training, p. 37, 2007.

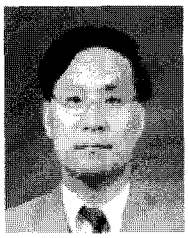
[7] http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais_how.shtml

〈著者紹介〉



김 동 국 (Kim Dong-Guk)

1991년 8월 : 서울산업대학교 전자계산학과 공학사
1998년 2월 : 홍익대학교 국제경영대학원 회계학과 경영학석사
2007년 2월 : 서울산업대학교 IT정책전문대학원 산업정보시스템 전공 박사과정 수료
2006년~현재 : (주)에이쓰리시큐리티 컨설팅사업부 수석 컨설턴트
<관심분야> 정보보호컨설팅, 내부통제, Forensics, 위험관리, SROI



장 성 용 (Jang Sung-Yong)

1980년 2월 : 서울대학교 산업공학과 공학사
1982년 2월 : 서울대학교 산업공학과 공학석사
1991년 2월 : 서울대학교 산업공학과 공학박사
1987년~현재 : 서울산업대학교 산업정보시스템공학과 교수
<관심분야> 시뮬레이션, e-비즈니스 프로젝트 경영, SCM, TOC