PCI DSS 보안 감사 체계와 동향

곽진* 한상우** 이동범**

사회가 점차 편리함을 추구하면서 결제의 방식도 화폐에서 신용카드로 바뀌어 가고 있는 추세이다. 이러한 신용카드는 편리함이라는 장점과 함께 인터넷을 이용한 전자결제시의 개인정보 유출과 가맹점들의 무분별한 고객정보 소유 등 보안적인 문제가 함께 야기되고 있다. 본 고에서는 이러한 보안 문제의 해결 및 보안 사고 예방을 위해 제정된 보안 감사인 PCI DSS에 대해 소개하고, 그 동향에 대해 기술하고자 한다.

목 차

Ⅰ. 서 론
Ⅱ. PCI DSS 제도
Ⅲ. 등록 과정
Ⅳ. 보안 감사 항목
Ⅴ. 결 론

* 순천향대학교 정보보호학과/교수
** 순천향대학교 정보보호응용 및 보증연구실/연구원

Ⅰ. 서 론

최근 신용카드 사용이 보편화되고 전자상거래가 활성화됨에 따라 금융, 주식거래, 경매, 물류, 유통 등 산업 전반에 빠르게 확산되고 있다. 하지만 해외의 경우 지난 2007 년 1 월 TJX Companies 에 공격자가 무선 POS 단말을 통해 내부 네트워크에 접근하여 내부 정보를 유출하는 사고가 발생하였고 국내의 경우 2008 년 2 월 대형 전자상거래 업체의 고객정보가 대량으로 유출되는 초유의 사고가 발생하기도 했다.

이와 같은 고객의 신용카드 정보를 노린 해킹 및 도난, 분실 사고가 급증하면서 고객정보를 보호하기 위하여 신용카드 및 직불카드 회사들의 연합체인 결제카드산업 보안 표준 위원회(Payment Card Industry Security Standards Council: PCI SSC)에서는 결제

카드산업 데이터보안표준(Payment Card Industry Data Security Standard: PCI DSS)을 제정하였다.

PCI DSS 는 고객의 신용카드 정보를 보호하기 위하여 VISA, MasterCard, American Express 등 대형 다국적 카드회사들이 참여하는 정보 보안 프로그램이다. 국내의 경우 2008 년 12 월부터 이를 강제 적용시켰지만 보안 감사 대상 업체들은 PCI DSS 의 요구사항을 완벽하게 준수하지 못하는 실정이다. 이에 본 고에서는 PCI DSS 의 보안 감사 체계와 동향에 대해서 살펴보고자 한다.

II. PCI DSS 제도

1. 개요

PCI DSS 는 기존의 국제카드 브랜드 사업자의 가맹점과 전자결제(Payment Gateway: PG), 부가가치통신망(Value Added Network: VAN) 사업자에 대한 독립적인 보안 감사 프로그램들을 하나의 통일된 표준으로 제정한 보안 감사 프로그램이다. 표준이 제정되기 이전에는 카드회사별로 VISA 는 CISP(Cardholder Information Security Program), MasterCard 는 SDP(Site Data Protection), American Express 는 자체의 DSS 프로그램, Discover 는 Data Security Guidelines 등 보안 감사 프로그램을 각각 운영해 왔다[1]. 하지만 고객의 신용카드 정보를 노린 해킹 및 도난, 분실 사고가 급증하면서 American Express, Discover Financial Services, JCB, MasterCard Worldwide 그리고 Visa International 등의 다국적 대형 카드회사들은 2006 년 6 월 PCI SSC 를 발족하고, 동시에 PCI DSS v1.1 의 효력을 발생시켰다. 그리고 2008 년 12 월부터 국내 모든 보안감사 대상에 대해 강제적으로 적용함으로써 이를 지키지 않는 감사 대상에 대해서는 벌금 부과 및 카드 결제 승인거부 등 강력한 제재를 하겠다고 발표하였다. 국내의 보안 감사 대상자는 <표 1>, <표 2>와 같이 연간 신용카드 결제 트랜잭션 중 VISA 트랜잭션이 600 만 건 이상인 가맹점과 VISA 의 AIS 프로그램에 적용 받으며 연간 VISA 트랜잭션이 60 만 건 이상인 PG 社와 VAN 社가 PCI DSS 보안감사 적용 대상이며, 앞으로 PCI DSS 를 적용 할

<표 1> PG, VAN 사의 보안감사 대상

연간 VISA 트랜잭션	600,000 건 이상	120,000~600,000 건	120,000 건 이하
자가진단서	선택	의무	의무
분기별 네트워크 스캔	의무	의무	권고
실사	의무	권고	권고

<표 2> 가맹점의 보안 감사 대상

가맹점 등급	선택 기준	검증 실행사항
1	- 연간 6,000,000 건 이상의 거래를 처리하는 모든 가맹점 (승인 채널 불문) - 고객 데이터 침해사고로 이어진 해킹, 공격을 받은 모든 가맹점 - 카드 협회에 의해 등급 1 로 분류된 모든 가맹점	- 매년 현장 보안감사 - 분기별 네트워크 스캔
2	- 연간 1,000,000~6,000,000 건의 거래를 처리하는 모든 전자상거래 가맹점	- 매년 PCI 자체 평가서 - 분기별 네트워크 스캔
3	- 연간 20,000~1,000,000 건의 거래를 처리하는 모든 전자상거래 가맹점	- 매년 PCI 자체 평가서 작성 권장 - 분기별 네트워크 스캔
4	- 그 외 모든 가맹점(승인 채널 불문)	- 매년 PCI 자체 평가서 작성 권장 - 매년 네트워크 스캔 권장

사업자들은 더 늘어날 것으로 예상된다[2].

2. 구조

PCI DSS 는 PCI SSC, PCI QSA, PCI DSS 보안 감사 절차로 구성되어 있다.

가. PCI SSC

기존의 카드회사별로 각각 가지고 있던 보안 감사 프로그램을 VISA 와 MasterCard 가 공동으로 PCI 정보보안 기준, PCI 자가진단서, PCI 취약점 분석 기준, PCI 보안실사 지침서를 마련하고, American Express, JCB, Diners 가 PCI DSS 에 동의함으로써 2006 년 9 월 7 일 PCI SSC 가 발족 되었다[3]. PCI SSC 는 새로운 규정을 제정하고 카드사의 준수를 요구하는 것은 물론 준수여부를 검사하는 QSA 업체를 선정하는 등의 역할을 담당한다. 현재 Microsoft, Wal-Mart, British Airways, Paypal, VeriFone 등이 위원회 회원사로 활동하고 있으며, 국내에서는 2008 년 9 월 한국 주니퍼 네트웍스가 회원사로 동참하여 활동 중이다.

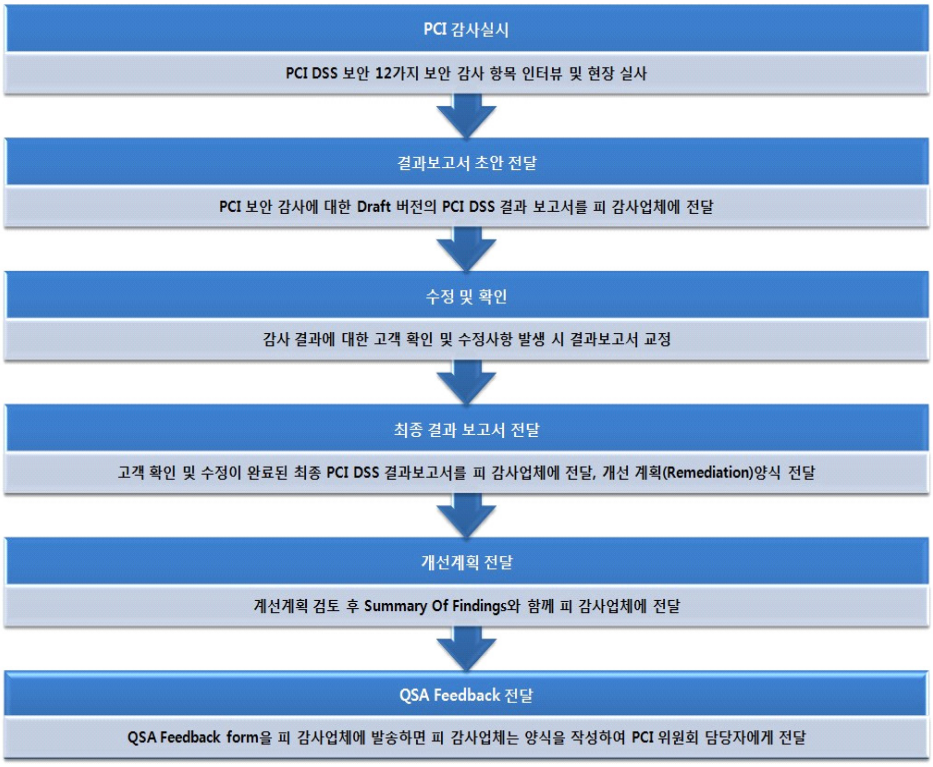
나. PCI QSA

PCI QSA(Qualified Security Assessor)는 실제 보안 감사를 실시하는 감사인으로써 PCI SSC 에서 매년 4~5 회 실시하는 QSA 자격 시험을 통해 선발하고 있다. 자격 요건은 QSA 가 근무하는 회사가 PCI SSC 보안 감사 인증기관으로 등록되어 있어야 하며, 인증기관으로 등록되기 위해서는 비즈니스 적법성, 독립성, 보장범위, QSA 비용, QSA Agreement 와 같은 경영요건을 갖추어야 하고, 다양한 보안 경험으로 얻은 지식과 기술을 가진 임직원과 기밀성 및 민감한 정보의 보호, 품질 보증 및 증거 보존을 위한 PCI 절차 엄수 등과 같은 관리 요건을 포함한 주요 조건을 충족하여야 한다[2].

다. PCI DSS 보안 감사 절차

PCI DSS 보안 감사는 모든 보안 감사 대상 업체에 대하여 보안 감사를 이행하도록 요구하며, 이러한 요구를 접수한 보안 감사 대상 업체들은 QSA 를 보유한 독립된 평가기관에 보안 감사를 신청하고 적합여부를 평가 받게 된다.

보안 감사는 (그림 1)과 같은 순서로 진행되며, 첫 번째로 시작되는 문서자료 검토는 PCI DSS 요구사항에 포함되는 모든 평가 범위에 관하여 문서화되어 증빙할 수 있는 자료를 검토한다. 이후 각 담당자와의 인터뷰를 통해 카드소유자 정보 통제 현황을 파악하며, 전산실 물리적 실사와 주요 시스템 보안설정 확인 등의 현장 실사를 진행한다. 인터뷰 진행 시 감사인은 PCI DSS 보안 감사의 12 가지 요구 사항에 의한 감사를 통해 통제사항이 적합한지 여부를 감사 기록 체크리스트에 기록한다. 이 기록은 '보안 감사 결과 보고서'로 작성되어 피감사인에게 전달되고, 결과에 대한 고객확인 및 수정사항 발생 시 보완한다. 또한 미이행으로 나타난 통제항목에 대하여 향후 보완계획인 '개선계획 보고서(Remediation Plan)'를 작성하여 미이행 항목에 대하



(그림 1) PCI DSS 보안 감사 절차[2]

여 개선하고 필요한 조치가 이루어지도록 계획한다.

QSA 는 피감사 업체가 제출한 개선계획 보고서를 검토 후, PCI DSS 보안 감사에 대한 요약본을 작성하여 피감사 업체에 전달한다. 이후 피감사 업체는 회원사(매입사)의 PCI DSS 보안 감사 결과 요청 시 QSA 로부터 전달받은 3 개의 결과 보고서를 전달하게 된다. 또한, 피감사인은 PCI DSS 보안 감사를 실시한 QSA 에 대한 평가 설문지를 작성하여 설문지에 기재된 PCI SSC 담당자의 메일주소로 발송한다[2].

III. 등록 과정

PCI DSS 보안 감사를 받기 위해 감사 대상 업체는 등록을 해야 하는데 VISA 의 경우 카드 사용자 데이터를 저장, 처리, 전송하는 지불 관련 서비스 제공 업체를 대상으로 하고 있다[4].

1. 등록 조건

VISA 계좌 번호, CVV, CVV2, iCVV, 기타 카드 사용자 정보를 저장, 처리, 전송하는 서비스 공급업체는 반드시 PCI DSS 를 준수하도록 하고 있으며, 현장 실사와 분기별 네트워크 스캔을 VISA 거래 건수별로 차등 시행해야 한다.

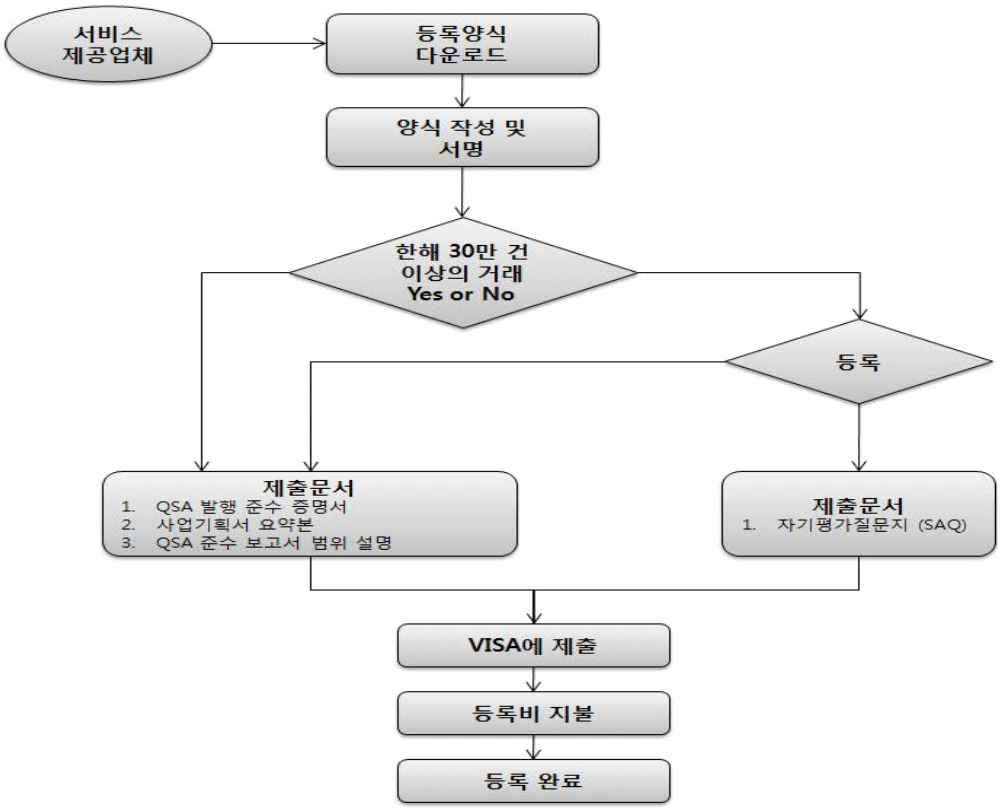
2. 등록 과정

등록 과정은 (그림 2)와 같은 순서로 진행된다. 등록 과정에서 제출해야 하는 서류는 QSA 와 서비스 제공업체가 서명한 '준수 증명서'와 '사업 기획서 요약본', QSA 가 발행한 '준수 보고서(ROC)' 중 업무 범위 및 접근법 부분 등이며, 등록 양식은 VISA 아시아 홈페이지에서 다운로드 받을 수 있다. 또한 등록 승인 후 VISA 는 서비스 제공업체에게 등록비 청구서를 발송하며, 등록비는 미화 5,000 달러를 매년 지불해야 한다.

3. 갱신

PCI DSS 를 준수해야 하는 서비스 제공업체는 준수 증명서 만료 2 개월 전 반드시 준수 검토를 실시해야 하며, VISA 는 서비스 제공업체에게 신규 준수 문서 제출과 등록비 지급을 통보한다. 그러나 요청 문서 및 등록비 미 제출시 VISA 는 다음과 같은 조치를 취할 수 있다.

- 준수 문서 만료일 이후 1~60 일: 서비스 제공업체가 목록에 노란색으로 표시
- 준수 문서 만료일 이후 61~90 일: 서비스 제공업체가 목록에 빨강색으로 표시



(그림 2) VISA 의 등록 과정

- 90 일 이후: 목록에서 서비스 등록업체가 삭제

IV. 보안 감사 항목

1. 안전한 네트워크 구축 및 유지

가. 요구사항 1: 데이터 보호를 위한 침입 차단 설치 및 유지

회사 네트워크의 내외부에 허용된 컴퓨터 트래픽 뿐만 아니라 회사 내부 네트워크 상에서 민감한 영역을 통과하는 트래픽을 통제하는 장비인 침입차단시스템을 이용하여 임직원들의 데스크탑 브라우저를 통한 인터넷 접속, 전자 메일 접근 등 인터넷 접속 시 모든 시스템을 인터넷 상에서의 비 인가된 접근으로부터 보호한다. 인터넷 상의 취약한 경로를 통해 주요 시스템으로 불법 접근할 수 있는 취약점을 차단하여 시스템과 데이터를 보호한다.

나. 요구사항 2: 기본적으로 제공되는 패스워드 및 기타 보안 설정 값 사용 금지

공격자들은 개발사가 제공한 기본 패스워드와 기타 개발사의 디폴트 값 등을 사용하여 시스템 침입을 시도한다. 이런 패스워드와 디폴트 값은 공격자 커뮤니티 사이에 이미 잘 알려져 있기 때문에 공개된 정보를 통해 쉽게 파악될 수 있는 경우를 대비한다.

2. 카드 소유자 정보보호

가. 요구사항 3: 저장 데이터 보호

암호화는 카드 소지자 정보보호를 위해 매우 중요한 사항이다. 침입자가 다른 보안 장치를 뚫고 암호화된 데이터에 접근한다 하더라도 암호 해독 없이는 데이터를 읽을 수도 없고 사용할 수도 없다. 잠재적인 위험 요소를 줄이기 위해 카드 소지자 정보보호를 위한 다른 방안도 강구되어야 한다. 예를 들면 반드시 필요한 경우가 아니면 카드 소유자 정보를 저장하지 않는다. 또한, PAN(Primary Account Number) 전체가 필요하지 않으면 카드 소지자 정보의 일부분만 저장하거나 암호화된 E-Mail 을 통해서만 PAN 전송 등 위험을 최소화할 수 있는 방안이다.

나. 요구사항 4: 카드 소유자 정보 및 민감한 정보의 암호화

네트워크 상에서 민감한 정보 전송 시, 반드시 암호화하여 전송 과정에서 공격자들에 의한 데이터 가로채기, 변조 등을 방지한다.

3. 취약점 관리 프로그램 유지

가. 요구사항 5: 바이러스 백신 소프트웨어 설치 및 정기적 업데이트

많은 취약점들과 악성 바이러스들이 직원들의 전자 메일을 통해 네트워크로 유입된다. 바이러스 유입을 방지하기 위해 모든 시스템에 바이러스 백신 소프트웨어를 설치해야 한다.

나. 요구사항 6: 안전한 시스템과 애플리케이션 개발 및 유지관리

공격자들은 보안 취약점을 악용하여 시스템의 특수 접근권한을 획득한다. 대부분의 취약점은 개발업체에서 제공한 보안 패치를 통해 수정되며 직원, 외부 공격자 및 바이러스로부터 침입 방지를 위해 최신 버전의 소프트웨어 패치를 적용하도록 해야 한다.

4. 강화된 접근 통제 방안 수립

가. 요구사항 7: 알 필요성(Need-to-Know) 원칙에 따른 통제

이 요구사항은 인가된 인원에 의해서만 중요 데이터에 접근할 수 있음을 보장한다.

나. 요구사항 8: 시스템 사용자별 고유 ID 부여

인가된 사용자만이 시스템과 데이터에 접근하며, 이들의 작업 내용을 추적하고 확인할 수 있도록 사용자별 고유 ID 를 부여하도록 한다.

다. 요구사항 9: 카드 소지자 정보에 대한 물리적 접근 통제

데이터 및 카드 소지자 정보를 저장하고 있는 시스템에 대한 물리적 접근은 사용자들에게 관련 장비와 데이터에 대한 접근과 시스템 및 하드카피 문서 제거 등의 기회를 제공함으로 적절히 제한되어야 한다.

5. 정기적 네트워크 모니터링 및 테스트

가. 요구사항 10: 카드 소지자 정보에 대한 접근추적 및 모니터링

로깅 메커니즘(Logging mechanism)과 사용자 활동 내역 추적은 매우 중요한 부분이다. 모든 환경에 로그를 생성함으로써 문제 발생시 이를 분석 및 추적할 수 있도록 해야 한다.

나. 요구사항 11: 보안시스템 및 프로세스의 정기적 테스트

공격자 및 연구진에 의해 새로운 취약점이 계속 발견되고 있고, 소프트웨어 도입으로 새로운 유형의 취약점이 지속적으로 발생된다. 시스템, 프로세스 및 자체 개발한 소프트웨어를 주기적으로 테스트하여 시간이 경과하거나 변경이 발생되어도 보안성이 유지될 수 있도록 해야 한다.

6. 정보보호정책 유지 관리

가. 요구사항 12 : 정보보호정책 유지 관리

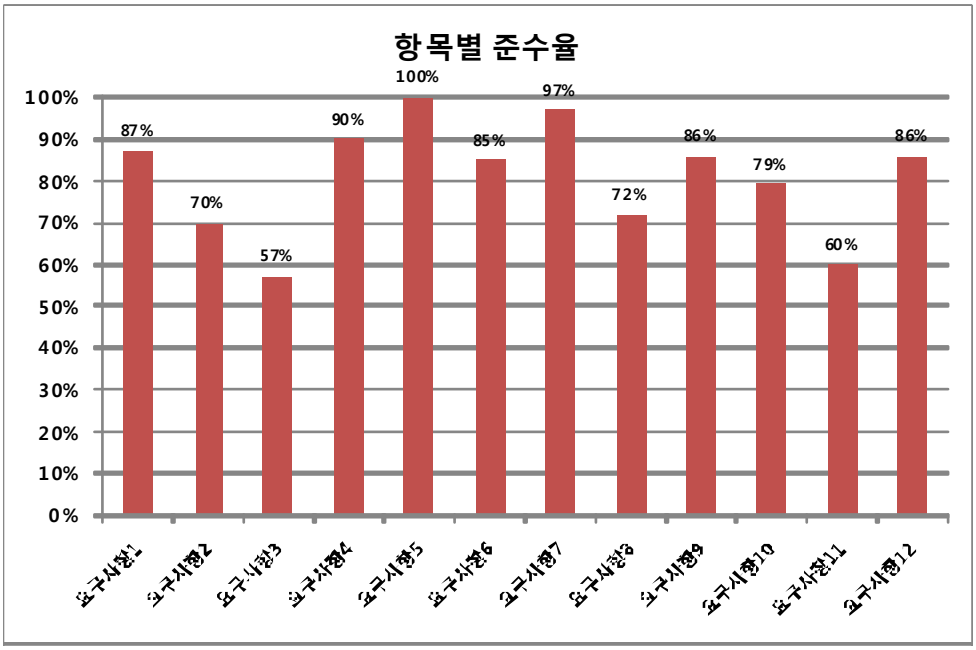
엄격한 정보보호 정책을 마련함으로써 회사 및 직원들의 보안 경각심을 제고할 수 있도록 해야 한다.

V. 결 론

강제적 효력을 발생시킨 PCI DSS 보안 감사로 인해 국내 보안 업계에서도 이에 대한 관련 사업이 확대될 것이라는 전망을 가지고 있지만, 가맹점이나 PG, VAN 사 측면에서는 신경써야 할 부담으로 작용되고 있다.

2008 년 말 기준으로 국내 QSA 감사 자격을 가진 전문가는 5 명으로 A3 Security 가 4 명, 한국 IBM 이 1 명을 보유하고 있어 그 수 역시 많지 않으며, 감사를 시행하는 업체는 QSA 자격을 가진 전문가를 3 명 이상 보유하고 있어야 한다는 위원회의 규정 때문에 실질적으로 감사대상 업체가 감사를 받기 위해 소요되는 시간도 상당할 것으로 예상된다[5].

국내의 경우 2008 년 5 월을 기준으로 감사 대상 기업은 43 개 사로 나타났으며, A3 Security 의 2008 년 7 월 발표에 따르면 2007 년에 실시한 기업에 대한 감사의 평균 만족도는 81%로 100%를 만족시켜야만 하는 PCI DSS 의 요구에는 못 미치고 있다. 보안 감사 12 가지 항목 중 '바이러스 백신 소프트웨어 설치 및 정기적 업데이트' 항목만이 100%의 준수율을 보였으며, '저장 데이터 보호' 항목은 57%로 최저 준수율을 보이고 있다[6]. 이것은 신용카드 정보의 유출로 이어질 수 있으며, 이에 대한 피해는 부정매출 증가, 신규카드 발급 비용 증가, 명의도용, 기업



(그림 3) PCI DSS 준수율[3]

이미지 손실, 기준 업무 및 시스템 프로세스에 혼란 등의 막대한 손실을 가져올 수 있다. 2009 년 6 월로 정해진 준수 마감으로 PCI DSS 보안 감사에 부합되는 보안 강화가 필요하며, 위원회에서 한국을 비롯한 아태지역에 대해 과태료 부과 방침을 정함에 따라 모든 보안 감사 항목에 대한 100%의 준수율을 보이지 않을 경우 상당한 액수의 과태료를 부과하게 될 전망이다.

2009 년 1 월부터 PCI v1.2 의 적용이 의무화 되었지만 이에 대한 불확실한 설명과 애매한 표현들로 미국 내에서도 이에 대한 문의가 쇄도하고 있으며, 국내 감사 대상 가맹점과 PG, VAN 社들의 현실을 감안해 볼 때 국내에 완전히 정착되는 것이 당장은 어려울 것으로 판단되지만, 언젠가는 이 보안 표준이 크게 확대될 것이며 이와 관련된 산업이 크게 성장될 것으로 예상되지만 현재 일본 등 해외에서는 PCI 에 대한 정부 차원의 지원이 활발하게 이루어지고 있는데 반해 국내에서는 PCI DSS 준수를 위한 가이드라인이나, 교육 등이 미흡한 것이 사실이다. 이미 PCI DSS 가 시행되었으며, 준수하지 않을 경우 과태료부과 등의 불이익이 예상되기 때문에 정부의 관심 및 지원이 시급하고, 국내 PCI DSS 보안 감사 대상 업체들의 준수 노력과 보안 업체들의 PCI SSC 가입이 필요할 것으로 분석된다.

<참 고 문 헌>

[1] 최대수, “효과적인 지불카드산업(PCI DSS) 컴플라이언스 구현 방안 연구”, 정보보호학회지 제 18 권 제 5 호, 2008. 10, pp.21-32.

[2] 김동국, 장성용, “결제카드산업 데이터보안표준(PCI DSS) 적용방안에 대한 고찰”, 정보보호학회지 제 18 권 제 4 호, 2008. 8, pp.66-75.

[3] “PCI DSS 개요 및 소개”, A3 Security PCI DSS 세미나, 2008. 7. 11.

[4] http://www.visa-asia.com/ap/kr/index.shtml, VISA 아시아 홈페이지

[5] 김동빈, “PCI DSS, 신용카드가 짓누른다(1)”, 보안뉴스, 2008. 11. 17.

[6] 문영순, “PCI DSS 보안감사 사례 및 준수 방안”, A3 Security PCI DSS 세미나, 2008. 7. 11.

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.