情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

효과적인 지불카드산업(PCI DSS) 컴플라이언스 구현 방안 연구

최 대 수*

요 약

신용카드 정보를 노린 해킹이나 카드 분실 도난 사고가 증가하면서 고객정보를 보호하고자 하는 지불카드산업 데이터 보안표준(PCI DSS[1]) 컴플라이언스가 제정되고 이를 준수하도록 강제화 되고 있다. 국내에서는 정보보호 인식이 높아지고 정보보호시스템이 운영되고 있음에도 불구하고 PCI DSS 를 준수하기 위한 중복된 정보보호활동이 필연적인 상황이다. 본 논문에서 제안하는 정보보호 통제항목 코드화 방안은 효과적인 PCI DSS 구현을 가능하게 하며 하나의 통제 항목 준수로 유사한 다중 정보보호관리체계 준수를 가능하게 한다. 결과적으로 IT 컴플라이언스 통제항목 준수의 상시적 자가진단을 할 수 있다.

Ⅰ. 서 론

1.1 IT 컴플라이언스[2] 동향

세계적으로 정보기술(IT : Information Technology) 분야에서 각종 규제는 오래전부터 있었지만 큰 관심을 끌지 못했다. 그러나 2001년 엔론 사 , 월드콤 사 등의 회계부정사건 이후 재무제표의 작성 및 공시 투명성을 높이기 위해서 2002년 미국에서 사베인즈-옥슬리 법안(SOA : Sarbanes-Oxley Act)이 재정되면서 주목되기 시작했다. 그 외에 미국의 HIPAA(Health Insurance Portability and Accountability Act)는 개인 의료정보와 건강보험의 정보보호와 책임추적성에 대한 규제를 정하고 있다. 그리고 고객의 신용카드 노출사고를 예방하기 위하여 카드 정보를 거래에 이용하는 신용카드 가맹점 및 처리업체에 지불카드산업 데이터보호표준(PCI DSS : Payment Card Industry Data Security Standard) 라는 정보보호 표준 규격을 재정하고 준수하도록 권고하고 있다. 해외에서는 PCI DSS 를 이행하지 않는 가맹점 등에 카드결제 승인을 거부하는 등의 강도 높은 제재방식을 적용하고 있다[1,2,3,6,10,11,14].

산업 분야 및 국가 별로 다수의 컴플라이언스(Compliance)를 개발 운영하고 있으며 준수 의무를 부과하여 미준수시 벌금과 같은 법적 책임을 물어 강제적으로 이행하도록 규제하고 있다. 컴플라이언스란 용어는 우리말로 규제(Regulation) 준수로 해석 할 수 있다. 그리고 IT 컴플라이언스란 기업, 정부기관 등 정보시스템 사용자가 고객 정보보호, 자료 보관, 재무보고서 공시 등과 관련하여 반드시 따라야 하는 규정, 지침 등의 규제를 준수하는 것을 의미한다[12]. 그 외 국내 민간기업의 경우 정보보호관리체계(ISMS : Information Security Management System) 인증 제도를 시행하고 있다. 인증을 획득하면 조직은 광범위하고 효율적인 정보보호 대책을 개발 할 수 있을 뿐만 아니라 자신의 정보보호 수준에 관하여 객관적인 심사를 통해 더욱 높은 신뢰를 가질 수 있다. 또한 위험관리체계를 상시적으로 유지하고 적절한 통제대책을 구현하여 정보보호사고와 패해 발생을 예방할 수 있다. 이러한 인증획득 기업은 기업의 입찰참여나 신용도 평가시 가산점을 획득하고 많은 혜택을 받을 수 있다[4]. 그 외 국제적으로는 ISO/IEC에서 표준화

* 이글루시큐리티 인터넷보안연구소 (dschoi@igloosec.com)

1) 지불카드산업 데이터보안표준은 PCI DSS 또는 PCI 와 일반적으로 혼용하여 사용됨
2) 컴플라이언스는 IT 컴플라이언스 또는 규제 준수와 혼용되어 사용되었음

한 ISO 27001 정보보호관리체계 표준이 있다. 이러한 인증은 정보보호 사고에 따른 법적 분쟁시 자산보호를 위한 주의 의무를 성실히 수행했음을 객관적인 전문가가 인정하였다고 제시할 수 있어 회사 책임을 물을 경우 책임의 감면효과가 있다.

1.2 금융관련 정보보호 동향

국내 금융 부분과 관련된 정보보안은 금융감독원을 중심으로 관심이 일찍부터 형성되어 2000년 9월 전자금융안전대책, 2005년 9월 전자금융거래 안정성 강화 종합대책이 발표된데 이어 전자금융 거래시 해킹이나 전산 장애시 금융기관에 엄중한 책임을 묻는 등 이용자 보호를 강화한 전자금융거래법을 시행하여 전자 금융거래에서의 정보보안이 강화되고 있다. 또한 법률 규정 뿐만 아니라 보안 전담기구를 통한 정보보안 강화노력을 하고 있다. 2006년 12월 금융감독원 산하에 금융 보안을 전담하는 기관으로 금융보안연구원과 일회용비밀번호(OTP : One Time Password) 의 통합인증센터가 공식 출범하여 금융 전자거래 보호에 노력하고 있다[2].

이러한 노력에도 불구하고 금융 거래중 카드 거래와 관련된 정보보호에 대한 요구는 증가되고 있고 국제 규제가 국내에 영향을 미치고 있지만 국내에서는 적극적으로 대처하지 못하는 게 현실이다. 당장 12월부터 시행될 신용카드 가맹점과 서비스 제공자에 대한 PCI DSS 준수에 대한 준비 및 권고, 교육에 손이 미치지 못하고 있다. 그러나 일본의 경우, 일본정보처리개발협회에서 기업정보보호관리체계인 ISMS 인증을 시행하고 있으며 PCI DSS 인증 시 중복검사를 면제해주고 두 가지 인증을 함께 도입하도록 권고하고 있다고 한다[3,14].

본 논문에서는 국내에서 아직 연구가 시도되지 않은 국내외 주요 정보보호관리체계 통제항목과 PCI DSS 통제항목의 연관성을 분석하였다. 국내에서 민간 기업들이 가장 많이 인증을 획득하고 있는 국제정보보호관리체계 표준 ISO 27001과 국내 ISMS의 통제항목을 분석하여 통제대상과 통제행위를 코드화하여 분류하였고 PCI DSS 의 통제항목에 코드를 할당하였다. 이 코드의 효용성을 입증하기 위하여 간단히 프로토타입을 설계하여 활용성을 보였다.

중소규모기업의 경우 인증 및 다수의 IT컴플라이언스 활동을 소수인원이 담당하고 있다. 그러나 유사한 통제항목을 중복 검사, 문서 작업 등을 수행하는 것이 현실이다. 본 논문에서 제시한 통제대상과 통제행위를 기반으로 통제항목 코드화 방안은 다수 IT 컴플라이언스 통제항목간의 공통부분을 구별하여 관련 시스템 개발 및 관련 정보보호활동의 중복노력을 감소시킬 수 있다.

본 논문은 다음과 같이 구성하였다. 2장에서는 PCI DSS와 카드정보관련 유출사고 동향과 인식에 대하여 서술한다. 3장에서는 국내외 정보보호관리체계 ISMS, ISO 27001에 대해 알아보고 PCI DSS 와의 관련성 및 차이점을 분석한다. 4장에서는 PCI DSS 를 기준으로 IT 컴플라이언스 통합 방안에 대해 서술하고 5장에서는 4장에서 서술한 통합 방안을 기반으로 프로토타입을 구현하였다. 6장에서 결론과 향후 연구방향을 제시하였다.

Ⅱ. 관련 연구

2.1 지불카드산업 데이터보안표준(PCI DSS)은 무엇인가?

카드 정보 노출 사고가 급증하고 카드정보보호에 대한 중요성이 인식되면서 2004년 주요카드회사들이 협력하여 PCI DSS(Payment Card Industry Data Security Standards)라는 카드보안 표준을 만들었다. PCI DSS는 지불카드산업 보안표준위원회(PCI SSC : Payment Card Industry Security Standards council)에서 관리한다. 이 위원회는 American Express, Disover, JCB, Diners Club 이 참여하고 있으며 현재 Microsoft, Wal-Mart, British Airways, Paypal, VeriFone 등이 위원회 멤버이다.

초기에는 카드 지불 브랜드 별로 별도의 보안 프로그램을 가지고 카드정보보호에 노력하다가 2006년 PCI SSC가 설립되면서 PCI DSS v1.1 의 효력을 발효하게 되었다. VISA는 2000년 4월 CISP(Cardholder Information Security Program)을 처음으로 시작했고 MasterCard는 SDP(Site Data Protection) 프로그램을 2002년 시행했다. American Express는 자체의 DSS 프로그램을 가지고 있었고 Discover는 Data Security Guidelines 프로그램을 운영했다[7,8,11].

모든 가맹점과 서비스 사업자는 PCI DSS 컴플라이언스 준수 의무를 갖는다. 회원사는 카드 소지자 데이터를 저장, 처리 또는 전송하는 소속 가맹점과 서비스 사업자로 하여금 프로그램을 준수하게 하는 책임이 있다. 즉, 카드 정보를 입력받고 물건을 판매하는 모든 매입사가 대상이 되며 연간 카드 거래 규모에 따라 평가 방법이 달라진다. 그러나 공통적으로 매입사는 PCI DSS 표

〔표 1〕 처리 건수에 의한 처리업체 구분

	연간 600,000 건 이상 처리	연간 120,000 건~600,000 건 처리	연간 120,000 건 이하 처리
자가진단서	선택	의무	의무
분기별 네트워크 점검	의무	의무	권고
실사	의무	권고	권고

〔표 2〕 처리 건수에 의한 가맹점 구분

	연간 6백만 건 이상 처리	연간 20,000 건 이상 처리	그 외 모든 가맹점
자가진단서	선택	의무	권고
분기별 네트워크 점검	의무	의무	권고
실사	의무	권고	선택

준안을 준수해야 하고 지침에 따른 절차 확인이 이루어져야 한다. PCI DSS 표준 준수 여부는 자가 진단서(SAQ : Self-Assessment Questionnaire)와 취약점 점검 결과, 실사에 의해 이루어진다. 가맹점(merchants)와 처리업체(service providers)는 카드 거래 규모에 따라 카드사마다 다르게 구분하여 처리 하고 있다. VISA의 경우를 처리 결과물에 의하여 분류하면 [표1]과 같다[11].

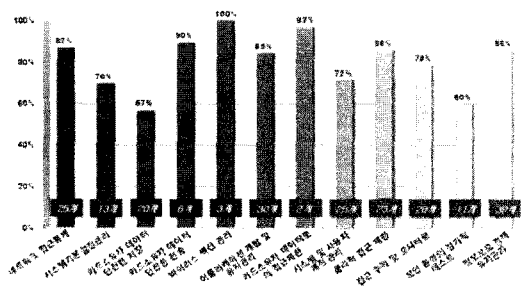
이상과 같이 자가진단서와 분기별 네트워크 점검은 모든 카드거래 업체가 의무 및 선택하여 처리하도록 되고 있다. 이를 만족하지 못할 경우 해당업체는 전자거래에 제재를 받을 수 있다. 세계적인 카드회사들이 신용카드 정보 유출을 막기 위해 PCI DSS 지침을 12월부터 국내에서도 본격적으로 시행할 예정이다. 이에 따라 카드 가맹점, 서비스 제공자, 카드결제 대행업자(VAN), 등은 PCI DSS가 마련한 기준 12개 항목을 2008년 11월 30일까지 모두 만족해야 한다.

2.2 카드 정보 유출사고와 PCI DSS 인식

지난 몇 년간 지불카드 데이터 도난과 노출 사고의 수가 급격히 증가하고 있다. 2005년 6월 CardSystems Solutions에서는 200,000개 이상의 신용카드 소유 계좌정보와 40,000,000명 이상의 개인정보가 노출되는 사고가 발생했다. 2005년 5월 미 연방법무부에서는 80,000명 이상의 고용인의 신용카드정보가 저장된 랩탑 컴퓨터를 분실하는 사고가 있었다. 같은해 HSBC Holdings는 180,000 마스터카드 계좌정보를 분실했다. 2003년 2월 Data Processors International에서는 560,000명의 비자와 마스터 카드 계좌정보가 해킹당했다. 2007년 1월 TJX Companies, Inc. 는 해커가 무선 POS 단말을 통해 내부 네트워크에 접근하여 내부 정보를 유출하는 사고가 발생하였다. 이러한 이유로 TJ Maxx 는 18건의 소송을 당하고 있다[5,6].

PCI DSS 는 카드정보보호를 위한 최소한의 요건을 규정한 보안 표준규격으로 PCI SSC는 100% 준수를 요구하고 있다. 다음 [그림 1] 은 국내 A 사에서 조사한 15개 기업의 보안감사 결과를 제시한다. 평균 준수율이 81% 로 나타났다. 100% 완벽하게 준수해야 하는 규정에 못 미치는 수준이었다. 카드 소유자 데이터의 안전한 저장은 57% 수준으로 가장 낮고, 보안 환경의 정기적 테스트가 60%, 시스템 기본설정 관리가 70%, 시스템 및 사용자 계정관리가 72% 준수에 그쳤다[11].

이러한 준수율이 시사하는 바는 크다. 국내 정보보호 컨설팅 업체에 비용을 지불하고 컨설팅을 받는 업체의 경우 규모가 크고 그 외 정보보호관리체계인증 및 내부 정보보호정책 및 절차가 마련되어있음에도 불구하고 상시적으로 고객 정보보호 생활화가 완벽히 되어 있지 않다는 것이다. 정보보호가 업무 프로세스에 부가적인 노력을 필요로 하지만 이미 익숙해진 정보보호체계와 PCI DSS 중복노력의 문제점이 있기 때문이다. 즉 유사



〔그림 1〕 PCI DSS 준수현황[11]

한 정보보호 통제항목 준수 노력이 PCI DSS에서 제시하는 통제항목과 약간의 차이가 있어서 노력을 하고 있음에도 불구하고 준수하지 못하는 현상이 나타나는 것이다. 이러한 문제점을 해결하고 다중의 정보보호체계 및 IT 컴플라이언스 준수를 위해 유사 통제항목 식별과 한번의 노력으로 다중의 통제항목을 준수하는 상시적인 정보보호 수준 평가 방안이 필요하다.

Ⅲ. IT 컴플라이언스

세계적으로 노동, 안전, 소비자 보호, 개인정보보호 등 다양한 분야에 걸쳐 15,000여개의 컴플라이언스들이 존재하고 있으며 지속적으로 증가하고 있다. 각국의 컴플라이언스들은 국가 간 비즈니스 환경에서 새로운 진입장벽이 되고 있으며, 미준수시 기업들에게 심각한 경제적 손실과 인지도 하락 및 비즈니스 상실과 같은 위험에 처해진다. IT 컴플라이언스는 기업의 비즈니스 IT 의존도가 심화되면서 기업 활동을 효과적으로 규제하기 위해서 비즈니스 활동을 지원하는 정보처리시스템과 디지털 데이터에 대한 규제가 필수적으로 요구되고 있고 특정 규제를 만족시킬 수 있도록 기업의 IT 인프라와 업무 프로세스를 구축하고 재정비하는 것을 말한다. [표 3]은 각종 IT 컴플라이언스를 규제 주체, 적용범위에 따라 분류하였다[3].

3.1 정보보호관리체계(ISMS)

정보보호관리체계(ISMS) 인증이란, 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 관리 체계를 수립하여 운영하고 있을 때, 그 관리체계가 정보보호관리체계의 인증심사 기준에 적합한지를 '정보보호관리체계 인증기관' 등 제3자가 객관적이고 독립적으로 평가하여 적합성 여부를 보증해 주는 것이다. 정보보호관리체계는 우리나라뿐만 아니라 세계각국에서도 유사한 제도를 수립하여 운영하고 있다. 영국의 경우, 가장 먼저 BS 7799-1이라는 정보보호관리에 관한 기준을 작성하여 보급하였고 이 내용은 국제 표준인 ISO/IEC 17799에 반영되었으며, 이에 기초하여 BS 7799-2 인증기관에 따른 인증 제도를 가장 먼저 수립하였다. 이 제도는 국제 표준 기구인 ISO를 통해 국제 표준으로 제정되어 현재 ISO/IEC 17799 : 2000과 이에 대한 인증 기준인 ISO/IEC 27001이 제정, 사용되고 있으며 현재 유럽 및 일본 등을 중심으로 ISO 인증이 제공되고 있다. 일본은 1981년 정보시스템 안전대책 실시 사업소 인정제도를 시행하여 ISMS 수립의 기반을 마련하고 현재 일본 통산성 산하의 JIPDEC(일본정보처리개발협회)에서 ISMS 인증을 제공하고 있다[4].

정보보호관리체계의 인증심사는 방법 및 시행령에 근거하여 정보통신부가 고시한 정보보호관리체계 인증심사기준(정보통신부고시 제2007-30호, 2007. 8.14 개정)과 정보보호관리체계 인증 업무지침(한국정보보호진흥원 2003. 12. 26 개정)에 따라 수행된다. 정보보호관리체계 인증 기준은 ISO/IEC 27001 국제 표준을 모두 포함하고 있다. 개인정보 및 고객정보 등 민감한 정보를 다루고 있는 기관이 인증 대상이 되며 IT 경영평가 및 신용평가, 회계감사 등 외부 평가에 영향을 준다.

일본의 경우, 민관의 유기적인 협조체제가 구축되어 최근에는 신용카드사는 물론 가맹점 서비스업체 등이

〔표 3〕 IT 컴플라이언스 분류

구분	상세구분	IT 컴플라이언스
규제 주체	외부 규제적	SOX, Basel II, GLBA 등
	자율 규제적	PCI DSS, ISO 27001, ISMS 등
적용범위	전체산업 범용	SOX(미국), 컴퍼니빌(영국), 외감법(한국) 등
	특정산업 범용	GLBA(금융), HIPAA(의료) 등
규제 목적	회계투명성	SOX, J-SOX, K-SOX 등
	개인 정보보호	EU Data Protection Act 등
	전자문서이용활성화	전자거래기본법, 전자서명법 등
보호대상	금융정보	Basel II 등
	카드 정보	PCI DSS 등
	환자정보	HIPAA, 의료법 등

〔표 4〕 ISMS 통제항목

통제분야	세부통제사항	통제 항목수	세부통제 항목수
1. 정보보호정책	정책의 승인 및 공표, 정책의 체계, 정책의 유지관리	5	10
2. 정보보호 조직	조직의 체계, 책임과 역할	4	11
3. 외부자 보안	계약 및 서비스 수준협약, 외부자 보안	4	8
4. 정보자산 분류	정보자산 조사 및 책임할당, 정보자산 분류 취급	4	7
5. 정보보호 교육 및 훈련	교육 및 훈련 프로그램 수립, 교육훈련시행 및 평가	4	14
6. 인적보안	책임할당 및 규정화, 직원의 적격심사, 주요직무 담당자 관리, 비밀유지	5	18
7. 물리적 보안	물리적 보안물리적 보호구역, 물리적접근통제, 데이터 센터보안, 장비보호, 사무실보호	12	36
8. 시스템 개발 보안	분석 및 설계, 구현 및 이행, 변경관리	13	53
9. 암호통제	암호정책, 암호사용, 키관리	3	6
10. 접근통제	접근통제 정책, 사용자 접근관리, 접근통제 영역	14	38
11. 운영관리	운영절차와 책임, 시스템 운영, 네트워크 운영 및 문서관리, 악성소프트웨어 통제, 원격 컴퓨터 및 원격 작업	22	99
12. 전자거래 보안	교환합의서, 전자거래, 전자우편, 공개서버의 보안관리, 이용자 공지사항	5	21
13. 보안사고 관리	대응계획 및 체계, 대응 및 복구, 사후관리	7	20
14. 검토 모니터링 및 감사	법적 요구사항 준수검토, 정보보호정책 및 대책 준수 검토, 모니터링, 보안감사	11	37
15. 업무연속성 관리	업무연속성 관리체계 수립, 업무연속성 계획수립과 구현, 업무연속성 계획 시험 및 유지관리	7	18
	총계	120	396

〔표 5〕 ISO 27001 통제항목

통제분야	세부통제사항	통제항목수
1. 보안정책	정보보호정책 문서 및 검토	2
2. 정보보호 조직	내부조직 및 외부관계자에 관한 정보보호 관리	11
3. 자산분류 및 통제	자산에 대한 책임, 정보분류	5
4. 인적자원 보안	고용 전, 고용 중, 고용 후에 대한 인적 자원 관리	9
5. 물리적, 환경적 보안	물리적 보안구역과 출입통제 보안구역에서 작업, 물리적 설비, 설비 폐기 재사용 보안	13
6. 통신 및 운영관리	운영절차와 책임, 제 3자의 서비스 제공관리, 시스템 계획 및 도입, 악성코드 보호, 백업, 네트워크 보안관리, 미디어 취급 관리, 전자거래 서비스,	32
7. 접근 통제	접근통제에 대한 업무요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근통제, 운영시스템 접근통제, 어플리케이션 접근통제, 모바일 컴퓨팅	25
8. 시스템 개발 및 유지관리	정보시스템보안요구사항, 어플리케이션 처리, 암호기법관리, 시스템 파일 보안, 개발 및 지원프로세스 보안, 기술적 취약점 관리	16
9. 침해사고대응	정보보안 이벤트 및 취약점 보고, 정보보안 사고 관리 및 개선	5
10. 사업연속성관리	사업연속성 관리의 정보보안	5
11. 준거성	법적요구사항준수, 보안정책 및 표준의 부합성 그리고 기술적 부합성, 정보시스템 감사 고려사항	10
	총계	133

ISMS는 물론 PCI DSS 인증 및 준수가 꾸준히 늘고 있다고 한다. 이는 일본 기업표준 정보보호관리체계인 ISMS 인증을 PCI DSS 인증시 중복검사를 면제해주고 두 가지 인증을 함께 도입하도록 권고하기 있기 때문이다. 이에 공통 요소 식별 및 준수 방안을 기준 제시가 필요하다.

3.2 ISO 27001

ISO 27001은 정보보호관리체계(ISMS)에 대한 국제적인 표준으로서 정보보호정책, 인력자원보안, 물리적 환경보안, 통신 및 운영관리, 정보시스템 구축 및 유지 등을 관리하는 기업의 경영에 대한 인증이다[9].

ISO 27001은 규모나 산업 부문에 관계없이 모든 기업에 적용된다. 그 중에서 특히 정보보호가 중요한 금융, 보건, 공공 및 IT 부문에 유용하게 사용될 수 있다. 해외의 경우 2007년 말까지 약 20,000여개 기업에서 인증을 획득하였으며 일본의 경우 5,000개 이상의 기업에서 인증을 획득했다. 국내의 경우 2007년 말까지 70여개 기업과 기관에서 인증을 획득하였다.

3.3 PCI DSS 와 주요 컴플라이언스 비교

국내외에서 대표적으로 많이 준수되고 알려진 정보보호관리체계 ISMS, ISO 27001과 PCI DSS 간의 통제항목 내용을 비교한다. 이는 서로 상호 보완적인 관계가 있는 내용으로서 평상시 효과적으로 PCI DSS 와 그 외 통제항목을 한 번의 노력으로 효과적으로 준수하기 위한 기반이 된다. [표 6]은 PCI DSS 의 통제분야와 통제항목수를 분류하였다[12].

관련연구에서 제시한 ISMS와 ISO 27001의 통제 항목수와 PCI DSS 를 비교하면 다음 [표 7]과 같다. [표 7]에서 통제 분야를 보면 ISO 27001과 ISMS는 개괄적인 정보보호 범위를 포함하고 있으며 PCI DSS 의 통제분야는 고객카드정보 보호를 위한 세부적인 통제 분야로 나누어진다. ISO 27001, ISMS는 기업의 기술적, 물리적, 환경적으로 정보보안 관리를 어떻게 해야 하는지에 대한 전반적인 가이드라인을 제시한다. PCI DSS 는 카드 업계를 대상으로 하는 정보보안 표준으로 외부 해킹 등 범죄로부터 카드 정보를 보호하기 위해 세부 기준을 제시한다[13]. 결과적으로 중복되는 부분도 많이 있고 상호보완적인 관계를 가지기도 한다. 또한 ISO 27001과 ISMS는 가능한 범위를 지정하고 범위 내에서 준수를 하지만 PCI DSS 는 100% 준수 의무를 갖는다.

Ⅳ. IT 컴플라이언스와 PCI DSS 통합 방안

4.1 통제항목 연관성 분석

정보보호관리체계 인증 및 감사는 주로 1회성의 통제가 많다. 또한 준수해야 할 IT 컴플라이언스가 많아지면서 감사 당시 1회성이 되어 질 가능성이 더욱 크다.

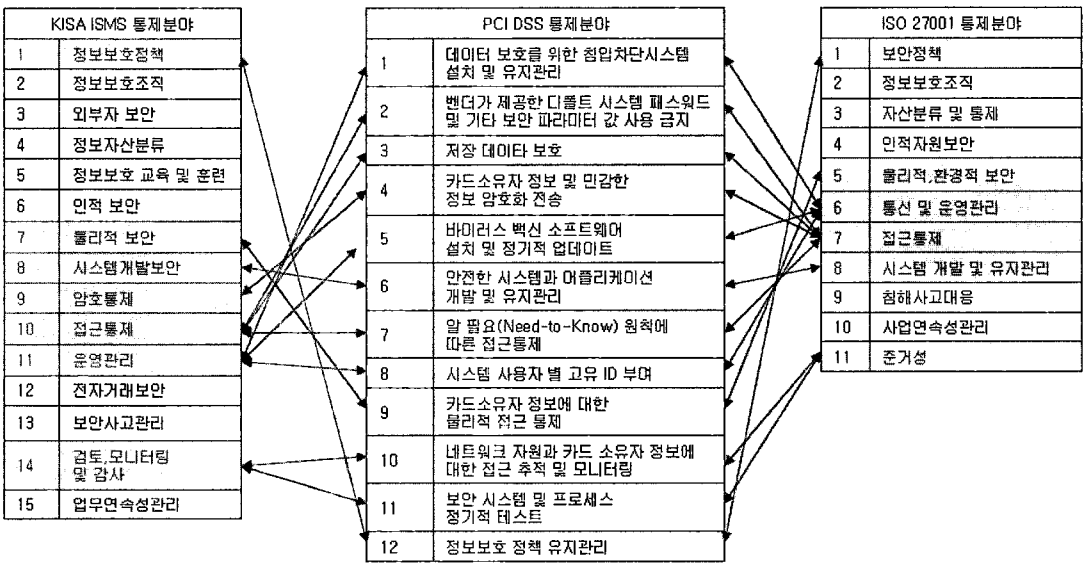
각종 산업 및 국내외 다양한 IT 컴플라이언스 규제가 증가됨에 따라 규제 준수를 효과적으로 이행하고 IT 컴플라이언스간 공통항목에 대한 중복 노력을 줄이고 상시적으로 관리할 수 있는 방법과 시스템이 필요하다. 본 논문에서는 이러한 목표를 위해 국내의 대표적인 정보보호관리체계 인증의 통제항목과 ISO/IEC의 ISO 27001 항목을 지불카드산업 데이터보호표준인 PCI

〔표 6〕 PCI DSS 통제항목

통제분야	통제항목수	세부통제항목수
1. 데이터보호를 위한 침입차단시스템 설치 및 유지관리	5	22
2. 벤더가 제공한 디폴트 시스템 패스워드 및 기타 보안 파라미터 값 사용 금지	4	7
3. 저장 데이터 보호	6	18
4. 카드 소유자 정보 및 민감한 정보 암호화 전송	2	2
5. 바이러스 백신 소프트웨어 설치 및 정기적 업데이트	2	2
6. 안전한 시스템과 어플리케이션 개발 및 유지관리	5	23
7. 알 필요 원칙에 따른 접근 통제	2	2
8. 시스템 사용자별 고유 ID 부여	5	20
9. 카드 소유자 정보에 대한 물리적 접근 통제	10	16
10. 네트워크 자원과 카드 소유자 정보에 대한 접근 추적 및 모니터링	7	22
11. 보안 시스템 및 프로세스 정기적 테스트	5	6
12. 정보보호 정책 유지관리	10	35
총계	63	175

〔표 7〕 PCI DSS, IS027001, ISMS 비교

특징	PCI DSS	ISO 27001	ISMS (KISA)
통제 구현 방법	필수	위험관리 기반	위험관리 기반
구현 상세 내용 정의	높음	낮음	낮음
유연성	낮음	높음	높음
주관기관	PCI SSC	ISO/IEC	KISA
대분류 수	12	11	15
통제항목 수 및 세부 통제항목	63개의 통제항목과 175개의 세부 통제 내용 정의	133개의 통제 항목과 세부 통제항목은 준수방법에 따라 달라짐	120개의 통제항목과 396 개의 세부 통제내용 정의
보호 및 처리 범위	고객카드 정보보호 안전한 네트워크 유지관리,취약점 관리, 접근제어관리, 네트워크 모니터링 및 정보보호정책 유지관리	국내외기업의 정보보호정책, 인력자원보안, 물리적 환경보안, 통신 및 운영관리, 정보시스템 구축 및 유지 등 정보보호체계 운영	국내 기업의 정보보호정책, 인력자원보안, 물리적 환경보안, 통신 및 운영관리, 정보시스템 구축 및 유지 등 정보보호체계 운영
대상기관	카드정보를 이용한 거래업체 (가맹점, 카드처리업체)	국내외 금융 등 모든 기업	정보통신망이용촉진및정보보호등에 관한법률에 따름 정보통신망을 운영하는 민간 사업자로 일반 제조업회사들도 해당
혜택 및 벌칙	미준수시 카드거래 제약 카드정보 노출 사고 발생시 벌금부과	고객 정보보호 준수 수립보장, 인증 후 보안사고 발생시 평시 정보보호준수에 대한 증거 효과	국내 경영평가와 신용평가시 우대, 공공사업 입찰시 우대, 보안사고 발생시 평시 정보보호준수에 대한 증거효과
기간	유효기간 1년 네트워크 취약점 점검은 분기별 점검	유효기간은 3년	유효기간 3년



〈그림 2〉 통제항목 연관성

DSS 1.1 기준과 통합 관리하기 위한 매핑 방안 제시한다. 이 방안을 프로토타입으로 구현함으로써 상시적 관리 효과를 증명한다.

4.2 세부항목 요소 식별

ISO 27001과 ISMS의 통제항목은 개괄적인 내용으

〔표 8〕 대분류 코드 내용

대분류 코드	ISO 27001, ISMS, PCI DSS 의 대분류
SecurityPolicy	정보보호정책, 보안정책, 정보보호 정책 유지관리
Organization	정보보호조직
HumanManagment	외부자보안, 인적보안, 인적자원보안
AssetManagment	정보자산분류, 자산분류및 통제
InformationSecurityEducation	정보보호교육 및 훈련,
PhysicalManagement	물리적보안, 물리적환경적보안, 카드 소유자 정보에 대한 물리적접근통제
DevelopManagement	시스템 개발보안, 시스템개발 및 유지관리, 안전한 시스템과 어플리케이션 개발 및 유지관리
CryptoManagement	암호통제, 카드소유자 정보 및 민감한 정보 암호화 전송
AccessControl	접근통제, 벤더가 제공한 디폴트 시스템 패스워드 및 기타보안파라미터 값 사용 금지, 저장 데이타보호, 알 필요 원칙에 따른 접근통제,
CommunicationOperation	운영관리, 통신 및 운영관리, 데이터보호를 위한 침입차단시스템 설치 및 유지관리, 바이러스 백신 소프트웨어 설치 및 정기적 업데이트, 시스템 사용자별 고유 ID 부여,
ElectronicCommerceSecurity	전자거래보안
IncidentManagement	보안사고관리, 침해사고대응
ComplianceAudit	검토 모니터링 및 감사, 준거성, 네트워크 자원과 카드 소유자 정보에 대한 접근 추적 및 모니터링, 보안시스템 및 프로세스 정기적 테스트
BusinessContinuityManagement	업무연속성관리, 사업연속성관리,

로 되어 있고 PCI DSS 통제항목은 상당히 세부적인 내용을 정의하고 있다. 이러한 차이로 인하여 3개 IT 컴플라이언스를 1 : 1 매핑은 불가능하다. 그래서 본 논문에서는 항목간의 유사성을 객관적으로 분류하기 위하여 대분류와 세부 통제항목을 코드화 하여 상호간에 매핑하는 방안을 이용하였다.

통제 항목별 코드화 가능한 요소에는 다음과 같은 요소들이 될 수 있다.

- 통제 주체 : 통제항목을 수행하는 주체 (정보보호 담당자, 네트워크 관리자)
- 통제 대상 : 통제항목의 대상 (네트워크, 서버 등)
- 통제 행위 : 정보보호 통제 행위 (주기적 점검, 삭제, 패치 등)
- 통제 유효기간 : 한번의 통제 행위로 보호되는 지속기간(1년, 분기, 매일)
- 통제 등급 : 통제 항목의 중요도 (상, 중, 하)
- 자동화 관련 도구 : 통제 항목을 자동화 수행할 수 있는 도구(취약점 분석도구, 방화벽)
- 수동 또는 자동 점검 : 통제 항목을 준수하기위한 방법 (문서화, 자동화도구)

이를 전부 코드화하고자 시도하였으나 너무 복잡해지는 문제와 IT 컴플라이언스별로 차이가 있어서 이들을 전부 코드화할 경우 공통 코드를 식별하기 어려워진다. 통제 주체는 대부분 정해져있고 전사적으로 담당하여야 하며, 통제 유효기간과 통제 등급은 IT 컴플라이언스별로 다르게 적용될 수 있다. 위 요소 중에서 제일

〔표 9〕 ISO 27001 통제항목 코드

	대분류	대분류코드	통제항목	통제항목코드 (통제대상,행위)
1	보안정책	SecurityPolicy	보안정책서	SecurityPolicyApproval
			정보보안 정책검토	SecurityPolicyReview
2	정보보안조직	Organization	정보보안에 대한 경영의지	InformatioSecuritySupport
			정보보안 협력관계	InformationSecurityCoordiation
			정보보안 책임할당	InformationSecurityResponsibility
			정보처리설비에 대한 인가절차	InformationSecurityFacilityAuthorization
			기밀서약	ConfidentialityAgreement

〔표 10〕 ISMS 통제항목 코드

	대분류	대분류코드	통제항목	통제항목코드 (통제대상,행위)
1	정보보호정책	SecurityPolicy	정책의 승인	SecurityPolicyApproval
			정책의 공표	SecurityPolicyPublish
			상위 정책과의 일관성	SecurityPolicyConsistencyManagement
			정책 문서의 유형	SecurityPolicyProcedureManagement
			주기적 검토	SecurityPolicyReview

〔표 11〕 PCI DSS 통제항목 코드

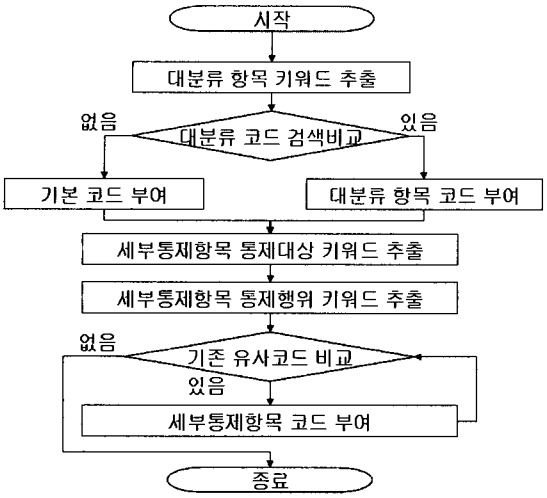
	대분류	대분류코드	통제항목	통제항목코드 (통제대상,행위)
1	데이터보호를 위한 침입차단시스템 설치 및 유지관리	Communication Operation	모든 외부네트워크 접속 및 침입차단시스템 구성 정보 변경시 공식적인 승인 하에 변경 및 테스트	NetworkControl NetworkConnectionControl ChangeManagement
			카드소유자 정보와 연결되 모든 네트워크에 대한 현황을 나타내는 네트워크 구성도	NetworkControl NetworkServiceControlManagement
			각각의 인터넷 접속 및 DMZ 구간과 내부 네트워크 구간 사이의 침입차단 시스템에 대한 요구사항	NetworkControl NetworkRoutingControl NetworkConnectionControl
			네트워크 구성 요소의 체계적 관리를 위한 그룹 역할 및 책임 정의	NetworkControl AccessControlPolicy DocumentedOperationProcedureAuthority
			업무에 필요한 서비스 및 포트 목록 문서화	NetworkControl NetworkServiceUsePolicy RemoteConfigurationPortProtect

중요한 요소가 통제대상과 통제행위이다. 이 2가지 키워드에 해당되는 영문 단어를 식별 후 결합하는 방안을 이용하였다. 키워드 2가지를 기준으로 ISO 27001과 ISMS의 세부 통제항목을 통제대상과 통제행위를 혼합하여 코드화하였다. 그래서 전체 167개를 코드화 하였다. PCI DSS 세부 통제항목의 내용을 통제대상과 통제행위로 키워드를 구분하여 사전에 정의한 167개 코드 중 유사한 다수개의 코드를 각각의 PCI DSS 세부통제항목에 할당하였다.

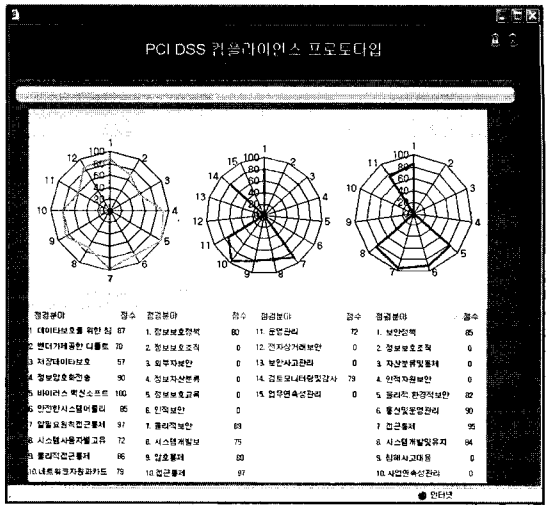
대분류는 [표 9]와 같이 코드화 한다. 먼저 ISO 27001과 ISMS의 세부 점검항목별로 코드화 하고 유사한 내용은 동일한 코드를 부여하였다. 그 다음 PCI DSS 의 세부 점검항 내용을 보면서 사전에 정의한 코드로 할당 하였다. 이때 1 : N 의 관계를 가질 수 있도록 했다. 즉, PCI DSS 의 점검항목은 하나 이상의 코드를 할당 받을 수 있다. 다음과 세부 통제항목 코드화의 일부이다. 1.1.1 항목 보안정책서의 경우, 통제내용을 보면 정보보호정책서가 작성되고 승인권자의 승인을 받았는가가 주요 골자이다. 이 내용의 핵심이 되는 통제대상과 통제행위를 식별해보면 '정보보호정책서'와 '승인' 이다. 이를 각각 영문화 코드를 부여하면Security Policy 와 Approval 이 되고 이를 연결하여 Security PolicyApproval 로 코드화 하였다. 이 항목의 코드는 아래 ISMS 의 1.1.1 의 의미와 유사하며 동일 코드를 부여하였다. 또한 PCI DSS에서 12번째 분류인 정보보호 정책 유지 부분의 12.3.1 명확한 관리자의 승인에 동일한 SecurityPolicyApproval 값을 부여하였다.

4.3 통제코드 할당 방법

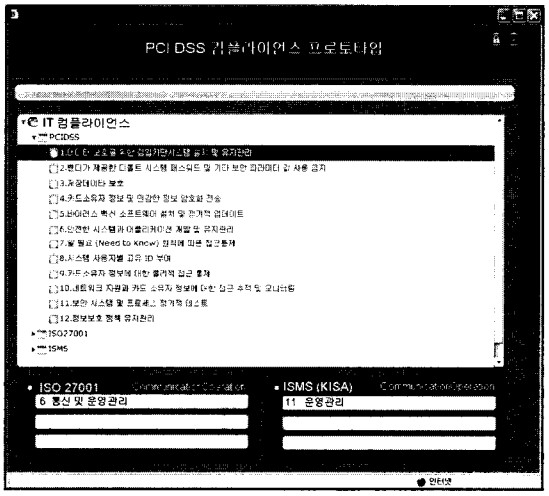
4.2에서 ISO 27001과 ISMS의 세부 통제항목별 코드를 부여하였고 이를 기반으로 하여 PCI DSS 통제항목에 유사한 통제항목 코드를 부여하였다. 예를 들어 PCI DSS 1.1.1 항목의 세부 통제 내용이 "모든 외부네트워크 접속 및 침입차단시스템 구성정보 변경시 공식적인 승인하에 변경 및 테스트" 이다. 이 용어의 통제대상은 네트워크(Network) 이고 통제행위는 공식적인 승인(Management) 이다. 이를 유사한 코드에서 찾아보



〔그림 3〕 PCI DSS 통제항목 코드 할당과정



〔그림 4〕 PCI DSS 컴플라이언스 프로토타입 화면



〔그림 5〕 PCI DSS 컴플라이언스 코드 매핑 화면

면 NetworkControl, NetworkConnectionControl, Change Management 정도로 할당 할 수 있다.

세부 통제항목의 코드만으로 물리적 부분과 기술적 부분, 관리적 부분들이 혼동 될 수 있어 대분류의 코드를 조합하여 세부 통제항목 코드를 할당 하는 방법을 이용하였다. PCI DSS 1.1.1 의 대분류는 "1 데이터 보호를 위한 침입차단 시스템 설치 및 유지관리" 로서 대분류 코드는 "CommunicationOperation" 으로 분류하였다. 즉 PCI DSS 1.1.1 의 대분류코드 "Communication Operation" 과 통제항목코드 "NetworkControl", "Network ConnectionControl", "Change Management" 를 다른 IT 컴플라이언스에서 찾아서 해당 항목의 준수여부를 평가하여 중복 준수 노력을 감소시킬 수 있다. 코드 부여 과정을 흐름도로 작성해 보면 [그림 3]과 같다.

V. 프로토타입 구현 및 평가

4장에서 정의한 통제항목 코드 방법을 활용하여 다중의 IT 컴플라이언스간의 준수 현황을 확인할 수 있는 프로토타입을 설계 개발하였다. 이로서 PCI DSS 통제항목을 기타 정보보호관리체계나 IT 컴플라이언스와 중복 노력 없이 비교 분석이 가능하며 상시적으로 정보보호 통제항목들을 관리할 수 있다. [그림 4]는 PCI DSS 통제항목에 대한 결과를 사전에 정의한 매핑 코드에 의해서 ISO 27001 과 ISMS 기준에 적용하여 나타난 결과를 보여주고 있다. [그림 4]에서 의미하는 것은 점수가 높고 낮음의 의미가 아니라 유사한 통제항목에 체계화된 코드를 부여하여 상호간의 연관성을 부여하고 이를 자동 매핑함으로서 PCI DSS 준수활동만으로도 ISO 27001과 ISMS의 활동을 자동화 할 수 있음을 의미한다.

또한 역으로도 가능하다. 기존에 준수하고 관리하고 있는 정보보호관리체계를 이 코드화 체계와 통합한다면 기존의 활동결과를 그대로 PCI DSS 에 적용할 수 있다. [그림 4]에서 보면 PCI DSS 의 분류들이 대부분 통신 및 운영관리, 접근통제, 시스템 개발 및 유지관리 물리적 보안 부분에 매핑이 되어 ISO 27001과 ISMS로 자동 변환해 보면 특정 분류부분으로 몰리는 현상이 발생하였다. [그림 5]는 PCI DSS와 ISO 27001, ISMS 대분류 코드간의 관계를 할당하는 템플릿이다.

Ⅵ. 결론 및 향후 연구 방향

6.1 결 론

신용카드 정보를 노린 해킹이나 카드 분실 도난 사고가 증가하면서 고객정보를 보호하고 보안사고로 인한 카드사, 가맹점, 서비스 제공업체 등의 잠재적 손실을 최소화하기 위해서 PCI DSS 라는 카드 업계 정보보호 표준 규격이 제정되었다. 이규정은 고객의 데이터를 저장, 처리, 전송하는 카드 가맹점 서비스 사업자라면 모두 준수해야 하고 일정 거래 규모 이상의 처리업체와 가맹점은 의무적으로 준수해야 한다. 대상 업체는 상시적으로 표준 규격을 준수하고 있음을 증명하기 위해 자가진단서와 분기별 네트워크 취약점 점검 등을 이행하고 결과를 제출해야 한다. 이를 만족하지 못할 경우 벌금과 카드결제 거부 등의 제재가 있다.

PCI DSS 가 규정하는 통제 분류는 네트워크 침입차단시스템 구축관리, 개인 신용카드 정보 암호화, 업데이트된 바이러스 백신 소프트웨어 사용, 정보접속 권한 부여, 네트워크 신용카드 정보 접속 모니터링 등이다. 즉, 많은 기업에서 정보보호활동을 하고 있고 그 외 기타 정보보호관리체계와 중복되는 부분들이 많이 있다.

그러나 PCI DSS 준수를 위한 가이드라인이나 교육, 시스템 등이 국내에는 미흡하다. 이미 정보보호관리체계 등의 인증 및 정보보호감사 시스템을 운영하고 있음에도 이를 어떻게 PCI DSS 와 매핑해서 활용하는지 방법이 없다. 그래서 PCI DSS 준수를 위한 준비, 그 외 정보보호활동 및 인증을 위한 준비 등을 중복되어 작업을 수행할 수밖에 없다.

본 논문에서는 이를 해결하고 중복노력 없이 상시적으로 PCI DSS 준수를 위한 방안을 연구하였다. 세부통제항목을 통제 대상과 통제 행위로 구분하여 코드화하였고 이를 유사한 통제항목에 매핑하여 통제항목 결과를 공유할 수 있도록 하였다. 또한 이 통제항목 코드를 활용한 프로토타입을 구현함으로서 활용가능성을 제시하였다. 여기서 제시한 통제항목 코드화 방안이 PCI DSS 컴플라이언스 준수를 위한 자동화 시스템 개발, 다중 IT 컴플라이언스와의 통합 준수 구현에 활용될 수 있는 기반이 되었으면 한다.

6.2 향후 연구방향

세계적으로 노동, 안전, 소비자 보호, 개인정보보호 등 다양한 분야에 걸쳐 15,000 여개의 컴플라이언스들이 존재하고 있으며 지속적으로 증가하고 있다. 각국의 컴플라이언스들은 국가 간 비즈니스 환경에서 새로운 진입장벽이 되고 있으며, 미준수시 기업들에게 심각한 경제적 손실과 인지도 하락 및 비즈니스 상실과 같은 위험에 처해진다. 정보보호연구기관에서는 IT 컴플라이언스 이행을 효과적으로 할 수 있는 방안과 시스템을 제시해주어야 한다. 일본의 경우 민관의 유기적인 협조체제가 구축되어 최근에는 신용카드사는 물론 가맹점 서비스업체 등이 ISMS 는 물론 PCI DSS 인증 및 준수가 꾸준히 늘고 있다고 한다. 이는 일본 기업표준 정보보호관리체계인 ISMS 인증을 PCI DSS 인증시 중복검사를 면제해주고 두 가지 인증을 함께 도입하도록 권고하기 있기 때문이다.

본 논문에서 제시한 세부 통제항목 코드화 방안을 활용하여 국내에서도 민관이 유기적으로 협조하여 PCI DSS 이행을 도와줄 수 있는 제도와 시스템이 개발되어야 할 것이며 이에 대한 연구가 필요하다.

참고문헌

[1] 김두규, "소프트웨어정책동향 - 정보시스템 관련규제와 IT Compliance 시장의 이해", 한국소프트웨어진흥원, 2005.

[2] "소프트웨어시장분석 보고서 - 정보보호 규제 강화와 관련 시스템 시장 동향", 한국소프트웨어진흥원, 2008. 2.

[3] 임종인, "기업의 IT 컴플라이언스 리스크 관점에서의 정보보호", ISUC2008 발표자료, 2008. 5.

[4] "정보보호관리체계인증 ISMS 홍보자료", 한국정보보호진흥원.

[5] "Hacker Hits up to 8M credit cards", CNN news, 2003. 2.

[6] Brodkin, Jon. "TJX breach may spur greater adoption of credit card security standards", Network World, 2007. 3.

[7] Dave Shackleford, "A SANS Whitepaper - Leveraging Event and Log Data for Security and Compliance", 2008. 4.

[8] Dave Shackleford, "A SANS Whitepaper - Using Security Information Management Systems for PCI Compliance", 2007. 6.

[9] ISO/IEC "ISO/IEC FDIS 27001 : 2005(E) INTER NATIONAL STANDARD FINAL DRAFT", ISO/IEC, 2005. 8.

[10] PCI Security Standards council Wet site https://www.pcisecuritystandards.org/

[11] "PCI DSS 보안감사에서부터 솔루션에 대한 모든 것", A3Security 세미나 자료, 2008. 7.

[12] "PCI 카드 보안 표준", PCISSC, 2006. 9. https://www.pcisecuritystandards.org/pdfs/k_pci_dss_v_1-1.pdf

[13] Robert Rowlingson and Richard Windsborrow, "A comparison of the Payment Card Industry data security standard with ISO17799", Computer Fraud & Security, pp.16-19, 2006. 3.

[14] Tony Bradley, "PCI Compliance - Understand and Implement Effective PCI Data Security Standard Compliance", Syngress, 2007.

〈著者紹介〉

최 대 수 (Dae-Soo Choi)

1997년 2월 : 호원대학교 전자계산학과 학사

1999년 2월 : 수원대학교 일반대학원 전자계산학과 석사

2008년 현재 : 전남대학교 일반대학원 정보보호협동과정 박사과정

2002년 4월~현재 : (주)이글루시큐리티 보안연구소 선임연구원

<관심분야> IT규제준수, IT종합위험관리시스템, IT융합시스템, 침입추론