The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 4, pp.193-201, Aug. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.4.193
JIIBC 2017-4-25

금융회사 대형 IT프로젝트 추진 시 외주직원에 대한 보안정책 적용 사례 연구

A Case Study on the Application of Security Policy for Outsourcing Personnel in case of Large-Scale Financial IT Projects

손병준*, 김인석*

Byoung-jun Son*, In-seok Kim*

요 약 금융회사에서는 내부자에 의한 개인정보유출 방지 및 내부통제 강화를 위하여 출력물 보안, 인터넷 망 분리시스템, 고객정보분리보관, 개인정보 암호화, 개인정보검색, DLP(Data Loss Prevention), 출력물보안, 개인정보모니터링 시스템 등의 보안 솔루션을 도입 운영하고 있다. 아울러 금융회사는 금융 소비채널의 변화 및 금융상품의 패러다임 변화를 겪으며 무한경쟁시대로 진입하고 있다. 금융회사가 보유한 고객정보의 보안에 대한 필요성이 높아지고 있다. '2014년 1월 발생한 카드 3사 대량고객정보 유출 사고는 외주 직원 한 명이 주요 카드사의 고객 개인정보를 탈취하여 대출광고업자와 대출모집인에게 팔아 넘겨졌던 사례이다. 대형 보안사고가 발생한지 3년여의 시간이 흐른 지금도 IT 외주인력의 보안 위협은 여전하다. 정부 및 감독기관은 '금융분야 개인정보 유출 재발방지 종합대책' 이행 점검 및 개인정보 유출에 대한 금융회사 제재수준 강화를 진행하고 있다. 본 논문은 금융회사 대형 IT프로젝트 추진 시에 외주직원에 대한 보안정책 적용 사례 분석을 통해 IT프로젝트 성공 및 효율적인 보안 준수를 위한 정책 설정을 연구함으로서 대형 IT프로젝트의 성공과 외주인력의 보안사고 위험도를 최소화할 수 있는 방안을 사례를 통해 제시해 보고자 한다.

주제어 : 개인정보보호, 보안정책, 대형 IT프로젝트

Abstract Financial firms strengthen to protect personal information from the leakage, introducing various security solutions such as print output security, internet network Isolation system, isolationg strorage of customer information, encrypting personal information, personal information detecting system, data loss prevention, personal information monitoring system, and so on. Financial companies are also entering the era of cutthroat competition due to accept of the new channels and the paradigm shift of financial instruments. Accordingly, The needs for security for customer information held by financial firms are keep growing. The large security accidents from the three card companies on January 2014 were happened, the case in which one of the outsourcing personnel seized customer personal information from the system of the thress card companies and sold them illegally to a loan publisher and lender. Three years after the large security accidents had been passed, nevertheless the security threat of the IT outsourcing workforce still exists. The governments including the regulatory agency realted to the financail firms are conducting a review efforts to prevent the leakage of personal information as well as strengthening the extent of the sanction. Through the analysis on the application of security policy for outsourcing personnel in case of large-scale Financial IT projects and the case study of appropriate security policies for security compliance, the theis is proposing a solution for both successfully completing large-scale financial IT Project and so far as possible minizing the risk from the security accidents by the outsouring personnel.

Key Word : Customer personal information, Security policy, Large-Scale IT project

*정회원, 고려대학교 정보보호대학원,
접수일자: 2017년 7월 20일, 수정완료: 2017년 8월 2일
게재확정일자: 2017년 8월 11일

Received: 20 July, 2017 / Revised: 2 August, 2017 /
Accepted: 11 August, 2017
*Corresponding Author: byoungjunson@gmail.com
Center for Information Security Technologies(CIST), Korea University, Korea

I. 서 론

개인정보유출사고는 최근에도 지속적으로 증가하고 있으며, 유출된 개인정보를 이용한 다양한 형태의 보안 사고가 발생하고 있다. 2014년 1월 카드 3사 1억여건의 대량 고객정보 유출사고에[1] 이어 2017년 3월에는 JT친애저축은행 고객정보 28만건 유출 사고[2] 등 크고 작은 정보유출 사건이 발생하고 있다. '2014년 1월 발생한 카드 3사 대량고객정보 유출 사고는 외주 직원 한 명이 주요 카드사의 고객 개인정보를 탈취하여 대출광고업자와 대출모집인에게 팔아 넘겨졌던 사례이다. 대형 보안사고가 발생한지 3년여의 시간이 흐른 지금도 IT 외주인력의 보안 위협은 여전하다. 정부 및 감독기관은 '금융분야 개인정보 유출 재발방지 종합대책' 이행 점검 및 개인정보 유출에 대한 금융회사 제재수준 강화를 진행하고 있다.

금융회사에서는 내부자에 의한 개인정보유출 방지 및 내부통제 강화를 위하여 출력물 보안, 인터넷 망 분리시스템, 고객정보분리보관, 개인정보 암호화, 개인정보검색, DLP(Data Loss Prevention), 개인정보모니터링 시스템 등의 보안 솔루션을 도입 운영하고 있다. 아울러 금융회사는 금융 소비채널의 변화 및 금융상품의 패러다임 변화를 겪으며 무한경쟁시대로 진입하고 있다.

본 논문은 금융회사 대형 IT프로젝트 추진 시에 외주직원의 행내 시스템 접근 등에 대한 보안 위협에 대하여 보안정책 적용 사례 분석을 통해 IT프로젝트 성공 및 효율적인 보안 준수를 위한 정책 설정을 연구함으로서 대형 IT프로젝트의 성공과 외주인력의 보안사고 위험도를 최소화할 수 있는 방안을 사례를 통해 제시해 보고자 한다.

논문의 구성은 총 5장으로 구성되었다. 2장에서는 본 연구와 관련한 외주인력 보안과 정보 접근 통제 정책의 중요성 및 H사 정책 사례에 대하여 살펴보았다. 다음으로 3장에서는 금융회사 대형 IT프로젝트 추진 현황 및 성공의 기반이 되는 데이터 정합성 필요성 확보, 외주직원들의 리얼 데이터 접근 필요성에 대해서 살펴 보았으며, 대형IT프로젝트 성공을 위한 보안정책 적용 제안을 제시하였다. 다음으로, 4장에서는 보안정책 적용 제안 내용을 H사 보안 정책 적용하여 효과성을 검증한다. 마지막으로, 5장에서는 본 연구에 대한 결론을 맺고, 향후 연구에 대한 방향을 제시하고자 한다.

II. 관련 연구

1. 외주인력 보안과 정보 접근 통제 정책의 필요성

국가정보원(NIS) 2016년 국가정보보호백서에서 공공기관의 보안 인식이 어떠한지 살펴보았다. 공공기관에서 가장 취약한 정보보호 분야로는 '인적보안'이 50%를 넘기며 압도적 1위를 차지하여 있다.[3]

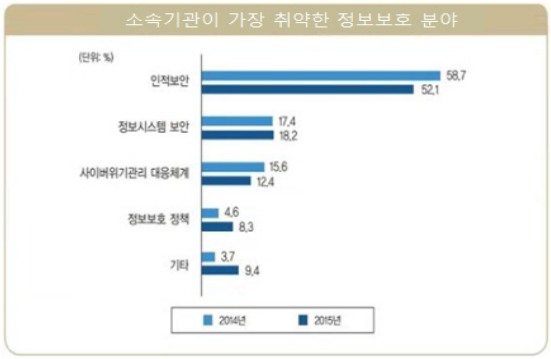


그림 1. 공공기관 소속기관이 가장 취약한 정보보호 분야
Fig. 1. The most vulnerable areas of information security

가장 우려하는 정보보호 위협요인으로는 범죄자 외에 '아웃소싱업체(직원 포함)와 재직 직원'이 꼽혔습니다.[3]

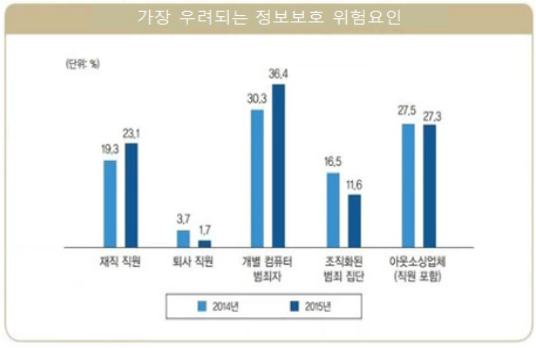


그림 2. 공공기관에서 가장 우려되는 정보보호 위험요인
Fig. 2. The most inportant information protection risks in publiic institutions

백서에서 조사된 위협요인들처럼 실제 개인정보 유출 사례를 살표보면 '2010년 신세계몰 등 25개 업체와 '2012년 7월, '2014년 3월 KT에서 발생한 개인정보 유출은 해

킹을 통하여 발행하였으며, 제재 조치는 과징금, 과태료, 시정명령 수준으로 징계가 내려졌습니다. '2011년 8월 삼성카드에서 발생한 사고는 내부유출에 의한 것으로 기관주의 및 유출직원 면직의 징계를 받았습니다. '2014년 1월 카드 3사에서 발생한 사고는 외주직원에 의한 고객정보유출로 8,700만건의 고객정보가 유출된 사고로 기관 3개월 영업정지 및 범죄 가담자 13명 실형을 선고 받았으며, 1심 판결에서 카드 3사에 벌금 부과 및 피해고객에 대한 손해배상 금액 1인당 10만원이 부과되는 판결이 내려졌습니다.

표 1. 카드3사 정보유출 피해상황[4]
Table 1. Three card company information leakage damage situation

구 분		AA	BA	CA
유출건수		5,41X만건	2,87X만건	2,69X만건
영업수익 손실(추정)		44X억 7천만원	33X억원	28X억 5천만원
소송자수		108,43X명	69,84X명	70,33X명
임직원 제재조치	임원	해임권고 상당 1명 주의적정고 2명 주의 상당 1명	주의적 경고 2명	해임권고 상당 1명, 문책 경고 1명, 주의적정고 상당 2명
	직원	면직 상당 1명, 정직9월 1명, 감봉 9월 6명, 견책 4명, 주의1명, 퇴직자 위본사유통지 2명, 기타	정직 1명, 정직상당 1명, 감봉 2명, 감봉상당2명, 기타	면직 상당 1명, 정직 9월 4명, 감봉 9월 6명, 감봉 9월 상당 2명, 견책 3명, 견책 상당 1명, 기타
기타 제재조치		업무일부정지 3개월 및 과태료 60억원 부과	업무일부정지 3개월 및 과태료 60억원 부과	업무일부정지 3개월 및 과태료 60억원 부과
카드재발급 비용		약 68억원 (약 223만건)	약 70억원 (약 19X만건)	약 76억원 (약 16X만건)
고객통보 우편발송		약 101억원	-	약 18억원
콜센터 추가운영		약 11억원	약 39억원	약 14억원

1심 판결의 의미는 금융기관의 주의의무 기준을 높게 설정하였으며, 유출된 정보가 제3자에게 열람되거나 열람될 가능성이 큰 경우에는 구체적인 손해가 발생하지 않더라도 위자료 배상책임을 인정하였다고 볼 수 있겠습니다.

금융기관 입장에서 볼 때 고객정보 유출 사고 발생으로 인해 손해배상 청구, 고객 이탈, 감독기관 검사를 통하여 배상금지급, 주가하락, 대외 이미지 추락으로 이어졌으며, 이로 인하여 추가된 규정으로 고객정보 유출 책임을 CEO에게 묻는 등 금융회사 제재 수준을 강화하는 추세입니다.

2. 외주인력 보안과 관련된 주요 법률 및 주요 통제 방안

외주인력 보안과 관련된 주요법률은 "전자금융감독규정", "신용정보의 이용 및 보호에 관한 법률", "개인정보보호법"에서 명확하게 규정하고 있다.

[전자금융감독규정][5]

제13조 (전산자료 보호대책)

① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.

"4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것"

"10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)"

제60조 (외주주문등에 대한 기준)

① 금융회사 또는 전자금융 업자는 전자금융 거래를 위한 외부주문 등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

"1. 외부주문등에 의한 정보처리시스템의 개발 업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영"

"4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립"

"14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시"

[신용정보의 이용 및 보호에 관한 법률][6]

제19조((신용정보전산시스템의 안전보호)

① 신용정보회사등은 신용정보 전산시스템에 대한 제3자의 불법적인 접근, 입력된 정보의 변경,훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적, 물리적, 관리적 보안대책을 수립 시행하여야 한다.

[개인정보보호법][7]

제29조(안전조치 의무)

개인정보처리자는 개인정보가 분실, 도난, 유출, 위조,

변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적, 관리적 및 물리적 조치를 하여야 한다.

위의 법률에 의거 외주인력에 대한 주요 통제 방안은 아래와 같다.

표 2. 주요 보안통제 방안
Table 2. Major security controls

구분	주요 목적	주요 통제 방안	
관리적 통제	실수나 부주의 예방, 정보보호 의식 제고	보안 정책, 직원 교육, 캠페인, 각서, 계약서, 포상/징계	
물리적 통제	도난 예방, 비인가 IT기기 반입 및 이를 통한 내부 자료 유출 방지	출입 인원 통제, IT기기 반/출입 통제, 개인 휴대품 반/출입 통제, PC 시건장치, 하드디스크 보호 테이프 등	
기술적 통제	산업 스파이, 인터넷이나 내부자의 해킹, 내부직원 및 방문객 등의 실수나 부주의로 인한 자료 유출 예방	단말	PC보안, 보안 USB, NAC, IP 관리를, 백신, HDD/Tape 데이터 영구 삭제, Thin Client
		네트워크	방화벽, 인터넷 모니터링 시스템, 내부망과 인터넷망 분리, ADSL 및 무선망 접근 통제, 무선 암호/인증 시스템, 무선 침입 방지시스템(WIPS)
		응용 프로그램	업무 서비스 접근 통제와 문서 보안
		서버 시스템	시스템 접근통제와 DB 암호화
		정보보안 위험관리	모의해킹/취약점 점검, 소스코드 보안, 위험 평가

3. H사 외주인력 관리적, 물리적, 기술적 보안 정책 사례

앞 절의 관련 법률에 적합하도록 제시되는 외주 직원에 대한 주요 통제 방안을 H사의 사례를 통하여 살펴보도록 하겠습니다.

외주직원들에 대한 관리적/물리적 통제를 외주인력 투입 및 철수 프로세스에 따라 정리하였습니다.

계약시 필요사항, 보안서류 징구, 외주직원에 대한 보안정책 적용, 보안교육/점검, 철수 시 보안정책 해제(권한 회수) 및 정보삭제/철수 승인 순으로 진행하는 것으로 각종 법률에 위반되지 않게 적정 보안 정책이 적용되어 운영되고 있었습니다.

외주직원에 대한 기술적 통제는 가상화(VDI) 기반의 보안통제를 사용하고 있었습니다. 아울러 네트워크, 단말, 서버 및 DB 접근제어 등의 통제 영역별 통제를 적절하게 유지 관리하고 있었습니다.

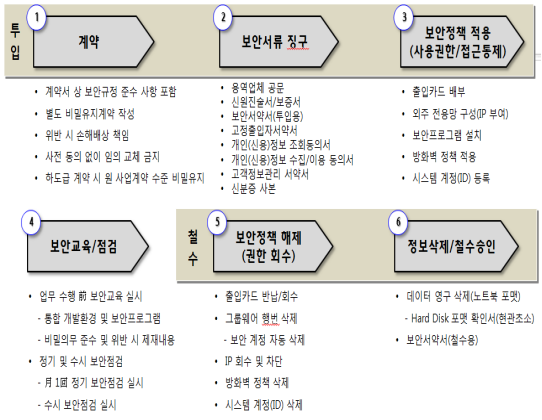
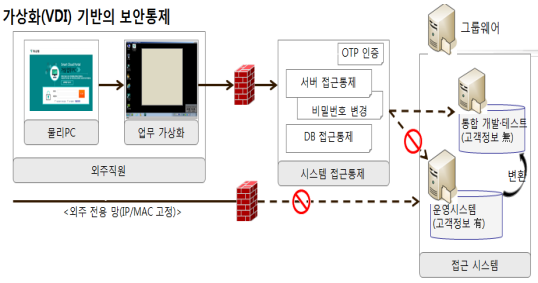


그림 3. 외주직원 투입 및 철수 프로세스
Fig. 3. Outsourcer input and withdrawal process



통제영역		통제내용
네트워크		외주 전용 망(NAC통제), 서버/DB 직접접속 금지, 인터넷 접속 금지, 이메일 사용 금지, 무선통신망 사용 금지
단말	물리PC	PC內 파일저장 금지, 가상화 프로그램 설치(물리PC 접근차단), USB 차단
	가상화	필수보안프로그램 강제 설치, USB 차단
접근통제	서버	서버 접근통제시스템 경유 접속, M-OTP 추가 인증, 공용계정 비밀번호 변경
	DB	DB 접근통제시스템 경유 접속, M-OTP 추가 인증
시스템		고객정보 無 또는 變換, 서버 개별 계정(ID) 부여, 서버보안(SecureOS)

※ 필수 보안프로그램 : PC보안, 문서보안(DRM), 개인정보지킴이(DLP), 출력물보안, 백신, NAC

그림 4. 기술적 통제 방안
Fig. 4. Technical control measures

III. 금융회사 대형 IT프로젝트 성공을 위한 보안정책 적용 제안

본 장에서는 금융회사 대형 IT프로젝트 추진현황을 살펴보고 대형 IT 프로젝트 성공의 기반이 되는 데이터 정합성 확보 방안 및 외주직원들의 리얼 데이터 접근 필요성에 대하여 살펴보고, IT프로젝트 성공과 외주직원들의 정보유출 방지를 위한 보안정책 적용에 대한 제안을 하고자 합니다.

1. 금융회사 대형 IT프로젝트 추진 현황

2011년 이후 6개 시중은행은 차세대시스템 구축, 농협은 중조분리 프로젝트, KEB하나은행은 구)하나은행과 외환은행간 IT통합 프로젝트를 막대한 예산을 투입하여 추진하였습니다.

'2014년 카드3사 고객 정보 유출에 따른 보안정책 강화로 인하여 프로젝트 추진과 보안 정책 적용에 대한 CIO와 CISO간의 대립될 수 있는 사안들이 많이 발생하여 이에 대한 합리적인 대안을 본장에서 제시코자 합니다.

표 3. 금융기관 대형 IT프로젝트 추진 현황
Table 3. Financial institution large IT project promotion status

기관명	프로젝트 기간	소요예산	비 고
IBM기업은행 POST 차세대	2012. 10 ~ 2014.10	2,500억	
경남은행 차세대	2012. 12 ~ 2014. 10	400억	
전북은행 차세대	2011.12 ~ 2013. 09	400억	
광주은행 차세대	2015. 07 ~ 2016. 11	500억	
농협 중조분리	2015. 02 ~ 2017. 02	2,500억	
KEB하나은행 IT통합	2015. 09 ~ 2016. 06	1,880억	
우리은행 차세대	2016. 02 ~ 2018. 02(예정)	3,000억	진행중
KDB산업은행 차세대	2017. 03 ~ 2019. 05(예정)	2,100억	진행중

2. 대형 IT프로젝트 성공 기반이 되는 데이터 정합성 확보

금융회사 대형 IT프로젝트의 성공을 위해서는 AS-IS 시스템의 데이터를 TO-BE시스템으로 정확히 새로운 시스템에 맞게 정확하게 이행을 하여야 프로젝트 성공을 할 수 있으며, 만일 데이터 이행에 문제가 발생 시에는 고객 민원 및 금융산업 전반에 걸쳐 많은 문제점을 야기시킬 수 있습니다. 이에 금융회사들은 대형 IT프로젝트 추진 시에 외부 보안 규정을 준수하여야 하며, 데이터 정합성 확보 역시 담보하여야 하는 어려운 상황에 직면하고 있습니다. 통상 대형IT프로젝트 추진 시 데이터 이행의 수행은 해당 금융기관 직원이 직접 수행하지 않고 전문적인 외주IT직원들을 이행담당으로 지정하여 운영하는 것이 일반적인 과정입니다. 이에 성공적인 프로젝트 수행을 위한 조직은 데이터 이행팀, 업무팀, 인프라팀으로 구분하여 각 팀별 역할을 수행합니다.

데이터이행팀은 데이터 이행 개발 및 테스트, 데이터 검증/이행 작업을 주로 수행하며, 은행의 업무팀은 매핑정의서 작성 및 데이터 논리검증, 데이터 기반 프로그램 테스트를 수행합니다. 인프라팀은 최적의 이행 환경구성을 지원합니다.

그림 5. 데이터 이행 관련 조직
Fig. 5. Data migration related clause

데이터 이행 검증 절차는 추출검증, 매핑적재검증, 업무논리검증 3단계와 업무테스트 검증으로 데이터 이행 검증을 수행합니다.

그림 6. 데이터 이행 검증 절차
Fig. 6. Data migration verification procedure

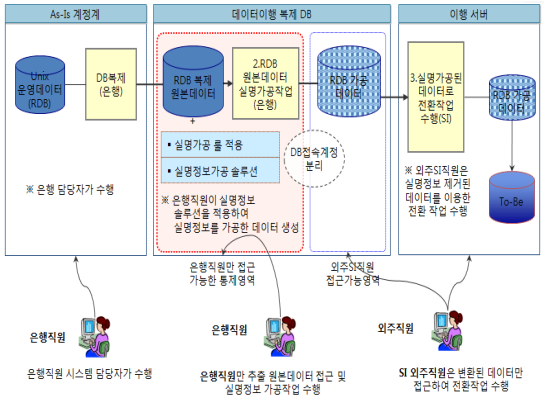


그림 7. 원칙적인 고객 정보 보안절차
Fig. 7. Principle Customer Information Security Procedures for Data Migration

아울러 전자금융감독규정 등에 따라 외주 IT직원들은 실명 가공된 데이터만을 가지고 데이터 전환작업을 수행하여야만 합니다. 운영 시스템의 실제 데이터는 은행 담당자가 추출 및 실명정보 가공 작업을 수행하며, 외주IT 직원들은 가공된 데이터를 가지고 데이터 변환작업을 수행토록 각 종 보안 정책은 규정하고 있습니다.

3. 외주직원들의 리얼 데이터 접근 필요성

개인정보보호 분야 일반 법인 개인정보보호법('11)과 금융관련 법령인 신용정보법('97), 금융실명법('97) 및 전자금융거래법('97) 등을 통해 개인정보보호 관련 제도의 적용을 받고 있으며, 전자금융감독규정을 통해 외주 IT 인력에 대한 규정으로 전산자료 보호대책, 외주주문 등에 대한 기준 등을 제시하고 있습니다. 하지만 금융회사 대형 IT프로젝트의 성공을 위해서는 부득이하게 외주 직원들의 리얼 데이터 접근이 허용되어 져야 되는 필요성이 존재하며, 이를 기술코자 합니다.

첫째, 대형IT프로젝트에서 데이터 전환 작업은 반복적인 훈련으로 안정성 확보가 필수입니다. 즉 프로젝트 오픈일과 동일한 프로세스를 구현하여야 성공을 담보할 수 있습니다. 앞 절에서 기술하였 듯이 테스트 수행 시 적용하였던 실명가공하여 데이터 전환 작업을 수행할 경우와 실제 당일 데이터 전환 작업절차가 다를 경우 프로젝트 실패 가능성은 가중될 수 있습니다.

둘째, 앞 절에서 기술하였듯이 데이터 부문(업무팀)과 데이터 처리 부분(데이터 이행팀)의 전문성을 극대화하여 프로젝트 리스크를 최소화 할 필요성입니다. 데이터 처리 부분은 시계적으로 대량의 데이터를 가공하는 작업으로 단순 반복 작업인바, 은행 직원들은 전문성이 필요한 데이터 부문에 집중하고, 데이터 처리 부분은 외주직원이 수행할 수 밖에 없습니다. 대형 IT프로젝트 수행 시 은행 직원이 절대적으로 부족한 것이 현실입니다.

셋째, 리얼 데이터를 활용하여 조직 전체 직원 대상 테스트가 필요합니다. 대국민에 대한 안전한 전자금융서비스 제공을 위해 조직 전체 직원들을 활용한 데이터 검증 테스트는 절대적으로 필요한 작업으로 모든 금융기관이 프로젝트 오픈전에 최소 3~4회 정도 수행하는 절차입니다.

마지막으로 촉박한 이행 시간 및 오류데이터에 대한 신속한 확인 및 조치입니다. 대형 IT프로젝트의 경우 3연휴를 활용하여 프로젝트를 오픈합니다. 대형 금융기관일수록 데이터 량이 방대하여 해당 기간동안 데이터 이행 작업, 기능 및 데이터 검증 작업에 소요되는 시간이 부족한 것이 일반적이며, 부득이 한 경우 ROLL-BACK 절차까지 감안하여 이행계획을 수립하여야 하는 바, 데이터 이행 작업을 최대한 단축하기 위한 노력이 필요합니다.

2. 보안정책 적용 제안

금융회사 대형 IT프로젝트의 성공을 위하면서 적절한 수준의 보안 통제를 수행하는 몇가지 방안에 대하여 제안하고자 합니다.

첫째, 대형 IT 프로젝트 초창기에 외주 직원들에 대한 보안정책을 CIO 및 CISO가 협의하여 대형 IT프로젝트 예외 사항에 대한 정의가 필요하며, 필요 시 "비조치의견서 요청서" 등을 활용하여 사전에 감독기관의 승인을 받아는 것 필요합니다. 예로 "전자금융감독규정 제13조(전산자료 보호대책) 10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)" 준수할 수 없는 특수한 상황이 대형IT프로젝트에서는 발생합니다. 이를 프로젝트 초창기에 정리하여야 원활한 프로젝트가 추진될 수 있습니다.

둘째, TO_BE 리얼 시스템은 현재 운영시스템과 동일한 수준의 보안 정책이 적용되어져야 합니다. TO_BE 리얼 시스템에는 현재 운영시스템에 있는 고객정보가 그대로 반영되어 있는 시스템입니다.

셋째, 대형 IT프로젝트에 맞는 추가 보안 정책 적용으로 안정성을 강화하는 것입니다. 예로 외주직원 역할에 따른 등급별 접근 권한 통제, 추가적인 기술적 통제 방안 마련, 외주 직원에 대하여 통상 반기 주기로 보안점검을 실시 하던 것을 프로젝트 기간내에 월 1회 정기 점검을 실시하고, 불시에 비정기적으로 보안 점검을 실시하며, 점검결과 위반자에 대하여는 제재할 수 있는 방안을 마련하는 등 강화된 보안 정책을 적용하는 방안입니다.[8]

제가 본 논문에서 제시되는 방안은 H은행 IT통합 프로젝트를 성공적으로 완성할 수 있었던 보안 정책으로 제4장 적용사례에서 구체적으로 제시코자 합니다.

IV. 적용사례

1. H은행 IT통합 프로젝트 개요

2015년 9월 1일 구)H은행과 구)K은행간 법인통합은 이뤄졌지만, IT통합은 완료되지 않아 진정한 의미의 통합을 위하여 2015년 9월부터 2016년 6월까지 IT통합 프로젝트를 추진하였습니다. 사전 컨설팅을 통하여 총 123개 업무중 리테일사업 및 PB사업에 강점이 있는 수신시스템, 여신규모 및 Risk 관리를 고려한 여신 시스템 등 79개 업무는 H은행 시스템을 Base 시스템으로 선정하였으며, 국내외 독보적인 시장 지배력과 글로벌 경쟁력을 보유한 외환업무, 국외 결제업무, 외환 전산망 등 30개 업무는 K은행 시스템을 Base 시스템으로 선정하였습니다.

Base 시스템으로 선정된 K은행의 외국환·수출입업무 등 30개 시스템은 사용자가 직접 사용하는 UI(화면 및 사용자 Interface)부터 상품, 규정, 프로세스 등 모든 Business 모델을 K은행 기준으로 통합 작업을 수행하게 되는 프로젝트로 통합 H은행 IT 자체 인력 주도로 진행하였으며, 부족한 인력은 외부 파트너사 도움으로 추진하였습니다. 예산은 약 1,880억원을 투입하였으며, 통합 H은행 직원 492명, 외주인력 1,116명이 투입되었습니다. 작업 규모만으로 보았을 때 데이터 전환 대상이 되는 테이블 숫자는 은행 계정성 업무만 4,000여개 이상이었으며, 양행 GAP 2,100여개의 개발 작업을 수행하였으며, 데이터 전환 프로그램 개수만 37,535개에 달하는 대규모 프로젝트 였습니다.

IT통합 프로젝트를 위하여 강화된 IT보안 정책의 원칙을 수립하여 운영하였습니다. 첫째, 1,116명의 외주 직원들의 운영시스템 접근 불가. 둘째, 실 고객 정보 조회 불가. 셋째, 인터넷 접속불가. 넷째, 전산 자료 행외 반출 불가로 요약 정리 됩니다. 아울러 보완된 IT보안정책은 외주직원 역할(직무)에 따라 등급별 접근 권한 통제, 기술적 통제 방안 마련, 외주 직원 투입/철수 프로세스 강화, 손해배상 청구 등 보안 정책 위반자에 대한 처리 방안 마련 등에 역점을 두었습니다. 또한 월 1회 정기 보안 점검 및 비정기 수시 점검을 수행하여 만에 하나 있을 보안 사고에 대비하였습니다.

2. H은행 보안정책 주요 내용

'2015년 H은행 관계사인 S카드사와 K카드사 간의 IT 통합프로젝트가 H은행 IT통합 프로젝트 추진 보다 빨리 진행되었다. 2번의 오픈 연기 등을 거쳐 우여곡절 끝에 통합 S카드사는 '2015년 7월에 오픈했으나, 일부 시스템에서 문제가 발견되어 혼란을 겪어야 했다. 손님의 불편은 물론 H 그룹 전체에 있어 대외 신뢰도가 떨어지는 결과를 초래 하였다. 프로젝트 실패의 원인중 하나는 IT 프로젝트 보안정책을 너무 강화함으로 인하여 프로젝트 생산성이 현저히 떨어진 것이 주요 원인으로 꼽혔다.

이에 H은행의 보안정책 첫째는 IT 프로젝트 초창기에 외주 직원들에 대한 보안정책을 CIO 및 CISO가 협의하여 대형 IT프로젝트 예외 사항에 대하여 정책 정의를 하였으며, "비조치의견서 요청서" 등을 활용하여 사전에 감독기관의 승인을 받아 프로젝트의 질을 향상시켰다.

"전자금융감독규정 제13조(전산자료 보호대책) 10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)" 는 규정을 준수할 경우 안전한 전자금융서비스 제공을 위해 사전 정합성 검증이 불가하고, 이행 당일과 동일한 이행 프로세스 구현이 불가하기에 때문이다. 이를 위한 기술적 통제 수단으로 클린룸을 설치하여 예외적으로 선별된 외주직원들이 운영시스템 접근을 허용하였으며, 영업점 테스트 수행 시 통합 H은행 객장내에서 고객정보를 변경하지않은 리얼 데이터를 활용하여 정합성 테스트를 수행하였다. 클린룸에서는 CCTV, CIO까지 출입통제를 하는 등 완벽한 물리적, 관리적, 기술적 통제를 구비하였다.

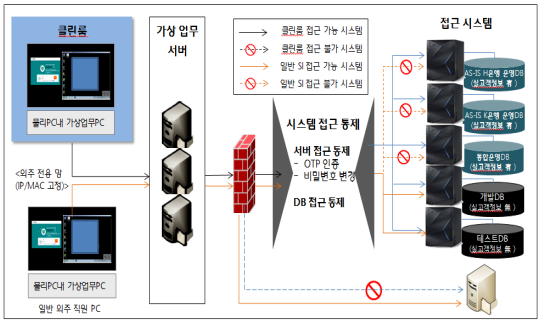


그림 8. H은행 외주직원 기술적 통제
Fig. 8. The Outsourcing employees technical contol of H bank

아울러 개인정보 데이터 변환없이 데이터 전환을 클린룸에서 수행하여 통합 운영DB를 구성하였으며, 데이터전환 개발자이외의 외주직원들이 활용할 테스트 및 개발 DB는 개인정보 데이터 변환 작업을 수행하여 데이터 정합성 향상 및 보안 강화에 중점을 두었다.[9]

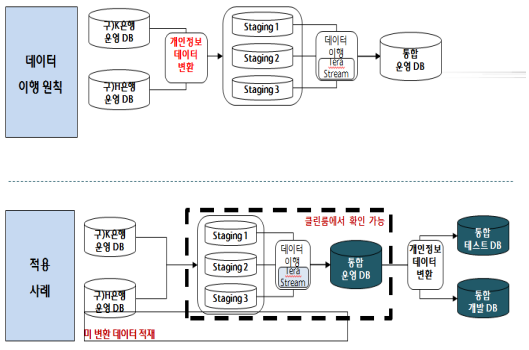


그림 9. H은행 데이터 이행 적용 사례
Fig. 9. H bank's data migration application example

H은행 보안정책 두 번째는 TO_BE 리얼 시스템은 현재 운영시스템과 동일한 수준의 보안 정책 적용입니다. TO_BE 리얼 시스템에는 비록 실제 운영시스템은 아니지만 현재 운영시스템에 있는 고객정보가 그대로 반영되어 있는 시스템이기 때문입니다.

H은행 보안정책 세 번째는 대형 IT프로젝트에 맞는 추가 보안 정책 적용으로 안정성을 강화하는 것입니다. 추가 보안 정책중 하나는 "외주직원 역할에 따른 등급별 접근 권한 통제"입니다.

표 4. H은행 외주직원 등급별 접근 권한 통제 대상
Table 4. H bank's outourcing employees gaded access rights control target

보안통제 \ 접근대상		그룹웨어, 메신저, PPMS	메타시스템	개발시스템	테스트시스템	운영시스템	비고
IP 부여		●	●	●	●	●	외주 전용망, NAC통제
업무 가상화		●	●	●	●	●	
보안프로그램		●	●	●	●	●	PC보안, 문서보안(DRM), 개인정보 차단이(DLP), 출력물보안, 백신
접근통제	서버접근 통제			●	●	●	
	DB 접근 통제			●	●	●	
보안등급		Level- I	Level- II	Level- III	Level-IV	Level- V	

※ 운영시스템 접근(Level-V)은 원칙적으로 불가, 단, 데이터 전환 등 특수목적의 경우 CIO/CISO 개별 승인 후 접근 허용

표 5. H은행 외주직원 대상별 보안 등급
Table 5. The security level of H bank's outsourcing employees

대상		보안등급	승인	비고
① 시스템 접근이 필요한 외주 직원	테스트 포함	Level Ⅰ ~ Level Ⅳ	해당 부서장 승인	
	개발업무	Level Ⅰ ~ Level Ⅲ	해당 부서장 승인	테스트 화면 접근허용
② 시스템 접근이 불필요한 외주직원(컨설팅,PM 등)		Level Ⅰ ~ Level Ⅱ	해당 업무팀 팀장	
③ 기타 행내 상주가 필요한 외주직원		Level Ⅰ	해당 업무팀 팀장	

또 다른 추가 보안 통제 방안은 외주 직원에 대하여 통상 반기 주기로 보안점검을 실시 하던 것을 프로젝트 기간내에 월 1회 정기 점검을 실시하고, 불시에 비정기적으로 보안 점검을 실시하며, 점검결과 위반자에 대하여는 제재할 수 있는 방안을 마련하는 등 강화된 보안 정책을 적용하는 것입니다.

표 6. H은행 외주직원 점검 내용
Table 6. H bank's outcourcing employees security check

점검항목	점검내용	비고
고객정보/전산자료 보호	고객정보 및 전산자료 무단 반출	
	정보 카메라 촬영 및 인쇄물 반출	
	물리PC內 고객정보 저장 여부	
단말기 관리	비인가 단말기(노트북) 무단 반입 및 반출	
	내부 망 이용 (IP 및 LAN 케이블 도용)	
	비인가 프로그램 임의 설치	
	악성코드 감염 여부	
보안 프로그램	필수 보안프로그램 설치 및 운영 현황	
	보안프로그램 우회 및 우회 시도	
해킹방지	비인가 무선장비 무단 반입 및 이용	
	접근권한 및 계정(ID) 도용 여부	
외주관리	전산자료 방치(책상, 프린터 등)	
	비인가 외주직원 투입 여부	외 정기점검
	투입·철수 프로세스 준수 여부	외 정기점검

V. 결론 및 향후 연구 과제

금융기관의 대형 IT 프로젝트 추진 시 막대한 자금 및 인력의 투입이 필요하며, 국가 경제를 위해 무조건 성공하여야 합니다. 대형 IT 프로젝트 기간중 감독기관의 컴플라이언스 준수에 대한 필요성 및 외주인력에 대한 보안 통제는 아무리 강조하여도 부족합니다. 프로젝트 실패 사례는 다수 발견됩니다. 실패 원인이 경직된 보안 통제로 인하여 프로젝트 생산성 저하가 주된 원인은 아닐 수 있으나, 강력한 외주인력 통제와 더불어 프로젝트 생산성 향상에 기여할 수 있는 보안정책 수립은 프로젝트 성공의 열쇠라 할 수 있습니다. 금융기관의 대형 IT프로젝트 성공을 위한 외주직원에 대한 통제 방안 및 보안정책 수립을 본 논문에서 제안한 내용을 H은행의 실제 대형 IT 프로젝트에 적용하였다. 그 결과 업계에서도 놀라울 정도로 성공적인 IT 프로젝트를 완수 하였으며 이로 인하여 H그룹 발전 및 고객 불편을 최소화 할 수 있었습니다. 본 논문을 통하여 금융기관의 대형 IT 프로젝트 추진 시 도움이 되었으면 합니다.

"2018년부터 적용되는 개인정보 암호화를 통하여 고유식별정보의 암호화 등으로 고객정보 유출의 안정성 확보

는 일부 해결될 수 있으나, 고유식별정보 이외 정보를 활용하여 고객 식별이 가능함에 대형 IT 프로젝트 추진 시에 보다 안정적이고, 효율적인 기술적, 관리적 방안이 지속적으로 연구되어 적용함으로서 외주 직원에 대한 보안사고의 위험을 최소화해 나가야 합니다.

References

[1] Yonhapnews, http://www.yonhapnews.co. kr/economy/2014/02/13/0301000000AKR20140213044400002.HTML
[2] Wow Korea Economic News, http://www.sostv.co.kr/newcenter/news/view.asp?bcode=T30001000&artid=A201
[3] National Intelligence Service, "2016 National Information Protection White Paper"
[4] Financial Supervisory Service, Financial Supervisory Service Infomation Disclosure System
[5] Electronic Financial Supervisory Reguration.
[6] Act on the Use and Protection of Credit Information Private Act.
[7] Jae-yoon Sim, "A Study on Information Access Control Policy Based on Risk Level of Security Incidents about IT Human Resources in Financial Institutions" Graduate School of Koear University, 2015.
DOI : http://dx.doi.org/ 10.13089/JKIISC.2015.25.2.343
[8] Yeong=jin Choi, " A Study on Data Security Control Model of the Test System in Financial Institutions" Graduate School of Koear University, 2014.
DOI : hhttp://dx.doi.org/10.13089/JKIISC.2014.24.6.1293

저자 소개

손 병 준(정회원)

- 1994년 2월 : 서강대학교 수학과 졸업
- 1994년 2월 ~ 현재 : KEB하나은행 IT기획부
- 2015년 3월 ~ 현재 : 고려대학교 정보보호대학원 금융보안학과 석사과정

<주관심분야 : 개인정보보호, 전자금융보안, 빅 데이터, 포렌식>

김 인 석(종신회원)

- 1973년 : 홍익대학교 전자계산학과 (학사)
- 2003년 : 동국대학교 정보보호학과 (석사)
- 2008년 : 고려대학교 정보경영공학과 (박사)
- 2009년 ~ 현재 : 고려대학교 정보보호대학원 전문교수

<주관심분야 : 전자금융보안, IT감사, 전자금융법규>