https://doi.org/10.33778/kcsa.2021.21.1.101

금융회사를 위한 기업 정보보호 포털(EISP) 시스템의 설계 및 구현

김 도 형*

요 약

금융회사는 금융정보를 보호하기 위해 정보보호 전략 및 계획을 수립하고 정보보호 관리체계 운영, 정보보호 시스템 구축 및 운영, 취약점 점검, 보안관제 등 다양한 정보보호 활동을 하고 있다. 본 논문에서는 금융회사에서 수행 중인 각종 정보보호 활동에 대한 가시성을 확보하고 통합 관리할 수 있는 금융회사를 위한 기업 정보보호 포털 시스템을 제시하고자 한다. 기업 정보보호 포털 시스템은 정보보호 부서의 활동을 시스템화하여 정보보호 활동이 정보보호 부서만의 활동이 아닌 최고경영자부터 임직원까지 참여할 수 있도록 통합된 환경을 제공한다. 이를 통해 최고경영진이 기업경영에 정보보호를 반영할 수 있는 정보보호 거버넌스로도 활용할 수 있다.

Design and Implementation of Enterprise Information Security Portal(EISP) System for Financial Companies

Do-Hyeong Kim*

ABSTRACT

To protect financial information, financial companies establish strategies and plans for information security, operate information security management systems, establish and operate information security systems, check vulnerabilities, and secure information. This paper aims to present an information security portal system for financial companies that can gain visibility into various information security activities being undertaken by financial companies and can be integrated and managed. The information security portal system systemizes the activities of the information security department, providing an integrated environment for information security activities to participate from CEOs to executives and employees, not just from the information security department. Through this, it can also be used as information security governance that can be used by top executives to reflect information security in corporate management.

Key words : Enterprise Information Security Portal, Information Security Governance, Information Security Management, Security Management

접수일(2021년 01월 10일), 수정일(1차: 2021년 03월 12일), 게재확정일(2021년 03월 27일)

* (주)대구은행 정보보호부

1. 서 론

금융회사들은 내·외부의 각종 보안 위협으로부터 금융정보를 보호하기 위해 정보보호 거버넌스 체계를 마련하여 정보보호 계획을 수립하고, 정보보호 체계를 구축 및 운영하고 컴플라이언스 감사, 취약점 분석 및 리스크 관리 등 다양한 활동을 하고 있다. 이러한 다양한 정보보호 활동이 실질적인 효과를 얻기 위해서는 이를 시스템화할 필요성이 있다.

본 연구에서는 금융회사의 다양한 정보보호 활동을 시스템화하기 위해 기업 정보보호 포털(EISP) 시스템을 설계하고 구현한다. 기업 정보보호 포털(EISP) 시스템은 금융회사의 다양한 정보보호 활동을 시스템화하여 정보보호 부서의 활동을 지원하고 기업의 정보보호 활동이 정보보호 부서만의 활동이 아닌 최고경영자부터 임직원까지 직접 참여할 수 있도록 통합된 환경을 제시한다.

기업 정보보호 포털 사이트를 통해 정보보호 목표를 공유하고 정보보호 운영현황, 모니터링 결과, 정보보호 수준 등을 최고경영자 및 임직원에게 가시화하여 보여줌으로써 정보보호 활동을 강화하고 이를 기업경영에 반영할 수 있다.

제2장 관련 연구에서는 금융회사의 정보보호 활동 및 기업 정보보호 포털(EISP)에 대해 살펴보고, 제3장에서는 금융회사를 위한 기업 정보보호 포털 시스템을 설계하고 구현한다. 제4장에서는 본 시스템의 효과성을 분석하고 결론을 맺는다.

2. 관련 연구

2.1 금융회사 정보보호 활동

금융회사는 회사 내의 각종 금융정보 및 금융거래 정보를 보호하기 위하여 보안계획을 수립하고, 각종 정보보호 시스템을 운영하며 정보보호 교육 및 훈련, 취약점 관리, 외부인력 관리, 각종 컴플라이언스 대응, 개인정보보호 등 다양한 정보보호 활동을 수행하고 있다[1][2].

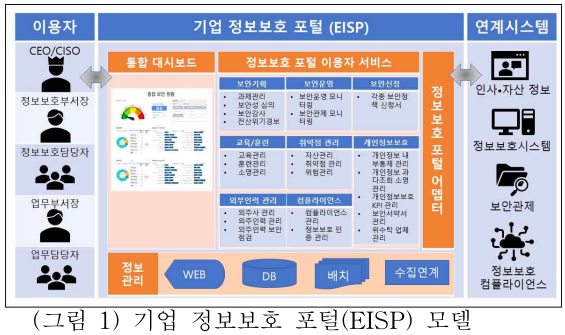
세부적인 수행 내용은 <표 1> 과 같다.

<표 1> 금융회사 정보보호 활동

구 분	세부 내용
보안계획 수립	■ 정보보호 연간계획 및 중·장기 계획, 정보보호 예산관리, 정보보호 정책 관리 ■ 각종 정보시스템 구축에 대한 보안성 심의 ■ 각종 정보보호 활동에 대한 감사 ■ 전산위기 관리
보안운영	■ 보안운영 모니터링: 보안시스템 운영 및 모니터링 현황 ■ 보안관제 모니터링
보안교육 및 훈련	■ 정보보호 교육 계획 및 운영 관리 ■ 정보보호 훈련 계획 및 운영 관리
취약점 관리	■ 정보자산 관리 ■ 정보시스템 취약점 수행 및 관리 ■ 정보보호 위협 관리
외주인력 관리	■ 외주회사 관리, 외주인력 관리, 외주인력 보안점검 관리
컴플라이언스 관리	■ 정보보호 관련 컴플라이언스 관리 ■ 정보보호 인증 관리: ISO27001 및 ISMS-P 등 정보보호 인증 관리
개인정보보호	■ 개인정보 내부통제 관리, 개인정보 과다조회 소명 관리, 개인정보보호 KPI 관리, 보안서약서 관리, 위수탁 업체 관리

2.2 기업 정보보호 포털(EISP) 모델

기업 정보보호 포털(EISP, Enterprise Information Security Portal) 모델은 EIP, Enterprise Information Portal을 기반으로 정보보호 활동을 통합 관리할 수 있는 모델이다. 기업 정보보호 포털 모델은 다음 (그림 1)과 같다[3].



(그림 1) 기업 정보보호 포털(EISP) 모델

기업 정보보호 포털 모델은 이용자, 기업 정보보호 포털, 연계시스템으로 구성되어 있다.

이용자 영역은 크게 5가지 이용자 그룹으로 나눌 수 있다. CEO/CISO가 속한 최고경영자 그룹, 정보보호 부서장, 정보보호 담당자 그룹, 업무 부서장 그룹, 업무 담당자 그룹이다. 최고경영자 그룹, 정보보호 부서장, 정보보호 담당자 그룹은 은행 전체의 정보보호 현황을 볼 수 있는 그룹이고, 정보보호 부서장 및 정보보호 담당자 그룹은 각 담당 영역별로 세부적인 정보를 관리할 수 있다. 업무 부서장 그룹 및 업무 담당자 그룹은 해당 부서별, 개인별 정보보호 수준 및 현황을 볼 수 있다.

기업 정보보호 포털 영역은 본 모델의 메인 영역으로 통합 대시보드, 정보보호 포털 이용자 서비스, 정보관리, 정보보호 포털 어뎁터로 구성이 되어 있다.

통합 대시보드는 정보보호 현황을 보여주고, 기업 정보보호 포털 이용자에 필요한 각종 메뉴를 보여준다. 해당 대시보드는 앞서 언급한 바와 같이 이용자 그룹별 필요한 정보를 보여준다.

정보보호 포털 이용자 서비스는 이용자별로 정보보호 활동을 하는 부분으로 정보보호 업무 담당자 및 일반 임직원들이 사용하는 서비스이다. 보안기획, 보안운영, 보안신청, 교육 및 훈련, 취약점 관리, 외부인력 관리, 컴플라이언스 관리, 개인정보보호로 구성되어 있다.

정보보호 포털 어뎁터는 기업 정보보호 포털 운영에 필요한 각종 정보를 수집하는 역할을 한다. 인사정보 및 자산정보 연동, 각종 정보보호시스템의 로그 수집 및 정제, 보안관제 데이터 수집 및 정제, 정보보호 관련 컴플라이언스 수집 및 정제 작업을 한다. 정보보호 포털 어뎁터에서는 기업 정보보호 포털에서 활용하기 위해 수집된 데이터의 가공작업도 반드시 필요하다.

정보관리에서는 기업 정보보호 포털을 시스템적으로 관리하는 영역이다. 수집된 데이터를 배치작업 등을 통해 DB에 저장하고, 통합 대시보드 및 이용자 서비스 영역에 사용할 수 있도록 DB를 구성하고, SSO 연동 및 웹 서비스를 제공하는 역할을 한다.

연계시스템 영역은 기업 정보보호 포털과 연동하는 각종 시스템이다.

3. 금융회사를 위한 기업 정보보호 포털 시스템의 설계 및 구현

시스템의 설계 및 구현은 기업 정보보호 포털(EISP, Enterprise Information Security Portal) 모델을 기반으로 하였다.

3.1 시스템의 설계

기업 정보보호 포털(EISP) 모델을 기반으로 금융회사에 특화된 시스템 설계를 하였으며 (그림 2)와 같다.

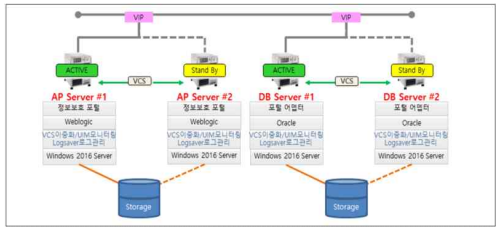
(그림 2) 금융회사 기업 정보보호 포털 시스템의 전체 구성도

3.2 시스템의 구현

시스템의 구현은 금융회사 D사를 대상으로 진행하였다. D사는 임직원 약 3,000여명으로 구성된 중견 금융회사이다.

(1) 서버 구성

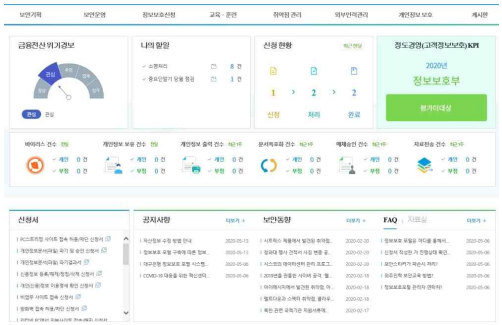
2대의 AP 서버와 2대의 DB 서버로 이중화 구성하고, OS는 Windows 2016, DBMS는 Oracle, WAS는 Weblogic으로 세부적인 구성내용은 (그림 3)과 같다. 서버의 이중화 구성으로 가용성을 확보하고 최신 Windows OS와 상용 WAS 및 DBMS 사용으로 안정성을 확보하였다.



(그림 3) 기업 정보보호 포털 시스템 서버 구성

(2) 기업 정보보호 포털 메인화면

포털 메인화면은 (그림 4)와 같이 정보보호 현황을 보여주고, 기업 정보보호 포털 사용자에 필요한 각종 메뉴를 보여준다. 금융전산 위기 경보, 나의 할 일, 신청현황, 부서 KPI 점수, 부서별 개인별 정보보호 현황, 신청서, 공지사항, 보안뉴스, 자료실 화면으로 구성되어 있다.



(그림 4) 기업 정보보호 포털 메인화면

금융전산 위기 경보는 금융위에서 발령하는 금융전산 위기를 표시해 준다. 나의 할 일은 각종 결재사항 및 보고사항 알림, 정보보호 교육 및 훈련 알림, 정보보호 점검 알림 등으로 본인이 해야될 일을 건수로 표현해 주며, 각 건수를 클릭하면 세부 메뉴로 이동한다. 신청현황은 본인이 신청한 정보보호 정책 신청서의 진행사항을 표시해 주는 화면이며, 숫자 클릭시 세부 신청 내역을 확인 할 수 있다. 부서 KPI점수는 각종 정보보호 활동을 수집하여 이를 점수화하여 소속 부서의 KPI 점수로 표시해 준다. 부서 및 개인 정보보호 현황은 소속 부서의 정보보호 현황과 개인의 정보보호 현황을 숫자로 표시해 준다. 신청서 메뉴는 각종 정보보호 정책 신청을 할 수 있는 메뉴이다. 공지사항, 보안뉴스, 자료실은 각종 정보보호 관련정보를 공유하는 게시판이다.

(3) 기업 정보보호 포털 대시보드

통합 대시보드는 (그림 5)와 가티 정보보호 전체 현황을 보여주는 화면으로 최고경영자 그룹, 정보보호 부서장, 정보보호 담당자 그룹이 볼 수 있는 화면이다.

(그림 5) 기업 정보보호 포털 대시보드

보안관제 현황은 통합보안관제에서 가지고 오는 정보로 정보보호 관제의 위험단계 및 보안장비 운영현황을 실시간으로 보여준다. 교육 이수별 현황은 임직원 정보보호 교육 현황 및 외주인력 정보보호 현황을 보여준다. 훈련 진행 현황은 정보보호 훈련의 일정을 보여준다. 기타 그래프들은 내부 정보유출 통제 현황 기준으로 전체 통제 건수를 그래프 형태로 보여 준다.

(4) 기업 정보보호 포털 메뉴

정보보호 메뉴 기능그룹은 기업 정보보호 포털의 핵심 기능으로 정보보호 활동에 필요한 각종 메뉴들이 구성되어 있다. 세부 메뉴 구성 내용은 다음 (그림 6)과 같다.

(그림 6) 기업 정보보호 포털 메뉴 구성

보안기획은 과제관리, 보안성 심의, 보안감사, 전산위기 경보로 구성되어 있다. 과제관리는 정보보호 연간계획 및 중·장기 계획 관리, 정보보호 예산관리 정보보호 정책 및 지침 관리 등을 수행한다. 보안성 심의는 각종 신규 구축 정보시스템에 대한 보안성 심의를 등록 관리하며 보안감사는 각종 정보보호 활동에

대한 감사를 수행 관리한다. 전산위기경보는 국가 전산위기수준을 등록하고 관리한다.

보안운영은 보안운영 모니터링, 보안관제 모니터링으로 구성되어 있다. 보안운영 모니터링은 보안시스템 운영현황을 보여주며, 보안관제 모니터링은 보안관제 현황을 보여준다.

보안정책은 각종 정보보안 정책 신청서로 구성이 되어 있다. 방화벽 정책 의뢰서, 무선기기 허용 정책 의뢰서, 매체허용 의뢰서, 업무사이트 접근 허용 의뢰서 등 각종 보안정책 의뢰서가 있으며, 임직원들은 해당 신청서를 통해 각종 보안정책 허용을 신청한다.

교육/훈련은 교육관리, 훈련관리, 소명관리로 구성이 되어 있다. 교육관리는 각종 정보보호 교육을 계획하여 운영하고 수료여부를 관리한다. 훈련관리는 각종 정보보호 훈련을 계획하여 운영하고 그 결과를 관리한다. 소명관리는 정보보호 교육 및 정보보호 훈련의 미흡자에 대해 소명요청을 하여 미흡사항을 관리한다.

취약점 관리는 자산관리, 취약점 관리, 위험관리로 구성이 되어 있다. 자산관리는 취약점 대상이 되는 각종 정보시스템을 등록 관리한다. 취약점 관리는 자산관리에 등록된 자산기준으로 취약점 계획을 수립하고 점검결과를 등록하여 취약점 현황을 볼 수 있다. 위험관리는 각종 보안위협 이슈를 등록하고 관리할 수 있다.

외부인력관리는 외주사 관리, 외주인력 관리, 외주인력 보안관리로 구성되어 있다. 외주사 관리는 회사에 출입하는 외주회사를 등록하고 관리한다. 외주인력 관리는 회사에 출입하는 외주인력을 등록하고 관리한다. 외주인력 보안관리는 정기적인 보안점검 활동을 통해 외주인력에 대한 보안관리를 수행한다.

컴플라이언스는 컴플라이언스 관리와 정보보호 인증 관리로 구성이 되어 있다. 컴플라이언스 관리는 각종 정보보호 관련 법규 및 내규를 확인할 수 있으며, 이를 기준으로 한 점검 체크리스트를 통해 컴플라이언스 준수 여부를 점검할 수 있다. 정보보호 인증 관리는 ISO27001 및 ISMS-P 등의 정보보호 관리체계 인증유지를 위해 체크리스트 기반으로 점검할 수 있다.

개인정보보호는 개인정보 내부통제 관리, 개인정보 과다조회 소명 관리, 개인정보보호 KPI(Key Performance Indicator 핵심성과지표) 관리, 보안서약서 관리, 위수탁 업체 관리로 구성되어 있다. 개인정보 내부통제는 기업이 개인정보보호를 이용현황을 모니터링하고 이용에 대한 승인정책을 관리한다. 개인정보 과다조회 소명 관리는 개인정보 처리시스템의 개인정보 과다조회 시 소명요청을 하여 적정성 여부를 판단할 수 있도록 한다. 개인정보보호 KPI 관리는 각종 개인정보보호 위반사항을 수집하여 KPI에 반영하고 그 결과를 점수화하여 보여준다. 보안서약서 관리는 개인정보를 이용함에 있어 각종 보안서약서 동의를 받고 관리하는 메뉴이다. 위수탁업체 관리는 우리 회사의 개인정보를 제공받아 업무를 처리하는 위수탁 업체에 대한 현황 및 개인정보보호 관리 준수여부를 점검한다.

4. 결 론

본 논문에서는 금융회사가 정보보호 활동을 시스템화하고 운영할 수 있도록 기업 정보보호 포털(EISP) 모델에 기반한 시스템을 설계 및 구현하였다. 구현된 시스템은 금융회사의 정보보호 활동을 실질적으로 활용할 수 있도록 하였다. 보안기획, 보안운영, 보안신청관리, 정보보안 교육 및 훈련, 취약점 관리, 외부인력관리, 개인정보보호 등 금융회사 정보보호의 모든 활동을 정보보호 업무 담당자가 기업 정보보호 포털을 통해 운영하고, 정보보호 최고책임자(CISO) 및 최고경영자(CEO)는 기업 정보보호 포털 통합 대시보드를 통해 기업 전체의 정보보호 현황을 볼 수 있다. 기업 정보보호 포털을 통해 정보보호 목표, 정보보호 운영현황, 모니터링 결과, 정보보호 수준 등을 통합된 화면으로 정보보호 최고책임자(CISO) 및 최고경영자(CEO)에게 보여줌으로써 기업 정보보호 거버넌스 또한 효율적으로 운영할 수 있다.

일반 임직원들도 직원 개개인의 정보보호 현황과 소속 부서의 정보보호 현황을 기업 정보보호 포털을 통해 확인할 수 있다, 또한 각종 정보보호 정책 신청을 기존 그룹웨어 또는 ITSM(IT Service Management)가 아닌 기업 정보보호 포털을 통해 통합된 화면으로 제공함으로써 정보보호 관련 업무가 IT서비스 영역이 아닌 별도의 정보보호 영역으로써 관리할 수 있다.

본 논문에서 구현한 금융회사를 위한 기업 정보보호 포털(EISP) 시스템은 정보보호 최고책임자(CISO) 및 최고경영자(CEO)가 기업 전체의 정보보호 현황을 통합적으로 볼 수 있도록 함으로써 최고경영진이 정보보호가 기업경영의 하나로 인식하고 정보보호 활동에 적극 참여할 수 있도록 한다. 또한 정보보호 최고책임자(CISO)는 비즈니스 목표에 맞는 정보보호 목표를 수립할 수 있고 운영함으로써 기업의 입장에서는 실질적이고 현실적인 정보보호 활동을 수행할 수 있다. 금융회사에 맞는 정보보호 전략 및 운영계획을 수립할 수 있으며, 비즈니스 목표에 맞는 정보보호 예산 수립, 정보보호 인력을 운영할 수가 있다.

본 논문을 기반으로 다른 산업군에도 해당 산업에 맞는 기업 정보보호 포털(EISP) 시스템을 설계 및 구현할 수 있을 것이다.

참고문헌

[1] 김도형, “최고경영자를 위한 정보보호 거버넌스 모델에 관한 연구”, 융합보안논문지, 제17권, 제1호, pp. 39-44, 2017.

[2] 금융보안원, “금융보안 거버넌스 가이드”, 2019.12.

[3] 김도형, “기업 정보보호 거버넌스를 위한 정보보호 포털 모델에 관한 연구”, 융합보안논문지, 제20권, 제3호, pp. 39-46, 2020.

[4] 이성일, “정보보호 거버넌스 프레임워크에 관한 연구”, 동국대학교 대학원 경영정보학과, 2011.

[5] 김귀남, 김민준, “정보보안 거버넌스 프레임워크에 관한 연구”, 융합보안논문지, 제10권, 제4호, pp. 14-19, 2010.

[6] 김세인, “포털기반 기업정보시스템의 통합”, 정보학연구, 제6권, 제4호, pp. 93-111, 2003.

[7] 정인근, 이명무, 노필영, “혁신의 확산 관점”에서 EIP 시스템의 도입에 관현 연구”, 한국경영정보학회, Vol.2002, No.1, pp. 807-812, 2002.

〔저자소개〕

김 도 형 (Do-Hyeong Kim)

2001년 2월 한국방송통신대학교 미디어영상학 학사
2003년 2월 경기대학교 정보보안전공 석사
2008년 8월 경기대학교 정보보호학 박사
현재 ㈜대구은행 정보보호부 차장

email : pccop@daum.net