

기업 정보보호 거버넌스를 위한 기업 정보보호 포털 모델에 대한 연구

김도형*

요약

기업은 기업의 비즈니스 정보를 보호하기 위해 정보보호 관리체계 구축, 정보보호 시스템 구축 및 운영, 취약점 점검, 보안 관제 등 다양한 정보보호 활동을 하고 있다. 기업 비즈니스를 위한 다양한 정보보호 활동들을 체계화한 것이 기업 정보보호 거버넌스라고 할 수 있으며, 이를 효과적으로 운영하기 위해서는 시스템화할 필요성이 있다. 본 연구에서는 기업 정보보호 거버넌스를 시스템화하기 위해 기존의 기업 정보 포털(EIP) 모델에 대해 알아보고, 이에 기반한 기업 정보보호 포털(EISP) 모델을 제시하고자 한다. 기업 정보보호 포털(EISP) 모델은 기업의 다양한 정보보호 활동인 기업 정보보호 거버넌스를 시스템화하여 정보보호부서의 활동을 지원하고 기업의 정보보호 활동이 정보보호부서만의 활동이 아닌 최고경영자부터 임직원까지 직접 참여할 수 있도록 통합된 환경을 제시한다.

A Study on Enterprise Information Security Portal Model for Enterprise Information Security Governance

Kim Do Hyeong*

ABSTRACT

In order to protect the business information of the enterprise, the company is engaged in various information security activities, such as establishing an information security management system, establishing and operating an information security system, checking vulnerabilities and security controls. It is an enterprise information security governance that organizes various information security activities for enterprise business, and it needs to be systematized to operate them effectively. In this study, to systematize the enterprise information security governance, we would like to explore the existing Enterprise Information Portal(EIP) model and propose an Enterprise Information Security Portal(EISP) model based on it. The Enterprise Information Security Portal(EISP) model provides an integrated environment for supporting the activities of the information security departments by systemizing the enterprise information security governance, which is a variety of information security activities of the enterprises, so that the information security activities of the enterprises can participate directly from CEO to executives and employees, not just from the information security departments.

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

접수일(2020년 08월 08일), 수정일(2020년 09월 14일),
계재확정일(2020년 09월 27일)

* (주)대구은행 정보보호부

1. 서 론

기업들은 내·외부의 각종 보안 위협으로부터 기업 비즈니스 정보를 보호하기 위해 정보보호 거버넌스를 마련하여 활동하고 있다. 정보보호 거버넌스 활동에는 정보보호 계획 수립하고 정보보호 체계를 구축 및 운영하고 컴플라이언스 감사, 취약점 분석 및 리스크 관리 등 다양한 활동이 있다. 정보보호 거버넌스가 실질적인 효과를 얻기 위해서는 이를 시스템화할 필요가 있으며 Dashboard(대시보드:현황판) 형태의 정보보호 포털사이트를 통해 정보보호 목표, 정보보호 운영현황, 모니터링 결과, 정보보호 수준 등을 최고경영자 및 임직원에게 가시화하여 보여줌으로써 정보보호 활동을 강화하고 이를 기업경영에 반영할 수 있다.

본 연구에서는 최고경영자 및 임직원이 기업 정보보호 거버넌스에 따라 정보보호 활동에 적극 참여하고 수행 할 수 있는 정보보호 포털 모델을 제시하고자 한다. 제2장 관련 연구에서는 정보보호 거버넌스 및 기업 정보 포털(EIP)에 대해 살펴보고, 제3장에서는 기업을 위한 기업 정보보호 포털 모델을 제시한다. 제4장에서는 본 모델의 효과성을 분석하고 결론을 맺는다.

2. 관련 연구

2.1 기업 정보보호 거버넌스

정보보호 거버넌스란 위협관리 노력의 일환으로, 정보보호 전략이 비즈니스 목표와 연계되고 이의 달성을 지원하며, 정책과 내부통제를 통해 관련 법규와 규정을 준수하는 것을 보장하고, 책임을 할당하기 위한 프레임워크와 이를 위한 경영 구조 및 프로세스를 수립하는 과정이다.[2]

기업 정보보호 거버넌스는 다음 (그림 1)과 같이 최고경영자(CEO)의 비즈니스 목표에 따라 정보보호 목표를 수립하고 운영되어야 한다. 물리적, 기술적, 관리적 보안이 유기적으로 연동된 융합보안체계를 통해 정보보호 프로세스 운영 및 통제를 하고, 지속적 모니터링을 통해 비즈니스 목표에

맞는 정보보호 활동을 수행한다.[1]



(그림 1) 기업 정보보호 거버넌스 모델

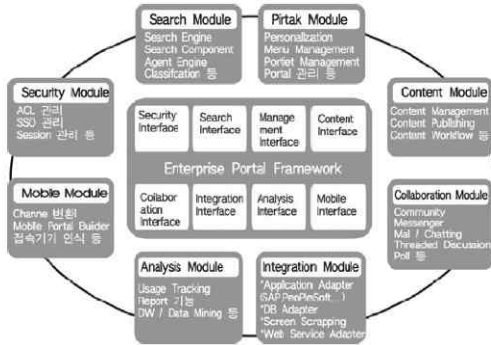
기업 정보보호 거버넌스가 실질적인 효과를 얻기 위해서는 해당 모델을 시스템화하는 연구가 필요하다.[1]

2.2 기업 정보 포털(EIP)

EIP, Enterprise Information Portal은 1996년 12월 Consumer Portal인 Yahoo가 개인화 서비스인 MyYahoo를 도입하여 1998년 5배 이상의 고정방문자를 확보하는 성과를 거두고 같은 해 Netscape도 이에 대항하여 MyNetscape를 출범시킨 데서 그 기원을 찾을 수 있다. 기업 정보 포털(EIP)이라는 용어가 처음으로 등장한 것은 1998년 11월 미국의 증권회사 Merrill Lynch가 발간한 보고서에서 “EIP는 기업 내부와 외부 정보를 통합하여 이용자가 단일 게이트웨이(gateway)를 통해 중요한 의사 결정을 내리는데 필요한 맞춤 정보를 제공할 수 있게 해주는 어플리케이션이다.” 라고 정의하면서부터라고 볼 수 있다.[4]

Portal의 사전적 의미가 ‘정문’, ‘관문’이라는 단어의 뜻에 알 수 있듯이 EIP는 개인과 조직이 여러 시스템으로 관리해온 정보를 통합해 하나의 웹 화면에서 제공하는 기업용 포털이며 인터넷 포털 사이트를 통하여 기업 활동에 필요한 모든 자원을 통합하여 관리 및 분석하고 제공할 수 있는 시스템이다. 기업의 내적, 외적 자원은 물론 사용자 간의 협업체계, 커뮤니케이션 및 제반 온라인을 통한 거래 등이 한꺼번에 제공된다고 정의하고 있

다.[4] 다음 (그림 2)는 기업 정보 포털(EIP)의 프레임워크 이다.



(그림 2) 기업 정보 포털(EIP)의 프레임워크

EIP의 구성 요소는 크게 3가지로 구분된다.[5]

첫 번째는 기업 내 정보의 통합이다. 기존의 기업에서 데이터베이스 형태로 저장되어 온 정형 데이터와 각종 사내 문서, 보고서, 도면, 웹 검색 자료 등 비정형 자료까지 포함하는 개념이다.

두 번째는 기존의 시스템과의 통합이다. 기업 내 정보를 하나로 통합하기 위한 필수적인 작업으로 기존의 데이터베이스와의 연계 및 ERP, CRM, SCM 등 이미 도입했던 시스템과의 통합 작업이 필요하다.

세 번째는 이용자가 활용할 수 있는 툴의 개발이다. EIP 구축을 통해 통합된 정보 중에서 이용자에게 필요한 정보만을 선택할 수 있는 기능과 통합된 시스템에 접근할 수 있는 단일 점점, 즉 싱글사인온(Single Sign On)의 구현, 그리고 이용자의 업무 특성과 권한에 따른 접근 권한 등 보안 설정 등이다.

EIP는 반드시 “Write-Once, Reuse-Many”라는 철학을 가져야 하며 컴포넌트 구조로 기존 시스템이나 다른 포털제품과의 통합을 위하여 산업 표준을 따르면서 전사적인 업무량 증가에 유연하게 대응할 수 있는 구조로 설계되어야 한다. 이를 바탕으로 기업 정보 포털(EIP)은 <표 1>과 같이 4가지의 영역으로 서비스를 구성할 수 있다. [4].

<표 1> 기업 정보 포털(EIP)의 서비스 구성요소

영역	세부 내용
프레젠테이션 서비스(Presentation Service)	각 서비스 기능들을 활용하여 사용자의 요구사항에 맞는 정보를 제공하는 기능을 담당하는 영역이다
이용자 서비스 (User Service)	각 서비스 모듈 및 응용 소프트웨어가 운용되는 영역으로 실질적으로 서비스가 실행되는 영역이다
정보관리(Information Management)	EIP의 정보 디렉터리 및 정보 디렉터리를 관리하고 있는 모듈들이 위치한 영역이다.
포털어댑터(Portal Adapter)	각 레거시 데이터 및 응용 어플리케이션과의 연결을 담당한다. 데이터 차원뿐만 아니라 응용에 이르는 연결을 수행해야 하며, 정형/비정형 데이터를 취급하게 된다.

프레젠테이션 서비스 영역은 각종 기능 서비스를 활용하여 사용자 요구사항에 맞는 정보를 제공하는 영역이다. 이용자 서비스 영역은 이용자들이 실질적으로 포털을 이용하는 영역이며, 정보관리 영역은 포털 운영에 필요한 정보를 관리하는 영역이다. 포털어댑터 영역은 포털운영에 필요한 시스템과 연동과 각종 데이터를 수집하는 영역이다.

3. 기업 정보보호 포털(EISP) 모델

기업 정보보호 포털은 EISP, Enterprise Information Security Portal로 기업의 내·외부 정보보호 활동을 통합하여 이용자에게 하나의 웹 화면으로 제공해 주는 시스템으로 정의할 수 있을 것이다. EISP를 통해 기업 정보보호 활동에 필요한 모든 자원을 통합하여 관리 및 분석하고 제공할 수 있고, 기업의 내적, 외적 정보보호 활동은 물론 사용자 간의 협업체계, 커뮤니케이션 및 제반 온라인을 통한 거래 등을 제공한다.

본 논문에서는 기업 정보보호 거버넌스를 기반으로 한 기업 정보보호 포털 모델을 제시한다.

3.1 기업 정보보호 포털의 필요 구성요소

기업 정보보호 포털의 구성요소는 3가지로 구성할 수 있다.

첫 번째는 기업 내 정보보호 활동의 통합이다. 기업 정보보호 거버넌스에 따른 각종 동적인 활동과 이에 따르는 각종 문서, 보고서 등의 정적인 자료까지 포함하는 개념이다.

두 번째는 기존의 정보보호 관련 시스템과의 통합이다. 기업 내 정보보호 관련 정보를 하나로 통합하기 위한 필수적인 작업으로 기존의 각종 정보보호시스템의 정보보호 상태에 대한 정보 및 정보보호 관제 정보 등 이미 도입했던 시스템과의 통합 작업이 필요하다.

세 번째는 이용자가 정보보호 활동을 할 수 있는 서비스의 개발이다. EISP 구축을 통해 통합된 정보보호 관련 정보 중에서 이용자에게 필요한 정보만을 선택할 수 있는 기능과 통합된 시스템에 접근할 수 있는 단일 접점, 즉 싱글사인온(Single Sign On)의 구현, 그리고 이용자의 업무 특성과 권한에 따른 접근 권한 등의 보안 설정이다.

3.2 기업 정보보호 포털의 설계

이를 기반으로 기업 정보보호 포털시스템을 실제 구현하기 위해 필요한 설계 구성요소는 다음의 <표 2>와 같다.

<표 2> 기업 정보보호 포털 설계 구성요소

구성 모듈		세부 내용
정보보호 통합 Dashboard		각종 정보보호 주요현황을 사용자, 부서별 역할에 따른 뷰화면
정보 보호 포털 이용자 서비스	보안 기획	관제관리: 정보보호 연간계획 및 중·장기 계획, 정보보호 예산관리, 정보보호 정책 관리 보안성 심의: 각종 정보시스템 구축에 대한 보안성 심의 보안감사: 각종 정보보호 활동에 대한 감사 전산위기경보: 전산위기경보 등록 관리

보안 운영	보안운영 모니터링: 보안시스템 운영 현황 보안관제 모니터링: 보안관제 운영 현황
보안 신청	각종 정보보호 정책 신청서
교육 훈련	교육관리: 정보보호 교육 계획 및 운영 관리 훈련관리: 정보보호 훈련 계획 및 운영 관리 소명관리: 교육 및 훈련 미흡자 소명 관리
취약점 관리	자산관리: 정보자산 등록 관리 취약점 관리: 정보시스템 취약점 등록 관리 위험관리: 정보보호 위협이슈 등록 관리
외부 인력	외주회사 관리, 외주인력 관리, 외주인력 보안점검 관리
컴플라이언스	컴플라이언스 관리: 정보보호 체크리스트를 통한 정보보호 관련 컴플라이언스 관리 정보보호 인증 관리: ISO27001 및 ISMS-P 등 정보보호 인증 관리
개인 정보 보호	개인정보 내부통제 관리, 개인정보 파다조회 소명 관리, 개인정보보호 KPI 관리, 보안서약서 관리, 위수탁 업체 관리
정보관리	정보보호 포털의 정보관리 수행
정보보호 포털 어댑터	인사정보, 자산정보, 정보보호 시스템, 보안관제, 정보보호 관리에 필요한 각종 시스템 연동, 컴플라이언스 관련 정보 수집 등

정보보호 통합 대시보드(Dashboard) 모듈은 포털의 프레젠테이션 서비스 영역으로 정보보호 거버넌스의 모니터링 영역이다. 정보보호의 현황을 부서별, 사용자별로 통합적으로 보여주고, 정보보호 위협 현황,

각종 정보보안 점검 수행현황, 정보보호 정책 신청 현황, 정보보호 KPI 점수, 정보보호 관련 뉴스 및 정보 게시판 등으로 구성할 수 있다.

정보보호 포털 이용자 서비스 모듈은 정보보호 거버넌스의 계획, 구축, 운영, 모니터링이 통합된 영역으로 보안기획, 보안운영, 보안신청, 교육/훈련, 취약점 관리, 외부인력 관리, 컴플라이언스, 개인정보보호로 구성되어 있다.

우선, 보안기획은 과제관리, 보안성 심의, 보안감사, 전산위기경보로 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, 보안관계 모니터링으로 구성되어 있다. 보안운영 모니터링은 보안시스템 운영현황을 보여주며, 보안관계 모니터링은 보안관계 현황을 보여준다.

보안정책은 각종 정보보안 정책 신청서로 구성되어 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 구성되어 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 자산 관리에 등록된 자산기준으로 취약점 계획을 수립하고 점검결과를 등록하여 취약점 현황을 볼 수 있다. 위험 관리는 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 법규기반으로 점검 체크리스트를 통해 컴플라이언스 준수 여부를 점검할 수 있도록 한다. 정보보호 인증 관리는 ISO27001 및 ISMS-P 등의 정보보호 관리체계 인증유지를 위해 체크리스트 기반으로 점검할 수 있도록 한다.

개인정보보호는 개인정보 내부통제 관리, 개인정보 파다조회 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 파다조회 소명 관리는 개인정보 처리시스템의 개인정보 파다 조회시 소명요청을 하여 적정성 여부를 판단할 수 있도록 한다. 개인정보보호 KPI 관리는 각종 개인정보보호 위반사례를 수집하여 KPI에 반영하고 그 결과를 점수화하여 보여준다. 보안서약서 관리는 개인정보를 이용함에 있어 각종 보안서약서 동의를 받고 관리하는 메뉴이다. 위수탁업체 관리는 우리회사의 개인정보를 제공받아 업무를 처리하는 위수탁 업체에 대한 현황 및 개인정보보호 관리 준수여부를 점검한다.

정보관리 모듈은 포털의 정보관리 영역으로 정보보호 포털에서 수집되는 정보를 표현해주고 이용자가 이용할 수 있도록 메뉴를 구성하고 관리하는 역할을 한다. 웹 애플리케이션, DB, 배치기능, SSO 연동 등이 이에 해당한다.

정보보호 포털 어댑터 모듈은 정보수집 및 연계 영역으로 정보보호 포털 운영에 필요한 인사정보 연동, 자산정보 수집, 정보보호 시스템 및 보안관계 정보 수집, 대외 컴플라이언스 정보 수집 등 각종 데이터 수집 및 연계 역할을 한다.



(그림 3) 기업 정보보호 포털 모델

3.3 기업 정보보호 포털 모델

기업 정보보호 포털 설계를 바탕으로 정보보호 포털 모델을 (그림3)과 같이 제시할 수 있다. 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 사용자 서비스, 정보관리, 정보보호 포털 어댑터로 구성이 되어 있다.

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

필요한 정보를 보여준다.

정보보호 포털 사용자 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. 세부내용은 앞서 설계단계에서 설명하였다.

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

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

연계시스템 영역은 정보보호 포털과 연동하는 각종 시스템이다.

지금까지 설명한 기업 정보보호 포털을 기업 정보

보호 거버넌스와 맵핑하여 효과성을 검증해 보면 다음 <표3>과 같다.

<표 3> 기업 정보보호 거버넌스와 기업 정보보호 포털의 맵핑

기업 정보보호 거버넌스	기업 정보보호 포털(EISP)
계 획	보안기획 - 과제관리(정보보호 중·장기계획, 정보보호 연간계획)
구 축	보안기획 - 과제관리(정보보호 정책 및 지침 관리, 정보보호 조직 및 예산 관리)
운 영	보안기획-보안성 심의, 전산위기 정보 보안운영-보안운영 모니터링 보안신청-각종 보안정책 신청서 교육/훈련-교육관리, 훈련관리, 소명관리 취약점 관리-자산관리 외부인력 관리-외주사 관리, 외주인력관리, 외주인력 보안점검 개인정보보호-개인정보 내부통제 관리, 개인정보 파다조회 소명관리, 개인정보보호 KPI 관리, 보안 서약서 관리, 우수탁 업체 관리
모 니 터 링	통합 대시보드(CEO/CISO, 정보보호 담당, 임직원 통합 모니터링 화면) 보안기획-보안감사 보안운영-보안관계 모니터링 취약점 관리 - 취약점 관리, 위협 관리 컴플라이언스-컴플라이언스 관리, 정보보호 인증 관리

<표3>과 같이 기업 정보보호 거버넌스와 기업 정보보호 포털 맵핑 정보를 보면 기업 정보보호 포털을 통해 기업 정보보호 거버넌스를 시스템화할 수 있음을 확인할 수 있다.

5. 결 론

본 논문에서는 기업이 정보보호 거버넌스를 시

스템화하여 운영할 수 있도록 기업 정보 보털(EIP)에 기반한 기업 정보보호 포털(EISP) 모델을 제안하였다. 제안한 모델은 기업 정보보호 거버넌스를 실질적으로 활용할 수 있도록 한다. 보안기획, 보안운영, 보안신청 관리, 정보보안 교육 및 훈련, 취약점 관리, 외부인력 관리, 개인정보보호 등 정보보호의 모든 활동을 각 정보보호 업무 담당자가 정보보호 포털을 통해 운영하고, 정보보호 최고책임자(CISO) 및 최고경영자(CEO)는 정보보호 포털 통합 대시보드를 통해 기업 전체의 정보보호 현황을 볼 수 있다. 정보보호 포털을 통해 정보보호 목표, 정보보호 운영현황, 모니터링 결과, 정보보호 수준 등을 통합된 화면으로 정보보호 최고책임자(CISO) 및 최고경영자(CEO)에게 보여줌으로써 기업 정보보호 거버넌스를 효율적으로 운영할 수 있다.

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

본 모델에서 제시하는 기업 정보보호 거버넌스 기반의 기업 정보보호 포털(EISP) 모델은 정보보호 최고책임자(CISO) 및 최고경영자(CEO)가 기업 전체의 정보보호 현황을 통합적으로 볼 수 있도록 하므로써 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. 기업 비즈니스에 맞는 정보보호 전략 및 운영계획을 세울 수 있으며, 비즈니스 목표에 맞는 정보보호 예산 수립, 정보보호 인력을 운영할 수가 있다.

본 논문에서 제안하는 모델을 실질적으로 시스템화하기 위해서는 세부적인 시스템 구성에서부터

기업 정보보호 포털(EISP) 모델의 세부적인 설계 및 구현이 필요하다. 기업의 산업군에 따라 시스템의 세부 설계가 상이 할 수 있을 것이다. 본 모델을 기반으로 특정 산업군에 맞는 정보보호 포털(EISP) 시스템을 설계 및 구현할 수 있을 것이다.

- [10] 한국데이터베이스진흥센터, “기업 정보 포털(EIP)의 개요”, 디지털콘텐츠, Vol.11, pp. 54-57, 2001
- [11] 박지홍, “차세대 Enterprise Portal 기능의 평가 프레임워크 개발에 관한 연구: 지식 창출 관점”, 정보관리학회지, Vol.24, No.3, pp. 67-82, 2007

참고문헌

- [1] 김도형, “최고경영자를 위한 정보보호 거버넌스 모델에 관한 연구”, 융합보안논문지, 제17권, 제1호, pp. 39-44, 2017
- [2] 이성일, “정보보호 거버넌스 프레임워크에 관한 연구”, 동국대학교 대학원 경영정보학과, 2011
- [3] 이창훈, 하옥현, “기밀유출방지를 위한 융합보안 관리 체계”, 융합보안논문지, 제10권, 제4호, pp. 61-67, 2010.
- [4] 박수경, “기업정보포털의 정보관리 구성요소 영역 구축에 관한 연구”, 숭실대학교 정보과학대학원 지식경영학과, 2008
- [5] 이혜승, “기업포털사이트의 사용성 연구”, 이화여자대학교 정보과학대학원 멀티미디어학, 2004
- [6] 김귀남, 김민준, “정보보안 거버넌스 프레임워크에 관한 연구”, 융합보안논문지, 제10권, 제4호, pp. 14-19, 2010.
- [7] 박상준, 강민철, 강주영, “성공적인 EIP(Enterprise Information Portal) 구축을 위한 연구: S(사) 구축사례 분석”, 한국산업정보학회논문지, 제11권, 제4호, pp. 10-24, 2006.
- [8] 김세인, “포털기반 기업정보시스템의 통합”, 정보학연구, 제6권, 제4호, pp. 93-111, 2003.
- [9] 정인근, 이명무, 노필영, “혁신의 확산 관점에서 EIP시스템의 도입에 관한 연구”, 한국경영정보학회, Vol.2002, No.1, pp. 807-812, 2002.

[저자소개]



김도형 (Do-hyeong Kim)

2003년 2월 경기대학교 정보보안전공
공학석사

2008년 8월 경기대학교 정보보호학
이학박사

현재, (주)대구은행 정보보호부 차장

email : pccop@daum.net