Journal of Knowledge Information Technology and Systems(JKITS), Vol. 9, No. 3, pp. 369~378, June 2014

Journal of The Korea Knowledge Information Technology Society

ISSN 1975-7700

http://www.kkits.or.kr

IT GRC-based IT security internal control system

Young-Rok Yu[1], Seong-Chae Seo[2], Sang-Joon Lee[*3], Byung-Ki Kim[2]

[1]*CAS Inc., Seoul Korea*
[2]*Dept. of Electornic and Computer Engineering, Chonnam National University*
[3]*School of Business Administration, Chonnam National University*

ABSTRACT

In this thesis, a novel IT security internal control system is proposed in order to guarantee the enterprise-wide perspective internal control which accommodates administrative, technical and physical internal control enforcement plan. Firstly, the proposed IT security internal control system synthetically manages IT security processes which are composed of information security processes, privacy processes and security service processes from the perspective of governance. Secondly, it integrates IT related logs based on Big Data to synthetically monitor information security control breach and information leakage anomaly, monitors Key Risk Indicator (KRI) for the information security threat scenario, analyses, alarms and reponses results of monitoring them from the perspective of the risk management. Lastly, it integrates and manages law and regulations related to IT security from the perspective of compliance and provides the automated and integrated IT security internal control environments to the system managers. The proposed thesis proves to be an automatical and efficient scheme to offer the IT security internal control environments through the case of a system installation in a financial company.

KEYWORDS: IT GRC, IT Internal Controls, Securities, Monitoring, IT Risks, IT Compliance

ARTICLE INFO: Received 22 May 2014, Accepted 13 June 2014.

1. 서 론

최근 지속적으로 발생하는 개인정보 유출사건 및 전산장애의 첫 번째 원인을 IT내부통제관리 소

[*]Corresponding author is with the School of Business Administration, Chonnam National University, 300 Yongbong-dong Buk-gu Gwangju, 500-757, KOREA.
E-mail address: s-lee@jnu.ac.kr

홀로 꼽고 있다. 관리당국도 IT 내부통제 강화를 위한 규정 및 규준을 개정하는 등 관련노력을 하고 있지만 해당기업의 자발적인 IT 내부통제 강화 방안이 필요한 시점이다. 2011년 금융보안연구원에서 발표한 금융IT 내부통제 강화 전략 이슈 리포트에서 보안사고의 60% 이상이 내부자에 의해 발생하였고 조직의 규모가 클수록 내부자 위협에 더욱 취약하다는 사실이다[1].

현재 내부 회계관리제도를 시행하는 기관에 한하여 IT업무를 대상으로 리스크, 통제, 테스팅을 통해서 IT 내부통제를 수행하고 있지만 형식적인 절차에 불과한 실정이다. 조직 내부에 증가하는 보안위협을 효율적으로 관리하고 통제하기 위해 정보보안 제품을 사용하고 있지만 단일 목적을 위한 내부통제 수준으로 제한되어 있다. 즉, 내부통제강화를 위한 개별적인 노력은 진행되고 있지만 관리적, 기술적, 물리적 방안을 통합하여 관리할 수 있는 전사적 관점의 내부통제를 위한 시스템 구축은 미흡한 상태이다. 현재 진행되고 있는 보안 내부통제시스템의 문제점은 다음과 같다. 첫째, 보안 내부통제를 위한 개별시스템 형태로 진행되어서 내부통제를 위한 통합적인 프로세스 관리가 부재하다. 둘째, 통합로그관리시스템, 보안관제, SIEM(Security Information and Event Management), 개인정보유출방지시스템 등 개별적인 분석 모니터링 시스템은 존재하지만 이를 통합적으로 모니터링할 수 있는 체계가 부족하다. 셋째, ISMS(Information Security Management System), 개인정보보호법 등 다양한 IT 보안 컴플라이언스가 존재하지만 이를 조직에 맞도록 통합관리하는 기능이 부족하다.

내부자 보안사고를 100% 차단한다는 것은 현실적으로 어려운 문제이나, 내부자 보안사고를 사전에 예방하고 사고발생 초기 신속한 대응이 가능하도록 관리적, 기술적, 물리적 측면의 내부통제 강화방안을 고려한 IT 보안 내부통제시스템을 자동화하여 위험을 상당히 줄이는 효과를 기대할 수 있다. 이를 위해 관리적, 기술적, 물리적 내부통제 강화 방안을 수용하면서 전사적 관점의 내부통제를 위한 IT 보안 내부통제시스템 구축이 필요하다.

본 논문에서는 위에서 언급한 문제점들을 해결하면서, 빅데이터 기반으로 확장성과 유연성을 제공하는 IT GRC(Governance, Risk management, Compliance) 기반의 IT 보안 내부통제시스템을 제시한다. IT 거버넌스 차원에서 보안성 검토, IT 자산관리, 취약점 및 위험관리, 인증 및 감사 대응, 개인정보처리시스템관리, 개인정보영향평가관리, 개인정보 라이프사이클 관리, 협력사 및 개인정보 수탁사 관리 등 정보보안 업무를 통합하여 일원화하도록 관리한다. 통합업무는 한 곳에서 보안관련 모든 업무를 처리할 수 있도록 한다. IT 리스크관리 차원에서는 네트워크장비, 서버, 보안장비, IT 관리 어플리케이션, 비즈니스 어플리케이션 등에서 IT 관련 모든 유형의 로그들을 빅데이터 기반으로 통합 관리하도록 한다. 이들 로그로부터 IT관리 관점, 보안 취약점 관점, 정보유출 관점, 보안 내부통제 관점 등의 IT 리스크(이상징후)에 해당되는 시나리오를 발췌하여 분석하고 상시 모니터링하므로서 보안사고를 예방점검하고 이상징후를 조기에 적발 및 대응할 수 있는 통합체계를 마련하도록 한다. IT 컴플라이언스 차원에서 정보보안 관련 법률 관련사항에 대한 통합 정보를 제공하여 자체적으로 준수사항을 점검 관리할 수 있도록 하고, 보안 정책 및 보안 프로세스 등과 보안 컴플라이언스를 매칭하여 운영할 수 있도록 한다.

논문의 구성은 다음과 같다. 2장에서는 관련연구로 IT GRC와 IT 내부통제, 지능형 사이버보안 기술 동향에 대해 살펴보고, 3장에서는 기존 IT 보안 내부통제시스템의 문제점 및 요구사항을 기술한다. 4장에서 IT 보안 내부통제시스템의 개선방안 대해

설명한다. 그리고 5장에서 금융회사에 적용한 사례를 소개하고, 6장에서 결론을 맺는다.

2. 관련연구

2.1 IT GRC

IT GRC는 거버넌스, 리스크관리, 컴플라이언스로 구성되어 있다. IT GRC 프로세스 모델은 IT 거버넌스, 리스크관리, 컴플라이언스 세 가지가 결합되어 분석을 진행하고 통제하는 모델이다[2]. 이 모델은 IT 거버넌스는 ISO/IEC 38500:2008[3]; 리스크관리는 COSO ERM(Committee of Sponsoring Organization Enterprise Risk Management) 프레임워크[4], 마지막으로 IT 컴플라이언스는 일반 모델을 따르고 있다.

2.2 IT 내부통제

COBIT(Control OBjectives for Information and related Technology)은 오늘날 IT가 기업의 비즈니스 전략에 중요한 요소로 위상이 높아짐에 따라 조직의 경영진과 업무 프로세스 책임자들에게 IT에 수반되는 위험을 이해시키고 관리할 수 있도록 도움을 주는 IT통제 프레임워크로 현재 COBIT 5가 발표되었다[5]. COBIT 5는 기업이 정보와 기술 투자를 최적화하는 일곱 동인들의 전체적인 세트를 기반으로 효과적인 거버넌스 및 관리 프레임워크를 구축하고 이해 관계자의 이익을 위해 사용할 수 있도록 다섯 가지 원칙을 함께 제공한다.

내부자 보안사고를 100% 막는 것은 현실적으로 어려운 문제이다. 그러나 내부자 보안사고를 사전에 예방하고 사고 발생 초기 신속한 대응이 가능하도록 내부통제를 강화한다면 위험을 상당히 줄일 수 있다. 내부자 위협의 특성상 단순 솔루션 도입이 아닌 종합적인 측면에서 내부통제 강화 전략을 위한 접근이 필요하다[1].

2.3 개인정보 접속기록 및 오·남용 내부통제

개인정보보호법 제29조 (안전조치의무)에서는 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다고 되어 있고, 제31조 (개인정보 보호책임자의 지정)에서는 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축을 개인정보 보호책임자의 업무로 규정하고 있다. 개인정보보호법 시행령 제30조 (개인정보의 안전성 확보 조치)에서는 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치를 하여야 한다고 규정되어 있고, 개인정보의 안전성 확보조치 기준 및 해설서 제8조 (접속기록의 보관 및 위·변조방지)에서는 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무(열람, 수정, 삭제, 인쇄, 입력 등) 등의 접속기록을 최소 6개월 이상 저장하고 정기적으로 확인·감독 하여야 한다고 규정되어 있다.

개인정보 접속기록을 생성하기 위해서는 개인정보 접속기록을 남기도록 개인정보처리시스템의 소스를 직접 수정하는 방법과 웹기반의 개인정보처리시스템인 경우에 한해 개인정보 접속기록을 생성하는 에이전트를 설치하여 자동으로 남기는 방법이 있고, 웹 및 C/S 등 다양한 개인정보처리시스템에 대하여 기존 개인정보처리시스템의 소스나 설정을 변경하지 않고 네트워크 기반으로 개인정

보 접속기록을 생성하는 어플라이언스를 설치하는 방법이 있다. 또한, 개인정보에 대한 오·남용을 시스템 기반으로 내부통제하는 방법은 개인정보 오·남용에 대한 상시모니터링 시스템을 구축하는 방법이 있다.

2.4 지능형 사이버보안 기술 동향

최근 보안 위협들은 기업의 주요 정보 유출, 천문학적 규모의 물리적 피해를 야기할 수 있는 산업제어시스템 마비, 전쟁행위 등의 사이버 공격으로 이어져 사회.국가적 위협으로 대두되고 있다. 이러한 발전된 보안 위협에 대한 새로운 방어 패러다임으로 지능형 보안이 최대의 이슈로 등장하고 있다. 지능형 보안의 개념은 APT(Advanced Persistent Threats) 공격과 같은 알려지지 않은 치명적인 공격에 대응하기 위해, 주요 IT 기반 시설의 네트워크, 시스템, 응용 서비스 등으로부터 발생하는 데이터 및 보안 이벤트 간의 연관성을 분석하여 보안 지능을 향상시키는 차세대 보안 정보 분석 패러다임으로 해석되고 있다[6].

과거 사이버 위협 방어 기술의 핵심 기술은 알려진 공격에 대한 공격 시그니처 데이터베이스를 확보하고 고성능 패턴매칭 알고리즘을 구현하여 얼마나 빨리 비교할 수 있느냐에 관심을 갖었다. 복합 데이터 처리 기술의 발달로 내부 망에서 발생하는 다중 소스의 누적 데이터에 대한 특성인자를 정의하고 연관성 분석을 할 수 있는 보안 기술로서 빅데이터를 활용한 보안 분석 기술이 부각되고 있다[7].

하지만 국내외 모두 대용량 데이터 처리 기술을 도입하고 있지만 오픈 빅데이터 기술을 SIEM(Security Information & Event Management)에 적용한 연구는 아직 부족한 실정이다.

3. IT 보안 내부통제시스템의 문제점 및 요구사항

3.1 보안 프로세스에 대한 통합 관리 부족

정보보안 프로세스는 크게 정보보호 프로세스와 개인정보보호 프로세스 및 이와 관련된 정보보안 서비스 프로세스로 구분할 수 있다. 보안 거버넌스 차원의 다양한 보안 프로세스는 크게 정보보호 프로세스와 개인정보보호 프로세스가 개별적으로 관리 운영되고 있고, 각각의 프로세스들도 상호 연관성에 따라 유기적으로 통합 관리되어야 함에도 불구하고 대부분 필요에 따라 구성되어 개별적으로 관리 운영되고 있다. 또한, 정보보안 서비스 프로세스도 정보보호 및 개인정보보호 프로세스와 유기적으로 연계 운영되어 보안 업무 창구가 일원화되도록 해야 한다. 예를 들어 개인정보보호 프로세스인 개인정보처리시스템 관리 및 개인정보영향평가 관리는 정보보호 프로세스인 IT 자산관리와 연계되어 관리되어야 한다. 또한, 정보보안 서비스 프로세스인 보안정책도 정보보호 및 개인정보보호 각각의 프로세스와 연련되어 관리되어져야 한다.

3.2 보안 모니터링에 대한 통합 관리 부족

IT 리스크를 관리하기 위한 지능형 사이버보안이 빅데이터 기반의 SIEM 형태로 발전되고 있으나 아직 다음과 같은 문제점은 안고 있다. 첫째, 통합로그 관리에서 시작하여 SIEM 으로 발전하여 APT 등 보안 취약점 및 정보유출 등 컴플라이언스 등으로 모니터링 범위를 확대하고 있지만, 다양한 보안 프로세스에 나오는 보안 거버너스 현황을 모니터링하는 수준은 아직 부족하다. 둘째, 보안 취약점 및 정보유출 등에 대한 경험 기반의 시나리오

가 부족하여 로그를 쌓아 놓고는 있지만 의미있는 분석이 현실적으로 부재하다. 많은 조직들이 고가의 외산 SIEM 솔루션을 도입 한 이후에도 단편적인 로그 수집과 모니터링 시나리오의 부재로 IT 리스크 관리 수준이 매우 낮은 상태이다. 셋째, IT 리스크 관리를 위한 통합 모니터링을 효율적으로 관리.운영하기 위한 기능적, 비기능적 요구사항에 대한 만족을 못 시키고 있다. 다양한 로그를 조합하여 새로운 시나리오를 만드는 동적 시나리오 기능과 오픈 빅데이터 플랫폼을 사용하여 비용 효율적으로 확장성 및 안전성 등 비기능적인 요구사항에 충족이 필요하다.

3.3 정보보안 컴플라이언스에 대한 통합 관리의 어려움

초창기 정보보호 규제 방식은 글로벌 표준인 Best Practice를 기반한 기업의 자율 규제 방식(Self Regulation)이 주를 이루었다. 그러나 2000년 중반 이후 각종 보안사고가 급속히 증가하고 이에 따른 피해 규모가 커지면서 국가가 해당 기업을 직접 규제하는 방식으로 전환되게 되었다. 이러한 정보보호 규제 방식의 변화는 기업에게 정보보호 컴플라이언스가 더 이상 선택이 아닌 필수 사항으로 기업의 비즈니스 연속성을 보장하는데 반드시 정보보호 컴플라이언스는 해결해야 하는 과제로 인식하게 되었다. 그러나 기업의 입장에서 정보보호 컴플라이언스를 효과적으로 대응하는데 다음과 같은 현실적인 어려움으로 인해 정보보호 컴플라이언스는 기업에게 새로운 도전이라 할 수 있다[8].

- 정보보호 관련 법률 등이 규제 기관별로 다양하게 존재하고, 각 요구사항 간 유사 또는 중복 적용 부분 존재
- 정보보호 관련 법률 등의 요구사항을 적절하게 구현하는데 참조할 수 있는 Best Practice 등 부족
- 제한된 인력과 비용으로 모든 정보보호 컴플라이언스의 요구사항들을 일일이 대응하는데 현실적인 한계

4. IT 보안 내부통제시스템의 개선방향

본 장에서는 IT 보안 내부통제시스템의 문제점을 해결하고 요구사항을 수용하기 위한 개선방향으로 IT GRC 기반 IT 보안 내부통제시스템을 제시한다.

4.1 IT Governace 관점의 보안 프로세스 통합

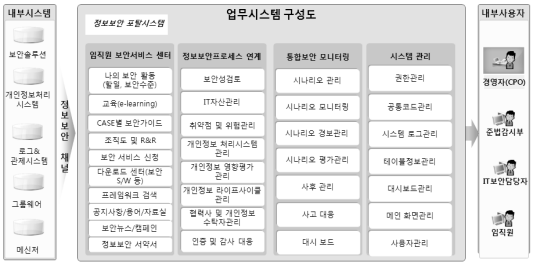


그림 1. 정보보안 프로세스 통합
Figure 1. Integration of security processes

<그림 1>과 같이 정보보호 프로세스는 IT 자산관리, 보안성검토, 취약점 및 위험관리 등이 있으며, 개인정보보호 프로세스는 개인정보처리시스템 관리, 개인정보영향평가 관리, 개인정보라이프사이클 관리, 수탁사 및 협력사 관리 등이 있으며, 공통적인 프로세스로 인증 및 감사 대응 등이 있다. 정보보안 서비스 프로세스는 보안정보공유, 보안활동, 보안솔루션, 보안교육, 보안서비스, 보안정책, 보안조직 등으로 구성된다.

<그림 1>의 정보보안 프로세스는 ISO27001(혹은 ISMS: Information Security Management System) 와 PIMS(Personal Information Management System 혹

은 PIPL: Personal Information Protection Level)의 프로세스를 포함하고 정보보안 프로세스의 수행 결과만으로 ISO27001(혹은 ISMS)와 PIMS(혹은 PIPL)의 인증을 위한 산출물을 자동으로 생성할 수 있도록 하여 인증을 위한 추가적인 업무를 최소화하여 정보보안 업무 효율성을 높인다.

4.2 IT 리스크 관점의 보안 통합모니터링

IT 리스크를 관리하기 위한 보안 통합모니터링은 <그림 2>와 같이 빅데이터 기반의 SIEM을 인프라로 구성하고 APT 등의 보안 취약점과 정보유출 뿐만 아니라 <그림 1>에서와 같이 다양한 보안 프로세스에 나오는 정보보안 거버너스 현황을 모니터링하여 보안 취약점, 정보유출, 정보보안 거버넌스 현황 등 정보보안의 전 영역을 통합적으로 모니터링 관리한다.

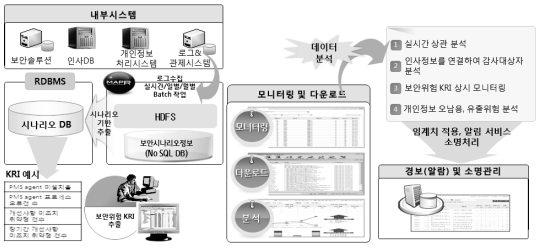


그림 2. 빅데이터 기반의 보안 통합모니터링
Figure 2. Integrated security monitoring based on bigdata

빅데이터 기반의 통합모니터링은 보안 취약점과 정보유출 및 보안 거버넌스와 관련된 다양한 로그 수집과 이러한 로그를 기반으로 한 모니터링 시나리오를 콘텐트로 다양한 IT 리스크를 관리한다. 기존 시스템에서는 보안 취약점과 정보유출을 일부 혹은 별도의 방식으로 모니터링하여 외부 공격에 의한 유출인지 내부자에 의한 유출인지 직시적인 확인이 불가능 했지만 통합 모니터링에서는 보안 취약점과 정보유출을 연계 분석하여 정보유출의 원인을 직시적으로 확인할 수 있다.

정보유출을 분석하기 위해서는 다양한 시나리오를 발굴할 수 있는 방법이 정의되고 이러한 방법으로부터 다양한 시나리오를 발굴, 관리하고 모니터링해야 한다. 기존 연구에서는 시나리오를 발굴하는 방법이 거의 연구되어 있지 않고 시나리오를 위한 소스 로그의 대상을 정의하고 개인정보 라이프 사이클별 시나리오 예시와 이를 스코어링하는 방법은 제시하고 있으나 분석을 위한 시나리오를 발굴하는 방법을 제시하지 않고 있다[9]. 갈수록 늘어나는 정보유출 방법 및 정보보호 솔루션 등을 고려할 때 이미 정의된 시나리오 뿐 만아니라 향후 비즈니스 변화에 능동적으로 대처할 수 있도록 시나리오를 발굴할 수 있는 방법을 정의하고 이를 사용자가 쉽게 활용할 수 있는 기능이 필요하다. 이를 위해서 본 논문에서는 <표 1>과 같이 정보유출 시나리오 발굴 방법을 제시한다.

표 1. 정보유출 시나리오 발굴 방법
Table 1. Method for developing the scenario of information leakage

구분 유형	구분 설명
Who	사용자 유형을 일반사용자, 퇴직자, 장기휴가자, 권한예외자, 중요보직자, 중요정보보유자 등으로 구분
When	사용 시간대를 근무시간, 근무 외 시간, 휴일, 휴가중 등으로 구분
How (접속유형)	개인정보 접속 유형을 개인정보 조회, 출력, 다운로드 등으로 구분
How (정보보호)	정보보호 해제 방법을 DRM, DLP, VPN, 출력보안, 공유폴더, 메신저해제, 방화벽해제, 웹접속해제 등으로 구분
How (정보반출)	정보반출 방법을 외부메일, 저장매체 기록, 출력, 노트북 반출, 웹게판/웹하드 업로드, 메신저 전송, FTP 전송, P2P 전송, 공유폴더 보관 등으로 구분

제시한 정보유출 시나리오 발굴 방법을 통하여 대상 개인정보시스템으로부터 누가, 언제, 어떻게 개인정보를 획득하고, 어떻게 정보보호를 우회하여, 어떻게 정보를 반출했는지에 대한 정보유출 위협 시나리오를 체계적으로 발굴할 수 있다. 이러한 정보유출 위협 시나리오를 모니터링할 수 있는 핵심위험지표(KRI : Key Risk Indicator)를 발굴하여 모니터링 결과에 대해 분석, 알림 및 소명 관리한다.

모니터링 대상자의 위험도를 평가하여 블랙리스트 형태로 집중 관리하는 것이 내부통제 위험을 관리하는 효율적인 방법이다. 위험지표별로 임계치를 기반으로 정상, 주의, 위험을 발생시키고 발생된 위험을 개인별, 조직별, 시나리오별로 평가하여 가장 위험한 개인, 조직, 시나리오의 순위를 정할 수 있다. 특히, Top N에 해당되는 개인을 블랙리스트로 집중 관리하여 위험을 사전에 예방한다. Top N 시나리오는 조직에서 가장 많이 발생하는 정보보안 이상징후로서 예방 차원의 교육 및 실증 보안감사의 방향을 설정하는데 활용된다.

4.3 IT 컴플라이언스 관점의 정보보안 컴플라이언스 통합

조직에 맞는 다양한 정보보안관련 컴플라이언스를 등록관리, 자가점검 및 현황관리, 체크리스트 관리, 준수현황 관리, 관련법률 변경관리 등 컴플라이언스 통합 및 컴플라이언스 관련 기능을 통합한다. ISMS, PIPL(Personal Information Protection Level), 개인정보보호법 등 다양한 정보보안관련 컴플라이언스 통제항목을 통일된 형태로 등록관리하고 체크리스트를 관리하여 정보보안 컴플라이언스에 대한 통합된 뷰를 제공한다. 또한, 이러한 체크리스트는 업무프로세스와 결합하여 업무를 수행할 때 해당 컴플라이언스를 체크하도록 하여 의도하지 않는 컴플라이언스 위반을 최소화 할 수 있다.

5. IT 보안 내부통제시스템의 금융회사 구축예시

금융회사의 구축 사례를 통해 제안하는 IT 보안 내부통제시스템의 적용시 장점과 개선이 필요한 사항 등을 확인한다. 해당 보험사는 고유의 보험업무를 위한 기간계 시스템과 고객 및 경영 분석을 위한 DW, CRM 등 다양한 분석 시스템을 운영하며 많은 시스템에 개인정보를 보유하고 있다.

모든 정보보안 업무를 정보보호, 개인정보보호, 정보보안서비스 업무로 분류하고, 정보보안 프로세스로 통합 정의하여 각 업무들이 유기적으로 운영되도록 하였다. 정보보안 사용자는 임직원, 보안담당자, 준법담당자, 임원 4가지 사용자로 구분하여 보안 관련된 모든 업무를 단일 시스템으로 통합 운영하도록 했다.

정보보안 통제위반 모니터링과 정보유출모니터링을 중심으로 보안 통합모니터링을 구축했다. <그림 3>과 같이 모니터링 소스는 응용프로그램 별 개인정보접속기록, 메일보안, DLP, DRM, 방화벽, 서버보안, APT솔루션 등으로 빅데이터 플랫폼을 활용하여 원본 데이터 및 분석용 데이터를 구축함으로 향후 추가되는 응용프로그램 및 보안솔루션 등의 로그에 대해서 무정지 확장성을 제공하고 정의된 시나리오뿐만 아니라 정의되지 않은 이상징후도 분석 가능하도록 하였다.

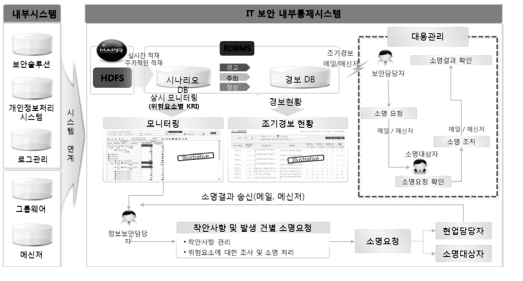


그림 3. 통합모니터링 흐름도
Figure 3. Integrated monitoring flowchart

〈표 1〉의 모니터링 시나리오 발굴 방법을 기반으로 정보유출 시나리오를 발굴 및 구현했고 〈표 2〉는 구현한 정보유출 모니터링 시나리오 예시를 보여준다.

표 2. 정보유출 모니터링 시나리오 예시
Table 2. Examples of the scenario of information leakage

영역	모니터링 시나리오
개인정보보안	근무일 사용자 평균대비 고객정보 출력/다운로드 건수 급증
	휴일 사용자 평균대비 고객정보 출력/다운로드 건수 급증
	PC별 개인정보파일 보유건수 급증
	퇴사자가 퇴사이후 조직 내부 네트워크 접근 시도 탐지
	퇴사자의 개인정보시스템 접속기록 탐지

통합모니터링은 지표(KRI : Key Risk Indicator)설정, 모니터링, 경보 및 알림, 대응관리 순서로 진행된다. 〈그림 4〉와 같이 지표설정은 시나리오 영역관리, 지표정보등록, 소명정보설정, 담당자지정, 임계치설정, 지표목록관리의 업무 흐름을 갖는다.

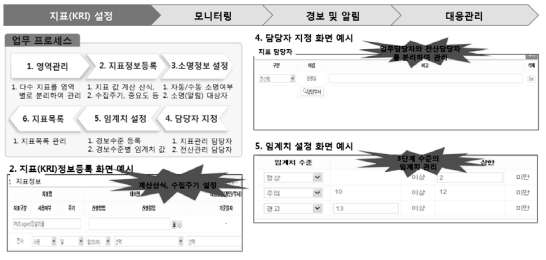


그림 4. 지표(KRI)설정 흐름도
Figure 4. KRI setting flowchart

〈그림 5〉는 모니터링화면을 구성하기 위해 모니터링 대상 테이블 정보 메타관리, 컬럼정보 메타데이터 관리, 지표별 테이블선택, 화면메타설정, 검색조건 메타설정, 모니터링 순으로 업무 흐름이 구성된다.

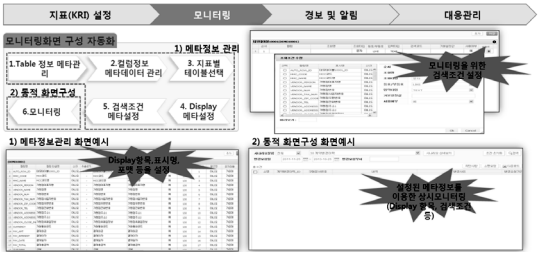


그림 5. 모니터링 화면 구성 흐름도
Figure . Monitoring display setting flowchart

〈그림 6〉은 경보 및 알림을 위한 업무 흐름으로 지표설정, 임계치설정, 알림대상설정, 경보발생, 메일/SMS알림, 경보 및 알림 모니터링 흐름으로 진행된다.

그림 6. 경보 및 알림 흐름도
Figure . Wanning and notice flowchart

〈그림 7〉은 경보 및 알림에 대한 대응관리를 위한 업무 흐름으로 경보현황, 소명요청, 메일/SMS 알림, 소명결과, 메일/SMS 알림, 소명결과 확인 흐름으로 진행된다.

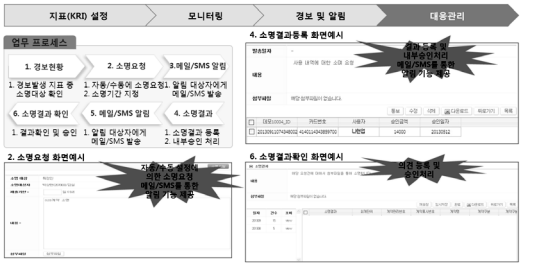


그림 7. 대응관리 흐름도
Figure . Response flowchart

PIMS, ISMS를 포함하는 금융IT 보안 컴플라이언스를 기반으로[10], 통합 IT 보안 컴플라이언스를 관리하고 이를 모든 사용자가 검색하여 업무에 참고하고 변경관리 할 수 있도록 IT 보안 컴플라이언스 프레임워크를 구축했다.

6. 결론

본 논문에서는 IT 내부통제 관리 소홀로 발생할 수 있는 정보보안 통제위반 및 내부정보유출을 사전 예측 혹인 사후 적발하기 위하여 거버넌스 관점의 정보보안 통합 프로세스, 리스크 관리 관점의 정보보안 위협 시나리오 기반의 통합모니터링, 컴플라이언스 관점의 통합 IT 보안 컴플라이언스를 포함하는 IT 보안 내부통제시스템을 제안했다.

제안된 IT 보안 내부통제시스템의 기대효과는 다음과 같이 세 가지로 요약할 수 있다.

첫째, 정보보안 프로세스가 통합되어 보안관련 모든 업무 현황을 즉시 파악 할 수 있고, ISMS 및 PIPL 등 정보보안 관련 인증을 위한 산출물을 수일 내에 작성할 수 있다.

둘째, 빅데이터 기반의 통합 모니터링을 통하여 이상징후 발생시 관련된 추가분석 및 리포팅 시간을 수십분으로 단축되고, 사전에 정의된 이상징후 뿐 만 아니라 사전에 알려지지 않은 패턴들도 분석하여 정보로 활용할 수 있고, IT 자산 및 사용자 정보 등 기존 정보와 연계하여 추가 분석이 용이하다.

셋째, 정보보안 관련 컴플라이언스 통합 관리하여 사용자가 쉽게 검색 및 활용하여 의도하지 않은 컴플라이언스 위반을 사전에 방지한다.

제안된 IT 보안 내부통제시스템의 효율성을 정량적으로 입증하는 추가적인 연구가 필요하다.

References

[1] S. H. Hong, *Strategies for strengthening of IT internal control over financial*, Isssue Report, 2011-008, Financial Security Agency, 2011.

[2] N. Racz, A. Seufert, and E. Weippl, *A process model for integrated it governance, risk, and compliance management,* in Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), pp. 155–170, 2010.

[3] Electronic Publication: C. McClean, K. McNabb and A. Dill, *The GRC technology puzzle: Getting all the pieces to fit,* 2009. Accessed 10 January, 2010.

[4] M. Rasmussen, *Hand in Hand,* Business Trends Quarterly, Vol. 2:2, pp. 44–46, May 2007.

[5] Electronic Publication: *Cobit 5.0,* at http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx.

[6] D. H. Kim, *Big data environments, evolving intelligent log management platform security information / event management (SIEM) trends*, NIPA weekly technology trends, 2013.

[7] J. H. Kim, S. H. Im, I. G. Kim, H. S. Jo, B. G. No, *Cyber security technology trends using Big Data*, ETRI, Electronics and Telecommunications Trends Vol. 28, No. 3, 2013.

[8] Y. T. Kim, *Information security and privacy management framework introduction,* Issue Report, vol. 2011-017, Institute of Financial Security, 2011.

[9] Y. G. Chae, *A study on the PIMS based methodology for monitoring to prevent leakage of personal information in the banking industry,* Master Thesis, Dongguk University School of International and Information, 2014.

[10] K. S. Kim, *Financial IT Security Compliance Guide*, Financial Security Agency, 2012. 12.

IT GRC 기반의 IT 보안 내부통제시스템

유영록[1], 서성채[2], 이상준[3], 김병기[2]
[1] *씨에이에스*
[2] *전남대학교 전자컴퓨터공학부*
[3] *전남대학교 경영학부*

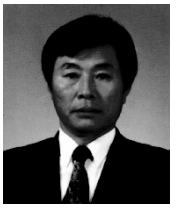
요 약

본 논문에서는 관리적, 기술적, 물리적 내부통제 강화 방안을 수용하면서 전사적 관점의 내부통제를 위한 IT 보안 내부통제시스템을 제시한다. IT 보안 내부통제시스템은 거버넌스 관점에서 IT 보안 프로세스를 정보보호 프로세스, 개인정보보호 프로세스, 정보보안 서비스 프로세스로 분류 및 통합 관리한다. 리스크 관리 관점에서 정보보안 통제 위반 및 내부정보 유출을 통합 모니터링하기 위하여 IT 관련 로그를 빅데이터 기반으로 통합하고 정보보안 위협 시나리오에 대한 핵심위험지표(KRI)를 모니터링하고 모니터링 결과 이벤트를 분석, 알림, 소명한다. 컴플라이언스 관점에서 IT 보안 관련 법.규정을 통합 관리하여 자동화되고 통합된 IT 보안 내부통제 환경을 제공한다. 금융회사 구축사례를 통하여 제안된 IT 보안 내부통제시스템이 다양한 조직의 IT 보안 내부통제를 위한 자동화되고 효율적인 내부통제환경을 제공함을 확인했다.

Young-Rok Yu have completed the Ph.D. course in the Deparatment of Computer science from Chonnam National University in 2001. He received the M.S. degree in the Deparatment of computer science from Chonnam National University in 1998. He has worked for CAS Inc. in Seoul, Korea. His research interests are in GRC(Governance, Risk management, Compliance), software security, software engineering.
E-mail address: yryu@casit.co.kr

Seong-Chae Seo received his Ph.D. in computer science from Chonnam National University in 2006. He received the M.S. degree in computer science from Chonnam National University in 1997. He is currently an post-doctoral researcher of the Deparatment of computer science in the Chonnam National University in Gwangju, Korea. His research interests are in software analysis, software engineering, software quality, software security, software process, UML.
E-mail address: scseo@jnu.ac.kr

Sang-Joon Lee received the B.S., M.S. and Ph.D. degrees in the Department of Computer Science and Statistics from Chonnam National University in 1991, 1993 and 1999, respectively. From 1995 to 2006, he was in Seonam University and Shingyeong University as assistant professor. Since 2007, he has been with Chonnam National University as a full professor in the School of Business Administration. His current research interests include Management Information Systems, Software Engineering, IT Service and Ubiquitous Business. He is a life member of the KKITS.
E-mail address: s-lee@jnu.ac.kr



Byung-Ki Kim received his Ph.D. in mathmatics from Chonbuk National University in 2000. He was chairman of Korea Information Process Science(KIPS) in 2007. He is currently a full professor of computer science in the Chonnam National University in Gwangju, Korea. His research interests are in software analysis, software engineering, software quality, software security, software process, software testing.
E-mail address: bgkim@jnu.ac.kr