www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.3.125

금융IT 보안조직 역량강화를 위한 핵심성과지표(KPI) 도출에 관한 연구

Developing key Performance Indicators for Financial IT Security

장성옥(Sung Ok Jang)*, 임종인(Jong In Lim)**

초 록

IT비즈니스의 전략적 연계가 강화됨에 따라 금융서비스에서 IT의존도는 높아지고 있다. 안전하고 신뢰된 금융서비스를 제공하기 위해서는 지속적인 정보보호활동을 수행해야 하며, 이에 관한 조직의 정보보호 업무성과 측정은 의사결정 및 경영지원 측면에서 유용하다. 본 논문은 정보보호관리체계(K-ISMS)와 금융IT 부문 정보보호 업무 모범규준의 평가기준을 기반으로 핵심성공요인(CSF, Critical Success Factor)과 핵심성과지표(KPI, Key Performance Indicator)를 도출한다. 이는 정보보호정책 준수에 유의한 영향을 주는 핵심성과지표를 판별하는 논리적 근거를 제공하며, 금융IT 정보보호 역량을 강화하기 위한 정책을 수립하기 위한 기초자료로 활용할 수 있다.

ABSTRACT

As a reinforcing strategic-alignment of IT business, Financial Service becomes more rely on IT systems. It needs to continuous information security activities to provide a secure and reliable finance service. Performance measurement of information security activities can be useful for decision and management support. The purpose of this study is to derive CSF(Critical Success Factor) and KPI(Key Performance Indicator) based on K-ISMS, Financial IT Information Security Standards. Providing a rationale can be used to determine key performance indicators, which are utilized as basic data for establishing security policies for financial IT security competency.

키워드 : 핵심성과지표, 금융IT 보안, 정보보호정책
Key Performance Indicator, Financial IT Security, Information Security Policy

* CIST(Center for Information Security and Technologies), Korea University
** Corresponding Author, CIST(Center for Information Security and Technologies), Korea University (E-mail : jilim@korea.ac.kr)
2013년 07월 12일 접수, 2013년 07월 23일 심사완료 후 2013년 08월 5일 게재확정

1. 서 론

정보기술이 하나의 기업 경쟁력으로 인식되면서 정보의 획득, 저장, 가공, 분석, 활용에 이르는 다양한 정보시스템으로 활용되고 있다. 최근 정보통신기술(ICT, Information and Communications Technology)을 기반으로 고부가가치의 창조경제를 실현하겠다는 정부의 기조도 이러한 시대적 흐름을 반영하고 있다. 그러나 현재까지의 국내 ICT기술은 정보의 획득과 전달, 가공 및 활용에 측면에만 초점이 맞추어져 있었다. 정보통신기술 발달에 따른 매체의 보급과 네트워크 인프라의 확충으로 누구든 언제어디서나 인터넷에 접속가능한 시대가 되었으나 이에 준하는 정보보호기술이나 인식의 수준은 그에 미치지 못하는 실정이다[15]. 최근의 3.20 사이버테러와 이전에 발생한 2011년 3.3 DDoS, 2009년 7.7 DDoS 등은 사회정치적 의도를 가지고 공격한 사이버공격으로서 향후 정보통신기술과 관련시설을 이용한 해킹에 대한 위협은 더욱 높아만 가고 있다.

특히, 국가 및 공공기관을 대상으로 한 사이버공격 외에도 대표적인 민간분야라 할 수 있는 금융권은 대국민 서비스를 제공한다는 점과 민주사회의 '자본'을 상징하고 있다는 점에서 높은 수준의 대국민 신뢰가 필요하다. 과거의 금융서비스는 직원과 금융소비자가 지점창구에서 면대면(face-to-face) 방식으로 제공되어 왔으나 현재는 비대면거래 방식인 컴퓨터, 모바일 등의 전자적장치를 이용한 전자금융서비스가 확대되어 제공되고 있다. 2012년 12월 금융서비스의 전달채널별 업무처리 비중을 볼 때 비대면거래는 87%를 차지(CD/ATM 39.8%, 텔레뱅킹 13.4%, 인터넷뱅킹 33.8%)하고 있음을 고려할 때, 앞으로 금융권에서 ICT의존도는 더욱 높아질 것으로 예상된다[28].

정보보호의 목표는 외부자의 의도적인 침해사고로부터 조직의 정보자산을 보호하기 위한 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 3개 영역의 보안목표를 확보하기 위한 기술이나 방법으로서 인식되어 왔으나 최근의 정보보호는 ICT의 서비스와 영역이 다양화됨에 따라 기존의 전통적인 보안목표 외에도 인증(Authentication)이나 부인방지(Non-repudiation)의 추가적인 보안목표를 달성해야함을 정의하고 있다[19]. 조직의 보안목표를 달성하기 위한 세부 실행방안으로 NIST (National Institute of Standards and Technology)에서는 보안통제의 영역을 구분하여 관리적, 기술적 통제영역의 지속가능한 프로세스의 개선과 모니터링을 통해 정보보호의 수준을 향상시킬 수 있음을 가이드하고 있다[22]. 즉, 정보보호의 수준 향상은 관리적, 기술적, 물리적 통제영역 내에서 지속적인 개선과 개인과 조직의 보안인식 수준향상을 통해 달성될 수 있다.

금융권에서는 최근 발생한 3.20사이버테러에 대비하여 학계 및 업계의 IT전문가들에 의한 금융전산 보안 강화종합대책을 수립하여 발표하였다. 강화 대책의 주요 추진방향과 내용은 관리적, 기술적 영역에 걸쳐 금융IT 인프라 보안강화, 금융IT 보안인력・조직 역량 강화, 금융회사 위기대응 체계 개선, 금융IT 검사・감독 내실화, IT분야 내부통제 강화, 금융정보보호 교육 및 홍보강화를 중점으로 두고 있다[2]. 이처럼 정보보호조직을 구성하고 운영하는 것은 관리적 보안통제영역에서 원활한 IT비즈니스를 지원하기 위한 경영상의 문제로도 다뤄진다.

본 논문은 이와 관련하여 금융IT 정보보호 역량강화를 위해 정보보호활동과 비즈니스 전략적 연계의 관점에서 성과측정을 위한 방법으로 성과지표에 가장 큰 영향을 미치는 핵심성공요인(CSF)이 무엇인지 식별하고, 연구가설에 대한 후보성과지표의 신뢰도, 요인 및 회귀분석 통해 핵심성과지표를 개발한다. 연구의 범위로서 보안목표와 보안통제영역에 대한 세부항목인 평가기준(K-ISMS)과 금융IT 부문 정보보호 업무 평가기준으로 한정한다. 궁극적으로 성과지표상의 변동을 측정오차나 임의의 변화를 제외한 설명 가능한 요인 중에서 정보보호활동 프로세스관리 및 모니터링(monitoring)을 지원할 수 있는 성과지표를 개발한다.

2. 관련 연구

2.1 IT 균형성과표(IT BSC, Balanced Scorecard)

1992년 Kaplan과 Norton에 의해 제안된 BSC는 재무적 성과와 비재무적 성과측정을 통한 전략실행의 도구이자 조직의 의사소통도구 및 무형자산의 관리도구로서 정의된다[12]. BSC가 제시하는 네 가지 관점은 각각 인과관계를 가지면서 기업의 재무적 지표와 비재무적 지표간 연결 관계를 보여주어 기업의 전략을 하부단위로 연계시키는 방향을 제시할 수 있다. Kaplan and Norton[11]은 BSC의 성과지표간의 인과관계를 다음과 같이 가정하고 있다. 조직의 학습 및 성장관점의 성과측정치는 내부 프로세스의 성과측정치에 영향을 주고, 내부 프로세스의 성과측정치는 고객관점의 성과측정치에 영향을 주며, 고객관점의 성과측정치는 재무관점의 성과측정치에 영향을 준다는 것이다[11]. 따라서 이들 측정지표들 간의 인과경로는 궁극적으로 재무적 관점으로 연결된다. 이러한 과정은 곧 전략이 인과관계에 대한 가설이 될 수 있음을 확인할 수 있다. 인과관계는 전략지도(Strategy Map)를 이용하여 각 관점별 성과측정구조를 설명가능하며, 조직의 무형자산이 유형의 고객 및 재무관점의 성과로 변환되는 과정을 설명해주고 있다. BSC의 전략지도에서는 존재하는 검증 가능한 인과관계는 전략상에서의 가설을 통해 설명될 수 있어야 한다. 전략상의 가설에서는 목표하는 성과지표를 이끌어내는 선행지표의 활동들을 명확히 해야할 필요가 있다[10]. 이러한 가설은 선행지표에 해당하는 비재무적 관점의 지표에 의해 후행지표인 재무적 관점의 지표가 예측가능하다는 점에서 중요하다. 따라서 측정치간에 인과관계가 존재한다는 가설에 대한 진위여부는 타당성 검증을 검증함으로써 판별할 수 있다. 최근에는 BSC의 궁극적 목표인 전략개발을 도와줄 수 있는 각 관점별 성과간의 가설적 인과관계를 계량적으로 추정하여 이에 대한 타당성을 검증하는 연구가 이루어지고 있다[27].

지금까지 IT조직의 활동과 관련하여 조직의 목표와 전략적 연계의 관점에서 BSC를 이용한 생산성과 성과측정에 대해서는 중요하게 인식해 왔으나, 기존 프로세스 관점에서 정보기술(IT)과 기업의 재무적 성과와 거리가 멀기 때문에 이에 따른 영향이나 효과를 측정하기란 쉽지 않다[23]. 특히 기존의 연구에서는 정보기술(IT) 예산과 같은 변수를 시장 점유율과 같은 기업의 성과변수에 직접적으로 연결하려는 연구방법들은 유의한 통계적 결과를 얻지

못한다고 역설한다[1, 4].

그러나 BSC를 IT 성과측정에 도입하기 위한 시도는 다양하게 이루어져 왔다[12]. 이들의 연구는 IT와 관련된 투자 수준이 기업의 생산성이나 수익성과는 직접 관련이 없다는 IT의 생산성을 비즈니스와의 연계에 의한 IT BSC구축이라는 방법으로 극복하고자 하였다. 즉 표준화된 IT BSC는 비즈니스 기여 관점을 통해 전사적인 BSC와 연계되어 성과를 측정하게 된다. IT BSC는 이러한 BSC의 개념을 IT조직의 활동에 적용하여 IT가 가지는 정량적·정성적 요인에 대한 관점과 평가지표를 제시한다. IT BSC는 IT가 투자에 대한 효과를 계량적으로 측정하기 어렵다는 점에서 그 성과를 측정하고 평가할 수 있는 프레임워크라고 볼 수 있다[3]. 특히, Steven[26]은 비즈니스 BSC에서 IT 거버넌스 전략, 그리고 개발과 운영에 이르는 단계적인 연계 BSC의 개발을 제안하였다[26]. 기존 문헌연구들은 IT BSC에 대한 각 연구자들의 관점에 따라 비즈니스의 목표를 설정하고 있고, 궁극적으로 기업의 전략을 지원하기 위한 IT 조직 활동에 대한 성과평가 목표와 상세지표들을 제시하고 있다. 대부분의 연구에서는 조사된 관점들과 핵심성공요인(CSF), 세부 성과지표(KPI)지표간의 인과관계 규명을 통해 실제 IT조직에 대한 성과지표에 대한 연구들을 수행해왔다. 이렇듯 기업의 전략을 지원한다는 IT BSC관점에서 정보보호활동에 대한 성과측정방법은 정의되어야 할 필요성이 있다.

2.2 IT부문 성과지표 도출연구

기존의 IT부문 내에서 소프트웨어개발 성과측정을 위해 후보성과지표를 도출하기 위한 연구로 Haley[5], Kraut[16], Park[24] 등이 있으며, <Table 1>에서 연구자들은 소프트웨어 개발업무에 있어서 생산성 향상을 위한 가장 효과적인 성과지표로서 생산성(양)과 품질을 가장 핵심적인 성과지표로서 선정하였다[5, 16, 24]. 정보통신분야에서의 최근 연구로는 방송통신 연구성과 측정지표 및 척도 도출에 관한 유사연구가 진행되었다[18]. 정보보호 활동에서의 성과지표에 대한 연구는 Martin[20]이 제안한 성과 매트릭스를 기반으로 보안정책의 준수여부를 정성적·정량적으로 평가하는 방법을 제안하였다[20]. 또한, 개인정보 보호분야에서 보안수준을 결정하기 위한 수준 및 성과측정방법에 관한 연구가 수행되었다[9].

IT비즈니스와 정보보호 활동이 이윤창출의 과정에 직접적으로 영향을 미친다는 인과관계를 증명하기 어렵다는 관점에서는 정보보호 성과지표를 도출하기란 어렵다. 그러나 연구자들은 조직의 보안목표에 대한 보안통제영역에 대한 준수성(Compliance)여부의 측면에서는 이에 따른 성과를 측정이 가능하다고 주장한다[21, 25]. 특히, NIST[21]에서는 정보보호 활동의 성과측정 및 구현은 해당 보안통제영역의 정보보호 활동의 모범사례를 정의하고, 그에 따른 사업영향(Business Impact)을 분석하여 보안정책을 갱신하는 방법으로 성과 및 변화관리의 표준을 정의하고 있다[21]. Lee[17]에서는 Martin[20]에서의 연구방법과 유사하게 성과 매트릭스에 의한 준수율로서 정보보호 수준에 대한 측정이 가능하다고 주장하였다[17]. 이에 Kim[14]은 정보보호 거버넌스 준수와 효율성 제고를 위한 정보보호 행위에 관해 연구하였고, 정보보호 준수에 영향을 주는 사용자 행동요인과 특성을 판별하였다. 이는 본 논문의

〈Table 1〉 Related Studies on Performance Indicators of IT R&D

IT Sector	Performance Indicator	Researchers
Software Development	Customer Satisfaction **Software Productivity** **Software Quality**	Kraut[16]
	Warranty costs **Software Productivity** Cost-performance **Despotic quality of products** Profits by other operations Profits by staff Predictability	Haley[5]
	Software Productivity Put effort/cost/defects/**quality**/duration	Park[24]
ICT (Information and Communication Technology)	**An Evaluation Method for R&D Projects in Telecom- munication and Broadcasting**	Lee[18]
Information Assurance and Security	**Degree of compliance with governance**	Posthumus[25]
	Achievement for Security objectives	Martin[20]
	How to develop performance measures defined	NIST[21]
	Measuring the level of information security model development	Lee[17]
	Dynamic Sensitivity Level Measurement for Privacy Protection	Jang[9]
	Employee's Deviant Behavior for Improving Efficiency of Information Security Governance	Kim[14]

업무성과의 영역에 해당하는 부분으로 볼 수 있다[14].

2.3 정보시스템 통제모형

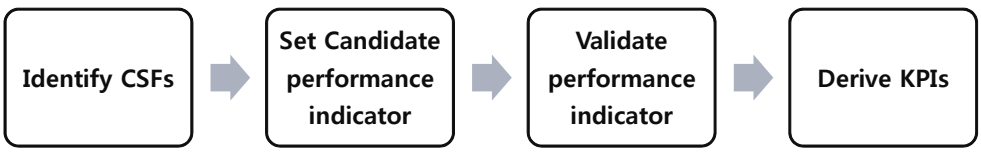
ISACA(Information Systems Audit and Control Association)는 국제정보시스템 감사통제협회로서 정보시스템 감사자의 기술력 향상과 사회적 지위확립을 위해 조직된 민간기관이다. 감사 및 정보기술과 관련된 세미나와 연구, 감사자의 활동지원 등에 관한 일을 수행하고 있다. ISACA에서 개발한 전략적 IT거버넌스 관리를 위한 COBIT은 널리 알려진 정보시스템 통제모형으로 알려져 있으며, COBIT은 조직 내의 34개의 IT프로세스를 평가하고 그 성과를 측정하기 위한 도구를 지원한다[7]. 이는 IT의 업무영역과 프로세스를 기반으로 모범사례를 제시하고, 수행해야 할 활동들을 논리적인 방법

으로 관리할 수 있도록 제안된 프레임워크이다. COBIT에서는 경영상의 요구사항과 연계, IT 활동을 프로세스 모델로의 조직화, 활용 가능한 IT자원의 식별, 경영진이 고려해야할 통제목적의 정의 등의 내용이 포함되어 있다. 이외에 알려진 성과측정과 관련된 IT서비스관리 프레임워크는 ITIL(IT Infrastructure Library), IT Baseline Protection Catalogs, or IT Grundschutz Catalogs, Information Security Management Maturity Model(ISM3), AS8015-2005 (ISO/IEC 38500)등이 있으며, 정보보호와 관련된 산업표준으로서는 ISO/IEC 27001로 대표적인 27000시리즈가 있다. 특히, ISO/IEC 27014는 정보보호 거버넌스 표준으로 이에 따른 개념과 원칙에 대해 가이드를 제공하며 조직의 평가와 지시, 모니터링, 의사소통 활동에 관한 프레임워크를 기술하고 있다[8].

확장된 IT거버넌스의 개념으로서 전사적 위험관리(ERM, Enterprise Risk Management)와 법적 준수성(Compliance)의 개념까지를 확장시킨 GRC(Governance, Risk Management, Compliance)를 도입과 실행방안에 관한 연구가 수행되고 있다[6]. IT거버넌스의 중점영역은 전략적 연계(Strategic alignment), 가치제공(Value delivery), 위험관리(Risk management), 자원관리(Resource management), 성과측정(Performance measurement)으로 분류되며, 이 중성과측정 영역은 전통적인 재무적인 관점 이상의 측정할 수 있는 목표를 달성하기 위한 전략을 실천과제로 변환하는 단계를 말한다[29]. 즉, 기존에 활용된 성과측정방법은 IT균형성과표를 이용하여 전략수행, 프로젝트 완수, 자원 이용, 프로세스 성과, 서비스 제공 등을 추적하고 모니터링 하는 것으로서 대표되었다. 성과관리는 모든 IT자원이 비즈니스에 가치를 전달할 수 있도록 기대한 성과를 내도록 하고 조기에 위험을 식별하여 위험을 감소시키는 성과지표로 표현되기 때문에 궁극적으로 성과지표는 측정된 성과수준에 대한 위험의 내용을 완화시키는 방법으로서 귀결될 수 있다.

3. 연구모형 설계

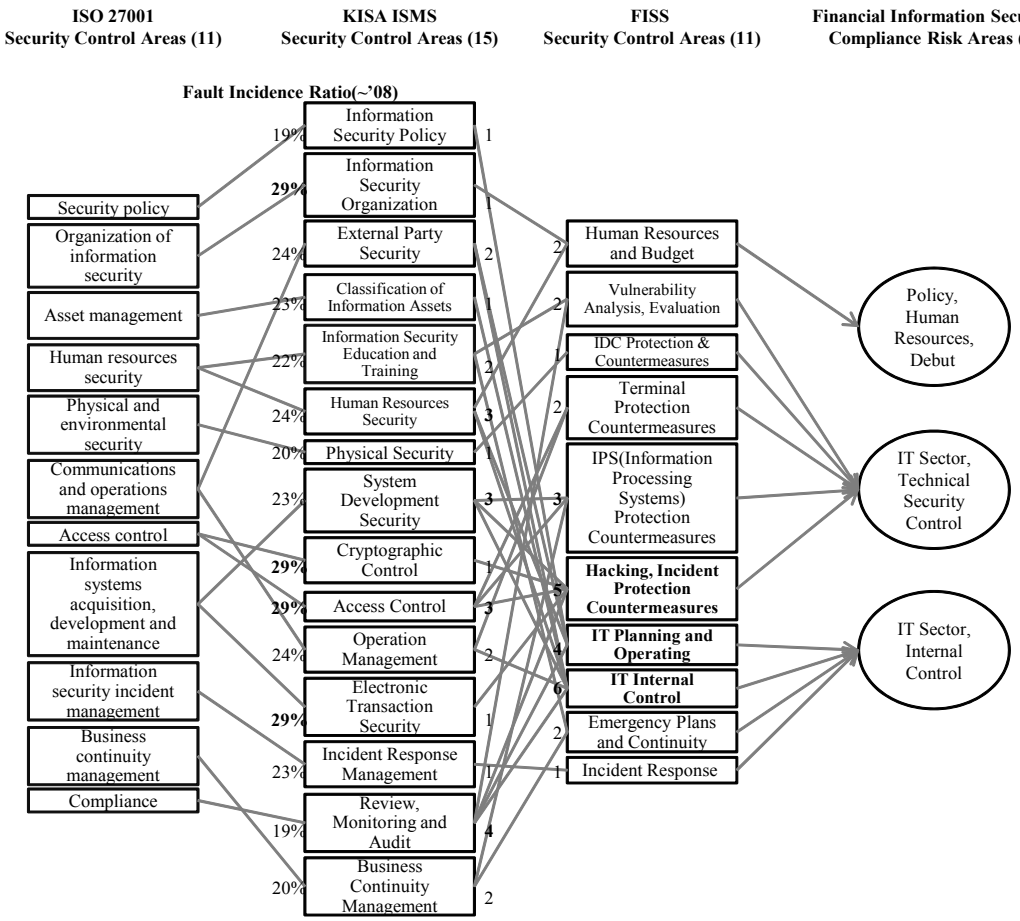
본 장에서는 핵심성과지표(KPI, Key Performance Indicator)를 도출하는 정량적이고 체계적인 기법을 개발하기 위한 과정과 요인분석을 위한 연구모형을 설명한다. 연구의 방법은 <Figure 1>과 같이 정량적인 방법으로 핵심성공요인(CSF)을 식별하고, 핵심성공요인에 대한 후보성과지표로서 연구가설을 설정한다. 금융IT 보안실무자 및 유관기관 보안전문가를 대상으로 실시한 인터뷰와 설문을 통해 얻어진 기초자료를 토대로 연구가설에 대한 타당성을 검증한 후, 성과지표를 도출한다.



〈Figure 1〉 A Process for Developing KPIs(Key Performance Indicators)

3.1 핵심성공요인(CSF) 식별

핵심성공요인 도출을 위해 전략지도(Strategy Map)의 방법을 활용하여 인과관계를 분석한다. 정보보호 관리체계 인증제도(이하 K-ISMS)는 정보통신망 이용촉진 및 정보보호에 관한 법률 제 47조에 의해 일정규모 이상의 정보통신 사업자에 대해 필수적으로 인증을 받아야 하는 정보보호 관리체계로서 13개 영역으로 정보보호 관리과정과 대책분야에 대한 104개의 통제 항목(방통위 고시 2013-4호)으로 구성되어 있다. 또한, 금융회사 정보기술(IT)부문 보호업무 모범규준은 전자금융거래법 및 전자금융감독규정에 근거하여 금융위원회에서 명기하여 금융회사가 정보보호 업무 수행을 위해 지켜야할 항목들을 대해 규정하고 있다. 이들 표준과 규정에 관한 연관성분석은 성과지표를 수립함에 있어서 어떤 영역이 보다 주요하게 다뤄져야 할 영역인지에 대한 우선순위의 문제로서 다뤄질 수 있는지를 설명한다. <Figure 2>는



〈Figure 2〉 Correlation Analysis on Security Control Areas

K-ISMS와 금융회사 정보기술(IT)부문 보호업무 모범규준(이하 모범규준)에 의한 연관성 및 인과관계가 어떻게 되어있는지를 보여준다[13]. 보안요구사항과 통제영역에 대한 연관성을 검토하여 매핑한 결과로 <Table 2>와 같이 정리되며, 연관관계 수가 많은 핵심성공요인(CSF)이 다른 요인보다 중요함을 알 수 있다.

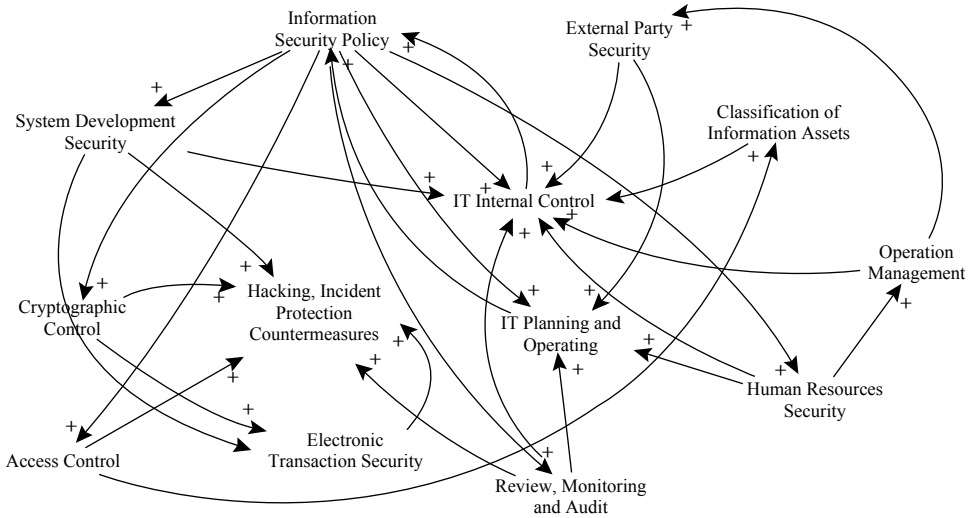
연관성 분석결과인 <Table 2>에서 '해킹 및 침해방지대책'과 'IT계획 및 운영', 'IT내부 통제'의 세 가지영역이 성과지표에 많은 영향을 줄 수 있는 핵심성공요인(CSF)으로 식별된다. 연관관계 수가 적다고 하여 유의하지 않는 것은 아니며, 연관관계 수가 많을수록 준수성(Compliance)에 보다 많은 영향을 줄 수 있는 항목으로서 평가된다.

<Figure 3>은 <Table 2>에서 식별된 상위 3개 영역에 대해 시스템다이내믹스 기법을 이용하여 전략지도(Strategy map)의 형태인 인과지도(Causal map)를 <Figure 3>과 같은 순환 그래프로 표현하였다. 인과지도는 모범규준에 명시된 상위 3개의 핵심요인과 K-ISMS에 의해 연관성을 갖는 모범규준의 3개 영역에 대한 K-ISMS의 각 요인간의 영향을 재분석하여 표현하였다. 인과지도에서 각 요인간 정의 영향을 주는 것은 '+'로 표현된다. 예를 들어, '정보보호정책'은 '정보자산분류'에 정(+)의 영향을 미친다. 또한, '암호통제'는 '해킹 및 침해방지대책'에 정(+)의 영향을 미친다.

Kim[13]에서는 평가기준간 연관성분석으로 '정보보호 정책'이 정보보호활동 영역에 전반적인 영향을 미침을 보였다. <Figure 3>과 같이

〈Table 2〉 CSFs(Critical Success Factors) Based on the Correlation Analysis

IT BSC Approach	Financial IT Security Control Factors	Number of Relations(N)	Security Control Areas : CSFs (Critical Success Factors)
Contribution to business performance	Human Resources and Budget	2	**Administrative Area : Policy**
User-oriented nature and operational efficiency	Vulnerability Analysis, Evaluation	2	Technical Area : IT Sector, Technical Security Controls
	IDC Protection and Countermeasures	1	
	Terminal Protection Countermeaures	2	
	IPS(Information Processing Systems) Protection Counter Measures	3	
	Hacking, Incident Protection Countermeasures	5	
	IT Planning and Operating	4	**Administrative Area : IT Sector, Internal Control**
	IT Internal Control	6	
Response for the Continuity	Emergency Plans and Continuity	2	
	Incident Response	1	
Total		28	



〈Figure 3〉 Causal Map of the CSFs(Critical Success Factors)

표현된 인과지도를 토대로 인과나무(Causal tree)를 표현할 때, 핵심성공요인과 K-ISMS간 가장 큰 정의 영향을 미치는 요인은 관리적 보안 통제영역의 '정보보호정책'의 준수임을 주장하였다[13]. 본 논문에서는 핵심성공요인인 '정보보호정책'에 해당하는 업무성과를 종속변수로 두고, 보안정책 준수정도와 정보보호 관리프로세스 달성도에 대한 10개의 문항을 개발하여 얻은 문항의 평균값으로 설정하였다.

3.2 후보성과지표 설정

본 절에서는 관리적 영역에서 '정보보호정책'과 '인적자원 및 예산'을 구성하는 개인적·조직적 영역으로 후보성과지표를 측정하기 위한 연구모형을 정의한다. 후보성과지표 수립을 위해 금융IT 보안실무자 및 유관기관 보안전문가의 인터뷰를 통하여 '정보보호정책'의 핵심성공요인에 유의하게 영향을 미칠 수 있는 7개의 후보성과지표를 다음과 같이 설정하였다.

[H1] 성과관리는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(9개 문항).

[H2] 변화관리는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(7개 문항).

[H3] 업무태도는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(2개 문항).

[H4] 자기개발은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(3개 문항).

[H5] 업무경험은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(1개 문항).

[H6] 업무능력은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(2개 문항).

[H7] 의사소통은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(5개 문항).

[H8] 인센티브는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(3개 문항).

4. 성과지표 도출

4.1 표본의 특성

금융IT 정보보호책임/담당자, 연구원 및 유관기관을 대상으로 총 33명을 설문하였다. 동일한 개념을 다수의 문항으로 질문할 경우에 응답자가 각 문항에 대하여 유사한 응답을 하였는지를 검증하는 방법인 내적일관성법(internal consistency method)으로 조사를 수행하였다. 리커트(Likert) 7점 척도를 이용하여 8개 후보성과지표에 대해 개인적·조직적 영역의 독립변수를 32개, 종속변수는 10개인 총 42개 측정항목들로 개발하였다.

4.2 신뢰도분석

독립변수의 신뢰도 분석을 위해 32개의 문항에 대한 크론바흐 알파(Cronbach's alpha) 계수가 0.6 미만인 경우에 해당 문항은 유의하지 않은 것으로 간주하였다. <Table 3>은 독립변수인 총 32개 문항 중에서 개인적 영역의 '자기개발' 요인(1개)과 개인적 영역의 '의사소통' 요인(2개)과 조직적 영역의 '의사소통' 요인(1개), 조직적 영역의 '인센티브' 요인(2개)을 항목에 대해 총

〈Table 3〉 Reliability Analysis on Statistical Data

'Self Development'-Reliability Analysis

	Scale Mean if item Deleted	Scale Variance if item Deleted	Corrected Item-Total Corelation	Cronbach's Alpha if item Deleted
I*-H4-SD1	8.6061	9.746	.443	.730
I-H4-SD2	9.6364	5.176	.783	**.246**
O**-H4-SD3	8.7879	8.047	.439	.740

'Communication'-Reliability Analysis

	Scale Mean if item Deleted	Scale Variance if item Deleted	Corrected Item-Total Corelation	Cronbach's Alpha if item Deleted
I-H7-CO1	19.1875	9.254	.310	.622
I-H7-CO2	19.3750	9.274	.527	**.523**
I-H7-CO3	19.1875	9.770	.434	**.563**
O-H7-CO4	20.2188	9.918	.208	.676
O-H7-CO5	19.9063	8.217	.536	**.498**

'Incentive'-Reliability Analysis

	Scale Mean if item Deleted	Scale Variance if item Deleted	Corrected Item-Total Corelation	Cronbach's Alpha if item Deleted
I-H8-INC1	8.9355	5.262	.368	.750
O-H8-INC2	8.9032	4.624	.612	**.432**
O-H8-INC3	9.1290	4.849	.517	**.553**

* I : Individual, ** O : Organization, SD : Self Development, CO : Communication, INC : Incentive.

6개의 문항을 기각하였다. 그 외의 26개의 문항에 대해서는 신뢰도 분석결과로 크론바흐 알바계수는 0.6 이상으로 채택하였다.

4.3 요인분석

분석결과에 어떤 항목이 서로 밀접하게 관련이 있는 지 몇 개의 요인으로 축소하기 위하여 요인분석을 수행한다. 요인분석(factor analysis)은 데이터축소(data reduction)를 통하여 정보를 함축적으로 사용할 수 있게 하는 동시에 항목간의 상관관계를 바탕으로 저변에 내재된 개념을 하나의 요인으로 추출해내는 분석방법이다[30]. <Table 4>는 요인분석의 결

〈Table 4〉 Factor Analysis

	Correlations							
	1	2	3	4	5	6	7	8
O-H2-CM2	**.880**	.138	.171	-.059	.157	-.109	-.160	.048
O-H2-CM5	**.845**	-.119	.026	.178	.000	.315	-.099	.105
O-H2-CM4	**.812**	-.110	.028	.129	.118	.336	.126	.109
O-H1-PM8	**.755**	.374	-.070	.051	.238	.270	.071	-.066
O-H1-PM4	**.729**	.403	-.217	.096	.308	-.136	.115	.077
O-H2-CM3	**.727**	.301	-.273	.133	-.115	.327	.198	.009
O-H1-PM5	**.606**	.499	-.150	.111	.329	-.312	-.050	.231
O-H1-PM6	**.540**	.190	-.343	-.368	.311	.295	.090	-.181
O-H2-CM6	-.031	**.899**	.103	.089	-.168	-.071	-.201	.132
O-H1-PM9	.111	**.869**	.167	.033	.082	.061	.024	-.093
O-H1-PM7	.378	**.690**	-.190	-.310	.094	.362	-.086	.138
O-H2-CM1	.262	**.660**	.232	.085	.468	.035	.033	-.007
O-H1-PM3	.335	**.535**	-.328	-.009	.193	.058	.092	.461
I-H5-WP1	.076	.037	**.848**	-.240	.221	-.156	.026	.219
I-H6-WA2	-.194	.036	**.846**	.091	.120	.025	.101	-.138
I-H1-PM1	.009	.094	**.827**	.150	-.118	-.048	.139	-.259
I-H6-WA1	-.012	.100	**.630**	.142	.002	.216	.465	.445
I-H3-WAT2	.134	.145	.095	**.851**	.232	.021	.139	.100
I-H3-WAT1	.141	-.131	-.093	**.758**	.349	.371	-.102	.145
O-H1-PM2	.192	.093	.038	.310	**.780**	.169	.158	.013
I-H8-INC1	.214	.045	.183	.199	**.735**	.238	-.079	.256
O-H2-CM7	.352	.171	-.022	.069	.242	**.820**	.088	.124
O-H4-SD3	.297	-.079	-.093	.428	.288	**.631**	-.105	.190
I-H7-CO1	.047	-.398	.209	-.073	.103	.028	**.839**	.126
I-H4-SD1	.016	.267	.338	.513	-.024	-.077	**.650**	-.189
O-H7-CO4	.075	.060	-.061	.130	.113	.120	.022	**.839**

CM : Change Management, PM : Performance Management, WP : Work Experience, WA : Workability, WAT : Work Attitude, INC : Incentive, SD : Self Development, CO : Communication.

과로서 주성분분석에 의한 베리맥스(varimax)방법으로 요인을 23번 회전하여 추출되었다. 설명된 요인은 8개의 요인으로 추출되었으며 추출된 요인별로 유사성을 판별할 때, 1은 조직 내 보안목표를 달성하기 위한 '정보보호 성과관리 및 측정'으로 표현되며, 2는 조직 내'정보보호 프로세스관리', 3은 개인의 '업무능력', 4는 개인의 '업무태도', 5는 개인의'정책준수', 6은 조직 내 '정책지원', 7은 개인의 '자기개발', 8은 조직 내 '의사소통'으로 표현된다.

4.4 회귀분석

요인분석의 결과를 토대로 요인점수를 이용한 다중회귀분석을 실시하였다. 요인점수는 요인분석에 의해 묶인 요인 8개에 대한 각 계수

〈Table 5〉 Regression Analysis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.953	.907	.866	.33359

AVONA

Model		Sum of Sqaure	df	Mean Square	F	Sig.
1	Regression	19.635	8	2.454	22.056	.000a
	Residual	2.003	18	.111		
	Total	21.639	26			

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.607	.064		71.768	.000
	Organization's performance management and measurement	.685	.065	.750	10.463	.000
	Managing information security in the organization process	.249	.065	.273	3.811	.001
	Individual's ability to work	-.055	.065	-.060	-.839	**.413**
	Individual's work attitude	.058	.065	.064	.891	**.385**
	Individual's compliance	.227	.065	.248	3.464	.003
	Policy support in the organization	.399	.065	.437	6.099	.000
	Individual's self-development	.048	.065	.053	.738	**.470**
	Communication within the organization	.072	.065	.079	1.099	**.286**

a. Dependent Variable : Information Security Policy Compliance (Average of Work Performance).

이다. <Table 5>의 모형요약에서 회귀식은 예측변수인 독립변수와 종속변수의 적률상관관계(Pearson r, $R=.953$)는 매우 높은 상관관계가 있음을 보이고 있다. 또, 결정계수($R^2=.907$)는 상관관계의 제곱값으로 독립변수에 의하여 설명되는 종속변수의 비율을 의미하며, 값은 1에 매우 가까우므로 유의하다. 분산(ANOVA) 분석의 결과로 휘귀선의 변량은 2.454이며, 잔차의 변량은 .111로 회귀선의 변량이 잔차의 변량보다 22.056배 더 큰 것으로 나타났다. 회귀분석의 결과로 독립변수 '개인의 업무능력'과 '개인의 업무태도', '개인의 자기개발', '조직 내 의사소통'은 유의확률(p-value)이 0.05보다 높아 기각하였다. 즉, $p<0.05$인 '조직 내 성과관리 및 측정'과 '조직 내 정보보호 프로세스 관리', '개인의 정책준수', '조직 내 정책지원'의 4개의 독립변수와 상수만이 종속변수에 영향력을 미치는 변수로 볼 수 있다. 이와 같은 사실로 회귀식 $Y=0.685X_1+0.249X_2+0.227X_3+0.399X_4+4.607$을 발견할 수 있다. 도출된 모든 독립변수가 정보보호정책 업무성과(정책준수와 관리프로세스 달성)에 대해 정(+)의 방향으로 영향을 미치고 있음을 알 수 있다. 표준화계수를 보아 '조직 내 성과관리 및 측정'의 영향력이 가장 크며, 다음으로 '조직 내 정책지원' 등의 순으로 나타났다.

4.5 결과해석 및 가설검정

<Table 6>은 회귀분석의 결과의 내용으로 종속변수인 '정보보호정책'의 업무성과인 '정보보호 정책준수와 관리프로세스 달성'에 영향을 주는 독립변수에 대해 가중치계수에 따라 순서대로 정리한 것이다. 전체적으로 조직적 영역에서 미치는 요인이 개인적 영역에서 미치는 요인보다 통계적으로 유의하였으며 조직 내 성과관리 및 측정활동과 정책적 지원, 정보보호 프로세스에 대한 관리활동들이 업무성과 달성에 있어서 직접적인 영향을 미치는 것으로 확인되었다. 조직 내 의사소통이나 개인의 업무태도, 자기개발, 업무능력은 통계적으로 유의하지 않았으며, 업무성과에 미치는 영향도 작다.

〈Table 6〉 Deriving KPIs for Financial IT Security

Candidate Performance Indicator	Rank	Effect	Weighting Coefficients
Organization's performance management and measurement	1	Positive(+)	.685
Policy support in the organization	2		.399
Managing information security in the organization process	3		.249
Individual's compliance	4		.227
Communication within the organization	Reject		.072
Individual's work attitude			.058
Individual's self-development			.048
Individual's work attitude		Negative(-)	-.055

[H1] 성과관리는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(채택).

[H1 수정] 조직 내 성과관리 및 측정활동은 정보보호 업무성과에 정(+)의 영향을 미쳤다.(연구결과)

[H2] 변화관리는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(채택).

[H2 수정] 조직 내 정보보호 프로세스관리는 정보보호 업무성과에 정(+)의 영향을 미쳤다 (연구결과).

[H3] 업무태도는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(기각).

[H4] 자기개발은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(기각).

[H5] 업무경험은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(기각).

[H6] 업무능력은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(기각).

[H7] 의사소통은 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(기각).

[H8] 인센티브는 정보보호 업무성과에 정(+)의 영향을 미칠 것이다(채택).

[H8 수정] 개인의 정책준수는 정보보호 업무성과에 정(+)의 영향을 미쳤다(연구결과).

[H9 신규] 조직 내 정책지원은 정보보호 업무성과에 정(+)의 영향을 미쳤다(연구결과).

채택된 연구가설은 금융IT 조직 내 정보보호활동에 대한 성과관리체계와 측정활동이 수립되어 있을 때 정보보호 업무성과를 향상시킬 수 있음을 설명한다. 또한, 정보보호 활동에 대한 프로세스관리가 선행되고, 지속될 때에 정보보호활동을 올바르게 실행되고 있음을 보증(Assurance)할 수 있다. 금융IT 보안조직의 보안정책준수의 여부가 일반조직의 보안정책준수 여부보다 보다 유의하게 영향을 미치며, 정보보호 활동을 위한 정책과 근거의 마련은 정보보호 활동과 인식을 개선할 수 있음을 역설한다. 반면에 조직 및 개인적 차원에서 자기개발활동이나 업무경험과 업무능력의 지원은 다른 요소와 비교하여 볼 때 유의하지 않은 것으로 나타났다.

5. 결 론

금융회사는 전자금융거래법, 정보통신망법, 개인정보보호법 등 10여 개의 관련 법률과 산업표준, 인증 제도를 준수해야하는 상황에 직면해 있으며 이에 경영지원을 위한 정보보호 활동에 있어 의사결정 복잡도는 증가하고 있는 실정이다. 본 논문은 금융IT 부문 모범규준의 보안통제영역과 평가기준에서 핵심성공요인(CSF)으로 식별된 '정보보호 정책의 준수와 달성도'를 정보보호 활동의 업무성과로 설정한 뒤, 이에 영향을 미치는 후보성과지표를 검증하였다. 금융IT 영역의 정보보호 활동에서 식별된 모범규준의 주요평가기준은 '해킹 및 침해방지대책'과 'IT 내부통제', 'IT계획 및 운영'에 관한 부문이었으나, 결국 기술적 보안통제의 영역도 관리적 보안통제영역인 조직 내 정보보호정책의 준수가 먼저 전제되지 않는다면 정보보호 통제활동의 연관관계에 있어 이에 따른 실효성은 부족할 수밖에 없다. 즉, 금융IT 영역에서 정보보호 통제모형에 대한 핵심성공요인(CSF)은 '정보보호정책의 준수'였으며, 이에 유

의한 영향을 미치는 요인인 핵심성과지표(KPI)는 개인적 측면보다 조직적 측면에서의 '정보보호 성과관리 및 측정', '정책적 지원', '정보보호 프로세스관리 활동'인 것으로 나타났다.

결론적으로 정보보호 활동은 개인과 같이 일부의 요소만 실행되어서 달성될 수 있는 것이 아니라 여러 개인과 요소가 조직 내에서 지속적으로 관리되고 준수되어질 때 보안목표를 달성할 수 있음을 역설한다. 수립된 핵심성과지표(KPI)는 조직의 정보보호정책준수(Compliance)에 대해 어떠한 요인과 지표가 정보보호 업무성과에 유의한 영향을 주는 지에 관해 판별할 수 있는 논리적 근거를 제공한다. 이를 토대로 금융IT 조직은 정보보호 역량을 강화하기 위한 내부 정책을 수립하기 위한 기초자료로 활용이 가능하다.

References

[1] Barua, A., Kriebel, C. H., and Mukhopadhyay, T., "Information Technology and Business Value : An Analytic and Empirical Investigation," Information Systems Research, Vol. 6, No. 1, pp. 3-23, 1995.

[2] Financial Services Commission, "Comprehensive Security Countermeasures for Financial IT Security," 2013.

[3] Grembergen, W. V. and Steven, D. H., "Measuring and Improving IT Governance Through the Balanced Scorecard," Information Systems Control Journal, Vol. 2, No. 1, pp. 35-49, 2005.

[4] Gurbaxani, V. and Lee, S. A., "Integrating Positivist and Interpretive Approaches to Organizational Research," Organization Science, Vol. 2, No. 4, pp. 342-365, 1991.

[5] Haley, T. J., "Software process improvement at Raytheon," IEEE Software, Vol. 13, No. 6, pp. 33-41, 1996.

[6] Humphreys, E., "Information security management standards : Compliance, governance and risk management," Information Security Technical Report, Vol. 13, No. 4, pp. 247-255, 2008.

[7] ISACA, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT, 2013, http:// www.isaca.org/COBIT/Pages/default.aspx.

[8] ISO/IEC 27014, ITU-T Recommendation X.1054 and ISO/IEC 27014 : 2013 Information technology - Security techniques - Governance of information security, http://www.iso27001security.com/html/27014.html.

[9] Jang, I. J. and Yoo, H. S., "Dynamic Sensitivity Level Measurement for Privacy Protection," The Journal of Society for e-Business Studies, Vol. 17, No. 1, pp. 137-150, 2012.

[10] Kaplan, R. and Norton, D., "The strategy focused organization," Harvard Business Press, 2001.

[11] Kaplan, R. and Norton D., "Using the balanced scorecard as a strategic man-

agement system," Harvard Business Review, Jan-Feb, 1996.

[12] Kaplan, R. and Norton, P., "Transforming the Balanced Scorecard from Performance Measurement to Strategic Management : Part I," Accounting Horizons, Vol. 15, No. 1, pp. 87-104, 2001.

[13] Kim, A. C., Lee, S. M., and Lee, D. H., "Compliance Risk Assessment Measures of Financial Information Security using System Dynamics," International Journal of Security and Its Applications(IJSIA), Vol. 6, No. 4, pp. 191-200, 2012.

[14] Kim, H. J. and Ahn, J. H., "An Empirical Study of Employee's Deviant Behavior for Improving Efficiency of Information Security Governance," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 147-164, 2013.

[15] KISA(Korea Internet and Security Agency), 2013 National Information Security White Paper, 2013.

[16] Kraut, R. E. and Streeter, L. A., "Coordination in software development," Communications of the ACM, Vol. 38, No. 3, pp. 69-81, 1995.

[17] Lee, H. M. and Lim, J. I., "A Study on the Development of Corporate Information Security Level Assessment Models," Journal of the Korea Institute of Information Security and Cryptology, Vol. 18, No. 5, pp. 161-170. 2008.

[18] Lee, U. K., Kim, K. K., Ryoo, S. Y., and Yoo, Y. S., "An Evaluation Method for R&D Projects in Telecommunication and Broadcasting," The Journal of Society for e-Business Studies, Vol. 17, No. 2, pp. 165-187, 2012.

[19] Maconachy, W. V., Schou, C. D., Ragsdale, D., and Welch, D., "A model for information assurance : An integrated approach," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, pp. 301-310, 2001.

[20] Martin, C. and Refai, M., "A Policy-Based Metrics Framework for Information Security Performance Measurement," 2007 2nd IEEE/IFIP International Workshop on Business-Driven IT Management, Munich, pp. 94-101, May, 2007.

[21] NIST, Performance Measurement Guide for Information Security, NIST SP800-55 Rev.1, Jul 2008.

[22] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP800-53 Rev. 4, Aprl 2013.

[23] Niven, P. R., Balanced scorecard step-by-step : maximizing performance and maintaining results, John Wiley and Sons, Hoboken, NJ. 2002.

[24] Park, S. H., Research on the impact on the outcome of the software project : Change management and improvement of processes, Korea University of Foreign Studies, Graduate School of Management Information Systems, Master Thesis, 2004.

[25] Posthumus, S. and Von Solms, R., "A

framework for the governance of information security," Computers and Security, Vol. 23, No. 8, pp. 638-646, Dec 2004.

[26] Steven, D. H. and Grembergen, W. V., "An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment," Information Systems Management, Vol. 26, No. 2, pp. 123-137, 2009.

[27] Tayler, B., "The Balanced Scorecard As A Strategy-Evaluation Tool : The Effects of Responsibility and CausalChain Focus," Working Paper, Cornell University, 2009.

[28] The Bank of Korea, "The usage of Internet banking services in Korea," 2013.

[29] Von Solms, S. H., "Information security governance-compliance management vs operational management," Computers and Security, Vol. 24, No. 6, pp. 443-447, 2005.

[30] Wikipedia, "factor analysis," 2013, http://en.wikipedia.org/wiki/Factor_analysis.

저 자 소 개

장성옥 (E-mail : sojang0808@gmail.com)
1992년 부산대학교 전자계산학과 (학사)
2012년~현재 고려대학교 정보보호대학원 정보보호학과 석사과정
1992년~현재 금융감독원 수석검사역
관심분야 정보보호정책, 금융보안

임종인 (E-mail : jilim@korea.ac.kr)
1980년 고려대학교 수학과 (학사)
1982년 고려대학교 수학과 (이학석사)
1986년 고려대학교 수학과 (이학박사)
1986년~2001년 고려대학교 자연과학대학 정교수
2001년~현재 고려대학교 정보보호대학원 원장,
대검찰청 디지털수사자문위원회 위원장,
금융보안연구원 보안전문기술위원회 위원장,
안전행정부 정책자문위원회 위원,
방송통신위원회 인터넷협의회 운영위원 등
관심분야 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안,
융합기술보안 등