情 報 保 護 學 會 誌
第22卷 第6號, 2012. 10

정보보호 거버넌스 국제표준화와 국내 도입 사례 연구

김 정 덕*, 이 성 일**

요 약

정보보호 활동에 대한 이사회 및 최고경영층의 역할과 책임을 강조하는 거버넌스에 대한 이슈가 최근 공공기관 및 민간기업 공히 화두로 등장하고 있다. 조직 내 정보보호가 효과적으로 수행되기 위해서는 무엇보다도 정보보호에 대한 주요 방향 제시와 통제 기능을 수행하는 최고경영층의 리더십과 지원체계가 핵심성공요인이라는 것을 인식하기 시작한 것이다. 이러한 정보보호의 새로운 패러다임을 반영하여 현재 정보보호 거버넌스에 관한 국제표준화 작업이 완성단계에 있어 2013년에는 국제표준으로 발표될 예정이고, 국내 KS 표준으로도 상정될 예정이다. 또한 최근 금융권을 비롯하여 정보보호 거버넌스 도입을 위한 프로젝트가 수행되었다. 본 연구에서 국제표준의 내용을 중심으로 거버넌스를 위한 원칙과 프로세스를 소개하고, 국내 정보보호 거버넌스 도입 사례 연구를 통해 거버넌스의 현 수준을 살펴보고 향후 추진되어야 할 과제를 제시하고자 한다.

Ⅰ. 서 론

최근 들어 CPO, CISO를 위한 교육 프로그램이 점차 확대되고 있으며, 사이버 보안관 3500명 양성 등 정부 및 민간단체에서 정보보호를 담당하는 중역/전문가의 역할과 책임에 대해 관심이 고조되고 있다. 이는 정보보호가 단순히 기술적 이슈를 넘어서서 비즈니스 이슈로 변화되고 있다는 점을 간접적으로 보여주고 있다.

해외 저명한 전문가들은 일찌감치 정보보호가 기술적 이슈가 아닌 관리적 이슈, 인적자원에 대한 이슈라는 점을 강조했으며, 정보보호 사고가 비즈니스에 미치는 영향이 점차 지대해 짐에 따라 이제는 정보보호가 IT 부서만 책임지는 것이 아닌 CEO를 위시한 회사의 중역이 직접 챙겨야 하는 사안이 되었음을 의미하고 있다.[2]

그러나 국내 현실은 여전히 정보보호를 기술적 이슈로 보는 시각이 지배적이며 따라서 정보보호 기능은 IT 부서에서 수행하는 여러 기능 중 하나로서 인식되고 있다. 설령 CSO나 CISO가 임명된 몇몇 조직에서도 주어진 역할을 적절하게 수행할 수 있는 전문지식과 역량이 명확하게 규정되어 있지 않으며 역할 수행에 필요한 방법도 제시되고 있지 않기 때문에 그 실효성에 의문이 있다.

이 결과, 투자의사결정권한을 가지고 있는 최고경영층에게 정보보호의 비즈니스 가치를 구체적으로 제시하지 못하는 현실에서 정보보호 투자는 항상 다른 투자에 비해 우선순위에서 밀리고 있으며, 최고경영층 역시 정보보호는 자신이 책임지거나 관리해야 할 대상이 아닌 정보시스템 관리자의 업무로 인식하고 있다. 그러나 정보보호 사고로 인한 직접적인 피해뿐만 아니라 기업 이미지 손상(reputational risk), 주식가치 하락(financial risk) 등의 문제는 비즈니스에 매우 심각한 영향을 주고 있으므로 전사적 차원에서의 정보보호 노력과 더불어 최고 경영층의 주도적 역할이 요구되고 있다.

이러한 문제를 해결하고 실효성 있는 정보보호를 조직 내 정착시키기 위해서는 정보보호의 새로운 패러다임이라고 하는 '정보보호 거버넌스(governance)' 구축이 필요하다.[1] 정보보호 거버넌스란 "조직 거버넌스의 일환으로서 비즈니스와의 전략적 연계와 관련 법/규정의 준수를 위해 기업의 모든 이해관계자를 고려하여 최고 경영층 및 이사회의 정보보호 프로그램에 대한 지시 및 통제 활동과 이를 위한 조직, 역할과 책임, 절차를 포함한다"라고 정의할 수 있다.[3,5,6]

다시 말해 최고경영층의 주요 아젠다에 정보보호가

* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)
** 딜로이트 안진회계법인 Senior manager(seongilee@deloitte.com)

포함되도록 하고, 또한 정보보호책임자는 최고경영층이 요구하는 비즈니스적 측면에서의 정보보호의 효과와 영향을 보고할 수 있도록 하는 체계구축을 의미한다.

이미 선진국에서는 정보보호 거버넌스 지침이나 기준들을 발표하여 정보보호 활동을 조직 차원에서 지시하고 통제하고 있다. 이러한 정보보호 거버넌스 활동이 최근 이슈화되고 있는 현상은 정보보호 활동을 기술적 이슈로 간주하여 중, 하위 관리자에 의해 수행되는 업무가 아니라 조직의 중요 자산인 이미지를 손상/제고시킬 수 있으며, 사회적 책임의 한 요소로서 지속적 성장을 가능케 하는 비즈니스 이슈로 인식하고 있기 때문이다. 따라서 거버넌스의 주체인 기관장, 간부급 책임관, 이사회 위원 등을 포함하는 주요 의사결정권자들이 정보보호에 대한 방향 제시와 지원 체계가 조직 내 정보보호 활동의 성공여부를 좌우하는 핵심요인이라는 점을 인식한 패러다임 변화를 반영하고 있다.[1] 이러한 정보보호의 새로운 패러다임을 반영하여 현재 정보보호 거버넌스에 관한 국제표준화 작업이 완성단계에 있어 2013년에는 국제표준으로 발표될 예정이고, 국내 KS 표준으로도 상정될 예정이다.

국내에서도 최근 금융권을 비롯하여 정보보호 거버넌스 도입을 위한 프로젝트가 수행되었다. 본 연구에서 국제표준의 내용을 중심으로 거버넌스가 지켜야 할 원칙과 프로세스를 소개하고, 국내 정보보호 거버넌스 도입 사례 연구를 통해 거버넌스의 현 수준을 살펴보고 향후 추진되어야 할 과제를 제시하고자 한다.

Ⅱ. 정보보호 거버넌스 국제표준 동향

2.1 정보보호 거버넌스 국제표준 진행과정

정보보호관리에 대한 국제표준화 활동의 주역인 ISO/IEC JTC 1 SC 27 WG 1에서는 내부에서의 요구와 JTC 1에서의 요구에 의해 정보보호 거버넌스 국제표준화 작업이 2008년 4월 회의부터 논의되기 시작하였다. 2008년 10월, 사이프러스에서 개최된 37차 회의에서 한국은 정보보호 거버넌스 프레임워크에 대해 기고문을 제출하였고 본 회의에서 약간의 수정을 거쳐 SC27의 공식의견으로 채택되었다. 기고문의 내용은 정보보호 거버넌스의 필요성과 개념을 언급하였으며, 기업과 IT 거버넌스와의 관계 및 ISMS와의 관계를 기술하였고, 정보보호 거버넌스의 프레임워크를 제시하였다. 프레임워크는 정보보호 거버넌스의 3가지 목표(Accountability, Business Alignment, Compliance)를 제시하였고, 이에 기반을 둔 10가지 원칙을 제시하였다. 또한 거버넌스를 구현하기 위한 프로세스와 주요 중점분야를 제시하였다.

이 회의 이후 “정보보호 거버넌스 프레임워크”를 새로운 표준화 항목으로 결정하였고 편집인(editor)으로 한국의 중앙대 김정덕 교수와 일본의 Kei Harada을 선정하였다.

한편 ITU-T에서는 2008년부터 한국 측의 건의로 “정보통신기업을 위한 정보보호 거버넌스”를 회계년도(2009-2012) 신규 표준안으로서 논의하기 시작하였다. 2009년 2월 제네바 회의에서는 한국 측의 기고문을 심층 검토하였고, ISO와의 공통 프로젝트 진행 가능성에 대해 많은 논의가 있었다. 결론적으로 공통 프로젝트가 되기 위해서는 동일한 문서로서 제시되어야 하기 때문에 문서명을 “정보보호 거버넌스 프레임워크(X.1054)”로 수정하였고 내용도 일반적인 정보보호 거버넌스 이슈만을 포함시켰다. 수정 기고문과 함께 ISO에 공통 프로젝트로 수행하자는 내용의 협조문을 보냈다. 이 작업의 편집인도 한국의 중앙대 김정덕 교수가 담당하기로 결정되었다.

2009년 4월 SC 27 회의에서는 ITU-T SG 17와 공동으로 진행하기로 결정(common text project)하였고 경영층의 거버넌스를 강조하기 위해서 표준 프로젝트 명칭을 “ISO/IEC 27014: Governance of information security”로 변경하였다. 3차에 걸친 WD를 거쳐 2010년 10월 회의에서 1차 CD로 추진하기로 결정된 후 2012년 5월 회의에서 FDIS로 추진하기로 결정하였다. 2012년 9월, ITU-T SG 17 회의에서 본 프로젝트가 최종 승인됨에 따라 2013년 상반기에 두 표준화 기구에서 국제표준으로 발간될 예정이다.

2.2 정보보호 거버넌스 국제표준 주요 내용

정보보호 거버넌스 국제표준 (ISO/IEC 27014: Governance of information security)은 정보보호 거버넌스의 개념, 원칙, 프로세스 등 전반적인 프레임워크를 제시하는 지침서이다.

정보보호 거버넌스 국제표준 문서는 다음과 같이 구

성되어 있다[4].

- 범위 : 정보보호 거버넌스의 대상과 국제 표준의 적용범에 대해 기술하고 있음
- 인용규격 : 정보보호 거버넌스 국제표준이 참조하는 다른 국제표준에 대한 소개
- 용어정의 : ISO27000 시리즈의 용어정의를 기반으로 정보보호 거버넌스 국제표준에 활용하는 용어의 정의
- 개념 : 정보보호 거버넌스의 개념적 정의와 목표, 기대효과 및 이해관계에 대해 정의
- 원칙과 프로세스 : 정보보호 거버넌스의 6개 원칙과 평가, 지시, 모니터링에 기반한 정보보호 거버넌스 프로세스 설명

다음 단락은 정보보호 거버넌스 국제표준에서 언급하고 있는 정보보호 거버넌스의 개념 및 원칙, 프로세스의 주요 내용이다.

2.2.1 정보보호 거버넌스의 개념

조직의 주요 의사결정과 이에 따른 성과에 대한 책임성을 지닌 거버넌스 주체들은 조직의 정보보호 활동이 효율적, 효과적이고 적용가능하며 이해관계자의 기대치에 부응할 수 있는 비즈니스 목표 및 전략과 일치할 수 있음을 입증하기 위해 정보보호 거버넌스 체계를 조직에 적용한다[4].

정보보호 거버넌스의 핵심 목표는 정보보호와 비즈니스의 전략적 연계, 정보보호 관련 이해관계자에 대한 가치전달, 정보 위험에 대한 책임성 있는 처리이며 IT, 정보보호 등 영역별 거버넌스 모델은 비즈니스 목표와의 연계 중요성을 강조하는 조직적 거버넌스(기업 거버넌스)의 일부를 구성하는 필수 요소이다.

다만, IT 거버넌스의 중요 범위는 정보를 획득, 처리, 저장 및 배포하기 위해 필요한 자원을 목적으로 하고 있는 반면, 정보보호 거버넌스의 범위는 정보의 기밀성, 무결성, 가용성 확보를 주요 목적으로 한다. 따라서 두 가지 유형의 거버넌스는 상호 중첩되는 영역이 존재하지만 차별화된 영역 또한 존재하므로 조직적 거버넌스의 주요 요소로서 공존할 수 있다.

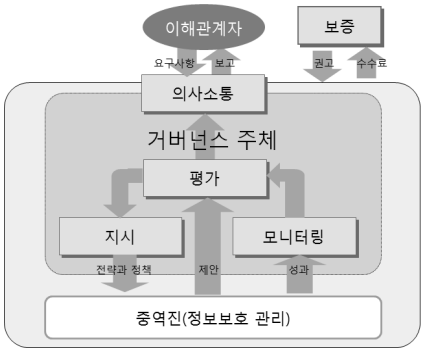
2.2.2 원칙 및 프로세스

정보보호 거버넌스의 원칙들은 정보보호 거버넌스 프로세스의 구현 시 지켜야 할 규칙 및 기반을 제공한다. 거버넌스 주체는 이러한 원칙들이 적용되고 누군가에 의해 원칙들이 구현될 수 있도록 책임과 권한을 할당해야만 한다. 정보보호 거버넌스의 조직 적용 및 구현을 위한 6개 원칙은 다음과 같다[4].

- 원칙 1: 조직 전반에 걸친 정보보호를 수립한다.
- 원칙 2: 위험기반 접근방법을 채택한다.
- 원칙 3: 투자 의사결정의 방향을 설정한다.
- 원칙 4: 내외부 요구사항의 준수를 입증한다.
- 원칙 5: 보안에 긍정적인 환경을 조성한다.
- 원칙 6: 업무 측면에서의 결과를 고려하여 정보보호 성과를 검토한다.

거버넌스 주체는 정보보호 거버넌스를 실행하기 위해 “평가”, “지시”, “모니터링”, “의사소통” 프로세스를 이행한다. 더해서 “보증” 프로세스는 정보보호 거버넌스와 적정 수준에 관한 독립적이고 객관적인 의견을 제공한다[4].

다음의 그림은 정보보호 거버넌스 프레임워크 내에서 평가, 지시, 모니터링, 보증 프로세스의 관계를 보여준다.



〔그림 1〕 정보보호 거버넌스 프로세스

“평가”는 현황을 고려하여 수립된 정보보호 활동 목표의 성취 여부를 측정하는 거버넌스 프로세스이다. 또한, “평가”를 통해 전략 목표 성취를 위한 주요 의사결정이 이루어진다.

“지시”는 거버넌스 주체에 의해 결정된 정보보호 목

표와 방향을 거버넌스 대상에게 적용하는 거버넌스 프로세스이다. 해당 방향에는 자원 투입수준과 자원 할당, 행위의 우선순위, 정책의 승인, 위험의 허용 및 위험관리 계획의 변화를 포함시킬 수 있다.

“모니터링”은 거버넌스 주체가 전략적 목표의 성취 여부 확인하는 프로세스 이다.

“의사소통”은 양측의 구체적 요구에 따라 정보보호에 관한 정보를 교환하는 거버넌스 주체와 이해관계자 양방향으로 작용하는 거버넌스 프로세스 이다.

“보증”은 거버넌스 주체에 의한 독립적이고 객관적인 감사, 검토 또는 인증을 정보보호 거버넌스 체계에 대해 수행하는 프로세스이다. 이러한 일련의 프로세스는 거버넌스 활동을 이행하고 원하는 정도의 정보보호 수준을 달성하기 위한 운영 활동이 이루어질 수 있도록 지원한다.

Ⅲ. 국내 구축 프로젝트 사례

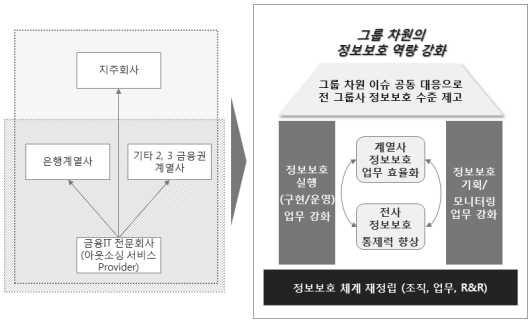
3.1 사례연구 개요

정보보호 거버넌스 국제표준의 가이드에 따르면 기업에 정보보호 거버넌스 체계를 수립하기 위해서는 정보보호 정책 제개정을 통한 목표와 원칙의 적용, 이해관계자(거버넌스 주체와 경영진, 적용 대상 회사 또는 담당자 등)의 명확화, 평가, 지시, 모니터링, 의사소통 프로세스의 구축이 필요하다.

본 논문에서는 A 금융그룹의 지주사와 계열사 간의 정보보호 거버넌스 체계구축 사례를 소개하고자 한다. A 금융그룹의 사례는 정보보호 거버넌스 국제표준의 요건을 모두 충족하지 못하지만 국제표준 수준으로 체계를 발전시키기 위한 사전 단계로서 계열사 간의 관계정의, 의사소통 체계수립, 거버넌스 대상 정보보호 업무의 정형화 등을 포함하고 있다.

3.2 정보보호 거버넌스 체계수립 목표

A 금융그룹 정보보호 거버넌스 체계수립 목표는 거버넌스 수뇌부(Governance Head)로서 지주회사의 입장, 거버넌스 주체(Governance Body)로서 개별 계열사의 입장, 거버넌스 대상으로서 금융IT전문회사의 입장으로 구분될 수 있다([그림 2] 참조).



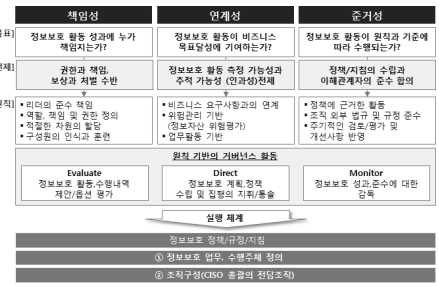
〔그림 2〕 A 금융그룹 체계수립 목표

[그림 2]에 나타난 바와 같이 거버넌스 구조의 최상위로서 지주회사는 그룹 차원의 정보보호 수준 상향 평준화 및 이를 위한 공동 협의체 구성을 목표로 하고 있다.

거버넌스 주체로서 은행계열사 및 기타 2,3 금융권 계열사는 정보보호 통합관리 위한 CISO 임명과 전담조직 구성을 목표로 하고 있다. 이러한 양쪽의 이해관계는 개별 계열사가 거버넌스 활동을 담당하는 경영진을 선임하고 이들이 연계할 수 있는 협의체를 지주회사에서 운영하는 거버넌스 구조로서 구현될 수 있다. 반면, 거버넌스의 대상이 되는 금융 IT 전문 계열사에 대해서는 해당사의 입장을 구조화 하는 것이 아니라 개별 계열사의 입장에서 위수탁 관계상의 정보보호 책임 소재를 명확히 하는 형태로 체계수립 목표가 정의되었다. 이것은 거버넌스 대상을 정립하기 위한 활동으로서 정보보호 거버넌스 국제표준 수준의 체계 수립을 위한 기초 작업으로 볼 수 있다.

3.3 정보보호 거버넌스 목표모델

A 금융그룹의 정보보호 거버넌스 목표 모델은 정보보호 거버넌스 국제표준에서 가이드 한 6개 원칙의 핵



〔그림 3〕 정보보호 거버넌스 목표 모델

심 단어로서 책임성(Accountability), 업무 연계성(Business Alignment), 준거성(Compliance)을 중심에 두고 평가, 지시, 모니터링 프로세스를 실현하기 위한 제반 체계(정보보호 정책, 조직, 의사소통 체계 등)를 수립하는 형태이다([그림 3] 참조).

[그림 3]의 목표 모델을 구현하기 위해서는 다음과 같은 제반사항이 사전 확보되어야 한다[7].

■ 정보보호 업무의 정형화
- 정보보호 업무의 근거인 정책/규정/지침 등 기반 조성
- 참조모델/가이드원칙/현재 업무 등을 참조하여 기획, 구현, 운영, 평가 및 모니터링 표준 업무 설계

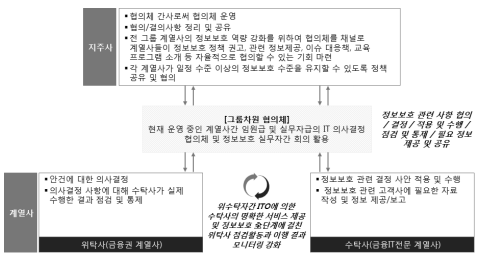
■ 업무별 수행 주체 및 역할의 명확화
- 주요 이해관계자 식별, 업무별 수행 주체 정의
- 의사소통을 위한 협의체 구성방안

■ 조직구성
- CISO 지정
- CISO 총괄 하의 정보보호 전담 조직

A 금융그룹은 이전 단락에서 기술된 정보보호 업무의 정형화, 업무별 수행 주체 및 역할의 명확화, 조직구성을 정보보호 거버넌스 체계수립의 핵심 산출물로서 정의하였다.

3.4 A 금융그룹의 정보보호 거버넌스 체계수립 결과

A 금융그룹은 정보보호 거버넌스 목표 모델을 구현하기 위해 지주사, 개별 계열사, 거버넌스 대상인 금융IT 전문 계열사의 위상을 정립하였고, 이를 정보보호 정책과 조직 설계(안) 반영함으로써 정보보호 거버넌스 체계수립을 위한 기반 조성을 완료하였다([그림 4] 참조)[7].



〔그림 4〕 A 금융그룹 거버넌스 이해관계자 별 위상

A 금융그룹은 지주사를 중심으로 한 거버넌스 주체와 대상을 확립함으로써 정보보호 거버넌스 실행을 위한 기본적인 지배구조를 구축한 것으로 판단되며, 정보보호 정책을 통해 해당 구조를 규정화 하였다. 이를 통해 A 금융그룹이 평가, 지시, 모니터링, 의사소통 프로세스를 향후실무에 적용한다면, 정보보호 거버넌스 국제표준 수준의 체계 운영이 가능할 것이다.

Ⅳ. 시사점

국내 대기업 및 금융그룹들은 지주사 출범을 통해 기업 거버넌스에서 요구하는 재무적인 지배구조를 확립하였고 이에 따라 IT와 정보보호 영역에서의 거버넌스 체계구축이 요구되고 있다. 금융그룹의 경우 차세대시스템 구축 프로젝트를 통해 지주회사와 계열사 간의 IT거버넌스 체계를 일부 구축하였으나 IT의 통합이나 선진화 수준으로서, ISO 38500 같은 국제 규격의 체계를 수립하였다고 보기에는 어려운 실정이다. 정보보호 거버넌스 영역은 IT 거버넌스 영역과 비교해도 더욱 열악한 실정이다.

이러한 정보보호 거버넌스의 국내 상황은 정보보호 관리체계의 활성화도 어려운 관리적 보안의 현주소를 나타내고 있으며, 정보보호관리체계의 확립 없이는 정보보호 거버넌스 체계수립 또한 어렵다는 것을 입증하고 있다.

국제 표준에서는 정보보호관리체계 이상의 정보보호 거버넌스를 요구하고 있는 현 상황에서 국내 정보보호의 저변이 국제적인 흐름과 발맞추기 위해서는 다음과 같은 국내 산업계 및 학계의 공동 노력이 절실히 요구된다.

첫째, 인식변화와 제도 구축 등 정보보호 거버넌스 구현을 위한 환경 조성이 필요하다. 최고경영층의 정보보호에 대한 보다 적극적이고 자주적인 인식변화와 더불어 제도적으로 최고경영층의 정보보호에 대한 역할과 책임을 보다 강화해야 할 것이다. 이미 미국과 유럽 일부 선진제국에서는 내부통제시스템의 일부로서 정보보호 구현에 대한 책임을 CEO와 CFO에게 묻고 있다.

둘째, 정보보호 거버넌스 구현 및 평가를 위한 제반 기준 및 지침 수립이 필요하다. 정보보호 투자관리, 정보보호 활동의 성과평가, 정보자산에 대한 위험관리, 비즈니스와의 전략적 연계 등에 관한 지침 및 방법 개발이 요구된다.

셋째, 정보보호 거버넌스를 용이하게 수행할 수 있는 제반 시스템이나 도구들이 개발될 필요가 있다. 최근 GRC (governance, risk, compliance) 시장이 점차 확대되고 있으며 이를 위한 시스템 개발이 해외에서 활발하게 진행되고 있다. 국내에서의 GRC 시장은 아직 초보 단계에 있으며 앞으로 많은 연구 개발이 요구된다.

과거 10년여에 걸친 국내 정보보호 확산 노력으로 인해 기술적 측면에서의 많은 업적을 이루었다는 점은 부인할 수 없다. 그러나 정보보호가 비즈니스에서 차지하는 중요성에 비추어 정보보호 거버넌스로의 패러다임 변화 없이는 더 이상의 발전을 기대하기 어려울 것이다.

참고문헌

[1] Basie von Solms, “Information Security - The Fourth Wave,” Computers & Security Vol. 25, pp. 165-168, 2006.

[2] David Newman, “Toolkit Information Governance Strategies for a Compliance-Driven World,” Gartner, 2007.

[3] ISO/IEC 27014 - Governance of information security, FDIS, 2012.

[4] ISO/IEC 38500 Governance of Information Technology, 2008.

[5] ITGI, “Information Security Governance : Guidance for Boards of Directors and Executive Management,” 2002.

[6] Software Engineering Institute, “Governing for Enterprise Security (GES) Implementation Guide”, Carnegie Mellon University, 2007.

[7] A 금융그룹, 정보보호 체계 선진화 프로젝트, Working Draft, 2012.

〈著者紹介〉

김 정 덕 (Jungduk Kim)
종신회원

1979년: 연세대학교 정치외교학과, 학사
1981년: 연세대학교 경제학과대학원, 석사
1986년: Univ. of S. Carolina, MBA
1990년: Texas A&M University, Ph. D. in MIS
1991년~1993년: 한국전산원, 선임연구원
1995~현재: 중앙대학교, 교수
<관심분야> 정보보호관리 및 거버넌스, 시스템감사, 정보시스템의 전략적 응용

이 성 일 (Lee, Seong il)
종신회원

1998년: 중앙대학교 정보시스템학과 학사
2002년: 중앙대학교 정보시스템학과 석사
2011년: 동국대학교 경영정보학과 박사
2000년~2009년: 정보보호 컨설팅 전문업체 근무
2010년~2011년: 언스트앤영 어드바이저리 근무
2012년 현재: 딜로이트 안진회계법인 Senior Manager
<관심분야> 정보보호관리체계, 정보보호거버넌스, BCM 등