情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

정보보안 공시제도 도입을 위한 타당성 분석과 운영체계 제언*

전 효 정,† 김 태 성‡
충북대학교 경영정보학과

A Feasibility Study on Introduction of Information Security Disclosure*

Hyo-Jung Jun,† Tae-Sung Kim‡
Department of Management Information Systems, Chungbuk National University

요 약

기업환경과 금융환경의 변화로 기업 스스로의 임의적이고 자발적인 동기로 이루어지는 제한적인 정보보안 정보의 공개가 아닌 전면적이고 포괄적인 정보보안 관련 정보 공개의 필요성이 제기되고 있다. 본 논문에서는 기존 공시제도의 고찰을 통해 정보보안 분야 공시제도(안)을 제시하고, 공시제도 전문가들의 검토의견을 수렴하여 정보보안 공시제도의 필요성과 정보보안 공시제도 도입의 타당성을 분석하였다.

ABSTRACT

This study intends to help establishing guidelines on providing easier access to security status-related information about business and public institutions by interested parties such as investors and civic societies, and to push ahead with the compulsory execution of the information security disclosure. We suggest a draft for the information disclosure system by reviewing the existing disclosure systems and validate the draft by surveying experts. It is expected that the result of this study will be the basis for the adoption of the information security disclosure system and be used as a referential material in the establishment of the relevant policy.

Keywords: Information Security, Disclosure, In-depth Interview, Security Incidents

I. 서 론

정보가 중요한 자산으로서의 가치를 갖게 되면서 정보의 획득은 곧 자산이나 권력의 획득을 의미하고 있다. 이처럼 정보가 자산화됨에 따라 공공기관 및 기업의 정보보안 관리 및 침해사고 대응 수준에 대한 정보는 고객이 자신의 경제적 이익 및 선택의 편의를 위한 중요한 참고자료가 될 것임은 분명하다. 더욱이, 개인정보의 과다 수집으로 인한 침해는 물론 개인정보 노출로 인한 피해도 증가 추세에 있어 사업자뿐만 아니라 개인까지도 정보보안 제품 및 서비스에 대한 수요를 확대하고 있다[8,9].

금융업계에서는 인터넷뱅킹 등 비대면 금융거래의 비중이 증가하는 상황에서 발생한 현대캐피탈 고객정보유출사고 및 농협 전산장애 사고 등으로 인해, 2011년 6월 신속하게 "금융회사 IT 보안강화 종합대책"을 마련하여 발표함으로써 기업의 강제적이고도 의무적인 보안조치 및 보안투자의 필요성을 강조하였다

접수일(2012년 8월 16일), 게재확정일(2012년 11월 9일)
* 본 논문은 2012년 한국정보보호학회 하계학술대회에서 우수논문상을 수상하였음
본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임 (2011-0025512). 2012년 지식정보보안 석사과정지원사업의 지원을 받아 수행되었음.
† 주저자, phdhyo@naver.com
‡ 교신저자, kimts@chungbuk.ac.kr

〔4〕. 이 종합대책은 사고발생에 따른 일시적 대응책이 아닌 근원적인 IT 보안강화 대책이 될 수 있도록 경영진의 인식 전환과 IT 보안조직의 실질적 역량 강화 등에 중점을 두고 있다. 또한, 2011년 10월에는 이를 뒷받침하기 위한 "전자금융감독규정"의 개정 및 시행이 예고되었으며〔5〕, 2011년 11월에는 "전자금융거래법 시행령(대통령령 제23776호)"이 공포되어 2012년 5월부터 발효되었다〔6,39〕. 미국의 증권거래위원회(Securities and Exchange Commission, SEC)도 2011년 10월 기업의 재정적 손실을 야기할 만한 수준의 보안사고가 발생한 경우 관련 정보 또는 잠재적인 보안사고의 가능성을 공표하도록 하는 새로운 가이드라인을 제정하여 발표하였다. 기업이 이 가이드라인을 검토하여 자율적으로 보안수준을 강화할 수 있도록 하는 일종의 방안을 제시한 수준이지만, 향후 언제든지 적극적인 보안정보공시 또는 보안사고내역공개 등을 강제하는 수준으로 발전할 수 있음을 시사하고 있다〔42〕.

이러한 상황에서, 정보보안 공시제도를 도입하는 것은 기업과 공공기관의 보다 안정적인 경영환경 구축과 국가의 산업경쟁력 향상을 위해 반드시 필요하다〔11〕. 보다 많은 정보서비스의 이용을 위해 안심하고 개인의 정보를 제공하고, 개인정보를 획득한 기업이 개인의 정보를 안전하게 지켜줄 것이라는 신뢰를 형성하여 산업의 활성화를 유도하기 위해서는 산업의 특성상 개인정보를 많이 취급하여 기업과 소비자 모두 보안에 민감할 수밖에 없는 공공·금융·인터넷·통신 분야의 기업 및 공공기관을 우선 대상으로 하는 정기적인 보안 관련 외부평가 또는 정보공개 제도(공시제도 등)의 도입이 필요하다.

본 논문에서는 의무적이고 강제적인 기업 및 공공기관의 정보보안 정보공개를 위한 제도로서 정보보안 공시제도 도입의 타당성 및 필요성을 분석하였다. 이를 위해 기존의 공시제도의 추진절차 및 추진목표를 살펴보고 기본 프레임워크를 벤치마킹하였다. 또한, 정보보안 관련 국내외 제도를 살펴보고 정보보안 공시제도에서 제시되어야 할 내용을 정리하였다. 이러한 문헌분석의 과정을 통해 정보보안 공시제도(안)를 마련하여 관련 전문가를 대상으로 검토를 받고 그 필요성과 타당성에 대한 의견을 수렴하였으며, 설문조사를 통해 제도화되었을 경우의 업계의 반응도 분석하였다.

II. 기존 제도에 대한 고찰

2.1 공시 관련 제도에 대한 고찰

공시(disclosure)란 용어는 '비밀 따위를 밖으로 드러내는 것'이라는 뜻으로 기업의 비밀에 속하는 특정한 사실을 정보화하여 이해당사자에게 공개적으로 전달하는 것을 의미한다〔2,3〕. 의무적으로 국내에서 시행되고 있는 공시제도로는 기업공시, 환경정보 공개제도, 교육정보공시, 부동산공시, 공공기관 경영정보 공개 등이 있다〔표 1 참조〕. 본 논문에서는 기존 시행되고 있는 공시제도들을 분석하여 정보보안 공시제도가 갖춰야 할 기본 프레임워크(공시내용, 공시범위, 공시방법, 공시대상 등)를 구성하였다.

2.2 기업공시

기업공시는 상장기업으로 하여금 자사주식의 투자판단에 중대한 영향을 미칠 수 있는 중요한 기업내용의 정보를 공시하도록 함으로써 투자자가 기업의 실체를 파악하여 투자결정을 할 수 있도록 하는 제도이다. 기업공시제도는 증권시장 내의 정보의 불균형을 해소하고 증권거래소의 공정성을 확보하여 투자자를 보호하는 기능을 담당하고 있다. 바람직한 공시제도의 수행을 위해서는 공시의 신속성, 정보의 정확성, 정보내용 이해의 용이성, 정보전달의 공평성 등의 요건이 만족되어야 한다〔38〕.

기업공시는 법정의무화 여부에 따라 법적·강제적 공시와 자율적·임의적 공시로 분류된다. 법적·강행적 공시는 다시 상법상의 공시와 자본시장과 금융투자업에 관한 법률(자본시장통합법)상의 공시로 분류된다. 또한, 시장별로 사본시장통합법에 따라 발생시장 공시와 유통시장 공시로 분류된다. 발행시장의 공시자료는 증권신고서, 투자설명서, 증권발행실적 보고서 등이 있으며, 유통시장의 공시자료는 사업보고서, 분기·반기보고서 등의 정기공시와 주요사항 보고서 및 거래소에 공시되는 주요경영사항 신고·공시와 공정공시, 조회공시, 자율공시 등이 있다〔2, 3, 10〕.

상장법인은 증권거래소에 공시하여야 하는 기업내용을 문서로 작성하여 이를 증권거래소 등의 공시기관에 우편, 인편, FAX 등의 방법으로 공시하여야 한다. 전자문서의 방법으로도 공시할 수 있도록 하는 전자공시도 시행 중인데, 상장법인으로 하여금 동일한 공시사항을 다수의 증권관계 기관에 중복적으로 전산네트

〔표 1〕 기존 공시제도 비교

구 분	대상기관	매체 및 방법	내용	기타
기업공시	상장기업, 코스닥등록 법인	• 문서 : 공시기관 책자 • 전자 : 전자공시시스템 (KIND시스템 등)	• 회사의 개황, 사업의 내용 등 • 기타 투자자 보호를 위하여 필요한 사항 등	• 자본시장과 금융투자업에 관한 법률 등 • 기업은 보수적 공개 입장
환경정보 공개제도	녹색기업, 공공기관, 환경민감기업 등 총 1,100여개 기업 및 기관	• 회계연도 시작 후 3월 이내에 환경정보공개시스템에 정보를 등록해야 함	• 기업개요(사업현황 등) • 녹색경영 전략 및 녹색경영 시스템 • 자원/에너지 • 온실가스/환경오염 • 녹색제품/서비스 • 사회/윤리적 책임	• 환경기술 및 환경산업 지원법
교육정보공시	학교, 교육행정기관, 교육연구기관 등 (교육관련 기관)	• 기관별 홈페이지 • 양식은 교과부 장관이 마련·보급	• 공시일 기준 최근 1년 정보 (매년1회 이상 공시) • 학생관련기록, 교육행정정보, 학교내부기록 등	• 교육정보공시법 (특별법, 교육법체계 복잡화 논란) • 제도정비 및 개인정보노출 논란
부동산공시	국가, 지방자치단체, 법원 (3자)	• 공적장부/관보에 등록, 등기, 게재 등 • 부동산공시가격 알리미 사이트 (국토해양부)	• 지적공시 • 건축물공시 • 권리관계공시/거래가격공시 • 평가가격공시	• 공시기관/ 공시내용 일원화 논란 계속 • 소유의 권리보호와 제3자의 권리/이익 해하지 않는 것이 목표
공공기관 경영정보 공시	공기업, 준정부기관, 기타 공공기관 (286개)	• 알리오시스템에 통합/공시 (기획재정부)	• 정원(현원), 인건비, 복리후생비, 노동조합 운영현황, 주요 재무 정보 등 (34개 항목)	• 정기/수시 • 공공기관 운영에 관한 법률, 공공기관의 정보공개에 관한 법률

워크를 통하여 신속·정확하고 광범위하게 전달받도록 하는 이점이 있어 현재 우리나라의 상장법인과 코스닥 등록법인들이 기본적으로 이용한다.

2.1.2 환경정보 공개제도

환경경영(Environmental Management)에 대한 관심이 높아지면서 시작된 환경정보 공개제도(Environmental Disclosure)는 정보보안 공시제도와 유사하게 공개되는 정보의 자산적 가치보다는 사회적 중요성에 의해 도입된 정보공개 제도이다.

기업경영정보 공시시 또는 기업의 연차보고서 작성시 환경투자 및 환경보호를 위한 사회적 투자 등의 항목을 자율적으로 제시하도록 되어 있던 '환경회계제도(1996년 증권감독원이 기업회계기준을 개정하면서 시작)'로 출발해 보다 높은 환경효익을 달성하고 기업의 적극적인 환경투자를 유도하기 위한 수단으로 '환경정보 공개제도'로서 2007년 제도 도입의 타당성 분석을 위한 정책과제로 시작되어 공청회와 기관설명회 등을 거쳐 5년만인 2012년 9월 본격 시작될 예정이다. 대상은 녹색기업, 공공기관, 환경민감기업 등 총 1100여개 기업 및 기관이며, 내용은 자원·에너지 절약, 환경오염물질 배출저감 목표·실적, 녹색경영 활동 등이다〔12,15,33〕.

환경정보공시 관련 연구는 환경정보공시 도입의 자발적 공시(공개) 대비 환경적·경제적 영향 분석〔16, 19,25,30〕, 환경정보공시 도입과 이해관계자들과의 관계 분석〔17,18,20,28〕, 환경정보공시 도입의 결정요인〔23,26,28,29,31〕 등이 이루어지고 있다. 기업의 환경경영을 위한 사회적 활동이나 투자활동을 공시하는 환경정보공시는 결코 기업의 기밀정보 또는 공개될 경우 또다른 침해의 가능성을 주는 등의 위험한 정보가 아니므로 공시의 내용이나 기본 프레임워크에 대한 검토보다는 환경정보공시가 제도화 될 경우의 효과를 분석하는 연구가 주로 수행되고 있는 것으로 파악된다.

2.1.3 교육정보공시

교육정보란 교육활동과 교육제도에 관한 정보이며 여기에는 학생 관련 기록, 교육행정기록, 학교내부기록 등이 포함된다〔41〕. 교육정보공시란 교육관련기관

이 보유·관리하는 정보를 국민의 정보공개에 대한 열람·교부 및 청구와 관계없이 미리 정보통신망 등 다른 법령으로 정하는 방법으로 적극적으로 알리거나 제공하는 공개의 한 방법이다[39]. 교육정보공시법 제정 이전 교육정보는 주로 정보공개법의 규정에 의거하여 교육기본법, 초·중등교육법 등 교육관계 법률에 따라 공개되어 왔다.

교육정보공시는 헌법상 보장된 국민의 알권리를 충족시키고 국민의 교육받을 권리를 보장해 줄 것이라는 기대가 큰 제도이지만, 정보공개법에 충분히 많은 공개대상정보가 무엇인지 공개방법은 무엇인지 등에 대한 설명이 있음에도 불구하고 특별법 형태로 제정되어 시행됨에 따라 교육법체계를 매우 복잡하게 만든다는 단점이 제시되었으며, 공시대상 정보의 과다, 학업성취도 등 주요 사회적 관심정보의 공시방법, 정보공시 시기의 비탄력성, 제도운영의 구체적 방안의 미비, 교육행정기관 및 교육연구기관의 정보공시 대상항목 규정의 흠결, 적극적 개인정보 보호대책의 미흡, 정보공시 신뢰성 확보 및 정보공시 불이행에 대한 대책 부족 등의 문제가 제시되고 있다.

2.1.4 부동산공시

부동산공시의 목적은 부동산의 물적사항, 권리관계, 가격 등을 공시함으로써 누구나 그 공시내용을 쉽게 알수 있도록 하고 소유자 자신의 권리가 어떻게 보호되고 있는지를 예측 가능하도록 하는 한편 제3자의 권리·이익을 해하지 않도록 하는 것이다[40]. 부동산 공시기관은 국가, 지방자치단체 및 법원으로 3원화되어 있으며, 공시방법은 공적장부와 관보에 등록·등기·게재 등의 방법이 있다. 부동산공시제도는 측량·수로조사 및 지적에 관한 법률에 근거한 지적공시제도, 건축법에 근거한 건축물공시제도, 부동산등기법에 근거한 권리관계공시제도 및 거래가격공시제도, 부동산가격공시 및 감정평가에 관한 법률에 근거한 평가가격공시제도 등으로 분류된다.

2.1.5 공공기관 경영정보공개

기획재정부는 2006년 12월 '알리오시스템(www.alio.go.kr)'을 구축하여 286개 공공기관의 경영정보를 통합하여 공시하고 있다[32]. 공개되는 사항은 정원, 인건비, 복리후생비, 노동조합 운영현황, 주요 재무정보 등 34개 항목이다. 공시주기는 정기공시와 수시공시로 구분하여 운영되며, 정기공시는 연간(4월말), 반기(4, 10월말), 분기(1, 4, 7, 10월말)로 구분되어 제공된다. 수시공시는 사유 발생일 기준 14일 이내에 공시하도록 되어 있다.

2.2 보안 관련 제도에 대한 고찰

현재 우리나라에서는 기업의 정보보안 현황을 알 수 있는 제도로서 여러 가지 인증 및 마크 제도가 있으나, 인증을 받기 위한 보고서를 자사 홈페이지에 공개 또는 공시할 의무는 없으며 다만 소비자에게 인증 보유현황 등을 보도자료나 홍보자료를 통해 제공하고 있는 수준이다. 국내외에서 기업 및 공공기관의 정보보안 정보를 알 수 있는 또는 유추할 수 있는 제도로는 정보보호 안전진단, 정보보호관리체계 인증(Information Security Management System, ISMS), 전자정부 정보보호관리체계 인증(G-ISMS), 영국 BSI의 ISO 270001(국제 정보보호관리체계), 국가정보원의 보안관리실태 평가, 개인정보보호관리체계 인증(Personal Information Management System, PIMS) 등이 있다[표 2 참조]. 본 논문에서는 이상의 제도에서 심사시 요구하는 기관의 보안정보의 내용을 정보보안 공시제도에서 담아야 하는 공시내용으로 설정하였다.

2.2.1 정보보호 안전진단

정보보호 안전진단은 주요 정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등의 정보통신서비스제공자의 정보통신망에 대한 침해사고 예방을 위하여 도입된 제도이다. 안전진단 대상자가 의무적으로 준수해야 할 '정보보호 조치 및 안전진단 방법·절차·수수료에 관한 지침'에 대한 이행여부를 안전진단 수행기관으로부터 매년 확인받도록 하고 있다[13,35].

정보보호 안전진단에서 제시하고 있는 정보보호 조치는 관리적, 기술적, 물리적 차원으로 나뉜다. 관리적 조치로는 정보보호조직의 구성·운영, 정보보호계획 등의 수립 및 관리, 인적보안, 이용자 보호, 침해사고 대응, 정보보호조치 점검, 정보자산 관리 등이 포함되며, 기술적 조치로는 네트워크 보안, 정보통신설비 보안 등이 포함되며, 물리적 조치로는 출입 및 접근 보안, 부대설비 및 시설 운영·관리 등이 포함된다.

〔표 2〕 국내외 정보보안 관련 제도 비교

구 분		주관기관	정보보안 정보
정보보호 안전진단		방통위	• 관리적/기술적/물리적 보호조치 (정보보호조직의 구성/운영, 네트워크 보안, 출입 및 접근 보안 등)
정보보호 관리체계	ISMS	KISA	• 정보보호 정책, 정보보호 조직, 자산관리, 인력자원 보안, 물리적 및 환경보안, 통신 및 운영관리, 접근통제, 정보시스템 구축/개발/유지, 정보보호 사고관리, 사업연속성 관리, 적법성 등
	G-ISMS	행안부	
	ISO 27001	영국 BSI	
공공기관 보안관리실태 평가		국가 정보원	• 정책 및 업무수행, 정보자산 관리, 비밀관리, 인적보안, 침해사고 대응체계 구축, 접근보안, 운영관리, 물리적 보안
개인정보 보호 관련제도	PIMS 인증	KISA	• 관리과정(개인정보 정책수립, 관리체계 범위설정, 위험관리, 사후관리) • 보호대책(개인정보보호 정책, 개인정보보호 조직, 개인정보 분류, 교육 및 훈련, 인적보안, 침해사고 처리 및 대응절차, 기술적 보호조치, 물리적 보호조치, 내부검토 및 감사 • 생명주기 준거(개인정보 수집, 개인정보 이용 및 제공, 개인정보 관리/파기)
	개인 정보보호 마크	KAIT	• 개인정보의 수집에 관한 조치, 개인정보의 이용 및 관리, 이용자의 권리, 공개 및 책임, 만14세 미만의 아동에 관한 특별조치, 이용자 권리구제 등
	개인 정보보호 지수	KISA	• 관리(개인정보보호정책, 개인정보보호 조직/교육), 기술/물리(보안기술, 물리적 보안, 개인정보보호정책)
	공공기관 개인정보보호수준	행안부	• 개인정보보호 정책환경(정책기반, 기술기반), 개인정보 처리분야(수집 및 보유, 이용 및 제공, 파기), 개인정보 침해대응(웹사이트 개인정보 노출방지대책, 개인정보유출 대응절차, 개인정보 침해 구제절차)
금융권의 보안강화 대책	금융회사 IT보안강화 종합대책	금융위/ 금감원	• IT 조직역량 강화 및 보안투자 확대, IT 업무 감독검사 강화 및 제도개선, IT 보안기술 인프라 및 내부통제 개선, IT 아웃소싱 관리 개선, IT 사고대응 및 재해복구 체계 강화
	사이버보안사고 공개에 대한 가이드라인	미국 SEC	• 기업의 재정적 손실을 야기할만한 수준의 보안사고가 발생한 경우 관련 정보 또는 잠재적인 보안사고의 가능성을 공표

2.2.2 정보보호관리체계 인증

한국인터넷진흥원(KISA)이 시행하고 있는 인증으로 대상 사업자가 자율적으로 신청하는 권고사항으로 '정보보호정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 근거하고 있다〔35〕. 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계에 대하여 제3자의 인증기관이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도이다.

심사기준은 3개 통제분야에 총 137개 통제항목으로 구성된다. 통제분야는 정보보호 관리과정(5단계, 14개 통제항목), 문서화(3개 통제항목), 정보보호 대책(15항목, 120개 통제항목)이다. 정보보호 관리과정에는 정보보호정책 수립, 관리체계범위설정, 위험관리, 구현, 사후관리 등이 포함되며 문서화에는 문서요건, 문서의 통제, 운영기록의 통제 등이 포함된다. 마지막으로, 정보보호 대책에는 정보보호 정책, 정보보호 조직, 외부자 보안, 정보자산 분류, 정보보호 교육 및 훈련, 인적보안, 물리적보안, 시스템개발 보안, 암호 통제, 접근 통제, 운영 관리, 전자거래 보안, 보안사고 관리, 검토, 모니터링 및 감사, 업무연속성 관리 등이 포함된다.

2.2.3 전자정부 정보보호관리체계 인증

전자정부 정보보호관리체계 인증(G-ISMS)은 기관이 수립하고 구축한 종합적인 정보보호관리체계를 제3자가 객관적으로 심사하여 인증을 부여하는 것으로 행정안전부에 의해 시행되고 있다〔35〕. 정부 행정기관 등의 조직 및 서비스의 특성에 적합하게 수립된 종합적인 정보보호관리체계로, 행정안전부의 '전자정부 정보보호관리체계 인증업무 지침'에 따라 지자체에 대해 정보보호 관리과정, 문서화, 정보보호 대책 등 정보보호 관리체계가 적절하게 수립·관리되고 있는지를 평가하여 인증하는 제도이다. 행정안전부와 한국인터넷진흥원이 인증심사 및 인증서 발급을 시행하고 있다.

2.2.4 ISO27001

국제적인 정보보호관리체계 인증으로 정보보호 경영시스템 요구사항을 정의하며, 적합한 보호관리시스템을 선택할 수 있도록 고안된 유일한 국제 표준이다. 인증을 위한 심사기준은 정보보호정책, 물리적 보안, 정보접근 통제 등 정보보안 관련 11개 영역, 133개 항목으로 구성되며, 국제 심판원들의 엄격한 심사와 검증을 통과하여야 한다[37].

정보보안 관련 11개 영역은 정보보호정책, 정보보호조직, 자산관리, 인력자원보안, 물리적 및 환경보안, 통신 및 운영관리, 접근통제, 정보시스템 구축·개발·유지, 정보보호 사고관리, 사업연속성 관리, 준수(compliance) 등이다.

2.2.5 공공기관 보안관리실태 평가

국가 주요 공공기관의 정보보안 관리 수준에 대한 종합평가로서 국가정보원 산하 국가사이버안전센터(National Cyber Security Center, NCSC)에서 실시하고 있다. 중앙행정부처·광역자치단체·주요 공공기관 등 총 100여개 국가·공공기관을 대상으로 정보보안 관리수준을 종합적으로 평가한다[1].

정보보안 규정 운영, 전자우편 보안, 악성코드 대응 등 기본항목에서부터 USB 메모리 사용, 노트북 디지털사무기기 등 최신 보안 이슈에 이르기까지 9개 분야 246개 항목에 대해 평가한다.

2.2.6 개인정보보호관리체계 인증

개인정보보호관리체계(PIMS) 인증은 기업이 개인정보 보호활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도이다[14,36].

PIMS 인증은 기업 자율제도로서 운영되고 있으며, 심사기준은 3개 통제분야에 118개 통제항목으로 구성된다. 통제분야는 개인정보보호 관리과정(5단계, 11개 통제항목), 개인정보보호 보호대책(9항목, 79개 통제항목), 생명주기 준거(3단계, 29개 통제항목) 등이다. 관리과정에는 개인정보 정책수립, 관리체계 범위설정, 위험관리, 구현, 사후관리 등이 포함되며, 보호대책에는 개인정보보호 정책, 개인정보보호 조직, 개인정보 분류, 교육 및 훈련, 인적보안, 침해사고 처리 및 대응절차, 기술적 보호조치, 물리적 보호조치, 내부검토 및 감사 등이 포함된다. 생명주기 준거에는 개인정보 수집, 개인정보 이용 및 제공, 개인정보 관리 및 파기 등이 포함된다.

III. 정보보안 공시제도에 대한 검토

3.1 정보보안 공시제도의 필요성 검토

정보보안 공시제도의 도입의 타당성 및 필요성에 대해 검토하기 위해 각종 공시제도와 정보보안 제도를 토대로 정보보안 공시제도의 초안(draft)을 마련하고 이에 대한 전문가들의 의견을 수렴하였다.

전문가 의견수렴은 공시제도 초안 작성을 위해 공시제도 운영 관련 전문가들을 대상으로 수행한 심층인터뷰와 심층인터뷰를 통해 정리된 공시제도 초안에 대한 서면 조사로 구분하여 단계적으로 수행하였다. 1단계 심층인터뷰는 2011년 10월 중순부터 11월 중순까지 5주간 수행하였으며, 기업경영 공시제도의 운영(방식, 내용 등)에 대해 공시제도의 운영기관(금융감독원, 한국거래소), 공시자료 작성 및 검증기관(회계법인), 공시제도 시행기관(금융기관 CIO) 등의 관계자들과의 검토를 받았다. 2단계로 수행한 공시제도 초안에 대한 의견 조사는 2011년 11월 말부터 12월 초까지 2주간 금융기관 CIO 및 공시담당자를 대상으로 진행하였다. 조사대상은 다소 생소한 정보보안 공시제도에 대해 묻는다는 점에서 기존 기업공시제도에 대해 잘 이해하고 있는 전문가들과 최근 규제기관의 보안대책 강화로 보안 관련 제도에 민감한 국내 대형금융기관의 CIO들로 선정하였다(CIO 대상 조사는 금융감독원 및 한국거래소의 협조로 진행).

3.1.1 정보보안 공시제도의 운영절차

기업정보공시의 필수서류 수정만으로 우선 실시하는 것이 타당하다는 의견을 수렴하였다. 처음 시행부터 별도의 제도인 정보보안 공시제도로 시행될 경우 대상기관들의 혼란과 어려움이 예상되기 때문에 이를 최소화하기 위한 도구로서 기존의 기업공시제도와의 병행시행이 타당하다는 의견을 수렴하였다. 그러나, 미국 SEC(Securities and Exchange Commission)에서도 2011년 10월 기업의 재정적 손실을 야기할만한 수준의 보안사고가 발생한 경우 관련 정보 또는 잠재적인 보안사고의 가능성을 공표하도록 하는 새로운 가이드라인을 제정하여 발표된 바[42], 정보보안 공

시제도의 도입은 반드시 필요한 절차라 할 수 있다.

3.1.2 정보보안 공시제도의 공시대상

최우선적으로 금융기관 및 공공기관에 대해 적용한 후, 단계적으로 범위를 확대하는 방안이 타당하다는 의견을 수렴하였다. 의무기업과 선택기업을 선별하여 적용하고 단계적으로 확대하자는 의견이다. 최근 3년간 보안침해사고 발생 경험이 있고 그로 인한 금전적·사회적 피해 및 고객정보의 유출로 인한 고객피해가 발생한 기업이나 증권거래소에 상장된 700여개 법인 가운데 업종별 특성 및 보안인식의 수준에 따라 단계적으로 확대하는 방안이다.

최근 개인정보보호의 중요성이 확대되고 있으므로 개인정보보호관리체계(PIMS) 인증의 대상기관 및 인증보유기관을 우선 적용하는 방안도 고려할 수 있다. 기업마다 외부에서는 미처 인지하지 못하고 있는 특수성이 있을 수 있고 보안(정보)에 대한 민감도가 다를 수 있으므로 이에 대해서는 매우 신중한 접근이 필요하다.

3.1.3 정보보안 공시제도의 공시내용

현재 대표적인 공시제도인 기업공시제도에 대해서도 기업에서는 매우 보수적인 입장을 취하는 것이 현실이다. 최소한의 정보를 제공하고자 하는 기업과 최대한의 정보를 알고자 하는 정부나 개인 및 투자자들의 입장이 대비되고 있는 것이다. 정보보안 관련 정보는 특히 매우 보수적일 수 밖에 없다. 기업의 보안현황 즉 보안투자 내역이나 보안설비나 인력 보유내역 등을 공개하는 것은 또 다른 위협을 발생시키는 원인이 될 수도 있는 것이다.

정보보안 공시제도의 공시내용은 투자자 및 일반인의 알권리 보호를 위한 최소한의 내용인가, 공개할 경우 기업이나 공공기관에게 피해가 발생할 가능성은 없는가, 공개할 경우 악의적인 자(해킹)로부터의 또다른

〔표 3〕 정보보안 공시제도 공시내용

구 분	공시항목	공시내용
필수사항	정보보안 조직	• 전담조직 구성 현황 • CEO의 책임범위 및 CIO/CISO 지정 여부 및 계획 • CEO/CIO에 대한 정기적인 정보보안 보고체계, 침해사고 대응범위(권한) 임명 여부 및 계획
	정보보안 투자	• 전체 인력 대비 보안전담인력 비율 (내부 및 아웃소싱 구분, 3년~5년 중장기 계획) • 전체 정보화예산 대비 보안예산 비율 (현황 및 3년~5년 중장기 계획) • 보안예산 확보계획 (3년~5년 중장기 계획)
	정보보안 인프라	• 정보보안시스템 구축 현황(인소싱/아웃소싱) • 보안인프라 구축계획 (3년~5년 중장기 계획)
선택사항	정보보호 정책	• 정보보호 정책
	정보보호 조직	• 기관장의 관심, 내부조직 설계, 외부조직 관리
	인력자원 보호	• 고용 전/중/변경 및 종결 관리, 외부자 보안
	정보자산 관리	• 자산관리의 책임, 정보자산 조사/책임할당, 정보자산의 분류/취급
	물리적 및 환경적 보안관리	• 정보보호 구역, 장비보호, 사무실 보호
	통신 및 운영관리	• 운영절차 및 책임, 제3자 서비스 관리, 시스템 계획 및 인수, 백업, 모니터링 등
	접근통제	• 접근통제 정책, 사용자 접근관리, 모바일 컴퓨팅 및 텔레워킹 등
	정보시스템 구매, 개발 및 유지보수	• 분석/설계 보안관리, 구현/이행 보안관리, 변경관리, 기술적 취약점 관리
	정보보호 사고관리	• 보안사고 대응계획/체계, 정보보호사건 및 약점에 대한 보고, 정보보호 사건관리/개선, 사후관리
	사업연속성 관리	• 사업연속성 관리
	정보보호 교육 및 훈련	• 교육 및 훈련 프로그램
	검토, 모니터링 및 감사	• 법적요구사항 준수검토, 정보보호정책 및 대책준수 검토, 모니터링, 보안감사
	개인정보보호	• 개인정보보호 관리/보호대책, 생명주기준거, 개인정보 침해대응
	법규 준수	• 법률요구조건들을 위한 준거성, 정보보호정책/규정 및 기술적 준거성에 대한 준수

〔표 4〕 정보보안 공시정보 검증방법

검증항목	검증내용	방법
내용 충실도	• 기재된 내용이 지침에 따라 작성되었는가? • 누락된 정보 또는 불분명한 정보가 없는가?	서면 검토
정보 신뢰성	• 기재된 내용이 실제와 다르지 않은가? • 최신 현황에 대한 시의성이 있는 정보인가? • 기업 환경정보 관리체계가 적정한가?	현장 검증
비교 가능성	• 데이터의 단위 및 시점이 적정한가? • 그래프, 수치 등이 일관성이 있는가?	서면 검토

공격의 대상이 될 가능성은 없는가, 기업이나 공공기관의 안정적인 운영에 해가 될 소지는 없는가 등을 고려하였다. 따라서, 정보보안 공시제도에서 포함하여야 할 공시내용은 필수사항(의무사항)과 선택사항으로 구성하는 것이 적절하다. 선택사항은 그 내용이 기업 경영정보이거나 기업이 보유한 내외부의 개인정보로서 보안에 매우 민감할 수 있다는 점을 고려하여 단계적으로 확대해 나갈만한 내용을 포함한다〔표 3 참조〕.

필수사항으로는 정보보안 조직, 정보보안 투자, 정보보안 인프라 등이 적정하다, 선택사항으로는 정보보호 정책, 정보보호 조직, 인력자원 보호, 정보자산 관리, 물리적·환경적 보안관리, 통신·운영관리, 접근통제, 정보시스템 구매·개발·유지보수, 정보보호 사고관리, 사업연속성 관리, 정보보호 교육·훈련, 검토·모니터링·감사, 개인정보보호, 법규 준수 등이 적정하다.
정보보안 공시제도의 검증방법

정보보안 데이터 또는 정보보안 보고서에 대한 제3자 검증체계를 마련하여 보고내용의 신뢰성을 검증하도록 하는 정보보안 공시정보 검증체계도 필요하다. 공시내용의 독립성과 전문성에 대한 검증기관의 자격요건을 규정하여 검증기관을 지정하고, 금정수수료는 실비기준 단가를 책정하여 고시하도록 하는 방안도 고려해 볼 수 있다〔표 4 참조〕.

3.2 정보보안 공시제도 도입의 타당성

본 연구에서 마련한 정보보안 공시제도의 운영형태와 정보공개의 범위 정도를 기준으로 하였을 때 정보보안 공시제도의 도입의 타당성과 제도 도입시 예상되는 어려움은 어느 정도가 되는지에 대해, 2011년 11월 말에서 12월 초까지 2주간에 걸쳐 18명의 국내 대형 금융기관의 CIO 및 공시담당자들의 의견을 수렴하였다.

그 결과, 정보보안 공시제도의 도입의 필요성에 대해서는 비교적 필요하지 않다(평균 3.3점; 1점 거의 없다, 4점 보통, 7점 매우 필요하다)고 응답하였으며, 제도가 도입될 경우 비교적 부담된다(평균 5.1; 1점 거의 없다, 4점 보통, 7점 매우 부담된다)고 응답하여 제도의 도입에 대해 신중하게 접근해야 할 것으로 분석되었다. 이는 1차 심층인터뷰의 결과와 동일한 것으로 처음 시행부터 별도의 제도인 정보보안 공시제도로 시행될 경우 대상 기관들의 혼란과 어려움이 예상되기 때문에 이를 최소화하기 위한 도구로서 기존의 기업공시제도와의 병행 시행이 타당하다는 의견과 궤를 같이 한다. 부담을 느끼는 주요 이유로는 보안정보 공개에 대한 부담이 높다는 점과 별도의 제도 시행으로 인한 추가적인 인력채용 및 전문교육의 부담이 높다는 의견이 많았다. 정보보안 공시제도의 시행 범위에 대해서도 별도의 제도로 시행하기보다는 기존 보안내역 보고서의 공개로 대체하는 것이 좋겠다는 의견이 전체의 50%가 넘어 매우 소극적인 반응을 보였으며, 정보보안 공시제도가 시행될 경우 정기공시의 형태가 적정하다는 의견이 전체의 72%로 나타났다.

그러나, 국내외 금융권에서 시작되고 있는 정보보안 정보의 공개를 통한 강제적인 보안투자 유도의 움직임은 갈수록 더해가고 있는 보안위협에 대한 기업의 적극적인 보안투자를 담보할 수 있는 제도가 될 수 있을 것으로 기대된다. 따라서, 단계적으로 제도의 범위를 확대해 나가면서 그 타당성과 필요성에 대해 설득할 수 있는 접근이 필요하다. 우선적으로는 제도의 안정적인 시행을 위해 정보보안 공시제도에서 포함될 정보의 공개범위에 대해 산학연관이 모두 참여하는 광범위한 협의가 선행되어야 할 것이며, 이와 함께 정부 차원에서 공시제도의 시행을 이끌어갈 수 있는 보안과 공시제도를 모두 이해할 수 있는 전문인력의 양성 및 기존 인력에 대한 재교육 프로그램의 운영도 필요하다.

〔표 5〕 정보보안 공시제도의 도입이 부담되는 이유 (2단계 공시제도 초안에 대한 의견 조사 결과)

구분	의 견
#1	보안에 대한 적극적인 투자 등은 고객의 회사에 대한 신뢰도, 이미지 향상의 효과를 주지만, 악의적인 해커의 목표물 탐색에 악용될 소지가 있음
#2	과도한 정보 제공에 따른 부담감 증가
#3	공시위한 자료 준비, 정확성/적합성 등 업무프로세스 추가·강화
#4	인력 및 예산부문에서 권고수준을 충족하고 있으므로 추가적인 제도의 시행은 부담됨
#5	제도가 시행되면 그에 따른 많은 비용이 수반됨
#6	인력 및 업무 가중에 대한 부담이 따름
#7	정보보안 공시제도에 대해 제대로 대처하지 못할 경우 또는 보안사고가 발생하여 이를 공개할 경우 기업의 이미지·명성에 해가 될 수 있음
#8	정보보안 공시제도의 시행에 따라 별도의 예산 및 인원을 확보해야 한다는 부담이 큼
#9	현 시점에서는 정보보안 공시제도의 역할과 목표가 명확하지 않으므로 정확한 양(+)적 음(-)적 영향 파악 불가
#10	공시의 빈도나 내용의 깊이에 따라 차이가 있겠으나 추가적으로 수행하여야 한다는 업무 부담은 발생할 것으로 예상됨
#11	해커가 공시자료를 토대로 특정회사의 보안 취약여부를 가늠하여 상대적으로 낮은 회사를 공격 대상으로 삼을 가능성이 높으므로 보안정보를 공개하는 것 자체가 우려됨
#12	기존 공시제도에 대한 업무강도 및 전문인력이 부족해 추가적인 제도 시행은 큰 업무 부담임
#13	정보보안 공시제도의 정확한 공개수준 및 역할에 대한 정의가 제시되지 않은 상황이므로 그 영향을 판단하기 어려움
#14	정보보안 업무에 대한 이해 등 해당공시를 위한 인력·시간이 추가적으로 소요될 것으로 예상됨

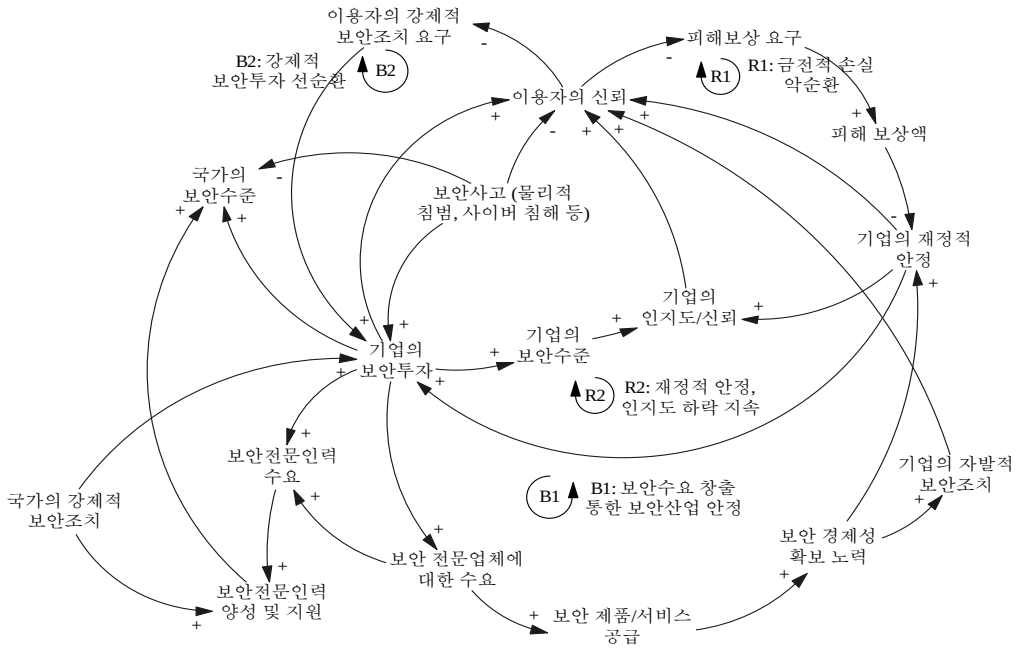
3.3 정보보안 공시제도 도입의 필요성

본 연구에서는 정보보안 공시제도의 필요성 및 타당성에 대한 연구를 진행하기 위해 문헌연구를 통해 정보보안 공시제도(안)을 마련하고 이에 대해 전문가들의 의견을 수렴하였다. 그러나, 이 초안은 정책적 드라이브를 통해 마련된 것도 아니고 몇몇 관련 공시제도와 보안제도를 벤치마킹하여 마련한 것으로 전문성도 부족하다. 따라서, 사실상 도입되었을 때의 효과를 정량적으로 분석하는 것은 시기상 어려웠다. 그러나, 환경정보 공개제도 시행의 예에서도 볼 수 있듯이, 국민적·사회적 기대효과를 통해 유사한 취지로 추진되고 있는 정보보안 공시제도 도입의 필요성은 매우 높으나, 국내 금융기관 CIO들을 대상으로 실시한 설문조사에서는 사실상 별도의 제도로서의 시행보다는 기존 경영공시 수준에 준하는 정도에서 실시되는 것을 선호하는 것으로 나타났다. 결과적으로, 제도의 도입 자체를 검토하기 전에 정보보안 공시제도의 도입효과에 대한 정량적·정성적 분석이 있어야 여러 이해관계자들을 설득할 수 있을 것으로 분석된다.

본 논문에서는 정성적인 정보보안 공시제도 도입의 효과를 분석하기 위해 시스템적 사고방식 기반의 시뮬레이션 모델링 기법의 하나인 인과지도(causal-loop diagram)를 이용하였다〔21,22,24,27〕.

정보보안 공시제도의 의무화(국가의 강제적 보안조치)는 기업과 공공기관이 정기적으로 내·외부의 인프라를 점검하고 보안조치를 취하고 보안을 위한 지속적인 투자를 할 수 있도록 하는 하나의 장치가 될 수 있을 것이다. 이는 기업의 보안수준을 높이고 기업의 인지도 및 신뢰를 높이는 것은 물론 안정적인 경영환경 구축을 통해 기업의 보다 높은 발전을 위한 발판이 될 것이다. 이에 일반 국민들은 이러한 기업 및 공공기관을 믿고 안심·안전하게 이용할 수 있어 소비활동을 촉진함으로써 내수시장 활성화도 기대할 수 있다. 보안사고의 발생으로 떨어진 이용자의 신뢰는 피해보상 요구와 소송 등으로 이어지고 이는 기업의 재정상태를 악화시킬 수 있으므로, 이러한 악순환이 생기기 전에 기업의 지속적인 보안에 대한 투자의 기반을 닦고 이용자의 신뢰를 유지하는 것은 매우 중요한 활동이라 하겠다. 궁극적으로, 기업의 지속적인 보안투자는 보안 전문업체에 대한 수요로 이어지고 이는 보안투자로 인한 경제성 확보 노력으로 이어져 기업의 자발적 보안조치의 증가를 통한 보안산업에의 수요 증가로 이어지는 선순환을 통한 지식정보보안산업의 발전도 기대해 볼 수 있다〔그림 1, 표 6 참조〕.

현재, 정보보호 안전진단 등으로 정부가 보안컨설



*주석: 화살표의 방향대로 영향을 주고받는 관계임. +는 양의 영향(같은 방향의 영향. 예를 들어, A→B에서 A가 많아짐으로써 B도 많아진다면 +)을 주는 것을 의미하며 -는 음의 영향(다른 방향의 영향)을 주는 것을 의미. 피드백을 형성하는 루프에 B(Balancing), R(Reinforcing)의 성격을 부여하게 되며, B는 시스템 전체에 균형을 가져오는 루프이며 R은 계속 강화(악화, 순화)시키기만 하는 루프

〔그림 1〕 인과지도(Causal-Loop Diagram)를 이용한 정보보안 공시제도 도입의 필요성 도식화

팅 업체를 지정·운영하고는 있지만 실질적으로 정보보안산업의 파이를 키우는 데에는 크게 기여하지 못하고 있다. 그러나, 정보보안 공시제도는 기업과 공공기관의 실질적인 보안투자를 촉진함으로써 정보보안산업의 양적인 성장을 꾀할 수 있을 것으로 기대되며, 이는 다시 기술력 향상을 위한 투자로 이어져 정보보안산업의 질적인 성장과 전문인력 확보를 위한 기반을 다질 수도 있다.

〔표 6〕 정보보안 공시제도 도입의 정성적 기대효과

구 분	긍정적인 효과	부정적인 효과
국가	• 정보통신인프라 확대/강화 • 정보통신 및 정보보호 관련 산업·기술경쟁력 강화	• 악의적인 보안공격
기관 (기업/공공) -보안수요-	• 보안투자 확대를 통한 보안 강화 • 보안전담인력 확보 가능 • 지속적인 보안점검 가능 • 투자자들의 신뢰를 향상시킬 수 있는 계기가 될 수 있음 (증권시장에서의 호재)	• 기관 내부 정보의 원하지 않는 유출 및 외부에서의 유추 가능 • 외부에서 기관의 보안인프라 현황 유추를 통한 새로운 보안공격 가능 • 보안투자에 대한 부담감 증가, 예산상의 어려움 가중
정보보안 산업 -보안공급-	• 기관의 보안투자 확대로 제품/컨설팅(인력)에 대한 수요 확대 기대 • 보안기술개발에 대한 투자확대로 질적성장 기대	• 바이러스 백신, 스팸 차단 등에 대한 공짜 제공 부담 가중
일반국민	• 국가/기관의 정보인프라를 안심·안전하게 이용 • 정보통신·정보보호 전공자의 경우, 취업을 원하는 기관의 투자방향을 알 수 있음	• 사용을 원하는 기관의 보안공시 내용이 미비할 경우 사용을 꺼리게 될 수 있음

IV. 결론 및 시사점

정보보안 공시제도의 실행으로 보안침해사고가 얼마나 줄어들 수 있을 것인지는 정확히 알 수 없다. 정보보안 공시제도에서 점검하는 사항들을 비껴가는 새로운 형태의 보안침해사고의 유형이 나타날 수도 있으며, 정보보안 공시제도에서 점검하는 사항들을 타겟으로 하는 보안침해사고가 새로이 발생할 수도 있다. 그러나, 정보보안 공시제도를 통해 이제까지의 기업 및 공공기관에서의 보안침해사고에 대한 대응이 '사고 발생후 대처'였던 것에서 '사고 발생전 대응'으로 전환될 수 있는 계기가 될 수 있을 것이다. 현재 대부분의 기업 및 공공기관들이 보안침해사고의 위험성과 보안투자의 필요성에 대해서는 높이 인식하고 있지만 이것이 실질적인 보안투자로 이어지지는 못하고 있다는 점에서[7], 정보보안 공시제도는 실질적인 보안투자를 강제적으로라도 시행할 수 있도록 해줄 것으로 기대된다. 물론 정부가 정보보안 공시제도를 기업을 통제하는 수단으로 활용되어서는 안된다. 그러면 오히려 기업 및 공공기관의 반발을 살 수도 있고 이에 동조하는 보안침해사고가 발생하거나 국가 인프라를 위협할 수도 있다. 결과적으로, 정보보안 공시제도는 기업공시제도와 같은 맥락에서 기업 및 공공기관의 안정적인 경영활동을 위한 수단이 되어야 할 것이며, 보안의 특성상 자국민을 보호하고 국가인프라의 안정성을 향상시키는 계기가 될 수 있을 것이다.

참고문헌

[1] 국가정보원, 보안관리실태 평가, 2009년.

[2] 금융감독원, 공정공시제도 도입방안, 2009년 9월.

[3] 금융감독원, 기업공시 실무 가이드라인, 2005년

[4] 금융위원회·금융감독원 보도자료, "금융회사 IT 보안강화 종합대책 마련," 2011년 6월 23일.

[5] 금융위원회 보도자료, "전자금융감독규정 개정·시행," 2011년 10월 10일.

[6] 금융위원회 보도자료, "전자금융거래법 시행령 개정·추진," 2011년 11월 16일.

[7] 방송통신위원회, 한국인터넷진흥원, 2010년 정보보호 실태조사(기업편), 2011년 5월.

[8] 방송통신위원회, 행정안전부, 지식경제부, 2011 국가정보보호백서, 2011년 5월.

[9] 방송통신위원회, 행정안전부, 지식경제부, 2012 국가정보보호백서, 2012년 5월.

[10] 윤계섭, 허희영, 우리나라의 기업공시제도, 서울대학교 출판부, 2005년 6월.

[11] 전자신문, "내년 2월, 정보보호감사제도 국내적용 틀 만든다", 2011년 7월 22일.

[12] 한국법제연구원, "기업의 환경정보공시 법제에 관한 고찰", 녹색성장 연구 11-19-7, 2011년 11월.

[13] 한국인터넷진흥원, 정보보호 안전진단 해설서, 2011년 2월.

[14] 행정안전부 보도자료, "공공기관 개인정보보호수준 크게 개선: 2010년 공공기관 개인정보보호수준 현장진단 결과 발표", 2011년 2월 7일.

[15] 환경부 보도자료, "지피지기! 환경정보 공개제도, 아는 만큼 앞서간다", 2012년 5월 4일.

[16] A.W. Sutantoputra, M. Lindorff and E. Prior Johnson, "The relationship between environmental performance and environmental disclosure," Australian Journal of Environmental Management, vol. 19, no. 1, pp. 51-65, Mar. 2012.

[17] C.L. Huang and F.H. Kung, "Drivers of environmental disclosure and stakeholder expectation: Evidence from Taiwan," Journal of Business Ethics, vol. 96, no. 3, pp. 435-451, Oct. 2001.

[18] D. Cormier and M. Magnan, "Environmental reporting management: A continental European perspective," Journal of Accounting and Public Policy, vol. 22, no. 1, pp. 43-62, Jan./Feb. 2003.

[19] E. Stanny and K. Ely, "Corporate environmental disclosures about the effects of climate change," Corporate Social Responsibility and Environmental Management, vol. 15, no. 6, pp. 338-348, Oct. 2008.

[20] F.K. Alnajjar, "Determinants of social responsibility disclosures of U.S. Fortune 200 firms: An application of content analysis," Advances in Environmental Accounting and Management, vol. 1, pp. 163-200, 2000.

[21] G.P. Richardson, "Problems with causal-loop diagrams," System Dynamics Review, vol. 2, no 2, pp. 158-170, Summer 1986.

〔22〕 G.P. Richardson, "Problems in causal loop diagrams revisited," System Dynamics Review, vol. 13, no. 3, pp. 247-252, Fall 1997.
〔23〕 I. Henriques and P. Sadorski, "The determinants of an environmentally responsive firm: An empirical approach," Journal of Environmental Economics and Management, vol. 30, no. 3, pp. 381-395, May 1996.
〔24〕 J.D.W. Morecroft, "A critical review of diagraming tools for system dynamics method," Dynamica, vol. 8, no. 1, pp. 20-29, Summer 1982.
〔25〕 K. Bewley and Y. Li, "Disclosure of environmental information by Canadian manufacturing companies: A voluntary disclosure perspective," Advances in Environmental Accounting and Management, vol. 1, pp. 201-226, 2000.
〔26〕 P. Healy, A.P. Hutton and K.G. Palepu, "Stock performance and intermediation changes surrounding sustained increase in disclosure," Contemporary Accounting Research, vol. 16, no. 3, pp. 485-520, Fall. 1999.
〔27〕 R.I. Hall, "Causal policy maps of managers: Formal methods for elicitation and analysis," System Dynamics Review, vol. 10, no. 4, pp. 337-360, Winter 1994.
〔28〕 R.M. Bowen, L. Ducharme, D. and D. Shores, "Stakeholders' implicit claims and accounting method choice," Journal of Accounting and Economics, vol. 20, no. 3, pp. 255-295, Dec. 1995.
〔29〕 S.M.S. Monteiro and B. Aibar-Guzman, "Determinants of environmental disclosure in the annual reports of large companies operating in Portugal," Corporate Social Responsibility and Environmental Management, vol. 17, no. 4, pp. 185-204, July/Aug. 2010.
〔30〕 W. Aerts, D. Cormier and M. Magnan, "Corporate environmental disclosure, financial markets and the media: An international perspective," Ecological Economics, vol. 64, no. 3, pp. 643-659, Jan. 2008.
〔31〕 X. Liu and V. Anbumozhi, "Determinant factors of corporate envionmental information disclosure: An empirical study of Chinese listed companies," Journal of Cleaner Production, vol. 17, no. 6, pp. 593-600, Apr. 2009.
〔32〕 http://www.alio.go.kr (공공기관 경영정보 공개시스템)
〔33〕 http://www.env-info.kr/member/index.do (환경부 환경정보공개검증시스템)
〔34〕 http://iscs.kisa.or.kr/kor/main.jsp (한국인터넷진흥원 정보보호 안전진단)
〔35〕 http://isms.kisa.or.kr (한국인터넷진흥원 정보보호관리체계)
〔36〕 http://privacy.kisa.or.kr (한국인터넷진흥원 개인정보보호)
〔37〕 http://www.iso27001pdf.org/iso-27001-pdf-download-free/ (ISO 27001)
〔38〕 http://www.krx.co.kr (KRX 한국거래소)
〔39〕 http://www.moleg.go.kr/ (법제처)
〔40〕 http://www.realtyprice.co.kr (국토해양부 부동산공시 메인페이지)
〔41〕 http://www.schoolinfo.go.kr/index.jsp (교육정보알리미)
〔42〕 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm(SEC "Guidance concerning cyber incident disclosure)

〈著者紹介〉

전 효 정 (Hyo-Jung Jun) 학생회원
2001년 2월: 충북대학교 경영정보학과 학사
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
2006년 9월~현재: 충북대학교 경영정보학과 박사과정
〈관심분야〉 정보시스템 정보보안, 보안감사, 정보보호정책

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수, 대학원 정보보호경영전공 주임교수
〈관심분야〉 정보보호 분야의 경영 및 정책 의사결정