情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

정보보호 거버넌스 이슈 및 연구 과제

김정덕*, 홍기향**

요 약

정보보호는 더 이상 기술적 이슈가 아니고 최고경영층의 적극적 역할 수행 및 책임을 요구하는 정보보호 거버넌스 이슈가 최근 대두되고 있다. 본 논문에서는 정보보호 거버넌스의 출현 배경과 필요성에 대해 간단히 기술하고 정보보호 거버넌스의 프레임워크를 제시한다. 그리고 정보보호 거버넌스 구현을 위한 주요 분야를 제시하고 이와 관련한 기존 연구의 한계점을 분석하면서 향후 해결되어야 할 연구과제를 제시한다.

Ⅰ. 정보보호 거버넌스 배경 및 필요성

1.1. 정보보호 패러다임의 변화

정보보호의 발전과정을 남아공의 Solm 교수는 4가지 패러다임의 변화로 구분하여 설명하고 있다[16]. 첫 번째 패러다임은 컴퓨터가 상용화하기 시작한 50년대 후반부터 70년대까지에 해당되는 '정보보호 기술 패러다임'으로서, 주로 메인프레임 접근통제를 중심으로 한 보안기술 발전이 이루어진 시기이며 정보보호를 주로 기술적인 이슈로 보는 것이다.

두 번째 패러다임은 80년대에서 90년대 중반까지에 해당되는 '정보보호 관리 패러다임'으로서, 기술적 솔루션으로는 정보보호 구현에 한계가 있으며 정보보호 조직 구성, 경영층의 참여, 시스템보안담당자 역할 등 정보보호를 관리적 이슈로 인식하게 된 시기였다.

세 번째 패러다임은 90년대 후반부터 2000년대 초반까지에 해당되는 '정보보호 조직화 패러다임'으로서, 효과적인 정보보호 구현을 위해서는 조직 내 특정인(정보보호 담당자)의 활동보다는 전체 조직 구성원의 노력과 참여가 중요함을 인식하여 조직에 정보보호 문화를 정착시키려는 시도가 있었다.

네 번째 패러다임은 200년대 초반 이후부터 시작된 움직임으로서 '정보보호 거버넌스 패러다임'이다. 이는 정보보호 구현에서 핵심성공요인으로 많이 언급되어 왔지만, 구체적 방법이 제시되지 않았던 '최고경영층의 정보보호에 대한 역할과 책임'을 중요시하는 관점이다. 이는 2000년대 이후 이슈화되고 있는 기업 거버넌스(corporate governance)의 일부로서 정보보호 거버넌스를 구현하고자 하는 시도이다. 또한 Sarbane-Oxley Act (SOX)를 위시한 내부통제 및 정보보호에 관한 법령 및 규정이 제정되면서, 이의 준수를 위한 최고경영층의 책임이 강화되었고 이에 따른 이사회나 최고경영층의 정보보호에 대한 관심과 역할을 해결하기 위한 노력이 필요함을 인식하였기 때문이다.

정보보호 거버넌스 패러다임은 '정보보호 조직화 패러다임'의 발전된 모습으로 전사적인 노력도 중요하지만, 그 중에서도 최고경영층의 노력으로 인한 전략적 정보보호 활동의 중요성을 강조하는 것이다. 이는 기존의 정보보호 노력이 주로 정보보호담당자 즉 중간 경영층이나 실제 IT 운영자들을 중심으로 수행되었으나, 전사적인 정보보호 구현을 위해서는 최고경영층과 이사진들의 적극적인 역할과 책임활동으로 인해 과거의 전술적 차원에서 전략적 차원으로의 정보보호 위상을 높여야 함을 인식하였기 때문이다.

1.2. 정보보호 거버넌스의 필요성

전통적으로 비즈니스 정보에 영향을 미치는 위험은 주로 정보기술(IT) 기반구조 관점에서 다루어져 왔다.

* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)
** 한국정보보호진흥원 선임연구원(hongkh@kisa.or.kr))

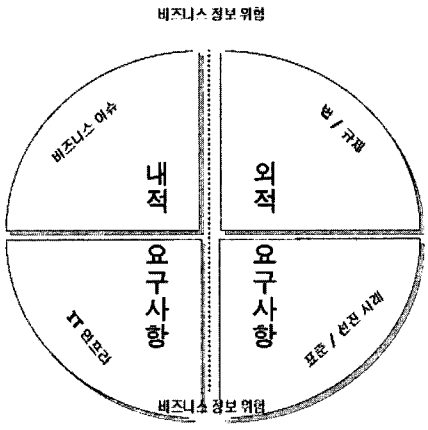
바로 이러한 관점이 IT가 중요한 비즈니스 정보자산의 저장, 처리, 전송에 관해 중요한 역할을 수행하게 된 주요 이유가 되었다. 더우기 정보보호는 단순히 기술적인 이슈로만 인식되어 왔으며[15], 최고경영층과 이사진들의 주의를 끌지는 못했다. 정보보호는 단순히 기술적 이슈가 아니라, 전략적 이슈이면서 심지어는 법적인 문제[12]일 수가 있다. Swindle and Conner[17]는 정보보호는 중역진과 이사진들의 위험관리 노력, 보고체계, 책임을 강조하는 전사적 거버넌스의 일부로서 취급되어야 함을 강조하고 있다. 따라서 정보보호 거버넌스는 중역진들이 어떻게 정보보호를 다루어야 하는가에 대한 프로세스라고 정의내릴 수 있다.

비즈니스 정보의 기밀성, 무결성, 가용성을 보존하기 위한 정보보호 노력을 위해서는 내, 외부의 정보보호 요구사항을 만족해야 한다. 외적 정보보호 요구사항은 크게 1) 정보보호 관련 표준과 최상의 업무처리방식(best practices)의 채택과 2) 관련 법/규정 준수 의무로 구분할 수 있다.

정보보호 국제표준이나 최상 업무처리방식을 채택함으로써 조직과 이해관계자간의 신뢰성 있는 관계를 설정할 수 있으며 범세계적으로 통용되는 정보보호 원칙을 구현함에 따라 다른 조직과의 파트너 쉽을 가능하게 해주고 있다. 한 예로서 ISO 27000 시리즈(정보보호관리체계: ISMS)는 11개 통제 영역과 PDCA 프로세스 제시함으로써 효과적 정보보호 전략 수립을 위한 출발점의 역할을 수행한다.

관련 법/규정 준수에 대한 요구사항은 실제로 조직 내 정보보호 구현의 가장 큰 이유로서 인식되고 있다(CSI/FBI Survey, 2006). 인터넷과 B2B 등 네트워크가 고도화/광역화됨에 따라, 새로운 위협요인이 출현하고 있으며, 이에 대한 대응노력으로서 정부 및 산업계에서는 정보보호에 관한 법규 제정을 통해 조직의 정보보호 노력을 강제화하고 있다. 미국의 Sarbane-Oxley Act (2002)와 FISMA[2], 남아공의 Electronic Communications and Transactions Act(2002), 한국의 정보통신기반보호법(2001), 금융산업의 International Basel II Accord[11] 등은 대표적 입법 사례이다.

내적 정보보호 요구사항은 크게 1) 정보보호 관련 비즈니스 이슈와 2) IT 인프라 이슈로 구분할 수 있다. 조직 내 민감한 정보자산의 기밀성, 무결성, 가용성을 보장하기 위한 내부의 필요성을 반영한다. 이러한 정보보호 요구사항은 조직의 정상적인 비즈니스 운영을 지속



〔그림 1〕 정보보호의 내외적 요구사항

시키기 위한 정보처리 측면에서의 전사적인 원칙, 목표, 요구사항을 보완하고 있다[16].

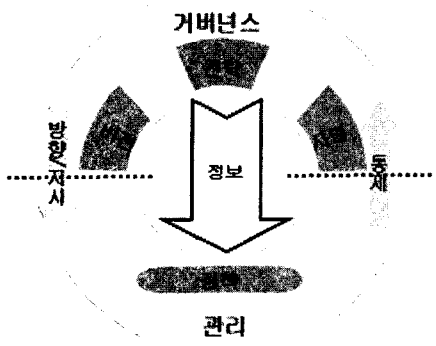
IT 인프라 이슈는 '정보 백본'을 형성하는 핵심 인프라를 보호하기 위한 요구사항으로서 위험분석 및 관리 과정을 통해 다루어지고 있다. 즉, 위험분석 과정을 통해 위협, 취약성, 위험수준을 도출하고, 이를 조직이 감수할 수 있는 수준으로 조정하기 위한 위험 감소, 전가, 예방 등의 위험처리 대안을 위한 적절한 통제를 선택, 구현, 모니터링 하는 위험관리과정을 통해 IT 인프라 관련 위험에 대처해야 한다.

〔그림 1〕은 비즈니스 정보에 영향을 미치는 위험을 경감시키기 위한 내적, 외적 정보보호 요구사항간의 관계를 보여주고 있다. 이러한 다양한 요구사항을 만족시키기 위해서는 정보보호가 비즈니스 경영에서 취급되어야 하며, 거버넌스 이슈로 해결되어야 한다. 궁극적으로는 현재의 정보보호 통제의 구현 및 관리 등 전술적 측면에 치중한 접근방법으로는 한계가 있으며 보다 전략적 측면에서의 정보보호 접근방식으로 변경될 필요가 있다.

Ⅱ. 정보보호 거버넌스 프레임워크와 주요 분야

2.1 정보보호 거버넌스 프레임워크

정보보호가 단순한 기술적 이슈가 아니고 전략적이고 법규적 이슈라는 점은 정보보호의 접근방식의 새로운 차원을 요구하게 되었으며, 조직의 전사적 거버넌스 프로그램에 통합시켜야 하는 필요성을 제기시켰다[14]



〔그림 2〕 정보보호의 내외적 요구사항

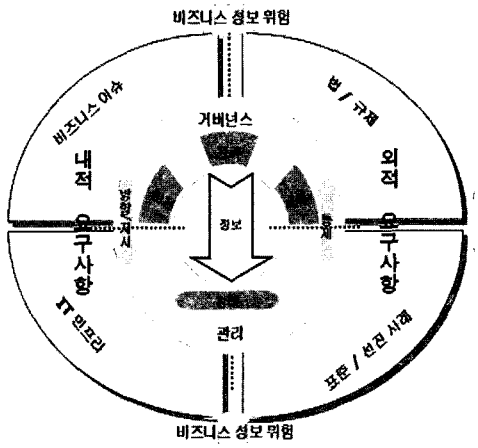
Corporate Governance Task Force (2004)에서는 "정보보호로 가는 길은 기업 거버넌스를 통해 간다."라고 언급하였다. 이는 기업 거버넌스 프로그램에 포함시키기 위해서는 정보보호가 내부통제에 일부로서 포함시켜야 되며 전략적 측면에서의 방향 설정 등이 필요함을 강조하고 있다.

정보보호 거버넌스는 기업 거버넌스 차원에서 비즈니스 정보 위험을 다룰 수 있는 효과적 전략 수립을 위해 두 가지 측면에서 고려해야 한다(〔그림 2〕 참조). 첫째, 이사회나 최고경영층이 정보보호 전략 및 방향을 설정하는 거버넌스 측면이 있고, 둘째, 조직의 정보보호 전략을 어떻게 구현하고 관리할 것인가에 관한 관리적 측면이 있다.

거버넌스 측면은 이사회나 최고경영층의 정보보호에 대한 방향제시와 통제 역할을 강조하는 것이다. 즉 이사회나 최고경영층은 전사적 정보보호 정책 및 계획을 수립함으로써 정보보호에 대한 책임과 의지를 보여주고, 조직의 임무, 목표, 전사적 정보보호 전략 수행을 지원해야 한다[18].

조직의 정보보호 노력을 통제하기 위해서는 이사회는 여러 부서장으로부터 정보보호계획의 효과성에 대해 주기적인 보고가 필요하며 이를 통해 전략 및 정책에 대한 재검토를 통해 미진한 부분을 도출하여 정보보호 수준의 지속적인 개선을 도모할 필요가 있다.

관리적 측면은 정보보호 정책이 어떻게 조직 내에 구현되는 가를 다루는 것으로, 전사적 정보보호 정책에서 제시한 사항을 구현하기 위한 여러 부서장과 관리자의 책임 및 의지를 반영해야 한다. 이를 위해 ISO 27002[13]에서 제시되는 통제를 구현함으로써 정보보호가 조직의 일상적 활동 및 기능의 하나로 통합될 수 있다. 정보보호 대책이 구현되었다면, 비즈니스 정보위험과 선택된 정보보호 통제의 유용성은 모니터링되어 최고경영층에 보고되어야 한다. 이러한 보고를 통해 조직의 정보보호 노력을 보다 정확하게 지시하고 통제할 수 있다.



〔그림 3〕 정보보호 거버넌스 프레임워크

정보보호 거버넌스는 조직의 내적, 외적 정보보호 요구사항을 효과적으로 만족시킬 수 있도록 함으로써 비즈니스 정보위험으로부터 보호할 수 있다. 이러한 정보보호 요구사항은 최고경영층으로 하여금 정보보호를 위해 무엇을 하여야 하는가를 보여주는 일종의 정보위험 명령체계라고 볼 수 있다. 결과적으로 요구사항은 기업 거버넌스를 통한 효과적인 정보보호 전략을 수립하고 구현하는데 방향제시 역할을 수행하고 있다.

이러한 접근방법은 기업 운영의 3가지 주요 요소(인적자원, 프로세스, 기술: PPT)에 대한 역할과 책임을 분명하게 해주는 효과도 있다[17].

〔그림 3〕은 효과적 정보보호 거버넌스 수립을 위한 프레임워크를 보여주고 있는데 주요 요구사항과 이를 만족시키기 위한 패러다임들을 소개하고 있다.

2.2. 정보보호 거버넌스의 주요 분야

정보보호 거버넌스의 주요 분야는 일반적으로 아래와 같은 5가지 영역으로 구분할 수 있다; 전략적 연계, 가치 전달, 위험관리, 자원관리, 성과측정.

- 전략적 연계(Strategic Alignment): 정보보호 노력과 조직의 목표 달성과의 연계를 보장하는 것으로 주로 정보보호 전략과 기타 전략과의 연계, '정보

보호 위원회'의 역할 및 책임에 대한 효과성을 시험하는 것이다.

-정보보호 전략수립과 비즈니스/IT 전략과의 연계
-정보보호 전략수립 기법
-정보보호 위원회/조직의 위상, R&R 정의
-보고체계

• 가치 전달(Value Delivery): 정보보호 투자에 대한 효과성을 증명하는 것으로 비용효과적인 정보보호 체계 구현과 정보보호 예산 및 투자결정 요인에 대한 관심사항을 전달해야 한다.

-표준 및 최상 업무수행(best practices)에 근거한 정보보호체계 구현 및 관리
-정보보호 예산수립 과정 및 IT 예산과의 관계
-조직의 자본계획 및 투자통제 과정과 정보보호와의 통합
-정보보호 투자수익율(ROSI: Return on Security Investment) 산출방법

• 위험관리(Risk Management): 정보보호 거버넌스의 초석이 되는 부분으로서 이를 통해 취약부분을 식별해 내고 정보보호 개선방향을 도출할 수 있다;

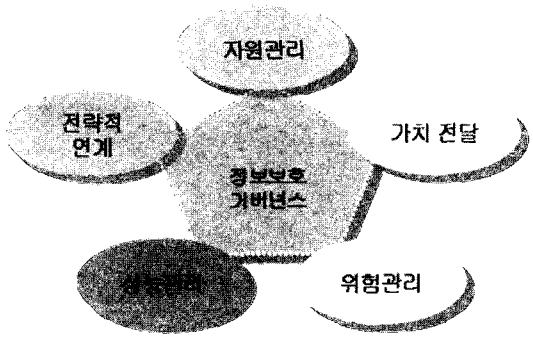
-산업별, 서비스별 위험 프로파일 개발
-위험의 비즈니스상의 영향도 및 손실 규모 산정
-조직에 적합한 위험관리 프로세스
-허용가능한 위험수준 결정 기준 및 방법
-위험분석 절차 및 도구

• 자원관리(Resource Management): 정보보호를 위한 활동 및 자원에 대한 관리로서 주로 전사적 정보보호 아키텍처에 대한 이슈와 정보보호 서비스 제공방식에서 현재 많이 채택하고 있는 정보보호 아웃소싱(outsourcing) 이슈가 주요 관심사항이다.

-ITA/EA와 정보보호 아키텍처와의 연계
-정보보호 아웃소싱 분야 및 통제
-정보보호 아웃소싱 서비스의 모니터링 및 책임

• 성과관리(Performance Management): 정보보호 노력의 성과를 측정하고 개선시키려는 노력으로서 정보보호 투자와 정보보호 수준 평가와의 관련성으로 최근 주요 이슈로 대두되고 있다.

-성과측정 대상, 주체, 방법(What, who, how)



〔그림 4〕 정보보호 거버넌스의 주요 영역

-성과척도 개발
-성과측정 프로세스(개선을 위한 피드백 포함)
-신뢰성있는 보장 (Independent assurance)

Ⅲ. 주요 이슈별 연구 개발 동향 분석

3.1. 전략적 연계

정보보호와 비즈니스/IT와의 전략적 연계에 관한 연구개발 동향은 다른 정보보호 거버넌스 분야에 비해 매우 미진하다고 할 수 있다. 정보보호가 그 자체로서의 존재 이유를 갖는 것이 아니라 조직의 임무달성을 위한 수단(means to an end)으로서의 가치를 가진다는 명제는 이미 보편화되었으나 구체적인 정보보호 전략의 유형 및 수립 방법에 대한 학술적, 실무적 연구 개발노력은 아직 상당히 미흡한 수준에 있다.

정보보호 마스터플랜 작성을 위한 정보보호 전략 수립은 정보보호 컨설팅업체에 의해 수행되었으나, 조직의 비즈니스/IT 전략과의 연계를 충분히 고려하지 못하고 단순히 정보보호 측면만 고려한 상태로 전략이 수립되는 경향이 있다. 즉 조직의 임무와 비즈니스 전략 및 방향을 정확히 파악하고 이를 지원할 수 있는 측면에서 정보보호의 목표와 방향이 설정되어야 하는데, 이런 부분이 간과된 상태에서 컨설팅 사업이 진행되는 것이 일반적이다. 즉. 조직의 대외적 환경분석과 대내 업무분석을 통한 정보보호 요구사항을 도출이 현저히 부족하고, 단순히 정보자산의 위험분석을 통한 정보보호 대책 선택 및 구현을 계획함으로써 정보보호 마스터플랜을 수립하기 때문에 비즈니스와의 연계성이 미흡하다고 할 수 있다.

관련된 연구개발로는 미국의 NIST에서 제시한 정보

보호 영향도(impact level)에 기초한 정보보호 분류작업이다. 즉, 조직의 임무수행 관점에서 정보시스템내의 정보유형이 가지는 기밀성, 무결성, 가용성 측면에서의 영향도를 측정함으로써 비즈니스와 정보보호와의 연계를 도모하는 것이 가장 대표적인 연구개발 결과라고 할 수 있다[4, 5]. 그러나 NIST의 표준 및 지침의 내용은 조직의 업무와 정보보호를 매우 단순한 방법으로 연결하고는 있지만 정보보호의 전략적 측면을 다루고 있다고 보기는 어렵다.

정보보호 전략수립을 위해서는 정보보호가 전략적으로 중요하다는 인식변화를 유도할 수 있는 '인식변화를 위한 프레임워크', 정보보호를 통해 비즈니스 상의 가치를 제고할 수 있는 분야를 식별할 수 있는 '기회포착용 프레임워크' 등에 대한 연구 개발이 필요하다. 또한 '정보화수준 또는 정보보호 성숙도와 연계된 정보보호 전략유형 개발'도 매우 시사성이 높은 연구 과제라고 할 수 있다. 즉, 정보보호 전략유형에 대한 연구와 정보화수준/정보보호 프로그램 성숙도와 연계된 전략유형 제시는 매우 시사점이 높을 것이다. 정보화수준 또는 정보보호수준에 따라 정보보호 접근방법과 대상이 다를 수 밖에 없으므로 이를 반영한 정보보호 전략수립이 필요하기 때문이다.

3.2. 가치 전달

정보보호의 가치 전달 이슈는 최고경영층이나 이사회에서 궁극적으로 관심을 가지는 분야이다. 즉 정보보호 투자를 통해 조직에 어떠한 가치를 제공했느냐를 정보보호 관리자는 물론이고 투자의 주체인 이사회와 중역들의 이해가 첨예한 부분이기 때문이다.

그러나 정보보호의 가치전달에 대한 학술적 연구는 아직 초기 상태라고 할 수 있다. 2002년부터 관심이 일기 시작한 정보보호 경제학 분야는 정보보호를 경제학적 관점에서 접근하려는 시도로서 대표적인 연구 활동은 정보보호 투자수익율(Return on Security Investment: ROSI) 산정 방법이라고 할 수 있다.

즉, 정보보호를 위해 얼마나 많은 돈을 지불해야 하는지에 대한 구체적인 분석의 필요성으로 경제학 방법론이 정보보호에 적용하기 시작하였고, 재무경제학자(Financial economists) 사이에 자본예산과 투자이론을 정보보호투자에 적용시키는 연구 흐름이 있었다. 그러나, 정보보호투자가 성공적일수록 측정할 수 있는 결과는 더 적어질 것이라는 역설 때문에 학문적으로는 결과가 뚜렷하지 않은 주제이기도 하다.

ROSI 연구는 정보보호구매와 제품배치로 인한 수익을 구체적으로 파악할 수 없어 투자수익률은 직접적으로 정보보호에 적용될 수 없으므로, 기대손실(expectation of loss)을 계산에 포함시켜서 산정하고 있다. 즉, 예상되는 손실의 금액은 크지만 주어진 해에 발생할 것 같지 않은 사건의 경우 일정 기간의 손실에 포함시켜 고려해야 한다.

그러나 회계기반의 투자수익률 개념은 경제학 이론의 주요 이론인 "화폐의 시간가치"를 고려하고 있지 않으므로, 순현재가치(Net Present Value: NPV) 개념의 도입이 시도되었다. 그러나 이 방법 역시 정보보호의 가치를 정량화해야 하는 근본적인 문제를 명확히 해결하지는 못하고 있다. 이외에도 정보보호와 관련된 의사결정 시 정보경제학에서 다루는 외부성, 무임승차 등의 문제를 정보보호와 연관하여 분석할 수 있는 분석도구 개발이 필요하다.

현실적으로 미 NIST에서는 SP 800-65[10]를 발표해, 정보보호 예산 및 투자 통제를 IT를 포함한 자본계획 및 투자통제 프로세스에 통합시키는 작업을 시도하고 있다. 정보보호를 독립적으로 간주하지 않고 전체적인 IT 자본계획 및 투자 통제과정에 통합시킴으로써 체계적인 예산수립 및 투자통제를 가능하게 했다는 점에서 국내에서도 참고할 만한 시사점을 가지고 있다. 국내의 예산편성제도가 미국과 상이하므로, 국내 현실을 반영한 정보보호 예산수립[3] 및 투자통제 프로세스 수립이 요구된다.

3.3. 위험관리

정보자산에 대한 위험관리는 정보보호 관리의 핵심과정으로 인식되어 학술적 연구 뿐 아니라 실무에 적용될 수 있는 기법이나 도구 등이 개발되어 온 매우 중요한 이슈이다. 그러나 위험분석이 주로 정성적인 방법을 사용함으로써 적절한 정보보호 대책을 선정하는 데는 큰 문제는 없으나, 조직의 이사진이나 최고경영진의 관심이나 이해를 유도하지는 못하고 있는 실정이다. 즉, 위험의 크기를 금액과 같은 정량적 단위로 측정하지 못하기 때문에 현실감이 부족하고 결과적으로 최고경영층의 무관심을 초래하고 있다.

따라서 정보자산의 위험이 비즈니스에 미치는 영향

도 및 기대손실 규모를 산정하는 방법 개발이 필요하며, 이는 정보보호 사고 피해 산정 방법과 깊은 연관이 있는 문제로서 매우 시의성이 높은 이슈이다. 과거에 정보보호 사고 피해 산정과 관련된 연구가 일부 진행되었으나, 현실적으로 적용하기에는 아직도 보완될 문제가 많다. 즉 일반적으로 하드웨어나 소프트웨어의 대체비용으로 사고 피해 규모를 산정하는 방식을 많이 취하나, 중요한 데이터 손실에 따른 비즈니스의 영향에 대한 피해 규모 산정 방식은 여전히 논리적으로나 실무적으로 취약한 면이 많다고 할 수 있다.

또한 위험관리 분석은 복잡하고 전문성을 요구하는 분야로서 대부분 정보보호컨설팅 전문업체에 의해 수행되고 있으므로, 많은 중소기업에서는 자금이나 인력부족 등의 이유로 위험관리를 수행하지 못하고 있는 실정이다. 따라서 실효성 있으면서 비교적 간단한 위험분석 도구 및 관리 프로세스 개발이 필요하다. 또한 주요 산업별 위협 프로파일 등을 개발하여 산업의 특성 및 환경을 반영한 위협 및 취약성 목록을 게시함으로써 위험관리 작업을 용이하게 수행할 수 있도록 하는 것이 필요하다.

유비쿼터스 환경에 진입함에 따라 위험관리체계 면에서도 새로운 패러다임이 요구되고 있다. 즉, 위험분석 및 관리 활동을 1년에 한번 또는 대규모 정보자산의 변경이 발생할 경우에 수행하는 것이 일반적인 관행인데, 최근 정보자산의 위협요인이 광범위해지고, 사이버 공격(zero-day attack 등)의 개시 및 파급속도도 신속하게 진행됨에 따라 실시간적인 위험관리에 대한 필요성이 높아지고 있다. 이를 위해서는 위험관리 프로세스를 자동화하여 실시간적으로 위협요인을 식별하고 대처할 수 있는 위험관리체계 수립을 통해 일상적인 활동으로서의 위험관리가 요구된다. 2004년부터 일부 금융권에서 기술적, 관리적 정보보호 통제를 포함한 자동화된 위험관리체계 수립을 시도하였으나, 아직 국내에서는 초보적인 단계로서 보완될 부분이 많다.

3.4. 자원관리

정보보호 거버넌스 측면에서의 자원관리라 함은 정보보호 활동에 필요한 자원 즉, 인프라, 설비, 응용시스템, 인적 자원에 대한 구성방식을 포함한 전사적 정보보호 아키텍처(enterprise-wide infosec architecture)개발과 정보보호 서비스 제공방식(in-house or outsourcing)에 대한 전략적 의사결정에 관한 이슈를 의미한다.

전사적 정보보호를 위한 아키텍처는 독자적으로 개발해서는 안되며 범세계적으로 추진되고 있는 전사적 아키텍처(EA/ITA)에 통합되어야 할 필요가 있다. 현재 정보보호 아키텍처에 대한 연구개발 성과로서는 2004년 한국전산원에서 전사적 아키텍처 모형을 적용한 정보보호 아키텍처[1]를 개발하였으나 전사적 아키텍처와 통합된 형태로서의 아키텍처는 제시하지 못했다. 즉 전사적 아키텍처를 개발할 때, 동시에 정보보호가 고려되어야 하기 때문에, EA/ITA와 통합된 정보보호 아키텍처 개발이 요구된다.

정보보호 아키텍처는 정보보호 요구사항을 반영한 인프라, 응용시스템, 데이터 측면에서의 정보보호 기능을 보여주는 세부적인 아키텍처가 개발되어야 하며 또한 정보보호 관리를 위한 관리조직 아키텍처도 포함되어야 한다.

특히 조직 전체의 정보보호에 대한 역할 및 책임(R&R)에 대한 명확한 정의와 함께 정보보호 보고체계, 정보보호 조직의 구성 및 위상, 물리적 정보보호 통제와 기술적 통제기능의 통합 등에 대한 전략적 의사결정은 최고경영층이나 이사진들의 주요 관심 이슈라고 할 수 있다. 이러한 의사결정을 위해서는 여러 대안에 대한 장단점 분석과 상황에 따른 최적 접근방식 등이 제시될 필요가 있다.

정보보호 서비스의 제공방식에 대한 논의로서 최근 정보보호 서비스의 아웃소싱(managed security services) 방식이 범세계적으로 확산되고 있다. 전문적인 정보보호 서비스에 대한 요구와 내부 비용부담을 감소시키기 위한 노력의 일환인 정보보호 아웃소싱의 유형은 단순한 관제 서비스에서 전체적인 위험/보안관리 서비스까지 포함하는 포괄적인 아웃소싱 서비스까지 광범위하다.

문제는 정보보호 아웃소싱에 대한 통제체계가 아직 제대로 구비가 되지 않은 상태에서 아웃소싱 서비스가 진행되고 있다는 점이다. 따라서 정보보호 아웃소싱 서비스의 모니터링 및 책임을 분명하게 할 수 있는 방법에 대한 연구가 필요하다. 즉, 정보보호 서비스수준협정(SLA)과 이를 가능하게 하는 기법에 대한 개발이 요구된다.

3.5. 성과관리

정보보호 성과관리 문제는 2000년 이후 정보보호 투

자 및 노력의 성과를 측정하고 개선시키려는 노력으로서 정보보호 투자와 정보보호 수준 평가와의 관련성으로 최근 주요 이슈로 대두되고 있다. 최고경영자나 이사진 등의 정보보호에 대한 궁극적인 관심은 바로 정보보호 투자에 대한 성과에 있기 때문이다. 이 문제는 다시 크게 두 가지 영역으로 구분할 수 있는데 첫째는 성과관리 프로세스에 관한 제반 이슈와 둘째는 정보보호 수준평가에 관한 제반 이슈를 포함한다.

성과관리 프로세스를 구축하기 위해서는 성과측정 대상(What to measure), 성과측정 주체(Who to measure), 성과측정 방법(How to measure)을 규정해야 한다. 이에 대한 연구 결과로는 NIST에서 개발한 SP 800-55[8], 800-80[9]에서 정보시스템에서의 정보보호 성과측정을 위한 척도(metric)개발과 전사적 정보보호 프로그램 차원에서의 성과측정 척도 개발에 관한 지침을 제시하고 있다. 또한 현재 ISO SC27에서는 정보보호관리의 효과성을 측정하기 위한 표준(ISO 27004)을 개발 중에 있다.

NIST에서는 정보보호 척도유형을 통제구현(implementation metric), 통제의 효과성 및 효율성(effectiveness & efficiency metric), 비즈니스에 대한 영향(impact metric)으로 구분하여 이를 정보보호 프로그램의 성숙도와 연계하여 제시하고 있다. 국내에서는 정보보호 컨설팅 사업의 일환으로 정보보호관리의 KPI(Key Performance Indicators)를 제시하고 있으나, 이 역시 정보보호 통제의 구현 정도를 측정하는 수준에 미치고 있어 경영에 미치는 영향이나 통제의 효과성 또는 효율성을 측정하는 수준은 아니다.

그러나 NIST나 국내에서의 연구결과는 정보보호 관리자 입장에서는 어느 정도 의미를 가질 수 있으나, 최고경영자 또는 기타 주요 이해관계자의 요구사항을 반영할 수 있는 차원에서의 성과 측정이라고는 보기 어렵다. 따라서 BSC(Balanced Score Card)와 같은 IT 또는 경영측면에서의 성과관리 기법을 정보보호에 적용함으로써 보다 다차원적인 측면에서의 성과관리를 가능하게 하는 방법이 요구된다.

또한 정보보호 성과관리의 목적이 지속적 개선이라면 이를 위해 현재 정보보호 수준을 정확히 평가할 수 있는 체계가 마련되어야 한다. 국내에서도 정보보호 수준 평가를 위한 관련 규정과 제도가 시행되고 있으나, 지속적 정보보호 수준의 개선이라는 목표의 달성 정도에 대해서는 의문을 가질 수 있다. 즉 중복성을 가진 평가제도가 존재함으로 인한 피평가대상 조직에서의 부담과 혼란으로 인해 평가의 실효성이 상실될 우려가 있다. 따라서 정보보호 평가제도에 대한 전면적 검토와 더불어 개선책 마련이 요구된다.

Ⅳ. 결 론

본 논문에서는 최근 이슈화되고 있는 정보보호 거버넌스에 대한 등장 배경과 필요성, 관련 연구동향을 분석하였고 향후 정보보호 거버넌스 구현을 위한 연구과제를 5가지 분야로 구분하여 제시하였다.

과거 10년이 정보보호를 위한 기술적 접근방법을 통한 하드웨어적, 전술적 측면에서의 정보보호 구축에 성공하였다고 본다면, 향후 10년은 정보보호 거버넌스를 중심으로 전략적인 위상을 제고하고, 기업 경영활동에 일부로서 정보보호 활동이 포함되어야 할 것이다.

본 논문에서 제시한 여러 연구과제들이 해결될 때, 비로소 정보보호 거버넌스가 모호한 개념이 아닌 구체적 실체로서 구현될 것이다.

참고문헌

[1] 한국전산원, "공공부문 정보보호 아키텍처 구성방안", 2004. 12

[2] 김정덕, "FISMA 준수를 위한 미국의 정보보호 구현 및 평가과정", 2006. 8.

[3] 김정덕, 박현효, 이동권, "자본계획 및 투자 프로세스를 통한 정보보호 예산 수립에 관한 연구", 정보보호학회지, 2004. 5.

[4] NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems", February 2004.

[5] NIST FIPS 200, "Minimum Security Requirements for Federal Information and Information System", February 2006.

[6] NIST SP 800-26, "Security Self-Assessment Guide for IT Systems", November 2001.

[7] NIST SP 800-26 Revision 1, "Guide for Information Security Program Assessments and System Reporting Form", August 2005.

[8] NIST SP 800-55, "Security Metrics Guide for Information Technology Systems", July 2003.

〔9〕 NIST SP 800-80, "Guide for Developing Performance Metrics for Information Security", May 2006.
〔10〕 NIST SP 800-65, "Integrating Security into the Capital Planning and Investment Control Process", January 2005.
〔11〕 Basel Committee, "Basel II: international convergence of capital measurement and capital standards", June 2004.
〔12〕 Birman, "KP, The next-generation internet: unsafe at any speed", *IEEE Computer, 30(8)*, pp. 54-60, 2000.
〔13〕 ISO 17799, "A code of practice for information security", 2005.
〔14〕 Corporate Governance Task Force, "Information security governance: a call to action", April 2004.
〔15〕 Entrust, "Information Security Governance (ISG): an essential of corporate governance", 2004.
〔16〕 Solm B, "Information Security_The Fourth Wave", Computers and Security, Vol. 25, pp.165-168, 2006.
〔17〕 Swindle O, Coner B, "The link between information security and corporate governance", May 2004.
〔18〕 Whitman ME, Mattford HJ, "Principles of information security", Course Technology, pp. 153-90, 2003.

〈著者紹介〉

김 정 덕 (Kim, Jungduk)
정회원
1979년 : 연세대학교 정치외교학과, 학사
1981년 : 연세대학교 경제학과 대학원, 석사
1986년 University of S. Carolina, MBA
1990년 Texas A&M University, Ph.D. in MIS
1991년 - 1993년 : 한국전산원, 선임연구원
1993년 - 1995년 : 원광대학교, 조교수
1995년 - 현재 : 중앙대학교, 교수
관심분야 : 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용 등

홍 기 향 (Hong, Kihyang)
정회원
1992년 : 이화여자대학교 전자계산학과 학사
1997년 : 국민대학교 정보통신석사
2004년 : 국민대학교 정보관리학과 정보관리학박사
2006년 ~ 현재: 한국정보보호진흥원 IT기반보호단 선임연구원
관심분야 : 정보보호 성과 및 평가방법론, IT 감사 및 통제