情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

정보보호 패러다임 변화 및 정보보호 동향에 대한 고찰

최명길*, 김세헌**

요 약

정보보호는 지난 세기에 걸쳐서 많은 발전을 이룩하여 왔다. 정보보호의 패러다임은 메임프레임을 기반으로 하는 제1세대, 정보보호관리를 중심으로 하는 제2세대, 제도화를 중심으로 하는 제3세대를 걸쳐 정보보호 가버넌스를 중심으로 하는 제4세대 이르러고 있다. 본 고는 정보보호의 패러다임의 변화를 살펴봄으로 향후에 전개될 정보보호 발전 양상을 고찰하고, 정보보호 패러다임의 혼재로 나타나고 있는 최근 정보보호 동향을 살펴본다.

Ⅰ. 정보보호 패러다임의 변화

지난 40~50년간의 정보보호의 발전에 대해서 다양한 관점으로 분석할 수 있지만, 본 고는 정보보호발전을 4세대로 구분하고, 각 세대의 특징을 간단히 서술하고, 향후의 정보보호 발전 방향을 제시하고자 한다.

정보보호발전의 제1세대는 80년대 초반까지의 기술적인 접근이 중심이 되는 시기이다. 제2세대는 80년대 초반에서 90년대 중반으로 '관리의 세대'로 특징지을 수 있는 시기로, 정보보호의 중요성을 인식하고 최고 경영자의 정보보호참여, 기술적인 정보보호대책의 조직내 구현 등이 활발하게 일어난 시기이다. 제2세대는 90년대 후반에 종결되었다. 제3세대는 90년대 후반부터 시작되었으며, 이 세대는 제도화(institut-ion)로 특징지을 수 있다. 제3세대의 주요 특징은 모범사례(best practice) 및 지침(code of practice) 개발, 정보보호인증(information security certif-cation)에 대한 국제적인 수요증가, 정보보호문화(information security culture)의 조성, 지속적인 정보보호측정(information security measurement) 등을 특징으로 꼽을 수 있다.

1.1. 제1세 및 제2세대 고찰

제1세대는 메인프레임을 기반으로 접근통제리스트, 사용자 계정과 패스워드 등을 사용한 메인프레임에 보보호대책을 구현하는 방식을 실현한 기술 중심의 접근이 중심이 된 시기이다. 제1세대에서는 정보보호정책, 사용자의 정보보호 경각심 등과 같은 측면은 중요하게 다루어지지 않았다. 그러나 정보보호대책의 구현을 책임지는 기술자들은 정보보호관리는 어느 시기에 있어서 반드시 중요하게 다루어져야 할 것이라고 인식하기 시작했다. 그럼에도 불구하고 정보보호는 전적으로 기술적인 문제로 여겨졌고, 전적으로 기술자에 의해서 이루어졌다.

제2세대에서는 분산 컴퓨팅, 인터넷과 전자상거래 등의 발전으로 정보보호의 문제는 최고 경영진의 중요 의사결정사항으로 간주되기 시작했다. 제2세대에서는 최고 경영진의 정보보호에 대한 관심과 정보보호 프로파일의 배포 등이 급격하게 증가하였고, 정보보호정책, 정보보호관리자, 정보보호에 적합한 조직 구조 등이 중요한 관심사가 되었다.

제2세대에서는 계속적으로 진행되고 있었던 제1세대의 노력과 병행하여 정보보호실무자가 비로소 최고경영진의 주의를 끌게 된다. 이 시기에 있어서 정보보호실무자는 최고경영자의 지원을 받을 수 있었고, 정보보호와 관련하여 조직의 의사결정구조를 구축할 수 있게 된다. 일련의 결과로 인해서 최고정보보호 관리자가 임명되어 정보보호정책 및 절차를 입안하였고, 정보보호와 관련된 사안이 조직의 공식 구조를 통해서 최고경영자에게 보고된다. 정보보호와 관련된 조직의 창설은 정보보호

* 인제대학교 시스템경영공학과 교수 (mgchoi@inje.ac.kr)
** 한국과학기술원 산업공학과 교수(shkim@kaist.ac.kr)

문제를 개선시킬 수 있었다. 그러나 정보보호의 개선을 위해서는 정보보호 조직의 창설 이상의 것이 필요했다. 조직은 자신의 정보보호가 어떠한 상황에 직면하고 있는지, 자신의 정보보호와 다른 조직의 정보보호를 어떻게 비교할 것인지, 정보보호와 관련하여 온라인에서 어떻게 도움을 받을 수 있는지 등을 알기를 원했고, 인적인 측면은 정보보호에 있어서 가장 큰 문제가 되었다. 이러한 고민이 제1세대, 제2세대의 노력과 병행이 된 제3세대의 정보보호의 물결을 만들었다.

Ⅱ. 제3세대의 정보보호-제도화

정보보호의 발전에 있어서 제3세대는 정보보호표준, 정보보호국제인증, 정보보호문화, 조직의 정보보호측정 등의 4가지 요소로 이루어졌다. 정보보호표준 또는 정보보호관리에 있어서 국제적인 모범 사례 등은 현재 조직이 놓치고 있는 정보보호의 문제를 지적해 줄 수 있었음으로 표준 또는 모범 사례가 급격하게 증가하였다. 정보보호와 관련된 국제인증은 정보보호의 개선 방식, 거래 상대자의 정보보호 상태를 알 수 없을 때, 상대방과의 협업의 문제 등을 해결 해 줄 수 있는 방안으로 대두되었다. 조직내의 정보보호문화 배양은 조직내의 사용자가 최대의 위협원이 될 수 있음을 인식하고, 이를 완화할 수 있는 해결책의 일환이었다. 조직내에서 정보보호를 지속적으로 측정하려는 메트릭스는 정보보호정책, 절차가 얼마나 적합한가를 측정하려는 척도이다.

제도화(institutionalization)라고 요약할 수 있는 정보보호 패러다임의 제3세대는 절차적이며, 기술적인 정보보호 인프라스트럭쳐 개발, 정보보호정책, 절차, 방법론, 책무 등을 지원하는 정보보호문화를 창달하였다. 정보보호문화는 정보보호는 조직의 모든 구성원이 매일 수행해야 하는 자연스러운 업무의 한 부분으로 자리잡게 해 주었다. 절차적, 기술적인 조직의 인프라스트럭쳐는 국제 모범 사례(international best practice)에 근거를 두었고, 경영자에게 정보보호관리를 적절하게 취급할 수 있는 제공해 줄 수 있는 광범위한 조직 단위의 정보보호관리시스템에 의해서 지원되었다.

2.1. 정보보호표준과 모범 사례

정보보호관리를 위한 모범 국제 사례 또는 국제지침은 정보보호를 관리하는 방식에 있어서 국제적으로 영향력이 있는 회사의 결합된 경험을 기반으로 생성된다. 국제적으로 영향력이 있는 회사의 경험은 동 회사들의 관련된 통제 방법, 정보보호의 적절한 수준을 유지하기 위해서 그들이 발견한 절차적이고, 기술적인 지침 등을 반영한다. 물론 모든 지침이 정확하고, 모든 지침이 모든 상황에게 적용될 수 없지만, 모범 지침은 정보보호를 위한 일종의 베이스라인을 제공할 수 있다. 모든 경우에서 특정한 위험 분석은 모범 지침을 수용할 의사를 가지고 있는 특정한 조직이 위험을 내포하고 있는지를 진단하기 위해서 반드시 수행되어야 한다. 이러한 기본적인 모범 지침을 따름으로 조직은 대부분의 정보보호와 관련된 문제가 지적될 수 있었다. 모범 지침의 구현과 수행을 통해서 조직은 국제적인 지침을 따른다는 기본적인 정보보증을 획득할 수 있었다.

BS7799로 알려진 ISO/IEC 17799는 영국표준협회에 의해서 만들어졌으며, 정보보호관리에 있어서 대표적인 모범지침이다. ISO/IEC 17799는 정보보호관리를 위한 지침을 제공하고 있다. BS7799는 part1, part2로 구성되어 있으며, part1은 100개 이상의 정보보호통제 항목을 구성하고 있으며, part2는 인증절차를 서술하고 있다.

2.2. 정보보호 국제인증

BS7799가 국제적으로 정보보호인증으로 활발하게 사용되고 있으며, 국내에서는 ISMS가 정보보호관리를 위한 정보보호인증으로 활발하게 사용되고 있다. 조직이 BS7799 정보보호인증을 통과한다면, 위험 분석에 의해서 식별된 BS7799가 서술한 통제항목을 만족한다는 의미이다. 따라서 동 조직은 BS7799 인증을 획득할 수 있다. BS799와 관련된 인증서를 받았다는 의미는 비즈니스 파트너에게 다음을 의미한다. "우리 조직의 정보보호는 평가를 받았고, 우리 조직은 BS7799의 베이스라인을 만족시킴을 증명한다. 따라서 당신이 우리 IT 시스템에 접속하기 위해서는 당신은 적어도 BS7799의 인증서를 받음으로 당신의 안전성을 반드시 입증할 것을 요구한다".

2.3. 정보보호문화의 육성

많은 조직은 자신의 구성원이 많은 경우에 있어서 IT 시스템을 위협하는 가장 큰 위협원이 될 수 있다는 사

실을 인식하고, 많은 조직은 광범위한 정보보호 교육을 시작하였다. 정보보호에 있어서 인적(人的) 측면은 아무리 좋은 기술적인 대책과 절차적인 대책에 의해서 완전히 해결될 수 없다. 정보보호문화는 반드시 조직내에서 창조될 수밖에 없고, 모든 구성원이 정보보호를 자연스럽게 자신의 업무 수행의 일부분으로 여길 수 있도게 해야 한다. 이를 위해서 정보보호교육은 지속적으로 조직의 정보보호계획에 내포되었으며, 조직은 끈임 없이 정보보호를 일상의 한 부분으로 정착시켜야만 하는 압박에 시달리고 있다. 왜냐하면, 적절한 정보보호 문화가 정착되지 않으면, 조직은 광대한 위험에 노출될 수밖에 없다는 사실을 인식하고 있기 때문이다.

2.4. 조직의 정보보호 측정

전통적으로 많은 조직은 내부 또는 외부의 정보보호 감사팀이 특정한 일이 발생할 때 비로소 자신의 조직의 정보보호를 측정한다. 정보보호감사 주기의 장기화나 비정기적인 정보보호감사는 위험이 너무 높기 때문에 더 이상 수용되지 않는 실정이다. 만약 6개월전에 이직한 사람이 여전히 조직의 IT 시스템에 접근할 수 있다면 정보보호감사는 이러한 위험을 줄일 수 있게 기간이 단축되어야만 한다. 정보보호관리 모델은 네트워크 관리 모델 형태로 발전되고 있다. 네트워크 관리 모델은 분단위로 정보보호의 상황을 관리할 수 있다. 이러한 네트워크 관리 모델을 채용하여 정보보호를 관리할 수 있는 방법론으로 Dynamic Information Security Management through Measurement(DISSM) 등이 제시되었다.

Ⅲ. 제4세대의 정보보호-가버넌스

제4세대의 정보보호는 정보보호 가버넌스(information security governance)의 발전이 핵심이다. 제4세대의 정보보호 패러다임을 움직이는 원동력은 기업 가버넌스(corporate governaance) 및 관련된 법·규제 등이다.

3.1. 기업 가버넌스와 정보보호

기업 가버넌스와 관련된 여러 문서가 지난 5년 동안 발간되었고, 기업 가버넌스의 중요성이 국제적인 수준에서 확산되었다. OECD 기업 가버넌스 원칙(OECD Principles of Corporate Geovernance,2004), 기업 가버넌스와 관련된 King 2 보고서(King 2 Report on Corporate Governance,2002) 등은 기업 가버넌스와 관련된 중요한 문서이다. 위 문서는 정보보호를 직접적으로 언급하고 있지 않지만, 보고 시스템, 통제 시스템, 관련된 표준의 준수, 위험 관리, 관련된 정보의 정확하고, 시기적절한 제공, 내부 통제 등의 측면을 언급하고 있다. 대부분의 조직은 정보의 획득, 저장, 처리, 분배를 위해서 IT 시스템에 의존하고 있다. 정보보호는 조직의 IT 자산의 기밀성, 무결성, 유용성 등에 영향을 미치는 위험을 완화하는 수단임으로 정보보호는 기업 가버넌스의 문서에서 요구하는 사항과 매우 관련이 높다. 기업 가버넌스와 관련된 다양한 법과 규제에 대한 개발은 기업 가버넌스의 책임자로서 최고경영층의 역할과 책임을 가중시켰다. Sarbanes-Oxley법(Sarbanes-Oxlley,2002)은 최고경영층의 책임을 단적으로 보여주고 있는데, 동법은 CEO, CFO는 회사의 적절한 내적인 통제장치를 갖출 것을 의무화하며, 정보시스템이 안전한 유지를 통해서 내적인 통제장치의 작동을 강제화하고 있다. 따라서 위의 문서 등의 서술과 같이 기업 가버넌스와 정보보호는 매우 밀접한 관련성을 가지고 있다.

3.2. 기업 가버넌스와 정보보호의 관련성

최근 발간된 문서는 가버넌스와 정보보호의 관련성을 명확하게 표현하고 있다. 미국의 사이버시큐리티 준비반(national cyber security summit task force)가 발간한 국가정보보호정보보호가버넌스(information security governance-a call to action) 문서는 '정책과 내부 통제로 구성된 기업 가버넌스는 관리되어야 하며, 정보보호 가버넌스는 조직의 가버넌스 프로그램의 하위 집합이다'라고 정의하고 있다. IT 가버넌스가 발간한 정보보호가버넌스(information security governance)는 정보보호의 역할은 위험 관리 또는 위험완화 관리라고 정의하고 있다. 정보보호 가버넌스에 대한 인식의 확산은 조직전반에 영향을 미치고 있으며, 정보보호 가버넌스계획에 의해 완화될 위험은 조직의 수행하는 모든 임무에 존재하는 위험을 의미한다.

물론 오랜 기간 동안 정보보호의 중요성이 강조되었지만, 정보보호의 중요성에 대해서 충분한 영향력을 획득하는데 실패하였다. 폭넓은 기업 가버넌스의 중요성에 대한 인식은 이제까지 강조된 정보보호의 중요성을

한층 강화할 전망이다. 다음 절에서 정보보호와 정보보호의 가버넌스에 대해서 살펴보자.

3.3. 정보보호와 정보보호 가버넌스와의 관련성

지난 3~4년에 걸친 기업 가버넌스 분야의 발전은 정보보호의 중요성을 한층 더 발전시켰다. 최근에는 정보보호 가버넌스 개념의 성숙과 발전이 이루어지고 있다.

정보보호 가버넌스는 정보보호 관리 이상이라는 것이 명확해지고 있다. 정보보호 가버넌스는 회사내에서 정보보호의 문제를 다루는 방식에 있어서 최고 경영자와 이사회가 중요한 역할을 수행해야 한다고 명확하게 지적하고 있다. 다음의 정의는 기업 가버넌스에 있어서 필수적인 부분으로 내포될 수 있는 정보보호 가버넌스에 대한 폭넓은 의미를 반영한다. '정보보호 가버넌스는 기업 가버넌스의 핵심적인 부분이며, 다음의 사항을 구성한다.

- 안전한 정보보호에 대한 이사회와 최고 경영자의 헌신된 관리 및 지도력
- 안전한 정보보호를 실현하기 위해 필요한 적절한 조직의 구조
- 안전한 정보보호를 위한 강화된 사용자 교육 및 헌신
- 필요한 정책, 절차, 프로세스 기술 및 정보보호 집행 메커니즘

위에 서술된 모든 요소는 언제나 회사의 전자적 자산의 기밀성, 무결성, 유용성을 보증할 수 있도록 유지되어야 한다.

따라서, 정보보호 가버넌스는 대표이사에서부터 데이터 입력 요원, 심지어 제품을 고객에게 인도하는 운전기사까지를 망라한 회사 내의 모든 구성원을 포함한다. 정보보호 가버넌스는 회사의 IT 위험을 완화시키기 위해서 사용되는 모든 수단으로서 간주될 수 있다. 정보보호 가버넌스의 핵심적인 특징 중 하나는 정보보호 가버넌스는 순환 구조로 이루어진다. 순환 구조는 최고경영자의 정보보호에 대한 헌신에서 시작된다. 최고경영자는 회사의 생존을 위하여 정보보호를 핵심 전략으로 다루어야 하며, 회사의 IT 위험을 완화하는 데 책임을 져야 한다. 이를 위해서 최고 경영자는 정보보호정책을 수립하고, 이사회의 추인을 받아야 한다 정보보호정책은 정보보호에 적합한 조직 구조에 의해서 실행되어야 하며, 모든 조직 수준에 적합한 권한과 책임을 가져야 한다. 이 권한과 책무는 IT 시스템 사용자를 위한 적절한 교육에 의해서 강화될 수 있다. 정보보호를 위해 필요한 기술은 식별 및 관리되고, 정보보호정책에 부합하는지를 측정할 수 있도록 제도화되어야 한다. IT 위험 관리의 상태를 최고경영자에게 알리기 위해서 정보보호정책의 준수 여부에 대한 감사가 실시되어야 한다. 최고경영자에 대한 감사 결과의 보고로 순환구조는 종결된다. 따라서 정보보호 가버넌스는 잘 알려진 기획(plan)-실행(control)-측정(measure)-보고(report) 등의 순환 구조를 가진다. 다음 절에서 제4세대의 변화를 가지고 온 동인을 살펴본다.

3.4. 제4대 변화의 동인

제4세대로 정보보호의 패러다임을 가져온 동인(動因)은 바람직한 기업 가버넌스와 이 분야에서의 법과 규제의 발전 등이다. 바람직한 기업 가버넌스와 지원하는 법과 제도적 발전에 대한 강조를 가져온 동인은 IT 시스템에 저장된 조직의 전자적 데이터를 이용한 기업 부정과 재정 자원의 남용을 막고자하는 시도에서 출발하였다. 따라서 회사 데이터의 조작을 통한 기업 부정에 대한 방지는 정보보호 패러다임을 가져온 핵심 동인이다. 이러한 동기에서부터 관련된 규제와 법이 개발되었고, 바람직한 기업 가버넌스에 대한 압력이 가중되었다. 지난 수년 동안 회사의 전략적 운영 목적으로 IT 통합이 이루어졌고, IT 서비스는 회사와 회사가 제공하는 서비스에 깊이 연관되어 있어서 회사의 IT 시스템을 이용한 부정을 행할 수 있는 가능성이 높아졌다. 결과적으로 심각한 위험이 발생할 수 있다. 이러한 위험 중 가장 심각한 위험은 사회 공학(social engineering)과 사회적 공학과 정보보호와의 관련성이다.

최고 경영층은 기술적인 보안 대책에 많은 재정 자원을 투자하였음에도 불구하고, 관련된 종업원, 의뢰인, 고객 등에 의한 인적 자원은 IT 시스템 사용과 관련한 심각한 위험을 일으킬 수 있다는 사실을 인지하였다. 최고 경영층은 정보보호문제는 기술적인 대책에 의해서만 해결될 수 없다는 사실과 모든 사용자가 잠재적인 위험과 IT 시스템을 공격하는 사회 공학의 영향을 인식할 수 있도록 경영층 차원에서 의사결정이 이루어져야 한다는 사실을 명확하게 인식하게 되었다. 부정 행위를 하는 수단으로 사회 공학을 사용하는 시도가 점차 증가하

는 것으로 나타나고 있다. 바람직한 정보보호 가버넌스는 이러한 위험을 지적하는 것이 필수적이다.

3.5. 제4대 변화의 결과

제4세 정보보호의 패러다임인 정보보호 가버넌스의 동인은 앞에서 서술했듯이 바람직한 기업 가버넌스와 조직, 규율의 발전 등이다. 이러한 이유로 인해서 제4대 정보보호 패러다임은 지속적으로 유지될 것이며, 최고경영자는 정보보호에 대한 관심을 지속적으로 가질 것이다. 일반적으로 정보보호에 대한 관심이 더욱 강화될 것이다. 감사 위원회는 정보보호에 대한 더욱 민감하게 될 수 있으며, 이사회의 특정 구성원이 정보보호를 책임지는 역할을 맡을 것으로 보인다. 그러나 제4세대 정보보호인 정보보호 가버넌스는 기술적인 이슈로만 해결될 수 없음을 주지해야 한다. 위험에 대한 보고 및 감사가 정보보호 가버넌스의 핵심임으로 제4세대 정보보호는 공식적인 보고 도구와 메커니즘을 필요로 한다.

Ⅳ. 정보보호 패러다임의 동시성과 최근 동향

4.1. 정보보호 패러다임의 동시성

현재 정보보호는 제1세대, 제2세대, 제3세대 등의 패러다임과 제4세대 패러다임이 혼재하고 있다. 제4세대 패러다임은 지난 과거의 패러다임 및 바람직한 기업 가버넌스의 강조에 대한 결과로 나타나고 있다. 정보보호의 제4세대 패러다임은 바람직한 기업 가버넌스의 핵심적인 부분으로 정보보호를 명확히 포함하는 프로세스이며, 정보보호 가버넌스 개념을 성숙화하는 프로세스이다. 따라서 정보보호 가버넌스는 IT 시스템의 보안성을 강화를 위해 반드시 사용되어야 한다.

4.2. 정보보호의 최근 동향

현재 정보보호는 위에서 언급한 것과 같이 제1세대에서 제4세대까지 혼재하여 나타나고 있다. 따라서 현재의 정보보호의 최근 동향에 대한 이해는 정보보호 패러다임의 변화방향에 대한 이해를 도울 수 있다. 다음은 정보보호 분야의 최근 동향을 소개한다.

- 이익을 목표로 한 컴퓨터 범죄의 증가:컴퓨터 범죄는 컴퓨터의 역사와 함께 오래 되었지만, 컴퓨터 범죄 형태는 지속적으로 변화하고 있다. 최근 개인정보에 대한 무차별적인 접근과 재정정보에 대한 무차별적인 피싱은 급격하게 증가하고 있다.
- 인프라스트럭쳐를 목표로 하는 공격 증가: 국가의 컴퓨팅 인프라스트럭쳐를 목표로 하는 공격과 관련된 정보는 알려져 있지 않고 있다. 그럼에도 불구하고 이러한 종류의 공격은 실제적으로 존재하고, 점차 증가하고 있다.
- 표준 및 보증 고려사항의 증가: E.U.국가와 미국에서 표준에 대한 준수의 필요성이 점차 강조되고 있다. 특히 Sarbanes-Oxley(SOX)와 Health Insurance Portability and Accountability (HIPAA)법은 상업 회사인 비자카드, 마스터카드 회사가 Payment Card Industry(PCI) 데이터 보안 표준을 채택하는 데 큰 영향을 끼쳤다.
- 강화된 2가지 종류의 정보보호 방법: 얼마전 가트너 그룹은 정보보호 방법이 위험 관리와 네트워크 보안 기술 기능으로 나누어질 것이며, 후자는 아웃소싱이 될 것으로 예상했다. 정보보호의 기술적인 측면과 비기술적인 측면간의 차이 거의 극복할 수 없을 정도로 되어 결과적으로 정보보호 방법은 2가지의 흐름을 나타내고 있다.
- 적절하게 보호되지 못하는 모바일 기술: 모바일 기술은 수많은 핸드폰과 다른 디바이스들을 포함하고 있지만, 적절한 보안 대책이 수립되고 있지 못하다. 무선 기술은 널리 확산되고 있지만, 불행히도 확산에 버금가는 정보보호 대책이 채용되지 못하고 있다. 향후에 개인과 조직이 정보보호 관련 위험을 인식하기 전에 안전하지 못한 모바일 기술로 인해서 막대한 비용을 치를 것으로 예상된다.
- 보안 관련 기술의 발전: 특정한 보안 관련 기술이 급속히 증가하고 있다. 특히 인증, 인증 관련 기술, 바이러스 방지 도구, 침입방지기술, 가상네트워크 기술, 보안사건관리기술(security event management), 웹 컨텐츠 필터링 기술과 비교할 때 급격히 발전하는 것으로 보인다.

Ⅴ. 결 론

실제 정보보호 실무 및 연구에서는 제1세대의 패러다임에서 제4세대의 패러다임이 혼재하여 나타나고 있는 것이 주지의 사실이다. 점차 정보보호의 향후 변화의

방향은 제4세대의 정보보호 가버넌스를 향해 가고 있으며, 개념의 면밀한 정립이 필요하다. 그러나 면밀한 개념의 정립 뿐만 아니라 정보보호 가버넌스 개념을 바탕으로 이를 구현할 수 있는 방안 및 대책에 대한 연구가 절실하다. 따라서 향후의 정보보호 연구 및 실무진들은 연구 및 실무 영역에서 정보보호 가버넌스의 구현을 어떻게 할 것인지에 대해서 고찰하고, 변화를 주도할 필요가 있다.

참고문헌

[1] E.Eugene Schultz, Predicting the future of InforSec, Computers and Security, Vol.25, pp. 553-554, 2006.

[2] E.Eugene Schultz, the Changing Winds of Information Security, Computers and Security, Vol.25, pp.315-316, 2006.

[3] OECD Principles of Corporate Governance, http://www.oecd.org/dataoecd/32/18/31557724.pdf

[4] King 2 Report on Corporate Governance, http://www.iodsa.co.za/corportate.htm;2202

[5] Sarbanes-Oxley,http://news.findlaw.com/hdocs/docs/gwbush/sarbanessoxley072302.pdf, 2002

[6] Information Security Governance-a call to action, National Cyber Security Summit Task Force, http://www.cyberpartnership.crg/InfoSecGov_04.pdf;2003

[7] Security Log, ComputerWorld, ttp://www.computerworld.com/securitytopics/security/story/0,10801,107706,00.html?source=NLT_SEC&nid=107706;2006

[8] von Solms B., Information Security Governance, Computers and Security Vol.24, pp.443-337, 2005.

[9] von Solms B., Information Security-the Third Wave, Computers and Security Vol.19, pp.615-620, 2000.

〈著者紹介〉

최 명 길 (Choi, Myeonggil)
종신회원
1993년 : 부산대학교 경영학과, 학사
1995년 : 부산대학교 경영정보학, 석사
2004년 : 한국과학기술원 공학 박사
1995년 - 2000년 : 국방과학연구소 연구원
2000년 - 2005년 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
2005년 - 현재 : 인제대학교 교수
관심분야 : 홈 네트워크 정보보호, 정보보호시스템 보안평가, 네트워크 정보보호, 정보보호관리 및 정책

김 세 헌 (Kim, Sehun)
종신회원
1972년 : 서울대학교 물리학과 학사
1977년 : 스탠포드 대학교 물리학과 석사
1981년 : 스탠포드 대학교 OR 박사
1982년~현재 한국과학기술원 교수
2003년 : 한국정보보호학회 회장
현 재 : 정보보호전략포룸 의장, 정보보호관리 및 정책연구회 회장
한국경영과학회 차기 회장
관심분야 : 침입탐지 및 조기경보, 정보보호관리 및 정책