

공공기관 정보보안수준 향상을 위한 분임담당자 중심 업무분장 개선에 관한 연구

김상균 · 김인석*

Job Assignment basis on Assistant-staff for The Information security improvement of Public Institution

Sang-Kyoon Kim · In-Seok Kim*

Graduate School for Information Security, Korea University, Seoul 02841, Korea

요 약

지난 2011년부터 2015년까지 공공기관 대상 해킹시도가 총 11만 5천 건에 달하는 것으로 밝혀졌다. 이에 국정원은 지난 2012년에는 준정부기관을 대상에 포함시키는 등 현재는 최대 800여개의 국가·공공기관을 광범위하게 평가하면서 미흡한 점을 보완하도록 지시하고 있다. 하지만 여전히 한수원 해킹과 같은 정보보안 침해사고가 일어나고 있다. 한수원은 전체 인력 2만여 명 중 전산 및 보안 인력이 53명에 불과했음에도 불구하고 2013년, 2014년 내부인원 관련 거의 완벽에 가까운 점수를 받았다. 이를 통해 우수한 평가를 받는 것과 정보보안사고 발생 시 조직적으로 대응하는 것은 별개라는 것을 확인할 수 있다. 본 논문에서는 정보보안 인력 확충이라는 공감대적인 문제에서 벗어나 공공기관의 전사적인 보안수준 향상이라는 과제를 현실화하기 위한 방편으로서 주로 비 전담 분임 인력을 효과적으로 운영할 수 있는 업무분장 개선안을 제시하고자 한다.

ABSTRACT

It was found to have hacking attempts totaling 115,000 to target the public sector since 2011 to 2015. National Intelligence Service was conducting survey information security management states of a wide range of national-public institutions up to 800 including government agencies in the 2012, while instructing to complement shortcomings. However, there is still going to occur invasions, such as Korea Hydro & Nuclear Power hacking. Even though KHNP's security personnel was only 53 people, in the total 20,000 workforces, got the almost perfect score in the 2013 and 2014 related to information security personnel. Through them, we can confirm that between the organizational response to information security incidents and something theoretical is very far. In this paper, we suggest solutions not using the professional staff management but the non-professional staff management to upgrade the level of public agencies information security.

키워드 : 공공기관, 분임정보보안담당자, 업무분장

Key word : Public Institution, Assistant of Information Security Branch Officer, Job Assignment

Received 22 September 2016, Revised 22 September 2016, Accepted 28 September 2016

* Corresponding Author In-Seok Kim(E-mail:iskim11@korea.ac.kr, Tel:+82-2-3290-4251)

Graduate School for Information Security, Korea University, Seoul 02841, Korea

Open Access <http://dx.doi.org/10.6109/jkice.2016.20.11.2007>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

공공기관은 그동안 법적·제도적 뒷받침을 활용하여 보안성 향상을 위한 보안전담인력의 확충, 보안전담담당관제의 도입 및 전산보안시스템에 대한 투자 등 거시적인 노력을 적지 않게 기울여 왔다. 반면 주어진 조직 환경에서 효율적인 인력운용 방안에 관한 구체적인 대책을 마련하는 데는 소홀해 왔던 것이 사실이다. 현재 공공기관은 정보보호업무와 보안업무를 구분하여 각각 인력을 운용하고 있다. 구체적으로 살펴보면 정보보호 최고책임자와 보안최고책임자는 공존하면서 각자를 보좌하는 전임담당자와 분임책임자를 임명할 수 있는데 이들로 하여금 정보보호업무와 보안업무를 이행하도록 지시하고 있다.

그런데 전산기술의 집약화 고도화 등으로 인해 전쟁 발발과 같은 전통적 의미의 보안사건을 중시하는 보안 최고책임자가 전산보안 부문을 이해하기 어렵게 되었고 양자 간 소통의 길은 괴리되고 있다. 이에 따라 유사한 정보보호 및 보안업무를 중복적으로 수행해야 하는 최종실무자인 분임담당자의 부담이 가중되고 있는 실정이다. 정보보호와 보안의 구분이 점점 모호해지고 현실에서 전산보안에 관해 전문성이 부족한 보안최고책임자가 정보보호최고책임자보다 상급자로서 보안업무와 전산 보안에 대해 포괄적인 권한을 갖고 있는 것도 문제지만 으레 각 부서의 최하급직원이 분임정보보호담당자가 되는 관행이 사라지지 않는 것도 문제이다. 이러한 실태는 수직적인 조직문화에서 조직구성원을 다소 불편하게 하는 정보보안활동을 분임정보·보안담당자가 적극적으로 전개하지 못하게 하는 원인이 되고 있다.

본 논문에서는 선행연구결과[1]를 수용하여 전사적인 보안수준과 정보보호담당자의 역할이 밀접하다고 가정한다. 이에 주목하여 정보보호담당자 중 상당수를 차지하는 분임정보보호담당자를 적극 활용하기 위한 업무분장 개선안을 찾는데 주력하고자 한다. 책임소재를 중시하는 공공기관 조직문화에서 업무분장의 수정 없이 그동안 강조되어 왔던 비전문 정보보호담당자의 전문성 개선을 위한 각종 노력은 결실을 맺기 어렵기 때문이다. 제2장에서는 공공기관의 현행 정보보호조직 체계 및 보안관리체계를 개관하고 정보보호책임자와 보안책임자의 임무, 분임 정보보호책임자와 보안책임자의 임무, 분임정보보호담당자와 분임보안실무자의

임무 등을 비교한다.

제3장에서는 분임정보보호담당자와 분임보안실무자의 업무분장을 구현한다. 제4장에서는 구현한 업무분장의 효과를 분석하기 위해 보안사고 발생을 가정한 의사결정과정 시뮬레이션을 실시하고 장점과 한계점을 평가한다. 제5장에서는 향후 연구 과제를 간단히 살펴 보고자 한다.

II. 정보보호관리체계와 보안관리체계

공공기관의 정보보호최고책임자는 사장이 정하고 있으며 보안최고책임자는 소속 정부부처에서 직접 임명하고 있는데 보안관리체계와 정보보호관리체계는 각각 그림 1, 그림 2와 같다.

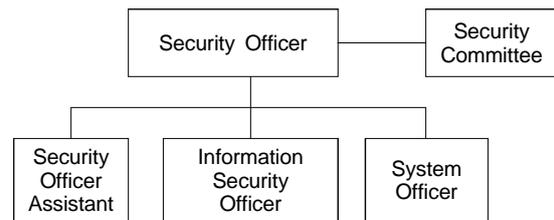


Fig. 1 Security Management System

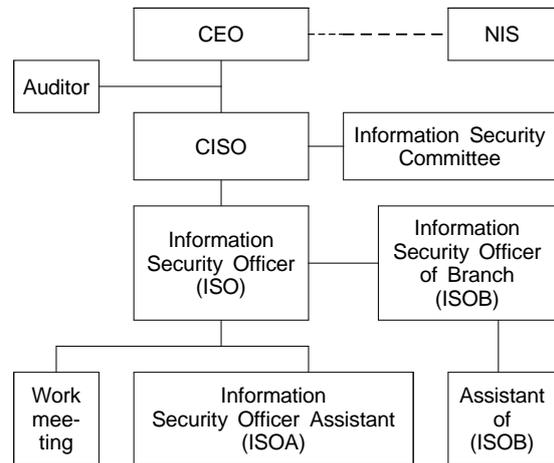


Fig. 2 Informaton Security Management System

현재는 정보보호관리체계가 전쟁발발 등 국가 비상 사태에 대비하는 전통적 의미의 보안을 강조하는 보안

관리체계보다 치밀하게 구성되어 있다는 것을 쉽게 확인할 수 있다. 아쉬운 사실은 전산보안에 관한 실무지식이 부족한 보안최고책임자가 전산보안에 관한 대책 등 전산보안업무를 총괄하고 있는 정보보호책임자보다 상급자로서 보안부문에 관한 포괄적인 권한을 갖고 있다는 점인데 이러한 현실은 전산보안 관련 비상사태 발생 시 정보보호책임자가 신속하게 능동적인 대처를 할 수 없게 만드는 원인이 되고 있다. 또한 정보보호업무 수행 시 전사적인 소통이 중요하다는 점을 고려하면 각각 정보보호책임자와 분임정보보호책임자를 보좌하는 정보보호담당자와 분임정보보호담당자 등 실무자간 연결고리가 없다는 점도 개선해야 할 사항이라고 볼 수 있다. 마지막으로 전사적인 유기성이 매우 중요한 정보보호 업무의 특성을 간과하고 정보보호 조직체계를 기타 조직체계와 유사하게 단순히 위성(衛星)식으로 운용하고 있는 점도 아쉽게 보인다. 결과적으로 현행 조직체계에서는 비 전담인력인 각 부서의 분임담당자에게 보안사고 발생 전후 적절한 대처 능력을 기대하기가 어렵다고 볼 수 있다[2].

2.1. 정보보호책임자와 보안책임자의 임무

정보보호책임자는 「정보통신기반보호법」, 「전자금융거래법」에 따라 전산업무를 추진함에 있어 다양한 정보보호사고를 예방하고, 정보보호업무에 대한 기준과 방향을 정함은 물론 「개인정보보호법」에 따라 개인정보 보호 업무에 관하여 필요한 사항을 지시하고 있다. 정보보호 업무와 개인정보보호 업무를 동시에 수행하고 있는 셈인데 수많은 개인정보를 보유하고 있는 공공기관의 성격을 고려하면 당연하다고 볼 수 있다. 정보보호책임자의 또 다른 중요한 책무는 사장이 정한 정보보호최고책임자를 보좌하는 것이다. 정보보호최고책임자는 정보보호와 관련한 주요사항을 사장에게 보고하는 것 외에 특별한 임무가 없다. 정보보호와 관련한 다음과 같은 대부분의 업무를 정보보호책임자가 직접 지시하고 있는 것이다.

1. 정보보호 기본계획의 수립·시행
2. 정보보호 관련 내규의 제·개정
3. 정보보호업무의 지도·감독
4. 정보보호 관리실태의 평가
5. 사이버 위협정보 수집·분석 및 보안관계
6. 정보보호를 위한 예산 및 인력 확보

7. 정보보호 사고의 조사 및 처리
8. 주요 정보시스템 보호활동
9. 통신망 보안대책의 수립·시행
10. 정보보호 정책 검토, 절차 수립
11. 취약점 분석평가 수행 및 결과에 따른 대응방안 검토
12. 임직원에 대한 정보보호 교육 및 홍보
13. 그 밖에 정보보호와 관련된 사항

한편 보안책임자는 보안담당관으로서 각 기관의 보안업무 전반을 총괄하면서 각 부서의 부서장이 맡고 있는 분임보안책임자의 직무를 감독하고 구체적으로 다음과 같은 임무를 맡고 있다[3].

1. 자체 보안업무 수행에 관한 계획, 조정 및 감독
2. 보안교육(통신보안교육 포함)
3. 비밀(대외비 포함)소유현황 조사
4. 통신보안에 관한 업무
5. 자체 보안심사분석 및 감사
6. 보안사고의 조사 보고
7. 그 밖에 보안업무에 관하여 필요한 사항

다음으로 정보보호책임자의 아래와 같은 전산보안 업무를 직접 관리·감독하고 있다.

1. 전산보안대책의 수립
2. 시스템운영실, 전산망 및 전산자료 등의 보안관리
3. 전산보안업무 지도, 감독 및 교육
4. 그 밖에 전산보안업무에 관하여 필요한 사항

이 밖에도 전산보안시스템을 관리·운영하는 전산부를 직접 통제하는 등 상당히 포괄적인 권한을 갖고 있다.

2.2. 분임 정보보호책임자와 보안책임자의 임무

부서장은 분임정보보호책임자와 분임개인정보보호책임자의 역할을 동시에 수행하면서 분임보안책임자의 책무까지 병행하고 있다. 각 부서의 정보보호업무 및 보안실무는 부서장이 지명하는 분임정보보호담당자와 분임보안실무자가 모두 수행하는데 분임담당자의 임무는 다음으로 미루고 우선 분임책임자의 임무를 간략히 살펴보면 다음과 같다.

1. 관리계획 상 개인정보 안전성 확보조치에 관한 사항
2. 소관업무 개인정보에 대한 세부 처리방침의 결정

3. 보유기간이 경과한 소관업무 개인정보의 파기
4. 소속직원 등에 대한 개인정보 보호 교육·관리·감독
5. 그 밖에 법령 및 내규에 의하거나 정보보호책임자가 요구하는 개인정보 보호에 관한 사항

주목해야 할 점은 조직·관리체계 상 보안최고책임자 및 정보보호책임자의 관련 업무 지시를 직접 받는 분임책임자의 역할을 모두 부서장이 수행한다는 사실이다. 보안최고책임자와 정보보호책임자는 상이한 데 이를 보좌하는 분임책임자는 동일하다는 이와 같은 현실은 공공기관의 업무분장이 대체로 ‘보여 주기식’이라는 인상을 지우기 어렵다. 국정원이 실시하는 ‘정보보안관리실태 평가’에서 우수한 평가를 받기 위해 정보보안인력을 양적으로 부풀리는 과정에서 일어난 과도기적 모습으로 보인다.

2.3. 분임 정보보호담당자와 보안실무자의 임무

분임정보보호담당자는 「전산업무관리규정」상 각 부서의 전산담당자로서 분임정보보호책임자를 보좌하여 다음의 정보보호 임무를 수행하는데 내규 상 열거된 내용은 다음과 같다.

1. 부서 내 악성프로그램 사용에 대한 예방
2. 정보보호책임자의 정보보호활동에 대한 지원
3. 부서별 정보보호 활동에 대한 기록 관리
4. 부서의 전산장비 반·출입 관리

정보보호책임자 및 분임정보보호책임자의 임무에 비해 분임정보보호담당자의 책무가 상당히 적게 열거되어 있는 것을 확인할 수 있는데 분임보안책임자의 지시를 받고 각 부서의 보안실무를 수행하는 분임보안담당자의 임무와 존재는 아예 찾아볼 수도 없다. 단적으로 말해서 현행업무분장은 분임담당자의 업무수행을 고려한 것이 아니라 책임자의 책무만 상세하게 나열하는 데 그치고 있다고 볼 수 있다. 이러한 환경에서는 분임담당자가 소관 업무를 정확히 이행하기가 매우 어렵다.

이에 더하여 분임담당자의 정보보안실무능력을 더 악화시키는 현실을 들춰보면 다음과 같다. 분임개인정보책임자 및 정보보호책임자, 분임보안책임자는 모두 부서장이 맡고 있는데 분임정보보호담당자, 분임개인정보보호담당자, 분임보안실무자는 모두 다른 경우가

대부분이다. 업무량을 균등하게 배분하기 위해 분임담당자를 모두 다르게 정하고 있는 것이다. 결과적으로 분임정보보호담당자가 해야 할 일을 분임개인정보보호담당자가 하게 되는 경우, 분임보안실무자가 해야 할 일을 분임정보보호담당자가 하고 있는 경우 등 바람직하지 못한 현실이 계속되고 있다. 이를 바로잡기 위해 보안전담부서의 업무지도 사항은 분임보안실무자가, 정보보호전담부서의 업무지도 사항은 분임정보보호담당자가 이행하기로 하는 등 나름대로 정보보안 활동을 질서 있게 수행하기 위한 시도를 하고는 있지만 다음과 같은 현실에 부딪쳐 문제가 해결되지 않고 있다. 보안책임자가 전산보안에 관한 권한까지 갖고 있고 정보보호책임자가 개인정보보호책임자와 동일한 조직체에서 해당 전담부서의 업무지도 사항이 개인·정보보호와 보안 사항으로 명확히 구분되지 않는 내재적 한계를 갖고 있는 것이다. 정보·보안 분임담당자가 업무분장 관련 애로사항을 겪을 수밖에 없는 원인을 이러한 현실에서 찾을 수 있다. 주 업무와 정보·보안업무를 병행해야 하는 분임담당자의 부담에 대한 문제는 수많은 선행연구에서 충분히 언급되었기 때문에 재조명하지 않기로 한다.

Ⅲ. 분임담당자 중심 업무분장 구현

공공기관 부서장은 분임정보보호책임자로서 부서 내 정보보호 활동을 위해 전산담당자를 정하고 있다. 전산담당자는 내규에 의해 분임정보보호담당자가 되며 앞서 살펴본 임무를 수행한다. 즉 각 부서의 부서장이 직접 분임정보보호담당자를 지정하는 셈인데 이 때문에 분임정보보호담당자는 조직체계 상 정보보호책임자로부터 더 멀어지게 된다. 또한 정보보호업무를 주 업무와 병행해야 하는 현행 조직 환경에서 분임정보보호담당자는 적지 않은 PC 및 네트워크 관련 정보·보안업무를 빠르게 수행해야 하기 때문에 각 부서의 최하급 직원인 경우가 대부분이다. 공공기관의 분임정보보호담당자가 적극적으로 정보보호활동을 수행하는 데 어려움을 겪는 원인 중 하나가 여기에 있다고 본다. 현실태를 극복하기 위한 방편으로 아래와 같은 업무분장을 제시하고자 한다.

3.1. 분임정보보호담당자 중심 업무분장 구현

분임정보보호담당자는 정보보호책임자가 정한 근무 기간 4년 이상의 직원으로 하며 다음의 정보보호담당자의 임무를 보좌하고 부서 내 정보보호 임무를 수행한다.

1. 정보보호 세부계획의 수립·실행
2. 보안성 검토 주관
3. 전산보안사고 실무
4. 정보보호시스템 운영 관리·감시
5. 정보보호 관련 정보수집 및 동향 파악
6. 업무의 전산화, 업무시스템 운영, 외부인력의 수행 업무 등에 대한 정보보호 관리
7. 전산관련 설비에 대한 정보보호 관리
8. 정보보호시스템의 운용 및 보안관리
9. 그밖에 분임보안담당자의 업무 외 기타사항

상기와 같이 전산보안전담부서의 정보보호책임자가 각 부서의 부점장 대신 분임정보보호담당자를 직접 지정하면 그림 3과 같이 정보보호책임자로부터 분임정보보호담당자에 이르기 까지 조직체계가 간명해진다. 또한 최소 4년 이상의 경력직원이 분임정보보호담당자의 임무를 수행함으로써 분임담당자의 위상이 높아짐은 물론 보다 더 수월하게 정보보호 업무를 처리할 수도 있게 된다[4].

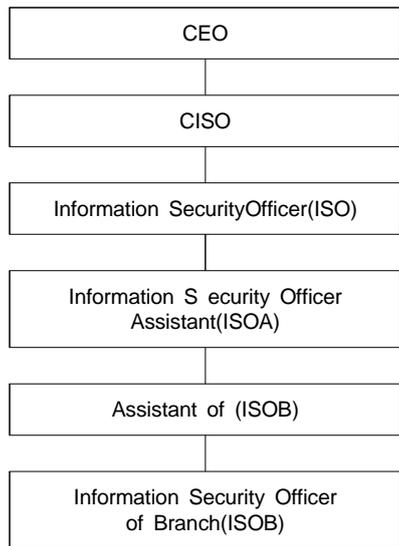


Fig. 3 Information Security Management System basis on Assistant of branch

3.2. 분임보안실무자 중심 업무분장 구현

현행 업무분장은 보안과 정보보호를 굳이 구분하면서 보안규정 내 정보보안에 관한 사항을 중복적으로 다루고 있다. 때문에 보안시스템의 책임에 관한 제 문제, 정보전산부 시스템운영실의 보안대책 수립과 같은 전산보안사항과 매우 밀접한 업무수행을 위한 보조업무를 최종적으로 분임보안실무자와 분임정보보호담당자가 중복적으로 이행하고 있다. 이와 같은 문제를 해결하기 위해 다음과 같이 분임보안실무자 중심 업무분장을 구현해 본다.

분임보안담당자는 정보보호책임자가 정한 근무기간 4년 이상의 직원으로 하며 다음의 부서내 전산보안 임무를 수행한다.

1. 정보통신망의 보안수준 보고
2. 보조기억매체의 현황파악
3. 비밀번호 사용여부의 주기적 점검
4. 그 밖에 전산보안에 관해 필요한 사항

앞서 잠시 언급했듯이 분임보안실무자의 존재를 내규 및 업무분장에 반영할 필요가 있다. 또한 전산보안 관련 중복업무 해소를 위해 분임정보보호담당자와 임무와 상이한 임무를 명시해서 불필요한 업무과중 문제를 해소할 필요도 있다[5].

IV. 평가

본 논문에서 밝힌 분임담당자 중심 업무분장이 구현될 경우 정보·보안사고 발생 시 전사적인 의사결정 과정을 살펴보기 위한 시뮬레이션을 위해 다음을 가정한다. 첫째, 모든 담당자는 직무수행 시 선 조치, 후 보고를 한다. 둘째, 가장 심각한 경우를 고려하기 위해 비전담부서의 분임담당자가 최초로 DDoS 등 정보·보안사고를 발견한다고 가정한다. 상기와 같은 두 가지 조건을 가정할 경우 정보·보안사고 발생 시 그림 4와 같은 시뮬레이션 결과를 확인할 수 있다.

먼저 분임담당자가 사고를 최초로 발견한다. 1. 분임담당자가 전산·보안사고를 최초로 발견하게 되면 평소 교육받은 대로 2. 선 조치를 실시하고 구현한 업무분장대로 분임담당자가 보좌하는 3. 전담부서 정보보호담당자에게 후 보고를 한다.

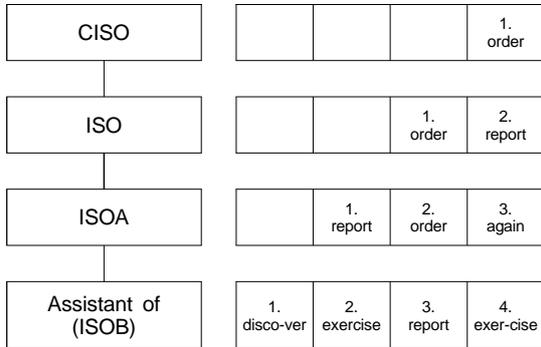


Fig. 4 Emergency Order System

전담부서 담당자는 분임담당자로부터 보고를 받고 1. 분임담당자에게 업무지시를 한 뒤 2. 정보보호책임자에게 보안사고 발생사실을 보고한다. 정보보호책임자는 1. 전담부서 정보보호담당자에게 업무지시를 한 뒤 2. 최고책임자에게 보고를 한다. 정보보호최고책임자가 사장에게 사후보고를 하거나 분임담당자가 분임책임자에게 사후보고를 하는 것은 이미 실무자(정보보호최고책임자-정보보호책임자-정보보호담당자-분임담당자)간 지시와 보고, 선 조치를 마친 이후이다. 현행 업무분장과 비교하면 표 1과 같은 장점을 갖는다.

Table. 1 Comparison

	The Present	The Proposal
Number of Staff	Six(Security Officer,CISO,ISO,ISOA,ISOB, Assistant of (ISOB))	four(CISO, ISO,ISOA, Assistant of (ISOB))
Principles	unclear	clear
Qualification for Assistant of (B)	anybody (newcomer)	career staff
Empowerment	ISOB	ISO
Common Works	a lot	almost nothing
Communication Number	-	increase
Information Security	-	upgrade

본 논문에서 제시하는 업무분장을 구현 할 경우 무엇보다 전산·보안사고 발생 시 의사결정 과정에 관여하는 직원 수가 감소해서 신속한 대응이 가능하다는 장점이

있다. 또한 전산보안에 관한 인사권한 등을 정보보호책임자가 갖게 되면 전산보안사고 발생 전 정보보호책임자가 독립적으로 의사결정 준칙을 수립할 수 있다. 마지막으로 전담부서장인 정보보호책임자가 경력직원 중 분임담당자를 직접 정하고 이들로 하여금 정보보호담당자를 보좌하도록 하면 분임담당자의 위상이 높아질 것은 물론 실무자 간 소통의 길이 열리고 분임담당자의 업무수행력이 향상 되어 전사적인 보안수준까지 개선될 수 있다[6]. 하지만 전산고도화 현실에서 보안업무와 전산보안업무가 매우 밀착되어 있는 까닭에 전산보안업무만 따로 분리하기가 쉽지 않고 전산보안 업무를 정보보호책임자가 포괄양도 받는다면 기타 보안업무만 수행하는 보안담당관 제도의 존립에 대한 의문이 발생할 수 있기 때문에 실현되기까지 적지 않은 시간이 소요될 수 있다.

V. 향후과제

본문에서 구현한 업무분장의 효과를 보다 더 정밀하게 분석하기 위해서는 수년에 걸쳐 통계자료 등을 수집 할 필요가 있다. 또한 정보보호와 개인정보보호의 구별실익, 정보보호와 보안의 분리 등 정보·보안 업무 특성 상 다루기 어려운 주제를 해결하기 위한 방안으로 실무자들로부터 광범위한 의견수렴을 할 필요가 있다고 본다.

REFERENCES

[1] D. K. Choi, M. S. Song, J. I. Im, K. H. Lee, "Study the role of information security personnel have on an organization's information security level," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 25, no. 1, pp. 197-362, Feb. 2015.

[2] S. S. Jang, S. J. Lee, B. N. Noh, "The effects of the operation of an information security management system on the performance of information security," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 22, no. 5, pp. 1123-1132, Oct. 2012.

[3] TTAS.KO-10.0089/R1, *GUIDELINES ON IT SECURITY POLICY FOR PUBLIC INSTITUTIONS AND ORGANIZATIONS*,

- TTA(Telecommunications Technology Association), 1999.
- [4] J. S. Song, M. J. Jeon, M. G. Choi, "A Study on Factors Affecting the Level of Information Security Governance in Korea Government Institutions and Agencies," *The Journal of Society for e-Business Studies*, vol. 16, no. 1, pp. 133-151, Feb. 2011.
- [5] J. S. Kim, S. Y. Lee, J. I. Lim, "Comparison of The ISMS Difference for Private and Public Sector," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 20, no. 2, pp. 117-129, Apr. 2010.
- [6] S. H. Ryu, D. R. Jeong, H. K. Jung, "Ways to establish public authorities information security governance utilizing E-government information security management system (G-ISMS)," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 4, pp. 769-774, Apr. 2013.



김상균(Sang-Kyoon Kim)

2009년 : 서울시립대학교 경제학부 졸업(학사)
2014년 ~ 현재 : 고려대학교 정보보호대학원 석사 과정
※관심분야 : 금융회사 개인정보보호, 금융보안정책, IT 감사



김인석(In-Seok Kim)

1973년 : 홍익대학교 전자계산학과(학사)
2003년 : 동국대학교 정보보호학과(석사)
2008년 : 고려대학교 정보경영공학과(박사)
2009년 ~ 현재 : 고려대학교정보보호 대학원 교수
※관심분야 : 전자금융보안, IT 감사, 전자금융법규