http://dx.doi.org/10.14400/JDC.2014.12.2.563

정보보호 관리의 한계점과 개선방안에 관한 연구

이수진[*], 최상용[**], 김재경[*], 오충식[*], 서창호[***,+]
한국과학기술정보연구원[*], 한국과학기술원[**], 공주대학교[***]

A Study for Limitations and Improvement of Information Security Management System

Sujin Lee[*], Sang-Yong Choi[**], JaeKyoung Kim[*], ChungShick Oh[*], Changho Seo[***]
Korea Institute of Science and Technology Information[*],
Korea Advanced Institute of Science and Technology[**], Kongju National University[***]

요 약 정보보호의 중요성이 커지면서 안전행정부, 미래창조과학부, 교육부, 국가정보원 등 소관부처별 정보보안에 대한 심사기준을 제정하고 평가를 시행하고 있는 실정이다. 특히 2010년 G-ISMS, 2011년 개인정보보호법 시행 등 최근 정보보호의 중요성이 커지면서 보다 효과적인 정보보호 관리를 위한 노력이 커지고 있다. 이러한 각종 정보보호 인증과 심사는 공공기관의 정보보호 수준을 향상시키는데 많은 도움을 주고 있으나, 실무 기관에서는 연중 수시로 있는 소관부처별 인증심사로 인해 업무효율성이 저하되고 효과적인 보안관리에는 한계가 있다. 본 논문에서는 현재 공공기관을 대상으로 실시되는 정보보호 관리 심사기준을 분석하고, 한계점과 개선방향을 제시하고자 한다.

주제어 : 정보보호 관리체계, 정보보호수준 진단지표, 보안관리 프로세스, G-ISMS, ISO/IEC 20771

Abstract As information security is becoming more important today, efforts in managing information security more efficiently is becoming greater. Each department such as Ministry of Security and Public Administration, Ministry of Science, Ministry of Education, National Intelligence Service, etc. is established screening criteria for information security and conducted the evaluation. Various information security certification and evaluation for public institutions effectively help to improve the level of information security. However, there are limitations of efficient security management because the examination to be performed frequently by each department. In this paper, we analyze screening criteria of the information security management that is being conducted in the public institutions. We also present limitations of information security management and the direction of improving the limitations.

Key Words : Information Security Management System, diagnosis index for information security, security management process, G-ISMS, ISO/IEC 27001

* This work was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education,Science and Technology, Republic of Korea (2011-0029927) and Basic Sciences Program through the National Research Foundation of Korea (NRF), Republic of Korea (2013-R1A1A2010382).
Received 15 January 2014, Revised 16 February 2014
Accepted 20 February 2014
Corresponding Author: ChungShick Oh (KISTI)
Email : ocs@kisti.re.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.otg/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 서론

인터넷과 정보통신망의 발전에 따라 사회생활의 편리성이 증대한 반면, 인터넷의 부작용인 정보보호 위협 또한 증가하고 있다. 과거 사회적 이슈가 되었던 2011년 농협 전산망 마비[1], SK컴즈 개인정보 유출 사태[2]를 포함한 최근 2013년 3.20사이버테러[3], 6.25 사이버테러[4] 등은 정보통신망을 이용한 정보보호 위협의 대표적인 사례이다.

이와 같은 심각한 피해가 지속적으로 발생됨에 따라 정보보호의 중요성 또한 높아지고 있으며, 이의 일환으로 각 분야별 정보보호 관리체계를 수립하고 운영하고 있다. 국제적으로는 영국의 정보보호 관리표준인 BS7799[5]를 확장한 ISO/IEC 27001[6]이 국제정보보안경영시스템으로 자리잡고 있으며, 국내에서는 민간기업을 대상으로 한 K-ISMS[7]와 공공기관을 대상으로 한 G-ISMS[8]가 표준으로 자리하고 있으며, 개인정보보호에 대해서는 특별히 PIMS[9]가 존재한다. 또한 공공기관의 경우 국가정보원의 정보보호 관리실태 평가, 국책 연구기관의 경우 교육부의 정보보호수준 자가진단[10]이 존재한다. 이와 같은 다양한 지침은 각 소관부처의 성격과 보안 평가의 특성에 부합하게 평가항목이 정해져 있으나 평가항목의 중복성 및 연중 평가기간 불일치 등으로 인한 실무기관의 중복업무 등 일부 비효율적으로 관리되는 한계점이 존재한다.

본 논문에서는 이와 같은 한계점을 도출하고 보다 효과적인 보안관리 업무를 수행하기 위한 개선방안을 제시한다. 이를 위해 먼저 2장에서는 기존 정보보호 관리체계의 통제항목 분석과 피 평가기관의 입장에서 정보보호 업무의 현황을 분석하고 이를 기반으로 현재 정보보호 관리체계의 한계점을 제시하고 3장에서는 이를 개선하기 위한 접근방법과 실무적 측면에서의 개선방안을 제시한다. 그리고 4장에서는 제안한 방안의 효과와 향후 연구방향으로 결론을 맺는다.

2. 관련연구

이번 장에서는 기존 정보보호 관리체계의 현황과 정보보호 업무현황을 분석한다. 분석은 국제 평가기준인 ISO/IEC 27001과 국내 공공기관의 정보보호 관리체계인 G-ISMS, 개인정보보호 평가, 교육부의 정보보호수준 자가진단 등 대표적인 평가 기준을 대상으로 한다.

2.1 ISO/IEC 27001

ISO/IEC 27001[6]은 과거 영국의 정보보호 관리표준인 BS7799[5]를 기반으로 하고 있으며, ISO27000 시리즈에는 ISMS수립 및 인증에 관한 원칙과 용어를 규정하는 표준인 ISO27000, 보안범위 및 자산정의, 정책시행, 모니터링과 검토, 지속적인 개선 등 ISMS구현을 위한 프로젝트 수행 시 참고해야할 구체적인 구현 권고사항을 규정한 ISO27003, ISMS에 구현된 정보보호 통제의 유효성을 측정하기 위한 프로그램과 프로세스를 규정한 ISO27004, 위험관리 과정을 환경설정, 위험평가, 위험처리, 위험소통, 위험 모니터링 및 검토 등 6개의 프로세스로 구분하고 프로세스별 활동을 기술한 문서인 ISO27005 등을 포함한 ISO27006 ~ ISO27009 까지의 표준이 포함된다. ISO27001에는 정보보호의 기본목표인 기밀성과 무결성, 가용성 및 책임성, 부인방지, 신뢰성 등의 속성을 만족하기 위한 정보보호 통제항목을 정의하고 있다.

〈Table 1〉 Classification of control items in ISO27001

Security control classification	Control domain	Items	Details	Total
administrative security	security policy	1	2	47
	organizational security	2	11	
	asset management	2	5	
	human resources security	3	9	
	information security accident management	2	5	
	business continuity management	1	5	
	compliance	3	10	
physical security	physical security and environmental security	2	13	13
technical security	communication and operation management	10	32	73
	access control	7	25	
	information system gain, development and maintenance	6	16	
total	11	39	133	

ISO27001의 세부 통제항목은 총 11개 통제영역의 133개 세부통제항목으로 그 현황은 표 1과 같다. 보안통제 유형으로 구분하는 경우에는 세부통제항목 수가 관리적 보안 47개, 물리적 보안 13개, 기술적 보안 73개로 분류할 수 있다. 정보와 정보처리설비에 의해 관리되는 정보자산의 특성에 따라 물리적 보안 대비, 기술적/관리적 보안 세부통제항목이 더 많은 비중을 보이고 있다.

2.2 전자정부 정보보호 관리체계

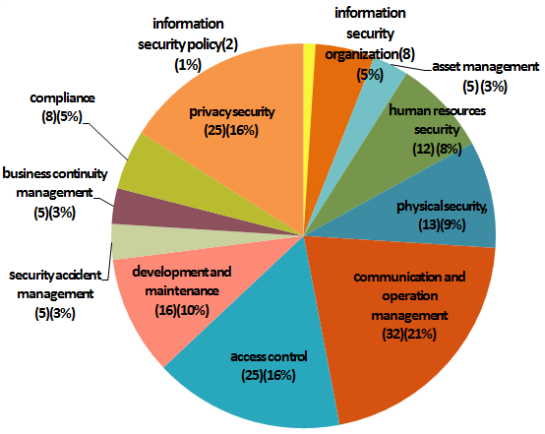
전자정부 정보보호 관리체계(G-ISMS)[8]는 조직의 정보 자산을 체계적으로 보호하고 사이버 침해 위협으로부터 조직이 유기적으로 대응하기 위한 종합적인 관리체계인 ISMS를 정부 행정기관 등의 조직 및 서비스 특성에 적합하게 수립한 종합적인 정보보호 관리체계이다.

G-ISMS는 역할과 책임에 따라 표2와 같이 정책기관, 인증위원회, 인증기관, 신청기관으로 구분하며 정책기관과 인증위원회는 안정행정부가, 인증기관은 한국인터넷진흥원(KISA)이 역할을 수행한다.

〈Table 2〉 Certification system of G-ISMS

Institution	Role
policy authority (MOSPA†)	establishment of G-ISMS certificate system, designation and supervision of certificate authority, composition and management of G-ISMS certificate committee, appointment of a G-ISMS certificate auditor, security of budget related to certificate, establishment of policies required for certificate
certification committee	deliberation/approval of certificate audit report submitted by certificate authority, tasks devolved by minister of MOSPA
certificate authority (KISA††)	G-ISMS certificate audit, G-ISMS certificate issue and management, G-ISMS certificate auditor training, G-ISMS certificate counsel and technical advice, research business required for certificate task ※ certificate authority organizes and manage certificate audit team.
application authority	authority applying for G-ISMS certificate ※ G-ISMS certificate is not mandatory and can be applied to any authority.

G-ISMS는 표 3과 같이 12개의 통제 분야, 43개의 통제사항, 그리고 156개의 세부 통제사항으로 구성되어 있다. 각 통제 분야별 항목수를 살펴보면 32개의 항목을 가지는 통신 및 운영관리 분야가 가장 큰 비율(21%)을 차지하고 있다. 접근통제와 개인정보보호도 각 분야별 25개의 항목을 가지며 총 G-ISMS에서 16%를 각각 차지하고 있다. 2개의 항목을 가져 전체 비율 중 1%를 나타내는 정보보호 정책 분야가 가장 적은 항목을 가지고 있다. 또한 자산관리, 보안사고 관리, 그리고 업무연속성 관리 분야 또한 각 통제 분야별 5개의 항목을 가져 전체 G-ISMS에서 3%의 비율을 차지하고 있다.



[Figure 1] Ratio of certification items in G-ISMS

G-ISMS의 전체 세부 통제사항에 대해 각각의 항목을 크게 관리적, 물리적, 기술적, 개인정보와 같이 4개의 분야로 나누어 각 분야별 비율을 살펴보면 그림1과 같이 관리적 보안에는 정보보호 정책, 정보보호 조직, 인적 보안, 업무연속성 관리, 준거성의 내용이 포함되었다. 물리적 보안에는 물리적 보안 분야를 포함시켰다. 기술적 보안에는 자산관리, 통신 및 운영관리, 접근통제, 정보시스템 요구사항, 개발 및 유지보수, 보안사고 관리 분야를 포함시켰다. 그리고 개인정보 보호 분야에는 개인정보화 관련된 세부 통제사항을 반영하였다.

G-ISMS에서는 총 156개의 세부 통제 항목 중 83개가 기술적 보안 영역에 포함된다. 이것은 총 비율 중 53%를 차지하는 것으로 G-ISMS에서는 기술적 보안 분야를 가

† Ministry Of Security and Public Administration
†† Korea Internet & Security Agency

장 중요시 하고 있다는 것을 알 수 있다. 그 다음으로 35개의 세부 통제항목이 포함 된 관리적 분야가 전체 비율 23%를 차지하고 있다. 25개의 세부 통제항목이 포함된 개인정보가 16%, 그리고 13개의 세부 통제항목이 포함된 물리적 보안 분야가 총 8%로 가장 낮은 비율이다. 즉, G-ISMS에서는 관리적(인적), 물리·환경적, 기술적, 개인정보보호 등 전체 분야를 다루고 있다.

〈Table 3〉 Classification of control items in G-ISMS

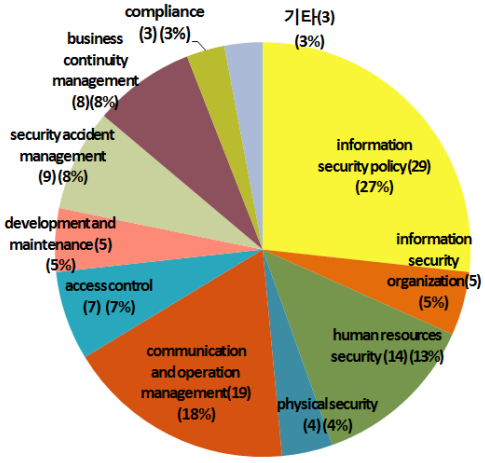
Domain	Items	Rate
1. information security policy	2	1%
2. information security organization	8	5%
3. asset management	5	3%
4. human resources security	12	8%
5. physical security	13	9%
6. communication and operation management	32	21%
7. access control	25	16%
8. information system requirement, development and maintenance	16	10%
9. security accident management	5	3%
10. business continuity management	5	3%
11. compliance	8	5%
12. privacy security	25	16%
total	156	100%

2.3 정보보호수준 자가진단

교육부의 정보보호수준 자가진단[10]은 6개의 Domain, 17개의 통제사항, 그리고 106개의 세부 통제항목으로 구성되어 있다. 이를 G-ISMS의 통제항목에 맞게 정보보호수준 자가진단의 평가 항목을 재구성 해보면 표 4와 같이 29개의 항목이 포함된 정보보호 정책 부분이 27%로 가장 많은 것을 알 수 있다. 그리고 통신 및 운영관리, 인적 보안 항목도 각각 19개, 14개로 전체 평가항목 중 18%, 13%를 차지한다. 교육부의 정보보호수준 자가진단에서는 개인정보보호와 관련된 항목을 찾을 수 없다. 이는 개인정보보호에 관한 부분은 따로 안정행정부에서 정책을 시행하기 때문이다. 정보보호 수준 자가진단을 관리적, 물리적, 기술적, 그리고 개인정보 분야로 나누어 살펴보면 그림 2와 같이 총 106개의 세부 통제항목 중 62개가 관리적 부분에 포함되어 전체 58%를 차지한다. 기술적 부분은 총 40개의 세부 통제항목이 포함되어 전체 비율 중 38%를 나타낸다. 이처럼 두 분야에 있어 96%의 비율을 보이는 것을 통해 주로 관리적 분야와 기술적 분야를 집중적으로 다루고 있다는 것을 알 수 있다.

〈Table 4〉 Classification of control items in ministry of education(MOE) for information security

Domain	Items	Rate
information security policy	29	27%
information security organization	5	5%
asset management	0	0%
human resources security	14	13%
physical security	4	4%
communication&operation management	19	18%
access control	7	7%
information system requirement, development and maintenance	5	5%
security accident management	9	8%
business continuity management	8	8%
compliance	3	3%
privacy security	0	0%
etc.	3	3%
total	106	100%



[Figure 2] Ratio of evaluation items in MOE

2.4 개인정보보호수준 자가진단

안정행정부의 개인정보 보호수준 진단지표는 3개 분야, 20개 진단지표, 84개 진단항목으로 구성된다. 84개의 진단항목 중 75개는 공통 진단항목이며 9개는 공공기관 진단항목으로 공공기관만 해당되는 진단항목이다. 이 평가체계는 개인정보보호 분야에만 특화된 것이다. 개인정보보호 평가항목을 G-ISMS의 항목과 비교해 보면 표 5

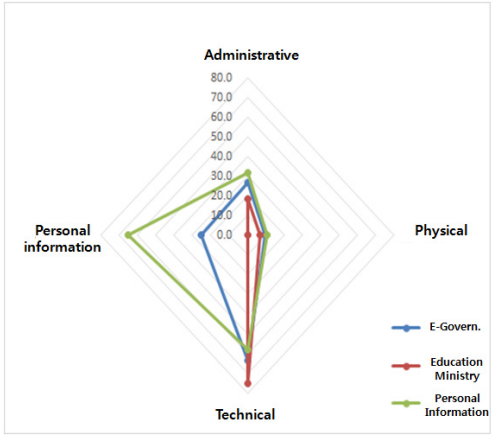
와 같이 분류된다. 개인정보 보호수준 자가진단 지표는 개인정보 보호수준 진단지표 항목과 개인정보 보호수준 진단지표 상세 설명으로 구성되어있다. 진단지표 상세 설명은 대분류, 중분류, 측정지표, 진단 항목, 세부 설명 그리고 증빙 자료로 구성된다. 정량적 판단을 위한 세부 기준이 제시되어 있지는 않으나, 일정 수준의 정량적 평가는 가능하다.

〈Table 5〉 Classification of evaluation items in personal information security

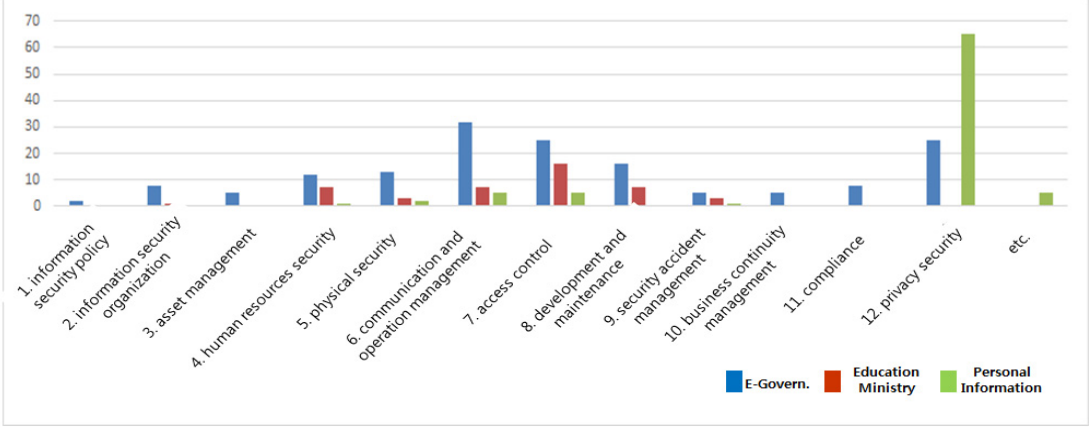
Domain	Items	Rate
information security policy	0	0%
information security organization	0	0%
asset management	0	0%
human resources security	1	1%
physical security	2	3%
communication and operation management	5	6%
access control	5	6%
information system requirement, development and maintenance	0	0%
security accident management	1	1%
business continuity management	0	0%
compliance	0	0%
privacy security	65	77%
etc.	5	6%
total	84	100%

2.5 기존 관리체계 종합분석 및 한계점

기존 관리체계를 분석한 결과 그림 3과 같이 전체적으로 기술적 보안 분야에 많은 부분이 집중되어 있고, 물리적 보안 분야는 상대적으로 정보보호 관리체계에서 적게 다루고 있다. 또한, 통제분야별 분포를 살펴보면, 그림 4와 같이 G-ISMS의 경우 전체적인 부분을 모두 다루고 있으나, 개인정보보호 자가진단의 경우 개인정보보호분야에, 교육부 평가의 경우 기술적 분야에만 집중되어 있음이 더욱 확연히 확인된다. 또한 전체적으로 12가지 분야로 정리한 결과 인적보안, 물리적보안, 통신 및 운영관리, 접근통제, 개발유지보수, 사고관리 등 6개 분야에 요구되는 관리수준과 항목의 수의 많고 적음의 차이가 있을 뿐 3개의 평가기준이 대동소이한 관리체계를 요구하고 있다.



[Figure 3] Distribution of fields



[Figure 4] Distribution of control items

이와 같은 다양한 정보보호 관리체계는 측정의 목적과 소관부처의 성격에 따라 효과적으로 수립되어 있다. 하지만 이와 같은 다양성으로 인해 실무기관의 정보보호 담당자 입장에서 한계점이 도출된다.

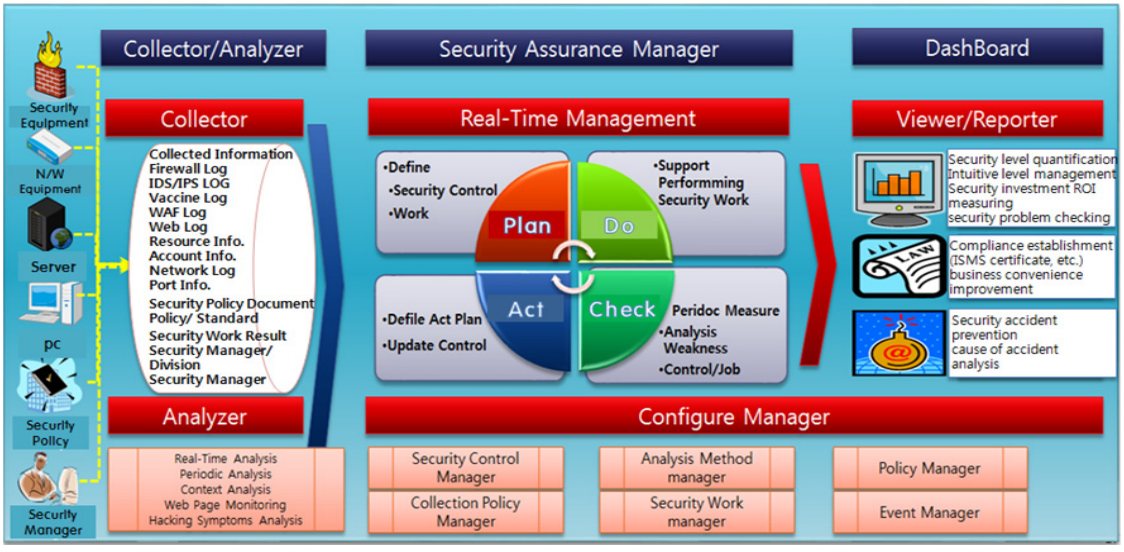
대표적인 한계점은 유사한 통제항목에 대해 안행부, 미래부 등 복수의 감독기관에서 별도로 실시하는 평가로 인한 업무능률 저하이다. 즉, 유사한 통제항목으로 구성되었지만 평가기간과 평가 시기가 관리기관마다 상이하여 실무기관 정보보호 담당자는 연중 수시로 평가에 대응해야 하는 필요성으로 인해 실제 정보보호 업무보다 평가에 더욱 많은 자원을 투입해야 하는 현실적인 한계점이 있다. 두 번째로는 각각의 평가 항목이 평가자의 정성적인 판단에 근거하게 되어 종합적으로 평가결과의 신뢰성이 하락되고 이로 인해 평가 결과를 활용한 예산확보 등 개선계획 수립 및 반영에 효과적으로 반영할 수 없는 한계점이 존재한다.

3. 공공기관 정보보호 관리체계 개선 제안

이번 장에서는 본 논문에서 제안하는 공공기관 정보보호 관리체계의 효율적 운영을 위한 방안을 설명한다. 효율적 운영을 위한 접근 방향은 실무 기관의 관점에서 정보보호 담당자의 업무효율을 증대시키고, 감독기관의 입장에서도 기관별 관리체계 수준평가의 목적을 달성할 수 있도록 한다.

다양한 정보보호 관리체계를 효과적으로 운영하기 위해서는 부처별 분산되어 있는 정보보호 관리체계의 통합이 필요하다. 물론 공공기관 정보보호 관리체계인 G-ISMS가 존재하지만, G-ISMS의 경우 인증에 관련된 관리체계이며, 민간기업의 ISMS와 통합작업이 이루어지고 있지만 이는 기본적으로 관리체계 수립의 현황을 점검하고 지속적인 활동을 보증하기 위한 프로세스로의 의미가 강하다. 반면 개인정보보호수준 자가진단, 정보보호 수준 자가진단 등의 평가는 해당기관의 수준을 평가하여 순위를 매기고 이를 기관평가의 기준으로 삼고 있어 실무기관 정보보호 담당자의 입장에서는 현실적으로 G-ISMS보다 강제성이 강하다. 즉, 실질적으로 보다 큰 의미가 있는 활동은 G-ISMS를 수립하는 활동이나, 현실적으로 평가를 위한 진단이 더 비중 있게 다루어지는 문제가 있다.

이를 해결하기 위해서는 먼저, G-ISMS를 중심으로 한 정보보호수준 자가진단, 개인정보보호수준 평가 등 정보보호 관리체계의 기준을 일원화하고 통일하여 실무기관 입장에서 지속적인 관리활동이 보장될 수 있는 환



[Figure 5] Architecture of information security management system

경을 조성해야 한다. G-ISMS를 중심으로 통합해야 하는 이유는 첫째, G-ISMS의 경우 국제적 표준인 ISO/IEC 27001을 기반으로 하고, 정보보호에 관한 물리적, 기술적, 관리적 분야의 항목들을 포괄적으로 포함하고 있어 통합을 위한 기준으로서 의미가 있으며, 둘째, 타 평가기준의 경우 평가 목적에 따라 특화된 일정분야에 대해서만 집중하고 있어 상대적으로 약한 분야가 존재한다.

다음으로 기존의 G-ISMS를 기준으로 통합한 후 통합된 정보보호 관리체계를 기존 G-ISMS와 같이 인증의 기준으로 삼는 것이 아니라 타 평가를 대체 할 수 있도록 보다 강제력을 강화하여야 한다. 즉, 현업에서 실제 비중있게 다루어지는 업무가 기관평가의 기준이 될 수 있도록 하여야 한다. 또한, 통합된 정보보호 관리체계의 평가방법에 대해 정성적인 평가를 지양하고 각 항목별 수준을 정량적으로 평가할 수 있는 측정방법을 개발하여야 한다. 정보보호 수준을 정량적인 수준으로 측정하여 정보보호 담당자로 하여금 부족한 부분을 쉽게 인지 할 수 있도록 지원하여야 하며, 정보보호 투자 대비 효과를 직관적으로 예상할 수 있도록 지원할 수 있다.

이와 같은 과정을 통해 실무기관에서는 정보보호 수준을 실시간으로 정량적으로 측정하고 관리할 수 있는 기반을 구축할 수 있다. 실시간 정보보호 관리체계 구축을 위해 필요한 요소로는 첫째, 자동화된 데이터 수집이 필요하다. 정보보호 관리체계에서 요구하는 지속적인 관리를 보증하기 위해 자동화된 데이터 수집과 이를 계량화하여 표출해 줄 수 있는 데시보드는 필수적이다. 둘째, 정보보호 관리체계의 표준운영 방법인 <계획 → 구현 → 점검 → 개선>의 4단계를 유기적으로 지원해 줄 수 있는 관리시스템이 필요하다. 마지막으로 정보보호 관리체계의 평가 항목을 관리해주고, 실제 수집된 데이터를 계량화 할 수 있는 분석 시스템이 필요하다. 이와 같은 요소를 포함하는 정보보호 관리체계의 통합된 아키텍처는 그림 5와 같다.

4. 결론 및 향후 연구방향

본 논문에서는 정보보호 관리체계를 운영하는 실무기관의 입장에서 소관부처가 다른 3가지 관리체계의 특징과 한계점을 살펴보고, 이를 해결하기 위한 방안을 제시하였다.

제시한 방안은 분산된 정보보호 관리체계를 통합하고, 정량적인 측정이 가능한 자동화된 시스템을 이용하여 실무기관의 정보보호 담당자로 하여금 문제점과 개선에 따른 효과를 직관적으로 식별하고 분석할 수 있도록 도와줄 수 있다. 이를 위해서는 기관 운영시스템으로부터의 자동화된 수집과 정량적 측정방법 그리고 지속적인 관리를 위한 시스템이 필요하다. 향후, 본 논문에서 제안하는 정보보호 관리체계 시스템을 개발하여 실 환경에서 충분히 검증하고 개선하여 실무기관 정보보호 담당자의 업무 효율성을 증대시키기 위한 연구가 지속적으로 필요하다.

REFERENCE

[1] Park Daewoo, “A study for problems of management security from National Agricultural Cooperative Federation case", KIECS Spring Annual Conference, 2011, 5.1: 25-28.

[2] Hauri, “Malicious code analysis report about nateon hacking", August, 2011.

[3] Graham Cluley, “DarkSeoul: Sophos-Labs identifies malware used in South Korean internet attack,", March, 2013.

[4] ASEC, “detailed Aanlysis for malicious code used 6.25 DDoS attacks", June, 2013

[5] KENNING, M. J., "Security management standard −iso 17799/bs 7799", BT Technology Journal, 2001, 19.3: 132-136.

[6] CALDER, Alan; WATKINS, Steve. IT Governanace: A Manager's Guide to Data Security and ISO27001/ISO 27002. 2008.

[7] "Information Security Management System(ISMS)", http://blog.naver.com/p1ngp1ng?Redirect-Log&logNo=120040448210

[8] KISA, "Manual for G-ISMS cretification", KISA, May, 2011

[9] "PIMS(Personal Information management System)", http://privacy.naver.com/80116523634

[10] KISA, "Diagnosis manual for personal information security management", KISA, July, 2013

이 수 진(Sujin Lee)

- 2001년 2월 : 고려대 전자정보공학(학사)
- 2003년 2월 : 고려대 전자정보공학(석사)
- 2009년 2월 : 고려대 전자정보공학(박사)
- 2009년 ~ 2010년 : 고려대 산업기술연구소
- 2010년 ~ 현재 : 한국과학기술정보연구원
- 관심분야 : MANET, 통신프로토콜, 정보보호
- E-Mail : sujin2010@kisti.re.kr

최 상 용(Sang-Yong Choi)

- 2000년 2월 : 한남대학교 수학과(학사)
- 2003년 2월 : 한남대학교 컴퓨터공학과(석사)
- 2014년 3월 ~ 현재 : 전남대학교 대학원 정보보안협동과정
- 2012년 1월 ~ 현재 : 한국과학기술원 사이버보안연구센터 선임연구원
- 관심분야 : 네트워크 보안, 악성코드, 해킹
- E-Mail : csyong95@gmail.com

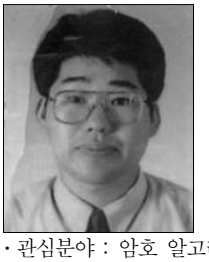
김 재 경(JaeKyoung Kim)

- 2005년 2월 : 광운대 컴퓨터과학과(석사)
- 2011년 1월 ~ 현재 : 한국과학기술정보연구원
- 관심분야 : 정보보안, 개인정보보호, 포렌식
- E-Mail : kjk@kisti.re.kr

오 충 식(ChungShick Oh)

- 2004년 2월 : 충북대 전자계산학과(석사)
- 2013년 2월 : 충북대 컴퓨터공학과(박사)
- 1986년 1월 ~ 현재 : 한국과학기술정보연구원 책임기술원
- 관심분야 : 보안, USN, 개인정보보호, 재난관리
- E-Mail : ocs@kisti.re.kr

서 창 호(Changho Seo)



- 1990년 2월 : 고려대 수학과(학사)
- 1992년 2월 : 고려대 수학과(석사)
- 1996년 8월 : 고려대 수학과(박사)
- 1996년 8월 ~ 2000년 : 한국전자통신연구원 선임연구원
- 2000년 3월 ~ 현재 : 공주대 응용수학과 교수
- 관심분야 : 암호 알고리즘, PKI, 무선 인터넷 보안 등
- E-Mail : chseo@kongju.ac.kr