Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.6, Dec. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1329

정보시스템 중요도 분류 방법론에 관한 연구*

최 명 길,†‡ 조 강 래
중앙대학교

A Study on the Methodology in Classifying the Importance of Information System*

Myeonggil Choi,†‡ Kang-rae Cho
Chung-Ang University

요 약

국가기관 및 공공기관, 민관기관에서 정보보안의 중요성이 나날이 커지고 있다. 정보시스템이 중단되면 대규모의 혼란이 발생할 가능성이 다분하기에, 정보보안관리체계의 확립이 필요하며, 고도화된 새로운 평가방법이 필요하다. 본 연구에서는 정보보안의 3요소인 기밀성, 무결성, 가용성을 기반으로 새로운 평가 지표인 업무영향도 평가를 도입하였고, 실제 사례를 통해 업무영향도 중요도를 등급별로 분류하여 새로운 정보보안 관리실태 평가가 정보보안 거버넌스의 핵심적인 역할을 수행할 수 있다.

ABSTRACT

The importance of information security is increasing in the public and private organizations. The interruption of the information system might cause massive disorder. To protect information systems effectively, information systems would be categorized and managed in terms of degree of importance. In this study, we suggest a new evaluation method that categorizes information systems based on the three nature of security, confidentiality, integrity and availability. For validation of the method, we use a case study in a public sector. Through the validation of method, the availability of applying the method for categorization information systems to other domains could be suggested.

Keywords: Classification of Information System, The Degree of Importance in Information System, Information Security Management

I. 서 론

2009년 7·7 대규모 DDoS 공격, 2011년 은행 전산망 마비, 재난 및 재해 발생 시 대규모의 국가·공공기관의 정보시스템의 운용이 중단되어 국가적 혼란이 발생 가능성이 잠재되어 있다. 대규모의 혼란이 발생하게 될 경우, 정보보안관리체계[1]가 확고히 정립되어 있지 않을 때, 재해 복구 및 연속성 유지에 상당한 시간이 소요될 것으로 예상되며, 피해를 최소화하고 신속한 정보시스템 운용의 정상화에 있어 정보보안관리체계가 중요하다.

정보보안관리체계 연구는 대상이 민간기관 또는 국가기관을 대상으로 하고 있으며, 민간기관은 물론 국가기관은 관련 데이터 공개를 매우 꺼리는 실정이다. 따라서 연구자가 활용할 수 있는 기존 선행 연구가 부재한 실정이다. 선행 연구의 부재는 정보보안관리체계를 이론적으로 흠결 없는 체계 개발에 있어서 큰 장애

접수일(2014년 11월 5일), 게재확정일(2014년 11월 17일)
* 이 논문은 2012년도 중앙대학교 연구장학기금 지원에 의한 것임
† 주저자, mgchoi@cau.ac.kr
‡ 교신저자, mgchoi@cau.ac.kr(Corresponding author)

가 된다. 이론 연구가 부재하고, 본 연구와 관련된 베스트 프랙티스(best practice) 등 정보보안 관리체계와 관련된 우수 사례 등이 거의 공개되어 있지 않아 다양한 정보보안 관리체계 수용 과정, 수용 결과의 성공 또는 실패 여부, 관리체계 도입의 효과성 등이 거의 보고되지 않고 있다.

따라서 위의 문제점을 보완하기 위해, 본 연구는 국가기관 정보보안 관리체계[6] 평가 항목 고도화를 주요 목적으로 한다. 국가기관의 정보보안 관리체계를 평가할 수 있는 프로세스 중심의 평가체계 개발과, 국가기관 정보보안 관리체계 평가 항목 개발을 중점 목표로 한다.

II. 연구의 중요성

정보보안관리실태평가[3]는 2006년에 처음 도입된 이후 중앙정부의 정보보안 수준 향상에 중요한 역할을 담당하고 있다. 특히 정보보안관리실태[2] 평가결과가 기관장 평가점수에 반영됨으로 실효성이 높은 제도로 정착되고 있으며, 정보보안 거버넌스의 중심축이 되고 있는 실정이다. 그러나 정보보안관리실태평가가 중앙 및 지방 행정기관, 정부출연연구기관 등으로 확대됨에 따라 정보보안관리실태 평가항목이 정보보안 수명주기(life cycle)를 기반으로 유연하게 적용할 수 있는 체계로 확대 발전될 필요가 있다.

정보보안관리실태평가가 국가기관의 정보보안 수준을 지속적으로 개선시키고 있지만, 동 평가는 정보자산의 중요성, 업무영향도, 정보보안속성(기밀성, 무결성, 가용성) 및 정보보안 자산의 선택, 구현, 평가, 개선 등에 따른 정보보안관리 수명주기를 고려하지 않음으로 정보보안의 연속성 및 효과성의 개선이 필요하다.

현 평가체계는 국가기관의 정보보안 환경 및 위험이 동일하다고 가정하고, 보안 대책 및 보안 활동을 평가하는 체계이다. 따라서 기관 고유의 위험 및 환경을 고려한 정보보안 계획 수립 및 자율 이행 과정을 평가하는 프로세스 평가 개념 및 체계를 도입해야 하며, 지속적으로 변화하는 정보보안 환경 및 기술을 비교적 빠른 시간 내에 국가기관이 자율적으로 수용할 수 있는 관리체계를 프로세스를 촉진 및 관리프로세스의 지속적인 성숙을 강화하는 성숙도 모델을 도입할 필요가 있다.

III. 정보보안관리실태 분석 및 개선 방향

현 평가체계는 정보보안규정준수 평가, 기관의 계층별 구성원(기관장, 정보보안담당자 및 일반직원)의 보안인식 평가, 기관자체 보안평가결과를 단기간의 실사 확인 등의 장점을 가지고 있다. 또한, 구성원에 대한 인터뷰, 테스트 등은 정보보안인식 개선에 상당한 성과를 거두고 있는 것으로 판단되며, 국가 기관의 기본적인 보안대책수준을 평균적으로 향상시키는 효과를 가지고 있다.

평가체계가 평가항목 중심으로 이루어짐으로 평가와 정보보안활동이 이원화 되는 경향이 있으며, 실태평가를 통해서 지적된 보안취약성이 개선되지 않고 있다. 정보보호수명주기인 '계획-실행-점검-개선(Plan-Do-Check-Act)'의 관점에서 평가항목을 분석하면 대부분 평가항목은 실행(do)에 해당되고, 검토(check) 및 조치(act)에 해당되는 활동은 소수로 구성되어있으며, 현 평가체계는 기관이 보유한 정보 및 정보시스템의 분류 및 중요도를 감안하지 않고 있어 해당 기관의 정보보안 특성을 반영하지 못한다는 단점이 있다.

따라서 단점을 보완할 필요가 있다. 현 평가대상은 중앙행정기관, 지방자치단체, 정부투자기관, 출연연구소 및 준정부기관 등 이질적인 특성을 가진 기관을 동일한 체계로 평가할 수 없으며, 이질적인 평가대상의 특성을 반영할 수 있는 체계로 개선이 필요하다. 또, 기관의 특성을 기관이 보유하고 있는 정보자산(정보, 정보시스템, 업무, 환경) 등의 중요도 및 위험도를 기준으로 분류하고[4], 기관은 정보자산의 특성을 반영한 정보보안대책을 수립함으로 기관의 특성을 반영할 수 있는 보안평가체계로 개선이 필요하다[7].

본 연구에서는 정보시스템의 중요도를 기준으로 정보시스템 보안평가 방법을 제시한다.

IV. 정보시스템 중요도 평가 측정 및 사례

중요도(업무중단 시)는 재난 발생으로 이전 단계에서 산출된 대응정도에 근거하여 업무가 중단될 경우, 복구 활동에 미치는 영향을 측정한 것으로, 영향도 측정 기준의 고려 사항은 업무 세부 기능 수행주기, 투입 인력 정도, 비상대응/복구가능 범위 및 예상복구소요 정도가 있다.

본 연구는 정보보안의 3요소인 기밀성(confidentiality), 무결성(intergrity), 가용성

(availability)를 중점으로 업무영향도 평가 방법을 제시하고, 실제 공공기관을 대상으로 업무영향도 평가를 실시하였다.

4.1 중요도 측정 사례

본 연구의 실효성을 확인 위해 서울의 D공사의 해당 업무 담당자와 정보보안 담당자를 대상으로 인터뷰를 실시하였으며 업무영향도 평가에 대해 설명하고 실제로 업무 영향도에 따라 정보시스템의 중요도를 결정하는 설문을 수행하였고, 각 정보보안의 속성에 따른 항목별로 점수를 매겨 중요도를 평가하였다.

업무담당자와 정보보안 담당자와의 인터뷰를 통해 확보한 정보시스템의 중요도와 새로운 평가방법을 통해 도출된 정보시스템의 중요도를 비교하였다.

측정 방법은 설문지법을 이용하여 리커트 5점 척도를 활용하여 1점 '매우 그렇지 않다' ~ 5점 '매우 그렇다'로 측정하였다. 본 연구에서는 D공사의 E-휴게소 시스템을 대상으로 설문하였다.

인터뷰를 통해, E-휴게소 시스템은 매출현황, 매출집계, 임대료 계산으로 구성되어있고 세부 시스템별로 업무담당자와 정보보안담당자가 생각하는 정보보안의 등급은 아래의 Table 1과 같다.

중요도를 계산하는 산식으로는 마크된 점수와 가중치를 곱하여 가중평균을 구하였다. 가중치(weight)는 업무 영향도에 있어 많은 영향을 미치는 것을 3점, 보통을 2점, 미미한 것을 1점으로 부여했다[8].

Table 1. The Degree of importance by Owners

classification	confidentiality	integrity	availability
presnt condition of sales (PS)	4-5	5	2-3
total sales (TS)	4-5	5	2-3
rental pricing (RP)	5	4-5	2-3

4.2 기밀성

허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다[9]. 비밀 보장이라고 할 수도 있으며, 원치 않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다[5].

본 연구에서는 업무영향도에 영향을 주는 기밀성에 관한 측정 도구로 29개의 문항을 포함한다.

Table 2. The Results of Confidentiality Assessment

confidentiality index	PS	TS	RP	W
relevance with information for policy, management, sales, and confidence-sensitive information	3	4	4	H
necessity of preventing disclosure of information	4	4	5	H
possibility of complaint in accordance with the information disclosure	3	5	5	H
necessity of limited reading of information assets	4	4	5	H
range of abusing of the information disclosure	4	4	5	H
possibility of occurring a damage when information exposes	5	4	4	H
necessity of audit log that records information reading	5	5	4	H
necessity of certification or biometric authentication etc, when accessing information	3	4	3	H
impact on information of institution's work performance	3	4	4	L
relevance with service provided by institutions and information	4			L
relevance with intellectual property right and privacy information				L
relevance with institution's personnel information of information				L
relevance with contingency plan of information				L
relevance with security and diplomacy of information				L
relevance with national critical infrastructure of information				L
relevance with institution's accounting and finance of information	4	4	3	L

impact on institution's financial of information	2	3		L
relevance with system development of information				L
relevance with information assets of information				L
relevance with national life of information				L
relevance with social security and social insurance of information				L
relevance with research and development of information				L
relevance with payment of taxes of information				L
relevance with environment and health of information				L
relevance with energy of information				L
relevance with immigration and transportation(aircraft, ships, etc) of information				L
relevance with international trade of information				L
relevance with disaster monitoring and forecasting of information				L
relevance with national health of information				L

4.3 무결성

허락 되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다[9]. 다시 말하면, 수신자가 정보를 수신했을 때, 또는 보관돼 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 첨삭되지 않았음을 확인할 수 있도록 하는 것이다[5].

본 연구에서는 업무영향도에 영향을 주는 무결성에 관한 측정 도구로 29개의 문항을 포함한다.

Table 3. The Results of Integrity Assessment

integrity index	CS	TS	RP	W
necessity of modulation and deletion prevention of information	4	4	4	H
necessity of audit record in accordance with the modified of information	5	5	5	H
possibility of complaint occurs according to modulation and deletion of information	5	5	5	H
range of abusing of the information discarded and modulated	4	4	4	H
reliability level of external public information	5	4	4	H
backup level of information	4	4	4	H
necessity of certification processing of information	3	4	3	H
necessity of verifying integrity of information	5	5	5	H
impact on information of institution's work performance	5	4	4	L
relevance with service provided by institutions and information	4			L
relevance with intellectual property right and privacy information				L
relevance with institution's personnel information of information				L
relevance with contingency plan of information				L
relevance with security and diplomacy of information				L
relevance with national critical infrastructure of information				L
relevance with institution's accounting and finance of information	4	4	4	L
impact on institution's financial of information	4	2	4	L
relevance with system development of information				L
relevance with information assets of information				L
relevance with national life of information				L
relevance with social security and social insurance of information				L
relevance with research and development of information				L
relevance with payment of taxes of information				L
relevance with environment and health of information				L
relevance with energy of information				L

relevance with immigration and transportation(aircraft, ships, etc) of information				L
relevance with international trade of information				L
relevance with disaster monitoring and forecasting of information				L
relevance with national health of information				L

4.4 가용성

허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것이다[9]. 최근에 네트워크의 고도화로 대중에 많이 알려진 서비스 거부 공격(DoS 공격, Denial of Service Attack)이 이러한 가용성을 해치는 공격이다[5].

본 연구에서는 업무영향도에 영향을 주는 가용성에 관한 측정 도구로 29개의 문항을 포함한다.

Table 4. The Results of Availability

Availability Index	CS	TS	RP	W
necessity of access and using information constantly	3	3	3	H
unique business continuity support of information	3	4	4	H
range of using information asset	5	3	3	H
range of abusing of the information access interference or using information	4	4	4	H
necessity of duplexing for access to information	5	4	5	H
in the event of a disaster, first of recovery	3	2	3	H
possibility of civil complaint in accordance with interference in access to information and using	2	2	4	H
level of necessity to backup of information	4	4	4	H
impact on information of institution's work performance	3	4	4	L
relevance with service provided by institutions and information	4			L
relevance with intellectual property right and privacy information				L
relevance with institution's personnel information of information				L
relevance with contingency plan of information				L
relevance with security and diplomacy of information				L
relevance with national critical infrastructure of information				L
relevance with institution's accounting and finance of information	4	4	4	L
impact on institution's financial of information	4	4	4	L
relevance with system development of information				L
relevance with information assets of information				L
relevance with national life of information				L
relevance with social security and social insurance of information				L
relevance with research and development of information				L
relevance with payment of taxes of information				L
relevance with environment and health of information				L
relevance with energy of information				L
relevance with immigration and transportation(aircraft, ships, etc) of information				L
relevance with international trade of information				L
relevance with disaster monitoring and forecasting of information				L
relevance with national health of information				L

4.5 설문 결과

각 속성별로 나타난 측정치의 평균값과 가중평균값, 업무영향도를 정리하면 Table 5와 같다.

Table 5. The Results of Questionnaires

presnt condition of sales	confidentiality	integrity	availability
average	3.67	4.33	3.67
weighted average	3.79	4.36	3.54
importance	H	H	H
business impact	H		

total sales	confidentiality	integrity	availability
average	4.09	4.09	3.45
weighted average	4.19	4.26	3.36
importance	H	H	M
business impact	H		

rental pricing	confidentiality	integrity	availability
average	4.18	4.18	3.82
weighted average	4.3	4.22	3.84
importance	H	H	H
business impact	H		

Table 1의 값과 비교하였을 때, 대동소이한 값이라고 볼 수 있다. 다시 말해, 업무 담당자와 정보보안 담당자가 생각하는 업무영향도가 설문 결과 값과 유사하게 도출되는 것으로 보아 어느 정도 신뢰성이 있다고 볼 수 있다.

V. 결 론

본 연구는 국가기관 및 공공기관, 민관기간을 대상으로 정보보안 관리실태 평가체계의 선진화를 목표로 하며, 업무영향도 평가로 정보보안 평가체계 및 평가지표의 신뢰성 향상을 통해 정보보안 관리실태 평가가 정보보안 거버넌스의 핵심적인 역할을 수행할 것이라고 본다.

본 연구는 정보보안 관리실태 체계 및 지표는 국가 및 공공기관의 정보보안 활동 강화를 위한 일상적인 가이드라인으로 활용할 수 있다.

학문적 의의로는 정보보안 관리체계 개념의 이론적 기반에 대한 학계의 논의를 촉발시키며, 그 과정에서 위험관리 개념에 대한 복합적 이해, 컴플라이언스 및 거버넌스의 새로운 이론적 명제들을 제시하게 될 것이다.

앞으로 나아갈 방향으로, 먼저 본 연구에서 업무영향도를 중심으로 측정하여 중요도를 등급별로 나누었다. 도출된 측정 결과를 토대로 재난·재해 발생에 대비하는 일련의 과정의 연구가 필요하다.

재난 발생으로 인한 정보시스템이 중단되는 경우, 발생할 영향과 손실을 측정하여 정보시스템이 업무에 미치는 영향을 정의하고, 정보시스템 복구 수준과 복구 우선순위를 설정하여, 재난 시 정보시스템을 우선순위에 따라 복구함으로 효과적으로 재난에 대처할 프로세스에 대한 연구가 필요하다.

References

〔1〕 National Cyber Security Center, National Cyber Security Manual, Jan. 2012.

〔2〕 National Cyber Security Center, The Explanation of Information Security Management Evaluation(Public Institution), pp. 3-7, 2013

〔3〕 National Cyber Security Center, The Explanation of Information Security Management Evaluation(National Institution), pp. 3-7, 2013

〔4〕 Youn, O.J., "The Methodology of Information Asset", M.S, Konkuk University, Aug. 2013.

〔5〕 Choi, M.G., Management of Internet Enterprise, iumbooks, 5112p, 2013

〔6〕 KISA, The Development of Information Security Managment Systems, pp. 8-24, Jun. 2009

〔7〕 KISA, The Method and the Criteria in Information Security Management, pp. 94-147, Sep. 2010

〔8〕 KISA, The Guide of Information Security Grade, 2010.3

〔9〕 http://vlex.com/vid/sec-definitions-19256373

〈저 자 소 개〉

최 명 길(Myeonggil Choi) 종신회원
1993년 2월: 부산대학교 경영학과 학사
2004년 8월: 한국과학기술원 박사
1995년 9월 ~ 2000년 1월: 국방과학기술연구소(ADD) 연구원
2000년 2월 ~ 2005년 8월: 한국전자통신연구원 (ETRI) 부설연구소 선임연구원
2005년 9월 ~ 2005년 2월: 인제대학교 시스템경영학과 교수
2008년 3월~현재: 중앙대학교 경영학과 교수
〈관심분야〉 정보보안관리, 정보보안시스템평가, 암호정책, CMVP

조 강 래(Kang-rae Cho) 학생회원
2012년 8월: 중앙대학교 경영학과 학사졸업
2013년 9월~현재: 중앙대학교 경영학과 MIS 전공 석사재학
〈관심분야〉 경영정보시스템, 정보보호, 정보보안