Journal of The Korea Society of Computer and Information
Vol. 22 No. 2, pp. 51-57, February 2017

www.ksci.re.kr
https://doi.org/10.9708/jksci.2017.22.02.051

A Study on Selection of Core Services for Deciding ISMS Scope

Hyunsik Kang*, Jungduk Kim**

Abstract

The first thing to be prioritized is to set the scope of the management system when establishing an information security management system for systematic and effective information security management. It is important to set the scope for an organization's information security goals due to the scope affects the organization's overall information security activities. If the scope is set incorrectly, it might become impossible to protect important services and therefore, the scope of the management system should be determined in consideration of the core business services of the organization. We propose a core service selection model based on the organization's mission-critical service and high risk service in order to determine the effective information security management system scope in this paper. Core service selection criteria include the type of service, contribution to sales, socio-economic impact, and linkage with other services

▸ Keyword : The Scope of ISMS, Information Security Task, Core services, Mission-critical Service, High risk service

I. Introduction

정보화의 급속한 발달과 함께 7.7 DDoS, 3.20 대란과 같은 사이버위협이 증가하고, 기업의 크고 작은 정보침해 사고가 연이어 발생함에 따라 정보보호의 중요성이 부각되고 있다. 이에 따라 공공 기관 및 민간 기업에서는 정보보호 수준향상을 위해 다양한 노력을 하고 있다. 국내에서는 2002년부터 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법)에 따라 정보보호 관리체계 인증 제도를 도입하여 시행하고 있다. 정보보호 관리체계 인증 제도는 기업이 다양한 보안위협으로부터 정보자산을 보호하기 위해 수립·관리·운영하는 제도로서, 정보보호 관리체계 구축을 통한 정보보호 수준의 지속적인 개선을 목적으로 한다[1].

정보보호 관리체계를 수립 시, 체계적이고 효율적인 정보보호 관리를 위하여 가장 먼저 선행되어야 할 과제는 관리체계의 범위를 결정하는 것이다. 정보보호 관리체계의 범위는 정보자산의 식별, 위험평가, 대책 선정 등 주요 정보보호 활동뿐만 아니라 정보보호 활동 전반에 영향을 미치게 때문에 조직의 정보보호 목표에 맞게 범위를 설정하는 것은 매우 중요하다. 자칫 범위를 잘못 설정하면 중요한 서비스를 보호하지 못하게 될 수 있으므로 조직의 핵심업무서비스를 고려하여 관리체계 범위를 결정하여야 한다[2]. 즉 조직 내·외적 환경에 중대한 영향을 미치는 핵심업무서비스를 식별하고, 이를 정보보호 관리체계 범위에 포함하는 것이 체계적이고 효율적인 정보보호 관리를 위한 최우선 과제라고 볼 수 있다.

따라서 본 논문에서는 보안 관점에서 핵심업무서비스를 정의하고, 정보보호 관리 범위를 결정 할 때 요구되는 사항에 대한 조사·분석을 통하여, 정보보호 관리 범위 결정을 위한 핵심업무서비스 선정모델을 도출하고자 하였다. 본 논문에서 제시하는 핵심업무서비스 선정모델은 포커스 그룹 인터뷰를 실시하여, 모델에 대한 적절성과 타당성을 검토하고, 각 선정기준에 대한 우선순위를 도출하였다.

• First Author: Hyunsik Kang, Corresponding Author: Jungduk Kim
*Hyunsik Kang(hskang8911@gmail.com), Dept. of Security Convergence, Chung-Ang University
**Jungduk Kim(jdkimsac@cau.ac.kr), Dept. of Industrial Security, Chung-Ang University
• Received: 2016. 12. 27, Revised: 2017. 01. 04, Accepted: 2017. 01. 31.
• This research was supported by the Chung-Ang University Graduate Research Scholarship in 2015

II. Preliminaries

1. Information security management scope requirements

정보보호 관리 범위 결정 시 가장 요구되는 사항은 조직의 정보보호 목적과 부합되는 범위를 결정하였는지 살펴보는 것이다. 범위를 잘못 설정하면 자칫 조직에 있어 중요한 서비스와 이와 관련된 핵심 자산들을 보호하지 못하게 될 수도 있기 때문이다[2].

ISO/IEC 27001(2013)에서는 정보보호 관리 범위를 결정할 때 조직의 내·외부 환경에 대한 이슈를 고려하여야 한다고 명시하였다. 또한 조직의 내·외부 이해당사자와 이들의 요구사항이 범위 결정 시 반영되어야 한다고 강조하였다. 즉 조직은 환경분석을 통해 정보보호가 필요한 범위(서비스)를 정보보호 관리범위로 선정하여야 한다[3]. 국내 정보보호 관리체계 인증제도(2013)에서도 조직에 미치는 영향을 고려하여 조직의 중요한 업무와 서비스가 정보보호 관리체계 범위에 포함되어야 한다고 강조한다. 따라서 조직에서 가장 먼저 선행되어야 할 과제는 조직의 핵심서비스가 무엇인지 식별하는 것이며, 그 후 핵심서비스와 관련된 조직, 정보시스템, 정보 등 유·무형의 자산을 고려하여 정보보호 관리체계를 수립하여야 한다[1].

ISO/IEC 27003(2010)에서는 효과적인 정보보호 관리체계를 구축하기 위해서는 먼저 조직의 핵심 업무서비스를 파악하여야 한다고 명시하고 있다. 핵심 업무서비스가 식별되면, 핵심업무서비스를 관리적, 물리적, 기술적 관점에서 관리체계의 범위로 결정하여야 한다고 강조한다. 즉 조직의 핵심업무서비스가 무엇인지 조직원 간에 합의가 선행되고, 이후 서비스를 기준으로 다각적인 관점에서 어떠한 정보보호 대책이 가능한지 논의되어야 한다[4]. 한국정보통신기술협회(2010)의 '정보보호관리체계 범위 설정 가이드'에서는 일반적으로 정보보호 관리체계 범위는 조직 전사를 대상으로 수립하는 것이 바람직하나, 전사를 대상으로 범위를 정하는 것이 불가능할 경우, 조직 내·외부 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호 관리체계의 범위를 설정해야 한다고 명시하고 있다. 따라서 범위 결정 시 핵심 업무서비스를 기본으로 하여 범위를 정의하여야 하며, 해당 서비스의 관련 요소를 조직적 측면, 기술적 측면, 물리적 측면에서 검토하여야 한다[2].

Ray Bernard(2007)는 정보보호 관리 범위를 잘못 설정할 시 발생될 수 있는 보안위험에 대하여 설명하며, 핵심 업무서비스를 범위에 포함하고 다각적인 측면에서 이를 검토할 것을 강조하였다. 예를 들어 매출이 가장 높은 판매지점의 물리적 보안장치가 부실해서 경쟁회사 직원이 침입해 중요한 판매정보를 유출할 위험이 있다[5]. 이는 매출이 가장 높은 서비스가 관리범위에 포함되지 않았을 뿐만 아니라, 해당 서비스에 대한 물리적 측면의 보안 활동이 고려되지 않았기 때문에 발생되는 위험으로 판단할 수 있다.

정보보호 관리 범위 설정 시 요구되는 사항에 대한 선행연구를 정리하자면, 대다수의 선행연구에서 체계적이고 효율적인 정보보호 관리 활동을 위해 조직의 핵심업무서비스를 범위 내에 반드시 포함할 것을 강조하고 있다. 따라서 조직의 핵심업무서비스를 파악하는 것이 선행되어야 하며, 수많은 업무서비스 중 무엇이 관리 범위에 포함되어야 하는 업무서비스인지 판단할 수 있는 기준에 대하여 살펴볼 필요가 있다.

즉 조직 내·외적 환경에 중대한 영향을 미칠 수 있는 핵심업무서비스가 무엇인지 판단할 수 있는 기준을 살펴보고, 기준에 근거한 핵심업무서비스를 관리 범위 내에 포함하는 것이 필요하다.

2. Core service

상기 '2.1 정보보호 관리 범위 설정요구사항'에서 언급하였듯이 체계적이고 효율적인 정보보호 관리 활동을 위하여, 사전에 조직의 핵심업무서비스에 대한 판단 기준을 마련하고, 정보보호 관리 범위에 포함할 핵심업무서비스를 정의하는 것이 필요하다.

일반적으로 핵심업무서비스란 조직의 근본적인 미션(임무)와 가장 근접한 업무서비스를 의미한다. 이주경(2013)은 핵심업무서비스를 조직의 미션(목적)과의 관련성, 수익공헌도, 장래성을 기준으로 하여, 각 요소가 커질 수록 핵심업무서비스에 근접한 것으로 정의하였으며, Handa Junichi(2005)는 각 서비스의 매출에 기여하는 정도와 기간을 기준으로 핵심업무서비스를 분류하였다. 한편 양지향, 최금옥(2011)은 조직의 업무서비스를 핵심서비스와 보조서비스로 분류하여, 핵심서비스는 조직의 미션을 달성하기 위하여 고객의 본질적인 욕구충족 만족을 위한 서비스로 정의하였으며 보조서비스는 핵심서비스를 가능하게 하거나 그 가치를 확장시키는 서비스로 정의하였다. 즉 핵심업무서비스는 조직의 존재 이유이자 주 수입원이 되는 중심 업무 분야로 정의할 수 있을 것이다.

정보보호 관점에서 핵심업무서비스의 정의는 정보보호 손실에 따른 피해규모를 고려하여야 할 것이다. 실제 침해사고 발생 시 재무적·비재무적 피해손실이 클 것으로 예상되는 서비스가 우선적으로 보호되어야 하기 때문이다. FIPS 199(2004)에서는 정보보호 손실에 따른 피해규모를 기반으로 서비스의 정보보호 영향도를 평가하고, 이를 기준으로 핵심서비스인지 판단한다. 정보보호 영향도를 평가할 때는 보안 요구사항인 기밀성, 무결성, 가용성의 개념을 반영한다[9]. 즉 핵심업무서비스 선정 시 보안 요구사항인 기밀성, 무결성, 가용성의 개념을 반영하여 [10], 높은 보안 수준이 요구되는 고위험 서비스인지 식별할 필요가 있다.

정보통신기반보호법(2015)에서는 해킹·악성프로그램 유포 등 각종 전자적 침해행위로부터 정보통신기반시설을 보호하기 위해, 주요정보통신기반시설의 지정하고 있다. 주요정보통신기반시설을 지정할 때는 보안 관점에서 국가사회적 영향도, 정보

통신기반시설에 대한 의존도, 타 기반시설과의 상호연계성, 침해사고 발생 피해규모, 복구 용이성을 기준으로 한다[11]. 주요정보통신기반시설 지정 기준을 살펴보면 침해행위 발생 시 사회·경제적으로 중대한 영향을 미칠 수 있는 고위험의 정보통신시설을 반드시 보호되어야 할 대상으로 판단하여 지정한 것으로 해석할 수 있다. 김낙현, 맹두열(2014)의 연구는 보호해야 할 대상의 우선순위를 선정하기 위한 정보보호 중요도 산정 기준을 제시하였다. 선정 기준은 처리정보의 민감도, 타 시스템 연계 수, 정부의 정책으로 구성되어있으며, 국가·사회적으로 얼마나 중대한 영향을 미치는가를 기준으로 서비스의 정보보호 중요도 평가하여 보호 수준을 결정한다[12]. 즉 정보보호 관점에서 핵심업무 서비스는 침해사고 발생 시 사회·경제적으로 중대한 영향을 미칠 수 있는 고위험의 서비스로 정의할 수 있을 것이다.

상기 선행연구를 요약하자면 하기 표와 같이 비즈니스와 정보보호 측면으로 분류하여 핵심업무서비스를 정의할 수 있다. 즉 핵심업무서비스란 조직의 임무를 달성하기 위하여 반드시 필요한 업무이며 동시에 높은 위험을 가지는 서비스로 정의할 수 있다. 그러나 일반적으로 정보보호 관리 범위 설정을 위해 핵심업무서비스를 식별 할 때, 비즈니스 측면은 간과하고 정보보호 측면만을 강조하는 경향이 있다. 이럴 경우, 중요한 업무서비스임에도 보호 대상에서 제외될 수 있기 때문에 전사적인 관점에서 비즈니스 측면과 보안 측면을 모두 고려하여 핵심업무서비스를 선정하는 것이 필요하다.

Table 1. A summary of core service definition

perspective	Contents	Reference
Business perspective	The organization's most mission critical service - Criteria: Relation to missions, Profitability and Prospect	J. K. Lee(2013); Handa junichi(2004); J. H. Yang et al.(2011);
security perspective	- High risk service requiring high security level - Criteria: Confidentiality, Integrity and Availability	NIST(2004); Ministry of Science(2015); N. H. Kim et al. (2014);

III. The Proposed Scheme

정보보호 관리 범위 설정 시 핵심업무서비스 선정이 중요한 이유는 범위 설정이 보안성과에 영향을 줄 수 있기 때문이다. 정보보호 관리체계의 범위는 정보자산의 식별, 위험평가, 대책선정 등 정보보호 활동 전반에 영향을 미치므로 조직의 정보보호 목표에 맞게 범위를 설정하는 것은 매우 중요하다.

본 논문에서는 효율적인 정보보호 활동을 위하여 보안 관점에서 Fig. 1.과 같이 핵심업무서비스 선정 모델을 제안하였다. 제시하는 모델은 관련 연구를 통해, 전사적인 관점에서 핵심업무서비스를 조직의 임무를 달성하기 위해 필요한 업무(mission-critical service)와 높은 위험을 가지는 서비스(high risk service)로 분류하여, 이에 따라 고려되어야 할 선정 기준을 제시하였다.

핵심업무서비스는 첫째, 먼저 해당 조직의 미션(목적)을 달성하기 위해 반드시 필요한 업무인지, 또는 핵심 서비스를 가능하게 하거나 그 가치를 확장시키는 보조적인 서비스인지, 해당 서비스의 유형을 분류할 필요가 있다[8]. 또한 해당 업무서비스의 수익 창출여부와 매출 기여도를 기반으로 핵심업무서비스의 우선순위를 분류할 수 있다[7]. 둘째, 사회·경제적으로 중대한 영향을 미치는 고위험의 서비스인지 판단한다. 판단하는데 있어 정보보호의 세가지 요소인 기밀성, 무결성, 가용성이 적절히 고려될 수 있도록 하여야 한다. 먼저 정보화 의존도가 증가함에 따라 침해사고 등 역기능 발생 시 사회·경제적인 파급력이 매우 광범위하게 영향을 미치고, 이는 조직에 재무적·비재무적인 손실을 가져다 줄 수 있으므로[11], 사회·경제적인 영향도를 고려하여 핵심업무서비스가 고위험 서비스인지 판단해야 한다. 또한 타 업무와의 연계성이 핵심업무서비스로 판단되기 위해 고려되어야 한다. 이는 연계도가 높을수록 위험 노출도가 증가하며, 다른 범위로 위험이 확장될 가능성이 높기 때문이다[12].

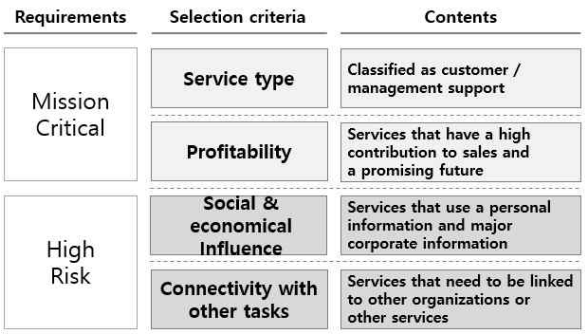

Fig. 1. The Selection model of Core Service

핵심업무서비스를 선정하기 위한 기준은 4가지로 구성하였다. 첫째, 고객을 대상으로 하는 서비스인지, 업무 효율 증대 목적의 경영지원 시스템인지 서비스의 유형을 구분하여야 한다. 대고객 서비스는 고객과 직접적인 접점으로, 업무지원 서비스 등 타 서비스 유형에 비해 조직의 임무 달성을 위한 가장 근원적인 서비스이다[6]. 또한 일반적으로 개방된 인터넷 환경에서 수행되는 경우가 많아 보안 위협에 노출될 가능성이 클 것으로 판단된다. 즉 대고객 서비스는 타 서비스 유형과 비교하여 침해사고 발생 가능성이 높을 수 있으며, 고객과 직접적으로 연계되기 때문에 침해 사고 발생 시 조직에 중대한 손실을 미칠 가능

성이 클 것으로 판단된다. 따라서 핵심업무서비스 선정 시에는 먼저 해당 서비스 유형이 대고객 서비스인지 아닌지 구별하여야 할 것이다. 최근 국내 정보보호 관리체계 인증제도에서도 의무 인증 대상자에 한하여 대외 서비스를 관리체계 범위로 지정하도록 의무화하는 등 대고객 서비스에 대한 정보보호 활동을 강조하고 있다[1].

둘째, 핵심 업무서비스 선정 시에는 단순 서비스 업무가 아닌 금전거래가 발생하는 업무가 우선되어야 한다[7]. 영리/비영리를 막론하고 매출이나 금전거래가 발생하는 서비스는 조직의 중심이 되는 업무 분야로 판단할 수 있기 때문이다. 더불어 금전거래가 발생하는 업무가 보안사고로 중단될 경우에는 직접적인 재무적 손실이 발생할 가능성이 크다.

셋째, 서비스의 기밀성, 무결성, 가용성을 고려하여 해당 서비스의 사회·경제적인 영향도가 측정되어야 한다. 사회·경제적 영향도가 높을수록 보안사고 발생 시 재무적·비재무적 손실규모가 크다고 판단할 수 있다. 특히 해당 업무서비스가 업무를 진행하거나 서비스를 제공함에 있어 개인정보를 활용하는지 파악하여야 한다. 개인정보 유출사고는 타 정보보호사고 보다 미치는 영향이 크고[13], 법적 요구사항도 충족해야하기 때문이다.

마지막으로 핵심 업무서비스 선정 시에는 타 업무와의 연계성이 고려되어야 한다. 타 기관이나 내부적으로 다른 서비스와의 연계도가 높을수록 그만큼 위험에 노출될 확률이 증가하며, 또한 다른 업무서비스로 위험이 확장될 가능성이 높기 때문이다[14]. 예를 들어 기업을 소개하는 홈페이지 자체는 중요도가 매우 낮다고 볼 수 있으나, 해당 홈페이지의 DB 서버를 중요한 업무서비스와 공유한다면 중요도가 낮다고 판단할 수는 없을 것이다.

IV. Focus Group Review

1. Research design and method

현재 정보보호 관리 범위 설정 관련 연구가 미흡하고 정보보호관점의 핵심업무서비스 식별과 관련된 데이터가 부족한 실정이므로 본 연구에서 제시한 모델의 타당성과 신뢰성을 객관적으로 검토하는 것은 어려운 문제이다. 이에 따라 본 논문에서는 보안을 위한 핵심업무서비스 선정모델을 검토하기 위하여 포커스 그룹을 대상으로 설문과 심층인터뷰를 수행하였다. 포커스 그룹 인터뷰는 전문가들의 집단 토의, 정보 교환 등의 과정을 통해 설문지보다 훨씬 다양한 범위의 의견들을 수렴할 수 있으며, 문헌연구에서 얻을 수 없는 심층적인 정보를 습득할 수 있다[15].

포커스 그룹의 수는 2~3개의 그룹과 5~10명의 인원 수로 이론적 포화상태에 도달할 수 있으며[16], 해당 선행연구를 근거로 하여 본 연구에서는 각 5명씩, 2개의 그룹으로 분할하여 그룹을 구성하였다. 각 그룹에는 중견기업의 CEO 1명과 제조업, IT기업 등의 CIO 1명, CISO 2명 및 정보보호 분야의 교수 1명으로 총 10명의 정보보호 전문가들로 구성하여 설문과 심층 인터뷰를 수행하였다.

2. Data collection and analysis

자료 수집을 위해, 참여자들에게 연구 목적을 설명하고 연구 참여에 동의한 자에 한하여 연구를 진행하였으며 자료 수집 기간은 2016년 5월부터 2016년 7월까지이다. 원활한 인터뷰 진행을 위하여, 아래 Table. 2.와 같이 Krueger & Casey(2000)가 제시한 질문방식을 활용하여 도입질문, 핵심질문, 마무리 질문의 3가지 종류로 인터뷰를 구성 하였다. 인터뷰 진행 시 핵심업무서비스 선정 기준의 중요도와 실현가능성에 대한 설문을 진행하였고, 설문 종료 후 1시간에 걸쳐 참여자들 간 의견을 교환하고 추가적인 검토사항에 대해 토론하였다. 자연스러운 진행을 위하여 질문의 순서를 바꾸거나, 활발한 토의가 일어나지 못할 때는 보조 질문을 하여 토의 진행을 유도하였다.

Table 2. Questionnaire format

<table>
<tr><th colspan="2">Question</th><th colspan="5">Question Contents</th></tr>
<tr><td colspan="2">Opening question</td><td colspan="5">Let's have a time to introduce myself.</td></tr>
<tr><td rowspan="5">Key Question</td><td rowspan="4">Survey</td><td colspan="5">1. Would you like to respond to the importance of selection criteria in determining the core services. Please evaluate the importance in terms of security importance, urgency and improvement effect.</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td colspan="5">2. Would you like to respond to the feasibility of selection criteria in determining the core services. Please evaluate the feasibility in terms of institutional ease, ease of implementation, and manageability.</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td>Open questions</td><td colspan="5">3. Do you think it is important to select core service in determining the scope of ISMS for efficient information protection activities?
4. Why do you think the selection criteria are difficult to implement in practice?</td></tr>
<tr><td colspan="2">Ending question</td><td colspan="5">I have discussed the selection criteria of core service. Do you have any additional comments?</td></tr>
</table>

수집된 자료에 대한 분석은 경영정보 분야에서 일반적으로 사용되는 평가 방법 및 우선순위 결정 기준을 참고하였다. 핵심업무서비스 선정 기준의 적용은 결국 조직의 목표달성을 위해 필요한 선정 기준 중 가장 우선순위가 높은 선정 기준이 적용되기 때문에 본 논문에서 도출된 선정 기준을 검토하기에 적합

하다고 판단하였다.

우선 Cabrera(2008)의 연구에서는 우선적으로 해결해야 하는 문제와 이런 문제를 효과적으로 해결하기 위한 방법들을 식별하고, 중요도(Importance)와 실현가능성(Feasibility)을 5점 척도를 이용해 우선순위를 결정하였다. 지식경제부(2012)에서는 정보화 전략계획 수립에 필요한 이행과제의 우선순위를 중요도와 실현가능성을 기준으로 5점 척도를 이용해 평가하였다. 중요성을 평가하기 위한 세부평가항목으로 정책적 중요도, 시급성, 개선효과를 제시하였으며, 실현가능성을 평가하기 위하여 세부평가항목으로 제도적 용이성, 구현 용이성, 관리용이성을 제시하였다.

본 연구에서는 연구 내용이 유사한 Carvrera(2008)의 연구에 따라 모델의 적절성을 판단하였다. 선정 기준의 중요성과 실현가능성을 측정하기 위해 리커드 5점 척도를 사용하였으며, 세부평가항목으로 지식경제부(2012)에서 제시한 내용을 활용하였다. 중요성과 실현가능성 모두 3.0 이하인 선정 기준은 기각하였고, 중요성은 높지만 실현가능성이 낮은 경우와 실현가능성은 높으나 중요성이 낮은 경우 포커스 그룹의 의견을 수렴하여 채택 및 기각 여부를 판단하였다[16].

3. Review results

포커스 그룹 인터뷰 결과, 본 연구에서 제시하는 선정 기준은 Table. 3.과 같이 모두 채택되었다. 또한 중요성과 실현가능성의 평균값을 기준으로 우선순위를 도출한 결과, 서비스 유형, 사회·경제적 영향도, 타 업무와의 연계성, 매출 기여도 순으로 우선해야할 기준으로 나타났다.

Table. 3. Focus Group Interview Results

Selection criteria	Importance	Feasibility	Priority
Service type	4.1	4.8	1
Social&economical Influence	4.7	2.8	2
Connectivity with other tasks	4.3	3.2	3
Profitability	3.2	4.0	4

먼저, 정보보호 관리 범위를 결정할 때 정보시스템이나 물리적인 위치 등이 아니라, 서비스를 기준으로 범위가 설정되어야 한다는 것은 모든 참여자들이 동의하였다.

"네트워크를 통해 상호 연결되어 있는 정보시스템을 기준으로 범위를 설정하는 것은 적절하지 못하다. 전자금융기반시설의 경우도 초기에는 인터넷뱅킹 등 직접적으로 전자금융거래를 제공하는 시스템으로 국한을 하였으나 현재 전자금융거래를 제공하는 서비스와 연동된 모든 시스템, 관련 외부업체까지 대상범위를 확대한 바가 있다." 그룹 1 인터뷰 中

기존 정보보호 관리 범위 설정의 경우, 일반적으로 정보시스템을 기준으로 설정되었기 때문에 연계되는 시스템과 조직이 범위에 누락되는 경우가 발생하였다. 따라서 서비스를 기준으로 하여, 서비스와 관련된 조직, 시스템, 물리적 위치 등 다각적인 관점에서 범위가 설정되어야 한다는 의견에 대다수의 참여자가 동의하였다.

서비스 유형(대고객 서비스)의 경우, 중요성과 실현가능성이 모두 높은 수준으로 나타나 선정 기준으로 채택되었다. 중요도가 높게 평가된 이유는 서비스 유형에 따라 조직 임무와의 연관성을 확인할 수 있고, 침해사고 발생 인한 영향도가 크게 다르기 때문으로 토의되었다. 이는 타 서비스 유형보다 대고객 서비스가 조직 임무 달성과 직접적인 관계를 가지고 있으며, 또한 침해사고 발생으로 우려되는 영향도가 높기 때문으로 해석할 수 있다. 또한 서비스 유형의 실현가능성은 각 서비스가 대고객 서비스인지, 그 외 서비스인지 유형을 판단하기 용이하여 높은 평가된 것으로 토의되었다. 한편 서비스 유형과 함께 서비스를 사용하는 이용자 수가 세부적인 평가 기준으로 포함되어야 한다는 의견이 제시되었으며, 향후 이용자 수와 침해사고 시 미치는 영향 간 관련성을 고려하여 세부적인 기준이 마련되어야 할 것을 시사하였다.

"서비스 이용자 수가 침해사고 발생 시 미치는 범위에 영향을 줄 수 있기 때문에 세부적인 평가기준으로 서비스 이용자 수를 고려하여야 한다." 그룹 1 인터뷰 中

사회·경제적 영향도는 타 선정 기준과 비교하여 중요도가 가장 높은 것으로 나타난다. 이는 핵심업무서비스 선정 시 정보보호 영향도가 핵심적인 항목임을 확인할 수 있는 결과이다. 반면 실현가능성은 2.8로 가장 낮게 평가되었다. 따라서 포커스 그룹의 의견을 수렴하여 채택/기각 여부를 결정하였으며 의논 결과, 사회·경제적 영향도의 중요성을 고려하여 선정 기준으로 채택되었다. 토론 결과, 서비스의 사회·경제적 영향도를 정량적으로 평가하기 어려워 실현가능성이 낮다는 의견이 다수 제시되었다. 먼저 서비스에서 처리되는 정보의 중요도를 기준으로 사회·경제적인 영향도를 판단할 수 있다는 것에는 대다수가 동의하였다. 다만 처리되는 개인정보의 양과 개인정보의 유형(민감정보, 바이오정보 등) 또는 중요정보 등급(1등급, 2등급, 대외비 등) 등을 활용하여 정량적으로 사회·경제적 영향도를 평가할 수 있는 추가적인 세부 기준이 마련되어야 실효성이 있을 것이라는 의견이 제시되었다.

"침해사고 발생 시 우려되는 영향은 해당 서비스의 위험수준을 평가할 수 있는 중요한 기준이다. 재무적, 사회적으로 미치는 영향이 크다면 타 서비스에 비해 보안 수준을 강화하여야 한다." 그룹 2 인터뷰 中

"보안 활동의 가치를 정량적으로 환산하는 것과 마찬가지로, 침해사고 발생 시 미치는 영향을 정량적으로 표현하는 것은 어

려운 문제이다. 따라서 처리되는 정보를 기준으로 정량적으로 서비스의 중요도를 평가할 수 있는 기준이 마련되어야 실효성이 있을 것으로 판단할 수 있다." 그룹 2 인터뷰 中

타 업무와의 연계성은 중요성에 비해 상대적으로 실현가능성이 낮게 측정되었으며, 평균 3.0 이상으로 선정 기준으로 채택되었다. 토의 결과, 중요성의 경우 침해사고 발생 시 연계될 수 있는 위험을 고려하여 높게 측정된 것으로 논의되었다. 반면 실현가능성의 경우 정보화의 고도화에 따라 업무 간 연계성을 파악하기 어렵기 때문에 상대적으로 낮게 나타난 것으로 해석된다. 따라서 향후 실현 가능성 제고에 기여할 수 있는 추가적인 연구가 필요함을 시사하였다.

매출 기여도의 경우, 타 선정 기준과 비교하여 중요도가 가장 낮은 것으로 나타났으나, 평균 3.0 이상으로 선정 기준으로 채택되었다. 토의 결과, 매출 기여도는 비즈니스 관점에서 매우 중요한 선정 기준이지만 보안 관점에서 핵심업무서비스의 선정 기준으로서 타 선정 기준보다 뚜렷한 관련성이 없어 중요성이 낮게 평가된 것으로 논의되었다. 이는 매출 기여도를 기준으로 사회적 영향도를 측정하기에는 한계가 존재하기 때문으로 해석된다. 하지만 매출이 높은 업무서비스가 중단될 경우 미칠 수 있는 재무적 손실을 고려하여 선정 기준에 포함되어야 한다는 의견이 다수 제시되었다

"어떤 서비스가 기업에 금전적인 이익을 얼마나 가져다주느냐는 비즈니스 관점에서 매우 중요한 기준이다. 하지만 매출이 높다고 해서, 침해사고 발생 시 사회적인 영향이 큰 것은 아니기 때문에 다른 선정 기준보다 중요성이 낮다고 생각된다." 그룹 2 인터뷰 中

"매출 비중이 큰 서비스일수록 업무 수행에 장애가 미치는 시간에 따라 기업에 미치는 재무적인 손실은 막대하기 때문에 재무적인 선정 기준이 고려되어야 한다." 그룹 1 인터뷰 中

V. Conclusions

체계적이고 효율적인 정보보호 활동을 위해서는 조직의 핵심업무서비스가 반드시 정보보호 관리 범위에 포함되어야 할 것이다. 본 연구에서는 전사적인 관점에서 핵심업무서비스를 정의하고, 이를 기반으로 핵심업무서비스 선정모델을 제시하였으며 다음과 같은 의의를 가진다. 첫째, 정보보호 관리 범위설정에 대한 이론적인 방법론을 제공할 수 있다. 둘째, 보안관점에서 핵심 서비스에 대한 선행연구는 비교적 활발히 진행되어 왔으나 비즈니스측면을 포함한 전사적인 관점에서의 핵심업무서비스에 관한 연구는 다소 부족하다고 판단되기 때문에 전사적인 관점에서 핵심업무서비스 선정에 관한 기초 연구로서 사용될 수 있다. 셋째, 정보보호 활동 범위설정은 정보보호 관리체계 수립 시 가장 선행되어야 할 과A Study on applicability of Mixed-methodology제로, 향후 이에 대한 근간이 되는 자료를 제공할 수 있다. 한 편 본 연구는 정보보호 전문가를 대상으로 핵심서비스 선정모델에 대한 적합성과 실현가능성을 검토하였으나, 특성 상 일반화가 다소 어렵다는 한계가 있다. 따라서 향후 연구에서는 사례연구, 실증연구 등을 통하여 본 연구에서 제시한 선정모델을 검증할 필요할 필요가 있다.

REFERENCES

[1] KISA, "*A Guide for the Certification of Information Security Management System*", KISA, Mar 2016.

[2] Telecommunications Technology Association, "*A Guide for Establishing the Scope of Information Security Management System*", TTAK.KO, Dec 2012.

[3] ISO/IEC JTC 1/SC 27, "*ISO/IEC 27001:2013 Information security management systems Requirements*", ISO/IEC, Sep 2013.

[4] ISO/IEC JTC 1/SC 27, "*ISO/IEC 27003:2010 Information security management systems implementation guidance*", ISO/IEC, Feb 2010.

[5] Ray Bernard, "Information Lifecycle Security Risk Assessment: A tool for closing security gaps", computers & security, Vol.26, No.1, pp.26-30, Feb 2007.

[6] J. K. Lee, "Diagnosis and evaluation of non-core businesses in Public enterprise", Public institution research focus, Vol.0, No.0, pp. 113-138, Apr 2013.

[7] Handa junichi, "*Centennial company*", New proposal Publishers, Mar 2004.

[8] J. H. Yang and K. Y. Choi, "*Service, Marketing*", INITIAL COMMUNICATIONS Corp, Feb 2011.

[9] ISO/IEC JTC 1/SC 27, "*ISO/IEC 27000:2016 Information security management systems: Overview and vocabulary*", ISO/IEC, Feb 2016.

[10] NIST, "*FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems*", NIST, Feb 2004.

[11] Ministry of Science, "*ICT and Future Planning, Guidelines for Designation Criteria for Major IT Infrastructure Facilities*", Ministry of Science, Mar 2015.

[12] N. H. Kim and D. Y. Maeng, "Criteria for

calculating the importance of information security in E-government public service", Internet & security focus, Vol.3, No.0, pp.47-59, Mar 2014.

[13] J. H. Eom, M. J. Kim, "Effect of Information Security Incident on Outcome of Investment by Type of Investors: Case of Personal Information Leakage Incident", Journal of The Korea Institute of Information Security & Cryptology, Vol.26, No.2, pp.463-474, Apr 2016.

[14] J. Hue, "A Study on New Methodology for Designating Core Information Infrastructure", Internet & Security Focus, Vol.9, No.1, pp.26-35, Sep 2013.

[15] Kang, M. A., Son, J. Y. and Kim, H. J., "Exploratory research on applicability of integrated research methods: Integrated application of survey and focus group method to community opinion survey for local health policy decision", Korean Public Administration Review, Vol. 41, No.4, pp. 415-437, Dec 2007.

[16] David L. Morgan, "Focus Groups", Annual Review of Sociology, Vol.22, No.1, pp.129-152, Aug 1996.

[17] Krueger, R. A. & Casey, M. A., "*Focus Groups: A Practical Guide for Applied Research*", SAGE Publications, Oct 2008.

[18] Derek Cabrera, James T.Mandel, Jason P. Andras and Mari L. Nydam, "What is the crisis? Defining and prioritizing the world's most pressing problems", Frontiers in Ecology and the Environment, Vol.6, No.9, pp.469-475, Nov 2008.

[19] Ministry of Knowledge Economy, "*Knowledge Economy Statistics Portal Information Strategy Planning*",Ministry of Knowledge Economy, Mar 2012.

Authors

Hyunsik Kang received the B.S. degrees in Information System from Chung-Ang University, Korea, in 2015.

He is currently a Master course in the Dept. of Security Convergence, Chung-Ang University. He is interested in Organization of Information Security and Information Security Management System.

Jungduk Kim received the Ph.D. degrees in MIS from Texas A&M Univ, USA, in 1990

Dr. Kim joined the faculty of the Dept. of Information System, Chung-Ang University, Seoul, Korea, in 1995. He is currently a Professor in the Dept. of Industrial Security, Chung-Ang University. He is interested in Information Security Management System and Governance of Information Security.