Journal of KIIT. Vol. 17, No. 7, pp. 123-131, Jul. 31, 2019. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2019.17.7.123

공공기관 정보보호서비스 대가 모델의 개선 방안

오상익*, 박남제**

The Improvement of Information Protection Service Cost Model in Public Institution

Sangik Oh*, Namje Park**

이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임
(과제번호:NRF-2019R1I1A3A01062789)

요 약

본 논문에서는 기존의 관련 연구를 SW 중심의 대가 산정, 비용-편익분석, 보안성 지속서비스 대가 산정으로 구분하여 조사하였고, 사례 분석은 미국과 일본, 국내 A기관을 대상으로 하였다. 이를 바탕으로 현 제도와의 비교를 통해 개선모델을 마련하였다. 비용-효용분석 측면에서 효용성이 높은 서비스 수준 협약(SLA ; Service Level Agreement)과 NIST Cybersecurity Framework를 적용하여 정보보호서비스별 특성과 수행기준, 가중치를 기준으로 대가를 산정하는 방식인 SCS(Security Continuity Service) 성과평가체계 기반 정보보호서비스 대가 산정 모델을 제안한다. 이 모델은 공공기관에서 정보보호서비스 대가를 객관적으로 산정하는 도구로 활용할 수 있다. 또한, 현재 권고수준인 법률을 적용 강제성 수준으로 강화, 국가기관 및 공공기관의 평가제도 개선, 국가인증기관의 정보보호서비스 검증제도 도입, 모든 정보시스템 및 서비스로의 확대 등을 통해 본 제도의 정착될 수 있을 것으로 기대된다.

Abstract

In this paper, related studies were investigated by dividing them into cost-benefit analysis, security continuity services, and SW-centric calculations. The case analysis was conducted on A institutions in the United States, Japan and South Korea. Based on this, an improvement model was prepared through comparison with the current system. The SCS(Security Continuity Service) performance evaluation system-based information protection service cost calculation model is proposed. This method applies a service level agreement(SLA) and NIST Cybersecurity framework that are highly effective through cost-effectiveness analysis and calculates consideration based on characteristics, performance criteria, and weights by information protection service. This model can be used as a tool to objectively calculate the cost of information protection services at public institutions. It is also expected that this system can be established by strengthening the current recommended statutory level to the enforceability level, improving the evaluation system of state agencies and public institutions, introducing a verification system of information protection services by national certification bodies, and expanding its scope to all systems.

Keywords
cybersecurity continuity service, cost of cybersecurity service, service level agreement, NIST CSF, security

* 제주대학교 대학원 융합정보보안학과 석사과정
- ORCID ID: https://orcid.org/0000-0002-9342-6689
** 제주대학교 초등컴퓨터교육전공 교수(교신저자)
- ORCID ID: https://orcid.org/0000-0003-4434-8933

· Received: Jul. 14, 2019, Revised: Jul. 23, 2019, Accepted: Jul. 26, 2019
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

우리나라는 2000년대 초반, 인터넷 보급률 세계 1위를 차지하며 IT강국으로 전자정부로서의 국제적으로 인정을 받고 있다. 이에 보안업계에서도 전자정부 시스템의 보안 문제를 해결하는데 집중해왔다. 하지만, 국가기관이나 공공기관에서는 보안에 대한 인식 부족으로 정보보호시스템을 도입한 후 제공되는 정보보호서비스에 대한 대가를 제대로 적용받지 못하였고, 보안업계의 경쟁력을 저하시키는 요인으로 작용하고 있다. 정보보호시스템은 하드웨어와 소프트웨어, 또는 하드웨어와 소프트웨어가 결합한 일체형으로 분류되어 있는데, 그동안은 하드웨어와 소프트웨어에 대해서만 유지보수에 따른 대가를 적용받도록 정책이 되어 있어, 보안위협에 대한 지속적인 보안 서비스에 대한 적정한 대가를 제대로 인정받지 못하는 결과를 얻게 되었다. 이에, 정보보안 산업의 위축으로 인해 글로벌 시장에서의 경쟁력 우위를 점하지 못하는 요인으로 작용하고 있다.

2015년 제정·시행된 정보보호산업 진흥에 관한 법률을 통해 정보보호제품에 대하여 정보보호서비스를 지속적으로 제공하여 이에 맞는 서비스 대가를 적용받을 수 있도록 법률적 근거를 마련하였다[1].

본 논문에서는 정보보호시스템을 포함한 정보시스템에 대한 정보보호 지속 서비스 대가 모델에 대한 기존 관련 연구, 도입기관의 적용사례 분석을 통해 보안 지속 서비스 대가를 제대로 받을 수 있도록 개선된 모델을 제안하였다.

Ⅱ. 이론적 배경과 선행연구 분석

2.1 정보보호 지속 서비스

정보보호 지속 서비스라는 개념은 새로운 개념으로, 정보시스템에 대한 해킹, 신규 악성코드, 정보유출 등 내·외부의 보안 위협에 대한 사후 대응 서비스나 무결성·기밀성·가용성이 보장되어야 하는 서비스 등 정보보호 서비스의 특징을 고려하여 정보보호 활동을 서비스 항목별로 도출하여 구성하였고, 서비스 유형별로는 표 1과 같이 보안성 지속서비스, 보안관제서비스, 보안컨설팅서비스 등으로 분류하였다[1]-[3].

이를 근거로 한국인터넷진흥원(2015)의 정보보호서비스 대가 산정 가이드에 따르면 보안성 지속 서비스는 정보보호제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위한 기술 기반의 서비스로 정의하였다[2][4].

표 1. 정보보호서비스의 유형별 분류
Table 1. Categorization by type of information protection service

Level1	Level2	Classification standard
Information security consulting	Vulnerability analysis assessment	Diagnose and assess infrastructure vulnerabilities, simulate hacking
	Information security management system	ISMS, ISO/IEC27001
	Personal information protection	Accreditation consulting for ISMS-P, PIA, etc.
	Consulting	Security consulting, security audit, system development security consulting, etc.
Security continuity service	Security update	Patches for pattern updates (rules pattern and signature), IT environment changes(new OS/systems and terminals/standard, etc.)
	Security policy management	Establishing/changing security policies according to the user experience
	Threat/accident analysis	Accident response (pre/post), threat analysis report by product line, etc.
	Maintain security authentication	Maintaining various security certifications, such as CC certification, security compliance verification, and KCMVP
	Security Technical Advisory	Simulated training response, information protection education, remote response, security audit support, etc.
Security control service	Basic service	Remote control, dispatch control, hybrid control, etc
	Additional service	Additional services for security system such as planning, diagnosis, analysis, operation, and individual services
	Training service	Simulated training response

2.2 선행연구 분석

정보보호 서비스 대가에 대한 연구는 표 2와 같이 SW 중심의 대가 산정에 대한 연구와 비용-편익 분석에 따른 대가 산정 연구, 보안성 지속서비스 대가 산정에 대한 연구로 구분할 수 있다.

먼저, 박유진(2011) 등은 정보보안 제품과 유지관리 활동별 유지보수 대가 기준 방식으로 활동별 유지보수 소요횟수, 해결 소요 시간, 소요인력 등을 학습곡선을 적용, 제품별 활동별 유지보수 대가 비용을 산정하고, 보정계수를 적용하여 유지보수 대가를 산정하는 형태를 제안하였다[5]. Böhme(2010) 등은 문헌에 대한 종합적인 검토를 수행하여, 그 지출로 실현되는 정보보안의 비용과 이익 사이의 관계를 검토하였다. 위험 완화를 위한 예방적 노력에 의해 제공되는 기준 수준의 보안과 그러한 요소들을 시험하는 것을 인정하였다. 어느 시점에서는 외부 침해를 강력하게 완화하기 위해 많은 조직이 투자하려는 것보다 훨씬 더 많은 비용이 들 수 있다. 그림 1과 같이 ROSI(Return on Security Investment)를 이용하여 편익을 비용보다 적게 하고, 비용으로 나누어서 백분율로 환산하는 형태를 제안하였다[6].

조연호(2015) 등은 정보보안솔루션의 보안성 지속을 위한 서비스 현황을 분석하고, 정보보안솔루션의 특성을 고려하여 보안업데이트, 보안정책, 위협분석, 인증유지, 기술자문 등 보안성 지속 서비스를 분류하고 표 3과 같이 서비스 대가를 요율방식과 정액제를 산정하는 형태를 제안하였다[7].

한국소프트웨어산업협회와 한국정보보호산업협회(2018)는 SW사업 대가 산정 가이드를 통해 보안성 지속 서비스 대상 제품의 보안성 지속 서비스 요율 책정 기준을 서비스 활동주기를 기준으로 하여 보안 서비스 포인트(Security Services Point, SSP) 측정 방식을 표 4와 같이 제시하였다[8].

표 4의 측정기준을 근거로 제품별로 보안성 지속 서비스 항목별 배점을 합산한 SSP를 표 5와 같이 적용한 요율을 적용할 수 있도록 제시하였다.

표 3. 보안성 지속 서비스 대가 산정방식
Table 3. Method of estimating the cost of security continuity service

Div.	Method
Rates system	Purchase price * Rate
Fixed charge system	License cost (Including security sustainable service cost)

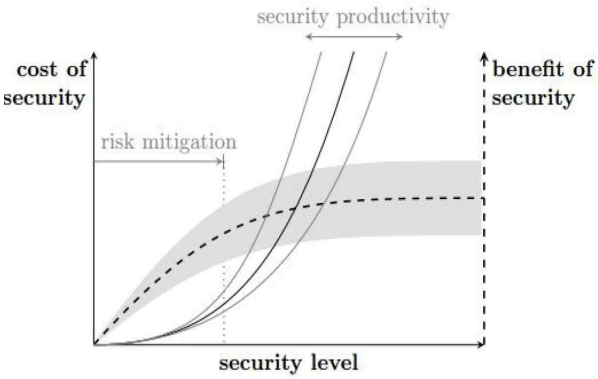

그림 1. 정보보안에 있어서의 비용/편익 관계
Fig. 1. Cost/benefit relationships in information security

표 2. 정보보안 서비스 대가 산정 연구현황
Table 2. Study on the cost estimation of information security services

Analysis	Researcher	Contents
Software-centric cost	You-Jin Park(2011)[5]	Calculate maintenance costs by applying correction factors based on the information security products and maintenance activities
Cost-benefit	Böhme(2010)[6]	ROSI (Return on security investment) suggests a form in which benefits are less than cost, divided by cost, and converted into percentages
Cost by Service Activity	Jo Yeon-Ho(2015)[7]	Analyzing the status of the service for the continuation of the security of the information security solution, and considering the characteristics of the information security solution, the rate method and fixed amount method are calculated.
	Korea Software Industry Association(2018)[8]	Security continuing service rate criteria applied to rates as a measure of security service point based on the service activity cycle

표 4. 보안 서비스 포인트 측정방식
Table 4. SSP measurement basis

Div.	Measurement criteria	Score
Security update	more than once a month	30
	more than once a quarter	25
	more than once a half year	20
Security policy management	more than once a month	20
	more than once a quarter	15
	more than once a half year	10
Threat/ accident analysis	more than once a month	20
	more than once a quarter	15
	more than once a half year	10
Maintain security authentication	Maintaining CC certification or KCMVP (cipher module) certification	20
	Keep other security certifications	10
Security technical advisory	Technical advice over 20 hours a year or simulated training more than twice a year	10
	Technical advice over 10 hours a year or simulated training more than once a year	5
		SSP

표 5. 보안성 지속 서비스 대가 산정방식
Table 5. Method of estimating the cost of security continuity service

Div.	Method
Security continuity service rate(%)	10 × (SSP / 100)

2.3 해외 정보보호서비스 대가 적용 사례

미국과 일본은 공급자와 수요자 간의 서비스 수준 협약(Service Level Agreement, SLA) 중심의 계약을 체결하여 수요자가 원하는 보안성 지속서비스를 명시하고 소요되는 비용을 개별적으로 체결하도록 하였다. 미국인 경우에는 정보보호제품 도입 후 2년째부터 연각 서비스 요금을 도입비용의 28% 이상으로 적용하고 있다[9].

표 6. 미국의 적용 사례
Table 6. U.S. application cases

Div.	Application rate
SI cost	SettingsInclude change 20% applied
Annual service cost	28% application of basic composition

표 7. 일본의 SLA 항목
Table 7. Example of SLA in Japan

Div.	Service type	Contents
Basic service	HW, SW, integral form	Phone, mail, remote assistance : office time
Optional service	Visiting service (office time), visit service (365 - 24 hours)	Separate contract
Other services	Visit service by case	Actual cost claim

일본인 경우에는 정보보호 제품의 유지관리에 대해서 SLA협약을 통해 통상 20%이상의 대가 적용을 발주요건에 명시하도록 하고 있다[4][7].

III. 도입기관의 적용사례 분석

본 장에서는 현재 정보보호 서비스를 도입 적용하고 있는 국내 유일한 기관인 제주특별자치도 A기관의 적용사례를 통해서 정보보호 서비스가 어떠한 효과를 미치는지 검증하고자 한다. A기관은 시군구 단위의 지방자치단체이며, SLA를 기반으로 하여 2017년부터 정보보호제품과 일부 정보시스템에 대한 정보보호 서비스 대가를 적용하고 있다.

3.1 A기관의 SLA 정책

서비스 수준 협약서(SLA)는 공급자가 IT 서비스를 제공함에 있어 소비자와 당사자 간에 서비스에 대하여 측정지표와 목표 등을 정한 협약서이다. 일반적으로 포함되는 측정지표는 시스템 가동률, 장애복구율, 서비스 응답율, 서비스 완료시간 등이다.

A기관은 2017년부터 제품군별 유지보수와 정보보호 지속 서비스를 SLA중심으로 측정하고 이를 바탕으로 적정한 대가를 적용하고 있다. 이 기관의 정보보호제품과 일부 정보시스템에 대한 정보보호 서비스 대가 측정기준을 표 8과 같이 적용하고 있다.

세부항목별로 측정기준은 수행주기를 주(W), 월(M), 분기(Q), 반기(H), 연간(Y)별로 세분화하였고, SLA 기준을 목표(Target Level, TL)와 최소치(Min.)를 정하였다.

표 8. A기관의 SLA 항목
Table 8. Standards for measuring security SLAs of a agency

Div.		Rate(%)	SLA	
			TL	Min.
Security update (SU)	Update pattern	0.5	99	95
	Security patch update	0.5	99	95
Risk analysis report by product (RA)	Asset identification and importance evaluation	0.2	99	95
	Check and take action for security weakness	0.8	99	95
	Risk analysis evaluation	0.5	99	95
	Establishing information protection measures and implementation plans	0.5	99	95
Intrusion accident response by product (IR)	Real-time security threat monitoring and detection and initial analysis	0.3	99	95
	Real-time response and reporting of cyber threat symptoms	0.5	99	95
	Monitor key IT infrastructure and check availability	0.2	99	95
	Collects and analyzes detailed data of security equipment based on initial analysis results	0.5	99	95
	Identify the extent of damage, such as data leakage, deviations of administrator authority, etc.	0.5	99	95
	Recovery Support and Countermeasures and Strategies for Different Types	0.5	99	95
	Backup equipment events and logs	0.3	99	95
	Malicious code analysis and distribution prevention service	0.2	99	95
Simulated training response (ST)	Hacking mail simulation training	0.5	99	95
	Disaster recovery test	0.5	99	95
Security audit support (SA)	Support for security audit of higher institutions	0.2	97	92
	Support for ISMS certification review	0.3	97	92
Technical advice (TA)	Information security training	0.2	97	92
	Quality control and improvement of work by security service area	0.1	95	90
	Security trend analysis	0.2	95	90

표 9. 서비스별 수행기준
Table 9. Criteria for performance by service

Div.		Criteria for implementation				
		W	M	Q	H	Y
SU			●			
RA				●		
IR		●				
ST					●	
SA					●	
TA	Information security training				●	
	Quality control and improvement of work by security service area					●
	Security trend analysis	●				

3.2 SLA 기반의 대가산정 방법

A기관은 SLA 측정 평가를 월단위로 실시하였으며, 표 10과 같이 SLA의 목표수준(TL) 대비 해당 월의 측정치(M)율을 계산한 후 가중치(R)를 적용하였다.

여기서 나온 SLA 측정 평가결과에 목표 달성도에 따른 부여된 가중치(V) 값으로 계산하여 제품별 정보보호 서비스 대가요율을 산정하였다.

표 10. SLA 기반의 대가 산정방법
Table 10. SLA-based pricing method

SLA evaluation result formula	Div.	Method
	SLA results (SL)	(M / TL × 100) × R

↓

SLA Objective Attainment Criteria	Result (V)	Above the target level	Minimum level and above	Minimal criterion attainment failure
		1.0	0.8	0.5

↓

Security Continuity Service Costs	Method
	SL × V

3.3 도입 효과 분석

정보보호 서비스 대가 적용의 효과를 전체적으로 평가하는 것은 많은 어려움이 따른다. 특히, 소프트웨어의 일반 유지보수 범위와 소프트웨어 성격이 강한 정보보호 서비스의 범위가 중복되는 부분으로 인해 서귀포시에서는 이를 최대한 구분지어 요율을 적용하고 있다. A기관의 도입 효과를 분석하기 위해 정보보호서비스 대가 도입하기 전인 2016년도(Y-1)의 유지관리 완료보고서와 도입을 시작한 2017년(Y), 2018년도(Y+1)의 유지관리 완료보고서를 참고하여 년간 보안업데이트, 보안 리스크 분석, 침해대응 처리, 모의훈련, 기술자문 건수 등을 기준으로 분석한 결과 도입 이전보다 도입 후의 효과가 표 11과 그림 2와 같이 나타났다[9].

표 11. A기관의 도입전과 후 효과 비교
Table 11. Comparison of effects before and after the introduction of the agency

DIV.	Process count		
	Y-1	Y	Y+1
SU	1	3.7	11
RA	0.3	12	25.7
IR	1	12	81.33
ST	0	2	4
SA	0	2	2
TA	0.5	4	8
Visit support count	0.5	4	7

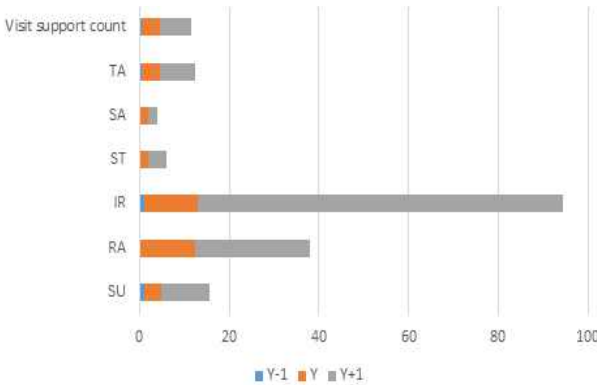

그림 2. A기관의 도입전과 후 효과 비교
Fig. 2. Comparison of effects before and after the introduction of the agency

IV. 정보보호서비스 개선모델 제안

본 장에서는 기존의 관련연구와 도입 기관의 적용사례를 바탕으로 현재의 정보보호서비스 대가 모델에 대한 개선안을 제시하고자 한다.

4.1 SCS 성과평가체계 기반 대가 산정 제안

A기관의 사례를 분석한 결과와 업무담당자의 인터뷰 결과, SLA 기반의 정보보호서비스 대가 산정의 효과는 비용-효용분석 측면에서 효용성이 높은 것으로 나타났다. 하지만, 보다 더 객관적인 지표를 위해서 항목은 국가표준기술원(NIST) Cybersecurity Framework(CSF)과 A기관의 SLA지표를 보완 적용하여 개선된 SCS(Security Continuity Service) 성과평가체계 모델을 제안한다. NIST의 CSF는 2014년 미국 사이버보안 강화법에 따라 미국의 NIST가 제작한 사이버보안 프레임워크이다. NIST CSF는 조직에서 사이버 보안 운영을 계획, 관리 및 지속적으로 개선하기 위해 제작한 프레임워크이다[10]-[14].

표 12는 NIST CSF, 정보보호서비스, SLA 기준을 결합하여 제안한 SCS 성과평가체계 모델이다. 이 모델은 사이버 보안 운영 및 위험 관리와 관련된 회계 시스템의 요소를 품질 비용 모델에 연결하는데 여전히 유용할 수 있다[15]-[21].

표 12의 SCS 성과평가체계 모델의 세부항목은 항목별 기준요율(Base Rate, BR), 측정기준인 SLA의 목표(Goal Level, GL)와 최소치(Min.), 세부 성과지표별 가중치(IRV), SCS 요율 등으로 구성하였다. 세부 성과지표별 가중치(Weight by Indicator, WI)는 표 13의 산출산식으로 세부 성과지표별 수행율(Performance Rate, PR)을 계산한 후 나온 결과를 SLA 측정기준과 비교하여 표 13의 평가방식인 세부 성과지표별 가중치(WI)를 구하였다.

SCS 성과평가체계 모델을 적용한 요율방식의 정보보호서비스 대가 산정방식은 제품별로 세부항목별 기준요율(BR)과 가중치(WI)를 곱한 후 도출된 최종 요율을 모두 합산하면 정보보호서비스 대가 요율(SCS Rate)이 결정된다.

표 12. 서비스 대가 기준 제안모델
Table 12. Service charge standards proposal model

Div.		BR (%)	SLA		WI	SCS rate (%)
			GL	Min		
Identify	Asset identification and importance evaluation	0.3	95	93	0.4~1.0	BR*WI
	Check and take action for security weakness	0.2	95	93	0.4~1.0	BR*WI
	Compliance with security procedures	0.2	95	93	0.4~1.0	BR*WI
	Maintaining important personnel	0.1	95	93	0.4~1.0	BR*WI
	Security update, security patch update	0.5	95	93	0.4~1.0	BR*WI
	Risk analysis evaluation	0.5	95	93	0.4~1.0	BR*WI
Protect	Establishing information protection measures and implementation plans	0.4	95	93	0.4~1.0	BR*WI
	Monitor key IT infrastructure and check availability	0.3	95	93	0.4~1.0	BR*WI
	Hacking simulation training	0.4	95	93	0.4~1.0	BR*WI
	Security audit support	0.3	95	93	0.4~1.0	BR*WI
	Technical advice	0.1	95	93	0.4~1.0	BR*WI
	Preventive inspection, regular inspection	0.3	95	93	0.4~1.0	BR*WI
	Failures and errors, failover time, and recovery time	0.3	95	93	0.4~1.0	BR*WI
Respond	Real-time security threat monitoring and detection and initial analysis	0.4	95	93	0.4~1.0	BR*WI
	preventive inspection, regular inspection	0.4	95	93	0.4~1.0	BR*WI
	Identify the extent of damage, such as data leakage, deviations of administrator authority, etc.	0.5	95	93	0.4~1.0	BR*WI
Detect	Real-time response and reporting of cyber threat symptoms	0.5	95	93	0.4~1.0	BR*WI
	Collects and analyzes detailed data of security equipment based on initial analysis results	0.5	95	93	0.4~1.0	BR*WI
	Malicious code analysis and distribution prevention service	0.5	95	93	0.4~1.0	BR*WI
Recover	Recovery support and countermeasures and strategies for different types	0.5	95	93	0.4~1.0	BR*WI
	Analyze backup appliance events and logs	0.5	95	93	0.4~1.0	BR*WI
	Disaster recovery test	0.3	95	93	0.4~1.0	BR*WI
SCS Rate(%)		8			0.4~1.0	BR*WI

표 13. 항목별 가중치 산출식 및 적용 기준
Table 13. Calculation formula and weight by indicator

Div.	Method			
Calculation formula	$PR = \sum\left(\frac{N}{T}\right) \times 100\%$ N : Number of performance cases T : Target count PR : Performance rate			
Weight by Indicator(WI)	Weight by SLA metric			
	100~95%	~93%	~90%	85%~
	1.0	0.8	0.6	0.4

표 14. 서비스 대가 산정방식
Table 14. Security continuity service cost

Div.	Contents
Security continuity service cost	Purchase price × SCS Rate(%)

표 14와 같이 제품별 정보보호서비스 대가 산정 방식은 제품공급가격에 SCS Rate를 곱하여 산정하는 방식이다.

Ⅳ. 결 론

본 논문에서는 기존에 마련된 정보보호 서비스 대가모델을 개선하여 공공분야와 민간분야에서 적용할 것인지에 대해 알아봤다. 날로 급증하고 있는 사이버 위협으로부터 사전 예방과 지속적인 대응을 위해 정보보호서비스의 중요성이 커지고 있으나 우리나라는 다른 국가들에 비해 제도적인 측면과 현실 측면에서 차이가 큰 것으로 나타났다. 그동안 국내 정보보안 산업계에서 정보보호서비스에 대한 적정한 대가를 받기 위해 지속적인 노력을 해왔다. 정부에서도 정보보호산업 진흥에 관한 법률 제정, 제품 특성에 맞는 대가 산정 기준 마련, 표준계약서 마련 등의 노력을 하고 있다. 하지만, 수요자인 공공기관 담당자와 공급자인 정보보안업체 간의 인식 차이가 크다보니 현실적으로 정착하는데 큰 걸림돌이 되고 있다. 이를 개선하기 위해서는 정보보호 서

비스 대가모델이 공공기관에 의무적으로 적용되기 위해서는 우선적으로 법제도가 개선되어야 한다.

첫째, 현재 권고수준으로 되어 있는 정보보호산업 진흥에 관한 법률 제10조를 강제성이 있도록 개정해야 한다. 2015년 제정된 정보보호산업 진흥에 관한 법률 제10조에는 공공기관 등이 정보보호사업을 발주하는 경우 정보보호제품과 정보보호서비스의 품질보장을 위해 적정한 수준의 대가를 지급하도록 노력해야 한다고 명시되어 있다. 이는 권장사항이기 때문에 강제성이 없다. 정보보안산업의 글로벌 경쟁력을 키우기 위해서는 공공기관이 우선적으로 정보보호서비스 대가에 대한 제값받기를 위해서 강제성을 띤 법률적 제도가 뒷받침이 되어야 한다. 특히, 국가 주요기반시설을 운영하고 있는 기관인 경우 정보통신기반보호법과 개인정보보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률 등 관련 법령에도 이에 대한 적용 강제성을 명시하여야 한다.

둘째, 현재 국가기관이나 공공기관을 대상으로 “국가기관・공공기관 정보보호관리실태평가”와 경영평가, 지방자치단체 합동평가 제도 등에 “정보보호 서비스 대가 반영실적”을 평가항목에 포함하여 확산될 수 있도록 하여야 한다. 그리고 정보보호 시스템뿐만 아니라 모든 정보시스템에도 보안 취약점 제거를 위한 정보보호 서비스를 받을 수 있도록 의무화하고 정부기관의 예산안 편성 지침에 정보보호서비스 대가 항목을 명시하여야 한다.

셋째, 정보보호서비스를 제공하는 업체의 자구노력이 필요하다. 수요자입장에서는 제품에 대한 적정한 정보보호서비스를 받고 있는지에 항상 의문을 갖고 있다. 이러한 의문을 해소하기 위해서는 공급자인 업체에서도 스스로 서비스에 대한 검증을 할 수 있어야 하며, 보다 객관적이고 공정한 수준평가를 위해 국가 차원의 공인인증기관을 지정 운영하는 것도 바람직할 것이다.

마지막으로 정보보호서비스 대가의 적용을 정보보호시스템으로 한정하지 말고 정보시스템, IoT, 소프트웨어, AI 등 정보화분야로 확대 적용하는 것이 보안위협으로부터 사전 예방 및 신속한 대응을 하는데 용이할 것이다. 향후에는 정보보호서비스 대가에 대한 수요자와 공급자간의 인식도 조사와 보안성 지속서비스와 보안관제서비스 등이 결합한 통합 정보보호서비스 대가 체계 개발 등의 연구가 필요할 것이다.

References

[1] Ministry of Government Legistation, http:/www.law.go.kr/lsInfoP.do?lsiSeq=202280&efYd=20180522#0000.

[2] KISA, "Information Protection System Implementation Practical Guide", 2018.

[3] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC).(2016). Information security management (ISO/IEC Standard No. 27001).

[4] KISA, "Information Protection Service Cost Estimating Guidelines", 2015.

[5] You-Jin Park, "A Study on an Estimation of Adjusted Coefficient for the Maintenance of Information Security Software in Korea Industry", 2011.

[6] Böhme, R., "Security Metrics and Security Investment Models", In IWSEC, pp. 10-24, 2010.

[7] Yeon-Ho Jo, "A Study on Policy for cost estimate of Security Sustainable Service in Information Security Solutions", 2015.

[8] Korea Software Industry Association, "Software Business Cost Reference Guide", 2018

[9] Seogwipo city, "2016-2018 Information Security System Maintenance Inspection Report", 2016~2018.

[10] NIST, https://www.researchgate.net/profile/Nicole_Radziwill/publication/318311904_Cybersecurity_Cost_of_Quality_Managing_the_Costs_of_Cybersecurity_Risk_Management/links/5962b402458515a35751ac26/Cybersecurity-Cost-of-Quality-Managing-the-Costs-of-Cybersecurity-Risk-Management.pdf?origin=publication_detail pp. 189-197, Sep. 2010.

[11] N. Park, H. Hu, and Q. Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)",

International Journal of Distributed Sensor Networks, Vol. 2016, No. 1, Jan. 2016. https://doi.org/10.1155/2016/2965438.

[12] D. Lee and N. Park, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", International Journal of Personal And Ubiquitous Computing, Vol. 22, No. 1, pp. 3-10, Feb. 2018.

[13] N. Park and M. Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", International Journal of Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[14] D. Lee and N. Park, "Geocasting- based synchronization of Almanac on the maritime cloud for distributed smart surveillance", International Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2016.

[15] N. Park, "Privacy-Enhanced Deduplication Technique in Closed Circuit Television Video Cloud Service Environment", International Journal of Engineering & Technology, Vol. 7, No. 24, pp. 65-66, May 2018.

[16] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", International Journal of ELECTRONICS, Vol. 8, No. 4, pp. 412-426, Apr. 2019.

[17] N. Park and N. Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", International Journal of Sensors(Basel), Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[18] N. Park, J. Kwak, S. Kim, D. Won, and H. Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conference of Advanced Web and Network Technologies, and Applications, Harbin, China, pp. 741-748, Jan. 2006.

[19] N. Park and H. Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", International Journal of Security And Communication Networks, Vol. 9, No. 6, pp. 500-512, Apr. 2016.

[20] D. Lee, N. Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", International Journal of Peer-to-Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[21] D. Lee and N. Park, "A Proposal of SH-Tree Based Data Synchronization Method for Secure Maritime Cloud", Journal of KIISC, Vol. 26, No. 4, pp. 929-940, Aug. 2016.

저자소개

오 상 익 (Sangik Oh)

2012년 2월 : 제주대학교 경영학과 (학사)
2018년 3월 ~ 현재 : 제주대학교 융합정보보안학과 석사과정
2002년 2월 ~ 현재 : 서귀포시청
관심분야 : 정보보호관리체계, 사이버침해, 블록체인 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 ASU대학교 연구과학자
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 융합정보보안학과 교수
관심분야 : 융합기술보안, 컴퓨터교육, 지능형영상 등