Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.905

정보보안솔루션 보안성 지속 서비스 대가 산정 정책 연구

조 연 호,† 이 용 필, 임 종 인, 이 경 호‡
고려대학교 정보보호대학원

A Study on Policy for cost estimate of Security Sustainable Service in Information Security Solutions

Yeon-ho Jo,† Yong-pil Lee, Jong-in Lim, Kyoung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

정보보안솔루션은 구축 후 일반적인 유지관리 활동 외에 외부 위협요인(공격)으로부터 보안성을 지속시키기 위해, 악성코드 분석 및 보안업데이트, 보안정책관리, 위협/사고분석, 보안성 인증 효력 유지, 보안기술자문 등의 추가활동이 수반되지만, 제공된 서비스만큼의 대가를 적용받지 못하는 현실적 문제점이 상존한다. 이에, 본 연구에서는 국내 정보보안솔루션의 보안성 지속을 위한 서비스 현황을 분석하고, 정보보안솔루션의 특성을 고려한 보안성 지속 서비스 대가가 반영될 수 있는 정책적 방안을 제시한다.

ABSTRACT

Once information security solution is implemented, it requires many services other than just general user management, such as malicious code analysis and security updated for consistent security against external threats or attacks, analysis of threat and attack, effectivity management of obtained security assurance, and advisory activities of security technical professionals. However, even if information security solutions provide those extra services, they are not properly treated in real market. Thus, for the security sustainable services, this study analyzes the service status of domestic information security, and suggest policy measure of price which could reflected the characteristics of information security solutions.

Keywords: Cost of Information Security, Cost Estimate of Information Security Solutions, Security Sustainable Service

I. 서 론

20년 이상의 역사를 가진 우리나라 정보보안 산업은 미국, 이스라엘에 이어 정보보안 전 분야에서 자국 솔루션을 보유한 국가로 자리 잡고 있으나, 국내 정보보안시장은 약 1조 7,000억으로 세계시장의 1.9% 수준에 불과하며, 매출액 중 서비스의 비중이 낮고, 내수시장 의존도가 높은 특성을 가지고 있다.

반면, 글로벌 정보보안 기업은 현재 세계시장의 25% 이상을 점유하는 등 시장지배력을 높여가고 있으며, 국내 시장에서도 점유율이 증가하는 추세로 국내 기업과의 경쟁이 심화될 것으로 예상된다.

정보보안솔루션은 그 형태에 따라 소프트웨어(이하 'SW')나 소프트웨어와 하드웨어(이하 'HW')가 결합된 일체형(Appliance)으로 구분되는데, 단순히 소프트웨어나 하드웨어로 분류되면서 이에 따른 정책이나 기준이 적용되어, 보안성 지속 서비스(Security Sustainable Service)가 제대로 인정받지 못하는 결과를 초래하였고, 이는 기술개발과 서비스 품질 향상을 위한 재투자를 어렵게 하는 동시에

접수일(2015년 5월 21일), 수정일(2015년 6월 22일), 게재확정일(2015년 7월 9일)
† 주저자, hesslerjo@gmail.com
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

글로벌 기업과의 공정한 경쟁을 저해하는 요인으로 작용하고 있다.

본 연구에서는 정보보안솔루션의 보안성 지속 서비스 현황을 분석하고, 정보보안의 특성을 고려한 대가가 반영될 수 있는 정책적 방안을 모색하고자 한다.

II. 관련 연구

보안성 지속 서비스는 기존에 없던 개념으로 이전 연구는 SW 관점의 정보보안 유지관리[1]를 중심으로 이루어져 왔다.

먼저, 지식경제부[2]는 정보보안과 SW와의 유지관리 차별성을 설명하고, 특히, 정보보안제품군별 보안 업데이트를 부각시키며, Table 1.과 같은 지표를 제시하였다.

Myeong-Gil Choi 등[3]은 국내 정보보안 SW와 일반 SW 산업현황 및 유지관리 체계와 해외 현황 등을 비교하여 국내 요율체계의 문제점을 지적하고, 보안정책 지원과 CC인증 등 정보보안의 추가적인 서비스 부분을 제시하였다.

You-Jin Park 등[4]은 정보보안의 유지관리 활동을 패턴 유지, 인증, 보완 개발, 기술지원 으로 분류하고 이를 반영한 정보보안 SW 유지관리 비용 표준의 적절한 수준을 제안하기 위해 일부 제품군에 대해 보정계수 추정을 시도하였다. 정보보안 제품과 활동별 유지보수 대가 기준 방식으로 활동별 유지보수 소요횟수, 해결 소요 시간, 소요 인력, 그리고 학습곡선을 적용하여 활동별 유지보수 대가 비용을 제품별로 산정하고, 보정계수를 적용하여 유지보수대가를 산정하는 형태를 제안하였다.

이처럼, 지금까지의 연구는 정보보안의 추가적인 서비스 활동을 강조하고, SW 관점에서 정보보안 유지관리를 개선하고자 하였다. 본 논문에서는 SW와 HW의 특성이 공존하는 정보보안의 특성에 맞게 보안성 지속 서비스 대가를 산정할 수 있는 방안을 제시한다.

1) 정부 위기관리대책회의('12.6.26, 상용SW 유지관리 합리화 대책)에 따라 "유지보수" 용어는 "유지관리"라는 것으로 활용하기로 한 만큼, 본 연구에서도 "유지관리" 용어를 적용

Table 1. Information security software maintenance costs applies

Category	Security Update	
	Frequency /year	Input/case
Firewall	10	1MM
IPS	500	3MD
UTM	100	1MD
ESM	50	1MM
TMS	200	3MD
PMS	100	1MD
Vulnerability/ log analysis	100	1MD
VPN	10	1MM
Anti Spam	100	1MD
Secure OS	10	5MD
PC Security	100	1MM
DLP	12	3MM
Security USB	30	1MM
DB Security	2	1MM
Keyboard Security	10	1MM
DRM	10	1MM
PKI	1	1MM-10MM
NAC	100	1MM
EAM, SSO, IM	1	1MM-10MM
Wireless / Mobile Security	10	1MM

III. 보안성 지속 서비스의 정의

3.1 보안성 지속 서비스의 정의

보안성 지속 서비스는 새로운 개념으로, 기존 정보보안 유지관리에 포함되어 있던 정보보호 활동을 서비스 항목별로 도출하여 구성하였으며, 기존 법률[2]에서 정하고 있는 정보보호의 정의를 활용하여 다음과 같이 정의하였다. "보안성 지속 서비스란 정보보호제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위한 기술 기반의 서비스를 말한다."

정보보안솔루션은 정보보안제품, 제품의 기능 유지를 위한 유지관리, 외부 위협요인(공격)으로부터 대응하기 위한 보안성 지속 서비스로 구성된다.

정보보안 제품은 형태에 따라 보안 소프트웨어 제품과 소프트웨어와 하드웨어가 결합된 일체형 제품으

2) 국가정보화 기본법 〔법률 제12844호〕 제3조(정의) 6

로 구분되고, 특성에 따라 네트워크 보안, 시스템(단말) 보안, 컨텐츠(데이터)/정보유출방지 보안, 암호/인증, 보안관리 등으로 분류된다.

유지관리는 구매한 제품을 최적의 상태에서 활용·유지하기 위해 제공되는 제품지원, 기술지원, 사용자 지원 등의 활동을 의미한다.

보안성 지속 서비스는 정보보안 제품의 보안기능을 최신으로 유지하기 위해 신규 악성코드 및 위협정보에 대한 분석과 보안업데이트, 환경 변화에 따른 보안정책 변경, 사고 발생 시 사고 조사 등의 서비스를 포함하는 것으로 일반 IT제품에는 존재하지 않는 정보보안솔루션만의 특화된 서비스이다.

3.2 보안성 지속 서비스의 특징 및 내용

정보보안솔루션은 보안성 지속 서비스가 정상적으로 제공되지 못할 경우 보안성이 약화되기 때문에 구축 시점부터 내·외부 보안위협에 대응하기 위한 보안성 지속 서비스가 필수적이다. 유지관리가 제품 내(內)적 요인 중심의 서비스인데 비해 보안성 지속 서비스는 제품 외(外)적 요인(해킹, 신규 악성코드 감염 등 외부자의 공격, 내부자에 의한 정보유출 등) 중심의 서비스이다. 소프트웨어의 경우 개발이 완료되면 투입인력이 급격히 줄어들지만, 정보보안솔루션은 개발완료 후에도 보안성 지속 서비스를 위해 개발인력을 포함한 서비스 인력들이 꾸준히 유지되거나 증가하는 구조적 특성을 가진다. Table 2.는 기존의 유지관리 서비스[1]와 보안성 지속 서비스와의 차별성을 활동과 요인별로 분류하고 있다.

Table 2. Comparison of Security Sustainable Service and Maintenance

Div.	Service Items*	Activity	Causes
Security Sustainable Service	SU	Security rule pattern and signature	External factors
	MSP	Security policy making and changes	
	TIA	Incident Response (pre/post), threat analysis report	
	MSC	CC, CMVP, etc.	
	STA	Cyber attack response exercises, security training/audit support, etc.	
Maintenance	PS	Patch, update, upgrade	Internal factors
	TS	Routine Support, Troubleshooting, Custom support, etc.	
	US	User/Operator training, etc.	

* SU: Security Update, MSP: Managing Security Policies, TIA: Threat/Incident Analysis, MSC: Maintain Security Certification, STA: Security Technical Advisory, PS: Product Support, TS: Technical Support, US: User Support

3.2.1 보안 업데이트

대부분의 보안시스템은 지속적으로 발견되는 공격기법을 시그니쳐로 변환하여 공격패턴 비교방식의 메커니즘을 사용하므로 보안 시그니쳐 업데이트를 지속적으로 관리함으로써 보안성을 향상시킬 수 있다. 또한, 신규 OS나 시스템 및 단말, 신규 표준이나 프로토콜 반영 등 IT환경변화에 대한 패치도 보안 업데이트에 포함되는 사항이다.

3.2.2 보안정책관리

보안정책 변경관리는 일반적으로 보안강화 또는 완화 등과 같이 보안 룰셋의 변경관리 업무와 납품된 보안시스템 자체에 대한 정책 변경관리가 있다. 보안정책 변경은 기업이나 기관의 변경사항이 발생하거나 보호해야 할 정보시스템에 변화가 있을 경우에 발생한다. 웹방화벽의 경우 보호할 웹 어플리케이션의 소스 또는 구조가 변경되었을 경우 보안정책의 변경이 필요하게 된다.

3.2.3 위협/사고분석

해킹이나 악성코드, 최신 정보보안 기술에 대한 정보를 제공하는 것으로, 제공 시기에 따라 정기적인 정보제공과 수시 정보제공 형태로 나눠진다. 수시 정보제공 형태는 침해사고 발생 시 그 원인과 대응방안 등을 제공하는 것이 일반적이며, 침해사고 대응 보고서, 침해사고 분석 보고서 제공 등도 해당된다. 이 서비스를 통해 대내외 서비스의 위협요소들에 대한 잠재적 취약점 분석과 침투경로에 대한 점검, 고객의 정보시스템을 가장 안전하게 보호할 수 있는 최적의 해결 방안 및 대응 방안을 제시할 수 있다.

3.2.4 보안성 인증효력 유지

정보보안 제품은 IT 정보보호 제품 보안성 평가/인증 정책에 따라 정보보호 제품에 특화된 인증이 필수요건으로 적용되는데, 해당하는 인증에는 국제공통평가기준(CC:Common Criteria) 인증, 보안적합성 검증, 암호검증 등이 포함된다. 이는 정보보호 제품 최초 개발단계부터 폐기시까지 전 주기에 걸쳐 지속적으로 관리되어야 하는 부분이다.

3.2.5 보안기술자문

발주기관의 사이버침해사고 모의훈련대응, 정보보호 교육(제품관련 교육 제외) 지원, 원격문의 대응, 보안감사 지원, 등 발주기관이 긴급한 문제 해결을 요청한 경우, 온라인과 전화를 이용하거나 전문인력의 방문지원 등을 통해 문제를 해결하는 서비스를 말한다.(제품에 대한 일반적 지원은 해당하지 않음)

IV. 국내외 보안성 지속 서비스 현황

4.1 국내 보안성 지속 서비스 현황

국내 정보보안 산업분류 내 보안성 지속 서비스를 제공하고 있는 네트워크 보안, 시스템 보안, 컨텐츠/정보유출방지, 보안관리 등에 속하는 정보보안 제품 주요 공급기업 35개사(58개 제품)를 대상으로 조사한 결과 다음과 같은 결과를 도출하였다.

4.1.1 제품군별 보안성 지속 서비스 제공 현황

Table 3.은 정보보안 유지관리 활동별 비중인데 보안성 지속 서비스 항목에 포함되는 보안 업데이트, 보안정책 변경관리, 제품 성능개선, 정보제공 등이 높은 분포를 보이고 있음을 확인할 수 있다.

기존의 정보보안 유지관리 활동에서 보안성 지속 서비스를 분리하여 항목별 우선순위를 조사한 결과는 보안 업데이트와 보안 정책관리가 공통적으로 상위를 차지하고 있으며, 이외의 항목들은 제품군별 특성에 따라 차이를 보이고 있다.

4.1.2 국내 보안성 지속 서비스 대가 적용 현황

현재까지는 보안성 지속 서비스가 별도로 구분되지 않고 유지관리에 포함되어, 대부분 공급제품의 납품가 대비 요율로 지급받고 있다. 단, 시스템 보안 제품군의 경우 라이선스 구매방식으로 매년 지급되는 라이선스 비용이 서비스 요율로 반영되어 상대적으로 높게 나타났다.

Table 3. The proportion of maintenance and security sustainable service activities (Unit: %)

Div.*	NS	SS	CITP	SM	Avg.
Security Update	12	29	11	8	15.00
Managing Security Policies	10	19	11	13	13.25
Product performance	10	8	14	9	10.25
Function Add developed	9	4	12	8	8.25
Training and documentation	6	4	7	7	6.00
Providing security trends	6	4	5	6	5.25
Troubleshooting	16	13	14	15	14.50
Daily Support	11	11	9	13	11.00
Routine Support	16	8	15	14	13.25
Other	4	0	2	7	3.25

* NS: Network Security, SS: System Security, CITP: Content/Information Theft Prevention, SM:Security Management

Table 4. Priorities of activities in maintenance and security sustainable service

Div.	NS	SS	CITP	SM
Security Update	1	1	1	2
Managing Security Policies	2	2	2	1
Threat/Incident Analysis	5	4	5	3
Maintain Security Certification	3	3	3	4
Security Technical Advisory	4	5	4	5

Table 5. Rates status of maintenance and security sustainable service (Unit: %)

Div.	NS	SS	CITP	SM	Avg.
Less than 5%	21	-	-	14	8.75
6~8%	53	-	37	43	33.25
9~10%	11	-	42	43	24.00
11~13%	5	-	16	-	5.25
14~15%	5	-	5	-	2.50
16~20%	5	50	-	-	13.75
More than 20%	-	50	-	-	12.50

4.2 해외 보안성 지속 서비스 대가 적용 현황

미국은 제품의 하자보수를 중심으로 하는 기본적인 유지관리 업무 외에 추가 서비스를 패키지화하여 적용하고 있으며, 사용자와 공급자간 SLA(Service Level Agreement)를 통해 도입가의 평균 20-30%에 해당하는 서비스 계약을 체결하고 있다[2].

일본은 비용보다는 보안 수준을 우선시 하는 SLA 중심의 정책을 전개하고 있으며[2], 정보보안 솔루션 유지관리 및 보안성 지속 서비스에 대해서 공급가 대비 30%이상의 요율을 적용하고 있다.

해외 업체의 일반 솔루션과 정보보안 솔루션의 서비스 정책을 비교한 결과 일체형 정보보안 솔루션은 10%이상, SW기반 정보보안 솔루션은 20% 이상의 추가적인 대가가 편성되는 것으로 나타나 보안성 지속 서비스에 대한 대가가 인정되고 있음을 알 수 있다.

<Product: UTM>
-Product price(A): $25,520
-Installation cost(20% of the A): $5,104
-Annual service cost(28% of the A): **$7,145**
-Total Cost(Sum): **$37,769**
<Product: Network-DLP>
-Licenses and installation costs(B): $10,000
-Annual service cost(30% of the B): **$3,000**

Fig. 1. Case of security service cost(USA)[18]

<Appliance>
-Product price(A): ￥1,000,000
-Annual service cost(Over 30% of the A): ￥300,000
-On-site service(general: ￥150,000),
(365/24: ￥400,000)
<Software>
-Product price(B): ￥1,000,000
-Annual service cost(Over 30% of the A): ￥300,000
-On-site service: Case-by-case charge

Fig. 2. Case of security service cost(Japan)[18]

<IS Solution(Appliance) Service cost>[15]

Div.		NW Product	IS Solution
Product price		$1,424	$4,749
Service cost	Engine update	$236(16%)	$1,281(27%)
	RMA	$331(23%)	$1,044(22%)
Rate		39%	49%

<IS Solution(SW) Service cost>[16],[17]

Div.	General SW	IS Solution
Product price	$2,000	$7,000
Service cost	$438	$3,000
Rate	22%	43%

***IS(Information Security), NW(Network)**

Fig. 3. Comparison of security and other

4.3 글로벌 기업의 서비스 현황 및 사례

네트워크 부문의 글로벌 기업인 A사는 스위치, 라우터, 네트워크 보안기술 등을 제공하는 업체로 제품 구매시 서비스를 함께 판매하며, 구매된 서비스는 최초 제품구매시 1년간 유효하고 매년 서비스를 갱신하는 형태를 취하고 있다. 이들은, 단순한 제품 납품에 그치지 않고 수요자에게 필요한 다양한 기술서비스를 상품화하여 수익구조를 다변화 했다[8]~[10].

UTM 분야를 주도하는 업체인 B사와 지능형방화벽을 주력상품으로 공급하는 C사는 서비스를 구체화하고 상품화하여 판매하고 있는데, 각 항목별 서비스들은 1년, 2년, 3년 단위로 서비스를 갱신할 수 있으며 년수에 따른 서비스 비용의 할인율이 달리 적용된다. 이는 최초 제품 구매시부터 적용되는 기본적인 정책이다[11~14].

이와 같이, 업체들은 제품 판매시 해당 제품 별로 여러 서비스를 적용시켜 판매하고 있다. 이는 제품을 판매하면서 제공할 수 있는 서비스도 함께 판매하는 것으로 RMA(Return Material Authorization) 서비스를 토대로 제품설치부터 긴급한 문제해결에 이르기까지 다양한 서비스 상품을 제시하고 있다.

여기서 중요한 부분은 제품 수요자들이 자연스럽게 서비스를 함께 구매하도록 하고 있다는 점인데, 제품에 대한 서비스는 최초 제품구매시 1년간 유효하며 이후 서비스에 대해 연간 비용을 요청한다. 이것이 곧 공급제품에 대한 유지관리 및 보안성 지속 서비스 대가가 된다.

국내에 판매되고 있는 해외의 정보보안솔루션들은 Warranty licence를 기본으로 RMA와 기술지원 서비스가 이루어진다. 이러한 서비스들은 Warranty가 포함된 기술지원 서비스로 1년, 2년, 3년의 계약기간을 두고 이루어지며 기간에 대한 가격할인이 적용된다. 보안업데이트, 보안정책관리, 보안기술자문 등 국내 업체들이 유지관리의 개념으로 무료 또는 낮은 요율로 제공하는 서비스들을 해외업체들은 세분화하고 차별화하여 또 다른 상품으로 함께 판매하고 있는 것이다. 또한 글로벌 보안기업인 D사의 경우에도 서비스 등급을 3단계로 구분하고, 서비스 항목을 세분화하여, 등급별로 제공되는 서비스를 차별화 하고 있으며, 특징적으로, 서비스 항목 중 비용부담이 가

중되는 일부를 선택항목으로 분류해 추가 비용을 요구하는 체계를 취하고 있다[19].

V. 보안성 지속 서비스 대가 산정 모델

5.1 보안성 지속 서비스 대가 산정 필요성

전술(前述)한 바와 같이 정보보안솔루션의 보안성 지속 서비스에 대한 논의는 유지관리에 포함되어 진행되어 왔다.

먼저, 2009년 5월 "소프트웨어 사업 대가기준 고시"에 정보보안 솔루션에 대한 차별화 항목이 일부 반영 되었으나, 2010년 관련 고시가 소멸되면서, 소프트웨어 대가정책에 포함되어 왔다. 이후 관련 업계는 대정부 건의 등을 통해 지속적인 대가 개선요청을 이어왔으며, 정부는 2013년 6월 발표된 "대 중소기업 동반발전 방안"에서 상용SW 유지관리 대가 현실화(現8%→ '14년 10%→ '17년 15%내 검토) 제시로 정부가 구매 하는 상용SW 유지관리대가를 현재 SW구매가의 8%에서 '14년에는 10%로 인상하고, '17년까지 15%로 상향하는 방안을 검토하는 것으로 발표하였다. 그러나, 이 역시 소프트웨어 정책의 일환으로, 일체형 제품이 공존하는 정보보안솔루션의 특성을 담아내기에는 한계가 있다.

정보보안솔루션은 검수 시점을 기준으로 제품도입과 보안성 지속 서비스 단계로 구분될 수 있는데, 제품도입 단계에서는 공급자와 사용자 모두 비용 및 편익이 발생하지만, 보안성 지속단계에서는 사용자 편익발생에 비해, 공급자는 비용만 발생하는 불합리한 구조가 이어져 오고 있다.

Table 6.의 원가비교에서 나타나듯이 정보보안솔루션은 보안성 지속 서비스 제공에 따른 인력 운용 등으로 일반SW 유지관리 대비 1.9배 이상의 추가비용이 소요되는 것으로 조사되었다[18].

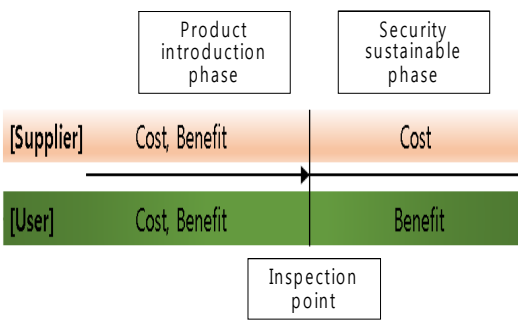

Fig. 4. Comparison of supplier and user

Table 6. Compare the cost of information security solutions and SW(Unit: One Thousand one)

Div.	Service Items	Information Security Solutions			SW		
		m/y	Unit price	Cost	m/y	Unit price	Cost
Security Sustainable Service	SU	2	45,000	90,000			
	MSP	1	45,000	45,000			
	TIA	3	60,000	180,000			
	MSC	1	60,000	60,000			
	STA	1	60,000	60,000			
Maintenance	PS	3	70,000	210,000	3	70,000	210,000
	TS	3	45,000	135,000	3	45,000	135,000
	US	3	45,000	135,000	3	45,000	135,000
Sum		-		915,000	-		480,000

이처럼, 투입비용과 대가가 부합하지 않는 구조에서는 유지관리 대가 산정과는 다른 접근방식이 필요하다는 관점에서 보안성 지속 서비스에 대한 별도의 대가 편성 필요성이 제기되었으며, 지금까지 국내 보안정책이 정부주도로 이루어져 왔고, 정부의 보안정책이 민간영역에도 확산되어 왔다는 점을 고려할 때 이를 실현하기 위해서는 정책적 뒷받침이 필수적이다.

5.2 보안성 지속 서비스 대가 산정 방안

지금까지 정보보안솔루션 대가 산정 체계는 정보보안 제품도입가(라이선스)와 유지관리비로 구성되어 있었지만, 앞으로는 여기에 보안성 지속 서비스가 추가되는 형태로 개선되어야 한다.

정보보안솔루션 보안성 지속 서비스의 대가 산정 방식은 요율제와 정액제로 구분될 수 있으며, 요율제

Table 7. Cost estimate structure of information security solutions

Div.	As-Is	To-Be
Product	Initial purchase cost or License cost	
Maintenance	Rates system or Fixed charge system	
Security Sustainable Service	-	Rates system or Fixed charge system

의 경우 서비스 투입율 및 난이도, 제공 기업의 정책에 따라 요율이 상이할 수 있으므로, 해당 정보보안 제품의 특성을 검토하여 선택(주로 일체형 정보보안 제품군에 적용)할 수 있도록 하고, 정액제의 경우, 라이선스와 보안성 지속 서비스의 내용 및 형태를 각각 검토하여 선택(주로 백신 등 정보보안 SW 제품군에 적용)한다. 또한 사고시 긴급 대응 등 고객의 특정 요구에 따라 별도로 제공되는 서비스의 경우, 서비스 투여시간 및 인건비 등에 따라 별도로 책정되어야 한다.

예를 들어, 요율제는 1차 년도에 정보보안 제품 공급가에 보안성 지속 서비스 대가(요율)을 포함하여 계약하고, 2차 년도부터는 보안성 지속 서비스 대가(요율) 금액으로 계약한다. 정액제는 1차 년도에 정보보안 제품 라이선스 및 구축비를 포함한 가격으로 계약하고, 2차 년도부터는 라이선스 금액으로 계약한다. 정액제의 경우 라이선스 금액에 보안성 지속 서비스 대가를 포함한다.

정보보안솔루션 공급자는 보안성 지속 서비스 항목별 우선순위를 도출하고, 항목별 비용(연간)을 산출하여 우선순위별 가중치(%)를 부여하는 형태로 대가를 산정할 수 있으며, 이것은 제품군과 사용자 환경에 따라 다르게 나타날 수 있다.

사용자는 해당 서비스 제공과 관련된 연간 예상

Table 8. Cost estimation methods for Security Sustainable Service

Div.	Method
Rates system	Purchase price * Rate
Fixed charge system	License cost (Including Security Sustainable Service cost)

Service Items	Priorities	Cost	Weight	Total
Security Update	1	$3,000	58.8%	$5,100
Managing Security Policies	2	$1,500	29.4%	
Threat/Incident Analysis	3	$300	5.9%	
Maintain Security Certification	4	$200	3.9%	
Security Technical Advisory	5	$100	2.0%	

Fig. 5. Example of cost estimation

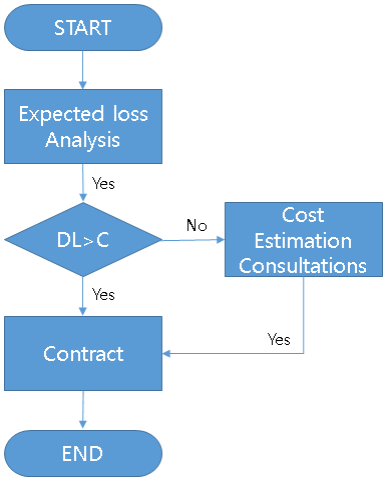

Fig. 6. Decision making process of the user

손실(서비스 전/후)을 산출하고, 공급자가 제시한 비용(C:Cost)을 서비스 전과 후의 예상손실액의 차이(DL: Difference of Loss)와 비교하여, 비용(C)이 낮은 경우 바로 그 대가를 적용하고, 높을 경우 공급자와 협의하여 대가를 산정하는 형태를 취할 수 있다. 이는 도입하는 정보보안솔루션에 대한 가치평가는 물론 공급기업이 제시한 서비스 비용에 대한 적정성을 판단하는 모델로 적용할 수 있다.

VI. 정책 적용방안 및 기대효과

앞에서 제시한 보안성 지속 서비스 대가 산정 방안을 정부 정책에 적용하기 위해서는 먼저, 산업계와 정부 협의 하에 공급자와 수요자가 공감할 수 있는 "보안성 지속 서비스 대가 산정 가이드"를 마련해 정보보호 서비스 항목과 내용, 계약방식 등을 제시해야 한다.

가이드에는 정보보안솔루션은 도입시점부터 '보안성 지속 정보보호 서비스' 예산을 산정하여 계약하고, 이후부터는 계약을 갱신하는 형태로 적용하도록 유도하는 내용을 포함하여, 현재까지 정보보안솔루션 공급 시 반영되지 않았던 '보안성 지속 서비스' 대가를 발주처(정부 및 공공부문)에서 책정할 수 있도록 하여야 할 것이다.

그리고, "보안성 지속 서비스 대가 산정 가이드"를 정책에 반영하기 위한 절차로 정부의 "정보화 시행계획에 작성지침"에 관련 내용을 추가하는 동시에 정부의 "예산안 편성 및 기금운용계획안 작성 세부지침"에 '보안성 지속 서비스 비용' 항목을 제시해야 한다.

Table 9. Classification of Information Security Services

Main Category	Sub Category
Information Security Service	IT Security Consulting
	Security Sustainable Service
	Maintenance
	Managed Security Services
	Education and Training
	Certification Services

아울러, 정부 조달시스템 적용에 대응하기 위해서는 조달물품분류에 "보안성 지속 서비스" 항목을 신설해야 하는데 이는 조달물품분류 상의 공학연구 및 기술기반서비스, 컴퓨터업 하위에 추가하는 것이 타당할 것으로 보인다. 또한, 정보보호 실태조사[7]의 정보보안 서비스 분류도 추가되어야 한다.

사용자(발주기관)와의 공감대 형성을 위한 활동도 필수적인데, 수립된 대가기준을 사용자 단체(CISO 협의회, 침해사고대응팀협의회, 공공부문발주자협의회 등)와 공유하여 활발한 검토와 의견수렴이 이루어져야 하며, 대가기준 적용 시 비용대비 효과 및 경제성 분석결과 제시를 통해 궁극적으로 정보보안 강화와 서비스 품질향상 등 수요자와 공급자 모두에게 유용한 것임을 인식할 수 있도록 해야 할 것이다.

'보안성 지속 서비스' 대가가 정착되어 민간부문까지 확대될 경우 연간 약 1,400억원 규모의 시장이 형성될 것으로 예상되며, 이는 1,600여명의 신규일자리 창출과 기술개발 투자 활성화 등 산업의 선순환 구조를 촉진하는 열쇠가 될 것이다. 또한, 제품 도입에 치중하던 정보보호 사업이 정보보호 본연의 서비스를 측정하고 적용하는 형태로 변화하여, 정보보호의 질적 수준 향상과 서비스 가치를 인정하는 문화 정착에 기여할 것으로 예상된다.

<Basis of calculation>
- o Calculated based on the Survey for Information Security Industry in Korea(Year 2014)
- o 2014 calculating the purchase price based on the average maintenance rate of 9.7%(estimate), and apply the Security Sustainable Service rate to 15%
  - 2014 Maintenance Products Purchase Price(estimated) = 935.8(billion won)
  - Rate of Security Sustainable Service = 15%
  - ∴ Cost of Security Sustainable Service = 935.8 * 15% = 140.3(billion won)
- o Job Creation: SW Industrial employment inducement coefficient (12 people / billion won)

Fig. 7. Proof of the budget estimates[7],[20]

VII. 결론 및 향후과제

이번 연구에서 국내 정보보안솔루션은 해외 업계에 비하여 서비스의 요율과 체계에서 차이가 큰 것으로 나타났다. 이러한 상황에서 국내 정보보안 업체들은 자체 서비스 등급체계를 마련하는 등 대가 현실화를 위해 지속적인 변화의 노력을 해오고 있으며, 정부에서도 유지관리 합리화 대책 수립, 소프트웨어 유지관리 표준하도급계약서 마련 등 불합리한 관행을 개선하려는 의지를 보이고 있다.

'보안성 지속 서비스' 대가 산정 추진과 함께, 국내 정보보안 업계에서도 제품의 성능과 서비스 수준 향상을 위한 투자 확대와 제공되는 서비스에 대한 내용과 실질적인 투입 예산(직접인건비, 기술개발비, 재료비 등)을 고객에게 인식시키기 위한 활동을 적극 추진하고, 관련 서비스를 체계적으로 상품화하여 고객 상황에 맞는 서비스를 유도해 나가야 할 것이다.

'보안성 지속 서비스'의 궁극적 목적은 정보보안 제품이 제 기능을 발휘할 수 있도록 지속적인 기술기반의 서비스를 제공하여 정보보호의 목표를 달성하는 것이다. 이런 관점에서, '보안성 지속 서비스' 대가는 국내 시장의 환경적 요인을 극복하기 위한 방안으로 추후 국내 시장이 성숙되어, 서비스에 대한 대가체계 정상화 문화가 정착되면 민간에서 자율적으로 적정 대가를 결정하게 하는 이른 바 시장논리에 일임하는 것이 합리적인 방법이라 하겠다.

향후에는 정보보안솔루션 분류별로 보안성 지속 서비스 항목을 분석하고, 정보보안 서비스에 포함되는 정보보안컨설팅, 보안관제 서비스 등 정보보안 서비스 전반의 대가체계 정립이 필요하다.

References

[1] KIPA, Guidelines Package SW maintenance services, 2005
[2] MKE, Necessity of raised cost in information security software maintenance, 2009
[3] Myeong-Gil Choi and Eun-Ju Park, "A study on the Information security software for the rate of maintenance," 2010 KMIS, pp. 403-408, 'Nov. 2010

[4] You-Jin Park and Eun-Ju Park "A Study on an Estimation of Adjusted Coefficient for the Maintenance of Information Security Software in Korea Industry," The Journal of Society for e-Business Studies, 16(4), pp. 109-123, Feb. 2012
[5] Cisco, International RMA Process. 2011
[6] Ministry of Security and Public Administration, Information Resource Manual for Maintenance measurement ratings, 2013.
[7] KISIA, Survey for Information Security Industry in Korea : Year 2014, 2014. 12.
[8] Cisco, product support service from Service Overview, 2013
[9] Cisco, Smart Care Service from Solution overview, 2013
[10] Cisco, Essential Operate Services Overview, 2013
[11] Juniper Networks, JTAC User Guide from Juniper Networks, 2013
[12] Juniper Networks,, Juniper Care Services datasheet, 2013
[13] WatchGuard, Global Customer Support Service terms and conditions, 2013
[14] WatchGuard, LiveSecurity Services datasheet, 2013
[15] NTSecurity. Policy of License Renewals, 2014
[16] Alt-N Technologies, MailStore Licensing Works, 2014
[17] Kaspersky Lab, Policy of Renewals, 2014
[18] KISIA, Cost comparisons of information security solutions and SW, 2014
[19] Symantec, Business Critical Services Handbook, 2014
[20] SPRi, http://spri.kr/post/4530

〈저자소개〉

조 연 호 (Yeon Ho Jo) 정회원
2002년 2월: 영남대학교 국어국문학과 졸업
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 정보보호학과 석사과정
〈관심분야〉 정보보호정책, 정보보호 관리체계, 융합보안

이 용 필 (Yong Pil Lee) 정회원
1995년 8월: 서울대학교 경제학과 졸업
2003년 8월: 서울대학교 행정대학원 석사
2008년 2월: 서울대학교 행정대학원 박사 수료
2003년 8월: 한국인터넷진흥원 입사
2015년 현재: 한국인터넷진흥원 보안산업정책팀장
〈관심분야〉 정보보호, 정보보호산업, IoT 보안

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 교수, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 안전행정부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

이 경 호 (Kyung Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 네트워크공학석사
2009년 7월: 고려대학교 정보경영대학원 박사
2011년 8월:~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 위험평가·관리, 정보보호 관리체계, 개인정보보호, 개인정보영향평가