Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1279

정보보호 기반 강화를 위한 정보보호 예산 확대 및 개선 방안 연구

배 선 하,† 김 소 정‡
국가보안기술연구소

Research on Expansion and Improvement Approaches of Information Security Budget for Cybersecurity Enhancement

Sunha Bae,† So Jeong KIM‡
National Security Research Institute

요 약

전자상거래, 전자정부 등 사이버 공간에서 활동 증가에 따라 안전하고, 신뢰성있는 정보화 기술 활용을 위한 정보보호의 중요성이 날로 높아지고 있다. 이에 미국, 영국을 비롯한 주요 선진국은 자국의 정보보호 강화를 위해 지속적으로 예산을 확대해 나가고 있다. 우리나라도 정보보호를 차세대 먹거리 산업 및 신성장동력 산업으로 육성하겠다는 계획을 발표하는 등 정보보호에 대한 관심이 지속적으로 높아지고 있다. 그러나 높아지는 관심과 필요성에 비해 우리나라의 정보보호 예산은 소폭 확대되었고, 정보보호 예산 부족이 우리나라의 정보보호 산업 성장 저해 요소로 지속적으로 지적되고 있다. 또한 정보보호 예산 편성 방안도 전체적인 정보보호 내용을 포괄하지 못하고, 정보화 사업 내에서 일부 보안 SW, HW, 서비스에 국한되어 요구가 가능하도록 되어 있어 명확한 예산 파악 및 실질적인 예산 확대에 어려움을 야기한다. 국가 전체적인 정보보호 역량 강화를 위해서는 정보보호 예산 및 투자의 확대가 필수적이다. 이에 본 논문에서는 우리나라의 정보보호 예산 현황 및 편성 방안에 대해서 검토하고, 미국의 정보보호 예산 현황 및 편성 방안을 분석하여 효과적인 정보보호 예산 확대 및 개선 방안을 제안하였다.

ABSTRACT

Information security to use information technology(IT) in safety and reliability environment is becoming of great importance. In advanced countries including United States and United Kingdom are consistently expanding budget for information security. Korea also has been a growing interest in information security and Korea government announced plan to develop information security into next-generation growth engine. However, information security budget has increased slightly in recent years, so many national institutions and state governments have budget shortfall to perform information security work. Moreover budget items do not include generic contents about information security and there are confined to some security SW, HW and services. It is necessary to expand information security budget for enhancement national capabilities of information security. In this paper, we analyze the IT and information security budget situation for Korea and United States and propose effective budget expansion and improvement approaches for Korea.

Keywords: IT security budget, IT budget, Budget Planning

Received(07. 13. 2016), Modified(09. 30 2016), Accepted(10. 04. 2016)

† 주저자, sunhabae@nsr.re.kr
‡ 교신저자, sjkim@nsr.re.kr(Corresponding author)

I. 서 론

정보화 기술의 발달은 인간을 더욱 자유롭고 편리하게 만들었지만 많은 역기능을 양산하는 부작용을 동반하였다. 이제 정보보호를 동반하지 않은 정보화 기술은 더 이상 안정적인 진보와 발전을 가져올 수 없다.

뿐만 아니라 정보보호는 단순히 정보화의 역기능이 아닌 국가 안보와 직결되며 차세대 고부가가치 산업으로 떠오르고 있다. 이러한 정보보호 산업을 국가의 신성장 동력으로 육성하기 위해서는 정보보호 분야 기술 및 정책 개발, 정보보호 인력 양성 등 국가 전체적으로 정보보호 역량 강화가 필요하다.

고조되는 사이버 위협에 대응하고, 국가 정보보호 기반 강화를 위한 실질적인 방안 마련을 위해서는 정보보호 예산 및 투자 확대가 필수적이다.

그러나 늘어가는 정보보호에 대한 관심에도 불구하고, 공공 분야 정보보호 예산은 매년 소폭의 비율로만 증액되었으며, 한국 정보보호의 문제점으로 예산 및 인력 부족이 꾸준히 도마에 오르고 있다. 공공분야 정보보호 예산의 소극적 확대는 적극적인 민간분야의 정보보호 투자 확대를 견인하지 못하고, 이로 인하여 민간 분야 정보보호 예산은 제자리걸음을 하고 있다. 결과적으로 한국의 정보보호 역량 강화에 악영향을 미치고 있다.

이에 정부는 각급기관의 정보보호 예산 실태 파악을 위해 정보화 사업 예산 요구 시 정보보호관련 예산 내역을 표로 작성하여 별도로 제출하도록 의무화하였다. 그러나 정보보호 예산 산정 기준 및 범위가 모호하고, 정보보호 예산 내역표가 일부 보안 시스템과 서비스에 대해서만 요구가 가능하도록 되어있어 명확한 예산 및 인력 규모 파악이 어렵고 정보보호 예산을 확대하는데 한계가 존재한다.

또한 정부는 2015년 4월 「국가 사이버안보 태세 강화 종합대책」에서 각급기관의 정보보호 예산을 별도 항목으로 분리하고, 취약점 분석·평가 지원, 사이버징후 탐지·대응기구 운영, 업무망과 인터넷 분리 등 관련 예산도 확대하겠다는 계획을 발표하였다[1]. 또한 2015년 6월에 제정된 「정보보호산업 진흥법」은 정보보호 서비스의 범위와 대가 기준을 명확하게 하여 정보보호 예산의 현실화를 통한 정보보호 예산 확대를 추진하고 있다.

이에 본 논문은 2장에서 현재 정부의 정보화 예산과 정보보호 예산 현황 및 편성 방안을 검토하고, 3장에서는 정보보호 분야 선진국인 미국의 정보화 예산과 정보보호 예산 현황 및 편성 방안을 검토하였다. 4장에서는 한국과 미국의 정보보호 예산 편성 구조를 비교·분석하고, 한국 정보보호 예산 편성 방안의 문제점을 분석하였다. 5장에서는 이를 개선하기 위한 방안과 한국의 정보보호 예산 확대 방안을 제안하였다. 마지막으로 6장에서는 결론을 맺는다.

II. 한국 정보화 및 정보보호 예산

2.1 예산 개요

한국의 예산 편성 과정은 먼저 기획재정부가 예산안 기본지침 및 사업유형별·비목별 세부지침을 정부기관 및 부처에 하달하고, 모든 정부기관 및 부처는 예산요구서를 작성하여 기획재정부에 제출한다. 기획재정부는 제출된 예산요구서를 분석하고, 정부의 투자중점 방향, 사업별 성과평가 등을 반영하여 부처별 예산 조정 및 협의를 통해 예산안을 마련한다. 국회는 정부의 예산안을 심의·확정하고, 확정된 예산이 최종적으로 집행된다.

한국은 기본적으로 사업예산제도를 택하고 있으

Table 1. Budget Program Types in Korea

no.	Program	no.	Program
1	Personnel Expense	13	Public State Property Fund
2	General Expense	14	Private Secondary
3	Total amount of Personnel Expense	15	Government Assistance
4	Government Institute & Assistance Institute	16	Local Matching Fund
5	Import Substitution Expenses	17	Voucher
6	R & D	18	Regional Development Special Account
7	ICT	19	Investment
8	ODA	20	Total Sum up
9	Employment	21	Treasury debt load
10	Events Support	22	BTL
11	Statistics	23	Acquisition of stake
12	Gender	24	Social Security

며, 이는 예산계획·편성·집행에 이르는 예산체계를 사업단위로 구조화하고, 이를 사업성과목표와 연결함으로써 성과를 관리하고자 하는 예산기법으로, 미국, 영국, 호주 등 많은 OECD 국가에서 활용되고 있다[2]. 한국 예산안 편성 지침 중 사업유형별 지침에는 주요 사업유형 외에 인건비, 기본경비, 총액인건비, 출연·보조기관 인건비 및 경상비, 수입대체경비를 포함하여 전체 24개의 항목으로 이루어져 있으며 Table 1과 같다[3].

또한 예산 관리의 편의를 위해 기능별 분류와 목별 분류를 모두 사용하고 있으며, 기능별 분류는 정부가 수행하는 기능에 초점을 맞춘 분류이고, 목별 분류는 예산의 지출 대상에 초점을 맞춘 분류이다. 기능별로는 약 12개의 항목으로 구성되며 분류는 Table 2와 같고, 목별로는 7개의 항목으로 구성되며 분류는 Table 3과 같다[4].

Table 2. Functional Classifications in Korea

no.	Sector	no.	Sector
1	General & Local Administration	9	Health
2	Public Order and Safety	10	Agriculture, Forestry, Maritime Affairs & Fisheries
3	National Unification & Foreign Affairs	11	Industry & Small and Medium Enterprise & Energy
4	National Defense	12	Traffic and Physical Distribution
5	Education	13	Communication
6	Culture & Tourism	14	National Land & Regional Development
7	Environmental Protection	15	Science & Technology
8	Social Welfare	16	Reserve Funds

Table 3. Object Classifications in Korea

no.	Sector
1	Personnel Expenses
2	Goods Services
3	Current Transfers
4	Asset Acquisition
5	Repayment of Loans
6	Transfers
7	Contingency & Others

2.2 정보화 및 정보보호 예산 현황

한국의 정보보호 예산은 2000년대 이후로 지속적으로 증가했으나 초반에는 정보화 예산의 1% 내외의 수준이었다. 정보화 사업에서 정보시스템 보호를 위한 예산을 포함하여 요구하도록 하는 수준에서 2008년에 정보보호 강화를 위한 예산이 보다 명확하게 정의되고, 항목 또한 구체화되었다[5]. 2017년에는 정보보호 예산 내역표의 항목이 미래창조부의 「2016년 국가 정보화 시행계획」의 정보보호솔루션과 통일성을 갖고, 최근 동향을 반영할 수 있도록 수정·보완되었다[2].

그러나 주요 기반시설에 대한 사이버 공격 및 개인정보 유출 등 사이버 공격에 대한 피해 범위와 규모의 확산에 비해 한국의 정보보호 예산은 이후에도 소폭 상승하는 데에 그쳤다. 최근 4년 동안 미국 정부는 자국의 정보보호 역량 강화를 위해 평균 13% 이상 정보보호 예산 증액을 추진하였다. 그러나 한국의 최근 4년 동안의 정보보호 예산 증액 비율의 평균은 4%로 소폭 증가한 것을 알 수 있다. 정보보호 예산이 정보화 예산의 1% 대에 머물렀던 2004년부터 2015년까지 비교해도 12% 대의 낮은 증액율을 보였다. 2004년부터 2015년까지 한국의 정보보호 예산 현황은 Table 4와 같다[6-8].

2010년에는 2009년 '7.7 DDoS' 사건을 계기로 사이버테러 대응을 위한 정보보호 분야에 투자가 확

Table 4. IT and Information Security Budget Situation in Korea (unit - billion won)

	IT budget	Information Security budget	Percentage of Information Security budget to IT budget
2004	28,445	364	1.2%
2005	29,052	363	1.2%
2006	34,343	450	1.3%
2007	34,104	1,018	2.9%
2008	34,048	1,608	4.7%
2009	31,378	1,742	5.5%
2010	32,869	2,702	8.2%
2011	32,897	2,034	6.1%
2012	33,053	2,633	7.9%
2013	32,967	2,402	7.2%
2014	39,404	2,460	6.2%
2015	41,070	2,543	6.2%

대되어 2,702억원으로 2000년대 이후로 가장 높은 예산이 편성되었다. 그러나 이후 하향세를 보이다가 2012년에 다시 투자가 확대되었는데 2011년에 발생한 '3.4 DDoS' 침해사건 역시 2012년에 정보보호 예산을 확대하는데 일정부분 기여했을 것이라 사료된다. 이후 정보보호 예산은 2013년에 다시 감소했다가 최근에 다시 소폭 상승하였다.

이처럼 한국의 정보보호 예산은 장기적인 계획을 가지고, 우선순위를 두고 투자를 확대해 나가기보다는 사고가 발생한 뒤 일시적으로 정보보호에 대한 투자를 확대하고, 다시 우선순위가 낮아지면 예산이 감소하는 들쭉날쭉한 편성이 이루어지고 있다.

또한 한국의 정보보호 예산 부족 문제는 정보보호의 공공분문 통계에서도 나타난다. Table 5의 국가정보보호 백서의 공공부문 통계에 나타난 공공기관에 정보보호 전담 조직이 신설되지 못하는 이유로 예산·인력 부족이 2015년 92.7%로 가장 높은 비율을 차지했다. 뿐만 아니라 Table 6의 실무에 종사하는 정보보호 담당자의 정보보호 업무 수행 중 가장 큰 어려움에서도 예산·인력 부족이 과반수이상인 54.5% 차지했다. 정보보호 인식 부족에 대한 어려움은 지속적으로 줄어드는 반면 예산·인력 부족으로 인한 어려움은 지속적으로 늘어나고 있는 것을 알 수 있다[9-11].

정보보호를 차세대 국가 먹거리산업으로 선정하고, 육성해 나가겠다는 정부 정책의 실제 정보보호 예산에 대한 반영은 아직 미미한 것으로 보인다. 정부가 공공기관 및 기업에 정보보호를 투자가 아닌 비용으로 인식할 수 있도록 개선을 촉구했지만 정부 스스로도 이에 대한 인식이 명확한지에 대해서는 다시 한 번 생각해 볼 문제이다.

Table 5. The reason why organization dedicated for information security is not established

	2013	2014	2015
shortage of budget·manpower	85.2%	88.1%	92.7%

Table 6. Difficulties in performing the information security work

	Shortage of budget·manpower	Shortage of awareness
2011	35%	40.8%
2012	41.7%	44.2%
2013	48.7%	42.6%
2014	55%	33.9%
2015	54.5%	39.7%

2.3 정보화 및 정보보호 예산 편성 방안 변화

한국의 정보보호 예산은 기획재정부의 「예산안 편성 및 기금운용계획안 작성 세부지침」에 근거하여 정보화 사업 내에서 공공·민간 정보화 지원 및 정보화 역기능 방지를 위해 요구하도록 분류되어 있다. 공공·민간 정보화 지원 및 정보화 역기능 방지 대상에는 정보보호 강화 외에 정보화 관련 표준화, 기술개발, 인력양성, 네트워크 구축, 전파관리, ICT 산업 기반조성, 정보격차 해소 등이 포함된다. 이에 따라 정보시스템 구축·운영 시 정보보호 예산을 포함하여 요구해야 한다[3].

한국의 정보화 및 정보보호 예산 편성 방안의 변화는 최근 10년 중 주요한 변화가 있었던 2008년과 2017년을 중심으로 분석하였고, 2009년, 2010년, 2012년, 2013년, 2014년 정보보호 예산 편성 지침은 예년과 큰 변화가 없는 것으로 나타났다.

2.3.1 2007년

2007년 예산안 세부지침에서는 전자문서의 위·변조 및 해킹·컴퓨터 바이러스 등 외부위협으로부터의 정보시스템 보호 예산을 포함하여 요구하도록 정의하였다[12]. 그리고 세부 작성 지침에서 S/W 구입비 항목으로 정보시스템 보호를 위해 사용하는 보안 S/W, 백업용 툴 등의 시스템 S/W 구입 시 정보화 예산을 활용할 수 있도록 하였다[12].

그러나 예산을 요구할 수 있는 정보시스템 보호 영역이 외부의 사이버 위협에 대한 전자문서 및 정보시스템 보호로 정의되어 있어 일반적인 정보보안 업무 범위를 포괄하기에는 한계가 있고[13], 세부적인 예산 요구 내역이 없어 각급기관에서 활용하는데 어려움이 있었다.

2.3.2 2008년

2008년에는 정보보호 예산에 대한 지침을 보다 명확하게 규정하였다. 기존의 정보화 예산의 적용 대상에 정보화 역기능 방지 사업을 신설하고, 그 중 한 가지로 정보보호 강화를 선정하였다. 또한 정보보호

예산 내역표를 신설하고, 제출을 의무화하여 보다 구체적으로 정보보호 예산을 요구하도록 하고, 각급기관에서 정보보호 예산 요구 시 고려해야할 항목을 제시하였다. 정보보호 예산 내역표의 항목은 컨텐츠 보안·네트워크 보안·정보보호서비스 등으로 이루어져 있고 세부항목은 Table 7과 같다[14].

2.3.3 2011년

2011년에는 예산을 요구할 수 있는 시스템 SW 항목에 서버보안, DB 보안, DB 접근제어, DB 모니터링, 백업 SW, 관제 SW, WAS(Web Application Server) 모니터링, HA(High Availability)용 SW를 추가하여 정보시스템 신규 구축 및 고도화 시 고려해야할 보안 관련 시스템 SW 항목의 범위를 넓혔다[15].

또한 정보보호 예산 내역표의 네트워크 보안에서 PC 통합 보안을 위한 PC통합보안(NAC, Network Access Control) 항목이 추가되었다.

Table 7. 2008 Information Security Budget Portfolio

Section	Type	Description
Contents Security	DB Security	DB Security
	DRM(Digital rights management)	DRM
	Privacy Protection	Security Server
	Data Backup	Data Backup System
System Security	User Authentication	Security Smart Card
		HW Token
		OTP
		Bio Recognition
	Anti Virus/Spam	Anti-Virus
		Anti-Spyware
		Spam Filtering SW
	Access Control	Secure OS
		EAM
		SSO
		IM/IAM
Network Security	Firewall System	Network Firewall
		System Firewall
		PC Firewall
		Web Firewall
	IDS	IDS, IPS
	VPN	VPN
	Electronic Signature	PKI
	Wireless/Mobile Security	Wireless/Mobile Security
	DDos Device	DDos Device
Information Security Service	Security Management	UTM
		TMS
		ESM
		PMS
		Log Management Tool
		PC Security(USB)
	Authentication Service	Public/Private Authentication Service
	Security Management Service	Security Management Service
	Security Consulting	Security Consulting
	Maintenance	Maintenance
	Rent	Device/SW Rent
	Etc.	Vulnerability Analysis Tool
		Education, Training
Etc.		Other Security Products, Service, Research and Development

2.3.4 2012년

2012년에는 2011년에 개인정보 유출과 오남용 방지를 위해 시행된 「개인정보보호법」에 따른 안전조치의무 이행을 위한 소요 경비에 대한 마련할 수 있도록 예산 세부지침이 개정되었다[16]. 이에 따라 각급기관은 정보화 예산 요구 시 기존의 정보시스템 보호를 위한 예산뿐만 아니라 정보시스템 중 개인정보를 수집 및 활용하는 시스템은 영향평가 등 개인정보보호법에 명시된 안전조치의무 사항을 고려하여 요구하도록 하였다.

2.3.5 2017년

2016년 4월에 발표된 「2017년 예산안 편성 및 기금운용계획안 작성 세부지침」에서는 정보보호 예산을 정보화 사업에서 기획·구축·운영 등의 예산과 구분하여 정보보호 예산 내역표에 포함된 사항을 구체적으로 작성하여 제출하도록 명시하였다[3].

또한 정보보호 예산 내역표와 「정보보호산업 진흥법」의 시행에 따라 작성된 국가 정보화 시행계획의 정보보호솔루션과 통일성을 갖도록 수정·보완이 이루어졌다. 변경된 정보보호 예산 내역표는 정보보호 제

Table 8. 2017 Information Security Budget Portfolio

Category	Section	Type	Description
Information Security Product	Information Security	Network Security	Web Firewall
			Network(System) Firewall
			IPS
			DDoS Prevention System
			UTM
			VPN
			NAC
			Wireless Network Security
			Virtualization(Network Partition)
		System Security	System Access Control(including PC Firewall)
			Anti Malware
			Spam Prevention SW
			Secure OS
			APT Response
			Mobile Security
		Contents(Data)/Information Leak Detection and Prevention	DB Security
			DB Password
			Security USB
			DRM
			Network DLP
			Device DLP
		Cryptograph/Authentication	Security Smart Card
			HW Token(HSM)
			OTP
			PKI
			EAM/SSO
			IM/IAM
		Security Management	ESM
			TMS
			PMS
			RMS
			Back up/Recovery Management System
			Log Management/Analysis System
			Vulnerability Analysis Tool
			Digital Forensic System
		Etc.	Other Information Security Products

Category	Section	Type	Description
	Physical Security	CCTV	CCTV System(Storage Device, Camera, Video Surveillance SW·Device, Intelligence Solution, Accessory)
		Bio Recognition	Face Recognition
			Fingerprint Recognition
			Iris Recognition
			Vein Recognition
			Etc.(Voice Recognition and Etc.)
		Access Control	Card & Reader(Number/Magnetic), Security Gate·SW
		Alarm Monitoring	Infrared Ray/Laser /Vibration/Tension Sensor, Motion Detector/IDS equipment
		Etc.	Other Physical Security Products
Information Service	Information Security Service	Management	Product Update, Technical Support
		Operating Cost	Information Security Product Operating Cost
		Sustainable security Service	Security Update, Security Policy Management, Threat/Accident Analysis, Security Audit(CC, KCVMP), Effective Maintenance, Technical Advice
		Security Monitoring	Remote Monitoring Service
			Detachment Monitoring Service
		Security Consulting	ISO, ISMS
			Infrastructure Security
			Diagnosis·Penetration Test
			Privacy Security Consulting
			Total Security Consulting
			Information Audit
		Education/Training	Education/Training Service
		Authentication Service	Authentication Service(Public/Private, CC Audit Authentication)
		Etc.	Information Security System Operation
	Physical Security Service	Video security service	
		Other security service	
Etc.			Other Security Products, Service, Research and Development

품과 정보보호 서비스, 기타로 분류하고, 정보보호 제품에는 정보보안 제품 및 물리보안 제품이 포함되고, 정보보호 서비스는 정보보안 서비스 및 물리보안 서비스를 포함한다. 세부항목은 Table 8과 같다[3].

정보보호 예산 내역표는 2008년에 신설된 이후로 2016년까지 큰 변화 없이 유지되다가 2017년에 가장 큰 폭으로 개정되었다. 새로운 정보보호 기술 동향을 반영한 시스템 및 서비스 항목이 추가되고, 보안 업무의 특성을 반영하여 단순 유지관리 및 관제가 아닌 각 기관의 보안을 지속하기 위한 서비스 항목을 신설하였다. 또한 정보보안 시스템을 위한 물리보안 제품 및 서비스 항목이 추가된 것이 기존 정보보호 예산 내역표와의 차이점이다.

III. 미국의 정보화 및 정보보호 예산

3.1 예산 개요

미국의 예산 편성은 입법부의 교유권한으로 행정부가 제출하는 대통령 예산안은 의회 예산 심의의 참고 자료로 활용되나, 입법부는 무제한 수정권한 및

독자적 예산 편성권을 가진다.

예산 편성 과정은 먼저 관리예산처(OMB: Office of Budget and Management)가 예산편성지침(Call for Estimates)을 각 연방기관에 하달하고, 모든 연방정부기관은 각 기관의 예산요구서를 작성하여 OMB에 제출한다. OMB는 제출된 예산요구서를 심의하여 현안을 파악하고, 경제전망, 업무 성과평가 등을 반영하여 예산 조정 및 협의 하여 예산결의안을 마련한다. 의회는 예산결의안을 심의하고, 확정된 예산이 최종적으로 집행된다.

한국과 유사하게 프로그램예산제도를 택하고 있으며, 각 연방기관 및 부처는 프로그램 기반으로 예산을 요구하고 프로그램에 대한 성과평가를 수행한다.

예산은 기능별로 약 20개의 항목으로 구성되며 분류는 Table 9와 같고, 목별 분류는 5개의 항목으로 구성되며 분류는 Table 10과 같다[17].

Table 9. Budget Functional Classifications

no.	Item	no.	Item
1	National Defense	11	Health
2	International Affairs	12	Medicare
3	General Science, Space and Technology	13	Income Security
4	Energy	14	Social Security
5	Natural Resources and Environment	15	Veterans Benefits and Services
6	Agriculture	16	Administration of Justice
7	Commerce and Housing Credit	17	General Government
8	Transportation	18	Net Interest
9	Community and Regional Development	19	Allowances
10	Education, Training, Employment, and Social Services	20	Undistributed Offsetting Receipts

Table 10. Budget Object Classifications

no.	item
1	Personnel Services and Benefits
2	Contractual services and Supplies
3	Acquisition of Capital Assets
4	Grants and Fixed Charges
5	Other

3.2 정보화 및 정보보호 예산 현황

미국 연방정부의 정보화 및 정보보호 예산 규모는 Table 11과 같다. 정보화 예산은 2012년(회계연도 2013년) 805.7억달러에서 2016년 898.5억달러로 매년 평균 2.6%의 비율로 증가하였다[18-21].

또한 미국 연방정부의 정보보호 예산은 정보보호의 중요성에 대한 강조와 함께 지속적으로 증가하고 있으며, 2012년 이후로는 IT 예산의 10%의 비율로 편성되고 있다. 특히 2016년에는 190억달러가 편성되어 정보화 예산의 21%를 차지하였다[22-25].

Table 11. IT and Information Security Budget Situation in U.S. (unit - billion USD)

	IT Budget	Information Security Budget	Percentage of Information Security budget to IT budget
2012	8057	10.3	12.7%
2013	8139	12.7	15.6%
2014	8417	13.1	15.5%
2015	8871	14.0	15.7%
2016	8985	19.0	21.1%

3.3 정보화 및 정보보호 예산 편성 방안 변화

미국의 정보화 및 정보보호 예산은 2000년대 이후로도 지속적으로 증가하고 있으며, 정보화 예산은 주요 IT 예산 항목 6가지와 투자 형태 4가지로 분류되는 기본적인 틀은 유지되고, 하위 항목은 해당연도의 필요에 따라 변경되고 있다. 또한 대통령의 관리방향과 부합되는 효과적인 IT 투자 항목을 선정하여 국가 전체적인 정보화 예산 방향을 제시한다.

미국 정보화 및 정보보호 예산 편성 방안의 변화는 최근 10년 중 주요한 변화가 있었던 2008년과 2010년, 2013년, 2015년을 중심으로 분석하였다.

3.3.1 2008년

2008년 주요 IT 예산 항목은 미국 관리예산처 회람 A-11의 Exhibit 53A에 정의되어 있으며, 연방정부 및 부처에 IT 예산 투자 내역인 IT 투자 포트폴리오 제출을 의무화하였다[26].

IT 예산 투자 항목 6가지는 Table 12와 같고,

Table 12. 2008 IT Investment Major Part

no.	part
1	IT investments for Mission Area Support
2	IT investments for Infrastructure, Office Automation, and Telecommunications
3	IT investments for Enterprise Architecture and Planning
4	IT investments for Grant Management Systems
5	Grants to State and Local IT investments
6	Nation Security Systems IT investments

정보보호는 이 중 1번과 2번 항목에 포함되어 요구된다.

투자 형태는 4가지로 첫 번째는 주요 IT 투자, 두 번째는 비주요 IT 투자, 세 번째는 대규모 자산의 IT 마이그레이션(migration)을 위한 투자, 네 번째는 기관간 협력을 위한 자금으로 분류된다.

또한 대통령의 관리 방향과 부합하는 효과적인 IT 투자 항목 9가지 중 3가지를 정보보호 관련 항목으로 선정하여 정보보호에 대한 예산 투자 확대를 활성화하였다. 선정된 3가지 항목은 첫째, 연방 정보 시스템 보안과 정보보호 시스템 구축, 둘째 IT 투자와 시스템에 대한 인증과 신임 획득, 셋째, 개인의 정보보호 보장을 위한 전자 활동 이행이다[26].

그리고 IT 예산과 IT 보안 예산을 분리하여 세부 IT 투자 시 IT 보안 대비를 위한 상품, 절차, 인력(연방정부 인력 또는 계약 인력)을 할당한 예산을 함께 산정하도록 하여 정보보호 인력에 대한 실태를 파악하고, 현재연도와 회계연도의 정보보호 예산 비율을 필수적으로 표기하도록 하여 정보보호 예산을 확대할 수 있도록 장려하였다.

또한 IT 보안 예산 항목 분류를 제공하여 IT 시스템 활용 시 필수적으로 고려하도록 권고하였다. IT 보안 예산 항목은 총 13가지 항목으로 분류되어 있으며 항목과 관련된 제품, 절차, 인력을 모두 포함한다. 세부적인 항목은 Table 13과 같다[26].

Table 13. 2008 IT Security Portfolio

no.	criteria
1	Risk assessment
2	Security planning and policy
3	Certification and accreditation
4	Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
5	Authentication or cryptographic applications
6	Education, awareness, and training
7	System reviews/evaluations
8	Oversight or compliance inspections
9	Contingency planning and testing
10	Physical and environmental controls for hardware and software
11	Auditing and monitoring
12	Computer security investigations and forensics
13	Reviews, inspections, audits and other evaluations performed on contractor facilities and operations

3.3.2 2010년

2010년에는 기본적으로 주요 IT 예산 항목과 투자 형태는 2008년과 동일하나 IT 보안 예산 항목 내역표를 신설하고, 2008년에 비하여 IT 보안 예산 항목을 보다 구체적으로 선정하여 요구하도록 하였다. IT 보안 예산 항목 내역표의 세부 항목은 Table 14와 같다[27].

공무원뿐만 아니라 계약직 직원에 대한 인건비 또한 예산 항목으로 도출하여 보다 정확한 보안 인력 현황을 파악하고, 추가적인 인력 편성을 위한 예산 확보 기반을 마련하였다.

2010년에는 대통령의 관리 방향과 부합하는 효과적인 IT 투자 항목에 정보보호 관련 항목은 선정되지 않았다.

Table 14. 2010 IT Security Portfolio

no.	criteria
1	Average cost per Government FTE(Full-time equivalent)
2	Average cost per Contractor FTE
3	Total IT Security Tools Costs
4	Anti-Virus Software Licensing Costs
5	Anti-Malware Software Licensing Costs
6	Intrusion Detection Systems Licensing Costs

no.	criteria
7	Intrusion Prevention Systems Licensing Costs
8	Web Filtering Software Licensing Costs
9	Email Filtering Software
10	SIM/SIEM tools
11	Data Leakage Protection tools
12	Costs for NIST 800-37 implementation
13	Costs for annual FISMA testing
14	Costs for network penetration testing activities
15	Security awareness training costs
16	Security training costs for employees with significant security responsibilities

3.3.3 2012년

2012년에는 주요 IT 예산 항목 중 다른 항목은 예년과 동일하고, 기반시설을 위한 IT 투자·사무 자동화· 통신 관련 항목에 IT 보안이 추가되었다[28].

또한 IT 보안 예산 항목 내역표의 항목을 간소화하여 2010년도에 별도 항목으로 분리되어 있었던 안티 바이러스 소프트웨어 라이선스 비용, 안티 맬웨어 소프트웨어 라이선스 비용, 침입 탐지 시스템(IDS) 라이선스 비용, 침입 예방 소프트웨어(IPS) 라이선스 비용, 웹 필터링 소프트웨어 라이선스 비용, 이메일 필터링 소프트웨어, SIM/SIEM 도구, 데이터 유출 방지 도구를 Table 15의 3번 항목인 전체 IT 보안 도구 비용에 통합하여 요구하도록 하였다.

대통령의 관리 방향과 부합하는 효과적인 IT 투자 항목으로 사이버보안 강화를 선정하고, 세부적으로는 증가하는 정교한 위협 환경과 비상상황 예방을 위한

Table 15. 2012 IT Security Portfolio

no.	criteria
1	Average cost per Government FTE(Full-time equivalent)
2	Average cost per Contractor FTE
3	Total IT Security Tools Costs
4	Costs for NIST 800-37 implementation
5	Costs for annual FISMA testing
6	Costs for network penetration testing activities
7	Security awareness training costs
8	Security training costs for employees with significant security responsibilities

혁신적인 솔루션 개발, 사이버보안을 위한 기관간 우선순위 목표 실행을 위한 책무, 정보보호 성능 향상을 위한 지속적인 기관 진행상황 평가를 위한 투자를 권장하였다[28].

3.3.4 2013년

2013년에는 주요 IT 예산 항목 외에 추가적으로 제출을 요청하던 IT 보안 예산 항목 내역표가 삭제되고, 별도의 요청에 의한 제출로 수정되었다.

주요 IT 예산 항목은 다른 항목은 예년과 동일하고, 세 번째 항목인 전사 아키텍쳐를 위한 IT 투자 외에 자금 계획, CIO(Chief Information Officer) 기능 강화를 위한 IT 투자 항목이 추가되었다[29].

3.3.5 2015년

2015년에는 주요 IT 예산 항목 중 IT 보안이 포함된 두 번째 항목인 IT 기반 시설비용 항목의 분류안이 신설되었다. 분류안은 크게 데이터 센터, 통신, 사용자 항목으로 분류되고, 그 중 데이터 센터와 통신 항목에 보안 관련 비용을 요구할 수 있도록 하였다[30].

첫 번째 데이터 센터 대분류의 데이터 센터 소프트웨어 항목에 보안 SW 항목이 포함되었고, 데이터 센터 마이그레이션 항목에 보안 인증 및 재인증 항목을 신설하여 데이터 마이그레이션 시 보안을 필수적으로 고려하도록 하였다. 통신 대분류에서는 데이터 통신 항목에 네트워크 신뢰성 확보를 위해 신뢰성 있는 인터넷 연결 인프라(인터넷 트래픽을 위한 통합 및 보안 계층 제공) 항목을 추가하였다[30].

IV. 한국과 미국의 정보보호 예산 비교 및 한국 정보보호 예산 편성 방안 문제점 분석

한국과 미국은 예산은 기본적으로 OECD와 IMF의 국가 예산에 관한 정책권고와 가이드라인에 기준하여 편성되었기에 유사한 구조를 갖추고 있다.

한국과 미국은 모두 법률에 기반한 예산법률주의로 근거법률의 종류에 따라 세출이 달라지며, 성과주의 예산제도를 도입하고, 예산의 효율적 집행 및 관리를 위한 프로그램예산제도를 도입하고 있다. 기능별 분류, 목별 분류 또한 각 나라의 정치적 특성을

반영하고 있기에 근소한 차이를 보이고 있지만 전체적으로는 유사한 구조로 이루어져 있다.

정보보호 예산도 세부적인 내용은 다르지만, 정보화 예산에서 정보보호 예산 내역표에 근거한 예산 요구 방식을 취하고 있어 기본적인 골격은 유사하다. 미국의 정보보호 예산 제도가 한국의 현실에 비추어 반드시 옳은 것은 아니지만, 한국과 유사한 정보보호 예산 구조를 가지면서 정보보호 분야 선진국가로 자리매김하고 있기에 한국의 정보보호 예산 제도의 문제점을 분석하고, 개선 방안을 마련하는 데 있어 참고자료로서는 충분한 가치를 가지고 있다. 이에 미국 정보보호 예산 구조에 기반하여 한국의 정보보호 예산 제도를 비교·분석한 결과 예산 규모, 정보화 예산과의 분리 구조, 인건비 편성 방안, 예산 항목에서 다소 차이를 보였다.

4.1 정보보호 예산 규모

미국의 정보화 예산 증가폭은 과거에 비해 둔화된 반면 정보보호에 대한 예산은 높은 폭으로 증가되고 있다. Table 16은 미국의 최근 4년간 정보화 예산 증가율과 정보보호 예산 증가율이다. 평균적으로 정보화 예산은 2.7% 증가된 반면 정보보호는 13.7%로 두 자리 수 이상의 성장세를 기록하고 있다. 이는 미국이 정보보호에 대한 중요성을 인식하고, 장기적으로 정보보호에 대한 투자를 강화해 나가는 것을 나타낸다.

또한 미국은 연방정부에서 정보보호 담당 업무를 수행하는 두 축인 사이버 사령부와 DHS의 정보보호에 대한 예산이 모두 지속적으로 증가하고 있고, 이를 통해 미국이 국방 분야뿐만 아니라 민간 분야에 대한 정보보호를 위해서도 꾸준히 예산을 투자하고, 각급기관 및 지자체에 정보보호 중요성을 강조하고 있다는 것을 알 수 있다.

이에 비해 한국은 최근 4년 동안의 정보보호 예산이 정보화 예산 대비 6-7%에 머물고 있다. Table 17은 한국의 최근 4년간 정보화 예산 증가율과 정보보호 예산 증가율이다. 평균적으로 정보화 예산은 5.2% 증가되었으며, 정보보호 예산 또한 4.7%로 한 자리 수로 소폭 성장하고 있다. 또한 정보보호 예산 증가율이 일정하지 않고, 사고 발생 시 일시적으로 대폭 증액되었다가 다시 감소하는 등 예산 편성에 일관성이 결여되어 있다는 것을 알 수 있다.

이러한 정부의 예산 투자는 정부기관 및 부처에서 정보보호의 중요성에 대한 인식을 강화하는데 부정적인 영향을 줄 수 있으며, 정보보호를 위한 장기적인 계획 수립 및 업무 수행에도 어려움을 야기한다.

Table 16. IT and Information Security Budget Increasing Rate in U.S.

	IT Budget increasing rate	Information Security Budget increasing rate
2013	1%	18.9%
2014	3.34%	3.1%
2015	5.1%	6.4%
2016	1.3%	26.3%
avg.	2.7%	13.7%

Table 17. IT and Information Security Budget Increasing Rate in Korea

	IT Budget increasing rate	Information Security Budget increasing rate
2013	0.5%	22.7%
2014	-0.3%	-9.6%
2015	16.3%	2.4%
2016	4.1%	3.3%
avg.	5.2%	4.7%

4.2 정보화·정보보호 예산 구조

미국은 정보보호 예산에 대한 인식 변경과 실태 파악 및 예산 확대를 위해 정보화 예산 대비 정보보호 예산 비율 제출을 의무화하고, 각 정부기관과 주에서 정보화 투자 시 일정 비율 이상을 정보보호 예산으로 편성하도록 하여 정보보호 예산에 대한 인식을 비용이 아닌 투자로 전환함으로써 정보보호를 강화하고자 하였다.

또한 IT 보안 예산 항목 분류표를 제공하여 IT 보안 예산 편성 시 필수 고려항목을 제시하고, 구체적인 예산 규모 파악과 실태 분석을 가능하게 하였다.

그러나 최근 정보보호 예산은 확대된 반면 정보화와 정보보호 예산의 분리가 명확하게 하지 않고, 연방정부 및 부처에서 경계를 유연하게 조절할 수 있도록 변화하는 경향이 나타나고 있다. 2013년부터 정보보호 예산 항목은 정보화 예산 제출 시 별도로 제출하지 않고, 정보보호 예산 내역으로 제출하던 IT 보안 예산 항목 내역표가 삭제되었다. 또한 정보보호 예산을 정보화 예산 내에서 요구되도록 다시 개편하고, 보안 예산은 추후 별도의 요청을 통해 제출하도

록 변경된 데에서 이와 같은 경향을 확인할 수 있다.

이는 정보보호의 특성상 정보화와 완전한 분리가 어렵고, 정보화 시스템 구축 시 함께 이루어지는 등 긴밀한 관계를 맺고 있기 때문에 정보화 예산 내에서 요구되는 것이 보다 효율적이라는 판단에서 기인한 것으로 사료된다.

한국 또한 정보화 예산과 정보보호 예산의 분리 기준이 모호한데, 미국과 다르게 실질적인 정보보호 예산 규모에 대한 파악과 실태 분석 없어 정보보호 예산 현실화 이루어지지 않은 상태이다. 또한 예산 편성 지침에 제시된 정보보호 예산 내역표의 보안 시스템 및 서비스에 국한되어 정확한 정보보호 예산 규모 파악을 어렵게 한다는 문제점을 가지고 있다.

단편적인 예를 들자면, 정보보호 업무를 위한 PC의 노후로 인한 교체이다. 현재의 정보보호 예산 편성 지침에는 PC 교체 비용을 정보화 예산으로 편성할 것인지, 정보보호 예산으로 편성할 것인지에 대한 명확한 기준이 없으며, 각급기관의 자율적 판단에 따라 예산이 요구되고 있어 정보화 예산으로 편성이 가능하고, 정보보호 예산으로도 편성이 가능하다. 이러한 편성 기준의 모호함은 실질적으로 각급기관에서 필요로 하는 정보보호 예산 실태 분석을 어렵게 하고, 결과적으로 정보보호 예산 확대에 한계를 가져올 수 있다.

또한 정보화 사업 내 정보보호 예산 편성 구조에서는 정보화 사업 추진 계획에 따라 정보보호 예산도 편성 및 조정되기 때문에 정보보호 계획 및 정책에 따른 정보보호 예산 편성에도 어려움을 초래한다.

4.3 정보보호 인력 인건비 편성 방안

한국과 미국의 사업(프로그램) 유형이 달라 정보보호 인력에 대한 인건비 편성 구조에서 차이점을 보이고 있다.

미국의 경우 프로그램은 연방기관 및 부처의 과제 중심으로 프로그램 별로 인건비 비목을 두고, 정규인력 및 계약인력에 대한 인건비를 편성하도록 되어있다. 반면 한국의 경우 예산을 인건비, 기본경비, 주요사업비로 구분하고, 사업유형별 지침에 사업 외에 인건비, 기본경비, 총액인건비, 출연·보조기관 인건비 및 경상비 등 사업에 관계없이 공무원 및 정부기관 인력에 대한 인건비가 지급될 수 있도록 별도의 항목을 두고 있다. 기본경비에는 이들 인력을 위한 교육훈련비 및 전산장비 구입비용이 포함된다. 따라서 한국은 사업에 대한 예산 편성 시 인건비는 별도로 편성하도록 되어있다는 점에서 미국의 예산 구조와 차이점을 가지고 있다.

이와 같은 인건비 편성 구조에서는 정보보호 예산이 정보화 사업 내에서 요구되도록 되어있어 별도의 인건비, 기본경비를 요구할 수 있는 기반이 마련되어 있지 않다는 문제점이 있다. 정부가 주도적으로 정보보호 인력 확대 시 인건비 항목으로 편성할 수 있지만 부처 및 기관의 수요에 따른 정보보호 전담 조직 시설 및 신규 인력 채용 및 이들 인력에 대한 교육훈련 예산 편성에는 어려움이 있다.

4.4 예산 항목 범위

미국은 각급기관에서 정보보호 예산 요구 시 정보보호 도구, 서비스에 대한 비용 외에도 정보보호 업무 수행을 위한 인건비, 정보보호 인식제고 및 교육·훈련 비용, 시스템 평가, FISMA 체계 이행 비용, 위험 관리 체계 구축에 대한 평가·감사에 대한 비용을 포함하는 포괄적인 예산을 요구할 수 있도록 IT 보안 예산 내역표를 제시하였다.

반면, 한국의 예산 편성 지침에 제시된 정보보호 예산 내역표는 보안 시스템 및 서비스에 대하여 예산 편성이 가능한 체계를 가지고 있다. 이로 인하여 정보보호 업무 수행을 위한 보안 시스템 및 서비스 항목의 예산은 세분화된 반면 정보보호 계획 및 정책수립·개선을 위한 예산 항목, 교육 및 인력 확보를 위한 예산 항목 등 각급기관의 전체적인 정보보호 체계 구축을 위한 예산 항목이 부재하다는 문제점이 있다. 또한 지속적인 정보보호 수행을 위한 정보보호 실태 평가 및 감사를 위한 예산 편성 항목도 마련되어 있지 않다.

이는 각급기관의 주도적인 정보보호 체계 구축 및 정책 수립 및 자체 역량 강화를 어렵게 하고, 각급기관의 정보보호에 대한 책임감 결여와 정보보호를 필수적인 기본사항이 아닌 정보화에 따른 부가적인 사항으로의 인식을 야기할 수 있다.

V. 한국의 정보보호 예산 확대 및 개선 방안

5.1 정보화·정보보호 예산 분리 편성

정보보호 예산 확대를 위해서는 기본적으로 정보화와 정보보호의 예산 분리가 필요하다. 예산 분리는

해당 항목에 대한 예산 실태 파악하고, 투자 확대를 가능하게 하여 정부는 정보보호 예산 분리 외에도 세월호 참사를 계기로 안전 예산 실태 파악 및 투자 확대를 위해 2015년 예산 편성과정에서 재난 ·안전 예산을 일반 예산과 분리하여 별도로 관리하도록 추진한 바 있다.

재난·안전 예산은 재난·안전 시스템 관리 및 장비 확충하고, 대국민 인식 제고를 위한 비용으로 대형 재난 예방을 위한 예산이다. 재난·안전 예산으로 분리되기 이전 기존의 안전 예산은 OECD를 비롯한 국제기구가 공인한 국가재정운용계획 상에서 공공질서 및 안전 예산에 포함되어 있었으나 법원과 검찰, 경찰·해양경찰, 소방방재청 등 안전 분야 담당 부처의 예산으로 해당 부처 예산 전체를 재난·안전 예산으로 볼 수 없고 해양수산부와 국토교통부의 안전 관리 예산은 빠져 있는 문제가 있었다. 또한 국가안전관리 기본계획 상의 안전관리 예산은 재해 예비비 등이 포함되어 있으나 재해 복구 예산이 빠져 있어 이 역시 재난 ·안전 예산으로 보기에는 문제가 있다. 이에 정부는 재난·안전 예산을 일반 예산과 분리하여 안전 예산 분류 기준을 명확하게 하고, 안전 예산에 대한 체계적 관리가 가능하도록 하였다[31].

실제로 재난·안전 예산이 분리되고 2015년도 예산에서는 전년대비 17.9%가 증가하였고, 이는 분야별 증가율 중 가장 높은 수준이다[32]. 또한 2016년도 국가 안전 예산이 14조 8천억원으로 선투자 1조원을 포함하면 2015년도에 비해 8% 가량 증가한 것으로 나타났다[33].

정보보호 예산을 정보화 예산에서 분리 편성 시 다음의 2가지 장점을 갖는다.

첫째, 정보보호 예산 현실화 및 확대 기반 마련이 가능하다. 정보보호 예산을 정보화 예산 내에서 분리 편성 시 정보화 예산과 정보보호 예산의 분리 기준의 보다 명확하게 하여 각급기관에서 필요로 하는 실질적인 정보보호 예산 실태 파악을 가능하게 한다. 또한 정보보호 예산이 정보화 예산의 일정 비율 이내로 편성되는 부작용을 없애고, 정보보호를 더 이상 정보화의 역기능 방지에 국한하지 않아 정보보호 가치 재평가 및 예산 확대에 기여할 것이다.

둘째, 정보보호에 대한 장기적 투자 계획 마련이 가능하다. 정보화 사업 추진 시 정보보호에 대한 고려가 필요한 것은 사실이나 정보화 사업 계획과 정보보호 사업 계획이 항상 일치하지는 않으며, 장기적인 정보보호 추진 계획에 대한 고려가 필요하다. 정보화 및 정보보호 예산 분리는 각급기관에서 정보화 사업과 별도로 각급기관의 정보보호 실태에 알맞은 정보보호 계획 수립을 장려하고, 이에 따른 예산 편성을 가능하게 한다. 이는 정보보호 예산의 정보화 사업 추진 계획 변화에 따른 편성 및 재조정과 일시적인 관심에 따른 고무줄 편성 관행을 없애고, 장기적인 투자 계획을 가지고 편성할 수 있도록 하는데 긍정적 영향을 미칠 수 있다.

그러나 미국의 사례에서도 알 수 있듯이 정보보호의 사업 특성상 정보화 사업과 완전한 분리가 어렵다. 때문에 정보화 사업 안에서 현재의 기본적인 정보화·정보보호 예산 구조의 골격을 유지하면서 정보보호 예산에 대한 명확한 기준을 제시하여 정보보호 예산을 분리 편성할 수 있도록 하는 것이 바람직하다.

현재의 예산 편성 방안에서 정보보호의 예산을 정보화 사업 내에서 예산을 요구할 경우에는 다음의 2가지 장점을 갖는다.

첫 번째, 효율적인 사업 관리가 가능하다. 이는 현재의 예산 지침이 사업 단위로 예산을 요구하고, 과제를 관리하고 있기 때문이다. 정보화 사업의 세부사업마다 정보보호 항목을 포함하고 있어 동일 사업에 대해 정보화와 정보보호로 분리하여 2가지 사업으로 예산을 요구할 경우 혼동을 초래할 수 있다.

둘째, 정보화 사업에 대한 낙찰차액을 정보보호에서 활용이 용이하다는 장점을 가지고 있다. 낙찰차액은 사업대상 및 범위의 조정 등으로 인한 예산절감액을 의미하며, 기본적으로 불필요하거나 시급성이 낮은 목적으로 낙찰차액이 사용되는 것을 예방하기 위해 불용이 원칙이다[34]. 그러나 정보화 사업의 낙찰차액은 정보시스템 감리비 또는 정보보호 강화를 위해서는 각급기관이 기획재정부와 협의 없이 활용 가능하도록 허하고 있어 예산이 부족한 정보보호를 위해 사용되고 있다.

따라서 정보화 사업 안에서의 예산 편성의 장점을 활용하면서, 정보보호 예산 확대에 기여가 가능하도록 하는 정보화 및 정보보호 예산 분리 편성 방안이 필요하다. 이를 위해서는 기존의 정보보호 예산 내역표에 따른 예산 요구가 아닌 정보화 사업 내에 항목별 지침의 신설하고, 정보보호 예산의 범위와 기준을 제시하는 것이 바람직하다.

이는 우선적으로는 각급기관의 정보보호 예산 현실화에 기여할 것이고, 이를 통해 정보보호 예산 확대 기반을 마련할 수 있다. 또한 정보보호를 기존의 정보화 역기능과 차별화하고, 정보보호를 단순한 정

보화 역기능 수준이 아닌 독립적인 기능으로 판단할 수 있도록 하여 각급기관에서 정보보호에 대한 가치를 재평가 하는 데 기여할 것으로 보인다.

5.2 정보보호 예산 항목 다양화

5.2.1 정보보호 체계 구축 및 인력 확대를 위한 예산 편성 방안 마련

기존의 정보보호 예산 내역표는 보안 시스템 및 서비스에 집중되어 있어 각급기관에서 주도적으로 정보보호 체계를 구축하고, 역량을 강화할 수 있는 환경을 마련할 수 있도록 세부내역 항목을 신설하거나 다양화하는 것이 바람직하다.

먼저 정보보호 계획·정책 연구 개발을 위한 항목과 종합적인 보안 컨설팅 및 지속적인 정보보호 계획 및 절차 수립을 위한 항목을 신설하여 각급기관에서 기관별 특성을 고려한 정보보호 체계를 구축할 수 있도록 지원할 필요가 있다.

또한 기존의 정보보호 제품 및 서비스에 대한 교육·훈련뿐만 아니라 정보보호 담당자 및 일반 직원의 정보보호 역량 강화를 위한 교육·훈련과 보안 인식 제고를 위한 교육·훈련 확대를 위하여 교육·훈련 분야의 예산 항목을 다양화할 필요가 있다.

무엇보다도 한국 정보보호의 근본적인 문제 해결 및 역량 강화를 위해서는 신규 정보보호 인력 채용을 위한 인건비 및 지속적인 정보보호 인력 양성을 위한 예산 항목 신설이 필요하다. 그러나 현재의 예산 지침의 기본 구조상 인건비와 기본경비가 사업 단위로 요구되도록 되어 있어 현실적으로 인건비에 대한 항목을 정보보호 예산 내역표 신설하기에는 어려움이 있다. 정보보호 인력에 대한 인건비 편성 방안은 이후에도 정보화 예산과 정보보호 예산의 완전한 분리가 이루어질 때까지 지속적인 논의를 통해 모색할 필요가 있겠다.

5.2.2 정보보호 제품 및 서비스 내역표 수정・보완

사이버보안 위협은 시시각각 변화하고 있으며, 이에 대응하는 신규 정보보호 시스템 및 서비스 또한 지속적으로 변화하고 있다.

정보보호 예산 내역표의 항목은 기본적으로는 각급기관에서 정보보호 예산을 요구하기 위해서 활용되지만, 이외에도 각급기관에서 정보보호 체계 구축을 위해 필수적으로 고려해야할 항목들을 제시하는 역할도 함께 수행한다.

2017년 예산 세부지침에서 기존의 정보보호 예산 내역표를 수정·보완하여 새로운 정보보호 제품 및 서비스 동향을 반영한 바 있으나 이는 2008년 이후로 9년 만의 성과이다. 각급기관에서 정보보호 예산 편성 시 정보보호 예산 내역표의 정보보호 제품 및 서비스를 참고하여 각급기관에 최적화된 정보보호 체계 구축 및 업무를 수행할 수 있도록 보안 시스템 및 서비스 항목을 주기적으로 업데이트 할 필요가 있다.

VI. 결 론

모든 것이 연결되는 초연결시대에서 정보보호는 이제 필수불가결한 요소가 되었다. 정보보호가 담보되지 않은 정보화는 무용지물임에도 불구하고, 아직도 한국의 정보보호 예산은 정보화 예산의 1/20 정도에 불과한 극히 일부분만을 차지하고 있을 뿐이다.

이에 비해 정보보호 분야 선진국인 미국은 정보화 예산 대비 정보보호 예산을 1/5로 확대하는 등 정보보호에 대한 중요성을 인식하고 정보보호 분야에 공격적으로 투자하고 있다. 또한 현실성 있는 정보보호 예산 편성을 위해 지속적으로 연방정부 및 부처의 정보보호 예산 실태 파악을 위해 노력하고, 효율적인 정보보호 예산 편성을 위해 정보보호 예산 항목을 수정하는 등 예산 편성 방안을 개선해 나가고 있다.

이에 본 논문에서는 한국의 정보보호 예산 확대 및 개선을 위하여 정보화·정보보호 예산 분리 편성과 협소한 정보보호 예산 항목 범위를 확대하여 정보보호 예산 항목이 일반적인 정보보호 항목까지 포괄할 수 있도록 다양화하는 방안을 제안하였다.

정보화·정보보호 예산 분리는 단기적으로는 한국의 정보보호 예산 실태 파악 및 현실화를 통해 각급기관의 정보보호 역량 강화에 기여하고, 장기적으로는 정보호호 예산 확대 기반 마련에 기여할 것으로 사료된다.

정보보호 예산 항목 다양화는 정보보호 예산을 단순히 정보보호 제품 및 서비스 구매 및 관리가 아닌 각급기관이 장기적인 관점에 정보보호 계획을 세우고, 체계를 구축하는데 예산 활용이 가능하게 한다.

그러나 근본적으로 한국의 정보보호 예산 확대 및 개선을 위해서는 지속적인 정보보호의 중요성과 필요성에 대한 인식이 뒷받침되어야 할 것이다.

또한 제안된 정보보호 예산 개선 방안은 한국과

미국의 정보보호 예산에 대한 비교와 한국 정보보호 예산 실태에 대한 분석 결과에 따른 것으로 객관성 검증을 위해서 정보보호 예산 분리 및 정보보호 예산 기준 명확화라는 정부 정책이 정보보호 예산 제도에 점진적으로 반영되는 과정에서 단계적인 추후 연구를 진행할 예정이다.

References

[1] NIS, "Whitepaper of national Cybersecurity 2015", pp. 10, Apr., 2016.

[2] Sunyoung Choi, "Assessment of Program budgeting System," The Korea Institute of Public Administration, pp. 44, Dec., 2013.

[3] Ministry of Strategy and Finance, "2017 Budget Submission and Execution Plan Guidelines," pp. 15-24, pp. 1-238, Apr., 2016.

[4] Ministry of Strategy and Finance, "Summary of Budget for FY2016," pp.230-236, Feb., 2016.

[5] Ministry of Strategy and Finance, "2008 Budget Submission Guidelines," pp. 138-149, May, 2007.

[6] Youngsun Lee, "Characteristics and implications of national ICT investment," NIA Policy Research, vol. 7, pp. 6, May, 2013.

[7] Ministry of Science ICT and Future Planning, "National institutions·State government, Enhancement of create economy using ICT," MSIP Press, pp. 1-10, Mar., 2014.

[8] Ministry of Science ICT and Future Planning, "National institutions·State government, Investment 5.2 trillion in Information Technology," MSIP Press, pp. 1-5, Jan., 2015.

[9] NIS, "Whitepaper of national Cybersecurity 2014", pp. 304-321, May, 2013.

[10] NIS, "Whitepaper of national Cybersecurity 2015", pp. 274-293, May, 2014.

[11] Ministry of Strategy and Finance, "2007 Budget Submission Guidelines," pp. 166-177, May, 2006.

[12] So Jeong KIM, Seok-jin Choi, Cheol-won Lee, "Study of the way of Institutionalized Budget for Information Security," KIPS-C, 14(2), pp. 115-122, 2007.

[13] Ministry of Strategy and Finance, "2009 Budget Submission Guidelines," pp. 81-92, May, 2008.

[14] Ministry of Strategy and Finance, "2009 Budget Submission Guidelines," pp. 81-92, May, 2008.

[15] Ministry of Strategy and Finance, "2011 Budget Submission Guidelines," pp. 72-83, May, 2010.

[16] Ministry of Strategy and Finance, "2012 Budget Submission Guidelines," pp. 75-86, May, 2011.

[17] Office of Management and Budget, "2015 CIRCULAR NO. A - 11 : PREPARATION, SUBMISSION, AND EXECUTION OF THE BUDGET," pp. 153, pp.228-229, Jun., 2015.

[18] OMB, "Analytical Perspectives-Budget of the U.S. Government:Fiscal Year 2014," pp. 349-358, 2013.

[19] OMB, "Analytical Perspectives-Budget of the U.S. Government:Fiscal Year 2015," pp. 207-301, 2014.

[20] OMB, "Analytical Perspectives-Budget of the U.S. Government:Fiscal Year 2016," pp. 281-285, 2015.

[21] OMB, "Analytical Perspectives-Budget of the U.S. Government:Fiscal Year 2017," pp. 287-292, Feb., 2016.

[22] John Slye, "OMB Reports $13.1 Billion Spent on Cybersecurity in FY 2015," GovWin from Deltek, Apr., 2016.

[23] Steven Roekel, "Federal Information Technology FY 2014 Budget Priorities," OMB, pp. 15, Apr., 2013.

[24] OMB, "The President Budget Fiscal Year

2016-Middle Class Economics:Cybersecurity," pp. 1-3, Jul., 2015.
〔25〕 The White House, "FACT SHEET: Cybersecurity National Action Plan," Feb., 2016.
〔26〕 Office of Management and Budget, "2008 CIRCULAR NO. A-11 : PREPARATION, SUBMISSION, AND EXECUTION OF THE BUDGET," pp. 133-151, Jun., 2008.
〔27〕 Office of Management and Budget, "2010 CIRCULAR NO. A-11 : PREPARATION, SUBMISSION, AND EXECUTION OF THE BUDGET," pp. 137-159, Nov., 2010.
〔28〕 Office of Management and Budget, "2012 GUIDANCE ON EXHIBITS 53 AND 300 - INFORMATION TECHNOLOGY AND E-GOVERNMENT," pp. 1-45, Aug., 2012.
〔29〕 Office of Management and Budget, "2013 GUIDANCE ON EXHIBITS 53 AND 300 - INFORMATION TECHNOLOGY AND E-GOVERNMENT," pp. 1-48, Jul., 2013.
〔30〕 Office of Management and Budget, "FY 2017 IT Budget - Capital Planning Guidance," pp. 1-45, Jun., 2015.
〔31〕 YonhapNews.(2014) "Government, disaster management·safety budgets are separated … separated from general account budgets," Jun., 2014.
〔32〕 Ministry of Strategy and Finance.(2014) "How would we use expanded safety budgets 2.2 trillion won next year?," Sep. 2014.
〔33〕 Safetyin.(2015) "Government safety budgets increased in 2016 by 1.1% 14.8 trillion won," Oct. 2015.
〔34〕 The Ministry of Government Administration and Home Affairs, "E-government support project management guidelines," pp. 2, pp. 6-7, Feb., 2015.

〈저자소개〉

사 진

배 선 하 (Sunha Bae) 정회원
2007년 2월: 한양대학교 미디어통신공학과(학사)
2009년 1월: 한국과학기술원 전기 및 전자공학과(석사)
2009년 1월~2013년 2월: LIG 넥스원 주임연구원
2013년 4월~2014년 1월: 두산중공업 기술연구원 주임연구원
2015년 2월~현재: 국가보안기술연구소 기술원
〈관심분야〉 정보보호, 전자공학, 제어시스템

사 진

김 소 정 (So Jeong KIM) 정회원
1998년 2월: 부산대학교 사학과(학사)
2001년 2월: 경희대학교 평화복지대학원 동북아학과(석사)
2005년 2월: 고려대학교 정보보호대학원 정보보호정책학과(박사)
2001년~2002년: 한국전파진흥협회 ITU-WRC 담당 연구원
2004년~ 현재: 국가보안기술연구소 정책연구실장, 선임연구원
〈관심분야〉 사이버안보 전략, 정보보호정책, 기반보호정책