자본계획 및 투자 프로세스를 통한 정보보호 예산 수립에 관한 연구

김정덕*°, 박현효**, 이동권**

*중앙대학교 정보시스템학과 교수,**중앙대학교 정보시스템학과 석사,

A Study on Information Security Budgeting through the Capital Planning and Investment Process

Kim, Jungduk, Park, Hyunhyo Lee, Donggwon

Chung-Ang University

E-mail : jdkim@cau.ac.kr, hyoyakke@wm.cau.ac.kr, dglee@wm.cau.ac.kr

요 약

최근 정보보호의 중요성에 대한 인식이 확산되고 있음에도 불구하고 정보보호에 관한 적절한 투자가 이루어지지 못하고 있다. 이는 전 세계적인 경제 불황이라는 원인도 있겠지만, 정보보호 예산 편성에 대한 제도적 장치 및 절차가 미흡하여 정보보호에 대한 요구사항이 적절하게 반영되지 못하는 구조적인 문제를 가지고 있다.

미 정부에서는 정보보호 예산편성을 체계적으로 수립하도록 여러 법규와 지침이 작성되어 현재 수행 중에 있는 반면, 국내에서는 예산편성지침에 정보보호 관련 예산편성에 대한 지시는 있으나 구체적인 방법 제시나 지침이 존재하지 않고 있다.

본 연구에서는 미국의 전자정부의 출범에 따른 정보기술 예산 편성과 관련된 미 연방정부정보보호관리법(FISMA) 및 관련 법규를 검토하고 자본계획 및 투자통제프로세스를 통한 정보보호 예산 편성 과정을 분석하고자 한다. 또한 국내 정부의 예산편성 과정을 미국의 경우와 비교분석함으로써 보다 효과적인 정보보호 예산 반영을 위한 제도적 방안 및 지침 수립을 위한 시사점을 제공하고자 한다.

1. 서론

지난 1. 25 인터넷 대란 이후, 정보보호의 중요성이 증대하고 있음에도 불구하고 정보보호에 대한 구체적인 투자계획은 언급만 될 뿐이며, 실제적인 투자는 적절하게 이루어지고 있지 않는 형편이다.

일반 기업체들과 정부 공공기관들의 전체 정보기술(IT) 투자에서 차지하는 정보보호 투자 비율은 약 5% 내외로 선진국의 약 10% 수준과 비교할 때 매우 낮은 수준이라고 할 수 있다[17, 18, 19]. 이러한 낮은 투자수준에 대한 원인 중 하나는 정보보호에 대한 일반적인 부정적인 인식 수준, 즉 정보보호를 기업경영을 수행하는데 있어 피할 수 없이 지불해야 하는 부대비용 정도로 인식하기 때문이다. 즉, 기업의 생존이나 경쟁력 제고를 위한 투자라는 보다 긍정적인 인식이 결여되어 있기 때문이라고 할 수 있다[17].

이러한 국내 현실에 비해 미국 정부에서는 정보보호에 대한 예산편성 및 투자를 구체적으로 수립하도록 법규와 지침이 작성되어 활용되고 있다. 또한, 지난 2003년 4월 17일 부시행정부내에 공식적으로 전자정부국이 출범함으로써, 정보보호에 대한 예산편성과 투자가 체계적이며 공식적인 방식으로 진행되고 있다[14].

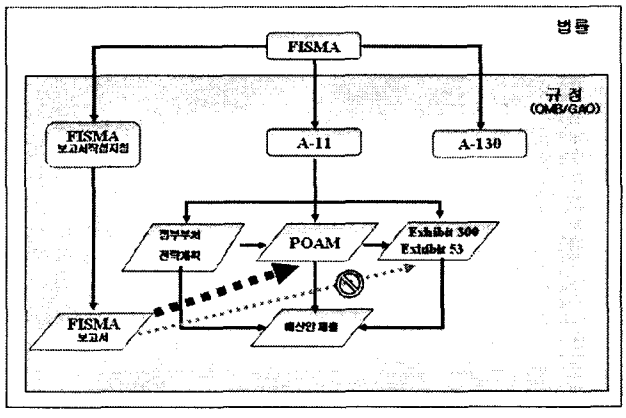
그러나, 국내에서는 정부예산편성지침에 정보보호와

관련된 예산편성 지시는 있으나, 구체적인 절차나 방법 등을 포함한 지침 등은 제시 되어있지 않은 실정이다 [17]. 이러한 상황은 일반 민간기업체에서도 마찬가지로 해당되며 따라서 국내 현실에 적절한 정보보호 예산편성 및 투자방법에 대한 연구 및 지침 개발이 시급하다.

본 연구에서는 미국의 전자정부의 출범에 따른 정보기술 예산 편성과 관련된 연방정부정보보호관리법(Federal Information Security Management Act: FISMA) 및 관련 법규를 검토하고 자본계획 및 투자통제 프로세스(Capital Planning and Investment Control: CPIC)를 통한 정보보호 예산 편성 과정을 분석하고자 한다. 또한 국내 정부의 예산편성 과정을 미국의 경우와 비교분석함으로써 보다 효과적인 정보보호 예산 반영을 위한 제도적 방안 및 지침 수립을 위한 시사점을 제공하고자 한다.

2. 미국의 FISMA 및 관련 법규

미 정부의 정보보호 예산편성 관련 법률 및 규정은 (그림 1)과 같다. 관련 법률로는 전자정부법의 정보보호에 관련된 부분인 FISMA가 있고, 관련 규정으로는 미 기획예산처(Office of Management and Budget: OMB) Circular A-11, A-130이 있다[8, 9, 10, 11, 14].



(그림 1) 미 정부의 정보보호예산 관련 법률 및 규정

FISMA(2002. 12)는 정보보호의 중요성을 인식하고 각 부처의 정보보호와 관련한 각종 피해를 최소화 시키고자, 정부정보보호개혁법(Government Information Security Reform Act: GISRA)를 더욱 확장시키고, 강화시켰으며, 연방정보자원 보안정책을 총괄 및 감독하는 OMB의 정책을 준수하도록 명하고 있다.

OMB Circular A-11은 전자정부 구현을 위한 정보보호 예산 및 정보기술 투자 정책에 필요한 규정들을 정책화하고 있다.

POAM(Plan of Action and Milestones)은 각 부처가 임무를 수행함에 있어서 필요한 모든 프로그램과 시스템의 정보보안에 대한 약점을 분석하고 이것을 해결하기 위한 자원을 정의하고, 대응책을 일정에 맞추어 구현하도록 하기 위한 계획서이다.

Exhibit 53은 전자정부 구현을 위한 정보기술요소 즉, 각 부처별 시스템 구축 비용, 시스템 운용 및 유지보수를 위한 인력 등에 관한 포트폴리오에 대한 규정을 제시하고 있다.

Exhibit 300은 정보보호관련 예산 자본 계획과 업무사례의 정당성을 평가하기 위한 규정을 담고 있다.

OMB Circular A-130는 정보자원의 관리와 정보보안에 있어 요구되는 임무 수행에 필요한 사항을 규정하고 있다.

GISRA에서 FISMA로의 주요 변화를 간략히 요약해 보면 다음과 같다[13]. ① 연차보고서가 갖추어야 할 요구사항의 변화를 가져왔다. ② 시스템의 구성 및 요구사항들은 각 부처에 의해 결정되어진다. ③ 보안 통제를 주기적으로 시스템의 보안 정책에 대해서 시험하고 평가한다. ④ 시스템 운영의 지속성을 유지시켜줄 수 있는 보안 프로그램 및 계획에 대한 정책적 요구사항을 분류한다. ⑤ 국가기술표준연구소(National Institute of Standards and Technology)에서 작성한 표준 및 지침을 토대로 각 부처에서 다루는 모든 정보와 정보시스템을 특정 기준에 따라 분류한다. ⑥ 정보보호책임자(Information Security Officer: ISO)의 세부적인 책임과 자격조건을 추가 했다. ⑦ 주요 손실 보고서(정책, 임무수행 절차, 시스템의 전체적인 손실, 취약점 등)에 대해 세부적 모니터링 보고서를 추가했다. ⑧ 주요 정보시스템의 명세서에 주요 정보시스템의 관리와 개선을 위한 요구사항과 지침들을 수정, 포함했다.

FISMA에 대해 한 가지 주목할 점은 미국 전자정부 하에 각 기관들이 수행하는 업무들을 원활히 수행할 수 있도록 하는 정보자원 및 기술에 대해서 이를 보호할 수 있는 정보보호에 대한 구체적으로 예산의 운영계획, 인수 그리고 관리 및 지속성을 규정하고 있다는 것이다.

FISMA에서 정보보호 예산 계획, 인수, 관리 등에 관한 규정을 담고 있는 제 300조의 주요 항을 중심으로 하

여 살펴보면 다음과 같다.

제 300조 5항: 각 부처들은 자본 계획 프로세스를 효과적으로 수립해야 한다. 효과적인 자본 계획 프로세스라 함은 각 부처가 정의하는 수행 목표에 따라 위험 및 임무 수행 라이프 사이클 비용의 최소화 및 이익의 최대화를 기본 수칙으로 한 장기간의 예산 의사결정 프로세스를 포함하고 있어야 한다고 규정하고 있다.

제 300조 6항: 예산 합병과 투자를 어떻게 해야 되는지에 대한 내용으로, 기초 요구사항으로 각 부처가 행하는 활동에 대한 모든 자본비용, 그리고 그 수행결과로써 얻어지는 이익은 회계에 전적으로 반영이 되어야 하며, 이에 영향을 주는 모든 원인이 의사결정시 반영이 되어야 한다.

제 300조 7항: Exhibit 300은 모든 자본 예산에 대해서 캐피탈 프로그래밍[1], 자본 계획 그리고 투자 통제 프로세스 등을 종합하여 주요 인수, 프로젝트, 시스템에 대한 예산을 측정하여 OMB에 보고해야하는 일종의 예산 계획안이다. 또한 이것은 OMB가 각 부처의 예산을 검토하는데 필요한 정보를 수집할 수 있도록 계획되었다. 각 부처들은 그들의 역할을 분명히 하고 매년 부처임무와 관련하여 실행 가능성과 우선권, 자원들에 대해서 재조정을 하거나 조정가능성을 짐작하고 그것을 지속 시킬 것인지 혹은, 그렇지 않을 것인지에 대한 예산 포트폴리오를 검토하여 제시 하여야 한다.

제 300조 8항: Exhibit 300은 미 연방획득법(Federal Acquisition Streamlining Act)과 Clinger-Cohen Act of 1996, 정부성과관리법(Government Performance Result Act of 1993)에 따라 정보기술, 정보보호, 프라이버시, 기록 관리, 전자거래정책 등이 각 부처의 장기적인 목표와 연차 수행 계획에서 이행해야 하는 요구사항들을 만족하고 있는지에 대한 정보를 요구하고 있다.

제 300조 9항: 새로운 프로젝트에 대해서는 1년에 두 번, 생명주기에 도달하기 전, 해당 부처의 비즈니스적 특이 사항에 대해서 그 정보가 보고될 가치가 있고, 의사결정이 가능해 질 때, OMB에 보고해야 한다. 실행 중인프로젝트가 비용, 스케줄 혹은 성능 측정치가 -10% 가 되거나, 그 이하로 떨어지게 된다면, 해당 사유와, 취해야 할 대안과 규칙 등에 대해서 분석 보고서를 제출해야 한다.

제 300조 10항: 각 부처가 제안하는 Exhibit 300에 대한 OMB의 평가 기준은 각 비즈니스 사례에 대하여 핵심 측정 기준과 각 부처에 제공된 예산 pass-back 프로세스의 결과를 통해서 점수로 환산되어 기록된다.

각 요소에 대한 최고점수(5점)는 다음과 같은 기준으로 부여된다.

- 비즈니스 사례(Business Case): 프로그램 요구사항들이 각 부처가 정의하는 이익과 자동적으로 연결된다.
- 정부개혁안 항목(Agenda Items): 각 지역 시민들의 요구사항을 e-비즈니스 기술을 통해 수렴하고 있다.
- 획득 전략(Acquisition Strategy): 강력한 획득 전략이 연방정부의 위험요소를 경감시킨다.
- 프로그램 관리(Program Management): 프로그램이 매우 건실하며, 그것을 관리하기 위한 자원을 내재하고 있다.
- 전사적 아키텍처(Enterprise Architecture): 해당 부처의 전사적 아키텍처와 CPIC 프로세스를 포함하고 있다.
- 대안분석(Alternatives Analysis): 이익과 합당한 이유를 갖고 있는 실행 가능한 대안이다.
- 위험관리(Risk Management): 프로젝트를 통해서 위험을 유발 시키는 필수적 요소들을 고려하고 있고, 관리될 수 있다.
- 성과 목표(Performance Goals): 연차보고서, 부처의 임무, 전략적 목표 등을 포함하고 있다.
- 정보보호와 프라이버시(Security and Privacy) : 정보보호와 프라이버시 문제들에 대한 해결책을 포함하고 있다.
- 성과기반 관리시스템 (Performance Based Management System): 획득가치관리시스템(EVMS)[2]을 사용하고 있다.
- 수명주기 비용(Life-Cycle Cost): 생명주기 비용이, 요구되는 자원과 위험을 수용하고 관리 할 수 있는 요소들을 수치화해서 예산에 포함하고 있다.

OMB는 위와 같은 요소에 근거하여, 1-5점에 해당하는 점수를 각 요소별로 부여하고 이를 합산하여 각 부처별 비즈니스 사례를 평가하고 예산을 편성한다.

---

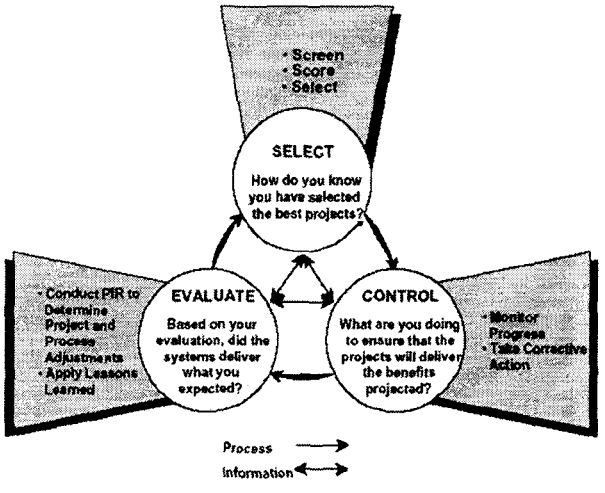
1) 부처의 예산의 계획 및 관리 등을 위하여 업무 프로세스를 분석하고 통합하는 것

2) 프로젝트의 범위, 일정, 비용요소 등의 최적화를 위한 프로젝트 계획 및 통제 관리 도구이다.

3 CPIC를 통한 정보보호 예산 편성

3.1 IT CPIC의 역할 및 절차

미국 OMB와 GAO에서는 IT CPIC(Capital Planning and Investment Control)에 관한 지침서를 통해, 정부부처에서 필요한 IT 투자가 비용 효과적이며 조직의 임무와 목표를 달성하기 위해 사용되게 하기 위한 투자결정과 관련된 정당화를 위한 프로세스를 규정하고 있다. CPIC의 목적은 개별적인 프로젝트 측면이 아닌 조직 전체 관점에서 IT 투자의 동향, 방향, 산출물 등에 초점을 맞추어 투자관리를 수행하고자 함이다[2, 3]. 일반적으로 IT 투자에 대한 의사결정 및 관리를 위한 CPIC는 (그림 2)와 같이 3 단계의 순환과정을 통해 이루어짐을 보여주고 있다.



(그림 2) IT CPIC 프로세스

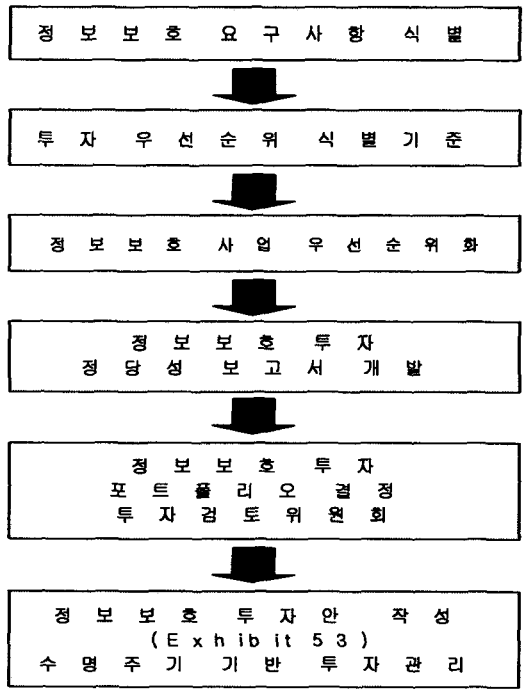
선택 단계: 여러 가능한 투자안을 도출하고 가능한 투자안들을 조직의 전략과 임무 수행에서의 필요성에 기초하여 선택한다. 투자안에 대한 분석이 수행되며 투자검토위원회에서 조직의 임무와 전사적 아키텍처를 지원하는 IT 프로젝트를 선정한다.

통제 단계: 감독, 품질통제, 관리자 검토 등을 통해 선택된 투자안이 적절하게 관리되고 일관성있게 수행되고 있는 지 보장한다.

평가 단계: 구현된 프로젝트의 결과와 기대치와 비교하여 투자 성과를 평가한다. 필요하다면, 투자관리 프로세스를 변경할 수 있다. 구현된 프로젝트가 성숙됨에 따라, 조직 임무달성 관련 효과성, 지속적인 유지보수 비용, 기술적 기회 등을 평가하여야 하며 시스템의 갱신 또는 교체를 고려할 수 있다.

3.2 IT CPIC 프로세스와 정보보호 통합

이와 같은 IT CPIC 프로세스에 정보보호를 반영하기 위한 절차는 (그림 3)과 같은 활동을 통해 수행되어진다.



(그림 3) IT CPIC 와 정보보호 통합절차

① 정보보호 요구사항 식별: 기존의 정보보호 척도 프로그램(metrics program)을 이용하여 요구사항을 식별할 수 있다. 즉 척도 프로그램을 통해 현존하는 정보보호 통제의 구현 수준(as-is)을 파악할 수 있으며 바람직한 성과(to-be)와의 차이분석(gap analysis)을 통해 필요한 정보보호 요구사항 또는 교정 활동이 식별될 수 있다. 척도 프로그램이 없으면, OMB의 POA&M 보고서, 내부 검토자료, 위험평가 및 침투시험 결과 등의 자료를 통해 정보보호 요구사항 및 교정 활동을 식별할 수 있다.

② 투자 우선순위 식별기준 개발: 제한된 투자자금으로 앞에서 식별된 정보보호 요구사항을 모두 만족시키기는 어려우므로 투자자원의 효과적 사용을 위해 우선순위를 통한 투자가 필요하다. 이를 위해 우선순위를 식별하기 위한 기준 개발이 요구된다. 기준은 정부부처의 CIO

나 최고관리자에 의해 결정되며 연방정부의 요구사항, 법/규정, 부처의 임무나 목표 등을 기초로 우선순위 기준을 개발 할 수 있다.

③ 정보보호 사업 우선순위 결정: 식별된 기준에 따라 정보보호 교정활동들은 우선순위가 할당된다. 우선순위는 시스템 수준과 전사적인 정보보호통제 수준에서 할당될 수 있다. 우선순위는 운영단위 수준과 CIO 수준에서 수행되어야 한다. 우선순위 과정의 효율성을 위해 척도의 사용 및 자동화 도구를 사용할 수 있다.

④ 정보보호 투자 정당성보고서 개발: 정보보호 사업에 대한 투자 정당성을 제공하기 위해 비즈니스 사례 분석(Business Case Analysis), 투자 위험평가 등 기존 자료를 사용하여 Exhibit 300을 작성하고, 투자검토위원회에게 제출한다. Exhibit 300은 프로젝트에 대한 최소 3가지 대안에 대해 타당성/성과/기대효과 분석을 포함하고 있다.

⑤ 정보보호 투자 포트폴리오 결정: 부처 내 투자검토위원회에서는 상정한 투자사업을 정당성 보고서에 기초하여 검토, 선택한다. 정보보호는 일반적으로 포트폴리오 결정시 주요한 원동력으로서의 역할은 수행하지는 않지만, 특히 e-비즈니스와 같은 경우, 주요한 전제조건 또는 동인(enabler)으로서 작용하기 때문에 투자전략 수립시 전략적으로 중요하다.

⑥ 정보보호 투자안 작성 및 투자관리: 검토위원회에서 선정된 투자사업을 기초로 Exhibit 300과 Exhibit 53을 작성하고 OMB로 보내 예산신청을 한다. 사업관리자(PM)는 투자 관련 비용 변경을 반영하기 위해 매년 Exhibit 300은 재검토하고 갱신한다.

3.3 CPIC 프로세스에 통합된 정보보호 실행계획 작성 실무

여기서는 CPIC의 활동 중 가장 중요하고 어려운 것은 세번째 활동인 '정보보호사업 우선순위 결정'이라고 할 수 있다. 이 과정을 가상 사례를 통해 어떻게 정보보호 사업의 우선순위가 결정되는 가를 기술함으로써 이해를 돕고자 한다[7]. XX 정부부처에서는 전자정부사업의 일환으로 정보보호 투자를 계획하고 있는데 NIST SP 800-26 (정보보호 자체평가 지침)을 기초로 필요한 투자안을 도출하려고 한다. 정보보호 자체평가 지침은 정보보호 통제를 17개의 정보보호 통제영역으로 구분하여 각 부분에 대해 자체평가를 할 수 있도록 해설 및 설문지 등을 포함한 문서이다. 투자안에 대한 우선순위 결정 과정은 아래에 표기된 바와 같이 크게 3단계를 거쳐 수행된다.

1단계: 전사적 차원에서의 우선순위화

- 정보보호 17개 통제영역에 대한 우선순위화: 부처 고위관리자와 이해관계자는 17개 영역에 대해 중요도에 따라 3 등급(H, M, B(basic))으로 순위를 할당한다.

[표 1] 정보보호 통제영역의 중요도 분류

카테고리	정보보호 통제영역
높음	사고처리 능력, 감사증적, 수명주기
평균	프로세싱 승인, 논리적 접근통제, 정보보호 인식 훈련 교육, 데이터의 무결성, 물리적 정보보호, 정보보호 통제의 재검토
낮음	문서화, 위험관리, 입력/출력 통제, 식별 및 인증, H/W S/W 지속성, 개인정보보호, 비상계획, 시스템 정보보호 계획

- 정보보호 교정활동의 영향분석: POAM의 데이터를 사용하여 정보보호 교정활동이 각 영역에 미치는 영향을 계산한다. 영향도 = ((정보보호 미준수 비율/정보보호 교정활동비용)*100). 영향도는 편의상 3 등급(높음(>.4), 평균(.2-.4), 낮음(<.2))으로 구분한다.

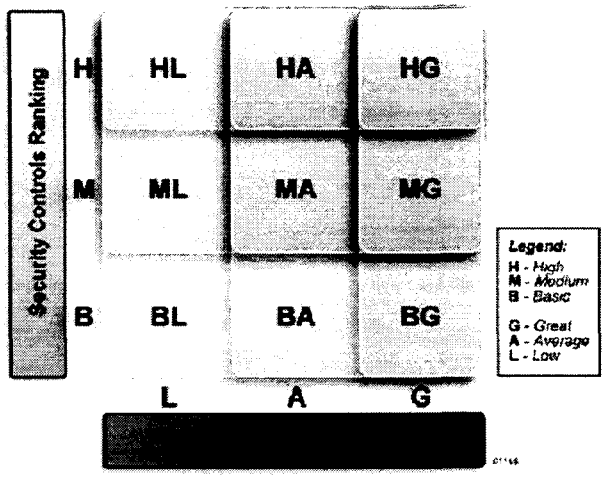
[표 2] 교정활동의 통제영역에 대한 영향 분석

NIST SP 800-26 Topic Area(TA)		정보보호 달성	정보보호 미준수	교정활동 비용	교정활동 영향	카테고리
ID		D	E	F	G	H
IR	사고처리 능력	35%	65%	$81,161	0.8	G
LC	수명주기	17%	83%	$117,789	0.7	G
AT	감사증적	58%	42%	$94,326	0.44	G
AP	프로세싱 승인	7%	93%	$237,350	0.39	A
SA	정보보호 인식, 훈련, 교육	50%	50%	$133,898	0.37	A
PH	물리적 정보보호	75%	25%	$88,762	0.28	A
LA	논리적 접근통제	37%	63%	$248,154	0.26	A
DI	데이터의 무결성	20%	80%	$328,506	0.24	A
RS	정보보호 통제검토	58%	42%	$179,139	0.23	A
	. . .	. . .	. . .	. . .	. . .	. . .

- 앞의 두 단계에서 결정된 순위를 3*3 행렬표에 입력한다.(그림 4 참조)

2단계: 시스템 수준에서의 우선순위화

- 시스템의 민감도에 대한 우선순위화: 정부부처내의 시스템에 대해 민감도에 따라 3 등급(H, M, B(basic))으로 순위를 할당한다.(표 3 참조)



(그림 4) 전사적 수준에서의 교정활동 우선순위 분석

[표 3] 시스템의 민감도에 따른 분류

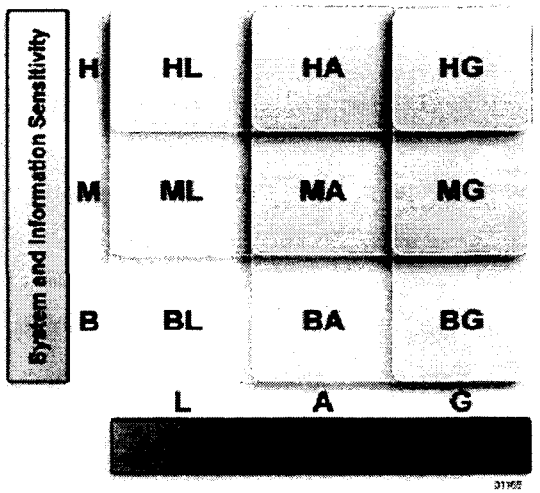
카테고리	정보시스템 목록
높음	시스템 N, 시스템 F, 시스템 S
평균	시스템 J, 시스템 K, 시스템 I, 시스템 A
낮음	시스템 P, 시스템 M, 시스템 H, 시스템 T, 시스템 C, 시스템 R, 시스템 E, 시스템 O, 시스템 G, 시스템 Q, 시스템 B, 시스템 L, 시스템 D

- 정보보호 교정활동의 영향분석: POAM의 데이터를 사용하여 정보보호 교정활동이 각 시스템에 미치는 영향을 계산한다. 계산공식은 1단계와 동일하다.

[표 4] 교정활동의 시스템민감도에 대한 영향 분석

시스템이름	민감도 순 위	정보 보호 미준수	교정 활동 비용	교정활동 영향	카테고리
ID	AA	A	B	C	D
N		85%	$ 3,800	22.37	G
S		16%	$ 1,456	10.99	G
F		10%	$ 1,000	10	A
J		88%	$ 17,431	5.05	A
I		89%	$ 26,387	3.37	A
K		95%	$ 45,566	2.08	A
A		90%	$ 75,000	1.2	L
		. . .			

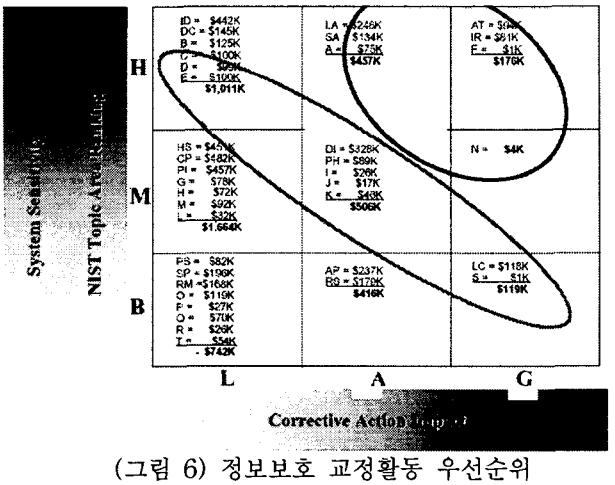
- 앞의 두 단계에서 결정된 순위를 3*3 행렬표에 입력한다.



(그림 5) 시스템 수준에서의 교정활동 우선순위 분석

3단계: 1, 2 단계 결과 통합과정

- 1, 2 단계에서의 결과를 결합하여 정보보호 교정활동 우선순위를 구한다.
- 투자 최우선순위는 우측상단(HG)에 있는 정보보호 교정활동이 될 것이고, 투자 가능 금액에 따라 좌측하단 방향으로 투자안을 실행시킬 수 있다.
- 이러한 모델은 정보보호 활동 이행을 위한 로드맵을 용이하게 작성하게 해 주는 역할을 수행한다.



(그림 6) 정보보호 교정활동 우선순위

4. 한·미간의 정보보호 예산편성과정 비교

미국의 정보보호 예산편성과정은 FISMA와 OMB에서 제정한 법, 규정 하에 의무적으로 각 정부부처 별로 IT 예산편성과 통합된 형태로 OMB에 보고하게 되어있으며, 특히 정보보호 투자에 대한 정당화를 위한 여러 기법과 절차가 포함된 지침서 등이 배포되어 합리적인 정보보호 관련 예산편성이 이루어지고 있다. IT 투자관리를 위한 프로세스(IT CPIP)에 정보보호를 통합하는 절차와 방법을 워크샵을 통해 관련자들을 교육시키고 있는 점은 시사하는 바가 크며 워크샵 결과 내용을 정리한 문서를 2004년도 초에 지침으로 발간할 예정이다.[7]

한국에서는 2003년도 초에 정통부는 기획예산처와 협의하여 정보보호 예산을 정부부처 예산편성시 포함시키도록 2004년도 예산편성지침에 "바이러스, 해킹 등에 대비한 정보보호예산을 반영해야 한다"라는 문구를 삽입시켰다. 그리고 "정보보호 업무활동을 위한 비용 유형"이라는 지침을 정통부 홈페이지에 등록시켜 해당 공무원들이 참고할 수 있도록 하였다. 이 지침은 정보보호 투자 비용과 운영비용으로 구분하고 투자 비용은 각종 정보화 사업에서 정보보호를 위한 여러 활동 및 솔루션 도입 및 개발에 소요되는 비용으로 구분하였고, 정보보호 운영/관리 비용은 정보보호시스템의 운영 및 관리에 소요되는 비용으로 구분하였다[17].

그러나 이 지침은 단순한 비용유형을 구분한 것에 지나지 않으며 정보보호 예산편성 절차나 기법에 대해서는 구체적 내용을 포함하고 있지 않다. 또한 정보보호 예산을 독립적으로 편성할 것이 아니라 전체적인 IT 예산편성과정과 통합되어야 함에도 불구하고 이에 대한 지침이나 방법이 서술되어 있지 않다.

이와 같이 한국에서는 정보보호 예산 관련 규정이나 지침 등 효과적인 정보보호 예산편성을 위한 제반 요건들은 미비한 형편이며 앞으로 많은 연구와 개발이 필요하다 하겠다.

5. 결론

본 논문에서는 미 정부의 정보보호 예산편성 관련 법률 및 규정 등을 분석하고 구체적으로 IT 투자관리과정에 정보보호 투자를 어떻게 통합시키는 가에 대한 지침을 소개하였다. 미국에서는 정보보호 예산편성을 IT CPIP에 통합시키려는 노력은 2003년도부터 시작되어 비교적 구체적인 작업이 수행되고 있으며 관련 지침이나 기법들이 지속적으로 보완되고 있다.

국내에서의 정보보호 예산편성 노력은 거의 전무하다고 할 수 있다. 즉, 관련 법/규정 제정 필요성에 대한 인식이 부족하며, 관련 지침 작성에 필요한 전문지식이 결여되어 있는 형편이다.

정부기관을 포함한 공공기관에서의 정보보호의 중요성이 점차 증대되어가고 있는 상황에서 정보보호 예산편성은 정보보호 활동을 효과적으로 이행하기 위한 필수 전제조건이라고 할 수 있다. 공공기관 예산 관련 법률이나 지침에 의무적인 정보보호 예산편성 및 보고 등의 조항을 포함하거나 관련 지침을 개발하는 것은 매우 시급한 과제이다. 이렇게 중대한 과제를 해결하기 위해서는 학제간의 연구, 즉 법, 회계, 정보보호, 재정학 등 관련 분야의 전문가들의 공동 노력이 있어야 하며 범정부적인 참여가 필요하다고 하겠다.

[참고문헌]

[1] Clinger-Cohen Act of 1996 Public Law No:104-208

[2] DOI, Office of the CIO, Guide to Implementing IT Capital Planning and Investment Control, April, 1998.

[3] GAO, Office of the CIO, IT Capital Planning and Investment Guide, Oct., 1997.

[4] NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, August 2001

[5] NIST SP 800-30, Risk Management Guide for Information Technology Systems, February 04, 2002.

[6] NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, June 11, 2002.

[7] NIST, Integrating IT Security into Capital Planning and Investment Process, Workshops, June 4, 30, 2003.

[8] OMB Circular A-11, Preparing and Submitting Budget Estimates, July, 2000.

[9] OMB Circular A-11, Section 53 - Information

Technology and e-Government, 2003.

[10] OMB Circular A-11, Section 300 - Planning, Budgeting, Acquisition, and Management of Capital Assets, 2003.

[11] OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, Feb. 1996.

[12] OMB, Evaluating Information Technology Investments, Feb., 1995.

[13] OMB M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, Aug. 6, 2003.

[14] USA Congress, E-Government Act, Title III, Federal Iinformation Security Management Act, 2002.

[15] 최선희, "미국 '전자정부 전략 2003'의 내용과 시사점", 정보통신정책, 제 15권, 9호, pp. 34-39 2003. 5.

[16] 한국전산원, "미국의 전자정부 입법동향 분석 '2002년 전자정부법안(S.803)'", 정보화 정책자료, 2002. 11.

[17] 한국정보보호진흥원, "정보보호제품 구축확대를 위한 법제도 조사 대응·방안 수립", 중간보고서, 2003.

[18] 한국정보보호진흥원, "주요 민간부문 실태조사", 2001.

[19] 한국정보보호진흥원, "전자상거래 기업의 정보보호 실태조사", 2002.

[20] 한국전자통신연구원, "정보보호 응용시장 수요조사", 2002.

[21] 정통부, "정보보호 실태조사 결과", 2003.