한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호 (2010. 7)

국가단위 신규 IT인프라의 위험수준 등급화모델에 대한 정책적 필요성

김상균°
°강원대학교 산업공학과
e-mail: saviour@kangwon.ac.kr

Government Necessity of Risk Rating Methodology for Nationwide Emerging IT Infrastructure

Sangkyun Kim°
°Dept. of Industrial Engineering, Kangwon National University

● 요 약 ●

국가단위로 구축예정인 신규 IT인프라의 계획 및 설계 단계에서 신규 IT인프라에 잠재하는 위험도를 사전에 종합적으로 분석하기 위하여 현재까지는 위험분석 이론이 사용되고 있으나 여러 가지 적용상 한계점이 지적되고 있다. 본 연구는 이와 관련하여 신규 IT인프라의 위험도를 일정 단위의 등급으로 분류하여 정부기관, 서비스 제공자, 서비스 수요자가 정확하게 인지하고 대응할 수 있도록 하기 위하여 신규 IT인프라에 대한 위험수준 등급화 모델의 필요성을 제시하는 것이 목적이다.

키워드: 위험분석(risk analysis), 사전진단(premature assessment), 위험등급(risk rating)

I. 서론

2006년부터 2009년 사이에 정부에서는 mRFID인프라, u-City 인프라 등에 대하여 정보보호 위험도를 사전 진단한 바 있다. 여기서 사전진단의 의미는 mRFID인프라, u-City 등 국가단위 신규IT인프라의 구축이 완성되기 이전인 계획 및 설계 단계에서 완성된 인프라의 위험도를 미리 예측하는 것을 의미한다. 국가단위 대규모 IT 인프라를 신규로 구축하기 이전에 계획 및 설계단계에서 정보보호 위험도를 사전에 점검하여 미리 대응함으로써 국가 경제적 손실을 절감하고, 신규 IT인프라의 활용성을 높이기 위함이다.

2006년부터 2009년 사이에 정부가 실시한 사전 진단의 결과는 신규 IT인프라의 계획에 내포된 위험을 위험분석(Risk analysis) 이론을 통해 산출한 것이다. 그 결과는 신규 IT인프라에 내재된 위험을 열거하는 형태가 되었다. 그러나 이는 신규 IT 인프라에 존재하는 위험이 실제 서비스 과정에서 어느 정도의 위험이 발생할 수 있으며, 어느 수준의 대응(투자)을 해야 하는 것인지에 대한 결정 기준을 제공하지 못한 점이 문제점으로 지적되었다.

이러한 문제점에도 불구하고 신규 IT인프라의 정보보호 위험도 등급화 자체에 대한 연구는 국내외적으로 활발하지 못하다. 본 연구에서는 현재 위험분석 이론이 대체 수단으로 사용되고 있는 신규 IT인프라의 정보보호 위험도 사전진단 분야에서 새로운 위험수준 등급화 모델의 필요성을 제시하는 것이 본 연구의 목적이다.

II. 관련 연구

1. 위험분석 이론

1.1 개요

위험분석 이론은 크게 정량적 분석과 정성적 분석으로 분류된다. 정량적 분석은 자산가치, 취약성, 위협 및 위험을 화폐 가치, 확률 및 빈도 등을 통해서 수치적인 형태로 산출하고 분석하는 것이다. 정성적 분석은 자산가치, 취약성, 위협 및 위험을 상대적 중요도, 순위 산정, 전문가 의견 등을 통해서 비수치적인 형태로 나타내고 분석하는 것이다 [1]. 위험분석 기법을 통해 구축이 완료된 시스템에 존재하는 자산별 위험을 산출할 수 있으며, 이에 대하여 개별적인 정보보호 시스템, 관리기법, 물리적 보호 등을 동원하여 위험도를 낮추는 형태의 대응을 한다.

1.2 본 연구목적과 연계된 한계성

위험분석 이론으로 위험도를 사전진단하는 방식에는 다음과 같은 문제점이 있다.

첫째, 기존의 위험분석 기법은 계획 및 설계 단계의 시스템에 대한 위험도를 분석하기에 한계가 있다. 따라서 국가단위 대규모 IT 인프라에 대한 투자단계에서의 사전진단에 활용하기 어려움이 있다.

둘째, 기존의 위험분석 기법은 개별적 자산의 위험도를 산출하는 것으로 이러한 자산의 집합체가 프로세스를 통해 운영되는 전체 서비스의 위험도를 제시하지 못한다.

셋째, 기존의 위험분석 기법은 신규 IT인프라의 특성별로 어느

수준의 위험도가 적정한 것인지를 나타내지 못하고 있다. 즉, 서비스의 특성이 상이한 A, B의 신규 IT인프라가 존재할 경우 A는 위험도 3등급에서도 서비스가 가능하고, B는 위험도 2등급에서 서비스가 가능할 수 있는데, 기존의 위험분석 기법으로는 신규 IT서비스가 어느 수준의 위험까지 감수(잔존위험으로 분류함을 의미)할 수 있는지 판단하지 못한다.

이러한 한계성으로 인하여 위험도가 존재하는 개별 자산은 전체적 서비스의 특성과 무관하게 최대한 정보보호에 대한 투자를 하여 위험도를 낮추는 형태로 지침이 제공되고 있으며, 이는 정보보호 투자에 대한 비효율성으로 이어지고 있다.

2. SSE-CMM[2]

2.1 개요

SSE-CMM은 정보보안 제품과 서비스의 품질과 비용, 가용성을 보다 향상시키고자 하는 목적으로 만들어졌다. 1996년 10월에 모델 version 1.0이 제시되었고, 1997년 4월에 평가방법 version 1.0이 발표되었으며, 1999년 4월에 모델과 평가방법 version 2.0이 제안되어, 현재(2010년 6월 기준)는 version 3.0까지 개발된 상태이다.

SSE-CMM은 영역(domain)과 능력(capability)이라는 두 측면으로 분류하여 평가가 진행된다. 영역 측면은 보안공학 공정의 기본적인 특징을 다루며, 능력 측면은 전반적인 공정관리와 조직화 능력에 관련된 보편적인 실무들로 구성되어 있다.

SSE-CMM에서 제시하는 5단계는 다음과 같다.

- Level 5 - Optimizing: 조직 차원에서 결함 예방적 사고로 활동하며, 신기술 도입 및 적용을 통한 지속적인 프로세스 향상에 초점을 두고 있다. (Level 4와 5는 결함 발생확률의 차이)
- Level 4 - Managed: 프로젝트 수행 시 성과의 조정이 가능하고, 프로세스와 산출물의 정량적인 분석 활동이 이루어진다.
- Level 3 - Defined: 전사적인 소프트웨어 프로세스 활동의 표준화가 이루어지는 단계로 모든 소프트웨어 관련 프로세스가 통합 관리된다.
- Level 2 - Repeatable: 단위 프로젝트 수준의 기본적인 프로젝트 관리 통제가 가능한 수준
- Level 1 - Initial: 가장 낮은 인증수준으로, 소프트웨어 개발시에 일관성 있는 방법론 없이 프로젝트가 진행되며, 산출물의 품질을 보장할 수 없고 아주 뛰어난 몇 사람에 의해 프로젝트의 성공이 결정된다.

2.2 본 연구목적과 연계된 한계성

SSE-CMM에서 의미하는 성숙도는 기업의 정보보호 수준을 의미하는 것이 아니다. SSE-CMM의 성숙도는 기업이 정보보호 관련 업무를 추진할 수 있는 공학적 능력의 성숙수준을 의미한다. 따라서 SSE-CMM모델 자체는 근본적으로 IT인프라의 정보보호 위험도를 평가하거나 등급화하는 과정에 사용할 수 없다. 다만, 정보보호와 관련된 등급을 표준화된 5단계 모델로 보여준다는 점에서 본 연구주제와 연관이 될 수 있다.

3. Kim et al.의 정보보호 성숙도 모델[3]

3.1 개요

Kim et al.의 모델은 SSE-CMM의 사상에 근거하여 개발되었다. 이 모델은 기업의 내부적 정보보호 위험도를 5단계로 나누어 평가할 수 있는 기준을 제공한다. 모델에서 제시하는 등급은 전략적 정보보호, 능동적 정보보호, 수동적 정보보호, 기술적 정보보호, 기능적 정보보호로 나뉜다. SSE-CMM이 서비스 공급자의 내부적 정보보호 역량을 평가한 반면에 본 모델은 SSE-CMM의 기준을 일부 차용하여 일반 기업이 내부적으로 어느 정도 정보보호 안전도를 유지하고 있는지 가늠하게 해준다. Kim et al. 모델의 5단계는 다음의 표 1과 같다.

표 1. Kim et al.의 정보보호 성숙도 5단계 모델
Table 1. Kim et al.'s information security maturity model of five levels.

정보보호 성숙단계		주요 특성
전략적 정보보호 (Strategic IS)		축적된 정보보호 기술을 이용하여 새로운 비즈니스를 창출하고 기업(조직)의 가치를 증대하는 전사적인 차원의 정보보호 단계
관리적 정보보호 (Managerial Information Security)	능동적 정보보호 (Active IS)	정보보호 우수상이 도입되고 선진사례를 도입하여 기업의 정보보호에 적극반영하며 최신 정보보호 기술을 획득하여 기업의 총체적인 정보보호를 실시
	수동적 정보보호 (Passive IS)	정보보호 위협에 대한 모든 것을 관리하는 단계로 정보보호 전문부서를 설치하고 정보보호 관리자를 임명하며 정보보호 전략계획이 수립되는 단계
기술적 정보보호 (Technical IS)		기업의 전산부서 중심의 인트라넷 정보보호가 실시되고 Firewall을 설치하며 중요문서에 대해서는 백업이 실시된다. 정보보호 전략계획이 수립되어 있지 않으며 정보보호 관련 지침이 없다.
기능적 정보보호 (Functional IS)		정보보호 전략 계획이 수립되어 있지 않고 기업내 전산시스템이 갖추어지며 개인 차원의 정보보호가 실시되는 단계로 백신, 화면보호기능의 소극적 정보보호 실시되며 관리상으로 명분화된 것이 없다.

3.2 본 연구목적과 연계된 한계성

Kim et al. 모델은 일부 정부기관 및 사기업의 내부 정보보호 수준을 평가하는 과정에 사용된 바 있으나, 본 연구주제의 목적에 직접적으로 사용하기에는 다음과 같은 한계점이 있다.

첫째, 본 모델은 기업의 정보보호 수준을 평가하는 모델로 IT인프라에 대한 평가 기준이 아니다.

둘째, 본 모델은 구축이 완성된 정보보호 체계에 대한 평가로 신규로 계획된 설계 단계의 모델에 대한 평가 기능이 없다.

셋째, 본 모델은 IT인프라의 적정한 정보보호 수준을 제시하지 못한다. 따라서 피평가대상은 가급적 최상위 등급인 5등급의 정보보호 수준을 유지하도록 전략을 수립하게 되며, 이는 피평가대상의 특성을 고려하지 않은 채 정보보호에 대한 투자를 일괄적으로 늘리도록 유도하여, 정보보호에 대한 투자 효율성을 고려하지 못하는 한계가 있다.

III. 본론

1. 급증하는 신규 IT인프라에 대한 점검

u-City, u-Healthcare, 기가인터넷망 등 다양한 신규 IT인프라와 서비스의 도입이 추진되는 상황에서 신규 IT인프라와 서비스에 대규모의 국고 및 민간 자금이 투입되고 있다. 이에 신규 IT인프라와 서비스에 대한 정보보호 위험도를 사전에 진단하고, 적정한 위험도를 권고하여 정보보호에 대한 경제적 투자를 유도해야 한다.

그러나 2006년부터 2009년 사이에 정부에서 실시한 신규 IT인프라에 대한 정보보호 사전진단 작업에서 위험분석 이론 기반 진단의 다양한 문제점이 제기된 바 있다. 앞서 언급한 SSE-CMM, Kim et al., ISO17799, ISMS관련 연구 등도 신규 IT인프라의 정보보호 위험도를 사전에 진단하고, 적정 수준의 위험도를 권고하는 목적에는 사용하기가 불가하다.

따라서 신규 IT인프라의 위험도를 사전에 진단하여 정책적 의사결정에 활용 가능한 형태로 표현할 수 있는 등급화 모델이 필요하다.

2. 법률적 수요

1996년 이후 미국의 일반회계원인 GAO(General Accounting Offce)에서는 미연방의 정부 시스템의 보안에 심각한 결함이 있음을 지속적으로 밝혀왔다 [4, 5].

미국은 정부정보보안개혁법 (GISRA: Government Information Security Reform Act)를 승계한 연방정보보안관리법(FISMA: Federal Information Security Management Act)를 제정하였다. FISMA는 미국 전자정부법(E-government Act of 2002)의 제3편인 정보보안(Information Security)에 포함되어 있는 상태이다.

FISMA는 GISRA에 규정되었던 IT보안에 대한 의무사항을 영구적으로 유지하는 역할을 하고 있다. FISMA는 관리예산처인 OMB(Office of Management and Budget)를 중심으로 미연방 정부 부처의 정보보안 개선 추진에 기여하고 있다. OMB는 정부기관의 보안 정책을 감독하는 권하는 가진다.

FISMA는 현재 미국내에서 적용상의 여러 가지 문제점이 지적되고 있는데, 그 중 본 연구와 관련된 것으로 정보보호관련 평가에 대한 해석상의 문제를 제시한다. FISMA가 정부기관의 정보보안을 평가한 것을 해석하는 과정에서 다음의 두 가지 문제점이 등장한다.

첫째, FISMA의 경우 FISMA에서 평가하는 결과는 매우 제한적이다. 또한 정부기관의 업무, 정보, 시스템의 특성을 개별적으로 고려하지 않는다. 따라서, FISMA의 평가 결과가 정부기관의 정보보안 실무를 제대로 평가하지 못한다. 즉, 기관이 지닌 정보보안 체계의 일부만 평가한다.

둘째, FISMA의 평가 대상은 정보보호 수준이나 정보보호 위험도가 아니다. FISMA는 규정된 의무사항에 따라서 기관이 정보보안 관련 업무를 빠짐없이 수행하고 있는지를 점검한다. 따라서, FISMA 평가결과가 우수하게 판단된 기관이라 할지라도 정보보호의 위험도가 반드시 낮은 것은 아니며, 그 역도 마찬가지이다. 즉 FISMA는 정보보안을 통한 위험감소를 측정하는 것이 아니라 과정을 평가하는 것이다.

국내에는 현재 FISMA와 같이 정부기관의 정보보안을 위한 통합화된 법률이 존재하지 않으나, 정보보안과 관련된 국내의 개별적인 법률들의 제정 취지와 용도를 고려할 때 전체적인 구조는 FISMA와 유사하다. 따라서 국내에서도 FISMA적용 과정에서 미국내에서 발생했던 문제점이 유사하게 등장할 수 있다.

미국내에서 논의되는 FISMA에 대한 한계점을 고려할 때 다음과 같은 접근이 필요하다. 과정에 대한 평가가 아닌 정보보안 체계를 통해 결과적으로 나타나는 위험수준을 평가해야 하며, 서비스별 특성을 고려하여 위험도 등급화를 표현해야 한다. 또한, 위험도에 대한 등급화 내용이 서비스의 정보보안 요소를 전체적으로 고려할 수 있어야 한다. 이를 위해 IT인프라의 잠재적 위험도를 서비스의 특성을 고려한 등급모델로 표현할 수 있는 기법이 요구된다.

IV. 결론

국가단위로 구축예정인 신규 IT인프라의 계획 및 설계 단계에서 신규 IT인프라에 잠재하는 위험도를 사전에 종합적으로 분석하기 위하여 현재까지는 위험분석 이론이 사용되고 있으나 여러 가지 적용상 한계점이 지적되고 있다. 본 연구는 이와 관련하여 신규 IT인프라의 위험도를 일정 단위의 등급으로 분류하여 정부기관, 서비스 제공자, 서비스 수요자가 정확하게 인지하고 대응할 수 있도록 하기 위하여 신규 IT인프라에 대한 위험수준 등급화 모델의 필요성을 제시하였다. 본 논문에서는 이를 위해 위험분석 이론, SSE-CMM, Kim et al.의 정보보호 성숙도 모델을 설명하였다. 최종적으로 급증하는 신규 IT인프라에 대한 점검, FISMA와 관련된 법률적 수요를 제시하였다.

참고문헌

[1] Ropoer, C.A. (1999) Risk Management for Security Professionals, Butterworth Heinemann.

[2] Systems Security Engineering Capability Maturity Model Project (2003) Systems Security Engineering Capability Maturity Model, SSE-CMM, Model Description Document, Version 3.0, Systems Security Engineering Capability Maturity Model Project.

[3] Kim, S., Leem, C.S. and Lee, H.J. (2005) “An evaluation methodology of enterprise security management systems”, International Journal of Operations and Quantitative Management, Vol 11, No 3.

[4] GAO (1998) Information Security: Serious Weakness Place Critical Federal Operations and Assets and Risk (GAO/AIMD-98-02)

[5] GAO (2000) Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies (GAO/AIMD-00-295)