情報保護學會論文誌
第20卷 第 6 號, 2010. 12

정보보호 사전진단제도의 경제적 효과에 대한 사례 분석*

공 희 경,[1†] 김 태 성[2‡]
[1]한국전자통신연구원, [2]충북대학교 경영정보학과/BK21사업팀

Economic Effects of Advance Diagnosis for Information Security: A Case Study*

Hee-Kyung Kong[1†], Tae-Sung Kim[2‡]
[1]Electronics and Telecommunications Research Institute, [2]Chungbuk National University

요 약

정보화 사회에서 유비쿼터스 사회로 변화함에 따라 정보보호의 중요성이 더욱 증가하고 있으며, 정부와 기업들은 효율적인 정보자산 운영을 위해 여러 가지 다양한 보안 활동을 수행하고 있다. 한국 정부에서는 2006년부터 정보보호의 안정성을 사전적으로 확보하기 위해 정보시스템 개발 초기 단계부터 정보보호의 취약성을 분석하여 비용·효과적 정보보호를 구현하기 위한 사전진단제도를 실시하고 있다. 본 논문에서는 사전진단제도의 경제적 효과를 분석하기 위한 개념적인 프레임워크를 제시하고 실제 사례에 적용하여 예시한다. 본 연구의 결과는 정보보호 관련하여 시행되는 제도의 경제적 효과를 산출함으로써 정책추진의 경제적 타당성을 확보하는데 참고가 될 수 있을 것이다.

ABSTRACT

As the information society changes into the ubiquitous computing society, the importance of information security has increased. Governments and enterprises are carrying out various information security activities to operate their information asset effectively. Since 2006, the Korean government has implemented 'Advance Diagnosis' policy to analyze the vulnerability of the information security from the early stage of the information system development to secure the information stability. This study proposes an analyzing framework for the economic effects of Advance Diagnosis for Information Security and presents an illustrative application on a real Advance Diagnosis case. The results of this study can be applied to secure the economic justification of government policies for the security of information systems.

Keywords: Economic Effects, Advance Diagnosis for Information Security, Case Study

I. 서 론

컴퓨터와 네트워크 등 정보시스템 관련 기술들이 급속하게 발전함과 더불어 정보시스템 및 조직의 정보자산 운영에 대한 공격 형태는 더욱 지능화, 자동화, 분산화, 고속화, 대규모화되고 있다. 또한 유비쿼터스 기술의 발전과 응용 기술의 고도화로 인해 기기 및 서비스에 대한 위협과 관련 보안 취약성도 계속적으로 증가하고 있다. 이에 따라 기업과 조직에 있어서 정보보호는 경쟁적 우위를 확보하기 위한 도구임과 동시에 비즈니스를 안정적으로 수행하기 위한 필수 경영요구사항으로 등장하였으며, 이에 조직은 정보자산에 대한

접수일(2010년 10월 4일), 게재확정일(2010년 12월 2일)
* 이 논문은 2010년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음.
† 주저자, konghk@etri.re.kr
‡ 교신저자, kimts@chungbuk.ac.kr

위협을 인식하고 적절한 관리를 필요로 한다. 정보자산의 가치는 기업 및 조직의 발전과 연속성을 결정할 수 있는 중요한 요소이며, 정보 유출에 대한 통제 및 예방이 기업의 손실을 최소화하고 경쟁우위 확보, 대외 신뢰도 및 고객의 만족도를 높일 수 있는 방법이다. 따라서 정보통신 인프라 및 관련 서비스를 운영하고 있는 조직에서는 주요 정보자산의 보안 위협 분석에 많은 관심이 고조되고 있으며 보안 위협에 따른 사회·경제적 피해규모 역시 그와 비례하여 증가하고 있다. 특히 유비쿼터스 컨버전스 컴퓨팅 기술의 특징인 정보의 이동성을 이용한 서비스의 경우 사용 범위가 한정되지 않고 서비스 대상 또한 계속적으로 확대되기 때문에 사용자의 프라이버시 문제나 공유정보의 기밀성, 무결성, 가용성에 대한 중요성이 매우 높아지고 있다. 또한 최근 들어 형성되고 있는 유비쿼터스 컴퓨팅 서비스를 제공함에 있어 발생할 수 있는 위험 요소를 최소화하기 위해서는 적절한 보호대책을 수립하고 구현하여 적용하는 것이 매우 중요하다. 지금까지의 보안 취약성에 대한 정보보호 대책 수립 및 구현은 시스템 개발 및 서비스 구축 이후 사후적으로 적용되는 것이 대부분이었다. 그러나 서비스 및 시스템 구축 시 보안 취약점을 도출하고 이에 대한 보안대책 수립 및 구현을 서비스 개발 단계 중 언제 적용할 것인지가 중요한 이슈가 되고 있다. 대부분의 경우 운영 단계에서 발생하는 취약점을 도출하고 이를 통제하는 제한적인 활동이 이루어졌으나 보안사고가 발생할 경우 복구 가능성 및 피해 규모를 최소화하기 위한 필요성이 대두되고 있다. 기존의 사후 통제적 보안컨설팅의 경우 운영 단계 이전에서 취약점을 도출하고 통제하는 제한적 활동이 이루어졌으나 보안사고가 발생할 경우 복구가능성 및 비용에 대한 문제가 증가함에 따라 보안취약점의 사전진단이 중요한 요소로 대두되고 있다. 이에 따라 정보시스템 개발 초기 즉, 설계 단계부터 필요한 정보보호 요구사항을 반영해야 한다는 예방통제의 필요성이 부각되고 있다.

캐나다의 경우, 정부 내에서 정보기술보안 제품들을 사용하기 위한 자격을 부여하기 위해서 캐나다 통신보안국, 공공 사업 서비스처에서 정보기술 보안제품 사전검증 제도(IPPP: ITS Product Pre-qualification Program)를 공동 개발하여 시행중이다[1]. 미국에서도 NIST의 SP 800-64 (Security Considerations in the Information System Development Life Cycle) 등을 통해, 정보시스템 개발 생명주기 초기부터 폐기 전까지의 전 과정에서 정보보호 반영하는 프레임워크를 제시하며 정보기술 자산의 위험관리를 필수적인 사항으로 제시하고 있다[2]. 이와 함께 정보시스템 개발 각 단계별로 정보보호 활동에 대한 기술적 요구사항과 그에 대한 정보보호 요구사항 제시의 중요성을 설명하고 있다. 이는 IT 개발 프로세스 초기단계에서 정보보호 취약성 및 환경설정의 오류를 분석하여 개발 프로세스 각 단계별로 정보보호를 확립할 수 있도록 하여 보다 비용 효과적이고 위험관리에 적절한 정보보호 활동을 하도록 시사하고 있다. 또한 IBM System Sciences Institute에서 수행한 정보시스템 정보보호 취약성 수정비용에 관한 연구에서도 정보시스템의 정보보호 취약성 수정에 소요되는 비용은 시스템 수명주기 후반으로 갈수록 커지며, 특히 운영 단계에서는 설계 단계에 비해 60~100배가 증가됨을 보여주고 있다[3]. 또한 사전 예방적 보안과 사후 대응적 보안 행위에 대한 정량적 상관관계에 대한 분석을 통해 한정된 예산으로 보안수준을 최대로 하기 위한 예산 및 자원 분배 방법 등의 최적화 문제에 대한 연구도 활발하게 진행되고 있다[4].

이러한 연구동향에 따라 국내에서도 u-IT 서비스 구축 시 설계 단계에서부터 위협을 분석하고 보안대책을 제시하는 '정보보호 사전진단 제도'가 2006년부터 운영되고 있다[5]. 이는 사전적으로 정보보호의 안정성을 확보하기 위한 것으로 u-IT 서비스의 기술적, 물리적, 관리적 위협요소와 취약점을 서비스 운영 이전에 식별하여 적절한 보호대책을 수립·적용함으로써 정보보호 투자의 실효성과 서비스의 안전 및 신뢰성을 제고하기 위한 제도이다. 그러나 사전진단 제도의 적용에 대한 효과분석은 아직 구체화되어 있지 않다. 이는 사전진단 제도가 2006년부터 시행되어 그 효과를 분석하기 위한 많은 양의 경험적 분석 자료가 아직 축적되지 않았으며, 적용 대상 서비스가 시범사업에 국한되어 적용되었기 때문에 그 효과를 일반화하기 어려운 수준이다. 따라서 사전진단 제도를 더욱 활성화하고, 보다 비용 효과적인 정보보호를 구현하기 위해서는 정보보호 투자효과의 특징을 고려한 경제적 측면의 사전진단 효과분석 모델을 제시하여 그 타당성을 검증할 필요가 있다.

그러나 사전진단을 비롯한 정보보호 투자는 투자 및 진단 시점의 시기와 상관없이 그 효과를 정량화하기가 매우 어려운 분야이다. 보통의 기술은 도입함으로써 늘어난 수입에서 도입 시 지불한 비용과 운영비를 제거하면 기술 도입으로 인한 이익을 계산해 낼 수

있다. 예를 들어 정보화 투자효과를 분석하기 위해서는 새로운 정보시스템 도입을 통한 업무효율 증가로 인해 발생한 매출 증가분을 정보화 투자효과로 측정할 수 있지만 보안 기술의 경우 도입한 후에 보안성의 증가를 측정하기란 매우 어렵다. 그 이유는 다음과 같다. 첫째, 정보보호 기술은 제조나 생산에 직접 관여하지 않아 수치화된 데이터가 제공되지 않는다. 둘째, 예방으로 인해 발생하지 않은 보안사고를 수치화하기 어렵다. 셋째, 보안사고 발생 시 서비스 및 시스템 복구, 이미지 하락 등으로 인한 이익 감소, 소송비용 등은 보호대책 및 기술 도입 당시에는 측정이 불가능하다. 이는 정보보호 투자효과 측정의 시간적 제약으로 인해 사고가 발생하고 일정 시간 후에 그 효과 측정이 가능하기 때문이다. 따라서 본 연구에서는 발생비용 절감분의 크기를 정보보호 투자의 수익으로 측정하고자 한다. 즉, 발생비용 절감분이란 정보보호의 측면에서 손실 예방이라고 할 수 있다. 이는 위협이 현실화되었을 때 발생했을 손실 중 정보보호 투자를 통해 예방되는 정도를 의미한다. 따라서 사전진단 대상 서비스의 보안사고 비용 산정 모형은 보안사고 발생 시 수반되는 피해를 비용으로 계량화하여 유추할 수 있다.

본 논문에서는 정보보호 투자효과의 특징을 적용하여 BSC 관점의 효과분석 프레임워크 수립에 대한 방향성을 제시하고, 사전진단 사례에 대한 경제적 효과를 분석한다. 이를 통해 사전진단 제도 적용의 경제적 타당성을 예시한다. 2 장에서는 정보보호 투자효과 분석에 대한 일반적 개념 고찰을 위해 기존의 정보보호 투자효과 분석에 관한 선행 연구 및 정보보호 투자효과의 특징과 BSC 활용에 대해 살펴보고, 3 장에서는 정보보호 사전진단 제도의 개요 및 특징에 대해서 알아본다. 4 장에서는 사전진단 효과분석의 중요성 및 사전진단 효과 측정 프레임워크를 제시하고, 5장에서는 앞서 도출된 사전진단 효과분석 프레임워크를 기수행된 정보보호 사전진단 사례에 적용하여 그 효과성 및 타당성을 제시하고 이를 통한 시사점 및 향후 연구방향에 대해 논의한다.

II. 이론적 배경

본 장에서는 기존의 정보보호 투자 효과 분석에 관한 선행 연구 및 정보보호 투자효과의 특징과 BSC 활용에 대해 살펴보고자 한다.

2.1 정보보호 투자효과 분석에 관한 선행연구

투자는 투자정도에 따른 효과 예측과 이에 대한 객관적인 평가가 수반된다. 정보보호 분야도 예외는 아니어서 기업이나 조직이 정보보호에 대한 투자를 추진하고 이에 대한 의사결정 시 투자효과 분석과 객관적인 평가가 요구되고 있다. 또한 시간이 지날수록 정보보호와 관련된 인간 행동의 중요성이 기술적인 측면의 중요성을 뛰어 넘게 됨에 따라, 정보보호를 위한 적정 투자수준, 정보보호 이슈에 대한 정보공유 문제, 정보보호 문제를 해결하기 위한 유인체계 정립 등의 경제적인 접근 방법들의 중요성이 새롭게 부각되고 있다. 전통적으로 경제학적 접근방법은 새로운 사회적인 현상이 어느 정도 정규화 되거나 그 현상에 대한 충분한 자료가 축적된 이후에 이론적으로나 실증적으로 그 사회현상을 규명하여 왔다. 정보보호 분야도 최근 들어 정규화 되거나 이에 대한 구체적인 자료가 축적되었다고 보이므로, 정보보호에 대한 경제학적인 접근방법은 지금까지보다도 앞으로 더욱 활발해질 것으로 보인다. 정보보호 연구자들은 대체로 암호학 분야와 시스템 설계 같은 기술적 분야에 집중하여 왔다. 이에 따라 평범한 사람들이 컴퓨터를 사용할 때 흔히 경험하는 사기 및 남용들을 방지하는 유인(incentive)체계를 만드는 소프트한 이슈들은 상대적으로 등한시 되어왔다. 전통적인 의미의 정보보호 전문가로 볼 수 있는 Odlyzko(2003) 및 Anderson(2001)도 정보보호의 문제들이 수학적 암호체계의 결함보다는 사회·경제적 요인에 의해 발생함을 주장하며 정보보호에 대한 사회·경제적 연구방법의 중요성을 말하고 있다[6, 7]. 또한 Soo Hoo(2000)는 보험 산업과 기업에서 정보보호 문제에 대한 사회·경제적 연구의 필요성을 분석하고 효율적인 투자 규모와 효과 분석에 대한 논의의 필요성을 제기하였다[8]. Gordon and Loeb(2002)의 연구에 의하면 정보보호의 투자는 초기에 투자되는 비용에 대비하여 큰 효과를 얻게 되나 일정 시점 이후엔 투자에 비해 그 보안수준의 향상은 완만하게 변화하는 것으로 나타나고 있다[9]. 이는 정보보호를 추진하는 현업에서 매우 중요하게 적용된다. 초기투자에 의해 정보보호 취약점이 80% 이상 제거되나, 나머지 20%의 보안 문제점을 제거하기 위해 초기대비 많은 시간과 투자가 필요하게 된다. 그러므로 기업과 조직은 정보보호의 체계와 추진상황을 정확히 파악하여 대상을 정의하고 초기에 정보보호 추진효과를 고려하여 집중적으로 투자를 하여 문제를 제거하는 전략이 필요하다. 또한 정보보호 투자의 비용요인은 유·무형의 정보자산과 같은 설비와 인력 등을 의미한

다. 비용요인은 대부분 정량화가 가능하여 효과요인에 비해 측정이 용이하다. 그러나 정보보호의 투자효과 측정은 이에 반해 매우 어렵다. 따라서 본 연구에서는 현 시점에서는 나타나지 않지만 오랜 시간을 두고 경영성과에 영향을 미치는 요소를 고려하기 위해 BSC 관점을 이용하여 장기적으로 발생하는 정보보호 투자효과에 대해 분석하고자 한다.

2.2 정보보호 투자효과 분석에서 BSC 활용

BSC는 1992년 미국 하버드대학의 Kaplan과 Norton에 의해 창시된 전략경영기법(Strategic Enterprise Management, SEM)으로 가치경영(Value Based Management, VBM), 활동기준원가관리(Activity Based Costing/Management, ABC) 등과 함께 전략경영기법의 핵심내용이다. BSC는 재무적 성과와 비재무적 성과 측정을 통한 전략 실행의 관리 도구이자 조직 내 커뮤니케이션 도구 및 무형자산의 관리 도구로 정의할 수 있다[10]. 기존의 재무적 성과지표 중심의 기업성과 평가는 무형자산의 비중이 커지고 있는 현대의 기업에 있어 적합하지 못하며, 유형자산만으로 기업의 가치를 평가하기에는 한계를 가지고 있다. 직원들의 지식, 고객관계 그리고 조직에 많은 가치를 창출해 주는 혁신과 변화 등으로 나타나는 무형자산이 기업을 이끌어가는 큰 역량으로써 인정을 받고 있다. BSC는 이러한 기업이 가지고 있는 무형자산을 평가할 수 있는 도구로서 기업 전략과 비전을 구체화하고 그 비전과 전략을 성공적으로 수행하기 위한 핵심성공요인을 측정할 수 있는 핵심성과지표를 공유함으로써 전략의 실행력을 최대화할 수 있다[10, 11].

정보보호 투자효과를 분석하는 기존의 실증 연구들에서는 기업의 수익성이나 정보보호 제품의 도입으로 인한 효과를 검증하는 경우, 대부분 기업의 경제적 지표를 성과 측정변수로 이용하였는데 대표적으로 사용된 측정변수로는 ROI(Return On Investment), NPV(Net Present Value), 주가변동 등 주로 기업의 재무적인 지표들을 들 수 있다. 그러나 재무적 지표는 현재 시점에서 나타난 성과를 숫자로 표시한 것이기 때문에 현재는 나타나지 않는 장기적 활동의 성과나 장기간 동안 성과에 영향을 미치는 요소를 고려할 수 없어 전체적인 활동성과를 정확히 평가하기에는 많은 문제가 있다. 특히 정보보호 투자는 장기적으로 발생하는 효과에 대한 측정 기준이 필요하다. 정보보호에 대한 투자는 보호 받는 자산의 가치를 기준으로 평가되어야 한다. 또한 정보보호에 대한 투자는 일반적으로 장기적 측면의 보장적 성격이 강하다. 따라서 장기적 위험은 줄여주지만 단기적으로 정량적인 투자효과를 제공해주지 못하는 경우도 많다. 따라서 정보보호 투자와 그 효과를 측정하기 위해서는 기업 이미지 향상, 정보시스템 취약성 감소 등의 전반적인 고객 만족도와 내부 프로세스 향상과 같은 비재무적 지표도 포함되어야 한다[12].

III. 정보보호 사전진단 제도

본 장에서는 정보보호 사전진단 제도의 개요와 방법론 등에 대해 기술하고자 한다.

3.1 사전진단 제도의 개요 및 대상

유비쿼터스 기술을 활용하는 u-IT 서비스의 경우, 이용자에 서비스 접근의 편의성을 제공하나, 무선 네트워크, 복합 단말기 등 정보시스템 사용의 복잡도 증가로 인해 보안위협 및 관련 취약성이 증가하여 보안사고 발생 가능성이 매우 높아지고 있다. 이러한 상황에서 신규 IT 서비스 개시 이전에 위협 및 취약점 분석 등의 정보보호 진단을 수행하여 개발 프로세스의 설계 단계에서부터 정보보호 대책을 적용하는 정보보호 활동을 사전진단이라 한다[13, 14]. 설계, 구현, 테스트, 운영 단계로 이루어지는 정보시스템 및 서비스 구축에서 일반적 보안컨설팅의 경우 대부분 테스트 및 운영 단계에서 취약성 및 위협 분석이 이루어지는데, 이에 반해 사전진단 수검의 경우 개발 프로세스의 초기단계인 설계 단계에서부터 설계서상의 위협 및 취약성 분석을 실시하여 보호대책을 수립하게 된다. 이는 정보시스템 및 서비스 구축의 초기단계 즉, 설계 단계에서부터 정보보호를 고려하여 위협 및 취약성 분석을 실시함에 따라 u-IT 서비스에 적용되는 보호대책의 안정성과 신뢰성을 제고시킬 수 있다. 이에 따라 u-IT 확산사업 추진 및 안전성 확보를 위해 RFID/USN 등의 기술을 이용한 융·복합형 u-IT 서비스에 대해 2006년부터 사전진단 제도 적용이 범부처 구축사업으로 추진되고 있다.

3.2 사전진단 방법론 및 평가체계

신규 IT 서비스 개발과정의 위협분석 및 보호대책

도출을 위한 사전진단 수검의 방법론은 크게 5 단계, 12 태스크, 23 개의 세부 활동으로 구성되어 있다. 각 단계는 상호연관성이 있는 태스크의 묶음으로 주요 산출물의 완성 및 검토 시점을 나타내고 있으며, 태스크는 하나의 산출물을 작성하기 위한 일련의 활동을, 가장 하위단계의 세부 활동은 상위 태스크 수행을 위한 세부 방법 및 절차를 나타내는 기초 단위로 구성되어 있다[5].

정보보호 사전진단 수행 절차는 다음과 같다. 첫째, 사전진단 대상이 되는 정보시스템 및 서비스의 아키텍처 분석을 통해 서비스의 정의 및 구조를 분석하고 관련 응용 서비스를 분석하여 보호대상의 데이터 및 구조를 분석하게 된다. 두 번째 단계로 서비스 운영환경을 분석하여 운영되는 서비스의 보안관리 현황을 분석 점검한다. 사전진단 수검은 정보시스템뿐만 아니라 운영되는 서비스 환경 및 서비스를 대상으로 수검을 실시하기 때문에 기술적 정보보호 대책만을 평가하는 것이 아닌 관리적, 운영적 대책을 포함하는 통합적 관점에서 정보보호를 고려하게 된다. 세 번째 단계로 보호대상을 식별하고 위험분석을 실시하여 보호되어야 하는 대상에 대한 위협과 취약성 분석을 통해 전체적인 위험을 분석하게 된다. 이를 통해 도출된 위험에 따라 보호대책 도출 및 구현현황을 비교 분석하여 구현상태 및 상세현황을 분석하게 된다. 마지막으로, 보호대상별 보안관리 현황 및 정보보호 요구사항을 도출하여 미 구현된 보안대책에 대한 보완 및 평가 작업을 실시하게 된다. 또한 보호대책 구현계획서 및 일정표를 작성하여 추후 보호대책 구현사항을 점검할 수 있도록 한다.

3.3 사전진단 제도의 중요성 및 특징

정보시스템 및 서비스 구축 시 초기 설계 단계부터 운영 단계까지 시스템 구축 단계 마다 정보보호를 고려하여 보안 취약점을 점검하게 되는 사전진단 제도를 적용하게 되면 보다 안정적이고 신뢰성 있는 서비스를 구축할 수 있다[14]. 기존의 시스템 구축 후에 보안 취약점을 점검하는 '사후약방문' 식의 정보보호 수검의 경우는 다음과 같은 몇 가지 치명적인 문제점을 갖고 있다. 우선 안정적인 서비스를 제공하는데 문제가 발생할 수 있다. 시스템을 구축한 후 정보보호를 고려하는 경우, 취약점을 찾거나 이를 보완하기 위해 운영중인 시스템을 중단시켜야 하는 경우가 발생하기 때문에 이런 경우에는 서비스 제공에 차질을 빚게 된다. 또한 취약점을 적절히 해결하는 데도 어려움을 겪을 수 있다. 이외에도 시스템을 구축한 후에 취약점을 보완하는 형식은 본 연구에서 분석한 바와 같이 상대적으로 막대한 비용이 소모된다. 이러한 문제점을 극복하기 위해 기업이 시스템 및 서비스를 구축할 때, 설계부터 구축, 테스트, 운영까지 단계 마다 정보보호를 고려하는, 시스템의 생명주기를 감안한 정보보호 사전진단 수검이 필요하다. 예를 들면 시스템 및 서비스 구축 라이프사이클 관점에서 진행되는 정보보호 수검은 시스템 설계 단계에서 인증, 인가, 암호화, 로깅 등의 요건들을 고려해 보안요구사항을 정의하고, 이에 따른 시스템 설계가 이뤄지도록 한다. 또한 구축 단계에선 시스템의 개별 컴포넌트들이 보안 요건을 반영하고 있는지 등에 대한 점검을 하며, 개발 모듈 단위에 대한 소스와 해당 시스템의 진단과 모의해킹 등을 통해 보안 취약점을 점검한다. 마지막 테스트 단계에서는 시스템 구축 초기 제시된 보안 점검 사항들이 구축된 시스템에 제대로 반영됐는지 등을 점검하는 작업이 이뤄진다. 이렇듯 개발 프로세스 초기 단계에서부터 정보보호를 고려할 경우 다음과 같은 특징들이 발현된다. 사전진단 제도의 특징을 살펴보면 다음과 같다. 첫째, 사전진단 수검은 기술적 정보보호 대책과 함께 운영적, 관리적 대책을 포함한다. 기존의 정보보호컨설팅은 기술적 정보보호 대책을 중심으로 위협분석이 이루어진 반면 사전진단은 그 수검 대상이 기술적 보호대책 뿐만 아니라 적용 서비스의 운영환경에 초점을 맞추어 관리적, 운영적 대책을 포함하는 통합적 관점에서 정보보호를 평가하는 기준 및 체계로 구성되어 있다. 둘째, 사전진단은 비용 및 기술 효과적 보호대책 수립이 가능하다. 사전진단 수검은 정보시스템 및 서비스 구축 시 설계 단계에서부터 보안관리 현황 점검 및 위험분석이 가능하기 때문에 보다 경제적이고, 기술적으로 효과적인 보호대책 구현이 가능하다. 셋째, 사전진단 수검을 통해 보안관리 현황분석 및 위협분석 뿐만 아니라 정보보호 수준개선의 효과도 기대할 수 있다. 테스트 및 운영 단계에서의 정보보호 수준 현황파악이 아닌 설계 단계에서의 정보보호에 대한 기술 및 관리, 운영 등의 고려가 가능함에 따라 서비스 구축 시 피수검자가 정보보호 활동에 대해 수동적 측면이 아니라 능동적이고 자발적으로 정보보호 수준의 개선을 고려할 수 있다.

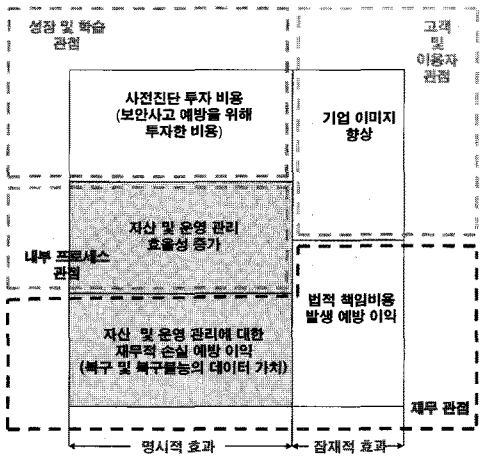
IV. 정보보호 사전진단 효과분석 프레임워크

본 장에서는 3장에서 제시한 사전진단 투자효과를

BSC관점의 정보보호 투자효과 분석 프레임워크에 적용하여 분석하고 사전진단 대상 서비스에 대한 보안사고 비용 산정 모형을 제시한다.

4.1 사전진단 투자효과 분석의 개념 및 중요성

보안사고 예방과 처리에 관련된 비용은 보안사고의 형태 또는 크기에 따라 직접 또는 간접적인 비용의 측면으로 구분할 수도 있고, 명시적 또는 잠재적인 비용으로 구분할 수도 있다[14]. 대부분의 경우에 직접 비용은 명시적인 경우가 많지만 간접비용 중에서도 명시적인 비용이 있을 수 있다. 명시적 비용이란 의미 그대로 눈에 보이는 대로 측정할 수 있는 비용이다. 예를 들면, 암호화, 방화벽, 접근제어, 침입 탐지 장치 도입 등과 같이 보안사고를 감지하고 사고발생 시 복구할 수 있는 모든 기술에 대한 비용이다. 명시적 비용에는 이러한 기술을 설치하고 사용하고 유지보수하는데 드는 비용과 관리자를 교육시키는 데 드는 비용도 포함된다. 이러한 비용들도 대부분 확실한 비용이기 때문에 어떤 곳에 비용이 들어가는지 파악할 수 있고, 그 비용의 크기도 비교적 명확하게 측정할 수 있다. 반면에 잠재적인 비용이란 눈에 보이지 않는 기회비용이라고 할 수 있다. 잠재적인 비용에는 여러 요소가 있는데, 가장 대표적인 것으로 기업에 대한 사용자들의 이미지 손상 등을 들 수 있다. 기업의 이미지 손상은 고객들에 대한 미래의 수요, 주식 가격의 변화 등의 다른 형태로 나타날 수 있으므로 직접적으로 계산하기는 매우 힘들지만 매우 중요하게 고려되어야 하는 대상이다. 보안사고 예방과 처리에 관련된 비용을 직접 비용과 간접비용으로 구분하면 다음과 같다. 보안사고와 직접적으로 관련되는 직접 비용으로는, 보안 기밀 유출을 예방하고, 그 유출행위를 찾아내며 사고 후 복구를 하는데 드는 인건비, 하드웨어, 소프트웨어 구입비와 같은 것들이 포함된다. 직접적인 비용의 형태는 사고의 종류나 크기에 따라 달라지지만, 그 비용의 크기는 보안사고로부터 비교적 정확하게 예측할 수 있다는 특징이 있다. 이와는 다르게 간접적인 비용은 보안사고와 직접적으로 연결할 수 없는 나머지 비용을 나타내며, 해커의 침입을 감지하는데 드는 비용이나 업무절차를 강화하여 보안사고를 미리 예방하는 데 드는 비용을 뜻한다. 따라서 본 연구에서는 사전진단 비용을 업무절차를 강화하여 보안사고를 예방하는데 투자되는 예방비용의 일종으로 정의하고, BSC 관점에서 정보보호 투자의 성장 및 학습관점의 예방투자로 간주한다.



[그림 1] BSC관점의 사전진단 수검효과 분석 프레임워크

본 연구에서 제시하는 BSC 관점의 사전진단 효과 분석 프레임워크는 다음과 같다. BSC 관점의 4가지 측면 즉, 성장 및 학습, 내부 프로세스, 이용자, 재무의 각각 관점 하에 보안사고 발생 시 발생 가능한 비용을 분석한다. 각 관점의 여러 지표는 정량적으로 측정이 가능한 명시적 비용과 정량적으로는 측정이 어려운 잠재적 비용으로 구분되며, 이러한 판단 기준 하에 직접적으로 정량화가 가능한 내부프로세스 관점의 복구비용 및 복구불능의 데이터 가치와 재무관점의 매출이익 손실 및 생산효율저하로 인한 손실 등은 직접비용으로, 고객 및 이용자 관점의 이미지 손상과 재무관점의 법적비용 등은 잠재적 비용으로 분류하였다. 4가지 관점에서 성장 및 학습관점은 보안사고 예방을 위해 투자한 비용으로 사전진단 비용을 포함한 정보보호 투자액을 재무적으로 정량화 할 수 있으며, 사전진단 수검 시 보안사고 발생 가정 하에 예방을 위해 투자한 비용 즉, 사전진단 수검을 받은 경우 사전진단 수검 비용을 성장 및 학습 관점의 1차적인 정보보호 투자로 간주한다. 따라서 사전진단 비용은 보안사고 예방을 위해 투자한 비용으로 성장 및 학습 측면의 정보보호 인프라스트럭처 구축을 위한 비용으로 간주될 수 있다. 반대로 사전진단 수검을 받지 않은 경우는 예방을 위해 투자한 비용이 없는 것으로 간주하여 보안사고 발생 시 관련 복구비용 및 소송비용을 직접비용으로 정량화 할 수 있다. 이는 보안사고 발생 시 정보보호의 목표인 가용성과 무결성을 유지하기 위해 발생하는 복구비용과 기밀성이 침해된 경우 발생하는 소송비용

〔표 1〕 내부프로세스 관점의 사전진단 복구비용 산정 예

구분	복구비용 산정 예
시스템 복구비용	S/W 복구비용 = 피해시스템 수 × 시스템 당 복구 소요시간 × 시스템대당 복구 투입인원
	H/W 복구비용 = 복구불능 피해시스템 수 × 시스템 당 평균 대체비용
	복구 가능한 데이터의 복구비용 = 복구가능 데이터 피해 시스템 수 × 피해 시스템 당 복구 소요시간 × 복구인력의 시간당 인건비
손실된 데이터의 가치산정	복구불능 데이터의 가치(데이터 재생산 비용) = 복구불능 데이터의 양 × 데이터별 평균 재생산 소요시간 × 재생산 인력의 시간당 인건비

을 직접비용으로 분석할 수 있다. 예를 들어, 내부프로세스 관점의 복구비용(Recovery Cost)에 대한 측정 산출식은 다음과 같다. 복구비용 측정은 보안사고 발생 가정 하에, 사전진단 수검을 받지 않은 경우 그 피해액으로 산출할 수 있다. 따라서 사전진단 수검을 받지 않은 경우 보안사고 발생 시 발생한 복구비용을 사전진단 수검을 받은 경우에 사전진단으로 인한 내부프로세스 관점의 손실예방이익 즉, 사전진단 수검의 투자효과로 간주하게 된다. 내부프로세스 관점의 사전진단 복구비용 산정 예는 〔표 1〕과 같다.

4.2 사전진단 대상 서비스의 보안사고 비용 산정 모형

사전진단 대상 서비스의 보안사고 관련 비용 산정 프로토타입(prototype)은 다음과 같다. 1차 피해비용(대체(추가 및 변경)비용)은 소프트웨어, 하드웨어, 관련 문서 등과 같이 대상 정보자산 구성요소의 추가 및 변경비용으로 망실되더라도 시장에서 재구입이 가능한 경우에 해당되며, 시장가격으로 비용을 산정할 수 있다.

$$C1 = \sum_{i=1}^{l} \alpha_i \quad (1)$$

(α_i = i 번째 장비의 시장 대체가격, l = 대체 장비 수)

2차 피해비용(비즈니스 손실 비용)은 장비 추가 및 교체 시 수거를 위한 인력파견 비용 및 서비스 개통일 지연에 대한 보상비용 등 정보 자산 및 서비스에 대한 이용이 불가한 시간 동안에 발생될 수 있는 각종 비용을 의미하며, 업무 중단, 매출 손실, 손실 보상 등의 정상적 업무나 비즈니스 거래의 중단에 따른 비용 외에도 대체 방안 수배 및 그에 다른 직원들의 교육, 초과 근무 수당 등의 항목을 비용으로 산정하고, 또한 이탈한 고객 및 이용자들이 경쟁사로 이동할 경우에 대한 비용과 신규 대기 고객 및 이용자의 이탈에 따른 비즈니스 기회 손실 비용을 의미한다. 이는 정량적으로는 산정이 불가능한 경우가 많다.

$$C2 = \sum_{j=1}^{m} \beta_j + P \quad (2)$$

(β_j = j 번째 장비의 교체 및 수거에 대한 인력파견 비용, m = 교체 및 수거 장비 수, P = 서비스 개통일 지연에 대한 보상비용)

3차 피해비용(비밀유출에 따른 비용)은 개인정보 및 기업비밀 유출에 따른 소송비용 및 대처 비용을 의미한다.

$$C3 = \sum_{k=1}^{n} \gamma_k + Q \quad (3)$$

(γ_k = k 번째 장비를 통해 유출된 개인정보 및 비밀유출에 따른 손해배상 비용, n = 개인정보 및 비밀유출 장비 수, Q = 서비스 제공 불가에 대한 보상비용)

따라서 위에서 열거한 보안사고를 통해 발생하게 되는 장비의 교체 및 변경비용과 이로 인한 비즈니스 손실비용 및 비밀유출에 따른 비용의 합을 총 피해비용(total cost)으로 간주하면 수식은 다음과 같다.

$$TC = \sum_{i=1}^{l} \alpha_i + (\sum_{j=1}^{m} \beta_j + P) + (\sum_{k=1}^{n} \gamma_k + Q) = C1 + C2 + C3 \quad (4)$$

V. 정보보호 사전진단 수검적용 사례에 대한 효과분석

4장에서 논의한 BSC관점의 사전진단 수검효과 분석 프레임워크는 각 관점별 성과지표의 도출, 관점간의 인과관계 분석 등 추가로 수행이 되어야 하는 연구가 방대하기 때문에, 실제 경제적 효과의 측정에 사용되기에는 아직 적합하지 않다.

본장에서는 정보보호 사전진단 수검사례에 대한 효과를 분석하기 위해 2006년도에 실시한 모바일 RFID 시범사업의 일환인 '양주진품 정보서비스의 정보보호 사전진단' 사례에 본 연구에서 제시하는 경제

성 효과 분석 프레임워크를 적용하여 비용을 모의 산정해 보고자 한다[14].

5.1 사전진단 사례 개요

양주진품 정보서비스 사전진단 개요는 양주에 RFID 태그를 부착하여 최종 소비자가 일반 마트에서 휴대폰으로 양주의 진위여부를 확인할 수 있는 서비스이다. 목적은 m-RFID 시범사업의 사전진단을 통해 상용화 시 예상되는 보안위협과 취약성을 사전에 파악하여 적절한 보호대책을 수립하도록 함으로써 서비스의 운영 이전에 안전과 신뢰성을 확보하기 위함이다. 권고된 보호대책으로는 태그정보의 접근암호 관리, 태그조회이력 메뉴 개발 시 정보접근 제한 암호 입력, 웹서버를 통한 상품정보 입력 시 암호 사용 및 포트 차단, 상품판매 후 개인정보추적방지를 위한 태그 폐기 및 암호관리 권고 등이다. 양주진품 정보서비스의 사전진단 대상은 A컨소시엄의 m-RFID 시범사업 중 양주진품 정보서비스를 대상으로, RFID 태그로부터 ODS, OIS 등 RFID 서버들을 포함하여 양주진품 정보서비스를 구성하는 모든 정보시스템 및 정보보호 대책을 그 범위로 포함한다. 또한 양주진품 정보서비스의 사전진단은 기존의 사전진단 수행 절차 및 방법에 따라 5단계 및 단계별 세부 활동으로 나누어 수행되었으며, 서면질의, 산출물 검토, 면담 및 모의해킹을 통하여 이루어졌다.

5.2 사전진단 적용 서비스의 보안사고 비용 산정

사전진단 적용 양주진품 정보서비스의 시범사업 운영환경은 [표 2]와 같다.

[표 2] 양주진품 정보서비스의 사전진단 적용 시법사업 운영환경

구분	양주 진품 정보서비스 시범사업 운영 환경
대상	RFID 태그부착 대상 양주 'B' 위스키 21년산, 17년산
수량	RFID 태그 부착 1만 5천병, 진품 확인용 휴대용 단말 RFID 리더기 135개
단가	부착된 태그 개당 300원, 진품 확인용 휴대용 단말 RFID 리더기 개당 25만원 책정
기간	'08.11.11부터 '08.12.31일까지 51일 동안 시범사업의 경우
참여 업체	제조업체 1개, 도매업체 24개, 유흥음식점 100개, 할인매장 10개의 업체

5.2.1 사전진단 적용 서비스의 보안사고 비용 산정

위와 같은 시범 운영환경을 바탕으로, 사전진단 적용 양주진품 정보서비스의 보안사고 비용 산정을 위한 대상은 다음과 같다. 본 연구에서 분석하고자 하는 사전진단 수검은 기존의 운영단계 또는 일부 테스트 단계에서 적용되던 위협 분석 및 보호대책을 설계 단계부터 적용하는 것이므로, 위협 분석 및 보호대책 적용 시점을 각각 설계 단계, 테스트 단계, 운영 단계로 적용시점을 구분하여 보안사고 발생 가정 하에 각 단계별 수정조치비용을 산정해보고자 한다. 본 연구에서 정의한 비용 산정 프로토타입에 따라 1차 피해비용이 발생하는 대상 장비는 양주에 부착되는 RFID 태그와 진품 확인용 휴대용 단말 RFID 리더기를 적용대상으로 한정한다. 2차 피해비용 적용대상 또한 1차 피해비용이 발생되는 적용 대상 장비의 교체 및 수거에 대한 인력파견 비용이므로 그 적용 대상이 동일하다. 또한 발생되는 RFID 태그와 휴대용 단말 RFID 리더기를 통해 개인정보의 노출이 발생가능하다는 가정을 통해 3차 피해비용을 산정하기로 한다. 1차 피해비용을 산정하기 위해 각 단계별로 수정 조치되는 장비의 수는 [표 2]와 같다. 설계단계에서는 위협 분석 및 보호대책 구현을 위해 단지 재설계 단계만 거치게 됨에 따라 장비의 물리적 교체 및 수정은 없는 것으로 간주한다. 테스트 단계에서는 단계의 특성에 따라 운영단계에서보다는 수정 조치되는 장비의 수가 줄어들게 된다. 예를 들어 [표 2]의 운영단계에서 수정 조치되는 태그와 리더기의 수가 각각 15,000개, 135개라면, 테스트 단계에서는 그 수가 각각 10개, 2개로 줄어들게 된다. 참고로 실제 테스트 단계에서는 실제 장비 대신 그 장비의 기능을 구현하는 에뮬레이터를 사용하지만 본 연구에서는 제한된 수량의 장비 사용으로 실제 테스트 상황을 가정한다. 설계단계에서는 위협 분석 및 보호대책 구현을 위해 재설계 단계만을 거치게 됨에 따라 장비의 물리적 교체 및 수정은 없는 것으로 간주한다. 따라서 관련 장비의 교체 및 수거에 대한 인력 파견비용도 존재하지 않는다. 테스트 단계에서는 장비의 물리적 교체 및 수정 발생가능성이 존재하지만 테스트 시 수정하므로 비용발생은 없는 것으로 간주한다. 그러나 테스트 단계에서 위협에 대한 보호대책 구현의 필요성을 발견하게 되면 장비의 교체 및 수정을 위해 필요한 시간만큼 대상 서비스의 개통 지연이 발생하게 되기 때문에 이에 대한 보상비용이 발생할 수 있다. 운영단계의 수정조치를 위한 인력파견 인원수는 [표 3]

과 같다. 태그 장비는, 1인당 1일 작업가능 개수를 100개로 가정하여 총 장비수로 나누고, 리더기 장비에 대해서는 수정조치를 필요로 하는 사이트(site) 개수로 산정하여 분석한다. 2차 피해비용을 산정하기 위한 각 단계별 장비 수정, 교체, 수거 등의 조치를 위한 인력파견 비용은 1일 기준 136,290원으로, 한국소프트웨어산업협회의 소프트웨어산업진흥법 시행령 제16조에 따른 '08년도 S/W 노임단가 공표를 기준으로 적용하였다. 3차 피해비용을 산정하기 위한 각 단계별 비밀유출에 따른 손해배상 비용 산정은 〔표 3〕과 같다. 설계단계에서는 위협 분석 및 보호대책 구현을 위해 재설계 단계만을 거치게 됨에 따라 비밀유출에 대한 영향은 없는 것으로 간주한다. 따라서 비밀유출에 따른 손해배상 비용도 존재하지 않는다. 테스트 단계에서도 서비스를 개시하기 이전이므로 비밀유출에 대한 손해배상 비용의 발생은 없는 것으로 간주한다. 그러나 테스트 단계에서 비밀유출에 대한 위협을 발견하게 되면 위협에 대한 보호대책 구현의 지연으로 인해 대상 서비스의 개통이 지연될 수 있으므로 이에 대한 보상비용이 발생할 수 있다.

운영단계의 비밀유출에 따른 손해배상 비용은 적용장비 개수를 서비스 이용자 수로 가정하여, 태그 부착 제품 개수와 리더기 개수를 각각 손해배상을 위한 가입자 수로 산정하였다. 또한 개인정보유출에 대한 손해배상 비용은 사전진단 수검 시점과 유사시기의 '07년도 국민은행 개인정보 유출사건에 대해 1인당 배상액으로 책정된 7만원(이메일을 통한 유출)과 '08년도 SK텔레콤사의 유무선 연동 네트워킹 'Tossi' 서비스의 베타테스터 개인정보 유출사건에 대한 1인당 배상 평균비용 7만원을 기준으로 적용하였다.

5.2.2 발생 가능한 위협 시나리오와 비용 산정

보안사고 발생 시 위협 시나리오 별 발생 가능성을 분석하면 다음과 같다. 본 연구에서 분석하고자 하는 시범사업 환경에서는 양주 진품 확인 서비스를 위해 관련 장비로 RFID 태그와 진품 확인용 휴대용 RFID 리더기를 사용하고 있으며, 각각 설계 단계,

〔표 3〕 수검 적용 시점별 비용 산정 적용 대상

수검 적용시점	설계			테스트			운영		
	수정 장비 수	파견 인력 수	손해배상 가입자수	수정 장비 수	파견 인력 수	손해배상 가입자수	수정 장비 수	파견 인력 수	손해배상 가입자수
태그 단가: 300원	-	-	-	10개	-	-	15,000개	150명	15,000명
리더기 단가: 250,000원	-	-	-	2개	-	-	135개	135명	135명

〔표 4〕 운영 단계의 시나리오 별 장비의 교체 및 수정내역

	시나리오 / 장비									
설계단계		가-A	가-B	가-C	가-D	가-E	가-F	가-G	가-H	가-I
	태그	R	R	U	U	R	U	-	-	-
	리더기	R	U	R	U	-	-	R	U	-
테스트단계	시나리오 / 장비	나-A	나-B	나-C	나-D	나-E	나-F	나-G	나-H	나-I
	태그	R	R	U	U	R	U	-	-	-
	리더기	R	U	R	U	-	-	R	U	-
운영단계	시나리오 / 장비	다-A	다-B	다-C	다-D	다-E	다-F	다-G	다-H	다-I
	태그	R	R	U	U	R	U	-	-	-
	리더기	R	U	R	U	-	-	R	U	-

※ 교체: R, 수정: U

테스트 단계, 운영 단계 별로 관련 장비의 교체와 수정에 대한 경우의 수를 정리하면 27가지의 위협 시나리오를 가정해 볼 수 있다〔표 4〕. 각 단계별 시나리오들의 1차 피해비용, 2차 피해비용, 3차 피해비용을 앞장에서 제시한 비용 산정 모형에 적용하여 추정하면 시나리오별로 수검시점과 적용 보호대상이 달라져 관련 피해비용이 각각 다르게 산정된다. 또한 대체비용은 장비의 구매 가능한 시장가격으로 하며, 수정비용은 시장가격의 50%로 가정하여 산정한다.

5.2.3 사전진단 사례에 대한 효과분석

본 연구에서는 사전진단 비용을 업무절차를 강화하여 보안사고를 예방하는데 투자되는 예방비용의 일환으로 분석하여 BSC의 성장 및 학습관점의 핵심성공요인으로 간주하였다. 이를 기반으로, 예방으로 인해 발생하지 않은 보안사고의 수치를 정량화하기 위해 정보보호 진단 수검시점을 각각 설계 단계, 테스트 단계, 운영 단계로 적용시점을 구분하여 보안사고 발생 가정 하에 각 단계별 수정조치비용을 산정하였다. 또한 사전진단 대상 서비스의 보안사고 비용 및 수반되는 피해를 전체 비용으로 산정하였다. 앞서 분석한 것과 같이 본 연구에서는, 보안사고 발생을 가정했을 때, 정보보호 진단 시점을 설계 단계, 테스트 단계, 운영 단계로 나누어 발생되는 예상 손실액을 비교함으로써 수검시점 별 효과를 분석하였다.

따라서 사전진단 수검 시 설계 단계부터 위협 분석 및 보호대책을 적용하는 경우와 테스트 단계와 운영단계에서 위협 분석 및 보호대책을 적용하는 경우를 비교하여 수검시점 적용 단계 별 취약점으로 인한 손실의 크기를 추정하였다. 앞서 가상의 시나리오들을 통해 발생할 수 있는 경우의 손실액을 각 시나리오별 가중치를 동일하다고 가정하고 수검시점 단계 별로 가중평균하여 보안 진단(사전진단 및 사후진단 포함) 검토 수검 단계 별 보안사고 수정조치 비용을 추정하면 〔표 5〕와 같다.

〔표 5〕 수검시점 별 수정조치 평균비용(양주진품 서비스의 경우 예시)

구분	시나리오 가(설계단계)	시나리오 나(테스트단계)	시나리오 다(운영단계)
보안사고 발생 시 수정조치 평균비용	0원	251,500원	751,320,100원
총 보안진단 비용	30,000,000원	30,251,500원	781,320,100원

〔표 5〕에서 설계 단계 수검의 경우인 시나리오 가의 보안진단 수검 비용과 보안조치 비용의 합계는 단계별 보안진단 수검 비용이 30,000,000원으로 동일하다고 가정하였다. 단, 본 연구에서는 사전진단 수검 비용을 약 30,000,000원으로 산정하지만, 실제 사전진단 수검은 진단 대상의 규모와 난이도에 의해 조정될 수 있다. 〔표 5〕에서 보는 바와 같이, 보안진단을 설계단계에 착수하는 것이 운영 단계에 착수하는 것보다 26배(=781,320,100원/30,000,000원)의 비용 절감효과가 있다. 사전진단을 설계단계에서부터 착수되는 보안진단으로 간주하면, 사전진단의 효과를 대략 26배 정도로 산정해 볼 수 있다. 본 연구에서는 사전진단 수검의 정량적이고 가시적인 효과분석을 위해 시범사업에 국한하여 여러 가지 상황을 가정한 상태에서 제한적 분석을 수행하였으나, 사전진단 수검의 적용사례를 시범사업이 아닌 본 사업을 대상으로 확장하여 효과를 추정할 경우, 사전진단 수검의 비용 대비 효과는 훨씬 클 것으로 예상된다.

본 연구에서 적용한 사례인 국내 양주진품 정보서비스의 경우, 시범사업에서 거래되는 양주시장 규모를 약 십억원 규모로 가정했을 때, 본 사업으로 서비스가 확대될 경우 실제 양주시장 규모를 대략 1조원대로 추산하여 비교하면 사전진단의 효과를 대략 23,190배(=695,696,759,259원/30,000,000원)에 달하는 것으로 추정할 수 있다. 사전진단 도입의 효과성은 다음과 같다. 첫째, 보호대책 추가에 따른 발생비용을 감소시킨다. 사전진단 수검을 통해 시스템 및 서비스 운영 이전에 위협 및 취약성 분석을 실시하고 보호대책을 제시함에 따라 운영 중인 시스템 및 서비스의 운영 중지 및 추가(add-on)적인 보호대책 설치를 예방할 수 있다. u-IT 서비스의 대표적 형태인 임베디드 S/W 서비스나 RFID/USN 기술을 이용한 융·복합형 서비스 개발 프로세스에 설계 단계에서부터 정보보호를 확립할 수 있도록 하여 보다 비용 효과적이고 위험관리가 적절하게 구현된 서비스를 가능하게 한다. 이는 빈번하게 변화하고 복잡화되고 있는 정보이용 환경에서 u-IT 서비스 정보시스템의 신뢰도 향상에 필수적으로 고려해야할 요소이다. 이러한 요소는 전반적인 개발 프로세스의 정보보호 역량을 강화시켜 결국 정보보호의 목표인 기밀성, 무결성, 가용성을 제고시킬 수 있다. 둘째, 조직단위가 아닌 사업단위(제품단위가 아닌 시스템 단위)의 수검을 통해 상세한 위협 시나리오 별 위협분석과 이에 대한 적절한 보호대책을

〔표 6〕 사전진단 수검효과 추정(양주진품 서비스의 경우 예시)

		시범사업의 경우	본 사업 확대 시
시장 규모		1,080,000,000원 (유통 양주 수 × 유통 양주 출고가격)	1,000,000,000,000원 ('08년도 국세청 추산규모)
보안사고 발생 시 수정조치 평균비용	설계	-	-
	테스트	251,500원	232,870,370원
	운영	751,320,100원	695,666,759,259원
총 보안진단 비용	설계	30,000,000원	30,000,000원
	테스트	30,251,500원	262,870,370원
	운영	781,320,100원	695,696,759,259원

제시할 수 있다. 사전진단 수검은 정보시스템뿐만 아니라 운영되는 서비스 환경 및 서비스를 대상으로 수검을 실시하기 때문에 기술적 정보보호 대책만을 평가하는 것이 아닌 관리적, 운영적 대책을 포함하는 통합적 관점에서 정보보호를 고려한다. 이를 통해 정보시스템의 구성 요소에 대한 기술적 기능평가와 서비스 운영환경에 대한 비 기술적인 환경평가를 모두 포함하여 정보보호를 고려할 수 있다. 또한 위협등급 별 시나리오 도출을 통해 보호대책 구현현황을 구체적으로 제시하고 주요 위협 시나리오 별 효과적인 보호대책을 제시할 수 있다.

셋째, 사전진단 수검을 통해 서비스 상용화 이전에 개인정보보호를 효과적으로 수행할 수 있다. u-IT 서비스에서는 유·무선 네트워크를 기반으로 이동 단말기기를 통한 개인정보의 다량 수집 및 유출 위협이 증가하고 있으며 다양한 유형과 기능의 무선 단말기 및 운영환경이 갖는 보안의 취약성은 시급한 과제로 부각되고 있다. 안전하고 신뢰성 있는 u-IT 서비스 보급을 위해서는 금융, 위치, 의료, 상황 정보 등 개인정보의 종합적인 보호체계를 정립할 필요가 있다. 또한 이동성이 강화된 서비스의 보안 기밀성 강화를 위해 사전진단의 수검을 통해 위험을 효율적으로 관리하고 최소화할 수 있는 관리체계가 필요하다.

VI. 결 론

본 연구의 대상이 되고 있는 사전진단 대상사업은 개발 소프트웨어 소스코드 공개여부와 서비스 형태의 특성에 따라 그 효과성을 극대화할 수 있다. 복잡화되고 빠르게 변화하는 정보이용환경에서, 소프트웨어의 보안취약성이 정보단말기와 인터넷에 미치는 위협이 더욱 커질 것으로 예상됨에 따라 그로인해 예상되는 보안 취약성을 획기적으로 줄이기 위해서는 사전진단 수검에 대한 적용 및 수검 체계의 체계적 구축 등의 중장기 대응 방안이 효과적이다.

본 사례연구에서 분석한 결과, 사전진단 수검을 통해 설계 단계에서부터 보안취약점을 분석해 적용한 결과 운영단계에서부터 적용되는 것보다 대략 26배(시범사업의 경우)의 소모비용 절감효과를 추정할 수 있는 것으로 분석되었다. 따라서 보안취약성을 효과적으로 제거하려면 개발 초기단계일수록 보안취약성의 해결비용이 크게 감소한다는 점을 감안해 보안성 강화를 위한 사전진단 제도 도입을 적극 고려할 필요가 있다. 본 연구에서는 사례적용을 통해 수검시점 별 보안사고의 손실의 크기를 측정하였다. 이를 위해 사전진단의 타당성 분석을 위한 기초연구로서 기존 정보보호 투자효과를 분석하고 사전진단 제도의 특징을 파악한 후 BSC 관점의 사전진단 제도 효과분석 프레임워크를 제시하였다. 이를 바탕으로 사례를 적용하여, 설계 단계의 수검에 대한 수정조치비용과 테스트 단계, 운영단계의 수검에 대한 수정조치비용을 비교 분석하였으며, 운영 단계 수검 시 발생한 보안사고의 손실의 크기를 사전진단 수검 시 예방되는 손실액으로 간주하였다. 따라서 설계단계에서 적용되는 사전진단 수검 비용을 업무절차를 강화하여 보안사고를 예방하는데 투자되는 예방비용의 일환으로 분석하였다. 이를 통해 설계 단계에서의 정보보호 활동이 최종적으로 재무 관점의 비용절감으로 연결된다는 BSC의 관점 간 인과관계를 검증하였다.

사전진단 제도의 활성화를 위해서는 본 연구에서 예시한 정보보호 사전진단 제도의 경제적 효과를 통해 그 타당성을 부각시킬 필요가 있다. 따라서 사전진단 수검이 적용된 구축 서비스의 경험적 분석자료 축적과 적용 대상 서비스의 확대를 통해 보다 체계적인 효과

분석이 필요하다. 이를 위해서는 사전진단 수검의 효과를 정량적이고 단기적인 측면을 중심으로 분석하기보다는 정보보호 투자효과의 특징을 고려한 정성적·장기적 측면의 효과도 고려되어야 한다. 이는 정보보호 투자효과의 무형성, 다면성, 불명확성, 측정의 시간적 제약 등을 고려하여 BSC 관점에서 사전진단 수검의 효과를 성장 및 학습 측면, 내부 프로세스 측면, 고객 및 이용자 만족도 측면, 재무적 측면까지 분석하여 보다 포괄적이고 체계적으로 그 효과를 분석하기 위함이다. 또한 사전진단 수검의 사례분석 또한 적용범위를 확대시켜, 그 효과를 제시할 수 있도록 관련 자료를 축적해야 한다. 본 논문에서 제시한 BSC 관점의 사전진단 효과분석 프레임워크는 향후 연구에 대한 방향성을 제시한 것에 해당하고, 본 프레임워크가 충분히 활용되기 위해서는 주요성과측도의 도출, 관점간 인과관계 분석 등에 대한 심도있는 연구가 추가로 필요하다. 본 사례연구에서의 수치결과를 사전진단 제도의 경제적 효과로 일반화하는 것에는 한계가 있다. 다양한 사전진단 사례에 대한 분석을 통해 경제적 효과에 대한 보편적인 접근 방법론의 개발이 가능해질 것이다.

이와 함께 사전진단 제도의 법 제도화가 필수적으로 수반되어야 한다. 기존에 수행되고 있는 정보보호 평가 제도인 정보보호 관리체계 인증제도 및 정보보호 안전진단 제도와의 연계도 고려해야 할 것이다. 이를 구체화하기 위해서는 사전진단 수검을 수행한 정보통신 설비 및 서비스에 대해 중복되는 정보보호 관련 인증을 면제 받도록 하는 제도적 장치를 고려해야 하며, 사전진단 수검을 수행한 서비스 사업자에 대하여는 IT 서비스의 신뢰성이 확보된 상황이므로 정부 출연 사업에 대한 신규 사업자 선정 평가 시 가산점을 부여하는 등의 우대를 받을 수 있는 제도적 장치가 요구된다.

사전진단 수검을 받은 IT 서비스 사업자에 대하여 효과분석 사례를 가시적으로 객관화하고 이를 통하여 관련 사업자의 인지도 향상의 기틀을 마련해야 한다. 이를 제도화하기 위해서는 사전진단 수검을 받은 서비스를 대상으로 사전진단 관련 인증을 발급하여 서비스 사용자의 신뢰도를 제고하고 이를 통하여 관련 서비스 제공업자의 인지도를 향상시켜 그 효과를 경영활동에 활용할 수 있도록 해야 한다.

사전진단 제도를 활성화하기 위해서는 개발 프로세스의 가장 초기단계인 기획 단계부터 정보보호를 고려하도록 하여야한다. 기존의 사전진단 수검의 경우, 설계 단계에서부터 정보보호를 고려해 보안 취약점을 점검하는 방식으로 이루어졌으나, 정보시스템 개발 및 서비스 구축의 기획단계에서부터 사전진단 제도를 도입하게 되면 개인정보에 민감한 서비스 구축의 경우 관련 시스템 및 서비스의 특징에 맞게 기획단계에서부터 개인정보보호를 효과적으로 고려할 수 있게 된다. 예를 들어, 유·무선 네트워크를 통해 서비스 이용자의 개인정보가 상호 공유되거나 제공될 수 있는 가능성이 큰 의료서비스와 금융서비스 구축의 경우, 또는 공공기관의 ISP (Information Strategy Planning) 사업이나 USP (U-City Strategy Planning) 사업처럼 정보를 공동으로 활용하는 서비스 구축의 경우, 접근제어와 암호화 기술을 시스템 기획단계시부터 고려하게 되면 프로세스의 설계오류나 기획오류로 인한 발생하는 개인정보 유출문제와 프라이버시 침해문제를 효율적으로 방지할 수 있다.

참고문헌

[1] 김준섭, 손경호, 이완석, 곽진, "캐나다 정보기술보안 제품 사전 검증 제도에 관한 분석," 한국정보보호학회지, 19(2), pp. 87-98, 2009년 4월.

[2] NIST, Security Considerations in the Information System Development Life Cycle, SP 800-64 Revision 2, 2008.

[3] K.J. Soo Hoo, "Tangible ROI through secure software engineering," Secure Business Quarterly, vol. 1, no. 2, pp. 1-3, 2001.

[4] 이은동, 서승우, "사전 예방적 보안과 사후 대응적 보안의 상관관계를 이용한 보안투자 최적화 방안," 한국경영정보학회 춘계학술대회, pp. 588-593, 2009년.

[5] KISA, 정보보호 사전진단 효과분석 및 활성화 방안 연구, 연구보고서, pp. 3, 2008년.

[6] 공희경, 김태성, "정보보호 투자효과에 대한 연구동향," 정보보호학회지, 17(4), pp. 12-19, 2007년 8월.

[7] R. Anderson, "Why information security is hard - An economic perspective," Computer Security Application Conference, pp.358-365, 2001.

[8] K.J. Soo Hoo, How much is enough? A Risk-Management Approach to Computer Security, Stanford University, 2000.

[9] L.A. Gordon and M.P. Loeb, "The economics of information security investment," ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438-457, 2002.
[10] R.S. Kaplan and D.P. Norton, "The balanced scorecard - Measures that drive," Harvard Business Review, pp. 71-79, 1992.
[11] R.S. Kaplan and D.P. Norton, "Having trouble with your strategy? Then map it," Harvard Business Review, pp. 167-176, 2000.
[12] H.K. Kong, T.S. Kim and J.D. Kim, "An analysis on effects of information security investments: A BSC perspective," Journal of Intelligent Manufacturing, Published online http://www.springerlink.com/content/fh33h7688j7626vp/, 2010.
[13] 한국정보보호진흥원, 오픈소스 보안성 관련 이슈 및 대응방안, CSO Briefing, 2008년.
[14] 한국정보사회진흥원, 정보보호 투자 추이분석 및 성과연구, 연구보고서, 2007년.

〈著者紹介〉

공 희 경 (Hee-Kyung Kong) 정회원
2008년 8월: 충북대학교 경영정보학과 졸업
2008년 8월: 충북대학교 경영학 박사
2009년 3월~현재: 한국전자통신연구원 기술전략연구본부
〈관심분야〉 정보보호, 기술경영, 기술경제성분석

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월 ~ 2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월 ~ 2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2000년 9월 ~ 현재: 충북대학교 경영정보학과 교수/BK21사업팀
2010년 7월 ~ 현재: Arizona State University 방문연구원
〈관심분야〉 정보보호 및 정보통신 분야의 경영 및 정책 의사결정