

# 정보보호 사전평가 제도 개발을 위한 국내외 관련 제도검토 및 정보화사업에서의 정보보호 현황분석

An Analysis of InfoSec Implementation Status in the Public Information System Projects for the Institutionalization of InfoSec Pre-Assessment

김정덕\* · 홍기향\*\*

## 목 차

I. 서론	III. 정보화사업에서의 정보보호 현황분석
II. 정보보호 사전평가 관련 제도 검토	1. 조사대상
1. 국내 정보보호 평가 제도	2. 조사과정 및 분석 결과
2. 국외 정보보호 평가 제도	3. 시사점
	IV. 결론

Key Words : 정보보호 사전평가, 정보보호 평가제도, 정보보호 평가 및 승인, 정보보호 분석

## Abstract

The purpose of this paper is to provide several considerations to be taken into account when institutionalizing the information security(Infosec) pre-assessment. Infosec pre-assessment is a necessary process to embed the security requirements into the information systems at the early stages in their development, resulting in more cost-effective infosec. In order to provide some institutional issues, domestic infosec assessment schemes and U.S. Infosec certification and accreditation schemes are reviewed. Also, the current status of infosec implementation in the public information systems projects is analyzed. Based on the analyses, the seven suggestions are proposed in developing and performing the infosec pre-assessment scheme.

\* 중앙대학교 정보시스템학과 교수, jdkim@cau.ac.kr, (031) 620-3061

\*\* 국민대학교 정보관리학과 대학원 박사

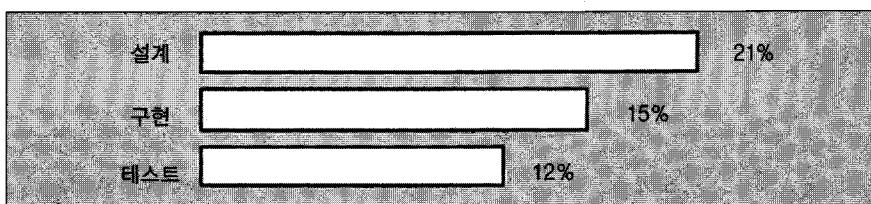
## I. 서 론

최근 정보의 역기능 증가에 따라 정보보호의 필요성이 대두되어 정보시스템의 개발과 운영 과정에서 정보보호를 제공하기 위한 방법이 관심의 대상이 되고 있다. 정보시스템의 정보보호를 제공하는 방법은 지금까지 추가(Add-on) 방식과 내장(embedded) 방식의 2 가지 방법으로 진행되어 왔다.

첫째, 추가 방식은 정보시스템의 설계 또는 구축 이후에 정보보호 제품이나 정보보호 시스템을 추가 구현하는 방식으로, 정보시스템 개발자가 정보보호 전문지식이 없는 경우에 추가적으로 정보보호 전문가로부터 검증 또는 보완을 받는 전통적 방식이다. 때로는 정보보호를 고려하지 않고 정보시스템을 구축한 후 운영 중에 상용 정보보호 제품이나 정보보호 시스템을 도입하여 부족한 정보보호 기능을 보완하는 경우도 볼 수 있다. 추가 방식은 정보보호 요구사항이 시스템 설계에 충분히 반영되지 못하거나 정보보호 제품과 정보 시스템 간의 상호운용성 문제로 정보보호 제품 및 운영 중인 정보시스템의 변경이 요구되는 등 성능 및 비용 측면에서 비효율성이 야기될 수 있는 문제점이 있다.

둘째, 내장 방식은 정보시스템 계획 단계에서부터 정보보호 요구사항을 파악하여 정보시스템 분석 및 설계에 정보보호 기능을 구현하는 방식으로, 초기에는 정보보호 요구사항 파악 및 기능 구현을 위한 시간과 노력이 요구되나 다른 정보시스템 기능과 원활한 상호운용성을 제공할 수 있어 결과적으로 비용효과적인 방식이라 할 수 있다.

정보보호 전문가에 의하면 추가 방식이 내장 방식에 비하여 10배의 추가 비용이 발생하는 것으로 나타났으며(Woods, 1996), MIT 경제학자 Hoo et al.(2001)의 연구에서도 정보시스템 개발 초기부터 정보보호 요구사항을 반영하면 유지 보수 과정의 많은 비용을 절감할 수 있는 것으로 나타났다. 특히, Hoo et al.(2001)의 연구는 정보보호 투자 수익률(Return On Security Investment)을 밝히기 위해 정보시스템 개발의 각 단계에서 정보보호 취약성을 수정하는데 드는 비용의 절감 효과를 측정한 것으로, 연구 결과 <그림 1>과 같이, 정보시스템 개발의 각 단계 중 설계 단계에서 정보보호가 고려될 경우 21%, 구현 단계에서는 15%, 시험 단계에서는 12%의 비용이 절감될 수 있음이 실증적으로 확인되었다.



<그림 1> 정보시스템 단계별 정보보호 투자수익률

정보시스템의 정보보호 제공을 위한 관련 국제 동향을 살펴보면, 정보시스템의 개발 초기에 정보보호를 반영하고 이를 평가하는 절차를 제도화하려는 움직임을 파악할 수 있다. OECD는 2002년 7월에 개정한 정보보호 가이드라인에서 정보통신 시스템 및 네트워크의 구축 및 설계 단계에서 정보보호를 고려하도록 권고하고 있다. 또한, 미국과 같은 선진국에서는 DITSCAP(DoD Information Technology Security Certification and Accreditation Process)과 NIST의 SP 800-37 (Guideline for the Security Certification and Accreditation of Federal IT Systems)과 같은 국방 및 민간 분야의 표준을 통해 정보시스템 구축 및 운영 시 정보보호를 반영하기 위한 평가절차를 시행하고 있다.

그러나 국내에서는 정보시스템의 개발 단계에서 정보보호를 고려하기 위한 제도나 표준이 마련되지 않고 있다. 국내 정보보호 평가제도는 정보통신 기반 시설 취약점 점검, 정보보호 관리체계 인증과 같이 조직을 대상으로 운영 단계의 정보시스템을 평가하거나 정보보호 진흥원의 정보보호 시스템 평가와 같이 정보보호 제품의 보안성을 평가하는데 그치고 있어 공공 및 민간 부분에서 개발 및 구축되는 정보시스템에 대한 평가가 실시되지 않고 있다. 또한 공공 부분의 정보시스템 구축 시 권장되는 정보 시스템 감리제도는 정보시스템의 효과성 및 효율성 평가에 주안점을 둠으로써 정보보호 분야에 대한 평가는 감리 우선순위, 기간 및 비용 등 한계로 소홀히 이루어지고 있으며, 정보보호 평가를 실시할 수 있는 전문 인력의 확보도

미비한 상황이기 때문에 정보시스템 감리제도를 통하여 정보시스템의 개발 및 구축 과정의 정보보호를 평가하기에는 어려움이 있다.

따라서 정보보호의 중요성이 점차 증대하는 사회적 요구에 대응하고, 비용 효과적으로 정보보호를 구현하기 위해서는 정보시스템의 계획 및 개발 초기 단계에 정보보호 기능이 고려될 수 있도록 제도화하는 방안이 필요하다. 이러한 제도의 도입을 위해서는 국내외 정보보호 관련 제도를 비교, 분석하여 시사점을 도출하고, 현재 진행 중인 정보시스템 계획 및 개발 사업의 정보보호 현황을 파악하여 비용 효과적이며, 실효성 있는 정보시스템 정보보호 평가 방법을 도출할 필요가 있다.

본 연구에서는 정보시스템의 정보보호 평가 제도(정보시스템 사전평가 제도)의 도입을 위한 기초 연구로서, 국내외 정보시스템 정보보호 평가 제도를 살펴보고, 정보화사업의 정보보호 현황을 분석하여 시사점을 제시하고자 한다.

## II. 정보보호 사전평가 관련 제도 검토

### 1. 국내 정보보호 평가 제도

국내의 정보시스템에 대한 정보보호 평가 제도를 살펴보면 <표 1>과 같이, 총 9개의 관련 제도가 있으나 이 중 정보보호관리체계 인증, 주요 정보통신 기반시설 평가, IDC 보호 지침,

ISP 보호 지침은 운영 중인 시스템 또는 조직에 대한 평가 제도이고, 국정원 보안성 검토 및 정보보호 시스템 평가는 정보보호 시스템만을 대상으로 하는 평가 제도이며, 감사원 감사는 정보화 사업의 비용 평가를 수행하는 것으로 계획 및 구축 단계의 정보시스템에 대한 정보보호 기능을 평가하기에는 적합하지 않다.

계획 및 구축 중인 정보시스템을 대상으로 하는 평가 제도는 정보시스템 감리 제도와 정보화 사업 평가 제도로 이는 상당 기간 운영되어 정착된 제도이기 때문에 이를 중심으로 정보시스템의 정보보호 평가를 위한 시사점을 찾아보도록 하겠다.

〈표 1〉 정보보호평가관련 현행제도

구 분	평가근거	평가주체(체계)	평가대상
정보시스템 감리	정보화촉진기본법 15조의2 -정보시스템감리기준 (정통부고시1999-104)	한국전산원 민간감리법인	공공부문(정보화지원사업, 지식정보관리사업,부처별 정보화사업) 민간부문
정보화사업 평가	정보화촉진기본법 9조 -국가정보화평가기본계획 (정보화추진위원회의)	정보화추진위원회 (정보화평가위원회, 한국전산원)	정보화사업
국정원 보안성검토	국가정보원법 3조 -정보및정보보호업무기획 · 조정규정 -정보보호업무규정(정보보호 감사,통신정보보호감사)	국정원 중앙행정기관의 장	국가기밀에 속하는 문서 · 자재 · 시설 및 지역에 대한 정보보호업무
감사원 감사	감사원법	감사원	전자정부구현 및 기업정보 화지원 등 첨단정보통신 진흥시책
정보보호 관리체계 인증	방법 47조 -정보보호관리체계인증심사 기준(정통부고시2002-22)	KISA	정보통신서비스제공자 및 물리적시설 제공자
주요정보통 신기반시설 평가	정보통신기반보호법 제9조	기반시설관리기관의 장 (KISA, 정보공유분석센터, 정보보호전문업체, ETRI)	주요정보통신기반시설
IDC보호 지침	방법 46조 -집적정보통신시설보호지침 (정통부고시 2001-83)	정보통신부	집적된 정보통신시설을 운 영, 관리하는 사업자

ISP보호 지침	방법 45조 -정보통신서비스정보보호지 침(정통부고시 2002-7)	정보통신부	정보통신서비스제공자
정보보호 시스템평가	정보화촉진기본법 15조 -정보보호시스템평가인증지 침(정통부고시 2002-41) -정보보호시스템공통평가기 준(정통부고시 2002-40)	KISA(평가), 국정원(인증)	정보보호시스템 (침입차단시스템, 침입탐지 시스템)

### 1) 정보시스템 감리 제도

정보시스템 감리는 「정보시스템의 구축·운영에 관한 사항을 종합적으로 점검·평가하고, 개선이 필요한 사항을 권고하는 것」으로 정보시스템의 효과성 및 안전성 확보를 위한 중요한 수단이다(한국전산원a, 2001).

정보시스템 감리제도는 정보화촉진기본법 제15조의2에 규정되어 있으며, 정보시스템의 정의와 정보시스템의 개발·구축 및 운영 시에 관련 감리기준을 준수하도록 명시하고 있다. 현재까지는 강제 규정이 아닌 권고사항으로 제시되고 있으나 향후 강제 규정으로 만들려는 움직임이 있다 감리제도의 목적은 정보시스템의 효율적 구축 및 운영, 안전성 및 신뢰성의 확보로서 안전성 및 신뢰성 확보를 목적으로 둔다는 점이 정보시스템 정보보호 평가와 공통되는 부분이다.

그러나 정보시스템 감리 제도는 발주자의 요구사항 구현 여부, 정보시스템의 효과성 및 효율성 중심으로 정보시스템을 평가하기 때문에 평가 과정에서 정보보호에 대한 고려는 미미하다. 또한 감리 계획 기간이 상대적으로 짧기 때

문에 정보보호 관련 항목을 심도 있게 선정할 수 없으며, 기본 점검 항목보다는 발주자의 요구에 따른 중점 검토 항목 위주로 정보시스템 평가를 수행하기 때문에 정보보호에 대한 평가 기준 및 결과의 품질이 일정하지 않은 한계가 있다.(한국전산원c, 2001)

한편 정보시스템의 정보보호 평가를 위한 「정보시스템 정보보호 감리 지침」은 정보시스템 계획, 분석, 설계 및 구현의 4단계에 대하여 49개 항목, 213개 세부 점검 항목으로 구성되어 있으나 정보보호 평가를 위한 세부 방법 및 기준을 제시하지 못하고 있어 체계적인 정보보호 평가가 이루어지기 어려운 측면이 있다.(한국전산원b, 2001).

이러한 현행 정보시스템 감리 제도의 문제점과 이에 따른 시사점은 다음과 같다. 첫째, 정보시스템 감리 제도는 정보시스템의 구축 및 이에 따른 효과성 및 효율성의 평가에 중점을 두고 있기 때문에 정보보호 기능에 대한 평가가 취약하므로(김동수, 김현수, 2003) 정보보호 사전평가 제도에서는 정보시스템 계획 및 구축 시 정보보호를 포함한 종합적 평가가 이루어질 수 있도록 해야 할 것이다.

둘째, 정보시스템 감리 제도는 평가 기간이 짧고, 특정 기간에만 평가를 실시하며, 정보보호 평가 인력의 부족 등으로 정보시스템의 정보보호 기능 및 안전성과 신뢰성에 대한 효과적인 평가가 이루어지기 어려운 상황이다.(한국전산원a, 2001). 따라서 정보보호 사전평가 제도는 적정한 평가 시기와 기간을 제시하고, 평가 전문 인력을 확보할 수 있는 방안을 포함하도록 하여야 한다.

셋째, 정보시스템 보안 및 평가 항목이 공공 및 민간, 혹은 기관별로 상이한 경우가 있어 정보시스템 사전평가 제도에서는 이를 포괄하는 종합적인 정보보호 평가 항목을 제시할 필요가 있다.

끝으로, 정보시스템 감리 제도는 정보보호 평가를 기술 아키텍처 평가와 함께 하나의 소분야로 다루어 충분한 시간과 인력을 투입하지 않는 상황이기 때문에 효과적인 정보보호 평가를 위해서는 정보보호 분야의 평가를 강화 또는 별도의 제도로 제도화할 필요가 있다.

## 2) 정보화사업 평가 제도

정보화사업 평가 제도는 정보화사업의 ‘성과 달성을’ 평가하는 것으로 정보보호 전문가가 아닌 평가위원들이 ‘운영 적정성’ 평가 지표 중 일부 보안성에 대하여만 평가를 수행하기 때문에 정보시스템에 대한 정보보호 평가라고 보기에는 어려운 측면이 있다.

그러나 정보화사업 평가 제도는 아직도 개선 점이 남아있지만 한국전산원의 주도 하에 6년 간 운영되어 온 안정된 제도로 정보시스템 사

전평가 제도의 도입을 위한 시사점을 찾을 수 있을 것으로 사료되어 추가 분석이 필요하다.

한국전산원이 발행한 ‘공공부문 정보화사업 평가를 위한 BSC 모형’(2001) 보고서에 따르면 정보화사업 평가 제도는 크게 추진 체계상의 문제와 평가모형 및 측정지표의 문제가 있다.(한국전산원, 2001). 추진 체계상의 문제로는 첫째, 정보화평가위원회의 위상이 낮으며 위원회 구성에 문제가 있다. 정보화평가위원회는 평가기간 동안 운영되는 한시적인 조직으로 정보화사업과 관련한 고도의 조정력 및 평가능력이 부족하며, 평가위원의 구성이 교수에 치중되고 산업체의 전문가가 배제되어 균형이 없고, 교수의 전공이 다양하지만 하나의 사업을 공동으로 평가하는 것이 아니라 개별적으로 몇 개의 사업을 평가하기 때문에 여러 분야의 전문성을 가진 평가위원의 구성에 따른 시너지효과를 거두기 어렵다는 것이다. 따라서 정보시스템 사전평가 제도는 정보보호 평가 인력이 정보보호와 관련된 정보시스템 및 조직의 조정 기능을 수행할 수 있도록 제도적으로 지원하고, 관리, 기술, 물리 보안 등 전문 분야에 따라 팀을 구성하되 하나의 정보시스템에 대한 평가를 공동으로 수행함으로써 시너지 효과를 얻을 수 있도록 팀을 운영할 필요가 있다.

둘째, 평가의 시행 기간이 지나치게 촉박하여 충분한 자료수집이나 면접 등이 이루어지지 못하고 평가가 피상적으로 흐를 수 있다는 지적이다. 또한, 평가에 필요한 자료의 수집에 있어서 각각의 부처마다 다양한 형태로 자료를 제공하기 때문에 평가위원이 일정에 쫓기

는 상황이 발생한다는 점이다. 특히 어느 부처는 전혀 자료를 제공하지 않고 외부평가를 위한 조사서 역시 부실하게 기재하여 평가의 객관성이 떨어지는 문제가 있다고 지적하고 있다. 따라서 정보시스템 사전평가 제도는 피평가기관이 평가를 위한 준비의 기준으로 사용함과 동시에 평가자가 효율적으로 평가를 수행할 수 있는 상세한 평가지침을 제공하여 효율적인 평가가 이루어질 수 있도록 할 필요가 있다.

평가모형 및 지표에 관한 문제로는 첫째, 현재의 평가모형이 공공부문과 정보화사업의 특성을 반영하고 있는가에 대한 의문을 제시한다. 즉, 사업 타당성검토 지표와 과정평가 지표, 사후평가 지표가 혼돈되어 있으며, 사업 성격상 항목별 성과의 차이가 발생할 수 있다는 점 등이 평가 지침에 반영되지 않는 등 세부적으로 의미 있는 평가 항목의 개발이 부족하며, 평가 후 이를 자동적으로 반영할 수 있는 후속 조치 방안이 명확히 제시되어 있지는 않다. 따라서 정보시스템 사전평가 제도는 정보시스템의 수명주기 단계별로 유의한 세부 평가 항목을 개발하고, 이를 지속적으로 개선해 나가도록 해야 할 것이다.

둘째, 정보화사업 평가 제도의 평가 모형은 평가 관점이나 평가 지표가 독립적으로 열거되어 있을 뿐 각 관점 및 지표의 우선순위나 인과관계가 설정되어 있지 않아 평가지표의 복잡성, 불균형성, 중복성의 문제가 야기되고 있다. 따라서 정보시스템 사전평가 제도는 각 평가항목의 우선 순위와 중요도 등을 명시하고 정보시스템 수명주기 간의 일관되게 적용

될 수 있도록 할 필요가 있다.

### 3) 시사점

정보시스템 감리 제도와 정보화사업 평가 제도의 분석을 통해 정보보호 사전평가 제도의 도입 및 확산을 위해 다음과 같은 시사점을 도출하였다. 첫째, 추진체계를 개발할 때, 확실한 법적 근거를 마련해야 하고, 전문성과 공정성을 겸비한 평가팀을 구성해야 한다. 또한 평가에 필요한 충분한 기간을 산정하여 투입해야 하며 평가대상기관에서 제출해야 할 자료양식을 통일하여 일관성 있는 자료제출을 요구해야 할 것이다. 그리고 평가대상기관의 적극적인 참여가 중요한 요인으로 평가목적 및 절차에 대한 충분한 홍보와 의견교환을 통해 자발적인 협조를 유도할 필요가 있다. 또한 제도의 조기 정착을 위해서는 약간의 강제성을 부여할 필요도 있으며 그 방법으로는 정보보호 사전평가 결과를 차기 년도 예산심의와 연계하는 방안도 고려해야 할 필요가 있겠다.

둘째, 정보화사업의 특성을 반영할 수 있도록 상세화(Tailoring) 요소들을 개발하여 보다 유연성 있는 제도를 개발할 필요가 있다. 특히 사전평가 대상이 되는 정보화사업 선정과 평가 수준 결정에서 유연성이 고려되어야 할 것이다. 정보화사업평가에서는 한국전산원이 사업 규모(현재 약 20억 규모를 기준)와 정보화 파급효과, 부처간 연계 필요성, 해당사업의 진척도 등을 고려하여 평가대상사업을 선정하고 있다. 즉, 사업이 일정 규모 이상이 되어야 사전 평가에 대한 비용부담이나 평가준비를 원활히

수행할 수 있기 때문이다. 따라서 평가대상사업 선정 시 사업규모를 고려하는 것은 필요하다 하겠다.

또한, 사업 특성에 따라 평가항목의 우선순위를 달리할 필요도 있다고 하겠다. 즉 정보보호 측면을 평가한다고 하여도 정보화사업의 특성을 고려하여 필요한 정보보호 평가항목에 보다 우선순위를 두어 평가할 필요가 있다.

## 2. 국외 정보보호 평가 제도

국외의 정보시스템 정보보호 평가 제도를 살펴보면, 정보보호 제품에 대한 평가는 1970년대부터 진행되어 왔으며, 조직에 대한 정보보호 평가는 1990년대 중반 이후 제도화되고 있으나, 정보시스템 개발 과정에서 정보보호의 반영 및 구현에 관련된 제도는 최근에 와서 도입되고 있다. 본 연구에서는 미국의 정보시스템 정보보호 평가 제도를 중심으로 국외 평가 제도를 살펴보고, 정보시스템 사전평가 제도의 도입을 위한 시사점을 도출하였다.

### 1) 미 국방부의 정보보호 평가 제도

미 국방부는 1988년 DoD Directive 5200.28, 'Security Requirement for Automated Information Systems'에서 정보시스템의 승인(accreditation)을 의무화하고, 1997년 DoD Instruction 5200.40, 'DoD Information Technology Security Certification and Accreditation Process (DITSCAP)'에서 정보시스템의 정보보호 평

가(certification) 및 승인(accreditation) 과정을 표준화하였다.

DITSCAP은 정보 보증 및 국방정보 기반구조의 보호를 위한 표준 정보시스템 평가 및 승인 프로세스로서 정보시스템과 관련된 전산환경과의 통합적 관점에서 정보보호에 접근하고 있다. 즉, 개발 중인 정보시스템에 대해, 적절한 정보보호 요구사항을 식별하고, 식별된 요구사항을 만족시키도록 설계하며, 설계에 따른 구현을 시험, 평가하고 운영중인 시스템의 모니터링을 통해 필요한 경우 재승인을 할 수 있도록 하는 것이 목적이다.

DITSCAP은 <그림 2>와 같이, 정의 단계(Definition), 검증 단계(Verification), 확인 단계(Validation), 사후 승인 단계(Post Accreditation)의 4단계로 구성되어 정보시스템 수명주기 전반의 정보보호 기능을 제공할 수 있도록 구성되어 있다.

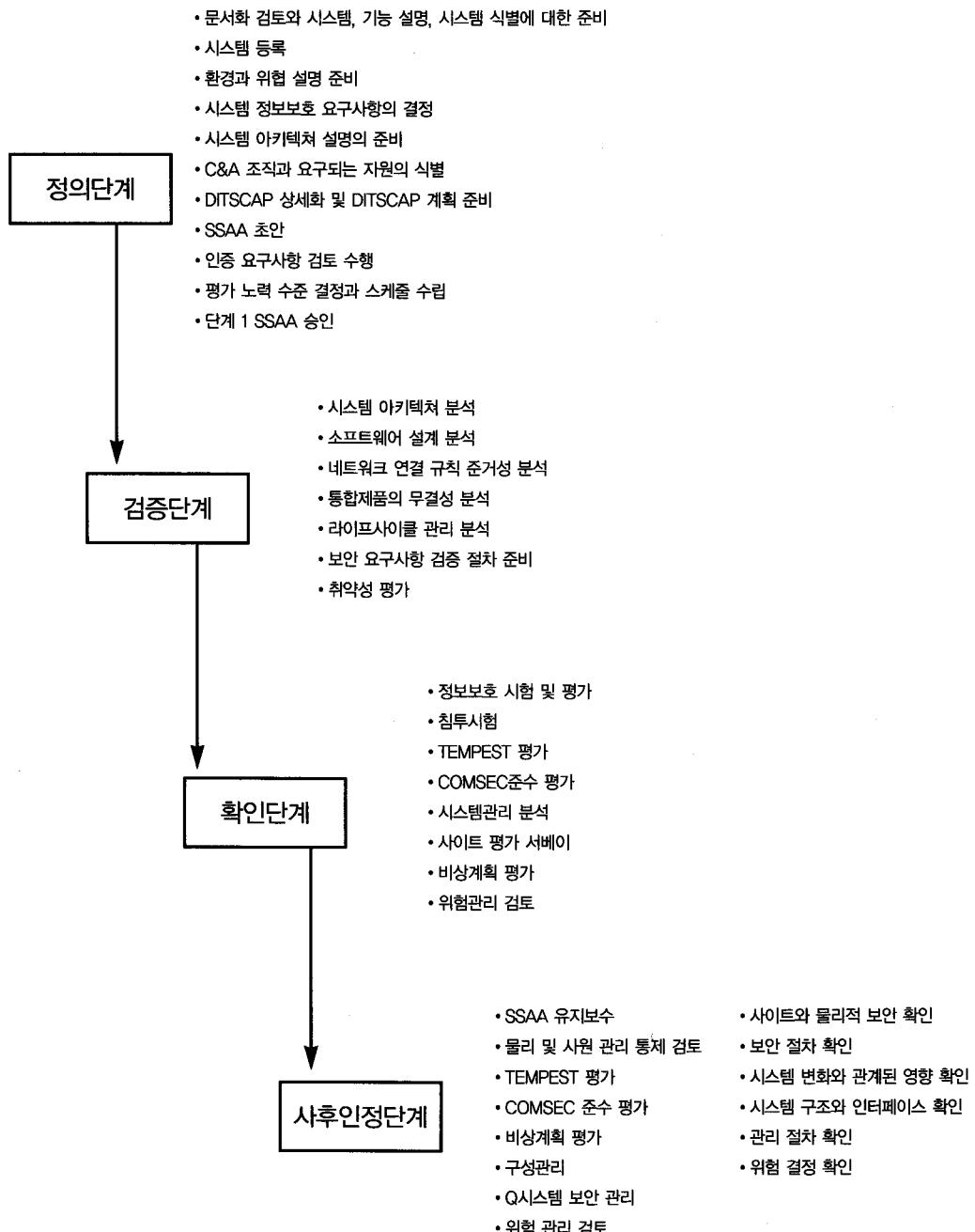
정의 단계는 평가 대상인 정보시스템을 이해하는데 필요한 정보를 획득하고 평가 및 승인 활동을 기획하는 단계로 평가수준을 정하고 이를 관련자간의 협의를 통해 조정한다. 승인 기관 (DAA: Designated Approving Authority)과 평가자를 확인하고, 평가 및 승인 정보보호 요구사항들을 문서화한다. 또한 프로그램 매니저, 승인기관, 평가자, 사용자 대표간의 의견수렴 과정을 통해 시스템 정보보호 승인 동의서(SSAA: Systems Security Authorization Agreement)를 문서화한다. SSAA는 지속적으로 수정 보완되는 살아있는 문서로서 전체 평가·승인 프로세스 전반에 걸쳐 사용된다.

검증 단계는 정보시스템 수명주기 중 시스템 설계 및 개발 단계에서 수행되는 활동으로 정보보호 요구사항이 시스템 설계에 반영되는가를 검증한다. 검증 단계는 정의 단계 이후의 변경사항이 SSAA에 반영되고, 관련자에게 제출되었는지 확인한다. 시스템 개발 완료 후에는 SSAA의 요구사항이 만족되는지를 검증하여 정보보호 명세서, 시험 계획 및 절차, 네트워크 및 기타 연결점 요구사항에 대한 문서를 생성한다. 평가분석 결과를 검토하여 SSAA와 큰 차이를 나타내면, DITSCAP은 문제 해결을 위한 정의 단계로 돌아간다.

확인 단계에서는 SSAA 요구사항과 동의서

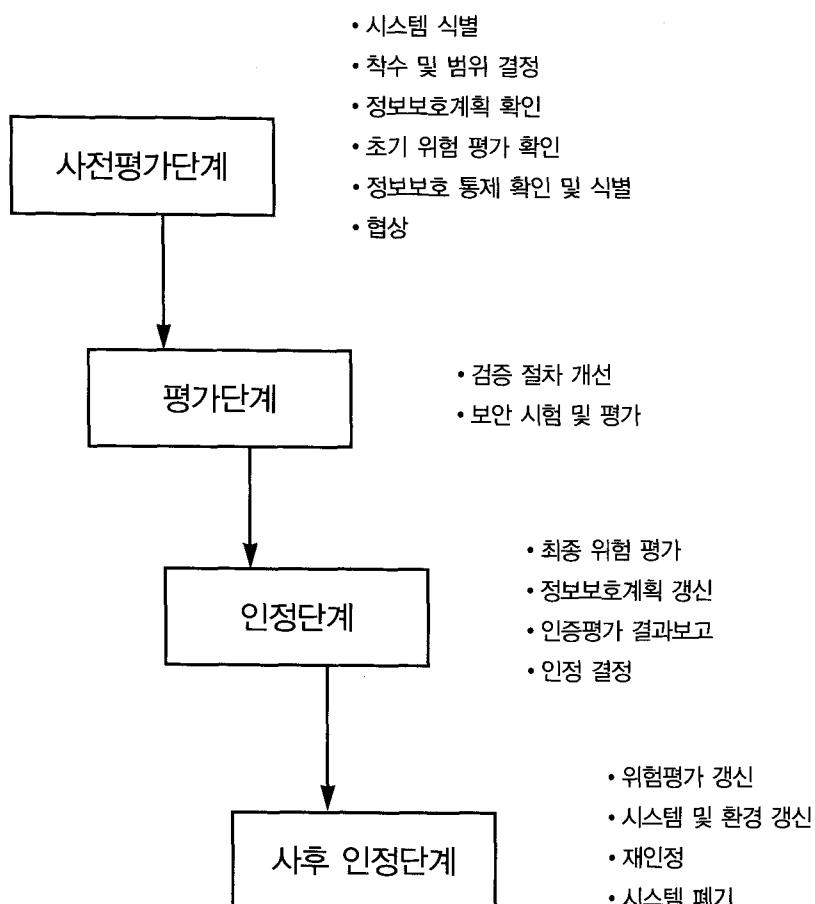
에 포함된 내용이 적용되는가를 확인하기 위해서 SSAA을 검토하고, 통합 시스템에 대하여 SSAA에 명시된 요구사항을 준수하는가를 검토하여 시스템이 수용 가능한 위험 하에서 운영될 것임을 보증한다.

사후승인 단계는 수용 가능한 위험 수준을 유지하기 위해 시스템을 운영하고 유지 보수하는 활동을 수행하는 것으로 시스템이 운영 환경으로 통합된 이후 폐기까지 지속적으로 적용된다. 이 단계에서는 시스템 정보보호 담당자의 역할이 매우 중요하며 시스템 운영자와 관리자, 승인기관과의 협조 하에 시스템의 정보보호 수준을 유지하도록 노력해야 한다.



〈그림 2〉 DITSCAP 단계의 개관

2) 미 표준원의 정보보호 평가 제도  
미 표준원에서는 국가의 정보기반구조를 형성하고 있는 정부 및 공공기관의 정보시스템에 대한 적절한 정보보호 평가를 위해 2002년 3월, 아래와 같은 지침 개발을 수행하기 시작하였다.



〈그림 3〉 평가 및 승인 단계와 활동

- 미국의 핵심정보기반구조를 포함하는 연방 정부기관의 정보시스템을 평가하고 승인하는 지침과 절차를 개발(SP 800-37 문서)
- 모든 연방 정부기관의 정보시스템에 필수적으로 적용되는 정보보호대책 정의(SP 800-53 문서)
- 비용 효과적이고 고품질의 정보보호 평가를 수행할 수 있는 평가인력과 공공 및 민간 평가기관의 양성(SP 800-53A 문서)

NIST 800-37에서는 정보시스템의 정보보호 평가 및 승인을 위해 <그림 3>과 같이, 사전 평가 단계(Pre-Certification Phase), 평가 단계(Certification Phase), 승인 단계(Accreditation Phase), 사후 승인 단계(Post-Accreditation Phase)의 4단계의 프로세스를 정의하고 있다.

사전 평가 단계의 목적은 평가 단계 동안 발생할 가능성이 있는 검증 활동을 준비하기 위한 것으로, ① 시스템 식별, ② 착수 및 범위 결정, ③ 정보보호계획 확인, ④ 초기 위험평가 확인, ⑤ 정보보호 통제 확인 및 식별, ⑥ 협상의 6개 태스크로 구성되어 있다.

평가 단계의 목적은 선택된 검증 기술 및 검증 절차를 활용하여 독립적인 평가를 통해 정보보호 통제대책들이 정확하게 효과적으로 구현되었음을 증명하기 위한 것으로 ① 검증절차 개선, ② 정보보호 시험 및 평가(ST&E)의 2개 태스크로 구성된다.

승인 단계는 평가 단계에서의 결과를 기초로 승인 여부를 결정하고 최종 위험평가를 수행하

여 잔여위험 수준을 적정성 여부를 판단하기 위한 것으로 ① 최종 위험평가, ② 정보보호계획 개선, ③ 평가 결과보고, ④ 승인 결정의 4개 태스크를 포함한다.

사후 승인 단계의 목적은 시스템 구성에 어떤 중요한 변화가 있는지, 또는 시스템에 의해 처리되고 저장되고 전송되는 정보의 기밀성, 무결성, 가용성에 영향을 줄 수 있는 운영 및 위협 환경에 대하여 이상 유무를 결정하기 위해서 정보 시스템의 상태를 감시하는 것을 말한다. 사후 승인 단계는 ① 위험평가 개선, ② 시스템 및 환경 개선, ③ 재승인, ④ 시스템 폐기의 4개 태스크로 구성된다.

### 3) 시사점

DITSCAP과 NIST SP 800-37은 대체로 유사한 정보보호 평가·승인 프로세스를 가지고 있다. 그러나 각 평가체계의 특징을 살펴보면 DITSCAP은 정보시스템의 정보보호 요구사항과 이의 구현 내용을 평가하는데 초점을 두는 반면, NIST 800-37은 평가 및 승인 프로세스를 통한 정보시스템의 정보보호 보증에 초점을 둔다는 사실을 알 수 있다. 이는 DITSCAP가 국가 정보보호에 중요한 정보보호시스템을 대상으로 한다는 점과 NIST 800-37이 민간 부문을 포함하는 정부기관의 정보보호 보증에 초점을 둔다는 문서의 목적에 따른 것으로 파악된다.

따라서 정보보호 평가의 대상이 외무 또는 국방 등 국가 정보보호와 직접적으로 관련되지 않은 공공 기관일 경우에는, NIST 800-37의

평가 및 승인 방식이 보다 적합하다는 것을 알 수 있다.

정보보호 사전평가 제도 도입과 관련하여 미국 사례로부터 얻을 수 있는 시사점으로는 첫째, 공공부문 정보화사업에서의 구축 단계별 정보보호 구현을 위한 평가제도는 미국에서도 비교적 초기 단계라고 할 수 있다. 현재 제도 도입을 위한 지침을 개발 중인 상태이다. 미국 이외의 국가에서는 아직 관련 제도를 시행하고 있거나 계획 중인 국가는 아직 발견되지 않고 있다. 본 절에서 분석한 미국의 자료는 국내 사전평가 제도 수립 시 밴치마킹 자료로서 사용 가능하나, 국내 현실에 적합한 제도 개발을 위해서는 많은 연구가 필요할 것으로 예상된다.

둘째, 관련 제도 도입 및 개선을 위해 충분한 연구와 검토기간을 가지고 있다는 점이다. 즉 2002년부터 2004년 후반기까지 약 3년간의 준비기간 동안 관련 지침과 체계를 구축하고자 하는 2단계 전략은 제도 도입에 따른 노력이 어느 정도 투입되어야 하는 가에 대한 시사점을 주기도 한다. 사전평가제도의 성격 상 평가 기관, 피평가기관, 정보화사업 수행업체, 관련 제도와의 관계 등 다양한 이해관계가 대립될 가능성이 있으며, 가능한 시행착오를 줄이기 위해서는 충분한 준비와 검토기간이 필요하다 하겠다.

### III. 정보화사업에서의 정보보호 현황 분석

#### 1. 조사 대상 선정

본 연구에서는 정보화사업에서의 정보보호 구현 현황을 파악하기 위하여 최근 2년간 수행된 정보화사업 중 규모, 사업의 성격, 개발방법론, 사업자 등 구분에 따라 일부를 선정하여 산출물 검토와 면담을 통한 분석을 실시하고, 분석 결과를 토대로 정보보호 사전평가 제도의 수립과 시행에 참고할 수 있는 시사점을 도출하였다.

정보화사업은 자금 출처에 따라 주관기관의 예산을 사용하는 일반예산 정보화사업과 정보화촉진기금을 사용하는 정보화지원사업으로 구분된다. <표 2>에서 보는 바와 같이, 일반예산 정보화사업과 정보화지원사업은 자금 출처, 관리 주체, 관리 방법 및 규모에 있어 차이가 존재하나 사업의 성격, 주관기관의 정보보호 요구사항, 사업자의 개발방법론 등에 따른 차이는 없는 것으로 나타났다. 자금 출처와 관리 주체는 정보화사업의 정보보호 구현 현황에 있어 차이를 유발하는 요인은 될 수 없으며, 규모와 관리 방법에 있어 정보화지원 사업이 일반예산 정보화사업에 비하여 규모가 크고, 관리가 엄격하기 때문에 정보보호 구현 현황이 일반예산 정보화사업에 비하여 양호할 가능성이 있다.

현황 조사의 목적이 정보화사업에서의 정보보호 구현 현황의 적절성을 파악하고, 정보보호 사전평가와 정보화사업의 정보보호 구현 현황의 차이를 파악하여 정보보호 사전평가 제도의 필요성과 정보보호 사전평가 제도의 시행 방법을 도출하기 위한 것이라고 정의하면 정보

보호의 구현에 있어 보다 양호할 것으로 예측되는 정보화지원사업의 현황을 파악해보는 것이 조사 목적을 위하여 적절할 것으로 사료된다.

따라서 현황 조사의 대상은 최근 2년간 수행된 정보화지원사업 중 규모, 사업의 성격, 사업자의 개발방법론 등 정보보보호의 구현 현황에 유의한 차이를 유발할 수 있는 특징별로 조사 대상을 선정하여 분석을 실시하였다.

먼저 2001~2002 기간의 정보화지원 사업의

규모를 분석한 결과, 〈표 3〉에서 보는 바와 같이, 구축 사업 총 74건의 평균 사업 규모는 20억원으로 나타났으며, ISP 사업 총 9건의 평균 사업 규모는 약 4억원으로 나타났다. 따라서 규모에 따른 조사 대상의 선정은 구축 사업의 경우에는 20억을 기준으로 각각 2건씩 총 4건, ISP 사업의 경우에는 4억원을 기준으로 각 1건씩 총 2건의 정보화지원사업을 대상으로 분석을 실시하였다.

〈표 2〉 일반예산 정보화사업과 정보화지원사업의 차이

구 분	일반예산 정보화사업	정보화지원사업	비 고
자금 출처	주관기관의 예산	정보화촉진기금	
관리 주체	주관기관	전산원	
관리 방법	특이사항 없음	의무 감리 시행	정보화지원사업이 정보보호 현황이 더욱 양호할 가능성이 있음
규모	평균 7 억원	평균 18 억원	정보화지원사업이 정보보호 현황이 더욱 양호할 가능성이 있음
사업의 성격	특이사항 없음	특이사항 없음	차이 없음
주관기관의 보안요구사항	"	"	차이 없음
사업자의 개발방법론	사업자에 따라 상이함	사업자에 따라 상이함	차이 없음

〈표 3〉 사업자의 개발방법론에 따른 조사대상의 선정 기준과 선정 결과

구 分	S사	I사	D사	Y사	비 고
수행 사업 건수	15	11	5	4	총 83건
개발방법론	있음	있음	있음	있음	모두 있음
정보보호구현방법	있음	없음	없음	있음	2개 사업자 있음
관련 산출물	보안계획서 보안정책서	-	-	보안계획서 보안정책서	
선정건수	2	2	1	1	총 6건

다음 정보화지원사업의 성격에 따라 정보보호가 주가 되는 사업은 2001-2002 동안 총 사업 건수 83건 중 5건으로 전체의 6%에 불과하

4개 주요 사업자의 방법론 담당자 및 사업관리자를 대상으로 전화 면담을 실시한 결과, 〈표 4〉과 같이 2개 사업자가 개발방법론에 정보보

〈표 4〉 사업 규모에 따른 조사 대상의 선정 기준 및 결과

구 분	구축사업	ISP사업	비 고
2001-2002 총 사업건수	74	9	총 83건
평균 사업 규모	20억원	4억원	
구분 기준	약 20억원	약 4억원	
선정 사업 (평균 이상)	2	1	
선정 사업 (평균 이하)	2	1	
선정 사업 (합계)	4	2	총 6건(7%)

기 때문에 정보화지원사업의 현황 조사 총 6건 중 1건만 포함하도록 하였다.

다음 사업자의 개발방법론에 의한 정보화지원사업의 정보보호 구현 현황의 차이를 검토하기 위하여 정보화지원사업의 사업자를 조사한 결과, 2001-2002 기간의 정보화지원사업의 사업자는 〈표 4〉과 같이 4개의 주요 사업자가 있음을 알게 되었다. 사업자의 정보보호 구현 방법은 사업자의 개발방법론에 따르기 때문에

호 구현 방법을 포함하고 있는 것으로 나타났다. 따라서 사업자의 개발방법론에 따른 정보화지원사업의 조사 대상은 정보보호 구현 방법을 가진 사업자가 수행한 사업 3건, 정보보호 구현 방법을 가지지 않은 사업자가 수행한 사업 3건을 선정하였다.

이상의 기준에 따라 선정한 정보화지원사업의 조사 대상은 〈표 5〉와 같이 총 6건으로, 구

〈표 5〉 정보화지원사업의 현황 조사 대상

사업명	사업 종류	규 모	사업성격	사업자의 정보보호 구현방법
[1차] 국민지향적 민원서비스 혁신계획 수립	ISP	4억 이상	일반 사업	있음
[2차] 민원서비스 혁신 (G4C) 시스템 구축사업	구축	20억 이상	"	없음
[2차] 인터넷을 통한 종합 국세 서비스체계 구축 2단계	구축	20억 이상	"	있음

사업명	사업 종류	규모	사업성격	사업자의 정보보호 구현방법
국무조정실 ISP	ISP	4억 미만	"	없음
교육정보유통 시범센터 구축	구축	20억 미만	"	있음
행정전자서명인증관리 시스템	구축	20억 미만	정보보호가 주가 되는 사업	없음

축 사업 4건, ISP 4건으로 구성되어 있다.

사업 규모에 따라서는 총 6건 중, 구축 사업의 20억 이상 2건, 20억 미만 2건이며, ISP 사업의 4억 이상 1건, 4억 미만 1건이며, 사업 성격에 따라서는 정보보호가 주가 되는 사업은 전체 6건 중 1건이며, 사업자의 개발방법론에 따라서는 정보보호 구현 방법이 있는 사업이 3건, 정보보호 구현 방법이 없는 사업이 3건으로 구성되어 있다.

## 2. 조사 과정 및 결과

정보화사업의 정보보호 구현 현황을 파악하기 위한 방법으로는 조사 대상으로 선정된 6개 사업의 산출물 검토와 개발자 면담을 실시하였

다. 조사 항목은 제출된 산출물의 정보보호 관련 부분을 파악하고, 정보보호 사전평가의 점검 항목을 기준으로 관련 자료의 존재 유무를 파악하는 방법으로 진행되었다.

ISP 사업의 경우, 현황 분석, 목표 수립, 계획 수립의 과정을 거쳐 작성된 현황분석서, 미래 모형 계획, 실행 계획 등 산출물을 검토하고, 정보보호 사전평가의 항목으로 도출된 내용과의 일치 정도를 비교 조사하였다.

검토 결과, <표 6>에서 보는 바와 같이 현황 분석 단계에서 정보보호의 현황 및 개선 사항을 파악하는 과정을 수행하는 경우는 조사 대상 2 건 중 1건으로 ISP 수행 과정에서 정보보호 현황의 분석이 필수적으로 이루어지지 않고 있음을 알 수 있었다.

<표 6> ISP 사업의 산출물 검토 결과

산출물	정보보호 관련 내용	비고	건수
현황분석서	정보보호 현황 파악(통제 중심)	관리, 물리, 기술적 통제 위주	1
미래모형기술서	정보보안체계구성방안, 보안체계개선안	관리, 물리, 기술적 통제 방안	2
실행계획	이행과제 도출	통제 방안의 이행 과제를 시스템 및 기능 측면에서 제시	2

또한 ISP 수행 과정 중 정보보호 현황 분석을 실시한 사업자는 개발방법론에 정보보호 구현 방법을 가지고 있지 않은 사업자였으며, 정보보호 구현 방법을 가지고 있는 사업자는 현황 분석 단계에서 정보보호 현황 파악을 실시하지 않은 것으로 나타났다. 또한 ISP 수행 중 정보보호 현황 분석이 이루어진 사업의 규모는 평균 ISP 사업 규모보다 작은 4억 미만의 사업이었으며, 정보보호 현황 파악이 이루어지지 않은 사업은 4억 이상의 규모를 가진 사업이었다.

따라서 ISP 수행 과정의 정보보호의 현황 파악은 사업자의 개발방법론, 규모 등과 관계없이 선택적으로 이루어지고 있음을 알 수 있었다.

또한 현황 분석 단계에서 정보보호의 현황 분석이 이루어진 경우에도, 관리, 기술, 물리적 통제의 관점에서 현황 분석이 이루어져 주요 자산의 식별 및 위험 분석은 수행되지 않아 위험과 균형을 이룬 통제의 선택을 확인할 수 있는 자료가 부족하였다. 그러나 현황 분석 단계에서 정보보호 현황 분석이 이루어진 경우에는 이후 단계의 미래 모형과 이행계획을 통하여 보안체계의 개선안이나 이행과제 등이 도출되어 정보보호의 요구사항이 ISP 수행 단계별로 일관되게 추적 가능하였다.

한편 현황 분석 단계에서 정보보호 현황 파악이 이루어지지 않은 경우에도 미래 모형이나 실행 계획에 정보보호의 구현 계획이 포함되어 있어 현황 파악이 없이 기준선 접근 방식에 따라 정보보호의 통제가 선택됨을 알 수 있었다.

따라서 ISP 사업에서 정보보호가 일관되게 고려되도록 하기 위해서는 현황 분석 단계에서 위험 분석을 포함하는 정보보호의 현황 파악이 수행되도록 할 필요가 있음을 알게 되었다.

구축 사업의 경우, 산출물의 검토는 개발과정에 따라 분석서, 설계서, 구현서 및 시험서에 명시된 정보보호 요구사항의 도출, 설계, 구현 및 시험의 실시 여부와 일관성을 확인하였다. 또한 기타 시스템 공통 문서 또는 아키텍처정의서를 통하여 요구사항으로 도출되지 않은 정보보호 통제의 구현 여부를 확인하였다.

검토 결과, <표 7>와 같이 정보화지원사업의 구축과정에서 정보보호의 요구사항은 기능 요구사항, 보안 요구사항 또는 시스템 아키텍처 정의를 통하여 명시되고 있다. 기능 요구사항으로 정의된 경우에는 설계, 구현 및 시험의 개발단계를 따라 요구사항의 추적이 가능하나 시험이 기능 위주로 실시되고 보안이 고려되지 않아 시험이 부족한 측면이 있었다. 한편 보안 요구사항으로 정의된 경우에는 개발단계에 따라 요구사항의 구현 과정을 추적하기 어려운 측면이 있으며, 아키텍처 정의서 등에 명시된 경우에는 구현 과정을 추적할 수 있는 산출물이 존재하지 않고, 보안 측면의 시험도 이루어지지 않고 있다.

따라서 정보화지원사업의 구축 과정에서 정보보호가 일관되게 고려되기 위해서는 분석 과정에서 위험 분석을 포함하는 정보보호 요구사항의 도출되어야 하고, 개발 단계를 따라 통합적으로 관리되어야 함을 알 수 있다.

〈표 7〉 구축 사업의 산출물 검토 결과

산출물	정보보호 관련 내용	비고	해당 천수
분석서	기능 및 보안 요구사항	시스템 관련 요구사항은 아키텍처정의서 등에 기술됨	4
설계서	기능 요구사항의 설계	보안 요구사항의 설계 추적이 어려움	4
구현서	기능 요구사항의 구현	보안 요구사항의 구현 내용 파악이 어려움	4
시험서	기능 요구사항의 시험	기능 위주의 시험이 실시되고, 보안 요구사항의 시험은 없음	4
기타 및 공통	아키텍처정의서	지원 요구사항 등에 포함된 보안 요구사항의 구현 내용	3

한편 정보화지원사업의 정보보호 구현 현황과 정보보호 사전평가 제도와의 차이를 파악하기 위하여 연구 과정에서 개발된 ISP 사업과 구축 사업의 정보보호 사전평가 항목을 중심으로 이미 선정된 6개의 사업에 대한 검토를 실시하였다.

#### ISP 사업의 정보보호 사전평가를 위한 산출

물은 〈표 8〉와 같이 시스템 설명, 보안 요구사항, 초기 위험평가, 정보보호 구현 계획 등으로 현재 ISP 사업의 산출물과는 차이가 있다. 따라서 각 산출물의 주요 내용을 위주로 관련 내용을 담고 있는 기존의 ISP 사업의 산출물과 상세 내용을 파악하였다.

〈표 8〉 ISP 사업의 정보보호 사전평가와 정보화사업 현황 비교

정보보호 사전평가	정보화사업 현황	비고
시스템 설명	미래 모형	일부 시스템 대상으로 한 것으로 내용이 부적절함
정보보호 요구사항	현황 분석, 미래 모형	현재 보안 시스템에 대한 파악 부분은 모두 결여되어 있고, 신규 정보보호 요구사항만이 미래 모형을 통해 일부 기술되어 있음
초기 위험평가	현황 분석, 미래 모형	정보보호의 대상이나 요구사항의 기능 설계는 미래 모형을 통하여 추출되나 정보보호의 특성과 가상 위험 시나리오는 결여되어 있음
정보보호 구현 계획	미래 모형, 실행 계획	대체로 일치함

검토 결과, 정보보호 사전평가의 각 산출물에 포함되어야 할 내용을 담고 있는 기존의 ISP 사업의 산출물이 일부 존재하나 여러 개의 산출물에 나누어져 있어 관련 내용을 파악하기 어렵고, 정보보호 사전평가의 대상이 되는 주요 내용을 포함하지 않고 있는 경우가 대부분이라는 것을 알게 되었다. 따라서 정보보호 사전평가를 실시하기 위해서는 정보보호 관련 내용을 통합된 산출물로 관리하여 정보보호 관련 내용의 정확한 파악이 이루어지고, 사업자에 있어서도 통합된 산출물을 통하여 정보보호 관련 사항을 지속적으로 개선하도록 함으로써 사업 관리의 편이가 증가할 수 있다.

또한 정보보호 사전평가 항목인 현재 보안 시스템 파악, 초기 위험 평가 등은 기존 ISP 사업의 산출물에 존재하지 않는 내용으로 파악되었다. 따라서 정보보호 사전평가를 위해서는 사업자가 ISP의 수행 과정에서 현재 시스템 파악과 위험 분석을 수행할 수 있는 지침과 절차가 제시되어야 할 필요가 있다.

구축 사업에서 정보보호 사전평가의 대상이 되는 검토 산출물은 <표 9>에서 보는 바와 같이 이 분석 또는 계획, 설계, 구현, 시험의 일련의 개발과정에 따른 산출물 및 기타 산출물이 포함되어 있다.

<표 9> 구축사업의 정보보호 사전평가와 정보보호 현황

정보보호 사전평가	정보화사업 정보보호 현황	비고
인정 수준의 결정	-	관련 내용 전혀 없음
시스템 개요	기술 아키텍처 설계서, 운영자 지침서 등	시스템, 운영조직, 사용자 관련 사항은 일부 사업에 명시되어 있으나 보안, 인터페이스, 시스템 현황은 관련 내용이 없음
보호 계획 작성	현행 시스템 분석서 등	일부 보안 기능에 대한 분석이 실시되었으나 위험평가의 수준은 아니며, 보안 통제 결정과 개발 보안계획은 전무함
시스템 개념 설계	분석서	정보보호 요구사항이 기능 요구사항으로 도출된 경우에는 해당되나 보안 요구사항이나 아키텍처 정의에서 명시된 경우에는 해당되지 않음
시스템 개발 및 구현	설계서, 프로그램 사양서	"
기능 시험 및 설명서	단위시험 계획서 및 결과서	"
통합 보안 시험	통합시험 계획서 및 결과서	기능 요구사항과 일부 보안 요구사항에 대한 시험이 실시됨
비기술적 대책 구현	운영지침서	물리, 운용, 인적 보안 대책이 상세하게 명시되어 있음
보호계획서 갱신	-	관련 내용 전혀 없음

검토 결과, 인정 수준의 결정과 보호계획서의 간신과 관련된 내용은 현재 구축 사업의 산출물에서는 찾아볼 수가 없었다. 또한 시스템 개요와 보호계획 작성에 있어서는 일부 관련 내용을 포함하는 산출물이 있으나 중요한 보안과 관련된 사항이 누락되고 위험 분석이 제대로 실시되지 않아 정보보호 사전평가 시 참고하기에는 부족한 현황이다. 또한 시스템 개념 설계, 개발 및 구현, 시험 산출물과 관련된 내용은 기능 요구사항으로 도출된 정보보호 요구사항에 한하여만 일관되게 관리되고 있었으며, 보안 요구사항이나 아키텍처 정의서 등을 통하여 도출된 경우에는 관련 내용의 추적이 어렵고 시험이 이루어지지 않는 경우도 있다. 그러나 비기술적 대책 구현 내용은 운영지침서 등에 상세히 기술되어 정보보호 사전평가에 활용할 수 있는 적절한 내용으로 구성된 경우가 많았다.

따라서 정보보호 사전평가의 실시를 위해서는 현재의 기능, 보안 및 아키텍처 부분에 분산된 정보보호 요구사항을 위험 분석을 통하여 통합적으로 추출 및 관리할 필요가 있다. 더불어 인정 수준의 결정이나 최종 위험 분석 등의 활동에 관해, 사업수행자가 관련 활동을 원활하게 수행할 수 있도록 관련 지침과 절차를 제시하여야 할 것이다.

### 3. 시사점

이상의 검토 결과를 요약하고, 정보보호 사전평가 제도의 수립과 실행에 참고할 수 있는 시사점을 도출하면 다음과 같다.

첫째, 대부분의 ISP 및 구축 사업자가 수행 과정에서 정보보호와 관련된 활동을 수행하지만 시스템 전체적인 측면에서 지속적으로 사업 기간 동안 일관되게 정보보호 활동을 수행하고 있지는 않다. 따라서 사업 기간 동안, 시스템 전체적인 측면에서 지속적으로 정보보호 활동이 수행될 수 있는 사업 관리 방식이 필요하다.

둘째, 현재 대부분의 ISP 및 구축 사업에서는 기능 요구사항, 정보보호 요구사항, 아키텍처 정의 등 정보보호 요구사항이 산재되어 있어 정보보호 구현 현황을 일관되게 관리하고 파악하기 어려운 점이 있다. 따라서 정보보호 관련 사항을 통합 관리할 수 있는 산출물의 체계를 제시하고, 사업 수행 전 기간에 걸쳐 지속적으로 개선하도록 할 필요가 있다.

셋째, ISP 사업의 현황 분석 단계, 구축 사업의 분석 단계에서 정보보호와 관련된 현황과 위험을 파악하기 위한 위험 분석이 적절히 수행되지 않아 위험과 통제의 균형이 이루어지기 어렵고, 사업 전반적 측면에서 위험이 고려되기 어려운 현실이다. 따라서 ISP 및 구축 사업의 초기 단계에서 위험 분석이 실시될 수 있도록 위험 분석의 방법과 범위 등을 지침 또는 절차를 통해 제시할 필요가 있다.

## IV. 결론

정보보호 사고를 예방하고, 효과적이고 효율적인 정보시스템의 개발 및 운영을 위한 정보 시스템의 정보보호 평가는 정보화 시대의 품질

관리 요건으로 자리 잡으면서 그 중요성이 더욱 증가할 것으로 예상된다. 이에 따라 국내에서도 정보시스템의 계획 및 개발 시부터 정보보호를 고려하기 위한 정보시스템 사전평가 제도의 개발을 필요하다.

본 연구는 정보시스템 사전평가 제도의 도입을 위한 기초 연구로서 기존 국내외 제도 및 국내 현황을 살펴보고, 시사점을 도출하고자 진행되었다. 연구 결과, 정보보호 사전평가제도 수립을 위한 시사점을 다음과 같이 제시할 수 있다.

첫째, 법적 근거 및 유사제도와의 차별성 측면에서는 정보시스템 감리제도 또는 국정원의 보안성검토제도 등과의 차별화 또는 통합방안에 대한 검토가 필요하다.

둘째, 평가 대상 사업 범위는 정보시스템 개발사업 뿐 아니라 정보화전략계획수립(ISP)사업을 포함하여 시행될 필요가 있다. 정보보호 사전평가를 위한 대상 사업범위를 정할 경우, 유연성을 부여하기 위해서 일정 기준에 근거한 선정방식(Screening)이 바람직하다고 사료된다. 선정 시 공정성을 보장하기 위해서는 산학연 전문가로 구성된 선정위원회가 구성될 필요가 있다.

셋째, 평가주체 측면에서는 민간업체 보다는 공정성을 반영할 수 있는 공공기관이 수행하는 것이 단기적으로는 바람직하다. 장기적으로는 자체평가 또는 공공 전문 평가기관과 협력 하에 평가를 수행할 수 있으나 이 경우에도 제3의 기관에서 엄격한 검토를 수행할 필요가 있다.

넷째, 평가범위 측면에서는 모든 정보화사업의 정보보호 평가를 위해서 동일한 평가항목을 적용하기 보다는 사업의 특성을 고려한 중점 평가항목을 설정하여 평가하거나, 또는 평가수준을 결정하는 Scoping 방식을 채택하는 것이 바람직하다.

다섯째, 평가시기 측면에서는 정보화사업에 대한 정보보호 평가는 가능한 한 초기 단계인 분석 단계에서의 평가를 통해 정보보호 요구사항의 충분성과 정확성을 평가할 필요가 있다. 그리고 정보보호 요구사항의 구현여부를 평가하기 위해서는 구축완료 시점에서 평가할 필요가 있다.

여섯째, 평가결과의 실효성 확보 측면에서는 정보보호 평가 결과를 차기년도 정보화 예산과의 연계를 통해 평가 결과에 대한 대응조치를 취하게 하거나 정보화사업 주관기관에 정보보호에 대한 책임과 의무를 구체적으로 명시함으로써 제도의 실효성을 도모할 필요가 있다.

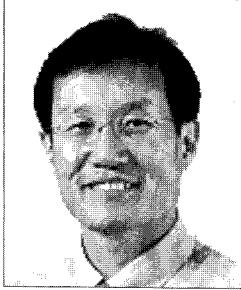
일곱째, 평가능력 제고 측면에서는 평가를 위한 표준 절차, 기법 등에 대한 연구와 훈련 등 충분한 준비 기간이 필요하다. 평가능력에 대한 신뢰성이 낮거나, 평가결과에 대한 일관성 등이 부족하면 평가제도 자체의 성공여부에 중요한 역할을 하기 때문이다.

본 연구는 국내의 정보시스템 정보보호 사전 평가 제도의 도입 시 이상의 시사점을 참고하여 실효성 있는 제도의 수립을 위한 기초 자료로 활용될 수 있을 것으로 사료된다.

## 참고문헌

1. 김동수, 김현수, “정보시스템 정보보호감리 평가와 정량화 방안에 관한 연구,” 2003 한국SI학회 춘계학술대회, 2003.
2. 한국전산원, 정보시스템 감리제도 연구, 한국전산원a, 2001.
3. 한국전산원, 정보시스템 감리제도 추진 기본계획(안), 한국전산원b, 2001.
4. 한국전산원, 감리결과 분석을 통한 주요 문제점 및 개선사례 연구, 한국전산원c, 2001.
5. 한국전산원, 공공부문 정보화사업 평가를 위한 BSC 모형, 한국전산원d 2001.
6. Kevin Soo Hoo, et al., “Tangible ROI through Secure Software Engineering”, SECURITY BUSINESS QUARTERLY, Dec, 2001.
7. NIST, SP 800-18, Guide for Developing Security Plan for IT Systems, 1998. 12.
8. NIST, SP 800-30, Risk Mgmt Guide for IT Systems, 2002. 1.
9. NIST, SP 800-53, Minimum Security Controls for Federal IT Systems, 2003. 5.
10. NIST, SP 800-53A, Techniques and Procedures for the Verification of Security Controls in Federal IT Systems, 2003. 5.
11. NIST, SP 800-14, Generally Accepted Principles and Practices for Security IT Systems, 1996. 9.
12. NIST, SP 800-16, IT Security Training Requirements, 1998. 4.
13. NIST, SP 800-26, Self-Assessment Guide for IT Systems, 2001. 11.
14. NIST, SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, 2002. 10.
15. OMB(Office of Management and Budget), Appendix III to OMB Circular No.A-130 Security of Federal Automated Information Resources, Dec, 1985.
16. U.S. DOD(Department Of Defense) 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process(DITSCAP), 2000. 7.
17. NCSC-TG-031, Certification and Accreditation Process Handbook for Certifiers, National Computer Security Center, 1996. 7.
18. Woods, C., “Effective Information Security Management,” Elesvier, 1996.

## 저자약력



### 김정덕 (Jung Duk Kim)

· 연세대학교에서 정치외교학 학사와 경제학 석사, University of South Carolina에서 MBA, Texas A&M University에서 경영정보학 박사를 취득하고 한국전산원 선임연구원, 원광대학교 정보관리학과 조교수를 거쳐, 현재 중앙대학교 정교수로 재직하고 있다. 한국경영정보학회 및 한국정보보호학회 이사장을 수행하고 있으며 ISO/IEC JTC1 SC27(정보보안기술표준화위원회) WG1 국내위원장을 맡고 있다. 주요 연구분야는 정보보안관리, 업무지속성관리, 시스템감사, 정보보증 등 정보시스템 통제분야와 전자지불 보안 및 신뢰구조를 포함하는 인터넷 비즈니스 시스템이다. 주요 저서로 '미국의 전자상거래 추진전략(소화, 1999)', '전자상거래와 e-비즈니스(쓰리엔테크, 2001), 'e-비즈니스 개론(2002, 도서출판 영민)' 등이 있고, 한국경영정보학회지, 한국정보처리학회지, 정보보호학회지 등에 논문을 싣고 있다.



### 홍기향 (Kih yang Hong)

· 저자는 이화여자대학교 전산과 이학사를 거쳐 국민대학교에서 경영정보학 박사를 취득하였다. 한국전력기술(주), 쌍용정보통신(주)에서 네트워크 구축 및 관리, 인터넷 시스템 개발, 보안 관리 업무 등을 수행하였으며, 현재 한국전산감리원에서 정보시스템 아키텍처 및 보안 감사 활동을 수행 중에 있다. 연구 관심 분야는 정보보호 관리, ITA Security Architecture, Security Auditing 등으로, 관련 논문들을 국내외 학회지 및 학술 대회에 게재한 바 있다.