通信情報保護學會誌
第 8 卷 第 4 號. 1998. 12

응용체계 보안성 평가·승인 절차에 관한 고찰

A Study on Certification and Accreditation Process of Application Systems

김 종 기*

요 약

응용체계 보안성 평가·승인 제도는 정보시스템의 보안성에 대한 품질보증을 위한 핵심적인 수단이다. 응용체계는 동일한 구성요소로 이루어져 있다고 할지라도 운영환경과 이용목적에 따라 보안 요구사항을 달리함으로 적절한 수준의 보안성을 확보하고 있는지를 확인하는 것은 매우 중요하다. 본 연구에서는 응용체계의 보안성을 평가하기 위한 몇 가지 방법론을 절차의 측면에서 살펴보고, 평가·승인 절차에 있어서 핵심적인 고려사항을 기술하였다

핵심어: 보안성 평가, 보안정책

Ⅰ. 개 요

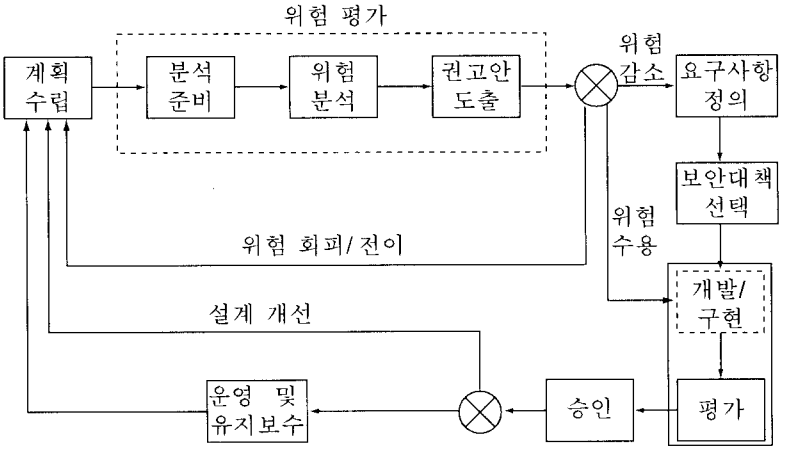
정보시스템의 보안기능에 대한 평가 활동은 상용제품을 위주로 활발하게 논의되고 있고, 우리 나라를 비롯하여 몇몇 국가에서 제도화되어 시행되고 있다. 보안기능을 제공하는 상용제품을 이용하여 정보시스템의 보안 요구사항을 충족시킬 수 있으나, 특정한 목적을 가지고 조직의 업무수행에 직접적으로 활용되는 대부분의 응용체계(application systems)는 상용제품을 시스템의 컴포넌트로 포함할 뿐만 아니라, 응용체계의 개발과정에서 자체적인 보안기능을 구현하기도 한다. 응용체계의 보안기능은 OS, DBMS, 네트워크, 응용 프로그램 등 다양한 구성요소에 분산되어 구현되는데, 아무리 높은보안 등급을 받은 제품들로 구성한 응용체계라고 하더라도 각각이 제공하는 보안기능이 시스템의 통합 차원에서 전체 시스템의 보안성을 보장하는지 확인할 필요가 있다.

정보시스템에서 요구되는 보안기능의 식별, 분석 및 설계, 구현, 그리고 운영에 이르는 일련의 과정은 정보보안 위험관리(risk management)의 틀 속에서 이루어진다. 위험관리는 보안 위험을 허용 가능한 범위 내로 한정하고 그에 수반되는 비용을 최소화하기 위한 제반 활동이다. 정보기술의 급격한 발전과 위험 요소의 역동적인 특성에 기인하는 문제점들로 인하여 보안 위험 요소에 대해 적절하고 즉각적인 대처를 하지 못한다면 보안대책이 비효율적이며 과다한 비용이 소요되는 결과를 초래한다. 따라서, 보안 위험관리는 전반적인 시스템 수명주기에 통합되어 수행되어야 한다.

보안위험을 관리한다는 의미는 위험을 정의하

*국방정보체계연구소

고, 위험의 심각성과 인과관계를 식별하며, 위험을 어떻게 처리할 것인가를 결정한다는 것이다. 식별된 보안위험은 그 파급효과를 감소시키거나, 회피 또는 전이하거나, 수용하게 된다. 위험은 운영적, 절차적, 물리적, 인적, 기술적인 제반 보안대책으로 구성된 보안 시스템의 구현에 의하여 감소시킬 수 있다. <그림 1>에서 나타난 바와 같이 보안기능에 대한 평가·승인은 정보시스템에서 요구하는 보안기능이 적절히 분석되고 구현되었는지 확인하기 위한 절차이다[1].



〈그림 1〉 정보보안 위험관리 절차

Ⅱ. 응용체계 평가·승인의 개념

평가·승인은 실제로 두 가지 독립된 활동으로 이루어진다. 평가는 정보시스템의 보안기능이 조직의 보안정책에 부합하는지 평가하는 과정이다. 즉, 정보시스템의 보안기능과 보안대책에 대한 기술적 평가로서, 특정한 정보시스템의 설계 및 구현이 사전에 정의된 보안 요구사항을 충족하는 정도를 측정하기 위하여 보안기능을 확인, 검증 및 시험하는 행위이며, 시스템이 예상된 대로 운영되는지를 확인하고 새로운 위험을 초래할 가능성이 있는 기능이 있는지를 검토하게 된다[2][3]. 이러한 활동의 주체는 평가기관(certification authority)으로서, 조직의 보안정책이 정보시스템에 구현되어 있고, 허용 가능한 수준에서 보안위험이 관리되고 있다는 신뢰의 척도를 보여주는 문서상의 증거를 확인하는 역할을 한다. 시스템 수명주기에서 평가·승인은 품질보증의 역할과 유사하다[4]. 이러한 측면에서 ISO 9000-3이나 SSE-CMM(System Security Enginee ring Capability Maturity Model), Trusted CMM, B-Method Engineering Environment 등을 정보보안의 평가에 적용하고자 하는 논의가 있다[5][6][7][8].

승인(accreditation)은 "정보시스템이 각종 보안대책을 이용하여 특정한 보안방식(security mode)으로 운영됨을 공식적으로 승인하는 것"[1][2]으로 평가 절차와 기타 관리적인 고려사항을 기반으로 하여 의사결정을 한다. 정보시스템의 운영주체의 입장에서 보면 승인은 "정보시스템의 보안위험을 공식적으로 수용(official acceptance)하는 행위"이다[4]. 즉, 보안대책이 강구되어 있다고 할지라도 여전히 남아있는 잔존위험을 감수하고 정보시스템을 운영함을 승인하는 것으로 정보시스템의 운영에 관련된 보안위험은 완전히 제거될 수 없으며, 설사 제거할 수 있다고 할지라도 비용 대 효과의 측면에서 바람직하지 않다는 전제

를 내포한다.

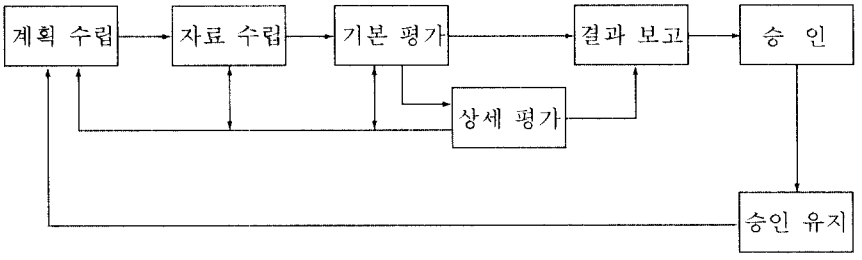
평가·승인을 체계적으로 수행하기 위해서는 방법론(methodology)의 정립이 우선되어야 한다. 방법론은 절차(process), 기법(method), 그리고 기준(criteria)으로 구성되는데[9], 본 고에서는 평가·승인을 수행하는 절차를 중심으로 살펴본다.

평가·승인 절차란 평가·승인을 수행하는 단계를 의미한다. 유의할 사항은 각 단계가 반복적으로 수행될 수 있으며, 여러 단계가 병행적으로 수행되기도 한다는 점이다. 즉, 한 단계의 산출물을 기반으로 이전 단계에서 미진한 활동을 다시 수행할 수 있다. 예를 들어, 평가 범위에 들어있지 않은 중요한 보안기능을 요구사항 평가단계에서 식별하였다면 계획단계에서 설정한 평가범위를 수정하고 추가적인 자료를 수집하게 된다.

평가·승인 절차는 시스템의 개발과 운영 단계를 모두 포함하여야 한다. 시스템 개발단계에서 평가·승인을 수행하는 경우에는 취약성 분석과 보안설계 분석을 통하여 시스템 전체의 차원에서 보안기능의 구현 측면이 강조된다. 평가·승인 활동은 개발절차와 밀접하게 연관되며, 개발단계별로 작성되는 문서를 기반으로 수행되고, 평가·승인 결과는 개발절차에 직접적으로 영향을 미친다. 운영중인 시스템의 평가·승인은 장애일지, 감사기록 데이터, 시스템 운영 통계, 보안위규 사례 등 시스템 운영상에서 작성되는 각종 문서에 기초하여 수행되며, 전체 시스템 중에서 문제 영역만을 분리하여 집중적으로 평가·승인이 수행될 수 있다.

Ⅲ. NIST의 평가·승인 절차

NIST는 민감한 정보를 처리하는 응용체계의 평가·승인을 위한 기술적인 절차를 수립하는데 지침을 제공하기 위하여 PIFS Publication 102[10]를 발간하였다. <그림 2>는 NIST에서 제시한 평가·승인 절차를 보여주는데 모두 일곱 단계로 구성된다.



〈그림 2〉 NIST의 평가·승인 절차

3.1 계획수립 단계

평가·승인을 위한 계획수립에는 문제영역을 식별하고, 평가에 필요한 기술과 지원도구를 확보하고, 인적·물적 소요 자원에 대한 예측하는 등의 활동을 포함한다. 특정 시스템의 환경에 대한 상당한 이해를 전제로 평가과정에서 발생하는 여러 문제들을 예상하여야 함으로 사실상 소규모의 기본평가 단계라고 할 수 있다. 이 단계는 다음의 하부 단계로 구분된다.

준비 단계 : 평가·승인 대상, 목적, 범위, 주요 문제, 제약사항, 입수가능 문서, 적용 기술 등을 식별하고, 평가·승인 대상 시스템의 보안 중요도를 평가하며, 계획 수립에 필요한 소요 시간 및 자원을 예측하고 준비한다.

분 석 : 관련 법규, 지침, 표준, 정책 및 요구사항

을 식별하고, 특정한 평가 방법의 선택과 요구되는 산출물을 정의하는데 필요한 자료를 수집한다. 평가·승인의 범위를 설정하고 시스템 규모와 복잡도, 입수가능한 문서의 품질 등에 따라 작업을 분할한다. 시스템 전반에 걸쳐 포괄적으로 검토되어야 하나, 취약성이 높은 부분은 집중적으로 분석하는데, 분석의 수준에 있어서 기본 평가 단계에서는 기능적 요구사항 수준이다.

필요 자원 확정 : 상기의 분석을 기초로 시간, 전문인력, 행정 지원, 도구 등 평가·승인 활동의 수행에 필요한 자원을 식별한다.

평가·승인계획서 작성 : 이상의 평가·승인 수행을 위한 사전 분석과 필요 자원의 식별 결과를 기반으로 계획서를 작성한다.

3.2 자료수집 단계

평가·승인은 시스템 개발과정에서 생산된 산출물을 기반으로 수행됨으로, 수행되는 대부분의 활동은 자료수집이며, 자료수집에 이용되는 기법은 평가 방법의 핵심적인 요소이다. 수집되는 자료의 정확한 내용은 선택된 평가 방법과 도구에 따른다. 자료 수집의 두 가지 주요 영역이 있는데, 첫째는 시스템이 수행하는 기능은 무엇이고, 이들이 어떻게 수행되는가에 대한 부분이고, 두 번째는 보안 위협에 대한 시스템의 보안 대책에 대한 사항이다. 보안 요구사항, 위험 분석, 시스템 흐름 다이어그램, 시스템 통제 목록 등이 수집되어야 할 핵심적인 자료이다.

3.3 기본평가 단계

기본평가 단계에서는 시스템의 전반적인 보안기능이 평가 대상이 되며, 개별적인 통제기능은 상세평가 단계에서 살펴본다. 기본평가에서는 요구되는 보안기능이 실제로 존재하며, 신뢰할 수 있는 구현방법이 사용되었는지를 검증한다. 반면에, 상세평가에서는 보안기능이 적절하게 작동하며, 성능 기준을 충족하고, 침투에 적절히 대응하는지를 살펴본다.

기본평가에서의 주요 작업은 다음과 같다.

보안 요구사항 평가 : 평가·승인의 주요 목적은 시스템의 보안대책이 보안 요구사항을 만족하는지 결정하는 것이다. 따라서, 보안 요구사항이 잘 정의되어 있을 때만이 의미 있는 평가가 된다. 보안 요구사항 평가에서 운영 환경적 요구사항과 정책적 요구사항 두 가지 영역이 고려된다. 운영 환경적 요구사항을 결정하기 위해서는 시스템의 자산, 보안 위협, 보안 위험 및 보안 통제의 네 가지 사항이 고려되어야 한다.

보안 기능 평가 : 정의된 보안 요구사항이 있을 때 기능 평가가 가장 중요한 요소가 되며, 보안 기능이 보안 요구사항을 만족하고 있는지를 평가한다. 만약 정의된 보안 요구사항이 없다면 기능 평가를 위한 적절한 방법을 찾아야 한다. 보안 요구사항을 식별하기 위해서는 입력, 출력, 처리 절차 및 시스템 성능 요구사항 등 기능적 요구사항을 설명한 문서를 참조한다.

통제 유무 확인 : 문서 또는 인터뷰에서 식별된 보안 기능의 실제 구현 여부를 검사한다.

구현 방법론 검토 : 통제 유무 확인은 보안기능의 존재만을 확인하며, 통제의 질적 수준은 고려하지 않는다. 구현 방법론 검토는 구현된 보안기능의 신뢰성을 보장하는 것이다. 체계적인 시스템 개발 방법론이 적용되지 않았다면 개발 과정에서 결함이 발생할 소지가 큼으로 상세평가가 요구된다.

3.4 상세평가 단계

기본평가 단계에서 추가적인 분석이 필요한 문제를 발견하거나, 시스템의 중요도가 높거나, 처리되는 데이터의 비밀등급이 높은 경우, 또는 주요한 보안기능이 내부기능으로 내장되어 있어 비가시적이거나 기본평가 수준에서 조사가 어려운 경우에는 상세평가가 필요하다. 상세평가는 보안대책에 대한 품질에 대한 분석으로, 다음의 세 가지 관점에서 수행한다.

기능적 운영(functional operation) : 요구되는 기능이 적절히 동작되는지 여부를 확인한다.

성 능 : 가용성 (신뢰성, 중복성, 유지보수성), 생존성, 정확성, 반응시간, 처리량 등의 기준으로 평가한다.

침투저항(penetration resistance) : 보안대책에 대한 확신을 갖기 위하여 통제가 쉽게 깨어지거나 우회될 수 있는지 평가한다.

상세분석의 수행에 있어서 분석 대상 영역을 한정하여 집중적인 조사가 필요하다. 분석의 집중화 전략은 자산, 취약점, 위협 및 보안대책 등 보안 관련 요소를 중심으로 분석하는 방법과 공격 시나리오 분석법, 트랜잭션 흐름 분석법 등 상황 분석 방법이 이용된다.

3.5 보고서 작성

보고서는 평가·승인 활동의 주요 산출물이며 승인권자와의 의사소통 수단이 된다. 승인권자는 평가·승인 보고서를 토대로 보안기능의 적절성에 대한 의사결정을 내린다. 따라서, 보고서는 간결하고 정확하며, 의미 있고 건설적이어야 한다. 평가 보고서에는 승인권자가 평가의 적절성을 확인할 수 있도록 평가 결과뿐만 아니라 평가 과정에 대해서도 서술하여야 한다.

3.6 승인 단계

승인권자는 평가·승인 과정에서 수집된 증거를 검토하여 보안대책의 적합성을 결정하고, 제안된 보완사항을 승인하며, 승인된 보완사항이 차후에 달성되었음을 확인할 책임이 있다. 이러한 활동은 평가·승인 보고서를 중심으로 이루어진다. 평가·승인 보고서의 활용은 다음의 항목들에 대한 사전 검토를 전제로 한다.

- 작업 내용 및 절차에 대한 평가가 가능하도록 검토 가능한 평가 산출물의 존재
- 정확한 데이터의 입수
- 효율적/효과적인 도구의 활용
- 효율적/효과적인 평가 기법의 활용

3.7 승인 유지 단계

시스템은 수명주기 동안에 항상 변화를 겪게 된다. 승인 결정은 시스템이 승인 조건을 유지한다는 전제하에서 내려지게 됨으로 운영·유지 단계에서 발생하는 모든 변화가 승인 조건에 부합하는지를 면밀하게 검토할 필요가 있다. 승인 조건의 변경을 유발할 가능성이 있는 상황은 다음과 같다.

- 시스템 형상의 변화
- 요구사항의 변화 (정책, 제도 포함)
- 승인 유효기간의 경과
- 중대한 보안사고의 발생

시스템의 모든 변경사항에 대해서 재승인이 필요한 것은 아니다. 변경의 중요도에 따라서 승인권자와 평가·승인 절차를 달리한다. <표 1>은 시스템의 변경의 수준에 따른 상이한 평가·승인 절차를 보여준다. 시스템에서 발생하는 모든 변화는 형상관리(configuration management) 절차를 통하여 통제된다. 시스템의 변경사항이 경미한 경우라 하더라도 시스템 자체의 중요도나 처리되는 자료의 비밀등급이 높다면 변경된 사항에 대하여 시험과 승인을 하여야 한다.

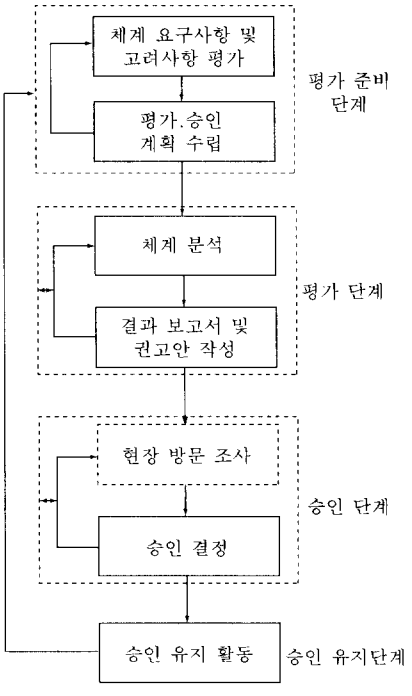
〈표 1〉 재승인 수준

변경의 정도	승인권자	평가 · 승인 절차
기본적인 보안설계에 영향을 미침 (예: 접근통제 패키지의 도입)	최초 승인권자	변경되지 않은 부분을 포함하여 시스템 전체에 대하여 전반적인 평가 · 승인 절차 적용
시스템 규격에 식별된 두 개 이상의 보안 모듈에 영향을 미치는 변경 또는 주요 하드웨어의 추가 또는 변경	중간 관리자	변경된 부분에만 적용 보안 관련 부분에 공식적 시험 실시
하나의 보안 모듈에만 영향을 미침	운영부서	일상적인 형상관리 절차 적용 공식적인 시험 불필요

Ⅳ. NCSC 평가 · 승인 절차

정보보안에 투입 가능한 자원의 감소와 기술의 급격한 발전은 시스템의 보안에 대한 평가와 정보보안 시스템 공학 절차의 구현에 변화를 초래하였다. 이러한 변화는 단편성을 감소시키고 시스템의 보안에 대한 모든 측면의 일관성과 호환성을 보장하고 유지하기 위하여 필요하다. 또한, 역동적인 위협 환경은 정보보안 영역을 더욱 효율적이고 통합된 관점에서 조망할 필요성을 요구한다.

시스템의 전반적인 보안을 고려함에 있어서, 시스템의 목표를 충족하고 변화하는 환경에서 요구되는 보안 기능을 제공하기 위하여 두 가지 핵심적인 개념, 즉 시스템의 보안 목표를 명확히 식별하고, 시스템의 능력에 대한 분석을 수행하여야 한다. 미 국방부는 이러한 개념을 정립하여 정보시스템을 운영하기 전에 기술적 분석과 관리적 승인을 반드시 거치도록 규정화하였다. 기술적 분석을 통하여 시스템이 운영환경에서 임무 수행에 필요한 일련의 구체적인 보안 요구사항을 충족하는 정도를 확인하며, 관리적 승인은 주어진 위험 수준에서 운영하는 책임을 공식적으로 수용하는 것이다. 이러한 기술적 분석과 관리적 승인절차를 통하여 통합적이고 비용 효과적인 정보시스템 보안을 제공할 수 있으며, 이를 위하여 필요한 가장 중요한 작업중의 하나는 일관된 평가 · 승인 지침을 개발하는 것이다. 이를 위하여 미국방부의 NCSC(National Computer Security Center)는 <그림 3>과 같은 평가 · 승인 절차를 제시하고 있는데, 크게 네 단계로 구성되며, 각 단계는 승인 사후 단계를 제외하고 두 개의 하부단계로 구성된다[11]. <표 2>는 평가 · 승인 단계별로 주요 고려사항을 보여준다.



〈그림 3〉 NCSC 평가 · 승인 모형

4.1 평가 준비 단계

첫째 단계는 시스템의 보안에 관련된 측면들을 식별하고 평가하는데 초점을 두며, 관련된 문서를 수집하

고 개발하는 활동을 수행한다. 관련 문서는 정책 구현 지침, 보안 규정 및 지침, 이전의 승인 보고서, 설계문서 등이다. 이러한 문서를 획득함으로써 이후 단계를 수행하기 위한 방향을 설정할 수 있다. 관련 문서의 수집과 분석 이후에는 평가·승인 계획을 수립한다. 정보보안은 시스템 개발의 구상과 더불어 고려되어야 함으로 평가·승인 계획은 시스템 보안 계획에서 자연스럽게 도출되어야 한다. 즉, 평가·승인 절차를 수행하기 위한 자원(인력, 장비 및 교육/훈련)과 기준점(milestone)이 식별된다. 평가·승인 계획에 대한 모든 정보는 시스템의 문서에 통합되어 관리된다.

4.2 평가 단계

평가 단계에서는 시스템 전체의 보안 측면을 분석한다. 즉, 시스템 전반에 걸쳐서 정보보안이 얼마나 잘 적용되었는지 살펴본다. 이 단계를 통하여 평가 팀은 시스템의 보안 요구사항과 개별 시스템 요소의 보안 측면에 친숙하게 된다. 이 단계에서는 시스템의 보안 대책이 요구사항을 적절히 만족하고 있는지 확인하는 활동이 수행된다. 이러한 목적을 달성하기 위하여 여러 가지의 보안대책이 통합적으로 평가되고 시험된다. 또한 시스템의 취약성과 잔여 위험이 식별된다. 분석이 끝나면 평가보고서와 승인보고서를 준비하기 위하여 이전 단계의 분석 결과와 권고안을 문서화하고 조정한다. 평가 활동의 결과는 승인 의사결정을 지원하는 문서로 사용된다.

〈표 2〉 NCSC 평가·승인 단계와 주요 고려사항

단 계		주요 고려사항
평가 준비 단계	체계 요구사항 및 고려사항 평가	- 임무 중요성 - 기능적 요구사항 - 체계 보안 영역 - 보안 정책 - 보안 운영개념 - 체계 요소 및 특징 - 외부 인터페이스 및 연결 요구사항 - 보안 운영방식 또는 전체 위험지수 - 체계 및 데이터 소유권 - 위협에 관한 정보 - 승인주체(DAA)의 식별
	평가·평가 계획 수립	- 이전 결과의 재사용성 - 수명주기 단계 - 시스템 이정표 (시간 제약성)
평가단계	체계 분석	- 요구사항 충족도 - 취약점 및 잔여 위험
	결과 보고서 및 권고안 작성	- 평가 보고서 작성 - 승인 보고서 작성
승인 단계	현장 방문 조사	- 평가 보고서 검토 - 필요한 경우 현장 방문 조사 수행
	승인 결정	- 전반적 위협 수준 - 체계 중요성/필요성 - 평가 결과 및 권고안 - 잔여 위험 - 비용효과적인 다른 보안대책의 존재
승인 사후 단계	승인 유지활동	- 승인 범위 내에서 체계 운영 - 재평가/재승인 수행

4.3 승인 단계

세 번째 단계는 현장 조사를 먼저 수행하는데, 이것은 선택적이다. 현장 조사는 보안 요구사항이 시스템의 요구사항을 충족하는지 확인하기 위하여 수행된다. 이때 식별된 잔여 위험이 시스템의 임무를 지원하는데 허용 가능한 수준인지를 확인하기 위하여 최종 시험이 수행된다. 분석결과와 현장조사에서 입수한 정보를 토대로 하여 승인 의사결정을 내린다. 이러한 결정은 전반적인 위협, 시스템의 필요성/중요성, 평가 결과 및 권고안, 잔여 위험, 대체적인 보안대책의 비용 또는 가용성 등의 여러 가지 요인을 고려하여 내려진다.

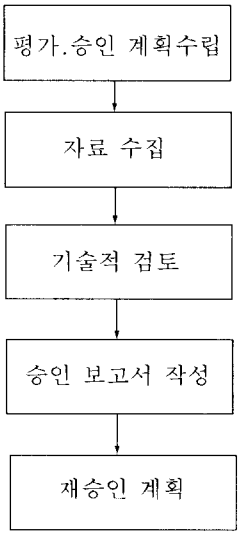
4.4 승인 유지 단계

마지막 단계에서는 시스템 운영자에 의하여 수명주기동안 승인 조건을 유지하는 활동을 수행한다. 승인 조건을 벗어나는 중대한 변화가 시스템에 발생하면 재평가 및 재승인 활동이 필요하다.

V. Hardy의 승인 절차 모형

Hardy[11]는 ITSEC을 기반으로 한 정보시스템의 보안성 승인을 위한 절차 모형을 제시하였는데, <그림 4>와 같이 다섯 단계로 구성된다. 첫 단계는 계획수립 단계로서 획득 가능한 지침을 기반으로 특정한 시스템에 적합하게 승인 과정을 설정하고, 승인 절차에 소요되는 시간과 노력을 추정하며, 승인에 요구되는 상세 수준과 보증 수준을 결정한다. 두 번째 단계는 자료수집 단계로 승인 활동에 필요한 문서를 결정하고, 문서의 내용에 대한 최소 요구사항을 정의한다. 다음에 문서를 수집하고 문서의 완전성을 검토한다. 세 번째는 기술적 검토 단계로서 각 문서의 완전성, 내부적 일관성, 타 문서와의 일치성, 그리고 전반적인 품질을 확인한다. 각 문서에 대해서 변경 없이 수용하거나, 사소한 수정 후 수용, 중대한 변경이 필요하여 수용 불가 또는 승인 목적에 합치하지 않아 완전히 거부하는 결정을 내리게 된다. 문서에 대한 검토 후에 평가자는 개별적인 보안 기능에 대해 추가적인 시험이 필요한지를 결정하게 된다. 추가적인 시험은 단순히 기능이 수행됨을 관찰하거나 메커니즘에 대한 상세한 분석을 수행한다.

네 번째는 승인 보고서를 작성하는 단계로 검토 결과를 요약한다. 승인 결과는 완전 승인(full accreditation), 부분적 승인(partial accreditation), 그리고 제한적 승인(limited accreditation)으로 구분한다. 제한적 승인은 시스템 전체가 승인되기는 하지만 시스템을 운영하여야만 하는 긴급한 이유로 인하여 제한된 기간 동안에만 승인 유효한 것이다. 보통 이 기간 동안에 시스템이나 환경에 일부 변경이 이루어진다. 승인서에는 시스템 운영에 책임진 기관이 일반적으로 수용되는 위험보다 높은 수준의 위험을 감수하고 운영하는 것을 수용함을 서술하는데, 재평가는 이러한 변경에만 적용된다.



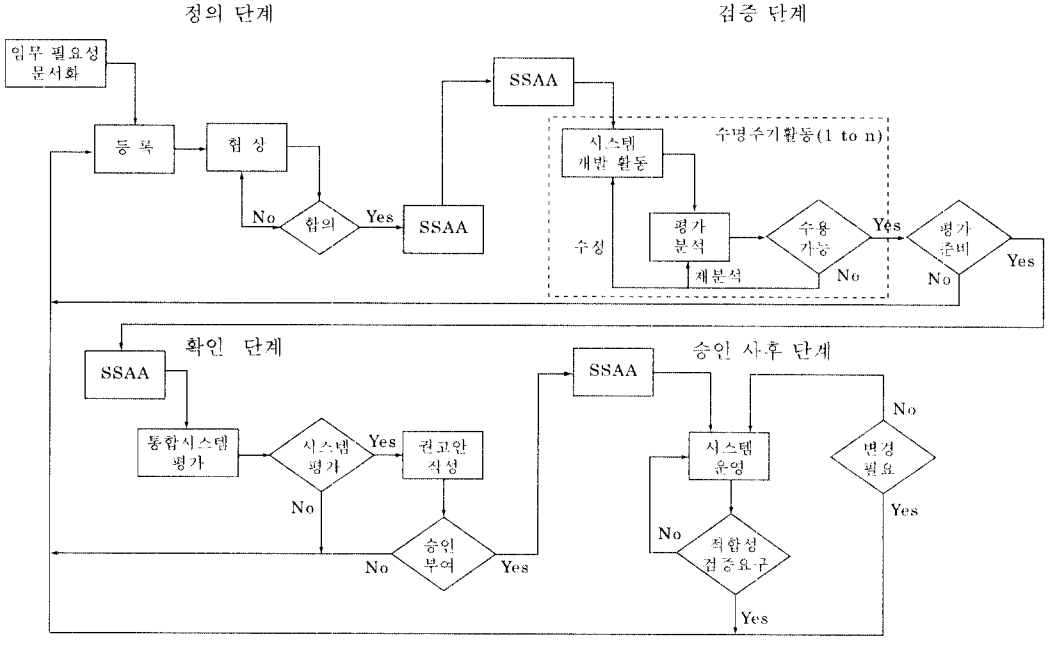
〈그림 4〉 Hardy의 승인절차모형

부분적 승인은 시스템의 의도된 기능 중에 일부만이 승인됨을 의미한다. 전체 승인을 획득하기 위하여 필요한 변경이 일정 기간 동안 수행되거나, 보안기능이 결여되거나 불충분하기 때문에 위험이 증대하여 제한된 기간 동안이라도 허용할 수 없을 경우에 부분 승인이 이루어진다. 마지막 단계는 재승인 계획을 수립하는 것이다. 시스템 자체, 운영환경 또는 시스템의 목적이 변경된 경우에는 승인의 기준도 변하며, 시스템의 재승인을 유발한다. 승인 보고서에는 승인 결과에 영향을 미치는 변경 분야가 명시되어 있으면 시스템에 특정한 변경이 발생하였을 때 재승인이 필요한지 판단하기가 쉽다.

Ⅵ. DoD의 평가·승인 절차

미 국방부는 국방정보기반구조(Defense Information Infrastructure; DII)를 구성하는 요소(entities)들을 보호하기 위하여 표준화된 평가·승인 절차를 수립하여 DoD Instruction 5200.40으로 공표 하였다[1][4]. 이 지침은 정보보안의 측면에서 시스템의 임무, 운영환경, 구조(architecture)를 고려하여 시스템의 운영이 DII에 미치는 영향을 평가하는 절차로서, 국방정보기술보안 평가·승인 절차(Defense Information Technology Security Certification and Accreditation Process; DITSCAP)라고 불린다.

DITSCAP은 <그림 5>에서와 같이 정의(definition), 검증(verification), 확인(validation), 그리고 승인 사후(post accreditation) 단계(phase)로 구성되어 있다. 각 단계는 복수의 활동(activity)으로 구성되며, 각 활동은 여러 개의 절차(procedure)와 작업(task)으로 구성된다. 단계와 활동은 모든 시스템에 대해 적용되며, 절차와 작업은 시스템과 시스템의 수용 가능한 위험 수준에 따라 선택적으로 적용된다. DITSCAP는 순차적인 것은 아니며, 반복적으로 수행된다.



〈그림 5〉 DITSCAP의 전반적인 과정

DITSCAP의 핵심은 정보시스템의 사업관리자, 승인권자 (Designated Accreditation Authority; DAA), 평가자 (Certification Authority; CA), 그리고 사용자간에 주요 일정표, 예산, 보안, 기능성, 성능 등의 문제에 대하여 합의를 기반으로 한다는 점이다. 합의된 사항은 시스템 보안 승인 합의서 (System Security Accreditation Agreement; SSAA)로 문서화되며, 평가·승인의 전반적인 절차에 지침을 제공하고 평가·승인의 결과를 문서화하는데 활용된다. SSAA를 통하여 시스템의 개발이 시작되기 전에 또는 시스템에 어떤 변경이 발생하기 전에 요구되는 보안 수준에 대하여 구속력 있는 합의를 도출한다.

6.1 정의 단계

DITSCAP의 첫 번째 단계인 정의 단계에서는 보안 요구사항과 승인을 득하는데 필요한 노력의 수준을 결정하기 위하여 임무, 환경 및 구조를 이해하는데 중점을 두고 있다. 이 단계에서 수행되는 작업들을 통하여 DAA와 CA를 식별하고, 보안 요구사항을 구현하는 방법에 대하여 사업관리자, DAA, CA, 그리고 사용자 대표간에 합의를 도출하여 SSAA에 문서화한다. SSAA에는 시스템 임무, 목표 환경, 목표 구조, 보안 요구사항, 그리고 적용되는 데이터 접근 정책이 포함된다. 정의 단계는 임무 필요성 (mission need) 문서화, 등록, 그리고 협상의 세 가지 활동으로 구성된다.

6.1.1 임무 필요성 문서화

식별된 운영 요구사항이나 임무의 필요성에 부응하기 위하여 정보 시스템을 신규로 개발하거나 변경하고자할 때 DITSCAP이 개시된다. 임무 필요성은 시스템의 요구사항을 기술하고 시스템의 의도된 능력을 묘사하는 문서 또는 정보의 집합체이다. 일반적으로 임무 필요성은 DITSCAP이 개시되기 전에 상위 수준의 요구사항 문서에서 설명된다. 임무 필요성에서 보안과 관련 있는 정보는 다음과 같다.

- 시스템 임무, 기능 및 시스템 인터페이스
- 운영 조직
- 정보 범주 및 분류
- 예상되는 시스템 수명 주기
- 시스템 사용자 특성
- 운영 환경

6.1.2 등록

사업관리자, DAA, CA, 그리고 사용자간의 공식적인 의견 교환이 시작되는 단계이다. 등록 활동의 일환으로서 적용 가능한 정보보안 요구사항을 결정하고, 위험 관리와 취약성 평가 활동을 개시하며, 평가·승인 활동을 위한 계획이 수립된다. 등록은 임무 필요성의 검토에서 시작하여 SSAA 초안의 준비로 끝난다. 등록 활동에서 수행되는 작업은 다음과 같다.

- DAA, CA, 및 사용자 대표에게 시스템이 평가·승인이 필요함을 알린다. 즉, 시스템을 등록한다.
- 임무 설명과 시스템 식별자를 준비한다.
- 환경과 위협 설명을 준비한다.
- 시스템 구조 설명과 평가·승인 범위를 준비한다.
- 정보보안 시스템 등급을 결정한다.
- 시스템 보안 요구사항을 결정한다.
- 평가·승인에 관련된 조직과 필요한 자원을 식별한다.
- DITSCAP 작업을 테일러링하고, 평가·승인 수준을 결정하며, DITSCAP 계획을 준비한다.
- SSAA 초안을 개발한다.

6.1.3 협상

정보시스템의 개발, 획득, 운영, 및 보안 평가와 승인에 참여한 모든 관련자들이 시스템 등록 활동에서 식별된 보안 요구사항을 충족시키기 위해 사용되는 구현 전략에 동의하는 과정이다. 협상이 진행되는 동안 동의에 이르러야 하는 주 대상은 사업관리자, DAA, CA, 사용자 대표 등이다. 협상의 목적은 시스템 설계에 포함된 보안기능 또는 운영환경에 구현되는 관리적인 절차를 이용하는 보안 방법론에 동의를 이끌어 내는 것이다. 협상 작업은 다음과 같다.

- SSAA 초안 검토
- 평가 요구사항 검토회(Certification Requirements Review: CRR) 수행
- 최종 SSAA 승인

CRR은 SSAA에 포함되는 정보(임무 및 시스템 정보, 운영과 보안 기능성, 운영환경, 시스템 분류, 보안 정책, 시스템 보안 요구사항, 알려진 보안 문제점 또는 약점과 기타 보안 관련 정보)에 대하여 사업관리자, DAA, CA, 사용자 대표 등이 검토하여 보안 요구사항을 구현하는 접근법에 대하여 합의를 이끌어내기 위하여 개최된다.

6.1.4 SSAA

SSAA를 작성하는 목적은 정보시스템의 평가·승인 조건에 대하여 관련 당사자들간의 합의를 문서화하는데 있다. SSAA는 전체 DITSCAP 동안에 활동 지침을 제공하고, 결정된 사항을 문서화하고, 정보보안 요구사항을 명시하며, 가능한 해결책을 식별하고, 운영되는 시스템의 보안을 유지하는데 활용된다. SSAA를 작성함으로써 시스템, 보안정책, 보안구조 등 평가·승인에 필요한 정보를 한 곳에 집중하여 불필요한 중복과 혼란을 피하고 문서화에 소요되는 과도한 노력을 줄이는데 있다. SSAA의 목적은 다음과 같다.

- DAA, CA, 사용자 대표, 사업관리자 사이의 공식적인 합의의 문서화
- 승인에 필요한 모든 요구사항 문서화
- 정보시스템 수명주기 동안 사용되는 모든 보안 기준 문서화
- 가용한 정보를 SSAA에 통합함으로서 문서화 요구사항 최소화
- DITSCAP 계획 문서화

6.2 검증 단계

검증은 개발 또는 변경된 시스템이 SSAA에서 합의된 요구사항에 합치하는지 확인하는 단계이다. 검증 단계의 목적은 평가 시험을 받을 수 있는 완전히 통합된 시스템을 생산하는데 있다. 검증 단계는 지속적인 SSAA 개선, 시스템 개발 또는 변경, 평가 분석, 그리고 분석결과 평가 활동으로 구성된다.

6.2.1 SSAA 개선

SSAA는 DITSCAP 전 과정을 통하여 시스템의 최신 상태를 반영할 수 있도록 검토되고 갱신된다. SSAA를 검토하고 갱신하는 경우는 다음과 같다.

- 필요에 따라 임무 설명과 시스템 기능 설명을 갱신한다.
- 필요에 따라 운영, 소프트웨어 개발 및 유지보수 환경을 갱신한다.
- 시스템 세부 사항이 포함되도록 시스템 구조 설명을 갱신한다.
- 요구에 따라 조직과 자원을 갱신한다.
- 필요에 따라 DITSCAP 계획을 갱신한다.

6.2.2 시스템 개발

정보시스템 컴포넌트를 개발하고 통합하기 위해 요구되는 활동이다. 구체적인 활동은 전반적인 사업 전략, 수명주기 관리 절차, 수명주기 상에서 정보시스템의 위치 등에 의해서 결정된다. 평

가 분석 활동은 정보시스템의 개발과 변경의 각 수명주기 동안에 따라야 하는 SSAA의 요구사항이 충족됨을 보장하기 위하여 수행된다. 따라서, 각각의 시스템 개발 활동은 대응하는 평가 분석 작업을 거치게 된다.

6.2.3 평가 분석

정보시스템이 3 단계(확인)에 의해서 평가되고 시험될 준비가 되어있는지 결정하는 활동이다. 즉, 이 단계에서 개발, 변경, 통합 노력이 다음 단계가 시작되기 전에 평가 가능하고 승인 가능한 정보시스템이 되도록 보장하기 위하여 수행된다. 검증 단계에서 수행되는 평가 작업은 다음과 같다.

- 시스템 구조 분석
- 소프트웨어 설계 분석
- 네트워크 연결 규칙 적합성 분석
- 통합된 제품의 무결성 분석
- 수명주기 관리 분석
- 취약성 평가

6.2.4 분석 결과 평가

수명주기의 각 개발단계가 종료되기 전에 분석 결과가 SSAA에 적합한지 여부를 검토한다. SSAA를 중대하게 벗어난 결과가 나온다면 문제해결을 위해 1 단계로 돌아간다. 수용할 수 있는 결과가 나오면 다음 단계로 진행한다.

6.3 확인 단계

3 단계는 완전하게 통합된 시스템이 SSAA에 명시된 정보에 일치하는지를 검증하는 것으로, 시스템 운영에 대한 승인을 받아들일 수 있도록 DAA에 요구되는 증거를 제시하는데 있다. 즉, 운영 환경에서 구현될 관리적인 절차 또는 시스템 설계에 포함될 보안기능을 활용하는 보안 방법론에 동의하는 것이다. 확인 단계는 SSAA 개선, 통합 시스템 평가, 권고안 작성, DAA 승인 등의 활동으로 구성된다.

6.3.1 SSAA 갱신

확인 단계는 요구사항과 합의가 여전히 적용되고 있음을 보장하기 위해 SSAA의 검토로부터 시작한다. SSAA에 대한 검토는 3 단계 전반에 걸쳐 이루어진다. 통합된 정보시스템을 수용하는 각 단계에서 시스템의 현재 상태를 반영하기 위한 세부사항을 SSAA에 추가하여 갱신한다. 요구되는 변경은 DAA, CA, 프로그램 관리자, 사용자 대표 등에게 제출되어 승인되고 실행되게 된다.

6.3.2 통합 시스템 평가

이 단계에서는 SSAA에 명시된 요구사항을 만족하고 수용할만한 잔여 위험을 가지고 운영되는 완전하게 통합되고 운영 가능한 시스템을 평가하는 것이다. 통합된 시스템의 배치가 가능한 수준으로 기능적으로 준비되었는지 평가하기 위하여 다음의 평가 작업이 수행된다. 평가 작업의 범위와 수준은 SSAA에 합의된 평가 분석의 수준에 의해서 결정된다.

- 시스템 보안 시험 및 평가
- 침투 시험
- TEMPEST 및 Red-Black 검증
- COMSEC 적합성 확인
- 시스템 관리 분석
- 사이트 승인 조사
- 비상 계획 평가
- 위험기반 관리(risk-based management) 검토

6.3.3 권고안 작성

모든 평가 작업이 종료된 후에 통합된 시스템에 대한 평가를 수행하는 동안에 발견된 결과를

종합하여 DAA에게 CA의 보고서를 제출하고, DAA가 승인 의사결정을 내리는데 활용하기 위하여 권고안이 작성된다. 통합된 정보시스템이 SSAA의 기술적 요구사항을 만족한다고 판단되면 CA는 시스템 인증서(certification)를 발급한다. 시스템의 보안을 향상시키기 위한 사항들이 권고안에 포함될 수도 있으며, 이것은 향후에 시스템을 개선하거나 변경관리 의사결정에 활용된다.

시스템의 보안 문제점을 발견하였지만 단기간 동안의 시스템 운영에는 수용 불가능한 위험이 존재하지 않는다고 판단되면, 특정한 기간 동안에 문제점을 바로 잡는다는 단서를 붙여서 승인 권고안을 제시할 수 있다. 이러한 문제점은 SSAA에 반영되어야 하며 시스템 운영의 조건과 문제점의 개선 기한에 대하여 합의하여야 한다.

6.3.4 승인 결정

DAA의 승인 의사결정은 CA의 권고안, DAA의 운영 승인 권한, 근거 문서, SSAA 등으로 구성되는 승인 패키지를 기반으로 내려진다. 근거 문서는 시스템 등급에 따라 차이가 있지만, 최소한 평가 결과, 문제점, 운영상의 위험을 포함하여야 한다. 승인 패키지에는 권고된 의사결정을 뒷받침하기 위하여 필요한 정보가 포함되어야 한다. 승인하는 것으로 결정한다면, 정보시스템이 어떤 운영 환경에서 운영되는지에 대한 사항이 포함되어야 한다. 시스템이 SSAA에 기술된 요구사항을 만족하지 않지만 임무의 중요성으로 인하여 시스템 운영을 해야만 한다면, 일시적인 승인이 주어진다. 임시 승인을 발급하기 위하여 수용된 해결책, 일정표, 필수적인 보안 활동 등을 협의하기 위해 1 단계를 다시 거쳐야 한다. 승인 결정이 내려짐으로써 SSAA의 책임이 시스템 운영기관으로 이전된다.

6.4 승인 사후 단계

승인된 정보시스템에 대한 잔여 위험이 수용 가능한 수준으로 유지하기 위해 요구되는 활동이 수행된다. 승인 사후 관리 활동은 SSAA의 지속적인 유지보수, 시스템 운영, 변경 관리, 적합성 확인 등으로 구성된다.

6.4.1 SSAA 유지 보수

시스템의 운영이 계속되는 동안에도 SSAA를 최신의 상태로 유지해야 한다. 승인 사후 단계는 모든 요구사항과 합의 사항이 지속적으로 적용되도록 SSAA를 검토한다. 임무, 환경, 구조 등의 변경에 대한 승인이 SSAA에 문서화되어야 한다.

6.4.2 시스템 운영

정보시스템의 안전한 운영과 운영환경을 고려하여 시스템 유지보수 작업을 수행할 때 승인조건 내에서 지속적으로 운영되도록 하여야 한다. 안전한 시스템 관리는 조직과 절차에 의존하며, 사이트의 운영 직원과 정보보안관리자는 수용 가능한 수준의 잔여 위험을 유지할 책임이 있다. 시스템 운영 작업에는 시스템 유지보수, 시스템 보안 관리, 비상 계획 등이 포함된다.

6.4.3 변경 관리

정보시스템이 특정 환경에서의 운영을 승인받은 후에는 정보시스템과 운영환경의 변경은 통제되어야 한다. 변경 자체는 기반구조와 정보시스템의 전반적인 보안성에 부정적으로 작용할 수 있지만, 사용자의 요구와 기술의 발전에 부응하여 변경이 지속적으로 이루어진다. 보안 위협이 점차 복잡해지거나 특정 자산에 집중해짐에 따라 보안 대책이 추가되거나 강화되어야 한다. 변경 관리 작업은 시스템 형상관리의 지원과 위험기반 관리의 검토로 이루어진다.

6.4.4 적합성 검증

시스템과 운영환경에 대한 검토는 SSAA에 명시된 간격으로 주기적으로 수행되어야 한다. 이 활동의 목적은 SSAA에 명시되고 합의된 보안 요구사항, 현재의 위협평가, 그리고 운영개념에 대한 합치성을 보장하는데 있다. SSAA의 내용이 정보시스템이 활용되는 곳의 기능적 환경을 적절하게 설명하고 있음을 확인하기 위하여 다음의 작업을 통하여 적합성을 검토한다.

- 물리적 보안 분석
- SSAA 검토
- 위험기반 관리 검토
- 절차 분석
- 적합성 재검증

Ⅶ. 평가·승인 절차의 비교와 고려사항

이상에서 살펴 본 평가·승인 절차들을 비교하면, NIST의 절차[10]는 기본평가와 상세평가 단계를 구분하여 평가영역을 집중화하는 전략이 특징적이다. NCSC의 절차[11]는 조직적 차원에서 업무분장을 반영하기 위하여 평가단계와 승인단계를 엄밀하게 구분하고 있으며, Hardy[12]는 ITSEC을 기반으로 민간환경에서 응용체계의 평가 절차를 제시하고 있다. DITSCAP[13][14]는 응용체계의 개발절차와 평가·승인 절차를 밀접하게 연계시키며, 평가·승인 절차를 상세하게 제시하고 있다. 또한, SSAA로 평가·승인에 관련된 정보를 집중하여 관리의 효율화를 도모한다.

응용체계의 보안성 평가·승인 절차를 수립할 때에는 다음의 몇 가지 사항을 고려하여야 한다. 첫 째는 보안성 평가·승인 절차가 시스템의 개발방법론 내에 반영되어 개발이 진행됨에 따라 평가·승인 절차가 자연적으로 진행되도록 하여야 한다. 우리 나라 공공기관의 경우 관계 규정에 따라 보안성 승인을 받도록 되어 있는데, 일반적으로 개발이 끝난 후 운영되기 전에 평가·승인이 이루어짐으로써 개발과정에서 미비점이 발생하여도 개선할 여지가 없게 된다. 평가·승인 절차가 개발과정에서 수행되어 응용체계의 보안성을 확보할 수 있는 보안대책이 지속적으로 검토되고 반영되도록 하여야 한다.

둘 째는 평가·승인에 관련된 이해 당사자간의 역할 분담이 명확히 되어야 한다. 응용체계의 개발에는 사용자 또는 사용자를 대신한 사업관리자, 개발자, 평가자, 승인권자 등이 관련된다. 응용체계의 보안대책을 식별하고 구현할 책임은 개발자에게 있으며, 사용자 또는 사업관리자는 개발자의 활동이 적절하게 수행되는지 확인하고 감독할 책임이 있다. 평가자는 식별된 보안대책이 해당 응용체계의 운영환경에 비추어 적절한 것인지를 확인하고 구현된 보안대책이 보안 요구사항을 충족하는지에 대하여 기술적인 측면에서 검토한다. 승인권자는 해당 응용체계의 운영에 최종적인 책임을 지며, 평가가의 기술적인 검토와 관리적인 고려사항을 기반으로 응용체계의 운영에 따른 잔여 위험의 수용 여부에 대하여 결정한다.

셋 째는 평가·승인에 필요한 문서화 요구사항을 충분히 반영하여야 한다. 평가·승인의 과정은 체계의 개발 과정에서 생산되는 산출물을 기반으로 이루어지는데, 사업관리 절차상에서 요구하는 산출물에 보안성의 평가·승인에 필요한 문서를 포함할 필요가 있다.

마지막으로 수명주기 관리의 측면에서 재평가·재승인 요건을 명확히 정의하여야 한다. 전형적인 재평가·재승인 요건은 다음과 같다.

- 응용체계에서 처리되는 데이터의 비밀등급 변화
- 외부 네트워크/시스템과의 연동
- 시스템의 주요 구성 요소(운영체제, 응용프로그램 등)의 변경
- 체계의 정상적인 운영을 저해하여 보안성에 심각한 영향을 미치는 보안사고의 발생

· 정보시스템을 수용하는 시설의 물리적 구조 변경 또는 이전

Ⅷ. 결론

응용체계의 보안성 평가·승인은 정보시스템의 기능, 성능, 품질, 신뢰성 등의 요구사항에 대한 일반적인 검증 활동의 일환으로 수행되어야 한다[15]. 평가·승인을 수행함으로써 정보보안의 적절성에 대한 품질보증 수단을 제공하며, 조직 내부의 보안 인지도의 향상에도 기여한다[10]. 정보시스템 평가·승인은 국가 및 공공기관 뿐만 아니라, EC/CALS의 도입에 의한 정보시스템의 개방화, 네트워크화 추세에 따라 조직간의 위험 전이 현상을 방지하기 위하여 민간 기업에도 적용하고자 하는 논의가 있다[12][16]. 따라서, 응용체계에 대한 평가·승인 제도는 정보시스템 전반의 보안성 향상을 위하여 필요한 제도이다.

정보시스템 보안 평가·승인 제도는 정보시스템의 보안성을 보장하기 위한 핵심적인 수단이다. 평가·승인 제도의 합리적인 시행을 위해서는 체계적인 방법론의 정립이 우선되어야 한다. 본 고에서는 평가·승인 방법론의 구성요소인 절차, 방법, 기준의 세 가지 요소 중에서 절차를 중심으로 살펴보았다. 평가·승인을 체계적으로 수행하기 위해서는 세 가지 요소를 통합적으로 적용해야 한다. 따라서, 평가·승인 방법 및 기준을 평가·승인 단계별로 세부적으로 식별하는 것이 향후 연구되어야 할 것이다. 평가·승인이 정보시스템 수명주기 전반에 걸쳐 수행되어야 한다는 관점에서 볼 때, 응용체계의 개발 방법론과 평가·승인 방법론간의 연계성을 구체화하는 방안에 대해서도 추후 연구가 필요한 부분이다.

〈참고문헌〉

[1] CSE, Guide to Security Risk Management for IT Systems, Government of Canada, Communications Security Establishment, 1996.

[2] DoD, Security Requirements for Automated Information Systems, DoD Directive 5200.28, Department of Defense, March 1988.

[3] DoA, Information Systems Security, Army Regulation 380-19, Department of Army, August 1990.

[4] CSE, Guide to Certification and Accreditation of Information Technology Systems, Government of Canada, Communications Security Establishment, 1996.

[5] C. Wood and K. Snow, "ISO 9000 and Information Security," Computers & Security, Vol. 14, No. 4, pp.287-288, June 1995.

[6] R. Solms and L. Meyer, "Information Security Accreditation - The ISO 9000 Route," Information Security - the Next Decade, Proceedings of the IFIP TC 11 eleventh international conference on information security, IFIP/Sec '95, Edited by J. Eloff and S. Solms, Chapman & Hall, pp.51-59, 1995.

[7] AAWG, AAWG TASK 1 REPORT - An Alternative Assurance Package(AAP) to the CC's EAL3 assurance level (draft version 0.9), Assurance Approaches Working Group, August 1997.

[8] G. Pijl, G. Swinkels and J. Verrijdt, "ISO 9000 versus CMM: Standardization and certification of IS development," Information and Management, Vol. 32, No. 6, pp.267-274, December 1997.

[9] 이강수 외 6인, 정보보호 시스템 평가방법론 연구, 한국정보보호센터, 1996.

[10] NBS, Guideline for Computer Security Certification and Accreditation, FIPS PUB 102, U.S. Department of Commerce/National Bureau of Standards, September 1983.

[11] NCSC, Introduction to Certification and Accreditation, NCSC-TG-029, National Computer Security Center, January 1994.

[12] G. Hardy, "Commercial Accreditation of Information Security," Computers & Security, Vol. 12, No. 8, pp.716-729, December 1993.

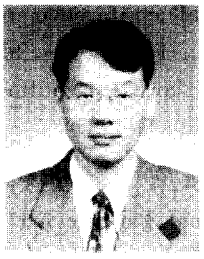
[13] DoD Information Technology Security Certification and Accreditation Process(DITSCAP), DoD Instruction 5200.40, Department of Defense, December 1997.

[14] Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document - Draft, CORB ETT Technologies, Inc., 1998.

[15] J. Lemieux, "The Evaluation of Secure Information Systems," (http://csrc.lse.ac.uk/Academic__Papers/Evaluation__Secure__IS.htm), May 1996.

[16] R. Solms, "Information Security Management: The Second Generation," Computers & Security, Vol. 15, No. 4, pp.281-288, June 1996.

□ 著者紹介



김 종 기

1987년 2월 부산대학교 경영학과 졸업
1988년12월 미국 아칸소 주립대 경영학 석사
1992년 12월 미국 미시시피 주립대 경영학 박사
1993년 3월 ~ 1998년 12월 국방정보체계 연구소 선임연구원
1991년 1월 ~ 현재 국방과학연구소 선임연구원

※ 주관심분야 : 위험분석, 비상계획, 정보시스템 평가 인증