정보시스템의 보안성 평가에 관한 연구

최명길*
*중앙대학교 경영학과
e-mail:mgchoi@cau.ac.kr

A Study on Evaluation of Information Systems

Myeonggil Choi*
*Dept of Business Administration, Chung-Ang

요 약

본 논문은 미국의 정보시스템 보안성 평가, 국제표준화 현황, 안전한 정보시스템 개발을 위한 노력 등을 살펴보고, 우리 나라에서 도입하여 시행중인 보안성 평가 제도를 분석하여 우리 나라에 적합한 국가정보시스템의 보안성 검증 체계 도입 방안을 제안한다.

1. 서론

정보보호는 국가기관의 정보시스템 주요 구성요소 중의 하나이며, 보안성의 확보를 위한 연구개발 노력과 더불어 제도, 절차의 개선에 상당한 관심이 기울여지고 있다. 정보시스템의 보안성을 보장하기 위한 보안대책은 정보보호 시스템, 데이터 통신 암호장비 등의 하드웨어와 더불어 응용 프로그램에 구현되는 보안기능 등 기술적인 측면과 인원보안, 시설보안, 제도, 절차 등 관리적인 측면으로 구분할 수 있다.

응용 시스템(application systems)의 규모가 거대해짐에 따라 자체 개발보다는 대부분 외부 위탁의 형태로 추진된다. 따라서 지금까지 국가가 직접 개발하던 관행에서 업체가 개발한 제품이나 시스템을 국가에서 구매하는 실정이며, 앞으로도 이러한 추세는 더욱 가속해질 것이라 전망된다.

응용 시스템 개발은 시스템 통합의 성격을 극명하게 표출하는 분야이며, 정보보호의 경우도 필요한 보안기능이 보안장비와 응용 프로그램, 그리고 관리적인 보안대책으로 분산되어 구현된다. 특히 동일한 구성요소로 이루어진 응용시스템이라 할지라도 운영환경과 임무에 따라서 요구되는 보안기능이 달라질 수 있으므로 응용시스템의 보안대책의 선택과 구현은 주의 깊게 이루어져야 한다. 따라서 본 연구는 응용체계의 보안성을 보장하기 위한 제반 대책의 효과성을 확보할 수 있는 방안으로서 구현된 보안대책의 평가·인증에 대해서 살펴보고자 한다

2. NIST 시스템 평가

NIST(National Institute of Standards and Technology) SP(Special Publication) 800-30은 정보시스템의 위험관리(Risk Management Guide for Information Technology Systems)를 서술하고 있다. 위험 평가는 위협과 취약성을 확인하고 계획된 보안대책수단을 분석하고 특정한 취약성이 발생할 가능성을 결정하는 데 유용하다. 초기 위험 평가 결과는 보안성 평가에 사용되고, 보안성 평가 결과물에 기초하여 재작성한다. 인가과정(accreditation process) 중 IT 시스템의 기술적, 비기술적 보안대책 수단의 설계와 구현이 보안 요구사항을 어느 정도 충족하는지를 결정하는 포괄적인 평가를 "인증(cerification)"이라 한다. 인증(cerification)은 허용할 만한 위험수준에서 IT 시스템의 운영을 공식적으로 승인하는 담당자게 필요한 정보를 제공한다. 시스템

을 인가함으로써 담당자는 IT 시스템과 관련된 위험을 수용하게 된다. 인가과정(accreditation process)을 공식화하는 이유는 IT 시스템 운영시 필요한 추가적인 검토 필요 가능성을 감소시킬 수 있기 때문이다.

검증된 제품을 사용하면 기존 평가 결과를 이용함으로써 C&A 비용을 감소시킬 수 있다. 컴포넌트 제품이 내포되거나 복수의 IT 시스템에 내포되면 평가된 제품 목록을 이용할 수 있음으로 시스템을 만들 때 이점이 있다.

응용시스템은 하드웨어, 소프트웨어, 통신 장치 등으로 구성된다. 구성요소는 단일 응용 소프트웨어 또는 하드웨어와 소프트웨어를 통합한 제품일 수도 있다. 응용 시스템은 목적과 관련된 기능을 제공하는데 초점을 두고 있다. 또한, 응용시스템은 여러 개의 개별 응용시스템으로 구성될 수도 있다[5].

일반지원시스템은 공통의 기능을 수행하는 동일한 통제 내에서 서로 연관된 정보자원이나 컴퓨터 환경의 집합체이다. 일반 지원 시스템은 보통 하드웨어, 소프트웨어, 정보, 데이터, 응용, 통신, 설비 사람 등을 포함하고 다양한 사용자와 공동의 응용시스템을 제공한다.

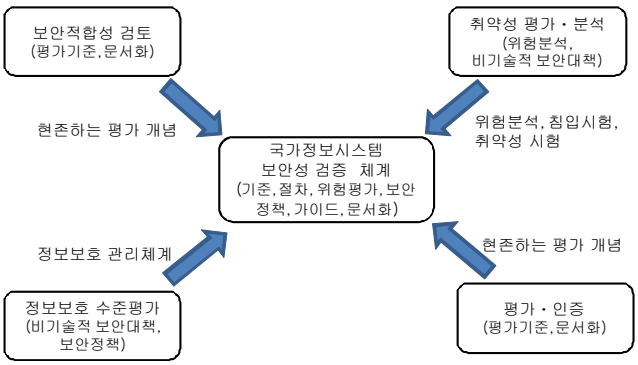
3. ISO/IEC 19791의 정보시스템 보안성 평가

ISO/IEC TR 19791의 정보시스템 보안성 평가는 기존의 ISO/IEC 15408 (국제공통기준)의 철학 및 개념을 정보시스템에 확장한 형태이다. 동 표준은 정보시스템을 운영시스템(operational system)으로 정의하고 있으며, 운영시스템은 기술기반의 기능, 메커니즘과 결합된 사용자, 절차, 프로세스 등으로 정의하고 있으며, 운영시스템은 정의된 운영 환경에서 잔존위험수준(level of residual risk)으로 형성하는데 적용된다. 본 논문은 운영시스템을 정보시스템과 동일한 것으로 간주한다

정보시스템은 속성과 복잡하고, 상용제품과 자체 개발 제품의 결합으로 구성되어 있다. 정보시스템은 하위 시스템들간 상호 작용과 의존성이 있다. 정보시스템은 다양한 공급자가 제공한 컴포넌트로 구성되어 있다. 정보시스템은 다음과 같은 속성을 가지고 있다. 첫째, 정보시스템은 전형적으로 특정한 필요와 운영을 위해서 개발된다. 둘째, 정보시스템은 기술적인 요구사항이나 환경적인 요구사항으로 인해서 자주 변경된다. 정보시스템은 상당한 숫자의 컴포넌트를 포함하고 있으며, 컴포넌트는 다양한 형상을 가진 외부에서 구매된다. 셋째, 정보시스템 소유자는 기술적, 비기술적인 보안 대책을 균형적으로 사용할 수 있다. 넷째, 정보시스템은 다양한 보증 수준을 가진 컴포넌트를 포함한다.

4. ISO/IEC 19791의 정보시스템 보안성 평가

국가 정보시스템의 보안성 검증은 우리 나라에서 운영 중인 보안성 평가 제도를 통괄한 제도로 볼 수 있다. (표 2)에서 살펴보듯이 국가 정보시스템의 보안성 평가를 위해서는 각종 보안 평가 제도를 총괄해야 할 것으로 판단된다. 따라서 국가 정보시스템의 보안성 검증을 위해서는 기존의 제도와 표준간의 관계를 명확하게 설정해야 하며, 기존의 평가 결과를 활용할 수 있는 형태로 발전되어야 한다. 따라서 본 논문은 (그림 1)과 같은 국가 정보시스템의 보안성 검증 체계를 제안한다.



(그림 1) 기존의 평가제도와 정보시스템 보안성 검증 체계

우리 나라는 현재 다양한 분야의 보안 평가제도가 활발히 시행중에 있다. 보안 평가제도의 근간을 이루는 평가 기준과 기술에는 중복성이 존재하고 있지만, 평가 대상과 평가 대상의 시점이 다르다. 따라서 기존의 평가 기술과 평가 기준을 (그림 1)과 같이 활용하면 비교적 빠른 시간내에 정보시스템 검증 체계를 확립할 수 있다.

국가정보시스템 보안성 검증을 위해서 확립되어야 할 기술은 평가기준, 평가절차, 위험평가기술, 보안정책, 평가가이드, 문서화 방법론 등이 있다. 평가기준, 문서화, 평가 가이드는 현존하는 평가 제도 중 보안적합성 검토 제도와 평가・인증제도가 이미 가지고 있는 평가기준, 문서화 방법론, 평가가이드 등을 활용할 수 있다. 비기술적 보안대책의 보안평가에 필요한 평가 기준, 평가 방법론은 정보보호수준평가 및 취약성 분석・평가에서 사용되고 있는 평가

기준, 위험분석, 침입시험, 취약성 시험 등의 방법론을 활용할 수 있다. 다만, 기존의 제도에서 사용하고 있는 평가기준, 제절차, 평가방법론 등은 정보시스템 보안성 검증에 적합한 형태로 변경이 되어야 하며, 각 제도에서 사용되는 기준, 방법론 등이 수정될 필요가 있다.

시스템 보안 검증은 보안 대책이 모든 요구사항을 만족하는 모든 개발수명주기에서 평가를 요구한다. 그러나 우리 나라가 시행 중인 평가 제도는 모든 보안 대책이 수립된 이후에 평가를 시행한다. 개발 환경에서 성공적으로 시험된 기술적인 보안대책은 운영환경에서 작동할 것이다. 그러나 비기술적인 보안대책의 경우는 시험 환경과 운영환경에서 적용될 때는 안정적인 적용을 보장할 수 없다. 정보시스템의 시험 기간에 비해서 정상적으로 정보시스템이 운영시기에서 정보시스템 관련 인력은 경험이 부족하고, 기술력이 부족한 것이 사실이다. 따라서 비기술적 보안대책에 있어서 개발 단계에서 보증된 보증 수준은 기술적 보안대책 보다 운영 환경으로 덜 이전된다. 따라서 초반의 평가는 운영 환경에서 재평가되어야 한다.

현재 국가기관은 보안성 검토를 필한 정보보호제품을 국가기관환경에서 사용할 수 있다. 기존의 평가제품이 정보시스템의 컴포넌트를 이루고 있을 경우에 사용정책을 살펴보자. 정보보호제품의 보안성을 검토할 경우, 정보보호제품이 정보시스템 보안성 검증에 재사용될 수 있는 평가 근거가 있다. 정보시스템 보안성 검증 주체는 보안성 검증의 평가 근거를 획득해야 한다. 문제는 정보제품의 보안성 검토를 획득한 제품을 사용할 수 없는 경우도 발생할 수 있다. 즉, 제품의 평가 기간 동안의 형상과 제품이 정보시스템에 통합될 때의 형상이 변경되는 경우, 보안성 검토를 통과한 제품의 보증 수준과 정보시스템에 통합될 때 필요한 보증 수준이 변경되는 경우 등이다. 다만, 우리 나라의 경우에 있어서 정보보호제품의 보안성 검토는 보증수준을 고려하지 않는다. 그러나 향후 정보시스템의 보안성 검증은 특정한 사용 환경을 고려하기 때문에 보안성 검토와 달리 보증 수준을 고려할 수 있는 경우가 있다. 정보시스템의 보증 수준이 보안성 검토가 요구하는 보증수준보다 높다면, 기존의 평가 제품을 어떠한 수정도 없이 사용하기는 어려울 것으로 예측된다.

4. 결 론

국가기관의 민감한 데이터를 취급하는 정보시스템이 지속적으로 증가할 것으로 전망된다. 정보시스템을 안전성을 담보하기 위해서 국가기관은 많은 자원을 사용하고 있는 실정이며, 많은 성과를 거두고 있다. 그러나 정보시스템 개발 전 과정의 보안성을 검증하는 체계는 여전히 미비한 실정이다. 다행히 현존하는 다양한 정보보안 평가제도가 성숙되게 운영되고 있어, 향후 정보시스템 보안성 검증에 필요한 다양한 기준, 절차, 평가 방법론을 쉽게 활용할 수 있을 것으로 전망된다.

참고문헌

[1] ISO/IEC 15408-1, Information Technology, Security Techniques, Evaluation Criteria fro IT Security, 1999.

[2] ISO/IEC JTC 1/SC27, Text for ISO/IEC 1st WD 19791, Information Technology, Security Techniques, Security Assessment of Operational Systems, May, 2008.

[3] NISP, Special Publication 800-36, Guide to Selecting Information Technology Security Products, Octorber, 2003.

[4] NISP, Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, to Selecting Information Technology Security Products, May, 2004.

[5] NIST, Special Publication 800-18, Guide for Developing Security Plan for Information Technology Systems, December 1985

[6] NIST, Special Publication 800-64 Revision 2, Security Considerations in the System Development Lifecycle, 2008.