# 공공기관 정보시스템의 자가진단 보안 분석·평가 연구

김인중*, 정윤정*, 이철원*, 장병화*, 원동호**
국가보안기술연구소*, 성균관대학교**

# Security Self-Analysis and Self-Evaluation for Public Information System

Injung Kim*, Yoonjung Jung*, Cheolwon Lee*, Byunghwa Chang*, Dongho Won**
National Securiy Research Institute*, SungKyunKwan University**

## 요 약

공공기관은 자신의 정보시스템에 대한 보안 대책을 수립하기 위하여 자체 보안·분석 평가를 수행함으로써 적절한 보안 목표와 방향을 설정해야 한다. 하지만, 현재 연구되어 있는 위험분석 및 보안평가방법론등은 복잡하고 전문적인 사항이 많으므로 자체 보안분석을 수행하기에는 인력 및 비용이 많이 소요된다.

이를 위하여 본 논문에서는 정보시스템의 위험분석방법론에서 제시하는 자산, 취약점, 위협, 대응책에 보안평가방법론을 포함하여 정보시스템에 대한 모델링, 가정, 증상, 원인, 해결책등을 통한 자가진단 보안 분석·평가 방법을 제시한다.

## 1. 서론

공공기관에서 정보통신망을 설치·운영 및 신·증설할 때 자체 보안 대책을 강구하여야 하며 이에 대한 보안성 검토를 받아야 한다[1]. 일반적으로 보안성 검토 절차는 기관내 자체 보안성 검토를 위한 사업계획서가 보안심의위원회의 자체 보안성 심의를 통과하고, 보안 부서 결재를 득한 후 이루어진다. 시스템 규모가 큰 경우에는 보안 관련 기관과 협의한 후 보안 측정을 수행하여 올바른 보안 대책이 이루어 졌는지를 확인한다. 이를 위하여 해당 공공 기관은 일반적인 업무처리 절차, 사용 시스템 구성도 그리고 보안 관리체계 등을 정리하고 보안 취약점 파악, 보호 대책 등을 작성한 후 보안성 검토를 요청한다. 이러한 보안성 검토는 정보시스템에 대한 단일제품의 보안 장비 적용 및 패스워트 관리 수준에서 처리됨에 따라 궁극적인 보안 대책이 되지 못하고 있다.

최근에 이러한 문제점을 보완하기 위하여 정보시스템 전반에 대한 보안 분석·평가가 시도되고 있으나 방대하고 복잡한 규모로 운영되고 있어 정확한 보안 분석·평가가 이루어지는 것이 매우 어렵다. 따라서 단일 장비 중심의 평가에 치우치고 있으며, 정보시스템에 대한 평가 기준 및 지침도 제시되어 있지 않은 상태이다.

일반적으로 국외 보안 평가의 현황을 살펴보면 TCSEC(Trusted Computer System Evaluation Criteria), ITSEC(Information Technology Security Evaluation Criteria), CC(Common Criteria) 등이 있으나 장비 위주의 평가이며, 보안관리지침으로 캐나다의 CSE에서 발표한 위험관리방법론, 미국 NIST에서 발표한 FIPS65, ISO/IEC JTC1 SC27의 정보보호관리지침(GMITS)등이 존재하나 이 역시 기술적 측면보다는 관리적 측면에 치중하고 있다. 다만 최근에 IOS/IEC에서는 CC를 기반으로 정보시스템 보안평가방법론 CEM(Common Methodology for Information Technology Security Evaluation)을 고려하고 있다.

한편 국내에서는 정보화촉진기본법에 의거 정보보호장비에 대한 평가·인증 제도를 시행하고 있으며 인증된 정보보호장비를 공공기관 주요 정보통신기반시설에 적용을 권고하고 있으나 이러한 부분적인 보안 대책을 통해서는 외부로부터의 침해 사고를 방지하기가 어려울 뿐만 아니라 종합적인 보안 대책을 세우는 데 있어 오히려 걸림돌이 되고 있는 실정이다.

이를 보완하기 위하여 공공기관은 정보통신기반시설에 대한 각종 위협으로부터 보안 취약점을 진단하기 위하여 정보통신보안측정을 요청하거나 일정 절차에 의하여 취약점 분석·평가를 수행하도록 하고 있다[2]. 대부분 공공 기관은 정보통신기반시설에 대한 취약점 분석·평가를 위하여 외부 기관에 보안 컨설팅을 의뢰하지만 자체적인 전담반을 구성하여 자가진단을 수행하는 경우가 드물다. 일반적으로 공공기관은 외부 기관에 보안 컨설팅을 의뢰하기 전에 자신들이 가지고 있는 정보시스템에 대한 정확한 보안 문제점을 인식하고 어떤 절차로 수행되는 지를 알고 있어야 만이 정확한 보안 대책을 세울 수 있게 된다.

하지만 보안 컨설팅의 대부분 절차와 방법은 보안컨설팅 전문업체의 독자적인 위험분석방법론 또는 보안평가방법론을 사용하고, 다양한 경험을

통한 전문 기술을 적용하므로, 공공 기관의 상호 협력을 통한 적절한 보안 대책 제시가 미흡한 상태이다. 이에 따라 공공기관은 보안 컨설팅의 결과를 통하여 정보시스템에 대한 보안성 검토를 의뢰 시 별도의 작업을 수행하게 되는 경우가 발생한다.

본 논문에서는 공공기관에서 자체 전담반을 편성하여 보안 분석·평가를 수행할 수 있도록 단순한 자가진단 보안분석·평가방법을 제시하고자 한다. 미국의 카네기멜론 대학 SEI(Software Engineering Institute)에서 정보보호 위험평가를 기술하기 위해 개발된 OCTAVE[3]나 NIST에서 제시한 ASSET[4][5]등은 국내 현실에 적용하기 어려운 부분(예를 들어, 상급자에 대한 인터뷰, 많은 설문 등)이 있으므로 국내 현실에 보다 적합하도록 구성하였다. 궁극적으로 기존의 문서 보안 또는 장비 도입과 관련한 보안성 검토가 아닌 정보시스템에 대한 보안 분석·평가 방안이라고 할 수 있다. 다만, 규정이나 지침 등에서 사용중인 보안성 검토라는 용어는 현재 존재하는 공공기관 정보시스템이 보안에 위배되는 지를 파악하고 올바르게 사용되는가 만을 심사하는 것이므로 보안 분석·평가라는 용어가 적절하며 국내 현실에 맞는 자가진단 보안 분석·평가 방법론을 제시한다.

## 2. 자가진단 보안분석·평가 방법론

공공기관은 주요 정보시스템에 대한 보호를 위하여 보안 정책 입안, 실제 정보시스템의 이해와 효과적인 사건 대응 능력 개발을 위한 보안 운영 지침 확립, 주요 자산에 대한 취약성 평가·수행, 각종 진단 도구 및 정보보호시스템 도입 등 과 관련한 보안 사업을 수행하고 있다. 보안 사업을 수행 시 또는 사업종료 후 정보시스템의 운영 시 사업이 얼마나 효율적으로 수행되었는 지를 알아야 한다. 일반사업의 경우에는 사용기록이나 데이터 양을 통하여 분석이 이루어질 수 있지만 보안 사업의 경우에는 정량화 할 수 없다. 따라서, 정보 자산의 보호를 위하여 위험분석의 전 단계로 전담반이 자가진단 보안 평가·분석을 통하여 보안 목적과 보안 정책을 세우는 데 필요한 자료로 활용함으로써 보안 요청에 드는 시간 및 비용을 절감하게 되고 시스템 담당자의 보안 지식을 향상시키게 된다. 즉, 자가진단을 통해 자신이 관리하는 정보시스템에 대하여 어떠한 문제점을 갖고 있고 해결해야 하는 문제점이 무엇인 지를 분명히 할 수 있다.

일반적으로 정보시스템 관리자는 보안 운영 방침이 제대로 되어 있지 않은 상황에서 보안 감사 또는 보안 측정이 실시됨에 따라 상호간에 많은 보안 의식 및 보안 수준 차이가 발생한다. 또한 보안 요구에 대한 보안 컨설팅 수행을 하는 과정에서 담당자가 보안 문제점을 점차 인식하게 되고 이에 대한 보안 사항에 대한 추가 요구를 제시하는 경우 사업 추진에 많은 어려움이 따르게 된다. 또한, 보안 수준에 따라 많은 비용과 인력이 소요되는 데 공공 기관에서는 단순히 보안 컨설팅을 통해 모든 보안 대책이 완성되고, 시스템의 진화 및 관리과 상관없이 대책이 이루어지는 것으로 알고 있다. 따라서 자가 진단의 보안 분석·평가를 사전에 적용함으로써 시스템 담당자가 의도하는 범위를 정확하게 파악해야 한다.

이를 위하여 현재 사용중인 위험 분석 기법을 도입하는 경우 자산 식별 및 선정, 위협, 취약성, 대응책과 관련된 항목들은 기존에 공공기관이 보안성 분석·평가를 통해 수행하고 있는 절차와 상이하기 때문에 적절한 결과를 도출하기가 어렵다. 따라서, 현재 규칙이나 법령에 있는 사항 및 기본 개념을 토대로 보완 적용하는 것이 바람직하다고 본다. 기존에 일반적으로 제출되는 보안성 검토 자료는 다음과 같다.

. 사업 목적 및 추진 계획
. 정보시스템 구성도
. 관리적 보안 대책
. 물리적 보안 대책
. 보안시스템의 운용 방안
. 주전산기, 단말기, 네트워크 등 정보시스템의 요소별 기술적 보안대책
. 기타 보안 사항

현재 보안관련 규칙을 보게 되면 정보시스템의 신·증설, 외부망과 연결하고자하는 경우, 그리고 보안장비를 도입하는 과정에서 보안성 검토가 하게 되어 있다. 하지만 기술적인 보안 분석 ·평가보다는 시스템을 도입하고 구축된 후에 이루어지는 것이 대부분의 현실이다. 따라서 보안 분석·평가가 이루어지는 시기는 시스템 도입시기와의 시간적 차이로 인하여 적절한 보호대책이 이루어질 수 없다. 따라서, 가장 좋은 방법은 정보시스템의 도입 전에 이루어지는 것이다.

한편으로 정보시스템이 도입되거나 증설하는 경우에도 시스템담당자는 보안성 평가를 평가위원회에 의뢰하지만 실제 보안성 평가에 대한 정확한 산출근거를 제시할 수 없다. 이는 객관적인 내용이 있는 것도 아니고 이에 대한 정확한 파악이 어려운 상태에서 제출된 보고서만을 가지고 처리하게 되므로 보안 침해 요소가 어느 부분에 있는 지 알 수 없다. 그리고 보안 침해 요소도 기본적으로 패스워드 또는 사용자 인증에 한하며 물리적 보안과 관리적 보안 대책에 치중하게 된다. 좀 더 중요하다고 보는 데이터에 대해서는 암호화를 고려하는 수준이다. 최근에 일부에서는 보안 진단 도구를 돌려서 취약점이 있는 지를 분석하기도 한다.

이러한 일련의 작업을 자가진단을 통하여 보안성 평가 및 평가를 수행함으로써 대상 기관이나 평가 기관에서 보안 측정 및 보안 컨설팅 수행 시 이를 기본으로 작업함으로써 올바른 보안 대책을 제시하고 장기적인 마스터플랜을 만들 수 있게 된다.

## 3. 제안한 자가진단 보안 분석·평가 방법

일반적으로 보안 평가는 크게 3가지로 구분할 수 있다. 서류나 문서에 대한 보안성 평가, 장비 도입에 대한 보안성 평가, 시스템에 대한 보안성 평가이다. 전 두 단계는 이미 많은 규정 및 지침이 나와있으므로 본 논문에서는 정보시스템에 대한 보안성 평가만을 다루기로 한다. 또한 물리적 관점과 관리적 관점은 3개 단계 모두 같은 정책 및 지침을 따르면 가능하므로 기술적 부분만을 다루기로 한다.

### 3.1 보안 분석 시점

먼저, 시스템 구축에 대한 보안성 분석도 시점에 따라 분석 관점이 다른데 시스템 착수시점, 진행시점, 종료시점으로 구분할 수 있다.

o 착수 시점 : 정보시스템의 보안대책이 효과적인가를 분석
o 진행 시점 : 정보시스템의 보안대책이 효율적인가를 분석
o 종료 시점 : 정보시스템이 목적에 맞게 바르게 작동하고 있는가를 분석

### 3.2 자가진단 절차

보안에 많은 관심을 갖는 가장 큰 이유는 책임성이 따르기 때문이다. 시스템에 대한 적용 및 관리상의 문제가 발생하는 경우에는 원인을 분석하고 해결하면 되지만, 보안 문제의 경우에는 이미 문제가 발생한 경우에는 많은 손실을 가지게 되며 이러한 손실은 결국 공공기관의 이미지를 실추된 후이므로 책임을 피하기가 어렵게된다. 따라서 예방이 무엇보다도 중요하고 원인에 대한 해결책을 찾는 것이 우선이라고 할 수 있다. 또한 원인이 밝혀지지 않은 경우에도 해결책을 세움으로써 피해에 대한 예방을 하는 것이다.

자가진단을 위해서는 기존의 위험분석 방법론을 적용하기에는 약간의 혼란이 있을 수 있다. 이는 자산, 위협, 취약성, 대응책을 가지고 이루어지고 있으나 컨설팅을 수행하는 입장에서 이루어지고 있으므로 자가진단을 수행 기관 입장에서는 자신의 정보시스템이 어느 정도 수준이고 어떤 문제점이 있는 지를 아는 것이 더 중요하므로 그림 1과 같은 절차를 수행한다.

가. 자가진단 실시

자가진단 실시를 위하여 준비해야 할 사항으로 수행 대상 조직에 대한 협조와 상위자의 동의 및 승인을 얻는다. 인터뷰와 설문등의 방식보다는 기존 문서나 지침을 통한 기본 자료를 수집한다. 수집된 자료가 미흡하거나, 의심스러운 부분 또는 상충되는 부분에 대해서는 담당자와 면담을 통하여 확인한다. 조직의 특성상 상위 및 차상위자에 대한 인터뷰는 가급적 자제하고 수집된 자료를 확인 검토하는 과정에서 보안 요구사항을 확인한다.

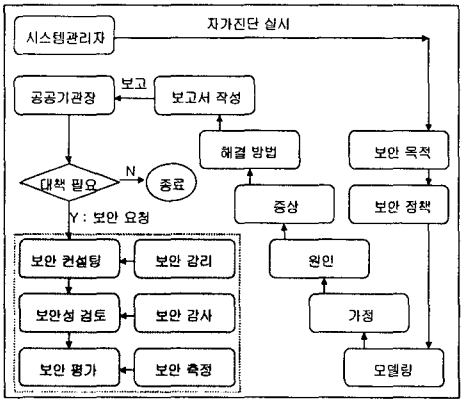


그림 1. 자가진단 보안 분석·평가 절차

나. 보안 목적

보안 평가를 실시하는 목적이 무엇인지를 파악한다. 이는 내부 시스템에 대한 접근 제어나 비인가자에 대한 비밀 유출 방지 등 정보시스템에 대한 보안 목적을 사전에 정의한다.

다. 보안 정책

인가된 사용자에 대한 접근 여부, 데이터의 열람 및 행위에 대한 허용 범위, 사용내역에 대한 기록 수준, 암호화 대상등 정의한다.

라. 모델링

먼저 자신의 시스템에 대하여 모델링을 한다. 복잡한 시스템에 대하여 최소한의 주요 장비를 식별하고 외부와의 연결점을 정의한다. 즉, 최소한의 주요 기반시설을 식별하는 데 핵심 업무 달성에 절대적으로 근본이 되는 임무에 필수적인 프로세스를 지원하기 위한 특정 장비의 구성요소들을 선정한다. 이때 모델링은 3가지 구성 요소는 장비, 연결 점, 연결 로이다. 장비는 서버, 클라이언트, 라우터, 허브, 패스, 보안 시스템, 보안모듈로 구분하며 간단한 기호나 블록으로 표시하는 것이 바람직하다. 그림 2는 시스템 모델링[6]의 한 방법을 실명한다.

필요시 각 도메인에 대한 보안 목적, 보안 정책, 보안 환경, 보안 요구사항, 보안 특성을 정의한다.

마. 가정

정보시스템에 대한 침해 요소가 어떤 것이 있을 것인 지를 열거한다. 해결방법이 제시되지 않은 문제점을 포함할 수 있으며, 각종 취약점 및 위협 요소들을 이용한다.

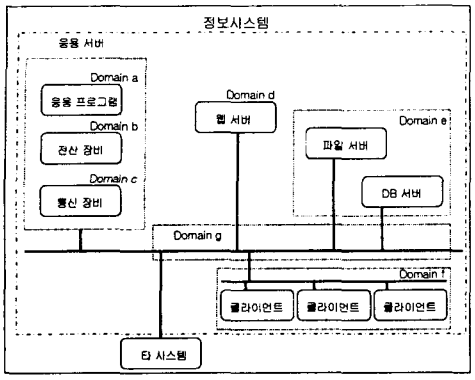


그림 2. 시스템 모델링

바. 원인

정보시스템에 발생한 문제점에 대하여 객체와 주체를 구분한다. 주체는 외부인지 내부인지를 파악하고 객체의 경우에는 운영체제, 시스템, 네트워크 등으로 분류한다.

사. 증상

정보시스템에 대한 피해가 발생하면 어떤 상태가 되는 지를 확인한다. 피해의 정도에 따른 손실을 고려한다.

아. 해결 방법

정보시스템을 원상 회복시키기 위한 대책을 강구한다. 해결방법이 보안 목적에 부합하는 지도 상관관계를 통하여 분석한다. 해결 방법이 없는 경우에는 보안컨설팅 과정에서 방법을 얻기 위하여 해당 사항을 기록한다.

자. 보고서 작성 및 보고

보고서의 내용은 자가진단의 결과를 제시하고 자체적으로 해결하지 못하는 부분에 대한 정밀한 보안 진단 계획을 제시한다.

차. 보안 요청

도출된 결과로부터 현재 정보시스템에 대한 보안 대책 수준을 점검할 수 있다. 하지만 도출된 내용을 분석해본 결과 보안 수준이 미약하거나 보안 강화가 요구되는 경우 자가진단 결과를 토대로 외부 전문기관에 보안컨설팅 또는 보안 분석·평가를 요청한다.

카. 보안 컨설팅, 보안 감리

정보시스템에 대한 전자적 침해행위에 대한 보호대책을 수립하기 위하여 위험분석 및 취약성분석·평가를 수행한다. 이때 외부 전문기관에 의뢰하는 경우 적절한 보안 대책을 수립하였는 지를 확인하기 위하여 보안 감리를 수행할 수 있다.

타. 보안성 검토, 보안 감사

정보시스템에 대한 올바른 보안 대책을 통하여 시행되고 있는 지에 대한 합법성, 정당성, 적적정성 등을 조사하고 신뢰성, 안전성, 효율성을 검증한다.

파. 보안 평가, 보안 측정

정보시스템에 대한 보안기능이 보안 요구사항을 어느 정도 만족시키는지 기밀성, 무결성, 가용성 등의 방법으로 종합적 분석하고, 평가 결과를 검토하여 보안기능의 적절성 여부를 판단한다.

## 4. 결론

최근에 많은 보안 제품들이 보안 평가를 받고, 보안성 평가를 받은 제품들을 공공기관 정보시스템에 적용하고 있다. 하지만 공공기관의 정보시스템이 이미 구축되어 있는 상태에서 평가를 마친 제품들이 적용된다고 해서 정보시스템에 대한 보안성이 제공되는 것은 아니다. 예를 들면, 침입탐지시스템 제품에 대한 보안성 평가를 받아 정보시스템 내에 적용하였다고 해도 침입탐지시스템의 룰 설정 및 위치가 적절한지는 알 수 없는 것이다. 이를 위하여, 공공기관 정보시스템에 대한 침해사고 및 위협을 분석하기 위한 취약점 분석·평가를 수행하게 된다. 이러한 취약점 분석·평가는 독립적인 전담반을 조직하거나 외부 전문업체에 의뢰하는 경우가 대부분이지만 수행 시부터 자산 평가 및 조직 운영방안과 같은 현황분석에서부터 각종 위협, 취약성을 분석하고 이에 대한 보안진단을 수행함에 따라 많은 시일이 걸리고 상호간에 이해 부족이 많이 발생하게 된다. 따라서, 보안 분석·평가를 수행하기 전에 자가진단 보안 분석·평가 방법론을 통하여 보안 사항에 대한 정보를 사전에 확보하는 것이 바람직하다.

### 참고 문헌

[1] 보안업무규정, 보안업무시행규칙, 보안업무시행세칙 등

[2] 정보통신기반보호법

[3] CMU/SEI, Operationally Critical Threat, Asset, Vulnerability Evaluation(OCTAVE) Framework, v1.0, CMU/SEI-99-TR-017, June 1999.

[4] NIST, Security Self-Evaluation Guide for Information Technology Systems, Nov 2001.

[5] Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26, Nov, 2001.

[6] Haruki Tabuchi, System Evaluation, Principles, concepts, Terms, ISO/IEC JTC1/SC27 conference, Oct 9, 2002.