개발 환경 보안수준 점검도구 연구*

고 일 석**

요 약

IT 제품 개발환경에 대한 보안수준을 점검하기 위해서는 IT 제품 개발환경에 존재하는 취약성과 각종 위협 요인을 분석하고 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준과 평가 도구가 필요하다. 또한 이를 위해 관련분야에 대한 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준과 이를 실제 IT 제품 개발환경에 적용할 수 있는 평가방법론이 연구되어야 한다. 본 연구는 IT 제품 개발 환경의 보안수준을 점검하기 위한 확인 도구를 개발하는 것을 목표로 하고 있다.

A Study on the Verification Tool for the Security Level in Development Environment*

Il Seok Ko**

ABSTRACT

For the verification of the security level against a IT product development environment, we should analyze the vulnerability and the various threatening factors which exists in the IT product development environment. Also we need the evaluation criteria and tools for the evaluation and improvement of the level of information security. For that, we need evaluation indices and the standard it will be able to improve the evaluation methodology in the actual IT product development environment which will reach it will be able to apply must be researched. In this study, our aims are the development of verification tools for the security level of IT product development environment.

Key word : Security Level, Evaluation Criteria, IT Product Development Environment

---

* This work was supported by a grant from Security Engineering Research Center of Ministry of Industry and Energy.

** 동국대학 컴퓨터학과

1. 서 론

정보화 사회에서는 모든 사회 활동과 인간 생활에 정보자체가 주요한 원천이 되고 있으며 정보의 수집, 분석 및 활용 능력이 한 나라의 국익이나 경쟁력을 좌우하는 중요한 자산이 되고 있다.

이러한 정보의 중요성에도 불구하고 정보를 취급하는 과정에서 오는 취약성으로 인하여 정보에 대한 무단 유출 및 파괴, 변조 등과 같은 공격이 자행되고 있으며, 또한 인가받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통 등과 같은 피해도 증가하고 있어 정보보호는 중요한 현안으로 인식되고 있다[1, 2].

개발환경 및 조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 개발 환경 또는 조직의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준이 필요하고 우리나라에서 적용 가능한 정보보호 시스템들의 평가방법론이 연구되어야 한다[1-4].

보안성을 실현하기 위해 정보 통신 하부 구조를 활용한 정보기술의 경우, 표준화, 개방화는 필수적인 사항이다. 이에 따라, 정보 통신 시스템은 1950년대부터 평가 및 인증 제도가 시작되었고, 소프트웨어 시스템의 경우에도 ISO 9001과 같은 소프트웨어 품질표준이 제시되고 이를 평가하는 기관들이 설립되고 있다. 그러나 정보보호 시스템의 경우 ITSEC, TCSEC, CC 등과 같은 평가 기준이 있으나 이는 정보보호 제품의 보안기능에 대한 기술적 평가를 위해 개발되어 졌으며, 그에 따른 한계를 가지고 있다[1, 4, 5].

기존연구의 내용에서 정보보호 평가는 크게 두 가지 접근방법에 의해 구분될 수 있었다. 기존의 정보시스템의 보안성 평가는 제품이나 시스템의 보안 기능과 성능에 대한 평가를 중심으로 발전해 왔다. 여기서 TCSEC, ITSEC, CC 등이 대표적 평가기준 이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다[6, 7, 9].

이에 IT 제품 개발환경에서의 보안은 개별 보안 제품의 조합으로만 달성될 수 없으며, 개발환경에서의 보안 기능을 제공하는 제품/시스템과 관리적인 보안대책이 적절히 융합되어 보안관리체계가 원활히 운영되고 있을 때 한 IT 제품 개발환경세어의 정보보안이 효과적으로 유지될 수 있다는 것을 인식해야 한다. 특히 IT 제품의 개발환경에 대한 안전성의 검토는 IT 제품 개발의 신뢰성과 안전성 확보 측면에서 그 필요성이 증대하고 있다.

IT 제품 개발환경에 대한 보안수준을 점검하기 위해서는 IT 제품 개발환경에 존재하는 취약성과 각종 위협 요인을 분석하고 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준과 평가 도구가 필요하다. 또한 이를 위해 관련분야에 대한 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준과 이를 실제 IT 제품 개발환경에 적용할 수 있는 평가방법론이 연구되어야 한다.

본 연구는 IT 제품 개발 환경의 보안수준을 점검하기 위한 확인 도구를 개발하는 것을 목표로 하고 있다.

2. 정보보호수준 평가방법론 관련 연구

정보화의 빠른 진행은 정보시스템의 안전·신뢰성 확보 등 정보보호의 중요성이 부각시켰고 이와 관련된 정보보호제품에 대한 수요도 점차적으로 증가하고 있다[1, 4, 9, 10].

정보보호산업의 성장구도는 보안인프라(infrastructure security), 위협관리(threat management), 취약성관리(vulnerability management), 그리고 정보위험관리(information risk management)의 단계

를 거쳐 발전하고 있다.

- 보안인프라 : 접근제어 기능을 갖춘 방화벽, 사용자의 신분을 확인하는 인증, 통신상의 데이터 보호를 위한 VPN 제품, 바이러스 치료를 목적으로 하는 백신 프로그램 등이 초기 정보보안 시장 육성에서 중요한 역할을 수행했다.
- 위협관리 : 보안 인프라가 구축된 후 정보보호 산업은 시스템의 내/외부 침입을 확인하기 위한 침입탐지, 실시간 경보, 데이터 및 시스템의 복구를 위한 재난복구 기능을 탑재한 제품군이 주도하였다.
- 취약성관리 : 취약성 분석 단계에서는 위협분석은 물론, 위협요인에 대한 대안분석, 정책 수립 등의 다소 상위 관점의 작업이 진행되었으며 이때부터 보안시장이 급격하게 증가하였다.
- 정보위험관리 : 정보위험 관리 단계는 정보보호 산업의 다음 발전 모델이라 할 수 있으며 단순한 제품군, 혹은 그 결합이 아니라 하나의 산업으로서의 형태를 모두 갖추게 되는 단계라 할 수 있다. 이 단계에서는 보안 컨설팅, 보안 정보전략 수립, 보안 정책 수립, 보안 강화를 위한 업무 프로세스 개선 등의 작업이 이루어지게 된다.

또한 정보보호 평가 측면에서 기존 연구의 내용들은 크게 두 가지 접근방법에 의해 구분된다[7-9]. 첫 번째는 TCSEC, ITSEC, CC 등과 같이 제품이나 시스템의 보안 기능과 성능 측면을 중심으로 하는 평가 체계이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다. 두 번째는 BS7799과 같이 관리적 측면을 중심으로 한 평가 체계이다[11-17].

2.1 BS7799

BS7799는 BT, HSBC, Marks and Spencer, Shell International, Unilever등 주요 업체와 더불어 영국의 상무성 주관으로 '정보보안관리 실무 규범(A Code of Practice for Information security management)'이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다.

BS7799는 1995년에 처음 제정되어 1999년에 개정되었으며, 영국 이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이, 핀란드, 인도 등에서 사용되고 있고, 1999년 10월에 ISO 표준으로 제안되어 ISO/IEC 17799-1이 되었다. 영국 정부에서는 전자정부를 향한 노력을 뒷받침하기 위하여 2001년 3월까지 대부분의 정보시스템에 대하여 BS7799 인증을 받도록 하여 국가 핵심 정보 기반구조를 보호하기 위한 수단으로 활용하고 있다.

BS7799는 기업이 고객정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 둔다. 또한 개발 배경은 기업들이 직면하고 있는 대부분의 상황에 필요한 통제를 식별하기 위한 단일한 참조점을 제공하고, 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 문서를 참조함으로써 기업들간의 네트워킹에 있어서 상호 신뢰가 가능하도록 한다. 물론 이 표준에서 제시하고 있는 통제들 모두가 모든 상황에 적용될 수 있는 것은 아니며, 개별적인 환경적 또는 기술적 제약조건을 고려하여 선택하여야 할 것이다. 따라서 BS7799 표준은 지침과 권고안의 성격을 갖는다.

BS7799의 구성요소를 살펴보면 다음과 같다.

(1) Part 1(Code of Practice for Information security management)

정보보호관리에 대한 실행지침으로 총 10개의 주요세션으로 구성되어 있으며, 127가지의 보안 지침을 제공함으로써, 정보보호관리에 대한 포괄적인 세트를 제공하고 있고, 참조문서로 사용할 수 있다. ISO/IEC 17799의 목적은 관련 회사가 공식

적으로 고객 정보에 대한 비밀성, 무결성, 가용성을 보장할 수 있도록 하는데 있다.

ISO/IEC 17799 : 2000은 실질적인 업무 또는 책임을 맡고 있는 사람들이 특별한 지역에 적합한 실질적인 세이프가드를 식별할 수 있도록 10개의 주요 섹션하에 127가지의 보안 통제항목을 정의하고 있다. 또한 이 규격은 위험관리(Risk Management)의 중요성을 강조하고 있으며 관련된 지침만 실행하면 되는 것으로 하고 있다.

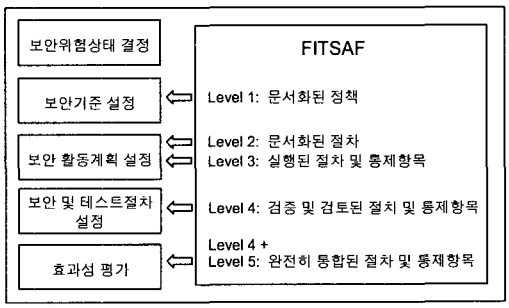
(2) Part 2 (Specification for Information Security Management)

정보보호관리체계(ISPM)에 대한 규격으로 정보보호관리체계 문서화 수립, 실행에 대한 요구사항과 개별조직의 필요성에 따라 실행될 수 있는 정보보호관리 요건을 규정하고 있다. 여기에서는 '조직은 문서화된 ISMS를 구축하고 유지해야 한다.'고 명시하고 있으며, 이는 보호대상의 자산과 위험관리에 대한 조직의 접근과 통제목표 및 방안, 그리고 요구되는 보장수준을 언급해야 한다는 것을 의미한다.

BS7799-2 : 1999는 어떻게 ISO/IEC 17799를 적용하고 ISPS를 구축하는지 알려주고 있다. 또한 6단계 프로세스를 정의하고 있다. 정보보호관리체계 프레임워크를 수립하는 단계로 1단계는 정보보호정책을 정의하고, 2단계는 정보보호관리체계의 범위를 정의, 3단계는 적절한 위험평가를 실시, 4단계는 관리해야 하는 위험영역을 조직의 정보보호 정책과 요구되는 보장수준을 토대로 식별, 5단계는 적절한 통제목표 및 방안의 선정과 그 선정을 정당화하고, 6단계에서 적용성 보고서를 설정한 통제목표 및 방안과 그것의 설정 사유는 적용성 보고서로 문서화하는 단계를 정의하고 있다.

2.2 FITSAF(연방 정보기술 보안평가 프레임워크)

미 정보화 책임관(Chief Information Officers ; CIO) 협의회내의 보안소위원회에 의해 개발된 연방 정보기술 보안평가 프레임워크(Federal Information Technology Security Assessment Framework ; FITSAF)는 각 기관의 담당자들이 기존의 정책과 관련하여 그들의 보안 프로그램의 현재 상태를 결정하고, 필요한 경우 향상 목표를 수립하기 위한 방법을 제공한다. 하지만 프레임워크가 새로운 보안 요구사항을 수립하지는 않는다.



(그림 1) FITSAF의 단계별 접근

프레임워크는 각 기관이 그들의 보안 프로그램에 대한 평가와 향상을 위한 노력의 우선순위를 결정하는데 도움을 주도록 다섯 수준으로 구성되어 있다. 다섯 수준은 구체적인 관리적, 운영적 및 기술적 통제 목적들을 측정한다. 각 수준에는 각 수준이 적절하게 구현되었는지를 확인하기 위한 기준들이 포함된다. 특정한 자산의 보안 상태에 대한 일관되고 효과적인 측정 도구로써 NIST에서 마련한 자체 평가 설문지를 활용할 수 있다. 프레임워크의 수준 1은 자산에 문서화된 보안 정책을 반영하고 있음을 반영한다. 수준 2에서는 정책을 구현하기 위한 문서화된 절차와 통제가 존재한다. 수준 3은 절차와 통제가 구현되었음을 나타낸다. 수준 4는 절차와 통제가 시험되고 검토되었음을 표시한다. 수준 5에서는 절차와 통제가 종합적인 프로그램에 완전히 통합된 상태를 나타낸다. 각 수준은 보다 완전하고 효과적인 보안 프로그램을 나타낸다. 각급 기관의 보안 필요성은 아주 다양하리

라는 전제하에서 자산과 그 자산이 의존하고 있는 상호 연결된 시스템의 효과성을 시험하는 것이 위험을 적절하게 완화하고 있는지의 여부를 이해하는데 핵심적이다. 개별 시스템이 수준 4를 달성하지 못했을 때 각급 기관은 시스템이 OMB 메모 M00-07 (2000년 2월 28일) "정보시스템 투자에 보안을 통합하고 재원을 마련한다."라는 기준을 충족하는지를 결정하여야 한다. 각급 기관은 모든 자산들을 수준 4 그리고 궁극적으로는 수준 5로 끌어올리는 방안을 강구하여야 한다.

3. 정보보호수준 평가체계

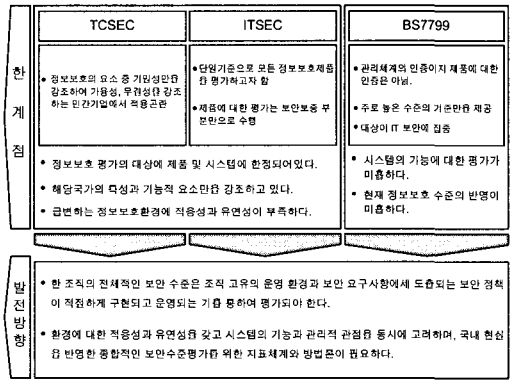
3.1 정보보호 평가 : 기존 연구의 한계점 개선 방안

기존연구의 내용에서 정보보호 평가는 크게 두 가지 접근방법에 의해 구분될 수 있었다. 기존의 정보시스템의 보안성 평가는 제품이나 시스템의 보안 기능과 성능에 대한 평가를 중심으로 발전해 왔다. 여기서 TCSEC, ITSEC, CC 등이 대표적 평가기준 이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다.

이에 IT 제품 개발환경에서의 보안은 개별 보안 제품의 조합으로만 달성될 수 없으며, 개발환경에서의 보안 기능을 제공하는 제품/시스템과 관리적인 보안대책이 적절히 융합되어 보안관리체계가 원활히 운영되고 있을 때 한 IT 제품 개발환경에서의 정보보안이 효과적으로 유지될 수 있다는 것을 인식해야 한다.

또한 IT 제품 개발환경의 전체적인 보안 수준은 전체 조직 고유의 운영 환경과 보안 요구사항에서 도출되는 보안 정책과 이를 통한 제품 개발 환경에서의 각종 정책과 관리가 적절하게 구현되고 운영되는지를 통하여 평가하여야 한다.

TCSEC의 특징을 살펴보면, 세계최초의 평가기준으로 여러 가지 자료가 많이 존재하고 여러 사례에 적용시킬 수 있는 해설서가 존재한다. 또한 시행착오를 거치면서 관련된 경험이 축적되어 있다. 그러나 기능성과 보증성의 구분이 없이 고정되어진 기준만을 사용하고 보안의 요소 중 기밀성만을 위주로 개정되어 가용성과 무결성을 중시하는 민간기업에 적용하기 어려운 한계점을 가지고 있다. 또한 이를 IT 작업 환경의 보안성 평가에 적용하기에는 충분한 연구와 수정이 있어야만 한다.

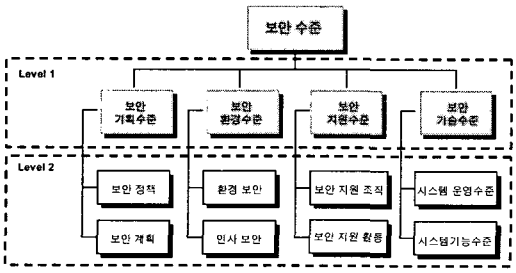


(그림 2) 기존 보안 평가도구 분석(정보보호수준 평가 항목 및 방법론 개발, 임춘성, 고일석, 2003년 KISA연구보고서)

또한 ITSEC은 세계최초의 국제 통합기준으로써 기능성과 보증성을 분리하고 있으며 기준을 일반적으로 정의하여 유동성을 유지하며 TCSEC의 내용을 대체로 포함하고 있다. 그러나 기준이 일반적으로 기술되어서 이해하기가 어렵고 보안수준에 의해서 세분화되어 있지 않아 평가 시 주관적인 견해가 포함될 수 있다는 한계점을 가지고 있다. 또한 이를 IT 작업 환경의 보안성 평가에 적용하기에는 충분한 연구와 수정이 있어야만 한다. 기존 보안 평가 도구들에 대한 분석 결과는 (그림 2)와 같다.

3.2 측정관점

측정관점이라 함은 현재의 상태를 있는 그대로 정적인 관점에서 바라보는 것으로, 현재의 있는 그대로의 상태를 측정이 가능한 상태로 구조화해서 보는 관점이다. 이러한 관점으로 IT 개발 환경에서의 정보보호는 다음 그림에서 보는 바와 같은 주제영역(Subject Area)으로 분할하여 볼 수 있다. 주제영역은 정보보호 수준평가를 위한 지표체계로 구성되어진다.

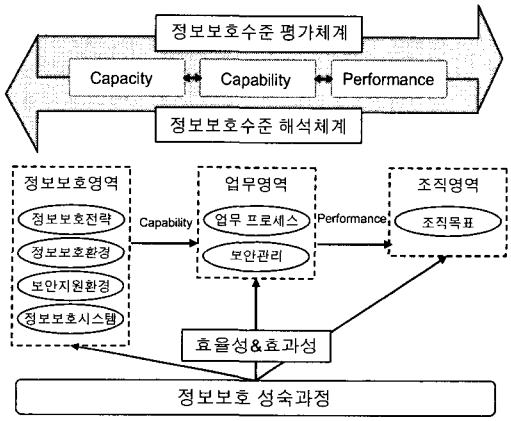


(그림 3) 측정관점의 정보보호 체계

(그림 3)에서 나타낸 보안수준은 아직 완성된 모델은 아니지만, 중간보고서를 작성하는 현 시점에서 본 연구를 통해 접근하고자하는 연구의 큰 방향을 나타낸 것이다.

3.3 해석관점

정보보호 체계의 해석관점이란 'IT 개발환경에서의 개발자(이하 사용자)가 정보보호시스템이 관리 및 활용 하에서 업무를 얼마나 효율적으로 수행할 수 있는가?'에 대한 동적인 관점으로 사용자의 능력 및 정보보호시스템을 사용하려는 마인드와 정보보호시스템이 가지는 성능이 업무를 수행함으로써 발생하는 영향을 도출하는 관점이다. 이러한 관점은 IT 제품 개발환경에서의 정보보호시스템, 사용자, 정보보호전략, 지원환경 및 정보보호 관련 제반 지침이나 규정이 자체적으로 충분한 능력을 확보하고, 이러한 능력을 조직의 업무 수행에 투여함으로써, 결국 개발환경에서의 정보보호 수준을 향상시킬 수 있다는 관점에서 출발한다. 기존 연구(정보보호진흥원, 2003)에서는 이러한 관점을 기본적으로 정보보호주체가 가지는 능력을 Capacity로 명명하고, 이러한 능력이 단위업무에 적용되어서 발휘되는 영향을 Capability로, 그리고 이러한 단위업무가 종합되어 조직 전체적으로 나타나는 조직의 능력을 Performance라고 명명하며, 이들 간의 관계는 (그림 4)에서 보는 바와 같다.



(그림 4) 해석관점의 정보보호체계

3.4 평가관점

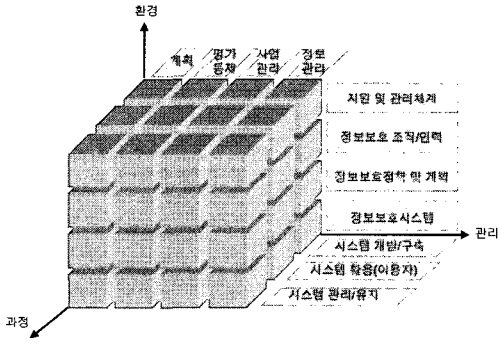
평가관점이라 함은 의사결정을 지원하기 위하여 관심사항에 맞도록 분류하는 관점으로, 실질적으로 IT 제품 개발환경에하에서의 정보보호를 관찰함에 있어서 관심의 초점이 되는 분야를 말하는 것이다. 이러한 관점은 개발자 및 사용자가 쉽게 이해하고, 판단할 수 있는 분야이므로 정보보호수준을 결정하는 기준으로 작용하게 된다. 기존 연구(정보보호진흥원, 2003)의 연구에서는 정보보호 프레임웍을 평가관점으로 전환하기 위하여 관리, 과정 및 환경의 3가지 축을 사용하였다.

- 과정축은 정보보호시스템의 구축과정에 관한 것으로, 이는 정보보호를 계획하고, 구축하며, 운

영 및 유지관리하는 절차를 따르게 된다.

- 환경축이란 전술한 측정관점과 동일한 것으로, 정보보호를 구성하는 제반 요소를 정적인 상태로 관찰하는 것을 말하며,
- 관리축은 조직의 정보보호를 효율적이며, 효과적을 관리하고, 활용을 극대화함으로써, 궁극적으로 정보보호를 통한 조직의 경영전략을 달성하고자 하는 것이다.

이러한 관점으로 재구성된 정보보호 프레임웍을 그림으로 표현하면 다음과 같다.



(그림 5) 평가관점의 정보보호 프레임워크

(그림 5)는 정보보호 프레임웍을 평가관점으로 나타낸 것이다. 그러나 이러한 형태로는 IT 제품 개발 환경에서의 정보보호 수준 평가는 의사결정자 및 관심을 가진 자들에게 유의미한 정보를 제공할 수 없으므로 이를 보다 유의미한 정보로 재구성할 필요가 있다.

본 연구는 이러한 다양한 관점을 기반으로 하여 IT 제품 개발 환경에서의 정보보호 수준을 평가하는 것을 목표로 하고 있다.

4. 결 론

개발환경 및 조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 개발 환경 또는 조직의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준이 필요하고 우리나라에서 적용 가능한 정보보호 시스템들의 평가방법론이 연구되어야 한다.

IT 제품 개발환경에서의 보안은 개별 보안 제품의 조합으로만 달성될 수 없으며, 개발환경에서의 보안 기능을 제공하는 제품/시스템과 관리적인 보안대책이 적절히 융합되어 보안관리체계가 원활히 운영되고 있을 때 한 IT 제품 개발환경세어의 정보보안이 효과적으로 유지될 수 있다는 것을 인식해야 한다. 특히 IT 제품의 개발환경에 대한 안전성의 검토는 IT 제품 개발의 신뢰성과 안전성 확보 측면에서 그 필요성이 증대하고 있다.

IT 제품 개발환경에 대한 보안수준을 점검하기 위해서는 IT 제품 개발환경에 존재하는 취약성과 각종 위협 요인을 분석하고 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준과 평가 도구가 필요하다. 또한 이를 위해 관련분야에 대한 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준과 이를 실제 IT 제품 개발환경에 적용할 수 있는 평가방법론이 연구되어야 한다.

참 고 문 헌

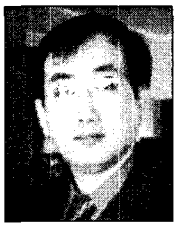
[1] 고일석, 임춘성, "정보보호수준 평가항목 및 방법론 개발", 한국정보보호진흥원, 2003.

[2] 김기윤, 나관식, "취약성 평가에 의한 정보보호지표의 계량화 : 정보자산가치가중치법", 통신정보보안학회지, 제10권, 제1호, 2000.

[3] 김정덕, 김기윤, "정보보호지표 항목개발 및 계량화 연구", 정보보호진흥원, 1998.

[4] 임춘성, "2001 기업정보화 수준평가 결과보

고서", 기업정보화지원센터, 2002.
[5] 한국정보보호진흥원, "정보보호시스템 평가 · 인증지침", 정보통신부, 2000.
[6] 서삼영, "국가정보화수준 측정 및 지표개발", 한국전산원, 2001.
[7] 김석우, 이백철, "정보보호제품 국제공통평가기준과 보호프로파일 해석", 안전경영학회지, 제2권, 제4호, 2000.
[8] 천예광, "지역정보화수준 지표체계 개발에 관한 연구", 국방대학교 석사논문, 1998.
[9] 강신원, "국가정보화지수 측정을 위한 가중치 연구 : RCSS를 중심으로", 정보통신정책연구, 제6권, 제2호, 1999.
[10] 한국정보보호센터, "정보보호시스템 평가 · 인증가이드", 2000.
[11] BSI, BS7799, BSI, 1999.
[12] B. B. Jenkins, security risk analysis and management, countermeasures, Inc, 1998.
[13] Common Criteria Project, common criteria for information technology security evaluation, common criteria, 1998.
[14] B. Guptill, C. Price, a security framework for enterprise using the internet, Gartner Group, 1996.
[15] NIST, an introduction to computer security : the NIST handbook, NIST (national institute of standards and technology), 1995.
[16] Lynette Barnard et al., "The evaluation and certification of information security against BS7799", Information Management & Computer Security, Vol. 6, No. 2, pp. 72-77, 1998.
[17] Rossouw von solms, "Information Security Management (3) : the code of practice for Information Security Management(BS7799)", Information Management & Computer Security Vol. 6, No. 5, pp. 224-225, 1998.



고 일 석

경북대 컴퓨터공학 학사
경북대 컴퓨터공학 석사
USID(San Diego, USA) 경영학 석사(MBA)
연세대 컴퓨터산업시스템공학 박사
현재 동국대학교 컴퓨터멀티미디어학과 조교수
현재 IBC(International Biographical Center) Deputy Director General, Cambridge, UK.