IT 시스템 보안수준관리를 위한 보안 평가 대상 항목 식별

김태훈[1], 코이치 사쿠라이[2], 나윤지[3]
[1,2]큐슈대학교 컴퓨터과학 및 통신공학과
[3]호남대학교 인터넷소프트웨어학과
taihoonn@empal.com

요 약

정보기술의 발달 및 정보화의 촉진으로 인해 IT 시스템의 복잡도는 급격히 증가하고 있으며, 이에 따라 정보보호제품을 설치·운영함으로써 보안목적을 달성하는 과거의 보안정책은 한계에 도달하였다고 할 수 있다.
대부분의 IT 시스템 사용자들은 해당 IT 시스템의 보안대책에 대한 신뢰가 적절한 수준인지 판단할 수 있기를 원하고 있으며, 또한 이러한 수준이 지속적으로 유지되기를 바라고 있다.
보안수준을 유지하기 위해서는 지속적으로 해당 시스템의 보안수준을 확인하여야 하는데, 이러한 확인 및 판단의 근거를 제공하는 가장 기본적이고 전통적인 방법은 보안수준에 대한 평가이다.
본 논문에서는 IT 시스템의 보안수준을 유지하기 위한 보안수준관리의 필요성과, 이를 위해 보안수준 확인이 필요한 평가 대상항목을 식별하고자 한다.

핵심어: IT 시스템 보안수준관리, 평가 대상 항목

Abstract

This paper identifies some components should be evaluated and certified to assure that IT systems are secure. Security objective of IT systems will be obtained by protecting all areas of IT systems, so not only visible parts but also non-visible parts must be protected. And for verifying all the parts of IT systems are protected, we should check the scope of evaluation and certification covers all necessary parts.

1. 서론

IT 시스템에서 다루는 정보는 조직을 유지하고 조직의 임무를 완수하는데 필요한 중요한 자원이며, 정보의 비인가된 누출, 변경, 손실로부터 파생된 문제점은 경제적 손실뿐만 아니라 조직의 지속성 차원에서도 중요한 의미를 갖게 된다.

보안은 모든 부분에서 유사한 수준을 확보하여야 일정 수준을 유지하고 달성할 수 있는 것이다. 따라서 보안을 고려하고 있는 조직은 해당 조직이 달성하고자 하는 보안 목표를 포함한 보안 정책으로부터 이 목표를 달성하기 위해 수행하는 위험평가, 보안대책평가, 개발 및 평가 조건에 대한 고려, 그리고 잔존 위험에 대한 평가 등 전반적인 내용이 균형을 이루도록 노력하여야 한다.

이러한 제반 사항들이 통합적으로 고려되기 위해서는, 현재 시행되고 있는 IT 제품에 대한 평가만으로는 한계가 있다. IT 제품은 제품 자체의 신뢰성과 안정성에 대한 보증을 제공하기에는 충분하지만, IT 제품이 설치되고 운영되는 환경을 포함한 전체 IT 시스템의 보안을 보증하기에는 부족하기 때문이다.
본 논문에서는 IT 시스템이 본래의 구현 목적을 달성하기 위해 유지하여야 하는 '보안수준'을 정의하고, 정의된 보안수준을 달성하기 위해 IT 시스템 수명주기 단계별로 평가되어야 하는 항목들을 제안하고자 한다.

2. 보안수준관리의 필요성

IT 시스템은 단순한 IT 제품의 조합만으로 구성되는 것은 아니다. IT 시스템이 구축되면, 이를 운용하는 사람들이 있고, 주어진 환경이나 업무에 따라 지켜야 하는 절차들도 있다. 따라서 IT 시스템은 이러한 모든 요소들을 포함하는 포괄적인 개념으로 이해되어야 한다.

보안은 위협으로부터 자산을 보호하는 것을 목적으로 하고 있다. 위협은 보호되어야 할 자산이 남용될 수 있는 가능성으로 분류되며, 원론적으로는 모

든 종류의 위협을 고려하여야 한다. 하지만 보안 분야에서는 악의적인 또는 그 밖의 인적 활동과 관련이 있는 위협에 더 많은 주의를 기울여야 한다.

중요한 자산을 보호하는 것은 자산에 가치를 부여하는 자산 소유자의 책임이다. 실제 또는 가상의 위협원도 자산에 가치를 부여하지만, 이는 자산 소유자의 이익과는 반대로 자산을 남용하기 위함이다.

자산 소유자는 자신의 환경에서 발생 가능한 위협을 분석하고, 분석의 결과를 위험으로 변환하여 보안대책을 선택하여 허용 가능한 수준까지 위험을 줄일 수 있다. 보안대책은 직접 혹은 간접으로 지침을 제공하여 취약성을 감소시키고, 자산 소유자의 보안정책을 충족시킬 수 있어야 한다. 하지만 보안대책이 적용된 후에도 취약성은 여전히 잔존할 수 있으며, 이러한 취약성은 당연히 위협원에 의해 악용될 수 있다. 따라서 자산 소유자는 다른 제약을 가함으로써 이러한 위험을 최소화하기 위해 노력할 것이다.

이와 같은 자산소유자와 자산, 위협원, 보안대책, 취약성 등의 상관관계를 도식화하면 (그림 1)처럼 표시될 수 있다.

(그림 1)은 IT 제품의 보안성을 평가하는 공통평가기준(CC, Common Criteria)에 포함되어 있는 것이지만, 전체 IT 시스템으로 개념을 확장하여도 무리없이 적용이 가능하다.

IT 시스템을 IT 제품, 인원, 절차 등의 요소를 포함하는 개념으로 확장한 경우, (그림 1)에서 사용된 블록들의 내용이 동시에 확장되어야 한다. 예를 들어 보안대책은 물리적 대책, 인적 대책, 운영적 대책 등으로 나뉘어 고려되어야 한다.

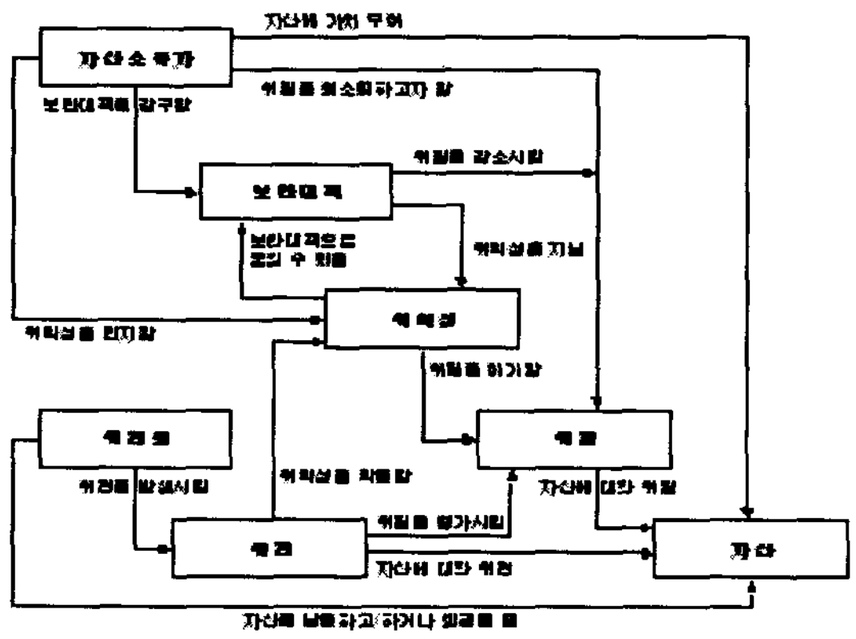

그림 1. 자산을 중심으로 한 보안개념 및 관계

(그림 1)의 화살표 방향에 맞추어 보안 개념을 정의하는 것이 가능하다.

자산의 소유자는 자산이 위협에 노출되기 전에 보안대책이 위협에 대응하는데 적절하다는 확신을 필요로 한다. 자산 소유자는 이러한 확신을 얻기 위해 보안대책을 평가하고자 할 것이다.

공통평가기준에서는 평가의 개념과 중요성을 설명하고 있으나, 보안대책을 수립하기 전에 수행되어야 하는 보안수준의 결정에 대해서는 설명을 생략하고 있다. 공통평가기준에서 기준으로 사용하는 보안수준은 대부분 평가보증등급(EAL)로 미리 결정되기 때문인데, 이 개념을 IT 시스템으로 확장하기 위해서는 보안수준을 정의하는 과정이 반드시 포함되어야 한다.

평가결과는 보안대책이 보호되어야 할 자산의 위험을 줄인다는 것을 신뢰할 수 있다는 보증을 의미하며, 이러한 보증은 보안대책을 적절히 활용하기 위한 신뢰의 근거가 된다.

일반적으로 자산 소유자는 자산에 대해 책임이 있으며, 위협에 자산이 노출되는 위험 허용 수준의 결정에 대해서도 정당화할 수 있어야 한다. 이는 평가로부터 도출된 결과가 정당해야 함을 의미한다. 따라서 평가는 믿을 수 있는 증거로 제시될 수 있는 반복적이고 객관적인 결과를 일관적으로 이끌어 낼 수 있어야 한다.

아쉽게도 모든 평가의 결과가 보안에 대한 보증을 제공한다고 보기에는 어려움이 있다. 평가자는 다양한 이론적 배경과 지식을 가지고 있으며, 이로 인해 평가기준을 해석하는 방식이 다르게 되고, 따라서 평가결과는 항상 유동적이다.

이와 같은 유동성과 변화가능성을 줄이기 위한 방법으로 사용할 수 있는 방안이 인증이다. 평가는 다양한 평가자가 자신의 경험을 통해 획득한 지식을 사용해서 평가기준을 해석하고 적용하는 과정으로 진행된다. 따라서 서로 다른 평가자가 평가한 결과를 검증하여 객관화된 형태로 변환하는 절차가 있어야만 사용자는 평가결과를 신뢰할 수 있을 것이다.

평가결과는 정형화된 문서의 증거 형태로 작성되지만, 실제로 평가를 통과하였는지를 판단하는 것은 절대적으로 평가자의 능력에 관한 문제가 된다. 따라서 문서화된 평가결과를 검토하여 평가자가 평가를 진행하는 동안 객관성과 일관성을 잃지 않았는지 확인하고, 의심스러운 부분에 대해서는 증거를 보완하도록 하는 인증 과정이 반드시 뒷받침되어야 한다.

3. IT 시스템 보안 평가·인증의 필요성

IT 시스템의 개념은 많은 부분에 있어서 혼동의 우려가 있으며, 대부분의 오해는 '시스템(Systems)'의 범위를 어떻게 설정하는가에 따라 발생하게 된다. 본 논문에서 사용하고 있는 시스템의 개념은, 단위 제품으로 구성된 물리적 형상을 포함하여, 물리적 구성품을 운영하고 관리하기 위한 제반 정책, 법/제도 및 절차 등의 관리, 그리고 실제로 시스템을 운용하는 인력 등을 모두 포함하는 포괄적인 개념이다.

이러한 의미의 확대는 정보보호의 개념에서 정보보증의 개념으로 전이되는 과정에서 유도되는 것이다. IT 시스템의 보안을 평가·인증하는 이유는, IT 시스템을 구성하는 세부 항목들의 작은 결함이 지속적으로 누적될 수 있다는 데 있다.

예를 들어, 단위 제품에 포함된 하나의 백도어는 종국에는 전체 IT 시스템의 침해로 이루질 수 있는 가능성을 내포하게 되며, 이러한 경향은 IT 시스템의 복잡도가 증가할수록 확대되게 된다.

하부 제품이나 기술에 포함된 취약점으로 인해 전체 IT 시스템의 위험도가 증가하는 개념은 (그림 2)에 설명되어 있다.

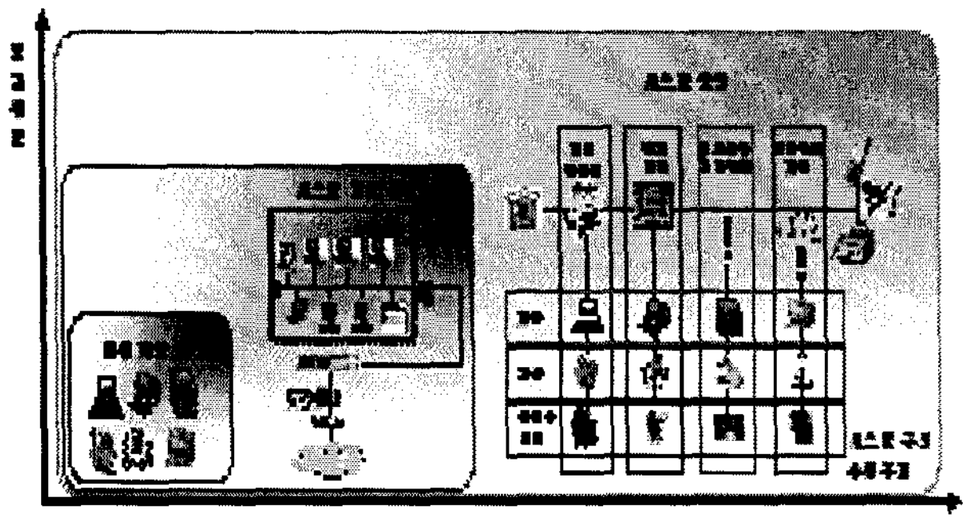

그림 2. IT 시스템 수명주기에 따른 위험 증가

최근까지의 정보보호 개념은 완성된 IT 시스템에 보안대책을부가하는 형식을 취하는 것이었다. 하지만 이러한 방법으로 시스템을 개발, 통합, 운영하게 되면 다음과 같은 문제점들이 계속 발생하게 될 것이다.

- 취약점 및 위협 요인의 누적
- 시스템 복잡도 증가에 따른 신규 취약점 및 위협의 발생
- 보안수준이 다른 시스템의 통합으로 인한 전체 시스템 보안수준 저하
- 인력, 운영 절차 등에 대한 관리 소홀로 인한 보안대응 능력 정체
- 변화하는 환경에 의해 수반되는 신규 위협요소에 대한 대응 요구사항 증가

따라서 해당 IT 시스템의 보안목적을 정확히 달성하기 위해서는 IT 시스템의 개발부터 폐기에 이르는 전체 수명주기에 대해 보안을 고려하여야 한다.

4. IT 시스템 보안 평가·인증의 범위

IT 시스템에 대한 보안 평가·인증 대상 범위는 IT가 사용되고 있는 정도와 IT 구성요소의 능력에 대한 관심 수준에 따라 결정되며, 자산이 안전함을 증명하기 위해서는 운영환경의 가장 추상적인 단계부터 최종 단계까지 모든 보안 관련 사항들이 고려되어야 한다.

따라서 현재 설계중인 IT 시스템의 경우에는 초기의 개념 정립 단계부터 보안공학(Security Engineering)을 접목하여 보안요구사항을 함께 고려하여야 하며, 이미 설치되어 운영되고 있는 IT 시스템의 경우에는 현재의 상태를 정확하게 분석하여 보완이 필요한 부분을 결정하고 이를 반영하여야 한다. 만일 후자의 경우라면, IT 시스템의 수명주기에 비추어 현재 상태 이전의 상태에 대한 내용은 문서화되어 있는 증거들에 기반을 두고 필요한 내용들을 유추할 필요가 있다.

수명주기의 각 단계들은 해당 단계의 평가결과에 대한 이론적 근거를 포함하여야 한다. 즉, 각 단계의 표현이 상위단계의 내용과 일치하는지, 표현물 자체가 완전하고 정확하며 내부적으로 일관성을 가지고 있는지를 합리적이고 확실하게 논증할 수 있어야 한다. 인접한 상위단계 표현물과의 일치성을 보이는 이론적 근거는 평가의 정확성을 증명하는데 중요한 역할을 할 뿐만 아니라, 평가결과에 대한 인증을 부여하는데 결정적인 역할을 한다.

인증은 평가가 논리적·객관적으로 수행되었고 평가과정이 일관성을 유지하였음을 보증하여 주는 것이지만, 대부분의 경우에 인증은 평가가 완료되어 평가결과가 도출된 이후에 수행하게 된다는 제한 요소를 포함하고 있다. 그러므로 인증 과정은 평가결과를 확실히 신뢰할 수 있을 때까지 진행되어야 하

며, 경우에 따라서 인증 담당자는 인증을 위해 평가 결과의 재현을 요구하거나 재평가를 요구할 수도 있다.

평가와 인증의 수행을 필요로 하는 궁극적인 목적은 해당 IT 시스템의 보안목표가 충실히 달성되는지 검증하는 것이며, 해당 IT 시스템을 활용하는 조직은 평가와 인증의 결과를 통해 조직의 운영 목표를 달성할 수 있는 기반을 마련하게 된다. 다시 말하자면, 평가결과를 통해 해당 IT 시스템의 보안목표가 준수되는지를 직접적으로 보이는 이론적 근거를 마련하고, 평가결과에 대한 보증을 통해 IT 시스템이 위협에 대응하고 조직의 보안정책을 수행하는데 적합함을 확인하는 것이다.

평가·인증을 통해 구현하고자 하는 목표는 IT 시스템의 보안대책들이 합리적으로 수립되었다는 것과 이들 보안대책들이 원래 의도한 목적을 달성하기 위해 정확하게 운용되고 있다는 것에 대한 보증을 제공하는 것이며, 이렇게 함으로써 IT 시스템의 안전성과 신뢰성을 확보하기 위한 것이다.

보안 평가·인증의 대상 범위는 현재 운용중인 IT 시스템과 향후 구축하고자 하는 IT 시스템 전체이다. 적절한 수순에 따라 필요한 부분에 대한 평가와 인증을 시행함으로써 IT 시스템에서 생성, 처리, 소통 및 저장되는 정보가 안전함을 보증하고, 이러한 과정을 수행하는 물리적 시스템 및 인력·운영·조직상의 문제로 인한 보안 취약성을 최소화할 수 있다. 따라서 IT 시스템의 설치 목적 및 운영 방침을 포함하고 있는 보안정책, IT 시스템을 구성하는 운영적 요소(인력적 요소 포함), 기술적 요소, 제품적 요소 등의 모든 내용들이 보안 평가·인증의 대상이 된다.

5. 평가 대상 항목 식별

정보시스템의 보안을 아주 짧은 시간에 단 한 번의 평가를 통해 확인할 수 있다면 상당히 효율적이고 바람직한 것이겠지만, 정보시스템의 규모, 소요시간, 기술의 발달로 인해 이러한 방법으로 얻은 결과는 오랫동안 신뢰를 제공할 수 없을 것이다. 또한 전체 정보시스템의 보안을 한 번에 점검하는 것은 신뢰성 측면에서도 바람직하지 않다. 어떤 부분은 다른 부분에 대해 빠르게 변화하는 환경에 따라 더 빠른 관리 주기를 요구할 수도 있기 때문이다.

기본적인 평가 대상 항목의 식별은 이미 (그림 3)과 같이 식별될 수 있다[5-6].

그림 3. 기본적인 평가 대상 항목의 그룹화

(그림 3)으로 정의된 대상 항목은 기본적인 관점에서의 평가 대상이라고 할 수 있으며, 각 그룹에는 다양한 내용들이 정의되거나 포함될 수 있다.

하지만 (그림 3)에 표시된 항목들은 다분히 결과 중심적인 내용이며, 이전 과정의 업무 수행이 적절하게 진행되었다는 가정을 필요로 하는 것이다. 즉, 단순히 (그림 3)에 정의된 평가 대상을 관리하는 것만으로 변화하는 환경적 요인들을 고려하기에는 무리가 있다. 따라서 평가 항목을 설정하기 위해 거쳐야 하는 이전 단계들에 대한 추가적인 고려가 필요한데, 가장 중요한 두 가지 요소가 포함되어야 한다.

첫 번째는 보안수준분석에 대한 고려이다. 보안수준관리 대상들은 실제로는 대부분 보안대책(Security Countermeasure)으로 구현되어 있으며, 보안수준분석은 보안대책 수립을 위한 근거가 된다. 따라서 변화하는 환경에 따라 분석된 결과가 보안수준관리 대상에 충실하게 반영되어 있는지 확인하여야 한다.

두 번째는 보안정책에 대한 고려이다. 정보시스템은 특정 목적을 수행하기 위해 구축되고 운영되므로, 정보시스템의 특성은 해당 정보시스템 소유자의 정책에 따라 설계, 개발, 운영되어야 한다. 따라서 보안과 관련된 내용은 정보시스템 소유자가 보유하고 있는 보안정책을 충분히 반영하고 있어야 한다.
이들 두 가지 항목은 평가 대상에 포함되어야 하며, 다른 대상 항목들과의 연관성이 항시 유지되어야 한다. 이들 두 가지 항목 이외에도, 추가적으로 보안수준관리 기반구조에 대한 내용과, 정보시스템 개발환경에 대한 내용도 평가 대상 항목에 포함시킬 수 있다. 또한 보안수준 보완계획에 대한 검토도 추가적으로 필요하다. 보안수준 보완계획은 일반적으로 알려진 잔존 위험 관리와 유사하다고 볼 수 있으며, 보안정책의 일부로 포함하여 고려하는 것도 가능하다.

이와 같은 개념은 (그림 4)에 표시되어 있다.

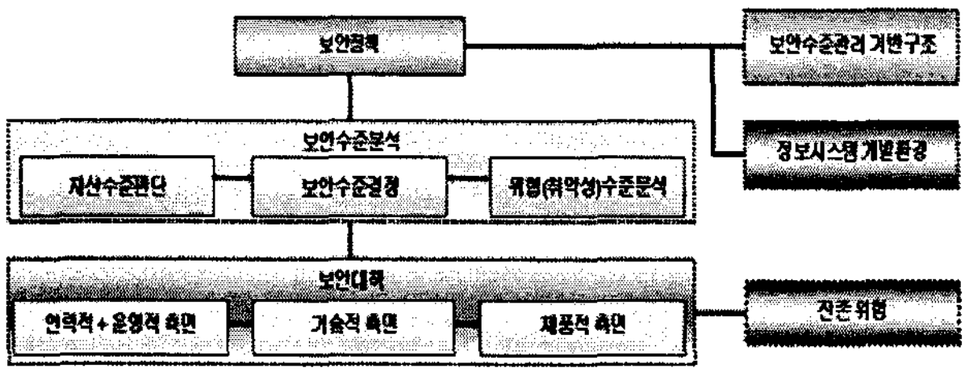

그림 4. 추가된 평가 대상 항목

6. 결론 및 향후 연구 방향

본 논문에서는 IT 시스템의 보안 평가·인증 필요성과 평가대상 항목을 제시하였다.

하지만 IT 시스템은 규모가 대단히 큰 경우가 많으며, 따라서 체계적으로 구성된 적절한 절차에 따라 보안 평가·인증을 수행하지 않으면 막대한 자원의 낭비를 초래할 수도 있다.

따라서 향후에는 구체적으로 시스템 수명주기에 어떻게 보안 평가·인증 요소가 반영되어야 하는지에 대한 세부 연구가 필요하다 할 것이다. 또한 보안 평가·인증 절차를 개발하기 위한 연구도 병행되어야 할 것이다.

참고문헌

[1] Tai-hoon Kim and Haeng-kon Kim: The Reduction Method of Threat Phrases by Classifying Assets, ICCSA 2004, LNCS 3043, Part 1, 2004.

[2] Tai-hoon Kim and Haeng-kon Kim: A Relationship between Security Engineering and Security Evaluation, ICCSA 2004, LNCS 3046, Part 4, 2004.

[3] Ho-Jun Shin, Haeng-Kon Kim, Tai-Hoon Kim, Sang-Ho Kim: A study onthe Requirement Analysis for Lifecycle based on Common Criteria, Proceedings of The 30th KISS Spring Conference, KISS (2003)

[4] Haeng-Kon Kim, Tai-Hoon Kim, Jae-sung Kim: Reliability Assurance in Development Process for TOE on the Common Criteria, 1st ACIS International Conference on SERA

[5] Tai-Hoon Kim, Seung-youn Lee: Design Procedure of IT Systems Security Countermeasures. ICCSA 2005: LNCS 3481, 468-473

[6] Tai-Hoon Kim, Chang-hwa Hong, Myoung-sub Kim: Towards New Areas of Security Engineering. RSFDGrC 2005, LNCS 3642, 568-574