情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

# CC를 적용한 시스템 보안평가 동향

이 경 구*, 손 경 호*

요 약

현재 미국을 비롯한 선진 국가에서는 ISO 국제 표준인 국제 공통 평가 기준 ISO/IEC 15408(CC v2.1, Common Criteria for Information Technology Security Evaluation))과 공통평가방법론(CEM, Common Methodology for Information Technology Security Evaluation)에 근거하여 IT 제품 및 시스템에 대한 보안성 평가를 하고 있다. 그러나, 현재 CC 및 CEM은 주로 IT 제품의 보안성 평가를 위한 것이며, 실제 IT 환경에서 운용되는 시스템에서 이를 적용해 평가하는데는 많은 어려움이 있다. ISO를 중심으로 각 국에서도 이와 관련해 시스템 평가에 CC를 적용하기 위한 방법론이 검토 중에 있다. 그리고 현재 개발 진행중이거나 시장에 출시된 많은 제품이 여러 단일 제품이 합성된 통합제품 형태로 구성되고 있는 추세이며, 이는 시스템 평가 문제와 더불어 향후 CC 기반의 평가를 활성화시키기 위해 풀어야 할 문제로 제기되고 있다.

본고에서는 각 국에서 추진 중인 시스템 평가 동향을 살펴보고, 현재 ISO/IEC SC27/WG3에 표준화로 제안된 "Security Assessment of Operational System"에 대해 살펴보고자 한다.

## Ⅰ. 서 론

1997년 8월에 Milkyway Black Hole firewall 제품이 1996년 1월에 완성된 CC v1의 EAL3 등급으로 캐나다 CSE(Communications Security Establishment)에서 평가를 받은 이후로 많은 제품이 CC로 평가를 받거나 진행 중에 있다.

선진 각 국을 비롯하여 전 세계적으로 정보보호를 위해 안전성이 보증된 제품의 활용이 증대되고 있다. 그러나, 많은 보안문제가 제품 자체에서 비롯되는 것이 아니라 제품을 실제 사용하는 환경에서 부실한 관리, 부실한 설치 등의 인적, 관리적, 물리적인 요인에 의한 시스템 차원에서 문제점이 발생된다. 게다가 네트워 시스템의 경우 다른 시스템에 연결되기 때문에 시스템에 발생하는 보안문제는 그 시스템 자체뿐만 아니라 네트워으로 연결되는 전체 시스템에 영향을 미친다.

이런 이유로 운영환경에서 시스템을 평가하기 위한 평가 방법은 시스템을 사용하는 조직뿐만 아니라 네트웍으로 연결된 모든 시스템의 보안을 위해 절실하게 필요하다. 그러나 CC는 시스템 평가(여기서 말하는 시스템 평가는 CC에서 정의하는 IT 시스템 뿐만 아니라 비 IT 보안 수단을 합친 것을 말한다.)를 위해 설계되지 않았기 때문에 CC를 시스템 평가에 적용하기엔 많은 어려움이 발생하다. 또한, CC에 근거한 보안성 평가는 CEM에 따라 평가를 수행하게 되어 있지만 CEM은 주로 IT 제품의 보안성을 평가하기 위해 설계되었기 때문에 시스템 평가에 이를 적용하기에는 불충분하다. 따라서 시스템 평가를 위해 적용할 수 있는 평가방법론이 존재하지 않는다.

이 문제를 해결하기 위해 각 국에서는 특정 시스템을 대상으로 한 새로운 보안성 평가 기술을 개발 중에 있으며, 이를 여러 시스템에 적용하기 위한 시스템 해석 방법이나 시스템 평가 방법론에 대한 연구를 진행 중에 있다.

또한 시스템 평가와 더불어 제품의 합성(Composite) 문제가 제시되고 있다. 이 문제는 다양한 제품의 추가적인 불임(Glue) 문제에서 출발한다. 이 문제에 대해 기능 컴포넌트의 합성문제 관점에서 보는 입장과 시스템으로부터의 보안요구사항 분해 관점에서

* 한국정보보호진흥원(KISA)(kglee, khson}@kisa.or.kr)

보는 관점이 있다.

본 고에서는 각 국 및 ISO/IEC SC27/WG3에서 진행 중인 시스템 평가와 합성제품 평가 동향을 살펴보고 추후, 이와 관련해 국내에서 시스템 및 합성제품에 대한 평가기준 및 평가방법론 수립 필요성을 마련하기 위함이다.

## II. 시스템 평가 개요

### 1. 시스템 평가 정의

시스템평가에서 시스템이란, 시스템이 제공하는 IT 기능과 메커니즘에 사람, 절차 등의 비-IT 요소가 통합되어 운영되는 것을 말한다.

시스템 평가는 시스템이 포함하는 IT요소와 비-IT 요소가 적용되는 특별한 운영환경에서 정확하고 올바른지 검증하며, 정의된 환경에서 수용 가능한 위험에 적절하게 대처하는지에 대한 검증을 하는데 초점을 맞춘다.

### 2. 시스템 평가를 위한 요구사항

시스템 평가에서 운영환경 고려는 시스템평가의 필수적인 요소다. 운영환경을 고려한 시스템평가는 아래와 같은 두 가지 중요한 부분이 있다.

- 보안정책 수행과 위협에 대응하기 위해 설계, 구현, 운영되는 기술에 기초한 기능
- 기술에 기초한 기능을 이용하는데 통제하는 정책과 절차

시스템 평가를 위한 운영 보안요구사항은 CC에서 정의한 IT 기능 요구사항과 보증요구사항에 추가되며, 조직의 보안정책 과 가정사항 들은 시스템의 비-IT 부분에 집중된다. 제품평가에서, 이런 보안수단(보안정책, 가정사항)은 일반적으로 운영환경에서 가정된다. 그러나, 시스템 평가에서는 이것이 존재하던 평가되어야 하며, 적절하게 보안목적에 부합되는지 검증되어야 한다.

## III. 각 국의 시스템평가 동향

### 1. 미국

미국에서는 CC체계 이전 자국의 보안 평가기준인 TCSEC[1]에서부터 이미 시스템 합성과 평가에 대해 작업을 진행 해 오고 있다. US 스킴(TPEP[2], TTAP[3])에서는 플랫폼에 독립적인 컴포넌트를 평가함에 따라, 이 평가 결과가 이후 시스템 및 다른 제품과의 통합이 필요함을 인지하고, 평가결과의 재사용 관점에서 평가된 컴포넌트를 합성하기 위해, TNI[4]에서는 C2 레벨에서 네트워으로 연결된 컴포넌트의 시스템 평가에 관심을 가졌다. 또한, 네트워 시스템 구조와 설계(NSAD, Network Security Architecture and Design) 문서에서는 네트워 시스템에서 허용된 컴포넌트 형태를 정의를 하고 있다. 그러나 여기에서는 네트워 제품의 특정 컴포넌트 사용과 특별한 레벨(C2)로 한정함으로써 일반적인 시스템 평가라고 하기에 범위가 너무 좁았다.

이후, 1996년에 미 항공 관리국, FAA[5]는 1370.82 "Information System Security Program"에서 정부의 항공 시스템(NAS[6])의 안전한 구축과 운용을 위해 보안 인증과 관리 패키지(SCAP[7])와 PP (Protection Profile)를 필요로 했으며 현재 NAS 시스템에 대한 PP를 작업 중에 있다.

그리고 IT 시스템의 인증과 인정을 위해 NIST에서 현재 C&A(System Certification and Accreditation) Project를 진행 중에 있다.

- 미 연방 항공 관리국(FAA)

미국에서는 안전한 항공 시스템을 구축하기 위해 국가 항공 시스템에 CC를 적용해 시스템 PP Template 개발을 추진해오고 있다. 이 Template은 PP의 "Top Level"(정책, 위협, 가정사항, 환경) 개발에서 공통적인 요구사항을 재사용하며, CC 전문어를 이해하기 쉬운 형태로 간략화 하기 위함이다.

이 작업은 미 MITRE라는 기관의 CASSD 연구소에서 진행 중에 있으며, 현재 PP와 관련해서 NAS_PP_Template_v1.0과 NAS_PP_Supplement_v1.0의 두 종류의 문서를 공개하고 있다.

또한, SCAP는 항공 시스템에서 제공하는 항법과 착륙 서비스, 교통관리, 비행 정보, 비행기 사이간격

1) Trusted Computer System Evaluation Criteria
2) Trusted Product Evaluation Program
3) Trusted Technology Assessment Program
4) Trusted Network Interpretation of the TCSEC
5) Federal Aiation Administration
6) National Airspace System
7) Security Certification and Authorization Package

보증 등의 서비스를 위해 요구되는 Tool 들을 포함한다.

CASSD는 시스템 통합과 평가를 위해 아래와 같이 몇 가지 문제점을 제기하고 있다.

- 첫 번째로 큰 시스템 개발은 법적인 문제, 정책과 절차가 불일치 하는 문제 등이 있을 수 있다는 것이다.
- 두 번째로 시스템 PP는 시스템 통합 시 COTS (Commerce Off The Self) 제품을 수용해야 하기 때문에 어떤 제품은 CC 기반 하에 평가를 받았지만, 평가를 받지 않은 제품이 있을 수 있으며, 평가받지 않은 제품에 대해서는 보안성이 검증되어야 했다. 그리고 COTS 제품은 시스템 통합자가 소스코드에 접근 할 수 없다. 또한, 이 제품들은 각기 다른 보안 모델에 의해 개발되었으며 다른 보안 정책을 가지고 있다. 또한, 내부적으로 다른 메커니즘을 사용하고 있다는 것이다.
- 세 번째로 COTS 제품들의 보안기능 및 속성을 합치기 위한 계산방법이 없으며 이에 대한 어떠한 지침도 제공되지 않다는 것이다.
- 네 번째로 CC는 제품개발 단계에서의 안전성에 대한 보증에 초점을 맞추고 있기 때문에 NAS 시스템 PP Template는 시스템 전체 생명주기동안 형상관리를 요구하며, 결함 권고, NAS 운영 중에 취약성 분석을 요구함으로써 전체 생명주기에 걸쳐 시스템의 보증을 요구한다는 것이다.

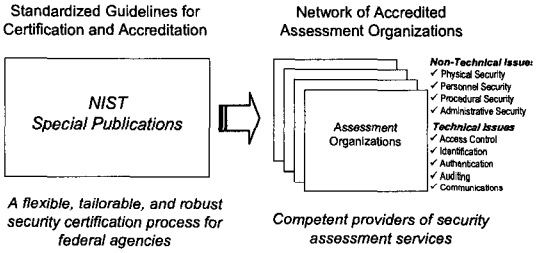
NAS 시스템 PP Template의 내용은 모든 NAS 시스템 PP에 적용하기 위해 요구되는 원문을 가지고 있으며, 목표 NAS 시스템에 특별히 요구되는 부분을 완전하게 하기 위한 특별한 지시를 가지고 있다. NAS 시스템 PP Supplement는 튜토리얼, 설명서를 제공하고 있으며, NAS 시스템 PP 작성자를 위한 가이드를 제시한다.

• NIST의 C&A

1996년 미국의 백악관에서 발표한 문서(OMB Circular A-130, Federal Information Resources)에서는 정부기관의 공무원은 시스템의 안전한 관리를 위해 계획하고, 위험을 이해하며, 현재 상태와 대응할 수 있는 수준의 위험을 적절하게 완화하는 방법을 알고 있어야함을 강조하며, 위험에 기초하여 Cost-effective 한 방법을 수립하도록 정의하고 있다. 이런 요구사항을 충족시키기 위해 C&A 프로젝트는 단계 1에서 정부 IT 시스템의 보안 인증과 인정을 위한 표준화된 지침을 개발하며, 단계 2에서는 표준화된 지침에 기초하여 비용 효과적이며, 질적인 보안 평가를 실시 해 안전한 국가네트워크 구현을 목표로 한다. 이를 위해 단계1에서 지침이 되는 문서, NIST SP 800-37, NIST SP 800-53, NIST SP 800-53A의 세 종류의 지침서를 개발 또는 개발 중에 있다.

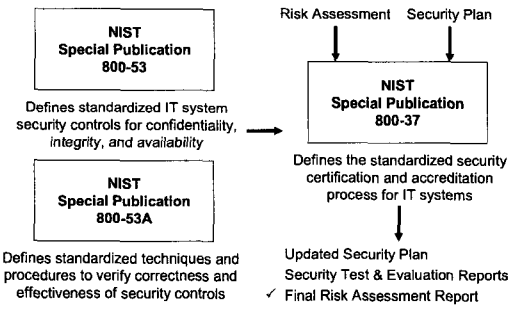
그리고 단계 2에서는 위 지침에 따라 공공부분과 사설 조직에 보안 인증을 해준다.

아래의 그림은 그 단계를 나타낸다.




〔그림 1〕 NIST의 C&A단계

그리고 각각의 문서는 아래와 같은 관계를 가진다.




〔그림 2〕 각 지침서 관계

이 지침에 따르면 먼저 각 IT시스템의 특성을 정의하며 시스템에 저장되는 정보와 전송되는 정보 등에 대한 중요도 또는 민감도를 검사하며, 시스템의 내/외부 노출 정도를 평가한다. 그리고 나서 적절한 등급을 정의하게 된다.

시스템의 중요도/민감도는 비밀성, 무결성, 가용성 측면에서 측정하며, 내/외부 노출은 위협에 대해 IT 시스템에 잠재적인 위험에 대해 측정한다. 등급은 "Low", "Moderate", "High"로 나누고 여기에 대한

보안 통제를 위해 관리, 운영, 기술적인 통제를 실시한다.

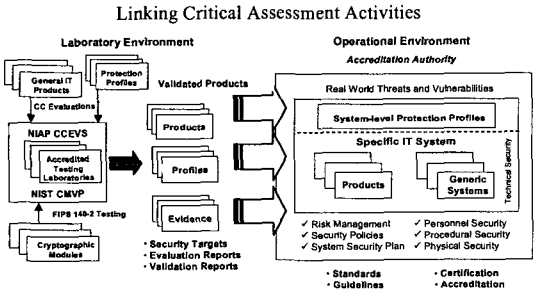
크고 복잡한 시스템에 대해서는 IT시스템의 인정경계를 수립하고 시스템 레벨 컴포넌트 집합 또는 서브시스템을 정의한다.

서브시스템 분해는 C&A 과정을 더욱 더 효과적으로 용이하게 하며 위험 관리와 방어 수준을 쉽게 할 수 있게 한다. 각 서브시스템 컴포넌트는 보안계획과 적절한 보안 요구사항 집합으로 완전히 특성화되며, 그 컴포넌트를 위해 보안 통제방법이 식별된다.

각 서브시스템 컴포넌트는 다른 인증 등급을 가질 것이다.

이런 C&A 과정은 NIST 암호 모듈 검증 프로그램, CMVP[8]과 NIAP의 공통 평가 기준과 검증 프로그램, CCEVS[9]의 지원을 받는다.

아래 그림은 중요평가 활동을 연결한 것이다.




〔그림 3〕 C&A와 다른 평가와의 관계

## 2. 영국

영국 CESG[10]에서는 시스템 평가를 위해 SYS 패키지를 통해 평가를 시행 중에 있다. 이를 위해 CC의 EAL1에서 EAL4까지의 보증 등급과 비슷한 개념으로 아래 표와 같이 SYS1에서 SYS4 패키지를 두고 있다. 또한, 세부적인 평가를 위해 "SYSn Assurance Package Framework" 문서를 제공하고 있다.

SYS 평가는 영국정부(HMG[11]) 시스템과 평가의 상호 인증이 요구되지 않는 시스템에 사용하기 위해 의도된 제품을 위해 고안되었으며, 이 SYSn 보증 패키지는 국방성(MoD[12])의 특별한 요구사항에 부합하기 위해 설계되었다. 또한 SYS 평가는 존재하는 방법론과 평가기준을 사용하며, 문서의 정확성보다는 취약성 테스트를 더 강조한다.

아래 표에서 보면 AVA_VLA.1 개발자 취약성 분석 컴포넌트에서 SYS2와 SYS3에서는 AVA_VAL.1+를 요구하고 있다. 이 컴포넌트에서 AVA_VAL.2.3E을 제외하고 AVA_VAL.2에서 요구하는 사항을 AVA_VAL.1에서 추가하고 있다. AVA_VAL.1+.3.E에서는 평가자가 제공된 평가 증거에 기초하여 독립적인 취약성 평가를 수행함을 나타낸다. 여기에서 제공된 평가 증거는 JIL[13]문서의 "Collection of Developer Evidence" 등에 소개하고 있다.

〔표 1〕 SYSn 보증 패키지

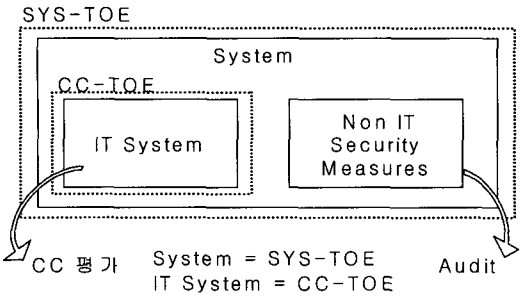
| 보증 클래스 | 보증 컴포넌트 | SYS1 | SYS2 | SYS3 | SYS4 |
|---|---|---|---|---|---|
| Configuration Management | ACM_AUT | | | | 1 |
| | ACM_CAP | 1 | 2 | 3 | 4 |
| | ACM_SCP | | | 1 | 2 |
| Delivery and Operation | ADO_DEL | | 1 | 1 | 2 |
| | ADO_IGS | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 |
| | ADV_HLD | | 1 | 2 | 2 |
| | ADV_IMP | | | | 1 |
| | ADV_LLD | | | | 1 |
| | ADV_RCR | 1 | 1 | 1 | 1 |
| | ADV_SPM | | | | 1 |
| Guidance Documents | AGD_ADM | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 |
| Life Cycle Support | ALC_DVS | | | 1 | 1 |
| | ALC_LCD | | | | 1 |
| | ALC_TAT | | | | 1 |
| Tests | ATE_COV | | 1 | 2 | 2 |
| | ATE_DPT | | | 1 | 1 |
| | ATE_FUN | | 1 | 1 | 1 |
| | ATE_IND | 1 | 2 | 2 | 2 |
| Vulnerability Assessment | AVA_MSU | | | 1 | 2 |
| | AVA_SOF | | 1 | 1 | 1 |
| | AVA_VLA | | 1+ | 1+ | 2 |

## 3. 프랑스

프랑스는 DCSSI[14]에서 시스템평가를 수행하고 있으며 시스템을 특별한 IT 설치로 단지 제품의 결합만 아니라 알려지고 통제된 비-IT 보안 수단의 제품 조합이라고 정의하고 있다.

그리고 평가되는 TOE(Target of Evaluation)는 아래 그림과 같이 구별해서 진행하고 있다.

8) Cryptographic Module Validation Program
9) Common Criteria and Validation Program
10) Communications-Electronics Security Group
11) Her Magesty's Government
12) Ministry of Defence
13) Joint Interpretation Library
14) Direction Center for Security of Systeme Information




〔그림 4〕 TOE 구별

위 그림과 같이 CC-TOE에 대해서는 IT 시스템 평가라고 하며 SYS-TOE에 대해서는 시스템 평가라고 한다.

시스템 평가를 위해서는 우선 IT 시스템에 대한 평가가 이루어져야 한다. 그러나, IT 시스템의 평가를 통해 전체 시스템에 이를 반영하기에는 많은 문제점이 존재한다고 말하고 있다.

먼저 IT시스템 평가의 문제점은 시스템 개발자 혹은 제품 통합자가 시스템을 구성하는 제품의 개발 단계에 포함되지 않는 다는 것이다. 이로 인해, 제품에 대한 정보가 부족하다. 또한, 시스템 내에 인증과 인증되지 않은 제품이 사용 될 수 있다는 것이다. 그리고 현재 보증등급, EAL 척도는 너무 IT 제품 평가에 치중되어 있다는 것이다.

이런 문제점을 해결하기 위해 시스템을 구성하는 각각의 CC-TOE가 완전하게 평가되어야 하며, IT 시스템 개발자가 시스템 통합자가 되어야 함을 강조한다. 그리고 특별한 보증 척도 정의가 필요한데 이를 위해 SEL1, SEL2, SEL3의 새로운 보증 패키지를 정의하고 있다.

그리고, 시스템 평가를 위해서 IT부분은 IT 시스템 평가와 동일하며 비-IT 수단에 추가적인 요소가 요구된다.

시스템 평가에서 IT 시스템에 대해 그것의 변화를 검사하고, 비-IT 보안 수단에 대해서는 그것이 여전히 적용되는지를 관리해야 한다고 말한다.

## 4. 캐나다

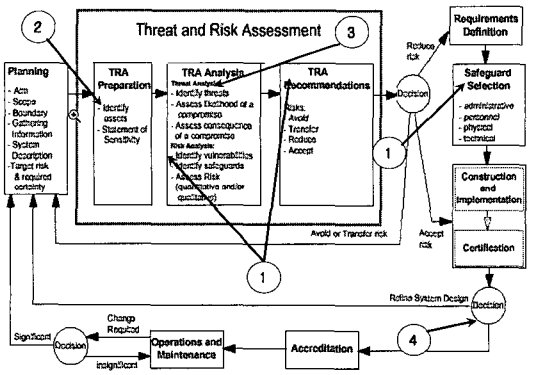
캐나다에서는 현재 CC에 TRA(Threat and Risk Assessment)를 연관시키는 작업을 CSE[15]에서 작업 중에 있다. 캐나다 정부의 보안 정책, GSP[16]에서는 TRA를 통해 IT시스템에서 위험을 완화시키기 위해 필요한 보안 통제를 식별하고 그 결정을 인증 및 신임하게 한다.

그러나, TRA 지침은 어떻게 TRA 결과가 시스템 보증 과정에 입력으로 사용되는지에 대한 세부적인 방향을 제시하고 있지 않다. 반면에 CC는 시스템에 기술적, 절차적, 정책적 정형화된 구조를 제공한다. CC를 TRA에 적용함으로써 시스템의 정해진 보증등급에 부합하는 보호방법을 선택하고 식별하는데 이용하고자 한다.

또한, TRA 보호방법이 어떻게 CC 클래스와 패밀리에 대응되는지에 대한 지침을 제공한다.

TRA 동안 CC 보안 요구사항 클래스와 패밀리 수준에 매핑시키는 두 가지 방법을 서술한다. 한가지 방법은 위험을 완화시키기 위해 분석된 후에 존재하거나 소개된 TRA 보호방법과 그것이 만족되는 기능과 보증 요구사항 사이의 연결이며, 다른 한가지는 TRA 결과물과 보호방법의 보증 등급이 위험을 수용할 수 있게 제공되어야 한다.

이런 작업을 위해 아래와 같이 TRA 방법에 추가적인 작업이 진행되어야 한다. 아래 그림에서와 같이 ①보호방법의 재 정의와 결정이며 ②에서 V(정보의 가치)를 할당하고, ③에서는 위협 등급을 판단한다. ④에서는 보호방법이 시스템 보증에 연관되게 매핑하는 결정을 한다.

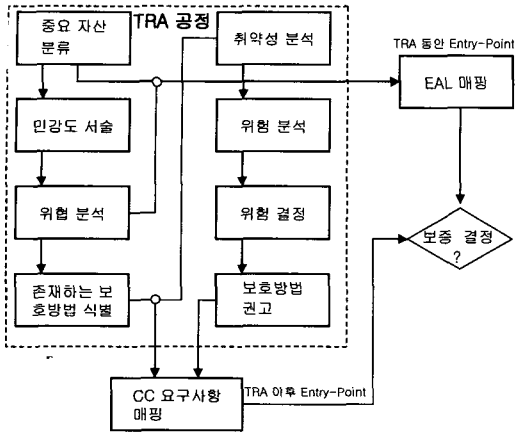



〔그림 5〕 TRA과정 중 추가작업

위의 그림을 간략하게 Entry-point로 다시 정의하면 다음과 같다.

15) Canadian Security Establishment

16) Government of Canada Security Policy




〔그림 6〕 TRA 공정

## 5. 러시아

러시아는 핵 원료 통제와 승인 자동화 시스템 (MC&A[17])의 통제를 위해 시스템 PP를 개발하고 있다. Multi-level MC&A는 몇 개의 통제된 영역 내에 분산되며 정보 비밀성을 몇 개의 등급으로 나눈다. MC&A의 사용자는 민감한 데이터에 대해 사용자마다 각기 다른 접근권한과 특권을 지니고 있다.

Multi-level MC&A PP 개발의 목표는 정보 보안에 식별된 위협에 대응하기 위해 높은 보증 보안 요구사항 표준 집합을 구축하는 것이다.

그리고, PP개발하는데 아래와 같은 어려움이 있다고 말한다.

- 첫 번째로 MC&A PP는 제품보다는 IT시스템에 대한 PP이기 때문에, PP 중에 IT 시스템을 위한 어떤 PP 도 없다는 것이다.
- 두 번째로 CEM은 신뢰된 IT제품 집합으로부터 신뢰된 IT시스템을 구축하는 방법에 대한 설명이 없다는 것이다.
- 세 번째로 IT시스템 PP개발을 위한 실제 예가 충분치 않다는 것이다.

MC&A 시스템은 LAN-based된 자동화 시스템이며 가장 낮은 등급의 MC&A 시스템(Class 3)은 하나의 보호되고 통제된 영역을 가지며, 모든 정보를 위한 하나의 비밀 등급이 존재하고, 사용자에게 동일한 접근 권한의 특성을 지닌다. 그리고 Class 3 MC&A 시스템은 요구되는 보안기능을 포함한 COTS IT 제품(OS, DBMS)을 포함한다. 그리고 이 IT 제품의 부족한 보안 기능은 관리적인 수단으로 쉽게 보상 할 수 있다고 말한다.

또한, 많은 위협들은 운영 환경의 적절한 선택(예, 물리적인 고립, 안전하게 통제된 영역과 확실한 인적 채용)에 의해 제거된다고 말한다.

Class 2 MC&A 시스템 정보는 한 개 이상의 비밀성 등급을 가지고 있으며, 사용자는 다양한 정보 접근 권한을 가진다. 그리고 모든 MC&A 장치는 하나 또는 그 이상의 보호되거나 통제된 영역 내에 존재한다.

그리고, MC&A 시스템 PP를 개발하기 위해 LSPP[18]를 참조했다. LSPP는 참조한 이유로는 다양한 레벨의 MC&A 시스템에 요구되는 다양한 환경을 지원하기 위한 강제적 접근 통제를 통합하고 있다는 것이다.

또한, LSPP 대부분의 기능요구사항은 Class 2 MC&A 시스템의 요구사항과 유사하다. 그것은 대부분의 기능 요구사항(접근통제, 인증, 감사)이 OS 레벨에서 구현되기 때문이라고 말한다.

Multi-level MC&A PP의 TOE는 자체 보유한 복잡한 소프트웨어와 MC&A 시스템의 안전한 운영을 쉽게 하도록 하는 사용자 매뉴얼로 구성되어 있다.

러시아에서는 가까운 미래에 PP가 개발될 것이라고 말하며, OS, DBMS 그리고 다른 응용을 포함한 다양한 MC&A 소프트웨어를 목표로 각각 분리된 PP로 개발하고자 한다.

## 6. 일본

일본은 1999년부터 ECMA PP를 참조해서 e-business systems PP를 IPA[19]와 JEIDA[20]에서 개발중이다. e-business systems PP의 목적은 일본 사업 환경에 수용하기 위해 최소한의 보안 요구사항을 정의하며, 과거의 보안 사건에 대해 대응(위협 분석과 보호방법의 미숙, 결함 권고 처리 미숙, 사고 처리와 탐지 부족 등)하기 위함이다.

17) Nuclear materials control and accounting automated systems

18) Labeled Security PP

19) Information technology promotion Agency Japan

20) Japan Electronic Industry Development Association

일본은 전자정부를 향한 시스템 적용을 목적으로 2000년도에 전자정부 전용 정보제공 시스템 PP, 전자정부 전용 전자신청 시스템 PP, 전자정부 전용 전자조달 시스템 PP를 개발했다. 현재 이 PP들은 공식적인 보안 평가·인증을 받고 있지 않다. 따라서, 이 PP의 내용을 그대로 참조해서 ST에 포함할 수 없다. 다만 ST작성 시 참고 자료로 활용 할 수 있다고 말하고 있다.

특히 일본 경제산업성의 "Haruki Tabuchi"는 ISO/IEC SC 27/WG3 "System Evaluation"을 제안했으며, 동시에 그는 "Guideline for System Evaluation"라는 문서를 제안하고 있다. 이 문서는 시스템 평가를 위한 여러 가지 사항을 담고 있으며, 시스템을 특별한 목적과 운영 환경에서 특정 IT가 설치된 것이며, 전형적으로 시스템 평가와 제품 평가 사이에는 차이점이 있다라고 말하며 시스템 평가는 실제 또는 식별되고 알려진 운영상의 환경이 고려되어야함을 정의한다.

이런 상황에서, 시스템 평가를 위해서는 인적 운영을 위한 대책, 시스템의 실제 개발과 운영 환경 고려, 시스템을 위한 스킴 관리 등의 몇몇 문제가 고려되어야 함을 정의한다.

그리고 이 문서는 시스템 개발환경과 운영환경의 고려사항을 정의하고 이런 점을 개선하기 위해 ISO/IEC 17799로부터 새로운 보증 컴포넌트와 관리 요구사항을 제안한다.

또한 제품평가의 국가 간 상호 인증을 시스템 평가에서의 국가 간 상호 인증으로 확장시키기 위해 아래와 같은 몇 가지 문제를 제시하고 있다.

- 첫 번째로 "어떻게 관리 통제 수단을 평가 할 것인가"이다. 이것은 평가 방법의 적용 이전에 보안 관리 요구사항이 제공되어야 하며, 인적 운영과 물리적 객체를 위한 보안 관리 요구사항의 정립이 필요함을 의미한다.
- 두 번째로 "개발 결과로 어떤 활동이 수행되며, 이 결과로부터 어떤 문서가 생성되는가" 하는 것이다. 이것은 시스템 개발 과정 중에 생성되는 증거를 위해 개발자에게 요구되는 것이다.
- 세 번째로 "어떻게 TOE가 변경 가능함을 관리하는가" 하는 것이다. 만약 시스템이 복잡하며, 다른 COTS 제품으로 이루어진다면 시스템에 안전한 방법으로 통합되는 것이 필요함을 의미한다.
- 네 번째로 "어떻게 시간과 비용을 향상시킬 수 있냐"는 것이다. 평가를 위해 소요되는 시간과 비용 때문에 시스템에서 효과적이며 적당한 보증 컴포넌트가 고려되어야 한다. 보통 TOE는 평가가 끝나고 나서 사용자에게 서비스를 제공한다. 따라서 그것이 서비스를 시작하고 나서 평가를 하는 것은 어렵다.

이런 시스템 평가에서의 문제점을 해결하기 위해 보안 관리 요구사항으로 인적 운영, 물리적 에러나 자연적 재해에 대응하기 위해 ISO/IEC 17799를 적용해 시스템 평가 방법론을 만들고 있다.

## Ⅳ. 표준화 동향

현재 시스템 평가와 관련해 일본의 경제산업성의 Haruki Tabuchi가 제안한 ISO/IEC JTC1/SC 27/WG3 N610, "Security Assessment of Operational Systems" 문서가 표준화 작업 중에 있다. 이 문서에서는 COTS 제품으로 합성된 시스템과, 구성된 제품의 운영환경에서의 평가는 현재 CC 제약 내에서는 부합되기 어렵다고 말하며, 이를 해결하기 위해 여러 종류의 실제 시스템 평가에서 사용될 수 있는 접근법을 제안하며, 시스템 평가에 CC를 적용하기 위한 평가기준과 가이드를 제공하고 있다.

또한, 이 문서는 시스템 평가 가이드와 CC의 IT 기능요구사항에 비-IT 기능요구사항과 운영 보증요구사항을 포함한 시스템 보안 요구사항, PP(Protection Profile)와 ST(Security Target)평가를 포함한 시스템 평가방법론에 대해 서술하고 있다.

### 1. 시스템 평가 개요

시스템 평가 가이드를 제공하기 위해 우선 CC에서 사용되는 용어 정의는 다음과 같다.

- ㅇ Product : 다양한 시스템 내에서 사용되거나 포함될 수 있도록 설계되어 기능을 제공하는 IT 소프트웨어, 펌웨어, 하드웨어 패키지이며, 시스템의 다양성 내에서 사용되거나 포함되도록 설계된 기능성 제공
- ㅇ Component : 시스템의 부분으로 다양한 환경에서 사용 가능한 제품(예, 오라클, NT)
- ㅇ System : 특별한 목적과 운영 환경에서 특정

IT가 설치된 것으로 알려진 환경에서 하나 또는 더 많은 컴포넌트가 사용되는 특별한 실 예를 말하며, 시스템 평가는 실제 또는 식별되고 알려진 운영상의 환경이 고려됨

- Composition : 두 개 이상의 IT 제품의 합성이며 Composition은 두 가지 레벨을 가지고 있다. 하나는 큰 레벨(예, IT 제품을 수집해서 "System"으로 합성(컴포넌트로부터 시스템 구축))이고 다른 하나는 작은 레벨(예, 데이터베이스 와 OS)
- Packages : 컴포넌트들의 중간 합성으로서 식별 가능한 보안 목적의 부분집합과 부합되는 기능 또는 보증요구사항의 집합 표현을 허용하며 재사용 가능하다.

그러나, 이 문서에서는 위의 정의에서 제품과 시스템 개념의 차이가 이해하기 어려워 제품과 시스템 평가의 차이점을 구별하기 위해 제품과 시스템의 특수성을 아래와 같이 정의해 제품과 시스템을 "제품 TOE", "System TOE" 개념으로 나타낸다.

- Product(TOE) : 평가에 필요한 관리와 사용자 가이드와 연관된 보안 컴포넌트 또는 컴포넌트 집합을 의미하며, 일반적으로 한 업체에 의해 개발된 다양한 컴포넌트로 구성된 것을 제품 TOE라 한다.
- System(TOE) : 따로 평가되거나 평가되지 않은 제품과 비 기술적 운영, 관리와 형상 통제 등으로 구성된 서버 시스템의 조합이다. 시스템 TOE는 다양한 업체에 의해 제공되는 다양한 컴포넌트를 가지고 있다. 이 컴포넌트들은 제품 개발에 참여하지 않는 시스템 통합자에 의해 시스템 합성이 이루어진다.

시스템을 합성할 때 컴포넌트 사이와 컴포넌트와 시스템 환경(예, 사용자, 외부 시스템) 사이에 인터페이스와 의존성에 대해 서술되어야 하며, 일반적으로 시스템은 관리적, 물리적 특성을 지닌 비-IT 보안 수단에 의존한다. 이를 위해 CC에서 정의하지 않는 보안 수단과 기능 사이 관리, 의존성을 정의하기 위해 다양한 표준(ISO 17799[21], ISO/IEC 15443[22], IS 18045[23])등을 참조한다.

또한, CC에서는 네트워크로 연결되거나 분산된 시스템에 대한 IT 보안 기능성을 명시하기 위한 지원을 제공하지만, 시스템평가는 인적, 절차적, 공정을 기술적 기능과 메커니즘에 통합시켜 정의된 운영환경에서 수용 가능한 위험등급에 함께 적용하기 위함이다. 따라서, CC에서 정의하지 않는 시스템에서 중요한 측면을 분석해야 한다. 이 중요한 측면은 시스템 내에서의 내부 인터페이스와 시스템 바깥에의 외부 인터페이스 명시가 필요하며, 시스템에서 사용되는 비-IT 정책과 절차를 명시하며, 시스템에 의해 수행되는 기술적인 기능과 물리적인 비-IT 기능을 포함한 보증 평가기준이 필요하다.

전형적으로 시스템평가와 제품평가의 차이점은 시스템평가는 실제적인 운영환경이 완전히 고려되어야 하는 반면에, 제품평가는 운영환경이 세부적으로 명시되지 않아도 되며, 이 운영환경은 평가동안 일반적으로 서술되며 검증되지는 않는다. 그러나, 제품평가는 전체 시스템 평가의 중요한 부분을 차지하며, 평가된 제품은 안전한 시스템을 구축하기 위해 중요하다. 그리고, 시스템의 보안목적은 시스템을 이루는 제품 각각의 기여뿐만 아니라, 이 제품을 지원하는 절차와 형상관리를 정확하게 적용해야 한다. 예를 들어, 업데이트의 부적절한 적용, 보안 설정 값의 정확하지 않은 설정, 또는 접근통제 규칙(예, 파이어월 필터링)의 불완전한 적용은 높은 보증 등급을 갖고 있어도 보안목적을 위반할 것이다.

## 2. 시스템 모델과 개발 환경

복잡한 시스템은 어떤 수의 물리적/논리적 부분을 가질 것이다. 이는 시스템이 한 개 제품의 하나의 기능을 제공하거나, 다양한 기능을 가지는 하나의 제품, 클라이언트 또는 서버로 이루어진 이중 제품, 이중 서버 그리고 클라이언트와 네트워, 여러 개의 클라이언트/서버 등으로 구성될 수 있음을 말한다.

보안정책은 시스템이 하나의 기능을 갖는 드문 경우를 제외하고 위에서처럼 각각의 다른 조합에 따라 다를 것이다. 논리적으로, 같은 보안정책 집합 하에 시스템의 모든 부분은 "domain"의 용어로 표현된다. 기능과 보증 요구사항은 각각의 도메인에 따라 다르며, 각각의 도메인은 자신의 보안정책, 보안환

21) Code of practice for information security management
22) Framework for IT Security Assurance
23) Evaluation Methodology for IT Security

경, 보안목적, 보안요구사항과 보안 특성을 가질 것이다. 그러나, 이 도메인 각각의 정책, 환경, 목적, 요구사항 그리고 특성들은 큰 시스템 레벨의 집합 안에서 운영되기 때문에, 각각의 도메인은 시스템 내에서 요구하는 보증 요구사항을 가질 것이다.

시스템 평가를 위해서는 제품 개발과 달리 개발 단계에서 추가적인 활동이 수행되어야 하며, 시스템 개발과정 단계에서 생성되는 증거를 위해 새로운 문서가 개발되어야 한다.

일반적으로 시스템 개발자와 통합자는 아래와 같은 개발 활동을 해야 한다.

- 개발환경 구축
- 형상 시스템 제공
- ST 제공
- 시스템 레벨의 구조적 설계 문서 제공
- COTS 제품 설치
- 고객 특성에 맞는 매뉴얼을 갖는 응용 패키지, 외부 설계 문서(기본 설계, 기능 설계와 HLD)와 내부 설계 문서(LLD와 구현물)
- 매뉴얼 문서
- 취약성 분석
- 필요한 각각의 컴포넌트 테스트
- 시스템 테스트

## 3. 시스템 평가를 위한 프레임워크

이 문서에서는 아래와 같은 시스템 평가 프레임워크를 제시한다.

• 제품평가와 시스템 평가 차이점

- 제품 평가 : 제품평가는 제품이 적용되어야 하는 운영 환경을 제외하고 수행된다. 즉, 제품이 어떤 특별한 환경에 독립적으로 구현된 보안 능력을 검증하는데 초점을 맞춘다. 제품 평가는 다양한 명세서, 설계 그리고 테스트 문서를 이용해 정확성을 판단을 실증한다.

  제품평가의 주요 목적은 제품이 정확히 구현되었는지에 대한 보증을 얻기 위함이다. 제품 평가의 완성은 시스템 합성을 위해 평가된 제품과 다른 제품(평가되거나 평가되지 않은)과의 적절한 통합이 필요하다. 결국, 시스템이 목적한 보안 속성과 운영 환경에서의 행동을 제공하는지 검증하는 것이다.

  제품 평가로부터 생성된 평가 증거와 평가 보고서는 시스템 통합과 검증 노력을 지원하기 위해 사용될 것이다.

- 시스템 평가 : 시스템 평가는 시스템이 적용되는 특별한 운영환경을 포함한 방법으로 수행된다. 시스템 평가는 시스템에 의해 구현된 IT 수행능력과 함께 운영, 형상 그리고 관리통제에 기초한 비-기술의 정확한 통합을 검증하는데 초점을 맞춘다.

  시스템 평가의 주요 목표는 제품이 정확하게 구현되었는지 IT와 비-IT 보안 능력을 보증하기 위함이며, IT와 비-IT 기능이 통합되어 보안 정책에 따라 운영될 때 잔여 위험 등급을 결정한다. 위험 평가를 통해 수용 가능한 잔여 위험 등급을 결정한다. 위험 평가는 시스템에 의해 부합되기 위한 목표를 수립하며, 시스템 평가는 이 목표가 부합되는지, 부합되지 않는지, 또는 능가하는지를 결정하기 위한 방법이다.

• 시스템 평가 접근법

시스템 평가의 일반적인 접근은 CC모델에 연관해 아래와 같다.

- 보안 위험 평가
  - 보호 해야할 시스템 자산과 위협 그리고 그 자산에 대한 취약성을 결정
  - 조직이 다룰 수 있는 위험 등급 결정
- 보안 문제에 부합하는 시스템의 IT와 비-IT 부분의 보안 목적
- 시스템의 IT와 비-IT 능력에 대한 정의된 구체적이며 접근 가능한 요구사항의 사용
- 위험 내구력에 기초하여 정의된 구체적으로 수용 가능한 보증 요구사항을 정의해 시스템의 IT와 비-IT 능력의 필수 신임 등급을 얻기 위한 수단 결정
- 시스템 ST에 결정사항 기록
- 시스템 개발과 통합
- 시스템 ST에 부합하는지 판단하기 위한 시스템 평가
- 보안 위험 정의와 보안 위험에 부합하는지에 대한 시스템 능력을 주기적으로 고려

• 평가된 제품을 이용한 제품 합성

시스템이 평가를 받을 때 아래와 같은 세 가지 조합 중에 하나로 제품이 합성될 것이다.

- 시스템에 합성되는 데 사용되는 모든 제품은 완전히 평가를 받아야 한다.
- 시스템 합성에 사용되는 어떤 제품은 완전한 평가를 받으며 어떤 제품은 그렇지 않다.
- 시스템의 어떤 제품도 완전한 평가를 받지 않았다.

이 세 가지 경우의 문제는 얼마나 많은 증거가 시스템 평가를 지원 할 수 있느냐는 것이다.

제품이 완전히 평가받았을 때는 제품의 평가결과가 시스템 평가에 유용하게 참조 될 것이다. 제품이 완전히 평가받지 않았을 때는 얼마나 많은 정보가 평가에 지원 가능한지 알지 못한다. 제품이 평가받지 않았을 때는 시스템 평가에 지원 가능한 정보가 없다.

또한, 제품이 완전히 평가받은 경우라도 아래와 같은 이유로 평가 증거가 시스템 평가에서 재 사용되지 않는다.

- 제품 평가 동안 제품의 구성과 시스템에 합성될 때의 제품 구성이 다를 경우, 제품 평가 결과는 시스템 평가에 적절하지 않을 것이다.
- 제품이 평가받은 보증 등급이 시스템의 구성 컴포넌트로 합성될 때 요구되는 제품 보증 등급보다 낮을 경우, 재사용 가능한 증거가 있지만, 새로운 증거가 생성되어야 한다.

• 시스템 평가 보증의 제한

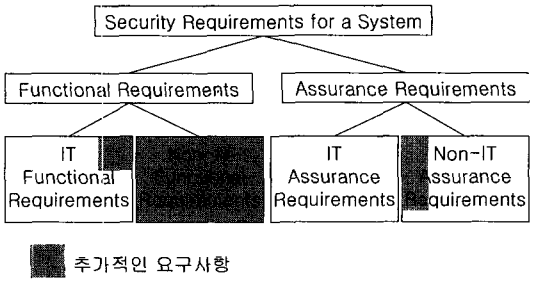
제품이 시스템에 통합 될 때 시스템의 다양성과 성숙도(개발 원리와 설계문서의 가용성에 관련하여) 때문에 시스템 평가에 의해 달성될 수 있는 최대 보증 등급은 제한된다. 시스템 평가의 보증등급은 시스템을 구성하는 컴포넌트의 다양한 보증등급의 최하 등급으로 할당된다. 그러므로 ST 작성자는 적절하게 평가동안 서브시스템에 적용될 수 있는 보증수단 집합에 관련한 도메인 정의를 고려해야 한다.

• 시스템 평가 테스트 시 고려사항

시스템 평가 테스트는 제품 평가에서 존재하지 않은 것을 고려해야 한다. 이는 제품이 시스템 안에서 운영되고 있지 않을 경우다. 이런 제품은 특수한 소프트웨어, 하드웨어, 펌웨어가 안전하게 동작되도록 하기 위해 개발된다. 결국, 시스템 평가의 목적은 시스템의 잔여 위험 등급이 어떤 수립된 위험 경계치 보다 아래에 관리되도록 하기 위한 보안 요구사항과 부합되는지 보증하는 것이다. 시스템 테스트는 이 요구사항이 만족됨을 지원하는 증거를 생성해야 한다.

## 4. 시스템 보안 요구사항

시스템 평가를 위해서는 기존 CC 체계에서 추가적인 보안요구사항이 필요하다.




〔그림 7〕 시스템을 위한 보안 요구사항

위 그림에서 시스템을 위한 기능요구사항은 IT 기능요구사항과 관리/절차적인 수단인 비-IT 기능요구사항이 추가된다.

그리고 보증요구사항은 IT 수단과 관리적/절차적 수단의 조합이 조직의 보안 목적에 부합하기 위해 추가적인 보증 활동이 요구된다.

• 기능 요구사항
- IT : 시스템에 의해 구현된 메커니즘과 서비스 시스템과 외부 환경 사이 인터페이스
- Non-IT : 메커니즘, 서비스, 인터페이스의 형상, 관리, 운영

• 보증 요구사항
- IT : 메커니즘, 서비스, 인터페이스가 정확히 설계, 개발, 구현되고, 테스트되었는지에 대한 검증을 위한 개발 증거
- Non-IT : 형상, 관리, 운영이 정확하며 효과적으로 수행되었는지에 대한 검증을 위한 활동 증거

다시 말해, IT 기능요구사항은 시스템 컴포넌트에 의해 제공되는 메커니즘과 서비스의 보안 능력을 정의하고, 시스템 컴포넌트 사이의 인터페이스와 시스템과 외부 컴포넌트 사이의 인터페이스 정의가 필요하며, 물리적 보호 메커니즘 정의가 필요하다.

비-IT 기능 요구사항은 시스템에 의해 구현된 정책과 절차 정의가 필요하며, IT 보안 능력의 형상 정의가 필요하다.

비-IT 보증요구사항은 CC Part3에서 정의한 요구사항과 TOE의 비-IT부분이 정확하고 효과적인 방법으로 구현되었는지에 대한 검증을 위해 추가적인 보증활동이 필요하다. 또한 모든 비-IT기능 요구사항이 정책과 절차에 부합하는지에 대한 등급을 따로 정의한다.

## V. 결 론

사실 시스템 평가는 매우 어려우며 혹자는 시스템 평가는 "Science" 보다는 "Art" 라고 주장하는 사람도 있다. 국외 보안 선진국들은 CC를 적용해 자국의 평가방법론들을 정립하고 있으며, 표준화도 추진 중에 있다. 향후, 우리나라에서도 ISO/IEC SC27/WG3에 표준화로 제안된 "Security Assessment of Operational System"에 상응하는 시스템 평가지침 및 방법론을 수립하여 국가기간전산망 및 국가주요정보통신 기반시설에 이를 적용함으로써, 시스템의 안정적 운영과 중요 정보에 대한 침해행위를 미연에 방지 할 수 있을 것이다. 또한, 정보통신기반보호법에 명시된 주요정보통신기반시설의 취약점 분석·평가와 CC 체계를 연계해 시스템에 대한 안전성을 보다 확실히 확보 할 수 있을 것이다.

## 참 고 문 헌


[1] Common Criteria for Information Technology Security Evaluation, Part1~Part3, Version2. 1, CCIMB, 1999.

[2] Common Methodology for Information Technology Security Evaluation, Part2, Version 1.0, CCIMB, 1999.

[3] 정보보호시스템 공통평가기준[정보통신부고시 제2002-40호] 2002. 8

[4] 정보보호시스템 평가·인증지침[정보통신부고시 제 2002-41호] 2002. 8

[5] ISO/IEC JTC1/SC 27/WG3 N610, "Security Assessment of Operational Systems" 2003. 4

[6] http://csrc.nist.gov/sec-cert/, Security Certification and Accreditation Project

[7] NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems".

[8] "Assessing the Security of Federal Information Technology Systems", Dr. Ron Ross.

[9] "Composition of Evaluated Components", 1996. 2

[10] http://www2.faa.gov/, The Federal Aviation Administration,

[11] Department Of Defense Computer Security Center. Department of Defense Trusted Computer System Evaluation Criteria, August 1983.

[12] http://www.radium.ncsc.mil/, TTAP(Trust Technology Assessment Program, TPEP (Trusted Product Evaluation Program

[13] http://www.radium.ncsc.mil/, TNI(Trusted Network Interpretation of the TCSEC).

[14] FAA System Security Testing and Evaluation 2003, 5 http://www.mitre.org/, Marshall D. Abrams

[15] FEDERAL AVIATION ADMINISTRATION National Airspace System(NAS) System Protection Profile Template Supplement v1.0.

[16] FEDERAL AVIATION ADMINISTRATION National Airspace System Protection Profile Template Version 1.0 2002. 3.

[17] http://csrc.nist.gov/, NIST SP 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems", NIST SP 800-53, "Minimum Security Controls for Federal Information Technology Systems", NIST SP 800-53A, "Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems".

[18] http://niap.nist.gov/cc-scheme/, CCEVS

[19] http://csrc.nist.gov/cryptval/, CMVP

[20] CESG, http://www.cesg.gov.uk

[21] DCSSI, http://www.ssi.gouv.fr/

[22] CSE, http://www.cse-cst.gc.ca/
[23] IPA, http://www.ipa.go.jp
[24] Composition of Evaluation Components, Howard Holm, 1st ICCC,
[25] Composition - A commercial evaluation view, Julian Straw, 1st ICCC
[26] Composite evaluation and application PP, Brono Baronnet, 2nd ICCC
[27] Engineered Composition for Secure Systems Using the Common Criteria, Shari Galitzer, 2nd ICCC, 3rd ICCC
[28] Trial System Evaluation based on CC/CEM, Haruki Tabuchi, 2nd ICCC
[29] System Evaluation, Patrick Redon, 3rd ICCC
[30] Development of the PP for IT system: multilevel MC&A, A.Shein, 3rd ICCC

## 〈著 者 紹 介〉

**이 경 구 (kounggoo Lee)**

1975년~1982년 2월 : 한양대학교 무기재료공학과(공학사)
1984년~1986년 5월 : University of Central Arkansas 전산학과(이학학사)
1986년~1988년 5월 : University of Central Arkansas 전산학과(이학석사)
1989년~1996년 5월 : Kent State University 전산학과(이학박사)
1996년~현재 : 한국정보보호진흥원(KISA) 근무. 현 산업지원단장

**손 경 호 (kyungho Son)**

2001년 2월 : 성균관대학교 전기전자컴퓨터공학과 공학사
2001년 1월~현재 : 한국정보보호진흥원(KISA) 연구원