CC(Common Criteria) 기반 보안위험분석 도구 개발

Development of CC Based Security Risk Analysis Tool

김 인 중* 정 윤 정** 고 재 영*** 원 동 호****
InJung Kim YoonJung Chung JaeYoung Koh Dongho Won

요 약

정보화 발전으로 정보통신 시스템에 대한 의존도가 높아지고, 이에 대한 위협, 취약성, 위험이 증가하고, 조직의 정보노출 및 보안침해 사고가 증가하고 있는 추세이다. 이러한 정보통신시스템에 대한 위협, 취약성, 위험을 분석하고 제거하기 위한 보안위험분석의 중요성이 부각되고 있다. 위험분석도구는 조직에 내재한 위험을 식별하여 보안침해 사고 발생을 사전에 예방하기 위한 도구로서 주요 정보시스템을 분석·평가하고, 위협, 취약성, 보안대책을 제시하여 조직의 위험 수준을 감소하는데 도움을 준다. 본 논문은 국제공통평가기준 CC 스키마를 도입하여 정형화된 위험분석 프로세스를 정의하고, 정보보안 관리자가 쉽게 위험분석을 적용 할 수 있도록 보안위험분석 도구를 제안한다.

Abstract

The importance of the Security Risk Analysis has emerged as security breaches and information leaks has occurred in the companies and organization; threats toward information system and its vulnerabilities has grown up as the dependence on the information-communication systems goes higher as a result of technological advances in IT industry. A Risk Analysis Tool helps to mitigate overall risk of an organization by analysing and evaluating critical information systems and providing security measures against threats to systems and its vulnerabilities as a means to identify the inherent dangers and prevent security intrusion incident.

This paper defines risk analysis process by introducing Common Criteria Scheme and suggest a risk analysis tool that can be easily implemented by an information security manager.

☞ Keyword : Risk Analysis, Asset, Threat, Vulnerability, Safeguard

1. 서 론

현재 정보보안 분야는 기존의 보안기술 중심 패러다임에서 보안관리의 중요성이 점차 부각하고 있다. 정보보안 분야의 지금까지 3단계의 발전과정으로 구분할 수가 있다. 첫 단계는 80년대 초반까지의 기술적 물결(technical wave)로 메인프레임 중심의 운영체제에 구현된 보안기술에 중점을 두었고, TCSEC, ITSEC, CC와 같이 보안기능에 대한 기술적 평가를 위주로 하는 보안 제품 및 시스템에 대한 평가방법론이 나타났다.[1-3] 두 번째 단계는 80년대 중반에서 90년대 중반까지의 관리적 물결로서 분산화 및 네트워크화라는 정보시스템의 기술적 환경의 변화에 따른 보안 관리의 중요성이 대두되었으며, 보안정책 및 관리 조직의 정립과 같은 이슈들이 체크리스트 또는 실무규범의 형태로 다루어졌다. 세 번째는 90년대 중반 이후의 조직화 물결로 정보보안 관리체계의 수립 및 운영에 대한 인증, 정보보안을 조직 문화의 일부분으로 정착하고, 능동적이고 지속적인 정보보안 수준의 측정으로 특징지을 수 있다. 이러한 흐름을 반영하여 ISO 13335 GMITS (Guideline for Management of Information Tech-

* 정 회 원 : 국가보안기술연구소 전임연구원
cipher@etri.re.kr
** 정 회 원 : 국가보안기술연구소 선임연구원
yjjung@etri.re.kr
*** 정 회 원 : 국가보안기술연구소 책임연구원
jykoh@etri.re.kr
**** 정 회 원 : 성균관대학교 정보통신공학부 교수
dhwon@security.re.kr
[2005/08/09 투고 - 2005/09/16 심사 - 2005/09/29 심사완료]

nology Security), BS7799의 정보보안관리체계(Information Security Management System), 시스템보안공학-능력성숙도모델(System Security Engineering-Capability Maturity Model) 등의 보안관리 프레임워크가 개발되었다.[5,6,11,12]

이러한 변화 속에서 2001년 7월 정보통신기반보호법이 시행됨으로써 국가사회적으로 중요한 시스템을 주요정보통신기반시설로 지정하고, 이를 운영하는 기관은 주기적인 취약점 분석·평가 수행을 강제화하고 있다. 또한 전 국민은 2003년 1.25 대란을 통한 국가기간망의 마비와 서비스 단절로 인하여 정보통신보안의 중요성이 더욱 고조되었다. 그러므로 정보시스템을 운영하는 조직에서는 정보보안을 강화시키기 위한 기술적인 취약점 분석[10], 체계적인 보안관리를 수행하기 위한 방법[13-15]들이 요구되어지고, 산학연에서 많은 연구가 이루어지고 있다. 아직까지 국내는 조직에서 정보보안 전담인력이 부족한 상태이기 때문에 많은 위험관리 방법 중에서 각 기관이나 조직에 적합한 방법들을 채택하고, 평가를 수행하기는 어려운 현실이다. 그러므로 보안위험분석을 사용자가 사용하기 편하고 이해하기 쉽도록 방법을 제시하고 이를 지원하기 위한 도구가 필요하다.

따라서 본 논문은 정형화된 위험분석 프로세스를 정의하기 위하여 국제공통평가기준인 CC 2.0을 기반으로 보안위험분석 프로세스를 정의하고, 보안위험분석을 수행하기 용이하도록 보안위험분석 도구를 제시한다.

2. 관련 연구

본 장은 여러 위험분석 방법론들 중에서 가장 널리 알려진 주요 위험 분석 방법론에 대하여 기술한다.

2.1 ISO/IEC SC27-GMITS

GMITS는 ISO/IEC의 국제표준으로 IT 보안 관리측면에 관한 솔루션이 아닌 지침서를 제공하고 있다. GMITS는 5개 Part로 구성되어 있다. Part 1은 기본 개념과 IT 보안관리를 기술하는데 사용되는 모델의 전체 개요를 제공하고, Part 2는 관리와 계획 측면을 기술하며, Part 3은 프로젝트 수명 주기 동안 관리활동에 적절한 보안 기법들을 기술한다. Part 4는 보안대책 선정에 관한 지침 제공과 베이스라인 모델 및 통제를 통한 지원과정을 기술하고, Part 5는 IT 시스템과 외부 네트워크를 연결하는 조직에 대한 지침을 제공한다.

2.2. OCTAVE

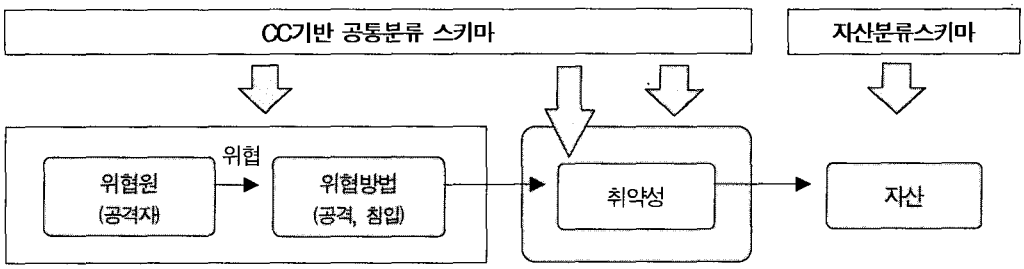
OCTAVE(Operationally Critical Threat, Assets and Vulnerability Evaluation)는 미국의 CMU SEI (Carnegie Mellon University Software Engineering Institute)에서 개발한 위험분석 방법론으로, 조직이 그들의 정보보안 위험을 식별하고 관리하기 위한 자가 활동을 정의하였다.[4] OCTAVE 프레임워크의 평가는 포괄적이며 조직의 사명에 중요한 자산, 자산에 대한 위협, 위협에 노출될 수 있는 정보자산의 취약점을 식별하는 것을 가능하게 한다.

OCTAVE는 기업이 필요로 하는 정보보안의 포괄적 그림을 구성하기 위해 조직적 이슈와 기술적 이슈 모두를 검토하고 전체적으로 3단계로 구성된다.

- 단계 1 : 전사적 보안 요구사항 구축
- 단계 2 : 기반구조 취약점 식별
- 단계 3 : 보안 위험관리 전략 결정

2.3 CSE 위험관리 방법론

CSE(Canadian Security Establishment)의 위험평가 수행지침은 캐나다의 정부 부서와 기관에서 필수적으로 요구되는 보안 위험 관리를 위한 것으로 개발되었다.[7] 위험 관리는 해당 영역에서 수용할 위험을 가진 자원을 확인하기 위하여 계획, 조직, 지휘, 통제하는 활동과 관련되어 있다. 그러나 현재의 모든 위협으로부터 자산을 보호하는 것이 아니라 위험의 정도에 따라서 위협과 취약점을 분석하고 비용 효과적인 보안대책을 선택하는 방법을 활용한다. 이러한 위험관리를 위한 선택사항으로는 위험의 전이, 회피, 수용 또는 위험 감소가 있다. 위험감소는 운영적, 절차적, 물리적, 인간적, 기술적 보안을 관리하기 위한 시스템의 구현을 통해서 이



〈그림 1〉 공통 분류기준에 의한 위험분석모델

루어진다. CSE의 위협과 위험 평가지침은 9개의 주요 항목과 46개의 단계와 관련된 세부적인 내용들로 구성되어 진다.

2.4 CRAMM

CRAMM(CCTA Risk Analysis and Management Method)은 1985년 영국의 CCTA와 BIS사에 의해서 개발된 정성적 위험분석 방법론이다.[9] 이 방법론은 영국의 정보시스템 보안위원회가 요구하는 13가지 필수 요구사항을 반영하기 위한 필요성에 의해 방법론을 개발하였다. 즉, 필수 요구사항을 위험분석 방법론이 반드시 갖추도록 요구하고 있다. CRAMM은 자동화 도구가 개발되어 현재 20개국 230여 기관에서 활용하고 있다.

3. CC 기반 위험분석 방법론 제안

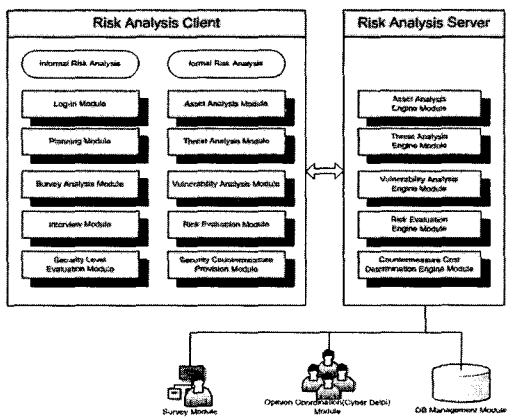
제안하는 위험분석 방법론은 정보보호 시스템 평가기준과 평가기술로써 국제공통평가기준(CC : Common Criteria 2.0)을 수용한다. 기존의 위험분석 방법들은 위협, 취약성 및 보호대책에 대한 분류체계가 다르고 체계적이지 못하기 때문에, 위협, 취약성 및 보호대책 파악이 매우 주관적이고 애매하며 중복되는 경향이 존재하였다. 따라서 국제공통평가기준(CC)의 기능요구사항 스키마를 위험분석에 공통적으로 적용하여, CC의 기능요구사항을 대응책으로 보고 위협 분류기준과 취약성 분류기준 및 보호대책 분류기준을 모두 동일하게 정의를 하였다. 그림 1은 국제공통분류기준에 의거한 위험분석 모델을 표현한 것이다.

3.1 CC 기반 프로세스 정의

공통 분류기준에 의한 위험분석모델을 적용한 위험분석 방법론은 표 1과 같이 3개의 클래스와 11개의 패밀리, 21개의 컴포넌트, 2개의 엘리먼트로 구성되며, 위험분석을 위한 사전 준비작업을 실시하고 이에 따라 본격적인 자산평가, 위협평가 및 취약성 평가를 수행하여 최종적으로 위험평가를 수행하고 이를 통해 도출된 내용에 따라 보안대책을 제시하는 순서로 이루어진다.

4. 제안하는 위험분석도구 구성

제안하는 위험분석도구는 평가대상기관의 위험을 평가하기 위하여 준비단계에서부터 보안대책 제시까지의 6단계 프로세스를 기반으로 하다. 위험분석 자동화를 지원하기 위한 도구로 전체 시스템 구조도[8]는 그림 2와 같다.



〈그림 2〉 위험분석도구 전체 구성

〈표 1〉 CC 기반 위험분석 방법 프로세스

Class	Family	Component	Element
P1 계획수립 및 상위수준 위험분석	P1.1 예비조사	1.1.1 예비조사 팀 구성	
		1.1.2 조직 일반현황 파악	
		1.1.3 정보시스템 현황 파악	
		1.1.4 단위시스템 구분	
	P1.3 상위수준 위험분석	1.2.1 팀 구성 및 참여자 선정	
		1.2.2 평가대상기관 인터뷰	
		1.2.3 위험수준평가	1.2.3.1 점검 실시
			1.2.3.2 결과 분석
	P1.4 하위수준 위험분석 계획	1.3.1 위험분석 범위 결정	
		1.3.2 분석팀 구성	
		1.3.3 분석일정 수립	
P2 하위수준 위험분석	P2.1 자산 평가	2.1.1 자산 파악	
		2.1.2 임계자산 선택	
		2.1.3 임계자산 평가	
	P2.2 기존/계획된 보안 통제 식별		
	P2.3 위협 평가	2.3.1 위협 파악	
		2.3.2 위협 선택	
		2.3.3 위협 평가	
	P2.4 취약성 평가	2.4.1 취약성 파악	
		2.4.2 취약성 선택	
		2.4.3 취약성 평가	
	P2.5 위험 평가	2.5.1 위험수준 평가	
		2.5.2 위험수준 평가결과 검토	
P3 보안대책 선택	P3.1 보안대책 목록화		
	P3.2 보안대책 우선순위 결정		
	P3.3 보안대책 목록 제시		

제안하는 위험분석도구는 도구 클라이언트와 서버로 구성되고, 각 시스템별 모듈들의 세부 기능들은 다음과 같다.

4.1 도구 클라이언트

4.1.1. 상위수준 분석(Informal Analysis)

· 로그인 모듈 : 사용자에 대한 아이디와 패스워드를 입력받아 사용자를 인증하는 기능을 수행하며, 인증된 사용자의 역할에 따라 수행할 수 있는 기능이 제한되는 역할기반 접근통제 기능 제공

· 가이드라인 모듈 : 위험분석 활동에 필요한 활동 가이드라인 및 평가기준 가이드라인 제공

· 인터뷰 모듈 : 평가대상기관에 대한 인터뷰 내용을 입력, 저장 및 출력하는 기능 수행

· 계획수립 모듈 : 위험분석 계획수립을 위한 기능을 제공하고, 위험분석 평가자와 참여자 구성 및 일정을 관리

· 위험수준평가 모듈 : 평가대상기관에 대한 위험수준평가를 위한 설문내역 출력 및 결과 저장과 통계치 출력 기능 수행

4.1.2. 하위수준 분석(Formal Analysis)

· 자산평가 모듈 : 평가대상기관의 자산파악 및 우선순위화, 임계자산 선택, 임계자산에 대한 기존 보안대책 파악 및 임계자산평가 기능 수행

· 위협평가 모듈 : 평가대상기관의 임계자산별 위협 파악, 임계자산에 대한 위협 선택 및 임계자산에 대한 위협평가 기능 수행

· 취약성평가 모듈 : 평가대상기관의 임계자산별 선택된 위협에 대한 취약성 파악, 취약성 선택 및 취약성평가 기능 수행

· 위험평가 모듈 : 평가대상기관의 위험수준 평가 및 평가결과 검토 기능 수행

· 보안대책 제시 모듈 : 평가대상기관의 보안대책 파악, 보안대책 선택 및 목록화, 보안대책 검토 기능 수행

4.2 도구 서버

· 데이터보안 모듈 : 데이터 처리나 인증과 같은 보안기능 수행

· DB 관리 모듈 : 처리되는 데이터를 DB에 저장하거나 읽어오는 기능 수행

· 감사로그 모듈 : 보안감사를 위한 사용자들의 각종 정보를 로그로 기록하고 관리하는 기능 수행

· 자산평가엔진 모듈 : 자산평가를 위한 평가엔진을 제공하며, 자산평가 모듈 수행시 임계자산평가를 위한 알고리즘 수행

· 위협평가엔진 모듈 : 위협평가를 위한 평가엔진을 제공하며, 위협평가 모듈 수행시 위협평가를 위한 알고리즘 수행

· 취약성평가엔진 모듈 : 취약성평가를 위한 평가엔진을 제공하며, 취약성평가 모듈 수행시 취약성평가를 위한 알고리즘 수행

· 위험평가엔진 모듈 : 위험평가를 위한 평가엔진을 제공하며, 위험평가 모듈 수행시 위험수준 평가를 위한 알고리즘 수행

· 보안대책분석엔진 모듈 : 보안대책 분석을 위한 평가엔진을 제공하며, 보안대책제시 모듈 수행시 보안대책 파악을 위한 알고리즘 수행

5. 위험분석도구 결과화면

5.1 자산 프로파일

· 자산을 대분류, 중분류, 소분류로 입력

· 자산에 대한 명칭, 도입일자, 버전, 제조회사, 도입비용, 관리책임자 입력

· 자산에 대한 자세한 설명을 입력하고, 자산 목록을 제시

· 해당 자산을 클릭할 때, 입력 폼에 해당 자산의 정보가 나타나고 수정 가능

5.2 위협 프로파일

· 위협문장을 위협원, 동기, 대상, 영향을 선택하여 위협문장 생성

· 위협에 대한 구체적인 설명 입력과 근거 작성

· 위협이 해당 시스템에서 실현될 경우의 손실가치 입력

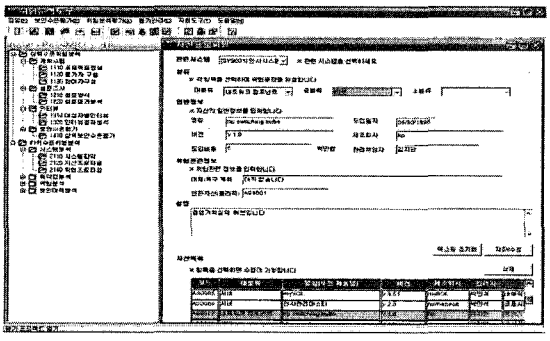
· 위협의 연간 발생빈도 입력하고, 위협 정보 저장/수정

· 입력한 위협 리스트를 제시

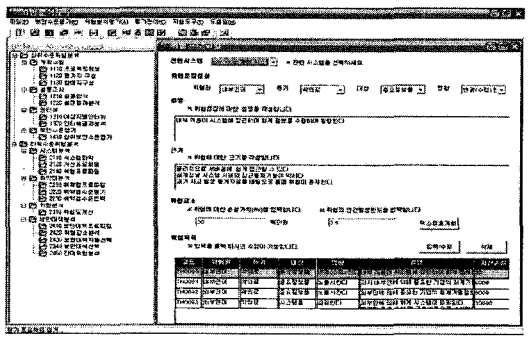
· 해당 위협을 클릭할 때, 입력 폼에 위협의 정보가 나타나고 수정 가능

5.3 취약점 프로파일

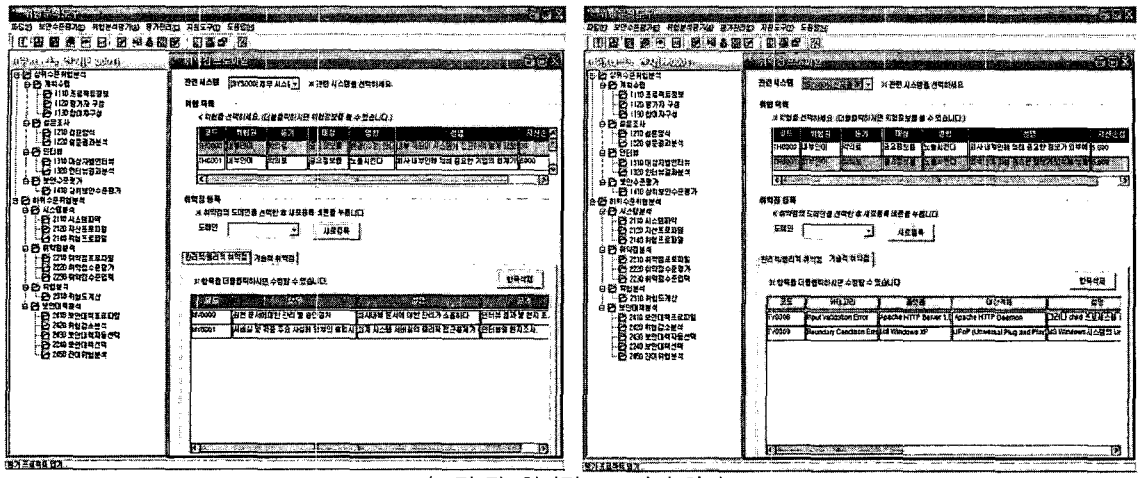
· 평가대상 위협목록에서 취약점을 입력할 위협 선택



〈그림 3〉 자산 프로파일 화면



〈그림 4〉 위협 프로파일 화면



〈그림 5〉 취약점 프로파일 화면

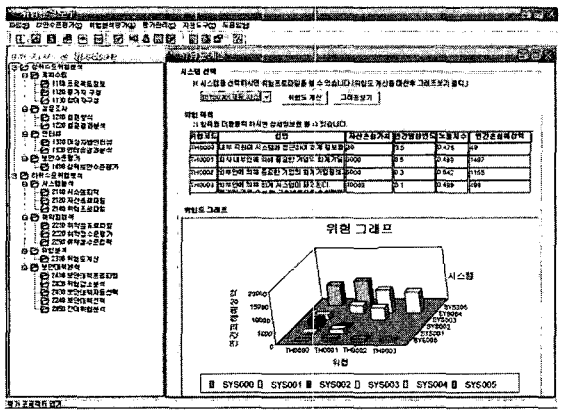
· 물리적/관리적 취약점, 기술적 취약점 중 도메인을 선택하여 추가등록 버튼을 이용하여 취약점 입력

· 선택하는 취약점 도메인에 따라 취약점 목록 변경

· 선택한 취약점을 삭제하고, 입력한 취약점 목록을 보여줌

5.4 위험도 산정

· 자산을 선택 후 위험도 계산을 수행하면 해당 시스템의 모든 위협의 노출지수 및 연간손실예상액이 입력되어 위협목록 화면 출력



〈그림 6〉 위험도 계산 화면

· 평가 대상기관 시스템 전체의 위험 그래프를 화면 출력

· 해당하는 시스템을 클릭하면 상세위험정보를 보여줌

6. 결 론

본 논문은 국제공통평가기준 CC 2.0 기반 정형화된 보안위험분석 프로세스를 정의하고, 보안위험관리 수행을 지원하기 위한 위험분석도구를 제시하였다. 또한 위험분석도구에서 각 모듈별 정의를 하고, 세부기능을 제시하였다. 제안한 도구를 활용하여 정보시스템에 대한 위협, 취약성을 분석하고, 정보시스템 가치를 고려하여 위험도를 평가가 가능하다. 또한 위험을 제거, 수용 또는 회피하기 위한 대책을 제시함으로써 궁극적으로 안전한 정보시스템 운영환경을 구축을 가능하게 한다. 현재 몇 개의 Case study를 진행한 상태이고, 보안위험분석에 대한 결과를 검토하고 있다. 국내에서 개발한 보안위험관리 도구는 1996년 한국전산원의 Hawk와 펜타 시큐리티의 위험분석도구가 있었지만, 현재는 사용하지 않는다. 제안한 위험분석 도구에 대한 많은 시험을 통하여 사용자가 쉽게 활용이 가능하고, 그 결과에 대한 신뢰가 검증이 되어 국내·외에 널리 사용되기를 기대한다.

향후 이 도구를 활용한 보안위험분석 결과에 대

한 신뢰성을 검증하기 위한 방법을 연구하고, 좀 더 많은 Case Study 연구를 진행할 예정이다.

참 고 문 헌

[1] CC, "Common Criteria for Information Technology Security Evaluation", Version 2.1, CCIMB-99-031, August 1999, http://www. commoncriteria.org/site_index.html.

[2] DoD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)", Dec. 1985.

[3] European Community, "Information Technology Security Evaluation Criteria(ITSEC)", Ver. 1.2, June 1991. (http://www.cesg.gov.uk /assurance/ iacs/itsec/index.htm)

[4] OCTAVE, "OCATVE Criteria, Version 2.0", Carnegie Mellon Software Engineering Institute (2001. 12), OCATVE Method Implementation Guide Version 2.0, OCTAVE, 2001. 6, http:// www.sei.cmu.edu/publications/ pubweb.html.

[5] SSE-CMM, "Project, Systems Security Engineering Capability Maturity Model(SSE-CMM) - Model Description Document", V.2, http:// www.sse-cmm.org, 1999. 4. 1.

[6] British Standards Institution(BSI), BS-7799, 1999.

[7] CSE, "A Guide to Security Risk Management for IT Systems", Government of Canada, Communications Security Establishment (CSE)", 1996.

[8] Hoh Peter In, Young-Gab Kim, Taek Lee, Chang-Joo Moon, Yoonjung Jung, Injung Kim, "Security Risk Analysis Model for Information Systems," LNCS 3398, Systems Modeling and Simulation: Theory and Applications: Third Asian Simulation Conference, AsianSim 2004.

[9] CRAMM, "A Practitioner's View of CRAMM", http://www.gammassl.co.uk/.

[10] Young-Hwan Bang, YoonJung Jung, Injung Kim, Namhoon Lee, GangSoo Lee, "Design and Development of a Risk Analysis Automatic Tool," ICCSA2004, LNCS 3043, pp.491-499, 2004.

[11] ISO/IEC TR 13335, 1부, "IT보안 개념 및 모델"(1996), 2부 "보안관리 및 계획"(1997).

[12] ISO/IEC TR 13335, 3부, "IT 보안관리 지침", 1998.

[13] InJung Kim, YoonJung Chung, YoungGyo Lee, Dongho Won, "A Time-Variant Risk Analysis and Damage Estimation for Large-Scale Network Systems," ICCSA2005, LNCS 3043, May 2005.

[14] Injung Kim, YoonJung Jung, JoongGil Park, Dongho Won, "A Study on Security Risk Modeling over Information and Communication Infrastructure," SAM04, pp. 249-253, 2004.

◐ 저 자 소 개 ◑

김 인 중 (InJung Kim)
1990년 충남대학교 전자공학과 졸업(학사)
1992년 충남대학교 대학원 전자공학과 졸업(석사)
2001년~2005년 성균관대학교 대학원 전기전자및컴퓨터공학부 졸업(박사)
1992년~2000년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 전임연구원
관심분야 : 위험분석, 취약점분석, 암호기술
E-mail : cipher@etri.re.kr

정 윤 정 (YoonJung Chung)
1997년 성균관대학교 정보공학과 졸업(학사)
1999년 성균관대학교 대학원 정보공학과 졸업(석사)
1999년 하나로정보통신 연구원
2000년~현재 국가보안기술연구소 선임연구원
관심분야 : 정보보안, 네트워크 보안, 위험분석
E-mail : yjjung@etri.re.kr

고 재 영 (JaeYoung Koh)
1998년 전북대학교 전자공학과 졸업(박사)
1984년~2000년 국방과학연구소 선임연구원
2000년~현재 국가보안기술연구소 책임연구원
2004년~2005년 국가정보보안협의회 사무국장
관심분야 : 정보보안, 전산망보안, 보안정책
E-mail : jykoh@etri.re.kr

원 동 호 (Dongho Won)
1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신 연구원 전임연구원
1988년~2003년 : 성균관대학교 교학처장, 전기전자및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 인증기술 연구센터(정통부지정 ITRC) 센터장
관심분야 : 암호이론, 정보이론, 정보보안관리
E-mail : dhwon@security.re.kr