NSA IDS System PP와 국가기관용 IDS PP 가정사항 비교분석

김 남 기* · 박 종 오* · 김 지 영*

요 약

보호프로파일은(Protection Profile)은 특정형태의 제품군이 지녀야 할 보안 목적을 사용자 그룹에서 요구한 명세서이며 보호프로파일의 가정사항은 TOE(Target Of Evaluation)의 물리적, 인적, 네트워크적 관점을 포함하는 사용 환경과 TOE의 사용제한, 잠재적인 자산 가치, 추가적인 적용의 관점을 포함하는 TOE 사용 방법상의 내용을 기술한 것이다.

본 논문에서는 NSA(National Security Agency) 침입탐지 시스템 시스템 보호프로파일과 국가기관용 침입탐지 시스템 보호프로파일의 가정사항 항목을 비교 분석하였다.

Comparison & Analysis of Intrusion Detection System System Protection Profile of NSA and MIC

Nam Ki Kim* · Jong Oh Park* · Ji Yeong Kim*

ABSTRACT

A protection profile is the required specification document by consumer groups to specify what security purpose they would like to have in their specialized products. A protection profile assumption is the document that specifies consumer environment in the physical, artificial, network perspective and the contents of intended usage which include usage limitation, the value of latent asset, and additional applications for a TOE (Target of Evaluation).

In this Paper, we compare the assumptions of the NSA IDS PP and the IDS PP for government.

* 경기대학교 정보통신대학원

1. 서 론

정보보호 시스템을 평가하기 위한 기준은 1985년 미국에서 제정한 정보보호 시스템 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)을 기반으로 영국, 독일, 프랑스, 캐나다 등 정보보호 선진국들에 의해 자국에 맞는 평가 기준을 계속적으로 제정해 왔다. 1990년 ISO에 의해 전 세계 정보기술 시장에서도 표준화된 보안 평가 결과로 인정될 수 있도록 하기 위한 공통평가 기준을 만들기 위해 1993년 6월 CTPEC, FC, TCSEC, ITSEC 작성자들이 단일의 국제 공통평가 기준 CC(Common Criteria)를 만들기 위해 프로젝트를 시작하였고, CC는 크게 제1부 일반모델, 제2부 보안 기능 요구사항, 제3부 보증요구사항으로 분류된다. 보호프로파일(Protection Profile)은 일반사용자가 이해하는데 용이하게 하기위해 공통평가 기준의 제2부와 제3부로부터 TOE (Target of Evaluation)의 보안목적을 만족시키는 요구사항을 식별하기 위해 문서화 한 것이다.

본 논문은 2장에서는 국내외 정보보호 시스템 평가 기준의 변화와 국제적인 정보보호 시스템 평가표준인 국제 공통 평가 기준에 대해 알아보고, 3장에서는 공통평가 기준의 산출물인 보호프로파일의 개념과 구성을, 4장에서는 NSA IDS System PP(National Security Agency, Intrusion Detection System System Protection Profile)와 국가기관용 IDS PP의 가정사항을 유형별로 분류하여 분석 및 비교하고, 5장에서 결론을 제시하고자 한다.

2. 국내·외 정보보호 시스템 평가 기준

2.1 국내의 정보보호 시스템 평가 기준

국내에서는 1996년에 제정된 정보화촉진기본법 및 동법 시행령에 근거하여 국내 정보보호 시스템에 대한 평가 제도가 마련되었다. 1998년 2월 침입차단 시스템에 대한 평가 기준이 고시되었고 2000년 2월 개정·고시되었으며 2000년 7월에 침입탐지 시스템 대한 평가 기준이 고시되었다[4-5].

현재 이 평가 기준의 근간이 되는 정보보호 시스템 평가 제도의 뜻은 "정보보호 시스템을 일반 사용자가 안전하게 사용할 수 있도록 제품의 신뢰성을 보증하기 위한 법적 제도 및 기술체계"이다.

국내 침입탐지 시스템에 대한 평가는 K1, K2, K3, K4, K5, K6, K7의 7등급으로 구분되며 K1이 최저 등급이며 K7은 최고 등급이다. 평가등급의 요구사항에 적합하지 않은 등급은 K0이다.

현재 국내 침입탐지 시스템 제품의 경우 <표 1>에서 같이 평가 완료된 제품이 16건, 평가진행중인 제품이 6건이 있다.

2.2 국외의 정보보호 시스템 평가 기준

국내에서의 침입탐지 시스템과 침입차단 시스템의 평가를 위한 기준이 발표되기 이전에 이미 선진 각국에서는 정보보호 시스템의 성능과 신뢰도를 평가하기 위한 노력의 일환으로 자국의 실정에 맞는 평가 기준을 제정하여 시행하고 있다.

미국에서는 오렌지 북(Orange book)으로 불리는 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)을 1985년에 제정하였으며, 이후 영국의 그린 북(Green Book)시리즈, 독일의 블루 & 화이트 북(Blue & White Book), 프랑스의 블루-화이트-레드 북(Blue-White-Red Book)등이 계속적으로 제정되면서 1990년에 영국, 독일, 프랑스, 네덜란드가 협력하여 유럽의 공통적인 평가 기준서인 ITSEC(Information Technology Security Criteria)을 산출하였다. 1991년에는 캐나다에서 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)이라는

〈표 1〉 국내 IDS 제품 평가 현황

	제 품 명	개 발 사	평가등급	인 증 일
평가 완료 제품	Siren 3.0	펜타시큐리티 시스템(주)	K4	2001년 9월 18일
	NeoWatcher@ESM Package V3.0	(주)인젠	K4	2001년 9월 18일
	Netspecter V1.2	넷시큐어테크놀러지(주)	K4	2001년 10월 26일
	TESS/TSN V2.0	(주)정보보호기술	K4	2002년 2월 8일
	Sniper v2.0	(주)윈스테크넷	K4	2002년 2월 8일
	SecuRadar v1.0	(주)데이타게이트 인터내셔널	K4	2002년 2월 8일
	Secuve IDS 2.0	(주)시큐브	K4	2002년 3월 26일
	수호신 IDS V1.0	(주)시큐어소프트	K4	2002년 7월 4일
	SafezoneNet V3.0	LG엔시스(주)	K4	2002년 7월 4일
	대정스핑크스 Ver2.0	(주)대정아이앤씨	K4	2002년 8월 12일
	Sniper v2.0L	(주)윈스테크넷	K2	2002년 8월 12일
	Cypollo-N v1.1	(주)조은시큐리티	K4	2002년 9월 18일
	NPol V1.3	(주)디엠디	K4	2002년 9월 18일
	NeoGuard@ESM Package V3.0	(주)인젠	K4	2003년 1월 8일
	Siren 3.0(for IBM)	펜타시큐리티 시스템(주)	K4	2003년 3월 25일
	Siren 3.0(Solaris 9)	펜타시큐리티 시스템(주)	K4	2003년 4월 16일
평가 진행 제품	SafezoneHost V2.0	LG 엔시스(주)	K4	2002년 6월 24일 계약
	TESS V3.5	(주)정보보호기술	K4	2003년 2월 4일 계약
	수호신 Absolute 400-IDS(V1.0)	(주)시큐어소프트	K4	2003년 2월 11일 계약
	수호신 Absolute 1000-IDS(V1.0)	(주)시큐어소프트	K4	2003년 2월 11일 계약
	Sniper v3.0	(주)윈스테크넷	K4	2003년 2월 20일 계약
	Sniper v3.0L	(주)윈스테크넷	K2	2003년 2월 20일 계약

평가 기준을 제정하였다. 한편 미국의 NIST(National Institute for Science and Technology)와 NSA(National Security Agency)는 1993년 1월에 합작으로 향후 TCSEC을 대체할 평가 기준서로 FC(Federal Criteria)를 배포하였다[5].

2.3 공통평가 기준(CC : Common Criteria)

1990년 ISO는 일반적인 사용을 위해 국제 표준 평가 기준을 개발하려는 작업을 시작하였다. 새로운 기준이 전 세계 정보기술 시장에서도 표준화된 보안 평가 결과로 인정될 수 있도록 상호 이해를 위한 요구를 충족시킬 필요가 있었다. 이와 관련된 작업들은 ISO/IEC/TC1/C27/WG3에 할당되었다. 1993년 6월에 CTPEC, FC, TCSEC, ITSEC 작성자들이 단일의 국제 공통 평가 기준 CC(Common Criteria)을 만들기 위한 프로젝트를 시작하여 1996년 1월에 버전 1.0을 발표하였으며 현재 버전 2.0이 ISO/IEC의 국제표준으로 승인된 상태이다. 평가 혹은 인증 체계를 갖추고 평가를 시행해오던 선진 국가들은 이미 CC체계로의 전환을 위하여 자국의 체계에 맞도록 준비해 왔으며 미국은 NIAP(National Information Assurance Partnership)을 1997년 8월에 구성하여 국제 공통 평가 기준 평가/인증 체계와 평가기관 인정 프로그램을 개발하고 있다.

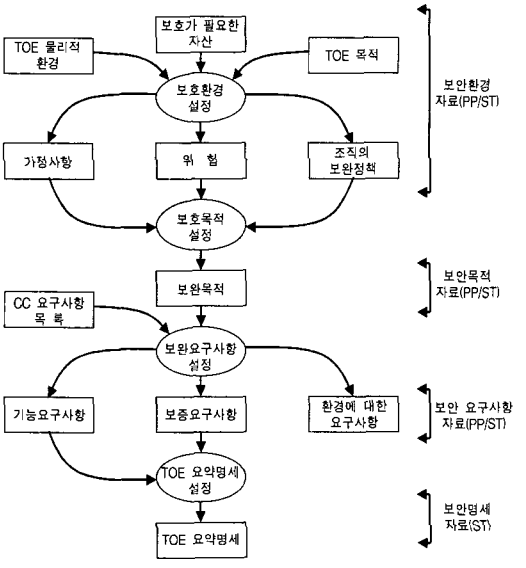
국내의 경우 2002년 8월 정보화촉진기본법 제

15조 제1항의 규정에 의거 정보보호 시스템 공통평가 기준을 고시하였다[6].

3. 보호프로파일(PP : Protection Profile)

3.1 보호프로파일 개념

국제 공통 평가 기준은 국내의 침입차단 시스템이나 침입탐지 시스템 평가 기준과는 달리 특정 유형의 정보보호 시스템 평가 기준이 아니며, 모든 정보보호 시스템 유형을 포괄할 수 있는 보안 요구사항을 제시한 것이다. 국제 공통 평가 기준에 따르면 보호프로파일은 특정 사용자들(일반사용자, 정부기관, 기업체)의 보안 문제를 다루기 위하여 국제 공통 평가 기준 보안기능 및 보증요구사항이나 국제 공통 평가 기준에 포함되어 있지 않은 별도의 보안 요구사항에 근거하여 구현 독립적인 집합이라고 정의하고 있다. 이러한 요구사항들은 공통평가 기준의 제2부와 제3부로부터 TOE의 보안목적을 만족시키는 요구사항으로서 식별되며 공통평가 기준의 내용으로 일반사용자가 이해하는데 용이한 문서가 되어야 한다. 보안 요구사항의 도출은 TOE의 용도와 보안환경으로 도출된다. (그림 1)은 보안 요구사항의 도출 과정이다.



(그림 1) 보안 요구사항의 도출

3.2 보호프로파일 구성

보호프로파일의 구성은 다음의 <표 2>와 같다.

〈표 2〉 보호프로파일 구성

1	보호프로파일소개(PP Introduction) 1.1 보호프로파일 식별(PP Identification) 1.2 보호프로파일 개요(PP Overview)
2	TOE 설명(TOE Description)
3	TOE 보안환경(TOE Security Environment) 3.1 가정사항(Assumptions) 3.2 위협(Threats) 3.3 조직의 보안정책(Organisational Security Policy)
4	보안목적Security Objectives) 4.1 TOE 보안목적(Security Objectives for the TOE) 4.2 환경에 대한 보안목적(Security Objectives for the Environment)
5	IT 보안 요구사항(IT Security Requirements) 5.1 TOE 보안 기능 요구사항(TOE Security Functional Requirements) 5.2 TOE 보증 요구사항(TOE Security Assurance Requirements) 5.3 IT 환경에 대한 보안 요구사항(Security Requirements for the IT Environments)
6	(보호프로파일 응용시 주의사항 (PP Application Notes)
7	이론적 근거(Rationale) 7.1 보안목적의 이론적 근거 (Security Objectives Rationale) 7.2 보안 요구사항의 이론적 근거 (Security Requirements Rationale)

3.2.1 보호프로파일 소개

보호프로파일 소개 부분은 보호프로파일이 다루고자 하는 TOE를 명시하고 보호프로파일을 요

약 서술한다. 또한 기존에 평가된 보호프로파일 목록 및 보호프로파일 등록상태를 서술할 수 있다.

3.2.2 TOE 설명

TOE 설명은 TOE의 일반적인 정보를 제공하며 TOE의 기능을 제공하고 범위에 대해 선택사항으로 설명할 수 있다. 또한 TOE의 사용 목적을 제공한다.

3.2.3 TOE 보안환경

TOE 보안환경은 가정사항, 위협, 조직의 보안정책으로 구성된다.

(1) 가정사항(Assumptions)

가정사항은 TOE의 물리적, 인적, 네트워크적 관점을 포함하는 사용 환경과 TOE의 사용제한, 잠재적인 자산 가치, 추가적인 적용의 관점을 포함하는 TOE 사용 방법상의 내용을 기술한다.

(2) 위협(Threats)

위협은 TOE나 TOE가 설치된 환경 내에 존재하는 특정한 보호가 필요한 자산에 대한 모든 위협에 대해 기술하여야 한다. 즉 데이터 파괴, 노출, 변경이나 서비스 거부 등을 통해서 자산에 해를 줄 수 있는 위협사항이나 위협원, 공격방법, 공격의 대상이 되는 자산에 대하여 서술하여야 한다.

(3) 조직의 보안정책(Organisational Security Policy)

조직의 보안정책은 조직에 의해서 강제되고 TOE가 따라야 하는 규칙, 절차, 관행, 지침에 대해서 서술해야 한다.

3.2.4 보안목적

보안목적은 보안환경 부분에서 정의된 가정사항 및 조직의 보안정책을 지원하고, 위협에 대응하기 위하여 TOE 또는 TOE 환경에서 만족시켜야 하는 보안목적을 제공한다.

3.2.5 IT 보안 요구사항

TOE의 보안 기능 요구사항과 보증 요구사항 및 TOE의 IT 환경에 대한 기타 보안 요구사항을 정의한다.

3.2.6 응용시 주의사항

보호프로파일 작성자가 추가 정보를 제공하기 위하여 선택적으로 사용된다. 응용 시 주의사항은 독립적인 절로 제공될 수도 있고 보호프로파일의 관련 부분에 분산되어 제공될 수도 있다.

3.2.7 이론적 근거

보호프로파일이 완전하고, TOE가 정의된 보안 문제를 효과적으로 다루며, IT 보안기능 및 보증수단 TOE 보안 요구사항을 만족시키기에 적합하다는 증거를 제공하는 부분이다.

4. NSA IDS System PP와 국가기관용 IDS PP 가정사항 비교분석

4.1 NSA IDS System PP 가정사항 분석

NSA IDS System PP 가정사항은 아래와 같이 크게 네 가지 유형이 제시되었다.

- TOE의 정해진 용법과 관련된 측면
- TOE의 임의의 부분에 대한 환경상의 보호 측면
- 인적 측면

NSA IDS System PP 가정사항 원문은 National Security Agency, "Intrusion Detection System System Protection Profile v.1.4", Feb.

2002를 참고하도록 하고, 본 논문에서는 그에 대한 간단한 설명만을 담는다.

4.1.1 TOE의 정해진 용법과 관련된 측면

(1) A.ACCESS

TOE는 자신의 기능을 수행하기 위하여 필요한 모든 IT System 데이터에 접근할 수 있음을 나타낸다.

(2) A.ASCOPE

TOE는 TOE가 모니터하고 있는 IT 시스템에 맞추어 적절하게 범위를 조정할 수 있음을 나타낸다.

(3) A.DYNMIC

TOE는 TOE가 모니터하는 IT 시스템의 변화를 적절하게 반영할 수 있도록 관리되어야 함을 나타낸다.

4.1.2 TOE의 임의의 부분에 대한 환경상의 보호측면

(1) A.LOCATE

TOE 처리 자원들은 비인가된 물리적 접근을 막을 수 있는 접근 통제 장치 안에 위치하여야 함을 나타낸다.

(2) A.PROTCT

번역 : 보안 정책 시행에 중용한 TOE 하드웨어와 소프트웨어는 비인가 된 물리적 수정으로부터 보호되어야 함을 나타낸다.

4.1.3 인적측면

(1) A.MANAGE

충분한 자격을 갖춘 한 사람 혹은 그 이상의 사람이 TOE와 TOE가 포함하고 있는 정보의 보안을 관리하도록 하여야 함을 나타낸다.

(2) A.NOEVIL

인증된 관리자는 사려 깊고, 태만하지 않으며, 악의가 없고, TOE 문서에 의하여 제공되는 지시사항을 따르고 준수하여야 함을 나타낸다.

(3) A.NOTRST

TOE는 오로지 인가된 사용자들에 의해서만 접근될 수 있음을 나타낸다.

4.2 국가기관용 IDS PP 가정사항 분석

국가기관용 IDS PP 가정사항 항목은 NSA IDS PP의 가정사항이 제시한 유형별 분류를 명시하고 있지 않다. 본 논문에서는 국가기관용 IDS PP가 제시한 가정사항 항목을 NSA IDS PP와 개념상 유사한 항목별로 유형분류를 하였다.

〈표 3〉 NSA IDS 시스템 PP와 국가기관용 IDS PP

	NSA IDS System PP 가정사항	국가기관용 IDS PP 가정사항
정해진 용법측면	A.ACCESS A.ASCOPE A.DYNMIC	A.접근 A.동적관리
환경상의 보호측면	A.PROTCT A.LOCATE	A.신뢰된실행환경 A.공격자수준 A.물리적보안
인적측면	A.MANAGE A.NOTRST A.NOEVIL	A.신뢰된관리자 A.관리역할할당
임의의 시스템 측면	-	A.배포설치운영 A.운영체제보강

<표 3>에서와 같이 항목별로 유형분류를 한 결과 국가기관용 IDS PP 가정사항 항목에는 NSA IDS PP에서 제시한 유형별 분류에 포함되지 않는 항목이 존재하여 본 논문에서는 이 항목을 임의의 시스템적 측면으로 고려하여 유형

분류를 시도하였다.

4.2.1 TOE의 정해진 용법과 관련된 측면

(1) A.접근

A.접근 항목은 NSA IDS PP의 A.ACCESS 항목과 비교되는 항목으로 같은 개념으로 파악되며 침입탐지 방식에 상관없이 모든 보호대상 시스템에 접근할 수 있어야함을 제시하고 있다.

(2) A.동적관리

이 항목은 보호대상 시스템의 변화에 따른 TOE의 유동성을 제시한 항목으로 여기에서 보호대상 시스템이란 IDS 시스템과 IT 시스템을 포괄하는 개념으로 해석된다. 이 항목은 본 논문 4.3절에서 자세히 분석한다.

4.2.2 TOE의 임의의 부분에 대한 환경상의 보호측면

(1) A.신뢰된실행환경

국가기관용 IDS PP에 의하면 TOE 실행환경은 침입탐지 시스템 실행에 필요한 주변 소프트웨어, 펌웨어, 하드웨어 등을 의미한다. 예로 소프트웨어로 구현된 네트워크-기반 침입탐지 시스템의 경우 운영체제, 네트워크 인터페이스 카드, 메모리, 저장 시스템 등이 포함될 수 있다.

(2) A.공격자수준

위협원의 수준에 대한 항목으로 위협원은 중간 수준의 전문지식, 자원, 동기를 가지고 있음을 가정한 항목이다.

(3) A.물리적보안

이 항목은 NSA IDS System PP의 A.LOCATE 항목과 유사한 항목으로 TOE는 인가된 관리자에 의해서만 접근 가능한 환경에 위치해야 함을 제시하고 있다.

4.2.3 인적측면

(1) A.신뢰된 관리자

이 항목은 NSA IDS System PP의 A.NOEVIL 항목과 유사개념으로 해석은 생략하도록 한다.

(2) A.관리역할할당

이 항목은 본 논문 4.3절에서 자세히 분석한다.

4.2.4 임의의 시스템적 측면

이 유형분류는 NSA IDS System PP에서 유사항 항목이 없는 관계로 본 논문에서는 임의로 유형분류를 하였으며 추가적인 연구가 필요한 항목들이다.

(1) A.배포설치운영

이 항목은 배포, 설치, 운영시 TOE의 보안성 문제를 제시하고 있다.

(2) A.운영체제보강

이 항목은 TOE가 설치된 환경에는 TOE와 연관이 없는 응용 프로그램들은 모두 제거하는 작업으로 운영체제상의 취약점에 신뢰성과 안전성 보장에 대한 문제를 제시하고 있다.

4.3 NSA IDS System PP와 국가기관용 IDS PP 항목비교분석

4.3.1 A. 동적관리와 A.DYNMIC, A.SCOPE 비교분석

A.DYNMIC 항목은 TOE가 설치된 ITSystem 유동성에 관한 내용을 내포하고 있으며, A.SCOPE 항목은 IT System 범위에 따른 TOE의 유동성에 관한 내용을 설명하고 있다. 국가기관용 IDS PP의 A.동적관리 항목에서 보호대상 시스템은 IDS와 IT System을 모두 포괄하는 개념으로 해석된다. 즉 NSA IDS PP의 A.DYNMIC 항목과 A.SCOPE 항목을 포괄하는 개념을 가지고 있

는 것이다. 하지만 현재 IDS 및 IT System의 다양한 유형의 제품이 있는 시점에서 두 가지의 변화를 한 항목에서 고려하는 것은 평가대상자 및 평가자 모두에게 혼란을 야기 할 우려가 있으므로 이 항목은 NSA IDS PP와 같이 분리시키는 방향으로 수정되는 것이 평가자나 평가대상자 모두에게 평가준비에 좀 더 효율적이라 생각된다.

4.3.2 A.관리역할 할당과 A.MANAGE, A.NOTRST 항목비교

A.MANAGE 항목은 TOE 관리에 대한 역할 할당 부분에 대한 항목이며 A.NOTRST는 인증된 관리자에 의한 TOE 접근, 즉 인증 및 권한식별에 관한 항목이다. 하지만 국가기관용 IDS PP는 NSA IDS System PP의 TOE 관리에 대한 역할 할당 부분만 존재하고 TOE에 대한 접근 권한 부분에 대한 가정사항은 고려치 않은 것으로 보인다. 현재 사용되는 System은 대부분 관리콘솔이 제공되고 있고 관리콘솔에 대해 접근할 경우에도 인증 및 권한식별이 요구되어진다. IDS 역시 관리콘솔을 제공하는 제품이 있으므로 콘솔 접근시 권한식별 및 인증에 대한 항목을 추가하거나 A.관리역할 할당 항목에 내용을 추가하는 방향으로 수정이 요구되어진다.

5. 결 론

본 논문에서는 국내외의 정보보호 시스템 평가 기준의 변화와 공통 평가 기준에 대해서 알아보고 국가 기관용 IDS PP와 NSA IDS System PP의 가정사항을 분석 및 비교하여 보았다. 향후 정보통신 시스템의 지속 발전 및 사용은 정보보호 시스템의 신뢰성과 안정성이라는 문제를 항상 동반하게 될 것이다. 이에 정보보호 시스템에 대한 평가 및 인증의 대한 중요성은 계속적으로 제기될 것이다. 정보보호 시스템의 평가 기준은 많은 변화가 예상되며, CC를 기반으로 하는 보호프로파일의 경우 IT 기반 환경의 변화에 따라 많은 변화가 예상된다. 본 연구에서 제시한 국가기관용 침입탐지 시스템 보호프로파일 가정사항 항목 중 A.동적관리, A.관리역할 할당 항목 외에 A.공격자수준 항목은 과도한 요구 및 다른 항목과의 분리 통합시키는 방향에 대해 연구의 필요성이 제기되며 본 논문에서 제시한 임의의 시스템적 측면으로 분류된 A.배포설치운영, A.운영체제보강 항목의 경우는 다른 항목과의 그 내용상의 유사성과 범위문제에 대해 연구가 필요할 것이다.

참 고 문 헌

[1] 정보통신부, 정보통신망 침입차단 시스템 평가 기준 개정 및 고시, 2000. 2.
[2] 정보통신부, 정보통신망 침입차단 시스템 평가 기준, 2000. 7.
[3] 정보보호진흥원, "정보보호 시스템 평가·인증 가이드", 2002. 12.
[4] 정보보호진흥원, "국가기관용 침입탐지 시스템 보호프로파일 v1.0", 2000. 7.
[5] 정보보호진흥원, http://www.kisa.or.kr.
[6] 국가정보원, http://www.nis.go.kr.
[7] CERTCC-KR, http://www.certcc.or.kr.
[8] 이강석, "IDS 구성 및 운영", 정보보호진흥원, 2002. 11.
[9] 정보통신부, "정보보호 시스템 공통평가 기준", 2002. 8.
[10] 조규민, "국제 공통 평가 기준 기반의 보호프로파일 개발을 위한 평가대상 범위설정 방법", 석사학위, 동국대 국제정보대학원, 2002.
[11] 장세현, "국방정보체계의 적합한 공통평가기준 기반의 리눅스 운영체제(PC) 보호프로파일에 관한 연구", 석사학위, 국방대학원 2002.
[12] 조범래, "기능과 품질에 기반한 침입탐지 시스템의 평가를 위한 실험 데이터 패턴 생성", 석사학위, 포항공과대학교 정보통신대

학원, 2002.
[13] http://www.commoncriteria.org.
[14] http://www.nsa.gov/.
[15] National Security Agency, "Intrusion Detection System System Protection Profile v.1.4", Feb. 2002.

김 남 기
2002년 경기대학교 산업공학과 (공학사)
2002년~현재 경기대학교 정보통신대학원 석사과정

박 종 오
2000년 호남대학교 컴퓨터공학과 (공학사)
2002년~현재 경기대학교 정보통신대학원 석사과정

김 지 영
2003년 방송통신대학교 방송정보학과(이학사)
2003년~현재 경기대학교 정보통신대학원 석사과정