정보보호 제품에서 CC 보안기능의 활용도에 관한 연구

최 성 자[†] · 최 상 수[††] · 이 강 수[†††]

요 약

CC내의 보안기능(클래스 패밀리-컴포넌트)을 실제 정보보호 제품이나 PP에서 사용하는 빈도에 대한 연구결과가 없으므로, 어떤 보안기능이 중요한지를 판단하기가 어렵다. 본 논문에서는 기존의 33종의 제품유형별 PP들이 CC내의 어떤 보안기능을 사용했는지를 조사하여, CC내의 보안기능들의 사용율과 제품유형별 보안기능의 사용율을 구하였다. 이 결과는 제품의 새로운 분류, 제품유형별 개발 및 평가비 산정 등에 활용할 수 있을 것이다.

A Study on Utilization of CC Security Function Components in IT Security Products

Choi Sung Ja[†] · Choi Sang Soo[††] · Lee Gang Soo[†††]

ABSTRACT

It is difficult to decide which security functions(class, family, component) in the Common Criteria(CC) are important, since there is no research result about the frequency of use of security functions in real security product or Protection Profiles(PPs). Thus, we survey security functions in CC and 33 PPs that can be classified by 10 product types, and create a set of "frequency of use of security functions" in CC and each types of security product. Our research results are useful for development of a new classification schema, as well as, estimation of development and evaluation efforts of security products.

키워드 : 국제공통평가기준(Common Criteria), 보안기능(Security Function), 사용율(Frequence Of Use)

1. 서 론

ISO/IEC 15408로 표준화된 CC(Common Criteria)는 우리나라를 포함한 선진 각국에서 정보보호 시스템 및 제품의 평가기준으로 사용하고 있으며 2004년 10월 현재 버전 2.2이 공식버전이며 버전 2.4를 개발중에 있다[1, 2]. 우리나라는 2002년 3월에 정보통신부에서 버전 2.1(1999년 개발)을 번역하여 "정보보호시스템 공통평가기준"으로 고시하였으므로[3], 본 논문에서는 버전 2.1을 이용하며, 관련 용어를 정보보호 "제품"으로 통칭하여 사용하였다.

CC의 파트 2에는 정보보호 제품이 가질 수 있는 전체 보안기능 요구사항 집합을 11개의 클래스, 67개의 패밀리, 136개의 컴포넌트로 분류하고 있다. 여기서, 보안기능 컴포넌트("컴포넌트"로 약칭함)는 단위 보안기능이며 임의의 제품은 전체 컴포넌트 중 일부를 포함한다. 또한, CC가 발표되기 이전에 개발된 제품에서도 CC와는 다른 이름을 가진 컴포넌트를 포함하지만, 이들은 CC의 컴포넌트에 대응된다.

한편, PP(Protection Profile)는 제품 유형별로 정의한 공통 보안기능 및 보증 요구사항에 해당하며 CC내의 보안기능 및 보증 요구사항에서 제품에 필요한 보안기능을 선택하여 구성한다. 또한, ST(Security Target)는 특정한 제품의 보안기능 및 보증요구사항이며 소속된 제품유형의 PP나 직접 CC로부터 보안기능 및 보증요구사항의 일부 또는 전부를 선택하여 구성한다[1, 4].

그러나, CC내의 컴포넌트에 관련된 다음과 같은 가설들은 CC에 포함되어 있지 않다.

- **[가설 1]** 컴포넌트의 구현에 필요한 "복잡도"(즉, 기능의 구현에 필요한 노력)가 일정하지 않다. 예컨대, FIA_UID.1 (식별)은 FAU_GEN.1(감사데이터 생성)을 구현하는 것보다 복잡도가 낮을 것이다.
- **[가설 2]** 컴포넌트의 "사용빈도"는 다르다. 예컨대, 모든 제품의 공통기능에 해당하는 FIA_UID.1(식별)은 프라이버시에만 관련된 기능인 FPR_PSE.1(가명성)보다 사용빈도가 높을 것이다.
- **[가설 3]** 제품유형별로 사용한 컴포넌트들은 서로 다르

※ 이 논문은 2004년도 한남대학교 교비연구지원에 의하여 수행되었음.
† 준 회 원 : 한남대학교 대학원 컴퓨터공학과 박사과정
†† 준 회 원 : 한남대학교 대학원 컴퓨터공학과 박사과정
††† 종신회원 : 한남대학교 컴퓨터공학과 정교수
논문접수 : 2004년 10월 15일, 심사완료 : 2004년 12월 28일

며, 이에 따라 제품유형별로 기능의 복잡도도 다를 것이다. 예컨대, 침입차단 유형에서 사용하는 컴포넌트들은 스마트카드 유형에서 사용하는 컴포넌트들과는 상이할 것이다.

[가설 1]을 검증하기 위해서는 각 컴포넌트를 실제 구현하고 소프트웨어공학 부문에서 사용하는 복잡도 및 개발비용 산정 방법(예: Cyclomatric number, Software science, COCOMO, Function Point 등)을 사용하여 실험조사적 방법을 통해 각 컴포넌트의 복잡도를 산정하면 되지만 많은 노력이 필요하다[5, 6]. 특히, 결과의 객관성을 확보하기 위해서는 서로 다른 환경에서 30회 이상을 구현하여 복잡도를 측정해야만 통계적 의미를 갖는다.

따라서, 본 논문에서는 기존의 제품유형별 PP에서 사용한 컴포넌트를 조사하여 [가설 2]와 [가설 3]을 검증하고자 한다. 즉, 각 컴포넌트의 사용률을 조사하고 각 컴포넌트의 복잡도를 동일한 것으로 가정하여 제품유형별 보안기능의 복잡도를 산정한다.

본 논문의 2장에서는 CC, PP 및 ST의 상호관계와 제품의 분류체계를 조사한다. 3장에서는 33종의 실제 PP들로부터 보안기능 컴포넌트, 패밀리 및 클래스의 사용빈도를 조사하고 제품유형별 PP들의 특성과 제품의 상대적 복잡도를 산정한다. 4장에서는 제시한 결과의 활용방안을 제시하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 CC, PP 및 ST 간의 관계

CC는 모든 정보보호 제품에서 필요로 하는 "보안기능 요구사항"의 전체 집합을 클래스-패밀리-컴포넌트-엘리먼트를 통해 계층적으로 분류한 것이다[1, 3]. 즉, CC는 보안기능의 분류스키마 중의 하나라 할 수 있다. 또한, 보안기능에 대한 구현의 정확성에 대한 "보증요구사항"의 전체 집합을 계층적으로 분류하였고, 7단계의 보증수준별로 요구하는 보증요구사항(컴포넌트)을 정의하고 있다. 상위의 보증수준은 하위의 보안수준보다 완전하고, 엄격하며 정형적이므로, 보증수준간에는 완전성, 엄격성 및 정형성 관계를 갖는다[1]. 또한, CC에는 컴포넌트간의 "종속성"이 정의되어있다. 예컨대, FAU_STG.1(감사증적 보호)은 FAU_GEN.1(감사데이터 생성)과 종속관계를 가진다. 즉, 두 가지 기능은 상호 연관되어 있음을 의미한다.

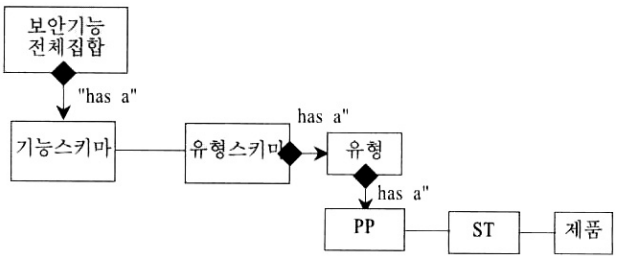
특히, 제품유형에 따라 CC의 보안기능 요구사항의 일부를 선택하여 7수준의 보안수준 중 하나를 택하여 PP 또는 ST를 구성한다. 예컨대, 만능이며 수학적으로 완벽한 제품은 CC의 모든 보안기능 요구사항과 모든 보증 요구사항(즉, EAL7수준)을 가진다.

PP는 제품유형별 공통 보안기능 요구사항명세서이며 특정한 제품유형의 운영에 대한 보안환경(가정, 보안정책, 위협문장을 포함), 보안목적, 보안대책(또는 보안기능)으로 구성된다. 보안대책은 CC의 보안기능요구사항집합의 부분집합이다. 일반적으로, 제품유형별 협회 및 기관 등에서 개발하며 별도의 PP평가와 인증이 요구된다.

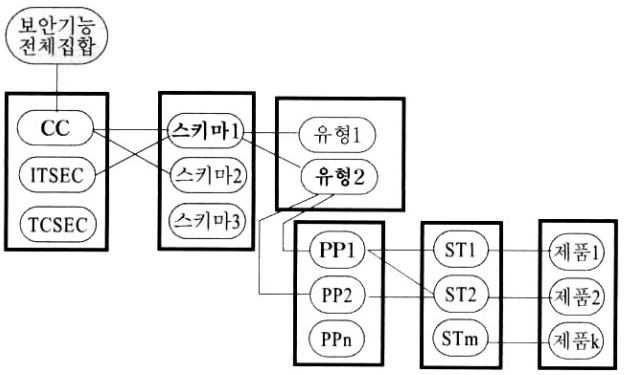
ST는 특정한 제품(즉, 평가대상물, TOE)의 보안기능 요구사항 명세서이다. 해당 제품유형의 PP가 존재할 경우, 기존의 PP에 개발환경을 부가하여 사용할 수 있으며 이 경우 "PP준수선언"이 필요하다[4]. ST는 TOE의 보안기능 요구사항명세서에 해당하므로, ST도 TOE와 함께 평가 및 인증한다.

2.2 정보보호 제품의 분류체계 모델

ITSEC이나 CC와 같은 평가기준마다 보안기능의 분류체계가 다르며, 평가기준은 곧 보안기능의 분류체계를 의미한다. 제품의 분류체계(즉, 유형 스키마)는 기존 PP, ST 또는 제품의 유형별 분류기준이다. (그림 1)은 CC기반의 제품 분류를 위한 모델을 제시하며, 해당 모델의 설계(인스턴스) 결과는 (그림 2)에서 보인다.



(그림 1) CC기반의 제품 분류모델(클래스다이어그램)



(그림 2) CC기반의 제품 분류모델의 인스턴스

예컨대, (그림 2)에서 스키마1(예: 영국의 분류)은 유형1(침입차단 제품)과 유형2(스마트카드 제품)로 분류함을 나타내며, PP1과 PP2는 유형2(스마트카드)로 분류된 스마트카드 PP들이다. 또한, ST1(A사의 스마트카드)은 PP1을 준수하며, ST2(B사의 스마트카드)는 PP1과 PP2를 동시에 준수함을 의미한다. 제품1(A사의 스마트카드 제품)은 ST1(A사의 스마트카드 ST)을 준수하여 개발했다는 것을 나타낸다.

2.3 기존의 정보보호 제품의 분류체계

<표 1>은 CC 평가환경 하에서 각 국의 제품의 분류체계들을 보이며, 다음과 같이 분석된다[6~13].

- **분류체계가 표준화 안됨 :** 보안기능과 보증수준은 ISO/EC 15408(즉, CC)을 통해 국제적으로 표준화되어 있지만, 제품의 유형에 대한 분류체계는 표준화되어 있지 않다. 따라서, 각국의 제품의 개발자, 판매자, 구매자 및 정부관리자들 사이에 혼선이 발생할 수 있다. 예컨대, 제품분류가 국가마다 다르므로, 수출입시의 관세, 통관 업무가 복잡해진다. 또한, 구매자 측에서도 각국의 "평가된 제품목록(EPL)"의 분류가 다르므로 제품을 검색하기가 어렵다. 특히, 우리나라의 경우, 제품유형별로 평가비용을 달리하므로 제품유형을 표준화하는 것이 중요하다.
- **제품간 기능중복 문제 :** 분류체계가 다양하기 때문에 개발된 제품간의 기능중복 문제가 발생된다. 예컨대, 영국에서 "네트워크 제품"으로 분류된 제품은 다른 나라에서는 다른 제품으로 분류될 수 있으므로, 제품을 가져다 정보시스템을 구축해야하는 개발자의 입장에서 혼선이 발생한다.
- **CC 및 PP와의 연계성 부족 :** CC에는 보안기능과 보증수준이 표준화되어 있지만, 제품의 분류시에 CC와의 연관성이 부족하다. 예컨대, 침입차단 제품은 CC의 기능요구사항 중 어떤 기능을 발휘하는지에 대한 정보가 부족하다. 물론 침입차단 제품용 PP에는 이 정보가 있지만 PP마다 편차가 심하다. 이러한 이유는 각국의 CC 기반의 정보보호시스템 평가체계에서 정보보호 제품의 분류에 대한 연구가 이루어지지 않았기 때문이다. 따라서, CC와 PP를 고려하여 제품의 분류체계를 시급히 개발해야한다.

3. 보안기능 사용빈도

10가지 제품 유형에 대한 33종의 실제 PP로부터 CC내의 보안기능 요구사항의 사용빈도를 조사하고 제품유형별 보안기능의 사용빈도를 조사한다.

3.1 전체 제품유형에서 보안기능의 사용빈도

3.1.1 척도의 정의

CC내의 보안기능들은 다음과 같이 정의한다.

- 클래스: CL = $\{CL_1, ..., CL_i, ..., CL_{11}\}$ = {FAU, FIA, FMT, FCS, FPT, FDP, FTP, FTA, FCO, FRU, FPR}
- 패밀리: FA = $\{FA_1, ..., FA_i, ..., FA_{67}\}$ = {FPT_RVM, FIA_ATD, FMT_MOF, FMT_MSA, ...}
- 컴포넌트: CO = $\{CO_1, ..., CO_2, ..., CO_{136}\}$ = {FPT_RVM.1, FMT_MTD.1, FMT_MSA.3, FIA_ATD.1, FMT_MSA.1, ... }

특히, 패밀리내의 컴포넌트들은 독립 및 계층관계를 갖는다. 독립관계를 갖는 컴포넌트들은 선택적으로 사용되며 계층관계를 갖는 컴포넌트의 경우, 상위수준의 컴포넌트는 하위의 것을 포함한다.

- 계층관계(CC내에서 정의됨): $CO_i < CO_j$: CO_i는 CO_j를 포함함(상위관계)
- 독립관계(CC내에서 정의됨): $CO_i \vee CO_j$: CO_i와 CO_j는 독립임

〈표 1〉 CC체계에서의 제품 분류[6-13]

국가	대분류	세부분류	비고
CC 포털	OS, DB, 침입탐지, 접근통제, 네트워크(라우터, VPN, 스캐너) 스마트카드(IC), 지역보호(boundary, 침입차단), 데이터보호(PC 가드, 암호모듈), 키관리(PKI), 기타(메시지관리)		제품 분류
미국 CC (NIAP)	네트워크 인프라	스위치와 라우터, 라우터, 무선LAN	PP 및 제품 분류
	네트워크 정보보호	침입차단, VPN, 원격접근, 이동코드, 다중영역 솔루션, 가드	
	컴퓨터 환경 정보보호	OS, 생체, 보안 메신저, 토큰, 단일수준 웹서버, 기밀자료보호, DB, PC접근통제, 장치공유 스위치, 기타(바이러스)	
	인프라 지원	네트워크 관리, 스마트카드, 키복구, PKI/PMI, 침입탐지, 기타(인증서관리)	
미 정부	OS, DB, 침입차단, 침입탐지, VPN, 토큰, 생체, 웹, PKI, 무선		PP 분류
영국	OS, DB, 통신(스위치, 메신저, 라우터), 자료삭제(erasure), 네트워크(PKI, 침입차단, VPN), PC 접근통제(가드), 기타(감사, PKI)		제품 분류
프랑스	IC(스마트카드IC), 스마트카드, 네트워크(침입차단,), 리더/단말, PC 제품, 시스템 (VPN)		제품 분류
호주	OS, 네트워크 보안(VPN, 침입차단), 공개키 기술(PKI), 스마트카드, PC 보안(가드), 생체, 호스트 보안모듈, 매체소제(sanitisation), 기타(DB)		제품 분류
과거의 CC 홈페이지 KISA수수료, 본 연구	**OS, DB, 침입차단, 침입탐지, VPN, 네트워크, 스마트카드, 접근통제, 키복구, 기타**		**PP 및 제품 분류**
염홍렬 제안	정보보호 인프라	암호지원, 보안관리, 인증, 생체, 스마트카드(토큰, USB)	제품 분류
	컴퓨팅 환경 정보보호	DB, 서버보안(OS)	
	네트워크 정보보호	네트워크 기반(라우터, 침입탐지, 스위치), 네트워크 간(침입차단, VPN , 가드)	
	컴퓨팅 정보보호	메일보안, 단일레벨 보안(웹서버 보안), PC보안, 공유스위치, 이동코드, 기타	

현재의 CC 포털싸이트 이전에 2003년까지 운영되었던 CC홈페이지와 본 연구팀은 제품의 유형을 다음과 같이 분류하고 각종 PP들을 분류하였다[6, 7].

- 제품유형: TYPE = {$TYPE_1$, $TYPE_2$, ..., $TYPE_{10}$} = {DB, 침입차단, VPN, 네트워크, OS, 스마트카드, 접근통제, 키복구, 침입탐지, 기타}
- 제품유형별 PP군: PP_TYPE = {PP_TYPE_1, PP_TYPE_2, ..., PP_TYPE_{10}}
- PP집합: PP_TYPE_{ij} = {PP_TYPE_{11}, PP_TYPE_{12}, ..., PP_TYPE_{10n}}

각 척도는 다음과 같이 정의한다.

- $\#PP\_TYPE_i$: 제품유형 i의 PP개수
- $\#PP\_TYPE_i\_CO_j$: 제품유형 i내에서 컴포넌트 CO_j를 사용한 PP수
- $TYPE_i\_CO_j$: 제품유형 i에서 사용한 컴포넌트 j
- $TYPE_i\_FA_j$: 제품유형 i에서 사용한 패밀리 j
- $TYPE_i\_CL_j$: 제품유형 i에서 사용한 클래스 j

3.1.2 사용빈도의 계산

각국의 CC 관련 홈페이지를 통해 공개된 10가지 제품유형의 33종의 PP로부터 CC내 보안기능 컴포넌트, 패밀리 및 클래스의 사용빈도는 다음과 같이 계산한다. **부록 A**에는 본 연구에서 사용한 33종의 PP 목록을 보인다.

〈표 2〉 기능컴포넌트 사용빈도

범위	보안기능 컴포넌트와 사용빈도(@COi)
980-1000	**FIA_UID.1(식별, 980), FPT_RVM.1(TSP우회불가성, 922), FMT_MTD.1(TSF데이터관리, 902)**
800-899	**FPT_SEP.1(보안기능 영역분리, 889), FMT_SMR.1(보안역할, 855), FMT_MSA.3(정적속성 초기화, 847), FIA_UAU.1(인증, 847), FIA_ATD.1(사용자속성 정의, 835), FMT_MSA.1(보안속성 관리, 807)**
700-799	FAU_STG.1(감사증적 보호, 797), FAU_GEN.1(감사데이터 생성, 774), FMT_MOF.1(보안기능 관리, 752)
600-699	FPT_STM.1(신뢰할 수 있는 타임스탬프, 655), FDP_ACC.1(부분적인 접근통제, 650), FIA_AFL.1(인증 실패처리, 643), FAU_STG.3(감사데이터 손실 예측시 대응행동, 640), FAU_SEL.1(선택적인 감사, 637), FDP_ACF.1(보안속성에 기반한 접근통제, 600)
500-599	FPT_TST.1(TSF자체시험, 570), FAU_SAR.1(감사검토, 557), FMT_MSA.2(안전한 보안속성, 552), FDP_RIP.1(부분적인 잔여정보 보호, 548), FCS_COP.1(암호연산, 545), FIA_UID.2(모든 행동이전에 사용자식별, 540), FPT_AMT.1(추상기계시험, 530), FDP_IFC.1(부분적인 정보흐름통제, 523)
400-499	FDP_IFF.1(단일계층 보안속성, 498), FCS_CKM.1(암호키 생성, 498), FAU_STG.4(감사데이터의 손실방지, 467), FIA_UAU.7(인증피드백 보호, 456), FMT_REV.1(폐지, 443), FAU_SAR.3(선택가능한 감사검토, 432), FAU_GEN.2(사용자신원 연관, 410), FAU_SAA.1(잠재적인 위반분석, 404), FIA_UAU.2(모든 행동 이전에 사용자인증, 401)
300-399	FIA_SOS.1(비밀정보의 검증, 398), FCS_CKM.4(암호키 파기, 398), FAU_ARP.1(보안경보, 397), FAU_SAR.2(감사검토 권한제한, 393), FIA_USB.1(사용자-주체 연결, 391), FPT_ITI.1(외부전송 TSF데이터의 변경탐지, 390), FTP_ITC.1(TSF간 안전한채널, 390), FPT_RPL.1(재사용공격 탐지 및 대응행동, 385), FPT_FLS.1(장애시 안전한상태 유지, 377), FPT_ITT.1(내부전송 TSF데이터의 기본적인 보호, 365), FMT_MTD.2(TSF데이터 한계치의 관리, 338), FDP_ITT.1(기본적인 내부전송 보호, 331), FCS_CKM.2(암호키 분배, 329), FCS_CKM.3(암호키 접근, 325), FPT_TDC.1(TSF간 전송되는 TSF데이터의 기본적인 일관성, 320), FPT_RCV.1(수동복구, 306)
200-299	FMT_MTD.3(안전한 TSF데이터, 298), FRU_RSA.1(최대할당치, 262), FDP_RIP.2(전체적인 잔여정보 보호, 261), FDP_UIT.1(전송데이터 무결성, 257), FTA_TSE.1(TOE세션 설정, 237), FTA_MCS.1(동시세션수의 제한: 사용자별, 237), FIA_UAU.4(재사용방지 인증매커니즘, 233), FPT_RCV.4(기복구, 223), FPT_PHP.3(물리적공격에 대한 저항, 220), FDP_ITC.2(보안속성을 포함한 사용자데이터 유입, 219), FDP_ETC.1(보안속성 없이 사용자데이터 유출, 216), FPT_ITC.1(외부전송 TSF데이터의 비밀성, 212)
100-199	FDP_ITC.1(보안속성 없이 사용자데이터 유입, 195), FTA_SSL.1(TSF에 의한 세션잠금, 195), FTP_TRP.1(안전한 경로, 186), FDP_ETC.2(보안속성을 포함한 사용자데이터 유출, 186), FPT_RCV.2(자동복구, 178), FDP_DAU.1(기본적인 데이터인증, 178), FMT_SMR.2 보안역할의 제한, 176), FDP_ACC.2(완전한 접근통제, 168), FCO_NRO.2(강제적인 발신증명, 165), FAU_STG.2(감사데이터의 가용성 보호, 145), FPT_RCV.3(과도한 손실없는 자동복구, 145), FPT_PHP.1(물리적공격의 기본적인 보호, 144), FDP_ITT.3(무결성검사, 136), FCO_NRO.1(선택적 발신증명, 135), FDP_SDI.1(저장된 데이터의 무결성검사, 120), FTA_SSL.3(TSF에 의한 세션종료, 117), FDP_IFC.2(완전한 정보흐름통제, 115), FPT_TRC.1(내부복제 TSF데이터의 일관성, 115), FRU_FLT.1(오류에대한 내성: 부분적용, 112), FMT_SMR.3(역할위임, 108), FCO_NRR.1(선택적인 수신증명, 107), FAU_SAA.3(단순공격학습, 100)
1-99	FTA_SSL.2(사용자에 의한 세션잠금, 95), FPT_SEP.2(보안기능 정책영역 분리, 95), FIA_UAU.5(다중 인증매커니즘, 93), FCO_NRR.2(강제적인 수신증명, 87), FPT_ITA.1(외부전송 TSF데이터의 가용성, 87), FIA_UAU.3(위조할수 없는 인증, 86), FPT_ITT.3(내부전송 TSF데이터 무결성검사, 83), FIA_SOS.2(비밀정보의 생성, 78), FMT_SAE.1(보안속성 유효기간의 관리, 75), FTA_TAB.1(기본적인TOE접근경고, 75), FTA_TAH.1(TOE접근 이력, 75), FRU_PRS.1(자원사용 우선순위: 부분적용, 70), FPR_UNO.4(인가된 사용자 관찰불가성, 67), FDP_DAU.2(증거생성자의 신원을 포함한 데이터인증, 67), FIA_UAU.6(재인증, 58), FPT_ITT.2(TSF데이터와 사용자데이터의 전송분리, 53), FPR_ANO.1(익명성, 53), FDP_UCT.1, 기본적인전송데이터비밀성, 53), FDP_SDI.2, 저장된 데이터의 무결성검사 및 대응행동, 53), FRU_PRS.2, 자원사용 우선순위: 전체적용, 50), FDP_UIT.2, 송신처에의한 데이터복구, 50), FDP_IFF.3, 허용되지 않은 정보흐름의 제한, 50), FPT_SSP.1, 수신자 응답, 45), FPT_SSP.2, 상호 응답, 45), FDP_ITT.2, 속성에 의한 데이터전송 분리, 45), FDP_UIT.3, 수신처에의한 데이터 복구, 25), FPT_SEP.3, 보안기능 정책영역의 완전한 분리, 25), FRU_RSA.2, 최대와 최소 할당치, 25), FTA_MCS.2, 동시세션수의 제한: 사용자속성별, 25), FDP_IFF.2, 계층적 보안속성, 25), FPR_ANO.2, 강화된 익명성, 20), FDP_ITT.4, 속성에 기반한 무결성감사, 20), FTA_LSA.1, 선택가능한 보안속성의 범위 제한, 20), FD_ROL.1, 기본 복구, 20), FPR_UNL.1, 연계불가성, 20)
0	FRU_FLT.2(오류에 대한 내성: 전체적용), FDP_IFF.5(허용되지 않은 흐름의 제거), FAU_SAA.2(프로파일에 기반한 비정상행위 탐지), FDP_IFF.4(허용되지 않은 정보흐름의 부분적 제거), FDP_IFF.6(허용되지 않은 흐름의 감시), FDP_ROL.2(전체 복구), FPR_PSE.3(이중가명성), FPR_PSE.2(추적가능한 가명성), FPR_PSE.1(가명성), FAU_SAA.4(복잡 공격학습), FPT_PHP.2(물리적공격의 탐지 및 통보), FPR_UNO.1(관찰불가성), FPT_ITI.2(외부전송 TSF데이터의 변경탐지 및 정정), FMT_SMF.1(관리기능명세), FPR_UNO.2(관찰불가성 관련 정보분산), FPR_UNO.3(TSF의 관찰불가성)

〈표 3〉 패밀리 사용빈도

범위	기능 패밀리와 사용빈도(@FAi)
900-999	**FIA_UID(사용자 식별, 980), FPT_RVM(참조모니터에의한 중재, 922)**
800-899	**FPT_SEP(영역분리, 889), FIA_ATD(사용자속성 정의, 835)**
700-799	FMT_MOF(기능관리, 752), FMT_MSA(보안속성 관리, 735), FAU_STG(보안감사사건 저장, 719)
600-699	FPT_STM(타임스탬프, 755), FDP_ACC(접근통제정책, 650), FIA_AFL(인증실패, 646), FAU_SEL(보안감사사건 선택, 637), FDP_ACF(접근통제기능, 600)
500-599	FAU_GEN(보안감사데이터 생성, 592), FPT_TST(TSF 자체시험, 570), FDP_RIP(잔여정보보호, 548), FCS_COP(암호연산, 545), FPT_AMT(추상기계 시험, 530), FDP_IFC(정보흐름 통제정책, 523), FMT_MTD(TSF데이터 관리, 513)
400-499	FMT_SMR(보안역할 관리(482), FAU_SAR(보안감사 검토, 461), FMT_REV(폐지, 443), FAU_SAA(보안감사 분석, 404)
300-399	FAU_ARP(보안감사 자동대응, 397), FIA_USB(사용자-주체 연결, 391), FTP_ITC(TSF간 안전한채널, 390), FPT_ITI(외부전송 TSF데이터의 무결성, 390), FCS_CKM(암호키 관리, 388), FPT_RPL(재가용공격 탐지, 385), FPT_FLS(안전한 상태유지, 377), FPT_TDC(TSF간 전송되는 TSF데이터의 기본적인 일관성, 320)
200-299	FIA_UAU(사용자 인증, 296), FPT_RCV(안전한 복구, 265), FRU_RSA(자원할당, 262), FIA_SOS(비밀정보의 검증 및 생성, 238), FTA_MCS(동시세션수의 제한, 237), FTA_TSE(TOE세션 설정, 237), FDP_ITT(TOE내부전송, 234), FPT_ITT(TSF데이터 내부전송, 224), FPT_ITC(외부전송 TSF데이터의 비밀성, 212), FDP_ITC(TSF통제 외부로부터 사용자 데이터 유입, 207), FDP_ETC(TSF통제 외부로 사용자 데이터 유출, 201)
100-199	FTP_TRP(안전한 경로, 186), FDP_IFF(정보흐름 통제기능, 183), FPT_PHP(물리적보호, 182), FDP_DAU(데이터인증, 178), FCO_NRO(발신 부인방지, 165), FDP_UIT(TSF간 전송되는 사용자데이터 무결성, 154), FTA_SSL(세션잠금, 136), FDP_SDI(저장된 데이터의 무결성, 120), FPT_TRC(내부복제 TSF데이터의 일관성, 115), FRU_FLT(오류에 대한 내성, 112), FCO_NRR(수신 부인방지, 107)
1-99	FPT_ITA(외부전송 TSF데이터의 가용성, 87), FTA_TAB(TOE접근경고, 75), FTA_TAH(TOE접근이력, 75), FMT_SAE(보안속성 유효기간, 75), FRU_PRS(자원사용 우선순위, 70), FDP_UCT(TSF간 전송되는 사용자데이터 비밀성, 53), FPR_ANO(익명성, 53), FPT_SSP(상태동기화 프로토콜, 45), FPR_UNO(관찰불가성, 22), FTA_LSA(선택가능한 보안속성의 범위제한, 20), FPR_UNL(연계불가성, 20), FDP_ROL(복구, 20)
0	FPR_PSE(가명성), FMT_SMF(관리기능 명세)

- **제품유형별 컴포넌트 사용빈도($\%TYPE_i\_CO_j$)**
  = (제품유형내에서 컴포넌트를 사용한 PP수 ÷ 제품유형내의 PP개수) × 100
  = $\%TYPE_i\_CO_j$) = ($\#PP\_TYPE_i\_FO_j$) ÷ $\#PP\_TYPE_i$) × 100
  if $CO_i < CO_j$, **then** $\%TYPE_k\_CO_i = \%TYPE_k\_CO_i + \%TYPE_k\_CO_j$. 계층관계시의 조정
  if $\%TYPE_k\_CO_i > 100$, **then** $\%TYPE_k\_CO_i = 100$.
  부록 B에는 제품유형별 컴포넌트 사용빈도의 계산 결과의 일부를 보인다.
- **컴포넌트 사용빈도($@CO_i$)**
  = 모든 제품유형내의 컴포넌트 사용빈도의 합계 = $\sum_j \%TYPE_j\_CO_i$
  <표 2>는 컴포넌트 사용빈도를 보인다.
- **패밀리 사용빈도($@FA_i$)** = 패밀리내 하위 컴포넌트의 사용빈도 변환평균치
  FA_i내의 컴포넌트 CO_{ij}, CO_{ik}에 대해,
  if ($CO_{ij} \vee CO_{ik}$), **then** $@FA_i$ = *Average* ($@CO_{ij}$, $@CO_{ik}$). ..... 독립관계시
  if ($CO_{ij} < CO_{ik}$), **then** $@FA_i$ = *Maximum* ($@CO_{ij}$, $@CO_{ik}$). ..... 계층관계시
  <표 3>은 패밀리 사용빈도를 보인다.
- **클래스 사용빈도($@CL_i$)** = 클래스내 하위 패밀리의 사용빈도 평균치
  FA_i내의 모든 컴포넌트 CO_{i*}에 대해, $@CL_i$ = Average ($@FA_{i*}$)

<표 4>는 클래스 사용빈도를 보인다.

〈표 4〉 클래스 사용빈도

범위	기능 클래스와 사용빈도 (@CLj)
500이상	**FAU(보안감사, 535), FIA(식별 및 인증, 564)**
400-499	**FMT(보안관리, 429), FCS(암호지원, 467)**
300-399	FPT(TSF보호, 386)
200-299	FDP(사용자데이터 보호, 282), FTP(안전한 경로/채널, 288)
100-199	FTA(TOE접근, 130), FCO(통신, 136), FRU(자원활용, 148)
0-99	FPR(프라이버시, 24)

3.2 제품유형별 보안기능 사용빈도

"PP 집중율"은 특정 제품유형의 PP들 내부의 보안기능이 얼마나 중복되어 있는가를 나타낸다. 예컨대, 100%란 모든 PP가 같은 보안기능을 가진 것이며 0%란 PP마다 서로 다른 기능을 가진 것을 의미한다. PP 집중율이 클수록 PP는 바람직하게 분류된 것이다. PP집 중율을 다음과 같이 계산한다.

- a = PP 개수
- b = 1%이상 사용된 컴포넌트 전체 개수
- f = 1%이상 사용된 컴포넌트 비율(%) = b×100/136
- c = 50%이상 사용된 컴포넌트 개수
- g = 50%이상 사용된 컴포넌트 사용비율(%) = c×100/136
- h = c×100/b, d = 100%사용된 컴포넌트 개수
- i = 100%사용된 컴포넌트 사용비율(%)= d×100/b

〈표 5〉 PP집중율의 계산

척도 \ 제품유형	DB	침입차단	VPN	네트워크	OS	스마트카드	접근통제	키복구	침입탐지	기타
a (PP개수)	2	5	3	4	4	1	5	3	3	3
b, f (1%이상 사용된 컴포넌트수 및 비율)	28 (20.6)	39 (28.7)	73 (53.7)	94 (69.1)	62 (45)	43 (31.6)	96 (70.6)	55 (40.4)	34 (25)	59 (43.4)
c, g (50%이상 사용된 컴포넌트수 및 비율)	28 (20.6)	25 (18.4)	50 (36.8)	55 (40.4)	57 (41.9)	43 (31.6)	32 (23.5)	34 (25)	24 (17.6)	29 (21.3)
d, i (100%사용된 컴포넌트수 및 비율)	25 (89.3)	15 (38.5)	33 (45.2)	6 (6.4)	26 (41.9)	43 (100)	4 (4.2)	14 (25.5)	15 (44.1)	12 (20.3)
e (컴포넌트사용율 합)	2650	2500	5232	4475	4275	4300	4000	3433	2433	3329
j (컴포넌트사용율 평균)	19.5	18.4	38.5	32.9	31.4	31.6	29.4	25.2	17.9	24.5
k (PP집중율 %)	**94.6**	**64.1**	**71.7**	**47.6**	**69.0**	**100**	**41.7**	**62.4**	**71.6**	**56.4**

- e = 컴포넌트 사용율 합
- j = 컴포넌트 사용율 평균(%) = e×100/13600
- k = PP집중율 = e/b×100%.

<표 5>는 각 척도의 값을 보인다. "제품유형별 보안기능 수의 상대적 비율"은 제품유형별 개발 및 평가복잡도 산정을 위한 기간 및 비용을 산정할 때 활용할 수 있다. 또한, "PP 집중율"은 PP들의 분류가 정확한가의 판단 척도로 활용할 수 있다. <표 5>로부터 DB(94%), OS(69%), VPN(71.7%) 및 침입탐지(71.6%)제품의 PP들은 집중율이 높다(즉, PP마다 공통기능 많음). 또한, 네트워크(47.6%) 접근통제(41.7%) 제품유형의 PP들은 공통기능이 적으므로, 제품유형의 분류가 잘못된 것으로 해석할 수 있다. 즉, 네트워크 제품유형 및 접근통제 제품유형은 분류가 잘못되어있으므로 이 분류를 제거하고 세분화해야한다. DB제품유형의 PP의 집중율이 높은 이유는 두 개의 PP를 동일기관(즉, Oracle사)이 개발했기 때문이다.

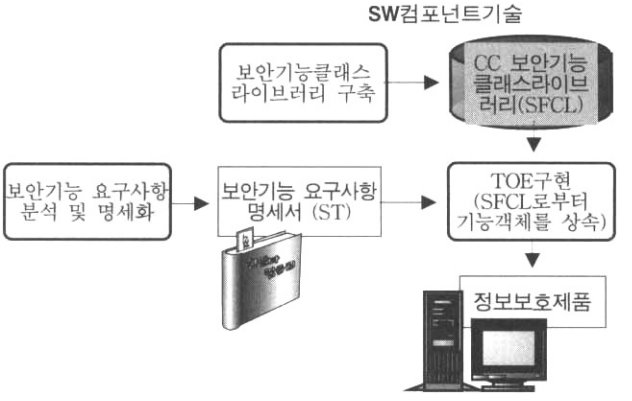
부록 B에는 각 제품유형별로 활용빈도($\%TYPE_i\_FO_j$)가 50%이상인 보안기능 컴포넌트를 보인다.

4. 보안기능사용 빈도의 활용방안

4.1 보안기능 클래스 라이브러리 구축

"보안기능 클래스 라이브러리"(SFCL)는 CC의 보안기능 컴포넌트를 미리 구현하여 재사용 가능하도록 한 것이며, (그림 3)은 SFCL의 개발과 사용에 대한 모델을 보인다.

- **SFCL 구축:** 136개의 보안기능 컴포넌트는 객체지향 및 컴포넌트 기술을 이용하여 136개의 "SW컴포넌트"(또는 함수)로 미리 구현하여 SFCL을 구축한다. CC내의 보안기능 컴포넌트에 대한 정의는 SFCL에 대한 API가 된다(즉, 라이브러리 내 각종 컴포넌트에 대한 호출정보). 본 논문에서 제시한 컴포넌트 "사용빈도"는 SFCL내의 SW컴포넌트를 구현할 때 구현 우선순위를 정하는데 활용될 수 있다. 기존 PP에서 75%이상 사용한 보안기능 컴포넌트는 다음과 같으며 SFCL 내에서 우선적으로 구현해야할 모듈이 된다.
  FIA_UID.1(식별), FPT_RVM.1(TSP우회불가성), FMT_MTD.1(TSF데이터관리), FPT_SEP.1(보안기능 영역분리), FMT_SMR.1(보안역할), FMT_MSA.3(정적속성 초기화), FIA_UAU.1(인증), FIA_ATD.1(사용자속성 정의), FMT_MSA.1(보안속성 관리), FAU_STG.1(감사증적 보호), FAU_GEN.1(감사데이터 생성), FMT_MOF.1(보안기능 관리)
- **SFCL의 사용:** SFCL은 SSL 프로토콜과 암호함수의 공개소스 라이브러리인 OpenSSL보다는 상위수준의 라이브러리이며 각종 제품을 구현할 때 사용될 수 있을 것이다[14]. 제품의 요구 보안기능은 이미 SFCL에 있으므로, 이를 상속하면 쉽게 제품을 개발할 수 있다. 즉, ST나 PP만 주어진다면 거의 SFCL을 이용하여 반자동적으로 구현이 가능하다.
- **SFCL의 평가:** SFCL을 구축할 때, 각 SW컴포넌트에 대해 CC 평가를 받았다면 SFCL로 개발한 제품은 쉽게 평가할 수 있다. 즉, 각 보안기능 컴포넌트의 평가결과를 재사용하고 컴포넌트간의 인터페이스 및 통합부문만 추가로 평가하면 된다.



(그림 3) 보안기능 클래스 라이브러리의 개발과 사용

4.2 제품유형별 개발 및 평가업무량 산정

각 제품유형마다 CC 기능컴포넌트의 사용율이 다르다. 사용율이란 CC의 전체 보안기능수(즉, 136개) 중 각 제품이 제공하는 보안기능수를 의미하며, 제품유형별 개발업무량과 개발비용에 영향을 준다. 비록 각 보안기능 컴포넌트마다 개발시의 업무량이 다르지만 대부분의 제품유형마다 공통적으로 사용한 보안기능이 많으므로(앞 절의 결과 참조), 사용율을 제품유형별 개발업무량의 상대적인 값으로 활용할 수 있다.

제품유형별 보안기능의 평균값은 제품유형별 개발 및 평가업무량의 척도로 활용할 수 있다[6]. <표 6>은 제품유형별 상대적 "복잡도"이며, 제품유형별 개발 및 평가업무량 및 비용산정시에 활용할 수 있다. 예컨대, VPN 제품유형은 136가지 CC 보안기능 중 38.5%를 발휘하고 있으며 19.5%인 DB 제품유형보다 2배의 기능이 요구되며, 개발비용 및 평가비용도 2배로 산정할 수 있다.

〈표 6〉 제품유형별 복잡도

제품유형 / 척도	DB	침입차단	VPN	네트워크	OS	스마트카드	접근통제	키복구	침입탐지	기타
컴포넌트 사용율 평균	19.5	18.4	38.5	32.9	31.4	31.6	29.4	25.2	17.9	24.5

4.3 제품유형 분류체계 개발

2장에서 보인바와 같이 제품의 분류체계는 다양하다. "PP 집중율" 척도는 제품유형과 PP의 분류체계를 개발할 때 사용할 수 있다. 분류를 위해, PP 집중율이 극대화되도록 기존 PP들을 클러스터링 한다. PP들의 클러스터링 결과는 곧 제품의 분류결과가 된다. 예컨대, 3장에서 보인 DB제품유형 내의 2개의 PP들의 집중율은 94.6%이므로 분류가 잘 된 것이지만, 접근통제 제품유형의 PP들 집중율은 41.7%이므로 재분류가 필요하다.

5. 결 론

CC는 각종 보안제품이 가져야할 공통 보안기능요구사항과 보증요구사항의 계층적 집합이다. 지금까지는 각 보안기능 요구사항(클래스, 패밀리 또는 컴포넌트)이 실제 제품에서 얼마나 활용되는가에 대한 연구가 없다. 예컨대, "보안감사" 기능클래스와 "프라이버시" 기능클래스는 동일 수준으로 분류되지만, 기능의 사용율은 매우 다르다. 본 논문의 연구분석 결과, 보안감사 기능의 사용율(특히, 사용빈도)은 535이지만 프라이버시 기능은 24에 지나지 않는다는 사실을 발견하였다. 이는 CC를 이용해 PP를 개발할 때, 또는 정보보호 제품유형을 분류할 때, CC 보안기능 라이브러리를 개발할 때에 활용할 수 있는 정보이다.

본 논문의 공헌사항은 다음과 같다.

- 33종의 PP를 대상으로 CC내의 보안기능과 기존 PP내의 보안기능의 사용현황을 조사하여 보안기능의 우선순위를 정할 때 사용하도록 함
- 제품의 분류체계의 다양성 문제을 파악하고, "PP 집중율" 척도를 활용해 이 문제를 해결하는 방안을 아이디어 수준으로 제시함
- 제품유형별 보안기능 "사용빈도"을 조사하여 제품유형별 상대적 복잡도 척도로 이용하고 이를 통해 제품별 개발 및 평가비용 산정에 활용

향후 연구과제는 다음과 같다.

- 본 논문에서는 33종의 PP를 대상으로 조사하였으나 계속 신규 PP들이 개발되고 있으므로, 이들에 대해서도 계속적인 조사가 필요하다.
- 본 논문에서 제시한 SFCL 모델을 이용하여, CC보안기능을 위한 "보안기능 클래스 라이브러리"의 개발이 필요하다.
- CC와 기발표된 PP들을 고려하고, PP의 분류체계와 제품의 분류체계를 통일한 새로운 정보보호 제품의 분류체계가 개발 및 표준화되어야 한다.

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] 강연희, 이강수, "공통평가기준(CC)과 공통평가방법론(CEM)의 변경내용 분석", 정보보호학회지, 14권 4호, pp.68-77, 2004년 8월.

[3] "국제공통평가기준 (CC) 2.0", 한국정보보호진흥원, 2002.8.

[4] ISO/IEC PDTR 15446, "Information technology- Security techniques-Guide for the production of protection profiles and security targets", Draft, Apr. 3, 2000.

[5] S. L. Pfleeger, "Software Engineering theory and practice", 2nd. ed., Prentice-Hall, 2001.

[6] 최상수, 최승, 이완석, 이강수, "CC기반에서 보증수준 및 제품유형을 동시에 고려한 평가업무량 모델", 정보보호학회논문지, 14권 1호, pp.25-34, 2004년 1월.

[7] CC 포털에서의 분류, http://www.commoncriteriaportal.org.

[8] 미국 CC체계에서의 제품분류, http://niap.nist.gov/cc-scheme/pp/index.html.

[9] 미 정부 PP Development Process For US Government Protection Profiles (PP), Version 3.0 1 March 2004. (http://niap.nist.gov/pp/pp_dev_proccess.pdf)

[10] 호주의 분류, http://www.dsd.gov.au/infosec/.

[11] 영국의 분류, http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=151.

[12] 프랑스의 분류, http://www.ssi.gouv.fr/fr/confiance/certificats.html#systemes.

[13] 오홍렬, 염홍렬, "국제공통평가기준(CC) 체계하에서 평가된 정보보호제품 분석", 정보보호학회지, 14권 4호, pp.54-67, 2004년 8월.

[14] J. Viega, M. Messier, P. Chandra, Network Security with OpenSSL, O'Reilly, 2002.

부록 A: 제품 유형별 PP 목록

제 품 유 형	PP고유번호 (CC체계내)	PP 이름
DB	PP-008	Oracle DBMS Protection Profile
	PP-003	Oracle Government Database
침입 차단	PP-005	Traffic Filter Firewall Protection Profile For Medium Robustness Environments
	PP-010	Traffic Filter Firewall Protection Profile for Low Risk Environments (v1.1)
	PP-015	Application-level Firewall Protection Profile For Medium Robustness Environments
	PP-011	Application Level Firewall Protection Profile for Low Risk Environments (v1.d)
	KPP-002	국가기관용 침입차단시스템 보호프로파일 v1.1
VPN	PP-026	A Goal VPN Protection Profile For Protecting Sensitive Information - v2.0
	KPP-001	국가기관용 게이트웨이형 가상사설망 보호프로파일 v1.1
	KPP-004	국가기관용 가상사설망 보호프로파일 v1.1
네트 워크	PP-029	The PKI Secure Kernel Protection Profile
	PP-023	Peer-to-Peer Wireless Local Area Network(WLAN) for Sensitive But Unclassified Environments - v0.6
	PP-024	Protection Profile for Switches and Routers
	PP-027	Infrastructure Wireless Local Area Network(WLAN) For Sensitive But Unclassified Environments
OS	PP-007	Labeled Security Protection Profile v1.b
	PP-012	Controlled Access Protection Profile
	PP-022	Protection Profile for Multilevel OS Requiring Medium Robustness
	PP-025	Single-level OS's in Environments Requiring Medium PP
스마트카드	PP-028	Smart Card Protection Profile
접근 통제	PP-001	Directory for US Department of Defense Class 4 PKI PP
	PP-006	Certificate Issuing and Management Components
	PP-009	Role-Based Access Control Protection Profile v1.0
	PP-014	Privilege Directed Content Protection Profile
	PP-002	Trusted Platform Module(TPM) Protection Profile
키 복구	PP-019	Key Recovery for Third Party Requestors v1.0
	PP-020	Key Recovery for Agent Systems v1.1
	PP-021	Key Recovery for End Systems v.2
침입 탐지	PP-017	Intrusion Detection System Analyzer Draft 3
	PP-018	Intrusion Detection System Sensor - Draft 3
	KPP 003	국가기관용 침입탐지시스템 보호프로파일 v1.1
기타	PP-013	Postage Meter Approval Protection Profile
	TCPATPMPP_V1.9.7	Trusted Computing Platform Alliance(TCPA) Trusted Platform Modle Protection Profile
	PP-016	U.S.Department of Defense Biometrics Office, Biometric System. Protection Profile For Medium Robustness Environment v0.02

부록 B. 제품유형별 50%이상 사용된 보안기능컴포넌트

DB 제품 (2종)	
100%	FAU_GEN.1(감사데이터 생성), FAU_GEN.2(사용자신원 연관), FAU_SAA.1(잠재적인 위반분석), FAU_SAA.3(단순공격 학습), FAU_SEL.1(선택적인 감사), FAU_STG.1(감사증적 보호), FAU_STG.3(감사데이터 손실 예측시 대응행동), FDP_ACC.1(부분적인 접근통제), FDP_ACF.1(보안속성에 기반한 접근통제), FIA_AFL.1(인증실패 처리), FIA_ATD.1(사용자속성 정의), FIA_SOS.1(비밀정보의 검증), FIA_UAU.1(인증), FIA_UID.1(식별), FIA_USB.1(사용자-주체 연결), FMT_MSA.1(보안속성관리), FMT_MSA.3(정적속성 초기화), FMT_MTD.1(TSF데이터관리), FMT_REV.1(폐지), FMT_SMR.1(보안역할), FPT_RVM.1(TSP우회불가성), FPT_SEP.1(보안기능영역 분리), FRU_RSA.1(최대할당치), FTA_MCS.1(동시세션수의 제한: 사용자별), FTA_TSE.1(TOE세션설정)
50%	FAU_STG.4(감사데이터의 손실방지), FDP_RIP.1(부분적인 잔여정보보호), FDP_RIP.2(전체적인 잔여정보보호)

침입차단 제품 (5종)	
100%	FAU_GEN.1 감사데이터생성, FAU_SAR.3 선택가능한감사검토, FAU_STG.1 감사증적보호, FAU_STG.3 감사데이터손실예측시대응행동, FAU_STG.4 감사데이터의손실방지, FDP_IFC.1 부분적인정보흐름통제, FDP_IFF.1 단일계층보안속성, FIA_AFL.1 인증실패처리, FIA_ATD.1 사용자속성정의, FMT_MOF.1 보안기능관리, FMT_MSA.3 정적속성초기화, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스탬프, FMT_SMR.1 보안역할
80%	FAU_SAR.1 감사검토, FCS_COP.1 암호연산, FDP_RIP.1 부분적인잔여정보보호, FIA_UID.1 식별, FIA_UID.2 모든행동이전에사용자식별
60%	FIA_UAU.1 인증, FIA_UAU.4 재사용방지인증메커니즘, FMT_MSA.1 보안속성관리, FMT_MTD.1 TSF데이터관리, FMT_MTD.2 TSF 데이터 한계치의관리

VPN 제품 (3종)	
100%	FAU_ARP.1 보안경보, FAU_GEN.1 감사데이터생성, FAU_SAR.1 감사검토, FAU_SEL.1 선택적인 감사, FAU_STG.3 감사데이터손실예측시대응행동, FCS_CKM.1 암호키생성, FCS_CKM.2 암호키분배, FCS_CKM.3 암호키접근, FCS_CKM.4 암호키파기, FCS_COP.1 암호연산, FIA_AFL.1 인증실패처리, FIA_ATD.1 사용자속성정의, FIA_SOS.1 비밀정보의검증, FIA_UAU.1 인증, FIA_UAU.2 모든행동이전에사용자인증, FIA_UAU.7 인증피드백보호, FIA_UID.1 식별, FIA_UID.2 모든행동이전에사용자식별, FMT_MOF.1 보안기능관리, FMT_MSA.1 보안속성관리, FMT_MSA.2 안전한보안속성, FMT_MSA.3 정적속성초기화, FMT_MTD.1 TSF데이터관리, FMT_MTD.2 TSF데이터한계치의 관리, FMT_MTD.3 안전한TSF 데이터, FMT_SMR.1 보안역할, FPT_AMT.1 추상기계시험, FPT_RPL.1 재사용공격 탐지및대응행동, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스템프, FPT_TST.1 TSF자체시험, FTP_ITC.1 TSF간안전한채널
67%	FAU_SAA.1 잠재적인위반분석, FAU_SAR.3 선택가능한감사검토, FAU_STG.1 감사증적보호, FAU_STG.4 감사데이터의손실방지, FDP_DAU.1 기본적인데이터인증, FDP_DAU.2 증거생성자의신원을포함한데이터인증, FDP_IFC.1 부분적인정보흐름통제, FDP_IFF.1 단일계층보안속성, FIA_UAU.4 재사용방지인증매커니즘, FPR_UNO.4 인가된사용자관찰불가성, FPT_FLS.1 장애시안전한상태유지, FRU_FLT.1 오류에대한내성:부분적용, FRU_RSA.1 최대할당치, FTA_MCS.1 동시세션수의제한:사용자별, FTA_SSL.1 TSF에의한세션잠금, FTA_SSL.3 TSF에의한세션종료, FTA_TSE.1 TOE세션설정

네트워크 제품 (4종)	
100%	FDP_IFC.1 부분적인정보흐름통제, FDP_IFF.1 단일계층보안속성, FIA_UID.1 식별, FIA_UID.2 모든행동이전에사용자식별, FMT_MSA.1 보안속성관리, FMT_MSA.3 정적속성초기화
75%	FAU_GEN.1 감사데이터생성, FCO_NRO.1 선택적발신증명, FCS_CKM.1 암호키생성, FCS_CKM.4 암호키파기, FCS_COP.1 암호연산, FDP_ITT.1 기본적인내부전송보호, FIA_ATD.1 사용자속성정의, FIA_UAU.1 인증, FIA_UAU.2 모든행동이전에사용자인증, FIA_USB.1 사용자-주체연결, FMT_MOF.1 보안기능관리, FMT_MSA.2 안전한보안속성, FMT_MTD.1 TSF데이터관리, FMT_SMR.1 보안역할, FPT_ITT.1 내부전송TSF데이터의기본적인보호, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스템프
50%	FAU_GEN.2 사용자신원연관, FAU_SAR.1 감사검토, FAU_SEL.1 선택적인감사, FAU_STG.1 감사증적보호, FAU_STG.4 감사데이터의손실방지, FDP_ACC.1 부분적인접근통제, FDP_ACF.1 보안속성에기반한접근통제, FDP_ETC.2 보안속성을포함한사용자데이터유출, FDP_IFC.2 완전한정보흐름통제, FDP_ITC.2 보안속성을포함한사용자데이터유입, FDP_ITT.3 무결성 검사, FDP_UIT.1 전송데이터무결성, FDP_UIT.2 송신처에의한데이터복구, FIA_AFL.1 인증실패처리, FIA_UAU.7 인증피드백보호, FMT_REV.1 폐지, FMT_SMR.2 보안역할의제한, FPT_AMT.1 추상기계시험, FPT_FLS.1 장애시안전한상태유지, FPT_ITI.1 외부전송 TSF데이터의변경탐지, FPT_RCV.1 수동복구, FPT_RCV.4 기복구, FPT_TDC.1 TSF간전송되는TSF데이터의기본적인일관성, FPT_TST.1 TSF자체시험, FRU_PRS.1 자원사용우선순위:부분적용, FRU_PRS.2 자원사용우선순위:전체적용, FTA_MCS.1 동시세션수의제한:사용자별, FTA_SSL.3 TSF에의한세션종료, FTA_TSE.1 TOE세션설정, FTP_ITC.1 TSF 간안전한채널, FTP_TRP.1 안전한경로

OS 제품 (4종)	
100%	FAU_GEN.1 감사데이터생성, FAU_GEN.2 사용자신원연관, FAU_SAR.1 감사검토, FAU_SAR.2 감사검토권한제한, FAU_SAR.3 선택가능한감사검토, FAU_SEL.1 선택적인감사, FAU_STG.1 감사증적보호, FAU_STG.3 감사데이터손실예측시대응행동, FAU_STG.4 감사데이터의손실방지, FDP_ACC.1 부분적인접근통제, FDP_RIP.1 부분적인잔여정보보호, FDP_RIP.2 전체적인잔여정보보호, FIA_ATD.1 사용자속성정의, FIA_SOS.1 비밀정보의검증, FIA_UAU.1 인증, FIA_UAU.7 인증피드백보호, FIA_UID.1 식별, FMT_MSA.1 보안속성관리, FMT_MSA.3 정적속성초기화, FMT_MTD.1 TSF데이터관리, FMT_REV.1 폐지, FMT_SMR.1 보안역할, FPT_AMT.1 추상기계시험, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스템프,
50%	FAU_ARP.1 보안경보, FAU_SAA.1 잠재적인위반분석, FCS_CKM.1 암호키생성, FCS_CKM.2 암호키분배, FCS_CKM.4 암호키파기, FCS_COP.1 암호연산, FDP_ACC.2 완전한 접근통제, FDP_ACF.1 보안속성에기반한 접근통제, FDP_ETC.2 보안속성을포함한사용자데이터유출, FDP_IFC.1 부분적인정보흐름통제, FDP_ITC.1 보안속성없이사용자데이터유입, FDP_ITC.2 보안속성을포함한사용자데이터유입, FDP_ITT.1 기본적인내부전송보호, FIA_USB.1 사용자-주체연결, FMT_MOF.1 보안기능관리, FMT_MSA.2 안전한보안속성, FMT_SAE.1 보안속성유효기간의관리, FMT_SMR.3 역할위임, FPT_ITT.1 내부전송TSF데이터의기본적인보호, FPT_ITT.3 내부전송TSF데이터무결성검사, FPT_RCV.1 수동복구, FPT_SEP.2 보안기능정책영역분리, FPT_TDC.1 TSF간전송되는TSF데이터의기본적인 일관성, FPT_TRC.1 내부복제TSF 데이터의 일관성, FPT_TST.1 TSF자체시험, FRU_RSA.1 최대할당치, FTA_SSL.1 TSF에의한세션잠금, FTA_SSL.2 사용자에의한세션잠금, FTA_TAB.1 기본적인TOE접근경고, FTA_TAH.1 TOE접근이력, FTP_TRP.1 안전한 경로

스마트카드 제품 (1종)	
100%	FAU_ARP.1 보안경보, FAU_SAA.1 잠재적인위반분석, FAU_SEL.1 선택적인감사, FAU_STG.1 감사증적보호, FAU_STG.3 감사데이터손실예측시대응행동, FCS_CKM.1 암호키생성, FCS_CKM.3 암호키접근, FCS_COP.1 암호연산, FDP_ACC.1 부분적인접근통제, FDP_ACF.1 보안속성에기반한 접근통제. FDP_ETC.1 보안속성없이사용자데이터유출, FDP_IFC.1 부분적인정보흐름통제, FDP_IFF.1 단일계층보안속성, FDP_ITC.1 보안속성없이사용자데이터유입, FDP_ITT.1 기본적인내부전송보호, FDP_RIP.1 부분적인잔여정보보호, FDP_RIP.2 전체적인잔여정보보호, FDP_UIT.1 전송데이터무결성, FIA_AFL.1 인증실패처리, FIA_ATD.1 사용자속성정의, FIA_UAU.1 인증, FIA_UAU.7 인증피드백보호, FIA_UID.1 식별, FMT_MOF.1 보안기능관리, FMT_MSA.1 보안속성관리, FMT_MSA.2 안전한보안속성, FMT_MSA.3 정적속성초기화, FMT_MTD.1 TSF 데이터관리, FMT_MTD.2 TSF데이터한계치의관리, FMT_MTD.3 안전한TSF데이터, FMT_REV.1 폐지, FPT_FLS.1 장애시안전한상태유지, FPT_ITI.1 외부전송TSF데이터의변경탐지, FPT_ITT.1 내부전송TSF데이터의기본적인 보호, FPT_PHP.3 물리적공격에대한저항, FPT_RCV.1 수동복구, FPT_RCV.2 자동복구, FPT_RCV.3 과도한손실없는자동복구, FPT_RCV.4 기복구, FPT_RPL.1 재사용공격탐지및대응행동, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_TST.1 TSF자체시험, FTP_ITC.1 TSF간안전한 채널

접근통제 제품 (5종)	
100%	FAU_GEN.1 감사데이터생성, FAU_SEL.1 선택적인감사, FIA_USB.1 사용자-주체연결, FMT_MTD.1 TSF데이터관리
80%	FAU_STG.1 감사증적보호, FDP_ACC.1 부분적인접근통제, FDP_ACF.1 보안속성에기반한접근통제, FMT_MSA.1 보안속성관리, FMT_MSA.3 정적속성초기화, FMT_SMR.1 보안역할, FPT_RVM.1 TSP우회불가성, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스탬프
60%	FAU_ARP.1 보안경보, FAU_GEN.2 사용자신원연관, FAU_SAR.1 감사검토, FAU_SAR.2 감사검토권한제한, FCO_NRO.1 선택적발신증명, FDP_RIP.1 부분적인잔여정보보호, FIA_AFL.1 인증실패처리, FIA_ATD.1 사용자속성정의, FIA_UAU.2 모든행동이전에사용자인증, FIA_UID.1 식별, FIA_UID.2 모든행동이전에사용자식별, FMT_MOF.1 보안기능관리, FMT_MSA.2 안전한 보안속성, FMT_REV.1 폐지, FMT_SMR.2 보안역할의제한, FPT_AMT.1 추상기계시험, FPT_FLS.1 장애시안전한상태유지, FPT_RPL.1 재사용공격탐지및대응행동, FPT_TST.1 TSF자체시험

키복구 제품	
100%	FCO_NRO.2 강제적인발신증명, FCS_COP.1 암호연산, FDP_ACC.1 부분적인접근통제, FDP_ACF.1 보안속성에기반한접근통제, FIA_UAU.1 인증, FIA_UAU.2 모든행동이전에사용자인증, FIA_UID.1 식별, FIA_UID.2 모든행동이전에 용자식별, FMT_MSA.1 보안속성관리, FMT_MSA.2 안전한보안속성, FMT_MSA.3 정적속성초기화, FMT_SMR.1 보안역할, FPT_RVM.1 TSP우회불가성, FPT_TDC.1 TSF간 전송되는TSF데이터의기본적인일관성
67%	FAU_GEN.1 감사데이터생성, FAU_GEN.2 사용자신원연관, FAU_SAR.1 감사검토, FAU_SAR.2 감사검토권한제한, FAU_STG.1 감사증적보호, FCO_NRR.1 선택적인수신증명, FCO_NRR.2 강제적인수신증명, FCS_CKM.2 암호키분배, FDP_SDI.1 저장된데이터의무결성검사, FDP_UIT.1 전송데이터무결성, FMT_MOF.1 보안기능관리, FMT_MTD.1 TSF 데이터관리, FPT_AMT.1 추상기계시험, FPT_ITC.1 외부전송TSF데이터의비밀성, FPT_ITI.1 외부전송TSF데이터의변경탐지, FPT_ITT.1 내부전송 TSF 데이터의기본적인보호, FPT_SEP.1 보안기능영역분리, FPT_STM.1 신뢰할수있는타임스탬프, FPT_TST.1 TSF자체시험, FTP_ITC.1 TSF간안전한채널

침입탐지 제품 (3종)	
100%	FAU_GEN.1(감사데이터생성, =IDS_COL1), FAU_SAR.1(감사검토, =IDS_SAR.1), FAU_SAR.2(감사검토권한제한, =IDS_RDR.1), FAU_SAR.3(선택가능한감사검토, =IDS_SAR.3), FAU_STG.1(감사증적보호, =IDS_STG.1), FAU_STG.3(감사데이터손실예측시대응행동, =IDS_STG.2), FAU_STG.4(감사데이터의손실방지, =IDS_STG.3, IDS_STG.2), FIA_AFL.1(인증실패 처리), FIA_ATD.1(사용자속성정의), FIA_UAU.1(인증), FIA_UID.1(식별), FMT_MOF.1(보안기능관리), FMT_MTD.1(TSF데이터관리), FMT_SMR.1(보안역할), FPT_STM.1(신뢰할수있는타임스탬프)
67%	FAU_ARP.1(보안경보, =IDS_RCT.1), FAU_SAA.1(잠재적인위반분석, =IDS_ANL.1), FAU_SEL.1(선택적인감사, FAU_STG.2(감사데이터의가용성보호, =IDS_STG.1), FPT_ITA.1(외부전송TSF데이터의가용성), FPT_ITC.1(외부전송TSF데이터의비밀성), FPT_ITI.1(외부전송TSF데이터의변경탐지), FPT_RVM.1(TSP우회불가성), FPT_SEP.1(보안기능영역분리)

기타 제품 (3종)	
100%	FCS_CKM.1(암호키생성), FCS_CKM.4(암호키파기), FCS_COP.1(암호연산), FIA_UID.1(식별), FMT_MOF.1(보안기능관리), FMT_MTD.1(TSF데이터관리), FMT_SMR.1(보안역할), FPT_AMT.1(추상기계시험), FPT_FLS.1(장애시안전한상태유지), FPT_RVM.1(TSP우회불가성), FPT_SEP.1(보안기능영역분리), FPT_TST.1 (TSF자체시험)
67%	FAU_GEN.1(감사데이터생성), FCO_NRO.2(강제적인발신증명), FCS_CKM.2(암호키분배), FCS_CKM.3(암호키접근), FDP_ACC.1(부분적인접근통제), FDP_ACF.1(보안속성에기반한접근통제), FDP_RIP.1(부분적인잔여정보보호), FIA_ATD.1(사용자속성정의), FIA_UAU.1(인증), FIA_UAU.6(재인증), FIA_UID.2(모든행동이전에사용자식별), FMT_MSA.1(보안속성관리), FMT_MSA.2(안전한보안속성), FMT_MSA.3(정적속성초기화), FPT_PHP.3(물리적공격에대한저항), FPT_RPL.1(재사용공격탐지및대응행동), FPT_TDC.1(TSF간전송되는TSF데이터의기본적인일관성)

최 성 자

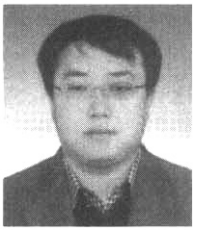
e-mail : irecomm@dreamwiz.com

1991년 한남대학교 컴퓨터공학과(학사)

1997년 한남대학교 대학원 컴퓨터공학과 (석사)

2002년~현재 한남대학교 대학원 컴퓨터공학과 박사과정

관심분야 : 소프트웨어공학, 웹공학, 보안공학, 소프트웨어 시험



최 상 수

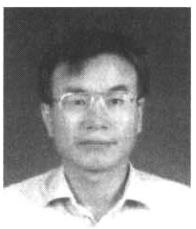
e-mail : gcss09@se.hannam.ac.kr

2001년 한남대학교 컴퓨터공학과(학사)

2003년 한남대학교 대학원 컴퓨터공학과 (석사)

2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정

관심분야 : 소프트웨어공학, 웹공학, 보안공학, 정보보호, 프로세스 모델링 및 분석



이 강 수

e-mail : gslee@eve.hannam.ac.kr

1981년 홍익대학교 컴퓨터공학과(학사)

1983년 서울대학교 대학원 전산학과(이학석사)

1989년 서울대학교 대학원 전산학과(이학박사)

1985년~1987년 국립대전산업대학교 전자계산학과 전임강사

1992년~1993년 미국일리노이대학교 객원교수

1995년 한국전자통신연구원 초빙연구원

1998년~1999년 한남대학교 멀티미디어학부장

1987년~현재 한남대학교 컴퓨터공학과 정교수

관심분야 : 소프트웨어공학, 병행시스템 모형화 및 분석, 정보보호시스템 평가, 멀티미디어교육 커리큘럼