

CC 평가수요 분석 및 차기 평가대상 제품군 선정

오 흥 룡^{a)† ‡}, 엄 흥 열^{b)}

한국정보통신기술협회^{a)}, 순천향대학교^{b)}

Analysis on CC Evaluation Demand and Selection of IT Security Products to be evaluated under CC Scheme in Korea

Heung-Ryong Oh^{a)† ‡}, Heung-Youl Youm^{b)}

Telecommunications Technology Association^{a)}, SoonChunHyang University^{b)}

요 약

정보보호 제품 평가를 위한 국제 공통평가기준(CC: Common Criteria)은 국제상호인정협정(CCRA: Common Criteria Recognition Arrangement)에 가입된 국가들 간에 자국에서 평가된 제품에 대해 다른 국가에서 재평가 없이 상호인정이 가능한 평가 기준이다. 본 논문에서 우리는 국내 정보보호 제품을 분류하기 위하여 CC 체제하에 평가된 미국, 영국, 호주의 평가된 정보보호 제품을 분석하였고, CC 평가를 위한 정보보호 제품군을 정의하였다. 그리고 주요 정보보호 제품에 대한 국내의 시장 동향과 국내 산업체 의견 및 수요 조사를 위하여 설문지를 만들어서 설문을 수행하였고, 그 결과를 취합하여 분석하였다. 그 결과 우리는 향후 5년간 국내에서 우선적으로 평가가 필요한 차기 정보보호 평가대상 제품 15개를 선정하였고, 선정된 정보보호 제품에 대한 특성과 장단점을 분석하였다. 본 논문의 결과는 우리나라 실정에 적합한 정보보호 제품 개발 및 평가를 위해 활용 가능하고, 차기 평가대상 확대시 정책 자료로 활용될 것으로 기대된다.

ABSTRACT

The Common Criteria can be used as a guideline for one CCRA member to avoid re-evaluating IT security products which were already evaluated by other CCRA members. In this paper, we have analyzed the evaluated IT security products under CC scheme in several nations, such as United States, Great Britain and Australia. and defined new category of the IT security products for the domestic CC evaluation. And we have analyzed the domestic and international market on the information security products, have conducted a poll to receive opinions and demands of the Korean industries for Korea policy decision maker to select the possible IT security products which will be evaluated in Korea under CC scheme. As a conclusion, we have selected 15 IT products based on the response to a poll by the industries, the market size, the evaluation amount demanded by the user, manufacturer, and evaluator, to select the possible IT security product under CC schemes in Korea during next 5 years. Moreover, the characteristics, the benefit, and the demerit of the selected IT products

접수일 : 2004년 5월 31일 ; 채택일 : 2004년 9월 7일

* 본 연구는 정보통신부(한국정보보호진흥원) 정보보호체계 구축사업과 충남대 IITRC 사업 연구결과로 수행되었습니다.

† 주저자, ‡ 교신저자 : hroh@tta.or.kr

were analyzed. This paper can be used as a guideline document for Korea policy decision maker to select the IT products to be evaluated under CC scheme in Korea for next 5 years.

Keywords : CC, CCRA, IT

I. 서 론

IT(Information Technology)가 지배하는 정보사회의 도래로 생활의 질적 향상과 더불어 네트워크 상 상호 교환되는 정보의 경제적 가치 또한 급격히 증가되고 있다. IT기반의 정보사회는 우리에게 많은 편리함을 제공하면서 또한 우리의 비밀정보 등의 해킹과 같은 많은 위험성과 취약성이 있다. 따라서 이를 해결하기 위하여 다양한 정보보호 제품이 필요하게 되고 이 제품들에 대한 평가기준이 필요하게 되었다.

CC로 불리어지는 국제 공통평가기준은 1999년 12월 CC version 2.1이 ISO/IEC 15408 국제표준^[20]으로 채택되어 활용되고 있다. 국내에서도 2002년 8월에 최초 고시되었으며, 2003년에 다시 개정되어 고시되었다^[19]. CC는 3부분으로 구성되어 있으며, Part1은 CC의 일반적 개념 및 원칙에 대해 소개하고, Part2는 보안기능 요구 사항, Part3은 보증 요구 사항을 표현하는 방법과 요구사항들을 명세하고 있다.

세계 각국가간에도 CC 체제하에서 평가된 제품에 대해서 구매자가 원하는 보호프로파일이 준수되었다면, 다른 나라에서도 이 제품에 대해 재평가 없이 상호인정이 가능토록 CCRA에 가입하려는 추세이다. 현재 우리나라도 국제적인 변화 추세에 맞추어 정보보호 제품의 보급 및 해외시장 진출을 위해 국내 평가인증제도의 보완이 필요하고 가능한 빨리 CCRA 가입을 고려해야 한다. 다행히 현재 우리나라 인증기관도 가입을 정책적으로 결정하고 이에 대한 요구 사항을 준비하고 있다.

본 논문에서는 국내 정보보호 제품에 대한 향후 5년 동안 CC 체제하에서 우선적으로 평가가 필요한 제품을 선정하기 위한 것이다. 우선적으로 국내 정보보호 제품을 분류하기 위하여 CC 체제하에서 평가된 미국, 영국, 호주의 정보보호 제품을 분석하고, CC 평가를 위한 정보보호 제품군을 정의하였다. 그리고 국내외 정보보호 제품 시장 동향과 국내 정보보호 산업체의 의견과 수요를 반영하기 위하여 설문지를 만들어 설문을 하고 이를 분석하였다. 이들 분

석을 바탕으로 우리는 국내에서 우선적으로 평가가 필요한 15개의 정보보호 제품들을 선정하였고, 이 제품들의 특징과 장·단점을 분석하였다.

본 논문의 II장에서는 국제 공통평가기준 동향 및 CCRA의 정보보호제품을 분석하고, III장에서는 CC 체제하에서 평가된 미국, 영국, 호주의 평가된 정보보호 제품을 분석하고, 국내 정보보호 제품 분류 체계를 제안한다. IV장에서는 국내·외 정보보호 제품의 시장 동향 및 기술 현황에 대해 살펴보고, V장에서는 차기 정보보호 제품 선정을 위해 국내 산업체의 의견 및 수요 조사를 위한 설문조사와 그 결과를 분석하였으며, VI장에서는 차기 정보보호 제품 15개를 선정하고 각 제품의 특징과 장·단점을 분석하며, VII장에서 결론을 맺는다.

II. 국제 공통평가기준 동향 및 분석

현재(2004년 6월) CCRA에 서명한 파트너로 인증서발행국(CAP: Certificate Authorizing Participants)은 미국, 영국, 프랑스, 독일, 캐나다, 호주/뉴질랜드, 일본이 있으며, 인증서수용국(CCP: Certificate Consuming Participants)은 네덜란드, 이탈리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴, 등이 있다^[1,12].

CC수용의 확대와 CCP 자격조건이 자국내 추가적인 비용을 수반하는 평가제도를 구비하지 않고도 CCRA에 참여할 수 있다는 점에서 CCRA의 확산이 가속화 될 것으로 예상되고, CC를 정보보호제품 평가에 활용하면서 실제 평가에 적용할 수 있는 요구사항들로 지속적으로 변화할 것으로 예상된다. 또한 CC와 ISO와의 연계를 포함한 다른 국제기구 및 국제 활동과의 연계과정에서 CC의 부단한 변화와 정보보호의 세계적 확산, 기술의 발전과 융합, 수요의 질적 변화 등을 적절하게 반영하기 위한 CC의 내용변화가 예상된다.

2.1 CCRA 정보보호 제품 분석

국제 공통평가기준의 보증평가등급은 EAL0에서

표 1. CCRA의 평가완료 제품과 평가중인 제품, 2003.8월말

구분	평가 등급				비고
	EAL1	EAL2	EAL3	EAL4	
DATABASE 용도 (Oracle 등)	11	23	17	47	총 99 종 평가완료 제품 (EAL5+ 제품이 1종 있음)
COMMUNICATION 용도 (Cisco 등)					
NETWORK 용도 (Firewall 등)					
OS 용도 (Sun 등)					
SMARTCARD 용도 (Phillips 등)					
ACCESS CONTROL 용도 (NSA 등)					
PKI 용도 (Entrust 등)					
In-Evaluation Product List (IEPL)	1	14	3	19	총 37 종 평가중인 제품

(참조 : <http://www.commoncriteria.org/> => 현재 <http://www.commoncriteriaportal.org/>)

※ 여기서 분석된 제품은 CC 체계하에서 평가된 제품만을 분석한 것이며, CCRA 홈페이지의 자료만을 참조했으므로 각국이 독자적으로 평가하고 이를 CCRA에 보고치 않은 제품은 누락될 가능성이 있음

EAL7등급으로 나누어져 있으며, 개발자는 해당 평가보증등급에서 요구하는 보증요구사항을 충족시키도록 평가제출물을 작성하여야 한다. 평가자는 제출된 평가제출물을 통해 TOE의 형상을 정확히 파악할 수 있으며, 구매자도 자신이 요구되는 보증사항들이 충족하는지를 파악할 수 있게 된다^[20].

우리는 차기 정보보호 제품 선정시 국외 평가된 제품 사례를 반영하기 위하여 2003년 8월말까지 CCRA 홈페이지에 등록된 평가완료 제품과 평가중인 제품의 통계 산출 결과는 표 1과 같다.

평가완료 제품중에서 Gemplus 사에 Gemplus

64k Java Card 제품이 유일하게 보증등급 EAL 5+를 받고 있다⁽⁷⁾.

III. 국외 평가된 정보보호 제품 분석 및 분류 체계 제안

본 장에서는 국내 정보보호 제품을 분류하기 위하여 미국, 영국, 호주의 평가된 정보보호 제품들을 분석하였다. 또한 분류된 제품에 대해서 별도의 분석 항목을 서술하지는 않았다. 제품들의 세부 분석들은 CCRA 홈페이지를 참조하기 바란다.

표 2. 미국의 정보보호 제품군

제품군	제품명	제품군	제품명
네트워크 인프라 정보보호 제품군	<ul style="list-style-type: none"> 스위치/라우터(switch and router) 라우터 무선 LAN 	네트워크간 정보보호 제품군	<ul style="list-style-type: none"> 방화벽(firewall) 가드(guard) 가상사설망(VPN) 원격 접근(remote access) 이동 코드(mobile code) 다중 영역 솔루션(multi-domain solutions)
컴퓨팅 환경 정보보호 제품군	<ul style="list-style-type: none"> 운영체제(operating system) 바이오메트릭(Biometric) 보안 메신저(secure messaging) 토큰(token) 단일-레벨 서버(single-level server) 민감한 데이터 보호 신뢰된 DBMS(trusted DBMS) PC 접근 제어(PC access control) 이동 코드(mobile code) 주변장치 공유 스위치(peripheral switch) 기타(misc-) 	인프라 지원 정보보호 제품군	<ul style="list-style-type: none"> 망관리(network management) 키복구(key recovery) 스마트카드(smart card) PKI/PMI 침입탐지시스템(IDS) 기타

3.1 미국의 정보보호 제품 분석

미국의 정보보호 제품들은 NIST의 산하 NIAP (National Information Assurance Partnership) 공통기준 평가 및 검증 기법과 CCRA의 기준 등에 준수하려 평가되고 검증된 제품 등이다. 목록상의 제품들은 미국 또는 IT 보안 평가를 위한 공통 기준에 순응하기 위하여 CCRA에 참여한 다른 나라들 중의 한 나라에 존재하는 인가/허가된 시설에서 평가되고 인가되었고, 검증된 제품들의 목록은 NIAP-CCEVS(Common Criteria Evaluation and Validation Scheme)로 평가된 제품들과 요구되는 평가 자료(ST와 최종 평가 보고서)를 제공했던 다른 나라의 기법에서 평가된 제품들로 구성된다. 다음의 표 2의 정보보호 제품군 구분은 미국 연방 정부가 마련한 PP의 존재에 따라서 구분한 것이다^(7,9).

3.2 영국의 정보보호 제품 분석

표 3의 영국 정보보호 제품들은 CESG의 홈페이지

지를 참조하여 분류하였다⁽⁸⁾.

3.3 호주의 정보보호 제품 분석

호주의 정보보호 제품들은 정보 보안의 적절한 수준을 선택하도록 도와주기 위하여 호주 정보 보안 평가 프로그램(AISEP: Australian Information Security Evaluation Program)을 위한 호주 인증기관인 DSD의 정보 보안 그룹에 의하여 만들어졌다. 표 4의 제품 목록들은 제품들이 합의된 보안 목표 설계서를 만족할만한 정도의 보증 수준을 제공하기 위하여 올바르고 효율적으로 동작한다는 것을 보증하기 위하여 자신의 보안성에 대한 세부적인 평가 절차를 거쳤다⁽¹¹⁾.

3.4 우리나라 정보보호 제품 분류 체계

우리는 미국, 영국, 호주의 정보보호 제품들의 분류체계를 반영하여 우리나라 정보보호 제품을 대분류와 중분류, 소분류로 다음과 같은 원칙으로 분류하였으며, CCRA 연구위원회를 통하여 검토하였다.

표 3. 영국의 정보보호 제품군

제품군	제품명
통신	• 데이터 암호화기 • 스위치 • 가드
데이터 삭제	• 데이터삭제
데이터베이스	• DBMS
네트워크링	• 방화벽 • VPN • 인증기관 • 등록기관
운영체제	• SUN의 솔라리스 8 • 소니사의 스마트카드 운영체제
PC 액세스 제어	• PC 액세스 제어 시스템
기타	• 다양한 PP

표 4. 호주의 정보보호 제품군

제품군	제품명
네트워크 보안 제품	• 방화벽 • 라우터 • 스위치 • VPN • 메시징 관리 • 네트워크 암호 • ATM 암호화기 • 신뢰된 네트워크 구분 장치 • 안전한 원격 액세스 • 보안관리
공개키 기술	• PKI 제품 • 공개키 클라이언트 제품
스마트카드	• 스마트카드 운영체제 • 스마트카드 응용
운영체제	• 솔라리스 • HP • AIX 운영체제
PC 보안	• PC 상의 민감한 데이터 및 등급화된 데이터 보호
생체기술	• 생체인증 제품
호스트 보안 모듈	• 암호학적 보안 모듈
기타	• 암호학적 지원 모듈 • 신뢰된 DBMS • 위성 암호화 장치 • 자장 중화 제품

○ 정보보호 제품군 분류 원칙

- 정통부의 2003년도 정보보호 5개년 개발 계획 (안)을 보면, 정보보호 제품의 분류는 대분류로 공통기반, 네트워크 및 시스템 보안, 그리고 응용 보안 분야로 설정되어 있으며, 공통기반은 다시 암호 분야와 인증 분야로 구분되어 있고, 시스템 및 네트워크 분야는 시스템 보안과 네트워크 보안 분야로 구분되며, 응용 보안 분야는 전자거래 분야와 서비스 이용 보호 분야로 구분되어 있다.
- 정보보호 제품군 분류는 대분류, 중분류, 그리고 소분류로 구분하였으며, 기본적으로 대분류는

표 2와 같이 미국의 CC 평가를 위한 제품군 분류를 기본으로 하였다. 다만, 네트워크 간과 네트워크 기반을 하나의 대분류로 통합하였다.

- 소항목의 설정은 미국, 영국, 호주에서 평가된 모든 정보보호 제품을 소분류 항목으로 선택하였고, 국내에서 현재 평가가 필요하다고 판단되고, 일정 규모 이상의 시장이 형성될 가능성이 있는 부분을 추가로 선정하였다(IPS, 취약성 분석도구, 불건전 정보 차단 도구 등).
- 중분류는 다시 소분류 정보보호 제품을 그룹핑하여 대분류에 넣고, 이를 다시 그룹핑하여 중분류 항목을 분류하였다. 중분류는 정통부의 정보보호

표 5. 우리나라의 정보보호 제품군 분류 체계

대분류	중분류	평가 대상 제품	대분류	중분류	평가 대상 제품
정보보호 기반 제품군	암호 지원 제품	<ul style="list-style-type: none"> • 암호학적 지원 모듈(암호 API 포함) • 암호학적 보안 모듈 • 자장 중화 장치(Eraser) • 기타 	네트워크 정보보호 제품군	네트 워크 기반(무선/ 모바일 보안, 망전환장치, 침입차단, 침입탐지)	<ul style="list-style-type: none"> • 라우터 • 스위치 • 게이트웨이 • 무선 LAN • 이동통신보안(이동단말, 기지국) • IDS(네트워크기반/호스트기반 침입탐지시스템) • IPS(네트워크기반/호스트기반 침입예방시스템) • ATM 암호화장치 • 위성 암호화장치 • xDSL 암호화 장치 • 전화기 암호화 장치 • 망관리장치 • 트래픽 관리장치 • 고속 네트워크 백본용 침입탐지/예방장치 • 기타
	보안 관리(S/W) 제품	<ul style="list-style-type: none"> • 항바이러스 및 취약성 점검도구 • 불건전정보차단도구 • 통합보안관리(ESM) • 위협분석도구 • 기타 			<ul style="list-style-type: none"> • 방화벽 • VPN • 가드(guard) • 다중영역 구분 보안제품 • 원격 접근(remote access) 제품 • 기타
	인증 솔루션(3A) 제품	<ul style="list-style-type: none"> • CA • RA • 권한관리기반(PMI) • OCSP • SCVP • DVCS • 시범확인 서비스 • DPD/DPV • KMI, 키복구 제품 • 공개키 클라이언트 제품 • Single Sign-on/EAM • 기타 			<ul style="list-style-type: none"> • 메일 보안(Anti Spam) 제품 • 기타
	생체 인식 제품	<ul style="list-style-type: none"> • 지문, 얼굴, 홍채, 정맥 • 서명, 화자인식 • 기타 			<ul style="list-style-type: none"> • 단일 레벨 보안 제품 • 기타
	보안 스마트카드 (USB 토큰, PCMCIA) 제품	<ul style="list-style-type: none"> • 칩 • COS(Chip Operating System) • 카드판독기 • 응용제품 • 기타 		<ul style="list-style-type: none"> • PC 보안 제품 • 기타 	
컴퓨팅 정보보호 제품군	운영체제 보안 제품	<ul style="list-style-type: none"> • 리눅스 기반 신뢰 운영체제 • 유닉스 기반 신뢰 운영체제 • 윈도우즈 기반 신뢰 운영체제 • 기타 	컴퓨팅 정보보호 제품군	공유 스위치	<ul style="list-style-type: none"> • 주변 장치 공유 스위치
	데이터베이 스제품	<ul style="list-style-type: none"> • 관계형 데이터베이스 • 기타 		이동 코드	<ul style="list-style-type: none"> • 이동 코드(mobile code)
				기타	

제품군 분류를 기본으로 하여 분류하였다.

정보보호 제품군 분류는 기본적으로 차기 평가대상 정보보호 제품군을 설정하는 연구의 기본 방향에서 보면 직접적으로 관련되어 있지 않고, 이에 대한 공통의 합의가 현재 나와 있지 않다. 연구 기관 또는 단체마다 다른 분류법을 적용하고 있다. 그래서 본 연구에서는 미국 CCRA의 정보보호 제품군 분류를 기본적으로 따랐으며, 중분류 제품 구분은 정통부의 분류를 참고로 하여 설정하였다. 이에 대한 이견은 있을 수 있으나, 설문이 최종 소분류 항목에 대하여 수행되었기 때문에 이는 본 연구의 결과에 크게 영향을 주지 않았다고 생각한다. 따라서 여기서 구분한 제품군 분류는 기본적으로 제품군 분류를 위한 참고 자료임을 밝힌다.

IV. 국내·외 정보보호 시장 동향 및 기술 현황

4.1 국내·외 정보보호 시장 동향

본 절에서는 국내·외 정보보호제품별 시장을 분석하여, 국내·외 정보보호제품의 성장 동향을 알아보고자 한다. 자료의 출처는 다음과 같다⁽³⁾⁽⁴⁾⁽⁵⁾.

4.1.1 세계 정보보호 시장

세계 정보보호 제품에 대한 시장규모와 특징을 분석한 결과, 세계 정보보호 시장은 2002년 200억 달러를 넘어선 것으로 파악되며, 연평균증가율 20.8%로 계속 증가될 것으로 전망된다. 또한 침입차단시스템/VPN이 가장 많았고, VPN, IDS는 네트워크 보안의 기초솔루션으로서 그 활용이 일반화되고 있으며, 세계 침입차단시스템/VPN시장은 침입차단시스템 소프트웨어 시장이 하드웨어 Appliance와 침입차단시스템과 VPN이 통합된 장비로 옮겨가는 추세에 있었다. 생체인식은 인간친화적 특성으로 인해 물리적 보안뿐만 네트워크 보안시장에서 크게 부각되고 있었으며, 2005년을 전후하여 급성장 할 것이며, 매년 30%이상의 급격한 성장세를 유지할 것으로 전망된다. 그리고 무선 인터넷보안은 시장은 작지만, 무선인터넷의 활용이 급증하면서 무선 정보보호 시장은 가장 큰 성장률을 보일 것으로 전망된다.

4.1.2 국내 정보보호 시장

국내 정보보호 제품에 대한 시장규모와 특징을 분

석한 결과, 국내 항바이러스 시장은 바이러스 침투의 다양화, 서버 등을 통한 바이러스 확산 등에 힘입어 꾸준히 증가할 것으로 전망되며, 국내 정보보호시장 중에서 시장점유율이 가장 높고, 안철수연구소와 하우리가 60% 이상의 시장 점유율을 차지할 것으로 예측된다. 그리고 국내 침입차단시스템은 e-business의 활성화 등 인터넷 기반사업의 증가에 힘입어 꾸준히 성장할 전망이다. 시장 자체가 성숙기에 접근하고 있어 성장률은 둔화될 전망이다. 국내 VPN 시장은 5, 6개 VPN전문업체들이 각축전을 벌이는 가운데 하반기 들어 급격히 외국계 솔루션업체들이 시장 진입을 확대하고 있으며 KT, 데이콤 등 통신사업자들도 VPN 서비스에 나설 방침이어서 경쟁이 더욱 가열될 것으로 전망된다. 그리고 침입탐지시스템은 시장이 형성되지 3-4년 밖에 되지 않았지만 시장에는 벌써 약 30여 개가 넘는 업체들이 시장에 진입하여 치열한 저가 경쟁을 벌이고 있고 IPS(Intrusion Prevent System)이 대두되어 있다. PKI 시장은 수년전의 폭발적인 성장전망에는 미치지 못하고 있으나, 사이버공간에서의 합리적 위험배분을 위한 유일한 대안인 점에 비추어 사용자 편의성, 설치·운영의 편의성, 상호연동성의 강화 등이 보완된다면 연평균 30%에 이르는 시장 성장이 기대된다. 국내 생체인식 시장은 지문인식 시장의 일시적 침체에도 불구하고 지문, 정맥, 홍채 및 음성에 대한 인식기술 및 장비가 개발되어 향후 5년간 급증가세 형태를 보일 것으로 예상된다. 최근 들어 무선 인터넷 서비스 및 그 사용자가 급속히 증가하고 있으며, 가까운 미래에 초고속 무선 인터넷을 기반으로 하는 IMT-2000 서비스 등이 개시되면 서비스 요구 및 사용 증가율은 더욱 커질 것으로 예측되고, 국내에서는 기존 이동통신 사업자들이 무선인터넷 시장을 주도하고 있는 가운데, 금융·증권업무 등에 무선인터넷을 활용하려는 움직임이 크게 일면서 무선인터넷 보안기술에 대한 관심이 고조되고 있다.

4.2 국내·외 정보보호기술 현황 및 전망

본 절의 내용은 “정통부의 정보보호 기술개발 5개년 계획 초안”을 참고로 하여 작성되었음을 밝힌다⁽¹⁷⁾. 국내 정보보호기술은 크게 공통기반기술(암호기술, 인증기술), 시스템·네트워크보호기술, 응용보호기술(전자거래보호기술, 서비스이용보호기술)로 나눌 수 있으며, 정보보호기술 현황 및 전망은 참고문헌

[17]을 참조하면 자세히 알 수 있다.

V. 설문조사

본 장에서는 차기 평가 대상 정보보호 제품군 선정을 위하여 정보보호 산업체를 대상으로 설문조사를 하였다.

5.1 평가 대상 제품 수요 분석

o 설문 목적 :

- 우리나라는 CCRA 가입을 준비 중이므로, 국내에서 수행하고 있는 CC 평가를 위한 제품군의 확대가 필요함

o 설문 대상 :

- 한국정보보호산업협회, 전자지불포럼, 생체인증포럼, 그리고 정보보호 관련 연구기관과 교육기관 관계자를 통해 설문을 실시하였음
- 설문 응답율은 한국정보보호산업협회가 35%로 가장 높고, 전자지불포럼의 설문 응답율이 가장 낮았음
- 한국정보보호산업협회 조직 위원회 업체는 60% 이상 설문 응답을 받았음
- 대표적인 설문업체는 (주)하우리, 안철수연구소, (주)해커스랩, (주)장미디어, (주)시큐아이닷컴 등의 국내 우수 정보보호 업체들이 응답하였음

o 조사 기간 및 방법

- 조사기간: 7월 31일 ~ 8월 30일
- 조사방법: 이메일 후 전화조사

o 조사결과

- 총 60개사 응답

5.1.1 설문 대상 업체 및 응답 업체 분석

표 6. 설문 대상 업체 및 응답율

설문 대상	회원사 수	설문 대상 업체	응답율
한국정보보호산업협회	135	47	약 35%
전자지불포럼	52	5	약 10%
생체인증포럼	20	5	약 25%
기타	3	3	100 %
계	210	60	약 29 %

5.1.2 설문 답변자의 생산(판매) 또는 관심 여부

설문 응답자의 소속 업체에서 현재 생산하고 있거나, 추후 생산 예정인 정보보호 제품에 대한 사항을 알아보기 위한 항목으로 중복 선택이 가능하였다. 가장 높은 관심도를 보인 중분류 항목은 전체 응답자의 24%가 관심이 있다고 응답한 네트워크 기반 정보보호 제품군이다. 이는 인터넷에서의 정보보호의 중요성이 대두되고 있고, 이미 큰 정보보호 시장을 구축하고 있기 때문인 것으로 분석된다.

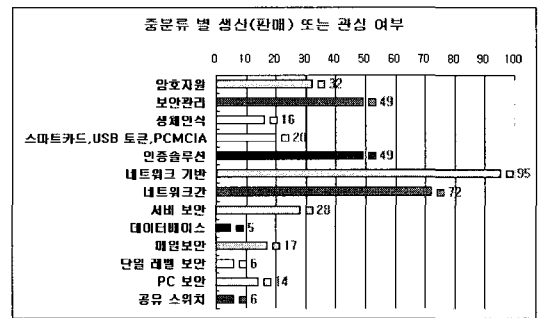


그림 1. 중분류 별 생산(판매) 또는 관심 여부

5.1.3 설문 답변자의 평가 요망 시기 및 제품 인지도 항목 분석

응답자가 향후 5년에 걸쳐 정보보호 제품의 평가 기준의 필요성과 그 적절한 시기를 알아보기 위한 항목이며, 2004년과 2005년에는 이미 정보보호 시장의 활성화가 된 제품을 중심으로 응답을 하였고, 제품 관련성과 인지도 항목에서도 현재 큰 시장을 형성하고 있는 제품이 높은 인지도를 갖고 있다고 분석되었다.

본 항목의 설문 결과로, 암호지원 제품에 대한 평가 요망 응답은 2004년 암호학적 지원모듈의 평가 요망의 수(7명)가 가장 많았고, 보안관리 제품에 대한 평가 요망 응답은 2005년 통합보안관리(ESM)의 평가 요망의 수(9명)가 가장 많았으며, 생체인식 제품에 대한 평가 요망 응답은 2004년 생체인식의 지문, 얼굴, 홍채, 정맥의 평가 요망의 수(8명)가 가장 많고, 스마트카드, USB 토큰, PCMCIA 제품에 대한 평가 요망 응답은 2004년 응용제품 평가 요망의 수(4명)가 가장 많은 것으로 나타났다. 그리고 인증 솔루션제품에 대한 평가 요망 응답은 2004년 CA 평가 요망의 수(6명)가 가장 많았고, 네트워크 기반제품에 대한 평가 요망 응답은 2004년 IPS(네트워크/호스트기반 침입 예방 시스템)의 평가 요망의 수(10명)가 가장 많았으며, 네트워크간 제품에 대한

표 7. 평가·인증 또는 시험의뢰 현황

번호	평가·인증 또는 시험 내역 (제품명, 시험기관, 정부/민간 평가기관, 평가등급, 국가)	분야			
		성능	보안성/보증	표준적합성	기타
1	얼굴인식 시스템, NIST, 정부평가기관, n/a, 미국	1			
2	Access Control system CE, EU	1			
3	VP-II System ETL(시험대행업체), 정부평가기관, 전자과적합등록, 한국			1	
4	VP-II System ETL(시험대행업체), 정부평가기관, FCC Part15.105/15.21, 미국			1	
5	VP-II System ETL(시험대행업체), 정부평가기관, 89/336/ECC, 유럽			1	
6	PC보안, 정보통신기술협회 GS(Good Software) 한국		1		
7	Firewall, KISA, 정부평가기관, K4E, 한국		2	1	
8	IDS, KISA, 정부평가기관, K4E, 한국	2	6	3	1
9	VPN, KISA, 정부평가기관, K4E, 한국	1	2	2	진행
10	Firewall, CMG, 민간평가기관, EAL3, 호주		1		
11	Firewall, ICASA, 민간평가기관, n/a, 미국	2	3	3	1
12	Firewall/VPN 미국 NSA	1	1	1	1
13	Firewall/VPN 미국 Tolly	1	1	1	1
14	키보드입력 정보보호제품(컴퓨세이프)/국정원/정부평가기관 보안 검토필 제품/한국	1	1	1	1
15	통합 PC 보안(세이프 아일랜드)/국정원/정부평가기관/보안 검토필 제품/한국	1	1	1	1
16	IDS, ICASA 민간평가기관 n/a 미국		1		
17	IDS(리눅스 기반), KISA, 정부평가기관, K2, 한국		1	1	
18	IDS 중국공안부, 정부평가기관, 중국공안부인증, 중국		1	1	
19	INITECH CA, Identrus 민간평가기관, n/a, 미국			1	
20	INITECH Crypto, NIST, 정부평가기관, n/a, 미국			1	
21	하이자드, 국보연, 국정원, 보안성평가 한국		1	1	
22	안티바이러스, 웨스트코스트랩, 민간평가기관, 체크마크, 영국	1			
23	안티바이러스, VirusBulletin, 민간평가기관, 100%, Award, 영국	1			
24	안티바이러스, ICASA, 민간평가기관, n/a, 미국	1			
25	SPIDER-1(ESM), Checkpoint, 민간평가기관, OPSEC, 미국	1	1	1	
26	CA/RA, 국정원보안성평가, Identrus 상호연동성		1	1	
27	암호, 국정원보안성평가		1		
28	EAM, 국정원보안성평가		1		
29	OCSF, Identrus 상호연동성			1	
30	SecureShield-Firewall V1.0, KISA, 정부평가기관, K4, 한국		1		
31	수호신 V2.0, KISA, 정부평가기관, K4E, 한국		1		
32	수호신 V3.0(AIX4.3), KISA, 정부평가기관, K4E, 한국		1		
33	수호신 V3.0(X86), KISA, 정부평가기관, K4E, 한국		1		
34	수호신 V3.0(SPARC), KISA, 정부평가기관, K4E, 한국		1		
35	수호신 IDS V1.0(SPARC), KISA, 정부평가기관, K4, 한국		1		
36	수호신 IDS V1.0(X86), KISA, 정부평가기관, K4, 한국		1		

표 8. 평가 인증 요청 사유

평가 인증 요청 사유란 표시를 위한 항목들		
1	국내외시장에서 자사 제품의 판매 촉진 기대	68
2	제품의 신뢰성과 공신력 확보	157
3	시장 요구 및 제품 사용자 요구	95
4	정부 정책에 호응하기 위해	1
5	국제적인 조류이기 때문에	18
6	기타	1

표 9. 평가 인증 거부 사유

평가 인증 거부 사유		
1	국내외시장에서 자사 제품판매에 별로 영향을 줄 것 같지 않음	0
2	평가된 제품이 하향 평준화되고 있는 추세여서 시장 개척 및 판매에 도움이 되지 않을 것으로 예측됨	0
3	제품의 공신력과 신뢰성 향상에 도움이 될 것 같지 않음	3
4	인력 및 시간의 추가 투입으로 인한 부담이 큼	8
5	평가 인증이 정부에 의한 새로운 규제로 인식됨	5
6	평가 인증 제도에 대하여 잘 모름	0
7	기타	6

은 응답이 있었다.

o 기타 사유

- 관심제품이 이미 평가되었음
- 당사 제품은 평가 대상이 아님
- 평가항목자체가 없음
- 솔루션 개발업체가 아니라 평가 인증 신청이 없음
- 미국본사에서 일괄적으로 평가, 국내 재평가의 미 없음(2개사)
- 국내의 CC의 경우 기존의 K4 등급과 같은 등급을 받으려면 소스코드를 공개해야 하므로 기피

Ⅶ. 차기 평가 대상 정보보호 제품군 선정

o 평가 방법

평가 항목은 외국 CCRA 가입국의 평가 사례, 국내 산업체의 수, 생산 또는 관심 여부 항목에 대한 응답 결과, 평가 시기에 대한 응답 결과, 그리고 사용자 요구를 반영하기 위한 행정정보보호 제품 포함

여부 등으로 구성된다.

- 외국 사례: CCRA 평가 제품 수(평가 진행중 및 완료된 제품 수)
- 설문 조사 결과 1: 제품의 생산 또는 관심 여부를 점수화함
- 설문 조사 결과 2: 설문 답변자의 평가 요망 시기를 점수화함
 점수계산 = ((2004년*5) + (2005년*4) + (2006년*3) + (2007년*2) + (2008년 이후))/응답수
- 행정정보보호시스템: 행정 정보보호용 시스템 목록 포함 여부, 2등급 평가
- 등급 조정 방법: 각 항목의 최소값과 최대값을 기준으로 5등급으로 구분하고, 이를 각각 등급화 함

o 최종 평가 점수 산출

최종 점수를 계산하기 위하여 중요도에 따라, 외국 사례, 국내 산업체 수, 행정정보보호 제품은 가중치를 1로 주고, 설문조사 2인 향후 생산 여부 및 관심 여부는 가중치 2로 주었으며, 설문조사 3인 평가요망 시기를 가중치 3으로 주어 전체 점수를 계산하였다. 정보보호 제품 평가 확대는 매년 3개 제품씩 추가로 시행한다고 가정하고, 5년을 기준으로 15개의 정보보호 제품을 선정하였다.

- 종합 점수 산정시 가중치
 - 외국사례 (가중치1) + 국내 산업체 수 (가중치1) + 설문조사(1) (가중치2) + 설문조사(2) (가중치3) + 행정정보보호용 시스템 (가중치1)
- 종합 평가: 전체 소분류의 종합 점수를 기준으로 최고 점수로부터 15개 정보보호 제품을 선정함. (2003년까지 평가되고 있고, 2004년에 평가 예정인 정보보호 제품은 선정에서 제외함)

6.1 제품 선정 점수표(기 선정 제품 포함)

다음 표 10은 기 평가 중이거나 예정인 정보보호 제품을 포함한 평가 우선순위를 나타낸 결과이다. 기 평가중이거나, 평가 예정인 제품은 높은 순위를 가짐을 알 수 있다.

6.2 선정 예측 제품(기 선정 제품 제외)

그럼 5는 기 평가 중인 정보보호 제품과 2004년에 평가 예정인 정보보호 제품을 제외한 15개 정보보호 제품을 선정한 결과이다.

표 10. 제품 선정 점수(기 선정제품 포함)

소분류	외국사례	산업체	설문조사(1) (생산 또는 관심제품)	설문조사(2) (평가요망 및 필요시기)	행정정보 보호용 시스템	종합점수	순위
IDS(침입예방시스템)	3	5	4	5	5	36	1
방화벽	5	3	4	5	5	36	1
VPN	5	3	4	5	5	36	1
지문, 얼굴, 홍채, 정맥	1	5	4	5	5	34	4
CA(Certificate Authority)	2	4	4	5	5	34	4
유닉스 기반	4	2	3	5	5	32	6
윈도우즈 기반	4	2	3	5	5	32	6
PC 보안	2	4	3	5	5	32	6
RA(Registration Authority)	2	4	3	5	5	32	6
IPS(네트워크/호스트기반 침입예방시스템)	3	5	4	5	0	31	10
망관리장치	3	5	1	5	5	30	11
리눅스 기반	4	2	2	5	5	30	11
응용제품	2	2	3	5	5	30	11
통합보안관리(ESM)	1	3	5	5	0	29	14
Single Sign-on(EAM)	2	4	4	5	0	29	14
무선 LAN	3	5	3	5	0	29	14
다중영역 구분 보안제품	5	3	2	4	5	29	14
권한관리기반(PMI)	2	4	3	5	0	27	18
공개키 클라이언트 제품	2	4	3	5	0	27	18
이동통신보안	3	5	2	5	0	27	18
암호학적 지원 모듈(암호 API 포함)	1	2	4	5	0	26	21
암호학적 보안 모듈	1	2	4	5	0	26	21
고속 네트워크 백본용 침입탐지/예방 장치	3	5	3	4	0	26	21
칩	2	2	1	5	5	26	21
COS(Chip Operating System)	2	2	1	5	5	26	21
카드판독기	2	2	1	5	5	26	21
항바이러스 및 취약성 점검도구	1	3	3	5	0	25	27
OCSP(Online Certificate Status Protocol)	2	4	2	5	0	25	27
시범확인 서비스(Time Stamping Service)	2	4	2	5	0	25	27
DVCS(Data Validation & Certification Server)	2	4	2	5	0	25	27
KMI, 키복구제품	2	4	2	5	0	25	27
라우터	3	5	1	5	0	25	27
스위치	3	5	1	5	0	25	27
게이트웨이	3	5	1	5	0	25	27
ATM 암호화장치	3	5	1	5	0	25	27
위성 암호화장치	3	5	1	5	0	25	27
xDSL 암호화 장치	3	5	1	5	0	25	27

표 10. 제품 선정 점수(기 선정제품 포함)(계속)

소분류	외국사례	산업체	설문조사(1) (생산 또는 관심제품)	설문조사(2) (평가요망 및 필요시기)	행정정보 보호용 시스템	종합점수	순위
전화기 암호화 장치	3	5	1	5	0	25	27
가드(guard)	5	3	1	5	0	25	27
원격 접근 제품	5	3	1	5	0	25	27
트래픽 관리 장치	3	5	2	4	0	24	41
SMIME 메일보안 제품	1	2	3	5	0	24	41
불건전정보차단도구	1	3	2	5	0	23	43
위험분석도구	1	3	2	5	0	23	43
SCVP(Simple Certificate Validation Protocol)	2	4	1	5	0	23	43
웹서버 보안	1	1	2	5	0	21	47
주변 장치 공유 스위치	1	1	2	5	0	21	47
서명, 화자인식	1	5	1	4	0	20	49
DPD/DPV	2	4	1	4	0	20	49
PGP 메일보안 제품	1	2	1	5	0	20	49

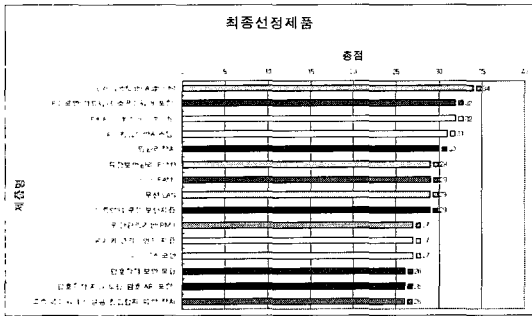


그림 5. 최종선정 제품

- o 종합점수가 같을 시 다음과 같이 우선순위를 정함
 - 가중치 -> 산업체수 -> 외국사례 -> 행정정보보호용 시스템
 - 순위 2-3에서,
PC보안은 행정정보보호용 시스템에서 PKI 보다 제품수가 높음으로 우선순위
 - 순위 10-11에서,
PMI는 공개키 클라이언트 제품보다 시장 규모와 미래 발전 전망이 더 크고, 공인인증기관 심사기준이 공개키 기반구조만을 대상으로 하므로 PMI에 우선순위를 부여함
 - 순위13-14에서,

암호학적 보안 모듈이 하드웨어 제품이므로 시장 규모가 더 클 것으로 예측되어 높은 우선순위를 부여함

6.3 연도별 평가대상제품군 선정

선정된 정보보호 제품군을 중분류 단위로 선정을 하면 다음과 같은 5차년도의 제품군 선정이 된다.

1차년도로 선정된 PC보안 제품은 데이터의 도난과 비인가된 사용을 막기 위한 접근 제어 메커니즘을 제공하고, 사용자의 신분확인과 패스워드를 통한 불법적인 액세스 제어 방지, 사용자보안 프로파일을 이용한 비인가된 파일 액세스 제어, 악의적인 악성 코드의 전파 방지, 비인가된 플로피 디스켓의 사용금지 등의 기능을 제공하는 제품들이다. 4차년도의 IPS는 자가 측정(인공지능) 기능으로 공격신호를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이뤄지는지를 감시하며, 자동으로 방어조치를 취하는 침입예방 시스템이다. 현재 SECUWORKS IPSWall 2000 v1.0, 3000 v1.0이 IDS PP와 방화벽 PP를 준용하여 KISA에서 EAL3+ 등급으로 평가중에 있다 (2004. 8).

표 11. 연도별 평가대상제품군 선정

중분류	소분류	평균 점수	연도별 순위
PC 보안	PC 보안	32	1차년
무선 LAN	무선 LAN	29	2차년
PKI/PMI 및 키복구	CA/RA, Single Sing-on, PMI(권한관리기반), 공개키 클라이언트 제품	28.8	3차년
네트워크기반 정보보호제품	IPS, 망관리장치, ESM(통합보안관리), 다중영역 구분 보안제품, 이동통신보안, 고속 네트워크 백본용 침입탐지/예방 장치	28.7	4차년
암호지원제품	암호학적 보안 모듈, 암호학적 지원 모듈(암호 API 포함)	26	5차년

※ 평균 점수 = 소분류 제품의 종합 점수의 총합 / 소분류 제품 수

6.4 선정 제품의 평가 및 분석

다음의 표 12는 차기 선정 평가 대상 인증 제품 현황 및 문제점과 특이사항을 분석한다.

6.5 평가대상 제품 선정(안)

다음의 표 13은 차기 선정 평가 대상 인증 제품의 평가시에 장점과 단점과 기대효과를 분석한다.

Ⅷ. 결 론

우리는 지금 CCRA 가입을 앞두고 있는 시점이다. 따라서 가입 후 이를 극대화하기 위하여 인증서를 발행할 수 있는 CAP 국가로 가입이 필요하고, 정보보호제품을 수출하고자 하는 국가 및 구매자들의 지속적인 동향 파악과 이들의 요구사항을 만족시킬 수 있는 평가 기술 확보를 위해 많은 연구와 준비가 필요하다. 본 논문에서는 국내 차기 평가대상 제품군을 선정하기 위하여 외국의 평가 대상 제품 분석, 평가대상 제품의 특성 분석, 국내의 정보보호 제품 시장 동향, 산업체의 설문 조사 및 분석 결과, 사용자의 요구를 고려하여, 평가대상 정보보호 제품군을 일년에 3 제품씩 확대된다고 가정하고, 총 5년동안 15개 정보보호 제품을 선정하였다. 또한 선정된 제품군에 대한 특성과 장단점을 분석하였다. 이의 근거는 2004년에 3개 제품을 확대한 사례를 따랐다. 그러나 만약 년차별 평가 대상 제품수가 줄어든다면, 선정된 우선순위에 따라 확대하는 것도 가능하다.

주요 연구 결과는 선진국에서 평가 완료 또는 진행 중인 제품군을 제시했으며, 각제품의 특성을 살펴 보았고, 방화벽, VPN, 스마트카드, 무선 랜 등의 국내의 정보보호 제품에 대한 시장 동향을 향후 5년 까지 제시했다. 2004년도 추가된 평가 제품군은 생체인식 제품군의 지문 제품, 스마트카드 제품군의 COS(Chip Operating System), 스마트카드 응용 제품, 운영체제보안 제품군의 윈도우즈, 리눅스, 유닉스 기반의 정보보호 제품 등이 있다. 설문 분석 결과 이들 제품군은 차기 정보보호 선정시에도 상위 그룹을 차지하고 있음을 알 수 있었다. 또한 설문 조사 결과, 사용자 요구, 국내 산업체 수요 등을 고려하여 차기 평가대상 정보보호제품을 2005년에서 2009년까지 15개 제품으로 선정 하였다. 선정된 제품은 CA, PC 보안, IPS(침입예방시스템), 망관리장치, 통합보안관리(ESM), Single Sign-On(EAM), 무선 랜, 다중영역장치 구분 보안제품, RA, 권한관리기반(PMI), 공개키 클라이언트 제품, 이동통신보안, 암호학적 지원모듈, 암호학적 보안모듈 그리고 마지막으로 고속 네트워크 백본용 침입탐지/예방 장치 등이다. 이와 같이 분류된 제품을 다시 그룹핑하여 장단점과 특성을 분석하였다. 분석 결과는 차기 평가대상 제품 선정을 위한 근거 자료 제시시에 이용 될 수 있다.

본 논문의 결과는 차기 정보보호 평가 제품 선정을 위한 정책 자료로 활용 가능하며, 향후 평가대상 선정을 위한 정책 결정을 할 정책 입안자, 구체적인 평가 계획을 수립할 평가기관, 그리고 평가를 준비할 정보보호 산업체에서 폭넓게 활용 될 수 있을 것이다.

표 12. 차기 선정 평가 대상 인증 제품 현황 및 문제점

중분류	제품분류	업체현황		문 제 점	특이사항
		개별	업체수		
암호지 원제품	▶암호학적 지원 모듈 (암호 API 포함) ▶암호학적 보안 모듈	▶4개 ▶4개	▶4개사	▶국내 시장 규모가 미미함 ▶암호 알고리즘의 설계 및 분석, 그리고 개발 측면에서 선진국과의 기술 격차가 4-5년 이상이 될것으 로 판단됨 ▶외국의 암호 응용 제품이 발빠른 대처로 국내 암호지원제품 시장을 잠식할 우려가 있음	▶최근 암호기술은 국가적 차 원의 프로젝트를 통해 차세 대 암호알고리즘을 선정하 고 있는 추세임 ※ 미국은 NIST에서, 유럽은 NESSIE에서, 일본은 CRYP TREC에서
PKI /PMI 및 키복구	▶CA(Certificate Authority) ▶통합보안관리(ESM) ▶RA(Registration Authority) ▶권한관리기반 (PMI) ▶Single Sign-on(EAM) ▶공개키 클라이언트 제품	▶10개 ▶4개 ▶10개 ▶4개 ▶5개 ▶4개	▶10개사	▶이미 공인 인증기관 지정시 평가 기준이 존재하여, 이종의 평가 소 지가 있음 ▶공인 인증기관만이 제품 구매자가 되어 시장이 매우 협소함 ▶PKI 관련 국제표준이 많이 있으 나, 이를 모두 만족할 제품을 생 산하기가 매우 어려움 ▶ESM의 경우 새로운 표준 개발 및 적용이 필요함	▶전자서명법에 의하여 6개 공인인증기관이 존재함 ▶사실 인증기관이 국내의 경 우 존재할 수 없음 ▶해외 시장 개척을 위해서 필요한 분야임
네트 워크 기반 정보 보호 제품	▶IPS(침입예방시스템) ▶망관리장치 ▶이동통신보안 ▶고속 네트워크 백본 용 침입탐지/예방 장치 ▶다중영역 구분 보안 제품	▶5개 ▶5개 ▶5개 ▶3개	▶5개사	▶네트워크 기반 정보보호제품은 기 반 기술의 낙후성으로 인하여 외 국의 주요 업체가 국내 시장을 독 점하고 있음 ▶이동통신 보안 분야의 경우, 독자 시장 규모와 외국 제품과의 호환 성을 고려하여 하나의 표준에 합 의하지 못하고 있음	▶1.25 인터넷 침해 사고 이후 에 중요성이 급증하고 있는 분야임. 특히, IPS, 고속 네 트워크 백본용 침해 대응장 치의 개발이 요구되고 있음 ▶무선 단말기 사용의 증가와 이를 통한 무선 데이터 통신 사용의 확산으로 모바일 환 경에서의 응용서비스가 활성화 되며, 차후 유·무선 통합 환경하에서 응용서비스가 폭 발적으로 증가될 것으로 예 상됨
무선 LAN	▶무선 LAN	▶5개	▶5개사	▶외국 경우의 무선랜의 표준을 채 용하여 상용화 단계에 이르렀으 나, 국내 기술은 아직 연구 개발 단계 ▶국내외 적으로 향후 시장 규모가 클 것으로 예측됨	▶무선 LAN은 이동성, 유연성, 휴대성, 간편성 등의 이점으 로 인해 beyond IMT-2000 이동 통신망의 유력한 무선 접속망 대안으로 등장
PC 보안	▶PC 보안	▶4개	▶4개사	▶개인 정보보호 인식의 증대 필요 ▶민간 수요보다는 공공 분야에 한 정된 수요를 가지고 있음 ▶백신을 유료로 이용하기 보다는 무료로 이용할 수 있다는 사용자 의 인식으로 인하여 시장 형성의 장애 요인이 되고 있음 ▶PC 보안의 근간인 암호 분야의 원천 기술의 부족	▶최근 개인정보의 중요성이 인식되면서, 개인 PC 방화 벽, 백신, 그리고 파일보호 시스템의 수요가 급증할 것 으로 예측됨

표 13. 평가 대상 선정(안)

중분류	소분류	장점	단점	기대효과
암호지원 제품	암호학적 지원모듈 암호학적 보안모듈 (암호 API 포함)	<ul style="list-style-type: none"> ▶ 암호제품 생산 및 연구 개발로 국내 독자적인 암호 구현 기술 달성 ▶ 고속 핵심 암호칩 안전성 평가 가능 ▶ 국내 암호기술의 기반 산업을 강화시킬 수 있음 ▶ 다양한 암호 알고리즘으로 고속 암호 라이브러리 개발 가능함 	<ul style="list-style-type: none"> ▶ 암호 알고리즘의 설계 및 분석, 그리고 개발 측면에서 선진국과의 기술력 차이 및 지적 재산권 문제가 있을 수 있음 ▶ 국내 독자 시장 형성이 의문임 ▶ 외국에 비해 고비도 암호기술이 부족함 	<ul style="list-style-type: none"> ▶ 앞으로 표준화가 중비도/고비도 암호 표준들의 맞추어 실현 암호 모듈 및 API 개발 가능하게 함 ▶ 고속 암호칩 개발 기폭제 ▶ 독자적인 시장 구축을 자극할 수 있음
PKI/PMI 및 키복구	CA/RA	<ul style="list-style-type: none"> ▶ 전자상거래, 인터넷뱅킹, 민원서류발급 등 위·변조 및 부인방지를 예방이 필요할 전 사회 영역에 수요증가로 인증기관 또한 증가 될 전망 ▶ 전자 정부의 CA 안전성을 제고 할 수 있음 ▶ 외국 PKI 시장 공략시 국내 CC 평가 제품이 유리 할 것으로 예측 	<ul style="list-style-type: none"> ▶ 국내 공인 인증기관 평가 기준이 있어서 이중의 평가가 될 수 있음 ▶ 6개의 공인 인증기관에서 국내 수요를 해결하고 있으므로 국내 시장의 포화로 인하여 외국 시장의 개척이 요구됨 	<ul style="list-style-type: none"> ▶ 전자상거래시 인증서를 통한 상호간의 신뢰성 확보 ▶ 스마트카드, 생체인증 등의 분야와 접목하여 소비자의 편리성, 응용성, 안전성의 요구를 충족 ▶ 급속도로 발전하는 무선랜에서 사용되는 무선 인증서에도 적용 가능함
	통합보안관리(ESM)	<ul style="list-style-type: none"> ▶ 세계 표준이 없으므로 국내 표준을 통한 세계 ESM 시장을 주도 가능함 ▶ 향후 정보보호 제품 시장에서 ESM 제품이 지속적인 수출품으로 증가 될 것으로 기대됨 	<ul style="list-style-type: none"> ▶ 국외 표준이 없으므로 국내 표준에만 의존할 수 있음 ▶ 관리되는 보안 제품의 범위, 관리를 위한 프로토콜, 데이터 구분 등의 표준이 부재함 	<ul style="list-style-type: none"> ▶ ESM을 위한 API모듈을 개발해 ESM 제품간의 연결 통로로 활용 가능함
	권한관리기반(PMI)	<ul style="list-style-type: none"> ▶ 공개키 기반 구조의 한계를 극복하기 위한 권한관리 기반 구조 시장이 점차로 커질 것으로 예측되고 있음(매년 30%의 성장률로 2006년 882억) ▶ 최근 IETF에서도 속성 인증서와 권한 인증서에 대한 표준이 현재 개발되고 있음 	<ul style="list-style-type: none"> ▶ 국외 PMI 제품에 대한 국내 PMI 제품의 기술 수준이 낮은 것으로 판단됨 	<ul style="list-style-type: none"> ▶ PMI의 발전은 PKI의 발전에 기여함 ▶ 한번 로그인으로 다양한 자원 및 시스템에 접근을 결정할 수 있으므로 단일화된 인터페이스 기능을 구현해 업무의 효율성과 보안성을 높일 수 있음
	Single Sign-on (EAM)	<ul style="list-style-type: none"> ▶ 최근 보안 응용솔루션으로 기업의 인터넷 시스템과 웹서비스가 대폭 확장됨에 따라 인증시스템을 간결화 함 ▶ 공공기관에 많은 도입이 예상되어 이에 대한 안전성 평가가 필요함 	<ul style="list-style-type: none"> ▶ 국내 민간 분야의 경우 고가 비용 때문에 설치를 꺼려하는 경향임 	<ul style="list-style-type: none"> ▶ 인증된 사용자에게 시스템 정보 및 자원에 접근할 수 있는 권한 부여 및 접근제어 권한까지 부여하는 PMI와 궁극적으로는 연동 될 것임
	공개키 클라이언트 제품	<ul style="list-style-type: none"> ▶ 전자상거래, 인터넷뱅킹 등에서 안전성을 위해 인증서를 많이 사용하는데, 공개키 클라이언트의 부하를 줄일 수 있는 기술이 발전하고 있는 추세 ▶ PKI 확장과 더불어 간결한 공개키 클라이언트 제품에 대해 평가가 요구됨 	<ul style="list-style-type: none"> ▶ 인증서 검증을 위한 클라이언트의 부하를 줄일 수 있는 기술이 필요 ▶ 클라이언트의 안전성을 위한 기술 필요 	<ul style="list-style-type: none"> ▶ 유무선 서비스를 고려한 타원곡선 암호 알고리즘의 적용이 요구됨

표 13. 평가 대상 선정(안)(계속)

중분류	소분류	장 점	단 점	기 대 효 과
네트워크 기반	IPS(네트워크/호스트 기반 침입예방시스템)	▶ 1·25 인터넷 대란 이후 IDS의 한계를 극복하고 모든 패킷에 대한 침입을 예방뿐만 아니라 자가 대응 조치, 공격자의 대한 역추적 기능이 추가되어서 현재 정보보호 분야에서 급속도로 증가하고 있음	▶ 제품에 대한 명확한 정의가 아직 이루어지고 있지 않아서 평가 범위 결정시 어려움이 예상됨 ▶ IDS과 IPS를 같이 사용할 경우 동시에 오류 경보를 발생 시킬 가능성이 있음	▶ Firewall과 IDS, Secure OS의 보안 기술을 기반으로 IPS 기술이 이루어지므로 다른 영역 발전에 기여 ▶ IPS 기술의 발전은 통합 보안솔루션으로 발전에 기여
	망관리장치	▶ 망관리장치를 위한 보안 프로토콜이 기 표준화되고 있음 ▶ 고속네트워크망과 무선네트워크망을 위한 광범위한 보안솔루션이 요구되고 있음	▶ 망관리장치를 위한 보안솔루션 업체는 많으나 평가 기술 미확보 ▶ ISP만이 사용하므로 시장 규모가 크지 않음	▶ 국내 안전한 네트워크망 구축을 위한 기술에 기여
	이동통신보안	▶ 세계 197개국 8억 6천만명이상이 사용하고 있고, 이동통신을 이용한 사용자들의 다양한 서비스를 지원하기 위해 이동통신보안이 증가하는 추세	▶ 국내에서는 기존 이동통신사업자들이 무선인터넷 시장까지 주도할 우려 ▶ 표준의 부재 및 수용자의 평가 요구가 크지 않은 분야임	▶ 이동통신 가입자인증모듈(USIM)을 위해 이동통신, 스마트카드 보안 기술 발전에 기여
	고속 네트워크 백본용 침입탐지/예방 장치	▶ 테라급의 고속 차세대 네트워크 정보보호 장치 개발이 추진되고 있음 ▶ 선로 속도로 연동될 수 있는 고속의 정보보호 장치가 요구됨	▶ 초고속망의 속도에 비해 현재 정보보호 하드웨어(칩 등)의 부재 ▶ 현재 개발 중인 제품으로 평가 범위, PP개발이 어려울 것 같음 ▶ 고속 패킷 처리기술이 미흡하여 많은 연구 개발이 필요함	▶ 초고속 통신망을 지원할 수 있는 암호 알고리즘 및 하드웨어 개발에 기여 ▶ 제품 개발이 2005년 완료될 예정이어서 평가 시기의 완급 조정이 필요
	다중영역	▶ 외국 수출용으로 평가가 필요	▶ 국내 시장이 거의 형성되지 않았음 ▶ 다중 등급을 갖는 네트워크 부재로 국내 사용자 요구가 크지 않음	▶ 평가 파급 효과가 낮을 것으로 예상됨
무선 LAN	무선 LAN	▶ 무선랜 접속 제어 서비스에 대한 요구가 급격히 증가할 것으로 예측됨 ▶ 정보통신부는 이용자의 급증으로 인한 '무선랜 보안 운영 권고지침'을 배포하고, '무선랜 정보보호 계획'을 마련하고 있음	▶ 사업자, 운영자 등이 무선랜 정보보호 인식이 부족하고 기본적인 보안조치 실천도 미흡	▶ 무선랜 장비업체 모임인 Wi-Fi의 단체표준을 준용하므로 상호 호환성이 기대 됨
PC 보안	PC 보안	▶ PC보안은 파일의 암호화와 접근통제에 있어 PC상에서의 정보보호는 반드시 필요하므로 중요성이 급증 ▶ 향후 정보보호 제품 시장에서 PC보안 제품이 지속적인 수출품으로 증가 될 것으로 기대됨 ▶ 생체 인식 제품과 결합이 요구됨	▶ 국내 정보보호 업체 기술이 아직은 국의 업체들에 비해 기술력이 부족 ▶ 여러 기술이 하나의 제품으로 수렴됨에 따라 다양한 정보보호 핵심 기술의 연동이 필요함	▶ 사용자가 직접 서비스 내용을 관리(업데이트)하지 않아도 자동으로 업데이트 및 감시를 하므로 사용자에게 편리성이 제공할 수 있음 ▶ 보안 관리 및 설정의 어려움을 해결할 수 있음

참고 문헌

- [1] 김광식, 남택용, "정보보호시스템 공통평가기준 기술동향", 전자통신동향분석, 제17권 제5호 pp. 89-101, 2002. 10.
- [2] 김광식, 남택용, 손승원, 박치항, "국제공동평가기준의 평가를 받기 위한 개발자 고려사항 분석", 제18권 제1호 pp. 17-24, 2003. 2.
- [3] IDC, "The Big Picture", 2002. 12.
- [4] Datamonitor, "Galbal network security markets", 2002. 7.
- [5] KISA, "국내 정보보호산업 통계조사 및 시장 조사연구", 2002. 12.
- [6] 김석우, "국제상호협정(CCRA)수용에 대비한 국내 산업체 고려사항." KISA 기획특집.
- [7] Common Criteria Homepage, <http://www.commoncriteriaportal.org/>
- [8] Communication-Electronics Security Group Homepage, <http://www.cesg.gov.uk/>
- [9] National Institute of Standards and Technology Homepage, <http://niap.nist.gov/cc-scheme/>
- [10] Chief Information Office Homepage, <http://www.cio.gov.at/>
- [11] AISEP Homepage, <http://www.dsd.gov.au/infosec>
- [12] KISA Homepage, <http://www.kisa.or.kr/>
- [13] MIC Homepage, <http://www.mic.go.kr>
- [14] 정보보호시스템 평가 인증 가이드, KISA, 2000.
- [15] 황성원, "정보보호산업 최근동향," KISA, 정책연구팀 기술자료.
- [16] 한국IDC 보고서, "한국 보안 소프트웨어 시장 동향 및 전망보고서, 2002-2007", 2003.
- [17] 정보통신부, "2003년 정보보호 기술개발 5개년 계획(안)", 2003.6.
- [18] 류재철, 박순태, 이승환, "국의 민간평가기관 평가 동향", 정보보호학회지 제13권 제6호 pp. 37-54, 2003.12.
- [19] 정보통신부고시 제 2003-52호, "정보보호시스템 공통평가기준개정", 2003. 11.
- [20] ISO/IEC 15480, "Information technology-Security Techniques Evaluation Criteria for IT security", 1999.

〈著者紹介〉



오 흥 룡 (Heung-Ryong Oh) 정회원
 2002년 2월 : 순천향대학교 전자공학과 학사
 2004년 2월 : 순천향대학교 정보보호학과 석사
 2004년 2월~현재 : 한국정보통신기술협회(TTA)
 <관심분야> 보안 프로토콜, 정보보호표준



염 흥 열 (Heung-Youl Youm) 정회원
 1981년 2월 : 한양대학교 전자공학과 학사
 1983년 2월 : 한양대학교 대학원 전자공학과 석사
 1990년 2월 : 한양대학교 대학원 전자공학과 박사
 1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
 1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
 1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
 2000년 4월~현재 : 순천향대학교 산학연진소시범센터 소장
 1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
 2003년 9월~2004년 3월 ITU-T SG17/Q10, Associate Rapporteur
 2004년 3월~현재 : ITU-T SG17/QL Rapporteur
 <관심분야> 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안