

# 국제 공통평가기준(CC) 체제하에 평가된 정보보호 제품 분석\*

오 흥 룡\*\*, 엄 흥 열\*\*\*

## 요 약

IT(Information Technology) 제품의 보안 기능을 평가하기 위하여 서로 다른 체제를 이용할 경우 평가를 위한 이중의 비용 소요와 추가의 시간 소모 등의 문제점을 해결하기 위하여, 미국, 영국, 호주 등의 선진국들은 국제간에 상호인정이 가능한 공통평가기준(CC: Common Criteria)에 대한 연구가 활발히 진행되고 있다. 현재 우리나라도 국제상호인정협정(CCRA)에 가입을 준비 중에 있으며, 다양한 IT 제품으로 평가 제도의 확대를 준비하고 있다. 본 논문에서는 미국, 영국, 호주의 CC 체제 하에서 평가된 정보보호 제품들의 특성을 분석하고, 이를 근거로 우리나라 IT 제품의 보안 기능 평가에 적용 가능한 분류 체계를 고찰해 본다.

## I. 서 론

CC는 IT 제품에서 보안성 평가를 위해 평가기준을 발전시킨 노력의 결과로써 기술 선진국 각 국에 널리 사용되고 있다. CC는 유럽, 미국, 캐나다 등의 평가 기준을 정리하고 발전시킨 것이기도 하고, 또한 다양한 평가기준의 개념적 차이와 기술적 차이를 해결한 것이며, 평가결과를 해당 상호국가간에 인정해주는 방식이기도 하다. CC 1993년부터 개발되기 시작하여 최종 버전인 2.1은 1999년 ISO/IEC 15408 국제표준으로 채택되어 활용되고 있다. CC의 주요 내용으로 Part 1은 일반적인 모델의 보안 설명서 및 평가 그리고 보호프로파일(PP: Protection Profile)과 보안 목표명세서(ST: Security Target)를 기본적으로 다루고 있으며, Part 2는 기본적으로 요구되는 보안 기능을 Part 3은 보안 보증 요구를 다루고 있다<sup>[5]</sup>.

국가간에 CC를 적용하여 평가된 결과를 상호인정을 목적으로 CCRA가 체결되었으며, 가입국 중 평가 인증서를 발행하고 상호 인정해 주는 CAP로 미국, 영국, 프랑스, 독일, 캐나다, 호주/뉴질랜드, 일본이 있으며, 인증서를 발급하지는 않고 상호 인정해 주는

CCP로 네델란드, 이탈리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴 등이 있다. 현재 우리나라를 포함하여 중국, 러시아 등이 CC를 자국의 평가 기준으로 제정하여 IT 제품들에 대한 보안성 평가에 적용하고 있으며 CCRA 가입을 준비하고 있다.

본 논문에서는 선진국의 CC 체제 하에서 평가된 정보보호 제품들의 특징을 분석하고, 이를 바탕으로 국내에 적합한 정보보호 제품 평가에 기여하고자 한다. 주요 내용으로 본론의 II장에서는 대표적인 선진국으로 미국, 영국, 호주의 평가된 정보보호 제품 유형과 각 제품들의 특징을 분석하고, III장에서는 국외 정보보호 제품 평가 사례를 기술한다. IV장에서 국내 정보보호 제품들을 우리 실정에 맞도록 분류해 보고, V장에서 결론을 기술한다.

## II. 본 론

본 장에서는 선진국 미국, 영국, 호주의 평가된 정보보호 제품들의 분류 형태 및 각 제품들의 특징들을 분석하였다.

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

\*\* 한국정보통신기술협회 표준화본부(hroh@tta.or.kr)

\*\*\* 순천향대학교 정보보호학과(hyyoum@sch.ac.kr)

1. 미국 정보보호 제품 분석

다음 제품들은 NIAP(National Information Assurance Partnership) 공통기준평가 및 검증 기법과 CCRA의 기준에 준수하여 평가되고 검증된 제품들이다. 목록상의 제품들은 미국 또는 IT 보안 평가를 위한 공통 기준에 준용하기 위하여 CCRA에 참여한 국가 중 한 나라에 존재하는 인가/허가된 시설에서 평가되고 인가되었다.

IT 제품들을 위하여 발행된 공통 기준 인증서는 이 제품의 정해진 버전과 제품명(release)에 대해서만 적용된다. 인증서를 승인하고 효력을 주는 NIST, NSA, 또는 다른 조직들에 의해 주어지는 인증서는 IT 제품의 우수함을 보증하지는 않는다. 인증서는 그 제품이 CC 요구사항을 만족하는 검증을 성공적으로 완료했음을 의미한다<sup>(3)</sup>.

1.1 미국 정보보호 제품군 및 제품 유형

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. CCRA에 의한 이 중요한 요약 문서는 평가 팀에 의하여 이루어진 판정이 완전한 것이고 일관된 것이라는 것을 확인하기 위한 정보와 수행된 검증 활동들, 그리고 평가의 결과를 보여주도록 설계되었다.

검증된 제품들의 확장된 목록은 <http://www.commoncriteriaportal.org/> 웹사이트에 가만 구할 수 있을 것이다. 이 웹사이트는 CC의 국제적인 사용자들을 위한 정보 역할을 한다. 다음 [표 1]의 정보보호 제품군 구분은 미국 연방 정부가 마련한 PP의 존재에 따라서 구분한 것이다.

[표 1]에서 제품 유형의 기술 범주를 위한 검증된 미국 정부 드래프트 PP가 이용 가능하지만 이 기술 범주 내에 존재하는 모든 개개의 제품들이 반드시 PP를 만족한다고 추론할 수는 없다. 드래프트 PP들은 여러 개발 단계에 존재하고 쓰여지고 있거나, 검토되거나, NIAP CCEVS CCTL(Common Criteria Testing Laboratory)에서 평가중에 있다.

1.1.1 네트워크 인프라 정보보호 제품군

네트워크 인프라 정보보호 제품군의 제품 설명은 [표 2]와 같다.

[표 1] 미국연방정부의 정보보호 제품군

| 제품군               | 제품 유형  |
|-------------------|--|
| 네트워크 인프라 정보보호 제품군 | <ul style="list-style-type: none"> <li>· 스위치/라우터</li> <li>· 라우터</li> <li>· 무선 LAN</li> </ul>   |
| 네트워크간 정보보호 제품군    | <ul style="list-style-type: none"> <li>· 방화벽</li> <li>· 원격 접근</li> <li>· 다중 영역 솔루션</li> <li>· 가상사설망</li> <li>· 이동 코드</li> <li>· 가드(guard)</li> </ul>   |
| 컴퓨터 환경 정보보호 제품군   | <ul style="list-style-type: none"> <li>· 운영체제</li> <li>· 보안 메신저</li> <li>· 단일-레벨 서버</li> <li>· 민감한 데이터 보호</li> <li>· 신뢰된 데이터베이스 관리 시스템</li> <li>· PC 접근 제어</li> <li>· 주변장치 공유 스위치</li> <li>· 기타</li> <li>· 바이오메트릭</li> <li>· 토큰</li> </ul> |
| 인프라 지원 정보보호 제품군   | <ul style="list-style-type: none"> <li>· 망관리</li> <li>· 키복구</li> <li>· 침입탐지시스템</li> <li>· 기타</li> <li>· 스마트카드</li> <li>· PKI/PMI</li> </ul>  |

[표 2] 네트워크 인프라 정보보호 제품군

| 제품 유형   | 설명   | 비고 |
|---------|--|----|
| 스위치/라우터 | <ul style="list-style-type: none"> <li>○ 근거리통신망 구축시 단말기의 접근 장치로 이용되는 스위칭 기능을 가진 통신장비</li> <li>○ 스위치와 라우터 기능을 동시에 수행하는 장치</li> </ul>                        |    |
| 라우터     | <ul style="list-style-type: none"> <li>○ 통신망 간을 연결해주는 장치로서, 한 통신망에서 오는 패킷을 수신하고, 패킷에 발신지 주소를 읽고 경로배정 테이블을 참고로 가장 적절한 통신로를 이용하여 다른 통신망으로 전송하는 장치</li> </ul> |    |
| 무선 LAN  | <ul style="list-style-type: none"> <li>○ 전파나 적외선 전송방식을 이용하는 근거리통신망(LAN)</li> </ul>   |    |

1.1.2 네트워크간 정보보호 제품군

네트워크간 정보보호 제품군의 제품 설명은 [표 3]과 같다.

1.1.3 컴퓨터 환경 정보보호 제품군

컴퓨터 환경 정보보호 제품군의 제품 설명은 [표 4]와 같다.

1.1.4 인프라 지원 정보보호 제품군

인프라 지원 정보보호 제품군의 제품 설명은 [표 5]와 같다.

[표 3] 네트워크간 정보보호 제품군

| 제품 유형     | 설명  | 비고 |
|-----------|---|----|
| 방화벽       | ○ 조직의 보안 정책을 지원하기 위하여 취약성 있는 서비스를 제한하고 특정 서비스로의 접근을 제어하기 위하여 네트워크 경계나 자국 호스트/서버 상에 배치됨        |    |
| 가상사설망     | ○ 공공 네트워크 상에 암호화된 터널을 생성함으로써, 이해 당사자간에 통신을 보호하거나 분리하는데 사용되는 기술                                |    |
| 원격 접근     | ○ 원격 접근을 위한 기술  |    |
| 이동코드      | ○ 이동 코드상에 보안 정책 제한을 집행하는 기술. 이 제한은 경계가 있는 보안 솔루션 내에서 실현되거나 사용자 호스트 또는 서버 상에서 집행됨              |    |
| 다중 영역 솔루션 | ○ 다중의 보안 영역간의 안전한 데이터의 전송을 위한 기술  |    |
| 가드        | ○ 등급화된 네트워크에서 비등급화된 네트워크로 연결을 보호하기 위하여 사용됨. 고보증 방화벽과 유사하나, 높은 등급 데이터의 누설을 보호하기 위한 추가적인 기능을 가짐 |    |

[표 4] 컴퓨터 환경 정보보호 제품군

| 제품 유형             | 설명   | 비고 |
|-------------------|--|----|
| 운영체제              | ○ 시스템 관리자나 사용자에게 의하여 설정된 보안 정책을 실행하기 위하여 인증, 접근 제어, 데이터 구분, 감사 등의 보안 메커니즘을 제공하는 운영체제   |    |
| 바이오메트릭            | ○ 당신이 알고 있는 것에 당신이 가지고 있는 것을 부가하여 구현한 설비나 워크스테이션에게 강한 인증을 제공하는 기술<br>○ 바이오메트릭 능력은 지문, 장문, 얼굴 인식, 또는 망막 스캔 장치와 연관됨                                |    |
| 보안메신저             | ○ 사용자 데이터를 위한 비밀성과 무결성 서비스를 제공하기 위한 인증, 서명, 암호 메커니즘을 제공하는 메신저 응용. 이 서비스는 공개된 키인증 기법을 사용하여 제공됨  |    |
| 토큰                | ○ 스마트카드를 포함하는 넓은 의미의 토큰으로 주로 크리덴셜 정보를 저장하는 수단을 제공함   |    |
| 단일-레벨 서버          | ○ 고수준의 네트워크를 사용하기 위하여 접근 제어, 감사 그리고 인증 및 데이터 암호 서비스를 제공하는 웹서버  |    |
| 민감한 데이터 보호        | ○ 데이터로의 비인가된 접근을 보호하기 위한 관리적, 기술적, 또는 물리적 조치들의 실현  |    |
| 신뢰된 데이터베이스 관리 시스템 | ○ 데이터베이스를 생성하고 유지하는 것과 데이터베이스를 사용하는 컴퓨터 프로그램의 수행을 지원하는 신뢰된 소프트웨어 시스템<br>○ 데이터베이스는 특정 목적을 위하여 요구되는 데이터의 집합이거나 시스템이나 프로젝트, 또는 기업에 기본이 되는 데이터의 집합   |    |
| PC 접근 제어          | ○ 저장 장치로 데이터를 두거나 저장 장치로 데이터를 가져오기 위한 개별 또는 응용 프로그램의 권한을 정의하거나 제한하기 위하여 사용되는 기술<br>○ 정보 시스템의 자원으로의 접근을 인가된 사용자, 프로그램, 프로세스, 또는 다른 시스템으로만 제한하는 기술 |    |
| 주변장치 공유 스위치       | ○ 서로 다른 고수준의 네트워크 상에서 동작하는 두 개의 워크스테이션을 통한 통신을 위하여 사용자에게 하나의 주변장치를 사용 가능케 하는 신뢰된 전자 또는 물리 장치<br>○ 스위치는 두 개의 네트워크를 통하여 전달되는 데이터의 누설을 예방해야 함       |    |

[표 5] 인프라 지원 정보보호 제품군

| 제품 유형      | 설명   | 비고 |
|------------|--|----|
| 네트워크(망) 관리 | ○ 네트워크 사용 또는 접근을 거부하는 악의적인 공격으로부터 네트워크를 보호하기 위한 기술. 예를 들어, 네트워크 관리 센터로의 접근을 제어하기 위하거나 여러 종류의 공격으로부터 네트워크 관리 트랜잭션을 보호하기 위하여 사용되는 기술 |    |
| 인증서 관리     | ○ 암호학적 시스템의 사용자들을 위한 공개키 인증서의 생성, 분배, 그리고 훼손 복구를 관리하기 위하여 사용되는 기술  |    |
| 키복구        | ○ 사용자의 개인키를 제삼의 위탁기관에 맡기고, 필요시 복구하는 기술   |    |
| 스마트카드      | ○ 사용자의 인증 크리덴셜을 안전하게 저장하고 이 크리덴셜(예를 들어, 공개키 재료의 비밀키 부분)의 사용과 접근을 제어하기 위하여 사용되는 작은 사용자 토큰   |    |
| 공개키 기반구조   | ○ 암호학적 제품 사용자에게 공개키와 키관리 서비스 설비를 관리하기 위하여 사용되는 기술. 설비, 사람, 그리고 절차의 집합을 나타냄   |    |
| 침입탐지 시스템   | ○ 비인가된 네트워크 침입이나 네트워크의 트래픽을 감시하고, 네트워크를 찾기 위하여 네트워크 또는 사용자 호스트 상에 배치되는 장치  |    |

2. 영국 정보보호 제품 분석

영국은 CESG <http://cesg.gov.uk/iacs/>와 NIST 홈페이지(<http://www.nist.gov/>)를 참조하여 분석하였다. 영국의 정보보호 제품군의 분류는 [표 6]과 같이 크게 7가지 분야로 구분하고 있다. 7가지 분야는 통신, 데이터 삭제, 데이터베이스, 네트워크, 운영체제, PC 액세스 제어, 그리고 기타 제품군으로 구성되어 있다<sup>[4,6]</sup>.

2.1 영국 정보보호 제품군 및 제품 유형

2.1.1 통신 정보보호 제품군

통신 정보보호 제품군의 제품 설명은 [표 7]과 같다.

2.1.2 데이터 삭제, 데이터베이스 정보보호 제품군

데이터 삭제, 데이터베이스 정보보호 제품군의 제품 설명은 [표 8]과 같다.

2.1.3 네트워크 정보보호 제품군

네트워크 정보보호 제품군의 제품 설명은 [표 9]와 같다.

[표 6] 영국의 정보보호 제품군

| 제품군       | 제품 유형                            |
|-----------|----------------------------------|
| 통신        | · 데이터 암호화기<br>· 스위치 · 보안메신저      |
| 데이터 삭제    | · 데이터 삭제                         |
| 데이터베이스    | · DBMS                           |
| 네트워크      | · 방화벽 · VPN<br>· 인증기관 · 등록기관     |
| 운영체제      | · SUN의 솔라리스<br>· 소니사의 스마트카드 운영체제 |
| PC 액세스 제어 | · PC 액세스 제어 시스템                  |
| 기타        | · 다양한 PP                         |

2.1.4 운영체제, PC 액세스 제어 시스템, 기타 정보보호 제품군

운영체제, PC 액세스 제어, 기타 정보보호 제품군의 제품 설명은 [표 10]과 같다.

3. 호주 정보보호 제품 분석

호주는 CIO 홈페이지(<http://www.cio.gov.au/>)

[표 7] 통신 정보보호 제품군

| 제품 유형    | 설명   | 비고 |
|----------|--|----|
| 데이터 암호화기 | ○ 다양한 선로 인터페이스를 사용하는 2Mbps t이상의 속도로 동작하는 회선에 대한 안전한 통신을 제공함<br>○ 비인가된 정보에 대한 접근 제어. 데이터의 도청을 예방, 안전한 키관리 기법을 사용하여 키를 생성 및 분배를 제공함  |    |
| 스위치      | ○ Nortel사의 DPN-100/20 switch. 패킷 교환 데이터 통신 서비스의 일부분을 구성하기 위하여 설계된 국방 통신 서비스에 사용되는 교환기<br>○ 이 장치는 사용자 선로와 네트워크 간에 인터페이스를 제공하며, 이는 자동화된 라우팅 기능을 제공하는 자원 모듈과 선로 인터페이스를 제공하는 액세스 모듈로 구성됨   |    |
| 보안메신저    | ○ Cerberus사의 Guard Processor. 신뢰되고 라벨화된 기법을 사용하여 통신을 하는 네트워크 간에 통과되는 메시지를 검사하는 기능을 수행<br>○ 두개의 네트워크는 서로 다른 보안 레벨이 존재하고, 상호 동작에 대한 보안 제한이 존재<br>○ 메시지의 보안 레벨이 발신지/목적지 주소 쌍에 대한 허용된 레벨의 집합 내에 존재하는지를 검사<br>○ 만약 가드에 의하여 검사되는 하나 이상의 검사가 실패하면 메시지의 전달은 중단되며, 관리자의 개입을 요청함 |    |

[표 8] 데이터 삭제, 데이터베이스 정보보호 제품군

| 제품 유형     | 설명  | 비고 |
|-----------|---|----|
| Degausser | ○ 동일한 안전 설비 내에서 재사용 될 때 평문 SECRET 과 TOP SECRET 데이터를 지우는데 사용<br>○ 안전한 설비 밖으로 저장 매체를 버릴 때, CONFIDENTIAL 과 SECRET 데이터를 지우는데 사용             |    |
| DBMS      | ○ 관계형 객체 데이터베이스 관리 시스템이며, 사용자들에게 향상된 보안 기능을 제공<br>○ 분산형 데이터베이스 환경을 제공하며, 보안 기능으로 미세한 액세스 제어를 위한 보안 정책, 응용 한정 보안 컨텍스트, 요청자와 정의자의 권리를 지원함 |    |

[표 9] 네트워킹 정보보호 제품군

| 제품 유형       | 설 명   | 비 고 |
|-------------|---|-----|
| 방화벽         | <ul style="list-style-type: none"> <li>○ 안전하고 효과적인 인터넷 연결을 위하여 필요한 모든 서비스들과 통합된 운영체제를 포함함</li> <li>○ 방화벽 운영체제는 알려진 취약점을 강화하고, 안전한 플랫폼을 제공</li> <li>○ 프락시 서버는 전자메일 서버, FTP 서버, WWW 서버, 그리고 이중 DNS 서버 등이며, 방화벽 서버는 전용 하드웨어나 소프트웨어 버전으로 설치됨</li> </ul> |     |
| VPN         | <ul style="list-style-type: none"> <li>○ IPSEC을 이용한 가상 전용망 장치</li> </ul>  |     |
| 인증기관 등의 PKI | <ul style="list-style-type: none"> <li>○ Entrust/Authority 5.1 은 공개키 기반구조를 위한 핵심 구성요소이며, 인증서를 발행하고, 키 관리기능을 수행</li> <li>○ 다른 인증기관에게 상호 인증서를 발행하고, 다양한 인증서 프로파일을 지원하며, 이는 다양한 서명 알고리즘과 다양한 키 길이를 지원함</li> </ul>                                      |     |

[표 10] 운영체제, PC 액세스 제어, 기타 정보보호 제품군

| 제품 유형         | 설 명  | 비 고 |
|---------------|--|-----|
| 솔라리스          | <ul style="list-style-type: none"> <li>○ 솔라리스 운영체제 보안에 관한 제품</li> </ul>  |     |
| 스마트카드 운영체제    | <ul style="list-style-type: none"> <li>○ 스마트카드를 위한 안전한 다중 응용 지원이 가능한 운영체제</li> <li>○ EMV, 전자화폐, GSM 등의 다양한 이 제품은 여러 벤더에 의하여 유용가능하며, 호환성 있는 동작을 보장, 카드 발행자 제어된 로드, 응용의 안전한 제거, 응용의 안전한 구분, 암호화된 응용의 인증과 안전한 로드 등의 기능을 지원함</li> </ul>                            |     |
| PC 액세스 제어 시스템 | <ul style="list-style-type: none"> <li>○ 데이터의 도난과 비인가된 사용을 막기 위한 액세스 제어 메커니즘을 제공</li> <li>○ 사용자의 신분확인과 패스워드를 통한 불법적인 액세스 제어 방지, 사용자보안 프로파일을 이용한 비인가된 파일 액세스 제어, 감시, 차일 액세스 제어 매트릭스, 악의적인 악성 코드의 전파 방지, 비인가된 플로피 디스켓의 사용 금지 등을 제공하며, 데이터 암호화 기능도 제공함</li> </ul> |     |
| 다양한 PP        | <ul style="list-style-type: none"> <li>○ PKI 안전한 커널 PP, 권한 관리에 기반을 둔 웹 사이트 콘텐츠 보호 PP, 역할 기반 액세스 제어 PP 등을 평가함</li> </ul>  |     |

를 참조하여 분석하였다. 평가 제품 목록은 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 만들어 졌다. 제품 목록들은 제품들이 합의된 보안 목표 설계서를 만족할만한 정도의 보증 수준을 제공하기 위하여 올바르게 효율적으로 동작한다는 것을 보증하기 위하여 자신의 보안성에 대한 세부적인 평가 절차를 거쳤다<sup>[8]</sup>.

3.1 호주 정보보호 제품군 및 제품 유형

3.1.1 네트워크 보안 정보보호 제품군

네트워크 보안 정보보호 제품군의 제품 설명은 [표 12]와 같다.

3.1.2 공개키 기술 정보보호 제품군

공개키 기술 정보보호 제품군의 제품 설명은 [표

13]과 같다.

[표 11] 호주의 정보보호 제품군

| 제품군        | 제품 유형  |
|------------|--|
| 네트워크 보안 제품 | <ul style="list-style-type: none"> <li>· 방화벽 · 라우터 · 스위치</li> <li>· VPN · 메시징 관리</li> <li>· 네트워크 암호 · ATM 암호화기</li> <li>· 신뢰된 네트워크 구분 장치</li> <li>· 안전한 원격 액세스 · 보안관리</li> </ul> |
| 공개키 기술     | <ul style="list-style-type: none"> <li>· PKI 제품</li> <li>· 공개키 클라이언트 제품</li> </ul>   |
| 스마트카드      | <ul style="list-style-type: none"> <li>· 스마트카드 운영체제</li> <li>· 스마트카드 응용</li> </ul>   |
| 운영체제       | <ul style="list-style-type: none"> <li>· 솔라리스 · HP</li> <li>· AIX 운영체제</li> </ul>  |
| PC 보안      | <ul style="list-style-type: none"> <li>· PC 상의 민감한 데이터 및 등급화된 데이터 보호</li> </ul>  |
| 생체기술       | <ul style="list-style-type: none"> <li>· 생체인증 제품</li> </ul>  |
| 호스트 보안 모듈  | <ul style="list-style-type: none"> <li>· 암호학적 보안 모듈</li> </ul>   |
| 기타         | <ul style="list-style-type: none"> <li>· 암호학적 지원 모듈</li> <li>· 위성 암호화 장치</li> <li>· 신뢰된 DBMS · 자장 중화 제품</li> </ul>   |

(표 12) 네트워크 보안 정보보호 제품군

| 제품 유형       | 설명   | 비고 |
|-------------|--|----|
| 방화벽         | <ul style="list-style-type: none"> <li>패킷 필터링, 네트워크 주소 변환, 응용 프락시, VPN, 그리고 원격 방화벽 관리 등의 기능을 수행함</li> </ul>  |    |
| 메시징 관리 시스템  | <ul style="list-style-type: none"> <li>안전한 메시지 보안(SMIME) 능력, 장기간 아카이빙 및 조회, 정책 기반 관리 통신, 그리고 메시지 감시 및 검토 등의 요구사항을 만족하기 위한 SMTP 통신 스트림과 HTTP 통신 스트림에 대한 관리기능을 제공하며, 콘텐츠 필터링, 스팸 메일 차단, 안티 바이러스 등의 메시징 대응 기능을 통신 레벨에서 적용함으로써 강화된 조직의 지배력을 제공하기 위하여 사용됨</li> <li>MMS는 정책 기반 시스템으로 특정 보안 정책에 기반을 둔 다양한 조치사항들을 수행 가능하며, 이 정책은 여러 개의 GUI 기반 정책 관리자에 의하여 설정되며, 이 정책 관리자는 법칙들과 결과들을 정의함</li> </ul>   |    |
| 네트워크 암호     | <ul style="list-style-type: none"> <li>국가 정보가 아닌 일반 정보를 보호하기 위한 서비스를 제공</li> <li>이 영역에는 VPN, 네트워크의 링크레벨 암호기 등의 제품으로 구성됨</li> <li>대표적인 제품은 KyberPASS 사의 Secure-Session VPN이며, 다음과 같은 네트워크 보안 서비스를 제공하기 위하여 PKI를 사용하는 미들웨어 클라이언트/서버 제품임                     <ul style="list-style-type: none"> <li>데스크탑이나 서버 응용에게 디지털 서명, 인증, 그리고 감사 서비스를 제공</li> <li>IP 네트워크를 통하여 방향성이 있는 가상 사설망 세션을 필요시 마다 생성하고, 세션키의 길이는 168-비트 삼중 DES에 적용되는 키 길이에 대응됨</li> <li>집중화된 정책 관리를 제공</li> <li>집중화된 감사, 로깅, 그리고 경보를 제공</li> <li>인증기관과 등록기관을 지원함</li> <li>LDAP v3 호환 X.500 디렉토리를 지원함</li> </ul> </li> </ul> |    |
| 신뢰된 네트워크 구분 | <ul style="list-style-type: none"> <li>신뢰된 제품의 사용을 통하여 서로 다른 등급의 네트워크간의 제어된 상호 동작을 제공하기 위한 보안 기능을 제공함</li> <li>대표적인 제품은 2in1 PC 이며, Voltaire Advanced Data Security 사에 의하여 개발된 하드웨어 기반 보안 제품임                     <ul style="list-style-type: none"> <li>2in1 PC는 하나의 PC가 두개의 물리적으로 구분된 네트워크들(공개 네트워크와 안전한 네트워크) 안전하게 접근하게 하는 ISA 슬롯 PC 카드임</li> <li>이 기능은 두개의 네트워크간의 연결성을 관리하는 하드웨어 기반 보안 제어기와 각 네트워크와 관련된 하드디스크 파티션을 통하여 달성될 수 있음</li> <li>2in1 PC는 다양한 운영체제(MS DOS, 윈도우즈 95/98, 윈도우즈 NT, 리눅스 등)상에서 동작 가능하며, PC는 반드시 하나 이상의 IDE-ATA 호환 디스크를 포함하고 있어야 함</li> </ul> </li> </ul>      |    |

(표 13) 공개키 기술 정보보호 제품군

| 제품 유형        | 설명   | 비고 |
|--------------|--|----|
| PKI 제품       | <ul style="list-style-type: none"> <li>인증기관, 등록기관, X.500 디렉토리 관련 공개키 기반구조 제품을 포함</li> <li>인증기관, 등록기관, 관리 기능을 제공하는 PKI 시스템과 타임스탬프 서버, 그리고 사용자에게 서명 기능 등을 제공하기 위한 클라이언트 응용에 공개키 기술을 적용한 제품으로 구성</li> </ul>   |    |
| 공개키 클라이언트 제품 | <ul style="list-style-type: none"> <li>공개키 기반구조내의 클라이언트이며, 안전한 전자메일, X.509 인증서 사용자 등과 같은 제품을 포함하며 대표 제품은 다음과 같다.                     <ul style="list-style-type: none"> <li>iKey 2032 스마트 토큰으로 안전한 2가지 요소 인증 장치이며, 사용자는 iKey 자체의 인증과 iKey의 PIN 인증을 수행하도록 요구됨</li> <li>스마트 토큰은 스마트카드와 구성 요소와 인터페이스가 다른 점을 제외하며 기술적으로는 동일함</li> <li>iKey 스마트 토큰은 온보드 키 생성, 안전한 키쌍의 저장, X.509 인증서의 저장, 디지털 서명은 온보드상에서의 수행등을 제공함으로써, 공개키 기반구조를 지원함</li> <li>iKey 스마트 토큰 내의 온보드 USB 제어기는 스마트카드 리더기와 동일한 기능을 수행하며, 암호학적 제어기 내에서 데이터를 사용하도록 변환됨</li> <li>iKey 스마트 토큰은 공개키, 암호키등을 저장하고 서명 동작을 수행하는 암호학적 제어기를 가지고 있고, 모든 암호학적 동작이 암호학적 제어기 내에서 수행되므로, 개인키는 절대로 클라이언트 컴퓨터로 노출되지 않으므로, 악의적인 소프트웨어에 의하여 개인키가 해킹되지 않음</li> <li>암호학적 프로세서는 의사 난수 생성기를 포함하며, 의사 난수 생성기는 개인키 생성을 위한 소수를 생성하는데 이용됨</li> </ul> </li> </ul> |    |

3.1.3 스마트카드, 운영체제 정보보호 제품군

스마트카드, 운영체제 정보보호 제품군의 제품 설명은 [표 14]와 같다.

3.1.4 PC 보안 정보보호 제품군

PC 보안 정보보호 제품군의 제품 설명은 [표 15]와 같다.

[표 14] 스마트카드, 운영체제 정보보호 제품군

| 제품 유형          | 설명  | 비고 |
|----------------|---|----|
| 스마트카드 운영체제와 응용 | <ul style="list-style-type: none"> <li>○ 대표적인 제품은 Keycorp's MULTOS 스마트카드 운영체제이며, MONDEX 사에 의하여 개발되었고, MULTOS 컨소시엄에 의하여 승인됨</li> <li>○ 이 제품은 하나의 카드 상에서 다중 응용을 지원하며, 고도의 보안 응용 레벨을 제공함</li> <li>○ 운영체제는 응용 콘텐츠의 기밀성, 응용 콘텐츠의 검증, 비인가된 응용의 로드 방지, 하나의 응용에서 다른 응용으로 로드되는 응용 콘텐츠의 기밀성 보호, 중요한 응용데이터의 갱신을 보호하기 위한 트랜잭션 보호, 그리고 응용의 비인가된 삭제 등의 기능을 제공함</li> </ul> |    |
| 운영체제 보안 제품     | <ul style="list-style-type: none"> <li>○ 범용 운영체제이며, 미국 NIST의 국립 컴퓨터 보안 센터에 의하여 평가된 제품</li> <li>○ 운영체제는 선사의 솔라리스 OS, AIX, HP사의 UNIX 등이며, 대표적인 평가 제품은 Solaris 8, 이는 유닉스 기반 운영체제이며, 하나의 분산 시스템을 구성하기 위하여 여러 개의 워크스테이션과 서버들로 구성되어 있음</li> <li>○ 이 제품은 선 마이크로시스템 사에 의하여 개발되었고, EAL4 로 인증됨</li> </ul>   |    |

[표 15] PC 보안 정보보호 제품군

| 제품 유형                              | 설명  | 비고 |
|------------------------------------|---|----|
| 정부를 위한 PC 보안 제품                    | <ul style="list-style-type: none"> <li>○ 민감하고 등급화된 데이터를 보호하는데 적합하며, 제한된(RESTRICTED) 데이터를 보호하는데 적합함</li> <li>○ 국가 보안 등급화된(national security classified) 정보를 보호하기 위해서 사용되어서는 안됨</li> <li>○ 예로 PCVault 제품이며, 이는 IBM PC호환 PC를 위한 액세스 제어 시스템                     <ul style="list-style-type: none"> <li>- 독립형으로 동작하고, 단일 사용자나 다중 사용자를 지원</li> <li>- DES를 사용하여 투명한 하드디스크 암호화를 지원하고, 패스워드로 액세스 제어를 지원하며, 디스켓과 포트에 대한 액세스 제어 기능, 스크린과 키보드 락, 부트 트랙 바이러스 보호 기능을 제공함</li> </ul> </li> </ul>   |    |
| 민감한 데이터 보호를 위한 PC 보안 제품            | <ul style="list-style-type: none"> <li>○ 민감하고 등급화된 데이터를 보호하기 위하여 적합하며, 제한된 데이터를 보호하는데 적합함</li> <li>○ 국가 보안 등급 데이터를 보호하는데 사용해서는 절대로 안됨</li> <li>○ 예로 Blockit 제품이며, IBM PC를 위한 소프트웨어만으로 구성된 보안 시스템                     <ul style="list-style-type: none"> <li>- 하드드라이브의 암호를 통하여 보호를 제공하며, 사용자는 드라이브 상에 데이터를 액세스를 허용받기 이전에 로그인 과정을 수행하도록 요구됨</li> <li>- 사용자는 관리자 지정 파일에 대한 액세스를 제한받을 수 있고, 플로피 드라이브의 액세스를 제한받을 수 있음</li> <li>- 소프트웨어로 구현된 DES가 파일을 암호화하기 위하여 사용되고, DES는 민감한 데이터를 보호하기 위하여 사용됨</li> <li>- 검사합이 부트 과정을 수행하는 파일의 무결성을 위하여 사용될 수 있고, 감사 추적이 대부분의 사용자의 접근제어를 위하여 사용됨</li> </ul> </li> </ul> |    |
| 단일 사용자를 위한 민감한 데이터 보호를 위한 PC 보안 제품 | <ul style="list-style-type: none"> <li>○ PC 보안 제품으로써 민감한 데이터를 보호하기 위하여 사용됨</li> <li>○ 대표적인 제품은 Cryptcard이며, PCMCIA 슬롯을 갖는 IBM PC 호환 노트북 컴퓨터를 위하여 설계됨                     <ul style="list-style-type: none"> <li>- 신용카드 크기이며, 고속의 DES 암호를 제공하며, 전체 디스크 암호를 위하여, ECB 모드의 DES가 사용되며, 선택된 파일의 암호를 위하여 CBC 모드 암호가 사용됨</li> <li>- 사용자는 암호 칩을 활성화하기 이전에 패스워드를 입력하도록 요구되며, 전체 하드디스크가 암호화되어 있는 경우, 사용자는 패스워드를 입력하지 않으면 하드디스크를 접근할 수 없음</li> </ul> </li> <li>○ 단일 사용자 노트북 상에서 정보를 보호하기 위하여 설계되었고, 민감하고 등급화된 데이터를 포함하는 컴퓨터에 적합함</li> </ul>   |    |
| 비등급화된 데이터 보호를 위한 PC 보안 제품          | <ul style="list-style-type: none"> <li>○ 비등급화 되어 있는 데이터를 보호하기 위하여 적합하고, 국가 보안 등급 또는 민감한 등급 정보를 위하여 사용되어서는 안됨</li> </ul>   |    |

(표 16) 호스트 보안 모듈, 기타 정보보호 제품군

| 제품 유형      | 설 명   | 비 고 |
|------------|---|-----|
| 암호학적 보안 모듈 | <ul style="list-style-type: none"> <li>○ 암호키를 보관하고 안전한 암호학적 동작을 수행하는 하드웨어 기반의 암호 모듈</li> <li>○ 대표적인 제품은 SureWare Keyper이며, 디지털 서명 생성과 검증을 위한 고도의 안전한 환경을 제공함                         <ul style="list-style-type: none"> <li>- FIPS 140-1 레벨 4의 암호키 무결성을 제공</li> <li>- 호스트 시스템과 표준화된 네트워킹 기술을 이용하여 연결됨</li> <li>- 응용은 PKCS #11을 통하여 이 제품과 통신함</li> </ul> </li> </ul> |     |
| 암호학적 지원 모듈 | <ul style="list-style-type: none"> <li>○ 다른 평가된 제품의 암호학적 구성요소로 이용됨</li> </ul>   |     |
| 신뢰된 DBMS   | <ul style="list-style-type: none"> <li>○ 데이터베이스 응용 내의 보안 기능을 제공하며, 신뢰된 DBMS는 특정 운영체제 플랫폼과 연관되어 평가됨</li> <li>○ 오라클과 인포믹스 제품이 평가됨</li> </ul>  |     |
| 자장 중화 제품   | <ul style="list-style-type: none"> <li>○ 마그네틱 매체에 저장된 등급화된 데이터를 삭제하는데 사용되는 보안 제품</li> </ul>   |     |
| 암호화 통신 장치  | <ul style="list-style-type: none"> <li>○ 대표적인 제품은 NEC S2 이고, 휴대용 이동 위성 단말이며, 사용자에게 위성이 커버하는 지역 내의 어느 곳에서부터 지상 PSTN으로 연결되는 어떤 다른 사용자에게로의 통신 설정을 가능케 함</li> <li>○ 위성 전송을 암호화함으로써 고도의 프라이버시를 제공</li> </ul>   |     |

3.1.5 호스트 보안 모듈, 기타 정보보호 제품군

호스트 보안 모듈, 기타 정보보호 제품군의 제품 설명은 (표 16)과 같다.

와 (표 23)과 같다.

III. 국외 정보보호 제품 평가 사례

본 장에서는 NIAP의 홈페이지에 등록되어 있는 정보보호 제품 평가 사례를 분석한다<sup>(6)</sup>.

1. 네트워크 인프라 정보보호 제품군 평가 사례

네트워크 인프라 정보보호 제품군 평가 사례는 (표 17)과 같다.

2. 네트워크간 정보보호 제품군 평가 사례

네트워크간 인프라 정보보호 제품군 평가 사례는 (표 18)과 (표 19)와 같다.

3. 컴퓨터 환경 정보보호 제품군 평가 사례

컴퓨터 환경 정보보호 제품군 평가 사례는 (표 20)과 (표 21)과 같다.

4. 인프라 지원 정보보호 제품군 평가 사례

인프라 지원 정보보호 제품군 평가 사례는 (표 22)

IV. 우리나라 정보보호 제품군 분류 체계

우리는 우선 미국의 평가된 정보보호 제품 분석을 바탕으로 대분류로 정보보호 기반 제품군, 네트워크 정보보호 제품군, 컴퓨팅 네트워크 제품군으로 분류하였다. 그리고 영국, 호주의 평가된 정보보호 제품 분석을 바탕으로 중분류로 암호지원제품, 보안관리제품, 생체인식제품, 스마트카드, USB 토큰, PCMCIA 제품, 인증 솔루션제품, 네트워크기반제품, 네트워크간 제품, 서버보안제품, 데이터베이스제품, 메일보안제품, 단일레벨보안제품, PC보안제품, 공유스위치제품, 이동코드제품 이다. 최종적으로 미국, 영국, 호주의 제품 유형들을 고려하여 평가 대상 제품들을 적절히 선정하였다. 이에 대한 사항은 (표 24)와 같다.

V. 결 론

본 논문에서는 국제 공통평가기준 체제하에 선진국 미국, 영국, 호주의 평가된 정보보호 제품 유형 및 특성에 대해 분석을 하였다. 그리고 이를 근거로 국내 환경에 맞게 IT 제품들을 분류해 보았다.

























국의 평가 제품에서는 침입차단시스템/VPN 이 현재 가장 많았고, 급성장하고 있는 생체인식, 무선인터넷 제품들이 빠르게 성장할 것으로 전망된다.















[표 17] 네트워크 인프라 정보보호 제품군 평가 사례

| 제품유형 | 제품이름                | 제조업체          | 평가등급  | 유효일시   | CC스킵  |
|------|---------------------|---------------|-------|--------|---|
| 라우터  | Cisco Router Models | Cisco Systems | EAL 2 | Mar 01 |  |

[표 18] 네트워크간 정보보호 제품군 평가 사례(1)

| 제품유형                        | 제품이름   | 제조업체                                  | 평가등급   | 유효일시  | CC스킵  |
|-----------------------------|--|---------------------------------------|--------|---|---|
| 방화벽                         | Borderware, V6.1.1 Firewall Server   | Borderware Technologies               | EAL 4  | Jan 00  |    |
|                             | Check Point VPN-1/FireWall-1® NG   | Check Point Software Technologies Ltd | EAL 4  | Jun 02  |    |
|                             | Check Point VPN-1/Firewall-1® NG on Nokia IPSO   | Nokia                                 | EAL 4  | Sep 03  |    |
|                             | 3Com® Embedded Firewall V1.5.1   | Secure Computing Corporation          | EAL 2  | Jun 03  |    |
|                             | Cisco Secure PIX Firewall V5.2(3)  | Cisco System, Inc.                    | EAL 4  | Jan 01  |    |
|                             | Cisco Secure PIX Firewall V6.2(2)  | Cisco System, Inc.                    | EAL 4  | Dec 02  |    |
|                             | Conceal Private Desktop for Windows 95/98  | Signal 9 Solutions, Inc.              | EAL 1  | Apr 99  |    |
|                             | CS Bastion IITM  | ClearSwift                            | EAL 4  | Jun 03  |    |
|                             | CyberGuard Firewall for Unix Ware Release 4.3/KnightStar Premium Appliance Firewall 4.3 AMA maintained release 5.1 - 28 Feb 2003 | CyberGuard Corporation                | EAL 4+ | Dec 00  |    |
|                             | DiamondTEK   | Cryptek Secure Communications, LLC    | EAL 4  | Jun 02  |    |
|                             | (ETM®) (Enterprise Telephony Management) System V4.0.1   | SecureLogix Corporation               | EAL 2  | Apr 03  |    |
|                             | Enterprise Telephony Management Platform, V3.0.1   | SecureLogix Corporation               | EAL 2+ | Feb 02  |    |
|                             | Gauntlet Firewall Version 6.0 on Sun Solaris, V2.8   | Secure Computing Australia Pty Ltd    | EAL 4  | Apr 02  |  |
|                             | Internet Security and Acceleration Server 2000 with Service Pack 1 and Feature Pack 1  | Microsoft Corporation                 | EAL 2  | Sep 03  |  |
|                             | Lucent Technologies Lucent VPN Firewall V7.0 (Patch 531)   | Lucent Technologies, Inc.             | EAL 2  | Oct 03  |  |
|                             | NetScreen Appliance Models 25, 50, 5XP, and 5XT with ScreenOS 4.0.2r7.0  | NetScreen Technologies, Inc.          | EAL 4  | Jan 04  |  |
|                             | NetScreen Appliance Models 500, 208, 204 with ScreenOS 4.0.2r7.0   | NetScreen Technologies, Inc.          | EAL 4  | Dec 03  |  |
|                             | NetScreen Appliance Models 5200 with ScreenOS 4.0.2r7.0  | NetScreen Technologies, Inc.          | EAL 4  | Oct 03  |  |
|                             | NetScreen Appliance includes models, 5XP, 5XT, 25, 50, 204, 208, 500, and 5200 each with ScreenOS 4.0.2r6                        | NetScreen Technologies, Inc.          | EAL 4  | Jun 03  |  |
|                             | Netscreen Appliances includes models, 5XP, 5XT, 25, 50, 100, 204, 208, 500, and 5200 each with ScreenOS 4.0.0r7.0                | NetScreen Technologies, Inc.          | EAL 2  | Nov 02  |  |
|                             | Nortel Networks Alteon Switched Firewall   | Nortel Networks                       | EAL 4  | Aug 03  |  |
|                             | Safegate Firewall, V2.0.2  | Fujitsu Limited                       | EAL 3  | Jan 00  |  |
|                             | SECUREWORKS V3.2   | Oullim Information Technology, Inc.   | EAL 3  | Sep 03  |  |
| Sidewinder Firewall, V5.2.1 | Secure Computing Corporation   | EAL2+                                 | Sep 02 |  |   |

[표 19] 네트워크간 정보보호 제품군 평가 사례(2)

| 제품유형 | 제품이름  | 제조업체                               | 평가등급   | 유효일시   | CC스킴  |
|------|---|------------------------------------|--------|--------|---|
| 방화벽  | Sidewinde® G2r FirewallTM, V6.0   | Secure Computing Corporation       | EAL 4  | May 03 |  |
|      | Stonesoft StoneGate Firewall V2.0.5   | Stonesoft Corporation              | EAL 4  | Sep 03 |  |
|      | Symantec Enterprise Firewall, v7.0.4 running on Windows 2000 SP3 and on Solaris 7 & 8               | Symantec Corporation               | EAL 4  | Sep 03 |  |
|      | Symantec Enterprise Firewall, v 7.0   | Symantec Corporation               | EAL 4  | May 02 |  |
|      | Symantec Enterprise Firewall on the Symantec Gateway Security, Version 2.0                          | Symantec Corporation               | EAL 4  | Mar 04 |  |
|      | TeleWall System, V 2.0 for NT 4.0   | SecureLogix Corporation            | EAL 2+ | oct 00 |  |
|      | Watchguard LiveSecurity System w/Firebox II   | Watchguard Tecnologies             | EAL 2  | Aug 00 |  |
| VPN  | DiamondTEK  | Cryptek Secure Communications, LLC | EAL 4  | Jun 02 |  |
| 이동코드 | SurfinGate, Version 5.6   | Finjan Software Incorporated       | EAL 3  | oct 01 |  |
| 가드   | owl Computing Technologies Data Diode Version 1 and owl Computing Technologies Data Diode Version 2 | owl Computing Technologies, Inc.   | EAL 2  | Nov 02 |  |
|      | DragonFly Companion, V3.02, Build 129   | ITT Industries                     | EAL 2  | oct 99 |  |
|      | DragonFly Guard Model G1.2  | ITT Industries                     | EAL 2  | oct 98 |  |






























[표 20] 컴퓨터 환경 정보보호 제품군 평가 사례(1)

| 제품유형              | 제품이름  | 제조업체   | 평가등급  | 유효일시   | CC스킴  |
|-------------------|---|--|-------|--------|---|
| 바이오메트릭            | Bioscrypt Enterprise for NT Logon, V2.1.3   | Bioscrypt, Inc.  | EAL 2 | Jun 01 |   |
|                   | KnoWho Authentication Server v1.2.2 and Private ID v2.1.15  | Iridian Technologies, Inc.   | EAL 2 | oct 01 |  |
| 보안 메신저            | Tumbleweed Messaging Management System, V4.6  | Tumbleweed Communications Pty. Ltd.                                | EAL 2 | Mar 02 |  |
|                   | California Microwave Mail List Agent and Profiling User Agent(MLA/PUA) Version 3.1.0 with Patch A | Northrop Grumman Systems Corporation, California Microwave Systems | EAL 2 | Aug 03 |  |
| 단일-레벨 서버          | Persona 5.0   | Esker Incorporated   | EAL 3 | Dec 02 |  |
|                   | Bodacion Technologies' HYDRA Server, Version 1.4  | Bodacion Technologies  | EAL 1 | Feb 03 |  |
|                   | G-Server Version 2.5  | Gilian Technologies Inc.   | EAL 1 | Aug 03 |  |
| 신뢰된 데이터베이스 관리 시스템 | oracle 8, Release 8.0.5.0.0   | Oracle Corporation   | EAL 4 | Oct 00 |  |
|                   | oracle 8i Release 8.1.7.0.0   | Oracle Corporation   | EAL 4 | Jul 01 |  |
|                   | oracle Label Security for oracle 8i Database Server Enterprise Edition, Release 8.1.7.3.0         | Oracle Corporation   | EAL 4 | Mar 03 |  |
|                   | oracle 9i Label Security  | Oracle Corporation   | EAL 4 | Sep 03 |  |
|                   | oracle 9i Release 9.2.0.1.0   | Oracle Corporation   | EAL 4 | Sep 03 |  |
| PC 접근 제어          | Sentinel Model III  | Delta Security Technologies  | EAL 4 | Sep 02 |  |
| 주변장치 공유 스위치       | SecureSwitch Dual Network Switch, Model #5000600  | Market Central, Inc.   | EAL 4 | Oct 01 |  |
|                   | Cybox SwitchView SC, Model 520-147-004/Model 520-319-003  | Avocent Huntsville Corp.   | EAL 4 | Jul 03 |  |

(표 21) 컴퓨터 환경 정보보호 제품군 평가 사례(2)

| 제품유형  | 제품이름  | 제조업체   | 평가등급              | 유효일시   | CC스킵   |
|---|---|--|-------------------|--------|--------|
| 운영체제  | B1/EST-X, V2.0.1 with AIX, V 4.3  | Bull S.A. and IBM Informationsysteme DeutschlandGmbH                           | EAL4+             | Nov 99 |        |
|   | AIX 5L for Power V5.2, Program Number 5765-E62  | IBM Corporation  | EAL 4             | Apr 02 |        |
|   | Hewlett-Packard HP-UX (11i) Version 11.11   | Hewlett-Packard Ltd.   | EAL 4             | Sep 01 |        |
|   | Hewlett Packard Tru64 UNIX V5.1A  | Hewlett Packard Ltd.   | EAL 1             | Feb 04 |        |
|   | IRIX v 6.5.13, with patches 4354, 4451, 4452  | Silicon Graphics, Inc.   | EAL 3             | Apr 02 |        |
|   | NOKIA IPSO 3.5 and 3.5.1  | Nokia Internet Communications  | EAL 4             | Jul 03 |        |
|   | Red Hat Enterprise Linux 3  | Red Hat, Inc.  | EAL 4             | Feb 04 |        |
|   | Solaris 8 2/02  | Sun Microsystems, Inc.   | EAL 4             | Apr 03 |        |
|   | Trusted IRIX/CMW v 6.5.13, with patches 4354, 4451, 4452, 4373, 4473  | Silicon Graphics, Inc.   | EAL 3             | May 02 |        |
|   | Sun Trusted Solaris, v 8 4/01   | Sun Microsystems, Inc.   | EAL 4             | Jun 02 |        |
|   | SuSE Linux Enterprise Server V8 (BSI-DSZ-CC-0216-2003)  | SuSE Linux AG  | EAL 2             | Feb 02 |        |
|   | Sun Solaris Version 8 with AdminSuite v3.0.1  | Sun Microsystems, Inc.   | EAL 4             | Nov 00 |        |
|   | Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886                                 | Microsoft Corporation  | EAL 4+            | Oct 02 |        |
|   | 민감한 데이터 보호  | Cryptographic Security Chip for PC Clients, Manufactured by ATMEL (AT90SP0801) | IBM Corporation   | EAL 3+ | Oct 01 |
| CISCO IOS/IPSec Version: Cisco 1700, 2600, 3600, 7100, 7200 routers Both with and without optional hardware crypto accelerators Releases 12.2(6) and 12.1(10) E |   | Cisco Systems Inc.   | EAL 4             | Sep 02 |        |
| Destroy & Destroy Lite 2.01   |   | The Australian Software Company Pty Limited                                    | EAL 2             | Aug 03 |        |
| Encryption Plus® Hard Disk 7.0  |   | PC Guardian  | EAL 1             | Apr 03 |        |
| Entrust TrueDelete, Version 4.0 for Win95/NT  |   | Entrust Technologies   | EAL 1             | Mar 99 |        |
| Groove Workspace, Groove Enterprise Management Server, and Groove Enterprise Relay Server, Version 2.5  |   | Groove Networks, Inc   | EAL 2             | Sep 03 |        |
| Pointsec PC version 4.3   |   | Pointsec Mobile Technologies, Inc.   | EAL 4             | Jan 04 |        |
| SafeGuard Easy for Windows 2000, Version 1.0  |   | Utimaco Safeware AG  | EAL 1             | Apr 02 |        |
| SecureDoc Disk Encryption, version 2.0 for Windows 95/98 and Windows NT   |   | WinMagic, Inc.   | EAL 1             | Jul 99 |        |
| Sentinel Model III  |   | Delta Security Technologies  | EAL 4             | Sep 02 |        |
| Supernet 2000   |   | Electronic Engineering Systems, Inc.   | EAL 4             | Oct 00 |        |
| Tripwire Manager 3.0 with Tripwire for Servers 3.0, Tripwire Manager 3.0 with Tripwire for Servers Check Point Edition 3.0                                      |   | Tripwire, Inc.   | EAL 1             | Mar 03 |        |
| UniShred Pro V3.3.1   |   | Los Altos Technologies   | EAL 1             | Dec 02 |        |
| Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886   |   | Microsoft Corporation  | EAL 4+: CAPP_v1.d | Oct 02 |        |
| 기타  | Sharp Corporation Multifunction Device with Data Security Kit (AR-FR4 V.M.10, AR-FR5 V.E.10, AR-FR6 V.J.10) | Sharp Electronics Corporation  | EAL 2             | Dec 02 |        |
|   | Sharp Data Security Kit(AR-FR1/AR-FR2/AR-FR3) for Sharp Imager Family (FR-287, AR-337, AR-407, and AR-507)  | Sharp Electronics Corporation  | EAL 2             | Apr 01 |        |

[표 22] 인프라 지원 정보보호 제품군 평가 사례(1)

| 제품유형                                   | 제품이름   | 제조업체                                   | 평가등급                | 유효일시  | CC스킵  |
|--|--|--|---------------------|---|---|
| 네트워크(망) 관리                             | DiamondTEK   | Cryptek Secure Communications, LLC     | EAL 4               | Jun 02  |    |
|  | BMC PATROL Perform/Predict. V6.5.30  | BMC Software                           | EAL 2               | Apr 02  |    |
|  | BMC Software PATROL, V3.4.11   | BMC Software                           | EAL 2               | Sep 02  |    |
|  | Citadel Hercules® Authomated Vulnerability Remediation v2.2.0                                    | Citadel Security Software Incorporated | EAL 3               | Mar 04  |    |
|  | Harris Corporation STAT® Scanner Professional Version 5.08                                       | Harris Corporation                     | EAL 2               | Apr 03  |    |
|  | Processor Resource/System Manager (PR/SM) on IBM zSeries 800 and 900 (BSI-DSZ-CC-0213-2003)      | IBM Corporation                        | EAL 4               | Jun 03  |    |
|  | Processor Resource/System Manager (PR/SM) for the IBM eServer zSeries 900 (BSI-DSZ-CC-0178-200.) | IBM corporation                        | EAL 4               | Feb 03  |    |
|  | Securify SecurVantage™ Version 3.1   | Securify, Inc.                         | EAL 2               | Jan 04  |    |
|  | Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886                      | Microsoft Corporation                  | EAL 4+ ; CAPP_v1. d | Oct 02  |    |
| 스마트카드                                  | Philips Smart Card Controller P8WE5032 VoB   | Philips Semiconductor Hamburg          | EAL 3               | Nov 99  |    |
|  | GemXpresso Pro E64 PK - Java Card Platform, Embedded Software V3 (Core)                          | GemPlus S.A.                           | EAL 4               | Jul 02  |    |
|  | GemXplore Xpresso V3 - Java Card Platform, Embedded Software V3 (Core)                           | GemPlus S.A.                           | EAL 4               | Apr 02  |    |
|  | Sony FeliCa Contactless Smart Card RC-S860   | Sony Corporation                       | EAL 4               | Mar 02  |  |
| PKI/PMI                                | Netscape Certificate Management System 6.1 Service Pack 1  | America Online, Inc.                   | EAL 4+              | Mar 03  |  |
|  | Alacris OCSP Client Professional v4.0.0  | Alacris Corporation                    | EAL 2               | Jan 04  |  |
|  | Alacris OCSP Client Professional v3.0.0  | Alacris Corporation                    | EAL 2               | Jan 04  |  |
|  | Chrysalis-ITS LunaCA3 V3.97, Software Versions 8.0 & 8.1   | Chrysalis-ITS                          | EAL 4               | Nov 02  |  |
|  | Diversinet Passport Certificate Server® version 4.1.1  | Diversinet Corporation                 | EaL 2               | Mar 03  |  |
|  | Entrust/Authority from Entrust/PKI 5.1   | Entrust Technologies, Inc.             | EAL 3               | Feb 01  |  |
|  | Entrust/RA from Entrust/PKI 5.1  | Entrust Technologies, Inc.             | EAL 3               | Feb 01  |  |
|  | IBM Directory Server 5.1   | IBM Corporation                        | EAL 2               | Aug 03  |  |
|  | Passport Certificate Product version 4.1.1   | Diversinet                             | EAL 2               | May 02  |  |
|  | RSA Keon CA System, Version 6.5  | RSA Security                           | EAL 4+              | Dec 02  |  |
|  | SecureNet TrustedNet Connect, V 2.0  | SecureNet Limited                      | EAL 4               | May 03  |  |
|  | Timestamp Server Version: 2.0.2 Patch 1  | Baltimore Technologies Pty Limited     | EAL 3               | May 03  |  |
| UniCERT Timestamp Server Version 2.0.2 | Baltimore Technologies   | EAL 3                                  | May 03              |  |   |
| 침입탐지 시스템                               | Intrusion, Inc. SecureNet Pro Intrusion Detection System Version 4.1                             | Intrusion, Inc. SecureNet Pro™         | EAL 2               | Dec 02  |  |
|  | Symantec Manhunt Version 2.11  | Symantec Corporation                   | EAL 3               | Dec 03  |  |
|  | TipppingPoint UnityOne™ Version 1.2  | TipppingPoint Technologies, Inc.       | EAL 2               | Aug 03  |  |

[표 23] 인프라 지원 정보보호 제품군 평가 사례(2)

| 제품유형      | 제품이름  | 제조업체                      | 평가등급   | 유효일시   | CC스킵 |
|-----------|---|---------------------------|--------|--------|------|
| 기타(인증서관리) | Data-Defender V1.0  | IBH-IMPEX Elektronik GmbH | EAL 1  | May 02 |      |
|           | DEP/PCI Version 3.0                                       | Banksys N.V.              | EAL 3+ | Aug 03 |      |
|           | Netscape Certificate Management System 6.1 Service Pack 1 | America Online, Inc.      | EAL 4+ | Mar 03 |      |
|           | RSA Keon CA System, Version 6.5                           | RSA Keon CA System        | EAL 4+ | Dec 02 |      |

[표 24] 우리나라의 정보보호 제품군 분류 체계

| 대분류                | 중분류                                   | 평가 대상 제품   | 대분류                 | 중분류                  | 평가 대상 제품   |  |                      |  |
|--------------------|---------------------------------------|--|---------------------|----------------------|--|--|----------------------|--|
| 정보보호<br>기반<br>제품군  | 암호<br>지원<br>제품                        | · 암호학적 지원 모듈(암호 API 포함)<br>· 암호학적 보안 모듈<br>· 자장 중화 장치(Eraser)<br>· 기타  | 네트워크<br>정보보호<br>제품군 | 네트<br>워크<br>기반       | · 라우터 · 스위치<br>· 게이트웨이 · 무선 LAN<br>· 이동통신보안(이동단말, 기지국)<br>· IDS(네트워크기반/호스트기반 침입탐<br>지시스템)<br>· IPS(네트워크기반/호스트기반 침입예<br>방시스템)<br>· ATM 암호화장치<br>· 위성 암호화장치<br>· xDSL 암호화 장치<br>· 전화기 암호화 장치<br>· 망관리장치<br>· 트래픽 관리장치<br>· 고속 네트워크 백본용 침입탐지/예방<br>장치<br>· 기타 |  |                      |  |
|                    | 보안<br>관리<br>제품                        | · 항바이러스 및 취약성 점검도구<br>· 불건전정보차단도구<br>· 통합보안관리(ESM)<br>· 위험분석도구<br>· 기타   |                     |                      | 네트<br>워크간  | · 방화벽 · VPN · 가드(guard)<br>· 다중영역 구분 보안제품<br>· 원격 접근(remote access) 제품<br>· 기타 |                      |  |
|                    | 인증<br>솔루션<br>제품                       | · CA · RA · 권한관리기반(PMI)<br>· OCSP · SCVP · DVCS<br>· 시범확인 서비스 · DPD/DPV<br>· KMI, 키복구 제품<br>· 공개키 클라이언트 제품<br>· Single Sign-on/EAM<br>· 기타 |                     |                      |  | 컴퓨팅<br>정보보호<br>제품군   | 메일<br>보안<br>제품       | · SMIME 메일보안 제품<br>· PGP 메일보안 제품<br>· 기타 |
|                    | 생체<br>인식<br>제품                        | · 지문, 얼굴, 홍채, 정맥<br>· 서명, 화자인식<br>· 기타   |                     |                      |  |  | 단일<br>레벨<br>보안<br>제품 | · 웹서버 보안<br>· 기타                         |
|                    | 스마트카<br>드, USB<br>토큰,<br>PCMCIA<br>제품 | · 칩<br>· COS(Chip Operating System)<br>· 카드판독기<br>· 응용제품<br>· 기타   |                     |                      |  | PC 보안<br>제품  | · PC 접근 통제<br>· 기타   |  |
| 컴퓨팅<br>정보보호<br>제품군 | 서버<br>보안<br>제품                        | · 리눅스 기반 신뢰 운영체제<br>· 유닉스 기반 신뢰 운영체제<br>· 윈도우즈 기반 신뢰 운영체제<br>· 기타  | 공유<br>스위치           | · 주변 장치 공유 스위치       |  |  |                      |  |
|                    | 데이터베<br>이스제품                          | · 관계형 데이터베이스<br>· 기타   | 이동<br>코드            | · 이동 코드(mobile code) |  |  |                      |  |
|                    |                                       |  | 기타                  |                      |  |  |                      |  |

현재 KISA에서 평가중에 있는 IDS, 방화벽, VPN 등을 제외하고, 향후 우선적으로 평가가 필요한 제품들을 선정하기 위한 평가수요조사에 이 분류 체계를 활용 할 수 있을 것으로 기대된다.

**참 고 문 헌**

- [1] 김광식, 남택용, "정보보호시스템 공통평가기준 기술동향," 전자통신동향분석, 제17권 제5호,

2002. 10., pp 89-101.

- [2] 김광식, 남택용, 손승원, 박치항, "국제공동평가 기준의 평가를 받기 위한 개발자 고려사항 분석," 제18권 제1호, 2003. 2., pp 17-24.
- [3] Common Criteria Homepage, <http://www.commoncriteriaportal.org/>
- [4] CESG Homepage, <http://www.cesg.uk/site/iacs/>
- [5] Syntegra Homepage, [http://www.syntegra.com/enterprisesecurity/security\\_evaluation/s/training.htm](http://www.syntegra.com/enterprisesecurity/security_evaluation/s/training.htm)
- [6] National Institute of Standards and Technology Homepage, <http://niap.nist.gov/cc-scheme/>
- [7] NSA Homepage, <http://www.nsa.gov/isso/programs/nietp/newspgl.htm>
- [8] Chief Information office Homepage, <http://www.cio.gov.at/>
- [9] 원현심, "CCRA 가입 추진 전략 및 현황" 2002.9. pp 13-15, KISA 정보보호뉴스.
- [10] KISA Homepage 정보보호평가 평가인증제품 현황. 2003.6., <http://www.kisa.or.kr>
- [11] 류재철, 박순태, 이승환, "국의 민간평가기관 평가 동향", 정보보호학회지, 제13권 제6호, 2003.12, pp 37-54.

**〈著者紹介〉**

**오 흥 룡 (HeungRyong Oh)**  
학생회원



2002년 2월 : 순천향대학교 전자공학과 학사

2004년 2월 : 순천향대학교 정보보호학과 석사

2004년 2월~현재 : 한국정보통신기술협회(TTA)  
〈관심분야〉 보안 프로토콜, 정보보호표준

**염 흥 열 (HeungYoul Youm)**  
정회원



1981년 2월 : 한양대학교 전자공학과 학사

1983년 2월 : 한양대학교 대학원 전자공학과 석사

1990년 2월 : 한양대학교 대학원 전

자공학과 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 산학연컨소시엄센터 소장

1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사

2003년 9월~2004년 3월 ITU-T SG17/Q10, Associate Rapporteur.

2004년 3월~현재 : ITU-T SG17/QL Rapporteur  
〈관심분야〉 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안