情報保護學會論文誌
第19卷 第2號, 2009. 4

국내 정보보호 제품 평가 서비스 간소화 방안

고 웅,† 이 동 범, 곽 진‡
순천향대학교

A Simple Program of Domestic IT Product Evaluation Service

Woong Go,† Dong-bum Lee, Jin Kwak‡
Soonchunhyang University

요 약

최근 공공 및 국가 기관 등의 조직에서 다양한 정보보호 제품을 설치, 운영함으로써 안전한 시스템을 구축하고 있다. 이러한 제품의 보안성 평가를 위해 공통평가기준을 요구하고 있지만 비용과 시간적 측면에서 문제가 발생함에 따라 기업의 제품 출시 시기 및 개발 투자에 대한 어려움이 증가되고 있다. 그러므로 본 논문에서는 국내 평가 서비스와 해외의 평가 서비스 제도를 비교 분석하고, 이를 바탕으로 비용과 시간적 측면의 효율성을 제공하는 간소화된 정보보호제품 평가 방안을 제안한다.

ABSTRACT

Recently, public and national institutions establish secure system with installed and operational by IT products for security. They required the Common Criteria for assurance of IT products. However, many company hard to decide when IT products release and develop investment because of cost and spend-time problem. Therefore, in this paper, we analyze domestic and international IT products evaluation services, and proposes simplification IT products evaluation service compared with previous services.

Keywords: Common Criteria, ST Confirmation, Simplification Assessment service

I. 서 론

네트워크의 발달과 인프라의 증가로 네트워크 제품들이 다양한 환경에서 사용되게 되면서 제품이 가지고 있는 안전성에 대한 평가의 필요성이 증가하게 되었다. 현재 대부분의 공공 및 국가기관 등의 조직에서는 다양한 정보보호 제품들을 도입하기 위해 제품의 안전성에 대한 공인된 평가를 요구하고 있다. 공통평가기준(CC: Common Criteria, 이하 CC)은 이러한 요구에 의해 적용되고 있으며, 전 세계적으로 공통평가기준을 통하여 제품의 보안성 평가를 통해 정보보호 제품을 도입하는 제도를 시행하고 있다. 이에 따라 보안성 평가의 중요성이 날로 증가하고 있는 실정이다. 그러나 CC 평가는 제품을 평가하기 위해 규정된 기준의 모든 요구 사항을 수용해야 함으로 인해 기업들의 제품 출시 결정 시기와 입찰자의 개발 투자 결정시기의 결정에 어려움을 주고 있다. 또한 소요 비용과 시간 비용의 부담으로 인해 CC 평가를 고사하는 경우도 발생하고 있다.

그러므로 본 논문에서는, 기존의 국내외 평가관련 서비스들의 특징에 대하여 분석하고, 이러한 분석결과를 바탕으로 국내 정보보호 제품의 평가서비스 간소화 방안에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 국내 평가 서비스 및 해외 평가 서비스에 대하여 분석하고, 3장에서 평가서비스들의 특징 및 장·단점을 비교 분석한다. 그리고 4장에서는 비교 분석 결과를 바탕으로 국내환경에 적용 가능한 정보보호 제품 평가 간소화 방안에 대하여 제안하고, 마지막으로 5장에서 결론을 맺는다.

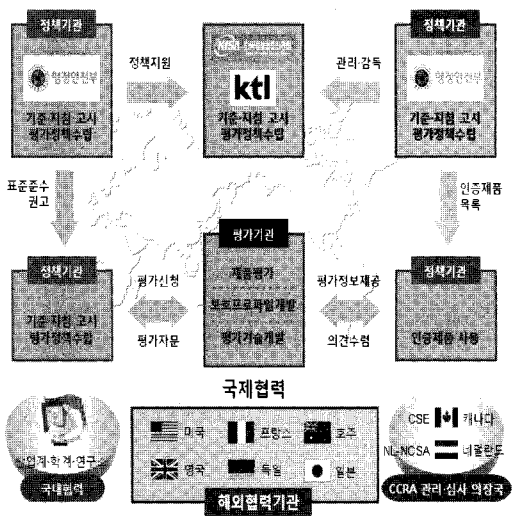
접수일(2008년 12월 11일), 게재확정일(2009년 4월 3일)
† 주저자, wgo@sch.ac.kr
‡ 교신저자, jkwak@sch.ac.kr

II. 관련 연구

2.1 정보보호시스템 평가·인증 제도

정보보호시스템의 평가 기준으로 현재 널리 사용되는 국제 공통평가기준(CC)은 정보보호시스템의 보안기능요구사항과 이를 평가하는 동안 적용하는 보증요구사항에 대한 공통의 집합을 정하여 서로 독립적으로 수행한 평가 결과들을 호환할 수 있도록 하기 위한 것이다.

국내의 정보보호시스템 평가·인증 제도는 정보보호제품의 보안기능을 검증하여 국가 정보보호 수준을 제고하고 정보보호제품의 객관적이고 공정한 평가·인증을 실시하여 제품의 경쟁력을 강화하는데 목적을 두고 있다. 이러한 제도는 국가 정보보호 수준을 향상시키고, 정보화 역기능으로부터 주요 자산을 보호할 수 있도록 국가·공공기관 사용자에게 신뢰할 수 있는 정보보호제품을 선택할 수 있는 체계의 필요성에 의해 시작되었다. 또한, 국가·공공기관 대상으로 안전성과 신뢰성이 검증된 정보보호제품 공급 및 이용 촉진을 위해 국가정보원과 행정안전부에서는 법률에 근거한 정보보호시스템 평가·인증제도 시행을 추진하고 있다[1].



〔그림 1〕 국내평가체계도

국내 평가·인증제도는 행정안전부가 정책기관, 국가정보원이 인증기관, 한국정보보호진흥원이 평가기관의 역할을 수행하고 있다.

〔표 1〕 관련 기관

구분	주관기관	주요역할
정책기관	행정안전부	- 정보보호시스템 평가 관련 법·제도 정비 - 평가관련 기준 및 지침 고시 등 정책 수립 - 정보보호시스템 개발자에 평가기준 준수 권고
인증기관	국가정보원	- 평가기관의 평가업무 감독 - 인증서 발급 및 인증제품 사후관리 - 국제상호인정협정 관련 정책결정
평가기관	한국정보보호진흥원	- 정보보호제품 평가 시행 - 평가 기준 및 방법론, 관련 기술개발 - 국제상호인정협정 관련 연구 및 활동
	한국산업기술시험원	- 정보보호제품 평가 시행
	한국시스템보증	- 정보보호제품 평가 시행

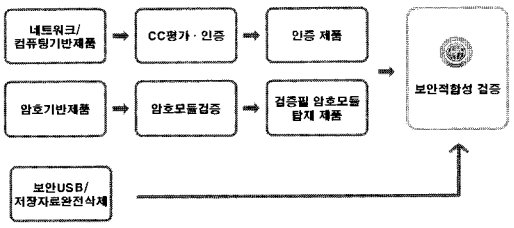
2.2 정보보호시스템 평가·인증 제도

2.2.1 보안적합성검증제도

보안적합성검증제도는 전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률 등 관계법규에 의거하여 공공기관에 도입하는 정보보호제품의 보안적합성과 안전성을 사전 검증함으로써 국가정보통신망의 보안수준을 제고하기 위해 시행하는 제도로, 전자정부법 제27조(정보통신망 등의 보안대책 수립시행) 및 국가 정보보안 기본지침 제91조에 근거하고 있다.

• 검증체계

보안적합성검증 신청의 주체는 정보보호제품 도입기관이며, 검증기관인 IT보안인증사무국이 검증대상 제품의 보안기능과 신청기관이 작성한 사용자 보안요구사항과의 일치성 여부를 검토한다. 〔그림 2〕는 보안적합성검증 체계를 나타낸다.



〔그림 2〕 보안적합성검증 체계

공공기관에서 도입하려는 네트워크 및 컴퓨팅 기반의 정보보호제품인 경우, 보안적합성검증을 통과하여야 하며, 보안성 평가를 받은 인증제품이어야만 보안적합성검증을 신청할 수 있다. 다만, 라우터, 보안 USB, 저장자료 완전 삭제 등 일반 IT 제품인 경우, CC 평가를 받지 않고 보안적합성검증을 신청할 수 있다. 암호기반 제품의 경우에는 암호검증제를 통과한 검증필 암호모듈이어야 보안적합성검증을 신청할 수 있다.

IT보안인증사무국은 검증대상제품에 대한 시험이 필요하다고 판단할 경우, 시험기관인 국가보안기술연구소에 보안적합성검증 시험을 의뢰한다. IT보안인증사무국은 검증대상제품의 시험결과와 국가암호정책의 준수여부를 참고하여 신청기관이 의뢰한 보안등급의 적합여부를 판정하여 신청기관과 관계기관에 통보한다[8].

• 검증절차

보안적합성검증절차는 사전검토 단계와 적합성시험 단계로 구분되며, 사전검토 단계에서는 시험을 위한 제출물의 완성도를 검토하고 시험단계에서는 실제 사용 환경에 기반을 둔 제품을 검증한다.

2.2.2 암호검증제도

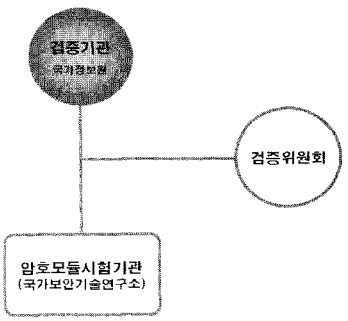
암호검증제도는 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보보호의 보호를 위해 사용하는 암호제품에 대해 안전성과 구현적합성을 검증하는 제도로서, '전자정부법 제27조(정보통신망 등의 보안 대책 수립시행)' 및 '암호모듈시험 및 검증지침'에 근거하여 시행되고 있다.

• 검증체계

암호모듈 시험기관은 국가기술보안연구소와 한국정보보호진흥원이며, IT보안인증사무국이 검증기관 업무를 수행하고 있다. 검증위원회는 관계기관, 학계, 연구기관, 검증/시험기관 등의 산·학·연 전문가로 구성하며, 시험/검증 결과의 타당성·공정성에 대한 심의/의결 및 신청인과 시험기관간 분쟁조정 등의 역할을 한다. [그림 3]은 암호검증체계를 나타낸다[8].

• 검증절차

암호모듈 시험 및 검증을 수행하기 위해 시험기관의 장은 시험반을 구성하여 검증대상 암호모듈이 시험기준에 명시된 요구조건을 만족하는지 여부를 시험한다. 만일 시험과정에서 제출물이 미비하여 시험 수행이 불가한 경우 정해진 기한 내에 신청인에게 제출물의 보완을 요청할 수 있다.



[그림 3] 암호검증체계

시험기관은 암호모듈 시험이 완료된 후, 시험결과 보고서를 검증기관에게 제출하며, 검증기관은 시험결과에 대한 검토 후 검증위원회의를 개최, 위원회의 심의결과에 따라 검증서를 발급하고 암호모듈 검증목록에 등재한다[9].

2.3 해외 평가 서비스

2.3.1 일본 ST 확인 제도

일본은 JISEC(Japan Information Technology Security Evaluation and Certification Scheme)의 보안성 평가 및 인증 제도를 통하여 자국의 IT 제품에 대한 보안성 평가를 실시하고 있다.

일본의 보안성 평가 및 인증 제도의 목적은 인증 식별 기능, 암호화 기능, 접근 통제 기능 등의 보안 기능을 갖추고 있는 하드웨어, 소프트웨어 또는 펌웨어로부터 구성되는 IT 제품 및 보호프로파일이 필요로 하는 정보 자산 및 시스템 자원을 적절히 보호하고 있는 것을 제3자가 평가 및 인증 하는 것으로써, IT 제품 또는 보호프로파일의 이용자가 정확하고 상세하게 파악할 수 있도록 하는 것을 목적으로 하고 있다. 이에 따라 높은 기술력에 근거해 적절한 평가 인증 및 ST 확인(Security Target Confirmation)을 실시하고 있다[7].

ST 확인은 보안 등급 기준 ISO/IEC 15408(Common Criteria)에 근거하여 개발자·신청자가 만든 보안목표명세서(ST: Security Target)와 기능사양을 평가 방법으로 하는 ISO/IEC 18045(CEM: Common Evaluation Methodology)에 따라 제3

자 기관이 평가하고 IPA(Information-Technology Promotion Agency)가 그 처리 결과를 확인하는 일본의 보안성 평가 서비스이다[2].

• 평가체계

ST는 일반적으로 설계 과정에서 작성한다. [그림 4]에서는 기본 설계에 대해 정보 시스템 또는 소프트웨어의 기능을 설계하는 것을 고려하고 있다. ST는 업무 사양이나 그것을 실현하는 정보 시스템 등의 기능을 설계하는 일환으로, 정보보호 측면에 관한 기능을 설계하는 것으로써 작성하는 명세서이며, 상세 설계나 코딩에 앞서 조기에 ST 평가 신청을 해야 한다.

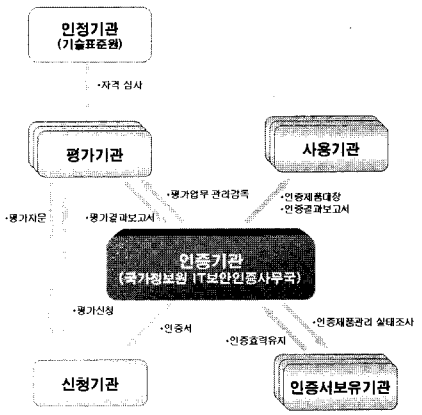
또한 ST 확인을 받는 과정에서 평가기관에 의한 평가에 대해 구현해야 할 보안기능의 추가·변경 등을 실시해야 한다. ST 확인을 완료한 후, ST 확인의 확인서가 교부되고 처음으로 정보 시스템 등에 구현하는 보안기능이 최종적으로 확정되면 정보 시스템의 구축 등에 대해 보안의 관점에서 ST 확인은 조기 완료하는 것이 중요하다.

정보 시스템의 구축 등을 외부 위탁 하는 경우에는 납품을 받기까지 위탁처에 대해 ST 확인을 완료시켜 ST 확인 확인서를 배부하는 것을 원칙으로 한다[2].

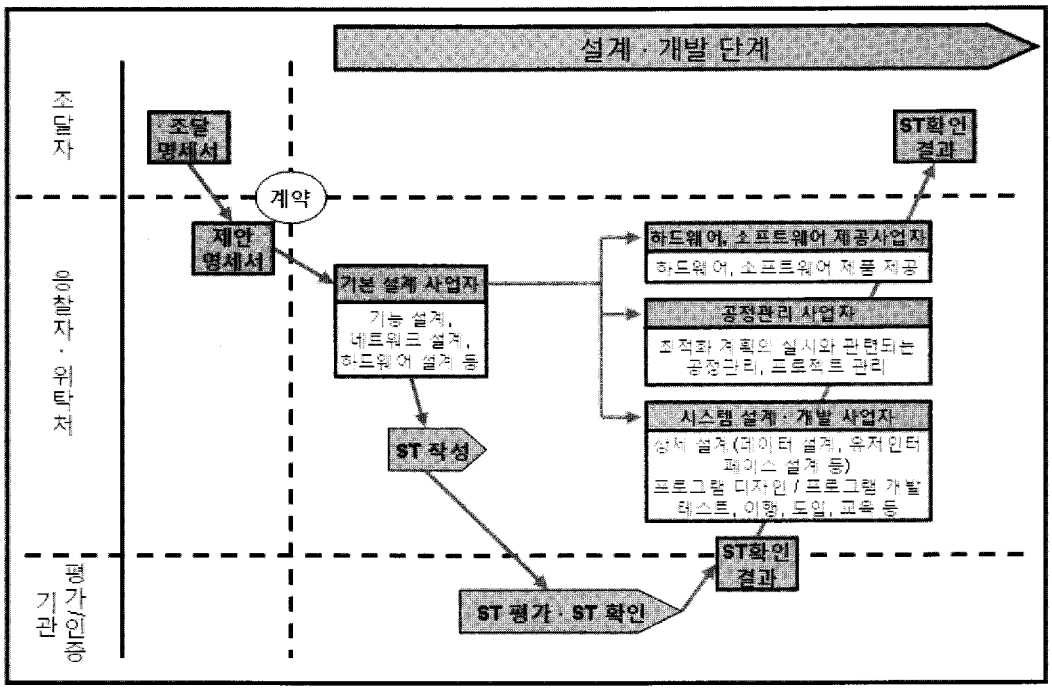
III. 평가서비스 비교 분석

국내에서는 현재 정보보호시스템 평가·인증 제도, 보안적합성검증제도, 암호검증제도(CMVP)가 진행되고 있다[3]. 하지만 CC 평가를 통하여 인증을 하는 경우, 그 기준이 복잡하고 상당한 시간과 비용이 요구되면서 기업들의 제품 출시 결정 시기와 입찰자의 개발 투자 결정시기의 결정에 어려움을 주고 있다.

그러나 일본에서는 이러한 CC 평가의 단점을 보완



[그림 5] 정보보호제품 평가인증체계



[그림 4] ST 확인 평가체계

하면서 이와 동일한 수준의 효력을 제공하는 ST 확인 제도를 운영하여 국가기관에 적용하고자 하는 IT 제품 평가에 보다 효율적으로 대처하고 있다.

〔표 2〕는 국내 평가서비스와 일본의 ST 확인 제도를 비교/분석한 결과를 정리한 것이다. 본 논문에서는, 〔표 2〕에 정리한 분석결과를 바탕으로 국내에 적용할 수 있는 정보보호 제품 평가 간소화 방안에 대하여 제안한다.

IV. 제안 방안

4.1 구성 및 절차

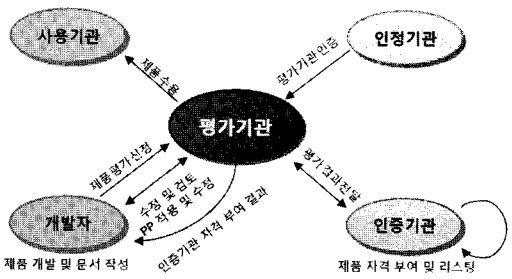
다음 〔그림 6〕은 본 논문에서 제안하는 국내 정보보호 제품 평가 간소화 서비스의 구성도를 도식화한 것이다.

본 논문에서 제안하는 국내 정보보호 제품 평가 서

〔표 2〕 국내 평가서비와 ST확인제도 비교 분석

	국내 CC 인증	보안적합성검증제도	암호검증제도	일본 ST 확인 제도
평가 신청	사용자에 의한 신청	사용자에 의한 신청	사용자에 의한 신청	사용자에 의한 신청
적용 범위	암호모듈을 제한 모든 IT 제품	CC인증 제품과 암호검증필 제품	암호 모듈 및 알고리즘	암호모듈을 제한 모든 IT 제품
PP 작성 지침	공통평가기준 준수(PP)	-	-	보안 위협과 보안목적 및 보안요구사항을 패키지화한 지침 제공
PP 준수 선언	준수 선언에 따른 2가지 방법 존재	-	-	준수 선언에 따른 2가지 방법 존재
검증 대상 설정	공통평가기준 준수(TOE)	정보보호 제품	미평가된 정보보호 제품, CC평가된 보안 제품	공통평가기준 준수(TOE)
패키지 가이드 (보안 위협, 목적, 요구사항)	없음	-	-	데이터베이스를 구축하여 PP 개발에 활용
평가 기준	공통평가기준, CEM	보안적합성시험기준 (국보연)	FIPS 140-1, 140-2	공통평가기준, CEM
제출 서류	공통평가기준 제출 서류	- CC 평가·인증 서류 - 암호모듈검증 서류	- 기본 및 상세설계 - 형상관리 - 제품 사용 설명 - 취약성 분석 대응 방법 - 개발과정 각 단개별 시험 항목, 목적, 절차, 결과 - 제품 및 원시프로그램 또는 하드웨어 설계서	보안목표명세서제출
평가 실시	모든 공통평가기준 문서의 작성 완료 후 평가 실시	- 네트워크/컴퓨팅기반 제품 - 암호기반 제품 - 보안USB/저장자료완전삭제	- 소프트웨어, 하드웨어 펌웨어 암호 모듈 및 알고리즘	- 기본 설계와 상세설계 포함하여 ST 확인 실시 - 기본 설계 후 ST확인 실시
평가 실시 시기	제품 설계 완료 후	제품 설계 완료 후	제품 설계 완료 후	제품 설계 완료 후
소요 시간	1년 이상	-	-	1년 미만
관련기관	신청기관, 평가기관, 인증기관, 인정기관, 인증서보유기관, 공인시험기관	국가보안기술연구소, 국가정보원, 각급기관	검증 신청인, 검증기관, 검증위원회, 암호모듈시험기관	신청인, 평가기관, 인증기관, 인정기관

비스 간소화 방안의 절차는 다음과 같다.



〔그림 6〕 제안 방안 구성도

① 개발자(신청기관)는 인정기관으로부터 인증을 받은 공인된 평가기관에게 제품의 평가를 의뢰한다.
② 평가기관과 개발자는 PP를 적용하고 세부 사항을 규정한다.
③ 개발자는 PP에 맞추어 제품을 개발하며 ST 문서를 작성한다.
④ 평가기관과 개발자는 총 3번의 정기적인 회의를 통하여 문서 작성 상의 문제점을 토의하고, 이를 수정한다.
⑤ 제품 개발 완료 후 최종적으로 작성된 ST 문서를 통하여 평가기관이 평가한다.
⑥ 평가기관이 평가한 결과를 인증기관에 전달하고 인증기관은 이에 대한 인증 자격 검토 후 결과를 평가기관에 전달한다.
⑦ 평가기관은 인증 결과를 개발자에게 전달하고 해당 제품의 사용기관에게도 전달한다.
⑧ 사용기관은 해당 제품을 시스템에 적용하고, 인증기관은 평가 제품을 웹사이트의 제품 리스트에 추가한다.

위의 평가 순서에 따라 제품의 개발과 함께 제출 문서를 작성하고 제품 개발 완료 후 일정기간 이내에 작성된 문서를 제출하여 평가를 받게 된다. 또한, 제품의 개발 시기 동안 개발자와 평가기관은 중간 점검 회의를 통해 문서 작성이 올바르게 진행되고 있는지 검토한다.

기존 평가서비스들이 제품 개발 완료 이후에 문서의 작성과 평가를 실시하는 것으로 인한 시간적 단점이 존재하였다. 하지만 본 논문에서 제안하는 방안은 제품의 개발과 동시에 문서 작성 및 검토를 실시하므로 시간적/비용적 효율성을 가지고 있다. 또한, 제품 개발 완료 후 평가 인증을 받지 못할 경우, 제품 수정에 막대한 예산과 시간적 손실을 가져오게 되지만, 본 논문에서 제안하는 방안은 제품의 사전 평가가 같이 진행됨으로 인해 수정의 범위가 좁고 즉각적인 수정이 가능하므로 기존의 평가서비스에 비해 효율성을 가지고 있다.

4.2 보안기능클래스 구성

보안기능클래스는 ISO/IEC 15408의 2부에 정의되어 있다. 보안기능요구사항의 목적은 TOE(Target of Evaluation)에 기대되는 보안 행동을 묘사하고, PP(Protection Profile) 또는 ST 내에 나타난 보안 목적을 충족한다. 또한, 사용자가 TOE와의 직접적인 상호작용으로 인지하거나 TOE 반응으로 인지할 수 있는 보안 특성을 명세하고 있다. 또한 TOE가 사용될 환경 내에서의 위협에 대응하며, 식별된 조직의 보안정책 및 가정 사항을 다룬다.

〔표 3〕은 CC의 보안기능클래스를 나열하고 기본 보안기능클래스를 구분하여 놓은 것이다[5].

〔표 3〕 CC의 보안기능클래스

클래스	클래스 명	설 명
FAU	보안감사	보안활동과 관련된 정보를 감지, 기록, 저장, 분석
FCO	통신	데이터를 교환하는 주체의 신원을 감지(부인방지)
FCS	암호지원	암호 운용 및 키관리
FDP	사용자 데이터 보호	사용자 데이터의 보호
FIA	식별 및 인증	사용자의 신원 확인 및 인증
FMT	보안관리	TSF(TOE보안기능성)데이터, 보안속성, 보안기능의 관리
FPR	프라이버시	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TSF 보호	TSF 데이터의 보호 및 관리
FRU	자원활용	TOE의 가용 자원을 확보
FTA	TOE 접근	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널	사용자-TSF/TSF-TSF간의 안전한 통신채널 확보

※ 기본 보안기능클래스: 보안감사, 식별 및 인증, 보안관리 클래스

현재 국내 보호프로파일의 보안기능클래스의 구성을 보면, 다음의 〔표 4〕와 같이 기본 보안기능클래스

〔표 4〕 국내 PP의 보안기능클래스 구성

	구분	기본 보안기능 이외 클래스	소계	기본 보안기능 클래스
1	침입탐지시스템 PP V2.0	TSF보호, TOE접근, 침입탐지	3	보안감사, 식별 및 인증, 보안관리
2	가상사설망 PP V2.0	암호지원, 사용자데이터보호, TSF보호, TOE접근	4	
3	침입차단시스템 PP V2.0	사용자데이터보호, TSF보호, TOE접근	3	
4	지문인식시스템 PP V2.0	사용자데이터보호, TSF보호, TOE접근	3	
5	등급기반 접근통제시스템 PP V2.0	사용자데이터보호, TSF보호, TOE접근	3	
6	침입차단시스템·가상사설망통합 PP V2.0	암호지원, 사용자데이터보호, TSF보호, TOE접근, 안전한경로/채널	5	
7	개방형 스마트카드 플랫폼 PP V2.0	암호지원, 사용자데이터보호, 프라이버시, TSF보호	4	
8	네트워크 침입방지시스템 PP V2.0	사용자데이터보호, TSF보호, 자원활용, TOE접근	3	
9	역할기반 접근통제시스템 PP V2.0	사용자데이터보호, TSF보호, TOE접근, 역할기능(확장)	4	
10	안티 바이러스 소프트웨어 PP V1.0	TSF보호, 안전한경로/채널, 바이러스차단(확장)	3	
11	네트워크 스팸메일차단시스템 PP V2.0	TSF보호, TOE접근, 스팸메일차단(확장)	3	
12	통합보안관리시스템 PP V1.0	사용자데이터보호, TSF보호, TOE접근, 안전한경로/채널	4	
13	무선랜 인증시스템 PP V1.0	암호지원, TSF보호, 안전한경로/채널	3	
14	전자여권 PP V1.0	암호지원, 사용자데이터보호, 프라이버시, TSF보호	4	식별 및 인증, 보안관리
15	보안토큰 PP V2.0	암호지원, 사용자데이터보호, TSF보호, TOE접근, 안전한경로/ 채널	5	
평균 클래스 개수			3.6	

를 제외한 그 외 보안기능클래스의 평균 개수는 3.6개로 나타나고 있다. 현재 국내에서 정의한 각 보호프로파일이 가지고 있는 보안 수준 이하의 IT 제품의 경우 기본 보안기능 클래스 이외에 2개 이하의 추가적인 클래스를 통하여 구성 할 수 있을 것으로 분석된다.

제안하는 방안은 기본 보안기능클래스 이외에 2개 이하의 추가적인 보안기능 클래스를 포함하는 제품군을 분류하고 이에 대한 보호프로파일을 기존 CC의 낮은 보증 수준의 PP/ST 구조로 정의하여 평가를 실시한다. 그리고 각 제품군에 따른 보안기능클래스를 정의하고 세부 엘리멘트는 제품의 평가의 실시 이전에 평가자와 협의하여 결정한다. 개발과 평가가 시작된 이후 3번의 중간 점검을 통하여 진행 중인 사항에 맞추어 이를 수정하여 진행한다. 이는 제품의 초기 단계에 추상적인 보안기능클래스에서 보다 세밀한 정의를 위해 필요하다.

〔표 5〕 낮은 보증수준의 PP/ST 구조[4]

낮은 보증수준의 PP/ST 구조	
PP/ST 소개	- PP/ST 참조, TOE 참조 - TOE 개요 - TOE 설명(ST)
준수 선언	- CC, PP, 패키지 준수 선언 - PP 준수 방법(PP)
보안목적	- 운영환경에 대한 보안목적
확장 컴포넌트 정의	-
보안요구사항	- 보안기능/보증 요구사항
요약명세	-

4.3 보호프로파일 준수 선언

보호프로파일(PP)은 표준에서 'PP의 목적은 TOE라고 하는 하나의 주어진 시스템 또는 제품의 집합에 대한 보안 문제를 엄격하게 기술하는 것이며, 보안 문제를 해결하기 위해 보안요구사항을 명세하되, 그에 대한 구현방법은 포함하지 않는다.'라고 정의하고 있다. 이러한 PP는 소비자에 의하여 작성되고 잠재적인 개발자와 시스템 통합자에 의하여 참고되며, 평가자에 의하여 검토되고 평가되고 있다.

국내에서 PP를 분류한 시스템들을 통하여 다양한 PP의 설정이 가능하다는 것을 알 수 있다. 이러한 제

품 구성 이외에 키보드보안, 저장자료완전삭제 제품 등과 같이 보안기능클래스의 개수를 소규모로 지정할 수 있는 구성을 분류할 수도 있다. 보안기능클래스의 소규모 분류를 통하여 각 제품군의 적합한 패키지를 만들고 이를 통하여 ST를 작성하도록 한다.

본 논문에서는 국내 환경에 맞춰 제안하는 사항으로 PP의 준수 선언 중 '입증 가능한 준수'를 기본사항으로 한다. 입증 가능한 준수는 보안목표명세서가 보호프로파일 내에 서술된 일반적인 보안 문제에 대한 적절한 해결책이라는 증거를 요구하는 보호프로파일 작성자를 위한 것이다. 가장 기본적인 규칙은, 보안목표명세서는 보호프로파일과 동등하거나 더 제한적이어야 한다는 것이다. 다음 조건이 만족되면 보안목표명세서는 보호프로파일과 동등하거나 더 제한적이라 할 수 있다[4].

- 보안목표명세서를 만족시키는 TOE는 모두 보호프로파일 또한 만족시킨다.
- 보호프로파일을 만족시키는 운영환경은 모두 보안목표명세서 또한 만족시킨다.

[표 6] 준수 선언

준수	내 용
엄격한 준수	- PP-ST: 부분-포함관계 - PP의 TOE(최소), 환경(최대) - TOE 측면 추가: 위협, OSP, O, SFR, SAR - 환경 측면 추가X: 가정사항, OE (단, OE를 O로 명세 가능)
입증 가능한 준수	- PP-ST: 동일/더 제한적 - ST는 PP와 같거나 제한적 : 보안문제정의, 보안목적, SFR (ST를 만족시키는 TOE -> PP 만족시킴) - 추가 가능: SAR

4.4 평가 절차

기존의 CC평가에서는 보호프로파일 작성 시 보안기능클래스와 보호프로파일 준수 선언을 제외한 부분은 CC의 기준을 따른다. 본 논문에서 제안하는 방안의 전체적인 평가 절차는 다음 [그림 7]과 같다.

• 보안요구사항 정의 단계

본 단계에서는 개발자와 평가기관이 최초 제품에 대한 평가를 위해 협의하는 단계이다. 개발자가 제시한 제품이 낮은 수준의 PP/ST 구조를 통하여 작성할 수 있는 보안수준을 가지고 있는지 평가하며, 이를 만족하였을 시 보호프로파일(PP) 협의를 시작한다.

보호프로파일은 낮은 수준의 PP/ST 구조를 통하여 작성하며, 기본 보안기능클래스 이외에 2개 이하의 추가적인 보안기능클래스를 정의하게 된다. 이를 위해 '입증 가능한 준수'를 기본사항으로 정하고, 정의된 제품군에 따른 패키지를 통하여 PP 참조를 실시한다.

• 설계 단계

앞서 보안요구사항 단계에서 보호프로파일을 규정하고 나면 개발자는 제품을 개발함과 동시에 ST의 작성을 실시한다. 본 단계에서는 제품을 개발함에 필요한 설계에 따라 모듈화를 하고, 이를 통하여 보호프로파일의 각 항목에 대응되는 ST의 작성을 실시하게 된다.

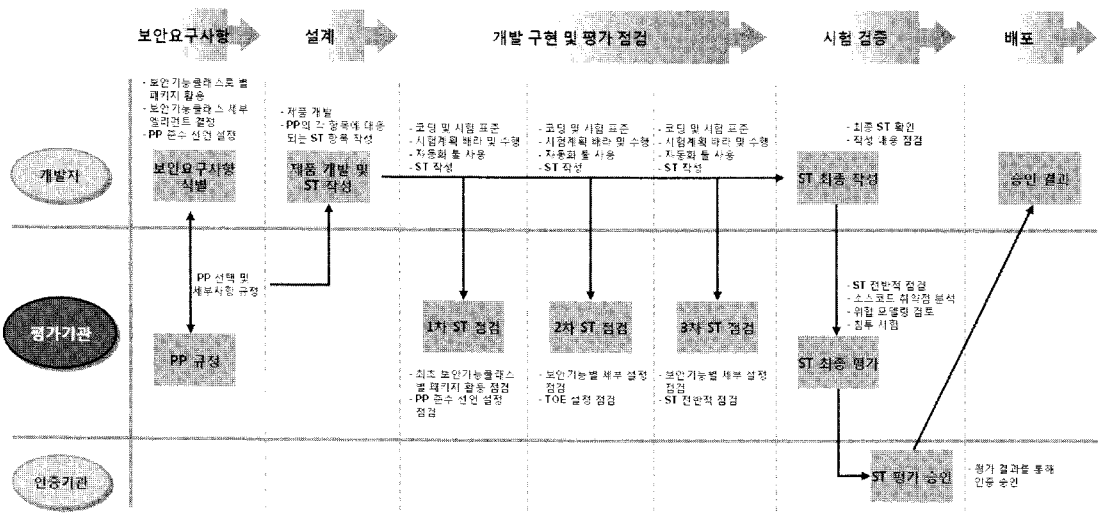
• 개발 구현 및 평가 점검 단계

본 단계에서는 앞서 설계한 제품 개발 모듈을 통하여 실제 제품의 개발 구현을 실시하며, 각 개발 모듈에 따른 ST의 작성을 실시한다. 개발자는 해당 제품의 모듈화를 단계별로 나누고 해당 사항을 평가기관에 전달하게 되며, 평가기관은 단계별 점검 구간을 설정하게 된다. 전체적인 개발 모듈에 따라 나누어진 ST 평가 점검에서는 해당 모듈에 적합하게 ST가 작성이 되는지에 대해 평가하며, 이를 만족하지 않을 시 평가기관의 지침에 따라 ST 작성의 변경을 가져올 수 있게 된다.

1차 ST 점검에서는 최초 보안기능클래스 별 패키지 적용 사항을 점검하고, PP 준수 선언 설정에 따른 작성이 이루어지고 있는지 점검한다. 또한, 제품의 모듈별 개발 사항에 대해 점검한다. 2차 ST 점검에서는 각 보안기능별 세부 설정 사항을 점검하고 적절한 TOE의 설정으로 ST의 작성이 이루어지고 있는지 점검한다. 1차 ST 점검과 마찬가지로 모듈별 개발 사항에 대해 점검한다. 3차 ST 점검에서는 ST의 전반적인 점검을 통해 최종 제품 출시에 앞서 필요한 모든 사항이 점검되었는지 확인한다.

• 시험 검증 단계

본 단계에서는 개발자가 그 동안 평가기관과 협의하여 작성한 ST의 최종본을 수정하여 제출하게 되며, 평가기관은 해당 ST의 전반적 점검, 소스코드 취약점 분석, 침투 시험 등과 같은 시험 검증을 실시하고 결



〔그림 7〕 제안 방안 프로세스

과를 인증기관에 전달하게 된다. 인증기관은 평가기관이 전달한 결과를 통하여 해당 제품에 대한 평가를 승인하게 되고 이를 개발자에게 전달하고, 웹 사이트에 리스팅 하게 된다.

V. 제안 방안 비교 분석

본 논문에서 제안한 정보보호 제품 평가 서비스 간소화 방안은 공통평가기준과 일본의 ST 확인 제도의 분석 결과를 통해 도출하였다. 따라서 본 제안 방안에 대해 공통평가기준, ST 확인 제도와 함께 비교하여 장·단점을 분석한다.

〔표 7〕 제안 방안 비교 분석

비교		CC	ST 확인	제안 방안
평가 제품 범위 축소에 의한 문서 작성 효율성	제품 범위 유연성	o	△	△
	PP 작성 지침 간소화	x	△	o
	PP 준수 선언 효율성	o	o	△
	ST 작성 지침 간소화	x	△	o
	평가 신청요건 간소화	x	△	o
	보안기능클래스 패키지 활용도	△	△	o
	제출 서류 간소화	x	o	o
제품 평가 시기에 의한 효율성	실시간 평가 가능성	x	x	o
	평가 소요 시간 단축	x	△	o
	평가 소요 비용 감소	x	△	o
	제품 수정 효율성	x	x	o
	평가에 대한 즉각적 대응	x	x	o

※ x: 낮음, △: 보통, o: 높음 (비교 항목 적용도)

〔표 7〕은 공통평가기준(CC)과 ST확인 제도, 제안하는 방안을 비교 분석한 결과이다. 비교 범위로는 '평가 제품 범위 축소에 의한 문서 작성 효율성'과 '제품 평가 시기에 의한 효율성'으로 분류하고 이에 해당하는 세부 항목으로 분류하였다. 각 항목의 적용 정도에 따라 '높음', '보통', '낮음' 으로 분류하였다.

비교 결과를 보면 CC 기준 대비 제안 방안은 평가 서비스의 간략화 및 소요 시간 단축, 비용 감소 등 다양한 장점을 통해 효율적인 평가를 진행 할 수 있음을 분석할 수 있다. 또한 제품의 실시간 평가는 CC 및 ST 확인 제도에서 실시하지 않는 부분으로 본 논문의 제안 방안에서 새롭게 제안된 평가 방식이다. 이로 인해 ST 작성에 소요되는 시간적 비용을 줄이고 문제점에 대한 즉각적 대응을 실시할 수 있게 되며 개발 중인 제품 오류 수정에 효율성을 부여할 수 있다.

- 평가 제품 범위 축소에 의한 문서 작성 효율성

- 평가 제품 범위 유연성: 제품의 범위의 경우, 평가 문서 작성의 대상 제품군을 말하며, 제품군의 다양성을 나타낸다. 기존의 CC 평가는 모든 제품군을 포함하며, ST 확인은 EAL3등급 이하와 동일한 제품군을 포함한다. 제안하는 방안은 EAL1 등급 이하와 동일한 제품군만 포함한다.
- PP 작성 지침 간소화: PP 작성 지침은 제품 평가에 필요한 문서 작성 기준을 의미한다. CC와

ST 확인 제도는 모든 PP 작성 지침을 적용하여 문서를 작성해야 하지만 제안 방안은 간소화된 작성 지침을 통해 문서를 작성한다.

- PP 준수 선언 효율성: PP 준수 선언은 엄격한 준수와 입증 가능한 준수로 나뉘며 이를 선택적으로 적용하게 된다. CC와 ST 확인 제도는 두가지 중 하나를 선택할 수 있는 유연성이 존재하고, 제안 방안은 입증 가능한 준수로 한정되어 있다.
- ST 작성 지침 간소화: PP 작성 지침을 통해 ST 문서를 작성하므로, 이와 동일한 조건을 갖는다. CC와 ST 확인 제도는 모든 PP 작성 지침을 통해 ST 문서를 작성하지만, 제안 방안은 간소화된 지침에 따라 ST를 작성하게 된다.
- 평가 신청요건 간소화: 평가 신청 시 필요한 제품의 규정에 따라 필요한 요건을 말한다. CC와 ST 확인 제도는 모든 제품군에 동일한 신청 요건이 적용되며, 이는 모든 보안 고려사항을 충족해야 한다. 하지만 제안 방안은 낮은 수준의 보안을 요구하므로 모든 고려사항을 만족하지 않아도 된다.
- 보안기능 클래스 패키지 활용도: 보안기능 클래스 패키지는 동일한 제품군에서 동일한 보안기능 클래스의 사용이 가능한 것을 말한다. CC와 ST 확인 제도, 제안 방안 모두 패키지를 활용할 수 있으나, 제안 방안에서는 제품군이 적으므로 패키지를 정의하는데 더욱 효율적이다.
- 제출 서류 간소화: 제출 서류는 평가에 필요한 문서화된 자료이다. CC 평가를 위해서는 PP, ST, CEM, TOE등 모든 평가 문서가 포함되어야 하지만, ST와 제안 방안은 미리 지정된 문서를 통해 평가 제출 서류가 간소화 된다.

• 제품 평가 시기에 의한 효율성

- 실시간 평가 가능성: 실시간 평가는 제품의 개발과 함께 진행되는 평가를 말한다. CC와 ST 확인 제도는 제품이 모두 완성된 이후에 평가가 시작되므로 실시간 평가가 불가능하다. 제안 방안은 제품의 개발 동안 3단계에 걸친 중간 점검과 지속적인 협의로 실시간으로 평가의 현황을 파악할 수 있다.
- 평가 소요 시간 단축: 평가 소요 시간은 제품의 개발 이후 소요되는 평가 시간을 말한다. CC와 ST확인 제도는 제품의 개발 후 평가 신청, ST 작성, 평가, 평가 인증 등을 거치게 되므로 오랜 시간을 요구하지만 제안 방안은 제품의 개발과 동시에 ST작성 및 평가가 진행되고 제품 개발 이후 작성된 ST문서와 제품을 평가함으로써 평가 기간을 줄일 수 있다.
- 평가 소요 비용 감소 : 평가 소요 비용은 평가에 드는 비용과 제품 수정 후 평가 비용까지 포함하고 있다. CC와 ST확인 제도는 제품 개발 수 평가로 인해 평가 인증을 받지 못할 경우 제품의 전반적이 수정이 불가피하게 되어 소요되는 비용이 많이 발생하는 반면, 제안 방안은 실시간으로 수정하며 진행되므로 이로 인한 비용문제가 발생하지 않게 된다.
- 제품 수정 효율성: 개발되는 제품의 평가 인증을 위한 추후 수정 여부를 말한다. CC와 ST확인 제도는 모든 개발이 완료된 제품에 대한 전체적인 수정을 거치므로 비효율적인 접근이 되고, 제안 방안의 경우, 즉각적인 제품 수정으로 인해 모듈 단위 수정이 가능하게 된다.
- 평가에 대한 즉각적 대응: 평가 결과에 따른 제품 변경 및 문서 작성에 대한 즉각적인 대응을 말한다. CC와 ST확인 제도는 평가 결과가 모든 제품 개발 및 ST 문서 작성 이후에 전달되므로 문제점에 대한 대응 및 수정의 시간이 오래걸린다. 하지만 제안 방안의 경우에는 중간 점검을 통해 모듈화된 개발 단계의 제품과 ST 문서를 평가 받아 상대적으로 적은 시간이 소요된다.

〔표 8〕 평가 소요 시간 비교 분석

	기존 방안(CC)	제안 방안
TFT 구성	개별적	좌동
제출물 템플릿 작성	3~6개월	1~2개월
평가 제출물 작성	3~4개월	1~2개월
평가자문 수행	약 2개월 (제출물 질에 따라 변동)	좌동
평가 진행	5~6개월 (제품의 형태 및 크기에 따라 변동)	2~3개월 (제품 개발 시 평가 동시 시행 후 최종 평가)
인증서 획득	약 1개월	좌동
총 소요 시간	최소 1년~1년 7개월 이상	최소 7개월~10개월 이상

비교 분석 결과에서도 알 수 있듯이, 일본의 ST 확인 제도 역시 기존의 CC 제도보다 효율적이고 시간과 비용을 줄이는 이점을 이끌어 내고 있지만, 제품의 평가 시기가 제품 개발 이후인 이유로 제품의 추후 수정에 필요한 시간적, 비용적 소요가 큰 것으로 분석된다. 그러나 본 논문에서 제안하는 방안은 정보보호 제품의 개발과 함께 평가를 실시함으로 인하여 보다 더 큰 효율성을 제공하고 있다.

5.1 평가 시나리오

본 논문에서 제안한 간략화 방안을 통하여 보안토큰에 대한 평가를 진행하게 되면 아래와 같이 각 단계별 적용 사항을 볼 수 있다. 최종 시험검증과 배포는 어떠한 제품에서도 동일한 평가를 진행하므로, 이에 대한 세부 사항의 분류는 적용하지 않고 진행하였다.

• 보안요구사항

개발자는 보안토큰의 평가를 위한 보안기능클래스를 적용하기 위하여 PP의 준수사항을 설정하고, TOE를 명확히 규정한다.

• 설계

제품의 개발을 위한 설계도를 작성하고 개발 계획을 수립한다. 이 때, TOE에 따라 필요한 보안기능클래스를 선택적으로 적용한다.

• 개발 구현 및 평가 점검

작성된 개발 계획을 통해 제품의 개발을 실시한다. 보안토큰을 위해 필요한 각 모듈별(암호화 모듈, 사용자 인터페이스, 접근 제어 등) 코딩 및 테스트를 실시하고, 해당 보안기능클래스별 ST 작성을 병행한다. 각 모듈별 개발이 완료된 후 최종 통합 과정을 거쳐 제품을 개발하고, 이와 동시에 TOE에 대한 설정 및 PP 준수 사항 등 기본적인 ST 작성을 병행한다.

개발 기간 동안 평가기관은 세 번의 정기적인 중간 점검을 통하여 ST의 작성이 올바른지 판단하며, 이를 수정할 수 있도록 조언한다. 또한, 수시로 개발자와 평가자가 제품 개발 시 올바른 ST 작성을 위한 협의를 진행한다.

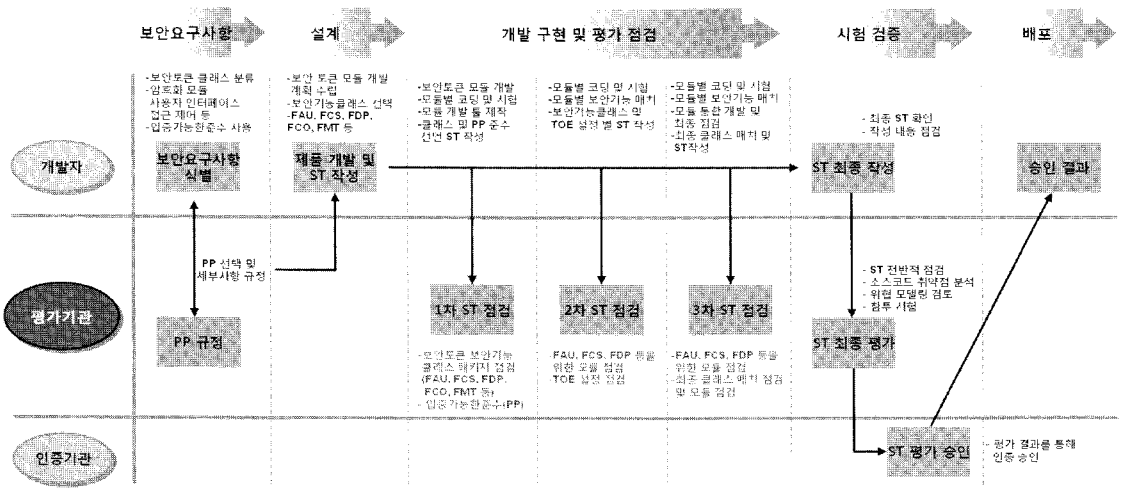
• 시험 검증

중간 점검을 통해 검증 받은 작성 분 이외의 제품 개발 후 필요한 내용을 ST 문서에 포함시키고, 이를 평가기관이 최종 점검한다. 보안토큰을 보안기능클래스 별 구현 모듈에 대해 소스코드 분석, 시뮬레이션, 테스트베드 구축 등을 실시한다.

평가 결과를 인증기관에 전달하고, 인증기관은 평가 결과를 통해 인증 승인 및 거부를 결정한다.

• 배포

개발자는 인증기관의 최종 결정된 승인 결과를 받고, 제품에 대한 평가 승인 결과에 따라 제품의 출시 및 판매를 실시한다.



〔그림 8〕 보안토큰 평가 시나리오

VI. 결 론

현재 세계적으로 정보보호 제품에 대한 보안성 평가에 대한 필요성 및 중요도가 증가하고 있는 실정이다. 그에 따라 공통평가기준이 나오게 되었으며, 현재 많은 공공기관 및 국가기관에서 공통평가기준을 통과한 제품을 요구하고 있다.

본 논문에서는 기존의 CC 평가가 가지고 있는 시간 및 비용의 문제점을 해결한 간략화 평가 서비스를 제안하였다. 이를 위하여 국내 평가 서비스와 일본의 ST 확인 제도를 비교 분석하였고, 분석 결과를 토대로 제안하는 평가 서비스에 적용하였다. 또한, 보안기능클래스를 소규모로 정의한 제품군으로 나누고 준수선언을 통한 패키지의 이용을 통해 정의하였다.

제안 방안을 통한 국내 정보보호제품에 대한 평가를 실시할 경우, 현재 소요되는 비용 및 시간의 문제점을 해결 할 것으로 기대되며, 그 간 비용과 시간상의 문제로 평가를 실시하지 못했던 제품들의 평가 요청이 증가할 것으로 기대된다. 이를 통해 국내 정보보호 제품의 안전성의 보증을 보다 증가 시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] "평가·인증 가이드," 한국정보보호진흥원, 2006년.

[2] "情報システムの構築等における ST 評価·ST 確認の實施に關する解說書," 일본 내각 관방 정보 보안 센터, 2007년.

[3] "정보보호제품 평가인증 수행규정," 국가정보원 IT 보안인증사무국, 2008년.

[4] "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 1: Introduction and general model," ISO/IEC 15408-1, Sep. 2007.

[5] "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 2: Security functional components," ISO/IEC 15408-2, Sep. 2007.

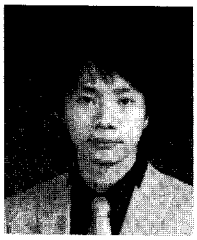
[6] "Common Criteria for Information Technology Security Evaluation version 3.1 Parts 3: Security assurance components," ISO/IEC 15408-3, Sep. 2007.

[7] 정학, 이광우, 김승주, 원동호, "보호프로파일 개발을 위한 보안요구사항 도출 방법에 관한 연구," 한국정보보호학회논문지, 17(1), pp. 133-138, 2007년 2월.

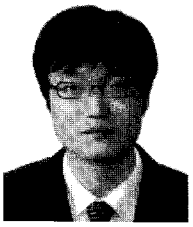
[8] 이대섭, 홍원순, "국내 평가·인증 정책의 현황 및 향후 추진방향," 한국정보보호학회지, 17(6), pp. 20-24, 2007년 12월.

[9] "암호모듈 시험 및 검증지침," 국가정보원 IT보안인증사무국, 2005년.

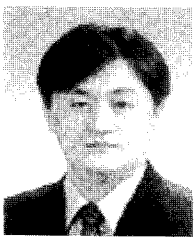
〈著者紹介〉



고 웅 (Woong Go) 학생회원
2008년 2월: 순천향대학교 정보보호학과 졸업
2008년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 보안성 평가, 개인정보보호 등



이 동 범 (Dong-bum Lee) 학생회원
2008년 2월: 순천향대학교 정보보호학과 졸업
2008년 3월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 보안성 평가, 전자여권 보안 등



곽 진 (Jin Kwak) 종신회원
성균관대학교 학사, 석사, 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재: 순천향대학교 정보보호학과 교수
〈관심분야〉 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 보안성 평가, 정보보호제품 평가, u-City 정보보호 기술 등