情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

온라인증명서 발급시스템 보호프로파일에 관한 연구*

이 현 정† , 원 동 호‡
성균관대학교 정보통신공학부 정보보호연구소

A Protection Profile for E-Document Issuing System*

Hyunjung Lee† , Dongho Won‡
Information Security Group, Sungkyunkwan University

요 약

오늘날 우리는 행정기관을 비롯하여 학교, 은행, 병원, 일반 기업 등 다양한 기관에서 해당 기관의 방문 없이 집·사무실 등 어디서든, 24시간 365일 인터넷을 통해 필요한 서류를 발행받을 수 있는 서비스를 받고 있다. 하지만, 서비스를 제공 및 이용하기 위해서는 인터넷을 통해 전달되는 정보에 대한 위변조 위협 및 출력 문서에 대한 위변조 위협에 대응할 수 있는 보안 기능이 요구된다. 이에 본 논문에서는 온라인상으로 문서를 발급하는 경우 해당 과정 동안에 발생할 수 있는 보안 위협을 도출하고, 이를 통해 온라인증명서 발급시스템이 반드시 갖추어야 할 필수 보안 기능을 공통평가기준 V3.1을 기반으로 도출하고자 한다. 이는 온라인증명서 발급시스템 평가 및 도입 시 참고자료로 충분히 활용될 수 있을 것이다.

ABSTRACT

We can use document issuance services provided by a school, bank, hospital, company, etc. either by visiting those facilities or by simply visiting their Web sites. Services available through the Internet allow us to use the same services as we do by actually going to those facilities at home or office any time. As much as it saves us time and money, there also arises a problem of information being forged on the Internet or on a printed document. There has to be security functions to deal with the problem. This paper intends to think of the possible security threats and draw out the necessary security functions that an on-line document issuance system should have based on the CC v3.1, so that anyone can use it as reference when they evaluate or introduce the system.

Keywords: E-Document Issuing System, Common Criteria, Protection Profile

I. 서 론

인터넷의 급속한 확산과 발전으로 지식정보화 사회에서 민원행정서비스의 내용과 정보전달 체계에 대한 국민들의 기대 수준과 요구 수준은 급속도로 커지고 있다. 이는 국가행정에서도 국가경쟁력을 확보하는 핵심적인 과제로서 '전자정부'의 등장으로 이어졌으며, 보다 편리하고 쉬운 민원서비스와 행정업무를 위해 민원서비스 혁신시스템인 G4C(현재 '민원24'로 개명)가 도입되게 되었다. 인터넷(온라인) 상에서의 민원서비스는 개인과 법인 등이 행정 관서를 거치지 않고

접수일(2011년 2월 16일), 수정일(2011년 10월 25일), 게재확정일(2011년 12월 9일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점 연구소 지원사업으로 수행된 연구임(2011-0020210). 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음(NIPA-2011-C1090-1001-0004).
† 주저자, hjlee@security.re.kr
‡ 교신저자, dhwon@security.re.kr

인터넷이 가능한 언제/어디서든 한 번의 클릭으로 민원을 신청하고 발급할 수 있는 서비스를 말한다.

이러한 인터넷민원서비스는 2000년 민원업무 재설계 및 정보화전략계획 수립을 시작으로 주민, 부동산, 자동차, 기업, 세금 등 5대 분야 835 종의 민원 중 이용 빈도가 높고 전자적 처리가 가능한 419종을 발굴하여 시스템을 구축하였고, 2002년 11월에 인터넷 민원서비스를 본격적으로 시작하였다. 2010년 현재 기준으로 인터넷 민원 신청 대상이 3019여종, 인터넷 열람 대상이 22여종, 인터넷 발급 대상이 1000여종으로 확대되었다[1]. 또한, 2004년 말 국세청에서 연말정산 증빙자료 인터넷 발급 분 인정을 기점으로 급속도로 금융권 전체로 인터넷 증명 발급 시스템이 보급되었으며, 각 협회, 교육기관, 일반기업뿐 아니라 병원까지 그 영역을 확대/발전하였다.

그러나 인터넷민원서비스 등 인터넷을 통한 증명서 발급 서비스에 대하여 인터넷 민원서류의 위·변조, 공인인증서의 도용, 개인정보 유출 등 다양한 형태의 정보보안 우려 및 사고의 발생 가능성에 대한 대책 마련을 통해 신뢰성 확보에 대한 요구가 제기되었다. 또한 현재 온라인 증명서 발급시스템에 대한 보안기준이 존재하지 않으므로 해당 시스템에 대한 안정성을 평가하는데 어려움이 존재한다. 이에 본 논문에서는 온라인증명서 발급시스템에 대해 정보시스템 공통평가기준 V3.1을 기반으로 보안기능요구사항을 도출하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 공통평가기준 및 보호프로파일, 온라인증명서 발급시스템에 대해 알아보고, 3장에서는 TOE 소개, 보안문제정의, 보안목적, 보안기능요구사항을 도출한다. 4장에서는 도출된 보안기능요구사항이 TOE의 안전한 운영을 보장함을 증명하고, 5장에서는 논문의 결론에 대해 기술한다.

II. 관련연구

2.1 공통평가기준 및 보호프로파일

공통평가기준(CC, Common Criteria)은 국가마다 다른 정보보호시스템 평가기준을 연계시키고 평가결과를 상호인증하기 위해 제정된 평가기준으로, IT 제품의 보안기능성과 평가 과정에서 그 제품에 적용되는 보증수단에 대한 공통의 요구사항들을 제시함으로써, 독립적으로 수행한 보안성 평가 결과들 간에 상호비교를 가능하게 한다. 공통평가기준은 소비자, 개발자, 평가자에 의해 활용되며, 소비자, 개발자는 자신이 원하는 제품의 보안기능을 공통평가기준에 의거하여 나열하고 서술할 수 있다[2].

공통평가기준은 크게 세부분으로 구성되어 있다. 제1부 소개 및 일반 모델, 제2부는 정보보호시스템에 요구되는 보안기능요구사항, 제3부는 보안보증요구사항으로 이루어져 있다. 보안기능요구사항에는 보안활동을 정의하고, 보증요구사항은 정보보호시스템이 보안수준에 맞게 정확하게 구현되어 있는지에 대한 신뢰를 입증할 수 있는 기록을 제공한다. CC의 핵심은 제2부와 제3부로 정보보호시스템이 제공해야 하는 기능 및 보증요구사항을 기술하고 있으며, 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발하거나 소비자는 자신에게 맞는 요구사항을 요청할 수 있다.

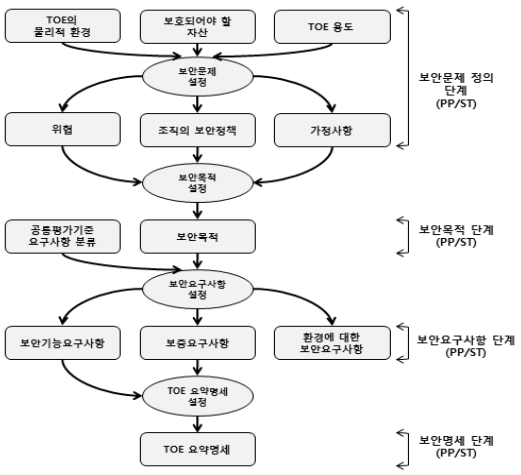
공통평가기준은 보안기능이 있는 IT제품이나 시스템 개발과 보안기능이 있는 상업용 제품 및 시스템을 선택하기 위한 지침으로 활용되며, 평가 과정에서는 대상이 되는 IT제품이나 시스템을 평가대상(TOE, Target OF Evaluation)이라고 부른다. TOE의 예로는 운영체제, 컴퓨터 네트워크, 분산시스템, 응용소프트웨어 등을 들 수 있다.

또한, 공통평가기준은 소비자 그룹과 이해집단이 그들의 보안 요구를 표현할 수 있도록 하고 보안목표명세서 작성을 용이하게 하기 위하여 보호프로파일(PP, Protection Profile)이라는 특별한 구조를 제공한다. 보안목표명세서(ST, Security Target)가 특정 TOE를 서술하는 반면, 보호프로파일은 TOE 유형(예: 침입차단시스템)을 서술한다. PP는 해당 유형의 제품에 대한 보안기능 설계 및 ST 개발의 기본 모델로써 사용됨으로 제품 개발의 잣대 및 평가 소요시간을 줄임으로써 평가의 효율성을 증대시킨다. 보호프로파일은 아래 [표 1]와 같이 보호프로파일 소개, 준수선언, 보안문제정의, 보안목적, 확장컴포넌트정의, 보안요구사항을 포함 한다[2].

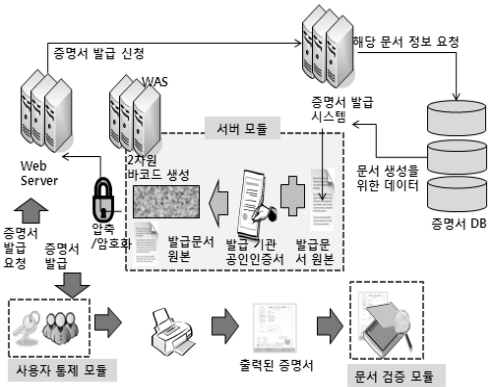
[그림 1]은 공통평가기준에서 PP를 개발하기 위한 보안요구사항에 대한 도출 과정 및 관계를 표현하고 있다. TOE의 보안요구사항은 일반적으로 TOE 및 TOE의 운영환경에 대한 보안문제정의를 도출하고 해당 분석을 기반으로 식별된 위협에 대응하고 식별된 조직의 보안정책 및 가정사항을 다루는 보안목적을 도출한다. 도출된 보안목적을 달성하기 위해 TOE가 갖추어야 할 보안요구사항에 대해 CC 2부와 3부를 통해 도출함으로써 TOE가 보안목적을 달성할 수 있음을 입증하게 된다.

〔표 1〕 보호프로파일 구성요소

구성요소	설명
보호프로파일 소개	TOE 유형에 대한 서술적인 설명문을 포함한다.
준수선언	보호프로파일이 다른 보호프로파일 또는 패키지에 대한 준수를 선언하는지의 여부와 그 대상이 어떤 보호파일 또는 패키지인지 서술한다.
보안문제 정의	TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항을 서술한다.
보안목적	보안문제의 해결책이 어떻게 TOE 보안목적과 TOE 운영환경에 대한 보안목적으로 구분되는지 서술한다. TOE 보안목적은 보안문제정의에서 서술된 문제의 위협과 조직의 보안정책부분을 해결하기 위한 보안 기능성을 제공한다. 이 해결책을 TOE 보안목적이라 하며 이는 문제해결을 위해 TOE가 달성해야 하는 목적의 집합니다. 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 지원하는 기술적, 절차적 수단을 구현한다. 이는 보안문제정의 가정사항 이나 조직의 보안정책 부분을 해결하기 위해 운영환경에서 달성해야 하는 보안사항을 기술한다.
확장 컴포넌트	공통평가기준 2부나 3부에 포함되지 않은 새로운 컴포넌트를 정의 할 경우 서술한다. (옵션)
보안요구사항	TOE 보안목적이 표준화된 언어로 표현되는 것으로, 보안기능요구사항(SFR, Security Functional Requirement)은 TOE의 보안목적을 표준화된 언어로 표현한 것이며, 보증요구사항(SAR, Security Assurance Requirement)은 TOE가 보안기능요구사항을 만족시킨다는 보증을 얻는 방법을 설명한다.



〔그림 1〕 PP의 요구사항 및 명세 유도과정



〔그림 2〕 온라인증명서 발급절차

2.2 온라인증명서 발급시스템

온라인증명서 발급시스템은 〔그림 2〕와 같이 보안기능이 구현되는 물리적인 측면에서 서버 모듈, 사용자통제 모듈, 검증 모듈로 구성된다.

서버모듈은 발급되는 전자문서의 위변조를 방지하기 위한 기능 및 사용자에게 전송되는 과정에서의 위협을 방지하기 위한 보안기능을 제공한다.

사용자통제 모듈은 사용자가 전자문서를 열람 시, 화면캡쳐 및 이미지 파일 저장 등에 의한 전자문서 데이터가 유출되는 것을 방지하기 위해 화면보호와 마우스/키보드, 메뉴 및 임시파일을 제어하는 웹브라우저 통제 기능을 제공한다. 또한, 보안 위험성이 있는 프린터를 통해 전자문서가 출력되거나 출력 임시파일에 의해 문서 데이터가 유출되는 것을 방지하는 보안인쇄 기능을 제공한다.

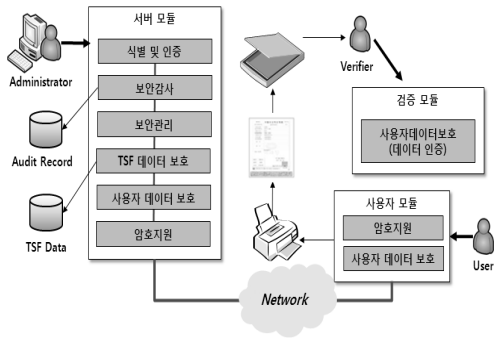
검증모듈은 출력된 전자문서의 위변조 여부를 검증하는 기능을 제공한다.

III. 온라인증명서발급시스템에 대한 보호프로파일

3.1 TOE 소개

TOE는 〔그림 3〕와 같이 온라인증명서 발급시스템의 구성요소에 따라 전자문서의 온라인 발급에 필요한 다양한 보안기능을 제공해야 한다.

- 식별 및 인증 : 보안 관리자를 유일하게 식별하여 TOE의 보안속성에 대한 접근 및 수정을 제한한다.
- 보안 관리 : TOE는 보안기능, TSF데이터, 보안역할 등과 관련된 사항을 관리한다.



〔그림 3〕 TOE 정의

- TSF보호 : TOE는 TOE보호를 위해 프로세스 및 TSF데이터에 대한 무결성 점검을 주기적으로 수행한다.
- 보안감사 : TOE는 보안 관련 행위에 대한 책임을 추적하기 위해 보안 관련 사고의 감사로그를 생성하고 기록한다.
- 사용자 데이터 보호 : 네트워크 구간의 데이터 보호 및 사용자 데이터 유출을 방지하기 위한 보안 인쇄, 화면 제어 등의 기능을 제공한다.
- 암호지원 : TOE 데이터의 기밀성을 보장하기 위하여 암호키 생성부터 폐기까지를 지원한다.
- 데이터 인증 : 출력된 전자문서의 진위여부를 확인할 수 있는 기능을 제공한다.

3.2 보안문제정의

TOE(Target of Evaluation)는 평가 대상으로 TOE 설명서, TOE를 구성하는 소프트웨어, 펌웨어 및/또는 하드웨어의 집합으로 정의되며, 본 논문에서 TOE는 온라인상으로 발급되는 전자문서의 위변조 등의 위협을 대응하는 온라인 증명서 발급시스템이다. 보안문제정의는 TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항을 서술한다. 위협은 TOE 및 TOE의 운영환경에 위험을 초래할 수 있는 모든 요소를 의미한다. 조직의 보안정책은 운영환경 내의 실제 또는 가정상의 조직에 의해 현재 및/또는 향후 부과되는 보안규칙 절차 지침을 의미한다. 가정사항은 보안기능성을 제공하기 위해 요구되는 운영환경에 대한 요구사항을 의미한다. 〔표 2〕는 본 논문이 수용하는 TOE, 즉 온라인증명서발급시스템의 운영환경 및 온라인증명서발급시스템에 존재하는 위협, 온라인증명서 발급시스템을 운영하기 위해 지켜야 하는 규칙인 조직의 보안정책 및 시스템이 운영되는 환경으로부터 제공되어야 하는 가정사항을 나타낸다.

본 TOE에 대한 위협원은 일반적으로 TOE가 보호하고자 하는 주요자산에 불법적인 접근을 시도하거나 가용성을 고갈하는 공격을 수행한다. 위협원은 일반적으로 외부에서 TOE가 보호하고자 하는 자산에 불법적인 접근을 시도하거나 비정상적인 방법으로 자산에 위해를 가하는 IT 실체 및 사용인이다. TOE가 보호하고자 하는 자산은 온라인증명서발급시스템에서 발급하는 전자문서 및 TOE 자체이다.

3.3 보안목적

보안목적은 보안문제정의에서 서술된 문제에 대한 해결책을 서술하는 것이며, TOE 보안목적과 운영환경에 대한 보안목적으로 나뉜다. TOE 보안목적은 보안문제정의에서 서술된 문제의 특정 부분을 해결하기 위한 TOE의 보안 기능성으로 제공되어야 하는 측면이며, 이는 TOE가 달성해야 하는 목적의 집합니다. 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 지원하는 기술적·절차적 수단을 말하며, 운영환경이 달성해야 하는 목적을 서술한다. 다음 〔표 3〕과 〔표 4〕는 〔표 2〕을 통해 도출된 위협, 조직의 보안정책, 가정사항에 대한 해결책을 제시하기 위해 도출된 환경에 대한 보안목적과 TOE에 대한 보안목적이다.

다음 〔표 5〕는 보안목적이 어떻게 보안문제정의에 서술된 위협, 조직의 보안정책, 가정사항으로 추적되는지를 보여주며 본 추적관계를 통해 보안목적이 적합하고 보안문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증하고 있다.

3.4 보안기능요구사항 도출

보안기능요구사항은 표준화된 언어로 TOE 보안목적을 변환한 것으로 TOE의 보안기능은 TOE 보안목적에 충족되도록 도출되어야 한다. 〔표 6〕는 〔표 4〕를 CC 2부 보안기능요구사항을 바탕으로 도출한 온라인증명서 발급시스템이 갖추어야할 필수 보안기능 요구사항이다. 〔표 7〕과 〔표 8〕은 도출된 보안기능요구사항이 보안목적을 만족시키기에 적합하고 그 결과 보안문제를 다루기에 적절함을 입증하고 있음을 보여주고 있다.

〔표 2〕 보안문제정의

위협	내 용
T.네트워크스니퍼링	위협원은 발급시스템에서 네트워크를 통해 전자문서를 발급하는 과정에서 전자문서의 데이터가 인가되지 않은 방식으로 노출, 변경, 삭제하여 악용할 수 있다.
T.화면캡쳐	Web Browser의 저장기능 및 화면캡쳐 기능 등을 이용하여 전자문서의 데이터가 유출될 수 있다.
T.임시파일저장	Web Browser의 임시파일 저장 설정을 통해 임시 디렉토리에 저장되는 경우 이를 통해 전자문서의 데이터가 유출될 수 있다.
T.프린터스풀	위협원은 인가된 사용자가 발급받은 전자문서를 프린트하는 과정에서 스풀된 상태의 전자문서를 유출할 수 있다.
T.가상프린터	위협원은 발급받은 전자문서를 프린트하는 과정에서 가상 프린터를 이용하여 전자문서의 데이터를 유출할 수 있다.
T.전자문서위변조	위협원은 출력된 증명서를 고밀도 해상도를 가진 스캐너 등을 이용하여 위/변조 할 위협이 존재한다.
T.무단복사	위협원은 발급기관에 신청한 전자문서의 발급 매수 이상을 무단 복사할 위협이 존재한다.
T.사용자위장	위협원은 연속인증시도 등 위장을 통하여 사용자 데이터 혹은 TOE에 대한 접근권한을 얻을 수 있다.
T.변경	위협원은 TOE나 자산에 접근하기 위해 TOE내의 TSF 데이터를 변경할 수 있다.
T.장애	TSF 데이터 혹은 사용자 데이터는 TOE 장애를 통해 위협원에게 변경되거나 노출될 수 있다.
조직의 보안정책	내 용
P.감사	TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 검토할 수 있어야 한다.
P.안전한관리	TOE는 인가된 관리자가 안전한 방법으로 TOE를 관리할 수 있도록 관리수단을 제공해야 한다.
P.인가된사용자	일반 사용자는 전자문서를 발급받기 전 공인인증서 등의 다양한 방법을 통해 식별 및 인증 과정을 거쳐야 한다.
P.검증모듈배포	전자문서의 진위 여부를 확인할 수 있는 SW는 누구든지 검증할 수 있도록 배포되어야 한다.
P.PC보안프로그램	전자문서를 요청하는 사용자 PC를 안전하게 보호하기 위해 PC보안 프로그램이 설치되어야 한다.
가정사항	내 용
A.신뢰된관리자	인가된 TOE 관리자는 악의가 없으며, TOE관리 기능에 대해 적절히 교육받았고, 모든 관리자 지침에 따라 정확하게 의무를 수행한다.
A.타임스탬프	TOE는 TOE운영환경이 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확하게 기록해야 한다.
A.물리적보안	온라인증명서 발급시스템은 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.
A.안전한배포및설치	사용자PC에 설치되는 TOE는 안전하게 배포, 설치되어야 한다.
A.서비스허용	TOE 서비스를 위해 필요한 모든 트래픽의 흐름은 항상 허가되어야 한다.
A.운영체제보강	온라인증명서 발급시스템은 불필요한 운영체제 상의 서비스나 수단 등을 모두 제거하는 작업과 운영제제 상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.

〔표 3〕 운영환경에 대한 보안목적

운영환경에 대한 보안목적	내 용
OE.신뢰된관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리기능에 대해 적절히 교육을 받았고, 모든 관리 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다.
OE.타임스탬프	TOE는 TOE운연환경이 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확하게 기록해야 한다.
OE.물리적보안	온라인증명서발급시스템은 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.
OE.안전한배포및설치	사용자 PC에 설치되는 TOE는 안전하게 배포, 설치되어야 한다.
OE.운영체제보강	문서발급시스템은 불필요한 운영체제 상의 서비스나 수단 등을 모두 제거하는 작업과 운영체제 상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.
OE.서비스허용	TOE 서비스를 위해 필요한 모든 트래픽의 흐름은 항상 허가되어야 한다.
OE.사용자식별및인증	온라인증명서발급시스템은 전자문서를 요청하고자하는 사용자는 전자문서를 요청하기 이전에 공인인증서 등 다양한 방법을 통해 식별 및 인증을 수행해야 한다.
OE.검증모듈배포	전자문서의 진위여부를 확인할 수 있는 SW는 누구든지 검증할 수 있도록 배포되어야 한다.
OE.PC보안프로그램	전자문서를 요청하는 사용자 PC는 안전하게 보호하기 위해 PC보안 프로그램이 설치되어야 한다.

〔표 4〕 TOE보안목적

보안목적	내용
O.전송데이터보호	TOE는 네트워크 상에서 전송되는 전자문서의 비밀성 및 무결성을 보장해야 한다.
O.화면보호	TOE는 전자문서 열람 시 화면보호 기능을 제공하여, OS에서 기본으로 제공하는 캡쳐 키(Print Screen)나 상용 캡쳐 프로그램 및 원격 제어 프로그램에 의한 열람화면의 데이터유출을 방지한다.
O.보안인쇄	TOE는 전자문서 출력 시 출력횟수 제어, 프린터 통제, 출력 임시파일 및 가상 프린터 접근통제를 통해 데이터유출을 방지하기 위해 보안인쇄 기능을 제공한다.
O.웹브라우저통제	TOE는 전자문서가 열람되는 연동 애플리케이션 (웹브라우저, 리포트 도구 등)을 통제함으로서 데이터유출방지 보안 기능을 제공한다.
O.위조방지	TOE는 2차원바코드, 워터마크, 전자서명 등을 이용하여 전자문서의 위변조를 방지하는 기능을 제공한다.
O.진위확인	TOE는 보안 출력물 상에 전자문서 등 디지털 데이터를 표현하고, 출력물의 진위여부 확인을 위한 2차원 바코드 해독 기능을 제공한다.
O.식별및인증	TOE는 관리자를 유일하게 식별해야 하고, TOE 접근을 허가하기 전에 사용자의 신원을 인증해야 한다.
O.감사	TOE는 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야 한다.
O.관리	TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.
O.저장데이터보호	TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경 또는 삭제로부터 보호해야 한다.
O.TSF장애보호	TOE의 주요 프로세스 및 실행파일의 변경, 삭제 등의 장애로부터 TSF데이터 및 사용자데이터를 안전하게 보호해야 한다.

〔표 5〕 보안문제정의와 보안목적의 대응 관계

보안문제정의 \ 보안목적	O.전송데이터보호	O.화면보호	O.보안인쇄	O.웹브라우저통제	O.위조방지	O.진위확인	O.식별및인증	O.감사	O.관리	O.저장데이터보호	O.TSF장애보호	OE.신뢰된관리자	OE.타임스탬프	OE.물리적보안	OE.안전한배포및설치	OE.운영체제보강	OE.서비스허용	OE.사용자식별및인증	OE.검증모듈배포	OE.PC보안프로그램
T.네트워크스니퍼링	X																			
T.화면캡쳐		X																		
T.임시파일저장			X																	
T.프린터스풀			X																	
T.가상프린터			X																	
T.전자문서위변조					X															
T.무단복사				X																
T.사용자위장							X													
T.변경						X				X										
T.장애								X			X									
P.감사									X											
P.안전한관리																				
P.인가된사용자																		X		
P.검증모듈배포																			X	
P.PC보안프로그램																				X
A.신뢰된관리자												X								
A.타임스탬프													X							
A.물리적보안														X						
A.안전한배포및설치															X					
A.서비스허용																	X			
A.운영체제보강																X				

〔표 6〕 TOE보안기능요구사항

보안기능 클래스	보안기능 컴포넌트		보안기능 클래스	보안기능 컴포넌트	
보안감사 (FAU)	FAU_GEN.1	감사 데이터 생성	식별및인증 (FIA)	FIA_AFL.1	인증 실패 처리
	FAU_GEN.2	사용자 신원 연관		FIA_ATD.1	사용자 속성 정의
	FAU_SAR.1	감사 검토		FIA_SOS.1	비밀정보의 검증
	FAU_STG.1	감사 증적 저장소 보호		FIA_UAU.1	인증
	FAU_STG.3	감사데이터 손실 예측 시 대응 행동		FIA_UAU.7	인증 피드백 보호
	FAU_STG.4	감사 데이터의 손실 방지		FIA_UID.1	식별
암호지원 (FCS)	FCS_CKM.1	암호키 생성	보안관리 (FMT)	FMT_MOF.1	보안기능 관리
	FCS_CKM.2	암호키 분배		FMT_MSA.1	보안속성 관리
	FCS_CKM.4	암호키 파기		FMT_MSA.2	안전한 보안속성
	FCS_COP.1	암호 연산		FMT_MSA.3	정적 속성 초기화
사용자 데이터 보호 (FDP)	FDP_ACC.1	부분적인 접근통제		FMT_MTD.1	TSF 데이터 관리
	FDP_ACF.1	보안속성에 기반한 접근통제		FMT_SMF.1	관리기능 명세
	FDP_IFF.1	단일 계층 정보 속성		FMT_SMR.1	보안 역할
	FDP_IFC.1	부분적인 정보흐름통제	TSF 보호 (FPT)	FTP_FLS.1	장애시 안전한 상태 유지
	FDP_DAU.2	증거 생성자의 신원을 포함한 데이터 인증		FPT_ITT.1	내부전송 TSF데이터의 기본적인 보호
	FDP_ITT.1	기본적인 내부전송 보호		FPT_TST.1	TSF자체 시험
	FDP_RIP.1	부분적인 잔여정보 보호	TOE접근 (FTA)	FTA_SSL.3	TSF에 의한 세션 종료

〔표 7〕 보안목적과 보안기능요구사항의 대응관계 I

보안목적 / 보안기능요구사항	O。전송데이터보호	O。화면보호	O。보안인쇄	O。웹브라우저통제	O。위조방지	O。진위확인	O。식별및인증	O。감사	O。관리	O。저장데이터보호	O。TSF장애보호
FAU_GEN.1								X			
FAU_GEN.2								X			
FAU_SAR.1								X			
FAU_STG.1								X			
FAU_STG.3								X			
FAU_STG.4								X			
FCS_CKM.1	X										
FCS_CKM.2	X										
FCS_CKM.4	X										
FCS_COP.1	X									X	
FDP_ACC.1		X	X								
FDP_ACF.1		X	X								
FDP_DAU.2					X	X					
FDP_IFC.1				X							
FDP_IFF.1				X							
FDP_ITT.1	X										
FDP_RIP.1			X	X							
FIA_AFL.1							X				
FIA_ATD.1							X				
FIA_SOS.1							X				
FIA_UAU.1							X				

〔표 8〕 보안목적과 보안기능요구사항의 대응관계 II

보안목적 / 보안기능요구사항	O. 전송데이터보호	O. 화면보호	O. 보안인쇄	O. 웹브라우저통제	O. 위조방지	O. 진위확인	O. 식별및인증	O. 감사	O. 관리	O. 저장데이터보호	O. TSF장애보호
FIA_UAU.7							X				
FIA_UID.1							X				
FMT_MOF.1									X		
FMT_MSA.1									X		
FMT_MSA.2									X		
FMT_MSA.3									X		
FMT_MTD.1									X		
FMT_SMF.1									X		
FMT_SMR.1									X		
FTP_FLS.1											X
FPT_ITT.1	X										
FPT_TST.1											X
FTA_SSL.3									X		X

IV. 결론

본 보안기능요구사항의 종속관계 중 FAU_GEN.1은 FPT_STM.1의 종속관계를 가지나, TOE는 TOE 운영환경에서 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확하게 기록하므로, FPT_STM.1 대신 운영환경에 대한 보안목적 OE.타임스탬프에 의해 FAU_GEN.1의 종속관계가 만족된다. 본 보호프로파일은 TOE에 대한 최소한의 보안요구사항을 포함하고 있으며, TOE 구현 모델에 대하여 정의하지는 않는다. TOE의 구현 모델에 따라 발생할 수 있는 사항에 대해서 개발자는 추가적인 보안문제, 보안목적, 보안요구사항을 정의해야 한다.

온라인증명서 발급시스템은 오프라인 상의 발급 부담을 획기적으로 덜어 줌으로써 문서를 언제 어디서나 편리하고 간편하게 발급 받을 수 있는 편리성을 제공하지만 그 만큼의 위험을 내포하고 있다. 본 보호프로파일에서는 온라인증명서 발급 서비스를 안전하게 사용하기 위해 시스템이 갖추어야 할 보안기능요구사항을 CC V3.1을 기반으로 도출하였다. 이에 본 논문은 온라인증명서 발급시스템을 도입하는 기관의 올바른 시스템 선택의 기준으로 사용될 수 있으며, 해당 시스템 개발자 및 해당 시스템을 평가하는 평가기관에서 참고자료로 활용될 것으로 기대된다.

참고문헌

〔1〕 송명원, IITA, 주간기술동향 1304호 "전자정부 인터넷 민원서비스(G4C)보안관리 방안," 2007년 7월.

〔2〕 정보보호시스템 공통평가기준, 1부 : 소개 및 일반 모델, 버전 V3.1r3, CCMB-2009-07-001. 2009년 7월.

〔3〕 정보보호시스템 공통평가기준, 2부 : 보안기능요구사항, V3.1r3, CCMB-2009-07-002, 2009년 7월.

〔4〕 정보보호시스템 공통평가기준, 3부 : 보증요구사항, V3.1r3, CCMB-2009-07-003, 2009년 7월.

〔5〕 조혜숙, 김승주, 원동호, "인터넷 뱅킹 시스템 관련 표준 분석 및 보호 프로파일 개발에 관한 연구,"한국정보처리학회논문지,17(3),pp.223-232, 2010년 6월.

〔6〕 홍원순, 김영태, 이완석, "기업용 바이러스차단 소프트웨어 보호프로파일에 대한 연구," 한국정보처리학회 추계학술발표대회 논문집 13(2), pp. 1541-1544, 2006년 11월.

〔7〕 무선랜 인증시스템 보호프로파일 V2.0, IT보안인증사무국, 2008년 9월.

〔8〕 소프트웨어 기반 보안USB 시스템 보호프로파일 V1.0, IT보안인증사무국, 2010년 4월.

〈著者紹介〉

이 현 정 (HyunJung Lee) 정회원
2001년 2월: 성신여자대학교 전산학과 졸업
2006년 9월~현재: 성균관대학교 전자공학과 석박사통합과정
2001년 7월~2007년 8월: 한국인터넷진흥원 연구원
2007년 9월~2008년 8월: 금융보안연구원 연구원
2008년 9월~현재: 한국시스템보증 팀장
〈관심분야〉 정보보호, 정보보호제품 보안성 평가, 개인정보보호, ISMS 등

원 동 호 (Dongho Won) 평생회원
1976년~1988년: 성균관대학교 전자공학과(공학사, 공학석사, 공학박사)
1978년~1980년: 한국전자통신연구원 전임연구원.
1985년~1986년: 일본 동경공업대 객원연구원
1998년~2003년: 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장
정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
현재: 성균관대학교 정보통신공학부 교수, BK21 사업단장, 한국정보보호학회 명예회장
〈관심분야〉 암호이론, 정보이론, 정보보호