사전 검증을 통한 행정정보보호시스템 도입 방안

Government Information Security System with ITS Product Pre-qualification

여상수*, 이동범**, 곽 진**

Sang-Soo Yeo*, Dong-Bum Lee** and Jin Kwak**

요 약

정보화 사회가 추진됨에 따라 다양한 행정정보보호시스템의 개발이 이루어지고, 국가 및 공공기관에서도 안전한 서비스 제공을 위해 행정정보보호시스템의 도입이 증가하고 있다. 특히 행정정보보호시스템은 보안성에 대한 검증이 무엇보다 중요시 되므로 행정정보보호시스템의 보안성 평가 서비스에 대한 관심이 증가하고 있다. 이에 따라 국·내외적으로 다양한 보안성 평가 서비스에 대한 연구가 진행되고 있다. 이에 본 논문에서는 영국 및 캐나다의 보안성 평가 서비스를 분석하고, 이를 바탕으로 국내의 국가 및 공공기관의 사용자에게 신뢰성을 제공할 수 있는 행정정보보호시스템의 사전 검증 도입방안에 대해서 제안한다.

Abstract

According as information-oriented society is propelled, development of various information security systems is achieved, and introduction of information security system is increasing for service offer securing from nation and public institution. In particular, government information system is increasing interest about security assessment service of government information system because verification about security is weighed first of all. Accordingly, study about various security assessment services is preceded in domestic and overseas. In this paper, analyze security assessment service of Britain and Canada, and we proposed about pre-qualification introduction plan of government information system that can offer user of nation and public institution reliability.

Key words : Government Information Security System, Pre-qualification

I. 서 론

국가 및 공공기관으로부터 행정정보보호시스템을 구축하려는 움직임이 활발해 지면서 보안성이 평가되고, 인증된 제품을 선호하게 되었다. 이로 인해 제품에 대한 보안성 인증 문제가 대두되기 시작하면서 국내·외에서 다양한 평가 서비스의 필요성이 증가하였다. 국내에서도 이러한 필요성의 증가로 암호 기능의 보증을 위한 검증필 암호모듈(CMVP : Cryptographic Module Validation Program), 공통평가기준(CC : Common Criteria)을 통한 정보보호제품 평가·인증제도, 운영 수준의 보증을 위한 정보보안관리체

* 목원대학교 컴퓨터공학부(Division of Computer Engineering, Mokwon University)
** 순천향대학교 정보보호학과(Department of Information Security Engineering, Soonchunhyang University)
· 교신저자(Corresponding Auther) : 곽진
· 투고일자 : 2009년 7월 22일
· 심사(수정)일자 : 2009년 7월 23일 (수정일자 : 2009년 10월 23일)
· 게재일자 : 2009년 10월 30일

계(ISMS : Information Security Management System) 등 다양한 보안성 평가 서비스를 제공함으로써 IT 제품의 보안기능을 검증하여 국가 정보보호 수준을 향상시키고 있다. 또한, 정보화 역기능으로부터 주요 자산을 보호할 수 있도록 국가 및 공공기관의 사용자에게 신뢰할 수 있는 정보보호 제품을 선택하는 방안을 마련하고 있다[1-3].

그러나 대부분의 제도는 제품 수준의 보증제도이거나 이미 운영되는 정보시스템에 대한 보안 관리 수준이며, 운용 및 응용 시스템에 대한 보증제도는 정착되어 있지 않다.

이러한 문제를 해결하기 위하여 영국 및 캐나다에서는 보안제품 특징과 성격에 맞는 평가와 인증을 수행하기 위한 보안성 평가 서비스를 제공하고 있으며 이외에도 다양한 시스템 평가 기준과 방법론이 개발 및 운영되고 있다[4-5].

따라서 본 논문에서는 기존의 행정정보보호시스템의 제품을 도입하기 위해 소요되는 비용과 시간의 비효율성을 고려하여 제품 명칭, 해당 제품의 암호기능 등 일반적인 요구사항을 분석하여 행정정보보호용 시스템의 제품 기능을 분석한다. 또한, 제품의 보안 기능 요구사항의 유효성 증명을 위해 시험을 통하여 인가된 제품에 보증 마크를 부여하는 스킴을 이용하여 국내 행정정보보호시스템의 사전 검증 도입 방안에 대하여 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 국내 및 국외 평가 서비스에 대해서 분석하고, 3장에서는 제안하는 행정정보보호시스템의 도입방안에 대해서 기술한다. 4장에서는 행정정보보호시스템의 도입 효과를 분석하고, 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

2-1 국내 평가 서비스

2-1-1 정보보호제품 평가·인증

정보보호제품 평가·인증은 정보보호제품의 보안기능을 검증하여 국가 정보보호 수준을 제고하고 정보보호제품의 객관적이고 공정 정보보·인증을 실시하여 제품의 경쟁력을 강화하는데 목적을 두고 있다. 이 제도는 국가 정보보호 수준을 향상시키고, 정보화 역기능으로부터 주요 자산을 보호할 수 있도록 국가 및 공공기관 사용자에게 신뢰할 수 있는 정보보호제품을 선택할 수 있는 수 보안기능에 의해 시작되었다. 또한, 국가 및 공공기관 대상으로 안전성과 신뢰능을 검증된 정보보호제품 공급 및 이용 촉진을 위해 국가정보원과 행정안전부에서는 법률에 근거록 국가 및시스템 평가 사용자에 시행을 추진하고 있다[6].

표 1은 관련기관의 역할을 나타낸다.

표 1. 정보보호제품 평가·인증 관련기관의 역할
Table 1. Role of information security product assessment and certification relevant organization

구 분	주관 기관	역 할
정책 기관	행정 안전부	· 정보보호시스템 평가 관련 법 · 제도 정비 · 평가관련 기준 및 지침 고시 등 정책 수립 · 정보보호시스템 개발자에 평가기준 준수 권고
인증 기관	국가 정보원	· 평가기관의 평가업무 감독 · 인증서 발급 및 인증제품 사후관리 · 국제상호인정협정 관련 정책결정
평가 기관	한국 인터넷 진흥원	· 정보보호제품 평가 시행 · 평가 기준 및 방법론, 관련 기술개발 · 국제상호인정협정 관련 연구 및 활동
	한국 산업기술 시험원	· 정보보호제품 평가 시행
	한국 시스템보증	· 정보보호제품 평가 시행

2-1-2 암호검증

암호검증은 국가 및 공공기관의 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용하는 암호제품에 대해서 안전성과 구현 적합성을 검증하는 제도로써, '전자정부법 제27조(정보통신망 등의 보안 대책 수립시행)' 및 '암호모듈시험 및 검증지침'에 근거하여 시행되고 있다.

암호모듈 시험기관은 국가보안기술연구소이며, IT 보안인증사무국이 검증기관 업무를 수행하고 있다. 암호검증위원회는 관계기관, 학계, 연구기관, 검증/시험기관 등의 산·학·연 전문가로 구성하며, 시험/검증결과의 타당성·공정성에 대한 심의/의결 및 신청인과 시험기관간 분쟁조정 등의 역할을 한다.

암호모듈 시험 및 검증을 수행하기 위해 시험기관

의 장은 시험반을 구성하여 검증대상 암호모듈이 시험기준에 명시된 요구조건을 만족하는지 여부를 시험한다. 만일 시험과정에서 제출물이 미비하여 시험수행이 불가한 경우 정해진 기한 내에 신청인에게 제출물의 보완을 요청할 수 있다.

시험기관은 암호모듈 시험이 완료된 후, 시험결과 보고서를 검증기관에게 제출하며, 검증기관은 시험결과에 대한 검토 후 검증위원회의를 개최하여 위원회의 심의결과에 따라 검증서를 발급하고 암호모듈 검증목록에 등재한다[7].

그림 1은 암호검증 체계를 나타낸다.

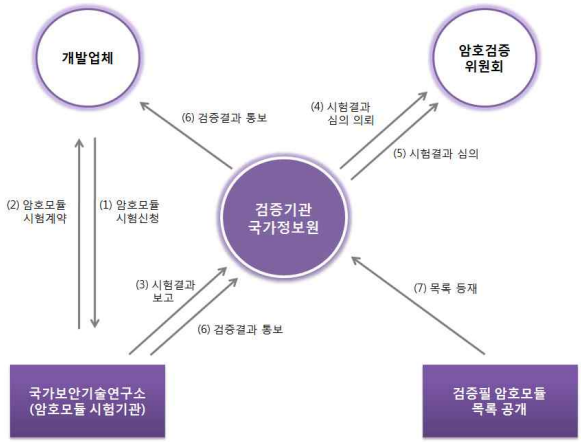

그림 1. 암호검증 체계
Fig. 1. Korea Cryptographic Module Validation Program (KCMVP)

2-2 영국 평가 서비스

2-2-1 SYS

SYS는 IT 솔루션의 보안 및 보증에 관한 영국 국방부(MOD)의 요구사항을 충족하기 위해 통신전자보안그룹(CESG : Communications Electronics Security Group)에 의해 개발된 평가 방법이며, 공통평가기준에서 파생된 것이다. 국방부의 전형적인 IT 시스템은 다양한 개발업체의 제품으로 구성되며, 하나의 데이터 센터에 도입된 시스템은 여러 사이트를 포함하는 엔터프라이즈 레벨의 솔루션으로 널리 사용되는 경우가 있어 이러한 평가 방법이 개발되었다.

SYS는 2002년에 영국의 IT 보안 평가 기준 제도(UK IT Security Evaluation Criteria (ITSEC) method)로 바뀌었다[8].

2-2-2 FTA

FTA는 시스템 레벨의 접근 방법을 통해 얻을 수 있는 이익과 접근이 모든 영국 정부 프로젝트에 대해 보다 넓게 적용할 수 있는 것을 인식한 CESG가 특정 제품의 평가 및 특정 구성요소 구현 등의 목적으로 사용할 수 있는 보다 일반적이고 유용한 fast track 평가 스킴으로 정의한 것이다.

사전에 평가에 소요되는 기간과 비용을 예측할 수 있다는 점이 특징이며, 보다 적은 비용으로 평가할 수 있다. 즉 규모가 작은 정부기관의 예산으로도 평가를 실시할 수 있도록 설계되었다.

FTA는 2001년에 CESG IA 서비스로 바뀌었다.

2-2-3 CHECK

영국 정부의 네트워크 및 솔루션을 대상으로 실시되는 모의 해킹 및 취약성 시험에 대한 기준이다. 원래는 네트워크 시험에 초점을 맞춘 것이지만, 최근에는 웹 기반 어플리케이션 및 다양한 소프트웨어 패키지의 상호작용, 상태, 사용자 지정 어플리케이션 코드의 존재에 의해 표면화하는 취약성을 대상으로 하는 시험 서비스가 추가되었다.

기밀성이 높은 정부의 정보 시스템을 인터넷에 연결하기 위해서는 모든 영국 정부 프로젝트에 대해 CHECK 서비스의 실시가 요구된다.

FTA와 달리 CC에서 파생된 것은 아니다.

2-2-4 CAPS

CAPS는 CESG의 개발업체를 대상으로 암호 기술에 대해 지원을 하는 제도이다. 개발 업체는 CAPS의 지침에 따라 정부 조달 제품을 개발하고, 해당 제품을 대상으로 CAPS 기준에 의한 평가 및 인증을 받는다. CAPS 인증을 받은 제품은 정보 조달 품목으로 보증 문서를 수여 받는다.

CAPS에서 제품이 가지고 있는 보증 레벨은 "Baseline", "Enhanced", "High Grade"의 3단계로 평가된다. Baseline은 보호 대상이 되고 있는 “Restricted” 보다 기밀성 레벨이 낮은 “Private"에 분류되는 정보 취급에 FIPS 140-2의 적합 인정 취득 제품의 사용이 권장되는 등 미국의 FIPS 140-2를 공식적으로 조달 요구사항으로 채택하고 있다.

CAPS에 근거하는 평가 결과는 CC에 의한 공식적인 평가를 통합하는 것이 가능하다[9].

2-2-5 CCTM

영국 내각 산하에서 정부기관의 정보보호 프로젝트에 대한 조정 역할을 수행하는 중앙정보보증기구(CSIA : Central Sponsor for Information Assurance)는 정보보증의 주요 고려 사항인 정보보호제품/서비스의 보안 기능에 대한 타당성을 시험하기 위해 보안검증표시 스킴(CCTM : CSIA Claims Tested Mark)을 2005년 1월에 제정하였다. 그 후 2008년 4월 7일부터 중앙정보보증기구의 소유권이 통신전자보안그룹(CESG : Communication Electronics Security Group)으로 이전하면서 보안검증표시 스킴(CCTM : CESG Claims Tested Mark)으로 명칭이 변경되었다.

표 2. 정보보증 방식의 요구사항
Table 2. Information Assurance Method Requirements

보증 요구사항	CC	SYS	FTA	CHECK	CAPS	CCTM
인증제품 마크 사용	√				√	√
상호 인정	√					
최상위 보증	√				√	
중간 보증	√	√	√		√	
최하위 보증				√		√
통과/실패 결과	√			√	√	√
위험 목록		√	√	√		
유동적 재사용	√					√
프로젝트 명세		√	√	√		
배포 명세		√	√	√		
단-대-단		√		√		
사전 명세		√	√	√		
다중제품/ 개발업체	√	√		√		
다형성 제품				√		√
구조/시스템		√		√		
서비스 전달						√
영국의 요구사항		√	√	√	√	
배포 시험		√		√		
오픈 종료/반복	√				√	
시간 범위		√	√	√		√
낮은 비용			√			
매우 낮은 비용				√		√

보안검증표시 스킴은 공공 및 개인을 위하여 보안기능 요구사항의 유효성 증명을 위해 고안된 독립적 시험을 통하여 인가된 제품에 정부 보증 품질 마크를 제공한다. 이러한 시험보고서는 ISO/IEC 17025와 영국의 인정기관(UKAS : United Kingdom Accreditation Service)에 의한 보안검증표시 스킴에 의거하여 인가를 받는다. 또한, 정보보호제품/서비스의 비용-효과 창출 및 요구사항 시험(claims testing) 기능의 능률성에 대한 정부와 산업체의 요구를 충족시킨다. 따라서 보안검증표시 스킴은 공공 및 국가 기관, 지방자치단체 등이 정보보증 요구사항을 만족하는 정보보호제품/서비스의 구매를 용이하게 한다[10].

표 2는 영국에서 사용되고 있는 각종 보안 기준의 특징을 정리한 것이다.

2-3 캐나다 평가 서비스

2-3-1 IPPP

캐나다의 정보기술 보안제품 사전검증(IPPP : ITS Product Pre-qualification Program)은 캐나다 정부 내에서 정보기술 보안제품들을 사용하기 위한 자격을 부여하기 위해서 캐나다 통신보안국 및 공공사업서비스처에서 공동으로 개발하였다. 이 제도의 목적은 캐나다 정부 내에서 통신보안국의 사전 자격 기준에 적합하게 정보기술 보안제품의 구매를 용이하게 하기 위한 목적을 가지고 있다.

정보기술 보안제품 사전검증은 캐나다 통신보안국에 의해 자격을 부여받은 정보기술 보안제품에 대하여 정보기술보안 사전자격 제품목록(IPPL : ITS Pre-qualification Product List)을 제공한다.

정보기술 보안제품이 정보기술보안 사전검증 제품 목록에 포함되기 위해서는 캐나다 통신보안국에서 규정한 다음의 요구사항 중 하나 이상을 만족해야 한다[11-12].

- FIPS 140-1 또는 FIPS 140-2로 검증된 통합 암호 모듈
- 캐나다 통신보안국의 암호보증제도로 보증된 제품
- 캐나다 공통평가기준으로 인증된 제품

정보기술 보안제품이 하나 이상의 요구사항을 만족하더라도 IT 제품에 대한 성공적인 사전 심사를 하기 위해서는 캐나다 통신보안국에 의해 수행된 시험 과정을 요구한다.

캐나다 통신보안국은 다음의 사항에 대하여 검증을 수행한다.

- 캐나다 통신보안국이 인가한 암호 알고리즘과 FIPS 140-1 또는 FIPS 140-2로 검증된 암호모듈을 사용한 제품
- CMVP, 암호보증제도, 캐나다 공통평가기준에서 검증된 제품

위의 조건을 만족할 경우, 캐나다 인증기관의 웹 사이트에서 정보기술보안 사전검증 제품 목록표로 유지 및 관리된다.

정부 기관에서는 정보기술 보안제품의 선택을 위해 제품 목록을 참고하고, 해당 제품의 구성과 사용에 관하여 캐나다 통신보안국에서는 지침을 제공한다.

정보기술보안 사전자격 제품 목록은 정보기술 보안제품 사전검증 제도에서 캐나다 통신보안국에 의해 자격을 부여받은 제품의 목록을 나타내며, 캐나다 정부의 조달 목적으로만 사용된다.

표 3은 정보기술보안 사전자격 제품 목록에 대한 분류를 나타낸다.

표 3. 정보기술보안 사전자격 제품 목록 분류표
Table 3. ITS Pre-qualified Product List Categories

정보기술보안 사전자격 제품 목록 분류	
암호화 가속기	디스크 암호화
전자상거래 응용프로그램	팩시밀리 암호화
방화벽	침입 탐지 및 방지 시스템
다기능 인쇄 및 복사	네트워크 암호화
네트워크 관리	보안 원격 접근 암호화
통신 방화벽	토큰 응용프로그램
토큰	가상 사설망
음성 암호화	무선 보안

Ⅲ. 사전 검증을 통한 행정정보보호시스템 도입 방안

본 장에서는 국가 및 공공기관에서 사용할 수 있는 행정정보보호시스템의 제품을 도입하기 위해 소요되는 비용과 시간의 효율성을 고려하여 일반적인 요구사항을 상세하게 나타낸 제품 목록을 이용하여 행정정보보호시스템의 제품을 선정하기 위한 도입 절차를 제안한다.

3-1 공통평가기준의 보안기능클래스

제안하는 시스템은 공통평가기준 평가제품군에 비해 보안 기능이 작은 저장자료완전삭제, 키보드 보안 등과 같은 제품군을 대상으로 하며 공통평가기준 평가의 기본 보안기능클래스를 제외한 그 외 보안기능클래스 개수가 2개 이하인 소규모 제품군을 대상으로 선정한다. 보안기능클래스는 ISO/IEC 15408의 2부에 정의되어 있다. 보안기능요구사항의 목적은 TOE(Target of Evaluation)에 기대되는 보안 행동을 묘사하고, PP(Protection Profile) 또는 ST(Security Target) 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 4는 공통평가기준의 보안기능 클래스를 나타내며 보안감사, 식별 및 인증, 보안관리는 공통평가기준의 기본 보안기능클래스를 나타낸다[13-15].

표 4. 공통평가기준의 보안기능 클래스
Table 4. Security function class of Common Criteria

클래스	클래스명	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 도용 방지
FPT	TSF 보호	TSF 데이터의 보호 및 관리
FRU	자원활용	TOE의 가용 자원을 확보
FTA	TOE 접근	TOE에 대한 사용자 섹션의 보호
FTP	안전한 경로 및 채널	사용자-TSF/TSF-TSF간의 안전한 통신채널 확보

3-2 행정정보보호시스템의 제품 목록표

제안하는 행정정보보호시스템은 대분류, 중분류, 제품 분류로 구분한다. 제안하는 행정정보보호시스템에 대한 목록은 제품명칭, 개발국가 및 업체, 버전, 요약설명, 암호제품 보안, 암호화 여부, 시험 정보 등을 기록하여 유지 및 관리한다. 표5는 제품 분류 기준을 나타내고, 표6은 제안하는 제품 목록표를 나타낸다[16].

표 5. 제품 분류 기준
Table 5. Standard of classification for product

대분류	중분류	제품 분류
네트워크 정보보호	네트워크 기반	· 라우터/스위치/게이트웨이
		· 무선랜
		· 이동통신 보안
		· VOIP
		· 침입탐지시스템
		· 침입방지시스템
		· 웹보안
		· 트래픽관리장치
		· 망관리장치
		· 스팸메일차단
	네트워크간	· 침입차단시스템
		· 가상사설망
		· 원격접근제품
		· SSO, EAM, IM/IAM
정보보호 기반	보안관리	· 안티바이러스
		· 취약성 분석도구
		· 통합보안관리시스템
		· DRM
		· 자료유출방지시스템
		· 저장자료완전삭제
	생체인식	· 지문/얼굴/홍채
	스마트카드	· 칩/COS
	인증솔루션	· 전자서명인증PKI
컴퓨팅 정보보호	서버 보안	· 운영체제보안
	데이터베이스	· DB보안
	메일보안	· SMIME/PGP
	디바이스 보안	· 복합기 보안
	PC 보안	· PC보안관리
		· 키보드 보안
		· 보안 USB

표 6. 제안하는 제품 목록표
Table 6. Proposing checklist

구 분	설 명	구 분	설 명
제품명칭	행정정보보호시스템의 제품에 대한 명칭	암호제품 보안	행정정보보호시스템의 제품에 대한 보안 기능과 국가 및 공공기관의 보안 요구사항을 확인 o 암호검증제도(유, 무)
개발국가	행정정보보호시스템의 제품을 개발한 국가를 표시	암호화 여부	행정정보보호시스템의 제품에 대한 암호화 여부를 표시 o 암호화 기능(유, 무)
개발업체	행정정보보호시스템의 제품을 개발한 업체를 표시	암호 알고리즘	행정정보보호시스템의 제품이 암호화 기능이 있다면, 이 부분에서 암호화 알고리즘을 표시 o 암호화 : Triple DES, AES, ARIA, RSA 등 o 디지털 서명 : RSA, DSA 등 o 키 교환 : Diffie-Hellman, RSA 등 o 해쉬 : SHA-1, SHA-256, SHA-384, SHA-512 등
제품버전	행정정보보호시스템의 제품에 대한 특정 소프트웨어나 펌웨어의 버전 번호 및 배포 번호를 표시	인증날짜	행정정보보호시스템의 제품에 대한 암호검증, 공통평가기준 인증 날짜를 표시 o 암호검증 : 2009. 00. 00 o 공통평가기준 인증 : 2009. 00. 00
제품요약 설명	행정정보보호시스템의 제품에 대한 목적과 보안 구성 및 기술적 세부 사항에 대한 설명	시험 정보	행정정보보호시스템의 제품을 시험한 플랫폼을 표시 o Windows XP Professional / 9X / ME / NT/ Server 2003 등 o HP-UX 11i v3, AIX v6.1, Solaris 9 / 10 등 o Fedora 9 / 10, Red Hat Enterprise Linux 4 / 5 등
저작권 정보	행정정보보호시스템의 제품에 대한 저작권 정보를 표시 o 개발업체가 저작권 보유 o 공개 소스, 오픈 소프트웨어	제품 지원	행정정보보호시스템을 개발한 업체의 지원 정보를 표시 o 개발업체 연락처, 홈페이지 등

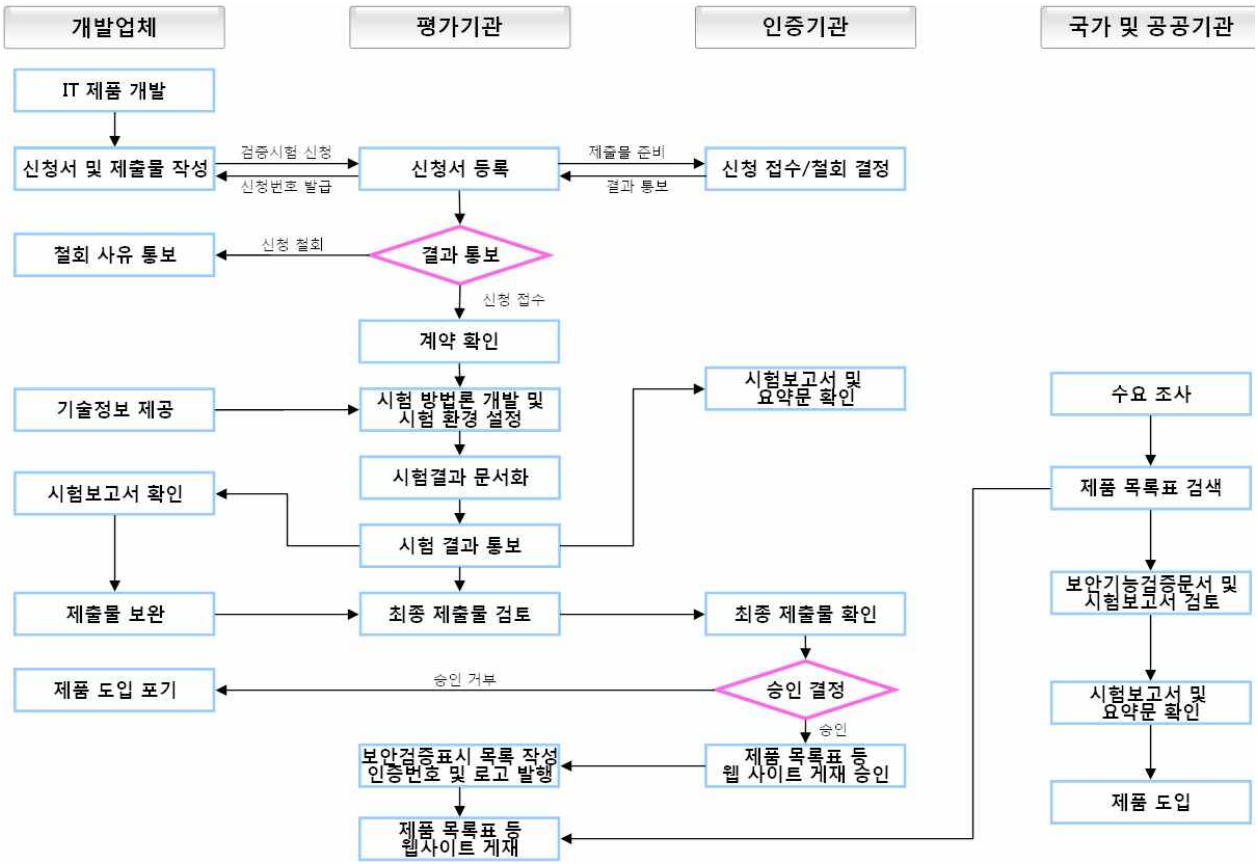

그림 2. 행정정보보호시스템 도입 절차
Fig. 2. Introduction procedure of government information system

3-3 행정정보보호시스템 도입 절차

다음은 제안하는 행정정보보호시스템의 도입 체계를 나타낸다. 제안하는 방식은 인증기관, 평가기관, 개발업체, 국가 및 공공기관으로 구성되며 행정정보보호시스템의 도입 절차는 다음과 같다.

3-3-1 준비 과정

개발업체는 등록 신청서를 제출하기 전에 평가기관의 검증시험 평가 항목에 따라 행정정보보호시스템의 보안기능검증문서를 작성한다. 다음 표 7은 평가기관의 검증시험 평가 항목을 나타낸다[17].

- 제품 기능에 대하여 명백하고 정확한 서술 제공
- 제품 기능 요구사항에 대한 요약문 포함
- 제품 버전과 플랫폼을 포함하여 명칭을 표시

표 7. 검증시험 평가 항목
Table 7. Evaluation items of verification test

항목	분류	평가요소
기능 설명	기능성	·업무형태, 업무절차의 적합 여부 ·사용자 역할별 인터페이스의 통제 여부 ·인터페이스별 기능구현의 정확여부
	사용성	·안전한 배포, 설치과정 기술 ·안전한 백업, 삭제 및 재설치 과정 기술 ·안전한 운영유지를 위한 오류 복구과정 기술 ·설명서의 일관된 기술 및 적절한 경고 포함 여부 ·모든 기능에 대한 설명서의 완전한 기술 ·기능, 인터페이스, 메시지 등 설명서의 명확 여부
	시험성	·모든 기능에 대한 시험항목의 기술 ·인터페이스의 각 매개변수, 오류메시지 등 시험절차의 상세기술 여부
기능 시험	설치 시험	·설명서의 IT환경과 시험서의 시험환경의 동일 여부 ·안전하고 오용가능성 없는 정확한 설치 기능 ·안전하고 정확한 제품 백업, 삭제 및 복구 기능
	기능 시험	·시험서의 시험결과와 실제 시험결과의 일관여부 ·인터페이스별 보안기능의 정확한 동작 여부 ·기능 설명서와 기능시험과의 일관성
취약성	취약성 식별	·암호 메커니즘의 안정여부 ·명백한 취약성 식별여부
	취약성 대처	·운영상 취약성 대처를 위한 다양한 시험 및 그 결과의 안전여부 ·사용자의 오용에 대한 대처여부 ·명백한 취약성 시험 및 취약성 대처 여부

3-3-2 등록

개발업체는 행정정보보호시스템의 시험을 신청하고, 보안검증표시를 부여받기 위해 행정정보보호시스템의 각 버전에 대한 신청서, 보안기능검증문서, 제품 목록표를 구별하여 인증기관에 제출한다.

평가기관은 스킴의 요구 사항을 만족하는 신청서를 등록하고, 개발업체는 행정정보보호시스템의 신청 번호를 발급 받는다[18].

- 행정정보보호시스템을 등록하기 위한 보안검증표시 신청서
- 행정정보보호시스템의 버전 및 플랫폼을 포함한 보안기능검증문서
- 행정정보보호시스템을 상세하게 나타낸 제품 목록표

3-3-3 신청 접수

평가기관은 인증기관이 검토 및 승인할 신청서와 제출물을 준비하고, 인증기관은 신청 접수/철회를 결정하여 평가기관에 알린다.

평가기관은 인증기관의 결정을 개발업체에게 통보하며, 신청 철회시 그 사유를 개발업체에게 통보한다. 신청 접수 시 평가기관은 개발업체의 계약서를 확인하고, 개발업체에게 신청 접수 확인을 통보한다. 스킴의 신청 접수에 정의된 조건들을 모두 만족하면 스킴 신청을 접수한다.

3-3-4 보안기능검증시험

개발업체는 스킴에 명시된 문서에 따라 보안기능검증문서를 접수한 평가기관이 시험을 진행할 수 있도록 계약을 체결하고 시험 방법론, 계획, 스크립트 제작에 필요한 모든 기술 정보를 시험 평가기관에 제공한다. 또한 필요시 기술적 설명, 기술 문서, 기술 관리자 연락처를 제공한다.

평가기관은 개발업체가 제공한 정보를 바탕으로 시험 방법론 개발과 시험 환경 설정을 위하여 사용한다.

3-3-5 시험보고서 작성

평가기관은 기능성 시험 및 평가기관 지침에 명시된 절차에 의거한 유효성 검사 및 감사 결과를 문서화해야 한다. 보안기능검증문서에 대한 모든 시험이 완료되면 평가기관은 최종 버전의 시험보고서를 개발업체에게 배포하고, 시험보고서와 시험보고서 요약문을 인증기관에 제출한다.

개발업체는 평가기관의 시험보고서에 대한 권고사항을 참고하여 보안기능검증문서를 수정하고 최종 보안기능검증문서를 작성한 후, 보안기능검증문서의 검토를 받기 위하여 평가기관에 최종 보안기능검증문서를 제출한다.

평가기관은 최종 보안기능검증문서, 시험보고서, 시험보고서 요약문을 인증기관에 제출한다.

3-3-6 보안검증표시 부여

평가기관은 인증기관이 검토할 시험보고서, 시험보고서 요약문, 최종 보안기능검증문서, 제품 목록표 및 보안검증표시 부여 절차를 준비한다.

인증기관은 시험보고서와 최종 보안기능검증문서에 대해서 다음 사항을 검토하고 보증한다[19].

- 스킴 기술 및 절차에 대한 보안기능검증문서의 권고 및 지침을 기반으로 각 신청서에 적용하는 것을 보증
- 보안기능검증시험 수행 및 보안검증표시를 부여하기 전에 보안기능검증문서의 요구사항에 대한 유효성과 무결성을 보증
- 보안기능검증문서의 시험 방법론이 보안기능검증문서의 모든 요구사항과 명백한 취약성을 다루며, 플랫폼의 조합이 관련 결함에 적합함을 보장
- 시험보고서의 검토를 기반으로 보안검증표시 부여 최종 결정
- 상위 기관의 권고에 따른 기준 및 절차의 정기적인 검토 보증

인증기관은 시험보고서를 검토하고 행정정보보호시스템에 대한 보안검증표시 부여 여부를 결정한다.

인증기관은 행정정보보호시스템의 보안검증표시 부여 여부를 검증하여 시험보고서 요약문, 최종 보안기능검증문서, 제품 목록표를 웹사이트에 게재하는

것을 승인한다.

평가기관은 인증기관의 결정을 개발업체에게 통보하고, 보안검증표시 부여가 승인되지 않으면 신청이 철회된다.

인증기관에 의해 보안검증표시 부여가 승인되면, 평가기관은 다음과 같은 사항을 수행한다.

- 스킴을 승인 받은 최종 보안기능검증문서, 시험보고서 요약문, 제품 목록표를 웹사이트에 게재
- 행정정보보호시스템의 명칭을 보안검증표시 부여 목록에 게재
- 개발업체에게 배부되는 인증번호와 보안검증표시 로고 발행

3-3-7 수요 조사

국가 및 공공기관은 업무에 필요로 하는 상용 제품으로서 조달 계약을 통해 구매하고자 하는 행정정보보호시스템에 대하여 각 기관을 대상으로 수요조사를 실시한다.

국가 및 공공기관은 각 기관의 운영 환경에 적합한 행정정보보호시스템의 제품 목록표를 검색하고, 평가기관이 제출한 최종 보안기능검증문서와 시험보고서를 검토하여 행정정보보호시스템을 최종 선정한다.

Ⅳ. 분 석

4-1 인증기관

인증기관에서는 스킴 기준 및 절차의 정기적인 검토와 보안기능문서의 요구사항에 대한 유효성과 무결성을 보증함으로써 평가기관에서 수행하는 시험의 신뢰성을 보증한다. 또한 해당 제품의 보안검증표시 부여에 대한 최종결정을 내린다.

4-2 평가기관

평가기관에서는 개발업체가 제출한 행정정보보호시스템의 제품 목록표를 검증하기 위해 검증시험 평가 항목을 토대로 보안기능시험을 실시하고 시험 보고서를 작성하여 국가 및 공공기관에서 제품을 도입할 때 유용한 자료로 사용할 수 있다.

4-3 개발업체

개발업체는 행정정보보호시스템의 제품을 개발하고 제품 목록표를 작성한다. 또한 보안검증표시 스킴을 신청하여 평가기관에서 시험을 받고 인증기관에서 보안검증표시를 부여 받아 국가 및 공공기관에 행정정보보호시스템의 제품을 납품할 수 있다.

4-4 국가 및 공공기관

국가 및 공공기관에서는 각 기관의 수요조사를 실시한 후 평가기관에서 시험을 받고, 인증기관에서 보안검증표시를 부여 받은 행정정보보호시스템의 제품 목록표를 평가기관의 웹 사이트에서 검색한다. 이로써 국가 및 공공기관에서는 사전에 검증을 받은 행정정보보호시스템을 선정하고 도입할 수 있다.

Ⅴ. 결 론

본 논문에서는 국내에서 시행되고 있는 정보보호 제품 평가·인증과 암호검증을 분석하였다. 또한 영국과 캐나다의 보안성 서비스를 분석하고, 이를 기반으로 국내에 적용할 수 있는 행정정보보호시스템의 사전 검증 도입 방안에 대해서 제안하였다. 본 연구의 결과는 행정정보보호 제품을 도입하기 위해 소요되는 비용과 시간의 비효율성을 개선할 수 있는 초석을 마련하고, 추후 국내 행정정보보호시스템의 개발 및 도입을 위한 기반 프레임워크로 발전할 것으로 기대된다.

참 고 문 헌

[1] http://csrc.nist.gov/
[2] http://www.commoncriteriaportal.org/
[3] http://www.kisa.or.kr/

[4] http://www.cse-cst.gc.ca/
[5] http://www.cesg.gov.uk/
[6] 국가정보원IT보안인증사무국, "정보보호제품 평가인증 수행규정", 2008.
[7] http://www.kecs.go.kr
[8] http://www.stsc.hill.af.mil
[9] http://www.cesg.gov.uk
[10] CESG, "Government Quality Mark-Directory of CESG Claims Tested Mark(CCTM) Awards for Products and Services", March 2009.
[11] NIST, "FIPS Publication 140-3(Draft) : Security Requirements for Cryptographic Modules", July 2007.
[12] CSEC, “Canadian Common Criteria Evaluation and Certification Scheme(CCS) Scheme Description, May 2000.
[13] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation", version 3.1, Parts 1, 2007.
[14] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation", version 3.1, Parts 2, 2007.
[15] ISO/IEC 15408, "Common Criteria for Information Technology Security Evaluation", version 3.1, Parts 3, 2007.
[16] NIST, "Special Publication 800-70 : Security Configuration Checklists Program for IT products - Guidance for Checklists Users and Developers", May 2005.
[17] CESG, "CESG CLAIMS TESTED MARK SCHEME : VENDOR GUIDE", March 2009.
[18] CESG, "CESG CLAIMS TESTED MARK SCHEME : TEST LABORATORY GUIDE", March 2009.
[19] CESG, "CESG CLAIMS TESTED MARK SCHEME : DECISION AUTHORITY GUIDE", February 2009.

여 상 수 (呂相壽)

200년 8월 : 중앙대학교 공학박사
2006년 3월~2007년 2월 : 단국대학교 강의전임강사
2007년 2월~2008년 1월 : 큐슈대학교 정보공학부 방문연구원
2008년 2월~2009년 2월 : (주)비티웍스 연구개발본부 부장
2009년 3월~현재 : 목원대학교 컴퓨터공학부 전임강사
관심분야 : 정보보호 기술 및 정책, 멀티미디어 시스템, 임베디드 시스템

이 동 범 (李東範)

2008년 2월 : 순천향대학교 정보보호학과(공학사)
2008년 3월~현재 : 순천향대학교 정보보호학과 석사과정
관심분야 : 정보보호, 보안성 평가, 전자여권 보안 등

곽 진 (郭鎭)

1994년~2006년 : 성균관대학교 전자공학과 (공학사, 공학석사, 공학박사)
2006년 4월~2006년 11월 : 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재 : 순천향대학교 정보보호학과 교수
관심분야 : 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, u-City 정보보호 기술 등