www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2012.17.4.057

CC인증이 정보보호 솔루션의 보안성에 미치는 영향 분석

Analysis of the Effects of Common Criteria Certification on the Information Security Solutions

홍영란(Young Ran Hong)*, 김동수(Dongsoo Kim)**

초 록

IT 정보보호 제품의 기능과 기술이 다양해지고 복잡해짐에 따라 제품 기능을 표준화할 필요가 생겼다. 이에 따라 2000년에 정보보호 제품의 보안 기능을 표준화한 CC(Common Criteria)인증 평가제도가 국내에 도입되었다. CC인증은 정보보호 솔루션이 갖추어야 할 보안기능 요구사항과 기능 명세의 문서화에 대해 엄격한 논리적 틀을 요구한다. CC인증을 도입한 이래 10년 이상이 지나는 동안 많은 정보보호 제품이 CC인증이 요구하는 사항에 따라 기능을 개발해왔다. CC인증의 실무자들과 심사 평가자들은 CC인증이 정보보호제품에 긍정적 효과를 주고 있다고 생각한다. 따라서 CC인증이 국내의 보안 솔루션에 미친 긍정적 효과에 대해 실증적으로 증명할 필요가 있다. 본 연구는 CC인증이 요구하는 보안의 기본적 요구사항을 고려하지 않고 제품을 개발했을 경우와 고려하여 개발한 경우를 비교 분석한다. 본 연구에서는 CC인증 효과의 비교 분석을 위해 국내 보안 솔루션 벤더들을 대상으로 설문지 기법을 사용하였다. 설문지 결과를 바탕으로 CC인증의 기본적 요구사항이 보안 솔루션에 끼친 긍정적 효과를 실증적으로 분석함으로써 CC인증이 정보보호제품 자체의 보안성 강화에 긍정적인 효과를 끼치고 있음을 입증한다. 본 연구는 국내에서 CC인증 효과의 실증조사라는 점에서 그 의의를 가진다.

ABSTRACT

As the functions and technology of IT security solution has been diversified and complicated, it is necessary to make the functions standardized. The common criteria (CC) evaluation and certification scheme was introduced with this background in 2000. For over 10 years after the introduction of CC evaluation and certification scheme, many security solution vendors have developed functions following the security functional requirement in CC. Most of CC evaluators and developers think that CC has helped to enhance the security of the solution. So, it is a right time to prove the affirmative effects of CC in quantity. In this research, we compare two cases, the security status of the solution before and after the experience of CC evaluation, and analyze the results. We made the questionnaire

* Dept of Industrial Information Systems Engineering, Soongsil University
** Corresponding Author, Dept of Industrial Information Systems Engineering, Soongsil University (E-mail : dskim@ssu.ac.kr)
2012년 08월 25일 접수, 2012년 09월 13일 심사완료 후 2012년 09월 28일 게재확정.

for the domestic solutions vendors. We show that CC has made positive effects on the security of the solution quantitatively using statistical analysis. This research is meaningful in that it is the first trial to measure the affirmative effects of Common Criteria on the security enhancement of domestic security solutions.

키워드 : CC인증, 평가 대상, 기밀성, 가용성, 무결성, 보호프로파일
Common Criteria, TOE(Target of Evaluation), Confidentiality, Integrity, Availability, Protection Profile

1. 서 론

IT 정보보호 솔루션 기능은 주로 고객의 요구사항에 따라 개발되어왔다. 이런 현상은 정보보호 제품의 패키지화나 표준화를 저해하는 요소로 작용한다. 이런 시장의 배경 때문에 국내 정보보호 제품의 체계적인 발전이 쉽지 않다. 이 현상은 제품을 도입하는 고객의 입장에서도 기능적 측면에서 어떤 것을 기준으로 보안제품을 선택할지에 대해 어려움을 주게 된다. 따라서 정보보호 담당자들은 정보보호 제품이 가져야 할 표준적인 기능과 기본 보안 사항을 보증할 수 있는 권위 있는 기준을 마련해줄 것을 요구하게 되었다.

2000년, CC인증이 국내에 소개되었다. CC인증은 보안 기능 요구사항, 안전한 개발 환경 그리고 안전한 개발 프로세스를 평가의 기본 요소로 정의하고 있다. 따라서 CC인증을 획득하고자 하는 개발 벤더들은 제품의 기획에서 구현에 이르는 전체 과정에 이런 요구사항을 반영해야 한다[7].

CC인증이 도입되기 전까지는 앞서 언급한 것처럼 고객의 요구사항에 따라 그때그때 기능이 개발되어 솔루션에 응용되는 경우가 많았고 따라서 개발 벤더들의 경우, 솔루션 자체가 갖는 보안성에 대해 크게 신경을 쓰지 않았다. 따라서 CC인증이 도입되고 10년 지난 이제 CC인증을 경험한 회사들이 이후 정보보호 솔루션을 기획할 때, CC인증에서 요구하는 기본적인 보안성을 얼마나 고려하여 제품을 구현하고 있는지에 대해 객관적으로 살펴볼 필요가 있다[12].

본 연구에서는 CC인증이 IT 정보보호 솔루션의 보안성 강화에 긍정적 영향을 끼치고 있음을 입증한다. 이 연구를 위해 설문지 기법이 사용되었고 결과를 통계적으로 분석한다. 해당 설문지를 받은 대상 개발 벤더들의 자격은 위해 3회 이상 CC인증 경험이 있는 곳으로 제한하였다. 이는 CC인증 경험이 인증 이후에 기획되는 신제품에 미치는 보안성 강화 효과를 측정하기 위해서다. 보안성 강화의 개념을 신제품 기획에 반영하는지 여부를 알아보기 위해 개발 벤더 별로 인증 경험 이전 솔루션 한 개와 인증 경험 이후 솔루션 한 개씩, 두 개를 비교하는 방법을 사용하였다.

본 연구의 설문은 CC인증 경험을 한 이후, 신제품이 자체적인 보안성 강화를 위해 어떤 기준을 가지고 기획하고 구현하는가에 초점을 맞추었다. 그리고 설문 결과에 대해 간단한 통계분석 기법을 사용하여 그 효과를 증명하였다.

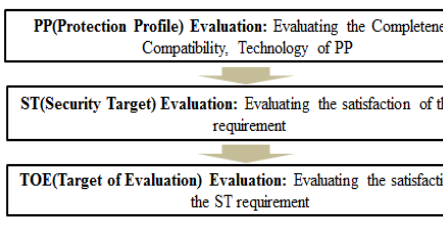
이 논문은 다음과 같은 구성을 갖고 있다. 제 1장에서는 연구의 배경과 연구의 목적에 대해 소개한다. 제 2장은 CC인증의 평가 프로세스와 보안제품의 3가지 원칙인 기밀성, 무결성, 가용성을 어떻게 제품에 반영시키는지에 관한 내용이다[10]. 제 3장은 연구모형 및 가설을 다룬다. 제 4장에서는 설문 결과를 통한 모형 검증을 실시한다. 마지막으로 제 5장에서는 본 연구의 결론과 함께 향후 연구 방향에 대해 언급한다.

2. CC 평가 방법론

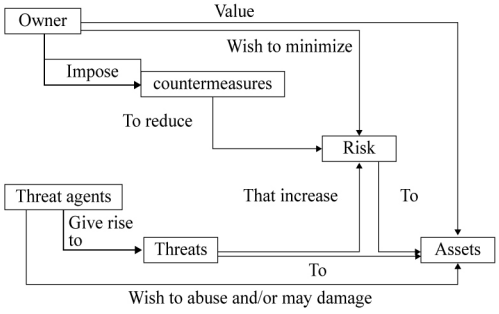
2.1 CC인증 평가 구조

IT 정보보호 솔루션의 원칙은 조직이 가지고 있는 자산을 보호하고 자산에 대한 위험을 최소화하는 것이다. CC인증 평가는 IT 정보보호 솔루션을 평가하는 엄격한 기준을 가지고 있다. CC인증 평가의 프로세스는 평가 스킴, 보안기능요구사항 그리고 평가 방법론이다. 다음 <Figure1>은 CC 평가의 일반적인 프로세스이다.

<Figure 1>에서 보는 것처럼 CC인증의 평가 준비를 위해서는 보호 프로파일(PP : Protection Profile)을 평가한 후, 보안목표명세서(ST : Security Target)을 평가하고 이후 평가의 대상인 TOE(Target Of Evaluation)을 평가하는 순서를 가진다[9]. 해당 평가 제품에 알맞은 보호 프로파일이 없는 경우, 개발 벤더는 자신의 제품에 맞는 보호 프로파일을 새로 구성하거나 보안목표명세서에서 평가 프로세스를 시작한다. 이제 정보보안 제품에서 사용되는 자산 등의 개념간의 상호관계에 대해 자세히 알아보기로 한다. <Figure 2>는 보안 내의 여러 가지 개념들의 상호관계를 도식화한 것이다.

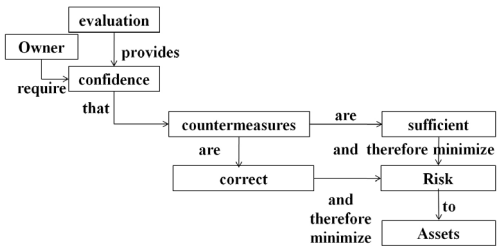


〈Figure 1〉 Common Criteria Evaluation Process



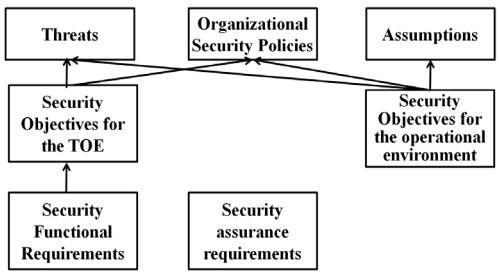
〈Figure 2〉 Security Concepts and Relationships

<Figure 2>에서 보는 것처럼 자산 소유자는 위험을 최소화하기를 원하고 자산에 가치를 부여한다. 자산은 평가대상이 되는 TOE (Target of Evaluation)가 우선적으로 보호해야 하는 대상이다. 위협원은 자산을 남용하고 나 손상시키고자 하기 때문에 자산을 위협하고 위험을 증대시킨다. 따라서 자산 소유자는 보안대책에 위험을 줄여줄 것을 기대한다. CC인증 평가의 보안 개념에 의해 평가개념과 요소 간의 상호관계는 다음 <Figure 3>과 같이 표현될 수 있다.



〈Figure 3〉 Evaluation Concepts and Relationships

<Figure 3>에서 보는 것처럼 자산 소유자는 보안대책이 충분하다고 믿을 수 있는 신뢰를 요구한다. 따라서 CC 평가에서 그 신뢰를 제공한다. 올바른 보안대책은 자산에 대한 위험을 최소화할 수 있다. 이제 자산의 보호를 위해 다음과 같은 사항을 알아보아야 한다. <Figure 4>는 보안문제를 정의하고, 보안 목적과 보안요구사항 간의 상호관계를 도식화한 그림이다.



〈Figure 4〉 Relations between the Security Problem Definition, Security Objectives and Security Requirements

<Figure 4>는 보안기능 요구사항이 TOE 보안 목적 및 조직의 보안 정책 등에 미치는 영향에 대해 그린 것이다. 보안 기능 요구사항을 구현할 때 TOE가 충분히 그 자산을 보호할 수 있는가에 초점을 맞춘다[11].

위의 <Figure 2>~<Figure 4>에서 보는 것처럼, CC인증 평가는 평가의 상부-하부 구조를 정확히 요구하는 매우 논리적인 구조를 가지고 있다.

2.2 보안목표명세서에서 구현까지의 단계

CC인증 평가는 개발 벤더 입장에서 많은 시간과 비용의 발생을 의미한다. CC인증의 구조가 소프트웨어 공학의 폭포수 모델(Waterfall Model)을 따르고 있기 때문에 한 단계가 잘못될 경우, 그 이후의 모든 단계의 내용이 수정되어야 한다[4].

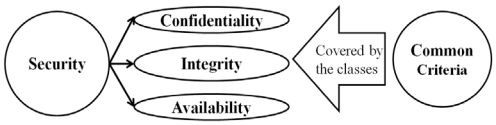
먼저 보안문제가 정의된다. 보안목적은 정의된 보안문제를 바탕으로 결정된다. 많은 보안문제가 정의될 경우, 각각의 보안문제에 대한 보안 목적이 정의되어야 한다. 보안기능은 보안 목적을 바탕으로 만들어진다. TOE 요약 명세는 보안기능이 가져야 할 조건과 보안성 및 기본 보안기능을 바탕으로 작성할 수 있다. 정책 모델은 보안 요구사항과 기능 명세에 동시에 영향을 끼친다. 위의 그림에서는 구현 명세가 하나로 표현되지만 정보보호시스템 공통평가방법론(CCMB) V 2.0을 따를 경우에는 이를 두 가지로 나누어서 서브시스템 별로, 그리고 구현 명세 정의 별로 나누어 기술할 수도 있다. 마지막으로 평가 대상이 되는 TOE가 명세서에 따라 구현된다. 어떤 단계에서라도 문제가 있다고 지적될 경우, 문제가 되는 단계부터 다시 문서화가 요구되기 때문에 처음에 보안 문제와 보안 목적을 정의하는 것이 CC인증에서 중요한 요소라고 할 수 있다[2].

2.3 기밀성, 무결성, 가용성의 반영

새로운 정보보호 솔루션을 기획할 때 앞서 언급한 보안의 기본 기능인 기밀성, 무결성, 가용성이 반드시 고려되어야 한다. 기밀성은 자산 소유자가 원하는 정보의 비밀이 유지되는 것을 의미한다. 각종 인증 데이터는 반드시 허가된 사용자만 접근할 수 있어야 하고 이를 위해 인증 데이터의 기밀성 유지가 중요하다. 최근 기밀성 구현의 대표적인 방법으로 비밀번호의 일방향 해쉬, SSL이나 SSH, 혹은 VPN 등을 통한 전송 데이터의 암호화 등이 구체적인 기능요구사항으로 요구되고 있다. 네트워크 구간에서의 기밀성 유지를 위해 접근제어나 데이터 암호화 등을 어떤 알고리즘으로 구현하는지도 평가에서 반영된다. CC인증에서는 사용자 데이터보호 클래스와 암호화 지원 클래스 등이 기밀성에 관련한 기능요구사항을 제공한다[6].

무결성은 허가되지 않은 접근에 의해 데이터가 위/변조되거나, 삭제, 혹은 무단으로 생성되는 경우를 방지하는 것이다. 무결성을 확인하기 위해 전송되는 데이터와 그것을 받는 데이터간의 상호비교가 필수적이다. 이것은 접근제어 및 데이터 보호에 의해 구현될 수 있다. 식별 및 인증 클래스는 이 보안기능을 제공한다[6].

가용성은 그 시간에 적절한 방법을 사용하여 허가된 사용자에게 적절한 데이터를 제공하는 것이다. 데이터를 저장하고 있는 솔루션이 공격을 받거나 요구되는 데이터를 제공하지 못하는 경우는 가용성이 손상되었음을 의미한다. 위협으로부터 가용성을 확보하기 위해 데이터를 백업하거나 시스템을 이중화하는 경우가 가용성을 확보하는 한 방법이다. 보안관리 클래스는 이 보안기능을 제공한다[6].



〈Figure 5〉 Relations between the Security Principle and the Common Criteria

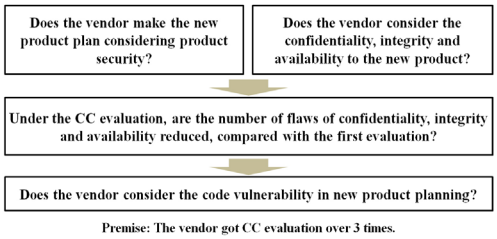
<Figure 5>에서와 같이 모든 클래스들은 기본적인 보안원칙인 기밀성, 무결성, 가용성을 위해 존재한다. 보안기능 요구사항은 구현 부분에 서로 섞여있기 때문에 클래스들과 컴포넌트들은 상호 종속관계로 묶이게 된다[1, 3, 5].

CC인증에서는 3가지 필수적인 보안 원칙을 지미고 구현하는가를 확인한다. 이를 위해 종속변수까지 모두 기능에 반영이 되어 있는지를 확인한다[2].

3. 연구 모형

3.1 연구모형 및 가설

<Figure 6>은 본 연구에서의 연구 모형 및 설문을 위한 가설을 보여준다.



〈Figure 6〉 Concept Flowchart in Questionnaire

<Figure 6>에서 보는 것처럼 가장 중요한 것은 문제를 정의하는 것이다. 문제는 CC인증 평가 방법론에 의해 정보보호 솔루션 자체의 보안성이 강화되었을까 이다. 일 문제에 대한 간단한 실마리는 앞선 <Figure 2>와 <Figure 3>에서 찾을 수 있다. 이들 그림은 CC인증에서의 기본적인 보안 개념과 상호관계의 구조를 보여주었다. TOE의 보안성에 대한 평가는 평가 기술보고서(ETR : Evaluation Technical Report)로 작성된다. 이 보고서에서 평가 인력은 솔루션 자체가 갖는 취약성을 중심으로 보고서를 작성한다.

보안문제가 정의되고 보안성이 어떻게 강화되었는지를 취약성을 중심으로 정의한 후, 다음 단계로 3가지의 필수사항인 기밀성, 무결성, 가용성이 제대로 반영되어 있는지를 정의한다[8]. 세 번째는 보안성 강화의 실증조사방법을 어떻게 결정할 것인가에 관한 것이다[13].

우선 설문지를 작성한다. 또한 누구를 대상으로 할지에 대해 결정한다. 설문지에 대한 답변을 받은 후 결과를 분석하여 가설의 채택여부를 결정한다.

3.2 설문 조사

모든 개발 벤더와 CC인증을 평가하는 인력들은 CC인증이 솔루션 자체의 보안성을 강화한다고 믿는다. 이를 어떻게 실증조사를 통해 증명할 수 있을까? 설문지를 통한 CC인증의 보안성 강화 측정에 대해 알아보기로 한다.

2012년 현재 국내에서 CC인증을 받은 개발 벤더는 102개로 파악되고 있다. CC인증을 받은 정보보호 솔루션의 개수는 300여개이다. 이들 중 23개의 개발 벤더들은 CC인증을 3회 이상 받았다[14]. 본 연구에서 설문조사는 CC인증을 3회 이상 받은 개발벤더들을 대상으로 실시하였다.

CC인증의 경험이 회사의 솔루션에 반영되기 위해서 3회를 기준으로 하였다. 4회 이상의 벤더는 10개 이하로 줄어들기 때문에 표본 집단으로서의 의미가 없다고 판단되었기 때문이다. 23개의 개발 벤더에게 설문지를 보냈고, 15개의 벤더로부터 답변이 도착했다.

우선 설문지 조사에 관해 언급한다. 대상 집단은 15개 개발 벤더이다. 이들 각각은 자사의 두 가지의 솔루션을 설문지 답변의 대상으로 삼았기 때문에 총 대상 솔루션은 30개이다.

본 연구에서는 솔루션을 중신으로 각 집단을 'a'집단과 'b'집단으로 나누었다. 두 집단의 구분은 설문지에서 *.1은 'a'집단, *.2는 'b'집단이 된다. 1과 2의 숫자에 없는 질문은 15개 벤더들이 공통적으로 대답한 것이다. 설문지에는 총 7개의 주요 문항으로 구성되었다. 각 질문은 단답형, 혹은 5점 척도로 답하도록 구성되었다. 다음 <Table 1>은 설문지 내용이다.

<Table 1>의 설문지는 필수보안기능 요구사항을 제품 기획 이전에 고려했는지 하지 않았는지에 초점을 맞추어 작성하였다. 설문지에는 5점 척도를 사용하였다.

〈Table 1〉 Questionnaire for Study of Common Criteria Influence on Solutions

No.	Content
Q1	How many times did you get the Common Criteria evaluation in this company?
Q2.1	How many number of vulnerability were pointed out at first Common Criteria Evaluation?
Q2.2	How many number of vulnerability were pointed out at 3th Common Criteria Evaluation?
Q3	Which tool was used for the vulnerability analysis?
Q4.1	Was the vulnerability of code considered in implementing the security solution at first Common Criteria Evaluation?
Q4.2	Was the vulnerability of code considered in implementing the security solution at 3th Common Criteria Evaluation?
Q5.1	Was the confidentiality considered in implementing the security solution at first Common Criteria Evaluation?
Q5.2	Was the confidentiality considered in implementing the security solution at 3th Common Criteria Evaluation?
Q6.1	Was the integrity considered in implementing the security solution at first Common Criteria Evaluation?
Q6.2	Was the integrity considered in implementing the security solution at 3th Common Criteria Evaluation?
Q7.1	Was the integrity considered in implementing the security solution at first Common Criteria Evaluation?
Q7.2	Was the availability considered in implementing the security solution at 3th Common Criteria Evaluation?

4. 가설 검증

모든 가설 기각역을 0.05수준으로 정했고, 등 분산을 가정하였다. P-Value는 양측 검정을 채택했다. 모든 계산 결과값은 소수점 2자리까지만 표시하고 반올림하였다.

질문 1번은 답변자가 CC인증에 대한 적절한 이해도를 가지고 있다는 가정사항 충족을 위한 간단한 질문이다. 질문 1번에 대한 답변 결과는 다음과 같다.

〈Table 2〉 Result of Q1

Common Criteria Times	The number of Vendos
3	8
Over 4	7

15개의 개발 벤더 중에서 8개의 벤더는 CC인증을 3회 받은 경험이 있고, 7개의 벤더는 CC인증을 4회 이상 받은 것으로 나타났다. 이것은 대상 벤더들이 모두 CC인증의 보안성에 대해 잘 파악하고 있음을 나타내는 지표라 할 수 있다.

질문 3번은 국내의 정보보호 솔루션이 사용하는 취약성 툴이 어떤 것들이 있는지 알아보기 위함이다. 다음 <Table 3>는 질문에 대한 답변이다.

〈Table 3〉 Result of Q3

Vulnerability Analysis Tool	The number of Answer
RATs	15
WireShark	6
Nessus	6

15개 모든 개발 벤더는 코드 취약성 점검을 위해 RATs를 사용하고 있었다. RATs는 CC인증 평가기관들이 주로 사용하는 코드 취약성 점검 툴이다. WireShark나 Nessus는 제품의 특성에 따라 일부 벤더들이 사용하고 있다.

질문 2번, 4번, 5번, 6번, 7번은 'a'집단과 'b' 집단의 비교를 위해 작성되었다. <Table 4>는 2번 질문에 대한 답변 결과이다.

〈Table 4〉 Result of Q 2, 4, 5, 6 and 7

The number of Flaws	1~5	6~10	Over 10
2.1 (a)	5	7	3
2.2 (b)	9	4	1
Scale	**1~2**	**3**	**4~5**
4.1 (a)	4	1	10
4.2 (b)	0	1	14
5.1 (a)	2	1	12
5.2 (b)	0	0	15
6.1 (a)	3	1	11
6.2 (b)	0	0	15
7.1 (a)	3	0	11
7.2 (b)	0	0	15

<Table 4>의 설문지 답변결과를 바탕으로 다음과 같이 각각의 질문에 대해 가설을 세울 수 있다.

질문 2번의 경우, CC인증의 경험 이전에는 취약성에 대한 고려가 적고 CC인증 이후, 신제품 기획 시 취약성에 대한 고려 정도가 강해질 것으로 가정하는 의도로 만들어졌다. 따라서 다음과 같은 가설을 세울 수 있다.

H2 : CC인증 경험을 한 후, 개발사는 CC 인증 평가 시 취약성 지적을 덜 받는다.

질문 4번의 경우는 평가 기관으로부터 취약성을 지적 받은 횟수를 보고 벤더가 취약성에 대한 고려를 이미 했는지를 알아보기 위함이다. 즉, 질문 2번과 질문 3번에 이어 질문 4번의 답변의 일관성 유지를 위해 작성되었다. 취약성지적 개수와 비교하여 CC인증 경험 후, 코드 취약성을 고려하여 제품이 개발되고 있다는 것으로 다음과 같이 가설을 세울 수 있다.

H4 : CC인증 경험을 한 후, 개발사는 신제품 기획 시 코드 취약성 등을 고려한다.

질문 5번의 경우, 질문 CC인증 경험 후, 신제품 기획 시 기밀성을 고려하여 제품이 개발하고 있다는 것으로 다음과 같이 가설을 세울 수 있다.

H5 : CC인증 경험을 한 후, 개발사는 신제품 기획 시 기밀성을 고려한다.

질문 6번의 경우, 질문 CC인증 경험 후, 신제품 기획 시 무결성을 고려하여 제품이 개발하고 있다는 것으로 다음과 같이 가설을 세울 수 있다.

H6 : CC인증 경험을 한 후, 개발사는 신제품 기획 시 무결성을 고려한다.

질문 7번의 경우, 질문 CC인증 경험 후, 신제품 기획 시 가용성을 고려하여 제품이 개발하고 있다는 것으로 다음과 같이 가설을 세울 수 있다.

H7 : CC인증 경험을 한 후, 개발사는 신제품 기획 시 가용성을 고려한다.

위의 가설에 대한 검증을 위해 설문 조사의 답변을 분석한 통계치는 다음 <Table 5>과 같다.

모든 가설 평균차는 0이다. 자유도는 모두 27의 값을 갖는다. 2번 가설의 기각 여부를 판단하기 위해 통계 결과를 보면 P-Value는 0.75 > 0.05이기 때문에 2번 가설(H2)을 채택한다. 4번 P-Value는 0.21 > 0.05이기 때문에 4번 가설(H4)을 채택한다. 5번의 0.22 > 0.05이기 때문에 5번 가설(H5)을 채택한다. 6번의 P-Value는 0.21 > 0.05이기 때문에 6번 가설(H6)을 채택한다. 7번의 P-Value는 0.22 > 0.05이기 때문에 7번 가설(H7)을 채택한다. 4번, 5번, 6번의 분산을 보면 'b'집단의 분산 값이 매우 큰 것을 알 수 있다. 이는 CC인증 이전에는 기밀성, 무결성, 가용성에 대한 고려가 적었으나, CC인증을 경험한 후, 제품을 기획할 때는 개발 벤더 모두가 이 세 가지 보안 원칙을 준수하기 때문이다.

〈Table 5〉 Result of Statistic Analysis

Group	2.1(a)	2.2(b)
Mean	15.86	12.71
Variance	642.44	647.14
Mean Difference	0	
Degree of Freedom	27	
P(T<=t) Two-Tailed test	0.75	
t-test Two-Tailed test	2.06	
Group	4.1(a)	4.2(b)
Mean	4.33	12.71
Variance	0.24	647.14
Mean Difference	0	
Degree of Freedom	27	
P(T<=t) Two-Tailed test	0.21	
t-test Two-Tailed test	2.051	
Group	5.1(a)	5.2(b)
Mean	4.53	12.71
Variance	0.267	647.14
Degree of Freedom	27	
P(T<=t) Two-Tailed test	0.22	
t-test Two-Tailed test	2.052	
Group	6.1(a)	6.2(b)
Mean	4.33	12.7
Variance	0.38	647.14
Degree of Freedom	27	
P(T<=t) Two-Tailed test	0.21	
t-test Two-Tailed test	2.05	
Group	7.1(a)	7.2(b)
Mean	4.2	12.71429
Variance	0.46	647.14
Degree of Freedom	27	
P(T<=t) Two-Tailed test	0.21	
t-test Two-Tailed test	2.05	

설문지 분석한 결과, CC인증을 해본 경험이 있는 회사들은 이후 CC인증이 보안성 강화의 중요한 요소임을 인정한다고 해석할 수 있다. 본 연구의 설문 조사 결과에 의하면 개발 벤더에 근무하는 CC인증 담당자들은 CC인증 프로세스가 사내에 확립된 이후에는 제품 기획 등에 CC인증의 기본원칙을 반영시키고 있음을 알 수 있다.

5. 결 론

기업이 획득하는 대부분의 인증은 제품의 품질 향상이나, 기업 비즈니스 프로세스의 향상을 목적으로 획득하게 된다. CC인증은 국제적으로 표준화된 인증 기준으로서 국내에 도입된 이래 10여년이 넘는 기간 동안 정보보호 분야의 개발 벤더들에게 기준의 준수를 의무화함으로써 개발 프로세스와 기능 안정화를 추구하는 데 공헌해 왔다.

본 연구는 CC인증이 도입된 10년 넘는 기간 동안 막연히 CC인증이 개발 보안 프로세스를 향상시키는 효과가 있을 거라는 믿음을 실증조사를 통해 보여 줌으로써 인증이 제품이 미치는 긍정적 효과에 대해 입증했다는 점에서 의의를 가진다.

그러나 CC인증에 대한 개발 벤더의 태도에는 아직 많은 문제점들이 존재한다. 첫째, 변화 관리의 문제이다. 재인증이나 변경 승인 등의 기준이 모호하고 인증 비용이 높기 때문에 개발 벤더는 동일 제품에 대한 변화 관리로서의 재인증 획득을 꺼려한다. 둘째로는 아직까지 만연한 국내의 역공학(Reverse)인증 프로세스를 지적할 수 있다. 많은 개발 벤더들이 CC인증에서 규정하는 기본 기능과 프로세스를 무시한 상태에서 제품을 개발한 후, CC인증을 받기 위해 대상 제품을 계속 수정하는 등 시간 비용의 문제가 발생하고 있다. 이런 현상은 아직 국내에 소프트웨어 공학의 개발 프로세스가 정립되지 않은 채, 주먹구구식의 개발 습관이 만연해 있음을 의미한다.

CC인증이 진정한 국제 표준인증으로 국내에서 자리잡고 그 기능을 다하기 위해서는 인증의 긍정적 효과의 홍보와 함께 인증 평가 기준을 강화함으로써 정기적인 변화 관리 등의 방법을 추구할 필요가 있다. 향후 연구에서는 CC인증 보안성 강화 효과 측정을 위해 본 논문에서 사용한 보안 3대 요소인 기밀성, 무결성, 가용성 이외에 사용자 인증과 전자 서명을 추가적인 변수로 사용할 계획이다. 또한 국내 CC인증 평가 프로세스와 국제 CC인증 평가 프로세스를 비교하고, 해외 사례의 비교 분석을 통해 좀 더 심도 있는 연구를 하고자 한다.

References

[1] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, CCRA management committee, 2000.

[2] Chapman, R., “A state of the practice approach to the Common Criteria implementation requirements,” 2nd International Common Criteria Conference, 2001.

[3] Common Criteria, CCMB, 2007.

[4] Common Criteria Portal site, http://www.commoncriteriaportal.org.

[5] Common Methodology for Information Technology Security Evaluation, CCMB, 2007.

[6] Fedeke, A., “Common Criteria for the assessment of critical infrastructure,” International Journal of Disaster Risk Science, Vol. 2, No. 1, pp. 15-24, 2011.

[7] Mellado, D., Fernández-Medina, E., and Piattini, M., “A common criteria based security requirements engineering process for the development of secure information systems,” Computer Standards and Interfaces, Vol. 29, No. 2, pp. 244-253, 2007.

[8] Merkow, M. S. and Breithaupt, J., “Computer security assurance using the common criteria,” Thomson, 2004.

[9] Nguyen, T. D., Levin, T. E., and Irvine, C. E., “High robustness requirements in a Common Criteria protection profile Infor-

mation Assurance," Information Assurance Workshop, pp. 10-78, 2006.

[10] Seo, Y. J. and Han, S. Y., "An Information Flow Security Based on Protected Area in eCommerce," Journal of Society for e-Business Studies, Vol. 15, No. 1, pp. 1-16, 2010.

[11] Singh, M. and Patterh, M. S., "Formal Specification of Common Criteria Based Access Control Policy Model," International Journal of Network Security, Vol. 11, No. 3, p. 112, 2010.

[12] Stoneburner, G., "Developer-focused assurance requirements [Evaluation Assurance Level and Common Criteria for IT system evaluation," IEEE Computer Society, Vol. 38, No. 7, pp. 91-93, 2005.

[13] Ware, M. S., Bowles, J. B., and Eastman, C. M., "Using the Common Criteria to Elicit Security Requirements with Use Cases," SoutheastCon, pp. 273-278, 2006.

[14] http://service2.nis.go.kr.

저 자 소 개

홍영란	(E-mail : yrhong@hotmail.com)
1994년	서울대학교 경영학과 (학사)
1996년	서울대학교 대학원 경영학과 (석사)
2010년	숭실대학교 산업정보시스템공학과 (박사과정)
관심분야	정보보호, DLP(Data Loss Prevention), Network and Endpoint Security

김동수	(E-mail : dskim@ssu.ac.kr)
1994년	서울대학교 산업공학과 (학사)
1996년	서울대학교 산업공학과 (석사)
2001년	서울대학교 산업공학과 (박사)
2001년~2003년	한국정보사회진흥원 전자거래연구부 e-Biz 표준팀장
2003년~2006년	가톨릭대학교 의료경영대학원 전임강사, 조교수
2006년~현재	숭실대학교 산업·정보시스템공학과 조교수, 부교수
관심분야	BPM, e-Business 정책 및 기술, 기업정보시스템, e-Health, 정보보호