신규 IT 서비스에 대한 정보보호 등급 인증 타당성 연구

A Study on Feasibility and Establishment of a Security Grade Certification Scheme for the New IT Services

장항배*, 조태희**, 김효진**

Chang Hang Bae*, Joe Tae Hee** and Kim Hyo Jin**

요 약

본 연구에서는 향후 전개될 신규 IT 서비스에 대하여 정보보호 요구사항 분석 및 정보보호 수준을 측정하기 위하여 신규 IT 서비스의 정보보호등급인증제를 설계하였다. 이를 위하여 본 연구에서 국내외 등급인증 제도를 분석하고 일반적인 정보시스템 정보보호 평가와는 차별되는 IT 서비스 자체의 특성을 반영한 평가모형을 개발하고 실제적인 추진체계를 개발하였다. 본 연구의 결과는 국내 IT 서비스의 정보보호 수준을 객관적으로 평가하는 데 활용될 수 있으며, 국내 IT 서비스 제공기업들의 정보보호 수준제고를 위한 정책수립의 합리적인 의사결정 도구로 응용될 수 있다.

Abstract

In this study we analyzed and gauged the information security needs for the new IT service which will be proceeding. Then we designed Information Security Rank Authentication System to raise the level of information security. To achieve this study, we analyzed rank authentication system of the inside and outside of the country and developed the practical propulsive system and the evaluation model which reflects IT service's own feature differing from the general evaluation of IS information security. The result of this study can be utilized to assess the level of domestic IT service information security objectively, and it can be applied as the means of rational decisionmaking for establishing a policy to raise degree of information security of corporations providing IT service.

Keyword: Security Grade Certification. New IT Service, Security Evaluation Model

I. 신규 IT 서비스와 정보보호

글로벌화 진전으로 국경 간 무한 경쟁이 심화되어 최고의 기술을 선점한 기업. 국가만이 생존(Winner Takes All)하는 냉엄한 현실에 대처하고 IT 산업의 글로벌 리더로 도약하기 위하여, 정부는 IT 산업의 경쟁력을 지속적으로 강화하여 세계 IT산업 발전을 선도하는 IT 정책을 개발하고 있다[2]. 그러나 이러한 IT 정책추진을 통하여 구현될 IT 서비스에 대해 간과해서는 안 될 부분은 정보화 혜택의 범위가 커짐에 따라 정보보호의 문제도 더 커진다는 점이다. 이미 인터넷의 급속한 보급으로 인한 개인정보 도용 및 유

* 대진대학교 경영학과
** 연세대학교 정보대학원
· 교신저자(Corresponding Author) : 장항배
· 투고일자 : 2008년 12월 30일
· 심사(수정)일자 : 2008년 12월 31일 (수정일자 : 2009년 1월 12일)
· 게재일자 : 2009년 2월 28일

출, 무단 스팸메일, 해킹과 같은 정보화의 역기능 현상의 피해범위와 수준도 예전에 비하여 급속도로 증가하고 있다. 새로 개발된 IT 서비스가 확산되기 위해서는 서비스 단계별 정보보호에 대한 치밀한 대책 수립과 서비스의 정보보호 수준에 대한 평가체계 수립이 필요하다[4].

따라서 본 연구에서는 새롭게 개발된 신규 IT 서비스에 대한 정보보호 등급인증제를 도입함에 따른 필요한 요구사항들을 도출하고, 이에 대한 해결방안들을 제시함으로써 현실적이고 실효성 있는 제도 개발을 진행하였다. 세부적으로 첫째, 정보보호 등급인증 제도화의 정당성을 제공하고 또한 제도화를 위한 기초자료를 제공해 주기 위한 목적으로 국내등급인증제도의 현황을 분석하였고 등급인증제의 결정방식과 성공요인을 분석하였다. 그 다음 신규 IT 서비스의 특성과 정보보호 현황을 분석하기 위하여 휴대 인터넷 서비스(WiBro)를 대상으로 서비스 특성과 정보보호 요구사항을 도출하였다. 마지막으로 앞서 정리된 현황분석을 기초로 신규 IT 서비스의 정보보호 등급인증을 위한 프레임워크와 함께 평가체계 및 모형을 개발하였다.

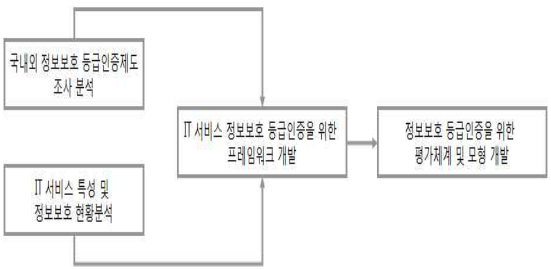

그림 1. 신규 IT 서비스에 대한 정보보호 등급인증 타당성 연구 방법론
Fig. 1 Research Methodology

II. 정보화 성숙도 모델 및 정보보호 인증 사례분석

2-1. 정보화 성숙도 모델

'Information Technology Architecture' 는 정보화의 효율적 추진을 위하여 조직 전체의 업무와 IT를 체계적이고 통합적으로 계획 관리하는 기반 체제로서 'Enterprise Architecture' 와 동일한 용어로 사용된다. 'Information Technology Architecture' 성숙도와 신규 IT 서비스의 정보보호 등급 평가의 유사점은 평가 목적이 투자 성과 및 Governance 획득이라는 점이다. 2개 평가체계 모두 IT 자체 또는 정보보호 측면만이 아닌 업무 측면의 목적 및 성과를 고려하고, IT 또는 정보보호체계의 업무 체계와의 연계(alignment)를 평가할 필요가 있다. 따라서 신규 IT 서비스의 정보보호 등급 평가 시, 업무 목적 및 성과를 파악하고 정보보호 체계의 업무 목적 지원 적절성을 평가할 필요가 있다. 이와 반면에 'Information Technology Architecture' 성숙도는 조직을 대상으로 하지만, 신규 IT 서비스의 정보보호 등급 평가는 서비스를 대상으로 한다. 서비스의 범위는 조직 전체를 포괄하지 않지만 서비스 제공 및 지원을 위한 외부 조직 또는 자원과 연계될 수 있다는 점에서 조직 범위와 차이가 있다. 따라서 신규 IT 서비스의 정보보호 등급 평가는 내부뿐 아니라 외부 조직 또는 자원과의 관계도 고려되어야 한다.

'Capability Maturity Model Integration' 는 미국 카네기멜론 대학의 소프트웨어공학연구소에서 개발한 소프트웨어 품질 측정 모델로 기존의 'Software SW-Capability Maturity Model Integration'을 개선한 것이다. 'Capability Maturity Model Integration' 성숙도 모델과 신규 IT 서비스의 정보보호 등급 평가를 비교하면, 이 평가 목적, 범위 및 대상은 상이하나 'Capability Maturity Model Integration' 평가단계 및 방법은 개선 영역 및 방향을 제시한다는 점에서 신규 IT 서비스의 정보보호 등급평가에 적용할 필요가 있다[11]

'IT Infrastructure Library'는 IT 서비스관리 프레임워크 구현을 위한 문서들의 집합으로, 특정 기업 내의 복잡한 IT 환경에 대해 업무와 서비스 중심의 프레임워크를 제시한다. 'IT Infrastructure Library' 성숙도 평가와 신규 IT 서비스의 정보보호 등급평가를 비교하면, 평가목적 및 평가 대상은 공통점이 있으며, 평가범위는 차이점이 있는 것으로 나타났다. 평가목적 및 대상에 있어 평가목적이 조직의 Governance 향상을 지향한다는 점, 평가 대상이 서비스 능력을 평가하는 점이 공통적이라 할 수 있다. 그러나 'IT

Infrastructure Library'가 프로세스 및 기능만을 평가하는 반면, 신규 IT 서비스의 정보보호 등급평가는 서비스 아키텍처를 포함한다는 점이 상이하다고 할 수 있다[3], [9].

2-2. 정보보호 인증 사례분석

'Systems Security Engineering-Capability Maturity Model'은 프로세스 개선을 통하여 비용 절감과 프로세스 수행 능력의 향상을 하고자 하는 프로세스 개선 모델이다. 이 방법은 위험 프로세스, 보증 프로세스 및 공학 프로세스의 순환적 활동으로 정보보호 관리 프로세스를 정의하고 있다. 위험 프로세스를 통해 정보보호의 위험을 도출하고, 공학 프로세스를 통해 위험을 해결하고, 보증 프로세스를 통해 문제의 해결을 확인하는 일련의 순환적 활동으로 구성된다. 'Systems Security Engineering-Capability Maturity Model' 인증 및 인정과정은 그림 2와 같이 소프트웨어개발의 생명주기를 따라 평가 계획, 평가준비, 현장평가 및 보고 단계로 구성되어 있다[10].

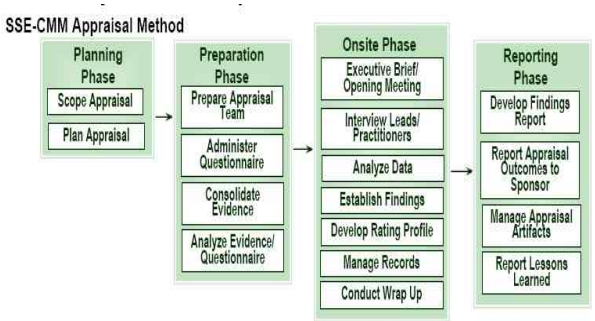

그림 2. 'Systems Security Engineering-Capability Maturity Model' 평가과정
Fig. 2 Systems Security Engineering-Capability Maturity Model

미국연방 정보보호 관리법인 'Federal Information Security Management Act' 는 정부기관으로 하여금 정보와 정보시스템 보호를 위해 전사적 정보보호 프로그램을 개발, 문서화, 구현하도록 요구하고 있다. 정보보호 통제의 효과성과 충분성을 보장하기 위하여 'Federal Information Security Management Act'는 기관의 정보화 및 와 정보보호 책임자로 하여금 정보보호 프로그램을 매년 검토하여 그 결과를 보고하도록 요구하고 있다[7],[8].

III. 신규 IT 서비스 특성 및 정보보호 현황분석

3-1. 휴대 인터넷 서비스 개요

휴대 인터넷 서비스(WiBro, Wireless Broadband Internet)'는 이동전화처럼 언제 어디서나 이동하면서도 초고속으로 인터넷을 이용할 수 있는 서비스로서 이동전화와 무선 랜의 중간 영역에 위치한다. 본 서비스의 특징은 정지 및 보행뿐만 아니라 시속 60Km 정도의 중저속 이동성 및 1Mbps 이상의 데이터 전송률을 지원하는 것인데, 휴대인터넷의 이동성은 서비스 자체가 도심지 위주의 서비스로 개발되었기 때문이며 지하철, 버스 등의 대중교통과, 도심지에서 승용차의 속도제한이 대부분 60Km/h 내외인 것을 감안한다면 그리 문제는 없으나 고속도로나 열차를 이용할 경우 문제가 발생한다[5].

휴대 인터넷의 상용 서비스를 안전하게 제공하기 위해서는 여러 가지 기술적 문제점이 해결되어야 한다. 그중 가장 중요한 기술 요소가 바로 보안이며, 안전한 서비스를 제공하기 위해 서비스 및 시스템 관점에서 다음과 같이 보안요구사항을 정리할 수 있다.

(1) 인증 및 보안 서비스 요구사항: 휴대 인터넷은 적법한 사용자 및 장치 이외 제3자의 불법적인 사용과 불법적인 액세스 네트워크의 서비스 제공을 금지하기 위한 인증 서비스와 사용자의 송수신 정보가 통신 당사자 이외의 제3자에게 노출되는 것을 예방할 수 있는 보안 서비스를 제공해야 한다.

(2) 네트워크 보안 요구사항: 접속 제어 기능으로 인증 기능을 제공해야하며, Extensible Authentication Protocol 기반의 인증 및 보안 프로토콜이 지원 가능하며, 필요시 공개키 기반으로 확장 가능해야 한다. 타 망과의 연동에 따른 타망 서비스 인증을 지원할 수 있어야 하며, 모바일 IP 등을 이용해 IP 이동성을 보장해야 한다.

(3) 단말 보안 요구사항: Extensible Authentication Protocol 기반의 인증 및 보안 프로토콜이 지원 가능하며, 필요시 공개키 기반으로 확장 가능해야 한다.

Ⅳ. 신규 IT 서비스 정보보호 평가 프레임워크

4-1. 신규 IT 서비스 특성

본 연구에서 정의하는 IT 서비스는 정보통신 사업자의 비즈니스 그 자체로서 일반 고객을 대상으로 IT 서비스를 제공함으로써 이익이나 가치를 추구하는 면에서 일반적인 IT 서비스와 차별할 필요가 있다. 즉 본 연구의 대상인 신규 IT 서비스는 IT 서비스 제공업자가 조직 외부의 고객을 대상으로 여러 다른 IT 서비스 공급업자와의 협력관계를 바탕으로 수익을 목적으로 제공하는 서비스라고 정의할 수 있다.

따라서 신규 IT 서비스의 정보보호 아키텍처는 이러한 IT 서비스의 개념도에 기초하여 해당 아키텍처 요소에서의 정보보호 요구사항을 도출하고 반영해야 할 필요가 있다.

4-2. 신규 IT 서비스에 대한 정보보호 아키텍처

신규 IT 서비스의 정보보호 아키텍처는 신규 IT 서비스의 특성을 반영하여 IT 서비스 제공을 위한 모든 구성요소에서의 정보보호 요구사항을 반영하여야 한다. 본 연구에서는 IT 아키텍처를 수립하는데 자주 사용되는 '인적 자원(People), 프로세스(Process), 기술(Technology)' 모델을 사용하여 표 1.과 같이 신규 IT 서비스에 대한 정보보호 아키텍처를 수립하였다[6].

표 1. 신규 IT 서비스에 대한 정보보호 아키텍처
Table 1. Security Architecture for New IT Service

	프로세스(Process)		인적 자원(People)		기술(Technology)		
	비즈니스 프로세스	IT 서비스 프로세스	서비스 제공자, 공급자	고객	기반구조	응용	단말기
IT 서비스 공통 정보보호 요구사항 (Generic)							
IT 서비스 개별 정보보호 요구사항 (Specific)							

4-3. 신규 IT 서비스 정보보호 평가제도 개발을 위한 프레임워크

신규 IT 서비스 정보보호 평가 제도를 개발하기 위해 우선적으로 평가제도로서 갖추어야 할 기본적인 요소들을 파악하기 위한 개념적 틀로서 프레임워크를 개발하였다. 평가제도의 기본적인 요소들은 6하 원칙(5W 1H)에 의해 파악될 수 있다.

우선 'Why' 측면은 평가제도의 근거와 평가목적으로 구체화되며, 'Who' 측면은 평가추진체계를 의미하는 것으로, 평가의 기획, 수행, 감독, 운영에 필요한 주체가 누가 되어야 하는 가를 결정하는 것으로 각 해당 주체의 위상과 능력에 대한 결정이 내려져야 한다. 'What' 측면은 평가대상을 의미하는 것으로, 평가대상 분야, 평가대상 선정기준 등이 결정되어야하며, 'When' 측면은 평가시기를 의미하는 것으로, 평가대상 사업 선정시점과 실제 평가시점 등이 결정되어야 한다. 'Where' 측면은 평가유형을 의미하는 것으로, 주로 문서 심사로 진행할 것인가 아니면 실사로 진행할 것인가 등이 결정되어야 한다. 마지막으로 'How' 측면은 평가수행방법을 의미하는 것으로, 평가절차, 기준, 및 기법 등이 결정되어야 한다.

Ⅴ. 신규 IT 서비스 정보보호 등급인증 평가 모형

5-1. 평가모형 설계 원칙 및 방법

일반적으로 정보보호 수준을 종합적이고 객관적으로 평가하는 것은 매우 복잡하고 어려우며 다양한 변수들의 상황적 적용에 따라 표준화가 쉽지 않고 평가모형이 개발되었다 하더라도 그 활용성에 있어 의문을 가지지 않을 수 없다. 따라서 본 연구에서는 보다 간단하고 효과적인 방법으로 IT 서비스의 정보보호 수준을 종합적이고 객관적으로 평가할 수 있는 모형 개발을 목적으로 한다. 본 연구의 목적을 달성하기 위하여 다음과 같이 연구를 진행하였다. 먼저 IT 서비스의 정보보호등급인증 평가모형을 설계하기 위한 요구사항을 정리하여 이를 만족 시키는 평가모형의 개념적 체계를 설계한다. 다음 단계로 개념적으로 설계된 모형에 대하여 실제 평가모형 개발 요구사항을 만족시키는 평가모형의 구성요소를 문헌적 방법과 전문가 의견을 통하여 구성을 완료한다.

IT 서비스 정보보호 평가모형을 설계하기 위한 전반적인 평가모형 설계원칙은 크게 3가지로 정리하였다. 먼저 정보시스템 정보보호 평가와는 차별되는 IT 서비스 자체의 특성을 반영하고자 하였으며, 서비스의 목적에 따라 달리 표현 되는 '개별' IT 서비스의 특성 또한 평가모형에 고려하였다. 마지막으로 서비스 제공기업들의 정보보호 추진 방향성을 제시하기 위하여 지속적인 정보보호 개선활동이 이루어 질 수 있도록 설계하고자 하였다. 이러한 설계원칙은 실제 평가모형을 개발하는 과정에서 IT 서비스의 특성은 평가항목을 앞서 설계한 신규 IT 서비스 정보보호 아키텍처에 근거하여 적용하였고, 일반 정보시스템과는 달리 IT 서비스를 사용하는 최종 종착지는 서비스 사용자이기 때문에 사용자의 정보보호 평가항목을 평가모형에 반영하고자 하였다. 개별 IT 서비스의 특성을 반영하기 위해서 각각의 IT 서비스가 정의하는 정보보호 요구사항 및 정도가 평가항목에 적용될 수 있도록 노력하였으며, 이는 세부 평가항목, 가중치, 측정방법 등에 변화를 주어 조정하였다. 마지막으로 지속적인 정보보호 개선활동이 가능하도록 하기 위하여 세부 평가항목에 대한 측정방법은 정보보호 성숙모형을 기초로 하고 이를 평가하고자 하였다.

5-2. 평가모형 설계

일반적으로 평가모형은 평가영역, 평가항목, 세부평가항목, 측정방법, 평가결과 등으로 구성된다. 본 연구에서는 앞서 설명한 전반적인 평가모형 설계원칙과 함께 각 항목을 구성하는 세부 구성요소에 대한 설계원칙을 설정하여 모형을 구성하였다.

(1) 평가영역

본 연구에서는 IT 서비스 본연의 업무를 방해하지 않으면서(빠른 시간 내에 평가를 종료), IT 서비스의 정보보호를 위한 통제와 프로세스를 포함하면서 정보보호 아키텍처 관점에서 평가항목을 도출하고자 하였다.

(2) 평가항목

평가영역에 부속되는 평가항목 및 세부 평가항목은, 국내에서 현재 연구되고 시행되고 있는 정보보호 평가항목(정보보호 수준평가, 정보보호 안전진단, 개인 정보보호, 정보보호 제품 보안성 검토, 정보보호 관리체계 등) 을 조사하여 정리하였다. 특히 세부 평가항목에 있어서는 개별 IT 서비스에 대한 정보보호 요구사항을 반영하기 위하여 세부 평가항목의 변화, 가중치의 변화, 측정 방법의 변화를 주었다.

평가측정 방법은 정보보호 개선활동에 관한 방향성 제시를 목적으로 하고 있기 때문에, 세부 평가항목들의 목적에 따라 정보보호 성숙모형을 기초로 하여 설계하였다[9, 10, 11]. 마지막으로 평가결과는 각 평가영역, 평가항목, 세부 평가항목들을 산술 종합하여, 점수 구간별로 1~5단계까지 연결하였다. 평가결과에 있어 다른 정보보호 평가모형과는 달리 각 단계별 정의를 하지 않은 이유는 산술 종합 된 평가결과가 단계별 구간의 특성을 대표적으로 반영하기 어렵기 때문이다. 평가 결과를 구성하는 각 단계별 특성에 대해서는 향후 연구를 통하여 정리할 예정이다.

(3) 평가 내용

본 연구에서는 IT 서비스를 구성하는 정보화 자산식별과 정보화 구성요소들을 정리한 다음 이들을 보호하기 위한 정보보호 범위와 함께 정보보호 평가영역을 IT 서비스 정보보호 지원환경, IT 서비스 정보보호 기반구조, IT 서비스 정보보호 운영관리 등으로 정의하였다. 그리고 평가 영역에 부속되는 평가항목들을 앞서 정의한 신규 IT 서비스 정보보호 프레임워크에 따라 정리하였다.평가영역에 부속되는 평가항목 및 세부 평가항목은, 국내에서 현재 연구되고 시행되고 있는 정보보호 평가항목(정보보호 수준평가, 정보보호 안전진단, 개인 정보보호, 정보보호 제품 보안성 검토, 정보보호 관리체계 등) 을 조사하여 정리하였다. 특히 세부 평가항목에 있어서는 개별 IT 서비스에 대한 정보보호 요구사항을 반영하기 위하여 세부 평가항목의 변화, 가중치의 변화, 측정 방법의 변화를 주었다.

IT 서비스 정보보호 지원환경은 IT 서비스 특성에 맞춘 정보보호 목표 수립 및 목표 달성을 위하여 지켜져야 하는 지침 및 절차를 의미하는 정보보호 정책과 IT 서비스를 구성하는 이해 관계자(stakeholder)에 따라 IT 서비스 위험평가를 실시하는 IT 서비스 제공자 및 공급자 정보보호 활동, 실제 IT 운영을 담당하는 인력에 대한 정보보호, 그리고 최종적으로 IT 서비스를 사용하는 사용자에 대한 정보보호 범위와

구체적인 활동 등을 정의하는 IT 서비스 사용자 보호 등으로 구성하였다.

IT 서비스 정보보호 기반구조는 정보보호 대상을 실제로 도입하여 운영 및 관리하는 것을 의미하여, 네트워크 보안, 서버, 단말기, 응용 프로그램, 정보 서비스(contents) 등과 같은 정보자산에 대하여 인증, 무결성, 비밀성, 가용성 유지를 위한 정보보호 활동을 측정한다. IT 서비스 정보보호 운영관리는 정보보호 기반구조 구축단계에서 구현되는 보안 대책의 안전하고 효율적인 운영을 위해 요구되는 관리 방안을 의미하며, 위험관리, 사후관리, 모니터링 및 재평가 등으로 구성하였다.

표 2. 신규 IT 서비스 정보보호등급인증제 평가모형
Fig. 2 Security Evaluation Framework for New IT Service

평가 영역	평가 항목	세부 평가항목
IT 서비스 정보보호 지원환경	정보보호 정책수립	서비스 고유 특성에 기반 한 정보보호 요구사항 식별
		정보보호 정책 및 준수
	서비스 제공자 및 공급자 정보보호(supplier, provider)	IT 서비스 자산식별 및 민감도 평가/ IT 서비스 위협평가
	서비스 운영조직 정보보호	서비스 운영조직 구성 및 활동/교육 훈련 프로그램 수행/인사보안(직무정의 와 고용보안)/문서보안
	서비스 사용자 정보보호 (customer)	개인정보 수집에 관한 조치/개인정보 이용 및 관리 서비스 사용자 권리/개인정보 공개 및 책임/서비스 사용자 권리규제
IT 서비스 정보보호 기반구조	서비스 기반구조 보호(접근통제, 보안 시스템 도입 및 지속적 갱신, 운영로그 분석)	네트워크보안/서버 보안/단말기 보안
	응용 서비스 보호	응용 프로그램 보안/정보 서비스 콘텐츠 보안
IT 서비스 정보보호 운영관리	위험관리	위협 관리/취약점 관리
	사후관리	형상관리/변경관리/유지보수/사고대응 및 복구
	모니터링 및 재평가	성과 분석 및 반영/평가 및 승인

(4) 정보보호 등급 결정

앞서 설명한 평가모형에 따라 각 평가항목별로 산출된 결과를 가지고 최종 평가등급을 결정하기 위한 다양한 방법은 선행연구를 고려하여 볼 때, 평가항목 점수 합산을 통하여 평가영역별로 평가점수를 산정한 다음, 문헌연구 및 전문가 의견조사 방법을 통하여 평가영역, 평가항목, 세부 평가항목별로 상대적 가중치를 산정하고 이를 합산하여 그 결과가 최종적인 정보보호 성숙모형 어느 부분에 위치하는 지를 설정함으로써 최종적인 정보보호 등급을 결정하는 방식을 취하는 것이 합리적이라고 할 수 있다.

등급의 구분은 정보보호 수준의 개선 정도를 표시하고 또한 사업자간 자율경쟁을 도모하기 위해서는 최소 5단계로 구분하는 것이 적절하다고 판단되었다. 3단계의 구분은 단계별 차별성을 보이기에는 너무 적으며 5단계 구분이 선행연구를 참고하여 볼 때 보편적인 방법으로 판단된다. 단계별 특성은 정보보호 성숙모형에 기초하여 IT 서비스 내에 정보보호통제 및 프로세스의 구현정도와 지속적인 개선을 표현하는 일반적인 성숙도 모형과 크게 다르지 않게 작성하였다. 따라서 등급의 명칭은 비교적 간단하고 명확한 방식으로 표현하되 등급의 특성은 일반적인 정보보호 성숙도수준을 표시하는 것으로 도입이전, 단편적 구축, 체계적 구축, 관리 및 측정, 최적화와 같이 설계하였다. 이 모델은 비교적 간단한 성숙단계를 제시하고 있는 정보보호 지배구조 모형을 도입하여 각 평가영역별 합산 점수에 따라 정보보호 수준 성숙단계를 설계하였다. 이러한 정보보호 성숙단계 측정을 통하여 신규 IT 서비스의 현재 정보보호 수준을 기준으로 현재의 IT 서비스가 어떠한 부분을 개선하면 정보보호 수준을 향상시킬 수 있는지에 대한 정보보호 추진 방향성을 제시할 수 있다.

VI. 신규 IT 서비스 정보보호 등급인증 타당성 평가 결과

최근에는 정보 획득기술과 획득된 정보를 바탕으로 사용자에게 원하는 정보를 스스로 자연스럽게 제공함으로써 가상의 전자공간과 물리공간이 결합된 새로운 형태의 지능적 서비스 환경이 개발되고 있다. 이러한 서비스들의 가장 큰 특징은 언제 어디서나 서비스 기업이 제공하는 정보에 쉽게 접근할 수 있다는 것이다. 그러나 이러한 특징을 다른 관점에서 살펴보면, 공유된 모든 정보가 언제 어디서나 사용할 수 있다는 것은 악의적인 경우 쉽게 정보가 노출되고 변경될 수 있다는 것을 의미하며, 현재의 서비스 환경보다 더욱 더 다양한 보안 취약성으로 인하여 정보의 안전한 관리가 힘들어 질것으로 예상된다.

본 연구에서는 향후 전개될 신규 IT 서비스에 대하여 정보보호 요구사항을 분석하고 측정하여 정보보호 수준을 제고하기 위한 목적으로 '신규 IT 서비스의 정보보호등급인증제'를 설계하였다. 본 연구의 결과는 국내 IT 서비스의 정보보호 수준을 객관적으로 평가하는 데 활용될 수 있으며, 국내 IT 서비스 제공기업들의 정보보호 수준제고를 위한 정책수립의 합리적인 의사결정 도구로 응용될 수 있다. 세부적으로 IT 서비스 사용자의 정보보호 현황과 의식변화에 대한 추이를 분석함으로써 새로운 IT 서비스를 설계하는 데 필요한 선결요건으로 정의될 수 있다. 또한 신규 IT 서비스의 정보보호에 대한 객관적인 조사 및 분석이 가능한 평가 지표 개발을 통하여 IT 서비스 정보보호 현황에 대한 정확한 이해를 돕고, 아울러 서비스 제공기업 스스로 정보보호를 추진할 수 있도록 동기를 부여할 수 있다.

참 고 문 헌

[1] 한국정보보호진흥원, 정보보호영향제도 도입방안 연구, 2003.

[2] 한국전산원, 범정부기술참조모델 1.0, 2004.

[3] 한국전산원, "ITA 성숙수준 평가모델 적용방안", 2005.

[4] 한국전자통신연구원, "u-정보보호 기본전략: 기술개발 계획", 2006.

[5] 서종렬, "WiBro 동향과 사업전략", *대한전자공학회지 제15권 제3호*, 2005.

[6] Christopher M. King, Curtis E. Dalton, & T. E. Osmanoglu, "Security Architecture Design, Development & Operations", *RSA Press,* 2001.

[7] NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for FIS", 2006. 2.

[8] NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories", 2004. 6.

[9] Rick Leopoldi, "A Business Based Approach to ITIL Maturity", RL Consulting, 2005

[10] Karen M. Zimmie, "Secure and Mature; Combining a CMMI with SSE-CMM Appraisal", 2004. 4. 8.

[11] Carnegie Mellon-Software Engineering Institute, CMMI Overview, 2005.

장 항 배(張恒培)

2006년 2월: 연세대학교 정보시스템관리 전공(정보시스템 박사)
2007년 3월 ~ 현재: 대진대학교 경영학과 교수
관심분야: 정보화 수준평가, 정보보호, 유비쿼터스 컴퓨팅

조 태 희(曺台姬)

1998년 8월 : 경북대학교 전자전기공학부(공학사)
2008년 3월 ~ 현재 : 연세대학교 정보대학원 석사과정
관심분야 : 정보보호 및 정보화 평가인증

김 효 진 (金孝珍)

2008년 2월: 서울여자대학교 문헌정보학과(문학사)
2008년 3월 ~ 현재 : 연세대학교 정보대학원 석사과정
관심분야 : 모바일 콘텐츠