정보보호 수준평가 방법 개선에 관한 연구

Developing the Assessment Method for Information Security Levels

오남석(Nam-Seok Oh)*, 한영순(Young-Soon Han)**, 엄찬왕(Chan-Wang Eom)**,
오경석(Kyeong-Seok Oh)**, 이봉규(Bong Gyou Lee)***

초 록

본 논문은 정보통신 서비스 제공기관 및 업체가 현재의 보안 상태를 단계별로 등급화된 지표에 따라 평가하고, 지속적으로 정보보호 수준을 상위 단계로 개선해 나갈 수 있도록 정보보호 수준평가방법을 제안하였다. 이를 위해 SP800-26의 17개 분야, SP800-53의 3개 분야, ISMS의 15개 분야, ISO27001의 10개 분야를 분석하여 중복적인 분야를 제거하고, 관련 전문가 회의를 통해 12개 평가분야와 SP800-26의 221개 항목, SP800-53의 17개 항목, ISMS의 137개 항목, ISO27001의 127개 항목을 분석하여 54개 평가항목을 도출하였다. 또한, 54개 평가항목에 대한 수준을 5단계로 구분된 지표에 따라 각각 평가하고, 각 평가분야별로 등급을 결정할 수 있도록 하였다. 아울러, 개발된 평가항목과 등급 등이 실제 운영환경에 잘 적용될 수 있도록 운영상에서 발생할 수 있는 문제점을 사전에 분석하고, 이를 고려한 수준평가의 효과적인 7가지 수행방안을 제시하였다. 본 논문에서 제안한 정보보호 수준평가 방법은 계량화된 데이터를 통해 해당조직의 정보보호 대책을 수립할 수 있도록 지원하며, 조직 관리자들의 정보보호 목표수준 설정을 위한 자료로 활용되어 국가적 차원의 정보보호 수준 향상에 기여할 수 있을 것이다.

ABSTRACT

In order for agencies and companies at the IT service industry to check as well as to upgrade the current status of their information security programs, this paper suggests the assessment method for information security levels. The study developed 12 assessment fields and 54 assessment items derived from domestic and foreign cases including SP800-26, SP800-53, ISMS, and ISO27001. It categorized 54 assessment items into 5 levels for determining information security levels. Also, the study presents 7 strategies for performing their efficient evaluations. The proposed method and process in this paper can be useful guidelines for improving the national information security level.

키워드 : 정보보호 수준평가 방법, 평가 지표, 정보보호, 보안성숙도
Assessment Method for Information Security Levels, Assessment Indicator, Information Security, Security Maturity

---

본 연구는 방송통신위원회의 방송통신정책연구센터운영지원사업의 연구결과로 수행되었음(KCA-2011-0902-1). 본 논문은 2010년 한국전자거래학회 춘계학술대회에서 우수논문으로 선정되어 학회지에 게재됨.

* 방송통신위원회 전파기획관
** 연세대학교 정보대학원 박사과정
*** 교신저자, 연세대학교 정보대학원 교수

2011년 04월 07일 접수, 2011년 05월 03일 심사완료 후 2011년 05월 23일 게재확정.

1. 서 론

최근 정보화의 진전으로 방송통신, 행정, 의료 등 각종 사회기반 서비스들의 IT 의존도가 심화되고, 이들을 대상으로 하는 각종 사이버 침해도 급증하고 있다. 물론 범정부 차원의 다양한 정보보호 정책과 제도들이 마련되어 시행되고 있지만, 아직 이러한 제도 수행 후 얼마나 보안 수준이 향상되었는지 또는 현재 보안 수준이 어느 정도인지 제대로 측정하기가 용이하지 않아 정보보호 수준평가가 제대로 이뤄지지 못하고 있는 실정이다[1-3]. 특히, 정보통신 서비스에 대한 정보보호 수준평가 방법은 정보통신 서비스의 특징이 충분히 반영되지 않은 평가항목들을 정보통신 서비스 관련조직이 자체적으로 평가하여 신뢰성이 저하되기도 한다. 또한, 컨설팅업체를 통해 취약점을 분석 및 평가하여 보호대책을 수립하는 경우에도 지속적으로 정보보호 수준을 개선해 나갈 수 있도록 현재의 보안 상태를 단계별로 등급화된 지표에 따라 평가할 수 있는 정량적인 평가가 이루어지기는 어려운 실정이다[4, 5]. 따라서 정보통신 서비스 제공기관 및 업체가 현재의 보안 상태를 단계별로 등급화한 지표에 따라 평가하고, 지속적으로 정보보호 수준을 상위 단계로 개선해 나갈 수 있도록 도와주는 정보보호 수준평가 방법론이 필요하다. 이러한 정보보호 수준평가는 국가적 차원에서의 보안 성숙도를 향상시키기 위한 발판이 될 것이다.

본 논문은 정보통신 서비스를 안정적으로 운영 및 관리하고, 정보통신 서비스별 정보보호 수준을 지속적으로 평가하고 개선할 수 있는 활동을 지원하기 위해 단계별로 구분된 평가지표를 마련하고, 평가항목들을 정리하였다. 특히, 국내·외 정보통신 서비스의 정보보호 수준평가 사례를 조사 및 분석하여 국내에 적용할 수 있는 평가지표를 만들어, 미국표준기술연구소(National Institute of Standards and Technology)의 SP800-53(Special Publications 800 Series)의 보안가이드와 SP 800-26, ISO27001, ISMS(Information Security Management System) 등과의 평가항목 비교·분석을 통해 정보보호 수준을 평가하기 위한 평가항목을 제시하였다[6, 7]. 또한, 국내·외 정보통신 서비스의 정보보호 수준평가 사례를 고찰하여, 정보통신 서비스의 정보보호 수준평가방법론과 정보보호 수준평가의 효과적인 수행방안을 제안하였다

2. 국내외 정보보호 수준평가 사례 조사

2.1 국내외 정보보호 수준평가 사례현황

2.1.1 정보보호 관리체계 인증(ISMS)

인터넷 침해사고 등으로 인해 조직적이고 전사적이며 관리·물리·기술 및 환경전반에 걸친 정보보호 관리의 중요성이 더욱 제시되고 있고 이러한 정보보호 등에 관한 전반적인 체계를 '정보보호 관리체계'라고 한다[5]. 국내에서는 정보보호에 대한 전반적인 인식수준의 제고와 경쟁력 향상을 위한 정보보호 관리체계를 수립하여 운영하고 있다. 또한 이를 공신력 있는 기관이 제 3자 인증을 부여함으로써 대외 경쟁력 향상과 신뢰 제고를 유도하고자 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조를 통하여 정보보호 관리체

계 인증제도의 근거를 마련하였으며 '정보보호 관리체계 인증심사기준'을 제정·고시하여 본격적으로 인증제도를 수행하고 있다[1, 5].

2.1.2 취약점 분석·평가

국내에서는 정보통신 기반 보호법의 제정·공포 및 시행에 따라 정보통신 서비스의 해킹 등 위협으로부터 보호할 수 있도록 정보보호 현황을 작성하고, 적정 수준의 기술적 정보보호 대책 및 정보보호 평가업무 프로세스를 수립하며, 안정적인 정보보호 체계를 구축하기 위해 취약점을 분석하고 평가한다.

취약점 분석·평가는 최초 지정일로부터 6개월 이내 실시토록 규정하고 있고, ISO17799(ISO27001), 한국인터넷진흥원의 ISMS, ISACA(Information Systems Audit and Control Association)의 COBIT, IDC(Internet Data Center) 안전운영 가이드, 정보통신 기반 보호법의 내용을 기준으로 평가를 수행하며, 기관의 보안 전담반이나 외부 정보보호 컨설팅 전문 업체를 지정하여 수행하고 있다. 특히, 취약점 분석·평가는 정보통신 서비스의 안정적 운영과 동 시설에 내장된 중요 정보의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 전자적 침해행위 등 다양한 위협요인을 파악하고 이들 위협요인에 대한 정보통신 서비스의 취약점 침해 시 파급효과 및 대책을 식별 분석 평가한다. 대부분의 정보통신 서비스에서 평가를 진행할 때에는 각각의 평가 방법론에 근거하여 물리적, 관리적, 기술적인 측면을 세부 모듈로 분류하여 취약점을 평가한다.

2.1.3 정보보호 안전진단

정보보호 안전진단 제도는 주요 정보통신 서비스제공자(ISP), 집적 정보통신 시설사업자(IDC), 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 정보보호 조치에 대한 관리적, 기술적, 물리적 보호조치를 이행하고 컨설팅업체로부터 안전진단을 받음으로써 정보통신망 및 정보통신 서비스에 대한 안정성 및 신뢰성을 확보하기 위한 제도이다. 정보보호 안전진단수행을 위한 절차는 관리적, 기술적, 물리적 정보보호 조치 이행 여부에 대해 안전진단을 수행한 후 개선사항을 권고하고 명령하는 절차로 수행된다.

2.1.4 SP800-26(Security Self-Assessment Guide for Information Technology System)

SP800-26은 NIST에서 해당조직의 자체 보안 평가를 위하여 제작한 가이드라인으로 시스템을 평가하기 위해 제공되는 표준이다. 여기서의 자체평가는 하나의 시스템(주요 어플리케이션, 일반지원 시스템) 또는 상호 연결된 시스템 그룹에 대한 현재 상태측정과 정보기술 보안 측정에 사용되는 방법으로 NIST에서 개발한 Federal IT Security Assessment Framework를 기초로 작성되어 있다[7].

2.1.5 SP800-53(Recommended Security Controls for Federal Information Systems)

연방 정부 행정기관을 지원하는 정보시스템에 대한 보안 평가를 선택 및 지정 하는 지침 제공을 목적으로 NIST에서 작성한 권고안이다. 권고안의 대상으로는 정보시스템 및 정보보안 관리 및 감독 책임이 있는 개인, 정보시스템 개발 책임이 있는 개인, 정보보안 실행 및

운영 책임이 있는 개인, 정보시스템 및 정보보안 평가 및 감독 책임이 있는 개인을 대상으로 한다[6].

2.1.6 ISO27001

ISO27001은 기업이 고객 정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 둔다. ISO27001은 영국의 상무성 주관으로 “정보보안 관리 실무 규범(A Code of Practice for Information Security Management)”이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 개발된 BS7799(British Standards)에 기반하여 국제표준화 기구인 ISO에서 표준화한 정보보호 관리체계이다. ISO27001은 기업들이 부딪치는 대부분의 상황에 필요한 평가를 식별하기 위한 단일한 참조점을 제공하고 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 분서를 참조함으로써 기업들 간의 네트워킹에 있어서 상호 신뢰가 가능하도록 한다[8].

2.2 국내·외 정보보호 수준평가 사례 분석 및 시사점

정보통신 서비스의 정보보호 수준 및 안전성을 점검 받기 위한 다양한 제도들이 운영되고 있다. ISMS는 ISO27001을 바탕으로 국내 실정에 맞도록 구성된 인증체계로서 정보보호 조치의 이행여부에 대한 점검 사항들로 구성되어 있으며, 이행여부에 대한 결과치를 통해 ISMS 인증을 부여하고 있다. 취약성 분석·평가는 관련조직의 취약성에 대해 주기적으로 분석을 수행하여 보호대책을 수립하기 위한 제도이고, 정보보호 안전진단 역시 보호조치 이행 여부에 대해 점검하고 있다[1].

이러한 제도의 특징은 평가사항들의 시행여부 또는 사전에 정의한 평가기준에 적합한지 등을 단순 점검하고 있다는 것이다. 따라서 정보보호 대책을 수립하고 시스템 및 서비스의 취약점을 점검하는 등 여러 가지 보호활동을 수행하지만 각각의 활동을 계량화된 등급으로 측정할 수 있는 평가지표가 마련되어 있지 않아 보안수준을 정확하게 측정하기 어려운 문제점을 안고 있다.

또한 “정보보호 수준평가”라는 의미는 평가사항의 지속적 관리 및 이행여부를 내포하고 있기 때문에 개선대책 수립 시에도 계량화된 자료를 통해 명확한 대책을 수립할 수 있어야 하는데 현재의 제도로는 한계가 있는 것이 사실이다.

따라서 이와 같은 문제점 해결을 위해 본 논문에서는 정보통신 서비스 제공기관 및 업체가 현재의 보안 상태를 단계별로 등급화된 지표에 따라 평가하고, 지속적으로 정보보호 수준을 상위 단계로 개선해 나갈 수 있도록 정보보호 수준평가 방법을 제안한다.

3. 정보통신 서비스의 정보보호 수준평가 방법

3.1 정보보호 수준평가를 위한 지표

본 연구에서는 정보보호 수준을 평가하기

위한 평가 지표 개발을 위해 여러 분야에서 평가 지표로 사용하는 것들을 분석하였다. 즉, SSE-CMM(Systems Security Engineering-Capability Maturity Model)에서 정보시스템의 보안기능과 성능의 평가는 요구되는 보안수준의 적정성을 결정하는데 매우 중요한 요소임을 알 수 있다. SP800-26는 자체 평가 시 각각의 보안평가 질문에 대해 해당되는 단계에 체크할 수 있도록 구성하고 있고, CC(Common Criteria)는 정보보호시스템의 보안성에 대한 신뢰성 정보를 위해 국제 공통평가 기준을 개발하고, 공정하고 객관적인 평가를 시행할 수 있는 평가 체계를 구축하여 고객이나 혹은 기업이 사용할 수 있게 하고 있다. 미국 국방부 표준 규격 문서인 TCSEC(Trusted Computer System Evaluation Criteria)는 컴퓨터 보안 제품을 평가하기 위해 채택한 컴퓨터 보안 평가 지침서로 활용되고, ITSEC(Information Technology Security Evaluation Criteria)는 모든 정보보호 제품을 평가하기 위해 사용된 기준을 활용한 지표를 보여 주고 있다[9-11].

본 연구에서 개발한 평가 지표는 SSE-CMM의 성숙도 측정 평가를 기반으로 한 단순화된 5단계 평가 지표를 제안하고자 한다. SSE-CMM에서 제안하고 있는 5단계 지표의 경우, 영역(domain)과 능력(capability)이라는 2가지 측면의 구조에 실무(practice) 활동들로 구성되어 있어 일반적인 정보보호 관리조직에 적용하기에는 너무 복잡하고 관리자가 이해하기 어려워, 수준평가를 진행하기에는 다소 무리가 있다고 판단하였다. 따라서 본 연구에서는 능력측면만을 지원하는 단순화된 5단계 평가지표에 한정하고, 영역측면은 평가항목을 구성하여 보완토록 고안하였다.

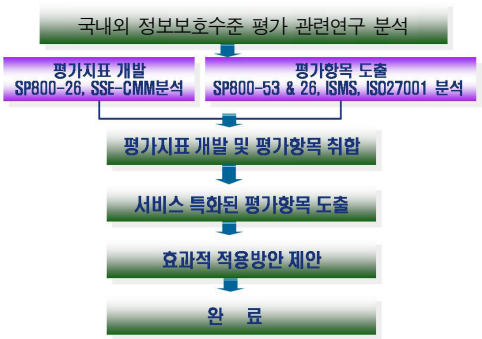
3.2 정보보호 수준평가를 위한 평가 항목

NIST의 평가리스트(SP800-53, SP800-26)와 보안 관리분야의 ISO27001, KISA의 ISMS

〈표 1〉 정보보호 수준평가 등급(예시)

등급	평가 착안 사항
1	평가항목에 대한 수행 시 특별한 관리체계나 계획 없이 수행되고 있는 단계 - 평가항목에 대한 내용을 수행하고 있으나, 구체적인 관리체계나 계획이 수립되지 않은 상태에서 수행하고 있는 단계를 의미
2	평가항목을 수행하기 위한 관리체계나 시행계획(구체적 절차 및 일정, 예산 등)이 수립되어 문서화되어 있는 단계
3	문서화된 관리체계나 계획에 따라 세부 평가 항목을 시행하거나 시행 완료된 단계 - 관리체계나 계획·절차 수립 후 이행되고 완료되어 있는 단계
4	평가항목에 대한 성과 측정이 수행되고 일정기간 동안 지속적으로 시행되는 단계 - 규정 및 절차 등은 규정 개정 이력 및 규정 위반자 조치 내용 등으로 평가할 수 있으며, 세부평가 항목 시행 결과분석이 정기적으로 이행됨을 증명할 수 있음 (특히 기술적 세부평가항목인 경우 최초 시행 일시 기술)
5	평가항목 시행성과 측정 결과가 검토되고 결과에 따라 개선되는 단계 - 평가항목 시행 결과 분석 후 차후 반영되어 실시되고 있어야 함

등을 비교분석하여 정보통신 서비스의 정보보호 수준을 측정하기 위한 평가 분야와 항목을 도출하였다. 이를 위해 <그림 1>에 명시된 바와 같이, SP800-26의 17개 분야, SP800-53의 3개 분야, ISMS의 15개 분야, ISO27001의 10개 분야를 분석하여 중복적인 분야를 제거하고, 국내 정보통신 서비스 실정에 맞는 분야를 관련 전문가 회의를 통해 12개로 선별 정리하였다.



〈그림 1〉 정보보호 수준 평가지표 및 항목 개발

두 번째는 평가분야별로 협의적 프로세스 의미를 담고 있는 항목으로 구성되어 있는데, 12개 평가분야와 마찬가지로 SP800-26의 221개 항목, SP800-53의 17개 항목, ISMS의 137개 항목, ISO27001의 127개 항목을 분석하여 중복적인 항목을 제거하고, 국내 정보통신 서비스 실정에 맞는 평가항목을 관련 전문가 회의를 통해 54개로 선별 정리하였다(<표 2> 참조).

3.2.1 정보보호 수준평가 방법

정보보호 수준평가 방법은 프로세스 관점에서 평가분야 12개에 대한 상태를 측정하는데, 각 분야별로 제시하고 있는 평가항목에 대해 측정한 평가값의 합을 구해 등급화 한다. 프로세스 측면에서의 평가와 기능적 측면에서의 평가는 5단계의 자체 평가 후, 현장평가와 문서 확인을 통해 계획수립-운영-시행-테스트 및 반영 등의 개념이 적용된 프로세스 측면에서의 평가를 수행한다.

정보보호 수준평가 결과를 산출하는 방법은 2단계로 진행하는데, 첫 번째는 54개 평가항목에 대한 수준을 5단계로 구분된 지표에 따라 각각 평가하고, 두 번째는 각 평가분야별로 등급을 결정한다. 이 때, 각 평가분야의 등급은 분야별 평가항목의 정보보호 성숙도 단계 중 최저 단계를 기준으로 채택하여 산출하게 된다. 다음 수식과 같이, 평가분야별 평가 값의 합을 평가분야 수로 나눈 AL(Assessment Level)이 평가된 기관 및 업체의 정보보호 수준이 된다.

$$AL = \frac{S}{\text{평가분야수}}$$

(AL : 평가등급, S : 평가합)

4. 정보보호 수준평가의 효과적 수행방안

본 논문에서 제안한 평가항목과 등급이 실제 운영환경에 잘 적용될 수 있도록 하기 위해서는 운영상에서 발생할 수 있는 문제점을 사전에 분석하고, 이를 고려한 효과적 수행방안을 제시할 필요가 있다. 즉, 정보통신 서비스 기관 및 업체에서 정보보호 수준 평가 시 발생할 수 있는 실질적인 문제점과 이를 고려한 수준평가의 효과적 수행방안은 다음

〈표 2〉 정보보호 수준평가 분야 및 항목

No	분야	평가 항목		분야	평가 항목
1	정보보호 정책	정보보호 조직	9	인적보안	신원조사
		정보보호 계획			인사관리
2	위험평가	자산분류			내부인력 관리
		자원할당			제3자 보안
		보안 요구사항 검토	10	사고대응	사고대응 모의 훈련
		위험평가			사고 모니터링
		취약성 진단			보안사고 보고
3	구성관리	구성변경 평가	11	감사 및 책임 추적성	감사대상 이벤트 생성 기능
		구성보안 설정			감사정보 관리
4	유지보수	유지보수 도구			감사 모니터링, 분석 및 보고
		원격 유지보수			감사기록 시간 표시 기능
5	매체보호	매체 출력물 표시			부인방지
		매체 접근 관리	12	시스템 접근평가 및 통신보호	계정관리
		매체 운반 방법			패스워드 관리
		문서관리			설정관리
		매체 및 기록 파기			접근통제
6	보안 인식과 교육	보안인식과 교육 및 훈련			접근시도 실패관리 기능
7	비상계획/ 업무 연속성 계획	비상교육			시스템 이용주의사항 공지기능
		비상계획 모의 훈련 및 갱신			이전로그인 정보 알림기능
		통신서비스 이중화			세션 통제 기능
		정보시스템 백업과 복구			시스템과 응용프로그램의 분리
8	물리적/ 환경적 보호	물리적 접근 통제			공유 시스템 자원 보안 관리
		디스플레이 매체 접근 통제			소프트웨어 결함 및 악성코드로부터의 보호
		물리적 접근 모니터링			침입탐지 및 차단 도구와 기술
		전력 장비 및 전력선 보호			서비스 거부 보호
		비상전력			보안통신경로
		비상조명			암호키 구축 및 관리
		환경통제			인터넷 전화

과 같다.

첫째, 정보통신 서비스의 정보보호 수준평가는 총 12개 평가분야 및 54개 평가항목에 대해 각각 등급을 산정하는 구조로 구성되어 있는데 등급 산정이 이뤄지면 반드시 이에 대한 증빙이 가능해야한다. 예를 들면, 3등급은 계획에 따라 평가항목을 수행되는 단계로 정의됨에 따라 “계획에 따라 시행한 후 어떤 결과물을 남겨야 된다.” 여기서 증빙방법은 계획서, 공문, 결재문서 등의 서류로 증빙하는 것

이 가장 확실한데, 정보보호 계획의 평가항목의 경우는 연간 정보보호 계획서, 정보보호 사업계획서, 매년 수행된 과제보고서와 예산편성 내역 등이 증빙자료로 검토될 수 있다.

둘째, 정보보호 수준평가를 자체 평가로 수행할 경우, 평가자가 보안전문가가 아닌 일반 직원이 수행하면 평가지표를 구분하는 잣대로서의 설명이 부족하여 일관된 평가 결과를 도출하기 어렵기 때문에 반드시 보안전문가가 수행하는 것이 바람직하다[10]. 예를 들어, 3등급이 세부 평가항목을 수행하는 시행하는 단계이고, 4등급은 세부 평가항목에 대한 성과 측정이 수행되는 단계이다. 그렇다면 “성과 측정은 도대체 무엇을 의미하는 것인가? 어떤 성과를 측정하라는 의미이며 측정을 위한 기준들은 무엇이 있는가? 분석이 정기적으로 이행되려면 어떤 분석이 필요한가?”와 같은 질의에 답할 수 있어야 한다. 즉, 대부분의 정보보호수준 평가는 보안전문가가 보안업무의 경험을 통해서만 할 수 있는 경우가 많기 때문에 보안전문가에 의해 수행하는 것이 바람직하다.

셋째, 등급 기준의 모호성 문제를 해결하기 위해서 평가항목에 대한 착안사항을 정의할 필요가 있다. 본 연구는 평가 착안사항을 구체적으로 기술하다보면 평가지표를 충족하는 모든 세부 활동을 언급하지 못하는 완전성의 오류와 평가지표의 정의를 충실히 따르지 못하는 일관성의 오류를 함께 범하게 될 우려가 있어 단순화하여 제안하고 있기 때문에 평가기관 및 업체는 평가를 수행하기 전에 각 평가항목별로 착안사항을 정의해야할 것이다.

넷째, 정보보호 수준평가가 수행되고 나면 평가분야 별로 해당기관의 강점과 약점을 분석할 수 있다. 따라서 보호수준이 취약한 분야에 대해서는 반드시 원인을 분석하여, 정보보호 수준 강화를 위한 보안대책을 마련하여 시행해야 한다. 즉, 정보보호 수준평가는 현재의 보호수준을 측정하고 취약한 분야에 대한 수준 강화가 목적이기 때문에 수준평가를 수행되고 나면 반드시 보안대책을 마련해야 할 것이다.

다섯째, 본 연구에서 제안된 총 12개 평가분야 및 54개 평가항목에 대하여 평가기관 및 업체에 환경을 고려하여 반영하고 있지 않는 항목은 적용항목에서 제외가 가능하다. 일부 기관의 경우 54개 항목을 반드시 체크해야하는 항목으로 인식하여 부담을 갖는 경우가 있었다. 그러나 각 항목들의 평가는 수행하고 있는 항목에 대해서만 평가 실시가 가능함으로 수행이 되고 있지 않거나 또는 보유하고 있지 않는 장비에 대해서는 제외하고 평가를 실시해도 무방하다. 따라서 기관 및 업체의 환경에 따라 54개 항목은 가변적으로 인식해서 사용해도 된다. 예를 들면, 12번째 평가분야인 시스템 접근통제 및 통신보호에서 평가항목은 총 16개로 구성되어 있는데, 평가기관에서 인터넷 전화를 사용하고 있지 않은 경우는 총 15개의 항목에 대해서만 평가해도 된다.

여섯째, 평가기관 및 업체의 서비스별 특성에 맞도록 평가항목별 가중치를 두어 평가를 실시하면 더욱 정확한 측정이 가능해 진다[12]. 물론 이러한 경우에는 반드시 가중치 선정의 적절성 확보 방안을 모색해야 한다. 국내・외 기관에서 사용하는 가중치 부여방법은 (1) 구성항목이나 지표에 대해 동일한 비중으로 가중치를 부여하는 단순평균방식, (2) 요인분석

등을 활용하여 항목 간 상대적 비중을 계산하여 가중치를 부여하는 방식, (3) 해당분야 전문가를 대상으로 항목의 상대적 중요성을 판단하도록 하여 가중치를 부여하는 방식의 세 가지로 구분된다[13]. 그러나 각 방식들은 제각기 한계가 있기 때문에 가중치를 부여하여 평가를 할 경우에는 주의가 필요하다. 즉, 단순평균방식은 모든 구성항목 및 평가지표가 동일하다고 가정하기 때문에 최종 단계를 산출하기는 쉽지만 부문별 상대성을 반영할 수 없는 단점이 있다. 요인분석 방식은 통계적으로 논리가 분명하고, 객관적일 수 있지만 향후 구성항목 및 평가지표가 확대된다면 적용에 문제점이 노출될 수 있다. 전문가를 활용한 델파이 기법은 전문가 의견을 종합할 수 있다는 장점이 있지만 가중치 논의과정에서 특정인의 주장에 따라 왜곡된 결과가 노출될 수도 있다. 따라서 가중치를 적용하여 평가를 수행하고자 할 경우에는 사전에 몇 가지 경우의 수를 고려하여 시뮬레이션해보는 방법도 바람직하다.

일곱째, 본 연구에서 제시한 평가지표가 평가기관 및 업체에 적용하기 어렵다고 판단될 경우에는 SSE-CMM에서 포함하고 있는 평가등급별 일반 실무(general practice)와 같은 형태의 가이드라인을 평가지표로 활용할 수도 있다. 특히 평가지표의 구성은 보안에 대한 일반 활동 보다는 절차에 부합하는 표준화 활동을 조직 측면에서 스스로 내재화하여 추진할 수 있는지를 평가하는 것이 단기적인 능력 평가가 아닌 조직의 중장기 능력 측면에 대한 평가로 이어지게 되기 때문에 절차중심의 조직에서는 SSE-CMM의 평가지표 활용도 가능하다.

5. 결 론

기존의 많은 정보보호 관련제도들은 평가사항들의 시행여부 또는 사전에 정의한 평가기준에 적합한지 등을 단순히 점검하는 것이 대부분이었다. 따라서 정보보호 대책을 수립하고 시스템 및 서비스의 취약점을 점검하는 등 여러 가지 보호활동을 수행하지만 각각의 활동을 계량화된 등급으로 측정할 수 있는 평가지표가 마련되어 있지 않아 보안수준을 정확하게 측정하기 어려운 문제점을 안고 있었다. 또한 “정보보호 수준평가”라는 의미는 평가사항의 지속적 관리 및 이행여부를 내포하고 있기 때문에 개선대책 수립 시에도 계량화된 자료를 통해 명확한 대책을 수립할 수 있어야 한다.

본 논문에서는 정보통신 서비스 제공기관 및 업체가 현재의 보안 상태를 단계별로 등급화된 지표에 따라 평가하고, 지속적으로 정보보호 수준을 상위 단계로 개선해 나갈 수 있도록 정보보호 수준평가방법을 제안하였다. 이를 위해 국내·외의 정보보호 수준 평가 사례를 분석하여 평가분야 및 평가항목을 도출하고, 정보보호 수준평가를 위한 단계별로 등급화된 평가지표를 제안하였다. 아울러, 개발된 평가항목과 등급 등이 실제 운영환경에 잘 적용될 수 있도록 운영상에서 발생할 수 있는 문제점을 사전에 분석하고, 이를 고려한 수준평가의 효과적 수행방안을 제시하였다. 본 연구에서 제안한 정보보호 수준평가방법은 정보통신 서비스 제공기관 및 업체에서 계량화된 데이터를 통해 해당조직의 정보보호 대책을 수립할 수 있도록 지원하며, 아울러 조직관리자들의 정보보호 목표수준 설정을 위한

자료로 활용되어 국가적 차원의 정보보호 수준 향상에 기여할 수 있을 것이다.

향후에는 기술적 측면에서 정보통신 서비스 분야를 중심으로 제시된 정보보호 수준평가 방법론을 여타 행정, 금융, 의료, 에너지 등 주요 국가사회기반 영역으로 확대 적용할 수 있도록 각 분야별 환경에 맞는 평가항목 및 기준을 개발할 필요가 있다. 또한, 제도적 측면에서는 사이버 침해사고 발생 시 경제적·사회적 피해의 파급효과가 큰 대국민서비스에 대하여는 서비스의 안정적 운영을 위해 정보보호 수준평가의 법적 의무화 방안을 검토할 필요가 있다.

참 고 문 헌

[1] 한국인터넷진흥원, 정보보호 수준평가 방법론 안내서, 2010. 3.

[2] 김진영, 정보보호수준 평가 방법론 개발에 관한 연구, 석사학위논문, 2003.

[3] 한근식, “정보보호 수준평가에서의 표본설계방법에 따른 허용오차”, 정보보호 심포지움, 2009. 6.

[4] 이강신, “정보보호관리체계 인증가이드”, 한국정보보호진흥원, 2002.

[5] 정경호, 민경식, “국가 정보보호수준 평가 모델 개발”, 한국정보보호진흥원, 2001.

[6] Ross, R., “Guide for Assessing the Security Controls in Federal Information Systems : Building Effective Security Assessment Plans,” NIST, Special Publications 800-53A, 2008.

[7] Swanson, M., “Security Self-Assessment Guide for Information Technology System,” NIST, SP800-26, 2001.

[8] ISO/IEC, Information Security Management System Part 2 : Specification for Information Security Management System, 2005.

[9] Carnegie Mellon University, “SSE-CMM Model Decripton Document,” SSE-CMM, 2003.

[10] Carley, M., Social Measurement and Social Indicators, George Allen and Unwin, Ltd., London, 1981.

[11] Carnegie Mellon University, “The SSE-CMM Appraisal Method (SSAM)-Capability Maturity Model,” 1999.

[12] 강신원, “국가정보화지수 측정을 위한 가중치 연구 : RCSS를 중심으로”, 정보통신정책연구, 제6권, 제2호, pp. 47-64, 1999.

[13] 황종성, “국가정보화종합지수 모델개발 연구”, 한국전산원, 2005.

저 자 소 개

오남석 (E-mail : nsoh@mic.go.kr)
2010년 연세대학교 정보대학원 IT경영전략 (석사)
1990년~현재 방송통신위원회 전파기획관
관심분야 IT 정책·산업, 방송통신융합정책, 정보보안

한영순 (E-mail : rache102@yonsei.ac.kr)
2009년~현재 연세대학교 정보대학원 IT 정책·산업 박사과정
2001년~현재 Volvo Group Korea (주) Truck CIO
관심분야 IT 정보보호, 방송통신융합정책, ITS

엄찬왕 (E-mail : eomcw@mke.go.kr)
2007년~현재 연세대학교 정보대학원 IT 정책·산업 박사과정
1992년~현재 지식경제부 전력산업과 과장
관심분야 IT 정책·산업, 정보보호

오경석 (E-mail : fastbikers@yonsei.ac.kr)
2007년~현재 연세대학교 정보대학원 IT 정책·산업 박사과정
2001년~현재 ETRI 사업화본부 선임연구원
관심분야 IT Policy, 방송통신융합정책, 정보보안

이봉규 (E-mail : bglee@yonsei.ac.kr)
1998년 연세대학교 상경대학 (학사)
1992년 Cornell University (석사)
1994년 Cornell University (박사)
1997년~2004년 한성대학교 정보전산학부 교수
2005년~현재 연세대학교 정보대학원 교수, 부원장
관심분야 IT 정책·산업, 방송통신융합정책, 정보보안