디지털산업정보학회 논문지 제14권 제3호-2018년 9월
http://dx.doi.org/10.17662/ksdim.2018.14.3.055

AHP를 이용한 정보보안 요소의 중요도 평가: 국방기관 정보시스템 외주개발 사례*

박 동 수** · 윤 한 성***

Assessing the Importance of Information Security Factors Using AHP: Case of Defense Agency's Outsourcing Development of Information Systems

Park Dongsoo · Yoon Hanseong

〈Abstract〉

In this paper, we identify and evaluate the information security factors considered in outsourcing development of information systems for defense agency with analytic hierarchy process(AHP). To assess the information security elements, we prepared three groups including the experts of a defense agency, subcontractor managers and subcontractor practitioners who are involved in developing information systems. And the relative importance of security factors were analyzed using questionnaires and responses. As a result of analysis of 27 security factors, factors corresponding to human and physical security as a whole were evaluated as having higher importance. Although there are some differences in the ranking of some importance according to human roles, they can be positive for the implementation of complementary information security. And administrative security and technical security can be relatively insignificant considering that they can be considered as infrastructure of the overall information environment. The result of this paper will be helpful to recognize the difference of perception of information security factors among the persons in the organization where collaboration is activated and to prepare countermeasures against them.

Key Words : Information Systems, Outsourcing, Information Security, AHP

Ⅰ. 서론

조직운영과 경영혁신의 기반으로서 역할이 확대되는 정보서비스의 요구에 대응하기 위하여, 공공기관의 경우 외주(outsourcing)를 통한 정보시스템 개발·운영이 지속적으로 증가하고 있다[1,2,3]. 공공기관의 정보시스템은 일반적으로 외주업체의 협력을

* 이 논문은 2018년도 경상대학교 경영행정대학원 최고관리자과정 연구장학재단 학술연구조성비에 의하여 연구되었음.
** 국방기술품질원 연구원 (주저자)
*** 경상대학교 경영대학 교수 (교신저자)

통해 개발되는 형태로 이루어진다.

공공기관의 경우 민간기업에 비해 정보시스템 및 정보시스템에서 처리되는 정보가 정보보안에 더욱 민감한 경우가 많다. 대표적 사례인 국내 국방기관의 정보시스템들은 다양한 비밀정보를 다루고 있으며, 이로 인해 정보시스템의 외주개발에서는 정보보안 취약요소를 확인하고 피해가 없도록 엄격히 관리된다. 예를 들어 정보보안과 관련하여 국방기관에 적용되는 제 규정[4,5,6]들은 일반 공공기관과 차별화된 강화된 정보보안 규칙을 포함하고 있다. 이러한 규칙들의 적용, 예외사항 처리에 대한 사전 검토·승인 등에 시간과 비용이 상당부분 소요되기도 한다.

정보시스템개발의 수행에는 통합관리, 스코프관리, 시간관리, 비용관리, 품질관리, 인적자원관리, 리스크관리, 커뮤니케이션관리, 획득관리 등의 관리요소가 지적되는데[7], 정보보안은 이들 요소와 모두 직·간접적으로 관련되는 포괄적인 관리대상이 된다. 이와 같은 정보보안에 대해 정보시스템개발에서 다루어야 할 정보보안 취약요소와 우선순위를 식별하고 적절한 보안대책을 구비하는 것은 전체 프로젝트 관리, 특히 국방기관의 경우에는 매우 중요한 사항이다.

본고는 정보보안이 강조되는 국내 특정 국방기관에 대해 정보시스템개발의 수행에 필요한 정보보안 요소를 식별하고 요소별 우선순위를 AHP(analytic hierarchy process)를 통해 분석하고자 한다. 이는 국방기관과 같이 정보보안이 강조되는 조직의 정보시스템 개발과정에서 정보보안의 효과적인 관리에 참고가 될 것으로 기대된다.

Ⅱ. 연구의 배경 및 범위

2.1 연구배경

국가 기밀정보를 다루는 입장에서 국방기관들의 정보시스템 개발·유지보수에는 특별한 정보보안 규칙들이 적용된다. 민간 및 공공 기관에서 정보시스템의 개발·운영 외주 관리업무의 표준으로서 대표적인 국내 자료인 '행정기관 및 공공기관 정보시스템 구축·운영 지침[8]', '소프트웨어 개발보안 가이드[9]', 'IT 아웃소싱 운영관리 매뉴얼[10]', '소프트웨어 보안약점 진단가이드[11]', 'IT외주인력 보안통제

<표 1> 정보시스템의 개발·운영 국내 기준자료

기준자료 (발간주체)	특징 및 성격	정보보안 관련성
행정기관 및 공공기관 정보시스템 구축·운영 지침[8]	정보보안보다는 외주 정보시스템 프로젝트의 관리에 필요한 지침	보안성검토 및 소프트웨어개발 보안의 일부 사항 고려
소프트웨어 개발보안 가이드[9]	정보시스템 개발단계와 동 단계에 필요한 정보보안 취약요소 고려	소프트웨어 및 보안정책 등과 관련한 보안기술 안내
IT 아웃소싱 운영관리 매뉴얼[10]	정보시스템 개발 후 운영에 초점이 맞춰진 관리 매뉴얼	외주업체 보안조직 및 절차상의 일부 보안사항을 부분적으로 고려
소프트웨어 보안약점 진단가이드[11]	전반적인 정보보안의 측면이 아니고 소프트웨어의 정보보안 취약요소에 초점	개발 중이거나 개발이 완료된 소프트웨어의 기술적 정보보안요소 확인
IT외주인력 보안통제 안내서[12]	정보시스템 외주의 모든 단계별 정보보안에 초점	외주 수행단계별로 정보보안요소(물리적·인적·관리적·기술적) 적용가이드

안내서[12]' 등의 기준자료를 활용할 수 있다. 이와 같은 5가지 자료에 대해 정보시스템의 일반적인 개발·운영 외주 단계인 '계획⇨계약⇨개발⇨운영'에서 가지는 특징과 정보보안 관련성을 확인해보면 <표 1>과 같다.

<표 1>에서 '소프트웨어 개발보안 가이드' 및 '소프트웨어 보안약점 진단가이드'의 경우 정보시스템 개발·운영에 대해 전반적인 프로젝트관리의 관점이 아니라 소프트웨어의 개발이라는 특정부분에 초점을 두고 있다. 그리고 정보보안 측면에서 '행정기관 및 공공기관 정보시스템 구축·운영 지침'은 정보보안보다는 프로젝트 수행의 일반적 사항을 규정화하고 있으며, 'IT아웃소싱 운영관리 매뉴얼'도 운영단계의 일반사항을 주로 명시하고 있다. 'IT외주인력 보안통제 안내서'는 정보보안에 초점을 맞추어 정보시스템 프로젝트의 프로젝트 외주수행 단계별, 정보보안 분야별(물리적·인적·관리적·기술적) 보안취약요소와 기본적인 대처방안을 명시하고 있다.

정보시스템 프로젝트에 대해 <표 1>의 자료들은 민간 또는 공공을 구별하지 않고 적용가능한 일반적이고 보편적인 측면이 강하다. 본고에서 대상으로 하고 있는 국내 국방기관 정보시스템의 외주개발의 정보보안 분야에 대해 특별히 적용하는 기준들은 '군사보안업무훈령[4]', '국방사이버안보훈령[5]', '국방정보화업무훈령[6]' 등으로 확인된다. '군사보안업무훈령[4]'은 국방기관들이 수행하는 전반적인 업무에 대해 정보보안 사항을 명시하여 정보보안의 핵심적인 규정이라고 할 수 있다. '국방사이버안보훈령[5]'은 국방기관이 준수해야할 전반적인 정보보안 규칙을 포함하는 규정으로 사이버안보와 관련된 침해대응과 정보시스템 운영·관리와 관련된 부분이 주로 명시되어 있다. '국방정보화업무훈령[6]'은 국방기관의 정보화시스템 구축·운영과 관련된 업무에 대해서 세부적으로 명시한 정보보안 규정이라고 할 수 있다.

2.2 연구내용 및 범위

정보시스템의 외주에 의한 개발·운영이 확산됨에 따라 관련한 정보보안 사고가 지속적으로 발생하고 있고, 이에 대한 대응책이 강조되고 있다. 구체적인 대응책을 위해서는, 정보시스템개발 프로젝트 수행을 주관하는 기관의 프로젝트 담당자와 해당 외주업체 직원의 정보보안 및 정보보안 요소에 대한 인식의 확인이 중요하다. 정보보안요소 및 정보보안요소 간의 중요도 등에 대한 인식의 상호간 공감 또는 차이는 정보보안 대응책의 선택 및 성과 등에서 차이를 초래하는 원인이 될 수 있다.

본고의 연구대상은 타 조직에 비해 보다 엄격한 정보보안이 강조되는 국방기관에서 외주를 활용한 정보시스템 프로젝트의 안정적인 수행에 필요한 보안요소를 식별하는데 있다. 식별된 보안요소의 우선순위와 주관기관인 국방기관과 외주 수행사간의 직원이 가지는 인식의 차이에 대해서도 확인하고자 한다.

2.3 연구 방법 및 관련 문헌

의사결정의 목표나 평가기준이 다수이고 복잡한 경우 체계적이고 합리적인 평가를 지원하는 계층분석적 의사결정지원기법으로 AHP(analytic hierarchy process)가 있다[13,14]. 본고에서 활용하고자 하는 AHP는 의사결정에 필요한 각종 요소들을 식별하고 계층화하여 주요인과 세부요인들을 분류한 후, 계층을 구성하는 요인들을 쌍대비교(pair-wise comparison)를 통하여 상대적인 중요도를 도출하게 된다. AHP는 정보시스템 분야에서도 폭넓게 적용되고 있는데, 정보시스템 개발 프로젝트

위험요인을 평가[15], 물류업체의 선정[19], 정보시스템 개발업체의 선정[20] 등 여러 연구사례가 확인된다. 그 외에 무기체계의 선정[21]에도 활용되는 등 다양한 활용사례가 있다.

Ⅲ. 정보보안 요소식별 및 계층모델

국내 특정 국방기관의 정보시스템개발에서 고려되는 정보보안요소의 식별과 평가를 3단계의 과정으로 수행하였다. 1단계에서는 문헌조사를 통하여 제반 정보보안요소를 확인하였다. 2단계에서는 국방기관 정보시스템분야의 전문가로 볼 수 있는 정보보안 관리자 및 정보시스템 프로젝트 관리자와 인터뷰를 통해 1단계에서 확인된 정보보안요소에 대하여 계층구조를 구성하였다. 3단계에서는 정보보안요소 계층구조의 각 계층 및 범주에 속하는 요소의 쌍대비교 설문지를 통하여 선별된 설문대상자 그룹들의 응답결과를 AHP를 통해 정보보안요소에 대한 인식을 분석하였다.

3.1 정보보안 요소의 식별

AHP의 기본단계인 주요인과 세부요인들의 계층화를 구성하기 위하여, 정보시스템 외주개발과 관련한 여러 정보보안 세부요소의 범주가 되는 최상위의 요소를 먼저 확인해보면 일반적으로 관리적 보안, 기술적 보안, 물리적 보안, 인적 보안의 네 가지 요소로 정리된다. 기관이나 연구자의 관점에 따라 <표 2>와 같이 인적 보안의 요소는 선택적으로 분류되고 있다. 국내 정보분야에서 많이 활용되는 'IT외주 인력 보안통제 안내서[12]'에서도 '보안위협'과 '보안통제 강화대책'의 양 측면에서 인적 보안을 선택적으로 고려하고 있다.

국방기관의 정보시스템 외주개발이 본 연구의 범위임을 고려하여 국방기관 정보시스템에 특별히 적용되는 제 기준[4,5,6]을 참조한 결과, 세부 정보보안 요소들의 구성에는 차이가 있으나 상위 정보보안요소의 범주로 관리적, 기술적, 물리적 보안 이외에 인적 보안을 별도로 범주로 규정하고 있다. 또한 본고의 사례에서 정보보안요소의 식별을 위해 수차례의

<표 2> 상위 범주에 포함되는 정보보안 요소의 범위

기관 또는 연구자		정보보안 요소의 범주			
		관리적 보안	기술적 보안	물리적 보안	인적 보안
방송통신위원회·한국인터넷진흥원(2011)[12]	보안위협영역	포함	포함	포함	미포함
	보안통제영역	포함	포함	포함	포함
손병준·김인석(2017)[16]		포함	포함	포함	미포함
이봉규(2014)[17], 이은섭·김신령·김영곤(2017)[18]		포함	포함	포함	포함

<표 3> 국방기관 정보시스템 외주개발의 정보보안 평가요소

계층-1	내용
관리적 보안	외주 수행사에 대한 정보보안상의 관리적 행위 및 규칙(절차)에 의한 정보보안
기술적 보안	정보기술 중심의 보안시스템이나 솔루션에 의존하는 정보보안
물리적 보안	정보시스템개발 수행인력의 출입통제 및 정보자료 유출방지와 관련한 정보보안
인적 보안	수행인력 및 업무조직의 행위나 의식과 관련한 정보보안

인터뷰를 수행한 10여명의 정보시스템 프로젝트수행 관리자들도 정보보안요소의 범주를 관리적, 기술적, 물리적, 인적 보안으로 정하는데 이견이 없었으며, 이들을 AHP의 상위계층인 계층-1의 정보보안요소로 두고 각각의 내용을 <표 3>과 같이 요약하였다.

국방기관의 정보시스템 외주개발에서 관리적 보안은 주로 외주업체에 대한 정보시스템개발의 주관기관의 각종 관리적 행위와 정보보안 규칙(절차)에 따른 이행의 확인과정으로 이루어진다. 기술적 보안은 주로 정보기술 중심의 보안시스템이나 솔루션에 의존하며 정보보안의 기능적인 측면에서 중요성이 확대되고 있다. 물리적 보안은 주관기관 및 외주업체의 수행인력에 대한 출입통제 및 정보자료 유출방지 등에 의해 이루어진다. 인적 보안은 해당 프로젝트 수행인력 및 업무조직, 즉 사람이나 조직의 행위나 의식으로 인하여 발생할 수 있는 정보보안 사고를 방지하는 것과 관련된 요소이다.

3.1.1 관리적 보안의 하부요소

관리적 보안은 정보보안을 위해 이루어지는 계획, 조직, 통제 등의 각종 관리적 행위를 의미하는 정보보안 요소이다. 본고에서 정리할 국방기관의 사례에서는 관리적 보안요소의 계층-2에 해당하는 하부요소로서 <표 4>와 같이 '진행관리'와 '보안규칙'으로 구성하고, 각 요소의 계층-3에 해당하는 세부 평가요소를 선정하였다.

진행관리는 정보시스템 개발의 외주업체 직원을 대상으로 진행되는 정보시스템 개발행위의 모니터링 및 관리를 통한 정보보안요소이다. 진행관리의 세부요소로서는 개발이 진행되는 정보시스템에 대해 외주 수행사 직원들의 사용자계정 관리 및 로그(log) 확인 등에 의한 작업내역 관리, 반출·입 자료 통제, 제공자료 회수 등을 선정하였다.

보안규칙은 정보시스템개발 수행상의 정보보안대책 및 정보시스템 결과물에 대해 보안기관이 정한 규칙에 의한 정보보안 검증과정에 관한 정보보안요소이다. 보안규칙의 세부요소로서는 개발수행 전 이루어지는 보안대책 수립 및 수립된 보안대책에 대한 보안기관의 확인이 필요한 보안대책, 개발완료 후 정보시스템 결과물에 대한 보안기관의 보안성 평가 및 검증이 이루어지는 보안검증 등을 선정하였다.

<표 4> 관리적 보안의 세부 평가요소

계층-2	계층-3	내용
진행관리	계정관리	정보시스템개발 수행직원의 사용자 계정 관리
	로그확인	정보시스템개발 수행직원의 작업기록 관찰 및 확인
	반출·입 자료통제	인쇄자료 및 디지털자료 반출·입의 기준에 따른 관찰 및 허용
	제공자료 회수	외주 수행사에 제공한 각종 자료의 회수
보안규칙	보안대책	프로젝트 수행 전 보안대책의 수립 및 상위 보안기관의 확인
	보안검증	프로젝트 완료직후 결과물에 대해 상위 보안기관의 보안성 평가

3.1.2 기술적 보안의 하부요소

기술적 보안은 다양한 기술을 통하여 정보보안 사고예방, 복구나 사후처리 등이 이루어지는 정보보안의 범위를 의미한다. 기술적 보안의 구현은 주로 정보보안 시스템이나 솔루션에 의존하게 되는데 네트워크 보안, 악성코드 보안, 디지털 콘텐츠 접근통제, 디지털 자료의 암·복호화 등과 관련된다. 본고의 사례에서는 기술적 보안요소의 계층-2에 해당하는 하부요소로서 <표 5>와 같이 '네트워크보호', '데이터보호' 및 '접근권한 통제'로 구성하고, 각 요소의 계층-3에 해당하는 세부요소를 선정하였다.

<표 5> 기술적 보안의 세부 평가요소

계층-2	계층-3	내용
네트워크 보호	유선네트워크 통제	정보시스템개발 수행직원의 유선 네트워크 접속허가 및 통제
	무선네트워크 통제	정보시스템개발 수행직원의 무선 네트워크 접속허가 및 통제
	네트워크분리 운영	네트워크 분리 및 차단을 통한 내부 정보자원 보호
데이터 보호	악성코드 관리	디지털 콘텐츠 및 데이터로부터 악성코드 차단 및 제거
	전자자료 유출방지	내부 디지털 콘텐츠 및 데이터의 외부유출 방지
	비인가 사이트 접속차단	내·외부 인터넷 사이트 접속의 인가 및 통제
접근권한 통제	시스템 접근제어	정보시스템·기능모듈별 개인별 접속권한 통제
	원격접속 통제	정보시스템·기능모듈별 원격접속 여부·접속권한 통제

네트워크보호는 네트워크상의 트래픽과 관련하여 발생하는 정보보안 사고에 대응하기 위한 정보보안 요소를 포함한다. 네트워크 보안의 세부 평가요소로는 외주업체 직원의 유·무선 네트워크 접속권한의 통제, 그리고 외부 네트워크와의 차단을 통한 정보보안 수단인 네트워크 분리운영 등을 선정하였다.

데이터보호는 조직의 데이터를 안전하게 보호하는 측면의 정보보안이며, 본고에서는 정보시스템 개발과 사용되는 데이터 자체의 완전성(integrity)이나 불법유출로부터 보호하는 측면이 중요하게 판단되었다. 사용자에 의한 데이터훼손 등은 관리적 보안의 진행관리 요소에서 통제가 가능한 것으로 고려되었다. 데이터 보안의 세부 평가요소로서 디지털 콘텐츠나 데이터에 보안위협이 되는 악성코드의 관리, 각종 저장매체의 차단과 전송통제를 통한 전자자료 유출방지, 사용자의 외부접속으로부터 내부 데이터 보호를 위한 비인가 인터넷사이트의 접속차단 등을 선정하였다.

접근권한통제는 정보시스템개발에 필요한 정보시스템 및 기능모듈의 접속을 통제하여 보안침해를 최소화하는 요소이다. 주어진 개발공간에서의 시스템 접속은 물론 외부에서 원격접속이 필요한 경우에도 적절한 접근권한 통제가 필요하다.

3.1.3 물리적 보안의 하부요소

물리적 보안요소는 물리적으로 발생가능한 각종 정보보안 침해요소에 대응하는 정보보안 요소이다. 본고에서는 주로 정보시스템 개발공간에서 발생할 수 있는 물리적 정보보안 침해요소를 고려하였다. 물리적 보안요소의 계층-2에 해당하는 하부요소로서 물리적인 자료유출 방지, 물리적 이동이 가능한 매체의 통제에 의한 정보자료 보안, 개발공간의 개발인력 출입관리를 선정하였다. 물리적 보안요소의 계층-2에 해당하는 하부요소 및 각 하부요소에 대한 계층-3의 세부요소를 요약하면 <표 6>과 같다.

자료유출방지에서는 디지털 매체의 저장자료 및 인쇄자료의 엄격한 자료보관관리, 복사 또는 프린터를 통한 자료출력 및 출력자료의 통제를 위한 출력자료관리 등을 세부요소로 선정하였다. 매체통제는 개발실 출입인원의 휴대용 매체를 통한 촬영 및 녹음의 통제, 그리고 장비 반입·출 통제 등을 세부요소로 선정하였다. 출입관리는 개발실의 인원출입을 통제하는 출입권한관리, 출입인원의 모니터링을 통해 실시간 또는 사후적 정보보안 대응을 위한 출입 모니터링 등을 세부요소로 선정하였다.

<표 6> 물리적 보안의 세부 평가요소

계층-2	계층-3	내용
자료 유출 방지	자료보관 관리	디지털매체의 저장자료 및 인쇄자료의 저장체계·열람권한 관리
	출력자료 관리	프린터출력·자료복사의 엄격한 관리, 출력물 유통의 통제·관리
매체 통제	촬영통제	고정식 및 이동식 촬영기기의 설치·활용 및 기능의 통제
	녹음통제	개인용 녹음기기의 휴대 및 기능의 통제
	장비 반입·출 통제	장비 및 장비의 기능·저장자료 반입·출 통제
출입 관리	출입권한 관리	개인별 출입증 및 출입허용 공간 등 출입권한 관리 및 통제
	출입 모니터링	개인별 실시간 출입여부 파악 및 출입기록 유지

3.1.4 인적 보안의 하부요소

인적 보안요소는 광범위하게 사람으로 인하여 발생할 수 있는 모든 정보보안 침해와 관련된 정보보안 요소를 의미한다. 인적 보안요소의 계층-2에 해당하는 하부요소로서 인적 정보보안 침해를 사전에 예방하는 측면의 사전예방, 그리고 정보시스템개발 수행인력의 철저한 파악 및 인원별 비밀취급 권한을 관리하는 신원관리로 선정하였다. 인적 보안요소의 계층-2에 해당하는 하부요소 및 각 하부요소에 대한 계층-3의 세부 평가요소를 요약하면 <표 7>과 같다.

사전예방의 세부요소로서는 정보시스템개발 수행인력에 대해 정보보안 환경·규칙 및 제반 준수사항 등에 관한 보안교육, 제반 정보보안규칙의 수칙 여부 점검 및 보완을 위한 보안점검, 수행인력별 정보보안규칙의 준수와 벌칙에 관한 서약서집행 등을 선정하였다. 그리고 신원관리에서는 수행조직 및 수행인력의 유지·모니터링을 위한 수행인원관리, 수행인력별 정보열람 및 시스템접속 차단의 기준이 되는 비밀취급인가, 수행인력의 신원을 주기적으로 파악·유지하는 신원조사 등으로 세부 평가요소를 선정하였다.

<그림 1> 국방기관 정보시스템 외주개발 수행의 정보보안요소 계층모델

<표 7> 인적 보안의 세부 평가요소

계층-2	계층-3	내용
사전 예방	보안교육	보안 환경·규칙 및 준수사항 등에 관한 개발수행인력 교육
	보안점검	제반 정보보안규칙의 수칙여부 점검 및 보완
	서약서 집행	수행인력의 정보보안규칙 준수 ·벌칙에 관한 서약서 관리·집행
신원 관리	수행인원 관리	수행조직 및 수행인력의 유지 및 모니터링
	비밀취급 인가	수행인력의 정보열람 및 시스템 접속차단 기준수립 및 집행관리
	신원조사	수행인력별 신원의 주기적 파악 및 유지

3.2 정보보안 요소의 계층구조

식별된 정보보안요소의 중요도 평가를 위하여 3개의 계층을 가지는 계층구조를 <그림 1>과 같이 구성하였다. 본고의 범위가 국방기관의 정보시스템 분야임을 고려할 때, 계층-3에 포함되는 정보보안요소들은 국가기관에서 정한 '군사보안업무훈령'에서 명시한 필수 보안요소를 거의 포함하고 있다.

Ⅳ. 분석결과

4.1 설문 및 설문대상자

<그림 1>의 정보보안요소의 계층모델에 대한 요소별 상대적 중요도의 평가를 위해, 각 요소의 요약된 설명과 함께 Saaty[13]가 제안한 9점 척도의 설문지를 구성하였다. 설문대상자로는 본고에서 다루는 정보시스템 외주개발을 잘 이해하고 몰입하는 업무종사자로서, 업무영역별로 대표적인 다음의 세 그룹을 선정하였다.

- 국방기관 전문가: 해당 국방기관 소속의 정보시스템 외주개발 전문가로서 정보시스템개발 프로젝트관리 업무를 수행하며 진행관리, 기술·보안 점검, 검수·인도 등 수행
- 외주업체 관리자: 해당 국방기관의 정보시스템 외주개발 관리전문가로서 발주기관의 요구사항 및 업무기준에 따라 해당 정보시스템 개발의 진행을 지휘 및 관리
- 외주업체 실무자: 해당 국방기관의 정보시스템 외주개발 실무수행자로서 외주업체 관리자의 지휘에 따라 해당 정보시스템의 개발업무의 실무를 수행

AHP에서는 설문대상자의 수보다 설문목적에 부합하는 설문대상자의 선정이 중요한 것으로 지적된다[19]. 이전 연구의 사례를 보면 정보시스템 개발업체의 선정[20], 최적 웹사이트 선정[22], 통신업체의 선정[23] 등에서 각각 7명, 10명, 5명의 설문대상자를 통해 AHP를 진행하였다. 본고에서는 위 3그룹에 대하여 전문지식을 갖추고 업무숙련도가 높게 평가되는 각 10명을 설문대상자로 선정하여 2017년 9월 동안 AHP설문지의 응답을 얻었다.

4.2 분석 및 결과

설문의 응답결과로부터 구한 일관성비율(consistency ration: CR)은 AHP분석에서 응답자가 일관성을 가지고 평가했는지를 판단하여 설문의 신뢰성을 확인하는 수치이다. 일관성비율의 값이 일반적으로 0.2 정도로 관측될 경우 응답의 논리적 일관성을 인정되고 0.1보다 작으면 응답자들의 논리적 일관성이 매우 높은 상황으로 간주된다[13]. 본고에서 일부 설문대상자의 설문결과에서 일관성비율이 0.2 이상이 되어 피드백과정을 거쳤으며, 최종 설문결과의 일관성비율은 모두 0.1 이하로서 평가기준보다 응답의 논리적 일관성이 대단히 높게 측정되었다. 따라서 국방기관의 정보시스템 외주개발

에 따른 정보보안 요소의 중요도를 산정함에 있어 설문대상자 그룹이 제시된 요인들을 잘 이해하고 있으며 일관된 관점에서 설문에 응답하였다고 추론할 수 있다.

4.2.1 계층-1의 정보보안 요소 중요도 분석

외주업체를 통한 정보시스템 개발이 기본적으로 다른 조직과의 협업으로 이루어지고 또 소속이 다른 인력과 업무상 상호신뢰가 중요하다는 면에서 <표 8>과 같이 인적 보안의 요소가 가장 중요하게 평가되었다. 그리고 별도의 정보시스템 개발공간을 중심으로 이루어지는 개발업무의 성격상 물리적 보안이 다음으로 중요하게 평가되었다. 다음으로는 지속적으로 발전하는 기술적 보안요소가 중요하게 평가되고 있으나, 실무적으로 기술적 보안에 더 익숙한 외주업체 실무자에게는 관리적 보안이 더 중요하게 평가되었다.

4.2.2 계층-2의 정보보안 요소 중요도 분석

계층-2의 요소에 대해서는 <표 9>와 같이 평가되었다. 관리적 보안에서는 구성원의 정보보안 규정이나 절차의 수립과 이의 준수, 그리고 정보시스템개발 결과물에 대한 보안성의 평가와 같은 보안규칙이 중요하게 평가되었다. 보안규칙이 관리자의 입장에

<표 8> 계층-1 요소의 응답자 그룹별 중요도 평가

계층-1	전체 설문대상자		국방기관 전문가		외주업체 관리자		외주업체 실무자	
	중요도	순위	중요도	순위	중요도	순위	중요도	순위
관리적 보안	0.120	4	0.121	4	0.099	4	0.145	3
기술적 보안	0.143	3	0.165	3	0.140	3	0.126	4
물리적 보안	0.320	2	0.334	2	0.289	2	0.337	2
인적 보안	0.417	1	0.381	1	0.471	1	0.392	1
CR	0.012		0.023		0.090		0.039	

<표 9> 계층-2 요소의 응답자 그룹별 중요도 평가

계층-1	계층-2	전체 설문대상자		국방기관 전문가		외주업체 관리자		외주업체 실무자	
		중요도 (전체)	순위 (전체)	중요도 (전체)	순위 (전체)	중요도 (전체)	순위 (전체)	중요도 (전체)	순위 (전체)
관리적 보안	진행관리	0.391(0.047)	2(8)	0.202(0.024)	2(10)	0.374(0.037)	2(8)	0.636(0.092)	1(5)
	보안규칙	0.609(0.073)	1(7)	0.798(0.097)	1(4)	0.626(0.062)	1(6)	0.364(0.053)	2(8)
기술적 보안	네트워크보호	0.133(0.019)	3(10)	0.172(0.028)	3(9)	0.096(0.013)	3(10)	0.131(0.017)	2(9)
	데이터보호	0.238(0.034)	2(9)	0.363(0.060)	2(8)	0.263(0.037)	2(9)	0.128(0.016)	3(10)
	접근권한통제	0.629(0.090)	1(5)	0.465(0.077)	1(6)	0.641(0.090)	1(4)	0.741(0.093)	1(4)
물리적 보안	자료유출방지	0.367(0.117)	1(3)	0.191(0.064)	3(7)	0.560(0.162)	1(2)	0.358(0.121)	2(3)
	매체통제	0.354(0.113)	2(4)	0.283(0.095)	2(5)	0.265(0.077)	2(5)	0.455(0.153)	1(2)
	출입관리	0.279(0.089)	3(6)	0.526(0.176)	1(2)	0.174(0.050)	3(7)	0.187(0.063)	3(6)
인적 보안	사전예방	0.545(0.227)	1(1)	0.381(0.145)	2(3)	0.342(0.161)	2(3)	0.843(0.330)	1(1)
	신원관리	0.455(0.190)	2(2)	0.619(0.236)	1(1)	0.658(0.310)	1(1)	0.157(0.062)	2(7)

서 중요한 관리적 보안요소이지만, 개발실무자 입장에서는 개발의 제반 업무를 규칙에 따라 진행하고 점검받는 진행관리 요소가 더 중요하게 평가되었다.

기술적 보안에서는 정보시스템 개발에서 빈번하게 이루어지는 필요한 정보시스템의 기능모듈 또는 타 정보시스템에 대한 접속통제, 그리고 외부에서의 원격접속 통제를 의미하는 접근권한통제가 가장 중요하게 평가되었다. 국방기관 전문가 및 외주업체 관리자는 네트워크보호에 비해 조직 내부의 데이터에 대해 유출방지 또는 완전성 유지를 의미하는 데이터보호를 더 중요시 하였으나, 외주업체 실무자는 원격으로 시스템이나 데이터접근을 차단하는 네트워크보호를 더 중요시하는 경향을 나타내었다.

물리적 보안에서는 설문대상자 그룹별로 중요도가 다양하게 평가되었다. 전반적으로 표면적인 통제를 중요하게 고려하는 국방기관 전문가 그룹은 출입관리 요소를, 물리적 보안의 실질적 피해 및 사후책임을 중요시 하는 외주업체 관리자 그룹은 자료유출방지 요소를, 실제 개발기기 또는 스마트폰 등의 장비 반출·입이나 통제에 민감한 외주업체 실무자 그룹은 매체통제 요소를 각각 가장 중요하게 평가하였다. 전체적으로 3가지 요소는 큰 차이는 아니지만 자료유출방지 요소가 좀 더 중요하게 평가되었다.

인적 보안에서는 국방기관 전문가 및 외주기관 관리자 그룹이 동일하게 수행인력의 파악과 권한관리를 포함하는 신원관리를 중요시 하였다. 반면, 외주기관 실무자 그룹에서는 실무자를 대상으로 하는 서약서 집행이나 보안교육, 정보보안 점검 등의 사전예방을 훨씬 높은 비율로 중요시하고 있었다. 전체적으로도 사전예방이 신원관리에 비해 중요하게 평가되는 것으로 나타났다.

4.2.3 계층-3의 정보보안 요소 중요도 분석

계층-3의 요소에 대한 중요도 분석결과를 전체 중요도와 같이 <표 10>에서 정리하였으며, 계층-2의 요소별로 가장 높은 중요도를 가지는 계층-3의 요소에 대해 음영으로 표시하였다. 모든 설문대상자 그룹이 다음에 속하는 계층-3의 요소에 대해 동일한 순위로 중요도를 평가하였는데, 이는 주어진 공간에서 개발이 이루어지는 측면과 관련 시스템에 대한 일관된 접근권한 통제로 인해 해당 요소에서 설문대상자 그룹이 서로 동일한 중요도 순위로 평가한 것으로 보인다.

- 계층-1의 '물리적 보안'에 해당하는 계층-2의 요소
- 계층-2의 '접근권한통제' 요소

반면 다음의 계층-2에 해당하는 계층-3의 요소에 대해서는 서로 다른 순위로 중요도가 평가되었는데, 이는 인적 보안에 포함된 계층-3의 요소별로 설문대상 그룹 각각이 개발과정 중에 규칙의 적용에 차이가 있고 또 정보보안 효과에서 그룹별로 업무상에서 정보보안의 위험성을 인식하는데 차이가 있음을 보여준다.

- 계층-1의 '인적 보안'에 해당하는 계층-2의 요소
- 계층-2의 '네트워크보호' 요소

나머지 계층-3의 요소에 대해서는 관리자와 실무자, 프로젝트의 주관조직과 외주업체, 정보보안의 중요도에 대한 인식차 등에 따라 다소간 중요도의 차이를 보였다. 그리고 설문대상자 그룹별로 계층-3에서 전체 중요도가 5순위에 속하는 요소들만 나열하면 <표 11>과 같다. 모든 설문대상자 그룹에서 계층-1의 '인적 요소'에 해당하는 계층-3의 요소들이 전반적으로 상위의 중요도로 평가되었으며, 계층-1의 '물리적 요소'에 해당하는 계층-3의 요소들이 대체로 그 다음의 중요도로 인식되고 있었다. 국방기관 전문가 그룹의 경우 '인적 보안' 요소 다음으로

'물리적 보안'의 가장 기본사항으로 볼 수 있는 출입 관리 요소를 중요하다고 인식하고 있었고, 외주업체 관리자 및 실무자 그룹은 자료유출방지 및 매체통제에 속하는 요소를 중요시 하는 경향을 보였다.

<표 10> 계층-3 요소의 응답자 그룹별 중요도 평가

계층-2	계층-3	전체 설문대상자	국방기관 전문가	외주업체 관리자	외주업체 실무자
		중요도(전체)	중요도(전체)	중요도(전체)	중요도(전체)
진행관리	계정관리	0.127(0.006)	0.188(0.005)	0.074(0.003)	0.117(0.009)
	로그확인	0.212(0.010)	0.215(0.005)	0.170(0.008)	0.227(0.017)
	반입자료확인	0.295(0.014)	0.423(0.010)	0.234(0.011)	0.222(0.017)
	제공자료확인	0.367(0.017)	0.174(0.004)	0.522(0.023)	0.434(0.033)
보안규칙	보안대책	0.654(0.048)	0.665(0.064)	0.412(0.031)	0.830(0.036)
	보안측정	0.346(0.025)	0.335(0.032)	0.588(0.044)	0.170(0.007)
네트워크 보호	무선네트워크보호	0.394(0.007)	0.384(0.009)	0.320(0.004)	0.340(0.006)
	유선네트워크보호	0.354(0.007)	0.350(0.009)	0.601(0.008)	0.146(0.003)
	분리네트워크보호	0.252(0.005)	0.267(0.007)	0.079(0.001)	0.515(0.010)
데이터 보호	악성코드관리	0.358(0.012)	0.310(0.016)	0.334(0.013)	0.323(0.006)
	전자자료유출방지	0.362(0.012)	0.337(0.017)	0.171(0.006)	0.585(0.011)
	비인가사이트접속차단	0.280(0.010)	0.353(0.018)	0.495(0.019)	0.092(0.002)
접근권한통제	시스템접근제어	0.278(0.025)	0.345(0.023)	0.233(0.021)	0.263(0.028)
	원격접속통제	0.722(0.065)	0.655(0.043)	0.767(0.070)	0.737(0.078)
자료유출방지	자료보관관리	0.454(0.053)	0.448(0.027)	0.494(0.089)	0.420(0.048)
	출력자료관리	0.546(0.064)	0.552(0.034)	0.506(0.091)	0.580(0.066)
매체통제	촬영통제	0.311(0.035)	0.420(0.038)	0.252(0.021)	0.275(0.040)
	녹음통제	0.589(0.067)	0.460(0.042)	0.653(0.056)	0.640(0.093)
	장비반입·출통제	0.100(0.011)	0.121(0.011)	0.095(0.008)	0.085(0.012)
출입관리	출입권한관리	0.223(0.020)	0.171(0.029)	0.226(0.013)	0.282(0.017)
	출입모니터링	0.777(0.069)	0.829(0.140)	0.774(0.043)	0.718(0.043)
사전예방	보안교육	0.307(0.070)	0.460(0.073)	0.370(0.053)	0.131(0.046)
	보안점검	0.264(0.060)	0.177(0.028)	0.151(0.022)	0.522(0.183)
	서약서집행	0.429(0.098)	0.363(0.058)	0.479(0.068)	0.347(0.122)
신원관리	수행인원관리	0.237(0.045)	0.146(0.038)	0.541(0.148)	0.110(0.007)
	비밀취급인가	0.302(0.057)	0.545(0.141)	0.130(0.036)	0.255(0.017)
	신원조사	0.461(0.087)	0.309(0.080)	0.328(0.090)	0.635(0.042)

<표 11> 계층-3의 응답자 그룹별 중요 요소(5순위 이내)

순위	전체 설문대상자	국방기관 전문가	외주업체 관리자	외주업체 실무자
1	서약서집행	비밀취급인가	수행인원관리	보안점검
2	신원조사	출입모니터링	출력자료관리	서약서집행
3	보안교육	신원조사	신원조사	녹음통제
4	출입모니터링	보안교육	자료보관관리	원격접속통제
5	녹음통제	보안대책	원격접속통제	출력자료관리

4.3 분석결과를 통한 발견점

AHP결과를 통해 본고의 사례인 국방기관의 정보시스템 외주개발에서 정보보안요소에 대한 업무종사자들의 평가 및 인식에서 다음의 발견점들을 확인할 수 있었다.

첫째로 전반적으로 인적·물리적 보안요소가 전반적으로 높은 순위로 평가되고 있다. 본고의 설문대상자들이 일상 업무에서 직접 접하는 정보보안요소가 인적·물리적 요소인 반면, 관리적·기술적 보안요소는 업무기반 또는 정보기반에 내재되어 암묵적으로 작용하여 실제 업무상 인식되는 정도가 낮은데서 나타나는 결과로 이해될 수 있다.

둘째로 국방기관 전문가 및 외주업체 관리자 그룹은 인적 보안요소의 신원관리, 즉 개발인력의 신원이나 정보취급의 인가 등 인적 보안의 관리적 측면을 중요시하고 있었다. 반면, 외주업체 실무자 그룹은 실무에 따른 점검 또는 책임소재와 관련되는 서약서 등을 더 중요하게 평가하고 있었다.

셋째로 물리적 보안의 측면에서 국방기관 전문가 그룹은 출입모니터링과 같이 인력의 출입과 같이 직접적이고 가시적인 측면을 중요시하였다. 반면, 외주업체 관리자 및 실무자 그룹은 정보보안 사고에 따른 책임이 중요한 자료유출방지 또는 기술적 특성의 보완이 필요한 매체통제 등의 요소를 강조하는 측면이 있었다.

넷째로 국방기관 전문가 그룹은 인적·물리적 보안요소 다음으로 보안대책과 같은 보안규칙 요소를 중요하게 평가하고 있었다. 그런데 실제 업무실무의 입장이 강한 외주업체 관리자 및 실무자 그룹은 업무수행과 직접 관련되는 원격접속통제와 같은 기술적 보안측면을 더 중요하게 평가하고 있었다.

Ⅴ. 결론 및 토의

본고에서는 국방기관의 정보시스템 외주개발 사례에서 고려되는 정보보안요소에 대하여 계층 모델을 구성하고, 계층별 요소들에 대하여 해당 업무종사자 그룹별로 AHP로써 중요도를 평가하였다. 이를 통해 국방기관 전문가 그룹, 외주업체 관리자 그룹, 외주업체 실무자 그룹 각각의 정보보안요소 인식에 대한 공통성과 차이점을 확인할 수 있었다.

정보시스템의 외주개발에서 서로 협업을 통해 발주 및 외주를 수행하는 조직의 직원들은 상호간에 역할의 차이가 있으며, 이로 인해 필요한 정보보안요소에 대해 인식하는 중요도에도 차이가 있음을 확인하였다. 이와 같은 분석결과 및 발견점에 대해 해당 국방기관에서는 전반적으로 다음과 같이 두 가지 대응방안을 마련하기로 하였다.

첫째, 상대적으로 높게 평가되는 인적·물리적 보안요소에 대해서는 정보보안요소에 대한 개발업무 종사자간 인식의 차이를 긍정적인 상호보완적 관계로 파악하고, 분석결과에 대한 개발업무 종사자의 이해 및 필요한 교육 등을 통해 전체 정보보안수준의 시너지를 추구하기로 하였다.

둘째, 상대적으로 낮게 평가되는 관리적·기술적 보안요소에 대해서는 정보시스템 개발주관 부서 이외에 해당 국방기관의 관련 부서에서 추구해야 할 정보보안의 조직적·기술적 인프라로 인식하여 수준을 제고해 나가고, 외주개발에 필요한 정보보안 사항의 적절한 교육을 통해 개발업무 종사자의 인식수준 및 협력수준을 제고해가기로 하였다.

정보보안 및 정보보안요소의 중요도에 대한 인식은 제반 정보환경의 변화 또는 조직 구성원의 특성에 따라 변화할 수 있으며, 이에 따라 조직의 정보보안 정책이나 수단은 적절히 개선되어야 한다. 이러한 측면에서 본고의 분석은 조직구성원이나 업무

종사자의 정보보안요소 중요도에 대한 인식을 파악함으로써 정보보안 수준평가 또는 대책의 수립에 중요하게 활용될 수 있다. 이와 같은 분석은 수시 또는 정기적인 정보보안 점검에 중요한 수단이 될 수 있을 것으로 평가된다. 또한 정보시스템개발 분야의 '착수⇨계약⇨기획⇨실행관리⇨조정·통제⇨종료'와 같은 일반적인 프로젝트관리의 단계별 정보보안요소의 평가에도 활용되면, 전체 정보시스템 개발주기에 대한 정보보안 수준향상에도 도움이 될 것으로 사료된다.

참고문헌

[1] 전제만·이선규, "공공기관의 정보시스템 아웃소싱에 미치는 영향 요인과 도입 성과," 한국콘텐츠학회논문지, 제13권, 제3호, 2013, pp.339-351.

[2] 전문석·김종화·차시호·진병욱, "퍼스널 클라우드 환경에서 사용자 관리를 위한 보안 프레임워크의 설계 및 평가," 디지털산업정보학회 논문지, 제12, 제1호, 2016, pp.81-87.

[3] 김기훈·엄정호, "사이버보안 전문인력 획득을 위한 사이버보안 훈련생에 특화된훈련성과 측정 모델에 관한 연구," 디지털산업정보학회 논문지, 제12, 제4호, 2016, pp.59-69.

[4] 국방부, "군사보안 업무훈령," 2013.

[5] 국방부, "국방 사이버안보 훈령," 2015.

[6] 국방부, "국방 정보화업무 훈령," 2018.

[7] 김경환·김흥재·박용범, "CMMI와 PMBOK의 비교 분석을 통한 정량적 프로젝트 관리," 정보처리학회지, 제12권, 제4호, 2005, pp.601-608.

[8] 행정안정부, "행정기관 및 공공기관 정보시스템 구축·운영 지침," 2018.

[9] 행정안정부, 한국인터넷진흥원, "소프트웨어 개발보안 가이드," 2017.

[10] 행정안정부, 한국정보화진흥원, "IT 아웃소싱 운영 관리 매뉴얼 V2.0," 2011.

[11] 행정안정부, "소프트웨어 보안약점 진단가이드," 2013.

[12] 방송통신위원회, 한국인터넷진흥원, "IT외주인력 보안통제 안내서," 2011.

[13] Saaty, T.L., The Analytic Hierarchy Process, McGraw-Hill, 1980.

[14] Saaty, T.L., "How to make decision: The Analytic Hierarchy Process," European Journal of Operational Research, Vol. 48, No. 1, 1990, pp.9-26.

[15] 정철용·손동기, "AHP기법을 활용한 정보시스템 개발 프로젝트 위험요인 평가에 관한 탐색적 연구," 한국정보시스템학회지, 제15권, 제2호, 2006, pp.77-93.

[16] 손병준·김인석, "금융회사 대형 IT프로젝트 추진 시 외주직원에 대한 보안정책 적용 사례 연구," 한국인터넷방송통신학회논문지, 제17권, 제4호, 2017, pp.193~201.

[17] 이봉규, "IT 외주용역 보안 강화 지침 개발 및 법제화 연구," 연세대학교 산학협력단, 2014, pp.56-72.

[18] 이은섭·김신령·김영곤, "정보시스템 구축 · 운영을 위한 IT 외주용역기반 보안관리 강화에 관한 연구", 한국인터넷방송통신학회 논문지, 제17권, 제4호, 2017, pp27-34.

[19] 김대기·권오경, "제3자 물류업체 선정을 위한 평가항목 개발 및 우선순위 설정에 관한 연구," 경영과학, 제20권, 제2호, 2003, pp.151-163.

[20] 장양철·안병석, "AHP를 이용한 정보시스템 개발업체 선정에 관한 연구," 한국IT서비스학회지, 제5권, 제3호, 2006, pp.187-201.

[21] Metin, D., Serkan Y., Nevzat K., "Weapon Selection Using The AHP and TOPSIS Methods under Fuzzy Environment", Expert Systems with Applications, Vol. 36, No. 4, 2009, pp.8143-8151.

[22] 오기성, "AHP기법을 이용한 최적의 웹사이트 선정 및 품질평가에 관한 연구," 정보처리학회 논문지, 제11권, 제2호, 2004, pp.381-386.

[23] Tama M.C.Y and Tummala, V.M.R, "An Application of The AHP in Vendor Selection of A Telecommunications System," Vol. 29, No 2, 2001, pp.171-182.

■ 저자소개 ■

박 동 수
(Park Dongsoo)

현재 국방기술품질원 연구원
2018년 2월 경상대학교 대학원 경영정보학과
(경영학석사)
관심분야 : 정보시스템, 정보보안, 데이터분석 등
E-mail : manpds@naver.com

윤 한 성
(Yoon Hanseong)

2001년 3월~현재
경상대학교 경영대학 교수
1998년 8월 한국과학기술원
테크노경영대학원(공학박사)
1987년 8월 한국과학기술원 산업공학과(공학석사)
1985년 2월 서울대학교 산업공학과(공학사)

관심분야 : e비즈니스, 공급망관리, 정보보안 등
E-mail : hsyun@gnu.ac.kr

논문접수일 : 2018년 07월 04일
수 정 일 : 2018년 08월 13일
게재확정일 : 2018년 08월 17일