The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 4, pp.27-34, Aug. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.4.27
JIIBC 2017-4-4

정보시스템 구축 · 운영을 위한 IT 외주용역기반 보안관리 강화에 관한 연구

A Study on Enhancing Security Management of IT Outsourcing for Information System Establishment and Operation

이은섭*, 김신령**, 김영곤**

Eun-Sub Lee*, Sin-Ryeong Kim, Young-Kon Kim****

요 약 최근 금융기관, 기업, 공공기관의 정보화사업 및 연구개발 등 IT 관련 용역사업을 수행하는 업체와 연구소의 관리 부주의로 인해 연구자료, 기밀문서 등 주요 보안자료들이 외부로 유출되는 사례가 빈번하게 발생하고 있다. 유출 사례들은 외주용역 과정에 있어서 관련 자료를 무단으로 유출하거나 보관하는 등 정보시스템 유지보수업체의 보안관리 부실로 개인정보가 유출되어 피해를 발생시키고 있다. 이에 본 논문에서는 기업 정보화 사업 환경 조사를 통해 용역사업에 대한 유형 및 관리현황을 파악하고 외부 용역 업체를 활용한 개발 및 유지보수 수행 시 문제점을 분석·조사 하였다. 더 나아가 본 논문에서는 고려한 항목들을 설계의 바탕으로 하여 기업 활동에 집중할 수 있는 정보시스템 서비스를 제공하는 동시에 불법소프트웨어 설치 금지, 외부로부터의 바이러스, 해킹 등에 대한 침투를 원천적으로 방지할 수 있는 기업의 정보화시스템 구축을 위한 단계별 보안강화 방법론을 제시하였다.

Abstract In recent years, major security data such as research data and confidential documents have been leaked to the outside due to the carelessness of the companies and research institutes performing IT related services such as information technology projects and research and development of financial institutions, companies and public institutions is. Leakage cases are caused by leakage of personal information due to lack of security management of information system maintenance companies, such as unauthorized leakage or storage of related materials in outsourcing service process. In this paper, we analyzed the types and management status of service business through the environmental survey of corporate informatization business and analyzed the problems in development and maintenance using external service companies. Furthermore, in this paper, we provide an information system service that focuses on the business activities based on the items considered, and at the same time, it provides the informatization service for companies that can prevent infiltration of viruses and hacking from the outside. This paper presents a methodology for enhancing security for the system construction.

Key Words : Personal information, outsourcing, information systems, Information security, Privacy

Ⅰ. 서 론

정보시스템은 기업의 발전과 치열한 경쟁 환경에서 우위를 유지하는 데 매우 중대한 역할을 담당한다. 하지만 이런 중요한 정보시스템을 개발·운영함에 있어 각 기업은 여러 가지 이유로 인하여 정보시스템에 대한 구

*준회원, 한국산업기술대학교 컴퓨터공학과
**정회원, 동서울대학교 정보통신과
***정회원, 한국산업기술대학교 컴퓨터공학과(교신저자)
접수일자: 2017년 7월 10일, 수정완료: 2017년 7월 29일
게재확정일자: 2017년 8월 11일

Received: 10 July, 2017 / Revised: 29 July, 2017 /
Accepted: 11 August, 2017
***Corresponding Author: ykkim@kpu.ac.kr
Dept. of Computer Engineering, Korea Polytechnic University, korea

축 및 유지보수를 제3자에게 아웃소싱을 하고 있다. 아웃소싱 활용은 IT 기업의 성장전략에 있어 중요한 변수로 작용하고 있어 IT아웃소싱 수탁기업의 선정요인은 기업성과에 중요한 영향을 미친다고 할 수 있다.[1]

하지만 이런 형태의 서비스가 품질저하 및 보안사고 등 또 다른 문제점들을 파생시키고 있다.

1980년대 이후 본격적으로 컴퓨터가 각 기업에 보급되기 시작하면서 정보기술이 기업에서 활용되기 시작했다. 1990년대 접어들면서 컴퓨터, 정보처리기술, 그리고 통신기술의 급속한 발전에 힘입어 정보·지식사회가 빠르게 진전하면서 기업 경영환경은 급변했다. 이러한 변화에 효율적으로 대응하고 좀 더 유리한 경쟁 입지를 확보하고자 기업은 정보기술을 전략 수단으로 중요시 여기고 있다. 하지만 기업이 급변하는 경영 환경에 적응하기 위해 정보시스템을 개발하고 유지, 보수하는 데에는 적잖은 비용과 노력이 따르기 마련이다.

아웃소싱(Outsourcing)은 기업간 네트워크가 증가하면서 그 중요성이 높아지고 있다. 아웃소싱이라는 단어 자체는 외부로부터 자원을 공급받는(Sourcing)것으로써 비용절감, 위험감소, 역량구축을 이유로 이루어진다.[2]

이에 따라 우리나라의 공공기관 및 기업들은 아웃소싱을 공공기관 및 기업들이 고려해야 할 전략 이슈의 하나로 받아들이기 시작 했다.

일반적으로 외주 인력을 활용함으로써 각 기업 내 개인정보 등 민감 정보의 유출 위험이 증가하고 있으며, PC 및 노트북 등 정보기기가 통제되지 않음으로써 발생하는 다양한 보안사고의 위험성이 증가하고 있다. 이러한 위협에 효과적으로 대처하기 위해서는 현재 사용 중인 외주 인력에 대한 PC환경과는 다른 관점에서 IT 외주 인력에 대한 보안통제가 이루어질 필요가 있다. IT 외주용역의 다양한 문제점들을 극복하고, 각 기업이 경쟁 우위를 유지하기 위해서 반드시 필요한 외주용역기반의 보안 강화 방안 연구가 필요하다.[3]

본 논문에서는 보안강화를 위한 IT 외주용역형태의 업무를 분석하고 각 업무별로 봉안강화 방안을 설계함으로 기업 활동에 집중할 수 있는 정보시스템 서비스를 제공하는 동시에 개인정보 유출, 불법소프트웨어 설치, 외부로부터의 바이러스, 해킹 등에 대한 침투를 원천적으로 방지할 수 있는 기업의 정보화시스템 구축에 대하여 고찰하였다.

II. IT 외주용역 및 보안사고

1. IT 외주용역

IT 외주용역은 정보시스템에 관련된 업무를 외부업체에 위탁하는 경영수단의 하나로써 대표적인 방식으로는 아웃소싱이 있다.

정보시스템(IT)의 아웃소싱이란 조직이 전략·전술적 목표를 가지고 정보시스템의 일부 또는 전부를 외부 전문사업자에게 위탁하는 전문서비스의 일종으로서, 정보시스템의 개발, 설계, 시공, 운영은 물론 시스템 구축을 위한 컨설팅, 교육 등의 서비스를 제공하는 장·단기 계약이라고 정의하고 있다.[4]

국내에서는 SM과 SI가 대표적이다.

- ○SM(System Management)은 주로 데이터센터 운영과 같은 업체와 기업의 꾸준한 관계가 요구되는 경우로 이를 위해 자산이나 인력이 이관되어 업무를 수행한다.
- ○SI(System Integration)은 주로 외주용역 업체에서 자산이나 인력을 이관하지 않으며 응용 소프트웨어나 네트워크개발과 관련된 업무를 수행한다.

좀 더 세분화된 IT 외주용역의 유형은 표 1과 같다.

표 1. IT 외주용역 유형
Table 1. IT outsourcing service type

IT 외부용역 유형		용 역 특 성				
		접근 IT자원		자원 사용 권한		접근 경로
유형 1	운영 용역	내부데이터	○	읽기	○	온라인
		IT시스템	○	쓰기	○	
유형 2	유지보수용역	내부데이터	○	읽기 (내부직원동행)	X (○)	온라인
		IT시스템	○	쓰기 (내부직원동행)	X (○)	
유형 3	SI 용역	내부데이터	○	읽기	○	온라인
		IT시스템	○	쓰기	X	
유형 4	데이터 처리 용역	내부데이터	○	읽기	○	온라인
		IT시스템	X	쓰기	X	
유형 5	오프라인지원	내부데이터	○	읽기	○	오프라인
		IT시스템	X	쓰기	X	

가. 운영용역

기업 내의 IT자원을 전담 운영하는 외주용역 유형으로서 기업 내의 모든 IT 시스템 및 내부 데이터에 온라인으로 접근할 수 있다. IT 외주용역 중 가능 높은 권한을 부여받는 유형으로서 모든 IT 자원에 읽기 및 쓰기 권한으로 접근하여 업무를 수행 할 수 있다.

이 유형에서 IT 용역 수행원은 내부직원과 동일한 권한으로 온라인상으로 자원에 접근하기 때문에 용역수행원은 NAC(Network Access Control) 에이전트가 설치된 PC를 이용하여 업무를 수행해야 한다.

나. 유지보수용역

유지보수는 크게 운영, 유지보수, 사용자 지원, 재개발로 나눌 수 있다.[5] 기업의 IT자원에 대한 유지 보수 업무를 수행하는 유형으로서 유지보수 업무 수행을 위해서는 운영용역과 같이 모든 IT자원에 대한 접근이 가능하고, 모든 업무를 수행할 수 있는 권한이 필요하다. 그러나 유지보수 업무의 경우, 외주용역 업체 내 에서 업무를 수행하거나 요청에 의해 단기간 동안만 작업을 할 수 있기 때문에 높은 권한을 부여할 수 없다. 따라서 용역 수행원은 IT자원 사용에 대한 모든 권한을 부여 받지는 못하고, 업무수행 시에는 기업의 내부직원과 동행함으로써 필요한 권한을 획득하게 하였다.

다. SI(소프트웨어개발) 용역

SI는 프로젝트 개발에 투입된 비용(Cost)과 일정(Time)으로 고객이 원하는 제품을 개발 완료하고 이를 통해 고객은 투자이익률 (ROI, Return-OnInvestment)을, 개발자는 개발 이익 (Profit)을 얻을 수 있어야 한다.[6]

기업의 IT자원을 구축하는 업무를 수행하는 용역 유형으로서 현재 기업의 IT환경에 적합한 시스템을 구축하기 위해서는 모든 IT자원에 접근할 수 있어야 한다. 그러나 개발용역 수행 중, 내부 데이터를 수정 또는 삭제하는 등의 오류를 범하는 것을 예방하기 위하여 쓰기 권한을 부여하지 않는다. 대신, 외주용역 수행원은 모든 IT 시스템 및 내부 데이터에 접근하여 읽기 권한을 통해 원하는 정보를 획득할 수 있기 때문에 내부 데이터의 복사본을 이용하여 개발된 시스템의 검증을 수행할 수 있다. SI 용역 유형은 개발 및 구축단계에서 발생할 수 있는 기업의 정보유출을 방지하기 위하여 기업에서 정한 보안 요구사항 및 보안대책을 반영하여 업무를 수행하여야 한다.

라. 데이터처리 용역

기업의 내부 데이터를 활용하여 업무를 수행하는 용역 유형으로서 기업의 콜센터 또는 헬프 데스크가 이 유형에 속하였다. 유형 1, 2, 3과 달리 IT 시스템에 대한 접근은 불가능하고, 온라인 접속을 통해 내부 데이터에 접근할 수 있다. 단, 내부 데이터의 수정 및 삭제를 방지하기 위하여“읽기 권한”만 부여 받게 된다. 기업의 IT자원에 대한 로그를 유지하고, 관리하는 데이터보안 용역업체 또한 이 유형에 속한다.

마. 오프라인지원

데이터처리용역과 같이 기업의 내부 데이터를 활용하여 업무를 수행하지만 오프라인으로만 접근 가능하다는 특성을 갖는다. 따라서 오프라인으로 출력된 산출물을 관리하는 용역업체가 이 유형에 해당되고, 출력된 내부 데이터에 대해 “읽기 권한”을 부여받아 면담 및 상담을 통해 컨설팅을 수행하는 회계 또는 보안컨설팅 등도 이 유형에 속할 수 있다

2. 보안사고

일반적으로 기업 보안사고의 유형은 제품의 취약점 때문에 발생하는 제품 보안사고, 기업이 운영하는 고객서비스 또는 사내 인프라가 해킹되는 침해사고, 기밀문서나 고객정보가 유출되는 정보유출사고 등으로 분류할 수 있다.[7]

최근 국가 혹은 공공기관의 정보화사업 및 연구개발 등 IT관련 용역사업을 수행하는 공공기관과 기업의 관리 부주의로 인해 연구자료, 기밀문서 등 주요 보안자료들이 외부로 유출되는 사례가 빈번하게 발생하고 있다.

이러한 유출 사례들은 IT 외주용역 과정에 있어서 관련 자료를 무단으로 유출하거나 보관하는 등 정보 시스템 유지보수 업체의 보안관리 부실로 개인정보가 유출되어 피해를 발생시키고 있다.[8]

대표적인 사례로 2014년 발생한 카드 3사의 정보유출 사고로 인한 카드 해지와 재발급, 창구방문, 업무폭증 및 영업 손실 등의 총 예산손실을 최소 1천억원 이상으로 추정하고 있다.[9] 각 카드 사에 파견되어 부정사용방지 시스템 개발을 수행하면서 전산망에 접근하였으며, 외

주용역 업체 직원은 자신의 USB(Universal Serial Bus)에 고객정보를 복사하여 1억 400만 건의 고객정보를 유출하였다.

이러한 IT 외주용역 업체를 통한 보안사고가 빈번한 환경 속에서 IT 외주용역을 통해 첨단 정보인프라를 구축하여 양질의 서비스를 제공하며 정보화 사업에서 괄목할만한 성장을 거듭하고 있는 기업 역시 내·외의 수많은 정보보안 위협으로부터 대응 방안을 모색하지 않을 수 없게 되었다.

외주용역으로 인한 대표적인 보안사고 사례는 표 2와 같다.

표 2. 외주용역 보안사고 사례
Table 2. Outsourcing Services Security Case

사례	사고 개요/원인
사례1	○사고개요 -포털게임 업체 A사의 고객 정보관련 DB업무를 위탁관리하고 있는 외주용역 업체 직원이 업무 외의 목적으로 고객정보를 무단으로 열람하고 조작 및 로그 등을 삭제하는 행위를 함 -해당직원은 DB접근 권한을 이용하여 수백 명에 달하는 회원들의 게임머니를 조작하고 로그를 삭제하여 1억 원 상당의 부당이득을 얻음 ○사고원인 -고객정보를 다루는 외주업체 직원의 보안인식 미흡 및 외주용역 직원의 행위에 대한 감사기능 미비
사례2	○사고개요 -OO社유지보수담당 직원이 9개 정부부처 정보화사업 자료를 OO기관의 유지보수 프로젝트에 활용키 위해 자택PC에 보관 -해당 자료들이 공유폴더로 설정된 폴더에 저장되어 있어 P2P에 접속하자 자택PC에 저장되어있던 자료들이 노출됨 ○사고원인 -기밀자료에 대한 무단 반출 및 P2P 공유 프로그램 사용으로 자료 유출 -기밀자료에 대한 접근통제, 보안관리 강화 및 외주용역 직원에 대한 보안 교육 미흡
사례3	○사고개요 -OO부처 정보화사업을 담당하는 하도급업체 직원이 네트워크 구성도, IP할당내역 등 전산망 이전 관련 자료를 웹하드에 보관 -인터넷 웹하드의 비밀번호를 설정하지 않아 해당 웹하드 가입자들이 제한없이 자료에 대한 검색은 물론 다운로드 가능하여 정보 유출 ○사고원인
	-외주용역 직원이 기업 핵심정보를 인가받지 않은 방식으로 관리
사례4	○사고개요 -해커는 외주업체가 운영관리하는 국내 포털사이트의 고객상담 관리시스템을 해킹 후 이를 볼모로 금품을 요구 -고객상담 관리를 맡은 외주업체는 적절한 보안시스템을 구축하지 않아 시스템이 외부 IP에서의 접근이 가능하였고, 이를 이용해 고객상담 관리자의 아이디와 비밀번호를 알아내 관리자 페이지에 접근 ○사고원인 -외주업체의 보안관리 감독 미흡지 않은 방식으로 관리

Ⅲ. 3장 외주용역 단계별 보안강화 지침

외주용역에 따른 보안사고 발생 문제점을 해결하고자 보안강화 방안을 크게 1.입찰 및 계약 단계, 2.개발 및 구축 단계, 3.사업완료단계, 4.운영 및 유지보수 단계로 구분하여 강화 방안 지침을 작성하였다.

1. 입찰 및 계약 단계

IT 외주용역 선정 및 계약 단계는 용역 환경에 대한 사업계획서 작성 단계에서부터 사전 보안 요구사항 도출 및 계약서에 보안대책을 반영한다.

가. 보안 요구 기준 마련

○외주용역과 관련된 정보 및 시스템에 대한 보안 위험을 파악하고, 적절한 통제 방안을 구상한다.

○입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 사항에 대하여 관련법령 및 자체 규정이 정하는 바에 따라 등급을 분류하고 필요한 보안요구기준을 마련한다.

○입찰 공고 시에 용역사업 관련 기밀유지 의무 및 위반 시 불이익 등의 내용을 사전 고지한다.

○제안서의 평가요소에 문서·시설·장비 등 보안관리 계획에 대한 평가항목 및 배점기준 마련한다.

○외주업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정 시 이를 반영한다.

○사업추진에 적용되는 법□ 제도, 정책, 지침의 정보

보호 요구사항 분석한다.

나. 보안을 고려한 계약 체결

○용역사업 자체 또는 투입되는 자료・장비 등에 대한 대외보안이 필요한 경우 보안의 범위 및 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서를 작성한다.

○비밀유지계약서에는 비밀정보의 범위, 보안 준수사항, 위반 시 손해배상책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시한다.

○발주업체의 요구사항을 사업자에게 명확히 전달하기 위해 작성하는 과업지시서에 자료 보안관리 방법, 인원・장비・시설 등에 대한 보안점검・교육 등 보안관련 제반사항을 상세히 기술한다.

2. 개발 및 구축단계

IT 외주용역 과정 중에 발생할 수 있는 정보 유출 등 보안 위협 요소에 대한 보안 요구사항 도출 및 보안대책을 반영하고 한다.

가. 자료에 대한 보안관리

○네트워크 구성도, IP현황, 개인정보 등 용역업체에 제공하는 비공개자료는 자료 관리대장을 작성하여 인계자(보안 책임자)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계・인수 한다.

○용역사업 관련 자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고 전자우편을 이용해 자료전송이 필요한 경우 자체 전자우편을 이용, 첨부자료는 암호화 후 수/발신한다.(단, 대외비 이상의 비밀은 전자우편으로 수・발신 금지)

○용역사업 수행으로 생산되는 산출물 및 기록은 보안책임자가 인가하지 않은 비인가자에게 제공・대여・열람을 금지한다.

나. 사무실・장비에 대한 보안관리

○용역사업 수행 장소는 발주업체가 시건장치와 통제가 가능한 공간을 제공하거나 협의를 통해 동일한 환경이 구축된 외부 사무실을 사용한다.

○발주업체 사무실에서 용역사업을 수행할 경우 용역 참여직원이 노트북등 관련 장비를 반출 또는 반입시 악성코드 감염여부 및 자료 무단반출 여부를 확인한다.

○인가받지 않은 USB 등의 보조기억매체 사용을 금지하며 산출물 저장을 위해 보조기억매체가 필요한 경우 보안책임자의 관리 하에 사용한다.

다. 내외부망 접근 시 보안관리

○사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여한다.

○보안책임자는 서버 및 장비 운영자로 하여금 내부 서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상 유무를 보고한다.

○용역업체에서 사용하는 노트북PC는 인터넷 연결을 금지, 다만 사업 수행상 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 보안책임자는 필요성이 인정될 경우 접속할 노트북을 지정하고 필요한 사이트에만 접속토록 방화벽 등을 통해 통제 후 사용한다.

라. 외주인력 신원확인

○용역사업 참여인원에 대해서는 각 개인의 친필 서명이 들어간 보안서약서를 징구한다.

○용역사업 수행 전 참여인원에 대해 법적 또는 발주업체 규정에 의한 비밀유지 의무 준수 및 위반 시 처벌 내용 등에 대한 보안교육을 실시한다.

3. 사업 완료 단계

IT 외주용역 사업 완료 시 발생 하는 보안 위협 요소에 대한 보안요구사항 도출 및 보안대책을 반영하고, 사업 완료 시 최종결과물 및 사업 중 사용된 장비, 자료의 외부 유출을 방지하기 위하여 자료의 수거 및 처리 방법에 대한 대책을 마련한다.

가. 사업완료 시 보안 대책

○사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성・관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.

○용역업체에 제공한 제반자료, 장비, 서류와 중간・최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도보관을 금지한다.

○노트북・보조기억매체 등 전자적으로 기록된 자료는 표 3의 '정보시스템 저장매체 불용처리 지침'에 따라 보안조치 한다.

표 3. 정보시스템 저장매체 불용처리 지침
Table 3. Information System Storage Media Insolvency Guidelines

구분	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크	㉮	㉮	㉮
자기 테이프	㉮, ㉯ 중 택일	㉮, ㉯ 중 택일	㉮, ㉯ 중 택일
반도체메모리 (EEPROM 등)	㉮, ㉰ 중 택일	㉮, ㉰ 중 택일	㉮, ㉰ 중 택일
	완전포맷이 되지 않는 저장매체는 ㉮방법 사용		
하드디스크	㉱	㉮, ㉯, ㉰	㉮, ㉯

㉮ 완전파괴(소각. 파쇄. 용해)
비밀이 저장된 플로피디스켓. 광디스크 파쇄시에는 파쇄조각의 크기가0.25mm 이하가 되도록 조치
㉯ 전용 소자장비 이용 저장자료 삭제
소자장비는 반드시 저장매체의 자기력보다 큰 자기력 보유
㉰ 완전포맷 3회 수행
저장매체 전체를 '난수'. '0'. '1'로 각각 중복 저장하는 방식으로 삭제
㉱ 완전포맷 1회 수행
저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

4. 유지 보수 단계

IT 외주용역을 통한 유지 보수 단계에서 발생할 수 있는 위협 요소에 대한 보안 요구사항 도출 및 보안대책을 반영하고 정보시스템 운영위탁 및 유지보수 단계에서 발생할 수 있는 시스템 불법 접근 등에 대한 대책마련과 접근방법에 대한 대책을 마련한다.

가. 정보시스템 위탁 운영 시 보안 대책

○위탁업체에게 정보시스템을 위탁하여 운영할 때에 위탁업체에게 다음 사항이 포함된 정보시스템 위탁운영계획서를 제출하여 받아 사전 검토한다.
-위탁시스템에 대한 정보통신 보안 및 개인정보보호 관리 실태
-기반시스템 공동 활용현황, 서비스수준협약서 준수사항 등 효율적 운영 및 서비스 개선상태
-위탁비용의 적절성
-기타 위탁계약의 이행사항 등 위탁에 따른 전반적인 사항

○위탁업체가 위탁 받아 운영하고 있는 정보시스템의 보안성 점검을 위한 다음 사항의 정기적 감사를 실시한다.
-위탁시스템에 대한 정보통신 보안 및 개인정보보호 관리 실태
-기반시스템 공동 활용현황, 서비스수준협약서 준수사항 등 효율적 운영 및 서비스 개선상태
-위탁비용의 적절성
-기타 위탁계약의 이행사항 등 위탁에 따른 전반적인 사항

Ⅳ. IT 외주인력 통제 강화 대책

외주 인력으로 인한 내부정보 유출 등 보안위협을 통제하기 위해 고려해야할 정보보호 실행지침을 크게 물리적 대책, 인적보안관리, 관리적 대책, 기술적 대책 등 4단계로 구분한다.

1. 물리적 대책

IT 외주인력이 중요정보가 보관된 장소에 대한 접근통제와 같은 물리적 대책은 표 4와 같다.

표 4. 물리적 대책
Table 4. Physical measures

구 분	세부 내용
1. 물리적 접급통제	・ 외주인력의 정보시스템, 정보보관소 접근통제 ・ 필요시 접근 유형 및 접근 사유 파악 ・ 제한구역, 접견구역, 장비출하구역 등을 구분하여 보안조치와 절차 수립
2. 출입이력 관리	・ 출입이력 관리대장 사용 ・ 접근통제의 방법과 범위 등을 문서화
3. 이동매체 반ㆍ출입 통제	・ 반·출입되는 이동매체에 대한 파악 ・ 이동매체 반ㆍ출입 과정의 문서화 ・ 반·출입되는 이동매체의 보안검사

2. 인적보안관리

IT 외주인력 통제를 위한 외주인력 신원확인 등과 같은 인적보안관리는 표 5와 같다.

표 5. 인적보안관리
Table 5. Human security management

구 분	세부 내용
1. 상주 유지보수 인력 신원확인	· 외주인력의 사전 신원확인 · 보안서약서 작성 · 보안의식 강화를 위한 보안교육 실시
2. 현장 동행·보안구역 출입관리 대장	· 외부인이 출입제한 구역에 출입할 경우 보안관리자와 동행

3. 관리적 대책

정보시스템과 연관되어 있는 인원, 조직, 기술상에 대한 전반적이고 총체적인 보안 대책으로 표 6과 같다.

표 6. 관리적 대책
Table 6. Administrative measures

구 분	세부 내용
1. 작업내역 관리	· 외주인력의 내부시스템 접근 기록 상시 감독 · 저장매체 사용 방지를 위한 조치 실시
2. 시스템 접근권한 관리	· 시스템 접근 라벨 정의 및 접근권한 개별 부여
3. 정보 시스템 관리	· PC 등과 같은 장비의 반입 전 초기화/점검 실시 · 외주인력에 대한 보안정책 수립 및 이행
4. 조직체계 정비 및 검사	· 용역업체의 보안 관리 계획 평가 · 입찰공고 이전에 투입 예상 자료·장비의 보안 요구기준 마련

4. 기술적 대책

IT 외주인력 통제를 위한 접근 통제와 저장 매체 통제 등의 기술적인 대책은 표 7과 같다.

표 7. 기술적 대책
Table 7. Technical measures

구 분	세부 내용
1. 접근관리	· 내부시스템에 접근하여 수행한 작업 등을 확인할 수 있는 접근이력 관리시스템 운영
2. 출력물 유출방지	· 비공개 자료 출력 시 출력자, 출력일시 등을 기록
3. 네트워크 제한	· 내부 운영 시스템 별 논리적 망 분리 운영 · 네트워크를 통한 통신 시 암호화 적용
4. 반·출입 매체관리	· 외주업무의 특성에 따라 반·출입매체의 제한/점검

V. 결 론

외주용역에 의한 정보유출 및 보안 사고가 급증하고 있으나, 기업의 보안시스템은 외부자 공격대응 위주로 구축하여 외주용역에 참여하고 있는 인력에 대한 적절한 기술적·관리적 보안대책 마련이 필요하다.

그러나 이러한 보안 대책을 마련하지 않아 발생하는 보안사고로 인하여 기업에 막대한 손실이 되고 있다.

본 논문에서 수행된 결과를 기업에서 적용한다면 이론적인 보고서에 그치지 않고 실제 정보화 사업 등에서 보다 효과적인 용역업체에 대한 보안성 강화에 도움이 될 것이며, 해당 결과물은 각 기업별·사업별 최적화 환경구축에 필요한 시간을 단축시키고, 구축 시 겪는 시행착오를 최소화하며 정책 변경 사항에 대해서 기술적인 대처가 가능 할 것이다. 그리고 기존 기업에서 운영 중인 정보보호시스템에서 용역업체에 대한 정보 보안을 강화하기 위하여 별도의 네트워크를 설계하고 사업비용을 투자하는 등 한시적 프로젝트 수행에 많은 예산을 배정할 수밖에 없었던 현실과 비교하여 사업 완료 후에도 다양한 측면에서 활용 가능하다는 점에서 경제적인 이득을 기대할 수 있다.

향후 이러한 보안관리 강화 방안을 활용하여 단계별 Check List를 체계화, 시스템화하여 조직의 외주용역 보안에 대한 Level을 Check 할 수 있는 프레임워크를 개발하여 외주용역기반의 보안 관리를 강화하고자 한다.

References

[1] Kil Ho Jung, 'A Study on the Performance of IT Outsourcing', 2015.12

[2] Cha Seung Ho, Yang Dong Hoon. (2011). A Study on the Effectiveness of Human Resource Outsourcing. Korean Jouranl of Business Administration, 24 (5), 2987-3006. 2011

[3] Kyung-Bae Min, Jang-Mook Kang, "Rights to Control Information and Related Security Technologies on the CyberSpace" The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), VOL. 10 No. 2, pp.135-141 2010

[4] Je-Man Jun, Seon-Gyu Yi. (2013). Influence Factors and the Introducing Outcomes over IT Outsourcing in the Government Offices. JOURNAL OF THE KOREA CONTENTS ASSOCIATION, 13(3), 339-351. 2013

[5] Byoung-Chol Lee, SungYul Rhew. (2013). The Maintenance Cost Estimation Model for Information System Maintenance Based on the Operation, Management and Service Metrics. Journal of the Korea Society of Computer and Information , 18(5), 77-85. 2013

[6] Sang-Un Lee, Myeong-Bok Choi, “A Definition and Evaluation Criteria for Software Development Success”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 12, No. 2, pp. 233-241. 2012
DOI: http://dx.doi.org/10.7236/JIWIT.2012.12.2.233

[7] Dongkun Lee and Jong In Lim. (2016). Forecast System for Security Incidents. Journal of the Institute of Electronics and Information Engineers, 53(6), 69-79. 2016

[8] Do-Hyun Choi, Mun-Seog Jun, Jung-OhPark, “A Study On Security Threat Analysis and Government Solution for Civil Service Online” The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), VOL. 14 NO. 5, pp.1-10 2014

[9] The total estimated damage due to leakage of the credit card company is 100 billion won, http://view.asiae.co.kr/news/view.htm?idxno=2014012711034390924

[10] National Intelligence Service, “Information System Storage Media Insolvency Guidelines”, 2006.3

[11] Bang, Min-Seok, Shin, Young-Jin. (2015). A comparative study on measures to secure the safety standards for privacy : Focused on the technical and management protection rules.GRI REVIEW, 17(3), 363-388. 2015

저자 소개

이 은 섭(준회원)

- 2017년 2월 : 한국산업기술대학교 컴퓨터공학과(석사)
- 2017년 3월 ~ 현재 : 한국산업기술대학교 컴퓨터공학과 박사과정

<주관심분야> : 보안, 정보보호, DB, 네트워크, 서버

김 신 령(정회원)

- 1983.2:경북대학교 전자공학과(공학사)
- 1985.2:연세대학교 본대학원 전자공학과(공학석사)
- 1990.2:연세대학교 본대학원 전자공학과(공학박사)
- 1992.2~:동서울대학교 정보통신과 부교수

<주관심분야> : 정보통신시스템, 부호화 방식, 보안>

김 영 곤(정회원)

- 1983.2:경북대학교 전자공학과(공학사)
- 1985.2:연세대학교 본대학원 전자공학과(공학석사)
- 2000.2:한국과학기술원 전산학과(공학박사)
- 1985~2007:KT 수석연구원
- 2007 ~ : 한국산업기술대학교 컴퓨터공학과 교수

<주관심분야> : 소프트웨어공학, 정보통신시스템 통합, 보안>