정 보 보 호 학 회 지
제24권 제1호, 2014. 2

ICT 아웃소싱 환경에서 보안관리 방안 연구

김 양 훈*, 문 제 욱**, 황 선 호***, 장 항 배****

요 약

대기업과 중소기업을 막론하고, 기업의 정보화는 기업의 지속가능한 발전을 위하여 필수불가결한 요소가 되어가고 있다. 또한, 기업들의 업무 프로세스는 기존의 정보화 시스템 및 신규 정보화 시스템 개발 및 보완을 통하여 전사적 단계로 진화되고 있으며, 자체적인 정보화 시스템 개발 및 운영인력을 보유하지 못하는 대다수의 기업들은 이러한 정보화 시스템 개발과 운영의 많은 부분을 기업 외부의 자원을 활용하는 아웃소싱에 위탁하여 수행하고 있다. 근래에 들어, 아웃소싱 인력을 포함한 내부자에 의한 정보유출 및 보안 사고의 규모는 매해 증가하고 있으나, 기업의 보안시스템은 해킹, 크래킹 등의 외부자 공격에 대한 방어위주로 구축되어 있다. 또한, 아웃소싱에 참여하고 있는 인력에 대한 적절한 기술적·관리적 보안체계의 수립이 미흡함으로써 발생하는 보안사고로 인하여 기업이 막대한 피해를 입는 사례가 나타나고 있다. 따라서, 아웃소싱 인력에 대한 보안수준을 향상하고 체계적인 아웃소싱 보안관리를 위한 가이드라인 수립이 필요한 시점이다. 본 연구에서는 기존의 선행연구를 조사하여 아웃소싱에 대한 보안 통제항목을 도출하고 도출된 보안 통제항목을 바탕으로 아웃소싱 보안수준을 높이기 위한 보안관리 추진방향을 제언하였다.

Ⅰ. 연구배경 및 목적

급속히 변화하는 경영환경 속에서 각 기업들이 이에 신속히 대응하기 위해서는 무엇보다 기업의 정보화가 우선적으로 고려되고 있다. 정보화 사회에서 정보기술이 융합됨에 따라 기업 내 ICT 활용 가치는 새롭게 해석되고 있다. 이에 따라, 기업은 제품의 품질 및 생산성의 향상을 통한 지속 가능한 성장을 위하여 현장에 정보화를 도입하고 있다. 이러한 ICT의 발달과 일반화는 기업의 가치창출을 위한 원동력이며 필수불가결한 요소가 되었다. 금융 및 보험업, 기술서비스업 뿐만 아니라 농림 수산업, 제조업, 건설업 등에 이르기까지 거의 모든 산업과 서비스 분야에서 ICT를 활용하고 있으며, ICT의 효율적인 활용이 산업 발전에 큰 영향을 미치게 되었다.

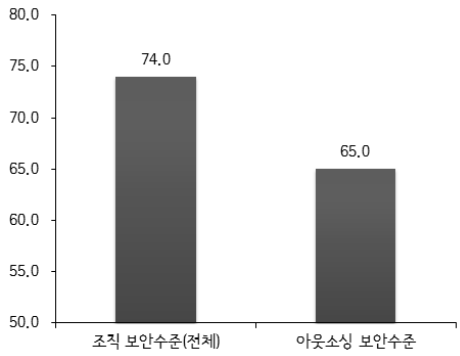
기업들이 ICT 환경을 구축 및 운영하기 위해서는 많은 인력과 기술력이 필요하다. 그러나 ICT를 주요사업으로 하고 있지 않은 대다수의 기업들은 자체의 인력과 기술력만으로 ICT 환경을 구축할 수 없기 때문에 대다수의 경우 ICT 아웃소싱 인력을 활용하고 있다[1]. 또한 ICT 부서의 운영비용이 평균적으로 매년 20%~30% 정도 증가하고 있으며, ICT의 변화속도가 너무나 급속하게 이루어지기 때문에 일반적으로 대규모의 자금이 소요되고 최신의 ICT 기술을 적시에 받아들이고 유지하는 것은 자체 기업 자체 전산부서로는 불가능하고, 이로 인하여 ICT 아웃소싱 인력의 활용이 증가하고 있다[2].

한편, 기업의 정보유출 주체는 전·현직 직원이 58.8%를 차지하고 있으며, 경쟁업체 종사자, 협력업체 종사자 등등 외부자에 의한 정보유출이 41.2%를 차지하고 있는 것으로 조사되었다[1]. 이와 관련하여, 현재 기업의 보안성 강화를 위한 연구는 전·현직 직원을 대상으로 하는 연구가 주를 이루고 있으며, 외부자에 의한 정보유출을 제재하기 위한 연구는 미흡한 상황이다. 특히, 정보화 도입을 위한 ICT 아웃소싱 참여인력을 유출 대상으로 한 보안사고 사례가 끊이지 않고 있으며, 기업의 보안시스템은 외부자 공격대응 위주로 구축되어 있다. 이

* 상명대학교 소프트웨어&미디어연구소 박사 후 연구원(kimyh7902@smu.ac.kr)
** 상명대학교 지식보안경영학과 석사과정(paulmoon@smu.ac.kr)
*** 상명대학교 지식보안경영학과 석사과정(lubshkoon@nate.com)
**** 상명대학교 경영학과 조교수(hbchang@smu.ac.kr)

에 따라서, ICT 아웃소싱에 참여하고 있는 인력에 대한 적절한 기술적·관리적 보안대책을 마련하지 않아 기업의 정보가 손쉽게 외부에 노출되거나 의도적으로 유출되는 사례가 발생하고 있다.

결국 기업들은 ICT 아웃소싱을 활용함으로써 ICT 관련 비용의 절감과 ICT 환경의 발전으로 기업 본연의 핵심역량에 집중할 수 있다는 장점 때문에 ICT 아웃소싱의 규모는 더욱 증가할 것이다. 그러나 일반적으로 ICT 아웃소싱의 인력을 활용하여 정보시스템을 구축 및 운영하는 경우는 기업 내부인력을 활용하여 정보시스템을 구축 및 운영할 때보다 보안에 더 취약한 것으로 알려져 있다[1].



〔그림 1〕 조직과 아웃소싱의 보안수준 비교

아웃소싱 업체의 낮은 보안수준, 장비의 부적절한 반출입, 보안통제 대상자의 증가 등으로 정보의 유출 위험이 증가되기 되기 때문이다. 이러한 취약점에 효과적으로 대처하며 기업의 정보를 보호하기 위해서는 자체 인력에 대한 보안방식과는 다른 관점에서 외부자 보안관리가 이루어질 필요성이 있다. 따라서 본고에는 기업 핵심정보의 중요성과 ICT 아웃소싱의 발전에 따른 기업의 핵심자산 보호를 위한 전략적 보안관리 방안을 제안하고자 한다.

세부적으로 기존에 발표된 선행연구 분석을 통하여 아웃소싱 수행에 대한 주요취약점을 도출한다. 그리고, 아웃소싱 보안관리와 관련된 항목을 물리적, 기술적, 관리적 통제항목으로 구분하여 분류하고 각 항목들을 취합하여 아웃소싱 보안관리에 대한 대응책을 설계한다. 마지막으로 이러한 보안 대응책의 적절한 점검을 위한 점검방안을 제언하고자 한다.

Ⅱ. 현황 및 선행연구

2.1. ICT 아웃소싱 정의 및 보안사고 현황

외주인력의 활용은 아웃소싱(Outsourcing)이라는 단어로 더욱 잘 알려져 있는데 아웃소싱은 외부를 뜻하는 'Out' 과 자원활용을 뜻하는 ‘Sourcing'의 합성어로 기업 외부의 자원을 활용하는 것으로 간단히 정의할 수 있다. ICT 아웃소싱은 기업의 외부에 있는 ICT 자원을 활용하는 것이다. Gartner(2010)는 운영조직으로부터 사업자로의 자산(컴퓨터, 네트워크, 인적자원 등)의 이전으로, 사업자와 장기계약을 체결하여 업무활동을 인계하여 책임을 지게하는 것이라 하였으며, IDC(2008)는 정보기술요소의 일부 또는 전부에 대한 관리 및 운영의 위임이라 하였다.

윤병남(1999)은 '전략적 목표'를 달성하기 위하여 '자산의 이전'을 포함하여 정보시스템의 일부 또는 전부를 외부 전문 업체에 '위탁'하여 운영하게 하는 '장, 단기 계약'이라 정의하였으며, 김용숙(2009)은 정보시스템 기능의 일부 혹은 전체를 외부 전문서비스 제공자에게 위탁하는 정보시스템, 데이터 처리, 하드웨어 소프트웨어, 커뮤니케이션 네트워크, 전산인력 등이 포함된다 하였다.

허용강(2010)은 기업경영에 있어서 필요한 기능을 자체적으로 수행하지 않고 외부에 위탁하여 조달하는 업무처리 방식이라 하였다. 이와 같은 ICT 아웃소싱의 국내외 정의는 표1과 같다[3].

이러한 아웃소싱은 업무의 성격, 내용 및 근무 장소에 의해 여러 가지 유형으로 구분할 수 있다. 우선, 아

〔표 1〕 ICT 아웃소싱의 국내외 정의

정의 주체	ICT 아웃소싱 정의
가트너 그룹 (2010)	운영조직으로부터 사업자로의 자산(컴퓨터, 네트워크 등)의 이전으로, 사업자와 장기계약을 체결하여 아웃소싱 활동을 인계하여 책임을 지게 하는 것
IDC (2008)	정보기술요소의 일부 또는 전부에 대한 관리 및 운영의 위임
안준모 (2013)	명확한 전략적 목표 하에서 정보시스템 관련 활동의 전부 또는 일부를 외부의 전문기간에 위탁하여 관리하게 하는 장·단기 계약
남기찬 (2006)	고객의 다양한 정보시스템 관리 및 개발업무를 외부전문회사가 위탁받아 수행하는 것

웃소싱은 프로그램 개발이나 시스템을 구축하는 '프로젝트' 성격의 아웃소싱과 시스템 운영·관제 및 유지보수를 수행하는 '운영'성격의 아웃소싱으로 구분할 수 있다. 세부적으로 업무 내용에 따라 ICT 업무를 수행하는 'ICT'아웃소싱과 ICT업무를 제외한 인사, 총무업무 등에서 활용하는 '일반'아웃소싱으로 나눌 수 있다. 그리고 근무 장소에 따라 조직 내부에서 수행하는 아웃소싱과 조직의 외부에서 수행하는 아웃소싱으로 나눌 수 있다. 프로젝트 업무 성격의 일반적인 업무로써 조직의 내부에서 수행하는 아웃소싱으로는 경영컨설팅, 회계감사 등이 있다.

프로젝트 업무 성격으로 ICT와 관련된 업무를 조직의 내부에서 수행하는 아웃소싱으로는 시스템 개발 프로젝트가 있다. 조직 외부에서 수행하는 시스템개발 프로젝트는 보안성 문제로 인하여 보편적으로 수행하지 않는다. 운영업무 성격의 일반적인 업무로써, 조직의 내부에서 수행하는 아웃소싱이 있다. 사내 고객 지원센터가 대표적이며, 조직의 외부에서 진행되는 경우는 사외 고객 센터, CRM 센터 등이 대표적이다.

한편 조직 시스템의 운영, 관제 및 유지보수 업무는 운영 업무성격의 아웃소싱으로써 조직의 내부와 외부에서 진행될 수 있다.

2011년 발생한 농협 전산사고를 필두로, 2014년 1월 19일 농협, 국민, 롯데 등 대표적인 카드 3사의 1억 4000만건의 신용카드 고객정보 유출은 협력업체에 대한 보안통제의 필요성을 나타내고 있으며, 이는 표2와 같이 정리할 수 있다.

2.2. ICT 아웃소싱 선행연구

이병웅[5]의 국내의 관련 연구로는 ICT 아웃소싱의 내부정보유출방지를 위한 보안관리 프로세스 개선에 대한 연구에서는, ICT 아웃소싱을 도입한 고객의 우려를 종식시키고 아웃소싱을 더욱 활성화하기 위하여 내부정보 유출방지방법을 도출하고 점검항목을 연구하였다. 정보사회진흥원에서 만든 정보시스템감리 점검프레임워크에서 시스템운영(OP)시점의 보안감리를 대상으로 하였으며 특별히 ICT아웃소싱이 도입되는 과정에서 발생할 수 있는 내부정보유출과 ICT아웃소싱으로 운영되는 환경에서 시스템운영자에 의한 내부정보요출을 범위로 하여 연구를 진행한 점에 의의가 있다. 현행 정보시스템 보안감리는 내부정보에 대한 접근을 통제하기 위해 접근통제와 권한통제의 수행여부 만을 점검하고 있기 때문에 시스템 운영자는 많은 시스템 접근권한을 가지고 있어 내부정보에 쉽게 접근할 수 있다. 이러한 문제점을 해결하기 위한 방법론을 제시하였고 실효성을 점검받았다.

심명섭[2]의 최근 연구로 ICT 아웃소싱에서 보안수준 향상에 관해 실증적 연구에서는, 설문을 통해 외주 프로젝트 통제 수준을 진단하고 보안위협요인을 제시하였으며 문헌 고찰을 통해 외주 인력에 대한 보안통제 수준을 향상시키는 방안에 대해 제시하였다. 그리고 보안 수

〔표 2〕 아웃소싱 인력에 의해 발생한 보안사고 사례

일시	해당기업	시스템 운영방법	정보유출방법
'14.1	oo카드 3사	고객정보 관리를 외부 업체에게 맡김	외부업체 담당자들의 의도적인 유출
'13.12	oo 은행	고객정보를 외부 재위탁 계약업체 직원에게 맡김	외부 재위탁 계약업체 직원 등이 문서 출력과 이동저장장치를 사용해 의도적으로 고객정보 유출
'12.12	00 기업	위탁업체에서 고객정보 저장 서버관리	외부 위탁업체 직원들이 고객정보 유출 및 유통
'11.9	oo 구청	구청 호적등본 자료의 전산화 작업을 외부업체에 맡김	문서고에 호적등본을 전산화하는 과정에서 주민정보를 스캔한 파일이 저장된 외장하드를 분실
'11.9	oo 기관	전자여권 발급기 시스템 운영을 외부업체에 맡김	여권 발급기 부품교체 주기를 파악한다는 명목으로 신상정보를 매주 본사로 보내 여권 발급에 필요한 개인정보 유출
'11.4	oo 은행	위탁업체에서 서버관리	위탁업체 직원 노트북을 통한 해킹으로 전산망 마비
'11.3	oo 캐피탈	위탁업체에서 보안업무 위탁관리	미 삭제된 퇴직자 계정 정보를 활용하여 중요시스템 접근
'10.9	oo 기관	위탁업체에서 시스템 전반을 위탁관리	서버유지보수 위탁업체 직원이 서버에 해킹 프로그램을 설치해 개인정보를 유출

준을 높이기 위해 관리적, 기술적, 물리적 영역, 각각의 보안통제 수준을 향상시킴으로써 전체적인 외주용역의 보안통제 수준을 높일 수 있다고 제안하였다.

한국인터넷진흥원[4]의 IT 외주인력 보안통제 안내서에서는 민간기업의 외주인력 보안통제를 위해 필수적으로 준수해야할 보호대책을 제시하였다. IT 환경의 개발·구축 및 운영에 대한 외주용역을 추진하고나 하는 기업들이 외주용역의 형태를 이해하고, 각 유형별 적용 가능한 기술적·관리적 대응방안을 제시하였다. 특히, 현재 운영 중인 IT 자원을 직접적으로 접근하는지에 대한 구분과 기업 내의 물리적 공간 이용여부에 따라, 유형별 차별화된 대응체계 수립에 대한 안내를 제공하고 있다. 또한 IT 외주용역의 유형과 기업의 IT 자원유형 및 사용권한, 자원에 대한 온라인 또는 오프라인을 통한 접근경로에 따라 분류하고 상세한 특성을 설명하고 있다. 향 후 각 기업에서 수행하고자 하는 외주용역의 유형을 판단하여, 이 안내서에서 제시되는 기술적·관리적 보호대책을 선택적으로 적용하여 활용할 수 있을 것이다. 이 안내서를 통해 외주 인력의 보안과 관련된 항목을 체계적이고 구체적으로 도출 할 수 있었다.

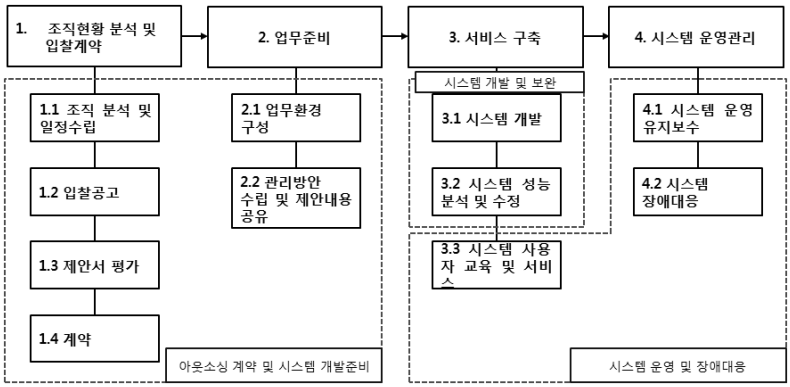
Nik Zulkarnaen 외[8]의 ICT 아웃소싱의 위험요인에 관한 연구에서는, ICT 아웃소싱 프로젝트에 대한 전략적 완화 계획을 준비하는 ICT 보안 담당관과 ICT 아웃소싱의 최고 효과를 원하는 조직을 위해 적성되었다. ICT 아웃소싱 중 18개의 위협요인과 30개의 위험요인들을 선행연구를 통해 조사하였다. 조사된 위협·위험 요인들을 보안담당관과 전문가를 대상으로 설문조사를 실시하여 우선순위를 선정하였다. 조사 결과 ICT 아웃소싱 프로젝트에서 매우 중요한 정보보안 위협 위험 요인들은 정보자산에 대한 무단 수정, 접근 및 파괴 착취, 유출, ICT 실패, 시스템 오류로 나타났고 중요한 정보보안 취약점 위험 요인은 시스템 설계 및 ICT 구현에서 인간 요인에 대한 부족한 관심으로 나타났다.

Ⅲ ICT 아웃소싱 환경에서 보안관리 방안

3.1 ICT 아웃소싱 보안관리 프로세스 분석

선행연구를 통해 조사 분석된 ICT 아웃소싱 프로세스는 '1. 조직현황 분석 및 입찰계약', '2. 업무준비'. '3. 서비스 구축', '4. 시스템 운영관리' 의 4단계로 구분할 수 있다.

조직 현황 분석 및 입찰계약 단계는 조직의 현황을 분석하고 용역사업을 시행하기 전·후의 일정을 수립하여 입찰공고를 낸 후, 제안서를 평가해 최종 선발자와 계약을 맺는 단계이다. 업무준비 단계는 용역사업을 실시할 업무 인원 구성 및 장비를 반입하여 업무에 필요한 환경을 구성하고 용역 작업을 진행할 때 필요한 관리방안을 수립, 세부 제안내용을 용역사업 업체의 작업 인력들과 공유하는 단계이다. 서비스 구축 단계는 조직의 요구에 따라 시스템을 개발하고 시범 운영을 통해 성능을 분석하며 세부사항을 조율하고 서비스에 대한 교육을 실시, 성과를 측정한 후에 서비스를 시행하는 단계이다. 시스템 운영관리 단계는 시스템의 모니터링과 업데이트를 통해 시스템을 운영 및 유지보수를 하여 장애 발생 시 신속한 장애대응과 장애관리를 하는 단계이다. 이러한 프로세스를 ICT 아웃소싱 보안관리를 위하여 프로세스 시간의 흐름에 따라 준비, 수행, 운영의 3



〔그림 2〕 ICT 아웃소싱 프로세스 및 보안관리 영역

부분으로 재배치하면 그림 2와 같이 ICT 아웃소싱 계약 및 시스템 개발준비 영역, 시스템 개발 및 보완 영역, 시스템 운영 및 장애대응 영역으로 나눌 수 있다.

3.2. ICT 아웃소싱 주요 취약점 분석

ICT 아웃소싱 보안관리 프로세스에 따른 주요 보안 취약점을 분석하면 다음과 같다. 우선, ICT 아웃소싱 계약 및 시스템 개발준비 영역에서는, 용역사업 담당자와 보안관리자를 동일한 인원이 역임하는 경우, 용역사업 진행 간 수행해야 하는 정기 보안감사 및 수시감사에 대한 신뢰성이 확보되지 않을 수 있다. 또한, 시스템 개발구역을 지정하지 않았거나, 개발구역에 대한 통제장치를 관리하지 않았을 경우 시스템 개발구역에 인가받지 않은 인원(접근 권한이 없는 인원)이 자유롭게 출입하여 조직의 자산에 접근할 수 있다. 그리고, 조직내부로 바이러스·악성코드에 감염되어 있던 장비가 조직내부로 반입될 수 있으며, 반입 장비의 기록을 하지 않을 경우 추후 반출되는 장비에 대한 관리가 어려울 수 있는 취약점 등등이 있다.

다음으로 시스템 개발 및 보완 영역에서는 시스템 개발PC에 자물쇠 등 시건장치를 설치하지 않을 경우, PC의 하드디스크 무단 교체로 시스템 개발 내용과 조직내부 정보가 유출될 수 있다. 그리고, 시스템 개발PC의 로그인 계정·비밀번호를 설정하지 않고, 화면보호기를 적용하지 않아 시스템 개발PC를 인가받지 않은 인원이 사용하여 시스템 개발내용과 조직내부 정보가 유출될 수 있다. 또한 조직내부에서 무선 API를 설정하여 사용할 경우, 시스템 개발PC의 인터넷 접속에 따른 조직 내부 정보의 유출경로(채널) 발생의 취약점 등등을 내포하고 있다.

마지막으로 시스템 운영 및 장애대응 영역에서는, 시스템 교육에 전 직원을 대상으로 보안교육을 수행하지 않았을 경우, 시스템의 주요 보안사항에 대한 보안인식 개선에 어려움이 있을 수 있다. 그리고 시스템 교육자료 및 성과측정 자료를 외부인이 접근 가능한 공개된 장소(website 등)에 개제하거나 조직내부 자료로 관리하지 않을 경우, 시스템 교육자료에 포함된 조직내부 자료에 인가받지 않은 인원이 접근 가능한 취약점이 있다. 또한, 시스템 관리자 및 모니터링 담당자가 시스템 특이사항 발생(시스템 장애 포함)시의 초동대응 조치 및 장애 매뉴얼을 숙지하고 있지 않을 경우, 시스템 특이사항이 더 큰 보안사고로 확산될 수 있는 취약점을 가지고 있다.

이와같은 보안 취약점의 근본적인 원인들을 정리해 보면 용역사업 담당자와 보안담당자가 같거나, 문서위주의 보안대책 업무 수행하고 있거나, 보호구역, 비공개 정보에 대한 물리적 관리 소홀(허술)이 하고 있으며, 용역업체 직원이 이동식 저장매체에 업무의 중요한 자료 저장 및 무단 반출하고, 무분별한 인터넷 사용으로 인한 악성코드 감염, 내부자료 유출 등으로 규명될 수 있다.

3.3. ICT 아웃소싱 보안대책 도출

ICT 아웃소싱 취약점을 기반으로 기존의 선행 연구에서 도출된 아웃소싱 인력에 대한 보안 항목을 물리적, 기술적, 관리적의 3가지 관점에서 각 지표의 통제항목을 분류하고 지표의 각 항목들을 하나의 표로 정리하여 아웃소싱 참여 인력에 대한 보안수준 향상을 위한 통제요소를 정리한다.

보안수준 향상을 위해 기존의 선행연구에서 제안하고 언급한 각 관점들의 보안 항목들을 추출하여 표 3과 같이 정리하였다. 각 항목들의 중복을 피하기 위하여 한국인터넷진흥원에서 발간된 ‘IT 외주인력 보안통제 안내서’ 의 명칭을 기준으로 정리하였다 때문에 한국인터넷진흥원의 ‘ IT 외주인력 보안통제 안내서’ 의 항목이 표의 제일 왼쪽에 위치하였고 그 다음은 논문이 발간된 순서로 정리하였고 마지막은 국외 논문의 순으로 표를 정리하였다.

각 통제항목을 살펴본 결과, 물리적 통제항목은 보호구역의 출입통제와 시건장치의 활용만이 언급되었다. 기술적 통제항목으로는 usb, 외장하드와 같은 이동식 저장매체의 통제와 보안 소프트웨어의 설치, 로그기록 관리, 사용자인증, 망분리. 암호화, 악성코드의 검사, 자료공유사이트의 통제, 용역완료시 제공자료 및 산출물의 회수, 원격작업 금지, 장비 반입 시 무결성을 검토해야 하는 것으로 나타났다.

관리적 통제항목으로는 아웃소싱 참여인력의 작업 전 사전 신원확인, 보안서약서 작성, 보안교육의 실시, 보호구역 출입 시 보안 관리자와 동행, 아웃소싱 참여인력에 대한 차별적 접근권한을 부여하는 것, 용역계약 시 보안요구기준과 손해배상 기준을 마련하는 것, 출력물 및 장비와 통제구입 출입 시 관리대장을 작성하는 것,

용역사업 수행 전 자산을 분석하는 것과 위험평가를 수행하는 것, 아웃소싱 업체가 아웃소싱 참여인력에 대한 임의변동을 금지하는 것, 퇴사자 관리를 해야 하는 것 등으로 나타났다.

각 통제항목 수를 비교한 결과 상대적으로 물리적인 통제항목이 적은 것으로 나타났다. 이는 아웃소싱 참여인력의 보안관리를 함에 있어 물리적인 위험보다 기술적, 관리적 위험의 비율이 높고 이에 대비해야 하는 부분이 더욱 많음을 보여준다. ICT의 발달로 인해 물리적으로 정보를 유출하는 것보다 기술과 인력을 활용하여 유출하는 사례가 늘고 있어 이에 따라 통제해야 하는 항목도 많은 것으로 나타났다.

도출된 보안관리 요소 27개의 통제항목 중에서 보호구역 출입통제, 암호화, 보안서약서작성, 보안요구기준 마련, 이 4가지 항목만이 공통적으로 나타난 통제항목이고 나머지 23개 항목은 각 연구들마다 상이하게 나타났다.

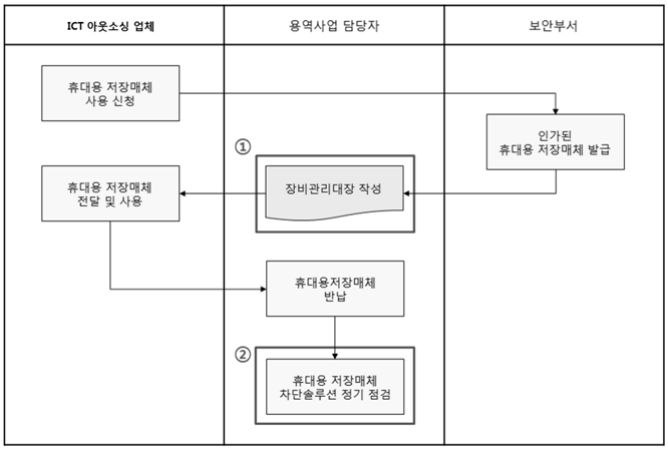
이는 각 연구들에서 언급한 보안 통제항목을 취합하여 ICT 아웃소싱 주요 취약점에 대한 보안대책을 설계하여 정보보호 추진방향을 제언하려는 본 연구의 타당성을 나타낸다.

3.4 ICT 아웃소싱 보안관리 점검방법

ICT 아웃소싱 보안관리는 보안관리 대응책의 적용을 통하여 새로운/기존의 보안 취약점을 감소시키는데 목적이 있다. 이러한 보안 대응책의 올바른 적용과 수행여부를 확인하기 위하여 수시 또는 정기적으로 보안관리 현황을 점검할 필요가 있다.

〔표 3〕 아웃소싱 보안수준 향상을 위한 보안통제요소

대분류	소분류	[3]	[1]	[4]	[7]
물리적 통제항목	보호구역 출입통제	√	√	√	√
	시건장치 통제			√	√
기술적 통제항목	이동식 저장매체 통제	√			
	보안SW 설치	√	√		√
	접근이력 관리시스템운영	√			
	사용자 인증	√			
	망분리	√	√		
	암호화	√	√	√	√
	악성코드검사	√	√		√
	웹하드, P2P등 자료공유 사이트 통제		√		
	원격작업 금지			√	
	장비 반입 시 무결성 검토			√	
관리적 통제항목	아웃소싱 참여인력 신원확인	√	√		√
	보안서약서작성	√	√	√	√
	보안교육실시	√	√		√
	보호구역 출입 시 보안관리자 동행	√	√		
	차별적 접근권한부여	√	√	√	
	보안요구기준마련	√	√	√	√
	손해배상 기준마련		√	√	√
	출력물 관리대장작성	√			√
	장비반출입대장작성	√	√		
	출입관리대장작성	√	√		
	자산분석			√	√
	위험평가 수행			√	
	아웃소싱 참여인력 임의 변동 금지	√		√	
	퇴사자 관리			√	
	제공자료 및 산출물 회수	√	√	√	√
합계		19	16	14	13



〔그림 3〕 ICT 아웃소싱 보안관리방안 및 점검 절차(휴대용 저장장치)

〔표 4〕 휴대용 저장장치 보안관리 대응책 및 점검방법(예시)

보안대응책	인가받지 않은 휴대용 저장매체의 사용을 금지하며, 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 기관의 승인 하에 장비관리대장 작성 후 사용
점검방법	용역사업 담당자는 장비관리대장의 작성 여부를 점검하고 인계자·인수자가 직접 서명을 했는지 확인

ICT 아웃소싱 프로세스 내의 보안 취약점과 이를 관리하기 위한 보안 대응책의 이행 유무를 점검하기 위하여 그림 3과 같은 형태의 점검 절차를 설계하여 점검한다. 그림 3은 휴대용 저장장치에 대한 보안관리 예시를 나타내었다. 이는, 휴대용 저장장치를 사용하기 위한 발주처-아웃소싱 업체간의 주요 절차(흐름)에 대해 나타내고 있다. 보안관리를 위한 보안 대응책을 적용할 부분은 ①장비관리대장 작성 부분에 대하여 설명하면 표 4와 같이 표현될 수 있다.

3.5 ICT 아웃소싱 보안관리 적용 및 점검사례

〔표 5〕 ICT 아웃소싱 보안관리 체계 적용사례 절차

ICT 아웃소싱 프로세스 확인 → ICT 아웃소싱 보안관리 영역 선정 → ICT 아웃소싱 보안관리 세부영역 선정 → 보안 취약점 도출 → 보안취약점 방지 대응책 설계 → 보안관리 점검방안 도출

본고에서 제언하는 ICT 아웃소싱 보안관리 방안을 적용하여 점검하기 위한 사례분석을 위하여 표 5과 같은 절차에 의해 수행하였다.

〔표 6〕 시스템 개발 및 보완 프로세스 보안취약점

분류	보안 취약점
물리적	인가받지 않은 인원의 시스템 개발구역 출입
물리적	ICT 아웃소싱 참여인원이 조직의 출입증 보유
관리적	시스템 개발에 투입된 조직내부 자료 미회수
관리적	ICT 아웃소싱 참여인원의 기관시스템 계정 유지
기술적	시스템 개발PC가 바이러스·악성코드에 감염
기술적	인가받지 않은 휴대용 저장장치 무단 사용
기술적	조직내부에서 허용되지 않은 무선 AP 사용을 통한 자료 유출*
...	

다시 말하면, ICT 아웃소싱 프로세스를 조직의 비즈니스 프로세스에 적합하게 재구성하고, 보안관리 영역을 도출한다. 그리고 도출된 보안관리 영역별 물리적/관리적/기술적 취약점을 분석하고 이에 대한 대응책을 마련한다. 마지막으로 대응책에 대하여 적용 현황을 주기적으로 점검한다.

우선, ICT 아웃소싱과 관련하여 정보화 시스템을 구축하는 단계인 서비스 구축 프로세스를 식별하고 보안관리를 위한 시스템 개발 및 보완단계를 선정하였다. 그

〔그림 4〕 이동식 저장장치 사용금지 정책 설정

리고 시스템 개발 및 보완단계의 취약점 중 기술적 취약점인 '인가받지 않은 휴대용 저장장치 무단 사용 통한 자료유출' 방지를 위하여 허용되지 않는 무선 AP 사용에 대한 보안관리 대응책을 표 7과 같이 설계하였다.

〔표 7〕 미 인가 USB 사용방지 대응책

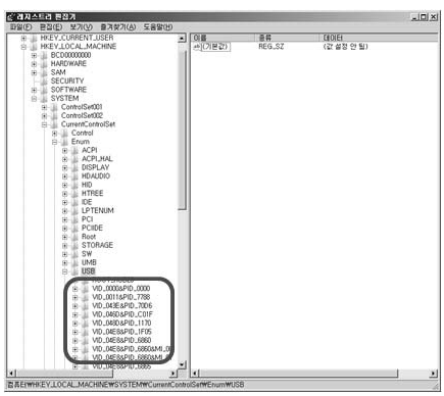
모든 이동식 저장매체에 대하여 이동식저장매체 등록대장을 작성하고, PC의 휴대용 저장매체 자동실행을 금지시킨다.

PC의 휴대용 저장매체 사용을 방지하기 위하여 그림 4와 같이 "시작버튼 → 'gpedit.msc'실행 → 컴퓨터 구성 → 관리 템플릿 → 시스템 → 장치 설치 → 장치 설치 제한 → 다른 정책 설정에 의해 기술된 장치 설치 방지 → 사용 → 확인 → 재부팅" 프로세스를 수행한다. 마지막으로 보안관리 대응책을 점검하기 위하여 표 8와 같은 방법에 의해 점검하면, 그림 5와 같은 형태로 임의 사용되고 있는 인가받지 않은 휴대용 저장장치 유무를 점검할 수 있다.

〔표 8〕 휴대용 저장장치 사용 흔적 점검방법

시작의 실행 창에 'regedit'을 입력하여 레지스트리 편집기를 실행한다. 레지스트리 편집기에서 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB' 의 경로로 가면 PC에 연결되었던 휴대용 저장매체 목록을 확인

PC에 접속한 휴대용 저장매체를 점검하는 방법은 그림 5와 같다. 기업에서 지정한 휴대용 저장매체 이외의 저장매체가 PC에 접속한 흔적이 있는지 확인하는 사례



〔그림 5〕 휴대용 저장매체 접속 확인

이다. 목록에 휴대용 저장매체의 일련번호와 이름을 확인할 수 있기 때문에 인가된 휴대용 저장매체와 인가되지 않은 휴대용 저장매체를 구분할 수 있다.

Ⅳ. 연구결과 및 향후 연구

기업의 보안시스템은 외부자 공격대응 위주로 구축되어 있으며, ICT 아웃소싱에 참여하고 있는 인력에 대한 적절한 기술적·관리적 보안대책을 마련하지 않아 기업의 핵심자산이 손쉽게 외부에 노출되거나 의도적으로 유출되는 사례가 발생하고 있다. 그러나 그간의 연구들은 보안의 중요성 강조와 함께 다양한 대상과 목적을 가진 관련 보안관리 방법 위주로 연구되어 왔다. 이에 따라, 본 연구에서는 ICT 아웃소싱 보안성 향상을 위한 보안관리 추진방향을 설계하였다.

본고에서는 ICT 아웃소싱 환경에서 보안관리를 위한 정보보호 추진방향 제언을 위하여 위해 기존에 외부자 보안에 대해 연구한 연구자료의 각 요소들을 취합하였다. 그리고 각 요소들을 물리적, 기술적, 관리적 요소들로 나누어 항목들을 구분하여 각 요소별 통제사항에 대해 정리하였다. 기술적, 관리적 통제항목의 수에 비해 물리적 통제항목의 수가 상대적으로 적었는데 이는 최근의 외부자의 정보유출을 방지함에 있어서 균형감이 부족한 것으로 분석되었다. 그리고, ICT 아웃소싱 프로세스를 분석하여 보안관리 영역을 도출하였으며, 이에 따르는 보안취약점을 기술하였다. 마지막으로, ICT 아웃소싱 보안관리 대응책을 설계하고 총체적인 적용사례를 기술하였다.

보안은 댐과 같아서 한곳이라도 작은 구멍이 생긴다면 다른 곳의 보안이 아무리 철저하다고 하더라도 그 기능이 유명무실해질 수밖에 없다. 따라서 연구를 통해 도출된 모든 통제 항목에 대해 보안 대책을 마련하고 그 보안 대책을 철저히 지켜야 보안 수준이 향상될 것이다.

참고문헌

[1] 중소기업청, *중소기업 기술보호 역량 및 수준조사*, 2012

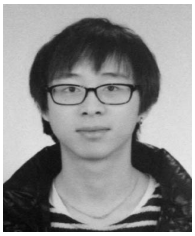
[2] 심명섭, "IT 외주용역에서 보안수준 향상에 관한 실증적 연구", 건국대학교, pp. 42-5, 2013

[3] 행정안전부IT, *아웃소싱 운영관리 매뉴얼*, 2011
[4] 한국인터넷진흥원, *IT 외주인력 보안통제 안내서*, 2012
[5] 이병웅(2009), “IT 아웃소싱 환경에서 내부정보유출방지를 위한 보안관리 프로세스 개선에 대한 연구”, 건국대학교, 17-67
[6] 조아라(2011), “IT 아웃소싱 산업의 현황 및 발전방향에 관한 연구”, 서울시립대학교, 16-19
[7] 송영주(2009), “공공기관의 IT 아웃소싱에 관한 연구”, 연세대학교, 12-38
[8] Nik Zulkarnaen Khidzir, “Information Security Risk Factors Critical Threats and Vulnerabilities in ICT Outsourcing”, Universiti Teknologi MARA, 2-6
[9] 이종만, 남기찬, “정보시스템 아웃소싱의 관계 관리 조합에 관한 개념연구”, 한국경영정보학회 2006년도 학술대회, pp. 491-496. 2006
[10] 곽정섭, 안준모, “어플리케이션 개발 해외아웃소싱의 핵심성공요인에 관한 연구”, Entrue Journal of Information Technology , 12(2), pp. 39-53, 2013
[11] 윤병남, *정보시스템 아웃소싱 방법론*, *한국전산원*, 1999.
[12] 김용숙, “외식기업의 경영정보시스템 상황변수, 아웃소싱 정도, 아웃소싱 성과와의 관련성 분석”, 관광연구저널, 23(4), pp.229-243, 2009.
[13] 안장수, 이창기, 허용강, “호텔경영 업무효율에서의 아웃소싱효과”, 한국호텔관광학회, pp.113-128, 2010

〈저자소개〉

김 양 훈 (Yanghoon Kim)
2011년 : 대진대학교 소프트웨어공학 전공 박사
2012년 ~ 현재 : 상명대학교 소프트웨어&미디어 연구소 박사 후 연구원
관심분야: 비즈니스 연속성 관리, 정보 오남용 및 유출방지, 소프트웨어 프레임워크

문 제 욱 (Yanghoon Kim)
2011년 : 상명대학교 경영학과 학사
2013년 ~ 현재 : 상명대학교 지식보안경영학과 석사과정
관심분야: 아웃소싱 보안관리, 인적 보안관리, 정보 유출방지



황 선 호 (Yanghoon Kim)
2013년 : 경남대학교 e-비즈니스학과 학사
2013년 ~ 현재 : 상명대학교 지식보안경영학과 석사과정
관심분야: 아웃소싱 보안관리, 정보 유출방지, 디지털 포렌식

장 항 배 (Hangbae Chang)
종신회원
2006년 : 연세대학교 정보시스템관리 전공 박사
2007년 ~ 2011년: 대진대학교 경영학과 조교수
2012년 ~ 현재 : 상명대학교 경영학과 조교수
관심분야 : 중소기업 정보보호, 정보 오남용 및 유출방지, 성과분석 체계