소규모 IT 서비스 기업 비즈니스 특성을 고려한 정보보호 참조모델 설계연구

A Study on Information Security Reference Model Considering Business Process Characteristics for Small IT Service Organization

김양훈(YangHoon Kim)*, 장항배(HangBae Chang)**
kimyh7902@daejin.ac.kr, hbchag@smu.ac.kr

초 록

지적 정보자산에 관한 의존도가 대기업이나 타 업종의 중소기업에 비하여 상대적으로 높은 소규모 IT 서비스 기업의 정보보호 필요성 및 중요성은 점차 증가되고 있다. 그러나, 한정된 자원과 인력으로 인하여 주요 정보를 저장하고 있는 IT 서비스 시스템을 대상으로 단순한 정보보호 시스템 도입만이 진행되고 있다. 한정된 자원과 인력으로 영위하는 소규모 IT 서비스 기업의 지속적 비즈니스 성장을 위해서, 비즈니스 프로세스 및 자원의 관점에서 정보보호 특성과 대응방안이 대기업과는 차별적으로 설계되어야 한다. 이처럼 소규모 IT 서비스 기업에 대한 조직, 비즈니스, 정보화 수준 등에 관한 특성을 고려하고 유형화함으로써 대기업 조직과 차별화된 정보보호 추진전략이 필요한 상태이다. 따라서 본 연구에서는 소규모 IT 서비스 기업의 특성을 고려한 정보보호 참조모델을 설계하고 IT 서비스 시스템에 따른 정보보호 대응책을 도출하고자 한다.

1. 서론

소규모 IT 서비스 기업의 경영방식은 직관적, 전근대적인 방법에 의하여 관리되며, 의사결정권이 경영진에 집중되기 때문에 신속하고 직접적인 의사결정 특성을 보인다. 업무조직은 비체계적, 비정형화된 특성을 가지며 업무기능의 분화가 부족한 실정이다[3]. 대기업에 비해 매출액, 자본, 인적 자원이 부족한 소규모 IT 서비스 기업은 정보보호 수행을 위한 정책과 시스템을 도입할 경우 다양한 어려움이 존재하며 소규모 IT 서비스 기업 정보보호 실태 조사에 관한 선행연구에 따르면 소규모 IT 서비스 기업이 정보보호를 추진하는 데 가장 큰 어려 움이

* 상명대학교 기술경영 및 보안 연구실 박사 후 연구원
** 상명대학교 경영학부 교수

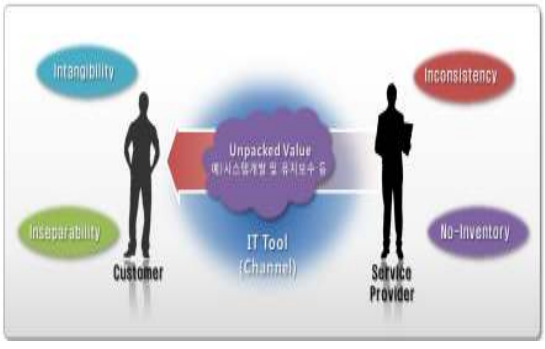
기업의 규모나 자금으로 볼 때 '정보보호 추진비용이 과다하다'고 느끼고 있는 것으로 나타나고 있다[2].

이처럼 소규모 IT 서비스 기업은 대기업에 비해 조직, 비즈니스, 정보화 수준과 특성이 상이하며, 소규모 IT 서비스 기업의 정보보호 전략 설립을 위해서는 이와 같은 특성을 고려하여야 한다. 따라서 본 연구에서는 소규모 IT 서비스 기업의 특성을 고려한 정보보호 참조모델 을 설계하고 IT 서비스 시스템에 따른 정보보호 대응책을 도출하고자 한다.

2. 선행연구

2.1 소규모 IT 서비스 개념

소규모 IT 서비스는 <그림 1>처럼 "기본 단위 형태로 구성되어 있지 않은(unpacked value) 무형의 제품(intangible goods)을 IT 적 수단(IT tool)을 통하여 고객에게 제공(≒ IT 활용을 서비스 하는 것)하는 것"으로 정의한다[1].



<그림 1> 소규모 IT 서비스의 개념

또한 소규모 IT 서비스 기업은 한국 IT 서비스 산업협회에서 분류한 IT 서비스 산업 분류와 한국 제8차 표준산업분류체계 기준, 한국 제9차 표준산업분류체계 기준을 고려하여, 비즈니스 종류를 SI(System Integration), SM(system Management), DB(Data Processing), IR(IT Rent), IP(Information)로 분류하였다[1,4]. SI/SM 업종은 IT 기술을 활용한 시스템 자문 및 구축/기 구축된 시스템 운영 및 유지보수를 비즈니스 프로세스로 하고 있으며 DB 업종은 물리적 형태의 자료를 디지털 화하는 것을 주 비즈니스 프로세스로 보유하고 있다. 그리고 IR 업종은 보유하고 있는 시스템 및 솔루션(서비스) 등을 임대하는 사업을 비즈니스 프로세스로 하고 있으며, IP업은 IT 기술을 통하여 생성된(가공된) 서비스 및 정보를 제공하는 사업을 주 비즈니스 프로세스로 운용하고 있다.

<표 1> 소규모 IT 서비스 기업 핵심 정보 자산

비즈니스	비즈니스 핵심정보자산	세부 정보 자산	보유율(%)
SI / SM	공동 작업 공간	공유 디렉터리	73.7
		파일 서버	94.7
		프로젝트 관리 프로그램	52.6
DB	입력처리장치 (OMR, OCR, Scanner 등)		91.7
	데이터베이스		91.7
IR	공용자원(저장 공간, 메모리 등)		100.0
	공급되는 IT 응용 서비스(기존, 신규)		100.0
IP	디지털 콘텐츠	웹 콘텐츠	96.2
		이미지/동영상 콘텐츠	84.6
	(개인정보) 데이터베이스		84.6

2.2 소규모 IT 서비스 기업 별 비즈니스 핵심자산

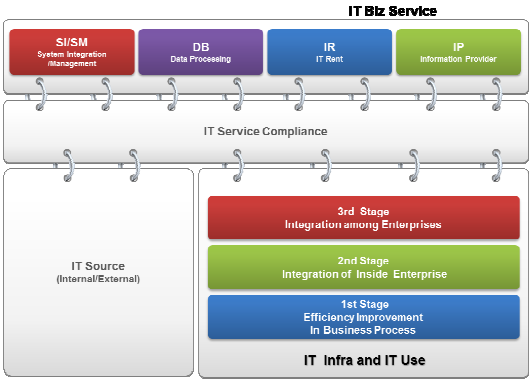
소규모 IT 서비스 기업의 비즈니스 별 핵

심 정보자산에 대하여 분석 한 결과, <표 1>과 같이 비즈니스 별 차별적으로 구분되는 핵심 정보자산이 있는 것으로 조사되었다.

3. 정보보호 참조모델 설계

3.1 소규모 IT 서비스 기업 정보보호 참조모델 설계

소규모 IT 서비스 기업은 비즈니스 형태에 따라 SI/SM, DB, IR, IP로 분류될 수 있으며, 각 비즈니스 별 핵심 정보자산을 보유하고 있다. 이러한 특성을 고려하여 소규모 IT 서비스 기업 정보보호 참조모델을 <그림 2>와 같이 설계하였다. 소규모 IT 서비스 기업의 IT 인프라와 IT 활용 정도를 기반사항으로 고려하며, 소규모 IT 서비스 기업 비즈니스 별 자산을 보호해야 한다. 이러한 IT 인프라 및 IT 활용도와 비즈니스 자산은 IT 서비스 컴플라이언스로 연결된다.



<그림 2> 소규모 IT 서비스 기업 정보보호 참조모델

3.2 핵심 정보자산 취약점 분석

설계한 정보보호 참조모델의 각 영역별 핵심자산과 정보보호 요구사항을 분석하였다. SI/SM 비즈니스 관점에서 디렉토리, 파일서버, 응용 프로그램 자산에 대해 정보보호 요구사항을 분석하였다. 다시 세부적으로 디렉토리 자산은 사용자 인증부분, 사용자 권한관리 부분으로 나뉘어지며, 파일서버 자산은 사용자 인증부분, 사용자 권한관리 부분, 운영관리 및 사고대응 부분으로 나뉘어진다. 그리고 응용 프로그램 자산은 프로그램 지원부분으로 나뉘어진다.

DB 비즈니스 관점에서 입력처리장치, 데이터베이스 접점(entrypoint), 데이터베이스 콘텐츠(data field) 자산에 대해 정보보호 요구사항을 분석하였다. 다시 세부적으로 입력처리장치 자산은 사용자 인증부분, 사용자 권한관리 부분으로 나뉘어지며, 데이터베이스 접점 자산은 사용자 인증부분, 사용자 권한관리 부분, 침입탐지/차단 부분으로 나뉘어진다. 그리고 데이터베이스 콘텐츠 자산은 사용자 인증 부분, 사용자 권한관리 부분, 운영관리/사고대응 부분으로 나뉘어진다.

IR 비즈니스 관점에서 저장 공간, 메모리 등의 공용자원, 공급되는 IT 응용서비스 자산에 대해 정보보호 요구사항을 분석하였다. 다시 세부적으로 공용자원 자산은 유출방지 부분으로, 공급되는 IT 응용 서비스 자산은 사용자 인증부분, 침입탐지/차단 부분으로 나뉘어진다.

IP 비즈니스 관점에서 사용자, 웹 콘텐츠, 이미지/동영상 콘텐츠, 개인정보 데이터베이스 자산에 대한 정보보호 요구사항을 분석하였다. 다시 세부적으로 사용자 자산은 사용자 인증 부분, 유출 방지 부분, 사용자 권한관리 부분으로 나뉘어진다. 그리고 웹 콘텐츠 자산은 유출방지 부분으로 나뉘어진

다. 또한 이미지/동영상 콘텐츠 자산은 사용자 인증 부분, 사용자 권한관리 부분, 사고대응 부분으로 나뉘어진다. 마지막으로, 개인정보 데이터베이스 자산은 보안 취약점 부분으로 나뉘어진다.

3.3 핵심 정보자산 정보보호 대응책

SI/SM 비즈니스는 핵심 정보자산을 보호하기 위하여 디렉토리 자산의 사용자인증 및 사용자 권한관리 요소 보안 대응을 위해 Active Directory를 운용할 수 있다. 그리고 파일서버 자산의 사용자인증 및 사용자 권한관리, 운영관리/사고대응 요소 보안을 위해 보안 파일 서버(File Server Security)를 활용해야 한다. 마지막으로, 응용 프로그램 자산의 프로그램 지원 요소 보안을 위해 응용 프로그램 (지원) 보안을 수행해야 한다.

DB 비즈니스는 핵심 정보자산을 보호하기 위하여 입력처리장치 자산의 사용자 인증 및 사용자 권한관리 요소 보안을 위해 전자 카드(RFID), 생체 인식(Bio Recognition) 솔루션을 도입할 수 있다. 그리고 데이터베이스 자산의 사용자인증 및 사용자 권한관리, 침입탐지/차단 요소 보안을 위해 DB 접근통제(DB Access Control)를 운용할 수 있다. 마지막으로, 데이터베이스 자산의 사용자인증 및 사용자 권한관리, 운영관리/사고대응 요소 보안을 위해 DB 암호화(DB Encryption)를 수행할 수 있다.

IR 비즈니스는 핵심 정보자산을 보호하기 위하여 공용자원 자산의 유출방지 요소 보안에서 검색 가능 암호 시스템(Public Key Searchable Encryption System), (Privacy Data) Preserving Data Mining을 운용할 수 있다. 그리고 공급되는 IT 응용서비스 자산의 사용자 인증 및 침입탐지/차단 요소 보안을 위해 분산 서비스 공격 대응 서비스(Anti DDos)를 도입할 수 있다.

IP 비즈니스는 핵심 정보자산을 보호하기 위하여 사용자 자산의 사용자인증 및 유출방지, 사용자 권한관리 요소 보안에서 공개키 기반구조(Public Key Infrastructure), One Time Password, 키보드 보안(Keyboard Security), 통합 계정관리(Identity Management), 통합 접근관리(Enterprise Access Management) 솔루션을 도입 할 수 있다. 그리고 웹 콘텐츠 자산의 유출방지를 위하여 웹 콘텐츠 보안(Web Contents Security) 솔루션을 운용할 수 있다. 또한 이미지/동영상 콘텐츠 자산의 사용자인증 및 사용자 권한관리, 사고대응 요소 보안을 위하여 저작물 보안(Contents Digital Right Management), 디지털 워터마킹(Digital Watermarking)을 운용할 수 있다. 마지막으로 (개인정보)데이터베이스 자산의 보안 취약점 해결 요소 보안을 위하여 개인정보 스캐너(Privacy Scanner)를 운용할 수 있다.

4. 결론

대기업과 상이한 특성을 지닌 소규모 IT 서비스 기업은 조직, 비즈니스, 정보화 수준 등에 대한 특성을 고려한 정보보호 추진 전략이 요구되고 있다. 이에, 본 연구에서는 소규모 IT 서비스 기업의 특성을 고려한 정보보호 참조모델을 설계하고 IT 서비스 시스템에 따른 정보보호 대응책을 도출하였다. 이는 소규모 IT 서비스 기업의 특성을 파악하여 기존의 단발성 정보보호 시스템의 단점을 보완할 수 있으며, 정보보호에 효과

적인 투자를 달성할 수 있는 조직수준(Managerial Level)의 관점에서 일관성 있는 정보보호 체계를 제시할 수 있다. 또한 소규모 IT 서비스 기업에 대한 조직, 비즈니스, 정보화 수준 등에 관한 특성을 도출하고 이를 유형화함으로써 대기업 조직과 차별화된 정보보호 추진전략을 제공할 수 있다.

이처럼, 본 연구에서 제시한 정보보호 참조모델은 소규모 IT 서비스 기업의 자원을 최소화로 소모하며 적용시킬 수 있는 모델이다. 향후 연구로는 자원을 소요하는 정보보호 접근 방법론 외에, 조직 내 인식 및 문화 그리고 교육을 통한 정보보호 대응책 개발에 관한 연구가 필요하다.

참고문헌

[1] 강종구, 이홍주, 임재환, 장항배, "소규모 IT 서비스 기업 비즈니스 특성을 고려한 정보자산 유형분류 설계연구", 한국전자거래학회지, 제16권 제4호,pp. 97-108, 2011.

[2] 김정덕, 이용덕, "EA 기반의 전사적 정보보호 아키텍처(EISA) 참조 모델에 관한 연구", 한국경영정보학회 학술대회 2009년 춘계학술대회, pp.341-346, 2009.

[3] “OECD 정보통신(ICT)산업 정의 및 범위”, OECD, 2006.

[4] 김지숙, 최명길, “국가기관의 정보보호 수준 평가에 관한 연구”, 정보보호학회지, 제18권, 제6호, 2008.

[5] 안중호, 최규철, 성기문, 이재홍, “보안위험 수준이 지식관리 시스템의 성공에 미치는 영향 : ‘신뢰’를 매개변인으로”, 한국전자거래학회지, 제15권, 제4호, 2010.

[6] 윤여웅, 이상호, " 정보보호제품 품질평가를 위한 품질 모델 및 메트릭에 관한 연구", 정보보호학회논문지, 제19권 제5호, pp. 131~142, 2009.