IoT환경에서 인간중심 보안관리체계 구축을 위한 효율적 인적자원관리 방법론 설계 연구

류보라*, 이효직**, 나원철***, 장항배****
*중앙대학교 산업융합보안학과
,*중앙대학교 융합보안학과
****중앙대학교 산업보안학과
e-mail:{fbqhfkfk*, shjlee7**, onechulnastop***}@gmail.com,
hbchang@cau.ac.kr****

A Study on Efficient Human Resource Management Methodology Design for Human-centered Security Management System Implementation in IoT Environment

Bora Ryu*, Hyojik Lee**, Onechul Na***, Hangbae Chang****
*Department of Industrial Convergence Security, Chung-Ang University
,*Department of Convergence Security, Chung-Ang University
****Department of Industrial Security, Chung-Ang University

요 약

보안은 오직 기술을 관리하는 것이 아닌 사람관리, 조직관리, 경영관리이다. 그 중에서도 인적자원은 모든 산업에서 가장 중요한 자원임과 동시에 보안의 측면에서 볼 때 가장 통제해야 하는 존재이다. 이는 산업보안에서 가장 큰 이슈인 산업기술·기밀 유출이 주로 전·현직 임직원 및 협력업체 직원 등 인적자원을 통했기 때문이다. 미래 산업의 중심이 될 IoT환경에서는 산업기술이 핵심자산이므로 이에 더 주목해야 할 필요가 있다. 이처럼 인적자원에 대한 통제와 관리가 산업보안에서 중요한 의미를 갖는 것에 비해 기존의 보안관리체계의 통제항목은 대부분 IT적인 부분에 치중되어있다. 또한, 체계적인 운영이 부족하고, 산업스파이, 정보절취 등 다양한 위험요소가 존재한다. 특히, 인적자원은 완벽한 예측이 불가능하므로 위험을 최소화하는 방법을 고안해 내는 것에 유념하여 IoT환경에서의 인간중심적인 보안관리체계 구축해야한다. 이를 위해 기존의 정보보호 관리체계 분석을 통하여, 기존의 인적보안 지침들의 적합성을 따져 우선순위를 적용하여 효율적인 인적자원관리 방법론을 설계하였다. 본 연구결과는 보유자원을 가장 효율적으로 활용하여, 그 조직에 적합한 보안체계를 구축하는데 도움이 될 것으로 기대된다.

1. 서론

인적자원에 대한 보안은 산업보안에서 가장 큰 이슈인 산업기술·기밀 유출과 아주 밀접한 관련이 있다. 그 유출의 경로가 주로 전·현직 임직원 및 협력업체 직원 등 인적자원을 통했기 때문이다. 이런 사건들은 뉴스를 통해 우리에게 빈번하게 들려온다. 그 한 예로, 2012년에 차세대 디스플레이기술이 이스라엘로 유출되었다. 디스플레이 검사장비를 다루는 외국계 기업의 직원 6명이 국내 디스플레이업체에서 파견 근무를 하면서 획득한 해당 업체의 기술자료 1,000여건을 초소형 USB에 담아 지갑·신발·벨트 등에 숨겨 유출한 것이다. 이들은 해당 기술자료를 외국 본사에 유출하는 등 세계최초로 상용화에 성공한 첨단 디스플레이 기술을 국외로 빼돌리려다 적발되었다.

또한, 인적자원을 통한 산업기술·기밀 유출의 심각성은 통계자료로도 입증되었다. 국가정보원 산업기밀보호센터(2012)의 자료는 2005년부터 2011년까지 적발된 총 264건의 기술·기밀 유출 사건 중 2007년부터 5년 동안(2007-2011)에 해당하는 204건을 분석하였다. 그 결과 유출의 주체가 퇴직(전직) 직원인 경우가 가장 많은 127건으로 62%였고, 현직 직원이 34건으로 17%, 그리고 협력업체가 26건으로 13%의 순으로 나타났다. 여기서 주목할 점은 전·현직 직원이 유출 주체인 사건이 모두 합쳐 161건으로 전체의 79%에 달해 기술·기밀 유출의 주된 경로로 판단된 것이다.[1] 미래 산업의 중심이 될 IoT환경에서는 산업 기술·기밀이 핵심자산이므로 이에 더 주목해야 할 필요가 있다.

이처럼 인적자원에 대한 통제와 관리가 산업보안에서 중요한 의미를 갖는 것에 비해 기존의 보안관리체계의 통제항목은 대부분 IT적인 부분에 치중되어있다. 또한, 체계적인 운영이 부족하고, 산업스파이, 정보절취 등 다양한 위

* 제 1저자
**** 교신저자

험요소가 존재한다. 특히, 인적자원은 완벽한 예측이 불가능하므로 위험을 최소화하는 방법을 고안해 내는 것에 유념하여 IoT환경에서의 인간중심적인 보안관리체계 구축해야한다.

따라서 본문에서는 기존의 인적보안 지침들의 적합성을 따져 우선순위를 적용하여, IoT환경에서의 인간중심적인 보안관리체계 구축을 위한 효율적인 인적자원관리 방법론을 설계하고자 한다.

2. 기존 정보보호 관리체계 중 인적보안 통제사항

본 논문에서는 기존의 정보보호 관리체계인 ISMS, PIMS, G-ISMS의 인적보안 통제사항을 조사하였다.

첫 번째로 기업이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계의 적합성에 대해 인증을 부여하는 제도인 ISMS(정보보호 관리체계)의 인적보안 통제사항은 주요 직무자 지정 및 감독, 직무분리, 비밀유지서약서, 퇴직 및 직무변경 관리, 상벌규정 5개로 구성되어있다.

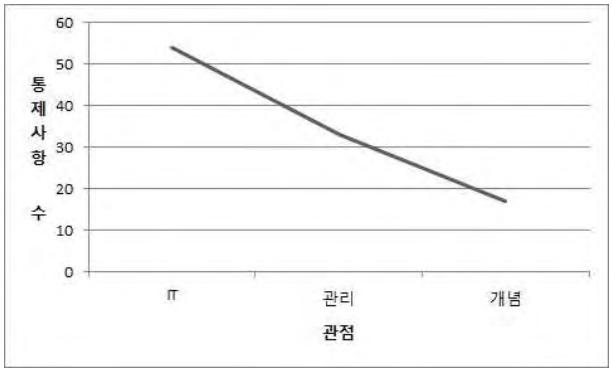
두 번째로 기업이 개인정보 보호 활동을 체계적 · 지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도인 PIMS(개인정보보호 관리체계)의 인적보안 통제사항은 개인정보취급자 지정 및 감독, 개인정보보호 서약, 퇴직 및 직무변경 관리, 상벌규정 4개로 구성되어있다.

세 번째로 기관의 주요 정보자산을 보호하기 위해 정보보호관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리 및 운영하기 위해 구축한 종합적인 체계인 G-ISMS(전자정부 정보보호 관리체계)의 인적보안 통제사항은 역할과 책임, 적격심사, 고용계약, 정보보호 수행관리, 정보보호 교육 및 훈련, 징계 규정, 퇴직 시 책임사항, 자산의 반납, 접근권한의 제거, 외부자와 관련된 위험파악, 민원인 접근에 대한 보안, 외주용역 계약에 대한 보안 12로 구성되어있다. 3가지 정보보호 관리체계의 인적보안 통제사항을 정리하면 아래와 같다.

<표 1> 기존 정보보호 관리체계 중 인적보안 통제사항

관리체계	세부사항		
ISMS	6. 인적보안	6.1 정보보호책임	6.1.1 주요 직무자 지정 및 감독
			6.1.2 직무분리
			6.1.3 비밀유지서약서
		6.2 인사 규정	6.2.1 퇴직 및 직무변경 관리
			6.2.2 상벌규정
PIM	5. 인적	5.1 개인정보취급자	5.1.1 개인정보취급자 지정 및 감독
S	보안	관리	5.1.2 개인정보보호서약
			5.1.3 퇴직 및 직무변경 관리
			5.1.4 상벌규정
G-ISMS	4. 인적보안	4.1 채용시 인적보안	4.1.1 역할과 책임
			4.1.2 적격심사
			4.1.3 고용계약
		4.2 재직시 인적보안	4.2.1 정보보호 수행관리
			4.2.2 정보보호 교육 및 훈련
			4.2.3 징계 규정
		4.3 퇴직 및 직무변경	4.3.1 퇴직 시 책임사항
			4.3.2 자산의 반납
			4.3.3 접근권한의 제거
		4.4 외부자 보안	4.4.1 외부자와 관련된 위험 파악
			4.4.2 민원인 접근에 대한 보안
			4.4.3 외주용역 계약에 대한 보안

이와 같이 각 정보보호 관리체계는 인적보안에 대한 통제사항을 보유하고 있지만, 전체 통제사항에서 인적보안 통제사항이 차지하는 비율은 매우 낮다. 그러므로 기존의 정보보호 관리체계들은 IT관점에서의 통제사항이 대부분이며, 인간중심보다는 기술중심의 체계라고 볼 수 있다. 본 논문에서는 가장 대표적인 정보보호 관리체계라고 할 수 있는 ISMS의 104개 통제사항을 IT적, 관리적, 개념적 관점으로 분류하였다. 각 관점별로 IT적 관점의 통제사항 54개, 관리적 관점의 통제사항 33개, 개념적 관점의 통제사항 17개로 분류되었다. IT적 관점의 통제사항이 54개로 절반이상을 차지함을 확인할 수 있다.



(그림 1) ISMS 통제사항의 관점별 분류

3. IoT환경에서 인간중심 보안관리체계 구축을 위한 효율적 인적자원관리 방법론 설계

효율적 인적자원관리 방법론 설계의 첫 단계로, 기존 정보보호 관리체계 인적보안 통제사항의 적합성을 따져 우선순위를 적용하였다. 이를 위해 3가지 정보보호 관리체계의 각 인적보안 통제사항들 중 서로 유사한 항목들을

도출하였다. 우선, ISMS의 '주요 직무자 지정 및 감독'항목은 PIMS의 '개인정보취급자 지정 및 감독'항목과 유사하였다. 또한 ISMS의 '비밀유지서약서'항목은 PIMS의 '개인정보보호 서약'항목과 유사하였다. 다음으로 ISMS의 '퇴직 및 직무변경 관리'항목은 PIMS의 '퇴직 및 직무변경 관리'항목과 G-ISMS의 '퇴직 시 책임사항', '자산의 반납', '접근권한의 제거'항목과 유사하였다. 마지막으로 ISMS의 '상벌규정'항목은 PIMS의 '상벌규정'항목과 G-ISMS의 '징계규정'항목과 유사하였다. 그러므로 위의 항목들은 효율적인 인적보안을 위한 우선적인 통제사항임을 확인할 수 있었다.

<표 2> 인적보안 공통 통제사항

공통사항	담당 직무자 지정 및 감독
	비밀유지서약서
	퇴직 및 직무변경 관리
	상벌규정

하지만 이러한 사항들은 인적자원의 심리는 고려하지 않고 단지 행위를 규제하고 있다. 그러므로 인간의 내면에 좀 더 접근한 보상제도와 지속적인 보안교육과 같은 사항이 추가적으로 필요하다.

4. 결론

본 연구에서 도출한 인적보안 사항들은 기존의 기술중심 보안관리체계에 인간의 내면을 고려한 사항들을 추가했기 때문에, IoT환경에서 인간중심 보안관리체계를 구축을 도울 수 있을 것으로 보인다. 향후 연구에서는 본 연구에서 도출한 인적보안 사항에 대한 타당성을 분석하여 검증할 필요가 있다.

감사의글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1018)

참고문헌

[1] 한국산업보안연구학회 "산업보안학" 박영사
[2] 민병설 "인원보안관리의 한계와 발전 과제" 「산업기술보호 이슈」 통권 제4호 한국산업기술보호협회
[3] 이태규 "산업정보유출 방지와 인적 보안관리" 성균관대학교 석사학위 논문
[4] 차인환, 김동현 "정보보호를 위한 인원관리 관리 방안" 추계종합학술대회지 제2권 제2호 한국전자통신학회
[5] 한국인터넷진흥원 "ISMS 인증기준 세부점검항목"
[6] 한국인터넷진흥원 "G-ISMS 인증기준 세부점검항목"
[7] 한국인터넷진흥원 "PIMS 인증기준 세부점검항목"