http://dx.doi.org/10.15207/JKCS.2015.6.4.139

산업융합환경에서 조직의 보안성 향상을 위한 센싱시스템 구축 연구

나원철[1], 이효직[2], 성소영[3], 장항배[4*]
[1,2,3]중앙대학교 대학원 융합보안학과, [4]중앙대학교 산업보안학과

A Study on Construction of Optimal Wireless Sensor System for Enhancing Organization Security Level on Industry Convergence Environment

Onechul Na[1], Hyojik Lee[2], Soyoung Sung[3], Hangbae Chang[4*]
[1,2,3]Department of Security Convergence, Graduate School, Chung-Ang University
[4,*]Department of Industrial Security, College of Business and Economics, Chung-Ang University

요 약 융합환경의 대표적인 도구인 WSN은 환경 구성의 기본 인프라에서부터 기업의 재고-생산-유통 관리에 이르는 비즈니스 모델까지 다양한 방향으로 활용되고 있다. 그러나, 안전하게 보호되어야 할 조직의 고유정보가 WSN과 같은 ICT와 융합되어 정보화 되면서 외부로 손쉽게 유출될 수 있는 위험에 놓여져 있다. 이에 따라, 안정적인 기업의 비즈니스를 위하여 보안성 있는 센서노드의 배치 전략이 필요한 시점이다. 조직의 보안현황을 고려하지 않은 단편적인 보안성 강화전략의 수립은 보안사고 발생 시 조직의 비즈니스 연속성에 큰 영향을 미친다. 그러나 그간의 조직의 보안성 진단을 위한 보안 수준평가 모형들은 대부분 기술적 중심의 측정방법이 진행되고 있으며, 관리적 요인과 환경적 요인에 대한 연구는 매우 부족한 상태이다. 따라서, 본 연구에서는 보안성 있는 센서노드 배치전략을 수립하기 위하여 융합환경을 기반으로 조직의 보안성을 진단하고 이에 따르는 전략수립방안을 연구하고자 한다.

• Key Words : 융합 환경, 무선 센서 네트워크 환경, 센서 노드 배치 전략, 보안현황 진단, 비즈니스 특성

Abstract WSN has been utilized in various directions from basic infrastructure of environment composition to business models including corporate inventory, production and distribution management. However, as energy organizations' private information, which should be protected safely, has been integrated with ICT such as WSN to be informatization, it is placed at potential risk of leaking out with ease. Accordingly, it is time to need secure sensor node deployment strategies for stable enterprise business. Establishment of fragmentary security enhancement strategies without considering energy organizations' security status has a great effect on energy organizations' business sustainability in the event of a security accident. However, most of the existing security level evaluation models for diagnosing energy organizations' security use technology-centered measurement methods, and there are very insufficient studies on managerial and environmental factors. Therefore, this study would like to diagnose energy organizations' security and to look into how to accordingly establish strategies for planning secure sensor node deployment strategies.

• Key Words : Convergence Environment, Wireless sensor networks environment, Sensor node deployment strategy, Security status diagnosis, Energy Organization, Business characteristics

*교신저자 : 장항배(hbchang@cau.ac.kr)
접수일 2015년 6월 8일 수정일 2015년 7월 26일 게재확정일 2015년 8월 20일

1. 연구배경

무선 센서 네트워크(이하 WSN)는 특정한 지역에 배치된 다수의 RFID, USN 등의 센서들을 통하여 환경정보를 수집하여 정보를 전달하는 환경이다[1]. WSN은 생태환경 조사에서부터 기업의 재고-생산-유통 관리에 이르는 비즈니스 모델까지 다양한 방향으로 확대되고 있다. 이러한 WSN를 기업의 비즈니스에 적용하기 위해서는 기술적인 요소뿐만이 아니라 관리적인 요소 또한 고려해야 한다[6]. 센서노드 배치는 효율적인 센서노드의 배치를 통하여 보다 적은 수의 센서만으로 적재적소에 배치하여 정확한 정보를 얻고자 하는 기술적 및 관리적 전략이다. WSN에서 센서노드의 배치는 중요한 문제 중에 하나이다. 그러나 현업에서는 센서 노드배치는 배치에 소모되는 비용과 시간을 줄이고자 일반적으로 무작위 배치(Random Deployment)를 적용해서 활용해왔다[14]. 그러나 무작위 배치는 센서 노드를 배치하고자 하는 핵심 대상에 규칙적으로 배치되는 것이 아니기 때문에, 임의적 배치로 인하여 센서 성능에 환경적 요소들이 많은 영향을 미치게 된다[11]. 그리하여, 센서 네트워크 노드 간 단절이 발생하고, 데이터 전송 지연이나 센서 노드의 메모리 제약에 따른 데이터 손실 등등 다양한 문제가 발생한다[3]. 이러한 문제를 해결하고자 이동물체에 대한 감지 및 배치 알고리즘, 트리기반 배치 알고리즘, 유전 알고리즘 등의 기술적 알고리즘을 통하여 센서노드 배치 최적화 전략을 수립하고 있다[2].

기업들은 조직의 정보화 환경에 적합한 형태로 센서노드를 배치함으로써 효율성 있는 재고 및 생산관리에 적용하여 비교우위의 비즈니스를 영위하기위해 노력하고 있다[10]. 그러나, 자율화된 센서노드를 활용으로 인하여 조직의 고유 정보가 노출될 수 있는 위험성을 내포하고 있다[8]. 이에 따라, 안정적인 기업의 비즈니스를 위하여 보안성 있는 센서노드의 배치 전략이 필요한 시점이다[4]. 한편, 지적 ICT 자산에 관한 의존도가 높은 조직은 WSN 도입에 따른 조직의 고유정보 유출을 방지하고자 기술적 센서 배치전략을 도입하고 있다[12]. 그러나, 조직의 비즈니스 프로세스에 따른 보안현황을 고려하지 않은 단편적인 기술적 센서배치 수행을 통한 보안성 강화전략의 수립은 보안사고 발생 시 조직의 비즈니스 연속성에 큰 영향을 미친다[7]. 그러나 그간의 조직의 비즈니스 프로세스를 분석하여 센서노드의 최적 배치를 위한 전략수립에 대한 연구는 미흡한 상황이다[15]. 더불어 조직의 보안현황 진단을 위한 기존의 보안 수준평가 모형들은 대부분 기술적 중심의 측정방법이 진행되고 있으며, 관리적 요인과 환경적 요인에 대한 연구는 매우 부족한 상태이다[13].

따라서, 본 연구에서는 보안성 있는 센서노드 배치전략을 수립하기 위하여 조직의 보안성을 진단하고 이에 따르는 전략수립방안을 연구하고자 한다. 세부적으로 보안현황 진단모형을 설계하고, WSN 환경을 기반으로 비즈니스를 영위하는 조직을 대상으로 실증분석을 수행하여 안정적인 센서노드 배치전략을 수립하도록 한다.

2. 선행연구

2.1 WSN 관련 선행연구

센서 장치들을 무선으로 연결하여 네트워크를 형성하는 WSN 기술은 사람을 중심으로 하던 정보 운용 형태를 확장하여 사람과 사물뿐만 아 니라 사물 간의 정보 공유를 언제 어디서든 가능하게 한다[9]. 이러한 WSN는 물리적 또는 환경적 조건을 모니터링 하기 위해 센서를 사용하는 독자적인 디바이스로 구성된 무선 네트워크로써 센서 노드, 게이트웨이, 라우터, PC 등으로 구성된다. WSN과 관련된 주요 연구들은 노드 배치, 스케쥴링, 위치인식 등의 WSN 시스템 운용 방법, WSN의 보안성 강화 방법, 실제 환경 도입을 위한 비즈니스 기반 WSN 시스템, WSN 내 노드 간 라우팅 방법 등에 대한 연구들이 주를 이루고 있다.

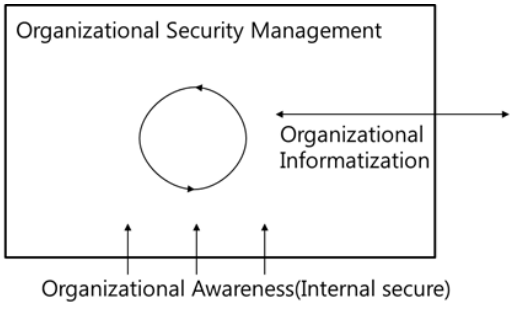
2.2 ICT 서비스 조직 분류 acl gortlawktks

ICT 서비스 조직은 비즈니스 형태에 따라 SI(System Integration), SM(system Management), DB(Data Processing), IR(ICT Rent), IP(Information)로 분류된다. SI/SM 업종은 ICT 기술을 활용한 시스템 자문 및 구축/기 구축된 시스템 운영 및 유지보수를 비즈니스 프로세스로 하고 있다. DB 업종 은 물리적형태의 자료를 디지털화하는 것을 주 비즈니스 프로세스로 보유하고 있다. 그리고 IR 업종은 보유하고 있는 시스템 및 솔루션(서비스) 등을 임대하는 사업을 비즈니스 프로세스로 하고 있다. 마지막으로, IP업은 ICT 기술을 통하여 생성된(가공된) 서비스 및 정보를 제공하는 사업을 주 비즈니스 프로세스로 운용하고 있다[5].

3. 융합환경을 고려한 선택적 보안관리 모델 개발

3.1 조직 보안현황 진단 개념적 체계

조직의 ICT 기술 내재화는 구성원, 구성원 간, 조직 외의 비즈니스 프로세스를 기반으로 하는 정보화 자산 보유현황을 기초로 한다. 조직이 보유한 정보화 자산을 기반으로 조직의 보안관리 지원환경을 구성하고 보안관리 활동을 하며, 조직의 보안 지속성관리를 수행한다. 이러한 조직 보안관리는 ICT 기술의 내재화와 유사한 구성으로써 구성원 보안인식, 조직 내 보안인식, 조직 외 보안인식에 의해 진행된다. 이와 같은 개념적 체계를 바탕으로 [Fig. 1]과 같은 조직의 보안현황을 진단하기 위한 개념적 체계를 설계하였다.



[Fig. 1] A conceptual system for diagnosing organizations security status

이러한 조직 보안현황 진단 개념적 체계를 바탕으로 전문가회의 및 선행연구를 참조하여 다음과 같은 진단영역에 대하여 진단항목 및 세부진단항목을 구성하였다.

- 정보화 현황 영역: 조직의 정보화현황 진단영역은 실질적으로 조직의 내 외부의 보안성을 진단하기 위한 요소들을 식별하는 영역이다. 선행연구, 문헌 및 전문가회의, 그리고 통계적 분석을 통하여, 조직들이 공통적으로 보유하고 있는 ICT 자산과 조직들의 비즈니스 특성을 분석하여 도출한 비즈니스 특화 ICT 자산으로 구분하였다. 세부적으로 공통적으로 모든 조직들의 정보화 성숙도에 따라 보유하고 있는 정보화 시스템을 식별하였다. 첫째, 조직의 내부에서 구성원 개인이 활용하는 정보화 시스템을 기능적 시스템으로 식별하였다. 둘째, 조직 구성원 간 정보화 시스템을 구축하는 전사시스템을 식별하였다. 셋째, 일반적으로 조직 외부의 비즈니스 프로세스를 영위하는 조직 간 정보화시스템을 식별하였다. 다음으로 조직의 비즈니스 특성을 분석하여 핵심 ICT 자산을 식별하였다.
- 보안관리 수행역량 영역: 보안관리 수행역량 진단영역은 식별된 공통 ICT 자산과 비즈니스 특화 ICT 자산을 기반으로, 조직이 ICT 자산을 보호하고 조직의 보안성 강화를 위한 활동을 수행할 수 있는 역량을 분석하는 영역이다. 국내외 보안관리 수행역량과 관련된 문헌분석 및 전문가 회의를 통하여, 보안관리 수행역량 영역을 진단하기 위한 영역을 보안관리 지원환경, 보안관리 활동, 보안 지속성관리 등의 세 진단항목으로 식별하였다. 우선, 보안관리 지원환경은 조직의 보안관리를 수행하기 위한 조직 차원의 지원역량 진단항목이다. 세부적으로, 보안관리를 위한 조직의 투자(예산), 보안관리 활동을 수행하기 위한 전문 조직, 보안관리에 대한 조직 수준의 정책의 세부 진단항목들을 식별하였다. 다음으로 보안관리 활동 영역은 실질적으로 모든 조직 구성원들의 활동을 진단하는 항목이다. 세부적으로 ICT 자산에 식별 및 관리체계 식별을 위한 자산 보안관리 활동과 조직 구성원(재직자 및 퇴직자)과 외부 인원에 대한 관리 활동, 그리고 물리적 보안활동 및 공통 ICT자산과 비즈니스 특화 ICT 자산에 대한 기술적 보안활동으로 구분하였다. 마지막으로 보안 지속성관리 영역은 보안관리 지원환경을 기반으로 보안관리 활동을 수행함에 있어서 조직의 지속적 성장을 위해 보안성을 관리하는 진단항목이다. 세부적으로 조직의 보안성 유지를 위한 운영관리 세부진단항목과 조직의 자산 유출 손실방지를 위한 사고대응 세부진단항목으로 구성된다.
- 보안인식 영역: 보안인식 진단영역은 조직을 구성하는 구성원들과 조직의 보안인식을 진단하기 위한 영역이다. 은 실질적으로 조직의 내 외부에 적용하기 위한 대상을 식별하는 영역이다. 조직의 보안인식과 조직의 보안역량의 영향성을 분석한 선행연구들을 분석하여 구성원 보안인식, 조직 내 보안인식, 조직 외 보안인식의 3개 진단항목으로 구성하였다. 세부적으로 구성원 보안인식 진단항목은 구성원 개개인의 보안에 대한 인식을 진단하고, 구성원의 보안과 관련된 도덕적 행위를 파악하며, 조직 구성원들 사이의 신뢰도를 진단한다. 그리고, 조직 내 보안인식을 진단하기 위하여, 보안

정책 및 절차에 대한 인식정도와 보안 예산 및 보안관리 활동에 대한 인식, 그리고 위험에 대한 인식을 세부 진단항목으로 식별하였다. 마지막으로 조직 외부로 연결되는 보안인식을 진단하기 위하여, 조직의 변화관리에 대한 인식, 보안관리체계 구축에 대한 인식정도를 세부 진단항목으로 식별하였다.

이러한 조직의 보안현황 진단 영역 및 진단항목, 그리고 세부 진단항목 구성요소에 대하여 진단하고, 보안성 값을 도출하기 위하여 보안전문가 10인의 AHP 분석을 통하여 <Table 1>과 같이 가중치를 도출하였다.

〈Table 1〉 Organization's security status diagnosis areas and items

Diagnosis area	Diagnosis item
Informatizatio n status (100)	Common ICT asset (37.5)
	Business ICT asset (62.5)
Security management performance competency (100)	Security management support environment (13)
	Security management activity (69)
	Security continuity management (18)
Security awareness (100)	Members' security awareness (50)
	Intra-organizational security awareness (30)
	Extra-organizational security awareness (20)

3.2 조직 보안현황 진단결과

조직 보안현황 진단을 위하여, 정보화 현황 진단영역은 진단항목을 세부진단항목으로 구성하여 민감도와 우선순위에 따라 진단하도록 설계하였고, 보안관리 수행역량 진단영역은 3개 진단항목과 9개 세부진단항목으로 구성하였으며, 보안인식 기반 진단영역은 9개 진단항목으로 설계하였다. 각 진단영역별 비율과 비교 수치는 문헌조사를 통하여 설계 후, 전문가회의(델파이회의)를 통해 가중치를 설계하여 구성하였다. 조직의 보안현황을 진단하기 위하여 비즈니스 프로세스에 종속된 ICT 자산이 명확히 구분될 수 있는 ICT 서비스 조직을 대상으로 설정하였다. 세부적으로 WSN 환경을 기반으로 SI/SM 및 DB업을 고유 비즈니스 프로세스로 수행하고 있는 A 조직과 SI/SM 및 IP을 고유 비즈니스 프로세스로 수행하고 있는 B 조직을 대상으로 설문조사를 실시하였다. 그 결과 <Table 2>와 같은 조직의 보안관리 현황을 진단하였다.

〈Table 2〉 Results of diagnosing organization's security management status

Diagnosis area	Diagnosis item	Organization A	Organization B
Informatization status (100)	Common ICT asset (37.5)	9.0	20.3
	Business ICT asset (62.5)	25.3	31.5
Total		34.3	51.8
Security management performance competency (100)	Security management support environment (13)	4.0	3.0
	Security management activity (69)	18.0	43.0
	Security continuity management (18)	0.0	6.0
Total		22.0	52.0
Security awareness (100)	Members' security awareness (50)	34.8	37.1
	Intra-organizational security awareness (30)	19.3	22.3
	Extra-organizational security awareness (20)	13.5	14.3
Total		67.6	73.7

정보화 현황 진단영역을 살펴보면, A 조직은 공통 ICT 자산과 비즈니스 ICT 자산 모두 평균 이하로 보유하고 있는 것으로 진단되었다. 이에 비하여, B 조직은 공통 ICT 자산과 비즈니스 ICT 자산은 평균 이상으로 보유하고 있는 것으로 분석되었다.

그리고, 보안관리 수행역량에 있어서, A 조직은 매우 미흡한 보안관리 수행역량을 보유하고 있는 것으로 진단되었으며, 특히 보안 지속성관리에 대해서는 현재 어떠한 역량 및 대응책도 고려하지 않고 있는 것으로 분석되었다. 반면에, B 조직은 보안관리 지원환경과 보안 지속성관리는 취약하지만 약간의 역량을 보유하고 있으며, 보안관리 활동에 대해서는 평균 이상의 역량을 보유하고 있는 것으로 분석되었다. 마지막으로 보안인식 진단영역을 살펴보면, A, B 조직은 보안인식 진단 항목에 대하여 모두 평균 이상의 보안인식을 보유한 것으로 분석되었다.

이와 같은 조직 보안 관리현황 진단결과를 분석해보면, A 조직의 경우 공통적으로 활용되는 다양한 ICT 자산의 보유 정도가 낮음으로 인하여, 정도에 맞는 수준의 보안관리 대응책 설계하면 되는 것으로 분석되었다. 반면에, 조직 규모에 비하여 공통 ICT 자산을 다량 보유한 B 조직은 다양한 보안관리 활동을 통하여 조직의 보안수

준을 유지할 필요성이 있는 것으로 분석되었다.

3.3 조직 보안현황 진단영역 별 상세분석

조직의 정보화 현황에 대하여 살펴보면 다음과 같다. 우선, 민감도는 높은 값, 우선순위는 낮은 값이 될수록 중요한 자산임을 나타내는 수치이다. A 조직은 SI/SM 및 DB 업을 비즈니스 프로세스로 수행하고 있기 때문에, 공통 ICT 자산은 기능적 시스템으로 재무회계시스템과 조직 간 시스템으로 전자결재시스템을 구축한 상태이다. 재무회계시스템의 민감도는 8, 우선순위는 2로 진단되었으며, 전자결제시스템의 민감도 2, 우선순위 6에 비하여 더 중요한 ICT 자산인 것으로 분석되었다. B 조직은 SI/SM 및 IP 업을 비즈니스 프로세스로 수행하고 있기 때문에, 공통 ICT 자산은 기능적 시스템으로 재무회계시스템과 인사관리시스템, 조직 간 시스템으로 전자결제시스템과 고객관계관리시스템을 구축한 상태이다. 이러한 B 조직의 가장 중요한 자산은 전자결제 시스템인 것으로 분석되었다.

〈Table 3〉 Results of diagnosing organizational informatization status areas and common ICT assets

Diagnosis item	Detailed diagnosis item (asset)		Organization A		Organization B	
			Sensitivity	Priority	Sensitivity	Priority
Common ICT asset	Functional system	Financial accounting system	8	2	5	2
		Personnel management system	-	-	5	5
	Inter-organization system	Electronic approval system	2	6	8	1
		Customer relationship management system	-	-	5	5

비즈니스 ICT 자산 진단결과를 살펴보면 다음과 같다. A 조직의 가장 중요한 비즈니스 ICT 자산은 데이터베이스로써 A 조직의 비즈니스를 영위하기위한 대표 비즈니스는 DB 업인 것으로 분석되었다. B 조직의 핵심 비즈니스 ICT 자산은 개인정보가 포함된 데이터베이스이며, 디지털콘텐츠도 중요한 자산으로 분류되었다. 이는 B 조직의 대표 비즈니스는 IP 업인 것으로 분석되었다.

〈Table 4〉 Results of diagnosing organizational informatization status areas and business ICT

Diagnosis item	Detailed diagnosis item (asset)		Organization A		Organization B	
			Sensitivity	Priority	Sensitivity	Priority
Business ICT asset	Collaboration space	Shared directory	4	3	2	6
		File server	3	1	5	1
		Project management program	4	2	5	5
	Input processing device (OCR, OMR and scanner etc.)		8	2	-	-
	Database		10	1	-	-
	IT application service supplied		-	-	5	3
	Digital contents	Web contents	-	-	8	2
		Image and video contents	-	-	8	2
	(Personal information) database		-	-	10	1

조직의 ICT 자산을 기반으로 각 조직의 보안관리 수행역량을 분석하면 다음과 같다. 보안관리 지원환경 진단항목에서 A 조직은 보안관리 정책, 조직, 투자에 있어서 골고루 역량을 보유하고 있는 반면에, B 조직은 보안관리 정책 역량만을 보유하고 있는 것으로 분석되었다. 이와 반대로, 보안관리 활동 진단항목에서는 A 조직은 퇴직자 및 외부인원관리에 대한 역량이 없는 반면에, B 조직은 전반적으로 보안관리활동 역량 수준이 양호한 것으로 분석되었다. 마지막으로 보안 지속성관리 진단항목에서 B 조직은 약간의 수행역량을 보유한 반면, A 조직은 운영관리 및 사고대응에 대한 수행역량이 없는 것으로 분석되었다.

조직의 보안인식을 살펴보면, A조직과 B 조직 모두 절반 이상의 수치를 보유하고 있는 것으로 분석되었다. 전체 세부진단항목에 있어서 B 조직이 A 조직에 비하여 비교 우위의 값을 보였다. 세부적으로 구성원 간 신뢰, 조직 보안예산, 보안관리 벤치 마킹에 대한 세부진단항목만 동일한 값으로 진단되었으며, 그 외의 모든 부분에 있어서 B 조직이 우위를 차지하고 있었다.

〈Table 5〉 Results of diagnosing organizational security management performance competency area

Diagnosis item	Detailed diagnosis item		Organization A	Organization B
Security management support environment	Security management policy (6)		2	3
	Security management organization (4)		1	0
	Security management investment (3)		1	0
Security management activity	Asset security management (13)		2	6
	Manpower management	Insider management: Incumbent (4)	2	4
		Insider management: Retiree (4)	0	3
		Outsider management (4)	0	4
	Physical security (15)		1	9
	Technological security	Common ICT asset security (6)	2	4
		Business ICT asset security (20)	8	13
Security continuity management	Operation management (4)		0	1
	Accident response (14)		0	5
Total			22.0	52.0

〈Table 6〉 Results of diagnosing the organizations' security awareness area

Diagnosis item	Detailed diagnosis item	Organization A	Organization B
Members' security awareness	Members' security awareness (21)	14.7	16.5
	Members' moral act (18)	11.3	11.8
	Reliability between members (11)	8.8	8.8
Intra-organization's security awareness	Organizational security policy and procedure (16)	10.1	11.2
	Organization's security budget (4)	3.2	3.2
	Organization's security management (6)	3.9	4.8
	Organization's risk management (4)	2.1	3.1
Extra-organization's security awareness	Organizational change management (10)	7.2	8
	Security management benchmarking (10)	6.3	6.3
Total		67.6	73.7

3.4 조직 선택적 보안관리 요소 설계

분석된 조직의 공통 ICT자산과 비즈니스 ICT 자산을 식별하고 이에 대한 중요도를 중심으로 조직의 보안인식을 기반으로 하여 보안관리 수행역량을 진단하였다. 세부적으로 A 조직의 보안관리 수행역량은 전반적으로 매우 취약한 것으로 나타났다. 특히, 퇴직자와 외부인원관리, 운영관리, 사고대응 대해 보안관리를 수행할 역량이 없는 것으로 나타났다. 이는 A 조직의 규모가 매우작음으로써 발생되는 것으로 분석되었으며, A조직의 핵심자산의 민감도와 우선순위를 고려하였을 때 보안사고 발생시 매우 위험한 상태인 것으로 분석되었다. 따라서, ICT 서비스 조직 A는 보안 지속성관리를 위한 외부 컨설팅을 수행할 필요가 있다. 반면에, 작은 규모로 인한 조직 구성원들은 규제로 인식되는 보안정책 및 절차를 제외하고 모두 보통~양호한 수준인것으로 나타났다. 이러한 보안인식 기반을 바탕으로 보안 수행역량의 향상이 필요하며, 우선적으로 조직의 핵심자산에 대한 기술적 보안과 보안관리 정책 수립이 우선적으로 필요하다.

그리고 B 조직의 보안관리 수행역량은 보통으로 분석되었고, 보안관리 수행역량의 기반이되는 조직원들의 보안인식 수준도 양호한 것으로 분석되었다. 그러나, 보안관리 활동을 비용소모의 개념이 아닌 투자 활동으로 인식할 필요성이 있으며, 이에 따라 보안관리 활동을 수행하는 전담인력의 배치가 필요하다.

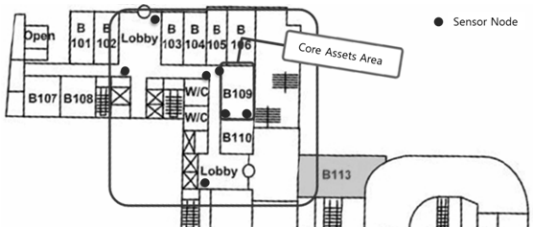
4. 결론

안전하게 보호되어야 할 조직의 고유정보가 WSN과 같은 ICT와 융합되어 정보화 되면서 외부로 손쉽게 유출될 수 있는 위험에 놓여져 있다. 이에 따라, 안정적인 기업의 비즈니스를 위하여 보안성 있는 센서노드의 배치전략이 필요한 시점이다. 따라서, 본 연구에서는 보안성 있는 센서노드 배치전략을 수립하기 위하여 조직의 비즈니스 프로세스를 기반으로 보안성을 진단하고 이에 따르는 전략수립방안을 연구하였다. 그 결과는 다음과 같이 세 가지로 요약할 수 있다.

- 조직 보안현황 진단 모형을 설계하였다. 세부적으로 조직 정보화 현황, 보안인식, 보안관리를 진단할 수 있는 개념적 체계를 설계하고, 사례분석을 위한 모형을 설계하였다.

- 설계된 진단모형을 ICT 서비스 조직인 두 조직을 대상으로 사례분석을 수행함으로써 보안관리 통제항목을 설계하였다. ICT 서비스 조직의 비즈니스 자산의 보유정도와 그에 대한 활용도를 측정하였으며, 조직의 공통 ICT 자산 및 비즈니스 ICT 자산에 대한 정보화현황을 분석하였다. 그리고, 조직의 보안관리 수행역량을 분석하기 위하여 보안관리 지원환경, 보안관리 활동, 보안지속성관리 측면에서 진단을 하였으며, 이러한 조직을 구성하는 구성원들의 보안인식에 대한 실증연구를 수행하였다.
- 마지막으로 분석된 조직의 공통 ICT자산과 비즈니스 ICT 자산을 식별하고 이에 대한 중요도를 중심으로 조직의 보안인식을 기반으로 하여 보안관리 수행역량을 향상시킬 수 있는 방안을 제시하였다.

조직의 보안관리 현황을 진단함으로써, 조직의 WSN 도입에 따른 ICT 융합환경 현황을 파악할 수 있다. 그리고, 이러한 신규환경 도입에 따른 보안성을 강화해야하는 부분을 도출할 수 있다. 또한 보안성을 한층 강화시키기 위한 조직 구성원들의 보안인식을 확보할 수 있다. 이와 같은 결과를 조합하여, 조직의 정보화 환경과 보안관리 핵심 부분, 그리고 조직 구성원들의 보안인식을 고려하여 조직 내 적재적소에 보안성이 강화된 센서노드 배치 전략을 수립하고 효율 및 효과성 있는 보안관리를 수행함으로써 지속적 성장이 가능한 조직구조를 구축할 수 있을 것이다. 세부적으로 민감도와 중요도가 높으나, 보안관리상태가 취약한 공통 및 비즈니스 ICT 자산을 위주로 센서노드 배치의 간격을 좁힘으로써 보안관리 전략과의 연계성을 만들어야 하며, 보안인식과 보안관리가 취약한 부분에 대한 위험관리의 방안으로 최적화된 센서노드 배치 전략을 수립해야 한다.



[Fig. 2] Sensor node deployment strategy according to organizations' security management status (example)

향후 연구로는 보안성이 강화된 센서노드 배치전략을 기술적 요소와 함께 구현함으로써, 균형 있는 조직의 WSN 환경 구축에 대한 연구를 수행하고자 한다.

ACKNOWLEDGMENTS

본 연구는 미래창조과학부산하 정보통신기술진흥센터(IITP)의 방송통신정책연구센터(CPRC) 지원사업의 연구결과로 수행되었음 (R0880-15-1007)

REFERENCES

[1] A. D'osta and A. M. Sayeed. Collaborative signal processing for distributed classification in sensor networks. In Proc. IPSN, Palo Alto, CA, 2003.

[2] Adam Silberstein, Rebecca Braynard, Carla Ellis, Kamesh Munagala, and Jun Yang, 2006, A Sampling-Based Approach to Optimizing Top-k Queries in Sensor Networks, Data Engineering, 2006. ICDE '06. Proceedings of the 22nd International Conference on, pp. 68, 2006.

[3] C. Moallemi and B. Van Roy, Distributed optimization in adaptive networks. In Proc. NIPS, Vancouver, BC, Canada, 2003.

[4] Da Veiga A, Eloff JHP., An information security governance framework, Information Systems Management, Vol. 24, No. 4, pp. 361-372, 2007.

[5] Jonggu Kang, Jaewhan Lim, Hongjoo Lee, Hangbae Chang, A Study on Classification of Information Asset Considering Business Process Characteristics for Small IT Service Organization, The Journal of Society for e-business Studies, vol. 16, No.4, pp. 97-108., 2011.

[6] Ken H. Guo, Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis, Computer&Security, Vol. 32, pp. 242-251, 2013.

[7] Martins A, Eloff JHP., Information security culture, IFIP/SEC2002. In: Security in the information society, Boston: Kluwer Academic, pp. 203-214,

2002.

[8] Michael Rabbat and Robert Nowak, Distributed Optimization in Sensor Networks, IPSN '04 Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 20-27, 2004.

[9] Mohamed Younis, Kemal Akkaya, Strategies and techniques for node placement in wireless sensor networks: A survey, Ad Hoc Networks, Vol. 6, Issue 4, pp. 621 - 655, 2008.

[10] Niki Trigoni, Yong Yao, Alan Demers, Johannes Gehrke, Rajmohan Rajaraman, Multi-query Optimization for Sensor Networks, Vol. 3560, pp. 307-321, 2005.

[11] Robbins S, Odendaal A, Roodt G., Organizational Behaviour - Global and Southern African perspectives, Cape Town: Pearson Education South Africa, 2003

[12] Robert Nowak and Urbashi Mitra, Boundary Estimation in Sensor Networks: Theory and Methods, Lecture notes in computer science, Vol. 2634, pp. 80-95, 2003

[13] Ruighaver AB, Maynard SB, Chang S. Organisational security, culture: extending the end-user perspective. Computers and Security, No. 26, pp. 56-62, 2007.

[14] Kyoung-nam Kim, Lee, Jae Moon, Sunghyuck Hong, MyounJae Lee, Convergent Secure Wireless Sensor Network Routing Algorithm, Journal of the Korea Convergence Society, Vol. 6, No. 1, pp. 65-70, 2015.

[15] Myung-Seong, Yim, Development of Measures of Information Security Policy Effectiveness To Maximize the Convergence Security, Journal of the Korea Convergence Society, Vol. 5, No. 4, pp. 27-32, 2014.

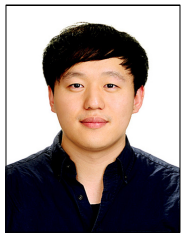
저자소개

나 원 철(One-Chul Na) [학생회원]

- 2014년 8월 : 한성대학교 컴퓨터공학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석사과정

<관심분야> : 정보보호, 융합보안, 개인정보보호

이 효 직(Hyo-Iik Lee) [학생회원]



- 2015년 2월 : 숭실대학교 글로벌통상학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석·박사 통합과정

<관심분야> : 정보보호, 산업보안, 보안문화, 클라우드보안

성 소 영(So-young Sung) [학생회원]

- 2013년 8월 : 상명대학교 경영학과 졸업(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과 석사과정

<관심분야> : 산업보안, IT협업, 개인정보보호

장 항 배(Hang-Bae Chang) [정회원]

- 2006년 2월 : 연세대학교 정보시스템관리 전공(박사)
- 2007년 3월 ~ 2012년 2월 : 대진대학교 경영학과 조교수
- 2012년 3월 ~ 2014년 2월 : 상명대학교 경영학과 조교수
- 2014년 3월 ~ 현재 : 중앙대학교 산업보안학과 부교수

<관심분야> : 중소기업 정보보호, 정보 오남용 및 유출 방지, 성과분석 체계