IoT시대의 기업 융합보안 전략에 대한 연구

노 종 호*, 이 종 형**, 권 헌 영***

요 약

사물인터넷(IoT) 시대의 본격화와 더불어, 융합보안이라는 개념은 어디서나 쉽게 접하고 있다. 그러나 기존의 융합보안이라는 개념이 IoT 특성을 제대로 반영하고 있다고 보기에는 다소 어려움이 있다. 이에, 기존의 융합보안 개념을 IoT 특성을 고려하여 보완된 개념을 제시하였다. 더불어, 융합보안의 개념 모델 재정립과 기업의 융합보안전략을 수립하는 데 있어 필요한 거버넌스 체계와 기술적 요인에 대해 기술하였다.

A Study on the Enterprise security convergence strategy in the IoT(the Internet of Things) Era

Jong-ho Noh*, Jong-hyeong Lee**, Hun-yeong Kwon***

ABSTRACT

In the age of full scale IoT, concept of “security convergence” has been popularized widely. However, it is not clear whether current “security convergence” concept reflects IoT characteristics and traits. In this thesis, a new concept, complementing “security convergence” concept researches up to date, has been suggested considering IoT characteristics. Required governance methodology and key technical factors are suggested for re-establishment of “security convergence” concept and for enterprise security strategy development.

Keywords : Security Convergence, IoT, Enterprise Security Strategy

접수일(2017년 5월 15일), 수정일(1차 : 2017년 6월 29일), 게재확정일(2017년 6월 30일)

* 고려대학교 정보보호대학원 박사과정
** 고려대학교 정보보호대학원 석사과정
***고려대학교 정보보호대학원 교수(교신저자)

1. 서 론

오늘날 빠르게 발전하는 기술의 진화로 전반적으로 기업보안 체계에 대한 혁신이 요구되어지고 있다.

현재 대부분의 기업에서는 사이버공간에만 국한하여 예방 및 대응하고 있는 정보보안부서와 물리적인 입출입자 관리 중심의 물리보안 부서를 개별 운영하고 있다.

본 연구에서는 IoT시대에 맞는 기업보안 체계를 융합보안 관점에서 찾아보고자 한다.

이를 위해 먼저 전통적인 융합보안에 대한 개념 및 모델을 살펴본다. 기업의 융합보안 개념모델을 재정의하고 융합보안 거버넌스 방안을 제시한다. 그리고, 현재의 기업보안 체계에 대한 고찰을 토대로 기업의 융합보안 개념과 모델을 새롭게 재정의 하고, 그에 따른 최적의 거버전스 전략을 제시하고 결론을 맺는다.

2. 관련 연구동향

IoT가 대중화 되기 전인 2000년대 초반에는 산업보안을 위해 물리보안 시스템과 사이버보안 시스템간의 상관관계 분석기술을 통해 융합관제할 수 있는 방안을 제시하였다[11].

최근에는 산업별로 IoT와 사이버물리시스템(CPS)의 도입이 확산됨에 따라 새로운 융합환경에서 보안사고에 대한 선제적 대응과 더불어 사이버거버넌스 체계 모델정립이 본격적으로 연구되고 있다[12].

3. 이론적 배경

3.1 융합보안의 개념적 이해

천재(天災)에 대비하는 활동을 말하는 '안전(safety)'과는 달리 '보안(security)'은 인재(人災), 즉, 범죄 등 사람의 행위로 인해 피해가 발생하는 상황을 방지하는 활동을 말한다.

또한 천재라 하더라도 사람의 과실로 발생한다면 그것은 인재로 볼 수 있을 것이며, 따라서 이를 방지하는 활동 또한 보안의 범주에 속한다 할 것이다. 이러한 점들을 종합할 때 '보안'이란 "범죄로부터 생명, 신체, 재산을 보호하고 사회의 안녕과 질서를 지키는 제반 활동"이라고 정의할 수 있다[1].

이러한 보안의 전통적 개념, 특히 산업기술이나 기밀 등의 정보를 보호하기 위한 목적의 산업보안은 지켜야 할 관리대상과 관리자를 기준으로 한 물리보안과 정보보안으로 구분되었다.[2]

종래의 물리보안 및 정보보안으로의 구별에서 나아가, 각 보안 요소들을 이용한 상호 협력 및 통합 체계를 구축·운용하기 위한 융합보안의 개념이 등장하게 되었다.

지식경제부에서는 2008년에 'Securing Knowledge Korea 2013'를 발표하는 자리에서 '정보보호 산업'을 '지식정보보안 산업'으로 재정의 하였고 '융합보안'이라는 용어를 처음 사용하였다. 보안산업을 정보보안, 물리보안, 융합보안으로 구분하고, 융합보안이란 '물리보안과 정보보안 간의 융합 또는 보안기술이 비 IT기술과 융복합되어 창출되는 보안제품 및 서비스'를 뜻한다고 정의하였다.

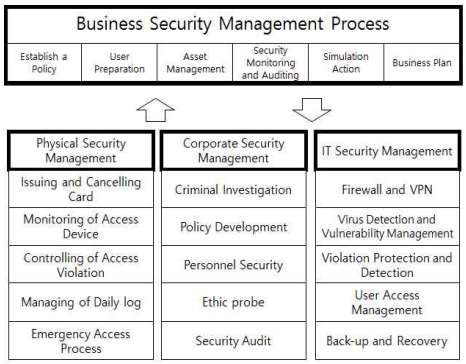
더불어, 해외 여러 기구에서는 <표 1>과 같이 융합보안의 개념을 설명하고 있다[4].

<표 1> Overseas Convergence Security Model

Sorting	Definition of Convergence Security
ASIS	Identify the interdependencies and security risks between business functions and processes that exist within the corporate, and establish business solutions that can manage them appropriately.[7] *ASIS(American Society for Information Science) International
OSE	Physical and IT Security move toward the same objective, process, and architecture.[8] Objective means cost reduction and operational efficiency improvement. *OSE(The Open Security Exchange)
Gartner	Physical and Information Security are similar, linked, or having the same processes and functions.[6]
COSO Online	Convergence traditional operational risk management capabilities to manage risk across the enterprise cost-effectively.[9]

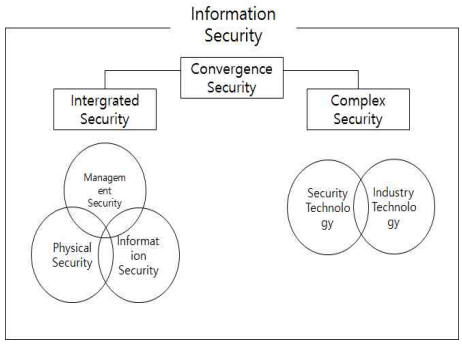
3.2 기업의 융합보안 개념모델

AESRM(Alliance for Enterprise Security Risk Management) 서는 서로 다른 조직의 인적자원, 프로세스, 기술들이 물리적, 기술적, 관리적 보안사고 예방, 탐지, 대응 주기와 서로 기능적으로 교차하는 융합보안 모델을 제시하였다[3].



(그림 1) AESRM's Model

국내에서는 김정덕 연구원 등이 융합의 개념을 조직 내 보안요소들을 상호 연계하여 보안의 효과성을 높이고자 하는 '통합적' 개념과 보안기술을 다른 산업기술들과 융화시켜 새로운 기술을 창출하는 '복합적' 개념으로 아래와 같이 구분하였다[5].



(그림 2) Kim's Convergence Security Model

3.3 IoT의 개념 및 특징

IoT는 인간과 사물, 서비스 세 가지 분산된 환경요소에 대해 인간의 명시적 개입없이 상호 협력적으로 센싱, 네트워킹, 정보처리 등 지능적 관계를 형성하는 사물 공간 연결망이다.

또한, IoT시대의 특징은 정보의 초연결사회, 비정보의 정보화, 정보의 대량화 등으로 정리할 수 있다. 이를 기업관점에서 보면 IoT환경에서 센싱되는 다양한 정보를 모두 포함하는 보안관리가 필요하다.

따라서 이러한 IoT시대에는 물리보안, 정보보안이라는 이분법적 구분보다는 '정보흐름'을 기준으로 하여 획득되는 정보의 통합을 바탕으로 한 정보보안과 비정보보안으로 구분하는 게 필요하다.

4. 융합보안의 전략방향

4.1 기업의 융합보안 개념 및 모델

앞에서 제시한 IoT 개념과 특징을 고려하여 기업의 융합보안 개념을 아래와 제안한다.

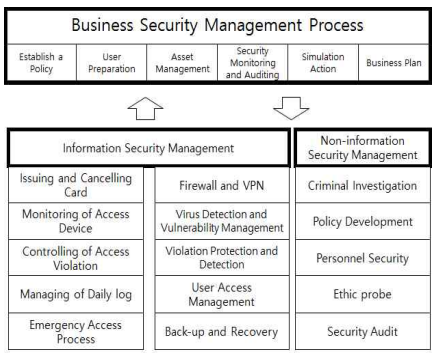
(1) 협의 : 보안 비용의 감소, 운영 효과성 및 효

율성을 향상하기 위해, 보안 위험 발생 수단과 방법을 중심으로 한 정보보안과 비정보보안과의 상호 협력 및 통합

(2) 광의 : 보안 비용의 감소, 운영 효과성 및 효율성을 향상하기 위해, 보안 위험 발생 수단과 방법을 모두 포괄하는 개념으로 관리보안(프로세스보안)과의 상호 협력 및 통합(인적 자원에 대한 관리 등의 필요성이 부각되는 현실 반영)

이를 토대로 본 연구에서는 기존 AESRM 모델을 기초로 정보보안과 비정보보안으로 구분하여 (그림 3)과 같이 제안한다.

기존의 물리보안영역에 있던 관리대상은 IoT기기를 통한 자료 수집, 운용, 모니터링이 가능하기 때문에 정보보안 관리 영역에 포함을 하였으며, 기타 영역을 비정보보안 관리영역으로 표기하였다.



(그림 3) Convergence Security Model in IoT

4.2 융합보안 거버넌스

기업의 융합보안 관리체계는 기업경영의 리스크 최소화를 위한 정보의 기밀성, 무결성, 연속성 보호를 위해 전략적 방향을 제시하고 목적달성, 위험관리, 자산관리 등을 모니터링 하고 피드백하는 것이다.

앞으로 기업의 핵심자산은 유무형의 정보이며 이를 효과적이고 효율적으로 관리하는 리더십, 조직구조, 프로세스로 구성되어야 한다.

이를 통해 정보의 단절로 인한 정보유출 리스크를 최소화 해야 한다.

현재 대부분의 기업에서 이루어지고 있는 거버넌스는 주요 영역별로 새로운 체계로 전환이 필요하다.

<표 2> Changes in Convergence Security Governance

Sorting	Problem	Improvement Direction
Asset type	Tangible assets	Intangible and tangible assets
Risk-Management	Physical/Information	Convergencing Physical and Information
Monitoring	Logs, events, etc. for security equipment	Logs, events, etc. for all IT equipment
Ownership	CISO	Expanded to individual information holders
Check Cycle	Regularly	Constantly
Control Principle	Block-based	Monitoring-based

기존의 보안장비에 대한 로그분석 중심에서 탈피하여 회사의 핵심 Value Chain상에서 모든 정보의 연동을 강화하고, 데이터의 기밀성, 무결성, 가용성을 보장하는 동시에 관련된 모든 정보의 흐름에 대한 이상 징후를 모니터링 함으로써 철저한 사전 예방과 더불어 문제 발생시 실시간 조치를 해야만 한다.

일일, 주간, 월간 형태의 점검주기도 시스템의 자동화된 알람과 리포트 기능을 활용하여 유무선 인프라를 활용하여 24시간 365일 점검하는 체계로 운영 되어야 한다.

또한, 무조건적인 차단중심의 통제원칙에서 탈피하여 업무의 효율성을 고려하여 최소한의 차단원칙을 기준으로 감시중심 체계로 전환이 필요하다.

더불어, 보안인력은 보안 엔지니어를 넘어 비즈니스 이해를 바탕으로 회사의 전체 리스크 매니저로서 역할로 반드시 확장하여야 한다.

다시 말해, 융합보안 전문가는 비즈니스 전반에 걸친 이해를 바탕으로 전사 리스크를 최소화하는 모든 활동하는 담당자로 규정 되어야 하며 CISO도 기존의 보안분야에 국한한 총괄책임자에서 탈피하여 회사의 리스크 총괄 책임자로서 역할로 탈바꿈 하여야 한다.

이를 위해 우선적으로, 조직구조의 근본적인 개선이 필요하다. 기존의 물리보안부서와 정보보안부서간 정보의 단절이 없도록 이를 효율적으로 지원할 수 있는 일원화된 조직체계의 개편이 필수적이다,

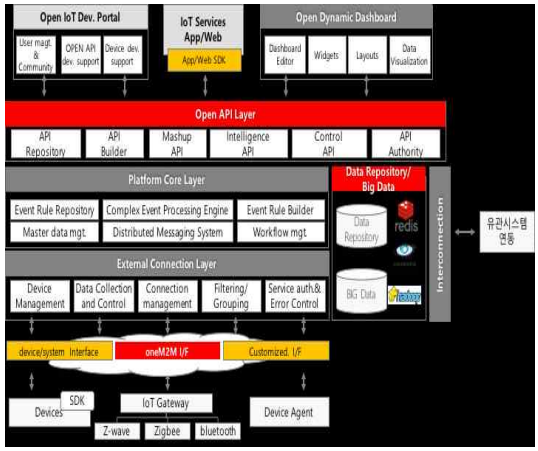
또한, 프로세스 측면에서 기존의 물리보안 정책, 정보보안 정책으로 구성된 개별 관리체계에 대한 개선이 시급하다. 물리보안, 정보보안의 정보가 상호 연동될 수 있도록 정보흐름 및 관리체계의 통합화를 회사정책에 명확히 반영하고 실천하여야 한다. 무엇보다도 중요한 것은 CEO의 Sponsorship이다.

기업의 근본적인 목적이 지속성장에 있는 만큼 이의 핵심적인 리스크 관리에 대해 CISO에 전폭적으로 위임하여야 한다.

4.3 기술적 구현방안

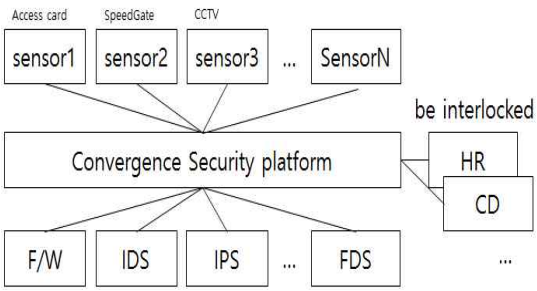
오늘날 IoT 플랫폼은 개방형 플랫폼을 지향하고 Big Data 분석엔진을 정착하고 글로벌 IoT data간의 교류를 위해 글로벌 협력을 빠르게 진행하고 있다.

기업의 물리보안 영역의 대부분의 장비는 IP화 되어있고, 리더기와 더불어 유무선 네트워크를 통해 실시간 정보가 흐르고 있다. 기존의 보안장비에 대한 이벤트 정보중심의 융합보안관제 플랫폼에 덧붙여 이에 대한 센서 수집정보와 분석정보를 연동하여 빅데이터 기반으로 실시간 정보를 활용한다면 보안정책 설계 및 운영의 효율화를 통해 사후관리 뿐만 아니라 사전예방을 철저히 할 수 있다.



(그림 4) IoT Platform Conceptual Diagram

대부분의 기업에서는 출입카드, 스피드게이트, CCTV 등 IoT 센서정보와 다양한 보안 시스템의 수집된 데이터를 융합플랫폼에 반영된 빅데이터 엔진을 통해 분석 활용하는 융합보안 인프라를 구축할 수 있다.



(그림 5) Convergence Security Conceptual Diagram

여기에 기업의 인사시스템, 문서관리시스템 등 기간계 시스템과 실시간 연동함으로써 보안업무의 효율성을 증대시킬 수 있다.

5. 결 론

본 연구는 IoT시대의 기업 융합보안 전략수립을 위한 융합보안 개념의 재정의, 융합보안 모델링, 거버넌스의 방향성에 대해 살펴보았다.

이를 각 기업의 환경에 맞게 적의 적용하고 관리한다면 기업의 보안 리스크를 예방하고 해결할 수 있다고 본다.

예를 들어, 지난 2016년 4월에 발생한 공무원 시험 준비생인 일반인이 5차례에 걸쳐 아무런 제재 없이 청사 사무실에 들어가 담당자PC를 해킹한 사고같은 경우, 본 연구에서 제시한 융합보안 관리체계 및 시스템 구축을 통해 근원적인 사고예방에 기여할 수 있을 것이다.

다만, 본 연구결과를 통해 실제적으로 산업현장에 적용하여 그 효과성을 검증하는 것이 필요하나, 이에 대해서는 후속연구에서 기업환경에 맞는 보안투자평가 모델을 만들고 실제 적용을 함으로써 정량적, 정성적인 결과값을 도출하여 증명하고자 한다.

참고문헌

[1] Lee Chang-Moo, A Study on the Conceptual Definition of Industrial Security, The Journal of Korean Association for Industry Security, The Korean Association for Research of Industrial Security, 2011. 6.

[2] Jeon Jeong-Hoon, A study on the classification systems of domestic security fields, Journal of the Korea Society of Computer and Information 20(3), 2015.3, 81-88,

[3] Booz, Allen, Hamilton, "Convergence of Enterprise Security Organizations", The Alliance for Enterprise Security Risk Management (AESRM), November 8, 2005.

[4] Woo Kwang Jea, “Research trend and Cocentualization of Defense Industry Security from Convergence security perspective” Korea Convergence Security Association, Vol 15, issue 6, pp.69-78, Oct. 2015.

[5] Kim Jungduk, Kim kunwoo, Lee Yongduk, “the concept of security convergence and approach method”, Journal of The Korea Institute of information Security & Cryptology, pp. 68-74, Dec. 2009.

[6] J.Kang, J. Lee, C. Hwang, and H. Chang. “ The study on a convergence security service for manufacturing industries”, Telecommunication Systems, Vol. 52, No. 2, pp. 1389-1397, 2013.

[7] Deloitte, "The Convergence of Physical and Information Security in the Context of Enterprise Risk Management", The Alliance for Enterprise Security Risk Management, 2007.

[8] The Open Security Exchange (OSE), "Physical/IT Security Convergence: What It Means, Why It's Needed, and How to Get There", 2007.

[9] Scalet S.D., "Convergence: Case Study", COSO online, 2005. W. Diffie and M.E, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[10] Nicole S. Latimer-Livingston, "Let's Get Physical What Clients Are Asking About the Integration of Physical and Logical (IT) Security", Gartner, November 9, 2007.

[11] Ha Ok Hyun, “A Study on Convergence Security Control System for Industrial Security”, Korea Convergence Security Association, Vol 9. issue 4, pp.1-6, 2009

[12] Kim Dong Hee, “A Study on the Establishment of Cyber Security Governance in

the Age of Convergence", Korea University, Doctoral thesis, 2017.

[저 자 소 개]

노 종 호 (Jong-ho Noh)
1994년 8월 전남대학교 전산통계학과 학사
2009년 2월 연세대학교 정보대학원 IT경영전략 석사
2016년 9월 ~ 고려대학교 정보보호대학원 정보보호학과 박사과정
현 KT IT 기획실 정보보안단
email : parker.noh@gmail.com

이 종 형 (Jong-hyeong Lee)
2011년 2월 성균관대학교 전자전기공학과 학사
2014년 2월 건국대학교 법학전문대학원 전문석사
2016년 9월 ~ 고려대학교 정보보호대학원 정보보호학과 석사과정
email : jonghyeong23@gmail.com

권 헌 영(Hun-yeong Kwon)
2008년 3월 ~ 2015년 8월 광운대학교 법과대학 교수
2015년 9월 ~ 고려대학교 정보보호대학원 교수
email : khy0@korea.ac.kr