# 융합 IT 환경의 물리적 취약요인에 관한 연구

전정훈* · 안창훈** · 김상춘***

## 요 약

최근 국내·외 여러 산업분야에서는 사물 인터넷(internet of things)과 클라우드 컴퓨팅 서비스(cloud computing service), 빅 데이터(big data) 등과 같은 융합 IT기술들의 등장으로 보안에 대한 중요성이 점차 높아지고 있다. 이러한 가운데 산업 보안(Industrial Security) 시장은 점차 커질 것으로 전망하고 있으며, 보안 기술의 진화뿐만 아니라 취약성 또한 증가할 것으로 예상되고 있다. 따라서 다양한 IT 환경으로의 진화로 인한 물리적 취약요인의 증가는 여러 산업분야들의 보안성을 결정짓는 잣대가 된다고 해도 과언이 아니다. 이에 대해 본 논문은 융합 IT환경에서의 물리 보안 기술들과 적용 사례, 물리적 취약요인들에 대해 조사 및 분석해 봄으로써, 향후, 물리적 침해 및 공격에 대한 대응 방안 마련에 활용될 것으로 기대한다.

# Study on the physical vulnerability factors in the convergence IT environment

Jeon Jeong Hoon* · Ahn Chang Hoon** · Kim Sang Choon***

## ABSTRACT

Recently, many domestic and foreign industries is increasing gradually in the importance of security such as the emergence of a Convergence Information Technology(internet of things, cloud computing service, big data etc). Among these techniques, the industrial security market is expected to grow gradually and the evolution of security technologies, as well as vulnerabilities are also expected to increase. Therefore, an increase in physical vulnerability factors it is no exaggeration to standards that are determining the security of industrial security. In this paper will be analyzed to the physical security technology and case study, physical vulnerability factor. Thereby this is expected to be utilized as a basis for the countermeasure of physical corresponding infringement and attack in a future.

**Key words : Industrial Security, Convergence Security, Internet of Things, Ubiquitous, Vulnerability factors, Physical Security**

접수일(2016년 2월12일), 수정일(1차: 2016년 2월23일), 게재확정일(2016년 2월29일)

★ 본 논문은 2015년도 강원대학교 대학회계 학술연구조성비로 연구하였음(관리번호-201510026) This study is supported by 2015 Research Grant from Kangwon National University (No. 201510026)

* 동덕여자대학교 컴퓨터학과(책임저자)

** ㈜컴엑스아이/대표이사

*** 강원대학교 정보통신공학전공(교신저자)

# 1. 서 론

최근 국내 여러 산업분야에서는 ICT를 결합한 융합 IT환경의 구축에 많은 투자를 하고 있다. 이와 같은 변화는 사물 인터넷(internet of things)과 클라우드 컴퓨팅(cloud computing), 빅 데이터(big data)와 같은 융합 IT환경을 통한 시간적, 경제적 효율성에 따른 것이다. 특히, 스마트 폰(smart phone)과 테블릿(tablet) PC와 같은 스마트 기기는 다양한 산업분야의 현장과 일상생활에서 실시간성과 편의성, 정확성 등을 제공하며, 보급 및 확산에 촉매제 역할을 하고 있다. 반면에 융합 IT환경으로의 변화로 인해 다양한 취약요인의 증가와 보안의 분류체계 변화를 예고하고 있다.

국내 보안 분류체계는 그림1과 같이 정보 보안(information security)과 물리 보안(physical security), 융합 보안(convergence security)으로 구분하며, 이중 융합 IT환경에 있어 융합 보안이 부상하고 있다. 융합 보안은 정보 보안과 물리 보안의 융합 또는 IT기술과 융·복합 시에 발생하는 위협들을 해결하는 기술을 의미하며, 정보와 물리 보안의 통합 개념인 융합 IT환경의 물리적 보안이라 정의할 수 있다. 여기서 융합 보안을 구체적으로 세분화해 본다면, IT기술과 연관된 물리 보안과 그렇지 않은 것으로 나누어 볼 수 있다. 이러한 배경에는 최근 여러 산업분야에서 IT기기들을 생산과 사무 환경에 적용하는 사례들이 증가하면서 산업현장 또한 변화해 감에 따라, 통합된 융합 IT환경으로의 보안체계로 진화해가고 있으며, 융합 보안의 중요성이 점차 높아지고 있기 때문이다[5][6].

이에 본 논문은 점차 융합 IT환경으로 변화하고 있는 상황에서 물리적 보안 위협 요인들을 IT와의 연관성에 따라 분석해 봄으로써, 향후 사물 인터넷과 클라우드 컴퓨팅, 빅 데이터 기술들이 융합된 또 다른 형태의 환경에서 대응 기술 개발과 취약성 분석을 위한 연구 자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 융합 IT환경의 보안 동향과 물리적 침해 유형, 물리적 보안 기술들에 대해 알아보고, 3장은 융합 IT환경의 물리적 취약요인을 알아본다. 그리고 4장은 융합 IT환경에서의 물리적 취약요인의 분류와 대응 방안을 분석하고, 마지막 5장에서 결론 부분으로써 이글을 마치도록 한다.

# 2. 관련 연구

## 2.1 융합 IT환경으로의 변화

국내 여러 산업분야에서는 생산과 서비스 등에 스마트 기기와 각종 IT 관련 신기술들을 활용하고 있다. 일부 산업 현장에서는 드론(dron)과 같은 사물 인터넷 기술을 사용하고 있으며, 금융 분야는 생체인식과 같은 인증 기술을 적용하고 있다[1][2]. 이밖에도 보다 신속하고, 정확한 정보들을 수집 및 전달하는데 효과적이며, 경제성과 편의성 등 다양한 장점들로 인해, 여러 산업 분야에서는 각 분야에 적합한 융합 IT환경들을 구축하고 있다. 최근 미국에서 개최되었던 국제 전자제품박람회인 CES(consumer electronics show)를 통해 전 세계 가전 기업들의 새로운 트랜드(trend) 및 이슈가 잘 반영되어 있음을 알 수 있다. 박람회는 전자제품에 사물 인터넷과 ICT를 결합한 제품들을 소개


(그림 1) 지식정보보안산업

하고 있으며, 제품들을 통해 커넥티드(connected) 중심의 기술 이동과 이종 기기들 간의 융합이 가속화되고 있음을 알 수 있다. 또한 유망분야에 대해 스마트 홈(smart home)과 웨어러블(wearable)기기, 드론(drone), 로봇(robot), 스마트 카(smart car), 스마트 TV, 3D 프린팅을 6대 이슈로 꼽고 있다[1][2][3].

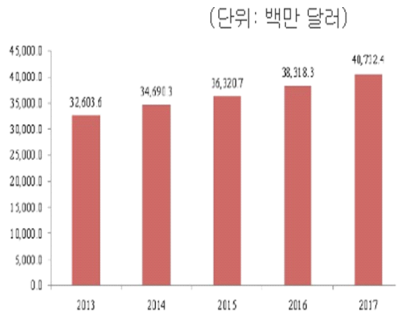
## 2.2 융합 환경에서 물리적 보안의 시장 동향

<표 1> 지식정보보안산업 기술 분류[3]

| 구분 | 정의 | 대표제품 |
|---|---|---|
| 정보보안 | ·컴퓨터 또는 네트워크상의 정보훼손, 변조, 유출 등을 방지하기 위한 보안기술 | 디지털 포렌식 툴<br>DDoS대응장비<br>안티바이러스 |
| 물리보안 | ·개인의 신변안전 및 주요 시설물의 안전한 관리환경 구축을 위한 개인 식별, 영상감시 및 재난·재해 등의 방지를 위한 보안기술 | 영상감시솔루션<br>지능형 카메라<br>바이오인식 |
| 융합보안 | ·IT기술과 타산업간 융·복합 시에 발생되는 보안위협을 해결하기 위한 보안 기술 | 차량블랙박스<br>U헬스케어보안장비<br>스마트미터 보안칩 |

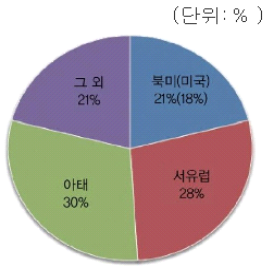
표1은 지식정보보안 산업 기술의 분류를 나타낸 것으로 정보와 물리, 융합 보안으로 정의하고 있다. 이 중 융합 보안의 대표 제품들을 살펴보면, 차량과 기록 및 감시, 증거자료의 결합체인 '차량 블랙박스', 'U-헬스케어 보안장비', '스마트 미터보안' 등을 포함하고 있는데, 이들을 통해 국내 여러 산업분야의 동향을 알 수 있다[3].

특히 물리 보안은 융합 및 커넥티드화 되고, 경계가 모호한 상황에서 융합 IT환경에 적합한 새로운 분류체계가 필요하다. 따라서 현 분류체계에서는 물리 보안과 융합 보안을 구분하고 있지만, 현실을 고려해 볼 때, 이미 물리 보안은 융합 보안에 포함되었다고 볼 수 있다.



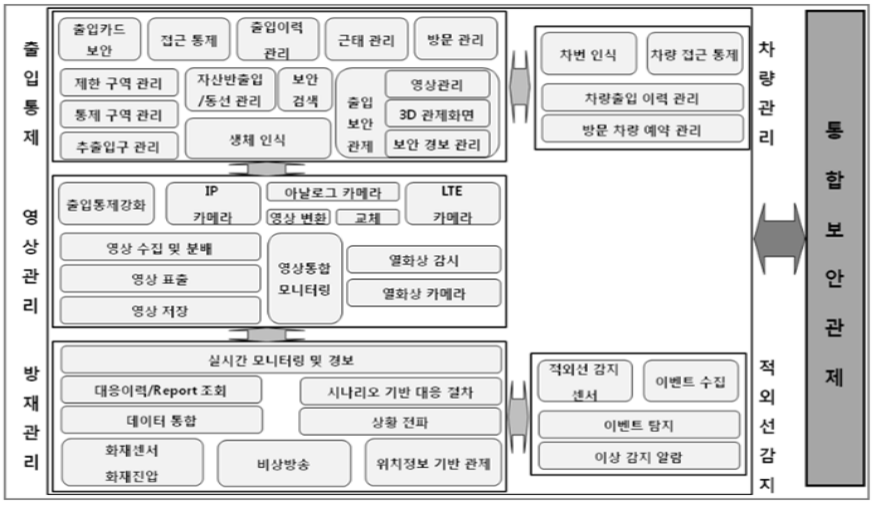

(그림 2) 미국
물리보안시장전망(2013~2017년)[4]

융합 IT환경의 물리적 보안 시장을 살펴보기 위해 물리 보안 시장의 동향을 통해 알아본다. 2008년 '인터넷데이터센터(IDC:internet data center)' 자료에 따르면, 미국의 물리 보안은 그림2에서와 같이 2013년에 세계 시장의 약 3,680억 달러(약460조원) 중 38%인 1,408억 달러였으며, 국내 보안 시장도 18조4000억원 중 19%에 해당하는 3조5000억원으로 추산되고 있다[4][7]. 최근 미국의 물리 보안 시장은 전 세계 시장의 약 18%를 차지하고 있으며, 경기회복과 더불어 2017년에는 점진적인 상승세가 이어질 것으로 전망하고 있다[2].




(그림 3) 전 세계 물리보안
시장 비중[2]

또한 전 세계 물리 보안 시장을 살펴보면, 그림3과 같이 아시아 태평양 지역의 비중이 가장 큰 것을 볼 수 있는데, 이는 국내 물리 보안 기업들에게 지역적, 경제적으로 유리한 위치로 시장 진출의 기회를 가질 수 있을 것으로 기대되며, 앞으로의 융합 환경에서의




(그림 4) 물리보안 및 통제보안 관제를 통한 융합보안의 기본 틀 구성(예시)
(출처LG CNS)

물리적 보안 시장은 더욱 확대될 것으로 전망된다.

## 2.3 융합 IT환경의 물리적 보안 기술 동향

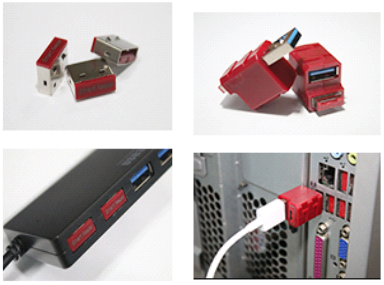
물리적 보안 기술은 표1과 같이 기존의 CCTV나 카메라, 출입 통제와 같은 단순 기능에서 바이오인식과 센서(sensor) 등 IT를 응용한 보다 진보한 제품들로 개발되고 있다. 이러한 동향은 사물 인터넷이나 스마트 기기의 보급으로 보다 융합된 IT환경에 맞는 진화로 볼 수 있다.

이에 대한 사례로는 인가된 자에 의한 침해 공격을 방지하기 위해 사전에 설정된 보안 등급에 따라, 엘리베이터의 동작을 제한 및 통제하는 기술이 사용되고 있는가 하면[1], 단순 녹화 기능만을 갖고 있던 CCTV는 보다 선명해지고, 지능화된 기능을 갖추어 침입자의 동선 및 패턴의 분석이 가능하게 되었다. 또한 지능형 자동차는 기존 바이오 인증기술을 통해 운전자를 인식할 수 있게 되었다.

이밖에도 IT장치들은 온라인 회선에 있어, 공격자의 악용을 방지하기 위해 네트워크 방지 모듈을 통해, 그림5와 같이 불필요한 네트워크 포트(port)나 USB 포트의 사용을 제한하기도 한다[8]. 이와 같은 보안 기술들은 융합 IT환경에서 여러 기술들이 융합된 기술로서, 앞으로 표2의 '사물인터넷 유럽 연구 클러스터(IERC:IoT European Research Cluster)'에서 추천한 사물 인터넷의 주요 기술들과 연계된 융합 IT환경의 물리적 보안 기술들을 예상해 볼 수 있다[4]. 다음 장에서는 융합 IT환경의 물리적 취약요인에 대해 알아본다.

<표 2> IERC의 사물 인터넷의 주요 기술 이슈[2]

| 구분 | 2012 ~ 2020 주요 이슈 |
|---|---|
| 식별 기술 | 사물의 식별ID, 네트워크 주소 등에 대한 체계 및 융합 |
| 서비스 아키텍쳐링 | 엑스트라넷을 포함한 글로벌 스케일 서비스 구조 |
| IoT 아키텍쳐 | 암호화, 인증, 위치인식, 에너지관리 |
| 인프라 기술 | 크로스 도메인간 통합 및 관리 기술 |
| 응용 기술 | 데이터 서비스를 위한 OpenAPI 기술 |
| 서비스 기술 | IoT-aware process 모델링 및 실행, QoS |
| 통신 기술 | Longer range, 상호호환성, 저전력 프로토콜 |
| 네트워크 기술 | Grid, 클라우드, 애드혹, 하이브리드, 메시 등 |
| SW 및 알고리즘 | 자가 제어/관리, 마이크로OS, 상황인지, 확장성 등 |
| 하드웨어 | 초저전력 칩/센서, 초박막 디스플레이, 안테나 등 |
| 데이터 및 신호처리 | 센서온톨로지, 자동 컴퓨팅, 인지 컴퓨팅 |
| 검색 기술 | 스케일러블 검색, IoT 브라우저 |
| 에너지 기술 | printed batteries, Photovoltaic cells, 무선전력 |
| 보안 기술 | Cognitive security, 자가관리적 보안, Localized Security |
| Societal 측면 기술 | Ambient Computing, 스마트 어시스턴스 |
| 소재 기술 | 카본 나노튜브, 컨덕티브 폴리머, 전도성 잉크 등 |



(그림 5) USB 및 네트워크 포트 폐쇄락[8]

## 3. 융합 IT환경의 물리적 취약요인

최근 사물 인터넷과 클라우드, 센서 네트워크, 빅 데이터 등과 같은 다양한 IT 신기술들과 각종 스마트 기기와의 결합으로 산업 분야의 IT환경은 크게 개선되고 있으나, 이에 따른 취약요인도 함께 증가하고 있다. 융합 IT환경의 물리적 취약요인은 IT환경과의 연관성에 따라 두 가지로 분류해 볼 수 있으며, 이러한 물리적 취약 요인들에 대한 대응 또한 온라인상에서와 차이를 갖는다. 온라인상의 해킹 공격은 변형 공격에 대응하기 위해 기존의 대응 기술을 업그레이드하거나 유사 기술로 대응하지만, 물리적인 취약요인에 대한 대응은 서로 다른 기술들을 복합적으로 사용함으로써 대응이 가능하다.

융합 IT환경 이전의 물리 보안은 대부분 주체가 사람으로 동작과 행위를 통제하거나 모니터링 하는 단순 기능의 제품들이지만, 융합 IT환경의 물리적 보안은 공격자가 IT환경에 접하기 전, 취약요인을 제거하여, 정보의 접근을 사전에 차단하는 점에서 차이를 갖는다. 따라서 이와 같은 융합 IT환경에서 물리적 대응 기술을 통해 취약요인들을 접점에서 제거함으로써, 제2차, 3차 공격을 사전에 예방할 수 있다.

최근 스마트 기기와 사물 인터넷 기기들의 보급이 확산되면서, 자동차와 항공, 선박 등 여러 산업분야에서 활용도가 높아지고 있으며, 드론을 이용한 해킹 공격과 원격지 CCTV의 모니터링, 지문 인식 정보의 크랙(crack), 도용 등 융합 IT환경에서의 치명적인 취약요인들이 추가적으로 새롭게 나타나고 있다. 이에 융합 IT환경의 취약요인들에 대한 물리적 대응 기술은 점차 산업분야의 보안성을 판단하는 잣대가 되고 있다고 해도 과언이 아니다.

## 4. 물리적 취약요인의 분류와 대응

물리적 보안과 침해는 IT환경과의 연결성에 따라 두 가지로 나누어 볼 수 있는데, 여기서 '연결성'이란 물리적 보안 장치와 IT기기 또는 인터넷, 통신매체, 또 다른 기술 간의 결합 등과의 연결을 의미한다. 본 장에서는 IT환경과 비 IT환경에 따른 침해 요인과 대응 방안을 알아본다.

### 4.1 비 IT환경의 물리적 취약요인 및 대응

비 IT환경의 물리적 보안장비는 대부분 단일 기능이거나 IT기술과는 연계성이 없다. 그리고 비 IT환경의 물리적 침해는 주체가 대부분 사람이며, 침해 대응은 주체의 동작이나 행동을 감시 및 모니터링 한다. IT환경과의 차이는 IT환경과의 '연결성' 여부로 구분한다. 이러한 비 IT환경의 물리적 침해와 대응 방안에 대해 그림4의 내용을 다음과 같이 정리하였다[5].

- 출입 관리에 따른 침해:


(그림 6) 방문자 엘리베이터 층수제한[9]

카드키는 비인가자의 건물전체에 대한 출입을 통제하기 위해 방문자의 이동경로를 방문 층으로 제한함으로써, 피해를 최소화하는데 목적이 있다. 그림6은 출입구에서 부여받은 카드키로 인가층만을 방문할 수 있도록 제한하고 있지만, 다른 사람들과 함께 탈 경

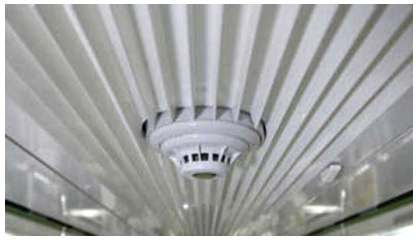
우, 출입통제가 무용지물이 되는 취약성이 있다. 따라서 대응책으로 엘리베이터에 대한 담당 인원의 추가 배치 등의 방안이 있다.

- 영상 관리에 따른 침해 유형:

(그림 7) CCTV 카메라[10]

비인가자의 동선 및 움직임을 그림7의 카메라를 통해 감시함으로써 보안시설이나 장소 등에 대한 안전을 모니터 하는 것이 목적이다. 그러나 취약성으로 카메라의 해상도 및 회전반경의 사각지대, 데이터의 보존기한 등의 문제가 발생한다. 따라서 대응책으로 관리자는 영상장비의 특성과 영상 데이터에 대한 보존기한 등의 관리와 충분한 모니터링 인원의 배치가 필요하다.

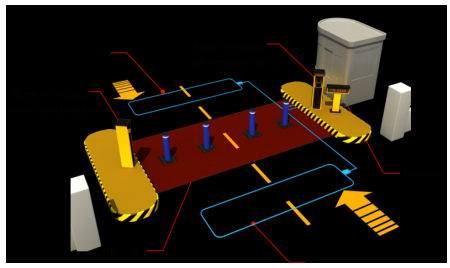
- 방재 관리에 따른 침해 유형:



(그림 8) 화재감지기[11]

시설 및 통제구역은 화재로 인한 피해 및 침해에 대한 취약요인을 포함하고 있다. 따라서 이에 대한 대응책으로 그림8과 같은 화재 감지기를 통한 알람 및 통보 체계를 통해 대응이 가능하다. 그러나 취약성으로 노후로 인한 오동작이나 고의적인 동작강제 등의 문제점이 있지만, 정기적인 점검과 CCTV와 같은 2차 물리보안장비를 함께 배치함으로써 동작강제 등의 취약성을 보완할 수 있다.

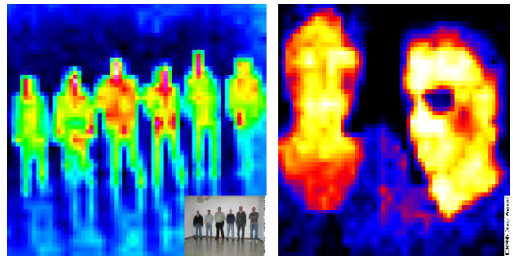
- 차량 관리에 따른 침해 유형:



(그림 9) 차량 통제[12]

비인가자에 의한 출입을 차단하기 위해 그림9와 같이 차량과 사람에 대한 통제를 하는 것이 목적이다. 출입을 통제하기 위해서는 사람에 의한 통제가 보다 효율적이지만, 카메라만으로도 관리하기도 한다. 그러나 취약성으로는 차량으로 진입시도를 할 경우와 통제지역 외의 출입이 되겠다. 따라서 대응책으로 통제 및 관리자는 카메라, 탐지견, 반사거울, 탐지기 등 2차, 3차의 물리적 보안 기술을 이용하거나 충분한 인원 배치가 있다.

- 적외선 관리에 따른 침해 유형:



(그림 10) 적외선 감지 카메라 통제[13]

인가자 및 비인가자에 대한 발열자와 야간 침입자에 대한 식별의 취약요인이 있다. 이에 대한 대응책으로 적외선 감지 카메라를 통해 발열자의 식별과 야간 침입자에 대한 동선 및 움직임을 모니터링 함으로써 대응이 가능하다. 대응 대상으로는 사람과 동물(온혈)

이 된다.

이와 같이 비 IT환경의 물리적 침해와 대응은 사람 외에도 연기와 같은 무형 것도 주체가 될 수 있으며, 서로 다른 대응 기술들을 복합적으로 사용하여 대응이 가능하다. 다시 말해 1차적으로 잠금장치의 취약요인을 CCTV를 통해 2차적으로 대응할 수 있다. 이러한 대응은 온라인상에서의 해킹공격과 차이를 갖으며, IT환경과의 연결이나 연계성이 없이 고유 기능만을 수행한다.

## 4.2 융합 IT환경의 물리적 취약요인 및 대응

융합 IT환경의 물리적 보안은 IT환경과 연결 또는 연계성을 갖는다. 그리고 이에 대한 물리적 침해의 주체는 사람이지만, IT환경의 구성요소가 대상이 되며, IT환경으로의 연결 접점에 위치해 이를 차단함으로써 대응이 가능하다. 그러나 물리적 취약요인의 대응 실패 시, IT환경과 연결된 공격으로 연계가 가능해진다. 융합 IT환경으로의 변화에 이와 같은 물리적 보안 기술은 점차 증가할 것으로 전망되며, 이러한 융합 IT환경의 물리적 침해 및 대응 사례들을 다음과 같이 정리해 볼 수 있다.

- 네트워크 포트(network port)의 물리적 침해:

(그림 11) 네트워크 포트 폐쇄락[14]

인가자와 비인가자로부터 네트워크의 무단 사용을 통제하는 것이 목적이다. 그러나 취약성으로는 이들에 의해 네트워크 포트를 오용 및 공격에 사용하는 문제가 발생한다. 따라서 대응책으로 그림 11에서와 같이 불필요한 네트워크 포트에 대해 통제하기 위해 포트를 막아버림으로써 2차적인 사고를 예방할 수 있다. 여기서 공격목표는 불필요 포트를 이용한 내부 연결이 되며, 침해접점은 네트워크 포트의 허용 여부가 된다. 그리고 취약성의 주체는 사람과 포트가 된다.

- USB 포트의 물리적 침해 :

(그림 12) USB 포트락[15]

인가자 및 비인가자로부터 USB를 이용한 정보의 유출을 방지하는 것이 목적이다. 그러나 취약성으로 타인의 USB뿐만 아니라 자신의 USB에 복사되어 있는 악성프로그램으로 인해 유출이 가능하다. 따라서 대응책으로 그림12와 같이 USB 포트락을 사용하여 불필요한 USB 포트에 대해 다른 사용을 금지하기 위해 포트자체를 막아버림으로써 2차적인 사고를 예방할 수 있다. 여기서 공격목표는 불필요 포트를 이용한 내부 정보유출이 되며, 침해접점은 USB 포트의 사용 허용 여부가 된다. 그리고 취약성의 주체는 사람과 포트가 된다.

- 시스템의 저장매체에 대한 물리적 침해:

(그림 13) 시스템 폐쇄락[16]

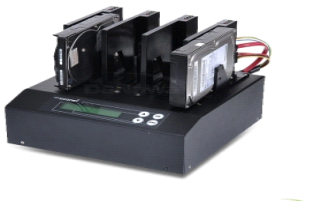
인가자 및 비인가자에 의해 타인의 시스템을 사용하는 사례가 빈번히 발생한다. 이에 시스템의 사용자를 통제하는 것이 목적이다. 그러나 취약성으로 내부 사용자의 경우, 신뢰를 전제로 대부분 사용을 허용하고 있어 정보의 유출이 쉽게 발생한다. 따라서 대응책으로는 그림13과 같이 시스템에 대한 접근을 차단하기 위한 폐쇄락을 사용해 제한하며, 이동 시스템에 대해 통제할 수 있다. 여기서 공격목표는 시스템 점유를 통한 2차적인 공격이 되며, 침해 접점은 시스템의 사용 허용 여부가 된다.

- 시스템 구동을 위한 물리적 침해:

(그림 14) 마우스 지문인식[17]

비인가자보다는 인가자에 의해 타인의 시스템을 사용하여, 정보를 유출하는 사례로 시스템 사용을 제한하는 것이 목적이다. 그러나 취약성으로는 내부자에 의해 시스템 사용을 요구받았을 때, 부득이하게 허용함으로써 유출문제가 쉽게 발생한다. 따라서 대응책으로는 그림14와 같이 마우스에 생체 인식장치를 이용해 사용을 제한한다. 여기서 공격목표는 시스템 점유를 통한 2차적인 공격이 되며, 침해 접점은 마우스 사용을 통한 시스템 점유가 된다.

- 저장매체에 저장된 데이터의 물리적 침해:



(그림 15) 하드디스크 삭제[18]

폐기된 하드디스크의 복사 및 복제, 파기 등에 따른 사례가 빈번히 발생하는 취약요인이 있다. 이에 대해 하드디스크의 데이터를 복원하지 못하도록 삭제하는 것이 목적이다. 그러나 취약성으로는 데이터의 완전 삭제방법에 일반적으로 알려져 있지 않아 오래된 하드디스크의 교체 등으로 데이터를 복원하는 사례가 발행하고 있다. 따라서 대응책으로 그림15와 같이 '디가우저'와 같은 전자기를 이용한 데이터 삭제를 통해 복원이 불가능하도록 한다. 여기서 공격목표는 저장매체로부터의 정보획득이 되며, 침해접점은 데이터 복원 허용여부가 된다.

- 모니터에 대한 물리적 침해:


(그림 16) LG 전자의 모니터 보호 필름[19]

인가자 및 비인가자에 의해 모니터를 통해 작업 내용이 유출되지 않아야 한다. 그러나 취약성으로 사회공학적 공격에 의해 쉽게 유출되는 사례가 나타나고 있다. 따라서 대응책으로는 그림16과 같이 모니터에 보안 필름을 붙여 시야 각도를 제한함으로써, 사회공학적 공격에 대응한다. 여기서 공격목표는 정보 유출을 통한 2차적인 공격이 되며, 침해 접점은 모니터의 열람 허용 여부가 된다.

이와 같이 IT환경의 물리적 취약요인은 대응 실패시, IT와 연계된 공격이 가능하며, 온라인상의 공격도 가능해 진다. 그리고 비 IT환경의 물리적 취약요인보다는 피해 규모가 크고 치명적이기 때문에 이에 대한 대응이 침해 접점에서 차단되어야 한다. 따라서 향후 융합 IT환경이 모든 산업분야로 확산될 경우, 융합

IT환경의 물리적 취약성은 더욱 증가할 것이며, 이에 따른 대응 기술에 대한 수요 증가와 시장 확대가 예상된다.

## 5. 결 론

최근 다양한 산업분야들은 IT기기 등을 활용한 융합 IT환경의 변화와 함께 여러 기술들을 응용하여 빠르게 진화하고 있다. 그러나 다양한 진화와 함께 공격기술도 함께 진화하고 있어, 융합 IT환경에서의 취약성 증가가 예상되고 있는 가운데 이에 따른 시간적 경제적 손실 규모도 증가할 것으로 전망된다. 특히, 다양한 산업분야에서의 신속성과 정확성, 실시간성을 고려한 각종 스마트 기기들의 활용은 융합 IT환경에서의 취약요인들의 증가로 이어져, 이에 대한 기술개발과 대응 방안 마련이 시급함을 알 수 있었으며, 융합 IT환경과 결합한 물리적 보안의 수요 증가와 이에 따른 시장 확대가 예상되고 있다.

따라서 본 논문은 융합 IT환경에서의 물리적 보안 기술과 동향, 사례를 알아보고, 취약요인에 대한 침해와 대응기술들을 통해, 융합 IT환경에서의 물리적 취약요인 경감과 함께 대응방안 마련, 사고예방, 보안기술의 개발 등에 유용한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후, 융합 IT환경에서의 개인 프라이버시(privacy)를 고려한 물리적 보안 기술의 개발과 함께, 폭넓은 산업분야의 IT관련 물리적 보안 위협요인 및 취약성 분석에 대한 체계적이고, 지속적인 연구를 통해 대응 방안 마련 및 새로운 보안 기술개발이 이뤄져야 할 것으로 사료된다.

## 참고문헌


[1] 전정훈, “사물인터넷의 보안 위협 요인들에 대한 분석,” 융합보안학회, vol.15, no.7, 2015.12

[2] 전정훈, “사물인터넷 기술동향과 전망에 관한 연구,” 융합보안학회, vol.14, no.7, 2014.12

[3] 정수환외 21명, “Part.10 지식정보보안,” 산업통산자원부, 한국산업기술평가관리원, 2015

[4] 미래인터넷팀, “미(美) 국제 전자제품 박람회(CES) 2015 동향분석,” 한국인터넷진흥원, Internet & Security Focus, pp.30-44, 2015.1

[5] http://blog.lgcns.com/856, “물리보안과 정보보안이 만나‘융합보안‘으로 진화하다,” LGCNS, 2015.7.27

[6] http://www.globalwindow.org/gw/overmarket/GWOMAL020M.html?BBS_ID=10&MENU_CD=M10103&UPPER_MENU_CD=M10102&MENU_STEP=3&ARTICLE_ID=5030165&ARTICLE_SE=20302, “물리적 보안시장을 통해 보는 미국 산업동향,” KOTRA 2015.7.16

[7] http://www.securityworldmag.co.kr/wsr/wsr_view.asp?idx=684&page=20&part_code=03&search=&searchstring=, “융합보안의 정의 및 적용사례,” 시큐리디월드 통권 제164호, 2015.11.

[8] http://www.newsis.com/ar_detail/view.html?ar_id=NISX20150203_0013454866&cID=10402&pID=10400, “[중기소식]컴엑스아이, 시스템본체 물리보안제품 개발,” Newsis, 2015.2.3

[9] http://m.monopalace.com/home/info/?dd=TRcnSipHMg==, “엘리베이터 보안”, 모노팰리스

[10] http://korean.hd-cctvcameras.com/sale-358744-black-color-osd-hd-cctv-video-camera-sony-effio-dome-camera-6000v-surge-protection.html, “CCTV”, 보스콤(boscom)

[11] http://news.sbs.co.kr/news/endPage.do?news_id=N1001080783, “화재경보기” sbs뉴스

[12] http://www.iysc.co.kr/bbs/board.php?bo_table=lock&wr_id=7, “차량출입통제”, ㈜와이에스씨

[13] http://www.sensolution.co.kr/product/pro08_5.htm, “적외선 감지”, (주)센솔루션

[14] http://www.comxi.co.kr/, “네트워크 포트락”, (주)컴엑스아이

[15] http://www.bodnara.co.kr/bbs/article.html?num=91472, “usb 포트락”, (주)컴엑스아이

[16] http://accessories.ap.dell.com/sna/PopupProductDetail.aspx?c=kr&l=ko&cs=krbsd1&sku=461-10216&price=32,900, “시스템 잠금장치”, ㈜dell

[17] http://digent.kr.ec21.com/GC03555781/제품정보.html, “마우스 지문 잠금장치”, (주)디젠트

[18] http://www.hardcopy.co.kr/shop/goods/goods_view.php?&goodsno=2010021710, “하드삭제 장치”,

㈜DZONEI
[19] http://www.betanews.net/article/536290, “모니터 보호필름”, Betanews IT· 경제신문

## [저 자 소 개]

**전 정 훈 (Jeong-hoon Jeon)**

2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr

**안 창 훈(Chnag Hoon Ahn)**

1998년 2월 경기대 무역학과 졸
2001년 ~ 현재: 컴엑스아이 대표
2008년 ~ 2013년: KPC 전문위원

e-mail :cosmohoon@comxi.com

**김 상 춘(Sang-Choon Kim)**

1999년 8월 충북대 이학박사
1983년 ~ 2001년: ETRI 선임
2001년 ~ 2010년: ETRI초빙연구원
2001년 ~ 현 강원대학교 정교수

e-mail : kimsc@kangwon.ac.kr