기업의 산업기밀정보 유출예방에 관한 연구: 사물인터넷 활용을 중심으로

최관* · 김민지**

요 약

이 연구는 사물인터넷 디바이스로 인해 발생가능 한 기업의 주요 핵심정보의 유출위협에 대해 살펴보고 유출예방을 위한 방안들을 관리보안과 기술보안 측면에서 살펴보는 것이 목적이다. 연구결과로서 관리보안측면에서는 첫째, 기업내부로 출입이 인가된 모든 사람들에 대해 사물인터넷 디바이스로 기업데이터가가 유출될 수 있음을 교육하고 주요 출입이 허가된 구역에 출입시점부터 사물인터넷 기기의 사용을 제한하는 가이드라인을 비치할 필요가 있다. 둘째, 사용자 요청 혹은 기업 자체의 보안운영 가이드라인을 마련할 필요가 있으며, 무선인터넷 공유가 가능한 전자기기에 무선인터넷 모듈을 도입시기부터 제거할 필요가 있다. 기술보안측면에서는 첫째, 컴퓨터에 대한 제어 솔루션으로서 기업정보들이 주로 저장되고 있는 컴퓨터 및 서버에 매체제어 솔루션 활용을 통해 사물인터넷 디바이스와 공유되는 경로를 대상으로 통제 솔루션을 실시해야 한다. 둘째, 네트워크에 대한 접근통제로서 네트워크에 공유된 사물인터넷 디바이스와 등록된 사물인터넷 디바이스의 현황을 정기적으로 확인하는 과정을 통해 보안관리 차원의 누수를 최소화해야 한다. 셋째, 암호화 방안으로서 컴퓨터, 서버 등의 정보자산에서 데이터 저장 및 암호화가 함께 이루어짐으로써 생성된 데이터가 외부로 불법적으로 유출되는 것을 예방하여야 한다.

Industry Secret Information Leakage Prevention : Focus on the Utilization of IoT

Choi Kwan* · Kim Minchi**

ABSTRACT

The purpose of this study is to examine possibilities of industry secret information leakage through IoT devices and to prevent information leakage from the perspective of administrative and technique security. From the administrative security perspective, first, it is important to face the possibility of industry information data leakage through anyone who can access companies and should establish guidelines to limit the use of IoT devices when entering companies. Second, security management guideline should be prepared by companies or upon user's request and use of any electronic devices sharing wireless internet connection should be eliminated or restricted. From technique security perspective, channels that sharing IoT devices in computers should be controlled since industry secret information are stored in computers and servers. Furthermore, IoT devices that accessing wireless internet network or devices that already registered should be regularly checked in order to minimize any information leakage. Lastly, data and information stored in computers and servers should be encrypted.

Key words : Company, Industry Secret Information, Leakage, Internet of Things (IoT), Prevention

접수일(2017년 9월 28일), 게재확정일(2017년 10월 24일)

* 삼성화재 보험범죄조사파트 실장 (주저자)

** 숙명여자대학교 사회심리학과 교수 (교신저자)

1. 서 론

21세기 한국사회는 ICT(Information and Communications Technology) 기술발전으로 다양한 사물기기들에 센싱기술들이 추가되고, 네트워크가 연결되어 여러 데이터들에 대한 활용도를 높이는 소위 '사물인터넷(Internet of things, 이하 사물인터넷)'기술이 주목되고 있다. 미국에서는 매년 10대 전략기술을 발표하는데 사물인터넷은 2015년 전략기술로 선정되기도 하였다. 구체적으로 이 기술에 2020년경 산업계에 3,000억 달러 이상의 수익을 가져올 것이며, 사물인터넷 기기들은 약 260억 개로 늘어날 것으로 예측되고 있다. 또한 미국의 시스코(Cisco) 보고서는 2020년경 260억 개 보다 많은 500억 개 이상의 사물인터넷 기기들이 상용화될 것으로 전망하였다[23].

한국도 21세기 신성장 동력원으로 사물인터넷 기술을 선정하였고, 2013년 2.3조 원의 투자를 시작으로 2020년경 약30조 원의 거대 산업시장으로의 확대를 목표로 육성을 시작하였으며, 산업분야(Industry)에서는 3대 이동통신사(LG U+, KT, SKT 등)와 삼성전자 및 LG전자 등이 플랫폼, 보안, 스마트홈 분야 등을 전략사업부문으로 규정하고 집중적으로 발전시키고 있다.

하지만 초연결사회는 여러 가지 부작용도 야기한데, 대표적인 것이 사물인터넷 기기를 통한 주요정보의 무단 유출이다. 군사기밀의 경우 00육군부대에서 소위 "훈련 일정, 지도·좌표 등" 군사 기밀에 해당하는 내용들을 스마트폰, 기타 전자기기를 통해 습득 후 카카오톡 대화로 주고받다가 외부로 유출되는 등 사물인터넷 기기로 인한 주요정보 유출이 심각한 수준이 이르고 있는 실정이다[24]. 그 결과, 2018년 사물인터넷 보안 관련 시장규모는 약6,244억 원 규모로 확대될 것으로 판단된다. 그러나 사물인터넷 디바이스 관련 보안성 강화 연구는 미비한 수준이며, 추가적으로 사물인터넷 기술을 활용한 기업의 주요핵심정보유출과 관련된 연구의 미비는 매우 심각한 수준에 머무르고 있다. 이 연구는 산업기밀정보와 사물인터넷에 대한 이해를 기반으로 하여 사물인터넷을 활용한 민간기업의 산업기밀정보 유출위협들을 살펴보고 기밀유출을 예방하기 위한 대책을 제시하는 것에 중점을 두었다.

2. 이론적 배경

2.1 산업기밀정보란 무엇인가

산업기밀정보는 정보보안 및 산업보안 관점에서 "지키며 보호한다"는 공통점이 있지만 대상 및 범위의 관점에서 차이점이 있다. 먼저 정보보안의 관점에서는 기밀가치가 있는 정보 및 정보시스템 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability)을 유지하기 위해서 해당 시스템에 부여된 보안조치로 국립표준 기술연구소는 정의하고 있다[2]. 이 개념은 2014년에 한국에서 제정된 『국가정보화기본법』에 영향을 미쳐 "정보의 수집, 가공, 저장, 검색, 송신, 수신" 중 발생 가능한 기밀정보의 훼손, 변조, 추가 유출을 사전에 예방하기 위해서 물리적 기술적 방안을 구비하는 일련의 작용으로 규정할 수 있다.

하지만 산업보안 차원에서는 산업(Industry)활동과정에서 활용도가 있는 모든 유무형의 정보, 인적, 물적 재산 등을 산업스파이 등 사용 허가되지 않은 사람 및 집단으로부터 훼손, 침해, 도난, 파괴 되는 것을 예방하기 위한 일련의 행위로 규정한다[11]. 즉, 산업보안관점에서 규정하고 있는 산업기밀정보의 범위는 정보시스템에 국한된 산업기밀정보보다 광범위하다.

산업기밀정보에 대한 보호 및 유출예방은 지역사회, 산업체 나아가 국가경쟁력에 심각한 영향을 미치는 만큼 핵심 산업기술 혹은 기밀에 대한 적절한 보호조치와 관리체계를 강화할 필요성이 제기되어 왔다[20]. 그 결과, 한국에서는 2017년 현재 산업기밀정보에 대한 침해행위유형파악과 구제방안들을 마련하고 해당 기밀정보들을 보호하기 위한 법제도적 방안을 마련해왔으며 구체적은 내용은 아래 <표 1>과 같다.

<표 1> 국내 기술보호관련 법률 및 보호대상

구분	법률		보 호 대 상
	이름	조항	내 용
1	산업기술유출방지 및 보호에 관한법률	2조 1호	산업기술 : 제품 또는 용역의 개발, 생산, 도금 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 관계중앙행정기관의 장이 지정, 고시, 공고하는 기술로서 제2조 제1호 각목에 해당하는 기술

2	부정경쟁방지 및 영업비밀보호에 관한법률	2조 2호	영업비밀 : 비공지성, 경제적 유용성, 비밀관리성을 가지고 있는 기술상, 경영상의 정보
3	대/중소기업 상생협력촉진에 관한법률	2조 9호	기술자료 : 물품 등의 제조 방법, 생산방법, 그 밖에 영업활동에 유용하고 독립된 경제적 가치가 있는 것
4	하도급거래 공정화에 관한법률	2조 15항	기술자료 : 상당한 노력에 의하여 비밀로 유지된 제조, 수리, 시공, 용역수행 방법에 관한 자료, 그 밖에 영업활동에 유용하고 독립된 경제적 가치를 가지는 것

산업기술정보에 대한 유출형태를 살펴보면 “의도된” 혹은 “비의도된” 유출로 구분가능하다. 의도된 유출은 유출의도를 가진 범죄자의 불법적인 목적에 기반을 두어 이루어지는 유출유형이며, 실수 혹은 부주의에 기반을 둔 비의도된 유출의 경우에는 정보 분실 그리고 누출 등이 있다[13]. 산업기술정보의 유출경로 및 방법에는 여러 가지가 있지만 일반적으로 사용되는 방법들은 아래의 <표 2>와 같다.

<표 2> 기업의 주요 기밀정보 유출경로 및 방법

구분		경 로	유 출 방 법
1	사내N/W	사내 Web 메일	- 파일 붙임 후 전송
		외부 Web 메일	- 일반파일 첨부
		외부 SSL 메일	- 암호화된 메일에 붙임 후 전송
		게시판	- 웹사이트에 파일 업로드
		메신저	- 외부메신저로 파일 전송
		웹하드	- 웹하드 전용 S/W 이용하여 전송
		P2P	- P2P S/W 이용하여 전송
		SMTP 서버	- 메일 Client S/W 이용 및 전송
		외부FTP서버	- 컴퓨터의 FTP로 파일 전송
		외부 Telnet 서버	- 컴퓨터의 Telnet 파일 전송
		Proxy Server	- Proxy S/W 이용
		Tunneling	- 암호화 전송
		외부 프린터	- 외부 네트워크 프린터로 출력
		NETBIOS 공유	- 외부 컴퓨터 공유 폴더로 파일 전송
		PC	- 전화망을 통한 팩스 전송
		모뎀	
		FAX 장비	- 복합기/팩스 기기 이용하여 전송
2	사내N/W	사내메일 서버	- 외부 컴퓨터에서 IMAP로 파일 다운로드
3	외부N/W	외부 무선AP	- 사내 컴퓨터에서 Netspot에 접속 후 전송
4	저장매체/ 출력물	휴대용 저장매체	- CD, DVD, USB 등에 복사 후 반출
		출력물 반출	- 프린터, 복사기, 복합기 이용 출력물 반출
5	BYOD	무선 N/W	- 개인휴대기로 사내 N/W접속 후 자료 전송
		촬영/ 녹음 후 반출	- 개인 휴대기로 촬영 및 녹음 후 전송 및 반출

2.2 사물인터넷이란 무엇인가

사물인터넷(Internet of Things, IoT)이란 주변 환경에 위치한 유/무형의 사물들이 유선/무선의 네트워크 연결을 기반으로 하여 상호 유기적 정보공유가 이루어지는 초지능형 네크워킹 기술과 환경으로 정의된다[8]. 추가적으로 현실과 가상공간의 연결을 통해 ‘사람과 사물’, ‘사물과 사물’ 사이의 24시간 소통이 가능하도록 하는 인터넷 기술로도 추가정의 가능하다[15].

2017년 현재 인터넷기술의 발달로 개개인이 원하는 정보에 대한 접근성이 과거와 비교하여 무한대로 상승하였으나, 여전히 사용자 기반에 근거하여 사용자의 직접적인 개입이 필수적으로 이루어져야 한다. 하지만 사물인터넷시대가 도래하면 사용자가 필요로 하는 정보를 능동적으로 찾지 않아도 필요한 정보가 사용자에게 자동으로 전달된다. 그리고 사용자가 직접 개입하지 않더라도 사용자를 둘러싼 사물들이 능동적으로 움직이는 시대가 올 것이다.

이러한 사물인터넷은 크게 세 가지 특성을 지니고 있다. 첫째 지능을 가진 사물의 등장이다. 데이터 등의 정보를 스스로의 힘으로 수집 및 전송하는 능력을 갖추게 되며, 이렇게 갖추어진 정보를 기반으로 변화의 패턴과 적절한 기능 등을 학습하게 된다[7]. 이에 대한 구체적인 세부기능들은 아래 <표 3>과 같다.

<표 3> 지능을 가진 사물 측면의 세부기능들

구 분	내 용
1	- 데이터나 제어정보를 송수신하기 위한 네트워크 기능

2	- 주위 환경 및 물리적 변화 측정, 데이터 생성
3	- 사용자의 다양한 활동에서 발생하는 데이터 수집
4	- 데이터나 정보를 텍스트, 소리, 이미지 등으로 표출
5	- 자신 혹은 자신과 연결된 다른 디바이스를 제어

둘째, 연결 및 소통기능이다. 사물인터넷으로 연결된 사물들은 독립된 IP로 구분된다[9]. 결국 인터넷에 기반을 둔 네트워크에 의해 서로 연결이 되는 것이다. 이렇게 '연결'된 사물들은 기존 물리적 제품으로서의 특성에서 벗어나 외부 세상으로 해당 기능을 확장시키는 효과를 가진다[16]. 사물인터넷이 가지는 연결성(Connectivity)에 대해 기존에 존재해 왔던 인터넷 환경이 언제, 어디서든지 상호 연결이 가능하다면 사물인터넷은 해당 연결 대상이 무엇이든 구분 없이 연결될 수 있다는 개념으로 정의할 수 있다고 하였다[17].

셋째, 새로운 가치 제공의 증가이다. 사물인터넷은 연결과 소통을 통해 얻어진 여러 가지 데이터를 통해 기존의 가치에서 나아가 새로운 가치 및 서비스를 제공할 수 있다. 사물인터넷을 통해 수집된 데이터는 모든 상황 및 목적 등을 고려하여 개개인들에게 제공되기 위해 소위 "가공 - 추출 - 처리 - 변환" 과정을 통해 서비스 인터페이스의 역할을 담당하게 될 것이다[21]. 이를 통해 정보소비자가 원하는 정보를 목적에 맞게 제공하는 자율화된 새로운 인터페이스가 가능하다.

3. 사물인터넷을 활용한 기업의 산업기밀정보 유출위협

3.1 사물인터넷에 의한 보안 위협

사물인터넷은 여러 유형의 통신인프라에 기초하여 다양한 서비스 제공 및 사물과의 연결이 가능하다. 그 결과, 사물인터넷에 의한 사생활 침해문제와 보안상의 안전문제가 지속적으로 발생하게 된다.

2016년 삼성화재에서 현재 사용빈도가 가장 높은 사물인터넷장비 20개를 선정하여 한 달간 보안안전성 검사를 실시한 결과, 가장 많이 발생한 문제가 ① 사생활 침해의 소지, ② 암호화된 데이터 전송의 미흡, ③ 관리자 웹 인터페이스의 취약점, ④ 불안전한 펌웨어 업데이트 방식, ⑤ 접속 인증 데이터의 무방비한 노출 등의 순서였다[18].

일반적으로, 정보보안에서 발생가능위협은 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에 대한 침해를 기반으로 불안전한 서비스의 발생 및 제공을 통해 지속적으로 보안위협을 증가시키는 것이다[19]. 문제는 이러한 위협들이 사물인터넷 환경에서 반복적으로 출현가능하다는 것이다. 사물인터넷 시대에는 사이버 상에서 발생하는 해킹으로 인해 기존의 개인용 혹은 업무용 서버에 국한되었든 피해들이 나아가 연결가능한 모든 사물들로 확대되는 특징이 있다. 결국 사이버 공격의 목표물의 다변화로 이어질 수 있고, 다양한 분야의 사물들을 대상으로 동시다발적인 보안상의 예방적 대응이 필수적으로 요구된다.

그리고 기존의 보안위협(웜 바이러스, DoS / DDoS, OS보안 취약성, 비인가 접근 등)에서 나아가 기존에 발생하지 않았던 보안문제(디바이스의 무한 복제, 보호되지 않은 펌웨어, 사물인터넷 통신/네트워크의 프로토콜 보안 취약성 등)들이 지속적으로 발생한다[22]. 사물인터넷 시대에 발생가능 한 보안관련 문제들을 어플리케이션, 네트워크, 단말기 등으로 세분화하여 살펴보면 아래 <표 4>와 같다.

<표 4> 어플리케이션, 네트워크, 단말기 측면의 보안 위협들

구 분	내 용
어플리케이션	- 비인가된 서비스 및 사용자 접근, 데이터 위변조, 데이터의 기밀성 침해 등
네트워크	- 인증 방해, 정보유출, 서비스 거부, 데이터 위변조 등
단말기	- 단말기 분석 및 물리적 파괴, 비인가된 접근, 단말기 무결성 침해 등

첫째, 단말기에 대한 분실 및 물리적 파괴이다. 사물인터넷 시대에 여러 가지 사물기기들을 유기적으로 연결하기 위해서는 감지기의 기능이 무엇보다도 중요

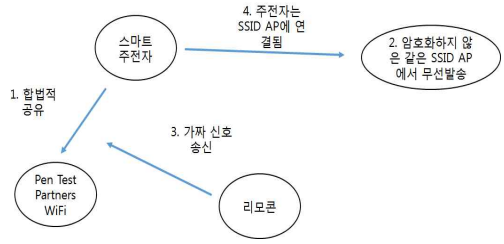
하다. 그러나 사물인터넷 서비스 제공을 위해서는 일반적으로 개방된 장소에 설치된 감지기 노드가 필요한데 이에 대해 인가되지 않은 사람에 의한 물리적 접근 및 파괴가 발생하고 나아가 특정 사용자 소유의 스마트폰과 스마트기기 등이 분실 혹은 물리적 파괴가 발생한다면 사물인터넷 서비스의 중단이 발생할 수 있다. 또한, 분실된 단말기를 통해 사용자의 개인정보들이 유출되는 문제 역시 발생할 수 있다[17].

둘째, 무선신호에 대한 인위적인 교란문제 발생이다. 사물인터넷 서비스의 차별화된 특징은 대부분 무선네트워크 통신에 기반을 두어 발생하게 된다[10]. 2017년 현재, GPS(Global Positioning System), 이동통신망 등 여러 가지 무선 인터페이스를 위한 전파 차단 장치들이 상용화되고 있어, 비인가 된 무선통신 교란 장비 설치를 통해 정상적으로 제공되어야 할 사물인터넷 서비스가 제공되지 못하는 문제 역시 발생가능하다.

셋째, 정보에 대한 유출문제이다. 사물인터넷환경에서 발생 가능한 정보유출 문제는 크게 네 가지(유/무선통신 구간에서 발생하는 스니핑(Sniffing), 불법도청, 서버, DB로의 비인가 접근 등)이다[4]. 구체적으로, 의료서비스의 한 형태인 원격진료과정에서 개인의 생체정보를 전송하는 과정에서 개인정보가 담긴 전자문서를 암호화과정을 거지치 안고 전송하는 경우 여러 가지 피해가 발생가능하다.

넷째, 서비스 거부(Denial of Service)이다. 사물인터넷 서비스를 위해 부착된 감지기들은 센서-센서, 센서-단말기 사이의 정보처리를 위해 게이트웨이를 통해 지속적으로 연결요청 등을 수행한다. 비인가된 해커는 이를 역이용하여 다량의 정보처리, 연결요청, 확인 패키지를 연속적으로 전송하고, 감지기를 이를 처리하는데 필요한 자원들을 지속적으로 소모시킬 수 있다. 결국, 사물기기의 전력을 모두 소모시켜 서비스 수행이 불가능하게 만들 수 있다.

다섯째, 네트워크를 통한 해킹 공격이다. 사물인터넷서비스는 서비스망(감지기 네트워크 서비스)과 제어망(감지기 네트워크 관리)으로 구성되는데, 서비스망과 제어망을 대상으로 비인가된 해커가 소위 중간자 공격(MIM; Man In the Middle Attack)을 실시하여 '사용자-서비스 인증과정-스트림 채널설정 과정'에서 개인정보를 불법적으로 수집하여 서비스망과 제어망을 해킹가능하고 결국, 서비스 거부와 제어권한을 무단으로 확보하여 감지기 네트워크 전체를 제어가능하다[12]. 2014년 영국의 펜 테스트 파트너스(Pen Test Partner)에서 중간자 공격을 기반으로 스마트주전자해킹 후, Wi-Fi 패스워드 해킹이 가능함을 증명하였고 이에 대한 구체적인 내용은 아래 [그림 1]과 같다.



(그림 1) Wi-Fi 패스워드 해킹 - 스마트 주전자 사례

3.2 사물인터넷에 의한 기업의 기밀정보 유출 위협

3.2.1 데이터 저장 기능에 기반을 둔 보안위협

일반적으로 업무용과 영업용으로 사용되는 경우가 많은 사물인터넷기기들은 내부 및 외부에 데이터저장공간을 두고 기업정보 등을 저장하기 때문에 도난 및 분실 등이 발생할 경우 기업보안과 관련된 주요기밀의 유출이 발생할 수 있다. 즉, 사물인터넷기기에 기반을 둔 정보유출은 CD 및 USB와 같은 이동식저장매체와 동일한 데이터 유출요인으로 기능한다[6]. 여러 가지 형태의 유형과 기능을 포함하고 있는 사물인터넷기기의 특성으로 인해 통상적으로 존재하는 컴퓨터의 보안유지정책을 일률적으로 적용하는 것 또한 불가능하며, 사물인터넷기기들의 소형화 추세에 따라 사내에서 반출 및 반입 시 적발 역시 쉽지 않다. 추가적으로, 민간기업의 영업기밀 데이터나 어플리케이션의 정보가 외장 SD Card를 통해 저장 및 유출된다면, SD Card분실 시, 기업핵심정보들의 유출이 발생하게 된다. 그러므로 업무 중에 어플리케이션이 실행되는 경우에는 외장 SD Card를 통한 데이터 저장을 지양하고, 내부 SD Card 암호화를 의무화하여 데이터저장이 이루어져야

한다.

3.2.2 통신 기능에 기반을 둔 보안위협

일반적으로 사물인터넷에 기반을 둔 기기들은 독립적으로 그리고 소위 'Client-Server'의 관계를 기반으로 통신서비스가 이루어짐으로서 데이터를 수집 및 변환한다. 그러나 추가적인 무선통신기능(Tethering, Wi-Fi, Bluetooth 등)들은 아래 <표 5>처럼 기업보안 측면에서 여러 가지 보안 상의 문제들을 야기한다.

<표 5> 무선통신들에 의한 보안야기 문제

구분	보안문제	유형
1	서비스마비	- 주파수 교란으로 서비스 장애 야기
2	정보유출	- 보안취약 암호화 방식 크랙 후 침입
3	정보유출	- 사용자 서버사이의 데이터 스니핑
4	서비스마비	- 과다 트래픽 유발
5	정보유출	- 비인가 AP 사용으로 내부망 침입
6	정보유출	- 내부인이 고의적으로 외부 AP 연결

첫째, Tethering은 내부 네트워크와 연결이 된 사물기기가 타 기기와 접속된 네트워크와 공유가 이루어질 경우, 해당 기기는 내부 네트워크에 상시접속이 가능해지고 내부네트워크에 침입 및 해킹을 통해 데이터 유출 역시 가능해지는 문제를 말한다. 둘째, Wi-Fi로 인해 발생하는 보안문제로서, 디바이스가 Rogue AP, 보안정책 위반 AP, 비인가 AP 등과 공유가 이루어지면 네트워크를 통해 외부로의 데이터 유출이 발생가능하며 비인가 된 외부인에 의해 해당 사용자의 취약점을 검색 및 해킹이 가능하다[14]. 무선 네트워크를 사용할 경우, 특정한 설정이 이루어져 있지 않을 경우에 가장 강한 전파에 기반을 둔 무선 AP에 자동적으로 접속하게 되어 있다. 이 경우, 사용자는 의심 없이 비인가자가 임의적으로 설치한 무선 AP에 접속하게 되고, 결국 '트래픽 가로채기' 등의 방법을 통해 데이터 유출 및 악성코드 감염 등이 야기될 수 있다.

셋째, 블루투스로 인해 발생하는 보안문제이다. 블루투스는 10m 안팎의 짧은 거리에서 낮은 전력에 기반을 둔 무선연결이 필요할 경우에 주로 사용되며, 대부분의 사물인터넷 기기와 모체가 공유하기 위해 사용된다. 그러나 이 과정에서 블루재킹(Bluejacking), 블루스나핑(Bluesnarfing) 등 블루투스가 가지는 본질적인 취약점에 노출되고[5] 또한, 블루투스통신이 가능한 사물 IT 디바이스와의 연결을 통해 내부정보에 대한 무단열람 및 데이터 해킹이 발생할 수 있다.

블루투스를 통한 악성코드 유포는 주변에 위치한 단말기의 블루투스 장치에 대한 끊임없는 스캐닝 과정을 통해 인식된 스마트 디바이스를 수단으로 악성코드를 전파한다[1]. 감염된 스마트 디바이스는 끊임없는 스캐닝 과정으로 인해 다량의 배터리 소모가 발생함으로써 서비스 거부 공격(DoS) 피해가 발생할 수 있다. 블루투스 기능은 디바이스들 사이의 공유에 의해 내부 네트워크 침입 및 모바일기기 내의 데이터를 무단으로 열람 및 유출시킬 수 있는 문제가 발생한다.

3.2.3 촬영 및 녹음기능에 기반을 둔 보안위협

사물인터넷 디바이스에서 촬영기능이 제공되는 경우 기업의 내부 자료, 시설물, 기타 정보를 무단으로 촬영할 수 있는 보안취약점이 발생하게 된다[3]. 스마트워치, 스마트글래스와 같은 사물인터넷 기기에 존재하는 카메라들의 특징은 크기가 소형이고 상대방이 활용여부를 명확히 확인하기가 쉽지 않기 때문에 몰래카메라 등으로 사용될 가능성이 있다. 이는 법률적으로 심각한 문제를 야기할 수 있는데, 2017년 현재, 미국에서는 매장, 극장 레스토랑 등에서 고객과 저작권 보호의 목적을 근거로 개인별 스마트글라스 착용을 금지하는 곳이 점점 늘어나고 있다.

녹음기능에 기반을 둔 보안위협으로서, 구체적으로 미국 마텔(Mattel) 社가 새롭게 개발한 바비 인형이 불법도청에 악용될 소지가 있다는 것이다. '안녕 바비'라는 이름의 이 인형은 몸통에 마이크와 스피커, 배터리가 내장되어 있으며, USB 포트를 통해 충전이 가능하다. 먼저, 도청의 구조를 살펴보면, ① 아이가 인형에게 말을 걸면, ② 인형은 해당 음성 파일을 녹취, 압축해 외부 서버의 자체 데이터 센터로 전송해 분석하고, ③ 분석이 완료되면 적절한 응답을 구성, ④ 다시 인형에게 전달되고 재생이 이뤄지는 형태로 동작한다[10]. 2017년 현재 재품으로 출시되는 스마트 TV들 역시 상

기와 같은 음성인식 및 재생 기능을 제공하고 있으며 이러한 기능은 도청장치로 충분히 활용가능하다. 결국, 사물인터넷디바이스의 녹음 기능은 기업 내부에서 발생하는 주요회의 및 임직원사이의 불법적인 대화녹음을 통해 기업의 주요 기밀정보에 대한 외부 유출이 이루어질 수 있다.

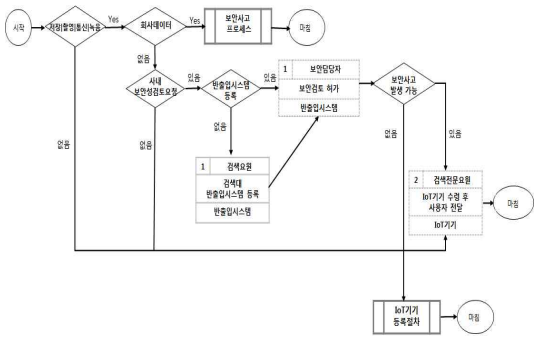
4. 유출예방 대책

4.1 관리보안 측면

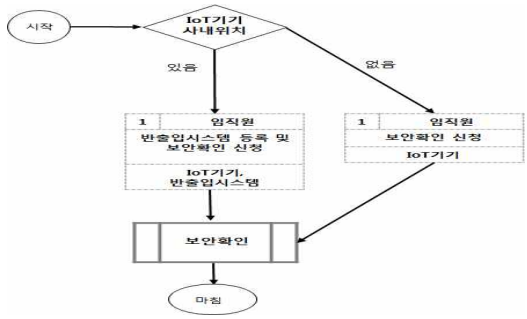
관리적 보안 측면에서 우선적으로 기업내부로 출입이 인가된 모든 사람들에 대해 사물인터넷기기가 수단이 되어 정보가 유출될 수 있다는 경각심을 가지고 주요 출입이 허가된 구역에 출입시점부터 사물인터넷 기기의 사용을 제한하는 가이드라인을 비치해야 한다. 구체적인 사용제한에 대한 내용은 가이드라인으로 만들어 주요출입구 및 유동인구가 많은 지점에 관련 장비 및 시설을 설치하는 등 보다 적극적인 보안예방을 실시할 필요가 있다.

또한, 사용자 요청 혹은 기업자체적으로 보안운영 가이드라인에 따른 절차를 마련해야 한다. 아래 [그림 2]와 같이, 기업내부로 반입이 허가된 기기에 대해 보안검토절차와아래 [그림 3]과 같이 보안성 확인 신청 절차를 마련하여 구체적으로 '누가, 언제, 어디서, 왜' 등의 디바이스 사용용도를 명확히 파악할 필요가 있고, 추가적인 보안준수 서약작성을 통해 회사내부에서도 사용 중인 사물인터넷 기기를 관리할 필요가 있다.

사물인터넷 디바이스와 블루투스, Wi-Fi 등의 무선인터넷 공유가 가능한 컴퓨터 및 노트북과 관련하여 해당 무선인터넷 모듈을 도입시기부터 제거할 필요가 있다. 모듈을 제거하는 것이 불가능한 노트북의 경우 구체적인 현황을 조사하고, 주기적으로 정보보안점검을 실시하는 등, 원칙적으로 사물인터넷기기와 사내 컴퓨터 그리고 인터넷 시스템과의 무선인터넷 모듈 접점을 차단하는 정책을 시행하여야 한다.



(그림 2) 사물인터넷 디바이스에 대한 보안확인 Process



(그림 3) 사내 사물인터넷 디바이스에 대한 보안확인 신청 Process

4.2 기술보안 측면

2017년 현재 사용되고 있는 사물인터넷 디바이스는 종류 및 기능 등이 다양하기 때문에 현재 존재하는 모든 사물인터넷 디바이스에 기술적으로 대응하는 것은 불가능하다. 결국, 기술보안 초기단계에는 ① 소위 대중적인 디바이스, 사용 및 반입빈도가 상대적으로 높은 디바이스들을 대상으로 보안점검을 검토 및 실시하고, ② 추가적으로 보안취약점이 발견된 디바이스에 대해서 보안관리가이드라인을 추가 설정하고 안정화 및 추가 도출된 취약점들에 대해 예방 및 관리해 나가는 방향으로 이루어질 필요가 있다.

사물인터넷 디바이스는 일반적으로 CPU, Memory, Storage 등을 기본구조로 하고 있기 때문에 소위 정보데이터를 스스로 생성 및 보관 그리고 처리할 수 있는 컴퓨팅 기능을 내재하고 있는 시스템으로 규정할 수

있다[11]. 그리므로, 기업은 기존 디바이스(개인 PC, USB, 카메라와 같은 저장, 통신, 촬영, 녹음이 가능한 기기)를 대상으로 시행해왔던 정보보안정책에 추가하여 솔루션을 융합한 중층통제(Multi-Layered Control) 방식을 통해 출현가능한 보안위협으로부터 대비할 필요가 있다.

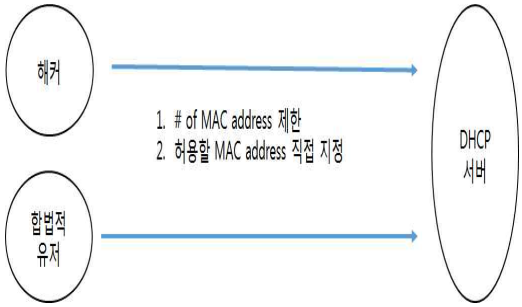
먼저, 컴퓨터에 대한 제어 솔루션이다. 일반적으로 기업정보들이 주로 저장되고 있는 컴퓨터 및 서버에 매체제어 솔루션 활용을 통해 사물인터넷 디바이스와 공유되는 경로를 대상으로 통제솔루션을 실시할 필요가 있다. 구체적으로 데이터유출이 발생할 수 있는 인터페이스에 대해 <표 6>과 같이 실시가능하다.

<표 6> 데이터유출 예방을 위한 경로 통제

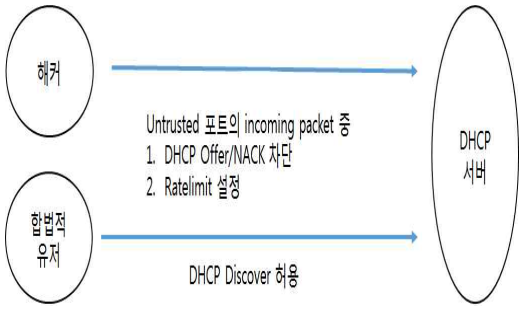
분 류	설 명
휴대기기 (스마트폰, PDA)	- 통제 기능 확인 · 허용 / 차단 / 로그 기록 · 원본 저장 / 읽기 전용
포트 통제 (USB 포트, Serial, IRDA 등)	
드라이브 통제 (USB, 프린터, 공유폴더 등)	

둘째, 네트워크에 대한 접근통제이다. WIPS (Wireless Intrusion Prevention System)는 등록되지 않은 사용자가 무선을 통해 기업의 내부인터넷망에 접속하거나, 등록된 사용자가 비인가된 AP를 기반으로 내부의 데이터를 외부로 유출하는 것을 탐지 및 예방하기 위해 무선 네트워크 시스템을 가지고 있는 조직의 경우 필연적으로 운영해야하는 보안솔루션이다[10]. 등록되지 않은 사용자가 분류될 수 있는 비인가된 사물인터넷 디바이스의 내부 네트워크 연결시도를 탐지하고, 허가된 디바이스의 이상행위를 사전에 차단가능하다는 특성이 있다[4]. WIPS운영을 통해 네트워크에 공유된 사물인터넷 디바이스와 등록된 사물인터넷 디바이스의 현황을 정기적으로 확인하는 과정을 통해 보안관리 차원의 누수를 최소화할 수 있다.

또한, IP 할당 프로세스에 대한 강화가 이루어져야 한다. DHCP(Dynamic Host Configuration Protocol)에 기반을 둔 IP 할당체계의 문제점을 개선하기 위해 (그림 4)와 같이 L3 장비의 경우 한 포트에서 허용되는 MAC 주소 제한을 통해, 정상적으로 연결된 포트를 제외하고 나머지 포트에 대한 필터링 기능을 사용하여 [그림 5]과 같이 DHCP Discover외에 소위 'Request, Nack, Offer, Ack' 메시지를 차단하고 Ratelimit를 설정하는 방식으로 운영할 필요가 있다.



(그림 4) DHCP MAC address 제한 모델



(그림 5) DHCP 메시지 제한 모델

추가적으로 LTE 무선 통신 모듈을 사용하고 있는 사물인터넷 디바이스의 경우, 내부 네트워크 장비에 대한 경유 없이, 외부의 ISP(Internet Service Provider)에 기반을 둔 기지국을 통해 내부에서의 데이터관리 모니터링을 우회하여 데이터를 유출할 수 있다[17]. 그러므로 데이터유출의 원인 제거를 위해 해당 디바이스의 반입 및 사용을 전면 통제하는 방안과 추가적으로 인근 기지국에서 수집된 데이터를 ISP로부터 별도로 제공받는 공조체제를 마련할 필요가 있다.

셋째, 암호화 방안이다. 기업 자체적으로 사용하는 컴퓨터 그리고 서버와 같은 정보자산에서 데이터 저장이 이루어짐과 동시에 이를 암호화함으로써 생성된 데이터가 외부로 불법적으로 유출은 것을 막을 수 있다. 또한 유출되었더라도 언제나 암호화가 이루어진 상태에서 유출이 발생하기 때문에 보호화 과정을 거치는

한 생성된 주요 정보들이 안전하게 보호되는 장점이 있다. 암호화하는 방법에는 ① 매번 저장 시, 해당 파일을 암호화 하는 방식, ② 하드웨어적으로 특정 폴더의 데이터를 암호화하는 방식, ③ 윈도우 OS 암호화 방식 등이 있고, 해당 기업의 보안정책에 준하여 암호화 알고리즘을 도입 및 운영하여야 한다.

5. 결 론

2000년 MIT에서 전 세계 처음으로 소위 '사물인터넷'이라는 단어를 사용한 이후, 사물인터넷 용어는 여러 대중 매체 등을 통해 일반인들에게 익숙한 단어가 된지 얼마 지나지 않았음에도 불구하고 Industry를 비롯한 여러 분야에서는 사물인터넷을 소위 '제4차 산업혁명'을 위한 필수요소로 규정하고 있다. 그 결과, 사물인터넷은 사회전반을 변화시킬 무한한 가능성으로 평가받고 있다. 그러나 이러한 신기술의 긍정적인 영향뿐만 아니라 부정적인 영향으로 인한 다양한 보안상의 위협 또한 야기하고 있는 것이 사실이다.

이 연구는 사물인터넷 디바이스로 인해 발생가능한 기업의 주요 핵심정보의 유출위협에 대한 심각성을 살펴보고 그 유출예방을 위한 방안들을 관리보안과 기술보안 측면에서 살펴보는 것이 목적이다. 본 연구의 결과들을 요약하면 다음과 같다. 관리보안측면에서는 기업내부로 출입이 인가된 모든 사람들에 대해 사물인터넷기기가 수단이 되어 정보가 유출될 수 있다는 경각심을 가지고 주요 출입이 허가된 구역에 출입시점부터 사물인터넷 기기의 사용을 제한하는 가이드라인을 비치할 필요가 있다. 또한, 사용자 요청 혹은 기업자체적으로 보안운영 가이드라인에 따른 절차를 마련할 필요가 있으며, 사물인터넷 디바이스와 블루투스, Wi-Fi 등의 무선인터넷 공유가 가능한 컴퓨터와 노트북과 관련하여 해당 무선인터넷 모듈을 도입시기부터 제거할 필요가 있다.

기술보안측면에서는 먼저, 컴퓨터에 대한 제어 솔루션이다. 일반적으로 기업정보들이 주로 저장되고 있는 컴퓨터 및 서버에 매체제어 솔루션 활용을 통해 사물인터넷 디바이스와 공유되는 경로를 대상으로 통제 솔루션을 실시할 필요가 있다. 둘째, 네트워크에 대한 접근통제이다. WIPS 운영을 통해 네트워크에 공유된 사물인터넷 디바이스와 등록된 사물인터넷 디바이스의 현황을 정기적으로 확인하는 과정을 통해 보안관리 차원의 누수를 최소화할 수 있다. 셋째, 암호화 방안으로서 기업 자체적으로 사용하는 컴퓨터 그리고 서버와 같은 정보자산에서 데이터 저장이 이루어짐과 동시에 이를 암호화함으로써 생성된 데이터가 외부로 불법적으로 유출되는 것을 막아야 한다.

본 연구를 통해 산업체 별 특성에 적합한 관리지침을 마련하여 기업보안전반에 적용될 수 있는 표준가이드라인 수립을 위한 지속적인 예방대책 마련과 함께 사용자 관점에서의 보안의식 개선연구가 후속연구로서 진행되어야 할 것이다.

참 고 문 헌

[1] 강경아, AHP 기법을 이용한 스마트폰 앱 개발을 위한 시큐어 코딩 항목 간 중요도 분석, 공주대학교 일반대학원 석사학위논문, 2014.
[2] 공배완, "사물인터넷의 활용과 민간시큐리티의 혁신", 융합보안논문지, 17권 1호, pp. 101-109, 2017.
[3] 김동희, 윤석웅, 이용필, "IoT 서비스를 위한 보안", 정보통신학회지, 30권 8호, pp. 53-59, 2013.
[4] 김진보, 사물인터넷 서비스 보안성 향상을 위한 접근제어 시스템, 목포대학교 대학원 박사학위논문, 2016.
[5] 김진보, 장데레사, 김미선, 서재현, "CapSG를 이용한 IoT 서비스 접근제어 플랫폼", 정보처리학회논문지, 4권 9호, pp. 337-346, 2015.
[6] 김호원, "사물인터넷환경에서의 보안/프라이버시 이슈", 한국정보통신기술협회, TTA Journal, 153호, pp. 35-39, 2014.
[7] 김호원, 김동규, "IoT 기술과 보안", 한국정보보호학회지, 22권 1호, pp. 7-13, 2012.
[8] 박성수, 사물인터넷 환경의 사이버 위협 분석, 공주대학교 대학원 석사학위 청구논문, 2015.
[9] 서화정, 이동건, 최종석, 김호원, "IoT 보안기술 동향", 한국전자파학회, 24권 4호, pp. 27-35, 2013.
[10] 성순화, "클라우드 컴퓨팅에서 안전한 사물인터넷 데이터를 위한 키 관리", 정보보호학회논문지, 27권 2호, pp. 353-360, 2017.

[11] 이명렬, 박재표, “스마트카 정보보안 침해위협 분석 및 대응방안 연구”, 한국산업기술학회논문지, 18권 3호, pp. 374-380, 2017.
[12] 이범기, 김미선, 서재현, “IoT에서 Capability 토큰 기반 접근제어 시스템 설계 및 구현”, 정보보호학회논문지, 25권 2호, pp. 439-448, 2015.
[13] 이윤희, 창조경제 실현을 위한 사물인터넷 기반 유망 시장 전망 및 과제, 한국정보진흥원, 2013.
[14] 전인호, “소프트웨어 개발인력의 업무 지속수행 증진방안에 대한 연구”, 서울과학기술대학교 대학원 석사학위논문, 2015.
[15] 정다혜, 최진영, 이송희, “시큐어 코딩 중심으로 본 원자력 관련 소프트웨어”, 정보보호학회논문지, 23권 2호, pp. 243-250, 2013.
[16] 정명규, 소프트웨어 보안성 관리를 위한 시큐어 코딩 프로세스와 방법에 관한 연구, 부경대학교 대학원 박사학위논문, 2015.
[17] 최관, 김민지, “국가안보를 위한 공공기관의 내부자 정보 유출 예방대책: 사이버안보·형사정책 관점”, 융합보안논문지. 16권 7호, pp. 167-172, 2016a.
[18] 최관, 김민지, “자동차 내부망 통신네트워크 해킹범죄예방을 위한 융합보안적 대응방안: Bluetooth 활용사례를 중심으로”, 융합보안논문지, 16권 6호, pp. 99-107, 2016b.
[19] 최관, “산업보안기밀 유출원인에 관한 연구: 내부자거래를 중심으로”, 한국산업보안연구, 5권 1호, pp. 71-93, 2015.
[20] 최관, 김민지, “조선기업출입보안관리 발전을 위한 시론적 연구: 융합보안적 접근”, 한국시큐리티 융합경영학회지, 4권 2호, pp. 187-202, 2015.
[21] 표철식, 강호용, 김내수, 방효찬, “IoT(M2M) 기술 동향 및 발전 전망”, 한국통신학회지, 30권 8호, pp. 1-10, 2013.
[22] 허대영, 황선태, “OAuth 기반의 대리 인증서 위임 서비스”, 인터넷정보학회논문지, 13권 6호, pp. 55-62, 2012.
[23] http://kast.tistory.com/122
[24] 데일리시사닷컴, http://dailysisa.com/default/all_news_body.php?idx=11817&board_data=aWR4JTNEMTE4MTclMjZzdGFydFBhZ2UlM0QyNjIwJTI2bGlzdE5vJTNEMTM1NiUyNnRvdGFsTGlzdCUzRDM5NzY=||&search_items=cGFydF9pZHglM0QlMjZ2aWV3X2NudCUzRDIwJTI2Z3JvdXBfaWQlM0QlMjZ2aWV3X3BhZ2UlM0QlMjZzZWFyY2hfb3JkZXIlM0Q=||

〔저 자 소 개〕

최 관 (Kwan Choi)
호주 국립 모나쉬대학교
범죄학·형사사법학 박사
모나쉬대학교 범죄학과 강사
한세대 인문사회학부 교수
삼성교통안전연구소 책임연구위원
現) 삼성화재 보험범죄조사파트 실장

email : schgosi@daum.net

김 민 지 (Minchi Kim)
미국 뉴욕시립대학교
법심리학 박사
한국형사정책연구원 부연구위원
現) 숙명여대 사회심리학과 교수

email : mkim76@sm.ac.kr