**보안시스템 조사 보고서**

**20152689**

**산업보안학과 황성은**

1. **서론**

먼저, 보고서를 작성하면서 보안의 기본인 정보보안, 물리보안, 융합보안 등 3가지로 보안 시스템을 분류했다. 그러나, 고려해야할 한 가지 사실은 현재 4차 산업혁명의 시대를 맞아 다양한 산업 및 사업이 유기적으로 연결, 융합하는 상황이라는 점이다. 보안산업은 4차산업 이전까지 네트워크 및 서버 시스템을 활용하는 정보보안과 통제 시스템 및 경비 등으로 시설과 설비를 보안하는 절차가 있었다. 그러나, 기존의 시스템으로 발전 및 진화하는 기술에 대해 유동적으로 대응하기가 매우 어려워진 상황이 계속해서 발생했고 이에 따라 최근 보안산업은 이 두가지의 영역을 접목한 지능보안 및 융합보안을 활용하여 물리적인 부분에서도 인공지능(AI), 클라우드 서비스 등 신기술을 도입하고 있다.

“한국 정보보호 산업협회(Kisia)”에 따르면 2019년 국내 정보보안 시장 규모는 10조원을 넘어설 정도로 성장했다. 또한, 그동안은 물리보안이 주도하여 보안시장을 이끌었지만 1) 사이버 보안과 관련하여 정부의 규제가 강화되었고 2) 국내 및 해외의 보안 서비스가 대형 DDOS 공격, 해킹 사고를 겪으면서 기업과 기관의 보안 태세에 관한 경각심이 대두되었다.

다시 말해서, 서비스의 안정성 및 다양한 악용사례와 해킹에 관한 대응력을 향상시키기 위해서는 기존의 분리된 보안 시스템의 구조가 아닌 차세대 통신 5G와 신기술을 융합하여 보안을 강화해야 한다는 것이다. 예를 들어 물리보안에서 IoT 시스템이 장착된 Smart Home의 경우 침입 방지 및 안정성을 유지하기위해 IOT 기기에 대한 해킹 공격을 방어 해야함과 동시에 인간의 침입에 대한 출동 및 경비 서비스까지 결합되어야 온전한 대응 절차를 갖춘 하나의 시스템이 구축된다는 것이다.

그 중에서도 특히 융합보안과 관련된 스마트 의료 보안, 스마트 팩토리 분야는 중요하다. 소규모의 공격이라고 할지라도 사이버 공격이 발생하여 성공할 경우, 의료 분야에서는 환자에 관한 개인정보가 모두 노출될 가능성이 있으며 후자의 경우는 스마트 팩토리의 진보된 기술이 중국이나 기타 등등의 국가로 전송되어 기업 및 국가 경쟁력에 막대한 손실이 발생하기 때문이다.

물리보안 시장의 선두를 달리는 삼성 S1은 18년 딥러닝 기술이 적용된 생체(얼굴)인식을 통한 출입관리 시스템을 개발하였고 이어서 영상 감시 기술과 접목하여 교통 위험 정보를 제공하는 스마트 솔루션을 만들었다. 통신사, 기업 보안업체 등의 기업들도 보안 사업에 5G, IoT, 클라우드 등의 신사업 분야와 기술을 결합하는 작업이 필수적으로 수행되고 있다.

결과적으로, 각각의 보안 시스템을 큰 틀로 분류하였으나, 4차 산업 혁명에서 이러한 보안 시스템은 결코 분리된 개념을 가지지 않으며 어떠한 솔루션을 사용하냐에 따라서 물리보안에도 IOT, AI 기술들이 결합되는 등 다양한 방식으로 보안 시스템이 구축될 수 있다는 것이다.

1. **본론**

* **보안시스템 분류기준**
* **사이버보안 (1, 2) / 융합보안 ( 3 ) / 물리보안**

1. **지능디지털 보안** **: IoT 보안**, AI 보안, 클라우드 보안, **빅데이터 보안**, 블록체인, 바이오 인증
2. **서버 보안** : **애플리케이션 보안**, 데이터 보안, 무선랜 보안, IPv6운영 보안, 보안 관제, 데이터 센터 보안
3. **스마트 보안** : 스마트 의료보안, 스마트 교통보안, 스마트 시티보안, **스마트 팩토리(OT) 보안,** 자동차 보안
4. **물리 보안** : 통합관제센터, 정보유출방지 보안, 보안관리, 시스템 및 단말보안, 임베디드 보안

* **5 가지 조사 대상 보안시스템**

1. **IOT 보안 2) 빅데이터 보안 3) 애플리케이션 보안 4) 스마트 팩토리(IO) 보안 5) 물리 보안을 선정하였다.**

**\_\_ 각 보안시스템의 선택 이유 항목에는 배경 및 목적이 포함되어 있다.**

* **조사 대상 보안시스템 선택 이유**

1. **IoT 보안 시스템**

: 사물인터넷(Internet of Things, IOT)는 사물과 사람 및 공간 등 모든 것이 인터넷 네트워크로 연결되어 유기적으로 연동함으로써 수십만개의 정보를 공유하고 생성하는 과정이며, 이러한 과정에서 나온 정보들을 활용할 수 있다.

현재, PC와 모바일을 넘어 집의 가전제품 그리고 의료기기, CCTV, 경비까지 하나의 도시 전체가 인터넷이 연결된 상황이다. 그러나, 최근 지능형 CCTV와 의료기기 해킹 사건이 발생하면서 IOT 보안에 대한 관심과 경각심이 동시에 커지고 있다.

현대연구소의 ‘사물인터넷 관련 유망 산업 동향 및 시사점’ 리포트에 의하면 세계 시장규모는 2020년에 1조달러까지 성장할 것으로 내다보았다. 이러한 상황에서 국내 IOT 시장도 기하급수적으로 성장하고 있으며, IOT에 대한 기술이 실생활에 접목되더라도 보안 대응책 및 보안 점검의 미비로 피해가 발생한다면 심각한 결과를 초래할 수 있기 때문에 IOT 보안 시스템을 조사하려고 함.

1. **빅데이터 보안 시스템**

최근 10년 간, IT 기업의 떠오르는 화두는 단연 빅데이터라고 할 수 있다.

먼저, 빅 데이터(Big Data)는 데이터의 디지털 환경에서 생성되는 데이터로 그 규모가 방대하고, 생성 주기도 짧으며 수치 데이터 및 문자와 영상 데이터를 포함하는 대규모 데이터를 말한다. 빅데이터는 3가지 특징이 있는데, 1) 데이터의 양 2) 데이터 생성속도 3) 다양성을 의미한다.

이처럼 방대한 규모의 데이터는 국가 경쟁력에서 우위를 차지할 수 있는 중요한 자산이자 기술로 활용될 수 있다는 점이다. 빅데이터를 활용한 분석방법론은 과거에 불가능했던 일을 가능으로 만들고 있다. 즉, 빅데이터는 이러한 혁신적인 변화를 선도할 수 있는 시스템이고 방대한 데이터를 가지고 있기 때문에, 이에 따라 이에 걸맞는 보안 시스템이 필요하다고 생각했다.

1. **애플리케이션 보안 시스템**

Application Security는 응용 소프트웨어의 보안 정책에서의 결함이나 시스템 개발에서의 눈에 띄지 않은 취약점들 같은 코드의 생명 주기 전체 과정을 말한다.

애플리케이션 보안의 종류는 크게 네트워크, 앱, 모바일, ERP, 클라이언트 서버 등으로 구성되어 있으며, 이러한 애플리케이션은 현존하는 대부분의 기업들이 가장 많이 사용하는 시스템 중에 하나라고 생각한다. “MOST VULNERABLE WEB APPLICATION IN 2013: XSS, PHP AND MEDIA SITES”라는 논문에 의하면 현 시대에서 기업의 가장 큰 보안 과제는 애플리케이션 내의 취약점들이 어떻게 기업과 브랜드에 피해를 발생시키는지 그 피해액은 얼마인지를 파악하는 것이라고 한다.

그러므로, 기업들은 전체 애플리케이션의 모든 취약점들을 탐지하고 기타 공격들을 사전에 차단할 수 있으며 주기적으로 신속한 패치가 이루어지는 애플리케이션 보안에 대한 스마트한 접근방식이 필요하기 때문에, 애플리케이션 보안 시스템을 조사 대상으로 선정했다.

1. **스마트 팩토리 보안 시스템**

스마트 팩토리(Smart Factory)는 ‘전통 제조산업에 ICT를 결합하여 제품의 기획, 설게, 생산, 유통, 판매 등 전 과정을 ICT 기술로 통합함으로써 최소 비용과 시간으로 고객 맞춤형 제품 생산을 지향하는 공장’을 의미한다.

보안의 관점에서 스마트 공장의 특징이 존재하는데, 이는 기존의 IT영역 그리고 제조 및 설계 영역 그리고 관리 영역까지 전 계층이 단 하나의 인터넷 네트워크로 연결되어 기능을 수행한다는 점이다. 즉, 이러한 시스템으로 인해 스마트 팩토리의 제조 공정이나 고도화의 정도에 따라서 전체 공정의 효율성 및 품질의 향상이 가능하는 점이 특징이지만, 외부로부터 기술적인 보안 위협이 지속적으로 발생하고 침투 가능성 및 기존 ICT 취약점을 이용하는 등의 리스크가 존재한다.

1. **자동차 보안 시스템**

이전에도 언급했듯이, 기술의 발달로 인해 편리함이 증가할수록 해킹 위협과 그 가능성이 비례하여 증가한다. 즉, 네트워크와 연결된 ICT 기술을 사용하는 자동차 시스템은 적절한 보안 장치가 존재하지 않는다면, 생명과 직결되는 위협이 발생할 수 있다는 것이다.

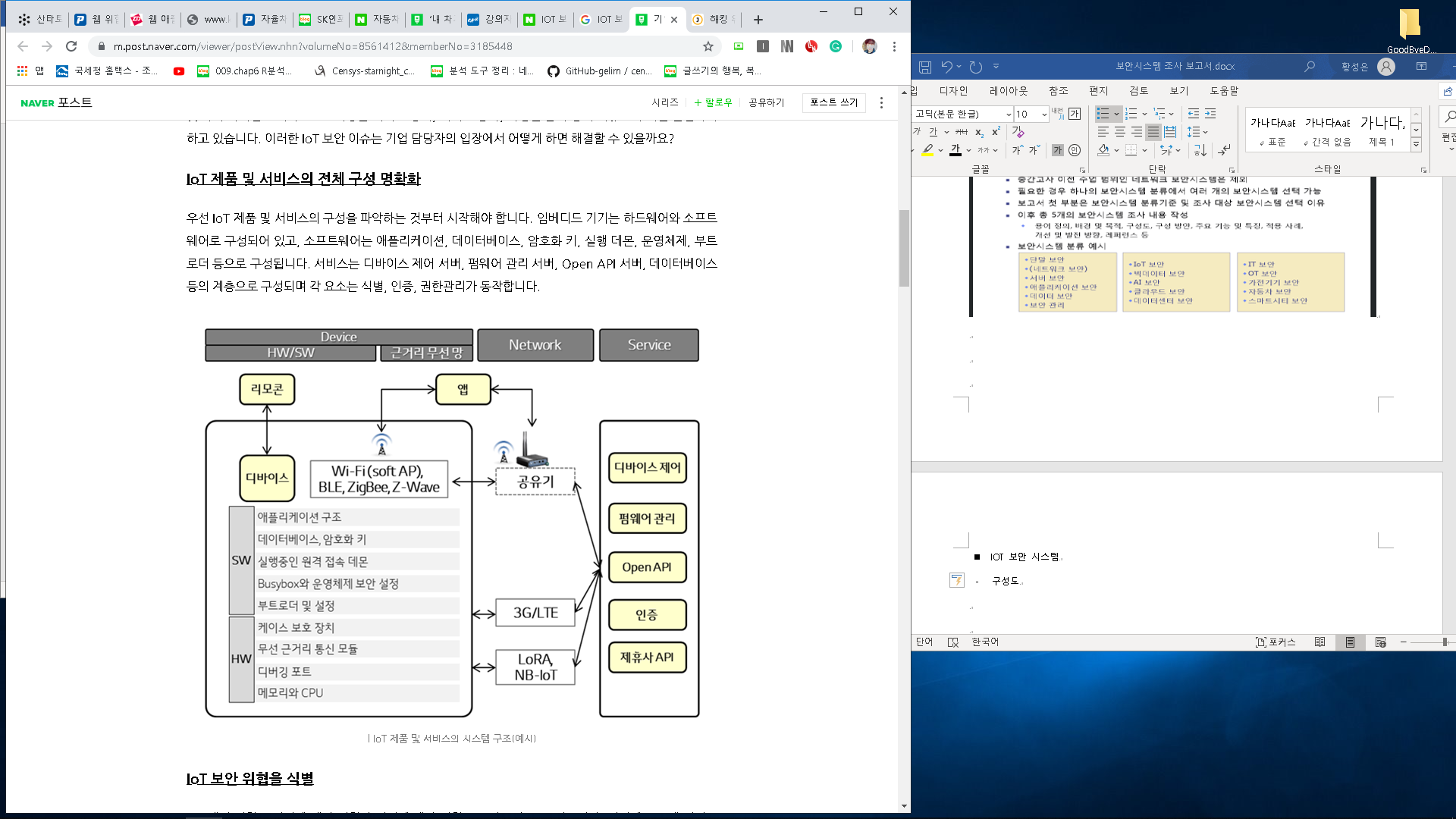
현대의 차량에는 전자제어장치가 내재되어 제조되고 있다. 여기서 전자제어장치란 Electronic control Unit으로 차량 내부간 각자 내제된 장치가 유기적으로 연결되어 상호 간의 네트워크를 형성하여 일률적인 통신을 수행한다. 이러한 방식으로 축적된 정보들은 차량 운행에 도움이 되는 데이터로 변환이 되어 다량의 데이터를 기반으로 새로운 스마트 자동차에 이용되는 장비를 개발할 수 있다.

그러나, 일반적인 시설 및 정보 시스템에 설치된 보안 수준과는 달리 자동차의 특수성으로 인해서 하나의 자동차 시스템에 수준 높은 보안을 구축할 수 없다는 점이다. 자동차의 네트워크 해킹에 관한 공격은 이미 수차례 존재했다. 일례로, 자동차 대리점의 시스템을 해킹하여 원격으로 자동차의 시스템을 조종한 “원격 조종”, 스마트폰 어플을 이용하여 원격으로 차량의 전자제어장치에 침투한 “스마트폰 해킹” 등이 있다. 이는 전세계에서 개발되는 모든 스마트 자동차에 적용되는 중대한 사항이며, 안정성을 가진 스마트 자동차의 시대를 열기 위해서는 설계 시에 ‘보안’을 무엇보다도 최우선의 과제로 삼아야하는 등의 체계적인 보안 기술의 개발이 필요하므로 조사 대상으로 선정하였다.

* **IOT 보안 시스템**
* **용어 정의**

|  |  |
| --- | --- |
| IOT의 기본적인 용어 | |
| AMQP  (Advanced Message Queuing Protocol) | 개별 애플리케이션이 기기와 네트워크에 관계없이 상호 통신할 수 있도록 해주는 오픈소스 표준이다. 원래 빠른 M2M 통신을 위해 금융 분야에서 개발됐으나 IoT 프로젝트에도 사용되기 시작했다. |
| 지그비(Zigbee) | 우수한 배터리 수명과 내장된 128비트 암호화를 통한 견고한 보안이라는 보기 드문 조합을 자랑하는 무선 메시 네트워킹 프로토콜이다. |
| 지웨이브(Z-Wave) | 지그비와 마찬가지로 저전력 단거리 무선 네트워크 기술로, 주로 스마트 홈 기기와 같은 애플리케이션에 사용된다. |
| SCADA | CADA는 산업용 제조 및 대형 화물 수송 애플리케이션에 대한 체계적이고 컴퓨터화된 제어를 구현하기 위해 메인프레임 시절부터 존재한 기술이다. |
| 홈킷(HomeKit) | 스마트 홈 기기를 위한 애플 브랜드의 프론트 엔드 및 제어 장치다. 설정과 사용이 간편하다는 애플만의 미덕을 갖추고 있다. |
| 시큐어 코딩(secure coding) | 개발하는 소프트웨어의 보안상 취약점이 발생할 수 있는 부분을 보완하면서 프로그래밍하는 것을 의미한다. |

* **구성도**





**그림 2. End to End IoT 보안의 구성요소 및 구성도**

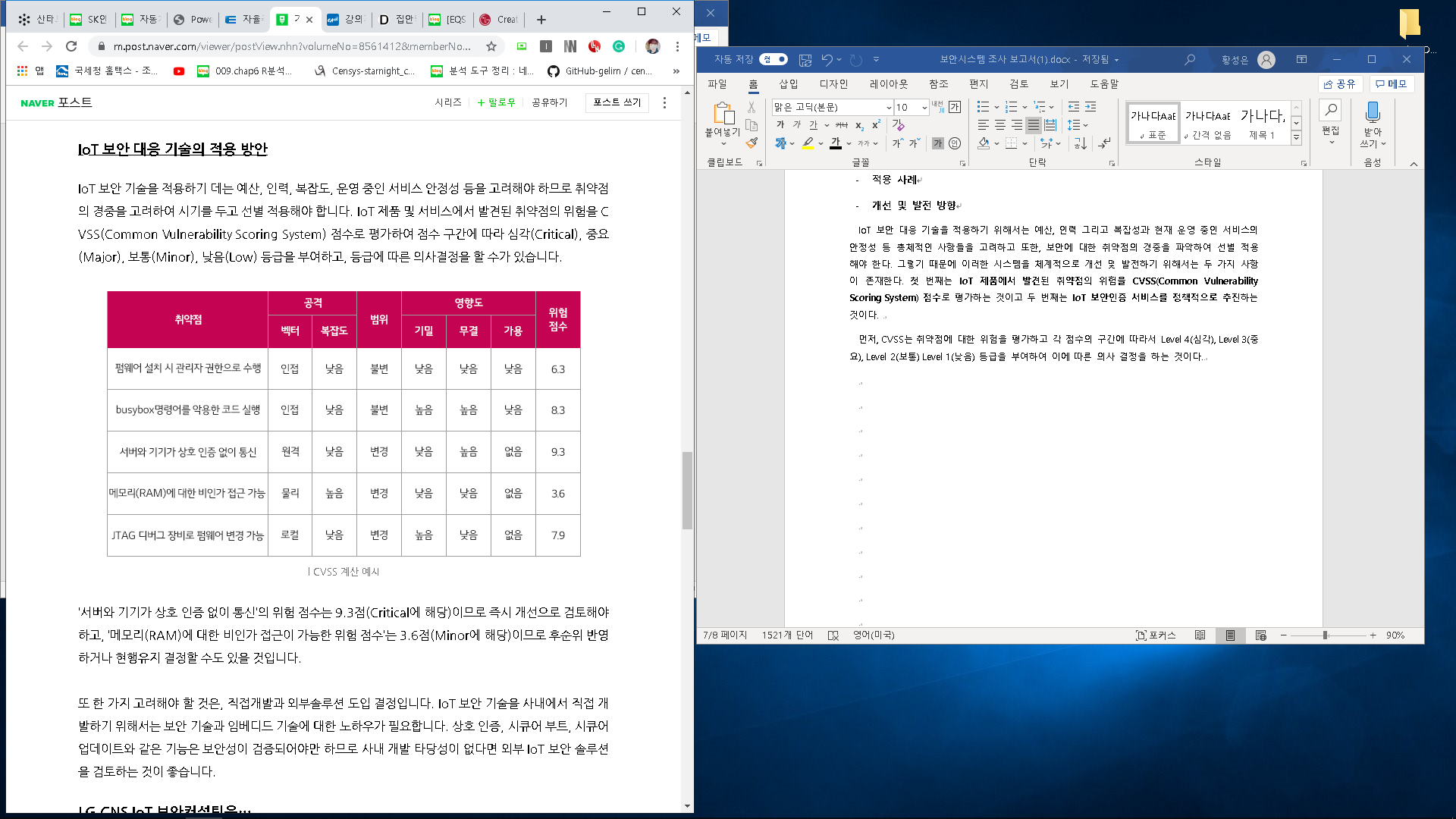
* **보안 시스템 주요 기능 및 특징**

|  |  |  |
| --- | --- | --- |
| 기술 | 설명 | 상세 기술 |
| 경량 암호화 기술 | 128비트 암호화 알고리즘(예:AES)을 실행할 수 없는 제약이 심한 기기에서도 적절한 수준의 암복호화 수행 | LEA, HIGHT  SIMON,SPECK |
| TLS | Transport Layer Security의 약어로 통신구간 암호화 및 인증 | TLSv1.2 |
| 펌웨어 암호화 및 서명 | 펌웨어를 암호화 및 서명하여 기밀성, 무결성, 데이터 인증 | AES-128 암호화  RSA-2048 서명 |
| 시큐어 업데이트 | IoT 기기에 체계적이고 신뢰할 수 있는 방법으로 보안 패치를 적요하는 방법 | 주기적인 패치 제공  안전한 암호 알고리즘 |
| 공개키 핀 | 서버 인증서가 전송 중에 변조되지 않음을 탐지하여 중간자공격 차단 | 공개키 정보(SPKI)  체인 검증, 키 갱신 |
| 칩 보안 | 기기에 보안 칩을 장착하여 안정성 확보 후 소프트웨어를 실행하면서 이상 유무 확인 | SE  TEE  PUF |
| 시큐어 부팅 | 기기 부팅 및 실행 전 서명 검사를 통해 해킹이나 악성코드 침투에 의한 소프트웨어 위조 및 변조를 근원적으로 방지 | Root of Trust  RSA 서명 및 검증 |
| 시큐어 디버그 | 디버그 포트에 전기적인 무작위공격을 가하더라도 반응하지 않도록 응답 차단하고, 별도의 하드웨어 장치를 연결하여 비밀 키를 송수한 경우에만 접근 활성화 | 암호화 통신  시큐어, JTAG-UART |
| 버퍼오버플로우 방지 | 스택, 힘, 라이브러리 메모리 공간의 버퍼 오버플로가 발생하지 않도록 실행 방지, 메모리 랜덤 할당, 덮어쓰기 탐지 등을 OS 및 바이너리 빌드 시 적용 | NX(non-execurte)  ASLR  Stack Smashing  Protector |

* **개선 및 발전 방향**

IoT 보안 대응 기술을 적용하기 위해서는 예산, 인력 그리고 복잡성과 현재 운영 중인 서비스의 안정성 등 총체적인 사항들을 고려하고 또한, 보안에 대한 취약점의 경중을 파악하여 선별 적용해야 한다. 그렇기 때문에 이러한 시스템을 체계적으로 개선 및 발전하기 위해서는 두 가지 사항이 존재한다. 첫 번째는 **IoT 제품에서 발견된 취약점의 위험을 CVSS(Common Vulnerability Scoring System) 점수**로 평가하는 것이고 두 번째는 **IoT 보안인증 서비스를 정책적으로 추진**하는 것이다.

먼저, CVSS는 취약점에 대한 위험을 평가하고 각 점수의 구간에 따라서 Level 4(심각), Level 3(중요), Level 2(보통) Level 1(낮음) 등급을 부여하여 이에 따른 의사 결정을 하는 것이다.



**그림 3. CVSS 예시 | 출처 : LG CNS**

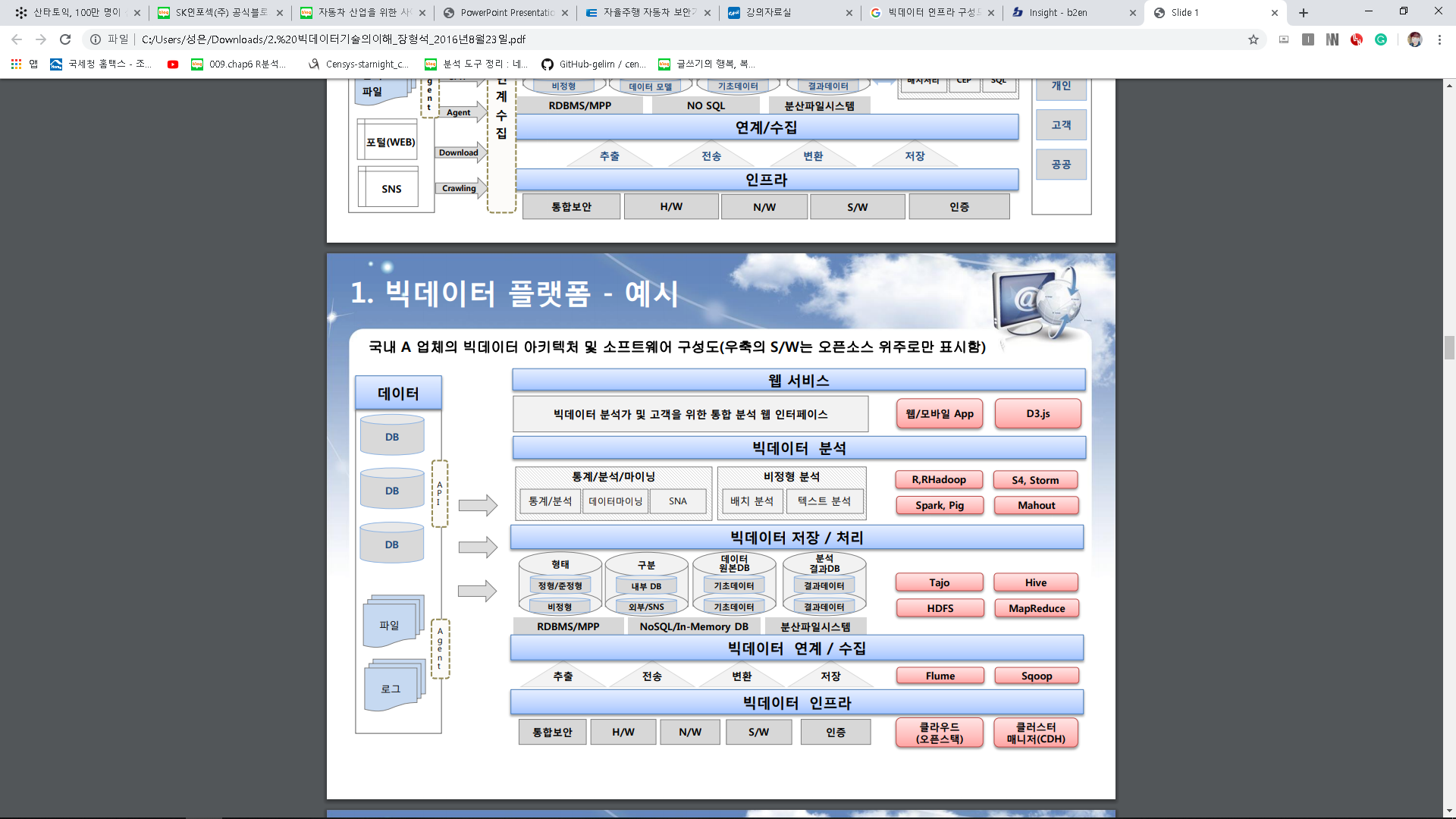
즉., 여기서 두번째인 ‘busybox 명령어를 악용한 코드 실행’ 항목의 경우 총 위험 점수가 8.3점으로 Level 3(중요)에 해당한다. 그러므로 확인된 취약점 중에서 2번째로 보안 기술 점검이 이루어 져야한다. 가장 낮은 점수인 3.6점을 받은 취약점 항목의 경우 후순위로 반영하거나 별다른 위험이 없다면 유지보수를 하는 것이 효율적이라고 판단하여 결정할 수 있다.

두 번째 개선 사항은 ‘IoT 보안인증 서비스’를 정책적으로 운영해야 한다는 것이다. 현재, IoT 시장은 급격하게 사업이 성장하고 있으며 동시에 사이버 공격에 따른 피해액도 급증하고 있다. 즉, 사용자 개개인이 사후 보안조치가 불가능한 상황에서 보안 기술을 활용한 보안 내재화가 필수라는 것이다. 또한, IoT 기술이 탑재되어 있는 제품에 대해 서비스 제공자 및 제조사 그리고 사용자가 모두 관심을 가져야한다. 이러한 이유로 국제적인 보안 가이드와 표준 등을 고려한 총체적인 기준을 선정하고 기기의 보안 기술이 일정 등급 이상으로 판단되면 해당 기기에 대해 표준 인증 서비스를 부여한다는 것이다. 이 서비스가 운영된다면 글로벌 진출시에도 수월하게 제품을 수출할 수 있을 뿐만 아니라 사용자들이 안정성이 있는 기기라는 인식을 가질 수 있기 때문이다.

* **빅데이터 보안 시스템**
* **용어 정리**

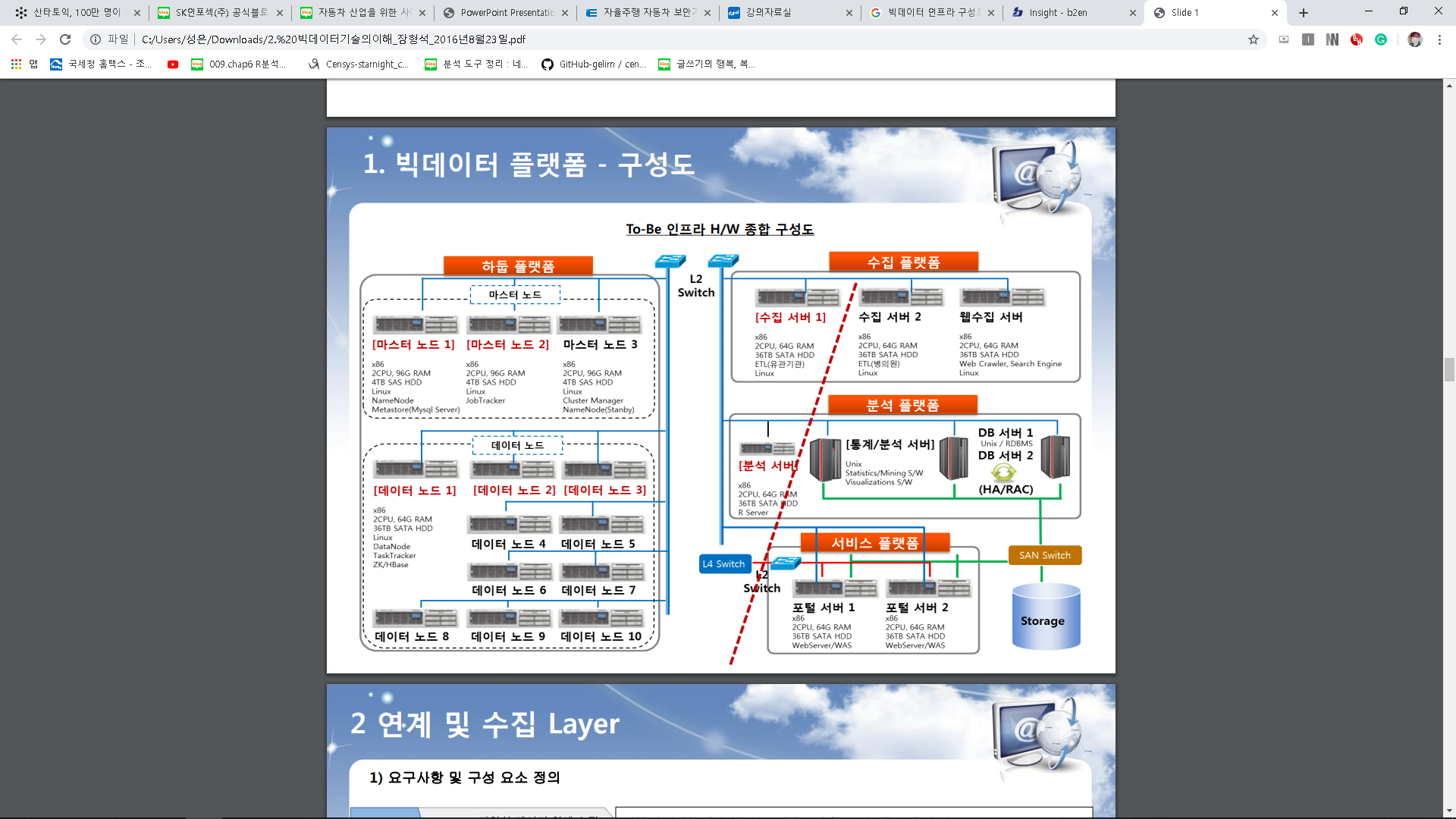
|  |  |
| --- | --- |
| 빅데이터 | * 3V를 만족하는 데이터 또는 그러한 데이터를 처리하는 기술 |
| 소셜 데이터 분석 | * 소셜 데이터를 통한 표본의 성질을 분석하는 것 |
| 데이터 마이닝 | * 통계학에서 패턴 인식에 이르는 다양한 계량 기법을 사용 * 탐색적자료분석, 다변량 분석 등의 방법론과 데이터베이스 * 의 OLAP(온라인 분석 처리) 등의 기술적인 방법론이 사용된다. |
| 텍스트 마이닝 | * 소셜상의 텍스트 데이터를 수집하여 자연어 처리를 통해 * 주 키워드와 특정 키워드에 대한 긍정 및 부정률을 판단한다. |
| 정형 데이터 | * 정형화 되어있는 데이터 |
| 비정형 데이터 | * 정형화 되어있지 않은 데이터이며, 음성, 영상 그리고 사운드 * 가 대표적인 예이다. |
| 데이터 웨어하우스 | * 사용자의 의사 결정에 도움을 주기 위해, 기간시스템에 데이터 * 베이스에 축적된 데이터를 공통의 형식으로 변환, 관리하는 * 데이터베이스이다. |

* **빅데이터 플랫폼**

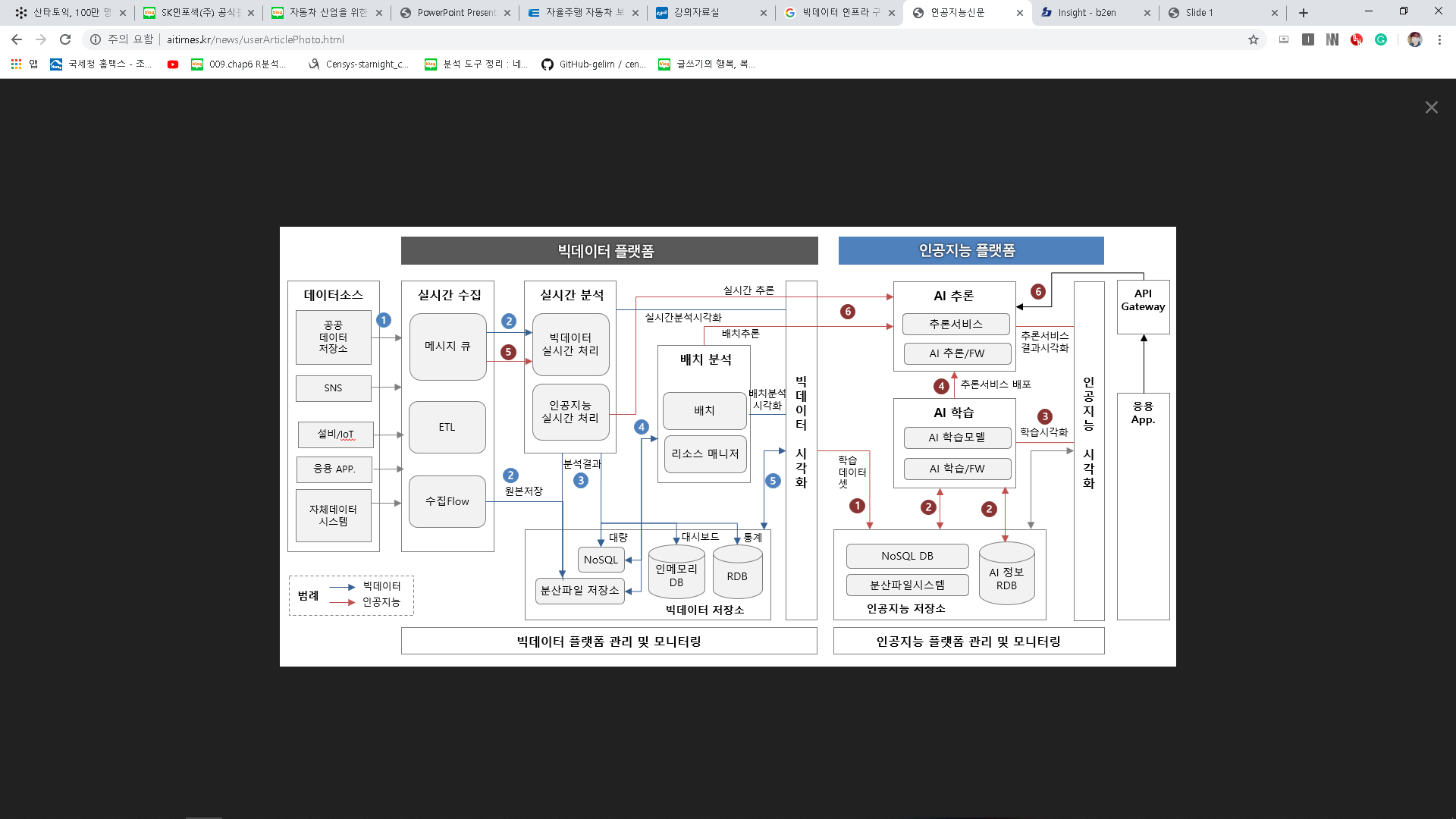


**그림 4. 빅데이터 플랫폼 | 출처 : “빅데이터 기술의 이해”, 강성일**

* **빅데이터 시스템 구성도**



**그림 5. 빅데이터 구성도 | 출처 : SK Infosec**



**그림 6. 빅데이터 및 인공지능 결합 구성도 예시 | 출처 : 티쓰리큐**

* **보안 시스템 주요 기능 및 특징**

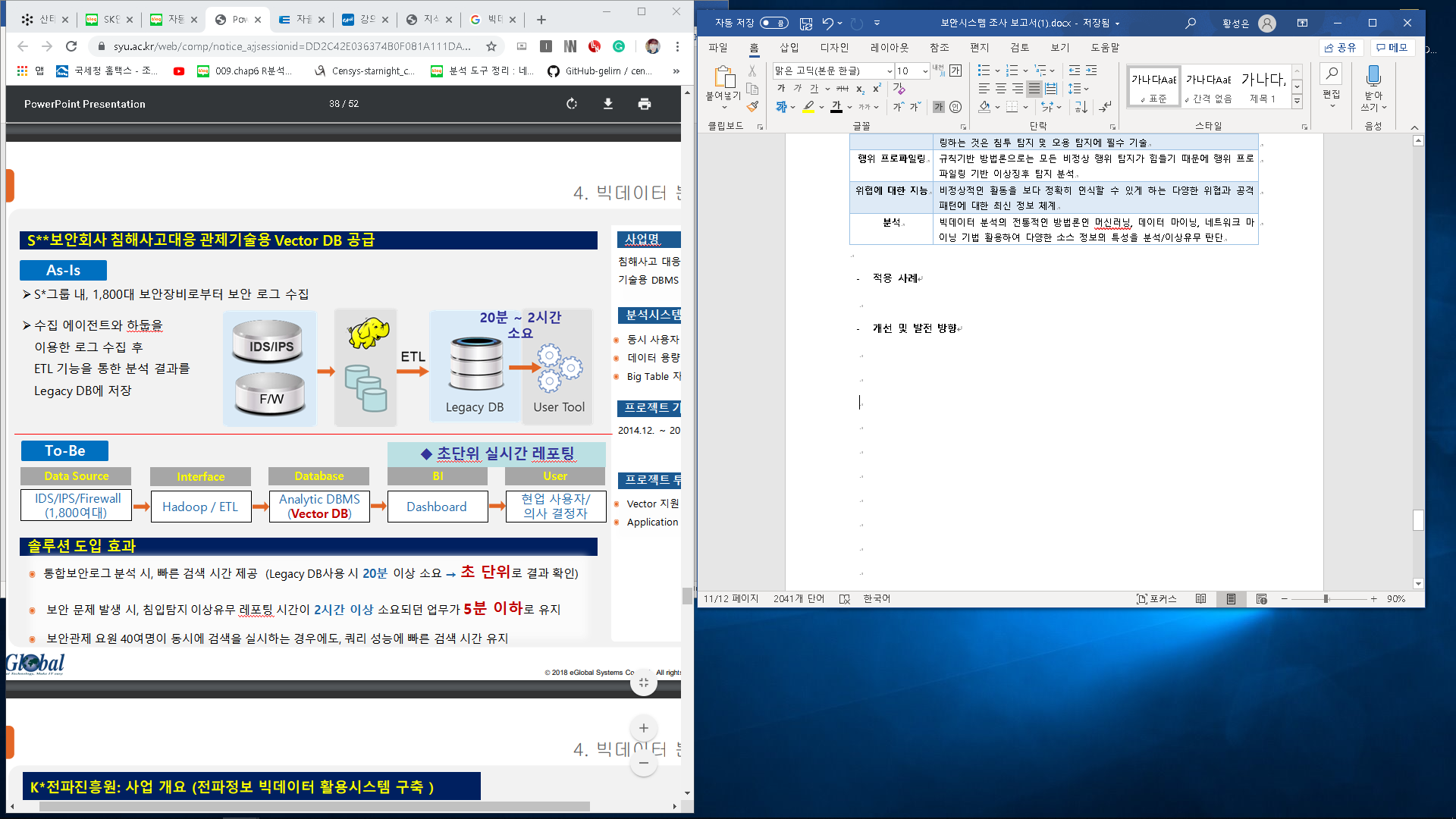
먼저, 빅데이터가 보안에서 갖추어야할 **4가지 핵심요인**이 존재한다.

|  |  |
| --- | --- |
| 핵심요인 | 특징 |
| 알고리즘(Algorithms) | 다량의 정보를 수집 및 가공함에 있어서 알고리즘을 이용하여 지능형 기술의 도움을 받아서 빠른 시간에 효율적으로 분석 가능 |
| 자동화(Automation) | 지속적으로 위협에 대해 탐지하며, 공격이 발생시 자동으로 대응하는 기능이 있다. |
| 텍스트(Context) | 사이버 공격을 탐지하고 디지털 포렌식의 기능을 활성화하여 지속적으로 모니터링을 하는 특징이 있다. |
| 시각화(Visualization) | 비정형 및 정형 데이터들의 시각화를 통해 다방면의 취약점이나 위협이 발생시 신속한 대처 능력이 향상된다. |

1. **빅데이터의 보안 분석기술**

|  |  |
| --- | --- |
| 분석기술 | 특징 |
| 실시간 모니터링 | 시스템 구성요소에 대한 공격상황을 추적하고 분석  응용 프로그램 상에서 사용자의 활동성을 모니터링하기 위하여 다양한 소스로부터 데이터를 수집 관리하는 기술 |
| 응용 모니터링 | 응용프로그램 취약점은 표적공격의 주요 타깃이므로 비정상 응용 프로그램의 활동성 모니터링 기술 |
| 데이터 모니터링 | 사용자 및 데이터의 컨텍스트를 포함한 데이터/사용자의 활동성을 모니터링하는 것은 침투 탐지 및 오용 탐지에 필수 기술 |
| 행위 프로파일링 | 규칙기반 방법론으로는 모든 비정상 행위 탐지가 힘들기 때문에 행위 프로파일링 기반 이상징후 탐지 분석 |
| 위협에 대한 지능 | 비정상적인 활동을 보다 정확히 인식할 수 있게 하는 다양한 위협과 공격 패턴에 대한 최신 정보 체계 |
| 분석 | 빅데이터 분석의 전통적인 방법론인 머신러닝, 데이터 마이닝, 네트워크 마이닝 기법 활용하여 다양한 소스 정보의 특성을 분석/이상유무 판단 |

* **적용 사례**



* **개선 및 발전 방향**

**가. 빅데이터 주요 위협 요인**

|  |  |  |
| --- | --- | --- |
| 구분 | 취약항목 | 위협 요인 |
| 저장(PPDM) | 개인정보유출 | BigData(회원정보, 고객정보)분석 수행시 개인정보 유출 및 다른 용도사용 |
| 시스템(Hadoop) | Kerberos | 네트워크로 블록접근 토큰(Kerveros) 취득하여 공유 비밀키 갱신전까지 해당 블록 접근 가능 |
| Securiy미지원 | Zookeeper, HttpFS(CDH3기준) |
| 응용(통합보안) | APT | 분석 데이터가 증가하고, 보안 위협 요소가 빅데이터에 잠복할 가능성 있음 |
| BYOD위협 | 기업의 IT통제권 상실, 단말기 취약점 및 악성코드로 인한 기업 내부 정보 유출 위협, 악성코드에 감염된 개인용 기기의 내부 접속으로 기업 IT자산 위협, 단말기 도난 또는 분실로 인한 데이터 유출 |

* APT(Advaned Persistent Threat) :clheo수개월에서 수년에 걸쳐 타겟 정하고 공격
* BYOD(Bring Your Own Device)

**나. 빅데이터 보안 위협 요인 대응방안**

|  |  |  |
| --- | --- | --- |
| 구분 | 대응방안 | 위협 요인 |
| 저장  (개인정보) | PPDM  (랜덤화/데이터섭동) | Privacy를 보호할 수 있도록 변환하거나 이를 보호할 수 있는 방법을 사용하여 데이터마이닝을 수행하고 그 결과를 얻어냄 |
| 다주체보안 연산 | SCM(Secure Multiparty Computation) |
| 시스템  (Hadoop) | CDH4기준 Security지원 | - MIT Kerberos 5(krb5-1.6.1)  - Hadoop Security with Active Directory  - ZooKeepter-support Kerberos |
| 응용  (통합보안) | APT | 분석 데이터가 증가하고, 보안 위협 요소가 빅데이터에 잠복할 가능성 있음 |

* **애플리케이션 보안**

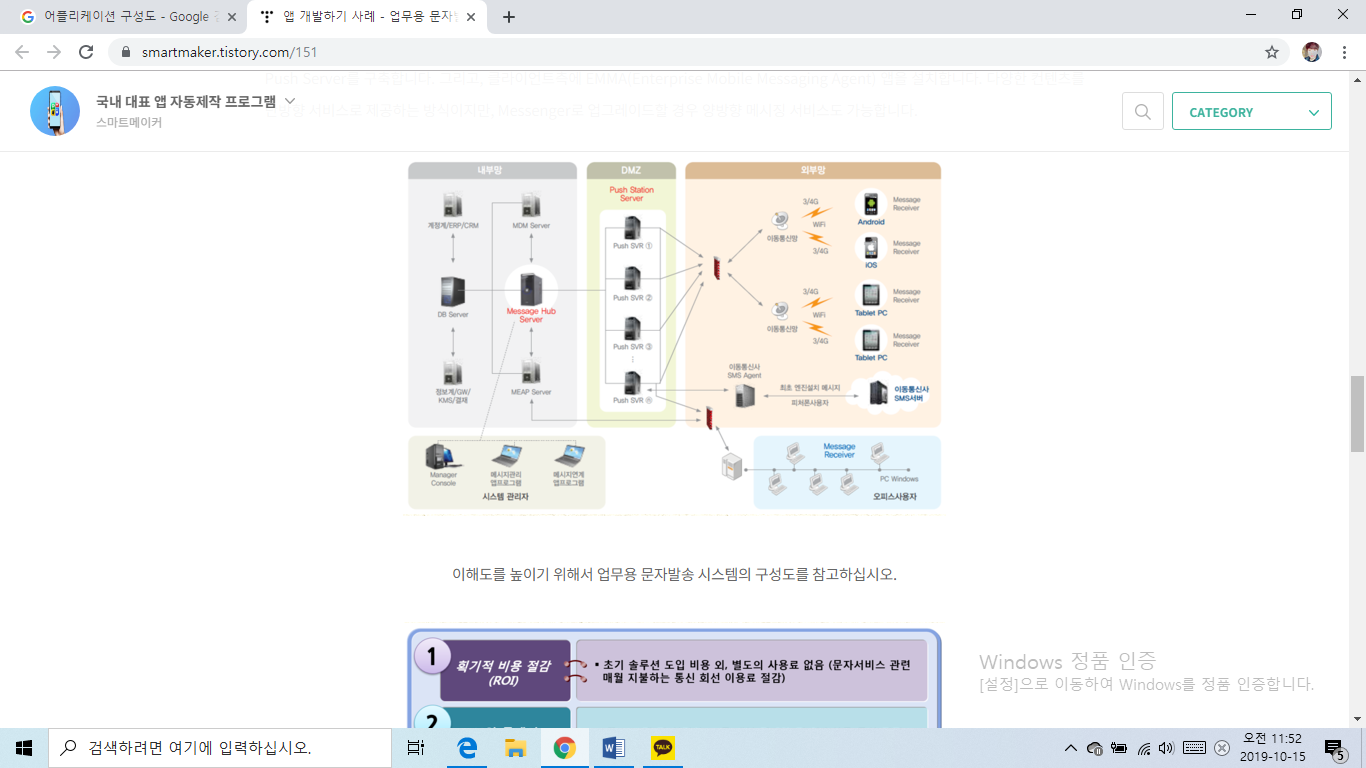
애플리케이션 보안은 외부의 공격으로부터 애플리케이션을 보호하는 역할을 한다. 사이버 범죄는 조직적이고 전문적이며 데이터, 지적 재산 및 민감한 직원 또는 고객 정보를 훔치기 위해 기업 애플리케이션에서 취약점을 찾아 악용하는 데 중점을 두는데, 애플리케이션 보안에서 80% 이상이 애플리케이션 레이어의 취약점을 표적으로 삼고 있으며 이는 기업 IT 부서가 애플리케이션 보안에 대한 경계 태세를 가져야 함을 의미한다.

* **용어정리**

|  |  |
| --- | --- |
| 용어 | * 기능 |
| 웹 스캐너 | * 외부에서 애플리케이션을 점검하는 역할 |
| 웹 어플리케이션 방화벽 | * SQL 인젝션, 버퍼 오버플로우, 악성 소스 등의 공격을 * 방어하는 방화벽의 역할 |
| 시큐어 코딩 | * 취약성이 있을 수 있는 코드를 배제하고 안전한 소스 * 프로그램을 사용하는 코딩 |
| 웹 해킹차단 시스템 | * 외부의 접근으로부터 보안을 위해 해킹차단 시스템을 설 * 치하여 웹 보안 취약점이 외부에 노출되지 않도록 함. |
| 데이터 보안 | * 데이터 베이스를 구축하여 데이터를 보안하고 관리 |
| 애플리케이션 악성코드  탐지 | * 애플리케이션 내부에서 동작하며, 웹셀 및 웹서버 악성 * 코드라고 불린다. |

* **구성도, 구성방안**
* 

**그림 7. 모바일 어플리케이션 보안**



**그림 8. 웹 어플리케이션 보안**

* **주요 기능 및 특징 (보안솔루션)**

|  |  |  |
| --- | --- | --- |
| 기술 | 설명 | 상세 기술 |
| Fortify Static Code Analyzer | 소프트웨어 개발 수명 주기 초기에 소스 코드에서 보안 취약점을 식별하고 감지. | SAST |
| Fortify Web Inspect | 실행 애플리케이션에 대한 실제 보안 공격을 시뮬레이션, 복잡한 웹 애플리케이션과 서비스에 대한 포괄적인 분석을 제공. | DAST |
| Interactive Application Security Testing | 동적 테스트와 런타임 분석을 통합하여 공격 표면 범위를 확대시키고 악용 사례를 노출시킴으로써 동적 테스트만 사용하는 경우보다 많은 취약점을 식별가능 |  |
| Fortify Application Defender | 알려진 취약점과 알려지지 않은 취약점이 있는 생산 환경에서 애플리케이션을 적극적으로 모니터링 및 보호. | 런타임 애플리케이션 자가 보안 |
| 모바일 보안 | 클라이언트, 네트워크, 서버를 포함한 3가지 계층을 모두 테스트하는 모바일 테스트 방법론 |  |
| 소프트웨어 보안 보증 | 중앙 집중식 관리 저장소가 보안 취약성 해결에 도움을 주는 가시성을 제공. |  |

* **개선 및 발전 방향**

안드로이드 앱 서비스 관련 구체적인 위협들에 대한 대응을 개선시킬 수 있는 방안을 몇 가지 고려하였다.

|  |  |
| --- | --- |
| 구분 | 위협 시나리오 |
| 1. 단말 내 인증-암호화 KEY 노출 | 앱 분석 및 역컴파일 등의 방법을 통해 중요 인증- 암호 KEY 노출 및 절취 대칭 키 암호, DeviceID 인증 및 PW 노출 |
| 1. 루팅 등 무결성 훼손 | 루팅 폰에서 앱 구동 시 데이터 처리 로직 및 서버 정보 등 비인가 정보 접근 가능 |
| 1. APK 추출 및 Decompile | APK 추출 후 Debug mode를 통해 취약점을 파악.  서비스의 중요 정보 및 개인정보를 얻을 수 있음. |
| 1. APP 위조 및 변조 | 코드 및 행동 분석 후 주요 정보에 대한 유출 |

이러한 유형의 취약점에 대한 대응 방안은 크게 OS보안, APP보안 및 암호화(H/W)가 있다.

**1) OS 보안**

Rooting 점검을 할 수 있는데, 이 경우 Boot OS의 무결성을 검증하고 보장할 수 있다.

**2) APP 보안**

App 보안 단계에서는 난독화 적용과 코드서명 그리고 Hash 검증을 통해 위협 시나리오에 대응이 가능하다. 만약, OS 보안 및 app 보안에도 불구하고 해킹을 당할 경우, OS 및 APP은 무력화되며 이 단계에서 암호화 보안이 적용되어야 한다.

**3) 암호화 보안**

하드웨어 기반 암호화 key의 안전한 보호를 통해 개인정보의 유출을 방지할 수 있다.

* **자동차 보안**

자동차 보안의 경우 사이버 보안에 큰 영향을 미치며, 각각의 복잡한 시스템에는 크고 작은 결함들이 존재하므로 절대적인 보안은 없다. 그러므로, 자동차 보안에 관하여 기업은 프로세스 및 네트워크 망에 대한 전체 Lifecycle을 통해 안정성을 가지고 동작할 수 있는 기반을 가진 취약점 보호 사이버 보안 관리를 확립해야한다.



**그림 9. 취약점 중심 보안의 전체 라이프 사이클**

|  |  |
| --- | --- |
| 용어 | * 기능 |
| ECU  (Electronic Control Unit) | * 전자 제어 유닛 |
| V2V  (Vehicle – to - Vehicle) | * 차량과 차량 간의 통신 |
| V2I | * 차량과 인프라 간의 통신 |
| UDS(Unified Diagnostics Service) | * 차량 안전/보안 진단을 위한 표준 |
| DoIP  (Diagnostics over IP) | * 인터넷 프로토콜을 통한 진단 표준 |
| V2N | * 차량과 클라우드 간의 연계 서비스 |
| CCC | * 차량과 연결된 컨소시엄 |
| OBD | * On-Board Diagnostics |
| FOTA | * 펌웨어를 활용한 기술 |
| AFW  (Application Firewall) | * 자동차용 AFW는 자동차 통신 프로토콜에 최적화된 어 * 어플리케이션 방화벽. |

* **주요 기능 및 특징**

안정성을 가진 자율주행 자동차 및 스마트 자동차의 실현을 위해서는 플랫폼, 내부 및 외부 네트워크 보안 그리고 유지관리 등 총 4가지 영역에 대한 보안이 구축되어야 한다.

각 영역에 대한 자동차 보안 **핵심기술**의 **주요 기능 및 특징**을 알아보겠다.

1. **자동차 전장 플랫폼에 대한 핵심 보안기술**
2. 자동차 ECU/IVI 가상화 기술

: ECU 해킹 및 비인가 접근 공격으로부터 자동차의 임의적인 제어를 보호하는 기술이다.

1. 다중 센서 융합 기반 주행 분석 기술

: 자동차의 각 부품에 도입된 시스템이 서로 오류가 나는 경우를 대비하여 센서를 다중으로 분석하여 연결을 유지하도록 하는 기술이다.

1. 자동차 키 관리 및 유지 기술

: 자동차의 네트워크 간 통신의 무결성과 기밀성을 확보하는 역할을 하는 기술이다.

1. **자동차 내부 및 외부 핵심 보안기술**
2. 자동차 방화벽

: 자동차 내부 네트워크에 대한 침투 및 공격을 보호하는 시스템이다.

1. 자동차 Ethernet 실시간 접근제어 기술

: 이더넷 기반의 시스템으로부터 외부에서 원격 제어하는 공격을 방지한다.

1. **자동차 보안 관리 및 유지 핵심 보안기술**
2. 취약성 자동분석 기술

: 자율주행자동차의 기능에 도입된 SW 설계를 표준화에 따라 분석하고 보안 수준을 도출하는 기술이다.

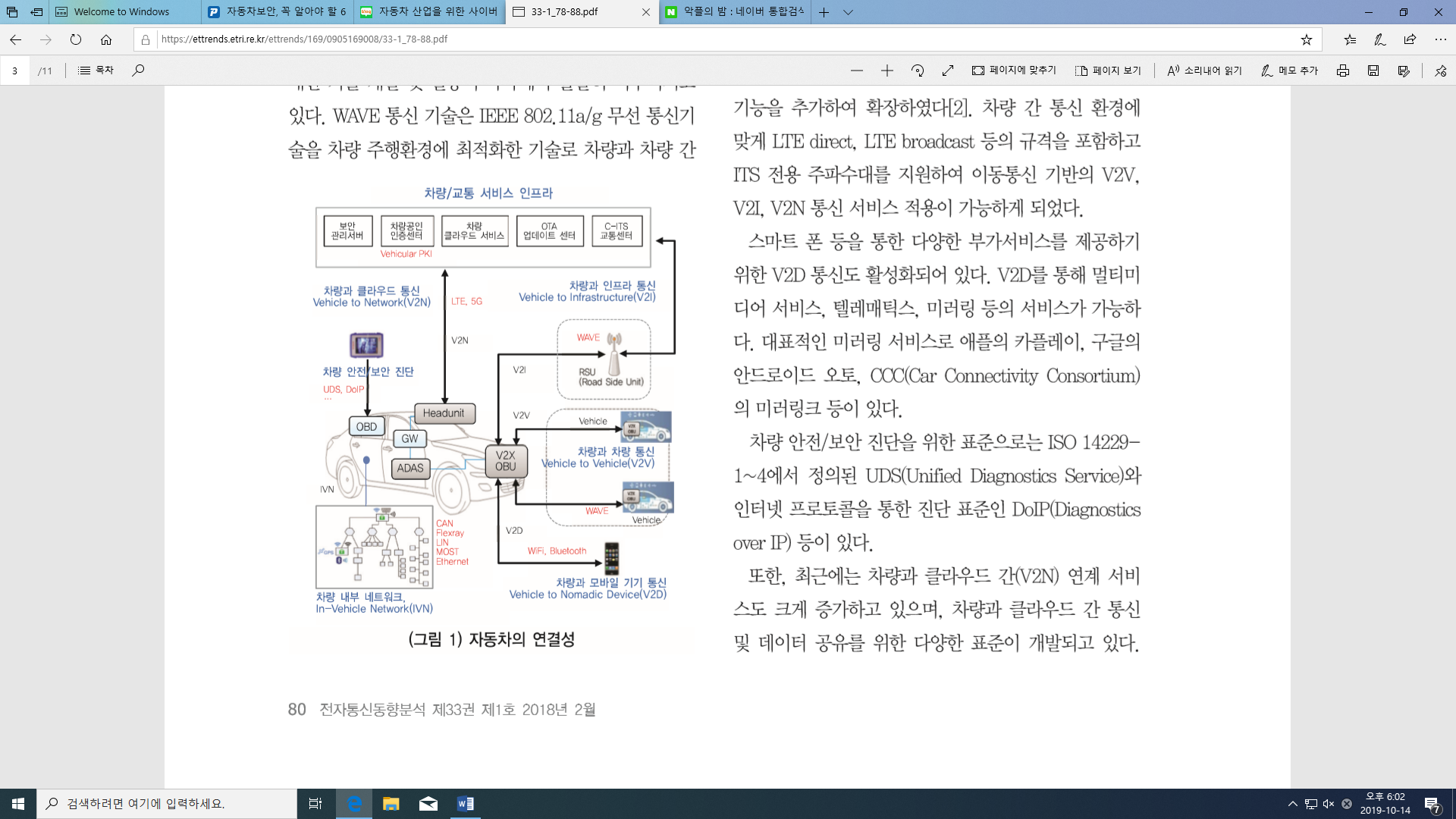
1. 침투시험 기술

: 시뮬레이션을 통해 알려지지 않은 취약성 및 공격으로부터 방어하고 대응책을 마련하는 기술.

* **구성도, 구성방안**



**그림 10. 자동차 보안 실제 설계도**



**그림 11. 자동차의 연결성**

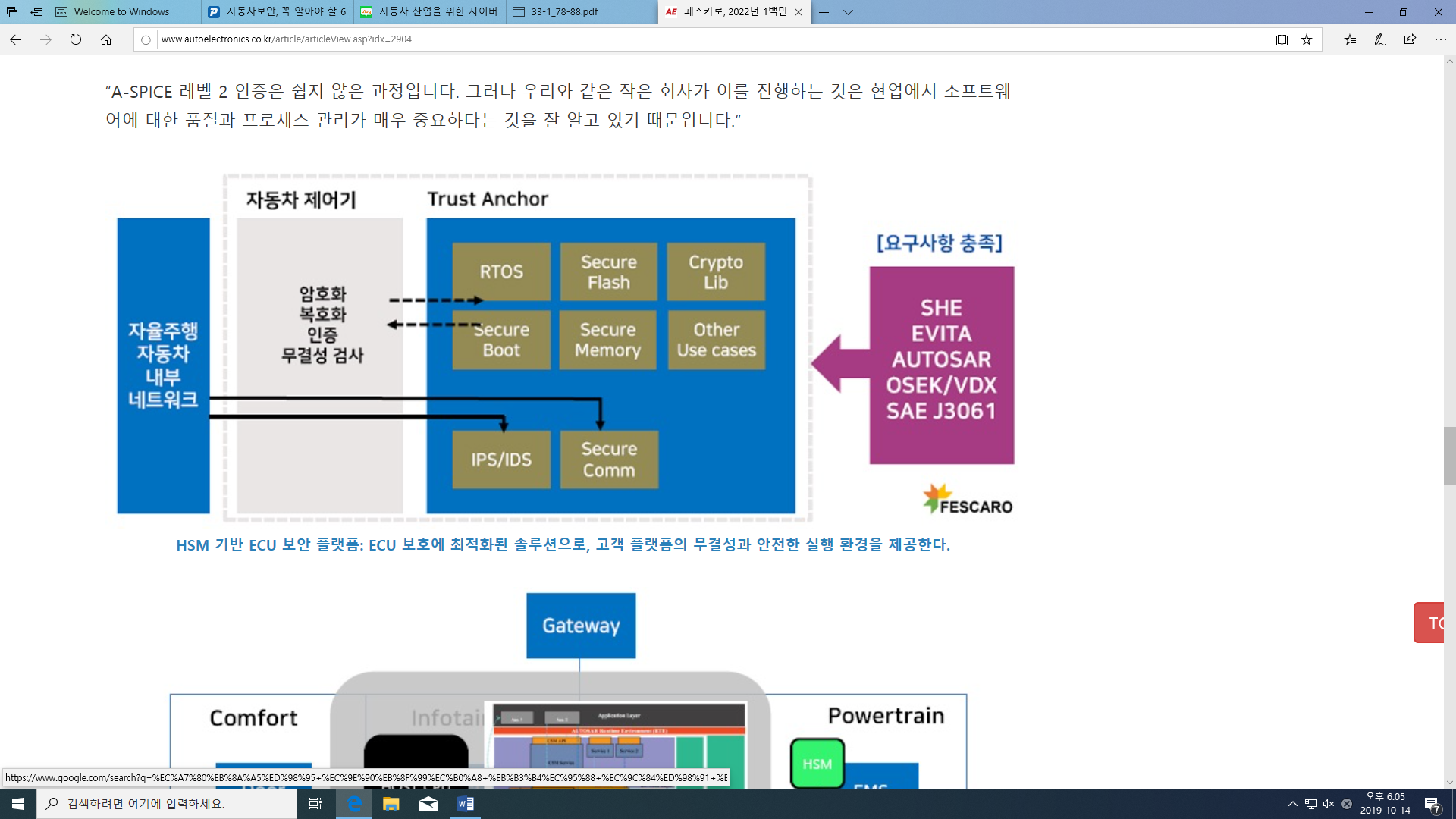
* **적용 사례**

자동차의 지능화 및 연결성의 확대로 인해 정밀한 자율주행 서비스가 가능한 측면도 존재하지만 반대급부로 취약점을 통한 사이버 공격 즉, 보안 위협이 계속적으로 증가하고 있다.

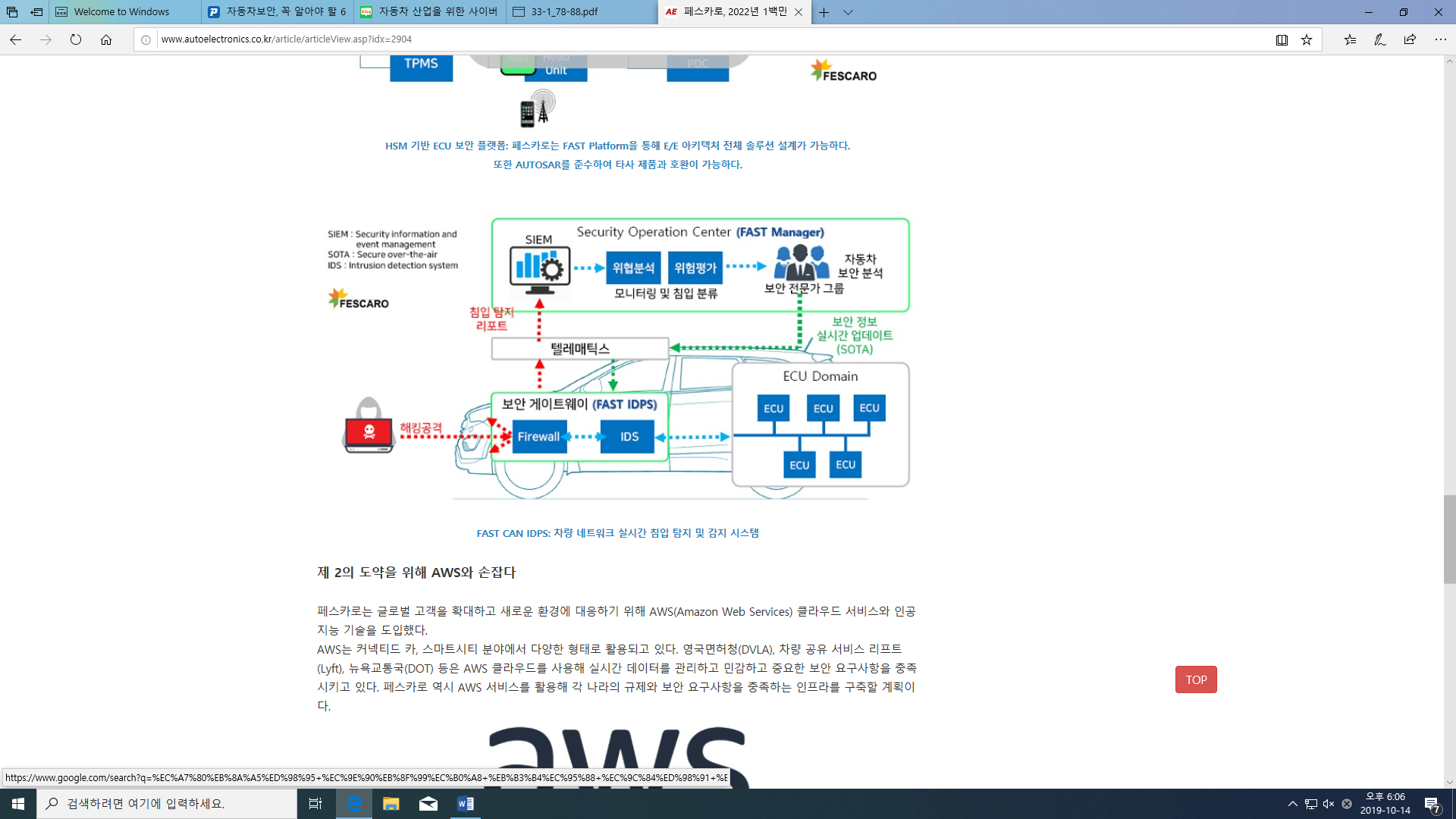
다양한 사례들이 존재하는데, 2014년 해커가 지프 체로키를 해킹한 후, 원격 조정하여 당시 주행중인 차량을 급정거함과 동시에 차량을 배수로로 곤두박질 시키는 사건이 있었다.

또한, 2016년에는 미쓰비시 차량의 와이파이 구간을 해킹하여 원격으로 차량의 제어장치를 조작하여 잠금을 해제하고 헤드라이트 및 다른 부품들을 임의로 제어한 사건도 발생하였다.

자동차 보안을 위해 여러가지의 방식의 보안 기술 및 시스템들이 개발, 적용되고 있으나 지속적으로 이러한 피해가 발생하며, 그 메커니즘은 점점 지능화 및 고도화되어지고 있다. 페스카로社의 자동차 보안에 대한 두 가지의 시스템을 차량에 적용한 사례를 알아보겠다.



**그림 12. 페스카로의 HSM 기반 보안 시스템 적용 사례**



**그림 13. 차량 네트워크 IDS 및 IPS 시스템 적용 사례**

이러한 적용 사례처럼 보안 기능에서 가장 중요한 것은 안정성이며, ‘안정성’이라는 핵심 요인을 확보하기위해 기업은 자동차 보안의 설계 단계에서 보안 위협의 식별과 위험 평가 시스템이 체계적으로 작동될 수 있도록 보안대책을 고려해야한다.

**또한,** 보안기술은 결과적으로 자동차의 제어기에 결합되어 제어 시스템과 함께 작동되어야 하기때문에, 사용자 입장에서 USE Case를 검토하여 최적의 가이드라인을 제시해야함을 알 수 있다.

* **개선 및 발전 방향**

1. **자율주행 자동차의 보안 위협**

|  |  |
| --- | --- |
| 분류 | 보안 위협 |
| 전장 플랫폼 | * ECU 소프트웨어 결함, ECU 리버스 엔지니어링 * ECU 펌웨어 해킹 및 위/변조 * IVI(In-Vehicle Infotainment) 해킹, 악성 감염, 스마트 센서 물리 공격(블라인딩, 스푸핑 등) |
| 내부 네트워크 | * 차량 내부네트워크에 악의적인 제어 메시지 주입 * 정상적인 내부네트워크 방해 (패킷 삽입, 삭제, 임의조작) * DoS, 리플레이, 스푸핑, 패킷 폐기 공격 |
| 외부 네트워크 | * 무선 통신망 해킹, DoS 공격 * 거짓 정보(Fake Message)제공 * 차량 접속 기기 해킹 |
| 관리, 진단 | * 프라이버시 침해, OBD-II 해킹 * 원격 업데이트 및 진단 프로토콜 해킹 * 해킹에 의한 사고원인 분석/증거 보존의 어려움. |

1. **자율주행 자동차의 보안 대응 시스템**

|  |  |
| --- | --- |
| 분류 | 보안 위협 |
| 전장 플랫폼  보안 | * Secure Boot , Secure placing, 접근제어 * 애플리케이션 샌드박스, 플랫폼 가상화 * HSM (Hardware Security Module) * 부채널 방지 |
| 내부 네트워크  보안 | * 침입 탐지 시스템(IDS) 및 침입 방지 시스템(IPS) * ECU 인증, 키 관리, 암호화 * 위협 탐지(Rule-Based, Machine Learning-based) |
| 외부 네트워크  보안 | * 차량 PKI, 메시지 검증 * IEEE 1609.2, CAMP VSC3 등의 표준화 사용 |
| 보안 관리, 진단 | * 보안 모니터링, 보안 취약성 분석 * 차량 이상지후, 비정상 행위 분석 * 포렌식 및 사고 원인 분석 기술 사용 * 원격 SW/FW 보안 업데이트 |

* **스마트 팩토리**
* **용어정리**

|  |  |
| --- | --- |
| 용어 | * 기능 |
| 스마트 공장  (Smart Factory) | * 전통 제조산업에 ICT를 결합하여 제품의 기획, 설계, * 유통 판매 등의 전체 과정을 ICT 기술로 통합하여 최소 * 비용과 시간으로 고객 맞춤형 제품 생산을 지향하는 * 공장을 의미한다. |
| CPS  (Cyber-Physical Systems) | * 다양한 상황 변경에서도 시행착오가 없는 효율적인 * ‘제조 최적화’를 달성할 수 있도록 만드는 시스템. |
| SCADA  (Supervisory Control And Data Acquisiton) | * 통신 경로 상의 아날로그 및 디지털 신호를 이용하여 * 원격 상태 정보 등의 자료를 수집 및 처리하여 중앙 * 제어 시스템이 원격 장치를 감시 제어하는 시스템이다. |
| 가치 흐름  (Value Stream) | * 원재료의 조달부터 최종 소비자에게 이르는 프로세스 * 를 시간과 함께 보여주는 것이다. |
| 공정제어(PLC) | * 프로세서를 이용한 프로그램으로 각 장치들이 * 제어될 수 있도록 통합시킨 컨트롤러이다. |
| 스테이션(Station) | * 일련의 제어 모듈 또는 설비 모듈 등이 그 이상 주요 * 공정을 수행하는 공정 설비를 의미한다. |
| ERP  (Enterprise Resource Planning) | * 기업 전체를 경영자원의 효과적 이용이라는 관점에서 * 통합적으로 관리하고 경영의 효율화를 기하기 위한 * 시스템이다. |
| 제품 데이터 관리 | * 제품의 기획에서 설계 및 인증에 이르는 제품을 개발 * 하고 그 과정에서의 모든 데이터를 일률적으로 관리 * 할 수 있는 시스템이다. |
| 인더스트리 4.0 | * 모듈 단위의 유연한 분산 및 자율 제어 생산 체계이다. |
| 지능화 | * 생산 현장의 기계들이 스스로 판단하여 제어하며, 각 기 * 계들 간에 자율적인 협업을 통해 최적의 효율성을 냄. |

* **주요 기능 및 특징**

1. **네트워크 보안**

네트워크 보안을 위해서는 업무 영역과 OT 영역을 세분화하여 네트워크를 분리하고, 세분화된 네트워크는 방화벽 및 네트워크 설정으로 접근을 통제해야 한다.

1. **침입/악성코드 탐지**

먼저 외부망에서 내부 스마트 팩토리를 보호하기 위해 인터넷 점접에서 침입을 탐지/방지할 수 있는 솔루션을 구축해야 한다. 또한, 공장 내부에서도 산업제어시스템 무결성 및 가용성 침해에 대응하여 산업제어시스템 이상징후 탐지 솔루션을 구축한다.

1. **생산 기술 및 중요 정보 보호**

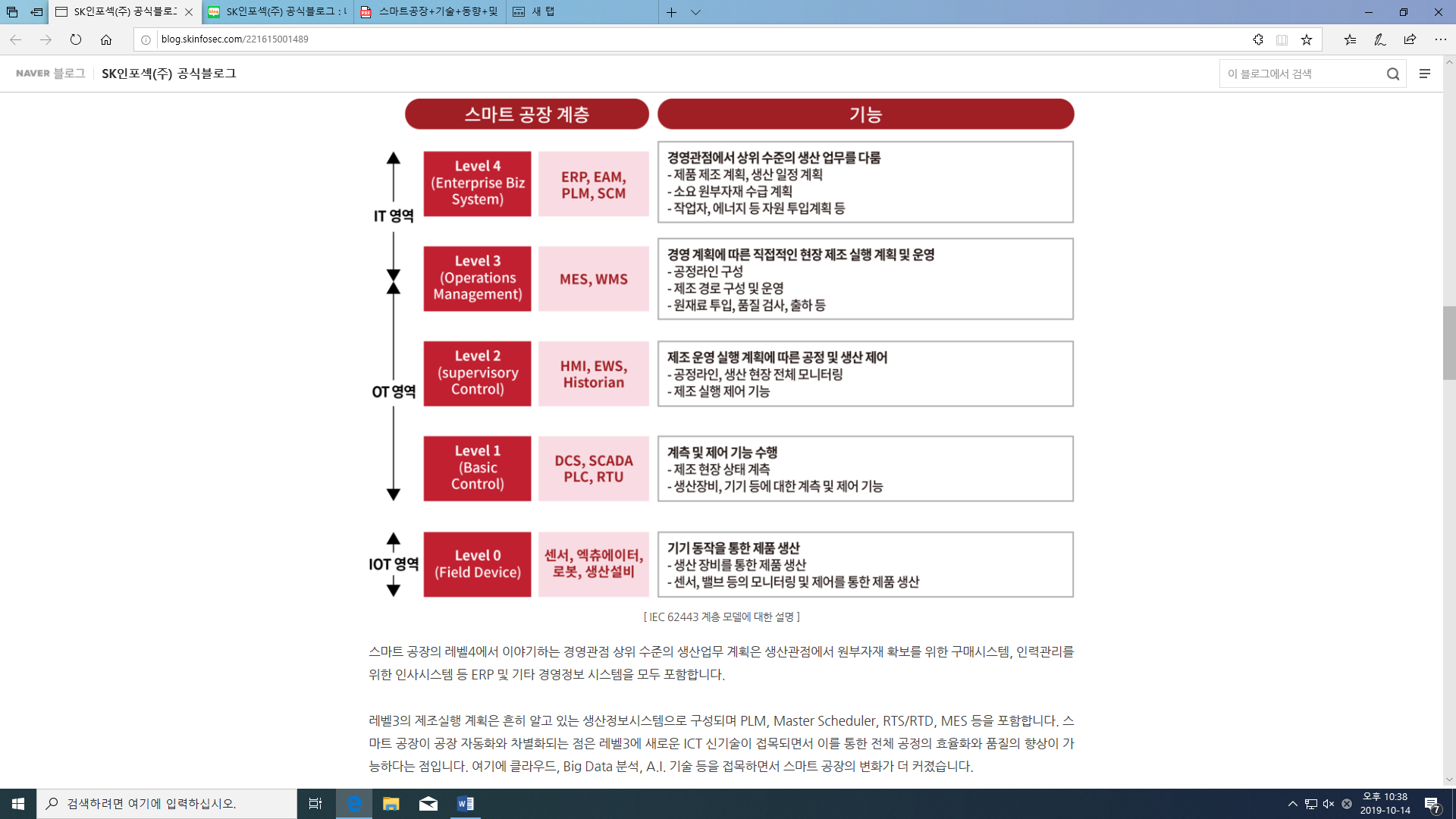
이러한 기술 및 중요 정보들을 보호하기 위해서는 각 기업의 중요한 정보가 무엇인지 파악하는 것이 중요하다. 스마트 팩토리의 중요정보는 국가 핵심기술 및 특허기술 그리고 제품생산정보, 제조공정도, 설계 도면 등이 존재하며, 기업마다 보호해야하는 정보들이 다르기 때문에, 어떠한 정보가 중요한지 어디에 저장되며 활용될 수 있는지를 파악해야 한다.

* **구성도, 구성방안**



**그림 14. 스마트팩토리 구성도 | 삼정KPMG 경제연구원**

* **플랫폼**



**그림 15. IEC 62443 계층 모델에 대한 플랫폼**

* **적용 사례**

국내에도 ‘스마트 공장’을 적용하는 사례가 지속적으로 증가하고 있다.

LS 산전은 충북 공장에서 시스템의 설계부터 시작하여 품질 관리 그리고 적용까지 Life cycle이 가능한 스마트 시스템을 적용하고 있다. 또한, 경남에 위치한 계란공장인 ‘젤란’은 마트에서 계란 판매량을 공장의 상황실 모니터로 실시간을 파악하여 계란의 신선도를 확인하고 적재적소에 도착할 수 있도록 만드는 체계적인 시스템을 이용하고 있다.

또한, 대기업인 삼성전자도 예외가 아니다. 삼성전자는 경북 창조 경제혁신센터와 협약을 맺고 경북지역에 100여 개의 스마트공장을 건설할 계획이며, 내후년까지 총 400여 개의 스마트 공장 육성을 목표로 한다. 삼성전자와 현대자동차는 국내가 아닌 국외에 설립되어 있는 생산라인에 대한 정보를 실시간으로 공유하는 스마트 시스템을 적용하여 제품의 라이프 사이클을 이전보다 50%이상 단축하는 효율성을 보여주었으며 이러한 시스템을 기반으로 시장에서 경쟁사를 제치고 경쟁 우위를 차지하고 있다.

* **개선 및 발전 방향**

스마트 팩토리의 특성상 제품의 생산을 주 목적으로 하므로 일반적인 팩토리와는 별개의 특성 및 성격을 가지고 있다. 그 중에서도 보안의 3요소인 기밀성, 무결성, 가용성이 핵심이며 IT 와 OT에 따라서 각 요소의 우선순위가 구별된다.

|  |  |  |
| --- | --- | --- |
| 우선순위 | 일반 Factory | 산업 Factory |
| 1 | 기밀성(Confidentiality) | 가용성(Availability) |
| 2 | 무결성(Integrity) | 무결성(Integrity) |
| 3 | 가용성(Availability) | 기밀성(Confidentiality) |

즉, 기밀성이 최우선적으로 보장되어야 하는 일반적인 공장과는 달리 스마트 팩토리에서는 어떠한 환경이더라도 지속적인 생산 활동이 이루어져야 하기 때문에 가용성이 가장 중요하다고 할 수 있다.

**스마트 팩토리의 전체 제조 영역에 대하여 보안을 유지할 수 있는 몇 가지의 사항이 존재한다.**

1. **보안을 위한 정책과 절차의 수립**

정책과 절차에는 인증 및 권한에 따라서 어떠한 정보까지 접근하고 제어할 수 있는지, 통신이 암호화되었는지, 변경사항이 주기적으로 업데이트되는지에 대한 내용이 명시되어야 한다. 이러한 정책 및 절차들이 표준적인 기준이 되어서 기업의 작업자나 사용자에게 적용이 될 경우, 효율적인 보안 시스템과 체계가 형성될 수 있다.

1. **각종 디바이스에 연결되어 있는 네트워크에 대한 지속적인 점검 및 유지 보수**

유지 보수에는 정기 업데이트와 바이러스 검사 및 악성코드 분석 프로그램이 필요하며, 장치 내에 불필요한 요소들을 제거해야 한다. 또한, 외부에서 들여온 매체들에 대한 엄격한 접근 제어가 실시되어야 할 것이다.

* **Reference**

<http://www.kisa.or.kr/uploadfile/201805/201805290956314977.pdf> “스마트 의료보안 구성 및 보안”

<https://search.zdnet.co.kr/?kwd=%EB%B3%B4%EC%95%88%EC%8B%9C%EC%8A%A4%ED%85%9C>

“ZdNet Korea, 보안시스템”

<http://blog.skinfosec.com/>“ SK 인포섹 공식블로그”

<https://blog.naver.com/controlinstrument/> “ 스마트그리드 최근 동향 및 보안 이슈”

<https://www.sciencetimes.co.kr/> “보안업계에 관한 기사”

<http://www.kisa.or.kr/public/laws/laws3.jsp> “ 한국인터넷 진흥원 기술안내서 가이드”

<http://www.digitaltoday.co.kr/> “5G AI IoT 빅데이터 ‘4차산업혁명 시대’

[https://www.pentasecurity.co.kr](https://www.pentasecurity.co.kr/) “Penta security 홈페이지”

[https://blog.lgcns.com](https://blog.lgcns.com/) “LG CNS 보안컨설팅팀”

<http://www.aitimes.kr/news/articleView.html?idxno=11782> 티쓰리큐, AI 플랫폼 'PATROL.ai' BC카드 '실시간빅데이터' 플랫폼에 적용

<http://www.autoelectronics.co.kr/article/articleView.asp?idx=2904>

“페스카로, 2022년 1백만대 자동차 보안 적용”

<https://blog.naver.com/vectorteam/220964152834> ”자동차 산업을 위한 사이버 보안”

<https://www.industrynews.co.kr/news/articleView.html?idxno=25956> “스마트 팩토리 구축의 핵심은 'CPS'”