**<보안기술>**

1. 원격근무 환경에서 계정 보안 강화 -> 차세대 방화벽
2. 클라우드 보안 클라우드 기반 WAAP
3. 버그바운티 플랫폼 : 집단지성을 활용한 보안취약점 대응 -> 버그 + 바운티(포상금) = 기업제품의 보안취약점 제보자에게 포상금을 지급하는 제도 기업이 허용하는 해킹범위 내에서 화이트해커가 해킹을 시도하여 보안취약점을 발견, 제보하면 기업은 제보된 취약점을 평가하고 그에 적합한 수준의 포상금을 지급한다.
4. OT보안 스마트팩토리 시대의 OT 보안 방안
5. 프라이버시 강화 기술

이러한 위협에 대응하기 위해 삼성SDS 보안전문가들이 이날 행사에서 **△비대면 업무환경의 보안 △클라우드 보안 △생산설비 및 제조공정(OT) 보안 △데이터 보안 분야를** 중심으로 대응 사례를 공유하고 해결책을 제시할 예정이다.  
  
이와 함께 한국인터넷진흥원(KISA)의 ‘디지털 르네상스 시대, 사이버 위협 동향’이 소개된다. 또, **엔드포인트 보안**(EDR, Endpoint Detection & Response) 분야 글로벌 리더 센티넬원(SentinelOne)社의 ‘정보 보호를 넘어 위협 탐지 및 대응 중심의 보안패러다임 전환 중요성’, 삼정KPMG의 ‘OT 보안 트렌드와 국내외 적용사례’가 공유될 예정이다.  
  
한편, 삼성SDS의 사내벤처 ‘팀나인’과 ‘해킹존’이 ‘**AI 기반 멀티미디어 위변조 검출 플랫폼’과 ‘집단지성 기반 버그바운티(보안취약점 신고 및 포상제도) 플랫폼’을** 각각 발표하며, 자회사 시큐아이도 차세대 방화벽을 통한 안전한 원격근무 환경구축 방안을 소개한다.

**데이터 보호 방안 찾아야**  
재택근무 환경에서 데이터를 보호하기 위해 DLP도 필수다. 소만사는 엔드포인트 DLP ‘프라이버시아이(Privacy-i)’와 EDR 솔루션 ‘프라이버시아이 EDR’을 하나의 에이전트로 결합시켜 에이전트 관리 복잡성을 제거하면서 재택근무 시 강화되는 엔드포인트 보안 관리 문제를 해결한다.  
  
**DLP란?**  
  
DLP는 Data Loss Prevention의 약자로, 데이터 손실 방지를 의미한다. 데이터의 흐름을 감시하여 기업 내부의 중요 정보에 대한 유출을 감시/차단하는 방식이다.  
  
기밀정보로 분류할 수 있는 정보의 범위는 매우 넓은데, 기업 구성원에 대한 정보와 기업 운영 프로세스, 고객과 직원에 관한 신원확인정보(PII), 영업정보, 재무제표, 마케팅 계획과 같은 전략 정보, 제품 기획과 같은 지적 재산(IP)를 포함한다.

**DRM이란?**  
  
디지털 콘텐츠의 저작권을 보호하는 기술인 DRM(Digital Rights Management)은 저작권자가 배포한 디지털 자료나 하드웨어의 사용을 제한하는 것을 말한다. 특정 자료를 저작권자가 의도한 용도로만 사용하도록 제한하는데 사용되는 모든 기술을 지칠하는 용어기 때문에 복사방지, 기술보호 장치도 그 일부라고 할 수 있다.  
  
DRM이 기업의 솔루션 용어로 사용될 때는 의미가 조금 달라지는데, 디지털 제약 관리(Digital Restrictions Management)에 더 가까운 의미가 된다. 각 문서 단위에 권한을 주고, 사용권한에 따라 접근할 수 있는 범위를 제한한다

 EDR이란?

**클라이언트 자체에서의 보안**을 말하는데, 클라이언트에 설치되어 특정한 행동이나 이상징후가 보이면 바로 탐지 그리고 그것에 대한 대응을 한다. 이러한 특징을 가지는 것에 대표는 백신이라고 할 수 있다. 그러나 백신과 다른 이유는 백신이 시그니처와 패턴 위주로 악성 공격을 탐지한다고 하면, EDR은 **머신러닝과 인공지능**을 활용해 탐지를 한다. 그렇다고 EDR이 패턴과 시그니처 탐지를 안 한다고 한다면 그것 또한 아니다. 클라이언트에 깔려 있는 EDR의 에이전트는 클라이언트의 거의 모든 행동을 관찰하고 분석하며, 그러한 관찰한 내용들을 서버에 있는 DB와 대조를 하고, 일치하는 것이 없으면 머신러닝과 인공지능을 이용해 위협을 대응해 가기 시작한다..

VPN이란?

**가상사설망**(假想私設網) 또는 **VPN**([영어](https://ko.wikipedia.org/wiki/%EC%98%81%EC%96%B4): virtual private network)은 공중 [네트워크](https://ko.wikipedia.org/wiki/%EB%84%A4%ED%8A%B8%EC%9B%8C%ED%81%AC)를 통해 한 회사나 몇몇 단체가 내용을 바깥 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망이다.[[1]](https://ko.wikipedia.org/wiki/%EA%B0%80%EC%83%81%EC%82%AC%EC%84%A4%EB%A7%9D#cite_note-1) 가상 사설망에서 메시지는 [인터넷](https://ko.wikipedia.org/wiki/%EC%9D%B8%ED%84%B0%EB%84%B7)과 같은 공공망 위에서 표준 [프로토콜](https://ko.wikipedia.org/wiki/%ED%86%B5%EC%8B%A0_%ED%94%84%EB%A1%9C%ED%86%A0%EC%BD%9C)을 써서 전달되거나, 가상 사설망 서비스 제공자와 고객이 서비스 수준 계약을 맺은 후 서비스 제공자의 사설망을 통해 전달된다.

**차세대 방화벽이란?**  
기업은 이러한 환경 변화에 대응하기 위해 방화벽 외에도 IPS, 안티 바이러스, 프록시, UTM 등 방화벽을 보완할 수 있는 제품을 추가해왔다. 하지만 이처럼 각 벤더의 제품을 도입한 결과 보안에 대한 중복 투자, 이기종 제품에 대한 관리 및 일관성 없는 정책, 운영 인력 부재 등 추가적인 문제가 발생했다. 특히, 다양한 장비를 거치면서 트래픽이나 패킷에 대한 중복 검사가 이뤄지는 만큼 네트워크 지연시간이 발생하고, 각 장비를 통한 정보를 통합적으로 확인하기 어려워 가시성도 떨어졌다.  
  
차세대 방화벽은 이러한 문제를 해결하기 위한 접근 방식이다. 가트너는 지난 2009년 차세대 방화벽(NGFW: Next Generation FireWall)이라는 개념을 새롭게 제안했다. 차세대 방화벽은 기존의 포트/프로토콜 검사 및 차단을 넘어 응용 프로그램 수준 검사, 침입방지(IPS), 안티 바이러스 등 복합적인 보안 기능과 함께 방화벽 외부에서 위협에 대한 인텔리전스를 가져온다. 이를 통해 알려지지 않은 위협에 대응하고, 클라우드 및 원격근무 등 새로운 환경을 이용한 업무 방식을 보호할 수 있다. 또한, 가트너는 차세대 방화벽의 필수 조건으로 응용 프로그램 단에서 사용자 단위로 콘텐츠를 제어해야 한다고 제시했다. 또한, 포트나 프로토콜 검사 및 차단 기능을 넘어 응용 프로그램 수준 검사, 침입방지 기능과 딥 패킷 검사까지 가능해야 한다고 규정했다.

[재택근무와 보안②] 보안 문제 해결해야 재택근무 성공

코로나19·집단 성착취 영상 거래 사건 위장 공격 유포  
임직원 보안 수칙 정비하고 지속적인 교육·캠페인·모니터링해야  
임직원 가정 내 스마트홈 기기 보안 수칙도 안내해야

재택근무의 긍정적인 면이 많지만, 부정적인 면도 그만큼 많다. 특히 보안위협이 높아진다는 점은 심각한 리스크인데, 코로나19 이슈를 악용한 스피어피싱, 스미싱 등이 급격하게 증가하고 있어 보안 위협은 매우 심각한 상황이다. 회사 공지사항, 관계기관 협조 공문 등으로 위장한 사회공학 기법의 악성메일은 사용자가 아무리 주의를 기울인다 해도 완벽하게 차단할 수 없다.

‘텔레그램 n번방’ 등 사회의 공분을 산 이슈를 이용하는 스피어피싱과 스미싱도 활개를 치고 있어 더욱 주의가 요구된다. 이러한 내용으로 위장한 악성 문자메시지의 URL을 클릭해 악성앱을 설치하면 기기의 중요 정보와 인증정보를 탈취당할 수 있다. 악성앱은 사용자 몰래 녹음·녹화를 해 사생활 정보 뿐 아니라 재택근무 중 일어나는 중요한 정보를 빼낼수도 있다.

**보안 수칙 재정비하고 이직원 교육 해야**

재택근무에 긴급하게 돌입했을 때 가장 취약한 것이 보안 문제다. 재택근무는 사무실 내 업무환경보다 보안에 취약하기 때문에 임직원의 보안 습관을 철저하게 갖고도록 교육하고 모니터링해야 한다.

특히 신뢰할 수 없는 사람이 보낸 메일이나 메시지 열람을 금지하고, 웹사이트 방문을 자제하며, 특히 코로나19 이슈를 담고 있는 메일과 메시지는 각별히 주의하도록 교육한다. 정상 사용자나 정상 기관·기업이 보낸 메일이나 메시지라도 다시 한 번 확인해 사칭한 것은 아닌지 살펴본다. 메일의 첨부파일은 다운로드 받지 말고 미리보기로 확인하며, 메일에서 안내하는 외부 링크 클릭도 자제하는 것이좋다.

모바일 앱 역시 정식 앱스토어 외에서는 다운받지 않도록 주의하며, 앱스토어 등록된 앱이라도 신뢰할 수 있는 기관에서 배포한 것인지, 사용자들의 리뷰를 먼저 확인해보는 것이 좋다.

재택근무 환경이라도 원격접속 지점을 가능한 최소화하는 것이 필요하다. 공격자가 중요 시스템으로 접근할 수 있는 경로를 가능한 차단하고, 원격접속 지점을 실시간 모니터링해 사용할 필요가 없거나 사용하지 않는 경우, 위험성이 높은 경우 우선 차단하는 것이 좋다. 특히 공격자들이 자주 사용하는 RDP 연결은 극히 제한된 경우만 사용한다.

**스마트홈 기기 취약점, 재택근무 위협**

재택근무를 위협하는 보안 문제 중 하나가 스마트홈 디바이스 취약점이다. 가족들이 함께 사용하는 PC를 사용하는 것보다 업무에 사용하던 노트북을 이용하면 더 안전하다고 느낄 수 있다. 그러나 그것으로 충분하지는 않다. 가정용 무선 공유기를 통해 스마트홈 기기에 악성코드가 전파된다면 업무 노트북도 감염될 수 있다.

개인과 업무용 계정을 동일하거나 유사한 것으로 사용할 경우, 공격자는 스마트홈 기기·네트워크 취약점을 이용해 침투한 후 기기와 네트워크에서 평문으로 저장된 계정정보를 탈취한다.

이를 업무 단말과 시스템에 대입해 쉽게 사용자 계정을 탈취할 수 있다. 공격자는 탈취한 계정을 이용해 정상 권한 사용자로 위장하고 협업 플랫폼으로 침투해 다양한 정보를 훔치는 한편 이 플랫폼에 연동된 또 다른 시스템으로 이동할 수 있다.

대부분의 협업 플랫폼은 계정정보 입력만으로 접속 가능하며, 협업 효율성을 높이기 위해 플랫폼 내 데이터는 암호화하지 않는다. 정상계정만 손에 넣으면 공격자는 쉽게 중요 데이터와 시스템에 접근할 수 있는데, 계정정보를 탈취하는 것도 어려운 일은 아니다.

따라서 회사 내 계정정보 뿐 아니라 스마트홈 기기의 계정 보안, 악성코드 감염 방지 등의 대책 마련이 반드시 필요하다.

**데이터 보호 방안 찾아야**

재택근무 환경에서 데이터를 보호하기 위해 DLP도 필수다. 소만사는 엔드포인트 DLP ‘프라이버시아이(Privacy-i)’와 EDR 솔루션 ‘프라이버시아이 EDR’을 하나의 에이전트로 결합시켜 에이전트 관리 복잡성을 제거하면서 재택근무 시 강화되는 엔드포인트 보안 관리 문제를 해결한다.

소만사의 유해·악성코드 배포 사이트 DB를 이용해 이메일·메신저 등을 통해 유입되는 악성 URL을 차단하며, 악성코드가 PC에 침투하면 EDR 엔진으로 차단하는 프로세스를 가진다. 소만사는 데이터 중요도에 따라 보호 수준을 달리 해 업무 생산성을 극대화하며, 마이터 어택(MITRE ATT&CK) 프레임워크를 적용해 고도화된 엔드포인트 보호를 제공한다.

김대환 소만사 대표는 “재택근무라는 분산된 엔드포인트 환경에서 백신, 샌드박스 등 포인트 솔루션만으로 다양한 엔드포인트 위협을 차단하지 못한다. DLP를 통한 데이터 유출 방지와 데이터 파괴·변조·무단 암호화 방지, 유해사이트 차단을 통한 악성코드 감염 방지와 함께 EDR의 제로데이 공격 방어 기능을 통해 보다 안전한 엔드포인트 환경을 만들 수 있다”며 “신속하고 자동화된 대응 능력을 가진 통합 엔드포인트 보호 솔루션으로 보안 위협이 높은 재택근무 환경까지 보호할 수 있다”고 설명했다.

**문서중앙화로 데이터 보호**

재택근무의 편리함을 보장하면서 데이터를 보호하는 방법 중 하나로 문서중앙화가 꼽힌다. 업무 데이터는 무조건 중앙 서버에 저장하도록 해 사용자 PC에 숨어있는 악성코드를 통한 데이터 유출을 방지하고 재택근무 시에도 체계적인 문서관리를 지원할 수 있다.

지란지교시큐리티, 사이버다임, 넷아이디, 소프트캠프 등 문서중앙화 솔루션 기업들이 이 점을 강조하며 자사 제품이 재택근무에 필수라고 주장한다. 사이버다임은 엔터프라이즈용 ‘데스티니 ECM’과 SMB를 위한 클라우드 기반 문서중앙화 ‘클라우디움’의 도입 컨설팅을 무료로 제공하며, 넷아이디 역시 ‘클라우독’과 클라우드 서비스 ‘엠클라우독’ 무상 컨설팅을 통해 고객 접근성을 높이고 있다.

지란지교시큐리티는 ‘다큐원 클라우드’를 중소기업에게 3개월 무상 지원하는 이벤트를 제공한다. 이 솔루션은 원활한 협업을 지원하기 위해 전사, 부서, 팀, 개인별 공유폴더를 제공하며, 개인정보보호법 등 각종 컴플라이언스 요구를 만족시킬 수 있다. 고객 담당자의 의견을 반영해 사용 편의성과 업무효율성을 높이고 있으며, 본문 추출 엔진으로 빠르게 데이터를 검색할 수 있게 한다. 문서 무해화(CDR) 기술을 적용해 저장된 문서에 숨은 악성코드까지 깨끗하게 제거한다.

**샌드박스(보안)란?**

컴퓨터에서 어떠한 프로그램/코드를 실행할 때 격리된 공간(샌드박스)를 제공하고 그곳이 아닌 다른 곳으로 벗어나 허용되지 않은 작업을 하지 못하도록 방지하는 기술.  
  
예를 들면, [웹 브라우저](https://namu.wiki/w/%EC%9B%B9%20%EB%B8%8C%EB%9D%BC%EC%9A%B0%EC%A0%80) 상에서 실행되는 [JavaScript](https://namu.wiki/w/JavaScript) 코드는 웹 브라우저가 허용하는 범위 안에서만 작동하며 브라우저 바깥의 컴퓨터 환경에 영향을 줄 수 없다. 플래시 파일들도 마찬가지 예이다.

**클라우드 WAAP 보안이란?**

클라우드 확산과 함께 API 보안 문제가 드러나면서 웹 보안 플랫폼에 API 보호 기능을 통합시킨 WAAP(Web Application and API Protection) 플랫폼 사용이 급증하고 있다. 가트너는 WAAP의 주요 기능으로 웹방화벽(WAF), 디도스 방어, 봇 관리, API 보호 등을 들었으며, 주로 클라우드를 통해 서비스된다고 설명했다. 웹방화벽 벤더들이 WAAP를 가상·물리 어플라이언스로 공급하는 추세에 있었지만, 점차 클라우드 기반 서비스에 중점을 두고 있다. 대규모 서비스 사업자의 경우 어플라이언스와 클라우드 서비스를 혼합한 방식을 선호한다.

| **OT 보안을 위한 넓고 얕은 지식** |
| --- |
| **■ 왜 에단 헌트는 해킹에 목숨을 걸어야 하는 걸까?**    영화 ‘미션 임파서블’에는 기밀 정보를 빼돌리기 위해 온갖 고생을 하는 주인공 ‘에단 헌트’의 모습이 잘 묘사되어 있다. 변장은 기본이고, 수심 60m의 급류 속에서 3분간 숨을 참는다. 공중에 매달려 침투하다 떨어진 땀 한 방울로 인해 발각될 위기에 처하기도 한다. 무사히 잘 끝나면 참 다행인데 문제는 이러한 시도가 포착될 위험이 높고 또 이 과정에서 누군가를 죽여야 하는 경우도 생기다 보니 안타깝게도 우리 편(?)의 희생을 치러야 하는 일 역시 종종 발생하게 된다는 것이다.    일반적으로 ‘해킹’ 또는 ‘사이버 공격’을 이야기할 때 이런 일들이 생명의 위협을 느끼는 위험천만한 일이라고는 생각하지 않는다. 왜냐하면 우리에게 익숙한 해커의 이미지는 어두운 공간에서 후드를 쓰고 컴퓨터 앞에 앉아 빠르게 타자를 치고 있는 모습에 가깝기 때문이다. 그런데 왜 영화나 드라마 속 주인공들은 언제나 위와 같이 어렵고 험난한 방법을 써가며 직접 침입을 시도하는 걸까? 보다 극적인 전개를 위한 허구나 과장인 걸까?    그 이유는 산업제어시스템(ICS: Industrial Control System)이 기본적으로 외부의 IT망과 분리된, 다시 말해 폐쇄망으로 구성되어 있다는 데 있다. 이러한 시설들은 보유하고 있는 정보의 중요도가 높을수록, 사회 전반에 미치는 영향력이 클수록 더욱 삼엄한 보안을 유지하게 된다. 그렇다면 조금 더 안전하게, 직접 가지 않고 해당 시설의 정보를 뺏거나 해킹하는 것은 정말 불가능한 일인 걸까? 산업제어시스템(ICS)의 환경, 더 나아가 OT(Operational Technology, 운영 기술)에 대해 살펴보며 그 가능성에 대해 논의하는 시간을 가져보고자 한다.    **■**​**OT란 무엇인가?**    최근 보안 트렌드를 살펴보면, 정보 기술을 의미하는 IT(Information Technology)와 비교되는 말로 운영 기술의 OT(Operational Technology)라는 용어가 등장한다. 기존 산업제어시스템으로 알려졌던 환경이 보다 넓은 영역인 OT로 확장돼 쓰이고 있는 추세다.    http://www.igloosec.co.kr/files/2020/07/01/20200701132354c6ff1857-0d76-40d7-9243-d9e2cb4c01e0.png  <이미지1. OT, ICS, SCADA 구성 / 출처: 가트너(Gartner), 이글루시큐리티 재구성>    가트너(Gartner)에 따르면 OT(Operational Technology)란 기업의 물리적 장치, 프로세스 및 이벤트를 직접 모니터링/제어하여 변경을 감지하거나 변경하는 하드웨어 및 소프트웨어로, 스마트 시티(Smart City), 스마트 팩토리(Smart Factory), 사회기반시설 등 다양한 환경에서 운영되고 있는 시스템을 말한다. 우리에게 익숙한 기존의 IT 환경과는 또 다른 환경으로, 운영 환경, 네트워크, 프로토콜, 인력, 제어 방법, 보안 등 거의 모든 부분에서 IT와는 사뭇 다른 모습을 보인다.    IT 전문가가 처음 OT를 접할 때 느끼는 가장 큰 차이는 바로 사용하는 언어다. 세종대왕이 나라말이 중국과 달라 서로 통하지 않아 훈민정음을 창제했다 하셨던 것처럼, IT와 OT는 매우 다른 언어를 사용한다. 모 산업 시설에서 OT 보안 컨설팅을 수행한 컨설턴트는 해당 프로젝트에서 가장 어려웠던 점으로 ‘IT와 OT 언어의 다름’을 꼽았다. 그간 IT 영역에서 오랜 기간 컨설팅을 수행하며 나름 자부심도 있는 베테랑 컨설턴트였는데, OT 영역에서 처음 실무자와 인터뷰를 하며 느꼈던 ‘언어의 다름’에 도저히 진도가 나가지 않아 언어를 습득하는데 꽤나 많은 시간과 노력을 들였다고 한다.    보안을 바라보는 관점에서도 IT와 OT 간의 큰 차이를 느낄 수 있다. 보안의 우선순위 관점에서 보았을 때 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 중 IT는 기밀성을, OT는 가용성을 가장 중요하게 여긴다. 이 차이는 두 영역의 업무 차이에서 비롯되기도 하지만 앞에서 이야기했듯 OT는 폐쇄망 환경, 즉 외부와 연결되어 있지 않은 환경에서 운영됨에 기인하는 바도 크다. 지금까지의 OT 환경은 ‘폐쇄성’을 담보로 안전한 보안을 보장받아 온 것이다. 그러나 시대가 변화함에 따라 이러한 OT의 폐쇄성 역시 시험대에 오르게 됐다. 4차 산업혁명과 더불어 IoT, 빅데이터 등 여러 신기술이 등장하면서 폐쇄망이었던 OT 망이 IT 망과 연결돼 운영되기 시작한 것이다.    http://www.igloosec.co.kr/files/2020/07/01/20200701132410dd0e468b-8bb8-49d6-9f35-ba9f58893539.png    <이미지2. IT와 OT 보안의 차이 / 출처: GE코리아, 이글루시큐리티 재구성>    **■**​**OT 환경에서의 보안 이슈**    보안에 관심 있는 사람이라면 ‘스턱스넷(Stuxnet)’이라는 단어를 기억하고 있을 것이다. 2010년 6월 발견된 스턱스넷은 산업제어시스템으로 유명한 독일 지멘스사의 산업용 소프트웨어를 선택적으로 공격해 해당 소프트웨어를 사용하는 산업시설에 침투, 오작동을 유발하는 악성코드였다. 이로 인해 이란의 핵 개발 시설이 큰 피해를 입었고 비단 이란뿐 아니라 중국을 비롯한 여타 많은 국가에도 빠르게 확산돼 다양한 산업시설들을 감염시켰다.    스턱스넷은 산업제어시스템을 겨냥하여 제작된 악성코드다. 해커의 자기 과시 또는 금전적인 이유로 제작된 기존의 악성코드와는 다르게 국가의 주요 산업시설 파괴를 목표로 한다. 그로 인해 당시 많은 보안 전문가들이 스턱스넷을 보안 위협의 패러다임을 바꾸는 악성코드라 평가하기도 했지만, 사실 스턱스넷 공격 그 자체보다 주목해야 할 것은 이렇듯 이미 오래 전부터, 긴 시간에 걸쳐 수많은 OT, 산업제어시스템들이 공격을 받아 오고 있다는 점이다. 이는 영화 ‘다이하드 4.0’에 잘 묘사된 ‘파이어 세일(Fire Sale)’이 더 이상 영화 속 허구가 아님을 잘 말해준다.    분명 앞에서 OT 환경은 폐쇄망으로 구성됐다고 했는데 어떻게 악성코드에 감염되고 시설에 대한 공격이 이뤄지게 된 것일까? 이를 알아보기 위해서는 OT 환경의 구조를 알아야 한다. OT 환경을 표현하기 위해서는 일반적으로 ‘퍼듀모델(Purdue Model)’을 사용하는데 이는 다음과 같다.  http://www.igloosec.co.kr/files/2020/07/01/202007011327013c8956ae-6ccf-44cd-a63d-a9de080dac3a.png  <이미지4. 퍼듀모델을 통한 OT 환경 표현 / 출처: CISCO, 이글루시큐리티 재구성>    기존에 우리가 ‘폐쇄망’이라고 부르던 OT 네트워크는 퍼듀모델 상의 Safety Zone부터 Industrial Zone까지, Level 0에서부터 Level 3까지를 가리킨다. 분명 이 영역은 외부와 단절되어 있고 IT와 다른 OT만의 별도 프로토콜(ABB, GE SRTP, Siemens S7 등)로 이루어져 있기 때문에 기본적으로는 외부로부터의 위협에서 안전하다고 여겨진다.    그런데 함정은 OT 환경이 이렇듯 폐쇄망으로만 구성될 수는 없다는 것이다. 운영 관리를 위해 Enterprise Zone, 즉 IT 망인 Level 4~Level 5의 영역이 존재하며 직원에 의한 운영, 유지관리를 위한 외부에서의 원격접속 등 다양한 이유로 IT 망과 OT 망의 접점인 ‘Industrial DMZ’, 속칭 ‘Level 3.5’가 존재할 수밖에 없다. 이 영역을 통해 IT와 OT가 연결되며 IT 영역에서 발생하는 수많은 위협이 결국 OT 환경에까지 영향을 주게 된다. OT보안 솔루션 전문업체 클래로티(Claroty)에 따르면 얼마나 많은 외부로부터의 접속이 내부의 폐쇄망으로 이루어지는지는 보안 담당자나 OT 담당자, 그 누구도 모른다고 한다.    결국 OT 환경은 우리가 알고 있던 것처럼 폐쇄망으로 이루어져 외부의 공격이 절대로 닿을 수 없는 것이 아닌, 오히려 이미 ‘외부의 공격에 노출된 환경’이라는 의미다. OT 환경에 접속하여 정보를 빼내거나 해킹 하기 위해 힘들게 변장하고, 공중에 매달리고, 물속에서 숨을 참고, 고층 건물을 기어올라가지 않아도 내부에서 PC를 통해 손쉽게 접속할 수 있는 방법도, 물론 쉽지는 않겠지만 존재한다는 말이다. 할 수만 있다면 이 사실을 얼른 ‘에단 헌트’에게 알려주고 싶은 마음이다.    **■**​**OT 보안, 어떻게 해야 할까?**    IT 환경과 OT 환경의 결합은 기존 IT 환경에서 발생 가능한 보안 위협을 OT 환경에까지 전이시키는 문제를 가져왔고, 이는 곧 실제 공격에 의한 피해로 이어지게 되었다. OT 환경에 대한 보안 위협은, 단순 정보 유출 등의 이슈에 그치지 않고 사회기반시설의 중단으로 야기되는 금전적 피해, 직간접적인 인명 피해, 더 나아가 대규모의 사회혼란까지 일으킬 수 있기에 그 심각도가 보다 높다. 따라서 가용성을 기밀성과 무결성보다 우선적으로 여겼던 OT 환경에서도 ‘보안’이 최우선적으로 고려해야 하는 중요한 요소로 떠오르게 된 것은, 어쩌면 너무나 당연한 일이다.    폐쇄망이기에 물리적인 보안만으로도 충분하다고 여겨졌던 OT 환경에 대한 보안 대책은 이제 IT 환경과의 결합을 고려해 새로이 수립되어야 한다. 이를 위해 수많은 컨설팅 및 보안 전문가들이 저마다의 경험과 판단을 토대로 OT 보안에 대한 정의, 고려 사항, 대응 방안 등을 내놓았고, 각각 상이한 내용을 정리해보면 다음과 같다.    http://www.igloosec.co.kr/files/2020/07/01/2020070113271474c6e124-8d39-4793-8345-f56d111c8fd0.png  <이미지5. OT 보안을 위한 요소 / 출처: 이글루시큐리티>    **1) 보안 관리체계 수립**    OT 보안을 위한 관리체계 수립 시 정책, 조직, 기술, 프로세스에 대한 내용이 모두 포함되어야 하지만, 무엇보다 중요한 건 경영진의 의지를 통한 예산 및 자원의 확보가 반드시 선행되어야 한다는 것이다.  일반적으로 OT 환경에서 기존의 ‘정보보호’조직은 IT 보안에 국한된 R&R을 부여받아 업무를 수행하고 OT 운영 담당자들은 보안에 대한 별도의 R&R이 부여되지 않는 경우가 대부분이다. 따라서 이 두 영역을 조율하여 융합된 보안 관리체계를 수립하기 위해서는 경영진의 적극적인 개입이 필요하다.    또 보안 관리체계를 수립하기 위해서는 관리체계의 표준이 필요한데, 최근 OT 환경에 대한 보안 위협이 크게 증가함에 따라 관련된 보안 규정의 제정도 활발하게 추진되고 있다. 대표적인 글로벌 표준으로는 ISA/IEC 62443, NIST 800-82 등이 있으며 국내에서도 한국인터넷진흥원(KISA)이 ‘스마트공장 사이버보안 가이드’를 발표하고 스마트 공장에서 발생할 수 있는 보안 위협과 접근통제, 데이터 보호, 정보보안 운영정책 및 절차, 자산관리 보안 사고 예방 및 대응 등의 보안 요구 사항을 명시하고 있다. 이렇듯 다양한 표준들을 바탕으로 보안 관리체계를 수립하는 추세라 할 수 있겠다.    더불어 금년 초 개최된 세계 최대 사이버 보안 컨퍼런스 RSA 2020에서는 OT 보안이 주요 이슈 중 하나로 다뤄졌다. OT 환경에 대한 보안체계 수립 시 NIST CSF(NIST Cyber Security Framework)를 IT 및 OT의 공통적인 언어로 사용하자는 논의가 있었다. 보안 운영 측면에서 IT와 OT는 융합될 것으로 예상되기 때문에 NIST CSF를 통해 IT뿐만 아니라 OT 보안 상태의 갭(Gap)을 식별하고, 리스크(Risk) 기반으로 우선순위를 도출하여 갭(Gap)을 줄이기 위한 전략적 로드맵을 수립하자는 것이다. 현시점에서는 OT 환경에 딱 맞는 표준뿐 아니라 IT 환경과의 융합을 고려한 관리체계의 수립이 무엇보다 중요하다는 사실을 시사해 준다.    http://www.igloosec.co.kr/files/2020/07/01/202007011327254d2695f7-edd7-4f95-8036-1585cb697e4b.png  <이미지6. Top10 List for Securing Your OT Environment / 출처: Rockwell Automation, 이글루시큐리티 재구성>      **2) 가시성(Security Visibility) 확보**    보이지 않는 대상을 보호할 수는 없다. IT 보안에서 ‘보호해야 하는 IT 자산에 대한 식별’이 중요하고도 필수적인 요소로 손꼽히듯이 OT 보안도 마찬가지다. 그러나 OT 영역에서의 가시성 확보는 대체로 IT 영역보다 어려운 경향을 보이는데 그 이유는 각기 다른 인력들이 담당하는 다양한 장비가 여러 사업장에 흩어져 있는 경우가 많기 때문이다. 이에 어떤 장비가 어디에 있는지를 모두 완벽하게 파악하고 있는 사람을 찾기는 더더욱 힘들다. 클래로티(Claroty), 사이버엑스(CyberX), 스카다가디언(SCADA guardian) 등 OT 보안 솔루션들이 OT 환경에서 BMT(Bench Marking Test, 성능 테스트) 또는 POC(Proof of Concept, 기술 검증)를 하게 될 때 가장 먼저 하는 일이 대상 장비를 시각화하여 찾아내는 것, 바로 가시성 확보라고 한다. 이 과정에서 각각의 담당자들조차 모르고 있던 장비를 찾아내곤 하는데 이러한 장비들은 보안의 구멍 역할을 할 가능성이 높다.    보호해야 할 장비를 모두 식별해냈다면 다음에는 각 장비들이 어디와 연결되어 있는지, 담당자는 누구인지, 어떠한 용도인지, 어떠한 프로토콜로 통신을 하고 있는지 등 해당 장비에 대한 정보를 파악해야 한다. 이렇듯 대상 장비들에 대한 가시성 확보가 이루어져야 어떻게 보안 아키텍처를 수립할 것인지에 대한 밑그림이 그려지게 된다.    http://www.igloosec.co.kr/files/2020/07/01/2020070113281080eb5f46-f79c-451c-a895-6f70e53da7e8.png  <이미지7. OT 보안 솔루션을 통한 가시성 확보 / 출처: 클래로티(Claroty)>    **3) 보안 아키텍처 수립**    GE의 라지브 나일(Rajiv Niles)은 ‘OT 시스템의 경우 악성코드 감염 등 장애 감지에 필요한 시간이 평균 272일로 알려져 있으나 보안을 갖춘 IT 시스템의 경우 24시간 이내’라고 말하며 OT 보안의 현주소를 지적한 바 있다. OT 환경에는 보안 위협을 탐지할 수 있는 설비나 도구가 충분하지 않아 대응은 물론이고 발생한 위험을 알아차리는 것조차 어렵다는 것이다,    다행히 오늘날의 OT 보안은 이전보다 체계화되고 프로세스화되는 모습을 보이고 있다. 일반적으로 OT의 보안 아키텍처는 앞에서 언급한 ‘퍼듀모델(Purdue Model)’을 기반으로 수립되는데, 퍼듀모델에서는 보안을 위해 ‘심층방어(Defense-in-Depth)’ 아키텍처를 제공하고 이를 기반으로 계층화된 보안 제어 및 구현 방안을 제시해 준다.    퍼듀모델을 바탕으로 IT와 OT가 융합된 환경에서의 보안 위협을 모니터링하고 대응하기 위해서는 IT 영역에서의 레거시 보안 솔루션(Firewall, IDS/IPS, Endpoint Protection 등)을 통한 보안체계 수립과 동시에 OT 영역의 고유한 네트워크 프로토콜을 기반으로 하는 별도의 보안 솔루션이 활용되어야 한다. TCP/IP로 대표되는 IT 프로토콜과 달리 OT 환경에서는 각 설비 업체의 고유한 프로토콜을 통해 통신하기 때문에 통칭 ‘OT 보안 솔루션’을 활용해야 하며, 이러한 OT 보안 솔루션들이 공통적으로 내세우는 특장점으로는 OT 프로토콜의 호환성을 비롯해 가시성 확보, 리스크 관리, 위협 분석 등이 있다.  http://www.igloosec.co.kr/files/2020/07/01/202007011328195224055c-d2e9-4517-80d1-cc0d56eb6d03.png  <이미지8. ICS/OT Security Reference Architecture / 출처: Gartner(August 2017) 일부 재가공>    IT와 OT, 두 영역 모두에 최적화된 보안 아키텍처를 수립했다면 이를 융합하여 통합 보안을 할 수 있는 ‘통합 SOC(Security Operation Center, 보안관제센터)’와 ‘SIEM(Security information and event management, 통합보안관제솔루션)’이 필요하다. IT와 OT를 아우르는 ‘통합 SOC’를 통해 식별-예방-탐지-대응-복구를 위한 일련의 보안 프로세스를 수립 및 운용해야 한다. 그리고 이를 위해서는 IT 영역과 OT 영역의 수많은 보안 솔루션에서 수집되는 정보를 통합적으로 모니터링을 할 수 있는 ‘SIEM’ 역시 필수불가결하다. 이미 IT 보안에서는 빅데이터 기반의 SIEM을 넘어 AI가 접목된 SIEM의 구축 및 운영이 이루어지고 있고, 이는 OT 보안 솔루션과의 연계를 통한 융합 관제 솔루션으로서 활용이 가능하다.    **■**​**OT 보안에 대한 이해, 어렵지 않아요.**    지금까지 OT 보안에 대해 살펴보았다. 정보보안업계에서 일을 하던 사람이라면 왠지 모를 기시감(旣視感, Deja vu)을 느꼈을 수도 있는데 OT 보안을 위해 고려하고 해야 하는 일들이 바로 초창기 IT 보안이 태동할 시기, 가장 중요하다고 강조되었던 것과 일맥상통하기 때문이다. 보호해야 할 자산을 식별하고, 경영진의 의지를 앞세우고, 조직 및 R&R을 명확히 하고, 정보보호관리체계를 수립해 관리하고, 적절한 보안 아키텍처를 구축하고 운영하는 것은 비단 IT뿐만 아니라 OT 보안을 관통하는 공통 요소다. 그동안 폐쇄망이라는 무적의 방패 뒤에 가려져 있던 OT 환경이 IT 환경과의 융합으로 여러 보안 위협에 노출되기 시작했고, 그로 인해 다소 늦게 보안에 대한 필요성이 제기된 것일 뿐이다.    IT 환경에 최적화된 여러 보안 요소들에 OT만의 고유한 특성을 반영한다면, 생각보다 어렵지 않게 OT 보안을 구현해낼 수 있다. 물론 세세한 차이점 하나하나가 실무 단계에서는 큰 어려움으로 다가올 수 있지만 우리는 언제나 그렇듯 해답을 찾아낼 것이다. 빠르게 변해가는 환경 속에 IT와 OT가 구분되지 않는, 완벽하게 융합된 보안 생태계를 구축해내는 시점은 머지않을 것으로 기대된다. 그러니 아쉽게도 ‘에단 헌트’가 사무실에 앉아 커피를 마시며 정보를 빼내는 일은, 또 다른 이유로 쉽지 않을 듯하다.  **[시장동향] 현실화되는 동형암호, 관건은 ‘성능’**   * *기자명* 권정수 기자   **상용화 앞두고 기술 연구에 박차, 데이터 처리 성능 향상에 초점**  차세대 암호기술로 각광받고 있는 동형암호 기술이 무르익고 있다. 상용화를 가로막고 있던 ‘성능’ 문제가 해결될 기미를 보이면서 실제 활용할 수 있는 방안에 대한 논의가 활발해지고 있다.  특히 동형암호 기술 분야에서는 우리나라가 세계 선두 그룹에 속해 있다. 지난해 미국에서 진행된 개인정보보호기술 경진대회 ‘iDASH’의 동형암호 부문에서 1위에 선정된 4개 팀 중 3개가 우리나라 팀이었다. 이외에도 동형암호 표준화를 위한 컨소시엄에 삼성SDS, 서울대가 MS, IBM, MIT 등 글로벌 기업 및 학교와 함께 참여해 기술 발전을 주도하고 있다.  현실로 다가온 ‘동형암호’  세계적으로 차세대 암호기술인 ‘동형암호’에 대한 연구가 활발히 진행되고 있다. **동형암호 기술은 암호화된 데이터를 연산할 수 있도록 지원하는 암호기술을 뜻한다**. 동형암호 기술은 1970년대 수학자들이 처음 구상한 이후, 2009년 스탠포드 대학과 IBM의 과학자 크레이그 젠트리(Craig Gentry)에 의해 개발됐다. 크레이그 젠트리는 개발 당시, 이 기술을 “독성 화학 물질을 취급하는 데 사용되는 장갑이 들어 있는 상자와 같다”고 비유하며 “모든 조작이 상자 안에서 이뤄지므로 화학 물질은 외부 세계에 절대 노출되지 않는다”고 설명했다.  동형암호 기술 개념(출처: 삼성SDS)동형암호 기술 개념(출처: 삼성SDS)  마이클 오스본(Michael Osborne) IBM 리서치 유럽 시큐리티 부문 매니저는 “완전 동형 암호화 기술은 기존 암호화와는 다르게 암호화된 데이터(암호문)에 대해 직접 계산을 수행할 수 있도록 설계된 수학적 알고리즘을 기반으로 한다”고 기술에 대해 소개했다. 그는 또한 “이 새로운 암호화 모델을 사용하면 원본 데이터를 일반 텍스트로 ‘볼’ 필요 없이 제3자가 클라우드에서 암호화된 데이터를 처리 및 분석해 나온 정확한 결과를 데이터 소유자에게 반환할 수 있다”고 강조했다.  이러한 기술 특성의 대표적인 예로 마이크로소프트에서 제공하고 있는 동형암호 기술 기반 비밀번호 유출 조회 서비스를 들 수 있다. 최근 MS는 에지(Edge) 브라우저 사용자를 대상으로 비밀번호 점검 서비스를 제공하고 있다. 이 서비스는 준동형암호 기술을 활용, 서비스를 제공하는 MS에서도 사용자의 비밀번호는 물론 비밀번호 유출 여부(연산 값)도 확인할 수 없다. 사용자만 데이터를 확인할 수 있는 것이다.  이러한 점 때문에 동형암호 기술은 개인정보보호는 물론, 데이터 활용에 있어서 획기적인 기술로 평가받고 있다. 개인정보보호의 경우 암호화된 개인정보를 제공함으로써 기업은 개인정보를 확인할 수 없지만, 사용자는 개인화된 서비스를 받을 수 있다. 더불어 기업의 관점에서 다른 기업 및 기관과 데이터를 결합하는 경우에도 데이터 유출에 대한 우려를 없앨 수 있다.  동형암호 기술은 ▲스토리지 아웃소싱 ▲헬스케어 ▲DNA 분석 ▲스마트 시티 등 가상 물리 시스템 ▲기계학습 ▲양자내성암호 ▲금융 협업 등에 활용될 수 있을 것으로 기대된다.  스토리지 아웃소싱의 경우 동형암호를 활용해 클라우드에 데이터를 안전하게 저장할 수 있으며, 데이터 연산 및 검색도 가능해진다. 헬스케어 분야는 환자의 건강정보 등 민감정보를 다루고 있기 때문에 정보규제가 엄격한 분야 중 하나다. 동형암호를 활용하면 민감정보를 보호하면서도 연산처리가 가능해진다. DNA분석도 마찬가지다. 개인의 유전정보를 이용하는 맞춤형 정밀 치료기술이 개발되고 있는데, 이를 위해 활용하는 DNA정보는 민감정보이기 때문에 필연적으로 프라이버시 이슈가 뒤따른다. 동형암호를 적용해 DNA 정보 유출을 방지하면서 데이터 연산이 가능해진다.  머신러닝 분야에서도 동형암호가 각광받고 있다. 개인정보보호가 적용된 환경에서는 머신러닝이 얻는 데이터의 정확성이 문제되는 경우가 있다. 비식별 처리된 데이터는 개인정보의 결합도가 낮아, 데이터 가치가 떨어지기 때문이다. 이러한 단점을 극복하기 위한 방법으로 순수 데이터를 그대로 암호화하고, 암호화된 데이터를 개인정보 유출없이 머신러닝에 활용하는 방안이 대두되고 있다.  금융 분야에서도 동형암호에 대한 관심이 높다. 이상거래 탐지나 개인신용평가, 개인 맞춤형 서비스 등에 동형암호를 적용하면 데이터 기밀성은 보장되면서 다자간 협업 환경을 구현할 수 있다. 알리바바의 자회사 앤트 파이낸셜(ANT Financial)은 신용분석 및 마케팅 분석, 은행데이터 결합분석에 동형암호 기술 적용을 추진중이다.  양자내성암호로의 활용도 가능하다. 현재 사용되고 있는 공개키 기반 구조의 암호화는 양자컴퓨터가 출현하면 폐기될 것으로 전망된다. 양자컴퓨터가 사용하는 ‘쇼어 알고리즘’으로 해독이 가능해 암호화가 무용지물이 될 수 있다는 것이다. 이에 양자컴퓨터에 대응할 수 있는 기술에 대한 연구도 활발하게 진행되고 있는데, 그중 하나가 바로 동형암호다. 동형암호를 포함한 격자기반암호 알고리즘은 양자컴퓨터가 도입돼도 깨지지 않는 차세대 암호체계로 평가받고 있다. 격자 문제는 ‘현재로서는 풀 수 있음이 증명되지 않은 문제’라는 뜻의 NP 완전 문제로 분류된다.  동형암호 기술은 ▲PHE(Partially Homomorphic Encryption) ▲SHE(Somewhat Homomorphic Encryption) ▲FHE(Fully Homomorphic Encryption) 등 크게 3가지로 구분된다. PHE는 주어진 데이터 세트에 대해 무제한의 시간동안 한 가지 유형의 수학연산만 허용한다. SHE는 PHE에 비해 허용범위가 넓지만 여전히 제한적인 방법이다. 주어진 데이터 집합에 대해 덧셈과 곱셈 등의 연산을 몇 차례만 허용한다. 지금 활발하게 연구되는 것은 FHE다. 동형암호 기술 중 최선의 방법으로 평가받고 있으며, 데이터에 대해 회수 제한 없이 다양한 유형의 연산을 허용하지만, ‘성능’이 문제로 지적된다.  컨소시엄 중심으로 표준화 추진  서울대학교와 삼성SDS 등 국내기업은 이러한 기술력을 바탕으로 동형암호 표준화에도 참여하고 있다. 2009년 IBM에서 동형암호를 제안한 이후, 산업계에서는 표준화 필요성을 인식해 컨소시엄 형태로 표준화를 진행해왔다. 지난해부터는 ISO/IEC 등 공적 표준화기구에서도 표준화를 추진하고 있다. 동형암호 표준화 관련 기구는 ‘Homomorphic Encryption Standardization’과 ITU-T SG17, ISO/IEC JTC 1/SC27이 있다.  먼저 ‘Homomorphic Encryption Standardization’은 동형암호의 보안, API 및 애플리케이션 등 세 가지 백서를 기반으로 동형암호에 대한 표준을 개발하고 있다. 2018년에는 동형암호 첫 번째 표준 버전을 제정했다. 이 표준 버전에는 스킴에 대한 설명, 보안 속성에 대한 설명, 보안 매개 변수에 대한 표 등이 포함됐다. 향후 표준 버전에는 동형암호를 위한 표준 API 및 프로그래밍 모델 등이 마련될 예정이다.  동형암호 기반 AI 예측 모델 개념도(출처: 삼성SDS)동형암호 기반 AI 예측 모델 개념도(출처: 삼성SDS)  기술의 관건은 ‘속도’  동형암호는 ‘데이터 활용’과 ‘보안’, 두 마리 토끼를 모두 잡을 수 있는 기술이다. 하지만 아직까진 완벽한 기술이 아니다. 암호화된 상태로 데이터를 연산해야 한다는 점 때문에 처리 속도에 대한 성능 이슈가 있다.  이런 이유로 동형암호 기술을 연구는 현재 ‘성능’에 초점을 맞춰져 있다. 초기 동형암호 기술은 실제 사용이 불가능할 만큼 성능에 문제가 있었다. 하지만 10여년 동안 기술에 대한 연구 개발이 지속되면서 성능 부분이 상당히 개선돼 활용할 수 있는 단계에 와있다. 암복호화 작업은 기존 RSA 알고리즘 처리속도에 근사한 수준까지 와있으며, 연산처리 과정에서의 속도를 개선하기 위한 연산 가속기 등에 대한 연구가 활발하게 진행되고 있다.  마이클 오스본 IBM 리서치 유럽 시큐리티 부문 매니저는 “IBM의 완전 동형 암호화 기술은 일반 데이터만큼 빠르지는 않지만, 비슷한 성능에 도달했다. 불과 몇 년 전만 하더라도 완전 동형 암호화를 적용하는 데 며칠이 걸렸지만, 현재는 동일한 기준을 적용했을 때 마이크로 초 안에 달성할 수 있다”고 설명했다. 그는 이어 “이제는 동형암호 기술을 통해 해결하려는 문제가 무엇인가에 달려 있다. 예를 들어 동형 암호 기술을 자율주행차에서 GPS 방향을 숨기는 것에 적용할 경우, 마이크로 초 단위도 너무 느리다. 하지만 은행 데이터를 사용해 고객이 단기 대출을 사용할 수 있는지를 결정하는 데는 충분한 성능이다”라고 말했다.  조지훈 삼성SDS 보안연구센터장 또한 “동형암호기술은 무엇보다 암호화된 상태로 데이터를 처리하다 보니 속도가 느리다는 단점이 있는데 이를 극복하기 위한 많은 연구개발이 진행되고 있다”고 말했다. 최근 연산 속도를 높이기 위해 AI 분야에서 널리 사용되고 있는 GPU, FPGA와 같은 하드웨어를 이용한 동형암호 가속 기술이 다양하게 검토되고 있다는 것이 조지훈 센터장의 설명이다.  조지훈 센터장은 미국 국방부에서 진행 중인 프로젝트를 예로 들었다. 미국 방위고등연구계획국(DARPA)는 ‘디프라이브(DPRIVE)’라는 프로젝트를 통해 동형암호향 하드웨어 개발에 많은 비용을 투자하고 있다. 이 프로젝트에는 인텔, MS 등 대기업부터 스타트업과 학계까지 참여하고 있으며, 최종 목표는 2025년까지 암호화 미적용 데이터 처리 속도 대비 10배로 알려져 있다.  또한 인텔에서는 동형암호를 가속화하기 위한 SW 기반의 최적화 툴도 개발, 제공하고 있다. 인텔의 동형암호화 툴킷은 최신 인텔 플랫폼에서 동형암호 기반 클라우드 솔루션의 성능을 향상시킬 수 있도록 설계돼 있다. 동형암호에서 사용되는 격자 암호 커널에 최적화된 ‘인텔 AVX-512(Intel Advanced Vector Extensions 512)’ 가속 지침을 구현한다. 다만 인텔의 동형암호 툴킷은 MS ‘씰(SEAL)’ 및 ‘팰리세이드’ 라이브러리에 최적화된 버전만 제공되고 있다.  인텔에서 예상하는 동형암호 활용 사례(출처: 인텔)인텔에서 예상하는 동형암호 활용 사례(출처: 인텔) 격자 기반 암호 알고리즘 적용  그렇다면 현재 상용화된 암호기술로는 동형암호를 구현할 수 없는 것일까. 업계에서는 제한된 연산을 지원하는 동형암호는 구현이 가능하지만, 사실상 어렵다고 말한다. 공인인증서, HTTPS 등에서 다양하게 활용되고 있는 공개키 기반 암호 기술인 ‘RSA(알고리즘 발명자인 Rivest, Shamir, Adelman 세 사람 이름의 첫 글자) 알고리즘’ 또는 국제 표준으로 지정된 ‘Paillier 알고리즘’ 등에도 곱셈 또는 덧셈 중 하나의 연산만 지원하는 부분 동형암호 알고리즘들이 포함돼 있다. 다만 실제 시스템에 적용돼 사용되고 있는 알고리즘에는 동일 데이터에 대해서도 다양한 암호문을 출력하기 위한 ‘랜덤 패딩 기술’이 적용돼 있어, 동형암호적인 성질을 만족하지 않는다.  현재 연구되고 있는 동형암호 기술은 격자 암호 알고리즘을 기반으로 한다. 격자 암호 알고리즘은 LWE(Learning with Errors) 등의 수학적 난제를 기반으로 설계된다. 격자 암호 알고리즘은 양자내성암호로도 각광받고 있을 만큼 보안성이 높은 기술로 평가받는다. 양자컴퓨터로도 풀어낼 수 없는 난제이기 때문에, 암호화된 데이터를 해독하는 것은 불가능하다는 것이다. 격자 암호 알고리즘에는 NTRU, SS-NTRU, BLISS, New Hope, NTRU 프라임, LWE-Frodo 등이 있다.  격자 암호 알고리즘 종류(출처: KISA)  격자 암호 알고리즘 종류(출처: KISA)  마이클 오스본 IBM 매니저는 “완전 동형 암호화는 격자 수학을 기반으로 한다. 격자 수학은 반복되는 다차원 격자 모양의 점 모음을 이용한다. 격자 기반 체계는 이 격자 내부에 데이터를 숨기는데, 한 지점에서 일정 거리 떨어뜨려 놓는다. 암호화된 메시지가 격자 지점에서 얼마나 멀리 떨어져 있는지 알아내는 것은 양자컴퓨터나 기존 컴퓨터 모두에서 매우 어려운 것으로 평가받고 있다. 그러나 비밀 키를 알고 있으면 메시지를 쉽게 얻을 수 있다”고 설명했다.  조지훈 삼성SDS 센터장 또한 “동형암호 기술의 경우 LWE 문제라고 불리는 수학적 난제에 기반해 데이터를 보호한다. 즉 LWE 문제가 어렵다면 동형암호 기술이 데이터를 보호할 수 있다는 의미”라면서, “기존 암호 기술은 데이터를 보호하기 위해 랜덤 패딩 기술을 활용하고 있으며, 동형암호에서도 기존 암호화 기술과 유사하게 암호화할 때 작은 임의의 값을 더하는 방식으로 암호 기술의 조건을 만족하고 있다”고 말했다.  현재 국내에서 동형암호 기술을 활용한 ‘K-통계시스템 구축 사업’을 수행하고 있는 마크애니의 김동호 부장은 “동형암호도 기존의 암호기술과 방식은 비슷하다. 하지만 동형암호적인 성질을 위해서는 암호문이 연산 후에도 그 구조를 유지해야 하는 것이 차이점”이라면서, “즉 암호화 기술 안전성에 기반이 되는 어려운 수학적 문제가 이러한 동형적 성질을 가져야 한다. 대표적으로 격자 암호 알고리즘은 이러한 성질을 만족한다. 그래서 현재 많은 동형암호들은 격자구조에서의 수학적 난제(LWE 종류)를 기반으로 설계되고 있다”고 설명했다.  국내에서도 동형암호 활용 방안 연구  국내에서도 동형암호를 활용하기 위한 연구가 활발하게 진행되고 있다. 지난 6월에는 마크애니가 동형암호 기술 활용한 ‘K-통계시스템 구축 사업’을 수주하고, 시스템 개발에 착수했다. 이 사업은 3년 간 총 55억 원이 투입되며, 주관기관인 마크애니를 비롯해 시큐센과 고려대학교가 참여한다. 마크애니는 동형암호 기반 통계분석시스템 설계와 개발을 담당한다.  동형암호를 활용한 국가통계분석시스템 개발 목표(출처: 마크애니)동형암호를 활용한 국가통계분석시스템 개발 목표(출처: 마크애니)  조지훈 센터장은 “데이터를 안전하게 활용하고 공유하려면 동형암호 외에도 PETs기술들이 필요하다. 삼성SDS는 ▲차등정보보호 ▲재현데이터 ▲동형암호 및 다자간계산 등 세 가지 관점에 맞춰 연구 개발을 진행하고 있다”고 말했다.  삼성SDS 개인정보보호 및 활용 기술 전략(출처: 삼성SDS)삼성SDS 개인정보보호 및 활용 기술 전략(출처: 삼성SDS)  그의 설명에 따르면, 첫 번째 데이터의 조회 및 분석 결과를 외부에 전송할 때 프라이버시의 노출 정도를 정확하게 측정할 필요가 있다. 프라이버시 측정 툴(Privacy Measurement Tool)로 주목 받고 있는 차세대 기술이 ‘차등정보보호기술(Differential Privacy)’이다. 차등정보보호기술은 구글이나 애플에서 사용하고 있으며, 올해부터 미국 인구조사(US Census)에서도 활용되고 있다.  두 번째, 데이터분석가들은 데이터 기반으로 전처리나 다양한 분석을 시도한다. 이러한 모든 기능이 동형암호로 제공되기는 어렵다. 이때 원본데이터와 유사한 통계적, 확률적 특징을 가지는 모조데이터를 AI기반으로 생성해 공유가 가능하다. 이렇게 생성된 데이터를 ‘재현데이터(Synthetic Data)’라고 하며, 현재 사용되고 있는 다양한 비식별화 기법(총계처리, 라운딩기법 등)보다 높은 개인정보보호와 데이터분석 정확도 분석 측면의 활용성을 제공할 수 있을 것으로 예상된다.  마지막으로 동형암호와 같이 데이터를 안전하게 결합, 분석할 수 있는 기술이 필요하다. 동형암호 단독으로는 많은 데이터 분석 활용 사례를 충족할 수 없기 때문에 다자간 계산, 혹은 연합학습 등 다양한 기술이 조합돼 사용이 돼야 한다는 설명이다. |