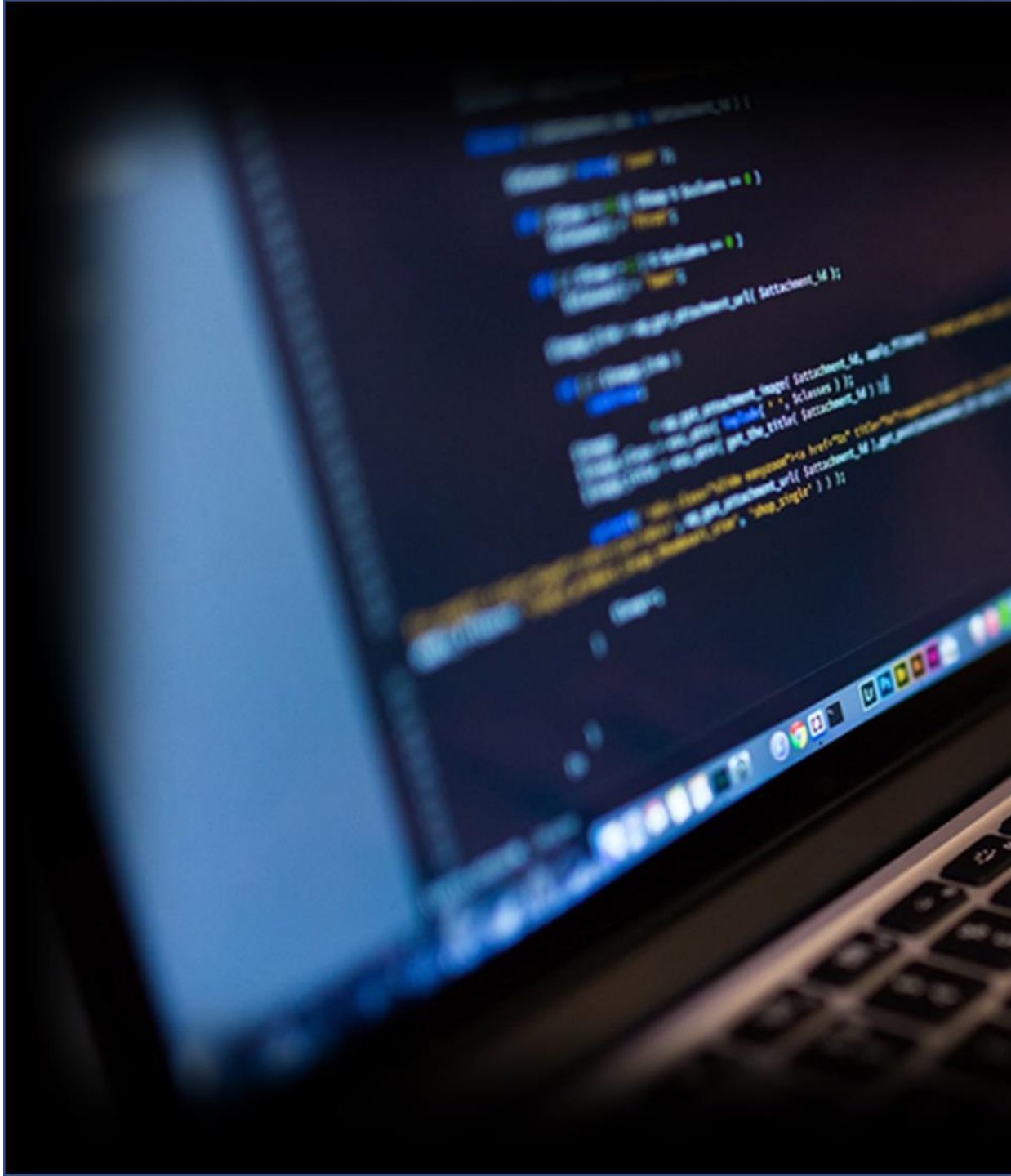
TrustSoT
Solution Intoduction

2022

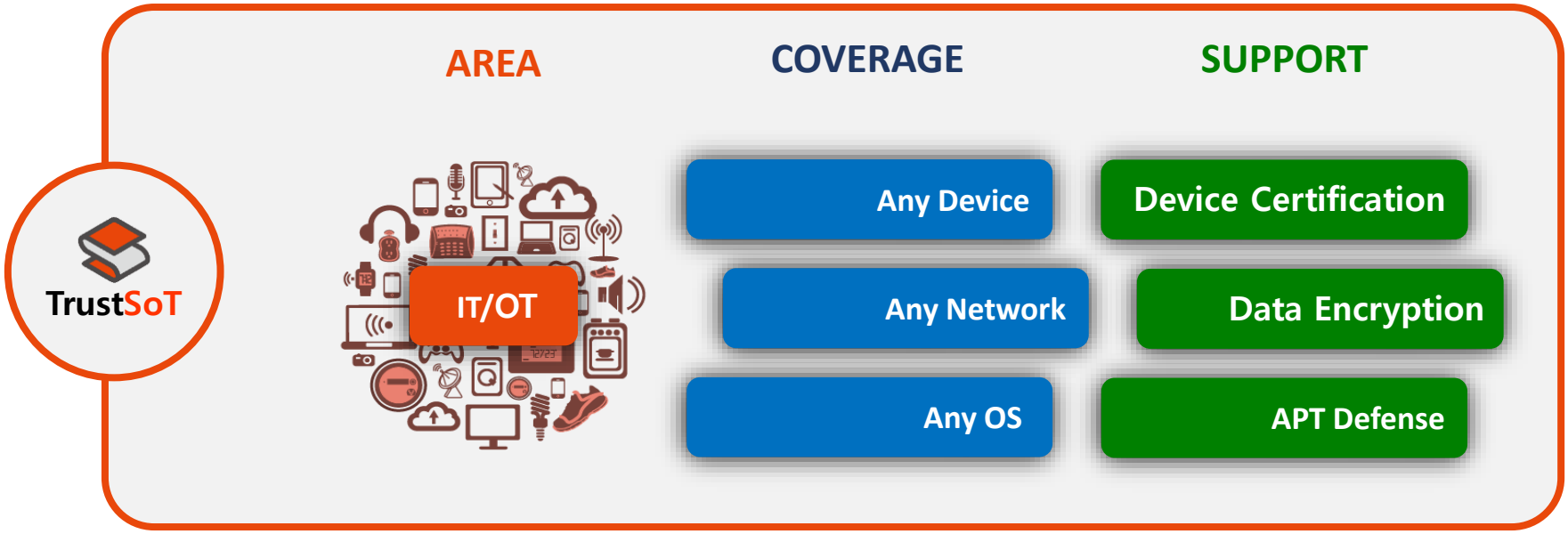


TrustSoT Concept

TrustSoT는 자체 특허를 기반으로

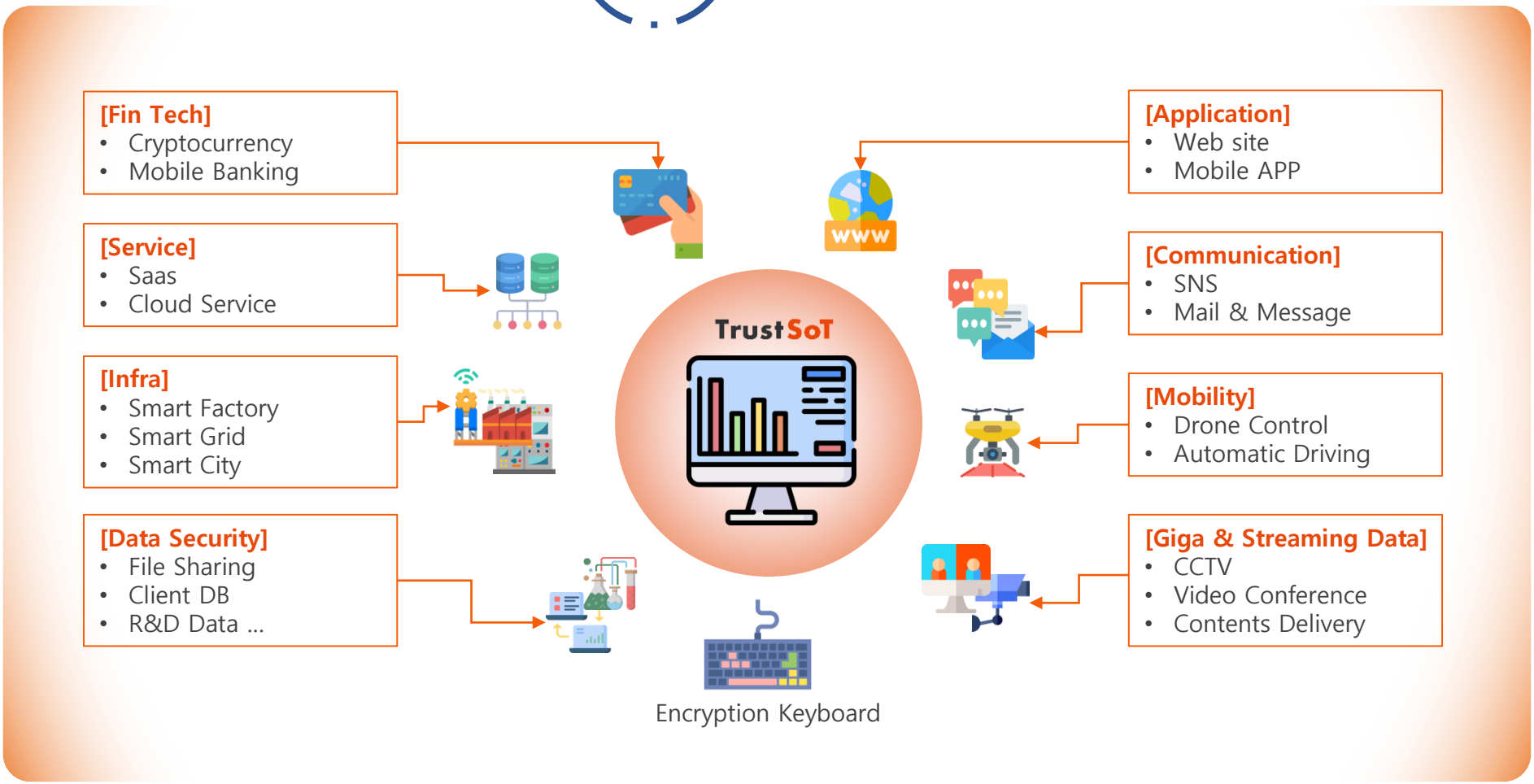
- 「**초경량 S/W Library**」,「**Device 인증**」과「**데이터 생성 시점 암호화**」기술을 이용하여
- 「**Decive**」,「**Network**」,「**OS**」종류에 **무관**하게
- 「**개인정보**」,「**기업 및 공공기관의 기밀정보**」,「**클라우드등의 위탁관리 정보**」「**대용량 스트리밍 영상**」은 물론

  「**원격 및 자동제어분야**(OT/ICS주1))」「**통신인프라 구성**」에서 고객의 목적에 따라 최상의 보안체계를 제공합니다.



주1) OT/ICS : "Operational Technology/Industrial Control System", 운영 기술/산업제어시스템

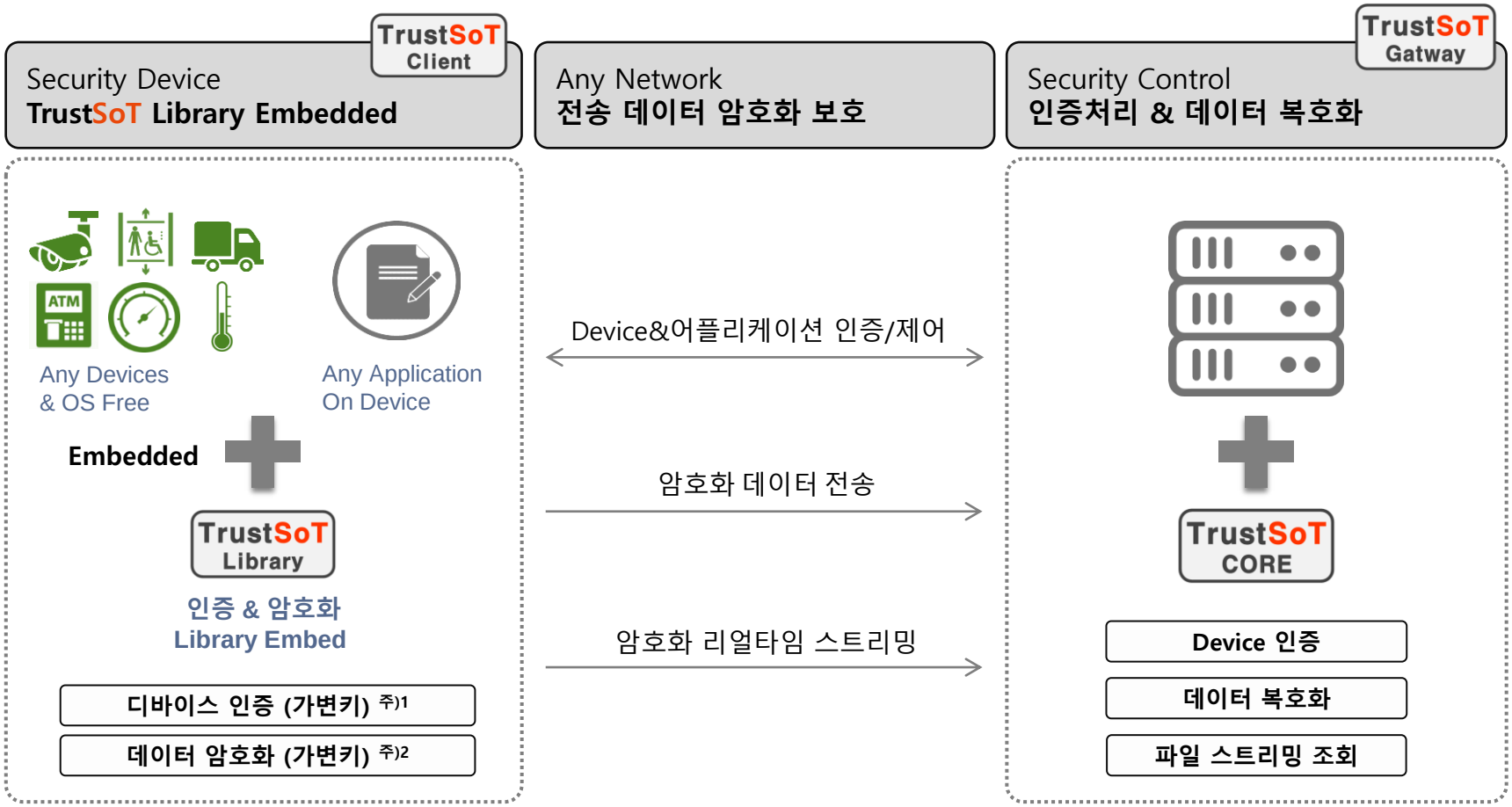
■ TrustSoT는 모든 분야에 적용 가능하며
다양한 형태의 네트워크 그리고 **주요 데이터와 제어명령을 암호화**하여 보호합니다.



TrustSoT Core Technology

핵심 기술

■ 인증/암호화

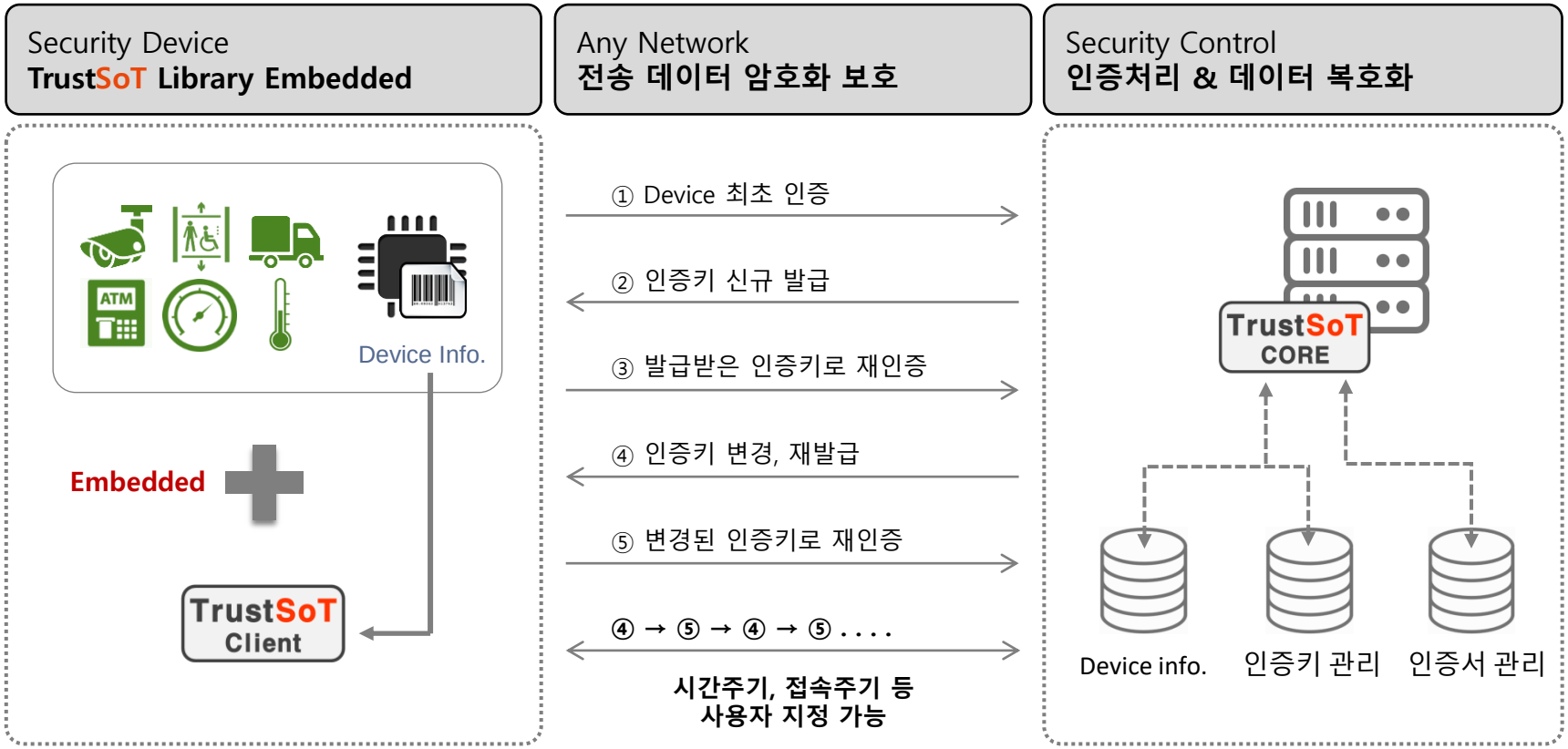


주)1 Page7~8 핵심기술「**디바이스 인증**」참조
주)2 Page9~10 핵심기술「**데이터 암호화**」참조

「디바이스 인증」

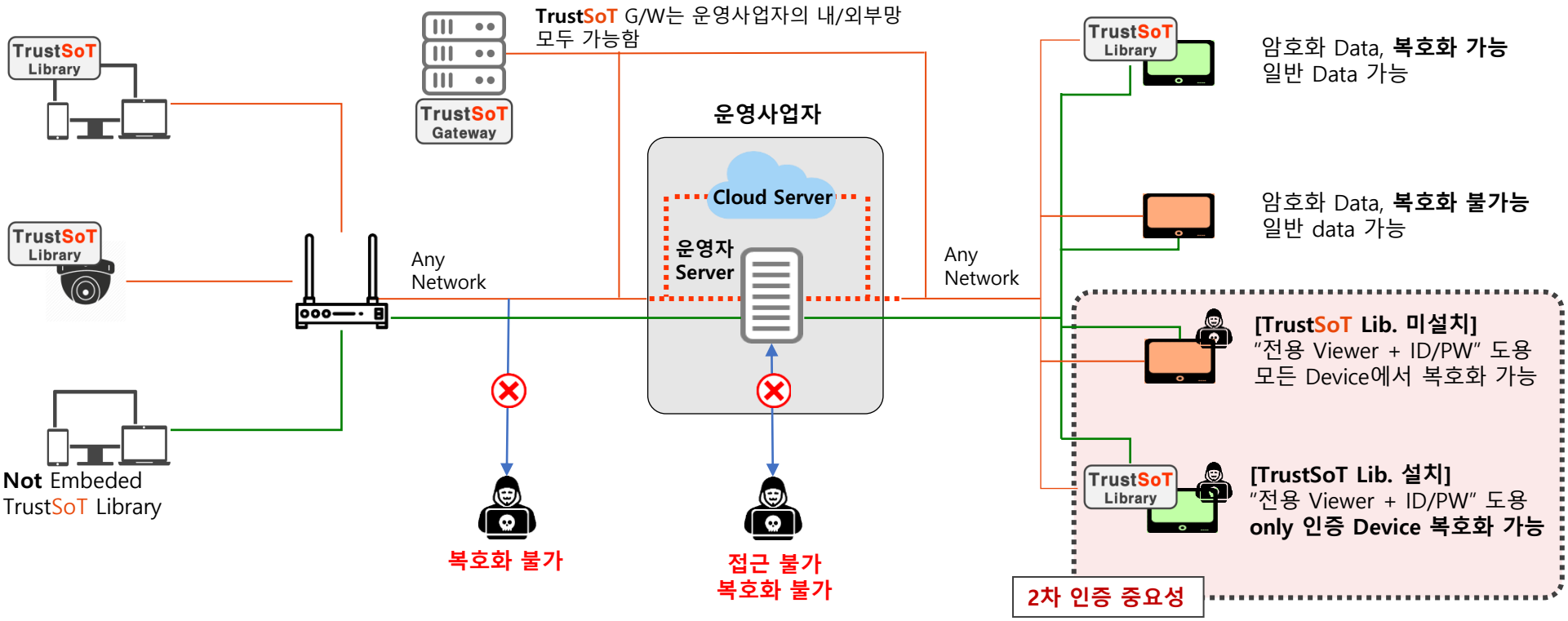
■ TrustSoT가 적용된 Device는

해당 기기의 Unique(개별) 정보 기반으로 인증되며, 초기 인증 이후부터는 시스템 연결 시 매번 신규 인증키를 갱신 받아 인증 신뢰성 극대화 합니다.

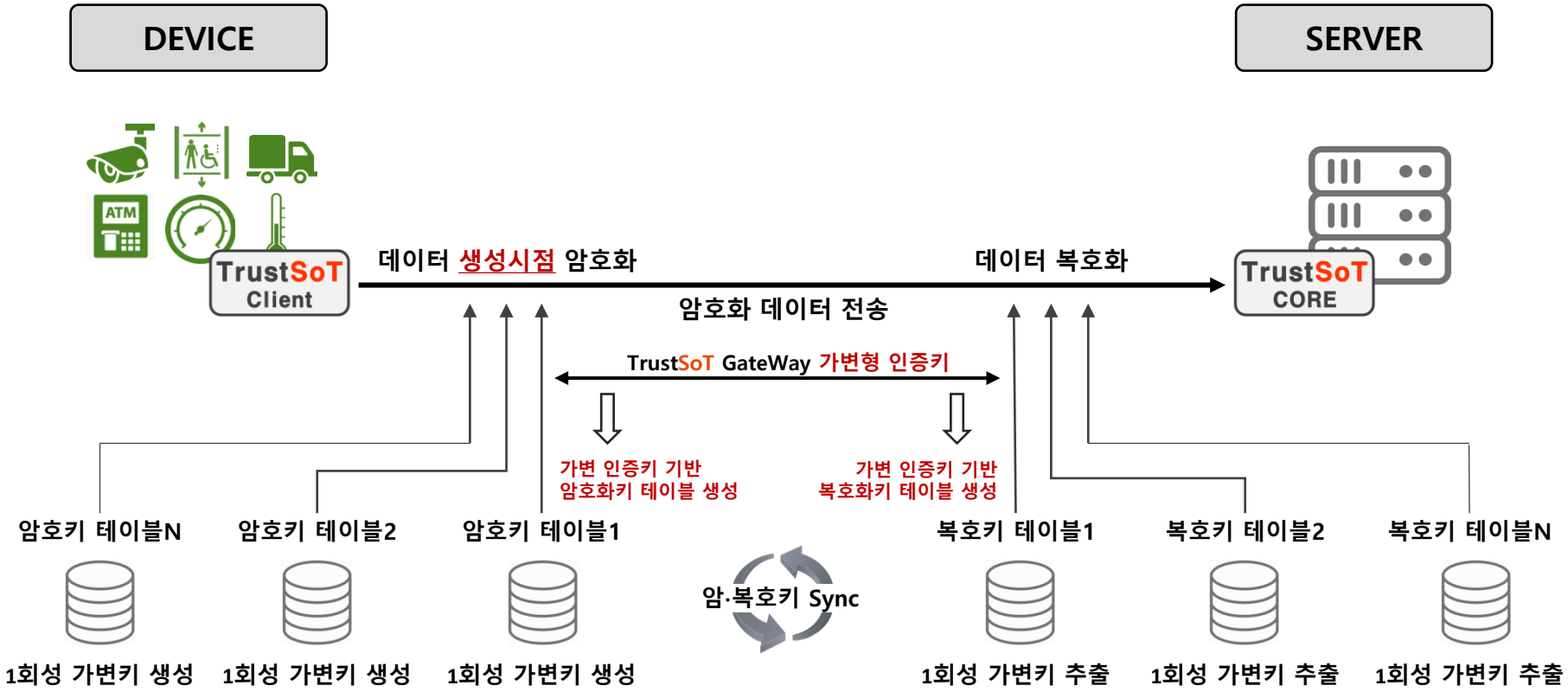


■ TrustSoT의 가변형 인증키 기반 Device 2차 인증의 중요성

- ID, PW를 통한 물리적인 1차 인증인 인증 후, 별도의 사용자 행위없이 정해진 정책(시간 기준, 접속 기준 등)에 따라 사용자의 별도의 행위없이 지속적 2차 인증 진행
- ID, PW 도용시에도 인증받은 Device 외에는 접근 불가하며, ID, PW, 인증 받은 DEVICE 모두 탈취시에도 Device를 제어 함으로영상 접근 및 정보탈취가 불가능합니다.



■ TrustSoT가 적용된 Device는
데이터 생성시점부터 비정규적(Random) 1회성 가변형 암호화 키를 기반으로 한 데이터 암호화를 수행하여
전송 또는 보관 중인 모든 데이터 완벽 보호 (표준 인증 암호 모듈 및 알고리즘 지원)

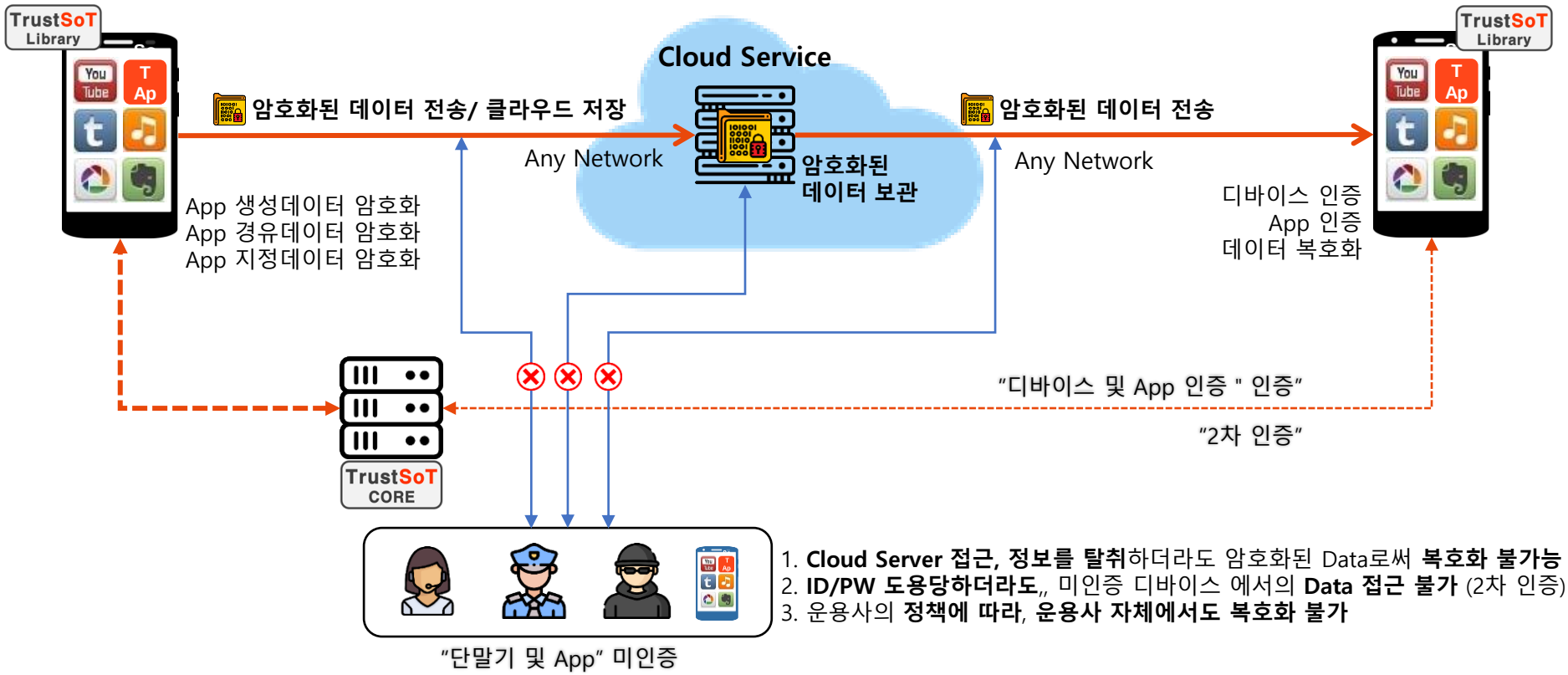


■ TrustSoT vs. 기존 데이터 암호화 기술

TrustSoT	TPM 방식	Chip 방식
■ SW기반 인증 및 암호화 라이브러리 적용만 으로도 보안이 가능. ※ 기 구축 장비에 업데이트 등을 통한 임베딩	□ TPM인증을 위해 HW 제작 단계부터 고려한 설계 필요.	△ Chip인증 및 데이터 암호화를 위해 H/W 제작 단계부터 고려한 설계 필요
■ 가변형 인증키 기반 기기인증	□ 고정키 기반의 인증방식	△ 대부분 고정키 기반의 인증방식 ※ 고정키 유출시 데이터 복호화 가능
■ 생성데이터 암호화 및 수신데이터 복호화 ※ 가변형 암호키 싱크 기술	□ 생성데이터 암호화 불가	
■ 통신구간암호화 불필요. ※ 전송데이터 암호화로 유출되어도 해독 불가		
■ TrustSoT 파일뷰어를 이용, 문서 보안 중앙관리 가능.		
■ 인증 및 데이터 수신현황 모니터링 및 제어		
■ IoT와 같은 저사양 저전력 환경에서도 구동	□ 저사양 저전력 환경에 적용이 어려움	△ 통신구간 암호화 필요 등으로 IoT와 같은 저사양 저전력 환경에 적용 어려움.

TrustSoT Case Study

■ TrustSoT가 적용된 App의 모든 데이터는 생성시점에 즉각 암호화되어 클라우드 서버로 업로드 됩니다.
따라서, 인증받지 않은 단말기는 물론, Cloud 서비스 운영자도 고객 데이터를 열람할 수 없습니다.
사내 기밀정보가 제3의 기관에서 보관되는 불안감을 해소 할수있는 Cloud 서비스 제공이 가능합니다.



Cloud 보관중인 암호화 데이터는 해커는 물론 운영자 및 공식적인 확인 절차에도 복호화 불가능

■ **TrustSoT Cloud Security** vs. 일반 Cloud Service

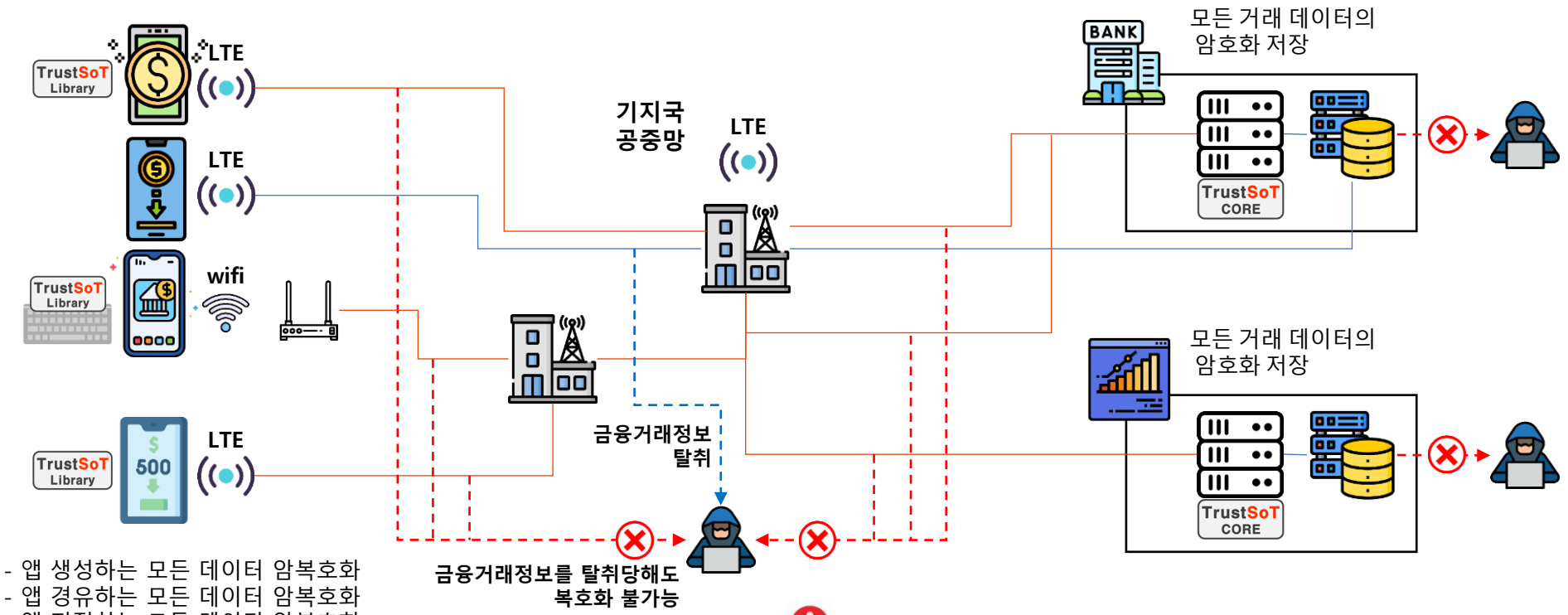
구분	TrustSoT Cloud Security	일반 Cloud Service
앱 인증방식	TrustSoT **가변형키**를 통한 단말기+앱 **2차 인증**방식	ID, 맥어드레스 기반 일반 인증방식
데이터 보호	TrustSoT인증앱에서 데이터 **생성순간** 암호화	별도의 데이터 보호(암호화 등) 지원 없음
네트워크 보안	**암호화 데이터 상태**로 클라우드 업/다운로드 (네트워크상 해킹 되어도 데이터 복호화 불가)	업로드시 네트워크해킹 데이터 유출가능
클라우드 해킹 대비책	암호화 된 데이터가 클라우드에 업로드되어 인증된 단말기(앱) 외에는 데이터 사용불가	클라우드 해킹 시(ID/PW유출 등) 모든 데이터 유출사고 발생 취약성
단말기 분실시 처리방식	해당 **분실 단말기** 앱을 **사용불가 설정**하여 클라우드에 업로드된 데이터 완벽 보호	클라우드 접속 ID/PW변경 이외 대안책 없음

■ Solution1

은행 App에 TrustSoT 를 적용하여 App에서 발생되는 모든 데이터는 생성시점에 즉각 암호화되어 모든 거래를 완벽히 보호합니다.

■ Solution2

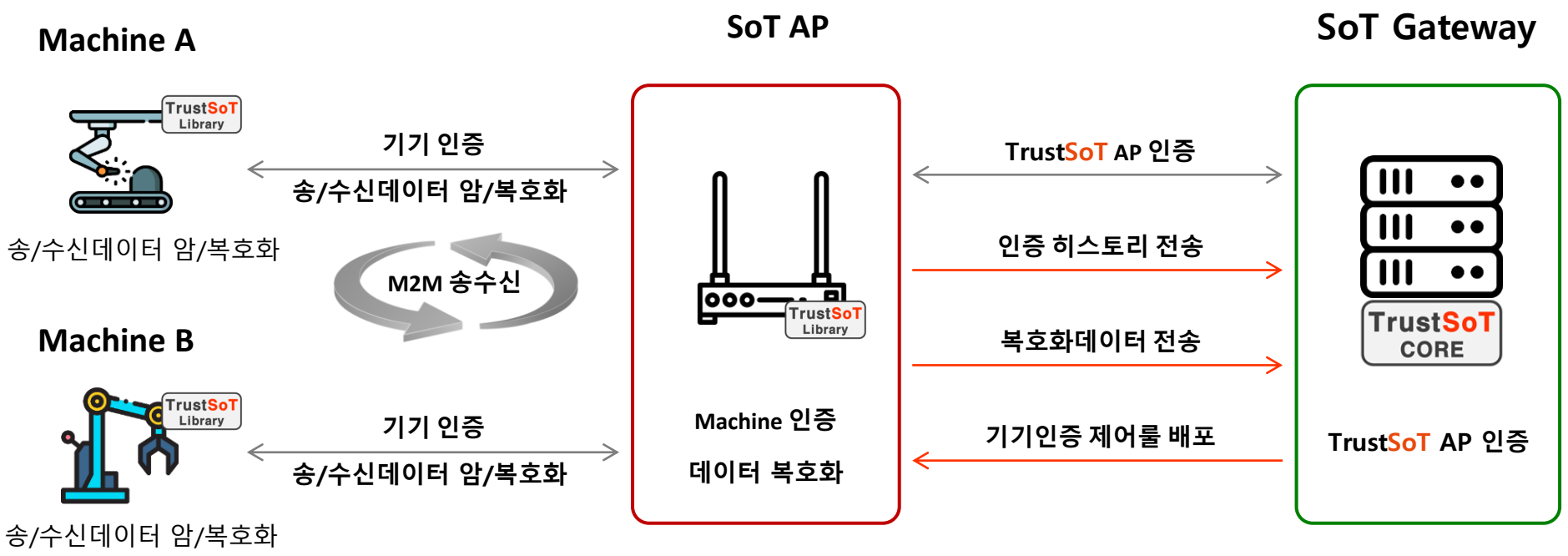
은행 App 내부에 TrustSoT "**보안키보드**" (page21) 적용을 통해 입력, 저장, 전송되는 모든 데이터의 암호화를 통해 모든 거래를 완벽히 보호합니다.



- 앱 생성하는 모든 데이터 암복호화
- 앱 경유하는 모든 데이터 암복호화
- 앱 지정하는 모든 데이터 암복호화

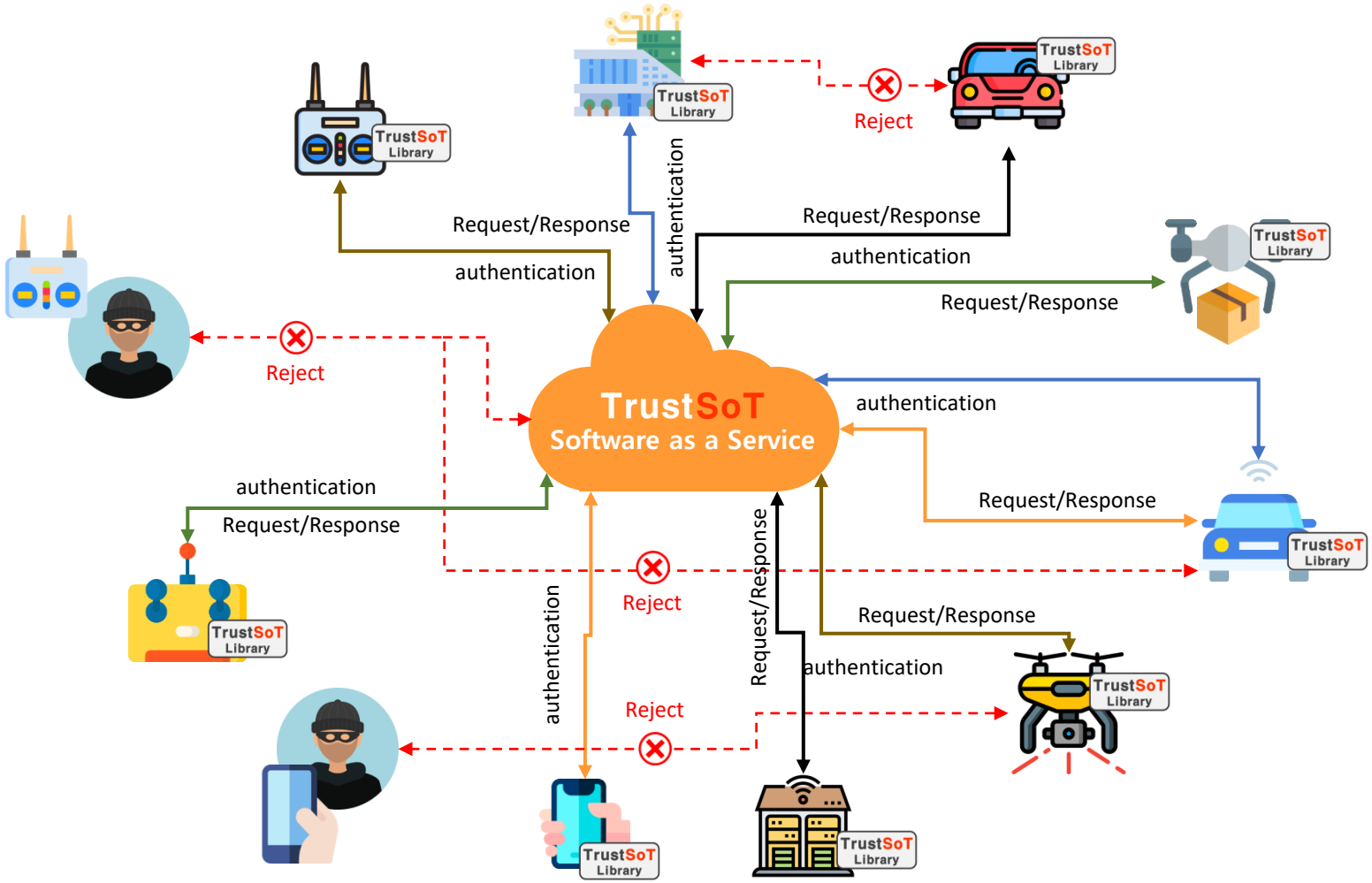
거래중 통신상에 데이터 보호는 물론 보관중인 거래 데이터 또한 완벽 보호
[ID/PW, 거래금액, 계좌번호, 거래 상대방 정보 등 모든 데이터]

■ TrustSoT는 다양한 IoT 컨버전스 분야에 최적화 된 Device 인증 및 데이터 보호를 지원합니다.



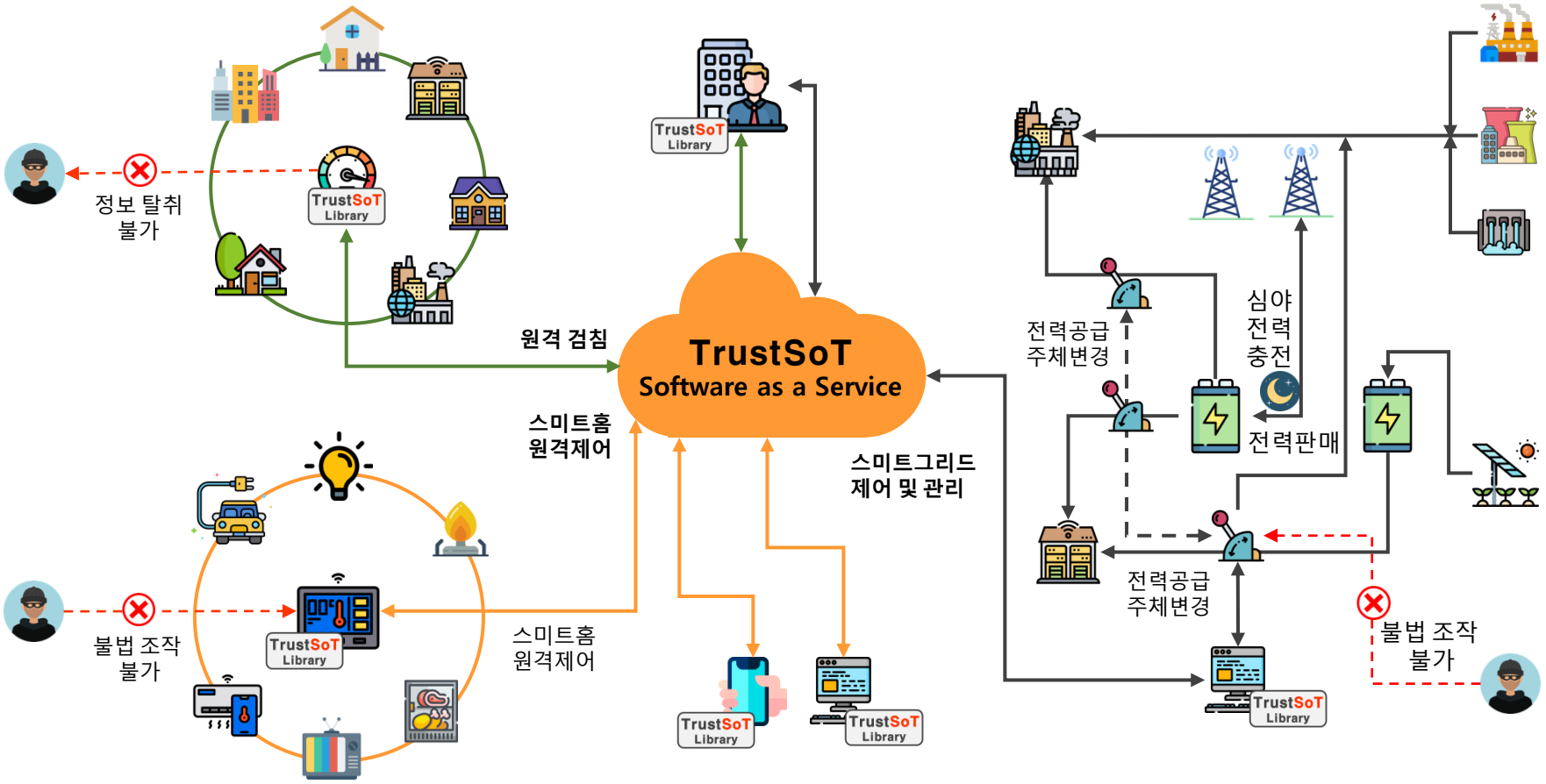
기업 및 공공인프라의 M2M 구성에 있어, TrustSoT 솔루션(AP, GateWay 등) 적용을 통해 기기간 인증 및 송수신 데이터에 대한 원천 보안이 가능

■ TrustSoT는 다양한 이동체의 제어신호 보호와 제어 Device에 대한 인증을 지원합니다.



이동체와 제어 Devices간의 인증 및 제어신호의 완벽한 보호를 통해 오동작을 사전에 방지

■ TrustSoT는 산업제는 물론 경량 IoT 디바이스예 이르는 다양한 디바이스에 대한 인증 및 상호 송수신 데이터의 보호를 지원합니다.



Devices간의 인증 및 제어신호 및 Device 발생 데이터의 완벽한 보호를 통해 오동작 및 정보유출 방지

TrustSoT Product

제품 및 적용 분야

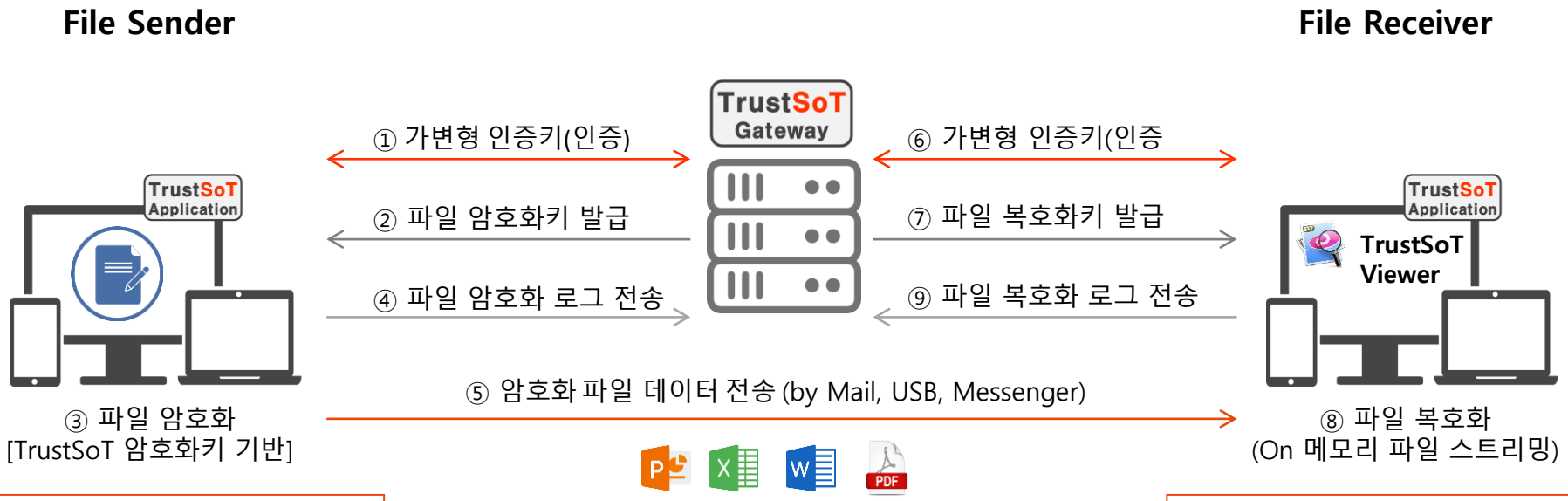
■ **TrustSoT** 기반기술을 IT 영역의 다양한 분야의 솔루션에 적용은 물론 OT/ICT 분야에 대한 산업용 제어분야에도 적용함으로써, 고객 환경에 바로 적용 가능한 Apllication 및 제품 개발을 계속 추진하고 있습니다.

Soft ware	**TrustSoT CORE** **Gateway** **Devices 인증 / Data 암호화** 네트워크 내 모든 Device에 대한 초경량 라이브러리기반 보안 인증 지원 및 상호 인증 Device의 데이터 송수신 시 완벽한 암호화 & 복호화 지원	**TrustSoT Keyboard** (키보드 입력 데이터 암호화) **Plug in + Gateway** TrustSoT 기술 기반의 가상 키보드 플러그인을 통해, 기존의 키보드의 변경없이 작성된 모든 텍스트도 암호화하여 보관/전송함으로써, 키보드를 통해 생성되는 모든 데이터를 원천 보호
	TrustSoT File (파일 암호화) **Application+Gateway** Device에 설치된 어플리케이션을 통해 파일을 암호화하여 전송하며, 파일 수신자는 TrustSoT 파일 전용 뷰어를 통해 해당 파일을 Streaming만 가능한 파일 보안 솔루션	**TrustSoT IMG** (영상 데이터 암호화) **Application+Gateway** Camera에 설치된 어플리케이션(에이전트)을 통해 영상 데이터를 암호화 암호화 및 복호화, 캡쳐방지, 원격 해킹 방지 등의 영상 컨텐츠 불법 복제 및 유통 방지 기능을 제공
	TrustSoT Mail (메일 암호화) **Plug in + Gateway** TrustSoT 기술 기반의 웹브라우저 플러그인을 활용, 모든 웹메일 서비스의 전송 텍스트 및 첨부 파일을 원천 보호 메일 전송 이후에도 보낸 메일 보안 제어를 지원	**TrustSoT OT/ICS** (SCADA/PLC 제어 데이터 암호화) **Application+Gateway** SCADA 제어 Device에 설치된 에이전트을 통해 Device의 인증 및 제어 Data의 암호화, 부정 Access, 정보 탈취 방지와 Agent 기반 Process 감시를 통해 악성코드 탐지, 경고 및 내부망 확산 차단
Hard ware	**TrustSoT Security Camera** (Security CCTV Camera) with **TrustSoT IMG**	**TrustSoT LTE Router** (Security LTE Router) with **TrustSoT CORE** (인증/암호화)

Software

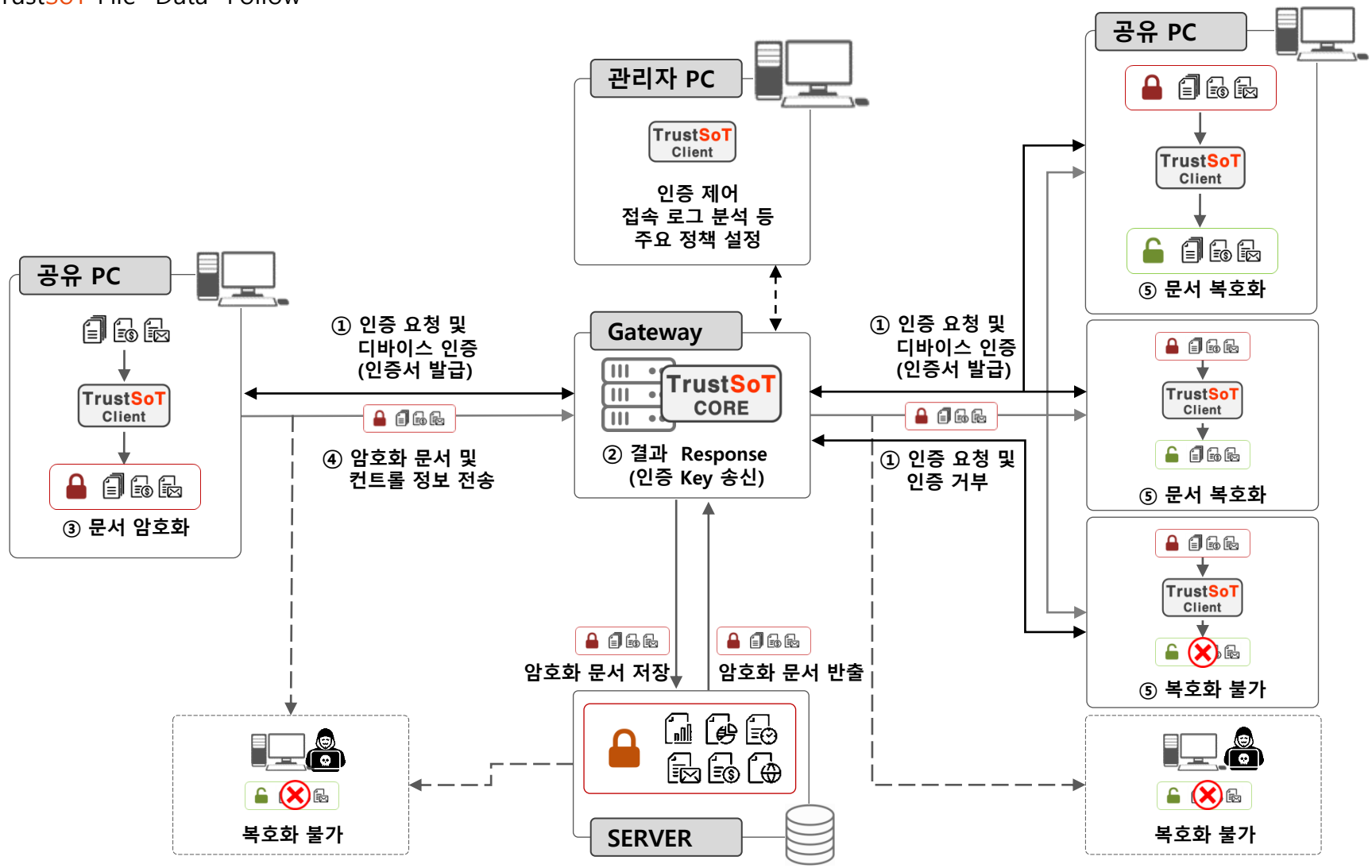
TrustSoT File (파일 암호화)

■ 「TrustSoT File」 어플리케이션이 설치된 Device는 파일을 암호화하고 전송하고
해당 파일을 수신받은 「TrustSoT File」 어플리케이션이 설치된 사용자는 「TrustSoT Gateway」를 통해 인증을 받은 후,
「TrustSoT File 뷰어」를 통해서만 복호화 및 조회가 가능 (Device에 저장 불가)하게 함으로써,
내부망에서 뿐만 아니라, 전 영역에서 문서 파일의 완벽한 보안 및 중앙 관리가 가능합니다.



「TrustSoT File」 User간 송수신 암호화 메일은 TrustSoT Gateway에서도 복호화 불가

■ TrustSoT File "Data" Follow

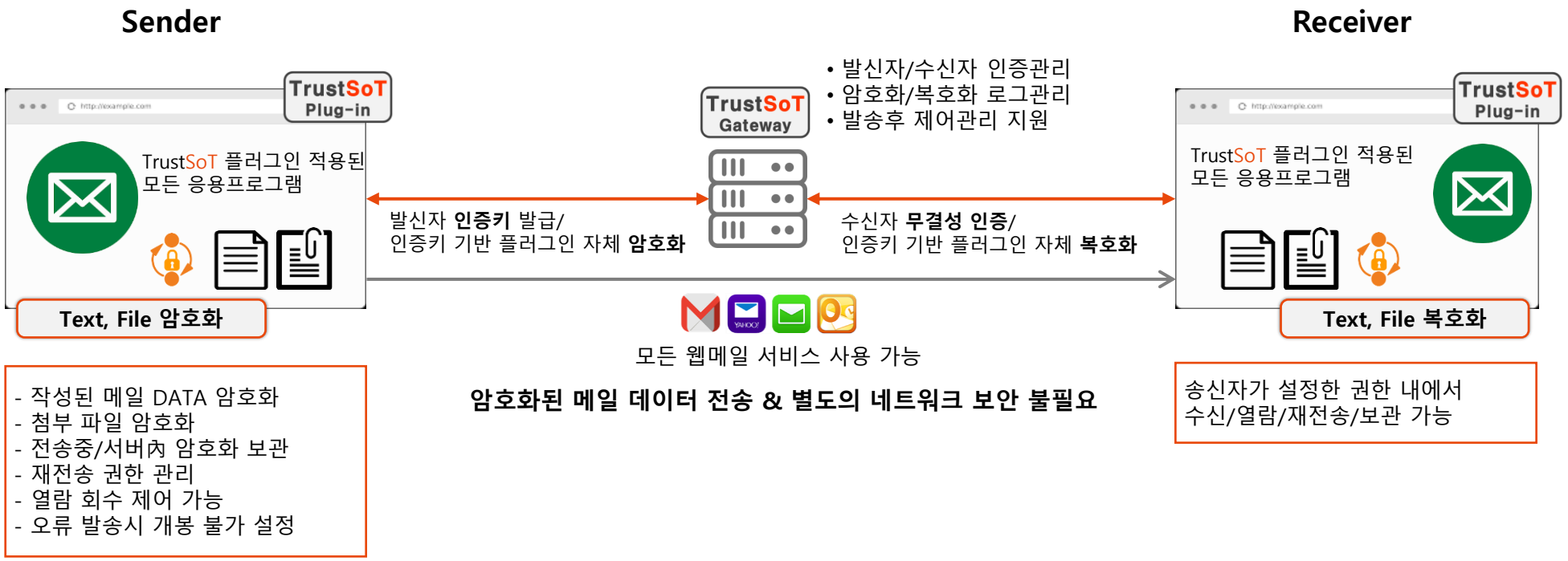


■ **TrustSoT File** vs. 일반 문서중앙화 기술

구분	TrustSoT File	일반 문서중앙화 방식
전송구간 제약	■ 데이터 전송구간 암호화 적용 불필요	□ 내부 폐쇄망 구현 필요
파일 암호화	■ 외부 파일 전송 시, 문서를 암호화하여 전송 ■ 가변형 암호화키를 통해 암호화 된 데이터를 전송하므로, 해킹시에도 파일유출을 방지	□ 파일 암호화는 옵션이며, 일반 암호화 방식 □ 외부 파일 반출 시, 허가 또는 권한 필요
파일 보호	■ 파일을 암호화 하는 유저가 수신자를 지정할 수 있고, 인증받은 수신자에 한해 파일 조회가 가능 ■ 수신자는 복호화 된 파일을 조회만 가능하며, 개인 Device에 저장할 수 없음.	□ 파일을 수신받은 외부 사용자의 컴퓨팅 환경을 □ 제어할 수 없음.(반출 기록만 존재)

TrustSoT Mail/SNS/App. 암호화

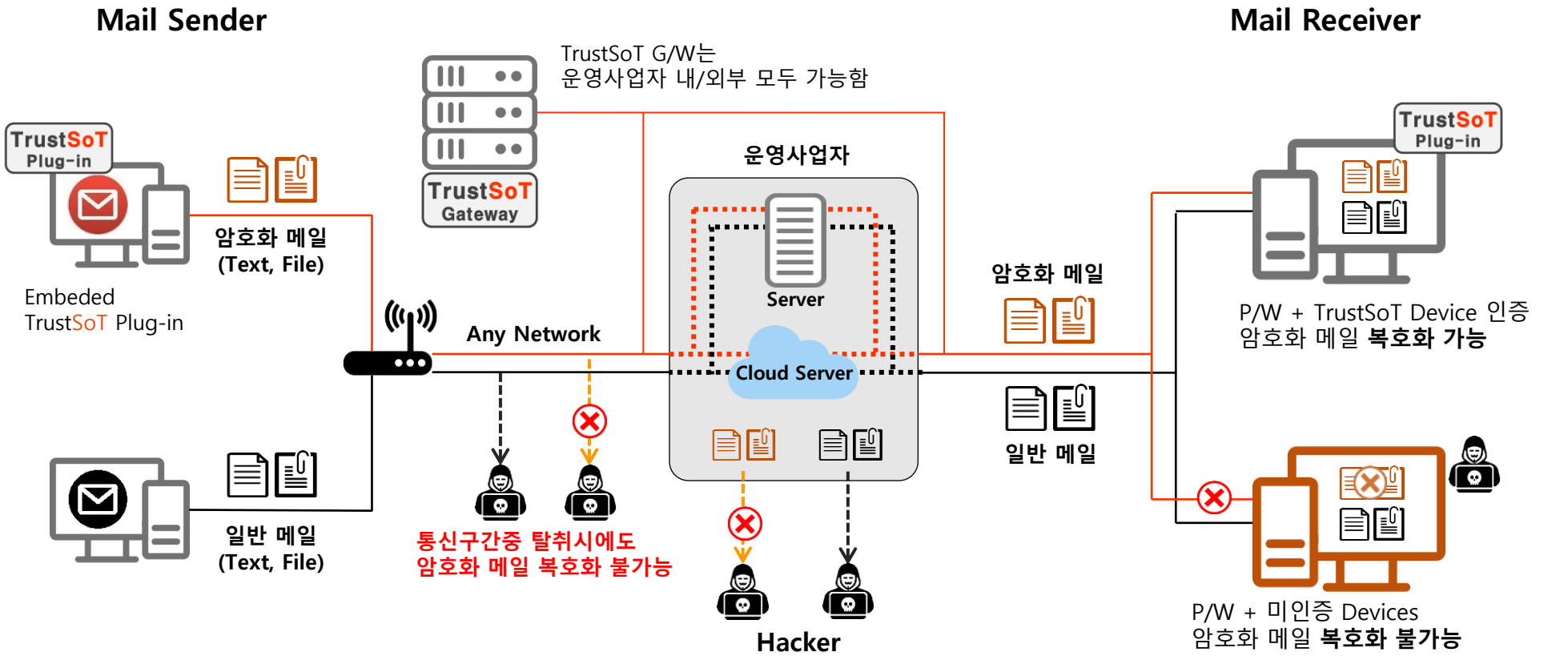
■ 「TrustSoT Mail」 웹브라우저용 Plug-in을 통하여 웹메일, SNS, Mobile App.의 텍스트 및 첨부파일에 대한 암호화를 수행합니다.
또한, 메일 전송후에도 다양한 보안제어 및 사후관리를 지원합니다.
별도의 네트워크 보안 솔루션이 없어도, TrustSoT Library or Plug-in 만으로도 보안 메일 및 이에 대한 사후관리가 가능합니다.



「TrustSoT Mail」 User간 송수신 암호화 메일은 TrustSoT Gateway에서도 복호화 불가

TrustSoT Mail (메일 암호화)

■ TrustSoT Mail "Text & File" Follow



운영자 Server, Cloud 보관중인 암호화 메일을 탈취시에도 복호화 불가능

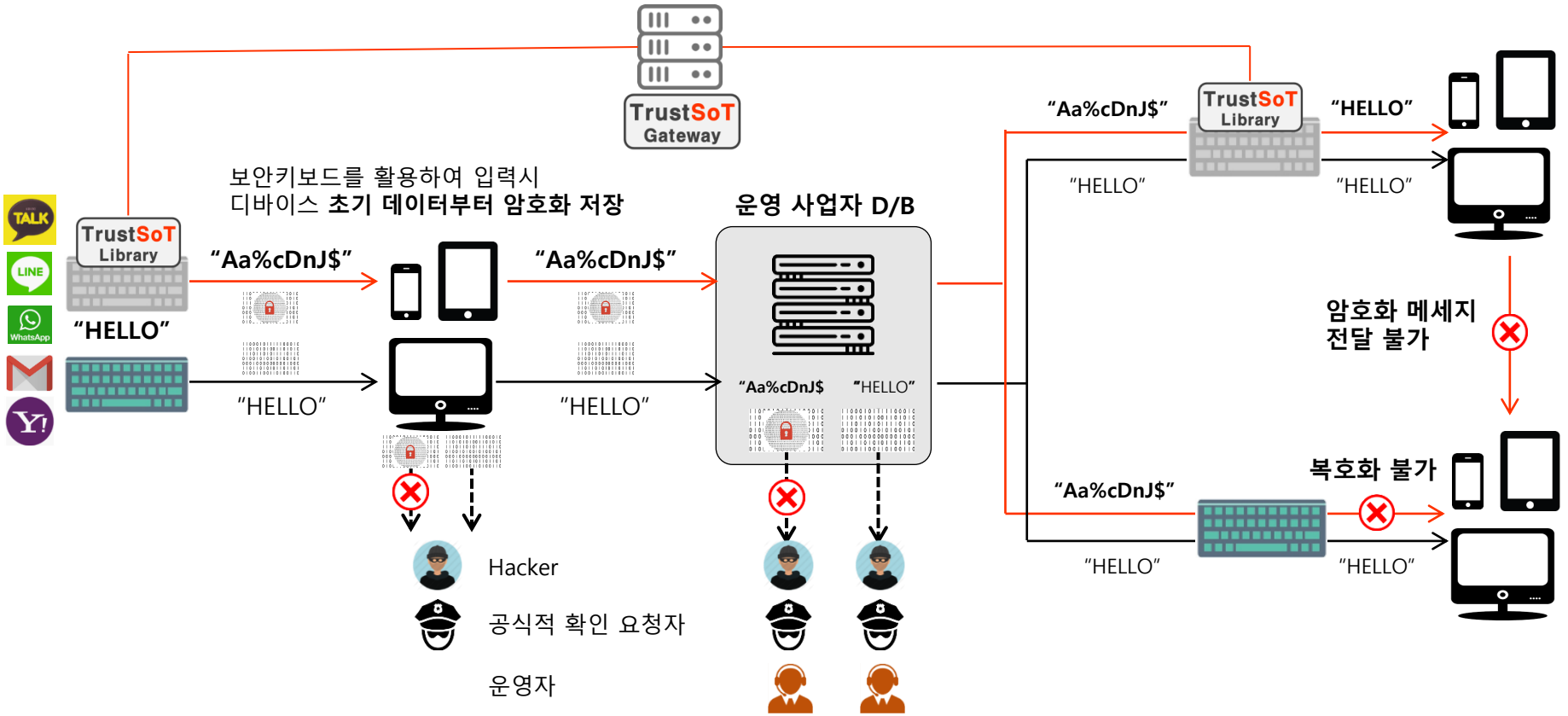
(보관중인 일반 메일 탈취시 내용 확인 가능)

■ TrustSoT Mail vs. 일반 보안 메일 솔루션

구분	TrustSoT Mail	Gmail 보안 서비스 (USA, C社)	정보유출 방지 솔루션 (KOR, U社)
사용자 인증	■ 브라우저 플러그인 통한 복합인증 ■ 별도 어플리케이션 설치 불필요 ■ 가변 인증으로, 완벽 인증 보안	□ 메일 수신자 PW를 통한 사용자 인증 □ 송신 PW 인지 시 모든 메일 열람 가능	△ Agent(Software) 설치를 통한 인증
데이터 보안	■ 모든 암호화 알고리즘 적용 가능 ■ TrustSoT 데이터 보안 기술 적용 ■ 메일 텍스트 브라우저상에서 암호화 ■ 플러그인을 통해 암호화된 파일 첨부 ■ 첨부파일 용량 제한 없음	□ 메일 송신자 설정 PW 기반 보안 □ 메일 텍스트 AES25 인코딩 지원 □ 메일 파일 첨부시 AES25 인코딩 후, C社 클라우드로 업로드/ 링크 방식 □ 첨부파일 용량 최대 100M	△ 텍스트 및 파일을 서버에 업로드하여 암호화 후, 데이터를 전송 △ 해당 데이터는 뷰어(Agent)가 설치된 모든 단말기에서 복호화 가능 △ 서버에서 첨부파일 용량 제한
호환성	■ 모든 OS, 모든 웹브라우저 호환 ■ 모든 모바일 앱 라이브러리 지원	□ 일부 웹브라우저, Gmail서비스 전용 □ 전용 모바일 앱 다운로드 필요	△ Agent가 제공하는 OS 환경만 지원 △ 데이터 조회 위해 전용 뷰어 설치 필요
솔루션 도입 ROI	■ TrustSoT Gateway 및 플러그인 비용만 발생 ■ 모든 메일 서비스 적용 가능	□ 사용자 당 일괄 5달러/월 서비스 요금 □ Gmail 서비스에 한해 이용가능	△ 솔루션 구축 발생(서버, Agent) △ 필요시 네트워크, 단말보안 비용 발생

TrustSoT Keyboard (암호화 가상키보드)

■ 「TrustSoT KeyBoard」 Library가 적용된 모든 디바이스의 초기 입력장치로의 Data의 생성시점 부터 암호화를 적용함으로써 통신 구간 보안 솔루션과 연동 없이도 완벽한 데이터의 보호가 가능합니다.
또한, 데이터의 공유 이후에도 암호화가 유지되며, "중앙의 명령"에 의해 각 디바이스의 복호화 가능/불가능합니다. (차별화)



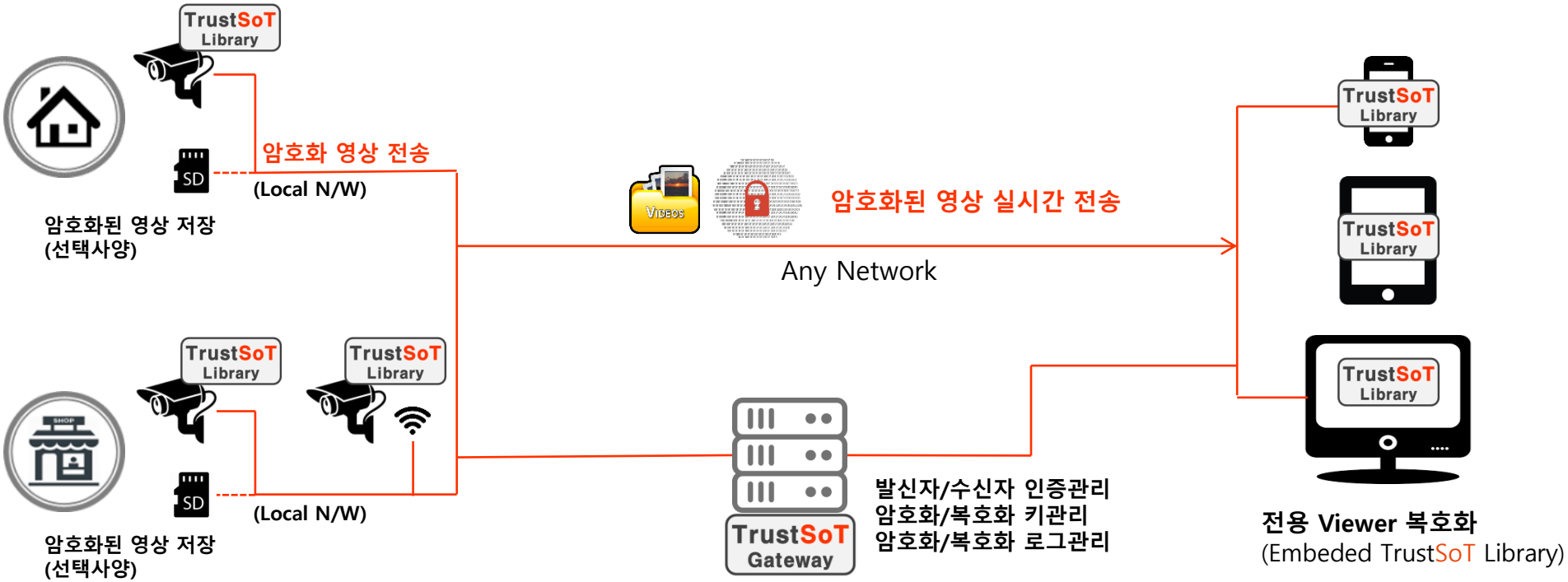
운영자 Server, Cloud 보관중인 암호화 데이터는 해커는 물론 운영자 및 공식적인 확인 절차에도 복호화 불가능

■ 주요 기능

구분	기능
상용 암호화 키보드	□ 메신저, 메일을 비롯한 모든 문서와 앱, 그리고 생성 데이터를 암호화 □ 암호화 데이터 공유시 복호화가 가능하도록 지정한 대상(사람, 디바이스)만 복호화 가능 □ 복호화에 대한 횟수, 기간 등 제한 가능 □ 복호화 권한의 취소 가능 (복호화 권한이 주어졌다 하더라도 이후 복호화 권한이 취소된 사용자는 권한 취소전, 후의 문장을 복호화 하는 것이 불가능)
기업 암호화 키보드	□ 일반 암호화 키보드 기능을 모두 적용 □ 키보드 입력/암호화/인증 로그 수집 □ 키보드가 설치된 디바이스에 대한 일부 감시 (스크린 캡쳐, 악성앱 구동 감시 등)
부가 특수기능	□ 암호화 문자열의 이미지화, RGB화 (저장, 공유) □ 운영자 제공 Open API를 활용, 화면에 출력되고 있는 메신저창(개인방, 단톡방 등의 회원 자동 인식 (복호화 권한 제어) **-암호화 데이터 클라우드 서비스(백업)로 데이터의 안전한 저장 및 복구 가능**

TrustSoT IMG (영상 데이터 암호화)

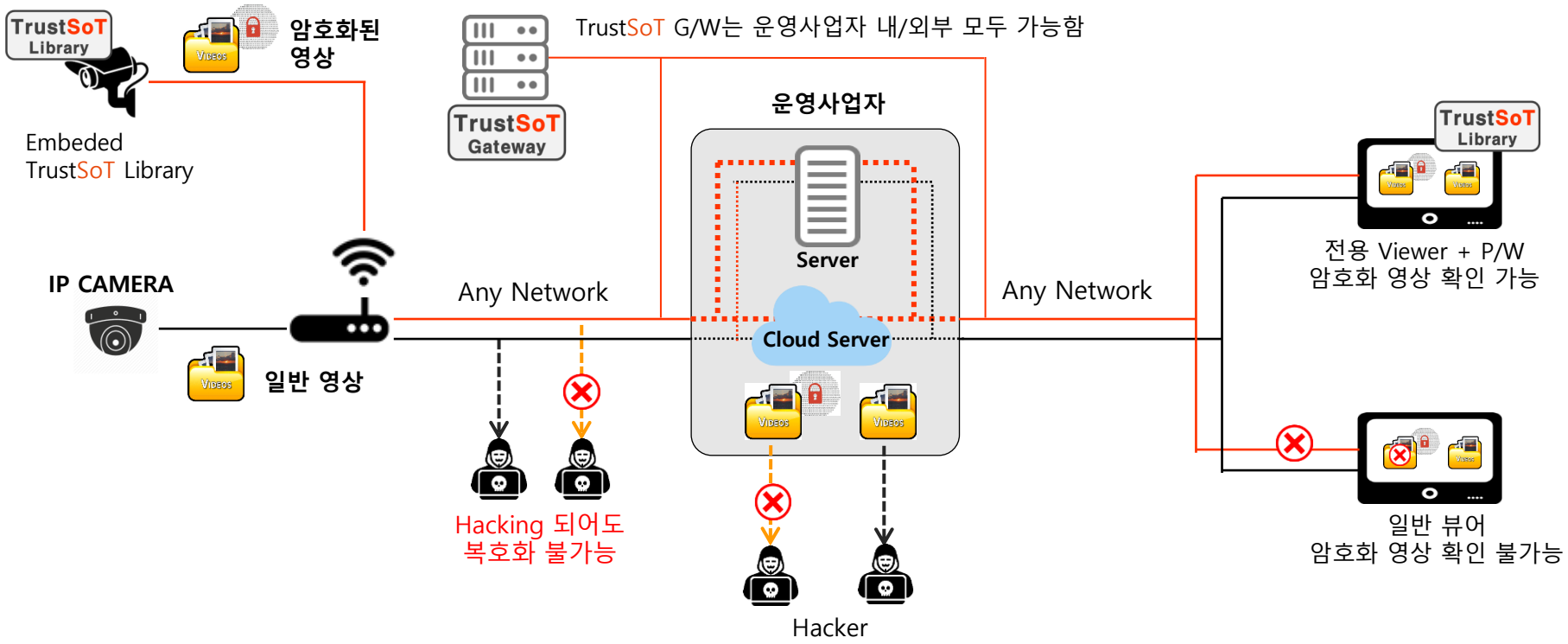
■ 「TrustSoT IMG」 Library가 적용된 CCTV 카메라 등 영상 데이터 발생 장치의 영상 데이터 발생시점 부터 암호화가 적용되어 영상 데이터가 유출되어도 해독이 불가능하여, 영상의 불법 탈취, 복제, 유통이 근본적으로 방지됩니다.



「TrustSoT IMGI」 User간 송수신 암호화 영상능 TrustSoT Gateway에서도 복호화 불가

TrustSoT IMG (영상 데이터 암호화)

■ TrustSoT IMG "Video & Image" Follow



운영자 Server, Cloud 보관중인 암호화 영상을 탈취시에도 복호화 불가능
(보관중인 일반 메일 탈취시 내용 확인 가능)

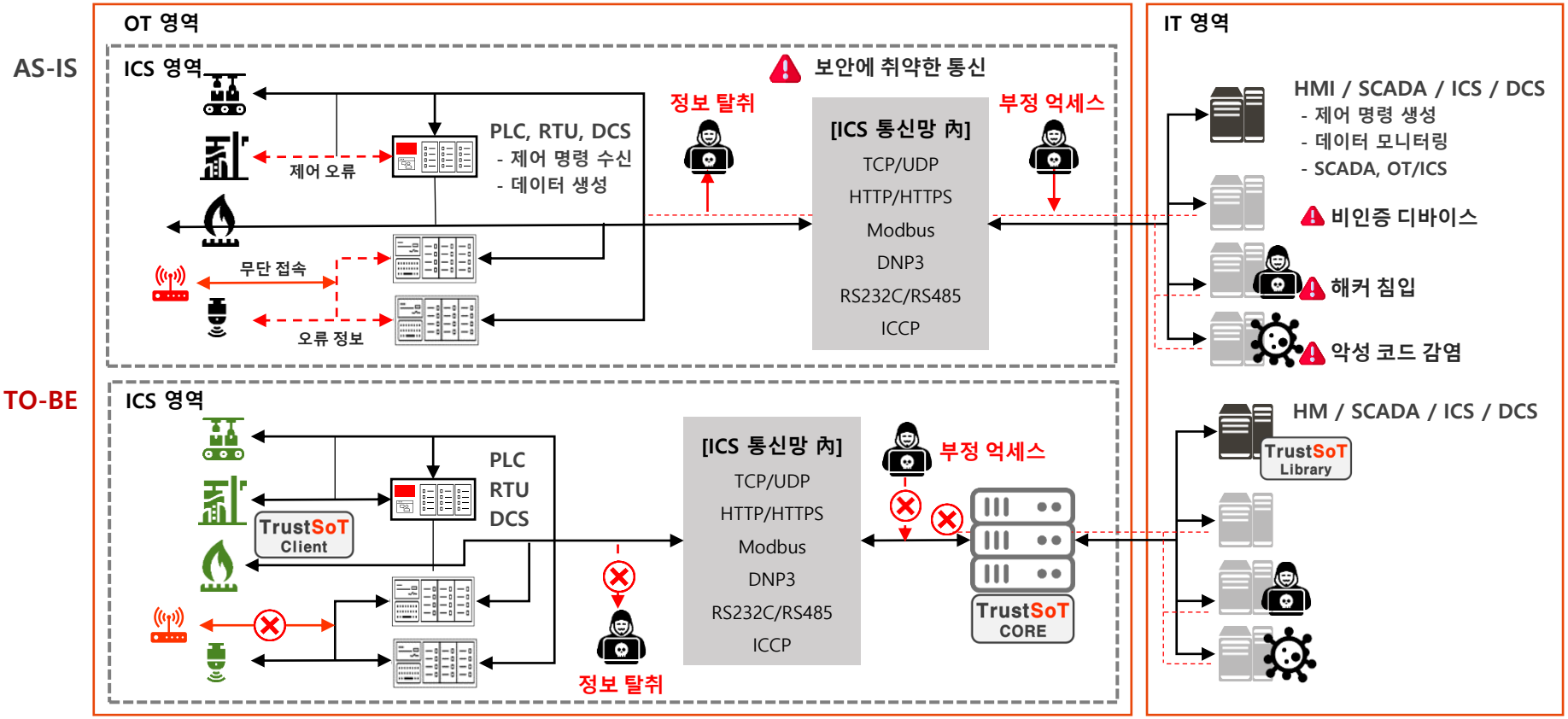
■ **TrustSoT IMG** vs 일반 CCTV 암호화 기술 비교

구분	TrustSoT IMG	일반 CCTV 암호화
전송구간제약	■ 영상 생성시점 즉시 Header 암호화 ■ 데이터 전송구간 암호화 적용 불필요	□ 영상 생성시점 암호화 불가 □ 데이터 전송구간 내 Header 암호화
데이터 보존	■ 영상 생성시점 즉시 Header 암호화 및 자체저장 ■ 통신 단절 시에도 한도용량 내 데이터 보존	□ 영상 데이터 전송시 암호화 방식 □ 통신 단절 시 송출되지 못한 영상 데이터 유실
데이터 보호	■ 가변형 인증키 기반 단말기 보안인증 지원 ■ 가변형 암호화키를 통해 실시간 암호화 된 데이터가 전송되므로, 해킹시에도 데이터 유출 방지	□ IP 또는 맥어드레스 방식의 기초적 단말기 인증 □ 전송구간 내 고정키 기반 Header 암호화 방식으로 해당키 유출 시 데이터 보안 불가
데이터 암호화 시점	■ CCTV 영상 데이터 생성순간부터 암호화 하는 유일한 경량 솔루션(AES256 이상)	□ 영상 생성시점이 아닌, 전송시점 암호화 방식

TrustSoT OT/ICS (산업 제어 신호/데이터 암호화)

■ 「TrustSoT OT/ICS 」는 망구성(내부망/폐쇄망) 특성상 기기 제어와 모니터링에 대한 특별한 보호 방안이 없어 각 부분별로 다양한 보호체계가 필요 기존 OT/ICS(산업제어) 분야에 대해, 발생할 수 있는 각종 보안 문제를 해결하기 위해 디바이스 인증, 데이터 암호화 및 이벤트 감시 등을 통한 제어 분야를 보호합니다.

■ TrustSoT OT/ICS "Control Signal/Data" Follow



Gateway 및 Module 주요 기능

TrustSoT Slave Agent	TrustSoT Gateway	TrustSoT Master Agent
복호화 키 요청 제어 명령 복호화 및 확인 인증서 발급/폐지 요청 데이터 생성, 인증 정보 전송 송신 데이터 생성 / 수신 데이터 분석	데이터 중개(Proxy) Master , Slave간 인증 및 접근제어 (인증, 암호화)가변키 관리 전송데이터 분석 모니터링로그수집	암호화 키 요청 제어 명령 암호화 인증서 발급/폐지 요청 데이터 인증 정보 확인 송신 데이터 생성 / 수신 데이터 분석

OT/ICS 부문에서의 추가 기능 : 악성 코드 내부 혹산 방지 기능

구분	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
악성코드 감염 후 내부 확산 방지 기능	× 공개/비공개 악성코드 차단	× 공개 악성코드 차단	○ 공개/비공개 악성코드 실행 경보 및 내부 확산 방지(**차단**)
생성 파일 보호	×	×	○
ICS(산업제어) 프로토콜 지원	×	×	○
기기 사용자 감시	×	×	○
파일 유출 보호	○	×	○
주요 기능	침입 차단	침입 차단	**확산 차단** **데이터 암호화**

Hardtware

Security Camera (TrustSoT IMG 적용)

항목		사양	항목		사양
무선		IEEE802.11b/g/n	움직임 감지		움직임이 감지되면 자동으로 켜짐 (감지 거리 5m)
동영상 출력		HD960P	렌즈		3.6mm/90° 시야각 렌즈 (Option : 2.8mm/120°)
압축방식		H.264	음성 지원		원격 양방향 음성 송수신 기능
OS	스마트폰	Android, iOS	소비전력		< 5W
	PC	Windows	전구 수량	LED	25pcs
저장 메모리		2 ~ 64GB micro SD		적외선	4pcs (Night vision 8~10m)
Back Up		Mobile, PC	소켓		E27/E26/B22
렌즈 해상도		1.3mega pixel	중량		280g
알람		동작 감지, 소리, 메시지, 조명	사용환경		-20°C ~ 50°C
저장 시간		최대24일/ 64G micro SD	사용전원		AC 100~250V

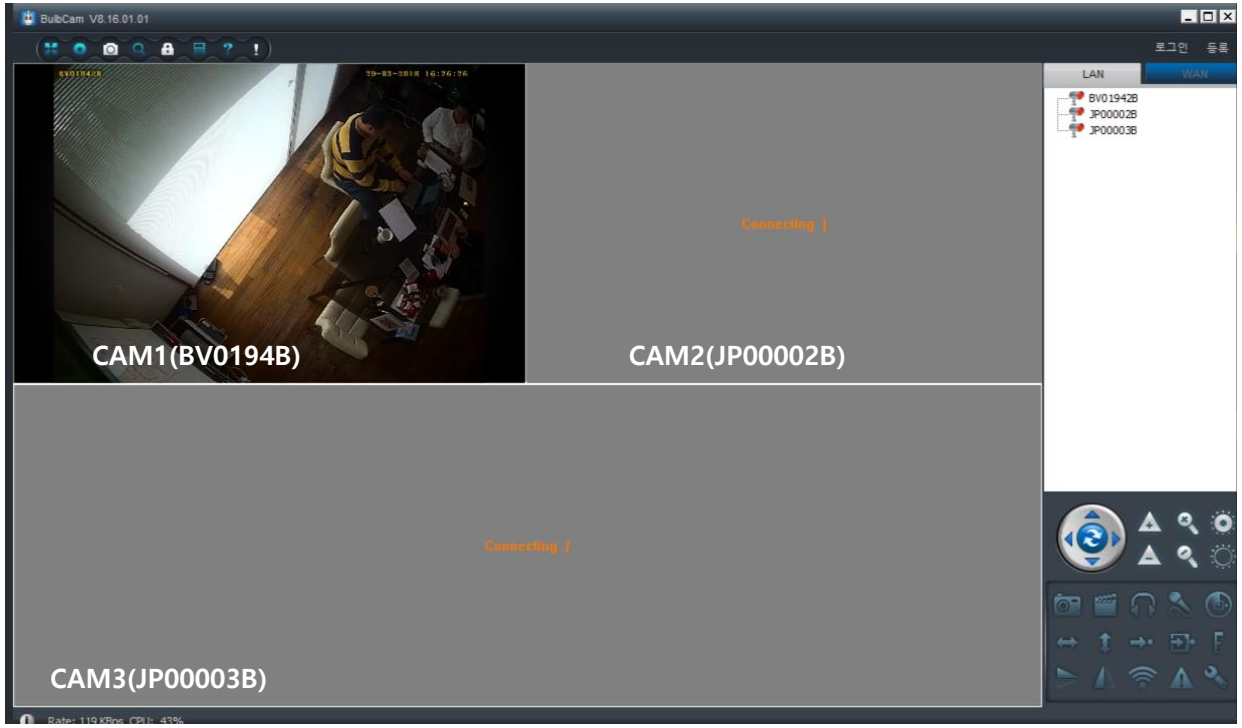
※본 규격은 제품 도입 검토 과정에서 변경 경될수도 있음

IB-175W [White Light]

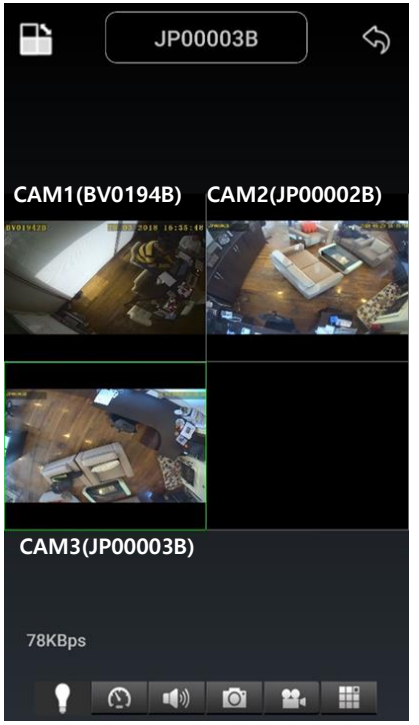
IB-175Y [Warm Light]

Security Camera (TrustSoT IMG 적용)

- 일반 뷰어 : TrustSoT Library 미적용 Camera "CAM1(BV0194B)"의 영상 확인 가능
  TrustSoT Security Camera "CAM2(JP00002B)"와 "CAM3(JP00003B)"의 암호화 영상 확인 불가능
- 전용 뷰어 : TrustSoT Security Camera의 암호화 영상 확인 가능 (복호화)



일반 Viewer (PC)



TrustSoT 전용 Viewer
(Android)

■ TrustSoT IMG 영상암호화 처리 성능 검사 결과

SoT 処理性能検証結果 (SOT처리성능확인결과)

측정①~암호화(SoT G/W 경유)·LOCAL 연결
測定①～暗号化(SoT G/W経由)・ローカル接続

PC時計	動画	差分	差分（平均）
15:50:53.277	15:50:52.119	00:00:01.158	
15:51:54.529	15:51:53.355	00:00:01.174	
15:52:55.836	15:52:54.685	00:00:01.151	00:00:01.172
15:53:58.118	15:53:56.944	00:00:01.174	
15:54:59.808	15:54:58.604	00:00:01.204	

측정②~비암호화(카메라 직접연결)·LOCAL 연결
測定②～暗号化なし(カメラ直接)・ローカル接続

PC時計	動画	差分	差分（平均）
15:58:01.560	15:58:00.387	00:00:01.173	
15:59:01.930	15:59:00.764	00:00:01.166	
16:00:03.291	16:00:02.132	00:00:01.159	00:00:01.166
16:01:09.404	16:01:08.238	00:00:01.166	
16:02:05.961	16:02:04.795	00:00:01.166	

결과 • 監視カメラ映像の暗号化／復号処理による遅延： 6ミリ秒 암/복호화처리 지연 : 6msec

[참고]측정③~암호화(SoT G/W 경유)·INTERNET 연결
【参考】測定③～暗号化(SoT G/W経由)・インターネット経由

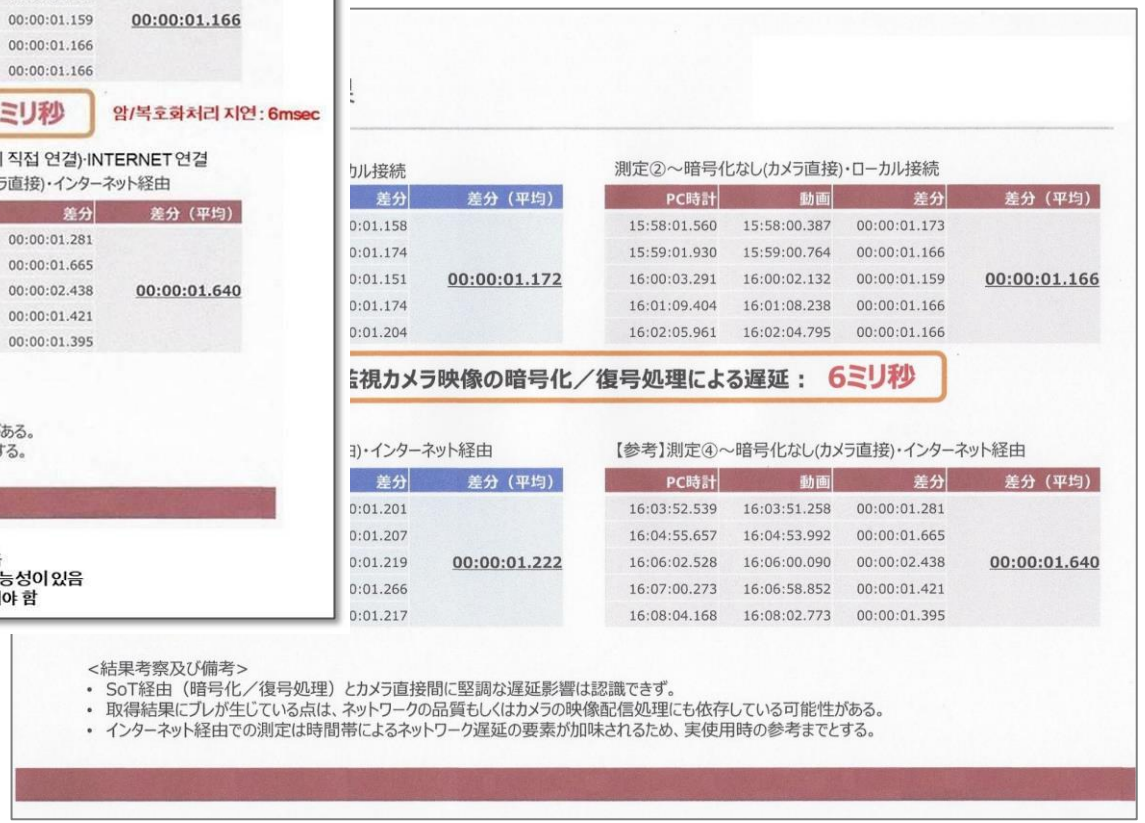
PC時計	動画	差分	差分（平均）
15:45:21.934	15:45:20.733	00:00:01.201	
15:46:23.730	15:46:22.523	00:00:01.207	
15:47:22.212	15:47:20.993	00:00:01.219	00:00:01.222
15:48:22.852	15:48:21.586	00:00:01.266	
15:49:24.069	15:49:22.852	00:00:01.217	

[참고]측정④~비암호화(카메리 직접 연결)·INTERNET 연결
【参考】測定④～暗号化なし(カメラ直接)・インターネット経由

PC時計	動画	差分	差分（平均）
16:03:52.539	16:03:51.258	00:00:01.281	
16:04:55.657	16:04:53.992	00:00:01.665	
16:06:02.528	16:06:00.090	00:00:02.438	00:00:01.640
16:07:00.273	16:06:58.852	00:00:01.421	
16:08:04.168	16:08:02.773	00:00:01.395	

<結果考察及び備考>
- SoT経由（暗号化／復号処理）とカメラ直接間に堅調な遅延影響は認識できず。
- 取得結果にブレが生じている点は、ネットワークの品質もしくはカメラの映像配信処理にも依存している可能性がある。
- インターネット経由での測定は時間帯によるネットワーク遅延の要素が加味されるため、実使用時の参考までとする。

〈결과 고찰 및 비고〉
- SoT 경유(암호화/복호화 처리)와 카메라 직접 연결과의 차이에서 확연한 지연 영향은 확인 할 수 없음
- 검토 결과에 차이가 발생하는 점은, 네트워크의 품질 또는 카메라의 영상 전송 처리에 의한 차이일 가능성이 있음
- 인터넷을 통한 측정시간은 네트워크 지연 요소가 추가되어야 하기 때문에, 실제 사용시에는 참고하여야 함



PanStarEnterprise

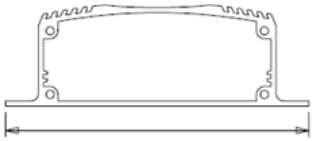
SoTIST

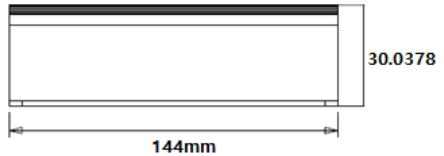
Security LTE Louter (TrustSoT CORE 적용)

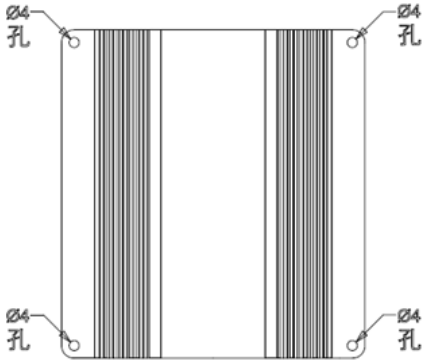
■ H/W	Indoor Type with PSE	Remark
CPU	ARM Cortext-A8 AM3352 (600MHz)	
Memory	512Mbyte	
Flash Memory	eMMC 4Gbyte	
LAN	1 x 10/100 Base-T With 35W PSE	
WAN	1 x 10/100 Base-T	
Wi-Fi	IEEE802.11 a/b/g/n 2.4G/5G Dual Band	
3G/LTE Dual Mode	M.2 Con. Support	
LTE Antenna	2dBi, 1T1R Dipole Antenna	
Status LED	1-LTE, 1-LAN, 1-WAN, 1-PWR, 1-WIFI	
USB 2.0	Host port 1	
Console	RS-232 Lite	RX,TX,GND
Surge Protection	10/700μs / 400W	
ESD Protection	Contact : ±8KV, Air : ±15KV	
Operating Temperature	-40 ~ 85℃	
Operating Humidity	10 ~ 90%	Non-condensing
Input Voltage/Current	DC 24V / 2.5A max Adaptor	
Power Consumption	<10W (35W / PSE 1port)	
Dimension	144mmx125mmx32mm	
Weight	< 380g (< 430g in case PSE)	

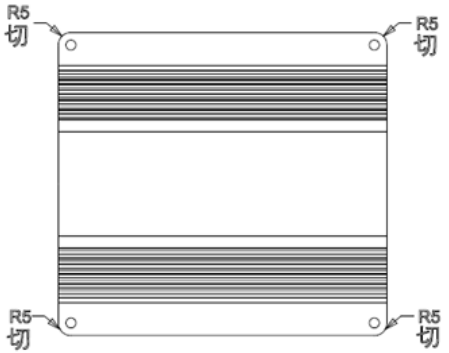
■ S/W	characteristics
VPN	Multi and Bonding Tunnel
	Split Tunneling
	IPsec, IKE Version 1,2
	Transport / Tunnel Mode
	Crypto Algorithms(3DES, AES123/192/256)
	Authentication Algorithms(MD5,SHA1,SHA2)
	Dead Peer Detection
	NAT Traversal
Firewall	Stateful packet Inspection
	Tuples direction/Type
	Static, Dynamic NAT
	Exclude, Double NAT
Network	Route Mode/ Multipath route
	Policy based routing
	QoS / DHCP Server, Relay
	DDNS/ LLDP
IPv6	IPv6 Routing/Firewall/Ipsec
	6 to 4, ISATAP
Management	SNMP v1/2/3
	CLI, Web UI
	Syslog
	System Firmware update function

Security LTE Louter (TrustSoT CORE 적용)



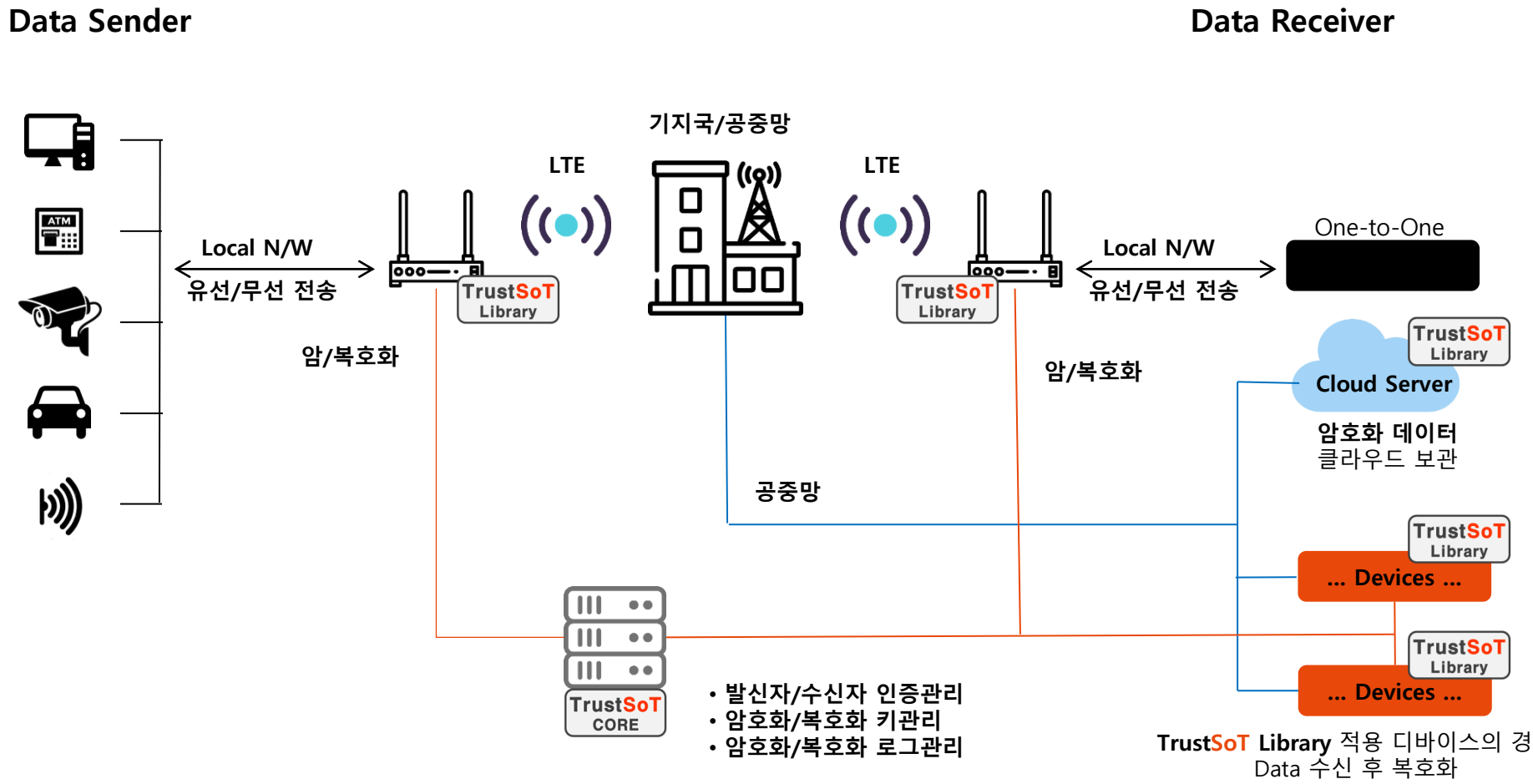






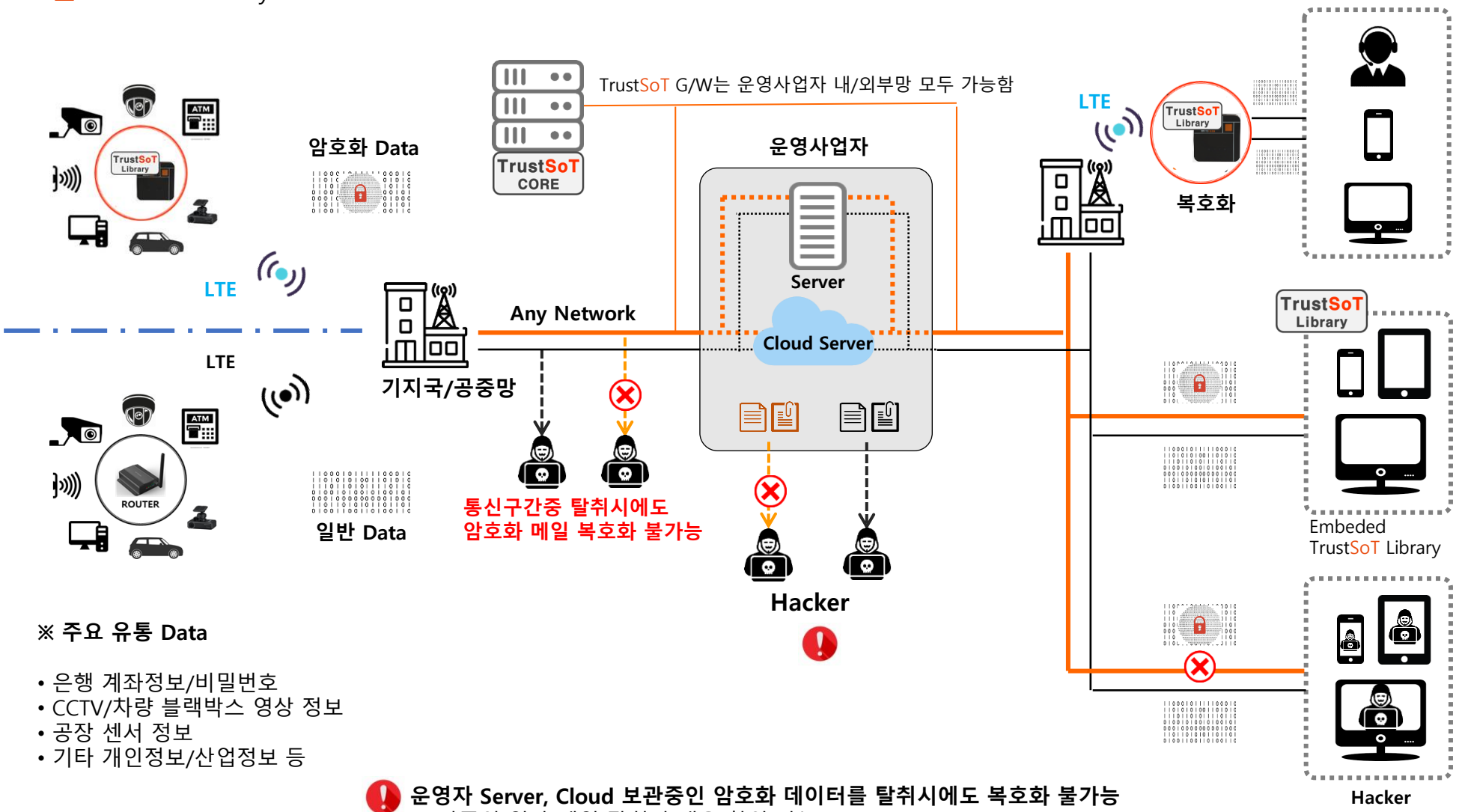
Security LTE Louter (TrustSoT CORE 적용)

■ 모든 Device에서 발생되는 Data를 "TrustSoT LTE Router"를 통해 LTE 전송시,
공중망을 통하거나 Cloud 서비스를 적용하더라도 Data의 암호화 전송 및 보관이 가능합니다.



Security LTE Louter (TrustSoT CORE 적용)

■ TrustSoT Security 4G Louter "Data" Follow



※ 주요 유통 Data

- 은행 계좌정보/비밀번호
- CCTV/차량 블랙박스 영상 정보
- 공장 센서 정보
- 기타 개인정보/산업정보 등

운영자 Server, Cloud 보관중인 암호화 데이터를 탈취시에도 복호화 불가능
(보관중인 일반 메일 탈취시 내용 확인 가능)

SCADA/PLC Demo Sys. (TrustSoT OT/ICS 적용)

TrustSoT SCADA/PLC Demo System S/W구성

구분	Linux	Windows
버전	Kernel 3.X 이상	7 이상
표준 배포본	Ubuntu 18.04, CentOS 7.6	Windows 7, Windows 10
구현 환경	C/C++, Python 3.X, Shell script	C/C++, Python 3.X, C#
라이브러리	GCC 7.1 이상	.NET 4.0 이상
개발 도구	대부분의 개발 도구 지원	Visual studio 2017 이상
데이터베이스	Postgressql 11 이상	Postgresql 11 이상
패키징 방식	자체 실행 및 Docker	자체 실행 및 Docker

TrustSoT SCADA/PLC Demo System H/W구성

구분	최소사양	평균사양	최고사양
CPU	4Core	8Core	8Core
CPU architecture	Intel x86_64	Intel x86_64	Intel Xeon
Memory	8GB	16GB	32GB
SSD	256GB	1TB	1TB x 4EA(RAID)
N/W card	Ethernet 1Gbps 2개 이상	Ethernet 1Gbps 2개 이상	Ethernet 1Gbps 2개 이상
Power Supply	2EA	2EA	2EA
Interface Port	USB 3.0	USB 3.0	USB 3.0
User	less than 1,000	less than 5,000	less than 10,000

SCADA/PLC Demo Sys. (TrustSoT OT/ICS 적용)

■ TrustSoT SCADA/PLC Demo System

구분	구성
CPU	Siemens PLC 315-2 PN/DP
DI	Siemens PLC 321 (32Points)
DO	Siemens PLC 322 (32Points)
DIN Rail	Siemens DIN Rail for CPU 3xx
Power	Weidmuller 100~240V AC
Button	24V DC Input Push Button
Lamp	24V DC Output Lamp

※ Sofrware
Siemens Operation, Engineering and
TrustSoT encrypt communication library

Supply Performance

삼성전자	삼성중공업	삼성SDS	삼성코닝정밀소재
삼성화재	삼성생명	삼성인력개발원	삼성전자서비스
삼성증권	삼성물산	삼성디스플레이	삼성코닝어드밴스드글라스

하나은행	하나캐피탈	하나금융투자
하나카드	하나저축은행	하나금융지주
하나생명	하나자산신탁	하나멤버스

중앙보훈병원	대전보훈병원	한국보훈복지의료공단
인천보훈병원	광주보훈병원	
부산보훈병원	대구보훈병원	