

모빌리티 사이버보안의 심장: **KMS (Key Management System)**

자동차 사이버보안 규제 시대, 왜 키 관리가 필수인가?

페스카로 구성서 CSO

November 2025

Table of Contents

1. 왜 지금 KMS인가?	8
2. KMS란 무엇인가?	21
3. 그럼 KMS를 위해 무엇을?	28
4. KMS 이렇게...	36

1. 왜 지금 KMS인가?

1. 왜 지금 KMS인가? (1/12)



1. 왜 지금 KMS인가? (2/12)

글로벌 규제 준수 필수 요소 (국가별 규제 & ISO/SAE 21434)

	2022	2023	2024	2025	2026	2027	2028	2029
미국 (현재 규제 없음)	NHTSA(도로교통안전국) 규정 권장 / 자기 인증							
유럽연합 (UN R155)	신 차종 대상('22.7)			모든 신차 대상('24.7)				
일본 (UN R155)	신 차종 대상('22.7)			모든 신차 대상('24.7)				
한국 (자동차관리법)					신 차종 대상('25.8)		모든 신차 대상('27.8)	
중국 (GB 44495-2024)					신 차종 대상('26.1)		모든 신차 대상('28.1)	
인도 (AIS-189)						신 차종 대상 ('27.10 예정)		모든 신차 대상 ('28.10 예정)

1. 왜 지금 KMS인가? (3/12)

사이버보안의 세가지 달성요소 : CIA Triad



기밀성 (Confidentiality)

viewed only
by authorized parties



무결성 (Integrity)

modified only
by authorized parties



가용성 (Availability)

used only
by authorized parties

1. 왜 지금 KMS인가? (4/12)

사이버보안의 세가지 달성요소 : CIA Triad



기밀성 (Confidentiality)

viewed only
by authorized parties

차량의 기밀성은 단순한 데이터 보호를 넘어서 **비인가자의 정보 접근 차단**

- ✓ **데이터 보호** : 운전자 개인정보(예 : 주소록, 위치 기록, 결제 정보 보호 등)
- ✓ **IP 보호** : 차량의 고유한 주행 알고리즘, SW/FW 등 지적 재산 보호
- ✓ **통신 보호** : 차량 내외 통신 내용의 도청(Eavesdropping) 방지

1. 왜 지금 KMS인가? (5/12)

사이버보안의 세가지 달성요소 : CIA Triad



무결성 (Integrity)

modified only
by authorized parties

차량이 '진짜' 제조사의 명령대로 움직인다는 보증, **비인가자의 조작 방지**

- ✓ **소프트웨어 무결성** : (Secure Boot) ECU가 신뢰할 수 있는 SW(예 : 부트로더)로만 부팅되도록 보장
- ✓ **메시지 무결성** : (SecOC) 신뢰할 수 있는 메시지(CAN/이더넷 등)만 처리하도록 보장, 메시지 위조 방지
- ✓ **데이터 무결성** : (Secure Flash): 제조사의 정식 전자 서명 받은 SW/FW만 차량(제어기) 설치 보장

1. 왜 지금 KMS인가? (6/12)

사이버보안의 세가지 달성요소 : CIA Triad



가용성 (Availability)

used only
by authorized parties

차량이 필요할 때 동작하는 것을 보장, 외부 공격에 따른 오동작 방지

- ✓ **기능 연속성** : 제동, 조향, ADAS 등 핵심 안전 기능이 어떠한 상황에서도 작동 보장
- ✓ **DoS 공격 방어** : 네트워크(CAN, 이더넷)가 마비되어 ECU 간 통신이 두절되는 것을 방지
- ✓ **서비스 접근성** : 필요시 원격 제어(시동)나 OTA 업데이트의 실패 방지

1. 왜 지금 KMS인가? (7/12)

사이버보안의 세가지 달성요소 : CIA Triad

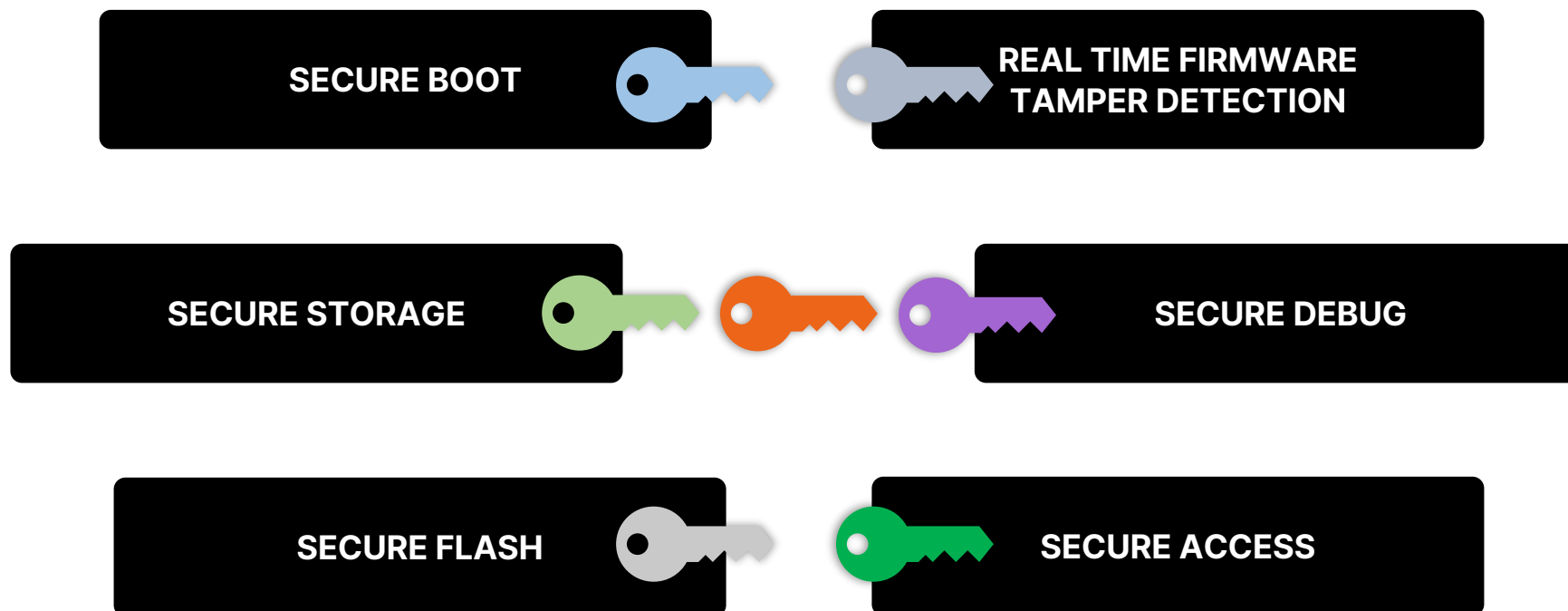


CIA 달성의 핵심 암호화 키 (Key)



1. 왜 지금 KMS인가? (8/12)

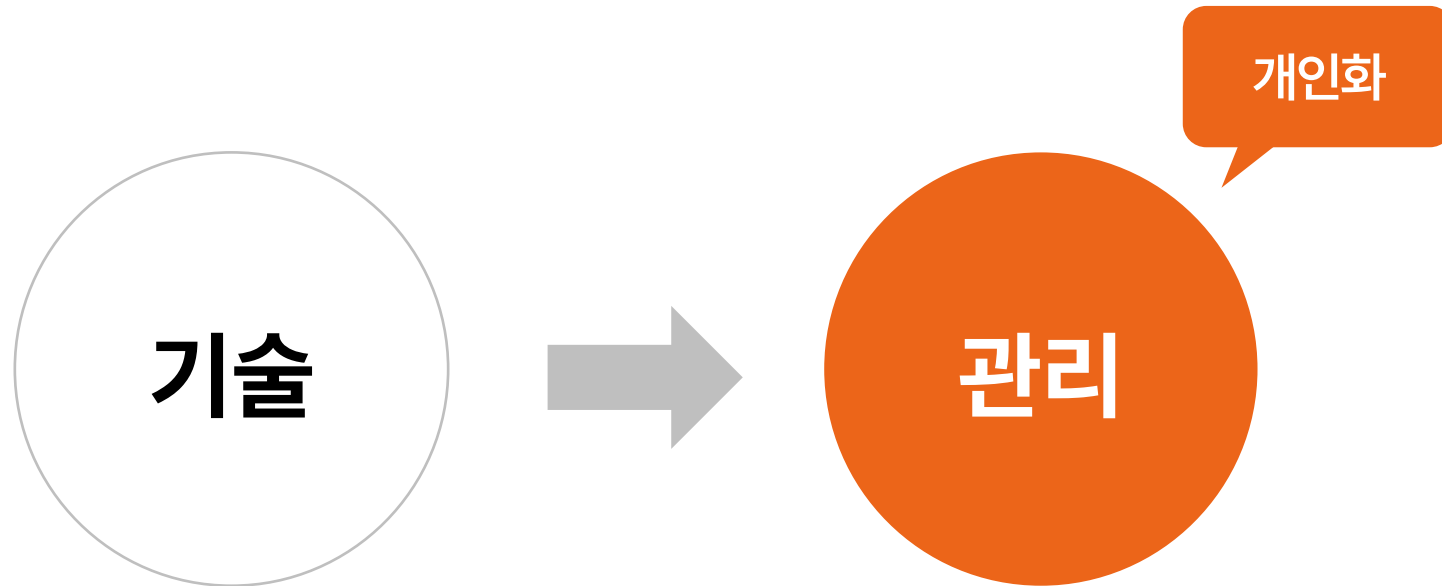
사이버보안 요구사항 모두 암호화 key와 관련



1. 왜 지금 KMS인가? (9/12)

사이버보안은 100% 완벽할 수 없다.

근본적 방어 보다는 후속 피해 최소화 및 빠른 대응으로 변화



1. 왜 지금 KMS인가? (10/12)

그런데 키 관리가 왜 지옥(Hell)인가?

혹시 우리도 이런 문제가?

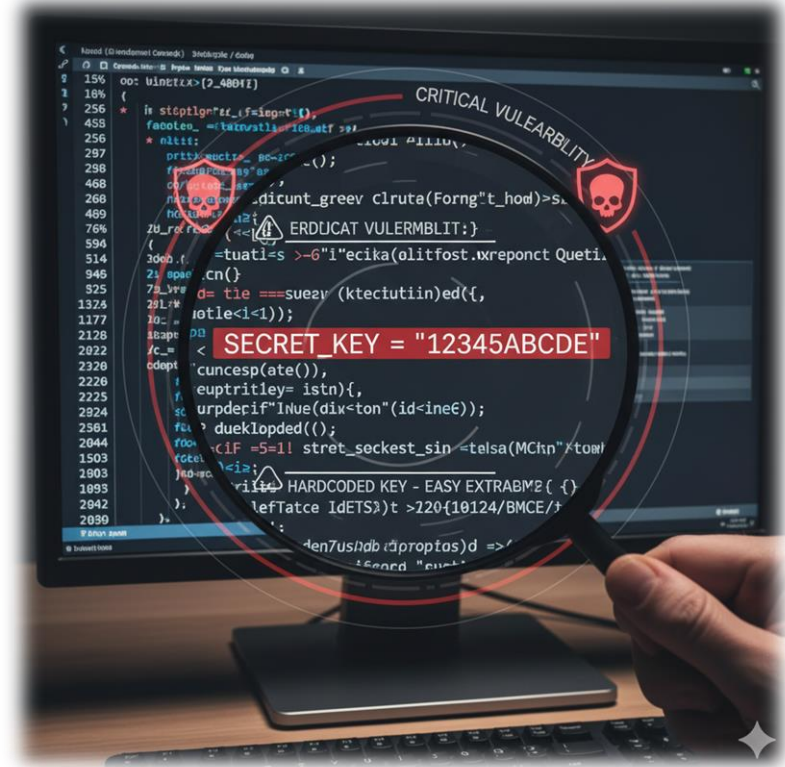


단일 장애점 (SPOF)

키 관리에 실패하면,
수천 억 원의 보안 투자가 무용지물이 됩니다.

1. 왜 지금 KMS인가? (11/12)

혹시 우리는?



1. 왜 지금 KMS인가? (12/12)

규제나 표준에서도...

UN R155

7.2.2.2 The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and **mitigations listed in Annex 5**. This shall include:....

Part B - M3. Protection of secrets (e.g. keys, credentials, etc.) held on backend servers.

Part D - M5. To ensure secure storage of parameters or **secrets (e.g. keys, configuration files, etc.)**.

M6. To protect **secrets (e.g. keys, credentials, etc.)** from being read-out from the vehicle.

ISO/SAE 21434

[11.4.6] Implementation of cryptographic algorithms

"If cryptographic algorithms are implemented, ... their implementation shall adhere to current **security best practices and guidelines**..."

[11.4.7] Secure storage of data and parameters

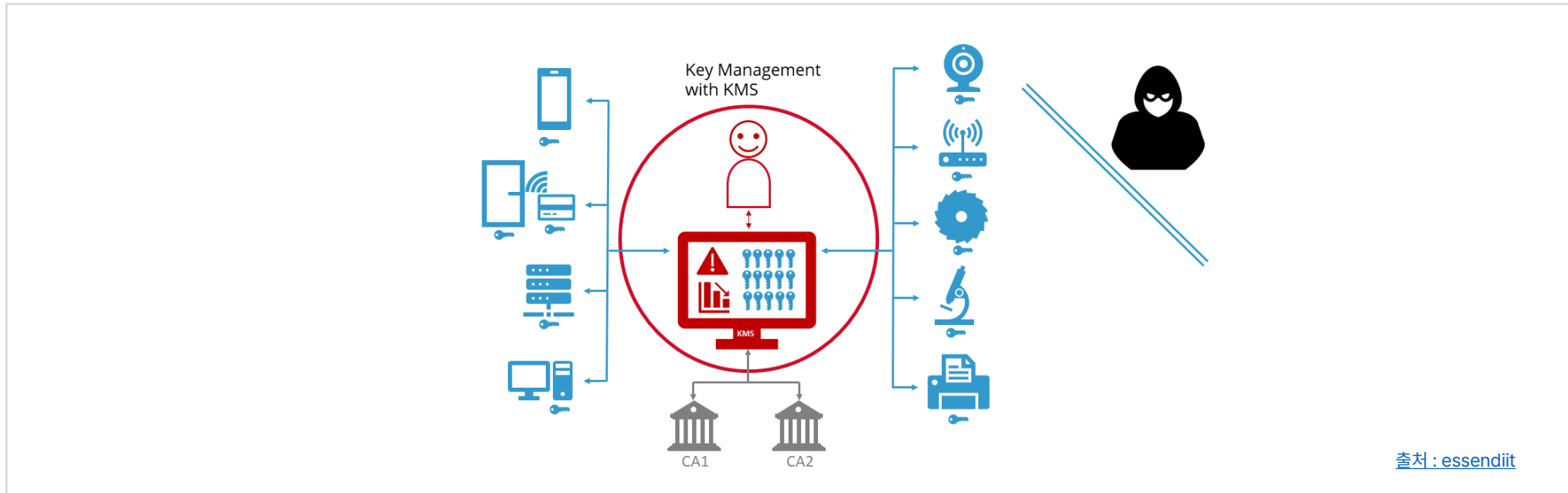
"If data and **parameters** are stored, ... their storage shall be implemented according to the **cybersecurity specifications**..."

2. KMS란 무엇인가?

2. KMS란 무엇인가? (1/6)

KMS(Key Management System) : 보안 자산 관리

자동차 생애 주기 전반에 걸쳐 보안자산의 생성, 저장, 배포, 폐기/갱신 등을 안전하고 효과적으로 관리



2. KMS란 무엇인가? (2/6)

키 관리의 전 과정 : 5단계 생애 주기 (Key Lifecycle)

1. Generation, 안전한 생성 : 누가 봐도 신뢰할 수 있는 키

2. Inject/Provision, 안전한 주입/배포 : 필요한 곳에, 필요한 키만, 안전하게 전달

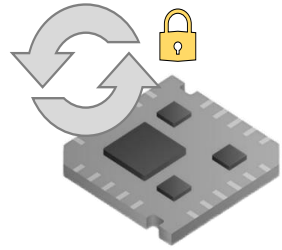
3. Storage, 안전한 저장 : ECU 내부에서 키를 안전하게 저장 (HSM)

4. Usage, 안전한 사용 : 신뢰할 수 있는 환경에서의 사용

5. Rotation/Destruction, 안전하고 신속한 교체/폐기 : *"가장 중요한 기능!"*

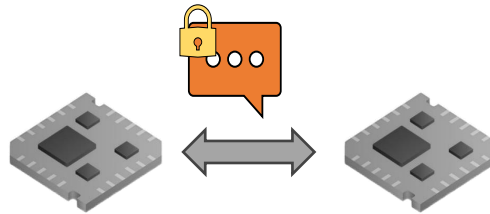
2. KMS란 무엇인가? (3/6)

KMS로 보안 기능에 사용되는 보안자산(암호 키, 서명 키, PW, 인증서 등) 관리



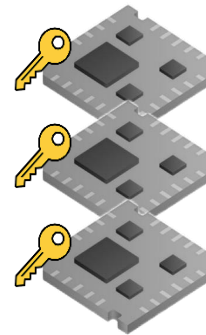
SecureFlash 2.0

전자서명 및 암호화 통해
인증된 펌웨어 프로그래밍 허용하는 기능



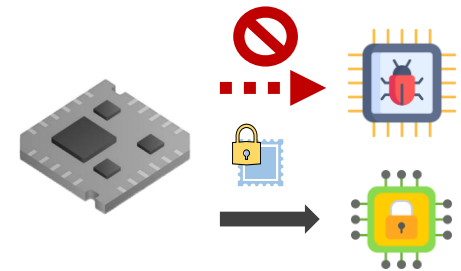
SecOC

KMS에서 발급 KEY 이용하여
MAC 생성 및 메시지 적용



SecureDebug

ECU 접근 가능한 개별 패스워드 사용



Secure Boot

무결성이 보장된 펌웨어만 부팅 허용

2. KMS란 무엇인가? (4/6)

KMS, 보안 리스크를 획기적으로 낮추는 방안

사례	KMS 도입 전의 "혼돈" (The Problem)	KMS 도입 후의 "질서" (The KMS Solution)	핵심 비즈니스 가치
Secure Flash	해커가 위조된 펌웨어 배포. 제어권 탈취 위험	[비대칭 키 관리] 안전한 환경에서의 펌웨어 서명(Private Key) 그리고 검증(Public Key)	안전한 기능 업데이트, 대규모 리콜 비용 절감
SecOC	CAN 통신 스푸핑(Spoofing). 가짜 제어 신호로 인한 사고 위험	[대칭 키 관리] CMAC 기반 메시지 인증. 키 자동 교체 (Rotation)	차량 내부 제어 신뢰성 확보 (생명 안전)
Secure Debug	디버그 포트를 통한 펌웨어 무단 추출. IP 탈취	[인증서/패스워드 관리] Challenge-Response 기반 차등적 접근 제어	정비/개발 효율성(Enabler) + 핵심 IP(펌웨어) 보호

2. KMS란 무엇인가? (5/6)

KMS, 규제 준수 (The "Stick") - UN R155/R156

" 귀사의 공급망(Supply Chain) 리스크는 어떻게 관리합니까? "

" 저희는 Tier 1 업체에 보안 가이드를 배포했고 주기적으로 점검합니다. "

OR



" 저희는 KMS를 통해 Tier 1에 키를 배포하는 정책을 강제합니다.
키의 하드코딩은 불가능하며, 모든 키의 배포와 사용 이력이 추적됩니다. "

2. KMS란 무엇인가? (6/6)

KMS, 규제 준수 (The "Stick") - UN R155/R156

" 귀사의 OTA 업데이트 프로세스가 안전하다는 것을 어떻게 증명합니까? "

" 저희는 펌웨어에 서명을 하고 있습니다. " (증적: 엑셀 시트, 내부 지침서)

OR

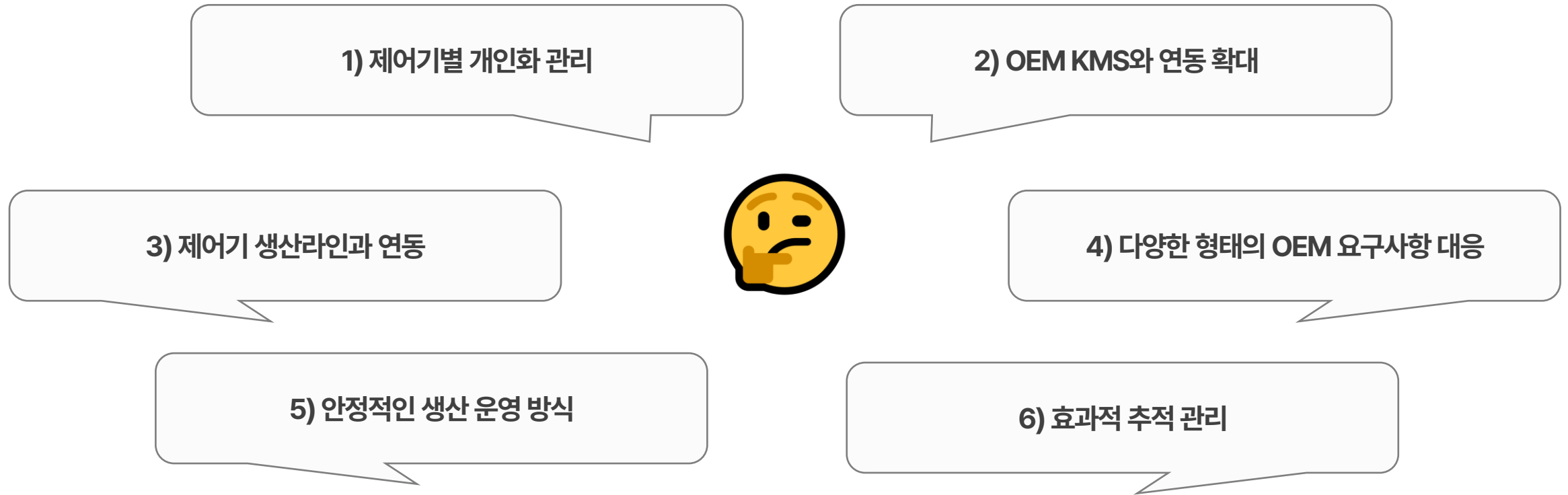


" 여기 KMS 감사 로그가 있습니다. 이 로그는 2025년 10월 5일 15:03분에, 'A' 펌웨어가 HSM 내부의 'Private Key-007'로 서명되었으며, 해당 키는 이러한 정책 하에 관리되고 있음을 증명합니다. "

3. 그럼 KMS를 위해 무엇을?

3. 그럼 KMS를 위해 무엇을? (1/7)

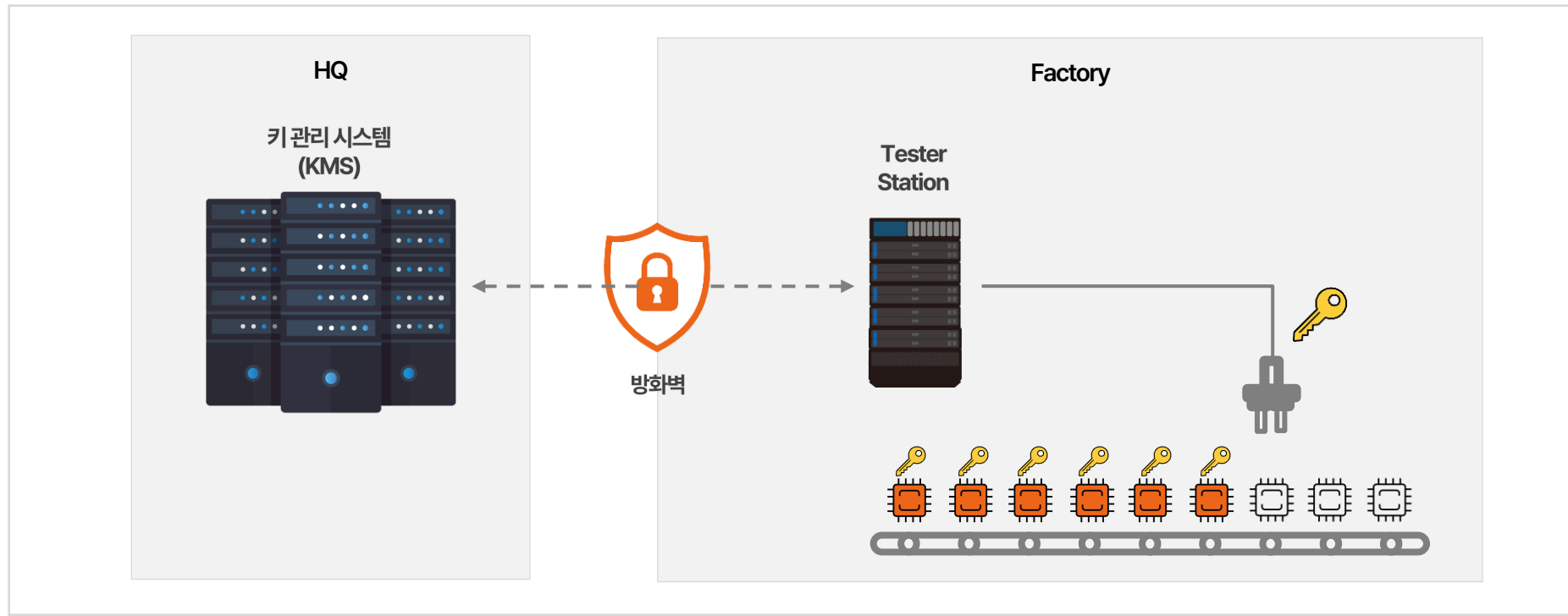
최적의 KMS 구축을 위한 6개의 고려 사항



3. 그럼 KMS를 위해 무엇을? (2/7)

1) 제어기별 개인화 관리

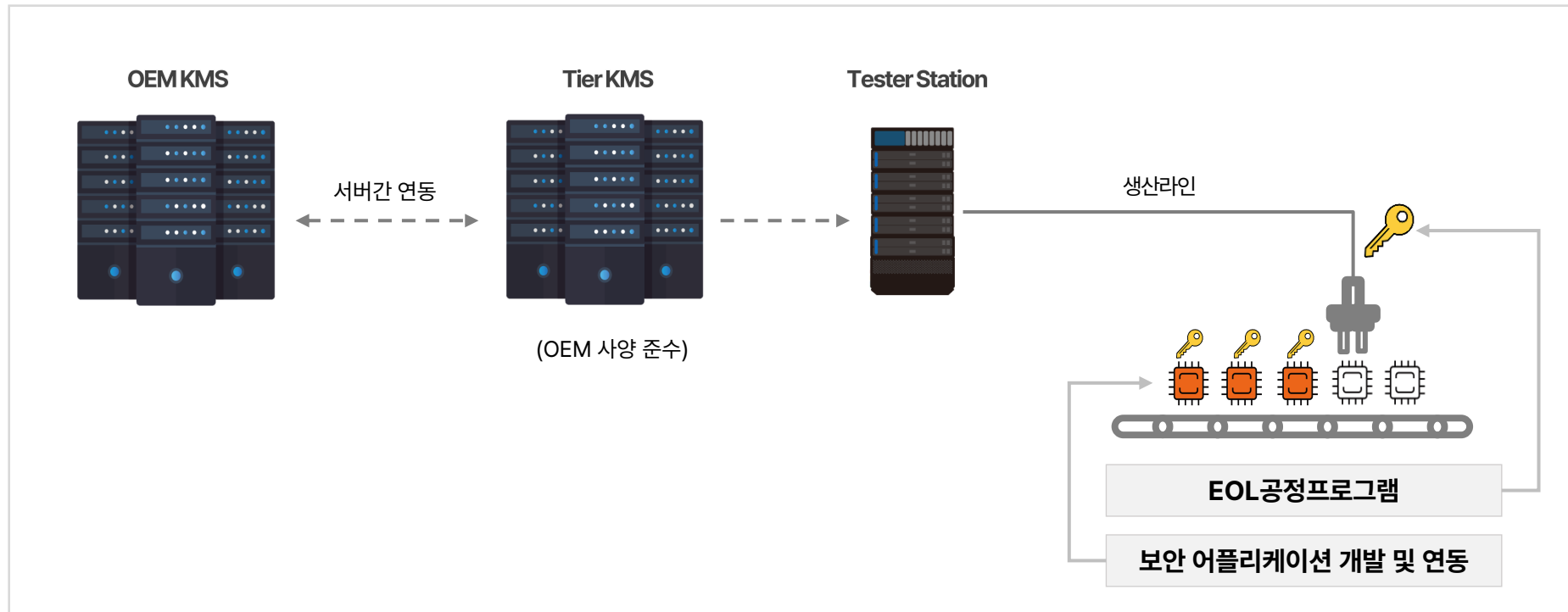
제어기 생산 시 개인화된 암호키 및 패스워드 주입 필요



3. 그럼 KMS를 위해 무엇을? (3/7)

2) OEM KMS와 연동 확대

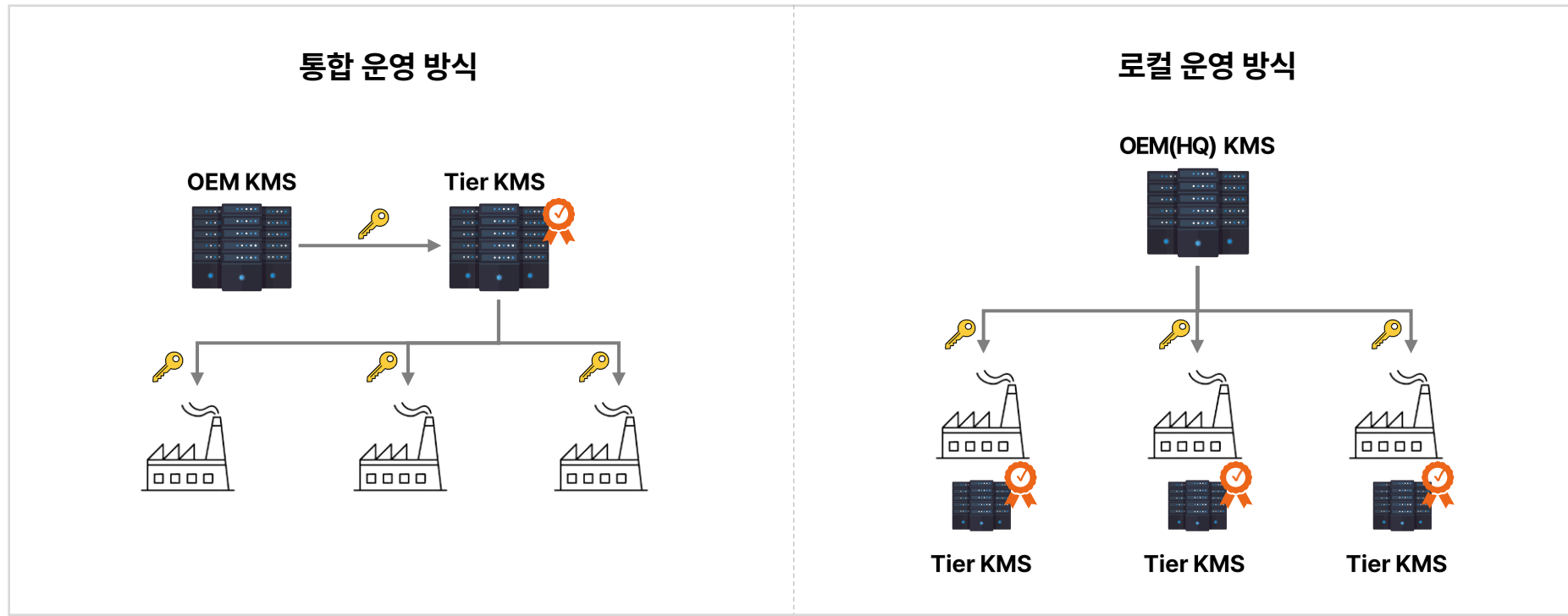
OEM이 제어기 보안 자산을 관리하는 경우 OEM KMS와 연동 필요



3. 그럼 KMS를 위해 무엇을? (4/7)

3) 제어기 생산라인과 연동

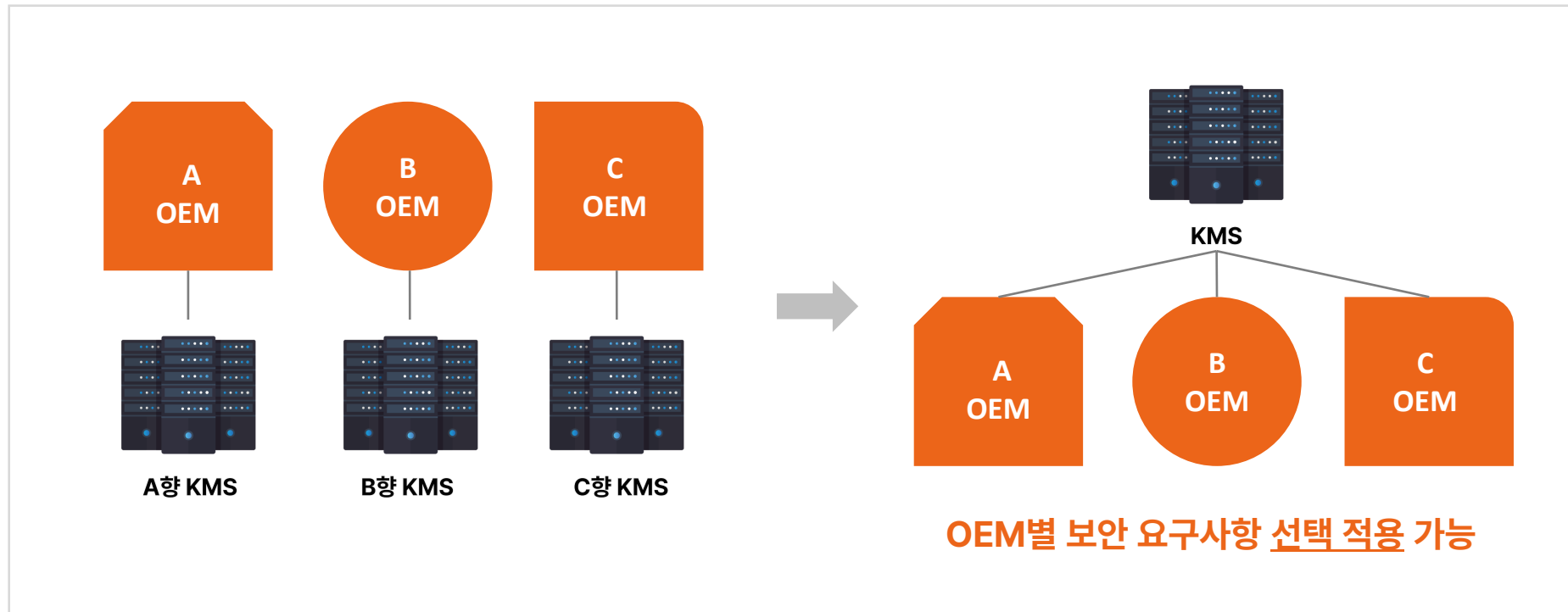
보안자산의 생성 방식, 생산라인 특성(예, 운영 방식, 위치 등)을 고려한 효과적인 연동 방식 구성 필요



3. 그럼 KMS를 위해 무엇을? (5/7)

4) 다양한 형태의 OEM 요구사항 대응

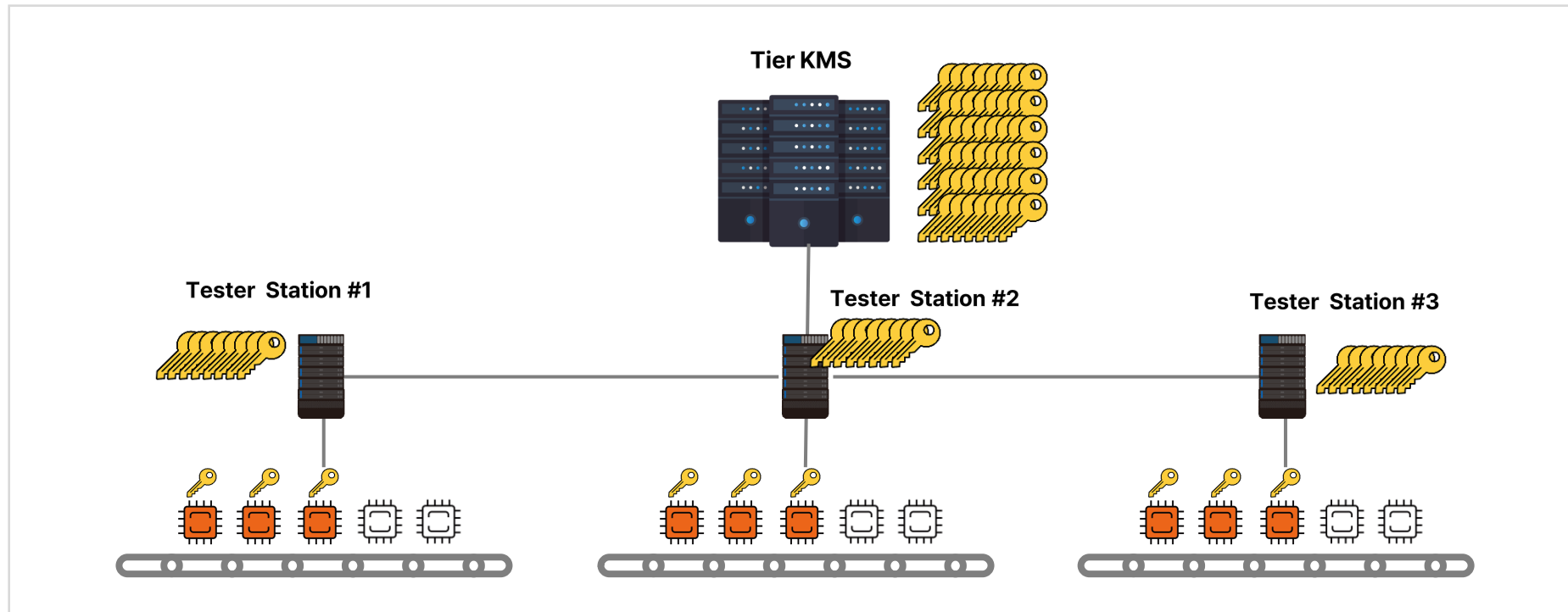
효과적으로 대응하기 위한 운영 방안 모색 필요



3. 그럼 KMS를 위해 무엇을? (6/7)

5) 안정적인 생산 운영 방식

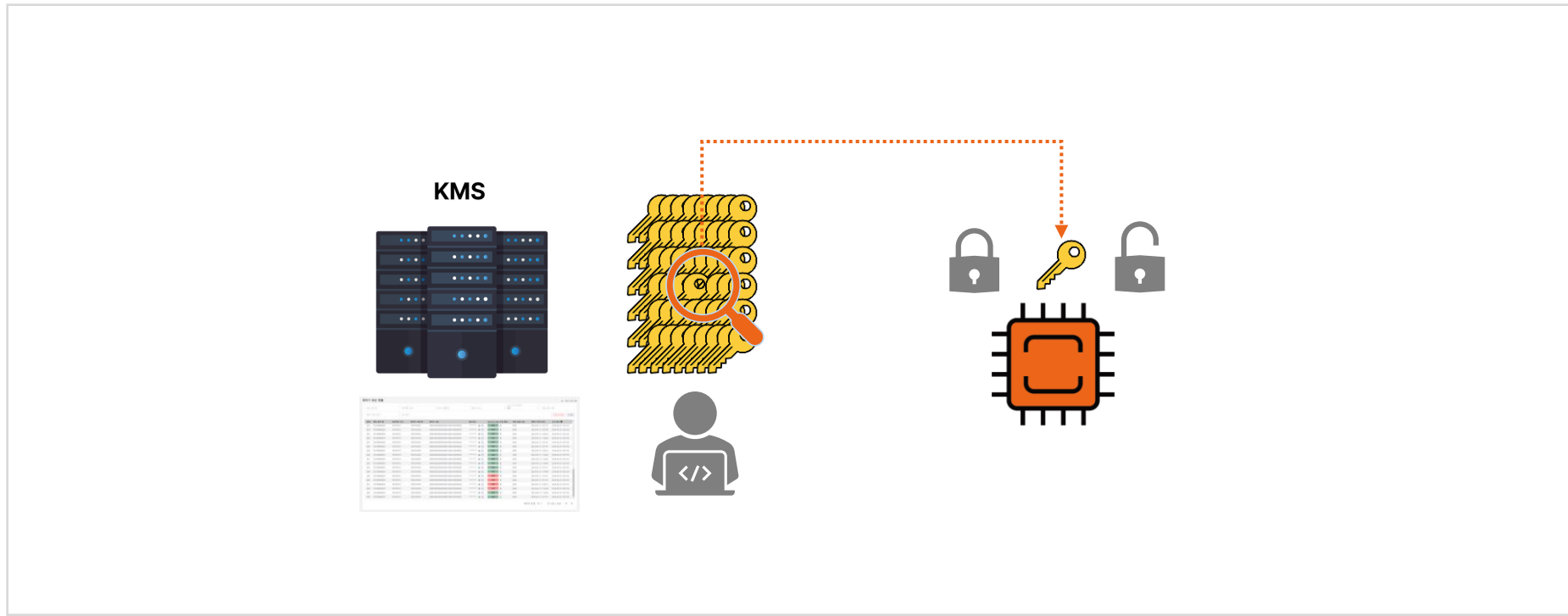
생산 과정에서의 Side-Effect에 의한 Risk 최소화 방안 수립 필요



3. 그럼 KMS를 위해 무엇을? (7/7)

6) 효과적 추적 관리

개별 제어기에 주입된 보안자산을 추적 관리하여 필요 시 신속한 대응 필요



4. KMS 어떻게?

4. KMS 어떻게? (1/7)

KMS 관련 역할 및 상호 관리 구조

OEM

- 보안 표준 정의 (KDF 알고리즘 및 파라미터)
- 인증서 체계 제공 (Root CA, IMI CA, IMA CA 등)
- 코드 서명 및 키 페어 관리 (Code Signing Private/Public Key)
- 최종 차량 점검 (In-Vehicle Provisioning 절차 주도)

Tier

- KMS 구출 및 운영 (Master ECU Key, Supplier ECU Symmetric Identity Key)
- 키/인증서 초기 주입 (CA 인증서, Code Signing Public Key)
- 디바이스 고유키 생성 (Device Identity Private Key)
- 보안 설정 및 잠금 (JTAG 및 HSM Configuration Lock 루틴 실행)

Service Provider

- PKI 인증서 체계 발급 (PKI 체계, 진단용 인증서)
- ADS-ECU 상호 인증 (UDS Service 0x29 양방향 인증, ECU 진단)
- 운영 중 키 업데이트 (SecOC Key 업데이트, IVP 요청)
- ADS 고유 통신 보안 (ADS-ECU Specific Key)

4. KMS 어떻게? (2/7)

현실적 어려움

구 분	내 용
1. 조직적 문제 (Governance Issue)	KMS 전담 조직 부재 및 거버넌스 모호 : 연구소/생산/IT팀 간 역할 분담 불명확으로 인한 키 관리 책임 공백 발생
2. 운영 변화의 어려움 (Operational Transition)	생산라인 변경 및 차질 우려 : 기존 생산 라인 수정 및 장비 교체 부담으로 KMS 도입 지연 및 소극적 적용
3. 프로세스 표준화 미흡 (Process Standardization)	End-to-End 관리 절차 미표준화 : 키 주입부터 운영까지의 프로세스 단절 및 담당자 교체 시 관리 누락 위험
4. OEM 요구사항 대응 어려움 (OEM Compliance)	OEM별 요구사항 상이 및 커스터마이징 부담 : 매번 새로운 보안 정책 및 복잡한 검증 항목 대응에 자원 집중
5. 보안·추적성 미흡 (Security & Traceability)	운영 보안 검증 체계 미비 : 인증서/키 백업 안전성 미확보 및 키 주입/사용 로그 추적성 부족

4. KMS 어떻게? (3/7)

현실적 어려움 – KMS 도입으로 해결?

구 분	내 용	KMS 도입을 통한 해결 방안
1. 조직적 문제 (Governance Issue)	KMS 전담 조직 부재 및 거버넌스 모호	키 관리 거버넌스 프레임워크 제공
2. 운영 변화의 어려움 (Operational Transition)	생산라인 변경 및 차질 우려	생산라인 비침습(Non-Intrusive) 통합 솔루션
3. 프로세스 표준화 미흡 (Process Standardization)	End-to-End 관리 절차 미표준화	시스템 기반 프로세스 표준화
4. OEM 요구사항 대응 어려움 (OEM Compliance)	OEM별 요구사항 상이 및 커스터마이징 부담	기능 모듈화 및 확장 가능 인터페이스
5. 보안·추적성 미흡 (Security & Traceability)	운영 보안 검증 체계 미비	Key 보안 검증 체계 및 로그 기반 추적성 확보

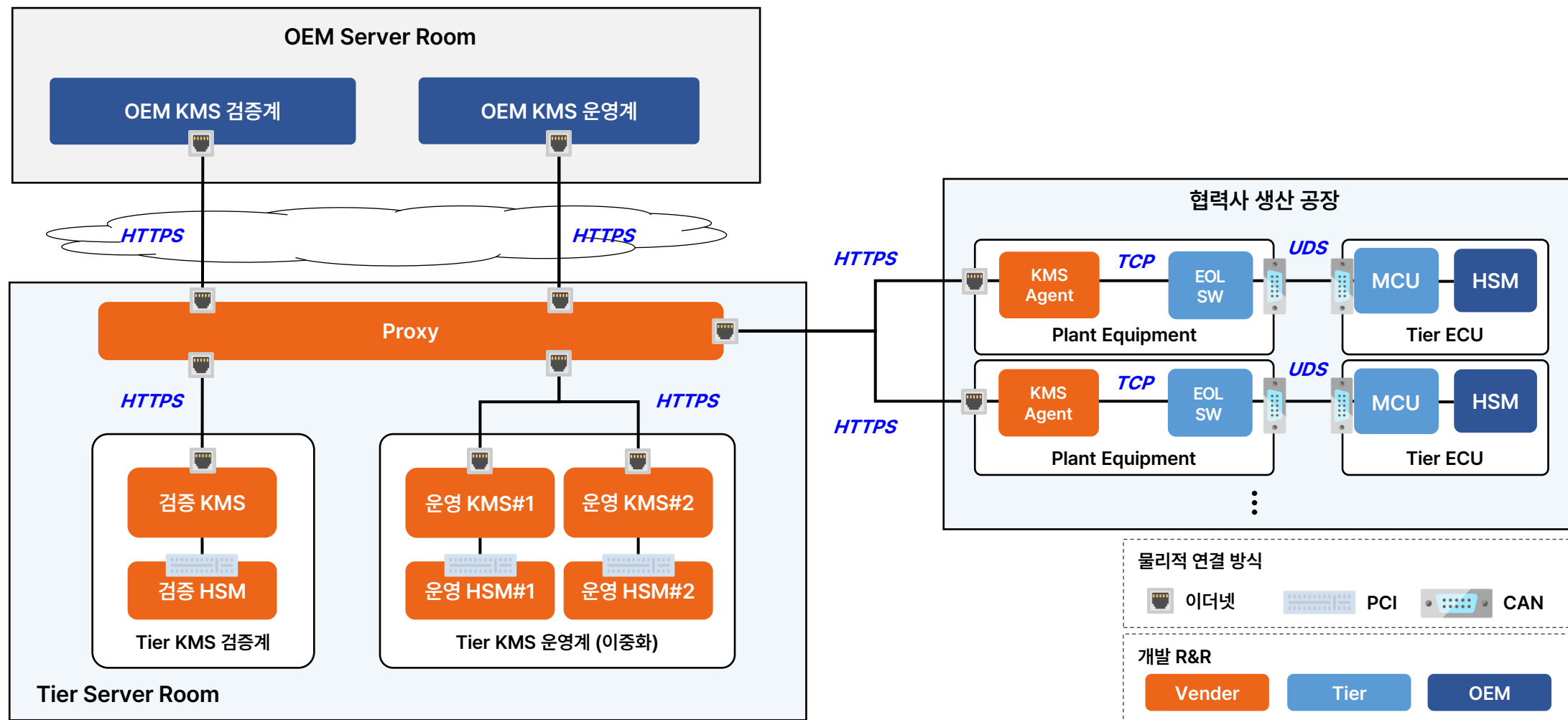
4. KMS 어떻게? (4/7)

• 구축사례 – Batch Update 방식 (1/4)

항목	상세 항목	Tier	KMS 개발사	비고
KMS Server	- 시스템 관리 기능 - 프로젝트 관리 기능 - 제어기 모델 관리 기능 - 보안 정책 관리 기능 - 생산 설비 관리 및 연동 기능 - OEM KMS 연동 기능 - Secure Debug 관리 기능 - SecOC 관리 기능 - Secure Authentication 관리 기능 (인증서, Optional) - Secure Flash 관리 기능 (전자서명, Optional)		●	
KMS Agent	- 프로젝트-제어기 모델 관리 기능 - KMS 연동 기능 - Legacy EOL Program 연동 기능 - SHE Spec. 기반 키 업데이트 유효성 검사 기능		●	
EOL Program	- KMS Agent 연동 기능 [진단] 암호 키 및 인증서, 패스워드 주입 기능	●		
제어기 (MCU)	[진단] 암호 키 및 인증서, 패스워드 수신 기능 [진단] In Vehicle Provisioning 기능	●		
	[보안] HSM 내 암호 키 및 인증서, 패스워드 저장 기능 [보안] HSM 기반 보안 어플리케이션 개발 * 보안 어플리케이션: Secure Authentication, SecOC, Secure Debug, Secure Flash 2.0, Secure Boot		●	

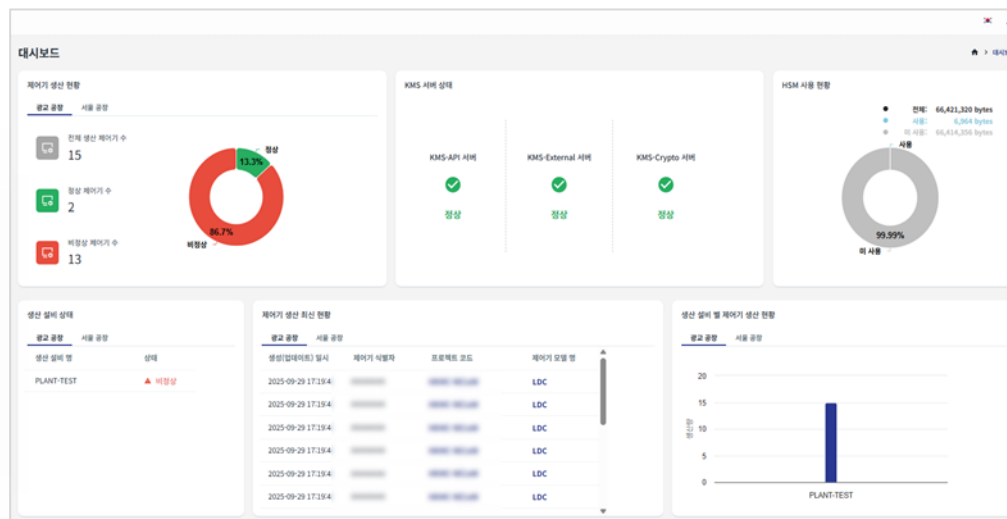
4. KMS 어떻게? (5/7)

- 구축사례 - Batch Update 방식 (2/4)



- 구축사례 - Batch Update 방식 (3/4)

KMS Server

[illegible]

생산 설비 관리

[홈](#) >
 [시스템 정보](#) >
 생산 설비 관리

번호	생산 장비 명	생산 장비 구분	공정	비고	장비의 상태	
1	PLANT TEST	PLANT-COMMON-UNIQUE-001	금강 공단	-	사용중	수정 <input checked="" type="button" value="제거하기 요청 목록"/> <input checked="" type="button" value="T13 인출서 출력"/>
2	PLANT01	PLANT-01-VALUE	서울 공장	-	사용중	수정 <input checked="" type="button" value="제거하기 요청 목록"/> <input checked="" type="button" value="T13 인출서 출력"/>

페이지당 열 50 1-2/2 < >

[illegible][illegible]

4. KMS 어떻게? (7/7)

- 구축사례 – Batch Update 방식 (4/4)

KMS Agent



KMS Plant Program (v1.0.0)

Program Settings Help

DashBoard

Batch Result Registration Status

Name	Total Count (Success/Fail/Discarded)	Uploaded Time	Registration Result	Retry Count

Dataset Usage

Name	Status

Schedule Monitor

Next Synchronization: Remain Time: Manual Sync:

Log

Tier KMS Log

Legacy Log

Program Log

```
[2025-10-17 19:34:46.662] All schedule item registered successfully
[2025-10-17 19:34:46.666] Scheduler started successfully
[2025-10-17 19:34:46.685] TCP server started on port 8080
[2025-10-17 19:34:46.690] Key injection service started successfully
[2025-10-17 19:34:46.730] UI Dashboard initialization completed successfully
[2025-10-17 19:34:46.735] Application initialization completed successfully
```

● Tier Kms ● Legacy

General Settings

Program Tier KMS TCP/IP

Client ID Create Copy

Partner Code

Display Option ☒ Noraml ☐ Minimize ☐ Tray

Legacy Project Code Length

Legacy ECU Model Length

HW Part Number Length

ECU Serial Number Length

Save Close

Database Settings

Mapping Table <Tier KMS-Legacy>

Database Detail	Tier KMS	Legacy
Name	Batch Request Size	Sync Time

Add Database

Tier KMS_Project Code

Tier KMS_ECU Model

Tier Kms_HW Part Number(8)

Legacy_Project Code(5)

Legacy_ECU Model(4)

Legacy_HW Part Number(8)

Batch Request Size (Max:1000)

Sync Time(HH:MM)

Sync Interval(Hrs)

OK Close

페스카로, 글로벌 자동차 사이버보안 컴플라이언스 전문가

높은 기술력 + 폭넓은 성공사례 + 독보적 지식베이스 기반 국제적 신뢰도 ▲

CIA를 달성을
위한 핵심
암호화 Key

복잡하고 어려운
암호화 Key 관리
KMS가 해답

우리에 맞는 KMS선택
전문가와의
협업 필요



경청해 주셔서 감사합니다.

사이버보안 고민이 있다면 편하게 문의해 주세요. 😊

(sales@fescaro.com)