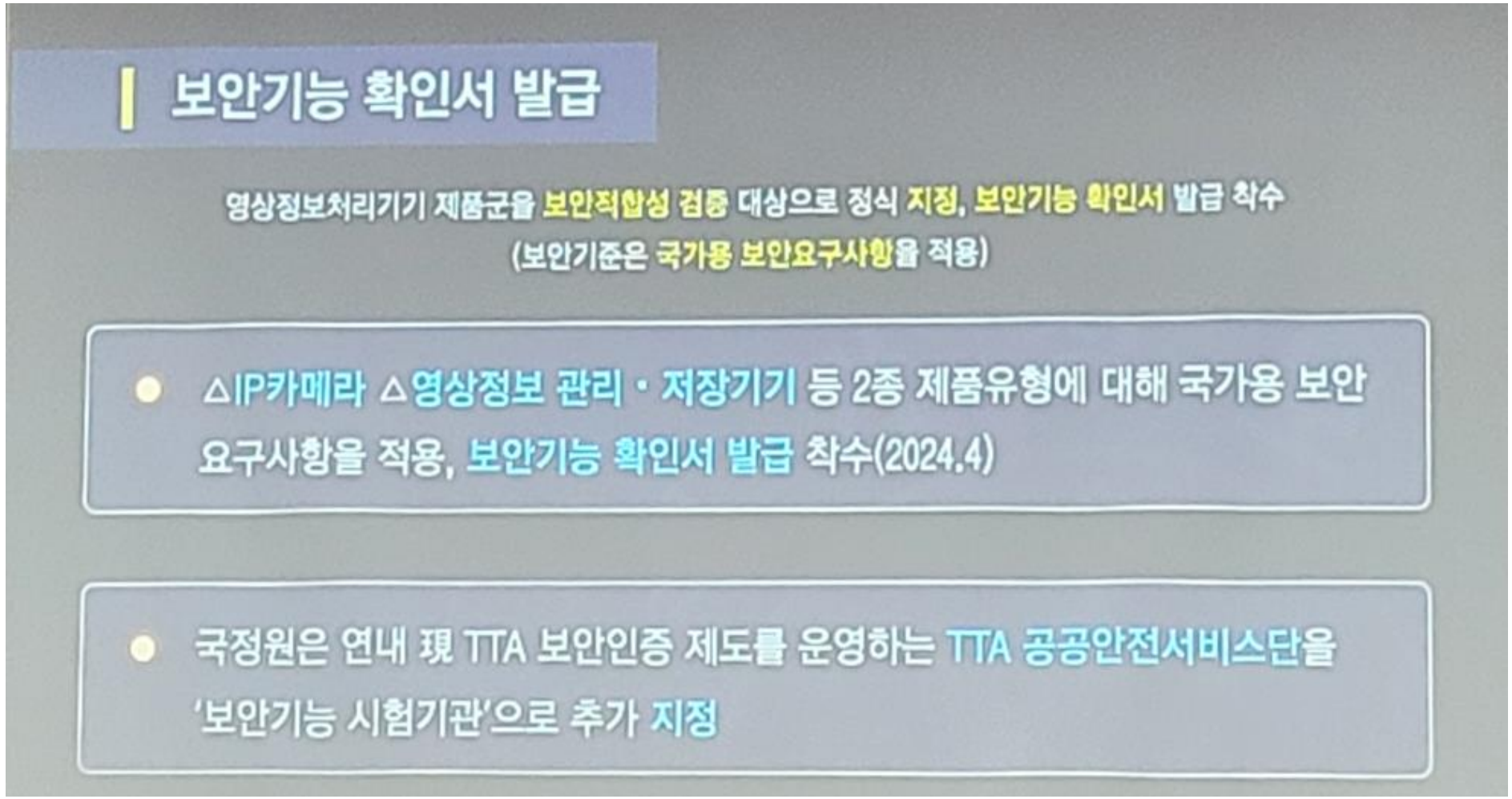
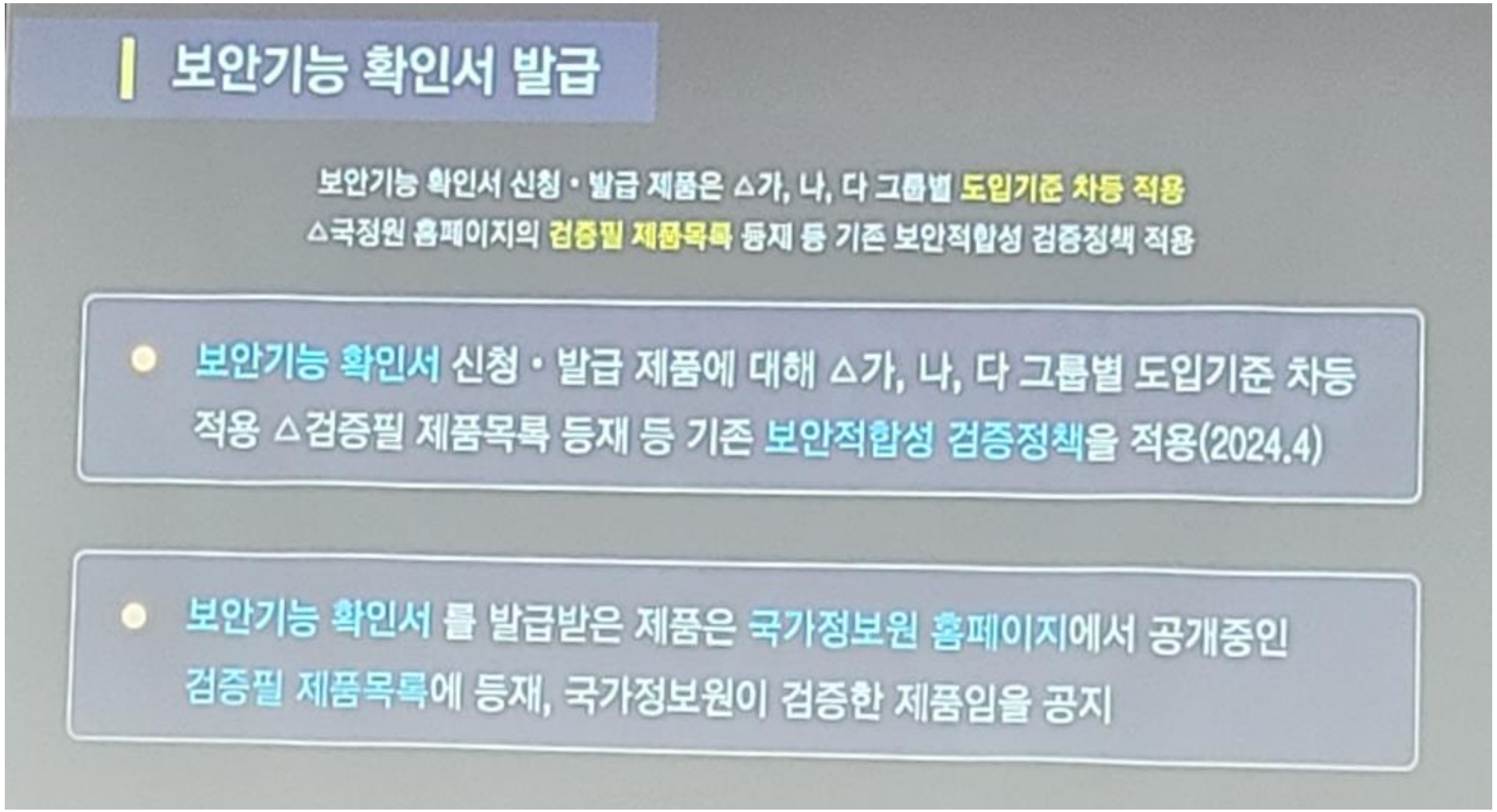
<영상정보처리기기 도입정책 변경내용>



1.2024년 4월부터 보안기능 확인서 접수 가능

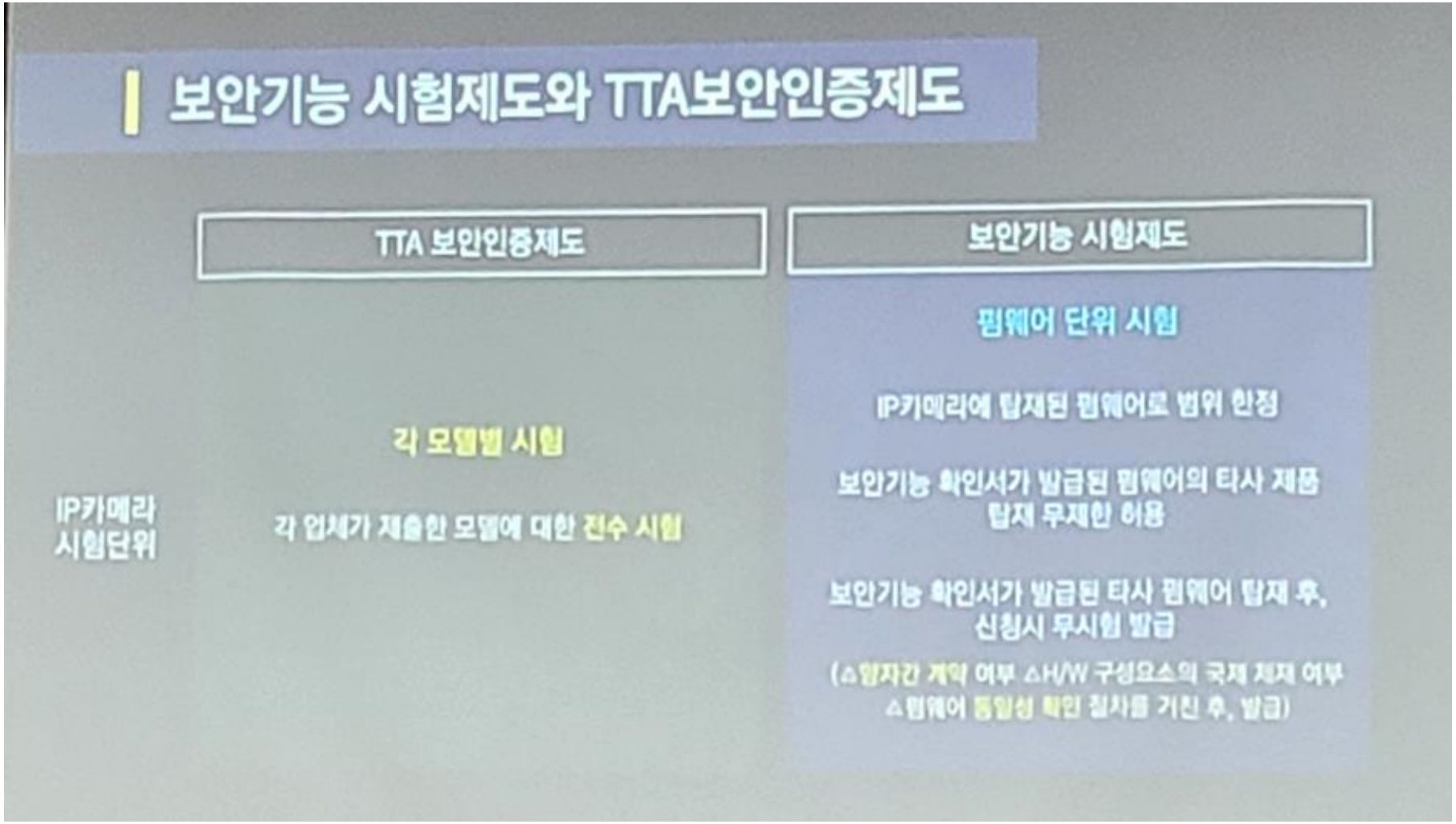
2.TTA 공공안전서비스단을 '보안기능 시험기관 ' 으로 추가 지정



1.보안기능 확인서 신청,발급 제품에 대해 **가,나,다 그룹별 도입기준 차등 적용**

-**국가기관의 중요도 별로 가,나,다 그룹으로 편성했으며 나,다 그룹이 전체기관의 80~90% 차지**

2.보안기능 확인서를 발급받은 제품은 국가정보원 홈페이지 검증필 제품목록에 등재

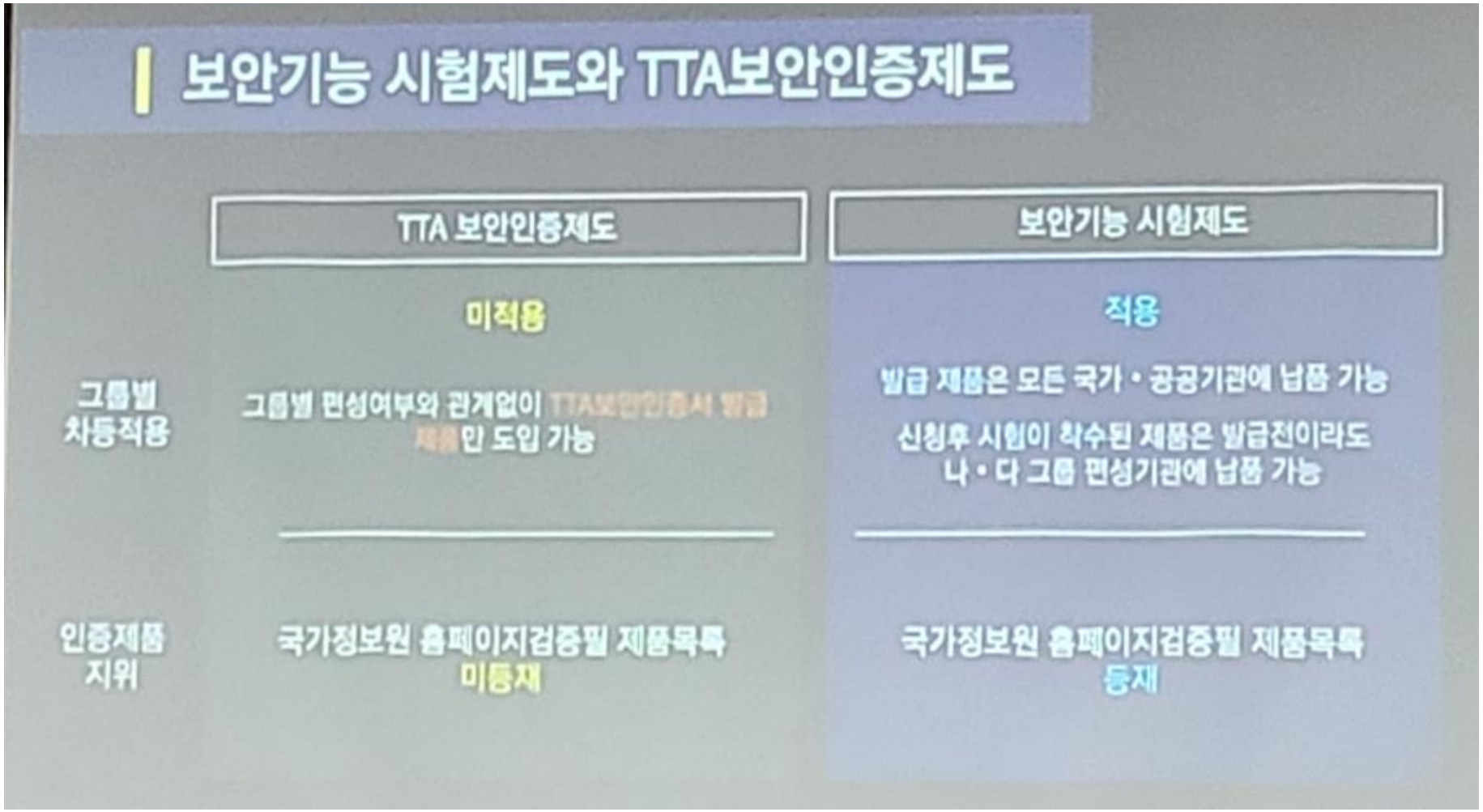


1.**기존 각 모델별 시험에서 펌웨어 단위 시험으로 변경**

-기관의 중요도 별로 편성했으며 나,다 그룹 편성기관이 전체기관의 80~90% 차지

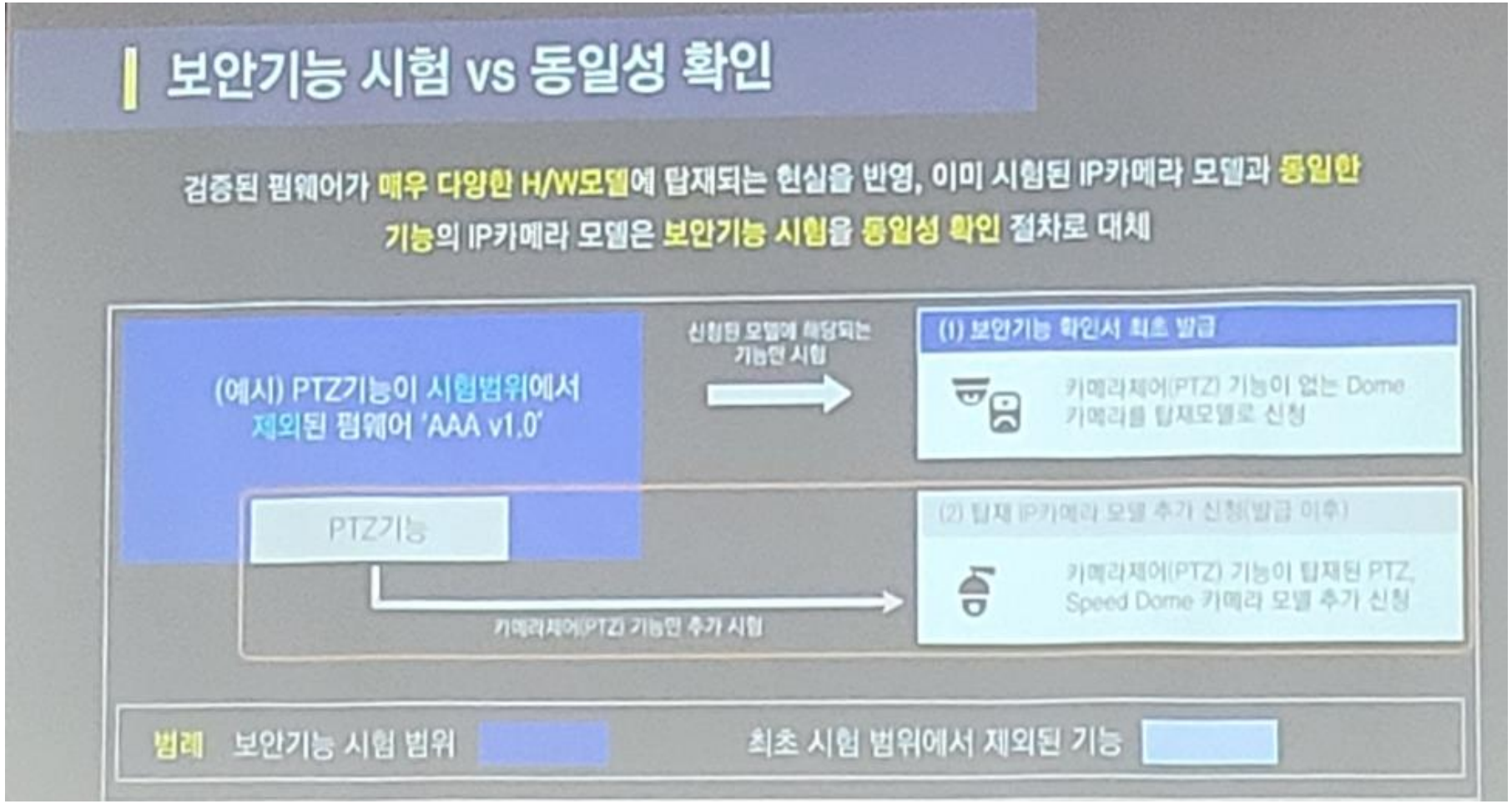
2.**보안기능 확인서가 발급된 펌웨어의 타사 제품 탑제 무제한 허용**

3.보안기능 확인서를 발급받은 제품은 국가정보원 홈페이지 검증필 제품목록에 등재



1.**발급 제품은 모든 국가 공공기관에 납품가능**

-신청 후 시험이 착수된 제품은 확인서 발급전이라도 나,다 그룹 편성기관에 납품 가능



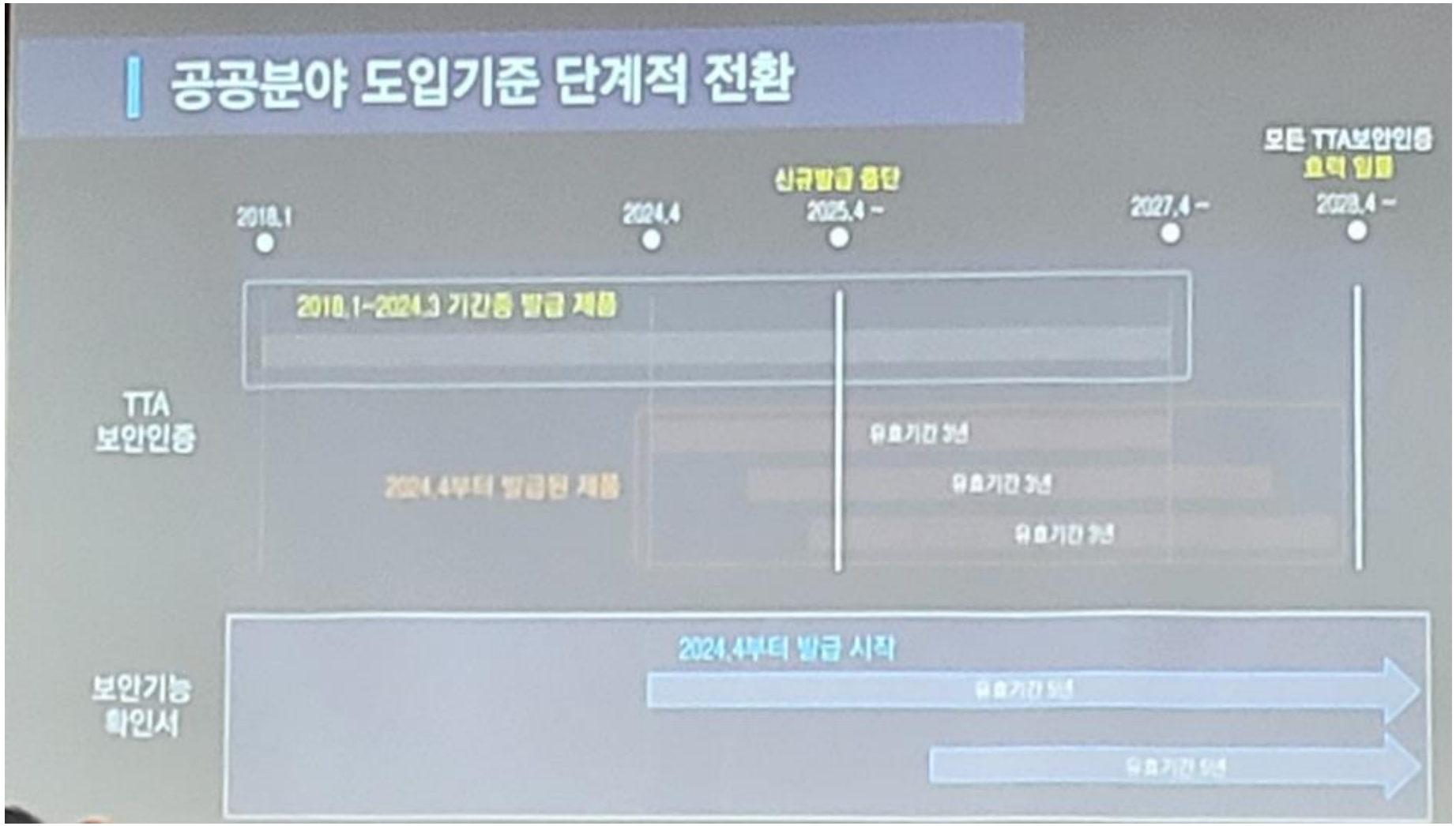
1.이미 시험된 IP카메라 모델과 **동일한 펌웨어의 IP카메라 모델은 보안기능 시험을 '동일성 확인 절차'로 대체**

-제품 형상은 다르지만 동일한 펌웨어를 사용하는 경우 무시험 발급, 해시값이 같아야함

-펌웨어 탑재에 관해 양사간 협의(계약) 또는 법적효력이 있는 공문 제출해야함

-계약내용은 펌웨어 유지보수내용, 업데이트, 취약점 개선부분에 대해 주체구분이 명확히 명시되어야함

-기간은 30~45일 소요예정, 수수료에 대한 부분은 내부검토중

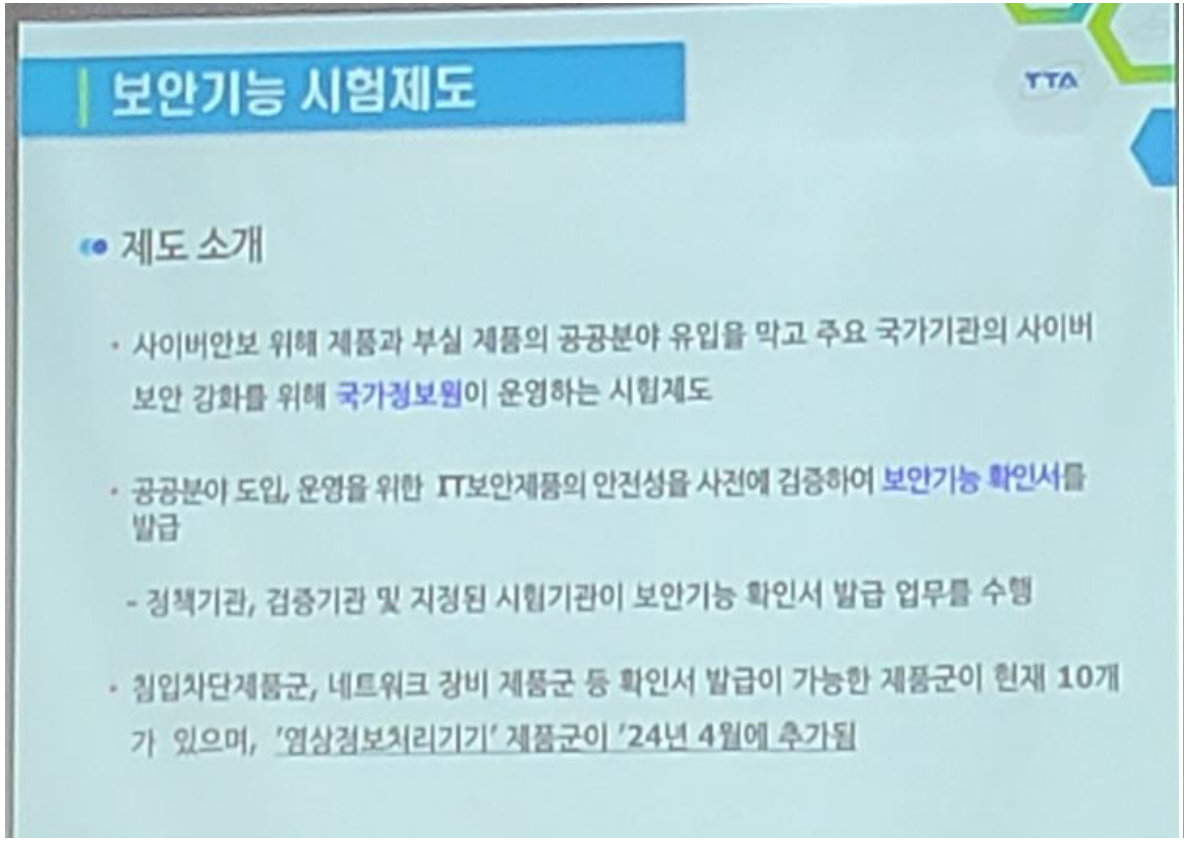


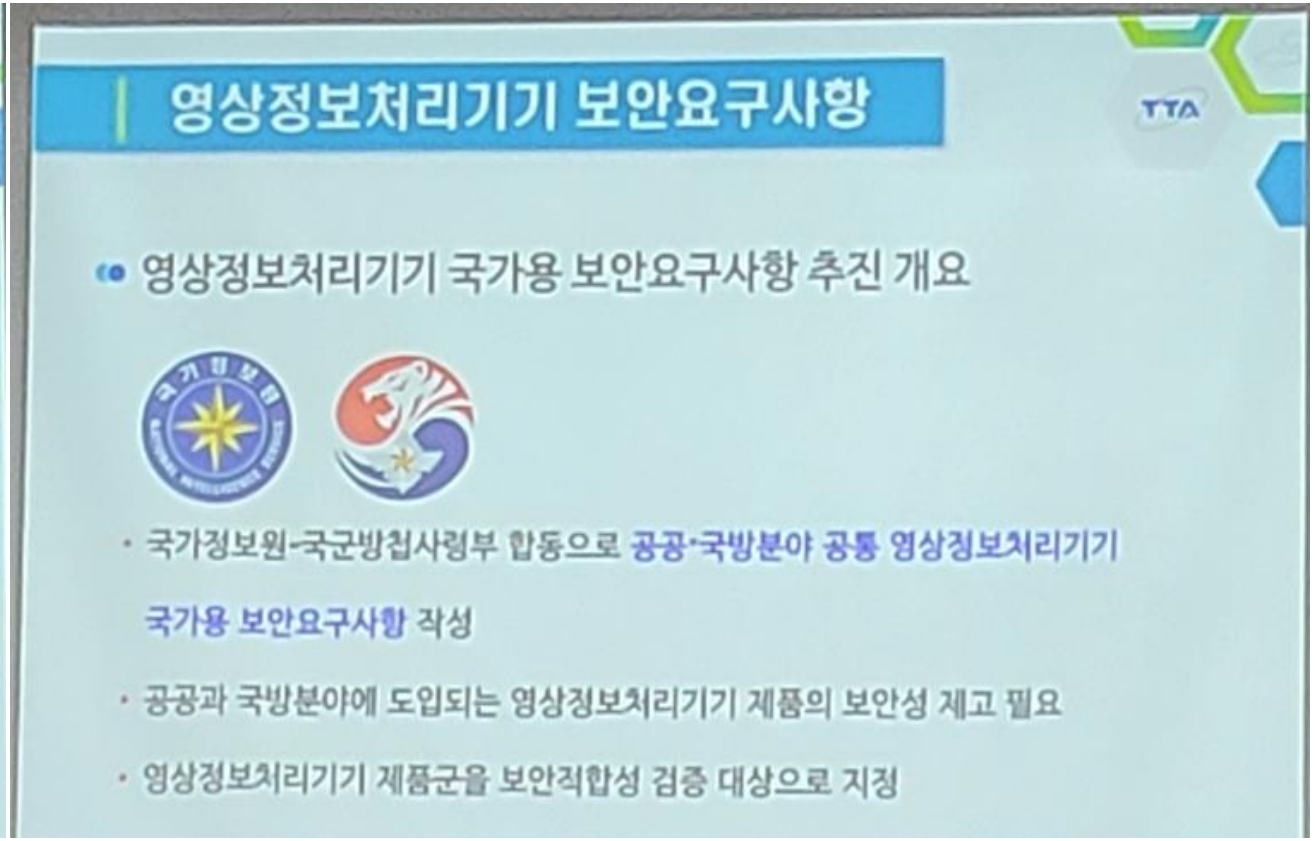
1.기존 TTA인증서: 2025년 4월 신규발급 중단/ 2027년 4월까지 기존 TTA인증서 유효함

/ 2028년 4월에 모든 TTA 인증서효력일몰

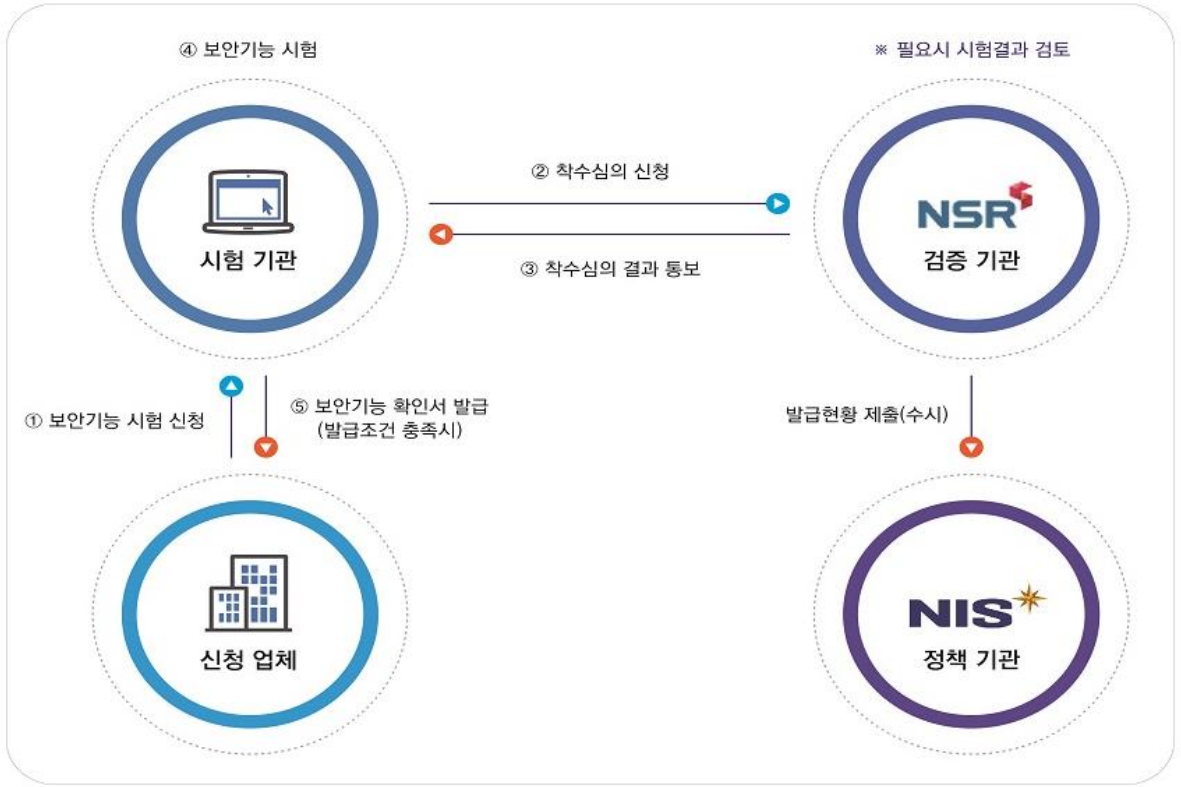
2.**신규 보안기능확인서: 2024년 4월부터 발급시작 (유효기간 5년)**

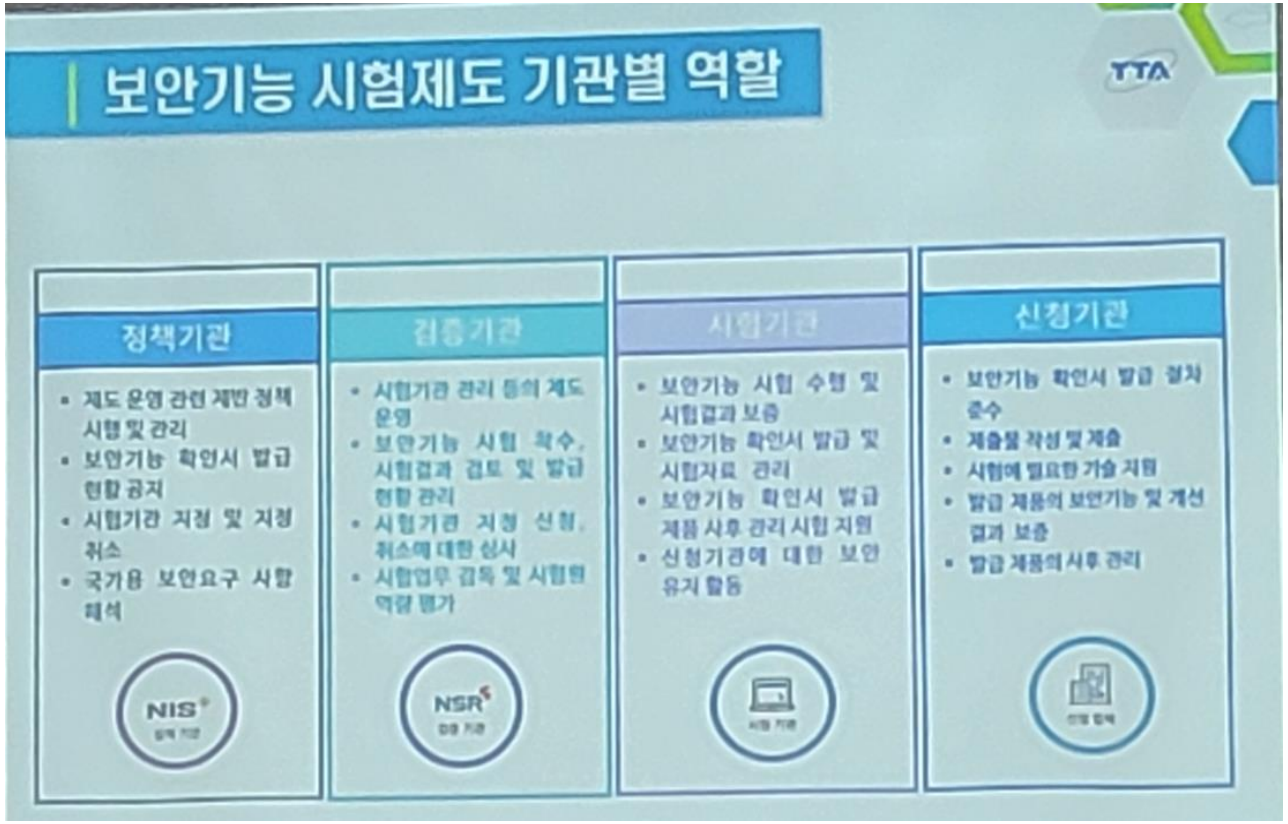
<보안기능확인서 발급절차>





1.국가정보원이 운영하는 보안기능 확인서에 **'영상정보처리기기 ' 제품군이 24년 4월에 추가됨**





1.**신청기관**: 신청에 필요한 문서 8종 제출

2.**시험기관(TTA 공공안전서비스단)** : 3일이내 착수심의 신청, 보안기능 시험 수행 및 시험결과 보증, 보안기능 확인서 발급 및 시험자료 관리

3.**검증기관(NSR 국가보안기술연구소):** 5일 이내 보안기능 시험 착수검토, 시험결과 검토 및 발급현황 관리,
시험기관 지정 신청 및 취소에 대한 심사

4.**정책기관(NIS국가정보원)**: 제도 운영 관련 제반 정책시행 및 관리, 보안기능 확인서 발급현황 공지

보안기능 시험 신청

신청에 필요한 제출문서(8종)

No.	제출문서	내용
1	보안기능 시험 신청서	양식 제공
2	신청기관 준수사항 확인서	양식 제공
3	취약점개선보증서약서	양식 제공
4	취약점개선내역서	• 양식 제공 • 신청 제품의 취약점 개선 이력과 그 내용을 기술한 문서

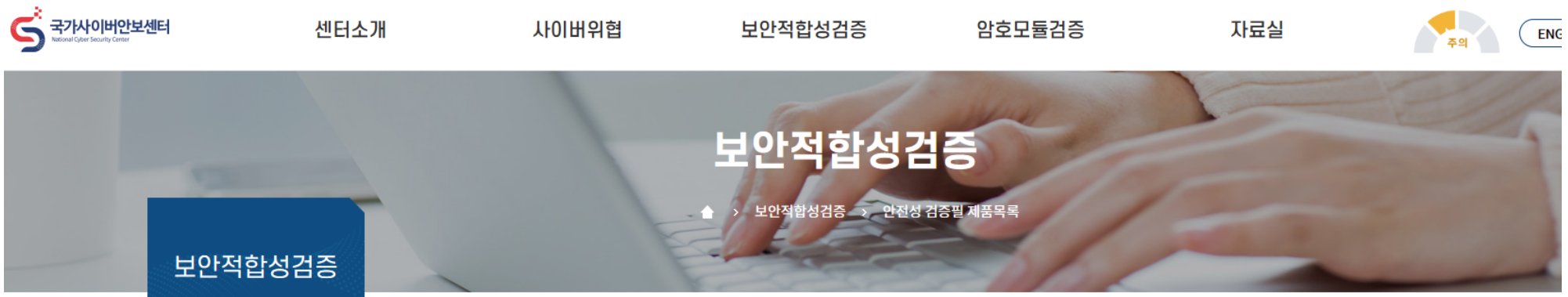
- ***제출문서에 사실이 아닌 내용을 기재할 경우,*** 시험이 중단될 수 있으며 보안기능 확인서가 발급되었더라도 효력이 무효화 될 수 있음

보안기능 시험 신청

신청에 필요한 제출문서 (8종)

No.	제출문서	내용
5	제품설명서	• 관리자, 사용자가 제품 목적에 맞게 활용할 수 있도록 운용 방법을 기술 • H/W 사양, 운용환경, 설치·사용법, 문제 해결 방법 필수 기재
6	보안기능 구현명세서	• 제품에 구현된 보안기능의 구현방법, 동작 절차 등에 대한 상세한 사항을 기술해야 하는 문서 • 보안기능 식별, 접속방법·인터페이스, 보안기능 구현 명세 • 보안기능 구현명세서 작성가이드 제공
7	보안기능 운용설명서	• 보안기능 구현명세서의 모든 보안기능의 설정, 운용절차·방법 등을 기재 • 제품 특징에 따라 '보안기능 구현명세서'에 통합 기재 가능
8	자체 시험결과서	• 신청업체가 사전에 국가용 보안요구사항을 시험하고, 결과를 기재한 문서 • 보안요구사항별로 시험환경, 시험절차, 시험결과를 작성

- ***제출문서에 사실이 아닌 내용을 기재할 경우,*** 시험이 중단될 수 있으며 보안기능 확인서가 발급되었더라도 효력이 무효화 될 수 있음

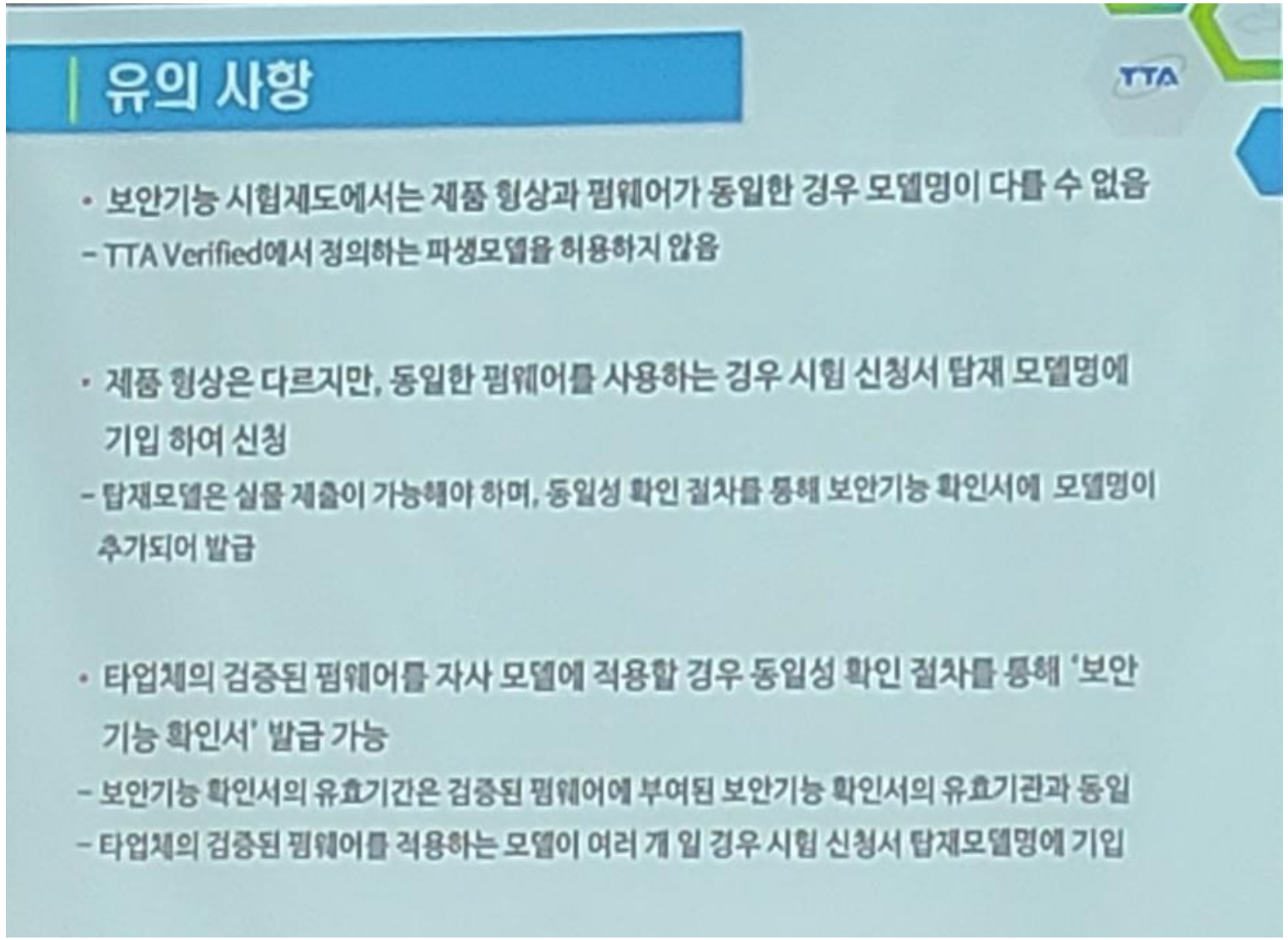


국가사이버안보센터에서 확인서 발급 제품 목록 확인 가능

보안기능 확인서 유효기간

공통 보안요구사항	제품 단위 보안요구사항	유효기간
영상정보처리기기 제품군 적용 대상 아님	국가용 보안요구사항 기반	5년
	구현명세서 기반	2년

- 적용 가능한 *국가용 보안요구사항*이 없는 경우 *구현명세서* 기반 시험
  - 영상정보처리기기 제품군에 속하지만 IP카메라 또는 영상정보 관리·저장제품과 현저히 달라 제정된 보안요구사항을 적용할 수 없을 경우 신청 업체가 제출한 *'보안기능 구현명세서'에서 보안기능 시험항목을 식별하여 시험 수행*



1.제품 형상과 펌웨어가 동일한 경우 모델명이 다를 수 없음 (파생모델 허용하지 않음)

2.제품 형상은 다르지만, 동일한 펌웨어를 사용하는 경우, 시험 신청서 탑재 모델명에 기입하여 신청

-탑재모델은 실물 제출이 가능해야함

-동일성 확인 절차를 통해 보안기능 확인서에 모델명이 추가되어 발급

참고 사항

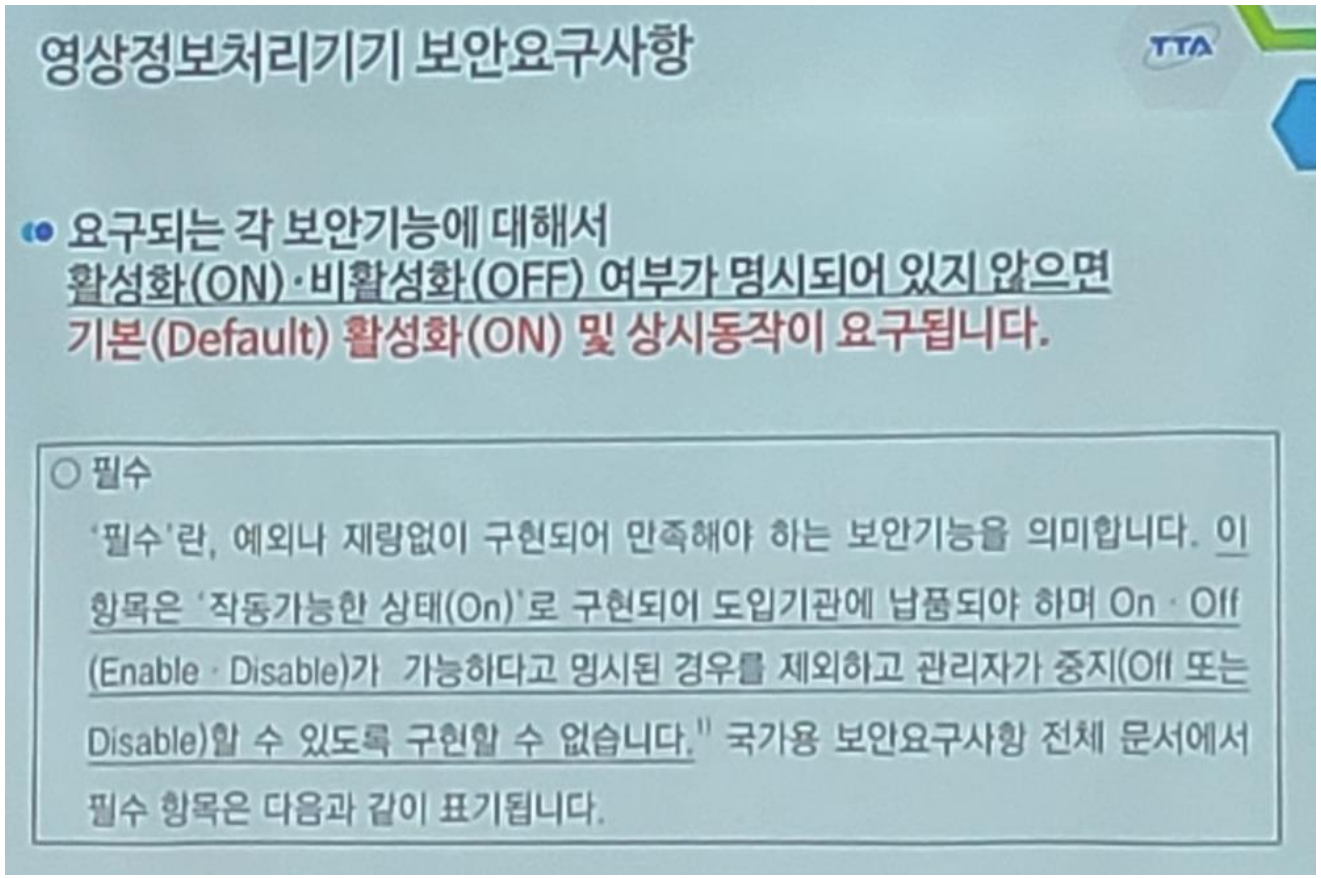
필독 사이트 및 파일

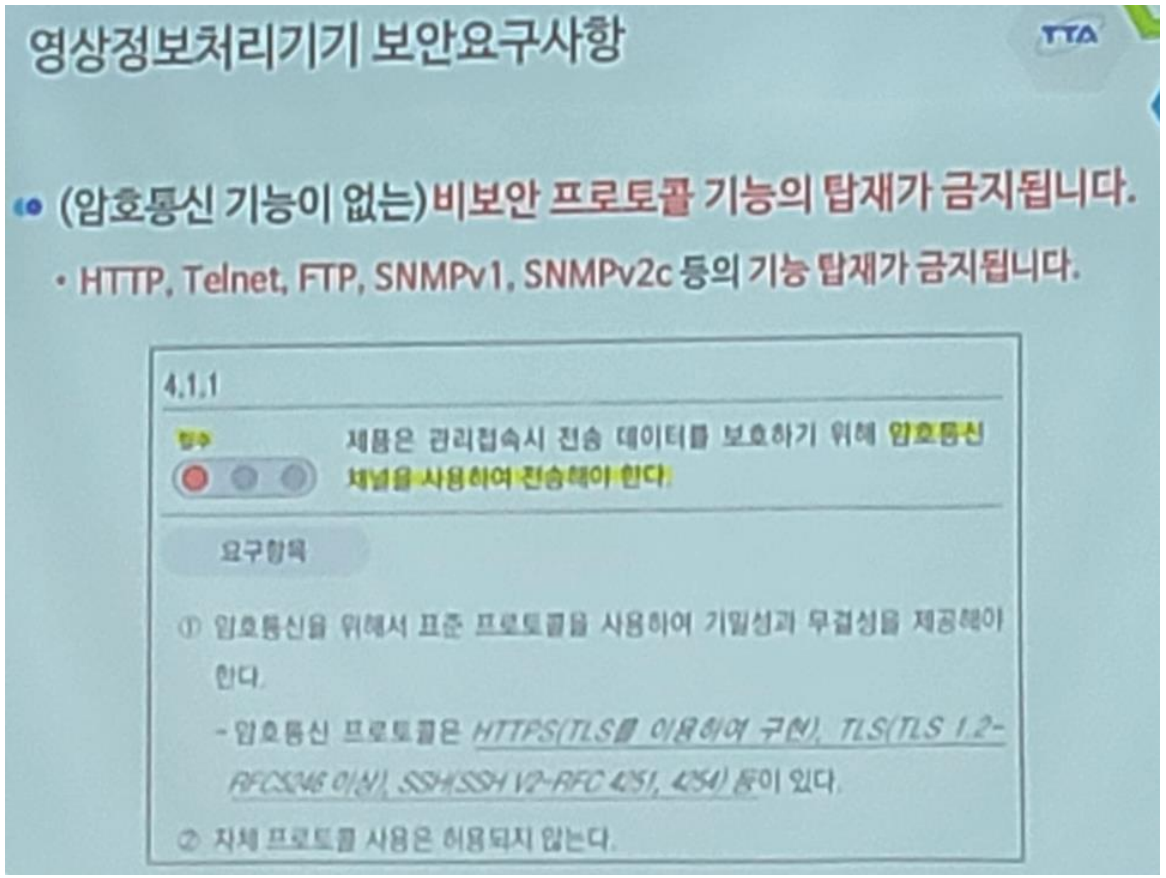
- NIS 국가정보원 www.nis.go.kr → 주요업무 →보안적합성 검증
- 국가사이버안보센터 www.ncsc.go.kr →보안적합성 검증 → 보안기능 시험제도
- 필독 파일
  - 보안기능 확인서 발급절차 안내 V2.2.
  - 보안기능 구현명세서 작성 가이드

보안기능 시험 컨설팅

- 기존 TTA 개발지원시험 서비스와 같이 보안기능 시험 신청전에 컨설팅 서비스를 이용하여 제출물 점검 및 사전시험 가능
  - 보안기능 시험제도의 공식적인 절차는 아니지만, 신청기관의 필요를 고려하여 시험기관들이 운영하고 있음

<영상정보처리기기 국가용 보안요구사항 주요사항 안내>





영상정보처리기기 보안요구사항

TTA

- (암호통신 기능이 없는)비보안 프로토콜 기능의 탑재가 금지됩니다.
  - 도입기관에서 허용하는 평문 통신(NTP, DNS 등)은 금지되지 않습니다.

3.1.3	
조건부 필수	제품은 외부 IT실체와 연동시 전송 데이터를 보호하기 위해 암호통신 채널을 사용하여 전송해야 한다.
조 건	외부 IT실체와 연동 지원시

참고 사항

① 외부 IT실체는 *인증서버, SNMP 서버, 업데이트 서버, 로그서버 등*이 있으며, 도입기관에서 허용하는 NTP 서버 등과의 평문 통신은 이 요구사항을 적용하지 않을 수 있다.

영상정보처리기기 보안요구사항

TTA

- 암호통신 기능에 대해 자체 프로토콜이 허용되지 않습니다.
  - 암호통신 채널 내에서 전송되는 메시지, 데이터 형식은 자체 프로토콜 사용이 금지되지 않습니다.

4.1.1	
필수	제품은 관리접속시 전송 데이터를 보호하기 위해 암호통신 채널을 사용하여 전송해야 한다.

요구항목

① 암호통신을 위해서 표준 프로토콜을 사용하여 기밀성과 무결성을 제공해야 한다.

- 암호통신 프로토콜은 *HTTPS(TLS를 이용하여 구현), TLS(TLS 1.2-RFC5246 이상), SSH(SSH V2-RFC 4251, 4254) 등*이 있다.

② 자체 프로토콜 사용은 허용되지 않는다.

IP카메라 보안요구사항

TTA

- 외부 저장매체(SD Card, USB 메모리 등)의 인식/사용 금지
  - IP카메라의 설치 형태는 물리적으로 안전한 장소의 설치로 간주되지 않습니다.

○ 제품은 외부 인터페이스에 저장 매체(SD Card, USB 메모리 등)가 연결되더라도 인식이 불가능해야 한다.

물리적으로 안전한 장소	제품의 설치 또는 운용을 위해 칸막이 등으로 분리되고 잠금장치 등을 활용하여 비인가자의 출입이 제한되거나 금지된 장소를 의미한다.

IP카메라 보안요구사항

TTA

- 관리도구(Discovery Tool, Install Tool) 사용의 제한적 허용
  - 관리도구의 사용이 아래와 같이 제한적으로 허용됩니다.

1.4.1	
조건부 필수	제품은 관리도구에 의한 최초설정을 기본(default) 상태에서만 허용해야 한다.
조 건	제품이 관리도구에 의한 최초 설정이 필요할 경우
요구항목	
① 관리도구의 기능은 장치 검색과 IP주소 설정 기능만 허용한다.	
② 기본(default) 상태에서 운용 상태로 전환되면, 관리도구에 의한 설정에 사용되는 포트 및 서비스는 즉시 비활성화되어야 한다.	

IP카메라 보안요구사항

TTA

- 기본(default) 상태 및 운용 상태 정의 추가

7. 용어 정의

■ 영상정보처리기기

기본(default) 상태	제품의 최초 관리자계정 · 비밀번호 설정/변경이 진행되지 않은 상태를 의미한다.
운용 상태	제품의 최초 관리자계정 · 비밀번호 설정/변경이 완료된 상태를 의미한다.

■ 운용 환경

제품의 최초 관리자계정 · 비밀번호 설정 및 변경이 진행되지 않은 상태를 '기본(default) 상태'로 정의하며, 최초 관리자계정 · 비밀번호 설정 및 변경이 완료된 상태를 '운용 상태'로 정의한다.

IP카메라 보안요구사항

TTA

- 관리도구의 검색 기능이 WS-Discovery(ONVIF)로 제한되나요?
  - 관리도구에 의한 검색, IP설정 기능은 특정 프로토콜로 제한되지 않습니다.

1.4.1

조건부 필수	제품은 관리도구에 의한 최초설정을 기본(default) 상태에서만 허용해야 한다.
조 건	제품이 관리도구에 의한 최초 설정이 필요할 경우

요구항목

① 관리도구의 기능은 장치 검색과 IP주소 설정 기능만 허용한다.

② 기본(default) 상태에서 운용 상태로 전환되면, 관리도구에 의한 설정에 사용되는 포트 및 서비스는 즉시 비활성화되어야 한다.

영상정보처리기기 보안요구사항

TTA

- **관리도구에 대해서 기본(default) 상태에서의 활성화, 암호통신의 미적용이 허용됩니다.**

1.4.1	
조건부 필수	제품은 관리도구에 의한 최초설정을 기본(default) 상태에서만 허용해야 한다.
조 건	제품이 관리도구에 의한 최초 설정이 필요할 경우

요구항목

① 관리도구의 기능은 장치 검색과 IP주소 설정 기능만 허용한다.

② 기본(default) 상태에서 운용 상태로 전환되면, 관리도구에 의한 설정에 사용되는 포트 및 서비스는 즉시 비활성화되어야 한다.

영상정보처리기기 보안요구사항

TTA

- **관리도구의 검색 기능은 운용 상태에서도 허용되면 안되나요?**
  - **허용되지 않습니다. 단순한 검색 요청에 의해 자신의 IP주소를 드러내는 것은 보안 측면에서 바람직하지 않습니다.**

1.4.1	
조건부 필수	제품은 관리도구에 의한 최초설정을 기본(default) 상태에서만 허용해야 한다.
조 건	제품이 관리도구에 의한 최초 설정이 필요할 경우

요구항목

① 관리도구의 기능은 장치 검색과 IP주소 설정 기능만 허용한다.

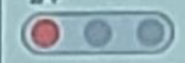
② 기본(default) 상태에서 운용 상태로 전환되면, 관리도구에 의한 설정에 사용되는 포트 및 서비스는 즉시 비활성화되어야 한다.

영상정보처리기기 보안요구사항

TTA

- 기본 접속 형태 및 기본(default) 활성화 허용 범위
  - IP카메라 : HTTPS 포트, 관리도구 서비스 포트
  - 영상정보 관리·저장제품 : 로컬

3.2.1

필수 

제품은 모든 관리접속에 대해 활성화 · 비활성화 기능을 제공해야 한다.

(중략)

IP카메라 ⇨

② 제품의 기본 접속 수단인 웹브라우저(HTTPS) 접속은 기본(default) 상태에서 활성화를 허용하며, 다른 모든 관리접속은 기본(default) 상태에서 비활성화되어 있어야 한다.

영상정보 관리·저장제품 ⇨

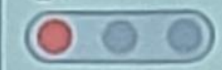
② 제품의 모든 관리접속은 기본(default) 상태에서 비활성화되어 있어야 한다.

영상정보처리기기 보안요구사항

TTA

- 패스워드뿐만 아니라, 계정(ID)도 최초 변경 또는 생성이 강제됩니다.

3.4.1

필수 

제품은 최초 제품 접속(*웹 브라우저 접속 등*) 시 기본 제공되는 계정에 대한 강제 변경 · 사용중지하는 기능을 제공해야 한다.

(중략)

③ 기본 제공되는 계정이 없는 경우, 신규 계정을 생성해야 하며 이후 제품의 관리 접속이 가능해야 한다.

④ 계정을 변경하거나 신규 생성할 경우, 유추가 가능한 명칭(*root, admin, 업체명, 카메라 모델명 등*)은 허용하지 않아야 한다.

영상정보처리기기 보안요구사항

TTA

- 페스워드 저장 시 일방향(해시) 암호 알고리즘이 강제되는가?
  - 편집 오류가 있습니다. 패스워드에도 양방향 암호 알고리즘 사용이 허용됩니다.

4.2.1

필수

중요정보를 제품 내부에 저장할 때 정해진 방식으로 저장해야 한다.

(중략)

⑤ 제품이 사용자 식별·인증을 위해 사용하는 사용자 패스워드는 복호화 되지 않도록 일방향 암호(해시)를 이용하여 저장해야 한다.

⇩

일방향 해시 알고리즘 또는 양방향 암호 알고리즘을 사용

영상정보처리기기 보안요구사항

TTA

- 양방향 암호 알고리즘으로 ARIA만 인정되는 것이 아닙니다.
  - 아래 "표 6"은 예시입니다.

〈표 6. 암호키 저장 및 파기 방법〉

암호키 종류	키 저장 및 파기 방법
TLS 개인키	• 형태 : RSA Private Key • 생성주체 : 제품에서 생성 • 저장·보호 : 제품 내부 저장 저장 영역 비인가자 접근 차단 • 파기 : 키 파기 명령 실행시 0, 1 로 3회 덮어씀
TLS 세션 암호화 키	• 형태 : ARIA Key • 생성주체 : 제품에서 생성 • 저장·보호 : 메모리(RAM)에만 저장 • 파기 : 세션 종료시 0, 1 로 3회 덮어씀
TLS 세션 무결성 검사키	• 형태 : HMAC Key • 생성주체 : 제품에서 생성 • 저장·보호 : 메모리(RAM)에만 저장 • 파기 : 세션 종료시 0, 1 로 3회 덮어씀

영상정보처리기기 보안요구사항

- 양방향 암호 알고리즘으로 ARIA만 인정되는 것이 아닙니다.
  - 아래 "표 6"은 예시입니다.

〈 표 6. 암호키 저장 및 파기 방법〉

암호키 종류	키 저장 및 파기 방법
TLS 개인키	• 형태 : RSA Pri • 생성주체 : 제품 • 저장 · 보호 : 제 • 파기 : 키 파기
TLS 세션 암호화 키	• 형태 : ARIA K • 생성주체 : 제 • 저장 · 보호 : 메 • 파기 : 세션 종
TLS 세션 무결성 검사키	• 형태 : HMAC • 생성주체 : 제 • 저장 · 보호 : 메 • 파기 : 세션 종

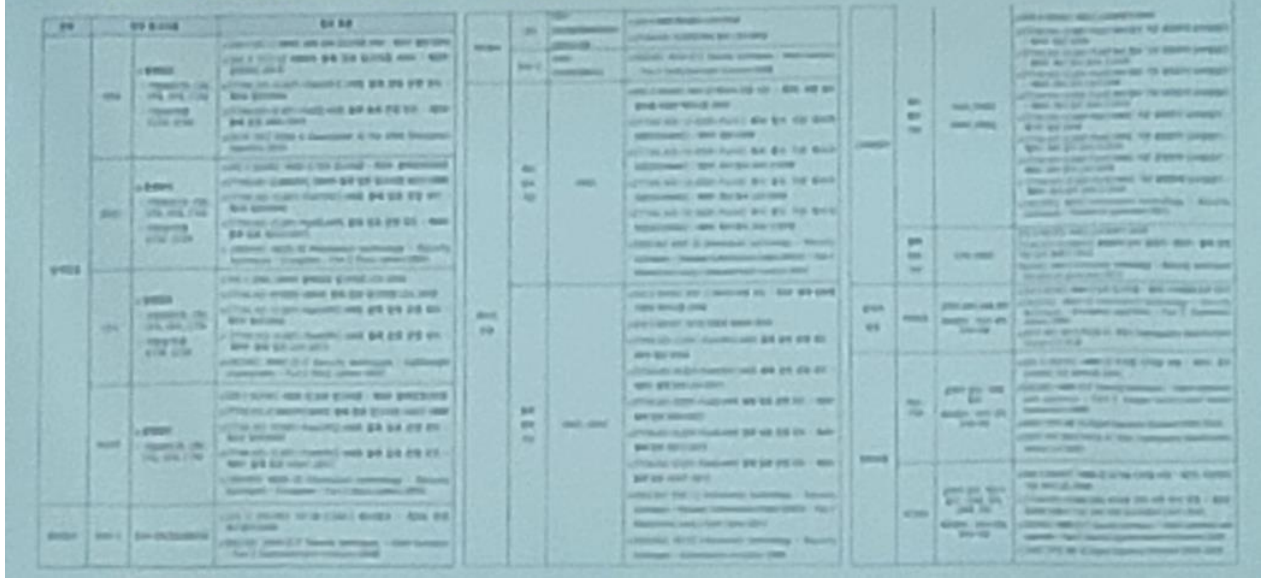
① 권고 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘으로 [별첨]을 참고하며, 예는 〈표 5〉와 같다.

〈 표5. 표준 알고리즘 예시〉

구분	예시
해시	SHA-224이상
대칭키 암호	키 길이 128bit 이상
공개키 암호	RSA 2048 이상, DSA(2048, 224) 이상
전자서명	RSA-PSS 2048 이상, KCDSA (2048, 224) 이상, ECDSA/EC-KCDSA (B-233, B-283, K-233, P-224, P-256)

영상정보처리기기 보안요구사항

- 〈별표 1〉 권고 암호 알고리즘
  - 암호 알고리즘 및 키 길이 이용 안내서, NIST SP800-131 Ar2 등도 참고



IP카메라 보안요구사항

- CMVP가 KCMVP를 대체할 수는 없습니다.
  - CMVP의 사용을 금지하지는 않습니다.

1.3.1	
조건부 필수	영상 저장시 암호화 저장 기능을 제공해야 한다.
조 건	영상 저장 기능 지원시
요구항목	
① IP카메라는 비디오, 이미지 등 영상을 제품 내부 저장소에 저장할 경우 검증필 암호모듈(KCMVP)로 암호화하여 저장해야 한다.	

영상정보처리기기 보안요구사항

- 암호화 관련 KCMVP 기반의 동작만 인정되는가?
  - 아닙니다. 오픈소스 라이브러리도 요구사항을 만족한다면 인정됩니다.
  - KCMVP는 IP카메라의 영상 내부 저장 시에만 조건부 필수로 강제됩니다.

4.2.1	
필수	중요정보를 제품 내부에 저장할 때 정해진 방식으로 저장해야 한다.
(중략)	
① 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.	
② 검증필 암호모듈(KCMVP)의 사용을 권고한다.	

IP카메라 보안요구사항

TTA

제품 내부 저장소가 무엇을 의미하나요?

- **탈부착이 불가능한 제품 내부의 비휘발성 메모리를 의미합니다.**

1.3.1

조건부 필수

영상 저장시 암호화 저장 기능을 제공해야 한다.

조 건 영상 저장 기능 지원시

요구항목

① IP카메라는 비디오, 이미지 등 영상을 **제품 내부 저장소**에 저장할 경우 검증필 암호모듈(KCMVP)로 암호화하여 저장해야 한다.

영상정보처리기기 보안요구사항

TTA

녹음(오디오 저장) 기능 관련

- **녹음(오디오 저장) 기능의 제거(삭제)를 요구하지 않습니다.**

점검시 유의사항

① 제품이 오디오 데이터 저장 기능을 제공하는 경우, 해당 기능에 대해 활성화 · 비활성화(On · Off) 기능을 제공하고 기본(default) 상태에서 비활성화되어 있는지 확인한다.

개인정보 보호법

⑤ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, **녹음기능은 사용할 수 없다.**

의료법

② 의료기관의 장이나 의료인이 제2항에 따라 수술을 하는 장면을 촬영하는 경우 **녹음 기능은 사용할 수 없다.** 다만, 환자 및 해당 수술에 참여한 의료인 등 **정보주체 모두의 동의를 받은 경우에는 그러하지 아니하다.**

IP카메라 보안요구사항

- IP카메라의 모든 계정은 관리자로 간주됩니다.
  - 라이브 모니터링 권한만 있어도 (영상모니터링) 관리자 입니다.

제품의 식별 및 인증 대상이 되는 사용자는 관리자이며, 제품이 제공하는 영상만을 취득하고자 하는 영상 모니터링 관리자 또한 식별 및 인증 대상에 포함된다.

7. 용어 정의

사용자	관리자와 일반사용자를 모두 포함한 제품에 접속할 수 있는 권한을 가진 실체를 의미한다.
관리자	제품의 보안기능을 구동 · 중지 · 재시작하거나 주어진 권한을 사용하여 보안 정책을 추가 · 변경 · 조회 · 삭제하는 등 제품을 운용 및 관리하는 사용자를 의미한다.
일반사용자	관리자가 설정한 보안정책에 따라 제품의 보안기능을 이용할 수 있는 사용자를 의미한다. 제품 유형에 따라 제품에 포함된 에이전트 또는 클라이언트를 사용할 수 있다.

영상정보 관리·저장제품 보안요구사항

- 영상정보 관리·저장제품의 모든 계정은 관리자로 간주됩니다.
  - 라이브 모니터링 권한만 있어도 (영상모니터링) 관리자 입니다.
  - 관리프로그램(CMS 등) 측의 계정은 일반사용자 계정입니다.

제품의 식별 및 인증 대상이 되는 사용자는 관리자이며, 제품이 제공하는 영상만을 취득하고자 하는 영상 모니터링 관리자 또한 식별 및 인증 대상에 포함된다.

7. 용어 정의

사용자	관리자와 일반사용자를 모두 포함한 제품에 접속할 수 있는 권한을 가진 실체를 의미한다.
관리자	제품의 보안기능을 구동 · 중지 · 재시작하거나 주어진 권한을 사용하여 보안 정책을 추가 · 변경 · 조회 · 삭제하는 등 제품을 운용 및 관리하는 사용자를 의미한다.
일반사용자	관리자가 설정한 보안정책에 따라 제품의 보안기능을 이용할 수 있는 사용자를 의미한다. 제품 유형에 따라 제품에 포함된 에이전트 또는 클라이언트를 사용할 수 있다.

영상정보처리기기 보안요구사항

TTA

- **동일 계정 또는 동일 권한의 중복 접속 금지**
  - **영상모니터링 계정에 대해서는 동일 권한의 중복 접속이 허용됩니다.**

7.2.1	
필수	제품은 동일한 관리자 계정 또는 동일 권한을 사용하여 제품 중복 접속을 허용하지 않아야 한다.

(중략)

참고 사항

① 영상 모니터링 관리자에 대해서는 적용하지 않을 수 있다.

② 다중 세션 연결이 이뤄질 수 있는 기기 간 연동 및 영상 전송 관련 표준프로토콜(ONVIF, RTSP 등)에 대해서는 이 요구사항을 적용하지 않는다.

영상정보처리기기 보안요구사항

TTA

- **"외부 IT실체" 관련**
  - **제품과 물리적으로 분리되어 있으며, 네트워크로 통신하는 IT실체**
  - (서버) 외부 IT실체 : Email 서버, FTP 서버, 로그 서버, DBMS, IP카메라 등
  - (클라이언트) 외부 IT실체 : 단말(PC), NVR, CMS, VMS 등

외부 IT실체	제품과 상호작용하는 IT실체를 의미한다. (제품이 제공하는 보안기능을 사용하는 것을 허용하기 이전에 제품에서 외부 IT실체를 인증하거나, 외부 IT실체가 제공하는 보안기능을 사용하기 이전에 외부 IT실체로부터 제품을 인증받아야 할 수 있다.)

영상정보처리기기 보안요구사항

TTA

"외부 IT실체" 관련

- 2장에서의 외부 IT실체에 대해 "제품"의 역할은 "서버"입니다.

2.1.2

조건부 필수

제품은 연동하는 외부 IT실체를 인증해야 한다.

조 건 제품에서 외부 IT실체를 인증하는 경우

2.3.2

조건부 필수

제품은 외부 IT실체 인증에 필요한 정보를 설정하는 기능을 제공해야 한다.

조 건 외부 IT실체 인증에 필요한 인증정보 설정이 요구되는 경우

영상정보처리기기 보안요구사항

TTA

"외부 IT실체" 관련

- 3장과 4장의 외부 IT실체에 대해 "제품"의 역할은 "클라이언트"입니다.

3.4.3

조건부 필수

제품은 내부 구성요소 또는 외부 IT실체에 접근하기 위해 사용하는 기본(default) 패스워드를 변경하는 기능을 제공해야 한다.

조 건 제품 내부 구성요소 또는 외부 IT실체에 접근을 위해 패스워드기 필요한 기능 제공시

3.4.4

조건부 필수

제품은 외부 IT실체로부터 인증받기 위해 필요한 인증정보를 설정하는 기능을 제공해야 한다.

조 건 제품과 연동하는 외부 IT실체가 제품 인증을 위해 인증정보를 요구하는 경우

4.1.2

조건부 필수

제품은 외부 IT실체와 연동시 전송 데이터를 보호하기 위해 암호통신 채널을 사용하여 전송해야 한다.

조 건 외부 IT실체와 연동 지원시

영상정보처리기기 보안요구사항

TTA

- 영상 프로토콜 사용자 인증 관련
  - HTTP(ONVIF)/RTSP Digest [MD5] 금지
  - HTTP(ONVIF)/RTSP Basic 금지
  - WSSE UsernameToken [SHA-1] 금지

1.1.1

필수

기기 간 연동 및 영상 관련 표준 프로토콜(ONVIF, RTSP 등)에서 사용자 인증 기능을 제공해야 한다.

요구항목

① ONVIF, RTSP 등에서 Digest 인증이 사용될 경우, RFC 7616 표준을 준수해야 한다.

② 사용자 인증에서의 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘을 사용해야 한다.

영상정보처리기기 보안요구사항

TTA

- 웹 브라우저와 제품 간의 사용자 인증 방식
  - 웹 브라우저와 제품 간의 사용자 인증 방식은 HTTP Digest로 제한되지 않습니다.
  - 외부 IT실체 또는 제품 구성요소와의 사용자 인증 방식도 특정 방식으로 제한되지 않습니다.
  - 어떤 사용자 인증 방식이든 "2. 식별 및 인증"의 요구사항을 만족하면 됩니다.

2. 식별 및 인증

제품의 관리자, 일반사용자, 외부 IT실체, 영상 프로토콜에 대한 식별 및 인증 기능을 확인한다.

- 2.1 사용자 등 식별 및 인증
- 2.2 인증실패 대응
- 2.3 패스워드 등 민감정보 생성 및 안전성 검증
- 2.4 인증 정보 재사용 방지
- 2.5 인증 피드백 보호

영상정보처리기기 보안요구사항

- Websocket 사용 시 내부 컨텐츠로 RTP/RTSP만 사용해야 하는가?
  - 아래 별표 1은 예시입니다. 다른 형태의 영상 전송 표준 프로토콜도 허용됩니다.

(별표 1)

영상 전송 관련 표준 프로토콜 목록

프로토콜	통신 형태	비고
ONVIF	HTTP/S/TCP HTTP/TCP	• www.onvif.org • IEC 62676-1-1:2019, IEC 62676-2-1:2019 • SOAP 기반의 HTTP/XML 메시지 프로토콜 (IP카메라의 영상 관련 정보 Read/Write) • 영상 전송에 대해 RTP/RTSP 등의 표준 지원
RTP	RTP/TCP RTP/UDP	• RFC 3550 • KS C IEC 62676-2-1:2013 • 실질적인 Video 및 Audio Data 전송
RTSP	RTSP/TCP RTSP/UDP	• RFC 2326 • KS C IEC 62676-2-1:2013 • RTP 스트림 제어
SRTP	SRTP/TCP SRTP/UDP	• RFC 3711, 5763 • RTP 프로토콜의 확장판 • 각 RTP 패킷의 데이터를 Encryption하여 전송
RTSPS	RTP/RTSP/TLS	• RFC 2326 • 각 RTSP 패킷의 데이터를 Encryption하여 전송
HTTP Tunneling	RTP/RTSP/HTTP/S/TCP	• RTP/RTSP 데이터를 HTTP Payload에 위치시키고 전송
Websocket	RTP/RTSP/HTTP/S/TCP	• RFC 6455 • RTP/RTSP 데이터를 Websocket 내에서 전송

영상정보처리기기 보안요구사항

- 하드웨어 일체형 장비는 펌웨어에 OS Kernel을 포함해야 한다.
  - Iptables, Network Interface, 잡음원(/dev/random) 등을 Kernel에 의존한다면 펌웨어에 OS Kernel이 포함되어 형상관리가 이뤄져야 합니다.

■ 제품 개요

IP카메라는 사람 또는 사물의 영상 등을 촬영하고 선택적으로 음성 획득도 가능하며, 영상과 음성을 IP 네트워크를 통하여 전송할 수 있는 하드웨어 일체형 장비이다.

■ 제품 개요

영상정보 관리 · 저장제품은 TCP/IP 네트워크를 통해 IP카메라로부터 영상을 전송받아 실시간 모니터링, 저장(녹화), 검색(재생) 등 영상정보를 처리하는 목적으

(중략)

제품은 하드웨어 일체형 또는 소프트웨어 등 다양한 형태로 구현될 수 있으며

영상정보처리기기 보안요구사항

TTA

- 펌웨어 업데이트 시에 매번 OS Kernel을 변경해야 하는가?
  - 펌웨어 업데이트 시에 OS Kernel에 대한 무결성 검사를 수행하고 현재 탑재된 Kernel와 해시 값이 동일하다면 OS Kernel은 변경되지 않아도 괜찮습니다.