공공분야 영상정보처리기기 제품군

보안적합성 검증 정책

2024. 4. 1.

NIS

목 차

1 영상정보처리기기 대상 보안검증 시행

Ⅰ 개요

국가정보원은 「국가정보원법」 제4조 제1항 제4호, 「사이버안보업무규정」 제9조 제2항 · 제3항 등 관련 법령에 따라 국가 · 공공기관이 도입 · 운용하는 '보안기능이 있는 정보통신기기'(이하, 'IT보안제품')에 대한 보안대책을 수립, 배포하며 도입 · 운용과정에서 이에 대한 부합 여부를 지속 검증하고 있습니다.

이의 일환으로 국가정보원은 국가 · 공공기관이 도입 · 운용하는 IT보안제품 중, 영상정보처리기기 제품군[1]에 대한 검증기준을 마련하고 도입 기준 · 절차를 정비하였습니다.

2 보안적합성 검증 정책 시행 관련 주요 사항

(1) 보안적합성 검증 시행 취지

〈 주요 내용 〉

❶ 영상정보처리기기에 은닉된 백도어 · 알려진 취약점 등 사이버안보 위해요인을 사전에 제거하고 취약점을 보완하여 보안성이 확인된 제품의 공공분야 도입을 촉진하기 위함입니다.

❷ 영상정보처리기기의 도입과 안전한 운용에 필요한 △제품에 구현된 보안기능 △원천 개발업체 △취약점 제거 책임 소재 등의 중요 정보를 명확히 확인하여 각급기관이 신뢰성있는 제품을 도입하도록 지원하기 위함입니다.

---

1) '영상정보처리기기 제품군'이란, 불특정 사람 또는 사물을 촬영한 영상을 유 · 무선 정보통신망으로 전송 · 저장 · 분석하는 기기 또는 장비를 의미합니다.

〈 주요 내용 〉

❸ 영상정보처리기기 제품군에 대한 보안기준과 검증 절차를 정비, 관련 업계의 어려움을 해소하고 공공분야에 **보안성 · 신뢰성**이 확인된 제품이 적시(適時) 도입되도록 지원하기 위함입니다.

(2) 정책 시행

영상정보처리기기 제품군에 속하는 제품은 **2024년 4월 1일**부터 국가정보원이 사이버안보업무규정 제9조에 따른 검증이 필요한 **보안기능이 있는 정보통신기기**로 취급되어 보안적합성 검증정책의 대상이 됩니다.

(3) 정책 대상 기관

영상정보처리기기에 대한 보안적합성 검증 정책 대상 기관은 기존 IT보안제품 검증 정책 대상기관[2]과 같습니다.

(4) 보안적합성 검증 대상으로 지정된 영상정보처리기기의 도입

영상정보처리기기 제품 유형 중 보안적합성 검증 대상으로 지정된 제품 유형은 이 문서에서 안내하는 **기준과 절차**에 따라 국가 · 공공기관에 도입되어야 합니다.

다만, 검증 대상에서 제외된 제품 유형은 **보안적합성 검증 정책과 무관**하게 국가 · 공공기관에 도입될 수 있습니다.

여 백

2) 「국가정보원법」·「전자정부법」·「사이버안보업무규정」(대통령령)에서 대상 기관으로 규정된 기관입니다.

영상정보처리기기 관련 업계를 위한

2 영상정보처리기기 제품군 보안검증 정책 설명

Ⅰ 보안적합성 검증 대상제품 중요

(1) IP카메라

□ 검증 대상 IP카메라 유형 정의

IP카메라는 일정한 공간 또는 특정한 위치에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상을 촬영하여 이를 유 · 무선 TCP/IP 네트워크를 통하여 전송하는 기기[3] 입니다.

예를 들어 실화상 카메라, 열화상 카메라, 머신비전 카메라 등[4] 카메라 유형에 관계없이 TCP/IP 네트워크에 연결되어 IP를 할당받고 영상데이터를 전송한다면 **보안적합성 검증 대상**에 해당됩니다. 그러나, TCP/IP 방식이 아닌 SDI(SMPTE) 방식으로 연결되어 영상데이터를 전송한다면 보안적합성 검증 대상에 해당되지 않습니다.

(2) 영상정보 저장 · 관리 제품

□ 검증 대상 영상정보 저장 · 관리 제품 유형 정의

△통제 대상 IP카메라의 관리 △통제 대상 카메라가 전송한 영상의 실시간 모니터링, 저장(녹화), 검색(재생) 등 영상정보 처리 △개별 통제 대상 카메라에 대한 제어(화각, 초점거리, 지향각도 조정 등) 기능 등을 보유한 기기입니다.

---

3) 「개인정보보호법」 제2조 제7호에 규정된 '고정형 영상정보처리기기'중에서 「개인정보보호법」 시행령 제3조 제1항 제2호에 규정된 '네트워크 카메라' 도 해당됩니다.

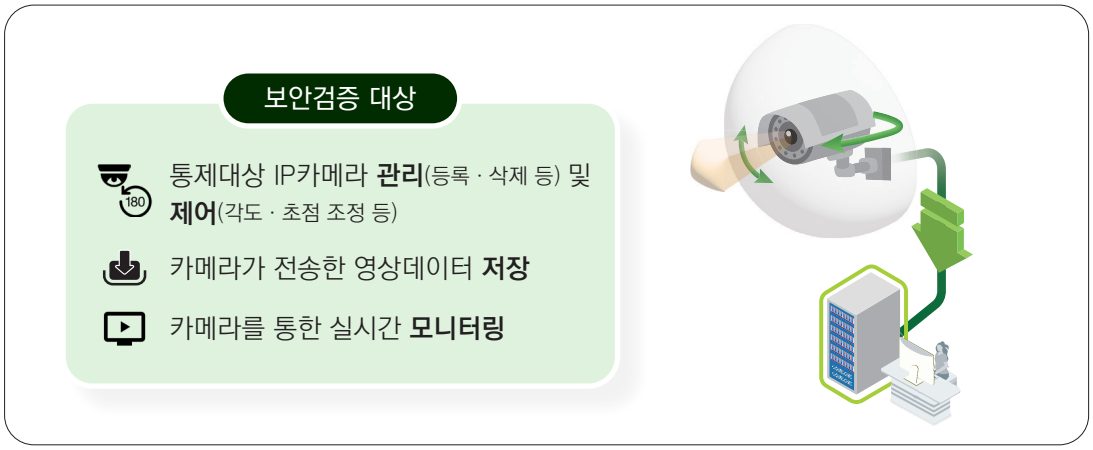
4) 기재된 카메라 유형은 열거가 아닌 **예시**로써 기재된 카메라 유형만이 보안적합성 검증 대상이라는 의미는 아닙니다.

영상정보 저장 · 관리 제품의 예로써 △NVR(Network Video Recorder) △VMS(Video Management System) △Hybrid-DVR(Digial Video Recoder) 등이 있습니다.

(3) 검증 대상 제품 유형에 대한 예시

□ 〈그림 1. 데이터 전송 프로토콜에 따른 IP 카메라 검증 대상 여부 〉

□ 〈그림 2. 검증 대상이 되는 영상정보 저장 · 관리 제품〉



2 국가용 보안요구사항

(1) 국가용 보안요구사항 적용 분야 및 작성 대상

□ 공공 · 국방분야 공통 국가용 보안요구사항

국가정보원과 국군방첩사령부는 공공 · 국방분야에 도입되는 영상정보처리기기중에서 'IP카메라 제품유형'과 '영상정보 저장 · 관리제품'이 기본적으로 준수해야하는 보안기능을 규정한 「공공 · 국방 공통 국가용 보안요구사항」을 제정하였습니다.

(2) 공공 · 국방분야 공통 국가용 보안요구사항의 준수

□ 국가용 보안요구사항이 적용되는 사전인증제도

공공 · 국방분야 공통 국가용 보안요구사항은 국가정보원이 시행하는 '보안기능 시험' 제도에 적용됩니다. 한국정보통신기술협회(TTA)가 시행하는 '공공기관용 CCTV 보안성능품질 인증' 제도 및 과학기술정보통신부가 시행하는 'CC인증' 제도에는 적용되지 않습니다.

□ 국가용 보안요구사항 준수 여부 입증

공공 · 국방분야 공통 국가용 보안요구사항은 '보안기능 시험' 제도를 통해 준수 여부를 입증할 수 있으며 준수가 확인된 IP카메라 제품과 영상정보 저장 · 관리제품은 시험기관[5]이 '보안기능 확인서'를 발급합니다.

3 보안기능 확인서 신청 및 발급[6]

(1) 보안기능 확인서 발급 대상 및 유효기간

□ 보안기능 확인서 발급 대상 제품 유형

보안기능 확인서 발급 대상은 보안적합성 검증 대상으로 지정된 'IP카메라 제품' 유형과 '영상정보 저장 · 관리제품' 유형입니다.

5) 정책 시행일(2024.4.1) 현재, 영상정보처리기기에 대한 보안기능 확인서는 전문 시험기관으로 지정된 'TTA 공공안전서비스단'에서 발급합니다.

6) 보안기능 시험 제도 및 보안기능 확인서 발급에 대한 자세한 사항은 국가사이버안보센터 홈페이지의 '보안적합성 검증 ⇨ 자료실'에 게시된 「보안기능 확인서 발급절차 안내」 문서를 확인하시기 바랍니다.

□ 보안기능 확인서 유효기간

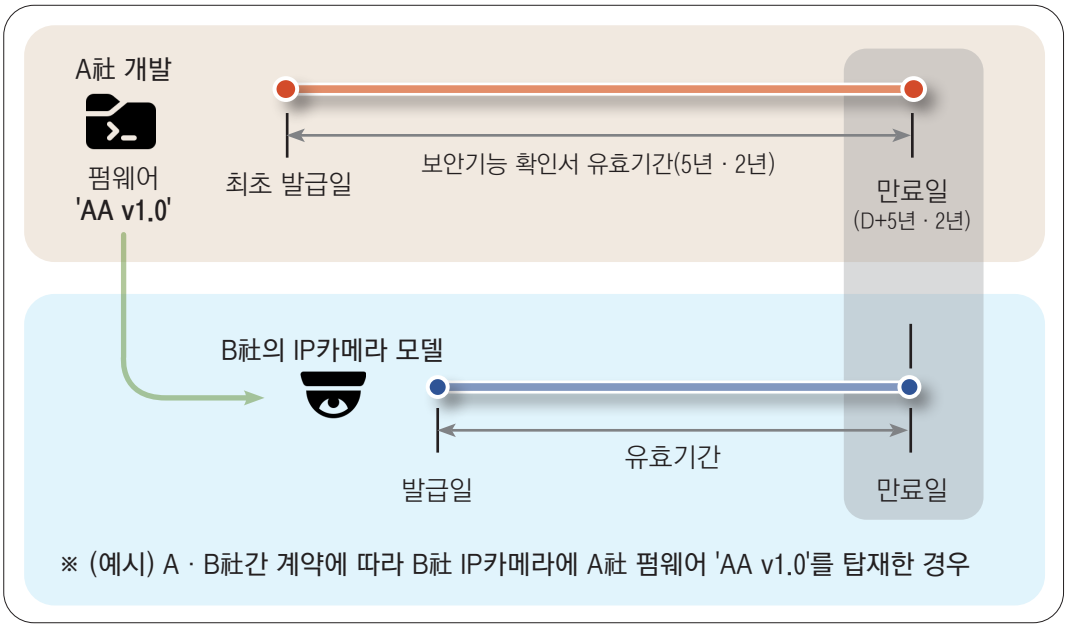
국가용 보안요구사항을 준수한 제품은 5년의 유효기간이 부여됩니다. 이 밖에 보안적합성 검증 대상에 속하지만 새로운 유형의 신기술 · 신종 영상정보처리기기 제품은 시험과정에서 국가용 보안요구사항이 적용되지 않을 경우, 2년의 유효기간[7]이 부여됩니다.

□ 제3자 개발 펌웨어 탑재 제품의 유효기간

신청 업체가 보안기능 시험을 신청한 H/W 모델[8]에 탑재된 펌웨어가 '제3자(타 업체)가 개발, 보안기능 확인서를 발급받은 펌웨어' 인 경우 신청 제품에 부여되는 유효기간은 펌웨어에 부여된 유효기간을 초과하지 않습니다.

〈그림 3〉을 참고하시기 바랍니다.

〈그림 3. 제3자 개발 펌웨어 탑재 제품의 유효기간〉



유효기간을 한정하는 이유는 동일 펌웨어를 탑재한 여러 대의 H/W에 대해 각 탑재 시점마다 새롭게 유효기간을 부여한다면 탑재 시점에 따라서 그 펌웨어에 부여된 검증의 **효력이 종료되지 않고 영원히 유지될 수 있는 부작용**을 막기 위함입니다.

---

7) 국가용 보안요구사항이 적용되지 않은 경우, 업체가 작성한 일반 보안요구사항 또는 보안기능 구현명세서 기반으로 보안기능 시험이 진행됩니다.

8) IP카메라와 영상정보관리 · 저장 제품 모두에 해당됩니다.

(2) 보안기능 시험 대상 및 범위 중요

□ 보안기능 시험 대상

보안기능 시험 신청이 가능한 영상정보처리기기는 개발이 완료되어 출시된 실제 존재하는 제품(탑재 모델이 정해진 펌웨어)이며 대한민국에 수입 · 판매되기 위해 거쳐야 하는 법적 요건 · 제반 절차[9]를 준수한 제품이어야 합니다.

보안기능 시험 대상은 〈표 1〉에 기재된 바와 같이 펌웨어 또는 구동 S/W이며, IP카메라의 경우, 신청 업체는 보안기능 시험을 신청할 때 그 펌웨어가 탑재되는 모든 모델을 함께 제출해야 합니다. 제출된 펌웨어와 모든 탑재 모델은 보안기능 확인서 발급 과정에서 펌웨어에 대한 보안기능 시험 또는 동일성 확인 절차를 거치게 됩니다.

〈표 1. 보안기능 시험 대상 〉

제품 유형	보안기능 시험	시험 신청시 최소 구비사항
IP 카메라	펌웨어	펌웨어와 모든 탑재 모델
하드웨어 일체형 영상정보 관리 · 저장제품	펌웨어	펌웨어와 모든 탑재 모델
소프트웨어 영상정보 관리 · 저장제품	구동 S/W	구동 S/W

신청 업체가 근시일내에 개발 완료 예정임을 약속하거나 사전에 모델명(번호)을 부여하였어도 출시되지 않았다면 보안기능 시험 대상으로 인정되지 않으며 신청하더라도 반려되므로 주의하시기 바랍니다.

□ 보안기능 시험 범위

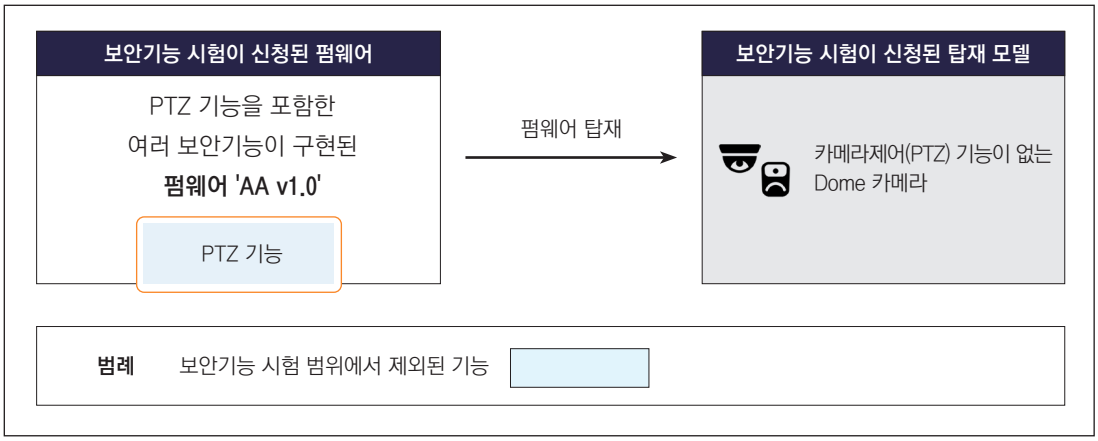
신청 업체가 「보안기능 시험 신청서」에 기재한 펌웨어(또는 S/W)와 H/W모델을 기준으로 보안기능 시험이 수행됩니다. 신청 업체가 이미 출시한 모델일지라도 「보안기능 시험 신청서」에 기재되지 않은 모델은 시험 대상이 아닙니다.

만약, 보안기능 시험 신청시 펌웨어에 구현된 보안기능중에서 일부만 지원하는 H/W 모델을 탑재 모델로 기재하였다면, 기재된 모델이 지원하지 않은 펌웨어의 기능은 〈그림 4〉에 표현된 예시와 같이 시험 범위에서 제외됩니다.

---

9) 예를 들어 전파법 제58조의 2에 의거, 국립전파연구원이 시행하는 '방송통신기자재 등의 적합성 평가제도'가 있습니다.

〈그림 4. (예시)보안기능 시험 범위〉



IP카메라에 대한 보안기능 시험은 펌웨어를 대상으로 시행됩니다. 그 외 광학 기능 등 여타 기능은 시험 대상이 아닙니다.

(3) 보안기능 시험 신청시 유의 사항 중요

☐ 제출문서 제출 시점 및 유의 사항

신청 업체가 제출하는 제출문서는 ①제품 설명서, ②보안기능 구현명세서 ③보안기능 운용 설명서, ④시험 결과서, ⑤취약점 개선 내역서 등 5종 입니다.

신청 업체는 보안기능 시험 신청시 5종의 제출물을 한국어(한글)로 작성, 모두 제출해야 하며 시험기관은 접수된 제출물의 작성 기준 만족 여부를 확인, 시험에 착수합니다.

신청 업체는 국가사이버안보센터 홈페이지에서 배포중인 「보안기능 구현명세서 작성 가이드」를 활용, 보안기능 구현명세서 작성이 가능합니다.

보안기능 시험의 지체를 예방하기 위해 '착수 후 일정기간 내 제출물 제출(또는 보완)을 조건으로 우선 시험 계약 체결' 등의 요청은 수용되지 않으니 주의하시기 바랍니다.

☐ 신청 제품에 대한 취약점 개선

「취약점 개선내역서」는 신청 제품의 취약점 개선 이력과 그 내용을 기술한 문서입니다. 「취약점 개선내역서」가 필요한 이유는 개발 업체에 의한 취약점 사전 점검 · 제거를 권장하고 제품의 보안성을 제고하여 시험과정에서 취약점 보완으로 인한 지체를 예방하기 위함입니다.

신청 업체는 보안기능 시험 신청전에 대상 제품에 대한 취약점 점검을 실시, 존재하는 취약점을 최대한 제거하고 그 내역을 「취약점 개선내역서」에 기재해야 합니다.

시험기관은「취약점 개선내역서」검토 결과에 따라 필요하다고 판단될 경우, 신청 제품에 대한 취약점 점검을 추가로 수행할 수 있습니다.

신청 업체와 펌웨어 개발 업체가 상이할 경우, 펌웨어의 탑재 · 활용과 관련된 계약에 기재된 취약점 보완 이행 주체가 작성합니다.

□ △**공동 · 위탁 개발(ODM) △제3자 개발 펌웨어의 책임 · 권리에 대한 명확한 규정**

신청 업체가 '공동 · 위탁 개발(ODM)하거나 제3자가 개발한 펌웨어' 를 탑재한 제품을 신청할 경우, 취약점 보완 및 탑재 · 판매 권리 등의 사항에 대해 각 당사자의 국적과 무관하게 상호간의 계약을 통해 규정[10]되어야 합니다.

〈표 2. 계약 또는 서면을 통해 규정되어야 하는 최소 사항〉

구분	내용
취약점 보완	발견된 취약점에 대한 보완 이행 주체
	해킹 사고 발생시 대응 행위 주체 및 범위
	기타 유지보수 책임 및 이행 주체
신청 업체의 권리	Δ신청업체가 해당 펌웨어에 대해 우리나라에서 보유하는 권리와 한계 Δ펌웨어 탑재 모델에 대한 식별 (예 : 펌웨어 활용에 대한 독점적 권리의 유무, 재판매 권리와 관련된 사항 등)

이는 운용중 발생할 수 있는 해킹사고 및 취약점에 대한 신속한 대응을 위한 것으로 신청 업체는 보안기능 시험 신청시 위 내용이 기재된 문서(계약서 또는 공문 등)의 사본을 시험기관에 제출해야 합니다.

다만, 계약서 내용중 계약 당사자 모두 또는 일방에 의해 기밀로 취급되는 사항이 있다면 해당 내용을 비닉(庇匿) 처리하여 제출할 수 있습니다.

□ **보안기능 확인서를 발급받은 펌웨어의 타사(他社) 탑재 허용**

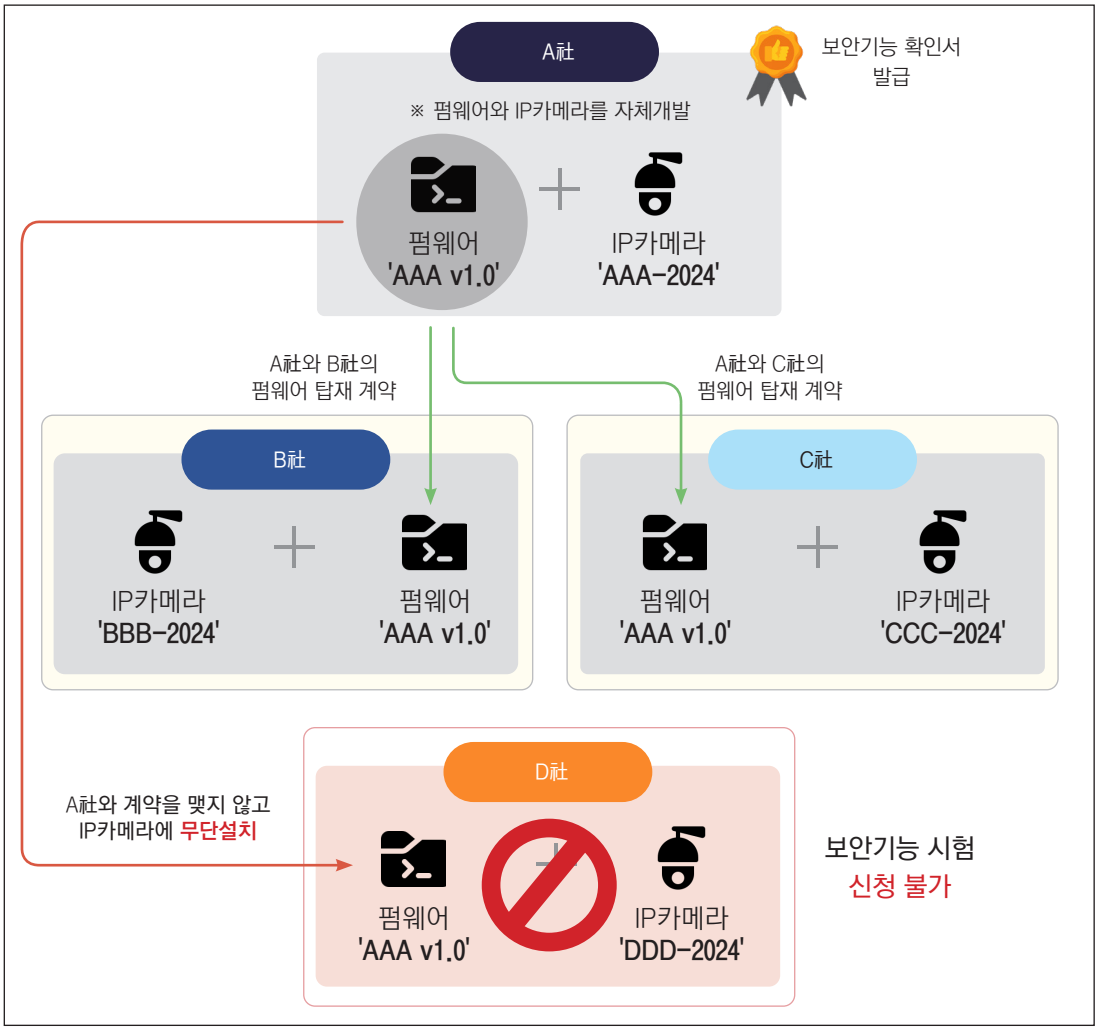
펌웨어에 대한 법적 권리를 보유한 업체와 IP카메라에 탑재를 원하는 업체간 계약을 통해 제반 사항이 규정될 경우, 검증된 펌웨어의 타사(他社) IP카메라 탑재가 무제한 허용됩니다.

10) 당초 계약에 반영되지 않았더라도 당사자간의 공문 등 법적 효력이 있는 서면을 통해 추가 규정하여도 인정됩니다.

예를 들어 B社가 보안기능 확인서를 발급받은 펌웨어 ‘AAA v1.0’을 보유한 A社와 펌웨어 탑재에 대한 **계약을 체결**하여 ‘AAA v1.0’을 IP카메라 ‘BBB-2024’ 모델에 탑재하였다면 보안기능 시험 신청이 가능합니다.

그러나, 계약에 의하지 않고 A社의 펌웨어를 자사(自社)의 카메라에 **무단 탑재**하였다면 보안기능 시험 신청이 **불가**합니다. 〈그림 5〉를 참고하시기 바랍니다.

〈그림 5. 타사(他社) 펌웨어 탑재 예시〉



☐ 동일한 펌웨어 · H/W 모델에 대한 중복 발급 배제 중요

보안기능 확인서는 **신청 업체의 동일 제품**에 대해 중복으로 발급되지 않습니다. 신청 업체가 이미 보안기능 확인서를 발급받은 펌웨어 · IP카메라의 보안기능 · H/W 구성요소에 대해 아무런 **형상 변경(추가 · 변경 등)을 하지 않고** 새로운 제품으로 명명(命名)하여 보안기능 시험을 신청한 경우, **중복 발급 배제에 해당**됩니다.

아래 예시를 참고하시기 바랍니다.

〈 중복 발급 배제의 예시 〉

❶ A社가 자사(自社)가 개발하여 보안기능 확인서를 발급받은 IP카메라 'AAA-2024'의 명칭만 'AAA-2025'으로 변경, 보안기능 확인서에 기재된 펌웨어 'AAA v1.0'을 탑재하여 보안기능 시험을 신청

(**설명**) IP카메라 'AAA-2024'의 형상 변경(H/W 구성요소 추가 · 변경) 없이 명칭만 단순 변경, 다른 IP카메라인것처럼 보안기능 시험을 신청하였으므로 중복 발급 배제에 해당

❷ A社가 자사(自社)가 개발하여 보안기능 확인서를 발급받은 펌웨어 'AAA v1.0'의 파일명을 'ABB v2.0'으로 변경, 보안기능 확인서에 기재된 IP카메라 모델 'AAA-2024'에 탑재하여 보안기능 시험을 신청

(**설명**) 펌웨어 'AAA v1.0'의 형상 변경(보안기능 추가 · 변경) 없이 파일명만 단순 변경, 다른 펌웨어인것처럼 보안기능 시험을 신청하였으므로 중복 발급 배제에 해당

(4) 보안기능 추가시험 및 동일성 확인 중요

□ **보안기능 추가 시험 또는 동일성 확인 적용**

시험기관은 보안기능 시험을 신청한 제품에 대해 탑재된 펌웨어 및 하드웨어 구성요소를 기준으로 ❶보안기능 추가시험[11] ❷동일성 확인중에서 어느 절차가 필요한지 판단합니다.

□ **보안기능 추가시험 적용**

신청 제품을 기준으로 ❶신청 업체가 추가 탑재를 신청한 새로운 IP카메라 모델이 시험 범위에서 제외된 기능을 활용하거나 ❷펌웨어에 새로운 기능을 추가로 구현하였을때, 보안기능 추가 시험이 적용됩니다.

시험기관은 보안기능 추가시험을 위해 필요한 경우, 이미 제출된 제출문서(보안기능 구현명세서 등)의 보완을 요청할 수 있습니다.

---

11) 보안기능 추가시험이란, 이미 검증을 받은 펌웨어에 대해 시험범위에서 제외되었거나 새롭게 구현된 특정 기능에 국한하여 추가로 적용되는 시험절차 입니다.

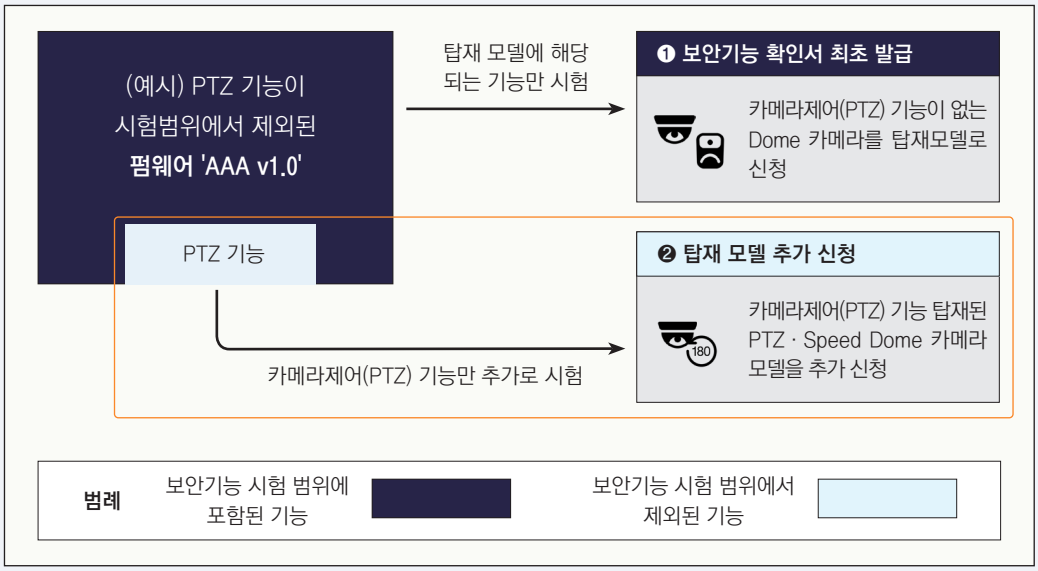
아래 예시를 참고하시기 바랍니다.

〈 보안기능 추가시험의 예시 〉

❶ (사례 A) A社가 기존 보안기능 확인서에 자사(自社)의 신규 IP카메라 모델 'AAA-2024'의 추가 기재를 신청한 경우

(**설명**) 신청 모델이 펌웨어의 보안기능중 최초 시험범위에서 제외된 기능을 활용한다면 펌웨어의 형상이 변경되지 않아도 〈그림 6〉의 예시와 같이 해당 보안기능에 한정하여 보안기능 추가시험 수행 후, 기존 보안기능 확인서에 추가 기재

〈그림 6. 자사(自社) 개발 IP카메라 신규 모델 추가〉



❷ (사례 B) IP카메라 모델만 보유한 B社가 보안기능 확인서를 발급받은 A社의 펌웨어 'AAA v1.0'을 자사(自社)의 IP카메라 모델 'BBB-2024'에 탑재, 보안기능 시험을 신청한 경우

(**설명**) 타사(他社)의 펌웨어를 자사의 IP카메라에 탑재한 경우에도 〈사례 A〉와 동일한 원칙이 적용되므로 최초 시험범위에서 제외된 기능을 활용한다면 보안기능 추가시험 수행 후, 보안기능 확인서 신규 발급

※ 다만, IP카메라가 펌웨어의 최초 시험범위에 해당되는 기능만 보유할 경우 동일성 확인 절차로 대체하고 보안기능 확인서 신규 발급

□ 동일성 확인 적용 기준

'동일성 확인'이란, 새로운 IP카메라 모델에 탑재하기 위해 보안기능 시험이 신청된 펌웨어가 ❶형상변경이 없으며 ❷함께 신청된 IP카메라의 기능이 펌웨어의 최초 시험 범위를 초과하지 않는 경우, 보안기능 시험 대신 적용되는 절차 입니다.

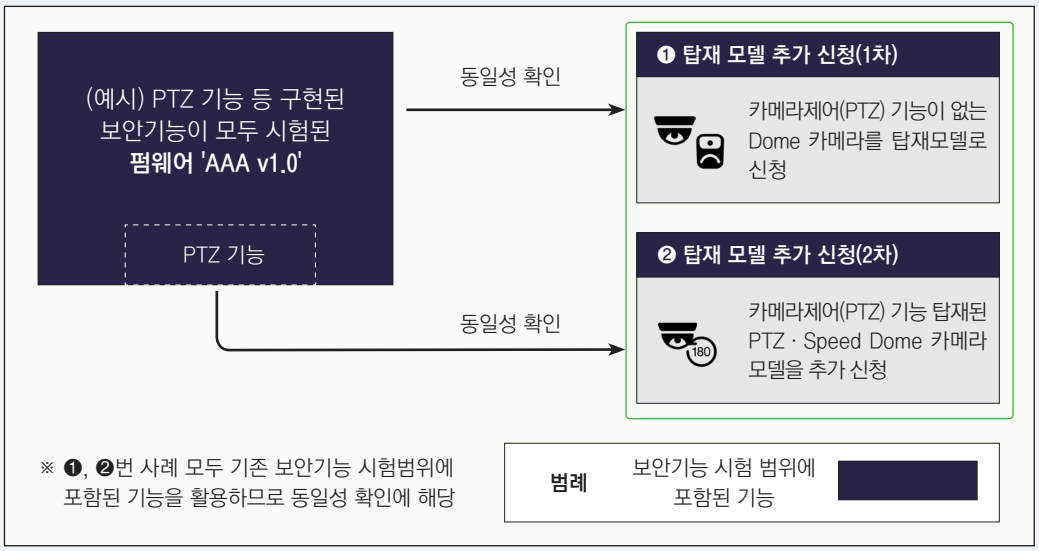
동일성 확인 절차가 적용될 경우, 펌웨어에 대한 보안기능 시험은 생략됩니다.

〈 동일성 확인의 예시 〉

❶ (사례 A) A社가 기존 보안기능 확인서에 자사(自社)의 신규 IP카메라 모델 'AAA-2024'의 추가 기재를 신청한 경우

(**설명**) 신청 모델이 펌웨어의 보안기능중 **최초 시험범위에 해당하는 기능을 활용**한다면 〈그림 7〉의 예시와 같이 **동일성 확인** 후, 기존 보안기능 확인서에 추가 기재

〈그림 7. 자사(自社) 개발 IP카메라 신규 모델 추가〉



❷ (사례 B) IP카메라 모델만 보유한 B社가 보안기능 확인서를 발급받은 A社의 펌웨어 'AAA v1.0'을 자사(自社)의 IP카메라 모델 'BBB-2024'에 탑재, 보안기능 시험을 신청한 경우

(**설명**) 타사(他社)의 펌웨어를 자사의 IP카메라에 탑재한 경우에도 〈사례 1〉과 동일한 원칙이 적용되므로 **최초 시험범위에 포함된 기능을 활용**한다면 동일성 확인 수행 후, 보안기능 확인서 **신규 발급**

국가 · 공공기관을 위한

3 영상정보처리기기 제품군 도입 정책 설명

Ⅰ 영상정보처리기기 제품군 도입 중요

(1) 각 그룹별 도입기준

□ '가', '나'그룹 편성 기관의 사전인증요건

'가', '나'그룹에 편성된 기관은 2024년 4월 1일부터 영상정보처리기기 제품군에 속하는 제품을 도입[12]할 경우, 〈표 3〉에 지정된 사전인증요건을 준수해야 합니다.

〈 '가', '나'그룹에 지정된 사전인증요건 〉

❶ 보안기능 시험제도 ❷공공기관용 CCTV 보안 성능품질 인증제도[13]

〈 표 3 '가', '나'그룹 도입 영상정보처리기기 제품군 사전인증요건 〉

제품군	제품 유형	사전인증요건
영상정보 처리기기 제품군	IP카메라	❶ · ❷ 중 어느 하나
	영상정보 저장 · 관리 제품	❶ · ❷ 중 어느 하나
	영상정보처리기기 제품군에 속한 신기술 · 신종 제품[14]	(권장) ❶ · ❷ 중 어느 하나 (未발급제품은 도입후, 검증신청)

12) '도입'의 시점은 계약일로 봅니다.

13) 한국정보통신기술협회(TTA)에서 시행하는 'TTA보안인증'제도의 정식명칭입니다.

14) '신기술 · 신종 제품'이란, 기존 IP카메라 · 영상정보 관리 · 저장제품에 비해 기능 · 형태가 현저히 달라 국가용 보안요구사항의 적용이 불가능한 제품을 의미합니다.

다만, '나'그룹 편성기관은 2022년 11월 1일부터 시행된 '新 보안적합성 검증체계'에서 발표한 정책에 따라 사전인증요건의 완화가 가능합니다.

이에 따라 '나'그룹 편성기관은 국내 시험기관에서 보안기능시험이 진행중[15]인 제품의 도입이 가능합니다. 다만, 도입한 제품이 다음 사항에 해당된다면 관계 중앙행정기관을 거치지 않고 국가정보원에 사후 검증을 직접 신청하여 전자정부법 제56조를 이행해야 합니다.

〈 국가정보원의 사후 검증이 필요한 경우 〉

① 영상정보처리기기 제품군에 속하는 신기술 · 신종제품이지만 △보안기능 확인서 △TTA보안인증서 중에서 어느 것도 획득하지 않은 제품을 도입한 경우

② 도입(계약일 기준) 당시, 국내에서 보안기능 시험이 진행중이었으나 결국 발급이 승인되지 아니한 경우

□ '다'그룹 편성 기관의 사전인증요건

'다'그룹 편성 기관은 제품 유형을 불문하고 자체 판단, 상위 그룹의 도입기준뿐 아니라 국내 · 외 다양한 인증제도 중에서 사전인증요건을 자율 지정[16], 도입할 수 있습니다.

(2) 도입기준 적용 원칙

□ 실제 설치기관 기준 원칙

사전인증요건은 도입하려는 제품이 실제 설치되는 기관을 기준으로 적용됩니다.

만약, 도입사업을 추진하는 기관과 제품이 설치된 기관이 다르다면 설치된 기관의 도입기준을 적용해야 합니다.

예를 들어, 도입 사업을 추진하는 기관이 보안적합성 검증 대상기관이지만, 실체 설치 · 운용되는 장소가 민간기관(시설)이라면 사전인증요건과 무관하게 도입할 수 있습니다.

---

15) 국가정보원이 영상정보처리기기 제품군에 대한 보안기능 시험기관으로 지정한 시험기관과 시험계약을 체결한 상태를 의미합니다. TTA가 자체 시행하는 '공공기관용 CCTV 보안성능품질 인증'에 대한 시험계약은 해당되지 않습니다.

16) '자율지정'이란, 다른 그룹의 사전인증요건과 무관하게 도입기관의 자체 판단에 의해 사전인증요건을 지정할 수 있음을 말합니다.

반대로 국가 · 공공기관이 민간업체로부터 영상정보처리기기 제품군이 포함된 물리 보안[17] 서비스를 제공받는다면 해당 서비스에 활용되는 제품은 각 그룹별 사전인증 요건을 준수해야 합니다. 아래 예시를 참고하시기 바랍니다.

〈 실제 설치기관 기준 원칙의 예시 〉

❶ 한국토지주택공사(일명, 'LH')가 '**OOO아파트 1공구 정보통신공사 CCTV 설치 사업**'을 추진하면서 일반 국민이 거주하는 'OOO아파트' 시설 관리를 위해 영상정보처리기기 제품군을 도입하는 경우

(**설명**) 한국토지주택공사는 '가'그룹에 편성된 기관이나, 제품이 일반 국민이 거주하는 아파트에 설치되므로 사전인증요건 적용 대상이 아님

❷ 경기도 용인교육지원청이 A社와 '**통합 CCTV보안관제 서비스**' 이용계약을 맺고 A社로부터 IP카메라와 NVR제품을 임대, 청사 건물 등에 설치, 운용

(**설명**) A社는 민간 업체이지만, 제품이 설치되는 기관인 경기도 용인교육지원청이 '나'그룹에 편성된 기관이므로 사전인증요건이 적용됨

□ 연동 전산망 · 설치 장소의 상위 그룹 기준 우선 원칙

제품이 실제 설치된 장소에 각기 다른 그룹 편성 기관이 혼재한다면 상위 그룹의 도입 기준을 적용합니다. 또한, 제품이 설치된 기관뿐 아니라 상위 그룹 편성기관의 전산망에 연동되거나 모니터링 또는 제어 권한이 부여된다면 상위 그룹의 도입기준을 적용합니다.

예를 들어 기초지자체 및 각급학교는 '다'그룹에 편성된 기관이지만, CCTV 영상을 상급 기관(광역지방자치단체 · 교육청 등)의 관제시스템 또는 경찰 · 소방기관과 연동, 공동 활용 한다면 '가'그룹 또는 '나'그룹의 도입기준을 적용합니다.

□ 도입기준의 상 · 하향 적용

영상정보처리기기 도입 기관은 편성된 그룹에 적용되는 도입기준에도 불구하고 사이버 보안 강화를 위해 필요하다고 판단할 경우 국가정보원과 사전 협의없이 자율 판단, 상위 그룹의 도입기준을 적용할 수 있습니다.

---

17) '물리 보안'이란, '주요 시설을 안전하게 운영하고 재난과 재해, 범죄 등을 방지하기 위한 보안 제품 및 보안 서비스'[국립국어원]를 의미합니다.

그러나, 편성된 그룹보다 하위 그룹의 도입기준 적용은 불가합니다.

(3) 영상정보처리기기의 안전한 운용

□ 안전성 유지를 위해 필요한 조치사항

영상정보처리기기 운용기관은 제품의 안전성 유지와 부실화 방지를 위해 개발업체가 제공하는 업데이트를 상시 적용하여 도입 당시의 보안기능이 훼손되거나 저하되지 않도록 제품을 유지 · 관리해야 합니다.

□ 형상변경 제품의 사전인증 반영 여부 결정 주체

운용중 업데이트 등으로 인한 제품의 형상변경은 불가피합니다. 이와 관련, 운용중 형상변경 사항의 사전인증 반영 여부는 운용기관이 아닌 인증서 보유기관[18]이 결정해야 합니다. 인증서 보유기관은 해당 사전인증의 갱신 내역을 운용기관에 통보할 수 있습니다.

(4) 도입기관이 가지는 재량 범위

□ 활용 목적에 따른 도입기준 적용 제외

국가 안보 · 방위 및 시설 · 인원 보안 등과 무관한 목적으로 설치 · 운용되는 영상정보처리기기는 다음 조건을 모두 만족할 경우, 도입 기관의 재량으로 보안기능 확인서 또는 TTA보안인증을 받지 않아도 도입할 수 있습니다.

〈 도입기준 적용 예외 조건 〉

❶ 보안상의 목적(△국가 안보 · 방위 △시설 · 출입 인원 보안 △치안 · 경비 · 공공 안전 등)으로 운용하지 않을 경우

(예시) △Dome 카메라중, 식물의 생장 관찰 목적으로 운용 △PTZ 카메라중, 쓰레기 무단투기 단속 목적으로 운용 △Machine vision 카메라중, 과금 · 과태료 부과(주차차량 번호 인식 · 과속단속 등)의 목적으로 운용

❷ 1번 항목의 목적으로 운용되는 IP카메라 관리 · 관제 네트워크에 연동하지 않고 독립적으로 운용하는 경우

18) '인증서 보유기관'이란, 보안기능 확인서 또는 TTA보안인증을 획득하거나 이의 사용권리를 양수하여 보유하고 있는 기관 또는 업체를 말합니다.

□ **도입기준 적용 제외 절차**

모든 국가 · 공공기관은 도입하는 영상정보처리기기에 대해 도입기준의 적용을 하지 않을 경우, 반드시 다음 절차를 거쳐야 합니다. 〈그림 8〉을 참고하십시오.

〈 그림 8. 도입기준 적용 제외 절차 〉

(1 단계) 제외 여부 판단	(2 단계) 보안성 검토	(3 단계) 결과 점검
❶ 도입사업 기획 단계에서 도입이 필요한 영상정보처리기기 유형을 선정 ❷ 운용 목적 · 전산망 연동 관계 등을 검토 , 도입기준 제외 조건 해당여부 판단	❶ 국가정보보안기본지침 제 14 조 제 1 항에 따라 보안성 검토 실시 - 보안성 검토 수행시 도입 제외 판단의 적절성 및 보안에 미치는 영향 등을 점검	❶ 보안성 검토 수행기관은 필요시 국가정보보안기본지침 제 18 조 제 2 항에 따라 보안성 검토결과 반영여부 확인을 위한 현장 점검 실시 - 보안성 검토사항과 일치 여부 등을 점검

2 사전인증요건 단계적 전환 일정 중요

(1) 사전인증요건 전환 시기

□ **보안기능 확인서 발급 대상 추가**

영상정보처리기기 제품군에 속하는 제품은 2024년 4월 1일부터 보안기능 확인서 발급 대상으로 추가됩니다. 관련 업체는 2024년 4월 1일부터 보안기능 시험 신청이 가능합니다.

□ **공공분야 도입에 필요한 사전인증요건 전환**

2028년 4월 1일부터 적용되는 영상정보처리기기 제품군의 사전인증요건은 다음과 같습니다. 〈표 4〉를 참고하십시오.

〈 표 4. '가', '나' 그룹 도입 영상정보처리기기 제품군 사전인증요건 〉

제품군	제품 유형	사전인증요건
영상정보처리기기 제품군	IP카메라	보안기능 확인서
	영상정보 저장 · 관리 제품	보안기능 확인서
	영상정보처리기기 제품군에 속한 신기술 · 신종 제품	(권장) 보안기능 확인서 (未발급제품은 도입후, 검증신청)

끝.