

신 · 구내용대비표

번호	세부항목	현 행	개 정 안
7	시험 및 인증기준	13 [필수] 사용자 인증  (중략)  ONVIF SOAP 사용자 인증을 WSSE UsernameToken의 Password Digest 인증 방식을 SHA-1 이상으로 사용해야 한다.	13 [필수] 사용자 인증  (중략)  <a href="#">ONVIF SOAP 사용자 인증(WSSE UsernameToken)</a> 을 지원하는 경우, Password Digest 인증 방식을 SHA-1 이상으로 사용해야 한다.
7	시험 및 인증기준	14 [필수] 인증 우회 취약점  (중략)  서버는 수신한 Digest 인증 요청에서 nc(nonce count) 값의 연속 증가를 확인해야 한다.  (없음)	14 [필수] 인증 우회 취약점  (중략)  <a href="#">Digest 인증을 지원할 경우, 사용자 인증 정보 재사용을 방지하기 위해</a> 수신한 Digest 인증 요청에서 nc(nonce count) 값의 연속 증가를 확인하거나, <a href="#">nonce의 유효한 사용횟수를 1회로 제한해야 한다.</a>  기타 다른 사용자 인증 방식을 사용하는 경우에도 사용자 인증 정보의 재사용은 방지되어야 한다.
10	인증 유효기간	(없음)	10. 인증 유효기간  인증 유효기간은 인증서의 인증연월일을 기준으로 3년으로 하며 2028년 3월 31일을 초과하지 않는다.  단, 2024년 3월 31일까지 발급된 인증서는 2027년 3월 31일까지 유효하다.
11	기타 사항	10 기타 사항  (시행일) 본 인증기준은 2023년 7월 1일부터 시행한다.  (중략)	11 기타 사항  (시행일) 본 인증기준은 <a href="#">2024년 4월 1일</a> 부터 시행한다.  (중략)

관리구분 : ☐관리본 ☐비관리본

문서번호 : TCP-2012/R09 : 2024

관리번호 :

# **공공기관용 IP카메라 보안 성능품질**

## **TTA Verified 인증 기준**

제·개정 이력 현황			
개정번호	제·개정일	개정쪽	제·개정내용
00	2017.12.22	-	인증 기준 마련에 따른 제정 (Ver. 1)
01	2018.06.12	P7~P8 P10 P10 P11 P11 P13 P15 P15 P15 P16 -	“5. 인증 유형” 추가 “6.11. 사용자 인증” 항목의 기준 내용 수정 “6.17. 원격 관리용 IP주소 지정 기능” 항목의 기준 내용 수정 “6.18. 원격관리서비스 활성화/비활성화 기능” 항목의 기준 내용 수정 “6.23. 일정시간 미사용시 세션 잠금/종료 기능” 항목의 기준 내용 수정 “6.37. 별도 서버와 연동 시 암호통신 수행 기능” 항목의 기준 내용 수정 “6.63. 영상 백업 시 암호화” 항목의 기준 내용 수정 “6.64. 상호연동” 항목의 참조 문서번호 현행화 “6.65. IP카메라 기능” 항목의 참조 문서번호 현행화 “7. 시험장비에 대한 제출 사항”에 포트 스캐닝 관련 사항 추가 “암호지원” 표현을 “(대분류) 암호지원”으로 변경
02	2019.04.16	P7 P7 P7	“5. 인증 유형” 삭제 “5. 파생 모델 판정 기준” 추가 “6. 동일 소프트웨어 모델 인증” 추가
03	2019.06.28	P7 P14 P16	“6. 동일 소프트웨어 모델 인증”의 적용 조건 변경 “7.64. 상호연동”, “7.65. IP카메라 기능” 항목을 “7.64. IP카메라 기능 및 상호연동”으로 통합하고 선택 항목으로 변경 “9. 인증 마크 표시” 성능품질 시험 여부에 따른 체크박스 표기 추가
04	2020.04.29	P8 P9 P9 P10 P10 P10	“6.2 동일 소프트웨어 모델”의 해시 비교 방법 추가 “7.1 최초 비밀번호 생성/변경 강제” 항목의 요구사항 추가 “7.2 최초 비밀번호 생성/변경 취약점 대응” 항목 추가 “7.8 에러 메시지에 인증 실패 사유 미포함 기능” 항목의 요구사항 추가 “7.10 비밀번호 암호화 저장 기능” 항목의 요구사항 추가 “7.11 비밀번호 읽기 방지 기능” 항목의 요구사항 변경

		P10	“7.12 비밀번호 임의 복구 기능 제한” 항목 추가
		P10	“7.13 사용자 인증” 항목의 요구사항 변경
		P11	“7.14 인증 우회 취약점 대응” 항목 추가
		P12	“7.22 DBMS 원격 접근 제한” 항목 추가
		P12	“7.23 웹 표준방식 지원” 항목을 필수로 변경, 요구사항 추가
		P12	“7.25 펌웨어/소프트웨어 버전 및 모델명 확인 기능” 항목의 요구사항 추가
		P12	“7.26 펌웨어/소프트웨어 업데이트 검증 기능” 항목의 요구사항 추가
		P12	“7.27 자동 업데이트 기능 제한” 항목 추가
		P12	“7.28 일정시간 미사용시 세션 잠금/종료 기능” 항목의 요구사항 변경
		P14	“7.45 OpenSSH, OpenSSL 버전 확인 기능” 항목의 요구사항 추가
		P15	“7.54 인증서/개인키/대칭키의 안전한 생성” 항목의 요구사항 추가
		P16	“7.66 영상 전송 시 암호화” 항목의 요구사항 변경
		P16	“7.68 오디오 데이터 저장 제한” 항목 추가
		-	“(대분류) 암호지원” 표현을 “암호지원 시험항목(15번, 16번)”으로 변경
05	21.06.29	P8	“6. 동일 소프트웨어 모델 인증” 내용 수정
		P10	“7.1 최초 비밀번호 생성/변경 강제” 인증기준 내용 추가
		P13	“7.23 웹 표준방식 지원” 항목을 필수로 변경
		P13	“7.26 펌웨어/소프트웨어 업데이트 검증 기능” 내용 수정
		P19	“10. 기타 사항” 의 7.23 시험항목 시행 날짜 문구 삭제
06	22.12.23	P10	“7.6 인증 실패 시 장비접속 제한기능” 인증기준 내용 추가
		P16	“7.55 암호 및 암호화키 하드코딩 방지 이행각서 공문” 인증기준 내용 추가
07	23.04.28	P8	5 파생 모델 판정 기준 추가 설명 6 동일 소프트웨어 모델 인증 내용 개정
		P22	[붙임 2] 파생 모델 확인서 추가
		P23	[붙임 3] 파생 모델 체크 사항 추가
		P24	[붙임 4] 동일 소프트웨어 모델 확인서 추가
		P26	[붙임 5] 동일 소프트웨어 모델의 동일성 확인 시험
08	23.06.09	P9	5 파생 모델 판정 기준 내용 수정
		P10	6.5 유의 사항 수정

		P22	사유 기재란 삭제, 책임 문구 및 별첨 문서 수정
			불임 문서 파생 모델 체크 사항 삭제
		P24	[불임 4] 동일 소프트웨어 모델 확인서 추가
		P26	[불임 5] 동일 소프트웨어 모델의 동일성 확인 시험
09	24.03.29	P12	“7.13 사용자 인증” 항목의 요구사항 변경
		P13	“7.14 인증 우회 취약점 대응” 항목의 요구사항 변경
		P20	“10 인증 유효기간” 내용 추가
		P20	“11 기타 사항” 시행일자 변경

## 목 차

1	적용 범위.....	6
2	관련 표준 및 규격.....	6
3	정의.....	6
4	시험 환경.....	8
5	파생 모델 판정 기준.....	9
6	동일 소프트웨어 모델 인증.....	9
7	시험 항목 및 인증 기준.....	11
8	시험대상장비에 대한 제출 사항.....	19
9	인증 마크 표시.....	20
10	인증 유효기간.....	20
11	기타 사항.....	20
[붙임 1]IP 카메라에 요구되는 감사데이터 .....		21
[붙임 2]파생 모델 확인서 .....		23
[붙임 3]동일 소프트웨어 모델 확인서 .....		24
[붙임 4]동일 소프트웨어 모델의 동일성 확인 시험 .....		26

## 1 적용 범위

본 문서는 정보통신 제품 및 서비스에 대한 인증 요령 제12조 및 공공기관용 영상정보 처리기기 보안 요구사항에 따라 IP카메라의 보안 성능품질에 대하여 기능 및 성능을 시험하고 인증하는 것을 적용범위로 한다.

## 2 관련 표준 및 규격

- [1] IETF RFC7616, HTTP Digest Access Authentication, September 2015.
- [2] IETF RFC5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008.
- [3] IETF RFC4492, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), May 2006.
- [4] IETF RFC3550, RTP:A Transport Protocol for Real-Time Applications, July 2003.
- [5] IETF RFC2326, Real Time Streaming Protocol (RTSP), April 1998.
- [6] IETF RFC4151, The Secure Shell (SSH) Protocol Architecture, January 2006.
- [7] IETF RFC4269, The SEED Encryption Algorithm, December 2005.
- [8] IEC 62676-2-3 Video surveillance systems for use in security application - Part 2-3: Video transmission protocols - IP interoperability implementation based on Web services, Edition 1.0, 2013. 11.
- [9] W3C, HTML5:A vocabulary and associated APIs for HTML and XHTML, Oct 2014.
- [10] KS X 1213-1, 128비트 블록 암호 알고리즘 ARIA – 제1부: 일반, 2009. 12.
- [11] KS X 1213-2, 128비트 블록 암호 알고리즘 ARIA – 제2부: 운용 모드, 2009. 12.
- [12] 영상정보 처리기기 설치·운영 가이드라인, 2015. 1., 행정자치부.
- [13] 영상보안시스템 상호연동 TTA Verified 인증 기준, TTA.
- [14] 영상보안시스템용 Full HD급 IP카메라 TTA Verified 인증 기준, TTA.
- [15] 영상보안시스템용 UHD급 IP카메라 TTA Verified 인증 기준, TTA.

## 3 정의

### 3.1 용어 정의

#### 시험대상장비(IP카메라)

이미지 센서로부터 획득한 영상 데이터를 IP 네트워크로 전송할 수 있는 영상정보처리기로 서버-클라이언트 모델에서 서버 역할을 수행한다. 구현 여부에 따라 SD카드 기반의 로컬 저장도 가능하며 원격 프로토콜(SSH 등), 웹 브라우저 등으로 접속 가능하다. 세부 유형으로는 Bullet, Dome, PTZ 카메라 등이 있다. IP카메라에 무선 통신 인터페이스가 존재하는 경우, 공장초기화 상태에서 비활성화되어 있어야 하며 최고 관리자만 무선 통신 인터페이스를 활성화/비활성화할 수 있어야 한다.

### 영상정보처리기기

일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치 및 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치로써 법 제2조제7호, 시행령 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 의미한다.

### 3.2 약어

<b>AES</b>	Advanced Encryption Standard
<b>ARIA</b>	Academy, Research Institute, Agency
<b>CCTV</b>	Closed Circuit Television
<b>CMS</b>	Client Management System
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DBMS</b>	Data Base Management System
<b>ECC</b>	Elliptic Curve Cryptosystems
<b>FTP</b>	File Transfer Protocol
<b>HTML5</b>	Hypertext Markup Language 5
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol over Secure Socket Layer
<b>IP</b>	Internet Protocol
<b>MD5</b>	Message-Digest algorithm 5
<b>NTP</b>	Network Time Protocol
<b>NVR</b>	Network Video Recorder
<b>PoE</b>	Power over Ethernet
<b>PTZ</b>	Pan, Tilt, Zoom
<b>RSA</b>	Rivest, Shamir, Adleman
<b>RTP</b>	Real Time Protocol
<b>RTSP</b>	Real Time Streaming Protocol
<b>SHA</b>	Secure Hash Algorithm
<b>SNMP</b>	Simple Network Management Protocol
<b>SOAP</b>	Simple Object Access Protocol
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Socket Layer
<b>TLS</b>	Transport Layer Security
<b>UHD</b>	Ultra High Definition
<b>VLAN</b>	Virtual Local Area Network
<b>VMS</b>	Video Management System
<b>WSSE</b>	Web Service Security



## 4 시험 환경

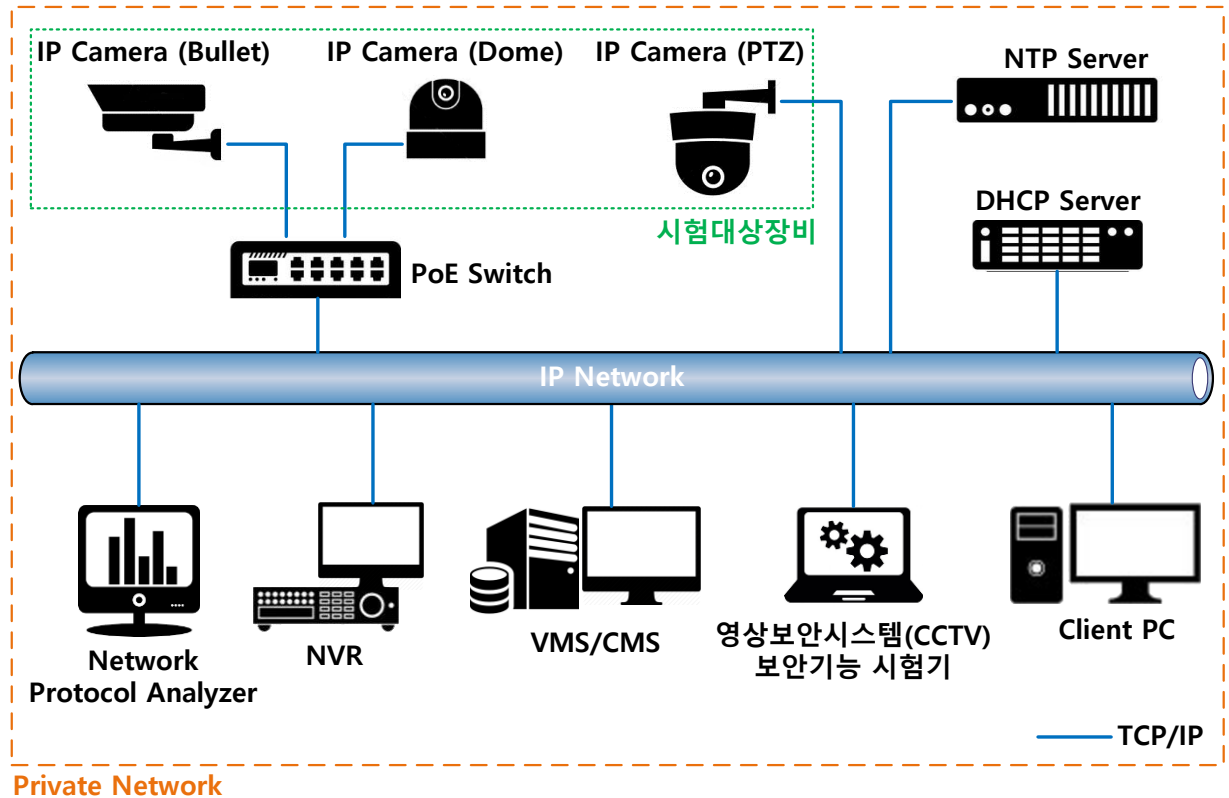


그림 1. 시험 환경 구성도

시험 환경 구성은 그림 1과 같다. 시험대상장비에 연결하는 NVR은 “공공기관용 NVR 보안 성능품질 TTA Verified 인증 기준”을 만족하는 장비를 활용한다. 시험대상장비인 IP카메라는 기본적으로 공장 초기화 상태에서 시험하고, 필요 시 장비의 설정을 변경하여 시험한다. 시험대상장비의 무선 통신 인터페이스 영역은 시험대상범위에서 제외한다.

## 5 파생 모델 판정 기준

파생 모델은 시험대상장비와 대비하여 아래의 요건을 모두 만족하는 경우에만 인정되며 파생 모델에 대한 시험은 진행하지 않는다.

- (1) 하드웨어 및 소프트웨어가 동일한 제품에 대해 모델명만 달리 사용하는 경우
- (2) KC 적합성 인증의 “방송통신기자재등의 적합등록 필증”에 기본 모델과 파생 모델이 등록되어 있어야 함

- ※ 파생 모델 확인서[붙임 2] 제출 필요
- ※ 파생 모델 확인서는 공문의 첨부 문서로 제출
- ※ 파생 모델의 사후 인정은 불가능함

## 6 동일 소프트웨어 모델 인증

### 6.1 기본 모델

“공공기관용 IP카메라 보안 성능품질 TTA Verified 인증기준”을 만족하는 제품을 기본 모델이라 하며, 아래와 같이 기본 모델을 나눈다.

- [기본 모델 1] “7.70 IP카메라 기능 및 상호연동 항목”을 선택하여 시험한 IP카메라  
[기본 모델 2] “7.70 IP카메라 기능 및 상호연동 항목”을 시험하지 않은 IP카메라

- ※ 기본 모델은 동일 소프트웨어 모델의 기능 범위(ex. PTZ, sd카드 저장 등)를 모두 포함해야 함, 단 보안 시험과 관련 없는 기능은 예외

### 6.2 동일 소프트웨어 모델

기본 모델과 서로 다른 하드웨어를 갖더라도 동일한 소프트웨어(펌웨어)를 사용하는 제품을 동일 소프트웨어 모델로 정의한다. 동일 소프트웨어 모델은 기본 모델과 소프트웨어(펌웨어) 해시 값(SHA-256 이상)이 동일해야 한다.

### 6.3 동일 소프트웨어 모델 인증

동일 소프트웨어 모델 인증은 “보안 동일 소프트웨어 모델 인증” 과 “보안 및 성능품질 동일 소프트웨어 모델 인증” 으로 구분한다. 구분에 따라 다음과 같은 요건을 만족해야 한다.

#### ■ 보안 동일 소프트웨어 모델 인증

- (1) 인증을 획득한 [기본 모델 1] 또는 [기본 모델 2]가 있어야 함
- (2) 동일 소프트웨어 모델은 동일성 확인 시험을 모두 만족해야 함

#### ■ 보안 및 성능품질 동일 소프트웨어 모델 인증

- (1) 인증을 획득한 [기본 모델 1] 이 있어야 함
- (2) 동일 소프트웨어 모델은 IP카메라 기능 항목(상호연동 시험 제외) 시험을 모두 만족해야 함
- (3) 동일 소프트웨어 모델은 동일성 확인 시험을 모두 만족해야 함

### 6.4 동일 소프트웨어 모델 인증 마크

보안 동일 소프트웨어 모델 인증 : 인증마크 보안 체크

보안 및 성능품질 동일 소프트웨어 모델 인증 : 인증마크 보안 및 성능품질 체크

### 6.5 유의 사항

- (1) 기본 모델과 동일 소프트웨어 모델의 인증시험을 동시에 진행할 수 있음
- (2) 자사 제품이 기본 모델인 경우 “동일 소프트웨어 모델 확인서 I”을 제출, 타사 제품이 기본 모델인 경우 “동일소프트웨어 모델 확인서 I,II” 제출 필요 [붙임 3]
- (3) 동일 소프트웨어 모델 확인서는 공문의 첨부 문서로 제출
- (4) 기본 모델 인증서의 인증기준 문서번호가 최신본이 아닐 경우, TTA는 인증기준의 개정 이력을 확인하여 동일 소프트웨어 모델 인증의 기본 모델 인정 여부를 판단할 수 있음
- (5) 동일 소프트웨어 모델 인증의 동일성 확인 시험 항목은 [붙임 4]를 참조

## 7 시험 항목 및 인증 기준

- [필수]: 인증을 위해 반드시 시험하는 항목
- [조건부필수]: 관련 기능이 구현된 경우에 반드시 시험하는 항목
- [선택]: 시험의뢰업체가 희망할 경우 시험하는 항목

대분류	중분류	번호	시험 항목	인증 기준
시험 및 인증	관리자 기본(default) 비밀번호 변경 기능	1	[필수] 최초 비밀번호 생성/변경 강제	<ul style="list-style-type: none"> <li>장비를 공장 초기화한 후 최초 장비 접속 및 최초 서비스 접속 시 관리자 기본(Default) 비밀번호에 대해 아래의 사항을 만족해야 한다. <ul style="list-style-type: none"> <li>관리자 기본(Default) 비밀번호가 있는 경우, 비밀번호 변경이 강제되어야 함</li> <li>관리자 기본(Default) 비밀번호가 없는 경우, 비밀번호 생성이 강제되어야 함</li> </ul> </li> <li>“방송통신기자재등의 적합등록 필증”을 받은 경우 본 시험 항목의 인증 기준을 만족하는 것으로 한다. <ol style="list-style-type: none"> <li>장비 접속 <ul style="list-style-type: none"> <li>웹 브라우저, 로컬 콘솔 등</li> </ul> </li> <li>서비스 접속 <ul style="list-style-type: none"> <li>SSH, HTTP, HTTPS, RTSP, FTP, TELNET, SNMP 등</li> </ul> </li> </ol> </li> </ul>
		2	[필수] 최초 비밀번호 생성/변경 취약점 대응	<ul style="list-style-type: none"> <li>최초 비밀번호 생성/변경 기능이 일반적인 비밀번호 생성/변경 기능과 동일하지 않은 경우, 해당 기능은 공장초기화 이후 처음 1 회만 동작해야 한다.</li> <li>최초 비밀번호 생성/변경 기능이 일반적인 비밀번호 생성/변경 기능과 동일한 경우, 해당 기능의 반복 동작이 허용되지만 반드시 안전한 사용자 인증이 요구되어야 한다.</li> </ul>
	안전한 비밀번호 설정 기능	3	[필수] 비밀번호 조합 구성	<ul style="list-style-type: none"> <li>생성하는 비밀번호는 9 자리 이상이어야 한다.</li> <li>숫자, 영문 대문자, 영문 소문자, 특수문자 중 3 가지 조합 이상으로 비밀번호를 생성할 수 있어야 한다. <ul style="list-style-type: none"> <li>숫자(0-9)</li> <li>영문자 대문자(A-Z)</li> <li>영문자 소문자(a-z)</li> <li>특수문자(!, @, #, \$, %, ^, &amp;, *, (, ) 등)</li> </ul> </li> </ul>
		4	[선택] 비밀번호 최소길이 설정	<ul style="list-style-type: none"> <li>비밀번호의 최소 길이를 관리자가 설정할 수 있는 기능을 제공해야 한다.</li> </ul> <p>※ 최소 길이의 기본값은 9 자리 이상이어야 한다.</p>
		5	[선택] 비밀번호 15 자리 이상 입력가능	<ul style="list-style-type: none"> <li>비밀번호는 15 자리 이상 입력이 가능해야 한다.</li> </ul>
	인증 실패 대응 기능	6	[필수] 인증 실패 시 장비접속 제한기능	<ul style="list-style-type: none"> <li>지정된 횟수(기본값 5 회 이하) 이상 인증 실패 시 일정 시간 (기본값 5 분 이상) 장비 접속을 제한하는 기능을 제공해야 한다. <ul style="list-style-type: none"> <li>On/Off 기능이 있는 경우 Default ON</li> </ul> </li> </ul>

대분류	중분류	번호	시험 항목	인증 기준
		7	[선택] 인증 실패 시 장비접속 제한시간 설정기능	<ul style="list-style-type: none"> <li>인증 실패 시 장비 접속 제한 시간을 관리자가 설정할 수 있는 기능을 제공해야 한다.</li> </ul>
		8	[필수] 에러 메시지에 인증 실패 사유 미포함 기능	<ul style="list-style-type: none"> <li>인증 실패 시 인증 실패 사유를 에러 메시지에 포함하지 않아야 한다. (인증 실패 사유 예시) - 잘못된 계정을 입력하였습니다. - 잘못된 비밀번호를 입력하였습니다.</li> <li>※ UI 뿐만 아니라 네트워크 상의 응답 메시지에도 실패 사유가 포함되지 않아야 한다.</li> </ul>
	인증 피드백 보호 기능	9	[필수] 입력 비밀번호 마스킹 기능	<ul style="list-style-type: none"> <li>입력되는 비밀번호를 화면에서 볼 수 없도록 마스킹하는 기능을 제공해야 한다.</li> </ul>
	인증 데이터 보호 기능	10	[필수] 비밀번호 암호화 저장 기능	<ul style="list-style-type: none"> <li>비밀번호를 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다.</li> <li>장비에서 백업할 수 있는 설정 파일 등에 비밀번호가 포함된 경우, 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다.</li> <li>웹 브라우저 등을 통해 장비 외부에서 비밀번호를 설정 받을 시 이를 암호 알고리즘(비대칭키 암호 등)을 이용하여 안전하게 전송해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
		11	[필수] 비밀정보 읽기 방지 기능	<ul style="list-style-type: none"> <li>장비에 저장된 모든 비밀정보(비밀번호, 대칭키, 개인키 등)를 읽거나 유출할 수 없어야 한다.</li> <li>비밀정보에 대한 평문 처리 및 Base64 단순 인코딩 등은 제한한다.</li> </ul>
		12	[필수] 비밀번호 임의 복구 기능 제한	<ul style="list-style-type: none"> <li>비밀번호 찾기 또는 2 차 비밀번호 등의 임의 복구 기능을 사용할 수 없어야 한다.</li> </ul>
	사용자 인증	13	[필수] 사용자 인증	<ul style="list-style-type: none"> <li>ONVIF HTTP Digest 사용자 인증을 지원하는 경우, Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다.</li> <li>RTSP Digest 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다.</li> <li>ONVIF SOAP 사용자 인증(WSSSE UsernameToken)을 지원하는 경우, Password Digest 인증 방식을 SHA-1 이상으로 사용해야 한다.</li> <li>기타 사용자 인증 방식은 암호지원 시험항목(15번, 16번)을 참조하여 안전한 방식을 사용해야 한다.</li> </ul>

대분류	중분류	번호	시험 항목	인증 기준
		14	[필수] 인증 우회 취약점 대응	<ul style="list-style-type: none"> <li>• 웹 브라우저와 원격 관리 통신 시 안전한 사용자 인증 절차 없이 세션 정보(세션 ID 등)만으로 인증 여부를 판단하지 않아야 한다.</li> <li>• 세션 정보에 계정 권한 정보가 포함되어 있는 경우, 해당 정보를 위·변조하여 권한 상승 등의 월권 행위를 할 수 없어야 한다.</li> <li>• Digest 인증의 nonce 등 서버가 생성한 인증 정보는 세션 만료 또는 재부팅 시 함께 만료되어야 한다.</li> <li>• <u>Digest 인증을 지원할 경우, 사용자 인증 정보 재사용을 방지하기 위해</u> 수신한 Digest 인증 요청에서 nc(nonce count) 값의 연속 증가를 확인하거나, <u>nonce의 유효한 사용횟수를 1 회로 제한해야 한다.</u></li> <li>• 기타 다른 사용자 인증 방식을 사용하는 경우에도, 사용자 인증 정보의 재사용은 방지되어야 한다.</li> </ul>
암호 지원	암호사용	15	[필수] 암호 알고리즘 보안 강도 만족 여부	<ul style="list-style-type: none"> <li>• 암호화 및 해시 알고리즘의 보안강도는 112bit 급 이상을 만족해야 한다. <ul style="list-style-type: none"> <li>※ 알고리즘의 보안강도는 한국인터넷진흥원의 “암호 알고리즘 및 키 길이 이용 안내서” 최신본을 참조 (예시) <ul style="list-style-type: none"> <li>- 해시(SHA-224/256/384/512)</li> <li>- 대칭키암호(SEED, ARIA-128/192/256, AES-128/192/256)</li> <li>- 공개키암호(RSA 2048)</li> <li>- 전자서명(RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA)</li> </ul> </li> </ul> </li> </ul>
		16	[선택] 국가용 암호 알고리즘 사용 여부	<ul style="list-style-type: none"> <li>• 국가용 암호 알고리즘의 사용을 권고한다. <ul style="list-style-type: none"> <li>- 국정원장 승인 알고리즘, 국가사이버안보센터 안내 참조</li> </ul> </li> </ul>
정보 흐름 통제	트래픽 제어	17	[선택] VLAN 기능	<ul style="list-style-type: none"> <li>• VLAN 기능 제공시 IEEE Std 802.1q-2011 이상을 지원해야 한다.</li> </ul>
		18	[필수] IP Filtering 기능	<ul style="list-style-type: none"> <li>• 특정 IP 주소에서의 접속을 허용/차단할 수 있는 기능을 제공해야 한다.</li> <li>※ Black List(Deny), White List(Allow) 동작 확인</li> </ul>
		19	[선택] ACL 기능	<ul style="list-style-type: none"> <li>• 장비별 다음과 같은 ACL 기능을 제공해야 한다. <ul style="list-style-type: none"> <li>- Source IP Address 정보 또는 Source Port Number 정보</li> </ul> </li> </ul>
보안 관리	장비 관리용 원격 접속 IP 주소 제한 기능	20	[필수] 원격 관리용 IP 주소 지정 기능	<ul style="list-style-type: none"> <li>• 원격 관리 서비스 용도의 IP 주소를 지정하는 기능을 제공해야 한다.</li> <li>※ IP 주소 지정은 대역이 아닌 개별 주소 단위로 등록 가능해야 함</li> <li>※ 원격 관리: 관리자 계정으로 접속하여 설정을 변경 하거나 PTZ를 제어하는 원격 세션의 모든 활동</li> </ul>

대분류	중분류	번호	시험 항목	인증 기준
	원격 관리 기능	21	[필수] 원격관리서비스 활성화/비활성화 기능	<ul style="list-style-type: none"> <li>공장 초기화 상태에서 원격 관리 서비스는 비활성화되어 있어야 하며 아래는 예외 사항으로 적용한다. <ul style="list-style-type: none"> <li>로컬 콘솔 포트가 없는 경우: HTTPS 만 활성화 허용</li> <li>로컬 콘솔 포트가 있는 경우: HTTPS 도 활성화 금지</li> </ul> </li> <li>관리자가 원할 때 원격 관리 서비스를 활성화/비활성화 할 수 있는 기능을 제공해야 한다. <ul style="list-style-type: none"> <li>원격 관리 서비스: SSH, HTTP, HTTPS, FTP, TELNET, SNMP 등</li> </ul> </li> </ul>
		22	[필수] DBMS 원격 접근 제한	<ul style="list-style-type: none"> <li>장비에서 운용되는 DBMS 에 대해 원격에서 직접 접근하는 것은 제한되어야 한다.</li> </ul>
		23	[필수] 웹 표준방식 지원	<ul style="list-style-type: none"> <li>HTML5 등의 웹 표준방식을 지원해야 한다.</li> </ul> <p>※ 영상(Video/Audio)에 관련되지 않은 웹 브라우저 동작을 위해 플러그인(ActiveX, EXE 등)을 사용하지 않아야 한다.</p>
		24	[조건부필수] SNMP V3 지원 기능	<ul style="list-style-type: none"> <li>SNMP 를 지원하는 경우, SNMP 는 V3 이상을 지원해야 한다. <ul style="list-style-type: none"> <li>암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul> </li> </ul>
	펌웨어 업데이트 관리 기능	25	[필수] 펌웨어/소프트웨어 버전 및 모델명 확인 기능	<ul style="list-style-type: none"> <li>펌웨어/소프트웨어의 현재 버전을 확인할 수 있는 기능을 제공해야 한다.</li> <li>시험대상장비의 UI 에서 모델명을 확인할 수 있어야 한다.</li> </ul>
		26	[필수] 펌웨어/소프트웨어 업데이트 검증 기능	<ul style="list-style-type: none"> <li>펌웨어/소프트웨어에 대한 해시 값 정보(모델명, 펌웨어/소프트웨어 파일명, 버전 정보 포함)를 홈페이지에 게시해야 한다. <ul style="list-style-type: none"> <li>암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조 (MD5 등 사용제한, SHA256 이상 사용권고)</li> </ul> </li> </ul>
		27	[필수] 자동 업데이트 기능 제한	<ul style="list-style-type: none"> <li>기본 설정 상태에서 자동 업데이트 기능을 사용할 수 없어야 한다.</li> </ul>
	세션 관리 기능	28	[필수] 일정시간 미사용시 세션 잠금/종료 기능	<ul style="list-style-type: none"> <li>일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료 하는 기능을 제공해야 한다. <ul style="list-style-type: none"> <li>Default ON, 기본값 10분 이하</li> </ul> </li> </ul> <p>※ 본 항목의 기능은 ON/OFF가 허용됨</p> <p>※ 관리자 활동: 관리자 계정으로 접속하여 설정을 변경 하거나 PTZ를 제어하는 로컬/원격 세션의 모든 활동</p>
	관리자의 동시 원격 접속 세션 제한	29	[선택] 동시접속 세션 수 제한 기능	<ul style="list-style-type: none"> <li>시험대상장비에 원격으로 접속하는 관리자의 동시 접속 세션을 하나만 허용하거나 동시 접속 세션 수를 제한 기능을 제공해야 한다.</li> </ul> <p>※ 본 항목의 기능은 ON/OFF가 허용됨</p>

대분류	중분류	번호	시험 항목	인증 기준
자체 시험	오류 검사 기능 ※ 제조업체에서 주요 프로세스를 사전정의 후 TTA와 시험협의	30	[조건부 필수] 하드웨어 자체검사 기능	<ul style="list-style-type: none"> <li>Embedded-HW 형 장비에 한하여, 장비 구동 시(Power On) 주요 하드웨어에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - CPU, 메모리, 플래시 메모리, 네트워크 인터페이스 등</li> </ul> ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함
		31	[필수] 소프트웨어 자체검사 기능	<ul style="list-style-type: none"> <li>장비 구동시(Power On) 또는 어플리케이션 로딩 후 주요 프로세스에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - 식별 및 인증 프로세스 - 정보흐름통제 프로세스 - 보안관리 프로세스 등</li> </ul> ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함
		32	[필수] 자체검사 내용 및 결과 확인 기능	<ul style="list-style-type: none"> <li>시험대상장비가 수행한 자체검사 내용 및 결과를 관리자가 확인할 수 있는 기능을 제공해야 한다. (예시) - 화면 출력 - 디스플레이 화면 - 감사데이터 생성 등</li> </ul>
		33	[선택] 자체검사 실행 기능	<ul style="list-style-type: none"> <li>관리자가 항목 30,31의 자체검사를 직접 실행하는 기능을 제공해야 한다.</li> </ul>
	무결성 검사 기능	34	[선택] 소프트웨어 무결성 검사 기능	<ul style="list-style-type: none"> <li>시험대상장비 구동 시(Power On) 또는 구동 이후 주요 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다.</li> </ul> ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함
		35	[선택] 무결성 검사 실행 기능	<ul style="list-style-type: none"> <li>관리자가 소프트웨어 무결성 검사를 직접 실행하는 기능을 제공해야 한다.</li> </ul>
		36	[선택] 설정 백업/복원시 무결성 검사 기능	<ul style="list-style-type: none"> <li>장비 설정 백업/복원 시 설정 파일에 대한 무결성 검사 기능을 제공해야 한다.</li> </ul>
접근 통제	접근 통제 기능	37	[필수] 계정별 접근권한 설정 기능	<ul style="list-style-type: none"> <li>관리자 계정별 접근권한을 설정하는 기능을 제공해야 한다.</li> </ul>
		38	[조건부필수] 운영모드 변경용 비밀번호 생성 기능	<ul style="list-style-type: none"> <li>운영모드 변경이 가능할 경우, 운영모드 변경용 비밀번호를 관리자가 생성/재설정할 수 있는 기능을 제공해야 한다.</li> </ul> ※ 비밀번호 생성 관련 부분은 안전한 비밀번호 설정 기능을 참고



대분류	중분류	번호	시험 항목	인증 기준
		39	[조건부필수] 운영모드 변경 시 추가 인증 기능	<ul style="list-style-type: none"> <li>운영모드 변경이 가능할 경우, 운영모드 변경 시 추가 인증을 수행하는 기능을 제공해야 한다.</li> </ul>
		40	[선택] 중요 명령 사용 제한 기능	<ul style="list-style-type: none"> <li>장비 상태를 변경하는 중요 명령(기능)에 대한 접근은 로컬 콘솔(콘솔포트 연결)로 제한하는 기능을 제공해야 한다. (중요 명령) - 재부팅, 디버깅(부트로姆 접속, 메모리 수정/덤프)</li> </ul>
전송 데이터 보호	제품과 원격으로 연결된 모든 통신 수단간 안전한 암호통신 프로토콜 사용	41	[필수] 원격 접속시 암호통신 수행 기능	<ul style="list-style-type: none"> <li>원격으로 접속 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. (예시) - HTTPS, SSL/TLS, SSH - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
		42	[조건부 필수] 별도 서버와 연동시 암호통신 수행 기능	<ul style="list-style-type: none"> <li>별도 서버(로그서버 등)와 원격으로 장비 연동 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. (예시) - HTTPS, SSL/TLS, SSH - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
		43	[필수] TLS 1.2 이상 지원 기능	<ul style="list-style-type: none"> <li>TLS 프로토콜은 TLS 1.2(RFC 5246) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
		44	[조건부필수] SSH 2.0 이상 지원 기능	<ul style="list-style-type: none"> <li>SSH 를 지원하는 경우, 프로토콜은 SSH v2(RFC 4251~4254) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
	OpenSSH, OpenSSL 버전 확인	45	[필수] OpenSSH, OpenSSL 버전 확인 기능	<ul style="list-style-type: none"> <li>암호통신을 위해 OpenSSH, OpenSSL 을 사용하는 경우 버전을 확인하는 기능을 제공해야 한다.</li> <li>버전의 표기는 패치 버전 정보를 포함해야 한다.</li> </ul>
감사 기록	감사데이터 생성 기능	46	[필수] 감사데이터 생성 기능	<ul style="list-style-type: none"> <li>"불임"에 해당하는 감사 데이터들을 생성하는 기능을 제공해야 한다.</li> </ul> <p>※ 감사 데이터 세부내역은 "[불임 1]" 참조</p>
	감사데이터에 최소 정보 포함 여부	47	[필수] 감사데이터에 최소 정보 포함 기능	<ul style="list-style-type: none"> <li>감사데이터에는 최소한 다음의 정보가 포함되어야 한다. <ul style="list-style-type: none"> <li>- 사건 발생 일시</li> <li>- 사건 유형</li> <li>- 사건 발생 주체(ID, IP 주소)</li> <li>- 사건의 결과(성공 또는 실패)</li> </ul> </li> </ul>
	감사증적의 크기가 제한용량 초과시 대응 행동	48	[필수] 감사 증적 초과시 관리자 확인 기능	<ul style="list-style-type: none"> <li>감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 관리자가 알 수 있는 기능을 제공해야 한다.</li> </ul>
		49	[필수] 감사 증적 초과시 대처 조치 기능	<ul style="list-style-type: none"> <li>감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 '외부로 로그 백업 또는 오래된 내용 덮어쓰기' 등 대처 조치를 해야 한다.</li> </ul>

대분류	중분류	번호	시험 항목	인증 기준
	감사데이터 보호	50	[선택] 외부 로그 서버 전송 기능	<ul style="list-style-type: none"> <li>감사데이터를 외부 로그 서버로 전송하는 기능을 제공해야 한다.</li> </ul>
		51	[필수] 감사 데이터 접근 제한 기능	<ul style="list-style-type: none"> <li>인가된 관리자만 감사데이터에 접근할 수 있어야 한다.</li> </ul>
		52	[선택] 감사 데이터 암호화 저장 기능	<ul style="list-style-type: none"> <li>감사데이터를 장비 내부에 저장할 경우 암호화하여 저장하는 기능을 제공해야 한다.</li> <li>- 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
인증서 관리	개인키 암호화 저장 확인	53	[필수] 개인키 암호화 저장 기능	<ul style="list-style-type: none"> <li>장비 내에 저장된 개인키는 암호화되어 저장되어야 한다.</li> <li>- 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조</li> </ul>
	인증서/개인키/대칭키 확인	54	[필수] 인증서/개인키/대칭키의 안전한 생성	<ul style="list-style-type: none"> <li>장비 내에서 인증서/개인키/대칭키를 생성하는 경우, 안전한 방법으로 생성해야 하며, 인증서/개인키/대칭키의 하드코딩 및 장비간 공통된 개인키/대칭키의 일괄 사용을 하지 않아야 한다.</li> </ul>
인증심의 항목	무단은닉 하드코딩 방지 이행	55	[필수] 암호 및 암호화키 하드코딩 방지 이행각서 공문	<ul style="list-style-type: none"> <li>이행각서 공문 접수               <ul style="list-style-type: none"> <li>- 주내용 : 방지 이행 약속 및 불이행시 관련 제품군에 대한 인증 취소 사전동의 (공문 내용)</li> <li>- "무단은닉 및 하드코딩된 암호 및 암호화키 없음" 선언</li> <li>- "운용 모드 변경 (개발자/디버깅 모드) 관련 유/무" 선언</li> <li>- "보안 및 성능품질 열화행위 하지 않음" 선언</li> <li>- "백도어 없음" 선언</li> <li>- "국내외 정보보호 전문기관에서 공지된 취약점은 해결되었음" 을 선언</li> </ul> </li> </ul>
	채증 자료 제출	56	[필수] 구동 소프트웨어 채증 자료 제출	<ul style="list-style-type: none"> <li>시험당시 구동 소프트웨어(어플리케이션 등) 해시 값 파일 제출</li> <li>※ 소스코드가 아닌 원본 소프트웨어 검증용 해시 값 또는 펌웨어 파일, 설치 파일 제출</li> </ul>
영상 전송 기본기능	표준 프로토콜-RTSP	57	[필수] 지원 명령어 확인	<ul style="list-style-type: none"> <li>OPTIONS 메시지로 지원하는 RTSP 명령어가 확인되어야 한다.</li> </ul>
		58	[필수] 세션 확인	<ul style="list-style-type: none"> <li>DESCRIBE 메시지로 제공 가능한 세션 내역이 확인 되어야 한다.</li> </ul>
		59	[필수] 연결 설정	<ul style="list-style-type: none"> <li>SETUP 메시지로 원하는 세션 연결 설정이 가능해야 한다.</li> </ul>
		60	[필수] 전송 시작	<ul style="list-style-type: none"> <li>PLAY 메시지로 영상 데이터 전송을 시작할 수 있어야 한다.</li> </ul>
		61	[필수] 전송 종료	<ul style="list-style-type: none"> <li>TEARDOWN 메시지로 영상 데이터 전송을 종료할 수 있어야 한다.</li> </ul>

대분류	중분류	번호	시험 항목	인증 기준
영상 전송 보안	TLS 제어 암호화	62	[필수] 기본 Flow 적용	• TLS 표준상의 기본 Flow가 적용되는지 확인한다.
		63	[필수] 인증서 적용	• TLS 연결 과정에서 서버 측의 인증서가 클라이언트에게 전달되는 지 확인한다. • Certificate Request 를 지원하는 경우, TLS 연결 과정에서 클라이언트 측의 인증서가 서버로 전달되는 지 확인한다.
		64	[선택] 전자서명	• TLS 연결 과정에서 전자서명 역할을 하는 Certificate Verify를 전송하는 지를 확인한다.
		65	[필수] 국제 표준 암호 알고리즘 수용 및 협상	• 적용된 암호화 알고리즘이 2 개 이상일 경우, 상호간 협상에 의하여 우선순위에 따라 암호화 알고리즘을 선택하여 적용하는 지를 확인한다. ECC 적용 장비의 경우, 별도 규격인 IETF RFC 4492 규격을 준용하여 파라미터 및 키를 생성하고 전송하는 지 확인한다.
	영상 전송 보안	66	[필수] 영상 전송 시 암호화	• 웹 브라우저 등에 영상을 전송하기 위한 암호통신 프로토콜 기반의 신뢰된 채널을 제공해야 한다. - (예시) HTTPS, TLS • HTTPS Tunneling(RTP/RTSP/HTTPS/TCP) 방식으로 영상 데이터를 송신할 수 있어야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조
영상 저장 보안	영상 저장 시 암호화	67	[선택] 영상 저장 시 암호화	• 영상 데이터를 장비 내부에 저장할 경우 암호화하여 저장해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조
	오디오 데이터 저장 제한	68	[필수] 오디오 데이터 저장 제한	• 기본 설정 상태에서 오디오 데이터 저장 기능을 사용할 수 없어야 한다.
영상 백업 보안	영상 백업 시 암호화	69	[조건부 필수] 영상 백업 시 암호화	• <u>장비에 저장된 영상 데이터를 외부로 백업/다운로드하는 것이 가능한 경우</u> , 암호화하여 백업/다운로드해야 한다. • 백업/다운로드하는 영상 데이터에 대한 무결성 검증 값 생성 및 확인이 가능해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(15번, 16번) 참조
성능품질	성능품질	70	[선택] IP카메라 기능 및 상호연동	• 시험대상장비는 지원하는 해상도에 따라 "영상보안시스템용 Full HD 급 IP 카메라 TTA Verified 인증 기준(TCP-2006)" 또는 "영상보안시스템용 UHD 급 IP 카메라 TTA Verified 인증 기준(TCP-2011)"을 만족해야 한다.  ※ 위 인증기준은 최신 개정본을 따름  ※ 위 인증기준의 "영상보안시스템용 IP 카메라 보안" 항목은 시험범위에서 제외함

## 8 시험대상장비에 대한 제출 사항

시험의뢰업체는 시험대상장비의 시험을 위해 아래와 같은 사항을 제출해야 한다.

항목	제시 내용
기본(Default) 비밀번호	<ul style="list-style-type: none"><li>기본(Default) 비밀번호가 존재하는 경우, 해당 정보 제출<ul style="list-style-type: none"><li>지원하는 원격 서비스 (SSH, SNMP 등)에 대한 기본(Default) 비밀번호 정보 포함</li><li>Web Server, DBMS 등에 접속 시 사용되는 기본(Default) 비밀번호 정보 포함</li></ul></li></ul>
포트 스캐닝 결과	<ul style="list-style-type: none"><li>장비에서 사용하는 포트 내역에 대한 내·외부 포트 스캐닝 결과 제출</li></ul>
제품 설명서(안내서)	<ul style="list-style-type: none"><li>제품의 전반적인 기능에 대한 상세</li></ul>
오류 검사 프로세스 설명 자료	<ul style="list-style-type: none"><li>하드웨어/소프트웨어 자체검사에 대한 상세</li></ul>
이행각서 [공문]	<ul style="list-style-type: none"><li>하기 내용을 포함해야 함<ul style="list-style-type: none"><li>"무단은닉 및 하드코딩된 암호 및 암호화키 없음" 선언</li><li>"운용 모드 변경 (개발자/디버깅 모드) 관련 유/무" 선언</li><li>"보안 및 성능품질 열화행위 하지 않음" 선언</li><li>"백도어 없음" 선언</li><li>"국내외 정보보호 전문기관에서 공지된 취약점은 해결되었음"을 선언</li></ul></li></ul>
구동 소프트웨어 채증 자료	<ul style="list-style-type: none"><li>하기 사항 중 1개 이상 제출<ul style="list-style-type: none"><li>펌웨어</li><li>펌웨어에 대한 해시값</li><li>소프트웨어 설치파일</li></ul></li></ul>

## 9 인증 마크 표시

인증된 제품에 대해서는 TTA Verified 마크의 사용을 승인한다. 이 로고는 TTA의 공공기관용 IP카메라 보안 성능품질 규격 시험 인증에 통과되어 TTA Verified 인증을 획득한 제품에만 부착이 허용된다. 시험 항목 및 인증 기준이 추가되는 중요 개정 이력이 발생할 경우, 인증 Version 번호가 증가될 수 있으며(예. Ver. 2, Ver. 3) 관련 내용 및 이력은 제·개정 이력 현황을 참조한다. 인증 마크의 체크박스 표기는 “7.70 IP카메라 기능 및 상호연동” 항목 시험 여부에 따라 결정된다.



## 10 인증 유효기간

인증 유효기간은 인증서의 인증연월일을 기준으로 3년으로 하며 2028년 3월 31일을 초과하지 않는다. 단, 2024년 3월 31일까지 발급된 인증서는 2027년 3월 31일까지 유효하다.

## 11 기타 사항

(시행일) 본 인증기준은 2024년 4월 1일부터 시행한다.

(경과조치) 이 기준의 시행 이전에 처리된 사항에 대해서는 이 기준에 의해 처리된 것으로 한다.

## [붙임 1] IP카메라에 요구되는 감사데이터

분류	로그 종류	기준
사용자 접근	[필수] 로그인	<ul style="list-style-type: none"><li>발생조건: 사용자의 정상 로그인 성공 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간</li></ul>
	[필수] 로그인 실패	<ul style="list-style-type: none"><li>발생조건: 사용자의 로그인 실패 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간</li></ul>
	[필수] 로그인 잠금	<ul style="list-style-type: none"><li>발생조건: 사용자가 지정된 횟수 이상 로그인 실패 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 계정 잠금 결과</li></ul>
	[조건부 필수] 로그아웃	<ul style="list-style-type: none"><li>발생조건: 사용자 로그아웃 동작 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 로그아웃 성공 여부</li></ul>
영상 백업	[조건부 필수] 시작	<ul style="list-style-type: none"><li>발생조건: 영상 백업 시작 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 백업하는 영상 채널 정보</li></ul>
	[조건부 필수] 종료 및 해시	<ul style="list-style-type: none"><li>발생조건: 영상 백업 종료 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 백업하는 영상 채널 및 구간 정보, 무결성 검증 정보(해시값)</li></ul>
사용자 계정관리	[필수] 사용자 계정 추가	<ul style="list-style-type: none"><li>발생조건: 사용자 계정 추가 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 추가한 사용자 정보</li></ul>
	[필수] 사용자 계정 삭제	<ul style="list-style-type: none"><li>발생조건: 사용자 계정 삭제 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 삭제한 사용자 정보</li></ul>
	[필수] 사용자 계정 정보 변경	<ul style="list-style-type: none"><li>발생조건: 사용자 계정의 정보 변경 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 사용자 정보</li></ul> <p>※ 사용자 계정 정보: 패스워드, 계정 권한 등</p>
PTZ 제어	[조건부 필수] PTZ 제어 시작	<ul style="list-style-type: none"><li>발생조건: PTZ 제어 시작 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 동작 성공여부</li></ul> <p>※ PTZ 카메라 및 광학 Zoom 기능이 있는 카메라는 필수로 적용</p>
	[조건부 필수] PTZ 제어 종료	<ul style="list-style-type: none"><li>발생조건: PTZ 제어 종료 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 동작 성공여부</li></ul> <p>※ PTZ 카메라 및 광학 Zoom 기능이 있는 카메라는 필수로 적용</p>
트래픽 제어 설정	[필수] IP Filtering	<ul style="list-style-type: none"><li>발생조건: IP Filtering 관련 설정 변경 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li></ul>
	[선택] ACL	<ul style="list-style-type: none"><li>발생조건: ACL 관련 설정 변경 시</li><li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li></ul>

분류	로그 종류	기준
원격 관리 설정	[필수] 원격 관리용 IP주소 설정	<ul style="list-style-type: none"> <li>발생조건: 원격 관리용 IP주소 설정 변경 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li> </ul>
	[필수] 원격 관리 서비스 설정	<ul style="list-style-type: none"> <li>발생조건: 원격 관리 서비스 활성화/비활성화 관련 설정 변경 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li> </ul>
관리자 세션 관리	[필수] 관리자 세션 잠금/종료	<ul style="list-style-type: none"> <li>발생조건: 일정시간 동안 동작이 없는 관리자 세션 잠금/종료 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 잠금/종료 결과</li> </ul>
	[선택] 관리자 동시접속 제한	<ul style="list-style-type: none"> <li>발생조건: 원격 동시접속 세션 수 제한 설정 변경 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li> </ul>
무결성 검사	[선택] 소프트웨어 무결성	<ul style="list-style-type: none"> <li>발생조건: 소프트웨어 무결성 검사 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 검사 결과, 무결성 검증 정보(해시값)</li> </ul>
	[선택] 설정 백업/복원 무결성	<ul style="list-style-type: none"> <li>발생조건: 설정 백업/복원 과정에서 무결성 검사 수행 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 무결성 검증 정보(해시값)</li> </ul>
환경 설정	[조건부 필수] 설정 백업/복원	<ul style="list-style-type: none"> <li>발생조건: 설정 백업/복원 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 성공 여부</li> </ul>
	[필수] 네트워크 설정	<ul style="list-style-type: none"> <li>발생조건: 네트워크 관련 설정 변경 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 변경한 내역</li> </ul>
	[필수] 시간 설정	<ul style="list-style-type: none"> <li>발생조건: 시간 설정 변경 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, <ul style="list-style-type: none"> <li>수동 시간설정: 변경 전 · 후의 시간</li> <li>자동 시간설정: NTP 설정 정보, 동기화 전 · 후 시간</li> </ul> </li> </ul>
	[조건부 필수] 녹화 설정	<ul style="list-style-type: none"> <li>발생조건: 녹화 관련 설정 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 녹화 설정정보</li> </ul>
시스템	[필수] 시스템 부팅	<ul style="list-style-type: none"> <li>발생조건: 시스템 부팅 시</li> <li>요구정보: 발생 시간</li> </ul>
	[조건부 필수] 시스템 재부팅	<ul style="list-style-type: none"> <li>발생조건: 시스템 재부팅 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간</li> </ul>
	[필수] 공장 초기화	<ul style="list-style-type: none"> <li>발생조건: 공장초기화 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간</li> <li>※ 공장 초기화 시에도 로그 이력은 유지해야 함</li> </ul>
	[필수] 시스템 업그레이드	<ul style="list-style-type: none"> <li>발생조건: 펌웨어 업그레이드 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 업그레이드 버전 정보, 성공여부</li> </ul>
	[조건부 필수] 저장매체 탈부착	<ul style="list-style-type: none"> <li>발생조건: 시스템 동작 중 저장매체 탈부착 시</li> <li>요구정보: 발생 시간</li> </ul>
	[조건부 필수] 저장매체 포맷	<ul style="list-style-type: none"> <li>발생조건: 시스템의 저장매체 포맷 시</li> <li>요구정보: 발생 주체(ID, IP주소), 발생 시간, 객체(저장매체가 여럿일 경우)</li> </ul>

## [붙임 2] 파생 모델 확인서

파생 모델 확인서	
업체명	
업체 주소	
제품명	
시험 의뢰(시료) 모델	○ 모델명 : ○ 인증 시험 프로젝트 번호 :
파생 모델	○ 모델명 : ○ 방송통신기자재등의 적합등록 필증, 부품리스트, 제품 사진 별첨
펌웨어(S/W) 버전	
방송통신기자재등의 적합등록 필증	○ 등록번호 : ○ 등록연월일 :
<p>상기 파생 모델은 마케팅, 비즈니스 등의 관리용으로 시험 의뢰(시료) 모델과 HW 및 SW가 동일한 제품임을 약속하며, 인증서 발급 이후 파생 모델 확인서 내용이 사 실과 다를 경우 해당 제품의 인증 취소(TTA 홈페이지 공지) 및 인증 취소일로부터 1년간 시험신청 불가 등의 불이익을 감수하겠습니다. 또한, 이로인해 발생할 수 있 는 모든 문제에 대해 민형사상의 법적 책임을 지겠습니다.</p> <p>년 월 일</p> <p>대표이사 : (인)</p> <p>한국정보통신기술협회장 귀하</p> <p>※ 공문의 첨부 문서로 제출 바랍니다.</p> <p>별첨:1. 방송통신기자재등의 적합등록 필증 사본 1부, 2. 파생 모델 부품리스트 각 1부 3. 모델명을 확인할 수 있는 파생 모델 외관 제품 사진(모델별)</p>	



[붙임 3] 동일 소프트웨어 모델 확인서

동일 소프트웨어 모델 확인서 I (신청업체)	
업체명	
업체 주소	
제품명	IP카메라
시험 의뢰 모델	○ 모델명 : ○ 인증시험 프로젝트 번호 : ○ 펌웨어(S/W) 버전 :
기본 모델	○ 업체명 : ○ 모델명 : ○ 인증시험 프로젝트 번호 : ○ 펌웨어(S/W) 버전 :
<p>상기 시험 의뢰 모델은 (기본 모델 업체명) 의 (기본 모델명)과(와) 동일 소프트웨어 모델임을 확인하며, 사실과 다를 경우 해당 제품의 인증 취소 및 인증 취소일로부터 1년간 시험 신청 불가에 동의합니다.</p> <p>년 월 일</p> <p>대표이사 : (인)</p> <p>한국정보통신기술협회장 귀하</p> <p>※ 공문의 첨부 문서로 제출 바랍니다.</p>	

## 동일 소프트웨어 모델 확인서 II (기본 모델 업체)

업체명	
업체 주소	
제품명	IP카메라
기본 모델	○ 모델명 : ○ 인증시험 프로젝트 번호 : ○ 펌웨어(S/W) 버전 :
시험 의뢰 모델	○ 업체명 : ○ 모델명 : ○ 인증시험 프로젝트 번호 : ○ 펌웨어(S/W) 버전 :

자사의 (기본 모델명)는 (시험 신청 업체명)의 (시험 신청 모델명)과 동일 소프트웨어를 사용함을 확인하며, (기본 모델명)의 시험성적서 결과를 발체하여 (시험 신청 모델명) 시험성적서 및 결과요약서에 반영하는 것을 동의합니다

년 월 일

대표이사 :

(인)

한국정보통신기술협회장 귀하

※ 공문의 첨부 문서로 제출 바랍니다.

## [붙임 4] 동일 소프트웨어 모델의 동일성 확인 시험

No.	시험명	확인 사항
1	펌웨어 해시값 확인	• 시험대상장비의 펌웨어/소프트웨어와 기본 모델의 펌웨어/소프트웨어의 해시값(SHA-256)이 동일한 지 확인
2	구동 시험	• 장비의 전원을 인가하여 웹브라우저로 접속이 가능한 지 확인 • 장비의 설정 변경이 가능하고 정상동작 확인 • 라이브 영상이 정상적으로 스트리밍 되는 지 확인
3	포트 스캔 결과 확인	• 공장 초기화 상태에서 외부 포트 스캔 결과가 기본 모델과 동일한 지 확인 - 내부 시스템 접근이 가능한 경우, 내부 포트 스캔 결과가 기본 모델과 동일한 지 확인
4	펌웨어/소프트웨어 버전 및 모델명 확인	• 업체에서 제공한 펌웨어를 설치 및 공장초기화 하여 펌웨어/소프트웨어 버전 및 모델명이 신청한 정보와 동일한 지 확인
5	펌웨어/소프트웨어 업데이트 관리	• 펌웨어/소프트웨어 대한 해시 값 정보(모델명, 펌웨어/소프트웨어 파일명, 버전 정보 포함)가 게시되어 있는지 확인
6	펌웨어의 파일시스템 커버리지 확인	• 시험대상장비에서 펌웨어를 업데이트할 때 갱신되지 않는 파일시스템 및 메모리 영역에 대한 자료 제출 - 로그 저장 파일시스템 위치 등과 같이 펌웨어에 영향을 받지 않는 파일시스템 및 메모리 영역을 설명 ※ 시험항목 55번의 이행각서에 제출 자료가 사실임을 명시
7	제출 사항 확인	• 시험항목 55번의 이행각서 문서 제출 • 구동 펌웨어/소프트웨어 파일 제출