

시험성적서

한국정보통신기술협회

주소: 경기도 성남시 분당구 분당로 47
전화: 010-5112-0955 Fax: 031-724-0189

성적서번호: TTA-24-0123



1. 의뢰자

- 회사(기관)명 : (주)엠스톤
- 주 소 : 서울특별시 구로구 디지털로29길 38, 에이스테크노타워 3차 310호(구로동)

2. 성적서의 용도 : 수요처 제출용

3. 제 품 명 : 영상보안시스템용 하드웨어 NVR

(모델명: EM-VMS1024 [파생모델명: EM-VMS512+, EM-VMS1024-T, EM-VMS512+-T])

4. 버 전

- Firmware(S/W) Version : v2.9.24.1.31

5. 시험장소 : ☒ 고정시험실, ☐ 현장시험

- 시험수행주소 : 경기도 성남시 분당구 분당로 47, TTA 6층

6. 시험기간 : 2024. 2. 20. ~ 2024. 4. 3.

7. 시험방법 : 공공기관용 NVR 보안 성능품질 TTA Verified 인증기준 (TCP-2013/R11:2024)

8. 시험환경 : 실온, 실습

9. 시험결과 : 시험결과 참조

- 비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 'KS Q ISO/IEC17025와 KOLAS 인정'과 관련 없습니다.
3. 이 성적서의 진위여부는 성적서에 표시된 2D바코드 또는 QR코드, 기업지원플러스(www.g4b.go.kr)의 진위확인코드로 확인 가능합니다.

확 인

작성자

성 명 : 김 슬 기

승인자

직 책 : 기술책임자

성 명 : 김 현 정

2024년 4월 25일

한국정보통신기술협회



TPG-1016-5(01)

페이지(1)/(총 15)

시험결과:

(주)엠스톤

영상보안시스템용 하드웨어 NVR

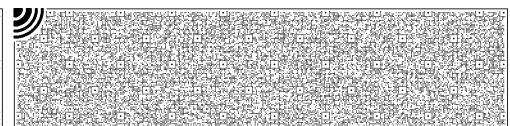
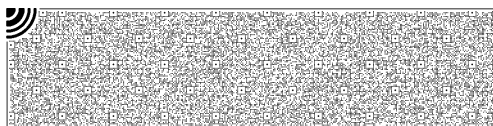
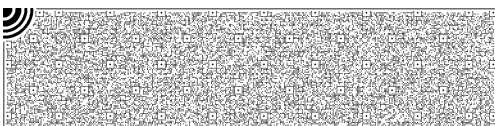
(모델명: EM-VMS1024 [파생모델명: EM-VMS512+, EM-VMS1024-T,
EM-VMS512+-T])

공공기관용 보안 성능품질 TTA Verified 인증시험

(보안 ☒ 성능품질 ☐)

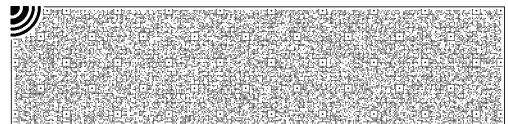
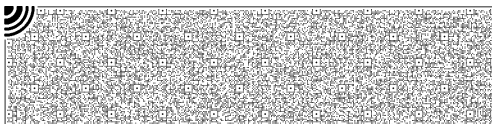
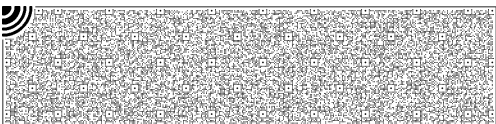


본 문서는 한국정보통신기술협회(TTA)의 시험 성적서로서 누구든지 TTA 의 사전승인 없이는 문서의 일부분만을 발췌하거나 인용하여 사용하거나 배포할 수 없습니다.



목 차

1 시험 개요	4
1.1 시험 목적	4
1.2 시험대상장비	4
1.3 시험 환경	5
1.4 시험 장비 및 도구	5
2 시험 결과	6
<첨부 1> 파생모델명	15



본 문서는 (주)엠스톤의 영상보안시스템용 하드웨어 NVR 을 대상으로 공공기관용 보안 성능품질 TTA Verified 인증시험에 대한 결과서로, 시험결과는 명시된 시험 환경, 제품명 및 버전에 국한된다.

1 시험 개요

1.1 시험 목적

본 시험은 (주)엠스톤의 영상보안시스템용 하드웨어 NVR 을 대상으로 “공공기관용 NVR 보안 성능품질 TTA Verified 인증기준(TCP-2013/R11:2024)”을 만족하는지 확인하는 데 목적이 있다.

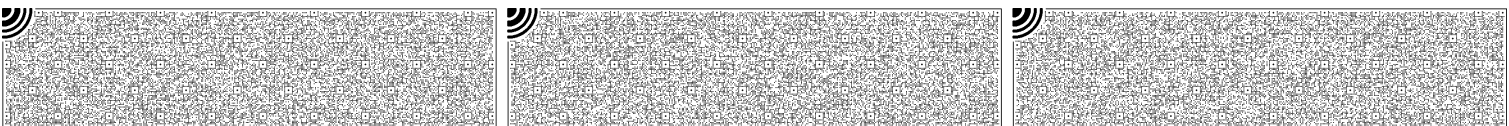
1.2 시험대상장비

본 시험의 시험대상장비(DUT: Device under Test)는 IP 카메라, 비디오 서버 등에서 보내는 영상, 음성 데이터 또는 제어 정보를 네트워크를 통해 전송 받아 저장, 검색, 모니터링하는 영상보안시스템용 저장 장치인 하드웨어 NVR(Network Video Recorder)이다. 시험대상장비 사진은 그림 1 과 같다.

- 모델명: EM-VMS1024
- 파생모델명: EM-VMS512+, EM-VMS1024-T, EM-VMS512+-T
- Firmware(S/W) Version: v2.9.24.1.31



그림 1. 시험대상장비



1.3 시험 환경

본 시험을 위한 시험 환경 구성도는 그림 2 와 같다. 보안 기능 시험을 위해 패킷 스니핑 장비, 네트워크 프로토콜 분석기, 보안 기능 시험기 등을 사용하였다. DUT 는 기본적으로 공장 초기화 상태에서 시험하고, 필요 시 DUT 의 설정을 변경하여 시험한다.

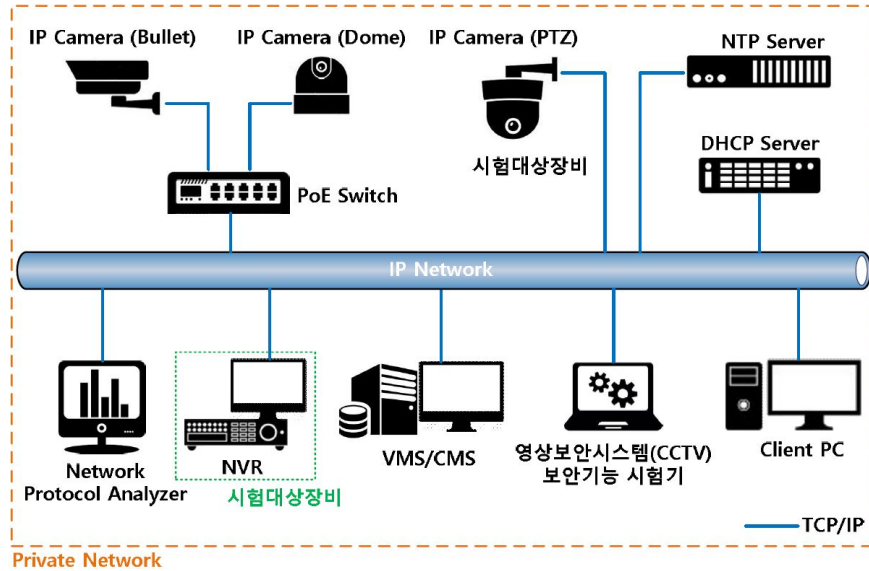


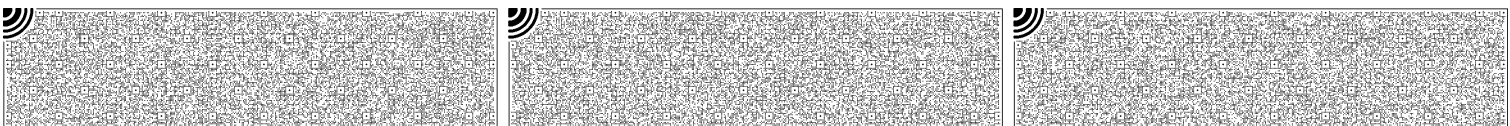
그림 2. 시험 환경 구성도

1.4 시험 장비 및 도구

본 시험에 사용한 시험 장비 및 도구는 표 1 과 같다.

표 1. 시험 장비 및 도구

장비명	모델명	제조사
IP 카메라	XNP-6370RH	한화테크윈(주)
IP 카메라	XNP-6120H	한화테크윈(주)
그 외 IP 카메라 다수	-	-
보안 기능 시험기	영상보안시스템(CCTV) 보안 기능 시험기	(주)서브
네트워크 프로토콜 분석기	Wireshark	Wireshark Foundation
스위치	FlexNetwork 5130 EL	HP

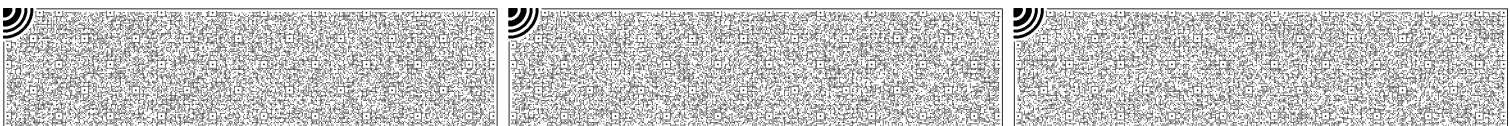


2 시험 결과

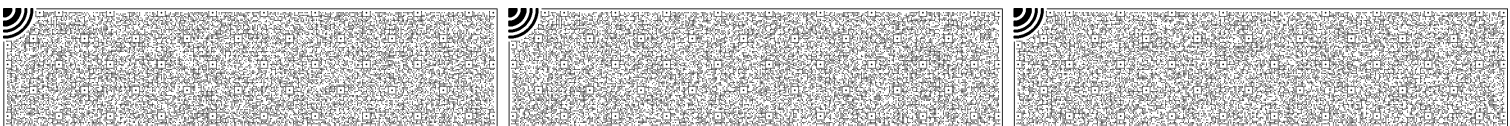
“공공기관용 NVR 보안 성능품질 TTA Verified 인증기준(TCP-2013/R11:2024)”의 만족 여부를 확인한 시험 결과는 표 2와 같다.

표 2. 시험 결과

번호	시험 항목	인증 기준	필수 여부	판정
1	최초 비밀번호 생성/변경 강제	- 장비를 공장 초기화한 후 최초 장비 접속 및 최초 서비스 접속 시 관리자 기본(Default) 비밀번호에 대해 아래의 사항을 만족해야 한다. - 관리자 기본(Default) 비밀번호가 있는 경우, 비밀번호 변경이 강제되어야 함 - 관리자 기본(Default) 비밀번호가 없는 경우, 비밀번호 생성이 강제되어야 함 “방송통신기자재등의 적합등록 필증”을 받은 경우 본 시험 항목의 인증 기준을 만족하는 것으로 한다. - 장비 접속 - 웹 브라우저, 로컬 콘솔 등 - 서비스 접속 - SSH, HTTP/HTTPS, RTSP, FTP, TELNET, SNMP 등	필수	PASS
2	비밀번호 조합 구성	- 생성하는 비밀번호는 9자리 이상이어야 한다. - 숫자, 영문 대문자, 영문 소문자, 특수문자 중 3가지 조합 이상으로 비밀번호를 생성할 수 있어야 한다. - 숫자(0-9) - 영문자 대문자(A-Z) - 영문자 소문자(a-z) - 특수문자(!, @, #, \$, %, ^, &, *, (,) 등)	필수	PASS
3	비밀번호 최소길이 설정	비밀번호의 최소 길이를 관리자가 설정할 수 있는 기능을 제공해야 한다. ※ 최소 길이의 기본값은 9자리 이상이어야 한다.	선택	해당사항 없음
4	비밀번호 15자리 이상 입력가능	비밀번호는 15자리 이상 입력이 가능해야 한다.	선택	PASS
5	인증 실패 시 장비접속 제한기능	- 지정된 횟수(기본값 5회 이하) 이상 인증 실패 시 일정 시간 (기본값 5분 이상) 장비 접속을 제한하는 기능을 제공해야 한다. - On/Off 기능이 있는 경우 Default ON	필수	PASS



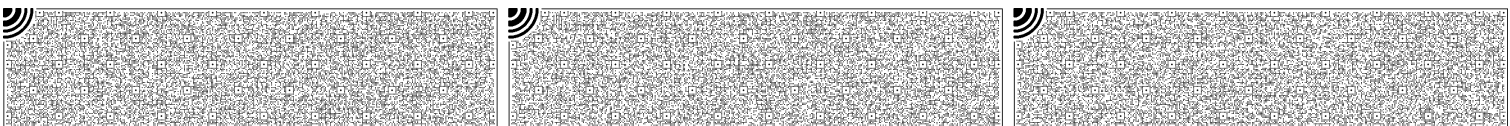
번 호	시험 항목	인증 기준	필수 여부	판정
6	인증 실패 시 장비접속 제한시간 설정기능	인증 실패 시 장비 접속 제한 시간을 관리자가 설정할 수 있는 기능을 제공해야 한다.	선택	PASS
7	에러 메시지에 인증 실패 사유 미포함 기능	- 인증 실패 시 인증 실패 사유를 에러 메시지에 포함하지 않아야 한다. (예시) - 잘못된 계정을 입력하였습니다. - 잘못된 비밀번호를 입력하였습니다. ※ UI뿐만 아니라 네트워크 상의 응답 메시지에도 실패 사유가 포함되지 않아야 한다.	필수	PASS
8	입력 비밀번호 마스킹 기능	입력되는 비밀번호를 화면에서 볼 수 없도록 마스킹하는 기능을 제공해야 한다.	필수	PASS
9	비밀번호 암호화 저장 기능	- 비밀번호를 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. - 장비에서 백업할 수 있는 설정 파일 등에 비밀번호가 포함된 경우, 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. - 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(14번, 15번) 참조	필수	PASS
10	비밀정보 읽기 방지 기능	- 장비에 저장된 모든 비밀정보(비밀번호, 대칭키, 개인키 등)를 읽거나 유추할 수 없어야 한다. - 비밀정보 평문 저장 및 Base64 단순 인코딩 등은 제한한다.	필수	PASS
11	비밀번호 임의 복구 기능 제한	비밀번호 찾기 또는 2차 비밀번호 등의 임의 복구 기능을 사용할 수 없어야 한다.	필수	PASS
12	사용자 인증	- ONVIF HTTP Digest 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. - RTSP Digest 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. - ONVIF SOAP 사용자 인증으로 WSSE UsernameToken의 PasswordDigest 인증 방식을 SHA-1 이상으로 사용해야 한다. - 기타 사용자 인증 방식은 암호지원 시험항목(14번, 15번)을 참조하여 안전한 방식을 사용해야 한다.	필수	PASS



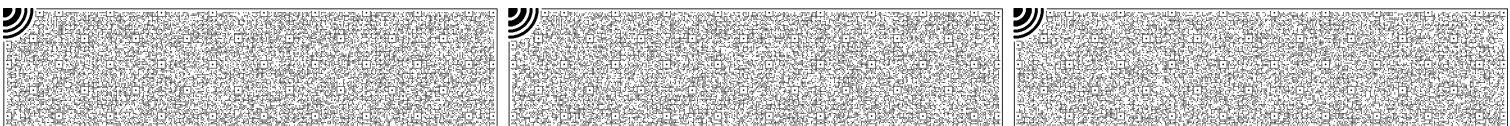
번 호	시험 항목	인증 기준	필수 여부	판정
13	인증 우회 취약점 대응	시험대상장비에 웹 브라우저 접속이 가능한 경우에 한하여, • 웹 브라우저와 원격 관리 통신 시 안전한 사용자 인증 절차 없이 세션 정보(세션 ID 등)만으로 인증 여부를 판단하지 않아야 한다. • 세션 정보에 계정 권한 정보가 포함되어 있는 경우, 해당 정보를 위·변조하여 권한 상승 등의 월권 행위를 할 수 없어야 한다. • Digest 인증의 nonce 등 서버가 생성한 인증 정보는 세션 만료 또는 재부팅 시 함께 만료되어야 한다. • 서버는 수신한 Digest 인증 요청에서 nc(nonce count) 값의 연속 증가를 확인해야 한다.	조건부 필수	해당사항 없음
14	암호 알고리즘 보안 강도 만족 여부	• 암호화 및 해시 알고리즘의 보안강도는 112bit 급 이상을 만족해야 한다. ※ 알고리즘의 보안강도는 한국인터넷진흥원의 “암호 알고리즘 및 키 길이 이용 안내서”최신본을 참조 (예시) - 해시(SHA-224/256/384/512 등) - 대칭키암호(SEED, ARIA-128/192/256, AES-128/192/256 등) - 공개키암호(RSA 2048 등) - 전자서명(RSA-PSS-2048/3072, ECDSA/KCDSA/EC-KCDSA 등)	필수	PASS
15	국가용 암호 알고리즘 사용 여부	• 국가용 암호 알고리즘의 사용을 권고한다. - 국정원장 승인 알고리즘, 국가사이버안전센터 안내 참조	선택	해당사항 없음
16	VLAN 기능	• VLAN 기능 제공시 IEEE Std 802.1q-2011 이상을 지원해야 한다.	선택	해당사항 없음
17	IP Filtering 기능	• 특정 IP주소에서의 접속을 허용/차단할 수 있는 기능을 제공해야 한다. ※ Black List(Deny), White List(Allow) 동작 확인	필수	PASS
18	ACL 기능	• 장비별 다음과 같은 ACL 기능을 제공해야 한다. - Source IP Address 정보 또는 Source Port Number 정보	선택	해당사항 없음
19	원격 관리용 IP 주소 지정 기능	• 원격 관리 서비스 용도의 IP주소를 지정하는 기능을 제공해야 한다. - IP주소 지정은 대역이 아닌 개별 주소 등록만 가능해야 함 - 원격 관리: 관리자 계정으로 접속하여 설정을 변경하거나 PTZ를 제어하는 원격 세션의 모든 활동	필수	PASS
20	원격관리서비스 활성화/비활성화	• 공장 초기화 상태에서 원격 관리 서비스는 비활성화되어 있어야 하며 아래는 예외 사항으로 적용한다. - 가상화 적용 장비의 경우 : HTTPS만 활성화 허용	필수	PASS



번 호	시험 항목	인증 기준	필수 여부	판정
	기능	- 가상화 적용 장비가 아닌 경우 :HTTPS도 활성화 금지 • 관리자가 원할 때 원격 관리 서비스를 활성화/비활성화 할 수 있는 기능을 제공해야 한다. - 원격 관리 서비스 : SSH, HTTP/HTTPS, FTP, TELNET, SNMP 등		
21	DBMS 원격 접근 제한	• 장비에서 운용되는 DBMS에 대해 원격에서 직접 접근하는 것은 제한되어야 한다.	필수	PASS
22	웹 표준방식 지원	• 웹 브라우저 접속을 지원하는 경우 영상(Video/Audio)에 관련되지 않은 웹 브라우저 동작을 위해 플러그인(ActiveX, EXE 등)을 사용하지 않아야 한다.	조건부 필수	해당사항 없음
23	SNMP V3 지원 기능	• SNMP를 지원하는 경우, SNMP는 V3 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	조건부 필수	해당사항 없음
24	펌웨어/소프트웨어 버전 및 모델명 확인 기능	• 펌웨어/소프트웨어의 현재 버전을 확인할 수 있는 기능을 제공해야 한다. • 시험대상장비의 UI에서 모델명을 확인할 수 있어야 한다.	필수	PASS
25	펌웨어/소프트웨어 업데이트 검증 기능	• 펌웨어/소프트웨어에 대한 해시 값 정보(모델명, 펌웨어/소프트웨어 파일명, 버전 정보를 포함)를 홈페이지에 게시해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조 (MD5 등 사용제한, SHA256 이상 사용권고)	필수	PASS
26	자동 업데이트 기능 제한	• 기본 설정 상태에서 자동 업데이트 기능을 사용할 수 없어야 한다.	필수	PASS
27	일정시간 미사용시 세션 잠금/종료 기능	• 일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료하는 기능을 제공해야 한다. - Default ON, 기본값 10 분 이하 ※ 본 항목의 기능은 ON/OFF가 허용됨 ※ 관리자 활동 : 관리자 계정으로 접속하여 설정을 변경하거나 PTZ를 제어하는 로컬/원격 세션의 모든 활동	필수	PASS
28	동시접속 세션 수 제한 기능	• 시험대상장비에 원격으로 접속하는 관리자의 동시 접속 세션을 하나만 허용하거나 동시 접속 세션 수를 제한 기능을 제공해야 한다. ※ 본 항목의 기능은 ON/OFF가 허용됨	선택	해당사항 없음



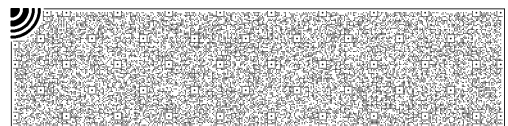
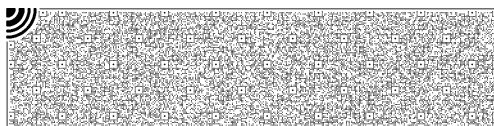
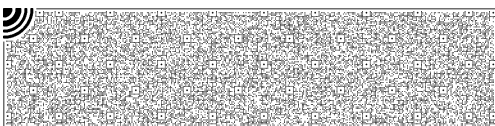
번호	시험 항목	인증 기준	필수 여부	판정
29	하드웨어 자체검사 기능	• Embedded-HW형 장비에 한하여, 장비 구동 시(Power On) 주요 하드웨어에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - CPU, 메모리, 플래시 메모리, 네트워크 인터페이스 등 ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함	조건부 필수	PASS
30	소프트웨어 자체검사 기능	• 장비 구동시(Power On) 또는 어플리케이션 로딩 후 주요 프로세스에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다. (예시) - 식별 및 인증 프로세스 - 정보흐름통제 프로세스 - 보안관리 프로세스 등 ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함	필수	PASS
31	자체검사 내용 및 결과 확인 기능	• 시험대상장비가 수행한 자체검사 내용 및 결과를 관리자가 확인할 수 있는 기능을 제공해야 한다. (예시) - 화면 출력 - 디스플레이 화면 - 감사데이터 생성 등	필수	PASS
32	자체검사 실행 기능	• 관리자가 항목 29,30의 자체검사를 직접 실행하는 기능을 제공해야 한다.	선택	해당사항 없음
33	소프트웨어 무결성 검사 기능	• 시험대상장비 구동 시(Power On) 또는 구동 이후 주요 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다. ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함	선택	해당사항 없음
34	무결성 검사 실행 기능	• 관리자가 소프트웨어 무결성 검사를 직접 실행하는 기능을 제공해야 한다.	선택	해당사항 없음
35	설정 백업/복원시 무결성 검사 기능	• 장비 설정 백업/복원 시 설정 파일에 대한 무결성 검사 기능을 제공해야 한다.	선택	해당사항 없음
36	계정별 접근권한 설정 기능	• 관리자 계정별 접근권한을 설정하는 기능을 제공해야 한다.	필수	PASS



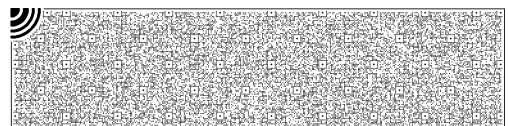
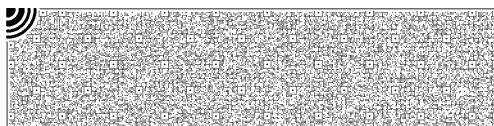
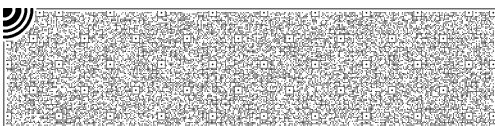
번호	시험 항목	인증 기준	필수 여부	판정
37	운영모드 변경용 비밀번호 생성 기능	• 운영모드 변경이 가능할 경우, 운영모드 변경용 비밀번호를 관리자가 생성/재설정할 수 있는 기능을 제공해야 한다. ※ 비밀번호 생성 관련 부분은 안전한 비밀번호 설정 기능을 참고	조건부 필수	PASS
38	운영모드 변경 시 추가 인증 기능	• 운영모드 변경이 가능할 경우, 운영모드 변경 시 추가 인증을 수행하는 기능을 제공해야 한다.	조건부 필수	PASS
39	중요 명령 사용 제한 기능	• 장비 상태를 변경하는 중요 명령(기능)에 대한 접근은 로컬 콘솔 (콘솔포트 연결)로 제한하는 기능을 제공해야 한다. (중요 명령) - 공장초기화, 재부팅, F/W 업그레이드, 디버깅(부트롬 접속, 메모리 수정/덤프)	선택	해당사항 없음
40	원격 접속시 암호통신 수행 기능	• 원격으로 접속 시 암호통신 프로토콜을 이용한 신뢰된 채널을 제공해야 한다. (예시) - HTTPS, SSL/TLS, SSH - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	필수	PASS
41	별도 서버와 연동시 암호통신 수행 기능	• 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(14번, 15번) 참조	조건부 필수	해당사항 없음
42	TLS 1.2 이상 지원 기능	• TLS 프로토콜은 TLS 1.2(RFC 5246) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	필수	PASS
43	SSH 2.0 이상 지원 기능	• SSH를 지원하는 경우, 프로토콜은 SSH v2(RFC 4251~4254) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	조건부 필수	PASS
44	OpenSSH, OpenSSL 버전 확인 기능	• 암호통신을 위해 OpenSSH, OpenSSL을 사용하는 경우 버전을 확인하는 기능을 제공해야 한다. • 버전의 표기는 패치 버전 정보를 포함해야 한다.	필수	PASS
45	감사데이터 생성 기능	• "불임"에 해당하는 감사 데이터들을 생성하는 기능을 제공 해야 한다. ※ 감사 데이터 세부내역은 "불임" 참조	필수	PASS
46	감사데이터에 최소 정보 포함 기능	• 감사데이터에는 최소한 다음의 정보가 포함되어야 한다. - 사건 발생 일시 - 사건 유형	필수	PASS



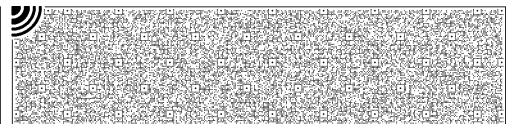
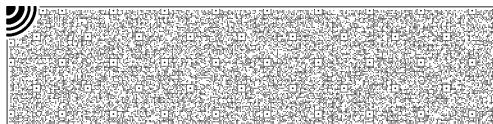
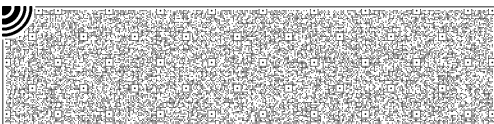
번호	시험 항목	인증 기준	필수 여부	판정
		- 사건 발생 주체(ID, IP주소) - 사건의 결과(성공 또는 실패)		
47	감사 증적 초과시 관리자 확인 기능	• 감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 관리자가 알 수 있는 기능을 제공해야 한다.	필수	PASS
48	감사 증적 초과시 대처 조치 기능	• 감사증적 크기가 로그 저장 용량의 일정 기준(예: 90% 이상) 초과 시 '외부로의 로그 백업 또는 오래된 내용 덮어쓰기' 등 대처 조치를 해야 한다.	필수	PASS
49	외부 로그서버 전송 기능	• 감사데이터를 외부 로그 서버로 전송하는 기능을 제공해야 한다.	선택	해당사항 없음
50	감사 데이터 접근 제한 기능	• 인가된 관리자만 감사데이터에 접근할 수 있어야 한다.	필수	PASS
51	감사 데이터 암호화 저장 기능	• 감사데이터를 장비 내부에 저장할 경우 암호화하여 저장하는 기능을 제공해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	선택	해당사항 없음
52	개인키 암호화 저장 기능	• 장비 내에 저장된 개인키는 암호화되어 저장되어야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	필수	PASS
53	인증서/개인키/대칭키의 안전한 생성	• 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.	필수	PASS
54	암호 및 암호화키 하드코딩 방지 이행각서 공문	• 이행각서 공문 접수 - 주내용 : 방지 이행 약속 및 불이행시 관련 제품군에 대한 인증 취소 사전동의 (공문 내용) - "무단은닉 및 하드코딩된 암호 및 암호화키 없음" 선언 - "운용 모드 변경 (개발자/디버깅 모드) 관련 유/무" 선언 - "보안 및 성능품질 열화행위 하지 않음" 선언 - "백도어 없음" 선언 - "국내외 정보보호 전문기관에서 공지된 취약점은 해결되었음"을 선언	필수	PASS
55	구동 소프트웨어 채증 자료 제출	• 시험당시 구동 소프트웨어(어플리케이션 등) 해시 값 파일 제출 ※ 소스코드가 아닌 원본 소프트웨어 검증용 해시 값 또는 펌웨어 파일, 설치 파일 제출	필수	PASS



번호	시험 항목	인증 기준	필수 여부	판정
56	지원 명령어 확인	• OPTIONS 메시지로 지원하는 RTSP 명령어가 확인되어야 한다.	필수	PASS
57	세션 확인	• DESCRIBE 메시지로 제공 가능한 세션 내역이 확인 되어야 한다.	필수	PASS
58	연결 설정	• SETUP 메시지로 원하는 세션 연결 설정이 가능해야 한다.	필수	PASS
59	전송 시작	• PLAY 메시지로 영상 데이터 전송을 시작할 수 있어야 한다.	필수	PASS
60	전송 종료	• TEARDOWN 메시지로 영상 데이터 전송을 종료할 수 있어야 한다.	필수	PASS
61	기본 Flow 적용	• TLS 표준상의 기본 Flow가 적용되는지 확인한다.	필수	PASS
62	인증서 적용	• TLS 연결 과정에서 서버 측의 인증서가 클라이언트에게 전달되는지 확인한다. • Certificate Request를 지원하는 경우, TLS 연결 과정에서 클라이언트 측의 인증서가 서버로 전달되는 지 확인한다.	필수	PASS
63	전자서명	• TLS 연결 과정에서 전자서명 역할을 하는 Certificate Verify를 전송하는 지를 확인한다.	선택	해당사항 없음
64	국제 표준 암호 알고리즘 수용 및 협상	• 적용된 암호화 알고리즘이 2개 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.	필수	PASS
65	영상 전송 시 암호화	• 웹 브라우저, CMS 등에 영상을 전송하기 위한 암호통신 프로토콜 기반의 신뢰된 채널을 제공해야 한다. - (예시) HTTPS, TLS • HTTPS Tunneling(RTP/RTSP/HTTPS/TCP) 방식으로 영상 데이터를 수신할 수 있어야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	필수	PASS
66	영상 저장 시 암호화	• 영상 데이터를 장비 내부에 저장할 경우 암호화하여 저장해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조	선택	해당사항 없음
67	오디오 데이터 저장 제한	• 기본 설정 상태에서 오디오 데이터 저장 기능을 사용할 수 없어야 한다.	필수	PASS
68	영상 백업 시 암호화	• 장비에 저장된 영상 데이터를 외부로 백업/다운로드하는 것이 가능한 경우, 암호화하여 백업/다운로드해야 한다.	필수	PASS



번 에	시험 항목	인증 기준	필수 여부	판정
		- 백업/다운로드하는 영상 데이터에 대한 무결성 검증 값 생성 및 확인이 가능해야 한다. - 암호화 방식에 관련된 부분은 암호지원 시험항목(14번, 15번) 참조		



<첨부 1> 파생모델명

파생모델명	
-------	--

