관리구분 : □관리본 □비관리본

문서번호 : TCP-2013/R00 : 2017

관리번호 :

공공기관용 NVR 보안 성능품질

TTA Verified 인증 기준

한국정보통신기술협회
Telecommunications Technology Association

제·개정 이력 현황

개정번호	제·개정일	개정쪽	제·개정내용
00	2017.12.22	-	인증 기준 마련에 따른 제정 (Ver. 1)

목 차

1 적용 범위

본 문서는 정보통신 제품 및 서비스에 대한 인증 요령 제12조 및 공공기관용 영상정보처리기기 보안 요구사항에 따라 NVR의 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, 2017. 9, TTA.
[14] 영상보안시스템용 NVR TTA Verified 인증 기준, 2017. 11, TTA.

3 정의

3.1 용어 정의

시험대상장비[하드웨어(H/W) NVR]

IP카메라, 비디오 서버 등에서 IP 네트워크로 영상을 전달받아 저장, 검색, 모니터링 할 수 있는 영상정보처리기기이며 임베디드 또는 PC 타입의 하드웨어 형태를 가진다. NVR에 무선 통신 인터페이스가 존재하는 경우, 공장초기화 상태에서 비활성화되어 있어야 하며 최고 관리자만 무선 통신 인터페이스를 활성화/비활성화할 수 있어야 한다.

시험대상장비[소프트웨어(S/W) NVR]

IP카메라, 비디오 서버 등에서 IP 네트워크로 영상을 전달받아 저장, 검색, 모니터링 할 수 있는 응용프로그램 형태의 영상정보처리기기이며 권장되는 사양의 하드웨어에 탑재하여 시험한다. NVR에 무선 통신 인터페이스가 존재하는 경우, 공장초기화 상태

에서 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

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

4 시험 환경

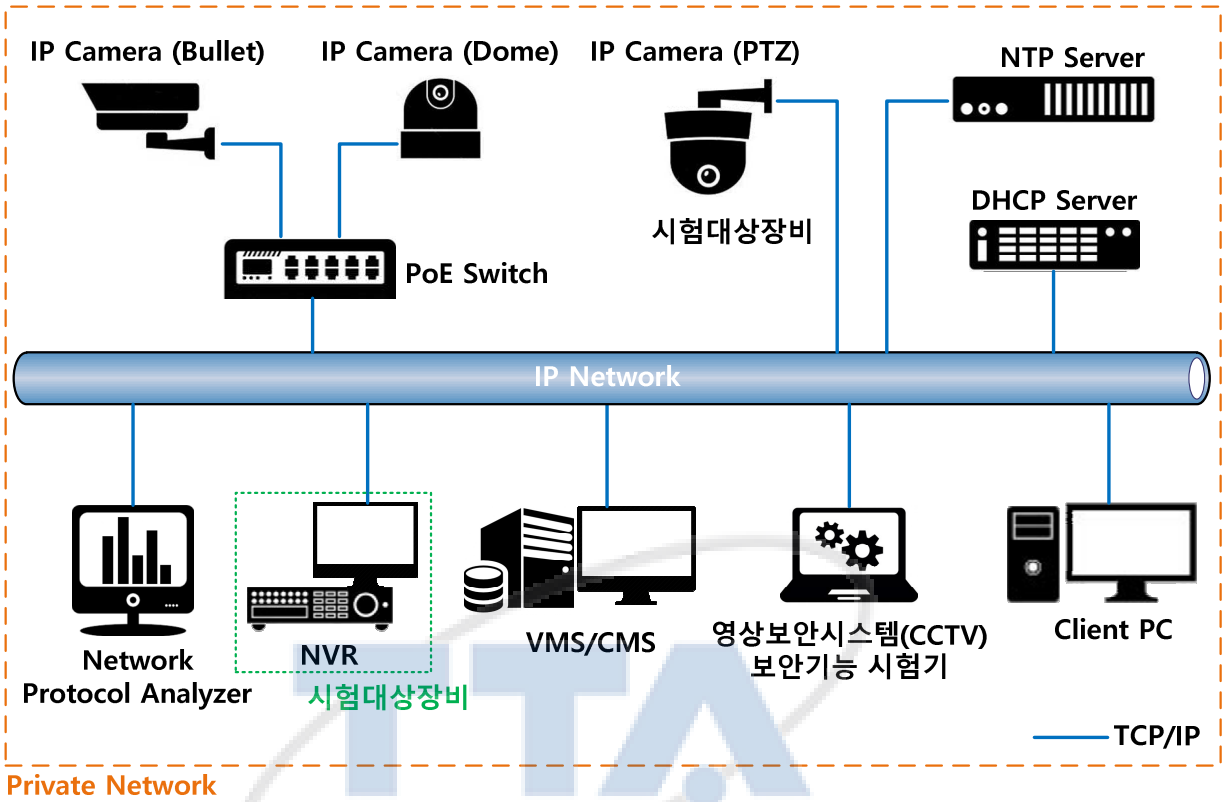

그림 1. 시험 환경 구성도

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

5 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
식별 및 인증	관리자 기본(default) 비밀번호 변경 기능	1	[필수] 최초 비밀번호 변경	• 장비를 공장 초기화한 후 최초 장비 접속 및 최초 서비스 접속 시 관리자 기본(Default) 비밀번호 유지는 제한되어야 하며 반드시 안전한 패턴으로 변경되어야 한다. 1) 장비 접속 - 웹 브라우저, 로컬 콘솔 등 2) 서비스 접속 - SSH, HTTP/HTTPS, RTSP, FTP, TELNET, SNMP 등
	안전한 비밀번호 설정 기능	2	[필수] 비밀번호 조합 구성	• 생성하는 비밀번호는 9 자리 이상이어야 한다. • 숫자, 영문 대문자, 영문 소문자, 특수문자 중 3 가지 조합 이상으로 비밀번호를 생성할 수 있어야 한다. - 숫자(0-9) - 영문자 대문자(A-Z) - 영문자 소문자(a-z) - 특수문자(!, @, #, $, %, ^, &, *, (,) 등)
		3	[선택] 비밀번호 최소길이 설정	• 비밀번호의 최소 길이를 관리자가 설정할 수 있는 기능을 제공해야 한다. ※ 최소 길이의 기본값은 9 자리 이상이어야 한다.
		4	[선택] 비밀번호 15 자리 이상 입력가능	• 비밀번호는 15 자리 이상 입력이 가능해야 한다.
	인증 실패 대응 기능	5	[필수] 인증 실패 시 장비접속 제한기능	• 지정된 횟수(기본값 5회 이하) 이상 인증 실패 시 일정 시간 (기본값 5 분 이상) 장비 접속을 제한하는 기능을 제공해야 한다.
		6	[선택] 인증 실패 시 장비접속 제한시간 설정기능	• 인증 실패 시 장비 접속 제한 시간을 관리자가 설정할 수 있는 기능을 제공해야 한다.
		7	[필수] 에러 메시지에 인증 실패 사유 미포함 기능	• 인증 실패 시 인증 실패 사유를 에러 메시지에 포함하지 않아야 한다. (인증 실패 사유 예시) - 잘못된 계정을 입력하였습니다. - 잘못된 비밀번호를 입력하였습니다.
	인증 피드백 보호 기능	8	[필수] 입력 비밀번호 마스킹 기능	• 입력되는 비밀번호를 화면에서 볼 수 없도록 마스킹하는 기능을 제공해야 한다.

대분류	중분류	번호	시험 항목	인증 기준
	인증 데이터 보호 기능	9	[필수] 비밀번호 암호화 저장 기능	• 비밀번호를 암호 알고리즘(대칭키 암호, 해시 함수 등)을 이용하여 안전하게 저장해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
		10	[필수] 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.
	사용자 인증	11	[필수] 사용자 인증	• HTTP 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. • RTSP 사용자 인증으로 Digest (RFC 7616) [SHA-2] 인증 방식을 사용해야 한다. • SOAP 사용자 인증으로 WSSE UsernameToken 의 PasswordDigest 인증 방식을 SHA-1 이상으로 사용해야 한다.
암호지원	암호사용	12	[필수] 암호 알고리즘 보안 강도 만족 여부	• 암호화 및 해시 알고리즘의 보안강도는 112bit 급 이상을 만족해야 한다. (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)
		13	[선택] 국가용 암호 알고리즘 사용 여부	• 국가용 암호 알고리즘의 사용을 권고한다. - 국정원장 승인 알고리즘, 국가사이버안전센터 안내 참조
정보 흐름 통제	트래픽 제어	14	[선택] VLAN 기능	• VLAN 기능 제공시 IEEE Std 802.1q-2011 이상을 지원해야 한다.
		15	[필수] IP Filtering 기능	• 특정 IP주소에서의 접속을 허용/차단할 수 있는 기능을 제공해야 한다. ※ Black List(Deny), White List(Allow) 동작 확인
		16	[선택] ACL 기능	• 장비별 다음과 같은 ACL 기능을 제공해야 한다. - Source IP Address 정보 또는 Source Port Number 정보
보안관리	장비 관리용 원격 접속 IP주소 제한 기능	17	[필수] 원격 관리용 IP주소 지정 기능	• 원격 관리 서비스 용도의 IP 주소를 지정하는 기능을 제공해야 한다. - IP주소 지정은 대역이 아닌 개별 주소 등록만 가능해야 함
	원격 관리 기능	18	[필수] 원격관리서비스 활성화/비활성화 기능	• 공장 초기화 상태에서 원격 관리 서비스는 비활성화되어 있어야 한다. • 관리자가 원할 때 원격 관리 서비스를 활성화/비활성화 할 수 있는 기능을 제공해야 한다. - 원격 관리 서비스 : SSH, HTTP/HTTPS, FTP, TELNET, SNMP 등 - 가상화 적용 장비의 경우 : HTTPS 만 활성화 허용 - 가상화 적용 장비가 아닌 경우 : HTTPS 도 활성화 금지

대분류	중분류	번호	시험 항목	인증 기준
		19	[선택] 웹 표준방식 지원	• HTML5 등의 웹 표준방식을 지원해야 한다. ※ ActiveX, EXE가 지원될 경우 해당 기능에 대한 ON/OFF 가 가능해야 한다.
		20	[조건부필수] SNMP V3 지원 기능	• SNMP를 지원하는 경우, SNMP는 V3 이상을 지원해야 한다. - 암호화 방식에 대한 상세는 "암호지원" 참조
	펌웨어 업데이트 관리 기능	21	[필수] 펌웨어/소프트웨어 버전 확인 기능	• 관리자가 어플리케이션/펌웨어의 현재 버전을 확인할 수 있는 기능을 제공해야 한다.
		22	[필수] 펌웨어 업데이트 검증 기능	• 펌웨어 업데이트 시 해시값 비교 또는 전자서명 등을 제공해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조 (MD5 등 사용제한, SHA256 이상 사용권고)
	일정시간 관리자 활동 없는 경우 세션 잠금 또는 세션 종료 기능	23	[필수] 일정시간 미사용시 세션 잠금/종료 기능	• 일정시간 관리자 활동이 없는 경우 세션을 잠그거나 종료하는 기능을 제공해야 한다. (예시) 기본값 10분 이하 ※ 본 항목의 기능은 ON/OFF가 허용됨 ※ 관리자 활동 : 관리자 계정으로 접속하여 설정을 변경할 수 있는 로컬/원격 세션의 모든 활동
	관리자의 동시 원격 접속 세션 제한	24	[선택] 동시접속 세션 수 제한 기능	• 시험대상장비에 원격으로 접속하는 관리자의 동시 접속 세션을 하나만 허용하거나 동시 접속 세션 수를 제한하는 기능을 제공해야 한다. ※ 본 항목의 기능은 ON/OFF가 허용됨
자체 시험	오류 검사 기능 ※제조업체에서 주요 프로세스를 사전정의 후 TTA와 시험협의	25	[조건부 필수] 하드웨어 자체검사 기능	• Embeded-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 ※ 개발업체는 장비가 지원하는 기능에 대한 상세 설명자료 제출해야 함
		26	[필수] 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

대분류	중분류	번호	시험 항목	인증 기준
		27	[필수] 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
		28	[선택] 자체검사 실행 기능	• 관리자가 항목 25,26 의 자체검사를 직접 실행하는 기능을 제공해야 한다.
	무결성 검사 기능	29	[선택] 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
		30	[선택] 무결성 검사 실행 기능	• 관리자가 소프트웨어 무결성 검사를 직접 실행하는 기능을 제공해야 한다.
		31	[선택] 설정 백업/복원시 무결성 검사 기능	• 장비 설정 백업/복원 시 설정 파일에 대한 무결성 검사 기능을 제공해야 한다.
접근 통제	접근 통제 기능	32	[필수] 계정별 접근권한 설정 기능	• 관리자 계정별 접근권한을 설정하는 기능을 제공해야 한다.
		33	[조건부필수] 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
		34	[조건부필수] 운영모드 변경 시 추가 인증 기능	• 운영모드 변경이 가능할 경우, 운영모드 변경 시 추가 인증을 수행하는 기능을 제공해야 한다.
		35	[선택] 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)
전송 데이터 보호	제품과 원격으로 연결된 모든 통신 수단간 안전한 암호통신 프로토콜 사용	36	[필수] 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" 참조
		37	[선택] 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" 참조

대분류	중분류	번호	시험 항목	인증 기준
		38	[필수] TLS 1.2 이상 지원 기능	• TLS 프로토콜은 TLS 1.2(RFC 5246) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
		39	[조건부필수] SSH2.0 이상 지원 기능	• SSH 를 지원하는 경우, 프로토콜은 SSH v2(RFC 4251~4254) 이상을 지원해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
	OpenSSH,OpenSSL 버전 확인	40	[필수] OpenSSH, OpenSSL 버전 확인 기능	• 암호통신을 위해 OpenSSH, OpenSSL 을 사용하는 경우 버전을 확인하는 기능을 제공해야 한다.
감사 기록	감사데이터 생성 기능	41	[필수] 감사데이터 생성 기능	• "붙임"에 해당하는 감사 데이터들을 생성하는 기능을 제공해야 한다. ※ 감사 데이터 세부내역은 "붙임" 참조
	감사데이터에 최소 정보 포함 여부	42	[필수] 감사데이터에 최소 정보 포함 기능	• 감사데이터에는 최소한 다음의 정보가 포함되어야 한다. - 사건 발생 일시 - 사건 유형 - 사건 발생 주체(ID, IP 주소) - 사건의 결과(성공 또는 실패)
	감사증적의 크기가 제한용량 초과시 대응 행동	43	[필수] 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.
		44	[필수] 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.
		45	[선택] 외부 로그서버 전송 기능	• 감사데이터를 외부 로그 서버로 전송하는 기능을 제공해야 한다.
	감사데이터 보호	46	[필수] 감사 데이터 접근 제한 기능	• 인가된 관리자만 감사데이터에 접근할 수 있어야 한다.
		47	[선택] 감사 데이터 암호화 저장 기능	• 감사데이터를 장비 내부에 저장할 경우 암호화하여 저장하는 기능을 제공해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
인증서 관리	개인키 암호화 저장 확인	48	[필수] 개인키 암호화 저장 기능	• 장비 내에 저장된 개인키는 암호화되어 저장되어야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
	인증서/개인키 확인	49	[필수] 인증서/개인키의 안전한 생성	• 장비 내에서 인증서/개인키를 생성하는 경우, 안전한 방법으로 생성해야 하며, 인증서/개인키의 하드코딩 및 장비간 공통된 개인키의 일괄 사용을 하지 않아야 한다.

대분류	중분류	번호	시험 항목	인증 기준
인증 심의 항목	무단은닉 하드코딩 방지 이행	50	[필수] 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
	채증 자료 제출	51	[필수] 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
영상/음성 전송 기본기능	표준 프로토콜-RTSP	52	[필수] 지원 명령어 확인	• OPTIONS 메시지로 지원하는 RTSP 명령어가 확인되어야 한다.
		53	[필수] 세션 확인	• DESCRIBE 메시지로 제공 가능한 세션 내역이 확인 되어야 한다.
		54	[필수] 연결 설정	• SETUP 메시지로 원하는 세션 연결 설정이 가능해야 한다.
		55	[필수] 전송 시작	• PLAY 메시지로 영상 데이터 전송을 시작할 수 있어야 한다.
		56	[필수] 전송 종료	• TEARDOWN 메시지로 영상 데이터 전송을 종료할 수 있어야 한다.
영상/음성 전송 보안	TLS 제어 암호화	57	[필수] 기본 Flow 적용	• TLS 표준상의 기본 Flow가 적용되는지 확인한다.
		58	[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.
		59	[선택] 전자서명	• TLS 연결과정에서 전자서명 역할을 하는 Certificate Verify를 전송하는 지를 확인한다.
		60	[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/음성 트래픽 보안	61	[필수] RTP 암호화 및 복호화	• 암호화된 RTP 메시지를 네트웍상에서 캡쳐하여 영상이 재생되는 지를 확인하며, 클라이언트에서 정상적으로 복호화를 수행하여 영상 재생이 되는 지를 확인한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조

대분류	중분류	번호	시험 항목	인증 기준
영상 저장 보안	영상 저장 시 암호화	62	[선택] 영상 저장 시 암호화	• 영상 데이터를 장비 내부에 저장할 경우 암호화하여 저장해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조 ※ 음성 데이터는 저장하지 않아야 함
영상 백업 보안	영상 백업 시 암호화	63	[필수] 영상 백업 시 암호화	• 영상 데이터를 장비 외부로 반출할 경우 암호화하여 반출해야 한다. • 반출하는 영상 데이터에 대한 무결성 검증 값 생성 및 확인이 가능해야 한다. - 암호화 방식에 관련된 부분은 "암호지원" 참조
상호연동	상호연동	64	[필수] 상호연동	• 시험대상장비는 "영상보안시스템 상호연동 TTA Verified 인증 기준(TCB-0060)"을 만족해야 한다. ※ 위 인증기준의 최신 개정이력이 발생한 경우, 최신 개정본의 내용을 따름
성능 품질	성능품질	65	[필수] NVR 기능	• 시험대상장비는 "영상보안시스템용 NVR TTA Verified 인증 기준(TCB-0062)"을 만족 해야 한다. ※ 위 인증기준의 "영상보안시스템용 NVR 보안" 항목은 시험범위에서 제외함 ※ 위 인증기준의 최신 개정이력이 발생한 경우, 최신 개정본의 내용을 따름

6 시험대상장비에 대한 제출 사항

시험의뢰업체는 시험대상장비의 시험을 위해 아래와 같은 사항을 제출해야 한다.

항목	제시 내용
기본(Default) 비밀번호	• 기본(Default) 비밀번호가 존재하는 경우, 해당 정보 제출 - 지원하는 원격 서비스 (SSH, SNMP 등)에 대한 기본(Default) 비밀번호 정보 포함 - Web Server, DBMS 등에 접속 시 사용되는 기본(Default) 비밀번호 정보 포함
제품 설명서(안내서)	• 제품의 전반적인 기능에 대한 상세
오류 검사 프로세스 설명 자료	• 하드웨어/소프트웨어 자체검사에 대한 상세
이행각서 [공문]	• 하기 내용을 포함해야 함 - "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
구동 소프트웨어 채증 자료	• 하기 사항 중 1개 이상 제출 - 펌웨어 - 펌웨어에 대한 해시값 - 소프트웨어 설치파일

7 인증 마크 표시

인증된 제품에 대해서는 TTA Verified 마크의 사용을 승인한다. 이 로고는 TTA의 공공기관용 NVR 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 증가되며(예. Ver. 2, Ver. 3) 관련 내용 및 이력은 제·개정 이력 현황을 참조한다.

8 기타 사항

(시행일) 본 인증기준은 2018년 1월 1일부터 시행한다.

[붙임] NVR에 요구되는 감사데이터

분류	로그 종류	기준
사용자 접근	[필수] 로그인	• 발생조건: 사용자의 정상 로그인 성공 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간
	[필수] 로그인 실패	• 발생조건: 사용자의 로그인 실패 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간
	[필수] 로그인 잠금	• 발생조건: 사용자가 지정된 횟수 이상 로그인 실패 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 계정 잠금 결과
	[필수] 로그아웃	• 발생조건: 사용자 로그아웃 동작 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 로그아웃 성공 여부
영상 백업	[필수] 시작	• 발생조건: 영상 백업 시작 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 백업하는 영상 채널 정보
	[필수] 종료 및 해시	• 발생조건: 영상 백업 종료 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 백업하는 영상 채널 및 구간 정보, 무결성 검증 정보(해시값)
사용자 계정관리	[필수] 사용자 계정 추가	• 발생조건: 사용자 계정 추가 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 추가한 사용자 정보
	[필수] 사용자 계정 삭제	• 발생조건: 사용자 계정 삭제 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 삭제한 사용자 정보
	[필수] 사용자 계정 정보 변경	• 발생조건: 사용자 계정의 정보 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 사용자 정보 ※ 사용자 계정 정보 : 패스워드, 계정 권한 등
PTZ 제어	[필수] PTZ 제어 시작	• 발생조건: PTZ 제어 시작 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 동작 성공여부
	[필수] PTZ 제어 종료	• 발생조건: PTZ 제어 종료 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 동작 성공여부
트래픽 제어 설정	[필수] IP Filtering	• 발생조건: IP Filtering 관련 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
	[선택] ACL	• 발생조건: ACL 관련 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
원격 관리 설정	[필수] 원격 관리용 IP주소 설정	• 발생조건: 원격 관리용 IP주소 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
	[필수] 원격 관리 서비스 설정	• 발생조건: 원격 관리 서비스 활성화/비활성화 관련 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
관리자 세션 관리	[필수] 관리자 세션 잠금/종료	• 발생조건: 일정시간 동안 동작이 없는 관리자 세션 잠금/종료 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 잠금/종료 결과

분류	로그 종류	기준
	[선택] 관리자 동시접속 제한	• 발생조건: 원격 동시접속 세션 수 제한 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
무결성 검사	[선택] 소프트웨어 무결성	• 발생조건: 소프트웨어 무결성 검사 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 검사 결과, 무결성 검증 정보(해시값)
	[선택] 설정 백업/복원 무결성	• 발생조건: 설정 백업/복원 과정에서 무결성 검사 수행 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 무결성 검증 정보(해시값)
환경 설정	[필수] 설정 백업/복원	• 발생조건: 설정 백업/복원 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 성공 여부
	[필수] 네트워크 설정	• 발생조건: 네트워크 관련 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 변경한 내역
	[필수] 시간 설정	• 발생조건: 시간 설정 변경 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, - 수동 시간설정: 변경 전 · 후의 시간 - 자동 시간설정: NTP 설정 정보, 동기화 전 · 후 시간
	[필수] 녹화 설정	• 발생조건: 녹화 관련 설정 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 녹화 설정정보
시스템	[필수] 시스템 부팅	• 발생조건: 시스템 부팅 시 • 요구정보: 발생 시간
	[필수] 시스템 재부팅	• 발생조건: 시스템 재부팅 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간
	[조건부 필수] 응용프로그램 삭제/재설치	• 발생조건: 응용프로그램 삭제/재설치 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간 ※ 응용프로그램 삭제/재설치 시에도 로그 이력은 유지해야 함
	[필수] 장비 초기화	• 발생조건: 공장 초기화 / 설정 초기화 / 응용프로그램 초기화 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간 ※ 공장 초기화 / 설정 초기화 / 응용프로그램 초기화 시에도 로그 이력은 유지해야 함
	[필수] 시스템 업그레이드	• 발생조건: 시스템 업그레이드 시 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 업그레이드 버전 정보, 성공여부
	[필수] 저장매체 탈부착	• 발생조건: 시스템 동작 중 저장매체 탈부착 시 ※ 시스템 운용이 불가능한 상황은 제외함 • 요구정보: 발생 시간
	[필수] 저장매체 포맷	• 발생조건: 시스템의 저장매체 포맷 시 ※ 시스템 운용이 불가능한 상황은 제외함 • 요구정보: 발생 주체(ID, IP주소 또는 로컬), 발생 시간, 객체(저장매체가 여럿일 경우)