국가 · 공공기관 도입 IT보안제품에 대한

국가용 보안요구사항

국가용 보안요구사항은 제품이 구현해야 하는 모든 보안기능이 아닌 기본적으로 만족해야 할 사항을 기술한 문서입니다. 국가정보원은 대상 제품이 다양한 보안위협에 대응하기 위해 국가용 보안요구사항에 기재된 항목뿐 아니라 다양한 보안기능을 추가 구현하여 제품의 보안성을 제고할 것을 적극 권장합니다.

NIS

3편 제품 보안요구사항

영상정보처리기기

영상정보처리기기 제품군 국가용 보안요구사항 작성에

기여한 업계 · 기관의 노력에 감사드립니다.

국군방첩사령부	(주)베스트디지탈	(주)세연테크	(주)셀링스시스템
(주)아이디스	(주)아이티엑스에이아이	(주)에이앤티코리아	(주)원우이엔지
(주)웹게이트	(주)트루엔	(주)프로브디지털	한국씨텍(주)
한화비전(주)			

공공 · 국방분야 공통

34장
IP카메라 보안요구사항

1절 일반사항

1. 운용 환경 정의

■ 가정사항

○ 제품의 인가된 관리자는 장비의 펌웨어 및 장비 내에서 사용되는 소프트웨어에 대한 최신 패치를 정기적으로 수행한다.

○ 제품의 인가된 관리자는 웹브라우저 등을 통해 제품에 접속할 수 있으며, 이 때 *HTTPS, TLS, SSH 등*의 통신을 이용하여 암호통신 프로토콜을 수행한다.

○ 제품은 로컬콘솔 형태의 접속이 불가능하며, 최초 및 운용을 위한 기본 접속 수단은 웹 브라우저이다.

■ 제품 개요

IP카메라는 사람 또는 사물의 영상 등을 촬영하고 선택적으로 오디오 획득도 가능하며, 영상과 오디오를 IP 네트워크를 통하여 전송할 수 있는 하드웨어 일체형 장비이다. 전송하는 데이터는 영상(이미지 또는 비디오)이며 관리자의 선택에 의해 오디오가 포함될 수 있다. 제품은 이미지 센서로 획득한 영상과 마이크로 획득한 오디오를 압축하여 IP 네트워크로 전송할 수 있으며 이를 위한 미디어 서버와 제어 · 관리를 위한 웹 서버를 포함하고 있다.

IP카메라 관리접속시 영상 모니터링이 가능해야 하며 IP카메라는 내장된 서버에서 영상을 송신한다. IP카메라와 영상정보 관리 · 저장제품간의 연동을 위해 〈별표 1〉에

기재된 예시와 같은 영상 전송 관련 표준 프로토콜을 사용할 수 있다.

■ 운용 환경

영상정보처리기기가 운용되는 네트워크는 인터넷 및 업무 · 행정망과 분리된 별도 단독망 구성이 원칙이며, 원격지 등에 설치하여 단독망 구성이 불가할 경우에는 VPN 등으로 암호화된 통신 구간에서 운용되어야 한다. 제품에 대한 관리 단말(PC)이 별도로 운용될 수 있으며 관리 단말에서는 웹브라우저 접속 등의 방법으로 관리 활동이 이뤄질 수 있다.

IP카메라는 연동된 영상정보 관리 · 저장제품의 요청에 따라 데이터(영상 또는 오디오)를 제공할 수 있다. 제품은 운용중 발생하는 로그의 외부 저장 및 관리를 위해 로그 서버, 시간 동기화를 위한 NTP 서버를 운용환경으로 포함할 수 있다. 이외에 제품에 따라 기능 활용을 위해 필요한 외부 실체가 있는 경우 운용 환경에 추가적으로 제시될 수 있다.

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.

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

■ 운용환경 요구사항

○ 제품의 인가된 관리자는 다음의 지침 및 가이드에서 부여한 의무를 정확하게 수행해야 한다.

분야	명칭	주관기관
공공	국가정보보안기본지침	국가정보원
	국가 · 공공기관 영상정보처리기기 도입 · 운영 가이드	
	공공기관 고정형 영상정보처리기기 설치 · 운영 가이드	개인정보보호위원회
국방	국방보안업무훈령	국방부
	국방정보보안시스템 업무훈령	

○ 제품의 인가된 사용자는 악의없이 도입한 목적에 맞게 제품을 운용해야 한다.

○ 제품의 인가된 사용자는 제품이 제공하는 저장기능이 아닌 방법으로 영상을 저장하지 않아야 한다.

○ 제품의 인가된 관리자는 감사기록 유실에 대비하여 감사 데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(*외부 로그 서버, 별도 저장장치 등*) 등을 수행한다.

○ 제품의 인가된 관리자는 제품 동작에 불필요한 운영체제상의 서비스나 수단 등을 제거하고 취약점에 대한 개선 작업을 통해 운영체제의 신뢰성과 안전성을 보장한다.

○ 제품의 인가된 관리자는 네트워크 구성, 변경, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 제품 운용정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.

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

■ 공통보안요구사항의 적용

공통보안요구사항을 적용하지 않는다.

여 백

2절 보안요구사항

1. 영상 보안

제품은 영상정보의 저장, 전송 등에 대한 보안기능을 제공해야 한다.

1.1 영상 프로토콜 인증

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.

1.2 영상 전송 보안

1.2.1

필수

기기 간 연동 및 영상 전송 관련 표준 프로토콜 통신시 전송 데이터를 보호하기 위해 암호통신 채널을 사용하여 전송해야 한다.

요구항목

① 암호통신을 위해서 표준 프로토콜(*ONVIF, RTSP 등*)을 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.

③ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

④ HTTPS Tunneling(RTP/RTSP/HTTPS/TCP) 전송 방식을 사용할 수 있다.

점검시 유의사항

① 패킷 모니터링 도구를 활용하여 전송 데이터에 대한 기밀성, 무결성을 제공하는지 확인해야 한다.

1.3 영상 저장 보안

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.

② 제품은 영상정보 관리 · 저장제품 이외 외부 IT실체에 영상정보를 파일로 제공하는 경우에는 파일을 암호화하여 제공해야 한다.

③ 저장하는 영상 스트림 중 모든 I-프레임은 암호화해야하며 다른 데이터는 개발업체의 선택에 따라 암호화될 수 있다.

④ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

⑤ 제품 내부 저장소에 저장된 영상의 일부를 제품 외부에 파일형태로 백업하는 기능을 제공할 경우, 암호화 및 무결성 검증 기능을 제공해야 한다.

점검시 유의사항

① 제품이 영상 저장 기능을 지원하지 않는 경우 '해당사항 없음'으로 판정한다.

② 휘발성 메모리에 저장하는 경우는 영상 저장으로 간주하지 않는다.

1.3.2

조건부 필수

카메라의 오디오 녹음을 on · off 할 수 있는 기능을 제공해야 한다.

조 건	오디오 녹음 기능 지원시

요구항목

① 기본(default) 상태에서 오디오 녹음 기능은 'on'과 'off'가 모두 선택 가능해야 하며 초기값은 'off'로 설정되어야 한다.

점검시 유의사항

① 오디오 녹음 기능은 'on'과 'off'가 모두 선택 가능한지 확인한다.

② 'on'과 'off'를 각각 선택하여 오디오 녹음 기능의 활성화 · 비활성화가 정상 작동하는지 확인한다.

③ 초기값이 'off'로 설정되어있는지 확인한다.

④ 제품이 오디오 녹음 기능을 지원하지 않는 경우 '해당사항 없음'으로 판정한다.

1.4 영상 관리 보안

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.

참고 사항

① 제품이 설정 초기화로 기본(default) 상태가 된 경우, 관리도구에 의한 설정은 다시 허용될 수 있다.

점검시 유의사항

① 제품이 관리도구에 의한 검색 · 설정 기능이 없는 경우 '해당사항 없음'으로 판정한다.

2. 식별 및 인증

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

2.1 사용자 등 식별 및 인증

2.1.1

필수

제품은 사용자의 신원을 검증하기 위해 사용자 계정 · 패스워드 기반 식별 및 인증 기능을 제공해야 한다.

요구항목

① 사용자가 제품의 정당한 사용자임을 확인하기 위해 반드시 식별 및 인증을 수행해야 한다.

② 관리자는 각 사용자 또는 그룹별로 권한을 부여할 수 있어야 한다.

③ 사용자 계정(ID)은 각각 고유한 값으로 등록되어 중복되지 않아야 한다.

점검시 유의사항

① 제품이 제공하는 전체 사용자 역할을 확인해야 한다.

- 관리자의 경우 관리접속 등 접속 경로별로 식별 및 인증을 요구하는지 확인해야 한다.
- 일반사용자가 존재하는 경우, 제품에 접근시 식별 및 인증을 요구하는지 확인해야 한다.

② 관리서비스 접근시 식별 및 인증을 요구하는지 확인해야 한다.

③ 영상 관련 기능(*실시간 영상 모니터링, 재생(검색), 제품 외부에 영상 저장 등*) 접근시 식별 및 인증을 요구하는지 확인해야 한다.

④ 관리자가 각 사용자 또는 그룹별로 권한을 설정할 수 있는지 확인해야 한다.

⑤ 알려진 취약점이 존재하는지 확인해야 한다.

- 계정 및 패스워드 입력필드에 입력 가능한 문자열을 제한하는지 확인이 필요하다.
- 시험기관이 '취약점 개선 내역서'를 제출받아 검토한 후 취약성 시험을 생략할 수 있다.

⑥ 시험기관은 취약점 점검 도구 사용의 적절성을 확인하고 시험에 사용해야 한다.

⑦ 사용자 인증을 우회하여 관리화면으로 접근할 수 있는지 확인해야 한다.

2.1.2

조건부 필수

제품은 연동하는 외부 IT실체를 인증해야 한다.

조 건	제품에서 외부 IT실체를 인증하는 경우

참고 사항

① *영상정보 관리 · 저장제품 연동을 위한 패스워드, SNMP 인증 패스워드, SNMP 암호화 패스워드 등*이 적용대상이 될 수 있다.

점검시 유의사항

① 시험원은 제품과 외부 IT실체가 연동하기 위해 제품이 인증해야 하는 외부 IT 실체를 모두 조사해야 한다.

② 제품이 인증하는 외부 IT실체가 없을 경우 '해당사항 없음'으로 판정한다.

2.2 인증실패 대응

2.2.1

필수

제품에서 사용자 인증이 설정된 횟수만큼 연속적으로 실패하면, 식별 및 인증 기능이 비활성화 되어야 한다.

요구항목

① 식별 및 인증 기능을 비활성화한 후 활성화 하는 방법의 예로써 *계정잠금 후 지정된 시간이 지난 이후 활성화, 계정잠금 후 활성화를 위한 다른 식별 및 인증 수단 제공 등*이 있다.

② 식별 및 인증이 비활성화되는 연속적인 인증 실패 횟수는 5회 이하의 값으로 고정되거나 5회 이하의 값으로 설정할 수 있어야 한다.

③ 일정시간 동안 인증 기능을 비활성화하도록 구현하는 경우 재활성화까지 소요되는 시간은 5분 이상의 값으로 고정되거나 설정할 수 있어야 한다.

점검시 유의사항

① 제출문서를 통해 잘못된 인증 정보를 사용한 반복된 인증 시도를 제한하는 방법이 있는지 확인해야 한다.

② 시험원은 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP, ONVIF, RTSP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

③ 비활성화 된 계정 외의 다른 관리자 계정으로 인증 성공시 잠금된 계정의 잠금이 해제되지 않는지 확인해야 한다.

④ 관리자 접속 PC의 시간을 식별 및 인증 비활성화 이전 시간으로 변경하여

인증을 시도하는 경우에도 비활성화 기능이 정상적으로 동작하는지 확인해야 한다.

⑤ 횟수(5회)나 기간(5분)은 기본값으로 고정되거나 설정할 수 있어야 한다.

2.2.2

필수

제품은 관리자 인증시 설정된 횟수만큼 연속적으로 실패하면, 관리자가 즉시 확인할 수 있는 수단을 통해 통보해야 한다.

요구항목

① *알람, 문자 메시지, 이메일 등* 중에서 한 가지 이상의 수단을 통해 통보해야 한다.

점검시 유의사항

① 시험원은 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP, ONVIF, RTSP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

2.3 패스워드 등 민감정보 생성 및 안전성 검증

2.3.1

필수

제품은 패스워드 등록 및 변경시 〈표 1〉의 보안성 기준을 만족해야 한다.

요구항목

〈 표 1. 패스워드 보안성 기준 유형(1)〉

구분	내용	비고
준수 사항	9자리 이상의 길이 확보	필수
	숫자, 대문자(영문), 소문자(영문), 특수문자가 각 1개 이상 포함	필수

구분	내용	비고
금지 항목	사용자계정(ID)과 동일한 패스워드 설정금지	필수
	동일한 문자 · 숫자 연속적으로 반복사용 금지	필수
	키보드의 연속된 문자 또는 숫자의 순차적 나열 금지	필수
	직전 사용된 패스워드 재사용 금지	둘중 어느 하나 구현
	3개월 이내 사용된 패스워드 재사용 금지	

점검시 유의사항

① ‘3개월 이내 사용된 패스워드 재사용 금지’ 기능을 선택, 구현한 경우 재사용 금지 기간은 3개월 이내에서 고정하거나 가변적으로 설정할 수 있어야 한다.

② ‘키보드상의 연속되거나 순차적인 입력’으로 간주되는 문자 · 숫자의 입력은 다음과 같다.

- △‘q’, ‘w’, ‘e’, ‘r’ △‘a’, ‘s’, ‘d’, ‘f’ △‘1’, ‘2’, ‘3’, ‘4’ 등 좌우로 연속한 문자 또는 숫자를 4개 이상 입력하는 경우.(특수문자는 제외한다.)

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

요구항목

① 적용대상으로 영상정보 관리 · 저장제품 연동을 위한 패스워드, SNMP 인증 · 암호화 패스워드 등이 될 수 있다.

② 외부 IT실체 인증에 패스워드가 사용되는 경우 △2.3.1의 보안성 기준을 준수해야 한다.

참고 사항

① 외부 IT실체 인증 기능을 위한 패스워드의 경우 보안성 기준에 포함된 문자라도

외부 IT실체가 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 제품과 외부 IT실체가 연동하기 위해 제품이 인증해야 하는 외부 IT 실체를 모두 조사하고 인증에 필요한 인증 정보를 설정하는 인터페이스가 제공되는지 확인해야 한다.

② 시험원은 외부 IT실체를 인증하는데 사용되는 인증 정보가 제품이 통제하는 저장소에 저장되는 경우 '4.2 저장 데이터 보호' 요구사항에 따라 저장되는지 확인해야 한다.

③ 제품이 인증하는 외부 IT실체가 없을 경우 '해당사항 없음'으로 판정한다.

2.4 인증 정보 재사용 방지

2.4.1

필수

제품은 사용자 인증 정보의 재사용을 방지해야 한다.

요구항목

① △1.1.1과 △2.1.1에서 규정한 식별 및 인증에 사용되는 인증 정보에 필수적으로 적용한다.

② 세션 ID를 암호화하거나 세션 ID의 유일성을 보장(*타임스탬프, 세션 만료시간 설정 등*)하여 방지할 수 있다.

③ 제품에서 재사용이 금지된 인증 정보의 재사용 시도를 탐지한 경우 인증에 실패해야 하며 인증 실패 사건에 대한 감사기록을 생성해야 한다.

참고 사항

① 제품이 외부 IT실체의 추가적인 식별 및 인증 수행 결과만을 전달받는 경우 해당 인증 정보의 재사용 방지는 외부 IT실체에서 제공한다고 가정한다.

② 세션 만료시간은 제공 서비스 특성을 고려하여 최소화 할 수 있는 값으로

설정해야 한다.

점검시 유의사항

① 사용자가 로그아웃 하지않고 이전에 사용한 인증 정보(*세션ID, 쿠키 등*)로 변경한 후 다시 로그인시 실패여부를 확인해야 한다.

② 사용자 로그아웃 이후 이전에 사용한 인증 정보(*세션ID, 쿠키 등*)로 변경하여 재로그인시 실패여부를 확인해야 한다.

③ 사용자 로그인시 사용자 패스워드는 암호화된 상태로 전송하는지 확인해야 한다.

2.5 인증 피드백 보호

2.5.1

필수

제품은 인증에서 사용되는 정보를 출력장치에 표시할 때 내용을 표시하지 않아야 한다.

요구항목

① △1.1.1 △2.1.1 △2.3.1에서 규정한 인증 정보가 출력장치에 표시되는 경우에 적용한다.

② 인증에 사용되는 정보는 *입력내용의 미표시, 입력문자 대신 "*" 으로 표시 등*의 형태로 출력해야 한다.

③ 사용자 로그인시 인증 정보가 메모리 영역에 평문으로 노출되지 않아야 한다.

점검시 유의사항

① 시험원은 제품의 인증 정보 입력이 필요한 보안 기능에 대해 조사해야 한다.

② 사용자가 로그인할 때 뿐 아니라 신규 사용자 계정 생성, 패스워드 변경 등 인증정보를 입력하는 기능을 모두 식별하여 요구사항 만족여부를 확인해야 한다.

③ 시험원은 사용자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP,*

ONVIF, RTSP 등)에 대해서 요구사항을 만족하는지 확인해야 한다.

2.5.2

필수

제품은 식별 및 인증 실패시, 실패 사유에 대한 피드백(*존재하지 않는 계정(ID), 패스워드 오류 등*)을 제공하지 않아야 한다.

점검시 유의사항

① 잘못된 인증 정보 입력으로 인증실패 유도 후, 알림 메시지에 인증 실패 사유를 추측할 수 있는 피드백을 제공하는지 확인해야 한다.

3. 보안관리

인가된 관리자만이 제품의 보안기능 및 중요데이터에 대한 관리를 수행하도록 허용함으로써 제품의 보안관리를 위한 요구사항을 만족하는지 확인한다.

3.1 보안관리 기능

3.1.1

필수

제품은 인가된 관리자에게 보안기능, 보안정책, 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공해야 한다.

요구항목

① 보안관리 기능에 해당되는 사항은 다음과 같다.

- 보안기능의 동작을 결정할 수 있는 조건 또는 규칙을 추가, 삭제, 변경하는 기능.
- 조건 또는 규칙에 따라 제품이 수행해야 할 행동을 추가, 제거, 변경하는 기능.
- 제품의 설정을 선택, 변경하는 기능.
- 카메라 제어를 설정, 변경하는 기능.

② 제품이 구현해야 하는 보안관리 기능은 아래 〈표 2〉 와 같다.

〈 표 2. 제품이 구현해야하는 보안관리 기능 〉

소분류	보안관리	비고
식별 및 인증	사용자의 등록, 삭제, 수정, 권한 부여	제품에 등록된 사용자가 유일한 경우 해당사항 없음
	사용자의 패스워드 조합 · 길이 정책 설정	기능 제공시 필수
	사용자의 인증 실패 허용 횟수 설정	기능 제공시 필수
	사용자의 인증 실패 대응방법 설정	기능 제공시 필수
	사용자 인증 기능 비활성화된 후 활성화까지의 시간 설정	기능 제공시 필수
	제품이 인증하는 외부 IT실체 인증정보 설정	기능 제공시 필수
보안 관리	관리용 단말기의 IP 등록, 삭제, 수정	
	중요 데이터, 설정정보, 감사기록 등의 백업	기능 제공시 필수
	중요 데이터, 설정정보, 감사기록 등의 복구	기능 제공시 필수
	관리접속 서비스 활성화, 비활성화	기능 제공시 필수
	외부 IT실체 접근을 위한 인증정보 설정	기능 제공시 필수
	카메라 제어(PTZ 등) 설정 및 동작 설정 초기화	기능 제공시 필수
자체보호	관리자 요청에 의한 제품의 보안기능 자체시험 수행	기능 제공시 필수
	자체시험 실패시 대응행동 설정	기능 제공시 필수
	관리자 요청에 의한 제품의 설정값 및 제품 자체의 무결성 검사 수행	
	무결성 검사 실패시 대응행동 설정	기능 제공시 필수
업데이트 보호	관리자에 의한 업데이트 파일 유효성 수동 검증	기능 제공시 필수
	관리자에 의한 업데이트 파일 설치 실패 수동 복구	기능 제공시 필수
	제품 버전정보 조회	
세션 관리	사용자 세션 잠금, 종료 시간 설정	기능 제공시 필수
	(세션 잠금의 경우) 세션의 잠금 해제시 관리자 또는 개별 사용자 인증	

소분류	보안관리	비고
세션 관리	사용자 동시 접속 세션수 설정	기능 제공시 필수
감사기록	감사기록의 조회	
	감사기록 손실 대응 관련 설정	기능 제공시 필수

점검시 유의사항

① 시험원은 제품이 제공하는 모든 보안관리 기능을 식별해야 한다.

- 시험원은 제품이 제공하는 모든 보안관리 기능이 「보안기능 구현명세서」 또는 「보안기능 운용설명서」에 기술되어 있는지 확인해야 한다.
- 시험원은 모든 보안관리 기능이 요구사항을 만족하는지 확인해야 한다.

② 보안관리 기능은 인가된 관리자만 실행할 수 있는지 확인해야 한다.

③ 입력값에 대한 검증(*허용되지 않는 문자, 길이 등 제한 등*)을 수행하는지 확인해야 한다.

3.2 관리접속 기능

3.2.1

필수

제품은 모든 관리접속에 대해 활성화 · 비활성화 기능을 제공해야 한다.

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리접속을 조사해야 한다.

② 제품의 기본 접속 수단인 웹브라우저(HTTPS) 접속은 기본(default) 상태에서 활성화를 허용하며, 다른 모든 관리접속은 기본(default) 상태에서 비활성화 되어 있어야 한다. 다만, 제품이 관리도구에 의한 최초 설정이 필요할 경우에는 △1.4.1의 요구사항에 따른 관리도구 접속의 활성화가 추가로 허용될 수 있다.

③ 제품 외부에서 포트스캔을 수행하여 불필요한 포트가 존재하는지 확인해야 한다.

④ 제품 내에서 운용되는 DBMS에 대해 원격으로 직접 접근하는 것은 제한되야 한다.

⑤ 외부에서 접근 가능한 API를 제공하는 장비의 경우, 시험원은 해당 서비스에 대한 활성화 · 비활성화 기능 여부를 확인해야 한다.

⑥ 시험원은 제품에서 관리접속이 암호통신만을 사용하는지 확인해야 한다.

3.3 보안관리용 IP제한

3.3.1

필수

제품은 접속 가능한 관리용 단말기의 IP를 제한하는 기능을 제공해야 한다.

요구항목

① 관리용 단말기 IP 주소를 등록, 삭제, 수정 가능해야 한다.

② 관리 용도 대신에 읽기 권한만 가지는 관리자(*영상 모니터링 관리자 등*)가 접속 가능한 관리용 단말기는 추가로 등록해서 운용 가능하다.

③ 접속 가능한 관리용 단말기의 IP는 단일 호스트 단위로 1개씩만 추가 가능하다.

④ 192.168.10.2~253 등과 같이 IP 주소 범위를 지정하여 추가하는 방식 또는 네트워크 전체 범위를 의미하는 0.0.0.0, 192.168.10.*, any 등을 이용한 등록은 허용되지 않는다.

⑤ 기본(default) 상태에서 운용 상태로 전환되기 전, 접속 가능한 관리용 단말기의 IP를 등록하는 과정이 있어야 한다.

점검시 유의사항

① IP 등록시 단일 IP별로 등록 가능한지 확인해야 한다.

② IP주소 범위 지정하여 추가하는 방식을 허용하지 않는지 확인해야 한다.

③ 관리 용도 대신에 읽기 권한만 가지는 관리자(*영상 모니터링 관리자 등*)가 접속 가능한 PC는 추가로 등록 가능하다.

3.4 기본 제공되는 계정 및 패스워드 등의 관리

3.4.1

필수

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

요구항목

① 최초 접속시, 기본 제공되는 계정을 화면에 출력해야 한다.

② 기본 제공되는 계정은 최초 접속시 강제 변경 또는 사용중지(Disable)되어야 한다.

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.

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리접속(*SSH, HTTPS, ONVIF, RTSP 등*)에 대해 조사해야 한다.

② 제품의 모든 기능은 제공되는 계정의 변경 · 사용중지 또는 생성이 진행된 이후에만 동작되는지 확인해야 한다.

③ 시험원은 화면에 출력되지 않는 계정이 있는지 확인해야 한다.

④ 시험원은 화면에 출력되지 않은 계정을 추가로 식별한 경우, 시험결과보고서에 해당 계정을 백도어로 기록하고 '불만족'으로 판정한다.

3.4.2

필수

제품은 최초 제품 접속(*웹 브라우저 접속 등*) 시 관리자 기본(default) 패스워드를 강제 변경 · 생성하는 기능을 제공해야 한다.

요구항목

① 기본(default) 패스워드가 존재하는 경우 최초 제품 접속시 기본(default) 패스워드를 변경하는 기능을 제공해야 하며, 이후 제품의 관리 접속이 가능해야 한다.

② 기본(default) 패스워드가 없는 경우, 신규 패스워드를 생성해야 하며, 이후 제품의 관리접속이 가능해야 한다.

- 패스워드는 2.3.1의 보안성 기준을 준수해야 한다.

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리접속(*SSH, HTTPS, ONVIF, RTSP 등*)에 대해 조사해야 한다.

② 제품의 모든 기능은 기본(default) 패스워드 변경 또는 생성이 진행된 이후에만 동작되는지 확인해야 한다.

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 패스워드가 필요한 기능 제공시

요구항목

① 기본(default) 패스워드의 예시로는 *DBMS 패스워드, 웹서버 · WAS서버 패스워드 등*이 있다.

② 제품이 DBMS에 접근하기 위한 기본(default) 패스워드를 저장하는 경우 제품에서 기본(default) 패스워드를 변경하는 기능을 제공해야 한다.

③ 제품이 웹서버 · WAS서버에 접근하기 위한 기본(default) 패스워드를 저장하는 경우 기본(default) 패스워드를 변경하는 기능을 제공해야 한다.

④ 패스워드 생성시 추가적 식별 및 인증 기능 병행 유무에 따라 2.3.1의 보안성

기준을 준수해야 한다.

⑤ 제품에 DBMS · 웹서버 · WAS서버에 접근하기 위한 기본(default) 계정(ID)이 존재하는 경우 이를 변경하는 기능을 제공할 수 있다.

참고 사항

① 제품 내에 DBMS · 웹서버 · WAS서버 등을 포함할 수 있고, 제품 외부에 별도로 존재하는 DBMS · 웹서버 · WAS서버 등과 연동할 수도 있다.

② 패스워드 보안성 기준에 포함된 문자라도 연동하는 외부 IT실체에서 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 기타 인증 정보가 필요한 제품 내에 존재하는 또는 제품과 연동하는 인증서버, DBMS · 웹서버 · WAS서버 등에 대해 조사해야 한다.

② 시험원은 인증 정보가 패스워드인 경우 2.3.1의 보안성 기준을 만족하는지 확인해야 한다.

③ DBMS · 웹서버 · WAS서버 관리자 기본(default) 계정(ID)을 변경하는 기능은 선택적으로 구현 가능하다.

④ 제품이 내부 구성요소 또는 외부 IT실체에 접근하는 기능이 없는 경우 '해당 사항 없음'으로 판정한다.

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

요구항목

① 인증정보의 예시로는 SMTP 서버에서 제품을 인증하기 위해 사용하는 패스워드 등이 있다.

② 패스워드는 '서버 공통보안요구사항 1.3.2'에 규정된 보안성 기준의 준수를 권고한다.

- 다만, 패스워드 보안성 기준에 포함된 문자라도 연동하는 외부 IT실체에서 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 제품과 연동시 제품을 인증한 후 접근을 허용하는 SMTP 서버 등에 대해 조사해야 한다.

② 시험원은 제품과 외부 IT실체간 연동을 위해 외부 IT실체에서 제품을 인증하는 경우를 모두 조사하고 인증 정보를 설정하는 인터페이스가 제공되는지 확인해야 한다.

③ 시험원은 인증 정보가 패스워드인 경우 '서버 공통보안요구사항 1.3.2'의 보안성 기준을 만족하는지 확인해야 한다.

④ 제품이 외부 IT실체에 인증받는 기능이 없는 경우 '해당사항 없음'으로 판정한다.

4. 데이터 보호

제품이 사용자 또는 외부 IT실체와의 통신 간에 전송되는 데이터를 노출 · 변경으로부터 보호하기 위해 암호통신을 지원하는지 확인한다. 제품은 저장소에 저장되는 보안기능 관련 데이터를 비인가 노출로부터 보호해야 한다.

4.1 전송 데이터 보호

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.

③ 암호통신 채널은 제품에 직접 구현하거나 제품이 운영환경을 이용하여 제공하도록 구현될 수 있다.

④ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

① 제품의 기본(default) 상태에서 관리도구와의 통신은 이 요구사항을 적용하지 않을 수 있다.

점검시 유의사항

① 패킷 모니터링 도구를 활용하여 전송 데이터에 대한 기밀성, 무결성을 제공하는지 확인해야 한다.

② 시험원은 요구사항에 따른 정확한 구현을 시험하기 위해 필요시 개발자를 직접 대면하여 구현내용에 대한 설명을 요청할 수 있다.

4.1.2

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

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.

③ 암호통신 채널은 제품에 직접 구현하거나 제품이 운영환경을 이용하여 제공하도록 구현될 수 있다.

④ 제품이 보안기능을 제공하기 위해 외부 IT실체와 연동하는 기능을 제공하는 경우 이 요구사항을 적용해야 한다.

⑤ 외부 IT실체와 연동시 암호통신 채널을 사용하여 전송 데이터를 보호하지 않는다면 전송 데이터 기밀성, 무결성 보호의 불필요성이 입증되어야 한다.

⑥ 암호통신 채널을 지원하지 않는 통신서비스는 비활성화 할 수 있어야 한다.

⑦ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

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.

점검시 유의사항

① 제품이 보안기능을 제공하기 위해 외부 IT실체와 연동을 지원하는 경우 이 요구사항을 적용해서 시험해야 한다.

② 다만, 외부 IT실체중에서 NTP 서버와의 통신에는 이 요구사항을 적용하지 않는다.

③ syslog를 지원하면 *syslog over TLS(RFC 5424), syslog over DTLS(RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.

④ 제품이 외부 IT실체와 연동하는 기능이 없는 경우 '해당사항 없음'으로 판정한다.

4.2 저장 데이터 보호

4.2.1

필수

중요정보를 제품 내부에 저장할 때 정해진 방식으로 저장해야 한다.

요구항목

① 최소한 다음의 중요정보를 제품이 저장하는 경우 암호화하여 저장해야 한다.

- 제품이 사용자 식별 및 인증을 위해 사용하는 패스워드.
- 제품이 추가적인 식별 및 인증을 위해 사용되는 인증정보.
- 데이터 암호화 키(DEK: Data Encryption Key)

② 데이터 암호화 키(DEK)는 키 암호화 키(KEK : Key Encryption Key)를 사용, 암호화하여 저장해야 한다.

③ 키 암호화 키(KEK) 생성 및 저장 등과 관련된 요구사항은 '9.2 암호키 생성' 및 '9.3 암호키 저장' 요구사항을 만족해야 한다.

④ 다음과 같은 정보를 제품이 저장하는 경우 *암호화, 접근통제 등*의 방식으로 저장해야 한다.

- 제품과 외부 IT실체의 연동시 상호간 인증에 사용되는 정보.
- 제품이 제품 내부 또는 외부에 존재하는 DBMS · 웹서버 · WAS서버에 접근하기 위해 필요한 DBMS · 웹서버 · WAS서버 관리자 패스워드.
- 암호키.(사전공유키, 대칭키, 개인키)
- 조직의 중요정보를 포함하는 탐지 규칙, 시그니처 등.

⑤ 제품이 사용자 식별 · 인증을 위해 사용하는 사용자 패스워드는 일방향 암호(해시) 또는 양방향 암호를 이용하여 저장해야 한다.

- 일방향 암호화 수행시 패스워드에 salt라는 랜덤하게 생성한 값을 추가하여 적용할 필요가 있다.
- salt 값은 비밀일 필요는 없으며, 난수발생기를 이용하여 생성하고 크기는 최소 48bit 이상이어야 한다.

- iteration count는 가능한 큰 값을 적용해야 한다.(최소 1000회 이상)

⑥ 제품 운영에 필요한 DBMS · 웹서버 · WAS서버 관리자 패스워드 등은 공개키 · 대칭키 암호 알고리즘을 적용하여 암호화하여 저장할 수 있다.

⑦ 암호키는 *사전공유키, 대칭키, 개인키 등*을 의미하며 제품 관리접속 · 로컬접속, 제품 구성요소간 연동 설정에 사용되는 키들이 모두 대상이다.

⑧ 암호화해서 저장해야 하는 최소한의 중요정보에 포함된 패스워드 및 암호키는 제품에 하드코딩하여 저장할 수 없다.

⑨ 신청업체는 제품이 지원하는 저장 데이터 보호 방법에 대한 상세한 설명자료(「보안기능 구현명세서」)를 제출하여 안전성을 입증해야 한다.

⑩ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

⑪ 검증필 암호모듈(KCMVP)의 사용을 권고한다.

참고 사항

① 제품을 운용하는 조직의 중요정보가 통합보안관리, 침입방지시스템 제품의 탐지 규칙, 시그니처 등에 포함될시 노출로부터 보호하는 방식으로 저장해야 한다.

② 저장된 모든 중요정보는 읽거나 유추할 수 없어야 한다.

③ 난수발생기는 '9. 암호 지원' 요구사항에 따라 국내 · 외 표준을 준수하여 구현되어야 한다.

점검시 유의사항

① 동일 패스워드 입력시 동일한 암호문이 생성 · 저장되지 않음을 확인해야 한다.

② 패스워드를 일방향 암호화 할 경우 표준에 따라 저장되는 값이 생성되는지 확인해야 한다.

③ 패스워드를 암호화 하여 저장할 경우 '9. 암호 지원' 요구사항에 따라 암호키가 저장되는지 확인해야 한다.

④ '9. 암호 지원' 요구사항에 따라 난수발생기를 사용하는지 확인해야 한다.

⑤ *DB 접속 패스워드, 자동 로그인에 필요한 패스워드, 키 암호화 키 등*이 제품에 하드코딩되어 있지 않는지 확인해야 한다.

4.2.2

필수

제품은 저장된 제품 설정값(*보안정책, 환경설정 매개변수 등*)에 인가된 관리자만이 접근할 수 있도록 보호하는 기능을 제공해야 한다.

요구항목

① 제품은 인가된 관리자만이 제품 설정값에 접근할 수 있도록 하는 인터페이스를 제공해야 하며, 인가된 관리자 외에는 제품 설정값에 접근할 수 없어야 한다.

- 접근이라 함은 읽기, 변경, 삭제 등의 오퍼레이션을 의미한다.

② 제품 설정값을 외부에 파일형태로 백업하는 기능을 제공할 경우, 암호화하는 기능을 제공해야 한다.

③ 암호화시 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

① 제품 설정값은 연동되는 운영환경인 DBMS에 파일형태로 저장될 수 있다.

② 제품 보안기능으로 완전히 구현할 수 없는 경우, 운영환경에서 제품 설정값 저장소를 보호할 수 있도록 지원할 수 있다.

- 제품 설정값이 연동되는 운영환경의 DBMS에 저장되는 경우, DBMS의 식별 및 인증 기능을 이용, 비인가된 사용자의 접근으로부터 보호할 수 있다.

점검시 유의사항

① 제품 설정값을 내부에 저장할 경우 암호화하여 보호하는 기능을 제공하는 경우도 요구사항 '만족'으로 판정이 가능하다.

② 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

5. 자체보호

제품은 보안기능이 정상적으로 동작함을 보장하기 위해서 주기적 또는 관리자 요청에 의해 자체시험을 수행할 수 있어야 한다. 보안기능을 제공하는 메커니즘 및 데이터의 무결성을 확인하여 제품의 보안 기능을 보호해야 한다.

5.1 보안기능 자체 시험

5.1.1

필수

제품은 구동(또는 실행) · 운용중에 주기적 또는 관리자의 요청에 의해 자체시험을 수행해야 한다.

요구항목

① 제품 구동(또는 실행)시 필수로 자체시험을 수행해야 하고 운용중에는 주기적 또는 관리자의 요청에 의한 수행을 지원해야 한다.

② 자체시험 대상은 제품의 주요 프로세스를 의미하며 프로세스가 정상적으로 실행되고 있는지 확인해야 한다.

③ 자체시험 대상은 신청업체가 선택 가능하나, 시험 대상이 되는 실체의 비정상 상태(*오류, 정지 등*)로 인하여 제품의 보안 기능에 영향을 미치는 경우 해당 실체는 자체시험 대상으로 반드시 포함해야 한다.

④ 자체시험 수행 이력은 화면 출력, 감사기록을 통해 확인할 수 있어야 한다.

⑤ 제품 시작시 및 운영중 제품 범위에 포함되는 하드웨어(*메모리, 플래시, NIC 등*) 및 소프트웨어(*프로세스 등*)의 오류를 탐지할 수 있는 자체시험을 수행해야 한다.

⑥ 신청기관은 제출문서에 자체시험 기능에 대해 상세히 기술해야한다.

점검시 유의사항

① 하드웨어 · 운영체제는 제품 범위에 포함된다.

② 시험원은 제출물에 자체시험에 대해 상세히 기술되어 있는지 확인한다.

5.1.2

필수

제품의 자체시험 결과가 실패인 경우 대응기능을 수행해야 한다.

요구항목

① 제품은 정확한 작동을 보장하기 위해 구현된 대응 기능을 수행하거나 관리자가 설정한 대응 기능을 수행해야 한다.

② 자체시험 결과에 대한 감사기록을 생성해야 한다.

③ 자체시험 결과 실패시 수행하는 대응기능의 예로써 *프로그램 실행중단, 경고 메시지 화면 출력, 프로세스 재구동 등*이 있다.

④ 관리자가 대응기능을 설정할 수 있도록 보안관리 기능을 제공할 수 있다.

점검시 유의사항

① 제품이 △처음 실행(또는 구동)시 △관리자 수동 요청시 자체시험이 실패한 경우를 모두 확인해야 한다.

② 대응기능에 대한 관리자 설정기능이 있는 경우, '3.1 보안관리 기능' 요구사항에 따라 시험을 수행해야 한다.

5.2 무결성 검증

5.2.1

필수

제품은 자체 및 설정값의 무결성을 검증하는 기능을 제공해야 한다.

요구항목

① 무결성 검증 대상은 제품의 설정값(*환경설정파일 등*) 및 제품 자체(*프로세스, 라이브러리, 실행파일 등*)이다.

② 제품을 처음 실행시(또는 구동시) 무결성 검증을 수행해야 하며, 부가적으로 주기적인 무결성 검증을 수행할 수 있다.

③ 무결성 검증 대상은 신청업체가 선택 가능하나, 검증 대상이 되는 실체의 비정상 상태(*오류, 정지 등*)로 인하여 제품의 보안 기능에 영향을 미치는 경우 해당 실체는 무결성 검증 대상으로 반드시 포함해야 한다.

④ 관리자가 무결성 검증을 수행하는 기능을 제공해야 한다.

⑤ 신청업체는 제품이 지원하는 무결성 검증 기능에 대한 상세한 설명자료(「보안 기능 구현명세서」)를 제출해야 한다.

⑥ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 시험원은 제품의 무결성 검증 대상 및 메커니즘을 조사해야 한다.

② 제품이 자동으로 무결성 검증을 수행하는 주기는 1일 이내의 값으로 고정 또는 설정 가능한지 확인해야 한다.

③ 해시값 비교 방법으로 무결성 점검 기능을 수행할 때 원본 해시값이 파일 시스템에 저장되는 형태일 경우, 원본 해시값이 보호되는지 확인해야 한다.

④ 시험원은 제품의 무결성 검증을 위한 데이터가 저장될 때 '4.2 저장 데이터 보호' 요구사항에 따라 저장되는지 확인해야 한다.

5.2.2

필수

제품은 운영체제 커널 또는 커널 레벨 모듈에 대한 무결성을 검증하는 기능을 제공해야 한다.

요구항목

① 해시값 비교 방법으로 무결성 검증시 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

5.2.3

필수

제품은 무결성 검증 내용 및 결과를 관리자가 확인하는 기능을 제공해야 한다.

요구항목

① 무결성 검증 내용 및 결과는 화면 출력, 감사기록을 통해 확인할 수 있어야 한다.

점검시 유의사항

① 무결성 검사 수행 주기가 매우 짧은 경우, 무결성 검사 성공에 대한 감사기록이 다수 발생할 수 있으므로 일정 시간 내에 발생한 무결성 검사 성공에 대해 감사기록을 1회 생성하고, 무결성 검사 성공 횟수를 감사기록에 추가, 생성이 가능하다.

5.2.4

필수

제품은 무결성 검증 실패인 경우 대응 기능을 수행해야 한다.

요구항목

① 제품은 자체에 구현된 대응기능을 수행하거나 관리자가 설정한 대응 기능을 수행해야 한다.

② 무결성 검증 결과에 대한 감사기록을 생성해야 한다.

③ 무결성 검증 결과 실패시 수행하는 대응 기능의 예로써 *프로그램 실행중단, 경고메시지 화면 출력 등*이 있다.

④ 관리자가 대응기능을 설정 할 수 있도록 보안관리 기능을 제공할 수 있다.

점검시 유의사항

① 제품이 △처음 실행시(또는 구동시) △관리자 수동 요청시 △주기적 실행시

무결성 검증이 실패한 경우를 모두 확인해야 한다.

② 대응기능에 대한 관리자 설정 기능이 없는 경우, 제품에 기본적으로 설정된 대응기능을 수행하면 요구사항을 만족한다고 판정한다.

③ 대응기능에 대한 관리자 설정기능이 있는 경우, '3.1 보안관리 기능' 요구사항에 따라 시험을 수행해야 한다.

6. 업데이트 보호

제품은 제품 설치 파일, 제품 운영에 필요한 파일 등 '업데이트 파일'을 설치 또는 적용하는 기능을 제공할 수 있다. 제품은 업데이트 파일을 설치하거나 적용하기 전에 업데이트 파일에 대한 유효성 검증 등을 수행해야 한다.

6.1 업데이트 지원

6.1.1

필수

제품은 업데이트 파일을 설치하거나 적용하기 전에 제품 업데이트 파일의 유효성을 검증해야 한다.

요구항목

① 제품은 업데이트 시, 유효성 검증에 성공한 업데이트 파일만 설치하거나 적용해야 한다.

② 업데이트 파일의 유효성 검증시 무결성 검증이 필수이며 *전자서명 검증, 공개된 해시값 검증 등*을 이용하여 구현해야 한다.

③ 전자서명 검증시 인증서 유효성 검증을 수행해야 한다.

④ 암호 알고리즘 및 암호키 안전성은 '9. 암호 지원' 요구사항을 만족해야 한다.

⑤ 업데이트 파일 유효성 검증결과(성공 · 실패)는 감사기록에 기록되어야 한다.

점검시 유의사항

① 업데이트 파일의 유효성 검증은 *전자서명 검증, 공개된 해시값 검증 등*을 통해

확인할 수 있다.

② 업데이트 설치 · 수행을 인가된 관리자로 제한하는지 확인해야 한다.

③ 유효성 확인이 없는 자동 업데이트 기능은 허용되지 않는다.

6.1.2

필수

제품은 '제품의 유일한 식별 정보'를 사용자가 확인하는 기능을 제공해야 한다.

요구항목

① 제품 식별 정보는 유일해야 하고 인터페이스를 통해 사용자가 확인할 수 있고 수정 · 변경할 수 없어야 하며 다음 사항이 포함되어야 한다.

– 제품 명칭, 제품 버전, 제품 릴리즈 또는 빌드 번호, 펌웨어의 해시 값

② 제품이 물리적으로 분리된 다수의 구성요소를 포함하는 경우 각 구성요소의 식별 정보는 유일해야 하고 사용자가 확인할 수 있어야할 뿐 아니라 수정 · 변경할 수 없어야 하며 다음 사항이 포함되어야 한다.

– 구성요소를 포함하는 제품 명칭 및 버전, 구성요소 명칭, 구성요소 버전, 구성요소 릴리즈 또는 빌드 번호.

③ 제품 · 구성요소의 패치 및 기능개선 여부를 확인할 수 있는 버전 관리 체계를 적용해야 한다.

(*패치 및 기능개선시 사안별로 Major 버전, Minor 버전, 릴리즈 번호 · 빌드 번호를 변경하는 체계를 마련하여 제품 · 구성요소 변경 사유를 버전 정보로 추적*)

④ 제품 식별 정보 외에 펌웨어의 유일한 식별 정보 및 해시 값을 제품 인터페이스를 통해 사용자가 확인할 수 있어야 한다.

6.1.3

필수

제품은 업데이트 설치 실패시 자동으로 기존 버전을 유지하는 기능을 제공해야 한다.

요구항목

① 업데이트 설치 결과 및 실패 사유에 대한 감사기록을 생성해야 한다.

② 제품에서 지원하지 않을 경우, 관리자에 의한 수동 복구를 지원해야 한다.

③ 개발업체는 관리자에 의한 수동 복구 절차를 제출물에 상세히 기술해야 한다.

점검시 유의사항

① 업데이트 설치 수행을 인가된 관리자로 제한하는지 확인해야 한다.

② 제품에서 지원하지 않는 경우, 제출물에 수동 복구 절차가 명시되어 있는지 확인해야 한다.

③ 수동 복구 방법으로 설정 초기화도 허용된다.

7. 세션 관리

제품은 사용자가 오랫동안 사용하지 않을 경우 세션을 잠그거나 종료시켜야 한다. 또한, 제품은 동시 접속 세션의 제한기능을 제공해야 한다.

7.1 세션 잠금 · 종료 기능

7.1.1

필수

제품은 관리자 세션 연결 이후 일정시간 동안 사용하지 않을 경우, 세션을 잠그거나 종료하는 기능을 제공해야 한다.

요구항목

① 사용되는 시간정보는 서버 시간을 기준으로 적용해야 한다.

② 일정시간은 세션 잠금 또는 종료행위를 촉발시키는 연결 이후, 누적 시간량을 의미한다.

- 일정시간은 관리자가 10분 이하의 값 중에서 고정하거나 인증 실패 횟수에 비례하여 설정할 수 있다.

③ 잠겨진 세션은 잠금시간이 경과한 후, 관리자에 의하거나 각 세션별 사용자 인증 기능을 통해서 해제되어야 한다.

④ 세션 잠금이나 종료 기능 동작시 감사기록을 생성해야 한다.

⑤ 제품에 포함되는 모든 관리접속에 적용해야 한다.

참고 사항

① 영상 모니터링 기능에 대해서는 적용하지 않을 수 있다.

점검시 유의사항

① 제품이 지원하는 모든 관리 접속(*SSH, HTTPS 등*)에 대해 확인해야 한다.

② 세션의 잠금 해제는 관리자 인증 또는 사용자 인증을 통해서 가능한지 확인해야 한다.

③ 영상 모니터링 기능에서 일정시간이 경과하고 다른 관리 기능으로 전환을 시도할 때 사용자 인증이 요구되는지 확인해야 한다.

7.2 동시접속 세션 제한

7.2.1

필수

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

요구항목

① 사용자 로그인 이후 다른 단말기에서 동일 계정으로 로그인을 수행하는 경우 신규 접속을 차단하거나 이전 접속의 종료를 요구한다.

② 동일 권한으로 중복 로그인을 허용하지 않아야 한다.

③ 중복 접속 차단시 감사기록을 생성해야 한다.

참고 사항

① 영상 모니터링 · PTZ 등 카메라 제어 목적으로 접속하는 관리자 계정 및 권한에

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.

점검시 유의사항

① 사용자 계정 동일 PC 또는 다른 PC에서 동시 접속시 차단 여부를 확인해야한다.

② 제품이 지원하는 모든 관리 접속(*SSH, HTTPS 등*)에 대해 확인해야 한다.

8. 감사기록

제품은 보안기능 및 관리자의 보안활동과 관련된 사항을 감지, 기록하고 분석하여 대응을 지원해야 한다. 또한 감사기록의 삭제 · 저장 실패 등 무력화에 대응하는 기능을 제공하는지 확인해야 한다.

8.1 감사기록 생성

8.1.1

필수

제품은 주요 감사사건에 대해 감사기록을 생성해야 한다.

요구항목

① 반드시 감사기록을 생성해야 하는 감사사건은 아래 〈표 3〉과 같다.

② 기능 제공시 감사기록을 생성해야 하는 감사사건은 아래 〈표 4〉와 같다.

〈 표 3. 필수 기록되어야 할 주요 감사사건〉

소분류	보안관리	추가적인 감사정보
식별 및 인증	사용자의 로그인, 로그아웃	
	사용자 등록, 변경, 삭제	
	사용자 인증 시도의 한계치 도달시 대응행동	
	패스워드에 대한 모든 변경	

소분류	보안관리	추가적인 감사정보
보안관리	〈표 2〉의 보안관리 기능의 수행과 보안속성 값의 모든 변경, 삭제 ※ 다만, 보안관리 기능중 '감사기록 조회' 및 '제품 버전정보 조회' 기능은 제외	변경된 보안속성 데이터
	기본 계정(ID) · 패스워드 변경	
	관리용 단말 접속 IP 차단	
세션 관리	사용자의 세션 잠금 또는 세션 종료	
	동일 계정의 중복 로그인 시도 탐지시 대응행동	
	동일세션 수 제한에 기반한 새로운 세션 거부	
암호키 생성	암호 키 생성 실패	
암호 사용	암호 연산 실패(암호 연산 유형 포함)	
감사기록	하드웨어 일체형 제품의 감사기능 시작과 종료	
	제품의 시간 설정 변경	

〈 표 4. 기능 제공시 기록할 수 있는 주요 감사사건〉

소분류	보안관리	추가적인 감사정보
영상 보안	영상 외부 저장 기능 수행	해시 값
	녹화 설정 및 변경	
보안 관리	카메라 제어(PTZ 등) 설정 및 동작	
자체보호	자체 시험 수행	실패한 보안기능
	제품 자체의 무결성 검사 수행	무결성 검사가 실패한 구성요소
업데이트 보호	관리자에 의한 업데이트 파일 유효성 검증	
	업데이트 파일의 유효성 검증 수행	
감사기록	감사기록 저장 실패시 대응행동	

점검시 유의사항

① 시험원은 제품의 모든 감사기록 행위를 조사해야 한다.

② 제품 시작시 감사기록이 생성되는 경우(*자체시험 결과, 무결성 검사 등*)에는 '감사기능 시작'을 명시하지 않아도 요구사항을 만족한다고 판정한다.

③ 취약성 시험 등에 의한 제품 강제 종료시 '감사기능 종료'를 기록하지 않아도 요구사항을 만족한다고 판정한다.

8.1.2

필수

감사기록은 필요 이상의 정보가 포함되지 않아야 한다.

요구항목

① 감사기록에 최소한 포함되어야 하는 항목은 다음과 같다.

- 사건 발생일시, 사건 유형, 사건을 발생시킨 주체의 신원(*계정, 프로세스, IP 등*), 사건의 결과(성공 · 실패)

② 인증 정보(*패스워드 등*), 암호키 등의 정보는 감사기록 내에 저장하지 않아야 한다.

8.1.3

필수

제품의 각 구성요소들은 신뢰된 시간 정보를 이용해서 감사 기록을 생성해야 한다.

요구항목

① 신뢰된 시간 정보는 NTP 서버나 운영체제에서 제공하는 시간 정보를 이용해야 한다.

점검시 유의사항

① 시험원은 제품에서 사용하는 시간정보, 동기화 설정 방법 등을 조사해야 한다.

- 제품 구성요소간 시간 동기화의 필수 구현을 요구하지는 않는다.

8.2 감사기록 조회

8.2.1

필수

제품은 인가된 관리자가 감사기록을 조회할 수 있는 기능을 제공해야 한다.

요구항목

① 제품에서 제공하는 보안기능을 통해서만 감사기록을 조회할 수 있어야 한다.

② 제품은 인가된 관리자가 정보를 해석하기에 적합하도록 감사기록을 제공해야 한다.

③ 감사기록에 민감한 데이터(*패스워드, 주민등록번호 등*)는 기록되지 않아야 하지만 기록이 불가피할 경우, 마스킹으로 처리하여 생성해야 한다.

점검시 유의사항

① 제품에서 제공하는 보안기능을 우회하여 외부에서 감사기록을 직접 조회하는 행위를 차단하는지 확인해야 한다.

- 제품 내부 DB에 감사기록을 저장하는 경우, 제품에서 DB에 대한 접근권한을 통제할 수 있어야 한다.

8.2.2

필수

제품은 감사기록 조회시 관리자가 논리 조건을 선택할 수 있고, 여러 조건에 따라 검색 또는 정렬하는 기능을 제공해야 한다.

점검시 유의사항

① 시험원은 제품이 제공하는 감사기록 조회시 설정가능한 논리 조건을 조사하고, 가능한 경우의 수를 모두 고려하여 조건에 따른 검색 및 정렬 기능을 확인해야 한다.

8.2.3

조건부 필수

제품은 WAS의 로그에 중요 정보가 포함되지 않도록 구현해야 한다.

조 건	WAS(*Tomcat, JEUS 등*)가 제품 패키지에 포함되는 경우

요구항목

① 제품 내 WAS(*Tomcat, JEUS 등*)가 함께 운용되는 경우 자체 로그를 남기지 않고 제품의 감사기록 저장소에만 로그를 남기도록 개발해야 한다.

② WAS 로그에 패스워드, 암호키 등 중요 정보가 평문으로 남지 않아야 한다.

8.3 감사기록 보호

8.3.1

필수

제품은 감사기록을 삭제 또는 변경할 수 없도록 보호해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT실체에 전송하여 저장하는 기능을 구현해야 한다.

② 인가된 관리자라도 감사기록을 삭제 및 변경할 수 없도록 관련 유저인터페이스(UI) 및 CLI 명령어가 제공되지 않아야 한다.

③ 저장된 감사기록을 보호하기 위해 비인가자의 접근을 통제할 수 있어야 한다.

④ 제품 보안기능으로 완전히 구현 할 수 없는 경우, 제품 운영환경에서 감사증적 저장소를 보호 할 수 있도록 지원할 수 있다.

- 제품과 동일한 운영체제상에 설치된 DBMS에 감사기록이 저장되는 경우 DBMS의 식별 및 인증 기능을 이용, 비인가 사용자의 삭제 또는 변경을 보호할 수 있다.

⑤ 감사기록이 제품 외부의 로그서버에 저장되는 경우 암호통신을 수행해야 한다.

- syslog를 지원하면 *syslog over TLS (RFC 5424), syslog over DTLS (RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.

참고 사항

① 감사기록을 실시간으로 외부 IT실체에 전송하여 저장하는 경우 감사기록 원본은 외부 실체에 저장된다고 본다.

점검시 유의사항

① 감사기록이 제품 외부의 로그서버에 저장되는 경우 암호통신 수행을 확인해야 한다.

② 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 감사기록을 실시간으로 외부 실체에 전송하여 저장하는 경우 만족한다고 판정한다.

8.3.2

선택

제품은 감사기록을 제품 내부에 저장할 경우 암호화하여 저장해야 한다.

요구항목

① 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

8.4 감사기록 손실 예측시 대응 행동

8.4.1

필수

제품은 감사기록의 크기가 미리 정의된 용량에 도달하는 경우 대응행동을 수행해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT 실체에 전송하여 저장하는 기능을 구현해야 한다.

② 관리자에게 통보하는 기능을 필수적으로 제공해야 하며, 기능의 예로써 *화면 알람, 관리자 이메일 발송 등*이 있다.

③ 감사기록 손실 대응관련 관리자에게 통보하는 조건의 예로써 *설정된 디스크 용량 90% 이상, 100MB 이상 등*이 있다.

④ 부가적으로, 관리자가 감사기록을 외부 로그서버로 전송하는 기능을 제공할 수 있다.

- syslog를 지원하면 *syslog over TLS (RFC 5424), syslog over DTLS (RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.
- 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 관리자에게 통보하기 위한 조건의 고정값 지원도 가능하다.

② 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 실시간으로 외부 IT 실체에 전송하여 저장하는 경우 '만족'으로 판정한다.

8.5 감사기록 손실 방지

8.5.1

필수

제품은 감사기록 저장 용량 포화시 적절한 방법으로 저장 실패에 대응해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT실체에 전송하여 저장하는 기능을 구현해야 한다.

② 저장 실패 대응 기능의 예로써 *가장 오래된 감사기록 덮어쓰기, 감사기록 압축 저장 등*이 있다.

점검시 유의사항

① 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 실시간으로 외부 IT 실체에 전송 · 저장시 '만족'으로 판정한다.

9. 암호 지원

제품의 데이터 저장 · 전송시 보호를 위해 사용되는 암호화 및 해시 알고리즘은 국가 · 공공기관이 요구하는 보안강도를 만족해야 한다. 또한 암호화를 사용하는 모든 보안기능은 '9. 암호지원'의 요구사항을 만족하도록 구현해야 한다.

9.1 암호사용

9.1.1

필수

중요 정보 전송 및 저장시 권고 암호 알고리즘을 사용해야 한다.

요구항목

① 권고 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘으로 [별표 1]을 참고한다. 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-223, P-224, P-256).*

② 다만, TDES(2 key, 3 key 포함) 사용은 허용하지 않는다.

③ 블록 암호 사용시 평문의 크기가 암호화 블록 크기보다 큰 경우 ECB 모드는 사용하지 않아야한다.

④ 블록 암호 사용시 CFB 또는 OFB 모드에서는 고정된 Ⅳ를 사용하지 않아야 한다.

⑤ 국내 · 외 표준 암호 알고리즘을 사용해야 하며, 국가용 암호알고리즘 사용을 권고한다.

⑥ 보안강도 112 bit 급 이상 암호 알고리즘의 세부 사항은 「암호 알고리즘 및 키 길이 이용 안내서」(과학기술정보통신부, 2018), 「소프트웨어 암호모듈 검증 기준」, 「NIST SP800-131 Ar2」를 참고한다.

점검시 유의사항

① 제출문서(「보안기능 구현명세서」 또는 「보안기능 운용설명서」)를 통해 제품이 보안기능에 적용한 암호화 방식을 확인해야 한다.

② 패스워드는 일방향 해시 알고리즘 또는 양방향 암호 알고리즘을 사용하여 암호화해야 하며, 동일한 평문 입력을 반복하여도 매번 다른 값이 출력되어야 한다.

③ 시험원은 요구사항에 따른 정확한 구현을 시험하기 위해 필요시 개발자를 직접 대면하여 구현내용에 대한 설명을 요청할 수 있다.

9.2 암호키 생성

9.2.1

필수

제품은 암호키를 아래 요구항목을 준수하여 생성해야 한다.

요구항목

① 암호키 생성 방식의 예로써 *패스워드 기반 키 유도(PKCS#5 v2.1(RFC 8018), NIST SP 800-132 등), 사전공유된 키로 키 유도(TTAK.KO-2.0272), 난수발생기 이용 키 생성(CTR_DRBG, HASH_DRBG, HMAC_DRBG 등)이 있다.*

② 난수발생기는 국내 · 외 표준을 준수하여 구현되어야 한다.

③ 난수발생기로 생성한 난수를 이용하여 비대칭키쌍(공개키 · 비공개키)이나 대칭키 생성이 가능하다.

④ 패스워드 기반 키 유도 기능은 키 암호화 키(KEK : Key Encryption Key) 생성에만 사용해야 한다.

- 최초의 키 암호화 키(KEK)는 제품마다 다르게 생성되어야 한다.
- 키 암호화 키(KEK)는 생성에 필요한 초기 데이터(*패스워드 등*)는 직접 입력받거나 스마트카드, 보안USB, 보안토큰(HSM : Hardware Security Module) 등 저장 매체에 저장된 값을 주입하여 사용할 수 있다.
- 저장매체는 보안기능 확인서 또는 국내 · 외 CC인증서를 획득한 제품의 사용을 권고한다.
- 세부 사항은 「암호 키 관리 안내서」(과학기술정보통신부, 2018) 암호키 생성 부분을 참고한다.
- 키 암호화 키(KEK) 생성을 위한 초기 데이터로 패스워드를 사용하는 경우, 제품 최초 설치시 입력된 값을 저장하여 사용할 수 있으며 저장된 데이터는 인가되지 않는 노출시도로부터 보호되어야 한다.

⑤ salt 값은 비밀일 필요는 없으며, 난수발생기를 이용하여 생성하고 크기는 최소 128bit 이상이어야 한다.

⑥ iteration count 는 가능한 큰 값을 적용해야 한다. (최소 1000회 이상)

점검시 유의사항

① 패스워드는 4자리 이상인지 확인한다.

② 시험원은 제품이 제공하는 암호키 생성 방식(*표준, 난수발생기 등*)을 조사해야 한다.

③ 제품에서 외부의 3rd Party Library나 오픈소스를 사용한 경우 사용 소프트웨어 이름, 버전 정보를 확인해야 한다.

④ 제품이 패스워드 기반 키 유도 기능을 구현한 경우, 사용자 인터페이스 확인, 디버깅 시험 등을 통해 확인해야 한다.

9.3 암호키 저장

9.3.1

필수

제품은 암호키를 아래 요구항목을 준수하여 저장해야 한다.

요구항목

① 데이터 암호화 키(DEK)는 암호화 키(KEK : Key Encryption Key)를 사용, 암호화하여 저장 할 수 있다.

② 키 암호화 키(KEK)는 여러 단계의 키 체인을 통해 생성할 수 있으며, 이 중 최종 키 암호화 키(KEK)는 이전 단계의 키 암호화 키(KEK)를 사용, 암호화하여 저장할 수 있다.

③ 키 체인에서 최종 키 암호화 키(KEK)를 제외한 키 암호화 키(KEK)는 저장할 수 없다.

④ 암호키를 제품 외부에 저장할 경우 스마트카드, 보안USB, 보안토큰(HSM) 등 안전성이 확인된 저장 매체의 이용을 권고한다.

- 저장 매체는 보안기능 확인서 또는 국내 · 외 CC인증서를 획득한 제품의 사용을 권고한다.

⑤ 암호키를 제품에 하드코딩하여 저장하는 방식은 허용되지 않는다.

⑥ 신청업체는 아래 〈표 6〉과 같이 제품에서 저장 및 전송시 사용하는 모든 암호키를 식별하여 키 저장 및 파기 방법에 대한 목록과 설명자료를 제출하여 안전성을 입증해야 한다.

⑦ 제품 관리를 위한 로컬 · 관리접속 및 별도 장비와 연동설정에 사용되는 암호키(*사전공유키, 대칭키, 개인키 등*)를 제품이 저장하는 경우 *암호화, 접근통제 등*의 방식으로 보호하여 저장해야 한다.

〈 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

참고 사항

① 암호키란 제품 관리를 위한 로컬접속 · 관리접속 및 별도 장비와 연동설정에 사용되는 사전공유키, 대칭키, 개인키 등의 키들을 모두 의미한다.

점검시 유의사항

① 시험원은 위 표와 같이 제품에서 사용되는 모든 암호키를 조사하고, 키 저장 및 파기 방법을 확인해야 한다.

② 제품의 데이터 암호화 키는 모두 암호화하여 내부에 저장하는지 확인해야 한다.

③ 제품 내부의 암호키 저장 영역에 비인가자의 접근을 차단하는지 확인해야 한다.

9.4 암호키 파기

9.4.1

필수

제품은 제품에서 생성하거나 사용한 암호키를 파기해야 한다.

요구항목

① △제품 실행 종료시 △암호키 삭제 함수 호출시 △암호통신 종료시 등의 경우

사용기간이 만료된 암호키 및 암호키 관련 정보를 모두 파기해야 한다.

② 암호키 파기시 0 또는 1의 값으로 3회 이상 덮어쓰기하는 방식을 이용할 수 있다.

③ 세부 사항은 「암호 키 관리 안내서」(과학기술정보통신부, 2018) 암호키 파기 방법을 참고한다.

점검시 유의사항

① 시험원은 암호키 및 암호키 관련 정보가 삭제되는 시기와 암호키를 파기하는 메커니즘을 조사해야 한다.

② 암호키 파기시 메모리에 적재(Load)된 암호키를 삭제하는지 확인해야 한다.

10. 취약성 대응

제품은 존재하는 알려진 취약점들을 제거해야 한다.

10.1 소스코드 보안약점 제거

10.1.1

선택

제품 개발시 소스코드에 보안약점이 존재하지 않도록 시큐어 코딩 규칙을 적용해야 한다.

요구항목

① 소프트웨어 개발 단계에서 보안약점을 최소화하여 구현해야 한다.

② 다음의 표준 · 가이드를 준수할 수 있다.

- 「ISO/IEC TS 17961:2013」, 「JAVA 시큐어코딩 가이드」 (KISA)

③ 신청업체는 자체 수행한 제품 보안약점 제거 결과를 제출, 안전성을 입증해야 한다.

④ 세부 사항은 「소프트웨어 개발보안 가이드」 (행정안전부, 2021.11)를 참고한다.

점검시 유의사항

① 시험원은 신청업체에서 제공한 시큐어코딩 점검 · 보완 결과의 적절성을 확인해야 한다.

② 검증필 제품목록에 등재된 소스코드 보안약점 진단도구를 이용, 제품에 대해 독립적인 보안약점 점검을 수행해야 한다.

③ 시험기관이 신청업체로부터 받은 '취약점 개선 보증 서약서' 및 '취약점 개선 내역서'를 제출 받아 검토한 후, 취약성 시험을 생략할 수 있다.

10.2 알려진 취약점 제거

10.2.1

필수

제품 내부에 알려진 보안취약점을 확인하고 제거해야 한다.

요구항목

① 공개영역을 통해 알려진 보안취약점(*CVE, NVD 논문 등*)에 대해 제품에서 사용중인 프로토콜, 라이브러리, 오픈소스 등(*OpenSSL, OpenSSH*)에 해당하는 보안취약점이 존재하는지 확인하고 제거해야 한다.

- 제품에 포함되는 커스터마이즈 운영체제에 낮은 버전의 커널(*Linux® 2.x*)은 사용하지 않도록 권고한다.

점검시 유의사항

① 시험원은 제품에서 사용중인 프로토콜, 라이브러리, 오픈소스 등에 대한 이름 및 버전 등을 조사해야 한다.

② 시험원은 조사한 3rd Party 제품(*Boot Loader, Busybox, OpenSSL, OpenSSH, Kernel 등*)에 대한 취약성 존재 및 최신 패치 적용 유무를 확인하여 패치되지 않을 경우 '불만족'으로 판정한다.

③ 시험원은 조사한 보안취약점 목록을 토대로 침투시험을 실시하여 악용 가능한

취약점이 확인되면 ‘불만족’으로 판정한다.

④ 시험기관은 취약점 점검 도구 사용의 적절성을 확인하고 시험에 사용해야 한다.

10.3 불필요한 서비스 제거

10.3.1

필수

제품 내부에 불필요한 서비스가 실행중이면 이를 확인하고 제거해야 한다.

요구항목

① 신청업체는 제품이 제공하는 서비스를 식별하여 필요성을 입증해야 한다.

② 제품에서 보안기능 구동에 필요한 필수 서비스와 불필요 서비스를 식별하여 불필요 서비스는 제거하거나 비활성화해야 한다.

점검시 유의사항

① 시험기관이 신청업체로부터 「보안기능 구현명세서」 또는 「보안기능 운용명세서」를 제출받아 필요 · 불필요 서비스의 식별 및 불필요 서비스 제거를 확인한 후 ‘만족’으로 판정할 수 있다.

끝.

〈 별 표 1 〉

영상 전송 관련 표준 프로토콜 목록(예시)

프로토콜	동작 형태	비고
ONVIF	HTTPS/TCP HTTP/TCP	- www.onvif.org - IEC 60839-11-31:2016, IEC 62676-2-31:2019 - SOAP 기반의 HTTP/XML 메시지 프로토콜 (IP카메라의 영상 관련 정보 Read/Write) - 영상 전송에 대해 RTP/RTSP 등의 표준 차용
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 7826 - 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

〈 별 표 2 〉

제 · 개정 이력

일 자	주요 변경 내용	문서 버전
2024. 4. 3.	o IP카메라 보안요구사항 제정	V3.0
2025. 11. 28.	o ‘신원정보기반 생체인식제품 보안요구사항’(제21장) 제정에 따른 번호 변경(제33장 → 제34장)	V3.0

공공 · 국방분야 공통

35장
영상정보 관리 · 저장제품 보안요구사항

1절 일반사항

1. 운용 환경 정의

■ 가정사항

○ 제품의 인가된 관리자는 장비의 펌웨어 및 장비 내에서 사용되는 소프트웨어에 대한 최신 패치를 정기적으로 수행한다.

○ 제품의 인가된 관리자는 관리프로그램, 웹브라우저 등을 통해 제품에 접속할 수 있으며, 이 때 HTTPS, TLS, SSH 등의 암호통신 프로토콜을 이용하여 보안관리를 수행한다.

○ 제품은 원격제어(RDP 등) 연결이 불가능해야 한다.

■ 제품 개요

영상정보 관리 · 저장제품은 TCP/IP 네트워크를 통해 IP카메라로부터 영상을 전송받아 실시간 모니터링, 저장(녹화), 검색(재생) 등 영상정보를 처리하는 목적으로 사용된다. 제품은 여러 채널의 IP카메라에서 영상 전송 관련 표준 프로토콜(*RTP/RTSP 등*)로 받은 영상정보를 통합하여 관리할 수 있으며, 기기 간 연동 프로토콜(*ONVIF 등*)로 IP카메라의 설정 관리, 카메라 제어(*PTZ 등*) 기능을 제공할 수 있다.

제품은 하드웨어 일체형 또는 소프트웨어 등 다양한 형태로 구현될 수 있으며

NVR, VMS, IP 네트워크 통신이 가능한 Hybrid-DVR 등을 포함한다.

제품의 구성요소로 관리프로그램이 있을 수 있으며, 관리프로그램은 기능 범위에 따라 원격 영상 모니터링, 보안기능 관리, 카메라 제어 등이 가능하다. 제품과 관리프로그램은 TCP/IP 네트워크를 통해 연결되며, 제품에 따라 관리프로그램 없이 단독으로 운용되는 형태도 있을 수 있다.

■ 운용 환경

영상정보처리기기가 운용되는 네트워크는 인터넷 및 업무 · 행정망과 분리된 별도 단독망 구성이 원칙이며, 원격지 등에 설치하여 단독망 구성이 불가할 경우에는 VPN 등으로 암호화된 통신 구간에서 운용되어야 한다. 제품에 대한 관리 단말(PC)이 별도로 운용될 수 있으며 관리 단말에서는 관리프로그램에 의해 영상감시 및 원격관리 활동이 이뤄질 수 있다. 이외에도, 제품에 따라 기능 활용을 위해 필요한 외부 실체가 있는 경우 운용 환경에 추가적으로 제시될 수 있다.

관리프로그램의 설치환경은 Windows® 또는 Linux® 운영체제가 설치된 PC이며, 영상정보처리기기 단독망 내의 관리 단말에서 운용된다.

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.

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

■ 운용환경 요구사항

○ 제품은 인가된 관리자만이 접근 가능한 환경에 설치 및 운용된다.

○ 제품의 인가된 관리자는 다음의 지침 및 가이드에서 부여한 의무를 정확하게 수행해야 한다.

분야	명칭	주관기관
공공	국가정보보안기본지침	국가정보원
	국가 · 공공기관 영상정보처리기기 도입 · 운영 가이드	
	공공기관 고정형 영상정보처리기기 설치 · 운영 가이드	개인정보보호위원회

분야	명칭	주관기관
국방	국방보안업무훈령	국방부
	국방정보보안시스템 업무훈령	

○ 제품의 인가된 사용자는 악의없이 도입한 목적에 맞게 제품을 운용해야 한다.

○ 제품의 인가된 관리자는 감사기록 유실에 대비하여 감사 데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그 서버, 별도 저장장치 등) 등을 수행한다.

○ 제품의 인가된 관리자는 제품 동작에 불필요한 운영체제상의 서비스나 수단 등을 제거하고 취약점에 대한 개선 작업을 통해 운영체제의 신뢰성과 안전성을 보장한다.

○ 제품의 인가된 관리자는 네트워크 구성, 변경, 카메라 채널의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 제품 운용정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.

○ 제품의 구성요소에 관리프로그램이 포함될 경우, 해당 관리프로그램에 의해서만 원격관리가 가능해야 하며 운용은 인가된 관리자만 가능해야 한다.

■ 공통보안요구사항의 적용

공통보안요구사항을 적용하지 않는다.

2절 보안요구사항

1. 영상 보안

제품은 영상정보의 저장, 전송, 백업 등에 대한 보안기능을 제공해야 한다.

1.1 영상 프로토콜 인증

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 1암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘을 사용해야 한다.

1.2 영상 전송 보안

1.2.1

필수

기기 간 연동 및 영상 전송 관련 표준 프로토콜(*ONVIF, RTSP 등*) 통신시 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.

③ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

④ HTTPS Tunneling(RTP/RTSP/HTTPS/TCP) 전송 방식을 사용할 수 있다.

점검시 유의사항

① 패킷 모니터링 도구를 활용하여 전송 데이터에 대한 기밀성, 무결성을 제공하는지 확인해야 한다.

1.3 영상 저장 보안

1.3.1

필수

영상 저장시 암호화 저장 기능을 제공해야 한다.

요구항목

① 제품 내 · 외부에 비디오, 이미지 등 영상을 암호화하여 저장해야 한다.

② 저장하는 영상 스트림 중 모든 I-프레임은 암호화해야하며 다른 데이터는 개발업체의 선택에 따라 암호화될 수 있다.

③ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

④ 제품 내부 저장소에 저장된 영상의 일부를 제품 외부에 파일형태로 백업하는 기능을 제공할 경우, 암호화 및 무결성 검증 기능을 제공해야 한다.

참고 사항

① 개발업체는 암호화 저장 기능을 위해 검증필 암호모듈(KCMVP)을 탑재할 수 있다.

점검시 유의사항

① 휘발성 메모리에 저장하는 경우는 영상 저장 기능으로 간주하지 않는다.

1.4 오디오 저장 보안

1.4.1

조건부 필수

오디오 저장을 on · off 할 수 있는 기능을 제공해야 한다.

조 건	오디오 저장 기능 지원시

요구항목

① 기본(default) 상태에서 오디오 저장 기능은 ‘on’과 ‘off’가 모두 선택 가능해야 하며 초기값은 ‘off’로 설정되어야 한다.

점검시 유의사항

① 오디오 저장 기능은 ‘on’과 ‘off’가 모두 선택 가능한지 확인한다.

② ‘on’과 ‘off’를 각각 선택하여 오디오 저장기능의 활성화 · 비활성화가 정상 작동하는지 확인한다.

③ 초기값이 ‘off’로 설정되어있는지 확인한다.

④ 제품이 오디오 녹음 기능을 지원하지 않는 경우 ‘해당사항 없음’으로 판정한다.

2. 식별 및 인증

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

2.1 사용자 등 식별 및 인증

2.1.1

필수

제품은 사용자의 신원을 검증하기 위해 사용자 계정 · 패스워드 기반 식별 및 인증 기능을 제공해야 한다.

요구항목

① 사용자가 제품의 정당한 사용자임을 확인하기 위해 반드시 식별 및 인증을 수행해야 한다.

② 관리자는 각 사용자 또는 그룹별로 권한을 부여할 수 있어야 한다.

③ 사용자 계정(ID)은 각각 고유한 값으로 등록되어 중복되지 않아야 한다.

점검시 유의사항

① 제품이 제공하는 전체 사용자 역할을 확인해야 한다.

- 관리자의 경우 관리접속 및 로컬운용 등 접속 경로별로 식별 및 인증을 요구하는지 확인해야 한다.
- 일반사용자가 존재하는 경우, 제품에 접근시 식별 및 인증을 요구하는지 확인해야 한다.

② 관리서비스 접근시 식별 및 인증을 요구하는지 확인해야 한다.

③ 영상 관련 기능(*실시간 영상 모니터링, 재생(검색), 제품 외부에 영상 저장 등*) 접근시 식별 및 인증을 요구하는지 확인해야 한다.

④ 관리자가 각 사용자 또는 그룹별로 권한을 설정할 수 있는지 확인해야 한다.

⑤ 알려진 취약점이 존재하는지 확인해야 한다.

- 계정 및 패스워드 입력필드에 입력 가능한 문자열을 제한하는지 확인이 필요하다.
- 시험기관이 '취약점 개선 내역서'를 제출받아 검토한 후 취약성 시험을 생략할 수 있다.

⑥ 시험기관은 취약점 점검 도구 사용의 적절성을 확인하고 시험에 사용해야 한다.

⑦ 사용자 인증을 우회하여 관리화면으로 접근할 수 있는지 확인해야 한다.

2.1.2

조건부 필수

제품은 사용자 식별 및 인증을 위해 2.1.1과 병행하여 추가적인 식별 및 인증 기능을 자체 또는 외부 IT실체와 연동하여 제공해야 한다.

조 건	추가적인 식별 및 인증 방식 지원시

요구항목

① 추가적인 식별 및 인증 기능 제공을 위해 △FIDO 표준을 준수한 2FA 지원 기기 △인증서 △일회용 비밀번호 생성기(OTP) 등을 활용할 수 있다.

- 제품 · 운용환경에서 지원할 경우 'FIDO 표준을 준수한 2FA 지원 기기'를 권고한다.

② 추가적인 식별 및 인증 기능이 제품에서 제공되는 경우 제품 내부로부터 인증 결과를 전달받거나, 연동하는 외부 IT실체의 인증 결과를 전달받아서 기능을 제공할 수 있다.

- 제품에서 인증서 활용 방식을 제공하는 경우 인증서 유효성 검증을 수행해야 한다.
- 외부 IT실체가 추가적인 식별 및 인증 방식을 수행하기 위해 사용하는 인증정보는 외부 IT실체에 의해 관리되어야 한다. 추가적인 식별 및 인증 방식을 수행하기 위해 사용하는 인증정보를 제품이 저장하는 경우 '4.2 저장 데이터 보호'를 적용해야 한다.

참고 사항

① 'FIDO 표준을 준수한 2FA 지원 기기'는 'FIDO Alliance' 홈페이지에 등재된 인증제품 목록에서 확인할 수 있다.

점검시 유의사항

① 시험원은 제품이 지원하는 추가적인 식별 및 인증 기능을 모두 조사하고 제품에 포함되는지 확인해야 한다.

- 시험원은 제품에 포함되는 기능의 정상동작을 확인해야 한다.
- 추가적인 식별 및 인증 기능의 인증 결과가 패스워드 기반 식별 및 인증 기능 수행시 추가적인 사용자 속성으로 사용되어 인증 실패 또는 인증 성공됨을 확인해야 한다.

② 제품에서 인증서를 활용한 방식을 제공하는 경우 제품은 인증서 유효성 검증을 수행해야 한다.

③ 추가적인 식별 및 인증 기능이 패스워드 기반 식별 및 인증 기능과 함께 동작하는지에 대해 확인해야 한다.

④ 생체인증 정보를 제품 내부에 저장하는 경우 '4.2 저장 데이터 보호' 요구사항에 따라 저장되는지 확인해야 한다.

⑤ 제품이 추가적인 식별 및 인증 방식을 지원하지 않는 경우 '해당사항 없음'으로 판정한다.

2.1.3

조건부 필수

제품은 연동하는 외부 IT실체를 인증해야 한다.

조 건	제품에서 외부 IT실체를 인증하는 경우

참고 사항

① *관리프로그램 연동을 위한 패스워드, SNMP 인증 패스워드, SNMP 암호화 패스워드 등*이 적용대상이 될 수 있다.

점검시 유의사항

① 시험원은 제품과 외부 IT실체가 연동하기 위해 제품이 인증해야 하는 외부 IT실체를 모두 조사해야 한다.

② 제품이 인증하는 외부 IT실체가 없을 경우 '해당사항 없음'으로 판정한다.

여 백

2.2 인증실패 대응

2.2.1

필수

제품에서 사용자 인증이 설정된 횟수만큼 연속적으로 실패하면, 식별 및 인증 기능이 비활성화 되어야 한다.

요구항목

① 식별 및 인증 기능을 비활성화한 후 활성화 하는 방법의 예로써 *계정잠금 후 지정된 시간이 지난 이후 활성화, 계정잠금 후 활성화를 위한 다른 식별 및 인증 수단 제공 등*이 있다.

② 2.1.2에서 규정한 추가적인 식별 및 인증 수단을 제공할 수 있으며, 추가적인 식별 및 인증 수단의 인증실패시 사용자 인증실패 횟수에 포함해야 한다.

③ 식별 및 인증이 비활성화되는 연속적인 인증 실패 횟수는 5회 이하의 값으로 고정되거나 5회 이하의 값으로 설정할 수 있어야 한다.

④ 일정시간 동안 인증 기능을 비활성화하도록 구현하는 경우 재활성화까지 소요되는 시간은 5분 이상의 값으로 고정되거나 설정할 수 있어야 한다.

참고 사항

① 단일 인증세션에서 △2.1.1에서 규정한 식별 및 인증 또는 △2.1.2에서 규정한 추가적인 식별 및 인증 중에서 하나만 실패하여도 해당 인증세션은 실패로 본다.

점검시 유의사항

① 제출문서를 통해 잘못된 인증 정보를 사용한 반복된 인증 시도를 제한하는 방법이 있는지 확인해야 한다.

② 시험원은 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP, ONVIF, RTSP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

③ 비활성화 된 계정 외의 다른 관리자 계정으로 인증 성공시 잠금된 계정의 잠금이 해제되지 않는지 확인해야 한다.

④ 관리자 접속 PC의 시간을 식별 및 인증 비활성화 이전 시간으로 변경하여 인증을 시도하는 경우에도 비활성화 기능이 정상적으로 동작하는지 확인해야 한다.

⑤ 횟수(5회)나 기간(5분)은 기본값으로 고정되거나 설정할 수 있어야 한다.

2.2.2

필수

제품은 관리자 인증시 설정된 횟수만큼 연속적으로 실패하면, 관리자가 즉시 확인할 수 있는 수단을 통해 통보해야 한다.

요구항목

① *알람, 문자 메시지, 이메일 등* 중에서 한 가지 이상의 수단을 통해 통보해야 한다.

점검시 유의사항

① 시험원은 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP, ONVIF, RTSP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

2.3 패스워드 등 민감정보 생성 및 안전성 검증

2.3.1

필수

제품은 패스워드 등록 및 변경시 〈표 1〉의 보안성 기준을 만족해야 한다.

요구항목

〈 표 1. 패스워드 보안성 기준 유형(1)〉

구분	내용	비고
준수 사항	9자리 이상의 길이 확보	필수
	숫자, 대문자(영문), 소문자(영문), 특수문자가 각 1개 이상 포함	필수

구분	내용	비고
금지 항목	사용자계정(ID)과 동일한 패스워드 설정금지	필수
	동일한 문자 · 숫자 연속적으로 반복사용 금지	필수
	키보드의 연속된 문자 또는 숫자의 순차적 나열 금지	필수
	직전 사용된 패스워드 재사용 금지	둘중 어느 하나 구현
	3개월 이내 사용된 패스워드 재사용 금지	

점검시 유의사항

① '3개월 이내 사용된 패스워드 재사용 금지' 기능을 선택, 구현한 경우 재사용 금지 기간은 3개월 이내에서 고정하거나 가변적으로 설정할 수 있어야 한다.

② '키보드상의 연속되거나 순차적인 입력'으로 간주되는 문자 · 숫자의 입력은 다음과 같다.

- △'q', 'w', 'e', 'r' △'a', 's', 'd', 'f' △'1', '2', '3', '4' 등 좌우로 연속한 문자 또는 숫자를 4개 이상 입력하는 경우.(특수문자는 제외한다.)

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

요구항목

① 적용대상으로 *관리프로그램 연동을 위한 패스워드, SNMP 인증 · 암호화 패스워드 등*이 될 수 있다.

② 외부 IT실체 인증에 패스워드가 사용되는 경우 △2.3.1의 보안성 기준을 준수해야 한다.

참고 사항

① 외부 IT실체 인증 기능을 위한 패스워드의 경우 보안성 기준에 포함된 문자라도

외부 IT실체가 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 제품과 외부 IT실체가 연동하기 위해 제품이 인증해야 하는 외부 IT 실체를 모두 조사하고 인증에 필요한 인증 정보를 설정하는 인터페이스가 제공되는지 확인해야 한다.

② 시험원은 외부 IT실체를 인증하는데 사용되는 인증 정보가 제품이 통제하는 저장소에 저장되는 경우 '4.2 저장 데이터 보호' 요구사항에 따라 저장되는지 확인해야 한다.

③ 제품이 인증하는 외부 IT실체가 없을 경우 '해당사항 없음'으로 판정한다.

2.4 인증 정보 재사용 방지

2.4.1

필수

제품은 사용자의 인증 정보의 재사용을 방지(*타임 스탬프 사용, 세션 ID 암호화 등*)해야 한다.

요구항목

① △1.1.1 △2.1.1 △2.1.2에서 규정한 식별 및 인증에 사용되는 인증 정보에 필수적으로 적용한다.

② △2.1.2에서 규정한 추가적인 식별 및 인증 방법을 제공하기 위해 제품이 사용자로부터 인증정보를 입력받는 경우 해당 인증 정보에 필수로 적용한다.

③ 세션 ID를 암호화하거나 세션 ID의 유일성을 보장(*타임스탬프, 난수 값 포함, 세션 만료시간 설정 등*)하여 방지할 수 있다.

④ 제품에서 재사용이 금지된 인증 정보의 재사용 시도를 탐지한 경우 인증에 실패해야 하며 인증 실패 사건에 대한 감사기록을 생성해야 한다.

참고 사항

① 제품이 외부 IT실체의 추가적인 식별 및 인증 수행 결과만을 전달받는 경우

해당 인증 정보의 재사용 방지는 외부 IT실체에서 제공한다고 가정한다.

② 세션 만료시간은 제공 서비스 특성을 고려하여 최소화 할 수 있는 값으로 설정해야 한다.

점검시 유의사항

① 사용자가 로그아웃 하지않고 이전에 사용한 인증 정보(*세션ID, 쿠키 등*)로 변경한 후 다시 로그인시 실패여부를 확인해야 한다.

② 사용자 로그아웃 이후 이전에 사용한 인증 정보(*세션ID, 쿠키 등*)로 변경하여 재로그인시 실패여부를 확인해야 한다.

③ 사용자 로그인시 사용자 패스워드는 암호화된 상태로 전송하는지 확인해야 한다.

2.5 인증 피드백 보호

2.5.1

필수

제품은 인증에서 사용되는 정보를 출력장치에 표시할 때 내용을 표시하지 않아야 한다.

요구항목

① △1.1.1 △2.1.1 △2.1.2 △2.3.1에서 규정한 인증 정보가 출력장치에 표시되는 경우에 적용한다.

② 인증에 사용되는 정보는 *입력내용의 미표시, 입력문자 대신 "*"으로 표시 등*의 형태로 출력해야 한다.

③ 사용자 로그인시 인증 정보가 메모리 영역에 평문으로 노출되지 않아야 한다.

점검시 유의사항

① 시험원은 제품의 인증 정보 입력이 필요한 보안 기능에 대해 조사해야 한다.

② 사용자가 로그인할 때 뿐 아니라 신규 사용자 계정 생성, 패스워드 변경 등 인증정보를 입력하는 기능을 모두 식별하여 요구사항 만족여부를 확인해야

한다.

③ 시험원은 사용자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP, ONVIF, RTSP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

2.5.2

필수

제품은 식별 및 인증 실패시, 실패 사유에 대한 피드백(*존재하지 않는 계정(ID), 패스워드 오류 등*)을 제공하지 않아야 한다.

점검시 유의사항

① 잘못된 인증 정보 입력으로 인증실패 유도 후, 알림 메시지에 인증 실패 사유를 추측할 수 있는 피드백을 제공하는지 확인해야 한다.

3. 보안관리

인가된 관리자만이 제품의 보안기능 및 중요데이터에 대한 관리를 수행하도록 허용함으로써 제품의 보안관리를 위한 요구사항을 만족하는지 확인한다.

3.1 보안관리 기능

3.1.1

필수

제품은 인가된 관리자에게 보안기능, 보안정책, 중요 데이터 등을 설정 및 관리할 수 있는 보안관리 기능을 제공해야 한다.

요구항목

① 보안관리 기능에 해당되는 항목은 다음과 같다.

- 보안기능의 동작을 결정할 수 있는 조건 또는 규칙을 추가, 삭제, 변경하는 기능.
- 조건 또는 규칙에 따라 제품이 수행해야 할 행동을 추가, 제거, 변경하는 기능.
- 제품의 설정을 선택, 변경하는 기능.

- 카메라 제어를 설정, 변경하는 기능.

② 제품이 구현해야 하는 보안관리 기능은 아래 〈표 2〉 와 같다.

〈 표 2. 제품이 구현해야하는 보안관리 기능 〉

소분류	보안관리	비고
식별 및 인증	사용자의 등록, 삭제, 수정, 권한 부여	제품에 등록된 사용자가 유일한 경우 해당사항 없음
	사용자의 패스워드 조합 · 길이 정책 설정	기능 제공시 필수
	사용자의 인증 실패 허용 횟수 설정	기능 제공시 필수
	사용자의 인증 실패 대응방법 설정	기능 제공시 필수
	사용자 인증 기능 비활성화된 후 활성화까지의 시간 설정	기능 제공시 필수
	제품이 인증하는 외부 IT실체 인증정보 설정	기능 제공시 필수
보안 관리	관리용 단말기의 IP 등록, 삭제, 수정	
	중요 데이터, 설정정보, 감사기록 등의 백업	기능 제공시 필수
	중요 데이터, 설정정보, 감사기록 등의 복구	기능 제공시 필수
	관리접속 서비스 활성화, 비활성화	기능 제공시 필수
보안 관리	외부 IT실체 접근을 위한 인증정보 설정	기능 제공시 필수
	카메라 제어(PTZ 등) 설정 및 동작 설정 초기화	기능 제공시 필수
자체보호	관리자 요청에 의한 제품의 보안기능 자체시험 수행	기능 제공시 필수
	자체시험 실패시 대응행동 설정	기능 제공시 필수
	관리자 요청에 의한 제품의 설정값 및 제품 자체의 무결성 검사 수행	
	무결성 검사 실패시 대응행동 설정	기능 제공시 필수
업데이트 보호	관리자에 의한 업데이트 파일 유효성 수동 검증	기능 제공시 필수
	관리자에 의한 업데이트 파일 설치 실패 수동 복구	기능 제공시 필수
	제품 버전정보 조회	
세션 관리	사용자 세션 잠금, 종료 시간 설정	기능 제공시 필수

소분류	보안관리	비고
세션 관리	(세션 잠금의 경우) 세션의 잠금 해제시 관리자 또는 개별 사용자 인증	
	사용자 동시 접속 세션수 설정	기능 제공시 필수
감사기록	감사기록의 조회	
	감사기록 손실 대응 관련 설정	기능 제공시 필수

참고 사항

① 제품의 관리프로그램은 〈표 2〉의 필수 보안관리 기능을 모두 수행할 수 있어야 한다.

점검시 유의사항

① 시험원은 제품이 제공하는 모든 보안관리 기능을 식별해야 한다.

- 시험원은 제품이 제공하는 모든 보안관리 기능이 「보안기능 구현명세서」 또는 「보안기능 운용설명서」에 기술되어 있는지 확인해야 한다.
- 시험원은 모든 보안관리 기능이 요구사항을 만족하는지 확인해야 한다.

② 보안관리 기능은 인가된 관리자만 실행할 수 있는지 확인해야 한다.

③ 입력값에 대한 검증(*허용되지 않는 문자, 길이 등 제한 등*)을 수행하는지 확인해야 한다.

3.2 관리접속 기능

3.2.1

조건부 필수

제품은 모든 관리접속에 대해 활성화 · 비활성화 기능을 제공해야 한다.

조 건	제품이 두 가지 이상의 관리접속을 지원하는 경우

여 백

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리접속을 조사해야 한다.

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

③ 제품에서 제공하는 기능을 이용하여 관리접속을 비활성화한 후, 제품 외부에서 포트스캔을 수행하여 열린 포트가 존재하는지 확인해야 한다.

④ 제품 내에서 운용되는 DBMS에 대해 원격으로 직접 접근은 제한되어야 한다.

⑤ 외부에서 접근 가능한 API를 제공하는 장비의 경우, 시험원은 해당 서비스에 대한 활성화 · 비활성화 기능 여부를 확인해야 한다.

⑥ 시험원은 제품에서 관리접속이 암호통신만을 사용하는지 확인해야 한다.

⑦ 제품이 하나의 관리접속만을 제공하는 경우 '해당사항 없음'으로 판정한다.

3.3 보안관리용 IP제한

3.3.1

필수

제품은 접속 가능한 관리용 단말기의 IP를 제한하는 기능을 제공해야 한다.

요구항목

① 관리용 단말기 IP 주소를 등록, 삭제, 수정 가능해야 한다.

② 관리 용도 대신에 읽기 권한만 가지는 관리자(*영상 모니터링 관리자 등*)가 접속 가능한 관리용 단말기는 추가로 등록해서 운용 가능하다.

③ 접속 가능한 관리용 단말기의 IP는 단일 호스트 단위로 1개씩만 추가 가능하다.

④ 192.168.10.2~253 등과 같이 IP 주소 범위를 지정하여 추가하는 방식 또는 네트워크 전체 범위를 의미하는 0.0.0.0, 192.168.10.*, any 등을 이용한 등록은 허용되지 않는다.

점검시 유의사항

① IP 등록시 단일 IP별로 등록 가능한지 확인해야 한다.

② IP주소 범위 지정하여 추가하는 방식을 허용하지 않는지 확인해야 한다.

③ 관리 용도 대신에 읽기 권한만 가지는 관리자(*영상 모니터링 관리자 등*)가 접속 가능한 PC는 추가로 등록 가능하다.

3.4 기본 제공되는 계정 및 패스워드 등의 관리

3.4.1

필수

제품은 최초 제품 접속(*로컬 운용 등*) 시 기본 제공되는 계정을 강제 변경 · 사용중지하는 기능을 제공해야 한다.

요구항목

① 최초 접속시, 기본 제공되는 계정을 화면에 출력해야 한다.

② 기본 제공되는 계정은 최초 접속시 강제 변경 또는 사용중지(Disable)되어야 한다.

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

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

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리접속(*SSH, HTTPS 등*), 로컬 운용에 대해 조사해야 한다.

② 제품의 모든 기능은 제공되는 계정의 변경 · 사용중지 또는 생성이 진행된 이후에만 동작되는지 확인해야 한다.

③ 시험원은 화면에 출력되지 않는 계정이 있는지 확인해야 한다.

④ 시험원은 화면에 출력되지 않은 계정을 추가로 식별한 경우, 시험결과보고서에 해당 계정을 백도어로 기록하고 '불만족'으로 판정한다.

3.4.2

필수

제품은 최초 제품 접속(*관리 접속, 로컬 운용 등*)시 관리자 기본(default) 패스워드를 강제 변경 · 생성하는 기능을 제공해야 한다.

요구항목

① 기본(default) 패스워드가 존재하는 경우 최초 제품 접속시 기본(default) 패스워드를 변경하는 기능을 제공해야 하며, 이후 제품의 관리 접속 · 로컬 운용이 가능해야 한다.

② 기본(default) 패스워드가 없는 경우, 신규 패스워드를 생성해야 하며, 이후 제품의 로컬 운용 · 관리접속이 가능해야 한다.

- 패스워드는 2.3.1의 보안성 기준을 준수해야 한다.

점검시 유의사항

① 시험원은 제품에서 지원하는 모든 관리 접속(*SSH, HTTPS 등*), 로컬 운용에 대해 조사해야 한다.

② 최초 접속이 로컬 운용으로 제한되어 있고 관리자 생성 이후 다른 관리접속이 가능한 경우 이 항목을 '만족'으로 판정한다.

③ 제품의 모든 기능은 기본(default) 패스워드 변경 또는 생성이 진행된 이후에만 동작되는지 확인해야 한다.

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 패스워드가 필요한 기능 제공시

요구항목

① 기본(default) 패스워드의 예시로는 DBMS 패스워드, 웹서버 · WAS서버 패스워드 등이 있다.

② 제품이 DBMS에 접근하기 위한 기본(default) 패스워드를 저장하는 경우 제품에서 기본(default) 패스워드를 변경하는 기능을 제공해야 한다.

③ 제품이 웹서버 · WAS서버에 접근하기 위한 기본(default) 패스워드를 저장하는 경우 기본(default) 패스워드를 변경하는 기능을 제공해야 한다.

④ 패스워드 생성시 추가적 식별 및 인증 기능 병행 유무에 따라 2.3.1의 보안성 기준을 준수해야 한다.

⑤ 제품에 DBMS · 웹서버 · WAS서버에 접근하기 위한 기본(default) 계정(ID)이 존재하는 경우 이를 변경하는 기능을 제공할 수 있다.

참고 사항

① 제품 내에 DBMS · 웹서버 · WAS서버 등을 포함할 수 있고(*예: 하드웨어 일체형 제품*), 제품 외부에 별도로 존재하는 DBMS · 웹서버 · WAS서버 등과 연동할 수도 있다.

② 패스워드 보안성 기준에 포함된 문자라도 연동하는 외부 IT실체에서 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 기타 인증 정보가 필요한 제품 내에 존재하는 또는 제품과 연동하는 인증서버, DBMS · 웹서버 · WAS서버 등에 대해 조사해야 한다.

② 시험원은 인증 정보가 패스워드인 경우 2.3.1의 보안성 기준을 만족하는지 확인해야 한다.

③ DBMS · 웹서버 · WAS서버 관리자 기본(default) 계정(ID)을 변경하는 기능은 선택적으로 구현 가능하다.

④ 제품이 내부 구성요소 또는 외부 IT실체에 접근하는 기능이 없는 경우 '해당 사항 없음'으로 판정한다.

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 인증정보 요구시

요구항목

① 인증정보의 예시로는 SMTP 서버에서 제품을 인증하기 위해 사용하는 패스워드 등이 있다.

② 패스워드 생성시 '서버 공통보안요구사항 1.3.2'에 규정된 보안성 기준의 준수를 권고한다.

- 다만, 패스워드 보안성 기준에 포함된 문자라도 연동하는 외부 IT실체에서 입력을 허용하지 않는 문자는 포함하지 않을 수 있다.

점검시 유의사항

① 시험원은 제품과 연동시 제품을 인증한 후 접근을 허용하는 SMTP 서버 등에 대해 조사해야 한다.

② 시험원은 제품과 외부 IT실체간 연동을 위해 외부 IT실체에서 제품을 인증하는 경우를 모두 조사하고 인증 정보 설정 인터페이스가 제공되는지 확인한다.

③ 시험원은 인증 정보가 패스워드인 경우 '서버 공통보안요구사항 1.3.2'의 보안성 기준을 만족하는지 확인해야 한다.

④ 제품이 외부 IT실체에 인증받는 기능이 없는 경우 '해당사항 없음'으로 판정한다.

4. 데이터 보호

제품이 사용자 또는 외부 IT실체와의 통신 간에 전송되는 데이터를 노출 · 변경으로부터 보호하기 위해 암호통신을 지원하는지 확인한다. 제품은 저장소에 저장되는 보안기능 관련 데이터를 비인가 노출로부터 보호해야 한다.

4.1 전송 데이터 보호

4.1.1

조건부 필수

제품은 제품 구성요소간 전송 데이터(*보안정책, 제어명령 등*)를 보호하기 위해 암호통신 채널을 사용하여 전송해야 한다.

조 건	제품 구성요소에 관리프로그램이 포함될 경우

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.

③ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 패킷 모니터링 도구를 활용하여 전송 데이터에 대한 기밀성, 무결성을 제공하는지 확인해야 한다.

② 시험원은 요구사항에 따른 정확한 구현을 시험하기 위해 필요시 개발자를 직접 대면하여 구현내용에 대한 설명을 요청할 수 있다.

③ 모든 구성요소간 전송 데이터를 암호화하여 전송하는지 확인해야 한다.

④ 물리적으로 분리된 곳에서 운용가능한 제품 구성요소가 없을 경우, '해당사항 없음'으로 판정한다.

4.1.2

조건부 필수

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

조 건	관리접속 기능 지원시

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.

③ 암호통신 채널은 제품에 직접 구현하거나 제품이 운영환경을 이용하여 제공하도록 구현될 수 있다.

④ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 패킷 모니터링 도구를 활용하여 전송 데이터에 대한 기밀성, 무결성을 제공하는지 확인해야 한다.

② 시험원은 요구사항에 따른 정확한 구현을 시험하기 위해 필요시 개발자를 직접 대면하여 구현내용에 대한 설명을 요청할 수 있다.

③ 제품에서 운용 가능한 관리접속이 없을 경우, '해당사항 없음'으로 판정한다.

4.1.3

조건부 필수

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

조 건	외부 IT실체와 연동 지원시

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.

③ 암호통신 채널은 제품에 직접 구현하거나 제품이 운영환경을 이용하여 제공하도록 구현될 수 있다.

④ 제품이 보안기능을 제공하기 위해 외부 IT실체와 연동하는 기능을 제공하는 경우 이 요구사항을 적용해야 한다.

⑤ 외부 IT실체와 연동시 암호통신 채널을 사용하여 전송 데이터를 보호하지 않는다면 전송 데이터 기밀성, 무결성 보호의 불필요성이 입증되어야 한다.

⑥ 암호통신 채널을 지원하지 않는 통신서비스는 비활성화 할 수 있어야 한다.

⑦ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

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.

점검시 유의사항

① 제품이 보안기능을 제공하기 위해 외부 IT실체와 연동을 지원하는 경우 이 요구사항을 적용해서 시험해야 한다.

② 다만, 외부 IT실체 중에서 NTP 서버와의 통신에는 이 요구사항을 적용하지 않는다.

③ syslog를 지원하면 *syslog over TLS(RFC 5424), syslog over DTLS(RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.

④ 제품이 외부 IT실체와 연동하는 기능이 없는 경우, '해당사항 없음'으로 판정한다.

여 백

4.2 저장 데이터 보호

4.2.1

필수

중요정보를 제품 내부에 저장할 때 정해진 방식으로 저장해야 한다.

요구항목

① 최소한 다음의 중요정보를 제품이 저장하는 경우 암호화하여 저장해야 한다.

- 제품이 사용자 식별 및 인증을 위해 사용하는 패스워드.
- 제품이 추가적인 식별 및 인증을 위해 사용되는 인증정보.
- 데이터 암호화 키(DEK: Data Encryption Key)

② 데이터 암호화 키(DEK)는 키 암호화 키(KEK : Key Encryption Key)를 사용, 암호화하여 저장해야 한다.

③ 키 암호화 키(KEK) 생성 및 저장 등과 관련된 요구사항은 '9.2 암호키 생성' 및 '9.3 암호키 저장' 요구사항을 만족해야 한다.

④ 다음과 같은 정보를 제품이 저장하는 경우 *암호화, 접근통제 등*의 방식으로 저장해야 한다.

- 제품과 외부 IT실체의 연동시 상호간 인증에 사용되는정보.
- 제품이 제품 내부 또는 외부에 존재하는 DBMS · 웹서버 · WAS서버에 접근하기 위해 필요한 DBMS · 웹서버 · WAS서버 관리자 패스워드.
- 암호키(사전공유키, 대칭키, 개인키)
- 조직의 중요정보를 포함하는 탐지 규칙, 시그니처 등.

⑤ 제품이 사용자 식별 · 인증을 위해 사용하는 사용자 패스워드는 일방향 암호(해시) 또는 양방향 암호를 이용하여 저장해야한다.

- 일방향 암호화 수행시 패스워드에 salt라는 랜덤하게 생성한 값을 추가하여 적용할 필요가 있다.
- salt 값은 비밀일 필요는 없으며, 난수발생기를 이용하여 생성하고 크기는 최소 48bit 이상이어야 한다.

- iteration count는 가능한 큰 값을 적용해야 한다.(최소 1000회 이상)

⑥ 제품 운영에 필요한 DBMS · 웹서버 · WAS서버 관리자 패스워드 등은 공개키 · 대칭키 암호 알고리즘을 적용하여 암호화하여 저장할 수 있다.

⑦ 암호키는 *사전공유키, 대칭키, 개인키 등*을 의미하며 제품 관리접속 · 로컬접속, 제품 구성요소간 연동 설정에 사용되는 키들이 모두 대상이다.

⑧ 암호화해서 저장해야 하는 최소한의 중요정보에 포함된 패스워드 및 암호키는 제품에 하드코딩하여 저장할 수 없다.

⑨ 신청업체는 제품이 지원하는 저장 데이터 보호 방법에 대한 상세한 설명자료(「보안기능 구현명세서」)를 제출하여 안전성을 입증해야 한다.

⑩ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

⑪ 검증필 암호모듈(KCMVP)의 사용을 권고한다.

참고 사항

① 제품을 운용하는 조직의 중요정보가 통합보안관리, 침입방지시스템 제품의 탐지 규칙, 시그니처 등에 포함될시 노출로부터 보호하는 방식으로 저장해야 한다.

② 저장된 모든 중요정보는 읽거나 유추할 수 없어야 한다.

③ 난수발생기는 '9. 암호 지원' 요구사항에 따라 국내 · 외 표준을 준수하여 구현되어야 한다.

점검시 유의사항

① 동일 패스워드 입력시 동일한 암호문이 생성 · 저장되지 않음을 확인해야 한다.

② 패스워드를 일방향 암호화 할 경우 표준에 따라 저장되는 값이 생성되는지 확인해야 한다.

③ 패스워드를 암호화 하여 저장할 경우 '9. 암호 지원' 요구사항에 따라 암호키가 저장되는지 확인해야 한다.

④ '9. 암호 지원' 요구사항에 따라 난수발생기를 사용하는지 확인해야 한다.

⑤ *DB 접속 패스워드, 자동 로그인에 필요한 패스워드, 키 암호화 키 등*이 제품에 하드코딩되어 있지 않는지 확인해야 한다.

4.2.2

필수

제품은 저장된 제품 설정값(*보안정책, 환경설정 매개변수 등*)에 인가된 관리자만이 접근할 수 있도록 보호하는 기능을 제공해야 한다.

요구항목

① 하드웨어 일체형 제품인 경우 내부에 저장된 제품 설정값을 보호해야한다. 소프트웨어 제품인 경우 설치된 후 제품이 통제하는 저장소에 저장된 제품 설정값을 보호해야 한다.

② 제품은 인가된 관리자만이 제품 설정값에 접근할 수 있도록 하는 인터페이스를 제공해야 하며, 인가된 관리자 외에는 제품 설정값에 접근할 수 없어야 한다.

- 접근이라 함은 읽기, 변경, 삭제 등의 오퍼레이션을 의미한다.

③ 제품 설정값을 외부에 파일형태로 백업하는 기능을 제공할 경우, 암호화하는 기능을 제공해야 한다.

④ 암호화시 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

① 제품 설정값은 연동되는 운영환경인 DBMS에 파일형태로 저장될 수 있다.

② 제품 보안기능으로 완전히 구현할 수 없는 경우, 운영환경에서 제품 설정값 저장소를 보호할 수 있도록 지원할 수 있다.

- 제품 설정값이 연동되는 운영환경의 DBMS에 저장되는 경우, DBMS의 식별 및 인증 기능을 이용, 비인가된 사용자의 접근으로부터 보호할 수 있다.

점검시 유의사항

① 제품 설정값을 내부에 저장할 경우 암호화하여 보호하는 기능을 제공하는 것도

요구사항 '만족'으로 판정이 가능하다.

② 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

5. 자체보호

제품은 보안기능이 정상적으로 동작함을 보장하기 위해서 주기적 또는 관리자 요청에 의해 자체시험을 수행할 수 있어야 한다. 보안기능을 제공하는 메커니즘 및 데이터의 무결성을 확인하여 제품의 보안 기능을 보호해야 한다.

5.1 보안기능 자체 시험

5.1.1

필수

제품은 구동(또는 실행) · 운용중에 주기적 또는 관리자의 요청에 의해 자체시험을 수행해야 한다.

요구항목

① 제품 구동(또는 실행)시 필수로 자체시험을 수행해야 하고 운용중에는 주기적 또는 관리자의 요청에 의한 수행을 지원해야 한다.

② 자체시험 대상은 제품의 주요 프로세스를 의미하며 프로세스가 정상적으로 실행되고 있는지 확인해야 한다.

③ 자체시험 대상은 신청업체가 선택 가능하나, 시험 대상이 되는 실체의 비정상 상태(*오류, 정지 등*)로 인하여 제품의 보안 기능에 영향을 미치는 경우 해당 실체는 자체시험 대상으로 반드시 포함해야 한다.

④ 자체시험 수행 이력은 화면 출력, 감사기록을 통해 확인할 수 있어야 한다.

⑤ 하드웨어 일체형 제품은 아래 요구사항을 만족해야 한다.

- 제품 시작시 및 운영중 제품 범위에 포함되는 하드웨어(*메모리, 플래시, NIC 등*) 및 소프트웨어(*프로세스 등*)의 오류를 탐지할 수 있는 자체시험을 수행해야 한다.

⑥ 물리적으로 분리된 제품 구성요소가 존재하는 경우 모든 구성요소를 포함하도록 대상을 선택하여 자체시험을 수행해야 한다.

⑦ 신청기관은 제출문서에 자체시험 기능에 대해 상세히 기술해야한다.

점검시 유의사항

① 하드웨어 · 운영체제는 하드웨어 일체형 제품일 경우 제품 범위에 포함된다. 소프트웨어 제품일 경우 포함되지 않는다.

② 관리프로그램은 자체검사의 대상에 포함되지 않는다.

③ 시험원은 제출물에 자체시험에 대해 상세히 기술되어 있는지 확인한다.

5.1.2

필수

제품의 자체시험 결과가 실패인 경우 대응기능을 수행해야 한다.

요구항목

① 제품은 정확한 작동을 보장하기 위해 구현된 대응 기능을 수행하거나 관리자가 설정한 대응 기능을 수행해야 한다.

② 자체시험 결과에 대한 감사기록을 생성해야 한다.

③ 자체시험 결과 실패시 수행하는 대응기능의 예로써 *프로그램 실행중단, 경고 메시지 화면 출력, 프로세스 재구동 등*이 있다.

④ 관리자가 대응기능을 설정할 수 있도록 보안관리 기능을 제공할 수 있다.

점검시 유의사항

① 제품이 △처음 실행(또는 구동)시 △관리자 수동 요청시 자체시험이 실패한 경우를 모두 확인해야 한다.

② 대응기능에 대한 관리자 설정기능이 있는 경우, ‘3.1 보안관리 기능’ 요구사항에 따라 시험을 수행해야 한다.

5.2 무결성 검증

5.2.1

필수

제품은 자체 및 설정값의 무결성을 검증하는 기능을 제공해야 한다.

요구항목

① 무결성 검증 대상은 제품의 설정값(*환경설정파일 등*) 및 제품 자체(*프로세스, 라이브러리, 실행파일 등*)이다.

② 제품을 처음 실행시(또는 구동시) 무결성 검증을 수행해야 하며, 부가적으로 주기적인 무결성 검증을 수행할 수 있다.

③ 무결성 검증 대상은 신청업체가 선택 가능하나, 검증 대상이 되는 실체의 비정상 상태(*오류, 정지 등*)로 인하여 제품의 보안 기능에 영향을 미치는 경우 해당 실체는 무결성 검증 대상으로 반드시 포함해야 한다.

④ 물리적으로 분리된 제품 구성요소가 존재하는 경우 모든 구성요소를 포함하도록 대상을 선택하여 무결성 검증을 수행해야 한다.

⑤ 관리자가 무결성 검증을 수행하는 기능을 제공해야 한다.

⑥ 신청업체는 제품이 지원하는 무결성 검증 기능에 대한 상세한 설명자료(「보안기능 구현명세서」)를 제출해야 한다.

⑦ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 시험원은 제품의 무결성 검증 대상 및 메커니즘을 조사해야 한다.

② 제품이 자동으로 무결성 검증을 수행하는 주기는 1일 이내의 값으로 고정 또는 설정 가능한지 확인해야 한다.

③ 해시값 비교 방법으로 무결성 점검 기능을 수행할 때 원본 해시값이 파일 시스템에 저장되는 형태일 경우, 원본 해시값이 보호되는지 확인해야 한다.

④ 시험원은 제품의 무결성 검증을 위한 데이터가 저장될 때 ‘4.2 저장 데이터 보호’ 요구사항에 따라 저장되는지 확인해야 한다.

5.2.2

조건부 필수

제품은 운영체제 커널 또는 커널 레벨 모듈에 대한 무결성을 검증하는 기능을 제공해야 한다.

조 건	제품 범위에 운영체제 커널 또는 커널 레벨 모듈이 포함된 경우

요구항목

① 해시값 비교 방법으로 무결성 검증시 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 ‘9. 암호 지원’ 요구사항을 만족해야 한다.

점검시 유의사항

① 하드웨어 일체형 제품에 대해서는 시험을 수행해야 한다.

② 제품에 운영체제 커널 또는 커널 레벨 모듈이 포함되지 않는 소프트웨어 제품은 ‘해당사항 없음’으로 판정한다.

5.2.3

필수

제품은 무결성 검증 내용 및 결과를 관리자가 확인하는 기능을 제공해야 한다.

요구항목

① 무결성 검증 내용 및 결과는 화면 출력, 감사기록을 통해 확인할 수 있어야 한다.

점검시 유의사항

① 무결성 검사 수행 주기가 매우 짧은 경우, 무결성 검사 성공에 대한 감사기록이 다수 발생할 수 있으므로 일정 시간 내에 발생한 무결성 검사 성공에 대해 감사기록을 1회 생성하고, 무결성 검사 성공 횟수를 감사기록에 추가하여

생성하는 것이 가능하다.

5.2.4

필수

제품은 무결성 검증 실패인 경우 대응 기능을 수행해야 한다.

요구항목

① 제품은 자체에 구현된 대응기능을 수행하거나 관리자가 설정한 대응 기능을 수행해야 한다.

② 무결성 검증 결과에 대한 감사기록을 생성해야 한다.

③ 무결성 검증 결과 실패시 수행하는 대응 기능의 예로써 *프로그램 실행중단, 경고메시지 화면 출력 등*이 있다.

④ 관리자가 대응기능을 설정 할 수 있도록 보안관리 기능을 제공할 수 있다.

점검시 유의사항

① 제품이 △처음 실행시(또는 구동시) △관리자 수동 요청시 △주기적 실행시 무결성 검증이 실패한 경우를 모두 확인해야 한다.

② 대응기능에 대한 관리자 설정 기능이 없는 경우, 제품에 기본적으로 설정된 대응기능을 수행하면 요구사항을 만족하는 것으로 판정한다.

③ 대응기능에 대한 관리자 설정기능이 있는 경우, '3.1 보안관리 기능' 요구사항에 따라 시험을 수행해야 한다.

6. 업데이트 보호

제품은 제품 설치 파일, 제품 운영에 필요한 파일 등 '업데이트 파일'을 설치 또는 적용하는 기능을 제공할 수 있다. 제품은 업데이트 파일을 설치하거나 적용하기 전에 업데이트 파일에 대한 유효성 검증 등을 수행해야 한다.

■ 6.1 업데이트 지원

6.1.1

필수

제품은 업데이트 파일을 설치하거나 적용하기 전에 제품 업데이트 파일의 유효성을 검증해야 한다.

요구항목

① 제품은 업데이트 시, 유효성 검증에 성공한 업데이트 파일만 설치하거나 적용해야 한다.

② 업데이트 파일의 유효성 검증시 무결성 검증이 필수이며 *전자서명 검증, 공개된 해시값 검증 등*을 이용하여 구현해야 한다.

③ 전자서명 검증시 인증서 유효성 검증을 수행해야 한다.

④ 암호 알고리즘 및 암호키 안전성은 '9. 암호 지원' 요구사항을 만족해야 한다.

⑤ 업데이트 파일 유효성 검증결과(성공 · 실패)는 감사기록에 기록되어야 한다.

점검시 유의사항

① 업데이트 파일의 유효성 검증은 *전자서명 검증, 공개된 해시값 검증 등*을 통해 확인할 수 있다.

② 업데이트 설치 · 수행을 인가된 관리자로 제한하는지 확인해야 한다.

③ 유효성 확인이 없는 자동 업데이트 기능은 허용되지 않는다.

6.1.2

필수

제품은 '제품의 유일한 식별 정보'를 사용자가 확인하는 기능을 제공해야 한다.

요구항목

① 제품 식별 정보는 유일해야 하고 인터페이스를 통해 사용자가 확인할 수 있고 수정 · 변경할 수 없어야 하며 다음 사항이 포함되어야 한다.

- 제품 명칭, 제품 버전, 제품 릴리즈 또는 빌드 번호, 펌웨어 또는 소프트웨어 해시 값

② 제품이 물리적으로 분리된 다수의 구성요소를 포함하는 경우 각 구성요소의 식별 정보는 유일해야 하고 사용자가 확인할 수 있어야할 뿐 아니라 수정 · 변경할 수 없어야 하며 다음 사항이 포함되어야 한다.

- 구성요소를 포함하는 제품 명칭 및 버전, 구성요소 명칭, 구성요소 버전, 구성요소 릴리즈 또는 빌드 번호.

③ 제품 · 구성요소의 패치 및 기능개선 여부를 확인할 수 있는 버전 관리 체계를 적용해야 한다.

(*패치 및 기능개선시 사안별로 Major 버전, Minor 버전, 릴리즈 번호 · 빌드 번호를 변경하는 체계를 마련하여 제품 · 구성요소 변경 사유를 버전 정보로 추적*)

④ 제품 식별 정보 외에 펌웨어의 유일한 식별 정보 및 해시 값을 제품 인터페이스를 통해 사용자가 확인할 수 있어야 한다.

점검시 유의사항

① 제품과 물리적으로 분리된 구성요소가 존재하는 경우 각각의 버전 정보를 출력할 수 있어야 한다.

6.1.3

필수

제품은 업데이트 설치 실패시 자동으로 기존 버전을 유지하는 기능을 제공해야 한다.

요구항목

① 업데이트 설치 결과 및 실패 사유에 대한 감사기록을 생성해야 한다.

② 제품에서 지원하지 않을 경우, 관리자에 의한 수동 복구를 지원해야 한다.

③ 개발업체는 관리자에 의한 수동 복구 절차를 제출물에 상세히 기술해야 한다.

점검시 유의사항

① 업데이트 설치 수행을 인가된 관리자로 제한하는지 확인해야 한다.

② 제품에서 지원하지 않는 경우, 제출물에 수동 복구 절차가 명시되어 있는지 확인해야 한다.

③ 하드웨어 일체형 제품의 경우 수동 복구 방법으로 설정 초기화도 허용된다.

7. 세션 관리

제품은 제3자 정보 유출 방지를 위해 사용자가 오랫동안 사용하지 않을 경우 세션을 잠그거나 종료시켜야 하며 동시 접속 세션의 제한기능을 제공해야 한다.

7.1 세션 잠금 · 종료 기능

7.1.1

필수

제품은 관리자 세션 연결 이후 일정시간 동안 사용하지 않을 경우, 세션을 잠그거나 종료하는 기능을 제공해야 한다.

요구항목

① 사용되는 시간정보는 서버 시간을 기준으로 적용해야 한다.

② 일정시간은 세션 잠금 또는 종료행위를 촉발시키는 연결 이후, 누적 시간량을 의미한다.

- 일정시간은 관리자가 10분 이하의 값 중에서 고정하거나 인증 실패 횟수에 비례하여 설정할 수 있다.

③ 잠겨진 세션은 잠금시간이 경과한 후, 관리자에 의하거나 각 세션별 사용자 인증 기능을 통해서 해제되어야 한다.

④ 세션 잠금이나 종료 기능 동작시 감사기록을 생성해야 한다.

⑤ 제품에 포함되는 모든 관리접속에 적용해야 한다.

참고 사항

① 영상 모니터링 기능에 대해서는 적용하지 않을 수 있다.

점검시 유의사항

① 제품이 지원하는 모든 로컬운용 · 관리 접속(*SSH, HTTPS 등*)에 대해 확인해야 한다.

② 세션의 잠금 해제는 관리자 인증 또는 사용자 인증을 통해서 가능한지 확인해야 한다.

③ 영상 모니터링 기능에서 일정시간이 경과하고 다른 관리 기능으로 전환을 시도할 때 사용자 인증이 요구되는지 확인해야 한다.

7.2 동시접속 세션 제한

7.2.1

필수

제품은 동일한 관리자 계정 또는 동일 권한으로 제품에 중복 접속하는 것을 허용하지 않아야 한다.

요구항목

① 사용자 로그인 이후 다른 단말기에서 동일 계정으로 로그인을 수행하는 경우 신규 접속을 차단하거나 이전 접속을 종료할 것을 요구한다.

② 동일 권한으로 중복 로그인을 허용하지 않아야 한다.

③ 중복 접속 차단시 감사기록을 생성해야 한다.

참고 사항

① 영상 모니터링 · PTZ 등 카메라 제어 목적으로 접속하는 관리자 계정 및 권한에 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.

점검시 유의사항

① 사용자 계정이 동일 PC 또는 다른 PC에서 동시 접속할 경우, 차단 여부를 확인

해야한다.

② 제품이 지원하는 모든 로컬운용 · 관리 접속(*SSH, HTTPS 등*)에 대해 확인해야 한다.

8. 감사기록

제품은 보안기능 및 관리자의 보안활동과 관련된 사항을 감지, 기록하고 분석하여 대응을 지원해야 한다. 또한 감사기록의 삭제 · 저장 실패 등 무력화에 대응하는 기능을 제공하는지 확인해야 한다.

8.1 감사기록 생성

8.1.1

필수

제품은 주요 감사사건에 대해 감사기록을 생성해야 한다.

요구항목

① 반드시 감사기록을 생성해야 하는 감사사건은 아래 〈표 3〉과 같다.

② 기능 제공시 감사기록을 생성해야 하는 감사사건은 아래 〈표 4〉와 같다.

〈 표 3. 필수 기록되어야 할 주요 감사사건〉

소분류	보안관리	추가적인 감사정보
식별 및 인증	사용자의 로그인, 로그아웃	
	사용자 등록, 변경, 삭제	
	사용자 인증 시도의 한계치 도달시 대응행동	
	패스워드에 대한 모든 변경	
보안관리	〈표 2〉의 보안관리 기능의 수행과 보안속성 값의 모든 변경, 삭제 ※ 다만, 보안관리 기능중 '감사기록 조회' 및 '제품 버전정보 조회' 기능은 제외	변경된 보안속성 데이터
	기본 계정(ID) · 패스워드 변경	

소분류	보안관리	추가적인 감사정보
보안관리	관리용 단말 접속 IP 차단	
세션 관리	사용자의 세션 잠금 또는 세션 종료	
	동일 계정의 중복 로그인 시도 탐지시 대응행동	
	동일세션 수 제한에 기반한 새로운 세션 거부	
암호키 생성	암호 키 생성 실패	
암호 사용	암호 연산 실패(암호 연산 유형 포함)	
감사기록	하드웨어 일체형 제품의 감사기능 시작과 종료	
	제품의 시간 설정 변경	

〈 표 4. 기능 제공시 기록할 수 있는 주요 감사사건〉

소분류	보안관리	추가적인 감사정보
영상 보안	영상 외부 저장 기능 수행	해시 값
	녹화 설정 및 변경	
보안 관리	카메라 제어(PTZ 등) 설정 및 동작	
	관리프로그램의 접속 상태 변화	
자체보호	자체 시험 수행	실패한 보안기능
	제품 자체의 무결성 검사 수행	무결성 검사가 실패한 구성요소
업데이트 보호	관리자에 의한 업데이트 파일 유효성 검증	
	업데이트 파일의 유효성 검증 수행	
감사기록	소프트웨어 제품의 감사기능 시작과 종료	
	감사기록 저장 실패시 대응행동	

점검시 유의사항

① 시험원은 제품의 모든 감사기록 행위를 조사해야 한다.

② 제품 시작시 감사기록이 생성되는 경우(*자체시험 결과, 무결성 검사 등*)에는

'감사기능 시작'을 명시하지 않아도 요구사항을 만족하는 것으로 판정한다.

③ 취약성 시험 등에 의한 제품 강제 종료시 '감사기능 종료'를 기록하지 않아도 요구사항을 만족하는 것으로 판정한다.

8.1.2

필수

감사기록은 필요 이상의 정보가 포함되지 않아야 한다.

요구항목

① 감사기록에 최소한 포함되어야 하는 항목은 다음과 같다.

- 사건 발생일시, 사건 유형, 사건을 발생시킨 주체의 신원(*계정, 프로세스, IP 등*), 사건의 결과(성공 · 실패)

② 인증 정보(*패스워드 등*), 암호키 등의 정보는 감사기록 내에 저장하지 않아야 한다.

8.1.3

필수

제품의 각 구성요소들은 신뢰된 시간 정보를 이용해서 감사기록을 생성해야 한다.

요구항목

① 신뢰된 시간 정보는 NTP 서버나 운영체제에서 제공하는 시간 정보를 이용해야 한다.

점검시 유의사항

① 시험원은 제품에서 사용하는 시간정보, 동기화 설정 방법 등을 조사해야 한다.

- 제품 구성요소간 시간 동기화를 반드시 구현할 것을 요구하지는 않는다.

8.2 감사기록 조회

8.2.1

필수

제품은 인가된 관리자가 감사기록을 조회할 수 있는 기능을 제공해야 한다.

요구항목

① 제품에서 제공하는 보안기능을 통해서만 감사기록을 조회할 수 있어야 한다.

② 제품은 인가된 관리자가 정보를 해석하기에 적합하도록 감사기록을 제공해야 한다.

③ 감사기록에 민감한 데이터(*패스워드, 주민등록번호 등*)는 기록되지 않아야 하지만 기록이 불가피할 경우, 마스킹으로 처리하여 생성해야 한다.

점검시 유의사항

① 제품에서 제공하는 보안기능을 우회하여 외부에서 감사기록을 직접 조회하는 행위를 차단하는지 확인해야 한다.

- 제품 내부 DB에 감사기록을 저장하는 경우, 제품에서 DB에 대한 접근권한을 통제할 수 있어야 한다.

8.2.2

필수

제품은 감사기록 조회시 관리자가 논리 조건을 선택할 수 있고, 여러 조건에 따라 검색 또는 정렬하는 기능을 제공해야 한다.

점검시 유의사항

① 시험원은 제품이 제공하는 감사기록 조회시 설정가능한 논리 조건을 조사하고, 가능한 경우의 수를 모두 고려하여 조건에 따른 검색 · 정렬 기능을 확인 한다.

여 백

8.2.3

조건부 필수

제품은 WAS의 로그에 중요 정보가 포함되지 않도록 구현해야 한다.

조 건	WAS(*Tomcat, JEUS 등*)가 제품 패키지에 포함되는 경우

요구항목

① 제품 내 WAS(*Tomcat, JEUS 등*)가 함께 운용되는 경우 자체 로그를 남기지 않고 제품의 감사기록 저장소에만 로그를 남기도록 개발해야 한다.

② WAS 로그에 패스워드, 암호키 등 중요 정보가 평문으로 남지 않아야 한다.

8.3 감사기록 보호

8.3.1

필수

제품은 감사기록을 삭제 또는 변경할 수 없도록 보호해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT실체에 전송하여 저장하는 기능을 구현해야 한다.

② 인가된 관리자라도 감사기록을 삭제 및 변경할 수 없도록 관련 유저인터페이스(UI) 및 CLI 명령어가 제공되지 않아야 한다.

③ 저장된 감사기록을 보호하기 위해 비인가자의 접근을 통제할 수 있어야 한다.

④ 제품 보안기능으로 완전히 구현 할 수 없는 경우, 제품 운영환경에서 감사증적 저장소를 보호 할 수 있도록 지원할 수 있다.

- 제품과 동일한 운영체제상에 설치된 DBMS에 감사기록이 저장되는 경우 DBMS의 식별 및 인증 기능을 이용, 비인가 사용자의 삭제 또는 변경을 보호할 수 있다.

⑤ 감사기록이 제품 외부의 로그서버에 저장되는 경우 암호통신을 수행해야 한다.

- syslog를 지원하면 *syslog over TLS (RFC 5424), syslog over DTLS (RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.

참고 사항

① 감사기록을 실시간으로 외부 IT실체에 전송하여 저장하는 경우 감사기록 원본은 외부 IT 실체에 저장되는 것으로 본다.

점검시 유의사항

① 하드웨어 일체형 제품은 필수로 제공해야 한다.

② 소프트웨어 제품은 감사기록 삭제 및 변경할 수 있는 UI나 CLI 명령어를 제공하지 않으면 '만족'으로 판정한다.

③ 감사기록이 제품 외부의 로그서버에 저장되는 경우 암호통신 수행을 확인해야 한다.

④ 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 실시간으로 외부 IT 실체에 전송하여 저장하는 경우 만족하는 것으로 간주한다.

8.3.2

선택

제품은 감사기록을 제품 내부에 저장할 경우 암호화하여 저장해야 한다.

요구항목

① 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장방식은 '9. 암호 지원' 요구사항을 만족해야 한다.

8.4 감사기록 손실 예측시 대응 행동

8.4.1

필수

제품은 감사기록의 크기가 미리 정의된 용량에 도달하는 경우 대응행동을 수행해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT 실체에 전송하여 저장하는 기능을 구현해야 한다.

② 관리자에게 통보하는 기능을 필수적으로 제공해야 하며, 기능의 예로써 *화면 알람, 관리자 이메일 발송 등*이 있다.

③ 감사기록 손실 대응관련 관리자에게 통보하는 조건의 예로써 *설정된 디스크 용량 90% 이상, 100MB 이상 등*이 있다.

④ 부가적으로, 관리자가 감사기록을 외부 로그서버로 전송하는 기능을 제공할 수 있다.

- syslog를 지원하면 *syslog over TLS (RFC 5424), syslog over DTLS (RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.
- 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '9. 암호지원' 요구사항을 만족해야 한다.

참고 사항

① 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 실시간으로 외부 IT 실체에 전송하여 저장하는 경우 만족하는 것으로 간주한다.

점검시 유의사항

① 관리자에게 통보하기 위한 조건을 고정값으로 지원하는 것도 가능하다.

8.5 감사기록 손실 방지

8.5.1

필수

제품은 감사기록 저장 용량 포화시 적절한 방법으로 저장 실패에 대응해야 한다.

요구항목

① 감사기록을 로컬 저장소에 저장하거나 실시간으로 외부 IT실체에 전송하여 저장하는 기능을 구현해야 한다.

② 저장 실패 대응 기능의 예로써 *가장 오래된 감사기록 덮어쓰기, 감사기록 압축 저장 등*이 있다.

점검시 유의사항

① 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 실시간으로 외부 IT 실체에 전송 · 저장시 '만족'으로 판정한다.

9. 암호 지원

제품의 데이터 저장 · 전송시 보호를 위해 사용되는 암호화 및 해시 알고리즘은 국가 · 공공기관이 요구하는 보안강도를 만족해야 한다. 또한 암호화를 사용하는 모든 보안기능은 '9. 암호지원'의 요구사항을 만족하도록 구현해야 한다.

9.1 암호사용

9.1.1

필수

중요 정보 전송 및 저장시 권고 암호 알고리즘을 사용해야 한다.

요구항목

① 권고 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘으로 [별표 1]을 참고한다. 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-223, P-224, P-256).*

② 다만, TDES(2 key, 3 key 포함) 사용은 허용하지 않는다.

③ 블록 암호 사용시 평문의 크기가 암호화 블록 크기보다 큰 경우 ECB 모드는 사용하지 않아야한다.

④ 블록 암호 사용시 CFB 또는 OFB 모드에서는 고정된 Ⅳ를 사용하지 않아야 한다.

⑤ 국내 · 외 표준 암호 알고리즘을 사용해야 하며, 국가용 암호알고리즘 사용을 권고한다.

⑥ 보안강도 112 bit 급 이상 암호 알고리즘의 세부 사항은「암호 알고리즘 및 키 길이 이용 안내서」(과학기술정보통신부, 2018),「소프트웨어 암호모듈 검증 기준」,「NIST SP800-131 Ar2」를 참고한다.

점검시 유의사항

① 제출문서(「보안기능 구현명세서」 또는 「보안기능 운용설명서」)를 통해 제품이 보안기능에 적용한 암호화 방식을 확인해야 한다.

② 패스워드는 일방향 해시 알고리즘 또는 양방향 암호 알고리즘을 사용하여 암호화해야 하며, 동일한 평문 입력을 반복하여도 매번 다른 값이 출력되어야 한다.

③ 시험원은 요구사항에 따른 정확한 구현을 시험하기 위해 필요시 개발자를 직접 대면하여 구현내용에 대한 설명을 요청할 수 있다.

9.2 암호키 생성

9.2.1

필수

제품은 암호키를 아래 요구항목을 준수하여 생성해야 한다.

요구항목

① 암호키 생성 방식의 예로써 *패스워드 기반 키 유도(PKCS#5 v2.1(RFC 8018), NIST SP 800-132 등), 사전공유된 키로 키 유도(TTAK.KO-2.0272), 난수발생기 이용 키 생성(CTR_DRBG, HASH_DRBG, HMAC_DRBG 등)*이 있다.

② 난수발생기는 국내 · 외 표준을 준수하여 구현된 것이어야 한다.

③ 난수발생기로 생성한 난수를 이용하여 비대칭키쌍(공개키 · 비공개키)이나 대칭키 생성이 가능하다.

④ 패스워드 기반 키 유도 기능은 키 암호화 키(KEK : Key Encryption Key) 생성에만 사용해야 한다.

- 최초의 키 암호화 키(KEK)는 제품마다 다르게 생성되어야 한다.
- 키 암호화 키(KEK)는 생성에 필요한 초기 데이터(*패스워드 등*)는 직접 입력받거나 스마트카드, 보안USB, 보안토큰(HSM : Hardware Security Module) 등 저장 매체에 저장된 값을 주입하여 사용할 수 있다.
- 저장매체는 보안기능 확인서 또는 국내 · 외 CC인증서를 획득한 제품을 사용할 것을 권고한다.
- 세부 사항은 「암호 키 관리 안내서」(과학기술정보통신부, 2018) 암호키 생성 부분을 참고한다.
- 키 암호화 키(KEK) 생성을 위한 초기 데이터로 패스워드를 사용하는 경우, 제품 최초 설치시 입력된 값을 저장하여 사용할 수 있으며 저장된 데이터는 인가되지 않는 노출시도로부터 보호되어야 한다.

⑤ salt 값은 비밀일 필요는 없으며, 난수발생기를 이용하여 생성하고 크기는 최소 128bit 이상이어야 한다.

⑥ iteration count 는 가능한 큰 값을 적용해야 한다. (최소 1000회 이상)

점검시 유의사항

① 시험원은 제품이 제공하는 암호키 생성 방식(*표준, 난수발생기 등*)을 조사해야 한다.

② 패스워드는 4자리 이상인지 확인한다.

③ 제품에서 외부의 3rd Party Library나 오픈소스를 사용한 경우 사용 소프트웨어 이름, 버전 정보를 확인해야 한다.

④ 제품이 패스워드 기반 키 유도 기능을 구현한 경우, 사용자 인터페이스 확인, 디버깅 시험 등을 통해 확인해야 한다.

9.3 암호키 저장

9.3.1

필수

제품은 암호키를 아래 요구항목을 준수하여 저장해야 한다.

요구항목

① 데이터 암호화 키(DEK)는 암호화 키(KEK : Key Encryption Key)를 사용, 암호화하여 저장 할 수 있다.

② 키 암호화 키(KEK)는 여러 단계의 키 체인을 통해 생성할 수 있으며, 이 중 최종 키 암호화 키(KEK)는 이전 단계의 키 암호화 키(KEK)를 사용, 암호화하여 저장할 수 있다.

③ 키 체인에서 최종 키 암호화 키(KEK)를 제외한 키 암호화 키(KEK)는 저장할 수 없다.

④ 암호키를 제품 외부에 저장할 경우 스마트카드, 보안USB, 보안토큰(HSM) 등 안전성이 확인된 저장 매체를 이용할 것을 권고한다.

- 저장 매체는 보안기능 확인서 또는 국내 · 외 CC인증서를 획득한 제품을 사용할 것을 권고한다.

⑤ 암호키를 제품에 하드코딩하여 저장하는 것은 허용되지 않는다.

⑥ 신청업체는 아래 〈표 6〉와 같이 제품에서 저장 및 전송시 사용하는 모든 암호키를 식별하여 키 저장 및 파기 방법에 대한 목록과 설명자료를 제출하여 안전성을 입증해야 한다.

⑦ 제품 관리를 위한 로컬 · 관리접속 및 별도 장비와 연동설정에 사용되는 암호키(*사전공유키, 대칭키, 개인키 등*)를 제품이 저장하는 경우 *암호화, 접근통제*

*등*의 방식으로 보호하여 저장해야 한다.

〈 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

참고 사항

① 암호키란 제품 관리를 위한 로컬접속 · 관리접속 및 별도 장비와 연동설정에 사용되는 사전공유키, 대칭키, 개인키 등의 키들을 모두 의미한다.

점검시 유의사항

① 시험원은 위 표와 같이 제품에서 사용되는 모든 암호키를 조사하고, 키 저장 및 파기 방법을 확인해야 한다.

② 제품의 데이터 암호화 키는 모두 암호화하여 내부에 저장하는지 확인해야 한다.

③ 제품 내부의 암호키 저장 영역에 비인가자의 접근을 차단하는지 확인해야 한다.

9.4 암호키 파기

9.4.1

필수

제품은 제품에서 생성하거나 사용한 암호키를 파기해야 한다.

요구항목

① △제품 실행 종료시 △암호키 삭제 함수 호출시 △암호통신 종료시 등의 경우 사용기간이 만료된 암호키 및 암호키 관련 정보를 모두 파기해야 한다.

② 암호키 파기시 0 또는 1의 값으로 3회 이상 덮어쓰기하는 방식을 이용할 수 있다.

③ 세부 사항은 「암호 키 관리 안내서」(과학기술정보통신부, 2018) 암호키 파기 방법을 참고한다.

점검시 유의사항

① 시험원은 암호키 및 암호키 관련 정보가 삭제되는 시기와 암호키를 파기하는 메커니즘을 조사해야 한다.

② 암호키 파기시 메모리에 적재(Load)된 암호키를 삭제하는지 확인해야 한다.

10. 취약성 대응

제품은 존재하는 알려진 취약점들을 제거해야 한다.

10.1 소스코드 보안약점 제거

10.1.1

조건부 필수

제품 개발시 소스코드에 보안약점이 존재하지 않도록 시큐어 코딩 규칙을 적용해야 한다.

조 건	소프트웨어 제품인 경우

요구항목

① 소프트웨어 개발 단계에서 보안약점을 최소화하여 구현해야 한다.

② 다음의 표준 · 가이드를 준수할 수 있다.

- 「ISO/IEC TS 17961:2013」, 「JAVA 시큐어코딩 가이드」 (KISA)

③ 신청업체는 자체 수행한 제품 보안약점 제거 결과를 제출, 안전성을 입증해야

한다.

④ 세부 사항은 「소프트웨어 개발보안 가이드」 (행정안전부, 2021.11)를 참고한다.

점검시 유의사항

① 시험원은 신청업체에서 제공한 시큐어코딩 점검 · 보완 결과의 적절성을 확인해야 한다.

② 검증필 제품목록에 등재된 소스코드 보안약점 진단도구를 이용, 제품에 대해 독립적인 보안약점 점검을 수행해야 한다.

③ 모든 제품 구성요소에 대하여 시험을 수행한다.

④ 시험기관이 신청업체로부터 받은 '취약점 개선 보증 서약서' 및 '취약점 개선 내역서'를 제출 받아 검토한 후, 취약성 시험을 생략할 수 있다.

10.2 알려진 취약점 제거

10.2.1

필수

제품 내부에 알려진 보안취약점을 확인하고 제거해야 한다.

요구항목

① 공개영역을 통해 알려진 보안취약점(*CVE, NVD 논문 등*)에 대해 제품에서 사용중인 프로토콜, 라이브러리, 오픈소스 등(*OpenSSL, OpenSSH*)에 해당하는 보안취약점이 존재하는지 확인하고 제거해야 한다.

- 제품에 포함되는 커스터마이즈 운영체제에 취약점이 확인된 낮은 버전의 커널(*Linux® 2.x*)을 사용하지 않는 것을 권고한다.

점검시 유의사항

① 시험원은 제품에서 사용중인 프로토콜, 라이브러리, 오픈소스 등에 대한 이름 및 버전 등을 조사해야 한다.

② 시험원은 조사한 3rd Party 제품(*Boot Loader, Busybox, OpenSSL,*

OpenSSH, Kernel 등)에 대한 취약성 존재 및 최신 패치 적용 유무를 확인하여 패치되지 않을 경우 '불만족'으로 판정한다.

③ 시험원은 조사한 보안취약점 목록을 토대로 침투시험을 실시하여 악용 가능한 취약점이 확인되면 '불만족'으로 판정한다.

④ 시험기관은 취약점 점검 도구 사용의 적절성을 확인하고 시험에 사용해야 한다.

10.3 불필요한 서비스 제거

10.3.1

필수

제품 내부에 불필요한 서비스가 실행중이면 이를 확인하고 제거해야 한다.

요구항목

① 신청업체는 제품이 제공하는 서비스를 식별하여 필요성을 입증해야 한다.

② 제품에서 보안기능 구동에 필요한 필수 서비스와 불필요 서비스를 식별하여 불필요 서비스는 제거하거나 비활성화해야 한다.

점검시 유의사항

① 시험기관이 신청업체로부터 「보안기능 구현명세서」 또는 「보안기능 운용설명서」를 제출받아 필요 · 불필요 서비스의 식별 및 불필요 서비스 제거를 확인한 후 '만족'으로 판정할 수 있다.

끝.

여 백

〈 별 표 1 〉

영상 전송 관련 표준 프로토콜 목록(예시)

프로토콜	동작 형태	비고
ONVIF	HTTPS/TCP HTTP/TCP	- www.onvif.org - IEC 60839-11-31:2016, IEC 62676-2-31:2019 - SOAP 기반의 HTTP/XML 메시지 프로토콜 (IP카메라의 영상 관련 정보 Read/Write) - 영상 전송에 대해 RTP/RTSP 등의 표준 차용
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 7826 - 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

〈 별 표 2 〉

제 · 개정 이력

일 자	주요 변경 내용	문서 버전
2024. 4. 3.	o 영상정보 관리 · 저장제품 보안요구사항 제정	V3.0
2025. 11. 28.	o ‘신원정보기반 생체인식제품 보안요구사항’(제21장) 제정에 따른 번호 변경(제34장 → 제35장)	V3.0