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

1편 국가용 보안요구사항 해설

해설

1장 국가용 보안요구사항 소개

1장
국가용 보안요구사항 소개

1절 개요 및 구성

1. 개요

■ 정의

‘국가용 보안요구사항’(Security Requirement for Government)이란, 국가 · 공공기관에 도입되는 보안기능이 있는 정보통신기기(정보보호시스템 등)가 기본적으로 구현해야 하는 보안기능의 △종류 △구현방식 △강도(强度) 등을 서술한 문서입니다. 국가용 보안요구사항은 ‘보안기능 시험’제도와 ‘국내용 CC인증’제도의 시험기준이며 「국가용 보호프로파일(Protection Profile)」의 기술적 기준입니다.

■ 국가용 보안요구사항의 구성

국가용 보안요구사항은 모든 검증 대상 제품에 공통으로 적용되는 ‘공통보안요구사항’과 제품별로 적용하는 ‘제품 보안요구사항’으로 구분됩니다. 공통보안요구사항은 ‘서버’, ‘엔드포인트’ 등 2종이며, 제품 보안요구사항은 ‘침입차단시스템’, ‘안티바이러스제품’, ‘스위치 · 라우터’, ‘랜섬웨어 대응제품’, ‘양자키관리장비’, ‘양자통신암호화장비’ 등 34종으로 구성되어 있습니다. (별지 1)

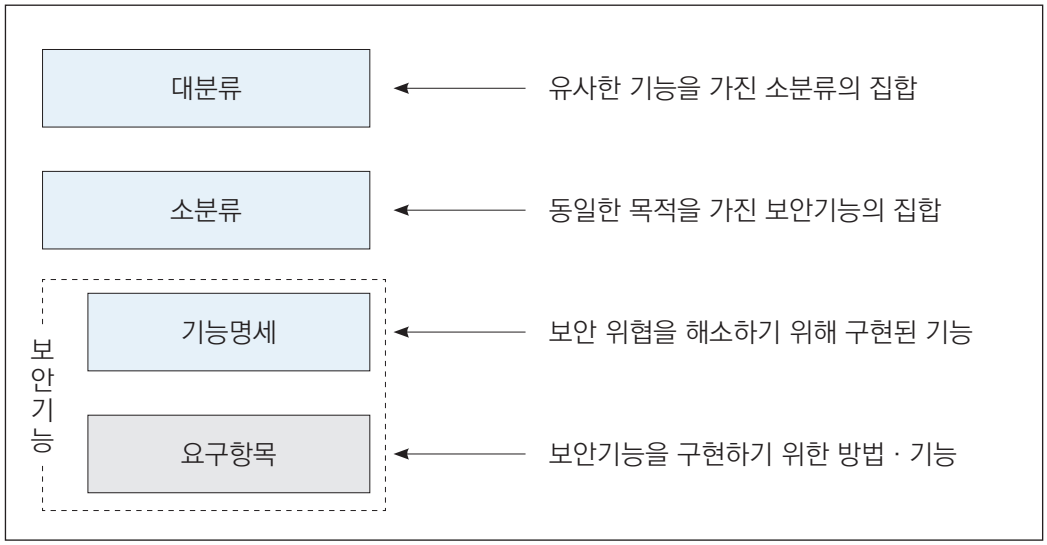
국가용 보안요구사항이 작성된 제품은 대부분 ‘보안기능 확인서’ 또는 ‘CC인증’ 등의 도입요건이 지정되어 있습니다. 그러나, 패스워드 관리제품 등과 같이 일정한 도입요건이 지정되지 않은 제품 유형도 있습니다.

2. 구조 및 기술(記述) 방식

■ 구조

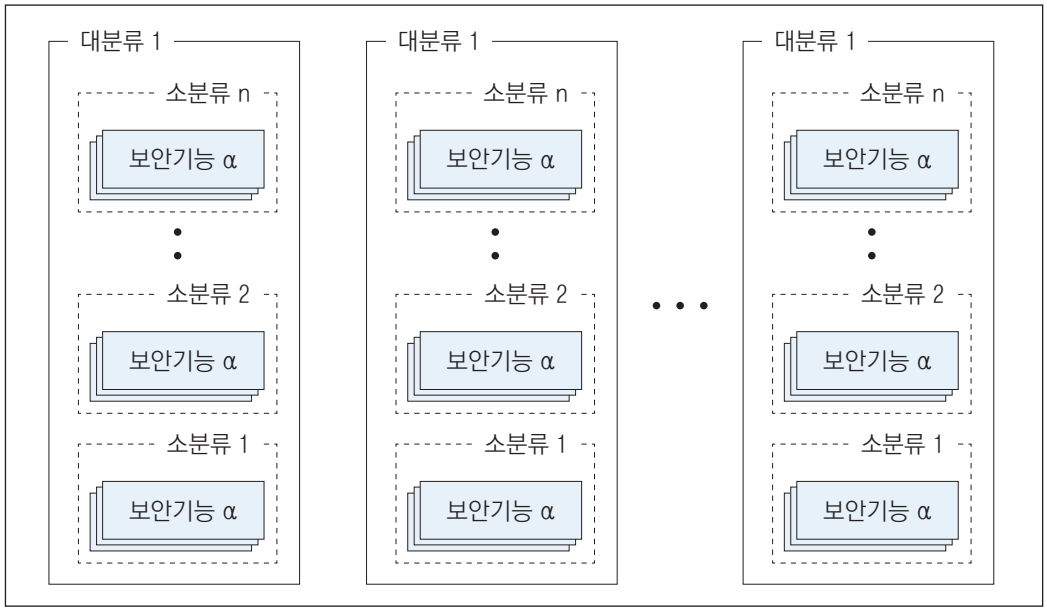
아래 〈그림 1〉과 같이 국가용 보안요구사항(공통 또는 제품 보안요구사항)은 동일한 목적의 보안기능으로 구성된 소분류와 유사한 목적의 소분류가 모인 대분류로 구성됩니다.

〈 그림 1. 국가용 보안요구사항의 세부 구조 〉



그리고 아래 〈그림 2〉와 같이 여러 개의 대분류 항목이 모여 전체 보안요구사항을 구성합니다.

〈 그림 2. 국가용 보안요구사항의 전체 구조 〉



공통보안요구사항은 ‘가정사항’, ‘제품 보안요구사항의 적용’, 각 대분류 등의 순서대로 기재되고, 제품 보안요구사항은 ‘가정사항’, ‘제품개요’, ‘운용환경’, ‘공통보안요구사항의 적용’, 각 대분류 등의 순서대로 기재됩니다.

■ 가정사항

제품이 운용되는 환경, 조건 등을 사전에 전제

○ ‘서버 공통보안요구사항’의 적용 대상이 되는 제품(또는 구성요소)은 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 설치 및 운용된다.

– 중 략 –

■ 제품 보안요구사항의 적용

‘서버 공통보안요구사항’이 적용되는 제품은 하드웨어 일체형 또는 소프트웨어 등 다양한 형태로 구현될 수 있다.

– 중 략 –

보안요구사항의 적용시 기준과 유의사항

1. 식별 및 인증 ← 대분류

■ 1.1 사용자 등 식별 및 인증 ← 소분류

1.1.2 ← 기능명세

필수 

에이전트 또는 클라이언트는 서버 · 업데이트 서버 주소에 대한 무결성 확인 기능을 제공해야 한다.

요구항목

② 사용자가 제품의 정당한 사용자임을 확인하기 위해 반드시 식별 및 인증을 수행해야 한다.

■ 보안기능의 구현 강도(强度) 중요

각 보안기능의 구현 강도는 중요도에 따라 ‘필수’, ‘조건부 필수’, ‘선택’으로 구분되며 개발업체의 구현을 지원하기 위한 ‘요구항목’이 함께 기술되어 있습니다.

○ 필수

‘필수’란, 예외나 재량없이 구현되어 만족해야 하는 보안기능을 의미합니다. 이 항목은 ‘작동가능한 상태(On)’로 구현되어 도입기관에 납품되야 하며 On · Off

(Enable · Disable)가 가능하다고 명시된 경우를 제외하고 관리자가 중지(Off 또는 Disable)할 수 있도록 구현할 수 없습니다.[1] 국가용 보안요구사항 전체 문서에서 필수 항목은 다음과 같이 표기됩니다.

〈 표기 예 〉 필수 항목의 표기

6.1.2	
필수 	**에이전트 또는 클라이언트는 서버 · 업데이트 서버 주소에 대한 무결성 확인 기능을 제공해야 한다.**

○ **조건부 필수**

'조건부 필수'란, 기재된 조건에 해당될 때 제품에서 예외나 재량없이 구현되어 만족되어야 하는 보안기능을 의미합니다. 국가용 보안요구사항 전체 문서에서 조건부 필수 항목은 다음과 같이 표기됩니다.

〈 표기 예 〉 조건부 필수 항목의 표기

6.1.2	
조건부 필수 	**에이전트 또는 클라이언트는 서버 · 업데이트 서버 주소에 대한 무결성 확인 기능을 제공해야 한다.**
조 건	에이전트가 설치된 경우

○ **선택**

'선택'이란, 개발자의 재량에 따라 구현 여부를 결정할 수 있는 보안기능을 의미합니다. 국가용 보안요구사항 전체 문서에서 선택 항목은 다음과 같이 표기됩니다.

〈 표기 예 〉 선택 항목의 표기

6.1.2	
선택 	**에이전트 또는 클라이언트는 서버 · 업데이트 서버 주소에 대한 무결성 확인 기능을 제공해야 한다.**

1) 다만, 가상화 환경에서 설치 · 운용되거나 국가용 · 일반 보안요구사항이 복합 적용된 경우 등 예외가 필요한 경우, 검증 · 정책기관과 협의하여 조정 할 수 있습니다.

■ 열거와 예시 중요

보안기능 또는 요구항목은 해당 보안기능의 구현에 필요한 하나 이상의 세부요소가 있으며 중요도에 따라 '열거' 또는 '예시'라는 방식으로 기술될 수 있습니다.

○ 열거

열거는 보안기능 구현시 반드시 포함되어야 하는 세부요소로써 기재된 내용 그대로 배제하거나 생략하지 않고 구현되어야 합니다. 국가용 보안요구사항의 전체 문서에서 열거 항목은 다음과 같이 표기됩니다.

〈 표기 예 〉 열거 항목의 표기

> ① 에이전트에 대한 조회 필수 정보는 다음과 같다.
>
> - 에이전트 버전, 에이전트에 적용된 보안정책, 에이전트 동작상태(활성화 · 비활성화), 에이전트 무결성 검증결과(성공 · 실패).

○ 예시

예시는 요구사항에 만족하도록 구현하기 위해 하나 이상의 선택이 필요한 항목을 나열한 방식입니다. 개발자는 내용에 '등'이 포함된 경우 예시된 항목을 선택하지 않고 자체적으로 요구사항을 만족하는 기능을 구현할 수 있습니다. 다만, 가급적 예시된 항목을 포함할 것을 권고합니다.

예시는 *밑줄 그은 기울임체*로 구별되며 국가용 보안요구사항의 전체 문서에서 예시 항목은 다음과 같이 표기됩니다.

〈 표기 예 〉 예시 항목의 표기

> ① 권고 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘으로 [별첨]을 참고하며, 예는 다음과 같다.
>
> - *해시 : SHA-224 이상.*
> - *대칭키 암호 : 키 길이 128bit 이상.*
> - *공개키 암호 : RSA 2048 이상, DSA(2048, 224) 이상.*
> - *전자서명 : RSA-PSS 2048 이상, KCDSA (2048, 224) 이상 등*

■ 해석

개발 업체 · 시험기관 등은 대상 제품에 대한 시험(평가)에 필요할 경우, 국가용 보안요구사항에 대한 해석을 요청할 수 있습니다. 국가용 보안요구사항은 △명시성 우선 △근시점(近時點) 해석 우선 △일관성 유지 △추측 · 예단(豫斷) · 확대 해석 금지 △접근성 보장 · 유지 등 5가지 원칙에 따라 해석됩니다.

○ **'명시성 우선' 원칙**

국가용 보안요구사항 배포 문서(1, 2, 3편)에 기재된 사항이 우선으로 적용됩니다. 특정 기능 · 구현방법 등에 대한 허용 또는 불허가 명시적으로 기재된 경우, 해당 기재내용이 우선적으로 해석에 반영됩니다.

○ **'근시점(近時點) 해석 우선' 원칙**

보안기술 발전 · 시험(평가)방법의 변화 등의 '변경사유'가 발생할 경우, 특정 보안기능[2]에 대한 해석이 달라질 수 있습니다. 특정 보안기능에 대해 다른 해석이 있을 경우, 가장 최근의 해석이 우선이며 유일한 해석입니다.

○ **'일관성 유지' 원칙**

국가용 보안요구사항의 해석은 △검증(인증)기관 △시험(평가)기관 등에 의해 기록되어야 하며 기록된 해석은 새로운 해석이 있기 전까지 일부 또는 전부가 변경 · 삭제되서는 안됩니다.

○ **'추측 · 예단(豫斷) · 확대 해석 금지' 원칙**

특정 보안기능에 대한 해석은 기록된 내용에 국한되며, 기록되지 않은 사항에 대해 어떠한 영향도 미치지 않습니다. 특정 해석을 토대로 다른 보안기능에 대한 해석을 추측하거나, 예단(豫斷)하거나 확대 해석하여 도출할 수 없습니다.

○ **'접근성 보장 · 유지' 원칙**

'접근성'이란, 국가용 보안요구사항의 해석이 필요한 경우 검증(인증)기관 · 시험기관을 통해 해석을 요청하고 이에 대한 답변을 받을 수 있음을 의미합니다. 이 원칙은 보장 · 유지되어야 하며 검증(인증)기관 · 시험기관 임의로 변경될 수 없습니다.

---

2) '보안기능'이란, '기능명세'(보안 위협을 해소하기 위해 구현된 기능)와 '요구항목'(보안기능을 구현하기 위한 방법 · 기능)의 집합입니다.

3. 일반 보안요구사항 중요

■ 정의

'일반 보안요구사항'이란, '보안기능 시험'을 신청한 제품중에서 적용 가능한 국가용 보안요구사항이 제정되지 않았거나 제품의 보안기능이 현행 국가용 보안요구사항과 현저히 다를 경우, 개발업체 등이 해당 제품의 시험을 위해 제품 또는 기능단위로 작성하는 보안요구사항입니다.

■ 일반 보안요구사항의 검토

일반 보안요구사항은 개발업체, 시험기관, 관련 전문가 등 누구나 작성할 수 있습니다. 작성자는 '보안기능 시험' 제도의 시험기관을 통해 대상 제품의 시험에 적용할 것을 제안할 수 있습니다. 제안된 일반 보안요구사항은 시험기관 등의 검토를 거쳐 해당 제품의 시험에 적용할 수 있습니다.

■ 작성 원칙

일반 보안요구사항은 기존 국가용 보안요구사항으로 정의되지 않은 신종 제품(기능)에 대해 작성되는 경우가 많습니다. 일반 보안요구사항 작성시 국가용 보안요구사항과 상충되지 않도록 다음의 3가지 작성 원칙을 준수해야 합니다.

○ **'명확성 유지' 원칙**

제품 단위의 경우, 구현된 보안기능과 일치하도록 명확하게 기재해야 하며, 하나 이상의 제품을 포함할 수 없습니다. 기능 단위로 작성되는 경우, 해당 기능의 보안 목적과 보호대상을 명확히 기재해야 합니다.

○ **'종속성 최소화' 원칙**

일반 보안요구사항을 구성하는 각 구성요소(대분류 · 소분류 · 보안기능)간의 상호 관계는 독립적이어야 하며, 특정 구성요소가 다른 구성요소를 전제하지 않는 이상 구성요소간 종속성 부여는 가급적 배제해야 합니다.

○ **'중복성 배제' 원칙**

일반 보안요구사항에 규정된 제품 유형 · 구성요소는 국가용 보안요구사항의 기존 제품 유형 또는 해당 일반 보안요구사항의 다른 구성요소와 중복되어서는 안됩니다.

4. 국가용 보안요구사항의 준수 및 적용 중요

■ 준수 수준

보안기능 시험 · 국내용 CC인증 대상 제품은 국가용 보안요구사항의 보안기능 항목 중 필수로 요구되는 항목은 기본적으로 만족해야 하며 추가로 보안기능을 구현할 수 있습니다. 이는 「정보보호시스템 공통평가기준」v3.1 개정 5판의 1부에 정의된 ▲정확한 준수(Exact Conformance) ▲엄격한 준수(Strict Conformance) ▲입증가능한 준수(Demonstrable Conformance)중에서 '엄격한 준수(Strict Conformance)'에 해당됩니다.

우리나라 국가 · 공공기관에 대한 사이버 위협에 대응하기 위해 제품에 추가적인 보안기능을 구현하여 보안성을 제고할 것을 적극 권고합니다.

■ 가정사항의 준수

가정사항이란 제품의 운용과 관련 개발업체와 도입 기관의 개발 및 운영환경 등에 대해 사전 전제된 조건을 의미합니다. 국가용 보안요구사항의 모든 항목은 가정사항에 기재된 내용을 전제로 하기 때문에 내용과 다른 조건 · 환경에서 운용될 경우, 검증의 유효성은 보장되지 않습니다. 따라서 개발업체는 가정사항을 유의하여 제품을 개발해야 하며, 도입기관은 가정사항을 준수하여 운용해야 합니다.

■ 국가용 보안요구사항의 복합 적용

시험자(평가자)는 제품에 구현된 보안기능이 모두 시험 · 평가 될 수 있도록 공통 보안요구사항과 제품 보안요구사항을 모두 적용해야 합니다.(〈그림 3, 4〉 참조)

또한, 제품에 구현된 보안기능 중에서 해당 제품의 보안요구사항에 규정되지 않은 보안기능에 대해서는 공통보안요구사항의 적용 원칙아래 타 제품 보안요구사항 전체 또는 일부를 적용할 수 있습니다.

이때 각 보안기능 요구사항은 독립적으로 적용할 수 있으나 종속관계로 묶여진 보안기능이 있다면 함께 적용되어야 합니다. 이를 '복합 적용'이라 합니다. 국가용 보안요구사항간 또는 국가용 보안요구사항과 일반 보안요구사항간 복합 적용시 다음의 3가지 원칙을 준수해야 합니다.

○ ‘국가용 보안요구사항 우선 적용’ 원칙

‘적용하지 않는다’고 명시한 경우를 제외하고 국가용 보안요구사항을 우선 적용합니다. 제품 단위로는 공통 보안요구사항을 적용해야하며, 기능 단위로는 국가용 보안요구사항에 정의된 동일 기능을 우선 식별하여 적용해야 합니다.

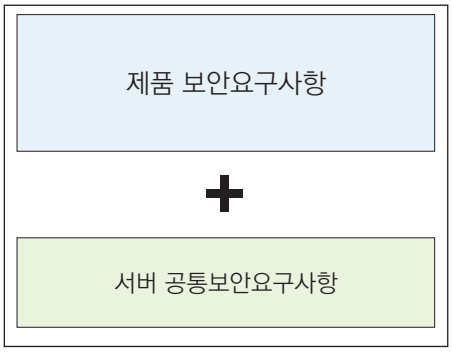
○ ‘제품 유형의 다양성 유지’ 원칙

복합 적용시 제품 유형의 다양성이 충분히 유지되어야 합니다. 국가용 · 일반 보안요구사항의 복합 적용 취지는 대상 제품(특히 신종 제품)이 국가용 보안요구사항 만족 여부 확인을 위한 **시험(평가) 과정에서 당초의 개발목적 · 유형 · 용도 등의 변형 가능성을 최소화**하여 국가 · 공공기관 도입 제품의 다양성을 유지하기 위함입니다.

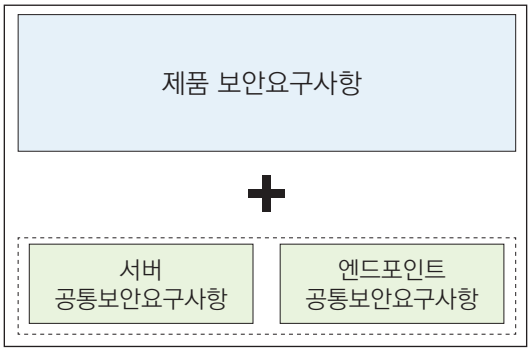
○ ‘중복 적용 배제’ 원칙

기능 단위 복합 적용시 동일한 기능에 대해 중복 적용을 배제해야 합니다. 국가용 보안요구사항과 일반 보안요구사항 복합 적용시 중복될 경우, ‘국가용 보안요구사항 우선 원칙‘에 따라 국가용 보안요구사항의 보안기능이 우선 적용되야 합니다.

〈 그림 3. 공통보안요구사항과 제품 보안요구사항의 적용〉

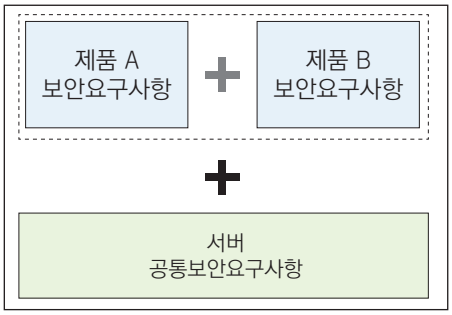


(예시 1) 서버 공통보안요구사항의 단독 적용

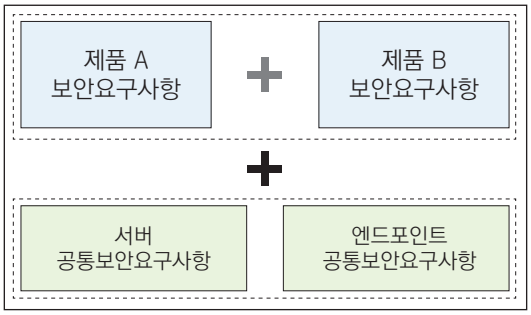


(예시 2) 서버 · 엔드포인트 공통보안요구사항을 함께 적용하는 경우

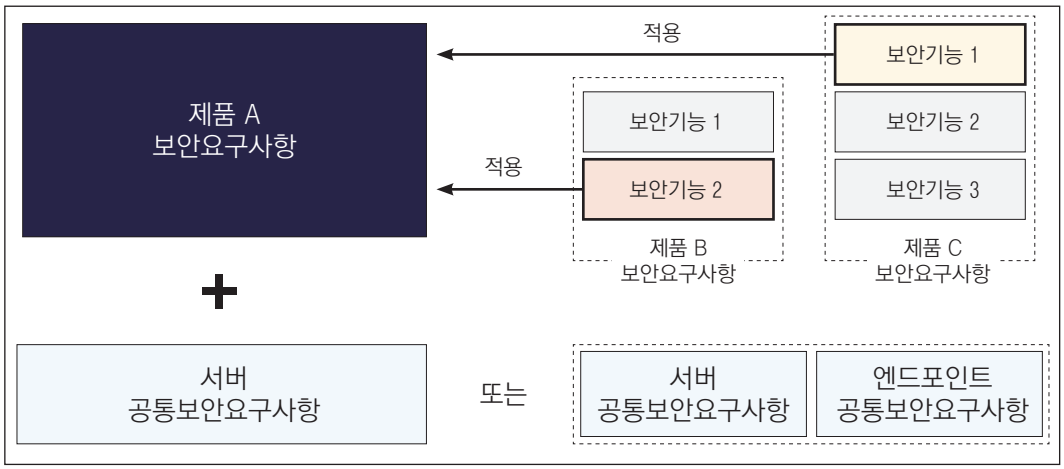
〈 그림 4. 서로 다른 제품 보안요구사항간의 복합적용〉



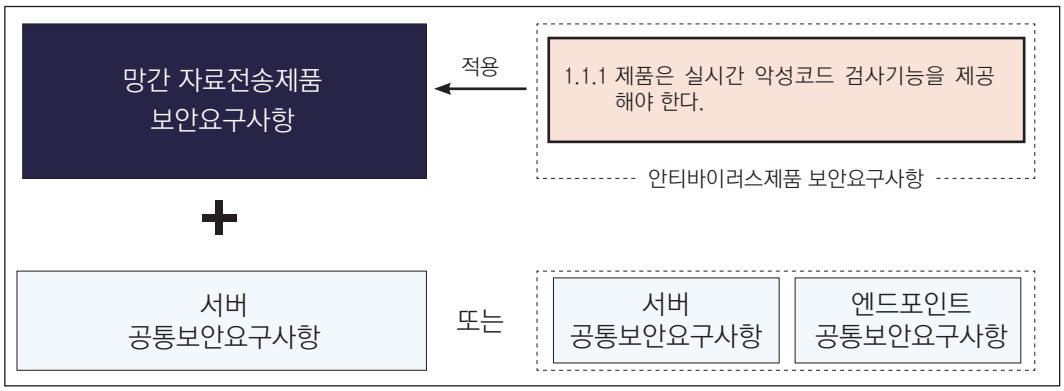
(예시 1) 서로 다른 제품 보안요구사항을 함께 적용



(예시 2) 공통보안요구사항과 서로 다른 제품 보안요구사항을 함께 적용



(예시 3) 제품 보안요구사항과 타 제품 보안요구사항의 일부 기능요구사항을 복합 적용



(예시 4) 악성코드 탐지기능이 구현된 망간 자료전송 제품에 대한 복합적용

○ 국가용 보안요구사항과 일반 보안요구사항의 복합 적용

일반 보안요구사항은 국가용 보안요구사항과 함께 적용됩니다. 공통보안요구사항의 필수 적용 전제아래 제품 또는 기능별 국가용 보안요구사항을 추가적으로 복합 적용할 수 있습니다. 〈그림 5〉를 참고하십시오.

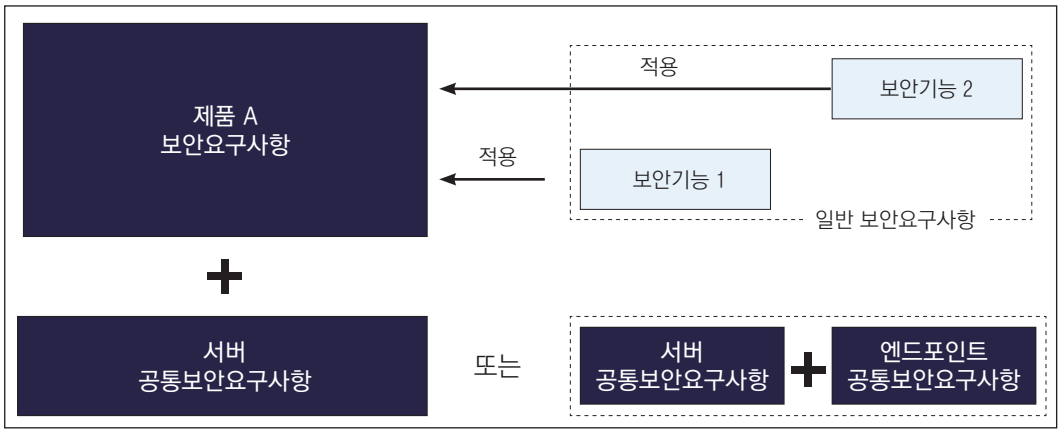
〈 그림 5. 공통 보안요구사항과 제품별 일반 보안요구사항의 복합적용 〉

(예시 1) 공통보안요구사항과 일반 보안요구사항의 복합 적용

(예시 2) 공통보안요구사항과 일반 보안요구사항의 복합 적용

기존 제품 유형과 다른 신종 제품이거나 새로운 기능이 구현된 제품의 시험을 위해 국가용 · 일반 보안요구사항을 복합 적용할 수 있습니다. 〈그림 6〉을 참고하십시오.

〈 그림 6. 제품 보안요구사항과 기능 단위 일반 보안요구사항의 복합 적용 〉

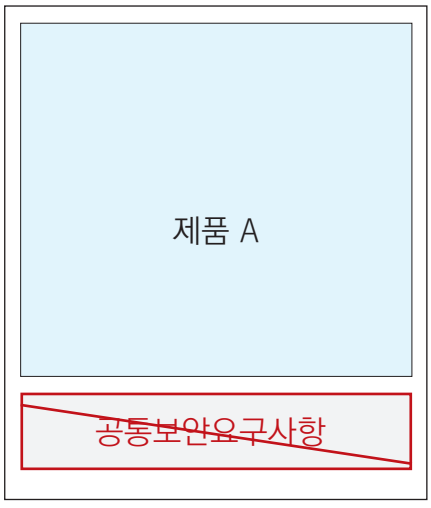


(예시) 제품 보안요구사항에 기능 단위로 작성된 일반 보안요구사항을 복합 적용

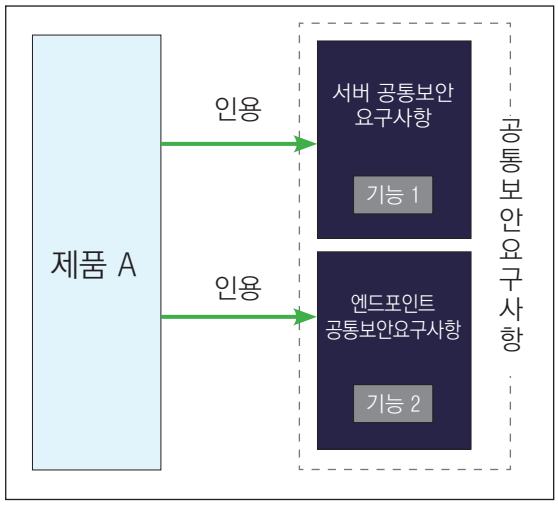
○ 공통보안요구사항 적용의 예외

보안기능의 특성상, 공통보안요구사항이 불필요한 제품 유형은 적용하지 않습니다. △패스워드 관리제품 △소스코드 보안약점 분석도구 △네트워크 장비 제품군(3종)이 대표적입니다. 또한, 일부 가상화 제품 유형도 특성에 따라 공통보안요구사항을 적용하지 않을 수 있습니다. 〈그림 7〉을 참고하십시오.

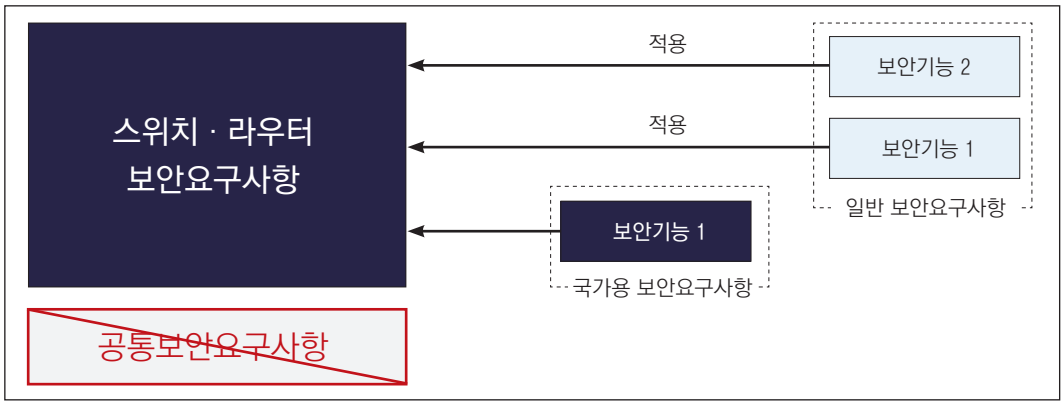
〈 그림 7. 공통보안요구사항 적용의 예외 〉



(예시 1) 공통보안요구사항 미적용



(예시 2) 공통보안요구사항 일부 인용



(예시 3) 추가 기능이 구현된 스위치 · 라우터에 대한 국가용 · 일반 보안요구사항의 복합 적용

다만, 공통보안요구사항을 적용하지 않더라도 보안기능 요구 수준의 일관성을 유지하기 위해서 공통보안요구사항 중 패스워드 생성기준 · 암호 관련 기준 등 일부 요구사항을 인용, 준수를 요구할 수 있습니다.

그리고, 국가용 · 일반 보안요구사항간의 복합 적용 원칙은 동일하게 적용됩니다.

입증

대상 제품의 국가용 보안요구사항 만족여부를 입증하기 위해 '보안기능 시험' 제도와 '국내용 CC인증' 제도를 통한 제출물 검토와 절차에 따른 시험이 필요합니다.

'보안기능 시험' 제도는 「보안기능 구현명세서」 등의 문서가 필요하며 국내용 CC인증 제도는 「보안목표명세서」 등의 문서가 필요합니다. 각 제도에서 요구되는 제출물에 대한 상세한 사항은 「보안기능 확인서 발급절차 안내」 또는 「정보보호 제품 평가 · 인증 수행규정」을 참고하시기 바랍니다.

다만, '보안기능 시험' 제도의 경우, 제품의 국가용 보안요구사항 만족 여부 입증 및 안보상 위해 여부 확인을 위해 추가적인 시험이 필요할 수 있습니다.

5. 국가용 보안요구사항 배포문서의 구성

■ 전체 구성

국가용 보안요구사항은 총 3편으로 구성되었으며 배포용 문서는 총 9개의 PDF 파일로 제작되어 배포됩니다. 배포되는 파일은 다음 〈표 1〉과 같습니다.

국가정보원은 인터넷을 통해 배포 · 공유되는 국가용 보안요구사항 파일의 위 · 변조 여부를 손쉽게 식별할 수 있도록 모든 배포파일의 고유 식별정보(Hash-256 또는 Hash-512)를 홈페이지에 공개하고 있습니다. 2024. 4. 1.

〈 표 1. 국가용 보안요구사항 배포문서 구성 〉

연번	제품군	보안요구사항 명칭	파일 명칭
1	공통	서버 공통보안요구사항	(1,2편) 해설 및 공통 보안 요구사항.pdf
2		엔드포인트 공통보안요구사항	
3	침입차단 제품군	침입차단시스템 보안요구사항	(3편) 침입차단 제품군.pdf
4		웹 방화벽 보안요구사항	
5		DDoS 대응장비 보안요구사항	
6		인터넷전화 보안제품 보안요구사항	
7	침입방지 제품군	침입방지시스템 보안요구사항	(3편) 침입방지 제품군.pdf
8		무선 침입방지시스템 보안요구사항	
9	구간보안 제품군	망간자료전송제품 보안요구사항	(3편) 구간보안 제품군.pdf
10		무선랜 인증제품 보안요구사항	
11		망간자료전송제품 보안요구사항	
12		무선랜 인증제품 보안요구사항	
13	전송자료보안 제품군	스팸메일차단시스템 보안요구사항	(3편) 전송자료보안 제품군.pdf
14		소프트웨어 기반 보안USB제품 보안요구사항	
15		호스트 자료유출방지제품 보안요구사항	
16		네트워크 자료유출방지제품 보안요구사항	
17	보안관리 제품군	통합보안관리제품 보안요구사항	(3편) 보안관리 제품군.pdf
18		소스코드 보안약점 분석도구 보안요구사항	

19	보안관리 제품군	패치관리시스템 보안요구사항	(3편) 보안관리 제품군.pdf
20		데이터베이스 접근통제제품 보안요구사항	
21		시스템 접근관리제품 보안요구사항	
22		패스워드관리제품 보안요구사항	
23	가상화제품군	가상화관리제품 보안요구사항	(3편) 가상화 제품군.pdf
24	엔드포인트 보안 제품군	안티바이러스제품 보안요구사항	(3편) 엔드포인트보안 제품군.pdf
25		스마트폰 보안관리제품 보안요구사항	
26		iOS · iPadOS 모바일 단말 보안관리제품 보안요구사항	
27		운영체제(서버) 접근통제제품 보안요구사항	
28		랜섬웨어 대응제품 보안요구사항	
29	네트워크 장비	스위치 · 라우터 보안요구사항	(3편) 네트워크 장비.pdf
30		SDN 컨트롤러 보안요구사항	
31		SDN 스위치 보안요구사항	
32	양자암호통신 장비 제품군	양자키관리장비 보안요구사항	(3편) 양자암호통신 장비.pdf
33		양자키분배장비 보안요구사항	
34		양자통신암호화장비 보안요구사항	
35	영상정보처리 기기 제품군	IP카메라 보안요구사항 2024. 4. 3.	(3편) 영상정보처리 기기 제품군.pdf
36		영상정보 관리 · 저장 제품 2024. 4. 3.	

6. 국가용 보안요구사항에 대한 문의

■ 문의처

개발 업체 및 관련 전문가 등 누구나 국가용 보안요구사항에 대한 문의사항이 있을 경우, 아래 〈표 2〉에 기재된 시험 · 평가기관을 통해 문의해 주시길 바랍니다.

별도로 요구되는 서식은 없으며 이메일을 통해 자유롭게 질의하실 수 있습니다.

〈 표 2. 시험 · 평가기관 문의처 〉 (기관명 가나다 순)

지정된 제도	기관명	이메일	제품 유형
보안기능 시험 제도 CC 인증 제도	한국기계전기전자 시험연구원 (KTC)	jhbang@ktc.re.kr	정보보호시스템 네트워크 장비

보안기능 시험 제도 CC 인증 제도	한국시스템보증 (KoSyAs)	info@kosyas.com	정보보호시스템 네트워크 장비
보안기능 시험 제도 CC 인증 제도	한국아이티평가원 (KSEL)	cc@ksel.co.kr	정보보호시스템 네트워크 장비
보안기능 시험 제도	한국전자통신연구원 ICT시험연구센터 (ETRI)	wideideal@etri.re.kr	네트워크 장비
보안기능 시험 제도 CC 인증 제도	한국정보보안기술원 (KOIST)	koist@koist.kr	정보보호시스템 네트워크 장비
보안기능 시험 제도 CC 인증 제도	한국정보통신기술협회 디지털정보보호단 (TTA)	보안기능 시험 : sc_info@tta.or.kr CC인증 : cc_info@tta.or.kr	정보보호시스템 네트워크 장비
보안기능 시험 제도	한국정보통신기술협회 방송통신인프라단 (TTA)	networker@tta.or.kr	네트워크 장비
보안기능 시험 제도	한국정보통신기술협회 공공안전서비스단 (TTA)	cctv@tta.or.kr	영상정보처리 기기
보안기능 시험 제도 CC 인증 제도	한국화학융합시험연구원	sw@ktr.or.kr	정보보호시스템 네트워크 장비

7. 용어 정의

■ 공통보안요구사항

용어	정의 내용
제품	상호작용하는 하나 이상의 보안기능이 소프트웨어 · 펌웨어 · 하드웨어로 구현된 IT실체를 의미한다.
사용자	관리자와 일반사용자를 모두 포함한 제품에 접속할 수 있는 권한을 가진 실체를 의미한다.

인증 정보	패스워드, 쿠키, 세션 정보 등 인증을 위해 사용되는 모든 정보를 의미한다.
관리자	제품의 보안기능을 구동 · 중지 · 재시작하거나 주어진 권한을 사용하여 보안정책을 추가 · 변경 · 조회 · 삭제하는 등 제품을 운용 및 관리하는 사용자를 의미한다.
일반사용자	관리자가 설정한 보안정책에 따라 제품의 보안기능을 이용할 수 있는 사용자를 의미한다. 제품 유형에 따라 제품에 포함된 에이전트 또는 클라이언트를 사용할 수 있다.
외부 IT실체	제품과 상호작용하는 IT실체를 의미한다. (제품이 제공하는 보안기능을 사용하는 것을 허용하기 이전에 제품에서 외부 IT실체를 인증하거나, 외부 IT실체가 제공하는 보안기능을 사용하기 이전에 외부 IT실체로부터 제품을 인증받아야 할 수 있다.)
필수	제품에서 예외나 재량없이 구현되어 만족해야 하는 보안기능을 의미한다.
조건부 필수	기재된 조건에 해당될 때 제품에서 예외나 재량없이 구현되어 만족해야 하는 보안기능을 의미한다.
선택	개발자의 재량에 따라 구현할 수 있는 보안기능을 의미한다.
물리적으로 안전한 장소	제품의 설치 또는 운용을 위해 칸막이 등으로 분리되고 잠금장치 등을 활용하여 비인가자의 출입이 제한되거나 금지된 장소를 의미한다.
원격관리	제품이 설치된 기관의 네트워크 내에서 제품 관리를 위해 관리자와 제품간에 설정(established)된 통신을 의미한다.
관리접속	HTTPS, SSH, TLS 등을 이용하여 설정(established)된 원격관리를 의미한다.
로컬접속	관리자와 제품간에 콘솔포트를 통해 설정(established)된 연결을 의미한다.
클라이언트	사용자의 호스트에 설치되어 사용자를 대신하여 서버와의 통신을 요청하는 역할을 수행하는 실체를 의미한다. (해당 제품 유형에는 가상사설망 제품 등이 있다.)
서버	제품의 보안관리, 감사기록, 사용자 식별 및 인증, 에이전트 관리(에이전트가 포함된 제품의 경우), 클라이언트 요청(클라이언트가 포함된 제품의 경우) 등을 중앙에서 처리하는 역할을 수행하는 실체를 의미한다. 제품이 다수의 소프트웨어를 포함하여 구현된 경우 관리서버, 관리콘솔 등과 같은 형태의 별도의 소프트웨어를 포함할 수도 있고, 하드웨어 일체형 제품으로 구현된 제품인 경우 하드웨어 일체형 제품 내에 포함된 기능으로 존재할 수도 있다. 이하 '서버'로 표기한 경우 '서버 역할을 수행하는 제품 구성요소'를 의미한다. * 제품의 일부로 포함되는 '서버'와 별개로 '인증서버', '로그서버', '업데이트 서버', '웹서버', 'WAS서버' 등과 같은 외부의 서버를 칭하는 용어를 사용하고 있으므로 유의한다.

자동복구	사용자가 개입하지 않은 복구행위를 의미한다.
수동복구	사용자가 실행하거나 사용자 개입에 의한 업데이트 서버 등을 통한 복구를 의미한다.
엔드포인트	더 이상의 하위 연동 실체가 없이 에이전트, 클라이언트 등의 제품 구성요소가 설치되어 운용되는 지점을 의미한다.
유효성	제품에 구현된 보안기능이 요구에 따른 보안 동작 및 위협차단에 대한 판단을 의미한다. (유효성은 파일 또는 데이터가 원본과 동일(예 : 업데이트 파일 유효성) 함을 판단하거나 파일 또는 데이터의 효력이 유효(예 : 인증서 유효성) 함을 판단하는 의미로 사용될 수 있다.)
에이전트	보안의 대상인 IT실체에 설치되어 서버로부터 보안정책을 전달받아서 사용자의 호스트에 적용하는 역할을 수행하는 실체를 의미한다. (에이전트를 포함할 수 있는 제품 유형에는 안티바이러스 제품, 소프트웨어 기반 보안USB 제품, 네트워크 접근통제 제품, 스마트폰 보안관리 제품, 운영체제(서버) 접근통제 제품, 통합보안관리 제품, 패치관리시스템 등이 있다.)

■ 침입차단시스템

용어	정의 내용
패킷 필터링	IP, 포트 번호를 이용해 패킷을 허용하거나 차단하는 기능을 의미한다.
상태기반 패킷 검사	OSI 3~4계층으로 동작하며, 패킷 필터링 및 TCP 연결에 관한 정보(세션 정보)를 이용해 패킷을 허용하거나 차단하는 기능으로 TCP 헤더에 포함된 특정 값들을 검사하기 때문에 가변적인 포트를 사용하는 서비스 처리 가능하다.
어플리케이션 검사	OSI 7 계층까지 검사하여 패킷을 허용하거나 차단하는 기능. 각 서비스 별로 프록시 데몬(백그라운드 프로세스)이 존재하여 일명 응용프로그램 게이트웨이라고 부르기도 한다. 구현 방식에 따라 프록시 서버는 1개만 사용하고 에이전트를 제공하는 제품도 있다.

■ 웹 방화벽

용어	정의 내용
비정상적인 웹 요청	HTTP 프로토콜에 정의된 정상적인 형태의 웹 요청 패킷이 아니라 악의적인 의도로 작성되어 유입되는 패킷을 총칭한다.
웹 콘텐츠	웹을 통해 전달될 수 있는 전자문서와 멀티미디어 콘텐츠를 의미한다. 전자문서는 웹 문서 파일, 그림 파일 등이 있으며, 멀티미디어 콘텐츠는 애니메이션, 동영상 등이 있다.

웹 서버	HTTP 프로토콜을 통해 클라이언트(웹 브라우저)의 요청 정보를 받아 처리하고 그 결과를 다시 클라이언트에 보내는 소프트웨어를 의미한다. (클라이언트가 요청하는 자원을 URL(Uniform Resource Locator) 형태로 받아 내부 파일 시스템과 매핑하여 처리하거나, URL과 입력 값(예 : 로그인 화면의 아이디, 패스워드 등)을 함께 받으면 사전에 약속된 처리를 한 후 그 결과를 클라이언트에 전달한다.)
웹 응용프로그램	인터넷 또는 인트라넷과 같은 네트워크를 통해 액세스되는 응용 프로그램을 의미한다. 주로 웹 브라우저 내 또는 웹 브라우저가 제어 가능한 환경에서 실행되며, 자바스크립트, 자바 애플릿 등과 같은 웹 브라우저가 실행 가능한 프로그래밍 언어를 사용하여 HTML과 같은 마크업 언어를 결합하여 만들어진다.
웹 존	웹 서버, 웹 응용프로그램 등이 존재하는 네트워크상의 영역을 의미한다.

■ DDoS 대응장비

용어	정의 내용
DDoS 공격	DDoS 공격(Distributed Denial of Service Attack)은 분산 배치된 여러 단말을 통해 특정 서버에 많은 양의 접속 시도를 동시에 수행하여 시스템이 정상적인 서비스를 제공할 수 없도록 하는 공격을 의미한다.
TCP Syn Flooding	TCP/IP의 3-Way Handshaking에 기반을 둔 공격으로, 공격자는 공격대상 서버에게 접속을 요청하는 TCP Syn 패킷을 대량으로 전송하여 공격대상 서버가 Ack 패킷을 받기 위한 TCP Syn-Ack 응답 패킷을 전송을 유도한다. 공격자는 TCP Syn-Ack 패킷에 응답하지 않음으로써 공격대상 서버에 '반만 열린(Half Open)' 연결이 대량으로 생성되어 시스템 자원을 고갈시켜 정상적인 서비스를 제공할 수 없게 방해하는 DDoS 공격 유형을 의미한다.
TCP Syn-Ack Flooding	송신자를 공격대상 서버 주소로 설정한 TCP Syn 패킷을 전송, 해당 패킷을 받은 수신자는 TCP Ack 패킷을 받을 때까지 공격대상 서버 주소로 TCP Syn-Ack 응답패킷을 계속 전송한다. TCP Syn 패킷을 전송하지 않은 공격대상 서버는 이를 무시하게 되고 계속되는 TCP Syn-Ack 패킷에 대응함으로써 시스템 자원을 고갈시켜 정상적인 서비스를 제공할 수 없게 방해하는 DDoS 공격 유형을 의미한다.
TCP Ack Flooding	TCP Ack 패킷을 대량으로 공격대상 서버로 전송하여 공격대상 서버의 Reset 발생으로 시스템 자원 고갈을 유도하는 DDoS 공격 유형을 의미한다.
TCP Fin Flooding	위조된 출발지 주소와 포트, Fin 플래그를 설정하여 대량의 패킷을 전송하여 공격대상 서버가 정상적인 서비스를 제공할 수 없게 방해하는 DDoS 공격 유형
ICMP Flooding	대량의 Echo Request(PING)를 공격대상 서버에 보냄으로써 버퍼오버플로우를 발생하게 하는 DDoS 공격 유형을 의미한다.
UDP Flooding	UDP의 비연결성 및 비신뢰성 때문에 공격이 용이한 방법으로 패킷 사이즈를 줄여 대량의 UDP 패킷을 공격대상 서버로 전송하여 공격대상 서버의 네트워크 자원을 소모시키는 DDoS 공격 유형을 의미한다.

TCP Multi-Connection	정상적인 TCP 3-Way Handshaking을 통해 공격대상 서버의 TCP 연결을 증가시켜 공격대상 서버의 자원을 소모시키는 DDoS 공격 유형을 의미한다.
Valid HTTP GET Flooding	정상적인 HTTP GET 요청을 대량으로 공격대상 서버에 전송하여 다른 정상적인 HTTP GET 요청을 정상적으로 처리할 수 없게 방해하는 DDoS 공격 유형을 의미한다.
Invalid HTTP GET Flooding	비정상적인 HTTP GET 요청을 대량으로 공격대상 서버에 전송하여 다른 정상적인 HTTP GET 요청을 정상적으로 처리할 수 없게 방해하는 DDoS 공격 유형을 의미한다.
CC(Cache Control) Attack	공격자가 HTTP User-Agent 헤더의 Cache-Control 값을 비정상적으로 조작한 후 공격대상 서버에게 웹페이지를 요청하여 비정상 동작을 유발하는 DDoS 공격 유형을 의미한다.
DNS Query Flooding	공격대상 서버(DNS 서버)로 대량의 변조된 Query를 전송하여 DNS 서비스의 정상운용을 불가능하게 하는 DDoS 공격 유형을 의미한다.
Amplifier DNS Reply flooding	DNS ANY Query를 요청하는 것으로 위장(IP Spoofing) 한 후, ripe.net의 ANY 레코드의 결과를 공격 네임 서버로 전송되도록 하는 DNS 증폭 DDoS 공격 유형을 의미한다.
저대역폭 HTTP DoS	공격대상 서버(HTTP 서버)의 연결 제한을 모두 소진시키도록 적은 양의 대역폭만을 사용하여 공격대상 서버에 연결을 시도한 후 해당 연결이 영구히 지속되게 만드는 공격 방법으로 연결 제한을 소진시키는 DDoS 공격 유형을 의미한다.
SQL Query Flooding	웹 서버가 WAS 서버 및 DB 서버와 연계되어 운영되는 것에 착안하여 만들어진 공격 방식으로 정상 또는 비정상 SQL Query를 웹서버에 지속적으로 전송함으로써, 웹 서버와 연결된 WAS서버와 DB 서버를 마비시키기 위한 DDoS 공격 유형을 의미한다.
Slowloris	널리 알려진 웹 서버인 Apache를 대상으로 가해지는 공격이다. 이 공격은 Apache 웹 서버가 '/r/n'을 전송받기 전에는 세션 종료를 인지하지 못하고 계속해서 세션을 유지하는 특성을 악용한 DDoS 공격을 의미한다.

■ 인터넷전화 보안제품

용어	정의 내용
IM(Instant Message)	인터넷전화 단말기를 통해 사용자간 간단한 메시지를 주고받을 수 있는 서비스를 의미한다.
IP-PBX(Internet Protocol-Private automatic Branch eXchange)	IP 네트워크에서 인터넷전화를 할 수 있도록 해주는 사설교환기를 의미한다.

RTP(Real-Time Transport Protocol)	오디오와 비디오 등 미디어 데이터를 실시간으로 전송하기 위한 IETF 표준 프로토콜(RFC3550)을 의미한다.
SBC(Session Boarder Controller)	신호, 데이터, 음성 및 비디오 트래픽을 처리하면서 IP 네트워크 경계 사이의 실시간 멀티미디어 트래픽 흐름을 제어 및 관리하는 시스템을 의미한다.
SIP(Session Initiation Protocol)	IP 네트워크에서 전화를 연결하기 위하여 일반전화 서비스의 호를 제어하는 IETF 표준 프로토콜(RFC3261)을 의미한다.
SRTP(Secure Real-time Transport Protocol)	RTP/RTCP를 통해 전달되는 미디어 트래픽을 보호하기 위한 IETF 표준 프로토콜(RFC 3711)을 의미한다.
TLS(Transport Layer Security)	SSL에 기반을 둔 서버와 클라이언트간의 암호화 통신 프로토콜(TLS v1.0: RFC2246, TLS v1.1: RFC4346, TLS v1.2: RFC5246)을 의미한다.

■ 침입방지시스템

용어	정의 내용
시그니처 기반 탐지	검사 대상을 사전에 알려진 공격 패턴인 시그니처와 비교하여 탐지하는 기법을 의미한다.
행위 기반 탐지	사용자, 호스트, 네트워크 커넥션, 어플리케이션 등에 대한 정상적인 활동을 정의한 프로파일을 이용, 관찰된 이벤트의 편차를 확인하는 기법을 의미한다.
실행 기반 탐지	파일 및 URL 등 검사대상을 가상 환경에서 실행하고 그 결과를 분석해서 탐지하는 기법을 의미한다.

■ 무선침입방지시스템

용어	정의 내용
IEEE 802.11	무선랜, 와이파이(Wi-Fi)라고 부르는 근거리 지역을 위한 무선 네트워크 기술로, IEEE의 LAN/MAN 표준 위원회 (IEEE 802)의 11번째 워킹그룹에서 개발된 표준 기술을 의미한다.
AP(Access Point)	무선 단말로부터 전달된 프레임을 다른 단말에게 중계하는 기능을 수행하는 유무선 연동 브리지 디바이스를 의미한다.

SSID(Service Set IDentifier)	무선랜에서 서비스 제공자가 여러 다른 무선 셀(Basic Service Set)들을 구분하는데 사용하는 무선 단말과 AP간에 접속용 식별자를 의미한다.
Rogue AP	다른 무선 디바이스들과 연결 및 통신이 가능한 무선 디바이스로 내부 무선랜에 인가되지 않고 설치된 AP를 의미한다.
Honeypot AP	공격 대상 AP의 SSID를 도용하여 사용자가 정상적인 AP에 접속한 것처럼 위장하여 아이디 및 패스워드 등 사용자 정보 유출을 유도하는 AP를 의미한다.
Ad-hoc 네트워크	고정된 유선망을 가지지 않고 각 단말끼리 서로 연결되어 통신하는 형태의 네트워크를 의미한다.
WDS(Wireless Distribution System)	유무선 공유기가 무선으로 다른 유무선 공유기 또는 AP에 연결되어 하나의 네트워크를 구성할 수 있게 해주는 시스템을 의미한다.
Wi-Fi Direct	AP 또는 라우터와 같은 별도의 장비 없이도 단말 간 직접 통신을 통하여 기기간 콘텐츠 및 서비스를 사용할 수 있는 기반을 제공하는 기술을 의미한다.
PMF(Protected Management Frame)	802.11w에서 규정된 일부 관리 프레임을 보호할 수 있는 표준을 의미한다. 관련 프레임은 De-Authentication, Disassocation 등이 있다.

■ 가상사설망제품

용어	정의 내용
통신상대	가상사설망 제품과 보안통신을 하기 위해 상호 인증된 외부 IT실체를 의미한다.
IPSec (Internet Protocol Security protocol)	네트워크나 네트워크 통신의 패킷 처리 계층에서의 보안을 위해 사용하는 프로토콜을 의미한다.
SSL (Secure Sockets Layer)	컴퓨터 네트워크 망에서 기밀성, 무결성과 같은 보안성을 제공하기 위한 보안 프로토콜을 의미한다

■ 네트워크 접근통제제품

용어	정의 내용
NAC (Network Access Control) 센서	NAC 서버로부터 네트워크 접근통제 정책을 전달받아 단말에 대한 네트워크 허용 · 차단을 수행하는 제품 구성요소를 의미한다.

NAC 서버	NAC 에이전트가 설치된 단말에서 일반사용자에 대한 식별 및 인증을 수행하고, NAC 에이전트로부터 수집된 정보를 바탕으로 네트워크 접근통제 정책을 생성하여 NAC 센서 및(또는) 에이전트에게 전달하는 제품의 구성요소를 의미한다.
NAC 에이전트	단말의 무결성 상태 정보를 NAC 서버로 전달하고, NAC 서버로부터 네트워크 접근통제 정책을 전달받아 단말에 대한 네트워크 허용/차단을 수행하는 제품의 구성요소를 의미한다.

■ 망간자료전송제품

용어	정의 내용
보안영역	인터넷과 물리적으로 분리되어 내부적으로 운영되는 네트워크를 의미한다.
비(非)-보안영역(인터넷망)	인터넷과 물리적으로 연결된 네트워크를 의미한다.
업무서버	보안영역 스트림연계 통제 보안요구사항과 관련하여 보안영역에 위치하고, 업무관련 자료가 저장되며 非-보안영역에서는 접근할 수 없는 서버를 의미한다.
스트림	보안영역과 非-보안영역사이에서 응용 프로토콜(예. HTTP, SNMP 등)로 전송되는 데이터의 연속적인 흐름을 의미한다.
전송통제서버	망간 자료전송 제품이 설치되어 보안 정책에 따라 비인가자(시스템) 접근통제 및 보안영역과 非보안영역 간 자료전송 통제 또는 스트림연계 통제를 수행하는 시스템을 의미한다.

■ 시스템 접근관리제품

용어	정의 내용
관리대상시스템	내부 네트워크의 서버 또는 네트워크 장비 등 시스템 접근관리 제품의 보호대상이 되는 시스템을 의미한다.

■ 스팸메일차단시스템

용어	정의 내용
스팸메일	본인이 원치 않음에도 일방적으로 전송되는 영리목적 등의 광고성 이메일을 의미한다.

스팸메일 시그니처	이미 알려진 스팸메일을 식별하는데 이용되는 스팸메일 패턴의 집합을 의미한다.
스팸메일 격리소	스팸메일로 분류된 이메일을 보관하는 저장소를 의미한다.

■ 무선랜 인증제품

용어	정의 내용
AP (Access Point)	유 · 무선 연동 브리지 기능을 수행하는 외부 IT실체로서, 무선랜 인증 서버와 무선랜 인증 클라이언트간 인증 관련 메시지를 중계하고 무선랜 접근통제 정책에 근거하여 무선랜 단말의 네트워크 사용을 통제하는 장치를 의미한다.
EAP (Extensible Authentication Protocol)	네트워크와 인터넷 연결에 사용되는 인증 프레임워크로써 RFC 3748(구 RFC 2284)에 정의되어 있으며 RFC 5247에 의해 업데이트되는 프로토콜을 의미한다.
무선랜 단말	무선 NIC를 장착하여 IEEE 802.11x 표준에 기반한 물리계층 및 MAC 계층의 동작을 수행하는 장치를 의미한다.
마스터키	무선랜 구간의 기밀성 및 무결성 확보를 위한 비밀키로써, 특정 EAP 인증 방법을 사용한 무선랜 인증 클라이언트와 무선랜 인증서버 사이의 상호인증 완료시 공유된 비밀정보를 기반으로 각각 생성되는 공유키를 의미한다.

■ 소프트웨어 기반 보안USB제품

용어	정의 내용
보안 USB 메모리	11바이트 이상의 패스워드 인증 메커니즘을 갖는 컨트롤러 칩을 내장하고 있는 USB 메모리로서, 인증 메커니즘을 통해 보안영역에 대한 접근통제를 수행하며 이동시 편의를 위해 CD 영역에 USB 에이전트 프로그램을 탑재하고 있는 장치를 의미한다.
휴대용 저장매체	호스트의 분해 없이 쉽게 분리 가능하도록 고안된 보조기억장치를 총칭하며, 이동식 디스크, 이동식 메모리, 이동식 미디어(CD/DVD/BD 등 광학 디스크) 등이 있다.

■ 호스트 자료유출방지제품

용어	정의 내용
민감 콘텐츠	관리자에 의해 외부 반출시 통제가 필요하다고 지정된 콘텐츠를 의미한다.

외부 인터페이스	호스트내 저장 데이터를 유출할 수 있는 물리적인 인터페이스를 의미한다. (USB, e-SATA, IEEE1394, ExpressCard, Modem, HDMI, Bluetooth, LAN 포트, WLAN 포트, Serial 포트, Parallel 포트, 적외선 포트 등이 있다.)
콘텐츠	호스트에 저장되거나 네트워크를 통하여 제공되는 각종 정보나 그 내용물로서 특정 파일 형식(HWP, TXT, DOC, PDF, DOCX, PPT, PPTX, XLS, XLSX, ZIP 등)으로 표현될 수 있으며, 정보 그 자체일 수도 있다.
휴대용 저장매체	이동식 디스크, 이동식 메모리, 이동식 미디어(CD/DVD/BD 등 광학 디스크) 등 호스트의 분해 없이 쉽게 분리 가능하도록 고안된 보조기억장치를 총칭한다.

■ 네트워크 자료유출방지제품

용어	정의 내용
콘텐츠	호스트에 저장 또는 네트워크로 제공되는 각종 정보 및 그 내용물을 의미한다. 특정 파일 형식(HWP, TXT, DOC, PDF, DOCX, PPT, PPTX, XLS, XLSX, ZIP 등)으로 표현될 수 있으며, 정보 그 자체일 수도 있다.
프로토콜	이메일, 메신저, 파일 업로드 · 다운로드, 웹 등 사용자 서비스를 제공하기 위한 통신 규칙(SMTP, HTTP, HTTPS, FTP, SFTP, SSH, TELNET, IMAP, IRC, RDP 등)을 의미한다.

■ 통합보안관리제품

용어	정의 내용
관리대상시스템	△침입차단시스템 △침입탐지시스템 △특정 OS가 설치된 PC · 서버 등 통합보안관리 제품이 보안정책을 적용하여 관제 및 관리하는 IT실체를 의미한다.
관제대상시스템	PC, 각종 서버, 네트워크 장치, 타사의 보안제품 등 통합보안관리 제품과 직접 연동되지 않아 시스템 상태에 대한 관제만 수행하는 시스템을 의미한다.
관제	대상 IT실체에 대하여 로그 데이터 및 이벤트 데이터 수집, 모니터링을 수행하는 행위를 의미한다.
상관분석	개별적인 침해탐지요소들을 다양한 조합으로 재해석하여 위협을 종합적으로 판단하는 분석기법을 의미한다.
관리	대상 시스템에 대하여 로그 데이터 및 이벤트 데이터 수집, 모니터링, 보안정책 설정을 수행하는 행위를 말한다.

■ 가상화관리제품

용어	정의 내용
가상영역	신뢰된 가상화 기술을 통해 컴퓨터 자원(CPU, 메모리, 디스크, 어플리케이션 등)을 논리적으로 가상화, 독립적인 컴퓨터 환경을 제공하는 영역을 의미한다.

실제영역	사용자가 컴퓨터(PC, 서버)를 사용하기 위해 설치한 운영환경으로 가상영역을 제외한 모든 영역을 의미한다.

■ 소스코드 보안약점 분석도구

용어	정의 내용
보안취약점 (Vulnerability)	악의적인 해커 등에 의한 중요정보 유출, 악성코드 유포, 서비스 방해 등의 사이버공격에 직 · 간접적으로 악용이 되는 보안약점을 의미한다.
보안약점 (Weakness)	소프트웨어 개발 전체 단계에서 개발자의 인식부족 및 부주의 등으로 발생하는 소프트웨어 결함, 오류, 버그, 에러 등을 의미하며, 이 문서에서는 소스코드 상의 보안약점으로 한정한다. * CWE(Common Weakness Enumeration) 및 '소스코드 보안약점 분석도구 보안요구사항'의 '〈별표〉 주요 소스코드 보안약점 예시' 참조

■ 패치관리시스템

용어	정의 내용
단말 (호스트 또는 패치대상)	엔드포인트에 위치한 패치관리시스템의 패치파일 설치 대상이 되는 IT실체를 의미한다.
업데이트 서버	소프트웨어 업체에서 패치파일의 안전성 및 운용성을 검증한 후 배포서버에게 최신 패치파일을 온라인으로 제공해 주는 외부 IT실체인 서버를 의미한다.
배포서버	에이전트와 상호 통신을 통해 패치 관련 정보를 주고받으며 패치 정책을 통해 에이전트를 관리하고 최신 패치파일을 배포해 주는 제품의 구성요소를 의미한다. ('서버 공통보안요구사항'이 적용되는 제품의 구성요소, 즉, '관리서버'가 배포서버 역할을 수행한다.)

■ 데이터베이스 접근통제제품

용어	정의 내용
데이터베이스 (DB, Database)	동시에 복수의 적용 업무를 지원할 수 있도록 복수 이용자의 요구에 호응해서 데이터를 받아들이고 저장, 공급하기 위하여 일정한 구조에 따라서 편성된 데이터의 집합을 의미한다. 여기서 의미하는 데이터베이스는 관계형 데이터베이스를 의미한다.

DCL (Data Control Language)	데이터베이스 사용자의 권한을 제어하는데 사용되는 SQL문(예: GRANT, REVOKE)을 의미한다.
보안취약점 (Vulnerability)	악의적인 해커 등에 의한 중요정보 유출, 악성코드 유포, 서비스 방해 등의 사이버공격에 직 · 간접적으로 악용이 되는 보안약점을 의미한다.
DDL (Data Definition Language)	데이터베이스에서 데이터와 데이터간의 관계를 정의하여 데이터베이스 구조를 설정하는 SQL문(예: CREATE, DROP)을 의미한다.
DML (Data Manipulation Language)	데이터베이스에 저장된 자료를 검색, 삽입, 삭제, 갱신하기 위해 사용되는 SQL문(예: SELECT, INSERT, DELETE, UPTDATE)을 의미한다.
SQL (Structured Query Language)	관계형 데이터베이스관리시스템에서 자료의 검색과 관리, 데이터베이스 스키마 생성과 수정 등을 위해 고안된 컴퓨터 언어를 의미한다.
DB 사용자	DCL, DDL, DML 등의 SQL을 사용하여 데이터 베이스 작업을 수행하는 데이터베이스 관리자(DBA, Database administrator), 개발자, DB 운영자(operator), 어플리케이션 서버 등을 의미한다. 데이터베이스 접근통제 제품은 보호대상 DB로 접근하기 위해 제품을 통과해야 하는 일반 사용자를 DB 사용자로 본다.

■ 스위치 · 라우터

용어	정의 내용
TDUT (Target Device Under Test)	‘보안기능 시험’제도에서 시험 대상 제품을 의미한다.
펌웨어 · 소프트웨어	장비에 설치되거나 업데이트를 위해 제공되는 설치 패키지 파일을 의미한다. ‘펌웨어’로 통칭하여 기술할 수 있다.

■ 안티바이러스제품

용어	정의 내용
악성코드	바이러스, 웜, 트로이목마, 스파이웨어 등과 같이 컴퓨터 및 네트워크에 악영향을 끼칠 수 있는 코드를 의미한다. (악성코드는 부트영역, 파일시스템, 메모리영역 등에 존재할 수 있다.)

바이러스	자기 자신을 복제할 수 있는 기능을 가지고 있으며 컴퓨터 프로그램 또는 실행 가능한 파일의 부분을 변형시키고 그곳에 자신 또는 자신의 변형을 복사해 넣는 명령어들의 조합을 의미한다.
스파이웨어	사용자의 동의 없이 또는 사용자를 속여 설치된 후 광고나 마케팅을 위한 정보를 수집하거나 중요한 개인 정보를 빼 가는 악의적 프로그램을 의미한다.
웜	컴퓨터 바이러스와 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해서 전파되는 프로그램을 의미한다.
트로이목마	시스템 내에 특정 코드를 만들어 놓음으로써 영구적으로 시스템 내에 침투하여 상주하거나 소기의 목적을 달성한 후 그 자취를 지워버릴 수 있는 프로그램을 의미한다.
시그니처	바이러스, 웜, 스파이웨어, 트로이목마 등 악성코드에 존재하는 특정 패턴 또는 해시값 등 악성코드 탐지를 위해 목록화 된 데이터를 의미한다.

■ 스마트폰보안관리제품

용어	정의 내용
모바일 단말	휴대 가능한 기기로 하드웨어 플랫폼과 시스템 소프트웨어로 구성된다. 일반적으로 전화, 이메일, 메시지 전송 등의 기능을 제공하는 소프트웨어를 포함하고 있으며, 무선 접속이 가능하고 3G, 4G, 5G 통신이 가능한 기기를 의미한다.
스마트폰	휴대 전화에 여러 컴퓨터 지원 기능을 추가한 지능형 단말기를 의미한다. * 국가용 보안요구사항에서 스마트폰이라 함은 모바일 업무수행을 위한 스마트패드 등을 포함한다.
테더링	USB 또는 블루투스 장치, Wi-Fi(무선랜) 등을 통해 스마트폰에 노트북, 넷북, 데스크톱 PC 등 IT 기기들을 연결하여 인터넷을 사용할 수 있도록 지원하는 기술을 의미한다.
공장 초기화	장치, 소프트웨어 등을 공장 출고 상태로 초기화 하는 것을 의미한다.

■ 운영체제(서버) 접근통제제품

용어	정의 내용
강제적 접근 통제 (Mandatory Access Control, MAC)	사용자에게 부여된 접근허가 범위(Clearance)에 기반하여 접근을 통제하는 방식을 의미한다.

보안등급 (Security Level)	사용자나 정보의 중요도를 표시하는 계층적인 보호등급(Hierarchical Classification) 및 비계층적인 보호범주(Non-Hierarchical Category)의 조합을 의미한다.
역할 (Role)	사용자와 제품 사이에 허용되는 상호작용을 설정하는 미리 정의된 규칙의 집합을 의미한다.
역할기반 접근통제 (Role Based Access Control, RBAC)	사용자가 객체에 접근할 때, 사용자와 접근허가의 직접적인 관계가 아닌 조직의 특성에 따른 역할을 매개자로 하여 사용자-역할, 접근허가-역할의 관계를 통해 접근을 제어하는 방식을 의미한다. 핵심 모델, 계층 모델, 직무분리 모델이 적용될 수 있다.
중요도 레이블 (Sensitivity Label)	주체나 객체의 보안등급을 표시하는 보안속성을 의미한다.
접근허가 (Permission)	객체에 대한 오퍼레이션을 할당하는 수단으로 객체와 오퍼레이션의 쌍으로 구성되며. RBAC을 적용하는 시점에 객체와 오퍼레이션은 미리 정의된 것으로 가정한다.
오퍼레이션 (Operation)	주체(사용자 등)가 객체(사용자 데이터 등)에 대해 수행하는 특정 행동을 의미한다.
임의적 접근통제 (Discretionary Access Control, DAC)	사용자 신원 혹은 그룹 신원에 기반하여 접근을 통제하는 방식을 의미한다
직무분리 (Separation of Duty, SOD)	한 명의 사용자에게 상충적인 역할을 동시에 제공하지 않음으로써 공모의 기회를 최소화하고 조직의 부정을 예방하는 수단을 의미한다.

■ 패스워드관리제품

용어	정의 내용
관리자	패스워드 정책을 설정하고 사용자의 패스워드 발급 요청에 대해 패스워드 발급을 승인할 수 있는 권한을 가진 사용자를 의미한다.
일반 사용자	관리대상에 접속하기 위해 패스워드 발급을 요청하는 사람을 의미한다.
안전하게 저장	시스템 관리자(패스워드 발급 승인권자가 아닌)이외의 접근이 차단되고 평문 · 단순 인코딩(Base 64 등)으로 저장되지 않음을 의미한다.

DRBG	결정론적 알고리즘에 입력하여 난수를 생성하는 장치 · 알고리즘을 의미한다.

■ 랜섬웨어 대응제품

용어	정의내용
랜섬웨어	사용자 PC(또는 서버)에 존재하는 데이터를 암호화하여 사용자의 접근을 불가능하게 하는 암호화 랜섬웨어를 의미한다.
목록 기반 탐지	알려진 랜섬웨어의 정보(시그니처, 해시값, DNA, 지문, 프로세스명)를 목록화하여, 목록의 정보와 일치하는 랜섬웨어를 탐지하는 행위를 의미한다.
비인가 암호화 행위	사용자의 허가 또는 설정없이 임의로 수행되는 암호화 행위를 의미한다.
의심 프로세스	비인가 암호화 행위를 수행하는 프로세스로, 알려지지 않은 신 · 변종 유형의 랜섬웨어이거나 제품에서 랜섬웨어로 오인하여 탐지한 정상 프로세스가 이에 해당된다.
검역소	제품에 의해 탐지된 의심 프로세스를 임시로 격리하여 저장하는 공간을 의미한다.
감시 영역	사용자 PC(또는 서버) 내 시스템에 침투하는 랜섬웨어와 비인가 암호화 행위를 감시하는 메모리 영역을 의미한다.

■ 랜섬웨어 대응제품

용어	정의내용
랜섬웨어	사용자 PC(또는 서버)에 존재하는 데이터를 암호화하여 사용자의 접근을 불가능하게 하는 암호화 랜섬웨어를 의미한다.
목록 기반 탐지	알려진 랜섬웨어의 정보(시그니처, 해시값, DNA, 지문, 프로세스명)를 목록화하여, 목록의 정보와 일치하는 랜섬웨어를 탐지하는 행위를 의미한다.
비인가 암호화 행위	사용자의 허가 또는 설정없이 임의로 수행되는 암호화 행위를 의미한다.
의심 프로세스	비인가 암호화 행위를 수행하는 프로세스로, 알려지지 않은 신 · 변종 유형의 랜섬웨어이거나 제품에서 랜섬웨어로 오인하여 탐지한 정상 프로세스가 이에 해당된다.

검역소	제품에 의해 탐지된 의심 프로세스를 임시로 격리하여 저장하는 공간을 의미한다.
감시 영역	사용자 PC(또는 서버) 내 시스템에 침투하는 랜섬웨어와 비인가 암호화 행위를 감시하는 메모리 영역을 의미한다.

■ 양자암호통신장비제품군

용어	정의 내용
비밀키	양자키 분배 메커니즘에 의해 QKD장비에서 생성된 최종키로서 QKMS에 공급된다.
가공키	제품이 원활한 키관리를 위해 비밀키를 분할 · 결합 방식으로 크기를 재구성하거나 키 메타데이터를 조합하여 가공한 키를 의미한다.
공급키	제품이 양자통신암호화장비(QENC)에게 공급하는 키 데이터이다. 이 키는 가공키의 일부 데이터 또는 가공키 자체가 될 수 있다. 3개 이상의 QKD 노드 연결이 필요한 종단 간 노드 사이에 키를 공급하는 경우, 제품은 키 전달 기능을 통해 종단 간 키를 설정하여 공급하며, 이때 공급키는 키 전달 방식 및 설정 방식에 따라 그 형태가 다양할 수 있다.
걸러진키	QKD 장비 후처리 단계중 오류정정을 거치기 직전의 키를 말한다.

■ 영상정보처리기기제품군

용어	정의 내용
영상정보 처리기기	일정한 공간 또는 특정 위치에 설치되어 사람 또는 사물의 영상 등을 촬영하고 영상데이터를 유 · 무선 TCP/IP 네트워크를 통해 전송하는 기기 및 전송받은 영상데이터의 녹화 기록, 통제 대상 카메라의 관리 · 제어, 실시간 모니터링 등을 수행 하는 기기를 의미한다.
IP카메라	일정한 공간 또는 특정 위치에 설치되어 사람 또는 사물의 영상 등을 촬영하고 영상데이터를 유 · 무선 TCP/IP 네트워크를 통해 전송하는 기기를 의미한다.
영상정보 관리 · 저장제품	IP카메라로부터 전송받은 영상데이터의 녹화 기록, 통제 대상 카메라의 관리 · 제어, 실시간 모니터링 등을 수행 하는 기기를 의미한다.
관리프로그램	영상정보처리기기에 대한 원격 영상 모니터링, 보안관리, 카메라 제어 등이 가능한 프로그램(CMS 등)을 의미한다.
영상관리 접속	영상정보처리기기에 기기 간 연동 및 영상 전송 관련 표준 프로토콜(예: ONVIF, RTSP 등)로 설정(established)된 원격관리를 의미한다.

카메라 제어	PTZ, Preset, Touring, Focus 조정 등 카메라가 촬영하는 물리적 위치를 변경하는 제어를 의미한다.
관제	영상을 포함한 다양한 정보를 통합 구성하여 목적에 맞게 모니터링 하거나 관리하는 것을 의미한다.
로컬 운용	로컬 콘솔포트로 접속하는 것이 아닌 제품의 로컬 환경에서 운용 및 관리하는 것을 의미한다.
영상 모니터링 관리자	실시간 또는 저장된 영상 모니터링을 위해 제품에 접속하는 사용자

8. 약어표

용어	정의 내용
AP	Access Point
CMS	Central Monitoring System
DAC	Discretionary Access Control
DB	Database
DBMS	Database Management System
DCL	Data Control Language
DDL	Data Definition Language
DDoS	Distributed Denial of Service
DML	Data Manipulation Language
DNS	Domain Name System
DVR	Digital Video Recorder
EAP	Extensible Authentication Protocol
GPS	Global Positioning System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ICMP	Internet control message protocol
IM	Instant Message
IMEI	International Mobile Equipment Identity

IP	Internet Protocol
IP-PBX	Internet Protocol-Private automatic Branch eXchange
IPSec	Internet Protocol Security
IT	Information Technology
MAC	Mandatory Access Control
MAC	Media Access Control
NFC	Near Field Communication
NTP	Network Time Protocol
DVR	Digital Video Recorder
OSI	Open System Interconnection
OTP	One Time Password
PMF	Protected Management Frame
RBAC	Role Based Access Control
RTP	Real-Time Transport Protocol
SBC	Session Boarder Controller
SIP	Session Initiation Protocol
SMS	Short Message Service
SQL	Structured Query Language
SRTP	Secure Real-time Transport Protocol
URL	Uniform Resource Locator
SOD	Separation of Duty
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDUT	Target Device Under Test
TLS	Transport Layer Security
UDID	Unique Device Identifier
UDP	User Datagram Protocol
WAS	Web Application Server
WDS	Wireless Distribution System

〈 별지 1 〉

〈 국가용 보안요구사항 체계 〉

※이 체계도는 국가정보원이 검증하는 모든 제품유형을 의미하지 않습니다.

〈 별지 2 〉

〈 국가용 보안요구사항 현황 〉

제품군	명칭	버전	적용되는 공통보안요구사항
공통	서버 공통보안요구사항	V3.0 R1	-
	엔드포인트 보안요구사항	V3.0	-
침입차단 제품군	침입차단시스템 보안요구사항	V3.0	서버 공통보안요구사항
	웹 방화벽 보안요구사항	V3.0 R1	서버 공통보안요구사항
	DDoS 대응장비 보안요구사항	V3.0	서버 공통보안요구사항
	인터넷전화 보안제품 보안요구사항	V3.0	서버 공통보안요구사항
침입방지 제품군	침입방지시스템 보안요구사항	V3.0 R1	서버 공통보안요구사항
	무선 침입방지시스템 보안요구사항	V3.0	서버 공통보안요구사항
구간보안 제품군	가상사설망제품 보안요구사항	V3.0 R1	서버+엔드포인트(해당시) 보안요구사항
	네트워크 접근통제제품 보안요구사항	V3.0 R1	서버+엔드포인트 보안요구사항
	망간 자료전송제품 보안요구사항	V3.0 R1	서버+엔드포인트(해당시) 보안요구사항
	무선랜 인증제품 보안요구사항	V3.0 R1	서버+엔드포인트 보안요구사항
전송자료보안 제품군	스팸메일차단시스템 보안요구사항	V3.0 R1	서버 공통보안요구사항
	소프트웨어 기반 보안USB제품 보안요구사항	V3.0 R1	서버+엔드포인트 보안요구사항
	호스트 자료유출방지제품 보안요구사항	V3.0	서버+엔드포인트 보안요구사항
	네트워크 자료유출방지제품 보안요구사항	V3.0 R1	서버 공통보안요구사항
보안관리 제품군	통합보안관리제품 보안요구사항	V3.0 R1	서버+엔드포인트(해당시) 보안요구사항
	소스코드 보안약점 분석도구 보안요구사항	V3.0	적용하지 않음
	패치관리시스템 보안요구사항	V3.0	서버+엔드포인트 보안요구사항
	데이터베이스 접근통제제품 보안요구사항	V3.0	서버+엔드포인트(해당시) 보안요구사항
	시스템접근관리제품 보안요구사항	V3.0	서버+엔드포인트(해당시) 보안요구사항
	패스워드관리제품 보안요구사항	V3.0 R1	적용하지 않음
가상화제품군	가상화관리제품 보안요구사항	V3.1	서버+엔드포인트 보안요구사항

제품군	명칭	버전	적용되는 공통보안요구사항
엔드포인트보안 제품군	안티바이러스제품 보안요구사항	V3.0 R1	서버(해당시)+엔드포인트 보안요구사항
	스마트폰 보안관리제품 보안요구사항	V3.1	서버 공통보안요구사항
	운영체제(서버) 접근통제제품 보안요구사항	V3.0 R1	서버+엔드포인트 보안요구사항
	iOS · iPadOS 모바일 단말 보안관리제품 보안요구사항	V3.0	서버 공통보안요구사항
	랜섬웨어 대응제품 보안요구사항	V3.0	서버+엔드포인트 보안요구사항
네트워크 장비	스위치 · 라우터 보안요구사항	V3.0 R1	적용하지 않음
	SDN 컨트롤러 보안요구사항	V3.0 R1	적용하지 않음
	SDN 스위치 보안요구사항	V3.0 R1	적용하지 않음
양자암호 통신장비	양자통신암호화장비 보안요구사항	V1.0	적용하지 않음
	양자키관리장비 보안요구사항	V1.0	적용하지 않음
	양자키분배장비 보안요구사항	V1.0	적용하지 않음
영상정보처리 기기	IP카메라 보안요구사항	V3.0	적용하지 않음
	영상정보 관리 · 저장제품	V3.0	적용하지 않음

〈 별 표 1 〉

제 · 개정 이력

일 자	주요 변경 내용
2021. 4. 2.	제정
2021. 9. 1.	o 국가용 보안요구사항의 해석 · 복합적용 원칙 추가 o 일반 보안요구사항 작성 원칙 추가
2022. 11. 3.	o 양자암호통신장비 제품군 추가 – ‘양자통신암호화장비 보안요구사항’추가 – ‘양자키관리장비 보안요구사항’추가 – ‘양자키분배장비 보안요구사항’추가
2023. 2. 14.	o ‘iOS · iPadOS 모바일 단말 보안관리제품 보안요구사항’추가
2023. 8. 21.	o ‘랜섬웨어 대응제품 보안요구사항’추가
2024. 4. 1.	o 영상정보처리기기 제품군 보안요구사항 추가

2편 공통보안요구사항

공통보안요구사항

1장
서버 공통보안요구사항

1절 일반사항

1. 운용 환경 정의

■ 가정사항

○ '서버 공통보안요구사항'의 적용 대상이 되는 제품(또는 구성요소)은 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 설치 및 운용된다.

○ 제품의 인가된 관리자는 악의가 없으며, 제품 관리 기능에 대하여 적절히 교육받았고 운용기관이 마련한 관리자 지침에 따라 정확하게 의무를 수행한다.

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

○ 제품의 인가된 관리자는 '서버 공통보안요구사항' 적용 대상 제품의 구성요소 작동에 불필요한 운영체제상의 서비스나 수단 등을 제거하고 취약점에 대한 개선 작업을 통해 운영체제의 신뢰성과 안전성을 보장한다.

○ 제품의 인가된 관리자는 웹브라우저, 관리프로그램 등을 통해 제품에 접속할 수 있으며, 이 때 HTTPS, TLS, SSH 등 안전한 통신을 이용하여 보안관리를 수행한다.

■ 제품 보안요구사항의 적용

‘서버 공통보안요구사항’이 적용되는 제품은 하드웨어 일체형 또는 소프트웨어 등 다양한 형태로 구현될 수 있다. ‘서버 공통보안요구사항’은 보안기능 시험 대상 제품 또는 CC 평가 대상 제품(이하 ‘대상 제품’이라 한다.)이 공통으로 구현해야 하는 보안요구사항을 정의하며, 제품 유형에 관계없이 적용할 수 있다. 다만, ‘엔드포인트 보안 제품군’ 중에서 안티바이러스 제품처럼 제품 관리를 위한 별도의 관리도구 없이 사용자 PC 또는 서버에 한정된 설치 · 운용이 허용된 제품은 ‘서버 공통보안요구사항’을 적용하지 않을 수 있다.

‘서버 공통보안요구사항’을 구성하는 각각의 보안기능은 ‘필수’, ‘조건부 필수’, ‘선택’으로 분류되며 적용시 다음에 유의해야 한다.

○ 식별 및 인증

제품 유형에 따라 식별 및 인증의 대상이 달라질 수 있으므로 제품에 접근하는 것을 허용하기 전에 식별 및 인증을 수행해야 하는 대상(예 : 관리자, 일반사용자, 외부 IT 실체 등)을 확인하고 적용해야 한다.

○ 보안 관리

제품의 구성요소 및 구현 형태에 따라 보안 관리 범위가 달라질 수 있으므로 제품에 에이전트 또는 클라이언트 포함 여부를 확인하고 적용해야 한다.

○ 데이터 보호

△제품이 여러 구성요소를 포함하여 구성요소간에 전송되는 데이터가 존재하는 경우(내부 전송 데이터) △제품과 외부 IT실체간에 전송되는 데이터가 존재하는 경우(외부 전송 데이터) △제품이 통제하는 저장소에 저장하는 데이터가 있는 경우(저장 데이터) 등 제품이 보호해야 하는 데이터가 존재하는지 확인하고 적용해야 한다.

○ 자체 보호

제품의 구성요소 및 구현 형태에 따라 제품의 자체시험 및 무결성 검증 대상이 달라질 수 있으므로 제품이 하드웨어 일체형인지 또는 개별적으로 설치되어 사용되는 여러 소프트웨어 요소를 포함하는지 여부를 확인하고 적용해야 한다.

○ 업데이트 보호

제품 유형에 따라 업데이트 기능 제공 유무, 업데이트 파일 유형 및 업데이트 파일을 적용하거나 설치하는 위치 등이 달라질 수 있으므로 제품 유형별로 확인하고 적용해야 한다.

○ 감사 기록

공통보안요구사항에는 최소한의 감사사건만을 포함하고 있으므로 제품 유형별 감사사건은 제품 보안요구사항을 함께 확인하고 적용해야 한다.

○ 암호 지원

암호키 관리 및 암호 연산 등 암호 관련 기능을 구현한 경우 확인하고 적용해야 한다. 다만, 검증필 암호모듈을 탑재하고 사용해야 하는 경우 암호 관련 보안요구사항은 해당 제품의 보안요구사항을 준수해야 한다.

2절 보안요구사항

1. 식별 및 인증

사용자(예 : 관리자, 일반사용자 등)에 대한 식별 및 인증 기능이 안전하게 구현되었는지 확인한다. 즉, 인증 실패 대응, 패스워드 등 인증 데이터 검증 · 생성, 인증 정보 재사용 방지 등 보안기능이 정상동작 하는지 점검한다.

관리자란 제품의 보안기능을 구동 · 중지 · 재시작하거나 보안정책을 추가 · 변경 · 조회 · 삭제하는 등 제품을 안전하게 운영 및 관리하는 사용자를 의미하며 모든 관리자는 식별 및 인증을 수행한 후 제품에 대한 접근을 허용해야 한다.

일반사용자는 관리자가 설정한 보안정책에 따라 제품의 보안기능을 이용하는 사용자로, 제품 유형에 따라 제품에 포함될 수 있는 에이전트 또는 클라이언트를 사용하여 제품의 보안기능을 이용할 수 있다. 통상적으로 일반사용자가 식별 및 인증을 수행한 후 제품에 접근이 허용되나, 식별 및 인증 과정 없이 제품의 보안기능을 사용할 수 있는 제품 유형도 존재한다(예 : 안티바이러스 제품).
그 밖에 관리자나 일반사용자는 아니지만 제품과 상호작용하는 IT실체인 외부 IT실체가 존재할 수 있다. 제품이 보안기능을 제공하기 이전에 제품에서 외부 IT실체를 인증해야 하는 경우 외부 IT실체 또한 제품의 인증 대상으로 간주할 수 있다. 또한, 제품이 외부 IT실체와 연동하기 위해 사용되는 인증 정보를 제품을 통해 관리할 수도 있다.

제품의 사용자는 관리자와 일반사용자를 모두 포함하며, 제품의 인증 대상에는 사용자 외에 외부 IT실체가 포함될 수 있다. 제품 유형에 따라 식별 및 인증 대상이 되는 사용자가 달라질 수 있으며, 이는 제품 보안요구사항을 참조해야 한다.

여 백

1.1 사용자 등 식별 및 인증

1.1.1

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 고유한 값으로 중복 등록되지 않아야 한다.

④ 제품을 구성하는 에이전트 또는 클라이언트에 존재하는 사용자를 식별 및 인증해야 하는 경우, 식별값은 중복 등록되지 않은 고유한 값이어야 한다.

- 사용자 인증시 등록된 에이전트 또는 클라이언트 부가속성도 함께 인증해야 한다.
- 부가 속성: IP 주소는 필수이며, *MAC 주소, Serial Number, 에이전트 자체를 유일하게 식별할 수 있는 정보* 중 최소 1가지 이상 추가 사용해야 한다.

점검시 유의사항

① 제품이 제공하는 전체 사용자 역할을 확인해야 한다.

- 관리자의 경우 관리접속 및 로컬접속 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 관리자가 각 사용자 또는 그룹별로 권한을 설정할 수 있는지 확인해야 한다.

④ 알려진 취약점이 존재하는지 확인해야 한다.

- 계정 및 패스워드 입력필드에 입력 가능한 문자열을 제한하는지 확인이 필요하다.
- ‘보안기능 시험’을 신청한 제품은 시험기관이 '취약점 개선 내역서'를 제출받아 검토한 후 취약성 시험을 생략할 수 있다.

⑤ 시험기관은 취약점 점검 도구 사용의 적절성을 확인하고 시험에 사용해야 한다.

- 인증 · 검증기관은 시험기관에 적절한 도구 사용에 대한 가이드를 제공할 수 있다.

⑥ 사용자 인증을 우회하여 관리화면으로 접근할 수 있는지 확인해야 한다.

1.1.2

조건부 필수	**제품은 사용자 식별 및 인증을 위해 1.1.1과 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) 등*을 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 안전하게 관리되어야 한다. 추가적인 식별 및 인증 방식을 수행하기 위해 사용하는 인증정보를 제품이 저장하는 경우 ‘3.2 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 시험자는 제품이 지원하는 추가적인 식별 및 인증 기능을 모두 조사하고 제품에 포함되는지 확인해야 한다.

- 시험자는 제품에 포함되는 기능의 정상동작을 확인해야 한다.
- ‘국내용 평가 · 인증제도’의 경우 추가적인 식별 및 인증 기능의 보증을 요구하는 것은 아니며, 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(유효기간 1년 이내) 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 ‘3.2 저장 데이터 보호’ 요구사항에 따라 안전하게 저장되는지 확인해야 한다.

1.1.3

조건부 필수

제품은 연동하는 외부 IT실체를 인증해야 한다.

조 건	제품에서 외부 IT실체를 인증하는 경우

참고 사항

① 인증서버 연동 사전공유키, SNMP 인증 패스워드, SNMP 암호화 패스워드 등이 적용대상이 될 수 있다.

점검시 유의사항

① 시험자는 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.

1.2 인증실패 대응

1.2.1

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 예는 다음과 같다.

- *계정잠금 후 지정된 시간이 지난 이후 활성화*.
- *계정잠금 후 활성화를 위한 다른 식별 및 인증 수단 제공 등*.

② 1.1.2에서 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 △1.1.1에서 규정한 식별 및 인증 또는 △1.1.2에서 규정한 추가적인 식별 및 인증 중에서 하나만 실패하여도 해당 인증세션은 실패로 본다.

점검시 유의사항

① 제출문서를 통해 잘못된 인증정보를 사용한 반복된 인증 시도를 안전하게

제한하는 방법이 있는지 확인해야 한다.

② (하드웨어 일체형 장비인 경우) 시험자는 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP 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 기능 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.

1.2.2

필수

제품은 관리자 인증이 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 (하드웨어 일체형 장비인 경우) 시험자는 관리자 인증을 지원하는 모든 서비스(*SSH, HTTPS, SFTP 등*)에 대해서 요구사항을 만족하는지 확인해야 한다.

1.3 패스워드 등 민감정보 생성 및 안전성 검증

1.3.1

조건부 필수

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

조 건	ID와 패스워드가 유일한 사용자 식별 · 인증 수단인 경우

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
금지 항목	사용자 계정(ID)과 동일한 패스워드 설정 금지	필수
	동일한 문자 · 숫자의 연속적인 반복입력 금지	필수
	키보드상의 연속된 문자 또는 숫자의 순차적 입력금지	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.)

1.3.2

조건부 필수	**제품은 패스워드 등록 및 변경시 〈표 2〉의 보안성 기준을 만족해야 한다.**
조 건	ID · 패스워드 입력과 추가적 식별 및 인증기능(1.1.2)을 병행할 경우

참고 사항

① 이 보안요구사항은 1.1.2에 해당하는 기기가 제품에 연결되어 추가적인 식별 및 인증기능을 수행할때 적용할 수 있다.

- 제품이 1.1.2를 지원한다는 사실만으로 적용할 수 없고, 기기가 제품에 설치 또는 연결되어 추가적인 식별 및 인증기능을 수행해야 한다.

〈 표 2. 패스워드 보안성 기준 유형(2) 〉

구분	내용	비고
준수 사항	6자리 이상의 길이 확보	필수
	숫자, 대문자(영문), 소문자(영문), 특수문자가 각 1개 이상 포함	선택
금지 항목	사용자 계정(ID)과 동일한 패스워드 설정 금지	필수
	동일한 문자 · 숫자의 연속적인 반복입력 금지	선택
	키보드상의 연속된 문자 또는 숫자의 순차적 입력금지	선택
	직전 사용된 패스워드 재사용 금지	선택
	3개월 이내 사용된 패스워드 재사용 금지	선택

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.)

1.3.3

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 *인증서버 연동 사전공유키, SNMP 인증 · 암호화 패스워드 등*이 될 수 있다.

② 외부 IT실체 인증에 패스워드가 사용되는 경우 1.3.1 또는 1.3.2의 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 시험자는 제품과 외부 IT실체가 연동하기 위해 제품이 인증해야 하는 외부 IT실체를 모두 조사하고 인증에 필요한 인증 정보를 설정하는 인터페이스가 제공되는지 확인해야 한다.

② 시험자는 외부 IT실체를 인증하는데 사용되는 인증 정보가 제품이 통제하는 저장소에 저장되는 경우 '3.2 저장 데이터 보호' 요구사항에 따라 안전하게 저장되는지 확인해야 한다.

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

1.4 인증 정보 재사용 방지

1.4.1

필수

제품은 사용자의 인증 정보가 재사용되는 것을 방지(*타임스탬프 사용, 세션 ID 암호화 등*)해야 한다.

요구항목

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

② 1.1.2에서 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.

1.5 인증 피드백 보호

1.5.1

필수

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

요구항목

① △1.1.1 △1.1.2 △1.3.1(또는 1.3.2)에서 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.

참고 사항

① 에이전트 또는 클라이언트와 같이 엔드포인트에 위치하는 제품의 구성요소를 통해 사용자 인증 정보를 입력하는 경우(예 : 일반사용자 식별 및 인증) 에이전트 또는 클라이언트에서 인증 피드백 보호 기능을 제공할 수 있으며 '엔드포인트 공통보안요구사항', '1.2 인증 피드백 보호'를 적용한다.

점검시 유의사항

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

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

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

1.5.2

필수

제품은 식별 및 인증 실패시, 실패 사유에 대한 피드백(*예 : 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.

2. 보안관리

인가된 관리자만이 제품의 보안기능 및 중요데이터에 대한 관리를 수행하도록 허용함으로써 제품이 안전하게 동작함을 보장하기 위한 요구사항을 만족하는지 확인한다.

여 백

2.1 보안관리 기능

2.1.1

필수

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

요구항목

① 보안관리 기능에 해당되는 것은 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.

② 제품이 구현해야 하는 보안관리 기능은 아래 〈표 3〉 과 같다.

〈 표 3. 제품이 구현해야 하는 보안관리기능 〉

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
보안 관리	관리접속 서비스 활성화, 비활성화	기능 제공시 필수
	에이전트 조회 – 상태, 버전, 적용 보안정책	에이전트 포함시 필수
	에이전트 보안정책 관리 – 정책설정, 정책전송	에이전트 포함시 필수
	외부 IT실체 접근을 위한 인증정보 설정	기능 제공시 필수

자체 보호	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	
안전한 세션 관리	사용자 세션 잠금, 종료 시간 설정	기능 제공시 필수
	(세션 잠금의 경우) 세션의 잠금 해제시 관리자 또는 개별 사용자 인증	
	사용자 동시 접속 세션수 설정	기능 제공시 필수
감사 기록	감사기록의 조회	
	감사 기록 손실 대응 관련 설정	기능 제공시 필수

점검시 유의사항

① 시험자는 제품에서 지원하는 모든 보안관리 기능을 조사해야 한다.

- 시험자는 제품이 제공하는 모든 보안관리 기능이 제출문서(예: 보안기능 운용 설명서)에 기술되어 있는지 확인해야 한다.
- 시험자는 모든 보안관리 기능이 요구사항에 따라 정상동작 하는지 확인해야 한다.

② 보안관리 기능은 권한을 가진 관리자만 실행할 수 있는지 확인해야 한다.

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

2.2 관리접속 기능

2.2.1

필수

제품은 모든 관리접속에 대해 활성화 · 비활성화 기능을 제공해야 한다.

점검시 유의사항

① 시험자는 제품에서 지원하는 모든 관리접속을 조사해야 한다.

② 제품에서 제공하는 기능을 이용하여 관리접속을 비활성화 한 후, 제품 외부에서 포트스캔을 수행하여 열린 포트가 존재하는지 확인해야 한다.

③ 시험자는 제품에서 관리접속이 암호통신만을 사용하는지 확인해야 한다.

④ 소프트웨어 제품과 같이 제품이 하나의 관리접속만을 제공하는 경우 '해당사항 없음'으로 판정한다.

2.3 보안관리용 IP제한

2.3.1

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(예 : *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 IP 미등록시 모든 IP에서 접속을 허용하지 않는지 확인해야 한다.

④ 관리 용도 대신에 읽기 권한만 가지는 관리자(예 : *모니터링 관리자 등*)가 접속 가능한 PC는 추가로 등록 가능하다.

2.4 기본(default) 패스워드 등의 관리

2.4.1

필수

제품은 최초 제품 접속(관리 접속, 로컬 접속)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 · 로컬접속이 가능해야 한다.

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

- 패스워드는 1.3.1 또는 1.3.2의 보안성 기준을 준수해야 한다.

③ 기본(default) 계정(ID)이 없는 경우, 신규 계정(ID)을 생성해야 하며, 이후 제품의 관리 접속 · 로컬 접속이 가능해야 한다.

점검시 유의사항

① 시험자는 제품에서 지원하는 모든 관리접속(*SSH, HTTPS 등*), 로컬접속에 대해 조사해야 한다.

② 최초 접속이 로컬접속으로 제한되어 있고 관리자 생성 이후 다른 관리접속이 가능한 경우 이 항목을 '만족'으로 처리한다.

2.4.2

조건부 필수

제품은 내부 구성요소 또는 외부 IT실체에 접근하기 위해 사용하는 기본(default) 패스워드 변경 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 1.3.1 또는 1.3.2의 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 시험자는 기타 인증 정보가 필요한 제품 내에 존재하는 또는 제품과 연동하는 인증서버, DBMS · 웹서버 · WAS서버 등에 대해 조사해야 한다.

② 시험자는 인증 정보가 패스워드인 경우 1.3.1 또는 1.3.2의 보안성 기준을 만족하는지 확인해야 한다.

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

2.4.3

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 1.3.2의 보안성 기준을 준수할 것을 권고 한다.

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

점검시 유의사항

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

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

③ 시험자는 인증 정보가 패스워드인 경우 1.3.2의 보안성 기준을 만족하는지 확인해야 한다.

2.5 에이전트 관리

2.5.1

조건부 필수

제품은 에이전트에 대한 정보를 조회할 수 있는 기능을 제공해야 한다.

조 건	제품에 에이전트가 포함된 경우

요구항목

① 에이전트에 대한 조회 필수 정보는 다음과 같다.

- 에이전트 버전, 에이전트에 적용된 보안정책, 에이전트 동작상태(활성화 · 비활성화), 에이전트 무결성 검증결과(성공 · 실패).

② 에이전트에 대한 부가적인 정보는 다음과 같다.

- *에이전트 부가속성, 기타(에이전트가 설치된 관리대상 시스템 운영체제 정보, IP 정보, 기타 정보 등) 등.*

2.5.2

조건부 필수

제품은 인가된 관리자만 에이전트 삭제(uninstall)를 설정할 수 있는 기능을 제공해야 한다.

조 건	제품에 에이전트가 포함되고 관리자가 서버에서 에이전트 삭제 설정 기능을 제공하는 경우

요구항목

① 관리자가 에이전트 삭제 허용시 에이전트를 사용하는 일반사용자가 에이전트를 삭제할 수 있다.

② 관리자가 에이전트 삭제를 설정하는 기능의 예시는 다음과 같다.

- *관리자가 서버에서 에이전트 삭제 허용 · 차단 설정, 삭제키 설정 등.*

점검시 유의사항

① 이 요구사항은 사용자 단말에 설치되는 에이전트에 적용한다.

2.5.3

조건부 필수

제품은 중앙에서 보안정책을 관리하고 에이전트로 서버의 보안정책을 강제 적용하는 기능을 제공해야 한다.

조 건	제품에 에이전트가 포함된 경우

요구항목

① 제품에 에이전트가 포함된 경우 서버가 중앙에서 정책을 관리해야 하며 에이전트 자체의 보안관리 기능 유무에 관계없이 서버의 보안정책을 강제할 수 있어야 한다.

② 에이전트 자체에 보안관리 기능이 존재하는 경우 서버에서 에이전트의 설정 기능을 활성화 · 비활성화 할 수 있어야 한다.

3. 데이터 보호

제품 구성요소간에 전송되는 데이터 및 제품과 외부 IT실체 간에 전송되는 데이터를 노출 · 변경으로부터 보호하기 위해 안전한 암호통신을 지원(기밀성, 무결성) 하는지 확인해야 한다. 제품은 저장소에 저장되는 보안기능 관련 데이터를 비인가된 노출로부터 보호해야 한다.

3.1 전송 데이터 보호

3.1.1

필수

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

요구항목

① 안전한 암호통신을 위해서 표준 프로토콜을 사용하여 기밀성과 무결성을 제공해야 한다.

- 안전한 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 '8. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

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

② 3.1.1 항목과 각 제품의 보안요구사항에 정의된 보안요구사항이 일치하지 않는 경우(예: 가상사설망 제품의 게이트웨이와 클라이언트간 통신), 제품 보안요구사항이 우선한다.

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

④ 제품이 에이전트, 서버 이외 다른 구성요소를 갖는 경우, 모든 구성요소간 전송 데이터를 암호화하여 전송하는지 확인해야 한다.

⑤ 물리적으로 분리된 곳에서 운용가능한 제품 구성요소가 없을 경우, '해당사항 없음'으로 판정한다.

3.1.2

필수

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

요구항목

① 안전한 암호통신을 위해서 표준 프로토콜을 사용하여 기밀성과 무결성을 제공해야 한다.

- 안전한 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 '8. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

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

② 공통보안요구사항 항목과 제품 보안요구사항 항목이 상충하는 경우, 제품 보안요구사항이 우선한다.

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

3.1.3

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

요구항목

① 안전한 암호통신을 위해서 표준 프로토콜을 사용하여 기밀성과 무결성을 제공해야 한다.

- 안전한 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 '8. 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 제품에서 온라인 업데이트 지원시 이 요구사항에 따라 안전한 암호통신을 수행하는지 확인해야 한다.

③ 다만, 외부 IT실체중에서 NTP 서버와의 통신에는 이 요구사항을 적용하지 않는다.

④ syslog를 지원하면 *syslog over TLS(RFC 5424), syslog over DTLS(RFC 6012) 등*을 통해 암호화 전송을 지원해야 한다.

3.2 저장 데이터 보호

3.2.1

필수

제품은 중요정보를 제품 내부에 저장할 때 안전한 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 '8.2 암호키 생성' 및 '8.3 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 복호화 되지 않도록 일방향 암호(해시)를 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.(최소1000회 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 등을 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 '보안기능 시험' 제도의 경우, 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 '8. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

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

② 하드웨어 일체형 제품에 저장된 모든 중요정보는 읽거나 유추할 수 없어야 한다.

③ 난수발생기는 '8. 암호 지원' 요구사항에 따라 국내 · 외 표준을 준수하여 구현된 것이어야 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 '8. 암호 지원' 요구사항에 따라 암호키가 저장되는지 확인해야 한다.

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

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

3.2.2

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 보호해야 하며, 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 '8. 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.

- 예 : 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 안전하게 암호화하여 보호하는 기능을 제공하는 것도 요구사항 '만족'으로 판정이 가능하다.

② 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '8. 암호 지원' 요구사항을 만족해야 한다.

4. 자체보호

제품은 보안기능의 정상적인 작동을 보장하기 위해서 주기적 또는 관리자 요청이 있을 때마다 자체시험을 수행할 수 있어야 한다. 보안기능을 제공하는 메커니즘 및 데이터의 무결성을 확인하여 제품의 보안기능을 보호해야 한다.

'서버 공통보안요구사항'의 자체 보호 기능은 제품에서 서버의 업데이트 파일뿐만 아니라 제품에 포함되는 물리적으로 분리된 구성요소에도 적용하기 위한 것이다. 다만, '엔드포인트 공통보안요구사항' 적용 대상이 되는 에이전트 또는 클라이언트에 적용하는 자체 보호 관련 보안기능은 제품 유형에 따라 다를 수 있으며 '엔드포인트 공통보안요구사항'을 참조한다.

4.1 보안기능 자체 시험

4.1.1

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(*예 : 오류, 정지 등*)로 인하여 제품의 보안 기능에 영향을 미치는 경우 해당 실체는 자체시험 대상으로 반드시 포함해야 한다.

④ 자체시험 수행 이력은 *화면 출력, 감사기록*을 통해 확인할 수 있어야 한다.

⑤ 하드웨어 일체형 제품은 아래 요구사항을 만족해야 한다.

- 제품 시작시 및 운영중 제품 범위에 포함되는 하드웨어(*예 : 메모리, 플래쉬, NIC 등*) 및 소프트웨어(*예 : 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 기본적으로 물리적으로 분리된 제품 구성요소 모두에 대해 확인해야 한다.

② 하드웨어 · 운영체제는 하드웨어 일체형 제품일 경우 제품 범위에 포함되며 소프트웨어 제품일 경우 포함되지 않는다.

③ 시험자는 제출물에 자체시험에 대해 상세히 기술되어 있는지 확인한다.

4.1.2

필수

제품의 자체시험 결과가 실패인 경우 대응기능을 수행해야 한다.

요구항목

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

② 자체시험 결과에 대한 감사기록을 생성해야 한다.

③ 자체시험 결과 실패시 수행하는 대응기능의 예는 다음과 같다.

- *프로그램 실행중단, 경고메시지 화면 출력, 프로세스 재구동 등.*

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, ‘2.1 보안관리’ 요구사항에 따라 시험을 수행해야 한다.

4.2 무결성 검증

4.2.1

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 제품 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(*예 : 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 '보안기능 시험' 제도의 경우, 신청업체는 제품이 지원하는 무결성 검증 기능에 대한 상세한 설명자료(「보안기능 구현명세서」)를 제출해야 한다.

⑦ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '8. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 시험자는 제품의 무결성 검증 대상 및 동작 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 안전하게 보호되는지 확인해야 한다.

④ 시험자는 제품의 무결성 검증을 위한 데이터가 저장될 때 '3.2 저장 데이터 보호' 요구사항에 따라 안전하게 저장되는지 확인해야 한다.

4.2.2

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 '8. 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.

4.2.3

필수

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

요구항목

① 무결성 검증 내용 및 결과는 *화면 출력, 감사기록*을 통해 확인할 수 있어야 한다.

참고 사항

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.

4.2.4

필수

제품은 무결성 검증 실패인 경우 대응기능을 수행해야 한다.

요구항목

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

② 무결성 검증 결과에 대한 감사기록을 생성해야 한다.

③ 무결성 검증 결과 실패시 수행하는 대응 기능의 예는 다음과 같다.

– *프로그램 실행중단, 경고메시지 화면 출력 등.*

④ 관리자가 대응기능을 설정할 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 설정 기능이 있는 경우, '2.1 보안관리' 요구사항에 따라 시험을 수행해야 한다.

5. 업데이트 보호

제품은 제품 설치 파일(예 : 제품 패치파일), 제품 운영에 필요한 파일(예 : 탐지규칙 등) 등 '업데이트 파일'을 온라인으로 수신하여 설치 또는 적용하거나 매체에 저장하여 수동으로 설치 또는 적용하는 기능을 제공할 수 있다. 제품이 온라인 업데이트 기능을 이용, 외부에 존재하는 업데이트 서버로부터 업데이트 파일을 수신하는 경우 '3.1 전송 데이터 보호'에 따라 기밀성과 무결성이 제공되는 암호통신 채널을 통해 업데이트 파일을 수신해야 한다.

제품은 △온라인으로 수신 △매체에 수동으로 저장하여 전달받은 업데이트 파일을 설치하거나 적용하기 전에 업데이트 파일에 대한 유효성 검증을 수행해야 한다.

'서버 공통보안요구사항'의 업데이트 보호 관련 보안요구사항은 제품에서 서버의 업데이트 파일에 적용하기 위한 것이다. '엔드포인트 공통보안요구사항'의 적용 대상인 에이전트 또는 클라이언트에 요구되는 업데이트 보호 관련 보안요구사항은 제품 유형에 따라 다를 수 있으며 '엔드포인트 공통보안요구사항'을 참조한다.

5.1 안전한 업데이트

5.1.1

조건부 필수

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

조 건	업데이트 기능 제공시

요구항목

① 제품이 온라인 업데이트 또는 수동 업데이트 기능을 제공하는 경우, 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(유효기간 1년 이내) 검증을 수행해야 한다.

④ 암호 알고리즘 및 암호키 안전성은 '8. 암호 지원' 요구사항을 만족해야 한다.

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

참고 사항

① '엔드포인트 공통보안요구사항' 적용 대상이 되는 에이전트 또는 클라이언트의 업데이트 파일의 안전한 업데이트 관련 보안요구사항은 '엔드포인트 공통보안요구사항', '6. 안전한 업데이트 및 파일 배포'를 참조한다.

점검시 유의사항

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

- Windows® 운영 체제 PC의 에이전트에 온라인 업데이트 기능을 포함하는 제품은 '엔드포인트 공통보안요구사항'을 적용하며, 업데이트 파일의 전자서명 검증을 수행해야 한다.

② 업데이트 설치 · 수행을 인가된 관리자로 제한하는지 확인해야 한다.

5.1.2

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.

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

④ 하드웨어 일체형 제품의 경우 제품 식별 정보 외에 펌웨어의 유일한 식별 정보를 제품 인터페이스를 통해 사용자가 확인할 수 있어야 한다.

점검시 유의사항

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

5.1.3

조건부 필수

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

조 건	업데이트 기능 제공시

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.

6. 안전한 세션 관리

제품은 사용자가 오랫동안 세션을 사용하지 않을 경우 제3자 정보 유출 방지를 위해 세션을 잠그거나 종료해야 한다. 제품은 사용자 인증 데이터 재사용 등의 위협이 존재할 수 있으므로 동시 접속 세션의 제한 기능을 제공하여야 한다.

6.1 세션 잠금 · 종료 기능

6.1.1

필수

제품은 사용자 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 관리접속, 로컬접속에 적용해야 한다.

참고 사항

① 모니터링만 수행하는 관리자 계정에 대해서는 적용하지 않을 수 있다.

점검시 유의사항

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

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

6.2 동시접속 세션 제한

6.2.1

필수

제품은 동일한 사용자 계정 또는 동일 권한으로 제품에 중복 접속 하는 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 모니터링만 수행하는 관리자 계정에 대해서는 중복 로그인을 허용할 수 있다.

점검시 유의사항

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

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

7. 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.

7.1 감사기록 생성

7.1.1

필수

제품은 주요 감사사건에 대해 감사기록을 생성해야 한다.

요구항목

① 반드시 감사기록을 생성해야 하는 감사사건은 아래 〈표 4〉와 같다.

〈 표 4. 필수 기록되어야 할 주요 감사사건 〉

소분류	감사사건	추가적인 감사정보
식별 및 인증	사용자의 로그인, 로그아웃	
	사용자 등록, 변경, 삭제	
	사용자 인증 시도의 한계치 도달시 대응행동	
	패스워드에 대한 모든 변경	
보안 관리	〈표 3〉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	

안전한 세션 관리	사용자의 세션 잠금 또는 종료	
	동일 계정의 중복 로그인 시도 탐지시 대응행동	
	동시세션 수 제한에 기반한 새로운 세션 거부	
암호키 생성	암호 키 생성 실패	
암호 사용	암호 연산 실패(암호 연산 유형 포함)	
감사 기록	하드웨어 일체형 제품의 감사기능 시작과 종료	

② 기능 제공시 감사기록을 생성해야 하는 감사사건은 아래 〈표 5〉와 같다.

〈 표 5. 기능 제공시 기록할 수 있는 주요 감사사건 〉

소분류	감사사건	추가적인 감사정보
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	
보안관리	에이전트 등록상태 변화	

점검시 유의사항

① 시험자는 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.

④ 〈표 3〉에 정의된 관리접속 서비스가 활성화 또는 비활성화 될 경우, 구현된 모든 프로토콜에 대해서 감사기록을 생성해야 한다.

7.1.2

필수

감사기록은 필요 이상의 정보가 포함되지 않아야 한다.

요구항목

① 감사기록에 최소한 포함되어야 하는 항목은 다음과 같다.

- 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원(*예 : 계정, 프로세스, IP 등*), 사건의 결과(성공 · 실패).

② 인증 정보(예 : *패스워드 등*), 암호키 등의 정보는 감사기록내에 저장하지 않아야 한다.

7.1.3

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 시험자는 제품에서 사용하는 시간정보, 동기화 설정 방법 등을 조사해야 한다.

- 제품 구성요소간 시간 동기화를 반드시 구현할 것을 요구하지는 않는다.

7.2 감사기록 조회

7.2.1

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(예: 패스워드, 주민등록번호 등)는 기록되지 않거나 기록이 불가피할 경우, 마스킹으로 처리하여 생성해야 한다.

점검시 유의사항

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

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

7.2.2

필수

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

점검시 유의사항

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

7.2.3

조건부 필수

제품은 WAS의 로그에 중요 정보가 포함되지 않도록 구현해야 한다.

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

요구항목

① WAS 자체 로그를 남기지 않고 제품의 감사기록 저장소에만 로그를 남기도록 구현 가능하다.

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

7.3 감사기록 보호

7.3.1

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 보호할 수 있도록 지원할 수 있다.

- 예: 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 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 감사기록을 실시간으로 외부 실체에 전송하여 저장하는 경우 만족하는 것으로 간주한다.

7.3.2

선택

제품은 감사기록을 제품 내부에 저장할 경우 안전하게 암호화하여 저장해야 한다.

요구항목

① 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '8. 암호 지원' 요구사항을 만족해야 한다.

7.4 감사기록 손실 예측시 대응행동

7.4.1

필수

제품은 감사기록의 크기가 미리 정의된 용량에 도달하는 경우 *관리자에게 통보 등* 대응행동을 수행해야 한다.

요구항목

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

② 관리자에게 통보하는 기능을 필수적으로 제공해야 하며, 기능의 예는 다음과 같다.

- *화면 알람, 관리자 이메일 발송 등.*

③ 감사기록 손실 대응관련 관리자에게 통보하는 조건의 예는 다음과 같다.

- *설정된 디스크 용량 90% 이상, 100MB 이상 등.*

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 '8. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

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

점검시 유의사항

① 관리자에게 통보하기 위한 조건을 고정값으로 지원하는 것도 가능하다.

7.5 감사기록 손실 방지

7.5.1

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 예는 다음과 같다.

- *가장 오래된 감사기록 덮어쓰기, 감사기록 압축 저장 등.*

참고 사항

① 감사기록을 로컬 저장소에 저장시 적용하며, 로컬 저장소 저장 유무에 관계없이 감사기록을 실시간으로 외부 실체에 전송 · 저장시 만족하는 것으로 간주한다.

8. 암호지원

제품은 데이터의 저장 · 전송시 보호를 위해 사용되는 암호화 및 해시 알고리즘은 국가 · 공공기관이 요구하는 보안강도를 만족해야 한다. 또한 암호화를 사용하는 모든 보안기능은 '8. 암호 지원'의 요구사항을 만족하도록 구현해야 한다. 제품 관리 또는 구성요소간 전송 데이터 보호를 위해 사용하는 암호통신 프로토콜 또는 관리자 패스워드 등 저장시 암호화에 필요한 암호키 생성 등에 적용한다.

8.1 암호사용

8.1.1

필수

중요 정보 전송 및 저장시 권고 암호 알고리즘을 사용해야 한다.

요구항목

① 권고 암호 알고리즘은 보안강도가 112bit 이상인 표준 알고리즘으로 〈별표 1〉을 참고하며, 예는 다음과 같다.

- *해시 : SHA-224 이상.*
- *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, K-283, 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 않아야 한다.

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 bit급 이상 암호알고리즘의 세부 사항은 「암호 알고리즘 및 키 길이 이용 안내서」(과학기술정보통신부, 2018), 「소프트웨어 암호모듈 검증기준」, 「NIST SP 800-131Ar2」를 참고한다.

점검시 유의사항

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

② 패스워드는 일방향 해시 알고리즘을 사용하여 암호화 해야 하며, 동일한 평문 입력을 반복하여도 매 번 다른 값이 출력되어야 한다.

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

8.2 암호키 생성

8.2.1

필수

제품은 암호키를 안전한 방식으로 생성해야 한다.

요구항목

① 안전한 암호키 생성 방식의 예는 다음과 같다.

- *패스워드 기반 키 유도(PKCS#5 v2.1(RFC 8018), NIST SP 800-132 등).*
- *사전 공유된 키로 키 유도(TTAK.KO-12.0272) .*
- *난수발생기 이용 키 생성(CTR_DRBG, HASH_DRBG, HMAC_DRBG 등).*

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) 생성에 필요한 초기 데이터(예 : *패스워드 등*)는 직접 입력받거나 스마트카드, 보안USB, 보안토큰(HSM : Hardware Security Module) 등 저장 매체에 저장된 값을 주입하여 사용할 수 있다.
- 저장 매체는 보안기능 확인서 또는 국내 · 외 CC인증서를 획득한 제품을 사용할 것을 권고한다.
- 세부 사항은 「암호 키 관리 안내서」(미래창조과학부, 2014) 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.

참고 사항

① 패스워드는 4자리 이상인지 확인한다.

② salt 값은 비밀일 필요는 없으며, 안전한 난수발생기를 이용하여 생성하고 크기는 최소 128bit 이상이어야 한다.

③ iteration count는 가능한 큰 값을 적용해야 한다.(최소1000회 이상)

점검시 유의사항

① 시험자는 제품이 제공하는 암호키 생성 방식(표준, 난수발생기 등)이 안전한 방식인지 조사해야 한다.

② 제품에서 외부의 3rd Party Library나 오픈소스를 사용한 경우 사용 소프트웨어 이름, 버전 정보를 확인해야 한다.

③ 제품이 패스워드 기반 키 유도 기능을 구현한 경우, 사용자 인터페이스 확인, 디버깅 시험 등을 통해 안전하게 구현하였는지 확인해야 한다.

8.3 암호키 저장

8.3.1

필수

제품은 암호키를 안전한 방식으로 저장해야 한다.

요구항목

① 데이터 암호화 키(DEK)는 키 암호화 키(KEK : Key Encryption Key)를 사용, 암호화하여 저장할 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〉과 같이 제품에서 저장 및 전송시 사용하는 모든 암호키를 식별하여 키 저장 및 파기 방법에 대한 목록과 설명자료를 제출하여 안전성을 입증해야 한다.

〈 표 6. 암호키 저장 및 파기 방법 〉

암호키 종류	키 저장 및 파기 방법
TLS 개인키	o 형태 : RSA Private Key o 생성주체 : 제품에서 생성 o 저장 · 보호 : 제품 내부 저장 · 저장 영역 비인가자 접근 차단 o 파기 : 키 파기 명령 실행시 0, 1로 3회 덮어씀
TLS 세션 암호화 키	o 형태 : ARIA Key o 생성주체 : 제품에서 생성 o 저장 · 보호 : 메모리(RAM)에만 저장 o 파기 : 세션 종료시 0, 1로 3회 덮어씀
TLS 세션 무결성 검사키	o 형태 : HMAC Key o 생성주체 : 제품에서 생성 o 저장 · 보호 : 메모리(RAM)에만 저장 o 파기 : 세션 종료시 0, 1로 3회 덮어씀

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.

참고 사항

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

점검시 유의사항

① 시험자는 위 표와 같이 제품에서 사용되는 모든 암호키를 조사하고, 키 저장 및 파기 방법에 대해 안전한 방식인지 확인해야 한다.

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

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

여 백

8.4 암호키 파기

8.4.1

필수

제품은 제품에서 생성하거나 사용한 암호키를 안전하게 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 '1'의 값으로 3회 이상 덮어쓰기하는 방식을 이용할 수 있다.

③ 세부 사항은 「암호 키 관리 안내서」(미래창조과학부, 2014) 암호키 파기 방법을 참고한다.

점검시 유의사항

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

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

9. 취약성 대응

제품은 존재하는 알려진 취약점들을 제거해야 한다. 제품을 안전하게 설정하고 운용할 수 있어야 한다.

9.1 소스코드 보안약점 제거

9.1.1

선택

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

요구항목

① 소프트웨어 개발 단계에서 보안약점을 최소화하여 안전하게 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」(행정자치부, 2019.11)를 참고한다.

점검시 유의사항

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

② CC인증 또는 성능평가를 받은 소스코드 보안약점 진단도구를 이용, 제품에 대해 독립적인 보안약점 점검을 수행해야 한다.

③ 에이전트를 포함하여 모든 제품 구성요소에 대하여 시험을 수행한다.

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

9.2 알려진 취약점 제거

9.2.1

조건부 필수

제품 내부에 알려진 보안취약점을 확인하고 제거해야 한다.

조 건	'보안기능 시험' 신청 제품일 경우

요구항목

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

- 하드웨어 일체형 제품인 경우 제품에 포함되는 커스터마이즈 운영체제에 취약점이 확인된 낮은 버전의 커널(예 : *Linux® 2.x*) 을 사용하지 않는 것을 권고한다.

참고 사항

① '국내용 CC인증서' 를 신청한 제품은 「정보보호제품 평가 · 인증 수행규정」에서 정한 평가기준 및 평가방법론 등에 따라 '취약성 평가'를 수행하므로 해당되지 않는다.

점검시 유의사항

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

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

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

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

9.3 불필요한 서비스 제거

9.3.1

조건부 필수	제품 내부에 불필요한 서비스가 실행중이면 이를 확인하고 제거해야 한다.
조 건	'보안기능 시험' 신청한 하드웨어 일체형 제품인 경우

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.

참고 사항

① '국내용 CC인증서'를 신청한 제품은 「정보보호제품 평가 · 인증 수행규정」에서 정한 평가기준 및 평가방법론 등에 따라 '취약성 평가'를 수행하므로 해당되지 않는다.

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 〉

권고 암호 알고리즘

분류	암호 알고리즘		참조 표준
블록암호	ARIA	o 운영모드 - 기밀성(ECB, CBC, CFB, OFB, CTR) - 기밀성/인증 (CCM, GCM)	o [KS X 1213-1] 128비트 블록 암호 알고리즘 ARIA - 제1부: 일반 (2014) o [KS X 1213-2] 128비트 블록 암호 알고리즘 ARIA - 제2부: 운영모드 (2014) o [TTAK.KO-12.0271-Part1/R1] n비트 블록 암호 운영 모드 - 제1부 일반(2016) o [TTAK.KO-12.0271-Part3] n비트 블록 암호 운영 모드 - 제3부: 블록 암호 ARIA (2017) o [IETF RFC 5794] A Description of the ARIA Encryption Algorithm (2010)
	SEED	o 운영모드 - 기밀성(ECB, CBC, CFB, OFB, CTR) - 기밀성/인증 (CCM, GCM)	o [KS X ISO/IEC 18033-3] 암호 알고리즘 - 제3부: 블록암호(2018) o [TTAS.KO-12.0004/R1] 128비트 블록 암호 알고리즘 SEED (2005) o [TTAK.KO-12.0271-Part1/R1] n비트 블록 암호 운영 모드 - 제1부 일반(2016) o [TTAK.KO-12.0271-Part4] n비트 블록 암호 운영 모드 - 제4부: 블록 암호 SEED (2017) o [ISO/IEC 18033-3] Information technology - Security techniques - Encryption - Part 3: Block ciphers (2010)
	LEA	o 운영모드 - 기밀성(ECB, CBC, CFB, OFB, CTR) - 기밀성/인증 (CCM, GCM)	o [KS X 3246] 128비트 블록암호 알고리즘 LEA (2016) o [TTAK.KO-12.0223] 128비트 블록 암호 알고리즘 LEA (2013) o [TTAK.KO-12.0271-Part1/R1] n비트 블록 암호 운영 모드 - 제1부 일반(2016) o [TTAK.KO-12.0271-Part2/R1] n비트 블록 암호 운영 모드 - 제2부: 블록 암호 LEA (2017) o [ISO/IEC 29192-2] IT Security techniques - Lightweight cryptography - Part 2: Block ciphers (2019)
	HIGHT	o 운영모드 - 기밀성(ECB, CBC, CFB, OFB, CTR)	o [KS X ISO/IEC 18033-3] 암호 알고리즘 - 제3부: 블록암호(2018) o [TTAS.KO.12.0040/R1] 64비트 블록 암호 알고리즘 HIGHT (2008) o [TTAK.KO-12.0271-Part1/R1] n비트 블록 암호 운영 모드 - 제1부 일반(2016) o [TTAK.KO-12.0271-Part5/R1] n비트 블록 암호 운영 모드 - 제5부: 블록 암호 HIGHT (2017) o [ISO/IEC 18033-3] Information technology - Security techniques - Encryption - Part 3: Block ciphers (2010)
해시함수	SHA-2	SHA-224/256/384/512	o [KS X ISO/IEC 10118-3:2001] 해시함수 - 제3부 전용 해시함수(2018) o [ISO/IEC 10118-3] IT Security techniques - Hash-functions - Part 3: Dedicated hash-functions (2018)

해시함수	LSH	LSH-224/256/384/512/512-224/512-256	o [KS X 3262] 해시함수 LSH (2018) o [TTAK.KO-12.0276] 해시 함수 LSH (2015)
	SHA-3	SHA3-224/256/384/512	o [ISO/IEC 10118-3] IT Security techniques - Hash-functions - Part 3: Dedicated hash-functions (2018)
메시지 인증	해시 함수 기반	HMAC	o [KS X ISO/IEC 9797-2] 메시지 인증 코드 - 제2부: 전용 해시 함수를 이용한 메커니즘 (2018) o [TTAK.KO-12.0330-Part1] 해시 함수 기반 메시지 인증코드(HMAC) - 제1부: 일반 (2018) o [TTAK.KO-12.0330-Part2] 해시 함수 기반 메시지 인증코드(HMAC) - 제2부: 해시 함수 SHA-2 (2018) o [TTAK.KO-12.0330-Part3] 해시 함수 기반 메시지 인증코드(HMAC) - 제3부: 해시 함수 LSH (2018) o [TTAK.KO-12.0330-Part4] 해시 함수 기반 메시지 인증코드(HMAC) - 제4부: 해시 함수 SHA-3 (2019) o [ISO/IEC 9797-2] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function (2011)
	블록 암호 기반	CMAC, GMAC	o [KS X ISO/IEC 9797-1] 메시지 인증 코드 - 제1부: 블록 암호를 이용한 메커니즘 (2018) o [KS X ISO/IEC 19772] 인증된 암호화 (2014) o [TTAK.KO-12.0271-Part1/R1] n비트 블록 암호 운영 모드 - 제1부 일반 (2016) o [TTAK.KO-12.0271-Part2/R1] n비트 블록 암호 운영 모드 - 제2부: 블록 암호 LEA (2017) o [TTAK.KO-12.0271-Part3] n비트 블록 암호 운영 모드 - 제3부: 블록 암호 ARIA (2017) o [TTAK.KO-12.0271-Part4] n비트 블록 암호 운영 모드 - 제4부: 블록 암호 SEED (2017) o [TTAK.KO-12.0271-Part5] n비트 블록 암호 운영 모드 - 제5부: 블록 암호 HIGHT (2017) o [ISO/IEC 9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher (2011) o [ISO/IEC 19772] Information technology - Security techniques - Authentication encryption (2009)

난수발생기	해시 함수 기반	Hash_DRBG HMAC_DRBG	o [KS X ISO/IEC 18031] 난수발생기 (2018) o [TTAK.KO-12.0331-Part1] 해시 함수 기반 결정론적 난수발생기 - 제1부: 일반 (2018) o [TTAK.KO-12.0331-Part2] 해시 함수 기반 결정론적 난수발생기 - 제2부: 해시 함수 SHA-2 (2018) o [TTAK.KO-12.0331-Part3] 해시 함수 기반 결정론적 난수발생기 - 제3부: 해시 함수 LSH (2018) o [TTAK.KO-12.0331-Part4] 해시 함수 기반 결정론적 난수발생기 - 제4부: 해시 함수 SHA-3 (2019) o [TTAK.KO-12.0332-Part1] HMAC 기반 결정론적 난수발생기 - 제1부: 일반 (2018) o [TTAK.KO-12.0332-Part2] HMAC 기반 결정론적 난수발생기 - 제2부: 해시 함수 SHA-2 (2018) o [TTAK.KO-12.0332-Part3] HMAC 기반 결정론적 난수발생기 - 제3부: 해시 함수 LSH (2018) o [TTAK.KO-12.0332-Part4] HMAC 기반 결정론적 난수발생기 - 제4부: 해시 함수 SHA-3 (2019) o [ISO/IEC 18031] Information technology - Security techniques - Random bit generation (2011)
	블록 암호 기반	CTR_DRBG	[KS X ISO/IEC 18031] 난수발생기 (2018) [TTAK.KO-12.0189/R1] 결정론적 난수 발생기 -제1부- 블록 암호 기반 난수 발생기 (2015) [ISO/IEC 18031] Information technology - Security techniques - Random bit generation (2011)
공개키 암호	RSAES	공개키 길이: 2048, 3072 해시함수 : SHA-224, SHA-256	o [KS X ISO/IEC 18033-2] 암호 알고리즘 - 제2부: 비대칭형 암호 (2017) o [ISO/IEC 18033-2] Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers (2006) o [IETF RFC 8017] PKCS #1: RSA Cryptography Specifications Version 2.2 (2016)
전자서명	RSA-PSS	공개키 길이 : 2048, 3072 해시함수 : SHA-224, SHA-256	o [KS X ISO/IEC 14888-2] 부가형 디지털 서명 - 제2부: 정수 인수분해 기반 메커니즘 (2011) o [ISO/IEC 14888-2] IT Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms (2008) o [NIST FIPS 186-4] Digital Signature Standard (DSS) (2013) o [IETF RFC 8017] PKCS #1: RSA Cryptography Specifications Version 2.2 (2016)
	KCDSA	공개키 길이, 개인키 길이 : (2048, 224), (2048, 256) 해시함수 : SHA-224, SHA-256	o [KS X ISO/IEC 14888-3] 부가형 디지털 서명 - 제2부: 이산대수 기반 메커니즘 (2018) o [TTAK.KO-12.0001/R4] 부가형 전자 서명 방식 표준 - 제2부: 한국형 인증서 기반 전자 서명 알고리즘(KCDSA) (2016) o [ISO/IEC 14888-3] IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms (2018) o [NIST FIPS 186-4] Digital Signature Standard (DSS) (2013)

전자서명	EC-KCDSA	P-224, P-256, B-233, B-283, K-233, K-283 해시함수: SHA-224, SHA-256	o [KS X ISO/IEC 14888-3] 부가형 디지털 서명 - 제2부: 이산대수 기반 메커니즘 (2018) o [TTAK.KO-12.0015/R3] 부가형 전자 서명 방식 표준- 제3부: 타원 곡선을 이용한 한국형 인증서 기반 전자 서명 알고리즘 (EC-KCDSA) (2016) o [ISO/IEC 14888-3] IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms (2018) o [NIST FIPS 186-4] Digital Signature Standard (DSS) (2013)
	ECDSA	P-224, P-256, B-233, B-283, K-233, K-283 해시함수: SHA-224, SHA-256	o [KS X ISO/IEC 14888-3] 부가형 디지털 서명 - 제2부: 이산대수 기반 메커니즘 (2018) o [ISO/IEC 14888-3] IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms (2018) o [NIST FIPS 186-4] Digital Signature Standard (DSS) (2013)
키설정	DH	(공개키 길이, 개인키 길이): (2048, 224), (2048, 256)	o [KS X ISO/IEC 11770-3] 키 관리 - 제3부: 비대칭 기법을 이용한 메커니즘 (2018) o [TTAK.KO-12.0001/R4] 부가형 전자 서명 방식 표준 - 제2부: 한국형 인증서 기반 전자 서명 알고리즘(KCDSA) (2016) o [ISO/IEC 11770-3] Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques (2015)
	ECDH	P-224, P-256, B-233, B-283, K-233, K-283	o [KS X ISO/IEC 11770-3] 키 관리 - 제3부: 비대칭 기법을 이용한 메커니즘 (2018) o [ISO/IEC 11770-3] Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques (2015) o [NIST FIPS 186-4] Digital Signature Standard (DSS) (2013)
키유도	KBKDF	HMAC, CMAC	o [TTAK.KO-12.0272] 블록 암호 기반 키 유도 함수 (2015) o [TTAK.KO-12.0333-Part1] HMAC 기반 키 유도 함수 - 제1부: 일반 (2018) o [TTAK.KO-12.0333-Part2] HMAC 기반 키 유도 함수 - 제2부: 해시 함수 SHA-2 (2018) o [TTAK.KO-12.0333-Part3] HMAC 기반 키 유도 함수 - 제3부: 해시 함수 LSH (2018) o [TTAK.KO-12.0333-Part4] HMAC 기반 키 유도 함수 - 제4부: 해시 함수 SHA-3 (2019) o [ISO/IEC 11770-6] Information technology - Security techniques - Key management - Part 6: Key derivation (2016)
	PBKDF	HMAC	o [TTAK.KO-12.0334-Part1] 패스워드 기반 키 유도 함수 - 제1부: 일반 (2018) o [TTAK.KO-12.0334-Part2] 패스워드 기반 키 유도 함수 - 제2부: 해시 함수 SHA-2 (2018) o [TTAK.KO-12.0334-Part3] 패스워드 기반 키 유도 함수 - 제3부: 해시 함수 LSH (2018) o [TTAK.KO-12.0334-Part4] 패스워드 기반 키 유도 함수 - 제4부: 해시 함수 SHA-3 (2019)

※ 이 표에 기재된 암호 알고리즘뿐 아니라 보안강도가 112bit 이상인 국내 · 외 표준 암호 알고리즘을 사용할 수 있습니다.

〈 별 표 2 〉

제 · 개정 이력

일 자	주요 변경 내용	문서 버전
2021. 4. 2.	‘단독제품 기본보안요구사항’과 ‘관리서버 기본보안요구사항’을 ‘서버 공통보안요구사항’으로 통합, 개정	V3.0
2021. 9. 1.	o 다음 보안기능의 요구사항에 대해 설명 수정 및 추가 – 1.3.1, 1.3.2, 2.4.2 3.1.1, 3.1.3, 7.1.1	V3.0 R1

2장
엔드포인트 공통보안요구사항

1절 일반사항

1. 운용 환경 정의

■ 가정사항

○ ‘엔드포인트 공통보안요구사항’ 적용 대상인 제품 구성요소의 인가된 사용자는 악의가 없으며, 제품의 기능을 정확하게 이해하고 「제품 설명서」 또는 「보안 기능 운용설명서」에 따라 제품을 사용한다.

○ 제품의 인가된 사용자는 ‘엔드포인트 공통보안요구사항’ 적용 대상 제품의 구성요소 작동에 불필요한 운영체제상의 취약점에 대한 개선작업을 수행하여 운영체제의 신뢰성과 안전성을 보장한다.

■ 제품 보안요구사항의 적용

사용자의 호스트나 모바일 단말 등 엔드포인트에 위치하는 에이전트, 클라이언트와 같은 제품의 구성요소에 적용한다. 에이전트는 사용자의 호스트에 설치되어 서버로부터 보안정책을 전달받아 사용자의 호스트에 적용하는 역할을 수행하는 실체이다. 에이전트를 포함할 수 있는 제품 유형은 다음과 같이 그룹화 될 수 있다.

○ **에이전트 유형 1** : 안티바이러스 제품, 소프트웨어기반 보안USB 제품, 호스트 자료유출방지 제품 등

- 에이전트가 위치하는 엔드포인트는 일반적으로 조직 내의 직원이 접근 가능한

Windows® 운영체제가 설치된 PC이며, 에이전트가 손상되는 경우 사용자 호스트에 존재하는 데이터의 손상 및 유출이 가능하여 기밀성, 무결성, 가용성 측면에서 엄격하게 보안요구사항을 적용해야 하는 제품 유형에 해당한다.

○ **에이전트 유형 2** : 네트워크 접근통제 제품, 패치관리시스템 등

- 에이전트가 위치하는 엔드포인트는 일반적으로 조직 내의 직원이 접근 가능한 Windows® 운영체제가 설치된 PC이며, 에이전트가 손상되는 경우 사용자 호스트에 존재하는 데이터의 손상 및 유출이 발생할 가능성은 낮지만 사용자가 조직에서 제공하는 자원을 정상적으로 사용하는데 문제가 발생할 수 있어 기밀성, 무결성 측면에서 보안요구사항을 적용해야 하는 제품 유형에 해당한다.

○ **에이전트 유형 3** : 데이터베이스 접근통제 제품, 운영체제(서버) 접근통제 제품, 통합보안관리 제품 등

- 에이전트가 위치하는 엔드포인트가 일반적으로 조직의 인가된 직원만이 접근 가능한 물리적으로 안전한 환경이기 때문에 위협 발생 가능성이 상대적으로 낮은 제품 유형에 해당한다.

○ **에이전트 유형 4** : 스마트폰 보안관리 제품 등

- 에이전트가 위치하는 엔드포인트가 스마트폰 등 모바일 기기 유형에 해당한다. 단, 스마트폰 보안관리 제품은 '엔드포인트 공통보안요구사항'을 적용하지 않으며, '스마트폰 보안관리 제품 보안요구사항'만을 적용한다.

○ **클라이언트 유형** : 가상사설망 제품, 무선랜 인증제품 등

클라이언트는 사용자의 호스트에 설치되어 사용자를 대신하여 서버와의 통신을 요청하는 역할을 수행하는 실체이다.

'엔드포인트 공통보안요구사항'은 위와 같이 △에이전트 유형 1 △에이전트 유형 2 △에이전트 유형 3, △에이전트 유형 4 △클라이언트로 구분하여 제품 유형별로 적용할 수 있다. 위의 분류에 명시적으로 포함되지 않은 제품 유형에 '엔드포인트 공통보안요구사항'을 적용하려는 경우 에이전트나 클라이언트가 위치하는 엔드포인트의 물리적인 위치 및 위협 발생 가능성, 위협 발생시 보안에 미치는 영향 정도(기밀성, 무결성, 가용성 측면 분석) 등을 고려하여 결정할 수 있다.

2절 보안요구사항

1. 식별 및 인증

엔드포인트에 위치하는 제품 구성요소 중 에이전트는 서버로부터 보안정책 등을 수신하여 적용하므로 정책을 송신하는 서버에 대한 식별 및 인증이 필요하다.

일반사용자는 관리자가 설정한 보안정책에 따라 제품의 보안기능을 이용하는 사용자로, 제품 유형에 따라 제품에 포함된 에이전트 또는 클라이언트를 사용하여 제품의 보안기능을 이용할 수 있다. 일반사용자 식별 및 인증이 필요한 경우에는 일반적으로 '서버 공통보안요구사항' 적용 대상이 되는 제품의 구성요소 즉, 서버에서 식별 및 인증된 후 제품에 대한 접근이 인가된다. 이 경우 엔드포인트에 위치하는 에이전트 또는 클라이언트는 일반사용자 식별 및 인증을 위한 인터페이스를 제공하며, 인증 피드백을 보호하는 기능을 제공할 수 있다.

1.1 서버 식별 및 인증

1.1.1

조건부 필수

에이전트는 서버에 대한 식별 및 인증을 수행해야 한다.

조 건	제품 구성요소에 서버와 이로부터 보안정책을 수신하는 에이전트가 포함된 경우
적용 유형	유형 1, 유형 2, 유형 3

요구항목

① 에이전트는 정당한 서버임을 확인하기 위해 식별 및 인증을 수행해야 한다.

② 서버 식별정보에 서버 IP 주소, 도메인 이름 중 하나는 필수로 포함되어야 하며, 부가적인 식별정보를 사용할 수 있다.

③ 서버에 대한 인증방식은 *인증서 기반 방식 등*이 있다.

④ 인증서를 이용할 경우 인증서 유효성(유효기간 1년 이내) 검증을 수행해야 한다.

점검시 유의사항

① 인증서 기반의 인증기능을 제공하는 경우 인증서 유효성 검증 기능도 시험해야 한다.

1.2 인증 피드백 보호

1.2.1

조건부 필수

에이전트 또는 클라이언트는 사용자 인증시 입력되는 정보의 내용을 출력장치에 표시하지 않아야 한다.

조 건	에이전트 또는 클라이언트에서 인증 피드백 보호 기능 제공시
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 에이전트 또는 클라이언트에서 제공하는 인터페이스를 통해 입력된 인증 정보가 출력장치에 표시되지 않아야 한다.

- *예 : 입력 내용이 전혀 표시되지 않거나 입력 문자 대신 “*” 표시 등.*

② 사용자 로그인시 인증정보가 메모리 영역에 평문으로 노출되지 않아야 한다.

참고 사항

① 에이전트 또는 클라이언트에서 제공하는 인터페이스를 통해 인증 정보를 입력하더라도 서버에서 인증 피드백 보호 기능을 제공할 수 있으며, 이 경우 ‘서버 공통보안요구사항’의 ‘1.5 인증 피드백 보호’를 적용한다.

점검시 유의사항

① 사용자 로그인할 때 뿐 아니라 신규 사용자 계정 생성, 패스워드 변경 등 에이전트나 클라이언트에서 제공하는 인터페이스를 사용하여 인증정보를 입력하는 기능을 모두 식별하여 요구사항 만족여부를 확인해야 한다.

2. 보안관리

에이전트 또는 클라이언트는 자신의 보안관리 기능을 제공할 수 있다.

2.1 보안관리 기능

2.1.1

조건부 필수	에이전트 또는 클라이언트는 사용자가 자체의 보안기능, 보안정책 및 중요 데이터 등을 설정 · 관리할 수 있는 보안관리 기능을 제공해야 한다.
조 건	에이전트 또는 클라이언트에서 관리기능 제공시
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 제품 구성요소에 서버와 에이전트가 포함된 경우, 에이전트는 서버가 전송한 보안정책을 에이전트의 설정으로 강제 적용할 수 있어야 한다.

② 에이전트 또는 클라이언트가 제공하는 모든 보안관리 기능을 식별 · 기재한 문서를 제출해야 한다.

- ‘보안기능 시험’제도의 경우 「보안기능 구현명세서」에 해당 내용을 기술하고 ‘국내용 평가 · 인증’ 제도는 「설명서)」에 기술하여 제출한다.

3. 데이터 보호

에이전트 또는 클라이언트는 엔드포인트 저장소에 저장되는 보안기능 관련 데이터를 비인가된 노출로부터 보호해야 한다.

여 백

3.1 저장 데이터 보호

3.1.1

조건부 필수

에이전트 또는 클라이언트는 중요정보를 엔드포인트의 파일 시스템 또는 레지스트리에 저장하는 경우 암호화하여 저장해야 한다.

조 건	중요정보를 파일 시스템 또는 레지스트리에 저장할 경우
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 최소한 다음과 같은 중요정보를 제품이 저장하는 경우 암호화하여 저장해야 한다.

- 사용자 패스워드.
- 암호키(사전공유키, 대칭키, 개인키).

② 사용자 패스워드에는 에이전트 삭제키도 포함되며 패스워드는 일반적으로 복호화되지 않도록 일방향 암호화(해시)를 이용하여 저장해야 한다.

- 일방향 암호화 수행시 패스워드에 랜덤하게 생성한 비밀값(salt)을 추가하여 적용이 필요하다.
- salt 값은 비밀일 필요는 없으며, 난수발생기를 이용하여 생성하고 크기는 최소 48bit 이상이어야 한다.
- iteration count는 가능한 큰 값을 적용해야 한다.(최소1000회 이상)

③ 암호키는 사전공유키, 대칭키, 개인키 등을 의미하며 제품 관리접속 · 로컬 접속, 제품 구성요소간 연동 설정에 사용되는 키들이 모두 대상이다.

④ 암호화해서 저장해야 하는 최소한의 중요정보에 포함된 패스워드 및 암호키는 제품에 하드코딩하여 저장할 수 없다.

⑤ '보안기능 시험' 제도의 경우, 신청업체는 제품이 지원하는 저장 데이터 보호 방법에 대한 상세한 설명자료(보안기능 구현명세서)를 제출하여 안전성을 입증해야 한다.

⑥ 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 ‘서버 공통보안요구사항’, ‘8. 암호 지원’ 요구사항을 만족해야 한다.

⑦ 암호화를 제공하더라도 추가적인 파일 숨김 · 접근 통제 등의 보호를 권고한다.

참고 사항

① 암호키는 키 암호화 키(KEK, Key Encryption Key)를 사용, 암호화하여 저장해야 한다. 키 암호화 키(KEK, Key Encryption Key) 생성 및 저장 등과 관련된 요구사항은 ‘서버 공통보안요구사항’, ‘8.2 암호키 생성’ 및 ‘8.3 암호키 저장’ 요구사항을 만족해야 한다.

② 난수발생기는 ‘서버 공통보안요구사항’, ‘8. 암호 지원’ 요구사항에 따라 국내 · 외 표준을 준수하여 구현된 것이어야 한다.

점검시 유의사항

① 삭제키 기능을 제공하는 제품의 경우, 삭제키는 패스워드와 동일하게 3.1.1의 요구항목을 적용하여 시험을 수행한다.

- 삭제키는 에이전트사용자가 에이전트를 제거(uninstall)할 때 사용하는 비밀번호이다.
- 삭제키 생성시 패스워드와 동일한 보안성 기준을 만족하도록 권고한다. 선택적으로 기능을 제공하지 않는 경우 문서에 권고사항으로 명시해야 하며 시험자는 이를 확인해야 한다.

3.1.2

제품의 설정값 및 감사데이터를 파일시스템 또는 레지스트리에 저장할 때는 비인가 접근으로부터 보호하는 기능을 제공해야 한다.

요구항목

① 감사 데이터는 에이전트 사용자라도 삭제 또는 변경할 수 없도록 관련 유저 인터페이스(UI) 및 CLI 명령어가 제공되지 않아야 한다.

② 저장된 제품 설정값에는 에이전트 사용자도 접근할 수 없어야 한다.

- 접근이라 함은 읽기, 변경, 삭제 등의 오퍼레이션을 의미한다.

③ 제품 보안기능으로 완전히 구현 할 수 없는 경우, 제품 운영환경에서 제품 설정값 저장소를 보호할 수 있도록 지원 할 수 있다.

④ 제품 설정값을 외부에 파일형태로 백업하는 기능을 제공할 경우, 암호화하는 기능을 제공해야 한다.

참고 사항

① 암호화시 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '서버 공통보안요구사항', '8. 암호 지원' 요구사항을 만족해야 한다.

점검시 유의사항

① 제품 설정값을 파일시스템 또는 레지스트리에 저장시 안전하게 암호화하여 보호하는 기능을 제공하여도 요구사항을 만족할 수 있다.

- 사용 암호 알고리즘, 암호키 안전성 및 암호키 저장 방식은 '서버 공통보안요구사항', '8. 암호 지원' 요구사항을 만족해야 한다.

4. 자체 보호

에이전트 또는 클라이언트는 보안기능을 제공하는 메커니즘 및 데이터의 무결성, 가용성을 확인하여 제품의 보안기능을 보호해야 한다.

4.1 무결성 확보

4.1.1

필수

에이전트 또는 클라이언트는 동작 초기화 단계에서 제품의 설정값 및 자체의 무결성을 검증하는 기능을 제공해야 한다.

적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 무결성 검증 대상은 에이전트 또는 클라이언트의 설정값(*정책, 환경설정 등*) 및 제품 자체(*실행파일, 필터 드라이버 등*)이다.

② '유형 1' 해당 제품은 설치 디렉토리에 대한 무결성 검증 기능도 제공해야 한다.

- 설치 디렉토리의 *위치 · 명칭 · 속성 등*을 변경, *권한 삭제 등*의 발생여부 검증.
- 설치 디렉토리 내에 포함된 바이너리, DLL 등의 *위치 · 명칭 · 속성 등*을 변경하여 *삭제 등*이 발생하는지 검증.

③ Windows® 운영체제에서 동작하는 제품인 경우, 운영체제의 안전모드 상에서 무결성 훼손이 발생하면 운영체제 정상 부팅시 해당 변조를 탐지해야 한다.

④ 무결성 검증결과에 대하여 감사기록으로 생성해야 한다.

⑤ 암호와 관련된 부분은 '서버 공통보안요구사항', '8. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

① 감사 데이터 등 변경이 빈번한 정보는 무결성 검사 대상에서 제외할 수 있다.

② 무결성 검증결과 '변조된 정보'에 대한 복구 기능은 4.2.2를 적용한다.

③ 서버가 포함되지 않은 제품(예: 안티바이러스 제품)의 경우 엔드포인트의 일반 사용자가 관리자 역할을 수행해야 한다.

점검시 유의사항

① 에이전트 또는 클라이언트가 포함된 제품인 경우 설정값, 실행파일, 필터 드라이버에 대한 무결성 검증 기능을 확인해야 한다.

② 시험자는 제품의 무결성 검증 대상 및 동작 메커니즘을 조사해야 한다.

4.1.2

필수	에이전트 또는 클라이언트는 주기적 또는 인가된 관리자 요구시 무결성을 검증하고 관리자에 결과 통보 기능을 제공해야 한다.
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 무결성 검증 대상은 4.1.1 제품 구동시 무결성을 검증하는 대상과 동일하다.

② △무결성 검증결과 이상 발생시 △관리자에 의한 무결성 검증결과는 관리자에게 통보해야 한다.

③ 무결성 검증결과에 대하여 감사기록으로 생성해야 한다.

④ 암호와 관련된 부분은 '서버 공통보안요구사항', '8. 암호 지원' 요구사항을 만족해야 한다.

참고 사항

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

② 무결성 검증결과 '변조된 정보'에 대한 복구 기능은 4.2.2를 적용한다.

4.2 가용성 확보

4.2.1

필수

에이전트는 설정값, 실행 파일 등에 대한 비인가된 삭제를 방지하는 기능을 제공해야 한다.

적용 유형	유형 1

참고 사항

① 삭제 방지 기능을 제공하지 못할 경우, 삭제 후 무결성 탐지를 통해 변조 여부를 확인하고 4.2.2에 따라 자동복구하는 기능을 제공하는 것도 허용한다.

4.2.2

필수

에이전트 또는 클라이언트는 변조된 정보(*설정값, 실행파일, 필터 드라이버 등*)를 복구할 수 있는 기능을 제공해야 한다.

적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① ‘변조된 정보’에는 제품의 정상적인 동작, 보안기능 수행에 영향을 미치는 파일을 모두 식별,포함해야 한다.

② ‘에이전트 유형 1’은 자동복구 기능을 제공해야 하고 △에이전트 유형2 △에이전트 유형3 △클라이언트 유형은 수동복구 기능을 제공할 수 있다.

점검시 유의사항

① 시험자는 변조된 정보의 복구 기능에 대해 복구 대상 및 동작 메커니즘을 조사해야 한다.

② 에이전트 유형1은 자동복구 기능을, 그 외 유형은 수동복구 기능을 제공해야 한다.

③ 「정보보호제품 평가인증 해설서」 문서의 ‘2.14. TOE 자체보호 기능’ 절을 참고한다.

- 변조된 정보에 대한 수동 복구의 예로 사용자가 개입한 재설치 및 서버 · 업데이트 서버를 통한 복구 기능의 제공이 있다.
- 사용자가 개입하지 않고 자동으로 복구하는 기능을 제공할 수도 있다.

4.2.3

필수

에이전트가 임의로 종료 및 중지되지 않도록 하는 기능을 제공해야 한다.

적용 유형	유형 1

요구항목

① 에이전트는 프로세스 및 서비스에 대한 종료 및 중지 방지 기능을 제공해야 한다.

참고 사항

① 종료 · 중지 방지 기능의 구현이 불가하다면 ‘우발적 종료시 PC 종료’ 등 대체 기능을 구현할 수 있다.

점검시 유의사항

① 시험자는 에이전트 프로세스 · 서비스를 모두 조사하고, 에이전트 강제 종료 · 중지 취약점이 존재하는지 시험해야 한다.

② 에이전트 프로세스나 서비스가 종료 · 중지되어도 보안기능이 정상적으로 동작한다면 요구사항을 만족하는 것으로 판정한다.

4.3 에이전트 제거

4.3.1

조건부 필수

관리자가 에이전트 제거(Uninstall)를 허용한 후 일반 사용자가 에이전트를 제거할 수 있도록 구현해야 한다.

조 건	‘호스트 자료유출 방지제품’과 ‘소프트웨어 기반 보안USB 제품’의 경우

요구항목

① 관리자가 에이전트 제거를 허용하는 방법의 예는 다음과 같다.

- *서버에서 에이전트 삭제 허용 · 차단 설정 기능을 이용해 삭제 허용.*
- *삭제키 설정 등의 방법을 이용한 삭제 허용.*
- *제공된 전용 삭제 프로그램을 이용한 삭제 허용 등.*

점검시 유의사항

① 서버의 설정 기능을 통한 에이전트 삭제시에는 서버 공통보안요구사항 2.5.2 항목을 함께 시험해야 한다.

② 안티바이러스 제품중 엔드포인트 공통보안요구사항만 적용되는 제품은 '해당사항 없음'으로 판정한다.

5. 감사기록

에이전트 또는 클라이언트가 보안기능 및 보안관리 기능을 제공하는 경우 보안관리 설정 등 보안활동과 관련된 사항을 감지 · 기록하여 서버로 전송하는 기능을 제공하는지 확인한다.

5.1 감사기록 생성

5.1.1

필수

〈표 1〉에 기재된 감사기록을 생성해야 한다.

적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 신청업체는 에이전트 또는 클라이언트가 제공하는 주요 사건에 대한 감사 목록을 문서로 제출해야 한다.

- '보안기능 시험'제도의 경우 「보안기능 구현명세서」에 해당 내용을 기술하고 '국내용 평가 · 인증' 제도는 「설명서)」에 기술하여 제출한다.

여 백

〈 표 1. 생성해야 하는 주요 감사사건 〉

보안기능	감사사건	추가감사정보
자체 보호	무결성 검사 수행 및 결과	
보안 관리	보안관리 기능을 제공하는 경우, 보안관리 기능의 수행과 보안속성 값의 모든 변경	변경된 보안속성 데이터
감사 기록	에이전트 시작	
	보안관리를 통해 일반 사용자가 감사기록을 서버로 전송 요청할 수 있는 경우, 감사기록 전송 수행	
안전한 업데이트 및 파일 배포	(온라인 업데이트 기능 제공시) 서버 및 외부 업데이트 서버로부터 수신한 파일의 전자서명 검증 수행 및 결과	전자서명 검증 실패한 파일

5.1.2

필수

감사기록에는 사건별 주요 정보가 포함되어야 한다.

적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 사건의 결과가 포함되어야 한다.

점검시 유의사항

① 제품 구성요소 마다 신뢰된 시간 정보를 사용하는 것을 요구한다.

② NTP 서버나 에이전트 · 클라이언트가 설치된 시스템 OS에서 제공하는 기능을 이용하여 시간 동기화 구현이 가능하다.

- 서버와 에이전트 · 클라이언트간 시간 동기화를 반드시 요구하지는 않는다.

5.2 감사기록 전송

5.2.1

조건부 필수

에이전트 또는 클라이언트가 생성한 주요 감사기록을 서버로 전송하는 기능을 제공해야 한다.

조 건	서버가 있는 경우
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① 5.1.1 항목의 〈표 1〉에 기재된 감사기록의 서버 전송 기능을 구현해야 한다.

② 서버와 연결이 끊어진 후, 다시 복구되면 연결이 끊긴 이후에 적재된 감사기록을 서버에 모두 전송해야 한다.

③ 서버로 전송되는 감사기록의 보호는 '서버 공통보안요구사항'의 '3.1 전송데이터 보호'중에서 '3.1.1' 요구사항을 만족해야 한다.

6. 안전한 업데이트 및 파일 배포

Windows® 운영체제가 설치된 엔드포인트에 존재하는 에이전트 또는 클라이언트가 온라인 업데이트 및 파일 배포 기능을 포함하는 경우 전자서명 검증을 통해 전송되는 파일에 대한 부인방지 및 무결성 보호가 제공되어야 한다.

에이전트 또는 클라이언트가 Windows® 운영체제가 아닌 Linux® 등이 설치된 엔드포인트에 존재하는 경우(예: 데이터베이스 접근통제 제품, 운영체제(서버) 접근통제 제품, 통합보안관리 제품 등), 인가된 관리자는 제품의 서버를 통해 엔드포인트에 설치된 에이전트 또는 클라이언트로 업데이트 파일을 전송할 수 있으며, 이 경우 서버와 엔드포인트에 설치된 에이전트 또는 클라이언트간에는 '서버 공통 보안요구사항'의 '3.1 전송데이터 보호'가 적용된다.

여 백

6.1 온라인 업데이트 및 파일 배포

6.1.1

조건부 필수 	**에이전트 또는 클라이언트는 서버 또는 업데이트 서버로부터 전송받는 업데이트 대상파일의 파일 생성 주체에 대한 전자서명 검증을 수행해야 한다.**
조 건	Windows® 환경의 엔드포인트에 설치된 에이전트 또는 클라이언트일 경우
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

요구항목

① Windows® 운영체제가 설치된 엔드포인트에 존재하는 에이전트 또는 클라이언트에 적용한다.

② 제품구성과 무관하며 설치파일 및 정책파일에 포함되지 않는 모든 파일(예: 패치파일, 일반 실행파일 등)은 에이전트 및 클라이언트로 배포하는 기능은 허용되지 않는다.

– 다만, 패치파일 배포가 주 기능인 패치관리시스템은 예외적으로 허용된다.

③ 전자서명 검증시 인증서 유효성(유효기간 1년 이내) 검증을 수행해야 한다.

④ 업데이트 파일 전자서명 검증결과(성공 · 실패)가 감사기록에 기록되어야 한다.

⑤ 암호와 관련된 부분은 ‘서버 공통보안요구사항’, ‘8. 암호 지원’ 요구사항을 만족해야 한다.

⑥ 개발업체 또는 관리자(업데이트 파일에 대해 전자서명을 수행하는)는 인터넷과 연결이 차단된 별도의 오프라인 서버에서 전자서명을 수행해야 한다.

참고 사항

① 이 요구사항에서 서버는 에이전트 · 클라이언트에 정책을 내려주는 서버, 개발업체에서 관리 · 운영하는 업데이트 서버가 대상이다.

② 업데이트 대상 파일은 *제품 설치파일(업데이트 파일 등) 및 에이전트 정책파일 등*이 될 수 있다.

- 제품 설치파일(업데이트 파일 등)은 제품구성과 관련된 모든 파일 및 에이전트 또는 클라이언트 업데이트 파일로, 안티바이러스 제품인 경우 엔진파일 및 시그니처를 포함한다.
- 에이전트 정책파일이 실행파일이 아니라면 전자서명 대상파일에서 제외되며 비밀성 및 무결성이 보장되는 안전한 통신구간 등 안전한 배포 수단이 제공되어야 한다.

점검시 유의사항

① '6. 안전한 업데이트 및 파일 배포' 시험시 최신 「정보보호제품 평가인증 해설서」의 '2.4. 업데이트 및 파일 전송 기능 보안수준 절'을 참고한다.

6.1.2

조건부 필수	**에이전트 또는 클라이언트는 서버 · 업데이트 서버 주소에 대한 무결성 확인 기능을 제공해야 한다.**
조 건	Windows® 환경의 엔드포인트에 설치된 에이전트 또는 클라이언트일 경우
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

점검시 유의사항

① 서버 주소가 포함된 파일에 대한 무결성 검증 기능을 제공하는지 확인한다.

② 설정파일에 서버 주소 저장시 4.1.1의 설정파일 무결성 검증을 통해 이를 확인할 수 있다.

③ 제품 실행파일 내에 서버 주소를 하드코딩 해서는 안된다.

여 백

6.1.3

조건부 필수 	수신 서버는 송신 서버의 주소에 대한 무결성 검증을 수행해야 한다.
조 건	파일 전송 경로상에 두 대 이상의 서버 또는 업데이트 서버가 존재하는 경우
적용 유형	유형 1, 유형 2, 유형 3, 클라이언트

끝.

〈 별 표 〉

제 · 개정 이력

일 자	주요 변경 내용	문서 버전
2021. 4. 2.	‘에이전트 기본보안요구사항’을 ‘엔드포인트 공통보안요구사항’으로 개정	V3.0