정보보호제품

평가·인증 해설서

V1.3

2021. 9. 1.

IT보안인증사무국

본 문서는 「정보보호제품 평가·인증 수행규정」 및 「정보보호제품 국내용 평가·인증 세부 수행절차」를 준수한 평가·인증 시 주의사항 등을 해설서로 제공한다.

목 차

목 차

('21. 9. 1., IT보안인증사무국)

[문서 변경이력]

날짜	변경 내용
2018.12.19.	o 최초 작성 - 평가·인증 과정에서 발생한 현안에 대한 인증기관 공지사항, 평가·인증 지시서, 기술검토위원회 결정사항 등을 반영
2019.02.25	o 인증기관 공지사항 등 추가
2019.03.22	o 평가·인증기관 검토의견 수렴
2019.03.25	o 편집 등 경미한 수정
2019.04.01	o 공개용 해설서
2020.01.10	o 2.1절 및 2.9절 일부 개정 o 국가·공공기관 도입 시 CC인증이 필요한 제품유형이 조정됨에 따라 불필요한 제품유형에 대한 가이드 삭제 o 오타 등 편집 수정
2021.05.17	o 2.2절 소제목 수정 o 2.3절, 2.4절, 2.5절, 2.13절, 2.14절 및 2.16절 일부 개정 o 3. 참고자료 최신문서로 수정 o 「정보보호제품 평가·인증 수행규정」 및 「정보보호제품 국내용 평가·인증 세부 수행절차」 개정에 따른 해설서 내용 개정 o 국가·공공기관 도입 시 CC인증이 필요한 제품유형이 조정됨에 따라 불필요한 제품유형에 대한 가이드 삭제 o 국가용 보안요구사항 V3.0 준수 관련 일부 내용 추가 o 오타 등 편집 수정
2021.9.01	o 2.9절 수정 및 2.16절 해석사항 추가

1. 개요

1.1 목적 및 범위

1 본 문서는 「정보보호제품 평가·인증 수행규정」(이하 '수행규정') 및 「정보보호제품 국내용 평가·인증 세부 수행절차」(이하 '국내용 수행절차')를 준수한 평가·인증 과정에서 발생한 현안에 대한 인증기관 공지사항, 평가·인증 지시서, 기술검토위원회 결정사항 등을 해설서로 제공하기 위한 것이다.

2 본 문서의 목적은 '수행규정' 및 '국내용 수행절차'에 의한 인증서 획득을 희망하는 개발업체, 평가·인증을 수행하는 평가자 및 인증자, 인증제품을 사용하고자 하는 사용자 등 다양한 관계자가 정보보호제품 평가·인증제도를 정확하게 이해하여 업무를 효율적으로 수행하기 위한 세부 기준, 지침, 가이드를 제공하기 위한 것이다.

3 본 문서는 평가·인증 관련 규정이 개정되거나, 관련 요구사항 및 기술 등이 변경되는 경우 업데이트될 것이며, 신청기관 및 평가기관 등 평가·인증 관련기관은 최신 문서를 적용한다.

1.2 용어정의

4 본 문서에서 사용되는 약어 및 용어는 '수행규정' 및 '국내용 수행절차', CC를 따른다.

2. 정보보호제품 평가·인증 해석사항

2.1 TOE 범위 산정 및 식별자 부여 방법

적용 범위	☑ 국제용 인증	☑ 국내용 인증

5 CC를 사용한 평가·인증에서 IT 제품의 평가·인증 범위는 TOE(평가대상)로 정의한다.[1)]

- 국내용은 2010년 4월 시행된 '국내용 정보보호제품 평가인증 수행지침'에 의해 전체 제품을 TOE 범위로 산정한다. 즉, 평가·인증된 TOE는 판매되어 배포되는 제품과 동일해야 한다.
- 국제용은 CC에 의해 제품과 동일하지 않게 TOE 범위 산정이 가능하다.

6 따라서, 형상항목, 배포절차, ST에 선언된 SFR과의 관계를 분석하여 TOE 범위를 산정할 필요가 있다.

2.1.1 기본 원칙

7 다음의 기본 원칙을 모두 고려하여 TOE 범위를 산정해야 하며, 구체적인 내용은 [세부 지침]을 참조한다.

8 ① IT 제품 구성요소 단위로 TOE 범위를 산정한다.

- (국내용) IT 제품의 전체 구성요소를 TOE에 포함해야 한다. 제3자가 제공한 요소가 '국가용 보안요구사항'에 해당하는 SFR을 구현한 경우 TOE 범위에서 제외할 수 없으며, 평가·인증 완료되어 판매·배포하는 제품에 포함하여 보증해야 한다.
- (국제용) IT 제품 일부 구성요소만을 TOE 범위로 산정할 수 있으나, 물리적인 구성요소 단위 및 TSF 의존성 등을 고려하여 범위를 산정해야 한다.

9 ② ST에 선언된 SFR과의 관련성을 분석하여 TOE 범위를 산정한다.

- (국내용, 국제용) ST에 서술된 TOE 용도 및 보안목적에 따라 TOE가 필수적으로 만족해야 하는 SFR을 구현한 부분은 TOE 범위에 포함해야 한다. 필수적인 SFR이 제3자가 제공한 요소에서 구현된 경우 제3자가 제공한 요소 또한 TOE 범위에 포함하여 보증해야 한다. TOE의 용도 및 보안목적과

1) '하나의 IT 제품을 대상으로 한 TOE 범위산정' 또는 '여러 개의 IT 제품들을 대상으로 한 TOE 범위산정'을 의미하며, 이하 'IT 제품'이란 하나 이상의 IT 제품을 통칭한다. 또한, IT 제품은 제3자가 제공한 요소를 포함할 수 있고 이는 소스코드, 라이브러리, 실행 모듈, IT 제품 등 다양한 형태일 수 있으며, 형태에 관계없이 '제3자가 제공한 요소'로 통칭한다.

무관하며 필수적인 보안기능성과 독립적인 부가기능의 경우 'TOE 범위에서 제외(위의 ①을 적용하여 판단, 국제용만 해당)'하거나 또는 'TOE 범위에 포함시키되 non-TSF로 분류'할 수 있다.

10 ③ TOE 버전에 영향을 주는 형상항목을 모두 포함하여 TOE 범위를 산정한다.

- (국내용, 국제용) TOE를 구성하는 형상항목으로 함께 컴파일/빌드되어 TOE 버전에 영향을 주는 제3자 제공 소스코드/라이브러리는 TOE 범위에 포함하고, ②번을 참조하여 TSF인지 non-TSF인지 결정할 수 있다.

- (국내용, 국제용) TOE를 포함하는 IT 제품과 함께 배포되는 제3자가 제공한 IT 제품의 경우 ①, ②번을 참조하여 TOE 범위에 포함 여부를 결정할 수 있다.

11 ④ 배포되는 TOE 구성요소를 고려하여 TOE 식별자를 부여한다.

- (국내용, 국제용) 평가되는 TOE 구성요소와 실제 배포되는 TOE 구성요소가 일치하도록 TOE 식별자를 부여해야 한다.

12 ⑤ 하드웨어 일체형 장비로 판매·배포되는 제품인 경우 다음을 적용한다.

- (국내용, 국제용) 개발업체 형상관리 체계에 따라 제품의 모델명은 내장되는 소프트웨어/펌웨어 및 하드웨어 모델에 대한 식별자 등을 고려하여 달라질 수 있으므로 형상관리 평가 시 TOE 식별자의 적절성 결정해야 한다.

- (국내용, 국제용) 특히, 신청기관이 하드웨어 모델이 다른 여러 개의 하드웨어 일체형 장비를 하나의 TOE로 평가신청하는 경우 사실상 여러 개의 하드웨어 일체형 장비 제품을 묶어서 하나의 'TOE 식별자'로 인증서 발급하는 것이므로, 'TOE 식별자'는 각각의 하드웨어 일체형 장비 제품을 칭하는 제품명이기보다는 해당 제품 라인의 대표성을 지닌 식별자로 간주한다.

  - 이와 같은 방식으로 인증서 발급을 희망하는 경우 TOE 식별자, 제품 식별자, 하드웨어 모델 식별자, 소프트웨어/펌웨어 식별자가 모두 제공되어야 한다.

  - 즉, 소비자가 TOE를 구매한다는 것은 인증범위에 포함된 하드웨어 일체형 장비 중 하나를 제품으로써 구매하는 것이지, 하드웨어 모델과 펌웨어를 각각 구매한 후 사용자가 하드웨어 일체형 장비를 조립하여 사용하는 것이 아님에 유의한다.

  - 따라서, 하드웨어 일체형 장비 형태로 인증되는 제품은 하드웨어 일체형 장비 자체를 형상식별하는 체계가 존재해야 한다.

- 모든 형상 식별자는 유일성이 보장되어야 한다(즉, 형상관리 체계에 따라 버전관리가 가능해야 한다.).

- 다음 그림은 부적합 및 적합 사례를 보여준다.

(그림 2.1-1) 하드웨어 일체형 장비 식별 예시

- 다음은 하드웨어 일체형 장비(즉, 제품)의 형상 식별자 유일성이 보장되지 않는 부적합한 사례이다.

<TOE 식별자: TOE V1.0>

구분	형상변경 전	형상변경 후
펌웨어	FW V1.0.0.1 Build 111	FW V1.0.0.2 Build 120
하드웨어 모델	HW 100	HW 100
하드웨어 일체형 장비	TOE V1.0 HW 100	TOE V1.0 HW 100

위의 예에서 하드웨어 일체형 장비 식별자는 구성요소인 펌웨어나 하드웨어 모델이 변경되는 경우 유일성이 보장되지 않음을 알 수 있다. 즉, 펌웨어가 서로 다른 두 가지 제품이 하나의 식별자로 식별되는 문제가 있다.

- 다음은 하드웨어 일체형 장비(즉, 제품)의 형상 식별자 유일성이 보장되는 적합한 사례이다.

<TOE 식별자: TOE V1.0>

구분	형상변경 전	형상변경 후
펌웨어	FW V1.0.0.1 Build 111	FW V1.0.0.2 Build 120
하드웨어 모델	HW 100	HW 100
하드웨어 일체형 장비	TOE V1.0.0.1 HW 100	TOE V1.0.0.2 HW 100

<TOE 식별자: TOE V1.0>

구분	형상변경 전	형상변경 후
펌웨어	FW V1.0.0.1 Build 111	FW V1.0.0.2 Build 120
하드웨어 모델	HW 100	HW 100
하드웨어 일체형 장비	TOE V1.0 HW 100 (R0)	TOE V1.0 HW 100 (R1)

- (국내용) TOE는 제품과 동일해야 하므로 하드웨어 일체형 장비 전체를 TOE 물리적 범위로 산정해야 한다.
- (국내용, 국제용) TOE는 TSF 제공을 위해 하나의 제품으로써 동작하므로 하드웨어 일체형 장비 전체를 TOE 물리적 범위로 산정해야 한다.

13 ⑥ 기타 원칙은 다음과 같다.

14 ⑥-1 (국내용, 국제용) '범용이 아닌 운영체제'의 사용은 운영체제의 커스터마이즈가 반드시 필요한 하드웨어 일체형 장비와 같은 형태의 제품으로 제한한다. 또한, 역으로 하드웨어 일체형 장비에는 그 명칭에서 직관적으로 의미하는 바와 같이 특정한 하드웨어에 의존하므로 '범용 운영체제'는 사용할 수 없으며, 하드웨어에 대한 종속성으로 인해 커스터마이즈가 반드시 필요한 '범용이 아닌 운영체제'만을 사용할 수 있다.

15 ⑥-2 (국내용, 국제용) '범용 운영체제'에 설치되는 소프트웨어 응용프로그램인 경우 해당 소프트웨어 응용프로그램만을 TOE 범위로 산정하며, 다음 원칙을 추가로 적용한다.

- 운영환경으로 하드웨어 일체형 장비와 같은 하드웨어 모델 명시를 허용하지 않는다(즉, TOE 운영에 필수적인 하드웨어/펌웨어/소프트웨어 사양 명시).
- 개발환경 보안점검 시 소프트웨어인 응용프로그램 TOE 배포 절차를 확인해야 한다.

2.1.2 세부 지침

16 CC는 TOE가 제공하는 보안기능성을 TSF(TOE 보안기능성)로 정의한다.

- TSF 범위는 ST에 정의된 SFR(보안기능요구사항)에 의해 결정된다.
- TOE가 제공하는 IT 기능에는 TSF 뿐만 아니라 non-TSF도 존재한다.
- 즉, CC의 SAR(보증요구사항)은 TSF에 중점을 두고 평가제출물을 요구하지만, **TOE 범위에서 non-TSF가 제외될 수 있는 것은 아니다.**

17 CC V3.1 R2/R5 1부에서 고려하는 다양한 TOE 형태는 다음과 같다.[2)]

Different representations of the TOE
In the CC, a TOE can occur in several representations, such as (for a software TOE):
- a list of files in a configuration management system;
- a single master copy, that has just been compiled;
- a box containing a CD-ROM and a manual, ready to be shipped to a customer;
- an installed and operational version.

18 TOE 범위산정 시 **형상항목, 배포절차, ST에 선언된 SFR과의 관계 분석** 부족함은 항상 문제점으로 인식되고 있다.

- 형상항목에 포함되는 TOE 구현의 표현(예: 소스코드) 및 컴파일/빌드된 TOE 실행파일(설치파일)을 고려해야 한다.
- 배포절차에서 다루어지는 TOE 구성요소를 고려해야 한다.
- ST에 선언된 SFR 직접 구현(SFR-수행), SFR 구현 보조(SFR-지원), SFR 수행을 위한 전제조건(SFR-비-간섭) 등 SFR과의 관계를 고려해야 한다.[3)]

19 결과적으로 TOE 범위산정 시 다음과 같은 오류를 범하기 쉽다.

- non-TSF를 TOE 범위에서 제외하고 TSF만을 TOE로 산정한다.
- 물리적으로 IT 제품을 구성하는 구성요소별로 TOE 범위를 산정하지 않고 논리적인 기능 단위로 TOE 범위를 산정한다.
- TOE를 구성하는 형상항목으로 함께 컴파일/빌드되어 TOE 버전에 영향을 줌에도 불구하고 제3자가 제공하는 소스코드/라이브러리의 기능은 TOE 범위에서 제외하고 TOE 범위로 산정한다.
- ST의 TOE 보안목적에 따라 TOE가 필수적으로 만족해야 하는 SFR을 구현한 부분임에도 불구하고 제3자가 제공하는 요소는 TOE 범위에서 제외한다.
- TOE 구성요소를 운영환경에 따라 필요한 구성요소만을 조합하여 배포, 설치, 운용함에도 불구하고 실제 배포, 설치, 운용되는 TOE 구성요소 단위로 TOE 식별자를 부여하지 않고 전체 TOE 구성요소를 하나의 TOE로 간주하여 하나의 식별자를 부여한다.

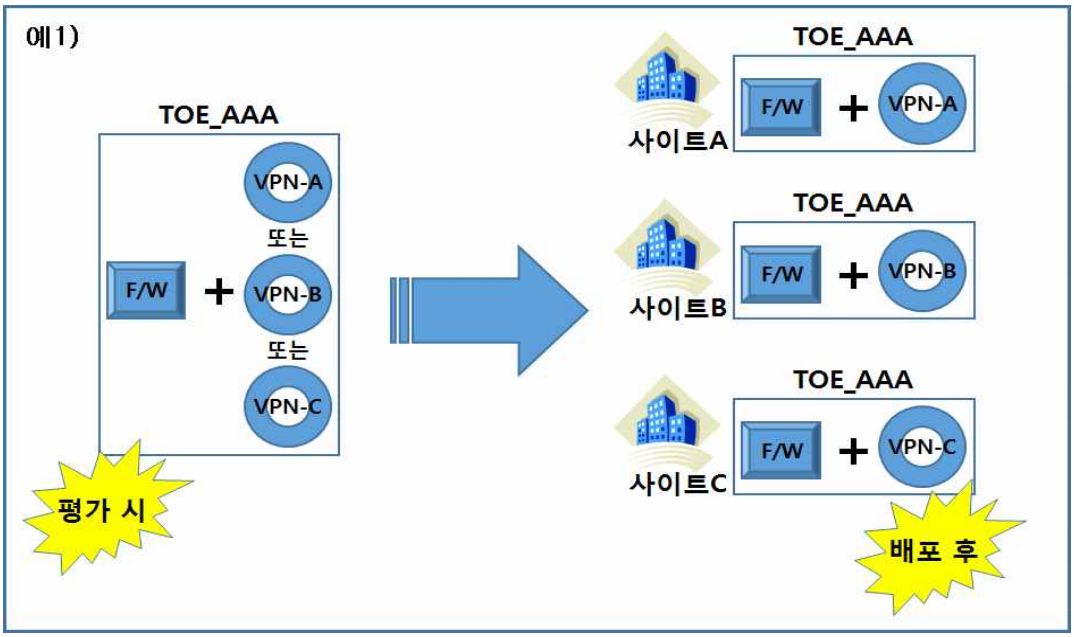
2) CC V3.1 R2는 1부 184항을, CC V3.1 R5는 1부 187항을 참조한다.

3) CC V3.1 R5의 TSF 정의에 따라 SFR-수행, SFR-지원, SFR-비-간섭 요소는 모두 TSF로 간주한다. 즉, 세 가지 요소는 모두 '보안 관련' 부분으로 정의된다.

- 하드웨어 일체형 장비의 경우 '범용 운영체제'[4]로는 TSF 동작에 필요한 운영 환경이 구축되지 않아서 '범용이 아닌 운영체제(customized OS)'[5]를 포함함에도 TOE 범위에서 운영체제/하드웨어를 제외한다.[6]

20 다음은 TOE 범위산정과 관련된 예이다.

- (예1) 평가된 TOE 구성요소와 배포된 TOE 구성요소가 일치하지 않아서 TOE 식별자가 부적절하다.



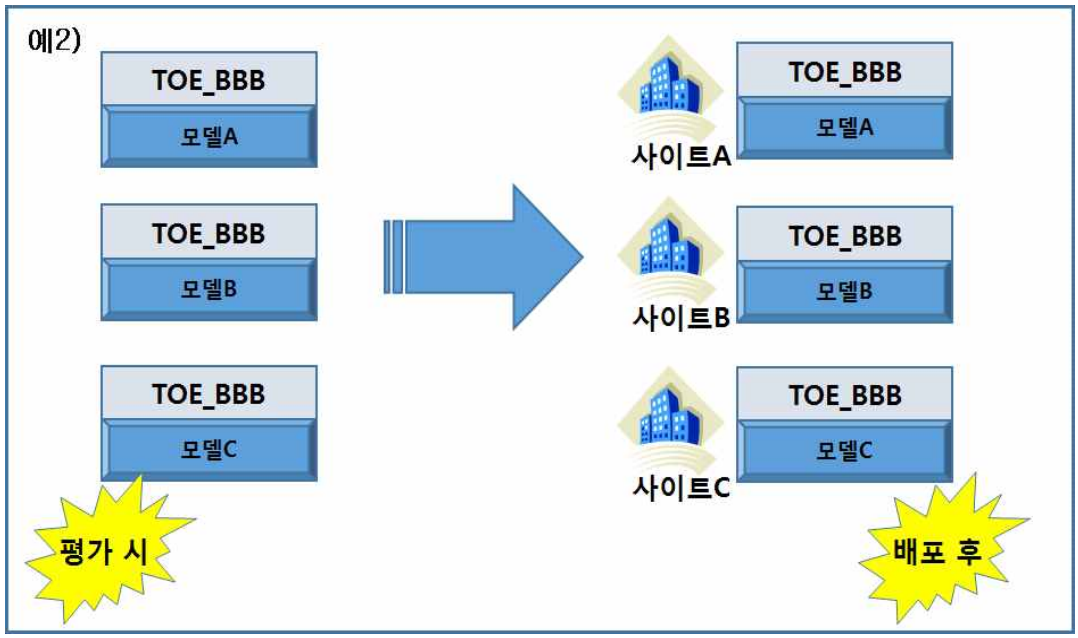
(그림 2.1-2)

- (예2) 평가된 TOE 구성요소와 배포된 TOE 구성요소가 일치하여 TOE 식별자가 적절하다.

4) '범용 운영체제'의 예로 「일반적으로 알려지고 사용되는」 Windows, HP, RedHat 등과 같은 '상용 운영체제' 및 Linux 계열(예: Fedora, CentOS), Debian 계열(Ubuntu) 등과 같은 '배포판 운영체제'를 들 수 있다.

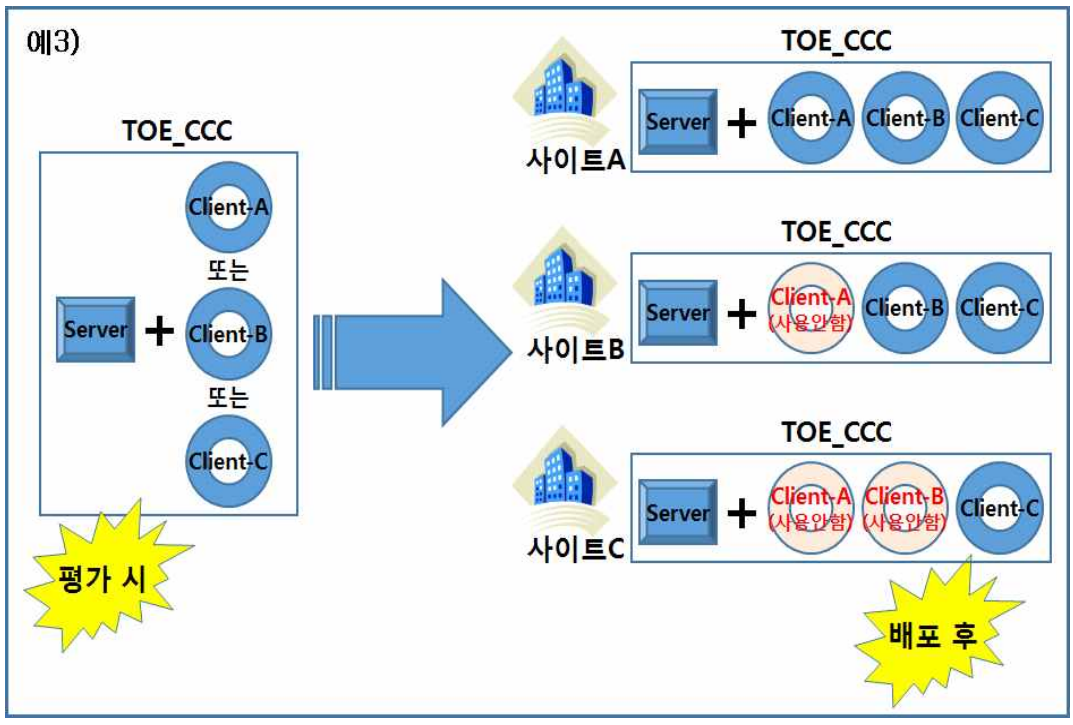
5) '범용 운영체제'가 아닌 운영체제는 모두 '범용이 아닌 운영체제'로 분류한다. 'Customized' 정도에 따라 분류하는 것은 현실적으로 불가능하며, 따라서 단순한 이분법을 적용한다. 즉, 하드웨어 일체형 장비에서 공개된 운영체제 소스코드를 사용하여 새로운 운영체제를 빌드(컴파일/링크)한 경우(커널 변경, 운영체제 환경 변경 등 변경 수준은 개발업체에 따라 상이할 수 있음), '범용 운영체제'로 분류할 수 없다.

6) 하드웨어 일체형 장비의 경우 구성요소를 물리적/논리적으로 분리하여 범위를 산정하기 어려우므로 원칙적으로 하드웨어 일체형 장비 전체를 TOE 물리적 범위로 산정해야 한다.



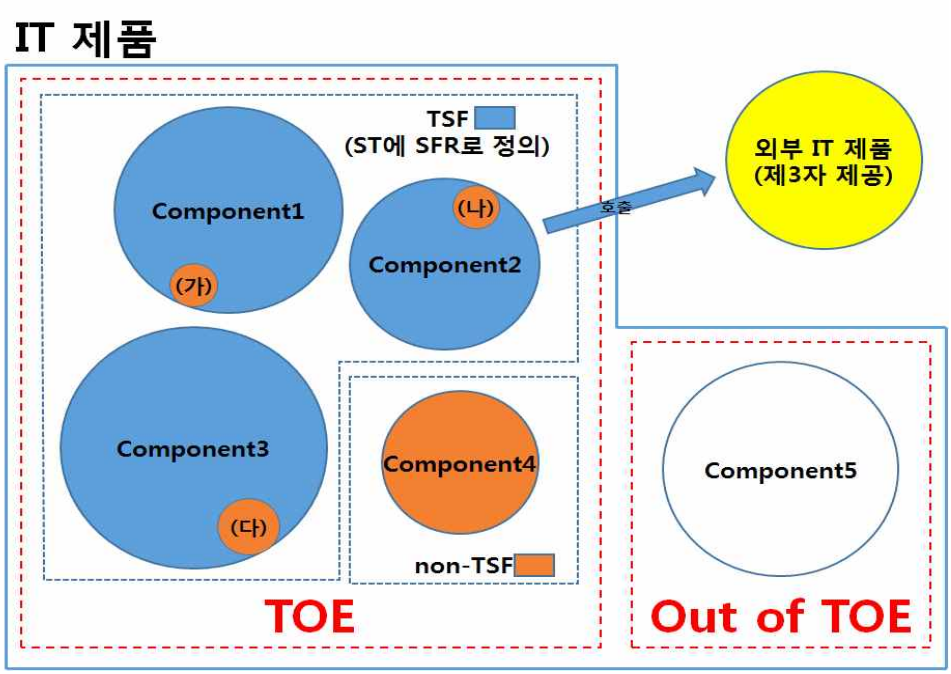
(그림 2.1-3)

- (예3) 사용자가 운용 시 구성요소 사용여부를 결정할 수 있으나, 평가된 TOE 구성요소와 배포된 TOE 구성요소가 일치하여 TOE 식별자가 적절하다.



(그림 2.1-4)

21 TOE 범위산정 시 고려사항을 설명하기 위해 다음 그림을 예시로 사용한다.



(그림 2.1-5)

22 **① IT 제품 구성요소 단위로 TOE 범위를 산정한다.**

23 (국내용) TOE와 IT 제품이 동일해야 하므로 IT 제품의 전체 구성요소가 TOE에 포함되어야 한다.

- 개발자가 구현한 IT 제품에서 TOE 유형에 필수인 보안기능성을 모두 제공하지 못하여 제3자가 제공한 요소가 필요한 경우 TOE 범위에 제3자가 제공한 요소가 추가될 수 있다(아래 ②번의 (예5) 참조).
- 제3자가 제공한 요소가 '국가용 보안요구사항'에 해당하는 SFR을 구현한 경우 TOE 범위에서 제외할 수 없으며, 평가·인증 완료되어 판매·배포하는 제품에 포함하여 보증해야 한다.
- (그림 2.1-5)의 예시에서, Component4 및 Component5가 독립적인 용도의 제품유형으로 인정되거나 TOE가 준수하는 국가용 보안요구사항에 명시된 보안기능요구사항과 무관한 경우, 제품의 일부가 아닌 별도의 독립적인 제품으로 분리되어야 할 수 있음에 유의한다(예: 안티바이러스 제품유형으로 국내용 평가신청한 제품 안에 안티바이러스 제품 외에 국가용 안티바이러스 제품 보안요구사항과 무관한 제품유형인 엔드포인트 보호 플랫폼 제품을 포함하여 하나의 제품으로 신청한 경우, 가상사설망 제품으로 국내용 평가신청한 하드웨어 일체형 장비 형태의 제품에 국가용 보안요구사항과 무관한 독립적인 소프트웨어를 더하여 하나의 제품으로 신청한 경우 등).

24 (국제용) IT 제품 일부 구성요소만을 TOE 범위로 산정할 수 있으나 다음을 확인해야 한다.

- IT 제품의 물리적인 구성요소 단위로 TOE 구성요소를 선택해야 한다. 예를 들어, (그림 2.1-5)에서 (가), (나), (다)는 보안과 관련 없는 기능이지만 TOE 범위에 포함되는 구성요소 안에 존재하는 기능이므로 TOE 범위에 포함되어야 한다.
- TOE와 TOE 범위에서 제외되는 구성요소는 각각 하나의 독립적인 IT 제품(또는 모듈)[7]으로써 동작 가능해야 한다.
- TOE의 TSF 수행 시 TOE 범위에서 제외되는 구성요소에 의존하지 않아야 한다. TSF 수행 시 의존해야 하는 부분은 SFR-지원 부분으로써 TOE 범위에 포함되어야 한다.
- TOE의 non-TSF 수행 시 의존하는 TOE 구성요소의 경우 TOE 범위에서 제외 가능하나, 해당 구성요소를 IT 환경으로 반드시 정의해야 한다.
- (그림 2.1-5)와 같은 예에서 'Component4'는 '보안 관련' 요소가 아니므로 위 조건들을 만족하는 경우 TOE 범위에서 제외하는 것도 가능하다 (TOE 범위 포함여부를 개발자가 선택 가능).

25 **② ST에 선언된 SFR과의 관련성을 분석하여 TOE 범위를 산정한다.**

26 (국내용, 국제용) ST에 서술된 TOE의 용도 및 보안목적에 따라 TOE가 필수적으로 만족해야 하는 SFR을 구현한 부분은 TOE 범위에 포함해야 한다.

- (예4) TOE 구성요소 간에 전송되는 데이터 암호화가 필수인 제품에서 암호화 메커니즘을 OpenSSL 라이브러리를 사용하여 구현한 경우 OpenSSL은 TSF로써 TOE 범위에 포함되어야 한다(아래 ③번 참조).
- (예5) 침입방지시스템이 유해트래픽 탐지 및 차단을 위해 제3자가 제공하는 탐지 모듈을 사용하는 경우 이는 TOE 범위에 포함되어야 한다.
- (예6) 소프트웨어 응용프로그램인 TOE가 감사 데이터 저장소로 운영체제에 별도로 설치된 DBMS를 사용하는 경우((그림 2.1-5)의 '외부 IT 제품'에 해당), TOE 운영에 필요한 IT 환경으로 정의할 수 있다.
- (예7) 국제용의 경우, 감사 데이터 통계를 위해 제3자가 제공하는 통계 소프트웨어를 IT 제품에 포함하여 배포하고, 통계 기능이 ST에 SFR로 선언되지 않은 경우 TOE 운영에 필요한 IT 환경으로 정의할 수 있다 ((그림 2.1-5)의 'Component5'에 해당).

7) 각각 독립적인 생성(예: 컴파일/빌드)이 가능해야 함

- (예8) TOE 버전에 영향을 주는 공개 소스코드/라이브러리 등의 경우 TOE 범위에 포함하되, 해당 소스코드/라이브러리 등이 제공하는 기능이 ST에 선언된 SFR과 관련 있는 경우 TSF로 정의하고, 관련 없는 경우 non-TSF로 간주할 수 있다(아래 ③번 참조).

- SFR이 제3자가 제공하는 요소에서 구현된 경우 해당 요소를 TOE 범위에 포함하되, ST에 선언된 SFR에 근거한 평가를 수행한다. CC 평가는 ST에 선언된 SFR에 근거하여 설계 및 시험 평가활동 등을 수행한다. 즉, 제3자가 제공하는 요소 전체에 대한 설계 및 시험 등은 불필요하며, SFR과 관련된 부분에 대한 설계 및 시험 등만 수행한다. 단, 취약성 분석 시 SFR과 관련 없는 기타 기능으로 인한 TSF 우회가능성 등 추가 분석이 필요하다.

- TOE의 용도 및 보안목적과 무관하며 필수적인 보안기능성과 독립적인 부가기능의 경우 인증기관과 협의하여 TOE 범위에서 제외(위의 ①을 적용하여 판단, 국제용만 해당), 또는 TOE 범위에 포함시키되 non-TSF로 분류할 수 있다.

27 **③ TOE 버전에 영향을 주는 형상항목을 모두 포함하여 TOE 범위를 산정한다.**

28 (국내용, 국제용) TOE를 구성하는 형상항목으로 함께 컴파일/빌드되어 TOE 버전에 영향을 주는 제3자가 제공한 요소는 TOE 범위에 포함해야 한다.

- ②번을 참조하여 관련 기능이 TSF인지 non-TSF인지 결정할 수 있다.

- ST에서 TOE 물리적 범위 식별 및 서술하는 것과 관련된 지침은 CEM V3.1 R5의 ASE_INT.1-9와 관련된 평가방법 참조한다.

29 (국내용, 국제용) TOE를 포함하는 IT 제품과 함께 배포되는 제3자가 제공한 요소의 경우 ①, ②번을 참조하여 TOE 범위 포함 여부를 결정할 수 있다.

30 **④ 배포되는 TOE 구성요소를 고려하여 TOE 식별자를 부여한다.**

31 (국내용, 국제용) 평가되는 TOE 구성요소와 실제 배포되는 TOE 구성요소가 일치하도록 TOE 식별자를 부여해야 한다.

- CC 3.1 R2/R5 1부 6.1.1절에 의해 설치 후 운용되는 버전이 하나의 TOE로 식별되어야 한다.

- (예1)의 경우 TOE 구성요소 중 VPN-A, VPN-B, VPN-C는 항상 TOE 구성요소로서 배포되는 것이 아니라 사이트에 따라 선택적으로 배포된다. 즉, 설치 후 운용되는 TOE 버전은 'F/W + VPN-A', 'F/W + VPN-B', 'F/W + VPN-B' 세 가지이며, 이는 각각 다른 레이블을 사용하여 식별되어야 한다.

- (예2)의 경우 TOE 버전은 하나이며, TOE가 포함하는 모델이 세 가지이므로 하나의 레이블 및 각 모델명을 조합하여 식별되어야 한다.
- (예3)의 경우 TOE 구성요소 중 Client-A, Client-B, Client-C는 항상 TOE 구성요소로서 배포되며, TOE가 설치 후 운용되는 IT 환경에 따라 사용자가 원하는 구성요소만을 선택적으로 사용하므로 하나의 레이블을 사용하여 식별할 수 있다. 다만, TOE 형상관리체계에서 Client-A, Client-B, Client-C 중 어느 것 하나라도 변경되는 경우 TOE 버전도 변경되도록 관리되어야 한다.
- (국제용) TOE가 배포되는 IT 제품의 일부인 경우 IT 제품과 TOE의 식별자를 분리하여 전체 IT 제품이 평가된 것으로 오도되지 않아야 한다.

32 **⑤ 하드웨어 일체형 장비로 판매·배포되는 제품의 경우 다음을 적용한다.**

33 개발업체 형상관리 체계에 따라 제품의 모델명은 내장되는 소프트웨어/펌웨어 및 하드웨어 모델에 대한 식별자 등을 고려하여 달라질 수 있으므로 형상관리 평가 시 TOE 식별자의 적절성을 결정해야 한다.

34 운영체제와 응용프로그램은 별개의 구성요소로 분리될 수도 있고, 혼합되어 경계가 명확하지 않을 수도 있다.

35 **⑤-1 (국내용, 국제용) TOE의 물리적 범위 평가 시 다음을 적용한다.**

36 (국내용) TOE는 제품과 동일해야 하고, (국내용, 국제용) TOE는 TSF 제공을 위해 하나의 제품으로써 동작하므로 하드웨어 일체형 장비 전체를 TOE의 물리적 범위로 산정해야 한다.

- TOE 및 TOE의 구성요소를 모두 식별해야 한다. 특히, TOE가 여러 하드웨어 일체형 장비 제품을 통칭하는 제품 라인의 대표성을 지닌 식별자인 경우, (그림 2.1-1)의 예를 참고한다.
- TOE 구성요소별 구현 형태(하드웨어, 펌웨어, 소프트웨어)를 모두 식별해야 한다.
- 개발업체 형상관리 체계에 따라 식별하며, TOE에 포함되는 '범용이 아닌' 운영체제 포함 제3자 제공 소프트웨어, 펌웨어 등을 모두 식별해야 한다.

37 '범용 운영체제'를 사용하는 경우, 응용프로그램만으로 TOE 물리적 범위를 산정하며, 하드웨어 일체형 장비의 모델명을 그대로 TOE 명칭에 사용하는 것은 허용되지 않는다.

38 **⑤-2 (국내용, 국제용) TOE의 논리적 범위 평가 시 다음을 적용한다.**

39 TOE 물리적 범위에 포함된 운영체제의 평가범위는 ST에 정의한 SFR과의 관련

성을 분석하여 TSF 부분을 신청된 평가보증등급에 적합하게 평가해야 한다(이는 TOE의 논리적 범위에서 결정).

40 즉, 하드웨어 일체형 장비 전체가 TOE의 물리적 범위로 산정되더라도 TSF를 제공하지 않는 하드웨어, OS 대부분은 보증의 범위가 아닐 수 있다.

41 평가 시 유의해야 할 사항의 예는 다음과 같다(EAL에 따라 적합하게 평가).

- ALC 전반적으로 개발자 절차에 OS가 포함되어 있는지 확인: 형상항목 목록에 OS 자체 및 OS 소스코드 포함 여부 확인 등 하드웨어 일체형 장비 전체에 대한 관리
- AGD(설명서) 평가: OS 명령어라도 TSF 운영에 필요한 명령어는 설명서에서 모두 설명
- ADV_FSP(기능명세) 평가: TSF 동작에 필요한 OS 환경설정 파일, 레지스트리 등은 모두 TSFI로 식별
- ADV_TDS(TOE 설계) 및 ADV_IMP(구현의 표현) 평가: TSF 동작에 필요한 OS 기능/서비스 변경, 추가 시 관련 부분은 모두 TSF이므로 설계문서 및 구현의 표현에 포함
- ADV_ARC(보안 아키텍쳐) 평가: OS가 제공하는 영역분리/자체보호/우회불가성 속성은 모두 TOE의 보안 속성으로 평가
- ATE(시험) 평가: TSF로써 식별된 OS 부분에 대한 기능시험 수행
- AVA(취약성 분석) 평가: TSF로써 식별되지 않은 OS 명령어, 서비스 등을 사용하여 TSF를 우회할 수 있는 경로 존재 여부 확인

42 ⑥ 기타 원칙은 다음과 같다.

43 ⑥-1 (국내용, 국제용) '범용이 아닌 운영체제'의 사용은 운영체제의 커스터마이즈가 반드시 필요한 하드웨어 일체형 장비와 같은 형태의 제품으로 제한한다. 또한, 역으로 하드웨어 일체형 장비에는 그 명칭에서 직관적으로 의미하는 바와 같이 특정한 하드웨어에 의존하므로 '범용 운영체제'는 사용할 수 없으며, 하드웨어에 대한 종속성으로 인해 커스터마이즈가 반드시 필요한 '범용이 아닌 운영체제'만을 사용할 수 있다.

44 ⑥-2 (국내용, 국제용) '범용 운영체제'에 설치되는 소프트웨어 응용프로그램인 경우 해당 소프트웨어인 응용프로그램만을 TOE 범위로 산정하며, 다음 원칙을 추가로 적용한다.

- TOE는 소프트웨어 응용프로그램으로서 평가·인증되어야 한다.
- 평가 시 ST, ATE, IND에 TOE 식별 시 소프트웨어로 식별하고, TOE를

설치하기 위해 필수적인 운영환경(즉, TOE 운영에 필수적인 하드웨어/펌웨어/소프트웨어 사양)을 명시해야 한다. 하드웨어 일체형 장비와 같은 하드웨어 모델명 명시는 허용되지 않는다.

- 개발환경 보안점검 평가 시 소프트웨어인 응용프로그램 TOE를 배포하는 수단(예: CD, USB 메모리, 온라인 다운로드 링크 제공 등) 및 절차를 검증해야 한다.
- AGD 평가 시 소프트웨어인 응용프로그램 관점에서 인수 및 설치, 운용하기 위한 설명서가 제공되는지 검증해야 한다. 사용자가 소프트웨어인 TOE를 설치하기 위해 필요한 하드웨어 및 '범용 운영체제'를 준비할 수 있도록 가이드를 제공하는지 검증해야 한다.
- 인증 완료 후 판매·배포되는 제품은 소프트웨어인 응용프로그램이어야 한다.

2.2 TOE 운영환경 서술 및 평가 시 주의사항

적용 범위	☑ 국제용 인증	☑ 국내용 인증

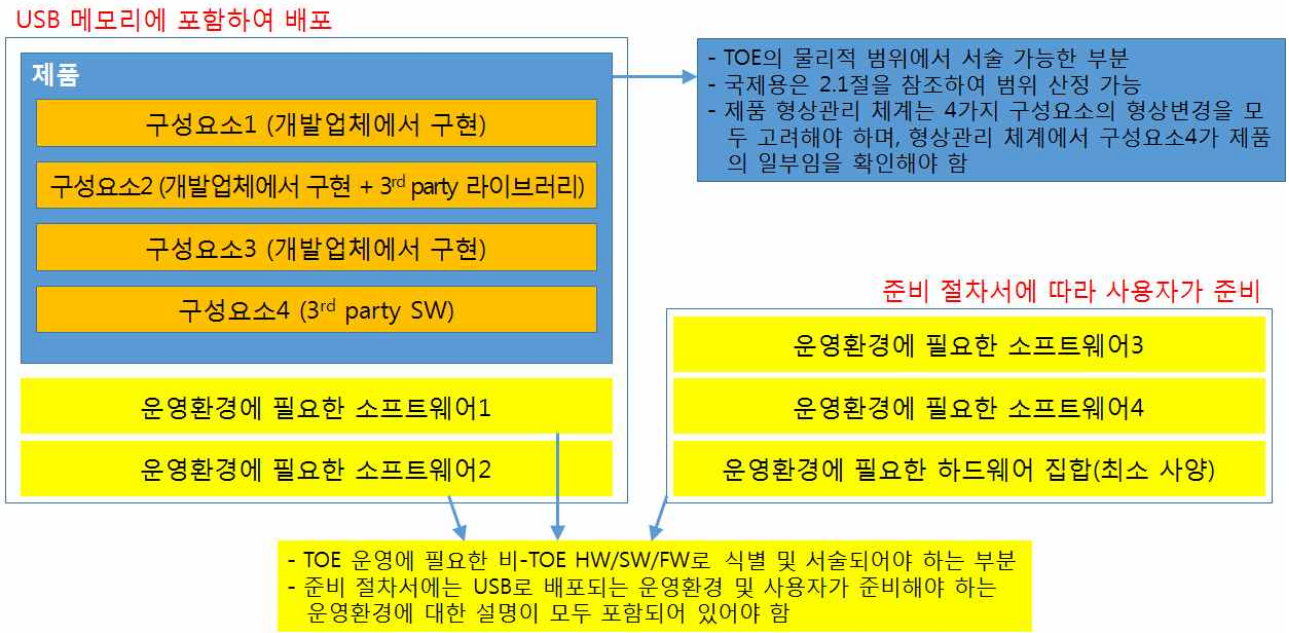
45 TOE는 TSF를 수행하기 위해 운영환경이 필요할 수 있으며, ST에 TOE가 아닌(non-TOE) 하드웨어/소프트웨어/펌웨어를 서술하는 것과 관련된 CEM의 작업 단위는 아래와 같다.

CEM V3.1 R2 CEM V3.1 R5	ASE_INT.1-8 TOE에서 **요구되는** 비-TOE에 해당하는 하드웨어 /소프트웨어 /펌웨어 non-TOE hardware/software/firmware **required** by the TOE 328항(R2) / 374항(R5) **TOE 운영에 의해 필요한** 모든 추가 하드웨어, 소프트웨어, 펌웨어 any additional hardware, software and firmware **needed by the TOE to operate** TOE의 잠재적인 소비가가 현재의 하드웨어 ,소프트웨어, 펌웨어가 **TOE의 사용을 지원하는지 결정할 수 있을 만큼 충분히 상세하게 서술** **detailed enough** for potential consumers of the TOE **to determine** whether their current hardware, software and firmware **support use of the TOE**

46 ASE_INT.1-8에서 서술한 바와 같이 TOE에서 요구되는 'non-TOE 하드웨어/소프트웨어/펌웨어'에 해당하여 ST에 TOE 운영환경으로 포함하고자 하는 경우 TOE 운영에 필요함을 설명하고 서술해야 한다.

- ① '제품'이 무엇인지 명확하게 식별해야 한다. 소프트웨어 형태의 제품이 이동식 저장매체(예: CD, USB 등)에 포함되어 배포되는 경우, 저장매체가 '제품'은 아님에 유의한다. 이동식 저장매체(예: CD, USB 등)에는 '제품'이 아닌 운영환경에 필요한 소프트웨어도 함께 포함될 수 있다.
- ② 2.1절을 적용하여 'TOE'의 물리적/논리적 범위를 명확하게 식별해야 한다.
- ③ TOE 운영에 필요한 비-TOE 하드웨어/소프트웨어/펌웨어는 TOE와 함께 배포될 수도 있으며(예: 소프트웨어 TOE가 포함된 CD, USB 등에 함께 포함), 준비 절차서(AGD_PRE.1)에 따라 사용자 사이트에서 구축할 수도 있다. 용도를 직관적으로 알 수 있는 경우도 있으나(예: CPU, RAM, HDD, NIC, OS 등), 용도에 대한 명확한 설명이 추가되어야 하는 경우도 있다(예: 운영환경에 필요한 소프트웨어).
- ④ 소프트웨어 TOE를 설치하고 운영하기 위한 '최소사양'을 서술하는 경우 실제 시험환경으로 구축 가능한 사양인지 확인해야 한다(예: RAM 용량, HDD 용량 등이 현실적으로 적용 가능한지 확인).

<예시>



47 소프트웨어 TOE의 하부 운영체제 식별 시 운영체제의 정식 배포판 명칭을 사용해야 하며, 운영체제의 bit수(32bit, 64bit)를 함께 표기해야 한다. 또한, Linux 계열의 경우 커널 버전을 함께 표기해야 한다.[8)9)]

8) TOE의 하부 운영체제는 평가 시 시험 및 취약성 분석 환경에 영향을 주는 중요한 운영환경으로 예상 평가기간 산정 시 영향을 준다. ST에 TOE 운영환경으로 여러 가지 하부 운영체제를 서술하는 경우, 신청기관 및 평가기관은 운영체제 배포판별로 TOE 평가에 어떤 영향을 주는지 분석하여 예상 평가기간 산정 시 반영할 수 있다.

9) TOE가 범용이 아닌 운영체제를 포함하는 하드웨어 일체형 장비와 같은 형태의 제품인 경우, 운영체제의 기반이 되는 커널 버

48 스마트폰에 설치되는 에이전트(예: 스마트폰 보안관리 에이전트, 가상사설망 에이전트 등) 형태의 소프트웨어인 경우 TOE 운영환경으로 다음과 같은 정보를 제공해야 한다.

- ST 및 ETR에는 아래와 같이 스마트폰 사양 등을 운영환경으로 표기

제품명	모델명	OS		빌드 버전	SDK 버전	APK 버전
		안드로이드 버전	커널 버전			
<스마트폰 명칭>	*<스마트폰 모델명칭>*	*4.4.2 (KitKAT)*	*3.4.5*			

  - 제품명: 제조사 포함한 제품명 표기
  - 모델명: 통신사 포함하여 모델명 표기
  - 안드로이드 버전: 버전 및 코드네임 포함하여 표기
  - 커널 버전: 운영체제 커널 버전 표기
  - 빌드 버전: APK 빌드 버전
  - SDK 버전: 사용한 SDK 버전
  - APK 버전: 스마트폰에 설치되는 에이전트의 APK 버전(TOE 구성요소 참조정보와 동일함)

- 인증보고서에는 아래와 같이 스마트폰 사양 등을 운영환경으로 표기

제품명	모델명	OS	
		안드로이드 버전	커널 버전
<스마트폰 명칭>	*<스마트폰 모델명칭>*	*4.4.2 (KitKAT)*	*3.4.5*

  - 빌드버전 및 SDK 버전은 공개하지 않음
  - APK 버전은 TOE 구성요소 참조정보로써 공개됨

49 소프트웨어 TOE의 운영에 필요한 하부 운영환경 중 하드디스크(HDD)의 경우 'TOE 설치에 필요한 공간 *<용량(예: 50GB)>* 이상'으로 표기한다. TOE 운영환경(예: 운영체제, TOE 운영에 필요한 필수 소프트웨어 등)을 위한 하드디스크 공간을 언급하지 않으며, TOE 설치에 필요한 공간 확인은 평가자가 설치 시험 시 수행해야 한다. 하드디스크(HDD)를 제외한 하드웨어(예: CPU, RAM, NIC 등)는 물리적인 하드웨어 사양을 기재해야 하며, 최소 사양 이상으로 표기할 수 있

전이나 배포판 명칭 및 bit수를 표기해야 한다.

다(예: RAM 512MB 이상).[10)]

50 또한, TOE 운영환경에는 TOE "사용자"가 존재할 수 있으며, CC 1부의 용어정의에 따라 사용자는 다음과 같으며, TOE의 외부 실체는 TOE와 상호작용해야 한다.

CC V3.1 R1 CC V3.1 R5	94항(R1) / 102항(R5) 사용자(User) - "외부 실체 " 참조 user - see external entity 44항(R1) 외 부 실체 (external entity) - TOE의 외부에서 TOE와 **상호작용하는**(또는 상호 작용할 수도 있는) 실체(**사람 또는 IT**) external entity - any entity(**human or IT**) outside the TOE that **interacts**(or may interact) with the TOE 50항(R5) 외부 실체(external entity) - TOE의 외부에서 TOE와 **상호작용하는 사람 또는 IT 실체** external entity - **human or IT entity** possibly **interacting** with the TOE from outside of the TOE boundary

- TOE가 감사 데이터 생성 시 필요한 타임스탬프를 외부 NTP 서버에서 제공 받는 경우(NTP 서버), 보안위반 사건 발생 시 관리자에게 이메일로 통보하는 기능이 있는 경우(SMTP 서버) 등, TOE와 연동하는 외부 IT 실체가 운영환경에 존재할 수 있으며, 명시적인 외부 IT 실체 식별자 없이 NTP 서버, SMTP 서버 등으로 식별하는 것이 가능하다.
- ESM 등과 같은 TOE의 경우 관리대상시스템, 관제대상시스템이 운영환경의 외부 IT 실체로 필수적으로 존재하고 TOE와 연동한다는 것을 시험을 통해 입증해야 하므로, 모든 외부 IT 실체를 명확히 식별해야 한다.
- TOE가 제공하는 인터페이스를 통해 TSF를 사용하는 TOE 사용자는 Human User(예: 관리자, 일반사용자 등), IT 실체 등 모두 가능하나, TSF를 사용하기 위해 '호출-응답'이 가능해야 한다.
- TOE가 TSF를 제공하는데 영향을 주지 않거나, TOE 운영환경에 필수적으로 존재해야 하는 타당한 사유가 없는 경우 명시하지 않는다.
- 인증된 TOE 운영환경은 TOE 설치 및 운영에 필요한(즉, 영향을 주는) 최소한의 운영환경만을 명시하며, 사용자가 특정 IT 실체를 운영환경에

10) TOE가 하드웨어 일체형 장비와 같은 형태의 제품인 경우 2.1절에 따라 전체 하드웨어 일체형 장비가 TOE로 산정되며, 이 때 하드웨어 모델별 사양은 고정해서 표기해야 한다. 다만, 2.3절에 따라 확장 모델을 표기하는 것이 가능하다.

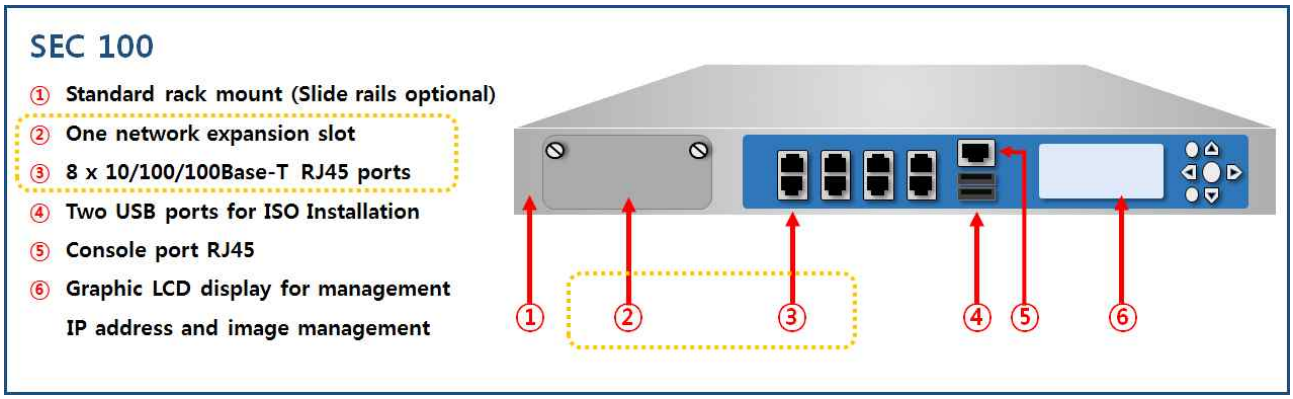
추가하여 TOE를 운영하는 것은 사용자가 결정할 사안이다.

51 평가자는 비-TOE 하드웨어/소프트웨어/펌웨어 및 TOE 외부 실체가 TOE 운영 환경에 존재함을 평가자 시험환경 구축을 통해 입증해야 한다.

2.3 하드웨어 일체형 장비의 확장 모델 서술 및 평가 방안

적용 범위	☑ 국제용 인증	☑ 국내용 인증

52 TOE가 하드웨어 일체형 장비 형태의 제품인 경우 하드웨어 모델 사양 일부가 확장 가능한 형태로 제공될 수 있다. 이 때 하드웨어 기본 모델을 중심으로 특정 하드웨어 사양 일부를 추가 장착하는 것을 하드웨어 확장 구성이라 한다. 다음은 하드웨어 확장 구성의 예시이다.



기본 모델[11]	확장 가능 범위	Network Expansion Slot options(1slot)
Intel Xeon Processor E3-1275 * 1 8x10/100/1000Base-T RJ45 Ports 4 GB Memory 250 GB Hard Disk drive One AC Power Supply	4 GB RAM upgrade(optional) Network Expansion slot : 1 slot	4X10/100/1000Base-T RJ45 Ports 8x10/100/1000Base-T RJ45 ports 2x1000Base-F SFP ports 4x10G Base-F SFP Ports

Max Configuration
16x10/100/1000Base-T RJ45 Ports 8x10/100/1000BSE-T RJ45 + 4x10G BaseF SFP Ports 8GB Memory

53 TOE가 하드웨어 일체형 장비 형태의 제품인 경우 NIC, HDD, Memory, 보안기능 수행 하드웨어(예: 암호가속기 등)는 확장할 수 있으며 그 밖의 하드웨어(예: CPU)는 확장 구성이 허용되지 않는다.

54 확장 가능한 하드웨어 모델의 표기 방법은 다음과 같다.

11) CPU는 유일하게 식별되어야 한다(예: CPU 모델명 표기).

- 확장이 가능한 하드웨어 모델을 표기하는 경우 기본 모델과 확장 가능한 범위, 최대 구성 가능한 하드웨어 사양을 서술해야 한다.
- 기본 모델은 제품이 동작하는데 필요한 최소 하드웨어 구성요소를 포함해야 한다(예: CPU, Memory, HDD, NIC).

55 ① NIC가 확장된 경우 다음 예시와 같이 기본 구성, 확장 구성, 최대 구성을 서술할 수 있다.

기본 구성	**설명**	기본구성은 기본으로 제공되는 NIC 슬롯 및 해당 슬롯이 제공 인터페이스 형태 및 개수를 기술
	작성 예시 1	기본 구성으로 선택 가능한 NIC 종류가 1종류인 경우 기본 구성 작성 예시 <작성 예> - NIC : 8 x 10/100/1000Base-T RJ45 ports
	작성 예시 2	기본구성으로 선택 가능한 NIC 종류가 2종 이상인 경우 기본 구성 작성 예시 ※ 다수의 NIC 중 기본 구성을 선택할 수 있도록 서술 가능 <작성 예> - 슬롯에 장착 가능한 다음 NIC 종류 중 1개 택일 - 슬롯에 장착 가능한 NIC 종류 ✓ 타입 1: 1 G Fiber – 4 Ports ✓ 타입 2: 10 G Fiber – 4 ports ✓ 타입 3: 10 G Fiber - 2 Ports1 ✓ 타입 4: 1 G Copper – 8 Ports
확장 구성	**설명**	확장 구성은 기본 슬롯 외 추가적으로 장착할 수 있는 NIC 슬롯에 대한 개수 및 제공 인터페이스 형태, 개수 기술
	작성 예시	<작성 예> NIC 확장 슬롯은 2개이며, 아래와 같은 NIC 슬롯이 추가 장착 가능 - 8 x 10/100/1000 Base-T RJ45 ports - 2 x 1000 Base-F SFP ports
최대 구성	**설명**	기본 구성 + 확장 구성을 통해 구성할 수 있는 최대 NIC 개수
	작성 예시 1	장착 가능한 NIC 종류별 최대 구성 가능한 NIC 종류 및 개수를 모두 기술하는 형태 <작성 예> - 16 x 10/100/1000Base-T RJ45 ports or - 8 x 10/100/1000Base-T RJ45 ports + 2 x 1000Base-F SFP ports
	작성 예시 2	제공되는 NIC의 종류가 다양하고 확장 가능한 슬롯의 개수가 많은 경우 최대 구성을 요약하여 기술하는 형태

		<작성 예> - 6개 슬롯(기본+확장 구성)에 장착 가능한 NIC 타입을 이용해 모두 장착한 형태 - 슬롯에 장착 가능한 NIC 종류 ✓ 타입 1: 1G Fiber – 4 Ports ✓ 타입 2: 10G Fiber – 4 Ports ✓ 타입 3: 10G Fiber – 2 Ports ✓ 타입 4: 1G Copper – 8 Ports

56 ② HDD가 확장되는 경우 다음 예시와 같이 기본 구성, 확장 구성, 최대 구성을 서술할 수 있다.

기본 구성	[설명] 기본으로 제공되는 HDD의 용량과 개수를 기술 [작성 예시] HDD : 500 GB **x** 1개 ※ 다수의 HDD 중 기본 구성을 선택할 수 있도록 서술 가능(NIC 기술 방식 참조)
확장 구성	[설명] 기본 구성 외 추가 장착 될 수 있는 HDD의 용량과 개수를 기술 [작성 예시] 확장 HDD **:** 500 GB **x** 1개
최대 구성	[설명] 기본 구성 + 확장 구성을 통해 구성할 수 있는 최대 HDD 용량 HDD : 500 GB **x** 2개

57 ③ 보안기능을 수행하는 하드웨어(예: 암호가속기 등)가 확장되는 경우 다음 예시와 같이 기본 구성 및 확장 구성을 서술할 수 있다.

기본 구성	[설명] 기본으로 장착되는 암호가속기의 사양 및 개수를 기술 [작성 예시] 암호가속기 : 장착되지 않음
확장 구성	[설명] 기본 구성 외 장착되는 암호가속기 사양 및 개수 기술 [작성 예시] 암호가속기 : Crypto Accelerator 1000 1개 장착

58 ④ Memory가 확장되는 경우 다음 예시와 같이 기본 구성, 확장 구성, 최대 구성으로 서술할 수 있다.

기본 구성	[설명] 기본으로 제공되는 Memory의 용량과 개수를 기술 [작성 예시] Memory : 1 GB **x** 1개 ※ 다수의 Memory 중 기본 구성을 선택할 수 있도록 서술 가능(NIC 기술 방식 참조)
확장 구성	[설명] 기본 구성 외 추가 장착 될 수 있는 Memory의 용량과 개수를 기술 [작성 예시] 확장 Memory **:** 1 GB **x** 1개
최대 구성	[설명] 기본 구성 + 확장 구성을 통해 구성할 수 있는 최대 Memory 용량 [작성 예시] Memory : 1 GB **x** 2개

59 신청기관은 ST, 설명서, 시험서 등의 평가제출물에 TOE의 하드웨어 모델별 사양을 명확히 표기해야 한다.

60 평가자는 최초평가 또는 재평가 시 하드웨어 확장(NIC, HDD, 보안기능 수행 하드웨어, Memory)에 대해 다음 사항을 고려하여 시험 및 취약성 분석을 수행하고 평가결과를 기록해야 한다. 관련된 평가산출물은 평가단위보고서(ASE,

AGD, ALC, ATE, AVA 등), 독립시험서, 침투시험서, 평가결과보고서 등 EAL 등급에 따라 달라질 수 있다. 하드웨어 확장에 대한 모든 경우의 수를 고려하여 시험 및 취약성 분석을 수행해야 하며, 하드웨어 변경사항이 TOE에 영향을 미치지 않음이 입증되어 한다.

- Memory나 HDD가 확장 구성처리 되는 경우 구성 가능한 모델 중 하나의 모델에 대해서 전수시험을 수행하며 확장 모델에 대해서는 시동 시험을 통해 확장 모델이 안정적으로 확장된 하드웨어 환경을 인식하는지 확인한다.
- NIC가 확장 구성처리 되는 경우 확장 가능한 NIC 형태를 모두 지원 가능한지 시험한다. 예를 들어, 기본 NIC로 1 GB를 지원하고 확장으로 10 GB 인터페이스를 지원하는 경우 1 GB와 10 GB가 모두 시험될 수 있도록 시험 시 고려해야 한다.
- 보안기능을 수행하는 하드웨어가 확장 구성처리 되는 경우 해당 하드웨어가 존재하는 경우와 존재하지 않는 경우 모두 보안기능이 정상적으로 동작하는지 시험해야 한다.

61 평가자는 인증효력유지(변경승인) 시 다음 사항을 고려해야 한다.

- 하드웨어가 확장 가능한 형태의 모델도 인증효력유지(변경승인) 가능하며, 인증효력유지(변경승인) 시에도 확장 가능한 하드웨어 범위는 NIC, HDD, 보안기능 수행 하드웨어, Memory로 최초 평가와 동일하다. 평가자는 하드웨어 확장에 대한 모든 경우를 고려하여 시험을 수행해야 하며, 하드웨어 변경사항이 TOE의 보증에 경미한 영향만을 미침을 입증해야 한다.
- 인증 받은 모델의 사양은 항시 유일성을 보장해야 하므로 인증효력유지(변경승인) 시 기 인증모델을 변경할 수 없다.
- 기존의 인증받은 모델의 하드웨어 단종 등을 이유로 하드웨어 사양을 변경하여 기존 모델의 인증효력유지(변경승인)할 수 없으며, 필요 시 신규 모델을 추가하여 인증효력유지(변경승인) 함으로써 기존 모델의 유일성을 유지해야 한다.
- 최초 평가 시 평가되지 않은 TOE 보증에 주요한 영향을 주는 하드웨어 종류는 인증효력유지(변경승인) 시 추가, 변경할 수 없다.[12)]

12) 예를 들어, 최초 평가 결과 하드웨어 암호 가속기가 없는 모델만 인증 받은 경우 암호 가속기가 포함된 모델에 대한 인증효력유지(변경승인)는 허용되지 않는다. 또 다른 예로, DDoS 대응장비의 경우 NIC을 Ethernet에서 Fiber로 변경하는 경우 성능 측정을 다시 해야 하는 사안이므로 경미한 변경으로 볼 수 없다.

2.4 업데이트 및 파일 전송 기능 보안수준

적용 범위	□ 국제용 인증[13]	☑ 국내용 인증

62 정보보호제품이 온라인 업데이트 기능을 포함하거나 파일을 배포하는 기능을 포함하는 경우 발생 가능한 보안 취약점(예: 업데이트 서버 위장, 업데이트 되는 파일 노출 및 위·변조, 악성코드 배포 등)에 대응하기 위하여 업데이트 기능 및 파일 배포 기능의 보안수준을 정의할 필요가 있다. 예를 들어, Windows 운영체제가 설치된 PC의 에이전트는 업데이트 서버 또는 관리서버(또는 배포서버)로부터 파일(예: 패치파일, 안티바이러스 제품 엔진 및 시그니처 등)을 업데이트할 수 있고, 네트워크기반 정보보호제품(예: 침입방지시스템 등)은 업데이트 서버로부터 파일(예: 시그니처 등)을 업데이트할 수 있으며, 정보보호제품은 필요 시 보안목적에 의해 파일(예: 패치파일 등)을 배포하는 기능을 포함해야 할 수 있다.

63 본 절에서 업데이트 서버, 관리서버(또는 배포서버)는 다음과 같은 역할을 수행하는 것으로 가정한다.

- 업데이트서버 : 제품 업데이트 파일, 안티바이러스 제품 시그니처 파일, 유해 트래픽 탐지 시그니처 파일 등을 보관하는 서버로 TOE 개발업체에서 관리/운영
- 관리서버(또는 배포서버) : 에이전트에 정책을 내려주는 서버

64 Windows 운영체제가 설치된 PC의 에이전트에 온라인 업데이트 기능 및 파일 배포 기능을 포함하는 정보보호제품은 기본적으로 다음과 같은 원칙을 적용하여 구현해야 한다.

- (업데이트 서버 ↔ 관리서버(또는 배포서버) ↔ 에이전트), (관리서버(또는 배포서버) ↔ 에이전트), (업데이트 서버 ↔ 에이전트) 간 파일 전송 시 전자서명 검증을 수행하여 전송되는 파일에 대한 부인방지 및 무결성 보호 기능 제공

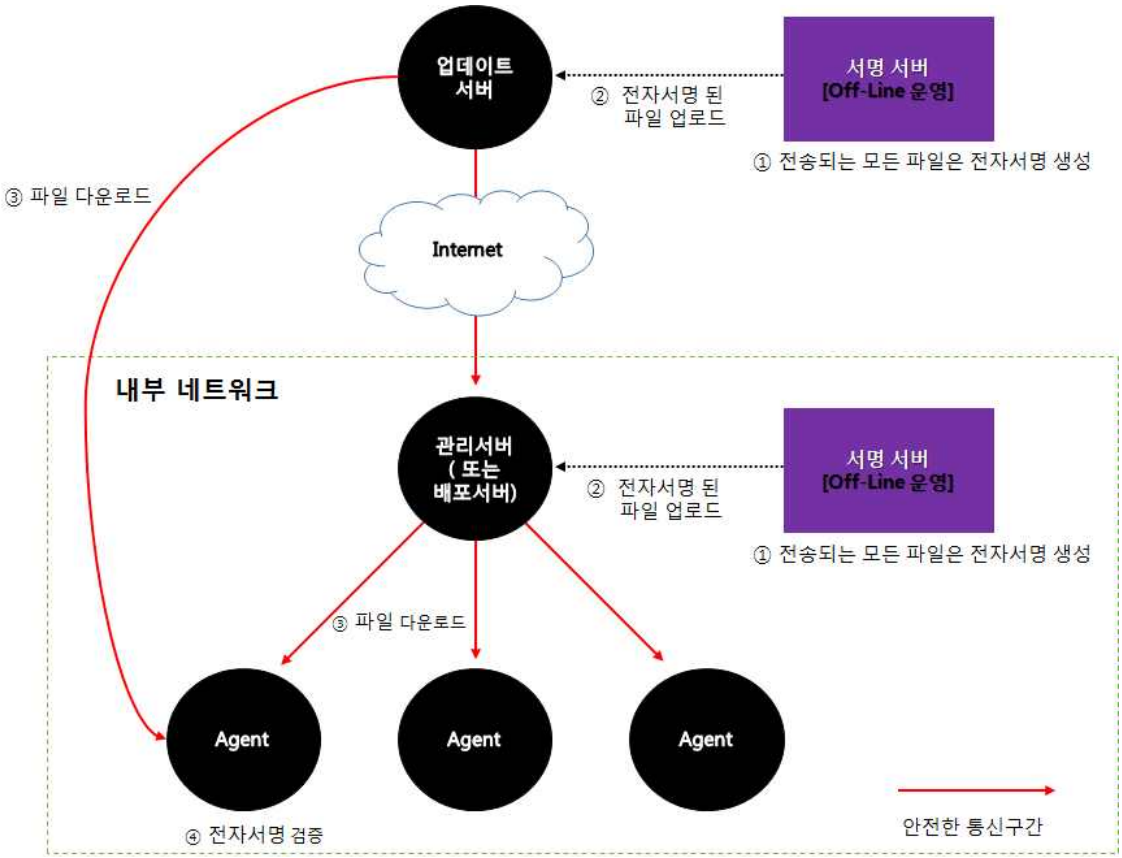
65 에이전트로 전송 가능한 파일의 종류는 다음과 같다.

- 업데이트 파일 등 제품 설치파일 : 제품구성과 관련된 모든 파일. 에이전트 업데이트 파일을 포함하며, 안티바이러스 제품인 경우 엔진파일 및 시그니처를 포함한다.
- 에이전트 정책 파일

13) 국제용 인증 시 준수하는 보호프로파일, 취약성 분석 등에 따라 요구사항이 존재할 수 있으므로 신청기관 및 평가기관은 본 문서가 아닌 평가신청한 TOE가 준수해야 하는 요구사항을 확인해야 한다.

- 일반파일: 제품구성과 무관하며 설치파일 및 정책파일에 포함되지 않는 모든 파일(예: 패치파일, 일반 실행파일 등). 일반파일 배포기능은 원칙적으로 허용되지 않으며, 일반파일 배포기능을 구현한 경우 배포 가능한 파일 유형 및 기능의 필요성을 보안적 측면으로 입증해야 한다. 스마트폰 보안관리 제품의 관리서버에서 스마트폰 보안관리 제품 에이전트로 일반파일(APK)을 배포하는 것은 원칙적으로 허용하지 않는다. 패치관리 시스템의 경우 패치파일을 배포하는 것이 주 기능이므로 이는 허용된다.

2.4.1 Windows 운영체제가 설치된 PC기반 정보보호제품(예: 패치관리시스템, 안티바이러스 제품 등)[14] 및 스마트폰 보안관리 제품



(그림 2.4-1)

66 (업데이트 서버 ↔ 관리서버(또는 배포서버) ↔ 에이전트)의 경로에서 개발업체의 업데이트 서버에서 전달된 업데이트 파일(개발업체에서 안전한 전자서명 수행)이 관리서버(또는 배포서버)를 통하여 에이전트로 직접 전달되는 경우, 관리서버(또는 배포서버)에서 추가적인 전자서명 검증 및 전자서명 생성은 수행할 필요가 없으며, 최종적으로 에이전트에서 전자서명 검증을 수행하도록 구현할 수 있다.

14) Windows 운영체제가 설치된 PC에 설치되는 가상사설망 클라이언트와 같이 PC기반 정보보호제품에는 해당하지 않으나, Windows 운영체제가 설치된 PC에서 설치되는 에이전트/클라이언트 업데이트 시에도 전자서명이 적용됨에 주의한다.

67 (업데이트 서버 ↔ 관리서버(또는 배포서버) ↔ 에이전트)의 경로 중 내부 네트워크의 관리서버(또는 배포서버)에서 TOE 개발업체가 서명하지 않은 파일을 TOE 관리자가 업로드 하는 경우 TOE 관리자가 본 절의 절차를 준수하여 전자서명을 생성해야 하며[15], 최종적으로 에이전트에서 전자서명 검증을 수행한다.

1) 전자서명 검증

68 에이전트는 업데이트 서버, 관리서버(또는 배포서버)에서 배포되는 모든 파일에 대해 전자서명 검증을 수행한다. 다만, 정책파일이 실행파일이 아닌 경우 전자서명 대상파일에서 제외되며, 비밀성 및 무결성이 보장되는 안전한 통신구간 등 안전한 배포 수단이 제공되어야 한다. 제품 설치 파일(예: 스마트폰 보안관리 제품 또는 패치관리시스템 등의 에이전트 파일)을 최초 배포하는 경우 안전한 통신(예: TLS 등)을 사용하는 조건으로 TOE(관리서버)로부터의 온라인 다운로드 할 수 있다.

69 에이전트는 서버(업데이트 서버, 관리서버(또는 배포서버))로부터 전송되는 모든 파일에 대해 부인방지 및 무결성 보장을 위해 파일 생성 주체에 대한 전자서명 검증을 수행해야 한다.

70 전자서명 검증 시 인증서 유효성도 검증해야 하며, 인증서 유효성에 대한 온라인 검증이 불가한 경우 또는 사설 인증서를 사용하는 경우 인증서의 오프라인 배포 등 대체 통제를 마련해야 한다.

2) 전자서명 생성

71 TOE 개발업체 또는 관리자가 파일에 대해 전자서명을 하는 경우 인터넷과 연결이 차단된 별도의 오프라인 서버에서 전자서명을 생성해야 한다.

72 일반파일 배포 기능이 보안적 측면에서 필요하여(예: 패치관리시스템에서 패치파일 배포) TOE 개발업체 또는 관리자가 일반파일을 배포하는 경우 전자서명을 생성한 역할의 책임추적이 가능한 방식(예: 지문형 보안토큰 사용)으로 전자서명을 생성한다.

- 패치관리시스템의 경우 패치파일을 배포할 때 반드시 TOE 개발업체 내 오프라인 서버에서 전자서명을 생성한 역할의 책임추적이 가능한 방식(예: 지문형 보안토큰 사용)으로 TOE 개발업체가 전자서명을 생성한 후 TOE 개발업체의 업데이트 서버로 업데이트 관리자가 업로드하여 배포해야 한다.[16]
- TOE 개발업체 또는 관리자는 배포되는 파일의 전자서명 생성 및 안전한 배포를 관리하기 위해 절차적 보안대책(예: 오프라인 서버에서 안전

15) TOE 개발업체가 전자서명한 파일을 관리자가 업로드 하는 경우 추가적으로 전자서명할 필요가 없다.

16) 패치파일 개발업체의 서명(예: Code Signing)이 TOE 개발업체의 전자서명 생성을 대체할 수 없음에 유의한다.

한 전자서명 생성 후 업데이트 서버로의 안전한 이동 및 업로드 절차 등)을 수립해야 한다.

73 TOE 개발업체가 전자서명을 생성하는 경우, 개발환경 보안점검을 위한 업체 실사 시 관련 보안대책이 적용되고 있는지 점검하고 기록해야 한다.

74 TOE 관리자가 전자서명을 생성한 파일을 배포할 수 있는 경우, TOE를 사용하는 조직에서 관련 보안대책을 준수할 수 있도록 설명서에 적절하게 서술하고 있는지 평가해야 한다.

3) 인증서 생성 및 갱신 규칙

75 서버의 인증서 유효기간은 1년 이내로 설정해야 하며, 암호 알고리즘 및 암호비도 정책에 따라 암호비도 112bit 이상을 만족하는 암호 알고리즘을 사용해야 한다.

76 인증서는 만료 전 갱신되어야 하며, 외부의 인증서기반 인증체계를 이용할 경우 갱신기능은 해당 인증체계를 따라 구현되어도 무방하다. 인증서 만료 전(최소 1개월 전)에 갱신된 인증서를 배포해야 하며, 인증서가 만료된 경우 개발업체가 이를 오프라인으로 업데이트를 해주거나 홈페이지에서 인증서를 제공하여 필요한 사용자가 인증서를 다운로드하여 사용할 수 있도록 조치할 수 있다.

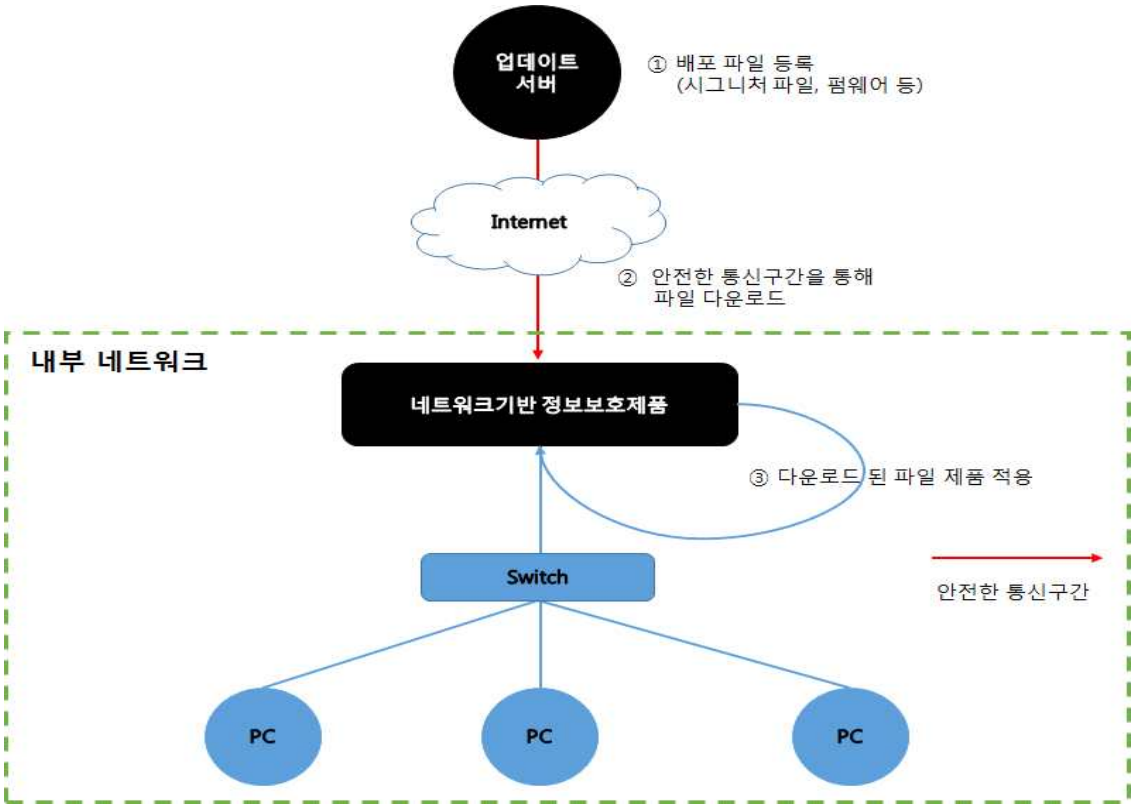
4) 주의사항

77 클라이언트 PC의 환경설정 파일 내에 업데이트 서버 주소 등이 포함된 경우 해당 정보가 포함된 파일에 대해 무결성을 보장해야 한다.

2.4.2 네트워크기반 정보보호제품(예: 침입방지시스템 등)

78 업데이트 서버에서 네트워크기반 정보보호제품(예: 침입방지시스템 등)으로 배포되는 모든 파일은 비밀성 및 무결성이 보장되는 안전한 통신구간 등의 안전한 배포 수단을 통해 배포되어야 한다.[17]

17) 국가용 보안요구사항 V3.0 준수 제품은 '서버 공통보안요구사항', '제품 보안요구사항'의 업데이트 관련 보안요구사항을 확인하여 필수, 조건부 필수, 선택 요구사항에 적합하게 보안요구사항을 구현해야 한다(예: 서버 공통보안요구사항'의 5.1.1).



(그림 2.4-2)

2.4.3 그 밖의 정보보호제품

79 그 밖의 정보보호제품(예: 서버접근통제 등)에 업데이트 서버로부터 온라인 업데이트하는 기능을 포함하거나 파일을 배포하는 기능을 포함하는 경우, 배포되는 모든 파일은 비밀성 및 무결성이 보장되는 안전한 통신구간 등의 안전한 배포 수단을 통해 배포되어야 한다.[18)]

2.4.4 평가 시 요구사항

80 AVA(취약성 평가), ALC(생명 주기지원), AGD(설명서) 평가 시 업데이트 기능이나 파일 전송 기능을 갖는 정보보호제품에 대해 본 절을 준수했음을 평가해야 한다.

18) 국가용 보안요구사항 V3.0 준수 제품은 '서버 공통보안요구사항', '제품 보안요구사항'의 업데이트 관련 보안요구사항을 확인하여 필수, 조건부 필수, 선택 요구사항에 적합하게 보안요구사항을 구현해야 한다(예: 서버 공통보안요구사항'의 5.1.1).

2.5 검증필 암호모듈 탑재 확인 절차

적용 범위	☑ 국제용 인증	☑ 국내용 인증

81 국가공공기관 도입을 목적으로 CC 인증을 받는 일부 정보보호제품은 검증필 암호모듈을 탑재해야 하며, 평가 신청기관은 평가 완료 전까지 반드시 암호모듈 검증제도에서 검증된 암호모듈을 적용해야하고 평가자는 검증필 암호모듈이 정확하게 탑재되었는지 확인해야 한다.[19)]

82 검증필 암호모듈 탑재 확인은 다음의 절차를 따른다. 본 지침은 평가보증등급(EAL)에 관계없이 적용한다.[20)]

83 신청기관은 평가대상 제품에 검증필 암호모듈을 탑재하여 사용하고자 하는 경우 다음에 유의한다.

- 검증필 암호모듈은 검증 시 형상을 그대로 사용해야 한다.
- 검증필 암호모듈의 보안정책문서에 서술된 운영환경과 검증필 암호모듈이 탑재된 평가대상 제품의 운영환경이 일치해야 한다.
- 검증필 암호모듈을 사용하여 암호키 생성/분배/파키, 암호 연산 등을 수행하는 경우 최신 관련 요구사항(예: 국가용 정보보호제품 보안요구사항, 국가용 보호프로파일 등)을 확인해야 한다.

2.5.1 준비단계

84 ① 평가자는 평가 신청기관의 평가대상 제품('이하 TOE')에 탑재된 검증필 암호모듈을 직접 채취한다.

85 ② 평가자는 제품의 운영체제 종류, 운영체제 버전 및 bit수를 확인한다.

86 ③ 평가자는 국가정보원 홈페이지(www.nis.go.kr)에서 암호모듈 형상 데이터를 생성하기 위한 해시값 프로그램과 검증필 암호모듈 목록에 등재된 해당 검증필 암호모듈의 보안정책문서 및 형상데이터(해시)를 다운로드한다.

2.5.2 검증단계

87 ① 평가 시 준비단계에서 수집된 정보(암호모듈명, 암호모듈 운영체제 명칭/버전/bit수 등)에 기반하여 제품에 탑재된 검증필 암호모듈이 형상 변경 없이 검증된 상태임을 확인하기 위해 평가기관 담당자는 국가정보원 홈페이지로부터

19) 검증필 암호모듈을 탑재해야 하는 제품유형은 가상사설망, 문서 암호화, 데이터베이스 암호화, 통합인증이다.

20) CEM에 따라 EAL에 관계없이 대체시험 방법으로 구현의 표현을 활용할 수 있으며, 신청기관은 검증필 암호모듈 탑재 확인 절차에서 EAL에 관계없이 구현의 표현을 검증할 수 있도록 지원해야 한다.

다운로드한 해시값 프로그램을 사용하여 형상 데이터(해시)를 획득한다.

88 ② 획득한 형상 데이터(해시)와 국가정보원 홈페이지에 등재된 해당 검증필 암호모듈 형상데이터(해시)값이 일치하는지 확인하여 검증필 암호모듈의 진위를 확인한다.

89 ③ 평가 시 신청기관 담당자로부터 검증필 암호모듈의 제품설명서를 수령한 후, 검증필 암호모듈의 사용범위를 파악하여 검증필 암호모듈에서 제공하는 API만이 사용되었는지 확인한다.

1) 운영모드 확인

- 암호모듈의 동작모드 확인
  - 검증필 암호모듈의 보안정책서를 확인하여 동작모드를 확인하고 검증대상 동작모드로만 동작하도록 설정되어 있는지 확인한다. 검증필 암호모듈은 검증대상 동작모드와 비검증대상 동작모드가 존재하므로 유의한다(일부 문서에는 승인모드, 비승인모드로 기술됨).
  - 커널모드 또는 유저모드를 확인한다. 검증필 암호모듈이 커널모드에서 동작하는 암호모듈 또는 유저모드에서 동작하는 암호모듈인지 확인하여 평가결과보고서에 기재한다. 검증필 암호모듈의 보안정책 문서에서 확인가능하며 유저모드는 '*.so' 또는 '*.dll'의 확장자를 가지며 커널모드는 '*.ko'의 확장자를 갖는다.

2) 암호모듈 초기화 확인

- 검증필 암호모듈의 초기화 함수 사용여부 확인
  - 검증필 암호모듈이 사용할 메모리를 초기화하는 함수(초기화 함수는 각 검증필 모듈마다 상이함)를 사용하는지 확인한다.
  - 해당 함수는 전역환경 변수 등 메모리 할당 및 초기화를 수행한다.

3) 알고리즘 구현함수 확인

- TOE의 소스코드에서 암호화(블록암호, 해시, 공개키암호, 전자서명, 키교환, 난수생성 등) 시 검증필 암호모듈이 제공하는 API를 정확하게 사용하는지 확인한다(⑤번 절차 참조).

4) 암호키 암호화 확인

- 암호모듈에서 사용되는 비밀키, 개인키, 공개키, 인증키 등 키 또는 보안매개변수에 대한 암호화 수행 시 암호 알고리즘을 호출하는지 확인한다.

90 ⑤ 평가 시 검증필 암호모듈 내 API가 실제 동작하는지 디버깅 시험, 모듈 시험 등으로 확인한다.

- 사용자 데이터의 암·복호화 및 키 교환을 위해 검증필 암호모듈의 API를 호출하는지 개발자에 요청하여 디버그 메시지를 통해 확인한다.
- 디버그 메시지 확인 시 함수 호출관계를 확인하여 실제 검증필 암호모듈의 API가 동작하는 부분의 메시지가 정확하게 출력되었는지 소스코드 상의 디버그 메시지 출력 함수 위치를 확인한다.

2.5.3 종료단계

91 ① 평가자는 평가 종료 이전에 검증필 암호모듈과 관련된 주요 소스코드에 대한 해시값을 생성한다.

92 ② 평가 종료 후 해시값 생성 단계에서 검증필 암호모듈과 관련된 주요 소스코드에 대한 해시값이 변경되었는지 이전에 생성한 해시값과 비교하고 암호모듈을 사용하지 않도록 소스코드의 수정이 발생되었는지 확인한다.

93 ③ 제품에 탑재된 검증필 암호모듈을 다시 채취 후 해시값을 생성한 후, 검증필 암호모듈의 형상데이터(해시)문서에 기록된 해시값과 일치하는지 확인한다.

94 ④ 평가자는 평가결과보고서에 평가제품의 '검증필 암호모듈명', '검증번호', '개발사' 및 '검증일' 정보를 식별 및 명시해야 한다.

- 다음은 평가결과보고서內 검증필 암호모듈 식별 정보 작성 예시이다.

구분	세부구분	내용
검증필 암호모듈	암호모듈명	*<암호모듈 명칭>*
	검증번호	*<검증번호>*
	개발사	*<암호모듈 개발업체 명칭>*
	검증일	*<검증일>*

- 인증보고서의 '[인증제품 식별정보]'에 검증필 암호모듈 정보가 명시된다.

95 ⑤ 평가기관은 검증필 암호모듈 확인 결과를 인증기관에 평가결과보고서 제출 시 함께 송부한다.

2.5.4 IPSec 기반 VPN 제품 평가 시 추가 확인 사항

96 ① 제품에서 전송 데이터의 비밀성 및 무결성 보장을 위해 IPSec 프로토콜 사용 시, 반드시 'ESP'를 사용해야 하며, 평가자는 'ESP'의 비밀성 알고리즘 및 무결성 알고리즘이 'Null' 값으로 설정되지 않도록 제품의 UI에서 확인한다.

97 ② 'AH'는 전송 데이터에 대한 암호화를 제공하지 않으므로 제품에서 전송 데이터의 비밀성 보장을 위해 IPSec 프로토콜을 사용하는 경우 'AH'가 단독으로

사용되지 않도록 확인한다.

98 ③ 국내용의 경우, 검증필 암호모듈의 보안정책문서에 기술된 검증대상 보호함수만을 사용하여야 하며 비검증대상 보호함수가 사용되지 않도록 제품의 UI에서 확인한다. 국제용의 경우, 검증필 암호모듈의 보안정책문서에 기술된 검증대상 보호함수를 사용하도록 기본 설정되어 있어야 하며, 비검증대상 보호함수를 사용하는 것이 가능하다.

2.6 국내용 및 국제용 개발환경 보안점검 목록

적용 범위	☑ 국제용 인증	☑ 국내용 인증

99 국내용 및 국제용 인증 시 개발환경 보안점검을 수행해야 하며, 개발환경 보안점검 목록은 EAL에 따라 상이하다.

2.6.1 국내용 인증

100 국내용 인증 시 ALC(생명주기지원 클래스) 일부 보증요구사항 평가를 개발환경 보안점검으로 대체하고 있으며, 다음을 적용하여 수행한다.

- EAL2에 형상관리와 관련된 개발환경 보안점검 목록을 포함하도록 한다.
- ALC 클래스 보증요구사항 중 개발환경 보안점검이 필요한 보증요구사항을 추가하여 평가하는 경우 추가된 보증요구사항에 대한 개발환경 보안점검을 수행한다.
- 필요 시 기타 항목에 대한 개발환경 보안점검을 수행할 수 있다(예: 2.4.4절 참조).
- 국내용 인증 시 등급별 개발환경 보안점검 목록은 [붙임1]을 참조한다.
- 원칙적으로 모든 최초/재평가의 경우 개발환경보안점검을 수행한다. 다만, 2년 이내('인증일'이 아닌 개발환경 보안점검 '시작일'을 기준으로 함) 개발환경 보안점검을 수행한 이력이 있는 경우 변경이 발생되지 않은 일부 점검항목에 대해서 생략이 가능하다.
- 평가자는 신청기관으로부터 2년 이내 개발환경 보안점검을 수행한 이력이 있는지 확인하여 평가수행계획서(EWP) 작성 시 관련 내용을 기록한다.
- 평가자는 제출물설명회 및 EWP 협의 시 개발환경 보안점검 재점검 여부와 대상 점검항목에 대해서 인증기관, 평가기관, 신청기관 3자간에 협

의한다. 2년 이내 개발환경 보안점검을 수행한 이력이 있는 경우 다음을 고려한다.

- 1) 동일 업체이나 제품이 다른 경우
- 2) TOE의 평가보증등급이 변경된 경우
- 3) 형상관리체계 및 배포절차 변경
- 4) 개발환경 이전

- 평가자는 제출물 설명회 자료에 개발환경 보안점검 생략근거(증빙)를 포함하도록 신청기관에 안내해야 하며, 신청기관은 제출물 설명회에서 인증기관과 평가기관에 개발환경보안점검 생략 근거에 대해서 증빙해야 한다.
- 국내용 인증의 경우 개발환경 보안점검 수행 시 개발환경 보안점검 계획서 작성은 생략 가능하다.
- 전체 점검항목에 대해서 생략하는 경우, 해당 사유를 회의록에 작성하고 개발환경 보안점검 보고서 작성은 생략 가능하나, 전체 점검항목이 생략 가능한지는 충분히 검토 및 증빙되어야 한다.

101 평가보증등급에 관계없이 개발환경 보안점검 시 소스코드 형상관리 체계 및 소스코드 접근통제 방법을 확인해야 한다.

102 평가보증등급을 추가하는 경우(예: EAL2+, EAL3+, EAL4+), 추가된 보증요구사항에 대한 개발환경 보안점검 필요성 확인 후 '[붙임1] 국내용 개발환경 보안점검 목록'에서 해당 보증컴포넌트에 대한 항목을 추가하여 점검한다.

2.6.2. 국제용 인증

103 국제용 인증 시 개발환경 보안점검은 CC/CEM 요구사항에 따라 수행하며, EAL2, EAL3, EAL4 개발환경 보안점검 목록은 '[붙임2] 국제용 개발환경 보안점검 목록'을 참조한다.

104 평가보증등급을 추가하는 경우(예: EAL2+, EAL3+, EAL4+), 추가된 보증요구사항에 대한 개발환경 보안점검 필요성 확인 후 '[붙임2] 국제용 개발환경 보안점검 목록'에서 해당 보증컴포넌트에 대한 항목을 추가하여 점검한다.

105 EAL5 이상으로 평가신청한 경우 평가기관은 EAL4 대비 추가된 보증요구사항에 대한 개발환경 보안점검 필요성 확인한 후 인증기관과 협의하여 점검 항목을 추가할 수 있다.

2.7 스마트카드 및 유사제품 평가

적용 범위	☑ 국제용 인증	□ 국내용 인증

106 CCRA는 CC 인증 시 특정 기술 분야에 적용하기 위한 보조문서를 사용하며, 보조문서를 '강제적용 기술문서(mandatory)'와 '참고문서(guidance)'로 구분하고 있다.

107 스마트카드 및 유사제품 평가에 적용되는 보조문서는 CCRA 홈페이지(www.commoncriteriaportal.org)에 공개되어 있으며, 이 중 '강제적용 기술문서(mandatory)'는 평가 시 반드시 적용되어야 한다.

108 신청기관은 CC에서 EAL별로 정한 평가제출물 외에 스마트카드 및 유사제품 평가에 적용되는 보조문서에 따라 추가적인 평가제출물을 평가기관에 제공할 것이 요구되며, 따라서 평가기관은 이에 상응하는 추가적인 평가결과물을 인증기관에 제출해야 한다.

109 스마트카드 및 유사제품 평가에 적용되는 보조문서는 CCRA에서 승인한 최신 문서를 준용한다.

2.8 TOE 범위에 가상화 기술을 포함하는 제품 평가[21]

적용 범위	☑ 국제용 인증	☑ 국내용 인증

2.8.1 국제용 인증

110 2.1절에서 정의한 TOE 범위산정 및 식별자 부여방법에 따라 국제용 인증 시 TOE의 물리적 범위에 가상화 기술이 포함되어야 하는지 확인하고, TOE의 물리적 범위에 포함되는 경우 SFR과의 관련성을 분석하여 가상화 기술을 제공하는 TOE 구성요소를 TSF 또는 non-TSF로 분류해야 한다.

111 TOE 범위에 가상화 기술을 포함하고자 하는 경우 신청기관은 평가신청한 EAL에 따라 신청기관이 보증해야 하는 평가제출물을 작성하여 제출, 수정, 보완할 수 있어야 하고 정당한 법적 권한을 가지고 있어야 한다.

112 가상화 기술을 포함하고 있는 TOE를 평가하고자 하는 평가기관은 TOE 평가에 필요한 인력, 기술력 등의 전문성을 확보하고 인증기관에 이를 입증해야 한다.

113 국제용 평가·인증은 CCRA 협정에 따라 CC/CEM을 준수한다.

21) 클라우드 서비스와 같은 가상화 기술을 활용하는 서비스를 대상으로 하지 않으며 정보보호제품을 대상으로 함에 유의한다.

2.8.2 좀비PC 대응 기능을 가진 기타 제품유형의 국내용 인증[22)]

114 TOE 범위에 가상화 기술을 포함하고자 하는 경우 신청기관은 평가신청한 EAL에 따라 신청기관이 보증해야 하는 평가제출물을 작성하여 제출, 수정, 보완할 수 있어야 하고 정당한 법적 권한을 가지고 있어야 한다.

115 좀비PC 대응 기능을 가진 제품의 경우 수집된 파일을 대상으로 동적 분석 또는 행위기반 분석을 수행하기 위해 하드웨어 일체형 장비에 하이퍼바이저를 포함하여 배포하는 제품이 존재할 수 있다.

116 이 경우 2.1절에서 정의한 TOE 범위산정 및 식별자 부여방법에 따라, 국내용 인증 시 TOE는 제품과 동일해야 하므로 하드웨어 일체형 장비 전체를 TOE 물리적 범위로 산정해야 하며 하이퍼바이저는 TOE 범위에 포함되어야 한다. 또한, SFR과의 관련성을 분석하여 하이퍼바이저를 TSF 또는 non-TSF로 분류해야 한다.

117 하드웨어 일체형 장비로 구현된 좀비PC 대응 기능을 가진 기타 제품에 하이퍼바이저가 포함되는 경우 하이퍼바이저 관련 취약점을 통한 권한 상승, 서비스 거부 등의 취약성이 존재할 수 있다.

118 이와 같은 제품의 평가 착수 전에 다음을 확인해야 한다.

- 평가 착수 전 신청기관이 신청한 EAL을 확인하여 평가 가능 여부를 확인해야 한다. 즉, 국내용 인증 시 EAL별로 신청기관이 보증해야 하는 평가제출물을 작성하여 제출, 수정, 보완할 수 있어야 하고 정당한 법적 권한을 가지고 있어야 한다.
- 인증자 지정 요청 시 평가기관은 평가대상 제품에 대해 인력(예: 동일 또는 유사 제품유형 평가 이력) 및 교육(예: 평가 범위에 포함된 가상화 기술에 대한 교육), 시험기술(예: 평가 범위에 포함된 가상화 기술 관련 기능시험 및 침투시험 방아 등) 등의 전문성을 확보하였음을 객관적인 증빙자료를 통해 입증하여야 한다.
- 하드웨어 일체형 장비에 탑재된 TOE 구성요소 중 가상화 기술 없이 동작 가능한 TOE 구성요소는 하이퍼바이저 상에서 동작하지 않는다고 가정한다.
- 좀비PC 대응 기능을 가진 기타 제품유형에서 가상화 기술은 행위기반 분석 시 샌드박스(sandbox)[23)]로서 역할을 수행함을 명확히 해야 한다.

119 이와 같은 제품의 평가 시에 다음을 확인해야 한다.

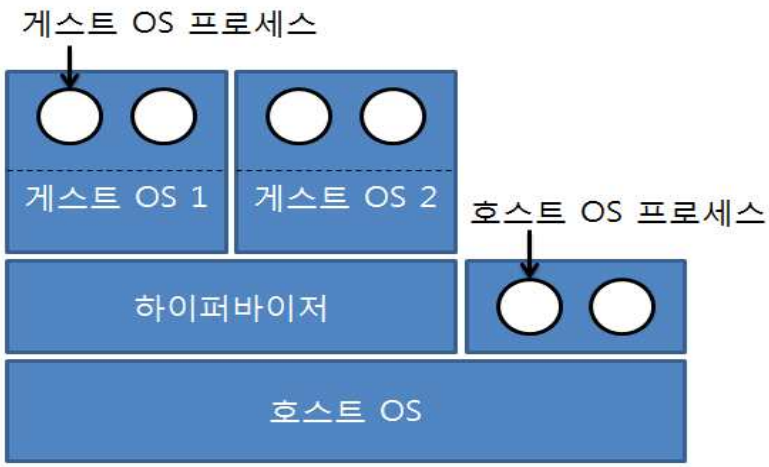
22) 국내용 인증 시 좀비PC 대응기능이 주요 기능인 기타 제품유형에 한해서 인증사례가 존재하며, 그 외 제품유형에는 해당하지 않음에 유의한다.

23) 샌드박스: 신뢰되지 않은 코드의 실행을 위한 제한된 환경

<보안목표명세서>

120 TOE 구성요소에 가상화 기술을 구현하는 모든 구성요소(예: 가상머신 모니터(VMM), 게스트 머신(또는 게스트 OS[24])) 등)가 포함되어야 하며, 평가자는 해당 가상화 기술을 구현하는 구성요소가 TOE 물리적 범위에 모두 식별 되었는지 확인하고 이름, 버전, 사용 목적(제공하는 기능) 등이 서술되었는지 확인한다.

121 게스트 OS 내에 설치되는 제3자 제공 소스코드/라이브러리를 식별하고 사용 목적이 정확하게 서술되었는지 확인한다.



(그림 2.8-1) hosted 타입 하이퍼바이저 아키텍쳐 예시

<형상관리>

122 게스트 OS 등 행위기반 분석을 수행하는 소프트웨어(즉, 가상화 기술을 구현한 요소)에 대한 형상관리 식별 체계가 서술되었는지 확인한다. 행위기반 분석을 위해 게스트 OS에 설치되는 신청기관에서 개발한 소프트웨어가 존재할 경우, 이에 대한 형상관리 식별 체계를 서술해야 한다.

<설계서>

123 TOE 설계서 또는 개발 업체의 자체 개발문서에 EAL에 따라 가상화 기술을 구현하는 요소가 포함된 TOE의 구조를 모듈 또는 서브시스템 측면으로 서술했는지 확인한다.

<취약성 분석서>

124 개발자 취약성 분석서에 가상화 기술을 구현하는 요소 및 게스트 OS를 고려하여 보안구조설명에 포함되어야 하는 보안특성과 시험내용이 서술되었는지 확인한다(예: 스냅샷을 이용한 게스트 OS 초기화 부팅, 3분 동안 신호가 없는 경우 게스트 OS 강제 종료, 외부망 통신 차단 등).

24) 게스트 OS가 TOE에 포함되어 배포되는 경우 물리적 구성요소로 식별되어야 한다.

<침투시험>

125 평가자는 하이퍼바이저 등 TOE에 탑재된 가상화 기술을 구현하는 요소에 의해 취약성이 발생하지 않음을 침투시험을 통해 보증하고 침투시험서에 기록한다.

- 평가제출물 및 공개영역 조사를 통해 하이퍼바이저 등 TOE에 탑재된 가상화 기술 또는 가상화 제품 관련 취약성을 조사하고 추가적인 침투시험 항목을 도출한다(예: 서비스 거부, 게스트 OS 메모리 손상, 호스트 OS 커널 제어, 권한상승, 가상머신 회피 악성코드 탐지 우회, 게스트 OS 네트워크 침해, 비인가 명령 전송 취약성 등).

126 가상화 기술(예 : 하이퍼바이저)을 커스트마이징 하는 경우 변경된 부분(예 : 디바이스 드라이버 등)으로 인해 발생할 수 있는 잠재적인 취약성을 고려해야 한다(예: 게스트 OS 침해, 게스트 OS로부터의 호스트 OS 침해, 하이퍼바이저 침해 등).

2.9 웹방화벽 평가 시 주의사항

적용 범위	☐ 국제용 인증[25]	☑ 국내용 인증

2.9.1 웹방화벽 보안기능 및 기본 정책설정 점검사항

127 웹방화벽은 잘 알려진 취약성에 대응할 수 있도록 보안기능이 구현되어 있어야 하며 기본 정책이 설정되어 있어야 한다. 다음은 웹방화벽에서 대응해야 하는 잘 알려진 취약성에 대한 평가 지침을 제공한다. 신청기관 및 평가자는 평가 시 TOE가 다음 취약성에 대응함을 입증해야 한다(본 절에서 설명하는 취약성은 평가 중에 분석해야 하는 웹방화벽 관련 취약성 중 일부임에 주의한다).

<IIS Short File/Folder Name Disclosure(IIS 웹서버 정보노출) 취약점>

o "IIS Short File/Folder Name Disclosure" 취약점 및 도구가 통해 공개됨('12. 7. 3)

※ 취약점 정보 출처 : http://www.exploit-db.com/exploits/19525
※ 도구 다운로드 : http://code.google.com/p/iis-shortname-scanner-poc/

o 공격자가 IIS 웹 서버의 요청을 틸드문자(~) 및 와일드카드 문자(* or ?)를 이용하여 웹 서버 내 파일 정보를 수집가능

※ MS 운영체제에서 틸드 기호(~)를 사용하여 11자 이상의 파일명에 대한 정보검색 가능
(예, "validlong.ext" 파일 검색시, "VALIDL~1.EXT" 파일명으로 검색 가능)
※ 단, 파일명이 8자 이상이 되어야 파일정보 수집이 가능함

o 공격 시나리오

25) 국제용 인증 시 준수하는 보호프로파일, 취약성 분석 등에 따라 요구사항이 존재할 수 있으므로 신청기관 및 평가기관은 본 문서가 아닌 평가신청한 TOE가 준수해야 하는 요구사항을 확인해야 한다.

① 취약한 웹서버 사이트 탐색

② 틸드문자가 포함된 URI를 사이트 주소창에 입력하여 결과를 확인

③ ②의 동작을 반복하여, 파일 이름을 추론

- 공격 예("http://sdl.me/AcSecret.html" 파일이름 추정가능)

구분	공격 URI	공격 결과	추론 내용
1	http://sdl.me/*~1*/.aspx	404 에러	웹서버 내 8.3 파일 이름 지정 체계를 가진 파일 또는 디렉터리가 존재함
2	http://sdl.me/a*~1*/.aspx	404 에러	대상의 첫 번째 글자는 'A'로 시작
3	http://sdl.me/aa*~1*/.aspx	400 에러	대상의 두 번째 글자는 'A'가 아님
4	http://sdl.me/ab*~1*/.aspx	400 에러	대상의 두 번째 글자는 'B'가 아님
5	http://sdl.me/ac*~1*/.aspx	404 에러	대상의 두 번째 글자는 'C'
6	http://sdl.me/ac%3f~1*/.aspx	400 에러	대상은 3글자 이상
7	http://sdl.me/ac%3f%3f%3f%3f~1*/.aspx	404 에러	대상은 6글자 이상
8	http://sdl.me/acsecr~1*/.aspx	404 에러	대상은 "ACSECR"로 시작
9	http://sdl.me/acsecr~1/.aspx	400 에러	대상은 디렉터리가 아니며 확장명을 가짐
10	http://sdl.me/acsecr~1.%3f/.aspx	400 에러	확장명은 1글자 이상
11	http://sdl.me/acsecr~1.%3f%3f%3f/.aspx	404 에러	확장명은 3글자 이상
12	http://sdl.me/acsecr~1.a%3f%3f/.aspx	400 에러	확장명은 'A'로 시작하지 않음
13	http://sdl.me/acsecr~1.h%3f%3f/.aspx	404 에러	확장명은 'H'로 시작함
14	http://sdl.me/acsecr~1.htm/.aspx	404 에러	확장명은 "HTM"으로 시작함

※ 404 에러 : 파일을 찾을 수 없을 때 나타나는 에러메세지
※ 400 에러 : 서버가 요청을 처리할 수 없을 때 나타나는 에러메세지

o 웹방화벽 제품 확인사항

① 해당 취약점에 대응하기 위한 보안기능을 제공해야 함

※ 웹방화벽 제품의 'Error Handling' 등과 같은 보안정책을 활용하여 해당 취약점에 대한 탐지 및 차단기능 수행이 가능함
※ Error Handling : 공격자가 웹서버가 출력하는 에러메시지를 통해 웹서버의 정보를 수집하지 못하도록 차단하는 정책(예, 웹서버에서 반환되는 400, 404 등의 에러메시지 차단)

② 해당 취약점에 대응하기 위한 **보안정책은 기본적으로 제공**하도록 설정되어 있어야 함

※ 예, 웹방화벽 제품이 'Error Handling' 보안정책을 활용하여 해당 취약점을 탐지 및 차단하는 경우, 400, 404 에러메시지를 제어하는 정책이 디폴트로 설정되어 있어야 함

o 평가제출물

- 설명서, 시험서 등 보증문서에 "IIS Short File/Folder Name Disclosure" 등과 같은 웹서버 정보노출 취약점에 대응하는 보안기능에 대한 설명 또는 시험내용을 서술

o 평가 시

- 평가자는 독립시험 및 침투시험 수행 과정에서 "IIS Short File/Folder Name Disclosure" 취약점에 대응 하는 웹방화벽 제품의 보안기능 및 보안정책 설정이 정상적으로 동작하는지 확인하며, 시험결과를 독립시험서 및 침투시험서 등과 같은 평가단위보고서에 명시하도록 함

<Big-HTTP Request 공격 등 3가지 웹방화벽 우회 취약점>

o 2013년 8월 발견된 웹방화벽 공격기법 3가지(Big-HTTP Request, 변형된 SQL 주석문 이용, Method Confusion)에 의해 웹방화벽을 우회할 수 있음

o 웹방화벽 우회 공격기법 개요

가. Big-HTTP Request 공격기법

HTTP 패킷의 데이터 크기가 4,096Bytes 이상일 경우 웹방화벽의 성능상 이유로 Bypass 시켜 웹방화벽을 우회하는 공격기법

나. 변형된 SQL 주석문을 이용한 공격기법

SQL에 사용되는 일반적인 주석문(/* */)을 사용하는 SQL Injection 공격에 대해서는 탐지 및 대응을 수행하나, 변형된 SQL 주석문(/* **/, /** **/, /** */)에 대해서는 탐지 및 대응을 수행하지 못하는 취약성을 이용한 공격기법

다. GET과 POST Method의 혼동을 이용하는 Method Confusion 공격기법

HTTP의 Method가 GET일 경우 Request Data 부분은 탐지에서 제외하는 경우가 존재하여, POST 데이터의 Method만 GET으로 전환하여 공격을 수행

o 공격 시나리오

가. Big-HTTP Request 공격기법

① 취약한 웹서버 사이트(로그인 페이지) 탐색
② 공격자(클라이언트)에서 공격코드가 포함된 4,096byte이상의 HTTP 데이터를 HTTP 프록시를 이용하여 웹서버의 로그인 페이지로 전송하여 공격

나. 변형된 SQL 주석문을 이용한 공격기법

① 취약한 웹서버 사이트(로그인 페이지) 탐색
② 공격자(클라이언트)에 설치된 Paros에서 Trap request 체크 후, 접속한 웹서버 로그인 페이지에 임의의 ID/PW를 입력(예) ID:test, PW:1111)
③ 수집된 Paros의 패킷에서 ID/PW 사이에 변형된 주석문을 이용한 공격코드 삽입(예) ID=test'/*1 or 1=1**/&PW=1111)

※ 변형된 주석문은 3가지 방식(/* **/, /** **/, /** */) 모두 수행

다. GET과 POST Method의 혼동을 이용하는 Method Confusion 공격기법

① 취약한 웹서버 사이트(로그인 페이지) 탐색

② 공격자(클라이언트)에 설치된 Paros에서 Trap request 체크 후, 접속한 웹서버 로그인 페이지에 임의의 ID/PW를 입력(예) ID:test, PW:1111)

③ 수집된 Paros의 패킷에서 request 패킷 헤더에 POST를 GET으로 변경하고 데이터 부분에 ID=test'1 or 1=1'--'&passwd=1111 등과 같은 공격 패킷 전송

o 웹방화벽 제품 확인사항

① 해당 취약점에 대응하기 위한 **보안기능을 제공**해야 함

가. Big-HTTP Request 공격기법

※ 공격 탐지 기능 : 웹방화벽에서 Big-HTTP Request 공격에 대한 탐지가 이루어지는지 확인

※ 공격 차단 기능 : 웹방화벽에서 Big-HTTP Request 공격 탐지 후 공격 IP 차단이 이루어지는지 확인

나. 변형된 SQL 주석문을 이용한 공격기법

※ 공격 탐지 기능 : 웹방화벽에서 변형된 SQL 주석문 이용 공격에 대한 탐지가 이루어지는지 확인

※ 공격 차단 기능 : 웹방화벽에서 변형된 SQL 주석문 이용 공격 탐지 후 공격 IP 차단이 이루어지는지 확인

다. GET과 POST Method의 혼동을 이용하는 Method Confusion 공격기법

※ 공격 탐지 기능 : 웹방화벽에서 Method Confusion 이용 공격에 대한 탐지가 이루어지는지 확인

※ 공격 차단 기능 : 웹방화벽에서 Method Confusion 이용 공격 탐지 후 공격 IP 차단이 이루어지는지 확인

② 해당 취약점에 대응하기 위한 **보안정책은 기본적으로 제공**하도록 설정되어 있어야 함

o 평가제출물

- 설명서, 시험서 등 보증문서에 웹방화벽 우회 취약점 3가지 (Big-HTTP Request 공격, 변형된 SQL 주석문을 이용한 공격, GET과 POST Method의 혼동을 이용하는 Method Confusion 공격)에 대응하는 보안기능에 대한 설명 또는 시험 내용을 서술

o 평가 시

- 평가자는 독립시험 및 침투시험 수행 과정에서 웹방화벽 우회 취약점 3가지 (Big-HTTP Request 공격, 변형된 SQL 주석문을 이용한 공격, GET과 POST Method의 혼동을 이용하는 Method Confusion 공격)에 대응하는 웹방화벽 제품의 보안기능 및 보안정책 설정이 정상적으로 동작하는지 확인하며, 시험결과를 독립시험서 및 침투시험서 등과 같은 평가단위보고서에 명시하도록 함

2.9.2 소프트웨어 형태의 웹방화벽 평가 시 유의사항

128 웹방화벽은 하드웨어 일체형 장비 또는 소프트웨어 형태로 구현될 수 있다. 국내용 인증 시 웹방화벽은 대체로 하드웨어 일체형 장비 형태로 인증되었으나, 최근 소프트웨어 형태의 웹방화벽에 대한 국내용 인증이 이루어지고 있다. 소프트웨어 형태로 구현된 웹방화벽 평가 시 다음에 유의해야 한다.

- 제품의 운영환경 및 보안기능요구사항은 국가용 정보보호제품 보안요구사항을 만족해야 한다.
  - 제품이 유일한 연결점이 되는 네트워크 구성을 만족하고 인터넷에 연결된 웹존 바로 앞에 위치해야 하며, 보호대상이 되는 웹서버 자체에 함께 설치되는 소프트웨어 웹방화벽은 허용하지 않는다.
- 온라인 업데이트 기능을 제공하는 경우 2.4절을 준수한다.
- TOE 운영환경 서술 방식은 2.2절을 준수한다.
  - 소프트웨어인 TOE 운영에 필요한 OS 및 H/W 등의 사양만을 서술한다. 예를 들어, 아래 그림과 같이 TOE 운영환경이 가상 영역 내에 존재하는 경우라도 TOE에 직접적으로 필요한 운영환경은 가상 영역이 아니므로 가상화 솔루션(예: Citirix, XEN, VMware 등)을 운영환경으로 식별하지 않는다.

(그림 2.9-1)

  - 평가자는 위 그림과 같은 운영환경에서 인증된 소프트웨어 웹방화벽이 가상화 기반 운영환경에서 인증서를 획득한 것으로 인증내용이 오남용되지 않도록 신청기관에 안내해야 한다.
- 웹방화벽 제품유형은 원칙적으로 Bypass 지원 NIC을 사용할 수 없으므로(2.11절 참조), 소프트웨어 형태의 웹방화벽 평가 시 평가자는 다음에 주의한다.
  - TOE 운영환경에서 NIC 표기 시 Bypass 지원 NIC은 사용할 수

없다.

- ST에 TOE 운영환경으로 NIC 표기 시 Bypass 지원 NIC은 사용할 수 없음을 명시해야 하고, 평가자는 '독립시험서'에 Bypass 기능을 제공하지 않는 NIC을 TOE 시험환경으로 명시하여 시험해야 한다.
- 평가자는 설명서에 TOE 운영환경 구성 시 Bypass NIC를 사용할 수 없음에 대한 적절한 주의사항이 포함되어 있는지 평가한다.

- TOE 범위산정 및 식별자 부여방법은 2.1절을 준수한다.
- 개발환경 보안점검 목록은 2.6절을 준수한다.
- 원격접속 기능을 제한하는 것과 관련된 지침은 2.13절을 준수한다.
- TOE는 소프트웨어이므로 이에 적합한 배포 방식(예: CD에 포함하여 배포, 소프트웨어 온라인 다운로드 등)만을 허용한다.
  - 개발환경 보안점검 시 배포 방식이 소프트웨어 TOE에 적합한지 확인한다.

2.10 SNMP 프로토콜 사용원칙

적용 범위	□ 국제용 인증	☑ 국내용 인증

129 TOE가 SNMP 프로토콜을 사용하는 경우 아래 사용 원칙을 준수해야 하여 평가자는 아래 사용 원칙이 준수되는지 확인해야 한다.

① SNMP V3 사용 원칙

- 평가자 유의사항
  - SNMP를 사용하는 경우, 보안목표명세서 운영환경에 사용되는 SNMP 버전 정확히 명시하는지 확인한다.
  - SNMP V3 표준에서 제시하는 최상위 암호비도를 갖는 암호알고리즘을 사용하는지 확인한다.
- SNMP V3 보안 방법
  - 사전공격 대응(사용자 이름, 인증용 패스워드, 암호용 패스워드)
  - 디폴트 '사용자이름' 및 '패스워드(인증용 패스워드, 암호용 패스워드)' 사용 금지

- 뷰 기반 접근통제 수행 시 뷰 모드 제한(write-view 및 notify-view 사용 금지, read-view 권한만 제공)[참조: RFC 3415]
- 디폴트 패스워드 하드코딩 금지
- MIB 데이터 내 기밀정보 사용 삭제(예, SMTPLoginPassword)
- 뷰 기반 접근통제 수행 시 보안레벨 제한(noAuthNoPriv 및 authNoPriv 사용 금지, authPriv 레벨만 제공)

② SNMP V1, V2 사용 원칙

- 평가자 유의사항
  - SNMP V1, V2가 반드시 필요한 경우만 허용(불필요시, 포트 차단)
  - SNMP V1, V2를 사용하는 경우, 보안목표명세서 운영환경에 SNMP 프로토콜 버전을 명시해야 하며, 관리자 설명서에 SNMP의 안전한 사용에 대해 기술해야 함
- SNMP V1, V2 보안 방법
  - 쓰기(write) 방지(read 권한만 제공)
  - 사전공격 대응(커뮤니티 스트링)
  - 디폴트 및 공개된 커뮤니티 이름 사용 금지(예, public, admin 등)
  - 디폴트 패스워드 사용 및 평문저장 금지
  - MIB 데이터 내 기밀정보 사용 삭제(예, SMTPLoginPassword)

130 SNMP 프로토콜이 평가범위에 포함된 경우, 평가제출물은 다음을 준수해야 한다.

- 보안목표명세서에 SNMP 프로토콜과 관련된 사항(운영환경 명시, 프로토콜 버전, 사용 목적 등)을 명시한다.
- 설명서에 SNMP 프로토콜에 대한 안전한 사용 방법에 대해 명시한다(SNMP V1, V2, V3 보안방법(상기 ①, ② 참조) 준수).
- 개발자 시험서/취약성 분석서에 "SNMP V1, V2, V3 보안방법(상기 ①, ② 참조)" 및 기능/취약점 시험을 통한 SNMP 안전한 사용을 보증해야 한다.
- 제품의 디폴트 정책은 "SNMP V1, V2, V3 보안방법" 준수해야 한다.

131 SNMP 프로토콜이 평가범위에 포함되지 않는 경우, 평가제출물은 다음을 준수해야 한다.

- 취약성 분석서에 제품운영을 위해 필요한 서비스(포트)를 식별하여, SNMP 프로토콜 등이 제품운영을 위해 필요하지 않음을 보증해야 한다.

132 SNMP 프로토콜이 평가범위에 포함된 경우, 평가자는 다음을 준수해야 한다.

- 평가자는 보안목표명세서와 설명서 등에서 SNMP 프로토콜과 관련된 사항(운영환경 명시, 프로토콜 버전, 사용 원칙 등)이 정확히 서술되어 있는지 확인해야 한다.
- 침투시험 수행 과정에서 SNMP 프로토콜 사용 원칙하에 SNMP 프로토콜이 정상적으로 동작하는지 확인하여, 확인 결과를 침투시험서에 명시해야 한다.
- 평가자는 제품운영을 위해 허용된 서비스(포트)를 침투시험서 및 평가결과보고서에 명시해야 한다.
- 평가자는 평가결과보고서의 권고사항에 SNMP 프로토콜 사용에 대한 안전한 사용을 권고해야 한다.

133 SNMP 프로토콜이 평가범위에 포함되지 않는 경우, 평가자는 다음을 준수해야 한다.

- 평가자는 SNMP 프로토콜이 제품 운영을 위해 필요하지 않은 경우 해당 사실을 평가결과보고서의 권고사항으로 기술해야 한다.
- 또한, 제품운영을 위해 허용된 서비스(포트)에 대해서는 침투시험서 및 평가결과보고서에 명시해야 한다.

평가결과보고서 권고사항 작성 (예)
제품 운영을 위해 필요하지 않은 서비스(포트)는 제거하거나 활성화하지 않음을 권고한다(예: SNMP 프로토콜 사용 금지)

2.11 NIC 우회불가성

적용 범위	□ 국제용 인증	☑ 국내용 인증

134 침입방지시스템, 침입차단시스템, 웹방화벽 기능이 포함된 네트워크 정보보호제품군의 하드웨어 장애(예: 전원 off 등) 발생 시 제품에 장착된 Bypass 보안기능 NIC(이하 'Bypass NIC[26]')의 Fail-over(장애 극복) 기능이 활성화되면, 인가

26) Bypass NIC : 주로 네트워크 정보보호제품군에 장착되어 장비의 하드웨어 장애(전원 off 등) 발생 시, Bypass NIC이 네트워크 케이블화 되어(단순 네트워크 케이블 기능) 자동으로 패킷을 통과시킴으로써 네트워크의 가용성을 높여주는 Fail-over(장애

되지 않은 네트워크 패킷이 차단되지 않고, Bypass NIC를 통해 내부망 또는 주요 서버로 통과되는 우회 취약점이 발생할 수 있다.

135 위와 같이 Bypass NIC가 장착된 네트워크 정보보호제품군은 국가용 보안요구사항에 의해 펌웨어 또는 하드웨어 방식(예: BIOS에서 조작 등)으로 Fail-over 기능을 사용불가능하게 해야 한다. 응용 소프트웨어 계층(사용자 인터페이스) 및 운영체제 계층(커널의 장치 드라이버)에서 소프트웨어 방식으로 Fail-over 기능을 사용불가능하게 구현하는 것은 허용하지 않는다.

136 평가자는 AVA_VAN(취약성 분석) 평가 시 Bypass NIC가 장착된 네트워크 정보보호제품군에 대한 평가제출물 평가결과를 기록한다(침투시험서, 평가결과보고서).

137 평가자는 네트워크 정보보호제품군의 하드웨어 사양 변경(Bypass NIC 추가/변경)에 따른 인증효력유지(변경승인) 시험 시 평가제출물 평가결과를 기록한다(인증효력유지 평가결과보고서).

2.12 다수의 네트워크 보안기능을 제공하는 제품 평가 방안

적용 범위	□ 국제용 인증	☑ 국내용 인증

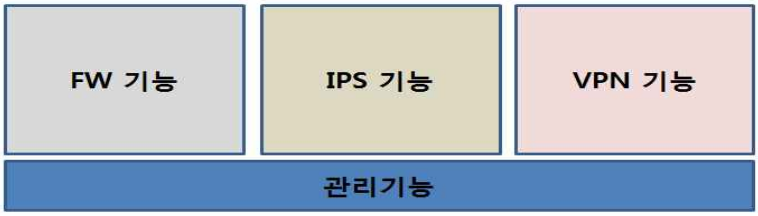
138 일부 네트워크 제품들의 제품 유형이 실제 기능과 일치하지 않거나 동일한 기능을 제공하는 제품들의 유형을 다르게 정의하는 등 국내용 인증 시 현안이 발생하여 다수의 네트워크 보안기능을 제공하는 제품들에 대한 제품 유형을 명확하게 정의하고 보안요구사항 수용 기준을 제공할 필요가 있다.

139 다수의 네트워크 보안기능을 제공하는 제품은 각각의 유형을 모두 더한 형태로 정의할 수 있다. 예를 들어, 침입차단 기능과 가상사설망 기능을 포함한 제품은 'FW+VPN'으로 정의할 수 있다.

140 다수의 네트워크 보안기능을 제공하는 제품의 경우 아래의 조건을 만족하는 경우 다수의 보안요구사항을 수용하는 것으로 허용할 수 있다.

- ① 각각의 보안기능이 독립적으로 구현된 경우
  - IPS, FW, VPN 기능을 포함한 경우 IPS 기능, FW 기능, VPN 기능은 독립적으로 구현되고 운영되어야 한다. 즉, 독립적인 구현이란 아래의 그림에서 FW 기능이 중단되더라도 IPS 기능과 VPN 기능은 정상적으로 동작되어야 함을 의미한다. 단, 관리기능은 하나로 통합되어야 한다.

극복) 기능을 제공하는 NIC을 의미한다.



(그림 2.12-1)

- 위의 그림에서 FW 기능이 중단될 경우 IPS 기능이 정상적으로 동작하지 않는다면 FW 기능과 IPS 기능은 독립적으로 구현되었다고 볼 수 없다.
- 독립적인 형태의 구현이 아닌 종속적인 형태의 구현일 경우, 각각의 모듈을 하나의 단일 제품으로 인정할 수 없기 때문에 복수 수용은 허용할 수 없으며, 가장 적합한 보안요구사항 하나를 선택하여 수용해야 한다.

• ② 구현의 증빙

- 평가준비단계에서 ①항의 내용을 확인하고 이를 증명할 수 있는 증빙자료를 인증기관에 제출한다.
- 증빙자료를 통해 제품의 아키텍처 수준에서 독립적인 구현 여부를 확인할 수 있어야 한다.

• ③ 다수의 보안요구사항 수용의 경우 보안요구사항 간 상충여부 확인

141 UTM에 대한 정의가 명확하지 않고, UTM이 가져야 하는 기본 기능을 정의하기 어려우므로 UTM 제품유형은 별도로 정의하지 않는다. 신청기관은 TOE가 다수의 네트워크 보안기능을 제공하는 경우 이를 직관적으로 인지할 수 있도록 TOE 명칭에서 UTM이란 용어를 사용할 수 있다.

142 하나의 TOE가 다수의 보안요구사항을 수용한 경우 평가기간 산정 시 다음을 고려해야 한다.

• ① SFR 개수 등 제품의 복잡도를 고려하여 평가기간 산정에 반영

• ② 준수한 보안요구사항 및 추가 기능을 모두 SFR로 도출하고 평가기간 산정에 반영

• ③ 다수의 보안기능을 동시에 제공하는 제품의 경우 평가자는 각각 독립된 제품유형에 대한 독립/침투시험 이외에 다수의 제품이 상호 연동하는 시스템 측면에서의 독립/침투시험을 고려하여야 함

2.13 원격접속 기능을 포함한 정보보호제품 평가 시 제약사항

적용 범위	□ 국제용 인증	☑ 국내용 인증

143 평가대상 정보보호제품은 클라이언트/에이전트, 관리서버 등 여러 구성요소를 포함할 수 있으며, 이와 같은 구성요소에 대한 접속은 다음 두 가지로 구분하여 정의한다.

- 관리접속[27]: 내부망에서 내부망으로 접속하는 경우
- 원격접속: 외부망에서 내부망으로 접속하는 경우

144 국가용 보안요구사항에 의해 내부망에 설치된 관리서버/클라이언트/에이전트에 외부망의 PC로부터 접속할 수 있는 '원격접속' 경로가 존재하는 경우 이는 원칙적으로 불허한다.[28]

145 동일한 내부망의 관리서버와 클라이언트/에이전트 PC간의 통신은 '원격접속'으로 정의하기 어려우며 '관리접속'으로 해석한다.

146 정보보호제품에서 '관리접속' 기능을 구현한 경우 목적을 명확히 서술하고, '관리접속' 기능에 의해 취약성이 발생하지 않음을 평가 시 입증하는 경우 포함할 수 있다.

147 평가제출물은 다음을 포함해야 한다.

- TOE가 '서버-클라이언트(에이전트 또는 PC 등)'간에 '관리접속' 기능을 포함하는 경우 동일 내부망에서 접속하는지 운영환경을 확인한다.
- ST에서 '관리접속' 기능을 TOE가 제공해야 하는 목적을 명확히 서술하고, 이에 대한 SFR로 식별한다.
- '관리접속' 기능을 정의한 SFR과 관리접속에 대한 권한의 범위와 권한을 제한하는 메커니즘 등의 관련된 내용을 설명서, 설계서, 시험서 등 평가보증등급에 따른 평가제출물에 서술한다.
- 취약성 분석서에 '관리접속'과 관련된 침투시험을 수행하여 기록한다.
- TOE가 제공하는 '관리접속' 기능이 외부망에서 내부망 서버로 접근하는데 악용될 수 없음을 입증한다(예: IP기반 접근 통제).

148 평가자는 평가제출물에 대해 평가 시 다음을 수행한다.

---

27) 국가용 보안요구사항 V3.0에서는 '관리접속'을 '원격관리'로 정의하고 있으며, 이는 본 문서의 2.13절에서 정의하는 '원격접속'과는 다름에 유의한다.

28) 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조 1항 3호 '다'에 의거, 「전자정부법」 2조 10호에 따른 정보통신망 또는 같은 조 13호에 따른 정보시스템의 구축 및 유지·보수 등 해당 계약의 이행과정에서 정보시스템 등에 허가 없이 접속하거나 무단으로 정보를 수집할 수 있는 비인가 프로그램을 설치하거나 그러한 행위에 악용될 수 있는 정보시스템 등의 약점을 고의로 생성 또는 방치하는 경우 부정당업자로 인정되어 입찰 참가자격이 제한되며, 상세한 내용은 해당 법령을 참고한다.

- 평가자는 평가제출물과 관련된 평가결과를 기록한다(독립시험서, 침투시험서, 평가결과보고서).
- 평가자는 해당 기능에 의해 취약성이 발생하지 않음을 침투시험을 통해 보증하고 평가결과를 기록한다(침투시험서).
- 위에서 정의한 원칙이 적용될 수 없다고 판단되는 정보보호제품군을 평가하는 경우 또는 신규 정보보호제품군을 발견하는 경우 인증기관과 사전 협의한다.

2.14 TOE 자체보호 기능

적용 범위	□ 국제용 인증[29]	☑ 국내용 인증

149 본 절은 국가용 보안요구사항 V1.0/V1.1을 준수하는 경우 추가적인 해석을 제공하기 위한 것이다. 국가용 보안요구사항 V3.0을 준수하는 경우 2편 '서버 공통보안요구사항'의 '4. 자체보호', '엔드포인트 공통보안요구사항'의 '4. 자체보호', 각 제품 보안요구사항을 적용해야 한다.

150 국가용 정보보호제품 보안요구사항에는 자체시험 요구사항이 명시되어 있으며, Windows 운영체제에 설치되는 에이전트가 포함되는 경우 추가적으로 에이전트 보호를 위한 보안요구사항이 존재한다. Windows 운영체제에 설치되는 에이전트 보호 요구사항은 제품유형에 따라 세 가지로 구분된다.

- 자체시험 요구사항

보안기능을 구성하는 메커니즘의 무결성과 보안관리에 대한 안전성을 보장하기 위해 다음의 요구사항을 만족해야 한다. o 제품의 정확한 운영을 보장하기 위해 시동시 및 정규 운영 동안 주기적으로 자체시험을 실행해야 한다. o 인가된 관리자에게 제품의 설정값 및 제품 자체의 무결성을 검증하는 기능을 제공해야 한다.

- 에이전트 보호 요구사항 유형1: 가상사설망, 네트워크 접근통제, 패치관리시스템

에이전트를 보유한 제품의 경우, 에이전트는 다음의 자체보호 기능을 제공해야 한다. o 기밀성 확보 - 부득이하게 사용자 패스워드, 제품 운영과 관련된 암호키 등을 파일시스템 또는 레지스트리에 저장시, 암호화 하여 저장해야 한다.

29) 국제용 인증 시 준수하는 보호프로파일, 취약성 분석 등에 따라 요구사항이 존재할 수 있으므로 신청기관 및 평가기관은 본 문서가 아닌 평가신청한 TOE가 준수해야 하는 요구사항을 확인해야 한다.

※ 적용시 주의사항 : 불가피한 경우, 패스워드는 암호화 대신 해시화 할 수 있다.
※ 적용시 주의사항 : 암호모듈검증제도에서 검증대상으로 지정된 안전한 암호 알고리즘의 사용을 권고한다.
※ 적용시 주의사항 : 본 요구사항 수행시 사용된 암호키는 삭제, 파일 숨김 및 접근통제 등을 통해 안전하게 보호되어야 한다.

- 제품의 설정값, 감사 데이터 등을 파일시스템 또는 레지스트리에 저장시, 평문으로 저장하지 않도록 암호화 또는 자체 구현한 인코딩 기법 등을 적용해야 한다.

o 무결성 확보

- 제품 동작 초기화 단계(서브시스템 로드)에서 제품의 설정값(정책, 환경), 실행파일, 필터 드라이버 등에 대해 무결성을 점검해야 한다.
※ 적용시 주의사항 : 운영체제의 안전모드 상에서 무결성 훼손이 발생할 경우, 이후 운영체제가 정상 부팅시 해당 변조를 탐지해야 한다.
- 주기적으로 또는 인가된 관리자 요구시, 무결성을 검증하여 관리자에게 실시간으로 통보하는 기능을 제공해야 한다.
※ 적용시 주의사항 : 변경이 매우 빈번한 정보(예 : 감사 데이터)의 경우 무결성 검사 대상에서 제외할 수 있다.

o 가용성 확보

- 변조된 정보(설정값, 실행파일, 필터 드라이버 등)를 수동으로 복구할 수 있는 기능을 제공해야 한다.

- 에이전트 보호 요구사항 유형2: 안티바이러스

에이전트를 보유한 제품의 경우, 에이전트는 다음의 자체보호 기능을 제공해야 한다.

o 기밀성 확보

- 부득이하게 사용자 패스워드, 제품 운영과 관련된 암호키 등을 파일시스템 또는 레지스트리에 저장시, 암호화 하여 저장해야 한다.
※ 적용시 주의사항 : 불가피한 경우, 패스워드는 암호화 대신 해시화 할 수 있다.
※ 적용시 주의사항 : 암호모듈검증제도에서 검증대상으로 지정된 안전한 암호 알고리즘의 사용을 권고한다.
※ 적용시 주의사항 : 본 요구사항 수행시 사용된 암호키는 삭제, 파일 숨김 및 접근통제 등을 통해 안전하게 보호되어야 한다.
- 제품의 설정값, 감사 데이터 등을 파일시스템 또는 레지스트리에 저장시, 평문으로 저장하지 않도록 암호화 또는 자체 구현한 인코딩 기법 등을 적용해야 한다.

o 무결성 확보

- 제품 동작 초기화 단계(서브시스템 로드)에서 제품의 설정값(정책, 환경), 실행파일, 필터 드라이버 등에 대해 무결성을 점검해야 한다.
※ 적용시 주의사항 : 운영체제의 안전모드 상에서 무결성 훼손이 발생할 경우, 이후 운영체제가 정상 부팅시 해당 변조를 탐지해야 한다.
- 주기적으로 또는 인가된 관리자 요구시, 무결성을 검증하여 관리자에게 실시간으로 통보하는 기능을 제공해야 한다.

※ 적용시 주의사항 : 변경이 매우 빈번한 정보(예 : 감사 데이터)의 경우 무결성 검사 대상에서 제외할 수 있다.

o 가용성 확보
- 제품의 설정값, 실행파일 등에 대한 비인가된 삭제 방지 기능을 제공해야 한다.
- 변조된 정보(설정값, 실행파일, 필터 드라이버 등)를 자동으로 복구할 수 있는 기능을 제공해야 한다.
- 제품의 실행파일(프로세스)이 악성코드 등에 의해 임의로 종료되지 않도록 실행파일(프로세스) 종료방지 기능을 제공해야 한다.

※ 적용시 주의사항: 종료방지 기능의 완벽한 구현이 불가할 경우, 임의 종료 발생시 PC 강제 종료 등 대체 통제를 구현할 수 있다.

- 에이전트 보호 요구사항 유형3: 스마트폰 보안관리

o 에이전트는 스마트폰에 설치된 에이전트의 설정값, 실행파일 등에 대한 비인가된 삭제 또는 변경을 방지하는 기능을 제공해야 한다.

o 에이전트는 스마트폰에 설치되어 실행되는 에이전트 프로세스가 임의로 종료되지 않도록 프로세스 종료방지 기능을 제공해야 한다.

o 에이전트는 USIM 카드 분리 또는 변경, 데이터 통신 차단, 비행 모드 등과 같은 예외 상황에서도 기존에 설정된 보안정책에 따른 정상적인 스마트폰 보호 기능을 제공해야 한다.

※ 적용 시 주의사항: 에이전트와 관리서버가 일정 시간동안 통신이 이루어지지 않는 경우, 에이전트가 자체적으로 기존에 설정된 보안정책을 적용하여 스마트폰 보호 기능을 제공해야 한다.

151 다음 표는 국가용 정보보호제품 보안요구사항의 자체시험 및 에이전트 보호 요구사항을 구분한 것이다.[30]

제품(유형)군	자체시험	에이전트 보호	비고
침입차단시스템(FW)	○	X	-
침입방지시스템(IPS)	○	X	-
통합보안관리제품	○	X	-
웹 응용프로그램 침입차단 제품	○	X	-
DDoS 대응장비	○	X	-
가상사설망 제품	○	○	「에이전트 보호」 유형 1
서버 접근통제 제품	○	X	-
DB 접근통제 제품	○	X	-
네트워크 접근통제 제품	○	○	「에이전트 보호」 유형 1
인터넷 전화 보안 제품	○	X	-
무선침입방지시스템	○	X	-
무선랜 인증 제품	○	X	-

30) 정보보호제품 국내용 평가.인증 세부 수행절차 최신문서의 [별표 3]에 포함된 제품 유형 및 명칭과 일부 상이할 수 있다.

제품(유형)군	자체시험	에이전트 보호	비고
스팸메일 차단시스템	○	X	-
안티바이러스 제품	○	○	「에이전트 보호」 유형 2
패치관리시스템	○	○	「에이전트 보호」 유형 1
망간 자료전송 제품	○	X	-
소스코드 보안약점 분석도구	X	X	-
스마트폰 보안관리 제품	X	○	「에이전트 보호」 유형 3

152 자체시험 요구사항에는 제품의 설정값 및 제품 자체의 무결성 검증 요구사항이 포함되어 있으며, 에이전트 보호 요구사항에는 노출로부터 보호하기 위한 비밀성, 손상으로부터 보호하기 위한 무결성, 손상으로부터 복구하기 위한 가용성 요구사항이 모두 포함되어 있다.

153 기밀성 확보가 필요한 경우 국가용 보안요구사항 요구수준에 따라 다음과 같은 보안대책으로 제공할 수 있다.

- 암호화를 위해 ARIA, SEED 등 암호 알고리즘 적용 가능(암호비도 112bit 이상 만족)
- 암호화 시 사용되는 암호키에 대한 보호대책은 암호화, 삭제 등 안전한 보호대책 사용 가능
- 패스워드의 경우 SHA-256 등 해시 알고리즘을 적용한 해시 가능(암호비도 112bit 이상 만족)
- 제품의 설정값, 감사 데이터 등의 경우 암호화 또는 자체 구현한 인코딩 기법 적용 가능

154 무결성 확보가 필요한 경우 국가용 보안요구사항 요구수준에 따라 다음과 같은 보안대책으로 제공할 수 있다.

- SHA-256 등 해시 알고리즘을 적용하여 해시값을 비교 검증함으로써 무결성이 손상된 경우 탐지 가능
- 변경이 매우 빈번한 정보(예: 감사 데이터)의 경우 무결성 검사 대상에서 제외 가능
- 무결성 검증 결과를 인가된 관리자에게 통보(예: 팝업 등)
- Windows 운영체제 부팅과 함께 TOE가 초기화 되는 시점에 따라 무결성 검증 기능을 우회할 수 있으므로 보안대책 구현 시 TOE 초기화 시점을 함께 고려해야 함

- Windows 운영체제 안전모드에서 무결성 오류가 발생한 경우, 운영체제 정상 부팅 후에는 무결성 오류에 대한 탐지가 가능해야 함

155 가용성 확보가 필요한 경우 국가용 보안요구사항 요구수준에 따라 다음과 같은 보안대책으로 제공할 수 있다.

- 사용자 인터페이스 및 상용 도구를 사용한 제품의 설정값, 실행파일 등의 비인가된 삭제 방지
  - 상용 도구는 일반적으로 운영체제의 파일시스템을 이용하여 파일을 삭제하며, 파일 삭제 행위를 탐지할 수 있음. 이 경우 단순히 상용 도구의 실행파일 명칭, 프로세스 정보 등을 사용하여 파일 삭제를 방지하는 것만으로는 불충분하며, 근본적인 삭제 방지 메커니즘을 구현해야 함
  - 상용 도구 중 일부는 운영체제의 파일시스템을 우회하여 파일을 삭제하거나, 안티디버그 기능으로 보호되어 있어 리버스 엔지니어링을 통한 분석이 어려워 삭제 행위 방지가 불가능할 수 있음. 이 경우 TOE가 대응할 수 없는 잔여 취약성으로 보고할 수 있음
- 변조된 정보에 대한 수동 복구의 예로 사용자가 개입하여 재설치, 관리서버/업데이트 서버를 통한 복구하는 기능을 TOE에서 제공하는 것을 들 수 있음. 사용자가 개입하지 않고 자동으로 복구하는 기능을 제공할 수도 있음[31)]
- 무결성 오류 발생 시점으로부터 복구가 시작되는 시점까지 자산이 노출 또는 유출되지 않도록 TOE가 구현되어야 함[32)]
- 제품의 실행파일(프로세스) 종료방지 기능 구현 시 프로세스 종료(kill), 중지(suspend), 속성값(예: 프로세스 종료 순서, 프로세스가 사용하는 핸들 값 등) 변경 등을 모두 고려해야 함

2.15 잘 알려진 취약성 정보

적용 범위	☑ 국제용 인증	☑ 국내용 인증

156 CC 평가 시 EAL 등급에 관계없이 공개 영역에서 잘 알려진 취약성 정보를 수집하여 활용해야 한다.

31) 국가용 보안요구사항 V3.0 준수 제품은 '서버 공통보안요구사항', '제품 보안요구사항'의 가용성 확보 관련 보안요구사항을 확인하여 필수, 조건부 필수, 선택 요구사항에 적합하게 보안요구사항을 구현해야 한다(예: 서버 공통보안요구사항'의 4.2.2).

32) 국가용 보안요구사항 V3.0 준수 제품은 '서버 공통보안요구사항', '제품 보안요구사항'의 가용성 확보 관련 보안요구사항을 확인하여 필수, 조건부 필수, 선택 요구사항에 적합하게 보안요구사항을 구현해야 한다(예: 서버 공통보안요구사항'의 4.2.2).

157 평가기관은 평가 착수 전에 신청기관이 평가대상에 잘 알려진 취약성이 존재하는지 자체 점검할 수 있도록 잠재적인 취약성 항목을 제공할 수 있으나, 악용 가능한 또는 잔여 취약성 존재 유무는 평가기관이 평가 과정에서 취약성 분석 및 침투시험을 통해 결정한다.

2.16 수행규정 및 국내용 수행절차에 대한 추가 해석사항

2.16.1 신청기관의 제출물에 대한 지적재산권

158 신청기관은 제출물에 대한 정당한 법적 권한을 가지고 있어야 하며, 신청기관이 제공한 제출물이 타인의 지적재산권을 침해하여 분쟁이 발생한 경우 이에 대한 모든 책임을 져야 한다.[33] 신청기관이 평가신청제품의 개발사가 아닌 경우, 제3자가 개발하거나 제공한 제출물을 사용하는 경우, 또는 신청기관 이외의 제3자와 공동으로 제출물에 대한 지적재산권을 보유한 경우 등이 해당하며, 신청기관은 '수행규정', '국내용 수행절차', 평가기준 및 평가방법론 등을 적용할 수 있는지 확인해야 한다. 또한 신청기관은 인증이 완료된 이후 '수행규정' 및 '국내용 수행절차'에서 정한 인증서보유기관으로서 인증제품에 대한 관리 등을 수행할 수 있어야 한다.

159 최초인증, 재인증, 인증효력유지(변경승인), 인증서효력연장이 완료되면 평가기관은 인증제품의 형상 정보를 기록하기 위해 인증제품 소스코드 및 실행파일(또는 이미지 파일)에 대한 해시값을 생성하며, 신청기관은 해시값 생성 대상이 되는 파일에 대한 평가기관의 접근을 허용해야 한다. 해시값 생성과 관련된 상세한 절차는 평가계약을 체결한 평가기관에 문의한다.

2.16.2 제품명 오용 및 인증내용 오·남용 금지

160 신청기관은 평가신청한 정보보호제품의 보안기능에 적합한 제품명으로 평가를 신청해야 한다. 제품명에 일반적으로 널리 알려진 특정 보안기능을 지칭하는 영문 약어 등을 사용하고 있으나 실제로는 관련 보안기능을 제공하지 않는 경우, 제품이 해당 보안기능을 제공하는 것으로 오해될 수 있으므로 허용되지 않는다. 또한 신청기관은 평가신청한 정보보호제품이 이미 인증서를 획득한 제품과 동일한 명칭을 사용할 수 없음에 유의한다.[34]

161 인증서보유기관은 인증제품에 대해 인증을 받은 내용 이외의 허위사실을 제품

33) '수행규정'에 의거, 제출물은 제품 및 관련 문서 등을 포함하며, 인증제품이 타사의 지적재산권을 침해한 경우 인증이 취소된다.

34) 동일한 인증제품 명칭으로 여러 인증서가 발급되는 경우 사용자에게 혼란을 초래하므로 인증제품목록에 포함되는 각 인증제품은 유일하게 식별되어야 한다.

에 표기·광고하거나, 인증제품의 형상을 변경하는 등 인증받지 않은 제품에 대해 인증제품으로 표기·광고하여서는 안된다. 이는 인증서보유기관 및 판매 대행사에서 제작한 제품 홍보물, 홈페이지, 지면 광고 등을 모두 포함한다. 전형적인 인증내용 오·남용 사례로는 인증제품 보안기능 허위 표기, 제품유형 변경 표기, 정부부처로 인증기관 허위 표기, 국내용 인증서를 국제용 인증서로 허위 표기, 로고 및 마크(IT보안인증사무국 로고, CC 인증마크, CCRA 서비스마크) 무단 사용[35] 등을 들 수 있다. 인증서보유기관이 인증내용을 오·남용 하는 경우 6개월 이내에 기간을 정해 인증서효력 정지가 가능하므로 이에 유의한다.[36]

2.16.3 정보 공개 동의서 제출 시 확인사항

162 신청기관은 '수행규정' 및 '국내용 수행절차'에 따라 평가계약을 체결할 때 ST(국제용 인증에 한함), 인증보고서 등 인증기관 홈페이지 및 CCRA 홈페이지에 공개될 정보에 대한 동의서를 평가기관에 제출해야 한다.

163 국제용 인증의 경우, 평가 완료 시 신청기관은 원칙적으로 '수행규정'에 따라 한글 및 영어로 작성된 최종 ST를 평가기관의 검토를 받아서 인증기관에 제출해야 한다. 최종 ST에 민감한 정보가 포함되어 있는 경우 신청기관은 별도로 공개용 ST를 작성하여 제출할 수 있다.[37]

- ST가 영어로 작성되어 평가된 경우 영어로 작성된 ST가 원본이며, 평가 인증 완료 시 이를 인증기관 및 CCRA 홈페이지에 공개한다(한글 ST 제출하지 않아도 무방하며, 공개용 영어 ST로 변환 가능).
- ST가 한글로 작성되어 평가된 경우 한글로 작성된 ST가 원본이며, 영어로 번역해야 한다(공개용 ST로 변환 후 번역 가능). 이 경우, 영어로 번역된 ST는 원본이 아니므로 ST 표지에 한글로 작성되어 평가된 ST를 영어로 번역했음을 반드시 표기해야 한다. 인증기관 홈페이지에는 한글 및 영어로 작성된 ST가 함께 공개될 수 있으며, CCRA 홈페이지에는 영어로 작성된 ST를 공개한다.

164 인증보고서에 공개되는 것을 희망하지 않는 정보에 대해서는 정보 공개 동의서 제출 단계에서 사전 확인해야 하며, '수행규정' 및 '국내용 수행절차'에 따라 타당한 사유를 제시해야 한다.

35) 인증서보유기관은 인증기관이 발급한 인증서를 사용하거나, '수행규정' 및 '국내용 수행절차'에 따라 인증마크를 발급받아서 사용할 수 있으며, 인증마크 발급을 희망하는 경우 공개된 양식을 사용하여 평가기관으로 신청한다.

36) 통상적으로 평가기관은 제출물 설명회 시 관련 규정을 설명하고 회의록에 포함한 후 신청기관의 서명을 득한다.

37) 공개용 ST를 작성하는 가이드는 CCRA 보조문서 「CCDB-2006-04-004 ST sanitising for publication」을 참조한다.

2.16.4 국가・공공기관 도입용 정보보호제품의 암호

165 국가・공공기관 도입을 목적으로 정보보호제품의 평가・인증을 신청한 경우 암호 알고리즘 및 암호비도 정책에 따라 암호비도 112bit 이상을 만족하는 암호 알고리즘을 사용해야 한다.[38] 신청기관은 정보보호제품에 포함된 암호 알고리즘, 암호키 길이, 암호 연산의 목적, 제3자 제공 암호 라이브러리 사용 여부 등을 ST의 '보안목표명세서 소개' 부분에 요약하여 서술해야 한다.

166 또한, 국가・공공기관 도입을 목적으로 가상사설망, DB 암호화, 통합인증, 문서암호화 제품의 평가・인증을 신청하는 경우 효력이 유효한 검증필 암호모듈을 탑재해야 한다. 검증필 암호모듈의 유효성은 아래와 같이 인증서를 발급하는 시점에서 확인한다.

- 최초평가를 통한 인증 완료에 따른 인증서 발급
- 재평가를 통한 인증 완료에 따른 인증서 발급
- 인증제품의 인증서효력연장 완료에 따른 인증서 발급

상기 제품유형은 인증서 발급 시점에서 검증필 암호모듈의 효력이 만료된 경우 인증서가 발급되지 않으므로, 신청기관은 검증필 암호모듈의 효력만료일이 경과하지 않았음을 반드시 확인한 후 신청해야 한다. 또한 평가・인증 진행 중에 검증필 암호모듈 효력만료가 예정된 경우 평가착수가 허용되지 않으므로, 신청기관은 평가기관에 문의하여 평가착수 가능 시기, 예상 평가・인증 기간 등을 고려하여 유효기간이 충분한 검증필 암호모듈을 사용해야 한다.

2.16.5 인증서 재발급 신청 시 유의사항

167 '수행규정'에 따라 인증서의 사용 권리를 양수하여 인증서 재발급을 신청[39]하는 경우 다음 각 호의 서류는 아래와 같은 기준을 만족해야 한다.

① 인증서 소유권 인수를 증명하는 서류

- 현재 인증서보유기관이 인증서 재발급을 신청해야 한다. 정보보호제품 평가・인증제도 관련 해당 인증제품(인증번호 포함)의 인증서 소유권 인수 범위(소스코드 포함) 및 내용, 법적 책임을 명확히 확인할 수 있는 문구가 명시적으로 포함되어 있어야 한다.

  - 인증서보유기관이 인증서 재발급 신청

38) 원칙적으로 112bit 미만의 낮은 비도 암호 알고리즘 사용을 허용하지 않으며, 필요 시 상세한 내용은 평가기관에 자문을 받을 것을 권고한다.

39) '인증서 사용 권리' 양수로 인해 인증서보유기관을 변경하여 인증서를 재발급하는 것은 인증서 발급 당시 인증서 효력범위에 포함되었던 개발업체를 변경하는 것은 아님에 유의한다. 또한 '인증서 사용 권리'와 '저작권'은 동일하지 않으므로 유의한다.

- "양도인" 및 "양수인" 명시
- "인증제품명" 및 "인증번호" 명시
- "양도 범위(소스코드, 제품 포함한 모든 제출물 등)" 명시
- "양도 내용(소유권 양도 등)" 명시
- "법적권한 및 책임 내용" 명시(확약서 또는 공문에 관련 내용 포함하여 제출 가능. '2.16.1절 신청기관의 제출물에 대한 지적재산권' 참고)

위의 정보가 명확하지 않거나, 인증제품의 "인증서 소유권"이 아닌 "저작권"을 양도하는 경우 인증서보유기관 변경이 허용되지 않음에 유의한다.

② 인증제품 소스코드 관리 등 보안관리대책

- 인증서 사용 권리를 양수하는 양수인의 소스코드 등 제출물 보안관리 책임 및 대책이 명시되어야 한다.
  - 양수인 측면에서의 소스코드 및 제출물에 대한 외부유출 방지 등 보안관리 위한 책임 및 대책(예, 제출물 안전한 보관 및 접근통제 수단, 외부 네트워크로부터 개발환경 보호 수단 등 물리적 보안 대책) 서술('2.6절 국내용 및 국제용 개발환경 보안점검 목록' 참조)
  - 보안관리 책임 관련 내용은 확약서 또는 공문에 포함하여 제출 가능

③ 수행규정 제66조(인증내용 오·남용 금지)에서 정한 인증제품 관리대책

- 인증내용 오남용 금지 관련 사항을 준수해야 함을 확약해야 한다.
  - 확약서 또는 공문에 관련 내용 포함하여 제출 가능

2.16.6 인증효력유지(변경승인) 시 유의사항

168 국제용 및 국내용 인증제품에 대한 인증효력유지(변경승인) 또는 재평가를 결정하기 위한 기준, 절차 등은 'CCRA 보조문서 보증 연속성 적용 가이드' 최신 문서[40]를 준수한다.[41]

40) CCRA 보조문서 'Assurance Continuity'가 개정되는 경우 최신 CCRA 보조문서를 따른다.

41) 다만, 검증필 암호모듈 탑재 의무화 대상 국내용 인증제품(가상사설망)의 검증필 암호모듈 교체 시 검증필 암호모듈을 호출하는 API 변경이 없는 경우에 한해 경미한 변경으로 판단하여 인증효력유지(변경승인)가 가능하다. 인증효력유지(변경승인) 신청일이 아닌 완료일 기준이므로, 인증서보유기관이 변경 이전 절차에 따른 인증효력유지(변경승인)를 희망하는 경우 평가에 소요되는 기간 및 인증에 소요되는 기간을 고려하여 미리 신청해야 한다. 국제용 인증제품의 경우 제품유형에 관계없이 'CCRA 보조문서 보증 연속성 적용 가이드' 최신 문서를 준수하여 인증효력유지(변경승인) 여부를 결정한다.

2.16.7 인증서효력연장 시 유의사항

169 국제용 인증제품의 인증서 효력을 연장하고자 하는 경우 'CCRA 보조문서 인증서 유효성 적용 가이드' 최신 문서[42]를 준수한다. 국내용 인증제품의 인증서 효력을 연장하고자 하는 경우에는 '국내용 중간점검 및 인증서효력연장 수행 가이드' 최신 문서를 준수한다.

170 인증서보유기관은 인증제품의 인증서효력연장을 신청하고자 하는 경우 다음에 유의해야 한다.

인증서효력연장을 위한 인증모델, 운영환경 확보 건

- 인증서효력연장은 인증제품을 유지보수하고 있음을 확인하는 과정이므로 인증서보유기관은 필요한 인증모델, 운영환경 등을 확보하고 있어야 하며, 인증서효력연장 시 인증범위에 포함되었던 하드웨어 일체형 인증제품의 인증모델, 소프트웨어 인증제품의 운영환경 등을 삭제할 수 없다.[43]

2.16.8 국가용 보안요구사항 V3.0 적용 시 유의사항

171 국가용 보안요구사항 V3.0은 '보안기능 시험'제도 및 '국내용 CC인증'제도의 기준으로, 1편의 <별지 2>에 포함된 제품 중 일부는 '국내용 CC인증'제도의 대상으로 포함되지 않는다.

172 국내용 CC인증이 가능한 정보보호제품 유형은 '국내용 수행절차'의 [별표 3]을 참조한다.

2.16.9 CC 평가 프레임워크에 적합한 대상

173 CC는 IT 제품[44]의 보안성을 평가하기 위한 기준으로 CCRA 회원국이 합의 하에 제·개정을 수행한다. 현재까지 CCRA 회원국은 IT 제품 이외에 서비스(예: 클라우드 서비스)는 CC 평가 프레임워크에 적합하지 않으므로 CC를 적용할 수 없다는 원칙을 표명하고 있다.[45]

174 따라서 정보보호제품 평가·인증은 현재까지 합의된 CC 평가 프레임워크에 적합한 IT 제품을 대상으로 수행한다.[46]

---

42) CCRA 보조문서 'Certificate Validity'가 개정되는 경우 최신 CCRA 보조문서를 따른다.

43) 통상적으로 평가기관은 제출물 설명회 시 관련 규정을 설명하고 회의록에 포함한 후 신청기관의 서명을 득한다.

44) CC 1부에서는 CC 평가 프레임워크를 서술하고 있다.

45) CCUF(CC Users Forum)는 CCRA의 CCDB에 클라우드 서비스에 대한 CC 평가·인증이 가능한지 문의한 바 있으며, CCDB는 CC의 적용 대상이 IT 제품이며 서비스에 적용할 수 없음을 공식적으로 답변했다.

46) 특히, 국내용 제품 평가신청은 「정보보호제품 국내용 평가·인증 세부 수행절차」에서 정한 제품 유형에 한한다.

2.16.20 인증제품 도입 시 운영환경 구축 관련

175 CC 인증서는 인증보고서에 명시된 버전의 인증제품을 대상으로 발급되며, 인증보고서에는 인증제품에 포함되지 않는 인증제품 운영에 필요한 최소한의 하드웨어, 소프트웨어를 운영환경으로 식별하고 있다.[47]

176 인증제품을 도입·운용하는 사용자는 도입정책을 준수하여 인증제품의 운영환경에 적합하게 인증제품을 설치하여 운용할 것을 권고한다. 사용자가 도입한 인증제품의 운영환경을 사용자 환경에 적합하게 구축하여 운용하는 것은 평가·인증제도에서 다루기 어려우므로, 사용자가 도입정책에 부합하는지 여부를 확인해야 한다. 또한, 사용자가 자신의 환경에 적합하게 구축한 운영환경에 대한 보안성은 인증제품의 보안기능과는 무관하며 인증제품이 보증할 수 없다.

47) 운영환경을 서술하고 평가하는 것과 관련된 원칙은 본 해설서의 2.2절을 참고한다. 또한, 2.2절의 원칙을 웹 방화벽에 적용한 사례는 2.9.2절을 참고한다.

3. 참고자료

CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017 - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components * 국제용 평가·인증 시 적용한다.
CEM	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017 * 국제용 평가·인증 시 적용한다.
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 1, CCMB-2006-09-001, September 2006 - Part 1: Introduction and general model Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, CCMB-2007-09-002 ~ CCMB-2007-09-003, September 2007 - Part 2: Security functional components - Part 3: Security assurance components * 국내용 평가·인증 시 적용한다.
CEM	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2, CCMB-2007-09-004, September 2007 * 국내용 평가·인증 시 적용한다.
수행규정	정보보호제품 평가·인증 수행규정(과학기술정보통신부·IT보안인증사무국, 2021.5.17.)
국내용 수행절차	정보보호제품 국내용 평가·인증 세부 수행절차 (과학기술정보통신부·IT보안인증사무국, 2021.5.17.)
국가용 보안요구사항	국가용 정보보호제품 보안요구사항 V1.0/V1.1 국가용 보안요구사항 V3.0 * 위 요구사항에 대한 정확한 해석은 관계기관의 자문을 통해 이루어졌다.

[붙임1] 국내용 개발환경 보안점검 목록

□ EAL2

1. 형상관리 (ALC_CMC.2, ALC_CMS.2)

점검 항목
1. TOE 구현의 표현에 대한 접근을 통제하는 수단은 무엇인가?
2. 형상관리 시스템에 의해서 통제되는 형상항목은 무엇이며, 형상목록은 각 형상항목을 유일하게 식별하는가?
3. TSF 관련 형상항목의 개발자는 누구인가?
4. TOE는 유일한 참조를 위한 레이블이 부착되어 있는가?
5. 형상항목을 유일하게 식별하는 데 사용한 방법은 무엇인가?
6. 형상관리시스템은 모든 형상항목을 유일하게 식별하는가?

2. 배포 (ALC_DEL.1)

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
3. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
4. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?
5. 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?

3. 기타

점검 항목
1. 내외부 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
2. 개발 영역 내에서 바이러스 등 악성 소프트웨어는 어떻게 검사하는가?
3. 개발/제조 시스템은 취약한 계정을 그대로 사용하고 있는가?

□ EAL3

1. 형상관리 (ALC_CMC.3, ALC_CMS.3)

점검 항목
1. 형상관리 시스템에 의해서 통제되는 형상항목은 무엇이며, 형상목록은 각 형상항목을 유일하게 식별하는가?
2. TSF 관련 형상항목의 개발자는 누구인가?
3. TOE는 유일한 참조를 위한 레이블이 부착되어 있는가?
4. 형상항목을 유일하게 식별하는 데 사용한 방법은 무엇인가?

점검 항목
5. 형상관리시스템은 모든 형상항목을 유일하게 식별하는가?
6. 사용하는 형상관리 시스템 및 도구는 무엇인가?
7. 형상관리 시스템에 정의된 역할 및 책임은 무엇인가?
8. 형상항목을 변경할 수 있도록 인가된 역할/사람은 누구이며, 인가된 사람만이 변경하도록 보장하는 수단은 무엇인가?
9. 형상항목에 대한 접근 권한을 부여하는 사람은 누구인가?

2. 배포 (ALC_DEL.1)

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
3. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
4. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?
5. 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?

3. 개발보안 (ALC_DVS.1)

3.1 일반적 보안대책

점검 항목
1. TOE가 개발/제조(설계/구현)되는 장소는 어디인가?
2. TOE 보안과 관련된 보안 조직은 어떻게 구성되어 있는가?
3. 물리적 보안 및 IT 보안에 대한 책임자는 누구인가?
4. 개발, 제조, 시험, 품질에 대한 통제를 분리하는 방법은 무엇인가?

3.2 인적 보안대책

점검 항목
1. 보안과 관련하여 직원들에게 부여되는 의무는 무엇인가?
2. 직원들이 보안과 관련된 의무를 이행하도록 하는 방법은 무엇인가?
3. 직원들에 대한 보안교육은 어떻게 이루어지는가?

3.3 물리적 보안대책

점검 항목
1. 개발/제조 영역에 대한 보안 수단은 무엇인가?
2. 근무시간 이후의 개발/제조 영역에 대한 보안수단은 무엇인가?
3. 개발/제조 영역의 접근통제 방법은 무엇인가?

점검 항목
4. 개발/제조 영역에 접근할 수 있는 사람은 누구인가?
5. 개발/제조 영역에 대한 접근 권한을 부여하는 사람은 누구인가?
6. 개발/제조 영역에 대한 접근이 기록되는 방법은 무엇인가?
7. 개발/제조 영역에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?

3.4 절차적 보안대책

점검 항목
1. 개발 영역 내에서 접근통제 되어야 하는 객체는 무엇인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료는 무엇인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료는 무엇인가?
2. 위의 객체에 대하여 접근통제 하는 방법 및 접근통제에 사용된 정보를 보호하는 방법은 무엇인가?
3. 위의 객체에 접근할 수 있는 사람은 누구인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료에 접근할 수 있는 직원은 누구인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료에 접근할 수 있는 직원은 누구인가?
4. 위의 객체에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 위의 객체에 대한 접근이 기록되는 방법은 무엇인가?
6. 위의 객체에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
7. 출력 장치는 어떤 것이 존재하며, 어디에 위치하는가? 출력장치를 보호하는 방법은 무엇인가?
8. 내외부 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
9. 개발 영역 내에서 바이러스 등 악성 소프트웨어는 어떻게 검사하는가?
10. 개발/제조 자료의 손상을 방지하기 위한 절차는 무엇인가?
11. 개발/제조 자료를 전송하기 위한 절차는 무엇인가?
12. TOE의 사용자용 복사본을 제조하고 사용자에게 전달하는 절차는 무엇인가?
13. 개발/제조 자료 및 TOE 구성요소를 파기하기 위한 절차는 무엇인가?
14. 개발장비 및 개발/제조 자료를 전송하거나 파기한 경우 이를 기록하는 방법은 무엇인가?
15. 데이터 백업 수행 주기는 어떻게 되는가?
16. 데이터 백업이 보관되는 장소 및 방법은 무엇인가?
17. 데이터 백업 시 이를 기록하는 방법은 무엇인가?
18. 비상 시 계획 및 절차는 무엇인가?
19. 비상 시 계획 및 절차는 직원들에게 어떻게 통보되는가?
20. 개발 인력에 변경이 발생한 경우 보안을 유지하기 위한 절차는 무엇인가?
21. 방문객에게 적용되는 보안 절차는 무엇인가?
22. 개발/제조 시스템은 취약한 계정을 그대로 사용하고 있는가?

□ EAL4

1. 형상관리 (ALC_CMC.4, ALC_CMS.4)

점검 항목
1. 형상관리 시스템에 의해서 통제되는 형상항목은 무엇이며, 형상목록은 각 형상항목을 유일하게 식별하는가?
2. TSF 관련 형상항목의 개발자는 누구인가?
3. TOE는 유일한 참조를 위한 레이블이 부착되어 있는가?
4. 형상항목을 유일하게 식별하는 데 사용한 방법은 무엇인가?
5. 형상관리시스템은 모든 형상항목을 유일하게 식별하는가?
6. 사용하는 형상관리 시스템 및 도구는 무엇인가?
7. 형상관리 시스템에 정의된 역할 및 책임은 무엇인가?
8. 형상항목을 변경할 수 있도록 인가된 역할/사람은 누구이며, 인가된 사람만이 변경하도록 보장하는 **자동화된** 수단은 무엇인가?
9. 형상항목에 대한 접근 권한을 부여하는 사람은 누구인가?
10. TOE 생산을 지원하는 자동화된 수단은 무엇인가?
11. 변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는 방법은 무엇인가?

2. 배포 (ALC_DEL.1)

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
3. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
4. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?
5. 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?

3. 개발보안 (ALC_DVS.1)

3.1 일반적 보안대책

점검 항목
1. TOE가 개발/제조(설계/구현)되는 장소는 어디인가?
2. TOE 보안과 관련된 보안 조직은 어떻게 구성되어 있는가?
3. 물리적 보안 및 IT 보안에 대한 책임자는 누구인가?
4. 개발, 제조, 시험, 품질에 대한 통제를 분리하는 방법은 무엇인가?

3.2 인적 보안대책

점검 항목
1. 보안과 관련하여 직원들에게 부여되는 의무는 무엇인가?
2. 직원들이 보안과 관련된 의무를 이행하도록 하는 방법은 무엇인가?
3. 직원들에 대한 보안교육은 어떻게 이루어지는가?

3.3 물리적 보안대책

점검 항목
1. 개발/제조 영역에 대한 보안 수단은 무엇인가?
2. 근무시간 이후의 개발/제조 영역에 대한 보안수단은 무엇인가?
3. 개발/제조 영역의 접근통제 방법은 무엇인가?
4. 개발/제조 영역에 접근할 수 있는 사람은 누구인가?
5. 개발/제조 영역에 대한 접근 권한을 부여하는 사람은 누구인가?
6. 개발/제조 영역에 대한 접근이 기록되는 방법은 무엇인가?
7. 개발/제조 영역에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?

3.4 절차적 보안대책

점검 항목
1. 개발 영역 내에서 접근통제 되어야 하는 객체는 무엇인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료는 무엇인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료는 무엇인가?
2. 위의 객체에 대하여 접근통제 하는 방법 및 접근통제에 사용된 정보를 보호하는 방법은 무엇인가?
3. 위의 객체에 접근할 수 있는 사람은 누구인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료에 접근할 수 있는 직원은 누구인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료에 접근할 수 있는 직원은 누구인가?
4. 위의 객체에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 위의 객체에 대한 접근이 기록되는 방법은 무엇인가?
6. 위의 객체에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
7. 출력 장치는 어떤 것이 존재하며, 어디에 위치하는가? 출력장치를 보호하는 방법은 무엇인가?
8. 내외부 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
9. 개발 영역 내에서 바이러스 등 악성 소프트웨어는 어떻게 검사하는가?
10. 개발/제조 자료의 손상을 방지하기 위한 절차는 무엇인가?
11. 개발/제조 자료를 전송하기 위한 절차는 무엇인가?
12. TOE의 사용자용 복사본을 제조하고 사용자에게 전달하는 절차는 무엇인가?
13. 개발/제조 자료 및 TOE 구성요소를 파기하기 위한 절차는 무엇인가?
14. 개발장비 및 개발/제조 자료를 전송하거나 파기한 경우 이를 기록하는 방법은 무엇인가?
15. 데이터 백업 수행 주기는 어떻게 되는가?

점검 항목
16. 데이터 백업이 보관되는 장소 및 방법은 무엇인가?
17. 데이터 백업 시 이를 기록하는 방법은 무엇인가?
18. 비상 시 계획 및 절차는 무엇인가?
19. 비상 시 계획 및 절차는 직원들에게 어떻게 통보되는가?
20. 개발 인력에 변경이 발생한 경우 보안을 유지하기 위한 절차는 무엇인가?
21. 방문객에게 적용되는 보안 절차는 무엇인가?
22. 개발/제조 시스템은 취약한 계정을 그대로 사용하고 있는가?

[붙임2] 국제용 개발환경 보안점검 목록

□ EAL2

1. 배포

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE의 어떤 부분에 배포 절차를 적용할 수 있는가?
3. 배포 절차가 적용되는 배포 단계는 무엇인가?
4. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
5. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
6. TOE가 사용자에게 배포되는 방법은 무엇인가?
7. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?

□ EAL3

1. 형상관리

점검 항목
1. 형상관리 방법은 무엇인가?
2. 사용하는 형상관리 시스템은 무엇인가?
3. 사용하는 형상관리 도구는 무엇인가?
4. 형상관리 시스템이 전체 TOE 개발 및 제조 과정에서 적용되는 방법은 무엇인가?
5. 형상관리 시스템이 전체 TOE 시험 및 분석 과정에서 적용되는 방법은 무엇인가?
6. 형상관리 시스템에 정의된 역할 및 책임은 무엇인가?
7. 형상관리 시스템에 의해서 통제되는 형상항목은 무엇인가?
8. 형상항목에 대한 행위 중 형상관리의 대상이 되는 행위는 무엇인가?
9. 형상항목을 변경할 수 있도록 인가된 역할/사람은 누구인가?
10. 인가된 사람만이 형상항목을 변경하도록 보장하는 수단은 무엇인가?
11. 형상항목을 변경했다는 사실은 어떻게 기록 및 감사되는가?
12. 형상항목에 대한 접근 권한을 부여하는 사람은 누구인가?
13. 형상항목에 대한 접근 권한을 변경했다는 사실은 어떻게 기록 및 감사되는가?
14. 형상관리 시스템에서 생성된 로그 파일을 보호하는 방법은 무엇인가?
15. 형상관리 시스템에서 생성된 로그 파일을 감사하는 방법은 무엇인가?
16. 각 버전의 TOE가 유일하게 참조 및 레이블 되는 방법은 무엇인가?
17. 어떤 형상관리문서가 존재하는가?
18. 형상관리문서와 관련된 역할 및 책임은 무엇인가?

2. 배포

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE의 어떤 부분에 배포 절차를 적용할 수 있는가?
3. 배포 절차가 적용되는 배포 단계는 무엇인가?
4. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
5. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
6. TOE가 사용자에게 배포되는 방법은 무엇인가?
7. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?

3. 개발보안

3.1 일반적 보안대책

점검 항목
1. TOE가 개발/제조(설계/구현)되는 장소는 어디인가?
2. TOE 보안과 관련된 보안 조직은 어떻게 구성되어 있는가?
3. 물리적 보안 및 IT 보안에 대한 책임자는 누구인가?
4. 개발, 제조, 시험, 품질에 대한 통제를 분리하는 방법은 무엇인가?

3.2 인적 보안대책

점검 항목
1. 보안과 관련하여 직원들에게 부여되는 의무는 무엇인가?
2. 직원들이 보안과 관련된 의무를 이행하도록 하는 방법은 무엇인가?
3. 직원들에 대한 보안교육은 어떻게 이루어지는가?
4. 직원들에 대한 보안교육은 어떻게 갱신되는가?

3.3 물리적 보안대책

점검 항목
1. 회사 건물에 대한 보안 수단은 무엇인가?
2. 회사 건물의 접근통제 방법은 무엇인가?
3. 회사 건물에 접근할 수 있는 사람은 누구인가?
4. 회사 건물에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 회사 건물에 대한 접근이 기록되는 방법은 무엇인가?
6. 회사 건물에 대한 접근 기록을 보호하는 방법은 무엇인가?
7. 회사 건물에 대한 접근 기록을 감사하는 사람은 누구인가?
8. 회사 건물에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
9. 개발/제조 영역에 대한 보안 수단은 무엇인가

점검 항목
10. 근무시간 이후의 개발/제조 영역에 대한 보안수단은 무엇인가?
11. 개발/제조 영역의 접근통제 방법은 무엇인가?
12. 개발/제조 영역에 접근할 수 있는 사람은 누구인가?
13. 개발/제조 영역에 대한 접근 권한을 부여하는 사람은 누구인가?
14. 개발/제조 영역에 대한 접근이 기록되는 방법은 무엇인가?
15. 개발/제조 영역에 대한 접근 기록을 보호하는 방법은 무엇인가?
16. 개발/제조 영역에 대한 접근 기록을 감사하는 사람은 누구인가?
17. 개발/제조 영역에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?

3.4 절차적 보안대책

점검 항목
1. 개발 영역 내에서 접근통제 되어야 하는 객체는 무엇인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료는 무엇인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료는 무엇인가?
2. 위의 객체에 대하여 접근통제 하는 방법 및 접근통제에 사용된 정보를 보호하는 방법은 무엇인가?
3. 위의 객체에 접근할 수 있는 사람은 누구인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료에 접근할 수 있는 직원은 누구인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료에 접근할 수 있는 직원은 누구인가?
4. 위의 객체에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 위의 객체에 대한 접근이 기록되는 방법은 무엇인가?
6. 위의 객체에 대한 접근 기록을 보호하는 방법은 무엇인가
7. 위의 객체에 대한 접근 기록을 감사하는 사람은 누구인가?
8. 위의 객체에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
9. 출력 장치는 어떤 것이 존재하며, 어디에 위치하는가? 출력장치를 보호하는 방법은 무엇인가?
10. 내부 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
11. 외부로 나가는 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
12. 개발 영역 내에서 바이러스 등 악성 소프트웨어는 어떻게 검사하는가?
13. 개발 장비가 이동되는 경우 안전하게 데이터를 파기하기 위한 절차는 무엇인가
14. 개발/제조 자료를 전송하거나 파기한 경우 이를 기록하는 방법은 무엇인가?
15. 데이터 백업과 관련된 역할 및 책임은 무엇인가?
16. 데이터 백업 수행 주기는 어떻게 되는가?
17. 데이터 백업에 사용되는 저장 매체는 무엇인가?
18. 데이터 백업이 보관되는 장소 및 방법은 무엇인가?
19. 데이터 백업 시 이를 기록하는 방법은 무엇인가?
20. 비상 시 계획 및 절차는 무엇인가?
21. 비상 시 계획 및 절차는 직원들에게 어떻게 통보되는가?
22. 비상 시 책임자는 누구인가?

점검 항목
23. TOE는 비상시에도 안전한가?

□ EAL4

1. 형상관리

점검 항목
1. 형상관리 방법은 무엇인가?
2. 사용하는 형상관리 시스템은 무엇인가?
3. 사용하는 형상관리 도구는 무엇인가?
4. TOE 구현의 표현에 대한 접근을 통제하는 자동화된 수단은 무엇인가?
5. 형상관리 시스템이 전체 TOE 개발 및 제조 과정에서 적용되는 방법은 무엇인가?
6. 형상관리 시스템이 전체 TOE 시험 및 분석 과정에서 적용되는 방법은 무엇인가?
7. 형상관리 시스템에 정의된 역할 및 책임은 무엇인가?
8. 형상관리 시스템에 의해서 통제되는 형상항목은 무엇인가?
9. 형상항목에 대한 행위 중 형상관리의 대상이 되는 행위는 무엇인가?
10. 형상항목을 변경할 수 있도록 인가된 역할/사람은 누구인가?
11. 인가된 사람만이 형상항목을 변경하도록 보장하는 수단은 무엇인가?
12. 형상항목을 변경했다는 사실은 어떻게 기록 및 감사되는가?
13. 형상항목에 대한 접근 권한을 부여하는 사람은 누구인가?
14. 형상항목에 대한 접근 권한을 변경했다는 사실은 어떻게 기록 및 감사되는가?
15. 형상관리 시스템에서 생성된 로그 파일을 보호하는 방법은 무엇인가?
16. 형상관리 시스템에서 생성된 로그 파일을 감사하는 방법은 무엇인가?
17. 각 버전의 TOE가 유일하게 참조 및 레이블 되는 방법은 무엇인가?
18. 각 버전의 TOE와 TOE 형상항목이 연결되는 방법은 무엇인가?
19. 각 버전의 TOE와 시험계획 및 결과가 연결되는 방법은 무엇인가?
20. TOE 및 TOE 컴포넌트를 운용하기 전에 이들을 검사하고 릴리즈 하기 위해 어떤 절차를 적용하는가?
21. TOE 및 설명서를 사용자에게 릴리즈 하기 전에 어떤 절차를 적용하는가?
22. 어떤 형상관리문서가 존재하는가?
23. 형상관리문서와 관련된 역할 및 책임은 무엇인가?

2. 배포

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE의 어떤 부분에 배포 절차를 적용할 수 있는가?
3. 배포 절차가 적용되는 배포 단계는 무엇인가?
4. TOE 배포 시 고려해야 하는 보안성은 무엇인가?

점검 항목
5. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
6. TOE가 사용자에게 배포되는 방법은 무엇인가?
7. 배포되어야 하는 버전의 TOE만이 배포됨은 보장하는 방법은 무엇인가?
8. 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?
9. 개발자로 위장한 배포 시도를 탐지하기 위한 방법은 무엇인가?

3. 개발보안

3.1 일반적 보안대책

점검 항목
1. TOE가 개발/제조(설계/구현)되는 장소는 어디인가?
2. TOE 보안과 관련된 보안 조직은 어떻게 구성되어 있는가?
3. 물리적 보안 및 IT 보안에 대한 책임자는 누구인가?
4. 개발, 제조, 시험, 품질에 대한 통제를 분리하는 방법은 무엇인가?

3.2 인적 보안대책

점검 항목
1. 보안과 관련하여 직원들에게 부여되는 의무는 무엇인가?
2. 직원들이 보안과 관련된 의무를 이행하도록 하는 방법은 무엇인가?
3. 직원들에 대한 보안교육은 어떻게 이루어지는가?
4. 직원들에 대한 보안교육은 어떻게 갱신되는가?

3.3 물리적 보안대책

점검 항목
1. 회사 건물에 대한 보안 수단은 무엇인가?
2. 회사 건물의 접근통제 방법은 무엇인가?
3. 회사 건물에 접근할 수 있는 사람은 누구인가?
4. 회사 건물에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 회사 건물에 대한 접근이 기록되는 방법은 무엇인가?
6. 회사 건물에 대한 접근 기록을 보호하는 방법은 무엇인가?
7. 회사 건물에 대한 접근 기록을 감사하는 사람은 누구인가?
8. 회사 건물에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
9. 개발/제조 영역에 대한 보안 수단은 무엇인가?
10. 근무시간 이후의 개발/제조 영역에 대한 보안수단은 무엇인가?
11. 개발/제조 영역의 접근통제 방법은 무엇인가?
12. 개발/제조 영역에 접근할 수 있는 사람은 누구인가?

점검 항목
13. 개발/제조 영역에 대한 접근 권한을 부여하는 사람은 누구인가?
14. 개발/제조 영역에 대한 접근이 기록되는 방법은 무엇인가?
15. 개발/제조 영역에 대한 접근 기록을 보호하는 방법은 무엇인가?
16. 개발/제조 영역에 대한 접근 기록을 감사하는 사람은 누구인가?
17. 개발/제조 영역에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?

3.4 절차적 보안대책

점검 항목
1. 개발 영역 내에서 접근통제 되어야 하는 객체는 무엇인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료는 무엇인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료는 무엇인가?
2. 위의 객체에 대하여 접근통제 하는 방법 및 접근통제에 사용된 정보를 보호하는 방법은 무엇인가?
3. 위의 객체에 접근할 수 있는 사람은 누구인가? 비밀성이 유지되어야 하는 TOE 개발/제조 자료에 접근할 수 있는 직원은 누구인가? TOE 무결성을 보호하기 위해 인가되지 않은 변경으로부터 보호되어야 하는 TOE 개발 자료에 접근할 수 있는 직원은 누구인가?
4. 위의 객체에 대한 접근 권한을 부여하는 사람은 누구인가?
5. 위의 객체에 대한 접근이 기록되는 방법은 무엇인가?
6. 위의 객체에 대한 접근 기록을 보호하는 방법은 무엇인가?
7. 위의 객체에 대한 접근 기록을 감사하는 사람은 누구인가?
8. 위의 객체에 대하여 인가되지 않은 접근 시도 시 취해지는 대응행동은 무엇인가?
9. 출력 장치는 어떤 것이 존재하며, 어디에 위치하는가? 출력장치를 보호하는 방법은 무엇인가?
10. 내부 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
11. 외부로 나가는 네트워크 연결은 어떻게 구성되며, 이들을 보호하는 방법은 무엇인가?
12. 개발 영역 내에서 바이러스 등 악성 소프트웨어는 어떻게 검사하는가?
13. 개발/제조 자료가 보관되는 장소 및 방법은 무엇인가?
14. 개발/제조 자료의 손상을 방지하기 위한 절차는 무엇인가?
15. 개발/제조 자료를 전송하기 위한 절차는 무엇인가?
16. TOE의 사용자용 복사본을 제조하고 사용자에게 전달하는 절차는 무엇인가?
17. 개발/제조 자료 및 TOE 구성요소를 파기하기 위한 절차는 무엇인가?
18. 개발 장비가 이동되는 경우 안전하게 데이터를 파기하기 위한 절차는 무엇인가?
19. 개발/제조 자료를 전송하거나 파기한 경우 이를 기록하는 방법은 무엇인가?
20. 데이터 백업과 관련된 역할 및 책임은 무엇인가?
21. 데이터 백업 수행 주기는 어떻게 되는가?
22. 데이터 백업에 사용되는 저장 매체는 무엇인가?
23. 데이터 백업이 보관되는 장소 및 방법은 무엇인가?
24. 데이터 백업 시 이를 기록하는 방법은 무엇인가?
25. 비상 시 계획 및 절차는 무엇인가?

점검 항목
26. 비상 시 계획 및 절차는 직원들에게 어떻게 통보되는가?
27. 비상 시 책임자는 누구인가?
28. TOE는 비상시에도 안전한가?
29. TOE 개발/제조에 사용되는 도구에 적용되는 절차는 무엇인가?
30. 개발 인력에 변경이 발생한 경우 보안을 유지하기 위한 절차는 무엇인가?
31. 방문객에게 적용되는 보안 절차는 무엇인가?