IT보안업체를 위한

보안기능 구현명세서 작성 가이드

V 1.0

NIS IT보안인증사무국

이 문서는 IT보안업체의 「보안기능 구현명세서」 작성에 필요한 사항을 안내하기 위한 목적으로 작성되었습니다.

이 문서의 ‘작성 예시’에 기재된 내용중 작성 의도와 무관하게 일부 보안제품에 구현된 보안기능과 유사하거나 동일한 내용이 있을 수 있으나 이는 해당되는 보안제품에 대한 승인 또는 추천의 의미는 아닙니다.

제 · 개정 이력

일 자	변경 내용	문서 버전
2023. 9. 19.	o ‘보안기능 구현명세서 작성 가이드’ 최초 작성, 배포	V1.0

목 차

1 개요

Ⅰ 일반 사항

(1) 보안기능 구현명세서 정의

「보안기능 구현명세서」란, **보안기능 시험을 신청한 업체가 대상 제품에 구현된 보안기능의 구현 방법 · 동작 절차 등에 대한 상세한 사항을 기술한 문서**입니다.

「보안기능 구현명세서」는 시험원이 신청 제품을 최대한 이해하여 제품에 대한 시험을 차질없이 진행하는데 활용되지만, 신청 업체의 사정으로 일반 보안요구사항의 작성이 어려울 경우 시험항목을 식별하기 위해 활용될 수도 있습니다.

(2) 작성 목적

이 문서는 보안기능 시험 신청을 준비하는 업체에게 「**보안기능 구현명세서**」의 작성 방법과 기준을 제시하고 시험기관에는 작성된 「보안기능 구현명세서」의 검토에 필요한 사항을 지원하기 위해 작성되었습니다.

(3) 식별 정보

이 문서의 식별정보는 다음과 같습니다.

작성자	국가정보원, 국가보안기술연구소 IT보안인증사무국
문서 버전	1.0
작성 일자	2023. 9. 19.
최종 수정일자	2023. 9. 19.

(4) 용어 정의

이 문서에서 사용되는 용어와 해석은 「국가용 보안요구사항」 V3.0에 기재된 내용을 따릅니다. 「국가용 보안요구사항」은 국가정보원 · 국가사이버안보센터 홈페이지에서 배포하고 있습니다.

2 작성시 유의사항

보안기능 구현명세서를 포함하여, 보안기능 확인서 신청에 필요한 모든 제출문서는 한국어(한글)로 작성되어야 합니다. 다만 제품 또는 보안기능 명칭 등의 고유명사는 외국어로 표기할 수 있습니다.

제출문서에 기재되는 내용을 바탕으로 보안기능 시험이 수행되므로 허위 · 과장 · 축소 · 누락없이 사실 그대로 기재해야 합니다. 고의로 제출문서에 사실이 아닌 내용을 기재할 경우, 시험이 중단될 수 있으며 보안기능 확인서가 발급되었더라도 효력이 무효화될 수 있습니다.

2 작성 기본 원칙

Ⅰ 준수 사항

(1) 작성 수준의 일관성

각 보안기능별 작성 수준이 일관성을 유지해야 합니다. 예를 들어 보안기능 'A'에 대해 '기능을 구현하는 방식과 동작에 대한 구체적인 수준'을 작성하는 수준이였다면 보안기능 'B'도 동일한 수준으로 작성해야 합니다.

〈 보안기능의 작성 수준에 대한 올바른 작성 예시 〉

❶ 첫 번째 예시

인증정보 재사용 방지

관리서버는 인증정보가 재사용되는 것을 방지하기 위해 OOO를 이용한 인증코드와 OOOO을 사용하고 있다.
관리자가 로그인을 위해 관리자ID를 입력하면, 해당 ID를 OOOOO에서 조회한 후에 .....
이때 OOO를 조회한 시간의 OOOO을 이용하여 인증코드를 생성한다.
인증코드는 'xxxxxx'과 같은 형태의 OOO 값을 OOO형태로 변환시킨 형태로 'xxxxxxx' 처럼 표현되며 ..... (후략)

〈 보안기능의 작성 수준에 대한 올바른 작성 예시 〉

❷ 두 번째 예시

무결성 검사 방법

제품은 저장된 중요 데이터의 무결성 검사는 OOO, OOO 및 암호 라이브러리를 대상으로 한다. 제품에서 사용하는 암호 라이브러리인 OpenSSL이 있으며 xxxx와 xxxx 폴더의 OOOO 값을 검사한다.
이때 AAAA 과정을 통해 OOOO 값이 xxxx 방식으로 처리되고 있음을 확인한다.
무결성 검증 과정에서 확인되는 항목은 다음의 표와 같다.
..... (표 생략)

(2) 작성된 내용의 합목적성

「보안기능 구현명세서」에 기재된 내용은 문서의 목적에 맞게 보안기능이 어떻게 구현되었는지 기재해야 하며 시험과 관련이 없는 내용은 기재하지 말아야 합니다. 다음에 해당하는 내용이 대표적인 예시입니다.

〈 보안기능 시험과 관련이 없는 항목의 예시 〉

❶ 최근 사이버보안 기술동향
❷ 제품과 관련된 보안위협 사례
❸ 제품의 필요성
❹ 제품의 우수성
❺ 제품의 최근 납품실적 및 주요 고객사
❻ 업체(또는 대표자)의 주요 수상경력
❼ 제품에 사용된 기술의 특허 사실 및 그 내용
❽ 업체의 사업 연혁 등

(3) 작성된 내용의 명확성

신청업체는 시험기관이 보안기능 구현명세서를 통해 제품의 각 구성요소가 제공하는 보안기능이 국가용 보안요구사항의 필수 요구항목을 모두 만족하는지 확인할 수 있도록 상세하게 기술해야 합니다.

제품에 구현된 보안기능에 대한 설명은 실제 구현과 일치하도록 작성해야 합니다. 보안기능은 각 기능별로 기재되어야 하며 다른 기능을 포함하여 기재할 수 없습니다. 다만, 기능간 연관관계 또는 인과관계는 기재할 수 있습니다.

신청업체는 제품 또는 제품의 특정 구성요소가 제공하는 보안기능이 **국가용 보안요구사항의 어떤 요구항목을 만족시키는지 명확하게 작성**해야 합니다. 다만, 국가용 보안요구사항 전체 문서에서 정의된 바 없는 새로운 보안기능일 경우, 국가용 보안요구사항의 준수여부를 기재하지 않아도 됩니다.

구성요소는 서버 · 에이전트 등 물리적으로 제품을 구성하는 구성요소를 의미합니다. 그리고 일부 보안기능을 서술하기 위해 데몬, 프로세스 등 보다 상세한 구성요소를 정의할 수 있습니다.

3 「보안기능 구현명세서」의 구성

Ⅰ 문서의 구성요소

(1) 표지

표지에는 「보안기능 구현명세서」가 보안기능 시험을 신청한 제품과 일치하며 신청 제품이 파생 제품과 구별되는 유일성을 확인할 수 있는 식별정보를 기재합니다. 기본적으로 △상세 버전이 포함된 제품명칭 △문서의 명칭 및 버전 △업체명칭 △문서의 작성 일자가 기재되야 합니다.

업체의 명칭은 보안기능 시험을 신청한 업체를 기재합니다. 제품에 따라서 개발업체와 신청업체가 상이할 수 있습니다. 하나 이상의 업체가 공동개발한 제품의 경우 공동개발 계약의 모든 당사자가 합의한 기재 방법에 따라 기재합니다.

(2) 제 · 개정 이력

「보안기능 구현명세서」의 제 · 개정 이력을 기재합니다. 기본적으로 △일자 △주요 개정 내용 △문서의 버전이 포함되어야 합니다.

(3) 권장 목차

「보안기능 구현명세서」에 기재가 필요한 주요 항목을 나타냅니다. 권장 목차는 아래 예시와 같이 구성될 수 있습니다.

그러나, 반드시 이 가이드의 권장 목차와 동일하게 「보안기능 구현명세서」의 목차를 구성해야 할 필요는 없습니다. 제품의 특성과 구현된 보안기능에 따라 일부 항목을 제외[1] 하거나 새로운 항목을 추가하는 등 신청 업체가 선택하여 목차를 구성할 수 있습니다.

---

1) 예를 들어 관리서버가 없는 제품은 관리서버의 보안기능을 기재할 필요가 없습니다.

〈 권장 목차 〉

(4) 권장 목차의 각 항목에 대한 설명

□ 1. 개요 항목

「보안기능 구현명세서」의 △식별정보 △수정 및 열람권한 등을 기재합니다.

‘개요’에 적힌 내용을 바탕으로 제출된 「보안기능 구현명세서」가 신청 제품에 대한 유일한 「보안기능 구현명세서」임을 입증할 수 있어야 합니다.

☐ 1.1 식별정보 **항목**

「보안기능 구현명세서」의 작성 주체 등 문서를 식별할 수 있는 정보를 기재합니다. 기본적으로 △문서의 명칭(예 : OOO v3.1.0 보안기능 구현명세서) △문서의 버전 △작성 일자 △파일명이 포함되어야 합니다.

☐ 1.2 수정 및 열람권한 **항목**

「보안기능 구현명세서」는 신청제품에 대한 비공개 사항이 포함되므로, 누구에게 열람 또는 수정의 권한이 부여되었는지 명확하게 선언되어야 합니다. 기본적으로 △문서의 작성 권한 △문서의 수정권한 △문서의 배포권한 △문서의 열람권한이 기재되야 합니다.

☐ 1.3 용어정의 **항목**

원칙적으로 「보안기능 구현명세서」에서 별도로 정의하지 않았다면 모든 용어는 **국가용 보안요구사항**에 기재된 내용대로 해석됩니다.

다만, 「보안기능 구현명세서」에서 별도로 정의하여 선언한 용어는 별도 선언한 바대로 해석됩니다.

☐ 2. 제품 설명 **항목**

신청 제품을 구성하고 있는 운용환경 및 H/W · S/W 구성요소와 배포절차를 설명하는 항목입니다.

☐ 2.1 운용환경 **항목**

신청 제품에 대한 시험원의 이해를 돕기 위해 제품이 운용되는 전산망의 표준구성도[1] 와 제품이 운용되는 운영체제(OS)에 대한 사항을 기재합니다.

〈 표준구성도 필수 기재항목 〉

❶ 전산망 구성도에서 제품의 설치위치에 대한 설명
❷ 전산망 구성도에 표기된 보호대상 IT실체(IT자산)에 대한 설명
❸ 제품의 보안기능과 IT실체의 연결표시 및 연관관계 설명

1) '표준구성도'란 신청 제품이 운용되는 전산망의 가장 일반적인 형태(Topology)로 묘사된 전산망 구성도를 말합니다.

표준구성도는 제품 및 제품이 보호하는 IT실체(IT자산)를 식별하고 설명을 기술해야 합니다.

S/W형태의 제품인 경우, 제품의 설치 · 동작에 필요한 운영체제(OS)를 추가로 기재해야 하며 이 경우, 제품이 설치되는 S/W 뿐 아니라, DB · Web 서버 등 제품에 연동되는 외부 IT실체도 포함됩니다.

운용 환경은 명확하게 식별되야 합니다. 단순히 'Redhat® Linux' · 'Windows® Server' 등 제품 명칭만 기재하지 않고, S/W의 특정 형상을 지정하는 버전도 기재해야 합니다.

〈 표 1. 운용 환경 기재 예시〉

잘못된 표기	올바른 표기
Windows 10	Windows 10 pro 20H2 19042.928
Linux	Release : Redhat linux x.x Kernel : Linux version 3.16.0-30-generic (이하 생략)
Apache Server	Apache/2.4.6 (Cent OS)

운용 환경 버전은 S/W(OS)에서 제공되는 명령어(예 : grep . /etc/*-release, httpd -v 등) 또는 버전 확인 기능을 사용하여 출력된 값을 기재합니다.

☐ 2.2.1 H/W 구성요소 **항목**

신청 제품이 설치되는 H/W사양을 식별하고 기술합니다. S/W 형태의 제품은 보안기능 시험을 신청한 사양인 '권장 사양'과 제품의 정상적인 동작에 필요한 '최소 사양'을 각각 기재해야 하며 H/W일체형 제품[1]은 보안기능 시험을 신청한 사양인 '권장 사양'을 기재합니다.

관리서버-에이전트의 형태인 경우, 각각의 H/W사양을 모두 식별하고 기재해야 하며 '권장 사양'과 '최소 사양'을 기재해야 합니다.

다만, 관리서버 또는 에이전트중 H/W일체형이 있다면 '권장 사양'만 기재합니다.

H/W사양에서 식별되어야 할 요소는 대표적으로 △메모리 △CPU(계열 포함) △저장장치 △네트워크 인터페이스(예 : NIC) 등이 있습니다.

1) 예를 들어 전용 H/W의 펌웨어 형태로 설치되는 △침입차단시스템 △침입방지시스템 △스위치 · 라우터 등이 있습니다.

□ 2.2.2 S/W 모듈 **항목**

신청 제품에 구현된 보안기능을 구성하고 있는 파일 또는 서비스 형태의 3rd party S/W 모듈을 의미합니다.

다만, 모든 모듈을 기재할 필요는 없으며 국가용 보안요구사항에 해당되는 모듈에 대해 상세한 버전 또는 Release를 명확히 표기합니다. 버전에 따른 호환성이 있는 경우, “0.0.0.0 R1 부터 1.1.1.1 Rn 까지”로 기술합니다. 관리서버-에이전트의 형태인 경우, 각각의 S/W모듈을 모두 식별하고 기재합니다.

S/W 모듈의 기재 예시는 아래와 같습니다.

〈 S/W 모듈 기재 예시 〉

연번	모듈 명칭	적용된 보안기능	OpenSource
1	OpenSSL 3.0.2	SSL암호통신, 키 생성	O
2	Apache Tomcat 10.0.18	관리자 식별 및 인증	O

□ 2.3 제품의 배포절차 **항목**

‘제품의 배포 절차’는 납품 요청에서 시작되어 납품 완료 및 검수까지의 절차와 납품 이후 유지보수 절차를 그림 또는 도표로 기재합니다.

그리고 제품 배포(판매)시 어떤 구성물이 포함되어 배포되는지 그 패키지 정보를 기술합니다. 패키지란, 국가 · 공공기관에 배포되는 문서(사용자 설명서 등)와 구성물의 정보를 의미합니다.

다음의 사항이 필수로 기재되어야 합니다.

〈 배포절차 기본 기재항목 〉

❶ 최초 제공되는 문서(예 : 사용자 설명서 등)

❷ (S/W제품인 경우) 제품이 저장되어 배포되는 매체 이미지(예 : CD · USB 메모리 등의 사진)

❸ (H/W제품인 경우) 제품이 설치된 H/W의 정면과 후면 사진

☐ 3.1 제품 접속경로 및 방법 **항목**

일반 사용자 및 관리자가 제품에 접속할 수 있는 경로 또는 방법을 빠짐없이 식별하여 기재합니다. **「보안기능 구현명세서」에 기재되지 않은 접속경로 및 방법은 백도어로 간주**됩니다. 시험과정에 발견되거나 뒤늦게 제출되더라도 인정되지 않기 때문에 각별히 유의하여 작성하시기 바랍니다.

다음의 사항이 필수로 포함되어야 합니다.

〈 접속경로 · 방법 필수 기재항목 〉

❶ 사람 또는 외부 IT실체의 제품 접속을 위해 제품이 제공하는 인터페이스[1] 정보
❷ 기본 설정된 관리자 및 유지보수용 계정
❸ 전원 인가시 또는 운용중 특정 조건 · 외부 신호 · 키보드 입력의 조합 등에 의해 활성화되는 인터페이스[2] · 계정

그러나, 관리자 · 유지보수용 계정의 비밀번호[3]는 「보안기능 구현명세서」에 기재하지 마십시오.

여 백

1) '인터페이스'란, 접속을 위해 실행(준비)되는 포트 · 서비스 · 프로세스 등을 말합니다.

2) 예를 들어 키보드의 특정 입력값에 의해 활성화되는 엔지니어 모드 등이 있습니다.

3) 다만, 시험을 위해 시험기관에 계정 비밀번호의 제공이 필요한 경우, 임시 비밀번호를 설정하여 별도로 시험기관에 통보하십시오. 시험이 끝나 신청 제품을 회수한 이후 제공했던 비밀번호와 다른 비밀번호로 변경해야 합니다.

4 보안기능에 대한 서술 예시

Ⅰ ‘식별 및 인증’ 기능

(1) 예시에 대한 설명

‘식별 및 인증’기능의 예시는 웹 기반 보안관리 화면을 통해 ID/PW 방식으로 관리자를 식별 및 인증하는 기능에 대한 작성 예시이며, ‘1.1 사용자 등 식별 및 인증’ 요구사항에 명시된 에이전트 또는 클라이언트에 대한 식별 및 인증은 해당되지 않습니다.

또한, 신청 제품이 보안관리 접속을 지원하는 형태가 다양할 수 있지만, 이 문서에 작성된 예시는 웹 기반 관리 접속에 대한 예시일뿐입니다.

또한, 이 문서의 웹 관리 기반 관리접속의 예시가 국가 · 공공기관에 납품되는 모든 제품에 웹 기반 관리 접속기능을 필수로 구현해야 한다는 정책을 의미하지는 않습니다.

(2) 예시 활용시 참고사항

이 예시는 「서버 공통보안요구사항 V3.0 R1」의 ‘1.1 사용자 등 식별 및 인증’ 중 1.1.1 요구사항에 대한 예시입니다.

요구항목 중 보안관리 측면에서 구현해야할 항목인 ‘② 관리자는 각 사용자 또는 그룹별로 권한을 부여할 수 있어야 한다.’ ‘③ 사용자 계정(ID)은 고유한 값으로 중복 등록되지 않아야 한다.’는 해당되지 않습니다.

또한 관리자 관리 접속에 대한 예시이므로 제품을 구성하는 에이전트 또는 클라이언트에 사용자가 존재하는 경우에는 식별 및 인증 시 IP 주소를 포함하여 부가 속성 정보도 함께 인증해야 함을 고려해야 합니다.

식별 및 인증 이후 인증을 관리하기 위해 Session ID를 이용한 방식을 예로 들었으나 토큰 기반 인증 방식 등 다양한 인증 방식이 고려될 수 있음을 참고하시기 바랍니다.

식별 및 인증 이후 인증을 관리하는 방안으로 Session ID를 이용한 방식을 예로 들었으나 토큰 기반 인증 방식 등 다양한 인증 방식이 고려될 수 있음을 참고하시기 바랍니다.

인증 방식은 그 특성에 따라 인증정보 재사용 등 다양한 취약점이 발생할 수 있으므로 이를 고려한 설계가 필요합니다.

(3) 작성 예시

〈 작성 예시 〉

1. 사용자 등의 식별 및 인증 기능

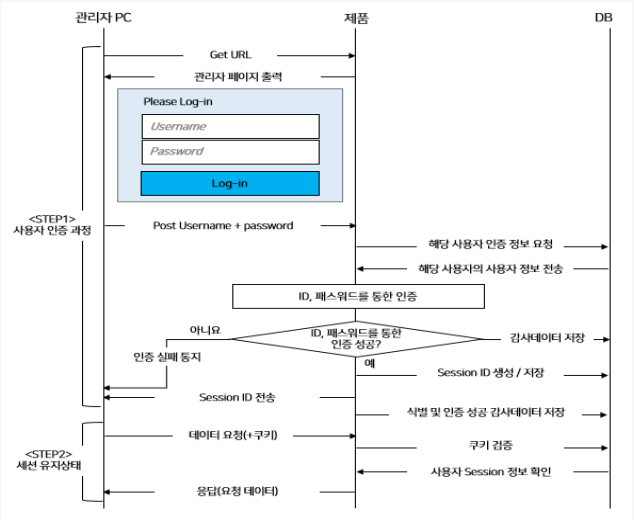
1.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 1.1.1

1.2 보안기능 설명

신청 제품은 관리자의 신원을 검증하기 위하여 사용자의 계정(ID)와 패스워드 기반 식별 및 인증 기능을 제공한다.

관리자 계정은 고유한 값으로 중복 등록되지 않으며, 관리자가 접속을 요청하면 입력된 계정 정보를 기반으로 관리자 등록시 저장된 패스워드 정보와 관리자 접속 요청시에 입력한 패스워드 정보를 비교하여 식별 및 인증을 수행한다. '식별 및 인증'을 통과한 사용자가 보안관리 페이지에 접속하는 동안 Session ID 값을 이용, 저장된 세션 정보를 비교하여 사용자 세션을 유지한다.

1.3 보안기능 동작 순서도



〈 작성 예시 〉

1.4 보안기능의 동작

(절차 1) 사용자가 제품에 인증을 요청하면 제품은 해당 사용자가 입력한 식별정보를 바탕으로 데이터베이스에 사용자 인증정보를 요청하여 인증정보를 수신한다.

부가 설명

❶ 관리자로 접속이 한정된 보안관리 웹페이지에 대한 접속은 '서버 공통보안요구사항 V3.0 R1'의 '2.3 보안관리용 IP제한'에 대한 메커니즘에 따라 보안관리 IP 지정 여부를 확인하여 지정된 IP일 경우, 식별 및 인증 페이지를 제공해야 합니다.

❷ 식별 및 인증에 대한 성공여부를 판단한 이후 중복 접속 여부 판단 과정에 대한 예시는 생략되었으므로 구현명세서 작성 시 '서버 공통보안요구사항 V3.0 R1'의 '6. 안전한 세션 관리' 중 '6.2 동시접속 세션 제한'에 대한 구현 메커니즘을 고려하여 설계할 필요가 있습니다.

※ '부가 설명'은 이 문서에 기재된 작성 예시에 대한 설명입니다. 신청업체가 작성하는 구현명세서에 기재되어야할 사항이 아닙니다.

〈 작성 예시 〉

(절차 2) 제품은 사용자가 입력한 인증정보와 데이터베이스로부터 수신한 인증정보를 비교하여 인증 성공/실패여부를 판단하여 인증이 실패인 경우 사용자에게 인증실패를 통지하고 감사기록을 생성하여 데이터베이스에 기록한다.

(절차 3) 사용자 인증이 성공하는 경우 제품은 사용자의 고유한 Session ID를 부여하고 해당 정보를 사용자에게 Session ID 값을 전달한다.

(절차 4) 식별 및 인증 과정이 종료되면 제품은 식별 및 인증 성공에 대한 감사데이터를 생성하여 저장한다.

(절차 5) 사용자는 제품에서 전달한 Session ID를 쿠키에 저장한 후, 인증이 필요한 페이지에 접근할 때 Session ID가 포함된 쿠키 정보를 함께 전송한다.

(절차 6) 제품은 수신한 Cookie와 저장된 세션 정보를 비교하여 세션의 유효성을 판단하여 사용자 요청에 대한 응답을 전달한다.

2 ‘기본(default) 패스워드 관리’ 기능

(1) 예시에 대한 설명

이 예시는 「서버 공통보안요구사항 V3.0 R1」의 △‘2.4.1 요구사항(최초 제품 접속시 관리자 비밀번호 강제 생성 · 변경)’에 대한 작성의 예시입니다.

〈 작성 예시 〉

1. 기본 패스워드 강제 변경 기능

1.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 2.4.1

1.2 보안기능 설명

제품은 기본 계정이 생성되어 있는 공장초기화 상태로 출하된다. 이후 관리자가 보안관리 기능 수행을 위해 최초 로컬콘솔 접속을 시도하는 경우, 기본값으로 설정된 관리자 패스워드를 강제로 변경하는 기능을 제공한다.

기본 계정 : admin
패스워드 : xxxxxxxxxxxx

기본값을 변경하지 않는 경우 보안관리 기능을 수행할 수 없으며 로컬콘솔에서 기본 패스워드를 변경하지 않는다면 SSH, WEB으로 접속이 불가하다.

기본 패스워드 변경을 완료하면 이후 제품 접속시에는 패스워드 변경을 유도하지 않는다. △펌웨어 재설치 △공장초기화 수행 후 관리자가 제품 최초 접속하는 경우 다시 패스워드를 강제로 변경하도록 유도한다.

3 ‘데이터 보호’ 기능

(1) 예시에 대한 설명

이 예시는 「서버 공통보안요구사항 V3.0 R1」의 △‘3.1.1 요구사항(제품 구성요소간 통신시 전송 데이터 보호)’ △‘3.1.1 요구사항(제품 구성요소간 통신시 전송 데이터 보호)’에 대한 작성의 예시입니다.

〈 작성 예시 〉

1. 전송 데이터 보호 기능

1.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 3.1.1

1.2 보안기능 설명

제품은 '제품의 구성요소간에 전송되는 데이터' 및 '제품과 외부 IT실체간에 전송되는 데이터'를 노출 · 변경으로부터 보호하기 위해 안전한 암호통신을 수행한다.

제품 구성요소간 전송되는 데이터 및 암호화 방식은 다음과 같다.

전송구간	전송 데이터	보호 방법
Server ↔ Agent	정책 데이터, 감사 데이터	TLS 1.2 사용 - OpenSSL 1.1.1 - AES256-CBC - SHA256
Server ↔ Consol	인증 데이터, 정책 데이터	TLS 1.2 사용 - OpenSSL 1.1.1 - AES256-CBC - SHA256

※ 작성 예시에 'Server↔Agent'와 'Server↔Colsol'만 있다고 하여 이 두 가지만 기재해야 한다는 의미는 아닙니다.

1.2.1 제품 구성요소간 전송 데이터(Server ↔ Agent)

Server는 Agent로 정책 데이터를 전송하며 Agent는 Server로 감사데이터를 전송한다.

관리자는 Server를 통해 보안정책을 설정하며 Agent는 Server로부터 정책을 전달받아 보안기능을 수행한다. 또한, Agent는 생성된 감사 데이터를 Server로 전송한다.

제품 구성요소간 전송되는 데이터는 OpenSSL 1.1.1 라이브러리를 이용한 TLS 1.2 프로토콜을 활용하여 전송 데이터에 대한 기밀성 및 무결성을 제공한다.

부가 설명

❶ 제품이 여러 개의 구성요소로 구분되어 있는 경우, 모든 구성요소 간 전송데이터에 대해 서술해야 합니다.

예) Server ↔ Agent, Server ↔ Console, Console ↔ Agent 등

❷ 제품이 외부 IT 실체와 통신하는 경우, 통신 가능한 모든 외부 IT 실체를 명시하고 전송데이터를 보호하는 방법에 대해 서술해야 합니다.

예) 인증서버, SNMP 서버, 업데이트 서버, 로그서버

〈 작성 예시 〉

2. 저장 데이터 보호 기능

2.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 3.2.1

2.2 보안기능 설명

제품은 제품에 저장되는 데이터를 안전하게 보호하고 있으며, 데이터의 저장위치 및 방법은 아래와 같다.

저장 데이터	저장 위치	보호 방법
인증 데이터	Server - DBMS	Hash 알고리즘 사용 - SHA256
DBMS 접속정보	Server - 파일시스템	암호알고리즘 사용 - ARIA256
정책 데이터	Server - DBMS	-
	Agent - 파일시스템	암호알고리즘 사용 - ARIA256

2.2.1 인증 데이터

제품 접속을 위해 사용되는 인증 데이터는 해시 알고리즘(SHA-256)을 통해 Server와 함께 설치되는 DBMS에 저장된다. 관리자 패스워드 저장시에는 salt 값을 적용하여 동일 패스워드에 대해 동일한 암호문이 생성되지 않도록 구현되었다.

〈 작성 예시 〉

2.2.2 DBMS 접속 정보

DBMS 접속 정보는 제품 설치 시 관리자가 설정하도록 구현되어 있으며, ARIA256를 통해 암호화하며 Server 내 파일시스템에 저장하여 보호하고 있다.

2.2.3 정책 데이터

관리자는 Console을 통해 Server에 접속하여 보안정책을 설정할 수 있으며, 정책 데이터는 Server와 함께 설치되는 DBMS에 저장되어 안전하게 보호된다.

Agent는 Server로부터 보안정책을 전달받아 보안기능을 수행하며, 전달받은 보안정책은 Agent 파일시스템에 암호화(ARIA-256)되어 저장된다.

부가 설명

❶ 제품 운용을 위해 저장되는 모든 데이터를 모두 식별하고 보호방법에 대해 서술해야 합니다.

❷ 제품의 데이터가 DBMS에 저장될 경우, DBMS의 식별 및 인증 기능을 통해 비인가된 사용자의 접근으로부터 보호되어야 합니다.

4 '자체 시험' 기능

(1) 예시에 대한 설명

이 예시는 「서버 공통보안요구사항 V3.0 R1」의 △'4.1.1 요구사항(운용중 주기적 또는 관리자에 의한 자체시험)' △'4.2.1 요구사항(제품 자체 및 설정값에 대한 무결성 검증)'에 대한 작성의 예시입니다.

〈 작성 예시 〉

1. 전송 데이터 보호 기능

1.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 4.1.1

1.2 보안기능 설명

〈 작성 예시 〉

1.2.1 서버에 대한 자체시험

서버는 총 5개의 프로세스로 구성되어 있으며, 그 중 보안기능을 수행하는 주요 프로세스는 다음과 같다.

〈 프로세스 목록 〉

연번	프로세스명(파일이름)	주요 기능(요약)
1	A	
2	B	
3	C	
4	D	
5	E	

A 프로세스는 감사기록, 식별 및 인증, 자체보호 기능을 제공하는 제품의 주요 프로세스로 최초 실행 시 B, C 프로세스가 정상 실행 중인지를 확인하여 감사로그를 생성한다.

그 결과를 다음과 같이 감사기록으로 저장한다.

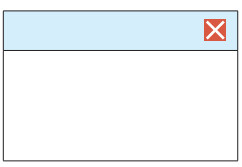
〈 감사로그 화면 출력 〉

.....
.....

이때 B 또는 C 프로세스 중 하나 이상이 정상 실행되고 있지 않은 경우 팝업으로 경고메시지를 출력하고 제품은 즉시 종료된다.

〈 경고 화면 출력 〉

.....
xxxxx. xxxxxxxx
.....



〈 작성 예시 〉

B 프로세스는 제품의 주요 프로세스로 자체보호, 암호지원, 전송데이터 보호 기능을 제공하며 최초 실행시 A, C 프로세스가 정상 실행 중인지 확인하여 감사로그를 생성한다.

이때 A 또는 C 프로세스 중 하나 이상의 프로세스가 정상 실행되고 있지 않은 경우 팝업으로 경고메시지를 출력하고 제품은 즉시 종료된다.

C 프로세스는 보안관리, 자체보호 기능을 제공하는 …(후략).

A, B, C 프로세스는 최초 실행 이후 5분 간격으로 자신 이외의 프로세스에 대해 정상 실행 여부를 확인하여 감사로그를 생성한다.

이때에도 하나 이상의 프로세스가 정상 실행되고 있지 않은 경우 팝업으로 경고메시지를 출력하고 제품은 즉시 종료된다.

D 프로세스는 주기적인 통계 리포트 생성 및 저장 기능을 제공하고 있으며 국가용 보안요구사항의 주요 기능과는 무관한 기능으로 자체시험을 수행하지 않는다.

1.2.2 에이전트에 대한 자체시험

에이전트는 1개의 서비스와 1개의 프로세스로 구성되어 있으며 에이전트의 최초 구동 시 서비스가 정상 동작하고 있는지 확인하고 그 결과를 서버로 전송한다. 서버의 A 프로세스는 전송받은 결과를 감사로그로 생성한다.

〈 감사로그 화면 출력 〉

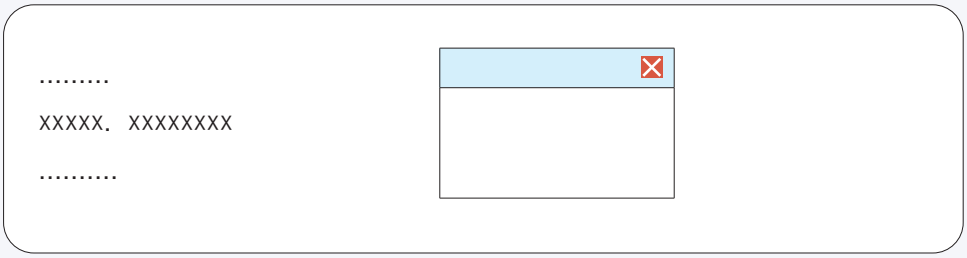
```
.....
.....
OOOOOOOOO XXXXXXX  OOOOOOOOOOOOOO
.....
OOOOOOXXXXXOOOOXX  XXXXXOOOOOOOO
```

이때 서비스가 정상 동작하지 않는 경우 팝업으로 경고메시지를 출력하고 제품은 즉시 종료된다.

〈 작성 예시 〉

에이전트 프로세는 실행 중 5분 간격으로 서비스의 정상 동작 여부를 확인하고 그 결과를 서버로 전송한다. 이때에도 서비스가 정상 동작하지 않는 경우 팝업으로 경고메시지를 출력하고 제품은 즉시 종료된다.

〈 경고 화면 출력 〉



서비스는 제품 설치 후 윈도우 OS 구동 시 자동으로 서비스를 시작하며 5분 간격으로 에이전트 프로세스의 실행 여부를 확인하여 그 결과를 서버로 전송한다.

2. 무결성 검증 기능

2.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 4.2.1

2.2 보안기능 설명

2.2.1 서버의 무결성 검증

서버는 /usr/home/~ 에 설치되며 최초 설치 시 총 xxxx개의 파일과 xx개의 디렉토리로 구성된다.

그 중에서 무결성 검증 대상에 포함되는 항목은 다음과 같다.

〈 무결성 검증 대상 목록 〉

연번	명칭	저장위치	해시값
1	A	.....	.....
2	B	.....	.....
3	B	.....	.....
4	D	.....	.....

〈 작성 예시 〉

무결성 검증 대상에서 제외되는 항목과 사유는 다음과 같다.

〈 무결성 검증 대상 제외 목록 〉

연번	명칭	저장위치	제외 사유
1	A	.....	.....
2	B	.....	.....
3	C	.....	.....

A 프로세스는 최초 실행 시 무결성 검증 대상에 포함되는 모든 파일에 대해 각 파일의 해시값을 생성(SHA512)하여 DBMS 내 xxx 테이블에 저장된 각 파일의 해시값과 비교하여 무결성 검증 기능을 수행한다.

또한 A프로세스는 관리자가 웹 UI의 '자체시험 – 서버 무결성 검사' 메뉴에서 실행 버튼을 클릭하면 위와 동일하게 무결성 검증 기능을 수행한다.

2.2.2 에이전트의 무결성 검증

에이전트는 c:/testagent/ 또는 설치 시 사용자가 설정한 폴더에 설치되며 최초 설치 시에는 총 xxxx개의 파일과 xx개의 폴더로 구성된다.

그 중에서 무결성 검증 대상에 포함되는 항목은 다음과 같다.

〈 무결성 검증 대상 목록 〉

연번	명칭	저장위치	해시값
1	A	.....	.....
2	B	.....	.....

무결성 검증 대상에서 제외되는 항목과 사유는 다음과 같다.

〈 무결성 검증 대상 제외 목록 〉

연번	명칭	저장위치	제외 사유
1	Logo.gif	C:/testagent/	웹 UI 메인화면에서 사용하는 그림파일이며 삭제 또는 변경되어도 제품 보안기능 수행에 영향을 주지 않는다.
2	B	.....	.....

〈 작성 예시 〉

에이전트 프로세스는 최초 실행 시 무결성 검증 대상에 포함되는 모든 파일에 대해서 SHA256으로 각 파일에 대한 해시값을 생성하여 서버로 전송하고, 서버의 A 프로세스는 DBMS 내 xxx 테이블에 저장된 각 파일의 해시값과 비교하여 무결성 검증 기능을 수행한다.

또한 A프로세스는 관리자가 웹 UI의 '자체시험 및 에이전트 무결성 검사' 메뉴에서 실행 버튼을 클릭하면 에이전트 프로세스에게 해시값 생성을 요청하여 무결성 검증 기능을 수행한다.

2.2.3 무결성 검증 실패 대응기능

A 프로세스는 무결성 검사 도중 특정 파일의 해시값이 일치하지 않는 경우에는 해당 파일명을 포함하여 다음과 같이 감사로그를 생성한다.

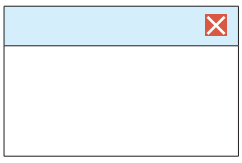
〈 감사로그 화면 출력 〉

.....
.....

또한 무결성 실패시 경고 팝업을 출력하고 제품을 즉시 종료한다.

〈 경고 화면 출력 〉

.....
xxxxx. xxxxxxxx
.....



5 '암호 사용' 기능

(1) 예시에 대한 설명

이 예시는 「서버 공통보안요구사항 V3.0 R1」의 △'8.1.1 요구사항(중요 정보 전송 및 저장시 권고 암호알고리즘 사용)'에 대한 작성의 예시입니다.

〈 작성 예시 〉

1. 암호 사용 기능

1.1 해당되는 국가용 보안요구사항 : 서버 공통보안요구사항 8.1.1

1.2 보안기능 설명

1.2.1 중요 정보 전송시 권고 암호 알고리즘 사용 여부

제품의 구성요소는 국가용 보안요구사항에서 사용을 권고하는 암호알고리즘을 사용하여 데이터를 전송하고 저장한다.

구성요소간 데이터 전송에 사용되는 프로토콜은 TLS v1.3으로 AES256으로 암호화를 수행한다. 사용하는 알고리즘과 사용 목적은 다음 표와 같다.

〈 권고 암호 알고리즘 명세 〉

암호알고리즘	사용 목적	적용된 모듈
ARIA 128 CBC	서버와 에이전트 간 데이터 전송시 기밀성을 보장하기 위해 사용	*검증필 암호모듈 명칭*
AES 128 CBC	서버와 관리자 PC(웹 브라우저) 간 데이터 전송시 기밀성을 보장하기 위해 사용	OpenSSL

부가 설명

❶ 제품이 데이터를 전송할 때 사용하는 암호 또는 해시 알고리즘을 기재합니다. 이때 암호 알고리즘에 대해서는 암호 알고리즘 명칭, 키 길이, 운영모드를 포함하여 기재하고 해시 알고리즘에 대해서는 해시 알고리즘 명칭, 길이를 포함하여 기재합니다.

❷ 제품이 통신하는 모든 경로를 기재합니다. 예로써 제품 구성요소(서버 및 에이전트)간 통신, 제품과 외부 IT 실체 간 통신 등이 있습니다.

❸ 해당 알고리즘을 사용하는 목적과 암호 또는 해시 알고리즘의 제공 주체를 기재합니다.

예를 들어 OpenSSL, OpenJDK, *검증필 암호모듈(명칭 기재)* 등이 있습니다.

〈 작성 예시 〉

1.2.2 중요 정보 저장 시 권고 암호 알고리즘 사용 여부

제품의 중요 정보는 제품의 OS인 Windows Server 2022의 레지스트리에 암호화되어 저장된다.

〈 작성 예시 〉

이중에서 데이터는 ARIA256-CBC-OOOOO 알고리즘으로 저장된다.

저장되는 데이터 위치 및 사용되는 암호 알고리즘은 다음의 표와 같다.

암호알고리즘	제품 구성요소	보호 대상 데이터	보호대상 데이터 저장위치	제품 주체
AES 128 CBC	에이전트	DEK	C:₩Program Files₩TEST₩dek.conf 설정 파일 내 'dek' 변수	OpenSSL
AES 128 CBC	서버	보안정책 설정값	/home/test/test.conf 파일	*검증필 암호모듈 명칭*

부가 설명

❶ 제품이 데이터를 저장할 때 사용하는 암호화 또는 해시 알고리즘을 기재합니다. 이때 암호 알고리즘에 대해서는 암호 알고리즘 명칭, 키 길이, 운영모드를 포함하여 기재하고 해시 알고리즘에 대해서는 해시 알고리즘 명칭, 길이를 포함하여 기재해야 합니다.

❷ 제품이 보호를 위해 암호화 또는 해시하여 저장하는 데이터(보호 대상 데이터)를 기재합니다. 예로써 관리자 · 사용자 패스워드, DBMS 패스워드, 설정값, 암호키(DEK), 중요 파일 등이 있습니다.

❸ 해당 알고리즘을 사용하는 목적과 암호 또는 해시 알고리즘의 제공 주체를 기재합니다. 예로써 OpenSSL, OpenJDK, *검증필 암호모듈(명칭 기재)* 등이 있습니다.

끝.

여 백

[별 지]

자주 묻는 질문

Q1 **보안기능 구현명세서**는 보안기능 확인서를 발급받기 위해 반드시 필요한 문서입니까?

답변 그렇습니다. 보안기능 구현명세서는 보안기능 시험 신청시 제출해야할 5종 문서(①제품 설명서, ②보안기능 구현명세서 ③보안기능 운용 설명서 ④시험 결과서 ⑤취약점 개선 내역서)중의 하나로써 반드시 제출해야 합니다.
다만, CC인증 수용발급의 경우에는 제출을 생략합니다.

Q2 작성 예시에는 서버 공통보안요구사항만을 인용하고 있습니다. 다른 제품 유형(예 : 안티바이러스제품)의 보안요구사항을 인용하면 안되나요?

답변 인용이 가능합니다. 서버 공통보안요구사항뿐 아니라, 다른 제품유형의 보안요구사항도 무제한으로 인용, 조합이 가능합니다.

Q3 신청 제품이 서버-에이전트 구조가 아닌 단독 구조로 구현되었습니다. 권장 목차대로 서버와 에이전트의 보안기능을 모두 기재해야 합니까?

답변 그렇지 않습니다. 권장 목차와 제품의 구성이 다르다면 당연히 제품의 구성에 맞게 권장 목차의 내용을 선별적으로 기재할 수 있습니다.

Q4 신청 제품의 보안기능과 관계없는 비 보안기능도 작성해야 합니까?

답변 그렇지 않습니다. 비 보안기능은 작성 대상에서 제외됩니다.

Q5 저희 회사는 신청 제품에 이때까지 존재하지 않았던 신기술로 국가용 보안요구사항에 없는 새로운 보안기능을 구현하였습니다.
작성 예시처럼 해당되는 국가용 보안요구사항을 찾을 수 없어 보안요구사항 번호를 입력할 수 없습니다.

답변 국가용 보안요구사항 전체(공통 및 제품별 보안요구사항)에서 찾을 수 없는 새로운 기능의 경우 해당되는 보안요구사항을 '없음'으로 기재하십시오.

Q6 Q5에 따라서, 보안요구사항을 '없음'으로 기재하면 보안기능의 내용도 기술하지 않아도 됩니까?

답변 그렇지 않습니다. 해당되는 보안요구사항의 번호를 기재하지 않아도 된다는 의미입니다. 보안기능의 내용은 기술해야 합니다.

Q7 보안기능 구현명세서를 다른 문서로 대체할 수 있습니까?

답변 대체할 수 없습니다.

여 백