|  |  |  |
| --- | --- | --- |
| **KSKSKSKS**  **KSKSKSK**  **KSKSKS**  **KSKSK**  **KSKS**  **KSK**  **KS** | |  |
|  | :2016 | |
| **방 송 통 신 표 준 심 의 회**  **2016년 12월 30일 제정** | | |

표준열람 : 국립전파연구원(http://www.rra.go.kr)

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

제 정 자：방송통신표준심의회 위원장 담당부처：미래창조과학부 국립전파연구원

제 정：2016년 12월 30일

심 의：방송통신표준심의회 정보보호 기술심의회(X)

원안작성협력：국가보안기술연구소

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

이 표준에 대한 의견 또는 질문은 국립전파연구원 웹사이트를 이용하여 주십시오.

이 표준은 방송통신표준화지침 제18조의 규정에 따라 매 5년마다 방송통신표준심의회에서 심의되어 확인, 개정 또는 폐지됩니다.

**심 의 :정보보호 기술심의회(X)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 성명 |  | 근 무 처 |  | 직위 |  |
| (회 장) |  | 염흥열 |  | 순천향대학교 |  | 교수 |  |
| (위 원) |  | 권대성 |  | 국가보안기술연구소 |  | 실장 |  |
|  |  | 김재성 |  | 한국인터넷진흥원 |  | 수석연구원 |  |
|  |  | 나재훈 |  | 한국전자통신연구원 |  | 전문위원 |  |
|  |  | 이창훈 |  | 서울과학기술대학교 |  | 교수 |  |
|  |  | 전명근 |  | 충북대학교 |  | 교수 |  |
|  |  | 진승헌 |  | 한국전자통신연구원 |  | 실장 |  |
| (간 사) |  | 오학태 |  | 미래창조과학부 국립전파연구원 |  | 과장 |  |

**원안작성협력 : 국가보안기술연구소**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 성명 |  | 근 무 처 |  | 직위 |  |
| (연구책임자) |  | 나학연 |  | 국가보안기술연구소 |  | 사무국장 |  |
| (참여연구원) |  | 김종홍 |  | 국가보안기술연구소 |  | 선임연구원 |  |
|  |  | 김일곤 |  | 국가보안기술연구소 |  | 책임연구원 |  |
|  |  | 이은경 |  | 국가보안기술연구소 |  | 선임연구원 |  |
|  |  | 안준호 |  | 국가보안기술연구소 |  | 선임연구원 |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

목 차

[머 리 말 ii](#_Toc468256446)

[개 요 iii](#_Toc468256447)

[1 적용범위 1](#_Toc468256448)

[2 인용표준 1](#_Toc468256449)

[3 용어와 정의 및 약어 1](#_Toc468256450)

[3.1 용어와 정의 1](#_Toc468256451)

[3.2 약어 3](#_Toc468256452)

[4 운영 환경 3](#_Toc468256453)

[5 보안기능 요구사항 3](#_Toc468256454)

[5.1 개인 정보 검출 및 정보 흐름 통제 3](#_Toc468256455)

[5.2 에이전트 보호 4](#_Toc468256456)

[5.3 에이전트와 서버 간 안전한 연동 5](#_Toc468256457)

[5.4 관리자 식별 및 인증 6](#_Toc468256458)

[5.5 안전한 세션 관리 6](#_Toc468256459)

[5.6 전송 데이터 보호 6](#_Toc468256460)

[5.7 보안관리 7](#_Toc468256461)

[5.8 감사 기록 7](#_Toc468256462)

[5.9 자체 시험 8](#_Toc468256463)

[KS X 3255:2016 해 설 9](#_Toc468256464)

머 리 말

이 표준은 방송통신발전기본법 관련 규정에 따라 한국정보통신기술협회의 TTAK.KO-12.0288를 방송통신표준심의회의 심의를 거쳐 제정한 방송통신표준이다.

이 표준의 목적은 컴퓨터 개인 정보 보호 제품의 개발ㆍ시험ㆍ도입ㆍ운용 시 참조하기 위한 보안 요구사항을 규정한다.

이 표준은 저작권법의 보호 대상이 되는 저작물이다.

이 표준의 일부가 기술적 성질을 가진 특허권, 출원공개 이후의 특허출원, 실용신안권 또는 출원공개 후의 실용신안등록출원에 저촉될 가능성이 있다는 것에 주의를 환기한다. 관계 중앙행정기관의 장과 산업표준심의회는 이러한 기술적 성질을 가진 특허권, 출원공개 이후의 특허출원, 실용신안권 또는 출원공개 후의 실용신안등록출원에 관계되는 확인에 대하여 책임을 지지 않는다.

개 요

이 표준은 컴퓨터 개인 정보 보호 제품의 보안 수준 제시를 위한 요구사항을 규정함으로써 제품에 대한 상호 운용성을 높이고, 정보 보호 업체에 보안성이 강화된 제품 개발을 유도하며, 도입기관은 이 표준을 통해 컴퓨터 개인 정보 보호 제품의 시험ㆍ도입ㆍ운용에 참고하기 위한 목적으로 사용된다. 보안기능 요구사항을 규정한 이 표준을 참조하여 개발된 제품의 평가 시 적용할 보증요구사항은 특정 평가보증등급에 한정되지 않는다.

**방송통신표준**

**:2016**

|  |
| --- |
|  |

|  |
| --- |
|  |

# 적용범위

이 표준은 컴퓨터 개인 정보 보호 제품에 대해 다음의 내용을 기술한다.

— 컴퓨터 개인 정보 보호 제품 운영 환경 설명

— 컴퓨터 개인 정보 보호 제품 보안 요구사항: 개인 정보 검출 및 보호, 에이전트 보호, 에이전트와 서버 간 안전한 연동, 감사 기록, 관리자 식별 및 인증, 보안 관리, 전송 데이터 보호, 자체 시험, 안전한 세션 관리

# 인용표준

해당 사항 없음.

# 용어와 정의 및 약어

## 용어와 정의

이 표준의 목적을 위하여 다음의 용어와 정의를 적용한다.

**개인 정보**

살아있는 개인에 관한 정보로서 이를 통해 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)

**개인 정보 검출**

전자파일, 디렉터리, 레지스트리, 프로세스 등에 기록된 내용을 검사하여 개인 정보 포함 여부를 확인하는 행위

**개인 정보 검출 대상 전자파일 내용**

일반적으로 사용자가 기록하는 본문 내용뿐 아니라 파일 머리부(header) 정보 등 파일을 구성하는 모든 데이터의 내용

**파일 속성**

전자파일의 파일 포맷(예: hwp, doc 등)을 결정하는 속성으로, 파일 속성 정보는 일반적으로 전자파일 머리부(header)의 속성 스트림 필드에 기록되어 있으며, 속성 스트림 시그니처, Class ID(파일 형태별 고유값), Section Format ID 등을 기반으로 파일 포맷을 결정함.

**문서 요약 정보**

전자파일의 파일 속성 정보에 포함된 파일 정보(제목, 주제, 지은이, 날짜 등)로 해당 목록은 파일 포맷별로 상이할 수 있음.

**관리 서버**

개인 정보 검출 정책, 에이전트 관리 등과 같은 보안 정책 관리기능을 수행하는 컴퓨터 개인 정보 보호 제품의 구성 요소

**에이전트**

컴퓨터에 저장된 개인 정보를 검출하여 암ㆍ복호화, 완전삭제 등의 보안 기능을 수행하는 컴퓨터 개인 정보 보호 제품의 구성 요소

**컴퓨터**

컴퓨터 개인 정보 보호 제품의 에이전트가 설치된 단말로서, 개인 정보를 저장 또는 처리하는 개인용 컴퓨터(personal computers)와 서버 컴퓨터(server computers)를 총칭함.

**인증정보**

아이디, 패스워드, 쿠키, 세션 정보 등 인증을 위해 사용되는 모든 정보

**감사**(audit)

정보 보호 제품의 운용 시 발생하는 사건에 대해 감시하는 작업. 해당 사건에 대해 제품에 설정된 정책의 위반 여부를 확인

**감사 증적**(audit trail)

감사의 결과의 기록. 기록에 대한 모든 처리행위를 추적하여 그것이 정책을 준수하여 이루어졌음을 확인할 수 있는 정보

**TOE**(target of evaluation)

가능한 설명서가 함께 제공되는 소프트웨어, 펌웨어 및/또는 하드웨어의 집합. 이 표준에서 TOE는 컴퓨터 개인 정보 보호 제품을 가리킴.

**인가된 관리자**

식별과 인증을 성공적으로 완료한 실체로서, 인가된 관리자는 읽기 권한만을 지닌 관리자를 포함하여 모든 등급 또는 종류의 관리자를 뜻함. 인가된 관리자는 다양한 등급 또는 종류의 관리자를 포함할 수 있음. 특히 **5.4**의 관리자는 식별 및 인증을 성공적으로 완료하기 전의 관리자를 가리킴.

## 약어

ID Identification

IP Internet Protocol

MAC Media Access Control

OS Operating System

TOE Target of Evaluation

# 운영 환경

컴퓨터 개인 정보 보호 제품은 그림 1과 같이 관리 서버와 에이전트로 구성된다. 이때 관리 서버는 에이전트에 보안 정책과 개인 정보 검사 명령을 전송하고, 에이전트는 개인용 컴퓨터와 서버 컴퓨터 등의 컴퓨터에 설치되어 해당 컴퓨터에 존재하는 개인 정보를 검출하고, 검출된 개인정보에 대한 대응행동(개인 정보 암ㆍ복호화와 완전 삭제 등)을 수행하여 그 결과를 관리 서버로 전송한다.

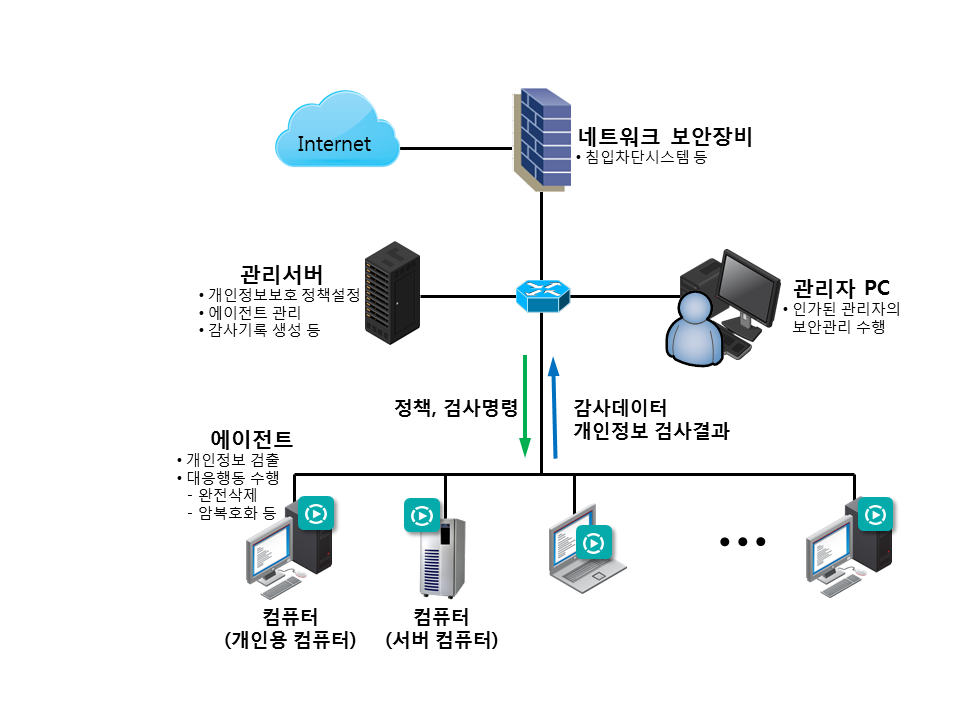


그림 1 — 컴퓨터 개인 정보 보호 제품 운영 환경

# 보안기능 요구사항

컴퓨터 개인 정보 보호 제품에 구현될 수 있는 보안기능 요구사항은 다음과 같다.

## 개인 정보 검출 및 정보 흐름 통제

### a) 컴퓨터에 평문으로 저장된 개인 정보를 검출해야 한다.

— 적용 시 주의 사항: 개인 정보 검출 대상 객체(전자파일, 디렉터리, 레지스트리, 프로세스 등)는 제품에서 선택 가능하며, 파일 포맷 및 유형의 예시는 표 1과 같다.

— 적용 시 주의 사항: 개인 정보 검출 대상 객체가 전자파일인 경우, 확장자명 및 파일 속성 기반으로 개인 정보 검출 대상 포맷을 식별해야 하고, 파일명 및 문서 요약 정보에 포함된 개인 정보도 검출해야 한다.

표 1 — 파일 포맷 및 파일 유형의 예시

|  |  |  |  |
| --- | --- | --- | --- |
| **개인 정보 검출 대상 파일 포맷** | | | **개인 정보 유형** |
| **구분** | **포맷** | **버전** |
| 한컴오피스 | hwp, hwt, show, hsdt, hpt, cell | 97－2014 | 주민등록번호,  여권번호,  운전면허번호,  외국인등록번호,  계좌번호,  신용카드번호 |
| MS Office | doc, xls, ppt, docx, dot, dotx, xlsx | 1.0－2014 |
| Open Office | odt, ods, odp, ott, otp, ots, sxw | 1.1－3.0 |
| 핸디소프트 | hwx, hwn | － |
| Acrobat | pdf | 1.0－10.0 |
| 텍스트/Web | txt, xml, rtf, dat, chm, htm, html, mht | － |
| 압축파일 | zip, tar, tgz, gz, gzip, 7z, iso | － |

### b) 인가된 관리자에 의한 개인 정보 검출(강제 검출) 기능을 제공해야 한다.

— 적용 시 주의 사항: 강제 검출 수행 중 에이전트는 기능을 중단시킬 수 없어야 한다.

— 적용 시 주의 사항: 개인 정보 검출 대상 객체가 전자파일인 경우, 에이전트가 설치된 컴퓨터에 연결된 모든 저장매체에 저장된 전자파일(에이전트에서 검출 제외 대상으로 설정한 저장매체ㆍ폴더 내 전자파일, 휴지통 내 전자파일, 다중 압축 전자파일, 숨김 전자파일 등 포함)에서 개인 정보 검출이 가능해야 한다.

### c) 개인 정보가 포함된 객체가 생성ㆍ저장ㆍ복사ㆍ이동하는 경우, 개인 정보를 검출하는 개인 정보 검출(실시간 검출) 기능을 제공해야 한다.

— 적용 시 주의 사항: 인가된 관리자에 의해 실시간 검출 기능의 활성화ㆍ비활성화가 가능한 제품의 경우, 인가된 관리자에 의해 활성화된 개인정보 검출기능은 에이전트에 의해 비활성화 될 수 없어야 한다.

— 적용 시 주의 사항: 개인 정보 검출 대상 객체가 전자파일일 경우, 에이전트가 설치된 컴퓨터에 연결된 모든 저장매체에 저장된 전자파일(에이전트에서 검출 제외 대상으로 설정한 저장매체ㆍ폴더 내 전자파일, 휴지통 내 전자파일, 다중 압축 전자파일, 숨김 전자파일 등 포함)에서 개인 정보 검출이 가능해야 한다.

### d) 사용자에 의한 개인 정보 검출(사용자 검출) 기능을 제공해야 한다.

### e) 인가된 관리자 또는 사용자에 의한 개인 정보 암ㆍ복호화 기능을 제공해야 한다.

— 적용 시 주의 사항: 개인 정보가 포함된 객체를 암호화하는 경우, 원본은 타이틀을 포함하여 복구 불가능하도록 완전 삭제해야 한다.

— 적용 시 주의 사항: 암호 모듈 검증 제도에서 검증 대상으로 지정된 안전한 암호 알고리즘의 사용을 권고한다.

### f) 제품은 인가된 사용자에 의해 개인 정보를 복구 불가능하도록 완전 삭제하는 기능을 제공해야 한다.

— 적용 시 주의 사항: 개인 정보가 포함된 객체를 완전 삭제하는 경우, 타이틀도 복구 불가능하도록 삭제해야 한다.

— 적용 시 주의 사항: 검출된 개인정보에 대한 대응 기능으로 마스킹 기능을 제공할 수 있다.

## 에이전트 보호

### a) 기밀성 확보

— 부득이하게 사용자 패스워드, 제품 운영과 관련된 암호 키 등을 파일시스템 또는 레지스트리에 저장 시, 암호화 하여 저장해야 한다.

• 적용 시 주의 사항: 불가피한 경우, 패스워드는 암호화 대신 해시화 할 수 있다.

• 적용 시 주의 사항: 암호 모듈 검증 제도에서 검증 대상으로 지정된 안전한 암호 알고리즘의 사용을 권고한다.

• 적용 시 주의 사항: 본 요구사항 수행 시 사용된 암호 키(사용자 패스워드, 제품 운영과 관련된 암호 키 등을 파일시스템 또는 레지스트리에 암호화하여 저장할 때 사용되는 암호 키)는 삭제, 파일 숨김 및 접근통제 등을 통해 안전하게 보호되어야 한다.

— 제품의 설정값, 감사 데이터 등을 파일시스템 또는 레지스트리에 저장 시, 평문으로 저장하지 않도록 암호화 등을 적용해야 한다.

• 적용 시 주의 사항: 자체구현한 인코딩 기법 적용 시, 취약점 점검 등을 통해 안전하게 사용해야 한다.

### b) 무결성 확보

— 제품 동작 초기화 단계(서브시스템 로드)에서 제품의 설정값(정책, 환경), 실행파일, 필터 드라이버 등에 대해 무결성을 점검해야 한다.

• 적용 시 주의 사항: 운영체제의 안전모드상에서 무결성 훼손이 발생할 경우, 이후 운영체제가 정상 부팅 시 해당 변조를 탐지해야 한다.

— 주기적으로 또는 인가된 관리자 요구 시, 무결성을 검증하여 관리자에게 실시간으로 통보하는 기능을 제공해야 한다.

• 적용 시 주의 사항: 변경이 매우 빈번한 정보(예: 감사 데이터)의 경우 무결성 검사 대상에서 제외할 수 있다.

### c) 가용성 확보

— 운영체제 부팅 후 자동 실행되어야 하고, 실행과 동시에 모든 보안 기능이 활성화되어야 한다.

— 변조된 정보(설정값, 실행 파일, 필터 드라이버 등)에 대한 자동 복구 기능을 제공해야 한다.

— 제품의 실행파일(프로세스)이 비정상적으로 임의 종료될 경우 재실행하는 기능을 제공해야 한다.

## 에이전트와 서버 간 안전한 연동

### a) 에이전트는 서버로부터 전송되는 파일에 대한 부인 방지 및 무결성 보장을 위해 파일 생성 주체에 대한 전자서명 검증을 수행해야 한다.

— 적용 시 주의 사항: 제조사 또는 관리자(관리자가 업데이트 파일에 대해 전자서명 할 경우)는 인터넷과 연결이 차단된 별도의 오프라인 서버에서 전자서명을 수행해야 한다.

— 적용 시 주의 사항: 전자서명 검증 시 인증서 유효성도 검증해야 하며, 온라인 검증이 불가한 경우 인증서의 오프라인 배포 등 대체 통제를 마련해야 한다.

— 적용 시 주의 사항: 인증서 유효기간은 1년 이내로 설정해야 하며, 키 길이, 해시 알고리즘 등은 국가 공인인증서 암호 체계 요구사항을 준수해야 한다.

### b) 에이전트는 서버 주소에 대한 무결성 검증을 수행해야 한다.

— 적용 시 주의 사항: 파일 전송 경로상에 두 대 이상의 서버가 존재하는 경우, 수신 서버는 송신 서버의 주소에 대한 무결성 검증을 수행해야 한다.

— 적용 시 주의 사항: 서버가 계층화 또는 복수화되어 있거나 서버와 정책 서버로 분리되어 있는 경우, 전송 경로에 있는 모든 구성 요소에 적용해야 한다.

### c) 서버와 에이전트는 신원을 검증하기 위해 상호 인증을 수행해야 한다.

— 적용 시 주의 사항: 본 요구사항은 IP 및 MAC 스푸핑 공격에 대응할 수 있어야 한다.

— 적용 시 주의 사항: 상호 인증을 지원하기 위한 방식에는 제한이 없으며, 안전성이 보장되는 수준에서 인증서 기반, 요청 및 응답 메커니즘 기반 등 다양한 방식 중 선택적으로 구현할 수 있다.

— 적용 시 주의 사항: 서버와 에이전트 간 안전한 연동을 위해, 연동 과정에서 안전한 암호 알고리즘을 사용해야 하며, 고정된 암호 키 방식(예: 암호 키를 소스코드에 고정하여 사용)을 사용하지 않아야 한다. 또한 서버로부터 에이전트가 수신하는 명령어에 대한 필터링 기능을 통해 비인가된 명령어가 에이전트에서 실행되지 않도록 해야 한다.

## 관리자 식별 및 인증

### a) 관리자의 신원을 검증하기 위해 식별 및 인증 기능을 제공해야 한다.

### b) 관리자 인증 실패가 설정된 횟수(기본값 5회 이하)에 도달하면, 인가된 관리자가 설정한 시간(기본값 5분 이상) 동안 식별 및 인증 기능이 비활성화 되어야 한다.

### c) 패스워드 등록 시 보안성 기준(영문자/숫자/특수문자 중 3가지 이상의 규칙 조합 및 9자리 이상으로 구성)을 만족하는지 검증해야 한다.

### d) 인증이 진행되는 동안 관리자에게 패스워드가 마스킹(예: “\*\*\*\*” 등)되어 보이도록 해야 한다.

### e) 식별 및 인증 실패 시, 실패 이유에 대한 피드백(예: ID 오류, 패스워드 오류 등)을 제공하지 않아야 한다.

### f) 관리자가 제품에 최초 접속 시 제품이 기본적(예: 설치 시 등)으로 제공하는 ID 및 패스워드의 변경을 강제화하는 기능을 제공해야 한다.

### g) 관리자의 패스워드가 제품에 하드코딩되거나 평문(단순 인코딩 포함)으로 저장되지 않아야 한다.

### h) 관리자 또는 사용자(사용자 인증에 대한 식별 및 인증 기능 구현 시)의 인증정보가 재사용되는 것을 방지(예: 타임스탬프 사용 등)해야 한다.

## 안전한 세션 관리

### a) 로그인 이후 일정 시간(기본값 10분 이하) 동안 동작이 없을 경우, 세션 잠금 또는 세션 종료 기능을 수행해야 한다.

### b) 로그인 이후 다른 단말에서 동일 계정 또는 동일 권한으로 로그인을 다시 수행하는 경우, 신규 접속을 차단하거나 이전 접속을 종료해야 한다.

— 적용 시 주의 사항: 제품 운영상황 등에 대한 모니터링만 수행하는 관리자 계정에 대해서는 중복 로그인을 허용할 수 있다.

— 적용 시 주의 사항: ‘동일 권한’으로 로그인 한 경우라도, 정책이 충돌하지 않음을 입증하면 중복 로그인을 허용할 수 있다.

## 전송 데이터 보호

### a) 물리적으로 분리된 제품 구성 요소 간 전송 데이터(보안 정책, 제어 명령, 감사 데이터 등)에 대한 암호화를 통해 기밀성 및 무결성을 보장해야 한다.

— 적용 시 주의 사항: 암호 모듈 검증 제도에서 검증 대상으로 지정된 안전한 암호 알고리즘의 사용을 권고한다.

— 적용 시 주의 사항: 본 요구사항을 제품의 보안 기능으로 완전히 구현할 수 없는 경우, 운영 환경의 지원을 받을 수 있다.

### b) 관리자의 웹 브라우저를 이용한 접속 등 제품과 연결된 모든 통신 수단은 안전한 암호 통신 프로토콜을 사용해야 한다.

— 적용 시 주의 사항: 본 요구사항을 제품의 보안 기능으로 완전히 구현할 수 없는 경우, 운영 환경의 지원을 받을 수 있다.

## 보안관리

### a) 인가된 관리자가 보안 기능, 보안 정책 및 중요 데이터 등을 설정 및 관리할 수 있는 보안 관리 기능을 제공해야 한다.

### b) 사전 등록된 IP 주소의 관리 콘솔만 제품에 접속할 수 있도록 해야 한다.

— 적용 시 주의 사항: 관리자 IP 주소 개수의 기본 값은 2개 이하로 설정되어야 하고, 관리자의 설정에 따라 변경 가능(2개 초과 가능)하다.

— 적용 시 주의 사항: IP 주소 기본 값 2개 이하 제한은 관리자 ID별 2개 이하가 아니라 정책 설정 권한이 있는 모든 관리자가 TOE에 접근할 수 있는 전체 IP 개수의 기본 값이 2개 이하임을 의미한다.

— 적용 시 주의 사항: 모니터링 등의 읽기 권한만을 갖는 관리자에 대해서는 예외적으로 TOE에 접속 가능한 관리자 IP 주소를 지정할 수 있다. 단, 192.168.10.2∼253 등과 같이 IP 주소 범위를 지정하여 추가하는 방식은 허용하지 않으며, 개별적으로 IP 주소를 1개씩 추가하도록 구현해야 한다. 또한 IP 주소 지정 시 네트워크 전체 범위를 의미하는 0.0.0.0, 192.168.10.\*, any 등에 대한 설정은 허용하지 않는다.

## 감사 기록

### a) 감사 기능의 시작/종료, 관리자에 대한 식별 및 인증 성공/실패, 제품 설정 변경 내역, 보안 기능 수행 내역 등에 대한 감사 데이터를 생성해야 한다.

— 적용 시 주의 사항: 허용 및 차단한 모든 트래픽에 대해 감사 데이터를 생성할 수 있는 기능을 제공해야 한다.

— 적용 시 주의 사항: 비밀번호 설정 등으로 개인 정보 검출이 불가능한 파일에 대한 감사 데이터를 생성해야 하며, 개인 정보는 저장은 금지한다.

— 적용 시 주의 사항: 감사 데이터 저장 시, 파일명에 개인 정보가 포함되어 있을 경우, 개인 정보를 마스킹(예: “\*\*\*\*”)하는 등 관리자가 개인 정보를 식별할 수 없도록 조치해야 한다.

### b) 감사 데이터는 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원(가능한 경우), 결과(성공/실패)를 상세히 포함해야 한다.

### c) 인가된 관리자가 제품 구성 요소에서 생성된 모든 감사 데이터를 검토할 수 있는 기능을 제공해야 한다.

### d) 인가된 관리자가 정보를 해석하기에 적합하도록 감사 레코드가 생성되어야 하며 AND, OR 등 논리적 관계 기준에 따른 선택적인 검토가 가능해야 한다.

### e) 감사 증적 내 저장된 감사 레코드에 대해 비인가된 삭제 및 변경이 발생하지 않도록 보호해야 한다.

— 적용 시 주의 사항: 인가된 관리자라 할지라도 삭제 및 변경을 할 수 없도록 삭제ㆍ변경 관련 보안기능 인터페이스가 제공되지 않아야 한다.

— 적용 시 주의 사항: 감사 레코드에 대한 보호 대책을 제품의 보안 기능으로 완전히 구현할 수 없는 경우, 운영 환경의 지원을 받을 수 있다.

### f) 감사 증적의 크기가 지정된 한도를 초과할 경우, 사전 정의한 방식에 따라 관리자에게 통보해야 한다.

### g) 감사 증적의 포화 시 적절한 방법(예: 오래된 감사 레코드 덮어쓰기 등)으로 저장 실패에 대응해야 한다.

### h) 주요 사건에 대한 정확한 시간 정보 생성을 위해 신뢰된 OS 등을 이용하여 시간 정보를 생성해야 한다.

### i) 잠재적인 보안 위반을 탐지한 경우, 인가된 관리자가 설정한 대응 행동(예: 경보 메시지 발송 등)을 수행할 수 있어야 한다.

## 자체 시험

### a) 제품의 정확한 운영을 보장하기 위해 시동 시 및 정규 운영 동안 주기적으로 자체 시험을 실행해야 한다.

### b) 인가된 관리자에게 제품의 설정값 및 제품 자체의 무결성을 검증하는 기능을 제공해야 한다.

KS X 3255:2016  
해 설

이 해설은 본체 및 부속서(규정)에 규정한 사항, 부속서(참고)에 기재한 사항 및 이들과 관련된 사항을 설명하는 것으로 표준의 일부는 아니다.

# 1 제정의 취지

이 표준은 컴퓨터 개인 정보 보호 제품에 대한 상호 운용성을 높이고, 정보 보호 업체에 보안성이 강화된 제품 개발을 유도하며, 도입기관은 이 표준을 통해 컴퓨터 개인 정보 보호 제품의 시험ㆍ도입ㆍ운용에 참고할 수 있다.

# 2 주요 제정 내용

이 표준은 개인용 컴퓨터와 서버 컴퓨터 등의 컴퓨터의 개인 정보 보호를 위한 제품에서 제공해야 하는 개인 정보 검출 및 정보 흐름 통제, 전송 데이터 보호, 식별 및 인증, 감사 기록 생성 등의 보안기능 요구사항을 규정한다.

:**2016**

|  |
| --- |
| **KSKSKS**  **KSKSK**  **KSKS**  **KSK**  **KS**  **KSK**  **KSKS**  **KSKSK**  **KSKSKS** |

|  |
| --- |
|  |
| **information protection application** |
| **in computers** |
| **ICS 35.040** |