2023 한국인터넷진흥원 본인확인서비스 교육

본인확인기관 지정정기심사 1장 물리적·기술적·관리적 조치계획

접속정보의 위·변조의 방지에 관한 사항과 본인확인업무와 다른 인터넷서비스 분리에 관한 사항

CONTENTS

CONTENTS

본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

01 개인정보처리시스템의 접속기록 관리 적정성 심사 기준

(1) 심사 대상
(2) 심사 영역
(3) 증적자료
(4) 현장실사
(5) 인터뷰 및 현장점검
(6) 미흡사례

개인정보처리시스템의 접속기록 관리 적정성 심사 기준

심사대상

- 개인정보처리시스템 접속기록 저장·검토 정보시스템
- 개인정보처리시스템 접속기록 검토 결과 및 보고 이력

심사영역

- 본인확인업무 관련 개인정보처리시스템 접속기록을 최소 1년 이상 보관하고 있는지 심사
- 본인확인업무 관련 개인정보처리시스템 접속기록 저장·검토 시 관련 법규 및 내부관리계획 준수 여부를 심사
- 본인확인업무 관련 개인정보처리시스템 접속기록을 주기적으로 검토하고 검토결과를 개인정보관리책임자에게 보고하고 있는지 심사

담당자가 “접속기록”이란 용어를 오해하여 개인정보처리시스템에 접속한 로그(Access Log)만 검토하는 경우가 발생합니다.

개인정보처리시스템의 접속기록 관리 적정성 심사 기준

"접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말하고 있어, 개인정보처리시스템에서의 행위이력을 주기적으로 검토해야 합니다. 최근 개인정보보호법이 개정됨에 따라 개인정보취급자 뿐만 아니라 이용자의 접속기록도 대상으로 추가되었습니다.

	기존	신규추가
대상	개인정보취급자	이용자
보관기간	개인정보취급자의 접속기록 1년 또는 2년 이상	이용자의 접속기록 3개월 이상

개인정보처리시스템의 접속기록 관리 적정성 심사 기준

증적자료

- 내부관리계획서 내에 개인정보처리시스템 접속기록 관리 조항
- 본인확인업무 관련 개인정보처리시스템 자산 목록표
- 본인확인업무 관련 개인정보처리시스템 접속기록 관리현황표
- 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 검토 절차
- 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 검토 결과 및 이상행위 처리 결과

현장실사(증적자료 확인과 담당자 인터뷰, 개인정보처리방침 점검을 통해 진행)

대상 담당자

- 개인정보처리시스템 운영자
- 접속기록 검토자

인터뷰

- 접속기록 수집, 저장, 보관 기간 설명 요청
- 주기적인 검토 절차 설명 요청
- 접속기록 검토 결과 및 이상행위 처리 결과 설명 요청

개인정보처리시스템의 접속기록 관리 적정성 심사 기준

현장점검

- 개인정보처리시스템 접속기록 관리계획 수립 여부
- 개인정보처리시스템 접속기록 관리현황표 작성 여부
- 개인정보처리시스템 접속기록 저장 현황
- 개인정보처리시스템 접속기록 검토 현황

미흡사례

(1) **접속기록 저장 관련** : 개인정보처리시스템 접속기록에서 사용자가 처리한 정보주체를 확인할 수 없거나, 사용자가 수행한 업무를 확인할 수 없는 문제점이 확인된 경우

접속기록 항목 예시

- 계정 : A0001(개인정보취급자 계정)
- 접속일시 : 2019-02-25, 17:00:00
- 접속지 정보 : 192.168.100.1(접속한 자의 IP주소)
- 처리한 정보주체 정보 : CLI06719(정보주체를 특정하여 처리한 경우 정보주체의 식별정보)
- 수행업무 : 회원목록 조회, 수정, 삭제, 다운로드 등

※ 위 정보는 반드시 기록하여야 하며 개인정보처리자의 업무환경에 따라 책임추적성 확보에 필요한 항목은 추가로 기록해야 한다.

개인정보처리시스템의 접속기록 관리 적정성 심사 기준

(2) **접속기록 검토 관련** :

- 개인정보취급자가 검토 담당자로 지정되어 모든 접속기록을 검토하고 있어 직무 분리가 미흡한 경우
- 대체수단 발급 관리자사이트, 본인확인서비스 관리자사이트, 본인확인서비스 이용자상담사이트에서 개인정보 다운로드 사유를 확인하고 있지 않는 경우

다운로드 사유확인이 필요한 기준 책정 예시

- (다운로드 정보주체의 수) 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모 기업에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
- (일정기간 내 다운로드 횟수) 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단기간에 수차례 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
- (업무시간 외 다운로드 수행) 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인

- 로그통합관리시스템에서 시나리오에 따라 접속기록 이상 징후를 탐지하고 있으나, 원인 확인 등 소명 절차를 수행하지 않은 경우

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

접속기록 내 비정상 행위 예시

- 계정 : 접근권한이 부여되지 않은 계정으로 접속한 행위 등
- 접속일시 : 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외에 접속한 행위 등
- 접속지 정보 : 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등
- 처리한 정보주체 정보 : 특정 정보주체에 대하여 과도하게 조회, 다운로드 등의 행위 등
- 수행업무 : 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
- 그 밖에 짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속한 행위 등

(3) DBA, 서비스 운영자 등이 DB서버 OS에서 DB접속명령어로 localhost DB에 접속하여 본인확인서비스 이용 개인정보를 처리한 행위에 대해 검토하지 않은 문제점이 확인된 경우

02 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 여부의 심사 기준

(1) 심사 대상
(2) 심사 영역
(3) 증적자료
(4) 현장실사
(5) 인터뷰 및 현장점검
(6) 미흡사례

개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 여부의 심사 기준

심사대상

- 개인정보처리시스템 접속기록 백업시스템
- 개인정보처리시스템 접속기록 백업본 저장장치
- 개인정보처리시스템 접속기록 백업 이력

심사영역

- 본인확인업무 관련 개인정보처리시스템 접속기록을 별도 저장장치에 백업하고 있는지 심사
- 둘째, 본인확인업무 관련 개인정보처리시스템 접속기록 백업 보관 시 관련 법규 및 내부관리계획을 준수하고 있는지 심사

증적자료

- 내부관리계획서 내에 개인정보처리시스템 접속기록 관리 조항
- 본인확인업무 관련 개인정보처리시스템 자산 목록표
- 본인확인업무 관련 개인정보처리시스템 접속기록 관리현황표
- 본인확인업무 관련 개인정보처리시스템 접속기록 백업 계획 및 이력

개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 여부의 심사 기준

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 개인정보처리시스템 접속기록 백업 담당자
- 개인정보처리시스템 접속기록 백업시스템 운영자 및 백업본 저장장치 담당자

인터뷰

- 접속기록 백업 절차 및 계획 설명
- 접속기록 백업 설정내역, 백업 이력

개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 여부의 심사 기준

현장점검

- 개인정보처리시스템 접속기록 백업 계획 수립 여부
- 개인정보처리시스템 접속기록 관리현황표 작성 여부
- 개인정보처리시스템 접속기록 백업 현황

미흡사례

(1) 개인정보처리시스템 접속기록 백업본을 별도 저장장치에 보관하지 않고 원본과 함께 로컬 정보시스템에 보관하고 있는 문제점이 확인된 경우

(2) 개인정보처리시스템 접속기록 백업본 보관 기간이 관련 법규 및 내부관리계획의 요구사항을 준수하지 못하는 문제점이 확인된 경우

03 본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

(1) 심사 대상
(2) 심사 영역
(3) 증적자료
(4) 현장실사
(5) 인터뷰 및 현장점검
(6) 미흡사례

본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

심사대상

- 대체수단 발급 시 본인확인기관의 다른 인터넷서비스에 대한 회원가입을 요구하지 않는 것
- 본인확인서비스 제공을 위한 시스템 및 개인정보 DB를 물리적 또는 논리적으로 다른 서비스와 분리하여 운영하는 것

심사영역

- 본인확인서비스를 위하여 대체수단 발급 시 본인확인서비스와는 관련 없는 다른 부가 서비스 가입 유도, 가입단계 화면 중 광고 노출 등이 없는 지 심사
- 본인확인서비스 전용 정보시스템 즉, 서버, 미들웨어(WAS, AP서버), DB가 물리적 또는 논리적으로 다른 서비스와는 분리하여 운영하는 지 심사

본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

증적자료

- 자산 목록 중 본인확인서비스 전용 정보시스템 상세 (버전, HA 구성 등)
- 서버 아키텍처 상세자료 : 단일구성, 가상머신, 컨테이너 구성 등
- WEB, AP서버, WAS 서비스 계정 목록, 인스턴스 현황
- 본인확인서비스 DB 엔진 구성, DB 서비스 계정 목록, DB 스키마, ERD 또는 테이블 명세서
- 가상화 적용 시 가상머신별 서비스 용도
- Docker, K8S 구성 시 컨테이너 목록/Node/Pod별 상세 서비스

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

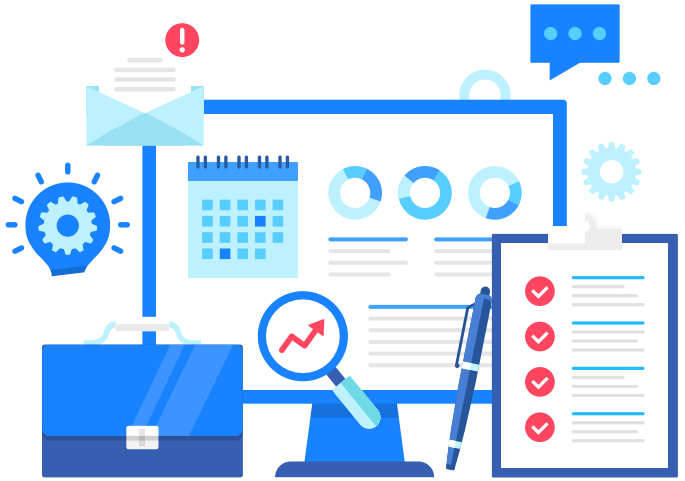
- 인프라 담당자, DBA, DA(데이터 아키텍처), 서버 운영자, WAS 운영자, 가상화 시스템 운영자

본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

인터뷰 및 현장점검

- 본인확인서비스 전용 DB와 공용 DB 차이점 설명
- 본인확인서비스 전용 DB 테이블 목록 및 상세 서비스 설명
- 서버, 미들웨어, DB 상세 아키텍처 설명
- 가상화 시스템 운영 시 가상화 적용 상세 아키텍처 설명
- 서버, DB 계정 및 인스턴스 목록, WAS 계정 및 인스턴스 목록, 본인확인서비스 인터페이스 목록

해당자료 및 설명을 요청하고 담당자 인터뷰 진행 후,
요청 받은 자료와 지침을 근거로 실제 현장점검을 수행합니다.



본인확인업무와 다른 인터넷 서비스와의 분리의 적정성 심사 기준

미흡사례

(1) WAS 서버(또는 AP 서버) 한 대로 WAS 계정만 분리하여 본인확인서비스와 다른 부가서비스를운영하는 경우

(2) 단일 DB에서 공통 DB계정으로 논리적으로 테이블만 분리하여 본인확인서비스 이외의 다른 인터넷 서비스를 제공하는 경우

(3) **가상화 적용 시** : 신규 도입된 본인확인서비스에 가상화(VM)을 적용했는데, 본인확인서비스 전용 DB를 동일 하드웨어에서 VM만으로 분리하는 경우

가상화 시스템은 현재 보안상 DB분리는 VM 분리 즉,
논리적 분리가 아닌 물리적 분리만 인정됩니다.