개인정보의 안전성 확보조치 점검사례 안내서

보건복지부

한국사회보장정보원

우리 기관의 개인정보처리시스템에 보관된 개인정보는 안전할까요?

개인정보보호센터는 2026년도 개인정보보호 컨설팅을 수행하며 자주 확인된 주요 점검사례 12종을 선정하고, 이에 대한 자가진단 요령과 실무 조치 방안을 알기 쉽게 정리하였습니다.

본 안내서가 개인정보보호 담당자분들의 실무에 도움이 되길 바라며, 앞으로도 개인정보보호센터는 각 기관이 안전하고 신뢰받는 개인정보 처리 환경을 조성할 수 있도록 함께 고민하는 든든한 조력자가 되겠습니다.

2026. 8.

목 차

※ 본 안내서에서는「**개인정보의 안전성 확보조치 기준**」을 「**고시**」로 축약하여 표기합니다.

접근 권한의 관리

사례1 **관리자 권한을 아무나 사용하고 있어요.**

① 문제가 뭔가요?

시스템 서버(웹, DB, 리눅스 등)에서 업무 담당자나 외부 유지보수 업체 직원이**root(최고 관리자) 권한이나 DBA(데이터베이스 전체 관리자) 권한**을 가지고 작업하고 있는 경우가 많습니다. 이 권한은 시스템의 모든 **데이터를 조회/수정/삭제**할 수 있는 가장 강력한 권한이기 때문에, 실제 업무에 꼭 필요한 사람에게만 제한적으로 부여해야 합니다.

▶ 쉽게 말하면: 은행 금고의 마스터키를 직원 모두가 돌려쓰는 것과 같습니다. 누가 무슨 일을 했는지 추적도 안 되고, 사고가 나면 책임 소재도 불분명해집니다.

② 왜 위험한가요?

- 고시 제5조 제1항에 따라 시스템 접근권한은 **업무 수행에 필요한 최소한의 범위로 차등 부여**해야 합니다.
- 최고 관리자(root/DBA) 권한이 남용되면 무관한 개인정보까지 열람·유출될 수 있고, 데이터 삭제 등 사고 발생 시 행위자 추적이 불가능합니다.
- **불필요한 관리자 권한 부여는 안전조치의무 위반**에 해당하며, 감사 지적 및 정보 유출 사고 시 중대 과실로 처벌받게 됩니다.

③ 어떻게 확인하나요?

외주 유지보수 업체나 내부 전산 담당자에게 다음 사항을 물어보세요.

확인 항목	확인 방법
서버에 root 권한을 가진 계정이 몇 개인가요?	**서버 담당자에게 확인해 달라고 요청하세요.** **ex. (리눅스 서버): grep '^wheel' /etc/group 명령어 확인 및 /etc/sudoers 파일 내 관리자 권한 계정 확인 요청 (또는 cat /etc/sudoers 파일 확인 요청)**
DB에 DBA 권한을 가진 계정이 몇 개인가요?	**DB 담당자에게 DBA 롤(role)을 부여받은 계정 목록을 뽑아 달라고 하세요.**
외부 유지보수 업체 직원도 root나 DBA 권한을 쓰고 있나요?	**계정 관리 대장이 있다면 함께 확인하고, 없다면 즉시 작성을 요청하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 계정 관리 대장을 만들어 현재 모든 서버·DB 계정과 권한 수준을 기록하세요.
2. 인사이동이나 프로젝트 종료 시 계정을 즉시 삭제/잠금 처리하는 절차를 문서로 만들어 공유하세요.

☑ **외주 업체에 요청할 사항**

"우리 시스템의 모든 서버와 DB에 대해, root 또는 DBA 권한을 사용하는 계정 목록을 제출해 주세요. 그리고 업무에 꼭 필요한 최소 권한만 남기고 불필요한 관리자 권한은 모두 회수해 주세요."

- 리눅스 서버: root 직접 접속을 금지하고, 필요시 sudo로 특정 명령만 허용하도록 변경
- DB 서버: DBA 권한을 회수하고, 업무에 필요한 최소 권한(SELECT, INSERT, UPDATE 등)만 부여
- 작업 완료 후 권한 변경 결과를 문서로 제출받을 것

사례2 **여러 사람이 같은 계정을 공유하고 있어요.**

① 문제가 뭔가요?

내부 직원끼리, 또는 내부 직원과 외부 유지보수 업체 직원이 **하나의 계정을 공유**해서 시스템에 접속하는 경우입니다. 예를 들어 admin이라는 계정 하나를 여러 명이 같이 쓰는 상황입니다.

▶ 쉽게 말하면: 사무실 출입 카드를 여러 명이 돌려쓰는 것과 같습니다. 누가 언제 들어왔는지 전혀 알 수 없습니다.

② 왜 위험한가요?

- 고시 제5조 제4항에 따라 **취급자별 1인 1계정을 발급**해야 하며, **계정 공유는 법적으로 엄격히 금지**됩니다.
- 하나의 계정을 여럿이 쓰면 로그가 남아도 실제 작업자를 특정할 수 없어 **책임추적성이 상실**되고, 내부 유출 사고 시 결백을 소명할 수도 없습니다.
- 계정 공유 행위는 보안 감사 지적 1순위 항목이며, 법 위반에 따른 시정명령 및 과태료 부과 대상이 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
공유 계정이 존재하나요?	**외주 업체에 "현재 사용 중인 모든 계정 목록을 실제 사용자 이름과 함께 제출해 달라"고 요청하세요.**
동시에 여러 사람이 같은 계정으로 접속할 수 있나요?	**리눅스/윈도우 서버에서 동일 계정의 중복 접속이 가능한지 확인 요청하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 계정 공유 금지를 내부 규정에 명시하고, 신규직원/외주 인력 투입 시 필수 교육에 포함하세요.
2. 개인정보처리시스템 사용자 계정은 1인 1계정 발급이 원칙이며 공유를 엄격히 금지하세요. 부득이 시스템 유지보수용 공용 계정(OS 등)을 사용하는 경우에만 **사전 승인 및 작업 대장을 작성**하세요.

☑ **외주 업체에 요청할 사항**

"현재 여러 사람이 공유해서 쓰는 계정이 있다면 모두 찾아서 알려주세요. 각 업무 담당자별로 개인 계정을 새로 발급하고, 공유 계정은 원칙적으로 모두 삭제해 주세요. 부득이하게 삭제가 어렵다면 동시 접속을 차단하고 계정 사용 대장을 작성하도록 조치해 주세요."

- 리눅스: 동일 계정 동시 접속 차단 설정 적용
- 윈도우: 원격 데스크톱 동시 세션 제한 설정 적용

사례3 | **권한을 누가, 언제, 왜 바꿨는지 기록이 없어요.**

① 문제가 뭔가요?

직원의 인사이동(승진, 부서 이동, 퇴사 등)에 따른 시스템 접근권한 변경 시, **시스템에 그 기록이 남아 있지 않거나**, 기록을 남기더라도 **법정 보관 기간인 3년을 채우지 못하는** 경우입니다.

▶ 쉽게 말하면: 누가, 언제, 어떤 근거로 개인정보에 접근할 수 있었는지 추적할 수 없어, 보안 사고나 감사 시 소명할 증빙이 없습니다.

② 왜 위험한가요?

- 고시 제5조 제3항에 따라 권한의 부여·변경·말소 내역은 **최소 3년간 의무적으로 보관**해야 합니다.
- 변경 이력이 없으면 퇴직자나 이동자의 권한이 방치되어 정보 유출 통로가 되며, 보안 감사나 사고 조사 시 정당성을 입증할 수 없습니다.
- 권한 변경 내역 미보관은 법정 의무 위반으로, 정기 점검 지적 및 과태료 처분을 받게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
권한 변경 이력이 기록되고 있나요?	**외주 업체에 "권한을 변경할 때마다 변경자, 변경 일시, 변경 전후 권한을 기록하고 있나요?"라고 물어보세요.**
기록이 3년 이상 보관되고 있나요?	**로그 데이터 보관주기는 3년 이상으로 설정되어 있는지, 스토리지 용량 초과 시 과거 로그가 덮어쓰기 되지 않고 안전하게 백업되고 있는지 확인하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 접근권한 변경 시 **신청 → 승인 → 적용 → 기록**에 이르는 **표준 절차**를 내부관리계획에 명시하세요.
2. **변경 요청 시 포함해야 할 정보**: 신청자, 승인자, 변경 사유, 변경 전/후 권한, 적용 일시
3. 인사 발령 문서와 실제 시스템상 접근권한 내역을 대조하는 주기적 점검(반기별 또는 분기별)을 수행하세요.

☑ **외주 업체에 요청할 사항**

"시스템에서 권한이 변경될 때마다 [신청자(대상자), 승인자, 변경 일시, 변경 전/후 권한, 근거 문서] 항목이 자동으로 기록되도록 개선해 주세요. 이 기록은 최소 3년 이상 보관해야 하므로, 용량 초과로 과거 데이터가 삭제되지 않도록 안전하게 백업 및 분리 보관되도록 설정해 주세요."

- 단일 서버 용량 증설 대신, 주기적인 로그 백업 및 안전한 외부 스토리지 이관 설정
- 애플리케이션에 권한 변경 이력 전용 테이블 신설 또는 감사 로그 기능 추가

접근통제

사례4 **관리자 페이지가 인터넷에 노출되어 있어요.**

① 문제가 뭔가요?

내부 직원만 사용해야 하는 **관리자 페이지, 서버 관리 화면, 데이터베이스 접속 포트가 인터넷 어디에서나 접속할 수 있는 상태**인 경우입니다. 내부 업무망에서만 접근하게 해야 하는데, 외부(인터넷)에서도 접속 주소만 알면 누구나 로그인 화면에 도달할 수 있습니다.

▶ 쉽게 말하면: 사무실 내부 회의실 문이 길거리에 그대로 열려 있는 것과 같습니다. 비밀번호만 뚫으면 내부 자료가 모두 노출됩니다.

② 왜 위험한가요?

- 고시 제6조 제1항·제3항에 따라 **비인가자 접근을 차단하고, 외부 접속 시 VPN 등 안전한 접속수단을 적용**해야 합니다.
- 관리자 페이지가 인터넷에 그대로 노출되거나 불필요한 공인 IP가 할당될 겨우, 해커의 직접적인 표적이 되므로 매우 위험합니다.
- 불필요한 인터넷 노출 및 접근통제 미비는 안전조치의무 위반으로, 점검 시 즉각적인 개선 권고 및 처분 대상이 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
관리자 페이지가 인터넷에서 열리나요?	**외주 업체에 "우리 시스템의 관리자 페이지 URL이 외부(인터넷망)에서도 접속되나요?"라고 물어보세요.**
서버에 공인 IP가 할당되어 있나요?	**내부 운영 서버(DB, WAS 등)의 IP주소 목록을 받아서, 불필요하게 공인 IP가 할당된 장비가 있는지 확인해 달라고 요청하세요.**
DMZ 구간은 분리되어 있나요?	**외부에 노출되어야 하는 서버(WEB)만 DMZ 구간에 있고, DB 등 내부 서버는 사설 IP로 분리되어 있는지 확인하세요.**

④ 어떻게 해결하나요?

☑ 내부 조치 사항

1. 전체 서버 목록과 IP 현황을 파악하세요. (외주 업체에 요청)
2. "인터넷에서 접근할 수 있는 장비 목록"을 따로 관리하고, 불필요한 건은 즉시 조치 지시하세요.

☑ 외주 업체에 요청할 사항

"내부 관리자 페이지만 접속할 수 있는 URL을 정리해서 알려주세요. 이 페이지들이 외부(인터넷)에서 접속되지 않도록 방화벽에서 접근을 차단해 주세요. (특정 사내 IP에서만 접속 허용 설정)"

"또한 내부 운영 장비(DB, 파일 서버 등)에 불필요하게 공인 IP가 할당된 장비가 있는지 전수 조사하고, 모두 사설 IP로 전환해 주세요."

"관리자 페이지는 사내 내부망(사설 IP)에서만 접근 가능하도록 방화벽 화이트리스트 정책을 적용해 주세요. 부득이 외부 원격 접속이 필요한 경우 사전에 인가된 PC에서 SSL-VPN 등을 통해서만 접근할 수 있도록 구성해 주세요."

- 방화벽에 내부 IP 대역에서만 접근 허용하는 화이트리스트 정책 적용
- DMZ 구간 재정비 (WEB 서버만 DMZ, DB/WAS 등은 내부망)

사례5 **비밀번호만으로 로그인하고 있어요. (2차 인증 부재)**

① 문제가 뭔가요?

시스템 로그인 시 **아이디와 비밀번호만으로 접속**하고, 추가적인 인증수단(OTP, 공동인증서, 휴대폰 인증 등)이 적용되어 있지 않은 상태입니다. 특히 **외부에서 접속하는 취급자**나 **관리자 계정**은 반드시 2차 인증이 필요합니다.

▶ 쉽게 말하면: 집 현관문이 비밀번호 하나에만 의존하는 것과 같습니다. 비밀번호가 유출되면 누구나 들어올 수 있습니다.

② 왜 위험한가요?

- 고시 제6조 제3항·제5항에 따라 관리자 및 외부 접속자 로그인 시 **안전한 인증수단(2차 인증)을 의무 적용**해야 합니다.
- 비밀번호만 사용하는 경우 피싱, 악성코드 등으로 계정이 탈취되면 누구든 시스템에 쉽게 침입하여 대규모 개인정보를 유출할 수 있습니다.
- 2차 인증 미적용 상태에서 유출 사고 발생 시, 안전조치의무 미이행으로 막대한 과징금 및 손해배상 책임을 지게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
관리자는 2차 인증을 사용하나요?	**직접 관리자 페이지에 로그인해 보세요. 아이디/비밀번호 외에 추가 인증 단계가 있는지 확인하세요.**
외부(협력 기관, 병원 등) 사용자는 어떻게 인증하나요?	**외부 사용자 로그인 시 OTP, 공동인증서 등이 적용되어 있는지 물어보세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 시스템 사용자 구분: 내부 직원(관리자) / 외부 취급자(협력 기관, 유지보수 등) / 일반 이용자
2. 관리자와 외부 취급자는 **반드시 2차 인증**을 적용한다는 원칙을 수립하세요.

☑ **외주 업체에 요청할 사항**

"관리자 계정과 외부에서 접속하는 모든 사용자 계정에 대해 아이디/비밀번호 외에 추가 인증을 적용해 주세요. 예산이 있다면 OTP(일회용 비밀번호 생성기) 방식을, 제한적이라면 휴대폰 SMS 인증이나 공동인증서 방식을 검토해 주세요."

- 2차 인증수단 예시: OTP 앱/토큰, SMS 인증, 카카오톡 인증, 공동인증서
- 최소한 관리자 계정과 외부 접속 계정부터 우선 적용

사례6 **일정 시간 지나도 자동 로그아웃이 안 돼요.**

① 문제가 뭔가요?

시스템에 로그인한 후 **일정 시간(예: 15분) 동안 아무 작업도 하지 않아도** 자동으로 로그아웃되지 않고 계속 접속 상태가 유지되는 경우입니다. 웹 서버뿐 아니라 서버에 직접 접속하는 터미널(리눅스, 윈도우 원격 접속)에도 해당됩니다.

▶ 쉽게 말하면: 은행 ATM에서 돈을 뽑고 떠났는데, 다음 사람이 내 카드가 그대로 꽂혀 있는 상태에서 계속 거래할 수 있는 상황입니다.

② 왜 위험한가요?

- 고시 제6조 제4항에 따라 일정 시간(해설서 및 복지부 지침 기준 10~15분) 이상 **미사용 시 자동으로 접속을 차단**해야 합니다.
- 자리를 비우거나 공용 PC를 사용한 후 로그아웃하지 않으면, 화면에 노출된 개인정보를 타인이 무단 열람하거나 탈취할 위험이 큽니다.
- 자동 로그아웃(세션 타임아웃) 미설정은 기술적 안전조치 미이행으로 감사 시 주요 지적 사항에 해당합니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
웹 시스템이 자동 로그아웃 되나요?	**직접 시스템에 로그인한 후 15~20분간 아무 작업도 하지 말고, 다시 사용하려 할 때 로그아웃되었는지 확인하세요.**
서버 접속도 타임아웃이 설정되어 있나요?	**외주 업체에 "리눅스/윈도우 서버의 세션 타임아웃이 몇 분으로 설정되어 있나요?"라고 물어보세요.**

④ 어떻게 해결하나요?

☑ 내부 조치 사항

1. 자리 비울 시 화면 잠금(Windows 키 + L) 생활화 교육
2. 시스템 자동 로그아웃 시간을 명시한 내부 보안 정책 수립 (예: 15분)

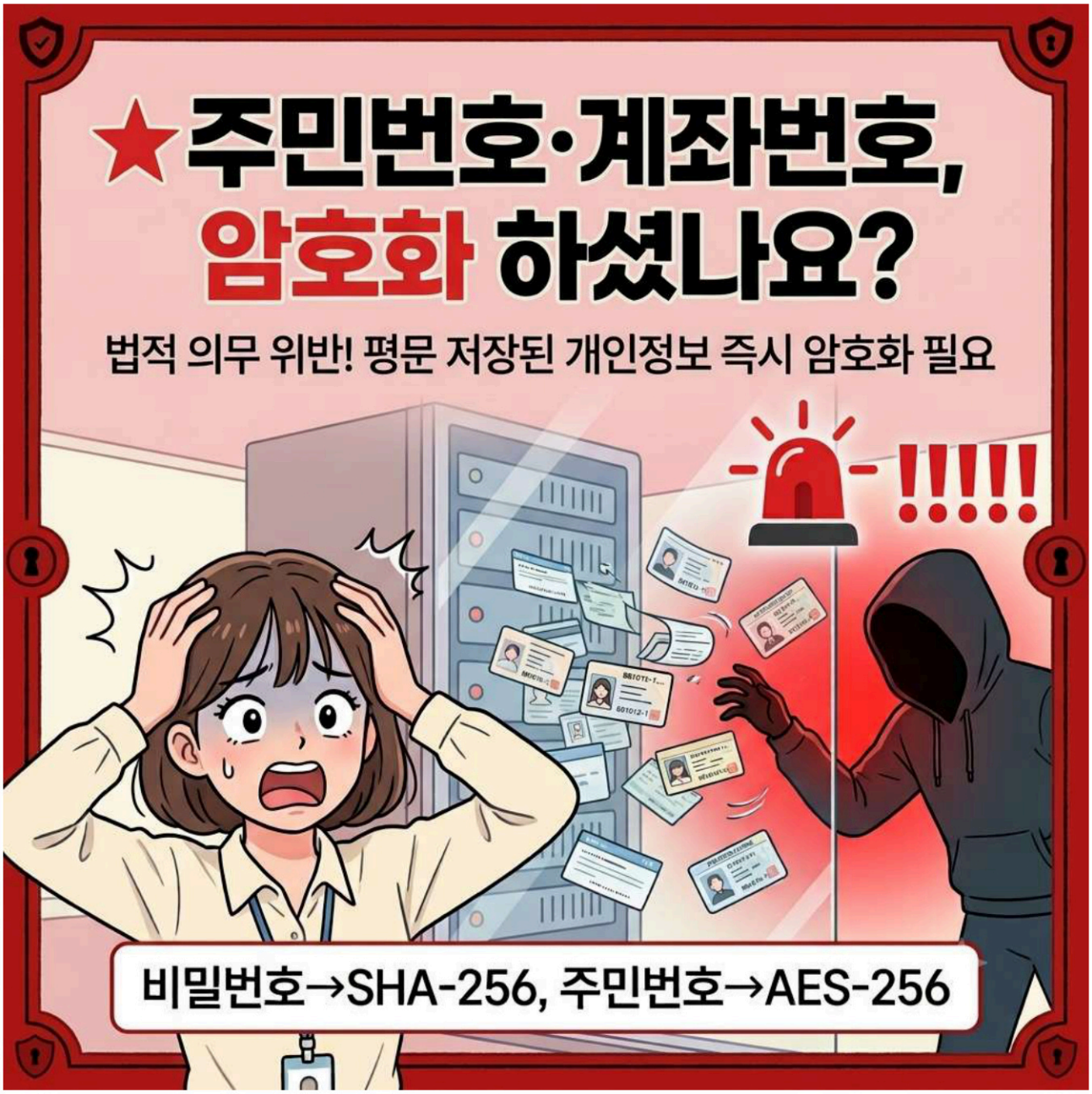
☑ 외주 업체에 요청할 사항

"웹 시스템과 서버 모두 15분 동안 사용하지 않으면 자동으로 로그아웃되도록 설정해 주세요. 설정 후에는 실제로 동작하는지 테스트하고 결과를 알려주세요."

- 웹 서버(WEB/WAS): 세션 타임아웃 15분으로 설정
- 윈도우 서버: 그룹 정책(gpedit.msc)에서 원격 데스크톱 세션 시간제한 15분 설정
- 리눅스 서버: .bash_profile 또는 /etc/profile에 TMOUT=900(15분=900초) 설정

개인정보의 암호화

사례7 **주민번호, 계좌번호가 암호화 없이 저장돼 있어요.**



① 문제가 뭔가요?

주민등록번호, 외국인등록번호, 계좌번호, 비밀번호 등의 중요 정보가 데이터베이스에 **암호화되지 않은 평문(원본 그대로)으로** 저장된 상태입니다. 이는 가장 심각한 수준의 위반 사항입니다.

▶ 쉽게 말하면: 고객의 주민번호와 계좌번호가 적힌 종이를 아무 잠금장치 없는 책상 위에 올려둔 것과 같습니다. DB가 한번 뚫리면 모든 정보가 그대로 노출됩니다.

② 왜 위험한가요?

- 「개인정보 보호법」 제24조의2 및 고시 제7조에 따라 **주민등록번호, 계좌번호, 비밀번호 등은 반드시 암호화하여 저장**해야 합니다.
- DB가 해킹되거나 백업 파일이 유출될 경우, 평문으로 저장된 민감 정보가 그대로 노출되어 2차 범죄와 심각한 피해로 이어집니다.
- 주요 개인정보 평문 저장은 가장 중대한 법 위반으로, 유출 시 전체 매출액(또는 예산) 기준의 과징금 부과 및 형사처벌 대상이 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
주민등록번호가 암호화되어 저장되어 있나요?	**외주 업체에 "데이터베이스에서 주민등록번호 컬럼을 직접 조회했을 때 원본 번호가 보이나요?"라고 물어보세요. 원본이 보이면 암호화되지 않은 것입니다.**
비밀번호도 암호화되어 있나요?	**마찬가지로 DB의 비밀번호 칼럼이 암호화되어 저장되고 있는지 확인 요청하세요.**
암호화되지 않은 개인정보가 또 있나요?	**DB 전체 테이블을 대상으로 개인정보(이름+주민번호+연락처 등)가 평문으로 저장된 곳이 없는지 전수 점검을 요청하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 이 문제는 **즉시 조치가 필요**한 최우선 과제입니다. 지체하지 말고 외주 업체에 조치를 요청하세요.
2. 암호화 대상 개인정보 목록을 파악하세요: 주민등록번호, 외국인등록번호, 계좌번호, 비밀번호, 여권번호, 운전면허번호 등

☑ **외주 업체에 요청할 사항**

"(긴급) 데이터베이스에 평문으로 저장된 주민등록번호, 계좌번호, 비밀번호를 전수 조사해 목록을 제출해 주세요. 그리고 해당 데이터들을 즉시 암호화해 주세요. 암호화 방식은 다음과 같이 적용해 주세요."

- 비밀번호 류: **복호화가 불가능한 일방향 암호화** (SHA-256 + Salt 권장)
- 주민등록번호/계좌번호 류: 업무상 복호화가 필요하면 **안전한 양방향 암호화** (AES-256 권장)
- 암호화 완료 후 평문 데이터 영역은 안전하게 삭제(복구 불가 방식)

사례8 **오래된 암호화 방식을 사용하고 있어요.**

① 문제가 뭔가요?

비밀번호나 개인정보를 암호화할 때 MD5, DES 같은 오래된 알고리즘을 사용하는 경우입니다. 이 알고리즘들은 이미 보안 취약점이 발견되어 **현재는 사용하지 말아야 할 방식**입니다.

▶ 쉽게 말하면: 녹슨 자물쇠로 문을 잠그는 것과 같습니다. 겉으로는 잠겨 있어 보이지만, 전문가 도구로 쉽게 열 수 있습니다.

② 왜 위험한가요?

- 고시 제7조 및 관련 가이드에 따라 **안전성이 검증된 알고리즘(SHA-256 이상, AES-256 등)을 사용**해야 합니다.
- 취약한 구형 알고리즘(MD5, DES 등)은 이미 해독 기술이 공개되어 암호화하지 않은 것과 같으며, 단시간 내에 평문이 복원될 수 있습니다.
- **취약 알고리즘 사용은 법령상 적법한 암호화 조치로 인정받지 못하므로**, 보안 점검 시 필수 교체 지적 및 개선 처분을 받게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
어떤 암호화 알고리즘을 사용하고 있나요?	**외주 업체에 "현재 비밀번호 저장과 개인정보 암호화에 사용 중인 알고리즘이 무엇인가요?"라고 물어보세요.**
MD5나 DES가 사용되고 있나요?	**만약 "MD5", "DES", "3DES"라는 답변이 나오면 교체가 필요합니다.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 암호화 알고리즘 목록을 확보하고, MD5/DES 사용 여부를 확인하세요.
2. 교체 일정과 예산을 수립하세요. (보통 외주 개발 공수 발생)

☑ **외주 업체에 요청할 사항**

"현재 사용 중인 암호화 알고리즘을 전부 확인하고, MD5, DES, 3DES 등 취약한 알고리즘을 사용 중이라면 아래 기준으로 교체해 주세요."

- 비밀번호: SHA-256 이상 + Salt(임의 문자열)를 적용한 일방향 암호화
- 개인정보 양방향 암호화: AES-256 (또는 국내 검증된 암호 알고리즘)

사례9 **암호화 키를 어디에 어떻게 보관하는지 정해진 게 없어요.**

① 문제가 뭔가요?

데이터를 암호화했더라도, **그 암호를 풀 수 있는 열쇠(= 암호화 키)**를 어떻게 관리할지에 대한 절차나 규정이 없는 상태입니다. 암호화 키가 유출되면 암호화는 아무 의미가 없습니다.

▶ 쉽게 말하면: 금고 비밀번호를 포스트잇에 적어 금고 옆에 붙여둔 것과 같습니다. 아무리 튼튼한 금고라도 비밀번호가 노출되면 소용없습니다.

② 왜 위험한가요?

- 고시 제7조 제5항에 따라 **암호키의 생성·보관·배포·파기 등에 관한 관리 절차를 수립·시행**해야 합니다.
- 암호키를 소스코드나 서버 내 평문 파일로 방치하면, 데이터가 암호화되어 있어도 키가 함께 노출되어 즉시 복호화됩니다.
- **암호키 관리 절차 부재 및 키 방치는 암호화 의무 불완전 이행으로 간주**되어 보안 감사 시 개선 처분을 받게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
암호화 키 관리 절차 문서가 있나요?	**담당 부서에 "암호화 키를 어떻게 관리하는지 문서로 만든 절차가 있나요?"라고 확인하세요.**
암호화 키는 어디에 보관되나요?	**"키는 누가, 어디에, 어떻게 보관하고 있나요?" (소스코드 내 하드코딩 여부 확인 필수)**

④ 어떻게 해결하나요?

☑ 내부 조치 사항

1. 암호화 키 관리 정책 문서를 작성하세요. 포함해야 할 항목:
   - ◦ 키 관리 담당자 지정
   - ◦ 키 생성 방법 및 주기
   - ◦ 키 보관 방법 (물리적·논리적 분리, 백업)
   - ◦ 키 배포 대상자 및 절차
   - ◦ 키 사용 유효기간(변경 주기)
   - ◦ 키 복구 및 폐기 절차와 방법

☑ 외주 업체에 요청할 사항

"암호화 키가 소스코드 안에 직접 적혀 있거나 서버 내에 평문 파일로 방치되어 있지 않은지 확인해 주세요. 키는 별도의 안전한 저장소(예: 별도 보안 서버, HSM 등)에 보관하고, 접근권한을 최소화해 주세요. 또한 키 관리 절차 수립에 필요한 현재 키 현황을 문서로 제출해 주세요."

- 키를 소스코드에서 분리하여 별도 보안 저장소에 보관
- 키 접근권한을 최소 인원으로 제한

접속기록의 보관 및 점검

사례10 | **누가 언제 접속했는지 기록이 남지 않고 있어요.**

① 문제가 뭔가요?

개인정보처리시스템에 **누가, 언제, 어디서, 무엇을 했는지**에 대한 **접속기록(로그)이 생성되지 않거나**, 생성되더라도 충분히 보관·점검되지 않는 상태입니다.

▶ 쉽게 말하면: 회사 건물에 CCTV가 전혀 없는 것과 같습니다. 사고가 나도 누가, 언제, 무엇을 했는지 전혀 알 수 없습니다.

② 왜 위험한가요?

- 고시 제8조에 따라 시스템 접속기록을 **1년(5만 명 이상 또는 민감정보 처리 시 2년) 이상 보관하고, 월 1회 이상 점검**해야 합니다.
- 내부 직원뿐만 아니라 시스템에 접속하는 유지보수 인력, 수탁사 등 접속한 모든 자(정보주체 제외)의 접속기록을 남겨야 합니다.
- 접속기록이 없거나 부실하면 개인정보가 무단 열람·다운로드 되어도 유출 사실을 알 수 없고, 사고 발생 시 책임자 규명이 불가능합니다.
- **접속기록 미생성 및 정기 점검 누락은 안전조치의무 위반**으로, 점검 시 3천만 원 이하의 과태료가 부과될 수 있습니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
접속기록이 생성되고 있나요?	**외주 업체에 "우리 시스템에 접속한 사용자의 로그인/로그아웃·작업 내역이 기록되고 있나요? 기록 화면이나 파일을 보여 달라"고 요청하세요.**
기록에 필수 항목이 포함되어 있나요?	**접속기록에 [접속자 ID, 접속 일시, 접속 IP, 수행업무, 조회/변경/삭제 정보]가 포함되어 있는지 확인하세요.**
접속기록을 정기적으로 점검하나요?	**월 1회 이상 접속기록을 확인하고 이상징후를 점검하는 절차가 있는지 확인하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 월 1회 접속기록 점검 담당자를 지정하세요.
2. 점검 결과를 문서로 남기고, 이상징후 발견 시 대응 절차를 마련하세요.
3. 개인정보 파일 다운로드 시 사유를 반드시 소명받고 점검대장에 기록하도록 규정하세요.

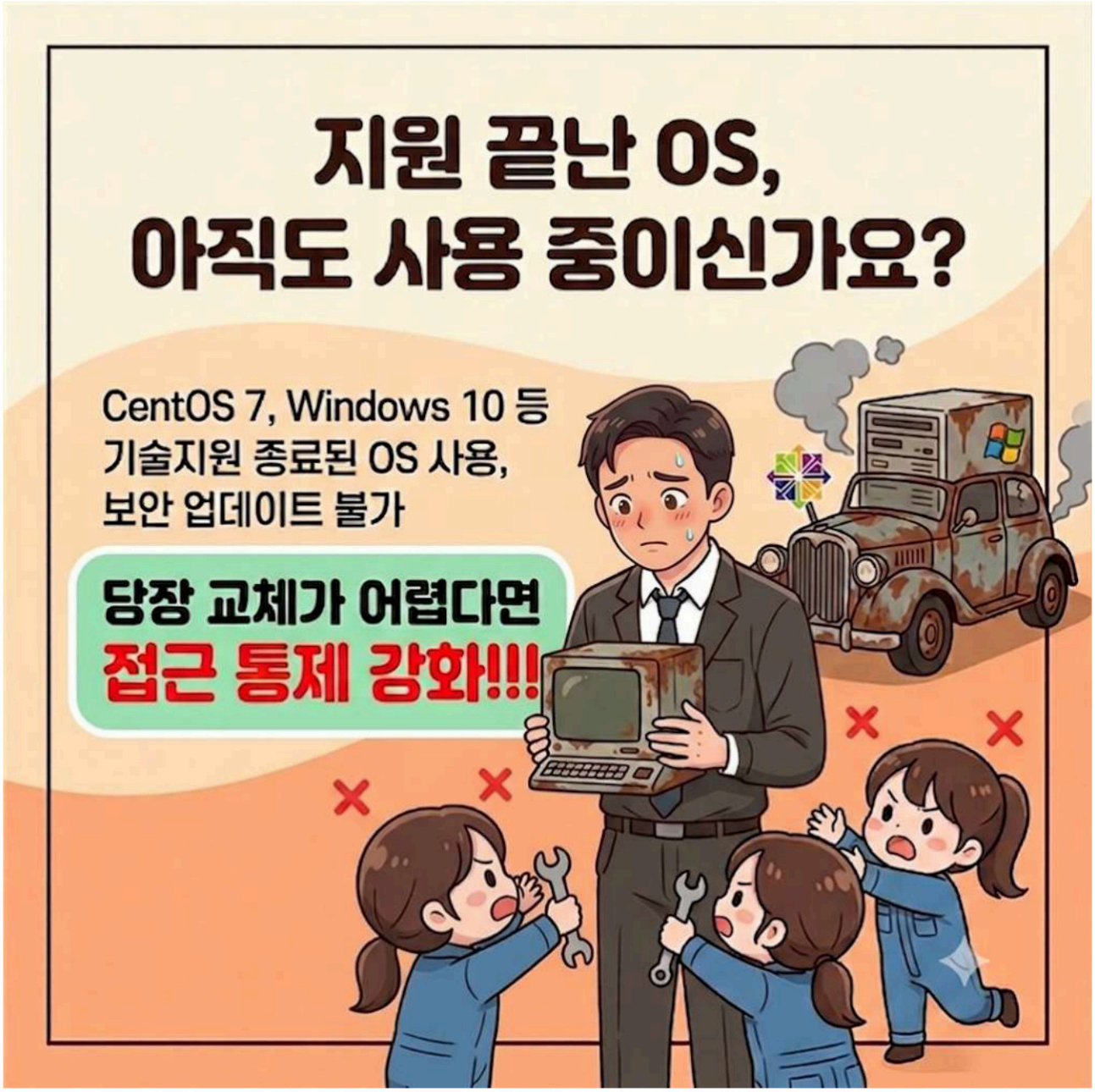
☑ **외주 업체에 요청할 사항**

"현재 접속기록이 생성되지 않거나 누락되고 있다면, 아래 항목을 포함한 접속기록이 생성되도록 시스템을 개선해 주세요. 또한 기록이 위·변조되지 않도록 별도 로그 서버에 저장하거나 WORM(쓰기 한 번만 가능한 저장장치) 방식을 검토해 주세요."

- **접속기록 필수 항목**: 접속자 ID, 접속 일시, 접속 IP주소, 정보주체, 수행업무(조회·변경·삭제·출력·다운로드 정보)
- **보관 기간:** 최소 1년 이상(다음 중 어느 하나에 해당하는 경우 2년 이상 보관)
  1)대규모 개인정보 처리: **5만 명 이상**의 정보주체에 관한 개인정보를 처리
  2)중요정보 처리: **고유식별정보 또는 민감정보**를 처리
  3)특정사업자:「전기통신사업법」제5조에 따른 **기간통신사업자**
- **보관 방법**: 덮어쓰기가 불가능한 저장 방식 권장, 주기적 백업

악성프로그램 등 방지

사례11 **지원이 끝난 운영체제(OS)를 아직 사용하고 있어요.**



① 문제가 뭔가요?

기술 지원이 종료된(EOS, End of Service) 운영체제를 서버나 업무용 PC에서 계속 사용하는 경우입니다. 예를 들어 CentOS 7, Windows 10, Windows Server 2012 등은 이미 제조사 보안 업데이트가 중단된 상태입니다.

▶ 쉽게 말하면: 이미 단종되어 부품도, 수리도 안 되는 오래된 자동차를 계속 타는 것과 같습니다. 새로 발견된 결함(보안 취약점)을 고칠 방법이 없습니다.

② 왜 위험한가요?

- 고시 제9조에 따라 OS와 소프트웨어의 **최신 보안 패치를 주기적으로 적용**해야 합니다.
- 기술지원 종료(EOS) 이후에는 공식 패치를 받을 수 없어 해킹이나 랜섬웨어 공격에 상시 노출되며, 백신 프로그램만으로는 OS의 구조적 결함을 막기 어렵습니다.
- **EOS OS 방치는 법령상 취약점 개선 의무 위반**에 해당하여, 보안 점검 시 지적 및 행정처분을 받게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
서버와 PC의 OS 버전이 무엇인가요?	**외주 업체에 "운영 중인 서버와 업무용 PC의 OS 종류와 버전 목록을 제출해 달라"고 요청하세요.**
기술 지원이 종료된 OS가 있나요?	**현재 지원 종료된 주요 OS** • **CentOS 7 이하 (2024년 6월 지원 종료됨)** • **Windows 10 (2025년 10월 지원 종료됨)** • **Windows Server 2012 / 2012 R2 (2023년 10월 지원 종료됨)** • **Windows 7, 8, 8.1 (지원 종료 완료)** • **Ubuntu 18.04 이하 (2023년 5월 지원 종료됨)**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 전체 IT 자산(서버 + PC)의 OS 버전 현황표를 확보하세요.
2. EOS OS을 교체하는 계획과 예산을 수립하세요. (단계적 마이그레이션)
3. 당장 교체가 어렵다면 해당 장비를 인터넷에서 격리하고, 접근통제를 강화하세요.

☑ **외주 업체에 요청할 사항**

"전체 서버와 업무 PC의 OS 현황을 조사해서 기술 지원이 종료된 OS 목록과 대수를 알려주세요. 교체 일정 계획을 함께 수립하고, 교체 전까지 임시 보안 조치(인터넷 격리, 접근통제 강화 등)를 적용해 주세요."

- 가능하면 CentOS 7 → Rocky Linux 8/9, AlmaLinux 등의 후속 OS로 마이그레이션
- Windows 10 → Windows 11로 업그레이드
- 교체 전까지 해당 장비는 별도 네트워크 분리 또는 인터넷 접속 차단

개인정보의 파기

사례12 **언제, 무엇을, 어떻게 파기했는지 기록이 없어요.**

① 문제가 뭔가요?

개인정보를 파기했다고 하지만 **파기 일시, 파기 대상, 파기 방법, 파기한 데이터양, 파기 작업자** 등에 대한 기록이 남아 있지 않은 상태입니다. "파기했다"라는 말만 있고 증빙이 없는 상황입니다.

▶ 쉽게 말하면: "서류는 폐기했어요"라고 말만 하고 파쇄 확인증이나 폐기 기록은 전혀 남기지 않는 것과 같습니다.

② 왜 위험한가요?

- 「개인정보 보호법」 제21조 및 고시 제12조에 따라 **목적 달성 시 지체 없이 파기하고, 파기 내역을 기록·관리**해야 합니다.
- 다른 법령에 따라 보존해야 하거나 일부만 분리보관 해야 할 경우, 기존 개인정보와 **물리적·논리적으로 분리하는 절차**를 갖추어야 합니다.
- 파기 확인서나 시스템 삭제 로그 등 객관적 증빙이 없으면 법적으로 파기하지 않고 방치한 것으로 간주되어 불필요한 개인정보 보유 위험이 지속되며, 파기 기록 부재 및 미파기 적발 시 법적 의무 위반으로 과태료 처분을 받게 됩니다.

③ 어떻게 확인하나요?

확인 항목	확인 방법
파기 결과를 기록하고 있나요?	**"개인정보 파기 후 파기 결과보고서나 파기 확인서를 작성해 보관하고 있나요?"라고 물어보세요.**
일부 보관이 필요한 데이터는 어떻게 관리하나요?	**법령에 따라 보존해야 하는 데이터(과세, 감사 관련 등)와 파기할 데이터를 분리하는 절차가 있는지 확인하세요.**

④ 어떻게 해결하나요?

☑ **내부 조치 사항**

1. 개인정보 파기 시 파기 결과 확인서를 의무 작성하도록 규정하세요. (포함할 항목)

- 파기 일시
- 파기 사유 (처리 목적 달성 / 보유기간 만료 / 탈퇴 / 기타)
- 파기 대상 (시스템명, DB 테이블 명, 개인정보 파일명)
- 파기 항목 (이름, 주민번호, 연락처 등 파기한 정보 종류)
- 파기 데이터 수 (건)
- 파기 방법 (DB 레코드 삭제, 파일 완전 삭제, 물리적 파쇄 등)
- 파기 작업자 및 확인자 서명
- 분기별 또는 반기별 파기 이행 실태를 점검하세요.

☑ **외주 업체에 요청할 사항**

"개인정보 파기 내역을 자동으로 기록하는 기능을 시스템에 추가하거나, 파기 작업 시 수동으로라도 파기 확인서를 생성해 제출해 주세요. 또한 법령상 보관 의무가 있는 정보와 파기 대상 정보를 분리하여 저장할 수 있도록 조치해 주세요."

- 파기 로그 자동화: 파기 시점, 대상, 작업자 등이 DB 로그로 기록되도록 구현
- 분리보관: 보존 대상 데이터는 별도 테이블/스키마로 이관하는 프로세스 구현