

2026년 연계정보 안전조치 실태점검 설명회

2026. 6.

- ✓ 점검 대상 선정 이유와 기준
- ✓ 실태점검 대응 및 증빙자료 제출 안내



실태점검 개요

대상	연계정보 이용기관 (정보통신망법 제23조의5제1항에 따라 본인확인기관으로부터 연계정보를 제공 받는 자)
항목	연계정보 처리 현황 및 안전조치 이행 여부 ※「별표 4」 연계정보 이용기관의 안전조치 참조
목적	「정보통신망법」제23조의6(연계정보의 안전조치 의무 등) 및 시행령 제13조에 따른 법적 의무 이행 여부 점검
방법	연계정보 안전조치 사항 이행여부 서면제출
점검기관	 방송미디어통신위원회  KISA 한국인터넷진흥원
제출기한	~ 08월 14일 (금) 까지

시행 근거

01



규정 취지

정보통신망법 제23조의6제3항에 따라 방송미디어통신위원회는 연계정보 이용기관의 안전조치에 대한 운영·관리를 적절히 취하고 있는지를 점검하도록 하여 연계정보 유출 및 오·남용을 사전에 방지하기 위한 제도적 장치를 마련함

『정보통신망법』 제23조의6(연계정보의 안전조치 의무 등)

- ③ 방송미디어통신위원회는 생성·처리하는 연계정보의 규모, 매출액 등이 대통령령으로 정하는 기준에 해당하는 본인확인기관의 물리적·기술적·관리적 조치 및 연계정보 이용기관의 안전조치에 대한 운영·관리 실태를 점검할 수 있다.

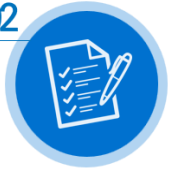
『정보통신망법 시행령』 제14조(운영·관리 실태점검의 대상)

법 제23조의6제3항에 따른 실태점검(이하 “실태점검”이라 한다)의 대상이 되는 본인확인기관 및 연계정보 이용기관은 다음 각 호의 구분에 따른 자로 한다.

- 2. 연계정보 이용기관의 경우: 법 제23조의5제1항에 따라 본인확인기관으로부터 연계정보를 1,000건 이상 제공받은 자

시행 근거

02



연계정보 이용기관의 안전조치 의무

정보통신망법은 연계정보가 분실·도난·유출·위조·변조·훼손되지 않도록 연계정보 이용기관에 안전조치 의무를 부여하고 있으며, 같은 법 시행령 제13조(본인확인기관의 물리적·기술적·관리적 보호조치 등)에 연계정보 이용기관이 준수하여야 할 안전조치 등 세부 기준을 마련함으로써 이를 『연계정보의 생성·처리 등에 관한 기준』 제11호 및 [별표 4]의 내용으로 구체화 함

「정보통신망법 시행령」 제13조(본인확인기관의 물리적·기술적·관리적 조치 등)

- ② 법 제23조의5제4항 본문에 따른 연계정보 이용기관(이하 “연계정보 이용기관”이라 한다)은 법 제23조의6제2항에 따라 연계정보를 주민등록번호와 분리하여 보관·관리하고 연계정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 다음 각 호의 조치(이하 “안전조치”라 한다)를 해야 한다.
1. 안전조치를 총괄하는 책임자 지정 등 연계정보의 안전한 처리를 위한 내부 규정의 수립 및 시행
 2. 연계정보를 제공받은 목적 범위 내 연계정보 처리
 3. 주민등록번호를 보관하는 경우에는 해당 주민등록번호와 연계정보를 분리·보관·관리
 4. 연계정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용
 5. 연계정보 분실·도난 등의 침해사고 발생 시 대응 계획의 수립 및 시행
 6. 연계정보 제공기관 및 제공시기 등에 관한 자료의 기록·보관

「연계정보의 생성·처리 등에 관한 기준」 제11호(연계정보 이용기관의 안전조치)

- ① 연계정보 이용기관은 연계정보의 안전한 활용 및 보호를 위하여 안전조치를 하여야 한다.
- ② 영 제13조제2항 각 호에 따라 연계정보 이용기관이 취하여야 할 안전조치의 세부 내용은 별표 4와 같다.

시행 근거

『연계정보의 생성·처리 등에 관한 기준』 [별표 4] 연계정보 이용기관의 안전조치

1. 연계정보의 안전한 처리를 위한 내부 규정의 수립 및 시행에 관한 사항

- 1-1. 안전조치를 총괄하는 책임자 지정에 관한 사항
- 1-2. 연계정보의 취급·관리 절차에 관한 사항
- 1-3. 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항
- 1-4. 연계정보의 안전한 저장·전송에 관한 사항
- 1-5. 연계정보의 유출, 도난 방지를 위한 취약점 점검에 관한 사항
- 1-6. 그 밖에 연계정보 보호를 위하여 필요한 사항

2. 연계정보를 제공받은 목적 범위 내 연계정보 처리에 관한 사항

- 2-1. 연계정보취급자를 최소한으로 제한
- 2-2. 연계정보취급자에 대한 정기적인 교육
- 2-3. 연계정보 처리 실태에 대한 연 1회 이상 정기적인 점검

3. 주민등록번호를 보관하는 경우 해당 주민등록번호와 연계정보의 분리·보관·관리에 관한 사항

- 3-1. 비인가자의 접근 등에 의해 연계정보와 주민등록번호가 함께 유출되지 않도록 물리적 또는 논리적으로 분리하여 보관

4. 연계정보를 안전하게 저장·전송할 수 있는 암호화 기술 적용에 관한 사항

- 4-1. 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우 안전한 암호 알고리즘으로 암호화
- 4-2. 10만 명 이상의 이용자 연계정보를 보유한 대기업·중견기업·법 제44조의5제1항 제1호에 해당하는 공공기관 등 또는 100만 명 이상의 이용자 연계정보를 보유한 중소기업·단체는 연계정보를 안전한 알고리즘으로 암호화하여 저장

5. 연계정보 분실·도난 등의 침해사고 발생 시 대응 계획의 수립 및 시행에 관한 사항

- 5-1. 다음 각 목을 포함하는 계획의 수립 및 시행
 - 가. 연계정보 수집 등 연계정보 처리에 관한 사항의 공개
 - 나. 연계정보 침해사고 발생 시 접수 절차
 - 다. 연계정보 이용내역 등 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의철회 등 요구 대응 절차

6. 연계정보 제공기관 및 제공 시기 등에 관한 자료의 기록·보관에 관한 사항

- 6-1. 연계정보 수집의 근거 및 현황을 확인할 수 있도록 다음 사항을 포함하여 기록
 - 가. 수집 출처
 - 나. 수집 시기
 - 다. 수집 목적
 - 라. 수집 대상 등
- 6-2. 연계정보의 수집 출처, 수집 시기 등에 관한 자료는 최소 1년간 저장·관리

실태점검 대상 선정기준

연계정보 이용기관

- ✓ 본인확인기관으로부터 연계정보(CI)를 제공받은 자로서, 일반적으로 본인확인서비스를 이용하는 정보통신서비스 제공자
- ✓ '보유' 여부가 아니라 '처리' 여부가 점검 대상 판단의 출발점

⚠ 주의사항

- CI를 저장하지 않고 조회·대조만 해도 처리로 볼 수 있음

대상 선정

전년도 CI 처리/제공 누적 규모 기반 선정

- ✓ 전년도(2025년 12월말 기준) CI 처리/제공 누적 규모
1,000건 이상 제공받은 기관 선정

비대상 기관도 준비 필요

올해 대상이 아니어도 내년도 점검 대상 가능성 있음

- i 2027년 5월 시행 예정 항목
분리보관, 저장 시 암호화, 수집기록 보존 등 준비 필요

실태점검 대상 기관 해당 여부

✔ 대상에 해당하는 경우 (O)

- ✔ CI 저장 안 하고 조회·대조만
처리 사실이 핵심, 저장 여부와 무관

대상 조회·대조

- 본인확인기관으로부터 CI를 제공받아 조회·대조하는 경우
- 저장하지 않더라도 처리 사실이 존재하는 경우
- 서비스 연계를 위한 일시적 대조 목적인 경우

- ✔ 외주/위탁 운영
책임·증빙 준비 의무 여전

대상 위탁

- CI 처리를 외부에 위탁한 경우
- 위수탁계약서, 처리현황 등 증빙 준비 필요
- 수탁사의 안전조치 이행 여부 확인 필요

✖ 대상에 해당하지 않는 경우 (X)

- ✖ DI만 처리
CI 처리하지 않는 경우

비대상 DI만

- 중복가입확인정보(DI)만 수집·처리하는 경우
- 본인확인기관으로부터 연계정보(CI)를 제공 받지 않는 경우

실태점검 절차



핵심 체크포인트

- 담당자 지정
- 증빙 자료 수집
- 내부 검토 수행
- 최종 제출본 구성

실태점검 대응 실무 가이드

실무 대응 절차

책임자 지정·내부 총괄체계 정비 → 자가점검표 작성 → 증빙 수집 → 내부검토/결재 → 제출본 구성



현장점검 전환 대상

현장점검 전환 포인트

자료 미제출·지연, 자료 간 상호모순·운영 부재 의심, 주요 항목 증빙 부실, 언론·민원·사고 등 외부 이슈

자료 미제출 또는 지연 제출

긴급

자료제출 기한 내 미제출 또는 지연 제출 시 현장점검 전환

- 자료제출 기한: 2026년 00월 00일(0)까지
- 미제출 시 현장점검 대상 선정 및 추가 검토 필요

위험도  90%

주의 : 3천만원 이하 과태료 부과 가능

자료 간 상호모순 등 운영 현황 의심 상황

주의

제출된 자료 간 내용 불일치 또는 모순 발견

- 정책 내용과 실제 운영 현황 불일치, 권한대장과 시스템 불일치
- 교육 이력과 실제 교육 내용 불일치

위험도  75%

주의: 서면 검토 후 보완 요청 가능

주요 항목 증빙 부실

긴급

분리보관, 권한관리, **연계정보 암호화** 등 핵심 항목 증빙 미흡

- 분리보관 조치 미흡 및 접근권한 관리 부실
- **연계정보 전송·저장 시 암호화 미흡**

위험도  85%

주의: 현장점검 시 집중 검토 대상

사고 등 외부 이슈 발생

긴급

언론·민원·사고 등 외부 이슈로 긴급 점검 필요성 발생

- 침해사고 등 사회적 이슈 발생 및
- 사고 대응 관련 민원 접수·처리 지연 발생

위험도  95%

주의: 즉시 현장점검 전환 가능

실태점검 항목별 준비사항(개요)

1	내부 규정 수립 및 시행 CI 처리 관련 내부 규정 수립, 결재 및 시행 이력 확보	필수
2	취급자 최소화 및 권한관리 총괄/취급/검직 기준 명확화, 최소권한 원칙 적용	필수
3	분리보관 CI와 주민등록번호 물리적/논리적 분리	2027
4	암호화 전송 시 암호화, 저장 시 암호화	필수 2027
5	침해사고 대응 계획 수립 및 시행 처리방침 공개, 열람·정정·삭제 대응 절차	필수
6	자료의 기록 보관 수집 출처, 시기, 목적, 대상 등 기록 보관	2027

실태점검 항목별 준비사항 - 1.내부 규정 수립 및 시행

내부 규정 수립 및 시행

별도 규정 또는 내부관리계획에 CI 항목 포함, 경영진 결재·시행 이력 확보

필수항목

결재필요

시행이력

☞ 해야 할 일

✓ 별도 규정 또는 내부관리계획에 CI 항목 포함
연계정보(CI) 처리에 관한 내용을 명확히 기재

✓ 경영진 결재·시행 이력 확보
결재일자, 결재자, 시행일자 등 기록 관리

📄 증빙

▶ 최신화된 규정서(개정이력)
버전 관리, 개정일자, 변경 내용 명시

▶ 시행 공지
전사 공지, 이메일, 게시판 등

⚠ 자주 실수하는 부분

● 서명/결재 누락
결재 라인, 서명, 날짜 등 필수 요소 누락

● 연계정보 항목 미포함
CI 처리, 보관, 파기 등 내용 누락

● 시행 흔적 부재
실제 운영 증거, 로그, 기록 없음

실태점검 항목별 준비사항 - 2.취급자 최소화 및 권한관리

취급자 최소화 및 권한관리

최소 권한 원칙에 따른 취급권한 부여, 직무 변경·퇴직 시 권한 회수, 권한 매트릭스 및 이력 관리

권한 매트릭스

구분	조회	다운로드	삭제	계정생성	비고
시스템 관리자	✓	✓	✓	✓	전체 권한
연계정보취급자	✓	✓	✗	✗	조회·다운로드
일반 사용자	✓	✗	✗	✗	조회만

✓ 허용 ✗ 거부

관리 요건

핵심 관리 포인트

- ✓ 최소권한 원칙: 업무 필요 최소 인원에게만 권한 부여
- ✓ 권한 분리: 조회/다운로드/삭제/관리자 권한 분리
- ✓ 직무 변경·퇴직 시 즉시 권한 회수 및 이력 관리
- ✓ 시스템 권한과 문서 대장 일치 여부 점검

▲ 주의사항

권한 부여/변경/삭제 이력을 반드시 기록
시스템 실제 권한과 문서 대장 일치 여부 정기 점검

실태점검 항목별 준비사항 - 2.취급자 최소화 및 권한관리

취급자 교육 및 점검

연계정보 보호 포함 교육 실시, 연계정보 처리 실태점검 수행 및 개선, 적정한 증빙 자료 준비

연 1회 이상

교육 실시

자체점검

☞ 해야 할 일



연계정보 보호 포함 교육 실시

연 1회 이상 정기 교육, CI 내용 반드시 포함



연계정보 처리 실태 자체점검 수행 및 개선

연 1회 이상, 문제 발견 시 개선 조치



교육 결과 및 점검 결과 기록 보관

📄 증빙 자료



교육 계획/결과

커리큘럼 · 수료증 · 참석자 명단



자체점검 계획/결과 보고서

점검 항목 · 발견 사항 · 개선 조치



교육 및 점검 결과 보고서

결과 요약 · 시정 조치 · 재점검 계획

⚠ 유의사항



'개인정보 내용'만 있고 CI 내용 포함 증적 없으면 불인정

연계정보 보호에 대한 구체적인 교육 내용이 포함되어야 함

실태점검 항목별 준비사항 - 2.취급자 최소화 및 권한관리

✓ 좋은 예 (O)

✓ 규정 최신화·시행증적

최신 버전 규정, 시행 흔적 확보

최신 시행증적

- 내부 규정 등 정책문서가 최신 버전으로 업데이트되어 있음
- 시행 공지, 개정 이력이 명확하게 기록됨
- 경영진 결재 및 시행 증적이 유지 관리되고 있음

✓ 시스템 권한과 일치

권한대장과 실제 시스템 권한 일치

일치 권한관리

- 권한대장과 실제 시스템 권한이 일치함
- 직무 변경·퇴직 시 즉시 권한 회수
- 권한 이력이 체계적으로 관리됨

✗ 나쁜 예 (X)

✗ 규정 있음(옛 버전)

최신 법령 반영 미흡, 내부 규정 검토 증적 및 개정 이력 없음

미흡 구버전

- 규정서가 옛 버전으로 최신화되지 않음
- 개정 이력이 없거나 불명확함
- 시행 공지, 결재 증적 등 이력 관리 미흡

✗ 권한대장과 시스템 불일치

실제 권한과 문서 상 권한 사이 불일치 발생

불일치 권한관리

- 권한대장과 실제 시스템 권한이 불일치
- 직무 변경·퇴직 시 권한 회수 지연
- 권한 이력 관리가 체계적이지 않음

실태점검 항목별 준비사항 - 3.분리 보관

주민등록번호와 연계정보의 분리 보관

물리적 분리와 논리적 분리 방법, 권한 관리 및 모니터링 강화

분리보관 대상 및 방법

분리보관 대상

⚠ 연계정보(CI)와 주민등록번호의 동시 유출 방지가 핵심 목표

물리적 분리

- 서버/DB 하드웨어 분리
- 물리적 독립 운영
- 완전한 격리

논리적 분리

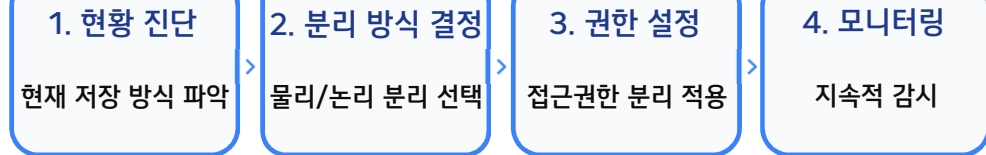
- DB 인스턴스 분리
- 스키마/테이블 분리
- 접근권한 분리

⚠ 유의사항

논리적 분리 시 권한·모니터링 강화, 동일 관리자·계정 사용 금지

분리보관 실행 단계

분리보관 실행 프로세스



✓ 핵심 체크리스트

- ✓ DB 인스턴스 분리
- ✓ 접근권한 분리
- ✓ 스키마/테이블 분리
- ✓ 로그 분리

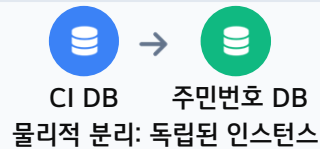
실태점검 항목별 준비사항 - 3.분리 보관

✓ 좋은 예 (O)

✓ DB 인스턴스 분리 물리적 분리로 보안 강화

물리 분리 전용 DB

- 별도의 DB 인스턴스로 CI와 주민등록번호 분리
- 독립된 서버/스토리지 구성 / 네트워크 구간 분리



✓ 전용 계정 + 접근 로그 분리 권한 분리 및 로그 관리

전용 계정 로그 분리

- CI 조회/처리용 전용 계정 운영
- 접근 로그 별도 저장 및 모니터링 및 권한 분리

[2026-03-15 10:30:15] USER_CI_001: SELECT * FROM ci_table...

✗ 나쁜 예 (X)

✗ 동일 테이블 보관 하나의 테이블에 모두 저장

테이블 미분리 보안 취약

- CI와 주민등록번호를 동일 테이블에 저장
- 하나의 컬럼에 민감정보 혼합 / 노출 위험



✗ 동일 관리자 계정 + 로그 미분리 권한 통합 및 로그 관리 부재

계정 미분리 로그 미분리

- CI/주민번호 조회에 동일 계정 사용
- 접근 로그 통합 저장 및 관리자 모든 데이터 접근

[2026-03-15 10:30:15] ADMIN: SELECT * FROM all_data

실태점검 항목별 준비사항 - 4. 암호화

저장 · 전송 암호화



전송구간 암호화

SSL/TLS 1.2 이상, VPN/SFTP 적용

1

전송구간 암호화

SSL/TLS 1.2 이상 필수 적용, 취약한 프로토콜(SSL v3, TLS 1.0) 사용 금지

2

VPN/SFTP 적용

안전한 파일 전송 프로토콜 사용, 외부 접근 차단

3

취약 프로토콜 금지

SSL v3, TLS 1.0, 1.1 등 취약한 프로토콜 완전 차단



주의사항

암호화 적용 시 유의사항

- i 암호화 알고리즘은 국가표준 준수
- i 키 관리는 별도 보안 체계 구축
- i 정기적인 암호화 강도 점검 필요



저장 시 암호화 (2027.05.01 시행)

대상 규모 기준 적용



저장 암호화 의무화

10만 명 이상 대기업/공공기관, 100만 명 이상 중소기업·단체

1

현황 진단

보유 연계정보 규모 및 저장 방식 파악

2

대상 판단

암호화 의무 대상 여부 확인

3

설계(알고리즘·키관리)

안전한 알고리즘 선택 및 키 관리 방안 수립

4

이행 계획

단계별 암호화 적용 일정 수립

실태점검 항목별 준비사항 - 5.침해사고 대응 계획 수립 및 시행

침해사고 대응 계획의 수립 및 시행

처리방침 공개, 권리행사 보장, 침해사고 대응 계획



대외 공개(처리방침 등)

홈페이지 등을 통한 연계정보 처리 현황 공개

- ✓ 수집·이용 근거, 목적, 보유 및 이용 기간 공개
- ✓ 제3자 제공 시 제공받는 자, 목적, 기간 공개
- ✓ 권리행사 방법 및 절차 안내



권리행사 대응

이용자의 열람·정정·삭제 요구 대응

- 1 열람 요청
정보주체의 연계정보 처리 현황 확인 요구
- 2 정정·삭제·처리정지
오류 정정, 삭제, 처리 일시 정지 요구



침해사고 대응

분실·도난·유출·위조·변조·훼손 대응



보고 체계

내부/외부 보고 체계 구축



대응 조직

역할·연락망 구성



단계별 절차

탐지→격리→분석→통지→복구



증빙 자료

처리방침 화면

권리행사 안내 페이지

사고대응매뉴얼

실태점검 항목별 준비사항 - 6.자료의 기록 보관

기록 보존

수집 출처, 시기, 목적, 대상을 포함한 연계정보 처리 이력 관리

 **기록보존 항목**
4가지 핵심 항목 필수 기록

항 목	내 용	보관기간
수집 출처	제공기관명 (본인확인기관)	1년
수집 시기	제공받은 일시 (YYYY-MM-DD HH:MM)	1년
수집 목적	서비스 연계, 본인확인 등	1년
수집 대상	회원 일련번호/아이디 (CI 값 제외)	1년

 **보안 원칙**
CI 값 노출 최소화

무결성
해시/타임스탬프

기밀성
암호화 저장

가용성
백업/복구

 **증빙 자료**
로그/DB 캡처 및 무결성 통제

1 **로그/DB 캡처**
연계정보 처리 이력 로그 및 DB 화면 캡처 저장

2 **보관·백업**
정기 백업 및 이중화 저장, 복구 테스트

3 **무결성 통제**
해시 체인/타임스탬프 적용, 위변조 방지

 **2027년 5월 1일 시행 예정**
연계정보 수집 기록 보관 의무화 (최소 1년)

FAQ

대상/범위 점검 대상 여부

? DI만 처리하면 대상인가요?

X. DI(중복가입확인정보)만 처리하는 경우 연계정보(CI) 미처리 시 보통 비대상입니다. CI를 실제로 수신·대조·연계하는 업무흐름이 존재하면 대상 가능성이 매우 높습니다.

? 저장 안 하고 조회만 해도 대상인가요?

O. 처리 사실이 핵심입니다. 저장 여부보다 '처리' 여부가 대상 판단의 출발점입니다. 조회·대조만 해도 연계정보 이용기관으로 간주될 수 있습니다.

점검서 작성 실태점검서 작성

? 연계정보 안전조치를 총괄하는 책임자는 개인정보 보호책임자와 겸직이 가능한가요?

O. CPO, CTO는 겸직이 가능합니다.
다만, CISO의 경우 겸직 금지에 해당하지 않는 경우 가능합니다.

? 시스템 캡처도 증빙이 되나요?

O. 자동으로 기록되는 로그나 DB 등의 화면을 캡처하여 제출하면 됩니다.
증빙자료에서 수집 출처, 시기, 목적 등을 확인할 수 있어야 합니다.

유예항목 2027 시행 대비

? 2027 시행 항목은 올해 제출 안 해도 되나요?

권고 항목의 경우 현재 예산확보, 준비기간 등을 고려하여 27년 5월 1일부터 필수 항목으로 시행될 예정입니다.
올해는 적용이 가능한 계획 형태로 작성하여 제출해주시길 바랍니다.

? 아직 교육/점검을 못했는데 어떻게 제출하나요?

아직 교육을 실시하지 못한 경우 금년도 안으로 교육 내용, 교육 예정일 등 계획서의 형태로 작성하여 제출하여 주시길 바랍니다.

현장점검 전환 조건

? 현장점검은 어떤 경우 나가나요?

- 미제출/지연 제출
- 서면자료 간 상호모순·운영 부재 의심
- 주요 항목(분리보관, 권한관리 등) 증빙 부실
- 언론·민원·사고 등 외부 이슈

? 어떻게 대비해야 하나요?

자료제출 기한 내에 실태점검서 및 증빙자료를 완성하여 제출하고, 모순이나 누락이 없도록 내부 검토를 철저히 해야 합니다.

감사합니다.



방송미디어통신위원회



한국인터넷진흥원