안전하고 편리한 온라인 본인확인서비스 제공

본인확인기관 정기 적합성심사 설명회

방송미디어통신위원회

KISA 한국인터넷진흥원

2026. 2. 11. 수요일

KISA 서울청사 대강당

CONTENTS

2026년 본인확인기관 정기 적합성 심사 안내

01

CHAPTER 1

본인확인서비스 적합성 심사

점검 대상 및 일정

점검 대상 및 일정

점검 대상

구분	현장실사	모의침투	취약점점검	비고
아이핀 3개사	NICE평가정보, 코리아크레딧뷰로, 서울평가정보,	아이핀 모듈 3개사 / 아이핀 모바일앱 3개사 / 아이핀 대행사 모듈 1개사	본인확인시스템 주설비 샘플링+ 현장 실사 시 확인	
인증서 13개사	금융결제원, 무역정보통신, 코스콤, 비바리퍼블리카, 한국정보인증, 한국전자인증, 신한은행, 우리은행, 하나은행, 국민은행, 기업은행, 농협은행, 카카오뱅크	인증서 13개사 인증서 본인확인 대행사모듈 9개사 (KG이니시스, 넥스원소프트, 라온시큐어, 드림시큐리티, 한국전자인증, NICE평가정보, 한국모바일인증, 한컴위드, 이니텍)	본인확인시스템 주설비 샘플링+ 현장 실사 시 확인	기업은행 농협은행 정기점검
휴대폰 3개사	SKT KT LGU+	휴대폰 모바일앱 3개사 / 휴대폰 인증대행사 모듈 8개사	본인확인시스템 주설비 샘플링+ 현장 실사 시 확인	**인증대행사 현장점검**
신용카드 4개사	삼성카드, 농협카드, 신한카드, 현대카드	신용카드 모바일앱 4개사 / 신용카드 제공대행사 4개사 (코리아크레딧뷰로, KG이니시스, 다우데이타, 라온시큐어)	본인확인시스템 주설비 샘플링+ 현장 실사 시 확인	

점검 대상 및 일정

점검 일정

* 상기 일정은 변경 가능

내용	일정	비고
아이핀 정기점검 사전 안내	1.30	
정기 적합성심사 설명회	2.11	심사 주안점 및 변경사항 안내
아이핀 정기점검	3.3~3.20	아이핀 3개 기관
공동인증서 정기점검 사전안내	2.10	
공동인증서 정기점검	3.23 ~ 4.24	공동인증서 5개 기관
민간인증서 정기점검 사전안내	4.27	
민간인증서 정기점검	5.26 ~ 7.17	민간인증서 8개 기관
휴대폰 정기점검 사전안내	7.24	
인증대행사 현장점검	8.24~8.28	본인확인기관 제외 5개 인증대행사
휴대폰 정기점검	8.31~9.18	휴대폰 3개 기관
신용카드 정기점검 사전안내	8.31	
신용카드 정기점검	10.12~11.6	신용카드 4개 기관

02

CHAPTER 2

본인확인서비스 적합성 심사
내용·기준·사후조치

점검 내용·기준·사후조치

점검 내용

인증모듈 • APP, 모의침투, 취약점 점검, 현장실사, 이행점검

점검검법	점검내용
모의침투	**본인확인 인증모듈 • APP** 대상 발생 가능한 **침투 시나리오 진행** - 인증모듈 : 최신 인증모듈 대상 테스트 베드 구축 및 모의침투 진행 - APP : Android, iOS 마켓에 업로드 된 최신 APP 대상 모의침투
취약점 진단	**본인확인 시스템**(네트워크 • 보안 • 서버 • DB 등)의 **취약점 진단** ※ 25년 개정된 최신 배포버전의 주요정보통신기반시설 및 전자금융기반시설 점검 가이드 기준 점검 수행
현장실사	**본인확인기관 적합성 심사 평가기준(87개 통제항목)**에 따른 현장 확인 - 개인정보, 정보보안, 관리체계 등 10인 이내 **전문가 구성(기관당 5일 진행)**
이행점검	이전 정기점검에서 확인된 **부적합 사항 및 보완사항에 대한 개선조치 이행여부와 개선내용의 적절성 현장 확인**

점검 내용·기준·사후조치

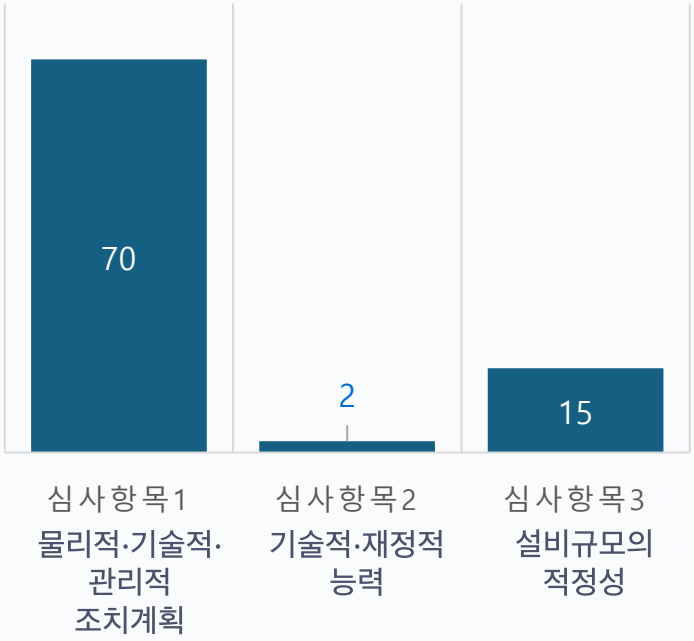
점검 기준

점검 기준 및 근거

본인확인서비스의 안전성·신뢰성 확보를 위한 요구사항

정보통신망법 제23조의 3 및 동법 시행령 제9조의 3

본인확인기관 지정 등에 관한 기준 (방통위 고시 제2022-1호) 제7조 (심사기준), 13조(사후관리)



심사항목 합계 **87** 개

방미통위 정책사항 및 2026년 적합성 심사 주안점 준수 여부

전년도 적합성 심사 결과에 따른 후속조치 내용의 적절정 등

점검 내용·기준·사후조치

점검 사후조치

점검 결과에 따른 사후조치

평가기준에 적합하지 않은 경우, 해당사항의 輕重에 따라 행정처분(경고, 업무정지, 지정취소) 또는 개선조치 지시

심사결과	적합	보완	부적합
심사결과 판정기준	본인확인기관 지정기준 및 세부 심사기준에 적합한 것으로 인정되는 경우	위반 애용 및 정도가 경미하여 즉시 시정할 수 있는 경우 고의나 중대한 과실이 아닌 사소한 부주의나 단순한 오류로 인한 경우	본인확인기관 지정기준에 부적합하여, 다수 이용자가 대체수단을 이용하는데 중대한 지장을 초래할 것으로 인정되는 경우
사후조치	지속 관리·감독	보완사항 개선조치 지시 개선조치 이행여부 및 조치내용의 적절성 확인	경중에 따라 행정처분 (경고, 업무정지, 지정취소)

03

CHAPTER 3

본인확인서비스 적합성 심사
26년 심사 변경점

26년 심사 변경사항

심사 변경사항 안내

1. 본인확인기관 인증 대행사 보안성 강화

현행(AS-IS)

매년 신용카드 본인확인기관 점검 전 ARS·중계운영사 4개사에 대한 현장실사 실시

변경사항(To-Be)

알뜰폰 부정개통 등 침해사고 방지를 위해 신용카드 중계운영사 대신 휴대폰 인증 대행사에 대한 점검 실시

개선 이유

매년 중계운영사에 대한 실태점검을 수행하는 것은 실효성 부족

최근 잇따른 보안 사고들로 인해 인증과정 상의 보안성 강화에 대한 요구 증대

휴대폰 인증 대행사 8사 모두 점검 대상에 해당

※ 아이핀 3사의 경우 본인확인기관 정기심사 과정 중에 함께 진행

인증 대행사에 대한 현장실사는 휴대폰 본인확인기관 정기심사

이전에 실시할 예정으로 정확한 일정 및 계획은 추후 안내

26년 심사 변경사항

심사 변경사항 안내

2. 서버 취약점 진단 결과에 대한 신뢰성 확보

현행(AS-IS)

본인확인기관 정기점검 전 심사 대상 기관으로부터 취약점 진단 결과를 받아 이상유무 검토

변경사항(To-Be)

- 본인확인기관이 제출한 취약점 진단 자산 중 기반시설에 해당하는 주요 자산(본인확인 AP, DB) 샘플링(2~3대) 하여 사전 점검 실시
- 사전 점검 내용과 본인확인기관이 제출한 취약점 진단 결과 비교 확인

개선 이유

본인확인기관이 사전 제출한 취약점 진단 결과가 현장실사 과정에서 확인한 실제 조치 현황과 상이한 경우 다수 존재

사전 제출 받은 취약점 진단의 결과를 신뢰할 수 없다고 판단하는 경우 본인확인설비 일체에 대한 취약점 재진단 및 결과 재제출 요구 예정

26년 심사 변경사항

심사 변경사항 안내

3. 정기점검 사전 준비자료 간소화

현행(AS-IS)

심사준비 자료로 55개 항목에 대해 인쇄물, 61개 항목에 대해 파일 자료 요구

변경사항(To-Be)

- 인쇄물로 사전 준비가 필요한 자료를 6개 항목으로 최소화하고 기타 준비자료는 파일로 준비
- 심사장에 심사자료가 담긴 PC/노트북(심사위원별) 및 프린터 사전 설치

개선 이유

페이퍼리스를 통해 불필요한 자원 낭비 최소화,
담당자 부담 경감 및 행정 효율 제고

사전 준비자료 목록

① 전년도 정기점검 및 이행점검 결과
② 심사일정표
③ 자산 목록
④ 정보시스템 구성도
⑤ 네트워크 구성도
⑥ 개인정보 흐름도

26년 심사 변경사항

심사 변경사항 안내

4. 정기점검 진행 일정 변경

현행(AS-IS)

- 심사 1일차 심사 점검단, 기관 담당자대상 착수회의 수행
- 정기점검 심사 기준, 일정에 대한 간략한 소개

변경사항(To-Be)

- 착수회의 일정 삭제 및 세부 일정 변경을 통한 심사 품질 향상
- 종결회의 시 착수회의에서 안내하는 내용 전달

개선 이유

**매년 반복되는 형식적인 절차를 지양함으로써 사업자 부담 줄이고,
심사시간을 충분히 확보하여 본연의 업무에 집중**

**심사 1일차 착수보고를 대신하여 전년도 보완사항 조치결과 확인, 기관 소개 및
본인확인서비스 브리핑, 담당자 사전 인터뷰 등 진행**

※ 세부 변경 일정은 사전안내 시 전달된 일정표 참고

26년 심사 변경사항

심사 변경사항 안내

5. 대체수단 발급/폐지/인증 시 알림

현행(AS-IS)

- 알림서비스는 이메일/SMS/앱 중 통상적으로 2가지 방식으로 제공

구분	수단
아이핀	이메일 + 앱
휴대폰	SMS + 이메일
인증서	이메일 + 앱
카드	이메일 + 앱

변경사항(To-Be)

- 부정 발급 등 침해사고를 사전에 방지하기 위해 알림 기능 강화 필요
  > 발급/폐지/인증 알림 필수
- 이메일 주소 형식 검증 절차 도입을 의무화하고 이메일 유효성 체크를 권장

개선 이유

알림 서비스 제공에 대한 이용자 동의 절차를 통해 선택권을 보장하고 침해사고 예방 기능을 강화

26년 심사 변경사항

심사 변경사항 안내

6. 허무인 검증 주기

현행(AS-IS) 본인확인기관 간 허무인 검증 주기가 상이
- 정보갱신을 위한 비용이 원인

→ **변경사항(To-Be)** 허무인 검증 주기를 최장 3개월로 설정

개선 이유 본인확인기관 별 허무인 정보가 불균형 편차를 해소하고 최신성을 확보하여 본인확인서비스 신뢰성을 강화

---

7. 구버전 모듈 사용에 대한 관리 및 조치

현행(AS-IS)

인력, 비용 등 기관 사정을 최대한 고려하여 개선 권장

→ **변경사항(To-Be)**

불가피한 경우를 제외하고 신버전으로 교체 필수

개선 이유 본인확인서비스 보안성 강화를 통해 침해사고 예방

26년 심사 변경사항

심사 변경사항 안내

8. 비대면 대체수단 발급 시 간편인증 활용 제한

현행(AS-IS) 비대면 대체수단 발급과정에서 본인확인 대신 간편인증으로 이용자 신원 확인

→

변경사항(To-Be) 간편인증 대신 본인확인기관이 제공하는 본인확인 수단으로 변경·도입

개선 이유 비대면 대체수단 발급 시 신원확인 절차를 강화하여 부정발급 예방

---

9. 본인확인 설비 내 DI 저장

현행(AS-IS)

본인확인설비 내 DI 저장 금지

→

변경사항(To-Be)

주민번호와 별도 분리 · 저장하는 경우 본인확인설비 내에 DI 저장 가능

개선 이유 해설서 【7.5.다】(중복가입확인정보의 제공)에 대한 해석 및 판단 기준 제시

향후 변경 계획(중 • 장기)

중·장기 변경 계획

1. 재외동포 국내거소등록번호를 통한 대체수단 발급

현행(AS-IS)

국내거소등록번호를 통한 대체수단 발급에 관한 법적 근거 불명확

일부 본인확인기관의 경우 국내거소등록번호로 대체수단 발급 불가

변경사항(To-Be)

정보통신망법 개정을 통해 연계정보 생성에 사용되는 정보로 주민등록번호 이외에 외국인등록번호, 국내거소등록번호를 추가하여 법적 기반 마련

2. 클라우드 기반 본인확인 설비 운영

현행(AS-IS)

현행 기준상 본인확인 전용설비는 반드시 본인확인기관이 단독소유하고 있어야 함

※ 퍼블릭이 아닌 프라이빗 클라우드는 사용해도 무방

변경사항(To-Be)

클라우드 보안 및 정보보호 정책 등을 검토·연구하여 클라우드 기반 본인확인 설비가 점진적으로 도입될 수 있는 환경 조성

- 클라우드 설비 구축에 대한 기준 및 가이드 마련 필요
- CSAP 인증 획득 의무화 검토 등

향후 변경 계획(중・장기)

중·장기 변경 계획

3. 서버 이중화(RTO, RPO)

현행(AS-IS)

현행 심사기준에 재해복구(Diaster Recovery, DR)에 관한 내용 부재

일부 본인확인기관은 업무영향분석(BIA)에서 본인확인 설비를 중요설비로 판단하지 않아 목표복구시간(RTO)을 1개월 등으로 정함

변경사항(To-Be)

서버 이중화가 필수는 아니더라도 본인확인기관은 24시간/365일 지속 가능성에 대한 보장 필요

정기·지정 심사 기준 해설서 개정을 통해 본인확인서비스에 대한 RTO, RPO에 대한 최소 기준 마련

4. 키 관리 주기

현행(AS-IS)

본인확인서비스 관련 대칭키 사용 시 연 1회 이상 운영계와 개발계 모두 비밀 key 갱신 필수

변경사항(To-Be)

KISA가 제공하는 암호키 가이드 및 NIST 가이드에서 1~3년으로 안내

타 고시 및 가이드를 참고하여 교환주기를 2년 주기로 개정【7.6.가】

향후 변경 계획(중 • 장기)

중·장기 변경 계획

5. 개인정보 파기 심사 기준 부재

현행(AS-IS)

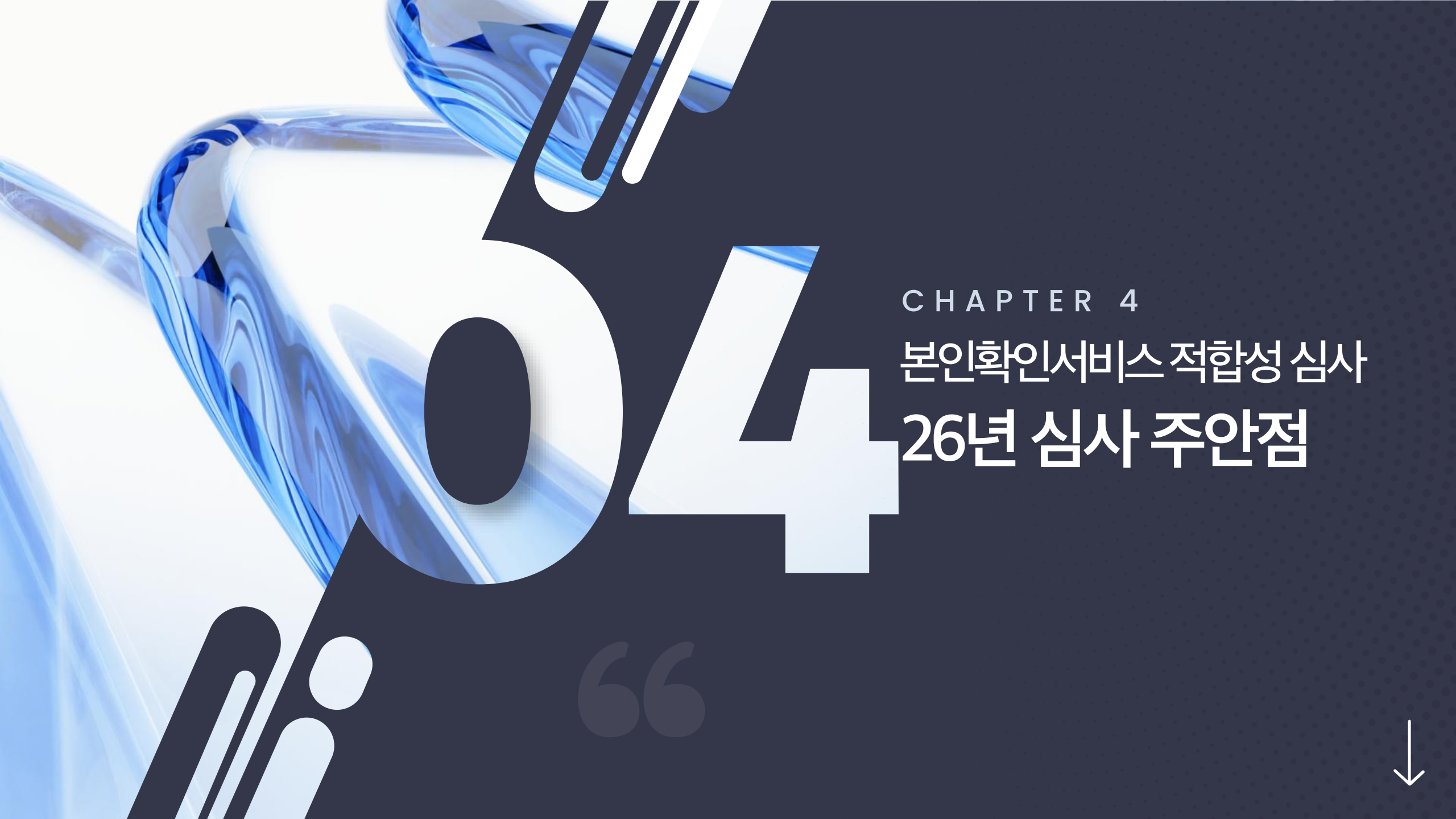
개인정보 파기에 관한 사항을【4.2.가】(개인정보의 수집·이용목적, 수집하는 개인정보 항목, 개인정보의 보유 및 이용기간을 이용자에게 고지하고 동의를 받아야 함) 항목으로 적용 · 심사 중

변경사항(To-Be)

「본인확인기관 지정 등에 관한 기준」 고시 및 해설서 개정을 통해 개인정보 파기에 관한 심사항목 신설

6. 기타 고려중인 사항

- 본인확인기관 유효기간제 도입(3년)
- 보완사항에 대한 시정명령 근거 조항 마련
- 연계정보 처리 범위 규정 개선



04

CHAPTER 4

본인확인서비스 적합성 심사
26년 심사 주안점

26년 심사 주안점

발급(대체수단 발급 시 신원확인, 구비서류, 유일성, CI/DI 처리 등)

본인확인기관의 허무인 검증 프로세스

허무인 검증 프로세스를 확인하고 해당 주기가 적절한지에 대한 확인

법적근거 없는 CI(미점유 인증, 실명인증서비스 등)에 대한 확인

모든 법적근거 없는 CI사용은 허용하지 않음

발급/폐지/인증 시 알림

발급 및 폐지가 발생할 경우 사용자에게 통지하는지 확인
메일로 통지 시 입력한 메일주소에 대한 형식 검증 확인(예, A@A.com 등과 같은 비 정상적인 주소 검증 여부)

비대면 신원확인 단계에서 안면인식 기술을 사용할 경우, 안면인식 기술의 신뢰성을 보장하기 위한 방안

안면인식 기술을 고도화 하는 방안 외에도 인증 후 수작업 검토 등 안면인식을 통한 신원확인의 신뢰성을 보장할 수 있는 방안의 적절성 여부 점검

말소된 외국인 등록정보 진위확인 실시간 연동 점검

허무인 검증 프로세스를 확인하고 해당 주기가 적절한지에 대한 확인
외국인 명의 도용 대포폰/계정 생성 방지를 위해 하이코리아 등 관할 기관과의 말소된 체류 자격 및 유효성 검증 절차 확인

크리덴셜 스터핑 공격 등에 대비 로그인/발급 실패 임계치 설정 및 CAPTCHA적용 검토 여부

예, 5회 실패 시 일정 시간 잠금 후 10회 실패 시 락 등

26년 심사 주안점

물리(시설 보안, 소방관리 등)

장애 대응 절차 및 훈련 계획 점검

본인확인서비스에 대한 BCP(업무 연속성 계획), RTO(복구 목표 시간) 및 RPO(복구 목표 시점) 정책, 장애 대응 절차 수립 내용의 적절성

UPS 및 리튬이온 배터리실이 서버룸과 방화벽 혹은 격실로 구분되고 배선 트레이에 내화 충전재 마감 여부 및 격실 천장으로 송전선 통과 여부 확인

리튬 배터리 사용 시, 전용 소화 장비(전용 소화기, 전용 스프링클러 등) 배치 여부 및 열 감지기 설치를 통한 조기 발화 탐지 가능 여부

배터리 교체/이설 등의 작업 시, 안전 및 작업 관리자 입회 절차 수립 여부 및 비상 대피 훈련 수행 여부

26년 심사 주안점

네트워크(FW, IDS, IPS, IP Scan, NAC, DDoS, VPN, WIPS 등)

외부 노출 자산(API, 인증 연계 서버)에 대한 상시 식별 체계 점검

Shadow IT, 임시 오픈 포트, 공격 표면(Attack Surface) 관리 여부

내부망 횡이동(Lateral Movement) 탐지 및 차단 점검

본인확인 서버와 일반 업무망 간의 불필요한 통신 허용 여부

네트워크 경계에 위치한 장비(라우터, 방화벽, VPN 등)에 대한 취약점 관리 현황 점검

본인확인 서비스 관련 대외 기관 또는 서비스와 연계 시 안전한 통신 채널 사용 여부 점검

(예, Rest API, 전문, 스크래핑 등을 통한 대외 통신 보호대책 점검)

웹 방화벽 설정을 차단 모드가 아닌 단순 탐지 모드 운영 여부

웹 방화벽이 단순 탐지 모드일 경우 다른 보안장비에서 충분한 보호대책을 수행하는지 점검

26년 심사 주안점

개발/암호(형상관리, 소스개발, 검수, 운영이관, 취약점, HSM, KMS 등)

오픈 소스 솔루션 사용 시 공급망 보안 점검 심사 강화

S-BOM(Software Bill of Materials)을 활용하여 오픈소스 소프트웨어의 버전 및 취약점 점검이 이루어지는지 확인
React 및 Next.js 사용 여부 및 등 사용 시, CVE-2025-55182, 66478 취약점에 대한 보안 패치 또는 별도의 보완대책 수립 여부

(해당 시)소스 코드 작성 시 개발자가 아닌 인공지능에 의한 코드 생성 시, 사람에 의한 보안점검 프로세스 점검

소프트웨어 및 본인확인 비즈니스에 LLM, 생성형 인공지능 등 AI 사용 여부 및 AI 사용 시 보안대책 점검

암호키 관리의 적절성

본인확인 관련 설비내 암호자산 식별 및 관리 현황 점검(암호모듈, 암호키, KMS, HSM 등)
암호키에 접근할 수 있는 권한 통제 현황 점검
암호키 생성, 저장, 배포, 사용, 정지, 폐기 등 암호키 생애주기에 따른 안전한 절차 마련 및 이행 여부 점검

코드 취약점, 라이브러리 취약점, 하드코딩 시크릿을 파이프라인 상에서 관리하고 있는지 점검

(예, SAST + SCA + Secret scan)

동일 IP/단말에서 단시간 내 다수 명의의 인증 시도 발생 시, 인증 횟수 제한 정책(FDS)의 유효성 점검 여부

26년 심사 주안점

서버(접근통제·권한, SecureOS, 취약점 스캐닝, 로그분석, 계정관리 등)

보안패치 적용 여부

서버OS 뿐만 아니라 Web, WAS, 미들웨어, DBMS, 보안시스템(특히 VPN), 가상화 S/W 등 패치 관리가 필요한 모든 구성요소에 대한 보안패치 현황을 식별하고 최신 보안패치를 신속히 적용하고 있는지 점검

업무변경, 퇴직 시 지체없는 계정, 접근권한 등의 회수 여부

- 조직변경, 퇴직, 업무변경시 지체없는 계정, 접근권한 회수를 보장할 수 있는 절차의 적정성 및 이행 여부 점검
- 특히, 특수권한(키관리 포함) 보유자의 업무변경, 퇴직시 강화된 통제절차에 따라 조치하고 있는지 여부 점검 (특수계정・권한을 빠짐없이 식별, 관리하고 있는지 여부도 함께 확인)
  ※ 서버뿐 아니라 응용프로그램, DBMS, 보안시스템 등 포함

클라우드 네이티브 보안(Container Security) 점검

- Kubernetes/Docker 환경 운영 시 컨테이너 이미지 취약점 스캔 및 런타임 보안 솔루션 적용 여부
- 컨테이너의 Root 권한 구동 제한 및 Pod 간 네트워크 격리 정책 확인

리눅스 서버 대상 악성코드 탐지·대응 수단 운영 현황 점검

본인확인 AP 서버 내 타 서비스 데몬이나 처리 로직을 운영하고 있는지 점검

관리자 접속 시 VPN/IP 통제 이외에 접속 단말의 보안 솔루션(백신, OS패치) 설치 및 설정 검증 여부 및 MFA 필수 적용 여부

26년 심사 주안점

심사 주안점

모듈/앱(시나리오, 인증우회, 위·변조, 원격제어, 화면캡처, 피싱방지 등)

구버전 모듈에 대한 관리 및 조치방안

구버전 배포 현황, 구버전을 신버전으로 교체 및 구버전 사용 시 신버전 전환 계획 확인

AOS 모바일앱 한정하여 전화번호를 가져가기 위해 USIM에 접근하기 위한 사용자 동의

- 앱 설치시 필요한 정보를 가져가기 위해서 사용자 동의를 받고 있는지 확인

아이핀, 인증서 기관 등 대행사 추가에 대한 현황 확인

- 대행사 추가에 대한 계약관계 및 연동현황, 기존 인증대행사의 보안 수준과 모듈관리에 대한 현황 점검 확인

악성 앱 탐지 및 실행 차단 연동 점검

- 본인확인 앱 실행 시, 단말기 내 악성 앱 설치 여부를 탐지하고 실행을 중단시키는 기능의 유효성 및 루팅 탐지 확인

앱 무결성 검증 및 안티 디버깅 강화 확인

- Frida, Xposed 등 후킹 툴을 이용한 메모리 변조 시도 탐지 및 앱 강제 종료 기능 확인
- 소스코드 난독화 수준이 최신 디컴파일러에 대응 가능한 수준인지 확인

매크로 등 자동화된 방식으로 비정상적인 본인확인 서비스 이용 시도에 대한 탐지·대응 현황 점검

- 매크로 등 자동화된 방식의 서비스 이용에 대한 탐지 및 챌린지 적용 여부 등 확인

26년 심사 주안점

심사 주안점

취약점진단(주요정보통신기반시설 분석·평가 기준, CSAP 기준 등)

최신 변경된 취약점 점검 프로세스 및 조치 결과 상세 확인 점검

- 2026년 변경된 기반시설 기술적 취약점 분석 • 평가 방법 상세 가이드에 따른 준비 및 수행 점검
- 2026년 변경된 금융보안원의 취약점 분석 • 평가 기준 개정에 따른 취약점 점검 준비 및 수행 점검

본인확인 주요설비 샘플링 점검

- 기반시설로 등록된 본인확인AP, 본인확인 DB에 대한 샘플링 취약점 점검

비즈니스 로직(Business Logic) 취약점 진단 강화

- 인증 단계 건너뛰기, 파라미터 변조를 통한 타인 명의 인증 등 프로세스상의 허점을 파고드는 시나리오 기반 모의해킹 수행 여부 확인

하이퍼바이저 취약점 관리 현황 점검

(예, VMware ESXi, MS Hyper-V, Nutanix AHV(Acropolis Hypervisor) 등)

26년 심사 주안점

심사 주안점

DB/준법(데이터 암호화, 접근통제·권한, 모니터링, 감사, 파기, 법규 현행화 등)

개인정보 보호법 및 시행령, 고시내용 반영여부

- 개인정보 보호법 적법체계로의 변화에 따른 대응의 적절성
  (정보주체 동의 이외의 다른 적법요건 활용 가능, 동의를 받을 경우 보호법 시행령 제17조제1항 준수 필요 등)
- 개인정보 처리방침 작성지침의 요건에 맞도록 개인정보 처리방침이 마련되어 있는지 점검
  (동의를 받아 처리하는 개인정보와 동의없이 처리하는 개인정보를 구분하여, 법적 처리근거 및 개인정보항목을 알리고 있는지 여부 등)
- 개인정보의 안전성 확보조치 기준 고시 개정사항 반영 여부
  (내부 관리계획 18개 항목, 접속기록 점검 관련 요건 개정 등)

본인확인 서비스 관련 DBMS에 불필요한 타 데이터베이스 간 링크나 procedure, function 등 운영 여부 점검

26년 심사 주안점

대체수단(대체수단별 특성에 따른 별도 점검사항)

공통

재외국민 비대면 인증에 대한 보호조치 점검

- 정상 인증인지 도용인지 확인하는 방안, 인증 국가 제한 현황, 인증 시 인증하는 사람과 발급받은 사람이 동일인 인지 여부 등 확인

회원가입용으로 수집한 CI값에 대한 분리저장 및 암호화 저장 사전 안내

- 법적용에는 유예기간이 남아있으나, 회원가입용 수집한 CI정보에 대하여 고객 마스터 DB에서 주민등록번호와 CI 분리 저장 및 암호화 저장 사전 안내

아이핀

장기 미사용 계정에 대한 재인증 절차 점검

- 장기간 미사용 계정이 별도의 재인증 절차(비대면 실명확인 등) 없이 로그인만으로 활성화되어 도용되는 것을 방지하는 절차 확인

26년 심사 주안점

대체수단(대체수단별 특성에 따른 별도 점검사항)

인증서

인증서 발급시 사용자에게 발급 위치 선택권 점검

- 발급되는 인증서의 위치가 이용자가 인지하고 선택할 수 있는지 확인

대체수단 유일성에 대한 점검

- 알 수 없는 오류로 발급된 인증서가 존재하는지 확인

클라우드 인증서 저장소 접근 통제

- 클라우드 기반 인증서 서비스 이용 시, 저장소에 대한 접근 권한 관리 및 부정 접근(비정상 트래픽) 탐지 체계 확인

휴대폰

통신사 본인확인기관 인증 대행사 점검

- 인증 대행사 사전점검 수행

SMS 본인확인 시 사용자에게 노출되는 문구 점검

- 사용자에게 노출되는 문구는 본인확인기관명으로 하고 있는지 확인

비대면 대체수단 발급 시 본인확인을 수행하고 있는지 확인

- 간편인증이 아닌 본인확인을 통한 인증을 수행하는지 점검

비대면 개통 절차에 안면인증 의무화 관련 사항 점검

- 신분증 및 안면인증 결과에 따른 동일인 여부 점검 방안 확인

05

CHAPTER 5

참석자 질의응답

안전하고 편리한 온라인 본인확인서비스 제공

The end.

감사합니다.