2024. 2.

본인확인기관 지정 등에 관한 기준

지정·정기심사 평가기준 해설서

방송통신위원회
Korea Communications Commission

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

「본인확인기관 지정 등에 관한 기준」

지정·정기심사 평가기준 해설서

CONTENTS

1장

서론

2장

본인확인기관 평가기준 해설

참고자료

「본인확인기관 지정 등에 관한 기준」

지정·정기심사 평가기준 해설서

1장 서론

Ⅰ. 해설서 개요

Ⅱ. 해설서 운영계획 및 개정절차

Ⅰ | 해설서 개요

■ 목적

- 신규 본인확인기관으로 지정받고자 하는 예정 사업자 및 기존 본인확인기관을 대상으로 본인확인기관 평가기준에 대한 이해도를 제고하기 위함

■ 필요성

- 정보통신서비스 이용자가 안전하고 편리하게 본인확인서비스를 이용할 수 있도록 본인확인기관의 보호 수준을 제고하기 위한 참고자료가 필요함
- 심사대상 사업자의 본인확인기관 평가기준에 대한 해석 오류로 인하여 심사대상 사업자가 지정심사 탈락, 지정취소 등이 발생되지 않도록 명확한 기준을 제시할 필요*가 있음

  * 정부 행정력, 사업자 인력·개발비용 등의 자원 낭비를 최소화하기 위함

■ 심사대상 법인

- 「정보통신망법」 제23조의3에 따라 신규 본인확인기관을 지정 받고자 하거나 기존 본인확인기관의 지위를 유지하는 경우에 지정기준을 충족하고 있는지 여부를 지정·정기심사를 통해 확인

구분	심사대상
지정심사	• 방송통신위원회 심사계획에 따라 신규 본인확인기관으로 지정받고자 신청한 법인
정기심사	• 방송통신위원회로부터 본인확인기관으로 지정받은 법인

※ 본인확인기관 지정현황('23년말 기준)

대체수단	본인확인기관
아이핀	NICE평가정보, SCI평가정보, 코리아크레딧뷰로
휴대폰	SK텔레콤, 케이티, LG유플러스
신용카드	국민카드, 롯데카드, 삼성카드, 신한카드, 하나카드, 현대카드, 농협은행
인증서	금융결제원, 코스콤, 한국전자인증, 한국정보인증, 한국무역정보통신, 비바리퍼블리카, 국민은행, 신한은행, 하나은행, 카카오뱅크, 우리은행

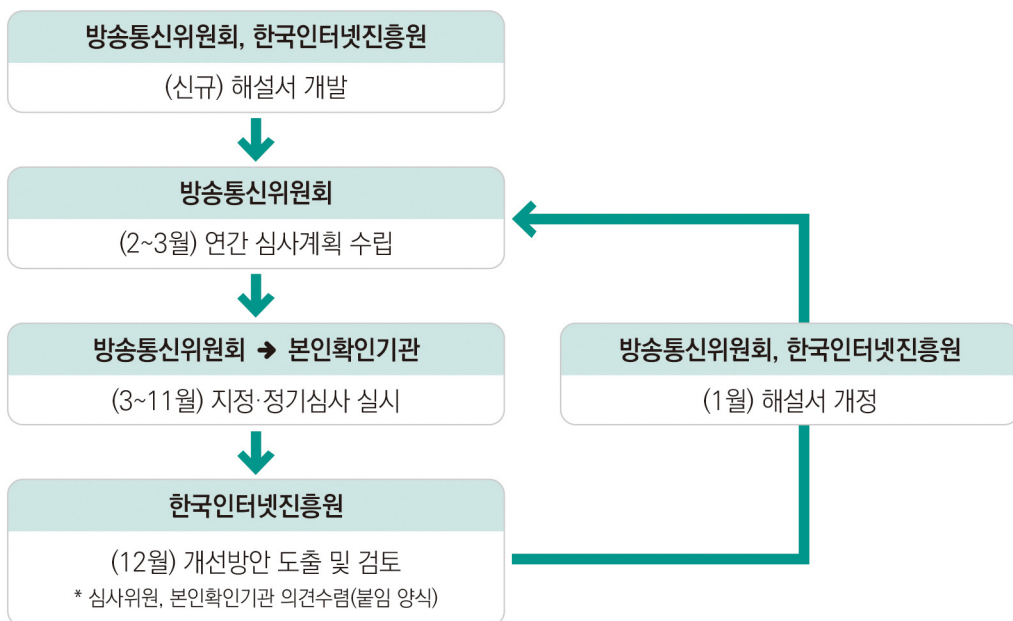
Ⅱ | 해설서 운영계획 및 개정절차

■ 운영 계획

- 본 해설서에서 명시한 내용을 기준으로 본인확인기관 지정·정기심사 실시
  - 명시되지 않은 내용도 심사대상 사업자가 조기에 인지하여 조치할 수 있도록 개선 안내
  - 해당 내용에 대하여 세부사항 검토하여 해설서 개정절차에 따라 내용 반영
- 본인확인기관은 본 해설서에서 제시한 평가기준을 우선 적용하되, 다른 법령에서 상이한 기준을 제시하고 있는 경우에는 더 높은 기준을 준수토록 함
  - 이후 세부 사항을 검토하여 결정된 개정내용을 아래의 개정 절차에 따라 해설서 반영

■ 개정 절차

- 지정·정기심사에서 도출된 사항에 대하여 심사위원, 본인확인기관 등 의견수렴 및 법률·기술 전문가 자문을 통해 개정 여부 결정



※ 상기 일정은 연간 사업계획에 따라 변동될 수 있음

「본인확인기관 지정 등에 관한 기준」

지정·정기심사 평가기준 해설서

2장 본인확인기관 평가기준 해설

Ⅰ. 물리적·기술적·관리적 조치계획

Ⅱ. 기술적 능력

Ⅲ. 재정적 능력

Ⅳ. 설비규모의 적정성

Ⅰ | 물리적·기술적·관리적 조치계획

1. 본인확인업무 관련 설비의 관리 및 운영에 관한 사항

1-1. 물리적 출입 및 접근 통제

1.1.가 비인가자 출입통제 및 감사

(1) 비인가자가 본인확인업무 관련 발급·관리 설비 운영실에 접근할 수 없도록 하는 물리적인 출입통제 기능

(2) 일련번호, 사건의 유형, 성공·실패 여부 및 실패 시 원인, 일자 및 시각, 행위자 등에 대한 정보의 감사기록 기능

■ 심사내용 설명

기준	주요 내용
보호구역	• 본인확인업무 관련 설비 운영실은 보호구역으로 지정하여 관리
출입권한	• 보호구역에 대한 출입권한 등록·삭제는 별도 신청하여 관리 • 본인확인업무 관련 보호구역에 비인가자가 접근·출입할 수 없도록 차단하여 본인확인설비에 대한 안전성을 확보
출입기록	• 출입기록은 즉시 확인할 수 있도록 출입통제 시스템 등을 통해 관리 ※ 출입통제 저장정보: 일련번호, 행위자, 출입유형(IN/OUT), 출입위치, 성공/실패 여부, 실패 원인, 일자/시간 등 • 출입기록은 최소 6개월 이상 보관

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

– 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

심사 대상

- 본인확인설비 보호구역(전산센터, 시스템 운영실, 보안관제실 등)
- 문서고(대체수단 발급서류, 개인정보 등 중요서류 보관소)

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 보호구역 출입절차 및 출입권한 등록절차 설명자료 • 본인확인서비스 관련 시스템 자산 목록 • 출입통제 장치 종류 및 운영사진 • 보호구역 배치도 (본인확인업무 관련 설비 위치, 출입동선 표시) • 출입권한 부여인원 현황 (이름, 등록기간, 담당업무, 등록사유 등)
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 설명 • 보호구역(전산센터, 운영실, 관제실) 담당자 – 보호구역 출입동선, 출입절차 설명 – 보호구역 출입권한 등록인원 및 등록사유 설명
현장실사	• 주요 물리적 보호구역에 대한 적절한 보호대책을 수립하고 있는지 확인 • 보호구역에 대한 비인가자 접근 시 출입을 통제할 수 있는지 확인 • 출입 동선상 통제되지 않은 출입문 및 우회경로가 있는지 확인 • 인가된 상시 출입자에 대한 주기적 검토 확인 • 보호구역 출입권한자 중에 불필요한 인원이 포함되어 있는지 확인 • 임시 출입자의 출입절차(카드키 반출입 등)의 적절성 확인 • 출입 이벤트 발생 시 출입내역을 기록하고 관리하는지 확인 • 보호구역 출입내역을 확인 하여 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 이상행위에 대한 감사절차가 있는지 확인

사례 검토

미흡사례 1	• 출입권한에 대한 주기적 검토 없이, 퇴사한 직원의 출입권한이 회수되지 않고 방치
미흡사례 2	• 본인확인업무 관련 설비에 대한 출입 실패기록이 저장되지 않고 있음
미흡사례 3	• 출입대장의 관리를 적절히 수행하고 있지 않아, 인터뷰에서 확인된 시스템 작업일자에 작업자의 출입기록이 남아있지 않음

1.1.나 생체특성기반(지문인식, 홍채인식 등)을 포함하는 2개 이상의 출입통제장치를 사용하는 기능

■ 심사내용 설명

기준	주요 내용
출입통제장치	• 본인확인업무 관련 보호구역에 생체특성기반을 포함하는 2개 이상의 출입통제 장치 확보하여야 함 ※ 신원확인이 가능한 생체특성의 종류(예) : 지문, 얼굴, 홍채, 음성, 손모양, 손등 정맥, 서명 인식 등
출입권한	• 생체특성기반 출입통제장치에 출입 권한 등록, 변경, 삭제 등 관리
출입기록	• 출입기록은 즉시 확인 가능하도록 출입통제 시스템 등을 통해 관리 ※ 출입통제 저장정보: 일련번호, 행위자, 출입유형(IN/OUT), 출입위치, 성공/실패 여부, 실패 원인, 일자/시간 등 • 출입기록은 최소 6개월 이상 보관

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 생체특성기반 출입통제장치
- 생체특성기반 출입통제장치에 대한 출입권한 등록, 변경 및 삭제
- 생체특성기반을 포함하는 2개 이상의 출입통제장치에 대한 출입기록 및 감사기록

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 생체특성기반 출입통제 장치 종류 및 운영 사진 • 생체특성기반 출입절차 및 출입권한 등록절차 설명자료 • 생체특성기반 출입통제 장치 및 배치도(설비 위치, 출입동선 표시) • 출입권한 부여인원 현황(이름, 등록기간, 담당업무, 등록사유 등) • 생체특성기반 출입통제 시스템 감사기록 예시
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 내 출입통제 관련 내용 설명 • 생체특성기반 출입통제 장치 담당자 – 생체특성기반 출입방법, 출입절차 설명 – 생체특성기반 출입권한 부여인원 및 감사기록 관리 과정 설명
현장실사	• 2종 이상의 생체특성기반 출입통제 장치를 적용하고 있는지 확인 • 생체특성기반 출입통제 장치에 권한 등록 과정 및 현황 확인 • 인가된 출입자의 감사기록에 대한 주기적 검토 여부 확인 • 생체특성기반 출입통제 장치에 불필요한 인원의 포함 여부 확인 • 출입내역을 확인하여 생체특성기반 출입통제 장치 내 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 실패 사유에 대한 감사절차가 있는지 확인

■ 사례 검토

미흡사례 1	• 보호구역 내 출입권한이 부여되지 않은 사용자가 생체특성기반 출입기록에서 확인됨
미흡사례 2	• 생체특성기반 출입통제 장치에 대한 실패기록이 저장되지 않고 있음
미흡사례 3	• 보호구역 출입 시 생체특성기반의 출입통제장치를 거치지 않고 우회하여 출입할 수 있는 통로가 확인됨

1.1.다 감사기록의 저장 및 백업

(1) CCTV 등을 통해 발급시스템 운영실을 감시·통제하는 기능
(2) 24시간 감시·통제에 대한 감사기록을 저장 및 백업하는 기능
(3) CCTV 시스템의 시간동기화 기능

■ 심사내용 설명

기준	주요 내용
CCTV 설치	• 본인확인업무 관련 설비가 위치한 곳에 CCTV 등을 설치 ※ CCTV는 24시간 운용하되 동작감지 기능 활용 가능 • CCTV 시스템 내 시간동기화(NTP 등) 기능을 적용
영상기록	• CCTV 영상기록을 저장하여 관리 ※ 시간, 위치 등이 특정 가능하여야 함 • 영상기록은 최소 6개월 이상 보관

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인업무 관련 설비를 감시·통제하는 CCTV 장비
- CCTV 감사기록에 대한 저장, 보관 및 백업
- CCTV 기반 24시간 감시·통제 장치 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 장비 목록 • 본인확인업무 관련 설비에 대한 CCTV 배치도 • CCTV 장치에 적용된 시간동기화 방법 및 적용 사진 • CCTV 감사기록에 대한 저장 및 보관주기 설정 사진 • CCTV 감사기록 저장 및 백업 관련 내부 규정 • CCTV 감사기록에 대한 주기적 백업 및 보관 증적

구분	준비사항
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 내 감사기록 저장 및 백업 관련 내용 설명 • CCTV 기반 24시간 감시·통제 장치 운영 담당자 – CCTV 장치 운영, 시간동기화 및 저장/백업 절차 설명 – CCTV 사각지대 여부 및 감사기록 저장/백업 과정 설명
현장실사	• 본인확인업무 관련 CCTV 시스템 설치 및 운영 현황 • CCTV 장치에 대한 관리자 및 접근권한 부여 현황 확인 • CCTV 장치에 적용된 시간동기화 방법 및 적용 현황 확인 • CCTV 감사기록에 대한 저장 및 보관주기 현황 확인 • CCTV 감사기록에 대한 주기적 백업 및 보관 방법 확인 • 백업 내부 규정 및 정책 내 CCTV 감사기록 백업 포함 여부 확인 • 보관 및 백업된 CCTV 감사기록에 대한 접근권한 부여 현황 확인 • 자산 목록내 본인확인업무 관련 주요 설비 및 신규 도입 장비에 대한 CCTV 사각지대 존재 여부 확인 • 보호구역내 본인확인업무 관련 설비에 대한 현장 방문 내용이 해당 시간에 CCTV 장치 내에 영상으로 저장되어 있는지 확인

■ 사례 검토

미흡사례 1	• 본인확인 업무 관련 설비에 대한 CCTV 설치·운영시 사각지대가 존재하여 설비에 대한 감시·통제 감사기록이 저장되지 않음
미흡사례 2	• 본인확인업무 관련하여 신규로 도입된 장비에 대한 CCTV가 설치되어 있지 않음
미흡사례 3	• CCTV 감사기록에 대한 주기적 백업이 이행되지 않았거나, 백업 장치내 백업 대상 목록에 누락되어 있음
미흡사례 4	• CCTV 시스템에 시간동기화 설정 기능이 없어 실제 시간과의 오차가 발생함

1-2. 화재·수해 등 재해 대비

1.2.가 화재 예방 및 대책

(1) 화재의 조기 감지 및 진화 계획

(2) 화재설비에 대한 정기점검 시행 및 점검일지 작성

■ 심사내용 설명

기준	주요 내용
비상계획수립	• 본인확인업무 관련 설비에 대한 화재 예방 관련 문서 및 내부 지침 수립
화재대비장치	• 본인확인업무 관련 설비를 대상으로 화재 감지 및 경보 장치 설치 ※ 화재 감지 및 경보 장치의 종류 : 연기 및 열감지, 덕트 감지기, 적외선 감지기 등 ※ 소화기의 종류 : 이산화탄소 소화기(탄산가스 소화기), 할론 소화기, 자동 확산 소화용구 ※ 전산장비가 있는 경우 물을 사용하는 스프링클러 제거 ※ 사용하는 소화제가 인체에 무해한지 확인해야 하며, 유해하다면 소화제 작동 전에 본인확인업무 관련 설비 운영자에게 통지하는 체계 수립
정기점검	• 화재 감지 및 경보 장치에 대한 정기점검(자동 화재감지 설비, 소방서 통보 설비 및 누전경보기 등)을 수행 • 소화설비에 대한 정기점검을 시행하고 점검일지를 작성하여 보관

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인업무 관련 설비에 대한 화재 예방 설비
- 화재 조기 감지 및 진화 계획 수립 현황
- 화재 예방 설비 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 설비에 대한 화재감지 및 경보 장치 현황 • 화재감지 및 경보 장치 구축 현황 사진 • 화재감지 및 경보 장치, 소화설비 및 비상구 등이 표시된 배치도 • 화재감지 및 경보 장치에 대한 정기점검 이행 현황 • 소화설비에 대한 정기점검 시행 현황 및 점검일지 사진 • 화재 대비 관련 문서, 내부 지침 및 비상연락망 현황
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 화재 예방 및 대책 관련 내용 설명 • 화재감지 및 경보 장치, 화재예방 설비 운영 담당자 – 화재감지 및 경보 장치 운영 현황과 정기점검 이행 현황 설명 – 소화설비 작동 방식 및 소화용재 사용 현황 설명 – 화재 발생 시 조기 감지 및 진화 계획 수립 현황 설명 – 화재 발생 시 대응체계 및 비상연락망 수립 현황 설명
현장실사	• 화재 조기 감지 및 진화 계획 수립, 화재 발생 시 비상연락망 • 화재 조기 감지 및 경보 장치 설치 현황 확인 • 화재 감지 및 경보 장치에 대한 정기점검 수행 현황 • 화재 발생 시 진화 계획, 진화 방식 관련 내부 지침 • 본인확인업무 관련 설비 대상 소화설비 구축 및 운영 현황 • 스프링클러 제거 여부 및 사용하고 있는 소화제 확인 • 소화기 비치 또는 자동 확산 소화용구 설치 현황 확인 • 소화설비에 대한 정기점검 시행 및 주기적 점검일지 작성 현황 • 화재 예방 관련 문서 및 내부 지침 수립 내용 확인

■ 사례 검토

미흡사례 1	• 본인확인업무 관련 주요 설비에 대한 화재감지 및 경보 장치가 설치되어 있지 않으며, 화재 설비에 대한 정기점검을 수행하지 않음
미흡사례 2	• 소화설비에 대한 정기점검 이행 내역과 소화용제 교체 작업일지가 비치되지 않으며, 최근 정기점검 및 교체 일시를 확인하기 어려워 소화설비와 소화용제에 대한 정상적인 작동 여부를 확인하기 어려움
미흡사례 3	• 신규 도입된 본인확인업무 관련 주요 설비가 비치된 공간에 스프링클러가 설치되어 있고, 화재감지 및 경보 장치가 설치되어 있지 않음

1.2.나 수해에 대비한 설비의 운영

■ 심사내용 설명

기준	주요 내용
비상계획수립	• 본인확인업무 관련 설비에 대한 수해 대비 관련 문서 및 내부 지침 수립
수해 대비	• 수해 피해가 발생하지 않도록 본인확인업무 관련 설비가 바닥으로부터 일정 간격(30cm 이상 권고) 이격된 상태로 설치
정기점검	• 수해 대비 설비에 대한 주기적 점검 및 관리

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

– 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

● 본인확인업무 관련 설비에 대한 수해 예방 설비

● 수해 예방 설비 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 수해 대비 설비에 대한 운영 및 관리 현황 • 본인확인업무 관련 설비 바닥 이격(30cm 이상) 설치 현황 사진 • 본인확인업무 관련 설비 전원접속장치 바닥 이격 설치 현황 사진 • 기타 본인확인업무 관련 설비에 대한 수해 예방 장치 운영 현황 • 수해 대비 관련 문서, 내부 지침 및 비상연락망
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 수해 예방 및 설비 운영 내용 설명 • 수해 예방 장치, 전원접속 장치 운영 담당자 – 수해 예방 장치 및 전원접속 장치 바닥 이격 설치 현황 설명 – 수해 발생 시 대응체계 및 비상연락망 수립 현황 설명 – 수해 대비 설비에 대한 주기적 점검 및 관리 현황 설명 – 수해 대비 관련 문서 및 내부 지침 수립 현황 설명

구분	준비사항
현장실사	• 수해 대비 설비에 대한 운영 및 관리 현황 • 본인확인업무 관련 설비 바닥 이격(30cm 이상) 설치 확인 • 본인확인업무 관련 설비 전원접속장치 바닥 이격 설치 확인 • 수해 대비 관련 주기적 점검 이행 내역 확인

■ 사례 검토

미흡사례 1	• 본인확인업무 관련 주요 설비가 바닥으로부터 일정 간격(30cm 이상 권고) 이격되지 않았거나 바닥에 배수 처리 기능을 제공하지 않아, 수해 발생 시 본인확인업무 관련 주요 시스템 및 장비가 정상적으로 작동하지 않음

1.2.다 정전 발생 대비 방안

■ 심사내용 설명

기준	주요 내용
비상계획수립	• 본인확인업무 관련 설비에 대한 정전 대비 관련 문서 및 내부 지침 수립
전원공급장치	• 정전 발생 시 본인확인업무의 수행이 가능하도록 전원공급장치 운영 ※ 전원공급 장치별 확인사항 가. 전원공급 장치(UPS) : 공급 용량 및 시간, 배터리 유효기간 등 나. 발전설비 : 발전용량, 연료 확보 여부 등 • 전원공급장치는 발전설비 가동 시까지 유지할 수 있는 충분한 용량(예: 20~30분)을 갖추어야 하며, 발전설비가 가동되어 전환될 수 있도록 하여야 함
정기점검	• 전원공급장치에 대한 주기적 점검 및 관리

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 정전 발생 대비 설비
- 정전 발생 대비 설비 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 지속적인 업무 수행이 가능하도록 전원공급 설비 운영 현황 • 무정전 전원공급 장치(UPS) 공급 용량, 시간, 배터리 유효기간 등 • 발전설비 용량 현황 사진 • 전원공급 장치에 대한 주기적 점검 및 관리 현황 사진 • 정전 대비 관련 문서, 내부 지침 및 비상연락망

구분	준비사항
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 정전 대비 전원공급 설비 운영 내용 설명 • 정전 대비 및 전원공급 설비 운영 담당자 – 무정전 전원공급 장치(UPS), 발전설비 운영 현황 설명 – 정전 발생 시 대응체계 및 비상연락망 수립 현황 설명 – 전원공급 설비에 대한 주기적 점검 및 관리 현황 설명 – 정전 대비 관련 문서 및 내부 지침 수립 현황 설명
현장실사	• 정전 대비 전원공급 설비에 대한 운영 및 관리 현황 • 무정전 전원공급 장치(UPS), 발전설비 운영 현황 확인 • 무정전 전원공급 장치(UPS)를 통해 공급 가능한 전력량, 시간 및 배터리 유효기간 확인 • 발전설비를 통해 공급 가능한 전력량 확인 • 정전 대비 전원공급 설비에 대한 주기적 점검 이행 내역 확인

■ 사례 검토

미흡사례 1	• 발전설비가 별도로 없는 상태에서 무정전 전원공급 장치(UPS)의 공급 용량이 작고 전원 공급 시간이 짧으며 배터리 유효기간도 지나 본인확인업무 관련 설비에 대한 정전 발생 시 지속적이고 안정적인 운영이 어려움
미흡사례 2	• 정전 발생 시 발전설비를 통해 공급 가능한 전력량이 본인확인업무 관련 주요 설비 운영에 필요한 최소 전력량보다 부족하여 지속적이고 본인확인서비스의 안정적인 운영이 어려움

1.2.라 시스템의 항온항습 유지 방안

■ 심사내용 설명

기준	주요 내용
비상계획수립	• 본인확인업무 관련 설비에 대한 항온항습 유지 관련 문서 및 내부 지침 수립
항온항습장치	• 항온항습장치를 통해 온도 및 습도를 일정하게 유지하여 본인확인업무 관련 설비에 대한 안정적 운영 ※ 본인확인업무 관련 설비에 대한 온도 및 습도 기준 가. 온도 : 18±2°C 나. 습도 : 50±5%
정기점검	• 온도·습도의 주기적 점검 및 관리

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 항온항습장치 운영 현황
- 본인확인업무 관련 설비에 대한 항온항습 유지 방안

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 설비에 대한 항온항습장치 설치 현황 • 본인확인업무 관련 설비 온도 점검일지 및 관리 현황 사진 • 본인확인업무 관련 설비 습도 점검일지 및 관리 현황 사진 • 항온항습 유지 관련 문서 및 내부 지침
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 또는 기관 내 항온항습 운영 지침 내용 설명 • 항온항습 설비 운영 담당자 – 항온항습 설비 운영 현황 설명 – 항온항습 관련 문서 및 내부 지침 수립 현황 설명

구분	준비사항
현장실사	• 본인확인업무 관련 설비에 대한 항온항습 유지 관련 문서 및 내부 지침 확인 • 항온항습 설비에 대한 주기적 점검 이행 내역 확인 • 본인확인업무 관련 설비에 대한 현장 방문 시 온도 및 습도를 확인하고 내부 지침에서 정한 범위에 해당하는지 확인

사례 검토

미흡사례 1	• 본인확인업무 관련 설비가 비치된 보호구역 내 온도가 내부 지침과 달리 매우 높고, 환풍구 등을 통한 예열 저감 기능 등도 원활하지 않아 시스템 과열(전기회로 오동작) 등으로 인해 본인확인서비스의 안정적인 운영이 어려움
미흡사례 2	• 본인확인업무 관련 설비가 비치된 보호구역 내 습도가 내부 지침과 달리 매우 높고, 습기 제거 기능도 원활하지 않아 정전기 발생(시스템 오동작) 등으로 인해 본인확인서비스의 안정적인 운영이 어려움

2. 정보통신망 침해행위의 방지에 관한 사항

2-1. 침입차단·탐지·방지 시스템

2.1.가 CC EAL2등급 이상의 Firewall, IDC 또는 IPS 운영

■ 심사내용 설명

기준	주요 내용
CC 인증	• 모든 Firewall, IDS 또는 IPS에 대한 EAL(보증) 등급 확인 – 인증서를 통해 EAL(보증) 등급 확인 및 만료일자를 확인 ※ (국내제품) IT보안인증사무국(www.itscc.kr) 참고 ※ (해외제품) CCRA(www.commoncriteriaportal.org) 참고 – 등급 구분이 없는 해외제품의 경우에는 CC인증 여부만 확인
인증 만료시	• CC인증의 유효기간이 만료 대응계획 확인 – CC인증서 만료기간의 잔여기간이 6개월 미만일 경우, 제조사의 인증서 갱신 절차의 진행 여부 확인하고 보안패치 제공 등의 제조사 지원내용을 확인 – CC인증서 유효기간 만료된 제품에 대해 장비 교체 등에 관한 계획 수립 및 위험관리 책임자 승인 여부 확인 ※ 만료일로부터 6개월 이내 교체

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인서비스를 보호하기 위해 접근통제규칙을 적용하는 모든 Firewall
- 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 구성도(Firewall, IDS 또는 IPS 명기) • 인증서 또는 Certification Report
담당자 인터뷰	• firewall, IDS 또는 IPS 담당자 – 각 시스템별 용도 설명 • 네트워크 담당자 – 본인확인시스템 관련 네트워크 및 트래픽 흐름에 대한 설명
현장실사	• CC인증서의 시스템과 운영 중인 시스템이 동일 시스템인지 확인 – 시스템의 모델명, OS 버전 등을 시스템 내에서 확인 – 시스템 내 정보와 인증서 정보가 일치하는지 확인

■ 사례 검토

미흡사례 1	• 심사 대상인 Firewall, IDS 또는 IPS가 EAL2 미만의 제품으로 운영되고 있음
미흡사례 2	• 심사 대상인 Firewall, IDS 또는 IPS의 CC인증서의 유효기간이 만료되었고, 제조사에서도 기술지원 제공 계획이 존재하지 않음에도 장비 교체계획이 수립되지 않음
미흡사례 3	• 심사 대상인 Firewall, IDS 또는 IPS의 CC인증서의 유효기간의 만료가 3개월 미만이고, 제조사에서 CC인증서 갱신을 계획하고 있지 않음에도 이에 대한 대책이 마련되어 있지 않음

2.1.나 본인확인업무에 한정된 접근통제규칙을 설정하여 사용

■ 심사내용 설명

기준	주요 내용
등록절차	• 접근통제규칙을 등록/변경/삭제하기 위한 공식적인 신청 절차 수립
접근통제규칙	• 접근통제규칙에 대한 점검 및 관리 – 모든 규칙이 공식적인 신청 절차를 통해서 설정된 규칙인지 확인 – 모든 규칙이 본인확인업무에 필요한 접근통제규칙인지 확인 – 신청 목적에 비해 과도하게 허용된 규칙이 존재하는지 확인 – 양방향 통신 허용, 보안에 취약한 Telnet, FTP 서비스 허용 등 보안에 취약한 규칙이 존재하는지 확인 – 접근제어시스템 등을 우회하는 예외 규칙이 있는지 확인 – L4의 slb(static load balancing)설정을 이용하여 우회하는 설정이 존재하는지 확인
주기적검토	• 접근통제규칙에 대하여 아래 내용을 주기적으로 검토 – 불필요한 규칙, 미승인 규칙, 장기간 미사용 규칙(Hitcount 0), 과도하게 허용된 규칙, 보호체계 우회 규칙 등

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인서비스를 보호하기 위해 접근통제규칙을 적용하는 있는 모든 Firewall
- ACL 등으로 일부 접근통제규칙을 적용한 네트워크 장비

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 구성도(Firewall) • 자산목록(Firewall) • IP주소목록(내부 네트워크 Vlan별 IP주소 및 용도) • Firewall 접근통제규칙(룰셋) • 네트워크 장비 Config
담당자 인터뷰	• firewall 담당자 – 심사대상인 Firewall 별 용도 설명 – 접근통제규칙의 신청 및 등록하는 절차에 대한 설명 – 접근통제규칙의 적정성에 대한 주기적 검토 절차에 대한 설명 – 접근통제규칙의 원칙에 대한 설명 – 등록된 접근통제규칙의 용도에 대한 설명 – 접근통제규칙의 예외 규칙에 대한 근거 및 설명 • 네트워크 담당자 – 본인확인시스템 관련 네트워크 구성 현황에 대한 설명 – 본인확인시스템 관련 트래픽 흐름에 대한 설명 – 사용자망, 중요단말망, 대외계, 본인확인시스템망, 기타 연계망 등에 대한 IP체계 및 Vlan, Routing 등 현황 설명
현장실사	• Firewall의 접근통제규칙 확인 • 네트워크 장비의 Config 확인

■ 사례 검토

미흡사례 1	• 출발지/목적지 IP주소, Service Port가 Any로 과도하게 허용되고 있는 규칙이 존재
미흡사례 2	• 보안에 취약한 Telnet과 FTP 서비스로의 접근을 허용하는 규칙이 존재
미흡사례 3	• 서버접근통제시스템에서 서버팜으로 접근을 양방향(Two-way) 허용하여 서버팜의 서버에서도 서버접근통제시스템으로 접근이 가능

2.1.다 모든 트래픽에 대한 점검 및 침입 탐지

■ 심사내용 설명

기준	주요 내용
트래픽 탐지	• 본인확인시스템의 모든 트래픽에 대하여 이상징후를 탐지 – 이상징후에 대한 패턴 업데이트를 수행하고 있는지 확인 – 네트워크 구성도에서 우회경로가 존재하는지 확인
트래픽 차단	• 이상 트래픽이 확인되는 경우 해당 트래픽에 대하여 차단하여야 함 – Firewall 연동 : 출발지 IP 등 약속된 정보를 연동된 Firewall에 전달하여 차단 – Reset Signal : 출발지/목적지 IP주소지에 TCP Reset 패킷을 전달하여 TCP 세션이 종료는 방법으로 차단 – 네트워크 장비: IPS 등을 이용한 이상 트래픽 차단 • IDS 및 IPS의 탐지/차단 옵션을 최적화하였는지 확인

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

– 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

● 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 구성도(IDS 또는 IPS 명기) • IDS, IPS의 연결방식 및 차단방식 설명자료 • Mirror 네트워크 장비 Config

구분	준비사항
담당자 인터뷰	• IDS/IPS 담당자 – 본인확인시스템 관련 내부 트래픽을 감시하고 침입 탐지하는 IDS 또는 IPS의 용도 설명 – IDS 및 IPS의 트래픽 감시 및 차단 방식에 대한 설명 – IDS 및 IPS의 패턴 정책에 차단 옵션 적용 여부 및 현황 대한 설명 – IDS 및 IPS의 SSL 가시화 적용 현황에 대한 설명 • 네트워크 담당자 – 본인확인시스템 관련 네트워크 구성 현황에 대한 설명 – 본인확인시스템 관련 트래픽 흐름에 대한 설명
현장실사	• IDS 또는 IPS의 연동/차단 방식 및 패턴 정책 등 확인 • IDS 또는 IPS의 SSL 가시화 적용 확인 • 네트워크 장비의 Config 확인

사례 검토

미흡사례 1	• IDS 및 IPS 패턴 정책의 학습을 위해 학습모드(탐지 옵션만 설정)로 3개월이 초과되었으나, 차단 옵션을 적용하고 있지 않음
미흡사례 2	• 대행사와 연동 시 SSL을 통한 통신으로 처리하고 있으나, SSL 가시화가 적용되지 않아 IDS 또는 IPS가 해당 트래픽에 대한 감시가 불가능함

2.1.라 새로운 패턴의 침입유형에 대한 추가 기능

■ 심사내용 설명

기준	주요 내용
패턴 업데이트	• 새로운 패턴의 침입유형에 대한 추가 기능(LiveUpdate 또는 수동 업데이트)을 수행 • 현장실사 당일 기준으로 최신 패턴을 업데이트 했는지 확인 • 침입탐지 및 차단 결과에 대하여 주기적인 검토를 수행 – 과도하게 많이 발생되거나 자주 발생되는 오탐 검토 – 서비스 영향으로 차단 옵션을 비활성화한 패턴에 대한 적절성 검토 – 업데이트된 패턴에 대한 학습(탐지만 활성)기간 종료에 따른 차단옵션 활성화에 대한 필요성 검토

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

– 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

● 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 구성도(IDS 또는 IPS 명기) • IDS 또는 IPS의 신규 패턴 업데이트 적용 이력 • IDS 또는 IPS의 신규 패턴별 탐지/차단 옵션 적용 현황
담당자 인터뷰	• IDS/IPS 담당자 – 신규 패턴 확인 방법 및 업데이트 방법 설명 – 신규 패턴 적용 전 영향도 검토 등의 절차 설명 – 신규 패턴 적용 시 학습모드 적용 여부 설명 – 신규 패턴의 탐지/차단 이벤트에 대한 분석 및 후속조치 등에 대한 설명
현장실사	• IDS 또는 IPS 등 시스템에서 업데이트 방법, 절차 및 적용 현황 등 확인

■ 사례 검토

미흡사례 1	• 신규 패턴을 수동으로 업데이트하도록 하였으나, 6개월간 신규 업데이트 절차가 이행되지 않음

2.1.마 침입이 탐지되었을 경우 이를 관리자에게 알리는 기능

■ 심사내용 설명

기준	주요 내용
알림기능	• IDS 또는 IPS에 대한 관제 방법 및 탐지 이벤트 발생 시 대응 절차 등에 대해 확인 – 통합보안관제 범위에 IDS 또는 IPS가 포함되어 있는 경우, 침입 탐지/차단 이벤트 발생 시 통보 방법 및 절차 확인 – IDS 또는 IPS를 단독으로 관제할 경우, 침입 탐지/차단된 이벤트를 관리자가 즉각 감지(예: 소리, SMS 등)할 수 있는지 확인 – IDS 또는 IPS 관련 침입 탐지된 이벤트에 대한 정탐 여부 분석 및 대응 절차 확인
분석 및 보고	• 일간, 주간, 월간 리포트 등 주기적으로 침입탐지 내역 분석 – 통합보안관제 중일 경우 관제 리포트 등 분석 보고서를 확인 – IDS 또는 IPS를 단독으로 모니터링할 경우, 별도 분석 및 보고 여부를 확인

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

– 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

● 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS를 대상으로 지정

– 본인확인시스템만 위치하고 있는 네트워크 영역(Zone)의 트래픽을 모니터링하는 IDS 또는 IPS

– 본인확인서비스 트래픽이 경유하는 각 외부 연결 지점(관문, 대외계 등)에 설치된 IPS

– 별도의 본인확인서비스 네트워크 영역을 감시하기 위한 IDS 등이 없을 경우, 내부망 세부 네트워크 영역을 감시하기 위한 IDS 또는 IPS 등이 운영 시 대상에 포함

– UTM, NGFW 등의 Firewall 장비에서 IPS 모듈을 활성화하여 운영 시 대상에 포함

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 침입 탐지 및 차단 결과의 주기적 분석 결과 보고서 • 통합보안관제 별도 운영 또는 위탁 시 제공받는 리포트(일일, 주간, 월간 등) • 보안이벤트 발생 시 보안관제로부터 통보받은 증적(SMS, 이메일 등) • 탐지/차단 이벤트 발생 시 대응 절차
담당자 인터뷰	• IDS/IPS 담당자 – 탐지 및 차단 이벤트 발생 시 대응 절차 설명 – 탐지 및 차단 이벤트 발생 시 모니터링 및 알림에 대한 설명 – 탐지 및 차단 이벤트 발생 시 대응 절차 설명 – 탐지 및 차단 결과에 대한 주기적 분석 및 패턴 정책에 반영 등에 관한 절차 설명
현장실사	• IDS/IPS 관제 현황 확인

■ 사례 검토

미흡사례 1	• IDS 또는 IPS를 단독 관제하고 있으나, 오탐으로 알림 소리가 빈번하게 발생하여 알림 기능을 비활성화하여 침입탐지 이벤트 발생 시 관리자가 즉시 감지 할 수 있는 수단이 없음
미흡사례 2	• IDS/IPS 담당자가 보안관제로부터 탐지 이벤트 통보받는 수단을 이메일로만 하고 있으나, 담당자가 전달받은 이벤트 메일을 장기간 열람 등 확인을 하지 않음
미흡사례 3	• 통합보안관제 월간 리포트에 오탐 정책에 대해 분석하였으나, 그 결과를 반영하지 않아 패턴 정책의 최적화 작업이 이행되지 않음

2.1.바 Firewall, IDS 또는 IPS에서의 로그 관리 기능

■ 심사내용 설명

기준	주요 내용
로그관리	• 로그 관리 절차를 수립하고 이에 따라 로깅하고 있는지 확인 – 로그기록 및 보존이 필요한 주요 정보시스템 지정 – 각 시스템 별 보존이 필요한 로그유형 및 보존기간 정의 – 로그기록 보존(백업) 방법 • 보존이 필요한 로그유형(예시) – 보안감사 로그 : 사용자 접속기록(사용자식별정보 : ID, 접속일시, 접속지 : 단말기 IP, 수행업무 : 정보생성, 수정, 삭제, 검색 출력 등), 인증 성공/실패 로그, 파일 접근, 계정 및 권한 등록/변경/삭제 등 – 시스템 로그 : 운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러코드 등) – 보안시스템 정책(룰셋 등)등록/변경/삭제 및 이벤트 로그 등 – 탐지/차단 등 접근통제 로그: 방화벽 허용/탐지 로그, IDS/IPS 탐지 로그, IPS 차단 로그 등 • 로그 보존기간은 최소 6개월 이상 보관 • 별도 저장장치를 사용하여 백업하고 있는지 확인 • 백업한 로그기록에 대한 접근권한 부여 최소화
로그분석	• 로그기록에 대한 분석 방법 및 주기 등에 대해 내부정책 수립 • 로그기록를 분석하고 결과를 보고하고 있는지 확인

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인서비스를 보호하기 위해 접근통제규칙을 적용하는 모든 Firewall
- 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 로그관리 절차 설명 자료 • Firewall, IDS 또는 IPS 로그 분석 보고서 • 로그기록 보존(백업) 현황 자료
담당자 인터뷰	• Firewal/IDS/IPS 담당자 – 로그의 Local 하드디스크(메모리 등) 또는 별도의 로그서버에 저장하는지 현황 설명 – 로그 수집서버(통합관제서버/SIEM 등)와 연동되어 로그를 실시간 전송하는지 설명 – 로그를 보존(백업)을 위한 별도의 절차가 존재하는지 설명 – Firewall의 주기적 로그 검토 시 보안관련 감사로그와 접근통제규칙 등록/변경/삭제 등 로그에 대해 이상 유무를 검토하는지 설명 – IDS또는 IPS의 주기적 로그 검토 시 보안관련 감사로그와 패턴 정책의 등록/변경/삭제 로그에 대해 이상 유무를 검토하는지 설명 – 주기적인 유지보수 점검 시 시스템 이벤트 로그를 검토하고, 결과에 따라 조치한 이력 등 존재 시 설명 – 로그백업서버로 수동 백업 시 로그백업파일 전달 절차 설명 • 로그백업서버 담당자 – 보관 중인 로그백업파일의 시스템 현황 설명 – 각 로그백업파일의 접근권한 현황 및 부여 절차 설명 • 로그 수집서버(통합관제서버 등) 담당자 – 실시간 로그 수집 중인 시스템 현황 및 연동 방법 등 설명 – 수집 로그에 대한 접근권한 현황 및 부여 절차 설명
현장실사	• firewall, IDS 또는 IPS의 로그 기록, 저장 등 현황 확인 • firewall, IDS 또는 IPS의 수집서버 연동 설정 확인 • 별도의 로그백업서버로 수동 백업 시 백업파일 생성, 로그서버로 전송, 등 각 단계별 실사 • 별도의 로그 수집서버(통합관제서버 등)의 접근권한 부여 현황 실사 • 로그백업서버의 로그 접근권한 부여 현황 실사

■ 사례 검토

미흡사례 1	• Firewall, IDS 또는 IPS 로그 조회 시 Local 메모리에 일시적으로 기록된 로그만 조회가 가능함
미흡사례 2	• 로그 수집서버에서 해당 로그가 3개월 이후 일괄삭제되고 있어 로그기록 보관기준을 충족하지 않음

2-2. 시스템 접근 통제

2.2.가 **접근권한이 없는 자가 시스템에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉·유출하는 행위에 대한 검사**

■ 심사내용 설명

기준	주요 내용
접근통제 정책수립	• 정보시스템 접근통제 및 정보보호시스템 운영 지침·절차를 수립하여 이행
접근통제 기능구현	• 정보시스템 및 정보보호시스템에서 접근권한이 없거나 접근권한을 초과한 자의 접근 및 행위에 대해 탐지 및 점검할 수 있도록 기능 구현
접근통제 주기적 검토	• 정보시스템 및 정보보호시스템에 설정한 보안 통제 정책의 적절성을 주기적으로 점검하여 안전하게 관리 • 비인가자의 접근 및 인가자의 비인가된 행위를 사전에 차단하거나, 행위기록을 실시간 모니터링 또는 주기적으로 점검하는 등 대응 절차를 수립

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립·시행 및 점검)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인업무 처리 정보시스템
- 정보보호시스템
- 로그관리시스템 및 통합로그모니터링시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획 및 정보시스템 운영 지침 • 본인확인서비스 정보자산 목록 – 정보보호시스템(DLP, 서버접근제어시스템, DB접근제어시스템, SecureOS 관리시스템 등) 솔루션명/용도/장비IP주소 – 로그관리시스템(솔루션명/용도/장비IP주소/수집대상로그) – 통합로그모니터링시스템(솔루션명/용도/장비IP주소/수집대상로그) • 정보시스템 접속·행위기록 점검 및 조치 결과
담당자 인터뷰	• 정보보호담당자 – 정보보호시스템 운영 현황 설명 • 접근통제시스템(네트워크/서버/DB/PC) 운영자 – 접근통제 정책 적용 현황 설명 • 로그관리시스템 및 통합로그모니터링시스템 운영자 – 정보시스템 접속·행위기록 점검 및 조치 현황 설명
현장실사	• 본인확인업무 처리 정보시스템에 접근 및 행위에 대해 검사하는 절차의 적절성 확인 • 접근 및 행위기록 점검 시 이상징후 판단 기준의 적절성 확인 • 접근 및 행위기록 점검 및 조치 결과 확인

■ 사례 검토

미흡사례 1	• 서버 OS 내에서 DB접속명령어를 수행한 행위에 대해 통합로그모니터링시스템에서 이상징후 룰에 등록하여 모니터링하고 있으나, 별도 승인 증적 없이 DBA 계정이 모니터링 대상에서 예외 처리되어 있음
미흡사례 2	• 데이터유출방지시스템을 통해 사내망에서 외부 인터넷망으로 전송되는 데이터에 개인정보 포함 여부를 탐지하고 있으나, 탐지 로그만 남기고 이상징후에 대해 점검하고 있지 않음

2.2.나 정당한 권한이 없는 사람이 본인확인서비스와 관련된 통신망의 접근과 침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영

■ 심사내용 설명

기준	주요 내용
정보보호 정책수립	• 정보시스템 접근통제 지침 및 정보보호시스템(네트워크/서버/DB/PC 보안솔루션 등) 운영 지침을 수립하여 이행
정보보호시스템 설치·운영	• 본인확인서비스 관련 통신망과 본인확인업무 처리 정보시스템에 접근을 통제하기 위한 정보보호시스템 설치 및 운영

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립·시행 및 점검)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인업무 처리 정보시스템
- 접근통제시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획 및 정보시스템 운영 지침 • 본인확인서비스 정보자산 목록 – 정보보호시스템(NAC, DLP, 계정관리시스템, 비밀번호관리시스템, 서버접근제어시스템, DB접근제어시스템, SecureOS관리시스템 등) 솔루션명/용도/장비IP주소 – 원격 접근 통제시스템 솔루션명/장비IP주소 • 본인확인서비스 네트워크 구성도 – 본인확인업무 처리 정보시스템 네트워크 – 사용자 단말 유·무선 네트워크 • 사용자 단말 망분리 및 망연계 구성도 • 본인확인업무 처리 정보시스템 접속 흐름도 • 원격 접근 통제 정책, 절차 및 흐름도 • 본인확인업무 직무자 명단 – 조직명, 이름, 업무(본인확인업무 인증담당자, 본인확인 관리자사이트 관리자/운영자, 개발자, 서버관리자, 미들웨어 운영자, DBA, 정보보호시스템 운영자 등), 사용자 단말(물리/논리) IP주소
담당자 인터뷰	• 정보보호담당자 – 정보보호시스템 운영 현황 설명 • 접근통제시스템(네트워크/서버/DB/PC) 운영자 – 접근통제 정책 적용 현황 설명
현장실사	• 본인확인업무 처리 정보시스템(네트워크/서버/DB/PC) 특성에 따라 접근통제 정책 적용 현황의 적절성 확인 • 접근통제시스템을 우회한 접근 경로가 있는지 확인 • 접근통제시스템에서 접근통제 정책 예외 적용자에 대한 관리 현황 확인 • 비인가자의 접근 및 인가자의 비인가된 행위에 대한 대응 절차 및 조치 결과 확인

■ 사례 검토

미흡사례 1	• 사용자 단말의 사내망 접근을 통제하고 있지 않음 – 사용자가 임의로 반입한 단말에 사내망 IP주소를 할당하여 사내망 접속 – 사용자가 업무망 단말에 인터넷망 단말의 IP주소를 할당하여 인터넷 접속
미흡사례 2	• 서버접근통제시스템에서 접근통제 정책 관리가 미흡함 – 업무상 불필요한 프로토콜(FTP)로 접속을 허용함 – 금지명령어 사용 차단 정책이 허용되어 있으나, 승인 증적을 확인불가

2.3. 저장정보의 조작·파괴·은닉 및 유출방지

2.3.가 **본인확인서비스와 관련된 데이터를 파괴하거나 본인확인서비스의 운영을 방해할 목적으로 바이러스·논리폭탄 등의 프로그램을 투입하는 행위의 검사**

■ 심사내용 설명

기준	주요 내용
정보보호 정책수립	• 발견된 악성프로그램에 대한 처리 절차 수립 및 이행 • 백신소프트웨어 등 보안 프로그램 운영 시 관련 법규 및 내부관리계획 준수
백신 소프트웨어	• 사용자 단말과 본인확인업무 관련 서버에 백신소프트웨어 등의 보안 프로그램을 설치 및 운영 • 본인확인서비스와 관련된 임의의 데이터 조작, 파괴, 은닉 또는 유출 시도를 탐지하는 기능 구성 및 운영 • 백신소프트웨어 등 보안 프로그램의 정상 동작 여부 주기적 점검 ※ 중앙백신관리서버와 클라이언트 백신소프트웨어 간 통신 상태 점검, 악성코드 탐지 패턴 일1회 이상 업데이트, 실시간 감시 등 보안 기능 적용 • 사용자 단말과 본인확인업무 관련 서버의 운영체제 및 응용프로그램의 보안 업데이트 현황 점검 • 사용자 단말과 본인확인업무 관련 서버에 비인가 및 불법 소프트웨어 설치 여부 점검

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제9조(악성프로그램 등 방지)

■ 심사 대상

- 백신소프트웨어 등 악성프로그램 관리 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획(악성프로그램 관리 조항) • 정보보호시스템 운영 지침 • 정보보호시스템 자산목록 • 네트워크 구성도(정보보호시스템 구성 명시) • 악성프로그램 관리 시스템 운영 현황
담당자 인터뷰	• 악성프로그램 관리 시스템 운영 담당자 – 악성프로그램 관리 시스템 구성 설명 – 악성프로그램 관리 시스템 통제 정책 설정 및 운영 현황 설명
현장실사	• 악성프로그램 관리 방안 수립 여부 확인 • 악성프로그램 관리 시스템 구성 현황 확인 • 악성프로그램 관리 시스템 통제 정책 설정 및 운영 현황 확인 • 사용자 단말 및 본인확인업무 관련 서버의 운영체제 및 응용프로그램의 보안업데이트 현황 확인 • 비인가 및 불법 소프트웨어 사용 여부 점검 현황 확인

■ 사례 검토

미흡사례 1	• 사용자 단말에 설치된 백신프로그램의 패턴이 정상적으로 업데이트되고 있지 않음
미흡사례 2	• 중앙백신관리서버 확인 결과, 특정 사용자 단말에서 최근 한 달간 다량의 악성코드 감염이 탐지되었으나 이에 대한 점검 및 조치 결과를 확인할 수 없음

2.3.나 본인확인서비스의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위의 검사

■ 심사내용 설명

기준	주요 내용
DDoS 대응	• 본인확인서비스 방해를 목적으로 하는 서비스 거부 공격에 대응하기 위한 방안을 마련하여 적용

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 서비스 거부 공격 탐지 및 대응 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스(정보시스템, 사용자) 네트워크 구성도 • 본인확인서비스 자산목록(정보보호시스템) • 서비스 거부 공격 대응 절차 • 서비스 거부 공격 점검 및 조치 결과
담당자 인터뷰	• 본인확인서비스 네트워크 및 정보보호 담당자 – 본인확인서비스 네트워크 및 정보보호시스템 구성 현황 설명 • 서비스 거부 공격 탐지 시스템 운영자 – 서비스 거부 공격 대응 절차 설명 – 서비스 거부 공격 탐지 시스템 구성 현황 및 탐지 정책 설명 – 서비스 거부 공격 점검 및 조치 결과 설명
현장실사	• 서비스 거부 공격 탐지 대응 절차의 적절성 확인 • 서비스 거부 공격 탐지 정책의 적절성 확인 • 서비스 거부 공격 점검 및 조치 결과의 적절성 확인

■ 사례 검토

미흡사례 1	• 본인확인서비스 통신망에 서비스 거부 공격을 탐지 및 대응하기 위한 기술적 조치가 적용되지 않음

2.3.다 대체수단 관련 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치

■ 심사내용 설명

기준	주요 내용
정책수립	• 본인확인업무 관련 정보가 대내 또는 대외 접근이 불필요한 자에게 유출·변조·삭제 등 행위가 발생하지 않도록 내부관리계획을 수립하고 기술적 보호조치 적용 • 사용자 단말을 망분리 하고 망간 자료전송 또는 통신 스트리밍 기능을 사용하는 경우, 보안 통제 정책을 수립하여 관리
기술적 보호조치	• 본인확인업무 관련 정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 본인확인서비스 관련 정보시스템과 사용자 단말 등에 기술적 보호조치 적용 • 내부 업무시스템(사내 포탈, 그룹웨어, 메일시스템, 메신저, 협업툴, 공유드라이브, 외부에 공개된 SaaS 서비스 등)을 통해 본인확인업무 관련 정보가 유출·변조·삭제 등이 발생하지 않도록 통제 적용 • 본인확인업무 관련 정보의 불법 유출·변조·삭제 등 이상행위 점검 절차 및 관련 로그 관리 절차를 수립하여 이행 ※ 본인확인업무 관련 정보: 대체수단 발급 정보 및 이용자 정보, 본인확인결과정보 및 대체수단 이용내역 등 본인확인업무 관련 정보시스템에서 처리하는 데이터

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립·시행 및 점검)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 사용자 단말 및 망연계 시스템
- 정보보호시스템
- 로그관리시스템 및 통합로그모니터링시스템

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획 • 본인확인서비스 정보자산 목록 – 정보보호시스템(솔루션명/용도/장비IP주소) – 로그관리시스템(솔루션명/용도/장비IP주소/수집대상로그) – 통합로그모니터링시스템(솔루션명/용도/장비IP주소/수집대상로그) • 본인확인서비스 네트워크 구성도 – 본인확인업무 처리 정보시스템 네트워크 – 사용자 단말 유·무선 네트워크 • 사용자 단말 망분리 및 망연계 구성도 • 본인확인업무 처리 정보시스템 접속 흐름도 • 내부업무시스템 사용 현황 – 사내 포탈, 그룹웨어, 메일시스템, 메신저, 협업툴, 공유드라이브, 외부에 공개된 SaaS 서비스 등의 용도 명시 – 내부업무시스템에 접속하는 사용자 단말(업무망/인터넷망 등) 명시 • 이상행위 점검 및 조치 결과
담당자 인터뷰	• 본인확인서비스 네트워크 담당자 – 본인확인서비스 네트워크 구성 설명 • 정보보호 담당자 및 정보보호시스템 운영자 – 내부업무시스템 사용 현황 설명 – 동 심사 항목에 대한 기술적 보호조치 현황 설명 – 이상행위 점검 및 조치 결과 설명 • 사용자 단말 망연계 시스템 운영자 – 사용자 단말 망분리 현황 및 망연계 보안 통제 정책 설명 – 이상행위 점검 및 조치 결과 설명
현장실사	• 본인확인업무 관련 정보가 서버, 사용자 단말, 내부업무시스템 등을 통해 외부 인터넷망으로 유출 경로가 있는지 확인 • 내부망에서 비인가자에게 본인확인업무 관련 정보가 불필요하게 공유 또는 유출 경로가 있는지 확인 • 관련 정보보호시스템에 설정된 통제 정책의 적절성 확인 • 관련 정보보호시스템 간 보완 통제의 적절성 확인 • 사용자 단말 망연계 시스템에 설정된 통제 정책의 적절성 확인 • 이상행위 점검 및 조치 적절성 확인

사례 검토

미흡사례 1	• 사용자가 임의로 본인확인서비스 이용자 개인정보파일을 사내 메일시스템을 통해 외부로 전송이 가능하나, 이에 대한 기술적 보호대책이 적용되지 않음
미흡사례 2	• 사용자 단말에서 문서작성 프로그램 공유 기능을 통해 본인확인서비스 이용자 개인정보파일이 외부 인터넷망 공유 드라이브에 저장이 가능함
미흡사례 3	• 주요 직무자(DBA 등 개인정보취급자)가 망연계 시스템을 통해 업무망 단말에서 인터넷망 단말로 별도 승인 절차 없이(자가 승인) 자료를 반출하고 있으며, 이에 대한 점검도 수행되지 않음

3. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항

3-1. 본인확인 시스템 보안

3.1.가 **관리자가 본인확인시스템 접속 시 일반 인터넷망과 분리되어 있는 별도의 PC 또는 접속경로를 사용하는 기능**

■ 심사내용 설명

기준	주요 내용
정책수립	• 접근통제 정책 및 사용자 단말 망분리 기준을 수립하여 이행
망분리 구성	• 관리자가 본인확인업무 전용 정보시스템(서버, DB, 관리자사이트) 접속 시 외부 인터넷망과 연결되어 있지 않도록 물리적 또는 논리적으로 분리된 PC를 사용 * 논리적 망분리의 경우 우회경로가 없는지 자체점검 및 증적자료 제시 필요
원격지 접속	• 외부 인터넷망에서 본인확인업무 처리 정보시스템으로 원격 접속은 원칙적으로 불허하나, 불가피한 사유로 인정되는 경우, 다음 사항 준수 – 법적요구사항을 준수하여 원격 접속 절차 수립 – 외부 접속 단말에서 본인확인 처리 정보시스템 접속 시, 접속 단말의 보안 상태(백신, 윈도우 보안업데이트 등) 점검, 인터넷 차단, 클립보드 차단, 추가 인증수단 적용, 접속기록 검토 등 관리적·기술적 보호조치 수립 및 이행

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 사용자 단말 및 본인확인업무 처리 정보시스템
- 사용자 단말 망분리 시스템
- 원격 접근 통제 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획 및 정보시스템 운영 지침 – 서버 및 사용자 단말 인터넷 접속통제(망분리) 정책 조항 • 본인확인서비스 정보자산 목록 – 정보보호시스템(DLP, 스팸차단시스템, 유해사이트차단시스템 등) 솔루션명/용도/장비IP주소 – 통합로그모니터링시스템 솔루션명/용도/장비IP주소/수집대상로그 • 본인확인서비스 네트워크 구성도 – 본인확인업무 처리 정보시스템 네트워크 – 사용자 단말 유·무선 네트워크 • 사용자 단말 망분리 및 망연계 구성도 • 본인확인업무 처리 정보시스템 접속 흐름도 • 원격 접근 통제 정책, 절차 및 흐름도 • 본인확인업무 직무자 명단 – 조직명, 이름, 직무(본인확인업무 인증담당자, 본인확인 관리자사이트 관리자/운영자, 개발자, 서버관리자, 미들웨어 운영자, DBA, 정보보호시스템 운영자 등), 사용자 단말(물리/논리) IP주소
담당자 인터뷰	• 본인확인서비스 네트워크 담당자 – 본인확인서비스 네트워크 구성 설명 – 사용자 단말 망분리 및 망연계 현황 설명 • 정보보호 담당자 – 본인확인서비스 관련 정보보호시스템 운영 현황 설명 – 본인확인업무 처리 정보시스템 접속 흐름도 설명 – 원격 접근 통제 절차 및 흐름도 설명 • 사용자 단말 망분리 솔루션 운영자 – 사용자 단말 망분리 정책(보안 통제 정책) 설명 • 원격 접근 통제 시스템 운영자 – 원격 접근 통제 정책(보안 통제 정책) 설명
현장실사	• 관리자가 본인확인업무 처리 정보시스템 접속 시 외부 인터넷망과 연결되어 있지 않은 PC를 사용하는지 확인 • 사용자 단말 망분리 정책에 따른 보안 정책 적용 여부 확인 • 법적 준거성 준수 여부 확인 • 원격접근통제 정책의 적절성 및 관리적·기술적 보호조치 이행 여부 확인

■ 사례 검토

미흡사례 1	• 사무실 단말에서 서버관리자와 DBA가 외부 인터넷망을 통해 본인확인업무 서버와 DB에 접속하고 있음
미흡사례 2	• 본인확인 관리자사이트의 최고관리자가 인터넷 접속이 허용된 사무실 단말에서 관리자사이트에 접속하고 있음

3.1.나 시스템에 접속 가능한 IP주소와 사용자 계정에 대한 데이터접근권한을 지정하는 기능

■ 심사내용 설명

기준	주요 내용
접근권한 등록관리	• 본인확인업무 처리 정보시스템에 접속하는 사용자 계정과 단말 IP주소에 대한 관리(신청, 등록, 변경, 삭제 등) 절차 수립 • 본인확인업무 처리 정보시스템에 접속하는 계정은 사용자용 계정, 어플리케이션용(어플리케이션 설치, 시스템 연동) 계정 등 용도에 따라 분리하여 생성하고, 접속 계정별 파일 및 데이터 접근권한은 업무상 필요한 범위 내 최소한으로 부여 • 본인확인업무 처리 정보시스템에 접속하는 단말 IP주소를 최소화 • 접속 단말 IP주소와 사용자 계정은 단말과 사용자를 명확히 식별하고 책임추적성을 확보할 수 있도록 부여
로그관리	• 사용자 계정에 대한 데이터 접근권한 부여 기록을 남기고 관리
사후관리	• 업무상 불필요한 계정 및 접근권한은 주기적으로 점검하고 관리

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제4조(내부관리계획의 수립·시행 및 점검)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인업무 처리 정보시스템
- 계정관리시스템 및 비밀번호관리시스템
- 접근통제시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획 및 정보시스템 운영 지침 – 정보시스템 계정 관리 및 접근권한 관리 조항 • 본인확인서비스 자산목록 – 대체수단 발급 관련 사이트, 본인확인 관리자사이트 URL 명기 – 정보보호시스템(계정관리시스템, 비밀번호관리시스템, 서버/DB접근제어시스템, SecureOS 관리시스템 등) 서버 IP주소 명기 • 본인확인업무 직무자 명단 – 조직명, 이름, 업무(본인확인업무 인증담당자, 본인확인 관리자사이트 관리자/운영자, 개발자, 서버관리자, 미들웨어 운영자, DBA, 정보보호시스템 운영자 등), 사용자 단말(물리, 논리) IP주소
담당자 인터뷰	• 정보보호 담당자 – 접근통제시스템 운영 현황 설명 • 본인확인업무 처리 정보시스템 운영자 – 접속 계정, 접속 단말 IP주소, 접근권한 관리 현황 설명 • 계정관리시스템 및 비밀번호관리시스템 운영자 – 정보시스템 접속 계정 및 비밀번호 관리 현황 설명 • 접근통제시스템 운영자 – 정보시스템 접속 계정, 접속 단말 IP주소, 접근권한 관리 현황 설명
현장실사	• 정보시스템 계정 및 비밀번호, 단말 IP주소, 데이터 접근권한이 통제 정책 및 절차에 따라 관리되고 있는지 확인 • 사용자 계정에 대한 데이터 접근권한 부여 기록 관리 현황 확인

■ 사례 검토

미흡사례 1	• 관리자사이트에서 사용자의 접속 단말 IP주소를 제한하지 않음
미흡사례 2	• 본인확인업무 서버의 HOST 방화벽에 불필요한 IP주소가 등록되어 있음
미흡사례 3	• 침입차단시스템 관리자사이트에서 관리자(2명) 계정별 접속 단말 IP주소가 과도하게 C class로 허용되어 있으며, 현재는 사용하지 않는 불필요한 IP주소도 등록되어 있음

3.1.다 시스템과 연결된 PC에서 이동저장매체 사용 시 이를 통제하는 기능

■ 심사내용 설명

기준	주요 내용
사용자 단말보안	• 본인확인업무 관련 정보시스템에 접속하는 사용자 단말에서 이동저장매체 사용 통제
이동저장매체 관리	• 회사 자산인 이동저장매체를 직원에게 배포하여 업무용으로 사용할 경우, 관리대장을 작성하여 반출·입 관리 • 회사 자산인 이동저장매체 분실 시 보안 통제 방안 마련 ※ 이동저장매체 접근 비밀번호 설정, 이동저장매체 사용 종료 후 저장 파일 완전 파기 등 • 이동저장매체를 통한 중요 파일의 외부 반출 및 사용자 단말에 악성코드 유입 등을 방지하기 위한 통제 정책 적용 필요 • 이동저장매체 통제솔루션을 운영하는 경우 – 사내 및 사외 통제 정책 적용(외장하드, USB 등) – 비인가된 이동저장매체 사용 통제 정책 적용 – 특정 사용자에게 기본 통제 정책이 아닌 예외 정책을 적용하는 경우, 예외 정책 신청·승인 절차 및 사후관리 절차(허용 매체, 허용 기간, 이상징후 모니터링 방안, 허용 기간 종료 후 회수 방안 등) 수립하여 적용 – 인가된 이동저장매체를 통한 파일 접근(파일 읽기, 쓰기 등) 기록 저장

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제6조(접근통제), 제10조(물리적 안전조치)

■ 심사 대상

- 이동저장매체 관리대장
- 이동저장매체 통제솔루션

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• PC 보안 지침(이동저장매체 통제 지침) • 정보보호시스템 자산목록(이동저장매체 통제시스템 명시) • 사용자 단말 용도별 이동저장매체 통제시스템 기본 정책(사내 및 사외 통제 정책)
담당자 인터뷰	• 전사 PC 보안 담당자 – 이동저장매체 통제 지침·정책 설명 – 이동저장매체 관리대장 설명 • 이동저장매체 통제시스템 운영자 – 사내 및 사외 통제 정책 설명 – 예외 정책 적용 절차 설명 – 이동저장매체를 통한 파일 접근(파일 읽기, 쓰기 등) 기록 설명
현장실사	• 사용자 단말 용도에 따른 기술적 또는 관리적 이동저장매체 통제 정책 확인 • 회사 자산인 이동저장매체 반출입 관리대장 확인 • 회사 자산인 이동저장매체 분실을 대비한 보안 통제 방안 확인 • 이동저장매체 통제솔루션에서 사내 및 사외 통제 정책 적절성 확인 • 이동저장매체 통제솔루션에서 예외 정책 관리 적절성 확인 • 인가된 이동저장매체를 통한 파일 접근(파일 읽기, 쓰기 등) 기록 저장 확인

■ 사례 검토

미흡사례 1	• 이동저장매체 통제솔루션에서 예외 정책 관리가 미흡함 – 별도의 승인 절차 없이 특정 사용자에게 예외 정책을 허용함 – 특정 사용자에게 허용한 예외 정책이 허용 기간이 종료되었으나, 차단되지 않음

3-2. 네트워크 및 시스템 안정성 점검

3.2.가 실시간으로 네트워크 및 시스템 상태를 점검할 수 있는 시스템 또는 장비 운영

■ 심사내용 설명

기준	주요 내용
정보시스템 모니터링	• 실시간으로 네트워크, 서버, DB, 정보보호시스템 등 정보시스템의 안정성을 점검할 수 있는 시스템 운영 • 가상머신, 컨테이너 등 정보시스템 구성 방식의 특성에 따라, 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고, 현황을 지속으로 모니터링 할 수 있는 방법 및 절차 수립 • 모니터링 결과를 기록·분석·보고하고, 개선사항 또는 특이사항 발생 시 안정성 확보 방안을 수립하여 이행

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 성능 및 용량 관리 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 정보시스템 운영 지침(성능 및 용량 관리 조항) • 성능 및 용량 모니터링 절차 • 정보시스템별 성능 및 용량 관리 시스템 목록(솔루션명, 용도 등) • 정보시스템별 성능 및 용량 모니터링 요구사항 정의 및 설정 내역 ※ 정보시스템: 네트워크, 서버, DB, 정보보호시스템 등 • 성능 및 용량 모니터링 결과 기록·분석·보고 내역 • 개선사항 또는 특이사항 발생 건에 대한 안정성 확보 조치 방안 및 이행 내역
담당자 인터뷰	• 정보시스템 성능 및 용량 관리자 • 정보시스템 성능 및 용량 관리 시스템 운영 담당자

구분	준비사항
현장실사	• 정보시스템별 성능 및 용량 모니터링 요구사항을 정의하고, 성능 및 용량 관리 시스템에 적용하여 운영하는지 여부 • 성능 및 용량 모니터링 결과를 기록·분석·보고하는지 여부 • 모니터링 결과에 따라 개선사항 및 특이사항에 대해 조치 방안을 마련하고 이행하는지 여부

사례 검토

미흡사례 1	• 신규로 교체된 서버가 성능 관리 시스템 등록 대상에 누락 되어 성능 및 용량이 모니터링 되고 있지 않음
미흡사례 2	• 정보시스템의 성능 또는 용량이 사전에 정의한 임계치를 지속적으로 초과하고 있으나, 이에 대한 조치 방안이 수립 및 이행되지 않음

3.2.나 본인확인업무와 관련된 주요 프로그램 또는 프로세스 동작여부를 점검할 수 있는 시스템 또는 장비 운영

■ 심사내용 설명

기준	주요 내용
필수프로그램 동작 확인	• 본인확인업무를 처리하는 주요 프로그램 또는 프로세스를 정의하고, 정상적으로 동작하고 있는지 점검할 수 있는 시스템 운영 ※ 본인확인업무: 대체수단 발급, 본인확인서비스(인증·식별) 등 • 본인확인업무 정보시스템 구성 환경에 따라, 본인확인업무를 처리하는 미들웨어(WEB·WAS·AP), DB, 서버보안솔루션, 컨테이너 관련 플랫폼 등의 프로그램 또는 프로세스가 정상적으로 동작하는지 점검
이상징후 대응	• 주요 프로그램 또는 프로세스에 대해 실시간 모니터링 체계 또는 특이사항 발생 시 관련 담당자에게 알림을 전송하는 기능 구축 • 주요 프로그램 또는 프로세스에 특이사항 발생 시 가용성 확보 방안 및 조치 절차를 마련하여 운영

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 프로세스 모니터링 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 정보시스템 운영 지침(프로세스 모니터링 조항) • 프로세스 모니터링 절차 • 프로세스 모니터링 시스템 목록(솔루션명, 용도 등) • 본인확인업무 서비스 흐름도 및 시스템 구성도 – 본인확인업무 서비스 흐름에 따라 처리하는 서버 식별 – 서버별로 서비스 처리 프로그램 또는 프로세스 명시

구분	준비사항
	※ 본인확인업무: 대체수단 발급, 본인확인서비스(인증·식별) 등 ※ 프로그램 또는 프로세스 : 미들웨어, AP 데몬, DB, 서버보안솔루션, 컨테이너 관련 플랫폼 등 ※ 서버 Hostname/IP, 프로그램 설치 위치, 프로세스명, 용도 명시 • 프로세스 모니터링 시스템 설정 내역 – 본인확인업무 서버별 주요 프로그램 또는 프로세스 등록 내역 – 특이사항 발생 시 알림 설정 내역
담당자 인터뷰	• 본인확인서비스 개발자 및 서비스 운영자 – 본인확인업무 서비스 흐름도 및 시스템 구성도 설명 • 본인확인업무 전용 서버 미들웨어 담당자 및 DBA – 본인확인업무 서비스 흐름도 및 시스템 구성도 • 프로세스 모니터링 시스템 운영자 – 본인확인업무 서버별 주요 프로그램 또는 프로세스 등록 현황 설명 – 실시간 모니터링 또는 특이사항 발생 시 알림 설정 현황 설명
현장실사	• 프로세스 모니터링 절차 수립 여부 • 본인확인업무 서비스 흐름도 및 시스템 구성도 현행화 확인 – 본인확인업무 서비스 흐름에 따라 처리하는 서버 식별 여부 – 서버별로 서비스 처리 프로그램 또는 프로세스 식별 여부 • 프로세스 모니터링 시스템에 등록 현황 확인 – 본인확인업무 서비스 흐름도 및 시스템 구성도에서 식별된 프로그램 및 프로세스가 등록되어 있는지 확인 – 실시간 모니터링 또는 특이사항 발생 시 알림 설정 현황 확인

■ 사례 검토

미흡사례 1	• 프로세스 모니터링 시스템에 본인확인 WEB/WAS서버의 프로세스(WEB/WAS)가 모니터링 대상으로 등록되어 있지 않음
미흡사례 2	• 프로세스 모니터링 시스템에 본인확인서버의 프로세스(본인확인서비스 데몬)가 등록되어 있으나, 정상 여부를 확인하는 기준값 및 특이사항 발생 시 알림 기능이 설정되어 있지 않음

3.2.다 대체수단의 부정사용 여부에 대한 모니터링 및 정책 수립

■ 심사내용 설명

기준	주요 내용
모니터링 정책 수립	• 대체수단 발급 및 본인확인서비스(인증·식별) 시 대체수단 발급 정보 및 본인확인정보의 부정사용 여부를 모니터링 하기 위한 정책 수립
모니터링 및 대응방안 마련	• 대체수단의 특성에 따라 부정사용 시나리오 개발 및 탐지 기준을 수립하고, 기술적 차단 방법 구현 및 사후관리 방안 마련 ※ 일 30회 인증 실패 시 차단 또는 존재하지 않는 본인확인정보 입력을 통해 인증 10회 시도 시 차단 등

■ 관련 법규

● 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의3(본인확인기관의 지정 등)

- 본인확인기관 지정 등에 관한 기준 [별표 3] 1장 3.2.다

■ 심사 대상

● 대체수단 부정사용 탐지 룰 구현 소스코드

● 대체수단 부정사용 모니터링 시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 부정사용 모니터링 정책 - 부정사용 시나리오 및 탐지 기준 - 모니터링 절차 및 대응 절차 • 대체수단 부정사용 모니터링 결과 및 조치 결과
담당자 인터뷰	• 본인확인서비스 인증 업무 담당자 - 대체수단 부정사용 모니터링 정책 및 현황 설명 • 본인확인서비스 개발자 - 대체수단 부정사용 시나리오별 탐지 룰 구현 현황 설명

구분	준비사항
현장실사	• 대체수단 부정사용 모니터링 정책의 적절성 및 실효성 확인 • 대체수단 부정사용 모니터링 정책에 따라 소스코드 또는 관련 정보시스템 상에 탐지 룰이 구현되어 있는지 확인 • 대체수단 부정사용 탐지 시 기술적 차단 방법 구현 여부 확인 • 대체수단 부정사용 발견 시 조치 및 사후관리의 적절성 확인

■ 사례 검토

미흡사례 1	• 대체수단 부정사용 모니터링 정책(시나리오 및 탐지 기준 등)은 수립되어 있으나, 정보시스템에 기술적으로 구현되어 있지 않음
미흡사례 2	• 대체수단 부정사용 모니터링 시스템에 모니터링 정책(시나리오 및 탐지 기준 등)과 상이하게 탐지 룰이 등록되어 있음

3-3. 시스템 취약점 점검

3.3.가 기존에 알려진 취약성 및 신규 취약성에 대비한 점검

■ 심사내용 설명

기준	주요 내용
주기적 취약점점검 수행	• 정보시스템 취약점 점검 절차 수립 및 정기적 점검 수행 여부
점검결과 이행조치	• 발견된 취약점에 대한 조치 활동 수립 및 보완조치 수행 – 취약점 확인에 대한 CISO 보고 및 승인절차 – 조치 지연 발생시 CISO 보고 및 위험관리 방안 수립

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

● 본인확인설비(클라우드 이용 시 클라우드 시스템 모두 포함), 본인확인서비스 어플리케이션(홈페이지, 안드로이드/IOS APP) 및 프레임워크, 본인확인서비스 소스 코드

● 전사 정보보호시스템 및 개인정보보호 솔루션 일체, 공용 네트워크 장비

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 취약점 점검 관련 정책, 지침, 절차, 매뉴얼 • 내부 관리계획 수립 및 시행 증적 • 주요정보통신기반시설 취약점 완료보고서 (2021.3 개정 기준) • 취약점 점검 계획서, 결과보고서, 조치계획서, 조치완료 보고서 • 취약점 위험수용을 위한 CISO 승인 증적 문서 • WEB/APP에 대한 모의해킹 결과 보고서, 조치완료 보고서 • CVE 취약점에 대한 정보시스템/오픈소스 패치 증적 자료

구분	준비사항
담당자 인터뷰	• 보안담당자 – 취약점 점검 및 조치에 대한 정책 및 수행 이력 • 시스템 운영자 – 발견된 취약점, CVE 코드에 대한 조치 진행 여부 • 프로그램 개발자 – 시큐어코딩 정책 준수 여부 및 예외사항 처리 승인 절차
현장실사	• 소스 코드 시큐어코딩 툴 및 QA 진단 프로세스 점검 • 본인확인설비 취약점 진단 및 조치완료 여부 점검 • 모의해킹에서 발견된 취약점, 정보시스템(DB, 서버, 네트워크장비, 보안시스템, 개인정보 보호 솔루션) 취약점 조치완료 여부 확인 • 오픈소스 사용 시 오픈소스 CVE코드 패치 이력 점검 • 어플리케이션 및 소스코드 변경 및 수정 이력 점검

■ 사례 검토

미흡사례 1	• 주요정보통신기반시설 기준 항목으로 취약점을 모두 조치완료하는 것이 내부규정이나, CISO 승인이력 없이 특정 주요정보통신기반시설 취약점에 대하여 운영자 임의적으로 위험수용한 경우
미흡사례 2	• 무료버전의 오픈소스를 사용하는 경우 해당 CVE 취약점 코드가 발견되면 패치를 수행하도록 되어있으나, CISO 위험수용 승인없이 해당 취약점 패치를 누락한 경우

3-4. 소프트웨어의 임의변경·삭제 방지

3.4.가 본인확인서비스 관련 소프트웨어를 임의로 변경 및 삭제할 수 없도록 하는 기능

■ 심사내용 설명

기준	주요 내용
정책수립	• 본인확인서비스 관련 소프트웨어, 소스코드에 대한 등록·변경·폐기에 대한 변경관리 정책 및 수행 여부
소스코드 형상관리	• 본인확인서비스 관련 소프트웨어에 대한 장애발생 시 복구할 수 있도록 소스코드에 대한 형상관리 수행

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인서비스 관련 소프트웨어, 어플리케이션, 프레임워크, 소스 코드
- 계정관리 시스템(IAM), 형상관리 솔루션, 변경관리 솔루션, 배포관리 솔루션, 버전관리 솔루션, 어플리케이션 영향분석 솔루션, APP 관리 전용 솔루션 등

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 관련 소프트웨어 접근 승인 이력 • 형상관리 솔루션 등에서 소스코드 변경/수정 승인 정책 • WEB/APP 소스코드 배포실패에 대한 변경관리 솔루션 정책 • APP 배포관리 시스템에 대한 주기적 점검 이력

구분	준비사항
담당자 인터뷰	• 보안담당자 – 본인확인서비스 관련 소프트웨어에 대한 등록·변경·폐기에 대한 승인 절차 및 정당성 판정 근거 이력 • 품질담당자(QA 또는 QC, 품질관리팀이 없는 경우 개발팀장) – 형상관리 시스템, 변경관리 시스템 등에서 예외정책 승인 절차 • 프로그램 개발자 – 소스코드 변경 후 장애 발생 시 프로그램 복구 절차
현장실사	• 본인확인서비스 관련 소프트웨어 접근 가능 인원 점검 • 형상관리, 버전관리, 변경관리, 배포관리, 영향분석 솔루션 운영현황 점검 • 변경관리 예외정책 실제 운영현황 • 본인확인서비스 관련 소프트웨어에 대한 등록·변경·폐기를 위한 사전신청서 작성 업무 적정성 점검 • APP 스토어 배포 관리 현황 점검

■ 사례 검토

미흡사례 1	• 외주개발자에 대한 본인확인서비스 관련 소프트웨어 접근 시 이에 대한 이상행위 분석 및 소프트웨어 변경에 대한 통제정책 및 이력관리를 수행하지 않음
미흡사례 2	• 개발자가 형상관리/변경관리 솔루션 등에 소스 코드 변경에 대한 QA/QC의 사전승인 등록 없이 소프트웨어를 변경하고 있음
미흡사례 3	• 본인확인서비스 관련 소프트웨어 접근이 필요없는 다른 업무 개발자 및 운영자가 접근가능한 계정이 삭제되지 않음

4. 이용자 보호 및 불만처리에 관한 사항

4-1. 개인정보처리방침의 공개

4.1 **대체수단 발급 절차에 개인정보처리방침을 공개하여 이용자가 쉽게 확인할 수 있도록 하여야 함**

■ 심사내용 설명

기준	주요 내용
개인정보 처리방침 공개	• 본인확인서비스에 대한 개인정보처리방침을 수립하여 공개하여야 함 • 개인정보처리방침을 인터넷 홈페이지 첫 화면에 공개하는 경우 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분하여 표시 • 개인정보처리방침이 변경되는 경우 사유 및 변경 내용을 이용자가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공지·공개
개인정보 처리방침 포함내용	• 개인정보처리방침은 법령에서 요구하는 내용을 모두 포함 1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정함) 4. 개인정보의 파기절차 및 파기방법(다른 법령에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다) 5. 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정함) 6. 개인정보처리의 위탁에 관한 사항(해당 되는 경우에만 정하며, 재위탁에 관한 사항 포함) 7. 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정함) 8. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항 9. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처 10. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정함) 11. 처리하는 개인정보의 항목 12. 개인정보의 안전성 확보 조치에 관한 사항 13. 개인정보의 열람청구를 접수·처리하는 부서 14. 정보주체의 권익침해에 대한 구제방법 15. 개인정보 처리방침의 변경에 관한 사항

관련 법규

- 개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
  - 개인정보 보호법 시행령 제31조(개인정보 처리방침의 내용 및 공개방법 등)
- 개인정보 보호법 제30조의2(개인정보 처리방침의 평가 및 개선권고)
  - 개인정보 보호법 시행령 제31조의2(개인정보 처리방침의 평가 대상 및 절차)
  - 개인정보 처리방침 평가에 관한 고시

심사 대상

- 개인정보처리방침
- 개인정보처리방침 관리 방법 및 절차(작성·검토·게시 등의 업무)

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 최신 개인정보처리방침 • 개인정보처리방침 관리 절차 증적(작성·검토·게시 등의 업무) • 개인정보처리방침 변경 시 이용자에게 고지한 증적 – 이메일 발송 내역, SMS 발송 내역, 게시판 등
담당자 인터뷰	• 개인정보처리방침 작성·검토·게시 담당자 – 개인정보처리방침 변경관리 절차 설명 – 개인정보처리방침 변경에 따른 이용자 고지 절차 및 방법 설명
현장실사	• 개인정보처리방침 작성·검토·게시 등 관리 절차 확인 • 개인정보처리방침의 변경에 따른 이용자 고지 이행현황 확인 • 개인정보처리 위·수탁, 제3자 제공 관련 사항이 개인정보처리방침에서 공개하고 있는 내용과 일치 여부 확인 • 개인정보처리방침의 공개 위치와 가독성에 대한 평가 • (필요할 경우) 개인정보처리 위·수탁 계약서, 제3자 제공 계약서 내용 확인 • (필요할 경우) 본 계약에 따른 보안 관련 약정서가 존재하는 경우 해당 내용 확인 • 개인정보처리방침을 정보주체가 알기 쉽게 작성하였는지 여부 확인

사례 검토

미흡사례 1	• 개인정보처리방침이 개정되었으나 예전 개인정보처리방침이 비공개되어 확인할 수 없음
미흡사례 2	• 개인정보 보호책임자 변경, 수탁자의 변경 등 변경사항이 발생하였음에도 개인정보처리방침의 내용을 현행화하지 않음
미흡사례 3	• 개인정보처리방침에 공개되어 있는 개인정보 수집 내역이 실제 수집 내역과 맞지 않음

4-2. 개인정보 수집에 대한 고지 및 동의

4.2.가 **개인정보의 수집·이용목적, 수집하는 개인정보 항목, 개인정보의 보유 및 이용기간을 이용자에게 고지하고 동의를 받아야 함**

■ 심사내용 설명

<table>
<tr><th>기준</th><th>주요 내용</th></tr>
<tr><td>개인정보
수집·이용
고지내용</td><td>• 개인정보의 수집·이용 동의 시 아래사항에 대하여 고지
1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용</td></tr>
<tr><td>개인정보
수집·이용 동의</td><td>• 본인확인서비스 가입시 개인정보 수집에 관한 사항에 대하여 동의 획득
• 이용자에게 동의를 받을 때에는 아래 중요한 내용을 명확히 표시하여 알아보기 쉽게 하여야 함
중요한 내용
1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 민감정보, 여권번호, 운전면허의 면허번호 및 외국인등록번호에 관한 사항
3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적</td></tr>
<tr><td>중요한 내용
표시 방법</td><td>• 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
• 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것</td></tr>
<tr><td>파기</td><td>• 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립
• 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기</td></tr>
</table>

■ 관련 법규

- 개인정보 보호법 제15조(개인정보의 수집·이용)
- 개인정보 보호법 제21조(개인정보의 파기)
  - 개인정보 보호법 시행령 제16조(개인정보의 파기 방법)
  - 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

- 개인정보 보호법 제22조(동의를 받는 방법)
  - 개인정보 보호법 시행령 제17조(동의를 받는 방법)
  - 개인정보 처리 방법에 관한 고시 제4조(서면 동의 시 중요한 내용의 표시 방법)
- 개인정보 보호법 제22조의2(아동의 개인정보 보호)
  - 개인정보 보호법 시행령 제17조의2(아동의 개인정보 보호)

■ 심사 대상

- 대체수단 발급/이용 시 이용자가 동의하는 동의서 전체 내용
- 이용자에게 동의를 받는 방법 및 시점의 적절성 여부
- 개인정보 파기 관련 내부 정책 및 개인정보의 파기 방법 및 시점

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 발급/이용 단계 동의서 • 서비스 이용 단계 동의서 • 개인정보처리 현황 및 흐름을 파악할 수 있는 문서 증적 – 개인정보흐름도, 개인정보흐름표 등 • 개인정보 파기 관련 내부 정책 • 파기 증적 – 전자적 자료에 대한 파기배치 스케줄 – 종이 등 문서에 대한 파기 확인서 등
담당자 인터뷰	• 개인정보처리 현황 및 흐름 관련 담당자 – 개인정보처리 흐름 설명 • 개인정보 파기 담당자 – 전자적 자료의 경우 파기 배치 설명 – 종이 등 문서의 경우 파기 시점 및 절차 설명
현장실사	• 개인정보의 수집·이용 동의 시 고지 내용 누락 여부 확인 • 각각의 동의 사항을 구분하여 이용자가 이를 명확하게 인지할 수 있도록 알리고 있는지 확인 • 대체수단 발급/이용 단계 등에서 이용자에게 동의를 받는 시점 및 방법 확인 – 개인정보를 미리 포괄적으로 수집하는지 확인 • 파기시점 도래 시 개인정보의 파기를 적절히 수행하고 있는 지 확인 – 파기의 방법 및 스케줄 확인

사례 검토

미흡사례 1	• 개인정보 수집 동의 시 수집하는 개인정보 항목을 구체적으로 명시하지 않고 '~등'과 같이 포괄적으로 고지하고 있음
미흡사례 2	• 고객센터에서 수집하는 민원처리 관련 개인정보(상담이력, 녹취 등)를 다른 법령을 근거로 3년간 보존하고 있으나, 3년이 경과한 후에도 파기하지 않고 보관하고 있음

4.2.나 본인확인서비스 외에 법령의 규정에 의해 정보통신서비스 제공자에게 연령확인 등 선별가입 서비스를 제공할 경우에는 이용자에게 이를 사전에 고지하고 동의를 받아야 함

■ 심사내용 설명

기준	주요 내용
연령확인	• 본인확인기관은 본인확인결과정보에 연령정보를 포함하여 제공

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 본인확인서비스 연동전문

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 연동전문
담당자 인터뷰	• 본인확인서비스 사업 담당자 – 본인확인서비스 이용결과 제공되는 본인확인결과정보에 대한 설명
현장실사	• 본인확인결과정보에 연령정보를 제공하고 있는지 확인

■ 사례 검토

미흡사례 1	• 본인확인서비스 이용시 연령정보를 제공할 수 있는 기능을 제공하고 있지 않음

4.2.다 본인확인서비스를 제공하는데 필요한 정보 이외의 이용자 개인정보 수집의 금지

■ 심사내용 설명

구분	주요 내용
개인정보 수집 최소화	• 필요한 최소한의 개인정보만을 수집 • 필수로 수집하는 개인정보에 불필요한 정보가 없는지 입증할 수 있어야 함

■ 관련 법규

- 개인정보 보호법 제3조(개인정보 보호 원칙)
- 개인정보 보호법 제16조(개인정보의 수집제한)
- 개인정보 보호법 제22조(동의를 받는 방법)
  - 개인정보 보호법 시행령 제17조(동의를 받는 방법)

■ 심사 대상

- 대체수단 발급/이용 등에서 필수로 수집하는 개인정보 항목
  - 꼭 필요한 최소한의 정보인지 확인
- 이용자의 개인정보 제공 여부 선택권 보장에 관한 사항
  - 필수 동의 항목과 선택 동의 항목으로 구분 등

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 개인정보처리방침 • 대체수단 발급/이용 단계에서 고지하고 있는 동의문 • 이용자 동의를 받는 단계의 화면 스크린샷 • 수집하는 개인정보가 서비스 제공 등에 필요한 최소한의 정보임을 입증할 수 있는 관련 자료
담당자 인터뷰	• 개인정보보호 담당자 및 서비스 담당자 – 동의문 내용 및 동의징구 시점, 방법 관련 설명 – 최소한의 정보 수집 관련 설명

구분	준비사항
현장실사	• 개인정보의 수집 시 필요한 최소한의 정보만을 수집하고 있는지 확인 • 이용자가 직접 동의 여부를 선택할 수 있도록 수집하는 개인정보의 항목을 필수 동의 항목과 선택 동의 항목으로 구분하여 각각 동의를 받을 수 있도록 제공하고 있는지 확인

사례 검토

미흡사례 1	• 본인확인서비스 제공을 위하여 필요한 최소한의 정보 외에 불필요한 개인정보를 포함하여 수집하고 있음

4.2.라 필요한 최소한의 정보 이외의 개인정보를 제공하지 아니한다는 이유로 이용자에게 서비스 제공을 거부할 수 없음

■ 심사내용 설명

구분	주요 내용
선택정보 수집거부	• 이용자가 선택항목에 대한 동의를 거부하더라도 서비스의 이용이 가능하다는 사실을 명확하게 표시하여 알 수 있도록 고지 • 서비스 가입 과정에서 선택정보에 대하여 동의를 하지 않거나 입력을 하지 않더라도 필수적인 서비스는 이용할 수 있도록 구현 – 다만, 선택정보의 수집이 없다면 해당사항 없음

■ 관련 법규

- 개인정보 보호법 제16조(개인정보의 수집제한)
- 개인정보 보호법 제22조(동의를 받는 방법)

■ 심사 대상

- 이용자가 선택항목에 대한 동의를 거부하더라도 서비스 이용이 가능하다는 내용에 대한 고지 여부
- 서비스 가입 과정 설계 및 구현 관련 사항

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 이용자가 선택항목에 대한 동의를 거부하더라도 서비스 이용이 가능하다는 고지 내용 및 관련 화면 스크린샷 • 서비스 가입 과정 설계 및 구현 관련 자료 – 가입 프로세스 설계 관련 문서, 소스코드 구현 부분 등

구분	준비사항
담당자 인터뷰	• 서비스 가입 프로세스 설계 담당자 – 서비스 가입 프로세스 설명 • 서비스 가입 프로세스 개발 담당자 – 관련 소스코드 구현 부분 설명
현장실사	• 이용자가 선택항목에 대한 동의를 거부하더라도 서비스 이용이 가능하다는 내용에 대한 고지 확인 • 서비스 가입 과정 설계 및 구현 관련 사항 확인

■ 사례 검토

미흡사례 1	• 선택정보에 대하여 동의하지 않아도 대체수단 발급/이용이 가능함을 이용자가 인지할 수 있도록 구체적으로 알리지 않고 있음
미흡사례 2	• 대체수단 발급 화면에서 선택사항에 동의하지 않거나 선택정보를 입력하지 않으면 다음 단계로 진행되지 않거나 대체수단 발급을 거부하고 있음

4-3. 민감 개인정보 수집 금지

4.3 **사상·신념·과거병력 등 개인의 권익이나 사생활을 현저하게 침해할 우려가 있는 민감한 개인정보의 수집 금지**

■ 심사내용 설명

<table>
<tr><th>구분</th><th>주요 내용</th></tr>
<tr><td>민감정보
수집금지</td><td>• 본인확인설비내 본인확인 목적 외에 민감정보 수집·이용 불가
※ 민감정보의 범위
<table>
<tr><th>구분</th><th>설명</th></tr>
<tr><td>사상·신념</td><td>• 각종 이데올로기 또는 사상적 경향, 종교적 신념</td></tr>
<tr><td>정치적 견해</td><td>• 정치적 사안에 대한 입장이나 특정 정당의지지 여부에 관한 정보</td></tr>
<tr><td>노동조합·정당의 가입·탈퇴</td><td>• 노동조합 또는 정당에의 가입·탈퇴에 관한 정보</td></tr>
<tr><td>건강 및 성생활에 관한 정보</td><td>• 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애(장애등급 유무 등), 성적취향 등에 관한정보
※ 혈액형은 이에 해당하지 않음</td></tr>
<tr><td>사생활을 현저하게 침해할 우려가 있는 개인정보</td><td>• 유전자 검사 등의 결과로 얻은 유전 정보, 범죄 경력에 관한 정보
• 벌금 이상의 형의 선고·면제 및 선고 유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소, 벌금 이상의 형과 함께 부과된 몰수, 추징, 사회봉사명령, 수감명령 등의 선고 또는 처분 등 범죄경력에 관한 정보
• 개인의 신체적·생리적·행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통하여 생성한 정보(생체인식정보)
• 인종이나 민족에 관한 정보</td></tr>
</table></td></tr>
<tr><td>생체인식정보
별도 동의</td><td>• 본인확인 목적을 위해 생체인식정보를 수집하는 경우 필요한 사항을 모두 알리고 다른 개인정보 처리에 대한 동의와 별도로 동의 획득
– 단, 법령에서 생체인식정보의 처리를 요구하거나 허용하는 경우에는 동의 없이 생체인식정보 처리 가능</td></tr>
</table>

■ 관련 법규

● 개인정보 보호법 제23조(민감정보의 처리 제한)

– 개인정보 보호법 시행령 제18조(민감정보의 범위)

■ 심사 대상

- 민감정보 수집 및 처리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 민감정보를 수집하는 경우 수집·처리 관련 자료 – 이용자 동의 징구 화면 스크린샷, 관련 법령 근거 등
담당자 인터뷰	• 개인정보보호 담당자 – 민감정보 처리 및 동의 징구 관련 설명 – 법령에 근거하여 민감정보 처리 시 해당 법령상의 구체적인 처리 근거 설명
현장실사	• 민감정보를 처리하는 경우 이용자로부터 별도의 동의를 받거나 관련 법령에 근거가 있는지 확인

■ 사례 검토

미흡사례 1	• 이용자에게 별도 동의 없이 민감정보를 수집하고 있으나 관련 법령에 구체적인 처리 근거가 없음
미흡사례 2	• 본인확인을 위해 생체인식정보 등 민감정보를 수집하고 있으나, 민감정보 처리에 관한 사항을 별도로 구분하지 않고 다른 개인정보 항목과 함께 포괄동의를 받고 있는 경우

4-4. 개인정보의 이용내역확인·동의철회 및 정정

4.4.가 본인확인서비스에 가입된 이용자가 개인정보의 수집·이용·제공에 대한 동의를 철회하는 기능

■ 심사내용 설명

<table>
<tr><th>구분</th><th>주요 내용</th></tr>
<tr><td>동의철회</td><td>• 이용자 또는 그 대리인의 동의 철회 요구를 개인정보 수집방법·절차보다 쉽게 할 수 있도록 권리 행사 방법 및 절차를 마련
• 이용자의 권리행사 방법 및 절차는 최소한의 개인정보 수집절차 또는 대체수단 발급 절차에 준하여 알기 쉽고 편리하여야 하며 개인정보 수집 시 요구하지 않던 증빙서류를 추가로 요구하지 않아야 함
• 이용자 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 수집된 개인정보는 보유기간 경과에 따라 지체없이 파기하는 등 필요한 조치를 수행
• 이용자 동의철회에도 불구하고 다른 법령 등의 요건에 따라 즉시 파기하지 않는 경우에는 해당 개인정보는 분리 보관
※ 다른 법령에 따른 개인정보 보존요건 예시
전자상거래 등에서 소비자 보호에 관한 법률
1. 표시·광고에 관한 기록: 6개월
2. 계약 또는 청약철회 등에 관한 기록: 5년
3. 대금결제 및 재화 등의 공급에 관한 기록: 5년
4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년</td></tr>
<tr><td>파기</td><td>• 동의를 철회한 때에는 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 이행
• 개인정보 파기 시 복구 또는 재생되지 아니하도록 조치</td></tr>
</table>

■ 관련 법규

- 개인정보 보호법 제21조(개인정보의 파기)
  - 개인정보 보호법 시행령 제16조(개인정보의 파기 방법)
  - 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)
- 개인정보 보호법 제37조(개인정보의 처리정지 등)
  - 개인정보 보호법 시행령 제44조(개인정보의 처리정지 등)

- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
  - 개인정보 보호법 시행령 제45조(대리인의 범위 등)

심사 대상

- 이용자 권리 행사 방법 및 절차
- 이용자 동의 철회 시 파기 등 조치 관련 사항

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 이용자 권리 행사 방법 및 절차 관련 자료 – 권리 행사 방법 및 절차서 등 관련 문서 자료 • 이용자 동의 철회 시 파기 등 조치 관련 자료 – 파기 등 조치 증적 – 보존의무가 부여된 경우 관련 법령 근거 자료
담당자 인터뷰	• 개인정보보호 담당자 – 권리 행사 방법 및 절차 관련 설명 – 이용자 동의 철회 시 파기 등 조치 관련 설명 – 보존의무가 부여된 경우 관련 법령 근거 설명
현장실사	• 이용자 또는 그 대리인의 동의 철회 요구 시 권리 행사 방법 및 절차를 마련하고 있는지 확인 • 이용자 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등의 조치사항 확인 • 동의 철회에도 불구하고 다른 법령에 따른 보존의무가 있는 경우 해당 개인정보를 분리하여 보관하고 있는지 확인

사례 검토

미흡사례 1	• 개인정보에 대한 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 요구 방법을 이용자가 알 수 있도록 공개하지 않음
미흡사례 2	• 대체수단 발급 시 온라인을 통해 쉽게 가입이 가능하였으나 대체수단 폐지 시에는 신분증 등 추가 서류를 제출하게 하거나 오프라인 방문을 통해서만 가능하도록 제한

4.4.나 이용자가 자신의 개인정보에 대한 열람 또는 이용내역의 제공을 요구할 수 있고, 오류가 있는 경우 정정을 요구하는 기능

■ 심사내용 설명

<table>
<tr><th>구분</th><th>주요 내용</th></tr>
<tr><td>열람요구</td><td>• 이용자 또는 그 대리인의 열람 요구 또는 이용내역 제공 요구를 개인정보 수집방법·절차보다 쉽게 할 수 있도록 권리 행사 방법 및 절차를 마련
• 이용자의 권리행사 방법 및 절차는 최소한의 개인정보 수집절차 또는 대체수단 발급 절차에 준하여 알기 쉽고 편리하여야 하며 개인정보 수집 시 요구하지 않던 증빙서류를 추가로 요구하지 않아야 함
• 이용자 또는 그 대리인으로부터 개인정보 열람 요구 또는 이용내역 제공 요구를 받은 경우 10일 이내(또는 지체없이)에 이용자가 해당 개인정보(또는 이용내역)를 열람 제공
이용자가 열람이나 제공을 요구할 수 있는 정보
1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용 목적
3. 개인정보의 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용</td></tr>
<tr><td>이용·제공 내역 통지</td><td>• 개인정보보호 법령에 따라 연1회 이상 주기적으로 해당 정보주체(이용자)에게 개인정보 이용·제공 내역을 통지
– 통지 사항 : 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목, 개인정보를 제공받은 제3자와 그 제공 목적 및 제공한 개인정보의 항목(다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외)
– 통지 방법 : 서면·전자우편·전화·문자전송, 알림창(단, 개인정보의 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 통지하는 경우로 한정) 등
– 통지 예외 : 통지에 대한 거부의사를 표시한 정보주체, 개인정보처리자가 업무수행을 위해 그에 소속된 임직원의 개인정보를 처리한 경우 해당 정보주체, 법률에 특별한 규정이 있거나 법령 상 의무를 준수하기 위하여 이용·제공한 개인정보의 정보주체 등</td></tr>
<tr><td>열람거부</td><td>• 10일 이내에 열람할 수 없는 정당한 사유가 있는 경우 이용자에게 그 사유를 알리고 열람을 연기할 수 있음
• 개인정보 열람 제한 및 거절의 사유가 있는 경우 이용자에게 그 사유를 알리고 열람을 제한 또는 거절할 수 있음
• 열람 요구사항 중 일부가 열람 제한 또는 거절의 사유가 있는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며 열람이 제한되는 사항을 제외한 부분에 대해서는 열람할 수 있도록 하여야 함
• 이용자가 열람 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내</td></tr>
</table>

구분	주요 내용
정정·삭제 요구	• 이용자 또는 그 대리인으로부터 개인정보의 정정·삭제를 요구받은 경우 이용자의 요구가 정당하다고 판단되면 지체 없이 그 개인정보를 조사하여 이용자의 요구에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 후 그 결과를 10일 이내에 이용자에게 알려야 함

관련 법규

- 개인정보 보호법 20조의2(개인정보 이용·제공 내역의 통지)
  - 개인정보 보호법 시행령 제15조의3(개인정보 이용·제공 내역의 통지)
- 개인정보 보호법 제35조(개인정보의 열람)
  - 개인정보 보호법 시행령 제41조(개인정보의 열람절차 등)
- 개인정보 보호법 제36조(개인정보의 정정·삭제)
  - 개인정보 보호법 시행령 제43조(개인정보의 정정·삭제 등)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
  - 개인정보 보호법 시행령 제45조(대리인의 범위 등)

심사 대상

- 이용자 권리 행사 방법 및 절차
- 이용자의 개인정보 열람권 보장 관련 사항
- 본인확인서비스 이용내역 제공 절차 및 방법
- 이용자의 개인정보 오류 정정 절차 및 방법

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 이용자 또는 대리인의 권리 행사 방법 및 절차 관련 자료 – 권리 행사 방법 및 절차서 등 관련 문서 자료 • 이용자 또는 대리인의 개인정보 열람 요구 또는 이용내역 제공 요구에 대한 절차 및 관련 자료 • 이용자 또는 대리인의 개인정보 정정·삭제 요구에 대한 절차 및 관련 자료

구분	준비사항
담당자 인터뷰	• 개인정보보호 담당자 – 권리 행사 방법 및 절차 관련 설명 – 개인정보 열람 요구 또는 이용내역 제공 요구에 대한 절차 설명 – 개인정보 정정·삭제 요구에 대한 절차 설명 – 법률에 따른 개인정보 열람 제한 및 거절되는 경우에 해당 되는 업무가 존재하는 확인 – 개인정보 이용·제공 내역 통지 절차가 적절한지 여부
현장실사	• 이용자 또는 그 대리인의 열람 요구 또는 이용내역 제공 요구 시 권리 행사 방법 및 절차를 마련하고 있는지 확인 • 개인정보의 열람 요구 또는 이용내역 제공 요구에 대하여 열람 요구를 접수받은 날로부터 10일 이내에 회신하고 있는지 확인 • 개인정보의 정정·삭제 요구에 대하여 정정·삭제 요구를 접수받은 날로부터 10일 이내에 회신하고 있는지 확인 • 개인정보 이용·제공 내역 통지 화면 및 통지 관련 프로그램 확인

■ 사례 검토

미흡사례 1	• 개인정보에 대한 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 요구 방법을 이용자가 알 수 있도록 공개하지 않음
미흡사례 2	• 개인정보의 열람 요구에 대하여 정당한 사유의 통지 없이 열람 요구를 접수받은 날로부터 10일을 초과함

4.4.다 이용자의 오류 정정요구에 대한 조치가 완료되기 전까지 해당 이용자의 개인정보 제공 또는 이용을 제한하는 기능

■ 심사내용 설명

구분	주요 내용
정정 조치 완료 전 이용·제공 제한	• 이용자의 오류 정정요구에 대한 조치가 완료되기 전까지는 해당 개인정보의 이용 및 제공을 제한
개인정보 처리정지 요구	• 이용자 또는 그 대리인으로부터 개인정보의 처리정지 요구를 받은 경우 특별한 사유가 없는 한 지체 없이 처리의 전부 또는 일부를 정지하고 그 결과를 이용자에게 제공 • 개인정보 처리정지 요구를 받은 날부터 10일 이내에 조치 결과를 이용자에게 회신 • 개인정보의 처리정지를 거절할 수 있는 사유가 있는 경우 관련 사실을 처리정지 요구자에게 요구를 받은 날로부터 10일 이내에 알려야 함 • 정보주체가 처리정지 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내

■ 관련 법규

- 개인정보 보호법 제36조(개인정보의 정정·삭제)
  - 개인정보 보호법 시행령 제43조(개인정보의 정정·삭제 등)
- 개인정보 보호법 제37조(개인정보의 처리정지 등)
  - 개인정보 보호법 시행령 제44조(개인정보의 처리정지 등)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
  - 개인정보 보호법 시행령 제45조(대리인의 범위 등)

■ 심사 대상

- 이용자 권리 행사 방법 및 절차
- 이용자의 개인정보 정정 요구 보장 관련 사항
- 이용자의 개인정보 처리정지 요구 보장 관련 사항

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 이용자 권리 행사 방법 및 절차 관련 자료 – 권리 행사 방법 및 절차서 등 관련 문서 자료 • 이용자의 개인정보 정정 요구에 대한 절차 및 관련 자료 • 이용자의 개인정보 처리정지 요구에 대한 절차 및 관련 자료
담당자 인터뷰	• 개인정보보호 담당자 – 권리 행사 방법 및 절차 관련 설명 – 개인정보 정정 요구에 대한 절차 설명 – 개인정보 처리정지 요구에 대한 절차 설명 – 법령에 따른 개인정보 처리정지 거절에 해당 되는 업무가 존재하는 지 확인
현장실사	• 이용자 또는 그 대리인의 정정 및 처리 정지 요구 시 권리 행사 방법 및 절차를 마련하고 있는지 확인 • 개인정보 정정 요구에 대한 조치가 완료되기 전까지 해당 이용자의 개인정보 제공 또는 이용을 제한하는 절차 및 기능이 적용되어 있는지 확인 • 개인정보의 처리정지 요구에 대하여 정정 및 처리정지 요구를 접수받은 날로부터 10일 이내에 조치 결과를 회신하고 있는지 확인

사례 검토

미흡사례 1	• 개인정보에 대한 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 요구 방법을 이용자가 알 수 있도록 공개하지 않음
미흡사례 2	• 개인정보의 처리정지 요구에 대하여 처리정지 요구를 접수받은 날로부터 10일을 초과함
미흡사례 3	• 이용자로부터의 개인정보 정정요구에 대한 정정조치가 진행 중인 단계에서 해당 개인정보의 이용 및 제공을 제한하지 않고 계속적으로 이용 또는 제공

4-5. 이용자 불만 등을 접수·처리하기 위한 절차

4.5.가 **대체수단의 발급·이용 및 연계정보의 제공 등과 관련한 불만을 접수·처리할 수 있는 절차를 마련하고 담당자를 지정하여야 함**

■ 심사내용 설명

구분	주요 내용
불만처리	• 본인확인서비스 이용자로부터 대체수단의 발급·이용 등과 관련한 불만을 접수하고 처리할 수 있는 상담창구를 마련 – 상담창구(예시): 전화, ARS, 이메일, 게시판 등 • 이용자 불만 접수 및 처리에 관한 기록을 남기고, 법적 요건 등을 고려하여 보유기간 설정 • 이용자 불만 관련 자료의 보유기간 경과 시 파기 절차를 마련 ※ 타 법령에 따른 최소 보유기간(예시) **전자상거래 등에서 소비자 보호에 관한 법률** 1. 표시·광고에 관한 기록: 6개월 2. 계약 또는 청약철회 등에 관한 기록: 5년 3. 대금결제 및 재화 등의 공급에 관한 기록: 5년 4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년

■ 관련 법규

- 개인정보 보호법 제21조(개인정보의 파기)
  - 개인정보 보호법 시행령 제16조(개인정보의 파기 방법)
  - 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

■ 심사 대상

- 이용자 불만 접수 방법 및 처리 절차
- 보유기간 경과 또는 처리목적이 달성된 이용자 불만 관련 자료의 파기 절차

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 이용자 불만 접수 및 처리 절차 관련 자료 • 보유기간이 경과된 이용자 불만 자료에 대한 파기 증적 – 파기배치 등 증적 – 보존의무가 부여된 경우 관련 법령 근거 자료
담당자 인터뷰	• 개인정보보호 담당자 – 이용자 불만 접수 및 처리 절차 관련 설명 – 불만 관련 자료 파기 배치 관련 설명
현장실사	• 이용자의 불만을 접수하고 처리하기 위한 방법 및 절차를 마련하고 있는지 확인 • 이용자 불만 접수 및 처리에 관한 기록을 법적 요건에 따른 기간 동안 보관하고 있는지 확인 • 이용자 불만 접수 및 처리에 관한 기록의 보유기간이 경과한 경우 지체없이 파기하고 있는지 확인

■ 사례 검토

미흡사례 1	• 본인확인서비스 이용자로부터 대체수단의 발급·이용 등과 관련한 불만을 접수하고 처리할 수 있는 상담창구를 운영하지 않음

4.5.나 부정한 방법으로 대체수단의 발급 또는 분실·훼손·도난·유출 시 해당 사실을 본인확인기관에 신고할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
부정사용 신고기능	• 부정한 방법으로 대체수단의 발급 또는 대체수단의 분실·훼손·도난·유출 시 해당 사실을 본인확인기관에 신고 기능 제공

■ 관련 법규

● 해당 없음

■ 심사 대상

● 대체수단의 발급 또는 분실·훼손·도난·유출 시 신고 방법 및 절차

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단의 발급 또는 분실·훼손·도난·유출 시 신고 방법 및 절차 관련 자료
담당자 인터뷰	• 개인정보보호 담당자 – 대체수단 부정발급 등 신고 방법 및 절차 관련 설명
현장실사	• 부정한 방법으로 대체수단의 발급 또는 분실·훼손·도난·유출 시 해당 사실을 본인확인기관에 신고할 수 있는 창구를 운영하고 있는지 확인

■ 사례 검토

미흡사례 1	• 대체수단 부정발급 또는 대체수단의 분실·훼손·도난·유출 시 본인확인기관에 신고할 수 있는 창구를 운영하지 않음

5. 긴급상황 및 비상상태의 대응에 관한 사항

5.1 장애 및 재해발생에 효과적으로 대처할 수 있는 비상계획 및 재난복구절차

■ 심사내용 설명

구분	주요 내용
정책수립	• 본인확인서비스 업무 연속성을 위협하는 IT재해를 분류하고 유형별 피해 규모 산정 및 본인확인업무 영향도 분석 수행 • 본인확인서비스에 대한 복구 목표시간(RTO), 복구 목표시점(RPO) 수립 • 본인확인서비스에 대한 재난/재해 발생 시 핵심서비스의 업무연속성을 보장할 수 있는 비상복구전략, 복구 조직 수립에 대한 계획 및 승인
재난 복구훈련	• 본인확인서비스에 대한 업무 연속성 모의훈련 수행 및 개선사항 도출

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인서비스를 위한 DB, 서버, 네트워크, 보안솔루션, 클라우드 솔루션 등
- IDC 내 2중화 전원, 항온항습기, UPS, 배터리, 소화장비, 출입통제장치, CCTV 등 설비 일체

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 업무연속성(BCP) 정책 및 지침 • 본인확인서비스 IT 재해 복구 지침서(본인확인서비스에 대한 RTO / RPO 산정근거, 업무영향도 분석, 비상연락망 등 포함) • 유지보수업체의 월간 정기점검 보고서(전원, UPS, 배터리 포함) • 본인확인서비스 업무연속성 관련 모의훈련 계획서 및 완료보고서

구분	준비사항
담당자 인터뷰	• 본인확인서비스 업무연속성에 대한 범위 및 투자 의사결정 프로세스 • 본인확인서비스 업무연속성 모의훈련 결과 개선사항 도출항목 • 월간 정기점검 보고서에 대한 검토 및 피드백 진행 여부
현장실사	• IDC 내 2중화 전원, 항온항습기, UPS, 전원공급장치, 소화장비, 출입통제장치, CCTV 등 설비 일체에 대한 현장확인 • 서버, DB, 네트워크, 보안솔루션 등 정보시스템에 대한 비상대응 현장확인

■ 사례 검토

미흡사례 1	• 업무연속성 및 IT재해 복구 지침서 등에 본인확인서비스 및 정보시스템에 대한 복구 우선순위, 복구 목표시간(RTO), 복구 목표시점(RPO) 등이 산정되어 있지 않음
미흡사례 2	• IDC 내 2중화 전원, 항온항습기, UPS, 배터리, 소화장비 등 설비에 대하여 유지보수업체가 진행한 수행업무 및 유지보수 일지에 대한 정기적인 점검 및 주요 이슈관리를 하지 않음
미흡사례 3	• 본인확인서비스 업무연속성을 위하여 백업센터를 구축 및 운영하고 있으나, 관련 정책에 백업센터를 활용한 재해 복구 절차 및 이행계획 등 이 수립되어 있지 않아 실질적인 장애복구를 수행이 불가함

5.2 운영데이터, 소프트웨어, 시스템, 설비에 대한 백업계획 및 복구계획

■ 심사내용 설명

구분	주요 내용
정책수립	• 본인확인서비스 관련 운영데이터, 소프트웨어, 어플리케이션, 소스코드, 정보시스템, 설비 등에 대한 백업 정책 및 복구 계획 수립 • 본인확인서비스 관련 백업 대상 선정기준, 백업 주기, 백업 방법, 백업 절차 등에 대한 수립
시스템 복구훈련	• 복구절차의 적절성을 확인하기 위한 정기적인 복구 테스트 수행 • 화재, 홍수 등 재해/재난에 대비하기 위한 백업 매체를 통한 소산 백업 등의 추가적인 보안 대책 마련 • 정기적인 복구 테스트와 재해·재난 대응 계획의 적정성 점검

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인서비스 운영데이터, 소프트웨어, 정보시스템, 소스 코드 등
- 본인확인서비스 DBMS(데이터+로그), 서버(OS+환경설정파일), 네트워크 장비 환경설정 파일

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 관련 백업 및 복구 지침서 • 본인확인서비스 관련 복구 테스트 결과 보고서 (유의미한 RPO, RTO 산정 기준 확인) • 소산 백업 현황
담당자 인터뷰	• 본인확인서비스 관련 백업 대상 및 선정기준 • 본인확인서비스 DBMS 복구 테스트를 위한 시나리오(작업계획서)
현장실사	• 본인확인서비스 운영데이터, 소스 코드, 어플리케이션, 소프트웨어, 정보시스템에 대한 백업 솔루션 현황 점검 • 지침서에 규정된 RPO/RTO와 실제 복구 테스트 결과 비교

사례 검토

미흡사례 1	• 본인확인서비스와 관련하여 백업 대상, 백업 주기, 백업 방법, 백업 절차 등이 포함된 백업 정책 및 복구 지침서가 존재하지 않음
미흡사례 2	• 상위 지침 또는 내부 지침에 주기적으로 백업매체에 대한 복구 테스트를 수행하도록 되어 있으나 본인확인서비스에 대하여 복구 테스트를 장기간 수행하지 않음
미흡사례 3	• 백업 및 복구 계획서에 명시된 본인확인서비스 관련 RPO와 RTO가 실제 복구테스트 수행 결과와 현저히 차이가 발생

5.3 연계정보 알고리즘 및 키 노출 시 대응절차

■ 심사내용 설명

구분	주요 내용
CI 처리절차	• 본인확인 연계정보 CI에 대한 정당한 생성 절차 수립
CI 생성 알고리즘 관리	• 본인확인 연계정보 생성을 위한 소스코드와 비밀정보에 대한 안전한 관리 및 접근통제 수행 • 본인확인 연계정보 생성용 알고리즘에 입력되는 KISA와 공유하는 비밀정보에 대한 안전한 암호화 수행 • 본인확인 연계정보 생성이 가능한 SW모듈을 외부환경으로 반출 시 안전한 방법 및 정보보호 최고책임자의 승인하에 수행 – CI 생성 알고리즘의 반출은 원칙적으로 불가하며, 규제샌드박스 제도에 따른 CI 일괄변환을 위하여 예외적으로 가능
CI 생성 비상대응	• 본인확인 연계정보 CI_1 필드 이외에 CI_2 필드도 사용가능하도록 인터페이스 전문 수정 반영 • 본인확인 연계정보 CI 생성 알고리즘에 KEY 노출 시 대응 절차 수립

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인서비스를 위한 연계정보(CI) 생성 및 인터페이스 소스코드, 해당 모듈
- 상용 암호화 솔루션 및 연계정보 관련 JAVA, C 언어를 위한 함수 및 유틸리티

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인 연계정보 생성모듈 보안관리 기준 • 본인확인 연계정보 생성모듈 접근통제 정책 • 본인확인 연계정보 알고리즘/KEY 노출 시 대응 훈련 시나리오 • 본인확인 연계정보 알고리즘 및 암호화 KEY 보안관리 현황 • CI_2 필드가 정의된 연계정보 인터페이스 전문 규격서
담당자 인터뷰	• 본인확인 연계정보 암호화에 대한 기준 및 접근통제 정책 • CI_2 필드가 적용된 인터페이스 전문 현행화 사용 여부 • 암호화 KEY 노출에 따른 비상 대응 절차 수립 여부
현장실사	• 본인확인 연계정보 생성모듈 소스 코드 점검 • 본인확인 연계정보 생성모듈 사용된 암호화 알고리즘 및 KEY 길이 점검 • CI_2 필드가 적용된 인터페이스 전문 모니터링 점검

■ 사례 검토

미흡사례 1	• 본인확인 연계정보 생성용 알고리즘에 입력되는 KISA와 공유하는 비밀정보에 대한 안전한 암호화를 수행하지 않거나 안전하지 않은 암호화 알고리즘을 사용하고 있음
미흡사례 2	• 본인확인 연계정보를 위한 암호화 KEY가 해당모듈 또는 소스코드, 인터페이스 전문에 하드 코딩 되어 있음
미흡사례 3	• 본인확인 연계정보 CI 생성 알고리즘에 사용되는 KEY 노출 시 비상 대응 절차가 수립되지 않음
미흡사례 4	• 비상사태 발생 시 CI_1 필드 이외에 CI_2 필드를 사용할 수 있도록 인터페이스 전문이 현행화 되지 않음

[붙임] CI 알고리즘 및 키 노출 시 대응 시나리오

- (사고발생 예시) CI 생성 알고리즘이 노출되거나 대규모 CI 유출사고 발생하여 CI 알고리즘의 교체가 필요한 경우

- 사실확인 절차

순번	대상	대응절차	기간
1	사업자	직원 또는 본인확인서비스 담당자가 이상 징후 발견 → 본인확인기관에 해당 사실을 전달 ※ 본인확인기관은 관련 업무담당자를 지정, 미리 사업자에게 공지	즉시전달
2	본인확인기관	사실 확인 후 KISA에 확인사실 전달	2일 이내
3	KISA	사실 확인	1일 이내

- 대응 절차

순번	대상	대응절차	기간
4	KISA	CI생성 본인확인기관에 CI 생성체계 변경 요청(CI_1 → CI_2)	사실 확인 후 즉시 전달
5	본인확인기관	CI_2 사업자 배포 ※ 본인확인기관은 CI_1과 CI_2를 함께 배포	2주 이내
6	KISA	CI_2 배포 현황파악 및 CI_1 제공 중단 여부 검토	2주~3개월
7	방송통신위원회 및 KISA	CI_1 제공 중단여부 결정 ※ 본인확인기관은 CI_2 체계로 전환	3개월* 이후

※ 3개월 : 비상상황의 경중, CI_2 배포현황, 전환절차 등 상황에 따라 해당기간(3개월)은 변동 가능

5.4 하나의 회선에 장애가 발생하더라도 본인확인 업무를 지속적으로 제공할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
정책수립	• 본인확인서비스 데몬 및 모듈에 대한 모니터링을 통하여 장애 최소화 정책 수립
회선 이중화	• 네트워크 장비의 BGP 라우팅 프로토콜 등을 통한 회선 2중화 구축
회선장애 대응	• 하나의 회선에 장애가 발생하더라도 자동 Fail-Over 또는 수동 절체를 통하여 지속적인 본인확인서비스 제공 • 본인확인서비스 어플리케이션 레벨에서 특정 트래픽을 변경할 수 있는 아키텍처 구축 – 관리자 페이지에서 회선 수동 절체 기능 또는 소스 코드에서 본인확인서비스 데몬 이상여부 체크 후 Fail-Over 기능 구현

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제12조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인서비스 관련 네트워크 장비 : L4 스위치, L3 라우터, L3 스위치
- 라우팅 프로토콜 및 라우팅 테이블, 네트워크 모니터링 시스템
  - NMS 툴, MRTG, PRTG 등
- 본인확인서비스 관련 관리자 페이지, Fail-Over 로직 수행 소스 코드 및 모듈

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 네트워크 구성도 • 본인확인서비스 네트워크 장비 Config, 라우팅 프로토콜 • 본인확인서비스 장애 모니터링 점검 증적 및 장애처리 정책 • 본인확인서비스 관리자 페이지, Fail-Over 적용 소스 코드

구분	준비사항
담당자 인터뷰	• 본인확인서비스 회선을 수동으로 절체하는 경우와 자동절체되는 경우 서비스 정상 여부 진단 근거 • 본인확인서비스 장애 방지 시나리오를 통한 훈련 수행 여부
현장실사	• 본인확인서비스 관련 네트워크 장비 Config 점검 • 본인확인서비스 트래픽 절체 소스 코드 및 모듈 점검 • 본인확인서비스 현재 데몬 및 패킷 실패율 모니터링 여부 점검

사례 검토

미흡사례 1	• 본인확인서비스 네트워크 장비 프로토콜에 BGP 프로토콜 미설정 또는 물리적으로 네트워크 회선이 2중화되지 않음
미흡사례 2	• 본인확인서비스 관련된 네트워크 및 어플리케이션 장애 모니터링을 수행하지 않음

6. 본인확인업무를 위한 내부규정의 수립 및 시행에 관한 사항

6.1 개인정보관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항

■ 심사내용 설명

구분	주요 내용
개인정보보호 조직 구성·운영	• 개인정보보호 업무를 수행하는 조직을 구성하여 운영
개인정보관리책임자 등 지정	• 개인정보보호 업무 관련 책임자와 담당자를 지정 • 개인정보 보호책임자는 관련 법령에 따른 자격요건을 갖춘 자로 지정

■ 관련 법규

- 개인정보 보호법 제29조(안전조치 의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
  - 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)
- 개인정보 보호법 제31조(개인정보 보호책임자의 지정)
  - 개인정보 보호법 시행령 제32조(개인정보 보호책임자의 업무 및 지정요건 등)

■ 심사 대상

- 개인정보보호 관련 책임자와 담당자 지정 여부
- 개인정보보호 관련 책임자의 역할 및 책임
- 개인정보보호 관련 책임자와 담당자의 활동에 대한 평가 체계
- 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통 체계

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 개인정보보호 조직도 • 개인정보 보호책임자 등 개인정보보호 관련 책임자와 담당자 지정 현황 • 개인정보보호 관련 책임자의 역할 및 책임 기술서 – 직무기술서 등 • 개인정보보호 관련 활동 평가 체계 – KPI, MBO, 인사평가 등 • 개인정보보호 관련 의사소통을 위한 협의체 등 운영 현황 – 관련 보고서, 회의록, 공지 등
담당자 인터뷰	• 개인정보보호 책임자 및 담당자 – 역할 및 책임 관련 설명 – 개인정보보호 관련 활동 평가 체계 설명 – 개인정보보호 관련 의사소통 체계 및 절차 설명
현장실사	• 개인정보보호 관련 책임자와 담당자를 지정하고 있는지 확인 • 개인정보 보호책임자가 개인정보 보호법 등에서 요구하는 자격요건을 갖추고 있는지 확인 • 개인정보보호 관련 책임자와 담당자의 역할과 책임을 명확히 정의하고 있는지 확인 • 개인정보보호 관련 책임자와 담당자의 활동의 평가할 수 있는 체계를 마련하여 주기적으로 평가하고 있는지 확인 • 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계 및 절차를 운영하고 있는지 확인

사례 검토

미흡사례 1	• 개인정보보호책임자가 지정되어 있으나 관련 법령에서 요구하는 역할 및 책임이 내부 지침이나 직무기술서 등에 구체적으로 명시되어 있지 않음
미흡사례 2	• 개인정보보호 관련 책임자 및 담당자의 활동을 주기적으로 평가할 수 있는 기준, 지표 등의 체계가 마련되어 있지 않음

6.2 개인정보를 처리하는 직원의 교육에 관한 사항

■ 심사내용 설명

구분	주요 내용
개인정보보호 교육	• 연간 개인정보보호 교육 계획을 수립하고 경영진의 승인을 받아야 함 ※ 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화 ※ 교육 목적 및 대상, 교육 내용, 교육일정 및 방법 등이 구체적으로 포함되어야 함 • 교육대상은 본인확인업무와 관련된 임직원, 임시직원, 외주용역업체 직원 등 모든 인력을 포함하여야 함 ※ 수탁자 및 파견된 직원인 경우 해당 업체가 교육 시행할 수 있도록 관련 자료 제공, 시행 여부를 관리·감독하는 방식도 가능 • 개인정보보호 교육 계획 등에 따라 연1회 이상 개인정보보호 교육 시행 • 교육 시행 후 교육 공지, 교육 자료, 출석부 등과 같은 기록 보관

■ 관련 법규

- 개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
  - 개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)
- 개인정보 보호법 제28조(개인정보취급자에 대한 감독)
- 개인정보 보호법 제29조(안전조치 의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
  - 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

■ 심사 대상

- 연간 개인정보보호 교육 수립 및 경영진 승인 여부
- 개인정보보호 교육 시행의 적절성
- 개인정보보호 교육에 대한 적절성 및 효과성 측정 등 평가 체계

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 연간 개인정보보호 교육 계획 • 연간 교육계획에 대한 경영진의 승인 증적 • 연간 교육계획에 따른 교육 시행 관련 증적 – 본인확인업무 관련 모든 임직원과 외부인 포함 여부 • 개인정보보호 교육에 대한 효과 측정 등 평가 관련 자료 – 설문, 퀴즈 등
담당자 인터뷰	• 개인정보보호 책임자 및 담당자 – 연간 개인정보보호 교육 계획 설명 – 교육 시행 현황 및 추가 교육 방안 설명 – 개인정보보호 교육 평가를 위한 설문 등 평가 체계 설명
현장실사	• 연간 개인정보보호 교육 계획을 수립하고 경영진의 승인을 받았는지 확인 • 교육 대상에 본인확인업무 관련 임직원 및 외부자가 누락 없이 모두 포함되었는지 확인 • 교육 시행에 따른 교육 효과와 적정성을 평가하고 개선사항을 도출하여 차기 교육 계획에 반영하고 있는지 확인

■ 사례 검토

미흡사례 1	• 타당한 사유 없이 연간 개인정보보호 교육 계획을 수립하지 않음
미흡사례 2	• 교육계획에 본인확인업무 관련 일부 임직원이 포함되어 있지 않음
미흡사례 3	• 교육 미이수자를 파악하지 않고 있거나, 해당 미이수자에 대한 추가교육방법(전달교육, 온라인교육 등)을 수립·이행하고 있지 않음

6.3 이용자의 개인정보를 취급하는 자를 최소한으로 제한

■ 심사내용 설명

구분	주요 내용
개인정보 취급자 권한관리	• 업무상 반드시 필요한 경우에 한하여 적절한 승인절차를 통해 처리 권한이 신청·부여될 수 있도록 관리 • 부여된 개인정보 처리 권한에 대하여 주기적으로 검토

■ 관련 법규

● 개인정보 보호법 제28조(개인정보취급자에 대한 감독)

■ 심사 대상

● 개인정보 및 중요정보 취급 등 주요 직무 기준 정의

● 개인정보취급자에 대한 감독 등 관리방안 수립·이행 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 개인정보 및 중요정보 취급 등 주요 직무 기준 정의서 • 주요 직무자 및 개인정보취급자 지정 현황 • 주요 직무자 및 개인정보취급자 권한 신청 및 부여에 대한 승인 절차 • 주요 직무자 및 개인정보취급자에 대한 관리 및 통제방안 관련 증적(교육 증적, 모니터링 증적 등)
담당자 인터뷰	• 개인정보보호 책임자 또는 담당자 – 개인정보취급자 지정 절차 및 지정 현황 설명 – 주요 직무자 및 개인정보취급자 권한 신청 절차 설명 – 주요 직무자 및 개인정보취급자에 대한 관리 및 통제방안 설명
현장실사	• 개인정보 및 중요정보 취급 등 주요 직무 기준을 명확히 정의하고 있는지 확인 • 업무상 반드시 필요한 경우에 한하여 주요 직무자 및 개인정보취급자로 지정하고 있는지 확인 • 주요 직무자 및 개인정보취급자에 대한 관리 및 통제방안이 적절한지 확인(교육, 모니터링 현황 확인)

사례 검토

미흡사례 1	• 본인확인기관 사업장에 상주하면서 본인확인업무 내 정보시스템 개발·운영·보안 등 업무를 수행하는 협력사 직원에 대해 주요 직무자 및 개인정보취급자 누락
미흡사례 2	• 부서 단위로 개인정보취급자 권한을 일괄 부여하고 있어 실제 개인정보를 취급할 필요가 없는 인원까지 과다하게 개인정보취급자로 지정됨
미흡사례 3	• 주요 직무자 및 개인정보취급자 목록을 관리하고 있으나, 퇴사한 임직원이 포함되어 있고 최근 투입된 인력이 포함되어 있지 않는 등 현행화가 되어 있지 않음

6.4 본인확인업무의 안전성·신뢰성 보장 및 이용자의 개인정보 보호조치를 이행하기 위해 필요한 세부사항

■ 심사내용 설명

<table>
<tr><th>구분</th><th>주요 내용</th></tr>
<tr><td>정책수립</td><td>• 개인정보를 보호하기 위한 내부지침 등을 마련
• 개인정보보호 정책에 명시된 사항을 시행하기 위하여 필요한 세부 방법, 절차, 주기, 수행주체 등을 규정하는 지침, 절차 등을 수립
• 개인정보보호 정책·시행문서 제·개정 시 최고경영자(또는 최고경영자로부터 권한을 위임받은 자)의 승인을 받아야 함

개인정보 내부 관리계획에 포함해야 할 사항
1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항</td></tr>
<tr><td>개인정보
보호조치</td><td>• 관련 법규에서 요구하는 개인정보 보호조치
※「개인정보보호법」 제29조(안전조치의무)에 따른 안전성 확보조치 기준 고시 참고</td></tr>
</table>

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
  - 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행 및 점검)

■ 심사 대상

- 개인정보보호 정책 및 정책시행문서(지침, 절차, 매뉴얼 등) 내용 및 관리 현황
- 개인정보보호 정책·시행문서 제·개정 절차 및 방법
- 내부 관리계획 내용 및 승인 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 개인정보보호 정책 및 시행문서(지침, 절차, 매뉴얼 등) • 개인정보보호 정책·시행문서 제·개정 시 최고경영자의 승인 증적 – 전자결재 문서 등 • 내부 관리계획 최신본
담당자 인터뷰	• 개인정보보호 책임자 및 담당자 – 개인정보보호 정책 수립 및 관리 현황 설명 – 정책 시행문서(지침, 절차, 매뉴얼 등) 수립 및 관리 현황 설명 – 개인정보보호 정책·시행문서 제·개정 절차 및 최고경영자(또는 최고경영자로부터 권한을 위임받은 자) 승인 여부 설명 – 내부 관리계획 수립 및 관리 현황 설명
현장실사	• 개인정보보호 활동의 근거를 포함하는 개인정보보호 정책을 수립하고 있는지 확인 • 개인정보보호 정책에 명시된 사항을 시행하기 위하여 필요한 세부 방법, 절차, 주기, 수행주체 등을 규정하는 지침, 절차 등을 수립하고 있는지 확인 • 내부 관리계획이 관련 법규에서 요구하는 사항을 모두 포함하고 있는지 확인 – 접근 권한의 관리, 접근통제, 접속기록의 보관 및 점검 등 보호조치 기준 명시 • 개인정보보호 정책·시행문서 제·개정 시 최고경영자(또는 최고경영자로부터 권한을 위임받은 자)의 승인을 받는지 확인

■ 사례 검토

미흡사례 1	• 개인정보보호 정책 및 지침서가 최근 개정되었으나 해당 사항이 관련 부서 및 임직원에게 공유·전달되지 않아 일부 부서에서는 구 버전의 지침서를 기준으로 업무를 수행하고 있는 경우
미흡사례 2	• 개인정보 보호법 및 개인정보의 안전성 확보조치 기준이 개정되었으나, 해당 법규 개정사항을 반영하여 내부 개인정보보호 정책 및 지침을 지체없이 개정하지 않은 경우

7. 대체수단의 안전성 확보에 관한 사항

7-1. 대체수단의 발급

7.1.가 장애인 웹 접근성 및 웹 표준의 준수

■ 심사내용 설명

구분	주요 내용
웹 접근성 및 웹 표준 준수	• 본인확인서비스 관련 웹페이지는 웹 접근성 및 웹 표준 준수 ※ 웹접근성 및 웹표준 준수여부를 확인하기 위하여 전문기관에서발급한 품질인증서를 통해 확인 가능

■ 관련 법규

- 지능정보화 기본법 제46조, 48조
- 장애인차별금지 및 권리구제 등에 관한 법률 제20조

■ 심사 대상

- 본인확인서비스 용 웹페이지
- 본인확인서비스 용 모바일 페이지

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 용 웹페이지 웹 접근성 적용 현황 • 모바일 애플리케이션 접근성 지침 • CP사 서비스 표준창 현황 • 웹접근성 및 웹표준 관련 품질인증서

구분	준비사항
담당자 인터뷰	• 어떠한 사용자(장애인, 노인 등)도 사용자가 전문적인 능력 없이 웹 사이트에서 제공하는 모든 정보에 접근할 수 있는지 여부 • 어떠한 기술 환경에서도 사용자가 전문적인 능력 없이 웹 사이트에서 제공하는 모든 정보에 접근할 수 있는지 여부
현장실사	• 본인확인서비스 용 웹페이지 • 본인확인서비스 용 모바일 페이지

사례 검토

미흡사례 1	• 본인확인서비스 용 웹페이지가 웹 접근성 표준을 준수하고 있지 않음

7.1.나 대체수단의 유일성

(1) 대체수단 유일성에 대한 검사 기능

■ 심사내용 설명

구분	주요 내용
유일성 확인(발급)	• 본인확인기관의 대체수단 운영정책에 따라 발급 관리 • 대체수단 발급 시에는 다른 사용자와 유일하게 구분할 수 있는 식별정보를 활용하여 발급하는 기능과 절차를 통해 구현 • 실지명의 기반의 신원확인 절차를 통해 대체수단 발급 – 실명확인 증표의 진위 여부 검증 절차 확인 – 주민등록번호, 외국인등록번호(국내거소번호 등)에 대한 유효성 검증 절차 확인 ※ 비대면 발급 시 기타 대체수단을 통한 이용자 신원확인을 하여야 함 • 대체수단 발급시 해당 대체수단이 이미 발급되어 있다면 명의자의 본인확인을 통해 기존 대체수단을 중지 또는 폐기 • 부정발급 및 명의도용 방지방안, 발급 후 관리되지 않는 계정에 대한 통제방안 등 마련
허무인 확인	• 이용자의 주민번호를 통해 허무인(사망자 등) 여부를 확인하는 기능 마련 • 신뢰되는 주민번호DB를 통해 실존하는 사람인지 주기적으로 검증하는 방안 마련

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

- 대체수단 발급 시 수집하는 개인정보 항목
- 대체수단 발급 시 수단의 형태
- 대체수단 발급 알고리즘 및 소소코드
- 대체수단 발급 신청자의 실명확인 처리 과정
- 대체수단 발급 신청자의 허무인 검증 처리 과정
- 대체수단 인증 시 인증수단의 발급 처리 과정
- 기 발급된 본인확인정보의 발급 처리 과정

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인정보 발급 현황 • 부정발급 시도 모니터링 기준 및 이행 현황 • 본인확인정보 발급 처리 흐름도 • 허무인 검증 과정 • 실지명의 확인 과정
담당자 인터뷰	• 본인확인정보가 이용자에 대해 유일하게 식별할 수 있고 이에 대해 검사할 수 있는 기능이 있는지 여부
현장실사	• 본인확인정보 발급 과정에서 대한 처리 단계 실시 • 본인확인정보 발급 시 안전성 확보에 대한 소스코드 • 본인확인정보 발급 시 이용자 신원확인 과정에 대한 소스코드

사례 검토

미흡사례 1	• 본인확인서비스에서 유일성에 대해서 점검하는 기능이 없음
미흡사례 2	• 대체수단 발급자에 대하여 주기적으로 허무인 여부를 체크하고 있지 않아, 사망자의 대체수단이 발급되어 이용될 가능성이 있음

7.1.다 법정대리인을 통한 대체수단의 발급

(1) 만14세 미만의 자가 대체수단을 발급받고자 하는 경우에는 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원을 확인한 후 동의를 받아야 함

(2) 법정대리인의 실명인증에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치 여부 검사

■ 심사내용 설명

구분	주요 내용
만14세미만 대체수단 발급	• 만14세 미만의 자가 대체수단을 발급받을 수 있는 절차 마련 • 만14세 미만의 자가 대체수단을 발급받고자 하는 경우 법정대리인의 신원확인 후 동의 획득
법정대리인 확인	• 해당 법정대리인이 만14세 미만의 자의 실제 법정대리인이 맞는지 여부를 검증 – 이용자와 법정대리인의 관계를 증명할 수 있는 구비서류(기본증명서, 가족관계증명서 등)의 진위확인 및 법정대리인의 실제 동의 여부 등 법정대리인 확인 절차의 적정성 ※ 법정대리인이란 본인의 의사에 의하지 않고 법률의 규정에 의하여 대리인이 된 자로 미성년자의 친권자(「민법」 제909조, 제911조, 제916조, 제920조), 후견인(「민법」 제931조에서 제936조까지), 법원이 선임한 부재자의 재산관리인(「민법」 제22조, 제23조) 등이 이에 해당됨

■ 관련 법규

● 개인정보 보호법 제22조의2(아동의 개인정보 보호)

– 개인정보 보호법 시행령 제17조의2(아동의 개인정보 보호)

■ 심사 대상

● 본인확인정보 발급 심사 과정

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 만14세 미만의 자의 대체수단 발급 절차 • 만14세 미만의 자의 대체수단 발급 시 법정대리인 동의서
담당자 인터뷰	• 만14세 미만의 자가 대체수단을 발급받고자 하는 경우 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원확인 후 동의 획득 여부 • 법정대리인의 실명인증에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치성 검사 여부

구분	준비사항
현장실사	• 대체수단 발급 시 발급절차상 14세미만인 경우를 확인하는 절차 및 시스템 확인 • 만14세 미만의 자에 대한 법정대리인 동의 여부 확인 • 만14세 미만의 자에 대한 법정대리인의 동의 확인 방법

사례 검토

미흡사례 1	• 법정대리인을 통한 대체수단 발급을 제공하지 않아 만 14세 미만자에 대하여 본인확인서비스를 제공하지 않고 있음

7-2. 대체수단의 변경·관리

7.2.가 이용자가 자신의 대체수단의 발급 및 갱신·폐지 등의 정보를 열람할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
대체수단 발급내역 열람	• 본인확인정보의 발급 및 갱신·폐지에 대하여 이용자가 열람할 수 있는 기능을 제공 – 정보주체 본인(대리인)이 맞는지 여부를 확인하는 방법 제공

■ 관련 법규

- 개인정보 보호법 제35조(개인정보의 열람)

■ 심사 대상

- 대체수단 이용내역 조회 페이지
- 대체수단 발급, 갱신, 폐지를 위한 웹 페이지

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 보관 기준 및 절차 • 본인확인정보의 발급 및 갱신·폐지와 제3자 제공 내역
담당자 인터뷰	• 대체수단의 발급·갱신·폐지 등 정보를 열람할 수 있는 인터페이스가 존재하는지와 정보 열람을 위한 정당한 권한이 있는지를 확인하는지 여부 • 민원발생으로 대체수단 사용 중지하거나 중지를 해제할 수 있는 절차가 있는지 여부 • 이용자 및 이용자의 법정대리인으로부터 이용자 개인정보에 대한 열람을 요구할 수 있는 방법 또는 절차를 제공하는지 여부 • 개인정보처리자가 개인정보에 대한 열람을 요구받을 경우 기간 내에 열람 가능하도록 처리하고, 열람 할 수 없는 정당한 사유가 있을 때에는 열람 요구자에게 그 사유를 알리는지 여부 • 개인정보에 대한 열람 요청을 받은 경우 본인 여부를 확인하는 절차가 있는지 여부
현장실사	• 대체수단 발급·갱신·폐지 내역 조회시스템 확인

■ 사례 검토

미흡사례 1	• 본인확인정보의 발급 및 갱신·폐지 내역이 저장되고 있지 않음

7.2.나 이용자가 자신의 대체수단 관련 정보를 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
이용내역 열람	• 본인확인서비스 이용내역에 대하여 이용자가 열람할 수 있는 기능을 제공 – 정보주체 본인(대리인)이 맞는지 여부를 확인하는 방법 제공 • 정보주체로부터 개인정보 열람을 요구받은 경우 10일 이내에 정보주체가 해당 개인정보를 열람 할 수 있도록 조치 – 10일 이내에 열람할 수 없는 정당한 사유가 있는 경우, 정보주체에게 그 사유를 알리고 열람을 연기할 수 있음 – 개인정보 열람 제한 및 거절의 사유가 있는 경우, 정보주체에게 그 사유를 알리고 열람을 제한 또는 거절할 수 있음 – 열람 요구사항 중 일부가 열람 제한 및 거절의 사유가 있는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분에 대해서는 열람할 수 있도록 해야 함
제3자제공 열람	• 본인확인 이외의 목적으로 이용하거나 제3자에게 제공하는 것은 원칙적으로 불가 – (예외) 법령에 따른 본인확인정보의 처리를 허용한 경우 ※ 규제샌드박스 제도에 따른 모바일 전자고지, 금융마이데이터

■ 관련 법규

- 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)
- 개인정보 보호법 제35조(개인정보의 열람)
  - 개인정보 보호법 시행령 제41조(개인정보의 열람절차 등)
- 개인정보 보호법 제38조(권리행사의 방법 및 절차)
  - 개인정보 보호법 시행령 제45조(대리인의 범위 등)

■ 심사 대상

- 개인정보처리방침
- 대체수단 이용내역 DB

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 이용내역 관리 페이지 • 개인정보처리방침
담당자 인터뷰	• 본인확인 이외의 목적으로 이용하거나 제3자에게 제공된 내역을 이용자가 확인할 수 있는 기능이 있는지 확인 • 본인확인정보 발급확인서비스 제공을 위해 해당 본인확인정보의 발급·이용내역 등을 송수신이 가능한지 여부
현장실사	• 개인정보처리방침 확인을 통한 제3자 제공 사실 확인

■ 사례 검토

미흡사례 1	• 본인확인서비스 이용내역을 열람할 수 있는 기능을 제공하고 있지 않음

7.2.다 이용자가 대체수단 관련 정보의 오류에 대해 정정을 요구할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
정보오류 정정요구	• 이용자에게 대체수단 관련 정보의 오류에 대한 정정·삭제 요구 방법 또는 절차를 제공 – 정보주체 본인(대리인)이 맞는지 여부를 확인하고 정정·삭제 기능을 제공
정정요구 절차	• 대체수단 관련 정보의 정정·삭제를 요구받은 경우 10일 이내에 정보주체의 요구에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 후 그 결과를 정보주체에게 알려야 함 – 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 삭제 요구를 거절할 수 있으며, – 이 경우 요구에 따르지 않기로 한 사실, 근거 법령의 내용 및 그 이유와 이의제기 방법을 정정·삭제 통지서로 해당 정보주체에게 알려야 함(전자상거래법에 따른 계약·청약 철회 기록 등)

■ 관련 법규

- 개인정보 보호법 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등), 제38조(권리행사의 방법 및 절차)
- 개인정보 보호법 제39조의8(개인정보 이용내역의 통지)
- 표준 개인정보 보호지침 제31조(개인정보 열람 연기 사유의 소멸), 제32조(개인정보의 정정·삭제), 제33조(개인정보의 처리정지)

■ 심사 대상

- 본인확인서비스 인증 웹페이지
- 본인확인서비스 모바일 페이지

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 정보관리 또는 정정요구 기능 설명자료
담당자 인터뷰	• 대체수단 관련 정보에 오류가 있는 경우 정정·삭제를 요구할 수 있는 방법 및 절차를 제공 여부 • 대체수단 관련 정보의 정정·삭제에 대한 요구가 있는 경우 지체 없이 필요한 조치 여부 • 대체수단 관련 정보의 정정·삭제 요청을 받은 경우 본인 여부를 확인하는 절차 여부 • 대체수단 관련 정보에 대한 오류 정정을 요구할 경우 오류를 정정할 때까지 해당 이용자의 개인정보 이용 및 제공을 중단하고 있는지 여부
현장실사	• 본인확인서비스 인증 페이지 시연

■ 사례 검토

미흡사례 1	• 개인정보의 삭제 조치가 이루어졌다고 회신하였음에도 해당 개인정보의 일부가 삭제되지 않고 있음

7.2.라 대체수단 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보 발송

■ 심사내용 설명

구분	주요 내용
이용자 알림기능	• 대체수단 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보를 이메일, 스마트폰 PUSH 등을 통해 이용자에게 알려야 함

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 대체수단 발급, 인증, 폐지, 정보 변경 웹 페이지

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 발급, 인증, 폐지, 정보변경 시 관리 절차
담당자 인터뷰	• 대체수단 신규 발급, 인증, 폐지 시 이용자에게 알리고 있는지 여부
현장실사	• 대체수단 정보 수정시 확인정보 발송여부 시연

■ 사례 검토

미흡사례 1	• 대체수단 발급, 인증 시 이용자에게 별도 이용내역을 알리고 있지 않음

7-3. 대체수단 관련 정보의 저장 및 백업

7.3.가 대체수단 관련 기록의 저장·백업·삭제

(1) 이용자의 대체수단 이용내역 등에 대한 이력 관리 기능

(2) 대체수단이 폐지된 날로부터 5년 경과 후 이용자 등록정보 삭제

■ 심사내용 설명

구분	주요 내용
이용내역 정보관리	• 대체수단 관리 기능을 통해 이용자가 조회할 수 있는 기능을 제공 • 대체수단 이용내역은 최소 2년 보관하여야 함
대체수단 정보관리	• 대체수단 발급내역은 폐지된 날로부터 최소 5년 보관
삭제방법	• 보유기간 종료시 해당 정보는 모두 삭제 ※ 삭제 절차에 따라 시스템에 반영되어 있는지 확인 • 이용자 등록정보 삭제 시 복구 불가능한 수준의 안전한 방법으로 파기

■ 관련 법규

- 개인정보 보호법 제21조(개인정보의 파기)
- 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

■ 심사 대상

- 본인확인시스템 관련 DB
- 본인확인정보가 보관된 로그기록 등

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 이용내역 저장 기준 • 이용자 등록정보 파기 기준

구분	준비사항
담당자 인터뷰	• 대체수단 이용내역 관리 여부 • 대체수단 이용내역에 대한 삭제 주기
현장실사	• 해당되는 정보가 실제로 삭제되었는지 데이터베이스 검색을 통해 확인

사례 검토

미흡사례 1	• 본인확인서비스 폐지 이후 5년이 도래하였음에도 이용자 등록정보를 삭제하지 않음

7.3.나 대체수단의 발급 및 갱신·폐지와 제3자 제공 내역의 저장·관리

(1) 대체수단 신청 및 폐지에 대한 기록, 신원확인 시 제출서류, 제시한 증명서 사본, 정보통신망을 통해 입력한 정보 등에 대한 백업 기능

■ 심사내용 설명

구분	주요 내용
백업 기능	• 백업 정책에 따라 대체수단 신청·폐지기록, 정보통신망을 통해 입력한 정보 등를 백업하는 기능을 마련 ※ 자동화된 방법으로 백업 수행 시, 백업이 수행되는 환경 설정 후 백업이 자동적으로 수행되는지 확인 ※ 수동적인 방법으로 백업 수행 시, 그 방법 및 절차를 확인

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

- 본인확인시스템 DB
- 본인확인 발급, 폐지, 정정 변경 시 서류
- 본인확인 관련 정보의 백업시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 백업관리 기준
담당자 인터뷰	• 대체수단 발급·갱신·폐지 및 제3자 제공에 대한 기록을 남기고 있는지 여부 • 신원확인 시 제출서류, 제시한 증명서 사본, 정보통신망을 통해 입력한 정보 등에 대한 백업 기능을 구현하고 있는지 여부

구분	준비사항
현장실사	• 데이터가 정확하게 백업되는지 확인하기 위해 백업된 데이터를 샘플링하여 확인 • 본인확인기관이 시행하고 있는 물리적인 백업 방법이 적합한지 확인 • 개인정보의 제3자 제공 내역이 저장·관리되고 있는지 확인 • 서류 백업 및 보관 확인 • 백업 정책이 마련되어 있는지 확인 • 백업 정책에 따른 이용자의 제출서류, 증명서 사본 등 백업, 보관·폐기절차 확인

사례 검토

미흡사례 1	• 본인확인 신청 시 접수받은 서류를 안전하게 보관하고 있지 않음

7-4. 대체수단의 폐지

7.4.가 대체수단 폐지 신청시 이용자의 정당한 권한 여부를 확인하는 절차

■ 심사내용 설명

구분	주요 내용
폐지 절차	• 이용자가 대체수단 발급폐지 요청 시 본인확인기관이 이용자의 권한을 확인하는 절차를 마련 – 정보주체 본인(대리인)이 맞는지 여부를 확인하는 방법 제공

■ 관련 법규

- 개인정보 보호법 제21조(개인정보의 파기)
- 개인정보의 안전성 확보조치 기준 제13조(개인정보의 파기)

■ 심사 대상

- 대체수단 폐지 절차

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 대체수단 폐지 절차 설명자료
담당자 인터뷰	• 이용자가 대체수단 발급폐지 요청 시 본인확인기관이 이용자의 권한을 확인하는 방법에 대한 보안성을 검토하고 있는지 확인 ※ 이용자가 대체수단 폐지요청 시 정당한 권한 소유 여부를 본인확인기관이 확인하는 방법 중 아래와 같은 적절한 수단을 선정하여 활용하는지 검토 ① 대면확인 : 신원확인증표(성명, 주민번호) ② 인증서 : 성명, 전자서명 수행 및 검증 및 VID 값 검증 ③ 휴대전화 정보 : 성명, 주민번호, SMS 인증번호 ④ 본인확인기관이 정한 안전한 이용자 식별방법 ※ 실제 Process 및 보안성 여부 확인 필요 • 대체수단을 발급받은 정당한 이용자를 통해 대체수단 폐지 신청하고 있는지 확인
현장실사	• DB 검색을 통해 해당 이용자의 대체수단이 폐지된 상태임을 확인

■ 사례 검토

미흡사례 1	• 대체수단 발급 이용자가 폐지 신청 시 정당한 본인의 신청인지 확인하는 절차를 마련하고 있지 않음

7.4.나 이용자의 대체수단 폐지 요청 후 대체수단 폐지 사실을 이용자에게 통지

■ 심사내용 설명

구분	주요 내용
이용자 통지	• 대체수단 폐지 시 등록된 메일(또는 정보 수정 전 메일) 또는 SMS 등으로 해당 사실을 전달하는 기능을 마련

■ 관련 법규

● 해당사항 없음

■ 심사 대상

● 본인확인 정보시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 폐지 이력
담당자 인터뷰	• 대체수단 폐지 시 등록된 메일(또는 정보 수정 전 메일) 또는 SMS 등으로 해당 사실을 전달하고 있는지 확인
현장실사	• 대체수단 폐지 사실 이용자 폐지 시연 • 대체수단 폐지 및 이용자통지 시스템 로직 확인

■ 사례 검토

미흡사례 1	• 대체수단 폐지 요청 이후 해당 사실을 이용자에게 통지하는 절차를 마련하고 있지 않음

7-5. 대체수단의 연동

7.5.가 본인확인 인증

(1) 본인확인 입력정보를 이용한 본인확인인증이 정상적으로 이루어져야 함

(2) 본인확인 입력정보를 안전하게 보호하기 위한 수단이 제공되어야 함

■ 심사내용 설명

구분	주요 내용
본인확인 인증	• 본인확인서비스 이용절차 상 본인확인인증이 적절히 수행 – 정보주체 본인이 맞는지 여부를 인증할 수 있어야 함 • 본인확인 입력정보를 안전하게 보호하기 위한 가상키보드 보안모듈, 바이러스 검출 모듈, 본인확인을 위하여 입력한 개인정보를 암호화하는 모듈 등을 제공하는 기능 ※ 웹표준에 따라 보안모듈의 설치는 강제 사항이 아님

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제6조(접근통제)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
- 개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제)
- 개인정보의 기술적·관리적 보호조치 기준 제6조(개인정보의 암호화)

■ 심사 대상

- 본인확인 입력정보 모듈 및 입력 화면(WEB, APP)
- 본인확인 입력정보 화면에 대한 해당 소스 코드
- 가상키보드 보안모듈, 바이러스 검출 모듈, 본인확인 입력정보 암호화 모듈 등

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인정보의 발급·갱신·폐지가 정리된 시퀀스 다이어그램 또는 개인정보흐름도 • 본인확인 입력정보 화면 시연 (WEB, APP) • 본인확인 입력정보 전문 인터페이스 규격서
담당자 인터뷰	• 본인확인 입력정보 오류 발생 시 대처 방안 및 절차 • WEB/APP에 도입된 소프트웨어 보안 모듈 리스트(루팅 방지 및 난독화 솔루션 포함)
현장실사	• 정상적인 본인확인인증과 오류 발생 시 예외사항 처리 로직 점검 • WEB/APP에 도입된 소프트웨어 보안 모듈 메모리 상주 및 정상 작동 여부 점검 • 본인확인정보 변경절차 및 이력관리 점검

사례 검토

미흡사례 1	• 본인확인 입력정보 오류 발생에 대한 예외처리 절차 및 루틴이 없거나 본인확인 인증에 대한 이력관리 업무를 수행하지 않음

7.5.나 정보통신서비스제공자와의 연동

(1) 본인확인인증 시 정보통신서비스 제공자에게 전달 형식에 이름, 생년월일 정보, 성별 정보 등 본인확인결과 정보를 제공하는 기능

(2) 연계정보를 필요로 하는 사업자가 대체수단 도입 사이트에 연계정보를 요청하였을 때 본인확인기관과 대체수단 도입 사이트 간 연동 기능

■ 심사내용 설명

구분	주요 내용
본인확인 서비스 연동	• 이용자 본인확인에 따라 이름, 생년월일, 성별, 내외국인정보 등 본인확인결과정보 제공될 수 있도록 연동 인터페이스 정의 • 본인확인결과정보 외에 불필요한 개인정보의 제공 금지 • 본인확인서비스 이용 계약을 통해 반드시 필요한 경우에만 연계정보(CI) 제공

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
- 개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제)
- 개인정보의 기술적·관리적 보호조치 기준 제6조(개인정보의 암호화)

■ 심사 대상

- 본인확인서비스 인터페이스 수행 서버 (WAS, 앱 서버, DB 서버, 게이트웨이 서버 등)
- 본인확인서비스 DBMS - 본인확인 이력관리 테이블, 이용자 마스터 테이블
- 본인확인서비스 관리자 페이지 – 정보통신서비스 제공자 계약내용 관련
- 본인확인서비스 UI 및 해당 모듈, 소스 코드

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 개인정보흐름도 및 상세 시퀀스 다이어그램 • 본인확인서비스 관련 인터페이스 전문 규격서 • 본인확인서비스 관련 인터페이스 목록 • 본인확인서비스 인터페이스 소스 코드 및 모듈 • 본인확인서비스 관리자 페이지 URL • 본인확인서비스 관련 DBMS 상세 ERD, 테이블 목록, 컬럼 정보
담당자 인터뷰	• 정보서비스제공자별 본인확인서비스 계약서 작성 및 변경관리 • 본인확인인증이 완료된 후에도 CI 정보에 대한 저장관리 여부
현장실사	• 본인확인서비스 관련 인터페이스 전문 규격서별 소스 코드 점검 • 본인확인서비스 관련 인터페이스 목록 점검 • 본인확인서비스 관련 DBMS ERD, 테이블 목록 및 컬럼 점검 • 본인확인서비스 연동 기관, 전송시간 등에 대한 로그 무결성 점검 • 연계정보 CI에 대한 저장 유무 점검

■ 사례 검토

미흡사례 1	• 정보통신서비스 제공자와의 계약서 또는 합의문서에 기반하지 않고 기본값으로 연계정보 CI값을 전송하는 경우
미흡사례 2	• 정보통신서비스 제공자와 본인확인 인터페이스 전문 규격서에 정의된 이름, 생년월일, 성별 이외에 별도의 연락처 및 주소 정보도 제공하는 경우

7.5.다 중복가입확인정보의 제공

(1) 주민등록번호, 본인확인기관간 공유 비밀정보 등을 이용하여 중복가입확인정보를 제공하는 기능

■ 심사내용 설명

구분	주요 내용
중복가입 확인정보	• 이용자 본인확인에 따라 이용기관에 중복가입확인정보(DI)를 제공하는 기능 • 중복가입확인정보를 직접 생성하지 않은 본인확인기관의 경우에는 중복가입확인정보의 획득 방법 확보 • 중복가입확인정보는 주민등록번호를 저장하고 있는 본인확인설비에 저장하지 않아야 함

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인서비스 DBMS
- 본인확인기관 간 인터페이스 정보시스템
- 본인확인서비스 UI 및 해당 모듈, 중복가입확인정보(DI) 관련 소스 코드

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 개인정보흐름도 및 상세 시퀀스 다이어그램 • 본인확인서비스 관련 인터페이스 전문 규격서 • 본인확인기관 간 인터페이스 목록 • 본인확인서비스 인터페이스 소스 코드 및 모듈
담당자 인터뷰	• 정보서비스제공자별 본인확인서비스 계약서 작성 여부 • 본인확인기관 간 본인확인서비스 관련 업무 협약 내용

구분	준비사항
현장실사	• 이용자의 웹 사이트 중복가입 여부 확인 기능 실사 • 본인확인서비스 관련 인터페이스 전문 규격서별 소스 코드 점검 • 본인확인기관 간 인터페이스 파라미터(식별정보, 비밀번호) 점검 • 본인확인서비스 관련 DBMS ERD, 테이블 목록 및 컬럼 점검 • 본인확인기관 간 전송내용, 전송시간 등에 대한 로그 무결성 점검

사례 검토

미흡사례 1	• 정보통신서비스 제공자가 본인확인정보에 대한 유효성 검증을 요청할 경우 본인확인서비스 인터페이스에서 중복가입확인정보(DI)를 제공하고 있지 않음

7.5.라 연계정보의 제공

(1) 주민등록번호, 본인확인기관간 공유 비밀정보 등을 이용하여 연계정보를 제공하는 기능

■ 심사내용 설명

구분	주요 내용
연계정보	• 이용자 본인확인에 따라 이용기관에 연계정보(CI)를 제공하는 기능 • 연계정보를 직접 생성하지 않은 본인확인기관의 경우에는 연계정보의 획득 방법 확보 • 연계정보는 주민등록번호를 저장하고 있는 본인확인설비에 저장하지 않아야 함

■ 관련 법규

- 해당사항 없음

■ 심사 대상

- 본인확인서비스을 위한 본인확인용 CI 연계, CI 저장 서버 전체
- 본인확인서비스 DBMS - 본인확인 이력관리 테이블, 이용자 마스터 테이블
- 본인확인서비스 관리자 페이지 – 정보통신서비스 제공자 계약내용 관련
- 본인확인서비스 UI 및 해당 모듈, 소스 코드

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 개인정보흐름도 및 상세 시퀀스 다이어그램 • 본인확인서비스 관련 인터페이스 전문 규격서 • 본인확인서비스 관련 인터페이스 목록 • 본인확인서비스 인터페이스 소스 코드 및 모듈 • 본인확인서비스 관리자 페이지 URL • 본인확인서비스 관련 DBMS 상세 ERD, 테이블 목록, 컬럼 정보 • 본인확인서비스 이용 계약서(양식), CI 제공 신청서(양식)
담당자 인터뷰	• 정보서비스제공자별 본인확인서비스 계약서 작성 및 변경관리 • CI 정보에 대한 저장관리 여부

구분	준비사항
현장실사	• 본인확인서비스 관련 인터페이스 전문 규격서별 소스 코드 점검 • 본인확인서비스 관련 인터페이스 목록 점검 • 본인확인서비스 관련 DBMS ERD, 테이블 목록 및 컬럼 점검 • 본인확인서비스 연동 내용, 전송시간 등에 대한 로그 무결성 점검 • 연계정보 CI에 대한 저장 유무 점검

사례 검토

미흡사례 1	• 정보통신서비스 제공자와의 연계정보 신청서 또는 계약서에 CI 제공 여부에 대한 승인없이 CI를 임의적으로 제공하는 경우
미흡사례 2	• 본인확인인증이 완료된 이후로도 명확한 관련 법률 근거없이 이용자의 CI정보를 24시간 이상 저장하는 경우

7-6. 본인확인서비스 연계 시 보호 조치

7.6.가 위조·변조·삭제 및 유출 방지를 위한 암호화

(1) 대칭키 암호방식을 이용하는 경우 정보통신서비스 제공자에 배포한 비밀키를 주기적으로 갱신하는 기능

(2) 권한 있는 관리자만이 시스템에 접근할 수 있는 접근통제 기능

(3) 본인확인서비스 관련 소프트웨어를 임의로 변경 및 삭제할 수 없도록 하는 기능

■ 심사내용 설명

구분	주요 내용
위조·변조·삭제 및 유출방지	• 본인확인서비스 관련 대칭 KEY(암호화 KEY = 복호화 KEY)를 사용하는 경우 1년에 1회 이상 운영계와 개발계 모두 비밀 KEY를 갱신 • 본인확인서비스 관련 개발계 서버 및 테스트 서버의 비밀 KEY는 운영계 서버와 서로 다르게 설정 • 본인확인서비스 정보시스템 접근통제 시스템 (서버 접근통제, DB 접근통제, 네트워크 접근통제, 단말기 통제 및 계정관리시스템 등) 접근통제 • 본인확인서비스 관련 형상관리 및 변경관리시스템을 통하여 소프트웨어 및 소스 코드 변경 시 사전 승인 프로세스 및 사후 감사 추적 이력관리

■ 관련 법규

- 개인정보 보호법 제24조(고유식별의 처리 제한)
- 개인정보 보호법 제24조의 2(주민등록번호 처리의 제한)
- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
- 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인서비스 관련 WAS, DBMS, 인터페이스 서버 등
- 암호화 솔루션(WAS API 방식, 플러그인 방식, 자체 TDE 방식, JAVA의 암호화 함수 및 라이브러리, 파일암호화 솔루션 등), HSM 장비, 암호화 KEY 관리 솔루션 등

- 통합계정관리시스템(IAM), 서버 접근통제 솔루션(SAC), DB 접근통제 솔루션(DAC), 네트워크 접근통제 솔루션(NAC), 단말기 통제 솔루션 등
- 본인확인서비스 소스 코드 접근통제 및 변경승인과 관련된 작업계획승인서, 테스트 케이스 산출물, 형상관리 솔루션, 배포관리 솔루션, 변경관리 솔루션, 버전관리 솔루션 등

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 암호화 대상 식별 및 암호화 알고리즘 종류 • 본인확인서비스 대칭 KEY 변경 및 교환일자 증적문서 • 본인확인서비스 암호화 KEY 관리 정책 • 본인확인서비스 관련 접속이력 관리시스템 운영 현황 • 서버, DB, 네트워크 등 접근통제 솔루션 운영 현황 • 본인확인서비스 소스 코드 배포 승인 프로세스
담당자 인터뷰	• 각 기관별 암호화 KEY 변경 처리 절차 및 방법 • 본인확인서비스 관련 정보시스템 계정 등록·변경·삭제 프로세스
현장실사	• 암호화 대상별 암호화 알고리즘 및 KEY 길이 점검 • 본인확인서비스 대칭 KEY 변경 및 교환일자 점검 • 본인확인서비스 관련 암호화 KEY 솔루션 직무 분리 점검 • 서버, DB, 네트워크 접근통제 솔루션별 운영 현황 점검 • 본인확인서비스 소스 관련 형상관리, 배포관리 솔루션 현황 점검 • APP 스토어 배포 관리 프로세스 및 노트북, 맥북 점검

사례 검토

미흡사례 1	• 본인확인서비스 관련 정보통신서비스 제공자와 1년에 1회 이상 비밀 KEY를 변경 및 갱신하지 않음
미흡사례 2	• 정보통신서비스 제공자에게 CI 정보 제공 등 관리자 권한이 부여된 본인확인서비스 관리자 페이지에 이미 퇴사한 전 담당자의 계정이 삭제되지 않음

7.6.나 본인확인서비스 전송구간의 암호화

(1) 암호알고리즘 등을 통해 중복가입확인정보 및 연계정보를 안전하게 전송하는 기능

(2) 전송된 정보의 위·변조 여부를 검증할 수 있는 기능

■ 심사내용 설명

구분	주요 내용
전송구간 암호화	• 본인확인 전송구간이 암호화된 HTTPS(SSL/443포트) 또는 웹 서버에 암호화 응용프로그램을 통해 개인정보를 암호화하여 전송 • 본인확인기관 내부구간에도 주민등록번호, CI 등 개인정보 전송 시 HTTPS 등으로 암호화하여 전송 • 본인확인서비스 관련 사이트가 보안상 취약한 SSL 버전, TLS 버전 사용 또는 취약한 OpenSSL 모듈의 업데이트 수행 • 전송된 정보의 위·변조 여부를 검증하기 위하여 CRC 체크, Check SUM 또는 무결성 정보 HASH값을 검증하는 기능

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

■ 심사 대상

- 본인확인서비스 WEB/APP 사이트
- 본인확인서비스 SSL 인증서(버전 정보 확인 등) 설치 여부를 확인할 수 있는 정보시스템 : WEB/WAS 서버, L4 스위치 등

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 관련 사이트 URL • WEB 서버 SSL 인증서 설치 Config • L4 스위치 SSL 인증서 설치 Config (네트워크 장비에 설치한 경우) • OpenSSL 패치 증적
담당자 인터뷰	• TLS 1.2 미만 버전의 이용자 접속현황 통계 • TLS 1.3 이상 버전 적용 유무 ※ (참고) 금융분야 마이데이터 기술 가이드라인에서는 보안 강화를 위해 TLS 1.3 이상만 허용
현장실사	• 본인확인서비스 URL SSL, TLS 버전 점검 • OpenSSL 패치 이력 점검 • 위·변조 체크를 위한 CRC 체크, Check SUM, 무결성 정보 HASH값 검증 로직 점검

■ 사례 검토

미흡사례 1	• 본인확인서비스 전송구간을 HTTPS 암호화 방식으로 설치했으나 해당 SSL 인증서 유효기간 만료로 HTTPS로 작동하지 않고 일반 80 포트의 HTTP로 Redirection 변경되어 평문 전송모드로 적용되어 있음
미흡사례 2	• 본인확인서비스 관련 사이트가 보안상 취약한 TLS 1.2 이하 버전까지도 접속 허용하고 있음

7.6.다 무결성 검증

(1) 이용자가 대체수단 신규발급 시 본인확인기관에 제공한 정보에 대하여 해쉬 체인을 구성하는 기능

■ 심사내용 설명

구분	주요 내용
무결성 검증	• 본인확인서비스 관련 이용자로부터 받은 개인정보를 HASH 처리하여 해쉬체인을 구성하는 기능 구현 • 본인확인서비스 관련 가입정보 해쉬체인에 대하여 접근통제 수행 및 위·변조 여부 등에 대한 무결성 검증 수행

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

- 본인확인서비스 DBMS, 로그관리 시스템
- 본인확인서비스에 대한 내부통제 시스템 또는 IT 감사 시스템
- 본인확인서비스 이용자 개인정보에 대한 HASH 처리 테이블

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 이용자 개인정보에 대한 HASH 처리현황
담당자 인터뷰	• 이용자가 본인확인정보 신규발급 시 제공한 개인정보를 HASH 처리하여 보관하는 기능 사용 유무 • KISA 등과 개인정보 해쉬체인에 대한 타임스템프 검증 실시 여부
현장실사	• 본인확인 DB에서 이용자 개인정보에 대한 HASH 현황 점검 • HASH 처리된 테이블에 대한 접근통제 및 무결성 로직 점검

■ 사례 검토

미흡사례 1	• 본인확인인증에 사용된 이용자 개인정보에 대하여 이상 여부 확인 및 무결성 검증 절차가 관리적인 방법이나 시스템(해쉬체인, 타임스템프 DB 저장 등)으로 전혀 구현되어 있지 않음

7-7. 이용자 개인정보의 암호화

7.7.가 비밀정보를 일방향 암호화하여 저장하는 기능

■ 심사내용 설명

구분	주요 내용
비밀정보 일방향 암호화	• 본인확인서비스 관련 이용자의 비밀번호(PIN 번호 포함)는 복호화 되지 아니하도록 안전한 암호 알고리즘을 이용하여 일방향 암호화(HASH) 적용

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

■ 심사 대상

- DB 암호화 솔루션
- 본인확인서비스 DBMS
- 본인확인서비스 관련 이용자 비밀번호 저장 소스 코드
- 안드로이드/IOS APP 클라이언트 모듈 PIN 6자리 저장 관련 소스 코드

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 암호 통제 지침 (암호화 대상, 암호화 방식, 암호화 알고리즘)
담당자 인터뷰	• 본인확인서비스 관련 개인정보 중 일방향 암호화(HASH) 알고리즘을 적용한 대상
현장실사	• 본인확인서비스 관련 이용자 비밀번호 저장 소스 코드 점검 • 안드로이드/IOS APP 클라이언트 모듈 PIN 6자리 저장 관련 소스 코드 점검

사례 검토

미흡사례 1	• 본인확인서비스 관련 안드로이드 APP에서 이용자 PIN 번호 6자리를 일방향 암호화가 아닌 양방향 암호화 방식(복호화 가능)의 알고리즘을 적용하고 있음
미흡사례 2	• 본인확인서비스 관련 이용자 비밀번호를 일방향 암호화 방식으로 적용하였으나 보안 취약점을 가지고 있는 MD5 알고리즘을 적용하고 있음

7.7.나 이용자 개인정보 중 주민등록번호를 암호화하여 저장하는 기능

■ 심사내용 설명

구분	주요 내용
암호화	• 주민등록번호는 반드시 암호화하여 저장 ※ 주민등록번호 외의 고유식별정보(외국인등록번호 등)도 암호화하여 저장 • 본인확인서비스 관련 이용자의 주민등록번호 암호화 적용 시 안전한 암호화 알고리즘 선택 및 적합한 KEY 길이 사용 • 평문으로 복호화가 가능한 주민등록번호 암호화 테이블 및 필드에 대한 접근통제 적용

■ 관련 법규

- 개인정보 보호법 제24조의 2(주민등록번호 처리의 제한)
  - 개인정보 보호법 시행령 제21조의2(주민등록번호 암호화 적용 대상 등)
- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)

■ 심사 대상

- 본인확인시스템 관련 DB 암호화 솔루션, 암호화 KEY 관리 솔루션
- 본인확인 DB 서버 이용자 마스터 테이블, 주민등록번호 암호화 저장 테이블
- 본인확인시스템 관련 주민등록번호 인터페이스 소스 코드
- 본인확인시스템 관련 주민등록번호 연계 관련 로그

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 암호화 KEY 관리 솔루션 운영 현황 • 본인확인시스템 관련 이용자 주민등록번호 평문 조회 가능 인력 현황 • 암호화 지침 (주민등록번호에 사용된 암호 알고리즘 및 KEY 길이)

구분	준비사항
담당자 인터뷰	• 이용자의 주민등록번호를 평문으로 조회해야 하는 업무 및 사유
현장실사	• 본인확인 DB 서버 또는 고객 원장 DB 내 주민등록번호 암호화 저장 테이블 점검 • 주민등록번호 처리 로그 내 주민등록번호 암호화 여부 점검 • 주민등록번호 암호화 테이블, 필드에 대한 접근통제 적용 여부 점검 • TDE 적용 시 개발자 소스 코드에서 이용자 주민등록번호 평문 조회 가능 여부 점검

■ 사례 검토

미흡사례 1	• 본인확인서비스 관련 이용자의 주민등록번호를 암호화하여 저장하고 있으나, 암호화 KEY 관리 서버가 아닌 개발자의 소스 코드에 복호화 KEY를 평문으로 하드 코딩하여 사용함
미흡사례 2	• 본인확인서비스 관련 이용자의 주민등록번호를 암호화하여 저장하고 있으나, 안전하지 않은 취약한 암호화 알고리즘을 사용함

7.7.다 암호화를 위한 알고리즘 및 비밀정보를 주기적으로 변경·관리하는 기능

■ 심사내용 설명

구분	주요 내용
암호키 관리	• 본인확인서비스 관련 암호 KEY 생성·이용·보관·배포·파기에 대한 암호화 정책 라이프 사이클 관리 • 본인확인서비스 관련 암호 KEY 배포 대상자 및 복호화 권한 부여 • 본인확인 소스 코드에 하드 코딩 방식의 암호 KEY 기록 및 저장 금지 원칙 준수 • 본인확인서비스 관련 암호 KEY에 대한 접근권한 최소화 및 접근 이력에 대한 모니터링

■ 관련 법규

- 개인정보 보호법 제24조(고유식별의 처리 제한)
- 개인정보 보호법 제24조의 2(주민등록번호 처리의 제한)
- 개인정보 보호법 제29조(안전조치의무)
- 개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
- 개인정보의 안전성 확보조치 기준 제6조(접근통제)

■ 심사 대상

- 본인확인서비스 관련 개인정보 암호화 수행 소스 코드
- 본인확인서비스 관련 WAS, DBMS, 인터페이스 서버 등
- 암호화 솔루션(WAS API 방식, 플러그인 방식, 자체 TDE 방식, JAVA의 암호화 함수 및 라이브러리, 파일암호화 솔루션 등), HSM 장비, 암호화 KEY 관리 솔루션 등

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 암호 알고리즘 및 KEY 관리 정책 • 암호 KEY 관리대장 또는 암호 KEY 변경 관리자 화면

구분	준비사항
담당자 인터뷰	• 암호화 대상 및 암호화 방식
현장실사	• 암호화 대상별 암호화 알고리즘 및 KEY 길이 점검 • 본인확인서비스 대칭 KEY 변경 및 교환일자 점검 • 본인확인서비스 관련 암호화 KEY 솔루션 직무 분리 점검 • 본인확인서비스 암호화 대상 소스 코드 점검 (하드 코딩 점검)

사례 검토

미흡사례 1	• 본인확인서비스 관련 업무에 이용자 개인정보를 암호화하고 있으나 업무별, 운영계와 개발계 서버에 동일한 암호화 KEY를 사용하고 있음
미흡사례 2	• 본인확인서비스 관련 본인확인기관 간 또는 정보통신서비스 제공자와 대칭 KEY 시스템을 사용하는 방식으로 1년에 1회 이상 비밀 KEY를 변경이나 갱신하지 않음

8. 접속정보의 위조·변조 방지에 관한 사항

8.1 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독

■ 심사내용 설명

구분	주요 내용
개인정보 처리시스템 관리감독	• 본인확인업무 관련 개인정보처리시스템 접속기록을 최소 2년 이상 보관 ※ 접속기록 필수 항목 : 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 ※ 사용자 단말 또는 서버 OS에 설치된 DB접속툴에서 DB에 원격 접속한 경우, DB서버 OS에서 DB접속명령어로 localhost DB에 접속한 경우 등 누락없이 관리하여야 함 • 본인확인업무 관련 개인정보처리시스템 접속기록 저장·검토 시 관련 법규 및 내부관리계획 준수 • 본인확인업무 관련 개인정보처리시스템 접속기록을 월 1회 이상 점검하고 점검결과를 개인정보관리책임자에게 보고 • 개인정보의 다운로드가 확인된 경우 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
  - 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

■ 심사 대상

- 개인정보처리시스템 접속기록 저장·검토(이상행위 모니터링) 정보시스템
  ※ DB, DB접근제어시스템, 서버접근제어시스템, 로그통합모니터링시스템, 개인정보접속기록관리시스템 등
- 개인정보처리시스템 접속기록 검토 결과 및 보고 이력

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획서(개인정보처리시스템 접속기록 관리 조항) • 본인확인업무 관련 개인정보처리시스템 자산 목록표(Host Name, IP, URL, 용도 명시) – DB: 본인확인 DB, 본인확인서비스 이용자 상담 처리 관련 DB 등 – 어플리케이션: 대체수단 발급 관리자사이트, 본인확인서비스 관리자사이트, 본인확인서비스 이용자 상담 처리 관련 사이트 등 • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 관리현황표 – 접속기록(원본): 저장 위치, 보관 기간, 위·변조 방지 기능 적용 여부, 검토 담당자 – 접속기록(백업본): 백업 방법, 백업 주기, 저장 위치, 보관 기간, 백업 담당자 ※ 저장 위치: 물리적 장소, 저장장치(DB, DB접근제어시스템, 로그통합관리시스템 등 시스템명 또는 외장하드 등 매체명) • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 검토 절차 ※ 검토 절차: 검토 담당자, 검토 주기, 검토 방법 및 기준, 이상행위 소명 절차, 검토 결과 보고체계 등 ※ 개인정보 다운로드 시 사유확인 기준 및 절차 등 • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 검토 결과 및 이상행위 처리 결과
담당자 인터뷰	• 개인정보처리시스템 접속기록(원본) 저장·검토 정보시스템 운영자 – 접속기록 조회 및 설명(저장 내역, 보관 기간 등) • 개인정보처리시스템 접속기록 검토 담당자 – 검토 절차 설명 – 접속기록 검토 결과 및 이상행위 처리 결과 설명 • 개인정보처리시스템에 대한 접속기록의 안전한 보관 방법 설명 • 접속기록 보관 및 위조·변조 방지를 위한 조치 설명
현장실사	• 개인정보처리시스템 접속기록 관리계획 수립 여부 확인 • 개인정보처리시스템 접속기록 관리현황표 작성 여부 확인 • 개인정보처리시스템 접속기록 저장 현황 확인 – 접속기록 저장 정보시스템 운영자와 직접 조회 • 개인정보처리시스템 접속기록 검토 현황 확인 – 접속기록 검토 절차의 적절성 확인 – 접속기록 검토 정보시스템의 이상징후 탐지 시나리오 확인 – 접속기록 검토 결과 및 보고 증적 확인 • 개인정보처리시스템에 접속한 자의 접속일시, 처리내역 등 접속기록의 저장·점검 및 이의 확인·감독 증적 확인

사례 검토

미흡사례 1	• 개인정보처리시스템 접속기록 저장 – 개인정보처리시스템(어플리케이션) 접속기록에서 사용자가 처리한 정보주체를 확인할 수 없음 – 개인정보처리시스템(어플리케이션) 접속기록에서 사용자가 수행한 업무(개인정보 조회, 수정, 삭제, 다운로드 등 처리내역)를 확인할 수 없음
미흡사례 2	• 개인정보처리시스템 접속기록 검토 – 개인정보취급자가 검토 담당자로 지정되어 모든 접속기록을 검토하고 있음(직무 분리 미흡) – 대체수단 발급 관리자사이트, 본인확인서비스 관리자사이트, 본인확인서비스 이용자 상담사이트에서 개인정보 다운로드 사유를 확인하고 있지 않음 – 로그통합관리시스템에서 시나리오에 따라 접속기록 이상징후를 탐지하고 있으나, 원인 확인 등 소명 절차를 수행하지 않음
미흡사례 3	• 사용자의 DB 접속경로에 따른 접속기록 검토 – DBA, 서비스 운영자 등이 DB서버 OS에서 DB접속명령어로 localhost DB에 접속하여 본인확인서비스 이용자 개인정보를 처리한 행위에 대해 검토하지 않음

8.2 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

■ 심사내용 설명

구분	주요 내용
접속기록 백업	• 본인확인업무 관련 개인정보처리시스템 접속기록을 별도 저장장치에 백업 ※ 접속기록: 접속자, 접속일시, 접속지 정보, 처리한 개인정보, 수행업무 등 • 본인확인업무 관련 개인정보처리시스템 접속기록 백업 보관 시 관련 법규 및 내부관리계획 준수

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

■ 심사 대상

- 개인정보처리시스템 접속기록 백업시스템
- 개인정보처리시스템 접속기록 백업본 저장장치(정보시스템 또는 매체)
- 개인정보처리시스템 접속기록 백업 이력

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 내부관리계획서(개인정보처리시스템 접속기록 관리 조항) • 본인확인업무 관련 개인정보처리시스템 자산 목록표(Host Name, IP, URL, 용도 명시) – DB: 본인확인 DB, 본인확인서비스 이용자 상담 처리 관련 DB 등 – 어플리케이션: 대체수단 발급 관리자사이트, 본인확인서비스 관리자사이트, 본인확인서비스 이용자 상담 처리 관련 사이트 등 • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 관리현황표 – 접속기록(원본): 저장 위치, 보관 기간, 위·변조 방지 기능 적용 여부, 검토 담당자 – 접속기록(백업본): 백업 방법, 백업 주기, 저장 위치, 보관 기간, 백업 담당자 ※ 저장 위치: 물리적 장소, 저장 장치명(DB, DB접근제어시스템, 로그통합관리시스템 등 시스템명 또는 외장하드 등 매체명) • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 백업 계획 • 본인확인업무 관련 개인정보처리시스템(DB, 어플리케이션) 접속기록 백업 이력

구분	준비사항
담당자 인터뷰	• 개인정보처리시스템 접속기록 백업 담당자 – 접속기록 백업 절차 및 계획 설명 • 개인정보처리시스템 접속기록 백업시스템 운영자 및 백업본 저장장치(정보시스템 또는 매체) 담당자 – 접속기록(백업본) 조회 및 설명(백업 일정 설정내역, 백업 이력 등)
현장실사	• 개인정보처리시스템 접속기록 백업 계획 수립 여부 확인 • 개인정보처리시스템 접속기록 관리현황표 작성 여부 확인 • 개인정보처리시스템 접속기록 백업 현황 확인 – 백업 담당자와 백업 절차 및 계획 확인 – 백업시스템 운영자 및 백업본 저장장치 담당자와 백업 일정 설정내역 및 백업 이력 직접 조회

사례 검토

미흡사례 1	• 개인정보처리시스템 접속기록 백업본을 별도 저장장치에 보관하지 않고 원본과 함께 로컬 정보시스템에 보관하고 있음
미흡사례 2	• 개인정보처리시스템 접속기록 백업본 보관 기간이 관련 법규 및 내부관리계획의 요구사항을 준수하지 못함

9. 본인확인업무와 다른 인터넷 서비스와의 분리

9.1 **대체수단 발급 시 본인확인기관의 다른 인터넷서비스에 대한 회원가입을 요구하지 않아야 함**

■ 심사내용 설명

구분	주요 내용
타 서비스 분리	• 대체수단 발급을 위해 본인확인서비스 이외의 다른 인터넷 서비스의 회원가입 요구 금지 – 본인확인서비스 발급·이용 절차상 다른 서비스 가입, 광고 등을 노출할 수 없음

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

● 본인확인서비스 가입 웹/모바일 페이지

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 가입 절차 • 본인확인 서비스 시스템 운영현황
담당자 인터뷰	• 본인확인정보 발급 시 본인확인기관의 다른 인터넷서비스에 대한 회원가입을 요구하고 있는지 여부
현장실사	• 본인확인서비스 가입 단계의 서비스 화면

■ 사례 검토

미흡사례 1	• 본인확인서비스 가입 시 본인확인서비스와 관련 없는 부가서비스의 가입을 유도하고 있음

9.2 본인확인서비스 제공을 위한 시스템 및 개인정보 DB를 물리적 또는 논리적으로 다른 서비스와 분리하여 운영하여야 함

■ 심사내용 설명

구분	주요 내용
본인확인 설비 분리	• 본인확인업무 전용 정보시스템 중 서버, 미들웨어, DB는 다른 설비와 물리적 또는 논리적으로 분리하여 구성하여야 함 – 「본인확인업무와 다른 인터넷 서비스와의 분리 안내서」 참고하여 본인확인설비의 물리적·논리적 분리 구성 방법을 확인 • 필수 분리 대상이 아닌 정보시스템은 본인확인서비스 운영 방침 및 내부 규정, 정보보호 및 개인정보보호 관리체계에 따라 본인확인서비스에 영향을 미치지 않도록 구성·운영·관리 필요

■ 관련 법규

● 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의3(본인확인기관의 지정 등)

– 본인확인기관 지정 등에 관한 기준 [별표 3] 1장 9.2

■ 심사 대상

● 본인확인업무 전용 정보시스템(서버, 미들웨어, DB)

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 정보자산 목록 – (본인확인업무 전용 및 전사 공용) 서버, 미들웨어, DB • 본인확인업무 전용 정보시스템 상세 구성도 – 서버(단일 구성 또는 가상머신·컨테이너 가상화 구성 등 현황) – 미들웨어(WEB·WAS·AP서버 내 서비스 계정, 단일 구성 또는 컨테이너 구성 등 현황) – DB(DB서버 내 DB엔진 구성, DB 서비스 계정, DB 스키마 등 현황) • 본인확인업무 전용 및 전사 공용 DB 테이블 명세서

구분	준비사항
담당자 인터뷰	• 본인확인서비스 인프라 운영 총괄 담당자 및 서버관리자, 미들웨어 관리자, DBA – 본인확인서비스 정보자산(서버, 미들웨어, DB) 현황 설명 – 본인확인업무 전용 정보시스템(서버, 미들웨어, DB) 상세 구성 설명 – 본인확인업무 전용 및 전사 공용 DB 테이블 명세서 설명
현장실사	• 「본인확인업무와 다른 인터넷 서비스와의 분리 가이드라인」에 따라 운영환경의 서버, 미들웨어, DB를 구성 및 운영하는지 확인

■ 사례 검토

미흡사례 1	• 단일 WAS서버에서 두 개의 미들웨어 계정(tomcat1, tomcat2)으로 인스턴스를 분리하여 본인확인서비스와 다른 인터넷 서비스를 운영하고 있음
미흡사례 2	• 단일 DB에서 하나의 DB 서비스 계정으로 테이블만 분리하여 본인확인서비스와 다른 인터넷 서비스를 운영하고 있음

Ⅱ | 기술적 능력

별표 5.의 자격 중 어느 하나를 갖춘 기술 인력을 8인 이상 보유할 것

■ 심사내용 설명

구분	주요 내용
기술적 능력	• 본인확인서비스의 안전성과 신뢰성 확보에 필요한 시설 및 장비의 운영을 위해 자격 및 경력 요건을 갖춘 자를 8인 이상 보유 – 자격 사항 : 정보통신기사·정보처리기사·전자계산기조직응용기사, 정보보안기사 이상의 국가기술자격과 동등이상인 자격 – 경력 사항 : 정보보호 또는 정보통신 운영·관리 분야에서 2년 이상 근무

■ 심사 대상

● 8인 이상의 기술인력

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 공통 : 국민연금가입증명서, 조직도, 업무분장표, 재직증명서 • case1 : 국가기술자격증 (참고자료 2-5) • case2 : 경력증명서
담당자 인터뷰	• 해당사항없음
현장실사	• 증적자료를 바탕으로 기술인력 보유여부 확인

Ⅲ | 재정적 능력

자본금 : 80억 원 이상일 것 (국가기관 및 지방자치단체는 제외한다)

■ 심사내용 설명

구분	주요 내용
재정적 능력	• 신청기관의 재정적 능력(자본금 80억원) 확보 • 첨부된 별지서식 확인 – [별지 제4호서식] 지정신청기관의 명세서 – [별지 제5호서식] 최근 3개년 주요 재무지표 – [별지 제6호서식] 최근 3개년 주요 재무수치

■ 심사 대상

- 최근 3년간 외부감사인의 감사보고서
- 전자공시시스템(dart.fss.or.kr)에서 심사 당해연도 반기보고서 열람

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 최근 3년간 외부감사인의 감사보고서, 법인등기부등본
담당자 인터뷰	• 해당사항없음
현장실사	• 증적자료 바탕으로 재정적 능력 확보 여부심사

Ⅳ | 설비규모의 적정성

1. 이용자의 개인정보를 검증·관리 및 보호하기 위한 설비

1.1 이용자의 등록정보를 관리하기 위한 설비

■ 심사내용 설명

- 이용자 개인정보를 관리하기 위해 필요한 설비를 보유하여야 함
- 본인확인기관은 이용자 개인정보를 관리하기 위한 다음과 같은 설비를 갖추고 있어야 함
  - 서버 : 인증 서버, 본인확인정보, 발급·관리 서버, 메일 서버, DB 서버, 백업 서버, 웹서버, 관리용 서버, 응용 서버, 로그 서버 등
  - 네트워크 : 라우터, 스위치, 허브 등
  - 정보보호시스템 : 침입차단시스템, 침입탐지(방지)시스템, 백업 및 복구 시스템, 인증시스템, 생체특성 기반, 출입통제장치, 감시·통제 시스템, 보안관제시스템, 무정전 전원공급시스템 등
  - 관리시스템 : 화재설비, 수재 예방 설비, 항온항습장치 등
- 본인확인기관의 이용자 개인정보 관리 설비는 이용자 개인정보 보호 및 관리를 위한 적절한 시스템 스펙 등을 가지고 있는지 확인할 수 있어야 함

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

- 본인확인 등록 및 관리 정보시스템

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 관련 설비 현황 • 관련 설비 스펙 현황
담당자 인터뷰	• 본인확인기관은 이용자의 개인정보를 관리하기 위한 적절한 설비 보유현황 설명
현장실사	• 본인확인 등록 및 관리하기 위한 설비

사례 검토

미흡사례 1	• 이용자의 등록정보를 관리하기 위한 설비를 보유하지 않고, 외부 Public Cloud 설비를 임차하여 운영하고 있음

1.2 신원확인을 수행하기 위한 설비(인증서, 신용카드, 휴대전화 SMS, 대면확인 등)

■ 심사내용 설명

● 본인확인서비스 제공을 위한 실명기반의 신원확인을 위한 인터페이스를 제공하여야 함

■ 관련 법규

● 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

● 본인확인 정보시스템

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인서비스 신원 확인 절차
담당자 인터뷰	• 신원확인을 수행하기 위한 설비(인증서, 휴대전화 SMS, 대면확인 등)를 보유현황에 대한 설명
현장실사	• 본인확인서비스 가입 시 신원확인 설비

■ 사례 검토

미흡사례 1	• 본인확인정보 발급 시 이용자의 신원을 확인하기 위한 설비를 보유하고 있지 않음
미흡사례 2	• 본인확인서비스를 위한 신원확인 시 대면확인을 통해 하고 있으며 이때 간단한 신청서류 작성만하고 별도의 신원확인 등은 하지 않고 있음

2. 대체수단을 생성·발급 및 관리하기 위한 설비

2.1 대체수단의 관리 및 제공하기 위한 설비

■ 심사내용 설명

- 본인확인정보, 중복가입확인정보 및 연계정보를 제공하기 위한 설비를 보유하여야하고, 그를 보호하기 위한 보호설비를 보유하여야 함
- 본인확인기관은 본인확인정보, 중복가입확인정보 및 연계정보를 제공하기 위한 다음과 같은 설비를 갖추고 있어야 함
  - 서버 : 인증 서버, 본인확인정보, 발급·관리 서버, 메일 서버, DB 서버, 백업 서버, 웹서버, 관리용 서버, 응용 서버, 로그 서버 등
  - 네트워크 : 라우터, 스위치, 허브 등
  - 정보보호시스템 : 침입차단시스템, 침입탐지(방지)시스템, 백업 및 복구 시스템, 인증시스템, 생체특성 기반, 출입통제장치, 감시·통제 시스템, 보안관제시스템, 무정전 전원공급시스템 등
  - 관리시스템 : 화재설비, 수재 예방 설비, 항온항습장치 등

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

■ 심사 대상

- 본인확인 정보시스템 및 관련 설비

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 관련 설비 현황 • 대체수단 생성, 발급, 관리 등 관련 설비 구성안
담당자 인터뷰	• 본인확인정보, 중복가입확인정보 및 연계정보를 제공하기 위한 설비 보유 현황 설명 • 본인확인서비스에 관한 시설 및 장비를 안전하게 운영하기 위한 보호설비를 보유 현황 설명
현장실사	• 대체수단 관련 본인확인정보시스템 보유 여부 확인

사례 검토

미흡사례 1	• 대체수단 등록정보를 관리하는 DB를 다른 서비스와 혼용하여 운영하고 있음

2.2 본인확인서비스에 관한 시설 및 장비를 안전하게 운영하기 위한 보호설비

■ 심사내용 설명

- 본인확인서비스 관련 시설 및 장비를 안전하게 운영하며 외부인으로부터 접근을 차단하기 위한 보호설비 구축하여야 함
- 본인확인서비스 관련 시설 및 장비에 대해서는 잠금장치가 있는 별도의 시스템 렉 또는 보호공간에 분리 운영할 수 있으며, 상시 잠금 상태로 유지하여야 함
- 본인확인정보, 중복가입확인정보 및 연계정보를 제공하기 위한 설비 등 본인확인업무 시스템을 보호철창 등과 같은 별도의 공간을 마련하여 출입을 통제하여야 함

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인서비스에 관한 시설 및 장비에 대한 보호구역
- 본인확인정보, 중복가입확인정보 및 연계정보를 제공하기 위한 설비

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 본인확인서비스 관련 시스템 자산 목록 • 본인확인서비스 관련 시스템에 대한 렉 분리 현황 사진 • 본인확인서비스 관련 시스템에 대한 렉 잠금장치 사진 • 출입통제 장치 종류 및 운영사진 • 보안구역 배치도 (본인확인서비스 관련 설비 위치, 출입동선 표시) • 출입권한 부여인원 현황 (이름, 등록기간, 담당업무, 등록사유 등)

구분	준비사항
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 설명 • 보호구역(본인확인서비스에 관한 주요 시설 및 장치) 담당자 – 본인확인서비스 관련 시스템에 대한 렉 분리 및 시건장치 현황 – 보호구역 출입절차 및 출입권한 등록절차 설명
현장실사	• 주요 물리적 보호구역에 대한 적절한 보호대책을 수립하고 있는지 확인 • 본인확인서비스 관련 시설 및 장치에 대한 출입통제 장치 확인 • 주요 시설 및 장치에 대한 렉 분리 및 잠금장치/시건장치 확인 • 보호철창 등과 같은 별도의 공간을 운영의 적절성 확인 • 보호구역 출입권한자 중에 불필요한 인원이 포함되어 있는지 확인 • 출입 이벤트 발생 시 출입내역을 기록하고 관리하는지 확인 • 렉 잠금장치/시건장치 관련 키 반출/반입 대장 작성 여부 확인

■ 사례 검토

미흡사례 1	• 본인확인서비스 관련 시설 및 장비가 보호철장 등 별도의 공간에 분리되지 않고 시건장치 없이 타 장비와 혼재되어 있는 경우

3. 출입통제 및 접근제한을 위한 보안설비

3.1 본인확인업무 시스템을 안전하게 운영할 수 있는 별도의 통제구역

■ 심사내용 설명

- 비인가자의 물리적 접근 및 각종 물리적·환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위해 접견구역, 제한구역, 통제구역 등 별도의 물리적 보호구역을 지정
- 본인확인업무의 중요도 및 개인정보 관리자산 위치에 따라 물리적 보호 구역을 구분하고 각 구역별 보호대책을 수립·이행

  ※ 물리적 보호 구역 구분 예시
  - 접견구역 : 외부인이 별다른 출입증 없이 출입이 가능한 구역 (예 : 접견장 소 등)
  - 제한구역 : 비인가된 접근을 방지하기 위하여 별도의 출입통제 장치 및 감 시시스템이 설치된 장소로 출입 시 직원 카드와 같은 출입증이 필요한 장소 (예 : 부서별 사무실 등)
  - 통제구역 : 제한구역의 통제항목을 모두 포함하고 출입자격(예 : 개인정보취 급자 등)이 최소인원으로 유지되며 출입을 위하여 추가적인 절차가 필요한 곳 (예 : 전산실, 통신장비실, 관제실, 공조실, 발전실, 전원실, 개인정보를 보관 하는 문서보관소 등)
- 본인확인업무 시스템이 안전하게 운영될 수 있도록 통제구역으로 지정

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인업무 시스템 운영을 위한 통제구역
- 물리적 보호 구역별 출입통제 시스템 및 운영 책임자

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 본인확인업무의 중요도 등에 따른 물리적 보호구역 구분 현황 • 본인확인서비스 관련 시스템 자산 목록 • 보호구역별 보호대책 수립 현황 • 보호구역 배치도 (본인확인업무 관련 설비 위치, 출입동선 표시) • 출입권한 부여인원 현황 (이름, 등록기간, 담당업무, 등록사유 등)
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 설명 • 보호구역(본인확인업무 관련 시설 및 장치 등) 담당자 – 보호구역 출입동선, 출입절차 설명 – 보호구역 출입권한 등록인원 및 등록사유 설명
현장실사	• 주요 물리적 보호구역에 대한 적절한 보호대책을 수립하고 있는지 확인 • 보호구역에 대한 비인가자 접근 시 출입을 통제할 수 있는지 확인 • 출입 동선상 통제되지 않은 출입문 및 우회경로가 있는지 확인 • 인가된 상시 출입자에 대한 주기적 검토 확인 • 보호구역 출입권한자 중에 불필요한 인원이 포함되어 있는지 확인 • 임시 출입자의 출입절차(카드키 반출입 등)의 적절성 확인 • 출입 이벤트 발생 시 출입내역을 기록하고 관리하는지 확인 • 보호구역 출입내역을 확인 하여 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 실패 사유에 대한 감사절차가 있는지 확인

■ 사례 검토

미흡사례 1	• 본인확인업무의 중요도 및 개인정보 관리자산 위치에 따라 보호구역, 접견구역, 통제구역 등이 별도로 구분되어 있지 않음

3.2 본인확인업무 시스템에 대한 출입을 통제하고 이에 대한 감사기록 기능을 갖는 장치

■ 심사내용 설명

- 본인확인업무 시스템에 대한 출입을 통제하는 방안을 수립
- 본인확인업무 시스템이 설치된 물리적 보호구역에 비인가자가 접근·출입할 수 없도록 감사기록 기능을 갖는 장치를 설치
- 부여된 권한에 따라 본인확인업무 시스템에 대한 출입통제를 수행
- 본인확인업무 시스템에 대한 출입기록을 일정 기간 보관하고 출입의 적정성을 확인하기 위해 출입기록을 주기적으로 검토
- 시스템적으로 출입 로그를 남기지 않는 단순 잠금장치(자물쇠)를 사용하는 경우에는 반드시 출입대장을 작성하여 출입기록을 확인할 수 있도록 하여야 함
- 통제구역에 대한 출입 인가자를 최소한으로 제한하고, 통제구역 출입자에 대한 감사기록 기능을 갖는 절차와 장치를 설치

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인업무 시스템에 대한 출입통제 시스템 및 감사기록 장치
- 본인확인업무 시스템에 대한 출입통제 및 감사기록 장치 운영 및 관리 방안

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 본인확인업무 시스템 관련 자산목록 대장 • 본인확인업무 시스템에 대한 출입통제 장치 구축 현황 • 본인확인업무 시스템에 대한 출입통제 감사기록 관리 현황 • 보호구역별 보호대책 수립 현황 • 보호구역 배치도 (본인확인업무 시스템 위치, 출입동선 표시) • 출입권한 부여인원 현황 (이름, 등록기간, 담당업무, 등록사유 등)
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 설명 • 본인확인업무 시스템(본인확인업무 관련 시설 및 장치 등) 담당자 – 본인확인업무 시스템 출입통제 장치 및 출입절차 설명 – 출입통제 장치 기반 감사기록 생성/저장/관리 체계 설명
현장실사	• 본인확인업무 시스템에 대한 적절한 보호대책을 수립하고 있는지 확인 • 보호구역에 대한 비인가자 접근 시 출입을 통제할 수 있는지 확인 • 보호구역 출입권한자 중에 불필요한 인원이 포함되어 있는지 확인 • 임시 출입자의 출입절차(카드키 반출입 등)의 적절성 확인 • 출입 이벤트 발생 시 출입내역을 기록하고 관리하는지 확인 • 보호구역 출입내역을 확인하여 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 실패 사유에 대한 감사절차가 있는지 확인

사례 검토

미흡사례 1	• 본인확인업무 시스템에 대한 출입통제 장치 및 절차 등이 마련되지 않았으며 본인확인업무 시스템에 대한 접근 이력 등이 감사기록으로 저장 및 관리되지 않음

3.3 생체기반을 포함한 다중 신원확인 기능을 갖는 출입통제장치

■ 심사내용 설명

- 본인확인업무 관련 보호구역에 생체특성기반 신원확인정보(지문인식, 홍채인식 등)을 포함하는 2개 이상의 다중 신원확인 기능을 제공하는 출입통제장치 확보

  ※ 신원확인이 가능한 생체특성의 종류 : 지문, 얼굴, 홍채, 음성, 손모양, 손등 정맥, 서명 인식 등

- 본인확인업무 관련 보호구역에 생체특성기반 출입통제를 통해 관리
- 보호구역 출입 시 2종 이상의 생체특성기반 출입통제장치를 운영하여 신원확인 과정을 수행하여 본인확인업무 관련 보호구역에 대한 출입통제 기능 운영
- 다중 신원확인 기반 출입통제장치에 출입 권한 등록, 변경 및 삭제 기능 제공
- 불필요한 출입권한이 부여되지 않도록 관리하여 본인확인업무 관련 설비에 대한 안전성을 확보
- 출입기록은 즉시 확인 가능하도록 출입통제 시스템 등을 통해 관리

  ※ 출입통제 저장정보: 일련번호, 행위자, 출입유형(IN/OUT), 출입위치, 성공/실패 여부, 실패원인, 일자/시간 등

- 출입기록은 최소 6개월 이상 보관
- 출입대장을 수기로 관리하는 경우에는 출입기록 누락 등이 발생되지 않도록 적절한 관리방안 수립 필요

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 생체특성기반 출입통제장치
- 다중 신원확인 기반 출입통제장치에 대한 출입권한 등록, 변경 및 삭제
- 생체특성기반을 포함한 2개 이상의 출입통제장치에 대한 출입기록 및 감사기록

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 생체특성기반 다중 신원확인 출입통제장치 설치 및 운영 사진 • 다중 신원확인 기반 출입절차 및 출입권한 등록절차 설명자료 • 다중 신원확인 기반 출입통제장치 및 배치도(설비 위치, 출입동선 표시) • 출입권한 부여인원 현황(이름, 등록기간, 담당업무, 등록사유 등) • 다중 신원확인 기반 출입통제 시스템 감사기록 예시
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 내 출입통제 관련 내용 설명 • 생체특성기반 다중 신원확인 출입통제 장치 담당자 – 생체특성기반 다중 신원확인 출입방법, 출입절차 설명 – 출입권한 부여인원 및 감사기록 관리 과정 설명
현장실사	• 2종 이상의 생체특성기반 출입통제 장치를 적용하고 있는지 확인 • 생체특성기반 출입통제 장치에 권한 등록 과정 및 현황 확인 • 인가된 출입자의 감사기록에 대한 주기적 검토 여부 확인 • 생체특성기반 출입통제 장치에 불필요한 인원의 포함 여부 확인 • 출입내역을 확인하여 생체특성기반 출입통제 장치 내 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 실패 사유에 대한 감사절차가 있는지 확인

■ 사례 검토

미흡사례 1	• 보호구역 내 출입권한이 부여되지 않은 사용자가 생체특성기반 출입기록에서 확인됨
미흡사례 2	• 생체특성기반 출입통제 장치에 대한 실패기록이 저장되지 않고 있음

3.4 본인확인업무 시스템 운영실을 감시·통제하고 이에 대한 감사기록 기능을 갖는 장치

■ 심사내용 설명

- 본인확인업무 시스템 운영실에 대한 감시·통제 절차 및 운영 방안을 수립
- 본인확인업무 시스템을 운영하는 물리적 보호구역에 대한 접근·출입 내용을 감사기록으로 저장·관리하는 장치를 설치
- 부여된 권한에 따라 본인확인업무 시스템 운영실에 대한 출입통제를 수행
- 본인확인업무 시스템 운영실에 대한 출입기록을 일정 기간 보관하고 출입의 적정성을 확인하기 위해 출입기록을 주기적으로 검토
- 시스템적으로 출입 로그를 남기지 않는 단순 잠금장치(자물쇠)를 사용하는 경우에는 반드시 출입대장을 작성하여 출입기록을 확인할 수 있도록 하여야 함
- 본인확인업무 시스템 운영실에 대한 출입 인가자를 최소한으로 제한

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제10조(물리적 안전조치)

■ 심사 대상

- 본인확인업무 시스템 운영실 감시·통제 시스템 및 감사기록 장치
- 본인확인업무 시스템 운영실을 위한 감시·통제 장치 시스템 및 감사기록 장치의 운영 및 관리 방안

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 물리적 보안 지침 • 본인확인업무 시스템 운영실에 대한 출입통제 장치 구축 현황 • 본인확인업무 시스템 운영실에 대한 출입통제 감사기록 관리 현황 • 보호구역별 보호대책 수립 현황 • 보호구역 배치도 (본인확인업무 시스템 운영실 위치, 출입동선 표시) • 출입권한 부여인원 현황 (이름, 등록기간, 담당업무, 등록사유 등)
담당자 인터뷰	• 물리보안 담당자 – 물리적 보안 지침·정책 설명 • 본인확인업무 시스템 운영실 담당자 – 본인확인 시스템 운영실 출입통제 장치 현황 및 출입절차 설명 – 출입통제 장치 기반 감사기록 생성/저장/관리 체계 설명
현장실사	• 본인확인업무 시스템 운영실에 대한 보호대책 수립 여부 확인 • 보호구역에 대한 비인가자 접근 시 출입을 통제할 수 있는지 확인 • 보호구역 출입권한자 중에 불필요한 인원이 포함되어 있는지 확인 • 임시 출입자의 출입절차(카드키 반출입 등)의 적절성 확인 • 출입 이벤트 발생 시 출입내역을 기록하고 관리하는지 확인 • 보호구역 출입내역을 확인하여 비인가자의 출입기록이 있는지 확인 • 출입기록은 성공·실패 내역이 모두 기록되어야 하며, 이상행위로 파악되는 경우에는 실패 사유에 대한 감사절차가 있는지 확인

사례 검토

미흡사례 1	• 본인확인 시스템 운영실에 출입통제 장치 기반 통제절차 등이 마련되지 않았으며 본인확인 시스템 운영실에 대한 접근 이력 등이 감사기록으로 저장 및 관리되지 않음

4. 시스템 및 네트워크의 보호설비

4.1 이중화된 네트워크 설비

■ 심사내용 설명

- 외부 네트워크와 연결되는 네트워크회선이 물리적으로 두개 이상으로 분리 구성되어 있는지 확인
  - 외부 네트워크와 연결된 회선이 두개 이상이고, 물리적으로 분리되어 있는지 여부
  - 회선을 제공하는 업체(ISP)가 2개 업체 이상, 국사가 2개 이상인지 여부
- 네트워크 구성도에 외부 네트워크와 연결된 네트워크 회선을 명기하고, 회선별 ISP업체 및 국사 정보 표기 확인
- 네트워크 구성도의 정보와 라우터 설정 내용이 동일한지 확인
  - 외부 네트워크 회선이 연결된 인터페이스 설정 정보
  - 연결된 외부 네트워크 회선들로 Routing 설정 정보
- 이중화된 네트워크 회선, 라우터 등 장애 시에도 정상적인 본인확인서비스 제공이 가능한지 여부 확인
  - 이중화된 연결된 회선 중 한 회선이 단선되어도 본인확인서비스를 제공할 수 있는지 확인
  - 이중화된 내부 네트워크 장비 중 한대에서 장애가 발생하여도 본인확인서비스를 제공할 수 있는지 확인

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 외부 네트워크와 연결되는 네트워크 회선
- 외부 네트워크와 연결되는 네트워크 장비

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 구성도 • 라우터 config
담당자 인터뷰	• 네트워크 담당자 – 본인확인시스템 관련 네트워크 구성 현황에 대한 설명 – 외부 네트워크와 연결되는 네트워크 회선의 이중화 설명 – 외부 네트워크와 연결되는 내부 네트워크 장비의 이중화 구성 설명
현장실사	• 외부 네트워크와 연결되는 관문의 네트워크 장비 실사

■ 사례 검토

미흡사례 1	• 외부 네트워크와 연결되는 네트워크 회선을 이중화하였으나, 1개의 ISP업체의 동일한 국사에 연결된 회선을 사용
미흡사례 2	• 네트워크 회선이 연결된 라우터부터 내부 백본까지의 네트워크 설비를 이중화 구성하였으나, 네트워크 순단이 발생하지 않도록 Full Mesh구조로 설정하지 않음
미흡사례 3	• 외부 네트워크와 연결되는 라우터의 Config가 네트워크 구성도의 회선 정보와 다르게 설정되어 있음

4.2 침입차단시스템, 침입탐지시스템 등 네트워크 보안설비

■ 심사내용 설명

- Firewall, IDS 또는 IPS 등의 운영절차를 수립하고, 절차에 따라 운영하는지 확인
- 수립된 운영절차 내 필수 내용이 포함되어 있는지 확인
  - 시스템 유형별 책임자 및 관리자 지정
  - 접근통제규칙(룰셋 등) 적용(등록, 변경, 삭제 등) 절차
  - 최신 패턴(시그니처) 업데이트 방법(LiveUpdate, 수동업데이트)별 절차
  - 시스템 이벤트 모니터링 절차 : 정책에 위배되는 이상징후 탐지 및 확인 등
  - 시스템 접근통제 정책
  - 시스템 운영현황 주기적 점검 등
- Firewall, IPS가 이중화 구성되어 있는지 확인
  - 네트워크 구성도를 통해 시스템의 이중화 여부 확인
  - Firewall, IPS의 이중화를 위해 HA(High Availability)를 적용 중인지 확인
  - 이중화로 Firewall의 접근통제규칙, IPS의 패턴 정책 등이 이중화 장비 간 서로 실시간 동기화되고 있는지 확인
  - A-S(Active-Standby)방식으로 이중화 적용 시, Standby로 전환 실패에 대한 대책이 마련되어 있는지 확인

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인서비스를 보호하기 위해 접근통제규칙을 적용하는 모든 Firewall
  - 본인확인서비스 네트워크 영역(Zone)을 분리 구성하는 Firewall
  - 각 외부 연결 지점(관문, 대외계 등)에 설치된 Firewal, 내부망 세부 네트워크 영역(Zone)을 분리 구성하는 Firewall 중 본인확인시스템에 대한 접근통제 규칙을 적용하는 설비

- 본인확인서비스 관련 모든 내부 트래픽을 감시하고 침입 탐지(방지)하는 모든 IDS 또는 IPS
  - 본인확인시스템만 위치하고 있는 네트워크 영역(Zone)의 트래픽을 모니터링하는 IDS 또는 IPS
  - 본인확인서비스 트래픽이 경유하는 각 외부 연결 지점(관문, 대외계 등)에 설치된 IPS
  - 별도의 본인확인서비스 네트워크 영역을 감시하기 위한 IDS 등이 없을 경우, 내부망 세부 네트워크 영역을 감시하기 위한 IDS 또는 IPS 등이 운영 시 대상에 포함
  - UTM, NGFW 등의 Firewall 장비에서 IPS 모듈을 활성화하여 운영 시 대상에 포함

담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• Firewall, IDS 또는 IPS 등 운영 절차서 • 네트워크 구성도(Firewall, IPS 이중화 명기)
담당자 인터뷰	• Firewall, IDS 또는 IPS 담당자 – Firewall, IDS 또는 IPS의 운영 절차에 대한 설명 – Firewall, IPS의 이중화 방식(A-A 또는 A-S)에 대한 설명 – Firewall, IPS의 HA 적용여부 및 정책 동기화에 대한 설명 – Active 장비 장애로 Standby 장비로 전환 중 전환 실패 시 대책에 대한 설명
현장실사	• Firewall, IDS 또는 IPS의 HA 적용 여부, Monitor/Hearbeat interface 설정 현황 및 Master/Slave 장비간 정책 동기화 여부 등 실사

사례 검토

미흡사례 1	• Firewal이 이중화로 구성되어 있고, HA 기능도 정상적이나, Active Firewall에 등록한 접근통제규칙이 Standby Firewall에 동기화가 적용되고 있지 않음(Heartbeat interface가 비정상적임)
미흡사례 2	• IPS 및 IDS를 위해 암호화 트래픽을 복호화해주는 SSL 가시성 시스템이 In-Line 모드로 연결되어 있으나, 이중화로 구성되지 않고 단일장비로 운영되고 있음
미흡사례 3	• IPS가 이중화로 구성되어 있으나, HA 기능이 비활성화(monitor interface가 비정상적임)로 운영되고 있음

4.3 네트워크 및 시스템 관리 설비

■ 심사내용 설명

- 네트워크 및 네트워크 설비, 네트워크 보안 설비 등의 상태를 점검

  ※ NMS에서 네트워크 장비 등에 접근 시 접근통제시스템(gateway) 등을 경유하지 않고 직접적인 Terminal에 대한 접근을 Firewall에서 허용하여 NMS를 통한 접근통제체계의 우회 접근이 가능한지 확인

- 서버 시스템의 CPU/메모리/하드디스크 등의 상태를 점검
- 어플리케이션의 트랜잭션 등의 상태를 점검
- 상태를 점검할 수 있는 모니터링 시스템을 통해 실시간으로 모니터링을 수행
  - 모니터링 대상 시스템에 본인확인 관련 설비 포함 여부 확인
  - 모니터링 대상 시스템에 대한 리소스에 대한 임계치의 설정 확인
- 모니터링 시스템에서 이상 징후 탐지 시 즉시 경보
- 이상 징후 발생 시 관리자가 즉각 확인하고 대응할 수 있는 대응 절차 수립

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 네트워크 성능 모니터링 시스템(NMS, MRTG, PRTG 등)
- 서버 성능 모니터링 시스템(SMS, Zabbix 등)
- 어플리케이션 성능 모니터링 시스템(APM, 프로메테우스 등)

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 네트워크 및 네트워크 장비 모니터링 절차서 • 네트워크 구성도 • NMS/SMS/APM 등 모니터링시스템 내 연동 시스템의 목록 • 네트워크 이상 징후 발생 시 대응 결과 보고서
담당자 인터뷰	• NMS 담당자 – 모니터링 시스템의 임계치 설정 및 모니터링에 대한 설명 – 이상 징후 발생 시 대응 절차에 대한 설명 – 네트워크 모니터링 및 config 백업 등 NMS의 용도에 대한 설명 • SMS 담당자 – 모니터링 시스템의 임계치 설정 및 모니터링에 대한 설명 – 이상 징후 발생 시 대응 절차에 대한 설명 – SMS의 용도 및 구성에 대한 설명 • APM 담당자 – 모니터링 시스템의 임계치 설정 및 모니터링에 대한 설명 – 이상 징후 발생 시 대응 절차에 대한 설명 – 분석 대상인 어플리케이션 로그 유형에 대한 설명
현장실사	• NMS/SMS/APM 등 성능 모니터링 시스템 실사

■ 사례 검토

미흡사례 1	• 네트워크 및 네트워크 장비의 성능을 NMS를 통해 모니터링하고 있으나, Firewall, IDS, IPS 등 네트워크 보안 설비는 NMS에 수용되어 있지 않음
미흡사례 2	• 본인확인 관련 어플리케이션이 APM에 수용되어 있으나, 모니터링 요원 부족으로 상시 모니터링 대상에 포함되어 있지 않음
미흡사례 3	• SMS으로 서버 시스템의 CPU/메모리/하드디스크 등의 자원 상태를 점검하고 있으나, 임계치를 설정하지 않거나 내부 기준 없이 높은 임계치 값(90점)으로 일괄 설정하고 있음
미흡사례 4	• NMS를 통해 네트워크 장비 모니터링하고, 장애 발생 시 NMS에서 네트워크 장비로 직접 터미널 접속을 하고 있어 접근통제 정책을 위반하고 있음

5. 화재·수해 및 정전 등 재난 방지를 위한 설비

5.1 화재 발생 시 이를 조기에 감지하고 진화하는 설비

■ 심사내용 설명

- 화재 발생 시 이를 조기에 감지하고 진화하는 설비 구비
- 연기감지장치, 온도감지장치 및 화재경보장치를 구비하고 배치도를 통해 확인

  ※ 화재 감지 및 경보 장치의 종류 : 연기 및 열감지, 덕트 감지기, 적·자외선 감지기 등
- 소규모 및 대규모 화재에 대처할 수 있는 소화장치 구비

  ※ 물을 사용하는 스프링클러를 제거하고, 시스템 운영에 악영향을 미칠 수 있는 소화약재를 사용하지 않음
- 사용하는 소화제가 인체에 무해한지 확인해야 하며, 유해하다면 소화제 작동 전에 본인확인업무 관련 설비 운영자에게 통지하는 체계 수립

  ※ 소화기의 종류 : 이산화탄소 소화기(탄산가스 소화기), 할론 소화기, 자동 확산 소화용구(시스템관리실이나 서버실의 천정에 설치)

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)

  – 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 화재조기감지 및 진화 설비
- 화재 조기 감지 및 진화 계획 수립 현황
- 화재 예방 설비 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 설비에 대한 화재조기감지 및 진화장치 현황 • 화재감지, 경보장치 및 진화장치 설치 현황 사진 • 화재감지, 경보장치와 소화설비 등 진화장치 등이 표시된 배치도 • 화재감지 및 경보장치에 대한 정기점검 이행 현황 • 소화설비 등 진화장치에 대한 정기점검 이행 및 점검일지 사진 • 화재 대비 관련 문서, 내부 지침 및 비상연락망 현황
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 화재 예방 및 대책 관련 내용 설명 • 화재감지, 경보장치 및 진화장치 운영 담당자 – 화재감지, 경보장치 운영 현황과 정기점검 이행 현황 설명 – 소화설비 작동 방식 및 소화용재 사용 현황 설명 – 화재 발생 시 조기감지 및 진화 계획 수립 현황 설명 – 화재 발생 시 대응체계 및 비상연락망 수립 현황 설명
현장실사	• 화재조기감지 및 진화 계획 수립, 화재 발생 시 비상연락망 • 화재조기감지 및 진화장치 설치 현황 확인 • 화재감지 및 경보장치에 대한 정기점검 수행 현황 • 화재 발생 시 진화 계획, 진화 방식 관련 내부 지침 • 본인확인업무 관련 설비 대상 소화설비 구축 및 운영 현황 • 스프링쿨러 제거 여부 및 사용하고 있는 소화제 확인 • 소화기 비치 또는 자동 확산 소화용구 설치 현황 확인 • 소화설비에 대한 정기점검 시행 및 주기적 점검일지 작성 현황 • 화재 예방 관련 문서 및 내부 지침 수립 내용 확인

■ 사례 검토

미흡사례 1	• 본인확인업무 관련 주요 설비에 대한 화재감지 및 경보 장치가 설치되어 있지 않으며, 화재 설비에 대한 정기점검 과정을 이행하지 않음
미흡사례 2	• 신규 도입된 본인확인업무 관련 주요 설비가 비치된 공간에 스프링쿨러가 설치되어 있고, 화재감지 및 경보 장치가 설치되어 있지 않음

5.2 수재 예방 설비

■ 심사내용 설명

- 수해에 대비한 설비를 구비하고 운영
- 본인확인정보의 발급/관리 및 유효성 확인 설비에 대해서는 물에 노출되지 않도록 바닥으로부터 이격하여 설치
- 본인확인관련 설비 및 주요 시스템실에는 Access Floor를 설치하여 운영

  ※ ACCESS FLOOR의 종류

  - STEEL형 : STEEL형은 앞뒤 판넬이 모두 강판으로 제작되어 있으며, 특히 뒷면은 특유의 역학적인 구조로 되어 있어 강도가 매우 뛰어남
  - WOOD형 : WOOD형은 목재 특유의 특성을 그대로 유지한 판넬로 가격이 가장 저렴하고, 목재특유의 보행감각을 유지시켜주며, 파티칼 보드의 우수한 흡음성에 의 하여 진동 및 소음감소특성이 매우 뛰어남
  - Aluminum형 : Aluminum Panel은 고순도의 Aluminum 합금 판넬로서 내부식 성, 청결성, 정밀성이 매우 우수한 경량성의 패널

- 전원접속장치를 바닥으로부터 이격 설치하여 수해 재해 예방 기능을 제공

  ※ 전원접속장치를 바닥에서 일정거리 이상 떨어지게 설치하여 바닥에 물이 차더라도 안정적으로 전원을 공급하고 감전이 되지 않도록 함

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 수해 예방 설비 구축 현황
- 수해 예방 설비 구축 및 운영 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 수해 대비 설비에 대한 구축 및 운영 현황 • 본인확인업무 관련 설비 바닥 이격(30cm 이상) 설치 현황 사진 • 본인확인업무 관련 설비 전원접속장치 바닥 이격 설치 현황 사진 • 기타 본인확인업무 관련 설비에 대한 수해 예방 장치 운영 현황 • 수해 대비 관련 문서, 내부 지침 및 비상연락망
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 수해 예방 및 설비 운영 내용 설명 • 수해 예방 장치, 전원접속 장치 운영 담당자 – 수해 예방 장치 및 전원접속 장치 바닥 이격 설치 현황 설명 – 수해 발생 시 대응체계 및 비상연락망 수립 현황 설명 – 수해 대비 설비에 대한 주기적 점검 및 관리 현황 설명 – 수해 대비 관련 문서 및 내부 지침 수립 현황 설명
현장실사	• 수해 대비 설비에 대한 운영 및 관리 현황 • 본인확인업무 관련 설비 바닥 이격(30cm 이상) 설치 확인 • 본인확인업무 관련 설비 전원접속장치 바닥 이격 설치 확인 • 수해 대비 관련 주기적 점검 이행 내역 확인

■ 사례 검토

미흡사례 1	• 본인확인관련 설비 및 주요 시스템실에 Access Floor가 설치되어 있지 않아 수해 발생 시 본인확인업무 관련 주요 시스템 및 장비가 정상적으로 작동하지 않음
미흡사례 2	• 본인확인관련 설비 및 주요 시스템실에 전원접속장치가 바닥으로부터 일정 간격(30cm 이상 권고) 이격되지 않은 상태에서 바닥에 배수 처리 기능을 제공하지 않아, 수해 발생 시 본인확인업무 관련 주요 시스템 및 장비에 대한 전원공급이 정상적으로 작동하지 않음

5.3 정전발생 시 지속적인 본인확인업무의 수행이 가능하도록 30분 이상 전원을 공급해줄 수 있는 장치

■ 심사내용 설명

- 정전 발생 시를 대비한 전원공급 설비 및 장치 구축
- 정전 발생 시 지속적인 본인확인업무의 수행이 가능하도록 30분 이상 전원을 공급하는 장치 설치

  ※ 전원공급 장치별 확인사항
  가. 무정전 전원공급 장치(UPS) : 공급 용량 및 시간, 배터리 유효기간 등
  나. 발전설비 : 발전용량, 연료 확보 여부 등

- UPS 및 발전설비 용량 대비 본인확인업무 수행에 필요한 최소 전력량(Load)을 확인하여 정전 발생 시 지속적인 본인확인업무 수행이 가능하도록 전원공급 설비 구축 및 운영

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 정전 발생 대비 설비 구축 현황
- 정전 발생 대비 설비 운영 및 관리 현황

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 설비 및 시스템에 대한 전원공급 장치 구축 현황 • 본인확인업무 수행에 필요한 최소 전력량(Load) 측정 수치 • 무정전 전원공급 장치(UPS) 공급 용량, 시간, 배터리 유효기간 등 • 정전을 대비한 발전설비 용량 및 운영 현황 사진 • 정전 대비 관련 문서, 내부 지침 및 비상연락망

구분	준비사항
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 내 정전 대비 전원공급 설비 운영 내용 설명 • 정전 대비 및 전원공급 설비 운영 담당자 – 무정전 전원공급 장치(UPS), 발전설비 구축 현황 설명 – 정전 발생 시 대응체계 및 비상연락망 수립 현황 설명 – 전원공급 설비에 대한 주기적 점검 및 관리 현황 설명 – 정전 대비 관련 문서 및 내부 지침 수립 현황 설명
현장실사	• 정전 대비 전원공급 설비에 대한 구축 및 운영 현황 • 무정전 전원공급 장치(UPS), 발전설비 운영 현황 확인 • 무정전 전원공급 장치(UPS)를 통해 공급 가능한 전력량, 시간 및 배터리 유효기간 확인 • 본인확인업무 수행에 필요한 최소 전력량(Load) 대비 UPS 또는 발전설비를 통해 공급 가능한 전력량 확인 • 정전 발생 시 지속적인 본인확인업무 수행이 가능하도록 30분 이상 전원 공급 여부 확인

사례 검토

미흡사례 1	• 본인확인업무 관련 설비 및 장치에 대한 정전 대비 UPS 또는 발전설비가 구비되지 않아 정전 발생 시 본인확인업무에 대한 지속적이고 안정적인 운영이 어려움
미흡사례 2	• 정전 발생 시 발전설비를 통해 공급 가능한 전력량이 본인확인업무 관련 주요 설비 운영에 필요한 최소 전력량보다 부족하여 지속적이고 본인확인서비스의 안정적인 운영이 어려움

5.4 온도 및 습도를 일정하게 유지하기 위한 항온항습장치

■ 심사내용 설명

- 본인확인업무 관련 설비의 안정적 운영을 위해 항온항습장치 설치
- 항온항습장치를 통해 온도 및 습도를 일정하게 유지하여 본인확인업무 관련 설비에 대한 안정적 운영

※ 본인확인업무 관련 설비에 대한 온도 및 습도 기준
가. 온도 : 18±2°C　　나. 습도 : 50±5%

■ 관련 법규

- 개인정보 보호법 제29조(안전조치의무)
  - 개인정보의 안전성 확보조치 기준 제11조(재해·재난 대비 안전조치)

■ 심사 대상

- 본인확인업무 관련 설비에 대한 항온항습장치 설치 현황
- 본인확인업무 관련 설비에 대한 항온항습 유지 방안

■ 담당자인터뷰, 증적자료, 현장실사 등 준비사항

구분	준비사항
증적자료	• 본인확인업무 관련 설비에 대한 항온항습장치 설치 현황 • 본인확인업무 관련 설비 온도 점검일지 및 관리 현황 사진 • 본인확인업무 관련 설비 습도 점검일지 및 관리 현황 사진 • 항온항습 유지 관련 문서 및 내부 지침
담당자 인터뷰	• 물리적 보안 및 재난·재해 관련 담당자 – 재난·재해 지침·정책 또는 기관 내 항온항습 운영 지침 내용 설명 • 항온항습 설비 운영 담당자 – 항온항습 설비 운영 현황 설명 – 항온항습 관련 문서 및 내부 지침 수립 현황 설명

구분	준비사항
현장실사	• 본인확인업무 관련 설비에 대한 항온항습 유지 관련 문서 및 내부 지침 확인 • 항온항습 설비에 대한 주기적 점검 이행 내역 확인 • 본인확인업무 관련 설비에 대한 현장 방문 시 온도 및 습도를 확인하고 내부 지침에서 정한 범위에 해당하는지 확인

사례 검토

미흡사례 1	• 본인확인업무 관련 설비가 비치된 보호구역 내 온도가 내부 지침과 달리 매우 높고, 환풍구 등을 통한 예열 저감 기능 등도 원활하지 않아 시스템 과열(전기회로 오동작) 등으로 인해 본인확인서비스의 안정적인 운영이 어려움
미흡사례 2	• 본인확인업무 관련 설비가 비치된 보호구역 내 습도가 내부 지침과 달리 매우 높고, 습기 제거 기능도 원활하지 않아 정전기 발생(시스템 오동작) 등으로 인해 본인확인서비스의 안정적인 운영이 어려움

참고자료

[참고1] 본인확인기관 평가기준 법령

■「정보통신망법」 제23조의2 내지 제23조의4

제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우
2. 삭제
3. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스 등을 제공받아 재판매하는 전기통신사업자가 제23조의3에 따라 본인확인기관으로 지정받은 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하는 경우

② 제1항제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

제23조의3(본인확인기관의 지정 등) ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.

1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적·재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

② 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다.

③ 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다.

④ 제1항부터 제3항까지의 규정에 따른 심사사항별 세부 심사기준·지정절차 및 휴지·폐지 등에 관하여 필요한 사항은 대통령령으로 정한다.

제23조의4(본인확인업무의 정지 및 지정취소) ① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

② 제1항에 따른 처분의 기준, 절차 및 그 밖에 필요한 사항은 대통령령으로 정한다.

■ 「정보통신망법」 시행령 제9조의3 내지 제9조의7

제9조의3(심사사항별 세부 심사기준) ① 법 제23조의3제1항에 따른 심사사항별 세부 심사기준은 다음 각 호와 같다.

1. 물리적·기술적·관리적 조치계획: 다음 각 목의 사항에 대한 조치계획을 마련할 것
   가. 법 제23조의3제1항에 따른 본인확인업무(이하 "본인확인업무"라 한다) 관련 설비의 관리 및 운영에 관한 사항
   나. 정보통신망 침해행위의 방지에 관한 사항
   다. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항
   라. 이용자 보호 및 불만처리에 관한 사항
   마. 긴급상황 및 비상상태의 대응에 관한 사항
   바. 본인확인업무를 위한 내부 규정의 수립 및 시행에 관한 사항
   사. 법 제23조의2제2항에 따른 대체수단(이하 "대체수단"이라 한다)의 안전성 확보에 관한 사항
   아. 접속정보의 위조·변조 방지에 관한 사항
   자. 그 밖에 본인확인업무를 위하여 방송통신위원회가 정하여 고시하는 사항
2. 기술적 능력: 다음 각 목의 어느 하나에 해당하는 요건을 갖춘 자를 8명 이상 보유할 것
   가. 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 방송통신위원회가 인정하는 자격을 갖출 것
   나. 방송통신위원회가 정하여 고시하는 정보보호 또는 정보통신운영·관리 분야에서 2년 이상 근무한 경력이 있을 것
3. 재정적 능력: 자본금이 80억원 이상일 것(국가기관 및 지방자치단체는 제외한다)
4. 설비규모의 적정성: 다음 각 목의 설비를 본인확인업무의 적절한 수행에 필요한 규모 이상 보유할 것
   가. 이용자의 개인정보(「개인정보 보호법」 제2조제1호에 따른 개인정보를 말한다. 이하 제9조의6에서 같다)를 검증·관리 및 보호하기 위한 설비
   나. 대체수단을 생성·발급 및 관리하기 위한 설비
   다. 출입통제 및 접근제한을 위한 보안설비
   라. 시스템 및 네트워크의 보호설비
   마. 화재·수해 및 정전 등 재난 방지를 위한 설비

② 제1항에 따른 심사사항별 세부 심사기준의 평가기준 및 평가방법 등에 관하여 필요한 사항은 방송통신위원회가 정하여 고시한다.

제9조의4(본인확인기관의 지정절차) ① 법 제23조의3제1항에 따라 본인확인기관으로 지정을 받으려는 자는 본인확인기관지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 방송통신위원회에 제출하여야 한다.

1. 조직·인력 및 설비 등의 현황을 기재한 사업계획서
2. 제9조의3에 따른 심사사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류
3. 법인의 정관 또는 단체의 규약(법인 또는 단체인 경우에만 해당한다)
4. 그 밖에 본인확인업무 수행의 전문성과 재무구조의 건전성 등을 확인하기 위하여 필요한 서류로서 방송통신위원회가 정하여 고시하는 서류

② 제1항에 따라 본인확인기관지정신청서를 제출받은 방송통신위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서(법인인 경우에만 해당한다)를 확인하여야 한다.

③ 방송통신위원회는 제1항에 따른 신청을 심사하는 데 필요하다고 인정하는 경우에는 그 신청인에게 자료의 제출을 요청하거나 그 의견을 들을 수 있다.

④ 방송통신위원회는 제1항에 따른 신청을 받은 경우에는 신청을 받은 날부터 90일 이내에 제9조의3에 따른 심사사항별 세부 심사기준의 충족 여부를 심사하여 그 심사결과를 신청인에게 통지하여야 한다. 다만, 부득이한 사유가 있는 경우에는 그 사유를 알리고 30일의 범위에서 그 기간을 연장할 수 있다.

⑤ 방송통신위원회는 제4항의 심사결과에 따라 본인확인기관을 지정한 경우에는 그 신청인에게 본인확인기관지정서를 발급하고, 본인확인기관의 명칭·소재지 및 지정일 등 지정내용을 관보에 고시하여야 한다.

⑥ 제1항부터 제5항까지의 규정에 따른 지정신청, 지정심사 등의 절차 및 방법 등에 관하여 필요한 사항은 방송통신위원회가 정하여 고시한다.

제9조의5(본인확인기관의 주민등록전산정보자료 확인 요청) 법 제23조의3제1항에 따라 본인확인기관으로 지정받은 자(이하 "본인확인기관"이라 한다)는 14세 미만의 아동 및 그 법정대리인의 신원 확인을 위하여 필요한 경우 행정안전부장관에게 「주민등록법」 제30조제1항에 따른 주민등록전산정보자료의 확인을 요청할 수 있다.

제9조의6(본인확인업무의 휴지·폐지) ① 본인확인기관이 법 제23조의3제2항 또는 제3항에 따라 업무를 휴지 또는 폐지하려면 다음 각 호의 사항을 이용자에게 통보하여야 한다.

1. 휴지 또는 폐지의 사유
2. 휴지 또는 폐지의 일시(휴지의 경우에는 사업의 개시일시를 포함한다)
3. 대체수단 및 개인정보의 이용 제한에 관한 사항(휴지의 경우에만 해당한다)
4. 대체수단 및 개인정보의 파기에 관한 사항(폐지의 경우에만 해당한다)

② 본인확인기관은 법 제23조의3제2항 또는 제3항에 따라 본인확인업무의 휴지 또는 폐지를 신고할 때에는 본인확인업무 휴지·폐지 신고서에 다음 각 호의 서류를 첨부하여 방송통신위원회에 제출하여야 한다.

1. 제1항 각 호의 사항을 기재한 통보 서류
2. 대체수단 및 개인정보의 이용 제한 또는 파기 계획에 관한 서류
3. 이용자의 보호조치 계획에 관한 서류
4. 본인확인기관지정서(폐지의 경우에만 해당한다)

③ 제1항 또는 제2항에 따른 휴지 또는 폐지의 통보 및 신고의 절차, 기준 및 방법 등에 관하여 필요한 세부사항은 방송통신위원회가 정하여 고시한다.

제9조의7(본인확인업무의 정지 및 지정취소) ① 법 제23조의4제1항에 따른 본인확인업무의 정지 또는 지정취소의 기준은 별표 1과 같다.

② 방송통신위원회는 제1항에 따라 본인확인업무를 정지하거나 지정을 취소한 경우에는 그 사실을 관보에 고시하여야 한다.

■「본인확인기관 지정 등에 관한 기준」 전문

제1조(목적) 이 기준은「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제23조의3 및 같은 법 시행령(이하 "영"이라 한다) 제9조의3부터 제9조의5까지의 본인확인기관의 지정에 필요한 세부심사기준 및 평가방법과 본인확인업무의 휴지 또는 폐지의 통보 및 신고의 절차 등을 정함을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 정의는 다음과 같다.

1. "본인확인기관"이라 함은 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하는 자로서 법 제23조의3제1항에 따라 방송통신위원회로부터 본인확인기관의 지정을 받은 자를 말한다.
2. "지정신청기관"이라 함은 본인확인기관지정을 받고자 하는 국가기관, 지방자치단체, 법인 또는 단체를 말한다.
3. "본인확인입력정보"라 함은 본인확인을 위하여 이용자에게 발급된 대체수단(아이디, 휴대전화 번호 등) 및 이용자가 입력하는 부가정보(비밀번호 등)를 말한다.
4. "본인확인결과정보"라 함은 이용자의 본인확인에 따라 본인확인기관이 본인확인서비스를 이용하는 기관에게 제공하는 결과정보(이름, 생년월일, 연계정보 등)를 말한다.
5. "이용자"라 함은 본인확인기관에 자신의 개인정보를 제공하고 대체수단을 부여 받은 자를 말한다.
6. "중복가입확인정보"라 함은 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는 데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관간 공유비밀정보를 이용하여 생성한 정보를 말한다.
7. "웹사이트 식별정보"라 함은 정보통신서비스 제공자가 운영하는 웹사이트를 다른 웹사이트와 구별하기 위하여 본인확인기관이 부여한 정보를 말한다.
8. "공유비밀정보"라 함은 본인확인기관이 특정 이용자에 대해 동일한 중복가입확인정보와 연계정보를 생성하기 위해 공유하는 정보를 말한다.
9. "연계정보"라 함은 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위해 본인확인기관이 이용자의 주민등록번호와 본인확인기관간 공유 비밀정보를 이용하여 생성한 정보를 말한다.
10. "본인확인서비스"라 함은 본인확인입력정보를 이용하여 이용자를 안전하게 식별·인증하기 위해 본인확인기관이 제공하는 서비스를 말한다.

제3조(지정심사 일정 및 절차 등의 공고) 방송통신위원회는 매년 3월 31일까지 지정심사의 일정 및 절차 등을 포함한 지정심사 계획을 공고할 수 있다.

제4조(지정신청방법) ① 지정신청기관은 별지 제1호서식의 본인확인기관지정신청서에 다음 각 호의 서류를 첨부하여 방송통신위원회에 제출하여야 한다.

1. 조직·인력 및 설비 등의 현황을 기재한 사업계획서

2. 영 제9조의3제1항에 따른 심사사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류
3. 정관 또는 규약(법인 또는 단체인 경우에만 해당한다)
4. 과거 3개년간의 재무제표(법인 또는 단체인 경우에만 해당한다)

② 제1항제1호의 사업계획서는 별표 1의 "사업계획서 작성요령"에 따라 작성하여야 한다.

③ 본인확인기관지정신청서 및 신청서류의 제출 부수는 다음 각 호와 같다.

1. 본인확인기관지정신청서 : 1부
2. 제1항 각 호에 따른 신청서류 : 원본 각 1부, 사본 각 15부 및 이동식 저장매체 1벌

제5조(지정심사계획의 수립) ① 방송통신위원회는 제4조에 따라 지정신청을 접수한 때에는 지정심사를 위한 계획을 수립·시행하여야 한다.

② 제1항에 따른 심사계획은 다음 각 호에 관한 사항을 포함한다.

1. 지정심사 일정, 장소 및 절차
2. 제10조에 따른 심사위원의 구성 및 운영에 관한 사항
3. 기타 지정심사를 위하여 필요한 사항

제6조(서류의 보정 등) ① 지정신청기관은 제3조제1항 각 호의 서류의 수정이 필요한 경우에는 지정심사 전일까지 이를 수정할 수 있다.

② 방송통신위원회가 지정심사에 필요하다고 인정하는 경우에는 모든 지정신청기관에 동일한 조건으로 서류를 추가로 제출하게 하거나 이 기준에서 정한 사업계획서 작성요령을 추가 또는 수정할 수 있다.

제7조(심사기준) ① 지정심사는 본인확인서비스의 안전성과 신뢰성을 보장하기 위한 물리적·기술적·관리적 보호조치와 정보통신설비 관련 시설 및 장비를 대상으로 한다.

② 영 제9조의3제2항에 따른 심사사항별 세부심사기준의 평가기준은 별표 3과 같다.

제8조(심사일) 지정심사는 이 기준에서 달리 정하지 않는 한 지정신청 접수일로부터 60일 이내에 실시한다. 다만, 특별한 사정이 있는 경우에는 30일 범위 내에서 1회에 한하여 연장할 수 있다.

제9조(심사방법) ① 지정심사는 서류심사와 현장실사, 종합심사로 구분하여 실시한다.

② 지정신청기관이 종합심사에서 별표 4에 따른 세부 심사기준별 점수 총점 1000점 만점에 800점 이상 받고, 중요 심사항목 및 계량평가 항목에 대해 적합 판정을 받은 경우 지정신청기관을 지정대상기관으로 선정한다.

③ 제2항에도 불구하고 별표 4에 따른 중요심사 항목 및 계량평가 항목에서 적합 판정을 받고 총점 800점 미만을 받은 경우 조건을 붙여 지정대상기관으로 선정할 수 있다.

④ 방송통신위원회가 심사에 필요하다고 인정하는 때에는 지정신청기관에게 자료제출을 요구하거나 지정신청기관의 의견을 들을 수 있다.

제10조(심사위원의 구성 및 자격) ① 방송통신위원회는 본인확인기관 지정심사를 위해 각 호의 자격 중 하나 이상을 가진 자를 15명 이내의 범위에서 심사위원으로 위촉하여 심사하게 할 수 있다.

1. 「고등교육법」제2조 제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 부교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 정보보호 연구경력이 10년 이상인 자
2. 정부, 공공기관 또는 정보보호 관련 업체 혹은 단체(협회, 조합)에서 10년 이상 정보보호 분야에 근무한 자
3. 정보보호 관련 심사제도의 인증심사원 자격이 있는 자
4. 정보보호 관련 분야 기술사 또는 변호사나 공인회계사의 자격이 있는 자
5. 그 밖에 정보보호에 관한 학식과 경험이 풍부한 자

② 심사위원은 서류심사 및 현장실사 심사항목별로 적정성 여부를 평가하고 개선이 필요하다고 판단되는 경우에는 의견을 제시할 수 있다.

③ 심사위원은 심사대상이 되는 지정신청기관 및 본인확인기관과 이해관계가 있다고 판단되는 경우 심사위원 위촉을 거부하거나 심사업무 수행이 불가한 사실을 즉시 방송통신위원회에 알려야 한다.

④ 본인확인기관 지정심사 및 사후관리를 위한 심사위원 보수는 다음 각 호의 기준을 고려하여 산정한다.

1. 지정기준의 적합성 여부를 판단하기 위하여 별도 책정한 전문가 활용비
2. 심사업무 수행을 위해 원거리 이동이 필요한 경우 지출되는 대중교통 운임
3. 본인확인기관 지정기준 적합성 확인에 필요한 심사기간

제11조(심사결과 통보) ① 본인확인기관의 지정 여부는 방송통신위원회의 심의·의결을 거쳐 확정한다. 이 경우 일부 항목에 대한 개선이 필요하다고 판단되는 경우에는 일정기간 내에 해당 사항에 대한 개선 등 조건을 붙일 수 있다.

② 방송통신위원회는 지정신청일로부터 90일 이내에 심사결과를 지정신청기관에게 통지하여야 한다. 다만, 부득이한 사유가 있을 때에는 그 사유를 알리고 30일의 범위 내에서 그 기한을 연기할 수 있다.

제12조(지정서 교부) ① 방송통신위원회는 지정신청기관에 대해 본인확인기관으로 지정을 하는 때에는 별지 제2호서식의 본인확인기관지정서를 교부한다.

② 방송통신위원회는 지정신청기관에 대해 제11조제1항에 따라 조건을 부과한 경우 그 조건의 이행 여부를 확인하고 본인확인기관지정서를 교부한다.

제12조의2(본인확인업무) ① 법 제23조의3제1항에 따라 지정된 본인확인기관은 다음 각 호의 본인확인 업무를 수행할 수 있다.

1. 대체수단을 제공하기 위해 이용자 신원의 진위여부를 확인하는 업무
2. 연계정보 등 본인확인결과정보 제공 및 관리 업무
3. 그 밖에 대체수단의 개발·제공·관리 등에 관한 업무

② 본인확인기관은 제1항제2호에 따른 본인확인 결과정보를 본인확인서비스를 거치지 아니하고 제3자에게 제공할 수 없다. 다만, 다른 법령에서 특별히 규정한 경우에는 그러지 아니한다.

제13조(사후관리) 방송통신위원회는 본인확인업무의 적정한 추진과 영 제9조의3의 심사사항별 세부 심사기준에 적합한지 여부를 확인하기 위하여 지정을 받은 기관에 대해 관련 자료의 제출을 요구하거나 현장실사를 할 수 있다.

제13조의2(사업계획의 변경) ① 본인확인기관은 대체수단의 추가 또는 변경 등 사업계획을 변경하고자 할 경우에는 제4조에 따른 지정신청에 준하는 방법으로 사업계획 변경을 신청하여야 한다.

② 방송통신위원회는 제1항에 따른 사업계획 변경심사를 하는 경우에는 제4조 내지 제12조를 준용한다.

③ 방송통신위원회는 제4조제1항에 따른 제출서류 외에도 사업계획 변경에 대한 추가서류를 요청할 수 있다.

제14조(이용자에 대한 통보방법) ① 영 제9조의5제1항에 따라 이용자에게 통보하는 때에는 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 하여야 한다.

② 제1항의 규정에 불구하고 본인확인기관이 과실 없이 이용자의 연락처를 알 수 없는 경우에는 인터넷 홈페이지에 30일 이상 게시하는 것으로 통보에 갈음할 수 있다.

제15조(본인확인업무의 휴지·폐지신고) ① 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다.

② 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다.

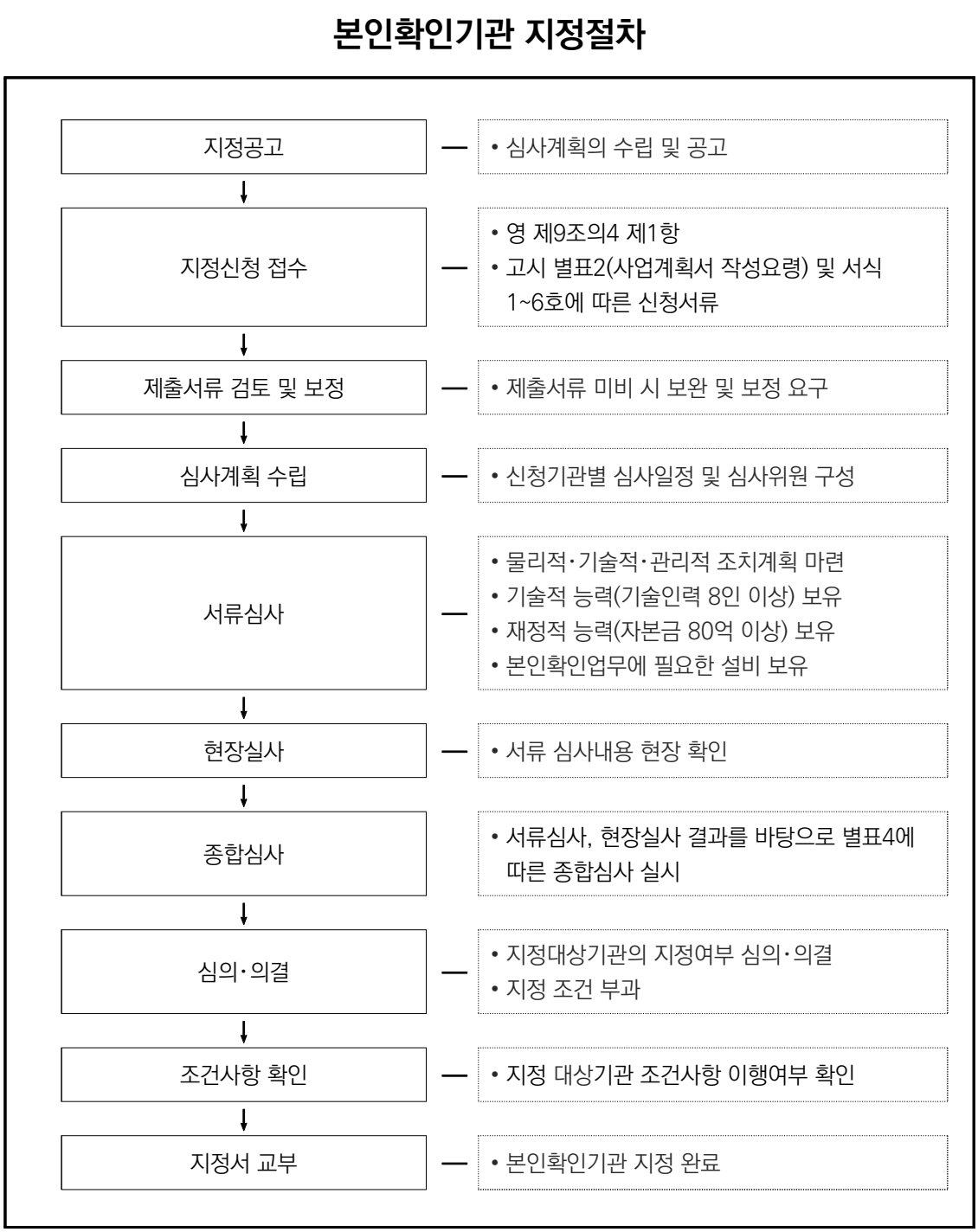
③ 영 제9조의5제2항에 따라 본인확인업무의 휴지 또는 폐지의 신고를 할 때에는 별지 제3호서식의 본인확인업무(휴지·폐지)신고서에 다음 각 호의 서류를 첨부하여 방송통신위원회에 제출하여야 한다.

1. 이용자에게 휴지·폐지 사실을 통보하였음을 확인할 수 있는 서류 1부
2. 대체수단 및 개인정보의 이용 제한 또는 파기 계획에 관한 서류 1부
3. 이용자의 보호조치 계획에 관한 서류 1부
4. 본인확인기관지정서(폐지의 경우에만 해당한다)

제16조(재검토 기한) 방송통신위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2021년 8월 1일 기준으로 매 3년이 되는 시점(매 3년째의 7월 31일까지를 말한다.)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

제17조(규제의 재검토) 방송통신위원회는 「행정규제기본법」에 따라 이 고시에 대하여 2021년 8월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 7월 31일까지를 말한다.)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

[참고2-1] 본인확인기관 지정절차



[참고2-2] 사업계획서 작성요령

Ⅰ. 사업계획서

사업계획서는 다음에 제시하고 있는 작성요령에 따라 분명하고 알아보기 쉬운 활자, 표 및 그림을 이용하여 작성하여야 한다.

요약문

사업계획서 제1권 및 제2권 본문의 주요 내용을 이해하기 쉽게 요약하여 기술하여야 한다.

제1권 지정신청기관에 관한 기본사항

지정신청기관에 관한 기본적인 사항을 기술한다.

제1장 지정신청기관의 명세 및 조직

제1절 지정신청기관의 명세

(국가기관 및 지방자치단체는 제외한다)

지정신청기관의 명칭, 자본금 규모 등을 별지 제4호 서식에 따라 기술한다.

제2절 기관의 조직에 관한 사항

(국가기관 및 지방자치단체는 해당되는 사항만 기재한다)

1. 조직형태

지정신청기관의 조직에 대하여 상세히 기술하여야 한다. 가능한 한 임원급 이상의 조직과 그 주요업무를 그림이나 표를 사용하여 기술하고, 인력현황을 분야별로 구분하여 명시하여야 한다.

2. 임원 등의 신상명세 및 수임권한

위의 조직 형태와 관련하여 지정신청기관의 대표자, 이사 및 감사의 권한과 역할을 기술하고, 이에 대해 구성주주 간에 합의한 사항이 있으면 이를 구성주주 간 계약서 등에 명기하여야 한다.

제2장 지정신청기관 등의 재무상태 및 자금조달능력

(국가기관 및 지방자치단체는 제외한다)

지정신청기관은 지정신청 접수일부터 3개월 이전의 기간 내에서 가능한 한 최근일을 기준으로 주요 재무상태에 관하여 기술하여야 한다.

지정신청기관은 최근 결산일을 기준으로 과거 3개년간의 주요 재무지표 및 재무수치를 별지 제5호서식과 별지 제6호서식에 따라 작성하여 부속서류로 제출하여야 한다(단, 부득이한 사유로 과거 3개년간의 재무지표, 재무수치 및 재무제표를 제출하지 못하는 경우에는 그 사유와 근거자료를 제출하여야 한다).

지정신청기관은 위의 재무관련 서류의 진위확인을 위하여 감사보고서중 대차대조표, 손익계산서 사본(회계감사법인 확인필) 또는 표준재무제표증명(재무제표확인원) 사본을 첨부하여 제출한다.

제2권 보호조치 계획 및 설비 규모

본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 보호조치 계획, 기술능력 및 설비 규모 등에 대한 사항을 차례대로 기술하여야 한다. 각 항목별 세부 내용은 [별표 3] 심사사항별 세부심사기준의 평가기준의 목차에 따라 작성한다.

[별표 3] 심사사항별 세부심사기준의 평가기준에서 가.나.다. 수준의 항목으로 구분하여 작성하며, 가.나.다. 없는 경우 상위 항목으로 작성한다. 작성내용의 증빙을 위하여 부속서류를 첨부할 수 있다.

Ⅱ. 사업계획서 작성 및 제출 시 유의사항

1. 사업계획서 작성 양식 및 분량

사업계획서는 양면인쇄를 원칙으로 하며, 지도·도면 등 불가피하게 A4 규격보다 큰 규격의 종이를 사용할 때는 같은 크기로 접어서 제출하여야 한다.

사업계획서의 요약문은 25쪽 이내로 작성하여야 한다. 본문은 제1권·제2권 모두 합하여(표지 포함) 200쪽을 넘지 않는 것을 원칙으로 하되, 각 권별 분량은 지정신청기관이 임의로 정한다.

사업계획서의 부속서류는 공공기관이 발행한 각종 증빙서류와 본 "사업계획서 작성요령"에서 부속서류로 제출하도록 정한 것으로 한다. 지정신청기관이 위에서 정한 내용 이외의 것을 부속서류로 제출하였을 때는 이를 심사하지 아니한다. 각 권별 부속서류가 200쪽을 넘을 때에는 본문과 구분하여 별도로 제출할 수 있다.

사업계획서의 요약문, 본문 및 부속서류는 쪽번호를 중앙하단에 각권을 구분하여 표시하여야 한다.

2. 사업계획서 작성의 전제조건

사업계획서는 다음의 전제조건에 따라 작성하여야 한다. 다만, 법률의 제·개정 등 기타 사정에 따라 변경될 수 있다.

가. 주요 경제지표는 다음 각목에 따른다.

(1) 물가 : 상반기 신청의 경우에는 전년도 12월 31일 현재가격, 하반기 신청의 경우에는 당해 연도 6월 30일 현재가격
(2) 환율 : 지정신청일을 기준으로 전 분기말일 최초로 고시된 한국은행의 매매기준율
(3) 차입금이자율 : 법인세법상 국세청장이 정하는 인정이자 계산 시 적용할 당좌대월 이자율
(4) 예금이자율 : 차입금이자율에서 2%를 차감한 이자율

나. 감가상각은 법인세법의 기준 내용연수에 의한 정액법을 적용한다.

다. 제세공과금은 전년도 12월 31일 현재의 소득세·법인세·관세 등 제세공과금에 관한 법률 등을 적용한다.

3. 언어, 화폐단위 및 도량형

지정신청서류는 한글로 작성하여야 한다. 다만, 명확한 의사전달을 위하여 외국어나 한자의 사용이 불가피한 경우에는 한글로 표기하고 괄호 안에 외국어나 한자를 함께 적어야 한다. 또한, 증빙서류 및 계약서의 원문이 외국어일 때는 원문과 함께 한글 번역본을 공증받아 붙여야 한다.

화폐단위는 원화로 표시하여야 한다. 다만, 증빙서류 등에 사용된 화폐의 단위가 외국 통화로 표기된 경우에는 원화로 환산된 수치를 함께 적어야 한다.

도량형은 미터법으로 하여야 한다. 다만, 각종 증빙서류 등이 미터법 이외의 도량형으로 작성되었을 경우에는 미터법으로 환산한 수치를 함께 적어야 한다.

4. 사업계획서의 서명

사업계획서의 원본에는 표지의 우측 상단에 "원본"임을 표시하고 표지의 다음쪽에 원본임이 틀림없다는 내용, 지정신청기관명, 대표자명을 기재한 후 대표자가 서명·날인(인감)하여야 하며 인감증명서를 부속서류로 제출하여야 한다.

사업계획서의 사본에는 표지의 우측 상단에 "사본" 및 사본번호를 표시하고 표지의 다음쪽에 원본과 동일하다는 내용, 지정신청기관명, 대표자명을 기재한 후 대표자가 서명·날인(인감)하여야 한다.

사업계획서의 원본과 사본의 내용이 달라서는 아니된다.

5. 지정신청서류의 분류 및 봉함

사업계획서는 본문(제1권·제2권 전체)에 대한 요약문, 제1권 본문 및 부속서류, 제2권 본문 및 부속서류를 합철하여 책자형태의 1책으로 하되, 제1권 및 제2권의 본문과 부속서류는 간지 등으로 구분하고 쪽수도 별도로 구분하여 기재한다.

사업계획서의 원본은 따로 불투명한 봉투에 넣어 봉인하고, 사업계획서의 사본 15부를 권별로 일괄 포장하여 봉인하여야 한다. 별도로 제출하는 이동식저장매체의 경우도 일괄 포장하여 봉인하여야 한다.

봉인된 봉투 또는 박스의 겉면에는 각각의 내용물에 대한 목록을 표기하여 운반이 용이한 파일박스(종이박스 가능)에 넣어 제출하여야 한다.

[참고2-3] 심사사항별 세부심사기준의 평가기준

Ⅰ. 물리적·기술적·관리적 조치계획

1. 본인확인업무 관련 설비의 관리 및 운영에 관한 사항

1-1. 물리적 출입 및 접근 통제

가. 비인가자 출입통제 및 감사

(1) 비인가자가 본인확인업무 관련 발급·관리 설비 운영실에 접근할 수 없도록 하는 물리적인 출입통제 기능

(2) 일련번호, 사건의 유형, 성공·실패 여부 및 실패 시 원인, 일자 및 시각, 행위자 등에 대한 정보의 감사기록 기능

나. 생체특성기반(지문인식, 홍채인식 등)을 포함하는 2개 이상의 출입통제장치를 사용하는 기능

다. 감사기록의 저장 및 백업

(1) CCTV 등을 통해 발급시스템 운영실을 감시·통제하는 기능

(2) 24시간 감시·통제에 대한 감사기록을 저장 및 백업하는 기능

(3) CCTV 시스템의 시간동기화 기능

1-2. 화재·수해 등 재해 대비

가. 화재 예방 및 대책

(1) 화재의 조기 감지 및 진화 계획

(2) 화재설비에 대한 정기점검 시행 및 점검일지 작성

나. 수해에 대비한 설비의 운영

다. 정전 발생 대비 방안

라. 시스템의 항온항습 유지 방안

2. 정보통신망 침해행위의 방지에 관한 사항

2-1. 침입차단·탐지·방지 시스템

가. CC EAL2등급 이상의 Firewall, IDS 또는 IPS 운영

나. 본인확인업무에 한정된 접근통제규칙을 설정하여 사용

다. 모든 트래픽에 대한 점검 및 침입 탐지

라. 새로운 패턴의 침입유형에 대한 추가 기능

마. 침입이 탐지되었을 경우 이를 관리자에게 알리는 기능

바. Firewall, IDS 또는 IPS에서의 로그 관리 기능

2-2. 시스템 접근 통제

가. 접근권한이 없는 자가 시스템에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉·유출하는 행위에 대한 검사

나. 정당한 권한이 없는 사람이 본인확인서비스와 관련된 통신망의 접근과 침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영

2-3. 저장정보의 조작·파괴·은닉 및 유출방지

가. 본인확인서비스와 관련된 데이터를 파괴하거나 본인확인서비스의 운영을 방해할 목적으로 바이러스·논리폭탄 등의 프로그램을 투입하는 행위의 검사

나. 본인확인서비스의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위의 검사

다. 대체수단 관련 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치

3. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항

3-1. 본인확인 시스템 보안

가. 관리자가 본인확인시스템 접속 시 일반 인터넷망과 분리되어 있는 별도의 PC 또는 접속경로를 사용하는 기능

나. 시스템에 접속 가능한 IP주소와 사용자 계정에 대한 데이터접근권한을 지정하는 기능

다. 시스템과 연결된 PC에서 이동저장매체 사용 시 이를 통제하는 기능

3-2. 네트워크 및 시스템 안정성 점검

가. 실시간으로 네트워크 및 시스템 상태를 점검할 수 있는 시스템 또는 장비 운영

나. 본인확인업무와 관련된 주요 프로그램 또는 프로세스 동작여부를 점검할 수 있는 시스템 또는 장비 운영

다. 대체수단의 부정사용 여부에 대한 모니터링 및 정책 수립

3-3. 시스템 취약점 점검

가. 기존에 알려진 취약성 및 신규 취약성에 대비한 점검

3-4. 소프트웨어의 임의변경·삭제 방지

가. 본인확인서비스 관련 소프트웨어를 임의로 변경 및 삭제할 수 없도록 하는 기능

4. 이용자 보호 및 불만처리에 관한 사항

4-1. 대체수단 발급 절차에 개인정보처리방침을 공개하여 이용자가 쉽게 확인할 수 있도록 하여야 함

4-2. 개인정보 수집에 대한 고지 및 동의

가. 개인정보의 수집·이용목적, 수집하는 개인정보 항목, 개인정보의 보유 및 이용기간을 이용자에게 고지하고 동의를 받아야 함

나. 본인확인서비스 외에 법령의 규정에 의해 정보통신서비스 제공자에게 연령확인 등 선별가입 서비스를 제공할 경우에는 이용자에게 이를 사전에 고지하고 동의를 받아야 함

다. 본인확인서비스를 제공하는데 필요한 정보 이외의 이용자 개인정보 수집의 금지

라. 필요한 최소한의 정보 이외의 개인정보를 제공하지 아니한다는 이유로 이용자에게 서비스 제공을 거부할 수 없음

4-3. 사상·신념·과거병력 등 개인의 권익이나 사생활을 현저하게 침해할 우려가 있는 민감한 개인정보의 수집 금지

4-4. 개인정보의 이용내역확인·동의철회 및 정정

가. 본인확인서비스에 가입된 이용자가 개인정보의 수집·이용·제공에 대한 동의를 철회하는 기능

나. 이용자가 자신의 개인정보에 대한 열람 또는 이용내역의 제공을 요구할 수 있고, 오류가 있는 경우 정정을 요구하는 기능

다. 이용자의 오류 정정요구에 대한 조치가 완료되기 전까지 해당 이용자의 개인정보 제공 또는 이용을 제한하는 기능

4-5. 이용자 불만 등을 접수·처리하기 위한 절차

가. 대체수단의 발급·이용 및 연계정보의 제공 등과 관련한 불만을 접수·처리할 수 있는 절차를 마련하고 담당자를 지정하여야 함

나. 부정한 방법으로 대체수단의 발급 또는 분실·훼손·도난·유출 시 해당 사실을 본인확인기관에 신고할 수 있는 기능

5. 긴급상황 및 비상상태의 대응에 관한 사항

5-1. 장애 및 재해발생에 효과적으로 대처할 수 있는 비상계획 및 재난복구절차

5-2. 운영데이터, 소프트웨어, 시스템, 설비에 대한 백업계획 및 복구계획

5-3. 연계정보 알고리즘 및 키 노출 시 대응절차

5-4. 하나의 회선에 장애가 발생하더라도 본인확인 업무를 지속적으로 제공할 수 있는 기능

6. 본인무를 확인업위한 내부 규정의 수립 및 시행에 관한 사항

6-1. 개인정보관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항

6-2. 개인정보를 처리하는 직원의 교육에 관한 사항

6-3. 이용자의 개인정보를 취급하는 자를 최소한으로 제한

6-4. 본인확인업무의 안전성·신뢰성 보장 및 이용자의 개인정보 보호조치를 이행하기 위해 필요한 세부사항

7. 대체수단의 안전성 확보에 관한 사항

7-1. 대체수단의 발급

가. 장애인 웹 접근성 및 웹 표준의 준수

나. 대체수단의 유일성

(1) 대체수단 유일성에 대한 검사 기능

다. 법정대리인을 통한 대체수단의 발급

(1) 만14세 미만의 자가 대체수단을 발급받고자 하는 경우에는 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원을 확인한 후 동의를 받아야 함

(2) 법정대리인의 실명인증에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치 여부 검사

7-2. 대체수단의 변경·관리

가. 이용자가 자신의 대체수단의 발급 및 갱신·폐지 등의 정보를 열람할 수 있는 기능

나. 이용자가 자신의 대체수단 관련 정보를 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는 기능

다. 이용자가 대체수단 관련 정보의 오류에 대해 정정을 요구할 수 있는 기능

라. 대체수단 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보 발송

7-3. 대체수단 관련 정보의 저장 및 백업

가. 대체수단 관련 기록의 저장·백업·삭제

(1) 이용자의 대체수단 이용내역 등에 대한 이력 관리 기능

(2) 대체수단이 폐지된 날로부터 5년 경과 후 이용자 등록정보 삭제

나. 대체수단의 발급 및 갱신·폐지와 제3자 제공 내역의 저장·관리

(1) 대체수단 신청 및 폐지에 대한 기록, 신원확인 시 제출서류, 제시한 증명서 사본, 정보통신망을 통해 입력한 정보 등에 대한 백업 기능

7-4. 대체수단의 폐지

가. 대체수단 폐지 신청시 이용자의 정당한 권한 여부를 확인하는 절차

나. 이용자의 대체수단 폐지 요청 후 대체수단 폐지 사실을 이용자에게 통지

7-5. 대체수단의 연동

가. 본인확인 인증

(1) 본인확인입력정보를 이용한 본인확인인증이 정상적으로 이루어져야 함

(2) 본인확인 입력정보를 안전하게 보호하기 위한 수단이 제공되어야 함

나. 정보통신서비스제공자와의 연동

(1) 본인확인인증 시 정보통신서비스 제공자에게 전달 형식에 이름, 생년월일 정보, 성별 정보 등 본인확인결과 정보를 제공하는 기능

(2) 연계정보를 필요로 하는 사업자가 대체수단 도입 사이트에 연계정보를 요청하였을 때 본인확인기관과 대체수단 도입 사이트 간 연동 기능

다. 중복가입확인정보의 제공

(1) 주민등록번호, 본인확인기관간 공유 비밀정보 등을 이용하여 중복가입확인정보를 제공하는 기능

라. 연계정보의 제공

(1) 주민등록번호, 본인확인기관간 공유 비밀정보 등을 이용하여 연계정보를 제공하는 기능

7-6. 본인확인서비스 연계 시 보호 조치

가. 위조·변조·삭제 및 유출 방지를 위한 암호화

(1) 대칭키 암호방식을 이용하는 경우 정보통신서비스 제공자에 배포한 비밀키를 주기적으로 갱신하는 기능

(2) 권한 있는 관리자만이 시스템에 접근할 수 있는 접근통제 기능

(3) 본인확인서비스 관련 소프트웨어를 임의로 변경 및 삭제할 수 없도록 하는 기능

나. 본인확인서비스 전송구간의 암호화

(1) 암호알고리즘 등을 통해 중복가입확인정보 및 연계정보를 안전하게 전송하는 기능

(2) 전송된 정보의 위·변조 여부를 검증할 수 있는 기능

다. 무결성 검증

(1) 이용자가 대체수단 신규발급 시 본인확인기관에 제공한 정보에 대하여 해쉬 체인을 구성하는 기능

7-7. 이용자 개인정보의 암호화

가. 비밀정보를 일방향 암호화하여 저장하는 기능

나. 이용자 개인정보 중 주민등록번호를 암호화하여 저장하는 기능

다. 암호화를 위한 알고리즘 및 비밀정보를 주기적으로 변경·관리하는 기능

8. 접속정보의 위조·변조 방지에 관한 사항

8-1. 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독

8-2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

9. 본인확인업무와 다른 인터넷 서비스와의 분리

9-1. 대체수단 발급 시 본인확인기관의 다른 인터넷서비스에 대한 회원가입을 요구하지 않아야 함

9-2. 본인확인서비스 제공을 위한 시스템 및 개인정보 DB를 물리적 또는 논리적으로 다른 서비스와 분리하여 운영하여야 함

Ⅱ. 기술적 능력

별표 5.의 자격 중 어느 하나를 갖춘 기술 인력을 8인 이상 보유할 것

Ⅲ. 재정적 능력

자본금 : 80억 원 이상일 것 (국가기관 및 지방자치단체는 제외한다)

Ⅳ. 설비규모의 적정성

1. 이용자의 개인정보를 검증·관리 및 보호하기 위한 설비

1-1. 이용자의 등록정보를 관리하기 위한 설비

1-2. 신원확인을 수행하기 위한 설비(인증서, 신용카드, 휴대전화 SMS, 대면확인 등)

2. 대체수단을 생성·발급 및 관리하기 위한 설비

2-1. 대체수단의 관리 및 제공하기 위한 설비
2-2. 본인확인서비스에 관한 시설 및 장비를 안전하게 운영하기 위한 보호설비

3. 출입통제 및 접근제한을 위한 보안설비

3-1. 본인확인업무 시스템을 안전하게 운영할 수 있는 별도의 통제구역
3-2. 본인확인업무 시스템에 대한 출입을 통제하고 이에 대한 감사기록 기능을 갖는 장치
3-3. 생체기반을 포함한 다중 신원확인 기능을 갖는 출입통제장치
3-4. 본인확인업무 시스템 운영실을 감시·통제하고 이에 대한 감사기록 기능을 갖는 장치

4. 시스템 및 네트워크의 보호설비

4-1. 이중화된 네트워크 설비
4-2. 침입차단시스템, 침입탐지시스템 등 네트워크 보안설비
4-3. 네트워크 및 시스템 관리 설비

5. 화재·수해 및 정전 등 재난 방지를 위한 설비

5-1. 화재 발생 시 이를 조기에 감지하고 진화하는 설비
    (1) 연기감지장치, 온도감지장치 등 화재경보장치
    (2) 소규모 및 대규모 화재에 대처할 수 있는 소화장치
    (3) 화재소화 장치 동작 시 다른 시스템에 악영향을 미치지 않는 소화약제
5-2. 수재 예방 설비
    (1) 대체수단의 발급·관리 설비 및 유효성 확인 설비를 물에 노출되지 않도록 바닥으로부터 이격 설치
    (2) 전원접속장치를 바닥으로부터 이격 설치 등 수재 예방장치의 설치
5-3. 정전발생 시 지속적인 본인확인업무의 수행이 가능하도록 30분 이상 전원을 공급해줄 수 있는 장치
5-4. 온도 및 습도를 일정하게 유지하기 위한 항온항습장치

[참고2-4] 본인확인기관 지정심사 세부 심사기준별 배점표

심사사항	세부 심사기준	배점(점)	비고
물리적·기술적·관리적 조치계획	본인확인업무 관련 설비의 관리 및 운영	90	**지정기준 :** ①총점 800점 이상 획득 ②중요심사항목 및 계량평가 항목 '적합' 평가 ※ 중요심사항목 및 계량평가항목 '적합' 평가를 받고 총점 800점 미만을 받은 경우 미지정 또는 조건부 지정할 수 있음
	정보통신망 침해행위의 방지	220	
	시스템 및 네트워크의 운영·보안 및 관리	160	
	이용자 보호 및 불만처리	130	
	긴급상황 및 비상상태의 대응	80	
	본인확인업무를 위한 내부규정의 수립 및 시행	50	
	대체수단의 안전성 확보**(중요심사항목)***	적합/부적합	
	접속정보의 위조·변조 방지	60	
	본인확인업무와 다른 인터넷 서비스와의 분리	60	
기술적·재정적 능력	기술적 능력**(계량평가 항목)***	적합/부적합	
	재정적 능력**(계량평가 항목)***	적합/부적합	
설비규모의 적정성	이용자 개인정보를 검증·관리 및 보호 설비	20	
	대체수단 생성·발급 및 관리 설비	20	
	출입통제 및 접근제한을 위한 보안 설비	40	
	시스템 및 네트워크의 보호설비	30	
	화재·수해 및 정전 등 재난 방지 설비	40	
합계**		1,000	

* **'적합' 판단기준**
- **(중요심사 항목)** 참석 심사위원의 2/3 이상이 '적합' 평가한 경우
- **(계량평가 항목)** 평가기준 조건을 만족한 경우

** **평가점수 산출방법**: 심사위원별 평가점수(세부 심사기준별 점수를 합산한 총점) 가운데 최고, 최저 평가점수를 제외하고, 나머지 평가점수의 평균

[참고2-5] 기술인력의 자격기준

기술인력의 자격기준

1. 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 방송통신위원회가 인정하는 자격

1-1. 전자·통신관련학과·정보처리기술관련학과 또는 암호 및 정보보호기술 관련학과 4년제 대학졸업자 또는 이와 동등 이상의 자격이 있다고 인정되는 자로서 동일 직무분야에서 3년 이상 실무에 종사한 자

1-2. 정보통신·정보처리 및 전자계산기조직응용 분야의 산업기사로서 2년 이상 실무에 종사한 자

1-3. 정보통신·정보처리 및 전자계산기조직응용 분야의 기능사로서 5년 이상 실무에 종사한 자

1-4. 정보통신·정보처리 및 전자계산기조직응용 분야의 기사수준에 해당하는 교육훈련을 실시하는 기관에서 노동부령이 정하는 교육훈련기관의 기술훈련과정을 이수한 자로서 전자·통신관련, 정보처리기술관련 또는 암호 및 정보보호기술관련 직무분야에서 3년 이상 실무에 종사한 자

1-5. 전자·통신관련학과, 정보처리기술관련학과 또는 암호 및 정보보호기술관련학과 전문대학졸업자 또는 이와 동등 이상의 학력이 있다고 인정되는 자로서 동일 직무분야에서 5년(3년제 전문대학의 경우에는 4년) 이상 실무에 종사한 자

1-6. 정보통신·정보처리 및 전자계산기조직응용 분야의 산업기사 수준에 해당하는 교육훈련을 실시하는 기관에서 노동부령이 정하는 교육훈련기관의 기술훈련 과정을 이수한 자로서 전자·통신관련, 정보처리기술관련 또는 암호 및 정보보호기술관련 직무분야에서 5년 이상 실무에 종사한 자

2. 정보보호 또는 정보통신운영·관리 분야에서 2년 이상 근무한 경력

2-1. 정보보호 운영·관리 분야
  가. 정보보호기술 분야
    (1) 암호 및 전자서명기술 분야
    (2) 컴퓨터 보안기술 분야
    (3) 네트워크 보안기술 분야
  나. 정보보호시스템 개발 및 운영·관리 분야

2-2. 정보통신 운영·관리 분야
  가. 정보통신기술 분야
  나. 정보통신시스템 개발 및 운영·관리 분야
  다. 정보통신망 구축 및 운영·관리 분야

[참고3] 본인확인기관 지정 등에 관한 기준(방통위고시) 서식

[별지 제1호서식]

<table>
<tr><td colspan="5">본인확인기관지정신청서</td><td>처리기간
3월</td></tr>
<tr><td rowspan="4">신청인</td><td>기관명(또는 명칭)</td><td colspan="2"></td><td>전화번호</td><td></td></tr>
<tr><td>대표자 성명</td><td colspan="2"></td><td>생년월일</td><td></td></tr>
<tr><td>주소(주된 사무소 소재지)</td><td colspan="4"></td></tr>
<tr><td>인터넷 홈페이지 주소</td><td colspan="4"></td></tr>
<tr><td colspan="2">사업의 종류 및 내용</td><td colspan="4"></td></tr>
<tr><td colspan="2">사업 대상 또는 지역</td><td colspan="4"></td></tr>
<tr><td colspan="2">주요장비의 개요 및 설치 장소</td><td colspan="4"></td></tr>
<tr><td colspan="6">「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3과 같은 법 시행령 제9조의4 제1항에 따라 위와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

방송통신위원회 귀하</td></tr>
<tr><td rowspan="2">구비서류</td><td colspan="2">신청인(대표자) 제출서류</td><td colspan="2">담당공무원 확인사항</td><td>수수료</td></tr>
<tr><td colspan="2">1. 조직·인력 및 설비 등의 현황을 기재한 사업계획서
2. 시행령 제9조의3 제1항에 따른 심사사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류
3. 법인의 정관 또는 단체의 규약(법인 또는 단체인 경우에만 해당한다)
4. 과거 3개년간의 재무제표(법인 또는 단체인 경우에만 해당한다)</td><td colspan="2">법인등기부등본</td><td>없음</td></tr>
<tr><td colspan="6">신청인(대표자) (서명 또는 인)</td></tr>
</table>

210mmx297mm[신문용지 54g/㎡(재활용품)]

[별지 제2호서식]

본인확인기관지정서

기 관 명 :

대 표 자 :

주 소 :

제 공 역 무 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3과 같은 법 시행령 제9조의4에 따라 위와 같이 본인확인기관으로 지정합니다.

년 월 일

방송통신위원회 인

210mmx297mm[보존용지(1종) 120g/㎡)]

[별지 제3호서식]

본인확인업무(휴지·폐지)신고서					처리기간 즉시
신고인	기관명(또는 명칭)		전화번호		
	대표자 성명		생년월일		
	주소(주된 사무소 소재지)				
휴지예정기간 또는 폐지예정일자					
휴지 또는 폐지 하고자 하는 업무					
휴지 또는 폐지의 사유					

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3과 같은 법 시행령 제9조의5 제2항에 의하여 위와 같이 신고합니다.

년 월 일

신고인 대표자 (서명 또는 인)

방송통신위원회 귀하

구비서류

1. 이용자에게 휴지·폐지 사실을 통보하였음을 확인할 수 있는 서류 1부
2. 대체수단 및 개인정보의 이용 제한 또는 파기 계획에 관한 서류 1부
3. 이용자의 보호조치 계획에 관한 서류 1부
4. 본인확인기관지정서(폐지의 경우에 한합니다)

210mm×297mm(일반용지 60g/㎡(재활용품))

[별지 제4호서식] 지정신청기관의 명세서

1. 법인명 :

2. 자본금(백만원) :

3. 최대주주 및 특수관계인의 주식소유 현황

구성주주의 성명 또는 명칭[1]	주식소유비율	유형[2]	주요업종[3]	비고[4]
계				

1) 성명 또는 명칭란에는 개인의 경우에는 성명을, 법인의 경우에는 법인의 명칭을 기입할 것.
2) 유형란에는 주식회사·유한회사·합자회사·합명회사·정부투자기관(정부소유비율 %)·정부투자기관의 출자회사(정부투자기관 소유비율 %)·정부출자기관(정부 소유비율 %)·외국법인·비영리법인·개인 등으로 구분하여 기입하고, 주식회사인 경우 상장 여부를 표시할 것.
3) 주요업종란에는 구성주주가 법인이거나 개인사업을 경영할 경우에는 한국표준산업분류(KSIC)에 의한 산업세분류 업종(외국인 구성주주의 경우 이와 유사한 분류방법에 의한 업종)을 기입하고, 2개 이상의 업종을 동시에 경영할 경우에는 매출액 비중이 가장 큰 업종을 기입할 것.
4) 비고란에는 구성주주간 독점규제및공정거래에관한법률시행령 제3조제1호 가목 내지 마목에 해당하는 관계에 있는 자(외국인 경우 표시)들을 적시할 것

[별지 제5호서식] 최근 3개년 주요 재무지표

1. 법인명 :

2. 결산기준일 :

구 분		년도	년도	년도
수익성	총자산영업이익률[1]			
안정성	부채비율[2]			
성장성·활동성	매출액(영업수익) 증가율[3]			

1) (영업이익)/[(기초자산총계+기말자산총계)/2]×100

2) (부채총계/자본총계)X100 ※ 부채총계 = 유동부채+비유동부채

3) [(당기매출액(영업수익)-전기매출액(영업수익))/전기매출액(영업수익)]×100

상기 사항이 사실과 틀림없음을 확인합니다.

년 월 일

대표자 : (인)

담당자 : (인)

[별지 제6호서식] 최근 3개년 주요 재무수치

1. 법인명 :

2. 결산일 :

(단위:백만원)

구 분			년도	년도	년도
재무상태표 항목	자산총계				
	부채총계				
	자본 총계	자본금			
		이익잉여금(결손금)			
		기타자본항목[1)]			
		계			
손익계산서 항목	영업수익(매출액)[2)]				
	영업이익(손실)				

1) 자본총계 중 자본금과 이익잉여금(결손금을)제외한 자본총계 구성항목
2) 재화의 판매 및 용역의 제공에 따른 수익액

첨부 : 1. 감사보고서중 대차대조표, 손익계산서 사본(회계감사법인의 확인필 자료)
2. 표준재무제표증명(재무제표확인원)

상기 사항이 사실과 틀림없음을 확인합니다.

년 월 일

대표자 : (인)

담당자 : (인)

[붙임] 해설서 개정의견 신청서(양식)

본인확인기관 평가기준 해설서

<table>
<tr><th colspan="3">개정 의견서</th></tr>
<tr><td rowspan="2">신청자</td><td>(소속)</td><td>(전화번호)</td></tr>
<tr><td>(이름)</td><td>(전자우편)</td></tr>
<tr><td>개정내용</td><td colspan="2">(개정부분) 00 페이지
(개정사유)</td></tr>
<tr><th colspan="2">기존</th><th>개정안</th></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

「본인확인기관 지정 등에 관한 기준」
지정·정기심사 평가기준 해설서

발 행 : 2024년 2월

인 쇄 : 2024년 2월

발행처 : **방송통신위원회**
경기도 관천시 관문로 47, 2동 (TEL : 02-500-9000)
https://www.kcc.go.kr

한국인터넷진흥원
전라남도 나주시 진흥길 9 (TEL : 1433-25)
https://www.kisa.or.kr

인쇄처 : 호정씨앤피(Tel. 02-2277-4718)