2023 한국인터넷진흥원 본인확인서비스 교육

본인확인기관 지정정기심사 1장 물리적·기술적·관리적 조치계획

대체수단의 안전성 확보에 관한 사항

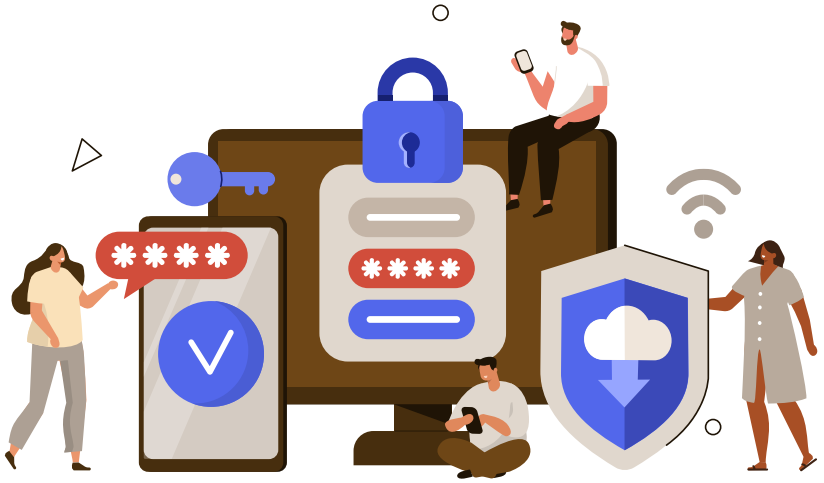
CONTENTS

CONTENTS

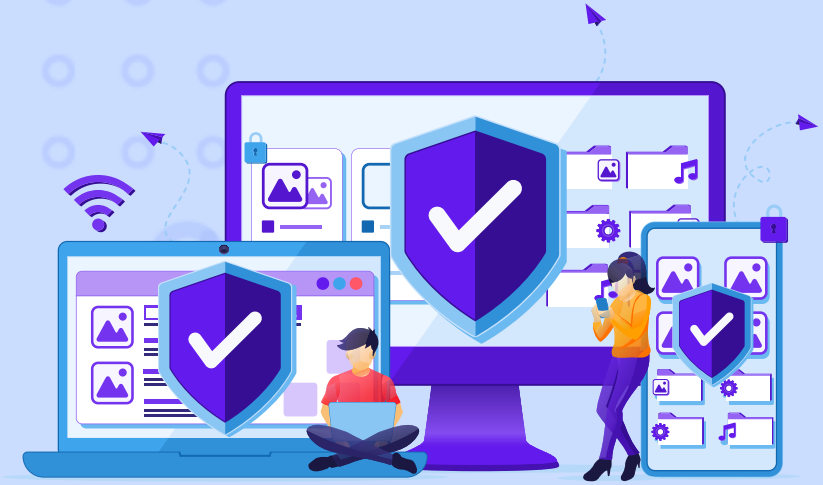
CONTENTS

CONTENTS

이용자 개인정보 암호화의 적정성 심사 기준



01 대체수단 안전성 확보에 관한 사항의 적정성 심사 기준



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

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

심사대상

- 본인확인서비스 관련 웹페이지의 웹 접근성 및 웹 표준을 준수 여부
- 대체수단 발급 시, 다른 사용자와 유일하게 구분되는 식별정보를 활용하여 발급하는 기능의 구현 여부
- 대체수단 발급 시, 발급 요청자의 신원에 대한 진위 여부를 확인 절차 운영 여부
- 부정발급, 명의도용 방지방안 및 발급 후 관리되지 않는 계정에 대한 관리방안
- 만 14세 미만의 자가 대체수단을 발급받고자 하는 경우 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원을 확인한 후 동의를 받고 있는지 여부
- 법정대리인의 실명인증에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치 여부를 검사하고 있는지 여부

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

심사영역

- 본인확인서비스 관련 웹페이지가 웹 접근성 및 웹 표준을 준수하고 있는지 심사
- 대체수단 발급 시, 다른 사용자와 유일하게 구분되는 식별정보를 활용하여 발급하는 기능이 구현되어 있는지 심사
- 대체수단 발급 시 발급 요청자의 신원에 대한 진위여부를 확인 절차를 운영하고 있는지 심사
- 부정발급, 명의도용 방지 및 발급 후 관리되지 않는 계정에 대한 관리 절차를 운영하고 있는지 심사
- 주기적으로 허무인(사망자 등) 여부를 확인하는 절차를 운영하고 있는지 심사
- 만 14세 미만의 자가 대체수단을 발급받고자 하는 경우 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원을 확인한 후 동의를 받는 절차를 운영하고 있는지 심사
- 해당 법정대리인이 만 14세 미만 미성년자의 실제 법정대리인이 맞는지 여부를 검증하는 절차를 운영하고 있는지 심사

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

증적자료

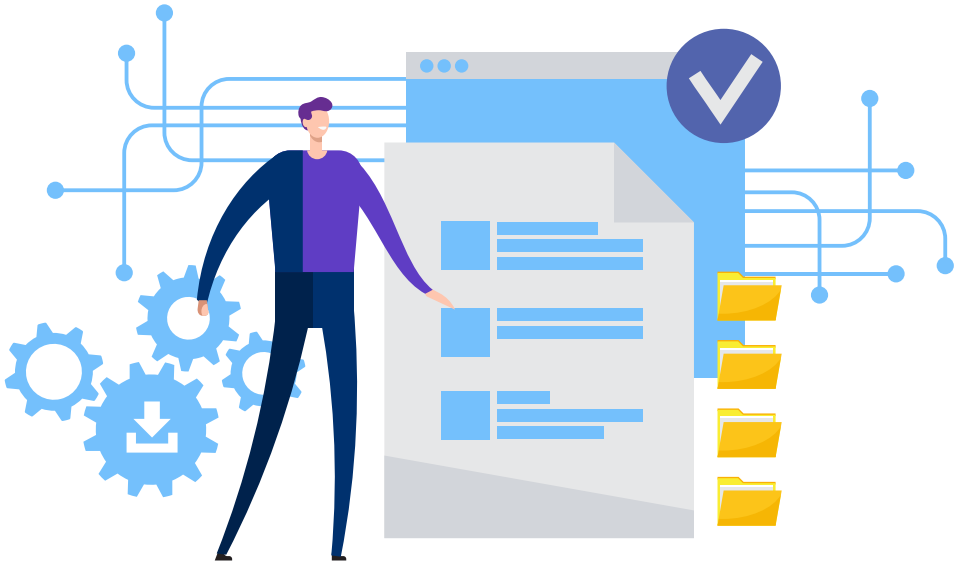
- 본인확인서비스 웹페이지에 대한 웹 접근성 및 웹 표준 적용 현황
- 본인확인서비스 이용자 표준창 제공 현황
- 웹 접근성 및 웹 표준 관련 품질인증서
- 본인확인정보 발급 현황
- 부정발급 시도 모니터링 기준 및 이행 현황
- 본인확인정보 발급 처리 흐름도
- 허무인 데이터 입수 및 검증 절차
- 발급 요청자의 실지명의 확인 과정
- 만 14세 미만의 미성년자에 대한 본인확인정보 발급 절차
- 발급 과정에서의 법정대리인 신원확인 절차
- 발급 과정에서의 법정대리인 동의 절차
- 신원확인수단을 갖지 않은 외국인에 대한 본인확인정보 발급 절차

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 본인확인서비스 개발자
- 본인확인서비스 담당자
- 개인정보 담당자



대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

인터뷰

- 본인확인서비스 웹 페이지 개발 시 준수하고 있는 웹 접근성 및 웹 표준 지침 관련 설명
- 본인확인 인증 모듈은 본인확인서비스 표준창 방식으로 제공하고 있는지 여부
- 표준창 방식이 아닌 소켓방식을 허용해주고 있는 이용기관 현황 관리 여부
- 전문기관을 통한 웹 접근성 및 웹 표준 관련 품질인증서 갱신 관리 현황
- 본인확인정보의 유일성 확보 및 이에 대한 검사 관련 설명
- 본인확인정보의 발급, 이용, 폐지 과정 관련 설명
- 신분증 진위확인 절차 관련 설명
- 허무인 정보 입수 및 후속 처리 관련 설명
- 부정 이용·발급 모니터링 체계 관련 설명
- 만 14세 미만의 자가 대체수단을 발급받고자 하는 경우 법정대리인 또는 청소년을 보호·양육·교육하거나 그 의무가 있는 자의 신원을 확인한 후 동의를 받고 있는지 여부
- 신원확인수단을 갖지 않은 외국인에 대한 본인확인정보 발급을 위해 신원확인수단을 가진 성인을 통해 본인확인정보의 발급이 가능한지 여부
- 신원보증인의 실명인증에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치성 검사 절차 관련 설명

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

현장점검

- 본인확인서비스 웹 페이지 점검
- 본인확인서비스 모바일 페이지 점검
- 웹 접근성 및 웹 표준 관련 품질인증서 유효기간 등 확인
- 본인확인서비스 관련 개발자들이 개발 시 웹 표준 및 웹 접근성을 준수하도록 교육받고 있는지
- 표준창 방식이 아닌 소켓방식 적용 이용기관 관리 현황
- 본인확인정보 발급 과정 점검
- 본인확인정보 발급 관련 소스코드 점검
- 본인확인정보 발급 시 발급 요청자에 대한 신원확인 관련 소스코드 점검
- 허무인 데이터 입수 후 후속 처리 절차 및 관련 소스코드 점검
- 부정발급 및 부정이용 탐지를 위한 FDS 운영 현황
- 만 14세 미만자에 대한 법정대리인 동의 여부 확인
- 신원보증인의 실명확인에 사용된 개인정보와 신원확인에 사용된 개인정보의 일치성 검사
- 본인확인정보의 폐지 시 법정대리인 개인정보 파기의 적절성

대체수단 안전성 확보에 관한 사항의 적정성 심사 기준

미흡사례

(1) 본인확인서비스 용 웹페이지가 웹 표준을 준수하도록 개발되지 않은 경우

(2) 본인확인서비스 이용기관이 본인확인정보를 입력하는 UI/UX를 본인확인서비스 표준창 대신 자체 제작한 UI/UX로 제공하는 문제점이 확인된 경우

(3) 허무인(사망자 등)에 대한 대체수단 발급·이용 차단 체계를 구축되지 않은 경우

(4) 휴대전화 개통 시 정상적으로 부여 받은 전화번호를 사용하는 이용 자가 본인의 본인확인인증이력을 조회하는데 이전에 해당 번호를 사용하던 고객의 본인확인 이력 정보까지 조회되는 문제점이 확인된 경우

(5) OO본인확인기관의 법정대리인을 통한 본인확인정보 발급 현황을 확인한 결과, 동일 신원보증인을 통해 10명의 만 14세 미만자의 본인확인정보가 발급된 경우

02 대체수단 변경·관리 적정성 심사 기준

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

대체수단 변경·관리 적정성 심사 기준

심사대상

- 본인확인정보의 발급 및 갱신·폐지에 대하여 이용자가 열람할 수 있는 기능을 제공하고 있는지 여부
- 본인확인정보의 발급 등의 정보를 본인확인정보 보유기간(폐기 후 5년) 종료 시 지체 없이 파기하고 있는지 여부
- 이용자가 자신의 본인확인정보를 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는지 여부
- 이용자의 권리보호를 위한 열람 권리보장 및 이용내역 통지를 이행하고 있는지 여부
- 이용자로부터 본인확인정보 등 오류에 대하여 정정을 요구받을 수 있는 기능을 제공하고 있는지 여부
- 이용자의 정정요구 절차 수립 등 이용자 권리보장체계 마련 여부
- 대체수단 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보를 이메일 또는 스마트폰 PUSH 등을 통해 이용자에게 알리고 있는지 여부

대체수단 변경·관리 적정성 심사 기준

심사영역

- 본인확인정보의 발급 및 갱신·폐지에 대하여 이용자가 열람할 수 있는 기능의 제공이 적절한지 심사
- 본인확인정보 보유기간(폐기 후 5년) 종료 시 본인확인정보의 발급·갱신 등의 정보를 지체 없이 파기하고 있는지 심사
- 이용자가 자신의 대체수단 관련 정보를 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는 기능이 적절한지 심사
- 이용자의 권리보호를 위한 열람권리 보장 및 이용내역 통지를 이행하고 있는지 심사
- 본인확인정보 등 오류에 대하여 이용자가 정정을 요구할 수 있는 기능 또는 방법이 적절한지 심사
- 이용자의 정정요구 절차 수립 등 이용자 권리보장체계를 마련하고 있는지 심사
- 대체수단 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보를 이메일 또는 스마트폰 PUSH 등을 통해 이용자에게 알리는 방법이 적절한지 심사
- 대체수단 발급, 인증, 폐지, 정보변경 시 관리절차를 심사

대체수단 변경·관리 적정성 심사 기준

증적자료

- 본인확인정보의 발급·폐지 등에 관한 기록 보관 기준 및 파기 절차
- 본인확인정보의 발급·폐지 등의 기록을 제3자 제공하고 있는 경우 제공 현황
- 본인확인서비스 인증이력 관리 현황(관리자 페이지 등)
- 개인정보처리방침
- 본인확인서비스 데이터베이스 인증이력 테이블 규격서
- 본인확인서비스 인증이력 파기 배치
- 본인확인서비스 인증 페이지
- 이용자 권리보장체계 관련 문서 증적
- 대체수단 발급, 인증, 폐지, 정보변경 시 관리 절차
- 이메일, SMS 등 발송 수단 운영 현황(UMS 등)
- 실제 발송이력 및 발송 실패 시 재발송 구현 여부
- 발송이력에 대한 보관 및 파기 관리 현황

대체수단 변경·관리 적정성 심사 기준

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 본인확인서비스 담당자
- 개인정보 담당자
- 본인확인서비스 개발자

인터뷰

- 본인확인 인증이력 조회 페이지 기능 구현 현황 설명
- 본인확인정보의 발급·이용·폐지 등에 관한 기록 보관 기준 및 파기 방법 설명
- 이용자 및 이용자의 법정대리인이 이용자 개인정보에 대한 열람 등을 요구할 수 있는 방법 또는 절차를 제공하는지 여부

대체수단 변경·관리 적정성 심사 기준

- 본인확인 이외 목적으로 이용자의 개인정보를 이용하는 서비스가 존재하는지 설명
- 이용자가 자신의 대체수단 관련 정보를 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는 방법이나 수단 제공에 관한 사항 설명
- 본인확인서비스 이용내역(일시, 이용기관 등)에 대한 보관 및 파기 관련 설명
- 이용자의 개인정보 이용내역 통지 관련 사항 설명
- 이용자 및 이용자의 법정대리인이 이용자의 개인정보에 오류가 있는 경우 정정·삭제를 요구할 수 있는 방법 및 절차에 관한 설명
- 이용자의 개인정보에 대한 오류 정정 요구가 접수된 경우 해당 오류를 정정할 때까지 해당 이용자의 개인정보 이용 및 제공 중단 관련 설명
- 이용자의 정정요구 절차 수립 등 이용자 권리보장체계 관련 설명
- 대체수단 신규 발급, 인증, 폐지, 정보변경 시 이용자에게 알리고 있는지 여부
- 대체수단 발급, 인증, 폐지, 정보변경 시 관리 절차 설명
- 발송 이력에 대한 보관 및 파기 관리 현황 설명

대체수단 변경·관리 적정성 심사 기준

현장점검

- 대체수단 발급·갱신·폐지 내역 조회시스템 확인
- 개인정보에 대한 열람을 요구받은 경우 기간 내 열람을 가능하도록 처리하고, 열람할 수 없는 정당한 사유가 있을 때에는 열람 요구자에게 그 사유를 알리고 있는지 여부 확인
- 관리자 페이지 등에서 이용자의 인증이력을 조회할 수 있는 인원을 최소한으로 통제하고 있는지 여부
- 본인확인서비스 데이터베이스 상의 인증이력 테이블 규격 확인
- 개인정보처리방침 확인
- 본인확인 이외의 목적으로 이용하거나 제3자에게 제공된 내역을 이용자가 열람할 수 있는 기능이 제공되고 있는지 확인
- 본인확인서비스 인증 페이지 시연
- 이용자의 정정요구 절차 수립 등 이용자 권리보장체계 점검
- 대체수단 발급, 폐지, 인증, 이메일 정보 수정 시 확인정보를 발송하는지 시연
- 발송이력에 대한 보관 기간 및 UMS로 통합 발송관리 되는 경우 본인확인업무코드로 발송내역 분류 가능한지 확인

대체수단 변경·관리 적정성 심사 기준

미흡사례

(1) 이용자가 자신의 대체수단 발급·갱신·폐기 등의 정보를 조회할 수 있는 기능을 제공하여야 하나 인증이력 조회 기능만 제공하고 대체수단 발급·갱신·폐기 등의 정보는 열람 기능을 제공하지 않은 문제점이 확인된 경우

(2) 본인확인 이외의 목적으로 이용하거나 제3자에게 제공한 내역을 열람할 수 있는 기능을 구현하지 않은 문제점이 확인된 경우

(3) OO본인확인기관에서 인증이력 정보를 확인한 결과, 동일 정보통신서비스제공자(CP)에 대해서 제공사 명칭이 상이하게 표시되는 문제점이 확인된 경우

대체수단 변경·관리 적정성 심사 기준

미흡사례

(4) 개인정보의 정정요구를 한 지 10일이 넘게 경과하여도 해당 오류 정정 요청 건이 처리되지 아니하고 결과도 회신 되지 않은 문제점이 확인된 경우

(5) 대체수단의 신규 발급, 인증 및 폐지, 이메일 정보 수정 시 확인정보를 발송하지 않는 문제점이 확인된 경우

03 대체수단 관련 정보의 저장 및 백업의 적정성 심사 기준

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

대체수단 관련 정보의 저장 및 백업의 적정성 심사 기준

심사대상

- 이용자의 대체수단 이용내역 등에 대한 이력관리의 적정성
- 대체수단이 폐지된 날로부터 5년 경과 후 이용자 등록정보 삭제처리
- 대체수단 신청 및 폐지에 대한 기록, 신원확인 시 제출서류, 제시한 증명서 사본, 정보통신망을 통해 입력한 정보 등에 대한 백업기능

심사영역

- 이용자에게 인증이력정보를 조회할 수 있는 기능을 제공하고 해당 이용내역을 2년 경과 후 파기하고 있는지 심사
- 대체수단 발급 관련 이용자 등록정보는 대체수단 폐지일로부터 5년 보관 후 파기하고 있는지 심사
- 대체수단 신청·폐지기록, 정보통신망을 통해 입력한 정보 등을 백업하는 기능을 마련하고 있는지 심사

대체수단 관련 정보의 저장 및 백업의 적정성 심사 기준

증적자료

- 본인확인서비스 이용자 인증이력, 등록정보 저장 및 파기 기준
- 인증이력 조회 페이지 기능 구현 현황(조회 UI/UX스크린샷 등)
- 대체수단 이용내역에 대한 파기 배치(배치 스크립트 등)
- 대체수단 폐지일로 부터 5년 경과 후 이용자 등록정보 파기 배치(배치 스크립트 등)
- 전사 또는 본인확인서비스 정보시스템 대상 백업 정책
- 본인확인서비스에 대한 백업 대상, 백업실행주기, 백업보관주기 등 관련 자료
- 통합 백업솔루션(관리콘솔 스크린샷 등)
- 오프라인 서류 등 비정형 개인정보 파일에 대한 관리 절차 관련 자료

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 본인확인서비스 개발자
- 파기배치 담당자
- 개인정보 담당자
- 백업 담당자

대체수단 관련 정보의 저장 및 백업의 적정성 심사 기준

인터뷰

- 본인확인서비스 이용자 인증이력정보의 저장·이용·파기 등 관리 현황 설명
- 본인확인서비스 관련 이용자 등록정보의 보관 기준 및 파기 방법 설명
- 대체수단의 발급 및 갱신·폐지 등에 대한 기록 관련 설명
- 본인확인서비스의 백업 대상 식별 관련 현황 설명
- 백업 자동화 관리 현황 설명
- 이용자 제출서류 등 비정형 개인정보에 대한 보관 및 백업 현황 설명

현장점검

- 인증이력 및 이용자 등록정보 파기 배치 스크립트 내 파기 로직
- 본인확인서비스 데이터베이스 확인(인증이력 테이블, 이용자 등록정보 테이블 검색 등)
- 본인확인서비스 관련 백업 대상이 정확히 식별되었는지 확인(누락된 백업대상은 없는지 등)
- 본인확인서비스 백업 대상이 정해진 스케줄대로 백업 수행되고 있는지 여부
- 이용자 제출서류 등 비정형 개인정보에 대한 보관 방법의 적정성

대체수단 관련 정보의 저장 및 백업의 적정성 심사 기준

미흡사례

(1) 이용자의 대체수단 폐지 이후 5년이 도래하였음에도 이용자 등록정보를 삭제하지 않은 문제점이 확인된 경우

(2) 대체수단 발급 신청 시 접수 받은 서류에 대한 관리 기준이 수립되지 않아 사무실 공용공간에 서류를 보관하고 있는 문제점이 확인된 경우

04 대체수단 폐지의 적정성 심사 기준

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

대체수단 폐지의 적정성 심사 기준

심사대상

- 이용자가 대체수단 폐지 요청 시 본인확인기관이 이용자의 권한을 확인하는 절차의 적정성
- 이용자의 대체수단 폐지 요청 후 대체수단 폐지 사실에 대한 통지의 적절성

심사영역

- 이용자가 대체수단 폐지 요청 시 본인확인기관이 이용자의 권한을 확인하는 방법이 적절한지 심사
- 대체수단 폐지 시 이메일 또는 SMS 등으로 해당 사실을 이용자에게 통지하는 기능이 적절한지 심사

대체수단 폐지의 적정성 심사 기준

증적자료

- 대체수단 폐지 절차
- 대체수단 폐지 요청에 대한 정당한 권한 소유 여부 확인 방법
- 대체수단 이용내역에 대한 파기 배치(배치 스크립트 등)
- 대체수단 폐지일로부터 5년 경과 후 이용자 등록정보 파기 배치(배치 스크립트 등)
- 대체수단 폐지 시 폐지사실에 대한 이용자 통지 절차
- 대체수단 폐지 사실 통지수단 운영 현황
- 대체수단 폐지 및 폐지 사실 통지 이력 자료

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 본인확인서비스 담당자
- 본인확인서비스 개발자

대체수단 폐지의 적정성 심사 기준

인터뷰

- 대체수단 폐지 절차 및 흐름 설명
- 대체수단 폐지 신청 시 이용자의 정당한 권한 확인 방법에 대한 설명
- 대면 확인으로 대체수단을 폐지하는 방법 제공 여부
- 비대면 확인으로 대체수단을 폐지하는 방법 제공 여부
- 대체수단 폐지 시 이메일 또는 SMS 등으로 해당 사실을 통지하고 있는지 여부
- 대체수단 폐지 사실 통지 수단 운영 및 구현 관련 설명

현장점검

- 대체수단 폐지 요청에 대한 정당한 권한 소유 여부 확인 절차
- 본인확인기관이 정한 이용자 식별방법 구현의 적절성 확인(소스코드 등 확인)
- 본인확인서비스 데이터베이스 확인(대체수단 폐지 관련 테이블 확인 등)
- 대체수단 폐지 이력과 대체수단 폐지 사실 통지 이력 비교
- 대체수단 폐지 시연을 통한 통지 여부 확인
- 통지 처리 오류 발생 시 재시도(동일 또는 다른 통지수단 활용 등) 구현

대체수단 폐지의 적정성 심사 기준

미흡사례

(1) 이용자가 대체수단 폐지 신청 시 본인의 정당한 신청인지 확인하는 절차를 운영하고 있지 않은 문제점이 확인된 경우

(2) 이용자가 대체수단을 폐지해도 폐지사실에 대한 통지가 이용자에게 전달되지 않는 문제점이 확인된 경우

05 대체수단 연동의 적정성 심사 기준

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

대체수단 연동의 적정성 심사 기준

심사대상

- 본인확인 입력정보를 이용한 본인확인인증이 정상적으로 처리되고 있는지 여부
- 본인확인 입력정보를 안전하게 보호하기 위한 보호수단을 제공하고 있는지 여부
- 본인확인인증 시 정보통신서비스제공자에게 전달되는 형식에 이름, 생년월일, 성별 등 본인확인결과 정보를 제공하는 기능이 정상적으로 구현되어 있는지 여부
- 연계정보를 필요로 하는 사업자가 대체수단 도입 사이트에 연계정보를 요청하였을 때 본인확인기관과 대체수단 도입 사이트 간 연동 기능이 정상적으로 동작하고 있는지 여부
- 주민등록번호, 본인확인기관 간 공유 비밀정보 등을 이용하여 중복가입확인정보(DI)를 제공하는 기능이 정상적으로 동작하고 있는지 여부
- 주민등록번호, 본인확인기관 간 공유 비밀번호 등을 이용하여 연계정보를 제공하는 기능이 정상적으로 구현되어 있는지 여부

대체수단 연동의 적정성 심사 기준

심사영역

- 본인확인서비스 이용절차 대로 입력한 정보를 이용한 본인확인인증이 정상적으로 이뤄지고 있는지 심사합니다.
- 본인확인 입력정보를 안전하게 보호하기 위한 수단을 제공하고 있는지 심사
- 이용자가 본인확인 수행 시 정보통신서비스제공자에게 본인확인결과정보(이름, 생년월일, 내·외국인정보 등)가 제공될 수 있도록 인터페이스에 연동되어 있는지 심사
- 본인확인서비스 이용 계약을 통해 반드시 필요한 경우에만 연계정보(CI)를 제공하도록 운영하고 있는지 심사
- 이용자가 본인확인 수행 시 정보통신서비스제공자에게 중복가입확인정보(DI)를 제공하는 기능이 정상적으로 작동하고 있는지 심사
- 중복가입확인정보(DI) 생성 시 사용되고 있는 CP Code에 대한 유일성 관리가 수행되고 있는지 심사
- 이용자가 본인확인 수행 시 정보통신서비스제공자에게 연계정보(CI)를 제공하는 기능이 정상적으로 작동하고 있는지 심사
- 연계정보(CI)를 직접 생성하지 않은 본인확인기관의 경우 연계정보의 획득방법이 적정한지 심사
- 연계정보(CI)에 대한 저장관리가 적정한지 심사

대체수단 연동의 적정성 심사 기준

증적자료

- 본인확인 입력정보 화면(WEB, APP)
- 본인확인서비스 시퀀스 다이어그램 및 개인정보흐름도
- 본인확인서비스 관련 인터페이스 전문 목록 및 규격서
- 본인확인서비스 관리자 페이지 URL
- 본인확인서비스 관련 DBMS 상세 ERD, 테이블 목록
- 본인확인서비스 인터페이스 연동 통신로그

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 본인확인서비스 담당자
- 본인확인서비스 개발자
- 대·내외연동 운영자

대체수단 연동의 적정성 심사 기준

인터뷰

- 본인확인 입력정보 오류 발생 시 대처 방안 및 절차 관련 설명
- WEB, APP에 도입된 소프트웨어 보안 모듈 현황(루팅 방지 및 난독화 솔루션 포함)
- 인터페이스 전문 관련 설명
- 정보통신서비스제공자별 본인확인서비스 계약 관리 현황 설명
- 본인확인서비스 관리자 페이지 주요 기능 관련 설명
- 중복가입확인정보(DI) 생성 기능 구현 관련 설명
- 본인확인서비스 관리자 페이지를 통한 CP Code 관리 현황 설명
- 본인확인서비스 대외 인터페이스 현황 및 관련 소스코드 설명
- 연계정보(CI) 값의 저장 여부
- 본인확인서비스 계약 상 연계정보(CI) 제공이 승인된 이용기관에게만 연계정보가 제공되는지 여부

대체수단 연동의 적정성 심사 기준

현장점검

- 본인확인정보 입력 오류 발생 시 예외사항 처리 로직 점검
- WEB, APP에 도입된 소프트웨어 보안 모듈 메모리 상주 및 정상 작동 여부 점검
- 본인확인정보 변경절차 및 이력 관리 점검
- 본인확인서비스 관련 인터페이스 전문규격 및 적용 현황 점검
- 본인확인서비스 관련 인터페이스 목록 점검
- 본인확인서비스 관련 DBMS ERD, 테이블 목록 점검
- 본인확인서비스 도입 계약 시 연계정보(CI) 제공 관련 절차 및 관리현황 점검
- 본인확인결과정보 제공 시 최소한의 개인정보만을 제공하고 있는지
- 중복가입확인정보 제공 관련 구현 부분 소스코드 점검
- 본인확인서비스 관련 인터페이스 파라미터 점검
- 본인확인서비스 계약 시 CP Code 생성 및 관리 현황 점검
- 본인확인서비스 관련 대·내외 통신 로그 점검
- 본인확인설비 내 연계정보(CI)를 저장하고 있는지 여부

대체수단 연동의 적정성 심사 기준

미흡사례

(1) 본인확인 입력정보 오류 발생에 대한 예외처리 루틴이 없어 빈번히 오류가 발생하는 경우

(2) 본인확인 입력정보에 대하여 가상키보드 보안, 바이러스 체크, 루팅 방지 및 난독화, 개인정보의 암호화 등이 전혀 제공되지 않는 문제점이 확인된 경우

(3) 정보통신서비스제공자와의 계약과는 별개로 기본 값으로 연계정보(CI) 값을 제공하는 경우

(4) 본인확인결과정보 제공 시 전문규격에 정의된 이름, 생년월일, 성별 외에 주소나 연락처 정보도 제공하는 문제점이 확인된 경우

대체수단 연동의 적정성 심사 기준

미흡사례

(5) 동일한 정보통신서비스제공자에게 제공되는 중복가입확인정보(DI)값이 요청 시점 및 조건에 따라 다른 값이 제공되도록 잘못 구현된 경우

(6) 정보통신서비스제공자와의 계약 내 연계정보(CI)제공에 대한 승인 내역이 없음에도 연계정보(CI)를 임의 제공하는 경우

(7) 본인확인인증이 완료된 이후에 명확한 법적 근거 없이 이용자의 연계정보(CI)를 24시간 이상 저장하고 있는 문제점이 확인된 경우

06 본인확인서비스 연계 시 보호조치의 적정성 심사 기준

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

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

심사대상

- 정보통신서비스 제공자에 배포한 비밀 키에 대한 주기적 갱신 현황
- 본인확인서비스 관련 정보시스템(서버, DB, 네트워크 장비 등)에 대한 접근통제 운영 현황
- 본인확인서비스 관련 소프트웨어의 형상관리 및 변경통제를 통하여 소스 코드 변경 시 승인절차를 거치고 사후에 감사추적이 가능하도록 이력로그를 저장·관리하고 있는지
- 암호알고리즘 등을 통해 중복가입정보(DI) 및 연계정보(CI)를 암호화하여 안전하게 전송하고 있는지 여부
- 전송된 정보의 위·변조 여부를 검증할 수 있는 무결성 체크 로직을 구현하였는지 여부
- 전송구간 암호화 방식에 대한 안전성을 확보하고 있는지 여부
- 이용자가 대체수단 신규발급 시 본인확인기관에 제공한 정보에 대하여 해쉬체인을 구성하고 있는지 여부

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

심사영역

- 대칭키 암호방식을 이용하는 경우 정보통신서비스 제공자에 배포한 비밀키를 주기적으로 갱신하고 있는지 심사
- 본인확인서비스 관련 정보시스템에 대한 접근은 권한 보유자만이 접근할 수 있도록 접근통제를 적절하게 적용하고 있는지 심사
- 본인확인서비스 관련 소프트웨어의 형상관리 및 변경통제가 적절히 수행되고 있는지 심사
- 암호알고리즘 등을 통해 중복가입정보(DI) 및 연계정보(CI)를 암호화하여 안전하게 전송하고 있는지 심사
- 전송된 정보의 위·변조 여부를 검증할 수 있는 무결성 체크 로직을 구현하였는지 심사
- 전송구간 암호화 방식에 대한 안전성을 확보하고 있는지 심사
- 이용자가 대체수단 신규발급 시 본인확인기관에 제공한 정보에 대하여 해쉬체인을 구성하고 있는지 여부를 심사

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

증적자료

- 본인확인서비스 관련 암호 정책, 지침 등 문서
- 정보통신서비스 제공자와 암호키 갱신 관련 증적문서
- 본인확인서비스 관련 정보시스템에 대한 접근통제정책 적용 현황
- 본인확인서비스 관련 소스 코드 점검 및 배포 승인 프로세스(CI/CD 파이프라인 전체)
- 본인확인서비스 관련 내부·외부 URI 리스트
- SSL 인증서 관련 Config(WEB서버, L4 스위치 등)
- OpenSSL 패치 증적
- 전문 통신 규격에서 반영된 암호화 적용 및 메시지 무결성 체크 관련 자료
- 대외 서비스의 경우 TLS1.2 미만 버전의 이용자 접속 현황 통계 자료
- 본인확인서비스 이용자 개인정보에 대한 HASH 처리현황
- 이용자가 제공한 정보의 위·변조 여부 등에 대한 무결성 검증 관련 자료

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 암호키 담당자
- 접근통제 도구 운영자
- 배포 담당자
- 개인정보 담당자

인터뷰

- 정보통신서비스 제공자에 배포한 비밀키에 대한 주기적 갱신 현황 관련 설명
- 본인확인서비스 관련 정보시스템(서버, DB, 네트워크 장비 등)에 대한 접근통제도구 운영 관련 설명
- 형상아이템(소스코드, 개발문서 등)에 대한 형상관리 및 소프트웨어 변경통제 절차 관련 설명
- 네트워크를 통한 본인확인 관련 정보 전송 시 보호조치 관련(암호화 등) 설명
- 전송된 정보의 위·변조 여부를 검증할 수 있는 무결성 체크 절차 운영 관련 설명
- 취약한 통신 프로토콜이나 암호 알고리즘이 사용되지 않도록 정기 점검 수행 관련 설명
- 이용자가 본인확인정보 신규 발급 시 제공한 개인정보를 HASH 처리하여 보관하는 기능 사용 여부
- 이용자 개인정보에 대한 위·변조 여부 검증 절차(해쉬체인, 타임스탬프저장 등) 관련 설명

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

현장점검

- 본인확인서비스 암호키 생성, 이용, 갱신 현황 점검
- 정보통신서비스 제공자와 암호키 갱신 이행 여부
- 암호키 관리 솔루션 관리콘솔
- 정보시스템 접근통제 도구 내 등록 장비 확인 및 접근통제 우회 방지 구현 확인
- 본인확인서비스에 대한 CI/CD 파이프라인 확인(소스코드 생산부터 최종 배포단계까지)
- 본인확인서비스에 사용되는 TLS 통신채널 점검(버전, 허용 프로토콜, Cipher suit 등)
- OpenSSL 패치 이력 점검
- 전송된 정보의 위·변조 여부를 검증할 수 있는 무결성 체크 로직 구현부 확인
- 인증서 설치 Config(웹서버 또는 L4 스위치 등)
- 본인확인서비스 데이터베이스에서 이용자 개인정보에 대한 HASH 처리 현황
- HASH 처리된 테이블에 대한 접근통제 및 무결성 로직 점검

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

미흡사례

(1) 본인확인서비스 관련 정보시스템에 대한 접근통제를 시행하고 있으나 접근통제정책 적용이 누락된 운영계 서버들이 확인된 경우

(2) 본인확인서비스 관련 소프트웨어의 최종 배포 시 승인절차 없이 배포하는 문제점이 확인된 경우

(3) 본인확인서비스 관련 서비스에 보안상 취약한 TLS1.0, TLS1.1 버전의 사용을 허용하고 있는 경우

본인확인서비스 연계 시 보호조치의 적정성 심사 기준

미흡사례

(4) 본인확인서비스 관련 대외 사이트가 구성상의 오류로 인하여 HTTP로 접속이 허용되는 문제점이 확인된 경우

(5) 본인확인서비스 관련 이용자 개인정보에 대한 무결성 검증 절차(해쉬체인, 타임스탬프DB저장, 관리적 방법 등)가 전혀 구현되어 있지 않은 경우

07 이용자 개인정보 암호화의 적정성 심사 기준

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

이용자 개인정보 암호화의 적정성 심사 기준

심사대상

- 본인확인서비스 관련 비밀번호 저장 시 양방향이 아닌 일방향 암호 알고리즘을 채택하고 있는지 여부
- 안전한 일방향 암호 알고리즘을 채택하고 있는지 여부
- 암호화 대상이나 암호화 조치가 누락된 정보가 있는지 여부
- 주민등록번호를 암호화하고 있는지 여부
- 주민등록번호 암호화 조치 시 안전한 암호 알고리즘을 채택하고 있는지 여부
- 암호키 관리 현황
- 복호화 함수 호출에 대한 통제 현황
- 본인확인서비스 관련 암호키의 생성, 이용, 보관, 배포, 파기를 위한 관리절차의 수립 여부
- 본인확인서비스 참여 기관 간 암호키 갱신 절차 및 이행 여부 확인
- 암호키 관리 절차에 따라 안전하게 암호키를 관리·운영하고 있는지 여부
- 암호키에 대한 접근통제 및 모니터링 현황

이용자 개인정보 암호화의 적정성 심사 기준

심사영역

- 본인확인서비스 대상 암호 정책이 적절하게 수립되었는지 심사
- 본인확인서비스 관련 비밀번호에 대한 암호화 조치 적용이 적절한지 심사
- 암호화 조치 시 안전한 일방향 암호 알고리즘을 채택하였는지 심사
- 본인확인서비스 대상 암호 정책이 적절하게 수립되었는지 심사
- 이용자 주민등록번호에 대한 암호화 조치 적용이 적절한지 심사
- 암호화 키 관리, 복호화 함수 호출 권한 통제 등이 적절한지 심사
- 본인확인서비스 관련 암호키의 생성, 이용, 보관, 배포, 파기를 위한 관리절차가 적절하게 수립되었는지 심사
- 본인확인서비스 참여 기관 간 암호키 변경(키교환 절차, 주기 등)이 적절한지 심사
- 암호키 관리절차에 따라 암호키가 적절히 통제되고 모니터링 되고 있는지 심사

이용자 개인정보 암호화의 적정성 심사 기준

증적자료

- 본인확인서비스 관련 암호 정책, 지침 등 문서
- 본인확인서비스 관련 이용자 비밀번호 암호화 적용 부분 소스코드 및 암호화 라이브러리
- 암호키 관리 절차 및 암호키 관리 솔루션 운영 현황
- 주민등록번호에 대한 복호화 조회 가능 인력 리스트
- 주민등록번호 인터페이스 현황 및 관련 소스 코드
- 본인확인서비스 참여 기관 간 암호키 갱신 현황 확인용 증적
- 암호키에 대한 접근통제 적용 현황

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 정보보호 담당자
- 본인확인서비스 개발자
- 암호키 담당자

이용자 개인정보 암호화의 적정성 심사 기준

인터뷰

- 본인확인서비스 관련 응용프로그램별 일방향 암호 알고리즘 적용 대상 설명
- 암호정책에 따라 현재 적용 중인 암호 알고리즘 및 암호화 방법 설명
- 암호화 조치를 위한 별도의 솔루션이 도입된 경우 암호화 적용 방식 등 설명
- 일방향 암호화 적용 시 솔트(Salt)를 사용하는 경우 솔트(Salt) 생성 로직 설명
- 본인확인업무 중 주민등록번호 사용 업무 관련 설명
- 암호정책 및 암호키 생성, 이용, 파기 등 관련 설명
- 암호화된 주민등록번호에 대한 복호화 및 표시제한 조치 적용(마스킹 등) 현황 설명
- 본인확인서비스 참여기관 간 주기적인 암호키 갱신 현황 설명
- 암호키에 대한 접근통제 및 모니터링 현황
- 암호키에 대한 소산 백업 현황

이용자 개인정보 암호화의 적정성 심사 기준

현장점검

- 본인확인서비스 관련 응용프로그램별 이용자 패스워드 저장 소스코드 점검
- 암호화된 비밀번호 저장 테이블 점검
- 조직의 암호정책 상 일방향 암호화 대상이나 암호화 조치가 누락된 경우가 없는지 확인
- 본인확인서비스 관련 데이터베이스 내 주민등록번호 컬럼 점검
- TDE 암호화 적용 시 주민등록번호에 대한 추가적인 보호 조치(표시제한 조치 등)
- 암호키 관리 솔루션 점검
- 복호화 함수 호출 권한 부여 현황
- 본인확인서비스 암호키 생성 및 이용 현황 점검
- 본인확인서비스 관련 참여기관 간 1년에 1회 이상 암호키 갱신 이행 여부
- 암호키를 소스 코드 또는 구성파일 내 하드코드 형태로 이용하는 경우 존재 여부

이용자 개인정보 암호화의 적정성 심사 기준

미흡사례

(1) 본인확인서비스 관련 안드로이드 APP에서 이용자 PIN 6자리를 일방향 암호화가 아닌 양방향 암호화 방식을 사용하는 문제점이 확인된 경우

(2) 본인확인서비스 이용자 비밀번호에 대한 암호화 조치 시 다수 취약점이 보고되어 사용이 불가한 MD5 알고리즘을 사용한 문제점이 확인된 경우

(3) 본인확인서비스 관련 이용자의 주민등록번호를 암호화하여 저장하고 있으나 암호키가 소스 코드 내에 하드 코드 형태로 존재하는 문제점이 확인된 경우

이용자 개인정보 암호화의 적정성 심사 기준

미흡사례

(4) 본인확인서비스 관련 이용자의 주민등록번호를 암호화하여 저장하고 있으나 안전하지 않은 암호 알고리즘을 사용한 문제점이 확인된 경우

(5) 본인확인서비스 관련 이용자의 개인정보를 암호화하여 저장하고 있으나 운영계 시스템과 개발계 시스템이 동일한 암호키를 사용하고 있는 문제점이 확인된 경우

(6) 본인확인서비스 관련 참여기관 간 1년에 1회 이상 암호키를 갱신하지 않고 지속적으로 사용하는 문제점이 확인된 경우