2023 한국인터넷진흥원 본인확인서비스 교육

본인확인기관 지정정기심사 1장 물리적·기술적·관리적 조치계획

본인확인기관 사후관리 절차 정기점검

(모의침투, 취약점진단, 현장실사, 이행점검)

CONTENTS

01 본인확인기관 정기점검의 절차

본인확인기관 정기점검의 절차

「본인확인기관 지정 등에 관한 기준」 제13조(사후관리)에 따라 본인확인서비스의 안전성 및 이용 편의성 제고를 위해 본인확인기관별 연 1회 적합성 심사, 즉 정기점검을 실시합니다.

정기점검 단계에서는 모의침투, 취약점진단, 현장실사 및 이행점검을 실시합니다.

모의침투 및 시스템 취약점 진단 수행사를 지정한 후 개인정보보호, 관리체계 보안 등 외부 전문가를 구성하여 본인확인기관과 유관기관에 대한 정기점검을 실시하고 있습니다.

본인확인서비스용 인증 앱과 인증 모듈에 대한 모의침투 및 시스템 취약점 점검 과정을 실시하고, ARS 대행사와 중계운영사 등을 대상으로 한 현장실사를 실시하며, 아이핀/휴대폰/인증서/카드 기반 본인확인기관 등을 대상으로 현장실사와 이행점검을 실시하는 등 본인확인기관에 대한 사후관리 절차로 정기점검을 진행합니다.

02 정기심사 진행 시 세부 점검방법

정기심사 진행 시 세부 점검방법

① 인증앱과 인증 모듈에 대한 모의침투 과정입니다.

테스트베드를 구축한 후 인증앱과 인증 모듈에 대한 모의침투 과정을 진행해서 신청기관에서
안드로이드 및 아이폰 모바일 앱 마켓에 업로드 한 최신 인증앱을 대상으로 모의침투 과정을 진행하며,

인증대행사/CP 사 등에서 사용하는 최신 인증모듈을 대상으로도 모의침투 과정을 진행하여 보안 취약성을 탐지하고
이에 대한 조치 여부를 정기적으로 점검합니다.

② 취약점 진단 과정입니다.

서버, DB, 네트워크 및 정보보호 시스템 등 본인확인서비스 주요 시스템을 대상으로 보안 취약점을 정기적으로
진단하고 발견된 보안 취약점에 대한 조치 여부를 정기적으로 점검합니다.

③ 본인확인기관에 대한 적합성 평가 현장실사 과정입니다.

적합성 심사 평가 기준인 87개 통제항목에 따라 아이폰/휴대폰/인증서/카드 기반 본인확인기관에 대해서
매번 정기적으로 현장실사를 진행하고 있습니다.

03 인증앱과 인증모듈에 대한 모의침투, 취약점 진단 과정

인증앱과 인증모듈에 대한 모의침투, 취약점 진단 과정

① 인증대행사가 배포하는 본인확인서비스 인증모듈에 대한 모의침투 과정 진행 절차입니다.

① 인증모듈 현황 파악을 위한 시스템 현황표 작성
② 본인확인서비스 인증모듈 목록 제출
③ 테스트베드 구축 후 모의침투 수행
④ 현장방문 시 결과 리뷰

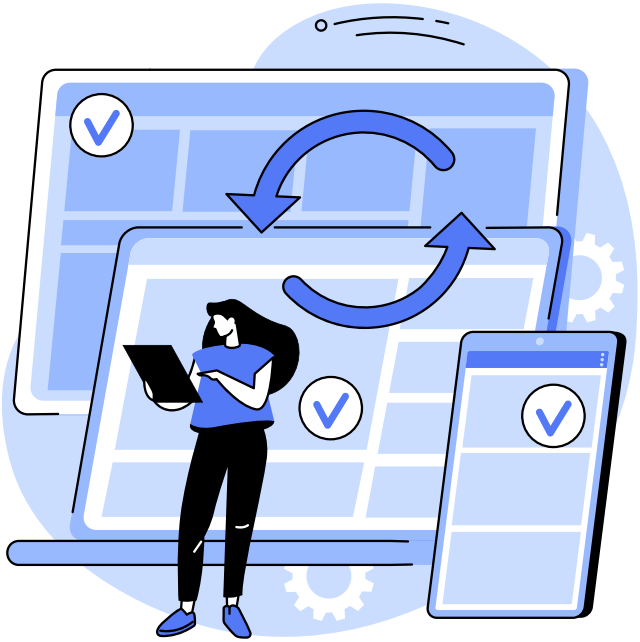
② 간편인증용 모바일 앱에 대한 모의침투 과정 진행 절차입니다.

① 모바일앱 현황 파악을 위한 시스템 현황표 작성
② 앱 마켓에서 최신버전 앱을 다운로드 후 모의침투 수행
③ 현장방문 시 결과 리뷰

인증앱과 인증모듈에 대한 모의침투, 취약점 진단 과정

③ 시스템 취약점 점검 진행 절차입니다.

① 취약점 진단 대상 파악을 위한 시스템 현황표 작성 및 회신
② 취약점 진단 대상 선정
③ 스크립트 전달 및 실행 결과 회신
④ 현장방문 인터뷰(현장실사 전 수행)
⑤ 현장실사 시 결과 리뷰



04 본인확인기관에 대한 현장실사

본인확인기관에 대한 현장실사

현장실사에서는 87개 적합성 심사 평가사항별 적합성을 평가하며, 각각의 심사사항에 대한 적합성 평가 기준의 유형과 판단기준은 아래와 같습니다.

적합

신청기관의 본인확인업무가 심사사항 별 세부 심사기준에 규정된 요구사항을 충족하는 경우

보완

본인확인기관 지정기준 및 세부 심사기준의 위반 사실 및 정도가 경미하여 즉시 시정할 수 있는 경우, 고의 또는 중대한 과실이 아닌 사소한 부주의나 단순한 오류로 인한 경우

부적합

본인확인기관 지정기준 및 세부 심사기준에 부합하지 않으며, 다수의 이용자가 대체수단을 이용하는데 중대한 지장을 초래할 것으로 인정되는 경우

본인확인기관에 대한 현장실사

① 신청기관의 본인확인업무가 심사사항별 세부 심사기준에 규정된 요구사항을 충족하는 경우 적합으로 판단.

② 본인확인기관 지정기준 및 세부 심사기준의 위반 사실 및 정도가 경미하여 즉시 시정할 수 있는 경우, 또는 사소한 부주의나 단순한 오류로 인한 경우로 판단되는 경우 보완사항으로 판단.

③ 본인확인기관 지정기준 및 세부 심사기준에 부합하기 않으며, 다수의 이용자가 대체수단을 이용하는데 중대한 지장을 초래할 것으로 인정되는 경우에는 부적합으로 판단.

본인확인기관에 대한 현장실사

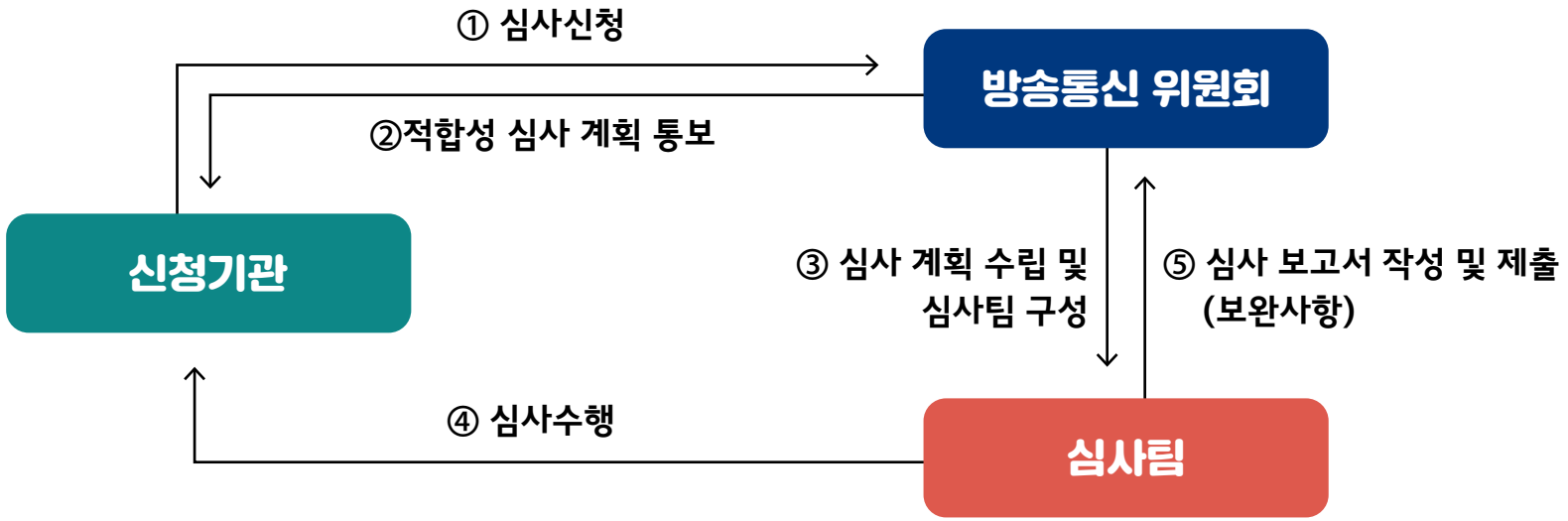
만일, 부적합한 사항이 발견된 경우, 해당사항의 경중에 따라 경고, 업무중지, 지정취소 등의 행정처분이 내려지거나 또는 후속조치를 안내해 드립니다.

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

05 본인확인기관 사후심사

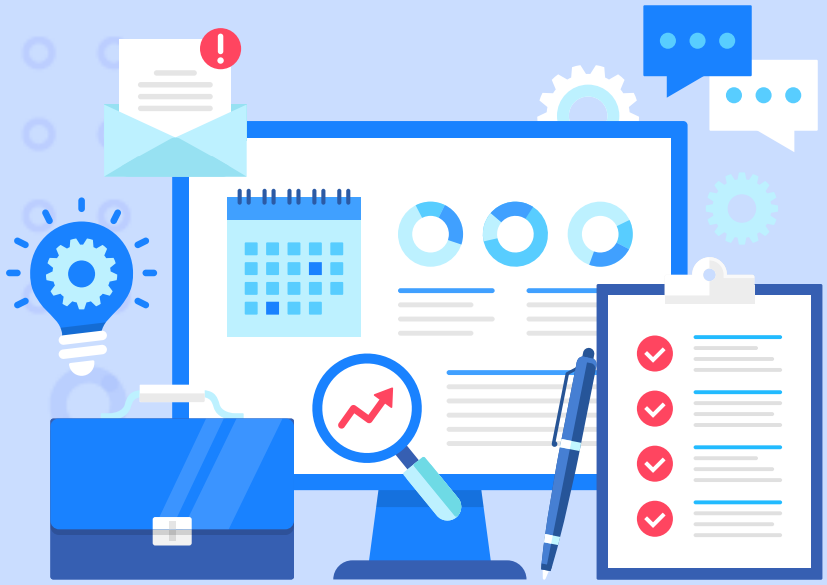
본인확인기관 사후심사

본인확인기관 사후관리 정기점검 적합성 심사 절차 흐름도



① 신청기관이 방송통신위원회에 본인확인기관 적합성 심사를 신청
② 방송통신위원회에서 신청기관에 적합성 심사 계획 통보
③ 방송통신위원회는 심사 계획을 수립하며 심사팀 구성
④ 심사팀은 신청기관에 대한 본인확인기관 적합성 심사를 실시
⑤ 심사팀은 현장실사 후 도출된 보완사항을 중심으로 심사보고서를 작성하여 방송통신위원회에 제출

06 적합성 심사 일정



적합성 심사 일정

기관별 적합성 심사 시 현장실사는 총 5일간 진행됩니다.

단계	일자	시간	주요 내용
착수회의	1일자	11시	• 기관 현황 소개(임직원 참석)
기관현황		13시 30분~17시	• 심사대상 문서 접수 및 검토 • 대체수단 발급, 본인확인 서비스 소개 • 본인확인 DB연동, NW 구성도 등 소개 • 기술인력 및 재정 심사(회계사)
서면심사 및 현장실사	2~4일자	10시~17시	• 현장실사/검증, 관련자 면담 • Server/NW/DB/AP OS 및 로그, 정책 점검 등 서면/ 현장실사
종료회의	5일자	11시	• CISO,CPO 등 임원급 참석 • 심사 결과 총평

1일차는 오전에 착수회의를 진행하고, 오후에는 심사대상 문서를 접수/검토한 후 대체수단 발급과 본인확인서비스, 본인확인DB와 네트워크 구성도 등을 중심으로 기관 현황을 파악합니다.

적합성 심사 일정

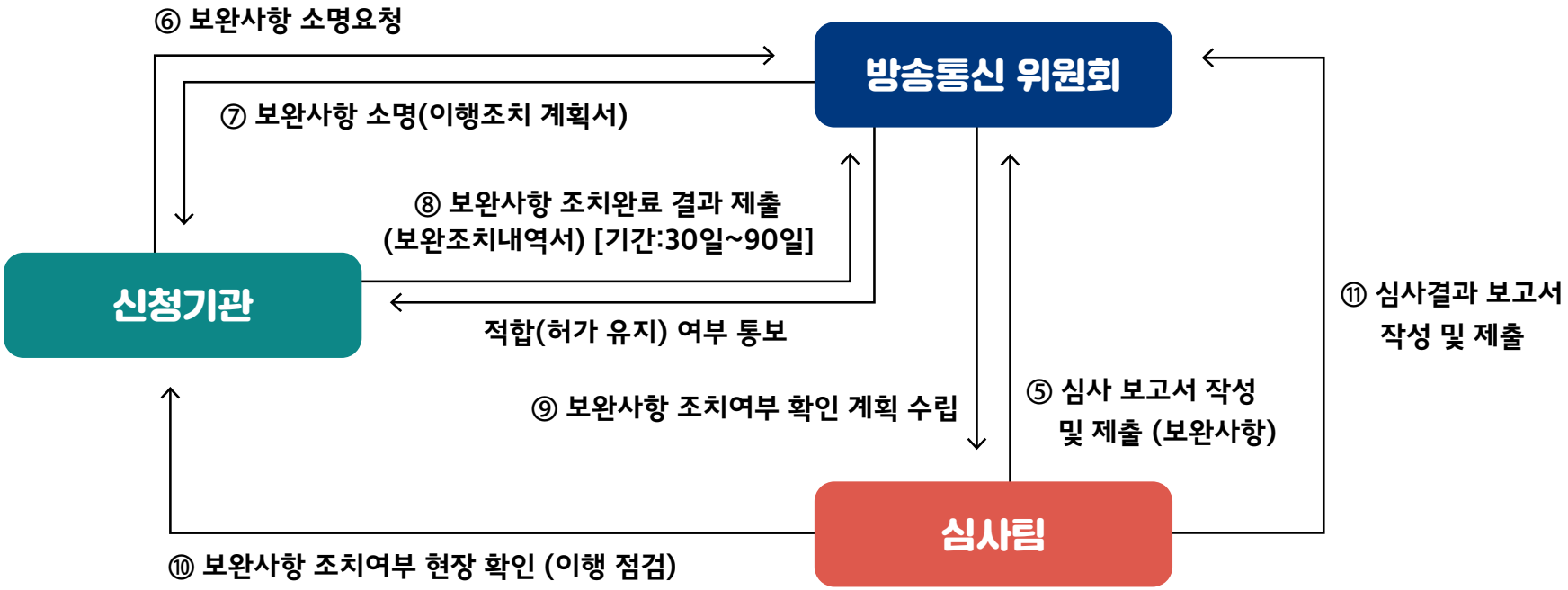
2일차부터 4일차는 서면실사와 현장실사를 진행합니다. 본인확인서비스 담당자 인터뷰를 진행하여 서버, 네트워크, DB, OS 및 로그, 정책 등에 대한 현장실사를 진행합니다.

마지막 5일차는 87개 통제항목에 대한 적합성 심사 결과를 총평 합니다. 종료회의를 통해 현장실사를 마무리합니다.

07 현장실사 이후 진행되는 일정

현장실사 이후 진행되는 일정

현장실사 심사팀이 구성되어 5일간 신청기관에 대한 적합성 심사 진행 후 방송통신위원회에 보완사항을 중심으로 심사 보고서를 제출 후에 진행되는 일정입니다.



⑥ 방송통신위원회는 신청기관에 현장실사에서 도출된 보완사항에 대해 소명을 요청

⑦ 신청기관은 방송통신위원회에 '이행조치계획서'를 제출 후, 보완사항에 대해 이행조치 계획을 수립

현장실사 이후 진행되는 일정

⑧ 30일 이내, 또는 조치 기간 60일 연장할 경우 최장 90일 이내에 도출된 보완사항에 대해 조치를 완료 후 이를 보완조치내역서에 작성하여 방송통신위원회에 제출

⑨ 방송통신위원회는 보완사항 조치여부 확인 계획을 수립한 후 다시 심사팀을 구성

⑩ 심사팀은 신청기관을 다시 방문하여 보완사항에 대한 조치여부를 현장에서 확인하는 '이행점검' 과정을 수행

⑪ 이행점검 종료 후에 심사팀은 심사결과보고서를 작성하여 이를 방송통신위원회에 제출

⑫ 최종적으로 방송통신위원회는 신청기관에 적합 또는 허가 유지 여부를 통보하는 순서로 적합성 심사가 진행

08 정기점검 후 본인확인업무의 정지 및 지정취소 등에 관한 행정처분의 내용과 기준

정기점검 후 본인확인업무의 정지 및 지정취소 등에 관한 행정처분의 내용과 기준

위반행위	근거법조문	위반 횟수별 처분기준		
		1차	2차	3차 이상
가. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우	법 제23조의4제1항제1호	지정취소		
나. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 않은 경우	법 제23조의4제1항제2호	지정취소		
다. 지정받은 날부터 6개월 이내에 본인확인 업무를 개시하지 않거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우	법 제23조의4제1항제3호	업무정지 3개월	지정취소	
라. 법 제23조의3제4항에 따른 지정기준에 적합하지 않게 된 경우	법 제23조의4제1항제4호	지정취소	업무정지 3개월	업무정지 6개월

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제9조의 7 제1항을 통해 본인확인 업무의 정지 및 지정취소 등에 관한 행정처분 기준이 제시되어 있습니다.

정기점검 후 본인확인업무의 정지 및 지정취소 등에 관한 행정처분의 내용과 기준

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제9조의 7 제1항을 통해 본인확인업무의 정지 및 지정취소 등에 관한 행정처분 기준이 제시되어 있습니다.

거짓이나 그 밖의 부정한 방법으로 본인확인기관을 지정 받은 경우, 또는 본인확인업무의 정지명령을 받은 자가 그 명령을 위한하여 업무를 정지하지 않은 경우, 정보통신망법 제23조의4 제1항 제1호 및 제2호에 따라 지정 취소될 수 있으며,

지정 받은 날로부터 6개월 이내에 본인확인업무를 개시하지 않거나 6개월 이상 계속하여 본인확인 업무를 휴지한 경우에는 1차로 업무정지 3개월, 2차 위반 시 지정 취소될 수 있습니다.

정보통신망법 제23조의3제4항에 따른 지정기준에 적법하지 않게 된 경우, 1차 위반 시 경고, 2차 위반 시 업무정지 3개월, 3차 위반 시 업무정지 6개월에 처해질 수 있습니다.

정기점검 후 본인확인업무의 정지 및 지정취소 등에 관한 행정처분의 내용과 기준

행정처분 기준에 대한 설명

위반행위가 둘 이상인 경우로서 그에 해당하는 각각의 처분기준이 다른 경우에는, 그 중 무거운 처분기준에 따르며, 다만, 둘 이상의 처분기준 중 경고가 포함되어 있는 경우에는 경고를 함께 부과할 수 있고, 둘 이상의 처분기준이 모두 업무정지인 경우에는 각 처분기준을 합산한 기간을 넘지 않는 범위에서 무거운 처분기준의 2분의 1의 범위에서 가중할 수 있습니다.

위반행위의 횟수에 따른 행정처분기준은 최근 1년간 같은 위반행위로 행정처분을 받은 경우에 적용하게 됩니다. 이 경우 위반행위에 대하여 행정처분을 받은 날과 다시 같은 위반행위로 적발된 날을 각각 기준으로 하여 위반횟수를 계산하게 됩니다.

다만, 처분권자는 다음 각 목에 해당하는 사유를 고려하여 처분을 감경(법 제23조의4제1항제1호 및 제2호에 해당하는 경우는 제외한다)할 수 있습니다. 이 경우 그 처분이 업무정지인 경우에는 그 처분기준의 2분의 1의 범위에서 감경할 수 있고, 지정취소인 경우에는 6개월의 업무정지로 감경할 수 있습니다.

09 본인확인업무 휴지/폐지 절차

본인확인업무 휴지/폐지 절차

본인확인기관 사후관리 : 행정처분 기준 - 행정처분 감경 사유

1) 위반행위가 고의나 중대한 과실이 아닌 사소한 부주의나 단순한 오류로 인한 것으로 인정되는 경우
2) 위반의 내용 · 정도가 경미하여 즉시 시정할 수 있다고 인정되는 경우
3) 업무정지 또는 지정취소 처분으로 다수의 이용자가 대체수단을 이용하는 데 중대한 지장을 초래할 것으로 인정되는 경우

본인확인업무 휴지/폐지 절차

본인확인기관 지정 후 여러 사유로 인해 본인확인기관 운영을 중단하거나 업무를 폐지할 경우 정보통신망법 제23조의3 제3항에 따라 본인확인기관이 본인확인업무를 폐지하고자 하는 때에 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고, 방송통신위원회에 신고하도록 규정하고 있습니다.

서비스 중단 통보 (신청기관→이용자)	신청서 제출 (신청기관→방통위)	신청서 검토 (방통위, KISA →신청기관)	본인확인기관 업무폐지
D-60	D-60	D-60	D-DAY

정보통신망법 시행령 제9조의6에 따라 본인확인기관은 폐지의 사유, 폐지의 일시와 대체수단 및 개인정보의 파기에 관한 사항을 이용자에게 통보하도록 정하고 있습니다.

본인확인업무의 폐지할 경우 본인확인업무 폐지 신고서에 다음 각 호의 서류를 첨부하여 방송통신위원회에 제출하도록 정하고 있습니다.

본인확인업무 휴지/폐지 절차

본인확인업무 폐지 신고서 및 첨부 자료

1. 제1항 각 호의 사항을 기재한 통보 서류
2. 대체수단 및 개인정보의 파기 계획에 관한 서류
3. 이용자의 보호조치 계획에 관한 서류
4. 본인확인기관지정서