2023 한국인터넷진흥원 본인확인서비스 교육

본인확인기관 지정정기심사 1장 물리적·기술적·관리적 조치계획

긴급상황 및 비상상태의 대응에 관한 사항 적정성 심사 기준

CONTENTS

CONTENTS

01 비상계획 및 재난복구절차의 적정성 심사 기준

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

비상계획 및 재난복구절차의 적정성 심사 기준

심사대상

- 본인확인서비스가 포함된 업무 연속성 계획(BCP)의 적정성
- 본인확인서비스에 대한 IT재해복구 체계의 적정성
- 본인확인서비스에 대한 적절한 복구 목표시간(RTO) 및 복구 목표시점(RPO) 수립 여부
- 본인확인서비스에 대한 IT재해복구 훈련 시행 여부

심사영역

- 본인확인서비스가 포함된 업무 연속성 계획(BCP) 및 IT재해복구 체계가 적절하게 구축되었는지 심사
- 본인확인서비스에 대한 복구 목표시간(RTO) 및 복구 목표시점(RPO)이 적절한지 심사
- 업무 연속성 계획(BCP) 및 IT재해복구 정책에 따라 재해복구 모의훈련을 수행하고 개선사항을 도출하는지 심사

비상계획 및 재난복구절차의 적정성 심사 기준

증적자료

- 본인확인서비스가 반영된 업무 연속성 계획(BCP)
- IT재해복구 관련 정책 및 지침
- 복구 목표시간(RTO) 및 복구 목표시점(RPO) 산정 근거
- IT재해복구 시 비상 대응 조직도 및 비상 연락망 현황
- 본인확인서비스 관련 정보시스템 정기점검 보고서(월간 보고서 등)
- IT재해복구 모의훈련 계획서 및 시행 결과 보고서

현장실사(증적자료 확인과 담당자 인터뷰, 개인정보처리방침 점검을 통해 진행)

대상 담당자

- 업무 연속성 계획 담당자
- IT재해복구 담당자

비상계획 및 재난복구절차의 적정성 심사 기준

인터뷰

- 본인확인서비스가 포함된 업무 연속성 계획(BCP) 관련 설명
- 본인확인서비스에 대한 서비스 운영 수준(고가용성 구성, DR 구축 등) 설명
- 복구 목표시간(RTO), 복구 목표시점(RPO) 산정 근거 관련 설명
- 본인확인 관련 정보시스템에 대한 월간 정기점검 현황 설명
- IT재해복구 모의훈련 시행 계획 및 결과 관련 설명

현장점검

- 본인확인서비스 핵심 설비의 고가용성 구성 및 DR운영 현황
- 복구 우선순위에 부합되게 가용성 확보조치가 적용되었는지 여부
- 복구 목표시간(RTO), 복구 목표시점(RPO)의 달성 가능성 검증
- 본인확인 정보시스템에 대한 백업 스케줄 및 수행 결과 현황

비상계획 및 재난복구절차의 적정성 심사 기준

미흡사례

(1) 업무 연속성 계획 또는 IT재해복구 지침 등에 본인확인서비스에 대한 복구 목표시간(RTO), 복구 목표시점(RPO)을 산정하지 않은 문제점이 확인된 경우

(2) 본인확인서비스 대상 데이터베이스의 백업정책이 조직에서 정의한 복구 목표시점(RPO)를 달성할 수 없는 상태로 운영되고 있는 문제점이 확인된 경우

02 백업 및 복구계획의 적정성 심사 기준

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

백업 및 복구계획의 적정성 심사 기준

심사대상

- 본인확인서비스 관련 운영데이터, 소프트웨어, 정보시스템 등에 대한 백업 및 복구 계획 수립의 적절성
- 본인확인서비스 관련 백업대상, 백업주기, 백업방법 등의 적절성
- 본인확인서비스 관련 정보시스템 복구 테스트 시나리오 및 수행 결과
- 재난에 대비하여 백업 매체를 소산하는 등의 추가적인 보안대책 마련 여부

심사영역

- 본인확인서비스 관련 운영데이터, 소프트웨어, 정보시스템 등에 대한 백업 및 복구정책이 적절하게 수립되었는지 심사
- 본인확인서비스 관련 백업 절차의 적절성 및 복구 테스트 결과가 조직의 복구 목표시간(RTO) 및 복구 목표시점(RPO)에 부합하는지 심사
- 재난에 대비하여 백업 매체를 소산하는 등의 추가적인 보안대책을 마련하고 있는지 심사

백업 및 복구계획의 적정성 심사 기준

증적자료

- 본인확인서비스 관련 백업 및 복구 정책, 지침, 절차 문서
- 본인확인서비스에 대한 복구 목표시간(RTO), 복구 목표시점(RPO) 정의 자료본인확인서비스 관련 복구 테스트 작업 계획서 및 결과 보고서
- 소산 백업 운영 현황 및 미디어 보관 장소 확인(현장 사진 등)
- (통합)백업도구에 반영된 실제 백업 스케줄 현황표(또는 스크린샷)

현장실사(증적자료 확인과 담당자 인터뷰, 개인정보처리방침 점검을 통해 진행)

대상 담당자

- 백업 담당자
- IT재해복구 담당자

백업 및 복구계획의 적정성 심사 기준

인터뷰

- 본인확인서비스 관련 백업 및 복구계획 관련 내용 설명
- 복구 목표시간(RTO), 복구 목표시점(RPO) 산정 근거 관련 설명
- 최근 수행된 복구 테스트 시나리오 및 결과 관련 설명
- 백업도구 운영 및 유지보수 관련 설명
- 백업 매체 소산 등 추가적인 보안대책 관련 설명

현장점검

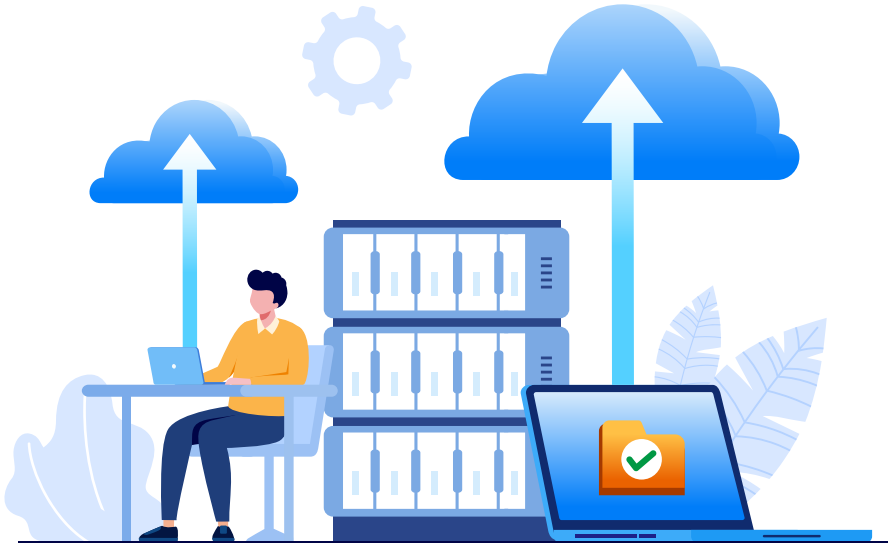
- 백업(운영체제, 데이터베이스, 파일시스템)을 수행하는 백업솔루션에 적용된 백업 정책 현황
- 최근 복구 테스트 결과가 조직의 복구 목표시간(RTO), 복구 목표시점(RPO)에 부합하는지 여부
- 소산 백업 운영 현황 및 미디어 보관 장소 확인(현장 사진 등)

백업 및 복구계획의 적정성 심사 기준

미흡사례

(1) 본인확인서비스 관련 백업 대상, 백업 주기, 백업 절차, 복구 절차 등이 포함된 백업 관련 정책 및 지침이 수립되지 않은 문제점이 확인된 경우

(2) 백업정책에 따라 백업은 수행되고 있으나 복구정책에 근거하여 정기적으로 수행되어야 할 복구 테스트를 수년간 수행하지 않은 문제점이 확인된 경우



03 연계정보 비상대응의 적정성 심사 기준

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

연계정보 비상대응의 적정성 심사 기준

심사대상

- 본인확인 연계정보(CI)에 대한 정당한 생성 절차 수립 여부
- 본인확인 연계정보(CI) 생성을 위한 소스코드와 비밀정보에 대한 안전한 관리 및 접근통제 수행 여부
- 본인확인 연계정보 생성 알고리즘에 입력되는 한국인터넷진흥원과 공유하는 비밀정보에 대한 안전한 암호화 수행 여부
- 본인확인 연계정보 생성이 가능한 SW모듈을 외부환경으로 반출 시 안전한 방법 및 정보보호최고책임자의 승인 하에 수행되는지 여부
- 인터페이스 전문 규격에 본인확인 연계정보 CI_1 필드 외에 CI_2 필드도 반영하고 있는지 여부
- 연계정보(CI) 생성 알고리즘에 사용되는 KEY 노출 시 대응 절차 수립 여부

연계정보 비상대응의 적정성 심사 기준

심사영역

(1) 연계정보 처리절차가 적절한지 심사

- 본인확인 연계정보(CI)에 대한 정당한 생성 절차 수립 · 운영 여부

(2) 연계정보 생성 알고리즘 관리 절차가 적절한지 심사

- 본인확인 연계정보(CI) 생성을 위한 소스코드와 비밀정보에 대한 안전한 관리 및 접근통제 수행 여부
- 본인확인 연계정보 생성 알고리즘에 입력되는 한국인터넷진흥원(KISA)과 공유하는 비밀정보에 대한 안전한 암호화수행 여부
- 본인확인 연계정보 생성이 가능한 SW모듈을 외부환경으로 반출 시 안전한 방법 및 정보보호최고책임자의 승인 하에 수행되는지 여부

(3) 연계정보 생성 비상대응 절차가 적절한지 심사

- 인터페이스 전문 규격에 본인확인 연계정보 CI_1 필드 외에 CI_2 필드도 반영하고 있는지 여부
- 연계정보(CI) 생성 알고리즘에 사용되는 KEY 노출 시 대응 절차 수립 여부

연계정보 비상대응의 적정성 심사 기준

증적자료

- 본인확인 연계정보 생성모듈에 대한 보안관리 기준
- 본인확인 연계정보 생성모듈 접근통제 정책
- 본인확인 연계정보 생성 SW 모듈 반출 및 승인 이력
- 본인확인 연계정보 생성 알고리즘 및 KEY 보안관리 현황
- 연계정보 제공 관련 전체 인터페이스 전문 규격서
- 연계정보 생성 암호키 노출 시 대응 절차서 및 훈련 시나리오

현장실사(증적자료 확인과 담당자 인터뷰, 개인정보처리방침 점검을 통해 진행)

대상 담당자

- 대·내외 인터페이스 담당자
- 암호키 담당자
- 본인확인서비스 개발자

연계정보 비상대응의 적정성 심사 기준

인터뷰

- 인터페이스 전문 적용 현황 및 인터페이스별 로깅 수준 설정 관련 설명
- 전문 통신 로그에 대한 파기 정책 적용 및 백업 관련 설명
- 암호키에 대한 보호대책 관련 설명(접근통제 정책 등)
- 연계정보 생성, 제공 관련 로직 구현부 소스코드에 대한 설명
- 암호키 노출에 따른 비상 대응 훈련 시나리오(조직구성, 책임과 역할 등) 관련 설명

현장점검

- 본인확인 연계정보 생성 모듈 소스코드 점검
- 인터페이스 전문 통신 시 실제 반영된 규격 점검
- 전문통신에 따른 통신 로깅(File로그, DB로그) 점검
- 본인확인 연계정보 생성 모듈에 사용된 암호화 알고리즘 확인
- 본인확인 연계정보 생성 SW 모듈 반출 대장 및 승인 현황

연계정보 비상대응의 적정성 심사 기준

미흡사례

(1) 본인확인 연계정보(CI) 생성 알고리즘에 사용되는 KEY 노출 시 비상 대응 절차를 수립하여야 하나 이에 대한 대응 절차를 수립하지 않은 문제점이 확인된 경우

(2) 암호키 노출 등 비상 상황에 대비하여 CI_2 필드로 전환할 수 있도록 준비하여야 하나 구)버전의 인터페이스 전문을 사용하고 있어 이에 대한 대비가 되어 있지 않은 문제점이 확인된 경우

04 회선장애대응의 적정성 심사 기준

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

회선장애대응의 적정성 심사 기준

심사대상

- 본인확인서비스에 대한 네트워크 모니터링 및 장애대응 체계 관련 현황
- 네트워크 회선 이중화 구성 관련 현황
- 본인확인서비스 응용프로그램 수준에서의 Fail-Over 기능 구현 여부

심사영역

- 본인확인서비스 네트워크에 대한 모니터링 및 장애 대응 정책이 적절하게 수립되었는지 심사
- 본인확인서비스 네트워크의 회선 이중화 구성이 적절한지 심사
- 본인확인서비스 응용프로그램 수준에서의 Fail-Over 기능 구현이 적절한지 심사

증적자료

- 본인확인서비스 전체 네트워크 구성도
- 본인확인서비스 네트워크 장비 Config 파일
- 본인확인서비스 네트워크 모니터링 현황 및 장애처리 보고서
- 본인확인서비스 Fail-Over 기능 구현부(소스코드 등)

회선장애대응의 적정성 심사 기준

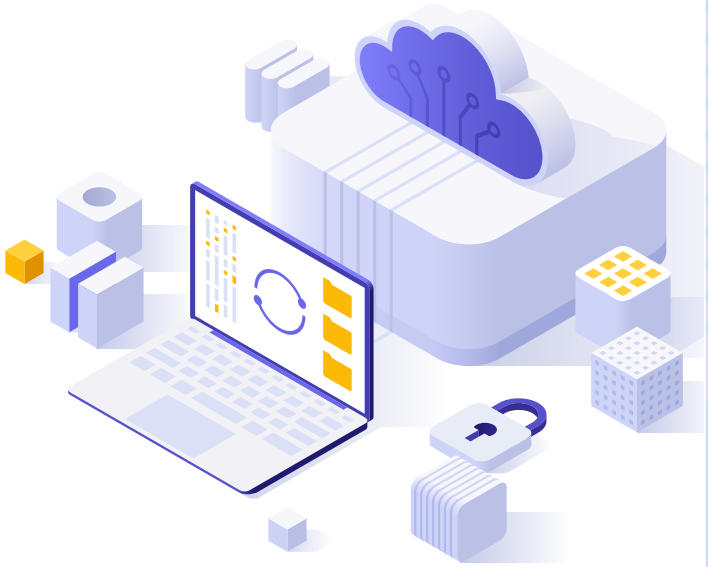
현장실사(증적자료 확인과 담당자 인터뷰, 개인정보처리방침 점검을 통해 진행)

대상 담당자

- 네트워크 담당자
- 본인확인서비스 개발자

인터뷰

- 네트워크 구성 및 운영 전반 관련 내용 설명
- 네트워크 장애 대응 모니터링 및 장애조치 현황 설명
- 본인확인서비스 회선 이중화 구성 관련 설명
- 본인확인서비스 응용프로그램 수준에서 Fail-Over 구현 로직 관련 설명



회선장애대응의 적정성 심사 기준

현장점검

- 본인확인서비스 관련 네트워크 장비(L4/L3스위치, 라우터 등) Config 점검
- 물리회선 이중화 및 관련 장비 구성 현황
- 네트워크 구성도와 실제 구현된 네트워크 아키텍처 일치 여부 확인
- 본인확인서비스 Fail-Over 기능 구현부(소스코드 등) 점검
- 네트워크 장비 접근통제 및 유지보수 현황 확인
- 본인확인서비스 네트워크 모니터링 및 장애처리 현황

미흡사례

(1) 본인확인서비스 회선을 이중화 하지 아니하고 단일 ISP의 회선만으로 서비스를 제공하는 문제점이 확인된 경우

(2) 본인확인서비스 네트워크는 이중화 구성이 되어 있었지만 주 네트워크 장애 발생 시
본인확인서비스 응용프로그램이 정상적으로 Fail-Over 동작을 하지 않아 본인확인 업무가 일시적으로
중단되는 문제점이 확인된 경우