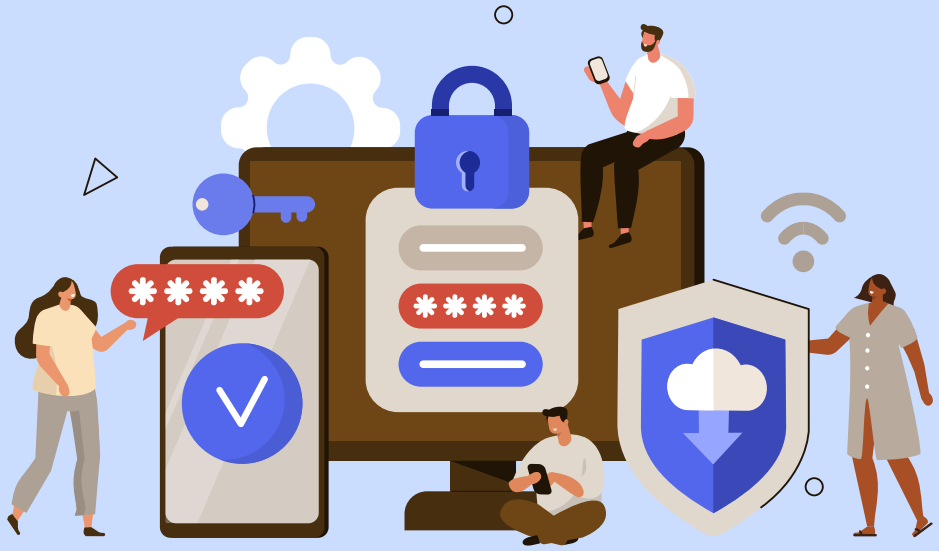
2023 한국인터넷진흥원 본인확인서비스 교육

본인확인기관 지정정기심사 1장 물리적·기술적·관리적 조치계획

정보통신망 침해행위의 방지에 관한 사항과 시스템 및 네트워크의 운영·보안·관리에 관한 사항



CONTENTS

정보통신망 침해행위 방지 사항의 적정성 심사 기준

(1) 심사대상
(2) 심사영역
(3) 증적자료
(4) 현장실사
(5) 인터뷰 및 현장점검
(6) 미흡사례

시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

(1) 심사 대상
(2) 심사 영역
(3) 증적자료
(4) 현장실사
(5) 미흡사례

01 정보통신망 침해행위 방지 사항의 적정성 심사 기준

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

정보통신망 침해행위 방지 사항의 적정성 심사 기준

정보통신망 침해행위 방지에 관한 사항의 적정성을 심사하는 기준은
개인정보 보호법의 구체적 고시인 '개인정보의 안전성 확보조치 기준' 중 제6조 접근통제와
밀접한 관련이 있습니다.

심사대상

- 침입차단(방화벽/웹 방화벽 등)·탐지(IDS)·방지(IPS/DDoS 등)
- 시스템시스템 접근 통제
- 저장정보의 조작·파괴·은닉 및 유출방지

정보통신망 침해행위 방지 사항의 적정성 심사 기준

심사영역

- 침입차단시스템인 방화벽 등을 통하여 외부의 불법적인 침해행위를 방지하기 위한 보안정책 및 보안솔루션에 대한 설정을 심사
- 서버를 비롯한 정보시스템 접속 시 접근통제 원칙과 운영을 확인하고, 개인정보취급자 등에 대하여 최소한의 권한 부여 여부와 적절한 접근통제를 수행하는 지 심사
- 내부의 안전한 보안을 보증하기 위하여 서버 및 단말기에 대한 백신 소프트웨어 설치 여부 및 최신 패턴을 주기적으로 업데이트하여 바이러스를 탐지하는 지 심사
- 외부 및 내부에서 발생하는 보안이벤트 현황과 본인확인 관련 주요 정보의 변조 및 삭제를 방지위한 모든 행위에 대한 모니터링 여부와 이를 로그형태로 저장하는 통합로그 시스템을 심사

정보통신망 침해행위 방지 사항의 적정성 심사 기준

증적자료

- 방화벽 등이 포함된 최신 네트워크 구성도
- 방화벽, 웹 방화벽, IPS, IDS, DDoS 방지 솔루션 등에 대한 자산목록 및 최신 패치 업데이트 일자
- 방화벽의 INBound /OUTBound 룰 설정 / 최신 취약점 진단 자료
- 서버 및 시스템 접근통제 원칙 / 보안시스템 root 권한자 목록
- 서버 To 서버 접근통제 현황 및 예외 사항 처리 프로세스
- 백신 소프트웨어 설치 현황 및 패턴 업데이트 정책
- 통합로그저장 시스템에 연동되는 보안솔루션 항목, 로그 보존 연한, 주기적 검토 이력

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 보안솔루션을 아웃소싱 외주위탁에 맡길 경우
- 기관 보안담당자 이외에 방화벽을 비롯한 네트워크 기반 보안솔루션 운영자
- 서버 접근통제 솔루션 운영자(서버 운영자) 및 백신소프트웨어, 통합로그 관리 운영자 등

정보통신망 침해행위 방지 사항의 적정성 심사 기준

인터뷰 및 현장점검

- 본인확인서비스와 관련된 방화벽 보안 정책
- 본인확인서비스 수행 시 보안솔루션 측면에서 트래픽 흐름 설명
- 서버 및 시스템 접근통제 원칙 및 예외 사항에 대한 별도 대책
- 백신 소프트웨어 운영현황 및 패턴 업데이트 방법
- 통합로그시스템으로 전송되는 보안솔루션 목록과 구체적 연동 로그

해당자료 및 설명을 요청하고 담당자 인터뷰 진행 후, 요청 받은 자료와 지침을 근거로 실제 현장점검을 수행합니다.

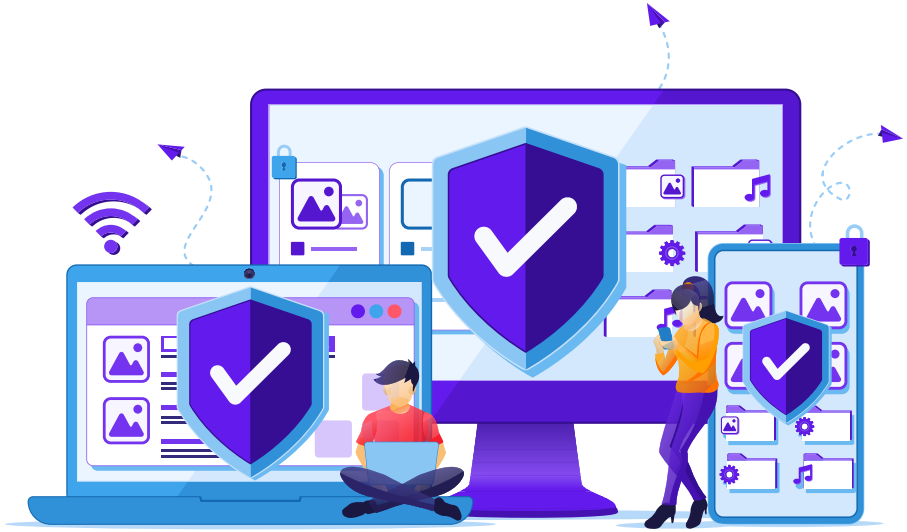
해당 영역은 개인정보 보호법 하위고시인 '개인정보의 안전성 확보조치 기준' 중 제6조 접근통제 영역에 해당되는 영역으로 개인정보 보호법에 제시한 필수 문서인 '개인정보 내부관리 계획' 지침 안에 해당 영역의 모든 내용이 반드시 포함되어 있어야 합니다.

정보통신망 침해행위 방지 사항의 적정성 심사 기준

미흡사례

(1) **방화벽 설정 관련**: 외부의 불법적인 침입을 막기 위한 방화벽 정책 중 일부가 1년이 지나도록 한 번도 사용한 적이 없는 정책이 삭제되지 않고 지속적으로 유지되는 경우

(2) **서버 접근 통제 영역**: 정보시스템 서버 접속 시에는 반드시 서버 접근통제 솔루션을 사용하지만, 서버 To 서버에 대한 접근통제 원칙이 없거나 적용하지 않을 경우



02 시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

(1) 심사대상
(2) 심사영역
(3) 증적자료
(4) 현장실사
(5) 미흡사례

시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

심사대상

- 본인확인시스템 보안
- 네트워크 및 시스템 안정성 점검
- 시스템 취약점 점검
- 소프트웨어의 임의변경·삭제방지

시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

심사영역

- 본인확인서비스와 관련된 네트워크, 서버 및 주요 개인정보취급자 PC의 망 분리 현황, 재택근무 등 원격근무 시 보안정책을 심사
- 본인확인서비스의 365일*24시간 지속적 서비스 제공을 위한 주요 프로그램, 프로세스, 데몬 등을 모니터링 하는 솔루션 및 운영체계를 심사
- 본인확인서비스의 대체수단 부정사용 여부에 대한 부정방지정책(FDS시스템) 및 이상행위에 대한 모니터링 여부를 심사
- 주요정보통신기반시설 및 전자금융기반시설 보안 취약점 점검 활동 여부와 실제 조치 완료한 항목을 심사
- 본인확인서비스 관련 소스 코드 보안을 위한 형상관리, 버전관리, 배포관리 등 소프트웨어 개발과 관련된 라이프사이클을 심사

시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

증적자료

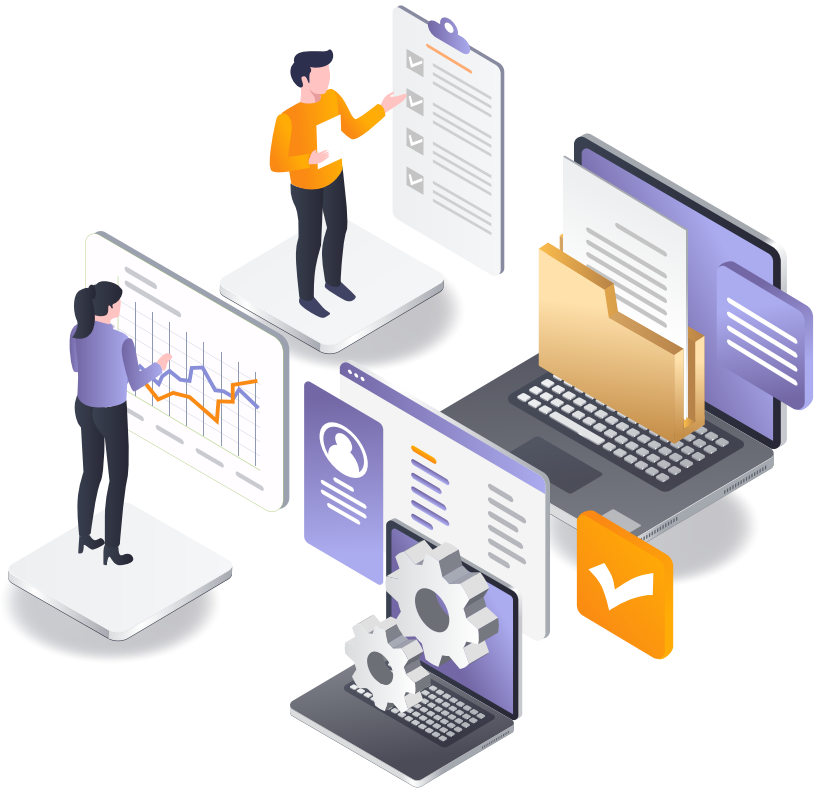
- 본인확인업무 관련 망 분리 대상자 리스트 / 망 분리 현황 네트워크 구성도 / 원격근무 보안 정책
- WEB, WAS(AP포함), EAI, ESB, FEP, DBMS, 컨테이너 등 본인확인서비스 프로그램 모니터링 현황
- FDS(부정방지솔루션) 정책 및 이상행위 분석 여부
- 시스템 취약점 점검 완료보고서, 모의해킹 결과보고서, 취약점 위험수용 시 CISO 승인 문서
- 운영체제, DBMS별 EoS(End of Service)/EoL(End of Life) 관리 목록, 오픈소스 주요 CVE 취약점 패치 이력
- 소스코드 형상관리(Git 계열 포함), 배포관리, 버전관리, 주요 레파지토리 권한 부여 현황
- 시큐어코딩 솔루션에 적용되는 보안정책(한국인터넷진흥원의 49가지 원칙, OWASP TOP10 등)
- Native APP(안드로이드, IOS) 통합IDE툴 버전관리, 난독화 솔루션 적용여부 및 APK/ IPA 빌드 배포 관리

시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

현장실사(증적자료 확인과 담당자 인터뷰, 현장점검을 통해 진행)

대상 담당자

- 정보보안담당자
- 취약점 수행 및 조치완료 담당자
- 모의해킹 담당자(기관에서 직접 수행 시)
- 서버 운영 및 FDS 담당자
- 서버 개발자와 안드로이드, IOS 앱 개발자

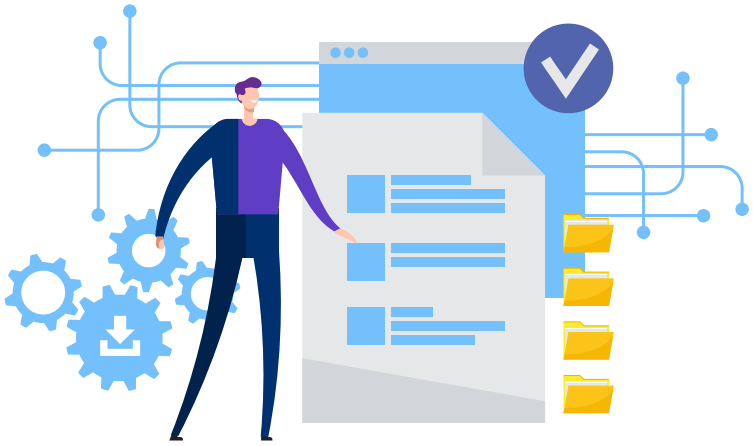


시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

인터뷰 및 현장점검

- 망 분리 대상과 적용된 망 분리 현황 설명 / 원격근무 절차 및 적용되는 보안정책
- 본인확인서비스 모니터링 정책과 장애 처리 프로세스
- 부정방지시스템(FDS)을 통한 이상행위 분석 여부
- 주요정보통신기반시설 및 전자금융기반시설 보안 취약점 점검 증적과 위험수용 CISO 승인이력
- 본인확인서비스와 관련된 서버 사이드 개발, 클라이언트 개발 시 보안 정책 및 시큐어코딩 정책

해당자료 및 설명을 요청하고 담당자 인터뷰 진행 후,
요청 받은 자료와 지침을 근거로 실제 현장점검을 수행합니다.



시스템 및 네트워크의 운영·보안 및 관리 사항의 적정성 심사 기준

미흡사례

- 본인확인기관 심사 시 시스템 취약점 점검은 정보통신기반보호법 기준인 주요정보통신기반시설 취약점 점검 항목을 우선으로 합니다.
- 정보통신기반보호법이 아닌 전자금융거래법이 우선 적용되어 전자금융감독규정 준수가 필수인 기관은 전자금융기반시설 보안 취약점 점검 이력과 주요정보통신기반시설 취약점 점검 이력 등 2가지 모두를 수행해야 하고 이에 대한 근거가 제시되어야 합니다.

(1) 시스템 취약점 점검

: 주요정보통신기반시설 취약점 점검 항목 중 '상'에 관련된 항목을 CISO 위험수용 승인없이 임의적으로 미조치한 경우

(2) 안드로이드 및 IOS 앱 보안 관련

: 본인확인서비스를 위한 별도의 Native APP이 존재하는 경우, 안드로이드 기준 난독화 솔루션이 적용되지 않은 경우, 앱 소스 코드 검증 가이드라인에 따라 미흡사례가 됩니다.