[별표 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. 본인확인업무를 위한 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