국회토론회

연계정보(CI) 제도의 위헌성과 제도 개선 방향

일시 | 2026년 4월 8일(수) 오전10시
장소 | 국회의원회관 제11간담회의실
주최 | 국회의원 김우영, 국회의원 김남근, 국회의원 이주희,
국회의원 한창민, 디지털정의네트워크,
민주사회를 위한 변호사모임 디지털정보위원회,
정보인권연구소, 참여연대

순 서

10:00 ~ 10:05	인사	**공동주최** 국회의원
	사회	**김기중** (법무법인 동서양재 변호사, 정보인권연구소 이사)
10:05 ~ 11:20	발제	**연계정보(CI) 제도의 역사** | 최새얀 변호사 (민변 디지털정보위원회)
		연계정보(CI)의 위헌성 검토 | 이장희 국립창원대학교 법학과 교수 (참여연대 공익법센터)
		연계정보(CI) 대체수단에 대한 해외 사례 | 오병일 대표 (디지털정의네트워크 대표)
11:20 ~ 11:50	토론	최경진 한국정보법학회 회장 (가천대학교 법학과 교수)
		이상목 방송미디어통신위원회 디지털이용자기반과 사무관
		김영훈 개인정보보호위원회 신기술지원과 사무관
11:50 ~ 12:00	**플로어 토론 및 참석자 전체 토론**	

인 사 말

김우영 | 더불어민주당 국회의원
(과학기술정보방송통신위원회)

반갑습니다.

더불어민주당 은평을 국회의원 김우영입니다.

「연계정보(CI) 제도의 위헌성과 제도 개선 방향」 토론회 개최를 진심으로 뜻깊게 생각합니다. 오늘 이 자리를 마련해주신 디지털정의네트워크와 민변, 정보인권연구소, 참여연대 관계자 여러분께 감사드립니다.

연계정보(CI)는 주민등록번호를 대체하기 위한 수단으로 도입됐지만, 활용 범위가 넓어지면서 사실상 또 하나의 범용 식별수단으로 작동할 수 있다는 우려가 커지고 있습니다. 정보주체가 충분히 인지하거나 통제하기 어려운 방식으로 생성·활용되고, 여러 개인정보를 연결하는 고리로 기능할 수 있다는 점에서 개인정보 자기결정권과 익명성의 자유를 침해할 가능성을 결코 가볍게 볼 수 없습니다.

이미 주민등록번호 제도가 가진 한계와 위험성은 오래전부터 지적돼 왔습니다. 연계정보 역시 같은 문제를 반복할 수 있다는 점은 결코 가볍게 볼 수 없습니다. 기술의 편의와 사회적 효율도 중요하지만, 그 과정에서 국민의 기본권이 훼손돼서는 안 됩니다.

디지털 환경이 빠르게 확장되는 지금, 식별체계는 단순한 기술 문제가 아니라 국민의 권리와 민주주의의 기준을 가르는 제도적 문제입니다. 이제는 어떻게 더 쉽게 식별할 것인가가 아니라, 어떻게 더 안전하게 보호하고 어떻게 정보주체의 통제를 실질적으로 보장할 것인가를 중심에 두어야 합니다.

오늘 토론회가 연계정보 제도의 헌법적 쟁점을 깊이 있게 점검하고, 식별체계의 필요성과 기본권 보호 사이의 바람직한 균형점을 찾는 출발점이 되길 바랍니다. 저 역시 국회에서 이 문제를 면밀히 살피고, 국민의 권리가 실질적으로 보호될 수 있도록 제도 개선 논의에 함께 하겠습니다. 감사합니다. ▢

인 사 말

김남근 | 더불어민주당 국회의원
(정무위원회)

안녕하십니까.

더불어민주당 성북을 국회의원 김남근입니다.

오늘 「연계정보(CI) 제도의 위헌성과 제도개선 방향」 국회토론회에 함께해 주신 모든 분들께 진심으로 감사드립니다. 뜻깊은 자리를 마련해주신 디지털정의네트워크, 민주사회를 위한 변호사모임 디지털정보위원회, 정보인권연구소, 참여연대 관계자 여러분께 깊이 감사드립니다. 또한 발제를 맡아주신 최새얀 변호사님, 이장희 교수님, 오병일 대표님과 토론에 참여해주신 모든 전문가 여러분께도 감사의 말씀을 드립니다.

연계정보(CI)는 주민등록번호를 암호화한 정보로, 온라인에서 개인을 식별하기 위해 도입되었습니다. 그러나 실제로는 주민등록번호와 1:1로 대응되는 구조를 가지고 있어, 사실상 '온라인 주민등록번호'로 기능하고 있다는 지적이 제기되고 있습니다.

문제는 이 제도가 도입된 취지와 달리, 개인정보 보호 원칙—특히 최소수집과 목적 제한 원칙—을 위배할 가능성이 크다는 점입니다. 주민등록번호 오남용을 막기 위해 도입된 제도가 오히려 또 다른 범용 식별자로 확대되고 있습니다.

나아가, 연계정보는 단순한 기술적 문제를 넘어 헌법적 기본권 문제로까지 이어지고 있습니다. 개인정보 자기결정권, 사생활의 비밀, 익명표현의 자유, 나아가 평등권까지 침해할 수 있다는 우려가 제기되고 있습니다.

특히 연계정보 없이는 서비스 이용 자체가 어려운 구조는, 사실상 국민에게 특정 식별체계를 강제하는 결과를 낳고 있습니다. 이는 과거 인터넷 실명제가 위헌 결정된 취지와도 충돌할 수 있는 지점입니다.

미국과 유럽은 하나의 범용 식별자를 사용하는 방식이 아니라, 서비스별로 다른 식별자를 사용하거나 필요한 정보만 선택적으로 제공하는 방향으로 나아가고 있습니다. 이는 개인정보 보호와 디지털 혁신을 동시에 달성하기 위한 중요한 기준이 되고 있습니다.

우리는 효율성과 편의성을 이유로 국민을 하나의 식별번호로 연결하는 사회로 갈 것인지, 아니면 개인정보 자기결정권과 기본권을 중심으로 디지털 신원체계를 재설계할 것인지에 대한 선택을 해야 할 기로에 서 있습니다.

국회 역시 국민의 기본권 보호라는 헌법적 책무에 따라, 연계정보 제도의 문제점을 면밀히 검토하고 필요한 입법적 개선을 적극 추진해 나가겠습니다. 오늘 이 자리에서 제기되는 다양한 의견과 대안들이 보다 안전하고, 보다 자유로운 디지털 사회로 나아가는 밑거름이 되기를 기대합니다.

다시 한번 함께해 주신 모든 분들께 감사드립니다. 감사합니다. ▢

인 사 말

이주희 | 더불어민주당 국회의원
(과학기술정보방송통신위원회)

안녕하십니까. 국회 과학기술정보방송통신위원회 소속 더불어민주당 이주희 국회의원입니다.

오늘 「연계정보(CI) 제도의 위헌성과 제도 개선 방향」에 함께해주신 모든 분들께 깊이 감사드립니다. 뜻깊은 자리를 함께 마련해주신 김우영, 김남근, 한창민 의원님들과 디지털정의네트워크, 민주사회를 위한 변호사모임 디지털정보위원회, 정보인권연구소, 참여연대에도 감사의 말씀을 드립니다.

연계정보, 이른바 CI는 처음에는 주민등록번호를 대체하는 수단으로 도입됐지만, 지금은 사실상 온라인공간에서 주민등록번호와 유사한 기능을 수행하는 식별수단으로 확대되어 왔습니다. 주민등록번호와 1대1로 연결되고, 서로 다른 서비스와 데이터베이스를 이어 붙이는 열쇠처럼 작동한다는 점에서, 이것이 과연 헌법이 보장하는 개인정보자기결정권과 사생활의 비밀, 익명표현의 자유에 부합하는 제도인지 근본적인 질문을 던지지 않을 수 없습니다.

더 큰 문제는 많은 시민들이 자신도 모르는 사이 이러한 구조 속에 편입되어 있다는 점입니다. 편의와 효율이라는 이름으로 개인의 권리가 너무 쉽게 후순위로 밀려난 것은 아닌지, 이제는 국회가 진지하게 점검해야 합니다.

오늘 토론회가 중요한 이유도 바로 여기에 있습니다. 연계정보 제도의 역사와 위헌성, 그리고 해외의 대체 가능 사례까지 함께 검토하면서 우리 사회가 반드시 지금의 방식만을 고집해야 하는 것은 아니라는 점을 확인할 수 있기 때문입니다. 식별의 필요성과 행정의 효율은 존중하되 그것이 국민의 기본권 침해를 정당화하는 근거가 될 수는 없습니다.

이제는 “편리하니까 유지하자”는 접근이 아니라 “기본권을 침해하지 않으면서도 가능한 제도는 무엇인가”라는 질문으로 논의를 전환해야 합니다. 국회 역시 국민의 권리를 더 두텁게 보호하는 방향에서 법과 제도를 점검하고 필요한 개선에 책임 있게 나서겠습니다.

오늘 이 자리가 연계정보 제도의 문제를 정확히 진단하고 보다 안전하고 민주적인 디지털 신원확인 체계를 모색하는 출발점이 되기를 기대합니다. 귀한 발제와 토론을 준비해주신 모든 분들께 다시 한 번 감사드립니다.

고맙습니다. ▢

인 사 말

한창민 | 사회민주당 국회의원
(정무위원회)

안녕하십니까. 정치를 새롭게, 복지를 강하게! 사회민주당 대표 국회의원 한창민입니다.

디지털 시대의 인권과 민주주의를 위해 애쓰시는 모든 분께 깊은 존경과 연대의 인사를 드립니다.

연계정보(CI)는 주민등록번호를 대체하기 위한 수단으로 도입되었지만, 현재는 사실상 '온라인상의 주민등록번호'로 기능하며 또 하나의 범용 국민식별번호로 자리 잡고 있습니다. 제도의 출발 취지와 달리, 오히려 개인정보 보호 원칙을 훼손하고 기본권 침해 가능성을 확대하는 방향으로 작동하고 있다는 점에서 깊은 우려를 표하지 않을 수 없습니다.

이미 우리는 주민등록번호 제도가 과도한 수집과 유출, 그리고 개인의 추적 가능성을 높인다는 비판 속에서 제도 개선 요구를 받아왔습니다. 그런데도 연계정보 제도는 동일한 문제를 반복하고 있습니다. 특히 서로 다른 데이터베이스를 손쉽게 결합할 수 있는 '열쇠'로 작동하면서, 개인의 삶을 상시적인 감시와 프로파일링의 위험에 노출시키고 있습니다.

발제문에서도 지적되었듯이, 연계정보는 목적 명확성 및 최소 수집 원칙을 위배할 소지가 크며, 정보주체가 인지하지 못한 상태에서 생성·활용되는 경우가 많다는 점에서 개인정보 자기결정권 침해 문제가 심각합니다. 또한 본인확인이 불필요한 다수의 민간 서비스에서도 관행적으로 활용되면서, 필요 이상의 개인정보 수집 구조가 일반화되고 있습니다.

더 중요한 점은, 이러한 범용 식별체계가 반드시 필요한 것이 아니라는 사실입니다. 미국과 유럽연합 등 주요 국가들은 전역 식별자 사용을 지양하고, 서비스별로 서로 다른 식별자 또는 최

소한의 정보만을 제공하는 방식으로 디지털 신원체계를 설계하고 있습니다. 이는 효율성보다 개인정보 보호와 시민의 통제권을 우선하는 방향으로 국제적 기준이 변화하고 있음을 보여줍니다.

이제 우리도 선택의 기로에 서 있습니다. 편의와 효율을 이유로 국민을 하나의 번호로 묶어 관리하는 사회로 갈 것인지, 아니면 시민의 권리와 자유를 중심에 둔 디지털 사회로 나아갈 것인지 결정해야 합니다.

디지털 전환은 거스를 수 없는 흐름입니다. 그러나 그 방향은 선택할 수 있습니다. 기술은 중립적이지 않습니다. 어떤 제도를 설계하느냐에 따라, 그것은 시민의 자유를 확장하는 도구가 될 수도 있고, 통제와 감시의 수단이 될 수도 있습니다.

무엇보다 중요한 것은 '시민의 통제권'입니다. 자신의 정보가 언제, 어떻게, 누구에 의해 활용되는지 국민이 알고 선택할 수 있어야 합니다. 오늘 토론회가 연계정보 제도의 헌법적 문제를 짚고, 보다 인권 친화적인 디지털 신원체계를 모색하는 중요한 출발점이 되기를 기대합니다.

저와 사회민주당은 국민의 기본권을 최우선으로 하는 디지털 정책을 위해 함께하겠습니다. 고맙습니다. ▢

연계정보(CI) 제도의 역사

최새얀 변호사 | 민주사회를위한변호사모임 디지털정보위원회

연계정보(CI)제도의 역사

민주사회를 위한 변호사모임 디지털정보위원회

최새얀 변호사

인터넷 실명제의 도입

- 2007년, 악성댓글 등으로 인한 사회적 폐해를 막는다는 이유로 포털사이트 등을 중심으로 인터넷 실명제(제한적 본인확인제) 도입

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 (게시판 이용자의 본인 확인)
① 다음 각 호의 어느 하나에 해당하는 자가 게시판을 설치·운영하려면 그 게시판 이용자의 본인 확인을 위한 방법 및 절차의 마련 등 대통령령으로 정하는 필요한 조치를 하여야 한다.
1. 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제5조제3항에 따른 공기업·준정부기관 및 「지방공기업법」에 따른 지방공사·지방공단
2. 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 10만 명 이상이면서 대통령령으로 정하는 기준에 해당되는 자

동법 시행령 제29조
①법 제44조의5제1항 각 호 외의 부분에서 "대통령령으로 정하는 필요한 조치"란 다음 각 호의 모두를 말한다.
1.「전자서명법」 제2조제10호에 따른 공인인증기관, 그 밖에 본인확인서비스를 제공하는 제3자 또는 행정기관에 의뢰하거나 모사전송 · 대면확인 등을 통하여 **게시판이용자가 본인임을 확인할 수 있는 수단**을 마련할 것

대형 개인정보 유출 사건, 헌법재판소의 위헌 결정

- 2008년 옥션에서 1700만 명, 2011년 네이트/싸이월드에서 3500만 명의 주민등록번호 등 개인정보가 대량으로 유출되는 사건 발생
- 2010년경 참여연대 등 인터넷 실명제에 대한 헌법소원 청구
- 헌법재판소, 2012년 8월 인터넷실명제 위헌 결정

<최소침해원칙 위반 판단 부분>
본인확인의 대상인 '게시판 이용자'는 '정보의 게시자'뿐만 아니라 불법행위를 할 가능성이 없는 '정보의 열람자'도 포함하고, 본인확인제 적용 대상인 정보통신서비스제공자 선정에 있어서 그 정확성과 기준이 불분명한 이용자수 산정 결과에 따라 적용대상의 범위가 정해지는 등 본인확인제는 인터넷의 특성을 고려하지 아니한 채 그 적용범위를 광범위하게 정함으로써 법집행자에게 자의적인 집행의 여지를 부여함

본인확인제에 따라 정보통신서비스제공자가 본인확인정보를 보관하여야 하는 기간은 정보의 게시가 종료된 후 6개월이 경과하는 날까지이므로, 정보를 삭제하여 그 게시를 종료하지 않는 한 본인확인정보는 무기한으로 정보통신서비스제공자에게 보관되는 결과 발생

주민등록번호 수집 제한, 그러나 실무와의 괴리

- 헌재 위헌결정 이후 2014년 개인정보보호법 개정에 따라 주민등록번호 수집 법정주의 도입. 법에 정해진 사유가 아닌 이상 주민등록번호 수집 불가

> 구 개인정보보호법(2014. 8. 7. 개정된 것)
> 제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
> ② 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

- 아이핀, 휴대폰 본인인증 등 대체수단 전면 도입

> [방통위 기본계획]
> 1단계(2009~11년) 아이핀 제도의 조기정착 및 이용 보편화를 위한 인프라 구축
> 2단계(2012~13년) 조세·금융 등 특수 분야를 제외한 모든 민간 온라인서비스에 아이핀 적용 3단계(2014~15년) 모든 분야에서 궁극적으로 주민번호 없는 안전한 인터넷 환경을 조성하는 것을 목표

연계정보(CI) 도입

- 한국인터넷진흥원, 2010년 '웹사이트 간 이용자의 구별이 가능하도록 연계정보를 제공할 필요가 있다면서, 가입 회원의 주민등록번호를 연계정보로 변환할 수 있는 모듈을 개발·제공한다'고 밝히며 아이핀 2.0라는 이름으로 연계정보 개발
- 연계정보: 주민등록번호를 해쉬함수를 이용하여 일방향으로 암호화하여 64바이트 코드 생성, 다시 한국인터넷진흥원이 생성하여 본인확인기관과 공유하는 '공유비밀정보'를 더하여 전체88바이트의 코드 생성
- 주민등록번호의 기능인 '개인식별기능', '인증기능', '연결기능' 및 차별적 특성인 '범용성', '효율성' 속성을 갖고 있음
- 2015년 방송통신위원회 고시의 방법으로 서둘러서 연계정보 도입

규제 샌드박스와 모바일 전자고지 도입

- 정부와 민간기업은 종이 고지서 제작 및 발송 비용을 줄이고 도달률 높이기 위해 카카오톡, 네이버 알림 등으로 고지서를 보내는 '모바일 전자고지' 사업 추진
- 행정기관이 보유하고 있는 국민의 개인정보(주민등록번호)와 통신기업이 보유하고 있는 가입자의 개인정보(전화번호)를 매칭하기 위해서 연계정보가 필요하였음
- 연계정보에 관한 별도의 법률적 근거가 없는 상태에서, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제37조(임시허가) 규정에 근거한, 신규 정보통신융합 등 기술 · 서비스에 대한 과학기술정보통신부장관의 '임시허가'라는 형식으로 연계정보 제도 시행

  *2018년 위 법 개정을 통해 신속처리를 거치지 않아도 임시허가가 가능하도록 하였고, 임시허가시 신기술 · 서비스심의위원회의 심의 · 의결 절차를 규정하며, 임시허가의 유효기간을 2년으로 확대
- 2021년, 민변/진보넷/참여연대 등은 위 임시허가에 대한 헌법소원 제기(각하)

정보통신망법에 연계정보 제도 공식 도입

- 2024년 1월 정보통신망법에 연계정보 제도 도입

정보통신망법 제23조의5
제23조의5(연계정보의 생성 · 처리 등) ① 본인확인기관은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보(이하 "연계정보"라 한다)를 생성 또는 제공 · 이용 · 대조 · 연계 등 그 밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 없다.

1. 이용자가 입력한 정보를 이용하여 이용자를 안전하게 식별 · 인증하기 위한 서비스를 제공하는 경우
2. 「개인정보 보호법」 제24조에 따른 고유식별정보(이하 이 조에서 "고유식별정보"라 한다)를 보유한 행정기관 및 공공기관(이하 "행정기관등"이라 한다)이 연계정보를 활용하여 「전자정부법」 제2조제5호에 따른 전자정부서비스를 제공하기 위한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
가. 「전자정부법」 제2조제4호에 따른 중앙사무관장기관의 장이 행정기관등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성 · 처리를 요청한 경우
나. 행정기관등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성 · 처리를 요청한 경우
3. 고유식별정보를 보유한 자가 「개인정보 보호법」 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성 · 처리를 요청한 경우
4. 「개인정보 보호법」 제24조의2제1항 각 호에 따라 주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 아니하고 연계정보 생성 · 처리가 불가피한 대통령령으로 정하는 정보통신서비스를 제공하기 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받은 경우

정보통신망법상 연계정보 제도의 문제

- 비현실적인 원칙적 금지, 제한적 허용 체계 - 이미 본인확인서비스 시장 매우 활성화, 연계정보 생성 및 처리가 광범위하게 이루어지고 있는 상황에서 원칙적 금지 / 단서로 제한적 허용 조항을 둔 것은 선언적 의미에 불과

- 보편적 개인식별번호으로서 통용: 사실상 제2의 주민등록번호로서 온라인 상에서 통용되며, 서로 다른 목적의 데이터베이스를 무분별하게 결합하도록 하여 사생활을 상시적 감시 상태로 몰아넣게 함

- 문턱이 낮은 본인확인기관: 연계정보의 생성 및 처리는 본인확인기관으로 지정된 자에 한정되나, 실제 사례에서는 방송통신위원회에 신청을 하면 엄격하지 않은 심사 절차를 거쳐 본인확인서비스 시장에 진입할 수 있음(2026. 3. 기준 23곳)

- 명확성 원칙의 문제: '불가피하게 이용자의 동의를 받지 않을 수 있는 경우', '주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 않고 연계정보 생성 및 처리가 불가피한 정보통신서비스를 제공하려는 경우' 등 동의 및 명확한 기준 없이 생성 및 처리할수 있는 여지를 둔 조항 존재

발 제

연계정보(CI)의 위헌성 검토

이장희 | 국립창원대학교 법학과 교수, 참여연대 공익법센터

"연계정보 제도의 위험성과 제도 개선 방향"
국회토론회, 2026. 4. 8.(수)

연계정보의 위헌성

이 장 희
국립창원대학교 법학과 교수

연계정보(CI)란?

- Connecting Information
- "**정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보**" (정보통신망법 제23조의5)
- ☞ 전 국민이 보유하고 있는 주민등록번호를 정보통신서비스에서도 그대로 이용할 수 있도록 하기 위해 만들어 낸 '**온라인용 주민등록번호**'

연계정보(CI) = 주민등록번호의 해쉬함수값 + 공유비밀정보

연계정보의 특징, 기능

- **주민등록번호와 1:1로 매칭**하여 생성되는 것이기 때문에 **'온라인 주민등록번호' 또는 '제2의 주민등록번호'**
- ☞ 따라서 연계정보는 주민등록번호와 마찬가지로 **고유성, 불변성, 범용성, 효율성**의 특징
- ☞ 주민등록번호와 마찬가지로 **개인별수단, 인증기능, 연결기능**
- ☞ **따라서 연계정보만 있으면 온라인에서 특정인의 정보를 알아내거나 어떤 정보가 동일인의 정보임을 확인 가능**

주민등록번호의 부활, 규제의 해제

- 과거 주민등록번호의 민간 영역 오남용, 유출 문제 심각
  - ☞ 따라서 주민등록번호의 대체수단 요구, 법적 규제 강화
- **그런데 대체수단으로서의 연계정보는 그 자체로 온라인상 주민등록번호의 부활이며, 법적 규제를 해제하는 효과**
- 연계정보는 여타의 대체수단과 다른 차별성을 지님
  - ☞ 연계정보는 주민등록번호의 장점과 문제점을 동시에 내포
  - ☞ **가령, 연계정보의 고유성, 불변성, 식별과 연결기능, 유출 및 오남용시 주민등록번호보다 더 파괴적인 피해 가능**

현행법상 연계정보의 생성·처리의 유형

- 첫째, **온라인 서비스의 이용자 본인확인을 위한 연계정보의 생성·처리**
- 둘째, **전자정부서비스를 위한 연계정보의 생성·처리**
- 셋째, **마이데이터 서비스를 위한 연계정보의 생성·처리**
- 넷째, **이용자의 동의 없는 연계정보의 일괄변환 등 비상적 생성·처리의 승인**

연계정보의 생성·처리 체계상 문제점

- (1) '원칙적 금지, 제한적 허용'의 체계의 허구성
- (2) 연계정보의 생성·처리의 주체의 한정의 기만성
- (3) 정보통신서비스 구현의 효율성에 치중된 연계정보
- (4) 목적구속성의 실효성 약화 가능성
- (5) 연계정보의 기술적 안전성의 취약성

연계정보의 생성·처리로 인한 기본권 침해의 문제

- (1) 온라인 서비스 이용자의 개인정보자기결정권 침해
- (2) 온라인 서비스 이용자의 사생활의 비밀과 자유 침해
- (3) 온라인 서비스 이용자의 익명표현의 자유 침해
- (4) 온라인 서비스 이용자의 평등권 침해
- ☞ **과잉금지원칙, 특히 (최소침해성 원칙 위반)**

개인정보자기결정권 침해(1)

- 문제의 핵심은 주민등록번호의 대체수단 자체에 있는 것이 아니라, **'온라인용 주민등록번호'라 할 수 있는 연계정보를 특별히 생성·처리할 수 있게 하면서 정보주체의 동의 등 본인에 의한 사전 또는 사후적 통제가능성이 전혀 부정되는 점**에 있으며, 이것이 정보주체의 '개인정보자기결정권'을 과도하게 제한
- ☞ 그 결과 **주민등록번호의 대체수단을 요구한 헌법적 취지를 무력화**하고 주민등록번호 주체의 의사와 무관하게 연계정보를 생성하도록 하여 **주민등록번호를 사실상 부활시켜 온라인 영역에서 사용하게 한 것**으로 평가
- ☞ 그럼에도 연계정보는 **주민등록번호만큼도 보호되고 있지도 못함**

개인정보자기결정권 침해(2)

- 정보주체가 온라인 서비스 제공자에게 자신의 연계정보의 처리정지나 삭제요구 어려움, 연계정보 없이는 해당 정보주체의 서비스 이용이 불가능
- ☞ 결국 스스로 '**온라인 난민**'이 되기로 결정하지 않는 이상 연계정보로부터 벗어나기는 불가능한 상황
- 연계정보의 생성·처리가 사실상 강요되고 있고 또 필요한 범위를 넘어서 광범위하게 사용되고 있음
- **그럼에도 현행법은 연계정보 이외에는 기본권을 덜 침해하는 다른 식별수단의 대체가능성은 마련하고 있지 않음. ☞ 최소침해성 원칙 위반**

사생활의 비밀과 자유 침해(1)

- 연계정보는 주민등록번호를 불가역적으로 암호화한 해쉬함수 값이므로 그 자체로는 사생활에 관한 내용을 담고 있는 것은 아니지만, 다른 정보와 결합하여 개인을 식별할 수 있는 고유식별정보로 기능 ☞ **연계정보 자체가 개인정보에 해당**! (그럼에도 연계정보를 개인정보가 아니라고 강변하는 경우가 존재함)
- **특히 고유, 불변의 범용연결자로서, 사생활 정보를 캘 수 있는 만능열쇠 ☞ 따라서 그 자체로 연계정보는 사생활의 중대한 침해 가능성을 내포하는 개인별 고유식별수단**

사생활의 비밀과 자유 침해(2)

- 그런데도 연계정보를 사실상 강제로 사용하게 하면서, 연계정보의 삭제, 처리정지조차 사실상 불가능한 상황
- ☞ 비유) 홈케어 서비스를 받기 위해 어쩔 수 없이 서비스 업자에게 현관문 마스터키를 맡긴 이후로 그가 계속 열쇠를 가지고 있는데 아직 그 업자가 마스터키를 이용하여 집안을 부당하게 수색하지 않았다는 이유만으로 사생활의 비밀과 자유에 아무런 위험이나 침해가 없다고 할 수 있는가?

익명표현의 자유 침해

- 연계정보의 생성・처리가 이루어지면서 불가피하게 이용자의 익명성 (匿名性) 이 사실상 소멸, 반대로 만약 연계정보가 아닌 다른 덜 침해적인 방법이라면 온라인 환경에서 이용자의 익명성 확보 가능
- **최소침해성 원칙 위반 ☞ 덜 침해적인 수단이 존재함에도 불구하고 위험성이 높은 연계정보의 사용을 요구함으로써, 결국 자신의 신원을 외부로 밝혀야만 온라인 서비스 이용이 가능하게 만드는 결과를 초래**
- ☞ 온라인 서비스 이용자가 자신의 신원을 외부로 밝히 않은 채 온라인 인터넷 서비스를 이용할 자유(익명표현의 자유)를 침해

평등권 침해(1)

- **연계정보를 이용하지 않으면서 온라인 서비스를 이용하는 사람들**에 비하여 **연계정보를 이용해서만 온라인 서비스를 이용할 수 있는 사람들**을 불합리하게 차별함 ☞ 평등권 침해
- **특히 전 세계의 많은 사람들은 연계정보와 같은 것이 없어도 그 밖의 다양한 방법으로 '본인확인'을 신뢰성 있게 할 수 있지만, 우리나라 국민들만 주민등록번호에 더하여 유독 연계정보까지 사용해야 하는 차별적인 상황에 처해 있는 것**

평등권 침해(2)

- **또한 연계정보의 강요(동의 없는 연계정보 생성/처리, 연계정보 삭제요구 및 처리정지요구도 사실상 불가능)는 연계정보를 원하지 않는 사람들을 소외시키는 결과 초래** ☞ 연계정보 없이는 비자발적으로 온라인 서비스를 이용할 수 없게 되기 때문
- **마치 대중교통에서 버스카드만 허용하고 현금승차를 허용하지 않는 상황에서 버스카드를 이용하길 원하지 않는 사람들이 대중교통이란 공공서비스의 이용이 불가능하게 되는 것과 유사** ☞ 이 경우, 현금승차는 사람들에게 익명성을 보장하고 일반적 행동자유도 보장하지만, 버스카드의 사용 강제는 버스이용자를 차별하여 익명성, 일반적 행동자유까지 침해

평등권 침해(3)

- 또한 연계정보의 사용 강제는 역차별의 결과도 초래
- 최근 외국인들이 국내 온라인쇼핑몰을 이용할 때 주민등록번호나 연계정보가 없어서 쇼핑몰 사이트에 접속 자체가 불가능해지는 상황 발생 – 외국인에게만 주민번호나 연계정보 없이도 본인확인이 가능하게 하도록 시스템 수정 요구 (한국은행 이슈노트, [제2025-20호] 참조)
- **그러나 우리 국민은 기본권 침해를 감수하면서 왜 연계정보를 계속 이용해야 하는가? 역차별의 문제 발생**
- **그만큼 우리나라의 온라인 서비스 환경은 폐쇄적이고 차별적!**

디지털 정보로 연결되지 않을 권리

- 앞으로 인공지능의 고도화, 디지털화된 초연결사회에서 인간의 존엄성과 자유, 평등, 아날로그적 삶의 가치를 어떻게 보존할 수 있을까?
- 연계정보의 무분별한 사용 및 확대 경향을 어떻게 멈출 수 있을까?
- **디지털화된 초연결사회가 심화될수록 그러한 과도한 연결로부터 자유로운 삶의 공간을 확보할 필요성이 더 커짐**
- **연계정보의 위험성을 거부하고 인간 존엄성을 확보하기 위한** 개인의 권리로서 '**디지털 정보로 연결되지 않을 권리**'가 필요한 상황

연계정보 제도의 폐지 필요

- 최근 개인정보 유출 사건 빈발 ☞ 연계정보도 유출, 오남용 위험 증대
- **연계정보 없이도 얼마든지 인공지능의 발전, 온라인 서비스 이용, 개인식별과 본인확인도 가능 (☞ 우리만 왜 연계정보를 써야 하는가?)**
- 온라인 서비스의 효율성과 편리함이 인간의 존엄, 자유, 평등보다 중요한가?
- **연계정보의 위험성을 방치**하는 것은 **국가의 '기본권보호의무' 위반**
- **국회의 법개정으로 연계정보를 폐지, 덜 침해적인 방법으로 전환 필요**
- **헌법재판소의 단순위헌 또는 헌법불합치 결정이 중요**

감사합니다.

연계정보(CI) 대체수단에 대한 해외 사례

오병일 대표 | 디지털정의네트워크 대표

1. 들어가며

애초에 주민등록번호가 보편적 국민식별번호로 사용되면서 과도한 수집 및 유출 문제가 심각해지자, 2011년에 온라인에서 ‘이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법’, 즉 주민등록번호 대체수단을 제공하도록 하였고, 방송통신위원회가 고시 제2012-48호 "본인확인기관 지정 등에 관한 기준 고시"를 제정하면서, '대체수단'의 구체적인 사항을 규정하면서 연계정보(CI)의 정의가 포함되었다. 이때 연계정보는 '정보통신서비스 제공자의 온오프라인 서비스 연계를 위해 생성한 정보'로 정의되었으나, 2024년에 정보통신망법 개정으로 제23조의5가 포함되어 이제 단지 '주민등록번호 대체수단'을 넘어 범용식별번호로 활용되고 있다. 그러나 범용식별번호는 그 개념 자체만 보더라도 목적의 명확성 및 최소 수집의 원칙 등 개인정보보호원칙에서 벗어나 있다. 비록 정보통신망법 제23조의5와 같이 처리의 법적 근거를 둘 경우 적법성 논란에서 벗어날 수 있을지는 모르나, 그렇다고 개인정보보호원칙 및 헌법에 부합하는 것은 아니다.

유럽연합의 경우 2024년 전자신원증명 및 신뢰 서비스 규정을 개정(eIDAS 2.0)하여 유럽 디지털 신원 지갑(EU Digital Identity Wallets) 제도를 도입하였는데, EUDI 지갑은

이용자의 프라이버시와 보안을 보호하고 이용자에게 자신의 데이터에 대한 통제권을 부여하는 것을 원칙으로 하고 있다. 데이터 최소화 원칙에 따라 필요한 정보만 공유하도록 하고, 법적 근거없는 추적이나 프로파일링을 할 수 없도록 설계하였다. 주민등록번호나 연계정보와 같은 보편적 개인식별번호는 서로 다른 기관이 보유한 개인정보를 연계, 결합하여 추적 및 프로파일링을 가능하도록 하기 때문에, 프라이버시 및 보안 원칙 하에서는 결코 허용될 수 없는 방식이다.

유럽 뿐만이 아니다. 미국 국립표준기술연구소(NIST)의 디지털 신원 가이드라인(Digital Identity Guidelines)은 디지털 신원 시스템 설계 시 프라이버시 문제를 반드시 고려해야 한다는 기본 원칙을 제시하는데, 프라이버시 기본 설계(Privacy by Design), 프라이버시 위험 평가의 수행 등을 권고하고 있다. 특히, 신원 제공자(Identity Provider, IdP)와 서비스제공자(Relying Party, RP) 간의 데이터 전송 최소화 의무를 규정하고, 이를 위해 여러 사이트에서 동일한 식별자를 사용하는 대신, 각 서비스마다 서로 다른 식별자(Pairwise Pseudonymous Identifiers)를 사용하도록 요구한다.[1)]

연계정보의 존치에 대한 논거 중 하나는, 그것이 '모바일 전자고지'와 같이 사회에 유용하게 활용될 수 있다는 것일 것이다. 그러나 현재 연계정보를 필요로 하는 작업을 덜 침해적인 다른 대체수단을 통해서 수행할 수 있다면, 개인정보 자기결정권에 대한 일정한 제한에도 불구하고 연계정보가 필요하지 않느냐는 논리는 힘을 잃게 될 것이다. 이에 정보통신망법 상 연계정보의 처리를 허용하고 있는 경우를 중심으로, 해당 목적을 달성하기 위해 연계정보가 반드시 필요한 것인지, 해외 사례를 참조하여 검토해보고자 한다.

2. 미국 및 유럽의 신원확인 및 인증 체계

(1) 미국

미국은 유럽과 같이 연방 차원에서 신원 확인이나 인증을 규율하는 법률이 존재하지 않으며, 국립표준기술연구소(NIST)의 기술 표준을 중심으로 민간의 자율적인 생태계가 발전되어 있다. NIST는 디지털 신원 가이드라인(Digital Identity Guidelines)으로서 SP 800-63 시리즈를 발표하고 있는데, 가장 최근 버전은 2025년 7월에 발표한 네번째 개정

1) SP 800-63C-4. 우리나라의 본인확인기관을 신원 제공자(IdP), 본인확인기관에 본인확인을 요구하는 인터넷 서비스 사업자들을 서비스제공자(RP)라고 할 수 있다.

판(Revision 4)이다.[2] 이 가이드라인은 디지털 신원 솔루션의 신원 증명(identity proofing), 인증(authentication), 연계(federation) 시 요구되는 보증 수준을 달성하기 위한 절차와 기술적 요구사항을 다룬다. 보안과 프라이버시는 물론 고객 편의성까지 고려한다. 이 가이드라인은 디지털 신원 가이드라인(SP 800-63-4), 신원 증명 및 등록(Identity Proofing & Enrollment, SP 800-63A-4), 인증 및 인증수단 관리(Authentication & Authenticator Management, SP 800-63B-4), 연계 및 주장(Federation & Assertions, SP 800-63C-4) 등 4개의 문서로 구성된다. 여기서 연계(federation)은 서로 다른 시스템이 사용자의 신원 정보를 서로 공유할 수 있도록 신뢰 관계를 맺는 것을 의미한다. 주장(Assertions)은 연계된 시스템 사이에서 주고 받는 일종의 신원증명서(가령 여권과 같은)라고 할 수 있다. NIST 가이드라인 체제에서는 연계정보처럼 국가 인프라 차원에서 서로 전혀 무관한 수많은 서비스 제공자(Relying Party, RP)가 범용적으로 공통 사용하는 '전역 식별자(Global Identifier)' 체계는 존재하지 않는다. NIST는 여러 RP가 사용자의 동의나 인지 없이 식별자를 매개로 활동을 추적하고 프로파일링하는 것을 막기 위해 이를 지양한다. 서로 다른 시스템 간의 연계와 신원 주장의 문제를 다루고 있는 SP 800-63C-4 문서에 따르면, 신원 제공자(Identity Provider, IdP)와 RP 간의 데이터 전송 최소화를 요구하고 있으며, 이를 위해 여러 사이트에서 동일한 식별자를 사용하는 대신, 각 서비스마다 서로 다른 식별자(Pairwise Pseudonymous Identifiers)를 사용하도록 요구한다.

(2) 유럽연합

EU는 2014년 제정된 전자신원증명 및 신뢰 서비스(eIDAS 1.0)를 바탕으로 범유럽 차원의 전자신원, 전자서명 체계를 확립하였다. 과거에 EU는 '전자서명 지침'을 제정하여 국가별로 전자서명 관련 법률을 시행했으나 인증기관의 운영, 감독체계 및 인증사업자의 신뢰목록 프레임 차이 등으로 회원국들 간 전자서명을 인정하기 어려웠다. 이에 EU는 유럽 디지털 단일시장 형성을 위한 신뢰 기반 마련 정책의 일환으로 eIDAS를 규정으로 제정하여 회원국의 국내법으로서의 법적 효력을 갖게 하였다. 이에 따르면, EU의 각 회원국은 자국의 전자신분증(eID) 체계를 EU 집행위에 통지하고 정해진 보증등급(Low, Substantial, High)을 충족할 경우 다른 회원국의 행정 서비스에서도 이를 수용해야 한다.[3]

---

2) https://pages.nist.gov/800-63-4/

그러나 기술과 시장의 급속한 발전으로 유럽은 2024년 EU는 eIDAS 2.0 으로 개정하였다. 이는 첫째, eIDAS 1.0에서 국가별 전자신분증(eID)의 상호인정 원칙을 도입했지만 실제 도입은 제한적이었기 때문이다. 모든 회원국이 시스템을 통보한 것은 아니며, 민간 부문의 시스템 통합은 복잡하고 비용이 많이 들었다. 둘째, 1.0 규정은 스마트폰이 지배하는 세상을 염두에 두고 설계된 것이 아니기 때문에, 보편적이고, 이동 가능하며, 사용자가 제어할 수 있는 신원 확인 시스템이 부재했으며, 시민들에게 데이터에 대한 완전한 통제권을 부여하지도 못했다. 셋째, 글로벌 플랫폼의 영향력이 확대되면서 소셜 미디어 계정을 이용한 로그인이 사실상 시장 표준이 되면서, 개인정보 보호 및 사용자 활동 추적에 대한 심각한 우려를 불러일으켰다. 이러한 문제에 대한 해결책으로 제시된 것이 유럽 디지털 신원 지갑(EU Digital Identity Wallets)이다. EUDI 지갑은 각 회원국이 자국민과 기업에 제공해야 하는 자발적이고 안전한 모바일 애플리케이션 이다. 기존의 국가별 솔루션과 달리, 이 지갑은 완전히 표준화되어 상호 운용 가능하다. 시민들은 국가신분증, 운전면허증 등 자신의 신분증을 디지털 지갑에 저장할 수 있다. 또한, 소위 전자 속성 인증서 기능도 제공되는데, 여기에는 대학 졸업장, 전문 자격증, 보험 증권 확인서 등 모든 종류의 디지털 인증서가 포함된다. 더불어 은행 등 공공 및 민간 서비스를 제공하는 웹사이트에서 신원을 인증하는 데 사용할 수 있다.

EUDI 지갑은 시민들에게 자신의 데이터에 대한 완전한 통제권을 되돌려주는 것을 목표로 설계되었다. 플랫폼이나 서비스 제공자가 아닌 사용자가 지갑의 유일한 소유자가 되어, 지갑에 저장할 정보와 데이터의 범위, 그리고 어떤 정보를 누구와 공유할지 스스로 결정할 수 있다. 여기서 중요한 것은 "선택적 데이터 공개" 메커니즘이다. 예를 들어, 전자상거래 플랫폼에서 나이 확인만 필요한 경우, 사용자는 지갑을 통해 이름이나 정확한 생년월일을 공개하지 않고 나이 확인 정보만 제공할 수 있다.[4] eIDAS 2.0은 2024년 5월 20일에 발효되었으며, 2024년 11월에 지갑의 기술적 사양과 표준에 대한 '이행 입법(Implementing Acts)' 초안이 확정되었다. 이로부터 24개월 이내에 회원국은 EUDI 지갑을 개발, 인증하고 자국 시민들에게 무료로 제공해야 하는데, 그것이 2026년 11월이다. 또한 강력한 고객인증이 필요한 민간 부문(은행, 보험, 통신, 의료 등)과 대형 온라인 플랫폼은 EUDI 지갑을 인증 수단으로 수용할 의무가 발생한다.

---

3) 김연수, 김성훈(2025), 전자적 본인확인 수단의 주요 현황 분석 및 시사점, 2025.12. KISA Insight Vol.04

4) BGK(2025), eIDAS 2.0: What is the EU Digital Identity Wallet and how will it change business in the EU? 2025.5.12.

물론 EUDI 지갑 체제에서 각 국가의 개인식별정보는 해당 개인의 신원을 고유하게 나타내는 핵심 자격 증명으로 사용된다. PID(person identification data)에는 성, 이름, 생년월일 등 필수속성과 성별, 출생지, 거주지 주소 등 선택 속성이 포함된다. 사용자가 다른 국가의 서비스 제공자(RP)에 처음 접근할 때에는 대상 국가 고유의 신원 증명 절차를 거치고, 신원 확인이 성공하면 해당 국가는 자국에서 사용하는 고유 식별자가 포함된 속성 증명서를 사용자의 지갑으로 발급해준다.[5] 그러나 전 유럽 시민을 대상으로 하는 단일하고 영구적인 공통 고유 식별자(Unique Identifier)를 기본적으로 제공하지 않는다. 회원국은 사회보장번호나 납세자식별번호 등 자국의 국가 식별자를 통합하기 위해 국내 PID 네임스페이스를 정의할 수도 있다.[6] 법적으로 실제 신원 확인이 강제되지 않는 서비스의 경우 RP는 사용자의 신원을 직접 알 필요가 없으며, 이 경우 EUDI 지갑은 고유한 가명(pseudonym)을 생성하여 RP에 제공할 수 있다. 가령 인터넷 서비스 제공자가 이에 해당할 수 있는데, EUDI 지갑 체제에서는 서로 다른 인터넷 서비스 제공자에게 한국과 같이 연계정보라는 동일 식별자가 아니라, 서로 다른 개인식별자(Pairwise Identifier)를 제공하도록 한다.

3. 정보통신망법 상 연계정보의 처리가 허용되는 경우

본인확인기관은 원칙적으로 연계정보를 처리할 수 없지만, 제23조의5 제1항 각호에서 정하는 경우에는 예외적으로 연계정보를 처리할 수 있다. 예외로 규정되어 있기는 하지만, 한국 이용자의 온라인 활동 과정에서 일상적으로 발생하고 있는 경우이기 때문에, 사실상 전면적으로 연계정보의 처리가 허용되고 있다고 말할 수 있다.

정보통신망법 제23조의5 제1항 제1호에 따라 본인확인기관은 이용자가 입력한 정보를 활용하여 이용자를 안전하게 식별·인증하고자 하는 경우에는 연계정보를 생성·처리할 수 있다.[7]

---

5) NOBID consortium, Deliverable D9.1 Design of cross-border identification matching process, 2024.6.

6) PID Rule Book - European Digital Identity Wallet

7) 방송통신위원회, 한국인터넷진흥원(2025), 연계정보 처리 및 안전조치 등에 관한 안내서, 2025.6.

정보통신망 이용촉진 및 정보보호 등에 관한 법률
제23조의5(연계정보의 생성 · 처리 등) ① 본인확인기관은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 정보통신서비스 제공자의 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화한 정보(이하 “연계정보”라 한다)를 생성 또는 제공 · 이용 · 대조 · 연계 등 그 밖에 이와 유사한 행위(이하 “처리”라 한다)를 할 수 없다. 〈개정 2025. 10. 1.〉
1. 이용자가 입력한 정보를 이용하여 이용자를 안전하게 식별 · 인증하기 위한 서비스를 제공하는 경우
2. 「개인정보 보호법」 제24조에 따른 고유식별정보(이하 이 조에서 “고유식별정보”라 한다)를 보유한 행정기관 및 공공기관(이하 “행정기관등”이라 한다)이 연계정보를 활용하여 「전자정부법」 제2조제5호에 따른 전자정부서비스를 제공하기 위한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
가.「전자정부법」 제2조제4호에 따른 중앙사무관장기관의 장이 행정기관등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성 · 처리를 요청한 경우
나. 행정기관등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성 · 처리를 요청한 경우
3. 고유식별정보를 보유한 자가 「개인정보 보호법」 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성 · 처리를 요청한 경우
4. 「개인정보 보호법」 제24조의2제1항 각 호에 따라 주민등록번호 처리가 허용된 경우로서 이용자의 동의를 받지 아니하고 연계정보 생성 · 처리가 불가피한 대통령령으로 정하는 정보통신서비스를 제공하기 위하여 본인확인기관과 해당 정보통신서비스 제공자가 함께 방송미디어통신위원회의 승인을 받은 경우

우리가 인터넷 사이트에 회원 가입을 할 때 통상적으로 본인확인을 요구하며, 주로 휴대전화 본인확인 방법을 통해 이루어지는데, 이때 본인확인 과정에서 연계정보가 서비스 사업자에게 전달된다. 본인확인기관으로는 3개 신용평가회사(아이핀), 3개 이동통신사, 4개 신용카드회사, 13개 금융기관(인증서)이 지정되어 있다.

정보통신망법 제23조의5 제1항 제2호는 고유식별정보를 보유한 행정기관 등이 연계정보를 활용하여 전자정부 서비스를 제공하기 위한 경우로 (i) 중앙사무관장기관[8]의 장이 행정기관 등의 이용자 식별을 통합적으로 지원하기 위하여 연계정보 생성·처리를 요청한 경우, (ii) 행정기관 등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성·처리를 요청한 경우에 본인확인기관이 연계정보를 생성하거나 처리할 수 있다고 규정하고 있다. 〈연계정보 처리 및 안전조치 등에 관한 안내서〉

8) 중앙사무관장기관: 국회 소속 기관에 대하여는 국회사무처, 법원 소속 기관에 대하여는 법원행정처, 헌법재판소 소속 기관에 대하여는 헌법재판소사무처, 중앙선거관리위원회 소속 기관에 대하여는 중앙선거관리위원회 사무처, 중앙행정기관 및 그 소속 기관과 지방자치단체에 대하여는 행정안전부

에서 구체적인 사례를 제시하고 있지는 않지만, 정부24나 홈택스 등 전자정부 서비스에서 이용자의 신원을 확인하거나 서로 다른 기관 간에 동일인임을 확인할 필요가 있는 경우로 보인다. “행정기관등이 고유식별정보 처리 목적 범위에서 불가피하게 이용자의 동의를 받지 아니하고 연계정보 생성 · 처리를 요청한 경우”는 과태료 고지서를 모바일 고지를 통해 시민에게 전달하는 등 당사자의 동의를 받기 힘든 경우를 의미하는 것으로 보인다.

정보통신망법 제23조의5 제1항 제3호에 따라 본인확인기관은 고유식별정보를 보유한 자가 개인정보 보호법 제35조의2에 따른 개인정보 전송의무를 수행하기 위하여 개인정보 전송을 요구한 정보주체의 연계정보 생성·처리를 요청한 경우에는 연계정보를 생성·처리할 수 있다.

개인정보보호법 제35조의2는 정보주체가 대통령령으로 정하는 기준에 해당하는 개인정보처리자에게 자신 또는 개인정보관리 전문기관이나 일반 수신자에게 자신의 개인정보를 전송할 것을 요구할 수 있도록 하고 있다. 소위 ‘마이데이터’와 관련한 규정이다. 즉, 이 경우는 즉, 개인정보보호법 제35조의2에 따른 정보전송자[9]가 전송을 하기 전에 전송 요구자의 본인 확인을 위해서이다.

법 제23조의5 제1항 제4호에 따라 연계정보를 생성·처리하기 위하여는 ① 연계정보 이용 기관이 제공하고자 하는 정보통신서비스를 위한 주민등록번호의 처리가 개인정보 보호법에 근거하여 허용되어야 하며, ② 해당 서비스 제공을 위하여 이용자의 동의를 받지 않고 연계정보를 생성·처리하는 것이 불가피하여야 하고, ③ 나아가 본인확인기관과 정보통신서비스 제공자가 함께 방송통신위원회의 승인을 받아야 한다. 이는 대통령령에 규정되어 있어야 한다.

9) 현재 개인정보보호법 시행령 제42조의2에 따라 정보전송자로는 질병관리청 등 보건의료정보전송자, 모바일 사업자 등 통신정보전송자, 에너지정보전송자 등이 정보전송자로 지정되어 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률
시행령 제10조(연계정보 생성 · 처리가 불가피한 정보통신서비스) ① 법
제23조의5제1항제4호에서 “대통령령으로 정하는 정보통신서비스”란 다음 각 호의 어느
하나에 해당하는 정보통신서비스를 말한다. 〈개정 2025. 10. 1.〉
1. 법령에 따라 이용자에게 고지하는 사항을 「전자문서 및 전자거래 기본법」
제2조제10호에 따른 공인전자문서중계자를 통해 고지하는 서비스
2. 「신용정보의 이용 및 보호에 관한 법률」 제33조의2제1항에 따른 전송 요구에 따라
본인에 관한 개인신용정보를 같은 법 제2조제9호의3에 따른 본인신용정보관리회사를
통해 해당 신용정보주체 본인에게 전송하는 서비스
3. 제1호 또는 제2호와 유사한 서비스로서 방송미디어통신위원회가 법 제23조의5제1항
각 호 외의 부분에 따른 연계정보(이하 “연계정보”라 한다)의 생성 또는
제공 · 이용 · 대조 · 연계 등 그 밖에 이와 유사한 행위(이하 “처리”라 한다)가
불가피하다고 인정하여 고시하는 서비스

현재 대통령령은 위와 같이 서비스에 대해 규정하고 있는데, 첫째는 공인전자문서중계자를 통한 전자고지 서비스, 둘째는 신용정보보호법에 따른 소위 ‘금융 마이데이터 서비스’를 말하며, 3호와 관련된 고시는 아직 존재하지 않는다. 공공기관 문서의 전자고지 서비스의 경우, 제23조의5 제1항 제2호는 공공기관이 연계정보를 처리하는 근거, 제4호와 시행령 제1호는 본인확인기관과 해당 정보통신서비스 제공자가 연계정보를 처리하는 근거를 규정한 것으로 보인다.

법령 상으로는 '식별 · 인증하기 위한 서비스 제공', '전자정부서비스 제공' 등으로 되어 있지만, 연계정보는 개념 상 '정보통신서비스 제공자의 서비스 연계를 위하여' 사용된다. 즉, 굳이 서로 다른 정보통신서비스 제공자의 서비스 연계를 목적으로 하지 않는다면, 연계정보가 필요할 이유는 없다. 이때 서로 다른 정보통신서비스 제공자의 서비스 연계는 민간-민간, 공공-공공, 공공-민간으로 나누어 살펴볼 수 있다.

4. 본인확인 서비스 대체수단

우선 국내 대부분의 사이트들이 회원 가입시 본인확인을 하는 관행에서부터 되돌아볼 필요가 있다. 대다수 해외 사이트는 회원 가입시 엄격한 본인 확인을 하지 않는다. 이메일이나 휴대폰으로 일회용 비밀번호나 인증 코드를 발송해서 확인할 뿐이다. 공공기관이나 은행 등 오프라인의 실지명의가 중요한 경우를 제외하고, 대부분의 민간 사이트에서 회원의 실제 신원을 확인해야만 할 이유는 별로 없다. 배달을 위해서라면 배달이 필요한 시점에 주소 정보만을 수집하면 되고(또한 회원의 신원과 배달 주소에 거주하는 사람의 신원은 다를 수 있다), 결제를 위해서라면 결제 시점에 신원 확인을 하면 된다. 사실 회

원과 결제자의 신원이 같은 필요도 없으며, 거래 액수나 중요도에 따라 신원확인의 수준을 달리할 수도 있다. 이러한 본인확인 관행은 개인정보 맥락에서보면 필요 이상의 개인정보 수집으로서 목적 명확성 및 최소수집의 원칙에 위배된다.[10] 또한 비즈니스 측면에서도 이는 해외 이용자에게는 회원가입 자체를 원천 봉쇄하는 장벽이 되며, 해외 소비자가 국내 플랫폼을 통해 한국 상품을 구매하는 '역직구'를 위축시키는 요인이 되기도 한다.[11]

설사 동일인의 중복가입을 방지하기 위해 본인확인이 필요한 경우라도, 이는 '중복가입확인정보'(DI)면 충분하다. 이미 DI도 〈본인확인기관 지정 등에 관한 기준〉에서 규정하고 있다. DI는 CI와 마찬가지로 이용자의 주민등록번호를 암호화하여 만들어지지만, DI 생성에 웹사이트 식별번호도 사용되기 때문에, 동일인이라도 본인확인을 요구하는 웹사이트마다 서로 다른 DI 값을 갖게 된다. DI를 사용하면 CI보다 서로 다른 웹사이트 개인정보의 연계나 통합이 어려워질 수 있어, 개인정보 보호 측면에서 보다 바람직하다.

성인 사이트 등에서 이용자의 연령을 확인하기 위해 본인확인 서비스를 하는경우도 있다. 그러나 연령 확인을 위해서 반드시 이용자의 실제 신원 정보를 확인해야하는 것은 아니다. 단지 회원 또는 지금 접속하려는 이용자가 성인인지 여부만을 알 수 있으면 된다. 유럽의 EUDI 지갑은 데이터 최소화 원칙에 따라 신원확인 제공자가 디지털 서비스 제공자에게 꼭 필요한 이용자 정보만을 제공하도록 하고 있다.[12]

결국 어떤 인터넷 서비스 제공자가 회원의 본인 확인을 요구할 때, 다른 서비스 제공자와의 제휴 서비스 제공을 위한 경우가 아니라면, 연계정보가 제공될 필요는 없다. 이메일을 통한 보안 코드를 통해 실제하는 이용자인지 여부만을 확인하거나, 성인 서비스를 제

---

10) 이와 관련해서는 개인정보 감독기구인 개인정보보호위원회가 개인정보 보호원칙에 맞는 회원 가입 관행이 이루어질 수 있도록 계도할 필요가 있다.

11) 한국에 체류 중인 외국인의 상황도 크게 다르지 않다. 한국에서 본인인증을 하려면 통상 외국인등록번호와 한국 휴대전화 번호가 모두 필요하다(박유미, 2025). 그러나 외국인등록번호는 90일 이상 거주하는 외국인에게만 발급되기 때문에, 단기 체류자는 제도상 본인인증 대상에서 아예 배제된다. (최한별(2025), 외국인에게 닫힌 문, K-본인인증의 불편한 진실, 2025.12.15. KISO저널 제61호.)

12) EUDI 지갑의 프라이버시 및 보안 안내 사이트는 다음과 같이 설명하고 있다. "속성 선택적 공개 기능을 사용 하면 서비스 제공자가 요청한 특정 정보만 공유하고 불필요한 정보는 공개하지 않을 수 있습니다. 예를 들어, 속성 선택적 공개를 통해 생년월일만 공유하고 프로파일링에 사용될 수 있는 다른 식별 정보는 공개하지 않도록 선택할 수 있습니다. 그 결과, 다양한 디지털 서비스를 이용하면서도 개인정보 보호가 강화됩니다."
https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/712508927/Security+and+Privacy

공하기 위해 (전체 신원이 아니라) 성인인지 여부만을 확인하거나, 중복가입 여부를 확인하기 위해 굳이 실제 신원 정보를 확인할 필요가 있더라도 '중복가입확인정보'(DI)면 충분하다. 한국인만을 대상으로 서비스를 제공하는 것이 아니라면 실제 신원 정보를 확인하는 것은 현실적으로 불가능한 일이며, 거꾸로 이런 식의 신원 확인을 하는 것은 해외의 이용자를 배제하겠다는 선언이나 마찬가지다. 여튼 다른 기관과 연계하여 제휴 서비스를 제공하려는 것이 아니라면 굳이 연계정보를 수집할 이유가 없다.

그렇다면, 다른 기관과 제휴 서비스를 제공하기 위해서는 반드시 연계정보가 필요할까? 예를 들어, 항공사 마일리지를 쇼핑몰에서 사용할 수 있도록 하기 위해서는 항공사와 쇼핑몰이 동일 이용자를 확인할 수 있어야 한다. 이때 항공사와 쇼핑몰이 동일한 이용자를 식별하기 위해 공통의 식별자가 필요할 수 있고, 이때 연계정보가 그러한 역할을 할 수 있다. 2009년 방송통신위원회의 “인터넷상 주민등록번호 대체수단(i-PIN) 활성화 종합대책”에 따르면, 중복가입확인정보(DI)가 이미 있음에도 불구하고 연계정보를 만든 이유로 “제휴 서비스 불가, 오프라인 사용불가, 본인확인기관 간 연계 불가를 제시”한 바 있다.[13]

그러나 서로 다른 기관의 제휴를 위해 반드시 연계정보와 같은 공통 식별자가 필요한 것은 아니다. 예를 들어, 어떤 이용자가 A 항공사의 마일리지를 A 항공사와 제휴관계를 맺고 있는 B 쇼핑몰에서 사용하고자 한다. 이용자는 AI 항공사 계정으로 로그인하여 마일리지를 B 쇼핑몰에서 사용할 수 있는 '거래용 토큰'(또는 바우처)으로 교환한다. 이용자는 이 '거래용 토큰'을 갖고 B 쇼핑몰에서 상품을 구매할 수 있으며, B 쇼핑몰은 단지 이 토큰이 유효한 토큰인지 검증만 하면 될 뿐, 고객의 실명이나 항공사 고객번호 등을 확인할 필요는 없다. A 항공사와 B 쇼핑몰은 같은 고객인지 여부를 확인할 필요가 없으며, 따라서 동일한 고객 식별번호도 필요없다.[14] 주요 국가의 신원확인 및 인증방식도 연계정보와 같은 범용 개인식별자를 오히려 배제하고 있다.(아래 4절 참고)

따라서 서로 다른 업체의 제휴 서비스를 위해서도 반드시 연계정보가 필요한 것은 아니며, 또한 연계정보가 없더라도 업체 간의 제휴 서비스가 불가능해지는 것도 아니다. 연계정보와 같은 시스템이 없는 해외 기업들이 상호 제휴를 하지 않을리는 없다. 다른 것은 한국은 정부가 기업의 편의를 위해 연계정보라는 인프라를 제공했으며, 그 과정에서

---

13) 민간 서비스 업체의 제휴 방법까지 정부가 마련해준다는 것은 어처구니없는 일이지만, 이 문제는 별론으로 하자.

14) https://blog.naver.com/mnonz/223730912888

시민들의 개인정보 자기결정권은 전혀 고려하지 않았다는 점이다.

5. 전자정부 서비스의 제공 및 전자고지

EUDI 지갑은 비단 민간 뿐만 아니라 공공 분야의 다양한 서비스 제공을 위해 사용될 예정이다. 전자정부 서비스 제공을 위해서 사용될 수도 있다. EUDI 지갑 홈페이지에서 다양한 사용 사례를 소개하고 있는데[15], 여기에는 디지털 운전면허증, 디지털 공공서비스 접근, 비자 및 여권 등 여행문서 목적으로 활용될 수 있다고 제시하고 있다. 은행 업무를 위해 온라인에서 신원 확인을 하거나 약국에 제출할 처방전을 보관하기 위한 목적으로도 지갑을 활용할 수 있다고 한다. 물론 앞서 언급한 바와 같이 서비스 제공자에게 범용 식별번호는 제공되지 않으며, 서비스 제공자마다 서로 다른 개인식별자가 제공되거나 서비스 제공자가 원하는 특정 속성만 제공된다. 다만, EUDI 지갑은 아직 본격적으로 시행되고 있는 상황은 아니다.

영국은 부처별로 파편화되어 있던 인증 시스템을 통합하고, 시민들이 한 번의 신원 확인으로 모든 정부 서비스에 접근할 수 있도록 하는 'GOV.UK One Login' 프로젝트를 추진 중이다. 이 시스템은 세금, 여권, 유권자 등록 등 200개 이상의 서비스를 하나의 계정으로 연결한다.[16] 기술적으로는 업계 표준인 OpenID Connect(OIDC) 프로토콜을 기반으로 작동한다. 정부 서비스는 이 시스템에 등록할 때 섹터 식별자(sector identifier)를 설정하게 되는데, 개별 사용자 식별자는 이 섹터 식별자를 바탕으로 생성되는 '주체 식별자(subject identifier)' 또는 'pairwise user identifier'이다. 이에 따라 제한적인 같은 섹터 내에서는 사용자를 안전하게 식별한다.[17] 다만, 이는 개별 서비스나 특정 서비스 그룹 내에서만 사용되므로, 영국 정부는 수많은 정부 부처와 서비스 전반에 걸쳐 동일한 사용자임을 일관되게 식별할 수 있기 위한 '범용 고유 식별자(Universal Unique Identifier)'를 '고려중'이라고 한다. 이 식별자는 공공 부문 외부로는 노출되지 않으며 시스템 내부적으로만 작동하게 된다. 영국 정부는 공공기관의 고지를 위해 메시지 전송 서비스인 'GOV.UK Notify'를 제공하고 있는데, 이를 이용하기 위해서는 각 공공기관이 시민들의 연락처 정보를 자체적으로 보유하거나 수집해야 한다.

---

15) The many use cases of EU Digital Identity Wallets, https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/716146139/The+many+use+cases+of+the+EU+Digital+Identity+Wallet

16) Making public services work for you with your digital identity - GOV.UK

17) Choose your sector identifier - One Login technical documentation

호주는 myID라는 공공 서비스를 위한 디지털 ID 체계를 2019년에 도입하여 운영 중인데, 이는 호주 정부의 디지털 ID 앱으로 호주 국민이 온라인 서비스를 이용할 때 신원 확인을 위해 이용된다. 호주는 디지털 ID 체계를 강화하여 국민에게 더 나은 디지털 ID 경험을 제공하기 위하여 'Digital ID Act 2024' 제정하였는데, 인증된 디지털 ID 서비스 제공자는 강화된 개인정보보호 조치를 준수해야 하는데, 여기에는 단일 식별자 사용 금지 조치가 포함된다.[18] 호주의 전자정부 서비스는 myGov 이다. myGov 계정이 있으면 국세청, 자녀 양육비, 보건부, 메디케어, 노동청 등 다양한 정부 서비스를 이용할 수 있다. MyGov에서 공공기관의 고지를 SMS나 이메일 등 자신이 원하는 수단을 통해 받아볼 수 있다.[19] MyGov는 각 기관으로 연결해주는 통로(포털) 역할만 할 뿐, 개인 식별은 디지털 ID를 통해 이루어지며, 처음 서비스를 연결할 때 각 기관의 고유식별자와 MyGov 계정이 매칭되게 된다.

각국은 서로 다른 방식으로 전자정부 서비스를 제공하고, 온라인을 통해 시민들에 대한 고지 서비스를 제공하고 있다. 개인 식별자의 범용성이 커질수록 서로 다른 기관 간에 일관된 개인 식별이 가능하기는 하지만, 공공기관 내에서 서로 다른 식별자를 사용하더라도 전자정부 서비스의 제공이 불가능한 것은 아니다. 또는 전자지갑과 같이 개인이 통제하는 방식을 사용할 경우, 서로 다른 기관이 동일한 수단으로 신원을 확인하더라도 서로 다른 기관 사이에 직접적으로 개인정보를 공유할 필요는 없다.

각국 정부는 종이를 사용하지 않는 전자적인 방식의 고지 시스템도 도입하고 있고, 이는 바람직한 일이다. 영국이나 호주의 경우 공공 서비스에 시민들이 자신이 선호하는 메시지 전달 수단을 선택하도록 하고 있다. 덴마크의 경우 디지털 포스트(Digital Post)라는 전자정부 서비스 및 전자고지 서비스를 제공하고 있는데, 시민들은 이를 위한 앱이나 시스템을 통해 고지를 수신한다.[20] 한국의 전자고지 시스템은 시민들이 많이 쓰는 카카오톡이나 네이버, SMS 등을 통해 전달한다는 점에서 편리할 수 있다. 그러나, 공공기관이 특정한 민간 서비스에 특혜를 준다는 비판에서 자유로울 수 없다. 정부에서 의지를 갖고 홍보를 한다면, 시민들이 자신이 원하는 소통 수단을 선택할 수 있도록 하더라도 충분히 온라인 고지로의 전환을 달성할 수 있을 것이다.

---

18) NIA, 주요국 디지털 ID 추진현황 및 시사점, 2024-05.

19) https://my.gov.au/en/about

20) About the National Digital Post, https://en.digst.dk/systems/digital-post/about-the-national-digital-post/

6. 결론

국가적인 본인 확인 및 인증 제도는 국가적 식별번호 체계, 디지털 ID 체계, 전자서명 제도 등 다양한 문제들이 복잡하게 얽혀있는 이슈이기 때문에, 국가간에 제도를 수평적으로 비교하는 것도 쉽지 않다. 이 글에서 종합적인 현황과 비교 분석을 다루지는 못했으며, 단지 한국의 연계정보 제도가 추구하는 목적을 달성하기 위해 반드시 현재의 방식을 채택할 필요는 없다는 것을 보여주고자 하였다. 각국의 본인 확인 및 인증 제도는 상당히 다르고, 이는 각국의 역사적인 맥락을 반영하는데, 이러한 제도 수립 과정에는 효율성, 인권, 기술 수준 등 다양한 측면이 고려되게 된다. 이런 맥락에서 한국의 연계정보 제도는 비즈니스나 행정의 효율성에 지나치게 치우쳐있으며, 반면 인권적 측면과 개인정보 보호원칙은 거의 고려되지 못하고 있다. 그런데 유럽연합, 영국, 호주 등 각국은 새로운 기술 발전을 고려하여 자국의 신원확인 및 인증 시스템을 모두 개편하는 와중에 있다. 한국도 보다 장기적인 관점에서, 현재의 기술적 발전을 고려하여, 그리고 이번에는 시민들의 인권 보호와 균형을 맞추면서 신원확인 및 인증 시스템의 전면적인 개편을 도모할 필요가 있다.

바람직한 개편을 위해 다음과 같이 몇 가지 제안을 하고자 한다.

첫째, 국내 인터넷 환경은 필요 이상으로 본인확인에 기반하고 있다. 과도하고 불필요한 본인확인 관행부터 개선이 필요하다. 금융분야와 같이 강력한 본인확인이 필요한 영역이 아니라면 기본적으로 오프라인 신원에 기반할 필요도 없다. 이는 비즈니스적 측면에서도 외국인에 대한 장벽을 세우는 것이나 마찬가지다. 본인확인이 반드시 필요한 분야 외에는 해외와 마찬가지로 단순한 가입 절차로 대체되도록 하고, 본인확인을 안하더라도 연령이나 주소 등 필요한 정보만 제공받는 시스템으로 전환해나갈 필요가 있다. 불필요한 본인확인 자체가 개인정보보호법 위반이 될 수 있기 때문에, 이는 개인정보보호위원회에서 적극적으로 가이드를 제시하고 불합리한 관행이 개선될 수 있도록 할 필요가 있다.

둘째, 앞서의 제안과 연결되는 것이지만, 신원확인 및 인증을 보증이 필요한 수준에 따라 차이를 두는 방식으로 할 필요가 있다.

셋째, 연계정보와 같은 보편적 식별번호를 사용하는 것은 프라이버시 측면에서 매우 위험하다. 국가인권위원회에서도 권고한 바와 같이 공공기관 내에서도 목적에 따라 서로 다른 식별번호 체계를 사용하는 방식으로 개편하는 것이 가장 바람직할 것이다. 최소한 공공서비스 제공을 위해 사용되는 개인 식별번호가 민간에서는 사용되지 않도록 할 필요가

있다. EUDI 지갑 시스템과 같이 개인 식별번호를 공유하지 않더라도 사용자의 통제 하에 민간과 공동 부문이 필요한 정보를 연계할 수 있다.

넷째, 국내 본인확인 관련 법제는 여러 개별법, 시행령, 고시가 결합된 다층 구조를 이루고 있으며, 이를 관할하는 기관도 분산되어 있다.[21] 본인확인, 신원확인, 본인인증 등 용어로 혼란스럽게 사용되고 있으며, 신원 확인(identity proofing)과 인증(authentication) 개념이 혼재되어 있기도 하다. 또한, 이용자 편의나 개인정보 자기결정권 등 인권적 관점도 부재한 상황이다. 방송통신위원회(본인확인기관), 과기정통부(전자서명), 금융위원회(전자금융거래), 개인정보보호위원회(개인정보), 행정안전부(주민등록번호, 전자정부) 등 여러 부처가 관련되어 있어 일관성과 통일성을 확보하기 힘들기도 하다. 그렇기에 논의 자체가 힘들기도 하지만, 그럼에도 불구하고 국내 신원확인, 인증 제도에 대한 통합적인 설계가 필요하다. ▢

---

21) 국내 본인확인 관련 법제는 이용자의 개인정보 보호와 신뢰성 있는 인증서비스 제공이라는 목표 달성을 위해 단일법이 아니라 여러 개별법·시행령·고시가 결합된 다층 구조를 이루고 있음.
각 법령은 적용 대상과 분야에 특화된 규율을 마련함으로써 세부적인 정책 목표를 달성해왔으나, 동시에 범분야에 걸친 일관성 확보라는 과제를 이행

- (정보통신망법 및 하위 고시) 온라인 실명확인을 위한 본인확인기관 지정 기준, 휴대폰·PASS·아이핀 등 대체 본인확인수단의 기술·관리 요건을 규정함
- (전자서명법) 전자서명의 법적 효력, 전자적 신원확인 수단으로서의 역할, 전자서명인증사업자의 보안·신뢰기준을 규정하면서 기술 중립적 전자서명 체계를 도입함
- (개인정보보호법) 주민등록번호 등 고유식별정보 처리 제한, 본인확인 과정에서 처리되는 개인정보의 안전성 확보 의무를 규율함
- (주민등록법) 주민등록증의 법적 효력, 발급·확인 절차를 규정하고, 모바일 주민등록증 근거를 마련함
- (전자금융거래법 및 감독규정) 금융회사가 계좌 개설·전자지급거래 시 고객에 대한 본인확인 의무(KYC)를 부담하도록 하고, 위험도에 따라 OTP, 간편인증 등 다양한 인증수단을 허용하는 방향으로 활용
- (도로교통법) 모바일 운전면허증의 추가 발급과 효력을 규정하며, 모바일 운전면허증의 법적 효력을 명시함

(김연수, 김성훈(2025), 전자적 본인확인 수단의 주요 현황 분석 및 시사점, 2025.12. KISA Insight Vol.04)

보론: 연계정보(CI)에 대한 정보주체 권리 행사 경과

1. 근거 법령

개인정보보호법
제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

개인정보보호법 시행령
제41조(개인정보의 열람절차 등)
② 개인정보처리자는 제1항에 따른 열람 요구 방법과 절차를 마련하는 경우 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 다음 각 호의 사항을 준수하여야 한다.
1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다. 이 경우 공공기관에 대해서는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구하거나 개인정보 처리에 대한 동의를 철회할 수 있다.
② 개인정보처리자는 제1항에 따른 처리정지 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.
1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명 · 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
③ 개인정보처리자는 정보주체가 제1항에 따라 동의를 철회한 때에는 지체 없이 수집된 개인정보를 복구 · 재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다. 다만, 제2항 각 호의 어느 하나에 해당하는 경우에는 동의 철회에 따른 조치를 하지 아니할 수 있다.
④ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하거나 제3항 단서에 따라 동의 철회에 따른 조치를 하지 아니하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.
⑤ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

2. 정보주체 권리 행사와 그 결과

○ 정보주체는 모두투어, 롯데카드 개인정보 유출사고 등에서 연계정보(CI)가 유출되었다는 언론보도를 접하였음. 그러나 해당 정보주체는 온라인 주민번호인 CI가 최초의 본인확인 목적을 넘어 여러 인터넷서비스에서 널리 공유되는 상황에 이르기까지 자신의 CI를 누가 언제 어떻게 처리하고 있는지는 물론, 누가 언제 생성하였는지조차 알고 있지 못한 상태임. 심지어 88byte에 달한다는 자신의 CI 원형이 어떻게 생겼는지도 본 적이 없었음.

○ 다만 일부 개인정보처리자는 개인정보처리방침에 CI 처리사실을 공개하고 있고, 가입자 본인확인 및 제휴사 연동 등의 목적으로 CI를 생성 및 처리하였을 것으로 추정되고 있음.

○ 이에 정보주체는 자신의 CI가 생성되고 처리되는 실태를 파악하고자, CI를 처리하는 복수의 인터넷서비스 제공자들과 CI를 생성하는 본인확인기관에 대하여 CI 처리의 목적, 제3자 제공 현황, 나아가 CI와 같이 본인확인 기능을 가진 DI의 처리 실태 및 CI 원형 등에 대하여 열람을 요구함.

○ 더불어 정보주체는 해당 업체 및 기관에 대하여 CI의 삭제 또는 처리정지를 요구하여 자신의 CI를 보호하고자 하였음.

2-1. CI 처리 일반

2-1-1. 열람권

(1) 요구 내용

1) 귀사가 보유하고 있는 본인의 연계정보(CI)를 수집, 이용, 제공 등 처리한 사실이 있는지 여부 1-1) 위와 같이 처리했다면 그 처리 일시, 처리 유형, 처리 목적, 보유 및 이용기간, 정보주체 동의 일시 또는 법적 근거, (제공의경우) 제공받는 자, 제공받는 자의 목적, 제공받는 자의 보유 및 이용기간 2) 귀사가 보유하고 있는 본인의 중복가입방지정보(DI)를 수집, 이용, 제공 등 처리한 사실이 있는지 여부 2-1) 위와 같이 처리했다면 그 처리 일시, 처리 유형, 처리 목적, 보유 및 이용기간, 정보주체 동의 일시 또는 법적 근거, (제공의경우) 제공받는 자, 제공받는 자의 목적, 제공받는 자의 보유 및 이용기간 3) 귀사가 수집 이용 / 처리 중인 본인의 CI 정보 원형(88byte)에 대한 열람

(2) 조치 결과

○ CI 처리 사실 및 목적

인터넷서비스제공자	CI 처리 목적
종합온라인쇼핑 A	이용자의 식별 및 서비스의 제공, 제휴사 회원 연동, 부정이용 방지
종합온라인쇼핑 B	서비스 이용에 따른 본인식별, 가입의사 확인, 연령제한 서비스 이용
전문온라인쇼핑 C	중복가입방지 (개인정보처리방침상 '이용자 동의 없이' 처리됨)
콘텐츠 플랫폼 D	서비스 이용을 위한 본인 확인
멤버십 플랫폼 E	멤버십 서비스 제공, 서비스 이용을 위한 본인 식별 및 확인

○ 제3자 제공

인터넷서비스제공자	제3자 제공
종합온라인쇼핑 A	제3자/위탁 제공내역 제공
종합온라인쇼핑 B	답변하지 않음
전문온라인쇼핑 C	처리사실 없음(본인확인사실 없음)
콘텐츠 플랫폼 D	제공사실 없음
멤버십 플랫폼 E	제3자 제공내역 제공

○ 중복가입정보(DI)의 처리 여부

인터넷서비스제공자	DI 처리사실
종합온라인쇼핑 A	DI 정보를 처리하지 않음
종합온라인쇼핑 B	처리 및 보관 (최초 본인인증 시점과 동의 시점에 대한 데이터는 보관기간이 초과되어 삭제 되었으며, 당시 식별된 CI/DI값을 보관하고 있음)
전문온라인쇼핑 C	처리사실 없음(본인확인사실 없음)
콘텐츠 플랫폼 D	처리 및 보관
멤버십 플랫폼 E	DI 수집저장 없음

○ CI 원형(88byte) 열람

인터넷서비스제공자	DI 처리사실
종합온라인쇼핑 A	탈퇴처리 후 즉시 파기되어 부존재
종합온라인쇼핑 B	열람조치
전문온라인쇼핑 C	처리사실 없음(본인확인사실 없음)
콘텐츠 플랫폼 D	열람조치
멤버십 플랫폼 E	열람조치

2-1-2. 처리정지권

(1) 요구 내용

향후에 본인의 CI 및 DI 처리에 대한 처리정지를 요구합니다. 그에 대한 회신을 주시고 불이익이 있을 경우 그 내용을 알려주시기 바랍니다

(2) 조치 결과

인터넷서비스제공자	조치 결과
종합온라인쇼핑 A	즉시탈퇴처리 사유: 필수정보 (이용자 식별 및 정상 서비스를 이용하기 위해, 당사 시스템에서 연계정보(CI)가 필수수집 정보인 이유로, CI 값 삭제 및 처리정지 시점을 기준으로 요청자의 계정이 탈퇴 처리됨)
종합온라인쇼핑 B	탈퇴처리방침 사유: 필수정보 (일부 서비스 이용 불가에 따라 정상적인 고객 서비스가 불가함으로 CI/DI 처리 정지가 필요한 경우 회원 탈퇴 등의 처리가 필요함)
전문온라인쇼핑 C	미해당
콘텐츠 플랫폼 D	개인정보 삭제(CI/DI 처리정지시 휴대폰번호도 동반 삭제 후, 휴대폰번호를 통한 아이디/비밀번호 재설정도 불가) 또는 탈퇴처리방침 사유: 처리정지 요청은 일괄 삭제 또는 탈퇴 처리 방침 ※처리방침에는 '선택정보'로 표시되어 있었으나 사실상 필수정보 취급

	(당사는 개인정보 처리정지 요청에 대하여 개인정보 초기화 또는 회원 탈퇴(3개월 보관 후 삭제)의 방법으로 조치를 취하고 있습니다. [처리정지에 따른 불이익 사항] CI 및 DI 처리정지(개인정보 초기화) 시 휴대폰 번호 및 본인인증 기록이 모두 사라지며, 향후 휴대폰 번호 또는 본인인증을 통해 아이디 찾기나 비밀번호를 재설정할 수 없습니다.)
멤버십 플랫폼 E	탈퇴처리방침 사유: 필수정보 (「개인정보 보호법」 제37조제2항제4호에 따라 / CI 회원정보 처리정지를 희망하실 경우, 서비스 이용에 필수적인 개인정보 처리를 진행할 수 없으므로 회원탈퇴 처리가 필요합니다.)

2-2. CI 생성

(1) 요구 내용

○ 일반적인 이용 목적으로 CI를 처리하는 기관과 별도로 CI를 생성하는 본인확인기관 X에 대하여 CI 생성사실, CI 원형, 제3자 제공 사실에 대한 열람 및 삭제/처리정지를 요구함

1. 정보주체 신청인 본인의 연계정보(CI)에 대하여 다음 정보의 열람을 조치하여 줄 것을 요구합니다. 1) 귀사가 본인의 연계정보(CI)를 생성한 사실이 있는지 여부에 대한 열람을 요구합니다 2) 위와 같이 생성했다면 본인의 CI 정보(88byte)에 대한 열람을 요구합니다 3) 본인의 CI를 제3자에게 제공한 일시, 정보주체 동의 일시 또는 법적 근거, 제공받는 자, 제공받는 자의 목적, 제공받는 자의 보유 및 이용기간에 대한 열람을 요구합니다 2. 본인의 CI에 대한 삭제를 요구합니다. 그에 대한 회신을 주시고 불이익이 있을 경우 그 내용을 알려주시기 바랍니다. 3. 만약 본인의 CI에 대한 삭제가 안된다면, 본인의 CI에 대한 제3자 제공의 처리정지를 요구합니다. 그에 대한 회신을 주시고 불이익이 있을 경우 그 내용을 알려주시기 바랍니다.

(2) 조치 결과

○ 본인확인기관 X는 요구 내용에 대하여 답변하지 않은 채 요구와 관련이 없는 아이핀 서비스 가입을 반복적으로 요구함.

1. 귀사가 본인의 연계정보(CI)를 생성한 사실이 있는지 여부에 대한 열람을 요구합니다
가. 당사에서 제공중인 NICE아이핀 서비스는 인증이 완료되면 이용자의 연계정보(CI)를 생성하여 인증처에 제공하고 있습니다.
최근 5년동안의 아이핀 인증이력은 아래 경로에서 확인하실 수 있습니다.
- www.niceipin.co.kr 접속 > '내 아이핀 설정' 버튼 클릭 > '이용내역' 메뉴 클릭 > 아이핀 인증 진행 > 이용내역 확인
2. 위와 같이 생성했다면 본인의 CI 정보(88Byte)에 대한 열람을 요구합니다
가. 고객님의 연계정보를 확인하기 위해,
아래 경로에서 본인 명의의 휴대폰으로 본인확인을 진행하신 뒤,
인증하신 시간과, 인증에 사용된 휴대폰 번호를 전달해주시기 바랍니다.
- NICE아이핀 홈페이지 > 아이핀 관리 > 좌상단 메인화면 ID/PW 찾기 > 휴대폰 본인확인
3. 본인의 CI를 제3자에게 제공한 일시, 정보주체 동의 일시 또는 법적 근거, 제공받는 자, 제공받는 자의 목적, 제공받는 자의 보유 및 이용기간에 대한 열람을 요구합니다.
가. 당사는 개인정보처리방침에 공개하고 있는 내용에 따라, 이용자의 연계정보(CI)를 제3자에게 제공하고 있습니다.
나. 고객님의 연계정보(CI)를 제3자에게 제공한 이력을 확인하기 위해,
'2-가'에서 안내드린 사항을 확인해주시기 바랍니다.
4. 본인의 CI에 대한 삭제를 요구합니다. 그에 대한 회신을 주시고 불이익이 있을 경우 그 내용을 알려주시기 바랍니다.
가. 연계정보(CI) 삭제를 희망하시는 경우, '2-가'에서 안내드린 사항을 확인해주시기 바랍니다.
나. 고객님의 연계정보(CI)가 확인되면, 연계정보(CI) 삭제 시 발생할 수 있는 영향범위를 안내드리도록 하겠습니다.

○ 그러나 정보주체는 이러한 조치가 다음과 같은 이유에서 부당하거나 위법하다고 봄.

○ 본인확인기관 X는 CI에 대한 열람을 위하여 해당 기관의 '아이핀' 서비스에 가입할 것을 요구함. 그러나 아이핀은 본 건 열람과 관계가 없으며, 정보주체가 아이핀 서비스에 가입하는 순간 CI 생성 및 처리에 대한 동의를 강제받을 것이 우려스러움.

○ 삭제 또는 처리정지에 대해서도 아무런 조치 없이, 정보주체에게 CI 확인을 선행할 것을 요구함. 정보주체가 본인확인기관 X에게 CI를 확인해 줄 것을 요구한 조치사항을 오히려 정보주체의 확인 사항이라며 엉뚱한 답변을 한 것임.

○ 위와 같은 경과로 정보주체는 본인확인기관 X에 대해 요구한 개인정보 열람, 삭제 및 처리정지에 대하여 제대로 된 답변을 받지 못하였으며, 이는 사실상 정보주체 요구에 대한 거절에 해당함.

○ 이에 정보주체는 본인확인기관X가 해당 정보주체의 개인정보인 CI에 대하여 정보주체가 요구한대로 열람, 삭제 및 처리정지를 조치하여 줄 것을 요구하며 개인정보분쟁조정위원회에 분쟁조정을 신청함.

(3) 개인정보분쟁조정 결과

안녕하세요. 개인정보 분쟁조정위원회입니다.귀하께서 신청해주신 개인정보 분쟁조정사건(26R02-00052)관련, CI생성 등 열람 및 처리정지 등에 관한 사항을 붙임과 같이 송부드립니다. 2026년 3월 26일 PM 4:38아울러, 피신청인 측에서는 실제로 주민등록번호로도 연계정보(CI)의 생성(인증) 내역을 확인할 수 있기에 신청인의 기존 접수 시 송부한 여권의 주민등록번호를 토대로 내역이 확인이 되었어야 하나, 그 당시 업무 담당자의 착오로 인해 추가 인증이 요청된 것으로 확인되었습니다. 이에 현재는 신청인께서 송부한 여권에서의 주민등록번호로 아래와 같이 인증 이력이 확인되었고, 신청인의 처리정지 요청에 따라 “나이스아아핀” 서비스에 대한 탈퇴조치가 완료되었음을 안내드립니다.이로써 신청인의 요청에 따른 조치가 이행되었기에 해당 사건을 종결처리하고자합니다.감사합니다.

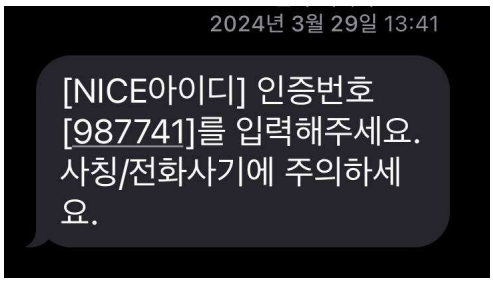
○ (열람) 요구한 사항 중 일부 내용만 열람되고 일방적으로 분쟁조정의 종결을 통보함 (1차례 통화를 통해 정보주체 의사를 전달하였음에도 조정에 반영되지 않았고, 조정 종결시에도 정보주체의 의사를 확인하지 않음)

서비스 명	가입시점	인증(가입)이력	탈퇴시점
나이스아이핀*	2024-10-31 17:24:37	최근 5 년 내 인증이력 없음	2026-03-23
나이스지키미**	미가입	최근 1 년 가입이력 없음	-
제휴서비스** (대납제휴/카드사/통신사)	미가입	최근 1 년 가입이력 없음	-

(*) 개인정보처리방침 및 전자상거래법에 따라 최근 5년 내 아이핀 인증이력 제공

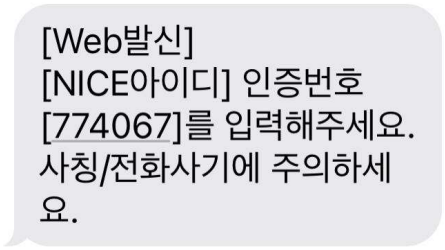
(**) 개인정보처리방침에 따라 최근 1년 내 지키미 및 제휴서비스 가입이력 제공

○ 그러나 위 내용조차 CI에 대한 내용이 아니라 “아이핀” 서비스의 가입에 대한 엉뚱한 답변임. 정보주체는 위 가입시점(2024. 10. 31. 17:24:37) 이전에도 인터넷서비스 이용과정에서 CI 생성 및 처리를 거쳤을 NICE 본인확인이 이루어진 기록이 있었음.



○ (처리정지) 처리정지 요청을 “나이스아이핀” 서비스에 대한 탈퇴조치로 처리하고 일방적으로 분쟁조정의 종결을 통보함.

○ 그러나 위 회신일(3월 26일) 이후 위 인터넷서비스(A~E 중 1곳)에서 본인확인 서비스를 진행해 본 결과(4월 4일) 여전히 NICE로부터 본인확인이 이루어지고 있는 것으로 확인되었음. 따라서 위 회신문의 CI정보의 “삭제”는 전혀 이루어지지 않았음.



○ 만약 삭제 후 CI가 재생성된 것이라 하더라도 정보주체는 그 사실과 구체적인 경위에 대하여 여전히 알 수 없으며, 동일한 규칙에 따라 생성된 CI의 원형은 이전과 완전히 동일할 것이기 때문에 탈퇴 이후에도 개인정보 유출 방지 효과가 전혀 없음.

3. 총평

○ (인터넷서비스 CI 처리 열람) 정보주체는 자신의 개인정보인 CI의 생성 및 처리 실태에 대하여 정확히 인지하거나 고지받고 있지 못함. 심지어 자신의 개인정보인 CI 원형(88byte)이 어떤 형태와 내용인지도 알고 있지 못함. 열람권 행사 후에야 일부 처리 실태에 접근할 수 있었으나, 일부에서는 정확한 CI 수집 시기에 대한 정보에 접근할 수 없었음.

○ (인터넷서비스 CI 처리정지) 사실상 정보주체에게 불이익한 탈퇴를 강제받고, 동의철회 또는 처리정지는 인정되지 않았음. CI 처리 목적 중 이용자 식별, 중복가입 방지의 경우 DI로 충분하다고 볼 수 있으며, 연령제한 서비스 역시 성인인지 여부(Yes/No)만 확인하면 충분함. 따라서, CI 처리가 필수가 아님에도 불구하고 대부분 CI를 필수정보로 분류하고 있었으며, 이에 따라 정보주체가 CI의 처리정지만을 요구하였음에도 아예 탈퇴 처리 방침을 통보받음.

○ (본인확인기관 CI 생성과 처리 열람 및 처리정지) 열람 및 처리정지 요구에 대해 자사 타서비스 가입을 요구하며 엉뚱한 답변을 함.

○ (개인정보분쟁조정제도) 정보주체의 의사가 반영되지 않았으며, 내용적으로도 형식적으로도 구제 접근이 이루어졌다고 보기 어려움. ▢

토 론

최경진 | 한국정보법학회 회장 (가천대학교 법학과 교수)

토 론

이상목 | 방송미디어통신위원회 디지털이용자기반과 사무관

토 론

김영훈 | 개인정보보호위원회 신기술지원과 사무관

메 모