보안 핫픽스 1~10차 변경 검토

보안 핫픽스 1~10차 변경 검토
사이트(회원) 화면 (stg)

서비스	보험유니버스 회원 사이트
접속 주소	https://s.insuniverse.com
환경	스테이징(stg) 서버. 실고객 데이터가 들어 있어 캡처의 개인정보는 가렸습니다.
대상	1~10차 보안 수정과 그 뒤 후속 수정이 회원 화면에서 무엇을 바꿨는지 확인합니다.
작성일	2026-10-21
작성	Claude Code (검토 요청에 따른 초안)

목차

1. 개요와 테스트 계정
2. 시나리오 1. 로그인
3. 시나리오 2. 회원정보 수정 (비밀번호 확인 단계)
4. 시나리오 3. 알림 목록 (본인 알림만)
5. 시나리오 4. 손해사정 (본인 목록과 타인 주소 차단)
6. 시나리오 5. 카드 목록 (더미 포함)
7. 시나리오 6. 카드 삭제 (더미 1장, 폐기 실패와 무관하게 진행)
8. 시나리오 7. 카드 삭제 실패 안내 (모의 응답)
9. 시나리오 8. 비밀번호 찾기 (본인인증과 탭 주소)
10. 시나리오 9. B2C 분석 공유 링크 (생년월일 확인)
11. 시나리오 10. 회원 게시판 문의 목록 (본인 글만)
12. 시나리오 11. 회원 게시판 타인 문의 주소 차단과 비노출 공지
13. 부록. 화면에 안 보이는 변경 — 실측 결과

1. 개요와 테스트 계정

이 문서는 보안 핫픽스 1차부터 10차까지의 수정과, 그 뒤 스테이징(stg) 서버에 배포한 후속 수정이 회원 사이트 화면에서 무엇을 바꿨는지 확인하는 절차입니다. 각 시나리오는 맨 앞에 바뀐 점(이전 → 지금)을 적었고, 그다음 목적·단계·그림·기대 결과·확인 포인트 순서로 이어집니다. 화면에 드러나지 않는 변경은 부록에서 요청 단위로 확인합니다.

이 문서가 다루는 변경

차수와 이름	바뀐 점	확인 방법
1차 토큰 종류 구분 (stg 반영 PR #99)	회원 API 가 갱신 토큰(refresh)을 받아들이지 않습니다. 로그인으로 받은 회원 토큰만 통과합니다.	시나리오 1, 부록
2차 무인증 개인정보 경로 (stg 반영 PR #98)	토큰 없이 진료 엑셀을 내려받을 수 없고, 다른 회원의 분석 조회가 403 으로 막힙니다.	부록
3차 비밀번호 재설정 결합 (stg 반영 PR #102)	본인인증을 거친 회원의 비밀번호만 바뀝니다. 인증 티켓은 10분 동안만 유효합니다.	시나리오 8, 부록
4차 회원 소유자 수정 (운영 재생)	다른 회원 번호로 카드를 조회·변경·삭제하면 403 입니다.	시나리오 5, 부록
5차 회원 소유자 대조 (stg 반영 PR #122)	알림·손해사정·FC 정보가 본인 번호로만 열립니다.	시나리오 3·4, 부록
6차 공개 분석 조회 (운영 이식 축)	쿠키와 토큰 없이 분석 결과를 조회할 수 없습니다. 공개 트리는 그대로 열립니다.	부록
7차 B2C 인증 쿠키 서명 (stg 반영 PR #122)	인증 쿠키가 고정 값이 아니라 분석 번호에 묶인 서명 값입니다. 꾸민 쿠키는 막힙니다.	시나리오 9, 부록
8차 개발용 인증 우회 차단 (stg 반영 PR #122·#124)	우회 헤더는 DEV_AUTH_BYPASS 가 true 일 때만 열리고, swagger 문서는 SWAGGER_ENABLED 가 true 일 때만 열립니다.	부록 (화면 확인 대상 아님)
9차 관리자 역할 경계	관리자 쪽 변경입니다.	관리자 화면 매뉴얼 (이 문서 범위 밖)
10차 카드 삭제 빌링키 폐기 (stg 반영 PR #122·#124·#127)	카드를 지울 때 토스 빌링키 폐기를 시도합니다. 폐기가 실패해도 카드는 지워지고 실패는 서버 오류 로그에 남습니다.	시나리오 6·7, 부록
후속: 서버 PR #124 (회원 게시판 경로)	회원용 게시판 상세 경로가 없어지고, 게시판 요청은 로그인한 회원 기준으로만 조회됩니다.	시나리오 10·11, 부록
후속: 서버 PR #128 (본인인증 창 연결)	본인인증 창의 결과가 찾기 화면에 전달됩니다. 보안 기능이 아니라 배포 변경입니다.	시나리오 8
후속: 사이트 PR #101 (카드 삭제 실패 안내)	삭제가 실패하면 실패 안내 창이 뜨고, 성공 창이 뜨지 않습니다.	시나리오 7

접속 주소와 테스트 계정

접속 주소	https://s.insuniverse.com (API: https://s-api.insuniverse.com)
아이디	회원 테스트 계정 1개. 값은 이 문서에 쓰지 않았습니다.
비밀번호	별도 전달
추가 인증	없음 (로그인 기준). 본인인증은 시나리오 8에서만 다루며, 이번 검토에서는 누르지 않았습니다.

공통 안내

- 저장·발송·비밀번호 변경·본인인증·신규 카드 등록·문의 저장 버튼은 누르지 않습니다. 되돌릴 수 없는 삭제는 검토용 더미 카드 1장에서만 실행했습니다(시나리오 6).
- 이동 주소는 참고용입니다. 메뉴에 있는 화면은 메뉴로 들어가고, 메뉴에 없는 화면은 주소창에 직접 입력합니다.
- 캡처 속 개인정보는 문서용으로만 가린 값입니다. 이름·아이디·휴대폰·카드 번호를 캡처 직전에 화면에서 ○○○○○ 또는 ****로 바꿔 찍었고, 실제 화면에서는 값이 그대로 보입니다. 확인 포인트는 실제 화면 기준입니다. 검토용 더미 데이터(「보안검토더미」)는 가리지 않았습니다. 빨간 박스 번호는 각 시나리오의 확인 포인트 번호와 같습니다.
- 건수는 2026-10-21 작성 시점 값입니다.

> 캡처 준비를 위해 stg 데이터베이스에 검토용 더미 행(회원·주문·구독·카드·공지 등)을 넣었습니다. 더미 행에는 「보안검토더미」 표식을 넣었습니다. 촬영이 끝난 뒤 넣은 행만 지웠고, 기존 행은 고치거나 지우지 않았습니다. 지금 stg 에 남은 더미 행은 없습니다.

시나리오 1. 로그인

> **바뀐 점(이전 → 지금)**
> 로그인 화면은 바뀌지 않았습니다. 바뀐 것은 로그인 뒤 회원 API 가 받는 토큰입니다. 이전에는 갱신 토큰(refresh)도 회원 API 를 통과했지만, 지금은 로그인으로 받은 회원 토큰만 통과합니다(1차 수정). 이 시나리오는 그 토큰으로 로그인이 정상 동작하는지 확인하는 출발점입니다.

목적	테스트 계정으로 회원 사이트에 로그인할 수 있는지 확인합니다.
사전조건	회원 테스트 계정의 아이디와 비밀번호를 받아 둡니다. 계정 값은 이 문서에 쓰지 않았습니다.

단계

1. 브라우저에서 `https://s.insuniverse.com/auth/login` 에 접속합니다 (그림 1-1).
2. 개인회원 탭에서 아이디 칸(그림 1-1의 **1**)에 테스트 계정 아이디를, 비밀번호 칸(그림 1-1의 **2**)에 비밀번호를 입력합니다.
3. 로그인 버튼(그림 1-1의 **3**)을 누릅니다.
4. 메인 화면이 열리면 헤더 오른쪽의 알림 아이콘(그림 1-2의 **1**)을 확인합니다.

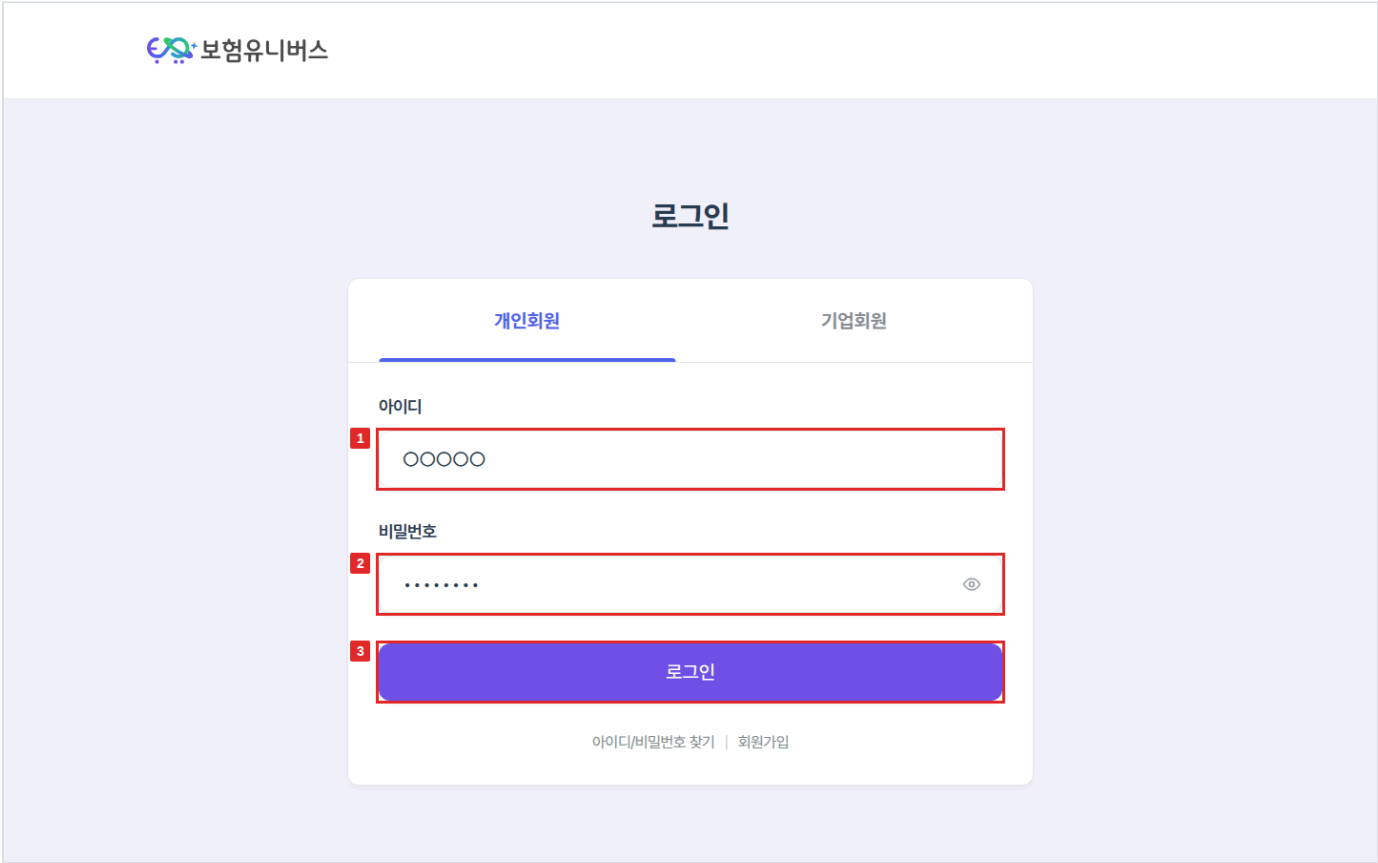


그림 1-1. 회원 로그인 화면. 개인회원 탭에서 아이디와 비밀번호를 입력한 상태입니다 (전체 화면, 아이디 가림).

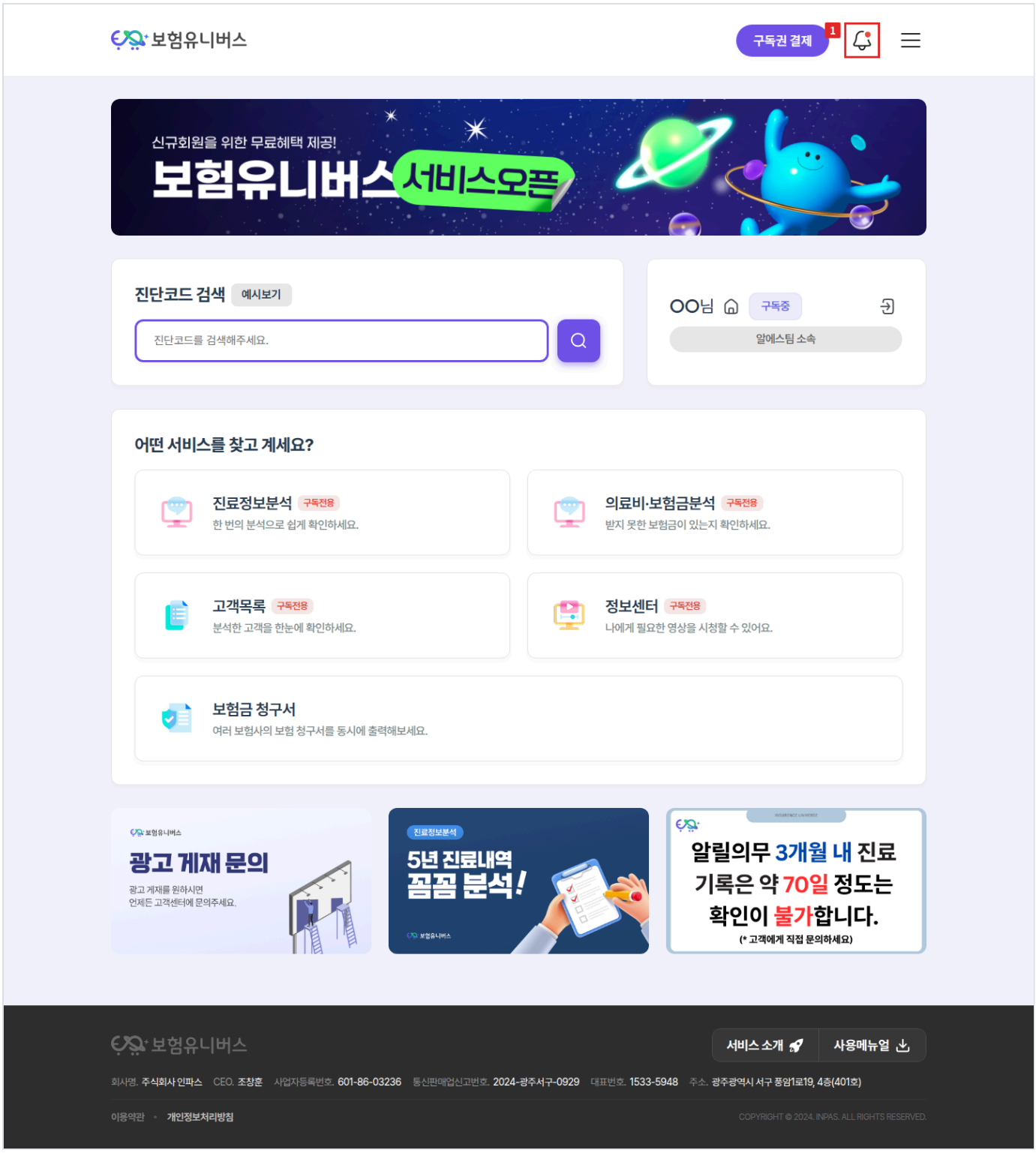


그림 1-2. 로그인 후 메인 화면 (전체 화면, 회원 이름은 ○○님으로 가림).

기대 결과

- 로그인 후 메인 화면(이동 주소: /main)으로 넘어가고, 로그인 실패 문구가 나오지 않습니다.
- 웹 로그인 화면에는 「로그인 유지」 칸이 없습니다.

확인 포인트 (그림 1-1)

1 아이디 칸: 입력한 아이디가 그대로 보이면 정상입니다. 그림의 가림은 문서용입니다.

2 비밀번호 칸: 값이 점(●)으로만 보이면 정상입니다.

3 로그인 버튼: 누르면 메인 화면으로 이동하면 정상입니다. 실패하면 「아이디 또는 비밀번호를 정확히 입력해 주세요.」가 나옵니다.

확인 포인트 (그림 1-2)

1 헤더 알림 아이콘: 헤더 오른쪽의 종 모양 아이콘이 보이면 정상입니다. 빨간 점은 읽지 않은 알림이 있다는 뜻입니다. 이 아이콘을 누르면 알림 목록이 열립니다 (시나리오 3).

> 이번 검토에서 하지 않은 확인: 로그인 상태에서 새로고침한 뒤에도 로그인이 유지되는지는 확인하지 않았습니다.

시나리오 2. 회원정보 수정 (비밀번호 확인 단계)

> **바뀐 점(이전 → 지금)**
> 화면과 입력 방식은 바뀌지 않았습니다. 이 화면이 쓰는 회원 요청도 회원 토큰 형상 검사(1차 수정)를 거칩니다. 이번 검토에서는 「저장」을 누르지 않고 화면 구성만 확인합니다.

목적	회원정보 수정으로 들어가면 비밀번호 확인 단계가 먼저 나오고, 통과하면 본인 정보가 채워진 2단계 화면이 열리는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태

단계

1. 마이페이지 메뉴에서 「회원정보 수정」을 누릅니다. 이동 주소: `/mypage/edit` (그림 2-1).
2. 비밀번호 확인 화면의 비밀번호 칸(그림 2-2의 **1**)에 본인 비밀번호를 입력하고, 「확인」(그림 2-2의 **2**)을 누릅니다.
3. 2단계 화면에 본인 정보가 채워져 있는지 확인합니다 (그림 2-3). 「저장」은 누르지 않고 화면을 떠납니다.



그림 2-1. 메뉴: 마이페이지 > 회원정보 수정 (메뉴 목록만 잘라 찍음)

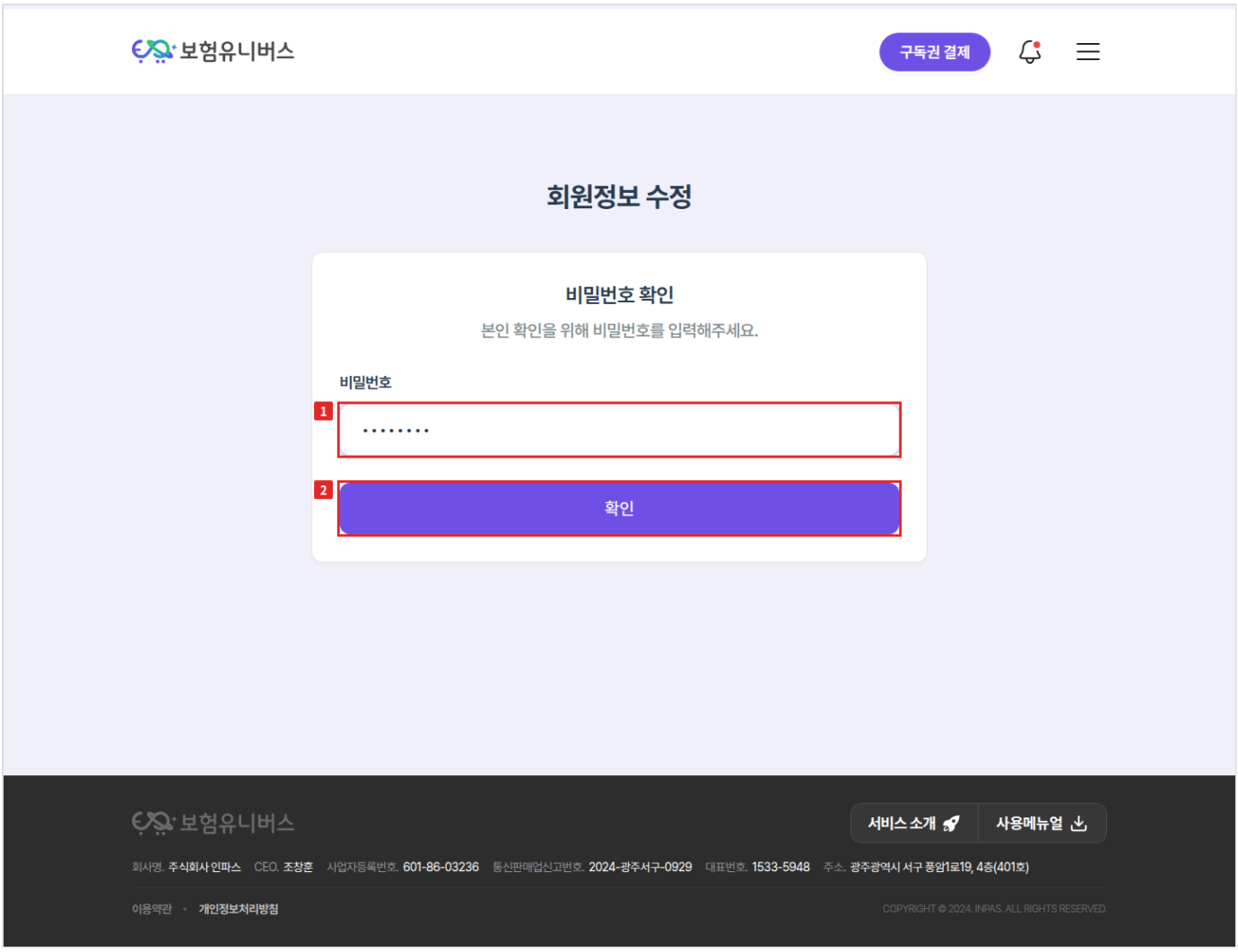


그림 2-2. 회원정보 수정 1단계: 비밀번호 확인 화면. 본인 확인용 비밀번호를 입력한 상태입니다 (전체 화면).

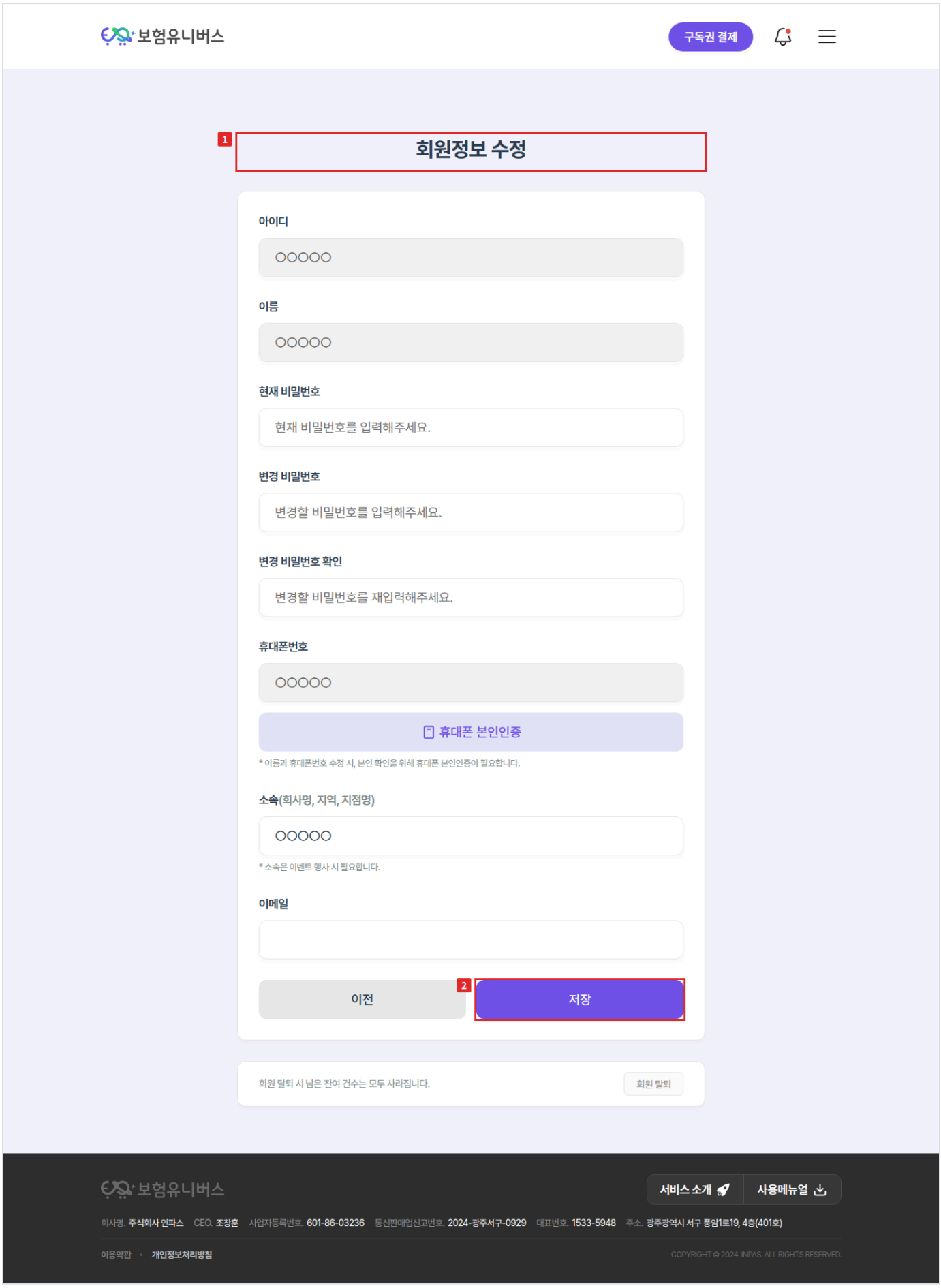


그림 2-3. 회원정보 수정 2단계: 본인 정보가 채워진 폼 (전체 화면, 아이디·이름·휴대폰·소속 값은 가림).

기대 결과

- 1단계에서 본인 비밀번호가 맞을 때만 2단계로 넘어갑니다.
- 2단계에서 아이디·이름·휴대폰·소속이 로그인한 본인 값으로 채워져 있고, 휴대폰 본인인증 안내가 보입니다.

확인 포인트 (그림 2-1)

1 「회원정보 수정」 메뉴 항목: 마이페이지 메뉴에 보이고, 누르면 회원정보 수정 화면(/mypage/edit)으로 이동하면 정상입니다.

확인 포인트 (그림 2-2)

1 비밀번호 입력 칸: 값이 점(●)으로만 보이면 정상입니다.

2 「확인」 버튼: 누르면 2단계로 넘어가면 정상입니다. 본인 비밀번호가 맞을 때만 넘어갑니다.

확인 포인트 (그림 2-3)

1 「회원정보 수정」 제목 아래 칸: 아이디·이름·휴대폰·소속이 로그인한 본인 정보로 채워져 있으면 정상입니다. 다른 회원의 정보가 보이면 이상입니다. 그림의 가림은 문서용입니다.

2 「저장」 버튼: **누르지 않습니다.** 저장하면 회원 정보가 바뀌므로, 이번 검토에서는 누르지 않고 화면을 떠납니다.

> 화면 아래의 「회원 탈퇴」 버튼도 누르지 않습니다.

시나리오 3. 알림 목록 (본인 알림만)

> **바뀐 점(이전 → 지금)**
> 이전에는 알림 목록 요청의 회원 번호(memId)를 바꾸면 다른 회원의 알림이 열렸습니다(운영 기준). 지금은 본인 번호만 열리고, 다른 회원 번호는 403 입니다(5차 수정). 화면에는 로그인한 회원의 알림만 보입니다.

목적	헤더 알림 패널에 본인 알림만 보이고, 탭 줄이 정상 동작하는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태. 알림이 몇 건 있어야 합니다.

단계

1. 메인 화면(이동 주소: /main) 헤더의 알림 아이콘을 누릅니다 (그림 3-1).
2. 패널이 열리면 항목 목록(그림 3-1의 **1**)과 탭 줄(그림 3-1의 **2**)을 확인합니다. 항목은 누르지 않습니다.



그림 3-1. 헤더 알림 아이콘을 눌러 연 알림 패널 (전체 화면, 알림 문구의 회원 이름은 ○○님으로 가림).

기대 결과

- 패널에 본인 알림 항목이 보이고, 「전체」 탭이 선택되어 있습니다.

확인 포인트 (그림 3-1)

1 알림 패널 전체: 패널 안에 알림 항목이 보이면 정상입니다. 모두 본인 알림이어야 합니다.

2 알림 탭 줄: 「전체」「결제」「분석」「팩스」「이벤트/혜택」 탭이 보이고 「전체」가 선택되어 있으면 정상입니다.

알림 읽음과 삭제는 쓰기 동작이라 이번 검토에서 누르지 않았습니다.

시나리오 4. 손해사정 (본인 목록과 타인 주소 차단)

> **바뀐 점(이전 → 지금)**
> 이전에는 손해사정 목록의 회원 번호(memId)만 바꿔 다른 회원의 신청 목록을 열 수 있었습니다(운영 기준). 지금은 본인 번호만 열리고 다른 회원 번호는 403 입니다(5차 수정). 다른 회원의 손해사정 주소(/loss/6)를 열면 본문이 없는 빈 화면이 나옵니다.

목적	본인 손해사정 신청 목록만 보이고, 다른 회원의 주소로는 내용이 나오지 않는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태. 본인 신청이 2건 있어야 합니다.

단계

1. 메뉴에 손해사정 항목이 없으므로 주소창에 직접 입력합니다. 이동 주소: `https://s.insuniverse.com/loss` (그림 4-1).
2. 신청 내역 목록에 본인 신청 2건이 있는지 확인합니다 (그림 4-1의 **1**). 「신청」 버튼은 누르지 않습니다.
3. 새 탭에서 다른 회원의 손해사정 주소 `https://s.insuniverse.com/loss/6` 를 엽니다. 본문이 없는 빈 화면인지 확인합니다 (그림 4-2).

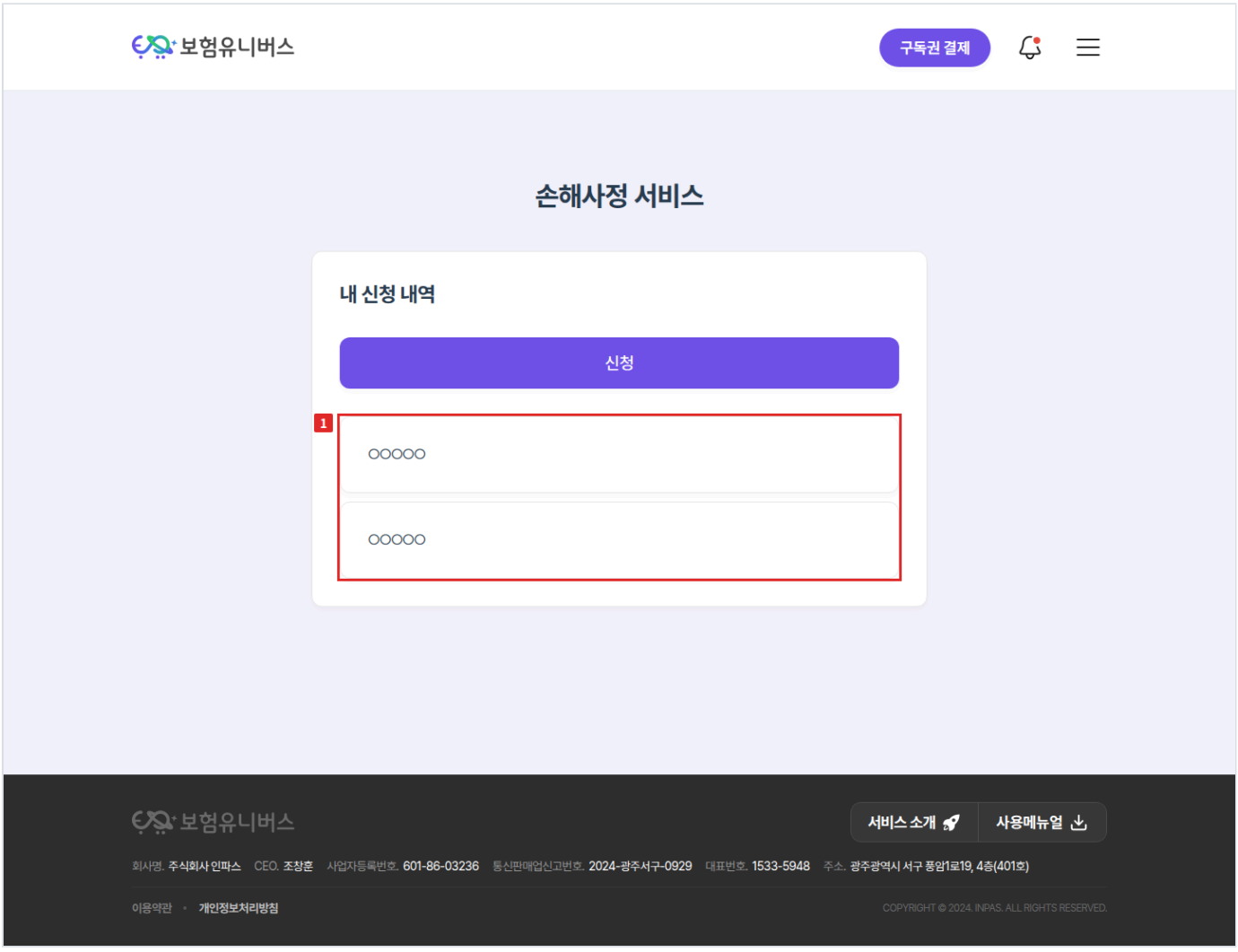


그림 4-1. 손해사정 서비스 목록: 주소 /loss 로 직접 들어간 화면입니다. 메뉴에는 항목이 없습니다 (전체 화면, 제목·날짜 가림).



그림 4-2. 다른 회원의 손해사정 주소(/loss/6)를 새 탭에서 열었을 때 화면 (전체 화면 크기, 빈 화면).

기대 결과

- 목록에는 본인 신청 2건만 있고, 다른 회원의 신청은 없습니다.
- 다른 회원 주소는 빈 화면이고, 「권한 없음」 같은 안내 문구는 나오지 않습니다. 주소창은 about:blank 로 바뀝니다.

확인 포인트 (그림 4-1)

1 신청 내역 목록 2건: 본인 신청 2건(예: 2건)이 보이면 정상입니다. 다른 회원의 신청은 목록에 없어야 합니다.

확인 포인트 (그림 4-2)

1 빈 화면 본문 전체: 본문이 없는 빈 화면이면 정상입니다. 신청 내용이 보이면 이상입니다. 같은 주소의 데이터 응답은 403 입니다 (부록).

> 「신청」 버튼은 새 신청을 만드는 쓰기 동작이라 누르지 않았습니다.

시나리오 5. 카드 목록 (더미 포함)

바뀐 점(이전 → 지금)
카드 목록 화면은 그대로입니다. 이전에는 회원 번호만 바꿔 다른 회원의 카드를 조회하고, 대표 카드를 바꾸고, 지울 수 있었습니다(운영 기준). 지금은 로그인한 회원 본인의 카드만 보이고, 다른 회원 번호는 403 입니다(4차 수정).

목적	구독 결제 수단 목록에 본인 카드만 보이고, 편집 모드로 바뀌는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태. 실카드 3장(토스뱅크카드 대표 1장, BC카드 2장)과 검토용 더미 카드 1장(「보안검토더미 (9001)」)이 있어야 합니다. 더미 카드는 시나리오 6에서 지웠습니다.

단계

1. 마이페이지 메뉴에서 「구독 결제 수단」을 누릅니다. 이동 주소: `/mypage/edit-payment-card` (그림 5-1).
2. 목록의 「카드 편집」 버튼(그림 5-1의 **3**)을 누르면 편집 모드로 바뀝니다 (그림 5-2).
3. 편집 모드에서 더미 행의 더보기(⋮) 버튼(그림 5-2의 **2**)이 있는지 확인합니다. 이 단계에서는 누르지 않습니다.

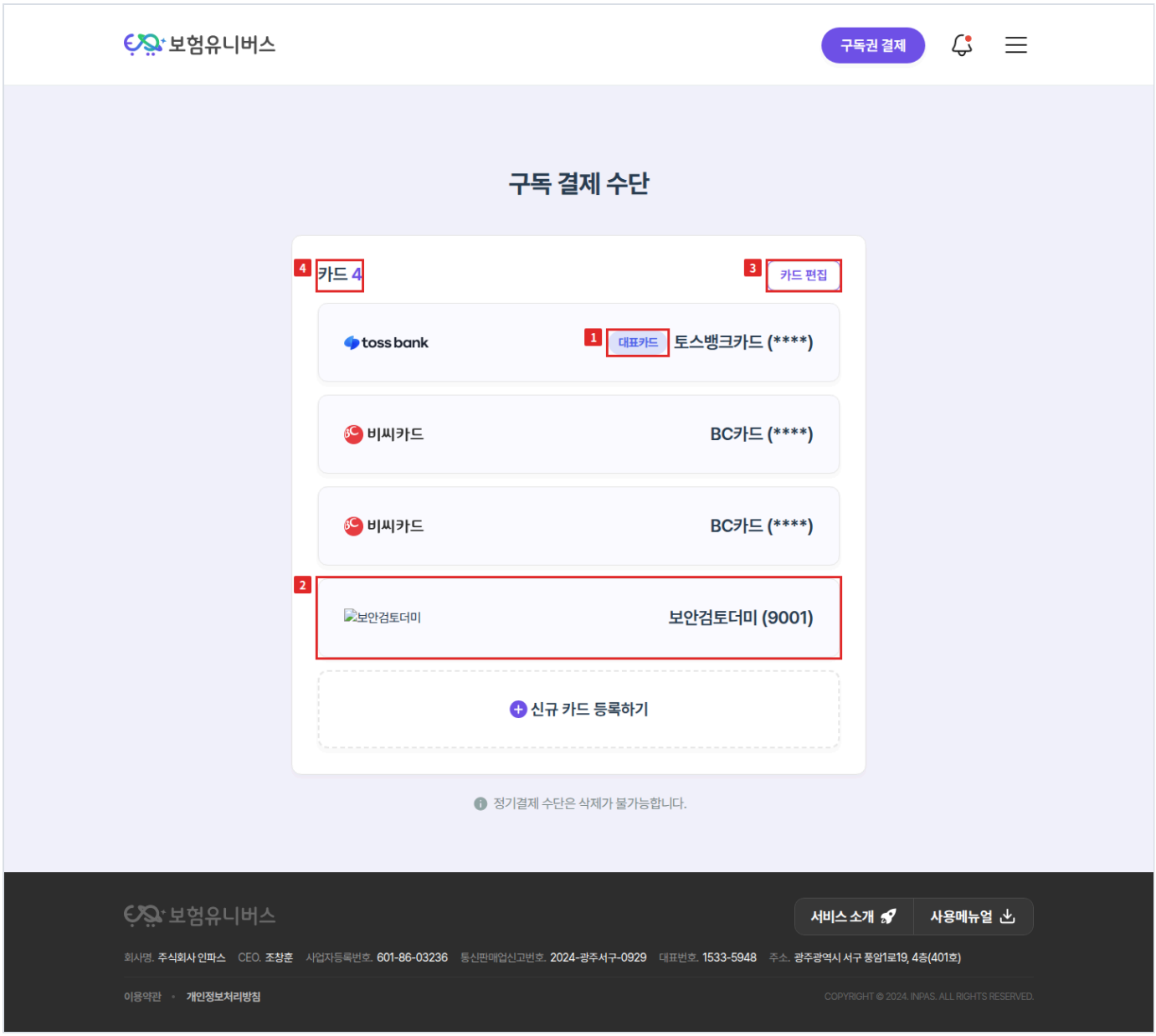


그림 5-1. 구독 결제 수단 목록 (전체 화면, 예시 데이터). 실카드 번호는 ****로 가렸고, 보안검토더미 행은 검토용 더미라 가리지 않았습니다.

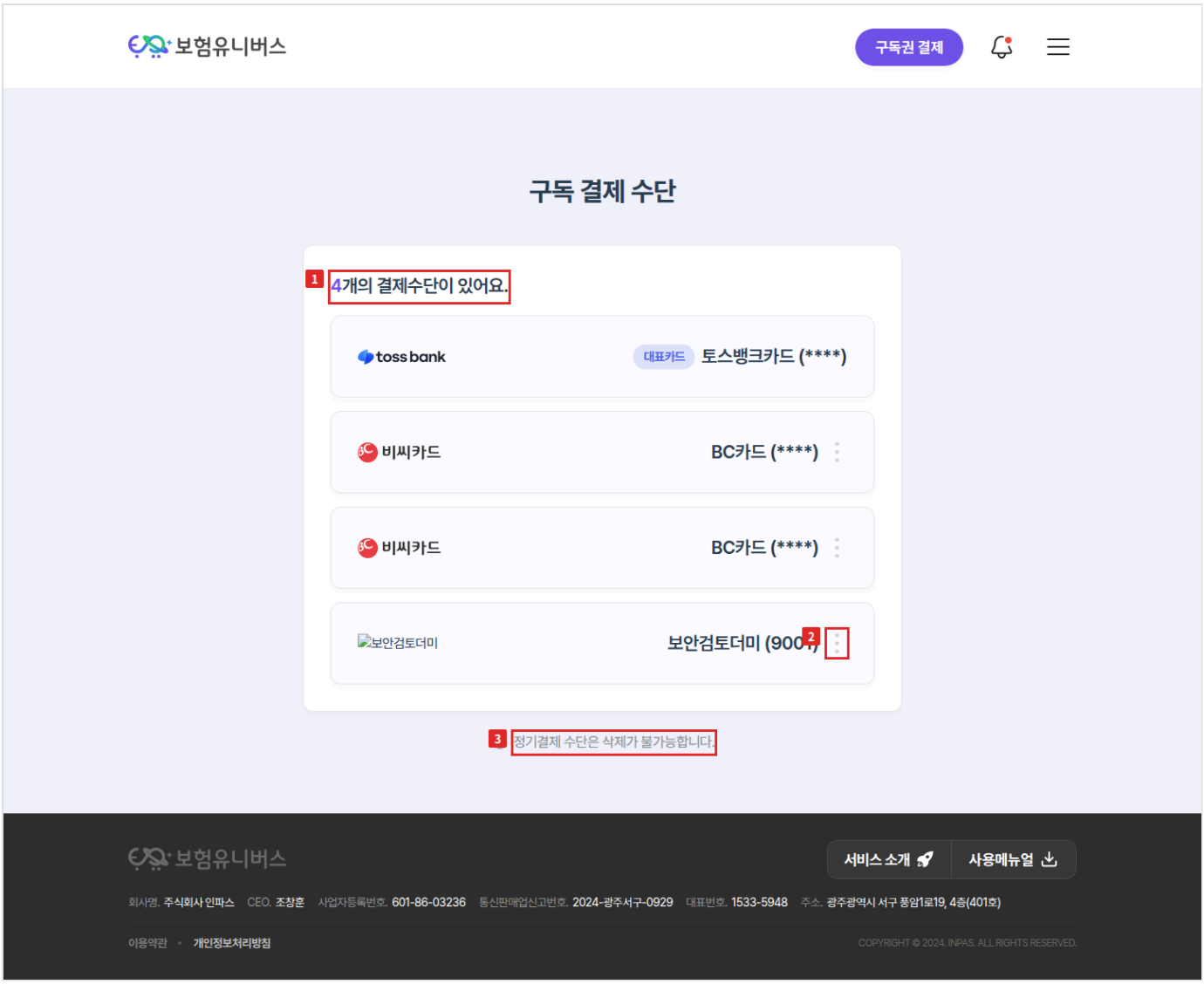


그림 5-2. 카드 편집 모드 (전체 화면, 예시 데이터). 실카드 번호는 ****로 가렸습니다.

기대 결과

- 카드는 4장입니다(실카드 3장과 검토용 더미 1장).
- 편집 모드에서 더보기(⋮)는 더미 행에만 있고, 첫 번째 대표카드 행에는 없습니다.

확인 포인트 (그림 5-1)

1 「대표카드」 태그: 첫 번째 카드에만 붙어 있으면 정상입니다.

2 4번째 행 「보안검토더미 (9001)」: 네 번째에 보이면 정상입니다. 이 행은 시나리오 6·7에서만 씁니다.

3 「카드 편집」 버튼: 보이면 정상입니다. 누르면 편집 모드로 바뀝니다.

4 「카드 4」 수 표시: 카드 수가 4 로 보이면 정상입니다 (실카드 3장 + 더미 1장).

확인 포인트 (그림 5-2)

1 「4개의 결제수단이 있어요.」 문구: 4개로 표시되면 정상입니다 (실카드 3 + 더미 1).

2 더미 행의 더보기(⋮) 버튼: 더미 행에 있으면 정상입니다. 첫 번째 대표카드 행에는 더보기 버튼이 없어야 합니다.

3 하단 안내 「정기결제 수단은 삭제가 불가능합니다.」: 안내 문구가 보이면 화면은 정상입니다. 다만 비대표 카드 삭제가 가능한 지금 동작과 문구가 맞는지는 검토자가 판단할 항목입니다.

> 「신규 카드 등록하기」는 외부 결제창이 열리므로 이번 검토에서 누르지 않았습니다.

시나리오 6. 카드 삭제 (더미 1장, 폐기 실패와 무관하게 진행)

바뀐 점(이전 → 지금)
이전에는 카드 행만 지우고 토스의 빌링키는 폐기하지 않아, 지운 카드의 정기결제 자격이 토스에 남았습니다. 10월 15일 정책은 폐기가 실패하면 카드를 남기고 500 을 돌려줬습니다. 지금은 폐기를 시도하고, 폐기가 실패해도 카드는 지워지며 화면은 성공으로 나옵니다. 실패 사실은 서버 오류 로그에 남습니다(10차 수정, 서버 PR #127).

목적	더미 카드 1장을 삭제했을 때 화면이 성공으로 나오고, 목록에서 그 카드만 사라지는지 확인합니다.
사전조건	시나리오 5와 같은 상태(검토용 더미 카드 1장이 있는 구독 결제 수단 목록). 실카드는 삭제하지 않습니다.

단계

1. 시나리오 5와 같이 구독 결제 수단 목록을 열고 「카드 편집」을 누릅니다.
2. 보안검토더미 행의 더보기(⋮) 버튼을 누르면 확인 창이 열립니다. 제목이 「보안검토더미(9001)카드」인지 확인합니다 (그림 6-1의 1).
3. 「카드 삭제」(그림 6-1의 2)를 누릅니다. 이 캡처에서는 더미 행에서만 눌렀습니다.
4. 「선택한 카드가 삭제되었습니다.」 창이 뜨는지 확인합니다 (그림 6-2의 1). 「확인」(그림 6-2의 2)을 누릅니다.
5. 목록이 다시 불러와지면 카드 수와 목록을 확인합니다 (그림 6-3의 1 · 2). 「신규 카드 등록하기」는 누르지 않습니다.

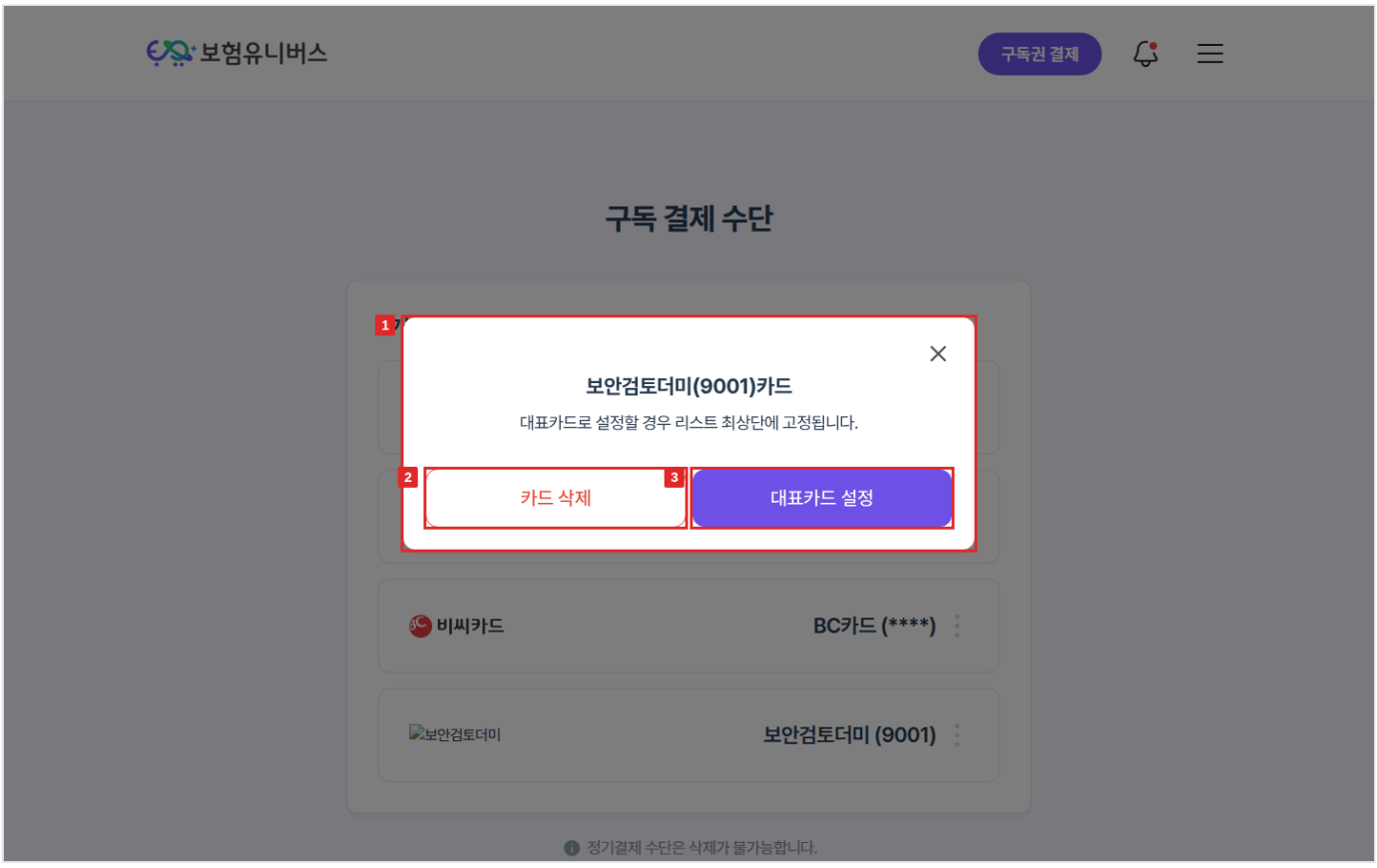


그림 6-1. 더미 카드(보안검토더미) 더보기 → 카드 삭제 확인 창 (전체 화면, 예시 데이터). 실카드 행은 열지 않았습니다.

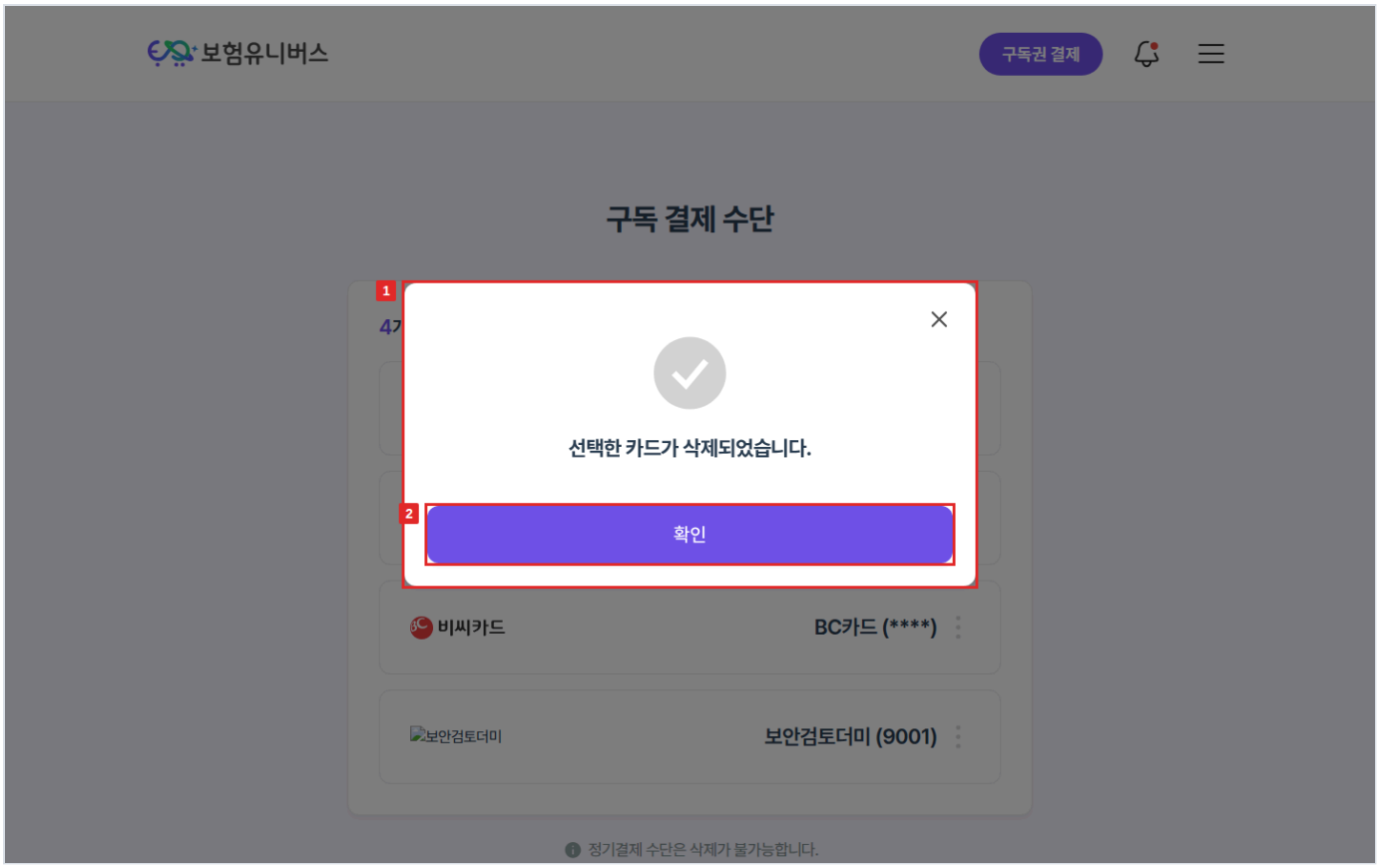


그림 6-2. 카드 삭제 뒤 성공 안내 창 (전체 화면, 예시 데이터). 뒤의 목록은 「확인」을 누른 뒤에 다시 불러와 갱신됩니다.

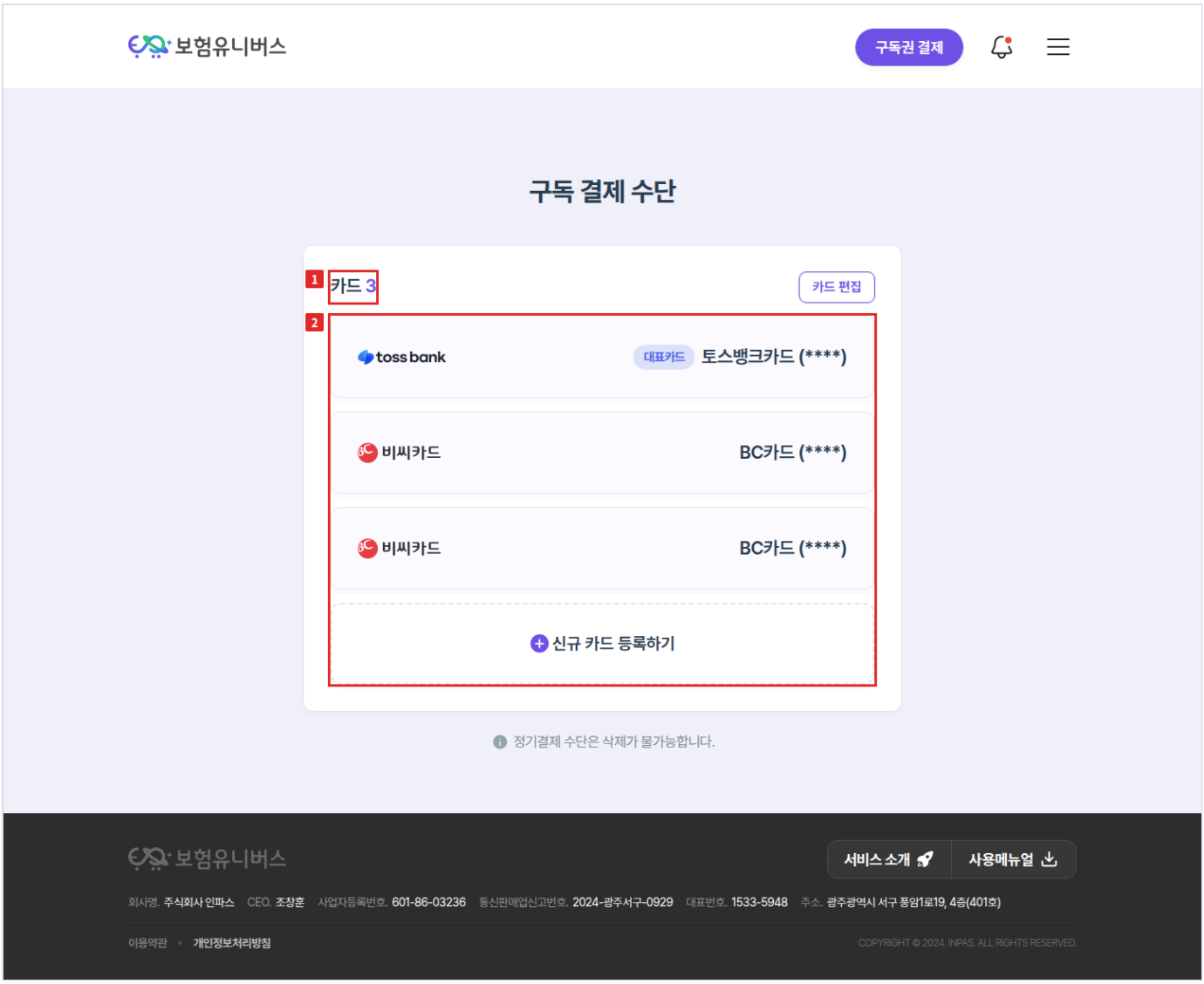


그림 6-3. 삭제 뒤 카드 목록 (전체 화면). 실카드 번호는 ****로 가렸습니다.

기대 결과

- 성공 안내 창이 뜨고, 「확인」 뒤에는 카드가 3장이 되며 더미 행이 사라집니다.

확인 포인트 (그림 6-1)

1 확인 창 전체: 제목이 「보안검토더미(9001)카드」로 보이면 정상입니다. 더미 카드인지 제목으로 확인한 뒤에만 「카드 삭제」를 누릅니다.

2 「카드 삭제」 버튼(빨간 글씨): 버튼이 보이면 정상입니다. 누르면 카드가 삭제됩니다.

3 「대표카드 설정」 버튼: **누르지 않습니다.** 이번 검토에서는 대표카드를 바꾸지 않습니다.

확인 포인트 (그림 6-2)

1 성공 안내 창: 「선택한 카드가 삭제되었습니다.」가 보이면 정상입니다. 이 더미 카드는 토스에 없는 키라 폐기는 실패하지만, 화면은 성공으로 나와야 합니다.

2 「확인」 버튼: 누르면 창이 닫히고 편집 모드가 해제되며 목록이 다시 불러와지면 정상입니다.

확인 포인트 (그림 6-3)

1 「카드 3」 수 표시: 카드 수가 3 으로 줄어 있으면 정상입니다. 토스뱅크카드(대표) 1장과 BC카드 2장이 그대로 남아야 합니다.

2 카드 목록 영역: 보안검토더미 행이 사라져 있으면 정상입니다.

> 이번 검토에서 더미 카드 삭제는 캡처를 다시 찍는 과정에서 세 차례 실행되었습니다. 세 번 모두 더미 행만 지웠고, 실카드 3장은 그대로 남았습니다. 서버 로그에 폐기 실패 기록이 남았는지는 확인하지 않았습니다.

시나리오 7. 카드 삭제 실패 안내 (모의 응답)

바뀐 점(이전 → 지금)
이전에는 카드 삭제 요청이 실패해도 「선택한 카드가 삭제되었습니다.」 성공 창이 떴습니다. 지금은 실패 안내 창이 뜨고, 「확인」을 누르면 편집 모드가 닫힙니다. 목록은 서버 응답이 실패일 때만 다시 불러오므로 카드 4장이 그대로 남습니다(사이트 PR #101). 실패 안내는 403, 서버 오류, 네트워크 실패에서만 뜹니다.

목적	삭제 요청이 실패했을 때 실패 안내가 뜨고, 성공으로 보이지 않는지 확인합니다.
사전조건	시나리오 5와 같은 상태(검토용 더미 카드가 있는 구독 결제 수단 목록). 이 시나리오는 브라우저에서 삭제 요청의 응답을 HTTP 500 으로 바꿔 찍은 모의 응답입니다. 서버와 DB 는 바뀌지 않았습니다.

단계

1. 시나리오 5와 같이 구독 결제 수단 목록을 열고 「카드 편집」을 누릅니다.
2. 보안검토더미 행의 더보기(⋮) 버튼을 누르고, 확인 창에서 「카드 삭제」를 누릅니다. 응답은 모의 500 입니다.
3. 실패 안내 창이 뜨는지 확인합니다 (그림 7-1의 1). 「확인」(그림 7-1의 2)을 누릅니다.
4. 편집 모드가 닫히고 목록이 4장 그대로인지 확인합니다 (그림 7-2).

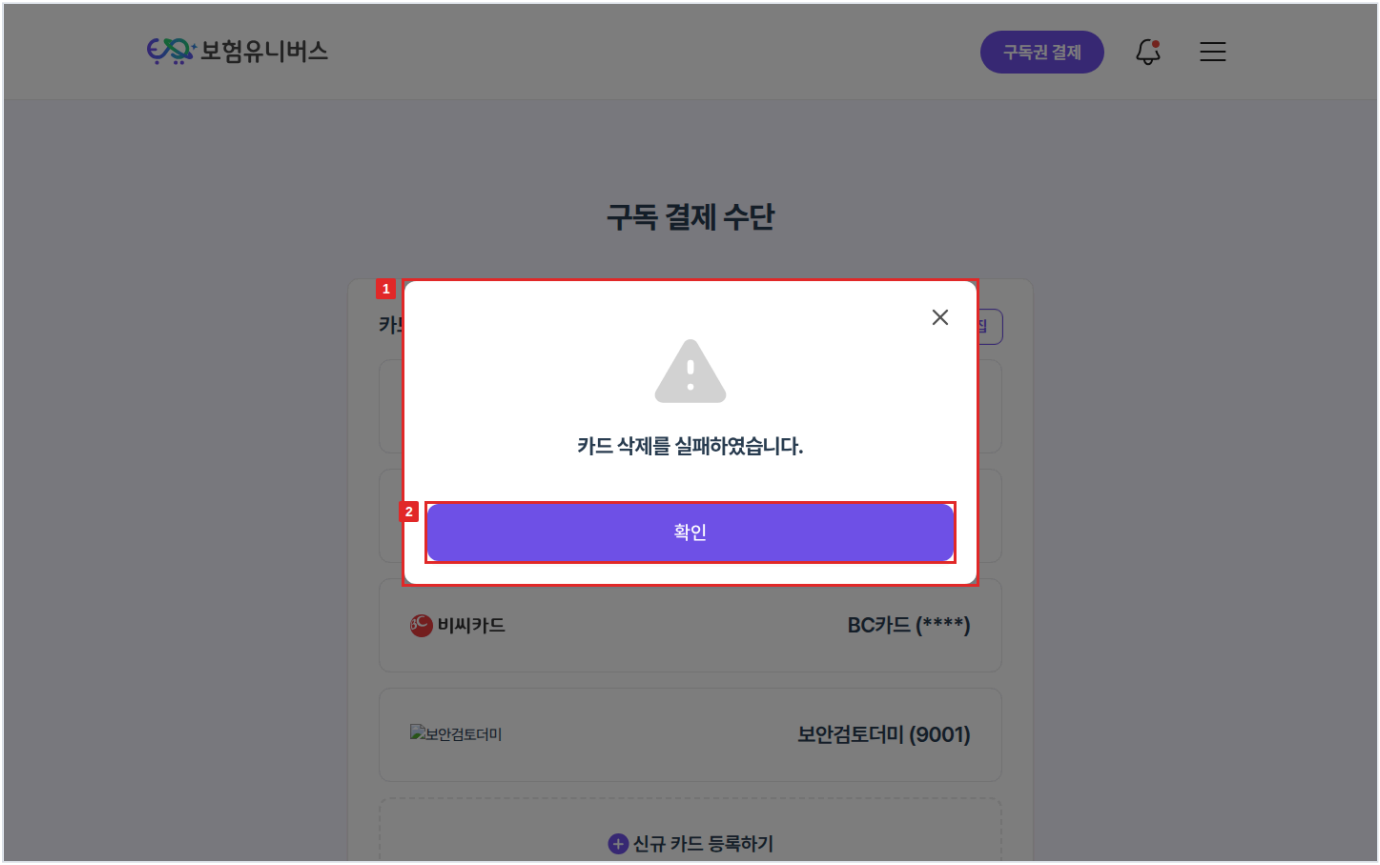


그림 7-1. 카드 삭제 실패 안내 창 (전체 화면, 예시 데이터, 모의 응답). 삭제 요청의 응답을 HTTP 500 으로 바꿔 찍었고, 서버와 DB 는 바뀌지 않았습니다.

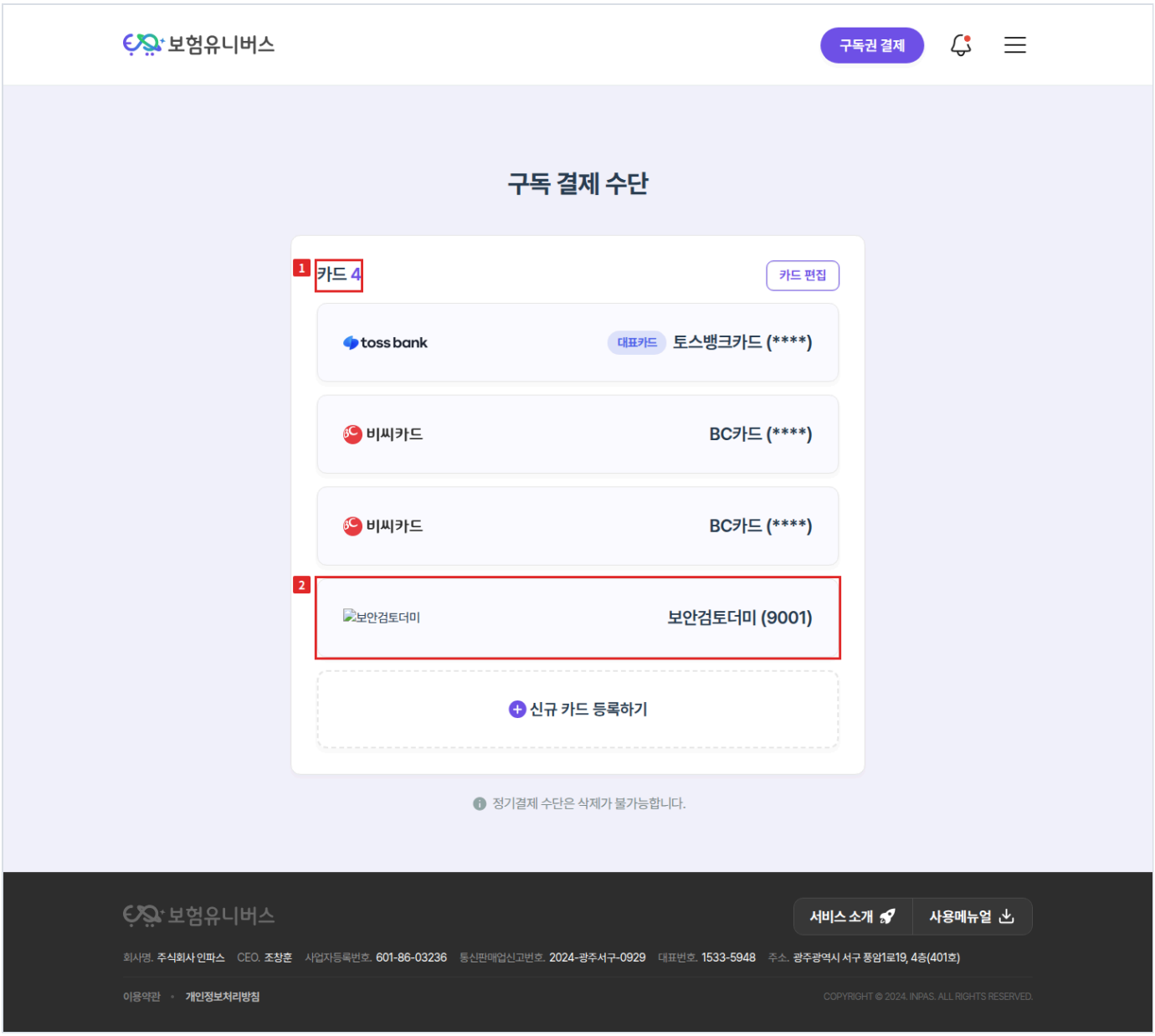


그림 7-2. 실패 안내를 닫은 뒤 카드 목록 (전체 화면, 예시 데이터). 모의 응답이라 더미 카드가 그대로 남아 있습니다.

기대 결과

- 「카드 삭제를 실패하였습니다.」 창이 뜹니다. 실패인데 「선택한 카드가 삭제되었습니다.」가 뜨면 이상입니다.
- 「확인」 뒤 편집 모드가 닫히고 카드 수는 4 그대로입니다. 서버에서 지워지지 않았기 때문입니다.
- 보안검토더미 행은 목록에 그대로 보입니다.

확인 포인트 (그림 7-1)

1 실패 안내 창: 「카드 삭제를 실패하였습니다.」 창이 뜨면 정상입니다.

2 「확인」 버튼: 누르면 창이 닫히고 편집 모드가 닫히면 정상입니다.

확인 포인트 (그림 7-2)

1 「카드 4」 수 표시: 카드 4 그대로 보이면 정상입니다. 서버에서 지워지지 않았기 때문입니다.

> 모의 응답이므로 서버 로그에는 이 요청이 남지 않습니다. 이 시나리오는 화면이 실패를 어떻게 보여 주는지만 확인합니다.

시나리오 8. 비밀번호 찾기 (본인인증과 탭 주소)

바뀐 점(이전 → 지금)
이전에는 로그인 ID 와 새 비밀번호만 보내면 비밀번호가 바뀌었고, 같은 로그인 ID 의 기업 회원 비밀번호도 함께 바뀌었습니다. 지금은 본인인증의 이름과 휴대폰이 맞는 일반 회원만 10분짜리 티켓을 받으며, 바뀌는 것은 그 회원 한 명의 비밀번호뿐입니다(3차 수정). 본인인증 창의 결과는 찾기 화면에 전달됩니다(서버 PR #128).

목적	비밀번호 찾기 탭과 본인인증 입력 칸이 보이고, 탭 주소가 유지되는지 확인합니다.
사전조건	로그아웃한 상태에서 시작합니다. 본인인증 창은 열지 않습니다.

단계

1. 로그인 화면(시나리오 1 그림 1-1)의 「아이디/비밀번호 찾기」를 누릅니다. 이동 주소: `/auth/find`. 기본으로 「아이디 찾기」 탭이 선택되어 있습니다 (그림 8-1).
2. 탭 줄의 「비밀번호 찾기」(그림 8-1의 **1**)를 누릅니다. 주소 뒤에 `?type=pw` 가 붙습니다.
3. 같은 주소를 직접 열면 「비밀번호 찾기」 탭이 선택된 상태로 열립니다 (그림 8-2). 입력 칸(그림 8-2의 **2** · **3** · **4**)을 확인합니다.
4. 「인증하기」(그림 8-2의 **5**)는 **누르지 않습니다.** 누르면 외부 본인인증 창이 열립니다.

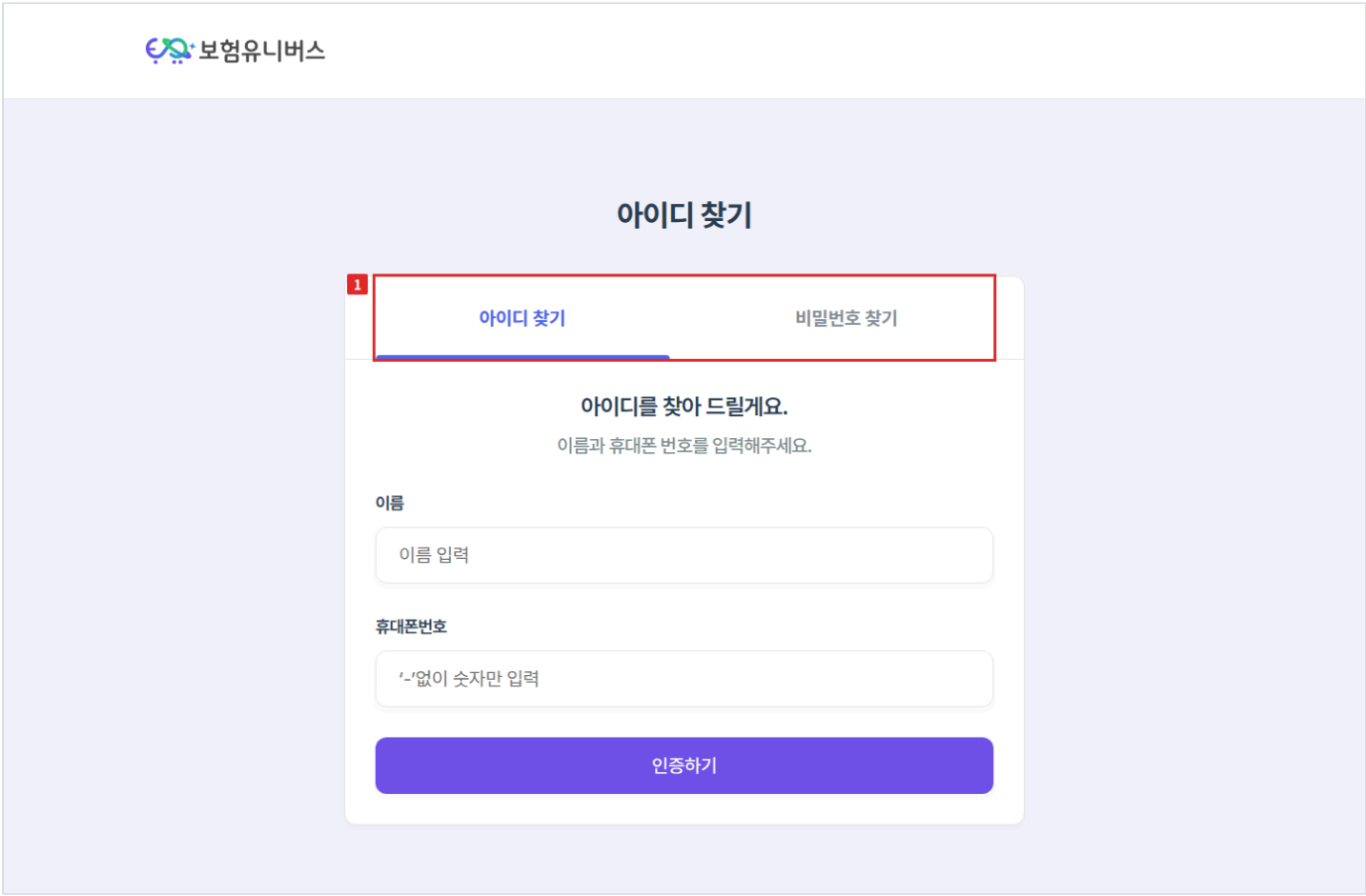


그림 8-1. 아이디/비밀번호 찾기 화면 (주소 /auth/find, 전체 화면). 기본으로 「아이디 찾기」 탭이 선택되어 있습니다.

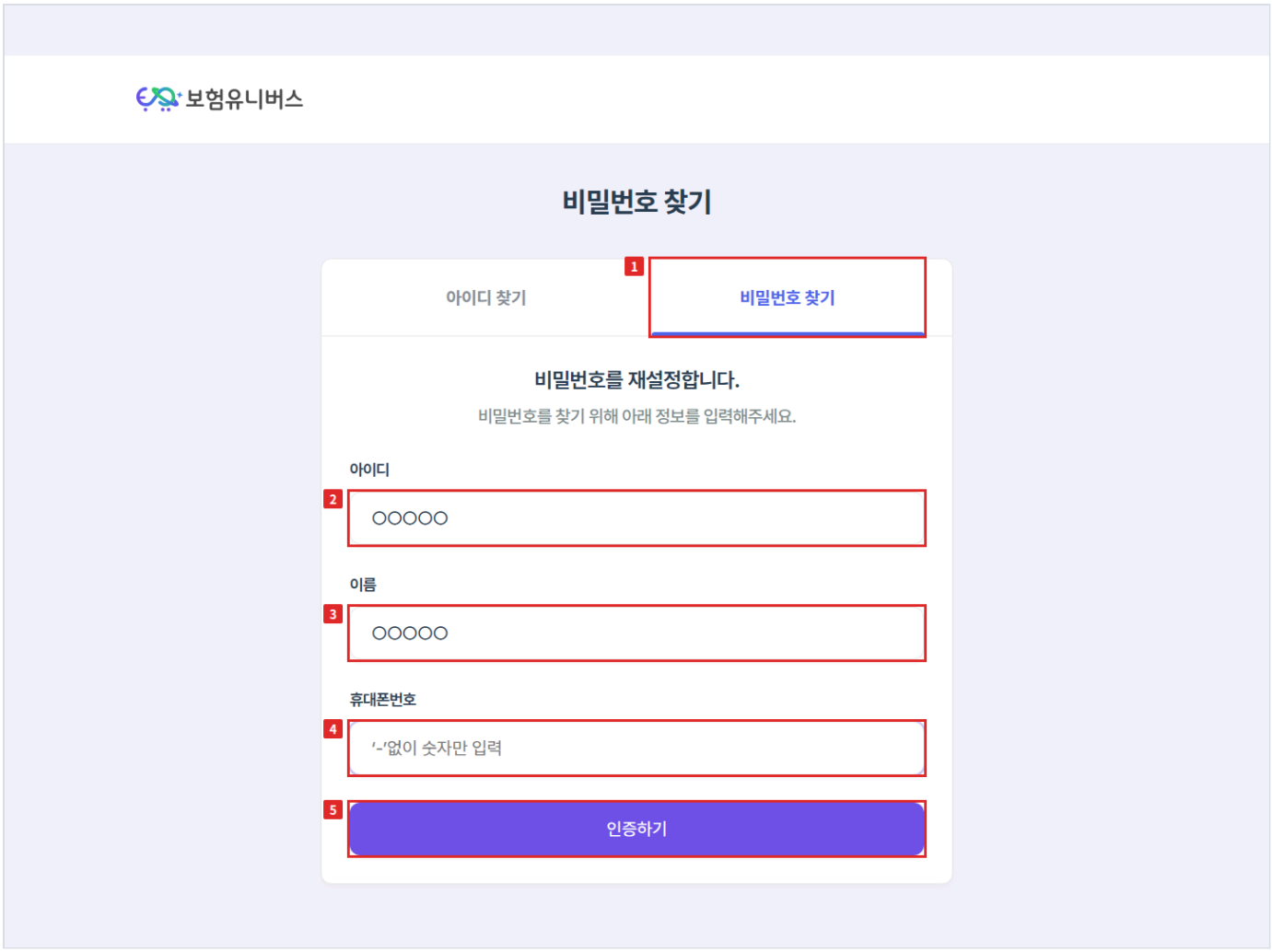


그림 8-2. 주소 /auth/find?type=pw 를 직접 입력한 화면 (전체 화면). 「비밀번호 찾기」 탭이 선택된 상태로 열립니다. 입력 값은 가렸고 「인증하기」는 누르지 않았습니다.

기대 결과

- 주소 ?type=pw 로 열면 「비밀번호 찾기」 탭이 선택되어 있습니다.
- 본인인증 입력 칸 3개와 「인증하기」 버튼이 보입니다.

확인 포인트 (그림 8-1)

1 탭 줄(아이디 찾기 · 비밀번호 찾기): 「아이디 찾기」에 밑줄이 있으면 정상입니다. 「비밀번호 찾기」를 누르면 주소 뒤에 ?type=pw 가 붙습니다 (실측).

확인 포인트 (그림 8-2)

1 「비밀번호 찾기」 탭: 이 탭이 선택된 상태로 열리면 정상입니다. 주소로 탭이 유지되는 동작입니다.

2 아이디 입력 칸: 입력한 아이디가 그대로 보이면 정상입니다. 그림의 가림은 문서용입니다.

3 이름 입력 칸: 입력한 이름이 그대로 보이면 정상입니다. 그림의 가림은 문서용입니다.

4 휴대폰번호 입력 칸: 입력한 번호가 숫자로 보이면 정상입니다. 그림에서 빈칸인 것은 문서용 가림 값이 숫자 칸에 들어가지 않아서입니다.

5 「인증하기」 버튼: **누르지 않습니다.** 누르면 외부 본인인증 창이 열리므로 이번 검토에서는 누르지 않았습니다.

이번 검토에서 하지 않은 확인: 본인인증 창을 여는 팝업 시작 확인은 하지 않았습니다. 본인인증 결과의 화면 전달은 서버 코드 주석의 2026-10-20 stg 실측 기록을 근거로 합니다.

시나리오 9. B2C 분석 공유 링크 (생년월일 확인)

바뀐 점(이전 → 지금)
이전에는 B2C 인증 쿠키 값이 고정 문자열(verified)이라, 쿠키만 꾸미면 그 분석 번호의 B2C 분석 결과가 보였습니다. 지금 인증 쿠키는 분석 번호에 묶인 서명 값이고 만료됩니다. 꾸민 쿠키나 다른 번호로 옮긴 쿠키로 분석 주소를 열면 분석 화면 대신 생년월일 확인 화면으로 돌아갑니다(7차 수정).

목적	생년월일 확인 전에는 분석 결과가 보이지 않고, 꾸민 인증 쿠키로도 결과가 열리지 않는지 확인합니다.
사전조건	로그아웃한 상태에서 시작합니다. 분석 공유 링크(분석 번호 47)가 필요합니다. 쿠키 확인은 브라우저의 쿠키 편집으로 b2c_auth_47 값을 verified 로 넣어 봅니다.

단계

1. 분석 공유 링크 `https://s.insuniverse.com/alimtalk/redirect/b2c-success-47` 를 엽니다. 자동으로 생년월일 확인 화면 (/analysis/b2c/auth/47)으로 넘어갑니다 (그림 9-1).
2. 생년월일 입력 칸(그림 9-1의 **2**)과 「확인」 버튼(그림 9-1의 **3**)을 확인합니다. 실고객의 생년월일은 입력하지 않았습니다.
3. 생년월일을 잘못 입력하면 입력 칸 아래에 오류 문구가 나옵니다 (그림 9-3).
4. 인증 쿠키 b2c_auth_47 의 값을 verified 로 넣은 상태에서 분석 주소 `https://s.insuniverse.com/analysis/b2c/47` 를 엽니다. 분석 화면이 아니라 생년월일 확인 화면이 보여야 합니다 (그림 9-2).

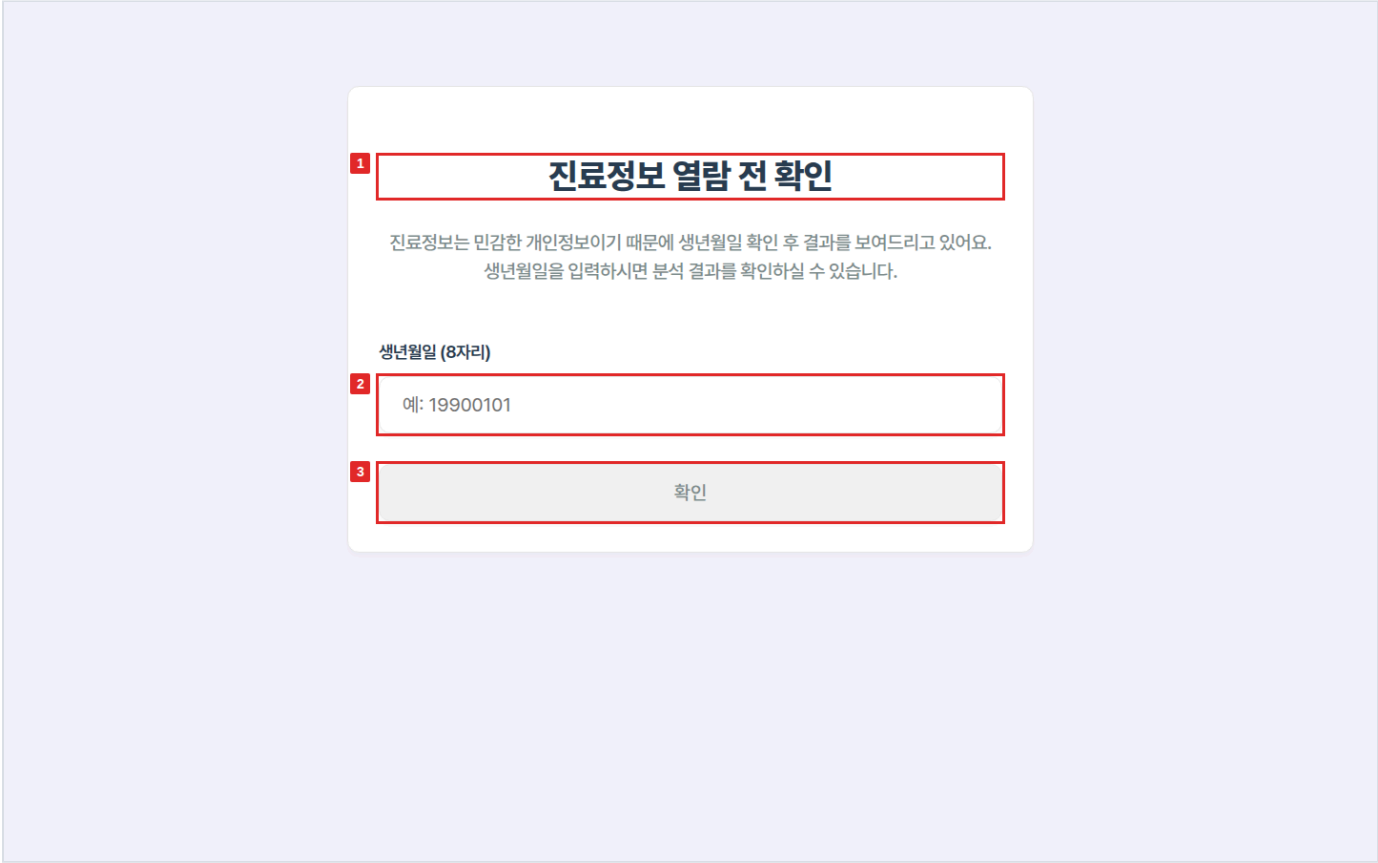


그림 9-1. 분석 공유 링크를 열면 자동으로 이동하는 생년월일 확인 화면 (/analysis/b2c/auth/47, 전체 화면).



그림 9-2. 인증 쿠키를 위조(b2c_auth_47=verified)해서 /analysis/b2c/47 을 열었을 때의 화면 (전체 화면). 분석 화면이 아니라 생년월일 확인 화면으로 돌아갑니다.

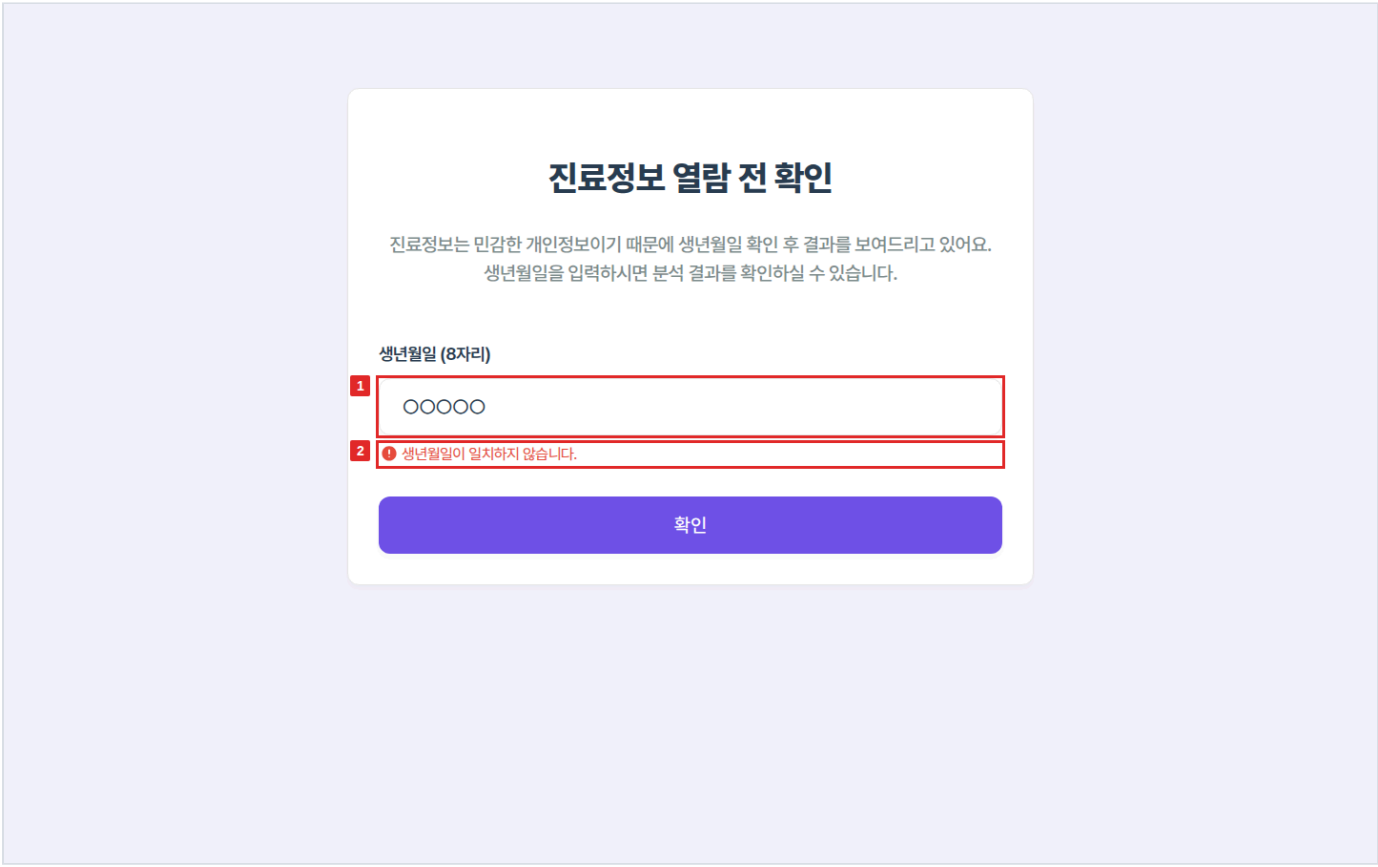


그림 9-3. 생년월일을 잘못 입력(1회)했을 때의 안내 문구 (입력 값은 가렸습니다).

기대 결과

- 분석 결과는 생년월일 확인 전에는 나오지 않습니다.
- 위조 쿠키로 분석 주소를 열어도 생년월일 확인 화면으로 돌아갑니다. 최종 주소는 /analysis/b2c/auth/47 입니다.

확인 포인트 (그림 9-1)

1 제목 「진료정보 열람 전 확인」: 제목과 안내 문구가 보이면 정상입니다. 이 화면을 통과하기 전에는 분석 결과가 나오지 않아야 합니다.

2 생년월일 입력 칸(8자리): 비어 있고 「예: 19900101」 안내가 보이면 정상입니다.

3 「확인」 버튼: 입력 전에는 회색으로 비활성 상태이면 정상입니다.

확인 포인트 (그림 9-2)

1 제목 「진료정보 열람 전 확인」: 위조 쿠키로 열었는데도 이 확인 화면이 보이면 정상입니다. 분석 결과 화면이 보이면 이상입니다.

2 생년월일 입력 칸: 비어 있으면 정상입니다. 분석 결과 본문은 보이지 않아야 합니다.

3 「확인」 버튼: 비활성(회색) 상태이면 정상입니다.

확인 포인트 (그림 9-3)

1 생년월일 입력 칸: 입력한 생년월일이 그대로 보이면 정상입니다. 그림의 가림은 문서용입니다.

2 오류 문구 「생년월일이 일치하지 않습니다.」: 입력 칸 아래 빨간 글씨로 보이면 정상입니다.

> 이번 검토에서 하지 않은 확인: 정상 생년월일을 넣고 분석 화면으로 넘어가는 단계는 생략했습니다. 실고객의 생년월일이 필요하기 때문입니다. 생년월일 입력 횟수 제한은 확인하지 않았습니다(부록의 남은 항목 참고).

시나리오 10. 회원 게시판 문의 목록 (본인 글만)

> **바뀐 점(이전 → 지금)**
> 이전에는 게시판 요청이 경로나 본문에 적힌 회원 값을 믿었습니다(서버 PR #124 본문 기준). 지금은 목록·수정·삭제가 로그인한 회원 기준으로만 조회되고, 회원용 게시판 상세 경로(/board-category/1)는 404 입니다.

목적	고객센터 Q&A 목록에 본인 문의만 보이는지, 새 문의 입력 화면이 빈 칸으로 열리는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태. 본인 문의가 2건(「답변준비중」 1건, 「답변완료」 1건) 있어야 합니다.

단계

1. 고객센터(이동 주소: `/board/qna`)에 들어가 「Q&A」 탭이 선택된 상태를 확인합니다 (그림 10-1).
2. 문의 목록 2건(그림 10-1의 **1**)과 상태 태그(그림 10-1의 **2**)를 확인합니다. 항목은 누르지 않습니다.
3. 「등록」 버튼(그림 10-1의 **3**)을 누르면 새 문의 등록 화면이 열립니다. 입력 칸만 확인하고, 저장하지 않고 돌아옵니다 (그림 10-2).

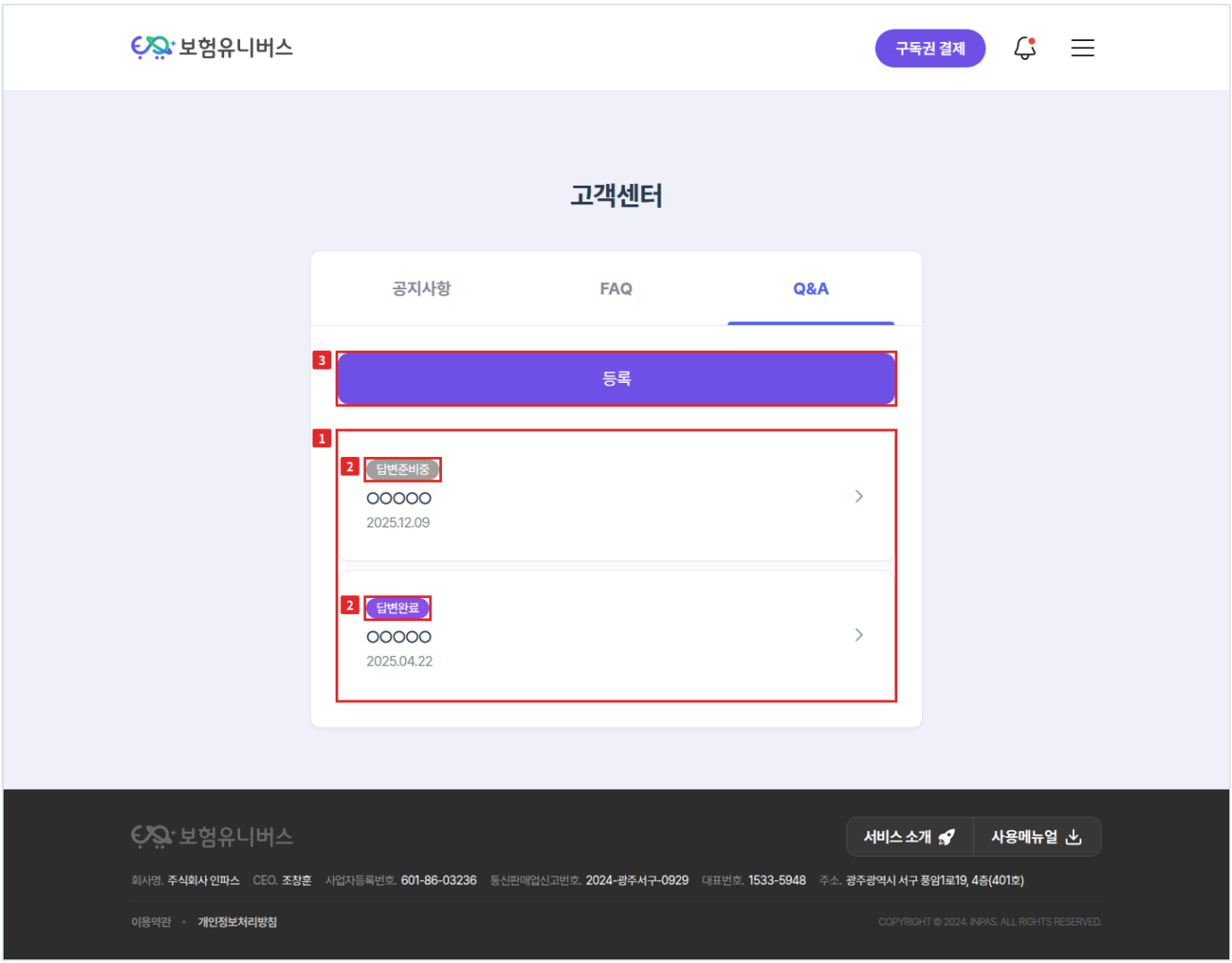


그림 10-1. 고객센터 Q&A 목록 (전체 화면). 제목과 본문 미리보기는 가렸습니다. 로그인한 회원 본인의 문의만 보입니다.

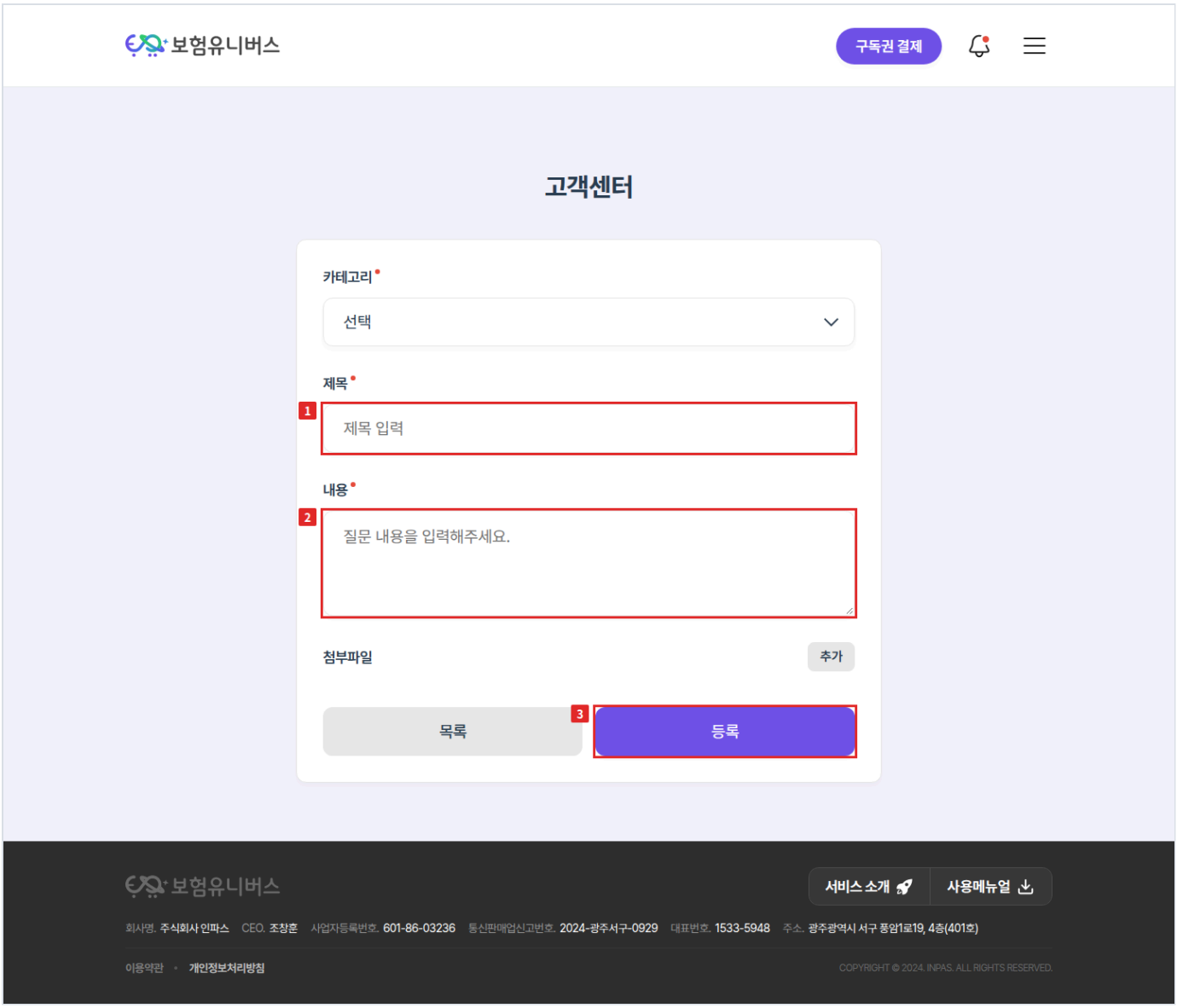


그림 10-2. 문의 등록 화면 (전체 화면). 입력 칸만 확인하고 저장하지 않았습니다.

기대 결과

- 목록에는 본인 문의 2건만 보입니다. 상태 태그는 「답변준비중」과 「답변완료」입니다.
- 등록 화면은 빈 입력 칸으로 열립니다.

확인 포인트 (그림 10-1)

1 문의 목록 2건: 본인 문의 2건이 보이면 정상입니다 (예: 2건). 다른 회원의 문의는 목록에 없어야 합니다.

2 상태 태그 2개: 「답변준비중」과 「답변완료」가 각각 보이면 정상입니다 (예: 준비중 1건, 완료 1건).

3 「등록」 버튼: 누르면 새 문의 등록 화면으로 갑니다. 이번 검토에서는 그 화면을 열어 입력 칸만 보고, 저장하지 않고 돌아왔습니다.

확인 포인트 (그림 10-2)

1 제목 입력 칸: 빈 칸으로 보이면 정상입니다. 이 화면에서는 값을 넣지 않습니다.

2 내용 입력 칸: 빈 칸으로 보이면 정상입니다.

3 「등록」 버튼: **누르지 않습니다.** 누르면 실제 문의가 저장됩니다.

시나리오 11. 회원 게시판 타인 문의 주소 차단과 비노출 공지

> **바뀐 점(이전 → 지금)**
> 이전에는 게시판 요청이 경로나 본문의 회원 값을 믿었습니다(서버 PR #124 본문 기준). 지금 다른 회원의 문의 주소와 비노출 공지 주소를 열면 본문 없는 빈 화면이 나오고, 같은 주소의 데이터 응답은 403 입니다. 본인 문의 상세는 그대로 열리고, 공지 목록에는 노출 중인 공지만 보입니다.

목적	다른 회원의 문의 주소와 비노출 공지 주소가 빈 화면인지, 공지 목록에 노출 공지만 보이는지, 본인 문의는 열리는지 확인합니다.
사전조건	시나리오 1로 로그인한 상태. 비노출 공지 1건(검토용 행)을 임시로 넣어 찍었고, 촬영이 끝난 뒤 그 행은 지웠습니다.

단계

1. 새 탭에서 다른 회원의 문의 주소 `https://s.insuniverse.com/board/qna/17` 를 엽니다. 본문 없는 빈 화면인지 확인합니다 (그림 11-1).
2. 새 탭에서 본인 문의 주소 `https://s.insuniverse.com/board/qna/19` 를 엽니다. 답변 상태만 확인합니다 (그림 11-2).
3. 고객센터의 「공지사항」 목록(이동 주소: `/board/notice`)을 엽니다. 노출 중인 공지 2건만 보이는지 확인합니다 (그림 11-3).
4. 새 탭에서 비노출 공지의 상세 주소 `https://s.insuniverse.com/board/notice/25` 를 엽니다 (그림 11-4).



그림 11-1. 다른 회원의 문의 주소(/board/qna/17)를 새 탭에서 열었을 때 화면 (전체 화면 크기, 빈 화면).

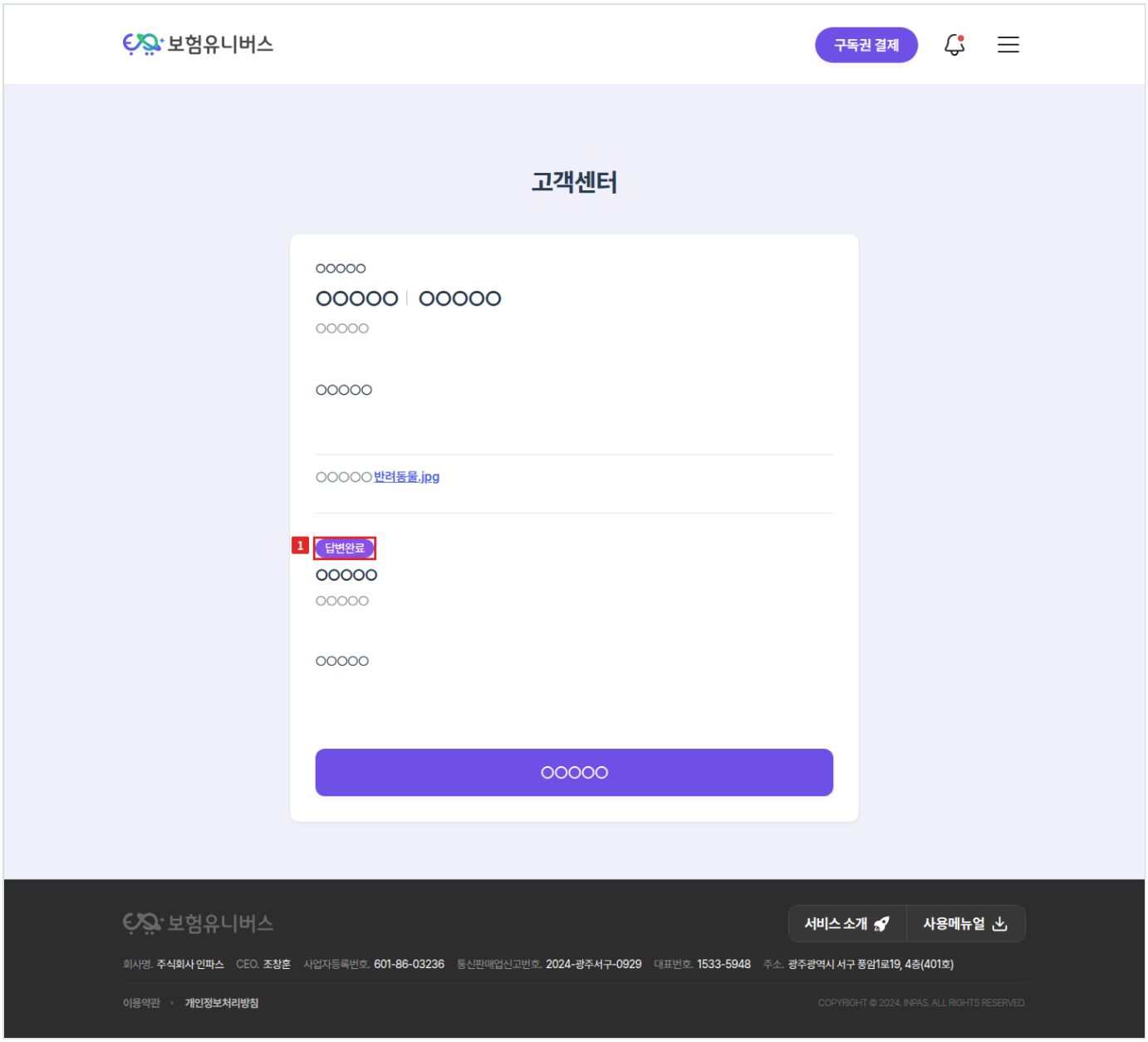


그림 11-2. 본인 문의 상세(/board/qna/19) (전체 화면). 제목·본문·답변 내용과 첨부 파일 이름의 앞부분은 가렸고, 답변 상태만 확인합니다.

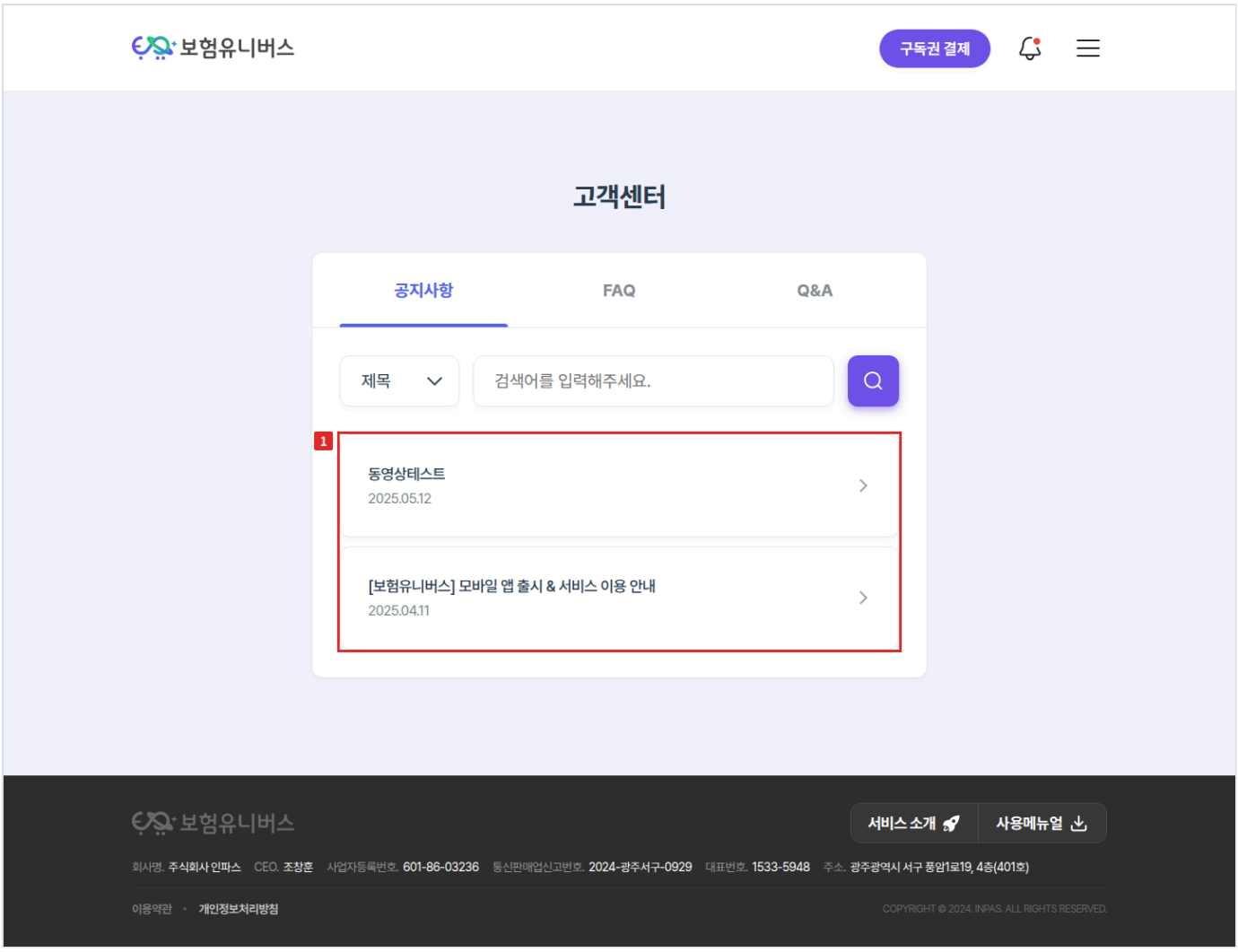


그림 11-3. 고객센터 공지사항 목록 (전체 화면). 노출 중인 공지 2건만 보입니다.



그림 11-4. 비노출 공지의 상세 주소(/board/notice/25)를 새 탭에서 열었을 때 화면 (전체 화면 크기, 빈 화면, 예시 데이터). 검토용 비노출 공지 행을 임시로 넣어 찍었습니다.

기대 결과

- 다른 회원 문의와 비노출 공지 주소는 빈 화면입니다. 「권한 없음」 같은 안내나 본문은 나오지 않고, 주소창은 about:blank 로 바뀝니다.
- 본인 문의 상세는 열리고, 「답변완료」 상태가 보입니다.
- 공지 목록에는 노출 중인 공지 2건만 있고, 비노출 공지는 없습니다.

확인 포인트 (그림 11-1)

1 빈 화면 본문 전체: 본문이 없는 빈 화면이면 정상입니다. 문의 제목이나 본문이 보이면 이상입니다. 같은 주소의 데이터 응답은 403 이고, 주소창은 about:blank 로 바뀝니다 (실측).

확인 포인트 (그림 11-2)

1 「답변완료」 상태 태그: 보이면 정상입니다. 본인 문의는 열립니다.

확인 포인트 (그림 11-3)

1 공지 목록 2건: 공지 2건이 보이면 정상입니다. 검토용 비노출 공지(보안검토더미)는 목록에 없어야 합니다.

확인 포인트 (그림 11-4)

1 빈 화면 본문 전체: 본문이 없는 빈 화면이면 정상입니다. 공지 내용이 보이면 이상입니다. 같은 주소의 데이터 응답은 403 입니다 (실측).

부록. 화면에 안 보이는 변경 — 실측 결과

이 부록은 바뀐 동작을 실제 요청으로 확인한 기록입니다. 실측 환경은 다음 셋 중 하나입니다. 재실측 목록은 오늘 stg API 에 다시 보낸 GET 요청 목록입니다.

1. **격리 실측 (2026-10-15)**: 통합 브랜치 빌드(서버 커밋 a3016d35)를 격리 MySQL(스키마 158표와 시드 데이터)과 격리 API 에 띄워 확인했습니다. 공유 stg 와 다른 세션의 자원은 건드리지 않았고, 끝난 뒤 컨테이너와 데이터를 지웠습니다.
2. **stg 사본 실측 (2026-10-19)**: stg DB 전체 사본(176표), 통합 빌드 서버, stg 프런트 빌드로 화면과 API 159건을 돌렸습니다. 외부 발송은 막았고 토스는 가짜 서버로 대신했습니다. 통과 149건, 실패 6건, 막힘 4건입니다. 실패 6건은 변경 전 stg 커밋(aff7ffcc)에서도 같은 결과여서 이번 변경의 회귀가 아닙니다.
3. **stg 배포 뒤 확인 (2026-10-19 ~ 10-20)**: 서버 PR #122(2026-10-19 머지), #124(2026-10-19 머지), #127·#128(2026-10-20 머지)과 사이트 PR #101(2026-10-19 머지)을 배포한 뒤 stg 에 직접 요청했습니다.

운영(prod) 반영은 이 부록의 범위 밖입니다. 운영 이식 PR(서버 #125, 사이트 #102)은 사람이 머지하기 전까지 운영에 들어가지 않습니다.

차수별 실측

1차 토큰 종류 구분 (stg 반영 PR #99)

확인한 요청	GET /card/{본인 id} 에 refresh 토큰을 Bearer 로 보냄
이전	회원 API 가 refresh 토큰을 통과시켰습니다. 로그아웃으로 저장값을 지워도 만료 전까지 쓸 수 있었고, 기업 회원 차단 검사도 건너뛰었습니다.
지금(기대)	401. 회원 access 형상(종류 필드와 회원 번호가 있고 역할 필드가 없는 토큰)만 회원 API 를 통과합니다.
실측 결과	2026-10-15 기준 라이브 실측 기록이 없었고 형상 검사의 명세 테스트로만 확인했습니다. 오늘(2026-10-21) stg 재실측에서 refresh 토큰 요청은 401 이었습니다.
실측 일자와 환경	명세 테스트 2026-10-15, stg 재실측 2026-10-21

2차 무인증 개인정보 경로 (stg 반영 PR #98)

확인한 요청	GET /medical/{oddId}/download 를 토큰 없이 호출. GET /analyze/{다른 회원 oddId}/basic 을 본인 토큰으로 호출
이전	토큰 없이 200 이었습니다. 환자 성명을 복호화하고 원본 진료 엑셀을 만들어 줬습니다. 분석 조회도 다른 회원의 oddId 로 열려 있었습니다.
지금(기대)	401. 토큰이 있어도 그 분석의 소유자가 아니면 403 이고 엑셀을 만들지 않습니다. 같은 소유 가드가 분석 조회 전체에 걸려 있습니다.
실측 결과	무토큰 401 을 확인했습니다. 다른 회원 분석 요청은 403 이었습니다. 소유자가 200 을 받는 경로는 실측하지 않았습니다.
실측 일자와 환경	2026-10-15 격리

3차 비밀번호 재설정 결합 (stg 반영 PR #102)

확인한 요청	POST /auth/lookup-password 다음 PATCH /auth/reset-password. 쓰기 요청이라 재실측 목록에는 넣지 않았습니다.
이전	로그인 ID 와 새 비밀번호만 보내면 바뀌었습니다. 같은 로그인 ID 의 기업 회원 비밀번호도 함께 바뀌었습니다.
지금(기대)	본인인증의 이름과 휴대폰이 맞는 일반 회원만 티켓을 받습니다. 티켓은 10분 동안만 유효하고 그 회원의 비밀번호 지문에 묶여 있어, 다른 회원의 비밀번호는 바뀌지 않습니다.
실측 결과	2026-10-13 stg 반영 뒤 비파괴 14건과 격리 16건이 통과했습니다(같은 로그인 ID 의 기업 회원 무변경 포함, 세부 목록은 저장소 밖 대조표에 있습니다). 2026-10-19 사본에서 무효한 본인인증 토큰을 넣으면 500 이 났습니다(기준선과 같음, 미조치).
실측 일자와 환경	2026-10-13 stg, 2026-10-19 stg 사본

4차 회원 소유자 수정 (운영 재생)

확인한 요청	GET /card/{다른 회원 id}. 카드 조회, 대표 카드 변경, 카드 삭제를 본인 토큰으로 요청
이전	운영에서 다른 회원의 카드를 조회하고 바꾸고 지울 수 있었습니다. stg 에는 이미 닫혀 있었습니다.
지금(기대)	403. 경로의 회원 id 가 토큰 회원과 다르면 그 id 가 실재하는지와 상관없이 403 입니다. 주문 목록과 주문 상세는 토큰 회원 기준으로만 조회합니다(코드 판독).
실측 결과	격리 실측: 카드 조회, 대표 카드 변경, 카드 삭제 모두 403 이었고 DB 행은 그대로였습니다. 구독 현황은 재실측 목록에 넣었습니다. 구독 생성·해지·결제, 주문 취소, 분석 숨김, 알림톡 초대는 코드 판독만 했습니다. 격리 시드에 연결된 주문이 없어 주문 목록에서 다른 회원 주문이 가려지는지는 확인하지 못했습니다.
실측 일자와 환경	카드는 2026-10-15 격리. 운영 반영은 2026-10-13 운영 배포(#105)입니다.

5차 회원 소유자 대조 (stg 반영 PR #122)

확인한 요청	GET /fc/{다른 회원 id}. GET /alarm?memId={다른 회원}. GET /loss?memId={다른 회원}. 본인 id 로는 같은 요청을 보냄
이전	다른 회원의 FC 정보, 알림 목록, 손해사정 목록을 id 만 바꿔 열람할 수 있었습니다. 운영에서 열려 있었습니다.
지금(기대)	403. 본인 id 요청은 그대로 200 입니다. 알림 읽음과 삭제, 손해사정 생성·수정·삭제는 소유 확인을 거친 뒤에만 실행됩니다.
실측 결과	격리 실측: FC 조회와 FC 수정, 손해사정 목록, 알림 목록이 모두 403 이었습니다. 본인 id 요청은 200 이었습니다. memId 를 빼면 전역 검증 파이프가 400 을 냅니다. 알림 읽음과 삭제, 시험 발송, 손해사정 쓰기 경로는 코드 판독만 했습니다.
실측 일자와 환경	2026-10-15 격리. stg 는 2026-10-19 서버 PR #122 배포로 반영되었습니다.

6차 공개 분석 조회 (운영 이식 축)

확인한 요청	GET /disease-prediction/recommended-insurance?bodId={id}, 쿠키 없음. GET /disease-prediction/treatment-log?codId={id}, 토큰 없음
이전	운영에서 쿠키와 토큰 없이 bodId 나 codId 로 분석 결과를 조회할 수 있었습니다. stg 는 10-06 #93 으로 이미 닫혀 있었습니다.
지금(기대)	403. bodId 는 B2C 인증 쿠키 보유자만, codId 는 통합 관리자만 통과합니다. 공개 트리(/disease-prediction/tree)는 그대로 200 입니다.
실측 결과	격리 실측: 위조 쿠키 요청은 403, 정상 서명 쿠키 요청은 200 이었습니다. 무쿠키 요청의 실측 기록은 없어서 재실측 목록에 넣었습니다. 2026-10-19 stg 배포 뒤 위조 쿠키로 treatment-log 를 요청하면 403 이었습니다.
실측 일자와 환경	2026-10-15 격리, 2026-10-19 stg

7차 B2C 인증 쿠키 서명 (stg 반영 PR #122)

확인한 요청	GET /analyze/b2c/{bodId}/basic?ansType=ANS001 과 GET /analyze/b2c/{bodId}/check-auth 를 쿠키 b2c_auth_{bodId}=verified 로 요청
이전	쿠키 값이 고정 문자열 verified 라서 쿠키만 꾸미면 그 bodId 의 B2C 분석 결과가 보였습니다(격리 기준선 실측 200). check-auth 도 authenticated 가 true 였습니다.
지금(기대)	403. 쿠키 값은 bodId 에 묶인 서명 토큰이고 만료됩니다. 변조한 값이나 다른 bodId 이름으로 옮긴 값은 403 입니다. 정상 서명 쿠키는 가드를 통과합니다.
실측 결과	격리 실측: 위조, 변조, 이름 옮김 세 경우 모두 403 이었습니다. 정상 서명 쿠키는 가드를 통과했고, 응답 500 은 시드에 B2C 주문이 없어서였습니다. 2026-10-19 stg 배포 뒤: 위조 쿠키의 basic 은 403, check-auth 는 authenticated=false 였습니다(배포 전에는 true). 오늘(2026-10-21) 재실측에서도 같았습니다.
실측 일자와 환경	2026-10-15 격리, 2026-10-19 stg, 2026-10-21 stg 재실측

8차 개발용 인증 우회 차단 (stg 반영 PR #122·#124)

확인한 요청	GET /card/{id} 를 Referer 에 swagger, X-Forwarded-For 에 사무실 IP 를 실어 보냄. GET /swagger
이전	운영의 NODE_ENV 값(dev) 때문에 사무실 IP 와 swagger 경로로 토큰 없이 회원 신원을 얻을 수 있었습니다. swagger 문서 화면도 열려 있었습니다.
지금(기대)	우회는 DEV_AUTH_BYPASS 가 정확히 true 일 때만 열립니다. 미설정이면 NODE_ENV 와 상관없이 꺼집니다. swagger 는 SWAGGER_ENABLED 가 true 일 때만 열립니다(서버 PR #124). 미설정 상태의 기대 결과는 401 과 404 입니다.
실측 결과	2026-10-19 stg 배포 뒤: 우회 헤더 요청은 401, /swagger 는 404 였습니다(5회씩 3라운드 연속). #122 배포 직후에는 /swagger 가 200 이었습니다. 오늘(2026-10-21) 재실측에서도 401 과 404 였습니다.
실측 일자와 환경	2026-10-19 stg, 2026-10-21 stg 재실측

10차 카드 삭제 빌링키 폐기 (stg 반영 PR #122·#124·#127)

확인한 요청	POST /card/delete 는 쓰기 요청이라 재실측 목록에서 뺐습니다. 실측은 격리의 더미 행에서만 했습니다.
이전	카드 행만 지우고 토스의 빌링키는 그대로 두었습니다. 지운 카드의 정기결제 자격이 토스에 살아 있었습니다.
지금(기대)	10-15 정책은 폐기 실패 시 행을 남기고 500 을 돌려줬습니다. 10-20 정책(서버 PR #127)은 폐기가 실패해도 카드 행을 지우고 실패를 오류 로그로 남깁니다. 다른 회원의 카드는 토스를 부르기 전에 막습니다.
실측 결과	2026-10-15 격리: 폐기 실패 시 행이 남고 500 이 났으며 로그에 card delete halted 가 찍혔습니다. 2026-10-19 토스 샌드박스: 이미 폐기된 키를 다시 지우면 400 ALREADY_REMOVED_BILLING_KEY 가 왔습니다. 코드는 404 NOT_FOUND_BILLING 을 가정하고 있었고, 서버 PR #124 에서 이미 없음으로 처리하게 고쳤습니다. 2026-10-20 정책은 격리 실측이 없고 단위 명세 8건과 반사실 확인만 했습니다.
실측 일자와 환경	2026-10-15 격리, 2026-10-19 토스 샌드박스, 2026-10-20 stg 배포

회원 게시판 경로 (서버 PR #124)

확인한 요청	GET /board-category/1
이전	회원용 게시판 상세 경로가 있었고, 게시판 요청이 본문이나 경로의 회원 값을 믿었습니다(PR 본문 기준).
지금(기대)	회원용 상세 경로는 제거되어 404 입니다. 수정·삭제·목록은 토큰 회원 기준으로 좁혀졌습니다.
실측 결과	2026-10-19 stg 배포 뒤 GET /board-category/1 은 404 였습니다. 오늘(2026-10-21) 재실측에서도 404 였습니다. 수정과 삭제는 쓰기라 실측하지 않았습니다.
실측 일자와 환경	2026-10-19 stg, 2026-10-21 stg 재실측

본인인증 창 연결 (서버 PR #128)

확인한 요청	본인인증 결과 응답(POST /mok-auth/result 의 302)
이전	응답에 Cross-Origin-Opener-Policy 가 붙어 창 연결이 끊겼고, 결과가 찾기·가입 화면에 전달되지 않았습니다.
지금(기대)	결과가 화면에 전달됩니다. 보안 기능이 아니라 배포 변경 사항입니다.
실측 결과	서버 코드 주석에 2026-10-20 stg 실측 기록이 있습니다.
실측 일자와 환경	2026-10-20 stg

9차 관리자 역할 경계는 관리자 화면 매뉴얼에서 다룹니다.

카드 삭제 폐기 정책 변화 (10월 15일에서 10월 20일까지)

1. 이전에는 카드 행만 지우고 토스 빌링키 폐기는 하지 않았습니다.
2. 10월 15일 정책은 토스 폐기가 실패하면 카드 행을 남기고 500 을 돌려주는 방식(fail-closed)이었습니다. 사용자는 그 카드를 지울 수 없었습니다.
3. 10월 20일 정책(서버 PR #127, stg 배포 성공)은 사용자가 카드를 지우려는데 우리 쪽 실패 때문에 지우지 못하는 것은 맞지 않다는 결정입니다. 카드마다 폐기를 시도하고 실패해도 다음 카드로 넘어가며, 소유가 확인된 카드 행은 모두 지웁니다. 실패한 카드는 `card billing key not revoked` 오류 로그에 회원 번호와 카드 번호로 남습니다. 이미 폐기된 키는 오류 로그 없이 넘어갑니다.
4. 사이트(사이트 PR #101, 2026-10-19 stg 배포)는 실패 안내 창을 띄우고 편집 모드를 닫습니다. 목록은 서버 응답이 실패일 때만 다시 불러옵니다. 실패 안내는 403, 서버 오류, 네트워크 실패에만 뜹니다. 토스 실패가 사용자에게 500 으로 보이지 않습니다.
5. 남는 것: 폐기하지 못한 빌링키는 토스에 그대로 남습니다. 우리 DB 에는 행이 없어 결제 경로가 쓰지 않지만, 토스 쪽 키를 정리하는 재시도 대기열은 없습니다. 실패 로그가 쌓이면 재시도 대기열을 두는 것이 후속 과제입니다.

실측하지 않았거나 남은 것 (2026-10-21 stg 코드 판독)

1. 요청 로그가 URL 을 그대로 남깁니다. 토스 빌링키 삭제 URL 에 빌링키가 들어 있어서 로그에 빌링키가 찍힙니다. 이는 구현 기록의 실측으로 확인되었고, 요청 로거가 URL 을 가리지 않는 것을 코드로 확인했습니다.
2. 생년월일 인증(B2C)과 비밀번호 찾기 요청에는 횟수 제한이 없습니다.
3. 비밀번호 찾기에 무효한 본인인증 토큰을 넣으면 500 이 납니다(2026-10-19 사본 실측, 기준선과 같음).
4. B2C 개발용 생년월일 조회(/analyze/b2c/{bodId}/birth-info)는 정상 쿠키를 가진 사람에게 성명, 생년월일, 휴대폰을 돌려줍니다. 쿠키 범위 안의 노출이라 관찰로만 둡니다.
5. FC 본인이 비밀번호를 바꿀 때 현재 비밀번호를 묻지 않습니다(코드 판독).
6. 구독 생성·해지·결제, 주문 취소, 분석 숨김, 알림톡 초대, 알림 읽음·삭제, 시험 발송, 손해사정 쓰기 경로는 실측하지 않았습니다. 코드 판독이나 명세 테스트만 있습니다.
7. 개발용 회원번호의 구독 면제는 실측 기록이 없습니다.
8. 서버 PR #123 이 넣은 FCM 토큰 등록의 회원 인증 필수는 안드로이드 앱이 인증을 싣지 않는 경로일 수 있어 등록 실패 위험이 있습니다(2026-10-19 기록). 모바일에서 확인하기 전입니다.
9. 운영 env 에 DEV_AUTH_BYPASS 와 SWAGGER_ENABLED 가 없는지는 저장소 밖이라 확인하지 못했습니다.

본문과 무관하게 확인된 실패 (2026-10-19 사본 실측, 기준선과 같음)

- 손해사정 신청 화면에서 분류 선택 칸을 바꾸면 검증에 막힙니다. 서버의 신청 요청 자체는 201 이었습니다.
- B2C 건강체 분석(ANS001)은 500 입니다. 테이블이 stg 에 없는 누락분입니다.
- 카드 삭제 실패 시 성공 모달이 뜨던 결함은 사이트 PR #101 로 고쳤습니다. 고친 뒤의 화면 확인은 이 문서 시나리오 7 에서 모의 응답으로 했습니다.
- 관리자 쪽 두 건은 관리자 화면 매뉴얼에서 다룹니다.

오늘(2026-10-21) stg 재실측 (사이트 쪽 GET 탐침)

회원 계정 1개와 관리자 계정으로 토큰을 받기 위해 로그인 2회를 했고, 나머지는 GET 요청입니다. 기대와 다른 2건은 판정 칸에 불일치로 적었습니다. 26건 중 24건이 일치하고 2건이 불일치합니다.

요청	인증 조건	기대	실측 (3회)	판정	비고
GET /medical/999999999/download	없음	401	401 / 401 / 401	일치	
GET /medical/999999999/download	회원 토큰	403	400 / 400 / 400	불일치	없는 번호는 소유 대조 전에 400 이 납니다(코드 판독, 실측 미확인). 존재하는 남의 주문은 실측하지 못했고, 데이터는 나가지 않았습니다.
GET /analyze/999999999/basic?ansType=ANS001	없음	401	401 / 401 / 401	일치	
GET /analyze/999999999/basic?ansType=ANS001	회원 토큰	403	400 / 400 / 400	불일치	위 medical 행과 같은 원인입니다.
GET /analyze/b2c/user/999999999	없음	404	404 / 404 / 404	일치	
GET /analyze/b2c/47/check-auth	위조 B2C 쿠키	authenticated=false	200, false / 200, false / 200, false	일치	배포 전에는 true 였습니다.
GET /analyze/b2c/999999999/basic?ansType=ANS001	위조 B2C 쿠키	403	403 / 403 / 403	일치	
GET /analyze/b2c/999999999/birth-info	위조 B2C 쿠키	403	403 / 403 / 403	일치	
GET /b2c/analyze/999999999/disease-prediction-pdf	위조 B2C 쿠키	403	403 / 403 / 403	일치	
GET /disease-prediction/recommended-insurance?bodId=999999999	없음	403	403 / 403 / 403	일치	
GET /disease-prediction/recommended-insurance?bodId=999999999	위조 B2C 쿠키	403	403 / 403 / 403	일치	
GET /disease-prediction/treatment-log?codId=999999999	없음	403	403 / 403 / 403	일치	
GET /disease-prediction/tree	없음	200	200 / 200 / 200	일치	공개 경로 회귀
GET /company-terms	없음	200	200 / 200 / 200	일치	공개 경로 회귀

GET /card/999999999	회원 토큰	403	403 / 403 / 403	일치	회원 토큰을 Bearer 헤더와 쿠키 양쪽에 실었습니다.
GET /card/{본인 회원 번호}	회원 토큰	200	200 / 200 / 200	일치	본인 회귀
GET /card/{본인 회원 번호}	갱신 토큰을 Bearer 로	401	401 / 401 / 401	일치	갱신 토큰은 사용자 에이전트 로그인에서만 발급됩니다.
GET /card/999999999	우회 헤더 (Referer 에 swagger, 사무실 IP)	401	401 / 401 / 401	일치	헤더가 실제로 나가는지 로컬 에코로 확인했습니다.
GET /subscribe/999999999	회원 토큰	403	403 / 403 / 403	일치	
GET /fc/999999999	회원 토큰	403	403 / 403 / 403	일치	
GET /fc/{본인 회원 번호}	회원 토큰	200	200 / 200 / 200	일치	본인 회귀
GET /alarm?memId=999999999	회원 토큰	403	403 / 403 / 403	일치	
GET /alarm?memId={본인 회원 번호}	회원 토큰	200	200 / 200 / 200	일치	본인 회귀
GET /loss?memId=999999999	회원 토큰	403	403 / 403 / 403	일치	
GET /loss?memId={본인 회원 번호}	회원 토큰	200	200 / 200 / 200	일치	본인 회귀
GET /board-category/1	회원 토큰	404	404 / 404 / 404	일치	회원용 상세 경로 제거 확인