

B2B SaaS 출시 전 보안 체크리스트

대표·CTO·개발리드가 출시 전에 확인해야 할 24개 보안 경계를
권한, 인증, 업무로직, 파일·외부연동 관점으로 정리했습니다.

24 QUESTIONS

10분 안에 PASS / UNKNOWN /
FAIL 표시

6 STOP SIGNALS

출시 전에 반드시 확인할 위험 경계

3 DECISIONS

GO / CONDITIONAL / STOP으로 다
음 행동 결정

HOW TO USE

- 01 각 질문을 PASS, UNKNOWN, FAIL 중 하나로 표시
- 02 UNKNOWN 1점, FAIL 2점으로 합산
- 03 즉시 중단 신호가 하나라도 있으면 총점과 무관하게 출시 보류
- 04 증거가 없는 PASS는 UNKNOWN으로 처리

01 권한과 테넌트 분리

다른 사용자·고객사·역할의 경계를 서버가 일관되게 강제하는지 확인합니다.

점검 질문

PASS

UNKNOWN

FAIL

A01 사용자 역할과 관리 권한이 문서로 정의돼 있는가?

증거: 역할표, 권한 매트릭스

☐☐☐

A02 모든 객체 조회·수정에서 서버가 소유자와 테넌트를 검증하는가?

증거: API 통합 테스트

☐☐☐

A03 URL·객체 ID를 바꿔도 다른 고객사 데이터에 접근할 수 없는가?

증거: 계정 A/B 음성 테스트

☐☐☐

A04 초대·역할변경·퇴사 뒤 기존 권한과 공유 토큰이 회수되는가?

증거: 권한 수명주기 테스트

☐☐☐

A05 관리자 기능은 화면 숨김이 아니라 서버에서 차단되는가?

증거: 비관리자 직접 요청

☐☐☐

A06 백오피스·지원도구가 고객 테넌트 경계를 우회하지 않는가?

증거: 운영자 역할·감사로그

☐☐☐

02 인증, 세션, 계정 복구

로그인보다 중요한 것은 세션 수명주기와 복구 경로의 우회 방지입니다.

점검 질문

PASS

UNKNOWN

FAIL

S01 로그인·MFA·비밀번호 재설정 흐름에 일관된 보호가 있는가?

증거: 정상·실패·복구 흐름

☐☐☐

S02 비밀번호 변경·탈퇴·권한 축소 시 기존 세션이 무효화되는가?

증거: 다중 기기 세션 테스트

☐☐☐

S03 세션 쿠키·토큰의 만료, Secure, HttpOnly, SameSite가 적절한가?

증거: 쿠키·토큰 설정

☐☐☐

S04 재설정 링크·인증 코드는 일회용이며 짧은 시간 안에 만료되는가?

증거: 재사용·동시요청 테스트

☐☐☐

S05 OAuth 연결에서 state, redirect URI, scope를 서버가 검증하는가?

증거: 승인·콜백 음성 테스트

☐☐☐

S06 로그인·복구·중요 변경에 탐지 가능한 감사로그가 남는가?

증거: 이벤트와 경보

☐☐☐

03

핵심 업무로직과 결제

가격·상태·한도를 클라이언트가 아니라 서버의 현재 상태로 결정해야 합니다.

점검 질문

PASS

UNKNOWN

FAIL

L01	결제·환불·크레딧·쿠폰 상태는 서버가 이전 단계를 검증하는가? 증거: 순서 변경·재전송 테스트	☐	☐	☐
L02	동시 요청에도 잔액·재고·사용량이 음수 또는 중복 처리되지 않는가? 증거: 제한된 동시성 테스트	☐	☐	☐
L03	클라이언트가 보낸 가격·등급·권한 값을 서버가 신뢰하지 않는가? 증거: 서버 기준 재계산	☐	☐	☐
L04	취소·만료·삭제 뒤에도 금지된 작업을 다시 실행할 수 없는가? 증거: 상태 전이 음성 테스트	☐	☐	☐
L05	대량 내보내기·관리 작업에 재인증과 권한 확인이 있는가? 증거: 중요 동작 보호	☐	☐	☐
L06	사용량·요금제 제한이 모든 API와 비동기 작업에 동일한가? 증거: UI/API/작업류 대조	☐	☐	☐

04

파일, API, 외부 연동

파일·Webhook·OAuth·서버측 요청은 서비스 밖의 신뢰 경계와 연결됩니다.

점검 질문

PASS

UNKNOWN

FAIL

I01	업로드 파일의 형식·크기·이름·저장 위치를 서버가 제한하는가? 증거: 허용/차단 샘플	☐	☐	☐
I02	다운로드·미리보기·공유 URL은 권한과 만료를 다시 확인하는가? 증거: 만료·권한변경 테스트	☐	☐	☐
I03	Webhook은 서명·시간·재전송을 검증하고 중복 처리에 안전한가? 증거: 위조·재전송 음성 테스트	☐	☐	☐
I04	외부 API 키·OAuth 토큰은 최소권한이며 폐기·회전 가능한가? 증거: 비밀관리·회전 절차	☐	☐	☐
I05	서버측 URL 요청이 내부망·메타데이터·로컬 주소를 차단하는가? 증거: 허용목록·네트워크 정책	☐	☐	☐
I06	오류·로그·분석도구에 토큰·PII·고객 데이터가 남지 않는가? 증거: 로그 샘플·마스킹	☐	☐	☐

05 점수를 다음 행동으로 바꾸기

PASS 0점, UNKNOWN 1점, FAIL 2점입니다. 증거가 없는 PASS는 UNKNOWN으로 계산합니다.

GO

0-6점

중대한 예외가 없다면 출시하되 UNKNOWN 항목의 담당자와 기한을 기록합니다.

CONDITIONAL

7-16점

고객 데이터·권한·결제와 연결된 FAIL부터 수정하고 제한된 재검증 후 출시합니다.

STOP

17점 이상

출시 범위를 줄이거나 보류하고, 핵심 경계를 독립적으로 검증합니다.

IMMEDIATE STOP SIGNALS

! 다른 고객사 객체에 접근 가능한지 확인하지 못함

! 관리자 API가 클라이언트 역할값만 신뢰함

! 비밀번호 재설정 뒤 기존 세션이 계속 유효함

! 가격·잔액·크레딧을 클라이언트 입력으로 결정함

! 업로드 파일이 실행 가능한 위치에 공개 저장됨

! 외부 토큰·PI가 로그 또는 오류 응답에 노출됨

WHEN TO USE EXTERNAL VALIDATION

01	LAUNCH CHECK	5영업일	웹 또는 API 1개, 역할 2개, 핵심 흐름 5개
02	WEB + API SPRINT	10영업일	웹 1개와 API, 역할 3개, 핵심 흐름 10개
03	RED TEAM VALIDATION	별도 설계	목표·범위·허용기법·중단 조건을 서면 합의

BARO SECURITY

출시 전에 실제 공격자가 악용할 수 있는 경로를 검증하고, 개발팀이 바로 수정할 수 있는 증거와 재검증을 제공합니다.

본 자료를 전달한 담당자에게 샘플 보고서와 범위표를 요청하세요.