먹튀를 노리는 집단이 다계정을 돌리는 방식은 해마다 정교해진다. 예전처럼 동일 IP, 동일 기기 정도만 잡아내서는 빈틈이 생긴다. 통신사 CGNAT, VPN, 클라우드 프록시, 가상머신, 자동화 프레임워크가 일상화되면서 흔적은 더 얇아지고, 반대로 정상 사용자의 환경 다양성은 더 커졌다. 다계정 식별은 더 섬세해야 하고, 근거는 더 단단해야 한다. 현장에서 쌓인 시행착오를 바탕으로, 실무자가 바로 적용할 수 있는 먹튀검증 관점의 노하우를 정리한다.

왜 다계정이 치명적인가

다계정은 단순히 가입자 수를 부풀리는 문제로 끝나지 않는다. 보너스 어뷰징, 자전거래를 통한 손실 이전, 환전 지연 후 잠수 같은 먹튀 시나리오의 핵심 도구가 된다. 피해는 두 갈래다. 첫째, 프로모션 비용이 눈덩이처럼 불어난다. 둘째, 리스크 통제 신뢰가 무너지면 양질의 사용자 이탈과 평판 하락으로 이어진다. 실무에서는 단일 사건의 금전 손실보다, 재발 방지 능력을 보여주지 못했을 때의 누적 손실이 훨씬 크다.

범주를 나눠야 흔적이 보인다

다계정의 목적이 무엇인지, 그리고 집단의 숙련도가 어느 정도인지에 따라 흔적의 패턴이 다르다. 보너스만 노리는 저숙련 그룹은 가입 시간, 로그인 구간, 접속 도시가 뭉치는 경향이 있고, 환전까지 노리는 중숙련 그룹은 결제 수단과 신원 정보를 분산시키려 노력한다. 가장 까다로운 고숙련 그룹은 자동화를 결합해 인간형 행동을 흉내 낸다. 실무자는 모든 케이스를 한 바구니에 넣지 말고, 목적과 숙련도별로 규칙과 임계치를 달리 가져가야 한다.

신호 설계의 기본 원리

다계정 식별은 결국 신호의 조합 싸움이다. 하나의 결정적 지문을 과신하면 오탐이 폭증한다. 대신 약한 신호 여러 개를 독립적으로 쌓아 리스크 스코어를 산출하는 편이 안정적이다. 정확도와 재현율의 트레이드오프를 인정하고, 수동 검토 대기열의 처리 용량을 고려한 임계치를 운용한다. 라벨링된 과거 사건 데이터를 기반으로 주기적으로 임계치를 재보정하면 정책 경직화를 막을 수 있다.

네트워크 흔적을 읽는 법

IP만 보는 시대는 지났다. 그렇다고 네트워크 신호가 쓸모없다는 뜻은 아니다. 결합과 해석이 관건이다. 예를 들어 같은 날 같은 시간대에 동일 ASN의 대역에서 짧은 간격으로 다수 계정이 로그인한다면, CGNAT 환경이라도 의심 점수는 오른다. 도시와 지연 시간의 조합도 힌트가 된다. 서울로 지오로케이션되는 IP인데 평균 RTT가 150ms 이상으로 치솟고 TLS 핸드셰이크에서 JA3 지문이 클라우드 프록시 특성과 일치하면, 우회 흔적일 가능성이 크다.

한국 환경에선 통신사 공유 NAT가 일반적이라 공용망에서 동일 IP로 보이는 일이 흔하다. 이럴 때는 연속 접속 시각 분포와 세션 중첩도를 본다. 예를 들어 30분 내에 8개 계정이 각각 60초 간격으로 로그인하고, 각 세션이 2분 이상 겹치지 않는다면 스크립트 배치일 확률이 높다. 반면 PC방처럼 10개 이상 계정이 동시에 접속하지만 페이지 이동 속도와 체류 시간이 사람다운 분포를 보인다면 정상일 가능성이 크다.

디바이스 지문과 환경 변수

브라우저 지문과 OS 환경을 결합하면 네트워크보다 변별력이 높은 경우가 많다. 사용자 에이전트 문자열은 손쉽게 위장된다. 대신 캔버스와 WebGL 렌더링 해시, 설치 폰트 목록 길이와 순서, 스크린 해상도와 색 심도, 타임존과 시스템 로케일의 조합이 반복적으로 동일하게 나타나는지 본다. 배터리 상태 이벤트나 미디어 디바이스 접근 권한의 응답 패턴처럼 위장 비용이 높은 신호는 특히 유용하다.

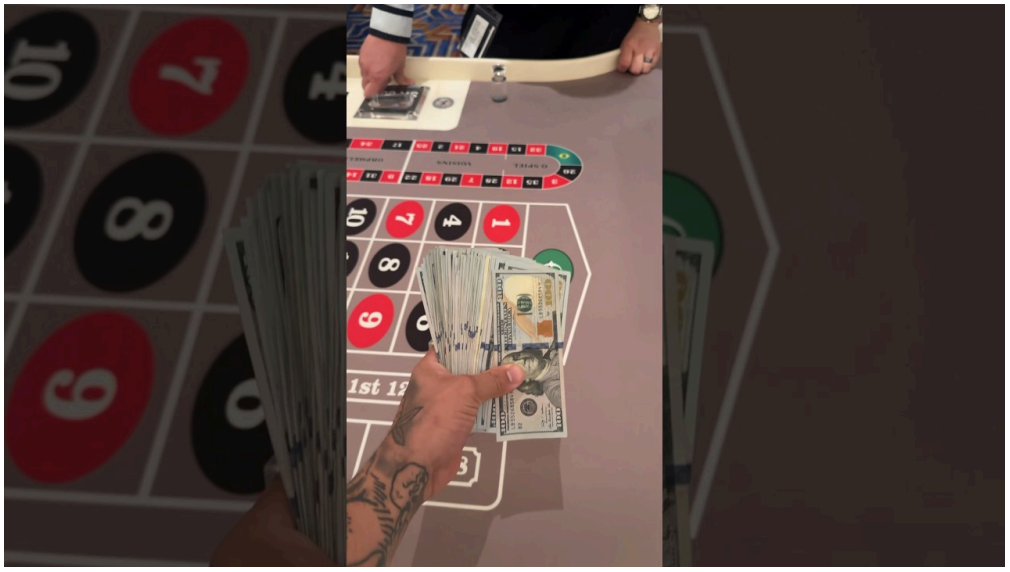
모바일에선 기기 모델명과 OS 빌드, 앱 설치 소스, 키체인 기반 설치 고유값의 지속성이 핵심이다. 루팅, 탈옥, 개발자 옵션 활성화 여부, 디버그 가능한 빌드 플래그도 함께 본다. 에뮬레이터는 가짜 센서 데이터와 일관성 없는

하드웨어 속성으로 자주 드러난다. 예를 들어 자이로스코프 노이즈가 고정되거나, 가속도계 값이 0에 가까운 상태로 길게 유지되는 경우다.

행동 데이터가 주는 결정적 차이

다계정 집단이 가장 흉내 내기 어려운 것은 미시적 행동 습관이다. 마우스 포인터 속도 분포, 클릭 간 간격의 변동성, 스크롤 가속 패턴, 화면 전환 후 첫 상호작용까지의 지연 등이 계정마다 개성 있게 나타나는지 측정한다. 패턴 유사도는 벡터화한 후 코사인 유사도나 동적 시간 워핑 거리로 비교한다. 자동화 툴의 행동은 표준편차가 낮고 규칙적이다. 예를 들어 회원가입 폼 6개 필드의 입력 완료까지 걸린 시간이 7개 계정에서 모두 평균 11초 안팎, 필드 간 전환 순서와 키 입력 오류율이 거의 0이라면, 사람이 여러 명이라고 보기 어렵다.

세션 내 페이지 체류 시간의 분산도 힌트다. 실사용자는 재방문 시 더 빨라지되, 여전히 콘텐츠에 따라 체류 시간 폭이 커진다. 반면 스크립트는 매번 비슷한 체류 시간을 만든다. 예외도 있다. 고급 자동화는 랜덤 지연과 노이즈를 섞는다. 이럴 땐 노이즈의 분포가 너무 균등하거나 베타 분포 형태가 반복되는지 의심해본다.



프로필, 결제, 계정 외부자원의 연결고리

다계정은 대개 자금 흐름과 연결된다. 카드 결제라면 BIN, 발급국, 선불카드 여부, 3D 인증 실패 이력, 동일 카드로 시도된 다른 계정 수가 단서가 된다. 휴대폰 본인인증 기반이라면 통신사, 개통 연월, MVNO 비중, 동일 명의의 최근 등록 밀도를 본다. 가상계좌나 간편결제는 토큰과 디바이스 바인딩 정보의 재사용이 흔하다.

이메일과 전화번호 패턴도 무시하지 않는다. 유사 로컬파트 규칙, 생성 일자, 임시메일 도메인 사용 여부가 반복되면 점수를 올린다. 추천 코드, 쿠폰 입력 타이밍, 동일 기기에서 다수 계정의 쿠폰 사용이 연쇄로 일어나는지도 본다. 특히 추천인 보상 구조가 있다면, 동일 디바이스 해시에서 피추천 5건 이상이 24시간 내 발생하는 패턴은 위험하다.

자동화 프레임워크의 흔적

Selenium, Playwright 같은 프레임워크는 점점 더 자연스러워지고 있지만, 완벽하진 않다. 브라우저 속성에서 webdriver 플래그가 제거되더라도, 네트워크 계층에서 HTTP/2 설정, TLS 확장 순서, 압축 사전 유무가 도구별로 일정한 경우가 많다. 헤드리스 모드가 감춰져도 입력 이벤트의 타임스탬프가 프레임 경계에 과도하게 정렬된다거나, 가시성 API와 포커스 이벤트의 순서가 인간 행동과 어긋나는 징후가 발견된다. 모바일 자동화는 ADB 브리지 흔적, 비정상적인 패키지 서명, 테스트용 인증서의 신뢰 설정에서 드러난다.

로그를 다루는 방식이 절반을 결정한다

다계정 식별이 실패하는 가장 흔한 이유는 신호의 부재가 아니라, 신호가 흩어져 있다는 점이다. 이벤트 스키마를 먼저 정리하자. 세션 시작과 종료, 디바이스 특성 스냅샷, 네트워크 지표, 폼 입력 이벤트, 결제 요청과 결과를

서로 참조 가능한 키로 저장한다. 피처 저장소를 별도로 두고, 계산 비용이 큰 지표는 사전 집계한다. 예를 들어 계정별 최근 7일 디바이스 해시 다양성과 로그인 도시 수, 동일 디바이스 해시에서 로그인한 계정 수를 매일 업데이트하면, 실시간 판단이 훨씬 빨라진다.

보존 기간과 샘플링 정책은 먹튀검증 목적에 맞춰야 한다. 보너스 어뷰징은 이벤트 발생 후 한 달 안에 집중되지만, 환전 기반 다계정은 길게 준비한다. 최소 6개월, 가능하면 12개월 단위로 핵심 지표를 보존하면 유의미한 상관관계를 더 많이 잡아낸다.

오탐을 줄이는 현장 감각

한국 특수성을 간과하면 오탐이 폭증한다. 대표적인 예외는 PC방과 학교 기숙사다. 같은 IP, 유사한 접속 시간대, 심지어 비슷한 게임 설치 환경을 공유한다. 이런 환경에선 세션 중첩과 행동 패턴의 다양성으로 구분한다. 다계정 집단은 보통 짧은 주기로 여러 계정을 순환시키고, 각 세션이 완결된 행동 흐름을 반복한다. 반면 정상 집단은 개별 플레이패턴의 변화가 크다.

모바일 통신사 CGNAT도 고민거리다. 특정 ASN에서 갑작스러운 다계정 의심이 쏟아지면, 통신사 라우팅 변경이나 대규모 NAT 풀 교체가 원인일 수 있다. 이런 변화를 감지하기 위해 ASN 시계열을 모니터링하고, 단순 IP 일치보다 디바이스와 행동 신호를 가중한다. 가족이 하나의 기기를 공유하는 경우도 있다. 이럴 때는 동일 기기 내 프로필 정보를 비교한다. 생년월일, 선호 언어, 접근 시간대, 결제 수단이 충분히 다르면 정상으로 본다. 당연하지만, 판정 근거는 반드시 로그로 남겨야 한다.

실무 워크플로우, 이 순서로 굴려라

- 수집과 정규화: 앱과 웹의 이벤트를 단일 스키마로 묶고, 디바이스, 네트워크, 행동 지표를 원천에서부터 추출한다.
- 매칭과 군집화: 디바이스 해시, 네트워크 지표, 행동 유사도를 이용해 계정 간 연결 그래프를 만든다. 연결 강도는 가중치로 표현한다.
- 스코어링: 약한 신호 다수를 점수화해 합산한다. 규칙 기반과 간단한 모델을 혼합하되 해석 가능성을 유지한다.
- 검토 대기열 운영: 임계치 이상은 즉시 제재가 아닌 수동 검토로 보낸다. 케이스당 5분 내 결론을 내릴 수 있도록 근거 패널을 설계한다.
- 조치와 피드백 루프: 정지, 제한, 추가 인증 같은 조치를 표준화하고, 결과를 라벨로 회수해 임계치와 규칙을 재보정한다.

점수 모델은 가볍고 설명 가능해야 한다

복잡한 딥러닝 모델로 시작할 필요는 없다. 다계정은 설명 가능성이 중요하고, 피의자 소명 요청에 대한 내부 설명이 가능해야 한다. 로지스틱 회귀나 점수 카드 방식이면 충분하다. 신호별 가중치는 데이터로 정하되, 인과는 도메인 지식으로 검증한다. 예를 들어 동일 디바이스 해시에서 3개 초과 계정이 24시간 내 생성된 경우 30점, 동일 JA3와 동일 ASN 범위에서 5개 계정의 순차 로그인은 15점, 회원가입 폼 입력 속도 분산이 극단적으로 낮으면 20점처럼 가중치를 시작하고, 검토 결과로 조정한다.

임계치는 큐 처리 능력에 맞춰 설정한다. 하루 1천 건 의심 사례 중 10퍼센트를 수동 검토할 수 있다면, 상위 100건이 실제 타격 가능성이 높은지, 정밀도와 재현율이 어느 정도인지 매주 점검한다. 필요하면 시뮬레이션 환경에서 A, B 정책을 병렬 운용해 손실 저감과 고객 불편의 균형을 맞춘다.

증거 보존과 고객 커뮤니케이션

먹튀검증은 기술 싸움이기도 하지만, 절차 싸움이기도 하다. 제재에 앞서 스냅샷을 확보한다. 의심 계정 묶음의 연결 근거, 주요 이벤트 타임라인, 디바이스와 네트워크 지표의 변동 내역을 PDF나 내부 리포트 형식으로 고정한다. 외부 분쟁이 생기면 이 기록이 방패가 된다.

고객 커뮤니케이션도 중요하다. 다계정 의심으로 제한을 걸 때는 모호한 문구 대신, 추가 인증이 필요한 이유와 범위를 명확히 설명한다. 예를 들어 최근 동일 기기에서 복수 계정이 단기간에 생성되어 본인 확인이 필요하다는 수준의 구체성이면 충분하다. 근거의 모든 기술적 세부를 공개할 필요는 없지만, 임의적 제재가 아니라는 인상을 주어야 한다.

개인정보보호와 규제 준수

다계정 식별을 강화하면서 개인정보를 과도하게 모으는 실수를 범하기 쉽다. 목적 제한과 최소 수집 원칙을 지킨다. 국내에서는 개인정보보호법과 정보통신망법, 전자금융거래법, 신용정보법 적용 범위를 고려해야 한다. 디바이스 지문처럼 개인을 식별할 수 있는 정보는 수집 목적과 보존 기간을 명시하고, 동의를 받거나 정당한 이익의 근거를 문서화한다. 정보는 암호화하고 접근 권한을 세분화한다. 개발, 분석, 운영 환경 간 반출 절차를 분리해 오남용을 막는다.

해외 트래픽이 섞인다면 역외 이전 요건과 국외 이전 고지도 챙긴다. 내부적으로는 프라이버시 영향평가를 정기적으로 수행하고, 민감한 신호의 사용을 검토 위원회에서 승인받는 절차를 만들어두면 나중에 도움이 된다.

현장에서 자주 쓰는 신호 조합 예시

보너스 어뷰징 방지에선 가입 직후 행동이 핵심이다. 회원가입 완료 후 5분 이내에 쿠폰 페이지를 열고, 동일 디바이스에서 다수 계정이 연쇄로 같은 경로를 밟는 패턴은 강력한 신호다. 여기에 이메일 도메인이 임시메일 서비스로 분포가 몰리고, 비정상적으로 빠른 폼 입력이 겹치면 스코어를 충분히 채울 수 있다.

환전형 먹튀 의심에선 결제와 인출 경로를 본다. 신규 계정 다수가 비슷한 금액대를 같은 시간대에 입금하고, 짧은 체류 후 특정 이벤트만 수행한 뒤, 새로운 기기에서 연쇄로 인출을 시도하는 경우가 있다. 이때 네트워크 신호는 분산돼도, 기기 지문과 행동 유사도가 연결해준다. 카드 BIN이나 간편결제 토큰이 반복되면 증거는 더 단단해진다.

간단한 사례로 보는 작업 흐름

작년 말, 보너스 어뷰징 신고가 하루에 200건 이상 들어왔다. 첫 스크리닝에선 IP가 제각각이라 잡히지 않았다. 디바이스 지문을 펼치니 WebGL 렌더러가 동일하고 캔버스 해시가 3가지 군집으로 묶였다. 각 군집에서 가입 시간 간격이 45초 내외로 일정했고, 회원가입 폼의 백스페이스 사용 빈도가 거의 0에 가까웠다. JA3 지문은 세 군집 모두 동일했고, ASN은 서로 달랐다. 프록시 회전을 돌린 것으로 보였다.

연결 그래프를 만들자 계정 27개가 세 묶음으로 정리됐다. 가입 후 쿠폰 페이지까지 도달하는 클릭 시퀀스가 14번 클릭, 총 소요 38초 내외로 거의 일치했다. 수동 검토에서 각 계정의 이메일 도메인 80퍼센트가 임시메일이었다. 스코어 카드 기준으로 70점 이상이었고, 조치 정책에 따라 보너스 환수와 본인 확인 요청이 나갔다. 이틀 뒤 동일 패턴이 사라졌고, 일주일 평균 보너스 비용이 34퍼센트 줄었다. 재발 방지를 위해 회원가입 폼에 동적 지연과 난수형 필드 순서를 일부 도입해 자동화 비용을 올렸다.

데이터 모델과 대시보드의 작은 차이가 실무 효율을 바꾼다

검토자가 5분 내 결론을 내려면, 근거가 한 화면에서 보이는 구성이 필요하다. 계정 요약, 연결 그래프, 최근 7일 이벤트 타임라인, 핵심 신호 점수 기여도를 정적 패널로 배치한다. 그래프는 과도한 상호작용보다, 강한 엣지 상위 10개만 보여주는 단순화가 낫다. 모델이 낸 총점만 보여주지 말고, 기여 상위 3개 신호의 세부값과 비교 기준을 함께 표기한다.

데이터 모델에서는 세 가지 키를 잊지 않는다. 계정 키, 디바이스 키, 네트워크 키다. 디바이스 키는 다중 해시를 갖게 두고, 신뢰도 점수를 부여한다. 예를 들어 브라우저 기반 지문과 앱 기반 설치 ID가 일치하면 신뢰도는 높아지고, 쿠키만 있을 때는 낮아진다. 네트워크 키는 IP 단독이 아니라 ASN, 도시, 프록시 여부, JA3를 묶은 복합 키를 쓴다. 이런 복합 키는 공격자가 부분을 바꿔도 연결성을 유지하게 해준다.

현장 점검 체크리스트

- 동일 디바이스 해시에서 생성된 계정 수와 생성 간격을 모니터링하고, 24시간 기준 임계치를 정했는가
- JA3, HTTP/2 설정, TLS 확장 순서 등 네트워크 지문을 수집하고, 프록시 지표와 결합했는가
- 폼 입력 시간 분포, 클릭 간격, 스크롤 패턴 등 행동 지표를 벡터화해 유사도 비교를 운영하고 있는가
- 결제 수단의 재사용, BIN 분포, 간편결제 토큰 연결을 정기 리포트로 검토하는가
- 제재 전 근거 스냅샷을 자동 생성하고, 고객 커뮤니케이션 문안을 표준화했는가

현업 도구와 구현 팁

상용 지문 솔루션을 쓰든, 자체 구축을 하든 원칙은 같다. 지문은 단일 값보다 다중 조각의 모음이어야 한다. 브라우저에선 캔버스와 WebGL, 오디오 컨텍스트, 폰트 측정, 타임존과 언어, 하드웨어 동시 스레드 수를 결합한다. 앱에선 설치 ID, 키체인 저장값, 서명 해시, 기기 모델과 OS 빌드, 루팅 지표를 묶는다. 저장 시 원시값을 그대로 보관하지 말고, 원시값과 해시를 분리해 관리한다. 해시는 비교에 쓰고, 원시값은 접근을 제한한다.

행동 데이터는 수집 비용이 부담스럽다. 전체 이벤트를 다 모으지 말고, 회원가입과 로그인, 결제, 인출 등 핵심 흐름에서만 고해상도 로그를 남긴다. 마우스 이벤트는 20ms 이내, 모바일 터치는 10ms 이내 해상도면 충분하다. 저장 용량을 줄이려면 히스토그램과 요약 통계를 병행하고, 원시 스트림은 단기 보관 후 폐기한다.

네트워크 지표는 서버단에서 캡처하는 편이 신뢰도가 높다. 클라이언트가 보낸 사용자 에이전트는 위장되기 쉽다. 반면 서버가 관찰하는 TLS 핸드셰이크, HTTP/2 우선순위, 헤더 순서, 압축 방식은 공격자가 제어하기 어렵다. 로드밸런서나 WAF 레벨에서 이 신호를 추출해 어플리케이션 로그와 연결하면 효과가 좋다.

먹튀검증 관점의 운영 전략

정책은 단단하게, 집행은 유연하게 가져간다. 다계정 의심이 스코어 임계치를 넘었다고 해서 즉시 영구 정지로 가면 반발과 분쟁이 커진다. 추가 인증과 사용 제한, 혜택 회수 같은 단계적 조치를 설계하면 손실을 막으면서도 오탐의 충격을 줄일 수 있다. 내부 리뷰 보드가 주기적으로 샘플을 점검하고 규칙의 적절성을 평가하는 루틴이 필요하다. 케이스 리뷰를 통해 새 신호를 발굴하고, 낡은 규칙을 퇴출시키는 속도가 곧 방어력이다.

먹튀 시도는 정책 변경 직후 흔히 재탐색을 시도한다. 릴리즈 이후 첫 72시간을 집중 모니터링하고, 트래픽 급증과 스코어 분포 변화를 함께 본다. 방어 수단이 알려질수록 상대는 우회 경로를 찾는다. 이 쫓고 쫓기는 게임에서 중요한 것은 완벽한 차단이 아니라, 공격 비용을 점점 비싸게 만드는 것이다.

마지막으로, 숫자로 관리하자

감으로 운영하면 금방 한계가 온다. 핵심 지표를 몇 가지로 좁혀 꾸준히 본다. 예를 들어 신규 가입 대비 의심 스코어 상위 5퍼센트의 비율, 먹튀검증 의심 묶음당 평균 계정 수, 보너스 비용 대비 환수율, 제재 후 재시도까지의 평균 시간, 수동 검토 정밀도와 재현율. 분모 분자를 명확히 하되, 시스템 변경이 있을 때 단절점을 표기한다. 그래프가 거짓말하지 않도록 정의를 문서화한다.

먹튀검증은 소프트웨어처럼 끊임없는 버전업이 필요하다. 오늘 유효한 신호가 내일 낡아질 수 있다. 강한 신호 하나에 기대지 말고, 여러 약한 신호를 결합해 점수를 만들자. 현장의 제약과 법적 테두리를 존중하되, 공격자의 비용을 높이는 방향으로 꾸준히 진화하자. 다계정의 흔적은 반드시 남는다. 우리가 그 조각을 모아 읽을 준비만 되어 있다면, 먹튀는 손쉬운 돈벌이가 아니다.