고액 먹튀(高額 未渡) 사례의 가속화 배경과 다층 방지·대응 전략

최태원 / (주)먹튀위크 대표

제1장. 서론

1.1 문제 제기 및 배경

최근 수년간 온라인 사설 승부(勝負) 시장에서 발생하는 고액 먹튀 사고의 규모와 빈도는 급증 추세를 보이고 있다. 기존에는 몇십 만 원에서 수백만 원 수준의 소액 피해가 주를 이루었다면, 현재는 수억 원에서 많게는 십억 원 단위에 이르는 고액 환전 불이행(이하 '고액 먹튀') 사례가 빈번히 보고되고 있다. 특히 2021년 이후 먹튀 사고 데이터베이스(DB) 상위 10건 중 7건이 1억 원 이상의 고액 피해로 분류되고 있으며, 이는 단순한 사용자 부주의나 일회성 사고로 보기 어려운 구조적 문제를 시사한다.

이러한 문제의 중심에는 이른바 '메이저놀이터'라 불리는 대형 사설 업장들의 경쟁 구도가 자리하고 있다. 이들 업장은 통상적으로 자동화된 입출금 시스템, 다종다양한 승부 종목, 고도화된 프론트엔드 UI/UX를 통해 사용자 편의성과 접근성을 극대화하며, 공격적인 온라인 마케팅을 기반으로 단기간에 대규모 이용자 유입을 유도한다. 문제는 이러한 성장 전략이 과도한 초기 가입 혜택(가입 첫충 30~40%, 무한 매충 10% 이상)과 과소한 환수율을 동반하며, 결과적으로 업장의 재무 건전성을 위협한다는 점이다. 환수율이 일정 수준 이하로 낮아질 경우, 이용자가 고액 환전을 청구하는 순간 업장은 유동성 부족 상황에 직면하게 되고, 이로 인해 먹튀라는 극단적 선택이 빈번하게 발생한다.

더욱이 업계 표준으로 자리잡은 몇몇 솔루션의 독점적 지위는 단일 취약점 공격 시 다수 업장이 동시에 피해를 입을 수 있는 '시스템 리스크'를 증대시키고 있다. 특히 탈취된 사용자 개인정보가 암시장에서 거래되며, 이를 이용한 유사 업장 가장(假裝) 및 재피싱 사례가 기하급수적으로 증가하고 있다. 피해자들은 자신이 이용하던 업장과 동일 계열이라 소개받은 사이트에 고액 자금을 예치하고, 결국 또 다른 먹튀 피해를 입게 된다.

본 연구는 이러한 다층적 문제 구조를 체계적으로 분석하고, 고액 먹튀 사고의 발생 메커니즘과 구조적 원인을 규명함으로써, 실효성 있는 방지 및 대응 전략을 제시하고자 한다.

1.2 연구 목적 및 질문

본 논문은 고액 먹튀 사례의 가속화 배경을 정량적·정성적으로 규명하고, 이를 방지하기 위한 기술적·제도적·행태적 대응 전략을 복합적으로 모색

하는 것을 주된 목적으로 한다. 이를 위해 다음과 같은 연구 질문을 설정하였다.

- RQ1: 메이저놀이터 간 경쟁 구조와 고액 먹튀 사고 발생 간에는 어떤 관계가 존재하는가?
- RQ2: 특정 솔루션에 대한 과의존 및 정보 유출은 고액 피해를 어떻게 증폭시키는가?
- RQ3: 호텔 게임 중심의 고빈도·고액 승부 트렌드는 피해 규모에 어떤 영향을 미치는가?
- RQ4: 고액 먹튀를 실질적으로 억제할 수 있는 기술적·제도적 대응은 무엇인가?

1.3 연구 방법 및 구성

본 연구는 먹튀 사고 사례를 다수 보유한 민간 데이터베이스와, 업계 종사자 및 보안 전문가 대상의 심층 인터뷰, 그리고 유저 커뮤니티 분석 등을 복합적으로 활용한 혼합연구(Mixed Method)를 통해 진행된다. 정량적으로는 로지스틱 회귀 분석과 민감도 시뮬레이션을 수행하며, 정성적으로는 주요 사례 분석과 델파이 조사(Delphi Survey)를 적용하였다.

논문의 구성은 다음과 같다. 2장에서는 국내외 선행 연구와 이론적 배경을 바탕으로 온라인 사설 승부 시장의 진화와 먹튀 사고의 변화를 고찰한다. 3장에서는 연구 설계, 데이터 수집 방식, 변수 구성과 분석 방법을 상세히 설명한다. 4장에서는 실증 분석 결과와 시나리오 시뮬레이션 결과를 제시하고, 5장에서는 이 결과에 기반한 기술·제도·이용자 대응 전략을 논의한다. 마지막 6장에서는 결론 및 정책적 시사점을 정리하고, 본 연구의 한계와 향후 과제를 제안한다.

제2장. 문헌 고찰

2.1 온라인 사설 승부 시장 개요

온라인 사설 승부 시장은 과거 ‘통협팀’이라 불리는 비공식 중개조직을 통한 폐쇄적 가입 경로가 지배적이었다. 당시에는 신규 가입 자체가 매우 제한적이었으며, ‘안전공원’이나 ‘환전 잘 되는 업장’이라는 구전 중심의 신뢰 체계에 의존해야 했다. 하지만 가상계좌 기반 자동화 시스템이 도입된 이후, 신규 가입의 진입 장벽은 급격히 낮아졌고, 이로 인해 시장의 규모가 폭발적으로 확대되었다. 기존의 수작업 기반 입출금 시스템이 자동화되면서, 운영 인건비는 대폭 절감되었고, 가입자 규모에 비례한 프로모션 마케팅이 핵심 경쟁 수단으로 부상하였다.

이러한 변화는 ‘메이저놀이터’라는 개념의 등장을 가져왔다. 메이저놀이터는 초기 안정성과 빠른 환전으로 입소문을 탄 후, 공격적인 인센티브 제공을 통해 대규모 트래픽을 흡수하였다. 그러나 곧장 심각한 부작용도 나타났다. 극단적인 출혈 경쟁과 무리한 혜택 제공은 환수율의 급락을 불러왔고, 일부 업장은 고액 이용자와의 환전 약속을 지킬 수 없는 상황에 직면했다. 이러한 구조적 취약성은 결과적으로 먹튀 사고의 원인으로 작용하게 된다.

2.2 먹튀 사례 연구 및 유형

기존 연구들은 먹튀 사고를 크게 세 가지 유형으로 분류한다. 첫째는 '계좌 고의 오류형'으로, 입금 오류나 계좌 일시 정지 등을 핑계로 환전을 거부하는 방식이다. 둘째는 '플랫폼 폐쇄형'으로, 운영체제를 갑작스럽게 종료하고 사이트를 폐쇄하는 형태이며, 이 경우 추적이 매우 어렵다. 셋째는 '사칭 유도형'으로, 기존 업장을 사칭하거나 유사한 이름을 사용하여 기존 사용자에게 접근한 뒤 신규 자금을 유도하는 방식이다. 특히 세 번째 유형은 솔루션 보안 취약점과 DB 유출이 주요 배경으로 작용한다.

고액 먹튀 사고는 이들 유형 중 두 번째, 세 번째에서 주로 발생하며, 사고 발생 시 피해자는 환전 거절 외에도 개인정보 악용, 반복적 스팸 피싱 등의 2차 피해에 노출된다. 그러나 해당 분야는 실증적 데이터 접근이 어렵고, 사고가 은폐되거나 신고되지 않는 경우가 많아 연구가 미진한 상황이다. 본 논문은 이 간극을 메우고자 실제 DB 기반 사례분석을 포함하여 논의 범위를 확장한다.

2.3 데이터 유출 및 솔루션 보안 문제

최근 먹튀 사고에서 핵심 리스크로 부상한 것은 솔루션 공급업체의 독점 구조다. 상위 2~3개의

솔루션이 전체 업장의 80% 이상을 점유하고 있으며, 동일한 백엔드 구조와 API를 공유하고 있어 단 하나의 취약점이 발생할 경우 수십 개의 업장이 동시에 피해를 입을 수 있는 '시스템 리스크(systemic risk)' 상태에 놓여 있다.

2022년 하반기, 이들 솔루션 중 하나에서 발생한 보안 결함은 19만여 명의 개인정보가 유출되는 대형 사고로 이어졌다. 이 데이터는 암시장에서 거래되었고, 이를 이용한 사칭업장 설계, 타겟 피싱, 유사 업장 유도 등 다양한 2차 범죄로 확산되었다. 본 연구는 이러한 데이터 유출의 구조적 원인을 식별하고, 기술적 대안을 제시하는 데 초점을 둔다.

2.4 유동성과 고액 먹튀의 상관성

전통적으로 사설 승부 업장에서는 스포츠 예측형 콘텐츠가 주류였다. 그러나 최근 미니게임 및 호텔 게임의 대중화는 사용자 행동 패턴에 커다란 변화를 일으켰다. 특히 1분, 3분 단위로 결과가 나오는 고빈도 게임의 등장은 사용자로 하여금 빠른 자금 순환과 고액 베팅을 유도했고, 이는 자연스럽게 업장의 유동성 부담을 가중시켰다.

이용자 입장에서는 연속된 승리로 거액의 환전 청구권을 확보했지만, 업장 입장에서는 한정된 유동성 풀에서 이 수요를 감당할 수 없어, 구조적으로 먹튀를 선택할 수밖에 없는 상황이 발생하고 있다. 즉, 유동성 리스크가 단일 업장 차원의 문제가 아니라, 산업 전반에 영향을 미치는 구조적 리스크로 전이되고 있는 것이다.

제3장. 연구 설계 및 방법론

3.1 데이터 수집 및 분석 절차

본 연구는 고액 먹튀 사고의 구조적 특성을 규명하기 위해 정량 데이터와 정성 데이터의 혼합 분석을 설계하였다. 우선 정량 데이터는 2019년 1월부터 2024년 3월까지 접수된 총 14,327건의 먹튀 사고 제보 중, 중복성 제거 및 1차 필터링을 거쳐 유효성 있는 6,412건을 분석 대상으로 선정하였다. 이 데이터는 국내 대표적인 먹튀 검증 전문 기관에서 축적한 실시간 사례를 기반으로 구성되었으며, 피해 금액, 업장 유형, 사용 솔루션, 게임 분류, 환전 거절 사유, 사고 발생 시점 등의 항목을 포함하고 있다.

정성 데이터의 경우, 업계 운영진 4명, 보안전문가 3명, 사고 피해자 7명, 탈취 DB 유통 브로커 2인 등 총 16명을 대상으로 심층 인터뷰를 실시하였다. 인터뷰는 반구조화된 방식으로 진행되었으며, 대화 내용은 녹취 후 텍스트화되어 질적 코딩(Qualitative Coding)을 통해 분석되었다. 또한 2022~2023년 동안 국내 주요 커뮤니티 4곳에서 발생한 먹튀 피해 사례 185건에 대한 댓글 및 피드백을 텍스트 마이닝 기법으로 수집·분석하여 사용자 인식과 피해 경험의 경향성을 파악하였다.

3.2 변수 구성 및 이론 모형

정량 분석에서는 고액 먹튀의 발생 확률 및 피해 규모를 설명하는 독립 변수로 다음의 항목을 채택하였다. 첫째, ‘솔루션 집중도(Solution Concentration)’는 전체 시장 내 상위 3개 솔루션의 점유율을 비율로 측정하였다. 둘째, ‘혜택 인플레이션(Benefit Index)’은 업장에서 제공하는 가입 충전 비율, 무한 매충, 이벤트 등 보너스 비율을 종합하여 0~100 범위의 지수로 산출하였다. 셋째, ‘호텔 게임 비중(Hotel Game Share)’은 전체 승부 금액 중 미니게임 및 딜러형 콘텐츠가 차지하는 비율로 측정하였다.

종속 변수는 크게 두 가지로 설정되었다. 첫 번째는 ‘고액 먹튀 여부(High-Level Default)’로, 피해 금액이 1,000만 원 이상일 경우 1, 미만일 경우 0으로 이분화된 더미 변수이다. 두 번째는 ‘피해 금액 규모(Damage Amount)’로, 로그 변환된 실수 값을 사용하여 이상치의 영향을 최소화하였다. 분석에는 통제 변수로서 업장의 운영 기간, 이용자 수, 1일 평균 거래 건수, 최근 3개월 내 사고 이력 여부 등을 포함하였다.

이론적 모형은 다음과 같다.

- H1: 솔루션 집중도가 높을수록 고액 먹튀 발생 확률이 증가한다.
- H2: 호텔 게임 비중이 높을수록 피해 금액이 증가한다.

- H3: 혜택 인플레이션 지수가 높을수록 고액 먹튀 빈도가 높다.
- H4: 솔루션 집중도와 혜택 인플레이션 간에는 상호작용 효과가 존재한다.

모형 검증은 로지스틱 회귀분석(Logistic Regression)과 OLS(Ordinary Least Squares) 회귀를 각각 수행하며, 상호작용 항(interaction term)의 유의성과 설명력을 비교 분석하였다.

3.3 정량적/정성적 분석 방법 설명

정량 분석의 경우, SPSS 및 Stata 프로그램을 사용하여 기술 통계 및 회귀분석을 실시하였다. 로지스틱 회귀에서는 종속변수로 고액 먹튀 여부를 설정하고, 주요 독립 변수 및 통제 변수들을 단계별로 투입하여 모형의 적합도(AIC, BIC)와 설명력(McFadden R^2)을 평가하였다. 피해 금액 규모를 종속변수로 한 OLS 회귀에서는 로그 정규 분포 조건을 충족시키기 위해 수치 데이터에 로그 변환을 사전 적용하였다. 다중공선성 여부는 VIF(Variance Inflation Factor)를 통해 진단하였다.

정성 분석은 NVivo 프로그램을 활용하여 인터뷰 내용을 주제별로 코딩하고, 반복적 주제의 출현 빈도를 기준으로 핵심 인사이트를 도출하였다. 주요 분석 항목은 다음과 같다: (1) 고액 환전 시 업장 대응 방식, (2) 솔루션 업체와의 관계, (3) 보안 취약점 경험 여부, (4) 사고 이후 이용자 대처 방식. 아울러 커뮤니티 기반 텍스트 마이닝에서는 형태소 분석과 토픽 모델링을 병행하여, 시간대별 이슈 확산 양상과 신뢰도 변화 추이를 시계열 형태로 시각화하였다.

이러한 분석 방법을 통해 고액 먹튀 사고가 발생하는 주요 조건과 패턴을 식별하고, 정성적 사례가 정량적 분석 결과를 어떻게 보완하는지를 종합적으로 검토할 수 있었다. 다음 장에서는 본 연구에서 도출된 실증 분석 결과를 제시하고, 이에 기반한 시뮬레이션을 통해 고액 먹튀의 확산 가능성과 예방 효과를 수치적으로 확인한다.

제4장. 실증 분석 및 시뮬레이션 결과

4.1 사고 유형별 통계

본 연구에서 분석한 6,412건의 유효 먹튀 사고 사례는 다음과 같은 특징을 보였다. 전체 사고 중 피해 금액이 1,000만 원 이상으로 분류되는 고액 먹튀 사례는 1,324건(20.6%)으로 나타났다. 이들 사례는 피해자의 자금 규모뿐만 아니라 업장의 규모, 운영 기간, 사용 솔루션 유형에서 통계적으로 유의미한 차이를 보였다. 특히 고액 먹튀 사고의 78.3%는 호텔 게임 기반 업장에서 발생하였으며, 전체 피해 금액의 64.1%가 이 범주에서 집중되었다.

또한, 상위 3대 솔루션이 사용된 업장에서 발생한 사고는 전체 사고의 85.7%를 차지하였으며, 이 중 1개 솔루션에 의존한 업장에서만 전체 피해액의 47.2%가 발생하였다. 이는 솔루션 모노컬처(monoculture)가 시스템 리스크를 어떻게 증폭시키는지를 방증한다. 가입자 수 대비 사고 발생률 또한 상위 20개 업장에서 집중적으로 나타났으며, 이들 업장은 모두 과도한 인센티브를 제공하고 있는 것으로 확인되었다.

정성 인터뷰 분석에서도 사고 피해자 대부분이 “이전 이용 경험이 있었던 메이저 업장과 동일한 디자인 및 구조의 사이트로부터 피싱을 당했다”고 진술하였으며, 이는 솔루션 기반 재활용이 먹튀 범죄에 악용되고 있다는 실증적 근거를 제공한다. 특히 피해 규모가 클수록 반복적 사고 노출 가능성이 높아졌으며, 인터뷰 응답자의 61%가 2회 이상 피해를 경험했다고 응답하였다.

4.2 회귀분석 결과

로지스틱 회귀 분석을 통해 고액 먹튀 여부에 영향을 미치는 주요 요인을 분석한 결과, 다음과 같은 계수 추정치가 도출되었다.

- 솔루션 집중도: $\beta = 1.17$ (OR = 3.22, $p < .001$)
- 호텔 게임 비중: $\beta = 0.07$ (OR = 1.07, $p < .01$)
- 혜택 인플레이션: $\beta = 0.05$ (OR = 1.05, $p < .05$)
- 솔루션 × 혜택 교호항: $\beta = 0.11$ (OR = 1.12, $p < .05$)
- McFadden $R^2 = 0.38$, AIC = 3,212

이는 솔루션 집중도가 고액 먹튀 발생에 있어 매우 유의한 설명력을 가지며, 호텔 게임 비중 또한 피해 확률을 유의하게 증가시킨다는 것을 나타낸다. 특히 솔루션 집중도와 혜택 인플레이션 간의 교호작용(interaction)은 상호 증폭 효과를 보이며, 이들 요인이 결합될 경우 고액 피해 확률이 더욱 높아짐을 시사한다.

OLS 회귀 결과에서도 동일한 경향이 확인되었다. 피해 금액 규모를 종속변수로 설정한 분석에서 솔루션 집중도는 로그 피해액 증가에 대해 $\beta = 0.43$ ($p < .001$)의 유의미한 영향을 미쳤으며, 호텔 게임 비중은 $\beta = 0.19$ ($p < .01$)로 나타났다. 혜택 인플레이션은 피해액 규모보다는 고액 먹튀 발생 빈도에 더 강한 영향력을 미치는 것으로 분석되었다.

4.3 시나리오 기반 시뮬레이션 결과

에이전트 기반 시뮬레이션(Agent-Based Simulation)을 통해 고액 먹튀 사고의 발생 가능성과 확산 속도를 추정하였다. 시뮬레이션은 10만 개의 가상 이용자와 500개의 업장을 대상으로 24개월간의 시간 축을 설정하였으며, 시나리오별로 (1) 솔루션 취약점 발생 여부, (2) 호텔 게임 집중도, (3) 혜택 인플레이션 정도를 조절하였다.

기본 시나리오에서는 월평균 고액 먹튀 발생 건수가 54건, 누적 피해액이 약 312억 원으로 추산되었다. 반면 솔루션 집중도가 높고, 혜택 인플레이션이 과도하며, 호텔 게임 집중도가 60% 이상인 고위험 시나리오에서는 월평균 고액 사고 118건, 연간 피해액 약 872억 원으로 증가하였다. 이는 기본 시나리오 대비 2.8배 높은 수치이며, 구조적 리스크가 통제되지 않을 경우 사고 규모가 기하급수적으로 증가할 수 있음을 보여준다.

한편, 방어 전략 시나리오(솔루션 다양화 + 혜택 상한선 도입 + 고액 트랜치 환전 시스템 적용)를 적용한 경우, 동일한 기간 동안 고액 먹튀 사고 건수는 31건으로 절반 가까이 감소하였고, 누적 피해액도 약 176억 원으로 낮아졌다. 이는 기술적·제도적·행태적 대응이 병행될 경우 사고 예방 효과가 상당함을 입증하는 결과이다.

다음 장에서는 이러한 분석 결과를 토대로 실제 적용 가능한 정책적 시사점을 논의하고, 각 대응 전략이 가질 수 있는 기대 효과와 구현 현실성을 평가한다.

제5장. 논의 및 정책적 시사점

5.1 기술적 방어 전략

실증 분석 결과는 고액 먹튀의 주요 발생 배경이 솔루션 집중도와 호텔 게임 중심의 자금 회전 구조에 있다는 점을 명확히 보여준다. 따라서 가장 먼저 요구되는 것은 기술적 인프라의 재설계이다. 현재의 솔루션 모노컬처 구조는 업계 전체를 하나의 취약점에 종속시키는 시스템 리스크 구조이며, 이를 해소하기 위해서는 다중 솔루션 아키텍처(multisolution architecture)를 채택할 필요가 있다.

다중 솔루션 아키텍처는 단순히 다양한 개발사에 의존하는 것을 넘어, 모듈형 서비스 (Microservices Architecture)를 통해 주요 기능별 독립적 검증 체계를 갖추는 방식이다. 예를 들어, 결제 모듈, 게임 모듈, 이용자 인증 모듈을 분리하여, 각각에 대해 상이한 보안 솔루션을 적용하면 단일 취약점이 전체 시스템에 영향을 미치는 것을 방지할 수 있다.

또한, 고액 환전에 대한 불투명성 해소를 위해 블록체인 기반의 영지식증명(Zero-Knowledge Proof, ZKP) 기술을 도입한 입출금 무결성 검증 체계 구축도 고려되어야 한다. 이를 통해 이용자는 자신의 거래가 실제 발생했음을 외부 감사 없이 확인할 수 있으며, 운영자는 데이터 위변조 리스크에서 벗어나게 된다. 해당 방식은 프라이버시 보호와 감사 투명성이라는 두 마리 토끼를 동시에 잡을 수 있는 방안으로 제시된다.

추가적으로, AI 기반 이상금융거래 탐지 시스템 (Fraud Detection System, FDS)의 고도화가 필수적이다. 기존 FDS는 일정 금액 초과 시 단순 경고 수준에 그쳤으나, 본 연구 결과를 기반으로 업장별 리스크 프로파일링과 거래 패턴의 실시간 학습이 가능한 머신러닝 기반 FDS 체계가 구축된다면, 고액 환전 요청 직전에 선제적 차단이 가능할 것이다.

5.2 제도적/거버넌스 모델

기술적 대응이 시스템 레벨의 리스크를 줄이는 데 효과적이라면, 제도적 대응은 산업 전반의 신뢰성을 회복하는 핵심 수단이다. 본 연구에서는 다음과 같은 거버넌스 모델을 제안한다.

첫째, 민간 중심의 '담보 예치형 공적 보증 기구' 설립이 필요하다. 이 기구는 각 업장이 일정 비율(예: 월간 총 입금액의 10%)을 별도 계좌에 담보 형태로 예치하게 하고, 고액 환전 요청 시 이 자금을 통해 지급 이행력을 확보하는 역할을 수행한다. 이를 통해 갑작스러운 유동성 부족으로 인한 먹튀 가능성을 선제적으로 차단할 수 있다.

둘째, '사고 이력 기반의 실명제 데이터 레이크' 구축을 제안한다. 현재는 사고 이력, 환전 성공률, 기술적 인증 상태 등이 분산적으로 존재하거나 전혀 공유되지 않기 때문에, 이용자는 업장을 선택할 때 충분한 정보를 얻기 어렵다. 이에 각 업장은 공시 항목을 기준으로 △누적 가입자 수 △고액 환전 이력 △시스템 감사 결과 등을 정기적으로 제출하고, 이를 종합한 신뢰 지표를 제공하는 구조가 필요하다.

셋째, '솔루션 보안 인증 제도'를 마련하여 최소한의 보안 기준을 통과한 솔루션만 업장에서 채택하도록 권고하거나 인센티브를 부여하는 제도가 도입되어야 한다. 한국인터넷진흥원(KISA)이나 정보보안 관련 공인기관과 협력하여, 업계별 기준을 수립하고 인증제를 도입하는 것이 바람직하다.

5.3 이용자 자율방어 전략

기술적·제도적 장치가 마련되더라도, 궁극적으로 고액 먹튀의 최종 피해자는 이용자 자신이므로 자율적 방어 전략 수립이 필수적이다. 본 연구에서는 다음과 같은 3단계 자율방어 프로토콜을 제안한다.

1단계: 사전 검증 체크리스트 활용. 이용자는 업장 선택 시 △솔루션의 다양성 △환전 이행률 △커뮤니티 평가 △공식 감사 이력 여부 등을 기준으로 15항목의 체크리스트를 기반으로 한 사전 점검을 수행해야 한다.

2단계: 트랜치(tranche) 방식 환전 요청. 고액 자금을 예치하거나 환전할 경우, 전체 금액을 일괄 요청하기보다 10% 단위로 분할 요청하여 업장의 유동성 부담을 분산시키고, 응답 시간을 통한 신뢰도를 측정해야 한다.

3단계: 커뮤니티 기반 사고 감시 네트워크 참여. 먹튀 사고는 단발적 피해에 그치지 않고 반복적 피해로 이어질 수 있으므로, 이용자는 커뮤니티나 검증 플랫폼을 통해 사고 발생 즉시 정보를 공유하고, 해당 업장을 블랙리스트에 등재함으로써 2차 피해를 예방해야 한다.

이러한 자율방어 프로토콜은 기술 및 제도 대응과 결합할 때 가장 큰 효과를 발휘하며, 업계 전반의 투명성 제고와 신뢰 회복에 결정적인 역할을 한다.

다음 장에서는 본 연구의 결론을 요약하고, 후속 과제를 제안하며 실천적 시사점을 정리한다.

제6장. 결론

6.1 요약 및 주요 발견

본 연구는 최근 급증하고 있는 고액 먹튀 사고의 구조적 원인을 분석하고, 이를 방지하기 위한 다층적 대응 전략을 제시하고자 하였다. 분석 결과, 고액 먹튀는 단순한 운영 실패나 일회성 사고가 아니라, 업계 전반의 시스템 리스크, 기술적 취약성, 유동성 관리 부재, 정보 비대칭 등 복합적 요인이 상호작용하는 결과물임이 드러났다.

특히 상위 3개 솔루션의 집중도가 80%를 넘는 시장 구조는 단일 취약점이 전체 업계로 확산되는 매우 위험한 구조임을 실증적으로 확인하였다. 또한 호텔 게임을 중심으로 한 고빈도·고액 자금 회전 구조는 환전 요청 시점에서 업장의 유동성 한계를 빠르게 드러내며, 결과적으로 먹튀를 유도하는 구조적 요인으로 작용한다. 이에 더해, 가입 혜택 중심의 출혈 경쟁은 재무 건전성을 악화시키고, 사고 발생 빈도를 높이는 데 기여하고 있었다.

정량적 분석에서는 솔루션 집중도, 호텔 게임 비중, 혜택 인플레이션 지수가 모두 고액 먹튀 발생 확률에 유의미한 영향을 미친다는 결과를 얻었으며, 시뮬레이션 결과 또한 이들 요인의 결합이 사고 확산을 가속화할 수 있음을 보여주었다. 방어 전략이 병행되었을 때 사고 발생률과 피해액이 절

반 이하로 감소한 것은, 다층 대응의 효과를 실증적으로 뒷받침하는 주요한 증거이다.

6.2 연구 한계 및 후속 과제

첫째, 본 연구는 민간 검증 플랫폼을 중심으로 구축된 사례 DB를 기반으로 분석을 진행하였다. 따라서 비공개 업장이나 사고를 은폐한 사례는 포함되지 않아 전체 시장에 대한 일반화에는 제한이 있을 수 있다. 둘째, 정성 분석은 주요 사례 중심의 인터뷰와 커뮤니티 기반 텍스트 마이닝에 국한되었으며, 보다 다양한 연령대와 성별, 승부 습관을 반영한 통합적 사용자 패널 조사가 필요하다. 셋째, 시뮬레이션 모델은 일정 수준의 가정을 바탕으로 구성되었기 때문에 실제 업장 운영 구조와 100% 동일하다고 보기 어렵다.

향후 연구에서는 다음과 같은 방향이 보완되어야 할 것이다. (1) 솔루션 보안 사고에 대한 로그 수준의 기술적 분석, (2) 업장별 회계 구조 및 유동성 관리 방식에 대한 금융공학적 모델링, (3) 피해자들의 장기적 행동 변화와 신뢰 회복 과정에 대한 심층 질적 연구 등이다. 또한, 해외 사례와의 비교를 통해 글로벌 수준에서의 사기 유형 분석 및 공동 대응 방안 모색도 가능할 것이다.

6.3 실천적 제언

본 연구의 결과를 바탕으로 다음과 같은 실천적 제언을 제시한다.

첫째, 업계는 기술 중심의 안정성 확보를 최우선 과제로 삼아야 한다. 다중 솔루션 도입, 블록체인 기반 무결성 검증 시스템, AI 기반 리스크 탐지 체계의 도입은 선택이 아닌 필수다. 둘째, 정책 결정자와 협회는 실명 기반의 데이터 레이크 구축, 담보 예치금 제도 마련, 보안 인증 제도 도입을 통해 업계 전반의 투명성과 책임성을 강화해야 한다. 셋째, 이용자는 단순한 혜택 중심의 업장 선택 기준에서 벗어나, 사전 검증과 분산 전략, 커뮤니티 연대 기반의 자율 방어를 생활화해야 한다.

고액 먹튀는 단일 주체의 노력만으로 해결될 수 없다. 기술, 제도, 행태의 삼위일체적 개입이 동시에 작동할 때 비로소 구조적 전환이 가능하다. 본 연구가 그러한 변화의 출발점이 되기를 기대한다.

참고문헌

1. Anderson, R., & Moore, T. (2022). The Economics of Information Security. *Journal of Cyber Risk*, 8(4), 321–346.
2. Basel Committee on Banking Supervision. (2023). *The 2023 Banking Turmoil and Liquidity Risk: A Progress Report*. Bank for International Settlements.
3. Gainsbury, S. (2012). *Internet Gambling: Current Research Findings and Implications*. Springer.
4. Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Global South*. Palgrave Macmillan.
5. Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. IBM Security.
6. Wood, R. T., & Williams, R. J. (2009). Internet Gambling: Prevalence, Patterns, Problems, and Policy Options. *Alberta Gaming Research Institute*.
7. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security & Privacy Workshops*, 180–184.
8. Kim, J. M., & Park, H. J. (2021). Zero-Trust Architecture for High-Risk Online Environments. *Korea Information Security Review*, 31(2), 57–74.
9. Lee, Y. S., & Cho, J. H. (2020). Liquidity Stress in High-Frequency Wagering Markets. *Journal of Risk Finance*, 21(4), 351–370.
10. Deloitte. (2023). *Managing Liquidity Risk in a Digital Age*. Deloitte Insights.

11. European Union Agency for Cybersecurity (ENISA). (2022). *Threat Landscape for Supply-Chain Attacks*.

12. Bank of Korea. (2024). *Household Liquidity Flow and Risk Concentration*. Financial Stability Report, June.

13. 먹튀위크. (2024). 메이저놀이터 리스크 지표 백서. 서울: 주식회사 먹튀위크.

부록 A. 고액 먹튀 대응 체크리스트 (요약)

1. 가입 업장의 솔루션 구조 확인 (단일 솔루션 의존 여부)
2. 최근 12개월 환전 이행률 검토 (공시자료 기준)
3. 고액 환전 시 트랜치 환전 방식 활용
4. 커뮤니티 기반 블랙리스트 점검 여부
5. 업장 리뷰/신고 사례 교차 확인
6. 자금 예치 전, 실거래 계좌 인증 절차 유무 확인

부록 B. 연구 설계 요약표

구분	내용
연구 방법	혼합연구 (정량 + 정성)
데이터 규모	사고 DB 6,412건 + 인터뷰 16건
분석 도구	SPSS, Stata, NVivo, Python (토픽 모델링)
주요 변수	솔루션 집중도, 호텔 게임 비중, 혜택 인플레이션
종속 변수	고액 먹튀 여부, 피해액 규모 (log)
시뮬레이션	100,000명 이용자 기반 ABM (24개월 시나리오)

※ 상세 내용은 온라인 부록 파일 참조.

※ 본 논문은 *(주)*먹튀위크의 *2024*년 먹튀검증 데이터베이스 및 검증 보고서를 바탕으로 작성되었으며, 연구 과정에서 식별된 개인 정보 및 사례는 비식별화 및 익명화 조치를 거쳤습니다.