

조직적 이상거래 탐지 함수

최신 버전

피처 설명

피처 뜻

S_{IP}

- IP 공유율 = 계정별 IP 수 / 총 IP 수

$S_{concurrent}$

- 동시 거래율 = 시간대별 중복 거래 비율

S_{price}

- 가격 유사도 = 계정 간 거래가격 CV

$S_{leverage}$

- 평균 레버리지 = 평균(leverage)

$S_{coordinated}$

- 조율된 거래 행동
- 동시에 거래하면서(시간 동기화), 유사한 가격을 선택(가격 동기화) → 동일 신호 사용 또는 조직적 조율 증거

IP 공유 점수

$$S_{IP} = \begin{cases} 0 & \text{if } r_{IP} = 0\% \\ 50 & \text{if } 0\% < r_{IP} \leq 5\% \\ 75 & \text{if } 5\% < r_{IP} \leq 15\% \\ 1000 & \text{if } r_{IP} > 15\% \end{cases}$$

지금 IP 공유율 기준을 뭘로 잡을지 애매해서... 그래프 보고 기준 잡은 뒤에 고치면 될 것 같아

동시 거래 점수

$$S_{concurrent} = \begin{cases} 0 & \text{if } r_{con} < 30\% \\ \frac{(r_{con}-30)}{20} \times 50 & \text{if } 30\% \leq r_{con} < 50\% \\ 50 + \frac{(r_{con}-50)}{50} \times 50 & \text{if } r_{con} \geq 50\% \end{cases}$$

- 근거
 - 30% 미만은 우연으로 간주 (정상 범위)
 - 50% 이상은 조직적 거래의 강력한 시간적 증거

가격 유사도 점수

$$S_{price} = \begin{cases} 0 & \text{if } r_{price} < 60\% \\ \frac{(r_{price}-60)}{20} \times 40 & \text{if } 60\% \leq r_{price} < 80\% \\ 40 + \frac{(r_{price}-80)}{20} \times 60 & \text{if } r_{price} \geq 80\% \end{cases}$$

- 근거
 - 60% 미만은 다양한 가격대 선택 (정상)
 - 80% 이상은 동일 신호/봇 사용 강력 시사

레버리지 점수

$$S_{leverage} = \begin{cases} 0 & \text{if } L < 30x \\ \frac{(L-30)}{20} \times 50 & \text{if } 30x \leq L < 50x \\ 50 + \min\left(\frac{L-50}{50}, 1\right) \times 50 & \text{if } L \geq 50x \end{cases}$$

- 논리

- 30x 미만은 일반적 레버리지 (정상)
- 50x 이상은 극단적 고위험 전략

조율된 거래 행동

$$S_{coordinated} = \sqrt{S_{concurrent} \times S_{price}}$$

최종 위험도 계산

Base Score (기본 위험도)

$$\text{Risk Score} = w_1 \cdot S_{IP} + w_2 \cdot S_{coordinated} + w_3 \cdot S_{leverage}$$

가중치 설정 (조직성 중심):

$$w_1 = 0.45 \quad (\text{IP 공유 - 계정 연결성})$$

$$w_2 = 0.45 \quad (\text{조율된 행동 - 거래 동기화})$$

$$w_3 = 0.10 \quad (\text{레버리지 - 리스크 성향})$$

Organizational Multiplier (조직성 증폭 계수)

조직적 거래의 핵심: 물리적 연결 + 행동 동기화가 동시에 발생

$$M_{org} = 1 + \alpha \cdot \frac{S_{IP} \times S_{coordinated}}{10000}$$

여기서 $\alpha = 0.5$ (최대 50% 증폭)

논리:

- IP 공유 없으면 ($S_{IP} = 0$) $\rightarrow M_{org} = 1$ (증폭 없음)
- IP 공유 있으면서 조율된 행동 높으면 \rightarrow 최대 1.5배 증폭
- 예: $S_{IP} = 80, S_{coordinated} = 80 \rightarrow M_{org} = 1 + 0.5 \times 0.64 = 1.32$

최종 점수

$$\text{Final Risk Score} = \min(100, \text{Risk Score} \times M_{org})$$

4. 위험도 판정

$$\text{Risk Level} = \begin{cases} \text{High Risk (고위험)} & \text{if Final Score} \geq 70 \\ \text{Medium Risk (의심)} & \text{if } 40 \leq \text{Final Score} < 70 \\ \text{Low Risk (정상)} & \text{if Final Score} < 40 \end{cases}$$

이전 버전

조직적 이상거래 탐지 수식 설계

1. 기본 구조: 가중합 모델 (Weighted Sum Model)

$$\text{RiskScore} = w_1 \cdot S_{IP} + w_2 \cdot S_{concurrent} + w_3 \cdot S_{price} + w_4 \cdot S_{leverage}$$

2. 피처별 세부 점수 계산 (0~100점 정규화)

Feature 1: IP 공유 점수 (S IP)