

[토스페이먼츠] DDoS 공격으로 인한 결제서비스 장애 보고서

수신	개별 안내	문서번호	2025-공문발급-8548
참조	개별 안내	주 소	서울시 강남구 테헤란로 131, 14층(역삼동, 한국지식재산센터)
발신	토스페이먼츠, 결제운영팀	사업자등록번호	411-86-01799
		전화번호 / 팩스	1544-7772 /

1. 귀사의 무궁한 발전을 기원합니다.
2. 2025년 10월 11일부터 15일까지 세 차례 발생한 토스페이먼츠 결제 서비스 장애 관련 내용을 아래와 같이 안내드립니다.

- 아 래 -

가. 장애 원인:

- 외부에서 유입된 대규모 DDoS(디도스) 공격으로 인해, 결제 처리 서비스에 지연 및 장애가 발생했습니다.
 - 특히, L7(HTTP) 계층을 포함한 고도화된 DDoS 공격으로, 정상 사용자 요청을 모방한 패턴이 반복됨에 따라 대응 및 차단이 복잡하였습니다.
- (※ 공격 및 방어 방식의 세부 내용은 향후 보안 위협으로 악용될 가능성이 있어 상세 공개가 어려운 점 양해 부탁드립니다.)

나. 장애 내용:

영향 범위에 속한 서비스에서는 장애 발생 시간대 동안 서비스 응답이 지연되어 일부 주문 건에서 결제창이 정상적으로 열리지 않거나, API 요청 시 Connect Timeout / Reset, Read Timeout 등의 실패 응답이 발생하였습니다. 특히 세 차례 모두 공격은 전체 결제 서비스를 대상으로 발생하였으나, 상대적으로 인프라 구조가 노후화된 LG U+ xPay 서비스에서 영향이 더 크게 나타났습니다.

구분	1차	2차	3차
영향 시간	‘25. 10. 11(토) 17:00~17:32 (32분)	‘25. 10. 13(월) 09:55~10:08 (13분)	‘25. 10. 15(수) 14:47~16:01 (74분)
공격 범위	xpay, tosspayments open api를 포함한 토스페이먼츠 전체 결제 서비스		
영향 범위	LG U+ xpay 서비스 toisspayments open api	LG U+ xpay 서비스	LG U+ xpay 서비스
공격 트래픽량	평상시 대비 최대 250배	평상시 대비 최대 250배	평상시 대비 최대 7800배

다. 조치 사항

* 1차 DDoS 공격 이후

- 식별된 공격 패턴 및 IP 차단
 - DDoS 자동 탐지 및 차단 정책 민감도 강화
- ⇒ DDoS 공격의 재발 가능성에 대비하여, 공격 직후 보안 정책을 한층 강화하여 운영하였습니다.

* 2차 DDoS 공격 이후

- 식별된 공격 패턴 및 IP 차단
 - 공격 패턴 분석을 통한 DDoS 대응 정책 추가 발굴 및 적용
 - 긴급 증설을 통한 서비스 가용량 확보
 - DDoS 공격 규모가 늘어날 것을 대비한 아키텍처 설계 검토
- ⇒ L7 DDoS 공격의 변형 가능성과 규모 확산에 대비하여 사전 대응 방안을 마련하였습니다.

* 3차 DDoS 공격 시

- Application 서버 가용량 증설
 - 트래픽 경로 우회 처리
 - 추가 식별된 공격 패턴 및 IP 차단
- ⇒ 3차 공격은 DDoS의 대상과 패턴이 변형된 형태로 발생하였으며, 평시 대비 최대 7,800배의 요청이 집중되었습니다. 변화된 공격 특성으로 초기 대응에 다소 시간이 소요되었으나, 클라우드 자원을 확장해 트래픽을 분산시키고 서비스를 안정화하였습니다.

라. 향후 대응 계획

현재 고도화된 형태의 DDoS 공격을 포함해, 당사 결제 서비스의 안정성 확보를 위해 아래 계획에 따라 단계적으로 개선 작업을 추진할 예정입니다.

- 즉시 (~10.17)
 - 인프라 예비 장비 투입하여 가용량 확보
- 단기 (10월 중)
 - 인프라 예비 장비 추가 투입
 - 클라우드 DR(Disaster Recovery) 환경을 활용한 DDoS 트래픽 수용 가능한 구조로 변경
- 중기 ('25년 내)
 - LG U+ xpay 서비스 안정성 확보를 위한 추가 가용 Zone 신설
- 장기 ('26년 1분기)
 - Active-Standby DR 구조 → Active-Active DR 구조로 전환 완료 목표 시점 단축
 - 차세대 WAF 보안 장비 선제 투입

토스페이먼츠는 이외에도 신속한 장애 전파와 서비스 현황 안내를 위해 서비스 상태 페이지(<https://status.tosspayments.com/>)를 운영하고 있습니다. 해당 페이지를 통해 결제 서비스의 운영 상태 및 복구 진행 현황을 실시간으로 확인하실 수 있습니다.

3. 당사를 믿고 협업 해주신 귀사의 업무에 불편을 끼쳐 드린 점 다시 한번 너른 양해 부탁드리며, 추후 재발 하여 불편함을 드리는 일이 없도록 개선에 만전을 기하겠습니다. 이번 장애로 귀사 서비스 운영에 불편을 드린 점 다시 한번 깊이 사과드립니다.

감사합니다.

끝.

2025-10-16

토스페이먼츠 주식회사

대표이사 임한욱



© Toss payments Co., Ltd.