

(주)아이티아이즈 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	클라우드서비스 센터장	경대진		
	검토	클라우드서비스 지원팀장	박수용		
	작성	담당자	김선환		

모의훈련 세부 수행계획서

2022.04.29

재·개정 이력사항

[illegible]

본 문서는 (주)아이티아이스 클라우드 서비스 제공을 위해서 컨설팅,
마이그레이션, 매니지드, XaaS 서비스 등을 대상으로 작성함.

I. 모의 훈련 개요

1. 모의훈련 대상

○ 훈련 대상 : IaaS 인증사업자 3개 총 3개 사업자

- IaaS 인증사업자 자원 고갈 공격, SaaS 인증사업자 APT 이메일 훈련

구분	훈련대상	훈련 사항
IaaS	KT, NHN, 네이버 클라우드	ICMP / GET / DNS / UDP Flooding
		통신량 한계 초과 / 접속처리 한계 초과 공격
		Slowloris / Cache-Control / HTTP Post Attck 홈페이지부하 가중 및 복합 공격 DNS Query Flooding (신청사업자)
IaaS(도상 훈련)	KT, NHN, 네이버 클라우드	훈련상황 : DDoS 공격으로 클라우드 IaaS 인증 서비스 10분 간 단절로 인한 사업자 침해사고 대응능력 확인

2. 모의훈련 일정(안)

- 훈련 대상 사업자별 1일씩 진행 총 6일 소요 예정(인증사업자와 협의)

※예상 일정 : 9월 30일(월) ~ 10월 2일(수) / 10월 7일(월) ~ 8일(화), 10일(목)

3. 모의훈련 전체 예상 소요 시간

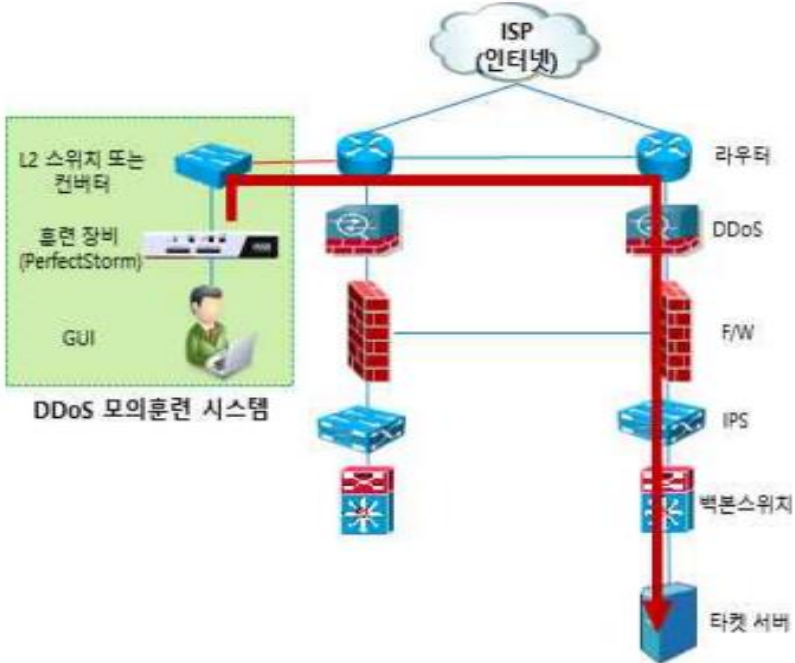
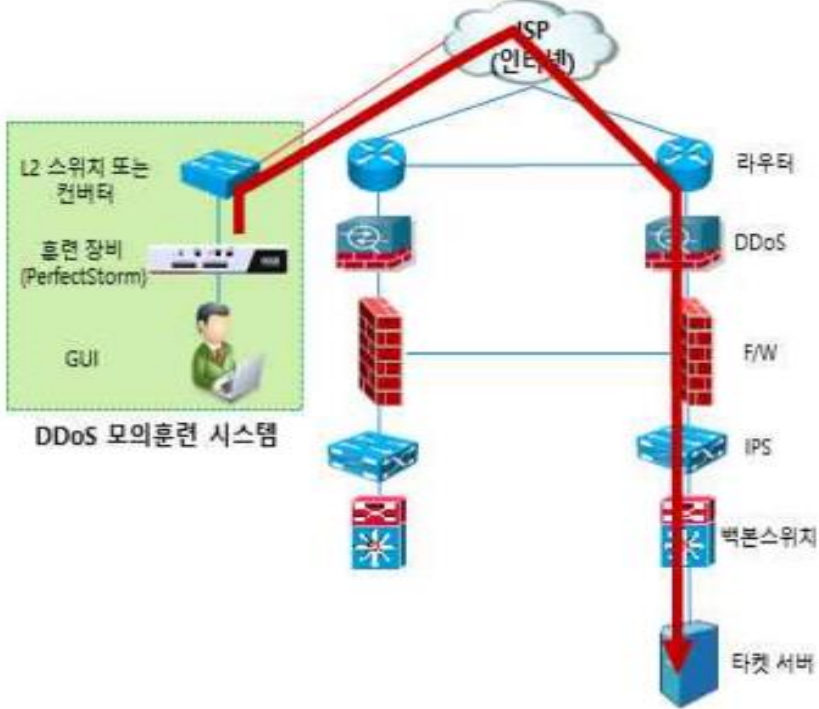
구분	내용	소요시간	훈련시작	종료시간	비고
DDoS 모의훈련 (IaaS)	공격 유형에 따른 모의훈련 진행	약 4시간	10:00	14:40	점심시간 1시간 제외
도상 훈련(IaaS)	침해대응 절차에 따른 도상훈련 진행	2시간	15:00	17:00	훈련 결과보고서
훈련 평가	침해대응 절차서 및 훈련 결과 보고서를 참고하여 훈련 평가	1시간	17:00	18:00	훈련 평가지표

II. 훈련 세부 내용

1. DDoS 모의훈련 구성 방안

○ 내부 수행 : 상단 Router에서 내부 보안 장비를 거쳐 타겟 서버(홈페이지 또는 테스트 서버) 공격

○ 외부 수행 : 외부(수행사내)에서 인터넷을 통해 인증 사업자 내부 보안 장비를 거쳐 타겟 서버(홈페이지 또는 테스트 서버) 공격

구분	구성도
<p>내부수행 : KT</p>	
<p>외부수행 : KT, NHN, 네이버 클라우드</p>	

2. DDoS 모의훈련 예상 시간

구분		내용	훈련시간	종료시간	비고
사전 준비		모의훈련 테스트 환경 구축	10:00	10:30	
유형	구분	내용	훈련시간	종료시간	비고
통신량 한계 초과공격 (10 회)	1.	TCP Syn Flag Flooding	10:30	10:35	1 차
			10:35	10:40	2 차
	2.	TCP FIN Flag Flooding	10:40	10:45	1 차
			10:45	10:50	2 차
	3.	IP Fragmentation Flooding	10:50	10:55	1 차
			10:55	11:00	2 차
	4.	UDP Flooding	11:00	11:05	1 차
			11:05	11:10	2 차
	5.	ICMP Floodin	11:10	11:15	1 차
			11:15	11:20	2 차
접속처리 한계공격(2 회)	6.	GET Flooding	11:20	11:25	1 차
			11:25	11:30	2 차
홈페이지 부하 가중공격 (10 회)	7.	Slowloris Attack	11:30	11:35	1 차
			11:35	11:40	2 차
	8.	Slowread Attac	11:40	11:45	1 차
			11:45	11:50	2 차
	점심 식사 (12:00 ~ 13:10)				
	9.	CC Attack	13:20	13:25	1 차
			13:25	13:30	2 차
	10.	RUDY Attack	13:30	13:35	1 차
			13:35	13:40	2 차
	11.	Post Attack	13:40	13:45	1 차
			13:45	13:50	2 차
복합 공격 (2 회)	12.	복합 공격 (1 + 7)	13:50	13:55	1 차
			13:55	14:00	2 차
DNS 부하 가중 공격(2 회)	13.	DNS Query Floodin	14:00	14:05	신청 사업자
			14:05	14:10	
훈련 결과 정리		• 점검현황 종합 및 결과정리 • 탐지/대응 시스템 로그 취합	14:10	14:40	

Ⅲ. 도상 훈련 세부 내용

1. IaaS 사업자 도상 훈련 수행 계획 1.1 훈련 진행 목적

○ DDoS 공격 모의침투를 통하여 클라우드 IaaS 인증 사업자가 사이버 위협에 대응할 수 있는 체계를 확인할 수 있는 목적으로 훈련 시행

1.2 IaaS 사업자 도상 훈련 절차



1.3 IaaS 사업자 도상 훈련 진행 순서

- 도상 훈련관련자 단톡방 소집 : KISA, 수행사, 인증사업자 훈련 참여자
- ※ 인증사업자 훈련 참여자 명단은 훈련일정 수립 시 제출요청 (참여자 성명/직책/이메일 주소)
- DDoS 트래픽 전송 : TCP Syn Flag Flooding 공격 (1 분)
- 훈련상황 전파 : 단톡방내 DDoS 공격으로 인해 클라우드 IaaS 인증 서비스 10분간 단절 발생 상황 전파
- ※ 관련근거 : 클라우드컴퓨팅 발전법 제 16 조(통지가 필요한 클라우드컴퓨팅서비스의 중단 기간)(1) 클라우드컴퓨팅서비스의 중단 기간이 연속해서 10 분 이상인 경우
- 훈련 절차서 확인 : KISA, 수행사
- 인증사업자 침해대응 절차에 따른 프로세스 진행
- 신고 메일 확인 : KISA 김대원 주임(big1@kisa.or.kr)
- 인증사업자 모의훈련 결과보고서 작성

8) 인증사업자 모의훈련 결과보고서 전달 확인

9) 인증사업자 훈련 절차 평가 : KISA, 수행사

※ 훈련 평가는 인증사업자 훈련 결과보고서 내용 참고하여 평가지표 체크리스트 활용