

클라우드 보안 인증사업자 DDoS/APT 모의훈련 세부 수행계획서

2019. 09.

목 차

I. 모의훈련 개요

1. 모의훈련 대상	1
2. 모의훈련 일정(안)	1
3. 모의훈련 전체 예상 소요 시간	1

II. 훈련 세부 내용

1. DDoS 모의훈련 구성방안	2
2. DDoS 모의훈련 예상 시간	3
3. DDoS 모의훈련 세부 진행 내용	4

III. APT 모의훈련 세부 내용

1. APT악성 이메일 모의훈련 개요	8
2. APT악성 이메일 모의훈련 방법 및 절차	8

IV. 도상 훈련 세부 내용

1. IaaS 사업자 도상 훈련 수행 계획	11
2. SaaS 사업자 도상 훈련 수행 계획	13

I 모의훈련 개요

1. 모의훈련 대상

- 훈련 대상 : IaaS 인증사업자 5개, SaaS 인증사업자 1개 **총 6개** 사업자
 - IaaS 인증사업자 **자원 고갈 공격**, SaaS 인증사업자 **APT 이메일 훈련**

구분	훈련 대상	훈련 사항
IaaS	KT, LG CNS, NHN, 가비아, 코스콤	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)
SaaS	인프라닉스	APT 모의훈련(악성 이메일)
IaaS/SaaS	KT, LG CNS, NHN, 가비아, 코스콤, 인프라닉스	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)

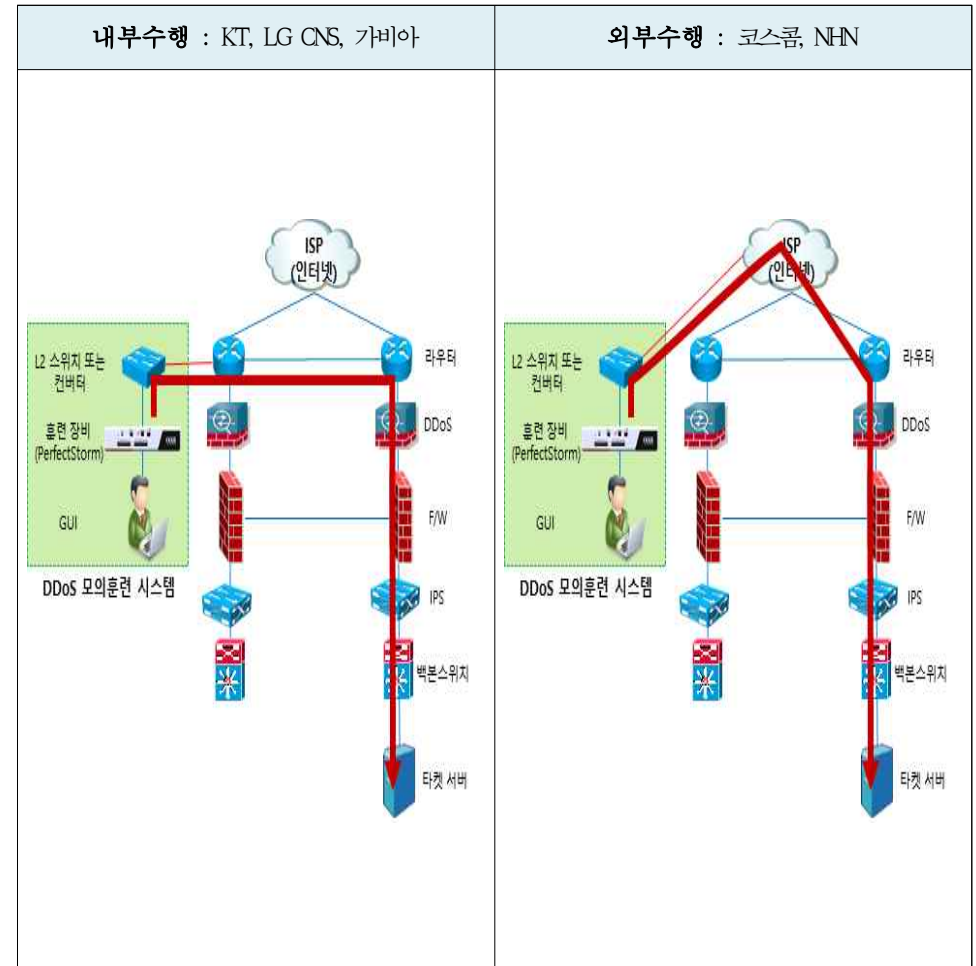
3. 모의훈련 전체 예상 소요 시간

구분	내용	소요 시간	훈련 시작	종료 시간	비고
DDoS 모의훈련 (IaaS)	공격 유형에 따른 모의훈련 진행	약 4시간	10:00	14:40	점심시간 (1시간) 제외
APT 모의훈련 (SaaS)	APT 악성 이메일 모의훈련 진행	1주			원격으로 별도 진행
도상 훈련 (IaaS/SaaS)	침해대응 절차에 따른 도상훈련 진행	2시간	15:00	17:00	훈련 결과보고서 작성 포함
훈련 평가 (IaaS/SaaS)	침해대응 절차서 및 훈련 결과 보고서를 참고하여 훈련 평가	1시간	17:00	18:00	훈련 평가지표 활용

II 훈련 세부 내용

1. DDoS 모의훈련 구성 방안

- 내부 수행 : 상단 Router에서 내부 보안 장비를 거쳐 타켓 서버(홈페이지 또는 테스트 서버) 공격
- 외부 수행 : 외부(수행사내)에서 인터넷을 통해 인증 사업자 내부 보안 장비를 거쳐 타켓 서버(홈페이지 또는 테스트 서버) 공격



2. DDoS 모의훈련 예상 시간

구분		내용	훈련 시작	종료 시간	비고
훈련 사전 준비		• 모의훈련 테스트 환경 구축	10:00	10:30	
유형	구분	내용	훈련 시작	종료 시간	비고
통신량 한계 초과공격 (10회)	1	TCP Syn Flag Flooding	10:30	10:35	1차
			10:35	10:40	2차
	2	TCP FIN Flag Flooding	10:40	10:45	1차
			10:45	10:50	2차
	3	IP Fragmentation Flooding	10:50	10:55	1차
			10:55	11:00	2차
	4	UDP Flooding	11:00	11:05	1차
			11:05	11:10	2차
	5	ICMP Flooding	11:10	11:15	1차
			11:15	11:20	2차
접속처리 한계공격 (2회)	6	GET Flooding	11:20	11:25	1차
			11:25	11:30	2차
홈페이지 부하 가중공격 (10회)	7	Slowloris Attack	11:30	11:35	1차
			11:35	11:40	2차
	8	Slowread Attack	11:40	11:45	1차
			11:45	11:50	2차
	점심 식사 (12 : 00 ~ 13 : 10)				
	9	CC Attack	13:20	13:25	1차
			13:25	13:30	2차
	10	RUDY Attack	13:30	13:35	1차
			13:35	13:40	2차
	11	Post Attack	13:40	13:45	1차
			13:45	13:50	2차
복합 공격 (2회)	12	복합 공격 (1 + 7)	13:50	13:55	1차
			13:55	14:00	2차
DNS 부하 가중 공격 (2회)	13	DNS Query Flooding	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	

3. DDoS 모의훈련 세부 진행 내용 (3시간 40분 소요)

구분	점검 시나리오		시간
사전 준비	• 모의훈련 테스트 환경 구축		30분
	공격/네트워크팀	트래픽 발생기 설치 및 테스트	10분
	운영/대응팀	보안 장비 사전 점검 및 정책 설정 확인	10분
	훈련 사전 미팅	공격 유형 최종 확인, 협조 요청 내용 공유	10분
	• 통신량 한계 초과 공격 (TCP Syn Flag Flooding) : 5분씩 2회 수행		10분
본 훈련	공격팀	과부하를 일으켜 서비스지연 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 통신량 한계 초과 공격 (TCP FIN Flag Flooding) : 5분씩 2회 수행		10분
	공격팀	과부하를 일으켜 서비스지연 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 통신량 한계 초과 공격 (IP Fragmentation Flooding) : 5분씩 2회 수행		10분
	공격팀	과부하를 일으켜 서비스지연 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분

구분	점검 시나리오		시간
본 훈련	• 통신량 한계 초과 공격 (UDP Flooding) : 5분씩 2회 수행		10분
	공격팀	과부하를 일으켜 서비스지연 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 통신량 한계 초과 공격 (ICMP Flooding) : 5분씩 2회 수행		10분
	공격팀	과부하를 일으켜 서비스지연 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 접속처리 한계 공격 (GET Flooding) : 5분씩 2회 수행		10분
	공격팀	접속처리 한계 공격	1분
	운영/분석팀	공격에 대한 F/W, Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 홈페이지 부하 가중 공격 (Slowloris Attack) : 5분씩 2회 수행		10분
	공격팀	홈페이지 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 홈페이지 부하 가중 공격 (Slowloread Attack) : 5분씩 2회 수행		10분
	공격팀	홈페이지 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분

구분	점검 시나리오		시간
본 훈련	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 홈페이지 부하 가중 공격 (Cache Control Attack) : 5분씩 2회 수행		10분
	공격팀	홈페이지 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 홈페이지 부하 가중 공격 (Rudy Attack) : 5분씩 2회 수행		10분
	공격팀	홈페이지 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 홈페이지 부하 가중 공격 (POST Attack) : 5분씩 2회 수행		10분
	공격팀	홈페이지 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• 복합 공격 (TCP Syn Flag Flooding + Slowloris Attack) : 5분씩 2회 수행		10분
	공격팀	대역폭 및 홈페이지 부하공격을 통한 복합 공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 다음 공격 준비		3분
	• DNS 부하 가중 공격 (DNS Query Flooding) : 5분씩 2회 수행 - NHN 사업자만 해당		10분

구분	점검 시나리오		시간
본 훈 련	공격팀	DNS 부하공격	1분
	운영/분석팀	공격에 대한 Anti-DDoS, IPS, IDS 등 탐지 및 대응	1분
	• 정상 서비스 확인 및 2차 공격 준비		3분
• 결과 정리			30분
	평가팀	점검현황 종합 및 결과 리뷰/정리	10분
	분석팀	탐지/대응 시스템 로그 취합	20분

III APT 모의훈련 세부 내용

1. APT 악성 이메일 훈련 개요

1.1 훈련 목적 : 악성 이메일 위협에 대응하기 위한 인증사업자 보안 인식 향상

1.2 훈련 대상 : 인프라닉스

※ 인증사업자 훈련 참여자 명단은 훈련일정 수립 시 제출요청 (참여자 성명/직책/이메일 주소)

1.3 훈련 기간 : 1주 (훈련 일정 인프라닉스와 협의)

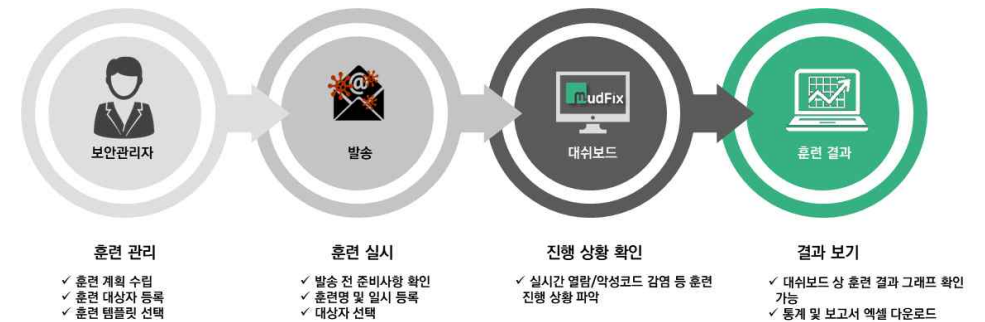
※ 도상훈련과는 별개로 원격으로 진행

2. APT 악성 이메일 훈련 방법 및 절차

2.1 훈련 방법 : APT 악성 이메일 훈련 시스템 이용

2.2 훈련 절차

- 1) 훈련 대상자 등록
- 2) 훈련 실시 (1주)
- 3) 훈련 진행 사항 확인
- 4) 훈련 종료
- 5) 결과 보고서 작성



2.3 훈련 이메일(샘플)

외부페이지 연동하는 기능의 개인정보 유출형 서식

※ 훈련용 이메일에 첨부된 링크 주소로 열리는 별도의 웹 페이지를 통해 훈련 대상자의 개인정보를 입력하게끔 유도하는 형태의 훈련 방식

감염PC 화면

악성 파일 경고문

- 본 프로그램은 악성 메일에 노출되어있는 사용자의 보안연식을 제고시키는 훈련입니다.
- 사용자의 컴퓨터에 심각한 손상이나 피해를 초래하지는 않습니다.

악성파일 감염 해제방법

- 비밀번호 입력창이 있는 경우 관리자계 비밀번호를 문의하여 입력하십시오.
- 백신파일 다운로드가 있는 경우 백신파일을 다운로드 한 후 실행시키십시오.

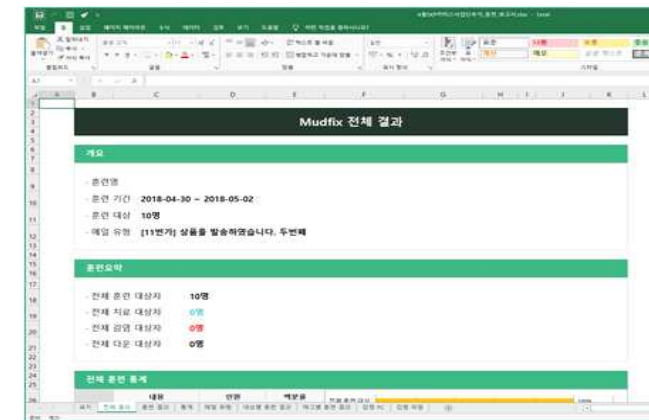
※ 훈련 메일에 첨부된 첨부파일 실행시 PC화면 잠금 기능 제공

2.4 훈련 진행 사항 관리



<input type="checkbox"/>	부문훈련	2018-04-30 ~ 2018-05-02	370	370	121	10	100%	828,948
<input type="checkbox"/>	그룹훈련	2018-04-30 ~ 2018-05-02	42	42	14	2	25%	206,158
<input type="checkbox"/>	그룹훈련	2018-04-30 ~ 2018-05-02	26	26	9	2	25%	181,484
<input type="checkbox"/>	1추가	2018-04-30 ~ 2018-05-02	10	10	2	0	20%	0,000
<input type="checkbox"/>	추진단	2018-04-30 ~ 2018-05-02	387	387	130	1	100%	62,794
<input type="checkbox"/>	사업단	2018-04-30 ~ 2018-05-02	542	542	87	10	100%	787,908

2.5 훈련 결과 관리(보고서 작성)



※ 훈련 대상자, 훈련기간, 감염 대상자, 파일 다운 대상자 등 결과관리

IV 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

- 1) 도상 훈련관련자 단독방 소집 : KISA, 수행사(쿠폰), 인증사업자 훈련 참여자
※ 인증사업자 훈련 참여자 명단은 훈련일정 수립 시 제출요청 (참여자 성명/직책/이메일 주소)
- 2) DDoS 트래픽 전송 : TCP Syn Flag Flooding 공격 (1분)
- 3) 훈련상황 전파 : 단독방내 DDoS 공격으로 인해 클라우드 IaaS 인증 서비스 10분간 단절 발생 상황 전파
※ 관련근거 : 클라우드컴퓨팅 발전법 제16조(통지가 필요한 클라우드컴퓨팅서비스의 중단 기간)
(1) 클라우드컴퓨팅서비스의 중단 기간이 연속해서 10분 이상인 경우
- 4) 훈련 절차서 확인 : KISA, 수행사(쿠폰)
- 5) 인증사업자 침해대응 절차에 따른 프로세스 진행

6) 신고 메일 확인 : KISA 김대원 주임(big1@kisa.or.kr)

7) 인증사업자 모의훈련 결과보고서 작성

8) 인증사업자 모의훈련 결과보고서 전달 확인

9) 인증사업자 훈련 절차 평가 : KISA, 수행사(쿠폰)

※ 훈련 평가는 인증사업자 훈련 결과보고서 내용 참고하여 평가지표 체크리스트 활용

2. SaaS 사업자 도상 훈련 수행 계획

2.1 훈련 진행 목적

- 모의훈련을 통하여 클라우드 SaaS 인증 사업자가 IaaS 사업자와 협업하여 사이버 위협에 대응할 수 있는 체계를 확인할 수 있는 목적으로 훈련 시행

2.2 SaaS 사업자 도상 훈련 절차



2.3 SaaS 사업자 도상 훈련 진행 순서

- 1) 도상 훈련관련자 단독방 소집 : KISA, 수행사(쿠폰), 인증사업자 훈련 참여자
 ※ 인증사업자 훈련 참여자 명단은 훈련일정 수립 시 제출요청 (참여자 성명/직책/이메일 주소)
- 2) DDoS 트래픽 전송 : TCP Syn Flag Flooding 공격 (1분)
- 3) 훈련상황 전파 : 단독방내 DDoS 공격으로 인해 클라우드 SaaS 인증 서비스
 10분간 단절 발생 상황 전파
 ※ 관련근거 : 클라우드컴퓨팅 발전법 제16조(통지가 필요한 클라우드컴퓨팅서비스의 중단 기간)
 (1) 클라우드컴퓨팅서비스의 중단 기간이 연속해서 10분 이상인 경우
- 4) 훈련 절차서 확인 : KISA, 수행사(쿠폰)

- 5) 인증사업자 침해대응 절차에 따른 프로세스 진행
- 6) 신고 메일 확인 : KISA 김대원 주임(big1@kisa.or.kr)
- 7) 인증사업자 모의훈련 결과보고서 작성
- 8) 인증사업자 모의훈련 결과보고서 전달 확인
- 9) 인증사업자 훈련 절차 평가 : KISA, 수행사(쿠폰)

※ 훈련 평가는 인증사업자 훈련 결과보고서 내용 참고하여 평가지표 체크리스트 활용