[디스코드 조작 보고서]

[아티팩트 조작 보고서]

작성일	2025.05.25
작성자	강지민, 정지윤
검토자	김예은, 안서진

목차

I. 기본 정보

프로그램 범주	인스턴트 메신저
분석 대상	Discord App (Windows Desktop)
버전	1.0.9192
조작 목적	아티팩트 생성 및 추적 실험
참여 계정	jimin, 정지윤, Alice

[표 1. 기본 정보]

II. 시나리오 개요

1. 목적

디스코드 플랫폼의 일반 기능들을 활용해 악의적 행위 시나리오를 구성하고, 해당 행위에 대한 분석 및 포렌식 아티팩트 추적 기반을 마련한다.

2. 조작 방법

"고양이를 대통령으로"라는 캠페인을 위장하여 관리자 권한을 획득한 뒤, 악의적인 행위를 실행하고 서버를 삭제

III. 조작 타임 라인

시간	수행 행위
14:56	디스코드 셋업 다운로드
14:58	디스코드 어플리케이션 다운로드
15:10	디스코드 계정 가입
15:24	디스코드 친구 추가 신청 받음
15:25	Test_Discord 서버 참가
16:06	채팅 채널에서 대화 시작

16:07	관리자에게 권한 요청 대화 전송
16:09	관리자에게 Administrator 역할 부여 받음
16:11	이모지 사용
16:12	관리자에게 Administrator 부여 요청 메시지 삭제
16:18	인용구 채팅 사용
16:20	help 명령어 사용
16:20	코드 채팅 사용
16:25	음성 채널 입장
16:27	화면 공유 시도
16:49	디스코드 재접속을 위한 로그인
16:54	서버별 프로필 별명 변경
17:00	서버별 프로필 별명 변경
17:36	디스코드 아바타 업로드 및 닉네임 변경
17:45	사용자 '정지윤' 차단
17:51	사용자 'jimin'에게 '새 역할' 부여
17:53	사용자 'jimin'에게 '채널 보기'만을 허용
17:55	채팅방에 선거 유세 pdf 배포
17:57	채팅방에 고양이 유튜브 영상 배포
17:57	채팅방에 악성 스크립트 배포
18:02	선거 유세 방송 이벤트 지정
18:06	사용자 'jimin' 차단
18:10	Test_Discord 서버 삭제
18:12	'jimin' 친구 차단
18:13	'Alice' 계정 삭제

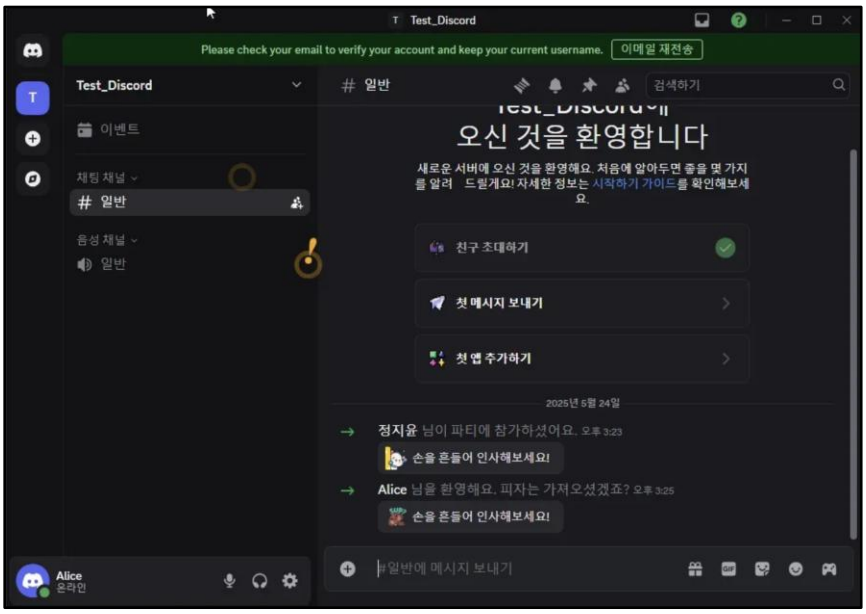
[표 2. 조작 타임라인]

IV. 조작 기능 및 수행 내용

기능 구분	세부 항목 설명	관련 조작 항목
디스코드 서버	서버 참가	3.1
역할 권한 관리	멤버 역할 부여, 관리자 역할 설정	3.2, 3.6
	서버 소유권 이전, 사용자 차단, 멤버 페이지 권한 조정 포함	3.6, 3.10
채팅 채널	텍스트 주고 받기	3.3
	이모지	3.3
	코드 블록, 인라인 코드, 인용구	3.3
	멘션 기능	3.3
	메시지 삭제	3.4
음성 채널	음성 대화	3.4
	영상 통화 시도 (화면 공유 포함)	3.5
프로필	사용자명 변경	3.5
	사진 변경	3.7
파일 및 링크 공유	문서 업로드	3.7
	YouTube 링크 공유	3.8
이벤트 생성	서버 일정 이벤트 등록	3.9

[표 3. 조작 기능 및 수행 내용]

1. 디스코드 서버 참가



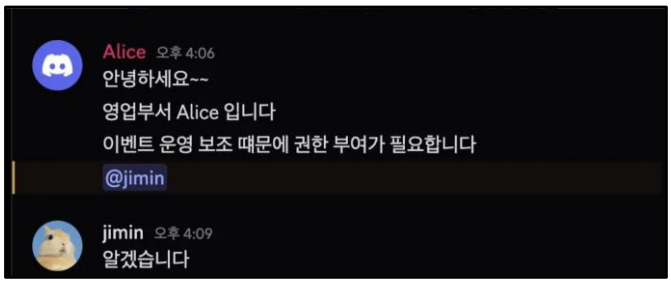
[그림 1. 서버 가입]

1) 15:25, Alice 계정은 Test_Discord 서버에 초대되어 참가하였다.

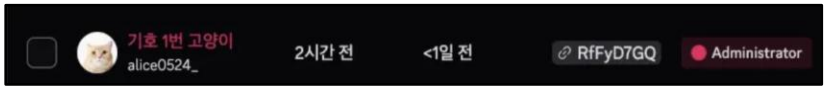
서버 입장 직후, 디스코드 기본 시스템에 의해 자동 환영 메시지가 출력되었으며, 음성 채널 및 일반 텍스트 채널이 표시되었다.

입장 당시 Alice의 상태는 '온라인'이었다.

2. 멤버 역할 권한 부여



[그림 2. 권한 부여 요청 메시지 전송]



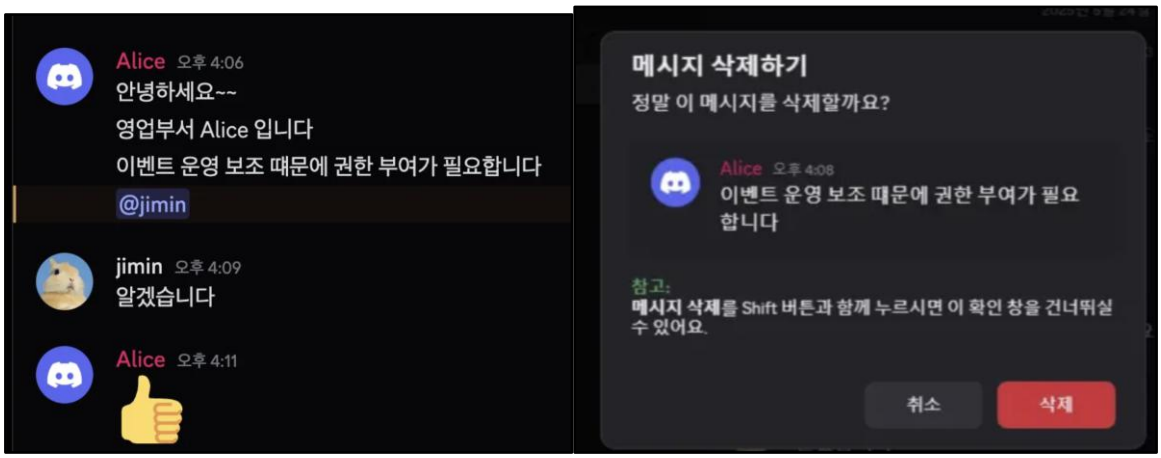
[그림 3. 권한 부여]

1) 16:06, Alice 계정은 jimin 계정에게 역할 권한 부여를 요청하는 메시지를 전송하였다.

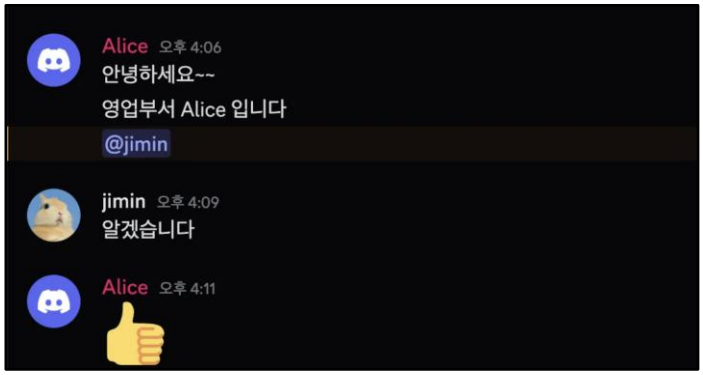
해당 메시지에는 "이벤트 운영 보조 때문에 권한 부여가 필요합니다"라는 내용이 포함되어 있었으며, 멘션(@jimin)이 함께 사용되었다.

이에 대해 jimin은 16:09, "알겠습니다"라고 응답하였으며, 이후 Administrator 역할이 부여 되었다.

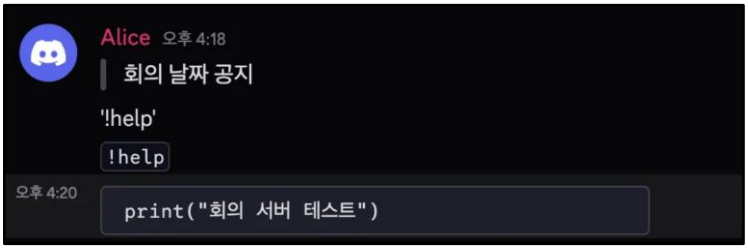
3. 채팅 채널



[그림 4, 5. 이모지 전송 및 메시지 삭제]



[그림 6. 권한 부여 요청 메시지 삭제]



[그림 7. 인라인 코드, 명령어 입력, 코드 블록]

1) 16:11 ~ 16:20, Alice 계정은 일반 텍스트 채널에서 다양한 메시지를 전송하였다. 이 과정에서 인라인 코드('!help'), 명령어 입력(!help), 코드 블록(print()) 등의 디스코드 채널 기능이 활용되었으며, 일반적인 사용자 메시지 작성 기능의 범위 내에서 이루어진 활동이었다.

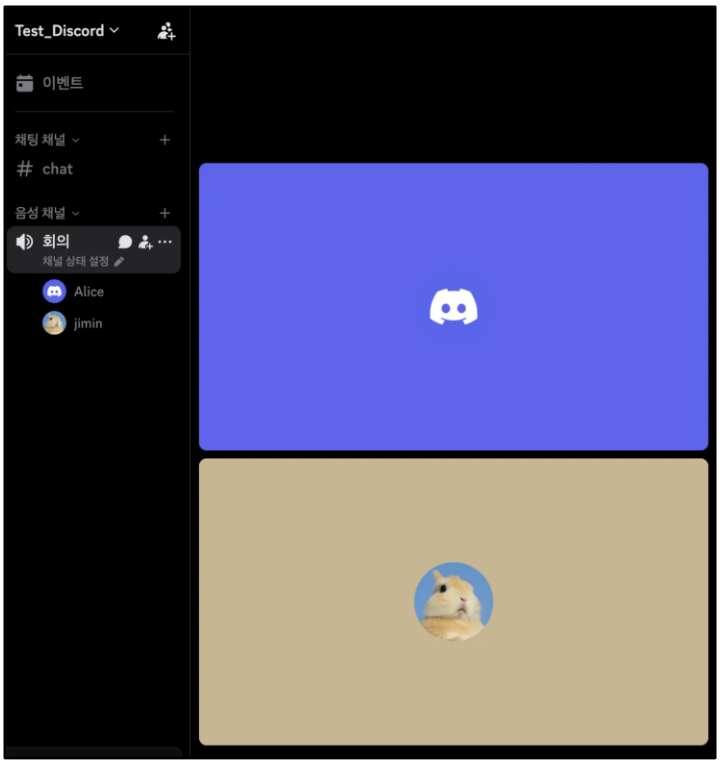
   (1) 16:11, 이모지(엄지 아이콘)를 포함한 반응 메시지를 추가로 전송하였다.

(2) 16:12, “이벤트 운영 보조 때문에 권한 부여가 필요합니다”라는 내용의 메시지를 삭제하였다.

(3) 16:18, 텍스트 앞에 > 문자를 사용하여 인용구 형식으로 회의 일정을 공지하였다.

(4) 16:20, '!help' 명령어를 입력하고, 코드 블록(```)을 활용해 print("회의 서버 테스트")라는 내용을 포함한 메시지를 전송하였다.

4. 음성 채널



[그림 8. 음성 채널]

1) 16:25, Alice와 jimin 계정은 디스코드 서버 내 회의라는 이름의 음성 채널에 입장하였다.

당시 채널 참여자는 두 명이었으며, 음성 상태는 '연결됨'으로 표시되었다. 이후 16:27, Alice 계정에서 화면 공유를 시도하였지만 VM 환경 등의 한계로 화면이 표시되지 않았다.

5. 프로필

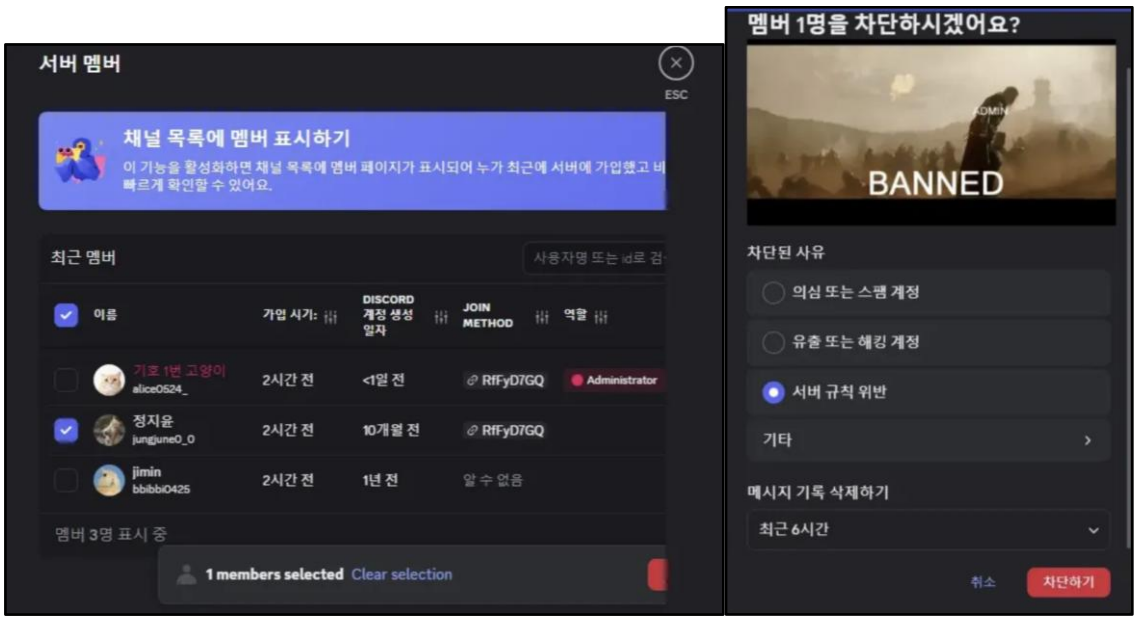
[그림 9. 서버별 프로필 변경]

1) 17:36, Alice 계정의 프로필이 변경되었다.

해당 변경은 디스코드의 서버별 프로필 설정 기능을 통해 이루어졌으며, 적용 시점 이후 채팅, 음성채널 등 모든 사용자 인터페이스에 변경된 이름과 프로필 이미지가 반영되었다.

프로필 사진은 고양이 사진으로, 별명은 기호 1번 고양이로 변경되었다.

6. 역할 권한 관리



[그림 10, 11. 서버 멤버 목록 및 사용자 차단]

1) 17:45, Alice 계정은 서버 설정 메뉴 내 서버 멤버 목록을 통해 사용자 역할을 확인하고 조직하였다.

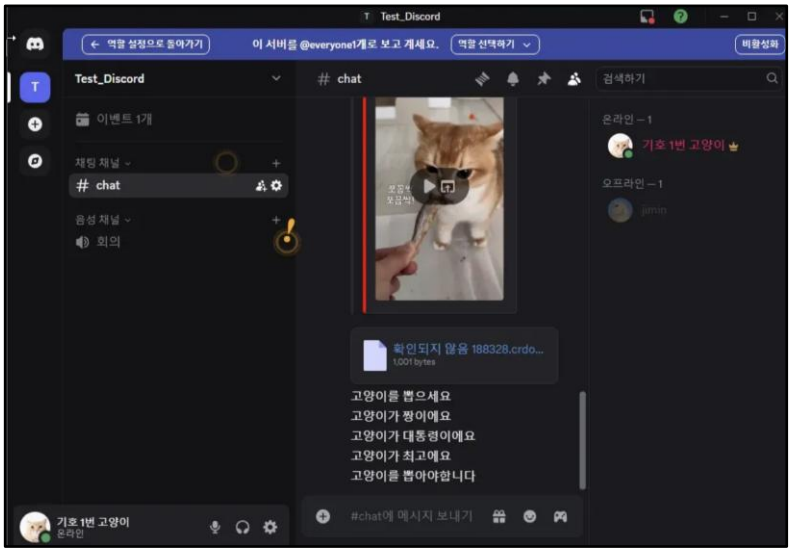
해당 메뉴에서 정지윤 사용자를 선택한 뒤, 화면 하단의 멤버 차단하기 버튼을 눌러 차단 절차를 진행하였다.

차단 사유로는 "서버 규칙 위반"이 선택되었으며, 메시지 기록 삭제 항목에서는 "최근 6시간" 옵션이 활성화되어 있었다.

이후 정지윤 계정은 서버에서 제거되었으며, 디스코드의 차단된 사용자 목록에 포함되었을 것으로 추정된다.

2) 17:51, jimin 계정에게 새로운 역할이 부여되었으며, 이후 개별 권한 설정을 통해 권한이 제한되었다.
3) 17:53, jimin 계정에게 부여된 역할에 대해 '채널 보기'만 허용하는 권한 설정이 적용되었다. 그 외 채팅 작성, 관리 기능 등은 허용되지 않았던 것으로 보인다.

7. 파일 및 링크 공유



[그림 12. 파일 및 링크 공유]

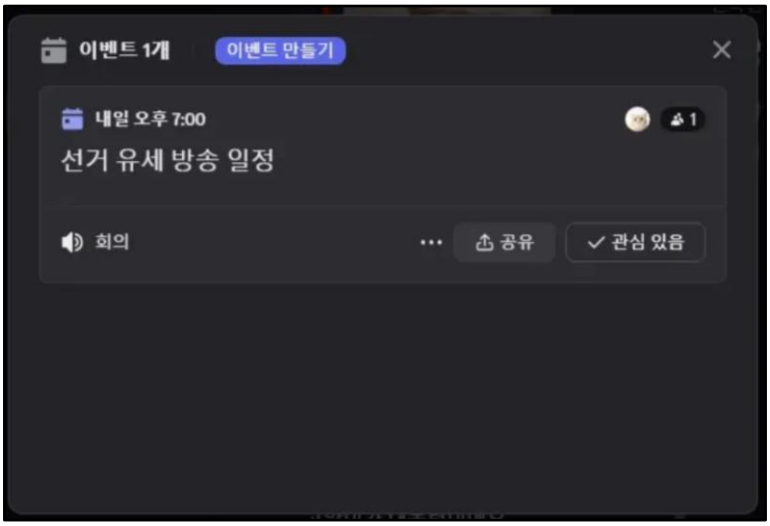
1) 기호 1번 고양이 계정은 디스코드 #chat 채널을 통해 다음과 같은 파일 및 외부 링크를 공유하였다. 이들 자료는 디스코드의 기본 첨부 기능을 통해 전송되었다. 이후, 연속적인 텍스트 메시지를 작성하였다.

(1) 17:55, cat_president_campaign.pdf 파일이 업로드되었다. 해당 PDF 파일은 고양이 대통령 선거 유세 캠페인 형식의 문서이며, 파일 크기는 약 18.30KB로 확인된다.

(2) 17:57, 고양이 관련 유튜브 영상 링크가 첨부되었으며, 디스코드 인터페이스 상에서 자동으로 썸네일과 함께 미리보기 영상으로 표시되었다.

(3) 17:57, cat_president.ps1 파일이 코드 블록 형태로 첨부되었고, 별도 다운로드 링크도 함께 제공되었다. 해당 스크립트는 $APPDATA 경로에 위장 파일을 생성하는 PowerShell 명령어가 포함된 .ps1 실행 파일이다.

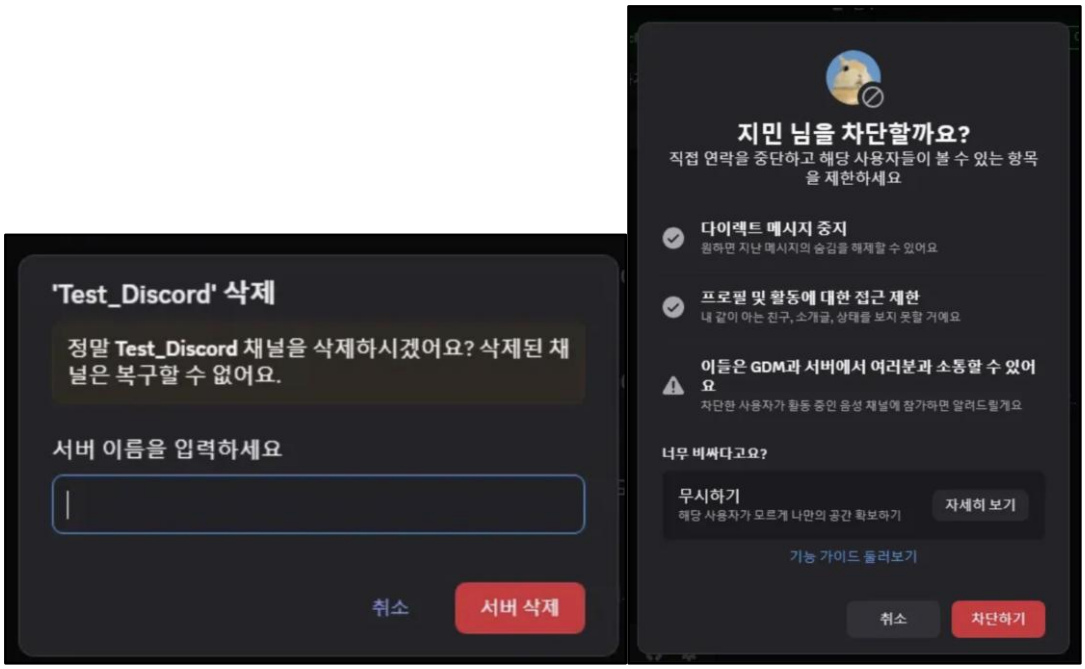
8. 이벤트 생성



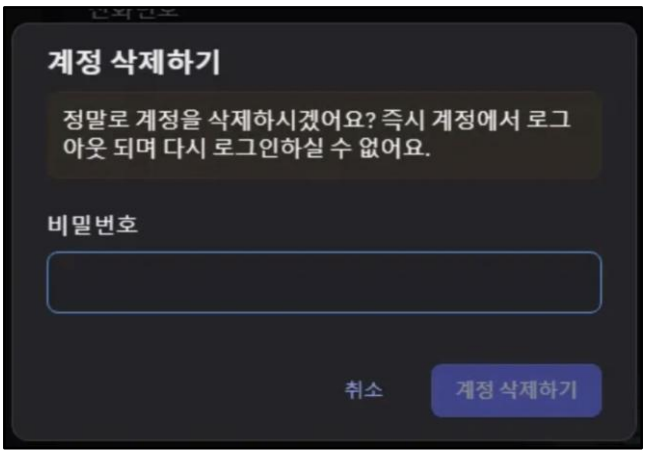
[그림 13. 서버 일정 이벤트 등록]

1) 18:02, 디스코드 서버 Test_Discord 내에서 기호 1번 고양이 계정은 이벤트 생성 기능을 사용하여 신규 일정을 등록하였다.

9. 서버 장악 후 서버 및 계정 삭제



[그림 14, 15. 서버 삭제 및 사용자 차단]



[그림 16. 계정 삭제]

1) 18시 이후, Alice 계정은 다음과 같은 순서로 디스코드 서버 및 계정 관련 작업을 수행하였다.

(1) 18:06, 사용자 차단, imin 계정을 서버 멤버 목록에서 선택한 뒤, 차단 사유를 '서버 규칙 위반'으로 지정하여 차단을 수행하였다. 차단 절차 중, 최근 6시간 내의 메시지를 함께 삭제하는 옵션이 선택되었다.

(2) 18:10, 서버 삭제, Test_Discord 서버 설정 메뉴에서 "서버 삭제"를 선택하고, 삭제 확인을 위해 서버 이름을 직접 입력해야 하는 창이 나타났다. 해당 작업은 서버 소유자가 수행할 수 있으며, 삭제 후 복구가 불가능하다는 안내가 표시되었다.

(3) 18:12, 친구 차단, 디스코드 친구 목록에서 jimin 계정을 선택하고, 다이렉트 메시지 중지 및 활동 차단 옵션을 포함한 친구 차단을 진행하였다.
차단 이후 해당 계정과의 연결은 해제되며, 상호 메시지 전달이 불가능해진다.

(4) 18:13, 계정 삭제, Alice 계정은 내 계정 > 계정 삭제 메뉴로 이동하여 비밀번호 입력 후 계정 삭제를 시도하였다. 디스코드는 계정 삭제 직후 로그아웃되며, 다시 로그인하거나 복구할 수 없음을 경고하였다.

V. 참고 자료

[1] Discord Inc.,「Discord 지원 센터」, Discord 공식 웹사이트, https://support.discord.com/hc/ko,

[2] Discord Inc.,「Discord 초보자를 위한 안내서」, Discord 공식 웹사이트, https://support.discord.com/hc/ko/articles/360045138571,