Office Security Center
악성코드

기술 컨택센터 - 조미희 매니저

[Proprietary Information]
본 문서는 안랩의 저작물로서 법적 보호를 받습니다.

© AhnLab, Inc. All rights reserved.

AhnLab

Table of Contents

1. 2026년 상반기 사이버 위협 동향

2. 악성코드 감염 경로

3. 악성코드 탐지 및 알림 프로세스

4. 악성코드 감염 이후 대응

5. 악성코드 감염 예방

AhnLab

1. 2026년 상반기 사이버 위협 동향

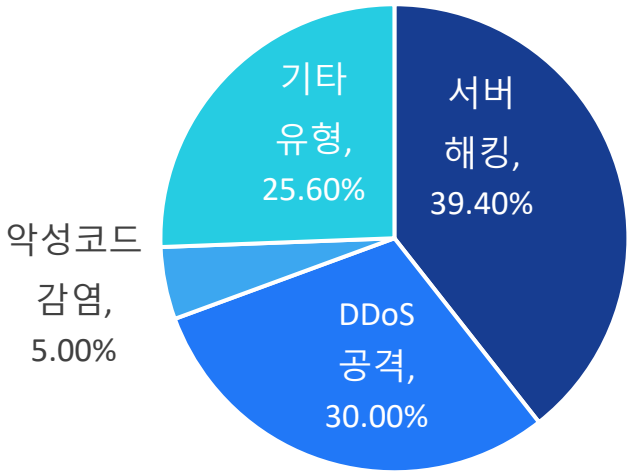
AhnLab

2026년 사이버 위협 동향

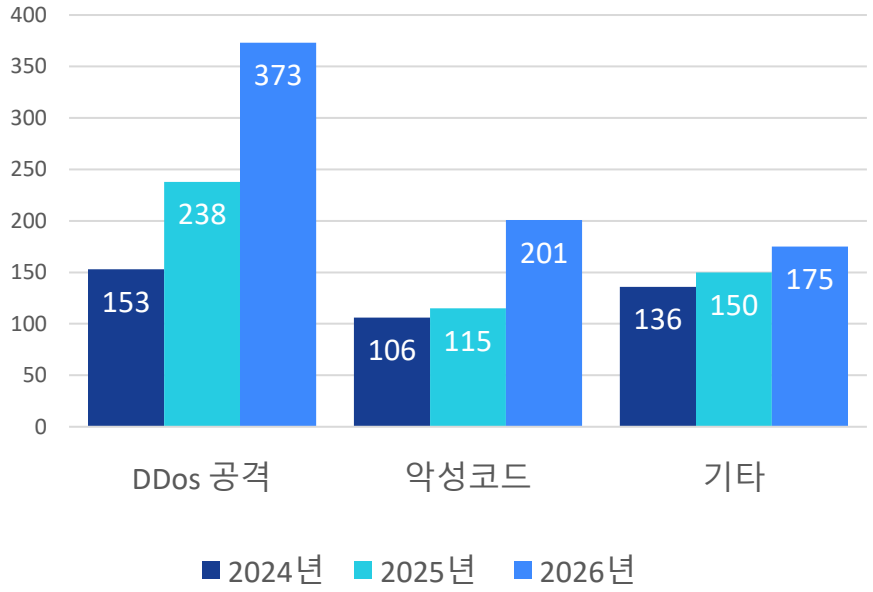
◆ 주요 악성코드 위협 트렌드

2026년 악성코드 동향은 인공지능(AI) 악용 증가, 랜섬웨어의 지속적 확산 및 정교화, 웹브라우저 기반의 우회 감염 수법 등 공격 방식이 다양해지고 공격자의 활동 범위도 넓어지고 있습니다.

1. 침해 유형



2. 침해 신고 접수 현황



2. 악성코드 감염 경로

01 이메일을 통한 감염

02 웹사이트를 통한 감염

03 USB를 통한 감염

AhnLab

01
이메일을 통한 감염

02
웹사이트를 통한 감염

03
USB를 통한 감염

01 이메일을 통한 감염

1. 감염 방법
- 견적서, 이력서, 급여 명세서 등 정상적인 이메일을 가장하여 첨부 파일을 실행하도록 유도
- 악성 사이트로 접속을 유도

2. 감염 예방법
- 발신자 이메일 주소 확인(도메인 주소 확인, 받기로 한 메일인지 확인)
- 첨부 파일의 확장자 확인
- V3 Office Security 의 실시간 검사로 파일 실행 및 압축 해제 시 검사



02 웹사이트를 통한 감염

1. 감염 방법
- 불법 공유, 무료 다운로드에서 악성코드가 포함된 파일 다운로드
- 정상 웹사이트 또는 웹사이트에 노출되어 있는 광고를 해킹하여 악성코드 배포
- 가짜 사이트(피싱 사이트) 접속을 유도한 후 접속하자마자 악성코드를 다운로드 받는 스크립트 실행

2. 감염 예방법
- 정품 소프트웨어 사용
- 공식 사이트 확인 후 접속
- V3 Office Security 의 실시간 검사로 악성 파일이 실행 되기 전 검사



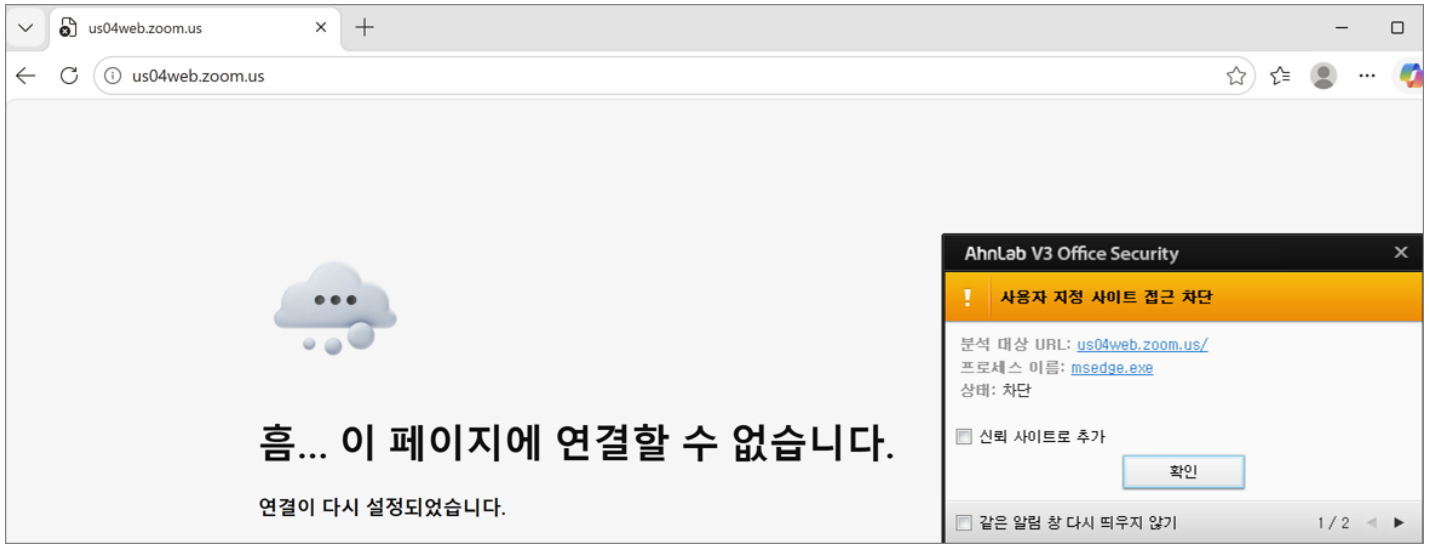
01
이메일을 통한 감염

02
웹사이트를 통한 감염

03
USB를 통한 감염

02 웹사이트를 통한 감염

- V3 Office Security 의 유해 사이트 차단 설정으로 피싱 사이트, 악성 사이트 접속 차단



01
이메일을 통한 감염

02
웹사이트를 통한 감염

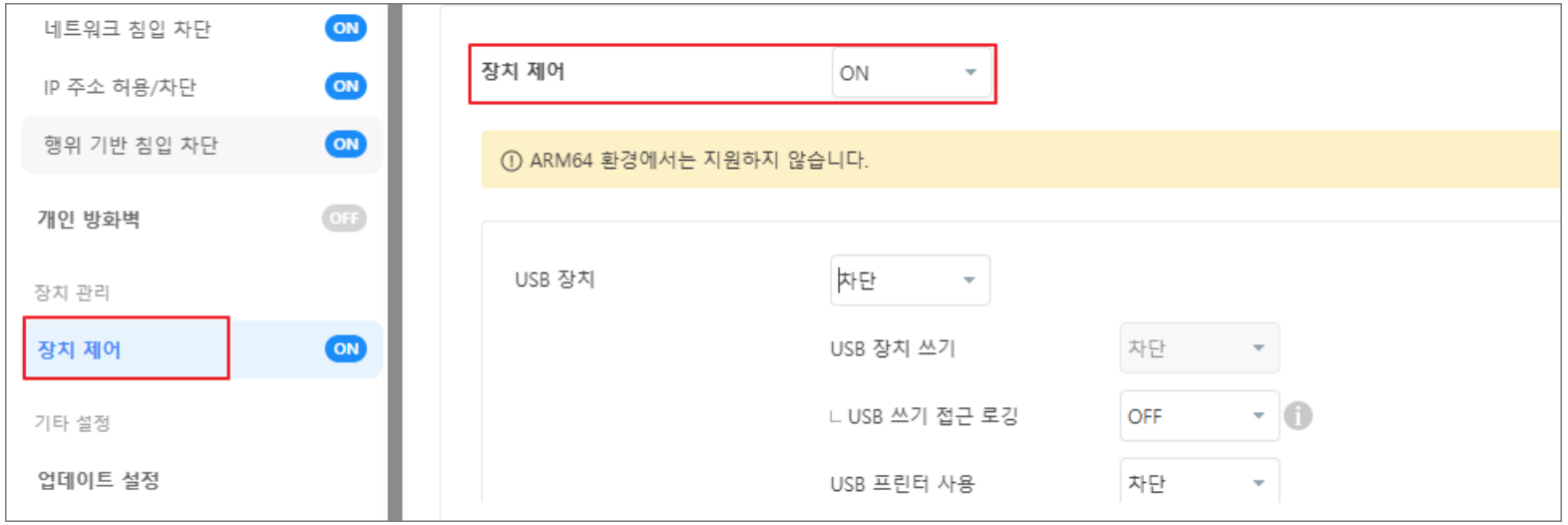
03
USB를 통한 감염

03 USB를 통한 감염

1. 감염 방법
- USB, 외장하드, 네트워크 드라이브 등의 이동식 저장 장치에 autorun.inf 파일을 생성하여 장치 연결 시 자동으로 악성코드를 실행

2. 감염 예방법
- V3 Office Security의 실시간 검사를 이용하여 악성 파일 실행 전 검사
- CD/USB 자동 실행 방지 및 자동 검사 기능으로 USB 연결하자 마자 자동 실행되는 악성코드 검사
- 장치 제어를 설정하여 허가되지 않은 USB 사용 차단





3. 악성코드 탐지 및 알림 프로세스

01 악성코드 탐지 및 알림 프로세스

02 악성코드 감염 알림 메일

AhnLab

01
악성코드 탐지 및 알림 프로세스

02
악성코드 감염 알림 메일

01 악성코드 탐지 및 알림 프로세스

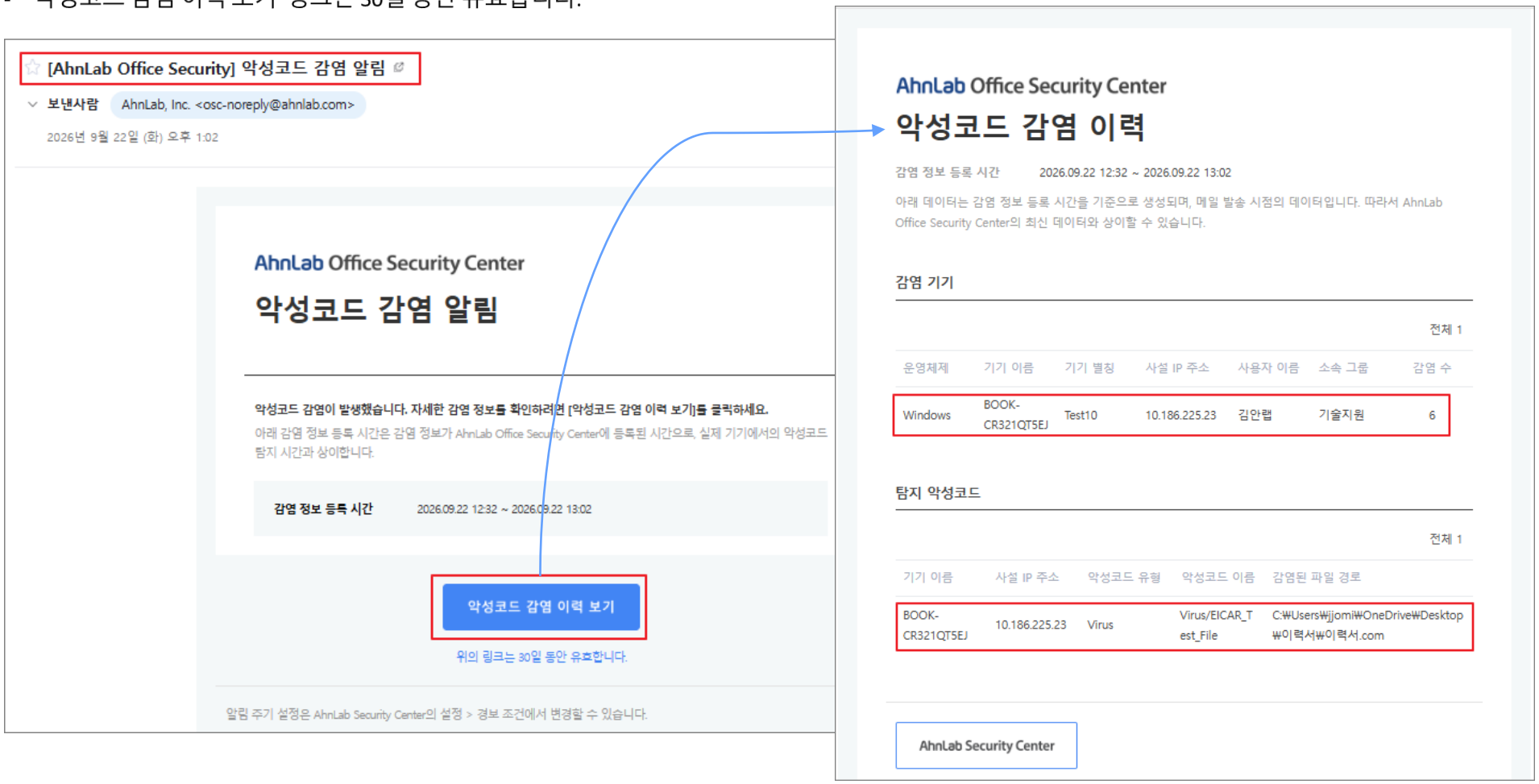
악성코드 유입	• 이메일의 첨부 파일이나 링크, 웹사이트 등 악성코드 감염 경로를 통해 악성코드가 시스템에 유입
⇩	
V3 Office Security 악성코드 진단	• V3 Office Security 의 실시간 검사, 정밀 검사를 통해 악성코드 진단
⇩	
서버로 진단 로그 전송	• V3 Office Security의 진단 로그를 20분 간격으로 서버로 전송
⇩	
악성코드 감염 알림 메일 발송	• 서버로 전송된 진단 로그를 30분 간격으로 확인하여 악성코드 진단 이력이 확인되면 등록된 관리자 이메일 주소로 알림 메일 발송

01
악성코드 탐지 및 알림 프로세스

02
악성코드 감염 알림 메일

02 악성코드 감염 알림 메일

1. 악성코드 감염 알림 메일
- 서버로 전송된 V3 Office Security의 로그를 30분 간격으로 확인하여 악성코드 진단 기록이 있는 경우, 등록된 관리자에게 '[AhnLab Office Security]악성코드 감염 알림' 제목으로 메일이 발송됩니다.
- 악성코드 감염 이력 보기를 클릭하면 감염된 사용자 정보와 악성코드 이름, 감염 파일명 등 감염 정보를 확인할 수 있습니다.
- 악성코드 감염 이력 보기 링크는 30일 동안 유효합니다.

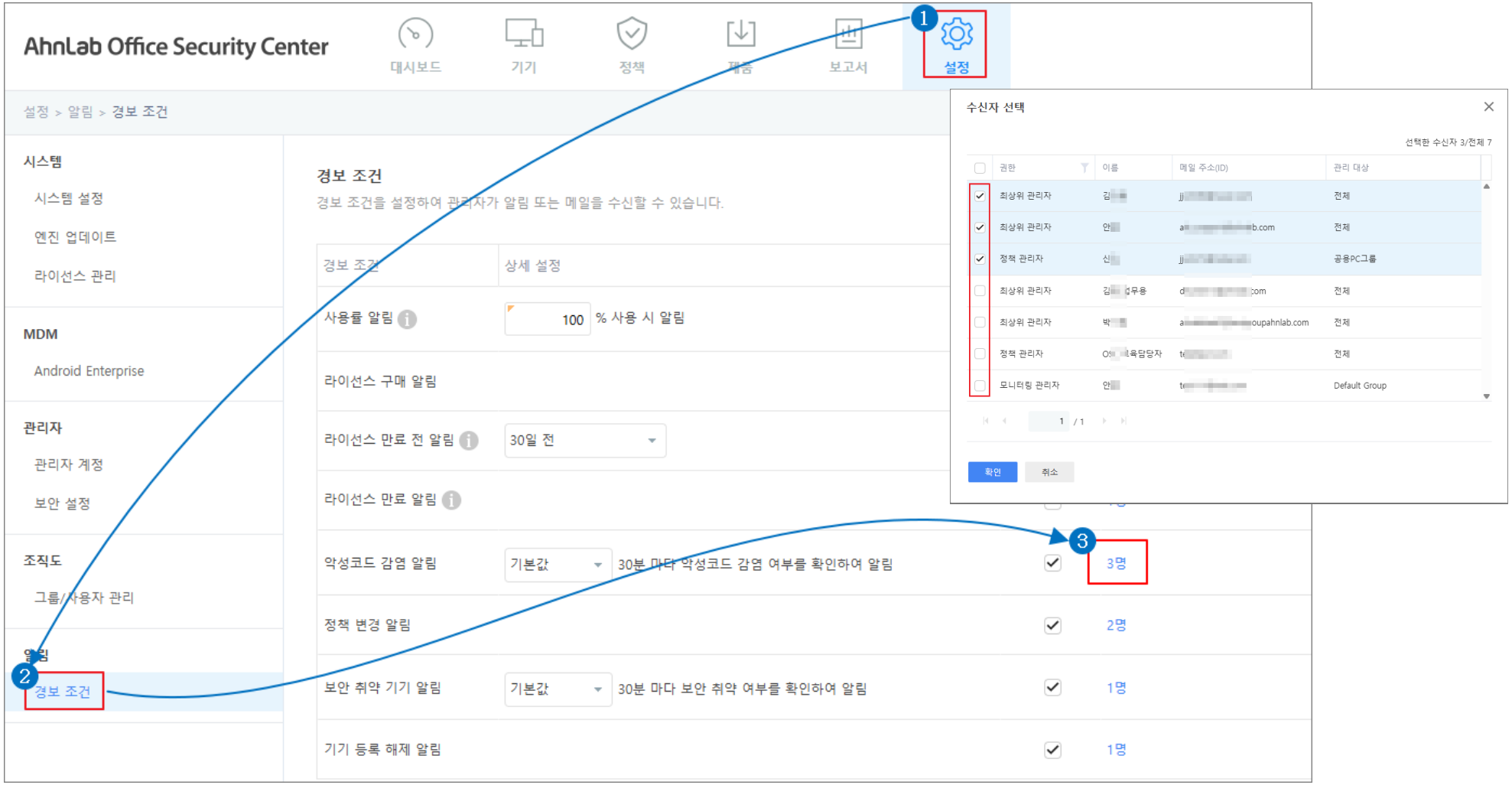


01
악성코드 탐지 및 알림 프로세스

02
악성코드 감염 알림 메일

02 악성코드 감염 알림 메일

2. 악성코드 감염 알림 메일 수신자 설정
- 악성코드 감염 알림 메일을 수신할 수신자는 [설정]메뉴에서 아래의 순서대로 진행하여 등록된 관리 중 수신자를 추가할 수 있습니다.



4. 악성코드 감염 이후 대응

01 악성코드 감염 후 대응 프로세스

02 감염 PC 및 정보 확인

03 치료 상태 점검

04 원격 검사

05 감염 원인 분석

06 신고센터 분석 요청

AhnLab

01
악성코드 감염 후 대응 프로세스

02
악성코드 감염 알림 메일

03
치료 상태 확인

04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

01 악성코드 탐지 및 알림 프로세스

감염 PC 및 악성코드 정보 확인	• 감염 알림 메일 또는 Office Security Center를 통해 감염 PC/감염된 사용자/악성코드 명/탐지 시간을 확인
치료 상태 확인	• Office Security Center에서 악성코드 치료 상태(치료 완료, 치료 불가, 재감염) 확인
정밀/원격 검사	• V3 Office Security 의 정밀 검사 또는 Office Security Center 의 원격 검사를 이용하여 남아 있는 악성코드가 있는지 확인
감염 원인 분석	• 악성코드 감염 직전 작업을 확인하여 악성코드 유입 경로를 파악하여 재감염 방지
신고센터 분석 요청	• 악성코드 치료 불가, 재감염 또는 악성코드에 대한 상세 정보가 필요한 경우 위협정보 신고센터로 분석 요청 접수

01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

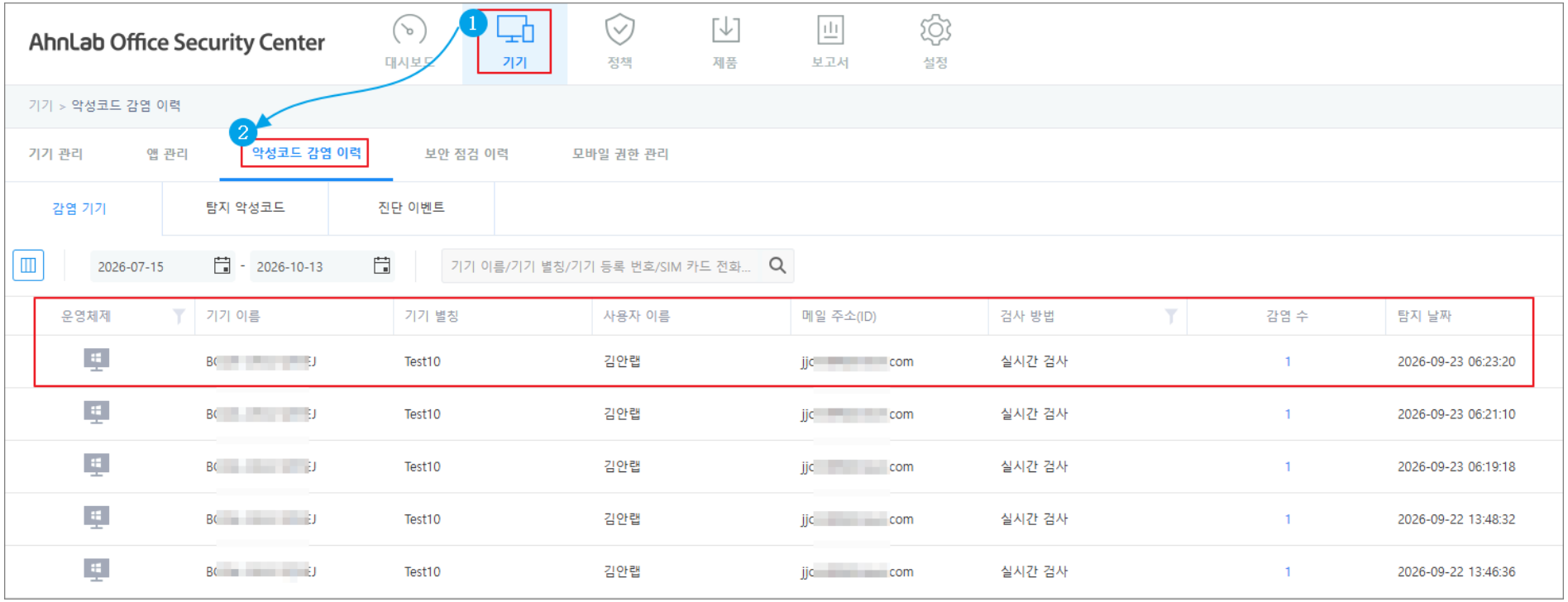
04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

02 감염 PC 및 악성코드 정보 확인

1. 악성코드 감염 정보
- Office Security Center 의 [기기] > [악성코드 감염 이력]을 클릭하여 그 동안 진단 됐던 악성코드 감염 이력을 확인



01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

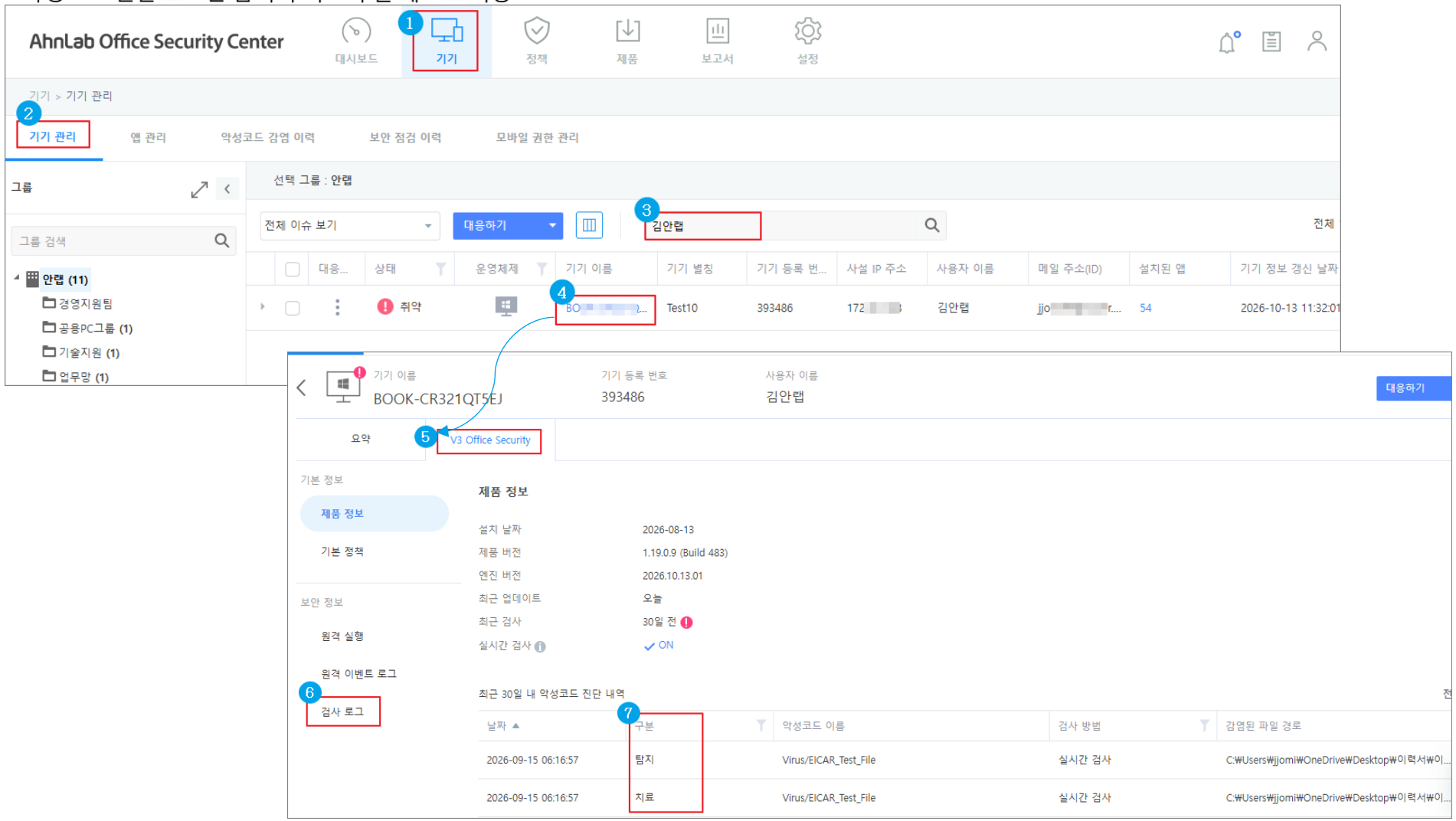
04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

03 치료 상태 확인

- 아래 그림과 같은 순서대로 [기기 관리]에서 감염 기기명을 검색한 후, 기기 상세 정보의 [감염 로그]에서 진단된 악성코드의 치료 상태 정보(치료 완료, 치료 불가, 재감염)를 확인
- 악성코드 진단 로그는 탐지와 치료가 한 세트로 저장



01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

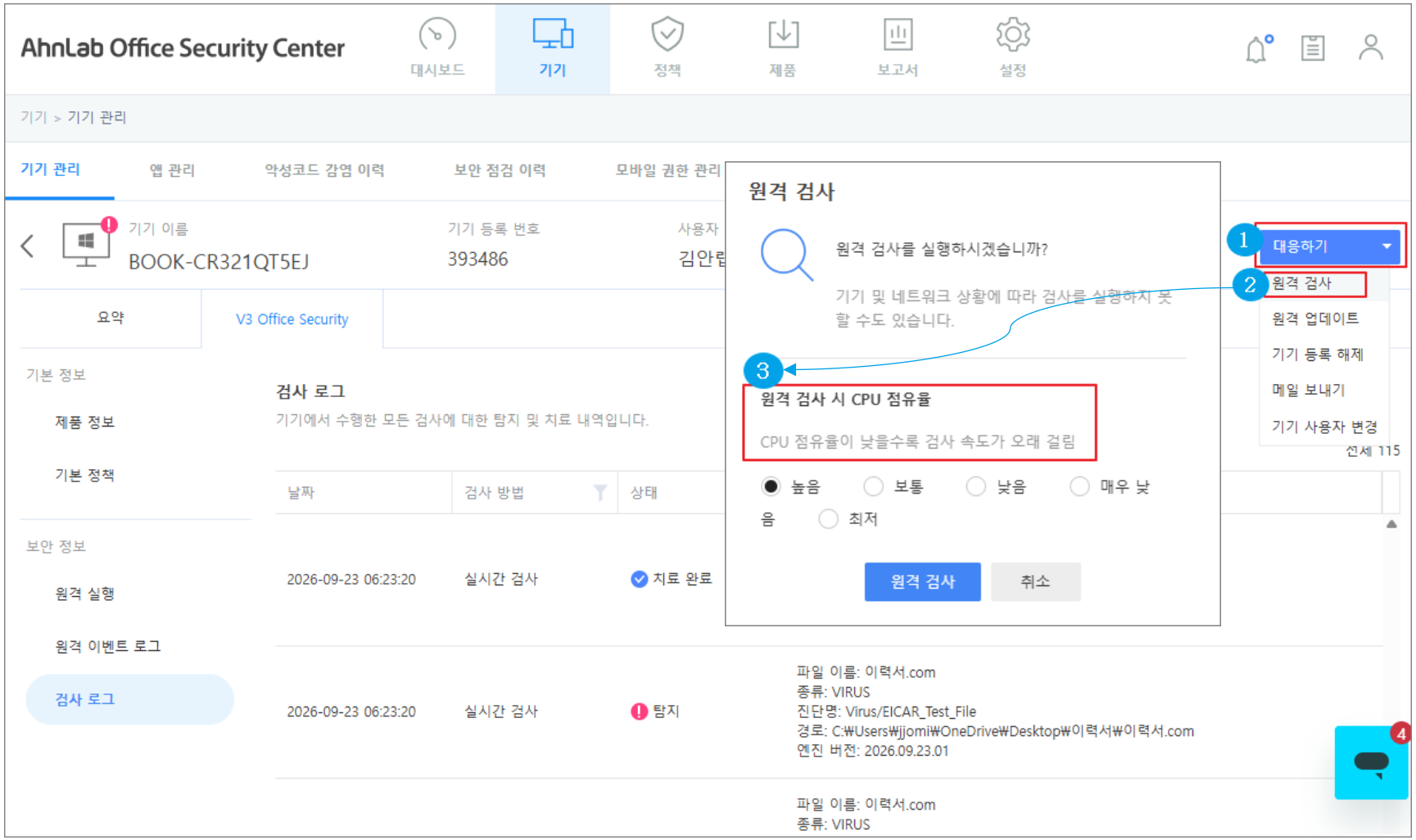
04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

04 원격 검사

- 실시간 검사는 저장되어 있는 파일에 대한 검사를 하지 않으므로 원격 검사를 실행하여 저장된 파일 중 악성코드가 감염된 파일이 있는지 확인
- CPU 점유율에 따라 검사 속도가 달라질 수 있으나, 업무에 영향을 줄 수 있으므로 적정한 선택 필요
- 원격 검사는 대상 PC가 온라인 상태인 경우, 원격 검사 실행 후 15분 정도 후에 명령이 전달되어 검사 동작



01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

06 신고센터 분석 요청

1. 신고센터 분석 요청이 필요한 경우

의심 파일/ 의심 증상 신고	• 악성코드로 의심되는 파일을 암호를 걸어 압축한 후 접수 • 악성코드 의심 증상이 있는 경우 Ahnreport를 이용하여 시스템 정보 수집 후 접수
오진 신고	• 정상 파일이 악성코드로 진단된 경우
악성코드 정보 요청	• 진단된 악성코드에 대한 상세 정보가 필요한 경우
악성코드 치료 불가/ 재감염	• 진단된 악성코드가 치료 불가 / 치료 후 재감염이 반복되는 경우

01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

06 신고센터 분석 요청

1. 신고센터 접수 방법

의심 파일/ 의심 증상 신고	• 악성코드로 의심되는 파일을 암호를 걸어 압축한 후 접수 • 악성코드 의심 증상이 있는 경우 Ahnreport를 이용하여 시스템 정보 수집 후 접수
오진 신고	• 정상 파일이 악성코드로 진단되는 경우
악성코드 정보 요청	• 진단된 악성코드에 대한 상세 정보가 필요한 경우
악성코드 치료 불가/ 재감염	• 진단된 악성코드가 치료 불가 / 치료 후 재감염이 반복되는 경우

01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

06 신고센터 분석 요청

2. 신고센터 접수 방법
- 안랩 닷컴 로그인 후 [고객지원] > [위협정보 신고센터]로 접속하여 신고서 작성 및 개인 정보 수집 동의 후 접수하기



01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

06 신고센터 분석 요청



- 신고 내용에 알맞은 제목 선택하거나 직접 입력

- 답변 완료 안내 문자를 수신할 핸드폰번호와 문자 수신 가능한 시간 설정

- 답변을 수신할 이메일 주소 입력 (관리자 이메일 주소 입력)

- 신고 내용을 자세히 기록

- 악성코드 의심 파일은 암호를 설정하고 압축
- 악성코드 의심 증상은 AhnReport 자동 수집 가이드를 참고 하여 정보를 수집한 후 첨부

01
악성코드 감염 후 대응 프로세스

02
감염 PC 및 악성코드 정보 확인

03
치료 상태 확인

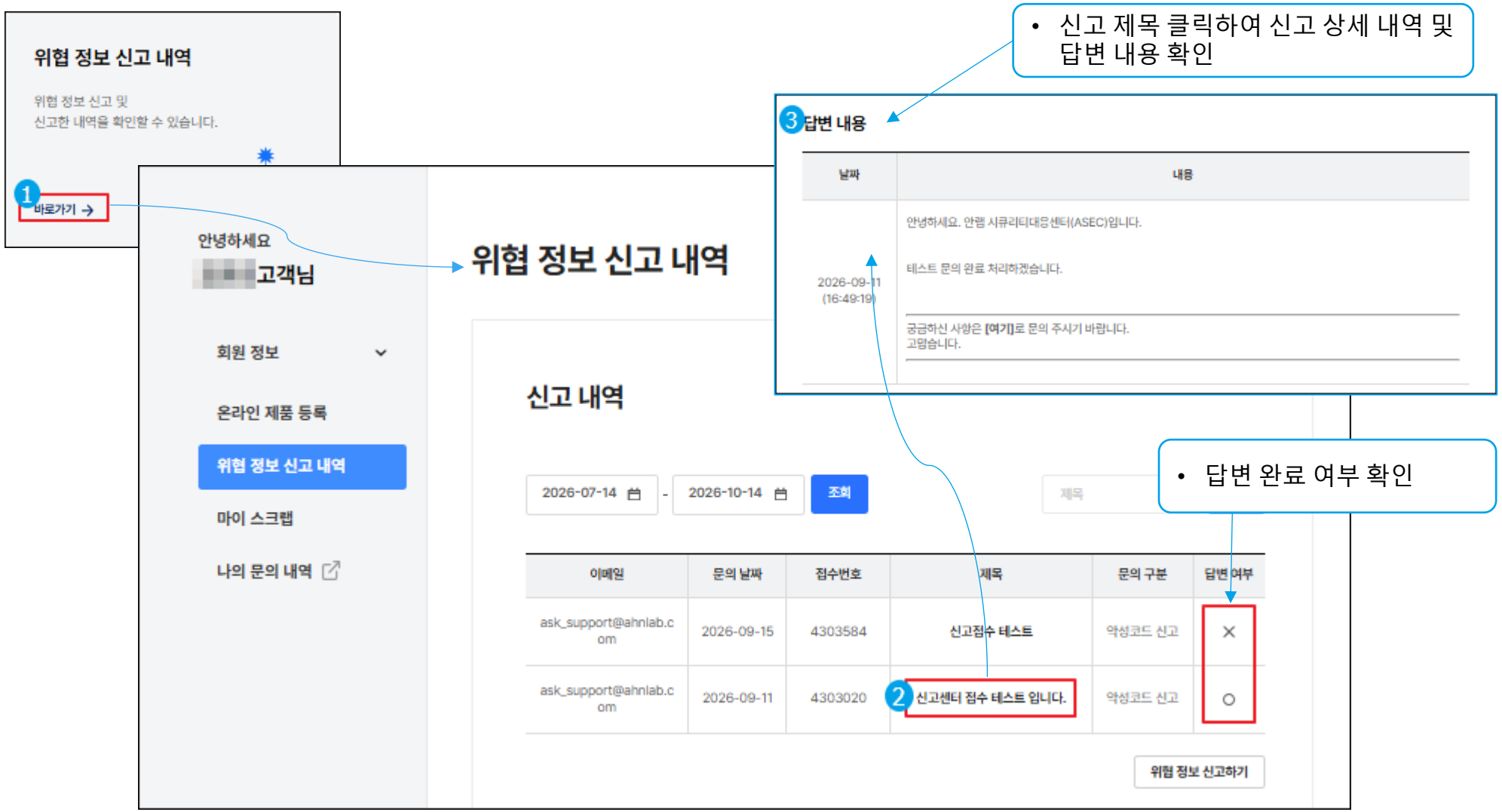
04
원격 검사

05
감염 원인 분석

06
신고센터 분석 요청

06 신고센터 분석 요청

2 신고센터 답변 확인
` 신고센터 접수 후 24시간 이내 답변
` 등록한 이메일 또는 안랩 닷컴 로그인 후 [마이페이지] > [위협 정보 신고 내역]을 클릭하여 확인



5. 악성코드 감염 예방

01 OSC

02 웹사이트를 통한 감염

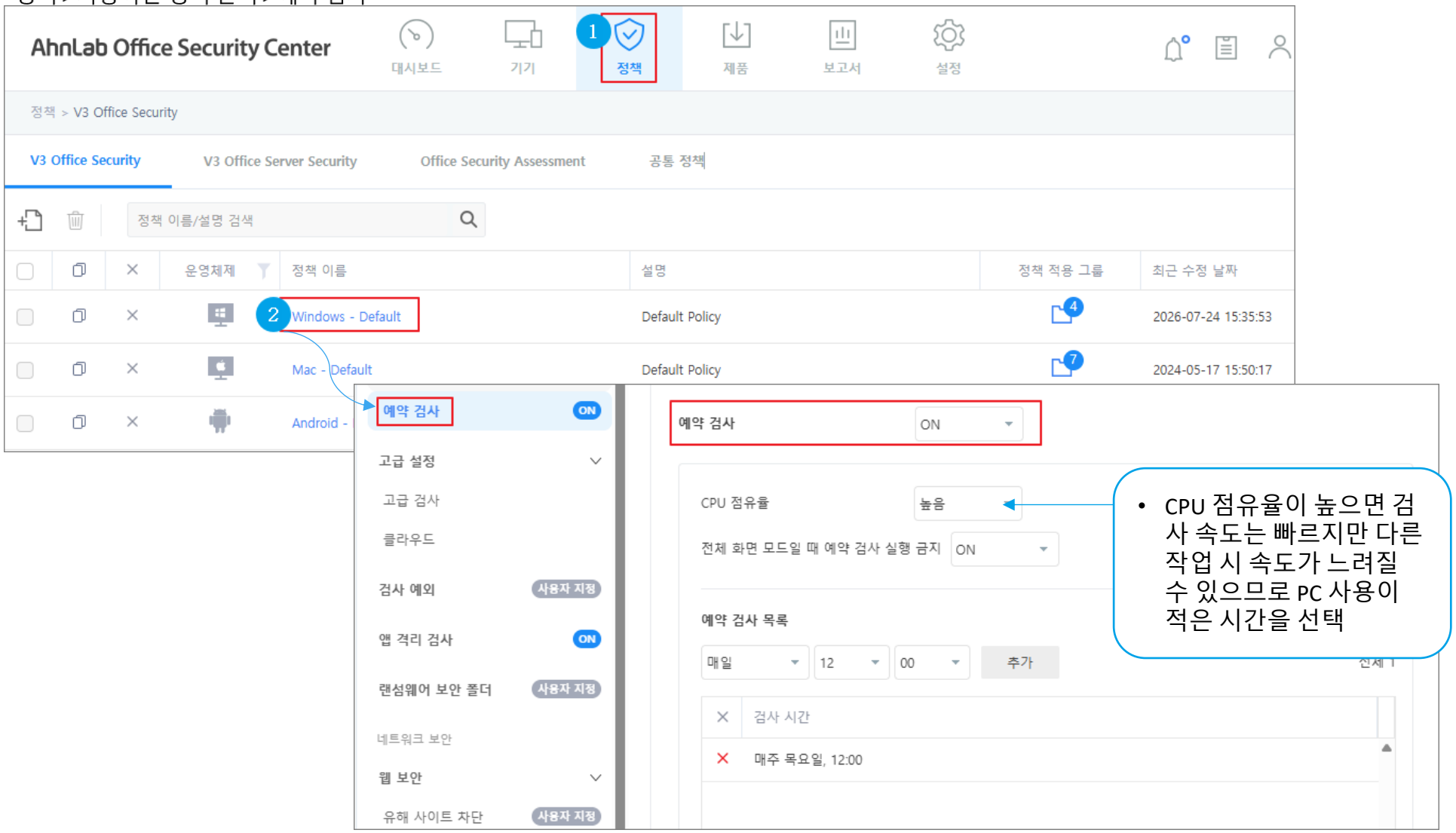
AhnLab

01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

1. 예약 검사 설정
- 저장되어 있는 모든 파일을 정기적으로 검사할 수 있도록 예약 검사 설정
- 정책 > 사용하는 정책 선택 > 예약 검사



- CPU 점유율이 높으면 검사 속도는 빠르지만 다른 작업 시 속도가 느려질 수 있으므로 PC 사용이 적은 시간을 선택

01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

2. USB 자동 실행 방지 및 자동 검사
- USB 연결 시 자동으로 악성코드가 실행되는 것을 방지하고 자동 검사 실행하도록 설정
- 정책 > 사용하는 정책 선택 > 고급 검사

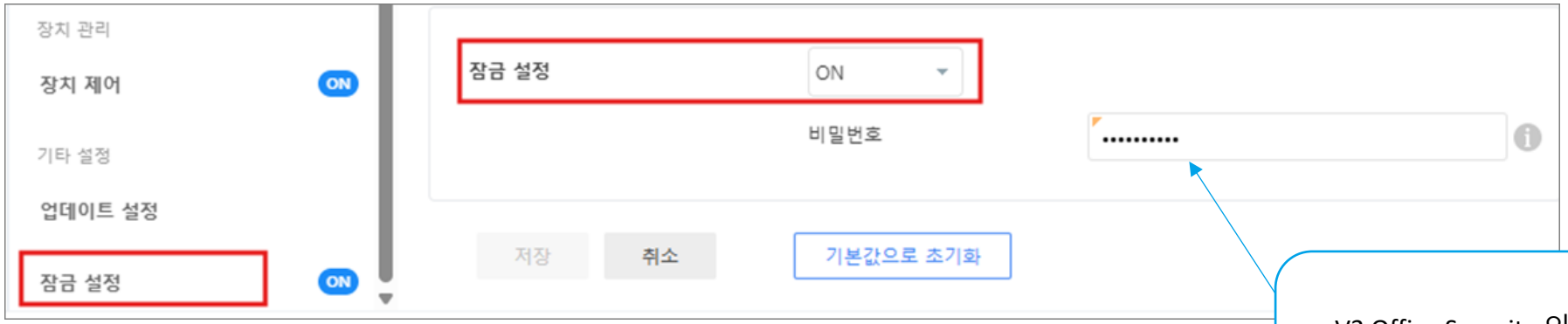


01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

3. 환경 설정 잠금
- 관리자가 설정한 환경 설정을 사용자가 임의로 변경하지 못하도록 환경 설정 비밀번호를 설정
- 정책 > 사용하는 정책 선택 > 잠금 설정



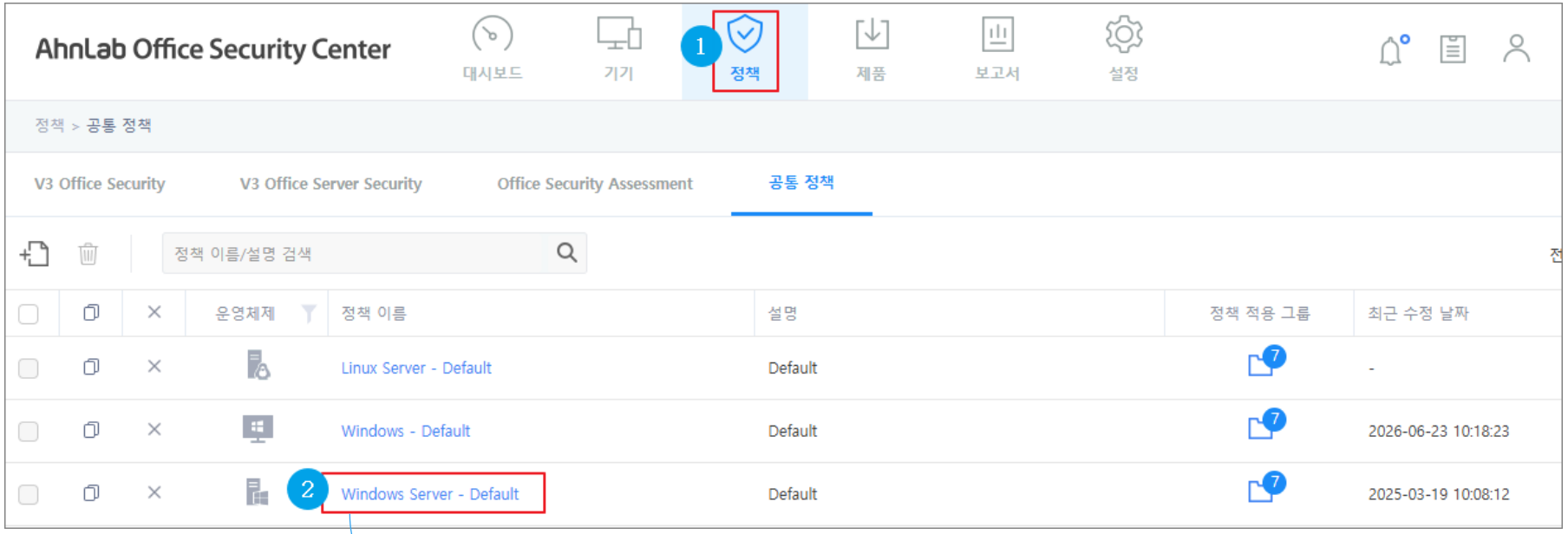
- V3 Office Security 의 환경 설정 클릭 시 비밀번호 입력 창 팝업

01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

4. V3 삭제 방지 설정
- 사용자가 임의로 V3 Office Security 삭제할 수 없도록 삭제 시 비밀번호 입력하도록 설정
- 정책 > 공통 정책 > 사용하는 정책 선택 > 제품 삭제 방지



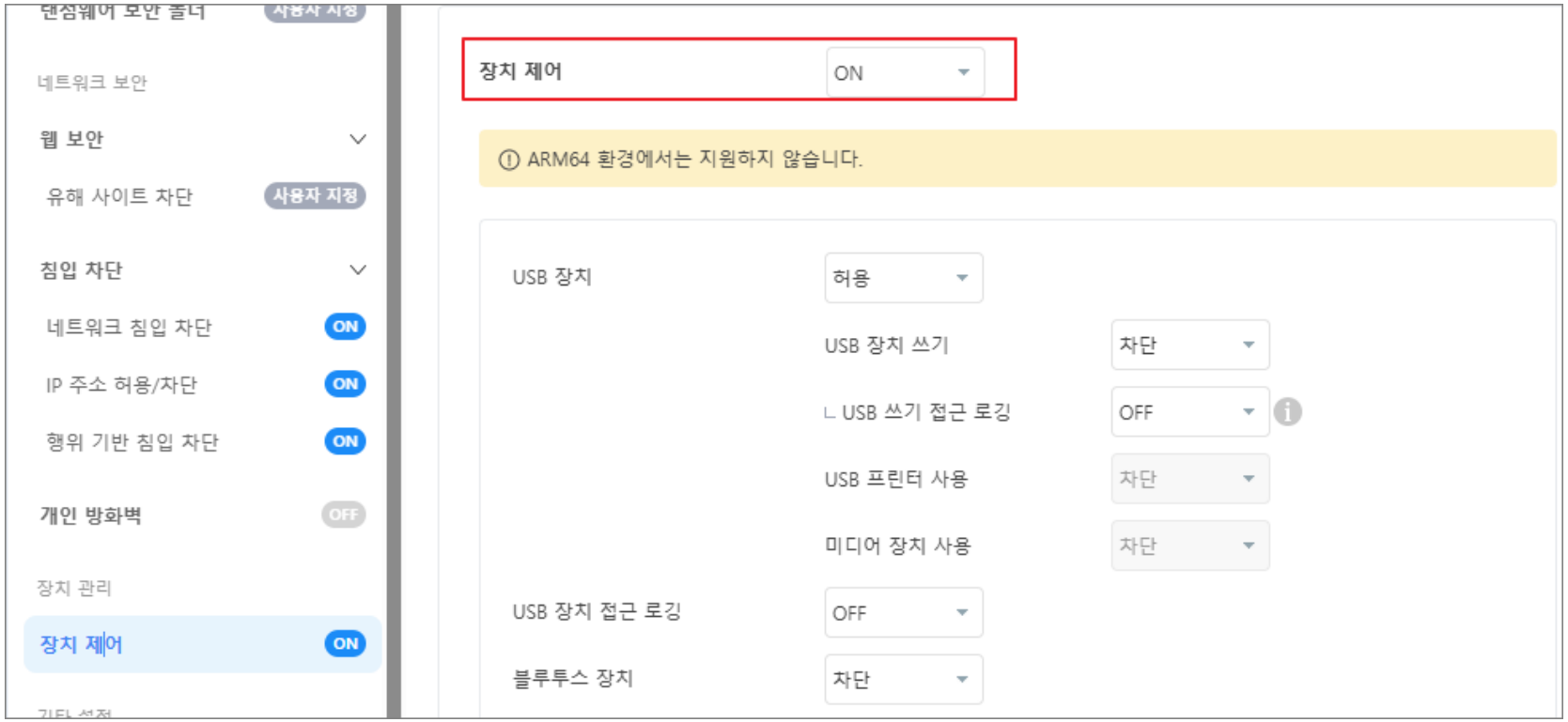


01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

5. 장치 제어 설정
- 허용으로 등록되지 않은 개인 USB 사용 차단
- 정책 > 사용하는 정책 선택 > 장치 제어

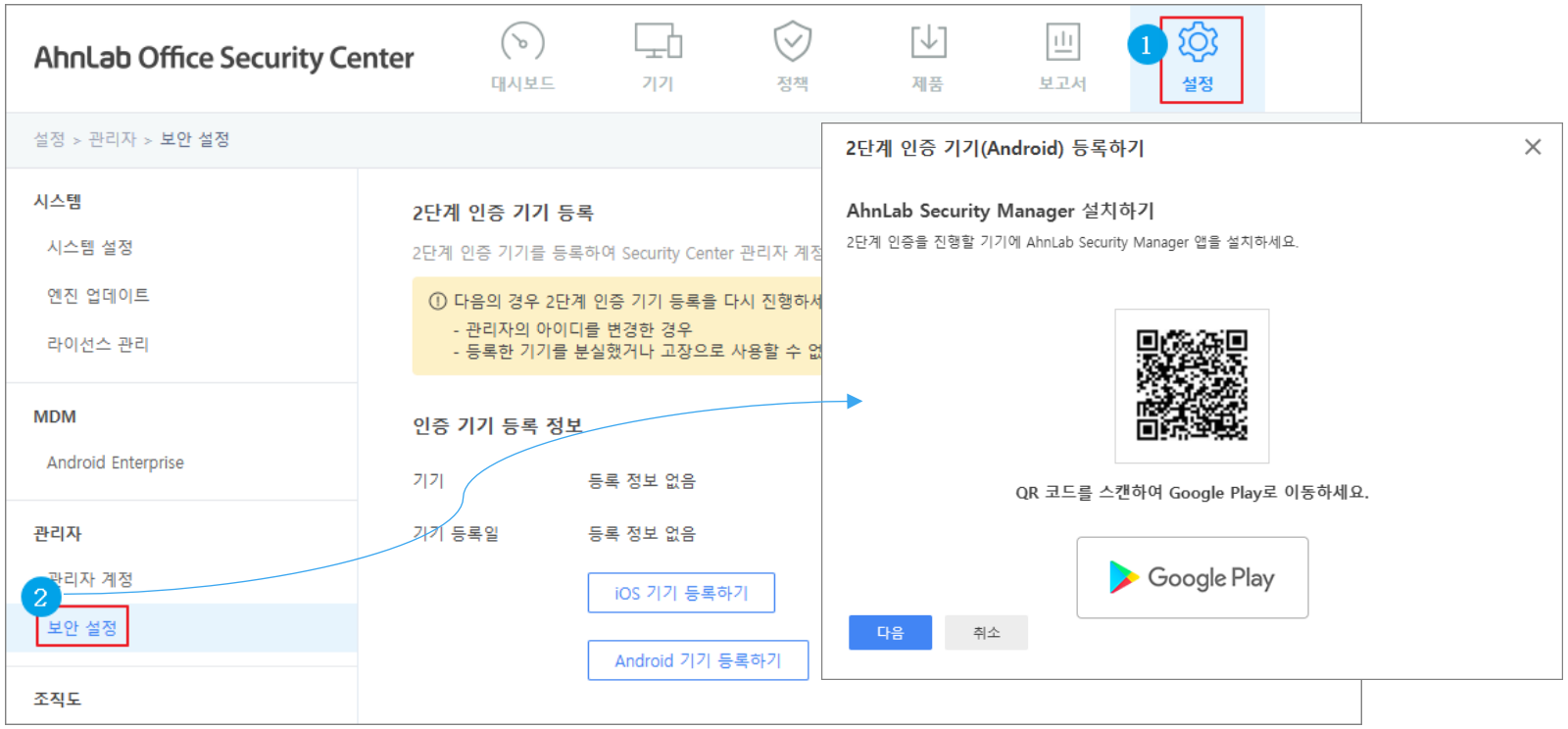


01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

5. OSC 2단계 인증
- Office Security Center 로그인 시 아이디/패스워드 입력 이후 관리자 핸드폰을 이용하여 2단계 인증 설정
- 설정 > 보안 설정 > iOS/Android 기기 등록하기 > QR 코드를 스캔하여 AhnLab Security Manager 설치 및 제품 등록

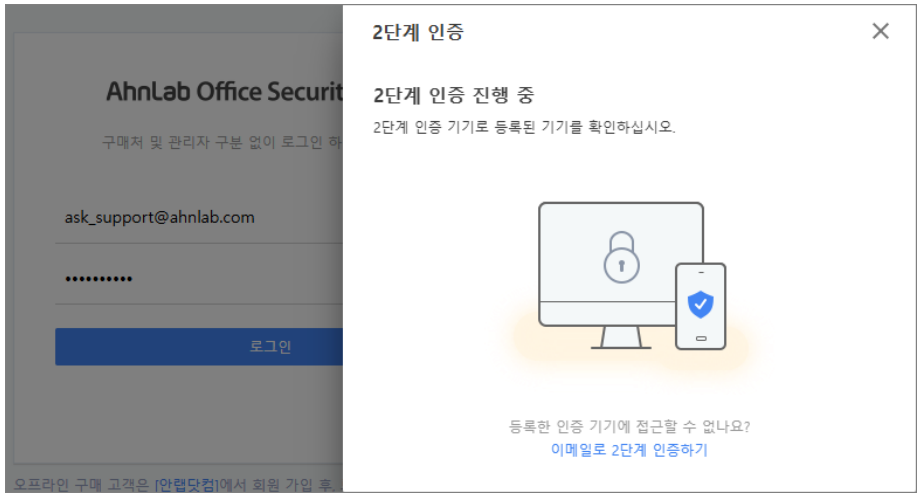


01
관리자의 악성코드 예방

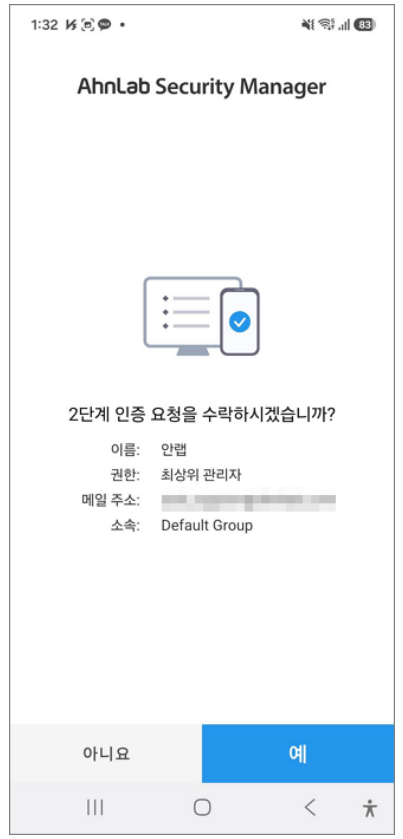
02
사용자의 악성코드 예방

01 관리자의 악성코드 예방

5. OSC 2단계 인증
- Office Security Center 로그인 시 아이디/패스워드 입력 이후 2단계 인증 창 팝업 > 등록된 관리자 휴대폰에서 2차 인증 진행







01
관리자의 악성코드 예방

02
사용자의 악성코드 예방

02 사용자의 악성코드 예방

백신 프로그램 설치 실시간/정밀 검사	• 백신을 설치하고 실시간 검사를 사용 • 주기적으로 정밀 검사를 진행하여 저장된 파일까지 검사
의심스러운 링크, 첨부 파일 클릭 금지	• 메일 수신 시 꼼꼼히 발신자 주소 확인 • 알고 있는 발신자라도 받기로 한 메일이 아니면 첨부파일이나 링크 클릭 금지
소프트웨어는 공식 경로를 통해 다운로드	• 무료 배포 파일 또는 크랙 파일은 악성코드가 포함되어 있는 경우가 많으므로 정품 소프트웨어를 사용하고 공식 경로를 통해 다운로드
운영체제 및 소프트웨어 최신 업데이트	• OS나 브라우저 등 프로그램의 취약점을 이용한 악성코드 감염 예방을 위해 최신 업데이트
공용 와이파이 사용 시 주의	• 공공장소, 카페의 보안이 설정되지 않은 와이파이 이용 시 개인정보 유출 위험성 • 보안이 설정되지 않은 와이파이 이용 시에는 VPN을 사용하고 개인정보 취급을 자제