

**NAVER WORKS**

# 네이버웍스 보안 가이드

- 
- 03 서비스 인프라 보안
  - 04 계정 접속 보안
  - 09 모바일 보안
  - 11 메일 보안
  - 17 기타 보안 기능
  - 19 감사/모니터링/아카이빙

# 가장 안전한 네이버웍스에서 기업 정보를 보관·관리하십시오.

네이버웍스는 국제 인증 기관으로부터 정보 보호 관리 체계에 대한 국제 표준 인증인 ISO/IEC 27001, 27017, 27018 및 SOC2, SOC3(Systrust)를 취득하여 정보 관리의 안정성과 신뢰성을 공인 받았습니다.



0013



## 1. 글로벌 최고 수준의 보안 서비스

네이버웍스는 정보 보안 전담 인력과 긴급 대응 조직에 의해 기업에 최적화된 서비스로 운영합니다.

## 2. 데이터 보관 및 관리

사용자 데이터는 완벽한 논리적·물리적 접근 통제를 통해 안전하게 보관하고 관리합니다.

## 3. 개인 정보 보호 및 관리

사용자 개인 정보를 국제 표준 규격 및 법률 기반으로 안전하고 체계적으로 관리합니다.

## 4. 보안 설정 및 관리

기업의 보안 정책에 맞춰 개인 정보와 데이터를 관리할 수 있도록 다양한 보안 설정 기능을 제공합니다.

# 서비스 인프라 보안

---

## 데이터 센터 물리 보안

---

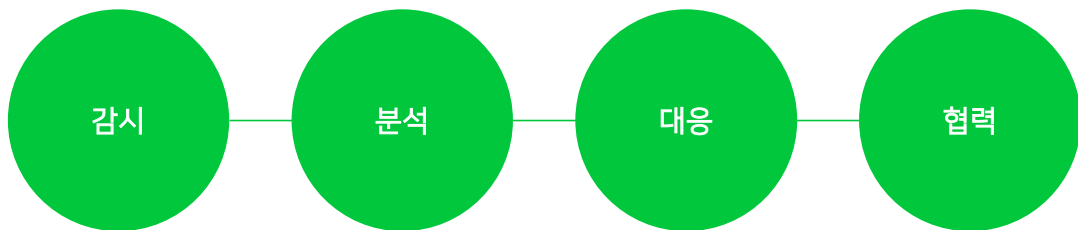
네이버웍스의 데이터는 논리·물리적 접근 통제를 통해 안전하게 보관 및 관리되고 있습니다. 데이터가 보관되어 있는 데이터 센터는 다양한 재해 상황에도 견딜 수 있도록 설계된 물리적 인프라와 시스템 구성을 갖추고 있으며, 다중 구조로 구성되어 데이터를 안전하게 백업하고 있습니다. 모든 서비스는 국제 인증을 받은 높은 수준의 정보 관리 시스템과 워크플로우로 운영됩니다.

필요한 최소 인력만 데이터 센터 출입이 허용되며, 인증된 직원 외에는 데이터 센터 출입이 일체 불가능합니다. 비인가 접속 및 자료 반입을 차단 및 감시하고 있으며, 데이터베이스 접속은 추가 인증을 통과한 직원만 접근이 가능합니다. 데이터베이스의 모든 접속 및 다운로드는 로그가 자동으로 생성되고 감시됩니다.

## 서비스 운영 보안

---

서비스 인프라는 일반 소비자 전용 서비스와 분리된 환경에서 운영됩니다. 네이버웍스의 시스템/보안 전문가 팀이 365일 24시간 면밀하게 시스템을 모니터링하며 고객의 데이터를 안전하게 지키고 있습니다. 실시간으로 멀웨어와 바이러스를 검사하고 최신 스팸 필터링, DoS, DDoS 공격을 지속 감시합니다. 보안 리스크는 발견 즉시 분석하여 대응하고, 재발 방지를 위해 관련 기관들과 정보를 공유하여 신속하고 정확하게 협력하고 있습니다.



OWASP(The Open Web Application Security Project) 상위 항목을 참고하여 정기적으로 취약점 점검을 수행하고 있습니다. 서비스 보안 검수, 정기적인 보안 진단 및 모의 해킹을 통하여 다각도로 보안성 강화를 위해 노력합니다.

# 계정 보안

## 계정 접속 보안

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

네이버웍스는 특정 계정에 비정상 로그인 시도가 발생하면 해당 계정을 자동으로 차단하여 고객 계정을 안전하게 보호합니다. 관리자는 계정이 특정 횟수 이상 로그인 실패 시 계정이 일시 정지되도록 설정할 수 있습니다.

메인 > 보안 > 계정 보안

### 계정 보안

취소 저장

비밀번호 정책

로그인 시도 횟수 제한

- 별도 제한 없음
- 3회 연속 실패 시 계정 일시정지
- 4회 연속 실패 시 계정 일시정지
- 5회 연속 실패 시 계정 일시정지
- 6회 연속 실패 시 계정 일시정지
- 7회 연속 실패 시 계정 일시정지
- 8회 연속 실패 시 계정 일시정지
- 9회 연속 실패 시 계정 일시정지
- 10회 연속 실패 시 계정 일시정지

## 계정 일시 정지

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

사내 정책에 따라 필요한 경우 구성원의 계정을 일시 정지할 수 있습니다.

메인 > 구성원 > 구성원 > 구성원 정보

### 구성원 정보

이전으로 돌아가기

다보기 구성원 수정

안소플  
소니조직 / 사장 / soni@soni.com  
사용중

원격 회사 소속  
회사 soni@soni.com  
ID soni@soni.com

조직/직책  
보조 이메일 ansoni@soni.com

업 차단  
부재 설정  
ID 변경  
계정 삭제  
일시 정지

#### 일시정지 하시겠습니까?

일시정지된 구성원은 NAVER WORKS 서비스를 더 이상 이용할 수 없습니다.

구성원의 계정과 데이터는 삭제되지 않으며, [일시정지 해제]를 통해 일시정지를 해제할 수 있습니다.

취소 확인

# 계정 보안

## 비밀번호 정책 설정

[비인가 접속](#)[정보 유출](#)[멀웨어 대응](#)[오발송 방지](#)[분실 및 도난](#)

고객사 보안 정책에 따라 각 구성원의 네이버웍스 서비스 로그인 비밀번호에 대한 난이도와 만료 날짜를 설정할 수 있습니다.

비밀번호 난이도	<ul style="list-style-type: none"><li>영문과 숫자 조합</li><li>영문, 숫자, 특수문자 혼합</li></ul>
비밀번호 최소 길이	<ul style="list-style-type: none"><li>8~20자</li></ul>
비밀번호 만료 날짜	<ul style="list-style-type: none"><li>30일~1년, 무제한</li></ul>
최근 사용한 비밀번호 재사용 제한	<ul style="list-style-type: none"><li>별도 제한 없음</li><li>최근 비밀번호 1~5개까지 사용 불가</li></ul>

## 구성원의 비밀번호 변경

[비인가 접속](#)[정보 유출](#)[멀웨어 대응](#)[오발송 방지](#)[분실 및 도난](#)

관리자는 각 구성원의 비밀번호를 변경할 수 있습니다. (단, 구성원이 설정한 암호는 확인 불가)  
비밀번호, 디바이스 분실 등의 경우 계정을 정지하거나 삭제할 필요 없이 무단 접속의 위험을 줄일 수 있습니다.

### 비밀번호 변경 방법

[비밀번호 변경](#)

구성원에게 비밀번호 변경을 요청합니다.

[비밀번호 강제 변경](#)

구성원의 비밀번호를 강제 변경합니다.

# 계정 보안

## 2단계 인증

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

관리자 및 구성원의 설정에 따라 계정을 안전하게 보호할 수 있도록 간편 로그인을 제외한 모든 로그인 시점에 2단계 인증을 제공합니다. 2단계 인증 수단은 **휴대폰 번호**나 **개인 이메일**로 제공하며, 관리자는 2단계 인증을 **필수**나 **선택**으로 적용할 수 있습니다.

메인 > 보안 > 계정 보안

### 계정 보안 ?

취소 저장

#### 로그인 설정

2단계 인증 (2-step verification) ?

필수 - 모든 구성원에게 2단계 인증 적용

선택 - 구성원 선택에 따름

LINE으로 로그인 ?

허용

휴대폰 번호로 로그인 ?

허용

모바일앱 간편 로그인 ?

허용

저장 취소

# 계정 보안

## 접속 현황 확인과 강제 로그아웃

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

각 구성원의 최근 90일 전체 접속 내역을 확인할 수 있습니다. 관리자가 구성원을 강제 로그아웃 처리할 수 있기 때문에 외부로부터의 무단 접속이나 사내의 웨도우 IT 모니터링에 효과적입니다.

The screenshot shows a user profile for '안소플' (An So-pl) with a dropdown menu open for '접속 현황' (Login History). The modal window displays a table of login records for the last 90 days.

접속 환경	위치(IP 주소)	관리
Chrome / Mac OS	대한민국 (10.78.139.183)	로그아웃
08-11 11:15	Chrome / Mac OS 대한민국 (10.78.72.48)	로그아웃

디바이스 분실 등으로 구성원의 앱 접속만을 차단하는 경우에는 앱 차단 기능을 활용하여 PC/모바일 앱 접속만 차단할 수 있습니다.

The screenshot shows the same user profile page, but with the dropdown menu open to '앱 차단' (App Blocking). Other options visible include '부재 설정', 'ID 변경', '계정 삭제', and '일시 정지'.

## 원격 장치 접속 관리 (MDM)

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

네이버웍스 MDM에 등록된 모바일 디바이스의 정보를 원격으로 삭제하거나 초기화할 수 있습니다.  
모바일 디바이스 분실 시 대책을 마련하고, 임의의 디바이스 접속에 의한 정보 유출을 방지할 수 있습니다.

※ 외부 MDM을 연동하여 구성원의 iOS 및 Android 디바이스 사용 관리도 가능

메인 > 보안 > 모바일 보안

### 모바일 보안 ?

취소 저장

#### 원격 디바이스 관리 (MDM)

NAVER WORKS MDM ^

필수 - 모든 구성원이 반드시 원격 디바이스 관리 등록

선택 - 구성원 선택에 따라 자율적으로 등록

사전에 구성원이 기기에 직접 NAVER WORKS 디바이스 관리자(Android)/MDM Profile(iOS)를 설치해서 등록된 디바이스에 한해서 원격 디바이스 관리 기능을 실행할 수 있습니다.

예외 관리 [124](#) >



# 모바일 보안

## 화면 잠금

사용자 설정

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

모바일 앱에서 암호 잠금 여부, 암호 형식(길이), 입력 횟수 제한을 설정하여 구성원 외에 제3자에 의한 모바일 앱 사용을 방지할 수 있습니다. 필수 여부를 선택하여 구성원 자율에 맡기는 여부를 선택할 수 있습니다.

메인 > 보안 > 모바일 보안

### 모바일 보안 ?

취소 저장

#### 화면 잠금

필수 여부

- 필수 - 모든 구성원이 반드시 화면 잠금 설정
- 선택 - 구성원 선택에 따라 자율적으로 설정

PIN 형식

- 숫자 4자
- 숫자 또는 영문 6자
- 숫자 또는 영문 8자

해제 시도 횟수 제한

5회 실패 시 모바일앱 로그아웃

## 데이터 저장 기간

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

모바일 디바이스에서 각 서비스의 데이터를 조회할 수 있는 기간을 설정합니다. 기간 외 캐시 데이터는 자동으로 삭제되기 때문에 데이터 관리의 안전성이 향상됩니다.

메인 > 보안 > 모바일 보안

### 모바일 보안 ?

취소 저장

#### 데이터 저장 기간 ?

제한 없음

제한 없음

최근 3일 이내의 데이터만 조회

최근 7일 이내의 데이터만 조회

최근 30일 이내의 데이터만 조회

# 모바일 보안

## 파일 다운로드/업로드 제한

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

모바일 디바이스에 저장되어 있는 파일의 업로드/다운로드를 제한하여 악성코드 등 악의적인 파일이나 데이터의 확산 위험을 줄일 수 있습니다.

메인 > 보안 > 파일 보안

파일 보안 ? 취소 저장

모바일 앱

모바일앱에서 파일 다운로드 제한 ? ^

게시판       메시지

메일       캘린더 (팀/그룹 일정)

주소록       드라이브 (팀/그룹 폴더)

할 일 (그룹 할 일)       설문

모바일앱에서 파일 업로드 제한 ? ^

## 텍스트 복사 제한

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

모바일 디바이스에서 각 서비스의 텍스트 복사를 제한하여 정보 유출을 사전 차단합니다.

메인 > 보안 > 모바일 보안

모바일 보안 ? 취소 저장

텍스트 복사 제한 ? ^

# 모바일 보안

## 화면 캡처 제한

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

관리자는 업무 자료 유출을 방지하기 위해 유저의 모바일 서비스 화면 캡처와 녹화를 제한할 수 있습니다.

※ iOS 기기는 OS 정책 상 캡처 방지가 제한되어 대안으로 화면 캡처 감사 로그가 제공됩니다.

[Admin>감사>모바일 화면 캡처 (iOS)]에서 iOS 기기로 화면 캡처를 시도한 구성원의 정보와 캡처 기록을 확인할 수 있습니다.



## 워터마크 표시

비인가 접속

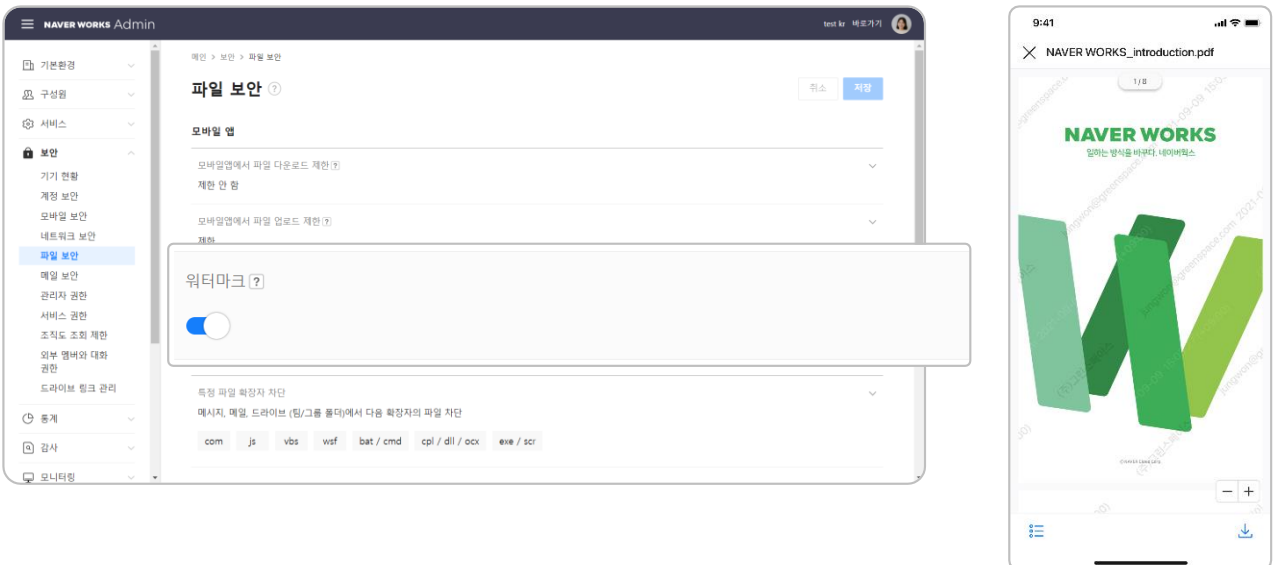
정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

외부 카메라 촬영으로 인한 사내 정보 유출을 방지하기 위해 모바일 공통 (이미지/영상/문서) 뷰어에 회사명, 계정정보 등의 워터마크를 표시할 수 있습니다.



비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

네이버웍스 메일에는 20년 이상 축적된 네이버 메일의 운영 노하우가 적용되어 국내 최고 수준의 Anti-Spam /Anti-Virus 품질을 제공합니다. 위법성 및 범죄성 내용이 포함된 메일, 구성원의 의도와 관련 없는 악성 메일, 수신자의 동의 없이 발송되는 광고 메일 등 스팸으로 분류되는 메일에 대해 상시 대응하고, 구성원이 메일 서비스를 편리하게 사용할 수 있도록 서비스하고 있습니다. 수신한 스팸 메일은 쉽게 삭제하고 수신 차단할 수 있습니다.

### 1. 스팸메일 신고하기 기능

스팸신고 | 연월일 | 이동 | 리마인드 | 더보기

#### 스팸메일 신고하기

선택한 메일의 스팸처리 방법을 설정해 주세요.

스팸메일함으로 보내기  영구 삭제하기

선택한 메일주소 수신 차단하기  
(0 개 / 1000 개)

선택한 메일주소에서 온 기존 메일을 함께 스팸처리

\* 스팸 신고된 메일은 스팸유형 분석에 활용됩니다.  
\* 영구 삭제된 메일은 복구할 수 없습니다.

다음부터 보지 않음

### 2. 스팸 자동 분류 기능

< 스팸 설정

#### 스팸 자동 분류

**스팸 자동 분류 항목**

- 받는 사람, 참조(송신 참조)에 내 메일 주소가 없으면 스팸으로 분류
- 보낸 사람의 주소가 주소록에 있으면 스팸으로 자동 분류
- 언어별 스팸 분류 설정 사용
  - 모든 외국어 메일을 스팸으로 분류
  - 스팸으로 분류할 언어 직접 선택
    - 영어  일본어  러시아어  중국어
  - 보내지 않은 메일에 대한 반송 메일을 스팸으로 분류

**스팸 자동 이동**

### 3. 수신 허용/차단 목록 관리 기능

< 수신 허용

수신할 메일 주소, 도메인, 그룹 메일 주소를 관리합니다.  
수신 허용된 메일 주소, 도메인, 그룹 메일 주소: 1001 / 1,000

**메일 주소/도메인 추가**

**내가 포함된 그룹 메일 주소 추가**

< 수신 차단

수신을 차단할 메일 주소, 도메인을 관리합니다.  
수신 차단된 메일 주소, 도메인: 1000 / 1,000

**메일 주소/도메인 추가**

# 메일 보안

## 외부 메일의 이미지/링크 차단

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

수신 메일에 이미지 및 링크가 포함된 경우, 메일 확인 시 정보가 직접 표시되지 않도록 제한할 수 있습니다. 스팸 및 악의적인 메일을 열어도 첨부 파일, 링크 접속으로 인한 보안 위험을 줄일 수 있습니다.



## 사내 메일 보안 등급 및 유효기간 설정

사용자 설정

비인가 접속

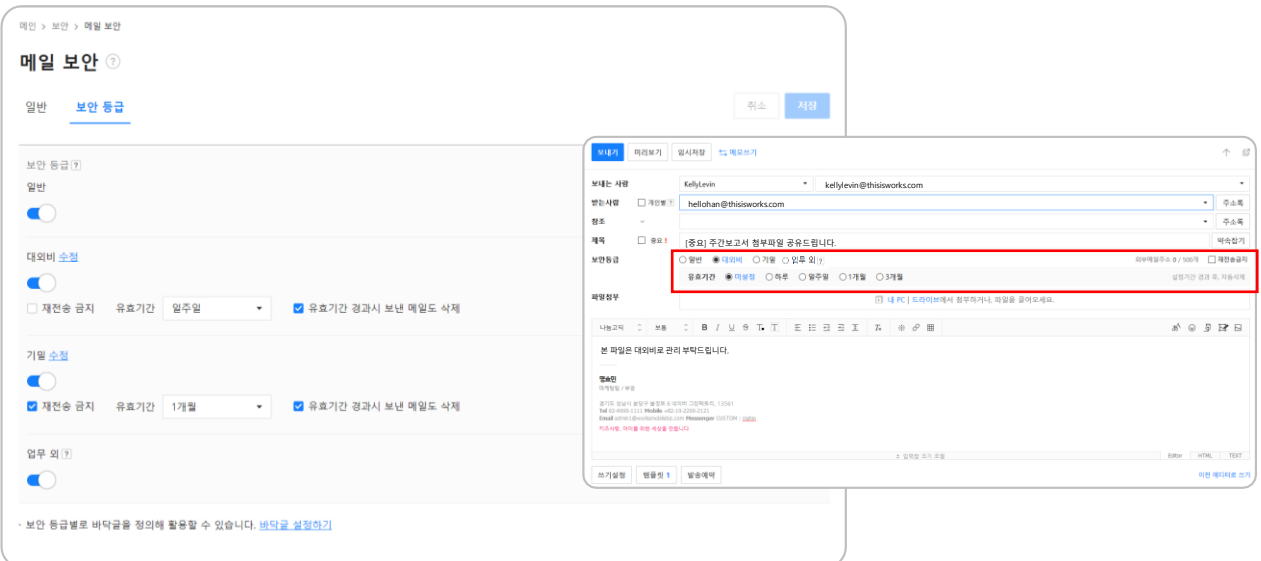
정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

사내 메일을 작성할 때 보안 등급과 메일의 유효 기간을 설정할 수 있습니다. 시간이 경과되면 자동으로 메일이 삭제되기 때문에 중요한 정보를 안전하게 보호할 수 있습니다. 또한 사내 정책에 따라 보안 등급명을 변경하고 보안 등급별로 바닥글을 정의하여 활용할 수 있습니다.



# 메일 보안

## 위험 메일 경고

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

수신한 메일에서 1) 메일 발신자로 표시되는 메일 주소와 실제 메일이 발송된 메일 서버가 다르거나 2) 스팸 필터로 차단되거나 3) 암호화된 압축 파일이 첨부되어 있는 경우 위험 메일 경고가 수신자에게 표시됩니다.

☆ RE:<담당자문의> PC웹 메시지 폴더 3차 개선 디자인 리뷰

2018. 9. 7 (금) 13:26 예약 수정

보낸사람 VIP 김혜수<husee.kim@gmail.com>

이 메일은 [gmail.com]을 통해 발송된 메일이 아닙니다. ?  
보낸사람의 주소가 실제 발송 주소와 다를 수 있으니 주의하시기 바랍니다.

받는사람 개인별 김지나<gjinkim@thisworks.com>, 김수미<sukim@thisworks.com>  
참조 이남수<namlee@thisworks.com>, 김이라<lelakim@thisworks.com>

이 메일이 스팸메일함에 있는 이유 스팸 필터로 자동 차단된 메일

이 메일은 암호화된 압축 파일이 첨부되어 있습니다. 암호화된 압축 파일은 악성코드 검사를 할 수 없어 파일 다운로드 및 압축 해제 시 주의 부탁드립니다.

안녕하세요,  
김혜수입니다

디자인 파일을 첨부 드리니 확인 부탁드립니다.

## 메일 주소 구분

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메일 작성 시 받는 사람(참조, 숨은 참조 포함)란에 입력하는 사내 구성원과 외부 메일 주소가 각각 다르게 표시됩니다. 사내와 사외 메일 주소를 색상으로 구분할 수 있기 때문에 외부로 메일을 잘못 발송하여 정보 유출이 발생하는 리스크를 줄일 수 있습니다.

보내기 예약 임시저장 더보기 메모

받는사람 개인별? 이철수 <lee.cheolso@thisworks.com> NC\_salesmembers <nc\_salesmemb@thisworks.com> 주소록

사내 메일 사외 메일

# 메일 보안

## 메일 백업

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

구성원들이 메일 백업 및 원문을 PC에 저장하도록 허용할지 여부를 설정할 수 있습니다.

메인 > 보안 > 메일 보안

### 메일 보안 ?

[취소](#) [저장](#)

외부 메일 가져오기 ?

허용

외부 메일의 이미지/ 링크를 차단 ?

모든 구성원의 메일에서 이미지/링크를 차단

보안 등급 설정 ?

사용

일반 유효기간 **미설정** / 재전송 **가능**

대외비 유효기간 **3개월** / 재전송 **불가**

기밀 유효기간 **일주일** / 재전송 **불가**

다운로드 기한이 있는 파일 (첨부 가능 용량을 초과하는 파일을 7일간/100회까지 다운로드 가능한 파일로 첨부)

허용

메일 백업/PC에 저장하기 ?

## 메일 인증(DKIM)

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

DKIM(Domain Keys Identified Mail)을 설정하여 발신측 메일이 임의로 변경되지 않았는지 확인하고 안전하게 메일을 수신할 수 있습니다.

메인 > 서비스 > 메일 > 메일 인증(DKIM)

### 메일 인증(DKIM) | 이전으로 돌아가기

[인증 시작](#)

인증 상태	인증 안됨
선택터	<input type="text" value="NAVERWORKS"/> <a href="#">생성</a>
호스트명	<input type="text" value="NAVERWORKS_domainkey"/> <a href="#">복사</a>
공개 도메인 키 (TXT 레코드)	<div>메일 인증을 이용하려면, 새로운 레코드가 필요합니다. 선택터 우측의 생성을 선택해 주세요</div> <a href="#">복사</a>

# 메일 보안

## 메일 수신 게이트웨이

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메일의 감사, 필터링, 아카이빙 등을 위한 외부 게이트웨이 서비스를 사용하고 싶은 경우 [어드민 > 서비스 > 메일](#) 메뉴를 차례대로 클릭한 다음 설정할 수 있습니다.

메일 > 서비스 > 메일

### 메일

일반 서명 [송수신 설정](#)

수신 허용 IP		관리
수신 게이트웨이(2)	sleepyddy.xyz 사용 안 함	관리
수신 라우팅	sleepyddy.xyz 사용 안 함	관리
발신 라우팅	sleepyddy.xyz 사용 안 함	관리
루트 관리	sleepyddy.xyz	관리
메일 인증	sleepyddy.xyz 인증 안 함	관리

## 메일 수신 차단

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

수신 차단 IP를 설정하여 지정된 IP에서 발송된 모든 메일을 차단할 수 있습니다. 수신 허용과 수신 차단에 동일한 IP를 등록하면 수신 허용 기준으로 적용되어 메일이 수신됩니다.

메일 > 서비스 > 메일

### 메일

일반 서명 [송수신 설정](#)

수신 허용 IP(2)		관리
수신 차단 IP(2)		관리
수신 게이트웨이(2)	abcdcompany.com 사용 안 함	관리
	abcdcompany.com 사용 안 함	관리
	abcdcompany.com 사용 안 함	관리
수신 라우팅	abcdcompany.com	관리



# 메일 보안

## 대기 발송

사용자 설정

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메일 보내기를 클릭 후 실제로 메일이 발송될 때까지의 시간을 설정할 수 있습니다. 메일 발송 후 중요 정보가 포함된 것을 발견하면 대기 발송 설정 시간 내에 메일 발송을 취소하여 정보 유출을 방지할 수 있습니다.

### < 메일 쓰기/답장

실수 방지

대기 발송 사용



30초

대기 후 발송

'보내기' 버튼 클릭 후, 설정한 시간만큼 대기하였다 발송하는 기능으로 실수로 메일을 보냈을 때 신속히 발송을 취소하거나 수정할 수 있습니다.

## 미리보기

사용자 설정

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메일 발송 전에 메일 내용을 미리 확인함으로써 잘못 발송하는 리스크를 줄일 수 있습니다.

### < 메일 쓰기/답장

발송 전 미리보기



중요 메일

모든 메일

# 기타 보안 기능

## 파일 보안

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메시지, 노트, 게시판, 메일, 캘린더, 드라이브, 설문에서 사용하는 파일 확장자를 제한할 수 있습니다. 확장자를 제한하여 악성코드 확산, 악성 프로그램을 포함한 실행 파일의 전송을 차단하고 보안 리스크를 줄일 수 있습니다. (단, 파일 보안 기능과 무관하게 바이러스 검사는 모든 서비스에서 기본으로 진행)

### 파일 확장자 차단

특정 파일 확장자 차단

차단할 서비스

게시판/노트  메시지

메일  캘린더 (팀/그룹 일정)

드라이브 (팀/그룹 폴더)  할 일 (그룹 할 일)

설문

차단할 확장자 <sup>?</sup>

일부 실행 파일은 확장자 차단 시 동일한 파일 유형도 함께 차단되어 보안을 강화할 수 있습니다. [자세히 알아보기](#)

확장자 직접 입력

## 외부 사용자와의 대화방에서 파일 전송 첨부 제한

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

외부 네이버웍스/LINE 사용자와 대화 시 정보 유출 방지를 위해 외부 대화방에서 파일 전송 첨부 제한할 수 있습니다. 파일 전송 첨부 제한하면 메시지방에서 파일(카메라, 동영상, 드라이브, 연락처)을 전송할 수 없으며, 외부 네이버웍스의 그룹 내 노트, 일정, 폴더에서도 파일을 첨부할 수 없습니다.

메인 > 보안 > 파일 보안

### 파일 보안 <sup>?</sup>

#### 외부 대화방에서 파일 전송 첨부 제한

LINE 사용자와의 대화방

외부 NAVERWORKS 사용자와의 대화방

# 기타 보안 기능

## 기기 현황

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

네이버웍스에서 구성원의 디바이스 정보, 모바일 앱 버전 등을 확인할 수 있습니다. 사내에서 허용하지 않는 디바이스의 로그인 이력을 확인하고, 모바일 앱 업데이트 알림도 가능하기 때문에 네이버웍스 도입에 따른 사내 보안을 강화할 수 있습니다.

### 기기 현황 ?

모바일 PC 다운로드

최근 30일 내 접속한 모바일 디바이스 66

<input type="checkbox"/>	디바이스-Vendor ID	OS	설치 앱	사용자	최근 접속 ↓
<input type="checkbox"/>	SM-G973N XXXXXXXXXXXX	Android 10	모바일앱 2.9.1.1.stage 업데이트 필요	김어드민 admin	
<input type="checkbox"/>	iPhone X 92805266-D39F-AA4B-0000-00...	iOS 13.1	모바일앱 2.8.6 최신	김어드민 admin	

#### 모바일앱 업데이트 알림

선택한 구성원에게 모바일앱 업데이트 알림을 보내시겠습니까?

취소 확인

## 접속 IP 제한

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

PC 앱, PC 웹을 통한 네이버웍스 서비스 및 드라이브 탐색기 접속을 특정 IP 주소로 제한합니다. 외부 디바이스를 통한 서비스 접속을 제한함으로써 제3자에 의한 악의적인 사용 차단 등 보안 위험을 줄일 수 있습니다. (모바일 앱 접속은 제한 불가)

메인 > 보안 > 네트워크 보안

### 네트워크 보안 ?

취소 저장

접속 IP 제한

모든 IP에서만 접속을 허용

지정한 IP에서만 접속을 허용

- NAVER WORKS의 PC웹, PC앱, 드라이브 탐색기, POP3/SMTP, CalDAV에 적용되며, 모바일앱에서는 IP와 관계 없이 접속할 수 있습니다.
- 안정적인 서비스 관리를 위해 관리자는 설정과 상관없이 NAVER WORKS 서비스에 접근할 수 있습니다.

IP 또는 IP 대역 입력  추가

# 감사/모니터링

## 감사

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

관리자는 감사 기능을 통해 구성원의 각 서비스의 모든 작업 내역을 확인할 수 있습니다. 각 작업 내용의 일시, 내용, 회원 정보 등이 표시되어 효과적으로 관리가 가능하며, 잘못된 사용을 방지할 수 있습니다.

메인 > 감사 > 어드민

어드민 ? 다운로드

2020. 02. 14 - 2020. 08. 11 검색 · Seoul (GMT +09:00) 상세

이벤트 대상	성공 여부	과업	사용자	날짜	IP 주소	서비스 타입	서비스
구성원 초대	성공	조회	김어드민 admin@test.com	2020. 08. 11. 11:35:32	XX.XX.XXX.XX	PC 웹	구성원 - 구성원 초대 - 구성원 초대
주소록	성공	조회	김어드민 admin@test.com	2020. 08. 11. 11:35:28	XX.XX.XXX.XX	PC 웹	검사 - 검사/로그 - 주소록
구성원 초대	성공	조회	김어드민 admin@test.com	2020. 08. 11. 11:35:28	XX.XX.XXX.XX	PC 웹	구성원 - 구성원 초대 - 구성원 초대
캘린더	성공	조회	김어드민 admin@test.com	2020. 08. 11. 11:35:26	XX.XX.XXX.XX	PC 웹	검사 - 검사/로그 - 캘린더
구성원 초대	성공	조회	김어드민	2020. 08. 11.	XX.XX.XXX.XX	PC 웹	구성원 - 구성원 초대 - 구

감사에서 지원하는 기능은 다음과 같습니다.

Admin	Admin 관리 페이지에서 수행된 모든 작업 내역 및 수행자를 표시
게시판	게시판에서 사용자가 게시글을 등록하거나 변경, 삭제한 내역을 표시
드라이브	드라이브에서의 파일 작성, 업데이트, 삭제, 공유 등 모든 작업 내역을 표시
캘린더	캘린더에서 수행한 모든 작업 내역을 표시
주소록	구성원의 주소록 정보를 조회한 내역과 수행한 사용자를 표시
할 일	할 일에서 사용자가 생성, 수정, 삭제한 이력을 표시
설문	설문에서 사용자가 새로운 설문을 생성하거나 변경, 삭제한 내역을 표시
화면 공유	화면 공유 참여자 및 대상을 표시
노트	노트에 사용자가 게시글을 등록하고 변경한 내역과 게시판 변경사항을 표시
메일	메일 수신 로그 검색을 통해 기준에 일치하는 메일을 찾고, 세부 정보를 조회하여 문제를 표시
메시지	구성원이 네이버웍스를 통해 주고 받은 메시지를 표시
통화	구성원의 통화 내역을 확인
템플릿	모든 템플릿의 생성, 수정, 삭제한 이력을 표시
Developer Console	Developer Console(개발자 콘솔)에서 이루어진 모든 활동 이력을 표시
로그인	도메인 내의 로그인 성공/실패 이력을 표시
모바일 화면 캡처 (iOS)	iOS 모바일 기기에서 네이버웍스 앱 화면을 캡처한 이력을 확인

# 감사/모니터링

## 메일 수/발신, 드라이브, 메시지 정책 관리 및 모니터링

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

구성원의 메일 수신 및 발신, 드라이브, 메시지 정책을 설정합니다. 특정 조건을 설정하고 필터링하여 구성원의 정보 유출 여부를 파악하고, 사내 컴플라이언스 준수 여부를 확인할 수 있습니다.

메인 > 모니터링 > 메일/발신 > 정책 추가

### 정책 추가

이전으로 돌아가기

제목:

조건 설정

메일 발신:  내부 발신  외부 발신

보낸 사람:  설정

받는 사람:  설정

콘텐츠 필터링:  설정

콘텐츠:

대소문자 구분

URL:

정부 파일:  일반 첨부  다운로드 기판이 있는 파일

수행 내용

수행 내용:

· 메일을 차단하여 수신자에게 메일을 전송하지 않

차단 알림:  설정

알림 설정

알림 사용:

메인 > 모니터링 > 드라이브 > 정책 추가(업로드)

### 정책 추가(업로드)

이전으로 돌아가기

다운로드  업로드  링크 공유

제목:

조건 설정

기본: 콘텐츠 필터링

파질명 + 내용:

구성원 지정:  설정

적용 기간 설정

기간:  -

시간대:

알림 설정

사용자에게 알림:  설정

전달 내용:

수신 방법:  메일 알림  메시지 알림

관리자에게 알림:  설정

메인 > 모니터링 > 메시지 > 정책 추가

### 정책 추가

이전으로 돌아가기

제목:

조건 설정

메시지 전송:  내부 전송  외부 전송

보낸 사람:  설정

받는 사람:  설정

콘텐츠 필터링:  설정

콘텐츠:

정부 파일:  설정

Bot 메시지:

알림 설정

알림 주기:

메일 알림:  설정

주소 추가

메시지 알림:  설정

## 아카이빙

비인가 접속

정보 유출

멀웨어 대응

오발송 방지

분실 및 도난

메일과 메시지의 원본 데이터를 최대 10년간 보관하며 검색 기능을 제공합니다. 원본 데이터를 언제든지 쉽게 검색하고 추출할 수 있기 때문에 효율적인 컴플라이언스 대응을 할 수 있습니다.

The image shows a configuration interface for archiving policies, divided into 'Email Archiving' and 'Message Archiving' sections. The 'Email Archiving' section is active, showing options for archiving scope (All domains, Specific domains, or Not used), retention period (1 year), and a search filter (currently empty). The 'Message Archiving' section is also visible, showing similar options. A tooltip or overlay is present over the 'Message Archiving' section, highlighting its settings. At the bottom, there are two footnotes: one stating that retention periods and specific domains cannot be changed simultaneously, and another stating that policies can be deleted at any time.

메일 아카이빙 | 메시지 아카이빙

아카이빙 정책

아카이빙 범위  전체 도메인  특정 구성원  사용 안 함

보관기간 1년

• 메일을 보낸 시각, 받은 시각을 기준으로 설정한 기간 동안 보관합니다.  
• 보관 처리를 완료하면 알림을 전달해드립니다. 보관할 데이터가 없으면 수일 동안 작업중입니다.

구성원 검색

특정 구성원 정민길 ✖ 김어드민 ✖

메일 아카이빙 | 메시지 아카이빙

아카이빙 정책

아카이빙 범위  전체 도메인  특정 구성원  사용 안 함

보관기간 1년

• 메시지를 보낸 시각, 받은 시각을 기준으로 설정한 기간 동안 보관합니다.

• 보관 기간과 구성원은 동시에 변경할 수 없습니다. 하나의 옵션을 먼저 변경하고 저장해주세요.  
• 정책을 저장하기 전에 언제든지 변경한 내용을 취소할 수 있습니다. 필요한 경우 [취소] 버튼을 눌러 내용을 취소해주세요.

# Appendix.

---

## 네이버웍스 사용 문의

[바로가기](#)



## 네이버웍스 가이드

[바로가기](#)



---

## 모바일 앱 다운로드 \*Android 6.0 이상, iOS 12 이상에서 이용하실 수 있습니다.

 Android



 iOS



---

## 다양한 활용 사례 (공식 블로그)

[바로가기](#)



## 네이버웍스 공식 홈페이지

[바로가기](#)



발행일자 2021년 9월 9일 (Version 1.1) | 이 문서는 NAVER WORKS V3.2을 기준으로 제작되었습니다.

NAVER WORKS는 NAVER (株)의 상표입니다.

이 문서는 ©NAVER Cloud Corp.에 저작권이 있습니다. 저작권자의 허락 없이 서비스 사용 목적 외의 용도로 수정될 수 없습니다.

이 문서의 내용은 ©NAVER Cloud Corp.에 의해 임의로 업데이트될 수 있습니다.

영업 문의 및 기술 지원, 기타 서비스에 대한 정보는 [NAVER WORKS 홈페이지](#)를 참고해 주십시오.