NAVER WORKS

네이버웍스 보안 가이드

라인웍스 (LINE WORKS) 브랜드명이 네이버웍스 (NAVER WORKS)로 변경되었으며, 순차적으로 브랜드 변경 작업이 진행될 예정입니다. 현재 일부 이미지에서는 라인웍스 (LINE WORKS)로 노출되는 점 안내해 드립니다.

기업 정보를 가장 안전한 네이버웍스에 보관하세요

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

1. 글로벌 최고 수준의 보안 서비스

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

2. 데이터 보관 및 관리

사용자의 데이터는 완벽한 논리적·물리적 접근 통제를 통해 안전하게 보관 및 관리됩니다.

3. 개인 정보 보호 및 관리

사용자의 개인 정보는 국제 표준 규격 및 법률을 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

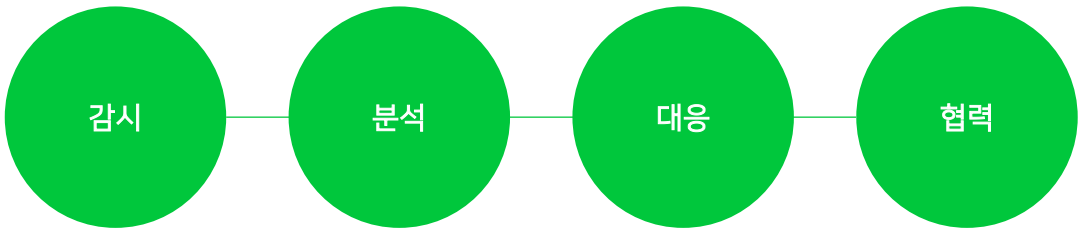
데이터센터 물리 보안

네이버웍스의 데이터는 논리/물리적 접근통제를 통해 안전하게 보관 및 관리되고 있습니다. 데이터가 보관되어 있는 데이터센터는 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 데이터센터 출입이 허용되며, 인증된 직원 외에는 데이터센터 출입이 일체 불가합니다. 비인가 접속 및 자료 반입을 차단 및 감사하고 있고, 데이터베이스 접속은 추가 인증을 통과한 직원만 접근이 가능합니다. 데이터베이스의 모든 접속 및 다운로드는 로그가 자동으로 생성되고 감사됩니다.

서비스 운영 보안

서비스 인프라는 다른 일반 소비자 전용 서비스와 분리된 환경에서 운영됩니다. 네이버웍스의 시스템/보안 전문가 팀이 24시간 365일 면밀하게 시스템을 모니터링하며 고객의 데이터를 안전하게 지키고 있습니다. 실시간 멀웨어/바이러스 감지 외에 최신 스팸 필터링, DoS, DDoS 공격을 지속 감시합니다. 보안 리스크가 발견된 경우에는 리스크를 바로 분석 및 대응하고, 재발 방지를 위해 관련 기관들과 정보를 공유하고 신속하게 협력하고 있습니다.



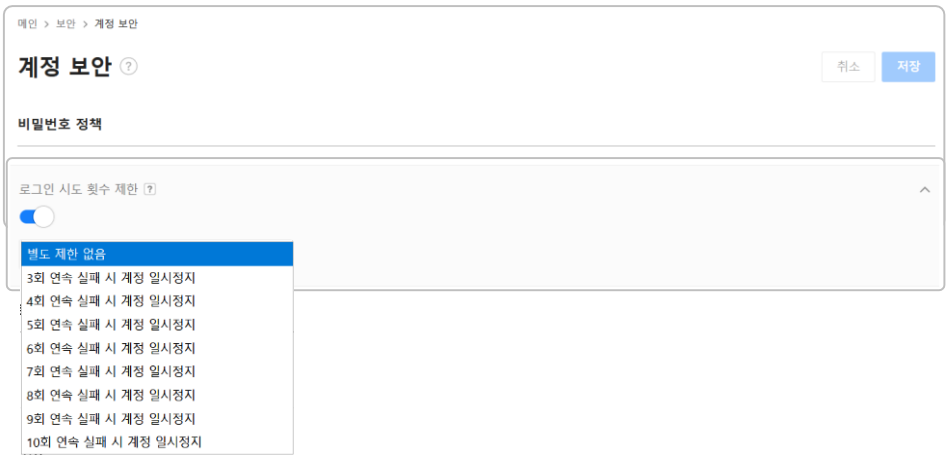
OWASP(The Open Web Application Security Project) 상위 항목을 참고하여 정기적으로 취약점 점검을 수행하고 있습니다. 서비스 보안검수, 정기적인 보안진단 및 모의 해킹을 통하여 다각도로 보안성 강화를 위해 노력합니다.

계정 보안

계정 접속 보안

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

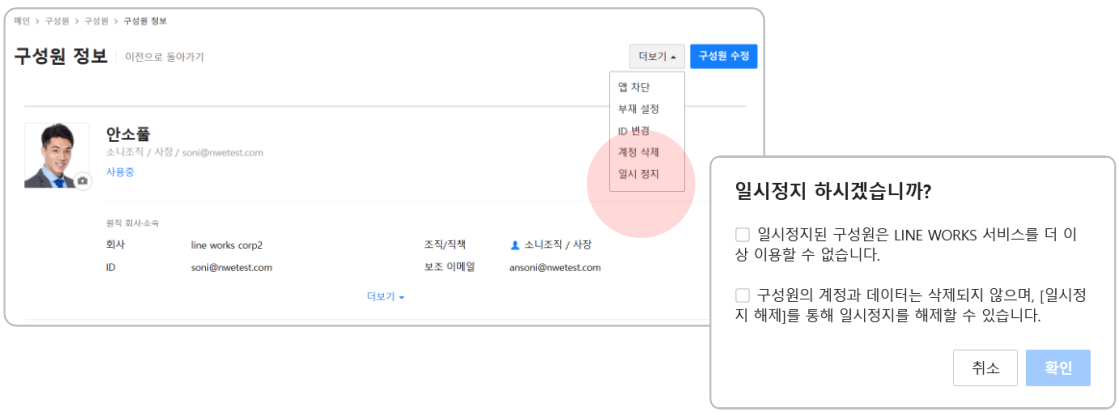
네이버웍스는 특정 계정으로 비정상 로그인 시도가 발생하면 해당 계정을 자동으로 차단하여 고객 계정을 안전하게 보호합니다. 이와 함께 관리자는 계정이 특정 횟수 이상 로그인 실패 시, 계정이 일시정지 되도록 설정할 수 있습니다.



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.



계정 보안

비밀번호 정책 설정

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

고객사 보안 정책에 따라 각 구성원이 네이버웍스 서비스에 로그인할 때 비밀번호 난이도와 만료일을 설정할 수 있습니다.

비밀번호 난이도	• 영문과 숫자 조합 • 영문, 숫자, 특수문자 혼합
비밀번호 최소길이	8~20자
비밀번호 만료일	30일 ~ 1년, 무제한
최근 사용한 비밀번호 재사용 제한	• 별도 제한 없음 • 최근 비밀번호 1~5개까지 사용 불가

구성원의 비밀번호 변경

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

비밀번호 변경 방법

비밀번호 변경 구성원에게 비밀번호 변경을 요청합니다.

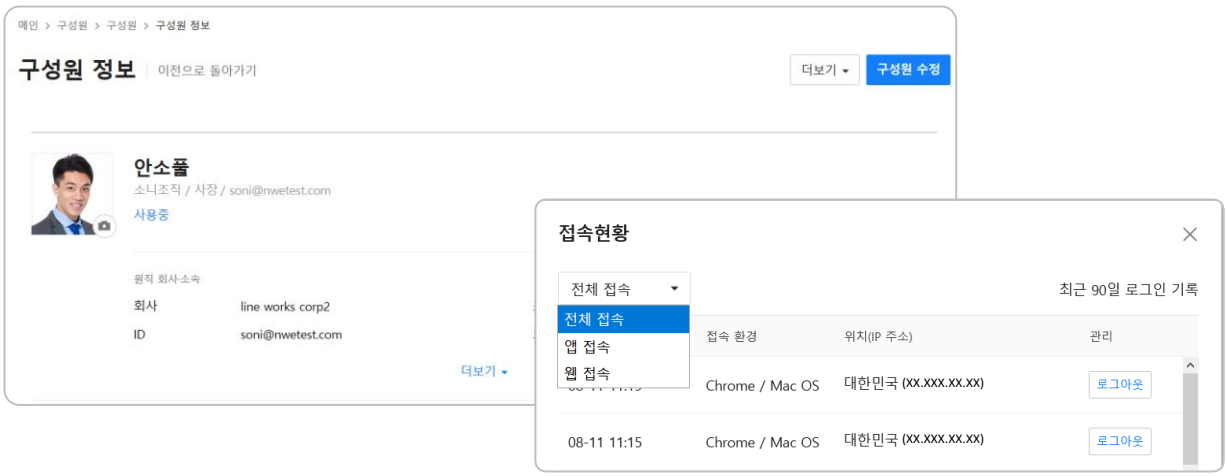
비밀번호 강제 변경 구성원의 비밀번호를 강제로 변경합니다.

계정 보안

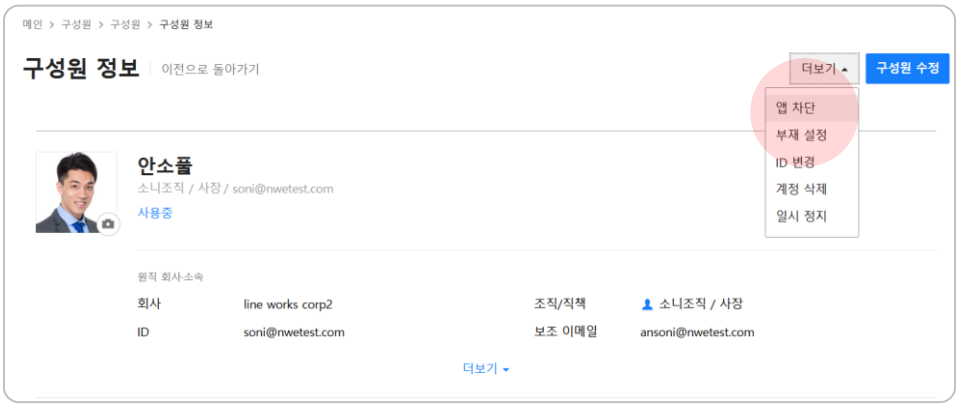
접속 현황 확인과 강제 로그아웃

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 쉐도우 IT 모니터링에 효과적입니다.



디바이스 분실 등으로 구성원의 앱 접속만을 차단하는 경우에는 '앱 차단' 기능을 활용해 PC/모바일앱 접속만 차단 가능합니다.



계정 보안

원격 장치 접속 관리 (MDM)

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

※ 이외에 외부 MDM을 연동하여 구성원의 iOS 및 Android 디바이스 사용을 관리할 수 있습니다.

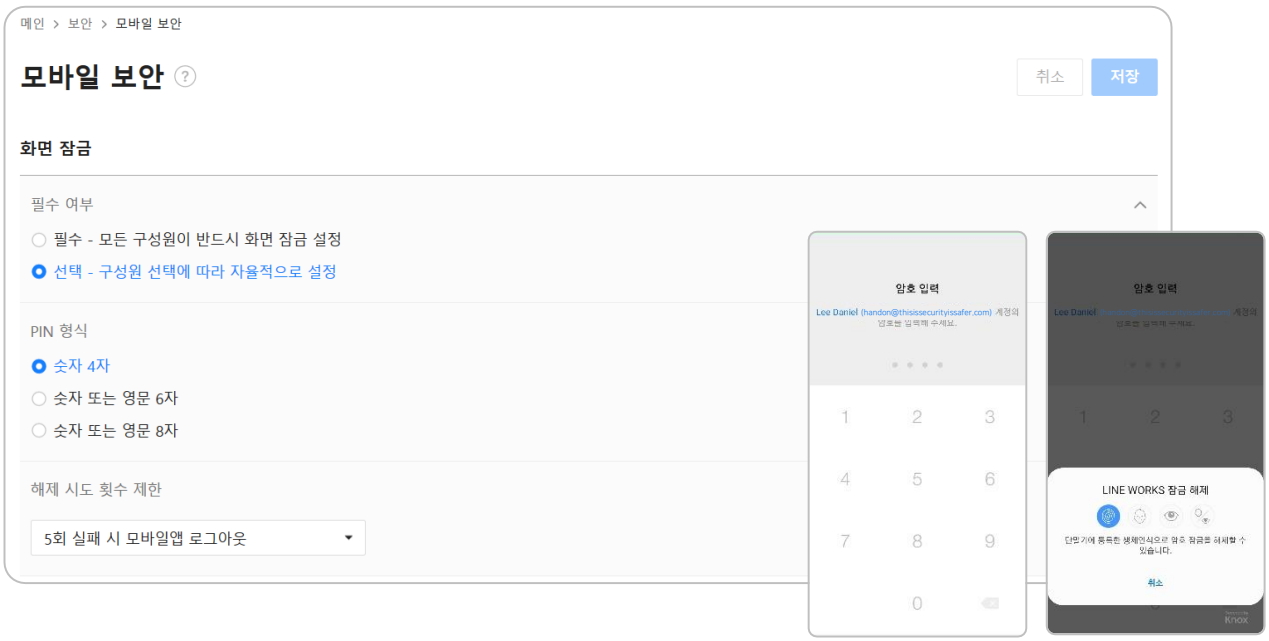
모바일 보안

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 이외에 제3자에 의한 모바일앱 사용을 방지 할 수 있습니다. '필수 여부'를 선택하여 구성원 자율에 맡길지 선택할 수 있습니다.



데이터 저장 기간

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

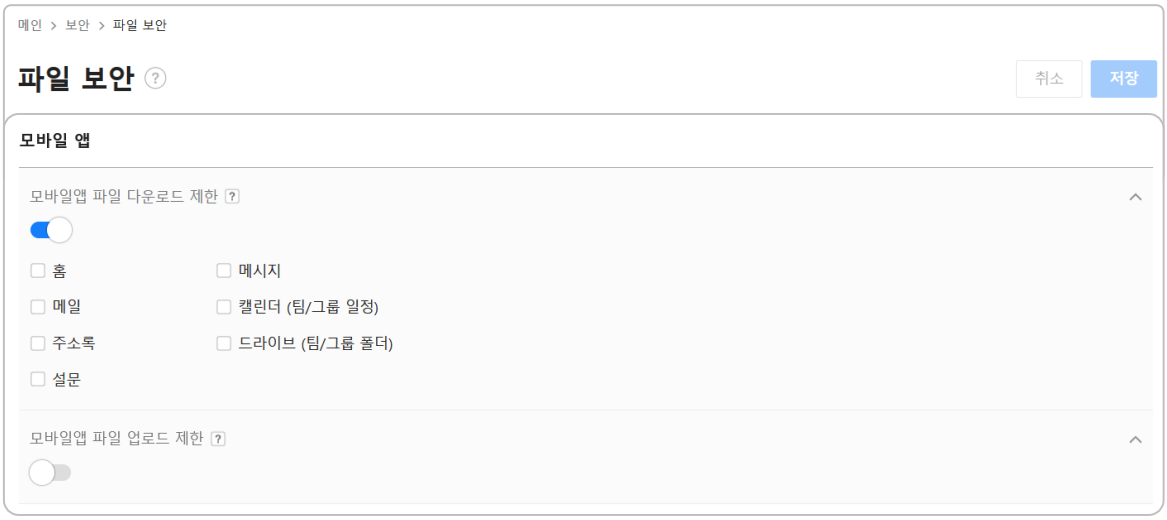
모바일 디바이스에서 각 서비스의 데이터를 볼 수 있는 기간을 설정합니다.
기간 외의 캐시 데이터는 자동으로 삭제되기 때문에 데이터 관리의 안전성이 향상됩니다.

모바일 보안

파일 다운로드/업로드 제한

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

모바일 디바이스에 저장되어 있는 파일의 다운로드/업로드를 제한하여 악성코드 등 악의적인 파일/데이터의 확산 위험을 줄일 수 있습니다.



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.

메일 보안

바이러스 및 스팸 메일 차단

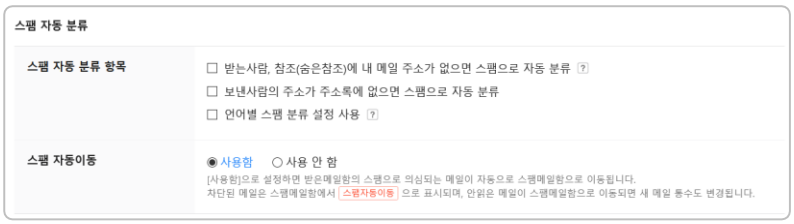
사용자 설정

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 노력하고 있습니다. 스팸 메일을 받은 경우 구성원은 메일을 쉽게 삭제하고 수신 차단할 수 있습니다.

1. '스팸메일 신고하기' 기능

2. '스팸자동 분류' 기능



3. 수신 허용/차단 목록 관리

메일 보안

외부 메일의 이미지/링크 차단

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

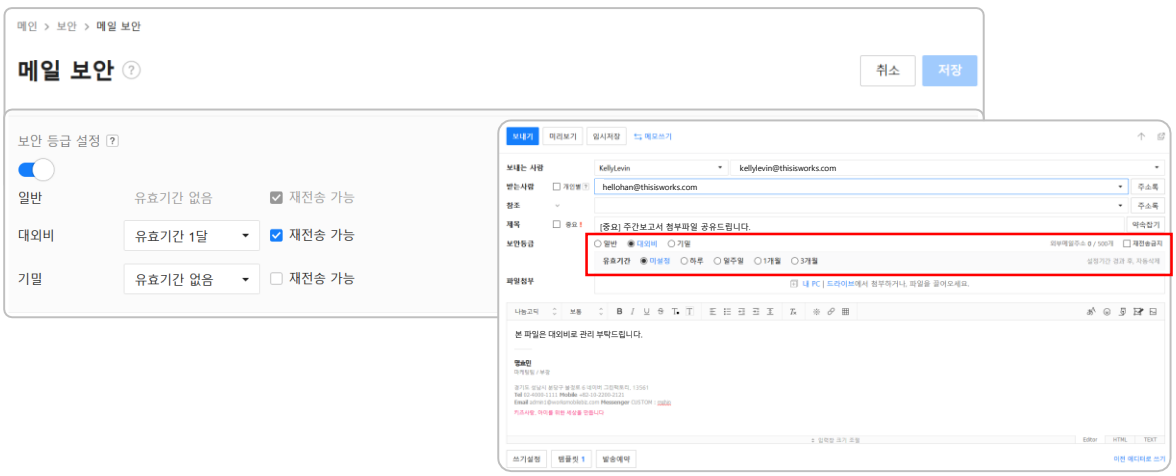
수신 메일에 이미지 및 링크가 포함된 경우, 메일 확인 시 정보가 직접 표시되지 않도록 제한할 수 있습니다. 스팸 및 악의적인 메일을 열어도 첨부 파일, 링크 접속으로 인한 보안 위험을 줄일 수 있습니다.

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 유효기간을 설정할 수 있습니다. 시간이 경과되면 자동으로 메일이 삭제되기 때문에 중요한 정보를 안전하게 보호할 수 있습니다.



메일 보안

위험 메일 경고

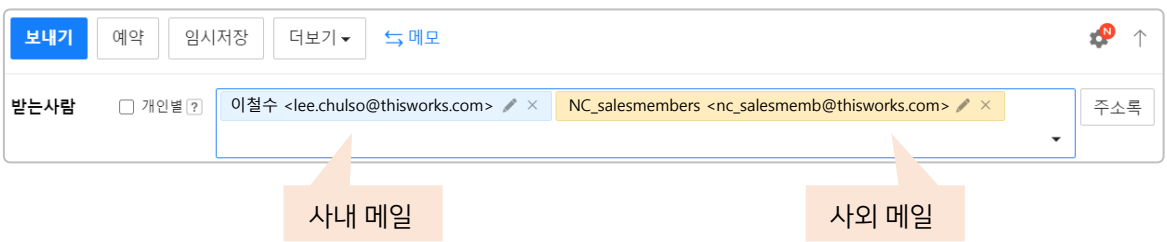
비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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.

메일 주소 구분

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

메일을 작성할 때 '받는사람' (참조, 숨은참조 포함)란에 입력하는 '사내 구성원' 과 '외부 메일 주소' 가 각각 다르게 표시됩니다. 사내와 사외 메일 주소를 색상으로 구분할 수 있어, 외부로 메일을 잘못 발송해 정보 유출이 발생하는 리스크를 줄일 수 있습니다.



메일 보안

메일 인증(DKIM)

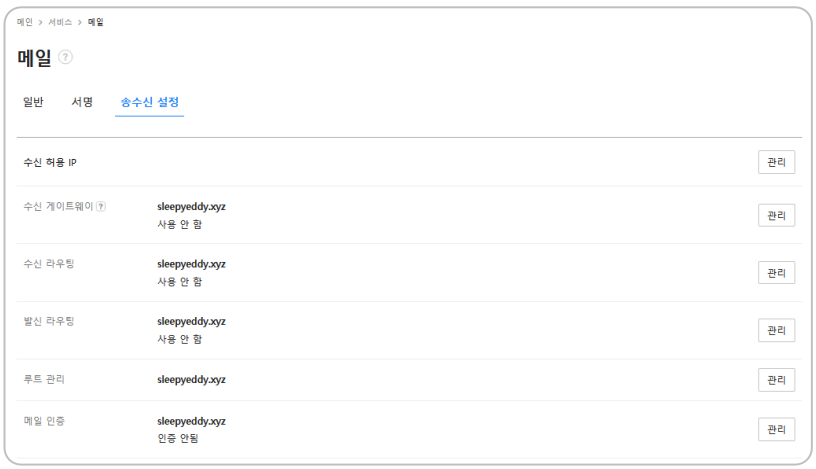
비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

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 메뉴에서 설정하여 사용할 수 있습니다.



메일 보안

대기 발송

사용자 설정

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

메일 '보내기'를 클릭 후 실제로 메일이 발송 될 때까지의 시간을 설정할 수 있습니다. 메일 발송 후 중요 정보가 포함된 것을 발견하면 대기 발송 설정 시간 내에 메일 발송을 취소하여 정보 유출을 방지 할 수 있습니다.

미리보기

사용자 설정

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

기타 보안 기능

파일 보안

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

메시지/노트/홈/메일/캘린더/드라이브/설문에서 사용하는 파일 확장자를 제한할 수 있습니다.
확장자 제한이 가능하기 때문에 악성 코드 확산, 악성 프로그램을 포함한 실행 파일의 전송을 차단하고 보안 리스크를 줄일 수 있습니다.
(본 기능과 관계 없이 바이러스 검사는 모든 서비스에서 기본으로 진행됩니다.)

외부 사용자와의 대화방에서 파일 전송 첨부 제한

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

기타 보안 기능

기기 현황

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

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

접속 IP 제한

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

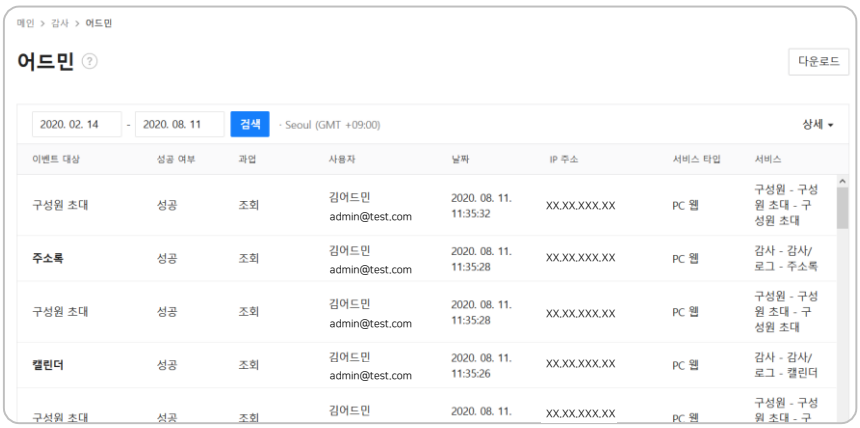
PC앱, PC웹을 통한 네이버웍스 서비스 및 드라이브 탐색기 접속을 특정 IP 주소로 제한합니다.
외부 디바이스를 통한 서비스 접속을 제한함으로써 제3자에 의한 악의적인 사용 차단 등 보안 위험을 줄일 수 있습니다. (모바일 앱 접속은 제한되지 않습니다.)

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 관리와 잘못된 사용을 방지할 수 있습니다.



'감사' 는 아래의 기능을 지원합니다.

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

감사/모니터링

메일 수/발신, 드라이브, 메시지 정책 관리 및 모니터링

비인가 접속 | 정보 유출 | 멀웨어 대응 | 오발송 방지 | 분실 및 도난

구성원의 메일 수/발신, 드라이브, 메시지 정책을 설정하고 특정 조건을 설정하고 필터링하여 구성원의 정보 유출 여부를 파악하고, 사내 컴플라이언스 준수 여부 확인이 가능합니다.

감사/모니터링

아카이빙

비인가 접속 | **정보 유출** | 멀웨어 대응 | 오발송 방지 | **분실 및 도난**

메일과 메시지의 원본 데이터를 최대 10년 간 보관 및 검색을 제공합니다. 원본 데이터를 언제든지 쉽게 검색하고 추출하여 효율적인 컴플라이언스 대응을 할 수 있습니다.

Appendix.

네이버웍스 사용 문의

바로가기

네이버웍스 가이드

바로가기

모바일 앱 다운로드 *Android 5.0 이상, iOS 11 이상에서 이용하실 수 있습니다.

Android

iOS

다양한 활용 사례 (공식 블로그)

바로가기

네이버웍스 공식 홈페이지

바로가기

발행일자 2020년 10월 15일 (Version 1.0) | 이 문서는 NAVER WORKS V2.9을 기준으로 제작되었습니다.

영업 문의 및 기술 지원, 기타 서비스에 대한 정보는 NAVER WORKS 홈페이지를 참고해 주십시오.