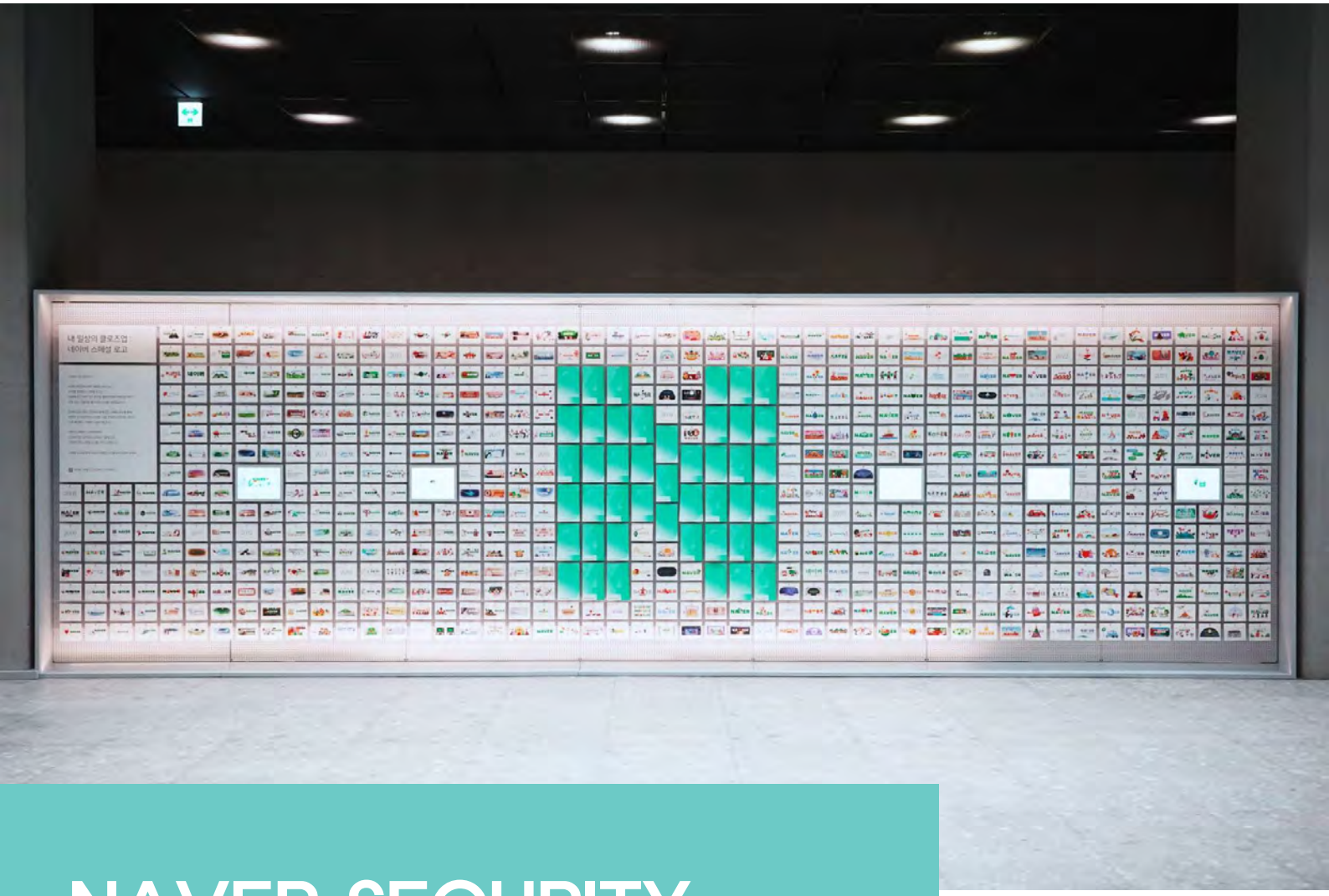
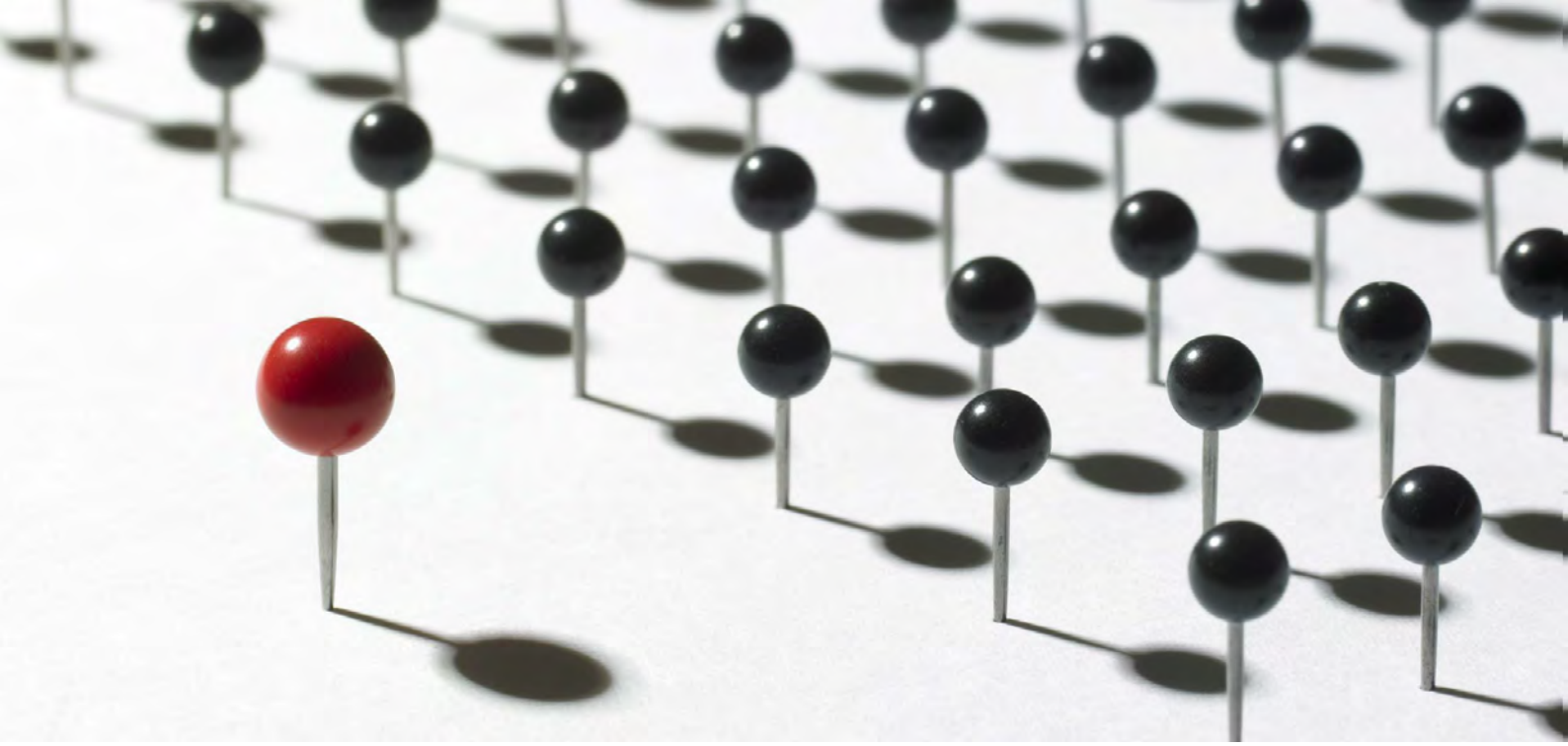


# NAVER SECURITY WHITE PAPER 2024

Last updated : 2025.02

# TABLE OF CONTENTS



# 1

# CISO 인사말


디지털 환경이 급변하고, 사이버 위협이 나날이 정교해지는 가운데, 정보보호는 기업의 지속 가능성과 신뢰를 결정짓는 필수 요소가 되었습니다. 이에 NAVER는 **정보보호가 기업 경쟁력의 핵심이라는 인식을 바탕으로, 선제적인 보안 정책을 수립**하고 **고도화된 보안 기술을 적용**하며, **다양한 보안 위협에 대한 대응** 역량을 지속적으로 강화해왔습니다.

NAVER는 '24년에 외부 위협 탐지 솔루션 운영 개시를 시작으로, 민감 정보 노출 대응, 검색 엔진 기반 피싱 유포 확산 방지 등 다방면의 보안 활동을 수행해왔습니다. 또한, 컨테이너 보안 플랫폼을 통합하고, 개인정보 노출 포인트 점검을 강화하는 등 정보보호 인프라와 서비스 대응역량을 지속적으로 발전시켜 왔습니다. 특히, AI 및 대규모 언어 모델(LLM) 기반 서비스의 보안 가이드를 마련하여 신기술을 안전하게 도입하기 위한 노력을 기울이는 등 **서비스의 안정성과 비즈니스의 편의성을 보장하는 보안 전략**을 지속적으로 실현하고 있습니다.

NAVER는 정보보호 분야에서 업계를 선도하는 기업으로서, 보다 강력한 보안 체계를 구축하고 글로벌 보안 표준을 준수하는 데 최선을 다하고 있습니다. 본 백서는 지난 1년간 저희가 수행한 정보보호 활동과 주요 성과를 정리한 결과물로, 이를 통해 보안 환경의 변화를 면밀히 분석하고 보다 안전한 디지털 생태계를 조성하기 위한 전략적 방향을 제시하고자 합니다.
또한, 본 백서가 업계 관계자 및 보안 전문가들에게 가치 있는 인사이트를 제공하고, 기업 보안의 중요성에 대한 공감대를 형성하는 데 기여하기를 바랍니다.

**앞으로도 NAVER는 고객의 신뢰를 최우선으로 삼고, 사이버 보안 위협을 선제적으로 대응하며, 보다 안전한 디지털 미래를 만들어가기 위해 끊임없이 노력하겠습니다.**

이 백서가 정보보호에 관심을 가지신 모든 분들께 유익한 자료가 되기를 바라며, NAVER 정보보호 조직의 향후 행보와 활동에 대해 지속적인 관심과 성원을 부탁드립니다.

감사합니다.

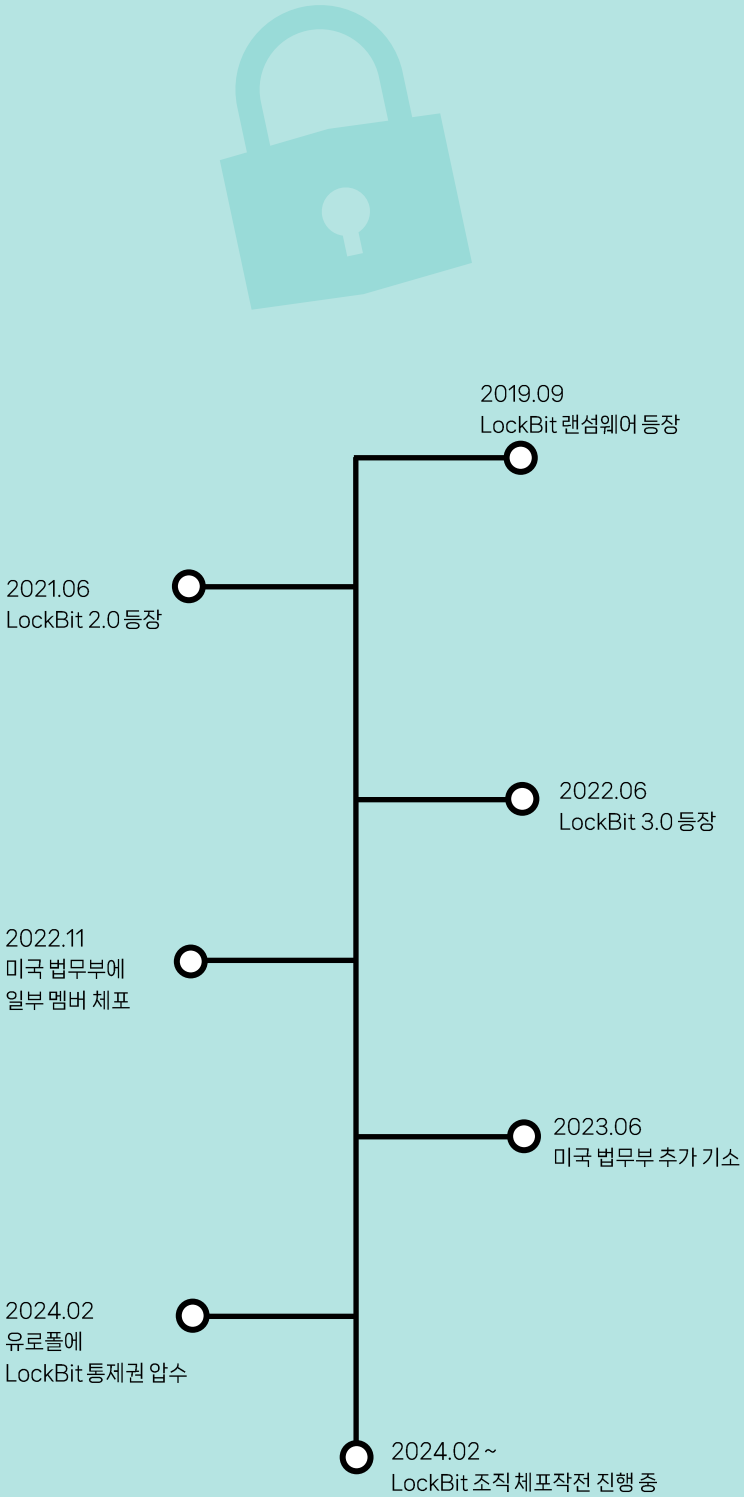
**NAVER CISO/CPO**

이진규

# 2

## 24년 국내/외 주요 보안 이슈

2024년 국내/외에서 발생한 주요 이슈들을 되돌아보며 대비해야 할 부분에 대해서 이야기해보려고 합니다.




## 2월 – LockBit 랜섬웨어 조직 검거

2019년 9월 최초 등장한 **LockBit 공격 그룹**은 **랜섬웨어를 대량으로 유포하여 수익을 얻는 사이버 범죄 집단**으로, 전 세계에서 가장 많은 **랜섬웨어**를 유포하여 미국에서만 약 9,100만 달러의 피해 금액을 발생시켰습니다.
랜섬웨어에 감염될 경우 저장된 파일이 모두 암호화되며, 공격자로부터 해독키에 대한 몸값을 요구받게 됩니다. 만약, 피해자가 협상에 응하지 않는 경우에는 중요 정보를 외부에 유출하여 2차 피해를 발생시키기도 합니다.

LockBit은 네트워크를 통해 패치되지 않은 **제로데이(0-Day) 취약점**을 이용하여 랜섬웨어를 유포하는 방식을 사용했습니다. 한 대의 PC가 최초 감염되면, 내부 네트워크에 있는 다른 취약한 PC를 자동으로 스캔하여 추가 감염을 시도하는 등의 자체 확산 기능이 존재합니다.
국내에서는 사칭 및 피싱 메일, 악성 파일 업로드 등을 통해 유포된 사례가 다수 발견되기도 했습니다.

LockBit 2.0 버전이 출시되면서 영국 자동차 회사를 공격하여 6,000만 달러를 요구하거나, 세계 각국의 정부 기관을 공격하는 등의 본격적인 대규모 감염사태가 발생하였습니다. 이후 기술적으로 더 발전한 3.0 버전이 출시되면서 훨씬 많은 피해가 발생하였고, LockBit을 잡기 위해서 유럽 정부기관들이 공조를 시작했습니다.

2024년 2월, 영국의 국가범죄수사국(NCA) 및 유로폴은 LockBit의 시스템 통제권을 장악하는 데 성공했으며 이를 바탕으로 공격자들을 체포하기 시작했습니다. 관계자들이 체포되면서 수년간 활동한 LockBit 공격 그룹의 30,000개의 암호화폐 지갑에서 2,200개의 비트코인이 발견되었습니다.

현재 "No More Ransom"사이트에서 LockBit의 시스템에서 확보한 LockBit의 해독키를 이용한 복구 툴을 무료로 배포하고 있습니다.

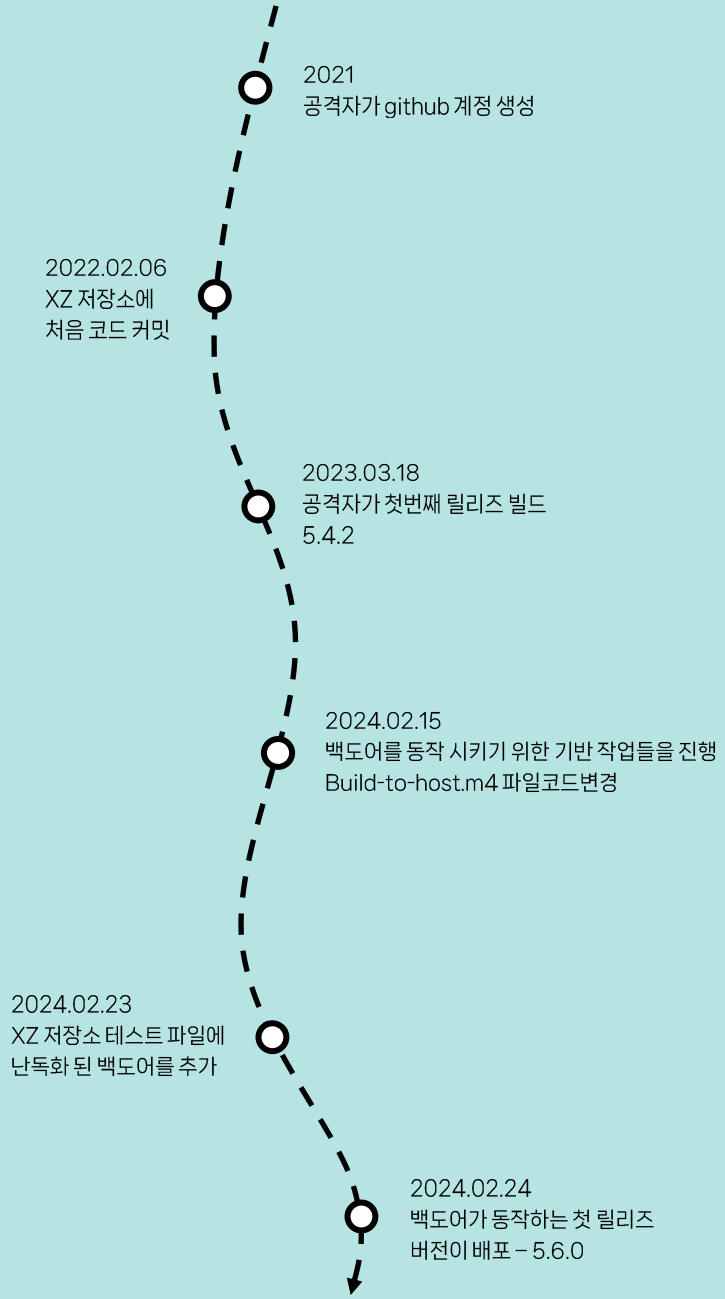
이러한 악성코드로부터 안전하기 위해서는 **의심스러운 메일 열람을 자제**하고, **불분명한 출처의 파일을 실행하지 않도록 하는 것**이 가장 중요합니다.

## 4월 – XZ Utils Backdoor

지난해 4월, XZ Utils의 5.6.0과 5.6.1 버전에서 백도어가 발견되는 사건이 있었습니다. XZ Utils는 리눅스와 GNU 운영체제에서 널리 사용되는 데이터 압축 프로그램입니다. 기존에 gzip, bzip2 보다 더 높은 압축률을 보여주고, CLI 기반으로 쉽게 접근이 가능하다는 장점이 있어 tar 파일 압축, 리눅스 배포 시 많이 사용되는 압축 프로그램입니다.

이번 이슈는 **공격자가 2021년부터 4년 동안 GitHub에서 XZ 개발자와 신뢰를 쌓아 XZ 프로젝트의 공식 참여자**로 인정받은 후, 악성코드를 삽입한 **공급망 공격**의 사례로 주목받았습니다. 이러한 방식은 소프트웨어 개발 과정에 침투하여 사용자들에게 배포되기 때문에 더욱 위험합니다.

다행히 해당 이슈는 PostgreSQL 개발자에 의해 빠르게 발견되었고, 저장소를 복구하고 백도어가 제거된 안전한 버전이 배포되었습니다.
이 사건은 **소프트웨어를 신뢰할 수 있는 경로에서 다운로드**하고, **무결성을 검증**하며, **정기적으로 업데이트하는 것**이 얼마나 중요한지를 강조합니다.



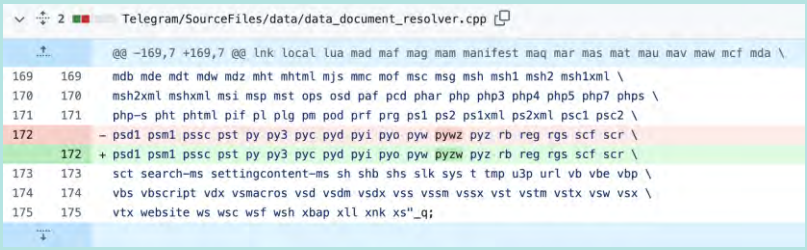
## 4월 – Telegram 치명적 취약점

Telegram은 강력한 익명성과 보안 기능으로 전 세계에서 많이 쓰이는 메신저 플랫폼 중 하나입니다.

2024년 4월, 보안업체 CertiK는 X(구 트위터)를 통해 Telegram 메신저의 **원격 명령 실행 취약점(Remote Code Execution)**이 담긴 동영상을 업로드했습니다. 영상 속 취약점은 Windows 환경의 Telegram 소프트웨어에서 발견되었으며, **공격자가 보낸 채팅을 피해자가 읽은 직후 임의의 명령이 실행**되는 내용이 담겨있습니다.

Telegram 측은 사실무근으로 대응하였지만, 익일 해킹 포럼을 통해 해당 취약점에 대한 공격코드(PoC)가 공개되었습니다.
취약점은 Telegram에 정의된 실행파일 확장자 목록에 **.pyzw 확장자를 .pywz 로 잘못 기입한 실수로 인해 발생**하였습니다.
그 결과, 실행 가능한 확장자인 .pyzw 파일에 대한 보안 경고 창이 누락되었고, 공격자가 보낸 악성 실행파일이 피해자 PC에서 경고 없이 실행되게 되었습니다.

이후 Telegram 측에서는 오타를 수정하여 빠르게 취약점을 패치 했지만, 매우 강력한 보안을 자랑하는 메신저임에도 **개발자의 단순한 오타 하나가 치명적인 취약점으로 이어질 수 있다는 사례**를 남기게 되었습니다.

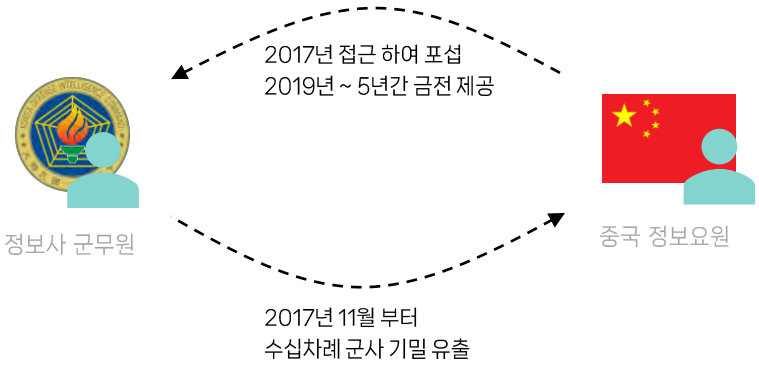


## 6월 – 정보사 군무원 기밀정보 유출

2024년 6월 중순, 대한민국 정보기관이 북한 당국의 서버를 침투하는 과정에서 정보사령부 소속 정보작전요원 명단이 발견되었습니다.

이후 방첩사에서 관련 수사를 진행하던 중, 군무원 A씨의 개인 노트북에서 정보작전요원 명단이 추가로 확인되었습니다.
7월 30일, 국방부 중앙군사법원은 군무원 A씨에 대해 구속영장을 발부했으며 조사 결과 A씨는 2017년 4월부터 약 7년간 **중국 정보원에게 국가기밀을 지속적으로 유출**한 사실이 드러났습니다.
더불어, 정보사령부가 지난 7년 동안 외부 감사를 받지 않았다는 사실 또한 밝혀지면서 조직 내 보안 관리 체계의 허점이 드러났습니다.

이 사건은 내부 관계자 **보안 인식 교육의 강화와, 정기적이고 철저한 보안 감사의 필요성**을 보여주는 사례입니다.
유사 사고를 예방하고, 기밀정보와 내부 자료를 보호할 수 있도록 **지속적이고 체계적인 보안 점검이 필요**합니다.




## 7월 – 암호화폐 거래소 해킹

2024년 7월, 인도의 주요 암호화폐 거래소 중 하나인 WazirX는 심각한 해킹 사고를 겪었습니다. 해커들은 **다중 서명 지갑(Multi-Signature Wallet)**을 대상으로 정교한 공격을 통해, 거래소 자산의 약 50%에 해당하는 **2억 3천만 달러 상당의 암호화폐를 탈취**했습니다.

이 과정에서 해커들은 트랜잭션 승인에 필요한 다수의 서명을 확보하여, **거래소 소유 지갑에서 암호화폐를 가져가는 데 성공**했습니다.
탈취된 자산은 주로 테더(USDT), 페페(PEPE), 갈라(GALA) 등의 암호화폐로 구성되어 있었으며, 해커들은 이를 세탁하기 위해 **암호화폐 믹싱 서비스인 토네이도 캐시(Tornado Cash)를 사용하여 이더리움(ETH)으로 전환**했습니다. 암호화폐 믹싱 서비스는 자산의 출처를 숨기기 위해 여러 트랜잭션을 섞어 자금 흐름을 익명화하는 데 사용됩니다.


WazirX 측은 탈취된 암호화폐를 회수하기 위해 현상금 프로그램 등 다양한 조치를 취했으나, 해커는 지속적으로 자금을 세탁하며 자산의 상당 부분을 성공적으로 은닉한 것으로 보입니다.

암호화폐 시장이 성장함에 따라, 공격자들이 해킹을 통해 얻을 수 있는 경제적 이득이 커지고 있습니다. 이에 따라 **암호화폐 거래소를 포함한 시장 전반을 겨냥한 사이버 위협이 점차 증가할 것으로 전망**됩니다.

## 7월 – CrowdStrike Update Crash

크라우드 스트라이크는 2011년에 설립된 미국 기업이며, 세계 2위 규모의 사이버 보안 기업입니다.

2024년 7월, 마이크로소프트 윈도우에서 실행되는 크라우드 스트라이크의 **EDR 보안 소프트웨어인 팰컨 센서의 오류로 인해 전 세계적으로 전산망 마비**와 서비스 장애가 발생하는 사태가 있었습니다.
**해당 패치는 MS 윈도우 호스트에 자동으로 설치**되었으며, 이 과정에서 오류가 발생해 다수의 PC에서 블루스크린 현상이 나타났습니다.

문제를 인지한 크라우드 스트라이크는 1시간 37분 만에 긴급 콜백 조치를 취했으나, 이미 **약 850만 대의 PC에서 장애가 발생**했던 것으로 추정됩니다.

크라우드 스트라이크는 이번 사건이 보안 사고나 사이버 공격이 아니라는 점을 강조하며 공식 입장을 발표했습니다.
크라우드 스트라이크는 IT 산업에서 높은 신뢰를 받아온 기업이었지만 이번 사건을 통해서 신뢰도가 높은 기업이라 할지라도 패치 과정에서 예상치 못한 문제를 완전히 방지할 수는 없음을 보여줍니다.

이러한 사례는 **소프트웨어 업데이트 및 패치 관리**를 사전에 시험하고 배포하는 과정을 강조하며, 철저한 **사전 테스트와 비상 대응 체계의 필요성**을 다시 한번 상기시킵니다

# 3

## 팀 네이버 주요 보안 이슈

국내/외 이슈들 이외 팀 네이버 내부에는 어떤 이슈들이 있었는지 이번 섹션을 통해서 살펴보려고 합니다.

# 2024

01
- ✓ 사내 취약점 탐지 자동화

02

03
- ✓ 검색 엔진 기반 피싱 유포 사례 대응

04
- ✓ 사내 DevSecOps 툴 필수 설치 가이드

05
- ✓ 서버 외부 오픈 시 보안성 검토 프로세스 강화

06

07
- ✓ 신규 버그바운티 프로그램 런칭

08
- ✓ 개인정보 노출 포인트 점검

09

10

11
- ✓ LLM 기반 애플리케이션 구축을 위한 개발 보안 가이드
- ✓ 중고나라 이용 시, 피싱 피해 예방을 위한 캠페인 진행

12

## 1월

### 사내 취약점 탐지 자동화

사내 취약점 탐지 자동화를 위해 탐지 스캐너 개발을 진행 하였고, 반복해서 발생하는 이슈에 대해서 취약점 스캔을 진행했습니다.
**다량의 신규 위협을 탐지하고 대응을 진행**해 네이버 서비스가 더욱 안전해질 수 있도록 하였습니다.

## 3월

### 검색 엔진 기반 피싱 유포 사례 대응

네이버 이용자의 피싱 피해 사례가 증가함에 따라서 피해를 줄이기 위한 목적으로
Naver Security 블로그에 **검색 기반 피싱 주의 공지와 함께 대응 방안에 대한 정보 제공 글을 작성**해 공유 하였습니다.
> 보러가기

## 4월

### 사내 DevSecOps 툴 필수 설치 가이드

네이버 서비스의 보안성 강화를 위해서 자체 개발한 **DevSecOps 툴 적용을 전사 확대** 진행하였습니다.
해당 툴은 **NShiftKey라는 이름으로 github 마켓을 통해서 외부에 공유**되기도 했습니다.
각 서비스 담당자 분들은 사내 DevSecOps 툴에서 탐지한 취약점들을 참고하여 취약점을 제거하는 등 필요한 조치를 직접 수행할 수 있게 되었습니다.
> NShiftKey

## 5월

### 서버 외부 오픈 시 보안성 검토 프로세스 강화

기본적으로 네이버는 외부 서비스를 위한 외부 오픈 시 보안 검토를 거치도록 프로세스화 하고 있습니다.
다만 일부 보안 검토를 거치지 않고 서버를 외부 오픈할 수 있는 프로세스가 발견되어 개선안을 통해서 외부 오픈 요청 시, **오픈 대상의 보안성 검토를 필수로 포함하는 것으로 강화** 하였습니다.

## 7월

### 버그바운티 신규 플랫폼 오픈

네이버는 2019년부터 자체적으로 버그바운티 프로그램을 운영해오고 있습니다.
제보자분들의 편의성 증대, 개인정보관리 강화 및 회원 체계 통일을 위해 기존 운영해오던 플랫폼을 대체하여 **7월 15일 신규 버그바운티 플랫폼을 오픈** 했습니다.
> 버그바운티 참여

## 8월

### 개인정보 노출 포인트 점검

국내 개인정보 노출 사례가 지속적으로 발생하고 이슈화 됨에 따라 **네이버 서비스의 유사 포인트에 대해서 기술적 점검 계획을 수립하고, 서비스 대상으로 한번 더 점검을 진행**했습니다.
네이버는 이처럼 서비스의 보안성 강화 및 외부 이슈에 민감하게 대응하여 **고객의 정보가 안전하게 보호될 수 있도록 관리**하고 있습니다.

## 11월

### LLM 기반 애플리케이션 구축 개발 보안 가이드 배포

AI 기술들이 서비스에 활용되는 상황이 증가함에 따라 LLM을 이용하여 서비스를 구축할 때 **보안 관점에서 고려해야 할 요소를 가이드**로 작성하고, 네이버 전사에 공개했습니다.
Prompt Injection 부터, 최신 RAG를 사용하는 케이스를 모두 고려하여 **9가지 주제로 작성**해 내부 서비스 개발 시 참고할 수 있도록 하였습니다.

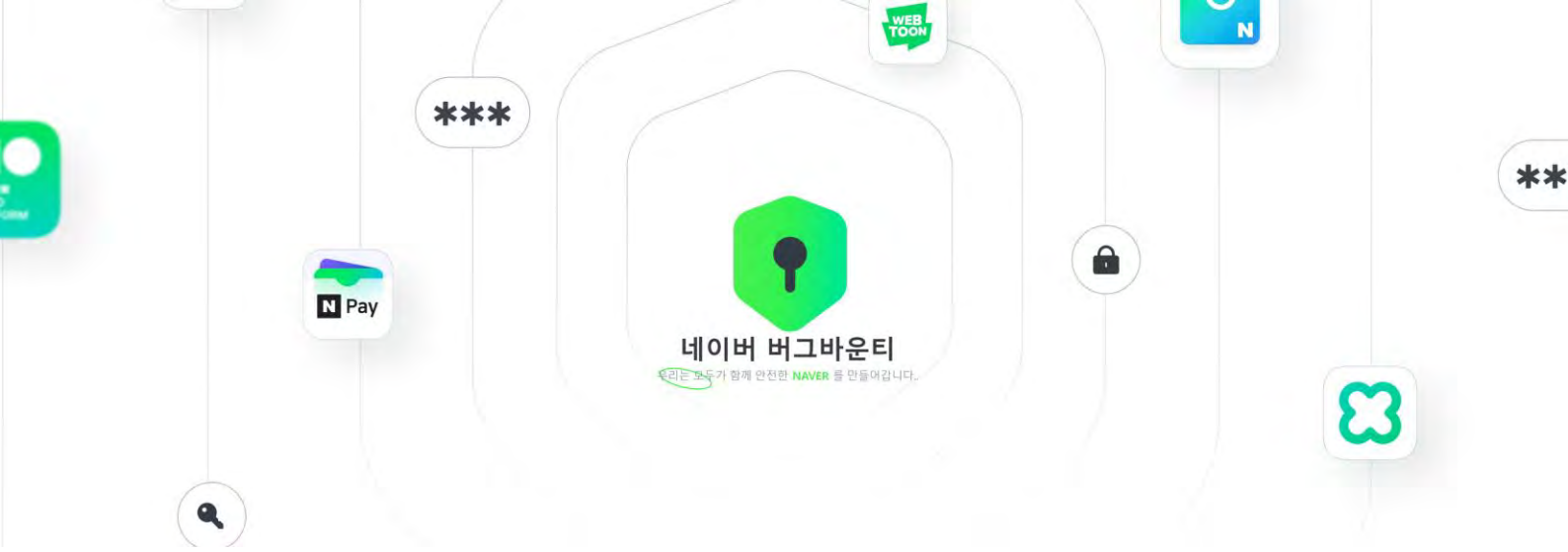
### 중고나라 이용 시, 피싱 피해 예방을 위한 캠페인 진행

이용자가 **피싱임을 인지할 수 있도록 중고 거래의 각 과정을 단계별로 나누어 정리**해 네이버 **시큐리티 블로그에 게재**하였습니다. 이외에도 **카페 서비스, 그린 인터넷 블로그, 고객센터에 함께 공지**하여 이용자 노출 빈도를 높였습니다.
> 보러가기

# 4

## 버그바운티와 보안 통계

네이버 버그바운티 프로그램의 성과를
살펴보고, 내부에서는 얼마나 많은 보안
위협들이 완화되었는지 알아보려고 합니다.




## Bug Bounty Program

버그바운티 프로그램은 소프트웨어 또는 서비스의 취약점을 찾아내고 이를 제보하는 사람에게 기업이 포상금을 지급하는 프로그램입니다.

네이버는 **2015년부터** 한국인터넷진흥원 **(KISA)과 공동으로 버그바운티 프로그램을 운영**하기 시작했으며, **2019년 9월부터는 자사 버그바운티 프로그램을 독립적으로 운영**하고 있습니다.

외부 보안 전문가의 눈으로 네이버 서비스의 취약점을 점검할 수 있어 네이버 서비스가 더 안전하고 투명하게 관리될 수 있습니다.

**2024년 한 해에는 총 296건의 서비스 보안 위협** 포인트가 외부 보안 전문가에 의해 제보 되었고, 그중 실제 약 **128건이 네이버 서비스에 영향이 있는 것으로 확인**하여 개발팀과 협의해 수정을 진행하였습니다.

외부 보안 전문가 **132명이 프로그램에 참여**해 주셨고, **지급된 리워드는 총 $58,960** 입니다.

네이버는 웹 서비스에 대한 버그바운티 프로그램 뿐 아니라 웨일 브라우저에 대한 버그바운티 프로그램도 함께 운영해오고 있습니다.

또한 네이버는 CNA로 버그바운티로 제보 된 이슈 중 패치 내용을 외부에 알리기 위해 CVE를 발급하고 있고, **24년에는 총 8건의 CVE가 발급**되었습니다.

완화된 위험 **128**건

지급된 리워드 **$58,960**

위험 제거 평균 기간 **35**일

도움을 준 전문가 **132**명

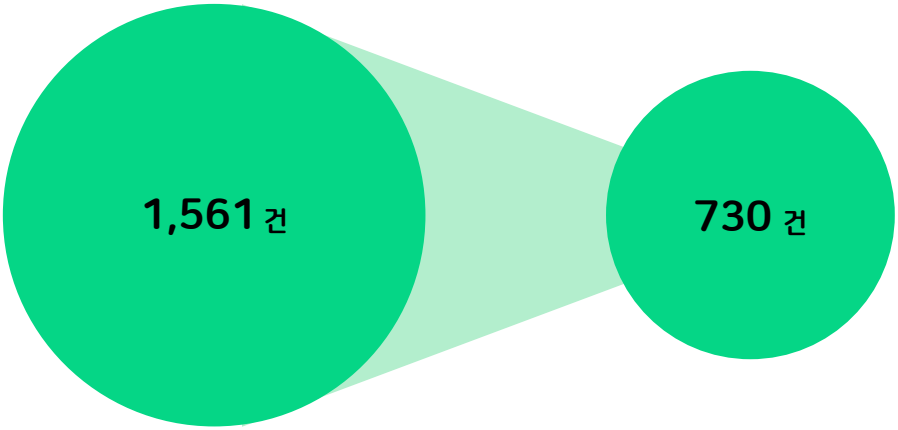
발급된 CVE **8**건

# 버그바운티 통계

## 4년간의 기록…

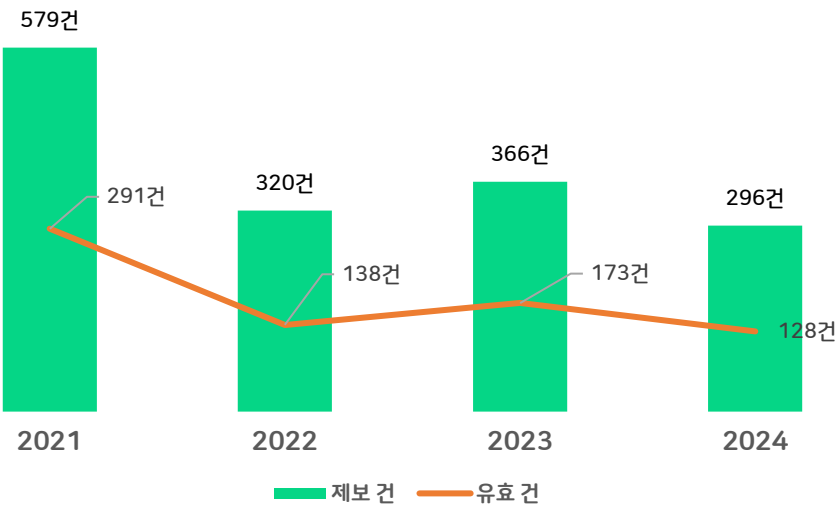
지난 4년간 네이버 버그바운티 프로그램을 통해 **제보된 보안 버그는 총 1,561건**으로 연간 약 400건 가까이 되는 이슈들이 발견되었습니다.
다만 제보된 보안 버그 모두가 네이버 서비스에 영향이 있었던 것은 아닙니다. 1,561건 중 절반 가량인 **730건이 실제 네이버 서비스에 영향**을 주는 취약점이었습니다.

외부에서 제보되어 실제 네이버 서비스에 위협이 되는 취약점으로 분류되는 이슈들은 빠르게 수정이 될 수 있도록 워킹 데이 3일 내에 서비스에 전달드리게 됩니다. 이에 맞춰서 담당 서비스 개발자분들이 적극적으로 취약점이 개선될 수 있도록 노력해 주셔서 앞서 언급한 **위험 제거 평균일인 35일**을 달성할 수 있게 되었습니다.




연도별로 조금 더 자세히 살펴보면 **2021년에는 제보된 이슈는 579건**으로 버그바운티 초기라 다수의 보안 버그가 발견되지 않았을까 생각됩니다. 발견된 보안 버그들을 해결하면서 네이버 서비스는 더욱 견고해졌고, 22년부터는 320건을 시작으로 400건이 넘지 않는 제보들이 있었습니다. 실제 서비스에 영향이 있는 보안 버그의 경우에도 매년 200건이 넘지 않고 있습니다.

버그바운티 프로그램을 운영하면서 **매년 서비스를 확장**해 나가고 있는 상황에서도 유효한 보안 버그가 크게 증가하지 않는다는 것은 서비스 출시 전에 보안 검수가 잘 진행되어서 **보안 위협들이 충분히 완화**되어 출시되고 있다고 볼 수 있습니다.
한편으로는 **개발자분들이 보안에 더 신경** 써 주셔서 취약한 코드를 생산하지 않는다고 볼 수도 있을 것 같습니다.



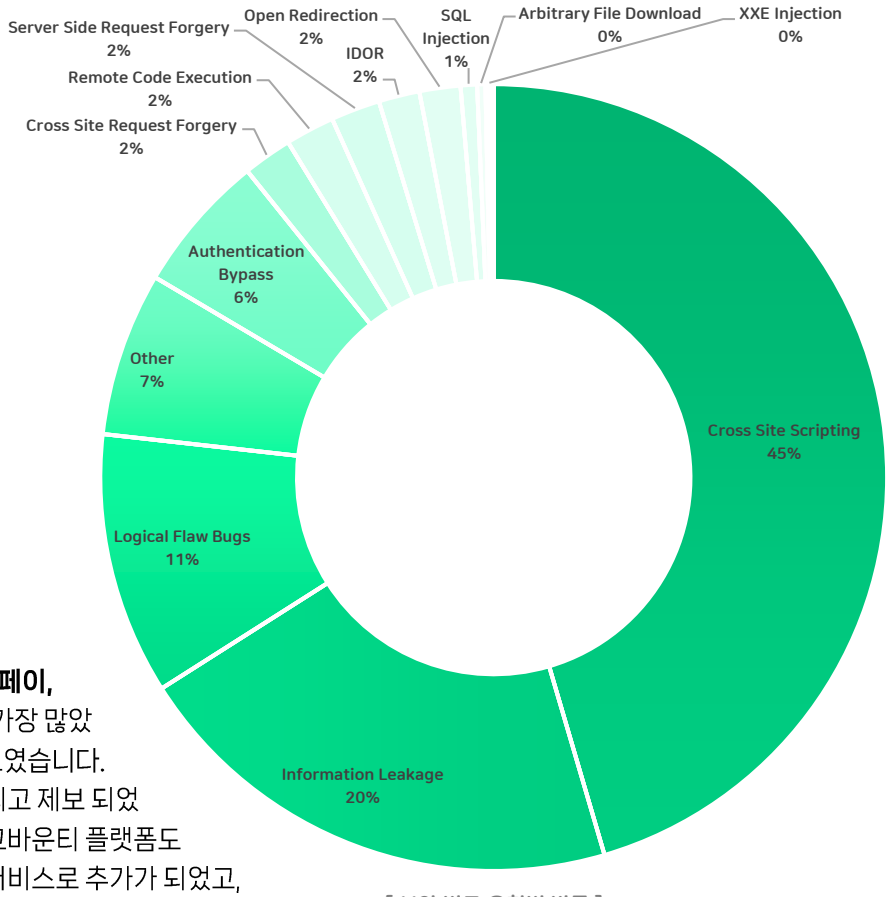
## 보안버그 유형별 통계

앞서 4년간의 지표를 통해서 버그바운티의 흐름을 볼 수 있었다면 이번에는 24년에 제보된 이슈들을 조금 더 상세하게 살펴보겠습니다.

우선 보안 버그의 유형별로는 어떤 종류의 취약점들이 있었는지 살펴보면 오른쪽 아래 표에서 보이는 것과 같이 **Cross Site Scripting (XSS) 보안 버그가 45%로 가장 많은 비율**의 제보를 차지했습니다. 네이버 서비스는 대부분이 웹 서비스 형태로 제공되고 있고, 웹 서비스에서 가장 흔하게 발견되는 보안 버그 중에 하나가 XSS 보안 버그이기도 하기 때문에 이런 결과는 어떻게 보면 당연한 결과라고 생각됩니다.

XSS 보안 버그 외에도 서비스의 중요 정보가 노출되는 **Information leakage 보안 버그가 20%**로 두 번째로 많이 제보가 되었고, **Logical Flaw Bugs가 11%**로 뒤를 이어 세 번째를 차지했습니다.

각 보안 버그의 유형에 대한 자세한 설명은 지난 2023 보안백서 버전에 자세히 설명되어 있습니다.
> 2023 백서 보러가기



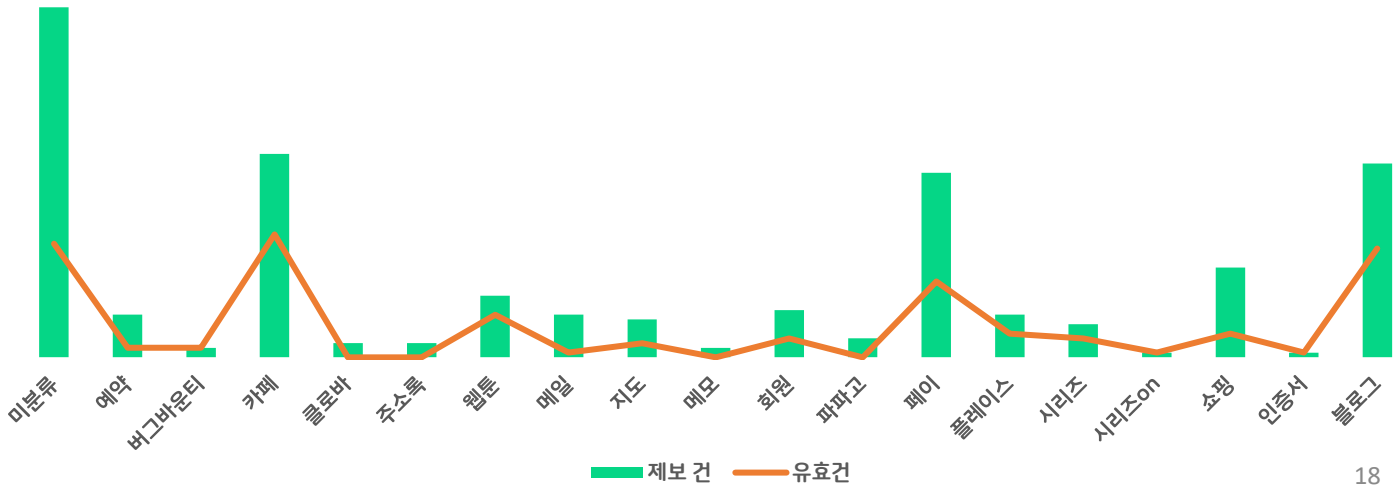
[ 보안 버그 유형별 비중 ]

## 서비스별 통계

서비스 기준으로 지표를 살펴보면 **카페, 블로그, 페이, 쇼핑 순**으로 많은 제보들이 있었습니다. **카페가** 가장 많았으며, **블로그, 페이는 카페와 비슷한 제보 건**을 보였습니다. 그 외의 서비스에도 다양하게 보안 버그가 발견되고 제보 되었습니다. 네이버 시큐리티에서 운영하고 있는 버그바운티 플랫폼도 이번 플랫폼 개편을 통하면서 버그바운티 대상 서비스로 추가가 되었고, 보안 버그가 제보되기도 했습니다.

제보가 많이 들어왔다고 해서 대상의 서비스들이 취약하다는 이야기는 아닙니다. **제보 건이 많았던 서비스**들을 살펴보면 이용자가 많은 서비스이기도 하고 공격자 입장에서 **접근성이 좋은 서비스**로 보이기도 합니다. 또한 **서비스의 복잡도가 높다** 보니 공격을 시도할 포인트가 많았던 것으로 생각됩니다.

보안 버그는 언제든지 발견될 수 있습니다. 다만 **발견된 보안 버그를 얼마나 안전하고 빠르게 조치해서 서비스의 위협을 완화할 수 있는지가 중요한 포인트**라고 생각합니다.



# 버그바운티 v2 출시 (/w VDC)

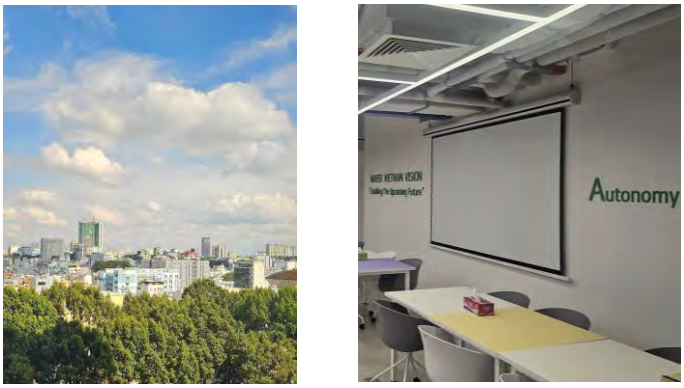
2019년부터 자체적으로 운영해오던 기존 버그바운티 플랫폼을 2024년 7월 새로운 모습으로 공개하였습니다. 새로운 버그바운티 플랫폼이 만들어진 과정과 개선된 점을 소개합니다.

**2019년부터 버그바운티 프로그램을 독립적으로 운영**하기 시작하면서 상용 이슈 관리 도구를 기반으로 프로그램을 운영해 오고 있었지만 시간이 지남에 따라 외부 참여자들을 대상으로 버그바운티 프로그램을 운영하는 과정에서 개선이 필요한 부분들이 늘어났고 실제 프로그램 운영 업무 흐름과도 맞지 않는 부분들이 존재하였습니다.

프로그램 운영 과정에서 발견된 문제 사항들과 참가자들의 프로그램 참여 경험을 향상시키기 위해 네이버 시큐리티는 기존 버그바운티 플랫폼을 개선하고자 새로운 버그바운티 플랫폼에 대해서 구상하였고, **2023년 03월부터 본격적으로 새로운 버그바운티 플랫폼에 대한 논의에 착수**했습니다.

[ 신규 버그바운티 플랫폼 설계 화면 ]

문제점들과 개선이 필요한 사항들에 대한 논의를 바탕으로 **24년 8월부터는 버그바운티 v2 플랫폼 개발을 위해 네이버 베트남 개발 센터와 협업을 시작**하였습니다.




[ 버그바운티 플랫폼을 위한 VDC 출장 ]

그렇게 약 1년간의 준비 과정을 통해 **2024년 7월 15일 새로운 버그바운티 플랫폼을 출시**하게 되었습니다.
> 블로그 글 보러가기

# 신규 플랫폼을 통한 개선 포인트

### ✓ 참여자의 개인정보 보호 기능 강화

버그바운티 프로그램 참여, 명예의 전당 등재, 리워드 서류 요청 등의 각 단계별 제보자에 대한 개인정보 보호를 고려할 수 있도록 개선하여 **컴플라이언스를 준수**할 수 있도록 했습니다.

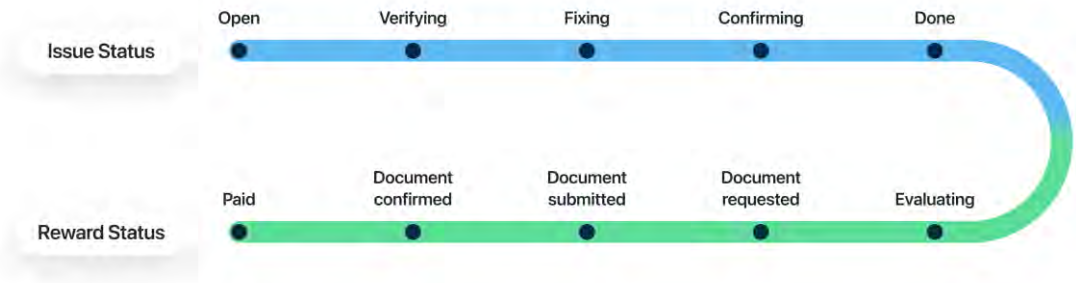
### ✓ 회원 체계 전환

기존 버그바운티 플랫폼에서 사용하던 자체 회원 체계에서 제보자들이 간편하고 안전하게 제보할 수 있도록 **네이버 아이디 회원 체계로 전환**하였습니다.

제보자들은 네이버 회원 서비스에서 제공하는 모든 유형의 계정 보호 기능과 정책을 적용받아 보다 안전하게 플랫폼을 사용할 수 있게 되었습니다.

### ✓ 제보 처리 과정 개선

이슈가 제보 되는 시점부터 포상금 지급이 완료되는 시점까지 제보가 처리되는 과정을 실제 업무가 처리되는 흐름에 맞게 세분화하여 **신규 플랫폼이 각 단계에 필요한 기능들을 지원할 수 있도록 개선**하였습니다.




네이버 시큐리티는 네이버의 모든 서비스가 안전하게 유저에게 서비스될 수 있도록 버그바운티 프로그램을 지속적으로 발전시키고 책임감 있게 운영해 나갈 것입니다.

# 서비스 보안 지표

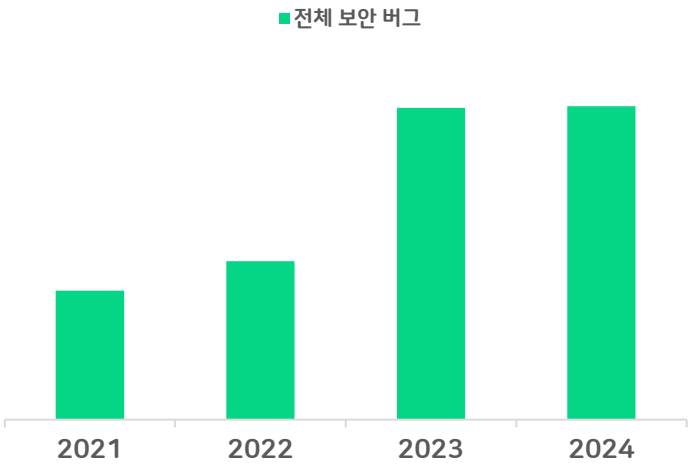
## 발견된 보안 버그

앞서 외부에서 발견된 보안 버그에 대해서 살펴 봤다면, 이번에는 네이버 내부에서 발견되어서 완화된 위협은 얼마나 되는지 살펴보려고 합니다.

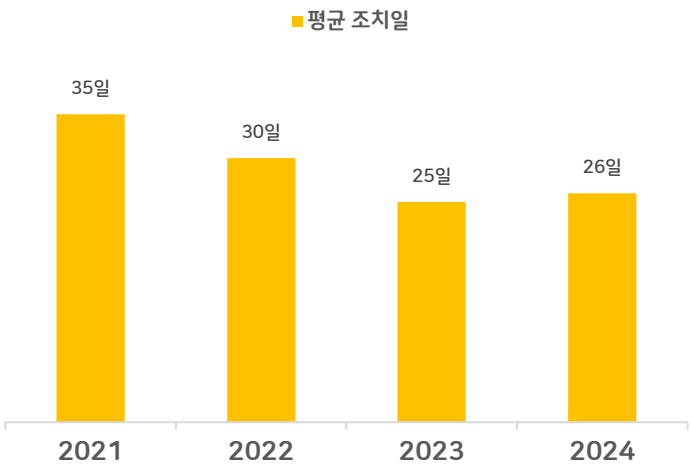
네이버 시큐리티에서는 서비스의 안전한 운영을 위해 서비스의 **기획, 설계 단계부터 출시까지 모든 단계에서 필요한 보안 리뷰 및 보안 점검을 진행**하고 있습니다. 또한 자동화된 탐지 툴도 사용해서 스캔도 진행하고 있습니다.

2024년 네이버 **내부에서 발견된 보안 버그의 경우 전년과 유사한 수준**입니다. 매년 많은 신규 서비스와 기능이 출시되면서 그에 따라 선제적으로 발견되는 보안 버그 또한 일정 부분 유지되는 것으로 보입니다. 또한 발견된 보안 버그가 조치되기까지는 **평균 26일의 시간이 소요**되었습니다.

보안 버그는 발견하는 것으로 끝나는 것이 아니라, 이처럼 빠르게 제거하여 서비스의 보안성을 항상 유지할 수 있도록 해야 합니다.




[ 연간 보안 버그 발견 건수 ]




[ 보안 버그 조치일 ]

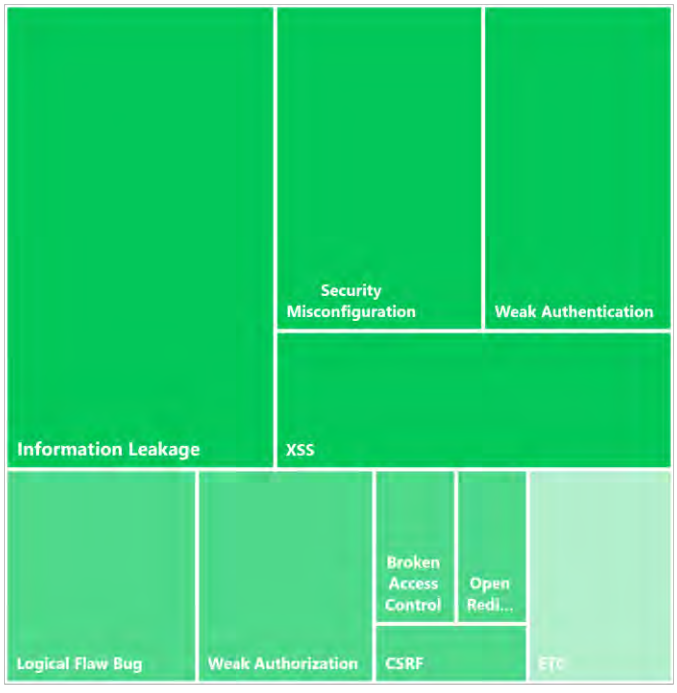
## 발견된 보안 버그 유형

보안 점검과 버그바운티를 통해 서비스에서 발견한 보안 버그들을 살펴본 결과, 불필요한 정보 노출로 발생하는 **Information Leakage 보안 버그가 가장 높은 비중**을 차지하였습니다.

이와 함께 애플리케이션, 서버 및 플랫폼 등의 **보안 설정이 미흡하여 발생하는 Security Misconfiguration**, 그리고 애플리케이션의 인증 검증이 누락되거나 미흡한 경우 발생하는 **Weak Authentication 보안 버그가 뒤**를 이었습니다.

또한, 버그바운티 프로그램을 통해 다수 제보되는 XSS(Cross-Site Scripting) 역시 상당한 비중을 차지하는 것으로 나타났습니다.

서비스의 보안성을 더욱 강화하기 위해 지속적인 보안 점검과 버그바운티 프로그램 운영을 이어가며, 서비스 부서와 함께 발견되는 보안 버그들에 대해 대응하고 해결할 수 있도록 최선을 다하겠습니다.

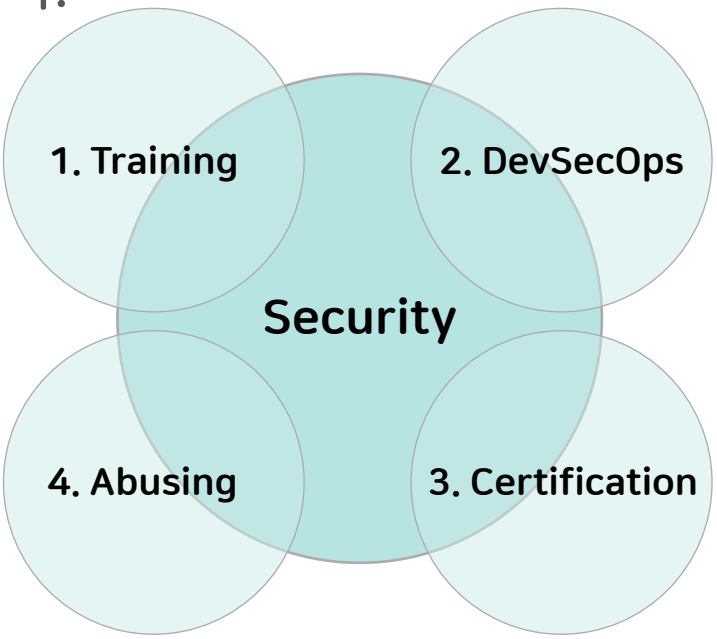



[ 보안 버그 유형별 비중 ]

# 5

## 네이버 시큐리티의 활동

이번 섹션에서는 2024년 네이버의 보안을 강화하기 위해 진행한 네이버 시큐리티의 다양한 활동에 대해서 이야기해 보겠습니다.



# 1. Training

네이버 시큐리티는 임직원의 보안 스킬 향상 및 보안 인식 개선을 위해 교육과 캠페인 등 다양한 활동을 진행하고 있습니다.



## 서비스 특화 보안교육

서비스 특화 보안 교육이란 분기마다 사내 개발직군을 대상으로 하는 보안 교육입니다.
서비스 또는 조직을 선정하여 모의 해킹을 수행해 취약점을 찾고, 발견된 이슈들을 사례로 하여 유형과 조치 방법, 조치 시 유의사항 등을 교육으로 진행하고 있습니다.

2018년 사전을 처음 시작으로 지금까지 매년 진행해오고 있으며, 현재까지 약 12개 서비스 및 조직을 대상으로 진행하였습니다.
2024년에는 **회원/인증서, 광고 서비스, 사내 플랫폼 서비스**에 대해서 점검 및 교육을 진행했습니다.

매년 대외 서비스를 대상으로 특화 보안 교육을 진행했지만, 내부 플랫폼의 보안 또한 중요하다고 판단되어 2024년 하반기에는 사내 **Cloud Native 플랫폼인 N3R**을 대상으로 진행했습니다.

7월
회원, 인증서, 자격증
45명 / 4.89점

10월
광고 서비스
166명 / 4.85점

12월 ~
사내 플랫폼 서비스
진행 중

네이버는 상시적인 보안 점검 뿐 아니라 이처럼 다방면으로 서비스에 대한 보안을 강화하기 위해서 노력하고 있습니다.

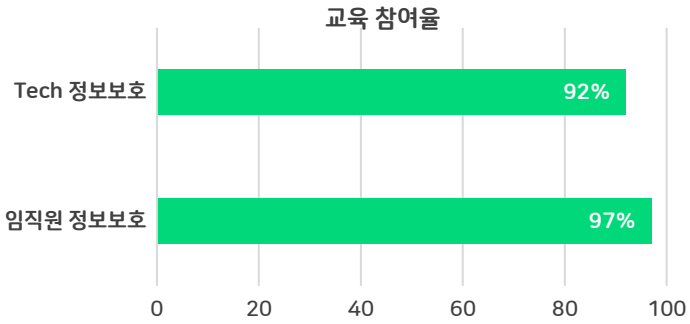
## 5월 – Tech 정보 보호 교육

24년 5월부터 **"개발자가 알아야 할 단계별 보안 프로세스"**를 주제로, 관리적 측면에서 본 기본적인 개발자 보안 수칙에 대한 내용을 안내하기 위한 교육을 시행하였습니다.

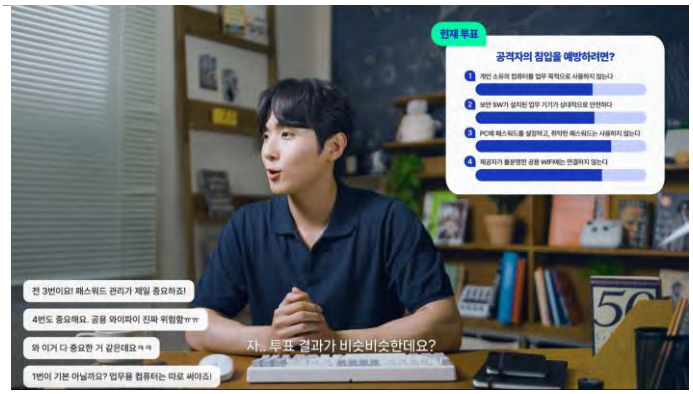
**교육 이수율은 네이버 법인 기준 92%**로 많은 Tech직군 임직원분들께서 참여해 주셨으며, 최초 시행 이후에는 매월 신규로 입사하는 Tech 직군 신규 입사자를 대상으로 지속적인 교육을 진행하고 있습니다.


[개발자가 알아야 할 단계별 보안 프로세스]

- ✓ 기획에서 배포까지, 보안을 고려해야 하는 전체 프로세스에 대한 이해
- ✓ 소스코드 관리, 컨테이너 보안, 서버/DB 보안 관리 등 보안 준수 사항 안내
- ✓ 소스코드와 비즈니스 로직 설계에 대한 보안 리뷰, 배포 전 보안 검수 등 보안 프로세스 안내








## 7월 – 임직원 정보 보호 교육

네이버 시큐리티에서는 임직원이 회사의 정보보호 정책을 잘 이해하고, 개인의 부주의로 인한 정보보호 위반이나 정보 유출이 발생하지 않도록 예방하기 위해 매년 정보보호 교육을 실시하고 있습니다.

24년에는 **"업무 수행 과정에서 실제 발생할 수 있는 사고 사례 및 위험성"**이라는 주제로, 발생 가능한 보안 사고 사례와 사고 발생 시 어떤 결과로 이어질 수 있는지 알아볼 수 있도록 교육을 진행하였습니다. 스트리밍 형식의 영상을 제작해 임직원분들의 교육 집중도를 높였습니다.

2024년 7월 10일 ~ 2024년 9월 23일의 기간 동안 총 8회에 걸친 연장 교육이 진행되었고, 네이버 임직원 (임원/정규직/계약직/파견직/인턴) 및 **네이버 계열사 28개 법인에서 동시 진행**되었습니다.

**교육 이수율은 네이버 법인 기준 97.3%, 교육 만족도 또한 5점 만점에 4.77점**으로 많은 임직원분들께서 참여해 주셨습니다. 다시 한번 교육에 참여해 주신 모든 분들께 감사드립니다.


## 정보보호 캠페인

네이버는 임직원의 정보보호 교육과 더불어 **업무 수행 시 꼭 지켜야 할 보안 수칙 및 주의사항** 안내를 위해 정보보호 캠페인도 함께 진행하고 있습니다.

**24년 3월부터 12월까지** 파일 유출 주의사항, 모바일 기기 사용 수칙 등 총 다섯 가지의 주제로 콘텐츠를 제작하여 캠페인을 진행했습니다.

흥미를 갖고 쉽게 다가갈 수 있도록 웹툰 형식으로 내용을 구성하였고, 사내 미디어 스크린을 통해 노출하여 접근성을 높이고, **임직원의 보안 인식 향상에 기여**할 수 있도록 했습니다.

- 3월 29일
  음성/영상 파일 유출 주의사항
- 5월 29일
  브라우저 '자동 로그인' 기능 사용 주의
- 7월 29일
  모바일 기기 사용 수칙 A to Z
- 9월 9일
  전사 임직원 정보보호 교육 다시 보기
- 12월 3일
  다운로드 폴더 관리 안내

## 2. DevSecOps

네이버 시큐리티는 개발 생산성을 방해하지 않고 보안이 CI/CD 단계에 잘 녹아들 수 있도록 항상 노력하고 있습니다.

컨테이너 환경에서는 Seawall을 통해서 보안을 향상해 나가고 있습니다.

# Container & Open Source

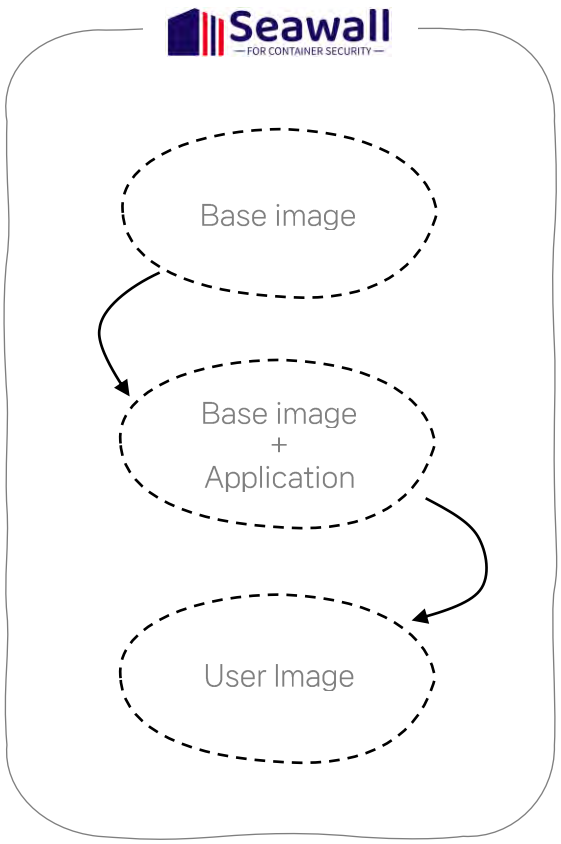
## Seawall 고도화

네이버의 사내 컨테이너 보안 관리 플랫폼인 Seawall이 별도로 관리되던 컨테이너 이미지 검사 기능을 통합하여 더욱 안전한 클라우드 네이티브 환경을 제공할 수 있도록 하였습니다.

이미지 검사 기능인 보안 강화 체크 와 취약점 검사를 별도의 단계 없이 Seawall을 통해서 제공하게 되어 **이미지 사용 전 단계부터 사용 중 단계까지 라이프 사이클 전반의 보안** 상태를 하나의 플랫폼을 통해서 모두 확인 및 관리할 수 있게 되었습니다.

또한 **탐지된 취약점의 상세 정보(취약한 라이브러리 이름 및 버전, 취약점이 조치된 버전)를 추가**하여 컨테이너 이미지에 대한 가시성을 더욱 증가 시켰습니다.

네이버는 클라우드 네이티브로 변화하는 개발 환경에서도 안전하게 서비스가 지속될 수 있도록 다양한 노력들을 진행하고 있습니다.




## OMS
## : Opensource Management System

오늘날 오픈소스의 사용은 필수 불가결한 요소이며, 이에 따라 오픈소스 취약점 역시 폭발적으로 늘어나고 있는 추세입니다.

네이버 시큐리티는 이런 환경에서 체계적으로 대응하기 위해서 **오픈소스 관리 시스템(OMS)을 자체 개발하여 운영**하고 있습니다.
네이버의 산출물(소스코드, 컨테이너 이미지 등)에서 **사용 중인 오픈소스 라이브러리의 라이선스 및 취약점(CVE) 정보를 제공**하도록 하였습니다.

### 기능

- 최신 CVE 현황 정보를 제공
- 각종 오픈소스 라이브러리 정보를 제공
- 사용자의 소스코드 / 컨테이너 이미지 내 오픈소스 라이브러리 사용 현황 및 취약점 정보를 제공

### 기대 효과

- 오픈소스 라이브러리 라이선스와 보안 취약점 현황을 파악하여 **가시성을 확보**
- 위협이 높은 취약점에 대한 노출을 빠르게 파악하고 **대응할 수 있는 기반 마련**

# 3. Certification

네이버의 정보보호 관리 체계를 외부의 객관적이고 공신력 있는 기관으로부터 검증 받기 위해 정보보호 인증 취득 활동들도 함께 진행하고 있습니다.

## ISMS/ISMS-P 인증

정보통신망법에 의한 의무를 준수하고 정보보호 관리 과정 및 보안대책 등 전반적인 정보보호 관리체계의 적정성과 개인정보의 수집·이용·파기 등 **개인정보보호 관리체계의 적정성에 대해 인증을 유지**하고 있습니다.

ISMS의 경우 네이버 데이터센터('각') 운영, ISMS-P의 경우 네이버 서비스 운영(고객센터, 비즈니스, 네이버 인증서 및 전자문서 포함) 및 이용자(B2C, B2B) 개인정보 관리 부문에 대해 **2024년 5월 7일 ~ 2024년 6월 14일 기간 동안 대응**을 수행하였습니다.

## ISO/IEC 27000 시리즈 인증

**네이버는 2022년 개정된 ISO/IEC 27001:2022 버전의 국제 표준 인증을 유지**하고 있으며, 27701, 27017, 27018 규격에 대한 인증 또한 유지하고 있습니다. 인증 범위는 네이버 내 모든 서비스의 개발, 유지, 운영에 대한 정보보안 관리 부문이며, **2024년 7월 8일 ~ 2024년 7월 12일 기간 동안 대응**이 진행되었습니다.




인증범위 : 네이버 데이터센터('각') 운영
유효기간 : 2024년 10월 16일 ~ 2027년 10월 15일


인증범위 : 네이버 서비스 운영 (고객센터, 비즈니스, 네이버 인증서 및 전자문서 포함) 및 이용자(B2C, B2B) 개인정보 관리
유효기간 : 2022년 10월 05일 ~ 2025년 10월 04일
*25년 ISMS-P 갱신심사 예정

## SOC 2,3 인증

SOC 인증은 국제감사인증기준위원회(IAASB)가 제정한 국제인증업무기준(ISAE)에 따라 **서비스의 안정성 및 관련 내부통제 수준을 평가하는 제도**입니다.

네이버는 **2012년 이후로 SOC (System and Organization Controls) 2, 3 인증을 취득하여 유지**하고 있으며, 2023년까지 독립된 감사인에 의해 내부통제의 적절성을 평가받아 **SOC Report를 발행**하였습니다.

현재 2024년 SOC 인증 평가를 진행 중에 있습니다. 인증 대상 서비스 범위는 스마트 플레이스, 마이 플레이스, 네이버 로그인, 밴드/밴드 키즈로 **2024년 12월 9일 ~ 2025년 5월 8일 기간 동안 진행**될 예정입니다. (참조)

# 4. Abusing

네이버 서비스에는 다양한 어뷰징 시도들이 발생하고 있습니다.

어뷰징에 대응하기 위해 여러 시스템을 개발 및 운영하고 있으며, 이용자 보호를 위해 노력하고 있습니다.

# Abuse Monitoring

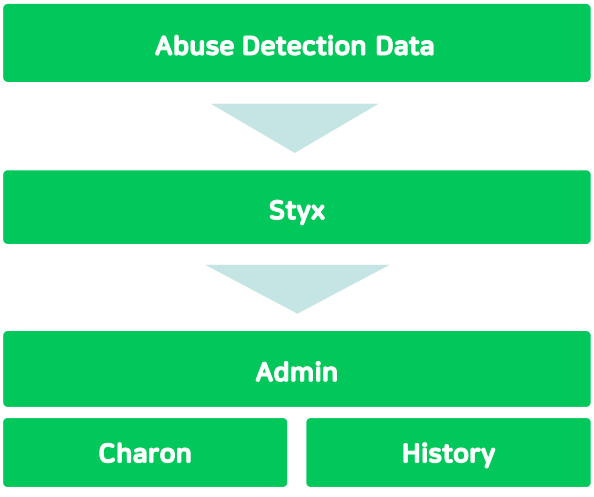
## AbuseHistory

네이버 시큐리티는 전사의 다양한 어뷰즈 활동들을 한곳에 모아 기록하고, 이를 가공하여 서비스 부서에 다시 제공하기 위해 **AbuseHistory 시스템을 운영**하고 있습니다.

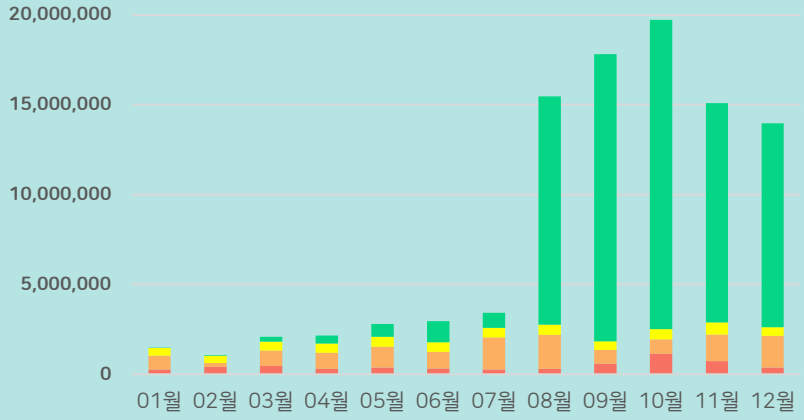
AbuseHistory는 어뷰즈 데이터를 유형에 따라 분류하고, 의심 정도에 따라 Risk Level을 설정하여 관리하고 있습니다.

새로운 유형의 어뷰즈를 지속적으로 분석 및 탐지해 **2023년 46개였던 유형을 2024년에는 107개까지 확장**했으며, 이에 따라 월평균 **100만 건 정도였던 수집 수도 250만 건으로 증가**했습니다.

어뷰징 행위나 유형에 따라 일반 사용자와 구분이 어려운 부분이 있습니다. 이를 더욱 **정확하게 탐지해내기 위해 지속적으로 개선해 나가고 있으며,** 네이버의 서비스 이용자들이 클린한 서비스를 이용할 수 있도록 지원할 예정입니다.




[ 어뷰즈 데이터 탐지 시스템 ]




[ 어뷰징 탐지 지표 ]

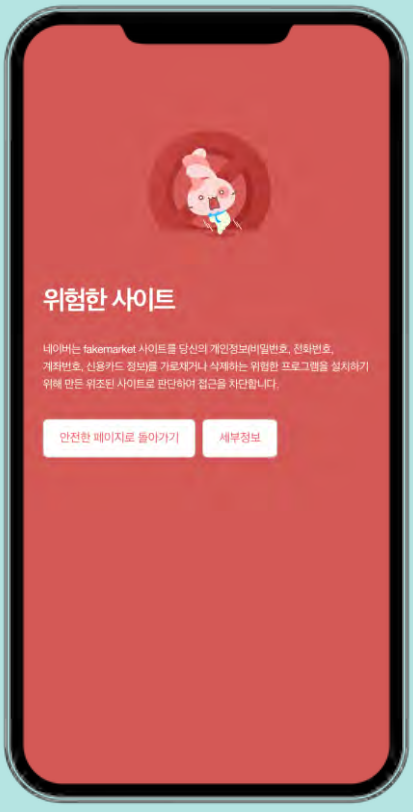
# NAVER SAFE BROWSING

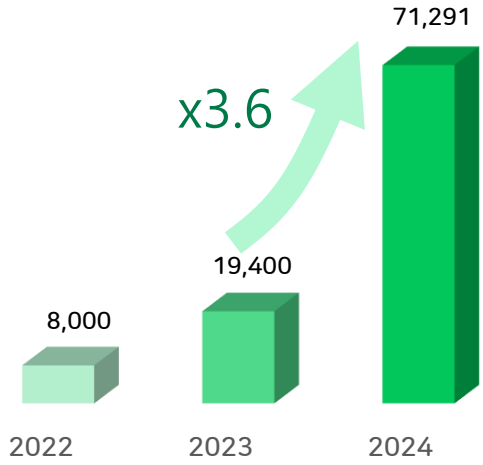
## NAPS
: NAVER Anti-Phshing System

피싱(Phishing)은 사용자의 로그인 정보 및 개인정보를 탈취하기 위한 공격 기법이며, 네이버 사용자를 대상으로 매우 빈번하게 발생하는 위협 중 하나입니다.

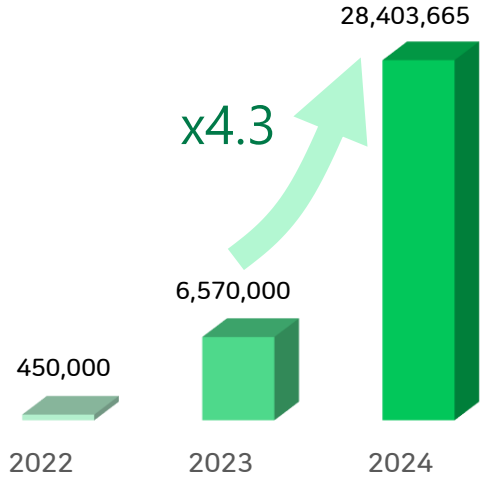
네이버 시큐리티는 오래전부터 피싱을 사전에 차단하기 위해 노력해 왔으며, 특히 **2022년부터 자체 피싱 수집 엔진(NAPS, NAVER Anti-Phishing System)을 개발**하여 피싱에 대한 대응을 강화해왔습니다.

NAPS는 **웨일 브라우저, 네이버 모바일 앱을 포함하여 카페 채팅**과 같이 이용자들이 피싱 공격에 노출될 수 있는 자사 **서비스에 확대 적용**하여 사용자가 금전적인 피해를 입지 않도록 접속을 차단합니다.




[ 피싱 사이트 등록 건수 ]




[ 피싱 메일 차단 건수 ]

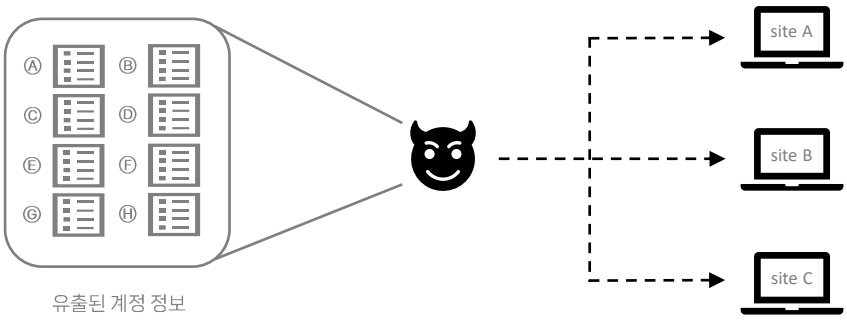
2024년에는 신규 수집 모듈을 추가 개발하였습니다. 신규 수집 모듈의 효과로 등록된 **피싱 사이트 URL 수가 전년 대비 약 3.6배 증가**하였습니다. 특히 24년에는 피싱 전용 도메인 수집 모듈을 개발하여 피싱 공격을 선제적으로 차단할 수 있도록 하였습니다.

이러한 노력은 피싱을 유포하는 메일을 **전년 대비 4.3배가량 더 차단하여 사용자를 안전한 환경**에 머물도록 하였습니다.

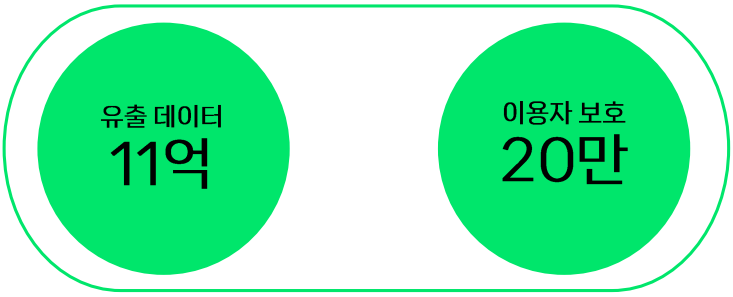
# Password Buster

## PW Buster
### : 계정 도용 사전 대응 서비스

글로벌 기업들의 정보 유출 사태가 빈번하게 발생하면서, 이용자의 계정 로그인 정보 또한 대량으로 유출되고 있습니다.
공격자들은 유출 정보를 이용한 **크리덴셜 스터핑(Credential Stuffing) 공격을 시도하여, 많은 피해 사례**를 만들고 있습니다.
PW Buster는 이러한 공격 방식으로부터 네이버 이용자의 계정이 도용되는 것을 방지하기 위한 서비스입니다.
**이용자의 유출 정보를 사전에 확보하여 네이버 서비스에서 사용하지 못하도록 안내하고 차단**하는 역할을 수행합니다.




2023년 시작된 PW Buster는 현재 **약 11억 건의 유출 정보 데이터베이스**를 확보하고 있으며, 최신 유출 정보를 실시간으로 수집 및 **해시화해서 안전하게 저장**하고 있습니다. **검증 시에도 해시 데이터를 기준으로 비교하는 방식으로 이용자의 정보가 노출되지 않도록 안전하게 관리** 및 대응하고 있습니다.
해당 기능은 현재 회원 서비스의 여러 가지 기능에 적용되어 서비스되고 있으며, **24년 한 해 동안 약 20만 건**의 위험한 아이디, 패스워드를 사용하려는 **이용자를 보호**하였습니다.




앞으로 더 많은 유출 정보를 확보하고 시스템을 고도화하여 2025년에는 이용자 보호가 필요한 많은 서비스에 적용을 목표로 열심히 달려갈 예정입니다.

# 5. More...

## 네이버의 보안관 - D2

2024년 3월에는 **보안 백서 발간을 주제로 네이버 DevRel 팀과 인터뷰를 진행**하였으며, 보안 백서를 발간하게 된 배경, 주요 내용, 그리고 보안 백서 외에도 네이버 시큐리티가 진행하는 대외활동에 대한 이야기도 함께 나눠보았습니다.

네이버 D2 인터뷰를 통해 네이버 보안 백서와 네이버 시큐리티에서 하는 다양한 활동에 대해서 외부에 알릴 수 있는 기회가 되었습니다.
> 인터뷰 보기


[인터뷰] 네이버의 보안관 - Security 윤상진, 김도경 님

2024.03.11 4930

안녕하세요. 네이버 DevRel 팀입니다.

네이버 서비스와 회원을 안전하게 보호하는 것을 목표로 대내외 다채로운 활동을 하고 계신 '네이버의 보안관' 네이버 Security 팀을 만났습니다. 네이버 Security 팀은 네이버 사내 팟캐스트 'Tech Radio : 보안 편'을 통해서도 만난 적이 있는데요.

소개되었던 활동 외에도 한 해 동안 Security 팀 활동과 보안 이슈를 정리한 보안 백서 2023 (Security Whitepaper)를 발간하게 되어 보안 백서를 통해 전하고 싶은 담당자들의 이야기를 들어보았습니다.

« 네이버 Security 윤상진 님, 김도경 님(좌측부터) »

## 보안 기술 교류회 (/w HYUNDAI)

HYUNDAI

네이버 시큐리티는 다양한 외부 교류를 통해 최신 보안 동향과 기술을 파악하고 기술 역량을 강화하고 있습니다.

**2024년 5월 현대자동차의 Cybersecurity Lab과 판교 사무실에서 세미나를 진행**하였습니다.

네이버 시큐리티에서는 **서비스 보안 관련 활동 내용과 컨테이너 보안, 피싱 현황 등에 대해 공유**하였으며, 현대자동차 측에서는 **차량 보안에 대한 전반적인 개요와 취약점 분석 플랫폼**을 만들기 위한 리서치 과정에 대해서 소개하였습니다.

## OSORI Project 참여

오소리는 오픈소스 정보 데이터를 통합 · 공개하여 누구나 쉽게 이를 확인할 수 있게 함으로써 보다 투명하고 신뢰성 있는 오픈소스 생태계 구축에 기여하는 것을 목적으로 하는 프로젝트입니다.

**기존 Board Member로는 삼성전자, LG전자, 카카오**가 있었고, 지난 2월 NAVER는 참여 요청을 받아 일반 회원사로 가입을 진행하게 되었습니다.

이후 **9월 오소리 프로젝트 가입 승인**되어 오픈소스 생태계를 구축하는데 협력하고 있습니다.

OSORI

## 마치며...

기술이 고려되지 않은 정책은 올바르게 운영되기 어렵고, 정책이 간과된 기술은 국지적인 해결책에 머물기 쉽습니다. 이에 NAVER Security는 언제나 기술과 정책을 함께 고려하여 설계하고 검토하며, 보안 플랫폼을 만들어 가고 있습니다.

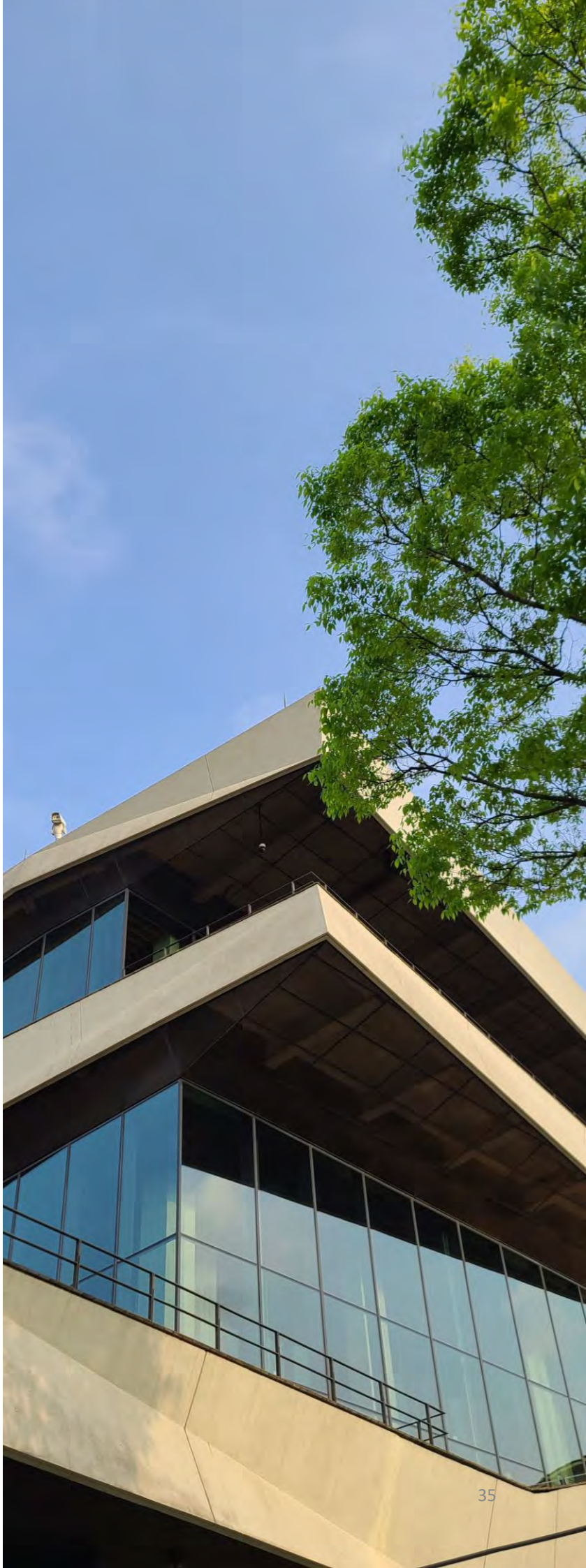
이러한 관점에서 2024년에도 NAVER Security는 팀 네이버를 안전하게 만들기 위해 폭넓은 시각에서 다양한 보안 업무를 수행하였으며, 올해도 보안 백서를 통해 그 성과를 정리하여 공유드립니다.

처음에는 큰 산을 넘는 것처럼 보였던 'Let's Shift Left' 슬로건은 네이버의 보안 요소 전반에 깊이 스며들었으며, 이를 통해 목표 달성을 향해 한 걸음 더 나아갔습니다.

앞으로도 NAVER Security는 네이버의 다양한 사업 모델을 대상으로 앞서가는 보안 전략을 수립하고, 이를 안전하게 구현하겠습니다. 함께해 주신 모든 분들께 감사드리며, 많은 관심을 부탁드립니다.

**Security Officer**

허 규




# CONTACT US

네이버 시큐리티는 보다 안전한 네이버 서비스를 위해서 항상 최선을 다해 노력하고 있습니다.

보안 백서 관련 궁금한 부분이 있다면 아래 채널을 통해서 문의 부탁드립니다.

https://blog.naver.com/naversecurity

naver.security@navercorp.com