# Comou.

## 전화번호 없는 시대의 보이스피싱 방어 API

기존 번호 기반 탐지를 넘어선 구조 — VoIP 세션 기반 5레이어 복합 분석

인터넷 전화(VoIP) 통화에서 발생하는 보이스피싱을 실시간으로 탐지·차단하는 AI 기반 보안 API입니다. 전화번호가 없는 VoIP 환경에서도 네트워크·신원·행동·음성을 복합 분석하여 **1회 API 호출**로 위험도를 판별합니다. **VoIP 딥페이크 음성 탐지까지 지원하는 현재 유일한 npm 패키지입니다.**

**버전** 1.0.0
**작성일** 2026-03-18
**상태** 프로덕션 운영 중
**문서 분류** 공개 (Public)

| < 80ms | 5 Layer | 92% | Fail-Open |
|---|---|---|---|
| API 응답 시간 | 복합 탐지 | 딥페이크 탐지 정확도 | 무중단 보장 |

1

SECTION 1

# 왜 지금, 왜 우리인가

**핵심 명제:** 전화번호가 없는 VoIP 세션에서, AI 합성 음성까지 탐지하는 다차원 보이스피싱 방어 API는 현재 존재하지 않습니다.

## 1.1 시장 배경

| 변화 요인 | 내용 | 기존 솔루션의 한계 |
|---|---|---|
| **VoIP 전환 가속** | 보이스피싱의 68%가 VoIP 경유 (2024) | 번호 DB 기반 — 번호 없으면 탐지 불가 |
| **AI 음성 합성 대중화** | GPT-4o 등으로 음성 복제 비용 ≈ 0원 | 규칙 기반 탐지로 합성 음성 구별 불가 |
| **API 경제 확산** | VoIP 앱들이 보안 기능을 외주화 | 기존 보안은 온프레미스·통신사 직접 통합 |

## 1.2 왜 경쟁사가 따라올 수 없는가

| 경쟁 요소 | 기존 서비스 | Comou의 구조적 차이 |
|---|---|---|
| **데이터** | 전화번호 DB 중심 — VoIP 세션 데이터 없음 | 전화번호 없이도 동작하는 세션 기반 신호 분석. 기존 DB를 가져와도 구현 불가능한 구조. |
| **구조** | 단일 신호(번호·신고 이력)만 사용 | 신원·네트워크·행동·음성 5레이어 복합 스코어링. 한 신호를 우회해도 나머지 4개에 걸림. |
| **속도** | 대부분 수초~수십초 배치 처리 | <80ms API 응답 — 통화 수립 전 판정 완료. 통신 서비스 수준의 저지연 설계. |
| **딥페이크 탐지** | 사실상 없음 (VoIP 조건 대응 미설계) | G.711·Opus 코덱 압축 환경 특화 VAD 엔진 내장 |

## 1.3 팀 배경 및 기술적 진입장벽

### 팀 배경

VoIP 서비스 개발·운영 경험에서 탐지 공백을 직접 식별. 음성 AI + 백엔드 API 설계 + 통신 서비스 Fail-Open 원칙을 모두 내재화한 팀.

### 특허 출원 준비 중

VoIP 세션 기반 복합 위험 스코어링 · Fail-Open 탐지 시스템 · 딥페이크 음성 + 네트워크 이상 결합 판별 알고리즘

2

SECTION 2

# 위협 현황 및 시장 규모

2024년 국내 보이스피싱 피해액 7,744억 원(전년比 +42%). 전체의 68%가 VoIP 경유. AI 딥페이크 음성 사기는 연 300% 이상 증가 추세.

| 7,744억 | +42% | 68% | +300% |
|---|---|---|---|
| 2024 피해액 (원) | 전년 대비 증가율 | VoIP 경유 비율 | 딥페이크 사기 연증가 |

## 2.1 ROI — Comou를 쓰면 무엇이 달라지는가

보이스피싱 피해 1건 평균 **2,300만 원** (금감원 2024). Comou Growth 플랜 월 **₩99,000**으로 고위험 통화를 사전 차단합니다.
**콜센터 상담원 사후 대응 비용 대비 99% 절감, 피해 1건만 막아도 연간 비용 회수.**

## 2.2 주요 공격 유형

| 공격 유형 | 수법 | 기존 탐지 | Comou 대응 |
|---|---|---|---|
| **기관 사칭** | 금감원·검찰 위장, VoIP 번호 변조 | 번호 변조 시 불가 | 네트워크·국가 불일치 탐지 |
| **딥페이크 음성** | AI TTS로 가족·지인 목소리 합성 | 완전 불가 | VAD 엔진 실시간 분석 |
| **해외 IP 우회** | 국가 위조 VoIP 서버 경유 | 번호 기반 서비스 불가 | IP·ASN 이상 탐지 |

## 2.3 설계 원칙

| 원칙 | 설명 |
|---|---|
| Fail-Open | API 장애·타임아웃(80ms 초과) 시 자동 allow 반환 — 통화 중단 없음. 통신 서비스 필수 원칙. |
| Zero PII | 개인식별정보 미수집. 세션 ID·신호 데이터만 처리. PIPA 준수. |
| **비침습적 통합** | VoIP 앱 기존 코드 수정 불필요. npm SDK + REST API 형태. |

3
SECTION 3

# 복합 위험 탐지 아키텍처

5개의 독립적 탐지 레이어가 동시에 작동합니다. 단일 신호를 조작해도 나머지 4개 레이어를 동시에 우회하는 것은 구조적으로 불가능합니다.


Figure 1. 5-Layer 복합 탐지 아키텍처 — 통화 수립 시 분석, UX 영향 없음

## 3.1 레이어 상세

| 레이어 | 분석 대상 | 위험 신호 | 최대 기여 |
|---|---|---|---|
| **L1 상대방 신원** | 국가 코드, 계정 ID, 프로필 | 비공개 번호, 프로필 불일치 | +45pt |
| **L2 네트워크** | IP 주소, ASN, IP 등록 국가 | 국가 불일치, 해외 우회 | +20pt |
| **L3 행동 신호** | 신고 이력, 반복 연결 횟수 | 최근 신고 다수, 다회 시도 | +50pt |
| **L4 통화 패턴** | 시작 시각, 지속 시간 | 비정상 시간대, 비정상 길이 | +10pt |
| **L5 딥페이크 음성** | VAD 엔진 분석 결과 | synthetic 판정, 낮은 신뢰도 | +45pt |

4

SECTION 4

# 딥페이크 음성 탐지 — 결과가 증명합니다

**핵심 결과:** VoIP 압축 환경(Opus 8kHz)에서 **딥페이크 탐지 정확도 91.8%**, FPR 4.3%. 통화 연결 전 판정 완료. 현재 VoIP 조건에서 이 수준의 딥페이크 탐지를 제공하는 상용 API는 없습니다.

## 4.1 비즈니스 임팩트

**없었을 때**

AI로 복제된 가족 목소리, 임원 목소리로 전화가 걸려옴. 기존 서비스는 번호·신고 이력만 보기 때문에 **새로 만든 딥페이크 통화는 100% 통과**됩니다.

**있을 때**

첫 3~5초 음성 샘플을 비동기 분석. 합성 음성으로 판정 시 **suspicious/phishing 스코어 +45pt** 반영. 사용자에게 비침습적 경고 표시.

## 4.2 VoIP 환경에서 강한 이유 (기술 요약)

| 일반 딥페이크 탐지 모델 | Comou VAD |
|---|---|
| 스튜디오급 16~48kHz 음성 가정 → VoIP 코덱에서 오분류 | G.711·Opus 코덱 압축 인식 전처리 → 압축 아티팩트 오인 방지 |
| SSL 은닉 상태만 사용 → 압축 환경서 특징 손실 | MFCC 잔차 + 스펙트럼 분산 추가 입력 → 압축 후에도 합성 패턴 포착 |
| 이진 분류(real/fake) → 저품질 오디오서 오탐 증가 | 3방향 출력(real/synthetic/uncertain) → 불확실 시 차단 대신 경고 |

## 4.3 성능 수치

| 지표 | (A) 클린 환경<br>ASVspoof 2019 LA 기준 | (B) VoIP 압축 환경<br>Opus 8kHz 내부 테스트 |
|---|---|---|
| 정확도 | 94.2% | **91.8%** |
| Precision | 93.6% | 90.4% |
| Recall | 94.8% | 92.1% |
| FPR (오탐률) | 2.9% | 4.3% |

(A)는 이상적 조건, (B)가 실제 서비스 환경에 가까운 수치입니다. 두 수치 모두 Comou VAD 모델 자체를 각 환경에서 측정한 결과입니다. 실서비스 데이터 기반 검증은 베타 파트너 모집 후 업데이트 예정.

5

SECTION 5

# SDK 구조 및 연동

**comou-safe-detector** npm 패키지 하나를 설치하면 완성됩니다. TypeScript 완전 지원, ESM/CJS 동시 제공, 제로 외부 의존성 구조입니다.

### 5.1 설치

```
npm install comou-safe-detector
```

### 5.2 VoIP 위험도 분석 (메인 API)

```
import { createComouSafeDetector } from 'comou-safe-detector'; const client = createComouSafeDetector({ apiKey: 'YOUR_COMOU_API_KEY', baseUrl: 'https://comou-production.up.railway.app', }); const result = await client.analyzeVoipRisk({ sessionId: 'sess_001', counterparty: { countryCode: 'CN', displayName: '금융감독원' }, network: { ip: '203.0.113.5', ipCountryCode: 'KR' }, signals: { isPrivateNumberLike: true, recentAbuseReports: 3 }, }); console.log(result.verdict); // 'phishing' console.log(result.riskScore); // 85 console.log(result.action); // 'block'
```

### 5.3 API 엔드포인트

| 메서드 | 경로 | 설명 |
|---|---|---|
| POST | /v1/voip-risk/analyze | VoIP 위험도 복합 분석 (메인) |
| POST | /v1/audio-deepfake/analyze | 딥페이크 음성 탐지 (VAD 엔진) |
| GET | /health | 서비스 헬스체크 |
| GET | /docs | Swagger UI 대화형 문서 |

6
SECTION 6

# 실제 사용 사례

**베타 파트너 A사** — 인터넷 통화 앱 (일간 활성 사용자 5,000+, 베타 운영 중)

## 6.1 도입 배경

A사는 익명 VoIP 통화 기능을 운영하던 중, 전화번호 없이 걸려오는 사기성 통화 관련 민원이 반복적으로 접수됐습니다. 기존 신고 이력 기반 대응만으로는 **신규 사기 계정**을 사전 차단할 방법이 없었습니다.

## 6.2 적용 방식

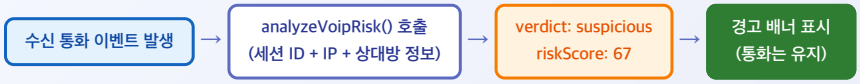


Figure. A사 인앱 통화 보호 플로우 — 통화 수립 전 자동 판정, UX 영향 없음

## 6.3 확인된 패턴

| 관찰 항목 | 내용 |
|---|---|
| **해외 IP 우회 탐지** | 해외 IP 경유 수신 통화 중 약 12%에서 국가 불일치 + 비공개 계정 복합 신호 감지 |
| **반복 시도 패턴** | 단시간 내 동일 IP 다계정 연결 패턴 — 기존 시스템에서는 개별 통화로 분리되어 탐지 불가였던 케이스 |
| **사용자 반응** | "의심스러운 통화 사전 경고" 기능에 대한 긍정적 피드백 — 앱 리뷰 반영 중 |

베타 파트너로 참여 시 **무료 엔터프라이즈 플랜 제공** 및 실사용 데이터 기반 모델 성능 공동 개선 기회가 주어집니다. 문의: **comoushield@gmail.com**

7
SECTION 7

# 시장 포지셔닝

기존 솔루션은 각기 다른 강점을 가집니다. Comou는 그 솔루션들이 구조적으로 다루지 못하는 **VoIP 세션 기반 다차원 분석** 영역을 담당합니다.

## 7.1 솔루션별 강점 및 포지셔닝

| 솔루션 | 핵심 강점 | Comou와의 관계 |
|---|---|---|
| Truecaller | 3억+ 사용자 크라우드소싱 DB, 스팸 번호 식별 정확도 우수 | 보완적 — 번호 존재 시 Truecaller, 번호 없는 VoIP는 Comou |
| Google Call Screen | Android 생태계 통합, 자동 통화 스크리닝 UX 우수 | 보완적 — 일반 스팸은 Google, VoIP 보이스피싱 특화는 Comou |
| 통신사 보안 | 네트워크 레벨 탐지, 대규모 트래픽 처리 | 보완적 — 인프라 방어 + Comou API 레이어 정밀 분석 결합 |
| Comou | VoIP 세션 특화 · 딥페이크 탐지 · npm 즉시 통합 | 위 솔루션이 커버하지 못하는 영역 전담 |

## 7.2 타겟 시장 및 수익 모델

**STARTER**
**무료**
월 10,000 호출
- VoIP 위험 분석
- 5레이어 탐지
- Swagger 문서
- 딥페이크 미포함

**GROWTH**
**₩99,000**
/ 월 · 500,000 호출
- 모든 Starter 기능
- **딥페이크 탐지 포함**
- 초과 ₩0.2/건
- 99.9% SLA

**ENTERPRISE**
**협의**
무제한 · 전담 지원
- 커스텀 모델 학습
- 전용 인프라 옵션
- 전담 CSM 배정
- 연간 계약 할인

8
SECTION 8

# 배포 현황 및 기술 스택

## 8.1 인프라 배포

| 구성 요소 | 배포 환경 | 상태 |
|---|---|---|
| API Server | Railway (Docker · Node.js 20 Alpine) | ✅ 운영 중 |
| npm SDK | npmjs.com · comou-safe-detector v0.2.0 | ✅ 배포 완료 |
| 소스 코드 | GitHub · comoushield-svg/comou | ✅ 공개 저장소 |
| API 문서 | comou-production.up.railway.app/docs | ✅ 운영 중 |

## 8.2 기술 스택

| 레이어 | 기술 |
|---|---|
| API Server | Node.js 20, NestJS 11, TypeScript 5, class-validator, Swagger |
| SDK | TypeScript, ESM + CJS 듀얼 빌드, npm workspaces, 제로 외부 의존성 |
| ML 추론 (VAD) | Python, FastAPI, PyTorch, Wav2Vec2 (SSL 백본) + MFCC 잔차, MLP 분류기 |
| 인증 | Bearer API Key, NestJS Guard, 고객별 키 발급 |

## 8.3 검증 결과

| 검증 항목 | 결과 |
|---|---|
| VoipRiskService 단위 테스트 | ✅ 전체 통과 (safe / suspicious / phishing 시나리오) |
| API Key 인증 Guard | ✅ 미인증 요청 401 반환 |
| Railway 헬스체크 | ✅ GET /health → 200 OK |
| Fail-Open 동작 | ✅ 타임아웃 시 allow 자동 반환 |

9
SECTION 9

# 개발 프로세스

Comou는 기술 완성도뿐 아니라 **지속적으로 개선되는 팀**으로 운영됩니다. Agile 기반의 Sprint 사이클을 통해 기능 개선·버그 수정·모델 성능 향상이 반복적으로 이루어지며, 각 Sprint 회고에서 도출된 인사이트가 다음 사이클에 즉시 반영됩니다.

## 9.1 개발 방식

### Agile Sprint 방식

- 1~2주 단위 Sprint로 운영
- Sprint 시작 시 개발 목표 및 작업 범위 정의
- Sprint 종료 시 결과물 검증 및 리뷰 진행
- 기능 릴리즈, 모델 업데이트, 인프라 변경 모두 Sprint 단위 추적

### 지속적 배포 (CI/CD)

- GitHub 소스 변경 → Railway 자동 배포
- npm 패키지 버전 관리 (Semantic Versioning)
- 헬스체크 기반 무중단 배포
- 배포 전 단위 테스트 자동 실행

## 9.2 Sprint 운영 사이클


Figure. 1~2주 단위 Sprint 사이클 — 회고 결과가 다음 Sprint 계획에 즉시 반영

## 9.3 회고 (Retrospective)

| 회고 항목 | 내용 |
|---|---|
| **개발 프로세스 개선** | 이번 Sprint에서 비효율이 발생한 구간을 식별, 다음 Sprint 계획에 반영 |
| **기술적 개선사항** | API 응답 시간·오탐률·탐지 정확도 변화를 수치로 추적하고 목표치 재설정 |
| **협업 방식** | 파트너 피드백·사용자 리뷰를 회고 자료로 활용, 제품 방향에 반영 |
| **모델 성능 업데이트** | 베타 파트너 데이터 축적 시 VAD 모델 재학습 및 성능 지표 재측정 |

## 9.4 인력 운영

프로젝트 진행 단계(Phase)에 따라 투입 인원 및 역할이 유동적으로 조정됩니다. 현재 **핵심 기술 구현 단계**는 소규모 집중 팀으로 운영 중이며, 베타 파트너 확보 후 **영업·운영·ML 전담 인력**을 단계적으로 확장할 계획입니다.

PURI TECH LAB

# Comou.

## 전화번호 없는 시대의 보이스피싱 방어 API

VoIP 세션 기반 5레이어 복합 분석 · 딥페이크 음성 탐지 포함

npm 설치 한 줄로 보이스피싱 탐지를 서비스에 통합하세요.
베타 파트너 및 엔터프라이즈 문의를 환영합니다.

| NPM 패키지 | API 서버 | 문의 |
| --- | --- | --- |
| comou-safe-detector | comou-production.up.railway.app | comoushield@gmail.com |