

KRNET 2026

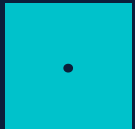
AI 시대, 라우팅 보안(RPKI)의 중요성

인터넷 경로 보안 고도화를 통한 AI 신뢰 인프라 완성

한국인터넷진흥원(KISA)
인터넷주소보호팀장 이한상

2026. 06.





AI 시대, 디지털 전환의 가속

폭증하는 트래픽과 AI가 바꾸는 인터넷 인프라



끊이지 않는 BGP 사고

2024~2026 글로벌·국내 라우팅 장애 사례



글로벌 RPKI 확산과 정책 동향

도입률·주요국 의무화 흐름



인터넷 경로(BGP)의 구조와 취약성

경로 선택 메커니즘과 근본적 보안 한계



해결책 — 라우팅 인증(RPKI)

경로 출처 검증으로 거짓 경로 차단



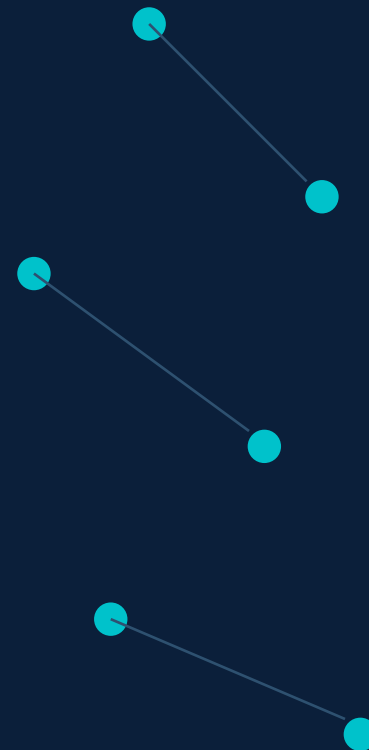
국내 현황과 과제

최하위 적용률, 전환점, 그리고 제언

I

AI 시대, 디지털 전환의 가속

모든 일상과 AI 서비스가 인터넷 경로 위에서 작동한다



대한민국, 사실상 전 국민이 인터넷에 연결되다

가구 인터넷 접속률

99.98%

전체 가구의 거의 전부가
인터넷 접속 가능 ('25)

인터넷 이용률

95.0%

만 3세 이상 국민
(전년 대비 +0.5%p)

생성형 AI 이용경험

44.5%

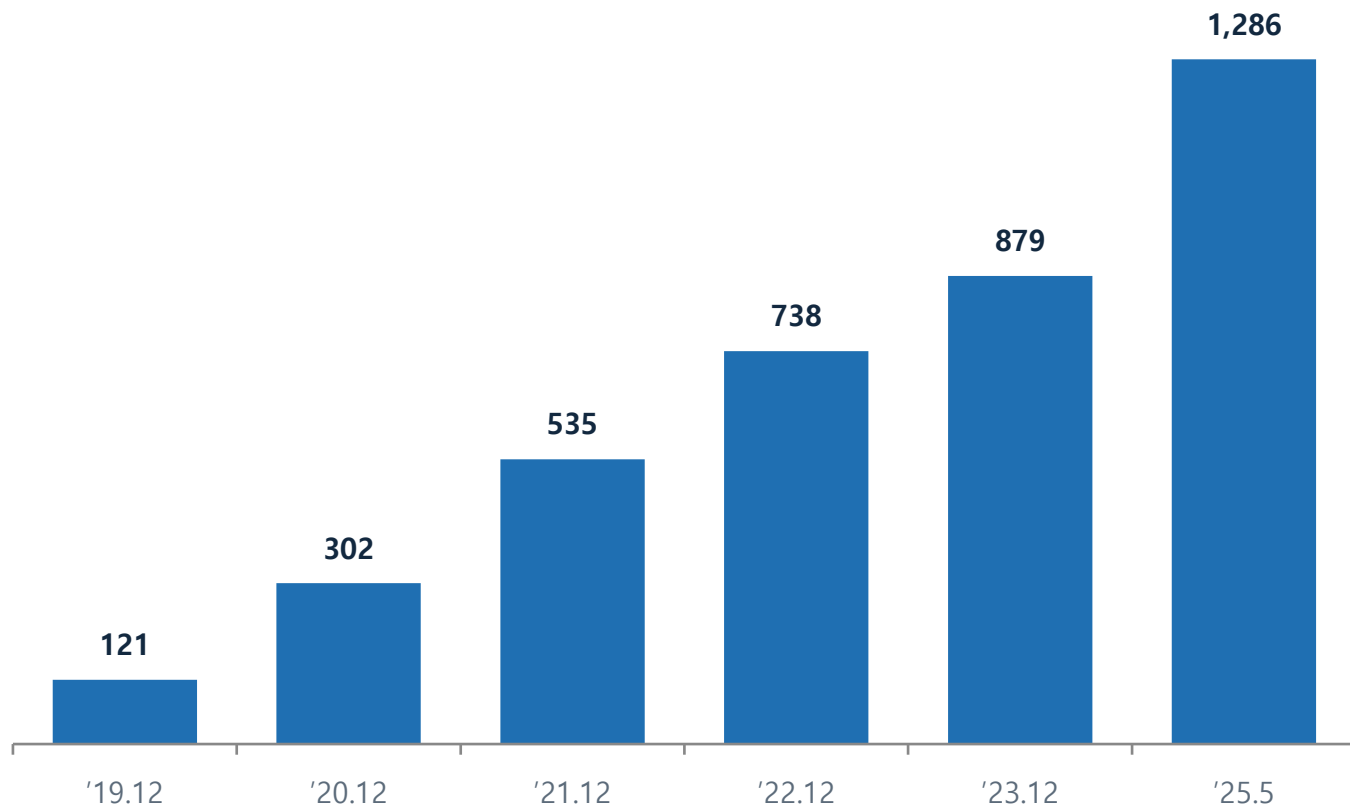
1년 새 +11.2%p 급증
ChatGPT 41.8%

시사점

인터넷은 더 이상 '서비스'가 아니라 전 국민의 생활·경제·행정 등 삶을 떠받치는 기반 시설이다.
여기에 생성형 AI, Agent AI, 향후 Physical AI까지 삶으로 들어오면,
데이터가 '올바른 경로'로 흐른다는 신뢰가 사회 전체의 전제 조건이다!

출처: 과학기술정보통신부·한국지능정보사회진흥원, 「2025 인터넷이용실태조사」(2026.3)

무선 트래픽 2년 새 약 1.5배 — AI·영상이 견인



월 1,286 PB

국내 무선데이터 트래픽 ('25.5) · 5G 비중 90.7%

월 521.9 EB

글로벌 인터넷 트래픽 ('25, 전년比 +16.2%) → '26 602 EB
전망

시사점

트래픽이 커질수록 한 번의 경로 오류가 미치는 충격도 커진다. 경로의 '양'이 아니라 '신뢰성'이 핵심 과제가 되었다.

출처: 과기정통부 무선데이터 트래픽 통계('25.5) · IBISWorld Internet Traffic Volume(2025)

AI는 '경로' 위에서 작동한다 — 새로운 의존성의 등장

1 데이터센터 트래픽 폭증

AI 학습·추론은 데이터센터 간 대규모 트래픽을 유발. AI 데이터센터 네트워킹 시장 \$10.3B('25)→\$30.2B('30), 연 24% 성장

2 경로 의존성 심화

글로벌 분산된 GPU·클라우드를 잇는 인터넷 경로(BGP)에 AI 서비스 품질이 직결. 경로 한 번의 오류가 AI 서비스 전체로 전이

3 WAN의 주력 부하로

Nokia: AI가 WAN 트래픽의 30% 차지('34F) · Cisco: AI 추론이 전체 트래픽의 약 25%('35F) — 인터넷 백본의 주력 수요로

4 공격 표면의 확대

AI 자동화로 경로 탈취·스푸핑 정찰이 정교·신속해질 수 있어, 경로 '출처'를 자동 검증하는 RPKI의 가치가 더 커진다

출처: MarketsandMarkets/Research and Markets(2026) · Nokia-Cisco WAN traffic forecast(2025)

‘연결’의 시대에서 ‘신뢰할 수 있는 연결’의 시대로

“경로를 신뢰할 수 없다면,

AI도, 금융도, 행정도
신뢰할 수 없다.”

인터넷 경로 프로토콜(BGP)은 30여 년 전 ‘상호 신뢰’를 전제로 설계되었다. AI 시대의 신뢰 인프라는 이 전제를 기술로 보증하는 데서 출발한다.

가용성

대규모 트래픽 시대, 경로 장애 = 사회적 마비

무결성

데이터가 ‘올바른 곳’으로 가야 AI 결과도 신뢰

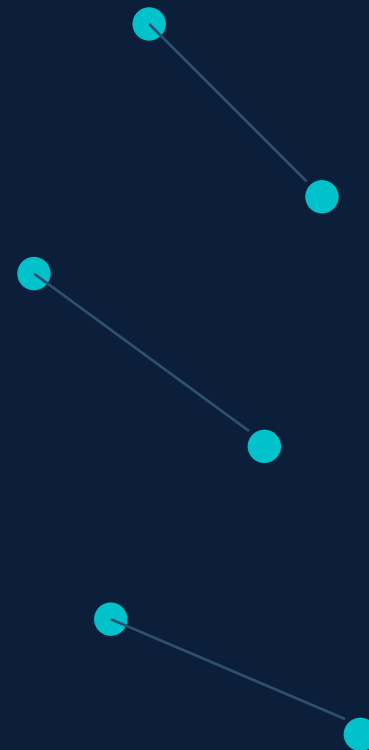
주권·안보

국가 핵심 인프라의 경로를 외부 탈취로부터 보호

II

인터넷 경로(BGP)의 구조와 취약성

수만 개 네트워크가 '신뢰'만으로 경로를 주고받는다



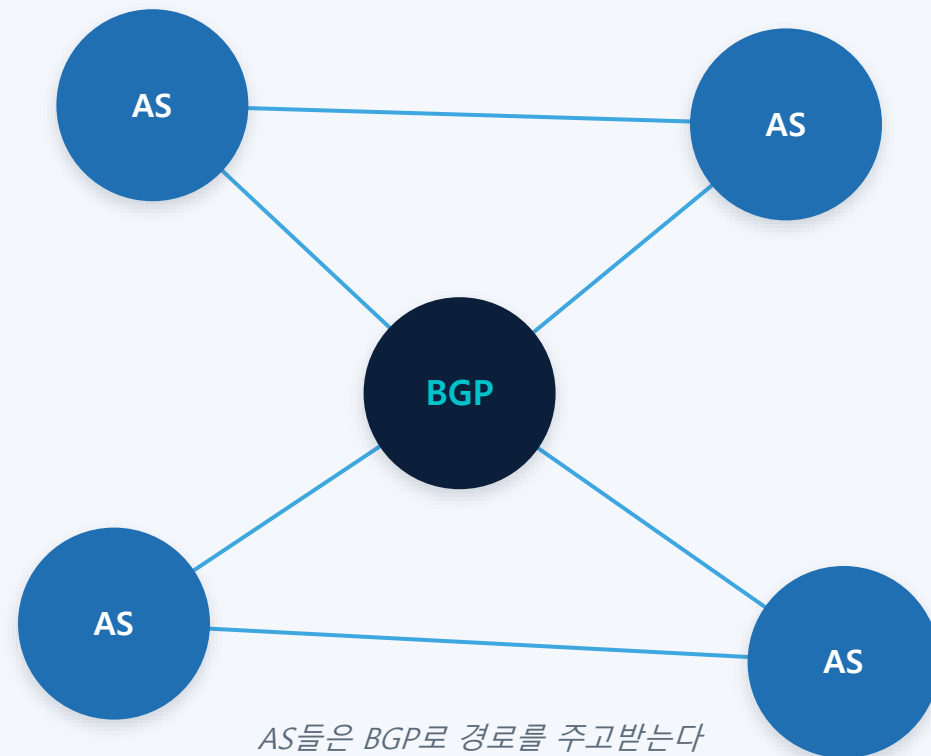
인터넷 = 네트워크들의 네트워크 (Network of Networks)

자율 시스템 (AS, Autonomous System)

통일된 라우팅 정책으로 운영되는 네트워크 단위. ISP·기업·기관마다 고유한 AS 번호(ASN)를 부여받아 인터넷에 참여한다.

BGP (Border Gateway Protocol)

AS와 AS 사이에서 '어느 경로로 갈지'를 교환하는 인터넷의 핵심 라우팅 프로토콜. 이웃 라우터의 경로 광고를 신뢰하고 그대로 전파한다.



수십만 개 경로가 실시간으로 광고·갱신된다

IPv4 BGP 경로(Prefix)

약 95만

전 세계 라우팅 테이블에
광고되는 IPv4 경로 수

IPv6 BGP 경로(Prefix)

약 13만

빠르게 늘어나는
IPv6 경로 수

전 세계 활성 AS 수

약 7만

인터넷에 참여하는
자율 시스템(네트워크) 수

이 방대한 경로 정보는 '누가 광고해도 일단 믿는' 구조로 교환된다. 단 하나의 잘못된·악의적 광고가 전 세계로 수 초 만에 퍼질 수 있는 이유다.

출처: CIDR Report / 글로벌 BGP 라우팅 테이블 현황(개략치)

'신뢰'를 전제한 설계 — 검증 장치가 없다

BGP 기본 경로 선택 원칙

01 가장 상세한(긴 prefix) 경로를 우선 선택

02 그 다음, 가장 짧은(AS-path) 경로를 선택

→ 공격자가 '더 상세한 경로'를 광고하면, 정상 경로를 제치고 트래픽을 끌어들 수 있다.

보안이 고려되지 않은 프로토콜

할당받지 않은 IP 대역도 경로로 광고 가능

→ 출처(Origin) 검증 부재

전달받은 경로 정보의 오류·위변조 확인 불가

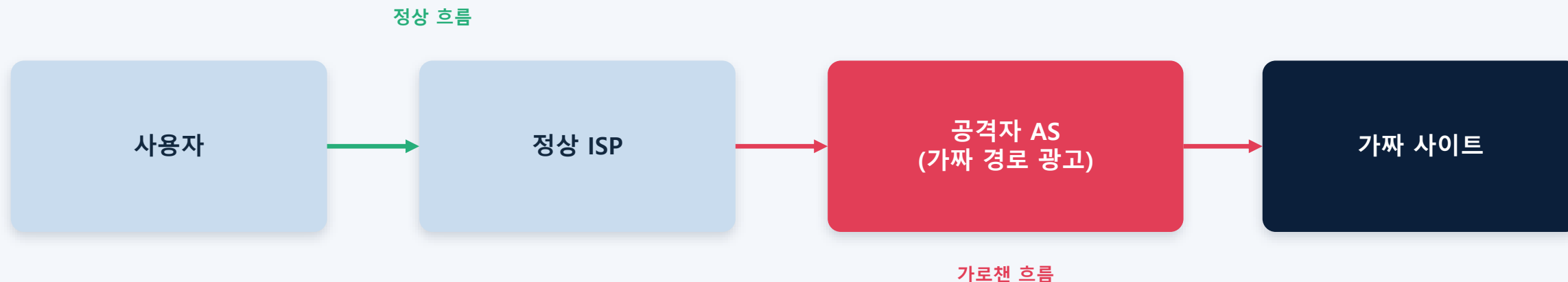
→ 무결성 검증 부재

광고는 수 초 만에 전 세계로 전파

→ 사고의 즉시·광역 확산

BGP 하이재킹 — 남의 IP 대역을 가로채다

악의적·실수로 특정 AS가 자신의 것이 아닌 IP 대역을 광고하면, 해당 목적지로 향하는 트래픽이 공격자에게 흘러든다.



피해: 트래픽 탈취·도청, 피싱·가짜사이트 유도, 서비스 마비, 암호화폐·인증 트래픽 가로채기 등

경로 유출(Route Leak) — 새어 나간 경로

일반적으로 외부에 광고하면 안 되는 라우팅 정보가 정책 오류로 의도치 않게 외부로 새어 나가, 트래픽이 비정상 경로로 우회·집중된다.



실수로 잘못 광고된 경로가 상위로 전파되며 대규모 우회를 유발

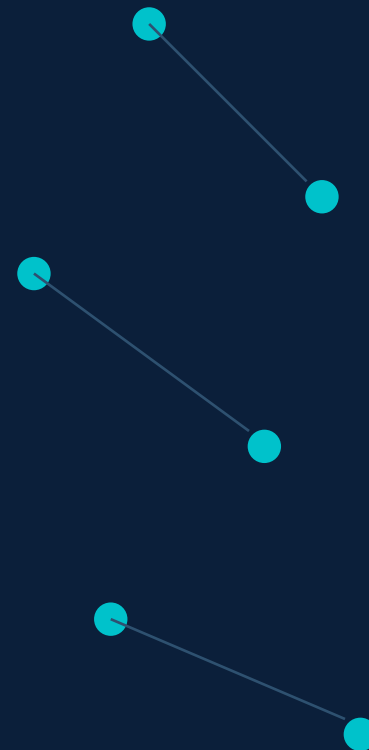
하이재킹 보통 '출처(Origin)' 위조 — 내 것이 아닌 대역 광고

경로 유출 주로 '전파 정책' 오류 — 새어 나간 경로의 비정상 전파

III

꿈이지 않는 BGP 사고

RPKI로 서명해도, 검증하지 않으면 막지 못한다



최근까지도 반복되는 글로벌 라우팅 사고

2024.1

스페인 Orange 대규모 장애

공격자가 RIPE 계정을 탈취해 BGP-RPKI 설정을 변조 → 전국 인터넷 장애

2024.6

Cloudflare 1.1.1.1 DNS 장애

브라질 ISP의 1.1.1.1/32 오광고 + 경로 유출 → 70개국 300여 네트워크 영향

2025

하이퍼볼류메트릭 공격 급증

경로·인프라를 겨냥한 초대형 DDoS가 사상 최대 31.4 Tbps 기록

2026.1

Cloudflare IPv6 경로 유출

정책 변경 실수로 25분간 IPv6 경로 유출 — 혼잡·패킷 손실(약 12 Gbps)

출처: Internet Society Pulse · Cloudflare Blog · Cloudflare Radar 2025 Year in Review

Cloudflare 1.1.1.1 (2024.6.27) — RPKI '서명'과 '검증'의 차이

무슨 일이 있었나

- 브라질 ISP가 1.1.1.1/32를 자기 것처럼 오광고
- 1분 뒤 또 다른 사업자가 1.1.1.0/24를 상위로 유출
- 결과: 70개국 약 300개 네트워크에서 1.1.1.1 접속 장애
- **Cloudflare는 해당 대역을 RPKI로 정상 서명(ROA)하고 있었다**
- 그러나 검증(ROV)을 하지 않는 네트워크들이 가짜 경로를 수용 — 일부 Tier-1까지

핵심 시사점

RPKI는 '서명(ROA)'만으로 완성되지 않는다.

경로를 받는 모든 네트워크가 '검증.필터링(ROV)'을 해야 가짜 경로가 차단된다.

“우리만 서명하면 된다”가 아니라 “우리도 검증한다”로 — 라우팅 보안은 네트워크 간 '집단적 참여'가 본질이다. AI 시대 핵심 인프라일수록 더 그렇다.

출처: Cloudflare, "Cloudflare 1.1.1.1 incident on June 27, 2024"

한 번의 경로 오류가 전국을 멈춘다

2022

KT 부산 — BGP 설정 실수

부산지사 기업용 라우터의 경로 설정 오류로 약 1시간 동안 전국망 장애 발생

2023

호주 Optus — BGP 장애

6시간 이상 전국망 마비, 인구의 약 1/3(1천만 명)이 인터넷 사용 불가 — 국가적 혼란

설정 실수든 악의적 공격이든, 결과는 동일하다 — 멈춘 인터넷. 그래서 '사람의 주의'가 아니라 '자동 검증'이 필요하다.

서명은 늘었지만, '검증'이 따라오지 못한다

두 단계 모두 필요하다

1

ROA 발급 (서명)

IP 소유자가 '이 경로는 내 것'이라고 인증서 발급

2

ROV 검증·필터링

경로를 받는 네트워크가 인증서로 검증해 가짜 경로 차단

②가 빠지면, 아무리 ①로 서명해도 가짜 경로는 그대로 통과한다.

전 세계 RPKI Valid 비율 ('25.12)



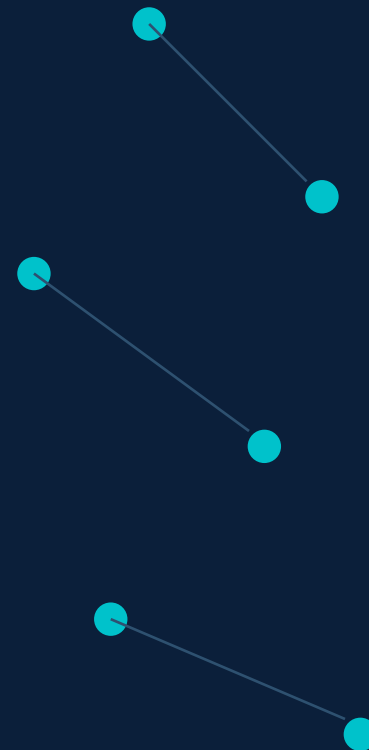
그러나 '검증(ROV)'을 실제 적용하는 네트워크는 여전히 부족 — 서명과 검증의 격차가 사고의 빈틈이다.

출처: Cloudflare Radar 2025 Year in Review · SIDN/Internet Society(2025)

IV

해결책 — 라우팅 인증(RPKI)

경로의 '출처'를 암호학적으로 보증하다



Resource Public Key Infrastructure

R esource

P ublic

K ey

I nfrastructure

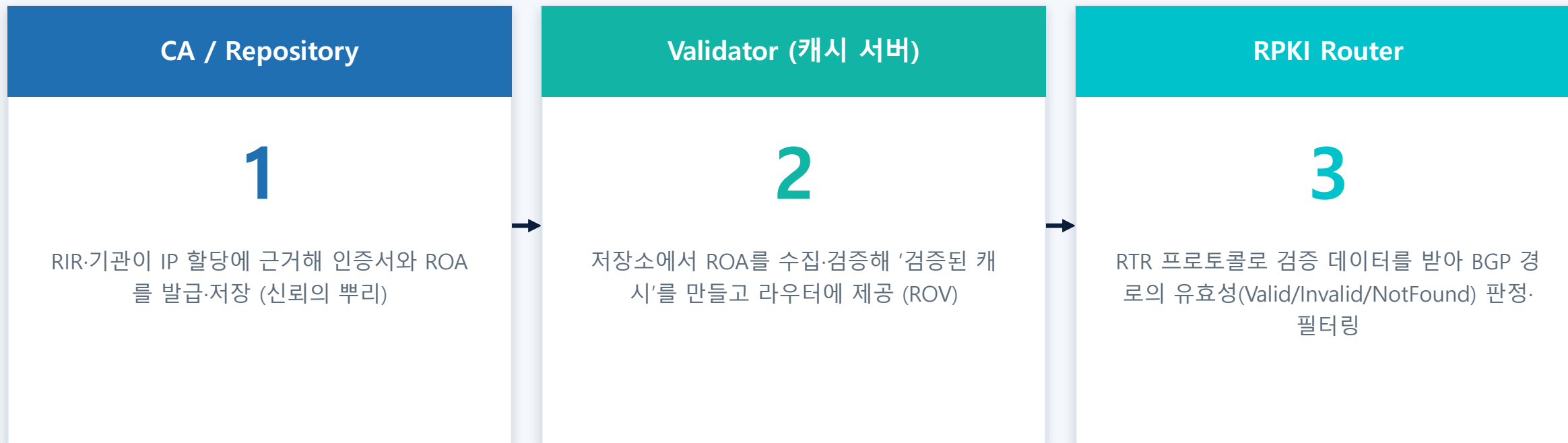
핵심 개념

인터넷 주소자원(IP/AS)을 X.509 공개키 인증서로 서명해, 해당 경로의 정당한 출처를 보증하는 보안 체계.

ROA(Route Origin Authorization): "이 IP 대역은 이 AS만 광고 할 수 있다"를 명시한 인증된 정보.

표준 RFC 6480·6482(ROA)·6810(RTR) 등 — 2011년부터 국제 표준화

서명 → 검증 → 라우터 적용의 3단계



라우터는 이웃에게서 받은 BGP 경로를 검증 데이터와 대조해, 운영자가 설정한 정책에 따라 'Invalid' 경로를 자동 차단한다.

검증하는 네트워크만이 가짜 경로를 막는다

RPKI 미적용

악의적인 경로 광고

가짜 사이트

검증 장치가 없어 악의적 경로 광고를 그대로 수용 → 트래픽이 가짜 목적지로

RPKI 적용

악의적 경로 광고

차단

정상 경로만 통과

정상 사이트

ROA로 검증 → 'Invalid' 경로를 자동 차단 → 정상 트래픽만 올바른 목적지로

기존 IRR 필터링의 한계를 넘어서

기존: IRR 기반 필터링

자율적·비정기적으로 갱신되는 등록 정보

→ 정확성 저하

수작업 필터(AS-path/IP) 의존

→ 오류·장애 가능성

출처의 '인증' 부재

→ 하이재킹 방어에 한계

전환



RPKI 기반 검증

암호학적 인증서로 출처를 보증

→ 높은 신뢰성

RTR로 자동 수집·검증·갱신

→ 사람 개입 최소화

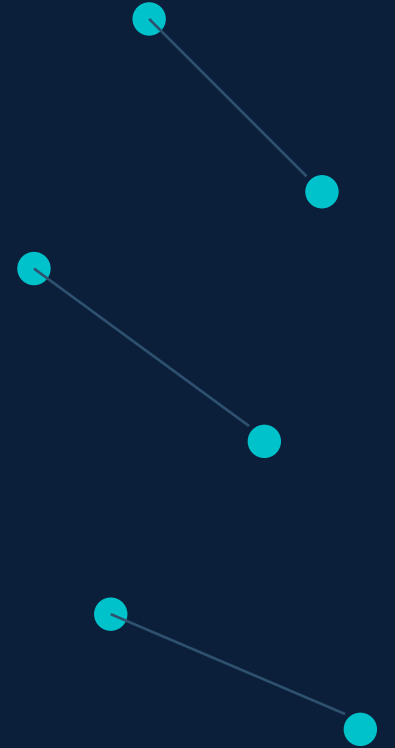
Invalid 경로 자동 차단

→ 하이재킹·유출 방어



글로벌 RPKI 확산과 정책 동향

절반을 넘어선 세계 — 의무화로 가는 주요국



세계 경로의 절반 이상이 RPKI로 보호된다

RPKI Valid IPv4 경로

53.9%

'25년 초 50.0% → 12월 53.9%

RPKI Valid IPv6 경로

60.1%

전년 대비 +4.7%p

RPKI 보호 목적지

약 75%

전 세계 IP 트래픽 중
RPKI 보호 대상 비중

5년간 약 3배 성장

2020년 이후 RPKI Valid IPv4 경로·주소공간 비중이 약 3배로 증가했다. 글로벌 표준은 '선택'이 아니라 '기본'으로 자리잡는 중이다. 다만 서명(ROA)에 비해 검증(ROV) 실적용은 아직 더디다는 점이 남은 과제다.

출처: Cloudflare Radar 2025 Year in Review ('25.12.2 기준)

권고를 넘어 '의무'로 — 라우팅 보안의 제도화

미국 백악관 ONCD

'인터넷 라우팅 보안 로드맵' 발표('24.9). RPKI를 성숙한 즉시 적용 가능 기술로 채택 권고, 민·관 협의체 구성

미국 FCC

BGP 보안 보고 의무화 추진('24.6 NPRM). 9개 대형 ISP는 연례 BGP 보안계획·분기 진척 보고 의무

네덜란드·EU

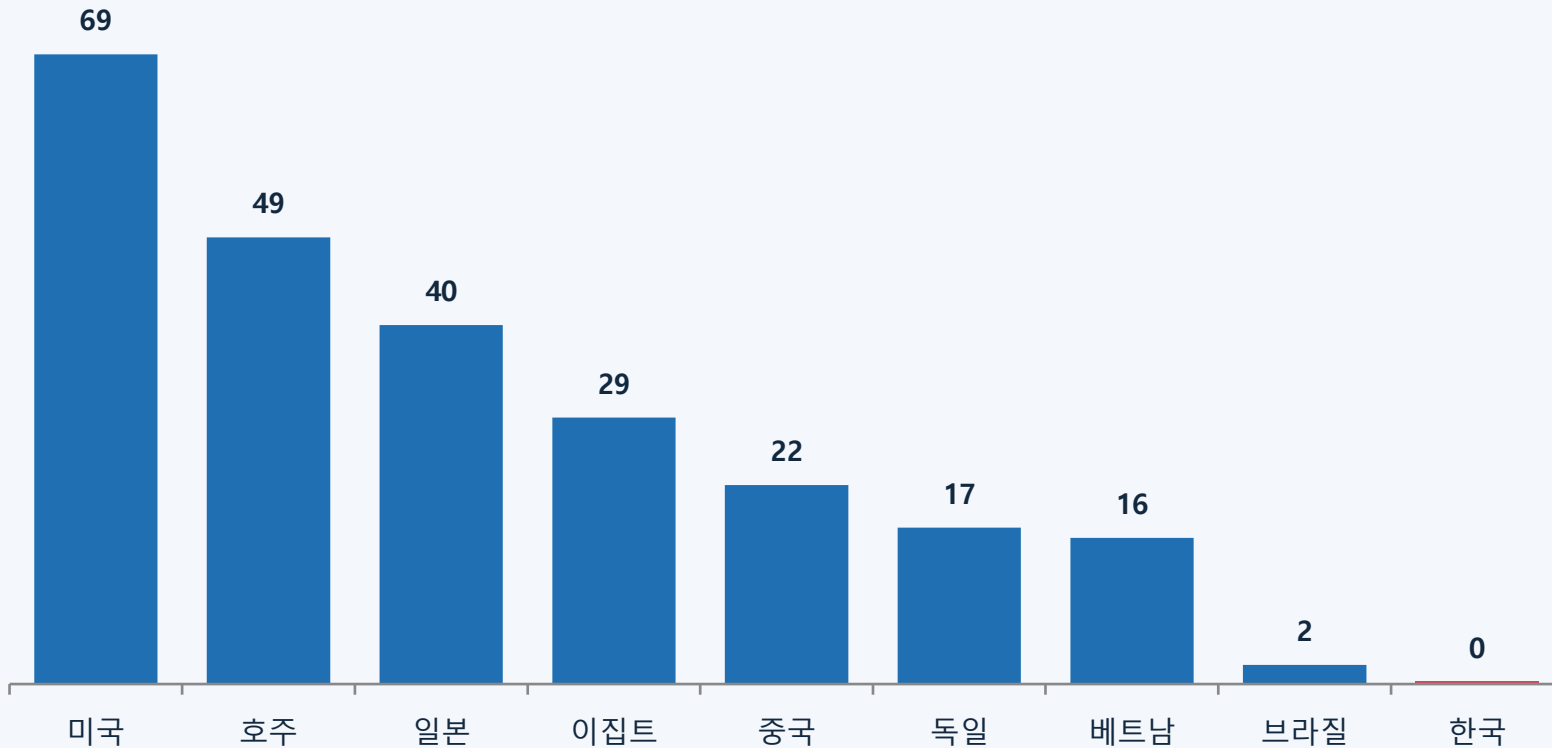
정부망 전반에 RPKI 적용 의무화 결정 등 유럽 전역으로 정부 주도 적용 확산

MANRS / RIR

ICANN·지역인터넷레지스트리(RIR)·MANRS가 모범사례·교육·툴을 제공하며 글로벌 참여 견인

출처: The White House ONCD Roadmap(2024.9) · FCC NPRM(2024.6) · Internet Society

주요국과 벌어진 한국의 격차



0.27%

한국 RPKI 적용률

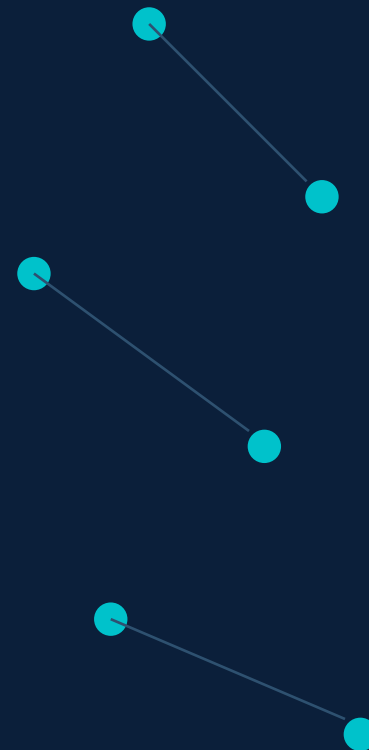
일본(39.56%)·중국(21.94%) 등 주변국과
비교해도 현저히 낮은 수준. OECD 38개
국 중 최하위권.

출처: 국가별 RPKI 적용(필터링) 현황, '23.11 기준 (최신 공개 비교치)

VI

국내 현황과 과제

최하위에서 전환점으로 — 그리고 AI 시대의 과제



왜 한국은 뒤처져 있는가

OECD 최하위권

0.27%

OECD 38개국 중 최하위 수준의 RPKI 적용률('23.11). AI 시대 핵심 인프라를 운영하는 나라로서 시급한 개선 과제.

도입 걸림돌

1

인식 부족

ISP·서비스 제공자의 RPKI 필요성에 대한 인식 미흡

2

장애 우려

운영 중 장비 구성 변경에 따른 서비스 장애 부담

3

검증 인프라 비용

Validator·라우터 도입·운영 비용 및 전문 인력 부담

4

예산·제도 공백

도입 확대를 뒷받침할 예산·제도적 동인 부족

출처: 보안뉴스(2024) · KISA 국내 RPKI 도입 현황 분석

KISTI, 국내 최초 RPKI 전면 도입 (2025.7)

국가과학기술연구망(KREONET)에 RPKI 전면 도입

한국과학기술정보연구원(KISTI)이 KISA와 협력해 연구망 ASN에 ROA를 발급하고 검증 체계를 구축 — 국내 첫 사례이자 MANRS 이행의 일환

국내 최초

운영망 전반에 RPKI를 전면 적용한 첫 사례

민·관 협력

KISTI-KISA 공동 구축으로 레퍼런스 확보

국제 정합

MANRS 등 글로벌 라우팅 보안 규범 이행

하나의 선도 사례가 국내 확산의 출발점 — 이제 ISP·공공·민간으로 '검증(ROV)'을 넓혀야 할 때.

출처: KISTI 보도자료 “국가과학기술연구망에 국내 최초 라우팅 인증(RPKI) 전면 도입”(2025.7.8)

인식 제고에서 체계 구축으로

그동안의 노력

- 도입 확대를 위한 인식 제고 회의 운영
- RPKI 시스템 구축 기술 교육 개최
- 구축 논의를 위한 협력 채널 개설
- KISTI·KREONET 선도 적용(레퍼런스)

향후 계획

- 보급 확대를 위한 예산 확보 추진
- 테스트베드 구축 및 구축 가이드 배포
- RPKI 보급 + BGP 모니터링 체계 중장기 구축
- ROA 발급에서 ROV 검증까지 단계적 확산

AI 시대, 신뢰할 수 있는 경로가 곧 경쟁력

1 AI는 경로 위에서 작동한다

트래픽 폭증·데이터센터 의존 심화로, 경로의 신뢰성이 AI 서비스 품질·안보와 직결된다

2 서명을 넘어 검증으로

ROA 발급만으로는 부족 — 경로를 받는 모든 네트워크의 ROV 검증·필터링이 핵심이다

3 집단적 참여가 본질

라우팅 보안은 한 기관의 문제가 아니라 ISP·공공·민간의 공동 행동으로 완성된다

4 지금이 골든타임

KISTI 선도 사례를 발판으로 제도·예산·교육을 결합해 국내 확산을 가속해야 한다

감사합니다

라우팅 인증(RPKI) 확산으로 완성하는 AI 신뢰 인프라

한국인터넷진흥원(KISA) · 인터넷주소보호팀 · KRNET 2026