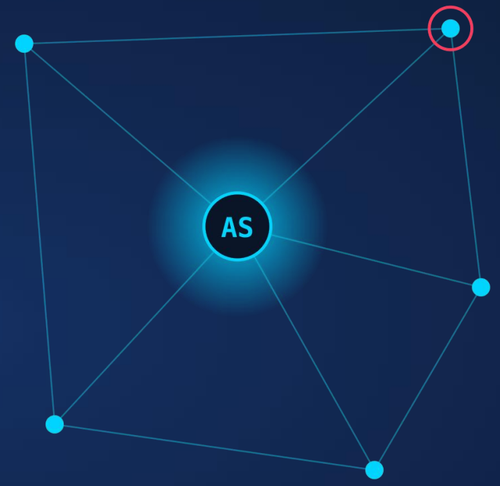
KOREA INTERNET GOVERNANCE FORUM · CYBERSECURITY TRACK

인터넷 거버넌스 · 사이버 안보 정책 세션



경계 없는 안보 위협의 시대, RPKI와 AI를 통한 국가 라우팅 체계의 사이버 복원력 강화

디지털 영토의 주권을 지키기 위한 라우팅 인프라 전략

발표자 : ㈜아레스 사이버전략연구소 대표이사 이화영

사이버 공간에는 국경이 없지만, 안보의 책임에는 국경이 있습니다

데이터는 국경을 자유롭게 넘나들지만, 국가는 자국을 통과하는 트래픽의 **경로·목적지·안전성**을 스스로 검증할 수 있어야 합니다.

01

라우팅은 여전히 '신뢰 기반'

BGP는 30년 전 설계된 프로토콜.
경로 광고를 검증 없이 서로 신뢰합니다.

02

한 번의 오류가 글로벌 규모 사고로

수 분 내 전 세계 트래픽 15%가 특정 국가로 우회된 사례가 이미 존재합니다.

03

디지털 영토의 주권 문제

라우팅 인프라를 통제하지 못하면 국가 데이터의 '길'을 잃습니다.

BGP는 왜 하이재킹에 무너지는가

인터넷의 '경로 안내판'인 BGP(Border Gateway Protocol)는 검증 없는 신뢰로 작동합니다.

HOW A HIJACK HAPPENS

타 AS가 "이 IP 대역은 내 소유"라고 거짓 광고 → 이웃 라우터가 그대로 신뢰 → 전 세계 경로 오염

THREE STRUCTURAL FLAWS

인증 없는 경로 광고

누가 어떤 IP 대역의 정당한 소유자인지 확인할 표준 인증 계층이 원래는 없었습니다.

전 세계로 즉시 전파

잘못된 광고는 수 분 안에 이웃 AS들에게 전파되어 글로벌 경로 테이블을 오염시킵니다.

실수와 공격의 구분 곤란

운영자의 오설정도, 국가 단위의 의도적 우회도 겉으로는 동일한 BGP 광고로 보입니다.

03

이미 일어난 일입니다.

가정이나 시나리오가 아닙니다. 세 건의 실제 사건이 전 세계 라우팅 체계의 취약성을 이미 증명했습니다.

THREE INCIDENTS

CASE 01

Russia · Rostelecom

2020–2022 · 200+ 네트워크 우회

CASE 02

Amazon Route 53

2018 · DNS 하이재킹 · 암호화폐 탈취

CASE 03

China Telecom

2010 · 18분 동안 전 세계 15%

러시아 로스테레콤이 Apple · Cloudflare · Google의 경로를 가져갔다

2020년 4월 · 2022년 우크라이나 전쟁 국면 재발 | AS12389 ROSTELECOM

01 무엇이 일어났는가

200개 이상의 글로벌 CDN·클라우드 경로가 러시아 망을 경유

- Apple, Google, Amazon, Cloudflare, Facebook, Akamai 등 200+ 네트워크의 IP 대역이 하이재킹
- 2022년 우크라이나 전쟁 직후에도 트위터·SNS 경로에 대한 러시아 ISP의 BGP 하이재킹이 관측
- 우크라이나 점령지 인터넷 트래픽이 러시아 인프라로 재라우팅

02 왜 국가 안보 문제인가

전시 상황에서 통신·정보 흐름을 적성국이 좌우

- 트래픽 감청·검열·차단이 국가 단위로 가능
- '어느 나라를 지나가는가'가 곧 '누가 우리 대화를 듣는가'의 문제
- 전쟁·제재·외교 갈등 국면에서 라우팅이 무기화되는 실증 사례

03 RPKI가 있었다면

잘못된 광고를 이웃 AS가 거부했을 것

- Apple·Google 등이 발행한 ROA로 정당 소유자가 미리 등록되어 있음
- 로스테레콤이 광고해도 RPKI 검증 라우터는 **invalid** 판정으로 자동 폐기
- 우회 규모가 근본적으로 축소되고, 국가 단위 개입이 어려워짐

자료: MANRS · Kentik · SecurityWeek · CPO Magazine · Cloudflare 공개 분석

Amazon Route 53의 DNS 경로가 가짜 서버로 연결되었다

2018년 4월 24일 · MyEtherWallet 이용자 · 약 US$ 150,000 상당 이더리움 탈취

ATTACK CHAIN

STEP 1 · BGP 광고
공격자가 Amazon Route 53의 IP 대역을 자신이 소유한 것처럼 광고

↓

STEP 2 · 경로 오염
이웃 AS들이 검증 없이 광고를 신뢰 → 전 세계 DNS 질의가 공격자 네임서버로 흐름

↓

STEP 3 · DNS 리디렉션
myetherwallet.com 이용자가 정교하게 위조된 피싱 사이트로 유도

↓

STEP 4 · 자산 탈취
개인 지갑 크리덴셜 입력 → 이더리움 자산 이체 · 약 US$ 150,000 손실

왜 국가 안보 문제인가

BGP 하이재킹이 금융·인증 시스템 공격의 관문이 된다

똑같은 수법으로 전자정부·본인인증·공공 클라우드 도메인이 위조 서버로 유도될 수 있음

RPKI가 있었다면

Amazon의 ROA로 위조 광고 즉시 차단

DNS 리디렉션 자체가 성립하지 못하고, 피싱 체인 초입에서 공격이 무력화됨

자료: Internet Society · ThousandEyes · Cloudflare · Kentik · WeLiveSecurity

18분 동안, 전 세계 트래픽의 15%가 한 나라로 흘러갔다

2010년 4월 8일 · China Telecom AS23724 · 약 50,000개 IP 접두어 잘못 광고

INCIDENT AT A GLANCE

DURATION

18분

전 세계 라우팅 테이블 오염 지속 시간

GLOBAL TRAFFIC

15%

중국을 경유하도록 우회된 인터넷 트래픽

PREFIXES

~50,000

잘못 광고된 IP 접두어(prefixes) 수

IMPACT SCOPE

美 정부·군
NASA·상원

우회 대상에 포함된 주요 기관

왜 국가 안보 문제인가

美 국방·정부·상원 사이트 트래픽이 수 시간 동안 해외 통신사 서버 경유

18분은 짧아 보이지만, 실효적 관측·수집·기록에는 충분한 시간. 국가 라우팅 통제권의 결여가 그대로 안보 공백으로 노출된 사례.

RPKI가 있었다면

5만 개 접두어 대부분이 검증 단계에서 invalid 판정

이웃 AS의 RPKI validator가 광고를 자동 폐기 → 우회 규모가 몇 자릿수 축소

자료: Citizen Lab · Ars Technica · The Atlantic · National Defense Magazine

RPKI, 라우팅에 '신원증명'을 붙이다

Resource Public Key Infrastructure · IP 대역의 정당한 소유자를 공개키로 인증하는 국제 표준 체계

HOW IT WORKS · 3 STEPS

01 ROA 발행 · 원본 인증

지역 인터넷 등록기관(RIR)이 IP 소유자에게 인증서 발급 →
소유자는 "이 IP 대역은 이 AS만 광고 가능"이라는 ROA(Route Origin Authorization) 등록

02 Validator · 실시간 검증

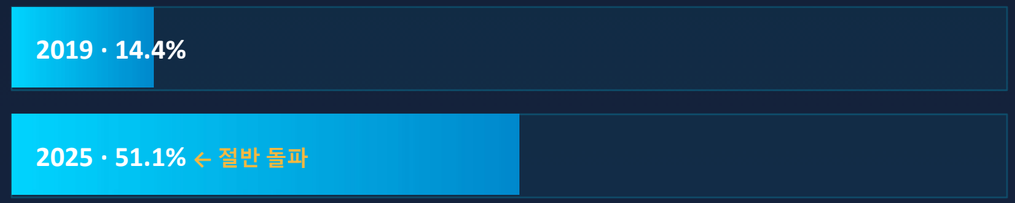
각 AS의 RPKI validator가 들어오는 BGP 광고를 ROA와 대조해
Valid · Invalid · NotFound 셋 중 하나로 판정

03 ROV · 잘못된 광고 폐기

Invalid 판정 광고는 라우팅 테이블에서 자동 폐기(ROV) →
잘못된 경로가 이웃 AS로 전파되기 전에 차단

GLOBAL ADOPTION · 2019 → 2025

RPKI 검증 유효 경로가 6년 만에 3배 이상 증가



IPv4 기준 · RPKI ROA로 보호되는 유효 경로 비율
출처: LACNIC · IIJ Research (imc2025)

그러나 절반은 여전히 무방비. 국가 단위의 배포 격차가 곧 안보 격차.

RPKI가 문(門)을 만든다면, AI는 그 문을 지키는 눈이다

RPKI = 정적 인증 계층 · AI = 실시간 이상탐지 · 예측 · 대응 자동화

LAYER 01

RPKI · 자물쇠

"이 IP 대역은 누가 광고할 수 있는가"에 대해
수학적으로 검증 가능한 답을 제공.
단, 등록된 규칙에 대해서만 판정 가능.

LAYER 02

AI · 감시자

글로벌 BGP 스트림을 실시간 학습하여
비정상 경로 · 새로운 우회 패턴 · NotFound 영역의
이상 신호를 조기 탐지.

WHERE AI ADDS VALUE ON TOP OF RPKI

A · DETECT

이상 경로 조기 탐지

ROA 미등록(NotFound) 영역에서도 학습된 패턴으로 비정상 경로 식별

B · PREDICT

공격 가능성 예측

특정 AS의 이상 광고 이력·지정학 리스크를 결합해 사전 경보 발행

C · RESPOND

대응 자동화

ROA 임시 갱신·필터 정책 배포 등 대응 절차를 자동 트리거

국가 라우팅 체계, 네 개의 축으로 세운다

기술만으로는 부족합니다. 정책·거버넌스·인재·다자협력이 함께 움직여야 합니다.

AXIS 01

RPKI 도입 의무화·인센티브

- 공공·금융·국방 관련 ISP 우선 적용
- 정부 조달 요건에 ROA 발행·ROV 수행 포함
- 중소 ISP 배포 지원 예산 확보

AXIS 02

국가 라우팅 모니터링 센터

- 국가 단위 24/7 BGP 관측 체계
- AI 기반 이상 경로 실시간 경보
- KISA·통신사업자·CERT 공동 운영

AXIS 03

국제 다자 협력 강화

- MANRS · APNIC · IETF 표준화 참여
- 우방국 간 이상 광고 정보 공유 협정
- 인터넷 파편화에 대응하는 공동 원칙

AXIS 04

차세대 라우팅 인재

- 대학·특성화고 라우팅 보안 커리큘럼
- 청년 세대 대상 BGP·RPKI 실습 프로그램
- 국가 인증 라우팅 엔지니어 트랙

디지털 영토의 주권은 라우팅 한 줄에서 시작됩니다

이 자리에 계신 정부·학계·기업·청년 세대에게 세 가지를 요청드립니다.

01

다자 협력 · 파편화를 막는다

인터넷은 국경으로 쪼갤 수 없는 공유 자산.
다자 표준과 공동 원칙에 우리의 목소리를 얹어야 합니다.

02

RPKI 도입 · 절반을 넘어선다

글로벌 51%를 넘긴 지금이 결단의 순간.
공공·금융·국방 트래픽부터 예외 없이 검증 체계 안으로.

03

AI 모니터링 · 지식을 공유한다

이상 경로 탐지 모델과 위협 인텔리전스를
국가 간·산업 간 공유해야 진짜 복원력이 완성됩니다.

사이버 복원력은 선택이 아니라 주권의 조건입니다.

라우팅의 신뢰가 국가의 복원력이다

오늘 나눈 문제의식이 정책 결단으로,
결단이 다시 일상의 인프라로 이어지길 바랍니다.

감사합니다.

㈜아레스 사이버전략연구소 02)6489-9100 / HP. 010-6651-9000(대표이사 이화영)