UCLab
Ubiquitous Computing Laboratory
Meijo University

V2X通信における安全性と接続性を確保するオーバレイネットワーク技術

鈴木　秀和
名城大学 情報工学部　准教授

Aug. 22, 2024 MEET UP CHUBU Vol. 46 モビリティ with Map NAGOYA
@ナゴヤ イノベーターズ ガレージ

researchmap

自己紹介

専門：情報通信ネットワーク，ユビキタスコンピューティング

日本学術振興会特別研究員DC2・PDを経て、2010年より名城大学にて教育・研究に従事。モバイルネットワーク、スマートホーム、スマートコミュニティ分野における研究開発を推進。2015年より東北大学電気通信研究所共同研究員として「ユビキタスシステムの実世界導入に向けた実証的研究」プロジェクトに若手研究者として参画。2020年より名古屋大学社会創造機構モビリティ社会研究所特任准教授を兼職（2023年より客員准教授）。学会活動や自治体における各種委員の他、シビックテックや技術系コミュニティ、イノベーション創出活動の運営など多数。IBM Champions 2019-2022（米国IBM公式外部アドボケイト）に認定。2021-2022年 総務省東海総合通信局「地域自営IoT無線システムの社会実証に向けた調査検討会」副主査。

Code for NAGOYA

UDC AICHI

Node-RED

IBM Champion 2022

鈴木　秀和

CASE

現在の自動車産業における4つの重要なトレンド

connected

shared &
services

autonomous

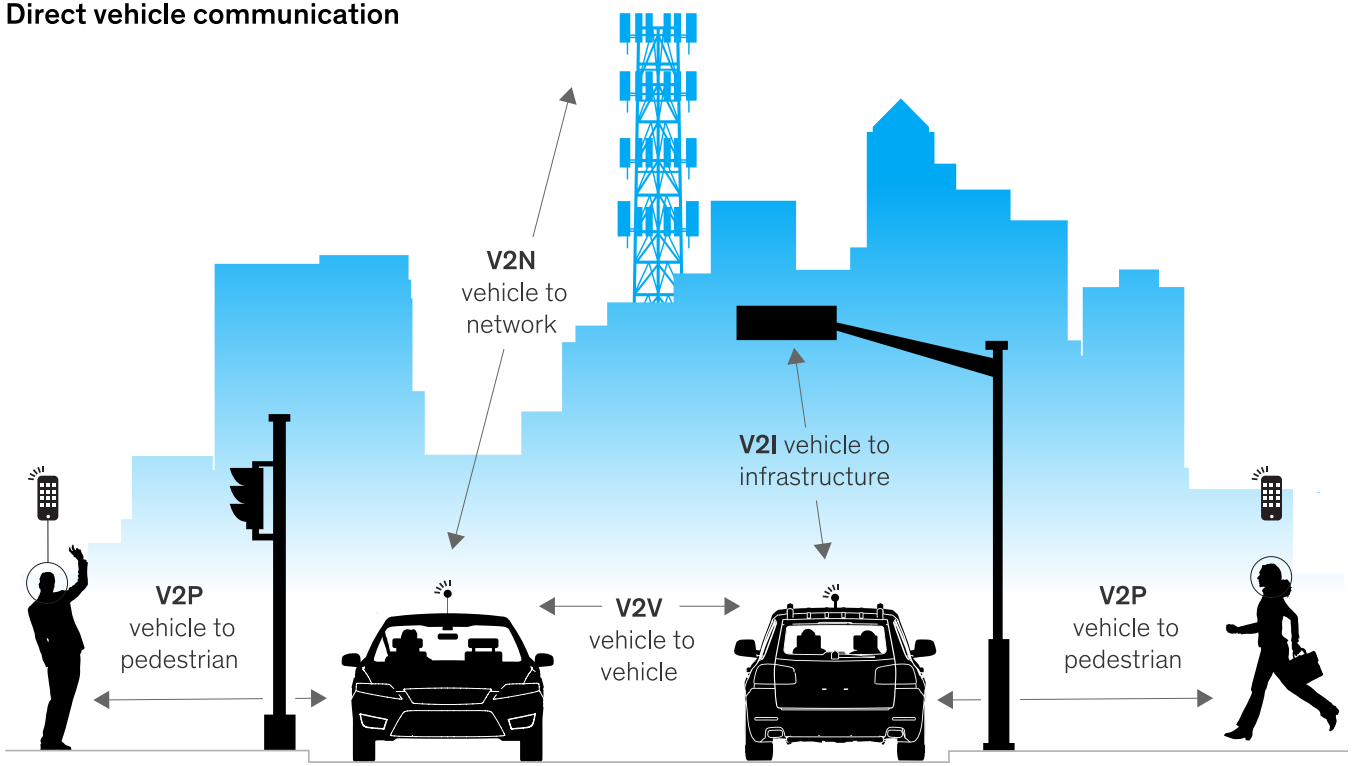
electric

DAIMLER Annual Report 2016.
https://group.mercedes-benz.com/documents/investors/reports/annual-report/daimler/daimler-ir-annualreport-2016.pdf

V2X（Vehicle-to-Everything）

Ubiquitous connectivity can facilitate automation and autonomy among cars on the road.

Direct vehicle communication



McKinsey & Company

K. Heineke, A. Ménard, F. Södergren and M. Wrulich, “Development in the mobility technology ecosystem—how can 5G help?” Automotive & Assembly Insights, McKinsey & Company, Jun. 2019.

V2V　自動車

- 追従走行
- 緊急車両存在通知
- 出会い頭注意喚起
- 右折時注意喚起

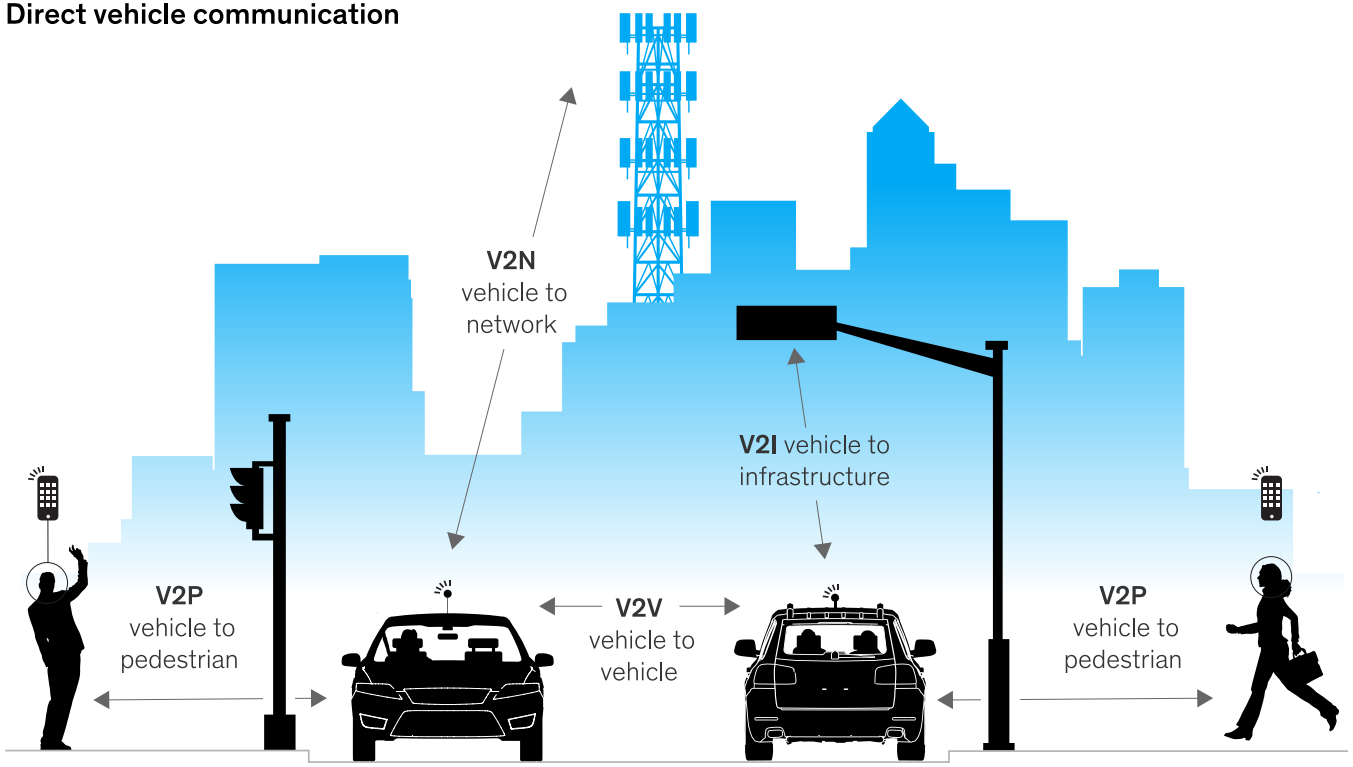
V2I　インフラ

- 右折時注意喚起
- 赤信号注意喚起
- 信号待ち発進準備案内

V2X（Vehicle-to-Everything）

Ubiquitous connectivity can facilitate automation and autonomy among cars on the road.

Direct vehicle communication



McKinsey & Company

K. Heineke, A. Ménard, F. Södergren and M. Wrulich, “Development in the mobility technology ecosystem—how can 5G help?” Automotive & Assembly Insights, McKinsey & Company, Jun. 2019.

V2P　歩行者

- 歩行者の携帯端末の位置情報や移動速度情報などを共有
- 見通し外の歩行者検知

V2N　ネットワーク

- 各種オンラインサービス（駐車場検索，ビデオストリーミング，ARナビゲーション等）
- 遠隔操縦
- 自動運転

V2X通信技術

DSRC（Dedicated Short Range Communications）

- IEEEが策定した無線通信方式（IEEE802.11p）
- 通信可能距離は通常400～500m（最大1kmまで）
- 非常に低遅延（約2ms）で安全性が重要な用途に最適
- 独自の通信システムを使用するため，専用のインフラ整備が必要

C-V2X（Cellular V2X）

- 3GPPによって標準化された無線通信方式（LTE-V2X，5G NR-V2X）
- DSRCより広範囲をカバー．特に障害物がある環境で優れた性能を発揮
- 5G NR-V2XはDSRCとほぼ同等で，数Gbpsのスループットを実現可能

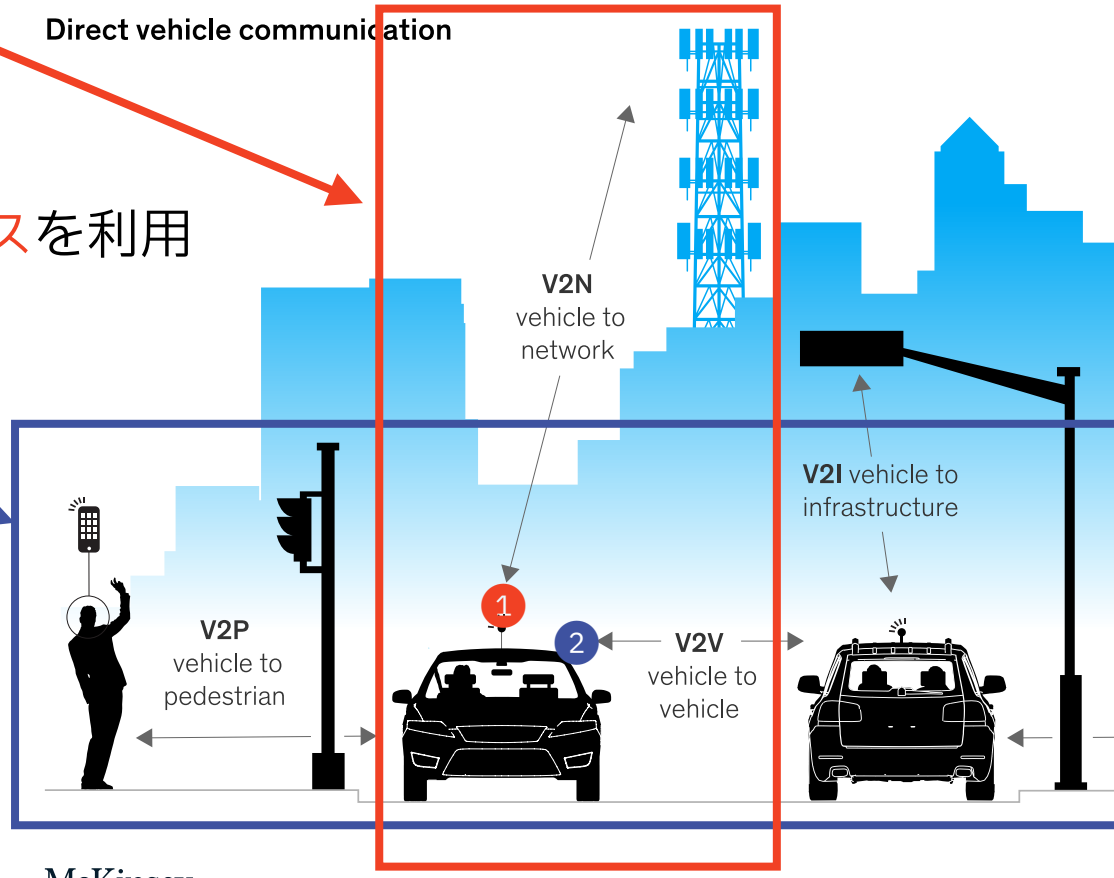
C-V2X通信インタフェースとIPv6通信

Uu（ネットワーク通信：V2N）

- 基地局に介してセルラーネットワークに接続
  （IPv6オンリー）
- 自動生成される❶グローバルユニキャストアドレスを利用
  （プライバシー保護の場合，定期的に更新*）

PC5（直接通信：V2V，V2I，V2P）

- 非IPまたはIPv6で通信
- 自動生成される❷リンクローカルアドレスを利用

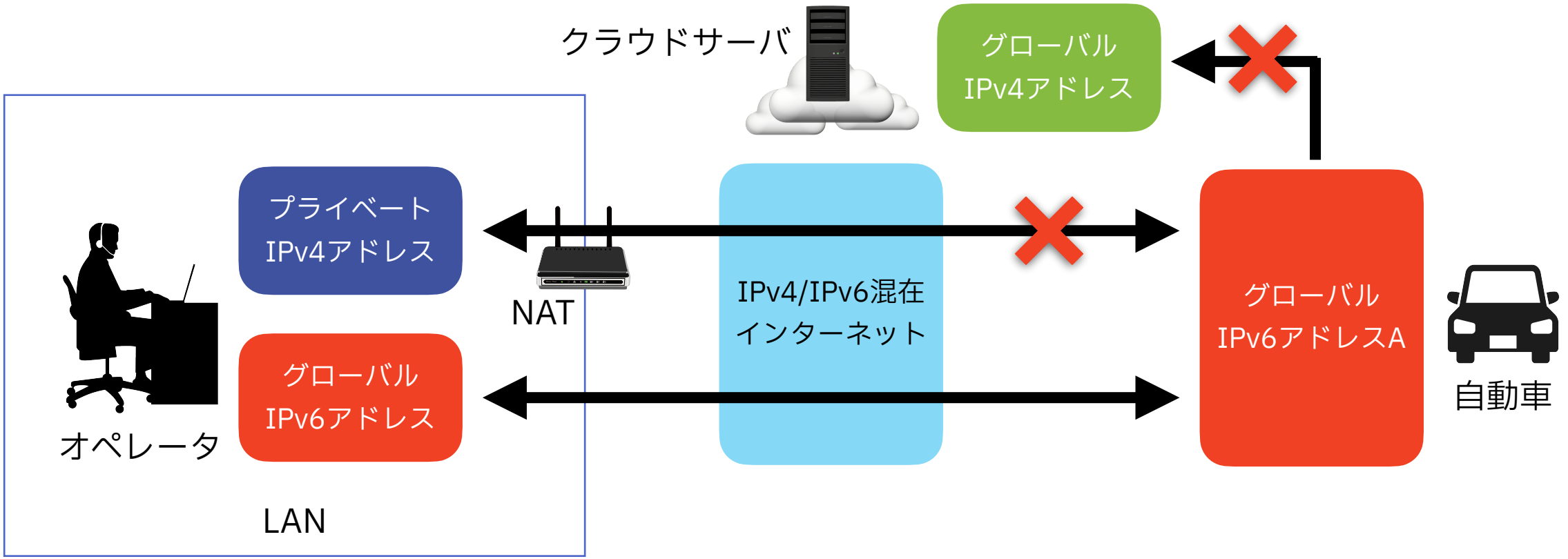


* J. Jeong, “IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases” RFC 9365, IETF, Mar. 2023.

McKinsey & Company

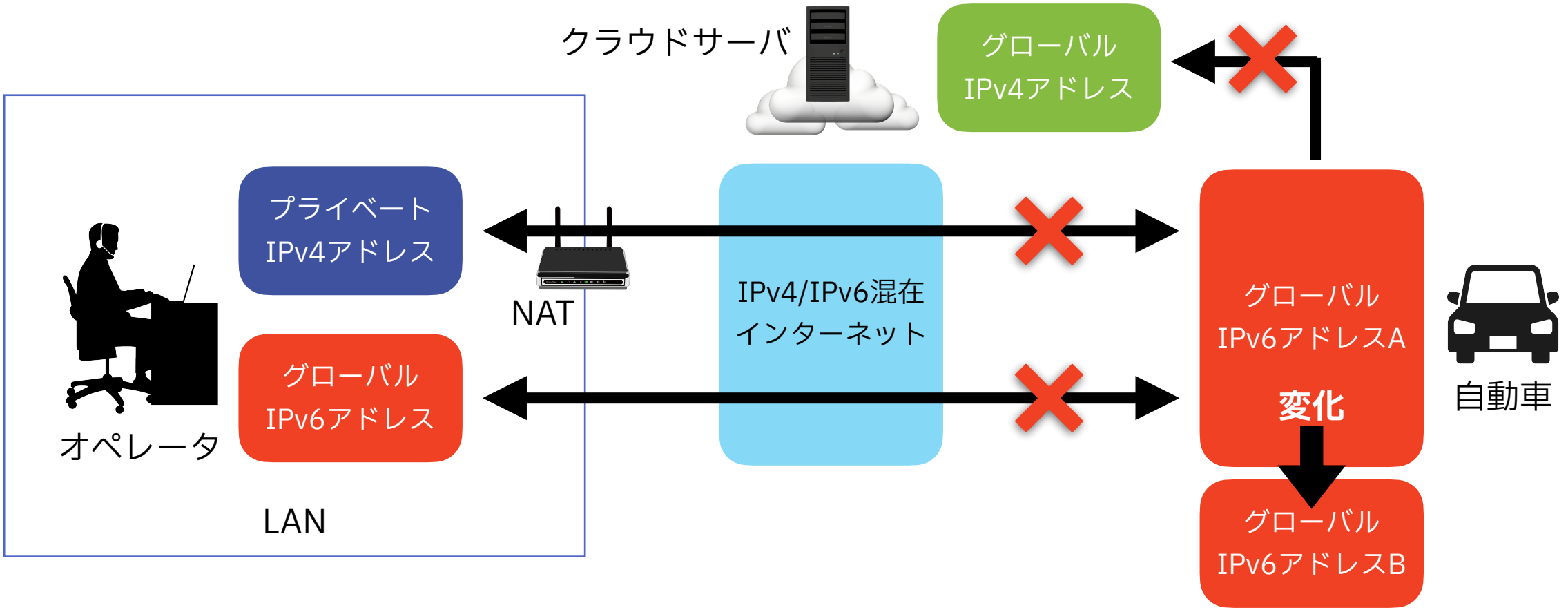
接続性に関する課題

- IPv4とIPv6間の互換性はなく，直接通信は不可能



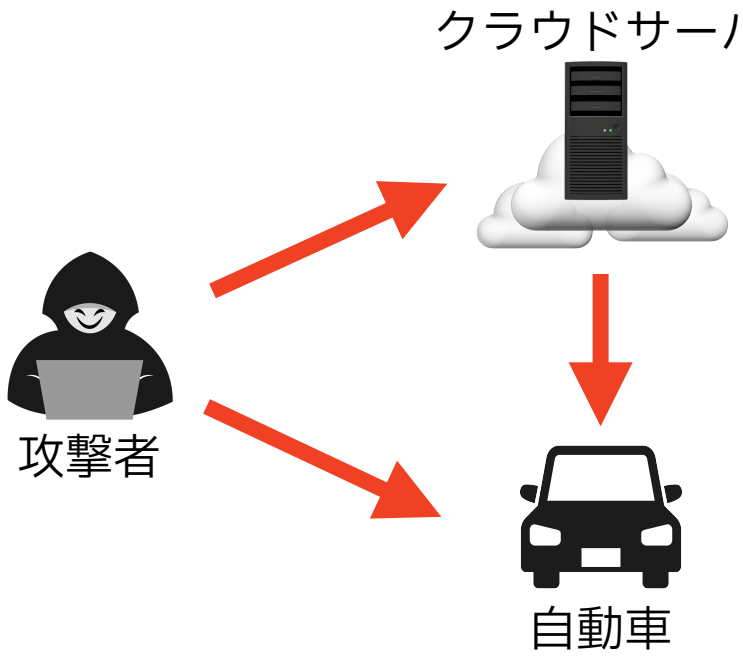
接続性に関する課題

- IPアドレスが変化すると，通信が切断されてしまう



安全性に関する課題

- **不特定多数の相手とIPv6通信するため，確実な認証が必要**
- **データの機密性とプライバシーの確保のため，暗号化は必須**



- C&Cサーバへの不正ログインによる
  コネクテッドカーの遠隔制御（2017）
- DDoS攻撃によるクラウドインフラへの攻撃

- Jeep Cherokeeのリモートハッキング（2015）
- Tesla Model Sのハッキング（2016）
- Spoofing攻撃（例：偽のメッセージを送信）

愛知工業大学・内藤克浩教授と共同開発

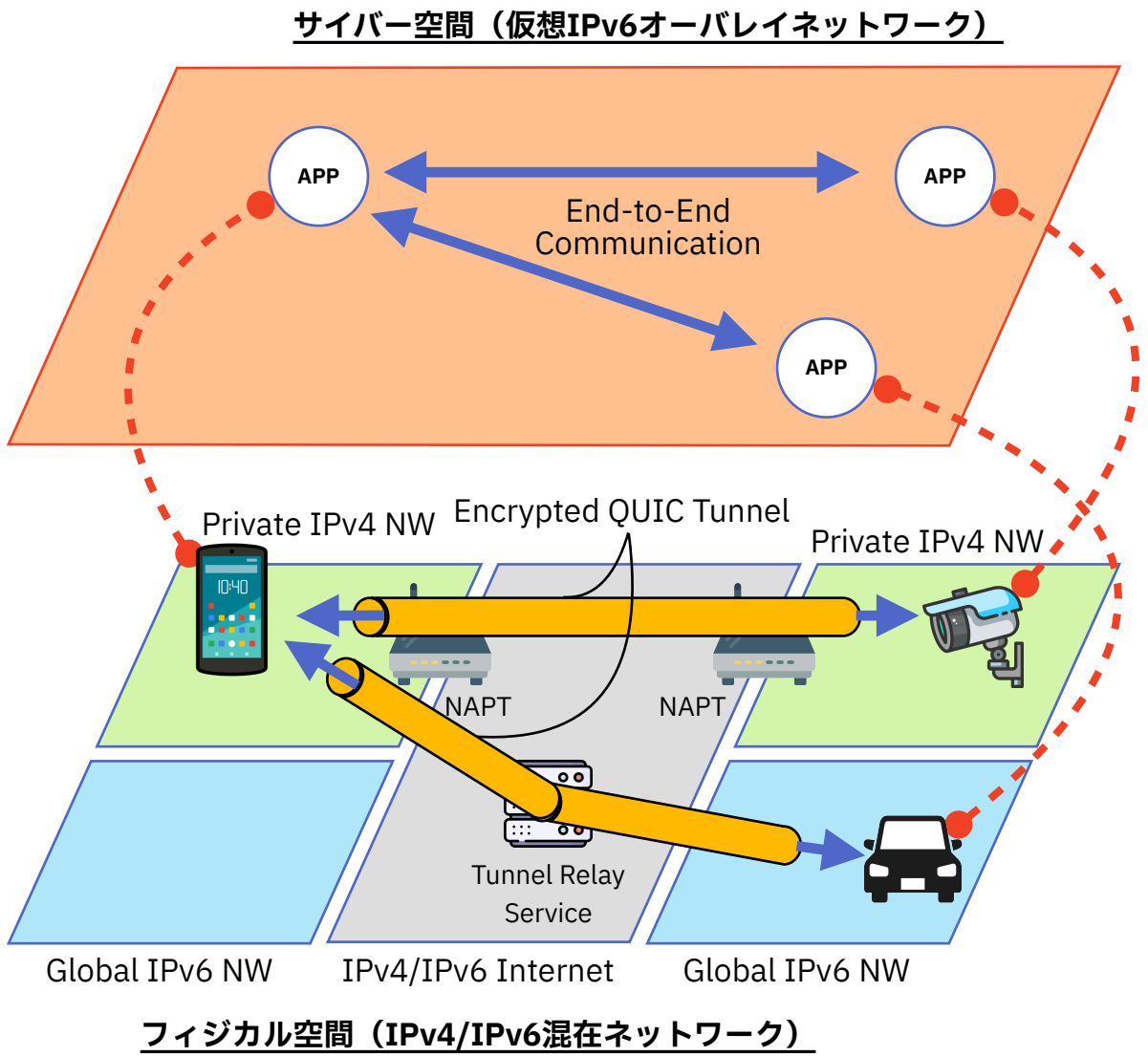
CYPHONIC（Cyber Physical Overlay Network over Internet Communication）

IPv4/IPv6混在環境でセキュアなオーバレイネットワークを構築する技術

- **通信接続性の実現**
  - エンドデバイスの接続ネットワーク環境に応じた暗号化通信経路の確立
- **移動透過性の実現**
  - 仮想IP通信により，実IPアドレスの変化をアプリケーションから隠蔽
- **機密性・完全性の実現**
  - ゼロトラストセキュリティに基づく全デバイスの認証を実施
  - 通信を行うエンドデバイスのみが知りうる共通鍵でデータを暗号化

CYPHONICの基本原理

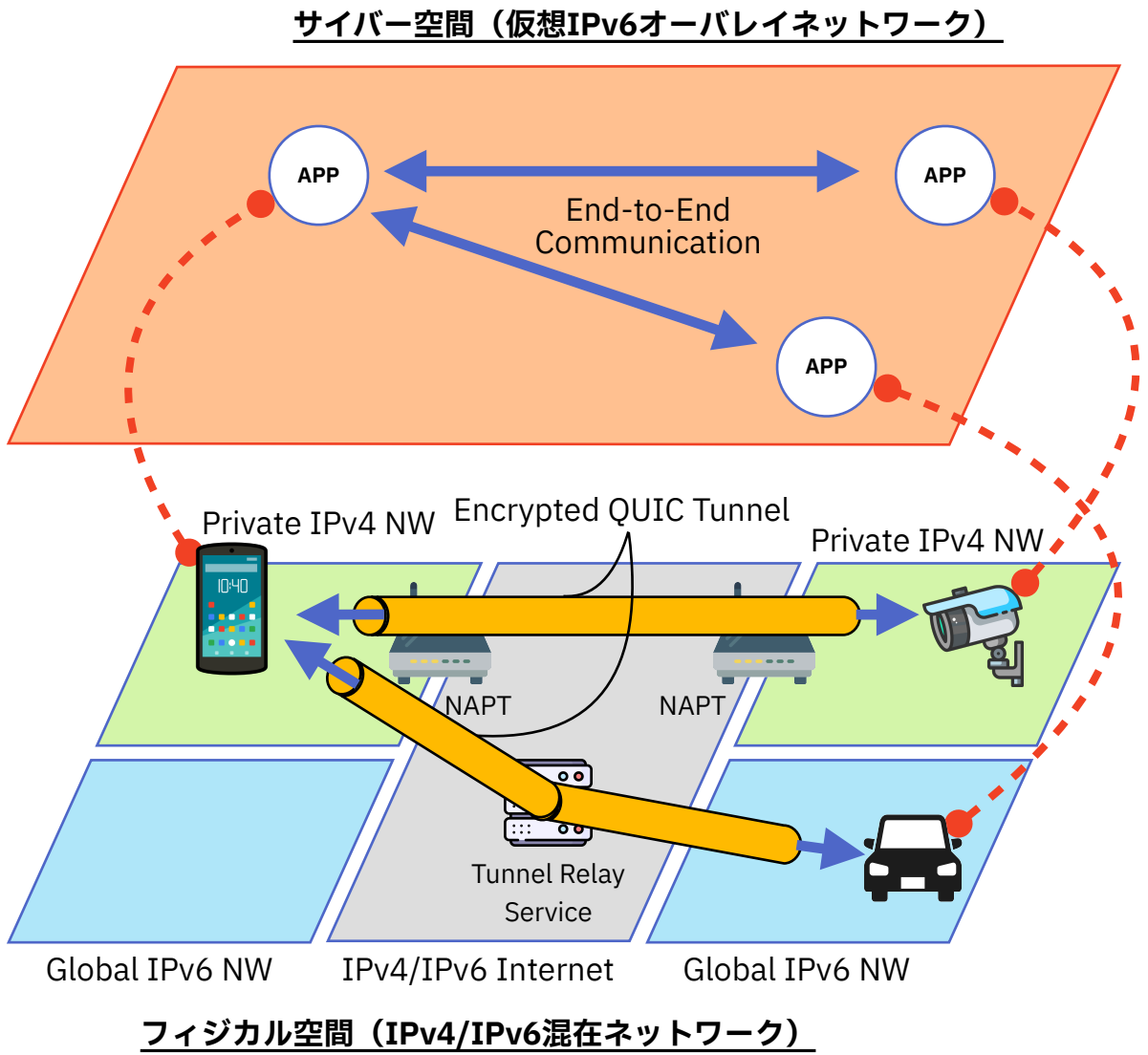
- 変化しない仮想IPv6アドレスを導入
- デバイス起動時に仮想IPv6オーバレイネットワークに参加
- 通信開始時に実ネットワーク上で通信相手デバイスとの間に暗号化通信トンネルを動的に構築
- アプリケーションはサイバー空間で直接通信し、そのパケットはフィジカル空間で暗号化通信トンネルを通じて伝送
- 実IPv6アドレスが変化したら，暗号化通信トンネルを再構築後，通信を継続



S. Horisaki, et al., “CYPHONIC-over-QUIC: Secure End-to-End Communication Architecture Traversing Firewalls/NATs”, Journal of Information Processing, Vol.32, pp.509-519, 2024.

CYPHONICの基本原理

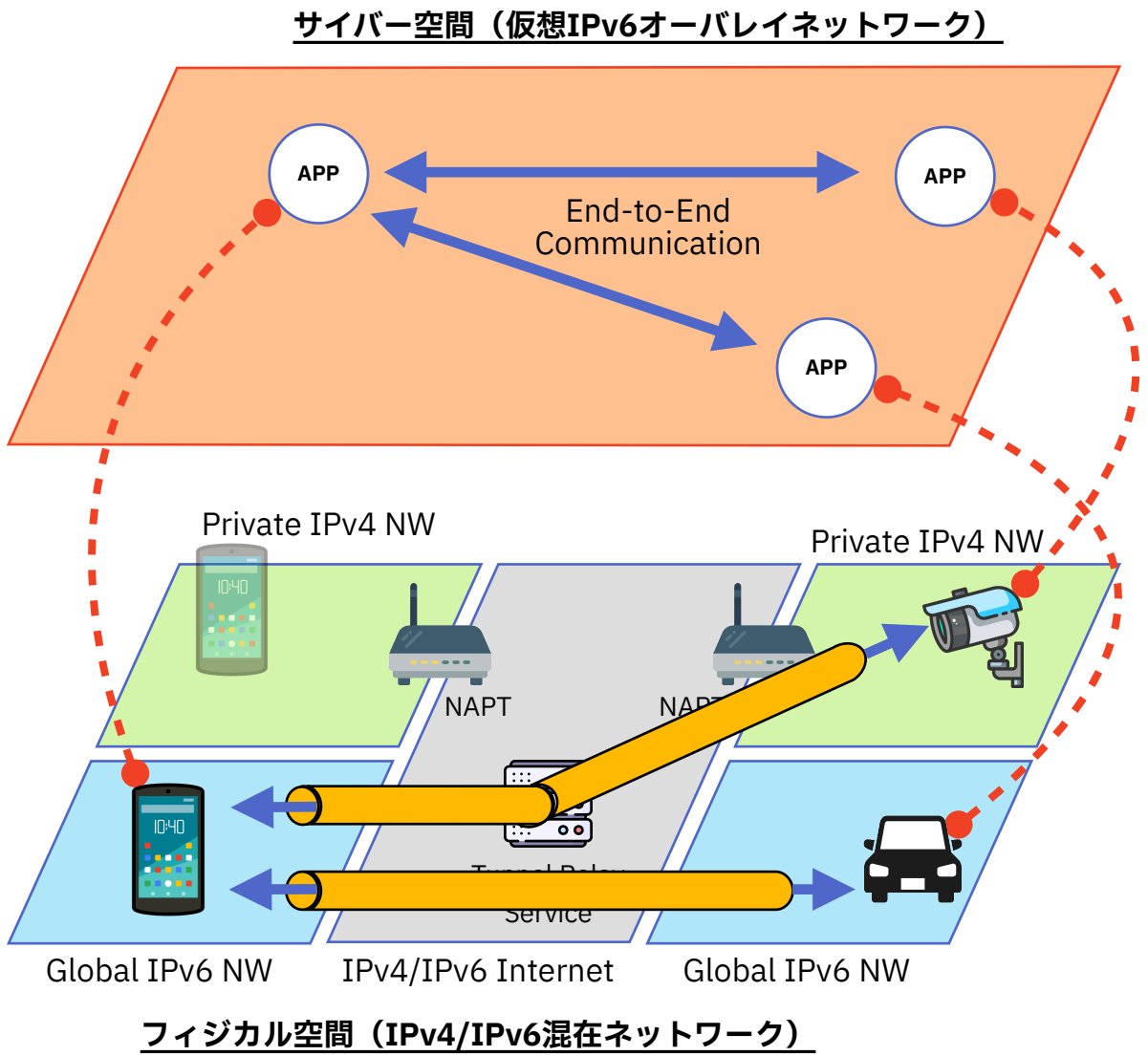
- 変化しない仮想IPv6アドレスを導入
- デバイス起動時に仮想IPv6オーバレイネットワークに参加
- 通信開始時に実ネットワーク上で通信相手デバイスとの間に暗号化通信トンネルを動的に構築
- アプリケーションはサイバー空間で直接通信し、そのパケットはフィジカル空間で暗号化通信トンネルを通じて伝送
- 実IPv6アドレスが変化したら，暗号化通信トンネルを再構築後，通信を継続



S. Horisaki, et al., “CYPHONIC-over-QUIC: Secure End-to-End Communication Architecture Traversing Firewalls/NATs”, Journal of Information Processing, Vol.32, pp.509-519, 2024.

CYPHONICの基本原理

- 変化しない仮想IPv6アドレスを導入
- デバイス起動時に仮想IPv6オーバレイネットワークに参加
- 通信開始時に実ネットワーク上で通信相手デバイスとの間に暗号化通信トンネルを動的に構築
- アプリケーションはサイバー空間で直接通信し、そのパケットはフィジカル空間で暗号化通信トンネルを通じて伝送
- 実IPv6アドレスが変化したら，暗号化通信トンネルを再構築後，通信を継続



S. Horisaki, et al., “CYPHONIC-over-QUIC: Secure End-to-End Communication Architecture Traversing Firewalls/NATs”, Journal of Information Processing, Vol.32, pp.509-519, 2024.

通信開始時の処理

アプリケーションが通信相手側ノードの名前解決（DNS処理）をトリガーとして，経路選択・トンネル構築処理を動的に開始

- 通信開始側・通信相手側ノードの接続ネットワークの組み合わせで経路を決定

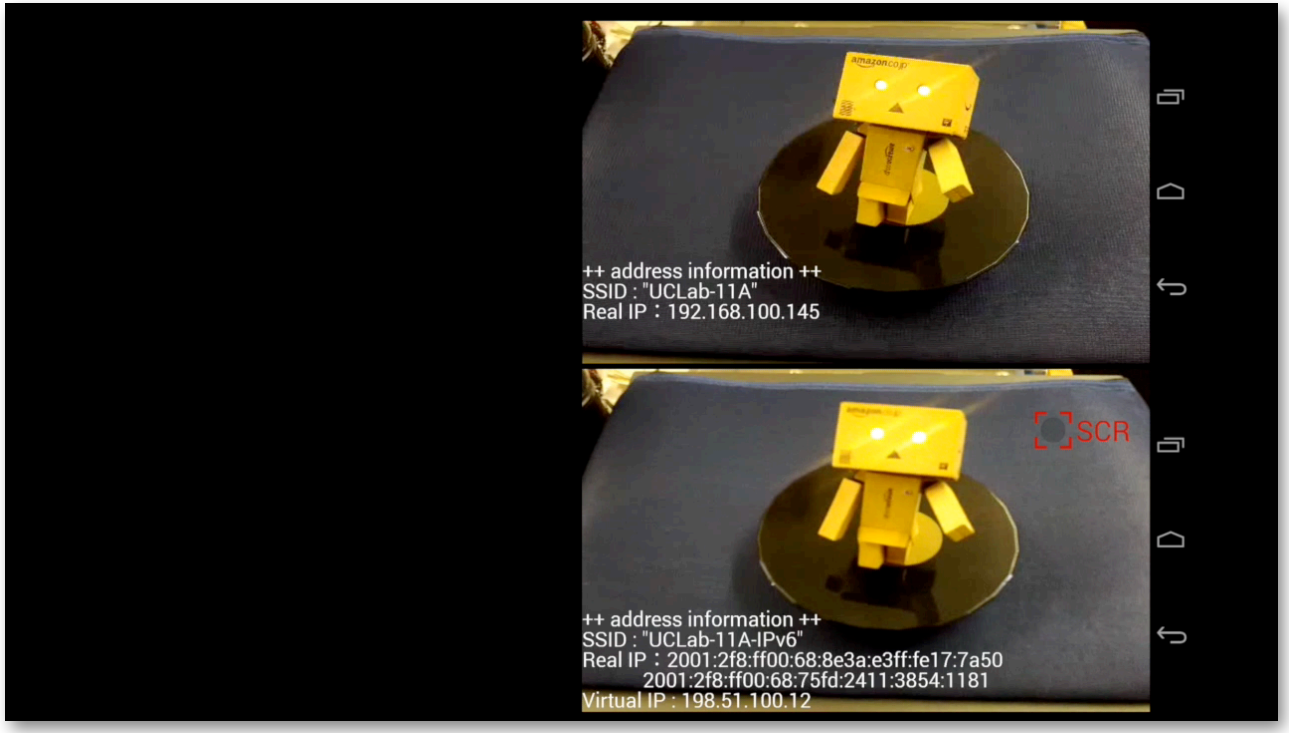
		通信相手側		
		Private IPv4	Global IPv4	Global IPv6
通信開始側	Private IPv4	○パターン4	◎パターン2	△パターン4
	Global IPv4	◎パターン3	◎パターン1	△パターン4
	Global IPv6	△パターン4	△パターン4	◎パターン1

- ◎：E2E
- ○：TRS経由（経路最適化処理後，E2E）
- △：TRS経由

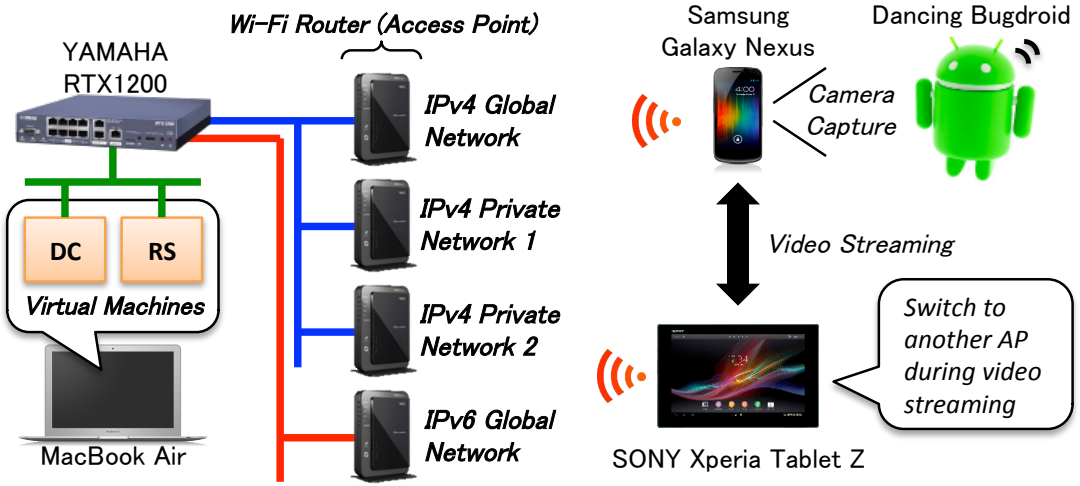
Androidスマートフォンによるハンドオーバデモ

CYPHONICの前身技術「NTMobile」を使ったデモ

2013年 ACM MobiCom 2013@USA



- Wi-FiからLTEにハンドオーバ
- IPv4-IPv6間の通信



H. Suzuki, et al., “New End-to-End Communication Architecture in IPv4 and IPv6 Networks”, ACM MobiCom 2013, 2013.

CYPHONICの利用方法

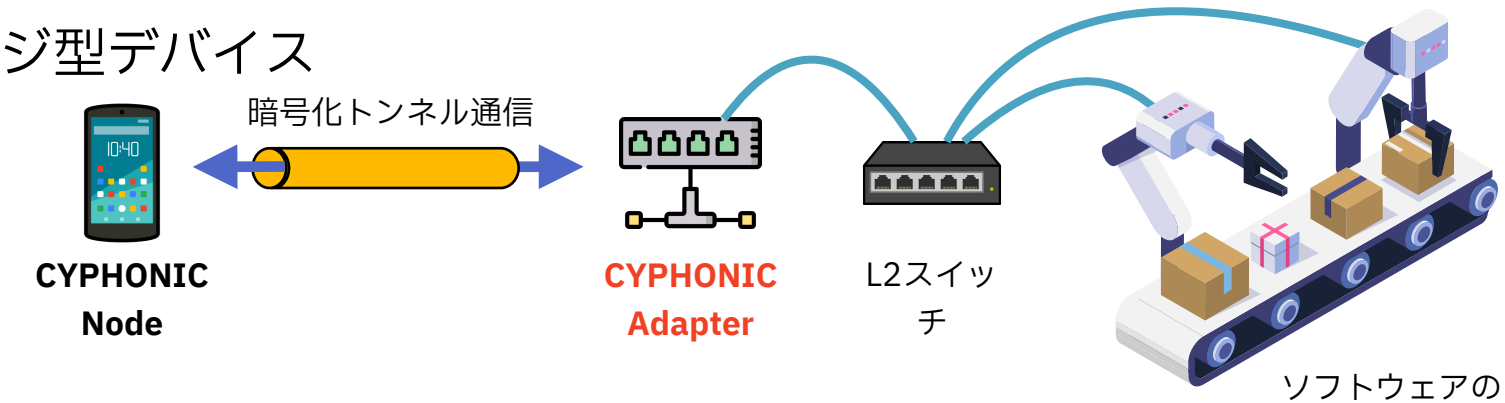
デバイスにCYPHONICソフトウェアをインストールする方法

- PCだけでなく，Linuxで動作するRaspberry Piなどのシングルボードコンピュータで動作確認済み

ubuntu　Windows 10　macOS　Raspberry Pi OS

CYPHONIC Adapterを利用する方法

- CYPHONICを実装したブリッジ型デバイス
- ソフトウェアの追加が困難な通信機器の代理でCYPHONICに関わる処理を実行



連携希望先

インターネットに接続する機器の安全性や接続性を確保したい企業

- **エンド接続系サービス**
  - ストリーム通信（セキュリティカメラ，音声・動画，ゲーム）
  - リモート接続（画面共有）
- **分散処理系サービス**
  - エッジコンピューティング，フォグコンピューティング
- **高セキュリティサービス**