# 仮想 IPv4 アドレスを想定した CYPHONIC アダプタの設計と基礎評価

後藤廉[1)], 吉川大貴[2)], 小村聖[2)], 眞玉和茂[1)], 内藤克浩[1)]

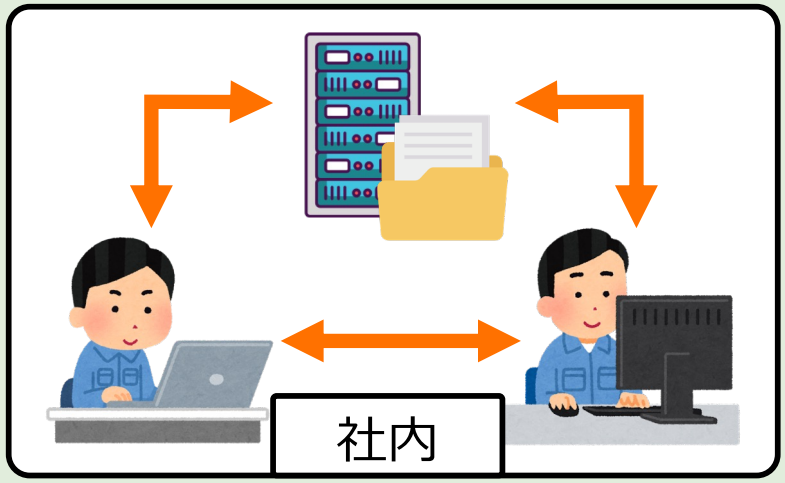
[1)] 愛知工業大学 情報科学部 情報科学科
[2)] 愛知工業大学大学院 経営情報科学研究科

第33回コンシューマ・デバイス＆システム (CDS) 研究会
2022年 1月 21日 (金)

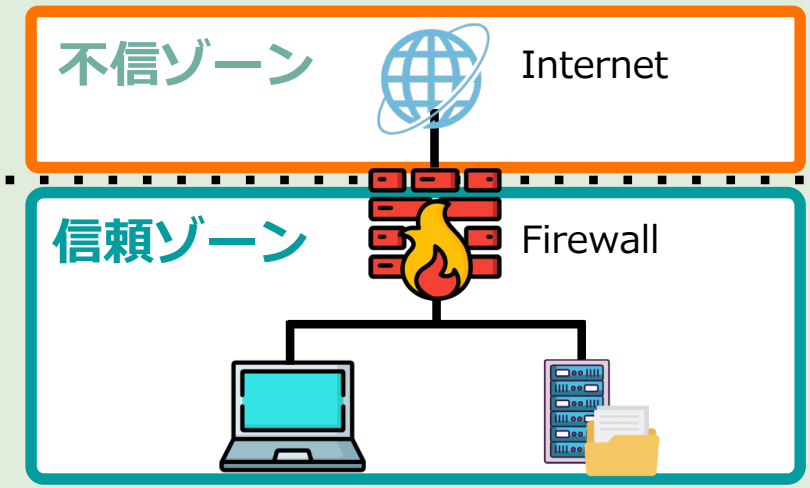
# 目次

# インターネット利用形態とセキュリティモデル

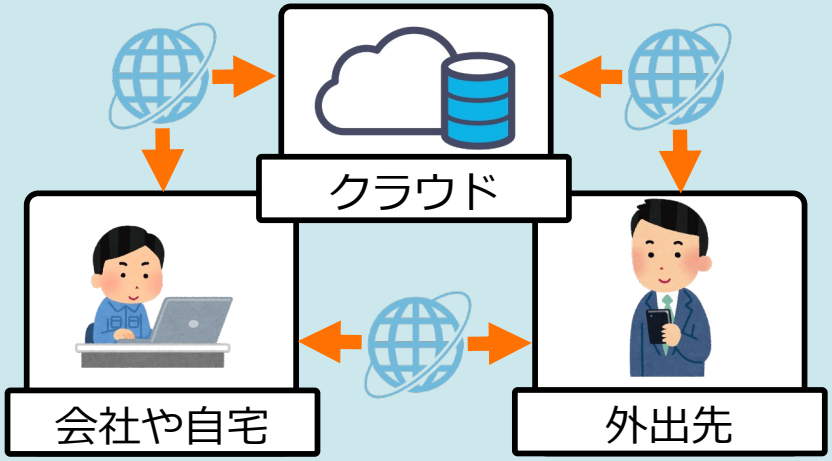
従来の利用形態



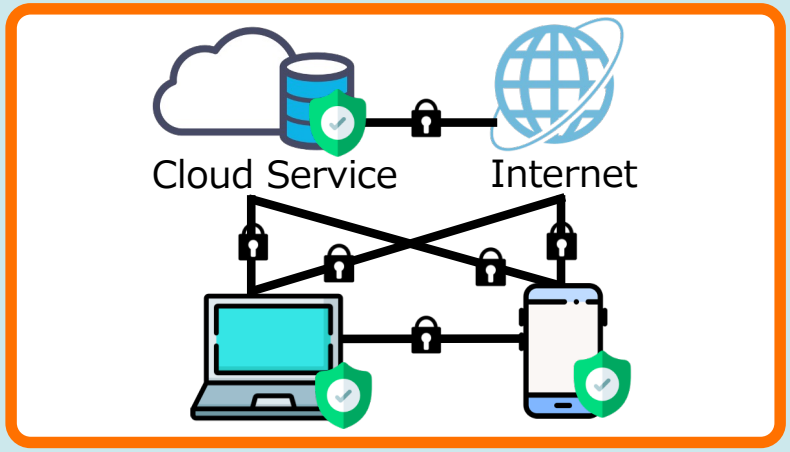

境界型モデル




今後の利用形態




ゼロトラストモデル



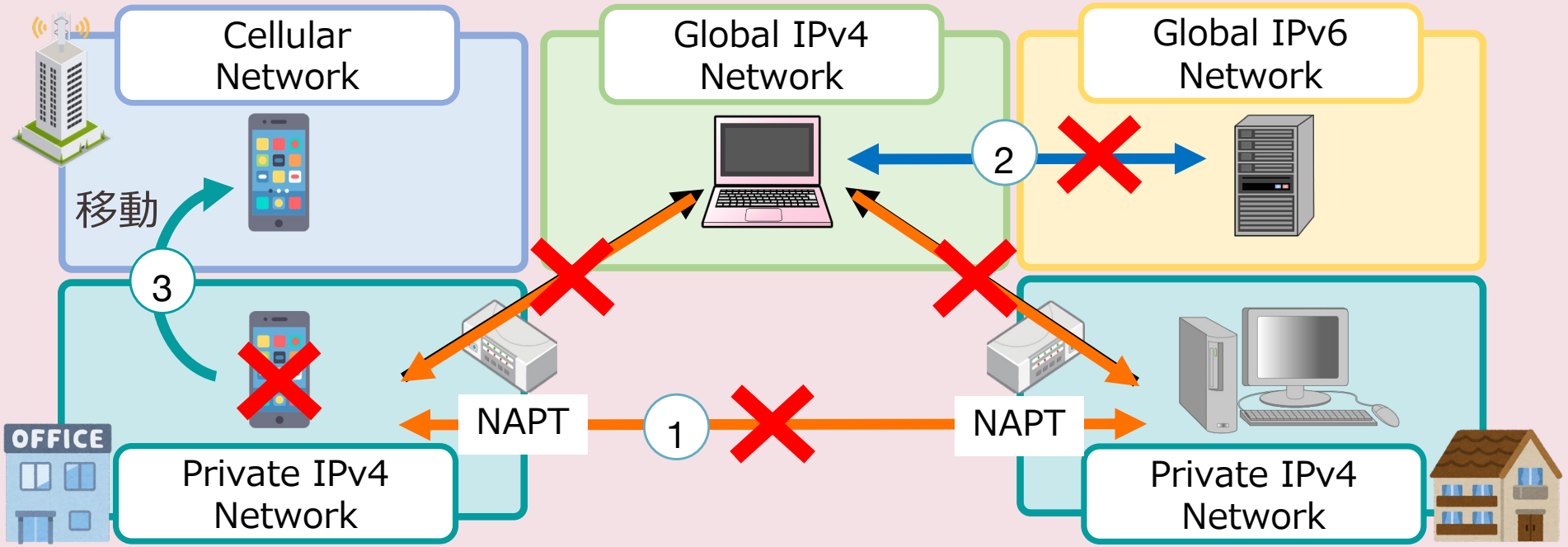

インターネット利用形態の多様化に伴い
セキュリティモデルも変化

# 現代のセキュリティ

ゼロトラストをはじめとした
端末間のセキュア通信への着目

通信を行う個々の端末を保護する必要があることから
端末間でのセキュアなエンド間通信への需要が向上

# エンド間通信に伴う課題




- IPv4アドレス枯渇対策のためNAPTとIPv6を導入
  課題１：NAPTによる通信の遮断
  課題２：IPv4とIPv6の非互換性
- IPは端末の移動について考慮されていない
  課題３：ネットワーク移動による通信切断

**エンド間での直接通信を実現する技術が必要**

# 既存技術と課題

| | 通信接続性 | 移動透過性 |
|---|---|---|
| | NAPTやIPバージョンの差異<br>依らず通信接続可能 | ネットワーク移動時も<br>通信継続可能 |
| Hole Punching / STUN | ● | X |
| ICE | ● | X |
| Mobile IP | X | ● |
| DSMIPv6 | X | ● |

- 既存技術にはそれぞれ課題が存在
- 概念実証の評価やセキュア通信に関する検討が不十分

端末間でのセキュアなエンド間通信を実現するために
通信接続性と移動透過性を確保する技術が必要

# CYPHONICの提案

**CYber PHysical Overlay Network over Internet Communication**

**セキュアなエンド間接続を実現する**
**オーバーレイネットワークプロトコル**

## ■ 端末間でのセキュアな通信を実現

・サービス利用端末の認証と送受信データの暗号化
・端末間でのエンドツーエンド通信を提供

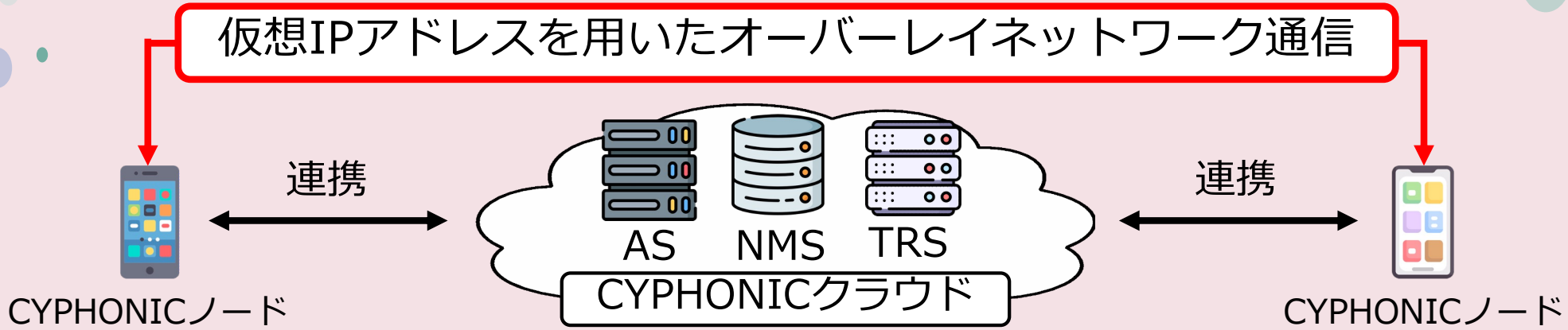
## ■ 通信接続性を実現

・NAPTの配下に存在する端末への通信を提供
・IPバージョンの互換性を提供

## ■ 移動透過性を実現

・端末の移動時も継続した通信を提供
・仮想IPアドレスによる通信で実ネットワークの影響を隠蔽

# CYPHONICの構成要素




## CYPHONICノード

・CYPHONICを用いた通信を行う端末
・クラウドサービスと連携することで相手端末と直接通信

## Authentication Service (AS)

・CYPHONICノ ードを認証
・CYPHONICノードの識別子としてFQDNを付与

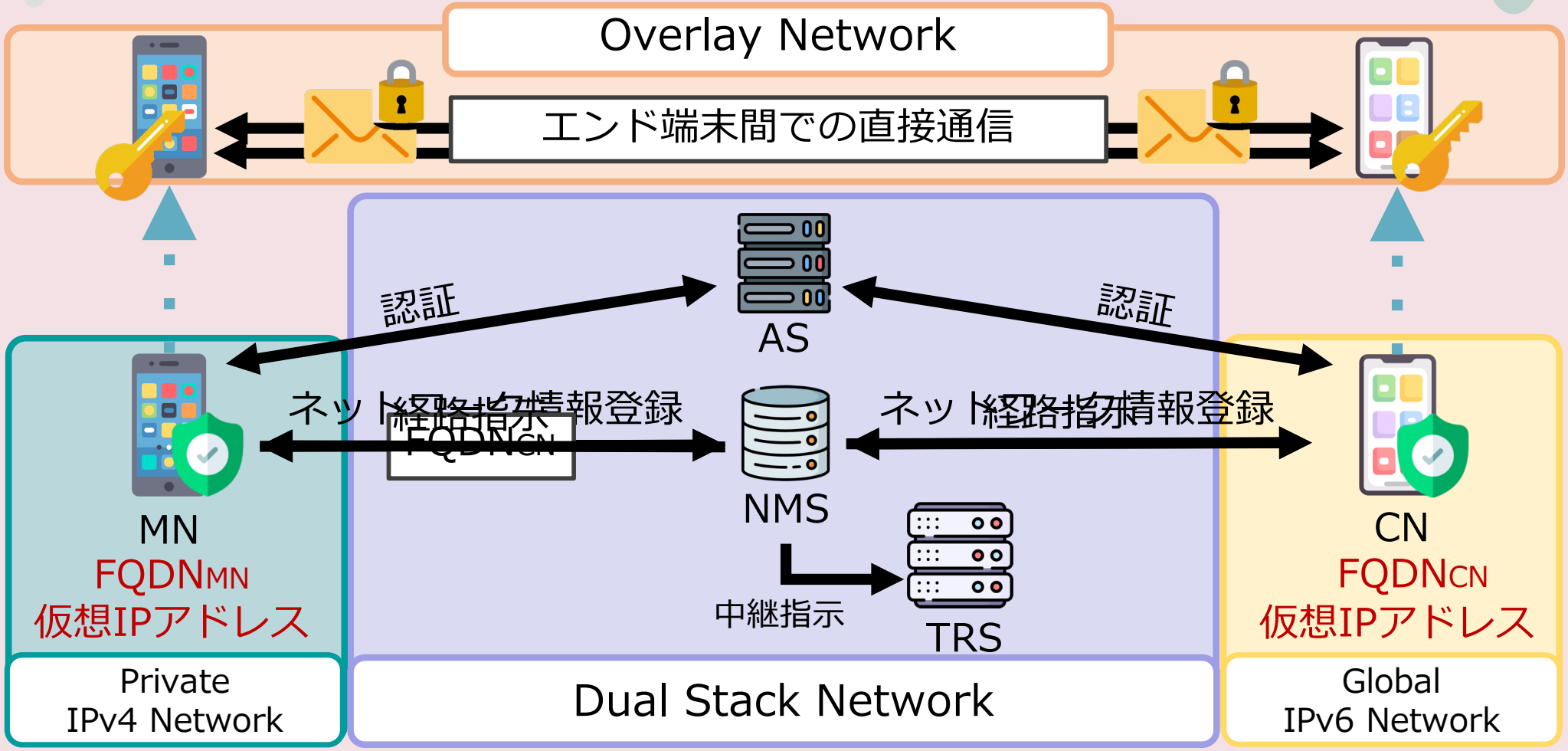
## Node Management Service (NMS)

・CYPHONICノードのネットワーク情報管理と通信経路の指示
・CYPHONICノードが通信に用いる仮想IPアドレスを付与

## Tunnel Relay Service (TRS)

・NAPTを跨いだ通信とIPv4/IPv6間の通信を中継

# オーバーレイネットワーク構築に伴う通信プロセス



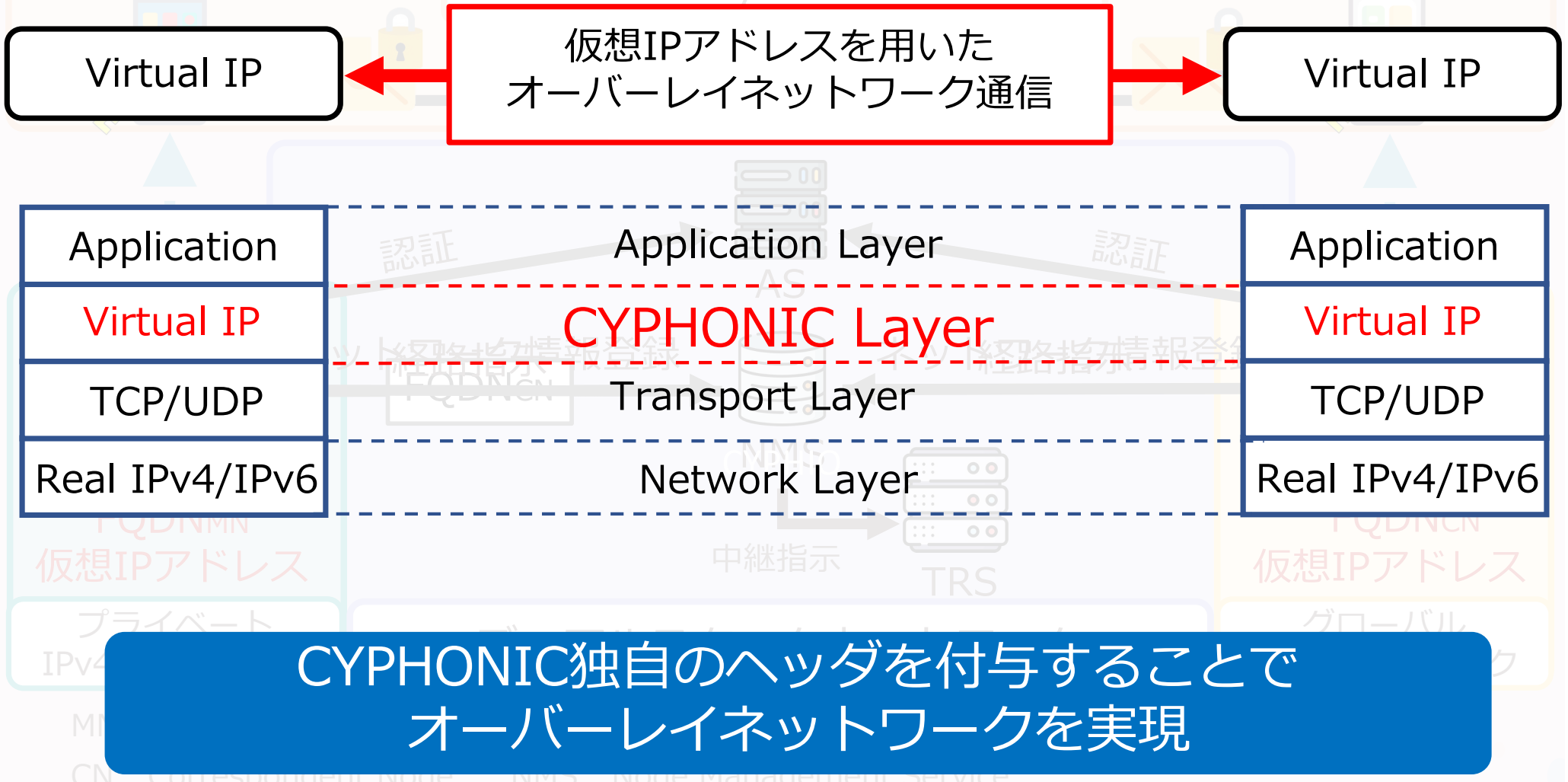

MN：Mobile Node　　AS：Authentication Service　　TRS：Tunnel Relay Service

CN：Correspondent Node　　NMS：Node Management Service

1. 認証処理　2. 位置情報登録処理　3. 経路選択処理

4. トンネル確立処理　5. データ通信処理

# オーバーレイネットワーク構築に伴う通信プロセス



# CYPHONICノードの機能

CYPHONICノードは端末プログラム (CYPHONIC Daemon) を導入することでCYPHONICを用いた通信を実現

- CYPHONICクラウドとのシグナリング
  - ・ノードの認証
  - ・仮想IPアドレスの取得
  - ・相手ノードとの通信経路を確立
- オーバーレイネットワーク上での通信
  - ・パケットにCYPHONICヘッダを付与
  - ・パケットの暗号化・復号化
  - ・パケットの改ざん検知

# CYPHONICノードの課題

既存機器に改良を加えることが困難な端末が存在

- 端末プログラムの変更が困難なIoT機器や組込み機器
- 特定のサービスを提供している専用サーバ

一般ノードはCYPHONIC上での通信が極めて困難

既存の端末やサービスに変更を加えることなく
CYPHONICの機能を提供可能なソリューションが必要

# 本研究の目的

CYPHONICの通信に必要な諸機能を代行する
**CYPHONICアダプタ** の提案

一般ノードはCYPHONICアダプタへ接続することで
CYPHONIC上でのセキュアなエンド間通信が可能

# CYPHONICアダプタの機能

CYPHONICアダプタが実装する機能

**CYPHONICの通信機能 ＋ 一般ノードの管理機能**

- **CYPHONICの通信機能**

  CYPHONICノードの既存機能を活用

- **一般ノードの管理機能**

  一般ノードにCYPHONICノードの機能を提供するため
  CYPHONICクラウドとの連携やパケットの処理を代行

# 一般ノードの管理機能

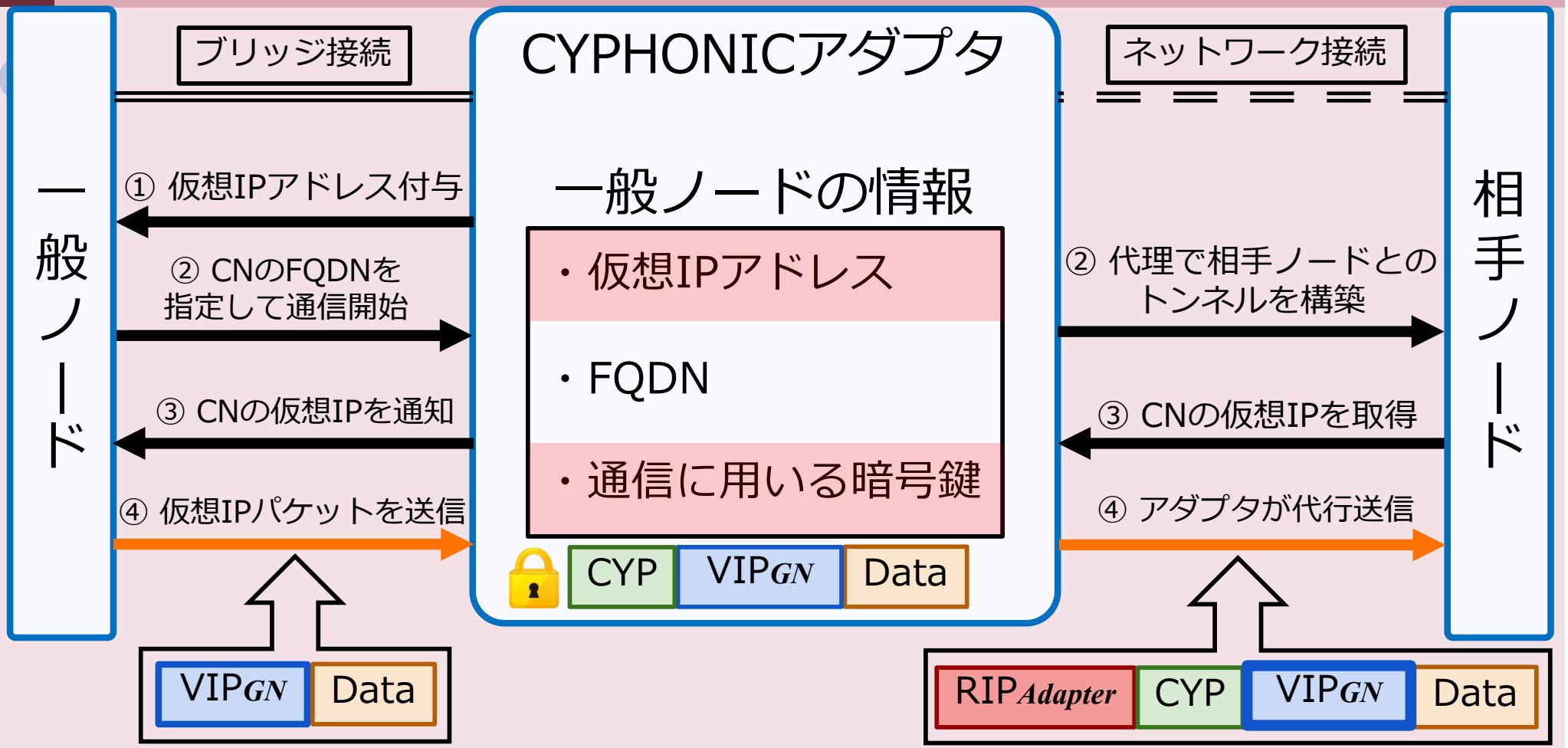
## CYPHONICノードに必要な機能

1. 仮想IPアドレスとFQDNの取得機能
2. 仮想IPパケットの処理機能
3. 送受信データを暗号化する暗号鍵の生成機能

## アダプタが一般ノードに提供する機能

1. 一般ノードを管理する機能
   - 一般ノードを識別するためのFQDNの管理
   - FQDNに対応する仮想IPアドレスの管理
   - 通信時の暗号鍵の生成
2. 一般ノードに仮想IPアドレスを付与する機能
   - DHCPv4により一般ノードへ仮想IPv4アドレスを付与
3. 一般ノードのパケットを取得する機能
   - 一般ノードから仮想IPパケットを取得して CYPHONIC Daemonへ転送

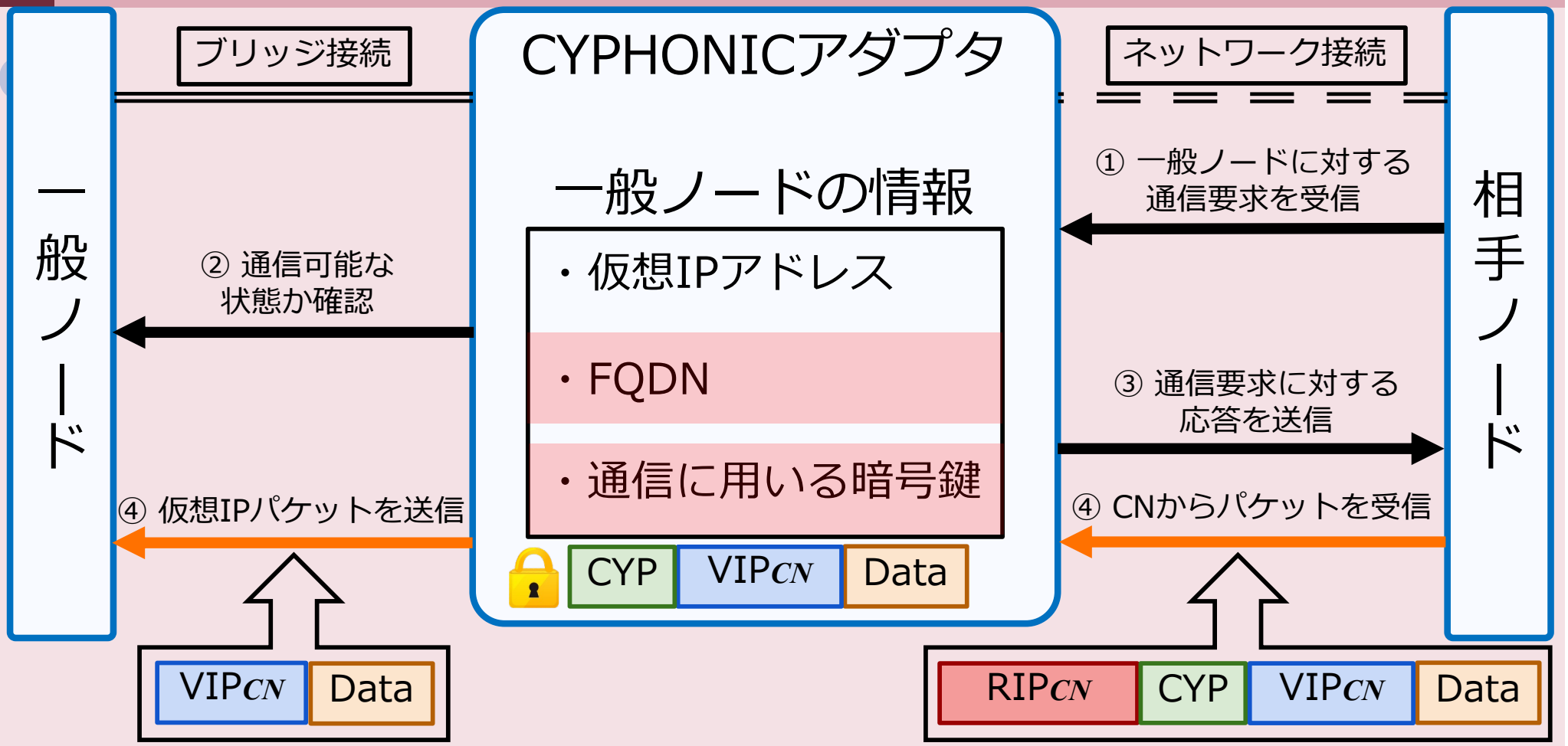
# 一般ノードから通信を開始する場合




GN :General Node　CN : Correspondent Node

1. 一般ノードに仮想IPアドレスを付与
2. 一般ノードは相手ノードのFQDNを指定して通信を開始
3. 取得した仮想IPアドレスを通知
4. アダプタで仮想IPパケットを処理して相手ノードへ送信

# 一般ノードへ通信を開始する場合




GN :General Node　CN : Correspondent Node

1. 一般ノードに対する通信要求を受信
2. 一般ノードが通信可能状態かを確認
3. 通信要求に対してアダプタが代理で応答
4. 受信したパケットをデカプセル化して一般ノードへ転送

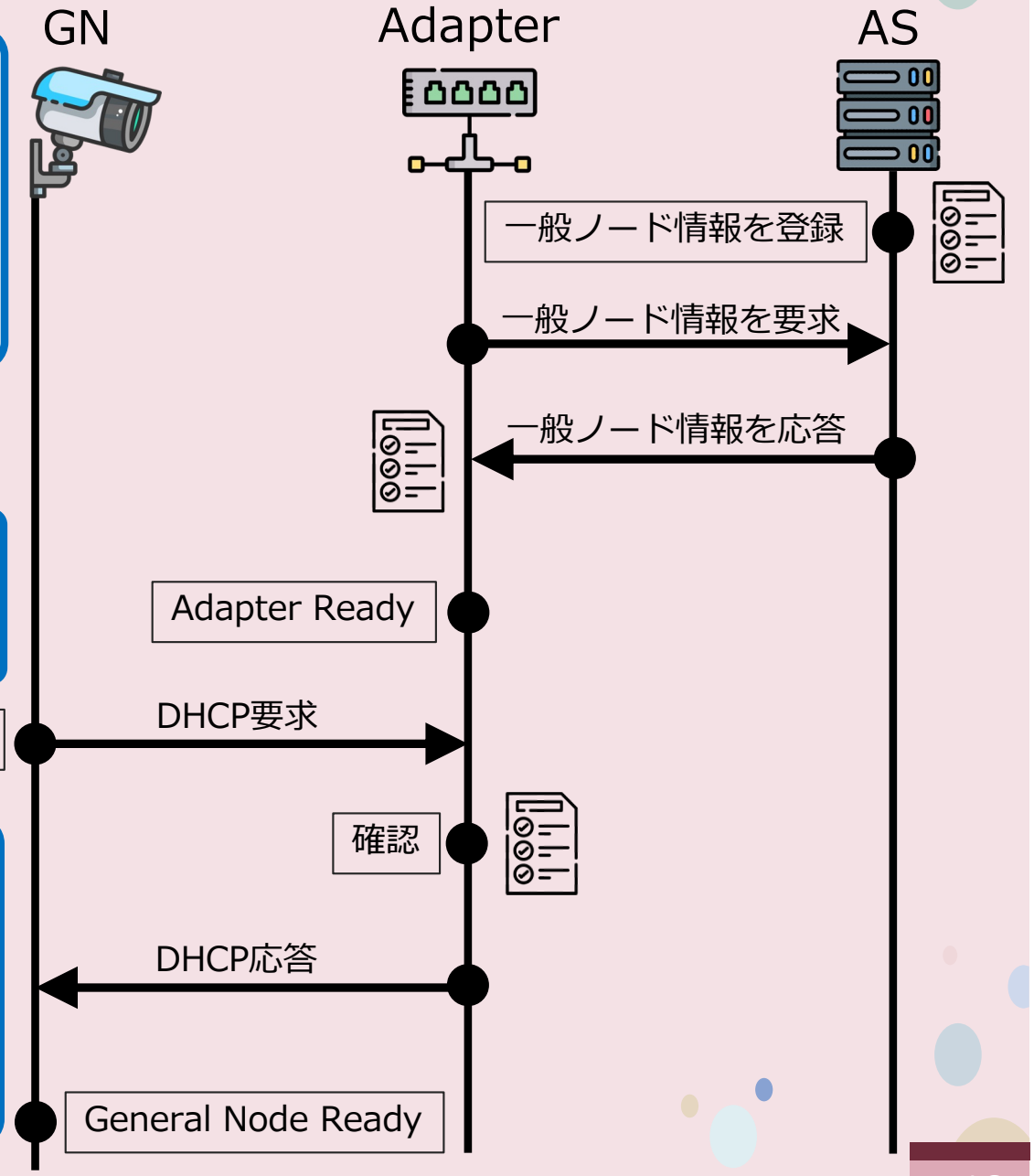
# 認証処理および登録処理

一般ノードの情報を
クラウドサービスに登録

・仮想IPアドレス
・FQDN
・MACアドレス

CYPHONICアダプタが
起動時に一般ノード情報を取得

管理している一般ノードの情報に
基づいて仮想IPアドレスを付与
→ クラウドサービスに登録された
端末のみが通信が可能



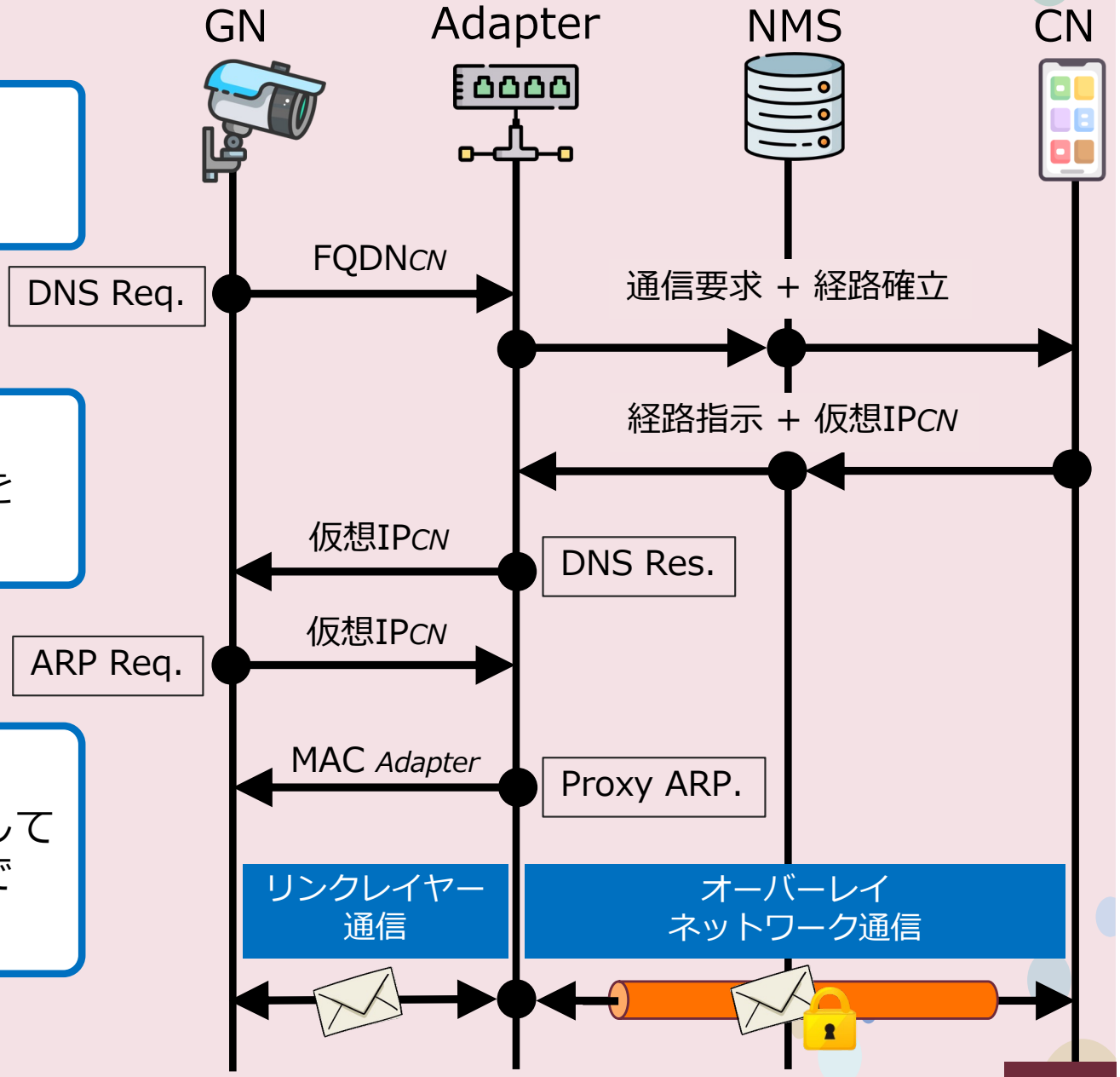

GN：General Node　AS：Authentication Service

# データ通信処理

DNSリクエストを受信して
NMSに通信開始要求を送信

DNSレスポンスを生成して
相手ノードの仮想IPアドレスを
一般ノードへ通知

リンクレイヤー通信によって
一般ノードからパケットを取得して
オーバーレイネットワーク上で
相手ノードと通信




GN：General Node　NMS：Node Management Service　CN：Correspondent Node

# 動作検証および性能評価

## 動作検証

**一般ノードとCYPHONICノード間の疎通を確認**

→ ICMP (ping) による疎通確認を実施

- 一般ノードからCYPHONICノードへの通信
- CYPHONICノードから一般ノードへの通信

## 性能評価

**一般ノードの通信スループットとRTT値を測定**

→ iperf3による一般ノードのスループット測定を実施

- 一般ノードとCYPHONICノード間での通信と
  CYPHONICノード間での通信スループットを比較

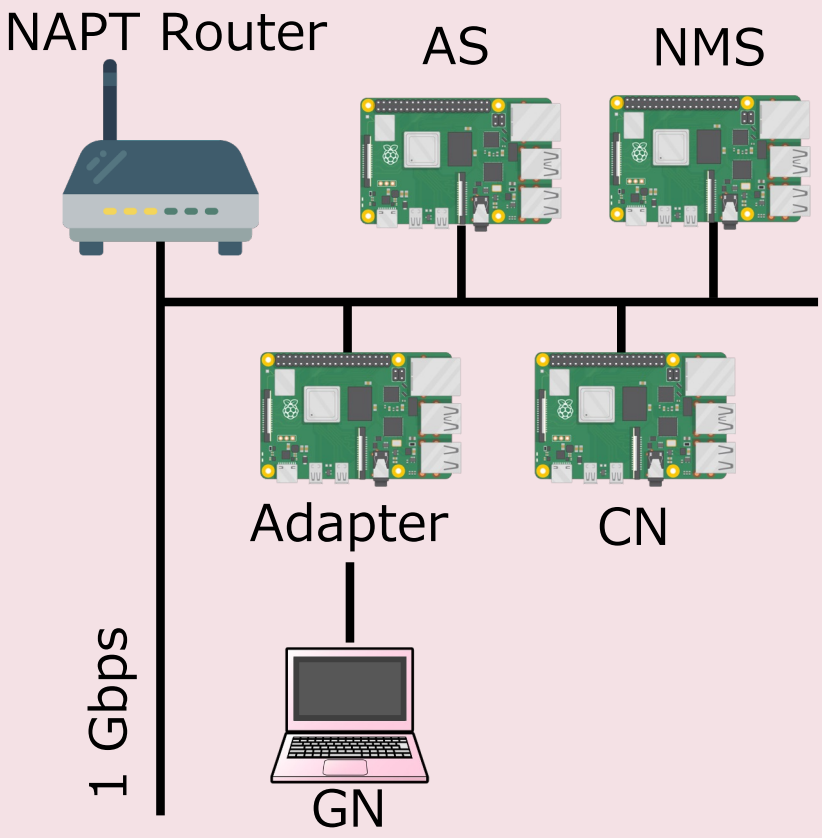
# 検証機器および評価環境

- **CYPHONICクラウド**
- **CYPHONICアダプタ/CYPHONICノード**

| | |
|---|---|
| Machine | Raspberry Pi 4 Model B |
| OS | Raspbian GNU/Linux 10.0 (Buster) |
| CPU | Quad Core 1.5GHz Broadcom BCM2711 64bit |
| Memory | 4GB RAM |

- **一般ノード**

| | |
|---|---|
| OS | macOS Big Sur Version 11.5 |
| CPU | Dual Core 2.20GHz Intel(R) Core i7-5650U 64bit |
| Memory | 8GB RAM |




AS：Authentication Service

NMS：Node Management Service

GN：General Node

CN：Correspondent Node

# 検証および評価結果

## ■ 動作検証

一般ノードとCYPHONICノード間で双方向通信が可能

→ CYPHONICアダプタは代行処理を実現

## ■ 性能評価

| | CYPHONIC Adapter | | CYPHONIC Node | |
|---|---|---|---|---|
| Traffic | Throughput | RTT | Throughput | RTT |
| 10Mbps<br>20Mbps<br>30Mbps | 10Mbps<br>20Mbps<br>30Mbps | 3.534ms<br>9.263ms<br>14.372ms | 10Mbps<br>20Mbps<br>30Mbps | 2.458ms<br>8.021ms<br>11.710ms |

30Mbps程度のトラフィックを処理可能

→ 複数人でHDビデオ (1080p送受信) の通信が可能

# まとめ

一般ノードをサポートするためのソリューションとして
CYPHONICアダプタの提案および概念実装を実施

CYPHONIC Daemonの通信機能を活用し
一般ノードをサポートする機能を追加実装することで
CYPHONICアダプタを実現

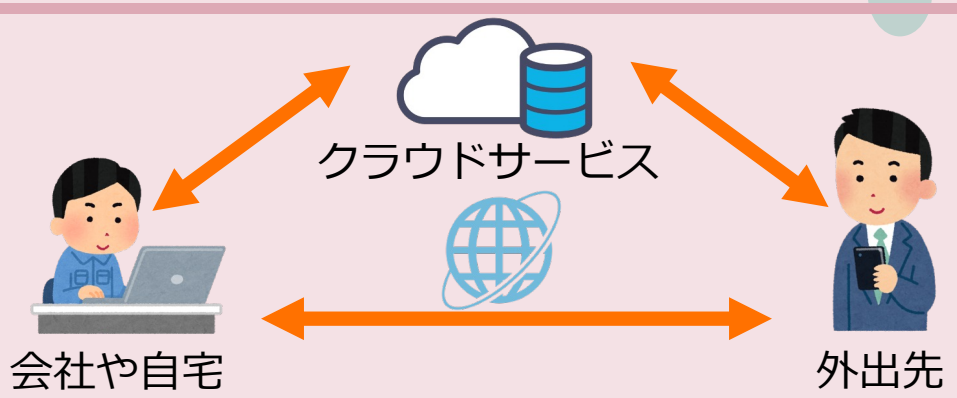
大きなオーバーヘッドを発生させることなく
一般ノードに通信機能を提供可能であることを確認

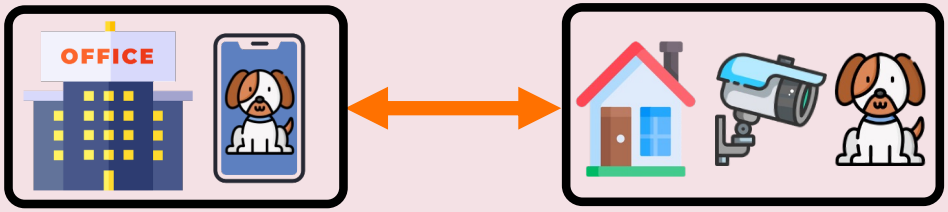
# 以下、予備スライド

# 現在のインターネット

## ■ インターネットの利用形態

- モバイル端末の普及
- クラウドサービスの利用
- リモートワークの増加
- IoT機器の活用



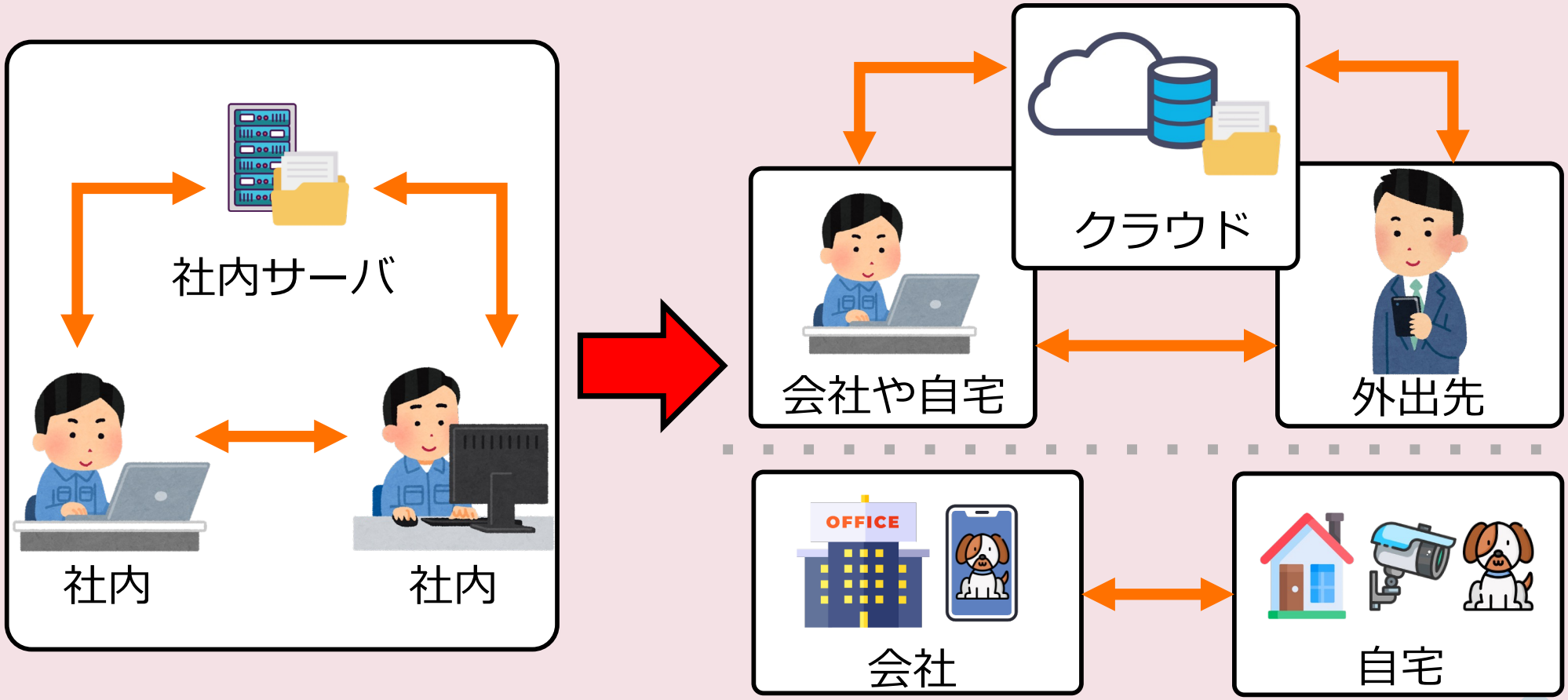

## ■ IP : Internet Protocol

- ネットワークを介した端末間の相互接続を実現
- 端末は一意となる識別子 (IPアドレス) を用いて通信

# インターネット利用形態の多様化

**従来の利用例**
- 必要なリソースは社内で管理
- 社内でのアクセス

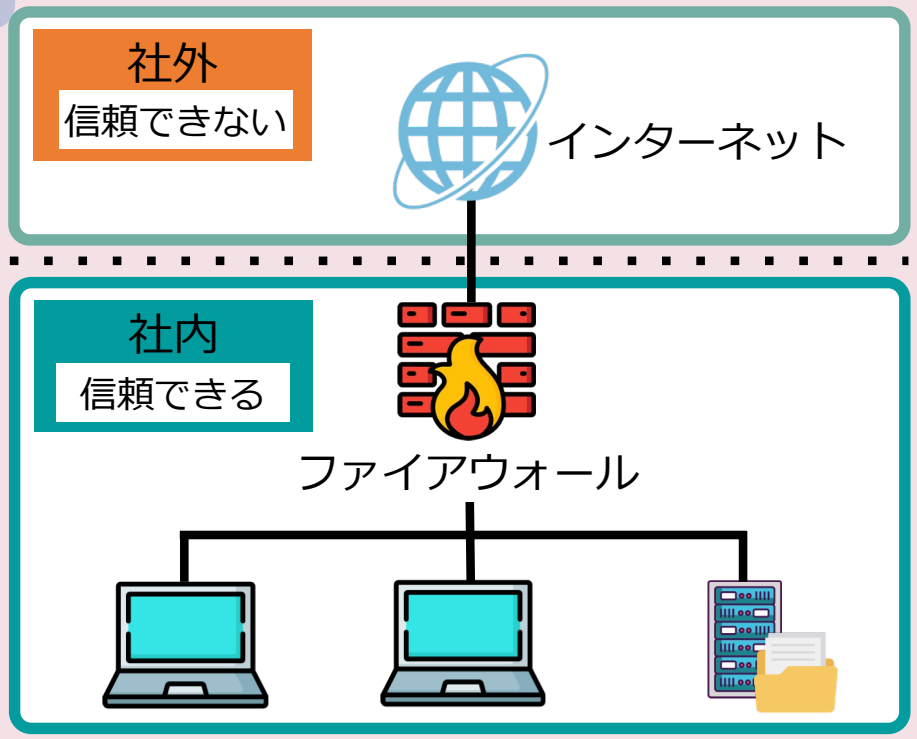
**今後の利用例**
- 社内リソースをクラウド上で管理
- 自宅や外出先等からもアクセス



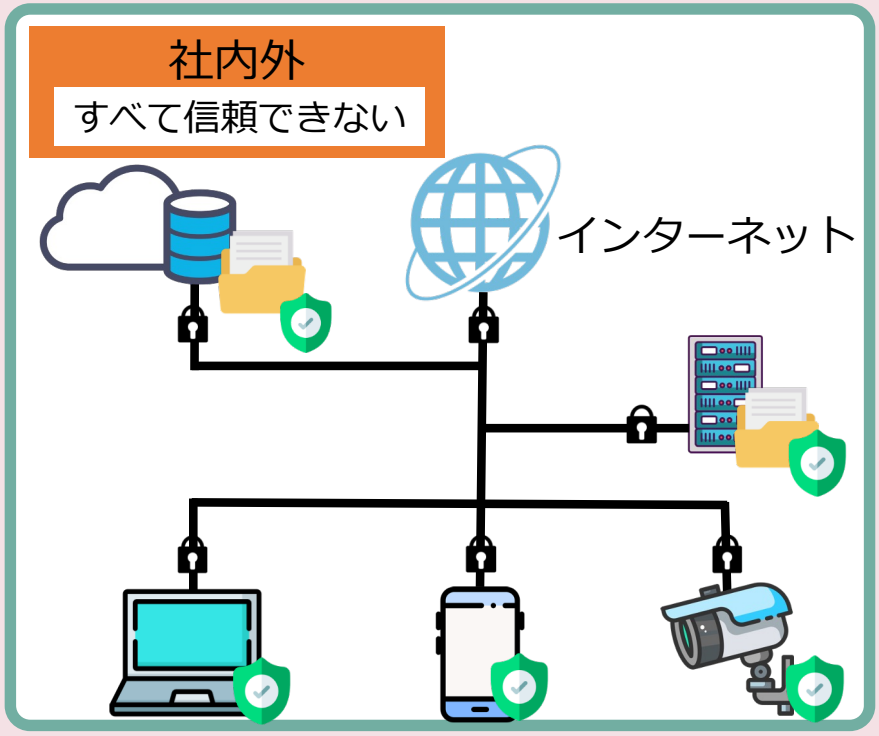

クラウドサービスやモバイル端末の普及により
コンピュータリソースの利用形態が多様化

# セキュリティモデルの変化

## 境界型モデル



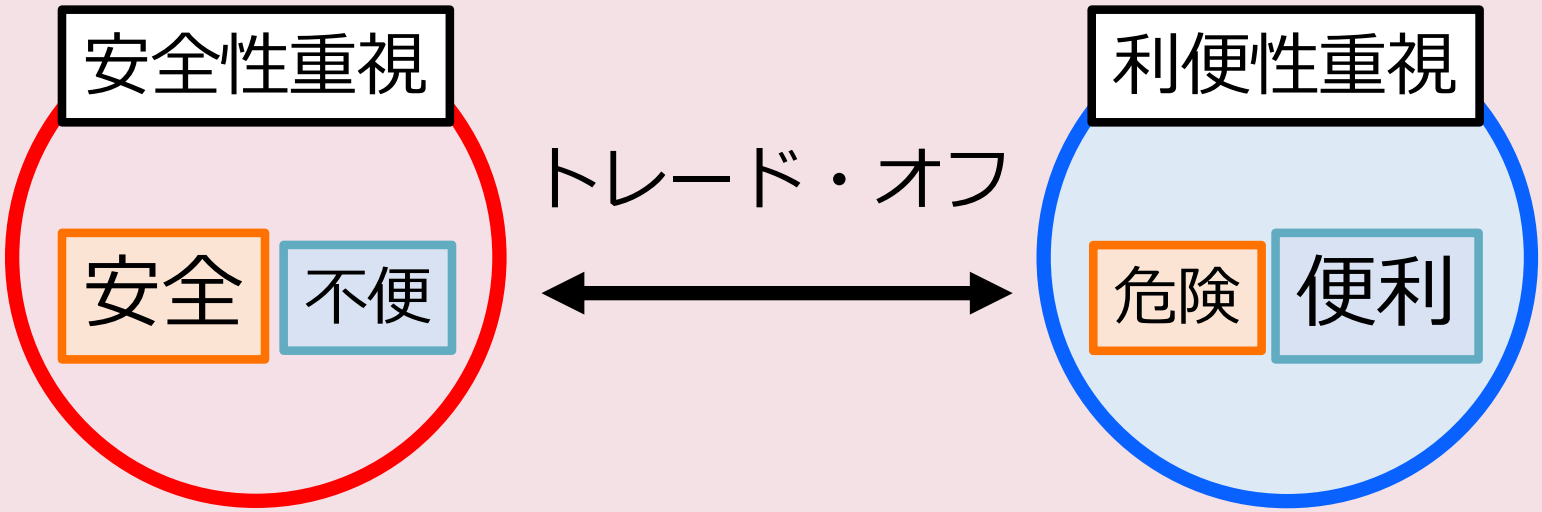

## ゼロトラストモデル




「どのネットワークと通信をするのか」ではなく
「誰と通信を行うのか」に着目したセキュリティ対策へ

ゼロトラストをはじめとした
エンド端末間でのセキュア通信の実現が必要

# セキュリティのトレード・オフ




セキュリティ対策において，**安全性**と**利便性**は
トレード・オフの関係

現在の複雑なIPネットワーク環境において
セキュリティ対策の複雑化が懸念

既存環境との共生を図りながら
効果的に導入することが重要

# 端末間相互接続性を担保する既存技術

**通信接続技術**：NAPT越え，IPv4/IPv6間通信を実現

- Intaractive Connectivity Establishment
  - サーバが各々の端末が存在するネットワーク情報を収集
  - サーバから指示される経路を用いることで適切なNAPT越えが可能
- Dual-Stack
  - 端末にIPv4/IPv6の両プロトコルスタックを実装
  - 相手端末のIPバージョンに対応した通信が実現可能

**移動透過技術**：移動に伴うコネクション切断を防止

- Mobile IP
  - サーバが端末の位置情報を管理
  - 送受信パケットを端末間でルーティングすることで移動を隠蔽

# 既存技術の課題

- Interactive Connectivity Establishment
  - NAPT越えを実現する際のシグナリングコストが増大
  - 移動透過性に関して考慮されていない
- Dual-Stack
  - 既存機器のOSカーネルに特定の改良が必要
  - IPv6に未対応の機器はDual-Stackの実装が困難
- Mobile IP
  - パケットルーティングによる冗長経路の発生
  - 通信接続性に関して考慮されていない

- 既存技術にはそれぞれ課題が存在
- 概念実証の評価やセキュア通信に関する検討が不十分

**通信接続性と移動透過性を包括的に実現し**
**エンド端末間の接続性を確保する技術が必要**

# CYPHONIC 通信シーケンス

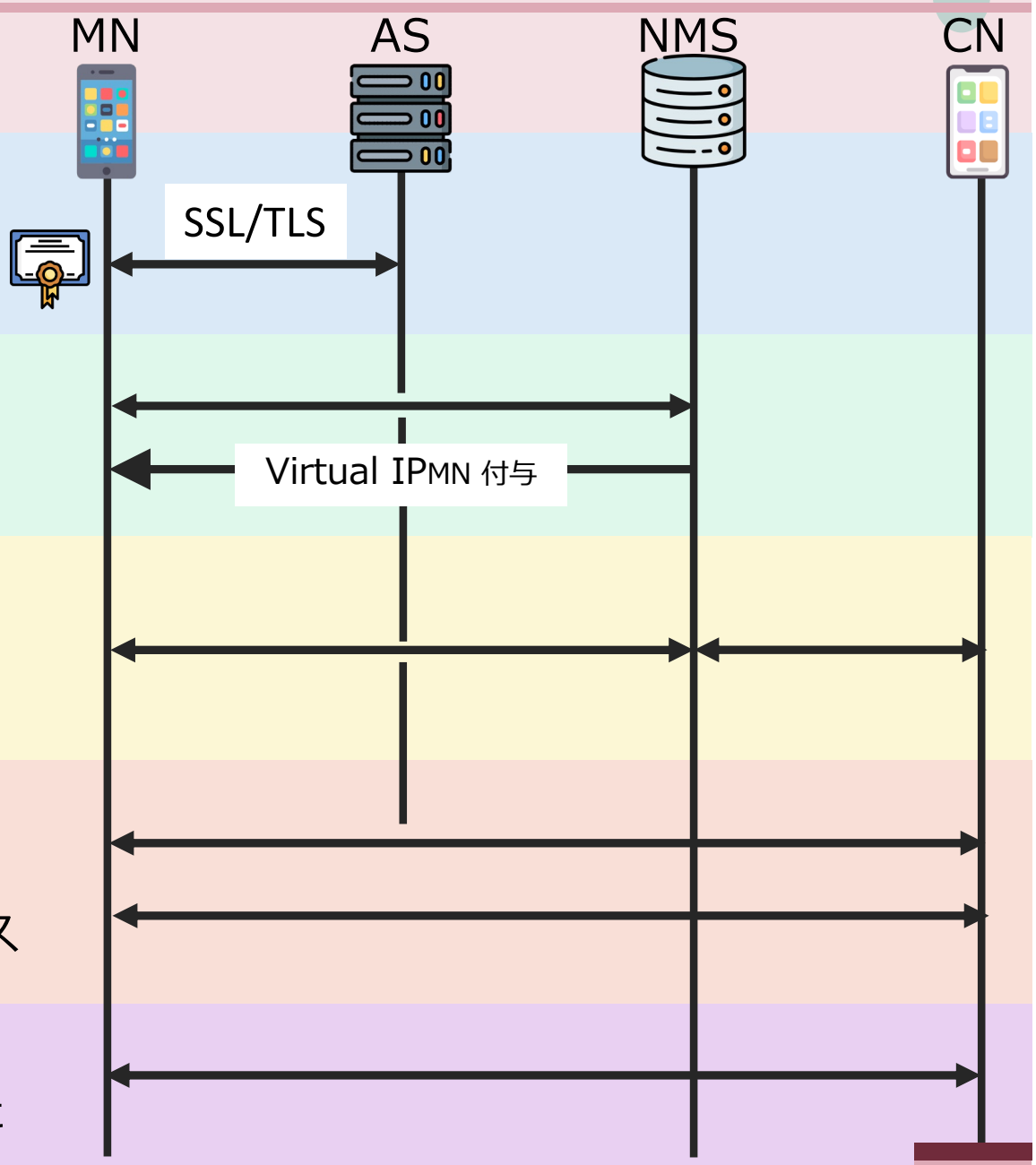
**① 認証処理**
CYPHONICノードの認証を行う
プロセス

**② 位置情報登録処理**
ノードのネットワーク環境情報を
NMSに登録するプロセス

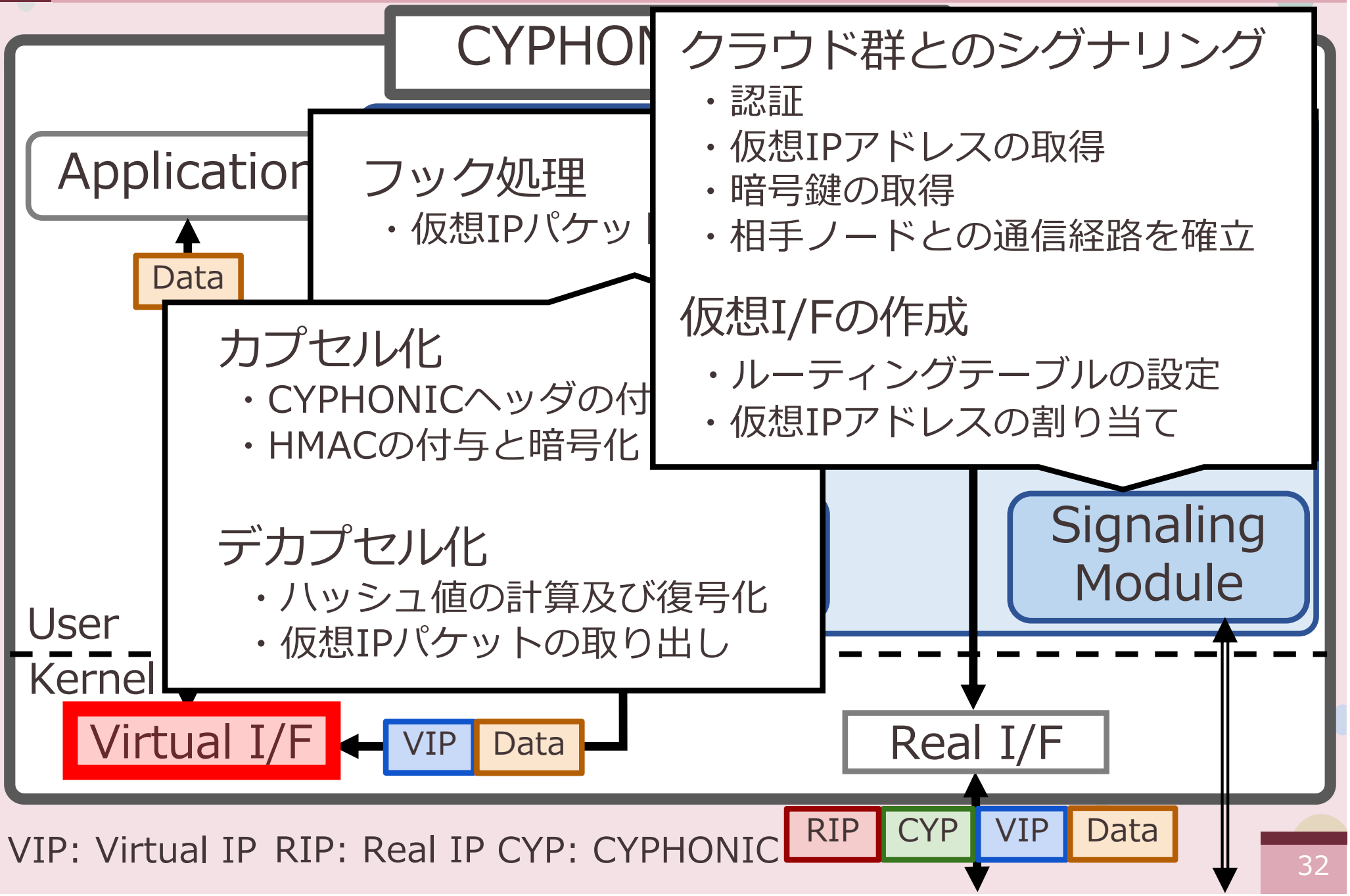
**③ 経路選択処理**
相手ノードとの通信に用いる経路を
決定するプロセス

**④ トンネル確立処理**
送受信データを暗号化するための
共通鍵を両ノードで交換するプロセス

**⑤ データ通信処理**
仮想IPパケットを暗号化し，構築した
トンネルを用いて通信するプロセス

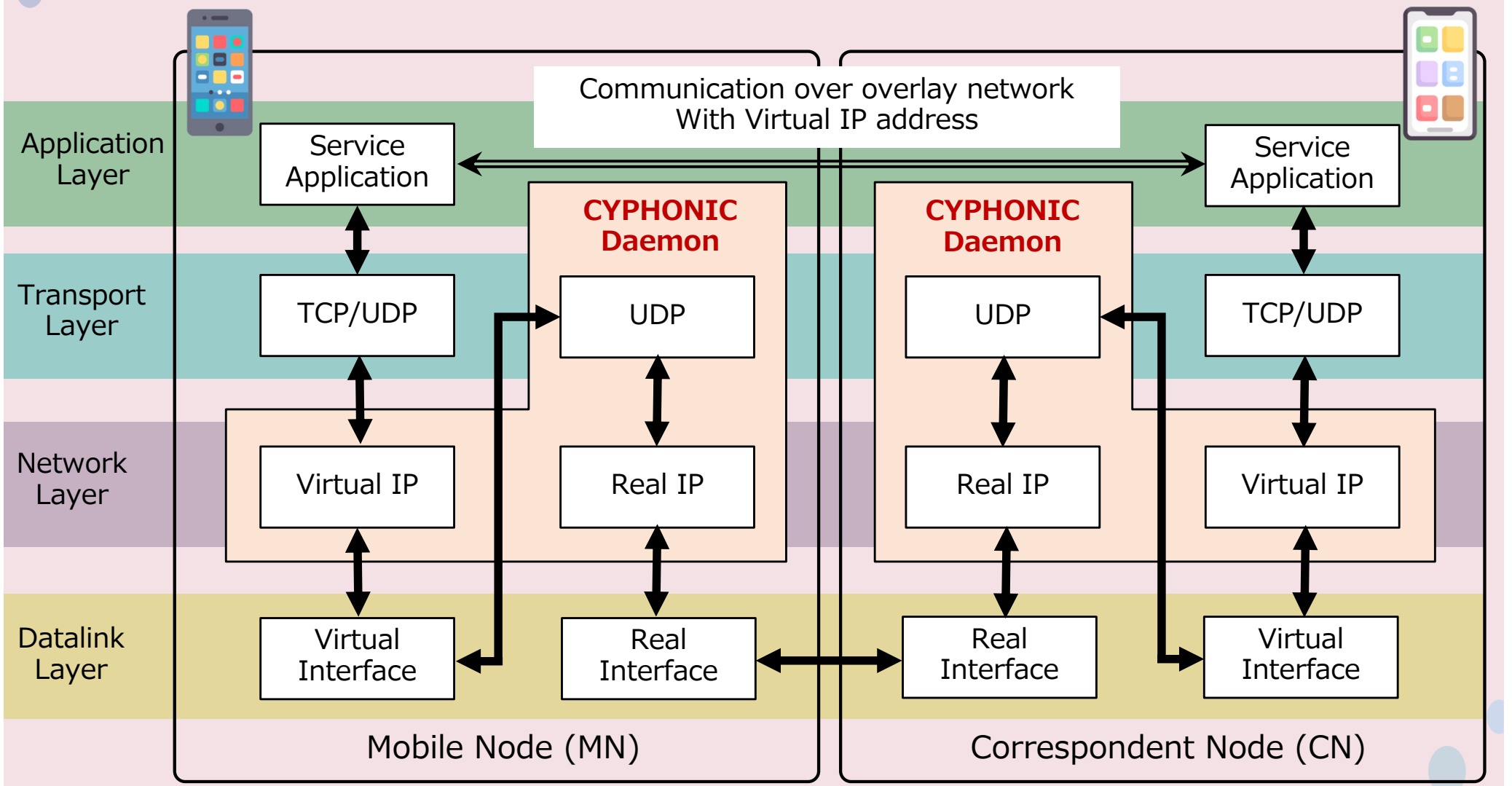


# CYPHONICノード システムモデル

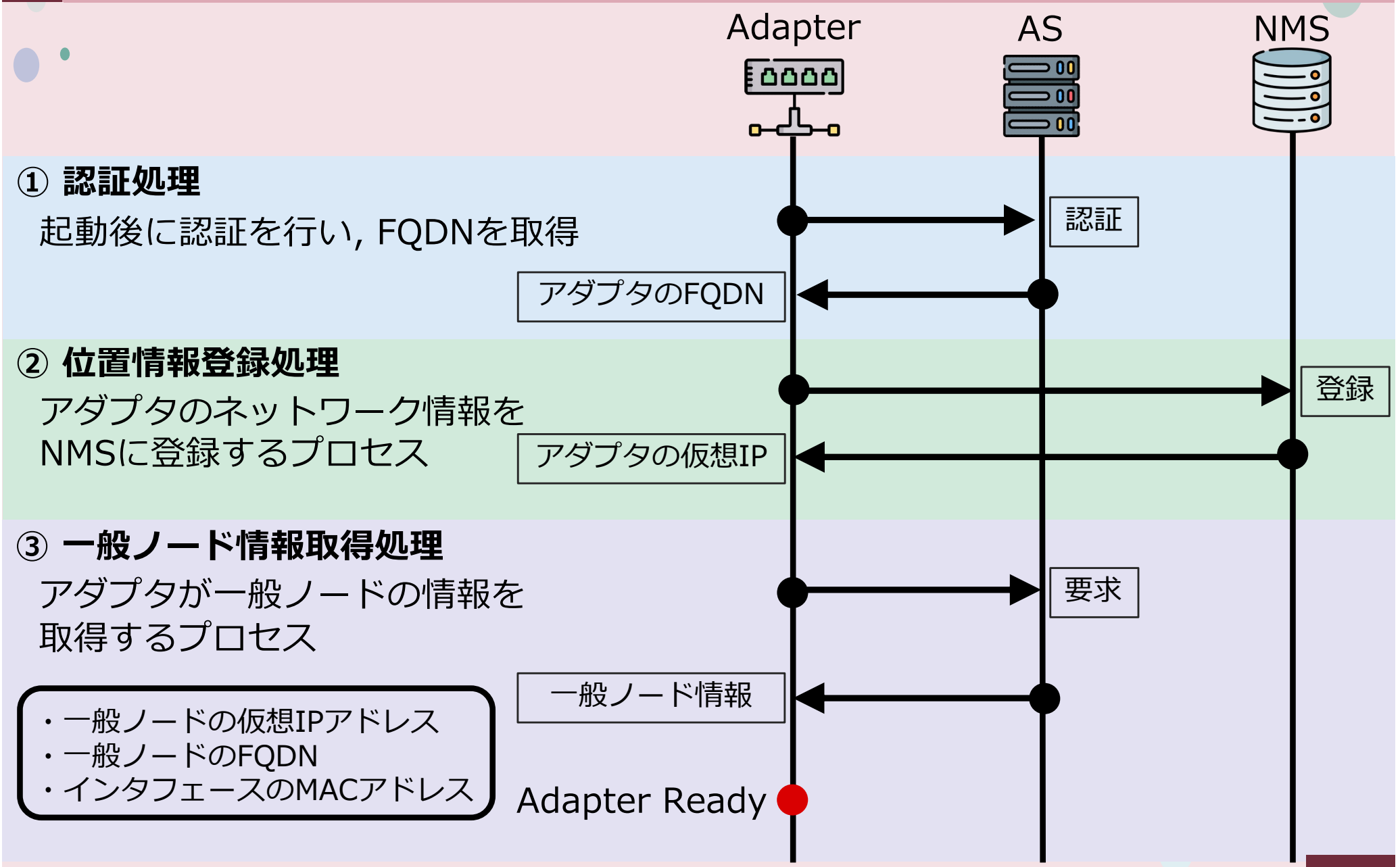



VIP: Virtual IP RIP: Real IP CYP: CYPHONIC

# CYPHONIC Daemon による PDU カプセル化フロー

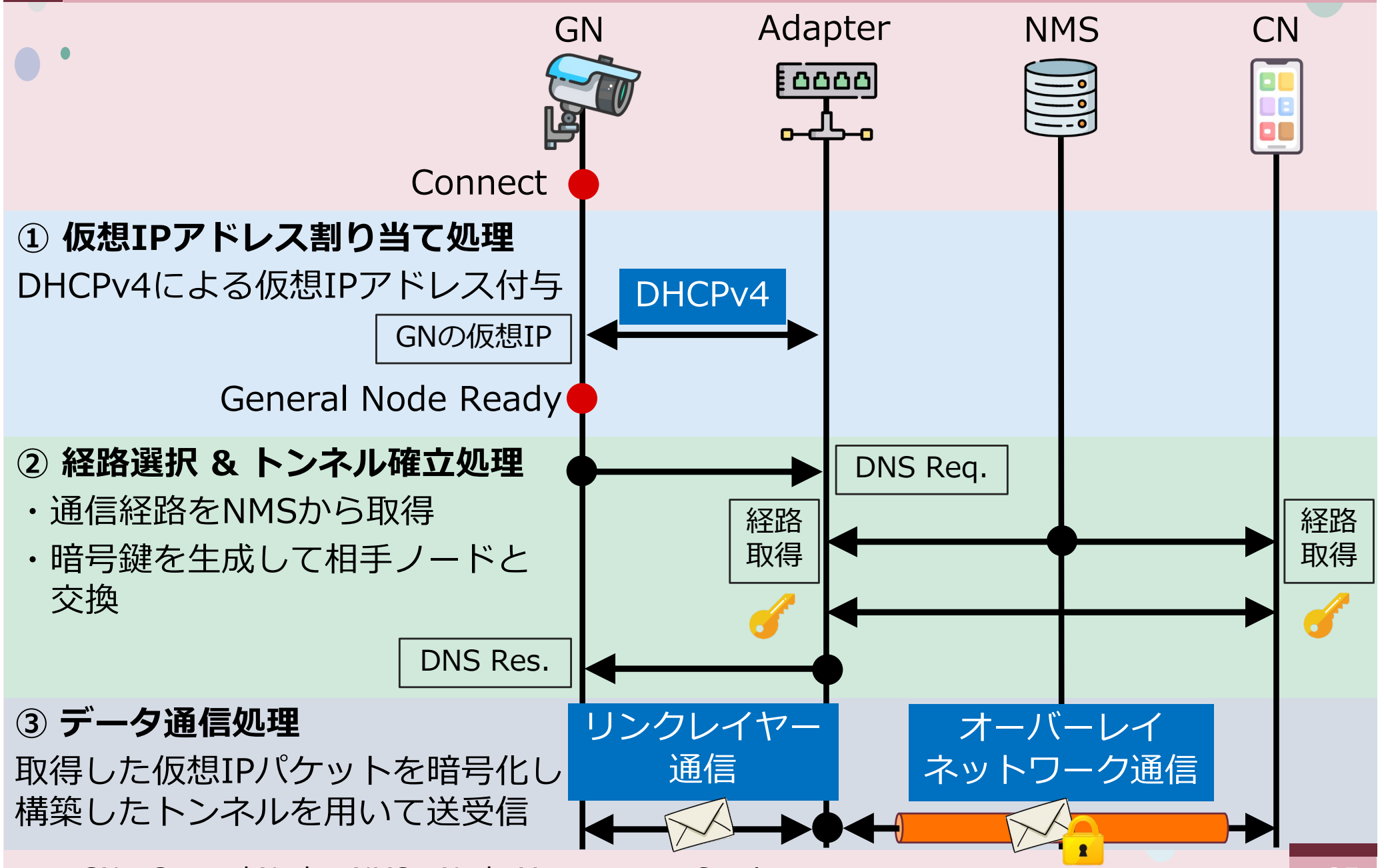


# CYPHONICアダプタの通信プロセス



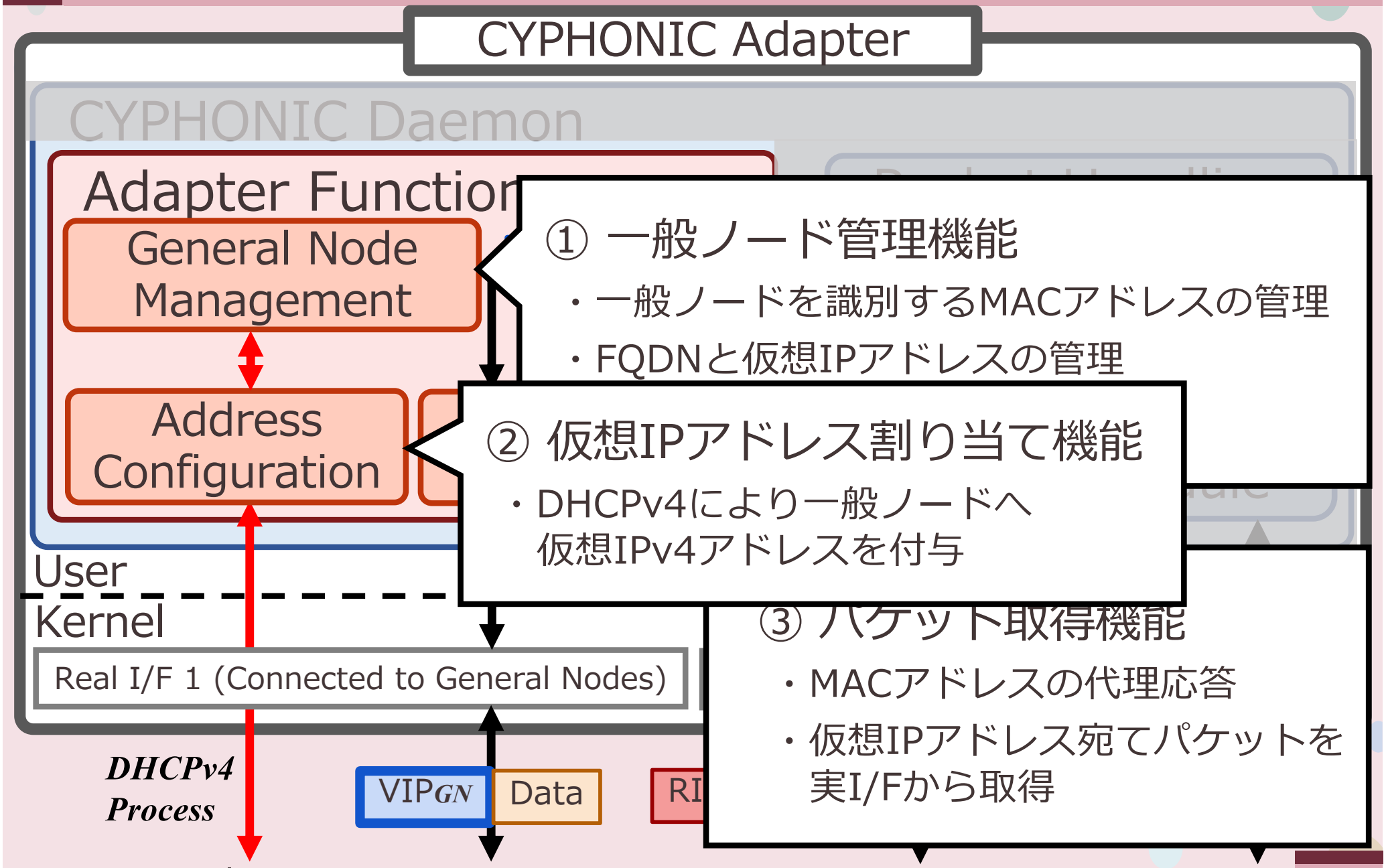

AS：Authentication Service　NMS：Node Management Service

# CYPHONICアダプタを介した通信




GN：General Node　NMS：Node Management Service　CN：Correspondent Node

# CYPHONICアダプタ システムモデル




VIP: Virtual IP RIP: Real IP GN: GeneralNode CYP: CYPHONIC