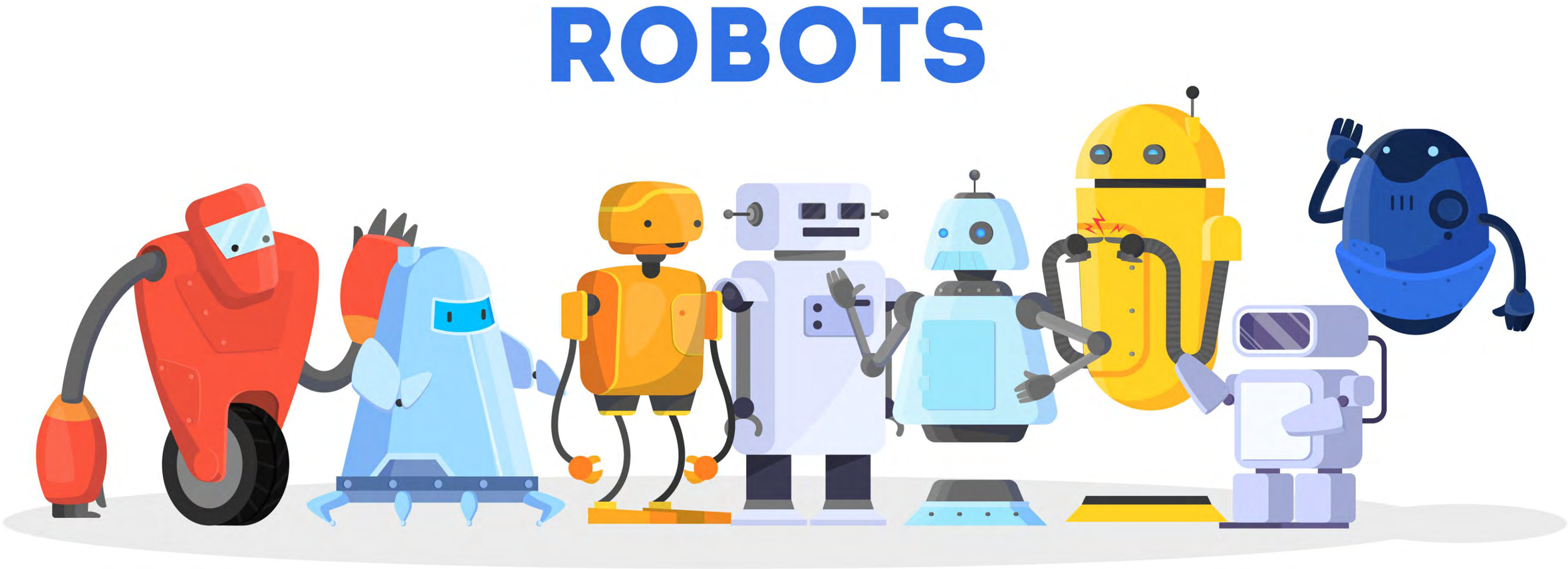
ロボットミドルウェアの
セキュリティを強化する

学習駆動コース　今岡ゼミ
磯野 玄光（Haruki Isono）

目次

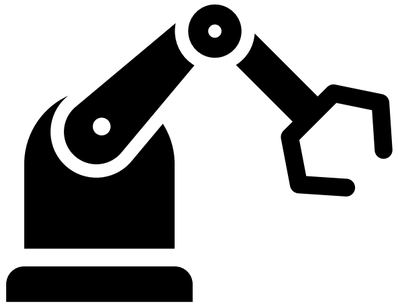
01 ロボットとは？



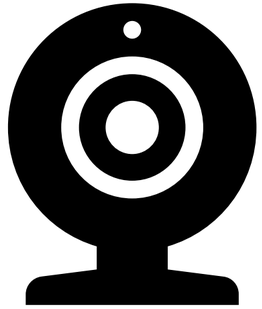
人間の代わって働いてくれるもの

01 ロボットを構成する要素

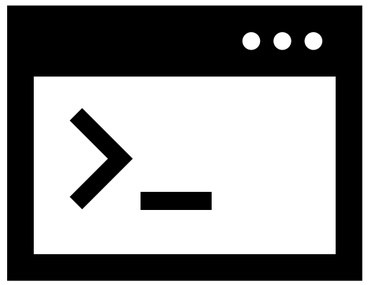
ロボットは複合的な技術である



actuators
モータ
機構



sensors
エンコーダ
力・加速度



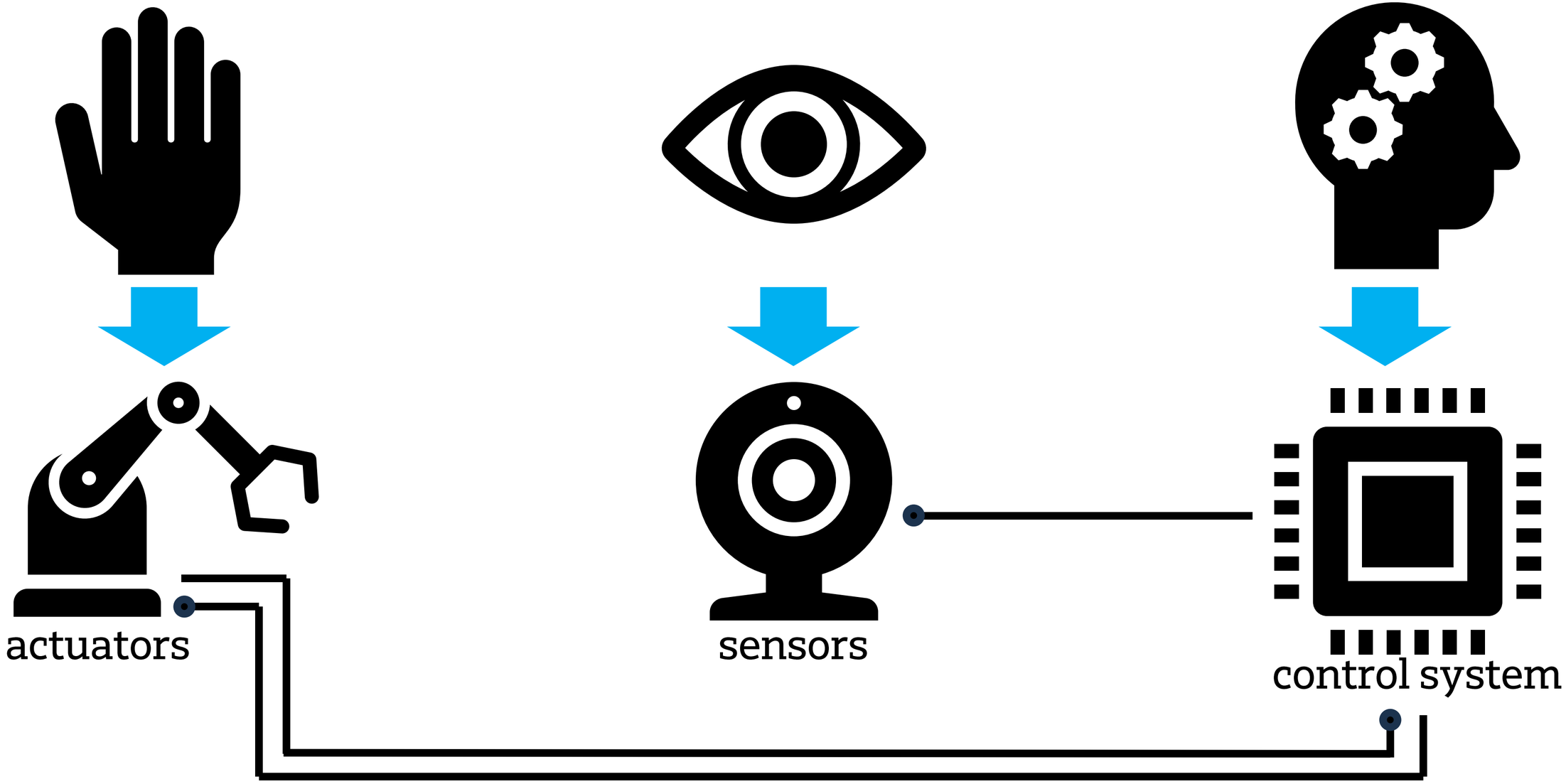
software
コンピュータ

batteries
電源
バッテリー

必要となる技術

電気工学・電子工学・機械工学・制御工学

01 ロボットが動作する仕組み



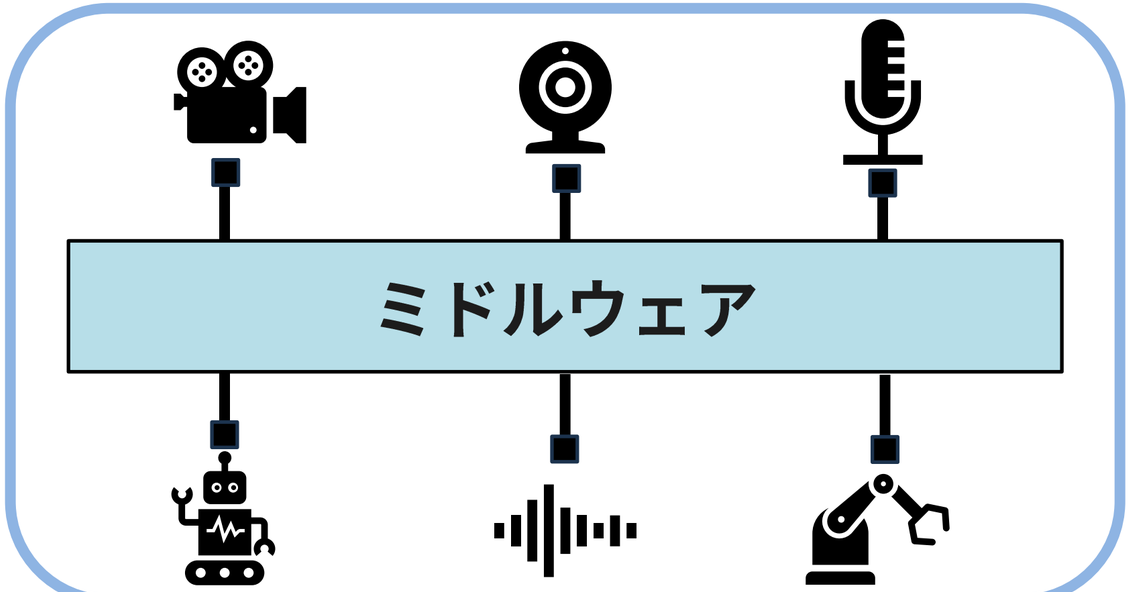
01 ロボットソフトウェア開発の方向

新規ロボット開発にミドルウェアを利用することが主流に

従来型開発

- 様々な機能を融合的に設計
- 実行時の効率は高い
- システムが複雑化すると開発が困難

コンポーネント指向開発

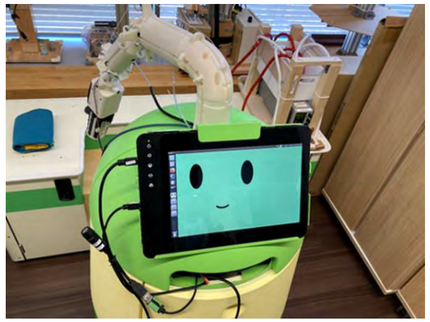


- 大規模複雑な機能の分割・統合
- 開発・保守効率化（モジュールの再利用）
- システムの柔軟性向上

01 モジュール化のメリット

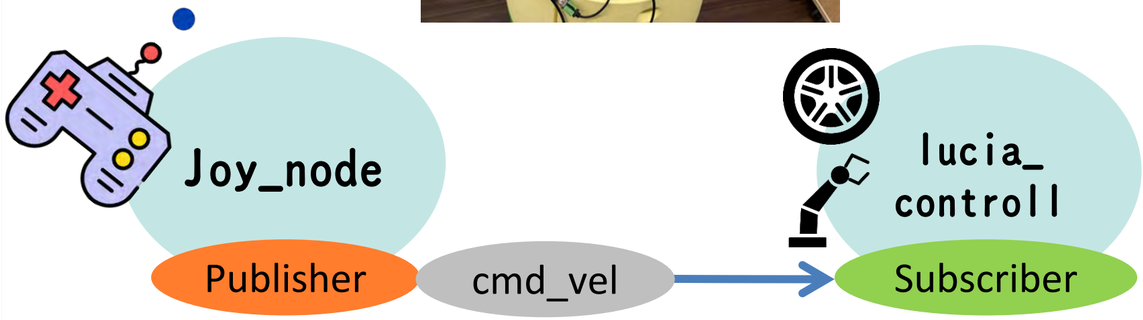
異なるハードウェアでも共通の速度コマンドが使える！！

ロボット1

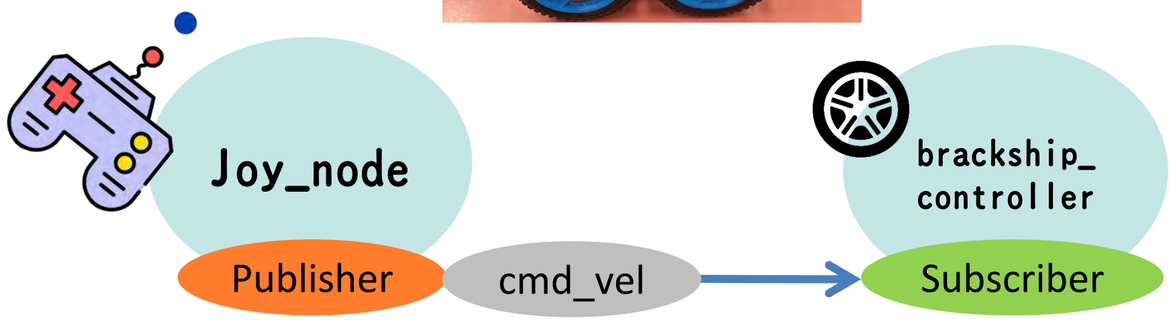


ロボット2

[cmd_vel]というtopicで
速度情報を送る



Node:[lucia_controller]
YARPとの通信
モータ，エンコーダの制御



Node:[brackship_controller]
シリアル通信
モータ，エンコーダの制御

02 ロボットミドルウェアとは？

ロボットシステム構築を効率化するための共通機能を提供する
基盤ソフトウェア

- 「ロボットOS」と呼ばれる
- インターフェース・プロトコルの共通化・標準化
  - モジュール化のフレームワークを提供
  - モジュール間通信機能を提供
  - OSや言語間連携・相互運用を実現
- 2000年頃から開発が活発化
  - 世界各国で様々なミドルウェアが開発された

RTミドルウェア

ROS/ROS2


Orocos

YARP

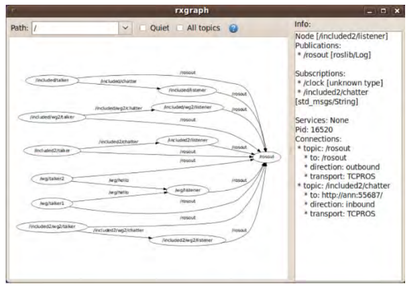
ORiN

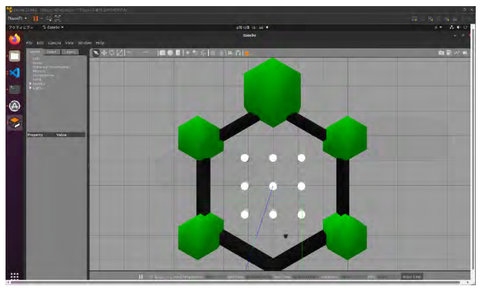
Robot Operating System

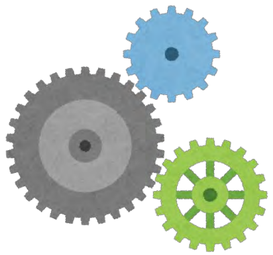
03 ROSって何？

Robot Operating System

- ロボット アプリケーションの構築に役立つソフトウェア ライブラリとツールのセット
- デバイスドライバー、アルゴリズム、開発ツールなどロボット開発に必要なものが揃っている
- オープンソースである



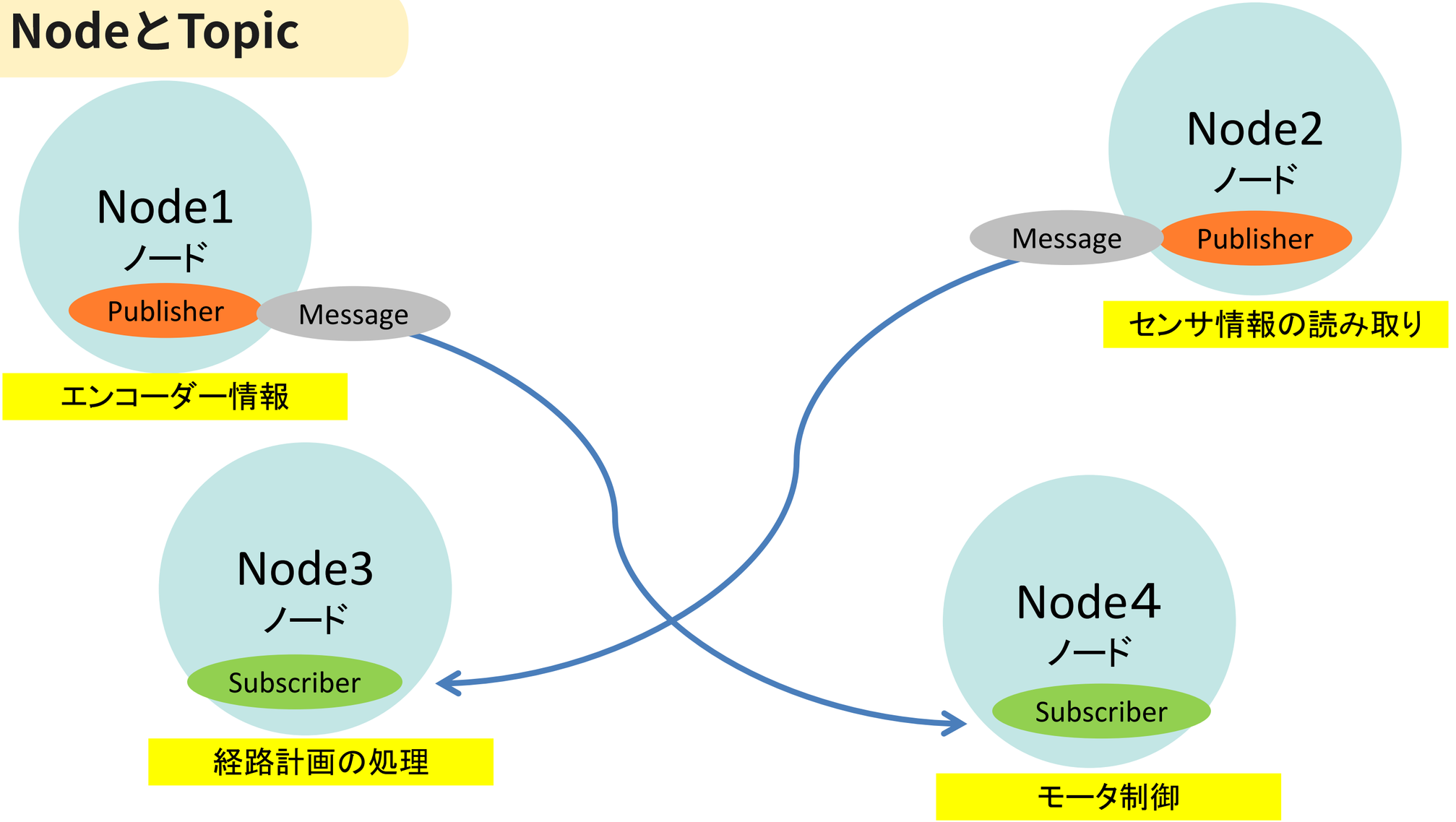




Plumbing ✚ Tools ✚ Capabilities ✚ Ecosystem

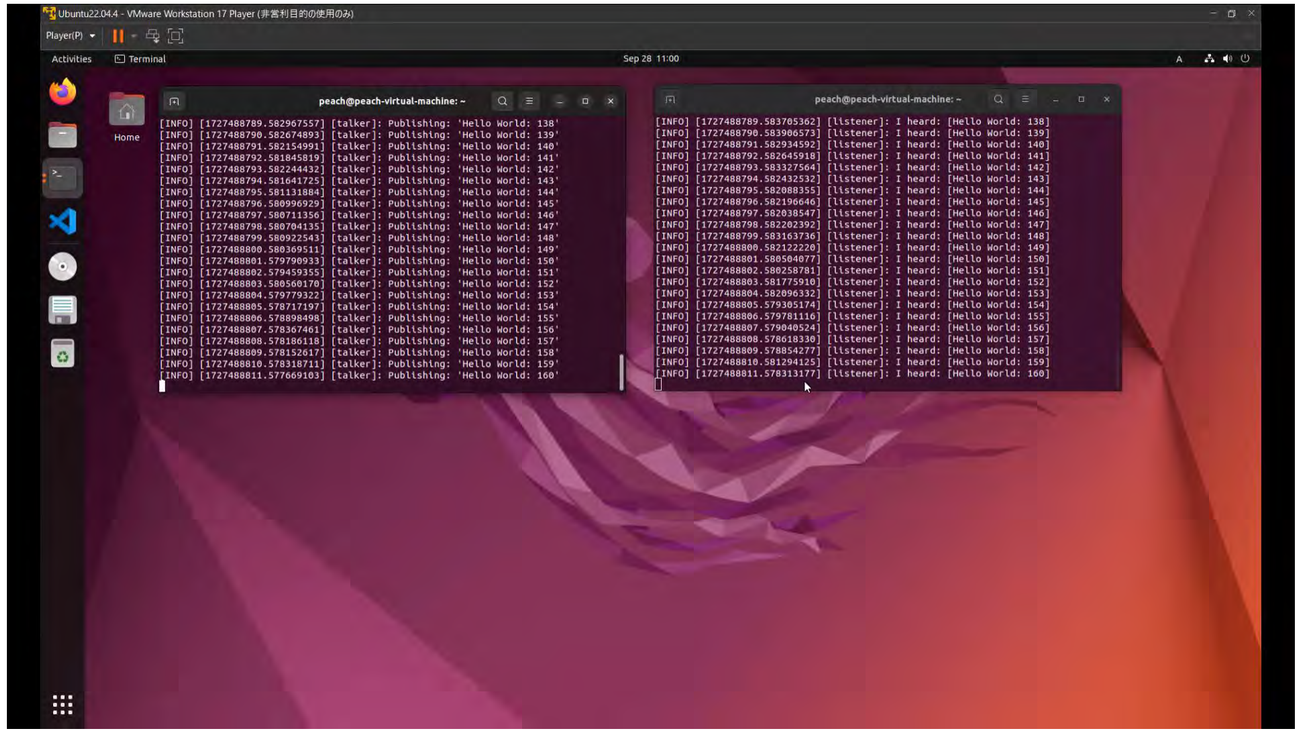
03 NodeとTopic

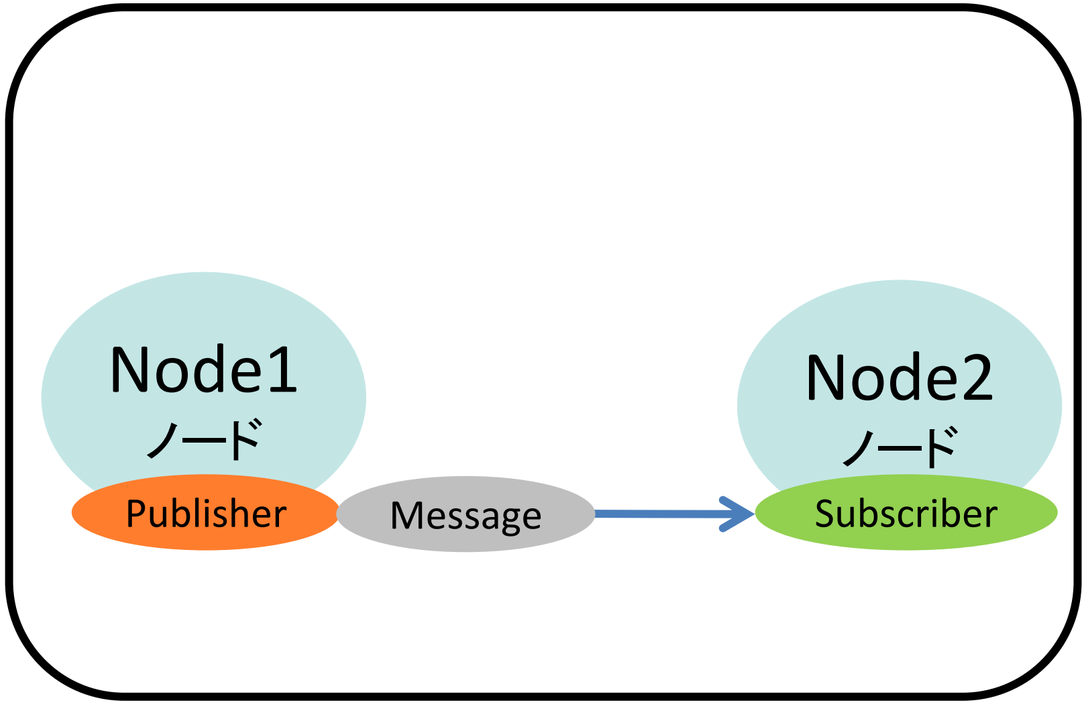
NodeとTopic



03 Node間通信

同一のデバイスでNode間通信

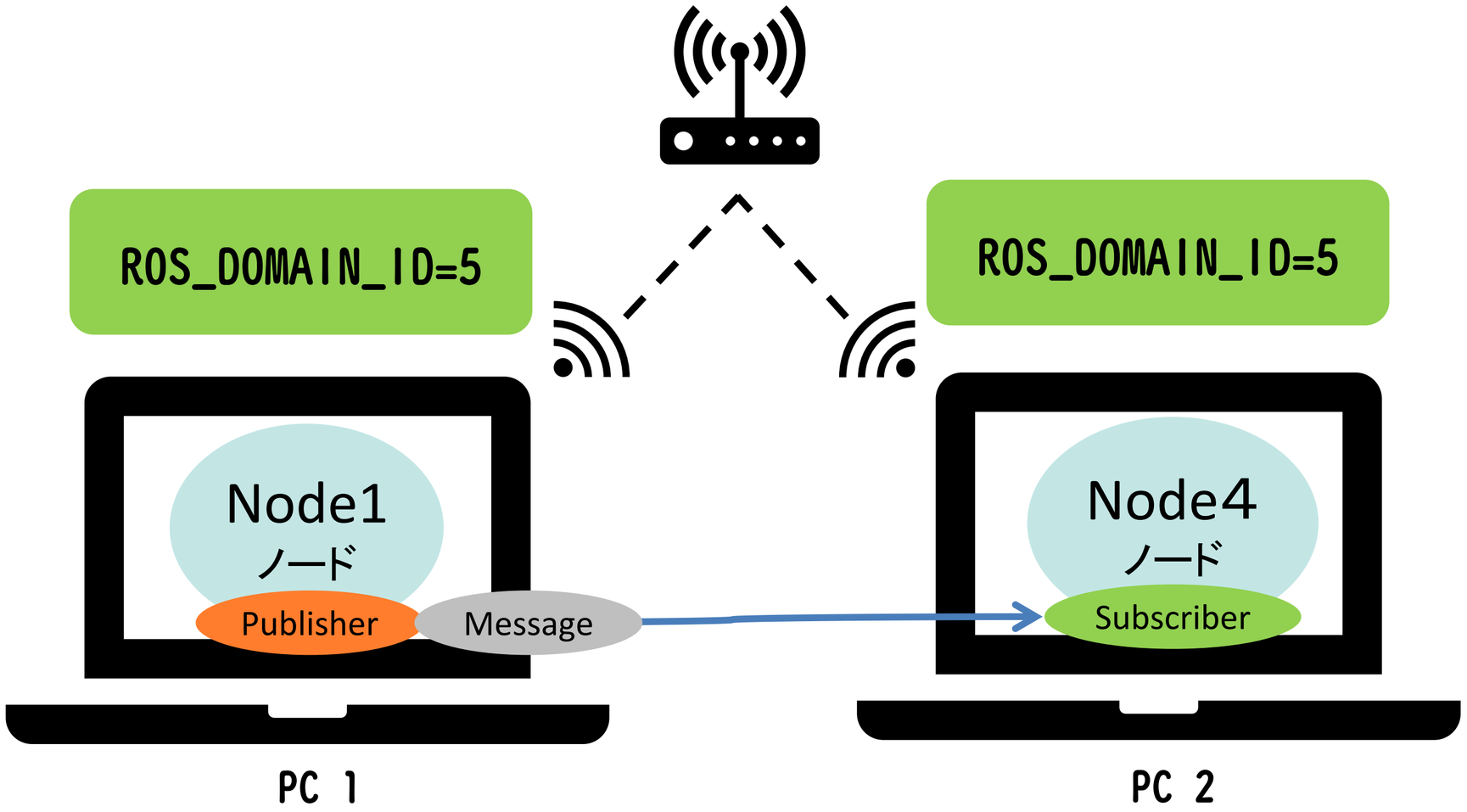




左の端末から右の端末に”Hello World”というメッセージを送信している

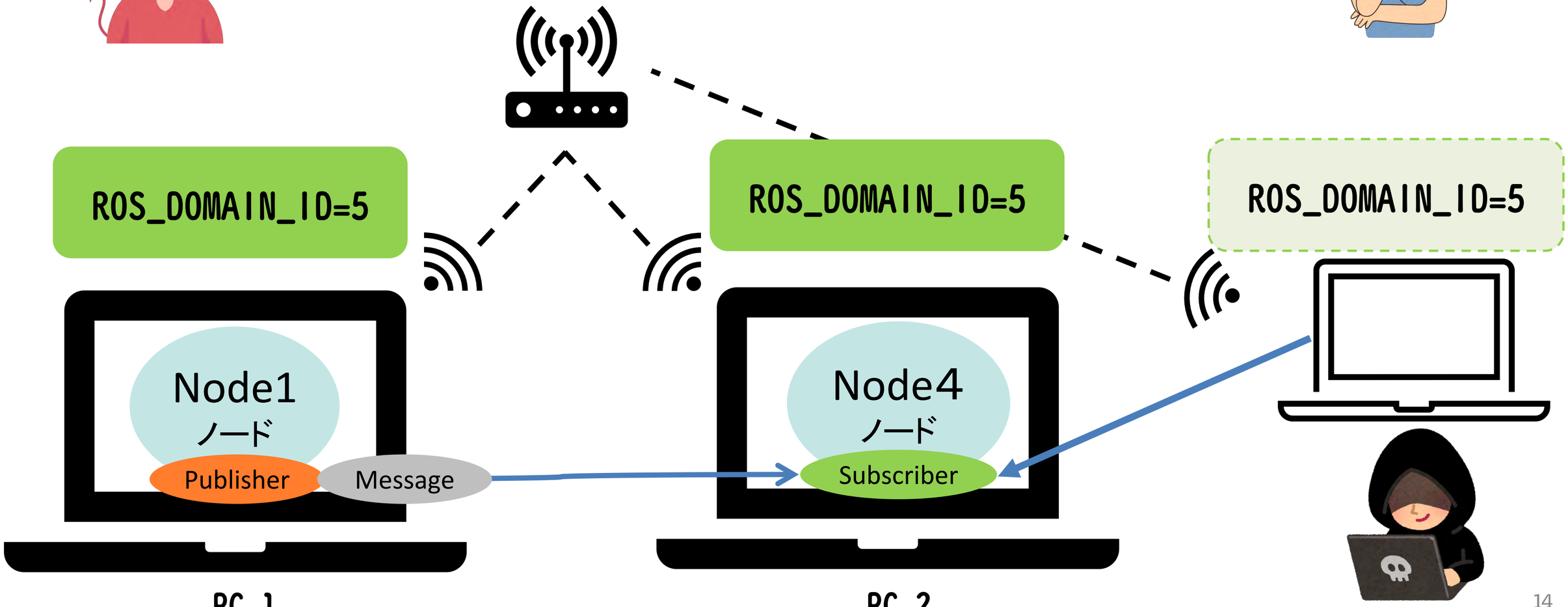
03 デバイス間通信

デバイス間でも通信ができる！



03 ROSのセキュリティに興味をもったきっかけ

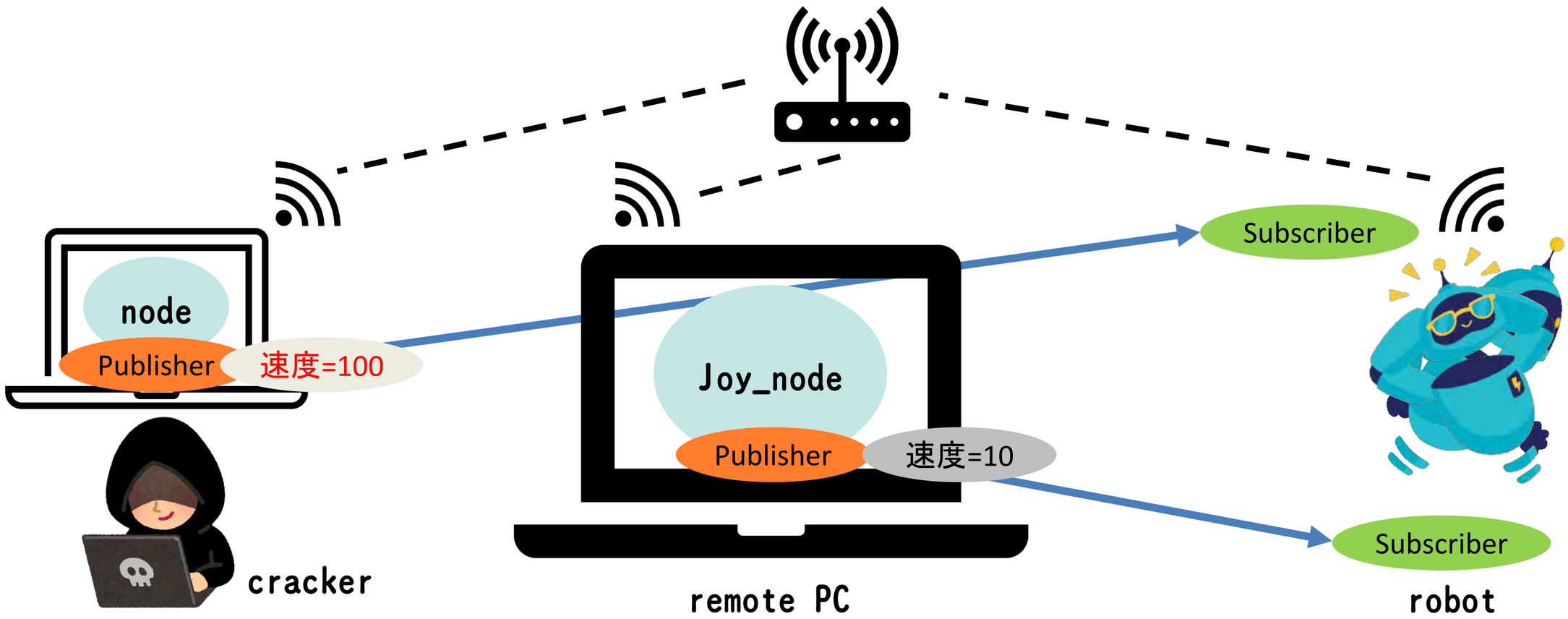
私のギモン：悪用できそう！



03 悪用したらどうなる？

悪用するとできること!?

ロボットを乗っ取ることが可能では？（暴走させるとか）



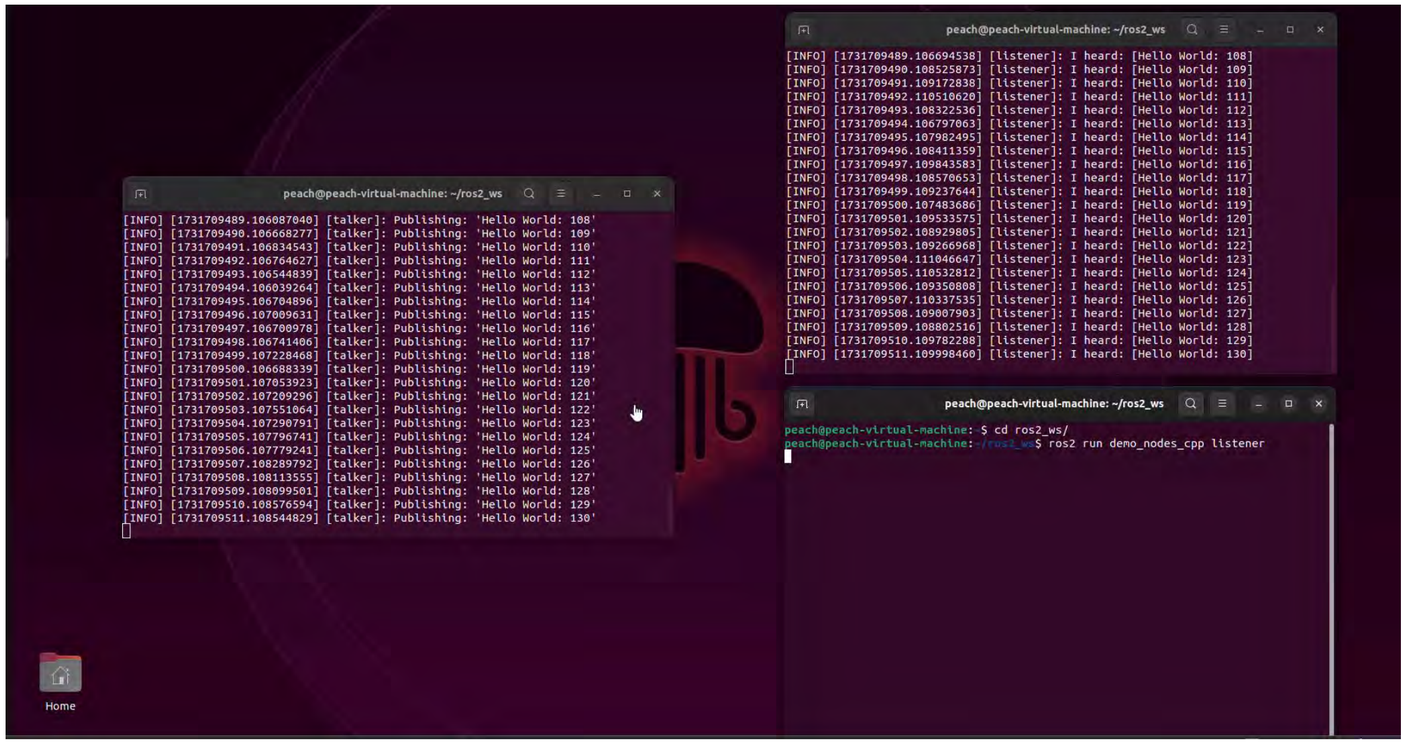
Sechack365で取り組んだこと

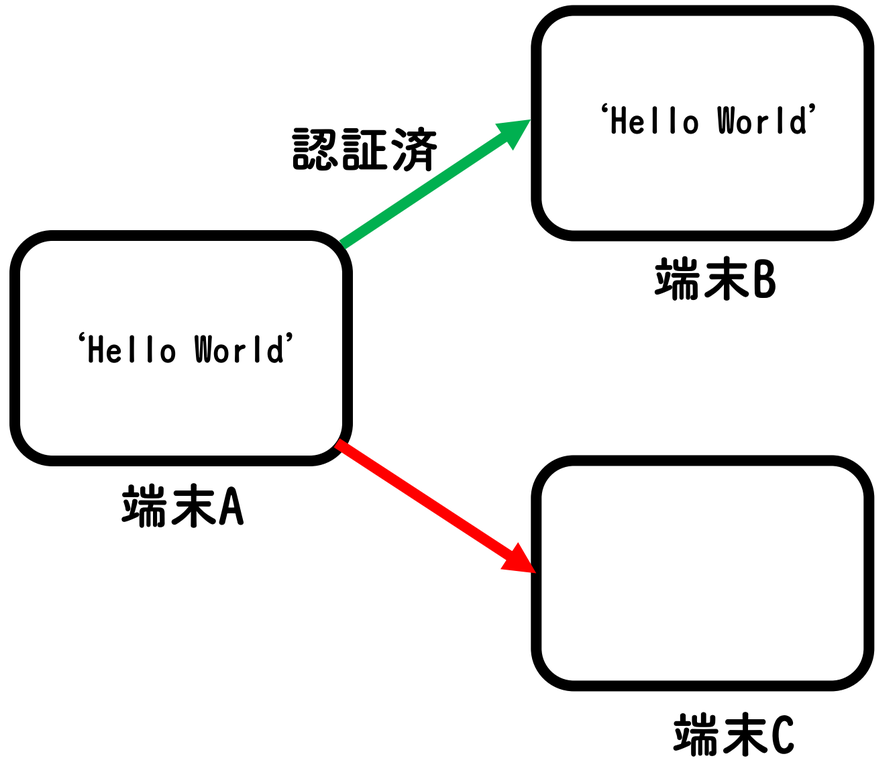
04 課題の設定：ROSのセキュリティを強化する

ソフトウェアベースでROSのセキュリティを強化したい

- **通信の暗号化**
  Topicの内容を第三者が盗聴できないようにする
- **Node間の認証**
  第三者にTopicの内容が改ざんされないようにする

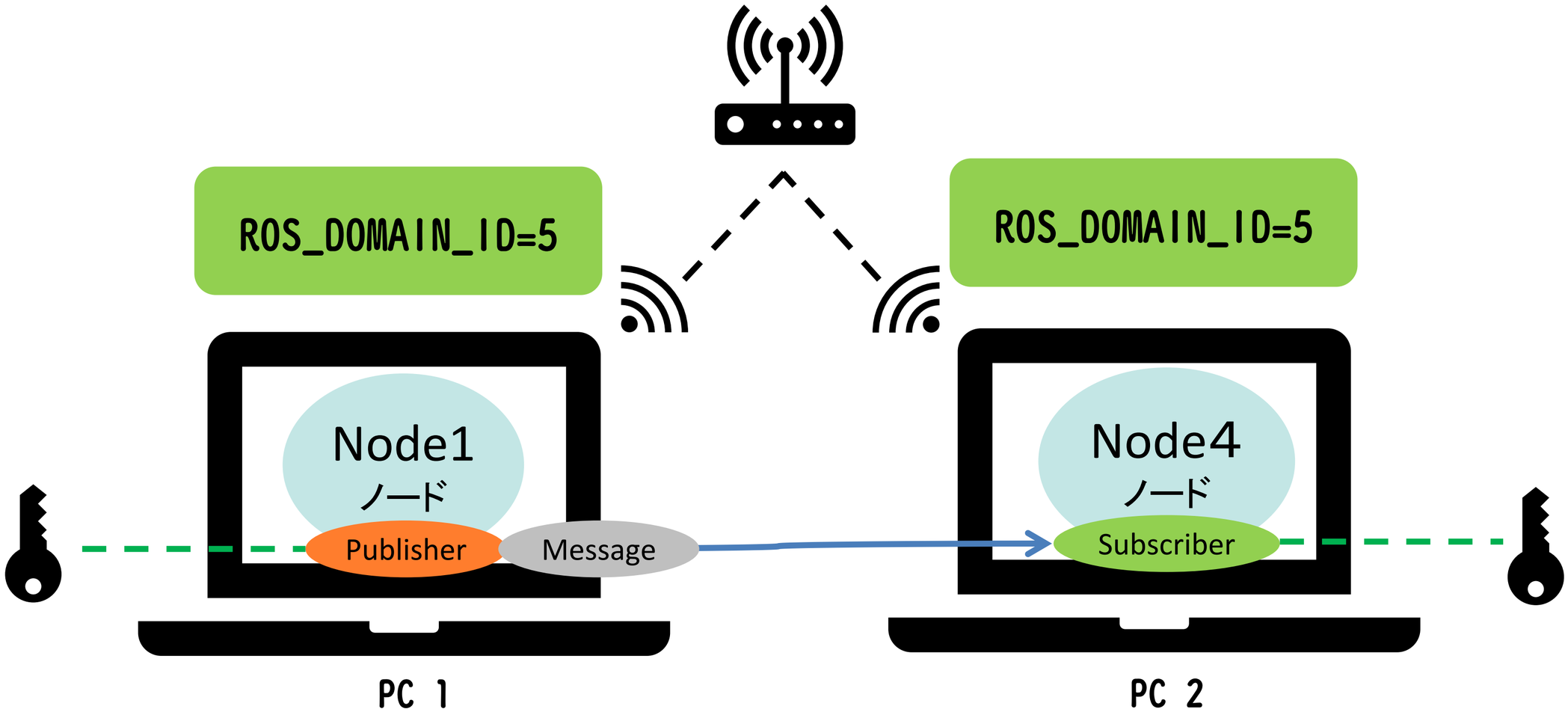
04 Node間認証





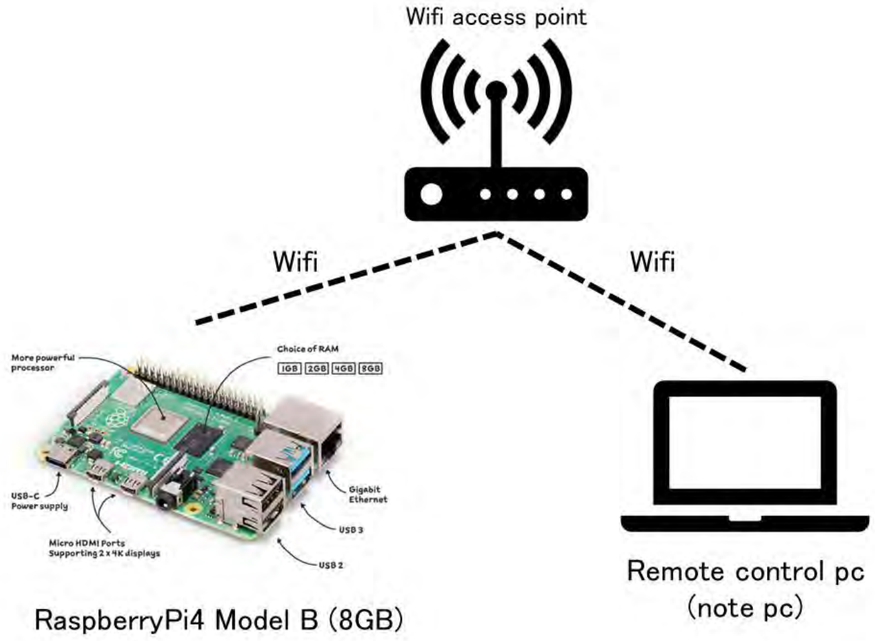
公開鍵暗号を用いて実装されている

04 Node間通信の暗号化

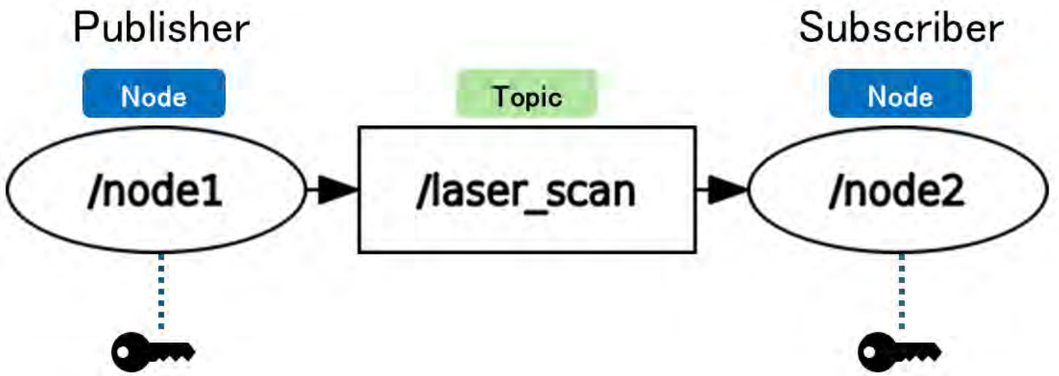


04 通信の遅延を測定してみた

実験方法



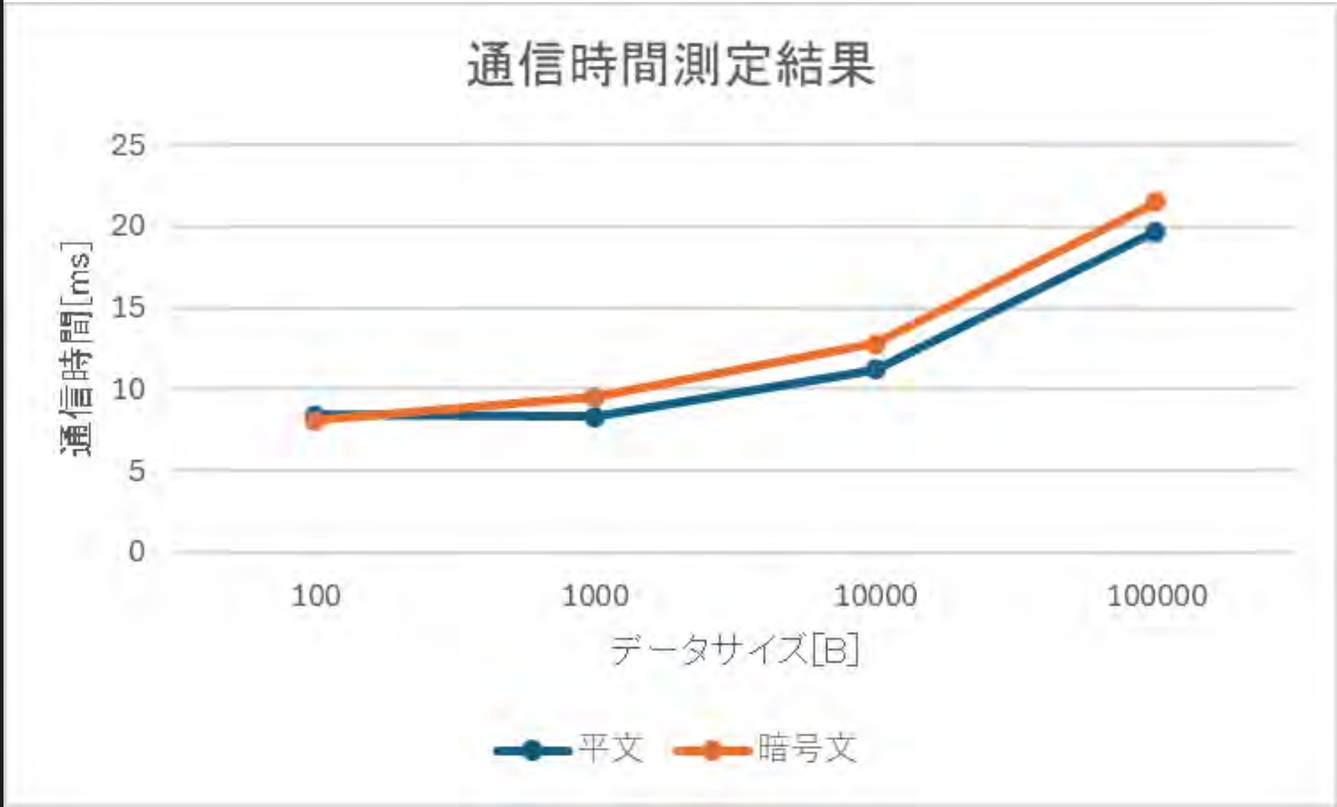
NodeとTopic



メッセージの暗号化による通信時間の遅延を測定した

04 測定結果

メッセージデータサイズと通信時間の関係

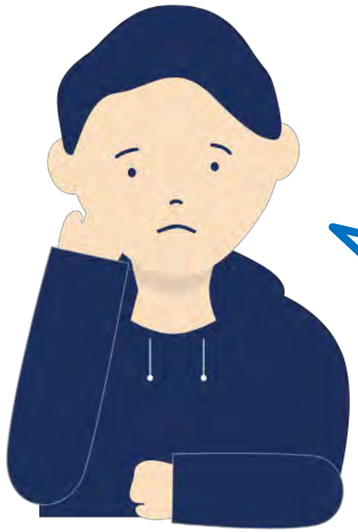


- メッセージを暗号化することによって，平文時よりも通信時間が1.2倍程度増加する
- データサイズが大きいほど，通信時間の差は増加する傾向がある

メッセージの暗号化によって通信時間は増加する

04 新たな疑問

- 通信時間の遅延はロボットの行動に影響を与えるだろうか

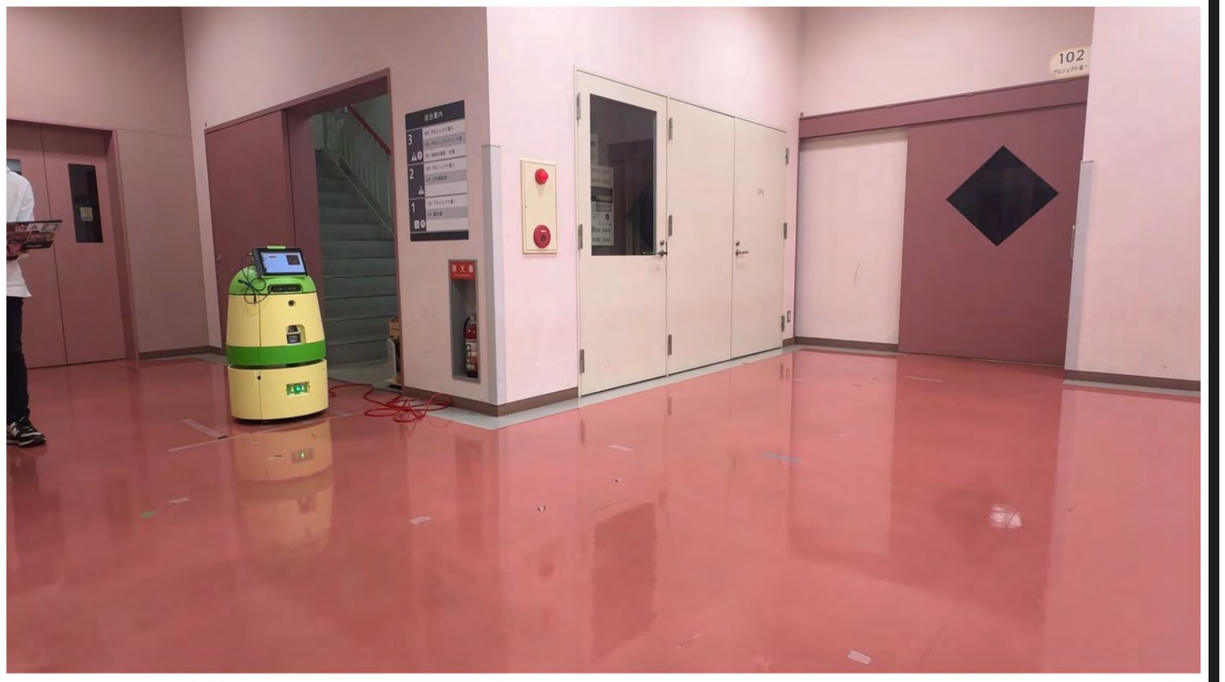


しかし…
ロボットの行動を評価する方法が分からない
評価基準をつくる！？

04 実際のロボットで測定してみた

暗号化した場合としていない場合のロボットの行動の比較

通常



暗号化

Remote-PCから一定周期で速度コマンドを送信した

撮影協力：神奈川工科大学　人間機械共生研究室（三枝亮研究室）

05 結果

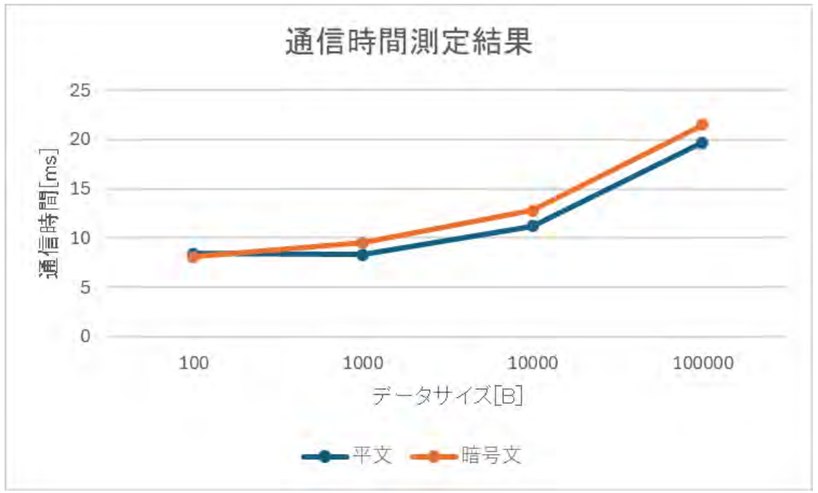
目視だと...

ほとんど差がない！

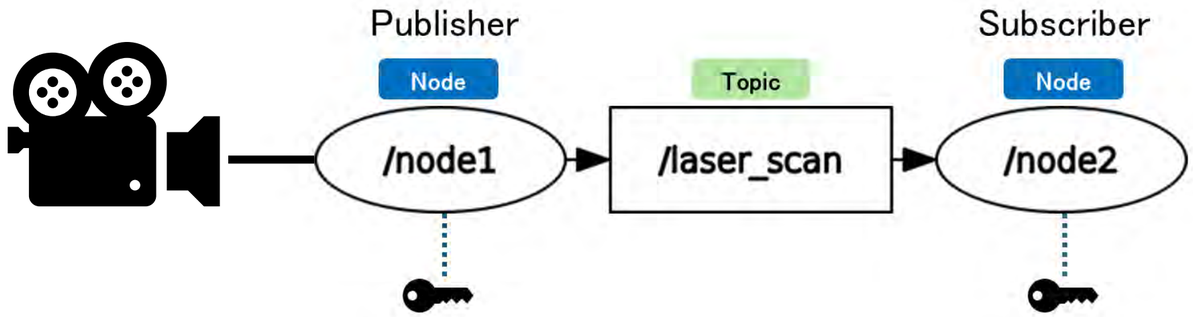
いや，暗号化した方が少し遅延している？

05 データサイズが大きいものにすれば...

メッセージデータサイズと通信時間の関係



画像などデータサイズが大きいもの



メッセージのデータサイズを大きくすれば

影響があるのでは？

今後の展望

05 セキュリティ強度を最適化する

周囲の環境に応じたセキュリティの変化

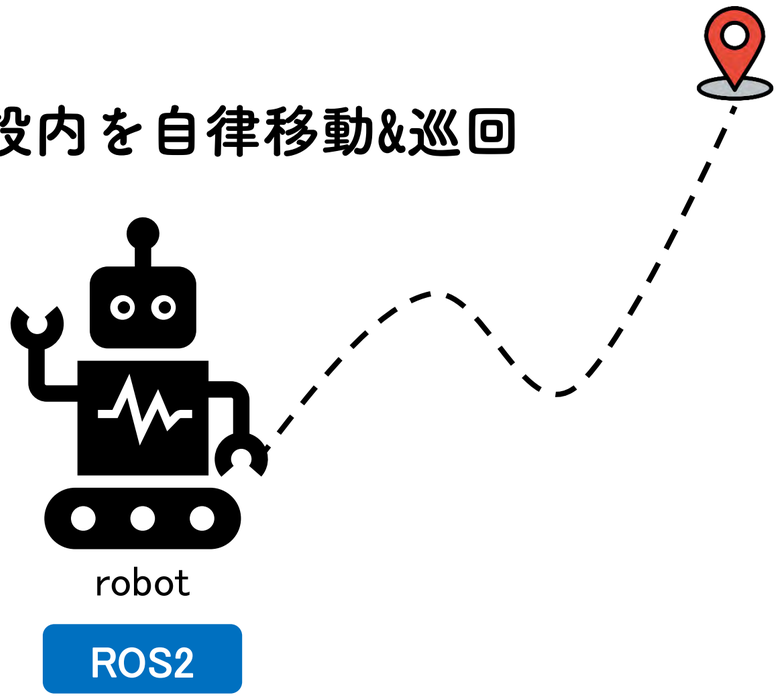
通常モード

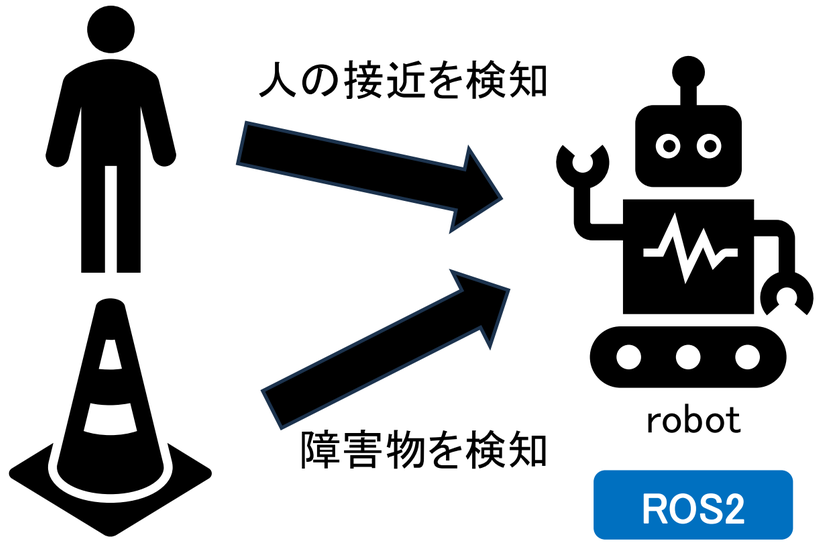
セキュリティ強度

Busyモード

セキュリティ強度の設定に強化学習を用いる

施設内を自律移動&巡回





人の接近により処理が増え
システムに負荷がかかる

06 まとめ

◆ロボットにもセキュリティが必要！

◆Node間の認証と通信の暗号化ができた

◆セキュリティの強化によるロボットの影響を調べる