ロボットオペレーティングシステムのセキュリティ研究

Security study of Robot Operating System

亘理克好・ネットワーク分科会・情報セキュリティ大学院大学

Abstruct:
The robot industry is expected to grow to an industry of 9.7 trillion yen in 2035. Not only industrial robots but also new fields like service field are expected to grow. An increase in robots leads to the possibility of becoming a target of a new cyber attack and can become a serious problem especially for service robots that operate near people. Under such circumstances, OS or middleware for robots are drawing attention, which greatly improves the complexity in developing robots with various functions by various hardware and efficient development in a short period of time. In this paper, paying attention to “Robot Operating System (ROS)” which is widely used in the world among middleware, we present overview of ROS and problems of security along with prior research.

1. はじめに

近年，様々な分野でロボットの活躍が期待されている．NEDOによる2010年公表のロボット産業市場予測によると，2035年には9.7兆円規模の産業へ成長すると予想されている．

そのような中，様々な機能を持つロボットに対し，より容易に開発を可能にするミドルウェアが使われるようになってきている．ロボットは個別機能を分散処理し機能を実現するが，それに適したソフトウェア環境を使用することで，開発期間の短縮や再利用可能なモジュールが利用できるといった利点がある．

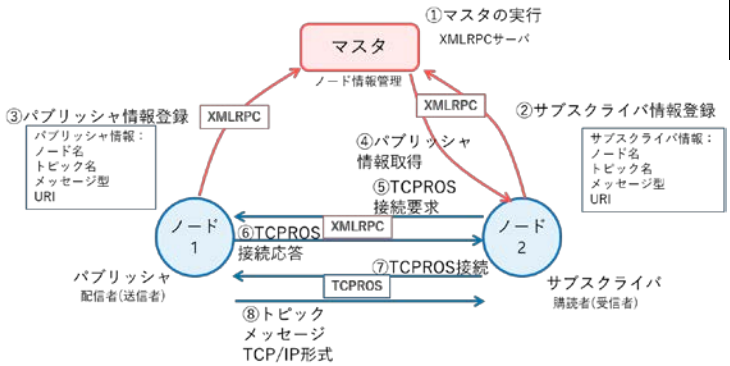
ロボット用のミドルウェア環境の中でも利用者が多いのが“ロボットオペレーティングシステム（ROS）”である．ROSはUbuntu Linux上で動作するミドルウェアである．

ROSには，通信ライブラリ，パッケージ管理などのツールが多々用意され，ユーザコミュニティにより5,000を超えるROSパッケージと80種類以上のセンサがサポートされている．

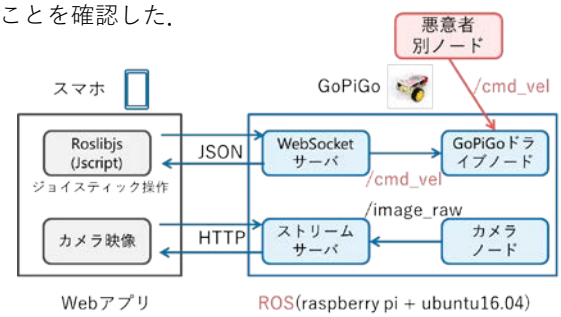
本研究ではROSに存在するセキュリティの問題点とその対策について検討することを目的とする．

2. ROS概要

ROSでは，実行可能な最小単位のプロセスをノードと呼びその集合で全体機能を実現する．ノードの情報はマスタノードが管理し，その情報に基づき各ノードが通信を行う．



通信は平文で行なわれ，認証はないため，容易に悪意ノードによる攻撃が可能である．簡単な車輪型ロボットを使ったROSノードテストにおいて悪意者のノードが移動指令を乗っ取ることができることを確認した．



3. 関連研究

ROS-RV	通信監視ノードを追加．事前定義されたモデルのランタイム検証を使用して予想される動作に適合しないアクションを検出する
ROS-ALG	ノードを認証する別のノードを用意し，ノードのログインリクエストに対し，認証と権限を応答する
Secure-ROS-Tarnsport	認証サーバを設置し，信頼できるノードのリストを持ち，サブスクライバがそれを受け取りそれを元に接続する
ROS-AES-Encryption	TLSハンドシェークによりノード間の認証を行い暗号化通信を行う
Secure ROS	IPSecを用い認証付き暗号で通信を行う
SROS1	TLSを用い認証付き暗号で通信を行う．アクセス制御が可能である
ROS2	2017/12に正式リリースされたROSの新バージョン．セキュリティが考慮された設計といわれ通信にDDSを使用する．暗号化通信とアクセス制御をサポートする

4. 考察

ROS1では容易に悪意者が接続できることが実際のテストで確認できた．そのような事象に対し，先行研究として様々な方法によりセキュリティを向上する手法が提案されており，また負荷に関しても考慮しておく必要があることがわかった．

2017年末に正式リリースされたROS2は通信方式がこれまでと変わりDDSを使用するように変更になり，セキュリティが最初から含まれているといわれている．しかし，キー管理についての検討や，負荷の問題，ログ出力などはどの程度考慮されているか明確になっていない部分もある．今後使用されるであろうROS2について検討していくことが必要であると考える．

5. 今後

現在，車輪型ロボットを使ったROS2のテスト環境を構築した．今後は，この環境を用いROS2のセキュリティ対策について把握し，想定システムでの脅威分析とテスト，それを元にした対策の検討を行っていく予定である．

参考文献

[1] ROS http://www.ros.org/
[2] B.Diberら Security for the Robot Operating System, Robotics and Autonomous Systems, Vol. 98, pp. 192–203, 2017.
[3] R. Whiteら SROS2 Tutorial, IROS, 2018