コンシュマー向けロボットの安全な運用に向けたセキュリティポリシー

齋藤 慶太[1,a)]　森 達哉[1,b)]

概要：コンシュマー向けロボット製品の多くはネットワークに接続して動作するため，既存の IoT デバイス等と同様に，攻撃者による侵入やマルウェア感染等のセキュリティ脅威がある．ロボットの動作は自由度が高いため，攻撃者はロボットに侵入した後に遠隔操作によって様々な物理的攻撃を行う可能性がある．例えばロボットが暖房器具に近づくことで火事や爆発等の物理的な被害をもたらすような脅威が考えられる．本研究はロボットの開発者が上述の脅威に対抗する際に参考となる汎用的なセキュリティポリシーを提案する．セキュリティポリシーはロボットが扱う様々な**入出力**とロボットが物理世界に対して行う様々な**行動**に対して適切な制御をかけることを狙いとする．ロボットを制御する OS として今日広く使われている ROS を題材として，入出力の代表例である通信に関するセキュリティポリシーを実現する具体的な方法を示す．また，ヒューマノイド型ロボットと掃除ロボットを対象として，行動に関するセキュリティポリシーをルールとして具現化した例を提示する..

キーワード：ロボットセキュリティ,ROS，IoT

Security Policy for secure robot operation

Keita Saito[1,a)]　Tatsuya Mori[1,b)]

Abstract: As consumer robot products are connected to the network, they have security threats such as attacks by intruders and malware infections as existing IoT devices do. Because the robot's motion has a high degree of freedom, an attacker can perform physical attacks by the remote control after exploiting the robot. For instance, a fire or an explosion could be caused by a remotely-controlled robot that approaches the heating appliance and turns on the switch. This work propose a set of generic security policies so that the developers of robot can secure their products. The security policy is aimed mainly to apply appropriate restrictions on the various I/Os and behavior of the robot. Using ROS, which is one of the most popular OSes for robot, as an example, we present the concrete methods to implement the rules on I/O and realize it on ROS. We also present several examples in which the policies on behavior are made into into a set of specific rules for the humanoid robots and cleaning robots.

Keywords: robot security, ROS, IoT

1. はじめに

米 IDC が発表した調査報告では，全世界におけるロボット産業の規模は 2016 年の 915 億ドル（約 10 兆円）から 2035 年には 1880 億ドル（約 20 兆円）にまで拡大すると予測されている [1]．今日のロボットの利用は製造，農林水産などがメインストリームであるが，エンターテイメントロボットや家庭用ロボットなどのコンシューマ向けロボット製品が登場し，一般家庭への普及の兆しがみえる．先の IDC によるレポートでは 2016 年のロボット市場では製造系が約 6 割を占める中，コンシューマ向けロボット製品は約 7 %に相当する 65 億ドル（約 7150 億円）を占め．今後

[1] 早稲田大学
Waseda University
[a)] keis@nsl.cs.waseda.ac.jp
[b)] mori@nsl.cs.waseda.ac.jp

の成長が見込まれている．普及したロボット製品の例として国内では Pepper [2] が著名であり，企業や商業施設，そしてアーリーアダプターと呼ばれる個人に広く普及した．

今後コンシュマー向けロボット製品が本格的に家庭に普及すれば，既存の IoT デバイス以上のセキュリティリスクが生じる．ロボット製品はその機能を高めるためにはネットワークに接続される必要があるため，攻撃者は脆弱性を悪用することでロボットの制御を奪うことができる．ロボットへの侵入は物理空間を対象とする自由度の高い攻撃が可能となることを意味する．ロボットは様々なアクションを可能とするセンサーやモーターを搭載しており，遠隔操作することで物理的攻撃—例えば暖房器具に近づくことで火事や爆発を引き起こすことも可能である．さらにロボットが有する特徴として，人間との円滑なコミュニケーション機能が挙げられる．遠隔されたロボットがオーナーである人間とコミュニケーションをとれば，嘘の情報を伝えたり，秘密の情報を聞き出すことが可能である [3]．

攻撃者による侵入にかぎらず，プログラムのバグや予期しない誤動作がもたらすリスクもある．例としてプログラムの誤動作やアルゴリズムの欠陥が原因で，ロボットが本来認識すべき対象物を見落としてしまう場合を考える．認識に失敗した結果，人間に対してロボットが衝突あるいは上部から落下する可能性がある．その相手が乳幼児であれば深刻な被害をもたらすことは想像に難くない．ロボット向けに開発されるアプリにもリスクがある．スマートフォンのアプリ配布モデルと同様，ロボットが実現するサービスに対してもアプリ化が進んでおり，ロボットのオーナーはアプリストアからアプリをインストールすることができる [4]．難読化されたマルウェアが信頼されるアプリストアにアップロードされれば，ユーザはマルウェアとは気が付かずにアプリをダウンロードしてインストールしてしまうだろう．標的型攻撃によって，システムのパッチを装ってロボットにマルウェアがインストールされる危険もある．

2.2 節で示すように，今日市販されているコンシュマー向けロボット製品にはいくつかの重大な脆弱性をもつものがある．特に深刻なのは認証機構の欠落であり，攻撃者は様々なチャネルから遠隔操作を実現出来てしまうリスクがある．こうした脆弱性は広く報告されているものの，未だに対策がなされていない製品も少なくない．著者らはそれらの製品は依然として実験的なフェーズにあり，セキュリティ対策が本格化するのは製品の普及が進んだ後になると見ている．しかしながら上述したような物理的な脅威を考慮すると，早い段階でロボットを安全に運用するための**セキュリティポリシー**を明らかにし，そのポリシーに基づく対策，すなわち**ロボット向け OS におけるセキュリティ制御のデザインと実装**を行う必要性を提唱する．

上述の背景の下，本論文はコンシュマー向けロボットを安全に運用するための汎用的なセキュリティポリシーを提案する．セキュリティポリシーはロボットが行う様々な入出力に関する**入出力ポリシー**と，ロボットの行動に関する**行動ポリシー**から成る．ロボットには様々な特徴・用途があり，アーキテクチャも多様であることからロボット向けのセキュリティポリシーは用途や機種に依存しないように抽象度を高め，汎用的なものとする．その上でロボットの開発者がロボット製品の OS をセキュアに設計する際に参考となる指針を与えるように心がけた．本研究ではセキュリティポリシーの具体的な適用例を示す．はじめにロボット制御用の OS として広く採用されている ROS を対象として，通信に関する入出力ポリシーを実現するための具体的な方法を示す．つぎにヒューマノイド型ロボットと掃除ロボットを対象として，行動ポリシーをルールとして具現化した例を示す．

2. 背景

本章ではコンシュマー向けロボット製品が搭載する代表的なメタ OS を簡単にレビューする．次にそれらのメタ OS を搭載したロボット製品に共通してみられる既知の脆弱性をまとめた結果を示す．

2.1 ロボットのメタ OS

ROS

ROS (Robot Operating System) [5] はロボット開発のためのオープンソースプラットフォームであり，デバイス制御やプロセス管理などを行うメタ OS である．ROS は世界中の研究機関や製品開発現場で利用されており，今後幅広い製品で採用される可能性が高い．ROS では複数のノードと呼ばれるプロセスがネットワーク上で通信をおこなう分散型のアーキテクチャを採用している．ノード間でのデータのやり取りは主にトピックを介した pub/sub 型の通信で行われ，ノードがあるトピックに対してデータを発行 (publish) すると，そのトピックを購読 (subscribe) しているノードに対して送信されたデータが送られる．トピックはデータの種別ごとに存在し，例としてはカメラの映像を扱うトピックやロボットの移動方向に関するトピックなどが挙げられる．各ノードが発行・購読しているトピックは master と呼ばれる特別なノードが管理しており，あるトピックに対してデータを発行するノードと購読するノードが存在する場合， master は発行者と購読者がお互いに通信するのに必要となる情報を提供し，以降は 2 つのノード間でデータを送受信する．

NAOqi OS

NAOqi OS は AldebaranRobotics 社が開発した Linux をベースとした独自のメタ OS であり，NAO [6] や Pepper [2] の他， ROMEO などに搭載されている．NAOqi OS には Python, C++, JavaScript 用の API が提供されており，ロボットの制御や各種センサー情報の取得，ロ

ボット本体システムの操作などを行うことが可能である．例えば，ロボットのカメラ映像を取得する，ロボットを移動させる，ロボットを再起動させる，といったことが可能である．これらの API を利用するための SDK は，ユーザー登録をすることで誰でも自由に利用できる．各種 API を利用する際には，まず NAOqi OS とセッションを確立する必要がある． Python，C++ によるセッションの確立にはロボットの IP アドレスと API 用のサービスが動作しているポート番号を， JavaScript によるセッションの確立にはロボットの IP アドレスのみをそれぞれ指定すればよい．セッションが確立された後，そのセッションを介して各種 API を利用できる．

2.2 コンシュマー向けロボット製品の脆弱性

Cesar ら [7] は 2017 年 3 月当時までに販売されていたロボット製品に対してセキュリティに関する調査を行った．調査対象のロボット製品は Asratec Corp 社，Rethink Robotics 社， ROBOTIS 社，SoftBank Robotics 社，UBTECH Robotics 社，Universal Robots 社が開発した合計 10 数台のロボットである．調査の結果，適切な認証・認可の機能が備わっていない，情報が全て平文でやり取りされているなどの共通した脆弱性が報告されている．

認証機能の欠落により，ロボットが存在するネットワーク上で API をにアクセスすることにより，任意の端末がロボットの制御を奪うことができる．攻撃者はこのようなロボットの脆弱性を利用することによって，ロボットに搭載されたカメラの映像を監視しながら，任意の場所にロボット移動させる遠隔操作が可能となる． 1 章で述べたように，遠隔操作によって家事や爆発につながる危険行動，あるいは人に対する物理的あるいは精神的ダメージを引き起こす脅威が生じる．これらの調査対象のロボット製品にはオープンソースである ROS [5] を採用した製品が存在する．ROS は海外のロボット開発プロジェクトでの採用率が高い．認証機構にかかる脆弱性は ROS の実装に起因するため，今回の調査対象となっていないコンシュマー向けロボット製品にも同様の脆弱性を持つ製品が存在すると考えられる．

上記の調査では脆弱性の概略について報告はしているものの，それぞれの脆弱性が個々のロボット製品に対してどのように悪用されるかに関して具体的な方法や手順等は一切示していない．そこで我々はあるロボット製品を対象に PoC 攻撃コードを作成し攻撃の検証を行った[*1]．この結果，外部ネットワークからロボットに対して遠隔操作を実現することが可能であることが判明した．

[*1] 5 章で示す理由により，本稿ではその製品名や攻撃の手順，実装方法は示さない．

3. ロボットのセキュリティポリシー

3.1 セキュリティポリシーの必要性と目的

2 章で示したように現在市販されているコンシュマー向けロボット製品の多くはセキュリティ対策は十分であるとは言い難い状況にある．我々がロボット製品向けに作った遠隔操作の攻撃コードは実際に一部の製品に対して有効であることを検証しており，深刻な脆弱性が残っている状態でロボットが販売，運用されている．さらには 1 章で議論したようにロボットには脆弱性を悪用した侵入に加え，ソフトウェアの不具合やマルウェアによる脅威が存在し，今後ロボットの普及に伴いそのような脅威が顕在化することが予想される．

上述したような状況に対応するためにはロボットの開発者や運用者が参考にする適切なガイドラインが必要である．しかしながら著者らの知る限りそのようなガイドラインはこれまでのところ存在しない．本章ではロボットの安全な運用に向け，コンシュマー向けロボット製品の OS が満たすべきセキュリティポリシーを提案する．このセキュリティポリシーは，ロボットの開発者がロボット製品の OS をセキュアなものとする際に必要となる指針を与えるガイドラインであり，ロボット向けアプリ開発者やロボットの運用・管理者が参考にすることもできる．ロボット製品は用途やアーキテクチャが多岐に及ぶため，セキュリティポリシーはそれらの差異に依存しないよう，抽象度を高めたハイレベルな記述に抑制している．次章で示すように対象となるアーキテクチャや用途を定めればセキュリティポリシーを具体的なルールや実装に落とし込むことができる．以下ではロボット OS が行う入出力に関するセキュリティポリシーを**入出力ポリシー**，ロボット OS が行う物理的な行動に関するセキュリティポリシーを**行動ポリシー**と呼ぶことにし，それぞれの概略を示す．

3.2 入出力ポリシー

コンシュマー向けロボットの特徴としてカメラ，マイク，9 軸センサー，タッチセンサー，ソナーセンサー等，様々なセンサーを搭載していることが挙げられる．これらのセンサーに対する入力あるいは出力も適切に制御する必要がある．センサーの読み取り値などを外部に出力する場合，そのデータを攻撃者が盗聴可能であれば個人情報の流出に繋がる可能性がある．例えば加速度センサーから位置情報を推定することが可能である [8]．前述したようにコンシュマー向けロボットはスタンドアローンで動作することは少なく，その機能をフルに活用するためにはネットワークに接続されたオープンシステムとして構成する必要がある．ネットワークに接続することによって他のデバイスとの協調，音声認識エンジン等のクラウドサービスの利用などが

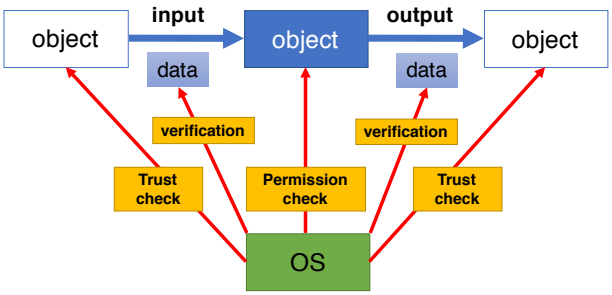

図 1　入出力ポリシーの概要

表 1　入出力ポリシーにおけるオブジェクトとデータの例.

	具体例
オブジェクト	センサー，プロセス，リソース，外部デバイス
データ	通信データ，センサー値，プロセスの出力，ファイル

可能となる．2 章で示したように，ロボットがネットワークを介して他の端末と通信を行う際に認証機構が不十分である場合，攻撃者による不正な操作を引き起こす可能性がある．さらにロボットが扱うデータが妥当なものであるかを検証する必要がある．例えばある条件下においてロボットの動作を支配するモーターに対してきわめて大きな数値が入力されることにより，物理的なダメージを引き起こす可能性がある．

以上よりロボット OS はロボットが扱う様々な入出力に関して，(1) データの入出力を行うオブジェクトはその権限があるか，(2) 入出力を行う相手は正しいか，(3) 入出力しているデータの数値は適切であるかを監視し，適切に制御する必要がある．コンシュマー向けロボットの入出力ポリシーは以下のようにまとめることができる (図 1 参照).

コンシュマー向けロボットの入出力ポリシー

- **Permission check**: オブジェクトがデータを入出力する権限を持っているかを確認しなければならない
- **Trust check**: オブジェクトがデータを入出力する他のオブジェクトは信頼できる相手であるかを検証しなければならない
- **verification**: オブジェクトが扱うデータが適切な値であるかを検証しなければならない

ここにオブジェクトおよびデータの具体例を表 1 にまとめた.

3.3　行動ポリシー

ロボットが IoT デバイス等の他のシステムと大きく異なる特徴は，物理世界に対する行動に大きな自由度があることである．ロボットはその用途によって様々な行動をする．例えば自立歩行ロボットはどこにでも歩いていくことができる．そしてその行動が適切に制御されなければ物理的な被害をもたらす可能性がある．ここでロボット OS が入出力ポリシーにしたがうだけでは十分ではないことに注意したい．例えばロボット上で動作するプログラムに異常行動を引き起こすバグが入る可能性や，信頼されるサーバ上に異常行動を引き起こすマルウェアがアップロードされる可能性がある．したがって我々は明確なポリシーにしたがってロボットの行動に何らかの制限をつける必要がある.

ロボットの行動規範を定めた規則としてアシモフによるロボット工学三原則 [9] とおよび Engineering and Physical Sciences Research Council (EPSRC) が 2010 年に制定した Principles for designers, builders and users of robots [10] が良く知られている (それぞれ下記参照).

ロボット工学三原則

- **第一条**: ロボットは人間に危害を加えてはならない．また，その危険を看過することによって，人間に危害を及ぼしてはならない.
- **第二条**: ロボットは人間に与えられた命令に服従しなければならない．ただし，与えられた命令が，第一条に反する場合は，この限りでない.
- **第三条**: ロボットは，前掲第一条および第二条に反するおそれのないかぎり，自己を守らなければならない.

Principles for designers, builders and users of robots

- Robots are multi-use tools. Robots should not be designed solely or primarily to kill or harm humans, except in the interests of national security.
- Humans, not robots, are responsible agents. Robots should be designed; operated as far as is practicable to comply with existing laws & fundamental rights & freedoms, including privacy.
- Robots are products. They should be designed using processes which assure their safety and security.
- Robots are manufactured artefacts. They should not be designed in a deceptive way to exploit vulnerable users; instead their machine nature should be transparent.
- The person with legal responsibility for a robot should be attributed.

これらの原理・原則は必ずしもすべてがロボットのセキュリティに関わることではなく，また人間によるロボットの利用に関する原則も含まれている.

著者らは上記 2 つの原理・原則を参考とし，また既存のシステムに対するセキュリティ・プライバシー脅威から得られた知見をベースとして，以下のようにコンシュマー向けロボットの行動ポリシーを規定した.

コンシュマー向けロボットの行動ポリシー

- **Physical Hazards**: ロボットは生物，物，自己自身等あらゆるものに対して物理的な危害を加えてはいけない.
- **Authority**: ロボットは使用者が許可していない人間や機械の命令にしたがってはいけない.
- **Privacy**: ロボットは使用者の許可なくプライバシー情報を漏えいしてはならない.
- **Faithfulness**: ロボットは人間や他の生物を騙したり，精神的なストレスを与えてはいけない.

我々の目的は上記に示したポリシーが完璧なものであると主張することではなく，成熟したロボット向けセキュリティポリシーの完成に向けたファーストステップを示し，研究者，開発者，ユーザとの議論および実機を用いた実験と運用を通じて今後さらに洗練させていくことを狙いとしている．ロボット向けの行動ポリシーの実装や解釈には本質的に難しい問題が含まれることも付記しておく．例えばロボットが人間に衝突することを回避するために自己を犠牲にせざるを得ない場合，すなわち互いに相反する条件に遭遇した際にロボットはどのように行動するべきか．このような問題はロボット三原則の元となったアシモフの著書 [9] でも啓示されている．このような問題は科学技術倫理の領域に踏み込むものであり，今後幅広い視点で議論することが必要である．

4. セキュリティポリシーの適用・実装例

本章では，3 章で導入したセキュリティポリシーを実際のロボット製品に対して適用・実装を試みた例を示す．はじめに 4.1 節では 2 章で示したコンシュマー向けロボット製品の通信に関する脆弱性を対象として，セキュリティポリシー (入出力ポリシー) を適用・実装した例を示す．次に 4.2 章では行動ポリシーをヒューマノイドロボットおよび掃除ロボットに適用する方法を示す．

4.1 入出力ポリシーの適用・実装

ケース 1: ROS

ROS におけるロボットの入出力はトピックを介したものであるため，トピックにアクセスを信頼できるノードのみに制限することで入出力ポリシーを守ることができる．こうしたポリシーを ROS 上で実現した例として，SROS [11] がある．SROS では x.509 証明書による PKI 基盤と TLS 通信による通信の暗号化を ROS に導入している．通信内容の暗号化により信頼できない第三者が情報を傍受することの防止や，証明書によって信頼する相手の真正性を担保できる．すなわちこれらの機能は trust check に相当する．

また，ノードごとにアクセスできるトピックを設定ファイルによって管理する機能や， AppArmor [12] といったアクセス制御機能が導入されている．これらは，入出力ポリシーにおける permission check に相当する．

一方で，入力された値がロボットの操作にとって適切なものかを判断する verification に相当する機能は SROS には実装されていない．ロボットは様々な性質や用途を持つため，入力値が適切であるかを判断する基準を一般化することは難しい．さらにその基準の多くはきわめて複雑なものである． したがって，そのようなポリシーは SROS 上にビルトインで実装するのではなく，ロボットを制御する各ノードが 4.2 章で示すような行動ポリシーの例を参考にして verification を行うように実装する形態が現実的であると考えられる．

ケース 2: NAOqi OS

NAOqi OS を搭載するロボット製品の入出力先（オブジェクト）は入力元がロボットが接続する外部ネットワーク上のマシン，およびマイク，カメラ等のセンサーであり，出力先がロボットが接続する外部ネットワーク上のマシン，およびスピーカー，モーターなどの出力装置である．以下ではこれらのオブジェクトに関して入出力ポリシーを適用するケースを考える．

はじめにロボットが接続する外部ネットワークとの通信の制限について述べる．NAOqi OS を搭載したロボットのネットワーク上での接続先はアプリストアやアプリが利用するデータサーバー， web サービスなどが挙げられる．ロボットが接続される相手はアプリ毎に異なるため，アプリのメタデータとしてそのアプリが接続するドメイン名，もしくは IP アドレスをホワイトリストとして登録しておき，指定外の接続先への接続を許可しない仕組みを導入することで意図しない相手と通信をしてしまうリスクを軽減できる．このホワイトリストは，ユーザがアプリをインストールする際の指標として非常に有用である．さらに，接続先の真正性を確保するために通信時に証明書を用いた SSL/TLS を利用することで，入出力ポリシーにおける trust check が可能となる．

次に，外部ネットワークとロボットの間で送受信されるデータについて考える．ロボットは外部ネットワークから得られた情報とセンサーの値を入力値として受け取る．ロボットはこれらの入力値をそのまま，あるいは入力値をもとに処理を行った結果を出力とする．よってロボットの出力にはカメラ映像やマイクの音声などのプライバシー情報を含む可能性がある．こうしたデータは信頼されたオブジェクトにのみ出力されなければならない．また，権限を持たないオブジェクトがスピーカーやモーターといった出力装置を利用できないようにする必要がある．

上記のデータに関する制限を実現する例として，センサーや出力装置を利用する権限を permission として設定することが考えられる．NAOqi OS を搭載したロボットにおいて，センサーや出力装置を利用するオブジェクトはインストールされたアプリと外部ネットワーク上のマシンである．これらのオブジェクト毎に利用するセンサーや出力装置が異なるため，permission は各アプリ，各 IP アドレス毎に設定する必要がある．さらに，permission は情報の読み取りに関する read permission と出力装置の利用に関する execute permission の二つに大別できる．permission を適切に設定することにより，入出力ポリシーにおける permission check が可能となる．

具体定期な例としてヒューマノイド型ロボットが見た物体を言い当てるアプリを考える．このアプリの機能は以下の通りである．

表 2 permission の設定例

オブジェクト	リソース	permission
解析サーバー	カメラ	read
解析サーバー	スピーカー	execute
アプリ	カメラ	read
アプリ	スピーカー	execute
アプリ	マイク	read
アプリ	腕部分のモーター	execute

- 取得したカメラ映像を画像解析の web サービスを提供するサーバー（以下，解析サーバー）に送信し，画像から物体認識した結果を音声で出力する．
- ユーザーはロボットが推測した答えと実際に見せた物体が同じかどうかを判断し，その正誤をロボットのマイク経由で通知する．
- 予測結果の回答や答え合わせをした際の反応時にはスピーカーを用いて音声を出力し，腕のモーターを動かして身振りを行う．

この場合，permission は表 2 のようになる．表 2 に示す permission を設定した場合，このアプリは指定した解析サーバー以外にカメラ映像を送信しないことが担保できる．また，解析サーバーからロボットのモーターを操作するための命令が送られてきた場合も，解析サーバーに execute permission が設定されていないため，ロボットの制御を奪われない．またアプリが腕以外のモーターを動かすことも制限できるため，不正な操作が行われる確率を低減できる．

以上のような permission check によって信頼できるオブジェクトとのみ通信を行うことができる．しかし，信頼できるオブジェクトとのみ情報をやり取りしていた場合であっても，アプリのバグや突発的な外的要因により，ロボット自身やその周囲の環境に対して安全を確保できなくなってしまうケースが想定される．例としては階段の上に位置しているロボットが前進するという命令を受けてしまい，ロボットが落下による衝撃で破損してしまったり，階下の物体や人間に対して危害を加えてしまう場合などである．このようなケースでは，自身の現状態の認識結果に基づいて，この後に予定している前進移動によって危険な状態に陥ってしまうか否かを判断し，危険な状態になると判断される移動距離が入力された場合には行動を停止するべきである．これは入出力ポリシーにおける verification の適用例である．どのようなケースについて移動距離の閾値を設定すべきかは 4.2 章で議論する．

4.2 行動ポリシーの適用

行動ポリシーは適用されるロボットの特徴や用途によってその実装は大きく異なる．ここではある特定の機能を持つロボットを対象に，ロボットが動作している文脈に応じて周囲の環境がある条件を満たした場合に行うべき動作をいくつかのルールとしてまとめたものを紹介する．対象とするロボットの特徴や紹介するルールは，現在実際の製品として販売されているものの挙動を参考にした．紹介したルールは入出力ポリシーにおける verification に相当するステップでの閾値を決定する指標として利用できる．

ロボットがセンサー読み取り値を元に周囲の環境が特定の条件を満たしているかを判定するためには，カメラ映像や加速度センサーを利用したオドメトリや物体認識が正確に行われる必要がある．これらの技術は現在活発に研究が進められているが，あらゆる分析をリアルタイムに，かつ正確に行うことは難しい．しかし，ここではあくまで今後開発されるロボット製品の行動に関するポリシーについて議論を行うために，こうした状況の分析が正確に行えるようになることを前提とする．

ケース 1: ヒューマノイド型ロボット

ヒューマノイド型ロボットは，姿勢制御が難しいため周囲の環境を適切にフィードバックしながら行動する必要がある．そのため，カメラやソナー，感圧センサーといった様々なセンサー類が搭載されていることが多い．また，腕や頭部を持つため，それらの部位を動作させた場合に周囲に影響がないかどうかについても判断する必要がある．ここでは，以下の特徴を持つロボットを考える．

- 腕を持ち，二足歩行が可能なロボットである
- 頭部にカメラが，胴体に加速度センサー，足の裏と両腕の先に感圧センサーを持つ
- スピーカーとマイクによって外部とのコミュニケーションが可能である
- 物を掴む，ボールを蹴るなどの運動能力がある

このようなロボットを対象として行動ポリシーをルール化した例を表 3 に示す．

行動ポリシーの基本事項である Physical Hazards に違反しないためには，障害物に対してロボットが接触することを防ぐことが重要である．しかし，ロボットの機能として物を拾う，運ぶといった動作を行う際には必ず対象と接触する必要がある．このような状況では，操作の対象以外に触れないよう行動するべきである．また，ロボットが落下や転倒した場合に自身や周囲を保護するための対策も必要となる．他にもスピーカーやマイクなどの音声デバイスを搭載しているロボットでは，有害な単語や重要な情報の出力を禁止する，もしくはロボットのオーナーが存在する場合にのみ音声操作を実行できるようにするなどの制限を課すべきである．これは Authority, Privacy, Faithfulness に該当するルールと言える．

ケース 2: 掃除ロボット

掃除ロボットは車輪により移動を行うことができる．姿勢制御の必要はほとんどなく，プライバシー情報を扱わないため，衝突や落下などの Physical Hazards に関するルー

表 3 ヒューマノイド型ロボットの行動ポリシーをルール化した例

文脈	条件	対応
移動中	人間や壁などの障害物が移動方向に存在	障害物のある方向への移動，及び腕の伸長を禁止
移動中	腕の感圧センサーが圧力を検知	停止して腕方向にカメラを向ける
移動中	急な加速度変化を検知	高低差最小方向に倒れつつ安全な姿勢をとる
移動中	進行方向に急な高低差が存在	停止
腕や足で物体を操作中	操作対象の物体以外が動作方向に存在	動作停止
任意の状態	カメラ映像が遮断される	動作を停止
任意の状態	閾値を超える速度でモーターを動作する命令を受信	閾値で動作を実行
音声認識中	許可されていない対象から命令を受信	命令を破棄
音声出力中	プライバシー情報の出力中に許可しない対象が存在	出力停止
音声出力中	有害な単語を検出	検出した単語を出力しない

ルが主となる．そのため，行動ポリシーを遵守するためのルールを簡潔にまとめることができる．ここでは，以下の特徴をもつロボットを考える．

- 車輪による移動が可能で，全方向への方向転換が可能
- 本体の周囲に感圧センサーとソナーセンサーを搭載
- ロボットの前方にある小さなものをゴミとして吸引する

掃除ロボットに関するルールをまとめたものを表 4 に示す．想定したロボットはプライバシー情報を持たず，出力はモーター部のみであるため， Privacy と Faithfulness を考慮する必要はない．Physical Hazards に関するルールとしては障害物をさけることに加え，ゴミ以外を吸い込んでしまうことによる被害を抑えるためのものが必要となる．また， Authority に対応するルールとして，ロボットが指定された領域内のみを移動するように制限する必要がある．この制限を課すことで，屋外に移動して車と衝突するなどの被害を防ぐことができる．

5. 議論

5.1 今後に残された研究課題

本論文ではロボットが備えるべきセキュリティポリシーについて論じた．これらのポリシーに基づいてロボット動作基盤の実装を行い，有用性を示すことは今後の課題である．本章では今後ポリシーを適用したシステムを実装するにあたり必要となる技術要素についてまとめる．

trust check の実装

trust check は通信相手が信頼できるオブジェクトかどうかを検証するプロセスである．実際の製品では平文で通信を行っているため，第三者が通信内容を解読できることや，なりすましが可能となってしまっているために信頼できないオブジェクトが情報を受け取ってしまう可能性がある． 4.1 章で述べた SROS に関する議論のように， PKI と SSL/TLS による暗号化通信の導入は trust check の実装方法として十分に信頼できるものであると考えられる．技術的にはこれらの既存の手法を利用することで実装可能であるが， TLS ハンドシェイクや暗号化処理のオーバーヘッドをできるだけ抑え，パフォーマンスに影響しないように注意する必要がある．こうした実装により，現存するコンシュマー向けロボットの脆弱性の多くは解決される．

permission check の実装

4.1 で紹介した入出力ポリシーの permission check に違反する例として，カメラに対する read permission がない外部オブジェクトに対し，アプリ内でカメラ映像を含むデータが送信される場合がある．これを検出するには，カメラの映像データがどのように扱われているかを把握する必要がある．これには，以下のような手法が考えられる．

- カメラ映像のデータに付加情報を付け，データの送信時に情報が外部オブジェクトに送信されるかを確認
- アプリを予め解析し，アプリごとに permission を設定

上記の手法によるオーバーヘッド等を考慮し，ユーザビリティとセキュリティのトレードオフを調整する必要がある．また，設定された permission をユーザーにわかりやすく提示したり， permission に違反する挙動を検知した場合はユーザーへ通知する仕組みの整備も必要である．

verification の実装

verification を行うには 4.2 章で示した行動ポリシーに基づくルールを適用するために，各種センサーを用いて正確な状況判断を行う必要がある，例として取り上げたヒューマノイド型ロボットのようにカメラやスピーカー，マイクといった重要な情報を取り扱うセンサーを利用できるロボットは考慮すべき点が多い．高度に状況を判断するためには， CV を利用したオドメトリや，物体認識技術，音声による個人識別など，様々な技術を複合的に組み合わせる必要がある．また，これらの状況分析を行うプロセスは，各センサーの値を利用できなければならないため，適切なパーミッションを設定する必要がある．

さらに，カメラを利用した位置解析は手法によってその処理量も様々であるが，一般にある程度の計算能力が必要となるため，高性能なプロセッサが搭載されないロボットではパフォーマンスに悪影響を及ぼす．これを緩和する手法として外部のマシンに解析処理を任せることが考えられ

表 4 掃除ロボットの行動ポリシーをルール化した例

文脈	条件	対応
移動中	人間や壁などの保護する対象や急な高低差が移動方向に存在する	その方向への移動を停止する
移動中	予め指定された領域を外れる	領域内へ戻る

るが，カメラ映像のような大きいデータを暗号化しつつを外部へ送信し続けなくてはならなくなるため，ネットワークの帯域が消費されてしまうことに加えて判定内容の送信に遅延が発生するという問題が想定される．そのため，常に画像解析による状況判断を行うタイミングをロボットが verification を行う際に限定したり，感圧センサーや赤外線センサーなどの情報を併用して計算量を削減する手法を構築するといった工夫が必要である．

5.2 研究倫理

2 章では現在市販されているロボット製品が持つ脆弱性を示した．これらの脆弱性はいずれも公知の情報である．我々は独自に脆弱性を調査した結果に基づいて PoC 攻撃コードを作成し，実際のロボット製品の遠隔操作が可能となることを検証している．現在は JPCERT/CC による協力の下，該当するロボット製品開発企業の CSIRT チームへの情報開示と調整を進めている段階である．このため，具体的な製品名と攻撃の手順は本稿から除外した．

6. 関連研究

ロボットのセキュリティに関する研究はいくつかの先行例がある．Denning ら [13] はいくつかの家庭用ロボットに対してセキュリティ調査を行い，情報漏えいや遠隔操作が可能などの多くの問題点を発見した．さらに，その調査を元に家庭用ロボットにおけるセキュリティを考える上での教訓をまとめている．また， Dieber ら [14] は ROS 上で動作するアプリ内に不正なノードが含まれないように監視を行い，加えてデータの暗号化を行うことによってアプリの安全を確保する手法を提案している．他にも，ロボットではないがセンサーを搭載する機械のセキュリティに関する研究の一例として， Rouf ら [15] の自動車の無線タイヤ圧力管理システムのセキュリティ調査を行い，情報の盗聴や車の追跡が可能であることを指摘している．彼らは調査結果から車に搭載される車のセンサーネットワークに必要なセキュリティ対策や教訓について述べている．

7. まとめ

本研究はコンシュマー向けロボット製品が安全に開発・運用されることを狙いとしてセキュリティポリシーを作成した．我々はロボットのセキュリティポリシーは広範な議論，実機を用いた実験と運用，そしてロボット製品のさらなる普及を通し，徐々に洗練されていく性質のものであり，現時点の検討結果はそのファーストステップであると考えている．本研究で示したコンセプト・研究の方向性が，ロボットのセキュリティポリシーに関わる議論を活性化するきっかけになることを期待したい．

参考文献

[1] IDC: Worldwide Semiannual Commercial Robotics Spending Guide, `http://www.idc.com/getdoc.jsp?containerId=IDC_P33201` (2017).

[2] : Pepper, `https://www.softbank.jp/robot/special/pepper/?cid=brsy_150727_robot/_045_b2cmv` (2017).

[3] Kahn Jr, P. H., Kanda, T., Ishiguro, H., Gill, B. T., Shen, S., Gary, H. E. and Ruckert, J. H.: Will people keep the secret of a humanoid robot?: Psychological intimacy in hri, *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction*, ACM, pp. 173–180 (2015).

[4] : Aldebaran Store, `https://store.aldebaran.com/` (2017).

[5] : ROS.org, `http://www.ros.org/` (2017).

[6] : Nao, `https://www.ald.softbankrobotics.com/en/robots/nao` (2017).

[7] Cerrudo, C. and Apa, L.: Hacking Robots Before Skynet, Technical report, IOActive, Inc (2017).

[8] Watanabe, T., Akiyama, M. and Mori, T.: RouteDetector: Sensor-based Positioning System That Exploits Spatio-Temporal Regularity of Human Mobility, *9th USENIX Workshop on Offensive Technologies, WOOT '15* (2015).

[9] アイザック・アシモフ：われはロボット (小尾芙佐訳)，早川書房 (1983).

[10] EPSRC: Principles for designers, builders and users of robots, `https://www.epsrc.ac.uk/research/ourportfolio/themes/engineering/activities/principlesofrobotics/` (2010).

[11] Breiling, B., Dieber, B. and Schartner, P.: Secure communication for the robot operating system (2017).

[12] : AppArmor, `http://wiki.apparmor.net/index.php/Main_Page` (20006).

[13] Denning, T., Matuszek, C., Koscher, K., Smith, J. R. and Kohno, T.: A spotlight on security and privacy risks with future household robots: attacks and lessons, *Proceedings of the 11th international conference on Ubiquitous computing*, ACM, pp. 105–114 (2009).

[14] Dieber, B., Kacianka, S., Rass, S. and Schartner, P.: Application-level security for ROS-based applications, *Intelligent Robots and Systems (IROS), 2016 IEEE/RSJ International Conference on*, IEEE, pp. 4477–4482 (2016).

[15] Ishtiaq Roufa, R. M., Mustafaa, H., Travis Taylora, S. O., Xua, W., Gruteserb, M., Trappeb, W. and Seskarb, I.: Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study, *19th USENIX Security Symposium*, pp. 11–13 (2010).