令和2年度ロボット関連産業基盤強化事業
セキュアなロボットシステムの技術開発

実証レポート

2021.03.31

TIS株式会社
サービス事業統括本部
デジタル社会サービス企画部

各組織役割

	役割
TIS株式会社	・プロジェクトの推進 ・情報資産の特定、脅威の洗い出し、リスク評価 ・リスク対策の設計と実装 　・ロボット管理プラットフォーム 　・自律移動ロボットのプログラム（一部） 　・改竄検知・復旧ソリューション ・実証実験の計画と推進 ・実証実験の実施 ・プロジェクト完了報告の取りまとめ
ネットワンシステムズ	・リスク評価の支援 ・実証実験の計画・実施の支援
会津大学	・自律移動ロボットとその周辺技術に関する技術的アドバイス ・サービスロボットとセキュリティに関する技術的アドバイス
イームズロボティクス	・自律移動ロボット（一号機）のハードウェア調整の支援
デジタル・インフォメーション・テクノロジー	・改竄検知・復旧ソリューション（WebARGUS for IoT）の試用 ・改竄検知・復旧に関する技術的支援 ・画像・映像の真正性担保に関する技術的アドバイス

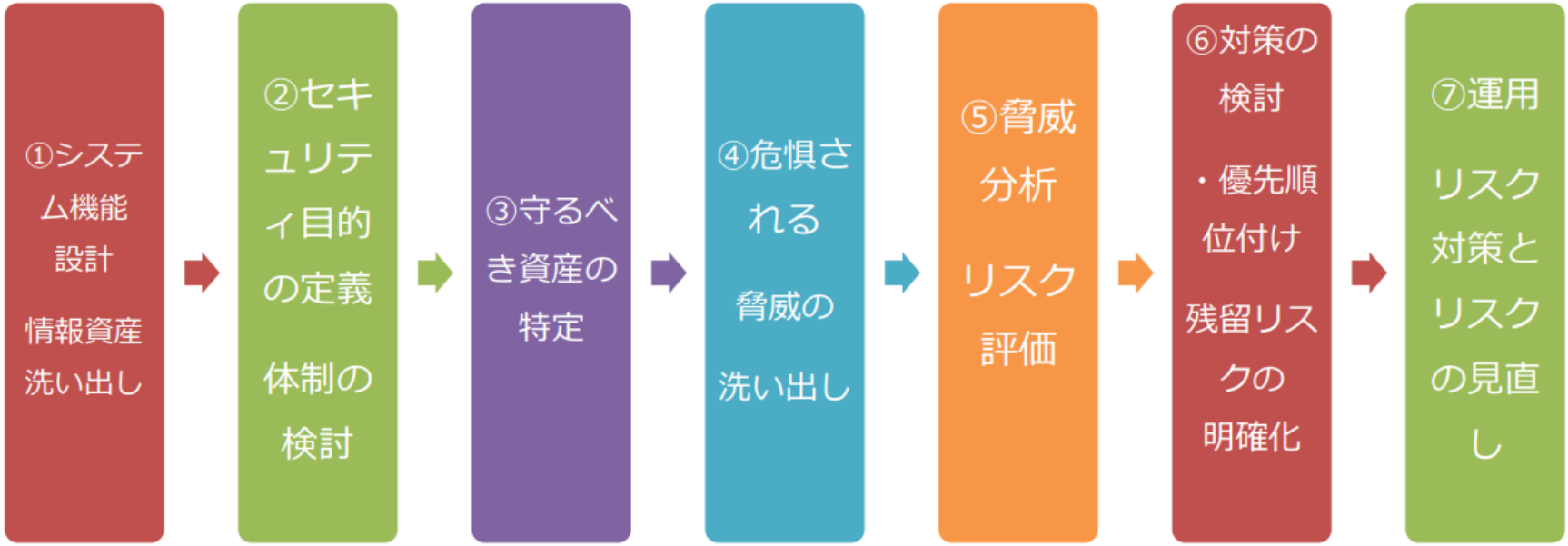
背景

- 自動走行ロボットを用いたラストワンマイル配送の無人化など、ロボティクス技術を物流事業に応用する試みが近年着目されている
- 日常空間で動き回る**サービスロボット**とその**管理プラットフォーム**の**セキュリティ**に着目した**ガイドライン**は**無い**

目的

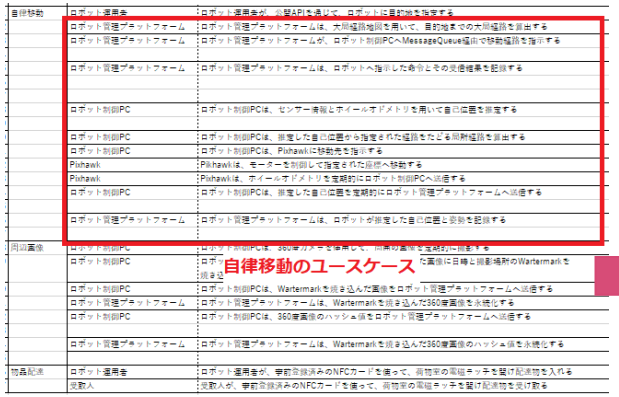
- 自律移動ロボットをクラウド上の管理プラットフォームに接続し、システム全体としてセキュアに保つ手法を研究する
- 研究成果を動作する**サンプルソフトウェア**及び**ガイドライン**として**公開**する

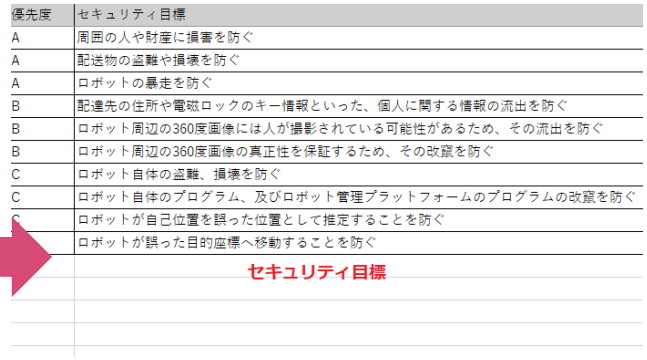
実施の流れ

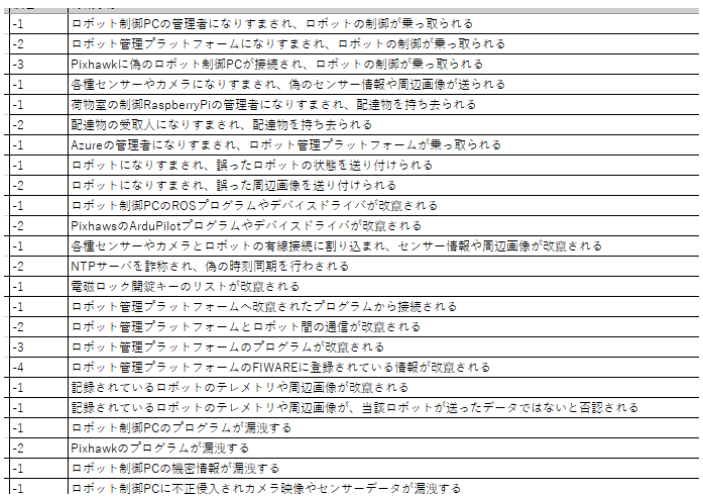


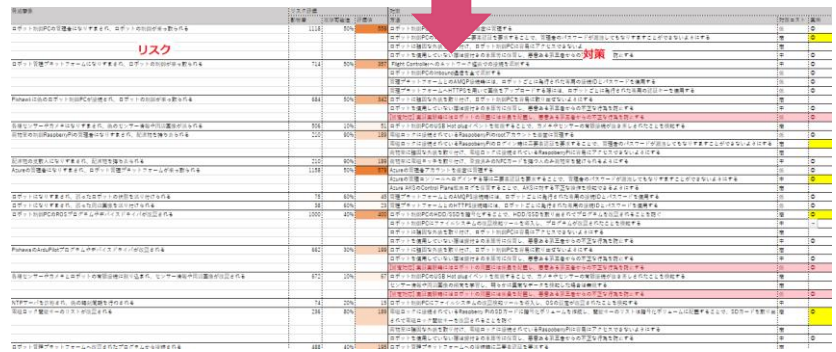
出典：サービスロボット・セキュリティガイドライン　第１版
（https://rtc-fukushima.jp/wp/wp-content/uploads/2019/05/e8d215d9e3f39a8c5e09f6a126b5f34f.pdf）

検討内容



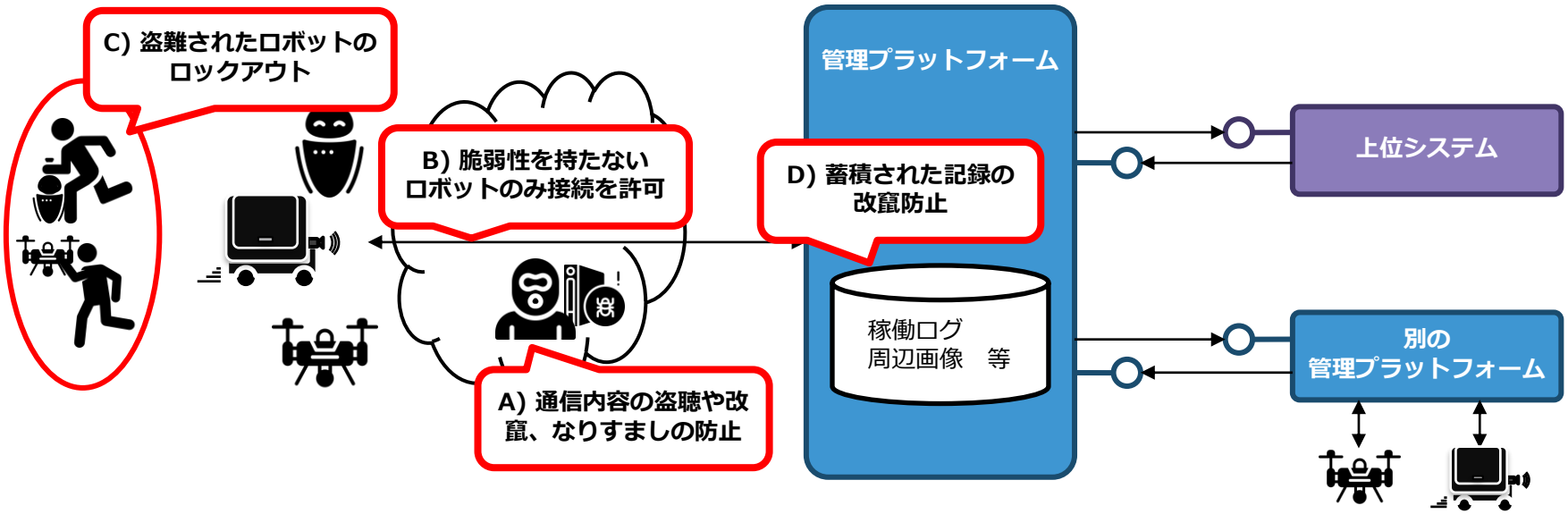






詳細は「リスク分析と評価シート」として公開

実施内容



A) ロボット管理プラットフォームのセキュア化の検証
- TLS対応で通信経路を暗号化、ポートやログイン制御など

B) 脆弱性を持つロボットの接続拒絶手段の検証
- 通信プログラムの真正性を担保、脆弱性のスキャンなど

C) 不正に持ち去られたロボットをロックアウトする手段の検証
- 盗難や走行妨害、荷物室の認証認可、ファイル改ざんの通知など

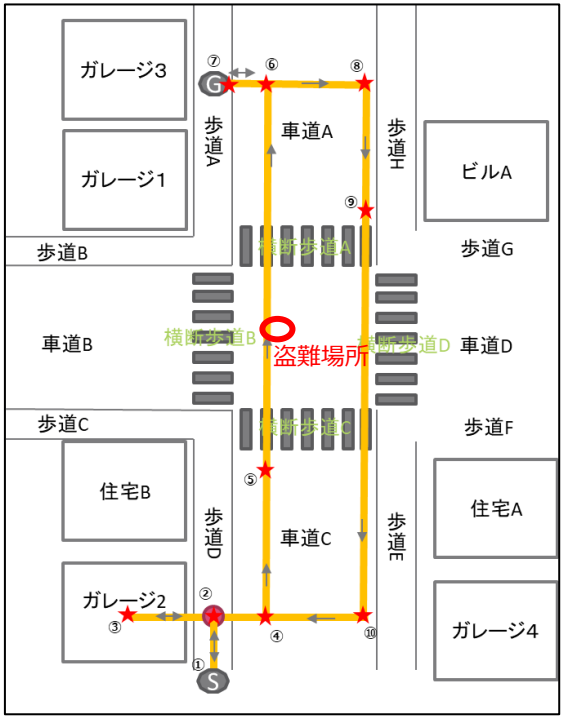
D) ロボットの稼働記録の保全手段の検証
- 360度カメラによる耐改ざん性のある周辺画像の撮影など

実証実験概要

- 実施予定日
  - 2021/01/12（火）準備日
  - 2021/01/13（水）実施日
- 実施場所
  - 福島県南相馬市　福島ロボットテストフィールド（RTF）市街地フィールド

- 実証実験　実施内容
  - 実施内容の(A)~(D)

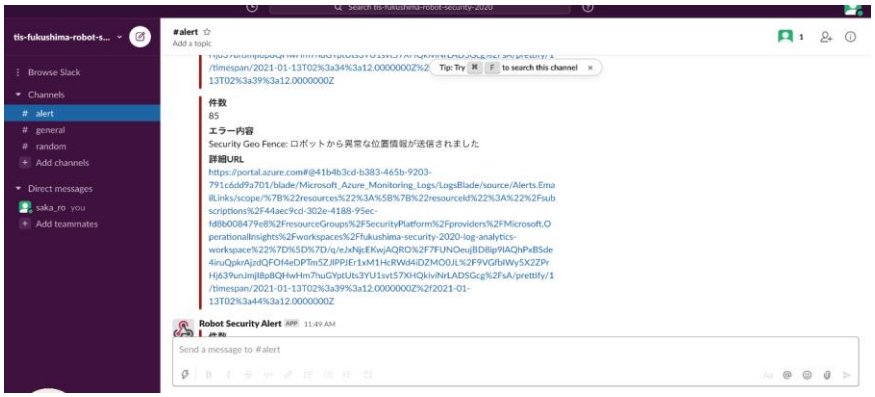
福島ロボットテストフィールド 市街地フィールド写真



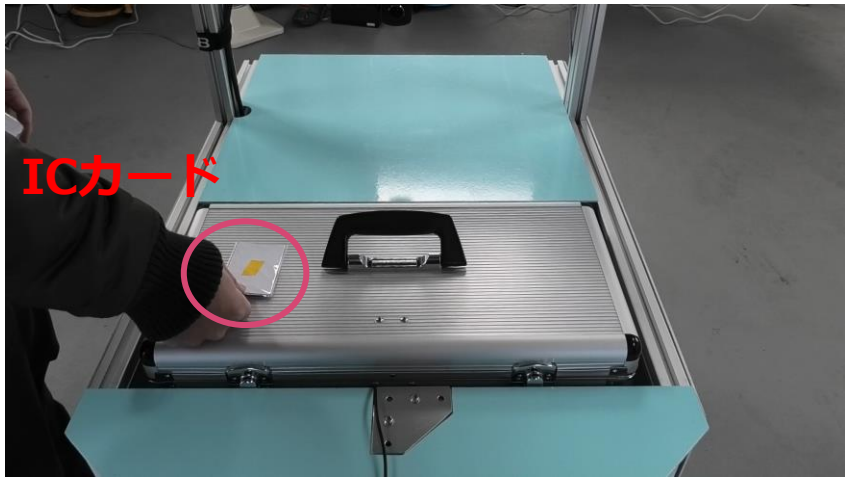
市街地フィールドでの走行ルート

実証実験 主な実施内容

(C)ファイル改ざんツールの管理画面
デジタル・インフォメーション・テクノロジー(株)製品
WebARGUS



(C)ロボットに異常が発生した際に
管理用Slackへ通知



(C)セキュリティボックスの外観
ICカードによる認証認可

(D)自律移動ロボットが盗難された際の
360度カメラの映像
画像下部に改ざん対策のハッシュ値が埋め込まれている

考察 今回実施しなかった内容

① ロボットPCにおけるOSレベルの暗号化について

OSレベルの暗号化はロボットの動作に遅延が発生し断念

⇒ 今後はロボットPCとハードウェア制御用オンボードの通信速度の向上により、OSレベルの暗号化に対応

② セキュリティボックスの実装方法について

荷物室はクラウドと接続せずにスタンドアローンで動作

⇒ 今後はクラウドと荷物室が繋がっている状態でのセキュリティリスを検討

③ ロボットの外装について

デバッグやメンテナンスを重視したため、容易に取り外し可能

⇒ 今後は内部のハードウェアへ容易にアクセスできないような外装を検討

④ ロボット制御PCと接続されたデバイスの抜き差し検知について

優先順位の観点からデバイスの抜き差し検知については実施せず

⇒ 今後はデバイスの抜き差しを検知して対応

⑤ ロボットのローカルでのログ保存について

優先順位の観点からロボットローカルでのログ保存は実施せず

⇒ 今後はインターネット接続が遮断された際にもログを終えるように対応

考察
実証で行なった内容が他のケースで通用するか

対策	対策詳細	自律移動ロボット全般で通用	理由
(A)ロボット管理プラットフォームのセキュア化	通信経路を暗号化	○ 通用	クラウドと接続する場合、何らかの方法で通信を行うので、改ざん、通信の傍受を防ぐ
	ロボットの制御PCや管理プラットフォームを要塞化	○ 通用	各種、情報漏洩や改竄、サービス拒否攻撃に対応する
	ロボットと管理プラットフォーム接続における認証認可	○ 通用	クラウドと接続する場合、不正アクセスを防ぐ
(B)脆弱性を持つロボットの接続拒絶手段	ロボットの通信プログラムの真正性を担保	○ 通用	不正なクライアントからデータを送信される可能性がある
	ロボットのOSやプログラムに対する脆弱性スキャン	△ 場合による	ロボットのOSが一般的でない場合、脆弱性スキャンが通用しない
(C)不正に持ち去られたロボットをロックアウトする手段	ロボット制御PCのログインにおける運用担当者のみの認可	○ 通用	漏洩などのリスクを抑えるため、担当者を限定する必要がある
	ロボットの盗難や走行妨害における検知および通知	○ 通用	自律移動ロボットである場合、物理的な攻撃がありえる
	ロボット制御PCにおけるファイル改ざん検知	○ 通用	何らかの方法でPCにアクセスされファイル改ざんの可能性がある
	荷物室の認証認可	△ 場合による	ユースケース次第で荷物室の搭載が異なる
(D)ロボットの稼働記録の保全手段	360度カメラによるセキュアな周辺画像の撮影	○ 通用	自律移動ロボットである場合、物理的な攻撃時に状況確認がある

考察
実証で行なった内容が他のケースで通用するか

対策	対策詳細	自律移動ロボット全般で通用	理由
(A)ロボット管理プラットフォームのセキュア化	通信経路を暗号化	○ 通用	クラウドと接続する場合、何らかの方法で通信を行うので、改ざん、通信の傍受を防ぐ
	ロボットの制御PCや管理プラットフォームを要塞化	○ 通用	各種、情報漏洩や改竄、サービス拒否攻撃に対応する
	ロボットと管理プラットフォーム接続における認証認可	○ 通用	クラウドと接続する場合、不正アクセスを防ぐ
(B)脆弱性スキャンによるロボットの接続拒絶手段	ロボットの通信プログラムの真正性を担保	○ 通用	不正なクライアントからデータを送信される可能性がある
	ロボットのOSやプログラムに対する脆弱性スキャン	△ 場合による	ロボットのOSが一般的でない場合、脆弱性スキャンが通用しない
(C)不正に持ち去られたロボットをロックアウトする手段	ロボット制御PCのログインにおける運用担当者のみの認可	○ 通用	漏洩などのリスクを抑えるため、担当者を限定する必要がある
	ロボットの盗難や走行妨害における検知および通知	○ 通用	自律移動ロボットである場合、物理的な攻撃がありえる
	ロボット制御PCにおけるファイル改ざん検知	○ 通用	何らかの方法でPCにアクセスされファイル改ざんの可能性がある
	荷物室の認証認可	△ 場合による	ユースケース次第で荷物室の搭載が異なる
(D)ロボットの稼働記録の保全手段	360度カメラによるセキュアな周辺画像の撮影	○ 通用	自律移動ロボットである場合、物理的な攻撃時に状況確認がある

本研究では研究用ロボットで柔軟に対策を行なった

既製品のロボットだと柔軟な対策が難しい可能性がある

- **運用の容易さ**・・・ロボットのメンテナンスのしやすさ
  - 実証実験でも対策によりメンテナンス性が下がった

    ⇒**ロボットインテグレータ**
    (IT技術などを統合しロボットビジネスを提案する業者)
    が要件定義の段階でセキュリティとメンテナンスのバランスを検討

- **コスト**　　・・・対策やそれに伴うハード等のコスト
  - 実証で行なった対策を既製品のロボットに施そうとすると、ハードウェアやOSの対応を確認する必要があり、特別に対応する場合はコストが上昇する可能性がある

    ⇒**共通して必要となるセキュリティ対策を既製品ロボットに実装**

運用が容易でコストが低く、ベースとなるセキュリティ実装が
施されているようなロボットの検討が必要

補助事業の効果

■　福島県内のロボットメーカーへの教育効果

今回の補助事業で用いた自律移動ロボットは、福島県内のドローン・ロボットメーカーであるイームズロボティクスが開発し、実証実験も共に実施した。

⇒セキュアな自律移動ロボットを開発するための実践的なノウハウを伝達

■　福島県内のロボット研究開発と産学連携への波及効果

今回の補助事業は会津大学に協力いただいており、ARDuC(会津大学デュアルウェア研究会)での共有や「福島県 令和２年度ロボット・ソフトウェア検討会」でのオンライン発表（2月26日実施）、報告書等を通じて、県内外の企業に成果を共有する予定。

⇒福島県のロボット産業に対してセキュアな自律移動ロボットを開発するための考え方やノウハウを伝達

■　ロボット関連業界への波及効果

今回の補助事業の成果をロボット関連の業界団体（ロボット革命・産業IoTイニシアティブ協議会 ロボットイノベーションWG ロボットセキュリティ調査検討委員会）にて発表し、考え方や実際に作成した成果物を共有した（2020/12/15）。

⇒セキュアな自律移動ロボットを開発するための考え方やノウハウを伝達

今後について

ロボット導入コンサルティングサービスへの組み込み検討

- 弊社のロボット導入コンサルティングサービスのメニューに組み込むことや、自社開発しているロボット管理プラットフォーム（RoboticBase）へセキュリティに関する要件を取り込むことができるか検討し、サービスの競争力強化へつなげていきたい。

https://www.tis.jp/service_solution/robotics-consulting/

THANK YOU

ITで、社会の願い叶えよう。

TIS INTEC
Group