



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

役割	
TIS株式会社	<ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・リスク評価の支援 ・実証実験の計画・実施の支援
会津大学	<ul style="list-style-type: none"> ・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

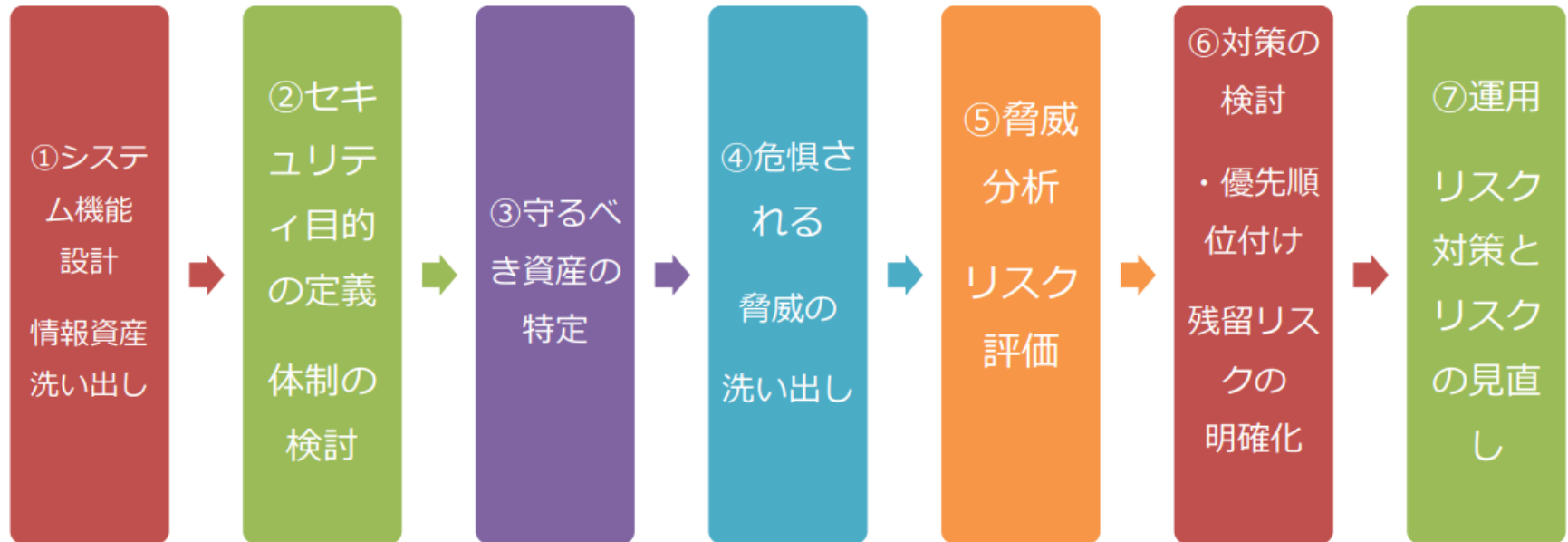
イームズロボティクス	<ul style="list-style-type: none"> ・自律移動ロボット（一号機）のハードウェア調整の支援
デジタル・インフォメーション・テクノロジー	<ul style="list-style-type: none"> ・改竄検知・復旧ソリューション（WebARGUS for IoT）の試用 ・改竄検知・復旧に関する技術的支援 ・画像・映像の真正性担保に関する技術的アドバイス

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



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>)

自律移動	ロボット運用者	ロボット運用者が、必要APIを呼び、ロボットは目的地へ移動する
ロボット管理プラットフォーム	ロボット管理プラットフォームは、大規模地図を用いて、目的地までの大規模経路を算出する	
ロボット管理プラットフォーム	ロボット管理プラットフォームは、ロボット制御PCにMessageQueue経由で移動経路を指示する	
ロボット管理プラットフォーム	ロボット管理プラットフォームは、ロボットへ指示した動作とその実施結果を記録する	
ロボット制御PC	ロボット制御PCは、センサー情報とAPIを呼び出して目的地へ移動する	
ロボット制御PC	ロボット制御PCは、指定した自己位置から指定された経路をたどる制御プログラムを算出する	
ロボット制御PC	ロボット制御PCは、Pixhawkに移動命令を送信する	
Pixhawk	Pixhawkは、モーターを制御して指定された目的地へ移動する	
Pixhawk	Pixhawkは、テレメトリデータを定期的にロボット制御PCへ送信する	
ロボット制御PC	ロボット制御PCは、指定した自己位置を定期的にロボット管理プラットフォームへ送信する	
ロボット管理プラットフォーム	ロボット管理プラットフォームは、ロボットが指定した自己位置を記録する	

対象	装置	資産
ロボット	ロボット制御PC	rootアカウント 実行アカウント NTP等の認証デーモン WiFiのアクセスポイントの接続IDとパスワード 改変ツール OS設定 OSログ ROSタイプリ 自律移動ROSプログラム (cartographer) 自ROSプログラム Azure ServiceBus 接続IDとパスワード 自律移動する目的地と経路 センサーから得た生データ 指定した自己位置と姿勢 ロボット周辺の360度画像 Wartemarkを結合込んだ360度画像 Wartemarkを結合込んだ360度画像のハッシュ値 360度画像のハッシュ値を計算するSalt Azure Blob Storageのキー
	Pixhawk	ArduPilot ArduPilot ArduPilot ArduPilot ArduPilot 移動先座標
		ロボット制御PCの情報資産

優先度	セキュリティ目標
A	周囲の人や財産に損害を防ぐ
A	配達物の盗難や損壊を防ぐ
A	ロボットの暴走を防ぐ
B	配達先の住所や電磁ロックのキー情報といった、個人に関する情報の流出を防ぐ
B	ロボット周辺の360度画像には人が撮影されている可能性があるため、その流出を防ぐ
B	ロボット周辺の360度画像の真正性を保証するため、その改変を防ぐ
C	ロボット自体の盗難、損壊を防ぐ
C	ロボット自体のプログラム、及びロボット管理プラットフォームのプログラムの改変を防ぐ
C	ロボットが自己位置を誤った位置として推定することを防ぐ
C	ロボットが誤った目的地座標へ移動することを防ぐ

セキュリティ目標



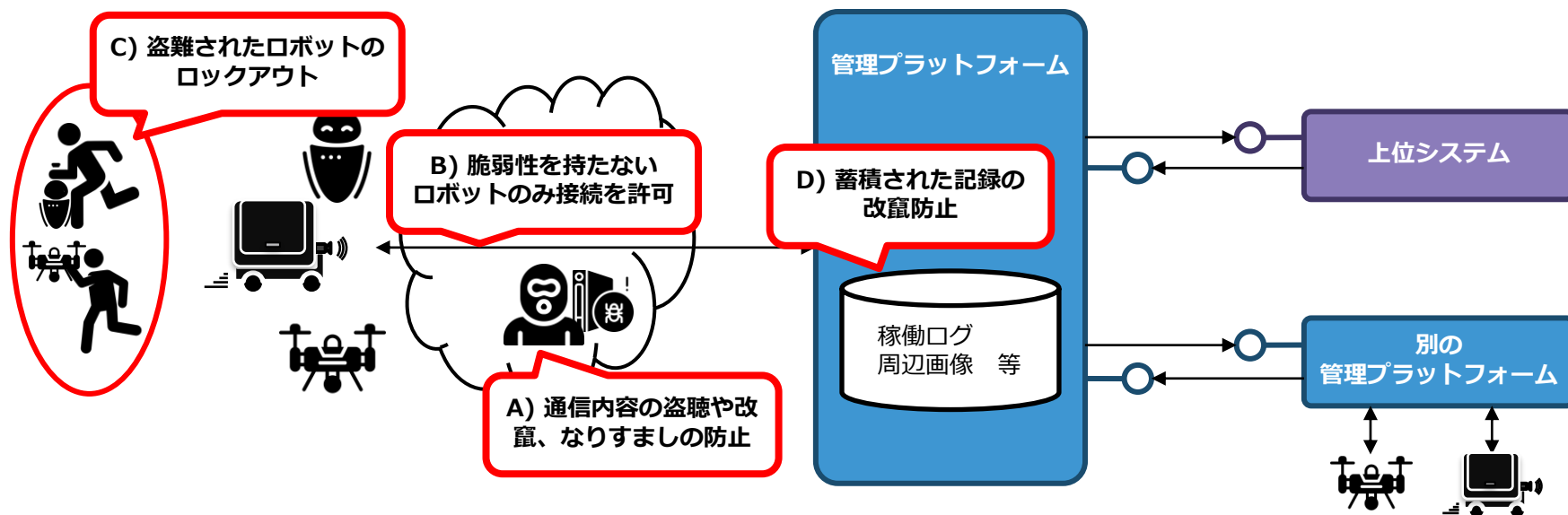
資産	脅威に曝される物理資産	脆弱性	侵害に曝される物理資産	侵害	侵害	侵害
ロボット制御PCの管理権になりすまされ、ロボットの制御が奪取される	rootアカウント	10	rootアカウント	10	4	1114
	実行アカウント	10	実行アカウント	10		
	NTP等の認証デーモン	9	Pixhawk	10		
	WiFiのアクセスポイントの接続IDとパスワード	10	通信OSIM	10		
	OS設定	10	360度画像	10		
	OSログ	10	OSログ	10		
	ROSタイプリ	10	自律移動ROSプログラム (cartographer)	10		
	自律移動ROSプログラム	10	自ROSプログラム	10		
	Azure ServiceBus 接続IDとパスワード	10	ロボットから得た生データ	80		
	自律移動する目的地と経路	10	センサーから得た生データ	80		
	センサーから得た生データ	10	指定した自己位置と姿勢	30		
	指定した自己位置と姿勢	10	ロボット周辺の360度画像	30		
	ロボット周辺の360度画像	10	Wartemarkを結合込んだ360度画像	30		
	Wartemarkを結合込んだ360度画像	10	Wartemarkを結合込んだ360度画像のハッシュ値	30		
	360度画像のハッシュ値を計算するSalt	10	360度画像のハッシュ値を計算するSalt	30		
	Azure Blob Storageのキー	10	Azure Blob Storageのキー	30		

脅威の優先度・影響度を評価

- 1 ロボット制御PCの管理者になりすまされ、ロボットの制御が奪取される
- 2 ロボット管理プラットフォームになりすまされ、ロボットの制御が奪取される
- 3 Pixhawkに偽のロボット制御PCが接続され、ロボットの制御が奪取される
- 1 各種センサーやカメラになりすまされ、偽のセンサー情報や周辺画像が送られる
- 1 荷物室の制御RaspberryPiの管理者になりすまされ、配達物を持ち去られる
- 2 配達物の受取人になりすまされ、配達物を持ち去られる
- 1 Azureの管理者になりすまされ、ロボット管理プラットフォームが奪取される
- 1 ロボットになりすまされ、誤ったロボットの状態を送り付けられる
- 2 ロボットになりすまされ、誤った周辺画像を送り付けられる
- 1 ロボット制御PCのROSプログラムやデバイスドライバが改変される
- 2 PixhawkのArduPilotプログラムやデバイスドライバが改変される
- 1 各種センサーやカメラとロボットの有線接続に割り込まれ、センサー情報や周辺画像が改変される
- 2 NTPサーバを詐称され、偽の時刻同期が行われる
- 1 電磁ロック関連キーのリストが改変される
- 1 ロボット管理プラットフォームへ改変されたプログラムから接続される
- 2 ロボット管理プラットフォームとロボット間の通信が改変される
- 3 ロボット管理プラットフォームのプログラムが改変される
- 4 ロボット管理プラットフォームのFIWAREに登録されている情報が改変される
- 1 記録されているロボットのテレメトリや周辺画像が改変される
- 1 記録されているロボットのテレメトリや周辺画像が、当該ロボットが送ったデータではないと否認される
- 1 ロボット制御PCのプログラムが漏洩する
- 2 Pixhawkのプログラムが漏洩する
- 1 ロボット制御PCの機密情報が漏洩する
- 1 ロボット制御PCに不正侵入されカメラ映像やセンサーデータが漏洩する

リスク	発生頻度	影響度	リスク	発生頻度	影響度
ロボット制御PCの管理権になりすまされ、ロボットの制御が奪取される	1114	800	rootアカウント	10	4
ロボット管理プラットフォームになりすまされ、ロボットの制御が奪取される	714	800	実行アカウント	10	80
Pixhawkに偽のロボット制御PCが接続され、ロボットの制御が奪取される	644	800	NTP等の認証デーモン	9	30
各種センサーやカメラになりすまされ、偽のセンサー情報や周辺画像が送られる	800	1000	WiFiのアクセスポイントの接続IDとパスワード	10	80
荷物室の制御RaspberryPiの管理者になりすまされ、配達物を持ち去られる	210	800	OS設定	10	30
Azureの管理者になりすまされ、ロボット管理プラットフォームが奪取される	1114	800	OSログ	10	30
ロボットになりすまされ、誤ったロボットの状態を送り付けられる	714	800	ROSタイプリ	10	30
ロボットになりすまされ、誤った周辺画像を送り付けられる	714	800	自律移動ROSプログラム	10	30
ロボット制御PCのROSプログラムやデバイスドライバが改変される	1114	800	自ROSプログラム	10	30
PixhawkのArduPilotプログラムやデバイスドライバが改変される	1114	800	Azure ServiceBus 接続IDとパスワード	10	30
各種センサーやカメラとロボットの有線接続に割り込まれ、センサー情報や周辺画像が改変される	800	1000	自律移動する目的地と経路	10	30
NTPサーバを詐称され、偽の時刻同期が行われる	644	800	センサーから得た生データ	10	30
電磁ロック関連キーのリストが改変される	644	800	指定した自己位置と姿勢	10	30
ロボット管理プラットフォームへ改変されたプログラムから接続される	1114	800	ロボット周辺の360度画像	10	30
ロボット管理プラットフォームとロボット間の通信が改変される	1114	800	Wartemarkを結合込んだ360度画像	10	30
ロボット管理プラットフォームのプログラムが改変される	1114	800	Wartemarkを結合込んだ360度画像のハッシュ値	10	30
ロボット管理プラットフォームのFIWAREに登録されている情報が改変される	1114	800	360度画像のハッシュ値を計算するSalt	10	30
記録されているロボットのテレメトリや周辺画像が改変される	1114	800	Azure Blob Storageのキー	10	30
記録されているロボットのテレメトリや周辺画像が、当該ロボットが送ったデータではないと否認される	1114	800			
ロボット制御PCのプログラムが漏洩する	1114	800			
Pixhawkのプログラムが漏洩する	1114	800			
ロボット制御PCの機密情報が漏洩する	1114	800			
ロボット制御PCに不正侵入されカメラ映像やセンサーデータが漏洩する	1114	800			

詳細は「リスク分析と評価シート」として公開



- 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

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

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からのみの認可	○ 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

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)脆弱な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
	ロボット制御PCのログインにおける運用担当者へのみの認可	○ 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
(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

ロボットビジネスをするうえで検討が必要なポイント

- **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

■ 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ます、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

■ 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。



The screenshot shows a web browser displaying the TIS website page for Robotics Consulting Services. The page title is "ロボット導入コンサルティングサービス" (Robotics Consulting Service). The main content area features a heading "ロボット導入コンサルティングサービス" and a sub-heading "運搬、清掃、案内、整備などの業務を担うロボット活用を目的としたサービスロボットの導入を支援" (Supporting the introduction of service robots for tasks such as transport, cleaning, guidance, and maintenance). Below this, there is a section titled "特長" (Features) with three bullet points:

- 特長 1：独立系システムインテグレータの知見を生かした中立的なコンサルティング**
TISインテックグループでは、元々独立系のシステムインテグレータとして、業界トップクラスの金融機関向けに業務・ITコンサルティングやクラウドサービス開発、そしてプロジェクトマネージメント等で実績を挙げてきました。TISの中立的なシステムインテグレータとしての実績・ノウハウによって、特定の製品やロボットを定型的に提案するのではなく、顧客ニーズに沿った製品、ロボットを組み合わせた最適なロボットシステムを提案することができます。
- 特長 2：CVCで増ったロボティクス・テクノロジーの深化と蓄積**
TISインテックグループでは、自社リソースに外部のロボット・AI技術やアイデア、サービスを柔軟に取り入れるオープンイノベーションによるコラボレーションビジネスを推進しています。自己資金によるプリンシパル投資を行い、ロボティクスのスタートアップ企業との協業により多くの先端技術のノウハウが蓄積されています。
- 特長 3：ロボットと企業システム、外部データを統合管理、稼働率や売上向上を支援**
権限施設にロボットやセンサ、カメラ、サイネージなどのIoTデバイスを設置し、収集したデータと既存の企業システム、外部データを統合する自社開発のソフトウェア「RoboticBase」、施設やロボット・人の稼働状況を分析し稼働率やナントの売上向上につながるよう支援します。ロボット群制御や人流最適化、そしてリスク管理、セキュリティ対策なども順次対応していく予定です。

THANK YOU

ITで、社会の願い叶えよう。



TIS INTEC
Group