「サービスロボットセキュリティガイドライン」に取り込むべく項目　- 案 -

2021 年 3 月 2 5日

TIS 株式会社

はじめに

会津大学様とネットワンシステムズ株式会社様が公開している、「サービスロボットセキュリティガイドライン」に、今回の事業結果を踏まえて TIS として取り込むべき内容として、設計フェーズを中心に案として整理しました。当内容をベースに、会津大学様およびネットワンシステムズ株式会社様と今後協議していく予定です。

1. 設計（コンセプト実証）フェーズ

4 章のコンセプトフェーズでの検討を受け、本章ではロボットシステム開発の設計フェーズにおけるセキュリティ検討項目について述べる。

設計フェーズのゴールは、コンセプトフェーズで検討した守るべきセキュリティゴールと攻撃を受けてしまった場合の想定される被害状況を踏まえ、ロボットシステム全体としてのセキュリティとセーフティを脅かす具体的な攻撃手段を可能な限り洗い出し、ロボットシステムに発生しうるリスクを定量的に評価して対策の優先順位を付けることで、ロボットシステム全体としての具体的なハードウェア・ソフトウェア及びネットワークアーキテクチャの設計にロボットシステムのあるべき姿を反映させることである。

1.1. 攻撃分析

設計フェーズのタスクは、ロボットシステム全体としてどのような攻撃に晒される可能性があるかを可能な限り洗い出すことから始まる。その際、ロボットシステムのハードウェア・ソフトウェアの特性やネットワーク構成など、具体的な設計仕様を念頭に置かねば、具体的な攻撃手段を見出すことができない。そのため自らのロボットシステムに採用する可能性のあるハードウェア・ソフトウェア・ネットワークアーキテクチャなどを列挙し、それぞれ CVE や CWE を参照に攻撃されうる脆弱性にはどのようなものがあるか、性能やコストのトレードオフを考えた場合に実施できるセキュリティ対策はどの程度のものかの概略を事前に把握しておくと進めやすい。

この攻撃手段を洗い出す上では、ロボットやその管理プラットフォーム等ロボットシステム全体の物理的な配置とデータの流れを図示化し、攻撃されやすそうな箇所にどのような脅威が潜んでいるかを一つ一つチェックしていく手法がわかりやすい。以下にその手法を例示する。

ただし新たな攻撃手段が日々発見され続けるセキュリティ界隈においては、この攻撃分析も一度実施すれば終わりというものではない。攻撃手段に関する情報を日々収集し、自らのロボットシステムに対して今まで想定していなかった攻撃が成立しないか、定期的に見直す必要があることを心に留めておくと良いだろう。

1.1.1. モデル化による脅威が潜むポイントの抽出

まずはロボットシステム全体をモデル化し、ロボットシステムを構成する物理的なコンポーネントの配置と、それらの間のデータの流れを図示化する。各コンポーネント間の物理的な境界面を通過するデータの流れがある場合、その境界面との交差地点が、脅威が潜むポイントになる。例えば管理プラットフォームと常時接続し、ロボットへの命令やロボットのテレメトリを送受信するロボットシステムの場合、その送受信するデータが攻撃対象になる。ロボットが受信したその命令は、本当に信頼できる管理プラットフォームから送られたものなのか？あるいは管理プラットフォームが受信したそのテレメトリは、本当にロボットの実際の状態を反映しているのか？が問われなければならない。

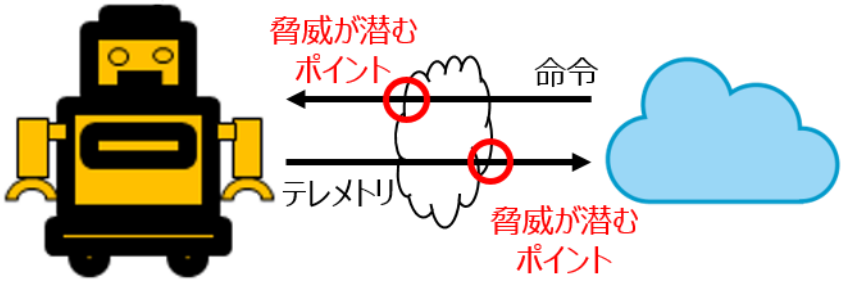

図 5.1 脅威が潜むポイントの例1

このモデル化は、多層的に検討しなければならない場合がある。例えば公道を走行する自律移動ロボットを想定した場合、悪意ある第三者が走行中のロボットを鹵獲し、ロボットに搭載されたセンサーと制御ユニットの間にデバイスを割り込ませて信号を改竄することも不可能ではない。あるいは制御ユニット自体をロボットから取り外し、ストレージを取り出して機密情報を盗難することも不可能ではない。このような攻撃手法も想定する場合、センサーと制御ユニット間の物理的な境界面、あるいは制御ユニット内部の境界面も脅威が潜むポイントになり得ることに注意が必要である。

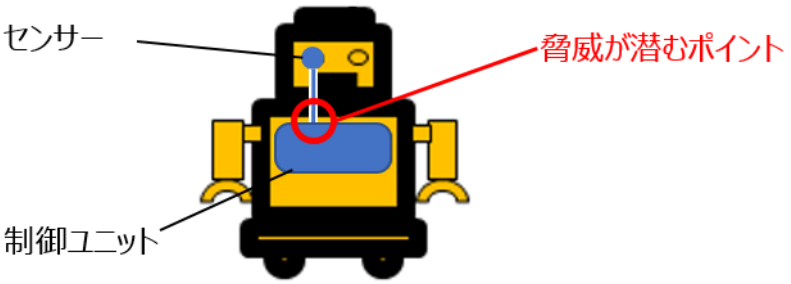

図 5.2 脅威が潜むポイントの例2

なお図 5.1 や図 5.2 のようなポンチ絵で脅威が潜むポイントを図示化しても良いが、DFD（Data Flow Diagram）を用いて脅威を洗い出す手法も Microsoft から提案されている（図 5.3）。詳細は参考文献を参照のこと。

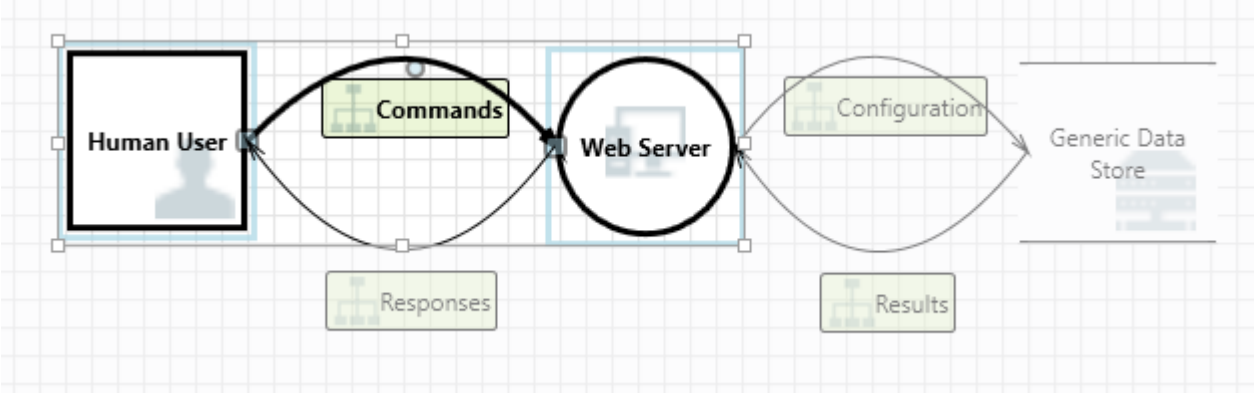

図 5.3 DFD を用いた脅威の洗い出し

出典：Microsoft Docs：Threat Modeling Tool の概要 [1]

1.1.2. キーワードを用いた脅威の発見

脅威が潜むポイントを抽出したら、次にそのポイントでどのような攻撃が成立しそうかを検討する。この際、闇雲に攻撃手段を考えるのではなく、表 5.1 にある 6 つのキーワードをヒントとして攻撃の可能性を検討すると整理が付けやすい。

ただしこの 6 つのキーワードによって全ての脅威が網羅されるわけではなく、あくまでも攻撃可能性を検討する際のきっかけ・ヒントであると捉えるべきである。そのためこれらのキーワードを用いて検討した後に、それ以外の視点からも脅威が発見されないか、続けて検討した方が良い。

表 5.1 脅威の発見に役立つキーワード（STRIDE）

出典：Microsoft Docs：Threat Modeling Tool の概要 [1]

S	Spoofing	なりすまし
	正規の人（やデバイス）を偽装する	
T	Tampering	改竄
	ファイルや通信パケット等のデータを書き換える	

R	Repudiation	否認
	不正な行為を実行した者は自分ではないと否定する	
I	Information Disclosure	情報漏洩
	正規の権限がない人へ情報が暴露される	
D	Denial of Service	サービス拒否
	システムが提供するサービスを停止させる	
E	Elevation of Privilege	権限の昇格
	正規の権限がない人がシステムの特権を得る	

例えばクラウド上に管理プラットフォームを持つ自律移動ロボットの脅威を STRIDE で検討した場合、表 5.2 のような攻撃可能性が見いだされるだろう。

表 5.2 STRIDE で検討した脅威の例

S	**なりすまし**	管理プラットフォームになりすまされ、ロボットに不正な命令が送信される
		各種センサーになりすまされ、偽のセンサー情報が送りこまれる
T	**改竄**	ロボットの制御プログラムが書き換えられ、ロボットが暴走させられる
		記録されているロボットのテレメトリや周辺画像が書き換えられ、事故発生時の証拠が消される
R	**否認**	ロボットに送信された命令を送ったのは自分ではないと否定され、ロボットが暴走した責任者がわからなくなる
		ロボットに記録された事故映像に対し、事後に書き換えられていると否定する
I	**情報漏洩**	ロボットの制御ユニットへログインできるアカウント情報が漏洩し、制御ユニットに不正アクセスされる
		管理プラットフォームを操作できるアカウント情報が漏洩し、ロボットに不正な命令が送信される
D	**サービス拒否**	管理プラットフォームがパケット過多でハングアップし、ロボットからのテレメトリが喪失する

		ロボットの制御ユニットがパケット過多でハングアップし、ロボットが暴走する
E	**権限の昇格**	ロボットの制御ユニットの特権が奪取され、制御ユニットに不正なプログラムが混入される
		管理プラットフォームの特権が奪取され、ロボットに不正な命令が送信される

1.2. 安全性リスクアセスメント

1.3. 対策要件定義

最後に、見いだされた脅威がロボットシステムに及ぼすリスクを定量的に評価し、ロボットシステムとして何から対策すべきか、優先順位を決めなければならない。ここで言うリスクは、「**ロボットシステムへ及ぼされる被害×その脅威が発生する可能性**」で見積もられる。この値を一定の評価軸で換算できるならばリスクを定量評価する手法は問わないが、アタックツリーを用いた手法が良く用いられる。

1.3.1. アタックツリーを用いたリスクの評価

アタックツリーは安全分析における分析手法（Fault Tree Analysis）をセキュリティの分野に応用したものである。ロボットシステムへの攻撃やその発生条件を、より抽象度の高い手段からより詳細で具体的な手段に木構造で分解する（図 5.4）。そして具体的で実行可能な末端ノード（葉）の攻撃手段に対して、攻撃はどの程度実行しやすいか（金銭・時間・専門知識・専用ツールの必要性等の総合的なコスト）を見積もる。アタックツリーを利用することで攻撃が実現する条件や攻撃される経路を可視化することができ、攻撃の可能性の検討を見通し良く実施することができる。

攻撃可能性の定量化には定まった方式は無いが、例えば攻撃可能性の多寡を相対的に見積もり、ロボットシステム内で一意な値を割り当てる方法や、攻撃を実行するために必要なコストを金額換算して定量化する方法などが用いられる。

攻撃可能性の定量化と共に、攻撃によって被る被害の定量化も実施する。攻撃が成立した場合に被る被害を金額換算して定量化することが多いが、被害の多寡を相対化しロボットシステム内で一意な値を割り当てる方法でもかまわない。

このようにして見積もった攻撃によって被る被害とその攻撃が成立する可能性を乗ずることで、ロボットシステムに内在するセキュリティリスクを定量的に評価することができる。この定量化したリスクと、そのリスクへの対策に要するコストを勘案し、対策の優先順位を付けてロボットシステムに実装することになる。