脅威分析ツールによる産業用制御機器に対する脅威分析の自動化

依田 安基

近年、工場のスマート化とオープン化に伴い、制御システムがサイバー攻撃を受けるリスクが高まり、各国・業界では法規制やガイドラインの整備が進んでいる。

製品セキュリティ対策を体系的に進めるために脅威分析が不可欠であるが、高度な専門知識と熟練を要する。世界的なセキュリティ専門人材の不足の中、製造業者が多数の製品に対して期限内に対応を進めることは困難となっている。脅威分析ツールの活用が解決策として期待されるものの、既存ツールは主に IT 領域を対象としており、産業用制御機器への適用可能性は不明であった。

本研究では、この課題に対し、産業用制御機器のシステム特性を考慮した脅威分析テンプレートを設計し、その正確性と有効性を Microsoft Threat Modeling Tool を用いて概念実証した。組み込み機器が特定の用途に限定して設計されていることに着目し、産業用制御機器特有の情報資産に対する脅威の検出を可能とするとともに、信頼境界内で発生する脅威の検出を抑制することで、脅威の未検出と誤検出を低減した。その結果、脅威分析の品質の均一化と必要となる工数の削減を実現できる可能性を得た。

Automating Threat Analysis for Industrial Control Devices using Threat Modeling Tool

YODA Yasuki

In recent years, the risk of cyberattacks on industrial control systems has increased due to the growing smartification and openness of factories, and accordingly, regulations and guidelines have been established by governments and industry worldwide.

Threat modeling is essential for systematically implementing product security measures; however, it requires specialized knowledge and expertise. Amid the global shortage of cybersecurity professionals, it has become difficult for manufacturers to complete threat modeling and implementation of security measures for large numbers of products within limited timeframes. Although threat modeling tools are expected to address this challenge, existing tools primarily target IT systems, and their applicability to industrial control devices has not been well established.

To address this issue, this study designs threat modeling templates tailored to the system characteristics of industrial control devices and demonstrates their accuracy and effectiveness through a proof of concept using the Microsoft Threat Modeling Tool. By focusing on the fact that embedded devices are designed for specific and limited purposes, the proposed templates enable the detection of threats against assets specific to industrial control devices while suppressing the detection of threats occurring within trust boundaries. As a result, both false negatives and false positives of threats are reduced. The results indicate the proposed approach has the potential to standardize quality of threat modeling and significantly reduce the required effort.

Contact : *YODA Yasuki* yasuki.yoda@omron.com

1. まえがき

1.1 製品セキュリティ対策の必要性

サイバー攻撃の対象は、従来からの情報システムに対する攻撃にとどまらず、工場などの制御システムへと拡大している。工場のスマート化とオープン化に伴い、IT（情報技術）領域とOT（制御技術）領域の融合が進んだことにより、いままで独自技術で構成され閉域網でのみ使用されていた産業用制御システムや産業用制御機器においてもサイバー攻撃のリスクにさらされるようになった。今や、制御システムであっても情報システム同様のセキュリティ対策が求められる時代となってきている。

このような背景を受けて、各国・業界はシステムだけでなく、製品そのものに対するセキュリティ法規制やガイドラインの整備を進めている。例えば、欧州サイバーレジリエンス法では広範な“デジタル要素を持つ製品”に対して、製品特性要件と脆弱性処理要件から構成されるサイバーセキュリティ必須要件への適合を要求しており、2027年12月11日より強制化される予定である[1)]。また、半導体製造装置ではSEMI E187/E188、船用機器ではIACS E27などのセキュリティ規格が制定され調達要件となっている。

製造業者にとってこれらの法規制・ガイドラインへの適合は市場での存続要件として不可欠となってきており、オムロンでも対応を進めている。

1.2 脅威分析の必要性と課題

製品のセキュリティ対策を体系的に進める上で、製品のセキュリティリスクを特定するための脅威分析が不可欠である。制御システムセキュリティの国際規格であるIEC 62443-4-1では、脅威モデリングと呼ばれるリスクベースのアプローチを採用することを求めている[2)]。

脅威モデリングとは、潜在的なセキュリティ上の問題を特定するためのセキュリティ設計分析手法であり、STRIDEなどのフレームワークに基づいて脅威を抽出する、構造化アプローチの脅威分析手法である[3)]。分析対象のシステム固有の特性や状況を考慮した精度の高い分析ができる一方で、分析者の分析対象およびセキュリティの専門知識や分析フレームワークに対する熟練を必要とする。また、システムの規模や採用したフレームワークによっては多くの工数がかかることがある。

欧州サイバーレジリエンス法では、既存の製品であっても、2027年12月11日以降に欧州に出荷する場合は本法の定める必須サイバーセキュリティ要件への適合を求めている。これは各製造業者が、欧州サイバーレジリエンス法の対応期限までに、多くの既存の製品に対して、脅威分析に基づくセキュリティ対策を行わなければいけないことを意味する。世界的にセキュリティ人材が不足する中、各製造業者がそのような人材を必要数確保し、期限までに対応することは難しい状況にある。

1.3 脅威分析ツールの導入による課題の解決

前述の課題の解決策の一つとして、コンピュータ支援による脅威分析の自動化がある。本研究では、脅威分析の未熟練者であっても産業用制御機器の脅威分析を一定品質かつ短期間で実施できるようにすることを目標とし、その手段として脅威分析ツールの導入を検討する。

脅威分析ツールでは、分析対象を表現したモデルに対して、あらかじめ定義された脅威生成ルールとのパターンマッチングを行うことで脅威を抽出する。このマッチング処理は汎用的な機構として実装される一方で、脅威生成ルールの定義は分析対象のシステム特性に依存する。そのため脅威分析の品質を確保するには、分析対象のシステム特性を適切に反映した脅威生成ルールの定義が不可欠である。

従来の脅威分析ツールはIT領域が対象であることが多く、それらとは異なる特性や運用環境を持つ産業用制御機器に対して、同様の脅威生成ルールを適用した場合の妥当性は必ずしも明らかではなかった。そこで本稿では、産業用制御機器のシステム特性に応じた脅威生成ルールを設計し、産業用制御機器に適した脅威を自動的に抽出する手法を提案する。また、具体的な概念実証として、代表的な脅威分析ツールであるMicrosoft Threat Modeling Tool（以下、Threat Modeling Tool）を用い、脅威生成ルールをテンプレートとして実装し、その効果を検証する。

2. 脅威モデリングおよび脅威分析ツールの基礎

本章では、次章で述べる産業用制御機器向け脅威モデリングテンプレートの設計を検討するための前提となる、脅威モデリングと脅威分析ツールに関する基礎的な知識について整理する。

2.1 STRIDEによる脅威モデリング[3)]

脅威モデリング手法には、高度な専門知識を前提としたものから、比較的簡単に適用可能なものまで多様なアプローチが存在するが、本稿では未熟練者であっても適用可能であり、かつツールによる自動化に適した手法として、STRIDEによる脅威モデリングを取り上げる。

STRIDEによる脅威モデリングは、システムのモデル表現であるデータフロー図に対して、脅威を抽出するためのガイドワードであるSTRIDEを体系的にパターンマッチングさせることで包括的な脅威を特定する手法である。以下にその手順を述べる。

Step 1：モデル作成

分析対象のモデルをデータフロー図で作成する。表1にデータフロー図の要素を示す。

表 1　データフロー図の要素

要素種別	説明	図記号
External Entity（外部エンティティ）	データの外部入出力先	
Data Store（データストア）	データが保存される場所	
Data Flow（データフロー）	データの流れ	
Process（プロセス）	データの処理	
Trust Boundary（信頼境界）	信頼レベルの切り替わる境界	

脅威モデリングでは、一般的なデータフロー図の図記号に加え、信頼境界の図記号を用いる。信頼境界は信頼できる領域と信頼できない領域を区切る境界線である。信頼境界を越えてくるデータフローは原則として信頼できない入力として扱われ、脅威分析においては認証や入力妥当性確認を検討すべき対象となる。信頼境界は外部からの入力がシステム内部に到達する箇所を明確化するための概念であり、信頼境界を跨ぐインタフェースやデータフローは、しばしば攻撃面として扱われる。

図 1 に産業用制御機器の代表である PLC（Programmable Logic Controller）の簡易的なデータフロー図の例を示す。本図では信頼境界は PLC の筐体、すなわち物理的境界と置いた。PLC の筐体の内部は信頼できる領域として扱い、PLC と Ethernet 通信をする PC は信頼できない領域と扱うことを意味する。

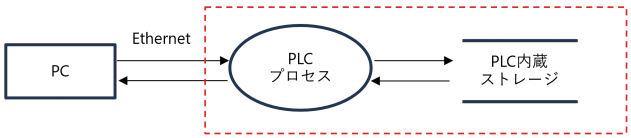

図 1　PLC の簡易的なデータフロー図の例

Step 2：脅威抽出

Step 1 で作成したデータフロー図に対して、代表的な脅威のカテゴリを表す STRIDE をガイドワードとして適用することで、脅威を抽出する。STRIDE とは表 2 に示す各ガイドワードの頭文字をとったものである。

表 2　STRIDE

ガイドワード	説明
Spoofing（なりすまし）	自分以外の誰か／何かになりすますこと
Tampering（改ざん）	変更してはいけないものを変更すること
Repudiation（否認）	何かの行為を、自分はやっていないと主張すること
Information Disclosure（情報漏洩）	権限のない人に情報が提供されてしまうこと
Denial of Service（サービス拒否）	システムがサービスを提供できないようにすること
Elevation of Privilege（特権昇格）	プログラムやユーザが、本来実行できてはならないことが実行できるようになること

STRIDE を体系的にデータフロー図へ適用する方法として、データフロー図の要素に着目する STRIDE per Element と相互作用に着目する STRIDE per Interaction がある。

STRIDE per Element では表 3 に定義されるような、データフロー図の要素と STRIDE の対応表を用いて、脅威を抽出する。STRIDE per Element は簡易的で扱いやすいため人による手動での分析に適しているが、脅威の抽象度が高く、その解釈には主観が入りやすいという特徴がある。

表 3　STRIDE per Element

要素	S	T	R	I	D	E
外部エンティティ	○		○			
データストア		○	○(*1)	○	○	
データフロー		○		○	○	
プロセス	○	○	○	○	○	○

(*1) データストアにログが保存されている場合のみ

図 1 のモデルに対して STRIDE per Element を適用した場合に抽出される脅威の一部抜粋を表 4 に示す。

表 4　STRIDE per Element を使って抽出した脅威の例（抜粋）

適用したデータフロー図の要素	適用したガイドワード	抽出された脅威
PC（外部エンティティ）	Spoofing（なりすまし）	なりすました PC からの PLC への不正アクセス
PLC 内蔵ストレージ（データストア）	Tampering（改ざん）	PLC 内蔵ストレージ上のデータの改ざん
Ethernet（データフロー）	Information Disclosure（情報漏洩）	Ethernet 上の通信データの傍受

表 5　STRIDE per Interaction

要素	相互作用	S	T	R	I	D	E
外部エンティティ	外部エンティティからプロセスへデータフローがある	○		○	○		
	プロセスから外部エンティティへのデータフローがある	○					
データストア	プロセスからデータストアへのデータフローがある		○	○	○	○	
	データストアからプロセスへのデータフローがある			○	○	○	
データフロー	データフローが信頼境界を超える		○		○	○	
プロセス	プロセスからデータストアへのデータフローがある	○			○		
	プロセスから他のプロセスへのデータフローがある	○		○	○	○	○
	プロセスから外部エンティティ（コード）へのデータフローがある	○		○	○	○	
	プロセスから外部エンティティ（人）へのデータフローがある			○			
	データストアからプロセスへのデータフローがある	○	○			○	○
	他のプロセスからプロセスへのデータフローがある	○		○		○	○
	外部エンティティからプロセスへのデータフローがある	○				○	○

一方、STRIDE per Interaction では表 5 に定義されるような、データフロー図の二つの要素間の相互作用と STRIDE の対応表を用いて、脅威を抽出する。STRIDE per Interaction は STRIDE per Element と比較して、複雑度が高くツールの支援が必要となるが、相互作用という文脈が追加されることにより脅威の具体度が高く客観的に理解しやすいという特徴がある。

STRIDE per Interaction を適用した場合の具体例は、2.2 で説明する。

Step 3：対策検討

一般的なリスク管理と同様に、脅威の発生可能性と発生時の影響度の観点からリスク評価を行い、リスク回避、リスク低減、リスク移転、リスク受容のいずれの対応を取るか判断する。リスク低減と判断したものについては製品への技術的な対策を実施し、リスク移転と判断したものについては、当該リスクおよび必要な対策をユーザに伝達する。表 6 に、リスク低減の際の製品への技術的な対策の例を示す。

表 6　製品への技術的な対策の例

抽出された脅威	技術的な対策
PC になりすました PLC への不正アクセス	ユーザの認証を行う
PLC 内蔵ストレージ上のデータの改ざん	データの改ざん検知を行う
Ethernet 上の通信データの傍受	通信を暗号化する

Step 4：レビュ

設計者、セキュリティ専門家、テスト担当者などの複数の視点から、Step 1 から Step 3 で検討したモデル・脅威・対策のそれぞれに対して、明瞭性、正確性、網羅性、妥当性、一貫性、追跡可能性などの観点を確認する。実施形態としては対面型、配布型、および、その組み合わせ型がある。いずれの場合もレビュ資料に基づき行われ、レビュ結果は記録され、必要に応じてモデル、脅威、対策にフィードバックされる。

2.2 STRIDE による脅威分析ツール

STRIDE による脅威分析ツールは、ユーザが作成したデータフロー図とあらかじめ定義された脅威生成ルールを機械的にパターンマッチングさせることで、該当する脅威を自動抽出する。表 7 に代表的な STRIDE による脅威分析ツールを示す。いずれも IT 領域の製品を主な分析対象としている。

表 7　STRIDE による脅威分析ツールの一例

名称	提供元	想定する主な分析対象	パターンマッチングの方式	脅威生成ルールのカスタマイズ
Threat Modeling Tool[4]	Microsoft	PC ソフトウェア エンタープライズ クラウドサービス	STRIDE per Interaction	可
Threat Dragon[5]	OWASP	Web アプリケーション	STRIDE per Element STRIDE per Interaction	不可

Threat Modeling Tool はユーザが脅威生成ルールをカスタマイズ可能なテンプレート機能を持つ。一方、Threat Dragon の脅威生成ルールはツール本体に組み込まれており、脅威生成ルールの変更はできない。

以下に、脅威生成ルールをカスタマイズ可能な Threat Modeling Tool を取り上げ、その仕組みについて説明する。表 8 にテンプレートに定義される脅威生成ルールの一部を示す。

表 8　Threat Modeling Tool の脅威生成ルールの例

脅威名称	条件式
認証情報の漏洩	［プロセス］から［データストア］へのデータフローがある AND［データストア］は認証情報を保存している
入力データの不正操作	（他の［プロセス］から［プロセス］へのデータフローがある OR［外部エンティティ］から［プロセス］へのデータフローがある） AND［データフロー］が信頼境界を超える

ここで、条件にある“［データストア］は認証情報を保存している”は、データストアに設定可能な属性値である。Threat Modeling Tool のテンプレートでは、脅威生成ルールに加えデータフロー図の要素が持つ属性も定義可能であり、各要素において保護すべき資産の取り扱い有無、セキュリティ対策の実装有無などの特性を考慮した脅威生成ルールを定義することができる。これによってデータフロー図の視覚的表現だけでは表しきれない要素の属性を考慮した脅威抽出を可能としている。

図 1 のデータフロー図に対して、表 8 に示した脅威生成ルールを適用した場合の、脅威の検出有無を表 9 に示す。

表 9　相互作用ごとの脅威の検出有無

データフロー（図 1 より）		脅威生成ルール（表 8 より）	
From	To	認証情報の漏洩	入力データの不正操作
PC（外部エンティティ）	PLC プロセス（プロセス）		○
PLC プロセス（プロセス）	PC（外部エンティティ）		
PLC プロセス（プロセス）	PLC 内蔵ストレージ（データストア）	○(*1)	
PLC 内蔵ストレージ（データストア）	PLC プロセス（プロセス）		

(*1) PLC 内蔵ストレージに認証情報を保存している場合のみ

脅威分析ツールの分析結果は、ツール本体の機能そのものよりも、テンプレートに定義された脅威生成ルールの内容に強く依存する。表 10 に示す Microsoft が提供する公式テンプレートにおいても、それぞれの想定する分析対象のシステム特性ごとに用意されていることがわかる。産業用制御機器においても同様に、そのシステム特性に応じたテンプレートの設計を行うことが、脅威分析結果の品質を高めるために重要となる。

表 10　Microsoft の提供する脅威モデリングテンプレート

名称	想定する分析対象
SDL TM Knowledge Base	PC ソフトウェア／エンタープライズ／クラウドサービス
Azure Threat Model Template	Azure
Medical Device Model	医療機器

3. 産業用制御機器のシステム特性を考慮した脅威分析テンプレートの設計

本章では、Threat Modeling Tool を用いた産業用制御機器向け脅威分析テンプレートの設計および実装について詳述する。IT 領域や他の組み込み機器とは異なる産業用制御機器のシステム特性を踏まえ、テンプレートの設計方針を示し、Threat Modeling Tool の産業用制御機器向けテンプレートを作成する。

3.1 脅威モデリングの前提となる産業用制御機器のシステム特性

産業用制御機器は特定の用途に限定して設計されている組み込み機器であり、汎用機器やソフトウェア製品、クラウドサービスといった IT 領域の製品、さらには他の用途を持つ組み込み機器（例：医療機器）とは異なるシステム特性を持つ。本稿では、主要なシステム特性として、保護すべき情報資産および想定すべき攻撃面の違いに着目し、脅威分析テンプレートの設計を行うこととする。

前述のとおり Threat Modeling Tool では、要素、相互関係、属性および信頼境界から構成される条件式によって脅威生成ルールを定義する。要素と相互関係はデータフロー図の一般的要素であるため、分析対象のシステム特性は、属性と信頼境界に現れる。保護すべき情報資産は属性に、想定すべき攻撃面は信頼境界にそれぞれ対応する。

3.1.1 保護すべき情報資産

表 11 に産業用制御機器の扱う代表的な情報資産とその保護特性を示す。一般に特定の用途に限定して設計されている組み込み機器では、汎用機器と比べて扱う情報資産も限定的である。セキュリティとして共通的な資産である認

証情報やログ、組み込み機器として共通的な資産であるファームウェアや設定情報に加え、産業用制御機器特有の情報資産として PLC におけるユーザプログラムがある。特に、産業用制御機器においては、制御ノウハウの流出防止や誤動作／危険動作の防止のために、ファームウェア、設定情報、ユーザプログラムの機密性および完全性の保護が重要となる。また、制御システムの安定稼働を実現するために、ファームウェアやユーザプログラムの可用性の保護も重要である。

表 11　産業用制御機器の代表的な情報資産とその保護特性

情報資産		機密性	完全性	可用性
セキュリティ共通	認証情報	○	○	
	ログ		○	
組み込み機器共通	ファームウェア	○	○	○
	設定情報	○	○	
産業用制御機器特有	ユーザプログラム	○	○	○

なお、本稿では、機密性と完全性はその情報資産がデータストアに保存またはデータフローを伝送されている状態に対する特性とし、可用性はその情報資産がプロセスとして実行されている状態に対する特性と位置付ける。

3.1.2 想定すべき攻撃面

表 12 に製品／サービス種別ごとの典型的な攻撃面の違いを示す。一般に特定の用途に限定して設計されている組み込み機器では、ユーザが OS にログインして自由な操作を行うようなローカル権限を提供していない。そのため、ローカル権限を悪用した攻撃の可能性よりも、ネットワーク経由での攻撃や、ハードウェア製品として特有の物理攻撃（製品の物理インタフェース経由での攻撃や、製品内部部品に対して直接読み書きする攻撃）を考慮する方が適切である。

3.2 産業用制御機器のシステム特性に基づくテンプレートの設計方針

本稿では、Threat Modeling Tool の公式テンプレートの中でも、最も汎用性が高い SDL TM Knowledge Base（以下、デフォルトテンプレート）に対して、3.1 で明らかにした産業用制御機器のシステム特性を考慮したカスタマイズを加えることで、産業用制御機器向けのテンプレートを作成する。

3.2.1 保護すべき情報資産

データストアの属性として、保護すべき情報資産を表現する方法を採用する。Threat Modeling Tool のデフォルトテンプレートのデータストアには、認証情報やログを保存していることを表す属性が存在している。産業用制御機器向けのテンプレートでは、これに、ファームウェア、設定情報、ユーザプログラムを保存していることを表す属性を追加する。また、これらの属性を参照した脅威生成ルールを追加し、該当する情報資産の機密性および完全性を脅かす脅威を検出する。

この方法により、“データストアの改ざん”という抽象的な脅威ではなく、“ファームウェアの改ざん”や“ユーザプログラムの情報漏洩”といった産業用制御機器として守るべき資産に対する具体的な脅威の検出を可能とする。なお、データフローやプロセスに関してはデフォルトテンプレートに存在している脅威生成ルールをそのまま利用することとした。

3.2.2 想定すべき攻撃面

産業用制御機器の物理的境界を信頼境界ととらえ、外部インタフェース経由での脅威を検出の対象とする。データフローが信頼境界を越えない脅威については、ローカル権限を必要とする攻撃と見なし、検出の対象から除外する。

一方で、組み込み機器として考慮すべき脅威として、外部インタフェースとして現れない電子回路基板上のデバッグインタフェースやメモリデバイスの直接読み書きなどの、製品内部への物理攻撃がある。データフロー図では表

表 12　製品／サービス種別ごとの典型的な攻撃面の違い

製品／サービス種別		ネットワーク	ローカル	物理
ソフトウェア製品		◎	○	×
クラウドサービス	IaaS（Infrastructure as a Service）/PaaS（Platform as a Service）	◎	△	×
	SaaS（Software as a Service）	◎	×	×
ハードウェア製品	汎用機器（PC ／サーバ機器など）	◎	○	△
	組み込み機器（産業用制御機器、医療機器、IoT 機器など）	◎	×	△

◎：よくある、○：たまにある、△：まれにある、×：めったにない

現が難しいこれらの脅威を検出するために、3.2.1 に挙げた保護すべき情報資産に対する脅威に限り、データフローが信頼境界を越えない場合においても脅威を検出する方法を採用する。

これらの方法により、リスクの高い外部インタフェース経由での攻撃と、製品内部に保存された保護すべき情報資産への物理攻撃を中心とした脅威の検出を可能とする。

3.3 産業用制御機器のシステム特性に基づくテンプレートの実装

3.2 に基づき、実際に Threat Modeling Tool のデフォルトテンプレートに対して行ったカスタマイズの内容を示す。

3.3.1 保護すべき情報資産

まず、産業用制御機器として保護すべき情報資産をデータストアの属性として定義した。実際に追加した属性を表 13 に示す。認証情報およびログについては、デフォルトテンプレートに定義されている属性をそのまま利用することとした。

表 13　データストアに追加した属性

要素種別	属性名	属性値
データストア	ファームウェアを保存している	Yes, No
	設定情報を保存している	Yes, No
	ユーザプログラムを保存している	Yes, No

次に、産業用制御機器として保護すべき情報資産に対する脅威生成ルールを追加した。追加した脅威のうち改ざんの脅威の抜粋を表 14 に示す。実際には情報漏洩についても同様に追加を行っている。なお、前述のとおり物理攻撃を想定するため、脅威生成ルールの条件式には“[データフロー] が信頼境界を超える”という条件は含めていない。また、認証情報の情報漏洩やログの改ざんに対する脅威は、デフォルトテンプレートに定義されているものをそのまま利用することとした。

3.3.2 想定すべき攻撃面

前述の産業用制御機器として保護すべき情報資産が対象となる脅威以外の脅威については信頼境界を超えた場合にのみ脅威を検出するよう変更を行った。表 15 に変更した脅威生成ルールの例を示す。なお、外部エンティティのなりすましや、信頼境界を超えるデータフローの盗聴などの脅威は、デフォルトテンプレートに定義されているものをそのまま利用することとした。

4. 検証結果と考察

4.1 検証方法

ユーザプログラム実行機能を持ったオムロンの産業用制御コントローラ製品に対して、スプレッドシートを使った手動による分析、Threat Modeling Tool のデフォルトテンプレートおよびカスタマイズ後のテンプレート（以下、カス

表 14　追加した脅威生成ルールの一部

脅威名称	条件式
ファームウェアの改ざん	[プロセス] から [データストア] へのデータフローがある AND [データストア] はファームウェアを保存している
設定情報の改ざん	[プロセス] から [データストア] へのデータフローがある AND [データストア] は設定情報を保存している
ユーザプログラムの改ざん	[プロセス] から [データストア] へのデータフローがある AND [データストア] はユーザプログラムを保存している
認証情報の改ざん	[プロセス] から [データストア] へのデータフローがある AND [データストア] は認証情報を保存している

表 15　変更した脅威生成ルールの例

名称	条件式（変更前）	条件式（変更後）
プロセスメモリの改ざん	[プロセス] から [プロセス] へのデータフローがある	[プロセス] から [プロセス] へのデータフローがある AND [データフロー] が信頼境界を超える
データストアのなりすまし	[プロセス] から [データストア] へのデータフローがある OR [データストア] から [プロセス] へのデータフローがある	([プロセス] から [データストア] へのデータフローがある OR [データストア] から [プロセス] へのデータフローがある) AND [データフロー] が信頼境界を超える

タムテンプレート）を使ったツールによる分析の結果に対し、脅威検出傾向の分析と工数削減効果を見積もることにより、カスタムテンプレートの正確性および有効性の評価を行う。また、それらの結果をもとに、本テンプレート設計の適用範囲と限界について考察を行う。なお、手動による分析の結果は、オムロンの制御機器事業で取り扱う製品に対する開発プロジェクトにおける実績に基づいている。

4.2 検証結果

4.2.1 正確性（誤検出・未検出）の評価

手動による分析と、Threat Modeling Toolのカスタマイズ前後のテンプレートでそれぞれ検出した脅威の傾向を表16に示す。手動による分析は、熟練者が実施し、専門家によるレビュを受けた後の値を示している。

デフォルトテンプレートを使った場合、誤検出や未検出の脅威があることがわかる。これは、デフォルトテンプレートが想定する分析対象のシステム特性が産業用制御機器に適しておらず、正確性に問題があることを示している。これに対し、カスタムテンプレートを使った場合、誤検出や未検出が取り除けていることがわかる。これは、テンプレートのカスタマイズにより産業用制御機器のシステム特性を適切に考慮できるようになり、未熟練者であっても熟練者が分析を行う場合と同等の正確性を持った脅威の抽出が可能になったことを意味している。

一方で、手動による分析と比較すると脅威の検出数が約2倍となっていることがわかる。これは主にSTRIDE per ElementとSTRIDE per Interactionの違いに起因する。STRIDE per Interactionは二つの要素間の相互作用に対して脅威を抽出する方式であるため、双方向のデータフローがある場合、その両端の要素に対する脅威がそれぞれの方向に対して検出される。相互作用を考慮せず要素ごとに独立して脅威を抽出するSTRIDE per Elementと比較して、脅威数は相対的に多くなる。なお、属性や信頼境界を条件として考慮していることと、同じ条件式であっても異なる脅威がある場合、脅威が複数種類検出されることがあるため、単純に2倍とはならない。

4.2.2 有効性（工数・再現性）の評価

手動による分析とカスタムテンプレートによる分析にかかる工数の削減効果を見積もった。その結果を図2に示す。なお、手動による分析は、熟練者が実施し、専門家によるレビュを受けた後の値を示している。また、工数は分析担当者のものであり、レビュ担当者などの工数は含んでいない。手動による分析では、熟練者であっても脅威分析全体の工程のうち、約36%の工数がかかっていることがわかる。カスタムテンプレートを使った分析では、脅威の自動生成が可能になったことから、脅威抽出にかかる工数は0とした。検出数は約2倍となったが、双方向のデータフローに対する脅威への対策は共通であることと、脅威の具体化・細分化により分析結果の理解容易性、追跡可能性、および再現性が向上することから、検出数増に伴う工数増を対策検討やレビュの効率化に伴う工数減で相殺可能と考え、対策検討工数とレビュ工数は変化なしとした。その結果約36%の工数の削減効果が見込めることが分かった。

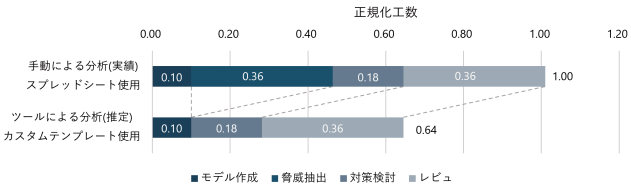

図2　産業用制御機器向け脅威分析ツール導入による工数削減効果（熟練者）

4.3 考察

本稿では産業用制御機器を対象として、脅威分析ツールにおけるテンプレートをシステム特性に基づいてカスタマイズすることにより、脅威分析の正確性および有効性を向上させる手法を示した。その結果、未熟練者であっても熟練者と同等品質の脅威抽出が可能となり、さらに脅威分析全体に対して約36%の工数削減効果があることを確認した。また、手動で分析した場合と比べ、抽出された脅威の数が約2倍となったが、これはSTRIDE per Interactionの特徴である脅威の具体化・細分化によるものであり、脅威シナリオの理解容易性の向上や標準的な対策の提案、脅威抑

表16　脅威分析の方法による検出件数の比較

脅威分析の方法		検出数	正検出	誤検出	未検出
手動による分析 (STRIDE per Element)	スプレッドシート使用	143	143	0	0
ツールによる分析 (STRIDE per Interaction)	Threat Modeling Tool 使用 (デフォルトテンプレート)	185	169	16	123
	Threat Modeling Tool 使用 (カスタムテンプレート)	292	292	0	0

制のための属性の追加などのテンプレートの改善を継続することで、さらなる対策検討工数およびレビュ工数の削減ができる可能性がある。

本手法の適用範囲は、特定の用途に限定して設計されている組み込み機器で、かつ、ユーザが OS にログインして自由に操作可能なローカル権限を持たないものに限定される。そのため産業用 PC や産業用シングルボードコンピュータのように、ユーザがローカル権限を利用可能な機器については、本稿で示した前提条件が成立せず、同一のテンプレート設計方針を適用することはできない。また、本稿では、製品のセキュリティ要件を定めるための、外部インタフェースや資産に着目した最上位レベルの抽象度での脅威分析を対象としている。そのため製品内部での多層防御を目的とした、製品アーキテクチャレベルでの詳細な脅威分析を行う場合については、適切な詳細度に応じたテンプレート設計が必要となる。

なお、本稿で提案した考え方は、特定のツールに依存するものではなく、分析対象をモデル化し、事前に定義されたルールによるパターンマッチングによって脅威を抽出する仕組みを持つ脅威分析ツール全般に適用可能なものである。さらに、本手法は、用途が限定され、ユーザがローカル権限を持たないという特性を有する組み込み機器に共通する考え方と位置付けることができ、産業用制御機器以外の組み込み機器全般においても、脅威分析のテンプレートを設計する際の指針として有用であると考える。

5. むすび

本稿では、製品セキュリティに関する法規制や業界要求の強化により、既存製品を含む多くの製品に対して脅威分析に基づくセキュリティ対策が求められている一方で、専門人材や対応工数の不足を社会課題と捉えた。これらの課題に対し、未熟練者であっても一定品質かつ短期間で脅威分析を実施可能とすることを目的として、産業用制御機器向けの脅威分析テンプレートの設計と自動化に取り組んだ。

その結果、産業用制御機器のシステム特性を考慮したテンプレートを用いることで、未熟練者であっても熟練者と同等品質の脅威抽出が可能となることを確認するとともに、脅威分析全体の工数を約 36%削減できることを示した。本成果は、従来、専門家や熟練者への依存度が高かった脅威分析を、分析者の熟練度に依存せず、複数の製品や開発チームに対して横断的かつ継続的に適用可能な、再現性の高いプロセスへと転換できる可能性を示している。特に IT 業界と比べてセキュリティの専門家や熟練者の少ない産業用制御機器業界にこそ、大きな効果が期待されるものである。

今後は、最新の脅威・技術動向や既存の攻撃・対策技術の知識体系を活用し、産業用制御機器特有の脅威シナリオや標準的対策をテンプレートに反映していくことで、継続的な製品セキュリティの向上を図る。

本稿で示した考え方は、特定のツールに依存するものではなく、同様の仕組みを持つ脅威分析ツールにも展開可能である。本アプローチが広く活用されることで、産業用制御機器をはじめとする組み込み機器分野における製品セキュリティ対応の迅速化と品質確保の両立が進み、産業界全体のサイバーレジリエンス向上に寄与することを期待する。

参考文献

1) European Union. “Regulation（EU）2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations（EU）No 168/2013 and（EU）2019/1020 and Directive（EU）2020/1828（Cyber Resilience Act）.” EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847（Accessed: Jan. 5, 2026）.
2) *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*, IEC 62443-4-1 Edition 1.0, 2018.
3) A. Shostack, *Threat Modeling: Designing for Security*, Wiley, 2014.
4) Microsoft Corporation. “Microsoft Threat Modeling Tool の概要.” Microsoft Learn. https://learn.microsoft.com/ja-jp/azure/security/develop/threat-modeling-tool-getting-started（Accessed: Jan. 5, 2026）.
5) OWASP Foundation. “OWASP Threat Dragon.” OWASP. https://owasp.org/www-project-threat-dragon/（Accessed: Jan. 5, 2026）.

執筆者紹介

依田 安基　YODA Yasuki
インダストリアルオートメーションビジネスカンパニー
商品事業本部　コントローラ事業部
PLC ソフトウェア開発部
専門：情報工学