多様なドメインの組込機器製品における費用対効果に優れた脅威分析手法の検討

芹川 正孝，丹羽 徹，吉岡 幸恵，原田 真太郎

IoT 時代の到来により、あらゆる機器がインターネットに接続されるようになり、増大する IoT のセキュリティ脅威[1)] は現実のものとなっている。安心してユーザが使用できる製品を提供するためにはセキュリティの脅威分析を行い、サイバー攻撃を受けても重大なインシデントに至らない対策を実施する必要がある。

従来の脅威分析手法は情報システムを対象としており、情報の機密性が重視されているが、安定した稼働を重視する組込機器では可用性をより重視する必要がある。加えて、発生確率の低い脅威も含めた網羅的な分析には膨大な工数がかかり、開発費の肥大化をまねく。

これらの課題に対して、効果的かつ効率的に組込機器製品のセキュリティ脅威を分析するための手法について検討し、重要な脅威を漏れなく抽出し、それらの抽出した脅威の対策を行いつつ、脅威分析に必要となる工数の大幅な削減の可能性を得た。

Study of Cost-effective Threat Analysis Methods for Embedded Devices in Various Domains

SERIKAWA Masataka, NIWA Toru, YOSHIOKA Sachie and HARADA Shintaro

By the arrival of the IoT era, embedded devices that connect to the Internet being exposed cyberattacks[1)] . In order to provide products that users can use with reassurance, it is necessary to analyze security threats and take countermeasures to avoid important cyberattacks. OMRON had a problem that there was no threat analysis method that focuses on availability for embedded devices, and there was no efficient and effective threat analysis method.

To address these issues, we studied a method for effectively and efficiently analyzing security threats to embedded equipment products and found that it has the potential to significantly reduce the number of man-hours required for threat analysis while extracting all important threats and implementing countermeasures against those extracted threats.

1. まえがき

1.1 サイバーセキュリティリスクの高まり

IoT 時代の到来により、あらゆる機器がインターネットに接続されるようになり、さまざまな分野で新しいサービスの提供や利便性の向上が図られている。一方で、機器がインターネットに接続されることで、組込機器を対象にしたサイバー攻撃が現実のものとなっており、サイバーセキュリティインシデントの防止が事業課題の一つとなっている。

オムロンの製品・サービスについてもサイバーセキュリティのリスクの高まりは同様であり、オムロンでは、公共システムや健康、製造システムといった幅広い分野で活用される製品、サービスを提供していること、人の安全に関わる製品や個人情報をはじめとした機密情報の取り扱いも多いことから、社会に与える影響も大きくなることが考えられる。多様な事業ドメイン、異なる特性の製品を持つオムロンにおいては、個々の事業に合ったセキュリティ対策が必要となった。これまで、オムロンでは製品のセキュリティ対策として多様な事業ドメインに対し体系立ったものはなく、開発者のスキルに依存した対応となっていた。未然にセキュリティインシデントを防ぐためには、開発工程の中で効率よくセキュリティ脅威を分析し、適切な対策を実施することが求められていた。

Contact : *SERIKAWA Masataka* masataka.serikawa@omron.com

1.2 オムロンでのセキュリティ対策の課題

情報システムでは標準的な機器や OS が利用され、ミド

ルウェアなども共通のものが使用されることが多く、セキュリティに対する知見は数多くあって、脅威となるリスクと対策が体系化されている。しかし、組込機器についてはドメインごとに異なる技術、異なるリスクがあり、種々の対策を模索している状況で、世の中に公表されている知見は少ない。そのため、組込機器においては、製品や利用環境におけるセキュリティ脅威を分析し、その結果に応じた対策が必要となっている。しかしながら、昨今の組込機器に搭載されるソフトウェアの規模の増大やオープンソースソフトウェアの活用などを考慮すると、製品や利用環境ごとに脅威分析を網羅的に実施し、対策を実施することは現実的ではない。また、オムロンでは多種多様な製品を持つことに加え、新規商品開発や新規ビジネスを展開する場合に、後戻りをなくすため、商品開発の上流で、効果的、効率的な脅威分析を行い、優先的に対策すべきリスクを抽出する必要があった。

オムロンの主力製品である組込機器のセキュリティ確保のために、脅威分析に求められる要件として、

・多様な事業ドメインに適用可能であること
・企画段階で重要なリスクを抽出できること
・効率的（低コスト、短期間）に実施が可能であること

を設定し、セキュリティリスクの低減と市場競争力の維持・強化を目的とする脅威分析手法を構築することに着目した。

2. 製品のセキュリティ対策の着目点

製品のセキュリティ対策とは、様々なセキュリティ脅威から製品の機密性、完全性、可用性を確保するための取り組みで、最近では、特にモノがつながる世界においてサイバー攻撃の脅威に重点を置いたセキュリティの対策を行うことを指す。

製品に対するセキュリティ脅威は、製品の企画から廃棄に至る各フェーズで存在しているため、ライフサイクル全体を通じて製品に合った適切なセキュリティ対策を行う必要がある。ここでは、企画、開発、運用、廃棄の４つのフェーズにおける一般的なセキュリティ対策について以下に示す。

・企画フェーズ

製品が属するシステム全体の脅威分析を行い、製品を取り巻くセキュリティ脅威を把握し、リスクを評価する。リスクの評価結果に基づいて、リスクへの対応を加味した開発期間や予算について検討し、セキュリティ要件を策定する。これにより、セキュリティに対する取り組みレベルを決定し、システム要件から来る脆弱性の対策を実施する。

・開発フェーズ

企画フェーズで策定したセキュリティ要件に基づき、セキュリティ対策について設計し、実装する。また、プログラムのコーディングなどの実装方法から来る脆弱性の混入を防止する。さらに、開発フェーズでは、セキュリティ要件に基づく脆弱性の検証を実施する。これらよって、実装時に混入する脆弱性への対策を実施する。

・運用フェーズ

運用フェーズとは、市場で製品が利用されている状態を指す。このフェーズの中で、新たに発見される製品の脆弱性や、製品に使用しているOSやミドルウェアの脆弱性の情報を収集し、パッチの提供や緩和策など、適切な対策を迅速に実施し、セキュリティインシデントの発生を予防する。また、インシデントが発生した場合も、その影響を最小限にするための同様の対策を実施することが必要となる。

・廃棄フェーズ

製品は買い替えや利用停止、故障などにより廃棄されることがあるため、製品内にある機密情報の漏洩防止を目的として、確実なデータの消去や製品の回収のための仕組みをセキュリティ対策として作っておくことが必要である。

このように、セキュリティ対策は各フェーズで様々なものがあるが、いずれにしても脅威分析を行い、製品ライフサイクル全体のセキュリティ脅威を把握しておくことが、重要なリスクを漏れなく抽出するために必要となる。そのため、企画段階から実施可能で各製品に適した脅威分析の手法に着目した。

2.1 一般的なセキュリティ脅威分析手法

一般的な脅威分析手法には、主に以下（表1）のような手法がある。

表1　脅威分析手法比較[3)]

分析手法		工数	リスク抽出精度	
ベースライン アプローチ		小	中	対策起点のリスク抽出であるため適合性が低い
非形式的 アプローチ		小	不明	属人的で経験に依存
詳細リスク分析	資産ベース	中	中	構成要素の脅威を網羅的に抽出
	攻撃ツリー解析（ATA）	大	中	攻撃の入口から網羅的にリスク抽出
	フォルトツリー解析（FTA）	大	中	想定される最終被害から網羅的にリスク抽出
組み合わせ アプローチ		中	中～高	精度は組み合わせにより向上

・ベースラインアプローチ
　既存の標準や基準をもとに、想定する典型的なシステムに対して、予め一定の確保すべきセキュリティレベルを設定し、それを達成するためのセキュリティ要件を定め、分析対象となるシステムの対策の適合性等をチェックする。

・非形式的アプローチ
　組織や担当者の経験や判断に基づき、リスク分析を実施する。

・詳細リスク分析
　分析対象のシステム自体に対して、そのシステムもしくはそれにより実現されている事業について、「重要度」（あるいは損なわれた場合の被害レベル）「脅威」「脆弱性」の評価指標の下で、攻撃ツリー解析（ATA）などの手法[2)]を用いてリスク分析を実施する。

・組み合わせアプローチ
　複数の手法の長所を取り込み、短所の改善をすることで、作業の効率化、異なった評価視点の活用によって、分析精度の向上と、作業工数増大の回避を図る。ただし、どう組み合わせるのか、それぞれのシステムや事業による差異にどのように対処するかの指針は示されていない。

　これらの一般的な脅威分析手法は、手法ごとに分析のアプローチが異なるため、分析対象に合わせて分析者が適切な手法を選択する必要がある。手法によっては、網羅的な分析が可能である一方、分析対象の規模によっては多くの分析工数が必要となる。

2.2 脅威分析をオムロン製品に適用する際の課題

　前述した「詳細リスク分析」の手法では、様々な情報資産、機能資産に対するセキュリティ脅威を攻撃ツリー解析（ATA）などの手法を用いて分析するが、すべての資産と種々の攻撃パターンを乗じた数百件から数千件に及ぶ脅威が特定される。オムロン製品でこのような網羅的手法を採用した場合、製品の主要な要件を設計、開発する以上の工数がセキュリティ対策にかかる恐れがあった。また、「組み合わせアプローチ」を採用した場合、オムロンでは、ファクトリーオートメーション（以降、FA）、ヘルスケア、モビリティ、エネルギーマネジメントを中心とする事業ドメインで製品・サービスを展開しており、取り扱っている情報・機能も様々で、リスクの種別や影響度合いも異なるため、事業ドメインの特性に応じた対処の指針が不足していた。

　情報システムの領域では、これまでの世の中の取り組みの成果で確立された対策があるが、組込機器の領域では、対象となる機器や取り扱う情報が多種多様で、共通的な脅威分析の手法も確立されていなかった。そのため、各事業ドメインや製品ごとに異なる脅威分析手法を用い、セキュリティ対策を行うことになって、知見の蓄積や人材育成、仕組み、体制の構築等において、事業ドメインごとの負担が大きくなることが想定された。これらのことから、「多様な事業ドメインに適用可能な脅威分析手法」と「効率的（低コスト、短期間）に実施が可能」というところに着目して、オムロンの主力製品である組込機器に適した脅威分析手法を構築することとした。

3. 提案する脅威分析手法

　企画フェーズにおける低コストの脅威分析手法として、特定のアーキテクチャ特徴を持つシステムで脅威頻出箇所表を作成し、類似するアーキテクチャを持つシステムの脅威分析コストの低減を提案している手法[4)]があるが、アーキテクチャごとに脅威頻出箇所表を作成する必要があるため、製品の種類が多いオムロンでは効果を得にくい。

　ここで提案する脅威分析手法では、次の 2 点を特徴とする。

（1）保護資産と保護資産へのアクセス経路に着目し、脅威をフィルタリングし、さらに脅威の分類をガイドワードとして用い、分析が発散することをコントロールする
（2）事業ドメイン、システム特性に応じた評価基準を設定することで製品に適した判断基準で分析する

　これらにより、リスクを抽出し、優先付けを行って、優先順位の高いものから対策を行うことにより、重要なリスクの対策漏れを防止しつつ、効率的に分析を行うことを狙いとしている。

　また、守りたい資産を起点として分析するため、製品の企画、構想段階から分析を行うことが可能となり、分析結果を開発計画に反映することが可能となる。

3.1 事業ドメインを反映した設定

　事業ドメインやシステムの特性を反映させるため、取り上げるセキュリティ脅威を効率よく絞り込むためのフィルタリング条件と、特定した脅威に対するリスクの評価基準を設定する。

3.1.1 脅威フィルタリング条件の設定

　分析対象の製品に対するセキュリティ脅威について、事業ドメインごとに保護資産、アクセス経路、脅威種別の洗い出しを行う。実際にサイバー攻撃で発生しうる脅威には、攻撃の目的となる保護資産とその保護資産へのアクセス経路が必ず存在するため、保護資産とアクセス経路の組み合わせで対象の分析を実施する。このとき、脅威をフィ

ルタリングする条件として、保護資産のレベル（表 2）やアクセス経路のレベル（表 3）を脅威分析の前提条件として設定する。保護資産のレベルは、安全の観点（死亡、重傷、軽傷）、影響範囲の観点（社会、企業、個人）、事業損失の観点（被害金額）を加味し、事業ドメインの特性を考慮して、設定する。アクセス経路のレベルについては、物理的障壁の有無（入退室管理など）、もしくはその障壁の高さ（ファイアウォールの強度など）をシステムの特性に合わせて、設定する。公共システムや工場の製造ラインなどではシステムの安定稼働が求められることが多いため、オムロンの製品は可用性が重要視される。一般的な情報システムでは、機密性、完全性、可用性の順にリスクを考えるが、オムロンの製品では、可用性、完全性、機密性の順序を念頭に置いて、保護資産のレベル設定を行うことが重要である。例えば、FA 制御機器の脅威分析では、保護資産レベル「中」以上、アクセス経路レベル「中」以上を対象とする。

また、発生しうる脅威をガイドワードとして分類（表 4）しておき、保護資産、アクセス経路の組み合わせに脅威の分類が当てはまるかどうかを分析することで脅威を抽出していく。

表 2　保護資産のレベル設定の例（FA 制御機器）

レベル	保護資産（情報）	保護資産（機能）
高	制御システムを動作させるためのプログラムやレシピデータ	機器の動作制御機能、プログラム、パラメータの変更機能
中	品質管理データ	アクセス管理機能（認証）
低	機器の死活監視情報	ラダープログラムデバッグ機能

保護資産には、情報資産と機能資産がある。

表 3　アクセス経路レベル設定の例（FA 制御機器）

レベル	アクセス経路
遠隔（高）	インターネットから直接アクセス可能な通信手段がある。もしくは、無線通信手段がある。
隣接（中）	ファイアウォールや VPN により、隔離されたイントラネットに接続されている。
ローカル（低）	インターネットへの接続経路がなく、機器の直接操作が必要。

表 4　ガイドワードの例（STRIDE）[5)]

脅威種別	備考
なりすまし（Spoofing）	他人へのなりすまし
改ざん（Tampering）	情報の改ざん
否認（Repudiation）	攻撃の否認
情報漏洩（Information Disclosure）	外部への個人情報や機密情報の漏洩
サービス拒否（Denial of Service）	サービスを停止させる
特権の昇格（Elevation of Privileges）	管理者等の権限を奪取し悪用

3.1.2 リスク評価基準の設定

抽出された脅威のリスク評価を行うために、事業ドメインに合ったリスクの発生確率と影響度による評価基準を設定しておく（表 5）。ミッションクリティカルな製品やサービスでは、発生確率が（低）であってもリスク対策が求められる。製品を取り巻く状況に応じて、リスク評価の基準を設定する。表 6 では、「アクセス経路、専門知識の要否、攻撃者の手間」の条件の組み合わせを元に発生確率を設定している。なお攻撃者の手間とは、攻撃成功までに物理的な時間や設備が必要であることや複数の手続きが必要となることを指す。

また、表 7 ではリスク評価基準の安全、評判、事業損失の観点から影響度を設定している。製品の特性を考慮し、これらの項目に適切なものを選択することで、多様な事業ドメインに適応させる。

表 5　リスク評価基準設定の例

リスク	影響小	影響中	影響大
発生確率（高）	B	A	A
発生確率（中）	C	B	A
発生確率（低）	C	C	B
発生確率（無）	C	C	C

A：リスク評価値高、B：リスク評価値中、C：リスク評価値低

表 6　発生確率設定の例

発生確率	アクセス経路	専門知識の要否	攻撃者の手間
高	遠隔（高）	不要	小
中	遠隔（高）	不要	大
中	遠隔（高）	要	小
中	隣接（中）	不要	小
低	遠隔（高）	要	大
低	隣接（中）	不要	大
低	隣接（中）	要	小
無	隣接（中）	要	大
無	ローカル（低）	考慮せず	考慮せず

アクセス経路がローカル（低）の場合、専門知識の要否、攻撃者の手間を考慮せず、発生確率を無とした。

表 7　影響度設定の例

影響度	安全	評判	事業損失
大	死亡、重症、火災	企業ブランドの風評被害	1 日以上の製造ライン停止
中	通院加療、製品発火	製品の風評被害	1 日未満の製造ライン停止
小	軽傷、発煙	−	−

3.2 脅威分析手順

提案する脅威分析の手順は、前述した「資産ベース」での詳細リスク分析の手法と大まかには共通しており、具体的には以下のようなフロー（図 1）で分析を進める。製品の事業ドメインに適合させるための仕組みは、各工程の詳細な作業を実施する際の手順として、以降の章で詳細に説明する。

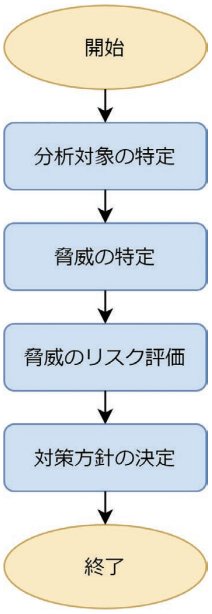


図 1　脅威分析フロー

3.2.1 分析対象の特定

システム要件などの入力文書から網羅的に資産を抽出すると分析対象が広くなり、莫大な工数がかかることとなる。分析対象の製品と利用環境を明確にすることで、保護すべき資産とその資産へのアクセス経路を明らかにする。そのために想定される利用環境をイメージし、システムの全体構成図を作成する。分析対象の製品については、保護すべき資産とそのアクセス経路についても記載し、その製品の事業ドメインで事前に定義した重要度を判断する保護資産のレベル表とアクセス経路のレベル表を用いることで、重要度の低い情報や機能、アクセス経路のフィルタリングを可能にした。図 2 の例では、機能資産であるラダープログラムデバッグ機能は表 2 のレベルで「低」、接点 I/O などのアクセス経路からのサイバー攻撃のリスクは、表 3 のレベルで「ローカル（低）」にあたると考え、対象外としている。このようにして分析対象となる保護資産とアクセス経路を洗い出す。

この場合は、デバッグ機能以外の機能と情報が分析対象の保護資産としている。また、アクセス経路としては、「LAN1」、「LAN2」、「SD カード」を分析対象としている。

3.2.2 脅威の特定

分析対象を明確にしたシステム構成図（図 2）をもとにして、それぞれの保護資産に対して、接続されるアクセス経路に着目し、表 4 のガイドワードを参考にして想定される脅威を特定する。これにより、必要最小限の組み合わせで脅威を洗い出すことができるため、分析工数を抑えて、漏れなく脅威の抽出を行うことが可能となる。

一例として、保護資産として「ファームウェア」に着目

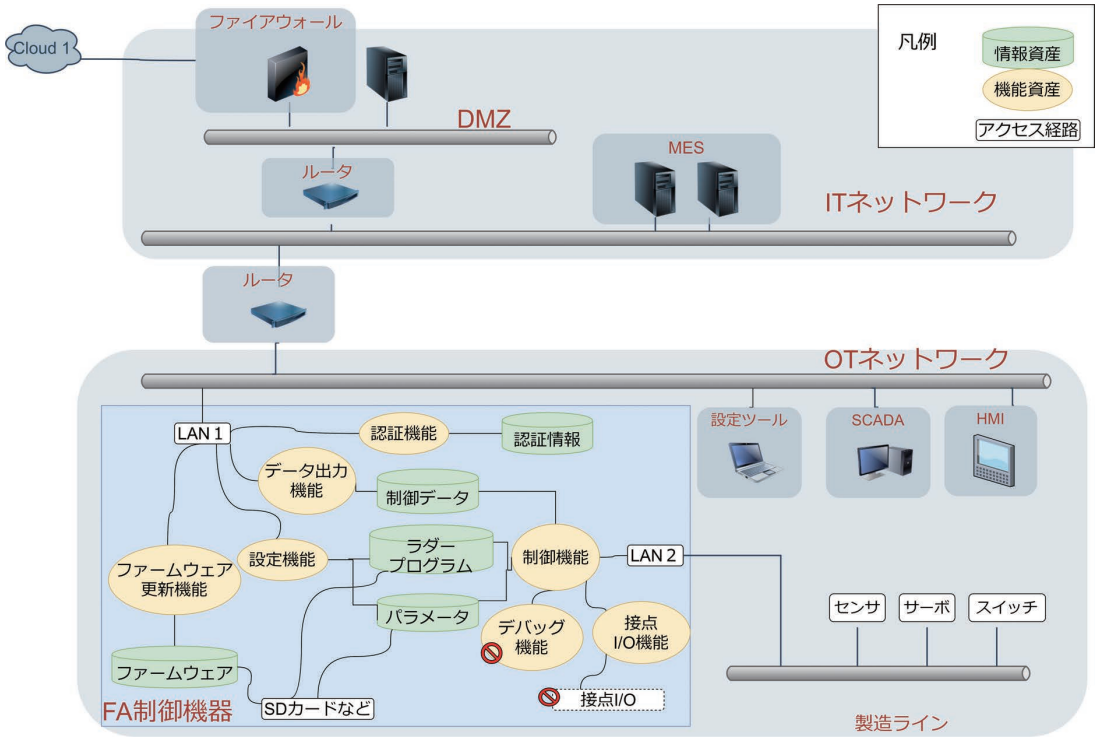


図 2　システム構成図の例（FA 制御機器の場合）

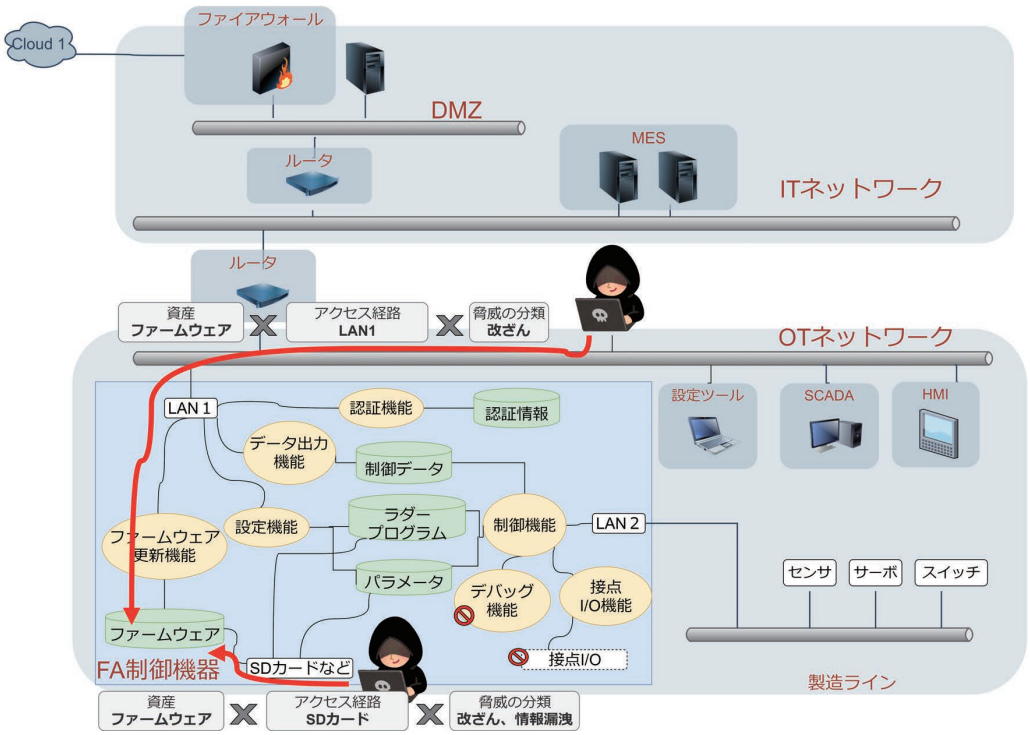


図 3　ファームウェアに着目した脅威の抽出

した場合の分析例（図3）を示す。この例では、「ファームウェア」へのアクセス可能な経路として、「LAN1」と「SD カード」がある。それぞれのアクセス経路について、ガイドワードから発生しうる脅威を記載していく。このようにして、すべての分析対象の資産に対して脅威を抽出し、脅威一覧（表 8）を作成する。

特定した脅威の検証として、「2. 製品のセキュリティ対策の着目点」で挙げた 4 つのフェーズのユースケースシナ

リオを用意し、シナリオに沿った脅威検証を行うことで、脅威の抽出漏れを確認できる。

表 8　脅威一覧の例

No.	対象資産	アクセス経路	脅威種別	脅威
1	ファームウェア	LAN1	改ざん	悪意のある第三者に、設定ツールでファームウェアを書き換えられる。
2	ファームウェア	SD カード	情報漏洩	悪意のある第三者に、SD カード経由でファームウェアを抽出される。
3	ファームウェア	SD カード	改ざん	悪意のある第三者に、SD カード経由でファームウェアを書き換えられる。
4	ラダープログラム	LAN1	改ざん	悪意のある第三者に、設定ツールでラダープログラムを書き換えられる。
5	ラダープログラム	LAN1	情報漏洩	悪意のある第三者に、設定ツールでラダープログラムを搾取される。
6	ラダープログラム	LAN1	情報漏洩	悪意のある第三者に、パケットキャプチャによりラダープログラムを搾取される。

3.2.3 脅威のリスク評価

抽出した脅威ごとに、その脅威がもたらす問題事象を列挙していく。次に、その問題事象について影響度と発生確率を表5～表7の設定に照らして、リスクを評価していく（表9）。

表 9　リスク評価の例

No.	対象資産	脅威がもたらす問題事象	影響度	発生確率の要素			発生確率	リスク評価
				アクセス経路の観点	攻撃者の専門知識の観点	攻撃者の手間の観点		
1	ファームウェア	製造ラインの長時間停止、製造品質の低下	大：事業損失	高	中	高	高	A
2	ファームウェア	PLC の設計機密の漏洩	中：事業損失	低	中	中	中	B
3	ファームウェア	製造ラインの長時間停止、製造品質の低下	大：事業損失	低	中	中	中	A
4	ラダープログラム	製造ラインの長時間停止、製造品質の低下	大：事業損失	高	中	高	高	A
5	ラダープログラム	顧客の製造データの流出	中：風評被害	高	中	高	高	A
6	ラダープログラム	顧客の製造データの流出	中：風評被害	中	低	高	中	B

3.2.4 対策方針の決定

リスク評価の結果に基づき、対策の要否を決定する。対策の要否決定は、費用対効果、対策後の残リスクをもとに判断する。そのためには、レベルの高い重要なリスクから順に対策の概要を想定していく。各リスクの対策を検討する中で、レベルの高いリスクの対策を実行することによって、他のいくつかのリスクは、個別に対策する必要がなくなる場合がある。共通の対策が有効となる脅威については、対策の検討を省略する（表 10）。これにより、対策の検討と実施の時間を節約し、効率化できる。レベルの低い保護資産については、潜在的な脆弱性とその脆弱性を突いて攻撃されるリスクのすべてを抽出、対策できる訳ではないが、これらについては発生確率と影響度を鑑みた事業リスクは低いと考えて受容し、インシデント発生時に対処を行うことにする。最終的に、実施する対策の実現性や対策後の残リスクを評価したうえで、リスク対策をまとめ、セキュリティ要件とする。

表 10　リスク対策と残リスクの例

No.	対象資産	発生確率の要素			発生確率	リスク評価	対策の要否	対策方針	残リスク
		アクセス経路の観点	専門知識の要否の観点	攻撃者の手間の観点					
1	ファームウェア	高	中	高	高	A	要	・通信暗号化 ・ユーザー認証機能	なし
2	ファームウェア	低	中	中	中	B	要	・ファームウェア暗号化	なし
3	ファームウェア	低	中	中	中	A	要	No. 2 で対策済	なし
4	ラダープログラム	高	中	高	高	A	要	No. 1 で対策済	なし
5	ラダープログラム	高	中	高	高	A	要	No. 1 で対策済	なし
6	ラダープログラム	中	低	高	中	B	要	No. 1 で対策済	なし

4. 成果・効果検証

本提案手法と資産ベースの「詳細リスク分析」のような総当りで脅威を分析しなければならない手法について、表 11 の製品について、分析が必要になる脅威パターン数を比較した（図 4）。

この図の通り、本提案手法を用いることで、保護資産の優先順位付けを行ったうえで分析を行うことで分析パターンの発散がコントロールされ、分析に必要になる脅威のパターン数は、概ね 10 分の 1 以下に削減されている。

製品 D のケースについて結果の詳細を表 12 に示す。具体的手順は以下のとおりである。製品の機密上一部詳細の記載は省略している。

表 11　検証製品の保護資産数と経路数

製品	情報資産数	機能資産数	経路数
製品 A	17	18	2
製品 B	5	1	4
製品 C	14	1	7
製品 D	7	7	5
製品 E	8	11	8
製品 F	27	1	7
製品 G	20	16	7

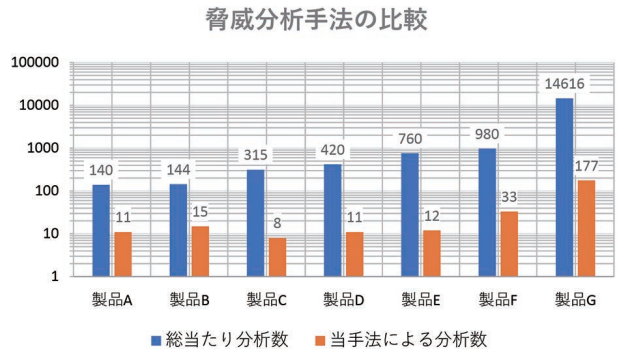


図 4　分析対象となる脅威のパターン数の比較

表 12　製品 D の脅威分析結果比較

脅威のレベル	総当たり時の脅威数	資産・経路による削減数	重複や提案手法による削減数	抽出した脅威数
高	60	0	58	2
中	240	0	143	7
低	120	120	–	2

資産レベル「低」の 2 件の脅威数は、検証により発生確率を考慮し、後工程で追加。

(1) 製品 D の 14 の資産のうち、インシデントの影響度が受容可能なレベル「低」とした 4 つの資産を分析対象外とした（表 13）。
(2) 製品 D の 5 のアクセス経路のうち、製品の設置環境の特性から困難である「機器の直接操作」と可能な攻撃のレベルが低い「シリアル通信、USB 通信」の 3 つのアクセス経路を分析の対象外とした（表 14）。
(3) 上記により、残った 20（10×2）の組み合わせに対して STRIDE の 6 つのガイドワード（表 4）により、120（20×6）パターンから攻撃手法が同じもの、資産が接続されていないアクセス経路の組み合わせを除外し、9 の脅威に絞り込んだ。
(4) 9 の脅威に対して、具体的な脅威とひき起こされる可能性のあるリスクを分析し、抽出した脅威の製品ライフサイクルにおける影響シナリオから、資産とアクセス経路の絞り込みを再度検証し、新たな脅威を 2 件追加。
(5) 最終的に抽出された 11 件の分析された脅威について、表 5 のリスク評価基準に基づいて評価を実施し、優先順位をつけて対応を行った。

表 13　製品 D の資産

影響度	資産の数	レベルの定義
高	2	死亡、重傷、個人情報の漏洩につながる可能性のある資産
中	8	ユーザや自社の金銭的な損害に繋がる可能性のある資産
低	4	軽微な情報の漏洩や誤動作の可能性がある資産

表 14　製品 D のアクセス経路

レベル	アクセス経路の数	レベルの定義
遠隔（高）	2	LAN 上で動作する通信プロトコル
隣接（中）	1	機器の直接操作
ローカル（低）	2	シリアル通信、USB 通信

上記の手順で脅威分析を行うことで、重要な資産について優先的に脅威を抽出するとともに、分析にかかる工数を削減でき、効率的な分析を可能なものにしている。

また、図 4 のグラフのデータは、FA、ヘルスケア、ソーシャルソリューション、デバイス・モジュールの製品など複数のドメインの製品の結果であり、本提案手法をこれらに適用した結果いずれも効果がみられ、多様なドメインに適用可能と考えられる。

5. むすび

本提案手法は、組込機器に適し、効率的な脅威分析手法がないという課題について、多様なドメインに適用でき、効果的な脅威分析組込機器に適した脅威分析手法として、効率面で一定の成果を上げることができた。ただ、実際のインシデントの発生は、悪意のある攻撃者の意思によって発生する確率が変化する。改善策としては、攻撃者の動機を加味した発生確率を設定することで、より具体性のある脅威の抽出につなげられると考える。

一方、本提案手法での脅威分析の手順を従来の開発手順に組み込み、製品品質の確保と製品セキュリティの確保を両立できるように、脅威分析の実施そのものを開発プロセスの一環として位置付けていく必要がある。現状は、脅威分析は一部の製品での実施となっているため、今後は、実

施の対象部門、対象製品の拡大が必要となる。また、開発プロセスの中に取り込んでいくために、開発者に対する啓蒙活動や教育も含めた展開を行っていく。

加えて、サイバー攻撃の技術やサイバー攻撃を防ぐ技術は日々進化しており、効果的、効率的な脅威分析を継続するためには、新たな技術に精通するとともに、脅威分析手法の在り方についても改善していくことが必要である。

参考文献

1）独立行政法人情報処理推進機構（IPA）．情報セキュリティ白書 2019．独立行政法人情報処理推進機構．P163.

2）Vineet Saini, Qiang Duan, Vamsi Paruchuri. “Threat Modeling Using Attack Trees”. 2008, https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees, (2020-3-1).

3）独立行政法人情報処理推進機構（IPA）技術本部セキュリティセンター．制御システムのセキュリティリスク分析ガイド第2版．2017, https://www.ipa.go.jp/files/000069436.pdf, (2020-3-1).

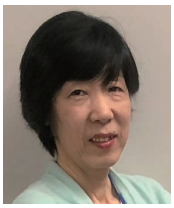
4）中野 学、堀部 千壽、小林 鉄平、松木 隆宏．システムに対する脅威分析におけるコスト及び属人性低減に向けた手法の提案．SCIS. 2018, No. 1C2-5, 8p.

5）Microsoft Corporation. “The STRIDE Threat Model”. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20). (accessed 2020-2-27)

執筆者紹介

芹川 正孝　SERIKAWA Masataka
グローバルものづくり革新本部
開発プロセス革新センタ SPILIT 推進部
専門：ソフトウェア工学

丹羽 徹　NIWA Toru
グローバルものづくり革新本部
開発プロセス革新センタ
専門：ソフトウェア工学
所属学会：電子情報通信学会



吉岡 幸恵　YOSHIKAWA Sachie
グローバルものづくり革新本部
開発プロセス革新センタ SPILIT 推進部
専門：ソフトウェア工学

原田 真太郎　HARADA Shintaro
オムロンソフトウェア株式会社
IST ソリューション事業部
プロセスエンジニアリング部
専門：ソフトウェア工学

本文に掲載の商品の名称は、各社が商標としている場合があります。