Vol.2019-DPS-178 No.4
Vol.2019-CSEC-84 No.4
2019/3/4

サイバー攻撃対策の自動選定に向けたセキュリティ分析

浅井 健志† 島邉 遼佑† 河内 清人†

概要：情報資産を取り扱う製品/システムにおけるセキュリティの重要性が増しており，これらの資産を保有する組織や企業には，十分なセキュリティ対策を実施することが求められる．一方で，今後セキュリティ専門家が不足し対策が間に合わなくなる恐れがある． そこで筆者らは，システムの設計者自身がセキュリティを適切に設計できるよう，セキュリティ分析及び対策選定を自動化することを目指している．本稿では，このうちセキュリティ分析の自動化についての検討，及び作成したプロトタイプについて報告する．

キーワード：セキュリティ分析，アタックツリー，対策選定

Security Analysis for Automated Countermeasure Selection

TAKESHI ASAI† RYOSUKE SHIMABE† KIYOTO KAWAUCHI†

The importance of security in products / systems with information assets is increasing and we have to take cybersecurity countermeasures sufficiently.But there is a risk that cybersecurity countermeasures is not taken due to lack of security experts.For this problem, we are developping the security analysis tool so that system designers themselves can design security properly.In this paper, we present the prototype of automatic security analysis tool.

Keywords: Security Analysis, Attack Tree, Cybersecurity Countermeasure Selection

1. はじめに

企業・組織に対する標的型攻撃や不正アクセスによる機密情報・個人情報の漏えいの被害が依然として報告されている．また，IoT 機器や，重要インフラなどの産業制御システム・OT システムに対するサイバー攻撃事例が増加している[1]. さらに，産業制御システムを狙ったものの中には，被害が現実のものとなれば，その影響が計り知れないようなものまで報告されている. 例えばFireEyeによると，2017 年 8 月，中東の重要インフラの産業制御システム内にある Schneider Electric 製の安全装置を不正に操作するマルウェアが検出された[2].「Triton」と名付けられたこのマルウェアは，その機能として，プログラムや機能の読み書き，安全システムコントローラとの通信・状態分析が可能で，当該コントローラの運行停止や遠隔からのリプログラミングが可能とのことである．重要インフラの制御システムにおいて，安全システムが，改ざんされて正常に動作しないとなると，事故や故障が発生したい際に，被害の拡大を止められず甚大なものとなる可能性がある．また，2017 年 6 月には，ホンダの生産工場がランサムウェア「WannaCry」によって，稼働停止することとなった[3]．これらの事例により，機器・システム / 製品を取り扱う企業や組織にとって，セキュリティを確保することは重要な課題であることが分かる．そのため，十分なセキュリティ対策の実施が求められる．

その一方で，企業におけるセキュリティ人材の不足が指摘されている．サイバーセキュリティ戦略本部は，サイバーセキュリティ人材育成プログラムの中で，次のように課題を示している.「新しい IT の利活用におけるサイバーセキュリティ対策については，(中略)，事業部門の人材が，事業そのものの企画，運用と併せてサイバーセキュリティ対策を行うことが理想的である. しかしながら, 多くの場合，(中略)事業部門をはじめとする組織においては，サイバーセキュリティに対する問題意識や理解が乏しい可能性がある．こうしたそれぞれの組織には長所，短所があり，組織の規模や事業内容にもよるが，例えば，単に一人だけ事業部門にサイバーセキュリティに詳しい人材を置くといった対応では解決しない可能性もある.」.

この課題に対するサイバーセキュリティ戦略本部の今後の取組み方針として「さらに，サイバーセキュリティの基礎知識を前提として，経営戦略や法令等による要求，業務の実態，予算・人材等による制約条件などに照らし，最も有効かつ実施可能なセキュリティ対策を考えられるよう，各部門の業務（業務そのものだけでなく，業務によって生み出される製品・サービスを含む）について分析を行った上で，サイバーセキュリティの視点を含めたリスクアセスメントができる人材育成を行うことが必要である.」としている．

一方当社においても，人材育成とは別のアプローチでセ

キュリティ人材不足の課題に取り組んでいる．当社では，特に開発を担う事業部門の担当者を対象に,担当する機器・システムのリスクアセスメント，有効なセキュリティ対策の選定・実装を，効率的に実施できるようするための仕組みづくりの検討・開発を行っている．より具体的には，対象とする機器やシステムの開発成果物(システム構成図，フローチャート，ソースコードなど)を基に，セキュリティ分析，セキュリティ対策の選定，ソースコードへの反映を自動で行うというものである．本稿では、このうちセキュリティ分析に関し，分析を支援するためのツールのプロトタイプを作成したので，その報告をする．

以降，2 章セキュリティ分析の手法及び関連研究を述べ，3 章で実装したセキュリティ分析ツールについて述べる．4 章でプロトタイプを用いた試行について述べ，5 章で考察し，6 章で本稿のまとめを行う．

2. セキュリティ分析の手法

2.1 分析手法の種類

セキュリティ分析は，対象の製品/システムの構成やデータフローから，当該システムに潜在するセキュリティ上の脅威やそのリスクを特定する技術である．製品/システムの開発者や運用する組織は，セキュリティ分析により特定した脅威に対し，事前に対策を講じることで，将来発生する可能性のあるサイバー攻撃に備えることができる．セキュリティ分析の手法は，様々なものが提案されており，IPA によるセキュリティ分析のガイド[5]では，ベースラインアプローチ，非形式的アプローチ，詳細リスク分析，組み合わせアプローチ等の手法がある．なお，[5]は制御システム向けのセキュリティ分析ガイドであるが，掲載されている手法自体は，適用対象を制御システムに制限するものではない．それぞれの手法概要は，以下の通りである．

- ベースラインアプローチ：

既存の標準や基準をもとに，予め一定のセキュリティレベル及び対策の要件を設定し、対象システムの適合度をチェックする

- 非形式的アプローチ：

組織や担当者の経験や判断によって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に合わせて，資産や避けるべき事業の被害を定義し，重要度や発生確率を基に評価する

- 組み合わせアプローチ：

複数のアプローチを併用することで、分析精度の向上，作業の効率化が図れる

また表 1 に，それぞれの分析手法の長所/短所を示す．中でも詳細リスク分析は，分析対象の実態に沿った分析を行うことで，他の手法に比べ，より正確・定量的な分析が可能である．我々の対象とする機器・システムの開発においては，1 章で示したように十分なセキュリティ対策を実施する必要があるため，以降では，詳細リスク分析及びその組み合わせアプローチを対象とする．

詳細リスク分析は，さらに資産ベースの分析，シナリオベースの分析がありそれぞれの手法概要は，以下の通り．

- 資産ベース：

保護すべきシステムを構成する資産を対象に，各資産に対して、その重要度，想定される脅威，脆弱性の３つを評価指標として、リスク値を評価する

- シナリオベース：

保護すべきシステムが実現する事業やサービスに対し，回避したい被害を定義し，被害が発生した際のレベル，アタックシナリオ，脆弱性の 3 つを評価指標として、リスク値を評価する．また，表 2 に手法の長所/短所を示す．なお，[5]ではシナリオベースの分析を，フォルトツリー解析(FTA)と攻撃ツリー解析(ATA)に分類している．

表 1 各種セキュリティ分析手法([5]からの一部抜粋)

手法名	長所	短所
ベースラインアプローチ	チェックリストやアンケートの活用により，作業工数は大きくない.	既存の基準を参照するため，自組織に適合しない場合がある(対策に過不足が生じる可能性あり)
非形式的アプローチ	分析者の経験に依存するが，作業工数は大きくない	属人的であり，分析の抜け漏れが発生する可能性あり
詳細リスク分析	自組織や自組織の開発する機器・システムに対する正確・定量的な分析が可能	システムの規模や手法により，作業工数が膨大になりがち
組み合わせアプローチ	各手法の長所の利用，短所の改善が期待できる	どの手法をどのように組み合わせるかの基準が定まっていない

表 2 詳細リスク分析の手法([5]からの一部抜粋)

手法名	長所	短所
資産ベース	システム資産を構成する各要素に対する一次（初段）の脅威は網羅的に洗い出すことができる	資産の要素間を渡って被害を及ぼす攻撃を追跡することは困難である
シナリオベース	システムに対する攻撃の入口を網羅して、最終被害を引き起こす攻撃の連鎖を追跡することができる.サイバー攻撃による被害を分析するには、想定しうる攻撃のステップを追跡するアプローチが自然である.	システムの構成や攻撃ツリーの作り方等によるが，攻撃ツリーの数が増大して，分析工数が膨大になる

被害が発生する攻撃対象から遡ってその原因を追究し，攻撃を行う拠点までを明らかにする分析を FTA 的アプローチ，また，攻撃の拠点までにいかにして辿り着くかを明らかにする分析を ATA 的アプローチとし，それら分析のアウトプットを統合したものを攻撃ツリーとしているが，本稿では，被害を発生させる攻撃活動を，攻撃対象から，攻撃の拠点，侵入口まで一貫して遡って特定する分析をアタックツリー分析，またその成果物をアタックツリーと呼ぶこととする．

2.2 本研究における分析手法

本研究では，2.1 に示した分析手法のうち，資産ベースの詳細リスク分析とシナリオベースの詳細リスク分析(アタックツリー分析)の組み合わせアプローチを採用しプロトタイプを作成した．その理由は，次の要件を満たすと考えたためである．

1. 開発部門の担当者が効率的に分析を実施できること
2. 開発部門の担当者が網羅的に分析を実施できること

製品開発プロセスの設計において，資産は必ず検討される一方で，好ましくない事象は，必ずしも検討されるわけではない．そこで，設計の開発成果物を流用して資産ベースの分析を行えば，分析が効率化され 1 を満たす．また，表 2 にあるように，脅威を網羅的に特定することが出来るため，2 を部分的に満たしている．一方で，システムを構成する要素間に渡る分析ができないため，その点においては 2 を満たしていない．そこで欠点を補うべく，資産ベースの分析で特定した脅威を引き起こす攻撃を，シナリオベースの分析で特定する(図 1 参照)．シナリオベースの分析を取り入れたことで，分析工数が増大し 1 を満たさなくなることが想定される．そこで，本研究では，分析を自動で実施するためのツールの実現することで，1, 2 を同時に満たす分析の実現を試みた．

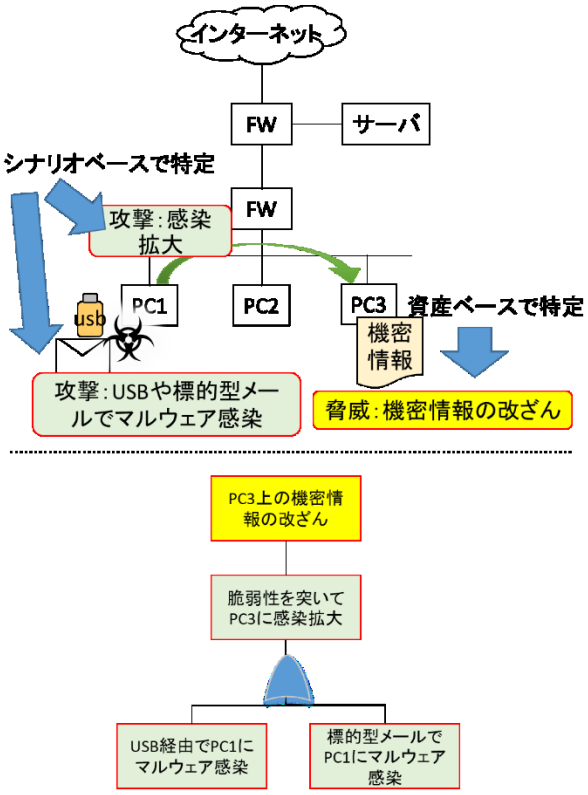

図 1 資産ベースとシナリオベースで特定する脅威・攻撃(上図)と対応するアタックツリー(下図)

ここで，本研究でのアタックツリー分析について補足する．本研究では，分析で出力するアタックツリー内の攻撃活動は，MITRE の策定する CAPEC(Common Attack Pattern Enumeration and Classification．共通攻撃パターン一覧)を使用して表現した．これは，攻撃方法の種類を一意に識別するために体系化・整理したものである．さらに，CAPEC で定義された攻撃パターンには，それぞれ関連する脆弱性として CWE の脆弱性が紐付いている．そこで，アタックツリーに対する付加情報として，アタックシナリオ毎に関連する脆弱性一覧も出力するようにした．セキュリティ対策の選定・実装は，この CWE を基に行う．詳細は，参考文献[6]～[9]を参照されたい．

3. 対策の自動選定に向けたセキュリティ分析ツール

2.2 で示した，セキュリティ分析ツールについて説明する．先ず，3.1 ツールの構成を概説し，3.2 でツールへ入力するシステム構成情報を説明し，3.3 で脅威及びアタックシナリオの設定について，3.3 でシナリオの生成方式について説明する．

3.1 構成の概要

セキュリティ分析ツールの構成は，以下のデータ，及び，機能からなる(図 3 参照)．また，実装にあたっては，Excel VBA, Python と，特に推論機能に対して論理型プログラミング言語 Prolog を使用した．

- 入力データ
  - システム構成情報：
    分析対象のシステムの情報（構成要素，情報資産，ネットワークトポロジ，登場人物）示すデータ．シ

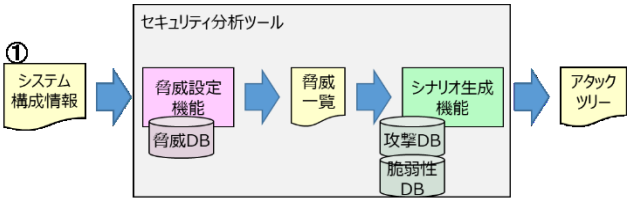

図 2 セキュリティ分析ツール構成概略

ステム開発者または分析者が，Microsoft の Visio ファイルとして作成する．

- 分析機能
  - 脅威設定機能：
    入力として与えられたシステム構成情報と，脅威 DB に登録された脅威を基に，対象システムで起こり得る脅威を具体化する機能．
  - 脅威 DB：
    攻撃者の達成したい最終目標(脅威)を，テンプレートとしてリスト化し保持したもの．「なりすまし」や「不正アクセス」等，脅威のカテゴリ毎に細分化しまとめられている．
  - アタックシナリオ生成機能：
    入力として与えられたシステム構成情報と，脅威設定機能が具体化した対象システム上での脅威，及び攻撃 DB に登録された攻撃手法を基に，対象システム内で，攻撃者が行う一連の活動(アタックシナリオ)を導出する機能．
  - 攻撃 DB：
    攻撃者の行う攻撃活動をリスト化し保持したもの．各攻撃活動は，MITER 社の定める APEC(Common Attack Pattern Enumeration and Classification：共通攻撃パターン一覧)を利用した．また，各攻撃活動同士の依存関係を攻撃ルールとして保持している．
  - 脆弱性 DB：
    アタックメソッドを導出する際に参照する情報．既知の脆弱性を含むプログラム名，バージョン，及び，脆弱性の種別が記述される．

- 出力データ
  - アタックツリー：
    分析機能が抽出した脅威及びアタックシナリオを統合し，アタックツリーとして出力したもの．Excel や XML ファイルとして出力される．

3.2 システム構成情報

分析ツールへと入力する，システム構成，及び，データフローは，Microsoft Visio を用いて表現する．これは，システム・機器の開発の設計段階において検討したものを流用できる．図 3 にサンプルの分析対象のシステムを示す．シート上の四角オブジェクトは，システムや機器を構成する装置等の要素，コネクタオブジェクトは，それら要素をつなぐ通信路，また，矢印オブジェクトは，データフローを表している．各オブジェクトは，それぞれ固有の属性データを保持しており，例えば，四角オブジェクトであれば，種別や搭載されているソフトウェア名称，セキュリティ機能等を入力することが出来る．属性は，入力必須のものと必須ではないものがある．

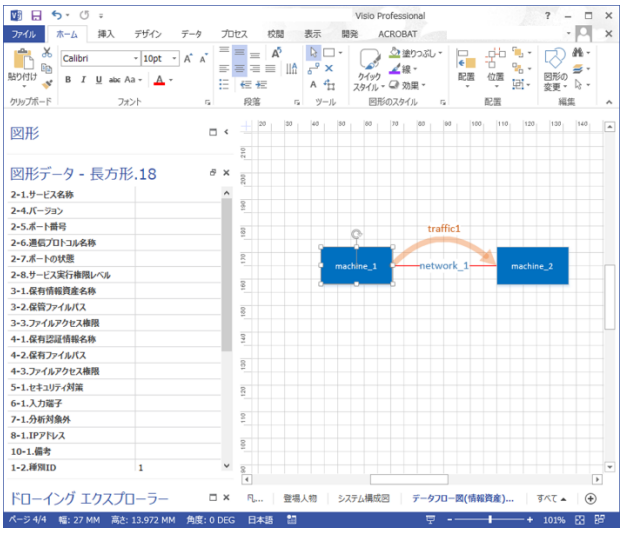

図 3 システム構成情報を示す Visio ファイル

3.3 分析

3.3.1 脅威の設定

脅威の設定は以下のようにして行う．先ず，入力として与えられた Visio ファイル(システム構成情報とデータフロー)から，対象を構成する全ての要素及び，要素同士の接続関係や，情報資産の存在する位置等を取得する．次に，各要素情上に存在する情報資産に対して，想定される脅威を特定する．想定される脅威は，脅威 DB(表 3 参照)に格納されたテンプレートとしての脅威から自動で選択される．テンプレートしての脅威の選択は，要素の種別に応じて選択される．例えば，対象の要素が PC ならば，脅威 DB 上で PC 用に定義された脅威を全て選択することで行う．最後に，対象機器の要素に応じて，テンプレートの脅威を具体化する．例えば，表 3 には通信路に対する脅威として，「[装置]からの意図的な回線過負荷」が登録されているが，[装置]には，対象のシステム構成図上の要素名が入力されることで具体化を行う．

表 3 脅威 DB の抜粋

脅威	種別		
	PC	通信路	…
偽メッセージの送信による改ざん	1	-	…
[装置]からの意図的な回線過負荷	-	1	…
…	…	…	…

3.3.2 シナリオの生成

アタックシナリオの導出には，論理型プログラミング言語 Prolog を採用した．Prolog は，事実，規則，質問の 3 要素からなり，一階述語論理を用いて再帰的なパターンマッ

Vol.2019-DPS-178 No.4
Vol.2019-CSEC-84 No.4
2019/3/4

チングを行うことで，与えられた質問の真偽，又は，解を推論する機能を持つ．上述した，再帰的なパターンマッチングの過程が，そのまま，攻撃者の攻撃活動の時系列(を逆に辿ったもの)と捉えることが出来る．システム構成情報や脆弱性情報を事実，攻撃ルールが規則，脅威リストが質問に相当する．事実，規則，質問はいずれも述語と変数を用いて表現され，以下の形式を取る．

述語(引数 1，引数 2，・・・)

という形式を取る．以下は，事実，規則，質問の形式と本研究で用いた例である．

- 事実：
  形式：述語(引数 1，引数 2，・・・).
  物事の事実の定義．本稿では，システム構成情報，及び、脆弱性情報．
  - 例．対象システム内に，userMachine1 という要素が存在し，Windows XP(日本語)という OS が搭載されている．
    hasProgram(userMachine,windowsXP,sp-japanese).
  - 例．windowsXP(日本語版)には，任意コード実行が可能となる脆弱性 CVE-2008-4250 が存在する．
    vulReport(windowsXP,sp-japanese,'CVE-2008-4250',execCode).

- 規則：
  形式：述語(引数 1，引数 2，・・・) :- 述語(引数 1，引数 2，・・・)，述語(引数 1，引数 2，・・・).
  複数の事実の関係の定義．右辺の事実が全て成立した場合に，左辺の事実が成立するという関係を示す．本稿では，攻撃ルール．
  - 例．対象 Machine 内の情報資産 Data に対し，権限 Priv で操作種別 Type が許可されており，攻撃者 Attacker が，対象 Machine 上で権限 Priv でアクセス可能な情報資産 Data を発見した時は，攻撃者がその情報資産 Data に対して操作種別 Type で情報の改ざんが可能．
    informationTampering (Attacker,Type,Data):-
    allowAction(Machine,Data,Type,Priv),
    dataDiscovery(Attacker,Machine,Data,Priv).
  但し，大文字で始まる単語は自由変数を表し，事実で定義されている引数が代入される．

- 質問：
  形式：?- 述語(引数 1，引数 2，・・・).
  事実の関係に対する質問．本稿では，脅威の成立可否に対する質問．

要素名	情報資産	搭載 SW	SWver	SW 権限
machine_1	data	machine_sw	指定なし	指定なし
machine_2	data	machine_sw	指定なし	指定なし
machine_3	-	-	-	-
machine_4	-	-	-	-

- 例．攻撃者 attacker は，情報資産 clientData を改ざん(削除 delete)可能か？
  ?- informationTampering (attacker, delete, 'clientData.csv').

Prolog は，先ず質問として与えられた脅威を与えられた攻撃ルールの中から探索する．次に，その脅威を左辺に持つ攻撃ルールの右辺の成立可否を問う．これは，上記と同様に攻撃ルールの中から探索を行い，さらにその右辺の成立可否を問う．このように，繰り返し攻撃ルールの右辺の成立可否を問い，最終的に，定義した事実と一致した場合には，これまでの成立可否は全て真であると判定する． 判定結果が真であった場合は，脅威から事実までの推論過程を，攻撃者の攻撃活動と見なし，アタックツリーにおけるアタックメソッドとする．

表 4　攻撃 DB の抜粋

攻撃手法	関連する脆弱性
ブルートフォース攻撃 (CAPEC 112)	・不十分な強度の暗号を使用 (CWE 326)
マルウェアのダウンロード (CAPEC 185)	・ダウンロードしたコードの完全性を検証しない(CWE 494)
…	…

4. 試行

簡易的なターゲットシステムを考え，作成したプロトタイプに適用し，脅威，及び，それを実現するためのアタックシナリオの自動生成を試行した．ターゲットシステムには，4 台の装置 machine1～machine4 が存在し，それぞれ通信路 network_1～network_3 を通じて，のように接続されている．また表 5 は，ターゲットシステム上の構成要素の主な属性情報である．図 4，表 5 から分かるように，

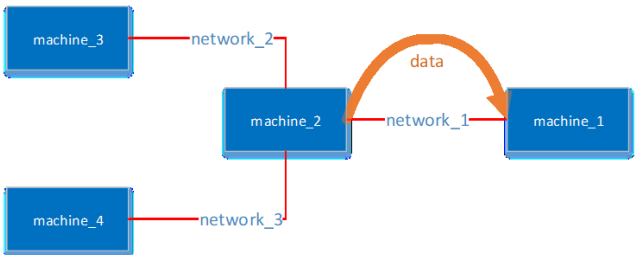

図 4 ターゲットシステム

表 5 ターゲットシステムの構成要素の主な属性情報

machine_2 上の情報資産 data が，通信路 network_1 を介して machine_1 へと送信されている．machine_1, machine_2 には，machine_sw というソフトウェアが搭載されており，本ソフトウェアが data を使用している．

セキュリティ分析ツールは，システム構成情報と脅威 DB から，自動で対象システムの脅威，即ち，攻撃者の最終目標を特定し出力する．引き続き，出力した脅威と攻撃 DB から，攻撃の成功可否を推論することで，自動で脅威を実現するために必要な攻撃活動の列，即ち，アタックシナリオを出力する．表 6 は，分析で得られた脅威，及び，そのアタックシナリオを Excel ファイルとして出力したものの一部である．ここで，攻撃者の最終目標である脅威は，「想定外のデータ入力による誤動作」である．これを実現するために，①攻撃者により USB 経由で machine_3 に感染したマルウェアが，②machine_2 の machine_sw の脆弱性を突いて権限を奪取し，③network_1 を盗聴・認証情報を取得後，④⑤machine_1 上の machine_sw に対して不正通信を送信し，⑥machine_1 上の machine_sw が誤動作する＝脅威，というシナリオが導出されていることが分かる(参照)．なお，表 5 に示した通り，今回の試行では，machine_1, machine_2 の搭載 SW のバージョンや権限レベルを指定していない．このような場合，分析ツールは攻撃の成功可否の推論において，任意の変数として扱う．これは，分析ツールが安全サイドに倒した分析を行うことを意味している．今回の場合だと，machine_sw は，脆弱性が存在するバージョンのものを使用

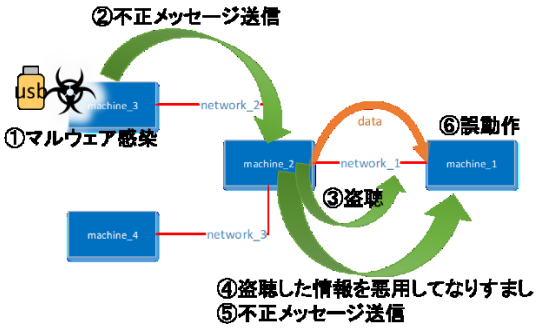

図 5 ターゲットシステムに対する脅威，及び，アタックシナリオの説明図

している，また権限においては，その攻撃を実行するに必要な権限を得ている，と判断し分析する．

5. 考察

5.1 事業部門の担当者を対象としたセキュリティ分析の結果

今回，事業部門の担当者がセキュリティ分析を実施することを想定し，効率的且つ網羅的な分析を行えるよう，脅威およびアタックシナリオを自動で特定するツールのプロトタイプを作成した．4 では，事業部門の担当者が，自身の担当する機器・システムの設計情報を，システム構成情報(Visio ファイル)として用意するだけで，セキュリティ分析が実施され，アタックツリーを得ることができた．

表 6 ターゲットシステムに対する脅威，及び，アタックシナリオの抜粋

シナリオ ID	ノード種別	攻撃活動(CAPEC)	攻撃活動(内容)	関連する脆弱性(CWE)	…
①	AM	maliciousLogicInsertion(attacker,machine_3,usb)	[攻撃者=attacker]が、[攻撃先装置=machine_3]の[入力端子=usb]へ不正な端末を挿入し、[攻撃先装置=machine_3]をマルウェア感染させる	-	…
②	AM	codeInjection(malware,machine_3,machine_2,machine_sw,_4722)	[攻撃者=malware]が、[攻撃元装置=machine_3]から[攻撃先装置=machine_2]の[サービス=machine_sw]へ不正なコードを送信し、[権限レベル=_4722]で操作する	74	…
③	AM	interception(malware,machine_2,network_1,traffic1)	[攻撃者=malware]が、[攻撃元装置=machine_2]から[ネットワーク=network_1]を盗聴し、[認証情報=traffic1]を取得する	200	…
④	AM	identitySpoofing(malware,machine_2,machine_1,machine_sw)	[攻撃者=malware]が、[攻撃元装置=machine_2]から[攻撃先装置=machine_1]の[サービス=machine_sw]に対して、窃盗したセッション ID を再利用してセッションを開始する	6,290, 302, 346, 384, 539, 602, 642, 664	…
⑤	AM	trafficInjection(malware,machine_2,machine_1,machine_sw)	[攻撃者=malware]が、[攻撃元装置=machine_2]から[攻撃先装置=machine_1]の[サービス=machine_sw]へ不正なメッセージを送信する	-	…
⑥	AG	unexpectedMalfanctioning(malware,machine_1,machine_sw)	[攻撃者=malware]によって、[攻撃先装置=machine_1]の[サービス=machine_sw]が誤動作する	-	…

これにより，担当者の分析にかかる作業工数は，削減できたといえる．一方で，分析結果の網羅性に関しては，分析ツールの利用する各種 DB の網羅性に帰着することになる．

5.2 各種 DB のアップデート

今回作成したプロトタイプでは，脅威及びアタックシナリオを特定するために，各種 DB(脅威 DB，攻撃 DB，脆弱性 DB)を利用した．これらは，日々新しい情報が報告されるため, 最新の攻撃事例や攻撃手法を分析に適用するには，高頻繁で調査・DB のアップデートを行う必要がある．今回作成したプロトタイプでは，各種 DB は全て人手で行っているため，上記作業は非常に作業負荷が高いと言える．そのため，今後は各種 DB のアップデートを自動もしくは支援するための仕組みが必要と考える．

6. まとめ

本研究では，サイバー攻撃対策の自動選定に向けて，自動で対象機器・システムの脅威を抽出し，さらにその脅威に至るアタックシナリオを導出するツールのプロトタイプを作成した．自動生成で得られるアタックツリーには，各攻撃活動で悪用される脆弱性(CWE)を含む．対策の選定及び実装は, CAPEC で表現された攻撃活動及び脆弱性を入力として行う．今後は，対策選定，実装機能を作成と性能評価を行う予定である．

参考文献

[1] シマンテック・コーポレーション, “ISTR インターネットセキュリティ脅威レポート 第 23 号”, 2018
[2] “産業制御システム（ICS）への新たな攻撃フレームワーク「TRITON」が重要インフラの運用停止を誘発”. https://www.fireeye.jp/company/press-releases/2017/attackers-deploy-new-ics-attack-framework-triton.html, (参照 2019-01-25)
[3] “ホンダの工場がランサムウェアの被害に、狙われたのは生産ライン制御の PC”. http://monoist.atmarkit.co.jp/mn/articles/1706/23/news029.html, (参照 2019-01-25)
[4] サイバーセキュリティ戦略本部, “サイバーセキュリティ人材育成プログラム”, 2017
[5] IPA, “制御システムのセキュリティリスク分析ガイド第 2 版”, 2018
[6]市川 幸宏, 中井 綱人, 清水 孝一, 植田 武, 日夏 俊, 浅井 健志, 小林 信博"脅威分析による対策を標準要件で分類するセキュリティ機能分類方式の提案", SCIS2018, 2018
[7]植田 武, 清水 孝一, 日夏 俊, 中井 綱人, 市川 幸宏, 浅井 健志, 小林 信博"設計モデルを用いたセキュリティ脆弱性分析方法", SCIS2018, 2018
[8]清水 孝一, 植田 武, 市川 幸宏, 中井 綱人, 日夏 俊, 浅井 健志, 小林 信博, ブノワ・ボワイエ, ダヴィド・モントレ, "ステートマシンで表した動作モデルを用いた脆弱性の特定", SCIS2018, 2018
[9]日夏 俊, 清水 孝一, 植田 武, 市川 幸宏, 中井 綱人, 小林 信博, "モデルベース開発技術を利用したセキュリティ機能導入パターン生成", SCIS2018, 2018