工場システムにおける APT 攻撃に注目した セキュリティリスク数値化手法の検討

川西康之 [123a)]　西原秀明 [1]　吉田博隆 [1]　加藤勇夫 [12]　井上博之 [13]

概要：工場への IT 導入による製品製造の効率化や製品管理が進む一方で，サイバー攻撃に対するセキュリティリスクも問題となりつつある．工場システムは個別の目的に合わせ特注され，外部から具体的なシステム構成や資産が分かりにくいという特徴がある．しかし，近年 APT(Advanced Persistent Threat)攻撃と呼ばれる，高度な技術を用いた持続的な調査に基づきシステムを分析し攻撃を実施するサイバー攻撃により重要インフラ施設の重要な資産が損なわれる事例が起きており，工場システムにおいてもそのリスクを評価し対策を行うことが喫緊の課題である．本論文では脅威分析におけるリスク数値化手法に着目し，APT 攻撃の特徴をもとにリスク数値化手法を定め，その実効性を検討する．そして実機と机上の 2 つのケーススタディを通じ，工場システムにおける APT 攻撃のリスクについて考察した．検討の結果，リスク数値化手法で APT 攻撃を評価するメトリックの選定についての目処は立ったが，それらの評価基準をどう定めるかについては検討の余地があることが分かった．

キーワード：工場セキュリティ，APT 攻撃，セキュリティ設計，リスク数値化，CVSS，CWSS

A Study on Security Risk Quantification Methods Focusing on APT Attacks in Factory Systems

YASUYUKI KAWANISHI[123a)]　HIDEAKI NISHIHARA[1]
HIROTAKA YOSHIDA[1]　ISAO KATO[12]　HIROYUKI INOUE[13]

Abstract: While the introduction of IT into factories has led to greater efficiency in manufacturing and improved product management, security risks from cyber attacks are also becoming an issue. Factory systems are typically custom-made for specific purposes, and the system configuration and assets are difficult to know from the outside. However, in recent years, there have been cases of important assets at critical infrastructure facilities being damaged by cyber attacks known as APT (Advanced Persistent Threat) attacks, which involve continuous investigation using advanced technology to analyze and attack systems. As a result, it is now urgent to assess the risk to factory systems and take measures. In this paper, we focus on risk quantification methods in threat analysis, define a risk quantification method based on the characteristics of APT attacks, and examine its effectiveness. We then considered the risk of APT attacks in factory systems through two case studies, one on actual equipment and one on a desk. As a result of the study, we were able to make progress in selecting metrics to evaluate APT attacks using risk quantification methods, but we found that there is still room for further consideration regarding how to define these evaluation criteria.

Keywords: Factory security, APT attacks, security design, risk quantification, CVSS, CWSS

1. はじめに

工場への IT 導入による製造の効率化や製品管理，通信を介した複数の工場の統合管理が進み，工場はより大規模なサイバーフィジカルシステムへと変貌を遂げつつある．その一方で，2010 年のマルウェア Stuxnet[1]による物理的な被害を伴うサイバー攻撃が現実のものとなり，セキュリティリスクへの対応も喫緊の課題となっている．

その一方で工場システムは，運用する企業や組織がそれぞれ用途に合わせてシステムを組み上げるものであり，基本的にはひとつひとつが特注品，同じものはないというものである．同様のサイバーフィジカルシステムである自動車システム等は世の中に同型モデルが数万台存在し，車両を合法的に購入することでのリバースエンジニアリングが可能であるのに対し，工場システムの場合は実際に侵入してみて手探りで攻撃目標を探索する必要がある．そのため工場システムへの攻撃を行う場合，以下の事項を考慮する必要がある．

- 自動車システムのように，購入等で複数のサンプルを用意できるシステムと異なり，リバースエンジニアリングによる事前の分析がほぼ不可能である．
- 侵入後，攻撃目標と手段を模索するために，長期に渡る潜伏および情報収集が必要になるケースがある．そして発覚を遅らせ，十分な情報を得るまでの時間を稼ぐために，活動の高い秘匿性が求められる．
- 水飲み場攻撃やフィッシングメール攻撃等，ソーシャルエンジニアリングを用いて内部利用者の過失

1　(国研) 産業技術総合研究所 住友電工―産総研サイバーセキュリティ連携研究室，〒563-8577 大阪府池田市緑丘 1-8-31, SEI-AIST Cyber Security Cooperative Research Laboratory, AIST, 1-8-31 Midorigaoka, Ikeda, Osaka 563-8577.
2　住友電気工業株式会社，〒541-0041 大阪府大阪市中央区北浜 4-5-33, Sumitomo Electric Industries, Ltd., 4-5-33 Kitahama, Chuo-ku, Osaka, Osaka 541-0041, Japan.
3　京都産業大学 情報理工学部，〒603-8555 京都府京都市北区上賀茂本山, Faculty of Information Science and Engineering, Kyoto Sangyo University, Motoyama, Kamigamo, Kita-ku, Kyoto, 603-8555, Japan.
a)　kawanishi.yasuyuki@aist.go.jp

を利用することが求められる．

さて近年，システムに侵入して収集した情報から作戦を立て，様々な攻撃手段を駆使してシステムに深く浸透し，工場設備の制御機能などの最深部にある重要資産を狙う攻撃が見られるようになった．このような攻撃はAPT (Advanced Persistent Threat)攻撃と呼ばれており，重要インフラ施設や工場システムに対する攻撃のひとつとして認識されている．例えば2015年から2016年にかけてウクライナの電力グリッドに行われた攻撃事例[2][3][4]が挙げられる．そして脅威分析・リスクアセスメント(Threat Analysis and Risk Assessment: TARA)手順において脅威の持つリスクを評価する際，従来このような攻撃は十分考慮されていなかった．

本論文では，上記TARAにおけるリスクの重要度の可視化に使用するリスク数値化手法に着目し，その観点からAPT攻撃の特徴について述べ，それらを評価するのに必要なメトリックについて言及する．そして従来の手法に代わりAPT攻撃を評価できるリスク数値化手法を定め，その実効性を検討する．さらに，2015年のウクライナの発電グリッドにおけるBlackEnergy3(BE3)の攻撃事例を元に構築した，評価用工場模擬システムでの攻撃シミュレーションおよび工場システムモデルを用いた机上分析の2つのケーススタディを通じ，APT攻撃の脅威としての評価手法における課題を考察する．

第二章で準備を行う．第三章では本論文の目的，アプローチおよび貢献について述べる．第四章ではケーススタディを通じて行ったAPT攻撃の評価結果と今後の課題について述べる．最後に第五章で結論を示す．

2. 準備

2.1 APT(Advanced Persistent Threat)攻撃

APT攻撃は，文字通り「高度な持続的脅威」をもたらす攻撃である．重要インフラ施設等の高度にセキュリティで守られているシステムに対し，侵入・潜伏・情報収集を行うことで，システムの重要な資産に対する攻撃を成功させる洗練されかつ組織的な攻撃である．文献[2]によると，APT攻撃は相当数のリソースを有する組織化された攻撃者によって実行され，長期間に渡り標的システムに適応し，攻撃を成功させるものとして言及されている．

2010年のStuxnetによるイランの核施設への攻撃，2015年のBlackEnergy3(BE3)や2016年のCrashOverrideによるウクライナ発電グリッドに対する攻撃等，主に重要インフラシステムの停止・破壊をもたらした攻撃が挙げられる．図1は2015年にウクライナの発電グリッドに対しBE3が起こしたAPT攻撃の事例[2]であるが，フィッシングメールによる企業ネットワークへの侵入からWindows Active Directoryサーバの信頼情報窃取を通じ，リモート管理者用に設けられていたVPN回線に正規に接続することでOT(Operational Technology)エリアへ侵入し，潜入を秘匿しつつ情報収集を行い，最終的に発電回路のリレーを司るRTU(Remote Terminal Unit)の制御掌握を実現している．この一連の攻撃は図1の手順③～⑬に示されている．

近年の製造業の工場もIT技術の導入が進められているため，ネットワーク構成や資産の重要性は重要インフラ施設のそれと同様になりつつある．従って侵入から攻撃の実施までの手順は同様であり，APT攻撃は工場システムでも十分起こり得ると考えられ，早急な対策が求められる．

APT攻撃の事例を見る限り，その攻撃は時にはソーシャルエンジニアリングを利用する等システム内外に対する様々な手段によるアプローチを組合せたものであり，攻撃目標だけ定めるがその過程は潜伏中に収集した情報を元に時間をかけつつ臨機応変に実施されている．これは個々の企業に合わせカスタマイズされている上に外部から入口や内部構成の把握が不明という，重要インフラ施設や工場といったシステムの事情があると言える．自動車システムのように世界に数千台数万台同じモデルが存在し，なおかつ購入してシステム内部をリバースエンジニアリングで解析できるものとは前提が異なるシステムである．このようなAPT攻撃のリスク評価が本論文の課題である．

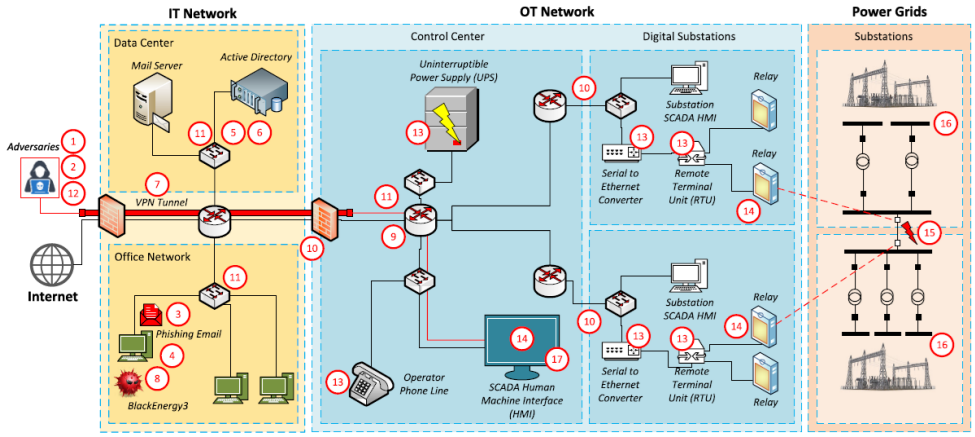

図1　2015年ウクライナでのAPT攻撃事例[2].

Figure 1　APT attack case in Ukraine in 2015[2].

2.2 脅威分析・リスクアセスメント

脅威分析・リスクアセスメント(Threat Analysis and Risk Assessment: TARA)は，主に初期のシステム設計段階，セキュリティ設計を行うフェーズで実施される手順である．

TARA は，工場等の産業制御システム向けのセキュリティ標準である ISA/IEC 62443-3-2[5], 自動車システム向けの標準 ISO/SAE 21434[6]等で定義されている．TARA の手順は以下のような 5 つのフェーズにまとめることが出来，脅威の特定とそのリスクの評価が実施され，対策が検討された後，セキュリティ標準に定義された要件が選定される．

1. **アイテム定義:** 評価対象のシステムのモデル化と資産の定義を行う. 実際のシステムもしくは設計段階の仕様書を元に, ある程度抽象化されたデータフロー図を作成し, 資産に相当する機能と情報の内容とそれらの所在を明らかにする．
2. **脅威の抽出:** 脅威シナリオを作成する．誰がいつどこからどの場所の資産を攻撃し, その結果資産がどうなるかについて要点を押さえた記述を行う(5W 法).
3. **リスク評価:** 脅威シナリオに基づき，後述するリスク数値化手法のメトリックに沿った観点でリスクを評価し数値化する. また脅威を実現する攻撃が成功する要因を攻撃ツリー分析等で分析する．
4. **対応検討:** リスクにどう対応するかを決定する．リスクを下げるために, 攻撃の成功要因に対する緩和策を検討する．また保険をかける等リスクを外注する，軽微なリスクは受け入れる等の判断も行う．
5. **セキュリティ要件の選定:** 立案した緩和策について，セキュリティ標準に示されたセキュリティ要件のどれが適用されるかを判定する. またその緩和策をどのように実装するか，技術的な要件(TCR: Technical Cybersecurity Requirement)にブレークダウンする．

2.3 リスク数値化手法

リスク数値化における代表的な従来手法は，大きな流れとして CVSS と Attack Potential の 2 つがある．また CVSS と近い手法で CWSS があり，本節ではこれら 3 つの手法について説明する．本論文で用いる手法は 3 番目の CWSS をベースとしたもので，3 章で詳細を説明する．そして 4 章のケーススタディで CVSS と分析結果を比較する．

2.3.1 CVSS (Common Vulnerability Scoring System)

CVSS は，産業制御システム分野を含む，サイバーフィジカルシステムのリスク分析でよく用いられている，脆弱性評価基準の 1 つである. 本論文では関連研究[7][8]で使用される CVSS Ver.3.1[9]に関して説明する．

CVSS の計算には脆弱性の他のシステムへの影響の有無で若干修正がかかり，最後に整数化するための切り上げを行うが，本論文で論じる本質的な部分ではないため，その部分を省略した計算式を(1-1)〜(1-3)に示す．

$$\text{影響度} = 6.42 \times [1 - (1 - C) \times (1 - I) \times (1 - A)] \quad (1\text{-}1)$$

$$\text{攻撃容易性} = 8.22 \times AV \times AC \times PR \times UI \quad (1\text{-}2)$$

$$\text{リスク値 Rr} = \min[(\text{影響度} + \text{攻撃容易性}), 10] \quad (1\text{-}3)$$

C，I，A：システムが保有する資産の重要度
それぞれ機密性，完全性，可用性に係る
AV: 侵入口の種別
AC: 攻撃の複雑さ
PR: 攻撃に必要な特権レベル
UI: 攻撃に必要なシステム利用者の関与

リスク値 Rr は 0〜10 の値を取り，値が大きいほどリスクが高いと評価される．

2.3.2 Attack Potential

Attack Potential は，ISO/IEC 18045 “CC CEM”[10]での評価手法で，攻撃者の資質や環境からリスクを分析する手法として, こちらもよく用いられている. 計算式を(2)に示す．

$$\text{攻撃容易性} = \text{所要時間} + \text{専門知識} + \text{攻撃対象の知識} + \text{攻撃機会} + \text{使用機器} \quad (2)$$

攻撃容易性は合計値の大小により 5 段階に評価され，値が小さいほどリスクが高いと評価される．

Attack Potential については，攻撃者の技量や知識，および周辺環境の充実具合で攻撃者の能力を評価するものであり，前述の CVSS や後述する CWSS のようにシステム関連の直接的な情報は用いられていない．こちらも脅威分析における重要な観点からのアプローチ手法であるが，本論文では従来手法としての比較は行わない．

2.3.3 CWSS (Common Weakness Scoring System)

CWSS[11]は CVSS と同様, システムの資産やシステム構成の特徴を基に評価を行う脆弱性評価基準であるが, CVSS とは一部異なる観点や評価基準を用いる．2015 年に ITU-T で標準化されており[12], 計算式を式(3-1)〜(3-5)に示す. リスク値 Rw は 0〜100 の値を取り, 値が大きいほどリスクが高いと評価される．

$$\text{リスク値 Rw} = \text{SBase} \times \text{SSurface} \times \text{SEnv} \quad (3\text{-}1)$$

$$\text{SBase} = 4\{f(TI) \cdot (10TI + 5(AP + AL) + 5FC) \cdot IC\} \quad (3\text{-}2)$$

$$\text{SSurface} = \{20(RP + RL + AV) + 20SC + 15IN + 5AS\}/100.0 \quad (3\text{-}3)$$

$$\text{SEnv} = \{f(BI) \cdot (10BI + 3DI + 4EX + 3P) \cdot EC\}/20.0 \quad (3\text{-}4)$$

$$f(x) = 0(\text{if } x = 0),\ 1(\text{otherwise}) \quad (3\text{-}5)$$

TI: 技術的なインパクト
BI: ビジネスに与える金銭的なインパクト
AV: 侵入口の種別
AS: 認証の強度
IN: 攻撃に必要なシステム利用者の関与
DI: 脆弱性の見つけやすさ
AP, AL: 攻撃により獲得できる特権レベル
RP, RL: 攻撃に必要な特権レベル

IC: 脆弱性を悪用できないよう阻止する内部の能力
EC: 脆弱性を悪用できないよう阻止する外部の能力
EX: 脆弱性を悪用できる機会
FC: 脆弱性レポートの信憑性
SC: 脆弱性の波及範囲
P: 脆弱性の普及度合い

CWSS は CVSS に比べ，メトリックの数も設定できるランクの数も多く，よりきめ細かなリスク評価を行えるという特徴がある．また資産が攻撃を受けることでのインパクトに関し，機密性，完全性，および可用性の評価のみならず，BI に見られる金銭的な要素も考慮されている．

3. 課題，アプローチ，および貢献

3.1 課題

前章でも述べたように，APT 攻撃とはカスタマイズされ内部構成の把握が困難なシステムを，さまざまなアプローチを組合せて手探りで調査し，最終的な攻撃目標を達成させる攻撃である．そして後述するように，APT 攻撃における攻撃容易性を評価するのに適切なメトリックを持つリスク数値化手法が現状無いことが課題である．

APT 攻撃の顕著な特徴は，システム侵入にソーシャルエンジニアリングが利用される場合があること，およびその後長期間に渡る潜伏および情報収集が行われることである．そのため，攻撃に際し以下を考慮することを求められる．

1) 攻撃対象の資産や攻撃経路が事前に分からない
2) 長期に渡る潜伏および情報収集が求められるため，発覚を遅らせるための，高い秘匿性が必要
3) システムへの侵入に内部利用者の過失があることが必須，もしくは有利に働く

前章で述べたリスク数値化手法のうち，CVSS と Attack Potential はシステムのリスク評価によく使用される手法であるが，これらの手法は 1)〜3)の特徴もしくは制約を全て満たす事ができないのが問題である．特に CVSS においては， APT 攻撃特有の事項について考慮されていないと問題提起されている[13]．また Attack Potential においても，「攻撃対象の知識」が 1)に相当するが，2)および 3)を評価できるものが無い．

3.2 課題を解決するためのアプローチ

課題を解決するためのアプローチとして，評価式として一定の信頼のある既存の脆弱性評価基準をベースに，APT 攻撃を考慮できる手法を考案することとした．

その場合，十分な検討や評価を経ずに既存の計算式に最初から無いメトリックを追加したり，メトリックの解釈自体を大きく変えたりすることは，計算式そのものの信頼性を損ないかねない．そのため，元々メトリックが多くその解釈の幅が広い CWSS をベースに，メトリックの選定と評価基準の再定義を行ったものをリスク数値化手法として用い，実効性を評価することとした．

川西らは，同様のアプローチを自動車システムに適用し，CWSS をベースとしたリスク数値化手法 RSS-CWSS_CPS を考案し，自動車システムのリスク数値化を行った [14]．本研究ではこのアプローチを採用する．

CWSS であっても，前節 1)〜3)をそのまま解釈できるメトリックは無かった．そのため 1)〜3)の要件を CWSS のメトリックの定義を大きく変えない範囲で，資産や攻撃手段について APT 攻撃のシーケンスで実現可能かどうかで評価できるよう，以下のように検討した．

- まず 2)に関しては, 潜伏や情報収集のために信頼情報の取得, 不正なソフトウェアのダウンロードとインストール, 通信解析による攻撃経路の探索等ができるよう, 高い権限が必要と考える. CWSS では RP(Required Privilege)というメトリックがあるので, これを導入し必要な権限を考慮することとした．
- 次に 1)に関しては, システム内部における機器のトポロジカルな構造よりも, 情報収集で辿ることのできる通信や信頼情報等が重要であることを示している．CWSS では DI(Likelihood of Discovery)というメトリックがあるので, 資産を見つけるために必要な探索手順の量で評価するメトリックとして導入する．
  また 2)に関しても, 目標の資産が見つけやすいほど潜伏期間を短くできるので有利であるという観点から, このメトリックの評価を行うことを検討した．
- 最後に 3)に関しては，IN(Level of Interaction)というシステム利用者の関与を示すメトリックが元々備わっている. これは攻撃が成功するためにシステム利用者の過失等による関与がどの程度見込まれるかというものである. これはしばしばソーシャルエンジニアリングによる手段で侵入が必要な APT 攻撃における，最初の侵入フェーズでの難易度を評価するのに利用することとした．

以上のように，IN は定義通り適用できそうだが，攻撃できるターゲットとその攻撃容易性を絞るために RP と DI の組合せを評価するのに検討が必要と思われた．これらメトリックの評価については 4 章のケーススタディで後述する．

3.3 APT 攻撃の評価を考慮したリスク数値化手法 RSS-CWSS_APT の検討

CWSS をベースに APT 攻撃の特徴 1)〜3)を考慮したリスク数値化手法を RSS-CWSS_APT と定義した．本手法の式(4-1)〜(4-5)は，評価に用いない CWSS のメトリックを固定値とし，リスク値 Rw が CVSS と同様 0〜10 の範囲となるよう，式(4-1)で Rw を 10 で割るようにしている．しかし基の計算式 (3-2)〜(3-5)の係数には一切手を加えていない．

リスク値 Rw =SBase×SSurface×SEnv / 10.0 (4-1)

SBase =4{f(TI)･(10TI+15)･IC} (4-2)

SSurface={20(RP+AV+1)+15IN+5AS+20}/100.0 (4-3)

SEnv ={f(BI)･(10BI+3DI+4EX+3)･EC}/20.0 (4-4)

f(x) =0(if x=0), 1(otherwise) (4-5)

TI: 技術的なインパクト

BI: ビジネスに与えるインパクト

AV: 侵入口の種別

AS: 認証の強度

IN: 攻撃に必要なシステム利用者の関与

DI: 脆弱性の見つけやすさ

RP: 攻撃に必要な特権レベル

IC: 脆弱性を悪用できないよう阻止する内部の能力

EC: 脆弱性を悪用できないよう阻止する外部の能力

EX: 脆弱性を悪用できる機会

図 2 に RSS-CWSS_APT のメトリック配置を示す．前節で述べたように，RSS-CWSS_APT の特徴は，IN，RP および DI の 3 つのメトリックを用いて APT 攻撃を評価する点である．なお本方式は，文献[14]で考案した，RSS-CWSS_CPS では評価しなかった，IN と RP の 2 つのメトリックを追加し，DI の評価基準を見直したものである．

3.4 貢献

本論文における貢献は以下の通りである．

- 工場システムに対する APT 攻撃に着目し，攻撃の特徴をどのように解釈し評価すべきか観点を提示する．
- 脅威分析で用いるリスク数値化手法において，従来考慮されていなかった工場システムへの APT 攻撃の評価を試みる，前節の計算式(4-1)～(4-5)で示した手法である，RSS-CWSS_APT を提示する．
- 工場の模擬システムを交えたケーススタディを実施し実効性を検証し，APT 攻撃のリスク評価にあたっての評価基準の決め方などの課題を示す．

4. ケーススタディ

RSS-CWSS_APT に基づき，工場のシステムモデルを用いたケーススタディを行った．まず実機で構築した攻撃模擬システムで APT 攻撃の一例をトレースし，実際にメトリックのランク設定を行ってみることで妥当性を評価した．次に机上の工場システムモデルで複数の攻撃事例を用意し，他の攻撃手法と比べ APT 攻撃がどのように評価されているか比較考察を行った．

4.1 攻撃模擬システムを用いた APT 攻撃の評価とリスク数値化手法への反映

攻撃模擬システムは，仮想空間内に仮想マシンを配置して実機 OS を搭載したもので構成した．システム構成図を図 3 に示す．ネットワークは業務系(Enterprise Network)と

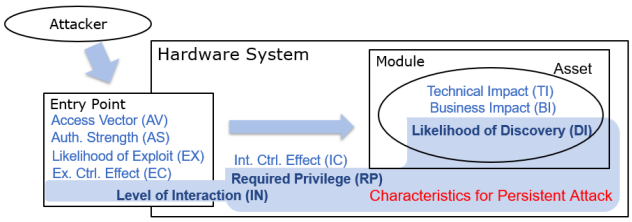

図2 RSS-CWSS_APTのメトリック．

Figure 2 The Metrics of RSS-CWSS_APT.

工場系に分かれ，さらに工場系ネットワークは管理エリア(Operation Management)とフィールド機器エリア(Field Layer)に分かれる．そして企業－社外間および企業－工場間にはファイアーウォールが置かれている．攻撃者は攻撃者 PC(Attacker's PC)と C&C サーバ(C&C Server)を持つ．

前述の BE3 を模した攻撃模擬システムへの攻撃は以下の①～⑤の順に行われる．

① フィッシングメールを利用して企業ネットワーク内の社員 PC(Employee's PC)へ侵入する．

② 認証サーバ(Authentication Server)の脆弱性を利用して認証サーバの管理者権限を取得，信頼情報を窃取する．

③ 社員 PC の通信ログから VPN サーバ(VPN Server)の外向き IP アドレスを把握し，②で窃取した信頼情報を用いて管理エリアの VPN サーバに接続する．

④ パスワード使い回しの不備を利用し，VPN サーバからコントローラ(Controller)へリモートログインする．

⑤ コントローラの制御命令を書き換え，フィールド機器エリアのマシン(Machine)へ送信する．

この攻撃をメトリック IN，RP，および DI に関して評価する場合，以下のようになる．

① システム利用者がメールのバイナリを開くという関与は容易で，攻撃のチャンスがある．メール到着時に警告が出ないなら IN=T(Typical/Limited)=0.9，警告が出て利用者がそれを無視する必要があるのなら M(Moderate)=0.8 と判定する．これらはメトリック IN でリスクを評価する際に，高い順に 2 位および 3 位となるランクである．この評価では T とする．

② 最低限社員 PC で管理者権限を取る必要があるが，ファイアーウォール等のネットワーク機器と比べ権限昇格が容易なので，RP=RU(Regular User)=0.7 とする．これはリスクの高い順に 3 位のランクである．認証サ

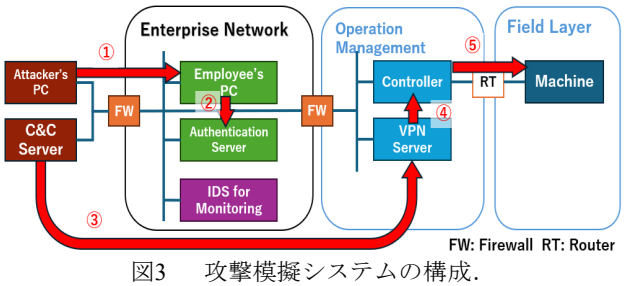

図3 攻撃模擬システムの構成．

Figure 3 The Configuration of Attack Simulation System.

ーバの権限昇格は脆弱性利用で比較的容易に実現できるので，本来必要な P(Partially-Privileged User)=0.6 よりもリスクが高くなるように評価している．

③ VPN サーバの IP アドレスと使用ポートは，社員 PC を乗っ取ることで容易に見つけ出せる．そして VPN 接続は②で窃取した信頼情報で接続できる．従ってメトリックのランクの変更は行わない．

④ 隣接する機器は VPN サーバの ARP テーブルで分かり，さらにパスワード使い回しという不備があるので，ここでもメトリックのランクの変更は行わない．

⑤ コントローラは PLC のようなセキュリティの弱い機器を想定しているので，制御信号書き換えには RP=RU(Regular User)=0.7 程度の権限で十分とみなす．ただ，制御命令についてはどの通信パケットか，フォーマットは何か，値をどうすれば故障を引き起こせるか等，C&C サーバに情報を送って解析する必要があるので，DI=L(Low)=0.2 とする．これは最もリスクが低くなる値である．

以上により，IN=0.9(T), RP=0.7(RU), DI=0.2(L)となった．他のメトリックについても以下の通り．ネットワークのトポロジカルな関係のみでの評価と異なり，APT 攻撃ではこれらのメトリックの評価も変わる．

- 制御ミスが事故を引き起こし，かつ企業の信用失墜につながると考え，TI と BI は C(Critical)=1.0 とする．
- VPN 接続から先は正規手続きでの通信かつ秘匿通信であるため，企業ネットワーク内のモニタ用 IDS(IDS for Monitoring)で攻撃を検知できないので，攻撃の検知のリスクはあるのは社員 PC から認証サーバへの攻撃のみ．IDS 等検知機器も備わっていないと考えた場合，IC は最もリスクの高い N(None)=1.0 とできる．
- AV はネットワーク経由の侵入なので I(Internet)=1.0．
- フィッシングメールに引っかかることで認証がバイパスされるので，AS は N(None)=1.0．本ケーススタディにおいてソーシャルエンジニアリングを手段に用いる場合，IN と AS はバーターの関係と考えている．
- EX は攻撃の機会の多さを評価する．社員 PC はメールや Web アクセスを含め，攻撃機会が多いので H(High)=1.0 とする．
- DMZ からは攻撃者は任意のタイミングで攻撃できるが，ファイアーウォールが偶然攻撃者のドメインをブロックしている等，多少の障害があるかもしれない．従って EC=L(Limited)=0.9 とする．

以上で 10 個のメトリックのランク値が決定できたので，式(4-1)～(4-5)に代入したところ，リスク値 Rw=7.33 が得られた．Rw は 0～10 の値を取る計算式からなり，7 を超えるリスクは重要脅威とみなしてよい．以上により，システム利用者の関与が必要な代わりに認証が突破できること，最低限の権限だけで攻撃が継続できること，そして信頼情報獲得後は VPN 接続の秘匿性により攻撃が発覚しづらいことで，RSS-CWSS_APT により高リスクであると評価された．

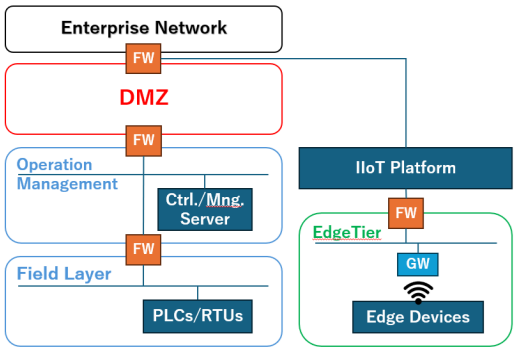

図4　工場システムの評価モデル(略図).

Figure 4　Factory System Evaluation Model (Simplified).

4.2 工場システムモデルでの机上分析

模擬システムで検討した攻撃手順の評価を工場システムモデルに適用し，高リスクの脅威と評価された APT 攻撃と他の攻撃について，評価結果を比較した．工場システムモデルは NIST SP800-82 r3[15] の Figure 19，DCS(Distributed Control System)と IIoT(Industrial Internet of Things)を統合したアーキテクチャ図をベースに，典型的な資産を想定し登

表 1 各手法によるリスク値の比較.

Table 1 Comparison of Risk Values between the Methods.

#	Typ.	Metrics of RSS-CWSS_APT										
		Attack Feasibility								Impact		Rw
		IC	AV	AS	EX	EC	IN	RP	DI	TI	BI	
1	A	1.0	1.0	1.0	1.0	0.9	0.3	0.6	1.0	1.0	1.0	7.34
2	N	1.0	1.0	1.0	1.0	0.9	0.9	0.7	1.0	1.0	1.0	8.33
3	L	1.0	0.5	0.8	0.6	1.0	1.0	0.7	1.0	1.0	1.0	7.64
4	M	1.0	0.7	0.9	0.6	0.9	1.0	1.0	1.0	1.0	1.0	7.74

#	Typ.	Metrics of RSS-CWSS_CPS										
		IC	AV	AS	EX	EC			DI	TI	BI	Rw
1	A	1.0	1.0	0.8	1.0	0.9			1.0	1.0	1.0	8.91
2	N	1.0	1.0	0.8	1.0	0.9			1.0	1.0	1.0	8.91
3	L	1.0	0.5	0.8	0.6	1.0			1.0	1.0	1.0	8.19
4	M	1.0	0.7	0.9	0.6	0.9			1.0	1.0	1.0	7.74

#	Typ.	Metrics of CVSS Ver.3.1										
		Attack Feasibility							Impact			Rr
		AV	AC	PR	UI				C	I	A	
1	A	0.85	0.77	0.62	0.62				0.0	0.56	0.56	7.25
2	N	0.85	0.77	0.62	0.62				0.0	0.56	0.56	7.25
3	L	0.55	0.77	0.62	0.85				0.0	0.56	0.56	7.01
4	M	0.62	0.77	0.62	0.85				0.0	0.56	0.56	7.25

Typ.: A=APT Attack, N=Network, L: Local,
M: man-in-the-middle

録したものを用いた．図 4 にその略図を示す．リスク数値化手法に関しては, RSS-CWSS_APT の他, 従来手法の CVSS 3.1 および文献[14]で川西らが考案した RSS-CWSS_CPS を比較対象とした．

表 1 は，工場システムモデルで高リスクと評価された 4 つの脅威を抜き出したものである．#1 は DMZ 経由で Edge Device の制御機能を攻撃する APT 攻撃，#2 は DMZ 経由で Operation Management の機器の重要機能への攻撃，#3 は Operation Management エリアへの物理的な侵入による機器の重要機能への攻撃, および#4 は Edge Tier エリア内の Wi-Fi を利用した重要機器への中間者攻撃を想定した．この 4 つの脅威でのリスク値の比較により以下の事が確認できた．

A) RSS-CWSS_APT で導入された IN および RP は，攻撃容易性の観点で APT 攻撃のリスク値を上昇させるのではなく，低下させる要因として働く．

表 1 の各事例について，RSS-CWSS_CPS と RSS-CWSS_APT の結果を比較すると，後者のリスク値は下がり，なおかつ APT 攻撃である#1 の下がり幅が最も大きい事がわかる(表 1 橙色マス).

B) RSS-CWSS_APT における IN および RP の値は#1 と #2 で異なり，#2 のリスク値が#1 のそれよりも値の低下が緩和される方向で値が設定されている．

これは侵入に用いた手段(フィッシングメール利用を想定する#1 とインターネットに面した DMZ で用いる Web サービス等への不正アクセスを想定した#2 という攻撃手段の違い)と侵入の深さ(侵入した PC の属するドメイン内の機器への攻撃を想定する#1 と侵入した機器のドメインからさらに隣接するドメインの機器への攻撃を想定する#2 との違い)で評価を行った結果である，そして#1 の侵入の方がシステム利用者の関与の程度と必要なアクセス権限の要求レベルが高いと判断されたため, リスク値が下がる方向で差が出ている (表 1 橙色マスと黄色マス).

C) CVSS Ver.3.1 における UI と PR もシステム利用者の関与と攻撃に必要なアクセス権限レベルを評価するメトリックであり, 攻撃容易性の観点でリスク値が下がる方向に働いている．しかし UI の取れるランクは関与のありなしを評価する 2 通り, PR も High, Low, None の 3 通りのランクと少ないため，APT 攻撃である#1 とそれ以外の DMZ 経由の攻撃#2 を評価するにあたり, 明確な違いとして現れていない. その結果 B) と異なり同一のリスク値となっている(表 1 青色マス).

4.3 考察

4.1 節のケーススタディを通じ, CWSS をベースとした手法 RSS-CWSS_APT を用いることで，APT 攻撃を評価できることを確認した．そして 4.2 節のケーススタディで複数の脅威について比較評価を行い，APT 攻撃の特徴である侵入・潜伏・調査などの手順を考慮しつつ他の攻撃との差別化を検討する際の知見をいくつか得た．本節ではさらに考察を深め課題を抽出する．

表 2　攻撃容易性における各メトリックの重み.

Table 3 Weight of each Metric in Attack Feasibility.

Change of Rw calculated by RSS-CWSS_APT							
AV	AS	IC	EC	EX	IN	RP	DI
0.2	0.05	1.0	1.0	0.2	0.15	0.2	0.15
Change of Rw calculated by RSS-CWSS_CPS							
AV	AS	IC	EC	EX			DI
0.2	0.05	1.0	1.0	0.2			0.15
Change of Rr calculated by CVSS Ver.3.1							
AV	AC				UI	PR	
0.822	0.822				0.822	0.822	

表 1 で比較を行った 3 つのリスク数値化手法における，各メトリックの変動量について補足したものが表 2 である．これは各手法において全てのメトリックの入力を 1 にしておいてから，該当するメトリックから 0.1 を減じた時の変動値であり，メトリックのランクが変動した時のリスク値変動の目安となる重みを示したものである．RSS-CWSS_APT における IN, RP, および DI の重みはそれぞれ 0.15，0.2，0.15 と小さいものの，APT 攻撃における侵入・潜伏・調査で制約がかかる要因についてリスク値の差別化に貢献している．CVSS Ver.3.1 でも UI と PR というシステム利用者の関与と攻撃に必要なアクセス権限を評価するメトリックがあり，重みが大きくリスク値の大きな変動をもたらしうるものであるが, DI に相当するメトリックが無く, また選択できるランクも UI の 2 通り，PR の 3 通りと少なく, 実際の運用で APT 攻撃とそうでない攻撃とでのリスク値の差別化に貢献しづらいことが分かった．

さらに 3.2 節における当初の予想と異なり，本手法におけるメトリックの解釈，特に IN の解釈が新たな課題となった．元々IN はフィッシングメール等のソーシャルエンジニアリングで攻撃者がシステム利用者を望ましく誘導できるかを評価するものと定義されており，4.1 節の BE3 の事例では問題なく IN の評価を行えた．しかし複数の攻撃事例を想定した 4.2 節のケーススタディにおいてはシステム利用者の誘導に加え，システム利用者のシステムの使い方についても厳密に考慮し評価する必要があると思われた．

例えば攻撃者がシステムに侵入する手段としてフィッシングメール等の実現可能性だけを評価するだけでは不足であり，侵入した PC を拠点としてさらに深く，OT エリアの機器に到達できるかどうかも，システム利用者の関与にかかっている．4.1 節で取り上げた BE3 が利用した VPN 接続の事例のように，最初に侵入した端末でシステム利用者がリモートで工場ネットワーク内の機器の監視や操作を行っているかどうかの違いで，その後の攻撃の難易度が大きく左右される．また攻撃者がシステム利用者を懐柔すること

で OT エリアにバックドアデバイスを設置できれば，攻撃経路のショートカットが可能になるが，それをどう定量的に評価するか．具体的にはそのあたりが課題となった．

以上，IN について見解を述べたが，RP についても攻撃手順や状況に応じて必要な権限が変わりうるため，その解釈が課題となった．例えば 4.2 節の B)で説明したケースでは，この観点における IN と RP の評価が若干曖昧で，課題を残した． APT 攻撃の攻撃容易性を評価する場合，これら CWSS における人的要因について評価するメトリックをどう定義し評価基準を設けるかがポイントとなると思われる．

5. 結論

本論文では IT の導入が進んだ工場システムモデルにおける APT 攻撃について着目し，脅威分析・リスクアセスメントの際に APT 攻撃の特徴を考慮し，リスク数値化手法 RSS-CWSS_APT を考案した. また実機による攻撃模擬システムを構築して実際に APT 攻撃を再現することで, リスク数値化手法のメトリックの評価基準の定め方について考察を行った．そして NIST SP800-82r3 掲載のアーキテクチャを適用した工場システムモデルを評価し，本手法による APT 攻撃の評価の実効性の確認と課題の抽出を行った．

まずリスク数値化手法の考案に際しては，APT 攻撃の特徴である 3 つの特徴に着目し，侵入後の攻撃目標の見つけやすさ，攻撃者が必要な特権のレベル，および被攻撃者であるシステム利用者の関与の度合いという，攻撃容易性に関わるメトリックを採用している CWSS をベースとしたリスク数値化手法，RSS-CWSS_APT を考案した．

次に，実際の攻撃事例を元に実機で構築した，工場の攻撃模擬システムを用いたケーススタディを行い，本手法で用いたメトリックの評価基準について考察した．攻撃模擬システムでは，フィッシングによるシステム内 PC のへの侵入後, 信頼情報の獲得を通じ OT エリアへの VPN 接続を行い，OT エリア内での情報収集を通じて攻撃目標を見つけ出すプロセスを実際に体験した．APT 攻撃は，システム利用者の過失や運用の不備等を突き，侵入と通信の解析や信用情報の取得を繰り返し，見つけた機器の皿に奥に侵入し攻撃目標への攻撃を行うプロセスであり，RSS-CWSS_APT の 3 つのメトリック IN，RP，および DI の観点から評価が行えることが確認できた．

さらに，上記 NIST SP800-82r3 掲載の工場システムモデルを元に，複数の脅威に対して机上でのリスク評価を実施し，従来手法である CVSS Ver.3.1 との分析結果の比較を行った. その結果, RSS-CWSS_APT で注目したメトリック IN および RP により，APT 攻撃とそうでない攻撃について CVSS Ver.3.1 よりリスクを細かく差別化出来た．

しかし一方で上記 IN や RP のような APT 攻撃における人的要因を評価するメトリックの評価基準の明確化が新たに課題となった．ケーススタディではフィッシングメール等のソーシャルエンジニアリングを利用した手段のみならず，システム利用者が工場ネットワーク内で監視制御を行うためのサービスの使い方までもが評価対象となり，これを IN と RP で総合的かつ明確にどのように評価すればよいか，今後考えていく必要があることが分かった．

APT 攻撃は攻撃目標達成のために，ソーシャルエンジニアリングやシステム内部の人的要因等，システム内外への様々なアプローチを組合せた柔軟かつ複雑な攻撃である．そのためシステム構成要素から評価を行う本手法では評価基準の定め方に課題がある．今後さらに検討を進め，APT の特徴から導かれる新たな視点に立った分析やセキュリティプロセスを考えていきたい．

参考文献

[1] Sumayah Al-Rabiaah: The “Stuxnet” Virus of 2010 As an Example of A “APT” and Its “Recent” Variances, 21st Saudi Computer Society National Computer Conference (NCC) (2018).

[2] A. Presekal, et al.: Advanced Persistent Threat Kill Chain for Cyber-Physical Power Systems, IEEE Access (2024).

[3] M. M. Aslam, et al.: Scrutinizing Security in Industrial Control Systems An Architectural Vulnerabilities and Communication Network Perspective, IEEE Access (2024).

[4] iTrust: BlackEnergy - Malware for Cyber-Physical Attacks (2016).

[5] ISA/IEC: Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design (2020).

[6] ISO/SAE: ISO/SAE 21434: Road vehicles - Cybersecurity engineering (2021).

[7] E. A. AbuEmera, H. A. ElZouka, and A. A. Saad: Security Framework for Identifying threats in Smart Manufacturing Systems Using STRIDE Approach, 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE) (2022).

[8] B. Brenner, et al.: Better Safe Than Sorry: Risk Management Based on a Safety-Augmented Network Intrusion Detection System, IEEE Open Journal of the Industrial Electronics Society, Vol. 4 (2023).

[9] FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST): Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System v3.1: Specification Document (online), available from <https://www.first.org/cvss/v3.1/specification-document> (accessed 2025-08-20).

[10] ISO/IEC: ISO/IEC 18045:2022, Information technology — Security techniques — Methodology for IT security evaluation (2022).

[11] Common Weakness Enumeration: Common Weakness Scoring System (CWSS) (online), available from <https://cwe.mitre.org/cwss/cwss_v1.0.1.html> (accessed 2025-08-20).

[12] ITU-T: ITU-T X.1525: Cybersecurity information exchange, Vulnerability/state exchange, Common weakness scoring system (2015).

[13] S. Islam and A. Sand: The CVSS Deception: How We've Been Misled on Vulnerability Severity, Black Hat Europe 2024 (2024).

[14] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto, and H. Inoue: A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS, IEEE Access (2023).

[15] NIST: NIST SP800-82r3 Guide to Operational Technology (OT) Security (2023).