Vol.2021-CSEC-93 No.11
Vol.2021-IOT-53 No.11
2021/5/13

攻撃手法情報を活用した マルウェアが制御システムに引き起こす脅威の導出手法の開発

笹 晋也[1]　太田原 千秋[1]　内山 宏樹[1]

概要：制御システムと情報システムの接続が進むにつれ，制御システムに対するサイバー攻撃が年々増加している．特に，近年ではマルウェアの流行によって制御システムが被害を受けるケースが増加している．システムに対するマルウェアの被害を防ぐためには，システム構成を踏まえてマルウェアの影響を評価し，適切な対策を講じることが必要である．しかし，制御システムについては資産管理システムの導入が難しい等の理由により，OS・ソフトウェアレベルの詳細なシステム構成情報の取得が困難である場合も多い．そのような場合にマルウェアの影響を評価するには，専門家による個別の分析が必要となり時間がかかってしまうという課題があった．このような課題を解決するため，本研究ではマルウェアが用いる攻撃手法の情報から制御システムに対する脅威を導出するルールを構築することにより，マルウェアが分析対象システムに引き起こし得る脅威を機械的に特定する手法を検討した．

キーワード：制御システム，セキュリティ設計，脅威分析，リスク評価，マルウェア

Development of a method to identify malware threats to control systems using attack technique information

SHINYA SASA[1]　CHIAKI OTAHARA[1]
HIROKI UCHIYAMA[1]

Abstract: As more control systems are connected with IT systems, the number of cyber attacks on control systems has been increasing. Especially, a growing number of control systems are damaged by the spread of malware in recent years. In order to prevent damage by malware, it is necessary to evaluate possible impacts of malware taking system configurations into account and take appropriate countermeasures. However, it is often difficult to obtain detailed configuration data including OS and software names due to difficulty in introducing asset management systems. In this case, evaluation of malware impacts requires manual analysis by experts and becomes a time-consuming process. In order to solve this problem, we devised a set of rules which derives threats to control systems from a list of attack techniques and developed a method to identify possible threats caused by specific malware using the rules.

Keywords: Control System, Security Design, Threat Analysis, Risk Evaluation, Malware

1. はじめに

近年, 制御システムと情報システムの接続が進むにつれ，制御システムに対するサイバー攻撃は増加傾向にある[1]．特に，近年ではランサムウェア WannaCry による自動車メーカー操業停止，BlackEnergy3 による電力システムへの攻撃を起因とした停電[2]，EKANS による医療関連企業の業務停止・情報漏えい[3]など，マルウェアの流行によって制御システムが被害を受けるケースが増加している．システムに対するマルウェアの被害を防ぐためには，システム構成を踏まえてマルウェアの影響を評価し，適切な対策を講じることが必要である．しかし，制御システムについては資産管理システムの導入が難しい等の理由により，OS・ソフトウェアレベルの詳細なシステム構成情報の取得が困難である場合も多い．そのような場合にマルウェアの影響を評価するには，専門家による個別の分析が必要となり時間がかかってしまうという課題があった．このような課題を解決するため，本稿ではマルウェアが用いる攻撃手法の情報から制御システムに対する脅威を導出するルールを構築することにより，マルウェアが分析対象システムに引き起こし得る脅威を機械的に特定する手法を提案する．

以下，まず 2 章において制御システムに対するセキュリティ設計の課題を述べる．次に，3 章で脅威分析結果からマルウェアが引き起こす脅威を抽出する手法を提案し，4 章で実際のマルウェアに適用し評価した結果を示す．最後に，5 章でまとめと今後の課題を述べる．

2. 制御システムに対するセキュリティ設計の課題

2.1 セキュリティ設計の概要

セキュリティ設計とは，システムをセキュアにすることを目的とした，適切なセキュリティ対策の立案に必要な一連のプロセスである．本稿では，セキュリティ設計を以下

1 (株)日立製作所
Hitachi Ltd.

Vol.2021-CSEC-93 No.11
Vol.2021-IOT-53 No.11
2021/5/13

の 3 つのステップに分けて議論する．

（1）評価対象定義

評価対象とするシステムの範囲を定義する．

（2）脅威分析・リスク評価

評価対象のシステムに対しセキュリティ上の損害を引き起こす脅威を網羅的に抽出し，それぞれの脅威がもたらすリスクを評価し，対策優先順位付けを行う．

（3）対策立案

各脅威に対し，対策実施箇所ごとに有効な対策を選定する．

脅威分析については，体系的・網羅的に脅威を抽出するためのフレームワークが数多く存在する．その一つが脅威分類 STRIDE[4]である．STRIDE はなりすまし（Spoofing），改ざん（Tampering），否認（Repudiation），情報漏えい（Information disclosure），サービス拒否（Denial of service），特権昇格（Elevation of privilege）からなる．脅威分析では，例えば STRIDE を組み合わせることで脅威発生時に起こる事象（脅威イベント）の順列を列挙し，その中から対象システムに起こり得るものを選択することにより，システムに対する脅威を抽出することができる．

リスク評価については，リスクを定量化するために開発されたフレークワークが多数存在し，それらを用途に応じて選択した上で評価することが多い．リスク評価手法を提供するフレームワークとしては，CRSS，RSMA[5]，DREAD[6]などがある．例えば，CRSS は攻撃元区分，攻撃条件の複雑さ，攻撃前の認証要否，機密性への影響，完全性への影響，可用性への影響の 6 指標を評価することでリスク値を計算し，対策すべき脅威の優先順位を決めることができる．

2.2 セキュリティ設計の課題

セキュリティ設計におけるリスク評価では，脅威そのものの特性や分析対象システムの性質をもとにリスク評価することが多く，各脅威の現時点での起こりやすさを考慮して動的にリスク評価することは少ない．これは，リスク評価に関する既存のフレームワークが脅威の流行状況を反映する仕組みを持たないことが原因の 1 つである．

特に，マルウェアの流行状況をリスク評価に反映するためには，システムに対し抽出された脅威のうちマルウェアが引き起こすものを特定する必要がある．しかし，マルウェアの挙動に関する体系化された情報源が少なく，個別の調査が必要となり工数がかかることが多い．また，マルウェアの挙動は技術的かつ詳細な記述がされていることも多く，脅威分析で抽出される STRIDE 等をベースにした粗い脅威との対応付けには専門知識が必要である．

マルウェアが引き起こす脅威の特定に適用可能性がある研究として，研究報告[7][8]の提案手法が挙げられる．この報告では，Latent Dirichlet Allocation（LDA）を用いて，脆弱性データベースの各脆弱性の説明文と既存攻撃事例の文章を突き合わせ，攻撃事例に使われた脆弱性に類似する脆弱性を抽出する手法が提案されている．マルウェアに関するレポート等の文章にこの手法を適用することにより，脅威分析で得られる脅威のうちマルウェアが引き起こすものを抽出できる可能性があるが，そのような評価は本稿執筆時点ではなされていない．

このような背景から，本研究では制御システムに対し STRIDE をベースに抽出された脅威のうち，流行中のマルウェアが引き起こすものを機械的に特定する手法を検討した．

3. 提案手法

3.1 提案手法の全体像

提案手法の全体像を図 1 に示す．本手法では，まずマルウェアの攻撃手法の情報を元にマルウェアが引き起こす脅威イベントを導出する（図中①）．このとき，導出する脅威イベントを決定するルールが脅威イベント導出ルールである．次に，マルウェアが引き起こす脅威イベントのリストと，分析対象システムに対する脅威分析の結果得られた脅威のリストを突き合わせ，マルウェアが引き起こす脅威のリストを得る（図中②）．

攻撃手法情報については 3.2 節，脅威イベント導出処理と脅威分析結果に用いられる脅威イベントの定義については 3.3 節，脅威イベント導出処理については 3.4 節，突合せ処理については 3.5 節で述べる．

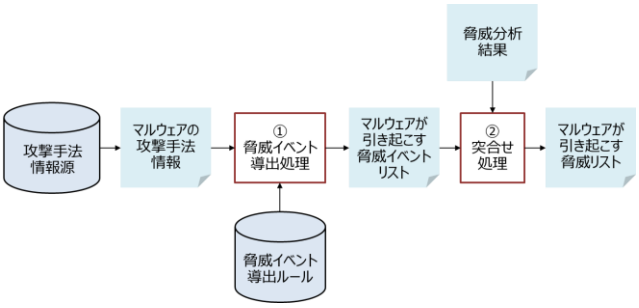

図 1　提案手法の全体像

3.2 攻撃手法情報

本手法では，マルウェアの攻撃手法の情報源として MITRE ATT&CK®[9]を用いる．ATT&CK は攻撃者が用いる technique（戦法）を tactic（戦術）ごとに分類し体系化したナレッジベースであり，マルウェアなどの各種ソフトウェアが用いる technique の情報を提供している．そのため，マルウェアに対する technique のリストを攻撃手法情報として活用することとした．ATT&CK にはドメインに応じて Enterprise，Mobile，ICS[10]の 3 つのマトリクスが用意され

ているが，本研究では technique の情報が掲載されているマルウェアの種類数が多い ATT&CK for Enterprise を用いた．

例として，マルウェア「WannaCry」に対する攻撃手法情報を表 1 に示す．

表 1　WannaCry の攻撃手法情報[11]

ID	Technique
T1543.003	Create or Modify System Process: Windows Service
T1486	Data Encrypted for Impact
T1573 .002	Encrypted Channel: Asymmetric Cryptography
T1210	Exploitation of Remote Services
T1083	File and Directory Discovery
T1222.001	File and Directory Permissions Modification: Windows File and Directory Permissions Modification
T1564.001	Hide Artifacts: Hidden Files and Directories
T1490	Inhibit System Recovery
T1570	Lateral Tool Transfer
T1120	Peripheral Device Discovery
T1090.003	Proxy: Multi-hop Proxy
T1563.002	Remote Service Session Hijacking: RDP Hijacking
T1018	Remote System Discovery
T1489	Service Stop
T1016	System Network Configuration Discovery
T1047	Windows Management Instrumentation

3.3 脅威イベントの定義

提案手法では，脅威イベント導出処理で出力される脅威イベントリストと脅威分析結果が同じ脅威分類に基づいている必要がある．脅威分類には先述した STRIDE だけでなくより詳細な分類も存在するが，抽出される脅威数が膨大となり解析が困難になることから，本手法では STRIDE を活用することとした．

本手法で用いた，STRIDE をベースに定義した脅威イベントの一覧を表 2 に示す．STRIDE にはマルウェアによる攻撃に不可欠なステップである不正アクセスが含まれていないため，脅威イベントとして追加した．また，STRIDE のうち「なりすまし」は，事前に認証情報を収集した上で感染拡大（ラテラルムーブメント）のために行われることがあるため，これに対応する脅威イベント「認証情報の調査」を追加した．更に，マルウェアによっては認証情報を使用せず脆弱性を利用して感染拡大する場合もあるため，これに対応する脅威イベントとして「感染拡大（脆弱性利用）」を追加した．一方，マルウェアが否認することによってシステムに直接的に損害を与えることは少ないため，本研究では脅威イベントに含めないこととした．

本手法では突合せ処理の入力として，表 2 の脅威イベントに基づく脅威分析結果を用いた．それに合わせ，表 2 の脅威イベントのうちマルウェアが引き起こすものを導出する脅威イベント導出ルールを作成した．

表 2　STRIDE ベースの脅威イベント

なりすまし
改ざん
情報漏えい
DoS 攻撃
特権昇格
不正アクセス
認証情報の調査
感染拡大（脆弱性利用）

3.4 脅威イベント導出処理

本節では，脅威イベント導出処理の詳細を述べる．

脅威イベント導出処理の入出力を図 2 に示す．入力である攻撃手法情報はマルウェアの用いる technique のリストであり，出力は表 2 の脅威イベントのうち，脅威イベント導出処理により導出されたもののリストである．

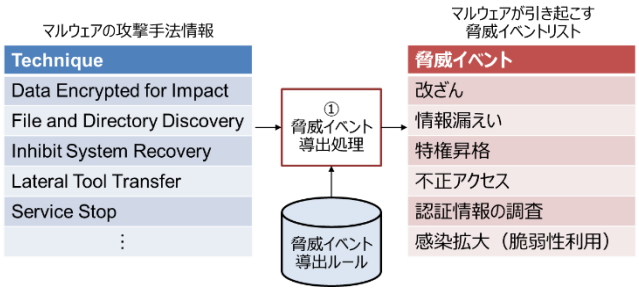

図 2　脅威イベント導出処理

最も単純な脅威イベント導出ルールとしては，ATT&CK の各 technique に対し，引き起こされる脅威イベントを対応させることが考えられる．しかし，このような単純な対応表ではマルウェアが引き起こす脅威イベントを正確に特定できない場合が存在した．例えば，既存のアカウントのクレデンシャルを取得する technique である“Valid Accounts”はなりすましと特権昇格の両方に用いられる可能性があり，マルウェアがどちらを引き起こしているかの判断が困難である．

この問題を解決するため，technique と脅威イベントの対応表ではなく，technique の組み合わせから脅威イベントを導出するルールを作成した．作成した脅威イベント導出ルールの一部を図 3 に示す．ルール作成の際，マルウェアのサンプルとして WannaCry，Emotet，Agent Tesla，IcedID，

BONDUPDATER, Calisto, DarkComet, HiddenWasp, Carberp, BabyShark, CosmicDuke, Flame, Shamoon を用い，これらのマルウェアが引き起こす脅威イベントを手動で調査・特定した上でルール作成の参考にした．

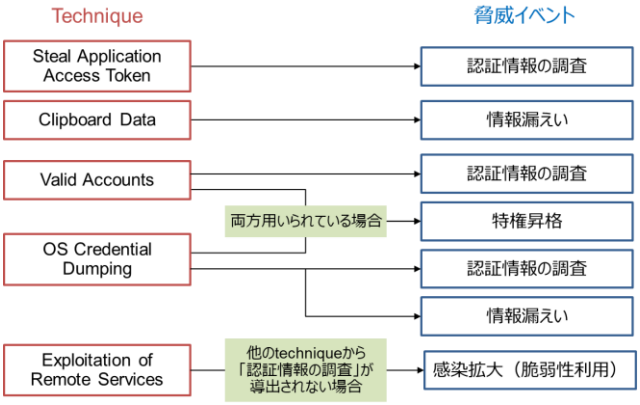

図 3　脅威イベント導出ルール（一部）

例えば，マルウェアが technique “Valid Accounts” を用いている場合，マルウェアが用いる他の technique の中に特権を必要とするものが含まれるか否かにより，導出する脅威イベントを変えることとした．ATT&CK では，各 technique を実行するために必要な権限（User, Administrator, SYSTEM, root など）が記載されている．この情報を用い，“Valid Accounts” と特権（Administrator, SYSTEM, root）を必要とする technique が同時に用いられている場合，特権昇格を脅威イベントとして導出するルールを設定した．特権昇格となりすましの両方を引き起こし得る他の technique についても，各 technique に必要な権限の情報を用いて同様の脅威イベント導出ルールを設定した．

別のルールとして，“Exploitation of Remote Services” は収集した認証情報を用いてなりすました上で行われる場合と，脆弱性を利用して行われる場合がある．従って，「なりすまし」「感染拡大（脆弱性利用）」の判定精度を向上させるため，“Exploitation of Remote Services” が用いられており，かつ脅威イベント導出ルールにより他の technique から「認証情報の調査」が導出されない場合，「感染拡大（脆弱性利用）」を導出するルールを構築した．“Exploitation of Remote Services” は tactic “Lateral Movement” に分類されるが，この tactic に分類される他の technique についても同様の脅威イベント導出ルールを設定した．

このように設定した脅威イベント導出ルールをマルウェアの攻撃手法情報に用いることで，マルウェアが引き起こす脅威イベントのリストが出力される．

3.5 突合せ処理

突合せ処理は，脅威イベント導出処理で得られたマルウェアが引き起こす脅威イベントのリストを元に，脅威分析結果のうちマルウェアに引き起こされる脅威を抽出する処理である．

突合せ処理の入力と出力を図 4 に示す．本手法では脅威分析結果として，論文[12]で提案された脅威テンプレートをベースに，Where（脅威発生箇所），Who（攻撃者），When（攻撃タイミング），Why（攻撃の動機），What（脅威事象）の観点から脅威を抽出したものを用いた．ただし，本評価の目的を考慮し，Who は「外部者」，When は「運用」，Why は「故意」に固定した．また，What は表 2 の脅威イベントを組み合わせることで生成した．

突合せ処理では最も単純な方式として，ある脅威の What に含まれる脅威イベントが全てマルウェアが引き起こす脅威イベントリストに含まれている場合，マルウェアが引き起こす脅威として出力することとした．例えば，脅威分析結果の中に，What が「インターネット経由で不正アクセス」「機器 B に感染拡大（脆弱性利用）」「機器 B の情報を改ざん」から構成される脅威が含まれる場合を考える．あるマルウェアの攻撃手法情報から脅威イベント「不正アクセス」「感染拡大（脆弱性利用）」「改ざん」が全て脅威イベント導出処理により導出された場合，この脅威はマルウェアが引き起こすものと判断され，「マルウェアが引き起こす脅威リスト」の 1 つとして出力される．

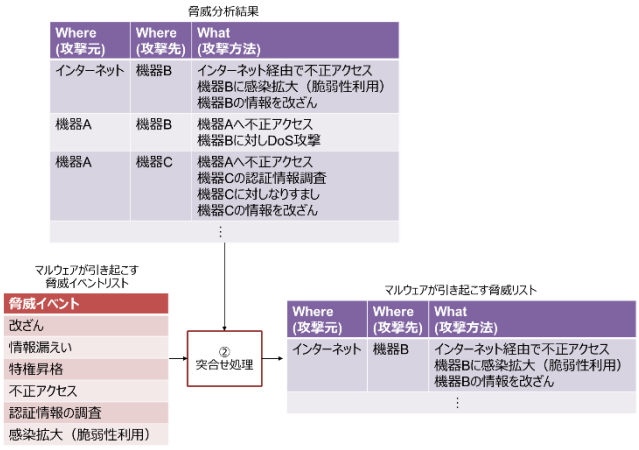

図 4　突合せ処理

4. 評価と考察

4.1 脅威イベント単位の評価

本節では，脅威イベント単位で脅威イベント導出ルールの精度を評価した結果を示す．本評価では，評価対象のマルウェアとして Ryuk, Backconfig, Hydraq, NotPetya, Attor, CozyCar, PowerShower を用い，公開情報を元に人手で特定した脅威イベントと，脅威イベント導出処理により導出された脅威イベントを比較した．比較結果を表 3 に示す．

人手で特定された脅威イベント 26 個のうち 25 個（96%）は脅威イベント導出ルールにより導出された．一方，脅威

Vol.2021-CSEC-93 No.11
Vol.2021-IOT-53 No.11
2021/5/13

イベント導出ルールにより導出された脅威イベント 29 個のうち 4 個（14%）は，人手での分析で導出されなかったものであった．

表 3　提案手法と人手で導出された脅威イベントの比較

	Ryuk	Backconfig	Hydraq	NotPetya	Attor	CozyCar	PowerShower
なりすまし							
改ざん	●	●	●	●	●	▲	▲
情報漏えい	▲	●	●	●	●	●	●
DoS 攻撃	●						
特権昇格	●		●	●			
不正アクセス	●	●	●	●	●	●	●
認証情報の調査						●	○
感染拡大（脆弱性利用）	▲		●	●			

●：人手での分析・提案手法両方で導出
○：人手での分析のみで導出
▲：提案手法のみで導出

4.2 サンプルシステムを用いた評価

本節では，サンプルシステムに対する脅威分析結果に提案手法を適用した結果を示す．本評価では，文献[13]に記載の仮想システムを参考に，図 5 に示すサンプルシステム構成を作成し，このシステムに対する脅威分析を行った上で，その結果に提案手法を適用した．

まず，このサンプルシステムに対する脅威分析の結果，全部で 248 件の脅威が抽出された．脅威分析結果の一部を表 4 に示す．

次に，7 種類のマルウェアに脅威イベント導出ルールを適用した結果（表 3）を入力として突合せ処理を行った．この結果導出された脅威を，脅威分析結果のうちマルウェアが引き起こすものを人手で特定した結果と比較した．

比較結果を集計したものを表 5 に示す．今回評価対象としたマルウェアについては，マルウェアが引き起こす脅威として人手で導出されたものは提案手法により全て導出されたことを確認した．一方，提案手法で導出された脅威のうち 25%は人手で特定されていない脅威であった．従って，本手法を用いた場合マルウェアに対する対策が一部過剰になるため，精度の向上が必要である．

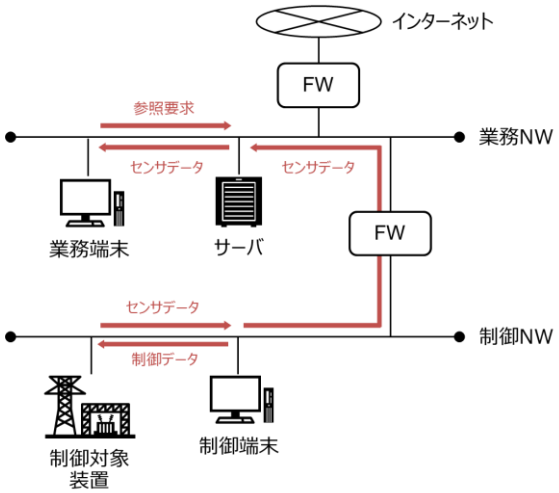

図 5　サンプルシステム（文献[13]を参考に作成）

表 4　サンプルシステムに対する脅威分析結果の例

Where（攻撃元）	Where（攻撃先）	What（攻撃方法）
業務端末	制御対象装置	1. 業務端末へ不正アクセス 2. 制御対象装置に感染拡大（脆弱性利用） 3. 制御装置の情報を改ざん
業務端末	制御端末	1. 業務端末へ不正アクセス 2. 制御端末の認証情報調査 3. 制御端末に対しなりすまし 4. 制御端末において特権昇格 5. 制御端末の情報を改ざん
インターネット	サーバ	1. インターネット経由で不正アクセス 2. サーバに感染拡大（脆弱性利用） 3. サーバ内の情報を改ざん
インターネット	制御対象装置	1. インターネット経由で不正アクセス 2. 制御対象装置に対し DoS 攻撃

表 5　サンプルシステムへの適用結果

		提案手法での導出	
		有	無
人手での導出	有	486	0
	無	164	1,086

4.3 考察

本手法では technique の組み合わせを考慮することにより，複数の脅威イベントを引き起こし得る technique が含まれる場合の脅威イベント導出精度を向上させることができたが，対応できなかった technique も存在した．

例えば，任意のコマンドやスクリプト等の実行に用いられる technique“Command and Scripting Interpreter”は任意の脅威イベントに繋がる可能性がある．そのため，他の technique との組み合わせを考慮しても導出される脅威を絞り込むことが難しい．今回作成した脅威イベント導出ルールでは暫定的に“Command and Scripting Interpreter”から「情報漏えい」「改ざん」を導出することとしているが，このような technique が上記評価における誤差の主な原因となっている．従って，マルウェアが引き起こす脅威に絞り込んで特定するためには，マルウェアが実際に実行したコード・スクリプト等に関する情報など，ATT&CK 以外の情報源を用いる必要があると考えられる．

また，表 3 に示したとおり，PowerShower による「認証情報の調査」が脅威イベント導出ルールによって導出されていない．これは，PowerShower が用いる technique の中に認証情報の調査に直接的に繋がるものが存在しなかったためである．一方で，PowerShower はシステムのユーザを特定する technique である“System Owner/User Discovery”を用いており，この technique は認証情報の調査の準備として用いられる可能性がある．しかし，“System Owner/User Discovery”から直接「認証情報の調査」を導出して良いかどうかは，他のマルウェアに適用した場合の精度を考慮しながら検討する必要がある．

本手法では情報源として ATT&CK for Enterprise を用いているが，制御システムに特化したマルウェアが掲載されていない場合がある．また，マルウェアによる technique のリストはセキュリティベンダなどによる公開情報を元に作成されているため，新しく出現したばかりのマルウェアへの対処には適さない．従って，対処可能なマルウェアの拡大には，制御システム向けマトリクスである ATT&CK for ICS や，マルウェアの挙動を ATT&CK の technique ベースで出力する機能を持つマルウェア解析サービス ANY.RUN[14]など，他の情報源を併用する必要がある．

5. まとめと今後の課題

本稿では，制御システムに対し導出された脅威のうちマルウェアが引き起こすものを特定するため，マルウェアが用いる ATT&CK の technique から脅威を導出する手法を構築した．複数のマルウェアに対し適用した結果，人手で特定した脅威イベントの 96%が導出されることを確認した．本手法の課題として，ATT&CK for ICS 等の情報源の活用による対応可能なマルウェアの拡大，より多くのマルウェアに対する評価を通した脅威イベント導出ルールの精度向上が挙げられる．

参考文献

[1] ICS-CERT: ICS-CERT Year in Review 2016, available from 〈https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf〉(accessed 2021-03-29).
[2] 福原聡，岡下博子：制御システムのセキュリティ　～サイバー攻撃の現状とリスク分析のすすめ～，入手先〈https://www.ipa.go.jp/files/000070062.pdf〉（参照 2021-3-20）.
[3] 独立行政法人情報処理推進機構：制御システムのセキュリティリスク分析ガイド補足資料 制御システム関連のサイバーインシデント事例 7　～2020 年 医療関連企業のランサムウェアによる業務停止～，入手先〈https://www.ipa.go.jp/files/000085318.pdf〉（参照 2021-03-30）.
[4] Microsoft: STRIDE chart, available from 〈https://www.microsoft.com/security/blog/2007/09/11/stride-chart/〉(accessed 2021-03-26).
[5] 公益社団法人自動車技術会：自動車の情報セキュリティ分析ガイド，JASO TP-15002（2015）.
[6] Microsoft: Threat modelling for drivers, available from 〈https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers〉(accessed: 2021-03-30).
[7] 小柳洋貴，寶木和夫，三科雄介，梅澤克之：脆弱性データベースを使用した脅威分析方法－LDA 分類器とコサイン類似度を用いたトピックモデル分析による攻撃事例と大規模脆弱性 DB の突合について－，情報処理学会研究報告，Vol.2020-DPS-182，No.38，pp.1-6（2020）.
[8] 小柳洋貴，寶木和夫，三科雄介，梅澤克之：脆弱性データベースを使用した脅威分析－トピックモデル分析による攻撃事例と大規模脆弱性 DB の突合手法の複数事例への適用－，情報処理学会研究報告，Vol.2020-CSEC-90，No.16，pp.1-6（2020）.
[9] MITRE: MITRE ATT&CK®, available from 〈https://attack.mitre.org/〉(accessed: 2021-03-30).
[10] MITRE: ATT&CK® for Industrial Control Systems, available from 〈https://collaborate.mitre.org/attackics/index.php/Main_Page〉(accessed 2021-04-02).
[11] MITRE: WannaCry, Software S0366 | MITRE ATT&CK®, available from 〈https://attack.mitre.org/software/S0366/〉(accessed 2021-04-07).
[12] 太田原千秋，内山宏樹，井口慎也，萱島信：社会インフラシステムを対象としたテンプレート型セキュリティ対策立案手

Vol.2021-CSEC-93 No.11
Vol.2021-IOT-53 No.11
2021/5/13

法の提案，情報処理学会論文誌，Vol.58，No.9，pp.1523-1534（2017）.

[13] 独立行政法人情報処理推進機構：制御システムのセキュリティリスク分析ガイド補足資料 制御システム関連のサイバーインシデント事例 2　～2016 年 ウクライナ マルウェアによる停電，入手先〈https://www.ipa.go.jp/files/000076756.pdf〉（参照 2021-03-29）.

[14] ANY.RUN: MITRE ATT&CK: The Most Comprehensive Behavior Database, available from〈https://any.run/cybersecurity-blog/mitre-attack/〉(accessed 2021-03-30).