情報処理学会論文誌 Vol.61 No.12 1802–1813 (Dec. 2020)

SoK：データ駆動型社会に向けたセキュリティ分野へのオントロジの活用に関する一考察

古川 凌也[1,2,a)] 白石 善明[2] 森井 昌克[2]

受付日 2020年3月9日, 採録日 2020年9月10日

概要：データ駆動型社会に向けて新たな技術の開発が進められる一方で，攻撃サーフェイスの拡大やデータ収集に関するプライバシ上の懸念など，解決すべきサイバーセキュリティ上のリスクや課題が議論されている．本論文では，そのような課題の解決に向け，オントロジを活用した手法による研究の方向性を考察する．その際，NICE Framework から抽出したサイバーセキュリティの機能と利用目的に基づき既存研究の分類と調査を行い，各課題に対して適用可能なアプローチを整理した．サイバーセキュリティ分野においてオントロジは汎用的に活用されており，幅広い課題の解決につながる発展性を示している．

キーワード：データ駆動型社会，オントロジ，NICE Framework，CPS，AI，プライバシ

SoK: Ontology Utilization in Security Field towards Data-driven Society

Ryoya Furukawa[1,2,a)] Yoshiaki Shiraishi[2] Masakatu Morii[2]

Received: March 9, 2020, Accepted: September 10, 2020

Abstract: While new technologies are being developed for a data-driven society, there are many cybersecurity risks and challenges with respect to the expansion of attack surfaces and privacy concerns about data collection. In this paper, we discuss the direction of research using ontology to address the challenges. We classify and survey the existing researches based on the functions and purposes in cybersecurity that extracted from the NICE Framework and organize the approaches applicable to each challenge. Ontology is widely used in the field of cybersecurity, and it shows the potential of research to solve a wide range of problems.

Keywords: data-driven society, ontology, NICE framework, cyber-physical system, artificial intelligence, privacy

1. はじめに

データ駆動型社会の実現に向けた取り組みが進んでいる．ドイツの「Industry 4.0」や中国の「中国製造 2025」に続き，日本でも「Society5.0」が提唱され，各国がデータの利活用による経済成長や社会的課題の解決を目指した国家プロジェクトを推進している．データ駆動型社会における「データドリブン」の定義は様々であるが，大規模に収集されたデータから意味のある情報を抽出し，定量的な事実に基づいた意思決定やプロセスの改善に利用することが基本となる．たとえば，Society5.0 の基盤とされているサイバーフィジカルシステム（CPS）は，現実世界（フィジカル空間）でセンサなどによって観測された膨大なデータをサイバー空間で監視，分析し，得られた情報や知識をもとに物理システムを制御するなどによって，より良い結果につながるアクションを現実世界にフィードバックする [1]．

新たな技術の開発が進められる一方で，解決すべきサイバーセキュリティ上のリスクや多くの課題がある．CPS では，物理システムがインターネットに接続されることによ

[1] デロイトトーマツサイバー合同会社
Deloitte Tohmatsu Cyber LLC, Chiyoda, Tokyo 100–0005, Japan
[2] 神戸大学
Kobe University, Kobe, Hyogo 657–8501, Japan
[a)] ryoya.furukawa.2@gmail.com

© 2020 Information Processing Society of Japan

る攻撃サーフェイスの拡大が懸念されている [2]．また，積極的なデータ収集・連携においては，個人情報の保護やプライバシの確保，法整備や関連する法規制への対処も必要になる [3]．

そうした課題に対応していくために，データ駆動型社会にサイバーセキュリティの機能を実装する必要がある．サイバーセキュリティ分野における様々な役割や業務，それらに求められる知識や能力などが体系的に定義されたフレームワークとして，National initiative for cybersecurity education cybersecurity workforce framework（NICE Framework）[4] がある．NICE Framework には，既存の業務からみたサイバーセキュリティの機能と利用目的が網羅されており，データ駆動型社会における課題の解決に向けたアプローチを機能別に整理するうえでの 1 つの切り口となる．

本論文では，データ駆動型社会におけるサイバーセキュリティの課題について，オントロジを使用した研究の方向性を考察する．その際，オントロジを活用したサイバーセキュリティ分野の既存研究について，NICE Framework から抽出したサイバーセキュリティ機能の利用目的に基づく分類と調査を行い，取り組むべき課題について議論するうえでの手がかりとした．

本論文の主な貢献は以下のとおりである．

- サイバーセキュリティにおける利用目的に基づく既存研究の分類と調査を行い，オントロジを活用した手法の汎用性を示した．
- データ駆動型社会に向けたサイバーセキュリティ上の課題について，サイバーセキュリティの機能や利用目的の観点から研究の方向性を考察し，オントロジを活用した手法の発展性を示した．

本論文の構成は以下のとおりである．2 章では，一般的なオントロジの定義や関連技術，利用例について述べる．次に 3 章ではオントロジを活用したサイバーセキュリティ分野の関連研究について，これまでの研究動向を調査した結果について述べる．4 章でデータ駆動型社会におけるオントロジを利用したサイバーセキュリティ研究の今後の展望について考察し，5 章でまとめを述べる．

2. オントロジの導入

本章では，オントロジの定義や利用例について述べる．

2.1 オントロジの定義

オントロジは哲学において存在を体系的に説明する存在論を指すが，情報科学の分野ではこれを借用し，「概念化の明示的仕様」と定義されている [5], [6]．ある現象について関連する概念を特定し，それらの概念に型やプロパティ，関係性といった制約を与えることで意味論的な解釈を可能にするものであり，主にセマンティック Web や人工知能の分野で活用されている [7], [8], [9], [10], [11]．一般的に Web Ontology Language（OWL）と呼ばれる記述論理に基づいた RDF 形式のファイルとして記述，保存される [12]．

2.2 オントロジの利用例

オントロジのいくつかの具体的な利用例を述べる．

(1) 標準化・相互運用性の確保

データ形式や通信プロトコルを制定するにあたってオントロジを構築することがある．異なるデータソースや通信機器の連携が必要な場合に，それぞれに存在する概念を明確に定義した共通の語彙体系を構築し，橋渡しを行うことで，相互運用性を高めることができる [13]．異なる種類の医療デバイスから収集されたデータを共通の疾患データベースに統合する研究や，共通のデータ仕様を持たない IoT デバイスとプラットフォームを接続する研究などが行われているほか，センサネットワークに関する各種の概念を統合するオントロジが提案されている [14], [15], [16]．

(2) 推論による認識・識別

オントロジに定義された概念間の関係性や制約をもとに，論理推論やルールベースの判定，識別を行うことができる．記述論理に基づく一般的な推論タスクの実行には，既存の推論エンジンを利用することができる [17], [18]．車両センサが認識したオブジェクトや収集した地図情報をもとに，オントロジに基づく論理推論を行うことで道路状況を認識することで歩行者の振舞いを予測する運転支援システムの研究や，スマートホームに配置したセンサネットワークの状態から居住者のアクティビティをリアルタイムで認識し，生活支援を行う研究などが行われている [19], [20]．

(3) 検索・レコメンデーション

検索対象のコンテンツにオントロジに基づいたアノテーションをメタデータとして付与することで，意味論的な類似度に基づいた検索結果の拡張や精度の向上が可能になる [21]．またレコメンデーションシステムを構築するアプローチの中にオントロジベースの手法があり，従来手法と組み合わせることでコールドスタートやスパース性といった問題の影響を軽減できることが示されており，e-learning システムの分野などで研究されている [22]．

3. サイバーセキュリティ分野におけるオントロジの活用の利用目的に基づく分類

サイバーセキュリティ分野においてオントロジがどのように活用されているのかを把握するために，オントロジを活用したサイバーセキュリティに関する既存研究を調査した．まず，サイバーセキュリティ分野におけるオントロジについてのサーベイ論文を収集し，主要な研究領域と関連研究を特定した．次に，NICE Framework から抽出したサイバーセキュリティ機能に基づいて既存研究を分類し，サイバーセキュリティ分野におけるオントロジの活用を利用

© 2020 Information Processing Society of Japan

表 1 既存のサーベイ論文の対象領域
Table 1 Target areas of existing surveys.

サーベイ論文	対象領域
[23], [24], [25]	セキュリティオントロジ全般
[26]	セキュリティ要件エンジニアリング
[27]	クラウド環境のセキュリティ運用
[28]	標的型攻撃の検知・分析
[29]	セキュリティ評価
[30]	ネットワークセキュリティ
[31]	脅威インテリジェンス

目的別に整理した．そして，利用目的別の分類をもとに複数の文献データベースを検索することで，既存のサーベイ論文にカバーされていない関連研究を補完的に収集し，分類ごとの研究動向をまとめた．

3.1 既存のサーベイ論文

Blanco らはセキュリティオントロジに関する主要な研究を体系的に分析する調査を行った [23], [24]．その後，Arbanas らは Blanco らの調査を拡張するものとしてセキュリティオントロジに関する研究の収集と分類を行った [25]．Souag らは，セキュリティ要件エンジニアリングへの応用に利用可能なセキュリティオントロジを調査した [26]．Singh はクラウドコンピューティング環境におけるセキュリティ運用を定義するオントロジの構築に向け，既存のセキュリティオントロジを調査した [27]．Luh らは，標的型攻撃の分析または検出に応用できる可能性の高いセマンティックな手法を用いた既存のセキュリティ研究を体系的に調査した [28]．Rosa らは，セキュリティ評価に関するオントロジの構築にむけて，研究動向の調査を行った [29]．Silva らは，ネットワークセキュリティに関するオントロジ研究を収集し，既存のオントロジがカバーする領域を特定した [30]．脅威インテリジェンスのモデルの構築のために利用可能な分類法，標準規格，オントロジについて調査した [31]．

既存のサーベイ論文が調査の前提または応用の対象としている領域を**表 1** にまとめる．文献 [23], [24], [25] では，セキュリティオントロジ全般を対象として調査が行われているが，特定の利用目的や応用を前提とした分類は行われていない．一方，文献 [26], [27], [28], [29], [30], [31] では利用目的や応用を前提とした調査が行われているが，対象は特定の領域に限定されており，サイバーセキュリティ分野における利用目的の全体は網羅されていない．

3.2 セキュリティオントロジ研究の分類

サイバーセキュリティに関するオントロジは大きく分けて General と Specific に分類される．Specific オントロジは，その利用目的に応じてある限られた領域の知識体系を表現することに特化したオントロジを指す．既存のサーベイ論文の分類に基づいた対象領域の例を**表 2** に示す [23], [24], [25], [26], [27]．一方，General オントロジはサイバーセキュリティドメインの知識全般を包含した汎用的に利用可能な知識ベースであり，Specific オントロジを統合するものとして研究がなされている [32], [33], [34]．既存のサーベイ論文における General や Specific といった分類は，オントロジが対象とする知識領域に基づいた一般的な分類であるといえる．しかしながら，表 2 に示されている，対象領域を表すキーワードのみでは，オントロジがサイバーセキュリティ分野の各知識領域において，どのように活用されるのかが具体的ではない．

表 2 Specific オントロジの対象領域の例
Table 2 Examples of specific ontologies.

Access Control; Application Based Security; Auditing; BRAC; Business Impact Analysis; Cloud Computing; Conversation Policies; Human Factor; Security Education; Information Security Metrics; Intrusions; Mobile Applications; Network Security; Physical Security; Policy-Based Network; QoS Constraints; Reliability; Risk Based Security; Security Attacks; Security Incidents; Security Reconfiguration; Security Requirements; Security Standards; Social Aspects; Software Development; VoIP Services; Vulnerabilities; Web Application Security; Web Services Attacks; WS and OWL Based;

そこで本論文では，サイバーセキュリティ分野におけるオントロジの有用性をより具体的に示すために，アプリケーションとしての利用目的に着目した分類と調査を行った．利用目的の分類にあたっては，NICE Framework におけるカテゴリ，専門領域，職種に関する記述を参考とした．なお，NICE Framework には類似の目的の業務が複数のカテゴリにまたがって要求される場合や，同一のカテゴリであっても目的の異なる業務が定義される場合があり，NICE Framework に定義されるカテゴリと本論文の分類は必ずしも 1 対 1 に対応するものではない．本論文の分類と NICE Framework の各カテゴリにおける記述との対応付けを**図 1** に示す．

さらに本論文では，カテゴリごとに関連するキーワードをもとに文献データベースを検索し，補完的に関連研究を収集した．なお，検索エンジンには主に Google Scholar を使用し，以下のような検索クエリを実行した．

- Ontology OR ontologies security requirement
- Ontology OR ontologies security “attack detection”

収集した関連研究の一覧を**表 3** にまとめる．以下，表 3 に示すカテゴリごとに既存研究の具体例を説明する．

(1) セキュリティ・マネジメント

組織におけるセキュリティ戦略やポリシの策定といったセキュリティ・マネジメントの領域に応用する目的で研究

© 2020 Information Processing Society of Japan

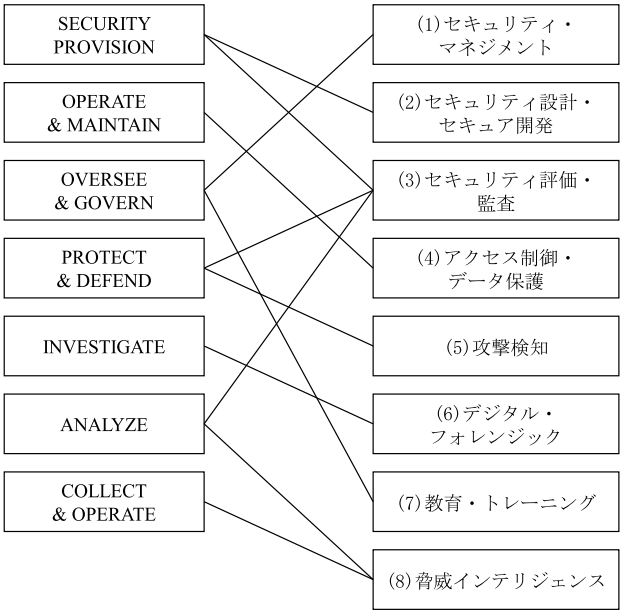


図 1 NICE Framework に定義されるカテゴリと本論文におけるサイバーセキュリティ上の利用目的との対応関係

Fig. 1 Mapping between categories defined in the NICE framework and purpose of use in cybersecurity field.

表 3 サイバーセキュリティ分野における利用目的に基づいた既存研究の分類

Table 3 Classification of existing research based on purpose of use in cybersecurity field.

番号	カテゴリ	関連研究
(1)	セキュリティ・マネジメント	[35], [36], [37], [38], [39]
(2)	セキュリティ設計・セキュア開発	[40], [41], [42], [43], [44], [45]
(3)	セキュリティ評価・監査	[46], [47], [48], [49], [50], [51]
(4)	アクセス制御・データ保護	[52], [53], [54], [55], [56], [57], [58]
(5)	攻撃検知	[59], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76]
(6)	デジタル・フォレンジック	[77], [78], [79], [80], [81]
(7)	教育・トレーニング	[82], [83], [84], [85], [86]
(8)	脅威インテリジェンス	[32], [33], [34]

がなされている [35]．オントロジは，組織のセキュリティに関するエコシステム全体を表す概念（脅威，脆弱性，資産など）で構成され，セキュリティ施策の費用対効果や，脅威が組織に及ぼす影響の分析に用いられる [36], [37], [38]．また，ISO 27001，PCI DSS，ISSA 5173，NISTIR 7621 といったセキュリティ標準をオントロジで表現し，可視化することによって，組織のポリシ策定を支援する研究も行われている [39]．

(2) セキュリティ設計・セキュア開発

攻撃シナリオや脆弱性をオントロジによって形式的に記述し，脅威を防止するためのセキュリティ要件を分析することで，ネットワークの構築やアプリケーションの開発に利用する研究がなされている [40]．セキュリティ要件に関する知識を体系的に定義したオントロジをソフトウェア設計のフレームワークとして利用することで，セキュリティの知識を持たない技術者によるセキュア開発を支援することができる [41], [42]．また，モバイルアプリや Web アプリ，クラウド環境といった特定の領域におけるセキュリティ要件を明確化することで，あまり経験のない領域で技術者が設計や開発を行う場合であっても，脆弱性が作りこまれることを防止することができる [43], [44], [45]．

(3) セキュリティ評価・監査

オントロジに基づいた攻撃モデルを構築し，攻撃の側面からセキュリティ評価のためのフレームワークを提示する研究や，オントロジに基づいた論理的推論によって，対象のネットワークに有効な攻撃経路を特定する研究がある [46], [47]．また，CAPEC や CWE といったオープンソースのセキュリティ評価指標を組み込んだオントロジを用いて，クエリベースで組織のセキュリティレベルの評価を行う研究もなされている [48]．攻撃や脅威，脆弱性などの概念を定義したセキュリティオントロジに ISO27001 といったセキュリティ標準を統合することで，組織のセキュリティ評価やシステム監査の支援を行う研究が行われている [49], [50], [51]．

(4) アクセス制御・データ保護

セキュリティポリシに関するアクセス制御モデルをオントロジで記述し，推論エンジンを適用することで，セキュリティポリシ仕様の柔軟性を高めるとともに動的なアクセス制御を行う研究がなされている [52], [53]．プライバシ情報の利用に関する設定をオントロジに基づいて記述し，ユーザとアプリケーションやサービスの間でプライバシ情報の開示，利用の可否を判断する研究がある [54], [55], [56]．また，Web サービスのプライバシポリシや GDPR といった法規制に関する概念をオントロジで表現し，プライバシポリシに記述されている文言のセマンティックな分析や，組織の運用における個人データの取扱いについて動的なコンプライアンスチェックを行う研究が行われている [57], [58]．

© 2020 Information Processing Society of Japan

(5) 攻撃検知

ネットワーク上の通信ログやIDSの出力するアラートを既知の攻撃手法に含まれるアクティビティの特徴などをモデル化したオントロジに対応付け，関連性の高いログやアラートのみを抽出することで，攻撃の検出精度を向上させる研究や，シグネチャで検出できないゼロデイ攻撃にも対応しようとする研究がある [59], [60], [61], [62]．また，マルウェアの振舞いをオントロジとしてモデル化し，ホスト上のプロセスやサービスの挙動と突き合わせることで，未知のマルウェアを検出する研究がある [63], [64], [65], [66], [67]．さらに，組織のネットワークに分散した異種のデータソースを共通のオントロジを介して統合し，セキュリティに関するイベントを抽出することで，複雑な攻撃や標的型攻撃の検知を支援する研究がなされている [68], [69], [70], [71]．

スパムメール対策の分野では，オントロジベースの分類ルールを構成し，スパムメールのフィルタリングをユーザごとにカスタマイズ可能にすることで，ユーザにとって有用なメールがスパムとして誤検出されることを防止する研究がある [72], [73], [74]．モバイル端末のSMSにおけるスパムメッセージやTwitterにおけるスパムツイートをオントロジベースで検出する方法も研究されている [75], [76]．

(6) デジタル・フォレンジック

デジタル・フォレンジックの分野では，発見された証拠データやマルウェアの動作を関連する法律や犯罪と関連付けることで，フォレンジック調査の支援やサイバー犯罪の立証を支援する研究がある [77], [78]．また，フォレンジック調査によって特定された証拠データを適切に管理するために，事前に構築したオントロジに基づいて証拠データにアノテーションを行う研究がなされている [79], [80]．デジタル・フォレンジックに関するドメイン知識全般を体系化する研究も行われている [81]．

(7) 教育・トレーニング

サイバーセキュリティに関する教育やトレーニングの分野でもオントロジを用いたアプローチが研究されており，学習カリキュラムや教材の整備，e-Learningシステムの構築を行う研究がなされている [82], [83], [84], [85], [86]．

(8) 脅威インテリジェンス

脅威インテリジェンスは，資産に対する既存，または新たな脅威に関する知識のことであり，脅威インテリジェンスの収集と分析は，サイバーセキュリティ分野における重要なタスクの1つとされる [31]．脅威インテリジェンスの表現にオントロジを用いることで，情報共有の標準化や分析の自動化に役立てられるが，この目的の達成にはサイバーセキュリティ分野の広い範囲の知識を包含，または統合するGeneralなオントロジが求められる．既存の複数の脅威インテリジェンスモデルを表現，または統合するための研究がなされている [32], [33], [34]．

表 4 既存のサーベイ論文におけるオントロジの対象領域と本論文における分類との対応付け

Table 4 Mapping of target areas of ontologies in existing surveys to our classification.

	(1) セキュリティ・マネジメント	(2) セキュリティ設計・セキュア開発	(3) セキュリティ評価・監査	(4) アクセス制御・データ保護	(5) 攻撃検知	(6) デジタル・フォレンジック	(7) 教育・トレーニング	(8) 脅威インテリジェンス
Access Control				✓				
Application Based Security		✓		✓	✓			
Auditing			✓					
BRAC				✓				
Business Impact Analysis	✓							
Cloud Computing		✓	✓	✓				
Conversation Policies				✓				
Human Factor	✓							
Security Education							✓	
Information Security Metrics		✓						
Intrusions					✓			
Mobile Applications		✓						
Network Security	✓	✓	✓		✓			✓
Physical Security	✓	✓	✓					
Policy-Based Network				✓				
QoS Constraints				✓				
Reliability				✓				
Risk Based Security	✓		✓					
Security Attacks			✓		✓			✓
Security Incidents					✓			✓
Security Reconfiguration	✓	✓		✓				
Security Requirements		✓	✓					
Security Standards	✓	✓	✓					
Social Aspects		✓						
Software Development		✓						
VoIP Services			✓		✓			
Vulnerabilities	✓	✓						✓
Web Application Security		✓			✓			
Web Services Attacks;					✓			
WS and OWL Based	✓			✓	✓			✓
General								✓

© 2020 Information Processing Society of Japan

3.3 まとめ

本章では，オントロジのサイバーセキュリティ分野における活用をより具体的に示すために，図 1 の NICE Framework から抽出したサイバーセキュリティ機能の利用目的別の分類に基づき，オントロジの既存研究を整理した．表 2 に示すように，既存のサーベイ論文におけるオントロジの対象領域を表すキーワードのみではサイバーセキュリティ分野におけるオントロジの具体的な利用目的の全体像は明らかではなかった．しかしながら，表 3 に示すように，それぞれの利用目的において関連する既存研究が存在し，サイバーセキュリティの各機能において汎用的にオントロジが活用されていることが分かった．

既存のサーベイ論文において示されているオントロジの対象領域と本論文における分類との対応を**表 4** に示す．表の左端列は表 2 に示すオントロジの対象領域を表すキーワードに対応している．NICE Framework においてデジタル・フォレンジックは INVESTIGATE カテゴリの専門領域として定義されているが，既存のサーベイ論文では調査の対象とされていなかった．本論文の追加調査により，既存のサーベイ論文でカバーされていない領域にもサイバーセキュリティ分野においてオントロジを活用する関連研究を特定することができた．

なお，本調査における利用目的に基づく分類の制限事項として，オントロジは必ずしも特定のアプリケーションや利用目的に用途を限定して作成されるとは限らず，汎用的に利用される知識ベースとして作成されることも多くあるため，関連研究のオントロジには本論文での分類における利用目的以外のユースケースが存在する場合もある．

4. 今後の展望についての考察

本章では，データ駆動型社会におけるサイバーセキュリティ上の課題について，3 章で調査したオントロジの利用目的と関連づけながら研究の方向性を考察する．

データ駆動型社会では，データの収集，分析，利用のための基盤として，CPS によるフィジカル空間とサイバー空間の融合，および人工知能（AI）関連技術の活用があげられている [1]．しかしながら，CPS によってネットワークに接続された物理デバイスや AI システムの利用が増加すると新たなサイバー攻撃の標的になりうる．また，サイバーセキュリティの対象範囲が広がることによって企業や組織が直面する課題として，サイバーセキュリティ人材の不足がある [87]．ネットワークや組み込みシステム，OT（Operational Technology）および IT など複数領域にまたがる専門知識が求められることになり，必要な人材の確保がより困難になると考えられる．さらに，データ駆動型社会では，大量のデータ収集が前提となっており，その中には個人情報や行動履歴などのパーソナルデータが含まれる場合がある．そういったパーソナルデータの取扱いに関して，プライバシ保護や法整備に関する議論がなされている [3]．以上をふまえ，本論文では，CPS の脆弱性管理，AI システムに対する攻撃，サイバーセキュリティ人材の不足，プライバシ保護や法規制への対応の 4 つを主な課題として定め，3 章における利用目的による分類から適用可能なアプローチと研究の方向性を検討する．その中で，3 章の調査では収集されなかったものを含め，各課題の対象領域や研究の方向性に関連する既存研究を示す．

4.1 CPS の脆弱性管理

スマートグリッド，ICS，配送システム，医療システム，スマートカーなど，多くの施設や製品が CPS の側面を持つようになり，今まで脅威にさらされなかった産業システムや製品がサイバー攻撃の標的となる可能性がある．また，フィジカル空間へのアクセスを持つという性質から，攻撃によるインパクトは重大なものになりやすい．Humayed らは，CPS に脆弱性を持たせる主な要因として，以下の 3 つを示している [2]．

- 従来の物理システムは外部から隔離されていることを前提とし，セキュリティよりも安定動作や信頼性のみに焦点が当てられてきたこと．
- これまでの前提に反し，CPS における物理システムは，外部との接続性が高まる傾向にあること．
- CPS はマルチベンダシステムとして，複数のコンポーネントを統合することで構築され，コンポーネントごとに固有の脆弱性や相互作用による予期しないバグが発生する可能性があること．

以上から，接続されるコンポーネントのセキュリティを確保することや，システム全体の脆弱性の有無を継続的に把握することが課題となる．これらの課題に対応するオントロジの活用として，「(2) セキュリティ開発・セキュア設計」，「(3) セキュリティ評価・監査」のアプローチが応用できると考えられる．具体的には，CPS のコンポーネントに求められるセキュリティ要件をオントロジベースで明確化し，システム構築時に脆弱性が作りこまれないようにしたり，システム全体に有効な攻撃パスや関連する脆弱性などをオントロジでモデル化してアセスメントに利用したりするなどの方向性が考えられる．その際，「(8) 脅威インテリジェンス」に関連して，最新の脅威情報を収集，共有できるようなオントロジベースのシステムを開発することも考えられる．また，最近の研究では，CPS の特定の領域におけるセキュリティを対象としたオントロジの研究もなされており，SCADA などの制御システムを標的とする攻撃をモデル化する研究がある [88], [89]．

4.2 AI システムに対する攻撃

AI 関連技術は，データ駆動型社会の中心となる重要な要素とされているが，ディープラーニングをはじめとする機

© 2020 Information Processing Society of Japan

械学習による AI システムに対する攻撃手法が提案されている．AI システムに対する攻撃は主に以下の 3 タイプに分類される [90]．

Adversarial Input 意図的に誤識別を引き起こすために入力データを細工する．顔認証システムに対して別の人物に誤認識させる攻撃や，自動運転システムに対して道路標識を誤認させるような攻撃などが提案されている [91], [92]．

Data Poisoning 学習データを汚染することによって，AI システムのアウトプットをコントロールする．e-commerce などのレコメンデーションシステムの信頼性を低下させる攻撃や，市場予測をコントロールするような攻撃モデルが提案されている [93], [94]．

Model-stealing attacks 学習データに関する情報や学習モデルを復元し，盗用する．機械学習 API の出力結果をもとに攻撃者のモデルを調整し，対象の学習モデルを再現する手法や，特定のユーザ情報が学習データ内に存在するかを判断するような攻撃が提案されている [95], [96]．

Adversarial Input や Data Poisoning のような攻撃によって自動運転車や物理システムが異常動作し，事故を引き起こすことを防止するためには，システムは単純に入力データを処理するのみではなく，自身や周囲の異常を認識できる必要がある．この課題に対して，「(5) 攻撃検知」のアプローチにおけるオントロジを用いた論理推論によるコンテクスト認識ベースの検知手法が応用できると考えられる．最近の研究では，オントロジに基づいて車両ネットワークの異常を検知し，攻撃を検出する研究がある [97]．また，攻撃検知を目的とした研究ではないが，コンテクスト認識や異常検知に関連する最近の研究として，工場における CPS のメンテナンスコストを抑えるために，オントロジを用いてシステムの異常動作を定義する研究や，スマートホームの居住者の異常状態をセンサとオントロジを用いたコンテクスト認識によって検出する研究などがある [98], [99]．

4.3 サイバーセキュリティ人材の不足

サイバーセキュリティのスキルを持つ人材は，世界中でおよそ 407 万人不足しているという調査がある [100]．データ駆動型社会では，以下の理由によりサイバーセキュリティに求められるスキルはより広範囲で複雑になると予想され，この問題は深刻化する可能性がある．

- ICT やデジタル技術が産業に深く入り込むことで，産業ドメインに特化したセキュリティの知識が必要とされる．
- プラットフォームやテクノロジが新たな攻撃のサーフェイスを生み，知識のアップデートが求められる．

サイバーセキュリティに関する知識やスキルの対象領域が増大することから，効果的な人材育成や雇用を行うために個々の組織において実際の業務に必要なスキルセットを具体化する必要がある．また，詳細なスキルセットに紐づけて人的リソースを管理することも重要になる．こうした課題に対しては，「(1) セキュリティ・マネジメント」，「(7) 教育・トレーニング」の利用目的に関するアプローチが活用できると考えられる．たとえば，人材育成においては，オントロジに基づいてサイバーセキュリティに関する知識体系を整理し，各個人に必要なスキルセットの範囲に応じて学習カリキュラムをカスタマイズすることが考えられる．また，各個人が持つ知識やスキルセットをオントロジで表現することができれば，業務と人材のマッチングや組織に不足する人的リソースの分析などに役立てることができる．関連する研究として，e-Learning やトレーニングの開発に活用するために，サイバー攻撃のパターンや防御メカニズムに対し，関係する知識やスキルを紐づけたオントロジの研究などがある [86]．

4.4 プライバシ保護や法規制への対応

センサなどから収集されるデータには，パーソナルデータに関するプライバシ上の懸念がある．たとえば，スマートメータなどのセンサが収集するデータには，各家庭の詳細なエネルギー消費のプロファイルが含まれる [101]．また欧州では，個人のプライバシの保護を目的とする一般データ保護規則（GDPR）が制定され，違反した場合には厳しい罰則が与えられる [102]．

データの収集と分析，活用が前提となるシステムの開発者やプラットフォームの管理者は，法令違反やプライバシ侵害を引き起こさないために，各種の法規制やプライバシ要件をふまえて設計や運用を行う必要がある．この課題に関し，「(4) アクセス制御・データ保護」におけるプライバシ保護に関するアプローチが利用できると考えられる．各種の法規制に紐づくプライバシ要件を体系化したオントロジを構築することで，プライバシを考慮したシステムの設計や運用を支援することができる [103]．また，「(6) デジタル・フォレンジック」における法律とマルウェアの動作をオントロジに基づいて関連付けるようなアプローチは，パーソナルデータの取扱いを各種法規制に紐づけて制御するために応用できる可能性がある [77], [78]．そのうえで，法規制に関する概念や個人データの取扱いに関する仕様を機械可読なオントロジとして記述するような研究は，システムがプライバシに関する情報をデータの中からセマンティックに解釈し，適切に処理するために重要になると考えられる [57], [58]．

5. おわりに

本論文では，データ駆動型社会におけるサイバーセキュリティ上の課題の解決に向け，オントロジを活用した手法による研究の方向性について考察した．オントロジは一般

© 2020 Information Processing Society of Japan

的に，仕様を明示的に記述することによる標準化の支援や相互運用性の確保，記述論理に基づく推論による認識や識別，コンテンツに関連性やメタデータを付与することによる検索結果の精度向上やカスタマイズなどに活用される．オントロジを活用した既存のセキュリティ研究を NICE Framework から抽出した利用目的別の分類に基づいて調査した結果，いずれの領域にも関連研究が存在し，サイバーセキュリティ分野においてオントロジが汎用的に活用されていることが分かった．また，データ駆動型社会におけるサイバーセキュリティ上の主な課題を利用目的別の分類と照らし合わせ，適用可能なアプローチから研究の方向性を考察した．3 章の調査で収集されなかったものも含め，課題の対象領域に関連する分野ですでに研究が存在することは，個別に具体的な研究を進めるうえでは対象領域ごとに関連するオントロジ研究をさらに調査する余地があると同時に，サイバーセキュリティ分野におけるオントロジを活用した研究は幅広い課題の解決につながる発展性を示している．

謝辞 本研究は国立研究開発法人情報通信研究機構の委託研究「機械学習に基づくサイバー攻撃情報分析基盤技術の研究開発」により行われた．

参考文献

[1] Society 5.0 — 科学技術政策 — 内閣府（オンライン），入手先 ⟨https://www8.cao.go.jp/cstp/society5_0/index.html⟩（参照 2020-03-07）．

[2] Humayed, A., Lin, J., Li, F. and Luo, B.: Cyber-Physical Systems Security – A Survey, *IEEE Internet of Things Journal*, Vol.4, No.6, pp.1802–1831 (Dec. 2017).

[3] Hernandez-Ramos, J.L., Geneiatakis, D., Kounelis, I., Steri, G. and Nai Fovino, I.: Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies, *IEEE Security Privacy*, Vol.18, No.1, pp.28–38 (2020).

[4] Newhouse, W., Keith, S., Scribner, B. and Witte, G.: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, National Institute of Standards and Technology, Gaithersburg, MD, DOI: 10.6028/NIST.SP.800-181 (2017).

[5] Gruber, T.R.: A translation approach to portable ontology specifications, *Knowledge Acquisition*, Vol.5, No.2, pp.199–221 (1993).

[6] Studer, R., Benjamins, V.R. and Fensel, D.: Knowledge engineering: Principles and methods, *Data Knowl. Eng.*, Vol.25, No.1, pp.161–197 (1998).

[7] Fensel, D., van Harmelen, F., Horrocks, I., McGuinness, D.L. and Patel-Schneider, P.F.: OIL: An ontology infrastructure for the Semantic Web, *IEEE Intell. Syst.*, Vol.16, No.2, pp.38–45 (2001).

[8] Doan, A., Madhavan, J., Domingos, P. and Halevy, A.: Learning to map between ontologies on the semantic web, *Proc. 11th International Conference on World Wide Web*, Honolulu, Hawaii, USA, pp.662–673 (2002).

[9] Maedche, A. and Staad, S.: Ontology Learning for the Semantic Web, *Intelligent Systems*, Vol.16, No.2, pp.1–18, IEEE (2005).

[10] Shadbolt, N., Berners-Lee, T. and Hall, W.: The Semantic Web Revisited, *IEEE Intell. Syst.*, Vol.21, No.3, pp.96–101 (2006).

[11] Ferrucci, D. et al.: Building Watson: An overview of the DeepQA project, *AI Magazine*, Vol.31, No.3, pp.59–79 (2010).

[12] Bechhofer, S. et al.: OWL web ontology language reference, *W3C recommendation*, Vol.10, No.2 (2004).

[13] Obrst, L.: Ontologies for semantically interoperable systems, *Proc. 12th International Conference on Information and Knowledge Management*, pp.366–369 (2003).

[14] Jabbar, S., Ullah, F., Khalid, S., Khan, M. and Han, K.: Semantic Interoperability in Heterogeneous IoT Infrastructure for Healthcare, *Proc. Int. Wirel. Commun. Mob. Comput. Conf.*, Vol.2017, DOI: 10.1155/2017/9731806 (2017).

[15] Desai, P., Sheth, A. and Anantharam, P.: Semantic Gateway as a Service Architecture for IoT Interoperability, *2015 IEEE International Conference on Mobile Services*, pp.313–319 (2015).

[16] Haller, A. et al.: The modular SSN ontology: A joint W3C and OGC standard specifying the semantics of sensors, observations, sampling, and actuation, *Semantic Web*, Vol.10, No.1, pp.9–32 (2019).

[17] Dentler, K., Cornet, R., ten Teije, A. and de Keizer, N.: Comparison of reasoners for large ontologies in the OWL 2 EL profile, *Semantic Web*, Vol.2, No.2, pp.71–87 (2011).

[18] Matentzoglu, N., Leo, J., Hudhra, V., Sattler, U. and Parsia, B.: A Survey of Current, Stand-alone OWL Reasoners, *ORE*, pp.68–79 (2015).

[19] Armand, A., Filliat, D. and Ibañez-Guzman, J.: Ontology-based context awareness for driving assistance systems, *Proc. 2014 IEEE Intelligent Vehicles Symposium*, pp.227–233 (2014).

[20] Chen, L., Nugent, C.D. and Wang, H.: A knowledge-driven approach to activity recognition in smart homes, *IEEE Trans. Knowl. Data Eng.*, Vol.24, No.6, pp.961–974 (2012).

[21] Fernández, M., Cantador, I., López, V., Vallet, D., Castells, P. and Motta, E.: Semantically enhanced Information Retrieval: An ontology-based approach, *Journal of Web Semantics*, Vol.9, No.4, pp.434–452 (2011).

[22] Tarus, J.K., Niu, Z. and Mustafa, G.: Knowledge-based recommendation: A review of ontology-based recommender systems for e-learning, *Artificial Intelligence Review*, Vol.50, No.1, pp.21–48 (2018).

[23] Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A. and Piattini, M.: A systematic review and comparison of security ontologies, *ARES 2008 – Proc. 3rd International Conference on Availability, Security, and Reliability*, No.June 2014, pp.813–820 (2008).

[24] Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R. and Toval, A.: Basis for an integrated security ontology according to a systematic review of existing proposals, *Comput. Stand. Interfaces*, Vol.33, No.4, pp.372–388 (2011).

[25] Arbanas, K. and Čubrilo, M.: Ontology in information security, *Journal of Information and Organizational Sciences*, Vol.39, No.2, pp.107–136 (2015).

[26] Souag, A., Salinesi, C. and Comyn-Wattiau, I.: Ontologies for security requirements: A literature survey and

© 2020 Information Processing Society of Japan

classification, *Lecture Notes in Business Information Processing*, Vol.112 LNBIP, No.October 2015, pp.61–69 (2012).
[27] Singh, V.: Revisiting Security Ontologies, *IJCSI International Journal of Computer Science Issues*, Vol.11, No.6, pp.150–159 (2014).
[28] Luh, R., Marschalek, S., Kaiser, M., Janicke, H. and Schrittwieser, S.: Semantics-aware detection of targeted attacks: A survey, *Journal of Computer Virology and Hacking Techniques*, Vol.13, No.1, pp.47–85 (2017).
[29] de Franco Rosa, F. and Jino, M.: A survey of security assessment ontologies, *Advances in Intelligent Systems and Computing*, Vol.569, pp.166–173 (2017).
[30] Silva, D.V. and Rafael, G.R.: Ontologies for network security and future challenges, *Proc. 12th International Conference on Cyber Warfare and Security, ICCWS 2017*, pp.541–547 (2017).
[31] Mavroeidis, V. and Bromander, S.: Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, *2017 European Intelligence and Security Informatics Conference* (*EISIC*), pp.91–98 (2017).
[32] Obrst, L., Chase, P. and Markeloff, R.: Developing an Ontology of the Cyber Security Domain, *STIDS*, pp.49–56 (2012).
[33] Iannacone, M. et al.: Developing an ontology for cyber security knowledge graphs, *Proc. 10th Annual Cyber and Information Security Research Conference*, pp.1–4 (2015).
[34] Syed, Z., Padia, A., Finin, T., Mathews, L. and Joshi, A.: UCO: A unified cybersecurity ontology, *Workshops at the Thirtieth AAAI Conference on Artificial Intelligence* (2016).
[35] Tsoumas, B. and Gritzalis, D.: Towards an ontology-based security management, *20th International Conference on Advanced Information Networking and Applications – Volume 1* (*AINA'06*), Vol.1, pp.985–992 (April 2006).
[36] Ekelhart, A., Fenz, S., Klemen, M. and Weippl, E.: Security ontologies: Improving quantitative risk analysis, *2007 40th Annual Hawaii International Conference on System Sciences* (*HICSS'07*), p.156a (Jan. 2007).
[37] Atighetchi, M., Simidchieva, B., Yaman, F., Eskridge, T., Carvalho, M. and Paltzer, N.: Using ontologies to quantify attack surfaces, *Proc. CEUR Workshop*, Vol.1788, pp.10–18 (2016).
[38] Fenz, S. and Ekelhart, A.: Formalizing information security knowledge, *Proc. 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09*, pp.183–194, ACM (2009).
[39] Ramanauskaite, S., Olifer, D., Goranin, N. and Cenys, A.: Security ontology for adaptive mapping of security standards, *International Journal of Computers, Communications & Control* (*IJCCC*), Vol.8, No.6, pp.813–825 (2013).
[40] Elahi, G., Yu, E. and Zannone, N.: A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations, *Conceptual Modeling – ER 2009*, pp.99–114 (2009).
[41] Velasco, J.L., Valencia-García, R., Fernández-Breis, J.T., Toval, A., et al.: Modelling reusable security requirements based on an ontology framework, *J. Res. Pract. Inf. Technol.*, Vol.41, No.2, p.119 (2009).
[42] Salini, P. and Kanmani, S.: A novel method: Ontology-based security requirements engineering framework, *2016 International Conference on Emerging Trends in Engineering, Technology and Science* (*ICETETS*), Pudukkottai, pp.1–5 (2016).
[43] Beji, S. and Kadhi, N.E.: Security ontology proposal for mobile applications, *2009 10th International Conference on Mobile Data Management: Systems, Services and Middleware*, pp.580–587 (May 2009).
[44] Salini, P. and Kanmani, S.: Ontology-based representation of reusable security requirements for developing secure web applications, *International Journal of Internet Technology and Secured Transactions*, Vol.5, No.1, pp.63–83 (2013).
[45] Bernsmed, K., Undheim, A., Meland, P.H. and Jaatun, M.G.: Towards an Ontology for Cloud Security Obligations, *2013 International Conference on Availability, Reliability and Security, Regensburg*, pp.577–581 (2013).
[46] Gao, J.-B., Zhang, B.-W., Chen, X.-H. and Luo, Z.: Ontology-based model of network and computer attacks for security assessment, *J. Shanghai Jiatong Univ.*, Vol.18, No.5, pp.554–562 (2013).
[47] Wu, S., Zhang, Y. and Cao, W.: Network security assessment using a semantic reasoning and graph based approach, *Comput. Electr. Eng.*, Vol.64, pp.96–109 (Nov. 2017).
[48] Doynikova, E., Fedorchenko, A. and Kotenko, I.: Ontology of metrics for cyber security assessment, *Proc. 14th International Conference on Availability, Reliability and Security*, pp.1–8 (2019).
[49] Fenz, S.: Ontology-based generation of IT-security metrics, *Proc. 2010 ACM Symposium on Applied Computing*, pp.1833–1839 (2010).
[50] Pereira, T. and Santos, H.: A Security Audit Framework to Manage Information System Security, *Global Security, Safety, and Sustainability*, pp.9–18 (2010).
[51] Fenz, S., Goluch, G., Ekelhart, A., Riedl, B. and Weippl, E.: Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard, *13th Pacific Rim International Symposium on Dependable Computing* (*PRDC 2007*), pp.381–388 (2007).
[52] Choi, C., Choi, J. and Kim, P.: Ontology-based access control model for security policy reasoning in cloud computing, *J. Supercomput.*, Vol.67, No.3, pp.711–722 (2014).
[53] Sharma, N.K. and Joshi, A.: Representing Attribute Based Access Control Policies in OWL, *2016 IEEE 10th International Conference on Semantic Computing* (*ICSC*), pp.333–336 (2016).
[54] Gao, F., He, J., Peng, S., Wu, X. and Liu, X.: An Approach for Privacy Protection Based-On Ontology, *2010 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing*, Vol.2, pp.397–400 (2010).
[55] Ciuciu, I., Claerhout, B., Schilders, L. and Meersman, R.: Ontology-Based Matching of Security Attributes for Personal Data Access in e-Health, *On the Move to Meaningful Internet Systems*: *OTM 2011*, pp.605–616 (2011).
[56] Yu, H., Sun, Y. and Hu, J.: An Ontology Based Privacy Protection Model for Third-Party Platform, *Active Media Technology*, pp.369–376 (2012).
[57] Oltramari, A. et al.: PrivOnto: A semantic framework for the analysis of privacy policies, *Semantic Web*, Vol.9, No.2, pp.185–203 (2018).
[58] Palmirani, M., Martoni, M., Rossi, A., Bartolini, C.

© 2020 Information Processing Society of Japan

and Robaldo, L.: PrOnto: Privacy Ontology for Legal Reasoning, *Electronic Government and the Information Systems Perspective*, pp.139–152 (2018).
[59] Sadighian, A., Fernandez, J.M., Lemay, A. and Zargar, S.T.: ONTIDS: A Highly Flexible Context-Aware and Ontology-Based Alert Correlation Framework, *Foundations and Practice of Security*, pp.161–177 (2014).
[60] Razzaq, A., Anwar, Z., Ahmad, H.F., Latif, K. and Munir, F.: Ontology for attack detection: An intelligent approach to web application security, *Comput. Secur.*, Vol.45, pp.124–146 (Sep. 2014).
[61] Karande, H.A. and Gupta, S.S.: Ontology based intrusion detection system for web application security, *2015 International Conference on Communication Networks* (*ICCN*), pp.228–232 (2015).
[62] Anusha, K. and Sathiyamoorthy, E.: OMAMIDS: Ontology Based Multi-Agent Model Intrusion Detection System for Detecting Web Service Attacks, *Journal of Applied Security Research*, Vol.11, No.4, pp.489–508 (2016).
[63] Huang, H., Chuang, T., Tsai, Y. and Lee, C.: Ontology-based intelligent system for malware behavioral analysis, *International Conference on Fuzzy Systems*, pp.1–6 (2010).
[64] Shabtai, A., Kanonov, U. and Elovici, Y.: Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method, *J. Syst. Softw.*, Vol.83, No.8, pp.1524–1537 (2010).
[65] Grégio, A., Bonacin, R., Nabuco, O., Afonso, V.M., Lício De Geus, P. and Jino, M.: Ontology for malware behavior: A core model proposal, *2014 IEEE 23rd International WETICE Conference*, pp.453–458 (2014).
[66] Grégio, A., Bonacin, R., de Marchi, A.C., Nabuco, O.F. and de Geus, P.L.: An ontology of suspicious software behavior, *Appl. Ontol.*, Vol.11, No.1, pp.29–49 (2016).
[67] Can, O., Unalir, M.O., Sezer, E., Bursa, O. and Erdogdu, B.: An Ontology Based Approach for Host Intrusion Detection Systems, *Metadata and Semantic Research*, pp.80–86 (2017).
[68] More, S., Matthews, M., Joshi, A. and Finin, T.: A Knowledge-Based Approach to Intrusion Detection Modeling, *2012 IEEE Symposium on Security and Privacy Workshops*, pp.75–81 (2012).
[69] Frye, L., Cheng, L. and Heflin, J.: An ontology-based system to identify complex network attacks, *2012 IEEE International Conference on Communications* (*ICC*), pp.6683–6688 (2012).
[70] Atighetchi, M., Griffith, J., Emmons, I., Mankins, D. and Guidorizzi, R.: Federated access to cyber observables for detection of targeted attacks (2014).
[71] Luh, R., Schrittwieser, S. and Marschalek, S.: TAON: An ontology-based approach to mitigating targeted attacks, *Proc. 18th International Conference on Information Integration and Web-based Applications and Services*, pp.303–312 (2016).
[72] Balakumar, M. and Vaidehi, V.: Ontology based classification and categorization of email, *2008 International Conference on Signal Processing, Communications and Networking*, pp.199–202 (2008).
[73] Youn, S.: SPONGY (SPam ONtoloGY): email classification using two-level dynamic ontology, *ScientificWorldJournal*, Vol.2014, p.414583 (Aug. 2014).
[74] Shoaib, M. and Farooq, M.: USpam – A User Centric Ontology Driven Spam Detection System, *2015 48th Hawaii International Conference on System Sciences*, pp.3661–3669 (2015).
[75] Cao, L., Nie, G. and Liu, P.: Ontology-based spam detection filtering system, *2011 International Conference on Business Management and Electronic Information*, Vol.3, pp.282–284 (2011).
[76] Halawi, B., Mourad, A., Otrok, H. and Damiani, E.: Few are as good as many: An ontology-based tweet spam detection approach, *IEEE Access*, Vol.6, pp.63890–63904 (2018).
[77] Park, H., Cho, S. and Kwon, H.-C.: Cyber Forensics Ontology for Cyber Criminal Investigation, *Forensics in Telecommunications, Information and Multimedia*, pp.160–165 (2009).
[78] Liu, J., Kammar, R., Sasaki, R. and Uehara, T.: Malware Behavior Ontology for Digital Evidence, *2017 IEEE International Conference on Software Quality, Reliability and Security Companion* (*QRS-C*), pp.585–586 (2017).
[79] Kahvedžić, D. and Kechadi, T.: Semantic Modelling of Digital Forensic Evidence, *Digital Forensics and Cyber Crime*, pp.149–156 (2011).
[80] Ćosić, J. and Ćosić, Z.: The necessity of developing a digital evidence ontology, *Proc. 23rd Central European Conference on Information and Intelligent Systems*, pp.325–230 (2012).
[81] Karie, N.M. and Venter, H.S.: Toward a general ontology for digital forensic disciplines, *J. Forensic Sci.*, Vol.59, No.5, pp.1231–1241 (2014).
[82] Takahashi, Y. et al.: An ontology-based e-learning system for network security, *19th International Conference on Advanced Information Networking and Applications* (*AINA'05*) Volume 1 (AINA papers), Vol.1, pp.197–202 (2005).
[83] Brinson, A., Robinson, A. and Rogers, M.: A cyber forensics ontology: Creating a new approach to studying cyber forensics, *Digital Investigation*, Vol.3, No.SUPPL., pp.37–43 (2006).
[84] Mangold, L.V.: Using Ontologies for Adaptive Information Security Training, *2012 7th International Conference on Availability, Reliability and Security*, pp.522–524 (2012).
[85] Modiba, N., Ojo, S. and Ncube, Z.: An Ontology Based Model for Cyber Security Awareness Education, *Proc. 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, Vol.12, pp.169–179 (2019).
[86] Katsantonis, M. and Mavridis, I.: Ontology-Based Modelling for Cyber Security E-Learning and Training, *Advances in Web-Based Learning – ICWL 2019*, pp.15–27 (2019).
[87] Industry 4.0 - Cybersecurity Challenges and Recommendations, [Online]. available from ⟨https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations⟩ (accessed 2020-06-24).
[88] Sartakov, V.A.: Ontological Representation of Networks for IDS in Cyber-Physical Systems, *Analysis of Images, Social Networks and Texts*, pp.421–430 (2015).
[89] Krauß, D. and Thomalla, C.: Ontology-based detection of cyber-attacks to SCADA-systems in critical infrastructures, *2016 6th International Conference on Digital Information and Communication Technology and its Applications* (*DICTAP*), pp.70–73 (2016).
[90] Bursztein, E.: Attacks against machine learning — an overview, Elie Bursztein's site, 30-May-2018 (online),

© 2020 Information Processing Society of Japan

available from ⟨https://www.elie.net/blog/ai/attacks-against-machine-learning-an-overview⟩ (accessed 2020-03-08).
[91] Kurakin, A., Goodfellow, I. and Bengio, S.: Adversarial examples in the physical world, arXiv [cs.CV] (2016).
[92] Evtimov, I. et al.: Robust physical-world attacks on deep learning models, arXiv preprint arXiv:1707.08945 (2017).
[93] Li, B., Wang, Y., Singh, A. and Vorobeychik, Y.: Data Poisoning Attacks on Factorization-Based Collaborative Filtering, *Advances in Neural Information Processing Systems 29*, pp.1885–1893, Curran Associates, Inc. (2016).
[94] Alfeld, S., Zhu, X. and Barford, P.: Data poisoning attacks against autoregressive models, *30th AAAI Conference on Artificial Intelligence* (2016).
[95] Tramèr, F., Zhang, F., Juels, A., Reiter, M.K. and Ristenpart, T.: Stealing machine learning models via prediction apis, *25th USENIX Security Symposium*, pp.601–618 (2016).
[96] Shokri, R., Stronati, M., Song, C. and Shmatikov, V.: Membership Inference Attacks Against Machine Learning Models, *2017 IEEE Symposium on Security and Privacy* (*SP*), pp.3–18 (2017).
[97] Sonntag, D., Zillner, S., van der Smagt, P. and Lörincz, A.: Overview of the CPS for Smart Factories Project: Deep Learning, Knowledge Acquisition, Anomaly Detection and Intelligent User Interfaces, *Industrial Internet of Things: Cybermanufacturing Systems*, Jeschke, S., Brecher, C., Song, H. and Rawat, D.B. (Eds.), Cham: Springer International Publishing, pp.487–504 (2017).
[98] Pardo, E., Espes, D. and Le Parc, P.: A framework for anomaly diagnosis in smart homes based on ontology, *The 7th International Conference on Ambient Systems, Networks and Technologies* (*ANT 2016*) (2016).
[99] Ricard, Q. and Owezarski, P.: Ontology Based Anomaly Detection for Cellular Vehicular Communications, *10th European Congress Embedded Real Time Systems* (2020).
[100] 2019 Cybersecurity Workforce Study (online), available from ⟨https://www.isc2.org/Research/Workforce-Study⟩ (accessed 2020-03-08).
[101] Ukil, A., Bandyopadhyay, S. and Pal, A.: IoT-Privacy: To be private or not to be private, *2014 IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), pp.123–124 (2014).
[102] Houser, K.A. and Voss, W.G.: GDPR: The end of Google and facebook or a new paradigm in data privacy, *Rich. JL & Tech.* (2018).
[103] Gharib, M., Giorgini, P. and Mylopoulos, J.: Towards an Ontology for Privacy Requirements via a Systematic Literature Review, *Conceptual Modeling*, pp.193–208 (2017).



古川 凌也 （学生会員）

デロイトトーマツサイバー合同会社サイバーセキュリティ先端研究所研究員．2015 年神戸大学工学部電気電子工学科卒業．2017 年同大学大学院博士課程前期課程修了．マルウェア解析や Android の脆弱性対策に興味を持つ．



白石 善明 （正会員）

1995 年愛媛大学工学部情報工学科卒業．1997 年同大学大学院博士前期課程修了．2000 年徳島大学大学院博士後期課程修了．博士（工学）．2002 年近畿大学理工学部情報学科講師．2006 年名古屋工業大学大学院情報工学専攻助教授．2013 年神戸大学大学院電気電子工学専攻准教授．2017 年同大数理・データサイエンスセンター兼任．2018 年より（株）国際電気通信基礎技術研究所客員研究員．情報セキュリティ，コンピュータネットワーク，教育支援，知識流通支援，機械学習に基づくサイバー攻撃分析等の研究・教育に従事．2002 年電子情報通信学会オフィスシステム研究賞，2003 年暗号と情報セキュリティシンポジウム（SCIS）20 周年記念賞，2006 年 SCIS 論文賞．2007，2008，2011，2013 年 DICOMO 優秀論文賞．2012 年電子情報通信学会ライフインテリジェンスとオフィス情報システム研究会功労賞．2015 年本会高度交通システム研究会優秀論文賞．2017 年電子情報通信学会関西支部活動功労賞．2017 年，2018 年電子情報通信学会情報通信システムセキュリティ研究専門委員会委員長．電子情報通信学会シニア会員．

© 2020 Information Processing Society of Japan



森井 昌克 （正会員）

1989 年大阪大学大学院工学研究科通信工学専攻博士課程修了．工学博士．同年京都工芸繊維大学工芸学部電子情報工学科助手，1990 年愛媛大学工学部情報工学科講師，1992 年同助教授，1995 年徳島大学工学部知能情報工学科教授，2005 年神戸大学工学部電気電子工学科教授．現在，同大学院工学研究科教授．主に代数的符号理論，離散数学，ディジタル信号処理アルゴリズム，情報セキュリティおよびコンピュータネットワーク等の研究・教育に従事．電子情報通信学会情報セキュリティ専門委員会，同ライフインテリジェンスとオフィス情報システム専門委員会，同情報通信システムセキュリティ専門委員会，各委員長を歴任．2007 年度電子情報通信学会功労賞，2010 年度 FIT 船井ベストペーパー賞，2013 年度電子情報通信学会論文賞，2020 年情報セキュリティ文化賞．電子情報通信学会フェロー．

© 2020 Information Processing Society of Japan