様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月 ２２ 日現在

機関番号：８２６２６
研究種目：若手研究(B)
研究期間：2017～2019
課題番号：１７Ｋ１２６６７

研究課題名（和文）統計手法と形式手法の融合によるサイバーフィジカルシステムの定量的検証

研究課題名（英文）Quantitative Verification of Cyber-Physical Systems by Integrating Statistical and Formal Approaches

研究代表者

川本　裕輔（Kawamoto, Yusuke）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：６０７６０００６

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：サイバーフィジカルシステム(CPS)の量的性質のモデル化・解析・検証技術およびその基礎理論について研究を行った。具体的には、プログラム解析と統計手法の融合により、プログラムからの情報漏洩量を推定するツールHyLeakを開発した。また、CPSからのプライバシ情報漏洩の定量化の基礎理論を研究し、ゲーム理論や差分プライバシを応用したプライバシ保護機構を提案し、CPSとして位置情報サービスを対象として、本研究の保護機構の有効性を実証した。さらに、統計手法と形式手法の融合により、統計的知識を記述できる様相論理StatELを提案し、CPS内部で用いられる機械学習モデルの統計的仕様の形式化手法を提案した。

研究成果の学術的意義や社会的意義
サイバーフィジカルシステム(CPS)の確率的な振る舞いをモデル化・解析・検証する上で、形式的アプローチと統計的アプローチの融合が有用であるということを様々な観点において明らかにした。具体的には、プログラム解析と統計手法の融合により、システムからの情報漏洩量の推定を高速化できることを示した。また、ゲーム理論と情報理論を組み合わせることで、適応的な攻撃者と防御者の下での情報漏洩のモデル化・解析を実現した。また、機械学習モデルを部品として用いるCPSの形式仕様を記述する手法を開発するために、統計的認識論理を導入し、機械学習モデルの統計的性質を論理式で形式化する手法を初めて提案した。

研究成果の概要（英文）：We studied theories and techniques for modeling, analyzing, and verifying quantitative properties of cyber-physical systems (CPSs). First, we developed HyLeak, a tool for estimating information leakage in programs by combining program analysis with statistical analysis. Second, we investigated quantitative models for privacy leakage in CPSs, proposed privacy protection mechanisms based on game theory and differential privacy, and demonstrated that the proposed mechanisms are effective for location-based services. Third, we introduced StatEL (statistical epistemic logic), a modal logic for describing statistical knowledge, and showed how this logic can be used to formalize the statistical specification of machine learning models used inside CPSs.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　プライバシ　システム検証　形式手法　定量的情報流解析　差分プライバシ　情報理論　様相論理

１．研究開始当初の背景

サイバーフィジカルシステム（CPS） は、センサやモニタなどのデバイスを通じて物理世界のデータを収集し、情報技術を用いて分析・活用する。CPS は、通信ネットワークを介して攻撃を受けやすく、脆弱性を悪用されると身体的危険や物理的破壊を引き起こすこともあるため、安全性や信頼性の解析・検証が不可欠である。特に、物理世界からの入力に応じて確率的に振る舞うため、システムの制御構造に基づく論理的な性質だけでなく、時間・空間などの量的性質や統計的性質を解析・検証する必要がある。

実用レベルまで発展してきた検証技術としては､形式手法(数理論理学を基礎とする検証手法)がある。しかし、形式手法を用いて CPS の量的性質や統計的性質を検証する場合、状態爆発のため、検証にかかる計算量は膨大である。そのため、形式手法を用いて検証できる CPS は小規模なものに限られる。また、CPS の統計的性質に関する仕様記述の手法は確立されておらず、特に、機械学習技術を利用する CPS が満たすべき統計的性質を論理式で記述する方法は提案されていない。

２．研究の目的

本研究の目的は、サイバーフィジカルシステム（CPS）の量的性質のモデル化・解析・検証技術およびその基礎理論を確立することである。具体的には、形式的アプローチと統計的アプローチを融合させることにより、従来手法で記述できない複雑な性質を論理式として記述する手法を提案する。また、下記の表に示す両アプローチの特性を生かすことにより、従来技術よりも高速に量的性質を解析・検証する手法を確立する。さらに、この手法を用いた解析・検証ツールを開発し、ツールを用いた実験により、提案技術の有効性を実証する。

	解析方法	検証の対象	検証結果	向いていない場合
形式手法	white-box	ソースコード	厳密	内部状態数が膨大、抽象化できない
統計手法	black-box	実行可能な実装	近似	実行時間が長い、観測値がスパース

３．研究の方法

サイバーフィジカルシステム(CPS)の量的性質のモデル化・解析・検証技術およびその基礎理論に関して、以下の研究を行った。まず、プログラム解析と統計手法の融合により、確率的プログラムからの情報漏洩量を推定する自動解析ツール HyLeak を開発した。また、CPS からのプライバシ情報漏洩の定量化のための基礎理論を構築し、ゲーム理論や差分プライバシを応用したプライバシ保護機構を提案し、CPS として位置情報サービスを対象として、これらの保護機構の有効性を実証した。さらに、統計的アプローチと形式的アプローチの融合により、統計的知識を記述できる様相論理 StatEL を提案し、CPS の部品として用いられる機械学習モデル等の統計的仕様を形式化する手法を提案した。

４．研究成果

サイバーフィジカルシステム(CPS)の確率的な振る舞いをモデル化・解析・検証する上で、形式的アプローチと統計的アプローチの融合が有用であることを、以下の研究成果を通じて明らかにした。

(1) 情報漏洩の量的性質の検証技術

複数の確率的システムから合成されたシステムの情報漏洩量の性質を定量的情報流解析（quantitative information flow）の枠組みで明らかにし、研究成果をまとめた論文を査読付き国際誌 Logical Methods in Computer Science で発表した。

また、確率的プログラムからの情報漏洩量を推定する自動解析ツール HyLeak を開発し、公開した。このツールでは、与えられたソースコードを解析し、指定した秘密変数から観測変数への情報漏洩量（相互情報量）を計算する。その際に、プログラム解析と統計手法の長所を組み合わせることで、計算をより高速化している。この HyLeak に関するツール論文を査読付き国際会議 ATVA ’17 で発表した。

さらに、解析ツール HyLeak やその基礎となる技術、実験結果などの研究成果をまとめた論文を査読付きの国際誌 Formal Aspects of Computing で発表した。

(2) ゲーム理論と情報理論の融合による情報漏洩のモデル化・解析

適応的に振る舞う攻撃者と防御者のもとでのプライバシ情報の漏洩量を分析するためのモデルを提案した。具体的には、定量的情報流解析とゲーム理論を融合させた枠組み「情報漏洩ゲーム」（information leakage game）を提案した。この情報漏洩ゲームでは、通常のゲーム理論と異なり、混合戦略の利得が純粋戦略の利得の期待値と異なることを明らかにし、ナッシュ均衡

点の存在を証明し、その計算アルゴリズムを与えた。研究成果をまとめた論文を査読付き国際会議 GameSec ’17 で発表した。

この提案モデルを発展させ、攻撃者が知ることのできる防御戦略についての情報の種類に応じて、情報漏洩の状況を様々なゲームで定式化した。また、これらのゲームの間の関係を明らかにした。さらに、情報漏洩ゲームでは、通常のゲーム理論と異なり、混合戦略と行動戦略が等価でないことも明らかにした。研究成果をまとめた論文を査読付き国際会議 POST ’18 と査読付き国際誌 Entropy で発表した。

(3) 位置情報サービスにおける属性情報のプライバシのモデル化・解析

プライバシの量的性質、特に確率分布についての情報漏洩の度合いをモデル化し解析する枠組みを提案した。具体的には、差分プライバシを確率分布に持ち上げた「分布プライバシ」(DistP, distribution privacy)を定義し、確率的ノイズやダミーデータの付加で実現できる分布プライバシを理論的に明らかにし、最適輸送問題（optimal transportation problem）との関連を示した。実験では、サイバーフィジカルシステムとして位置情報サービスを対象とし、ユーザの属性情報の保護メカニズムの分布プライバシと有用性を実証した。研究成果をまとめた論文を査読付き国際会議 ESORICS'19 と Allerton'19 で発表した。

(4) 位置情報サービスにおける機微情報のプライバシのモデル化・解析

プライバシの量的性質、特に差分プライバシ（differential privacy）の変種について研究をおこなった。具体的には、機微な情報のみを保護するメカニズムを提案し、実現できるプライバシ（ULDP, utility-optimized local differential privacy）や有用性を理論的に明らかにした。また、サイバーフィジカルシステムとして位置情報サービスを対象とした実験により、提案メカニズムの有用性を実証した。研究成果をまとめた論文を査読付き国際会議 USENIX Security'19 で発表した。

(5) 位置情報サービスにおける匿名性のモデル化・解析

サイバーフィジカルシステムとして位置情報サービスを対象とし、プライバシの量的性質、特に差分プライバシと k 匿名性について研究をおこなった。具体的には、位置情報サービスプロバイダが各ユーザから確率的ノイズを加えた位置情報を収集し、得られたデータセットを匿名化して第三者に提供する場合の匿名性と有用性のトレードオフを評価した。研究成果をまとめた論文を査読付きの国際会議 ISITA ’18 で発表した。

(6) 機械学習モデルの統計的仕様を記述するための様相論理

機械学習技術を利用するサイバーフィジカルシステムが満たすべき統計的仕様の記述方法を開発することを目指し、形式的アプローチと統計的アプローチの融合により、論理的知識と統計的知識を記述できる様相論理 StatEL（statistical epistemic logic)を提案し、分布間の距離に基づく可能世界意味論を与えた。また、統計的仮説検定や機械学習モデルの様々な統計的性質（精度、頑健性、公平性など）を StatEL の論理式を用いて形式化した。研究成果をまとめた論文を査読付き国際会議 SEFM ’19 と査読付き国際ワークショップで発表した。

<u>まとめと今後の展望</u>

本研究を通じて、サイバーフィジカルシステム(CPS)のモデル化・解析・検証の様々な点において、形式的アプローチと統計的アプローチの融合が有用であることを明らかにした。

本研究では、検証対象の性質として、プライバシ情報漏洩に関する量的性質を主に扱ってきたが、今後の研究においては、これまでの研究成果に基づき、その他の量的性質についてもモデル化・解析・検証に取り組みたいと考えている。また、本研究では、CPS の具体例として位置情報サービスのみを扱ってきたが、今後の研究においては、これまでの研究成果に基づき、他の種類の CPS についても対象としていきたいと考えている。

本研究の上記(6)では、形式的アプローチと統計的アプローチの融合により、機械学習モデルの様々な統計的性質を論理式として形式化する初めての枠組みを提案したが、今後、機械学習モデルを部品として用いる CPS 全体が満たすべき仕様を形式化する手法を研究していく上での土台となると考えている。

５．主な発表論文等

〔雑誌論文〕　計12件（うち査読付論文　12件／うち国際共著　6件／うちオープンアクセス　3件）

１．著者名 Mario S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi	４．巻 20(5:382)
２．論文標題 A Game-Theoretic Approach to Information-Flow Control via Protocol Composition	５．発行年 2018年
３．雑誌名 Entropy	６．最初と最後の頁 1-43
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/e20050382	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Yusuke Kawamoto and Takao Murakami	４．巻 -
２．論文標題 On the Anonymization of Differentially Private Location Obfuscation	５．発行年 2018年
３．雑誌名 Proc. of the 2018 International Symposium on Information Theory and Its Applications (ISITA 2018)	６．最初と最後の頁 159-163
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/ISITA.2018.8664351	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Fabrizio Biondi, Yusuke Kawamoto, Axel Legay, and Louis-Marie Traonouez	４．巻 31(2)
２．論文標題 Hybrid Statistical Estimation of Mutual Information and its Application to Information Flow	５．発行年 2019年
３．雑誌名 Formal Aspects of Computing	６．最初と最後の頁 165-206
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00165-018-0469-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yusuke Kawamoto, Konstantinos Chatzikokolakis, and Catuscia Palamidessi	４．巻 13
２．論文標題 On the Compositionality of Quantitative Information Flow	５．発行年 2017年
３．雑誌名 Logical Methods in Computer Science	６．最初と最後の頁 1-31
掲載論文のDOI（デジタルオブジェクト識別子） 10.23638/LMCS-13(3:11)2017	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Fabrizio Biondi, Yusuke Kawamoto, Axel Legay, and Louis-Marie Traonouez	4．巻 10482
2．論文標題 HyLeak: Hybrid Analysis Tool for Information Leakage	5．発行年 2017年
3．雑誌名 Proc. of the 15th International Symposium on Automated Technology for Verification and Analysis (ATVA 2017), Lecture Notes in Computer Science	6．最初と最後の頁 156-163
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-68167-2_11	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Mario S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi	4．巻 10575
2．論文標題 Information Leakage Games	5．発行年 2017年
3．雑誌名 Proc. of the 8th International Conference on Decision and Game Theory for Security (GameSec 2017), Lecture Notes in Computer Science	6．最初と最後の頁 437-457
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-68711-7_23	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Mario S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi	4．巻 10804
2．論文標題 Leakage and Protocol Composition in a Game-Theoretic Perspective	5．発行年 2018年
3．雑誌名 Proc. of the 7th International Conference on Principles of Security and Trust (POST 2018), Lecture Notes in Computer Science	6．最初と最後の頁 134-159
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-89722-6_6	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Takao Murakami, Yusuke Kawamoto	4．巻 -
2．論文標題 Utility-Optimized Local Differential Privacy Mechanisms for Distribution Estimation	5．発行年 2019年
3．雑誌名 Proc. of the 28th USENIX Security Symposium (USENIX Security 2019)	6．最初と最後の頁 1877-1894
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Kawamoto Yusuke, Murakami Takao	4．巻 11735
2．論文標題 Local Obfuscation Mechanisms for Hiding Probability Distributions	5．発行年 2019年
3．雑誌名 Proc. of the 24th European Symposium on Research in Computer Security (ESORICS 2019), Part I, Lecture Notes in Computer Science	6．最初と最後の頁 128-148
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-29959-0_7	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kawamoto Yusuke, Murakami Takao	4．巻 -
2．論文標題 Local Distribution Obfuscation via Probability Coupling	5．発行年 2019年
3．雑誌名 Proc. of the 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2019)	6．最初と最後の頁 718-725
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ALLERTON.2019.8919803	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kawamoto Yusuke	4．巻 11760
2．論文標題 Statistical Epistemic Logic	5．発行年 2019年
3．雑誌名 The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy, Lecture Notes in Computer Science	6．最初と最後の頁 344-362
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-31175-9_20	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kawamoto Yusuke	4．巻 11724
2．論文標題 Towards Logical Specification of Statistical Machine Learning	5．発行年 2019年
3．雑誌名 Proc. of the 17th International Conference on Software Engineering and Formal Methods (SEFM 2019), Lecture Notes in Computer Science	6．最初と最後の頁 293-311
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-30446-1_16	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計15件（うち招待講演　1件／うち国際学会　13件）

１．発表者名
Yusuke Kawamoto

２．発表標題
Obfuscation Mechanisms with Distribution Privacy

３．学会等名
4th Franco-Japanese Cybersecurity Workshop（国際学会）

４．発表年
2018年

１．発表者名
Yusuke Kawamoto and Takao Murakami

２．発表標題
On the Anonymization of Differentially Private Location Obfuscation

３．学会等名
2018 International Symposium on Information Theory and Its Applications (ISITA 2018)（国際学会）

４．発表年
2018年

１．発表者名
川本裕輔

２．発表標題
情報量を利得とするゲームとプライバシー定量化への応用

３．学会等名
ゲーム理論ワークショップ2019

４．発表年
2019年

１．発表者名
Yusuke Kawamoto

２．発表標題
Modeling and Analysis of Information Leakage

３．学会等名
Third French Japanese Meeting on Cybersecurity（国際学会）

４．発表年
2017年

１．発表者名
川本裕輔

２．発表標題
プライバシの定量的モデルと保護メカニズム

３．学会等名
日本応用数理学会2017年度年会 「数理的技法による情報セキュリティ」研究部会（招待講演）

４．発表年
2017年

１．発表者名
Fabrizio Biondi, Yusuke Kawamoto, Axel Legay, and Louis-Marie Traonouez

２．発表標題
HyLeak: Hybrid Analysis Tool for Information Leakage

３．学会等名
15th International Symposium on Automated Technology for Verification and Analysis (ATVA 2017)（国際学会）

４．発表年
2017年

１．発表者名
Mario S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi

２．発表標題
Information Leakage Games

３．学会等名
8th International Conference on Decision and Game Theory for Security (GameSec 2017)（国際学会）

４．発表年
2017年

１．発表者名
Yusuke Kawamoto

２．発表標題
Extension of Differential Privacy to Distribution Obfuscation

３．学会等名
NII Shonan Meeting Seminar 116（国際学会）

４．発表年
2018年

１．発表者名
Mario S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi

２．発表標題
Leakage and Protocol Composition in a Game-Theoretic Perspective

３．学会等名
7th International Conference on Principles of Security and Trust (POST 2018)（国際学会）

４．発表年
2018年

１．発表者名
Yusuke Kawamoto

２．発表標題
Epistemic logic for expressing the statistical security of machine learning

３．学会等名
5th France-Japan Cybersecurity Workshop（国際学会）

４．発表年
2019年

１．発表者名
Takao Murakami, Yusuke Kawamoto

２．発表標題
Utility-Optimized Local Differential Privacy Mechanisms for Distribution Estimation

３．学会等名
28th USENIX Security Symposium (USENIX Security 2019)（国際学会）

４．発表年
2019年

１．発表者名
Kawamoto Yusuke, Murakami Takao

２．発表標題
Local Obfuscation Mechanisms for Hiding Probability Distributions

３．学会等名
24th European Symposium on Research in Computer Security (ESORICS 2019)（国際学会）

４．発表年
2019年

１．発表者名
Kawamoto Yusuke, Murakami Takao

２．発表標題
Local Distribution Obfuscation via Probability Coupling

３．学会等名
57th Annual Allerton Conference on Communication, Control, and Computing (Allerton 2019)（国際学会）

４．発表年
2019年

１．発表者名
Yusuke Kawamoto

２．発表標題
Statistical Epistemic Logic

３．学会等名
The Art of Modelling Computational Systems: A Journey from Logic and Concurrency to Security and Privacy（国際学会）

４．発表年
2019年

１．発表者名
Yusuke Kawamoto

２．発表標題
Towards Logical Specification of Statistical Machine Learning

３．学会等名
17th International Conference on Software Engineering and Formal Methods (SEFM 2019)（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
タイミング攻撃に対抗するための情報処理方法、システム及びプログラム	川本 裕輔，村上隆夫	産業技術総合研究所
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2018-153830	2018年	国内

〔取得〕　計0件

〔その他〕

HyLeak: Hybrid Analysis Tool for Information Leakage
https://project.inria.fr/hyleak/

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考