HITACHI
Inspire the Next

MWS 2022 プレミーティング

MWS 受賞論文の研究テーマの決め方、取り組み方

2022/07/12

株式会社 日立製作所 研究開発グループ
セキュリティ・トラスト研究部

藤井 翔太

© Hitachi, Ltd. 2022. All rights reserved.

自己紹介

HITACHI
Inspire the Next

■ **名前：**藤井 翔太

■ **所属：**
- ✓ 日立製作所 研究開発グループ
- ✓ 岡山大学 大学院自然科学研究科 産業創成工学専攻

■ **主な経歴：**
- ✓ 学士課程～博士前期課程ではシステムセキュリティの研究を実施
  - MWS Cup，情報危機管理コンテスト，SECCON等にも参加
- ✓ 2016年より現職
  - 主な研究テーマ：サイバー/ネットワークセキュリティ
  - 最近はユーザブルセキュリティにも興味あり
- ✓ 2020年に博士後期課程に社会人学生として進学（在学中）

© Hitachi, Ltd. 2022. All rights reserved.

本日の内容について

HITACHI
Inspire the Next

■ 今日主にお話ししようと思っていること（お題）

- ✓ 研究テーマの選定
- ✓ 研究の進め方
- ✓ 研究を進めるうえでの苦労

- ✓ 以降は，主に企業研究者（+社会人博士）の立場でのお話です
- ✓ あくまで自分の経験やスタイルを記載しており，万人に当てはまるものではないと思いますが，少しでも何かの参考になれば幸いです

© Hitachi, Ltd. 2022. All rights reserved.

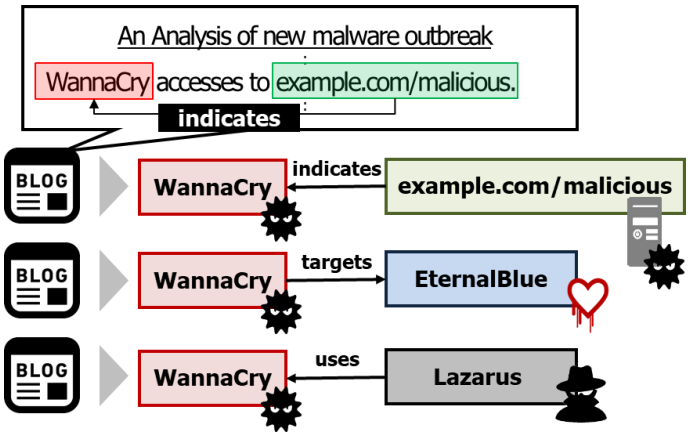
受賞稿に係る研究の概要

HITACHI
Inspire the Next

機械学習を用いたCyber Threat Intelligenceの構造化と横断的分析

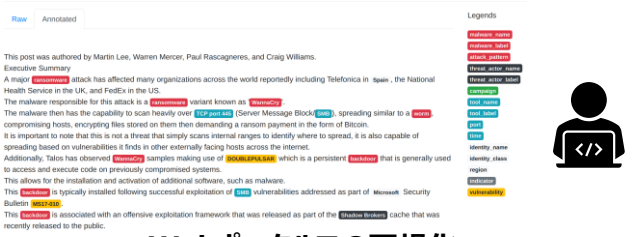
- セキュリティインテリジェンス（CTI）を自動的に共通フォーマット（STIX）で構造化し，効率的な分析を支援
- 自然言語処理/機械学習を用いて，マルウェア名や脆弱性名等のサイバーセキュリティドメインにおける固有表現を抽出して分析の効率化を狙うとともに，固有表現間の関係を抽出することにより，文脈情報を維持した形で構造化
- システムを実装して各種精度を定量的に評価すると共に，構造化したCTIを分析してその活用性を定性的に実証

固有表現・関係抽出

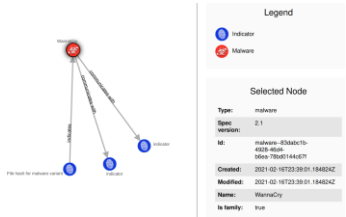


非構造なCTIを自然言語処理/機械学習で分析し，
共通フォーマット（STIX）で構造化

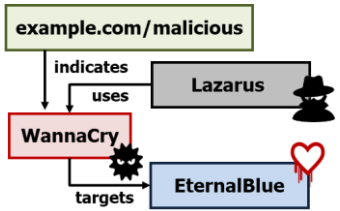
脅威ナレッジ化・可視化



Webポータルでの可視化



STIX用機能を用いた可視化



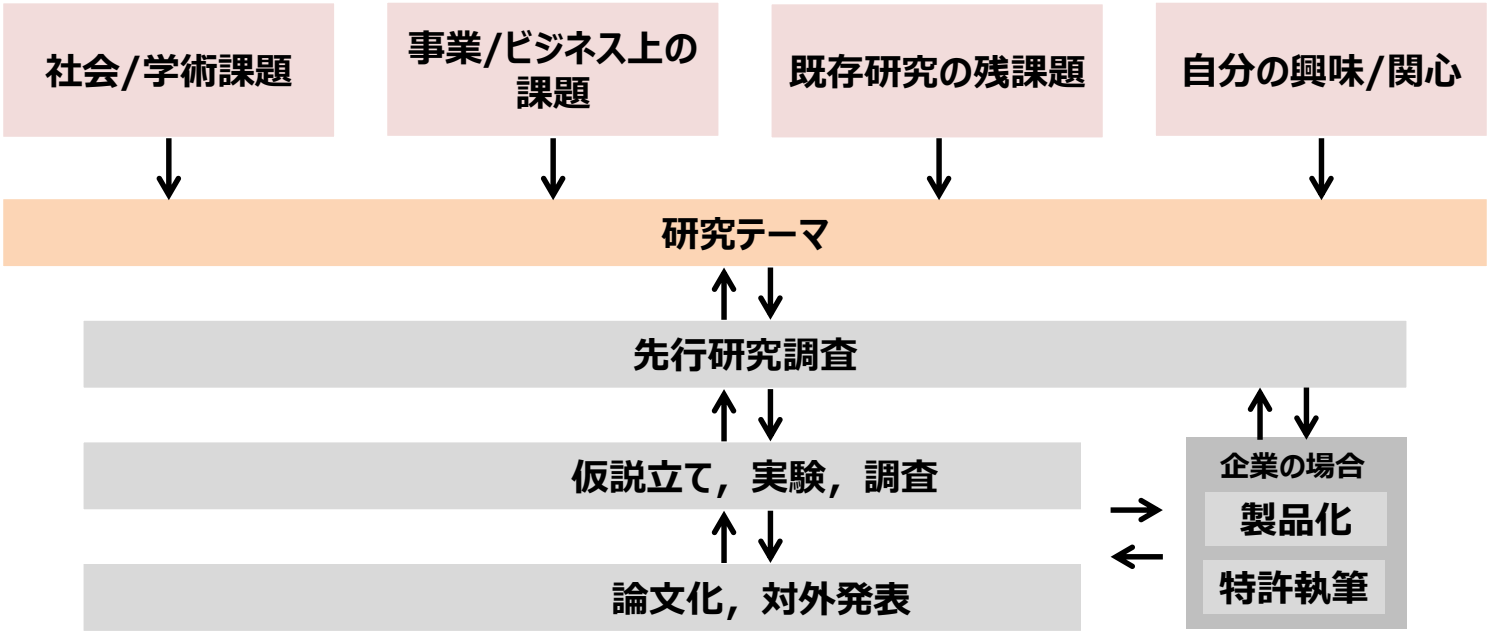
脅威ナレッジ化

© Hitachi, Ltd. 2022. All rights reserved.

研究テーマの選定

HITACHI
Inspire the Next

■ 社会課題や学術課題（等）を抽出し，研究テーマへ昇華
- ✓ 課題の抽出は，文献調査や現場へのヒアリングを通して実施
  - 研究テーマは自分の興味や趣味を入れ込めると吉
- ✓ 先行研究調査や実験を通して研究テーマを錬磨，最終的に論文化・発表



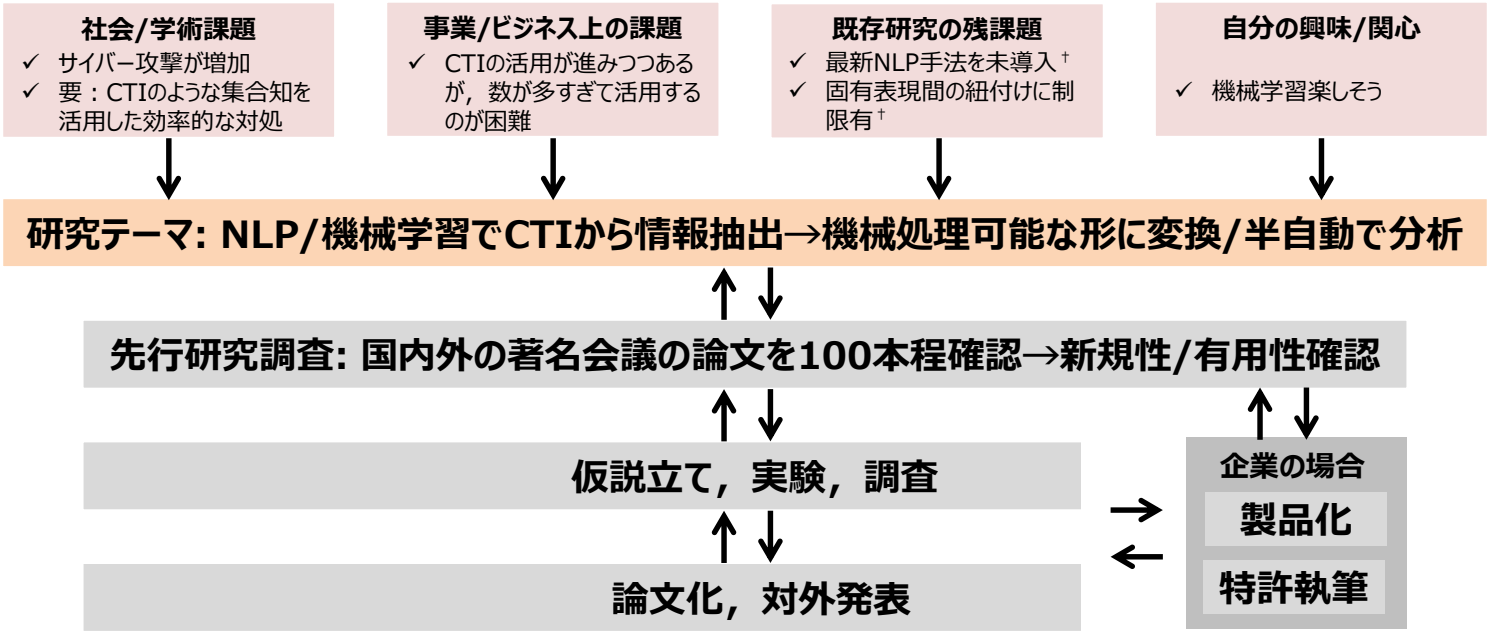
© Hitachi, Ltd. 2022. All rights reserved.

研究テーマの選定

HITACHI
Inspire the Next

■ 社会課題や学術課題（等）を抽出し，研究テーマへ昇華
- ✓ 課題の抽出は，文献調査や現場へのヒアリングを通して実施
  - 研究テーマは自分の興味や趣味を入れ込めると吉
- ✓ 先行研究調査や実験を通して研究テーマを錬磨，最終的に論文化・発表

本研究の場合



† Xiaojing Liao, et al.:Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence, ACM CCS '16 pp. 755－766 (2016).

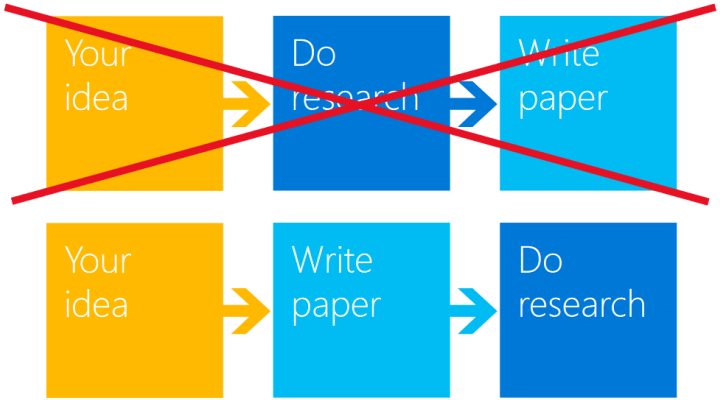
© Hitachi, Ltd. 2022. All rights reserved.

研究の進め方

HITACHI
Inspire the Next

■ 研究が一段落してから論文を書くのではなく，論文を書きつつ研究を実施

- ✓ 研究の焦点や全体像がクリアになる
  - 最後に論文を書いてみると初期の検討に漏れがあったことに気づいた，といった致命的なミスも抑制できる
- ✓ 研究/論文がぶれにくくなる
  - 最後にまとめて文章化するとどうしても一貫性に欠けたり切り貼り感が出る可能性が高くなる



How to write a great research paper†

■ 共著者/先生との議論は定期的に実施

1週間のスケジュール例

月	火	水	木	金
雑務	評価	資料作成	検討	評価
実装	資料作成	定例	実装	雑務

† Microsoft: How to write a great research paper, available from: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/How-to-write-a-great-research-paper.pdf

© Hitachi, Ltd. 2022. All rights reserved.

研究の進め方

HITACHI
Inspire the Next

■ **研究が一段落してから論文を書くのではなく，論文を書きつつ研究を実施**

✓ はじめに/背景の章は最初に書いて研究全体を整理

✓ 2章以降は全体の整理後に調査・仮説ベースで執筆し，それに合わせる形で実験を実施

大まかな論文の構成

#	章構成
1	はじめに・背景
2	提案手法
3	評価
4	考察・議論
5	関連研究

一番最初に執筆

先に大まかに原稿を書いておき，それに合わせる形で
実験等を実施・ブラッシュアップ

随時調査・加筆, e.g., top-4の実施タイミング

© Hitachi, Ltd. 2022. All rights reserved.

苦労話（1/2）

HITACHI
Inspire the Next

関連性のある研究が次々と発表される

- ✓ 脅威情報（CTI）を取り扱う研究が難関会議で次々と発表
- ✓ 場合によっては，実験中の内容が発表と被ってしまい，原稿の構成を変更することも

2016

Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence (ACM CCS ‘16)

非構造なCTIから正規表現やグラフマイニングの活用によってIOCを抽出し，構造化

2017

TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources (ACSAC ‘17)

CTIをテキストマイニングし，記載内容を攻撃手口（TTPs）やCyber Kill Chainに割り当て

2018

ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports (EuroS&P ’18)

CTIからのIOCの抽出とIOCの攻撃における役割・フェーズの推定

2019

Reading the tea leaves: a comparative analysis of threat intelligence (USENIX Security ’19)

複数のCTIを横断的に分析した研究，IOCは提供者ユニークが多いことから複数情報の活用が重要なことや偽陽性の存在から内容の精査が必要なことを示唆

Towards the detection of inconsistencies in public security vulnerability reports (USENIX Security ’19)

脆弱性情報（CVE等）を正規表現や自然言語処理を駆使して分析し，内容の矛盾（情報源と構造化された脆弱性の矛盾）を抽出

Understanding and securing device vulnerabilities through automated bug report analysis (USENIX Security ‘19)

CTIから製品名，脆弱性，IOC等を自動抽出し，対応要否を判定するとともに，要対応と判定したものについては自動で検出シグネチャを作成

© Hitachi, Ltd. 2022. All rights reserved.

苦労話（2/2）

HITACHI
Inspire the Next

何度もリジェクトされる

- ✓ 査読付きの国際会議に投稿してはリジェクトされる次期が1年ほど続いていた
  - 右図参照
- ✓ **投稿の度に査読コメントをいただけて研究・論文はブラッシュアップされていく**ので研究的にはネガティブではない
  - CSS2021優秀論文賞の受賞稿にも査読コメントを受けてアップデートした内容あり
  - ぜひ積極的に査読付き会議に投稿しましょう！

© Hitachi, Ltd. 2022. All rights reserved.

まとめ

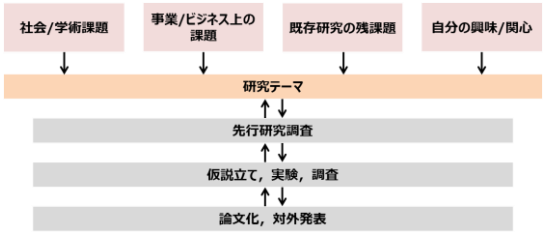
HITACHI
Inspire the Next

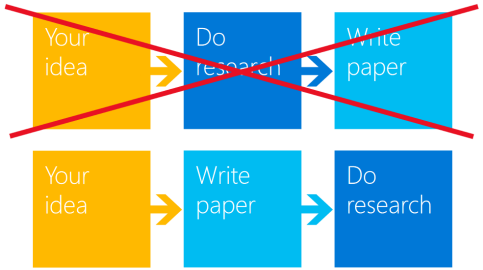
■ 今日主にお話ししたこと

✓ 研究テーマの選定
- 社会課題や学術課題（等）を抽出し，研究テーマへ昇華
- 研究テーマは自分の興味や趣味を入れ込めると吉

✓ 研究の進め方
- 研究が一段落してから論文を書くのではなく，論文を書きつつ研究を実施
- 共著者/先生との議論は定期的に実施

✓ 研究を進めるうえでの苦労
- リジェクトされて辛い時もありますが頑張りましょう！





How to write a great research paper†

† Microsoft: How to write a great research paper, available from: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/07/How-to-write-a-great-research-paper.pdf

© Hitachi, Ltd. 2022. All rights reserved.

HITACHI

Inspire the Next