MWS 2024に
投稿された論文・されなかった論文

MWS2024 プログラム委員長

2024-12-25

MWS2024のスコープ

MWSの活動目的

マルウェアとサイバー攻撃対策研究人材育成ワークショップanti-Malware and anti-cyberattacks engineering WorkShop (MWS)は、サイバー攻撃の一端を担うマルウェアだけでなく、攻撃者やTTPs(Tactics、Techniques、Procedures)を俯瞰的に捉えた対策研究を推進し、人材育成を行います。また、新たな脆弱性や攻撃手法を発見し先行して対処を行うオフェンシブセキュリティも、攻撃者による悪用を未然に防止する点で、重要な研究領域と位置付けています。さらには、将来に渡って必要となる対策技術や人材育成に関わる新たな問題提起を行っていきます。

CSS2024のCFPに掲載したMWSトラックの説明文（150字以内）

MWSトラックでは，サイバー攻撃の一端を担うマルウェアだけでなく，攻撃者や攻撃者の活動を俯瞰的に捉えた対策研究に関する論文を広く募集します．また，新たな脆弱性や攻撃手法を発見し先行して対処を行うオフェンシブセキュリティ，および，将来に渡って必要となる対策技術に関する論文も募集します．詳細はMWSのウェブページをご覧ください．

MWS発表数の集計

	セッション数	論文総数	学生論文数	データセット活用論文
2015	10	32	-	23
2016	17	67	-	11
2017	17	67	-	16
2018	14	55	-	13
2019	13	53	29	9
2020	10	36	26	9
2021	9	35	21	8
2022	8	34	23	2
2023	6	27	12	2
2024	**9**	**41**	**30**	**5**

投稿された論文一覧

9セッション，41件の発表（38件申込，4件を別トラックから移動，1件取下）

セッション名	和文タイトル
攻撃活動の分析と対策	アクティブ・ディフェンス実現に向けたサイバー抑止のモデル化および実装についての一考察
	ハニーポットで観測される新規エクスプロイトの分類手法の提案
	OSINTを活用したインシデント防御戦略支援システムの提案
	攻撃者と攻撃対象のインテリジェンス統合によるサイバーセキュリティ対策
IoTマルウェア	クロスアーキテクチャに対応したIoTマルウェアMiraiの設定情報抽出ツール
	IoTマルウェアの系統樹クラスタリングにおける機能面に踏み込んだ解析のための距離定義の改良
	32bit Armバイナリにおける間接的に呼び出される関数の呼び出し関係とシステムコールの検出
	関数呼び出し時系列グラフを用いたIoTマルウェアの機能分析のためのグラフ作成手法および比較手法の検討
Webセキュリティ	JavaScript実行環境を共有するブラウザ拡張機能によるWebプッシュ通知制御と上書き防止手法
	ブラウザーフィンガープリンティングによるルールベースを用いた端末推定
	大規模言語モデルを用いたフィッシングサイト検出
	大規模言語モデルを用いたクロスサイトスクリプティング攻撃の検知手法の提案
	大規模言語モデルを用いた悪性JavaScriptの検知手法の提案
マルウェア解析	動的解析時の画面から取得可能な情報の調査と応用可能性の検討
	マルウェア動的解析システムAlkanetによるWindowsサービスの追跡
	自動表層解析システムにおけるFFRI Dataset scriptsの利用と拡張
	Rustで生成されたマルウェアを解析するためのGhidra拡張機能の開発
	ログ間の特徴量予測によるマルウェアの目的推定に関する検討

マルウェア検知	深層学習ベースのスタッキングを用いたAndroidマルウェア検知
	ファイル情報を考慮した画像ベース難読化マルウェア検出手法の検討
	APIコールの時系列情報に注目したLSTMによるマルウェアの早期検知と分類
	文字コード付きAPIとプロセスの親子関係情報に着目したランサムウェアの分析と検知
	LSTMによるAPIコール系列の正常性スコアに基づくマルウェア分析
異常検知	VAEによるサブネット単位での異常検知
	ConvNeXtによるネットワークトラフィック中の異常検出
	ダークネット通信におけるTCP応答時間の変動分析と不審送信元の経路視覚化
	エントロピーの変化点に基づくネットワークパケットの異常検知
解析回避への対策	LLMを用いて作成した解析回避検体がサンドボックス解析に与える影響の調査
	Linuxファイルレスマルウェア検知手法に対するeBPFを用いた回避手法の提案とその対策
	デバッガ検知回避および不要なループからの脱出により例外発生マルウェアを実行継続させる動的解析手法
	シンボリック実行による解析環境検知マルウェアの解析手法改善
	シンボリック実行の動作ログを用いたマルウェアの耐解析機能無効化手法の提案
監視	ログ収集のための機械学習を用いたJSON形式ログファイル判別の検討
	機械学習を用いた異常ログ可視化のための誤検知された正常ログ対策の検討
	ファイル操作ログの取得による永続化マルウェアの追跡手法
	特定されたボット活動に基づく大規模ネットワーク分析によるボットネット検知方法
攻撃手法と保護メカニズム	ランサムウェアに対する破壊的書き込みの監視による仮想ディスク保護機構
	eBPFを利用した暗号化ランサムウェアからの回復
	DarkWrt: IoT機器における不正機能のデータセット作成に向けた事例調査と分類
	CTFを活用した攻撃難易度の定量化手法の提案
	周期に基づく CAN 侵入検知アルゴリズムへの 攻撃手法と対策手法の提案

セッション構成(MWS)(9セッション)

セッション名	キーワード
攻撃活動の分析と対策	ハニーポット，OSINT，脅威インテリジェンス
IoTマルウェア	IoT，マルウェア，…
Webセキュリティ	Web，ブラウザ，大規模言語モデル，フィッシング， XSS
マルウェア解析	動的解析，表層解析，ログ分析
マルウェア検知	分類，機械学習
異常検知	ネットワークの異常検知，エントロピー， IDS
解析回避への対策	解析回避，検知回避，サンドボックス，シンボリック実行
監視	フォレンジック，ログ解析，機械学習，ボットネット
攻撃手法と保護メカニズム	ランサムウェア，不正機能

例年どおり
（若干減少傾向？）

例年より多め
→**リスコープに適合**

セッション構成(システムトラック)(17セッション)

セッション名
IoTセキュリティ
サイバー攻撃検知
サイバーフィジカルシステム
Web・メールセキュリティ
車両システム
自動運転
ソフトウェアセキュリティ
リスク評価
システムソフトウェア

セッション名
認証
通信・プロトコル
フィッシング検知
フィッシング分析
ハードウェアセキュリティ
ネットワークセキュリティ
セキュリティ分析
デバイス推定

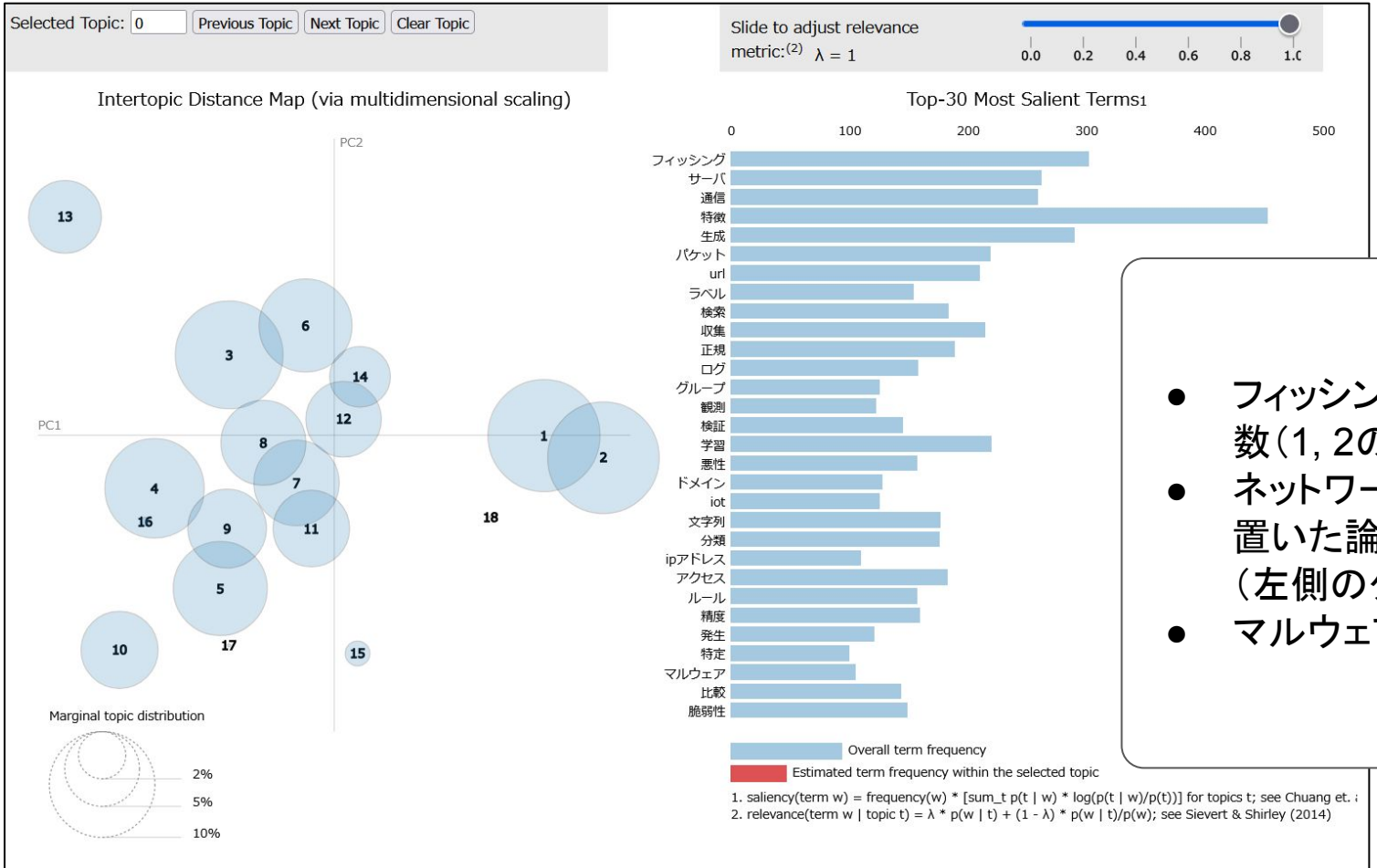
システムトラックからの移動を打診された論文（33件）

- 32(システム)+1(PWS)件の計33件をMWSへ移動できないか打診された
  - MWSはPC委員が他トラックに比べて多いので妥当
- 当該論文の分野はMWSのスコープ内
  - マルウェア検知・解析
  - フィッシング
  - 攻撃通信検知
  - 脅威インテリジェンス
  - デジタルフォレンジック
  - 脆弱性発見・対応
- CSSプログラム委員長／委員長補佐と相談
  - 著者の意向を尊重→大幅なトラック間移動は避ける
  - システムトラックの負荷分散も必要
    - MWSより少ない人員で約90件を扱う必要有
- 最終的にシステムから3件，PWSから1件の計4件をMWSへ移動
  - MWSと関連が強いと思われるものを選出
  - MWSと関連が弱い論文1件はMWS→システムトラックへ移動

MWSトラックで発表された論文（41件）

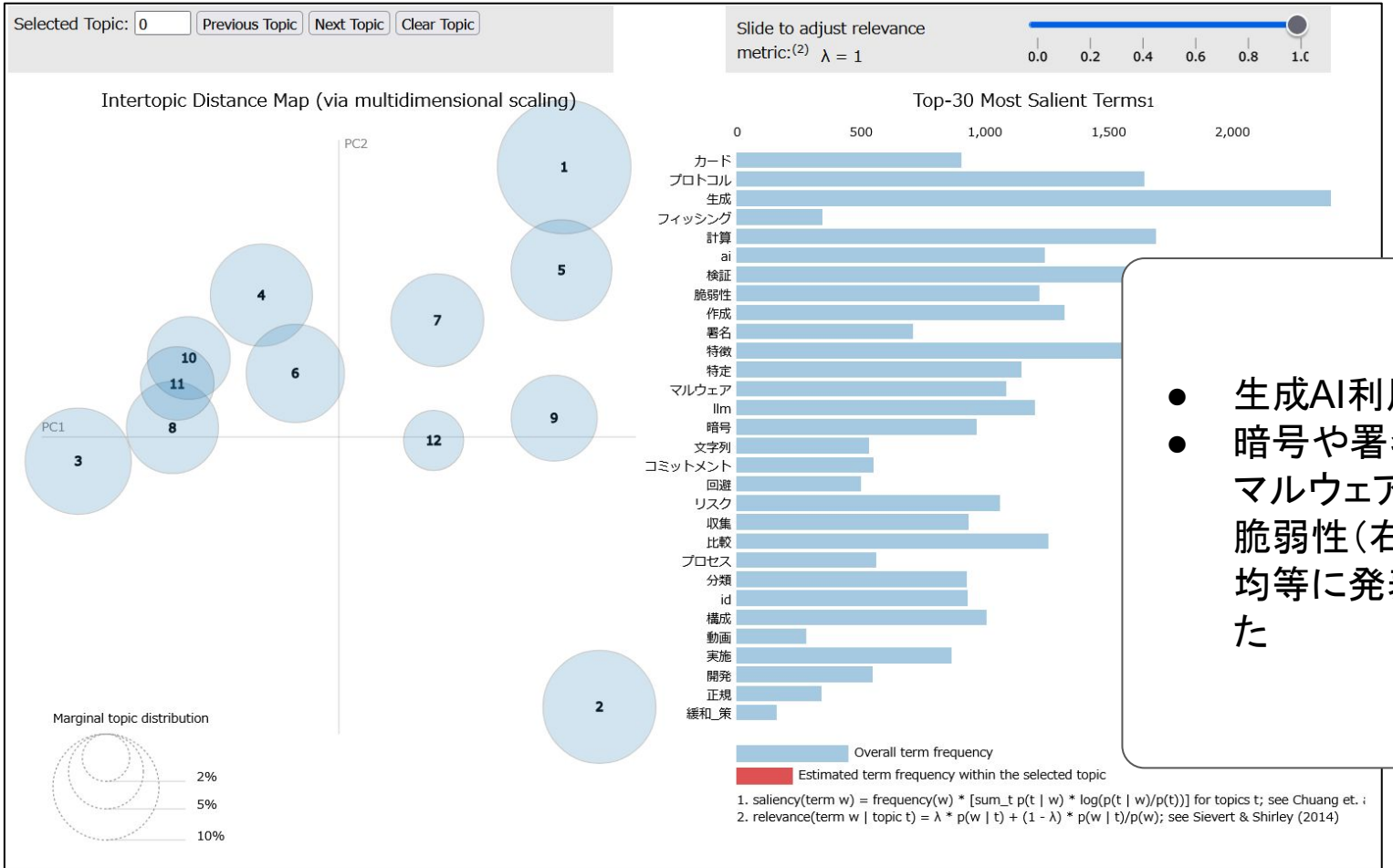
- マルウェア検知，解析，分類など
- マルウェアの中でもランサムウェアが特徴的

システム→MWSへ移動を打診された(が移動しなかった)論文（26件）



- フィッシング関係が多数（1, 2の円）
- ネットワークに重点を置いた論文が多い（左側のグループ）
- マルウェア検知・解析

CSS全体の論文（269件）



- 生成AI利用が多数
- 暗号や署名（左端），マルウェア（右上），脆弱性（右下）が概ね均等に発表されていた

トピックの比較

MWSに投稿された論文

- マルウェア
- 解析回避
- ランサムウェア
- Web
- 脆弱性
- LLM

- LLMを活用した研究が増加
- 解析回避などマルウェア解析のコアな研究も増加

移動を打診された論文

- マルウェア検知・解析
- フィッシング
- 攻撃通信検知
- 脅威インテリジェンス
- デジタルフォレンジック
- 脆弱性発見・対応

- フィッシング関係が多数
- どれもMWSに投稿されていても違和感ない

システムトラックでオフェンシブなもの

- サイバーフィジカルシステム(3/5)
- 車両システム(0/3)
- 自動運転(4/4)

- 攻撃を提案しているものが多い(7/12)
- ハードウェア寄りはシステムトラックに投稿？

まとめ

- MWSへの投稿
  - リスコープの効果でオフェンシブセキュリティの投稿が増加して分野が広がりつつある
  - マルウェア関係は技術的に深い内容が増加
- MWSへ投稿されなかった論文
  - 自動車やデバイスが関係する論文はシステムトラックへ投稿される傾向にある
    - MWSは名前にマルウェアが入っているのでソフトウェアに偏りがちか
  - フィッシング関係・ネットワーク関係はシステムトラック
    - MWSにも投稿されているので棲み分けが不明瞭
  - CSS全体で脆弱性に関する発表が増えているように見えるが MWSでは…？
    - システム・OWSとの棲み分けが不明瞭
- 課題
  - トラック間のスコープの調整
  - キーワードの具体化

補足: CSS2024プログラム抜粋（自動車等）

https://www.iwsec.org/css/2024/program.html

1B6: サイバーフィジカルシステム

座長：藤本 大介（奈良先端大学院大学）

1B6-1

複数のセンサ情報を用いたMRにおける視界操作攻撃検知の提案

◎ 荒川 貴彦 (静岡大学), 金岡 晃 (東邦大学), 西垣 正勝 (静岡大学), 大木 哲史 (静岡大学)

1B6-2

rPPG 信号に基づく個人識別攻撃の提案と対策

○ 飯島 涼 (国立研究開発法人 産業技術総合研究所 / 早稲田大学), 長谷川 幸己 (早稲田大学), 河岡 諒 (早稲田大学), 森 達哉 (早稲田大学 / 国立研究開発法人情報通信研究機構 / 理研AIP)

1B6-3

ステレオカメラ深度推定技術を用いたドローンの衝突回避機構に対する錯視画像の影響評価

○ 河岡 諒 (早稲田大学), 海老根 佑雅 (早稲田大学), 森 達哉 (早稲田大学)

1B6-4

Security Analysis of the Smart Lock Products against the Device Hijacking Attacks

○ Hiroki Kimura(Graduate School of Information Science, University of Hyogo), Jun Kurihara (Graduate School of Information Science, University of Hyogo), Toshiaki Tanaka (Graduate School of Information Science, University of Hyogo)

1B6-5

チケットの中売り対策の提案

◎ 梅本 琉奈 (長崎県立大学), 松崎 なつめ (長崎県立大学)

2C1: 車両システム

座長：倉地 亮（名古屋大学）

2C1-1

車両システムへの古典的及び最新のセキュリティアーキテクチャの適用に関する一考察

○ 安齋 潤 (パナソニック オートモーティブシステムズ株式会社), 今本 吉治 (パナソニック オートモーティブシステムズ株式会社)

2C1-2

AIを利用する車両システムのセキュリティと安全論証について

○ 溝口 誠一郎 (DNVビジネスアシュアランスジャパン株式会社), 櫻井 幸一 (九州大学)

2C1-3

低遅延CANメッセージフィルタリング技術Gated-CAN

○ 前川 陽介 (トヨタ自動車株式会社/横浜国立大学), Camille Gay (Toyota Motor Corporation), 吉岡 克成 (横浜国立大学), 松本 勉 (横浜国立大学)

2C2: 自動運転

座長：吉田 直樹（横浜国立大学）

2C2-1

自動運転システムのセキュリティ評価プラットフォーム Overpass による敵対的攻撃の E2E 評価

○ 野本 一輝 (早稲田大学/デロイト トーマツ サイバー合同会社), 福永 拓海 (デロイト トーマツ サイバー合同会社), 鶴岡 豪 (早稲田大学), 小林 竜之輔 (早稲田大学), 田中 優奈 (早稲田大学), 神薗 雅紀 (デロイト トーマツ サイバー合同会社), 森 達哉 (早稲田大学/NICT/理研AIP)

2C2-2

ヘッドライトの反射光を悪用する敵対的パッチ攻撃の提案と評価

◎ 鶴岡 豪 (早稲田大学), 佐藤 貴海 (カリフォルニア大学アーバイン校), Qi Alfred Chen (カリフォルニア大学アーバイン校), 野本 一輝 (早稲田大学 / デロイト トーマツ サイバー合同会社), 小林 竜之輔 (早稲田大学), 田中 優奈 (早稲田大学), 森 達哉 (早稲田大学 / NICT / 理研AIP)

2C2-3

LiDAR 点群の物理的消失による誤検出誘発攻撃と防御

◎ 小林 竜之輔 (早稲田大学), 野本 一輝 (早稲田大学/デロイト トーマツ サイバー合同会社), 田中 優奈 (早稲田大学), 鶴岡 豪 (早稲田大学), 森 達哉 (早稲田大学/情報通信研究機構/理研AIP)

2C2-4

自動運転システムの LiDAR 点群前処理フィルタに対する人工霧を用いた敵対的攻撃

◎ 田中 優奈 (早稲田大学), 野本 一輝 (早稲田大学/デロイト トーマツ サイバー合同会社), 小林 竜之輔 (早稲田大学), 鶴岡 豪 (早稲田大学), 森 達哉 (早稲田大学/情報通信研究機構/理研AIP)