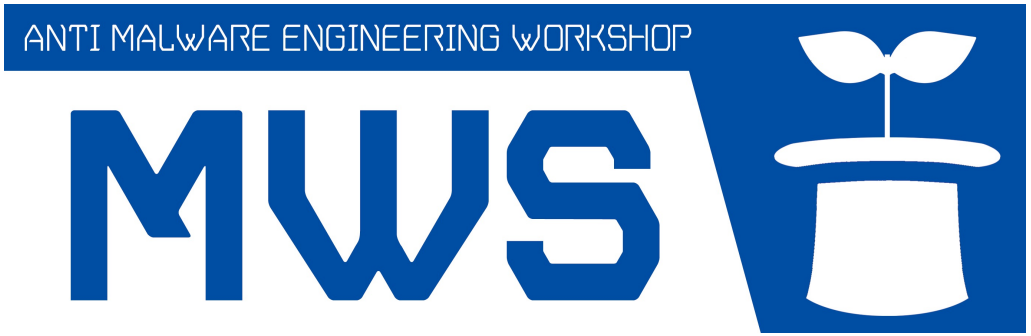
マルウェア対策研究人材育成ワークショップ
MWS 2021 @オンライン



MWS2021 トラックチェアからの講評

MWS 2021 プログラム委員長
高田 雄太

目次

- MWSトラックについて
- 表彰の選考について
- 表彰の結果発表

1

MWS トラックについて

MWS データセットを活用した研究に加え、マルウェア・CSIRT/インシデント対応・脅威インテリジェンス等に関する研究論文を募集しました

トラック概要

CSS のトラック制

CSS では発表分野ごとに下記 6 つのトラックからなる構成でプログラムを編成しています

- システム
- 暗号
- MWS
- PWS
- UWS
- OWS

MWS トラック

従来、似たタイトルのセッション・発表がシステムトラックとMWSトラック間で散在していたため、スケジュール含めなるべく被らないよう今年から各 CFP を少し更新しました

MWSトラック
MWSデータセットを利用した研究成果，及びマルウェア対策，CSIRT/インシデント対応，脅威インテリジェンス等を中心としたサイバーセキュリティ全般に関連する研究技術の論文を募集します．

システムトラック
コンピュータシステムや社会システムの安全を支える通信プロトコル，ネットワーク，アーキテクチャ，オペレーティングシステム，アプリケーション，ウェブに関するセキュリティ，およびその適用事例，管理運用など

※緑字が追記箇所

プログラム委員は合計18名で構成されております
皆さまご協力いただき、ありがとうございます！🙏

MWS2021 プログラム委員の皆さま

市野 将嗣	電気通信大学	**齋藤 彰一**	名古屋工業大学
岩本 一樹	株式会社セキュアブレイン	**佐藤 将也**	岡山県立大学
内田 真人	早稲田大学	**嶋田 創**	名古屋大学
海野 由紀	(株) 富士通研究所	**高田 雄太**	デロイトトーマツサイバー合同会社
岡本 剛	神奈川工科大学	**田中 恭之**	NTTコミュニケーションズ株式会社
沖野 浩二	富山大学	**田辺 瑠偉**	横浜国立大学
折田 彰	(株) 日立システムズ	**千葉 大紀**	NTTセキュアプラットフォーム研究所
加藤 雅彦	長崎県立大学	**羽田 大樹**	NTTセキュリティ・ジャパン株式会社
川口 信隆	株式会社日立製作所	**村上 洸介**	KDDI総合研究所

「ウェブセキュリティ」関連の発表はシステムトラックへ統合し、最終的に合計34件の研究発表、9件のセッションを編成しました

ANTI MALWARE ENGINEERING WORKSHOP
MWS

セッション編成

マルウェア解析	プログラム解析
ネットワーク異常検知	ネットワークセキュリティ
AI・機械学習による検知	敵対的学習
CSIRT	脅威インテリジェンス
IoT マルウェア	ウェブセキュリティ

→ システムトラックへ移動

研究テーマやトピックの傾向は昨年から大きく変わらず、多様なテーマを扱う論文が集まりました。
依然としてマルウェアを起点としたサイバー攻撃への抜本的 & 実用的な対策の検討が求められます

昨年同様 2021 年もオンラインによる開催となり、論文件数は昨年から微減でした

数字でわかる MWS 2021

	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	34	20	8

MWS では、主にマルウェアを起点としたサイバー攻撃に関する論文や MWS Datasets を用いた研究論文を取り扱っており、一見 MWS では研究活動が減少傾向に見えますが、昨今のサイバー攻撃の多様化や OWS/BWS 等の研究テーマの多様化を踏まえますと、MWS から CSS（セキュリティ業界）全体として専門性の多様化が進んでいるとも言えます。

[参考] 研究用データセット MWS Datasets を用いた研究活動について
https://www.iwsec.org/mws/achievements.html

このあとの「MWS 企画②」にて、研究に関する BoF を開催します

少し宣伝

16:10 -- 17:30 に予定している「 MWS **企画②** BoF 」にて、

「**サイバーセキュリティ研究相談**」と題して、

研究の進め方等の一般論に加え、具体的な研究事例を交えつつ、
サイバーセキュリティ研究を推進・盛り上げるための検討をすべく、
参加者の皆さんで議論する予定ですので、ぜひご参加ください！

2

表彰の選考について

論文集に掲載された論文を審査対象とし、
既定の評価基準に基づいた厳正な審査を行いました

ANTI MALWARE ENGINEERING WORKSHOP
MWS

MWS の表彰

- **表彰の方針：『石を拾うことはあっても玉を捨てることなかれ』**
  - なるべく多くの人が受賞となるように幅広く選定する
  - MWS データセットを使用した研究は積極的に評価する
  - ただし、賞の価値を毀損しないようにする

- **評価基準：各 1 ～ 6 点で評価**
  - 新規性：類似の研究がこれまでに無く独創的なものであるか、
    または、類似の研究と比較して進歩改善の度合が大きいかどうか。
  - 妥当性および信頼性：著者の主張に対する的確な証拠、証明、評価が示されているかどうか、
    および、評価検証の結果は一貫しており安定しているか。
  - 実用性：現在の計算機環境で実装が容易かどうか、または、既に実装済でその完成度が高いかどうか。
  - 総合評価：上記 3 つの平均点ではなく、論文の良い面があればそれを総合的に反映する。

プログラム委員ならびに評価委員の複数人で審査し、優秀論文賞とベストプラクティカル研究賞を決めました

選奨プロセスと表彰の種類

● 大まかな選奨手順

- 一次査読： 1本の論文を2人の査読者で評価
- 二次査読： プログラム委員全員で評価
- 最終審査： MWSトラックの点数上位の論文を CSS へ推薦
  - ✓ 優秀論文章候補を選び、その後に学生論文賞候補を選定する

● 表彰の種類（今年から変更あり）

(従来) MWS優秀論文賞

↓ MWS で候補を選出し、名称を統合

CSS 最優秀論文賞
もしくは
CSS 優秀論文賞

(従来) MWS学生論文賞

↓ MWSで候補を選出し、名称を統合

CSS学生論文賞

＋

後ほどご紹介

MWS ベストプラクティカル研究賞（1件）

- 著者全員を表彰対象とする。
- 論文集に掲載された論文を審査対象とする。
- **過去の受賞経歴を問わない。**
- **実用性の高さやサイバーセキュリティに関する研究コミュニティとしての有用性を評価する。**

表彰総数は全投稿数の10%以内とする

研究人材の育成が MWS の設立趣旨であることに留意し、良い研究成果を表彰対象にできるよう配慮しています

選奨時における配慮

- **論文評価のべからず集**
  - ライバルの研究成果に低い点数をつけるべからず
  - 知り合いの研究成果に高い点数をつけるべからず
  - 自分の好みで判断するべからず
  - 一律に同じ点数をつけるべからず

- **推薦したい論文は「なぜ良かったのか」に関するコメントを残し、二次査読対象の論文著者にはフィードバックいたします**
  - 論文改善のアドバイス
  - プログラム委員会での議論メモ
  - その他の参考情報やコメント

3

(ちょっとだけ)

表彰の結果発表 🎉

論文 34件への一次選考の結果、総合評価の高かった11件が論文賞候補、実用点の高かった 6件が BP 研究賞候補として選ばれました

一次選考の結果

※いずれの候補も重複を含む

MWS 推薦 優秀論文賞 候補（5件）

- 遺伝的アルゴリズムに基づいた広域スキャンのフィンガープリント特定技術の提案
- 機械学習を用いたCyber Threat Intelligenceの構造化と横断的分析
- Soliton Dataset 2021におけるマルウェアによる解析回避処理の調査
- IoTマルウェアにおける関数の依存関係と結合の順序関係に基づくライブラリ関数名の特定
- スクリプト実行環境に対する実行遅延・実行停止を回避する機能の自動付与手法

MWS 推薦 学生論文賞 候補（6件）

- 異議あり！：XAIによる誤識別された悪性活動の特定
- 遺伝的アルゴリズムに基づいた広域スキャンのフィンガープリント特定技術の提案
- SleepHop: 動的バイナリ計装によるマルウェアのタイミング攻撃の無効化
- 動的解析ログと表層情報を組み合わせたマルウェア感染活動の最終進行度推定手法
- ラベル付きオープンデータセットを活用した2入力深層学習モデルによるネットワーク異常検知
- Androidマルウェア分類器に対するパッキングを用いた効果的な回避攻撃

MWS ベストプラクティカル 研究賞 候補（6件）

- HDLコードに対するSMTソルバを用いた自動検証システムの提案
- 機械学習を用いたCyber Threat Intelligenceの構造化と横断的分析
- Soliton Dataset 2021におけるマルウェアによる解析回避処理の調査
- IoTマルウェアにおける関数の依存関係と結合の順序関係に基づくライブラリ関数名の特定
- C2サーバを対象とした相互協力による継続的監視システムの提案
- スクリプト実行環境に対する実行遅延・実行停止を回避する機能の自動付与手法

受賞おめでとうございます！

二次選考の結果

※いずれの候補も重複を含む

MWS 推薦 優秀論文賞

- スクリプト実行環境に対する実行遅延・実行停止を回避する機能の自動付与手法
- 機械学習を用いたCyber Threat Intelligenceの構造化と横断的分析

MWS 推薦 学生論文賞

- 遺伝的アルゴリズムに基づいた広域スキャンのフィンガープリント特定技術の提案
- ラベル付きオープンデータセットを活用した2入力深層学習モデルによるネットワーク異常検知

MWS ベストプラクティカル 研究賞

- Soliton Dataset 2021におけるマルウェアによる解析回避処理の調査

MWS ベストプラクティカル研究賞は、MWS トラックの全論文を審査対象とし、研究成果の実用性の高さが際立つ論文に与えられます

MWS ベストプラクティカル研究賞

4A1-2

Soliton Dataset 2021におけるマルウェアによる解析回避処理の調査

大山 恵弘 (筑波大学)

選奨時のコメント

- MWSデータセットの1つである「 Soliton Dataset2021」におけるマルウエアの解析回避処理を網羅的に、丁寧に、そして詳細に調査しており、資料としての価値が高く、MWS/CSSのシンポジウム原稿としてはきわめて有用である。
- データセットにおける検体選択方式が2020年版と2021年版で大きく変化しており、時間経過に基づく評価を難しくしているという問題提起もしており、MWSデータセット提供側や MWS コミュニティにとって重要なフィードバックになり得る。
- このような重要かつタイムリーなフィードバックをもとに、MWSデータセットの公開やデータセットを利用した研究活動がさらに発展することに期待したい。

論文著者の皆さま、プログラム委員の皆さま、ご協力いただいた皆さま ありがとうございました！

さいごに

- 来年 MWS2022 のプログラム委員長は、

早稲田大学　「内田 真人先生」

引き続き、よろしくお願いいたします！🙇‍♀️🙇‍♀️🙇‍♀️