MWS2017 開催報告
―10 周年を迎えた MWS コミュニティ―

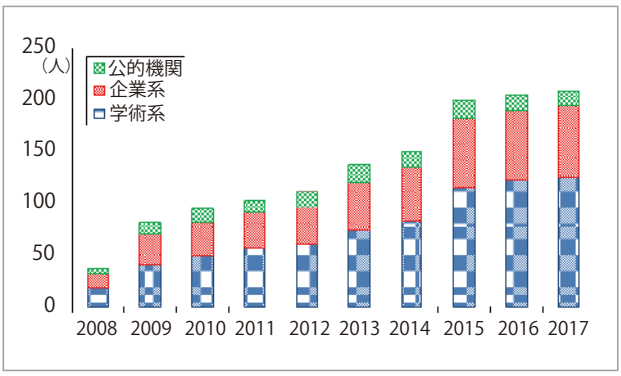

図 -1　研究用データセット活用 WG 登録者数（累積）

MWS とは

マルウェア対策研究人材育成ワークショップ（以下，MWS）は，研究用データセットの提供，研究成果の共有ならびに切磋琢磨する環境の提供を通して，マルウェアに関する専門知識を備えた研究者／実務者を育成していくことを目的に 2008 年に始まり，2017 年 10 月 23 ～ 25 日に山形国際ホテルで開催された MWS2017 で記念すべき 10 周年を迎えました．MWS は初回からコンピュータセキュリティシンポジウム（以下，CSS）との合同開催という形式で開催しており，会場手配や参加者登録といった全体運営については CSS 実行委員会に一元的に担っていただいております．これにより MWS 開催の負荷が大きく軽減されており非常に助かっております．MWS コミュニティを代表して 10 年分の感謝の意を表したいと思います．ありがとうございます．

今回は，MWS2017 開催報告として 3 つの取り組みについて紹介しながら，この 10 年間の推移についても少し触れていきます．

研究用データセットの提供

当初 MWS では，サイバークリーンセンター（2006 ～ 2011 年まで総務省と経済産業省が共同で運営していたボット対策事業）が収集したデータを共通の研究用データセットとして提供していましたが，その後はさまざまな組織にご協力いただき，Web 感染型マルウェアの観測データや，マルウェア動的解析のログデータ，大規模なネットワーク観測データ，標的型攻撃における攻撃者の活動観測データなど，サイバー攻撃の多様化に合わせてデータセットを拡充させています．マルウェア対策技術の研究開発では有効性検証のために実際の攻撃データの利用が欠かせませんが，サイバー攻撃は年々複雑化しており，本分野に参入したばかりの組織ではデータ収集が難しいケースも多々あります．そのような組織でも研究開発に取り組めるように研究用データセットを継続的に提供する取り組みは，世界的に見ても稀であり，MWS の大きな特色の 1 つとなっています．また，共通のデータセットを用いて各々の手法を評価することで相互比較ができるというメリットもあります．

このデータセットを入手するためには，まず研究用データセット活用 WG へ参加し，データセット利用申請書等のやりとりが必要ですが，初年度 40 名弱であった WG 登録者数も今では 200 名を超えており（**図 -1** 参照），10 年間における MWS コミュニティの広がりが見てとれます．しかしながら，「データセットの利用方法が分からない」といった問合せは今でも頻繁にいただきます．新規参入者への積極的な情報公開は重要です．その一方で，「データセットを誰でも自由にダウンロードできるようにしてほしい」といった要望もあります．しかし，実際の攻撃データを配布するという面で慎重にならざるを得ない部分もあり，両方のバランスをうまく取りながら良い方策を模索していく必要があります．

研究成果の共有（MWS2017）

MWS の本会議は 2016 年からは CSS のマルウェア対策・サイバーセキュリティトラック（通称 MWS トラック）として開催されており，MWS2017 では 17 セッション計 67 本の論文発表が行われました．トラック制に変更した影響も大きいとはいえ MWS2008 では 22 件の論文発表だったことを考えると，本分野の研究開発がますます活性化していることが分かります．ちなみに，MWS トラックの投稿論文は研究用データセットを利用していないといけないという条件はありませんので，関連するテーマであれば MWS トラックで発表されます（さらに言うと MWS 研究用データセットを使った成果は MWS 以外で発表しても問題ありません）．MWS のセッションは毎年多くの聴講者が集まることから今年は最も大きな会場を割り当てていただき，注目度の高いセッションでは 200 名を超える聴講者が集まったセッションもありました．

MWS2017 では 18 名のプログラム委員会によって各論文の審査が行われ，優秀論文賞，学生論文賞，ベストプラクティカル研究賞の各賞 1 本ずつ計 3 本が選出されました．MWS の投稿論文数は年々増加していますが今のとこ

ろ受賞は各1本のままですので，MWS2017では各賞の受賞率は約1.5%という非常に狭き門になっています．ちなみに，今年の優秀論文賞は岡山大学の上川氏らによる「API操作ログ取得による難読化JavaScriptコード解析支援システム」が受賞しました．本論文では，悪性Webサイトで用いられる難読化JavaScriptを効果的に解析する新たな手法を提案し解析支援システムとして実装しています．また学生論文賞には，Androidアプリについてアプリ開発者による脆弱性対応の実態調査を行った，早稲田大学の安松氏らによる「モバイルアプリ開発者による脆弱性対応の実態調査」が受賞し，ベストプラクティカル研究賞には，標的型攻撃を観測するための模倣環境構築システムを提案した，NICTの津田氏らによる「サイバー攻撃誘引基盤STARDUST」が受賞しました．こうして受賞論文を見るだけでも，Webからモバイル，標的型攻撃と非常に多岐に渡る研究発表が行われていることが分かります．

また，今年のMWSでは参加者間のコミュニケーションの活性化を目的に，いくつかの新たな施策を試してみました．1つは発表者席の固定化です．各発表の時間は質疑込みで20分ですので，発表中に十分な質疑ができないケースも多々ありますが，時に300名を超える規模の会場になることも多いMWSセッションでは，セッション終了時に発表者に質問しようとしても，どこに発表者が座っているのか分からなくなることがありました．そこで，MWS2017では座長席の前を発表者席とし，また発表者にもセッション終了後に質問に来る方のために会場に少しとどまってもらうようにお願いしました．今年の様子を見る限り，この施策は割と好評だったと感じています．

もう1つの施策はSlackの導入です．オンラインでも議論等ができるようにMWSのワークスペースを作り招待用のURLをQRコード化して会場の壁に貼ってみた結果，会期中に183ユーザがSlackに参加してくださいました．正直，用意はしたものの誰にも参加していただけない可能性もあるかと思っていたので，これは意外な結果でした．一方で，Slack上で積極的にコメントしていただいたユーザは全体の1割程度くらいで，よく利用されたかというとそれほどでもなかった印象でした．せっかくオフラインで集まっているのにSlack上でばかり議論しているのも本末転倒ですので，会期中よりは会期後に参加者間でつながるコミュニケーションツールとしての活用が有効なのかもしれません．

切磋琢磨する場（MWS Cup）

MWS Cupは2年目のMWS2009から開始した取り組みで，実際のマルウェア（悪性プログラム）を解析したり，悪性Webサイトの挙動を解析したりと研究開発に必要な基礎技術を競い合うコンテストです．MWS Cup 2017は，本会議が始まる1カ月程度前から取り組む事前課題と，初日の午前中に取り組む3つの当日課題から構成され，

図-2　MWS Cup当日課題に取り組む参加者の様子

14チーム79名が参加してしのぎを削り合いました（**図-2**参照）．こうしたセキュリティのコンテストとしてはCTF（Capture The Flag）が有名で，世界中でさまざまなCTFが開催されていますが，MWS CupがCTFと異なる最も大事な点は研究開発に必要な技術を身につけることを主眼に置いていることです．つまり，MWS Cupでは単に与えられた問題を解いて決まった答えを出すことだけを求めているのではなく，それを限られた時間で上手くプレゼンして相手に伝える能力を見たり，自分自身で課題を見つけ解決方法を考えさせるような設問を用意したりする取り組みを通じて，自分で考え・解き・伝えるという総合的な能力を身につけてほしいと考えています．ちなみに，今年は事前課題を「MWSコミュニティに必要な何か（データセットや解析ツールなど）を考えて作る」という自由課題にしましたが，新たなデータセットや有効性の高いツールの提案，セキュリティ初心者のための学習ツールなど参加者のユニークな発想でさまざまなものが生み出され，非常に面白い結果になったと思います．こうして生み出されたものはMWSコミュニティに還元され，また新たな研究に繋がるなど正のループが回ることを期待しています．

10年後のMWSの在るべき姿とは？

MWSは今年で10周年を迎えましたが，2008年と今の状況は色々変わっていて，その中でMWSコミュニティが果たすべき役割も変化していると感じています．MWS2017の企画セッションでは「次世代につなげるMWS」というタイトルでこの先10年のMWSの在り方についてパネルディスカッションを行いましたが，なかなかすぐにこれだ！という答えは出ません．ただ1つだけ確かなことは，我々は常に新しい風を求めていて，この記事を読んだあなたがもしMWSに興味があれば，いつでもコンタクトしてほしいということです．ぜひ一緒に10年後の世界を想像しませんか？

（笠間貴弘／国立研究開発法人情報通信研究機構）