MWS 2008 関係者アンケート集計結果

MWS 2008 実行委員会

はじめに

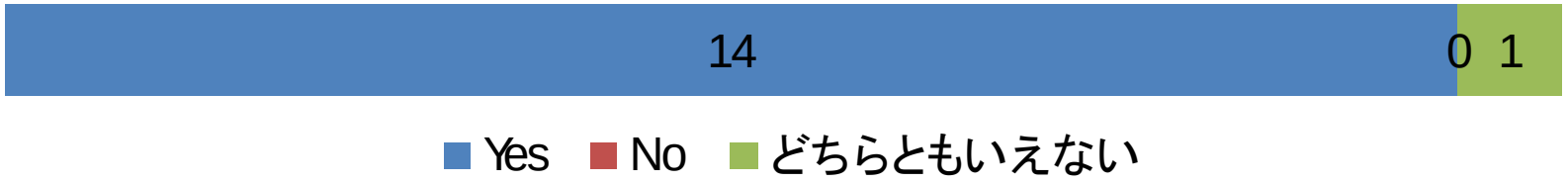
- アンケート項目
  - ワークショップ（MWS 2008）に関すること：Q1～Q5
  - 研究用データセット（CCC DATAset 2008）に関すること：Q6～Q10
  - その他、MWS 2008 についてのご意見：Q11

- アンケート収集期間
  - 2008年10月24日～11月10日

    ※MWS 2008 開催期間：2008年10月8日～10月10日

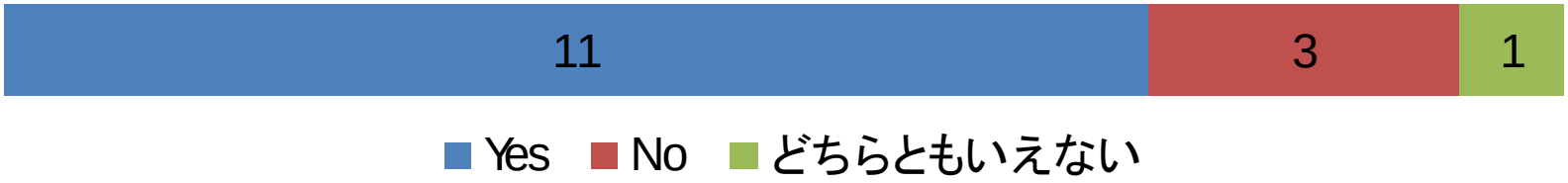
- アンケート対象者
  - MWS 2008 発表関係者
  - 回答数：15

Q1.他者の論文や発表から有用な情報を得ることができたか



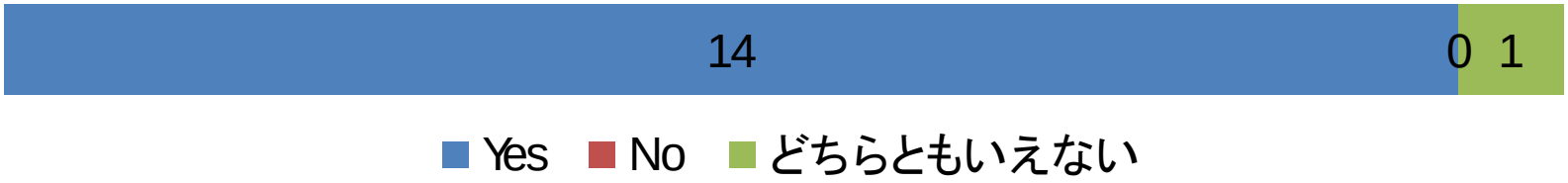
- ご意見（抜粋）
  - 同一のデータセットに対して異なる視点からの解析データ結果は非常に興味深かった。自身の研究にも利用できそうな解析結果や手法も多数発表され、今後の研究を行う上での良い参考となった。
  - 特に、自社のデータとの比較については、従来のワークショップでは得られない興味深いデータも含まれており、有益であった。
  - 同じ研究素材を対象に異研究領域の専門化が研究し、知見を報告しあうことに意義を感じる。同じ素材を各研究者（発表者）も触っていたこともあり、異研究領域の発表内容への理解も比較的容易であった。
  - 分析結果の矛盾や解釈の違いなどをもっと議論したかった。

Q2.他者の研究者との情報共有や意見交換ができたか



- ご意見（抜粋）
  - 同じデータセットを解析した者同士しか分かり合えない箇所、困難について意見交換することができた。また自身が分からなかったところを他者の結果と比較するとより大きな全体像が見えてきて、情報交換、連携の重要性を再確認した。
  - 本分野の日本の研究者の顔が分かるようになったのは有意義であった。
  - 意見交換のための時間が十分に確保できなかった。同一データセットを利用することで、研究結果の情報共有ができたと思う。
  - セッションでは質疑応答時間が限られるため、オフラインで質問したりする機会が欲しかった。

Q3.他研究者との情報共有や意見交換を今後しようと思うか



- ご意見（抜粋）
  - 対策実務側として、今後も対策手法の議論やデータ共有といった面などからも交流できればと考えています。
  - MWS会期中の出会い等をよいきっかけとして、今後とも是非交流を続けさせて頂ければと思っています。
  - 研究用メーリングリストや掲示板など、情報共有インフラが整えばぜひ継続したい。ただし、データセットの利用が制限されている以上、本ワークショップの延長線での活発な議論は難しい。

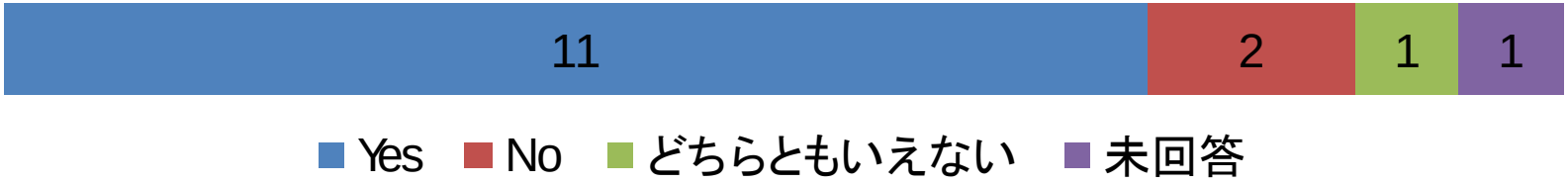
Q4.研究発表に期待していた内容

- ネットワークの運用現場に近い研究と、対策につなげられそうなアイデアの発表や議論を期待していました。例えそうしたアイデアが現在の製品技術や法制度などの制限で即時の実施は難しくとも、今後実現のために技術開発や法制度整備の活動をしていけば良いので、実際の現場の制限にとらわれず自由な発想のアイデアの発表や、研究者との議論ができればありがたいと考えていました。
- マルウェア解析を容易にする解析ツール、もしくは環境の提案を期待していました。
- 本ワークショップでの発表は、どちらかと言うと、研究者側からのシーズの発表が多かったのではないかと感じています。ISPの皆様からのニーズをご発表して頂くことによって、ニーズとシーズが絡み合うような効果が得られると更に良いのではないかと思っていました。
- このようなワークショップ自体が初めての試みでしたので、どのようなワークショップになるのかということ自体が興味深かった。

Q5.データセット毎の研究発表とパネルディスカッションというセッション構成の他に有意なセッション

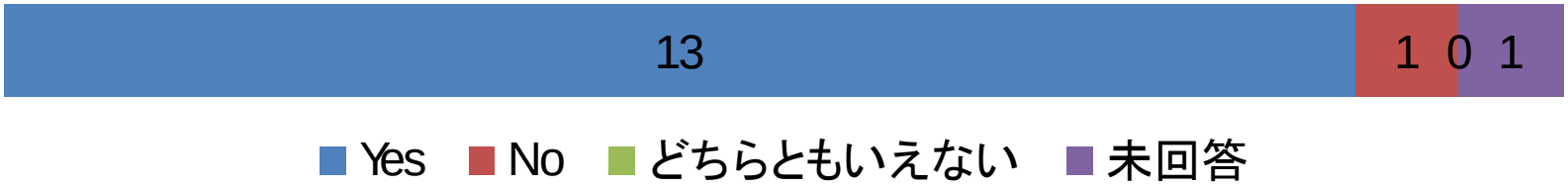
- より多くの時間を発表者と聴講者で議論する時間としてポスターセッションがあればさらに有意義だと思います。
- 研究発表のセッション毎に発表者によるパネルや、産業界へのフィードバックを考えるパネルなど、テーマを絞ったパネルディスカッション。さらに、今後の展開を議論する時間がもっとあった方がよかったと思います。
- データセット自身を研究題材としたセッション（観測環境、収集方法、既存ツールの比較評価、など）があると良いと思いました。ゆくゆくは、ある組織が責任もってデータを提供するのではなく、参加者がその雛形に基づき事前に収集/観測できるような、本ワークショップ向け専用の収集環境の雛形を構築してもよいのではないでしょうか。
- 調査報告、研究報告、デモ、ハンズオンなど、色々な形式での発表があってもよいと思う。発表時間枠を複数決めて、発表者が選べるような柔軟性を持たせても面白いのではないでしょうか。

Q6.データセットにより従来実施できなかったことができたか



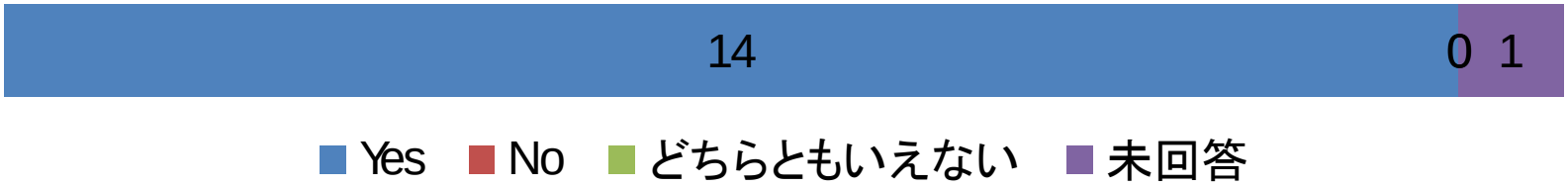
- ご意見（抜粋）
  - 独自に収集しているデータと比較することができ、その差異や共通する点など多くの知見を得ることができた。
  - 提案手法の有効性を評価することができ、理論を証明するための実践的なデータの必要性・重要性をあらためて感じた。
  - データセットによって、新たにマルウェアの研究を行うことができた。大学等、マルウェアのデータを取得することが難しい研究機関にとって、データセットの提供は非常に有意義なものであると思う。

Q7.データセットの使用により新たな研究課題の発見につながったか



- ご意見（抜粋）
  - 異なるネットワークでは、ハッシュ値で比較する限り、収集した検体が一致する件数は思っていたよりも少ないという発表もあり、全体の傾向を知ることの困難さに課題を感じました。
  - 長期間の「攻撃元ログ」は各自で運用しているハニーポットでは収集するのが難しく新しい課題の発見などにつながる。逆に攻撃通信データのようなデータは一般に収集するのはそこまで難しくないので、そこから新しい研究課題の発見につなげるのは難しい。
  - データセットを利用することで、マルウェアの動作傾向を調査することができた。その結果から、対策手法の検討等を行うことができるため、新たな研究課題の発見につながったといえると考えている。

Q8.データセットを対象とした研究の必要性を感じたか



- ご意見（抜粋）
  - この研究分野が非常に多くのサブエリアを含んでいると感じました。様々な視点からの研究を可能にするために、データセット自身がどうあるべきかという議論もとても重要だと思います。
  - 実データに基く研究は必須ではありながら、機密性の高い情報が含まれる可能性があり、研究者個人で収集する必要があるため、研究とは少し逸れた所で労力を費やす必要がある。今回のように有用なデータセットを提供して頂けると手法の研究開発に注力することができ非常に必要性を感じた。
  - 理論の実データによる有効性の検証、他技術との定量的な比較検証を実施するためには、普遍的なデータセットの存在が必要不可欠である。

Q9.研究を行って感じたデータセットへの要件（優先度順）

- 「マルウェア検体」について
  - 耐解析性が高い、ウイルス対策ソフトで検出できない、機能が豊富、一般に取得が困難、攻撃対象OS種類、その他（鮮度、量）
- 「攻撃通信データ」について
  - ハニーポットのグローバルIPアドレス情報、データ収集台数、データ収集期間、ハニーポットの動作特性、攻撃対象OS種類、その他（鮮度、攻撃元データとの照合）
- 「攻撃元データ」について
  - ハニーポットのグローバルIPアドレス情報（または識別子）、データ収集台数、データ収集期間、送信元・宛先のポート番号、障害による停止期間、期間中の構成変更情報、ハニーポットの動作特性、攻撃対象OS種類、その他（データの鮮度、攻撃通信データとの照合）

Q10.データセットとして提供されるのが望ましいデータ群

- Web感染型をはじめとして、様々な感染経路（入手経路）で得られたマルウェア検体や関連するデータを提供いただけると、その違いを調査したり、と色々興味深い研究につながると思います。
- 最近の検体はVMやデバッガを検知して活動をやめる機能を備えているため、素のPC上で検体を実際に起動させた際のPCの挙動（ファイル変化、プロセス起動、通信ポート開放、など）に関するデータが提供されていると助かります。
- 既存の解析結果にはない新たな挙動が見つかることもあるし、自分の解析力の目安にもなるので、人材育成を考慮し、「マルウェア検体」はすでに解析結果が公表されているもの、あるいは解析結果の模範解答があっても良い。

Q11.その他、MWS 2008 についてのご意見

- 実務側からの人々もさらに多く参加して情報共有や議論を行えるような場になることを期待しています。論文執筆が不要の発表のみのセッションを設けるなども、そうした場の形成に役立つのではないかと思います。
- マルウェア対策についてのアカデミックな場ということで、論文として形に残すことは有意義だと考えます。継続的に行うことで見えてくる問題や発見があると思うので、継続的な実施ができるとよい。
- 論文提出が不要な発表が可能であれば、ちょっとした小ネタを持ち寄る場として有益です。また、1ヶ月か2ヶ月に1回程度の報告会のようなものがあっても良いかもしれません。
- ワークショップで解析された結果をまとめて海外に対して発表してはどうか。また、研究用データセットもオープンにし、発表者を広く募ってもらいたい。

Q11.その他、MWS 2008 についてのご意見（Cont.）

- 入出力フォーマット等を規定することによって検体に対する処理を自動実行するようなテストベッドを、システムとして開発・運用できると良い。もしくは検体を確実に実行できる実行環境も提供すると良い。
- 主催者であるサイバークリーンセンター（CCC）に何らかのフィードバックができるよう現状の課題、問題点などを明らかにし、それを解決するための研究を一つのジャンルとして募集するとよいかと思います。
- 検体の種類数等を数える時のルールや用語が統一されてくるとよいと感じました。回を重ねることで参加者の共通意識として整理される面もあると思いますので、是非、今後も実施していただければと思います。
- 開催に向けた様々な準備をありがとうございました。今回だけで終わることなく、ぜひ、継続して開催できるようにして欲しいと思いますし、そのために微力ながらもご協力できればと思います。