MWS 2009 関係者アンケート集計結果

MWS2009実行委員会

はじめに

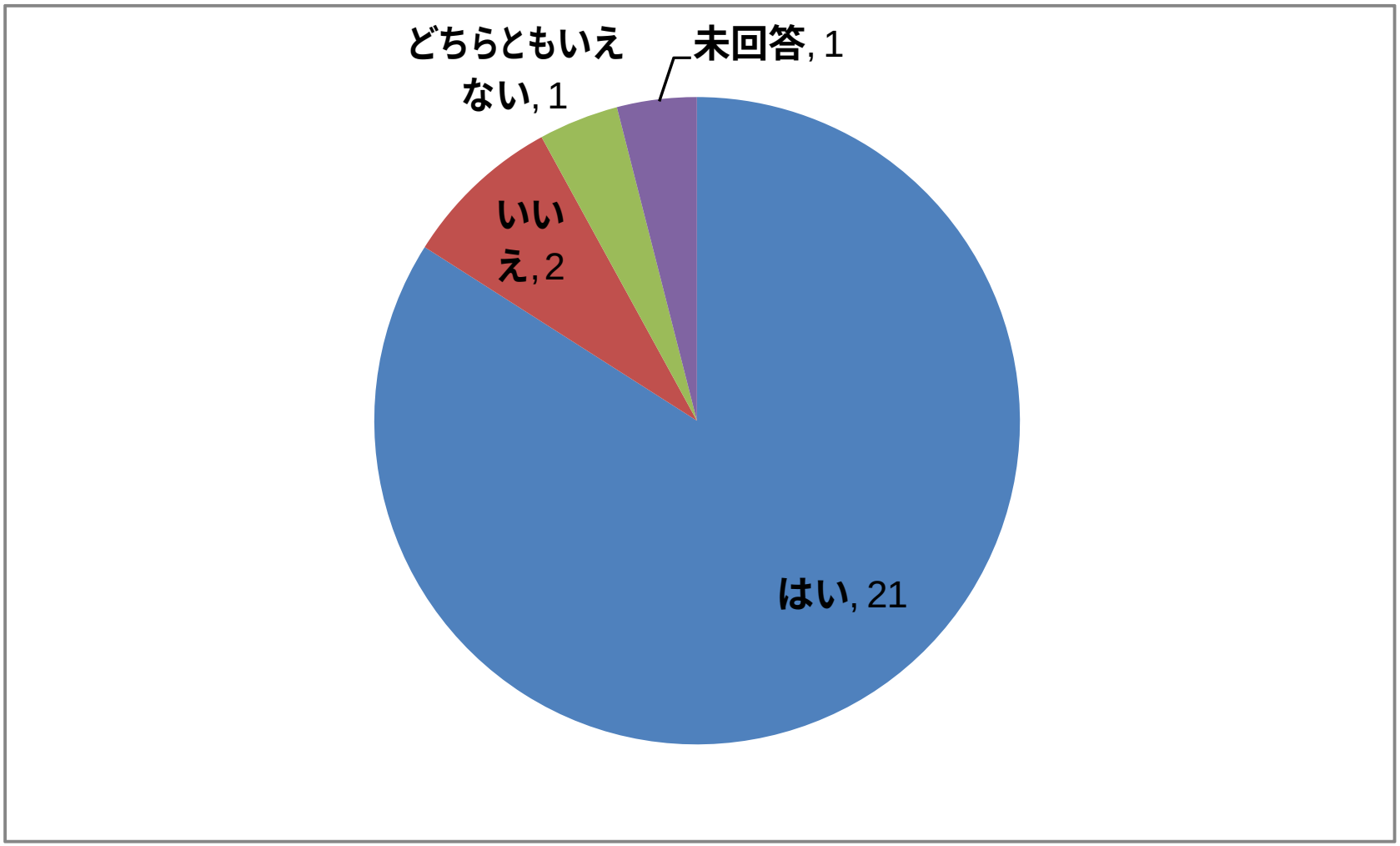
- **アンケート項目**
  - MWS 2009 **に関すること**：Q1～Q6
  - CCC DATAset 2008/2009 **に関すること**：Q7～Q14
  - MWS Cup 2009 **に関すること**：Q15～Q17
  - **その他**：Q18

- **アンケート収集期間**
  - 2009年11月24日～12月7日

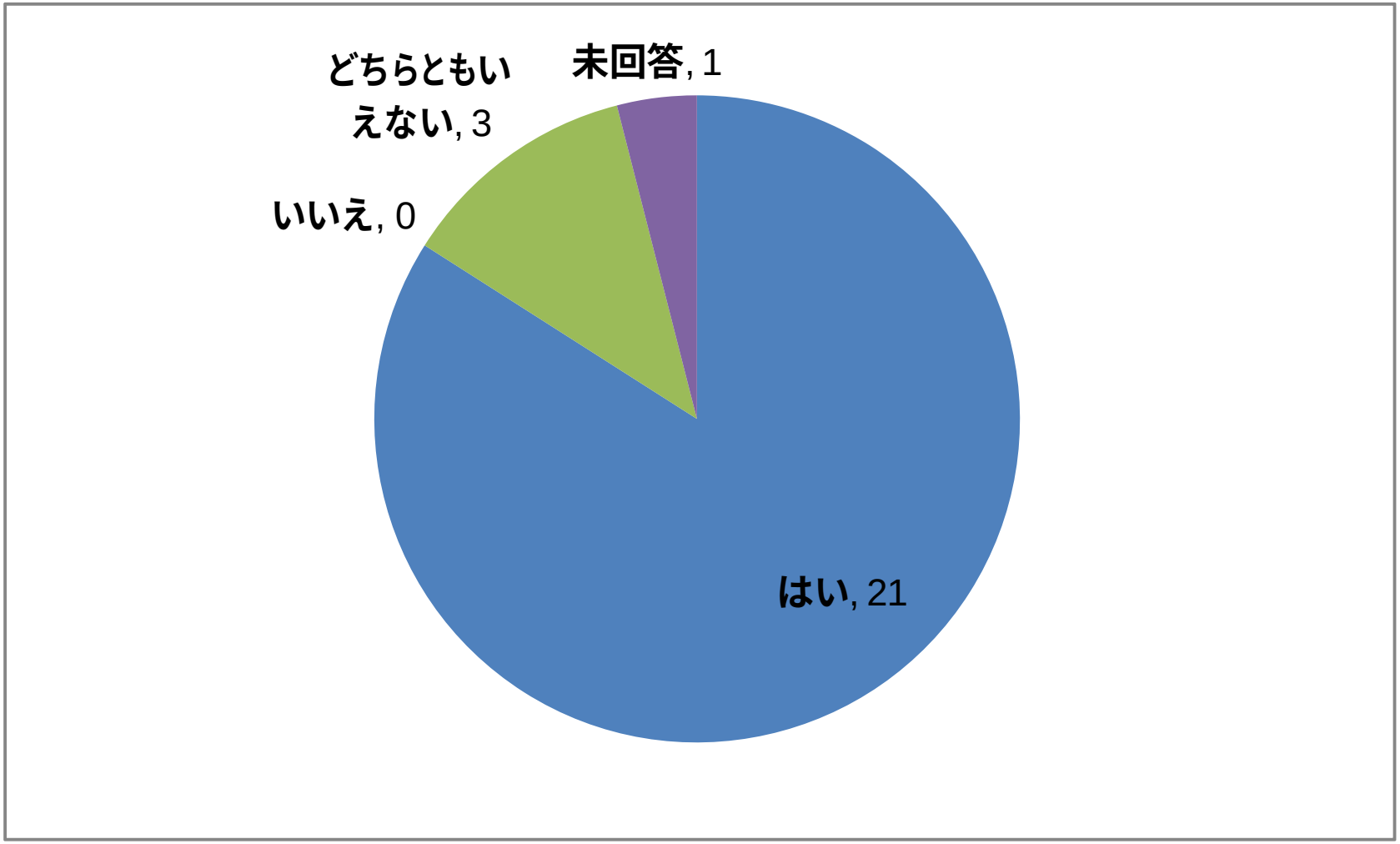
    ※MWS 2009**開催期間**：2009年10月26日～10月28日

- **アンケート対象者**
  - MWS 2009 **発表関係者**
  - **回答数**：25**名** (16**組織**)

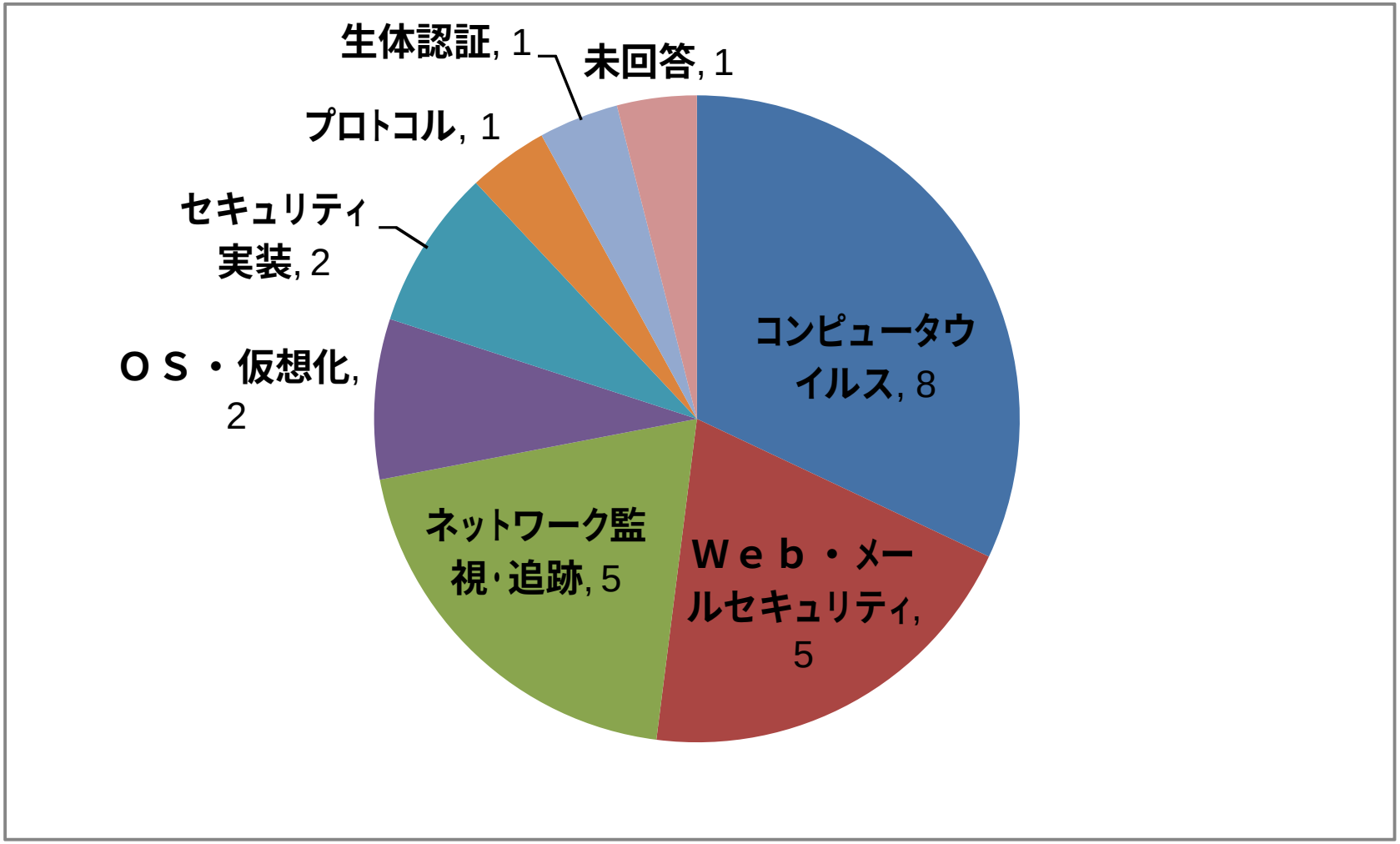
Q1.他の論文や発表から研究課題や目標が発見できたか？



Q2.他の研究者との情報共有や意見交換ができたか？



Q3.合同開催のCSSで一番参加したかったセッションは？



Q4.パネルディスカッションはどんなテーマがいいですか？

- MWSでの成果を現実のマルウェア対策にどう活用していくか
- ウィルススキャナやパターンファイルを作っている人が，研究に何を期待するのか聞いてみたい
- 研究･開発の成果をサービス化するための課題や方法について
- マルウェア対策研究の今後の方向性や課題について
- マルウェア対策研究を進めるために必要となる共通の研究開発基盤について、誰がどのようなものを整備し、公開･運用するべきか

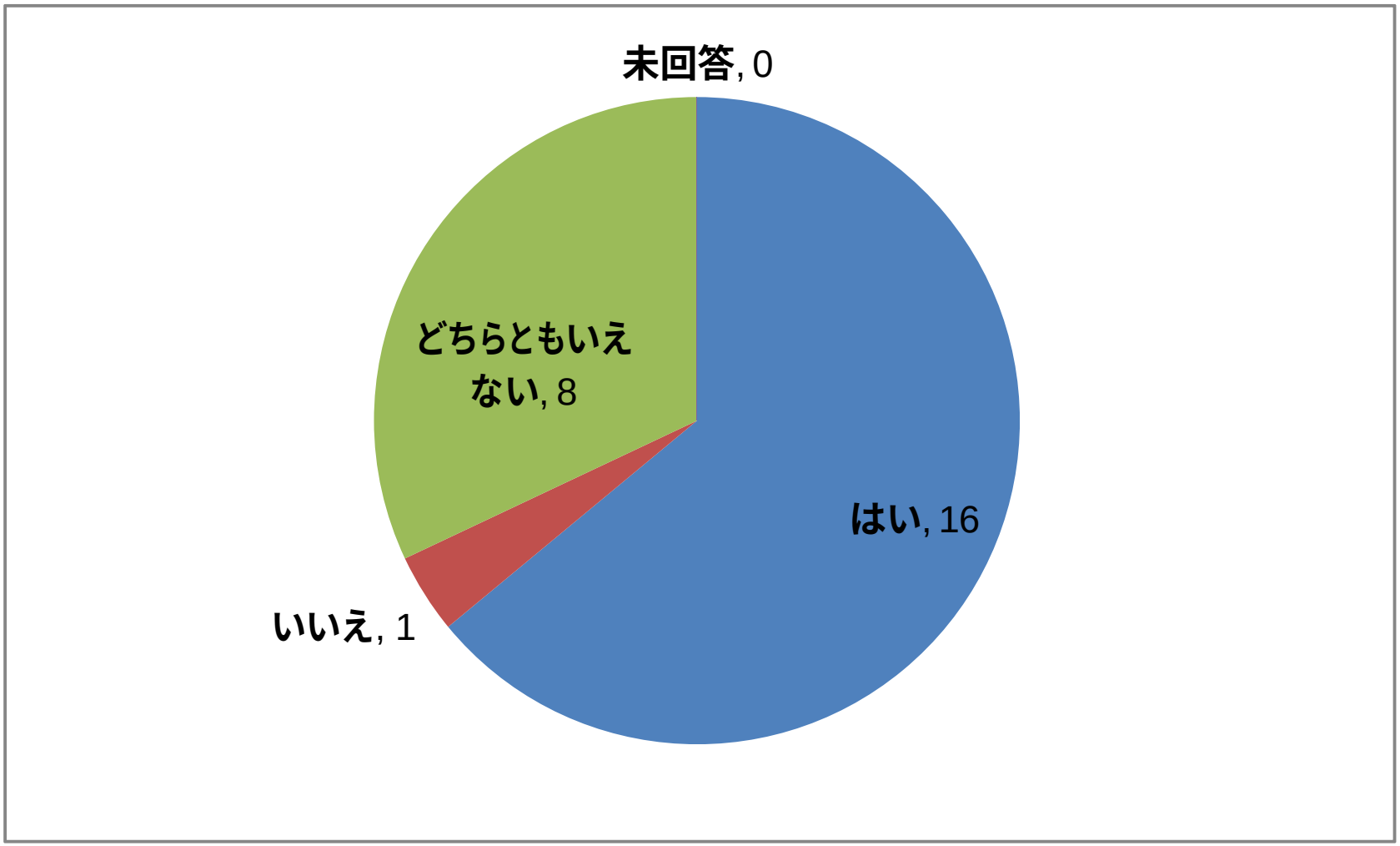
Q4.（Cont.）

- 企業／現場からの研究への期待
- 国内と海外での研究結果の比較や研究環境の違い
- 「最近のこれ、どう?」といったテーマについて
- 研究技術を産業界へどのようなステップで、利活用していくべきか
- 最新ネットワークインフラ（クラウドetc）とマルウェアについて（新しい感染経路が確立されるのか等）
- 解析技術や解析手法、現場で実際に対応している方のやり方などから、どうすれば効率よく解析できるか
- 会場からも自由に発言し合う場があるとよい

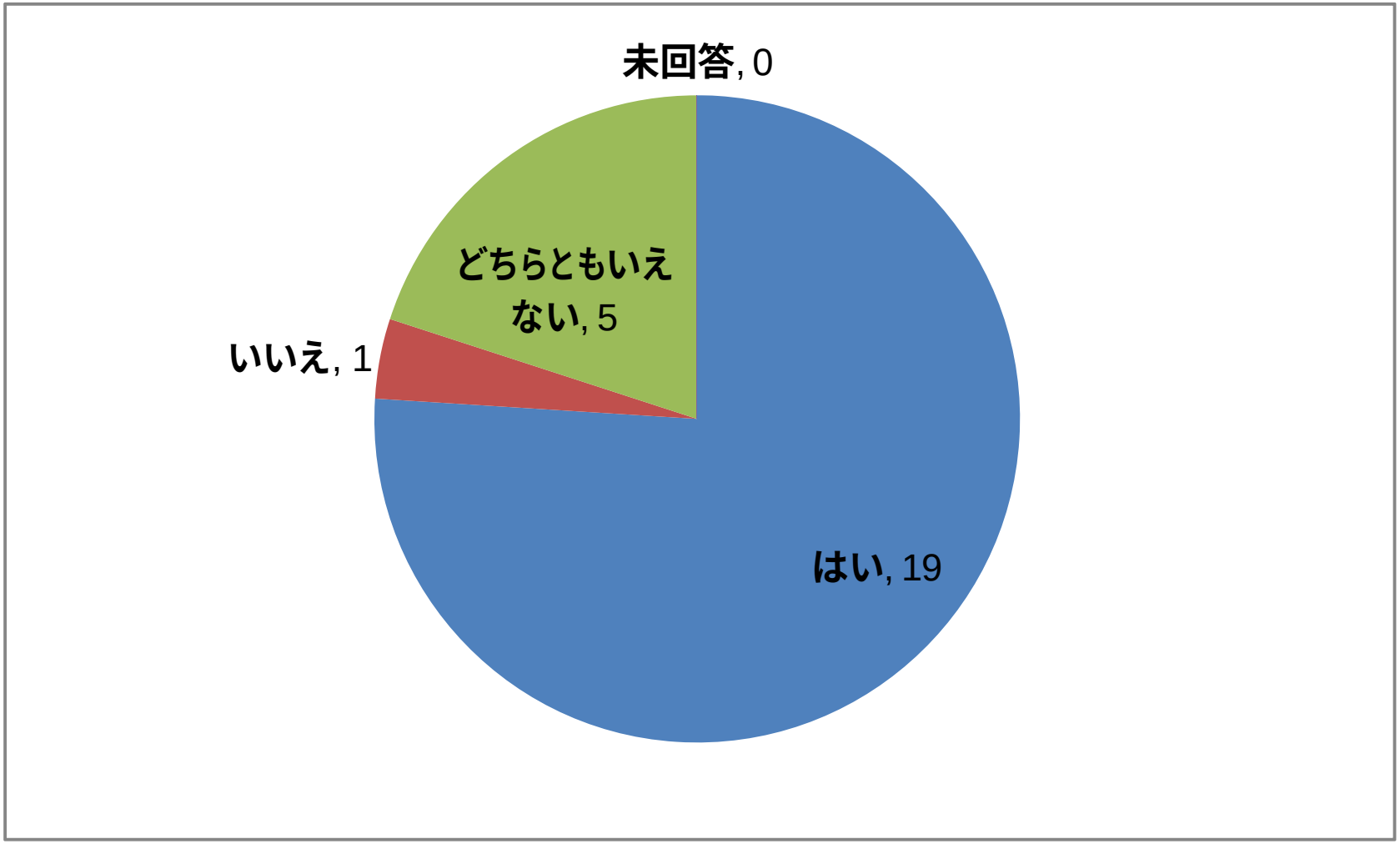
Q5.研究発表、パネル以外にどんなセッションがあるといいですか？

- マルウェア解析のチュートリアル
- データセット未使用での研究発表
- 論文なしプレゼン
- BOF
- デモセッション
- ポスターセッション，査読付き論文（口頭発表）
- 同一データセットの解析について深い議論をするために、各セッションの最後に発表者間でのディスカッション
- 双方向で議論/意見交換できるようなセッション
- 話題・課題提供のみのセッション

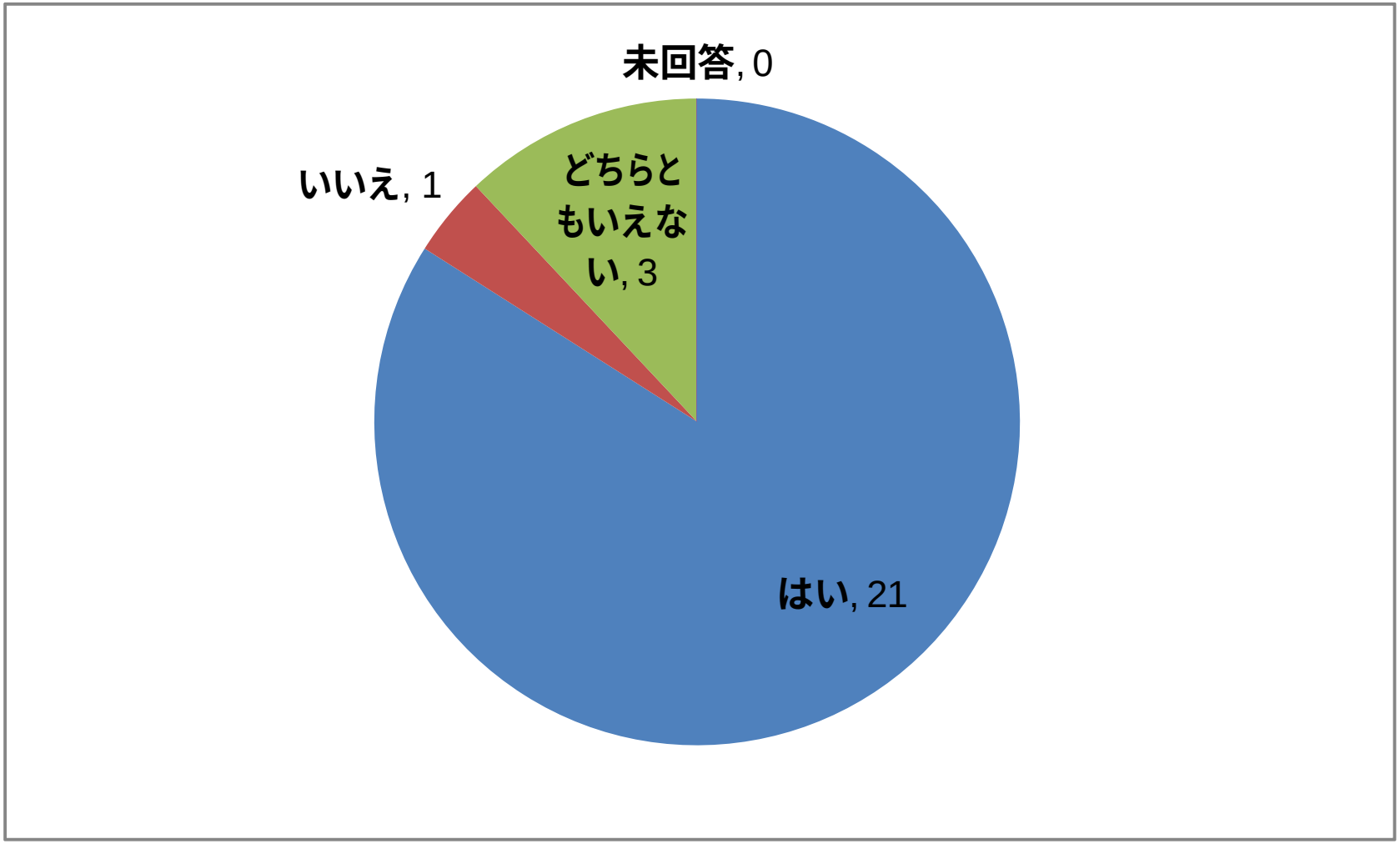
Q6.来年の MWS2010 でも発表しようと思いますか？



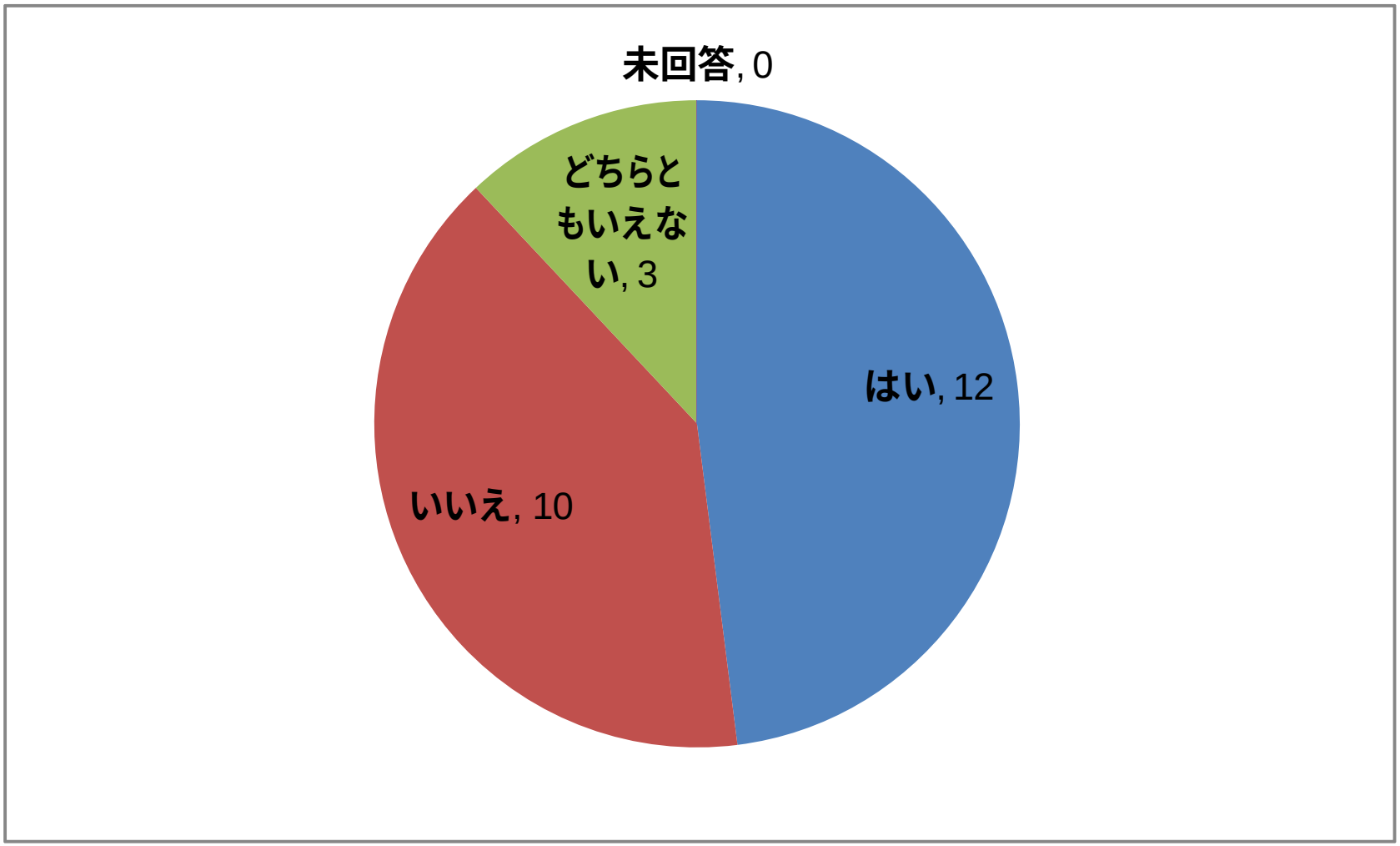
Q7.データセットにより従来実施できなかったことができたか？



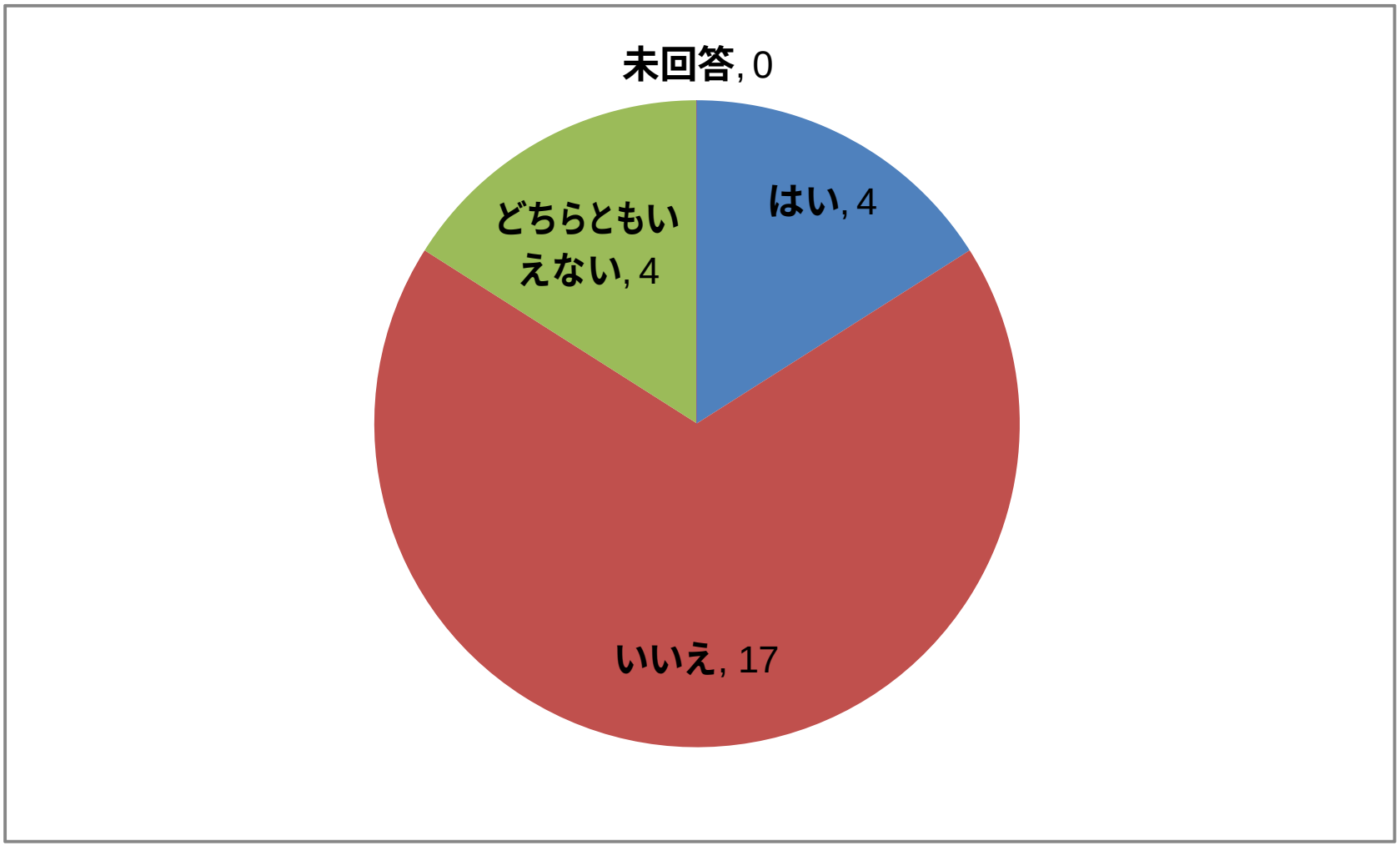
Q8.データセットそのものの研究の必要性を感じたか？



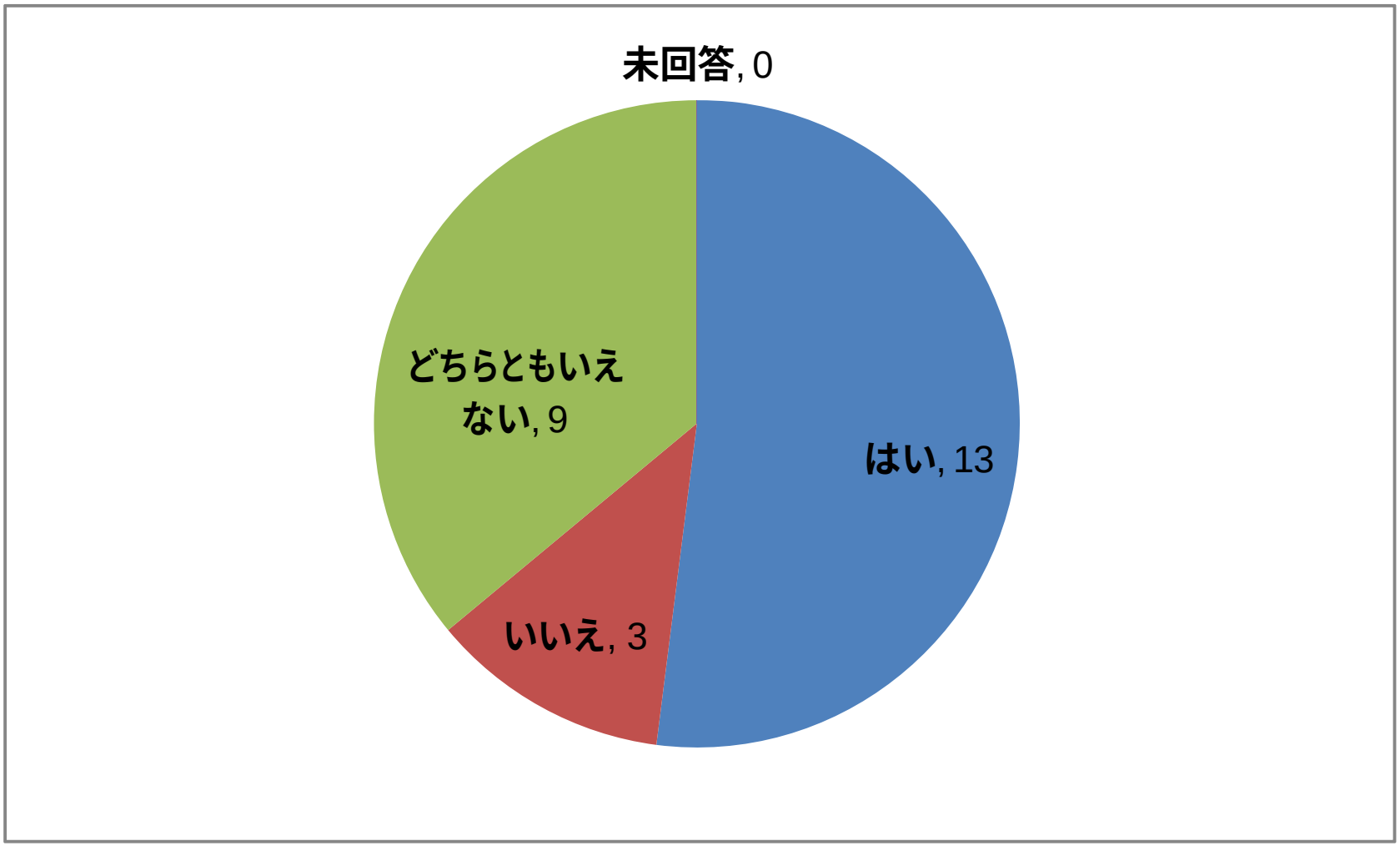
Q9.昨年 (2008) のデータセットも提供しましたが、発表に限らず利用しましたか？



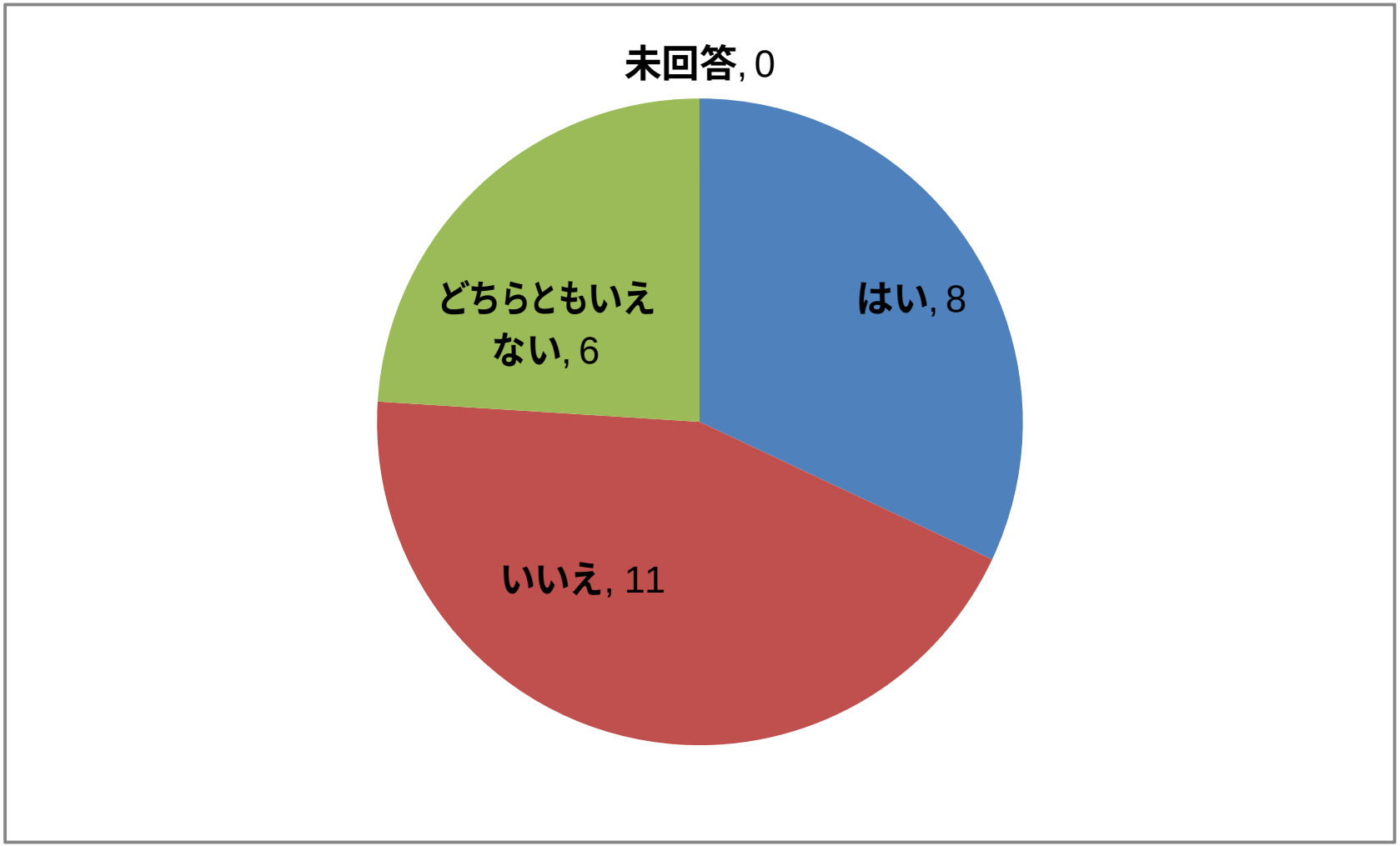
Q10.分割して時期を少し早めて提供開始しましたが、その間に利用しましたか？



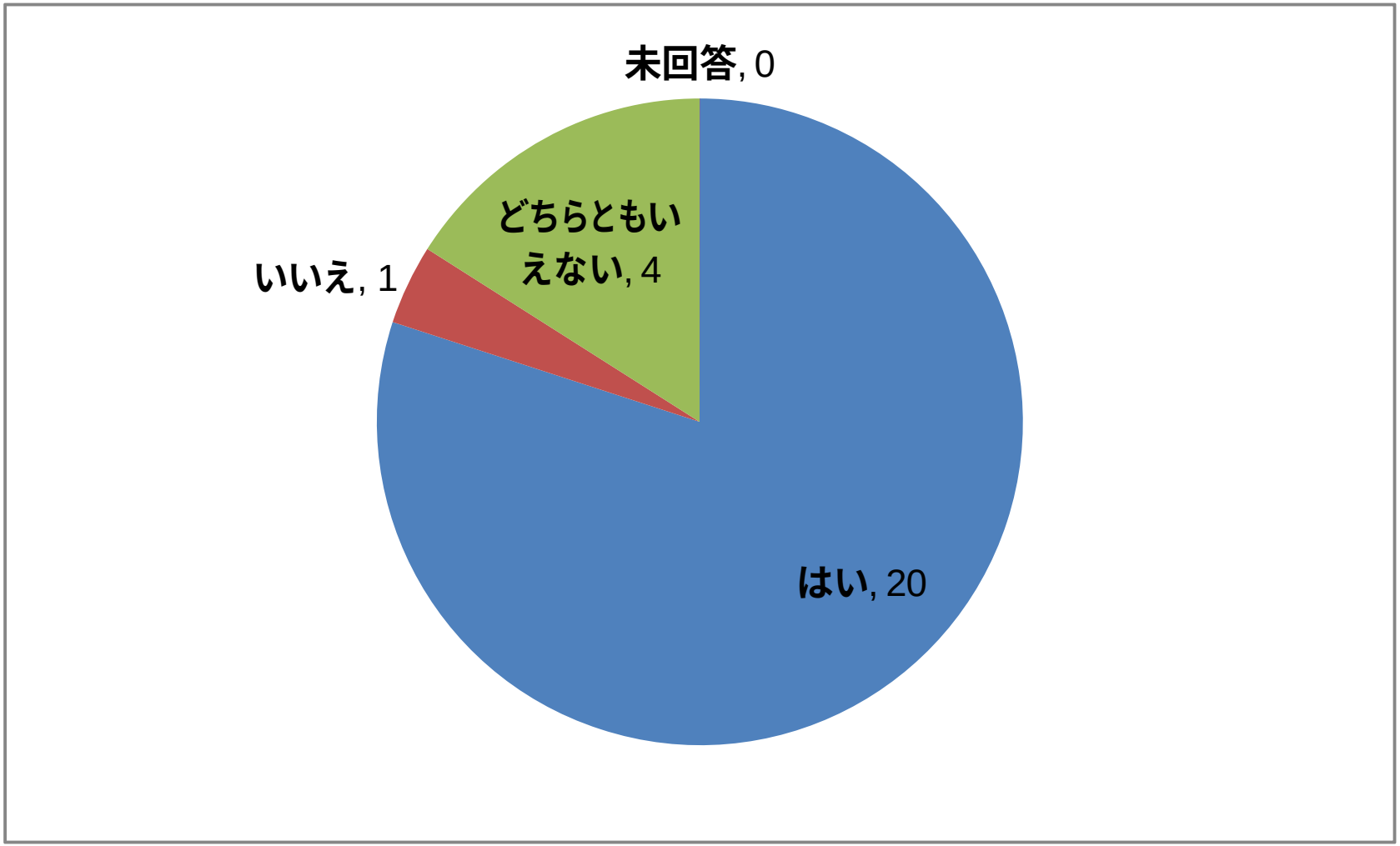
Q11.利用期限を年度末までに拡大しましたが、MWS2009後に利用します/利用しましたか？



Q12.MWS2009以外でデータセットを利用した発表予定はありますか？



Q13.動作記録データを実際に見てみたいですか？



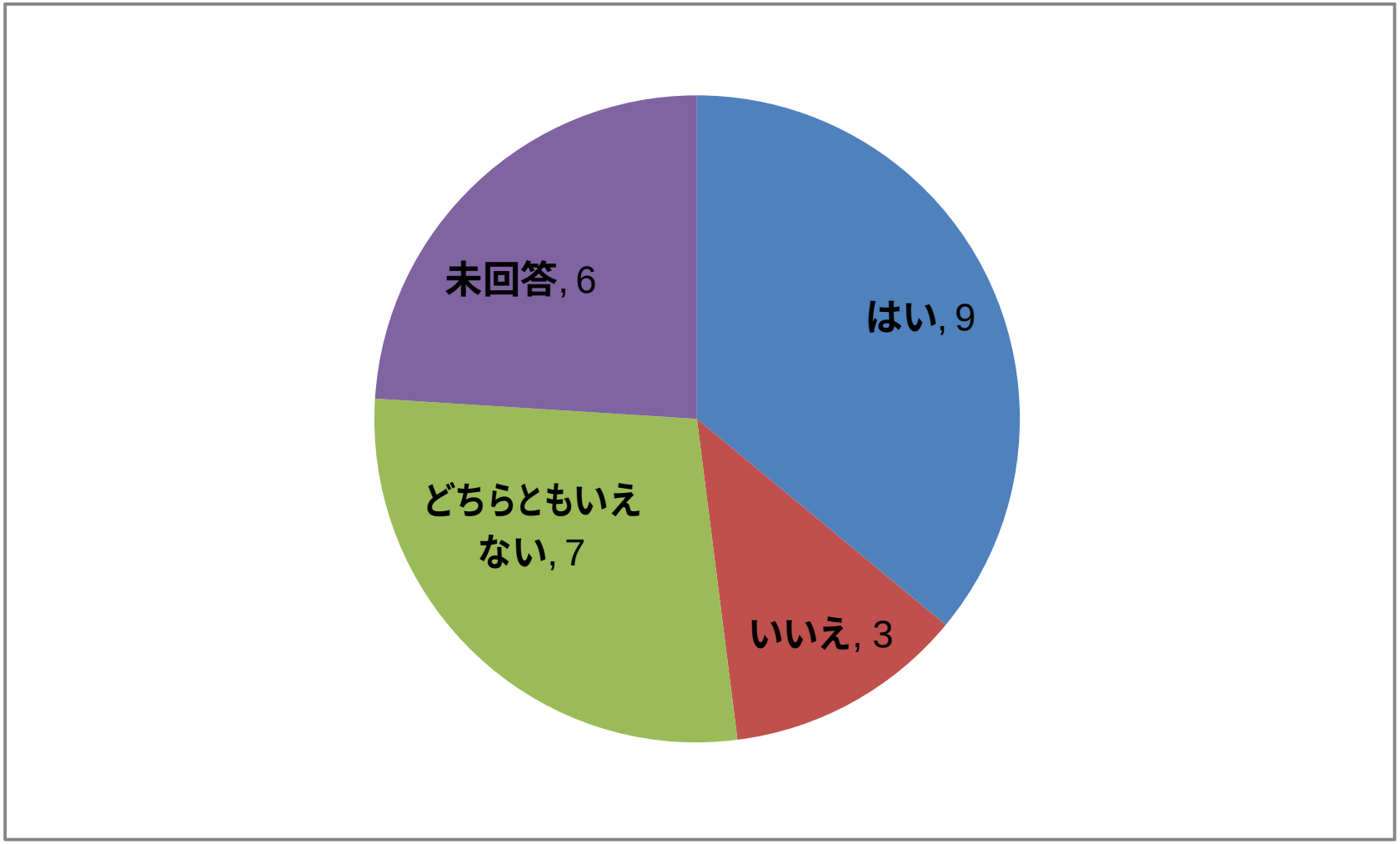
Q14.どんなデータセットが提供されるといいですか？

- より長時間、かつ実際の動作環境に近い環境でマルウェアが動作した時のデータ
- ハニーポットのネットワーク構成や位置がわかる情報（相対的な位置であれば一定の処理により実際のIPアドレスを隠蔽する等も可能）
- 様々なOS・サービスパックのハニーポットで収集したデータ
- 誰でも自由にアクセス出来て，検証が可能な公開データ
- 常に最新の情報が入っていて、かつ、いつでも入手可能で、かつ、長期間にわたって利用可能なデータ
- 代表的なマルウェア解析ツールによる分析結果

Q14.（Cont.）

- ネットワーク(LAN)単位や、数ヶ月規模のトラヒックデータ
- アンチウイルスソフトの検知率の評価に利用できる多数のマルウェア
- IDSの検知率を評価できる教師付き攻撃パケットデータ
- 外観から感染マルウェアがわかる感染時のPCの挙動
- もう少し長期間のpcapデータ
- Web感染型を例とする様々な感染経路で収集されたマルウェアに関するデータ
- その年に話題となったマルウェアに関するデータ
- 通常トラフィックのpcapデータとIDS（ｳｲﾙｽGW含）の検知データ

Q15.競技用データに関しての事前情報は足りてましたか？



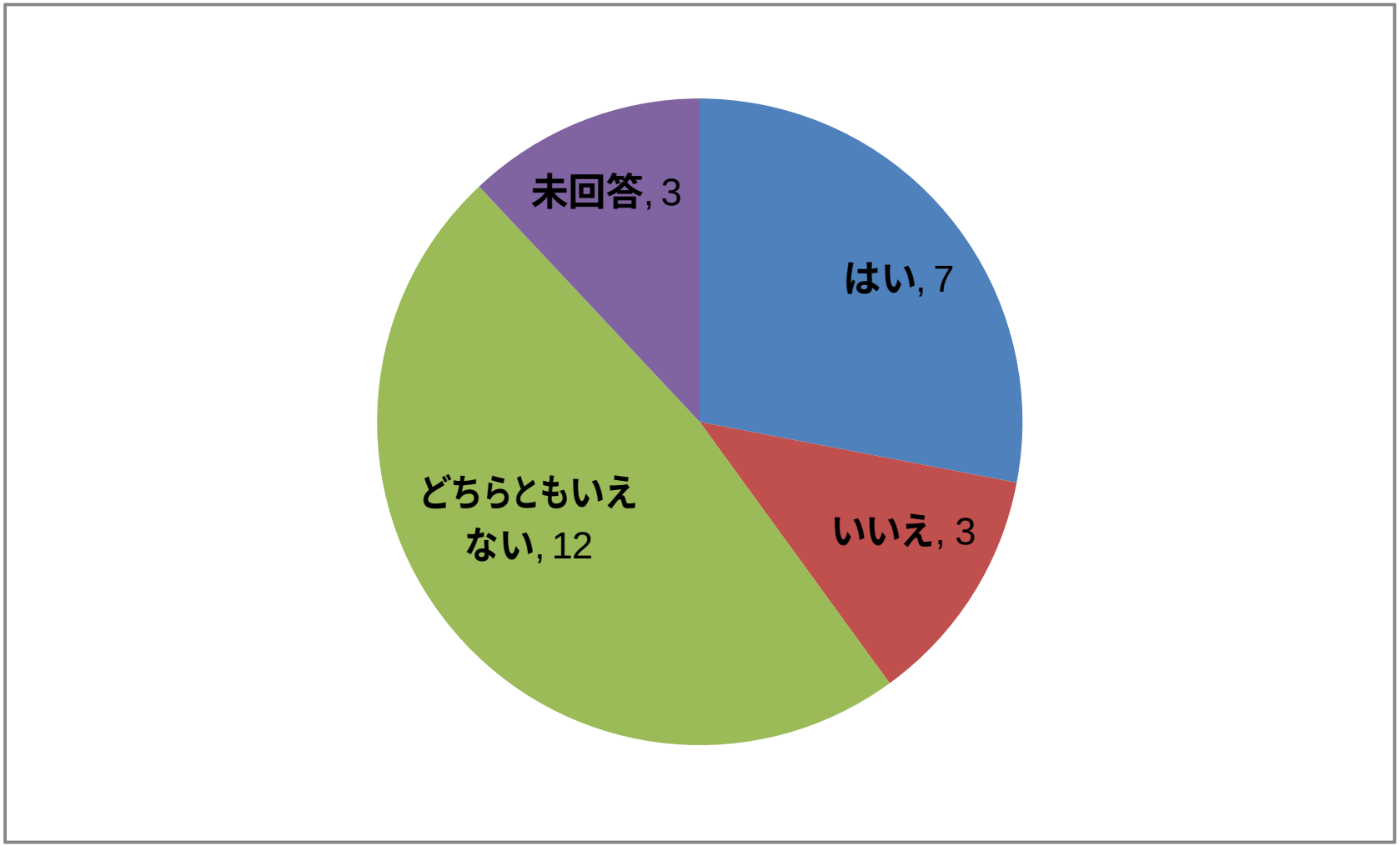
Q16.競技、発表についての率直な感想

- 発表を聞く限りでは、想定していたより難易度が高かったように感じた。
- Cupを実施する側も参加する側も、新たなチャレンジという意味で、やることそのものに意義があったことは間違いないと思う。
- 参加者が実際にどのような方法でトライしたのか、なぜうまくいって、なぜうまくいかなかったのかの報告や議論が発表を通じてできると、人材育成の面からもなお良い。
- やってみて、とてもおもしろかったです。継続できると良いと思う。
- お互いに各チームの解析の進捗がわかると盛り上がりそう。

Q16.（Cont.）

- 問題の難しさとそれを公平に評価するための競技の難しさを痛感した。
- 実攻撃から離れてしまうため、加工無しのデータを使いたい。
- 事前に解析用データのサンプルがあるとよかった。
- 取り組み・発表とも面白く、興味深かった。学生が積極的に参加していたのが印象的。
- 今後も続けて欲しい。トラヒックデータ以外を使った競技会（例えばマルウェア検体）などがあってもよい。
- 短時間での解析が要求される点が面白い。

Q17.来年の競技（MWS Cup 2010）に参加しようと思いますか？



Q18.MWS全般についてご意見お待ちしております

- 卒業に伴い来年の参加はできませんが、興味を持っている研究室の後輩がいるので、これからもこのような試みを続けて頂きたい。
- MWSの開催、データセットの提供について、ぜひ今後とも継続していきましょう。とても意義のあるものだと思いますし、成果を得るにはある程度の期間が必要と思う。
- 攻撃元データを分析したが、現在の情報量だと意味のあるパラメータの抽出が結構難しく、もう少し情報がリッチなほうがより深い調査ができると思う。
- 論文としてまとまることは、ノウハウの水平展開に繋がりとても良いことだと思う。今後も参考にしていきたい。

Q18.（Cont.）

- ぜひ継続的な取組みとして続けて頂きたい。
- 初参加でしたが、自分が考えたことが無い視点で取り組まれた論文が多数発表され、大変勉強になった。
- 聴衆を交えた意見交換がさらに活発になると、多面的な深い知見が得られると思うので、質疑応答の時間を多めに確保できると良い。
- 非常に順調に成長している取組だと感じている。今後も継続して頂きたい。
- 静的解析周りの話題などすこし幅があるとより興味深い議論ができると思う。