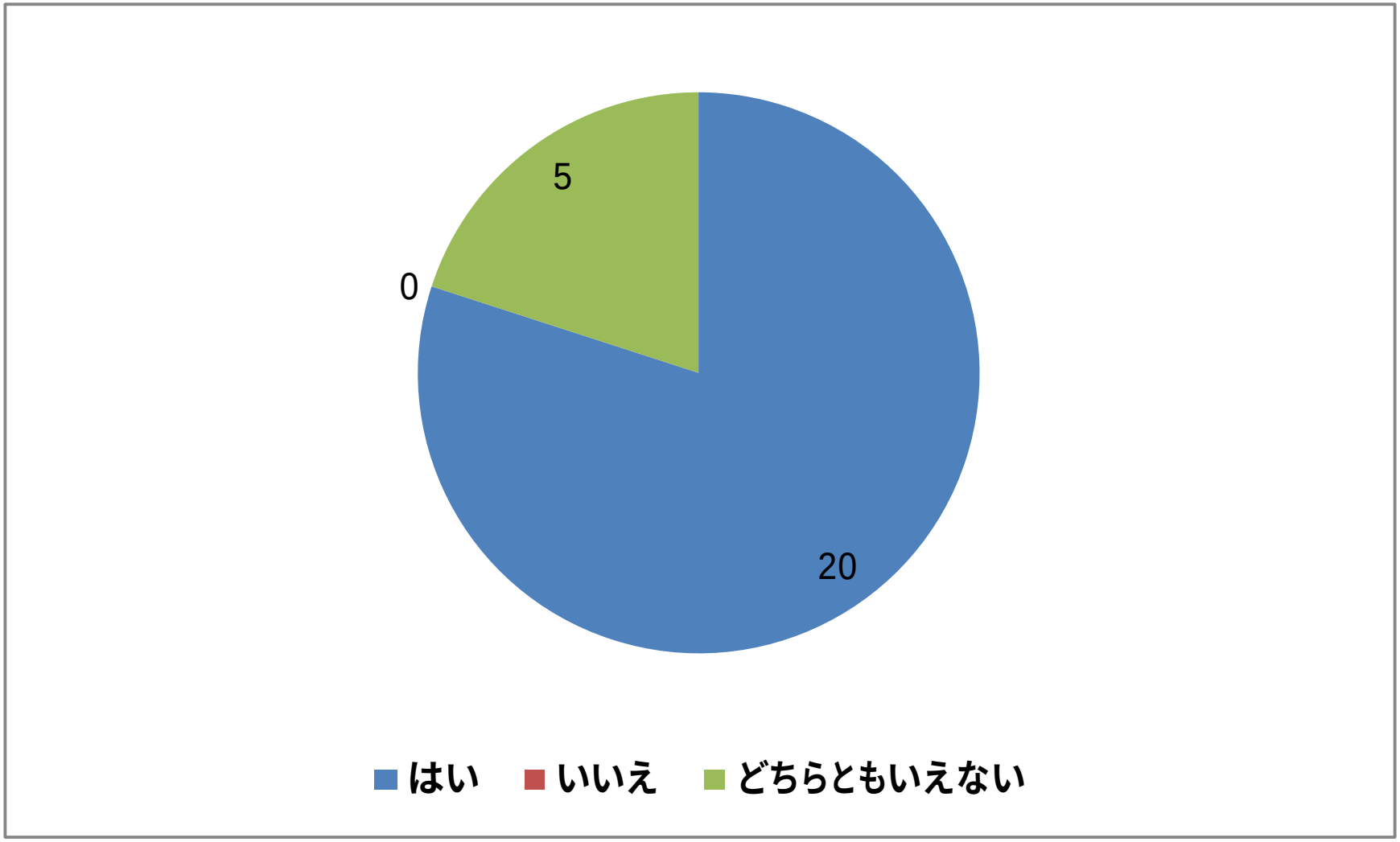
MWS 2010 関係者アンケート集計結果

MWS2010実行委員会

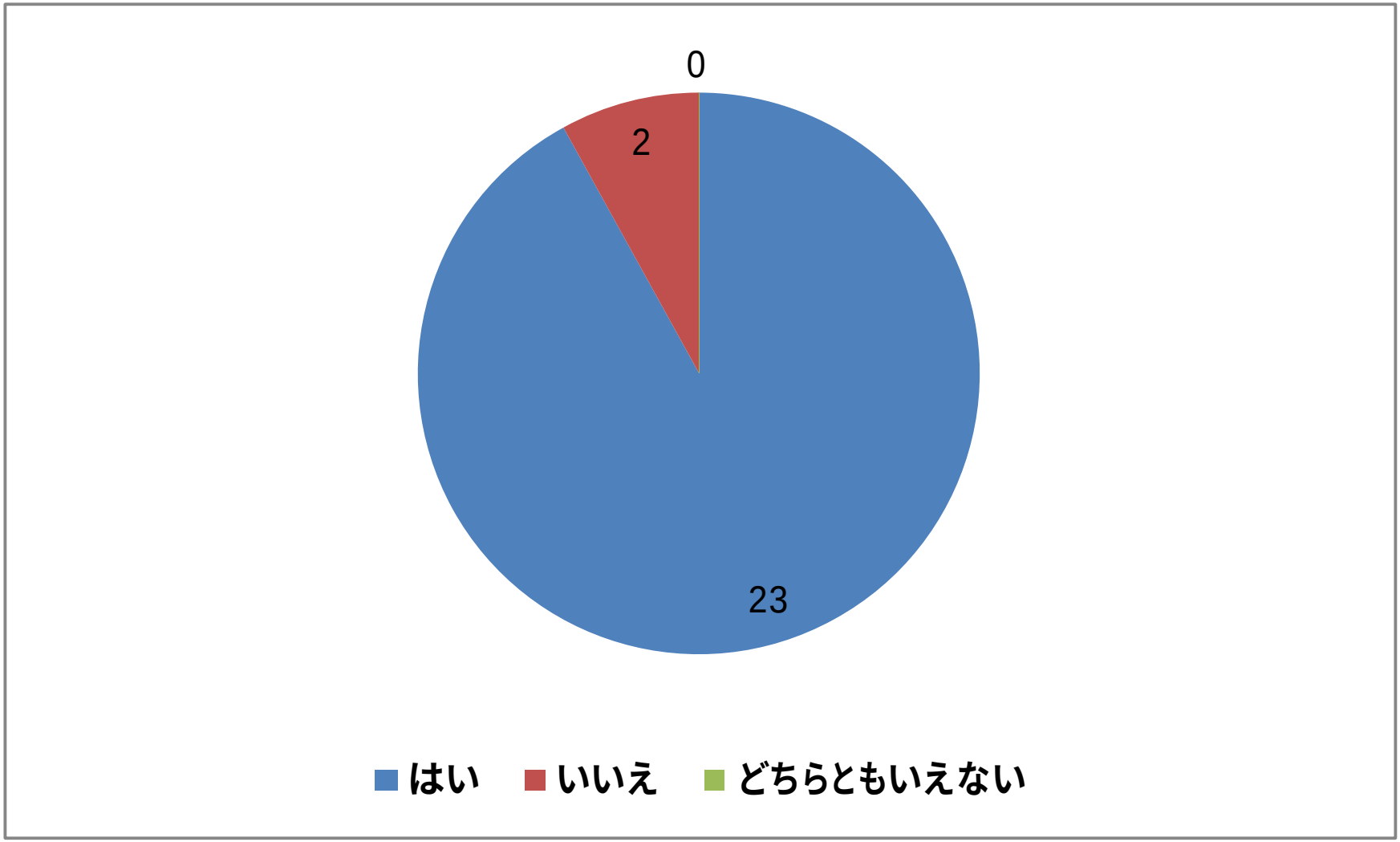
はじめに

- **アンケート項目**
  - MWS 2010 **に関すること**：Q1～Q5
  - MWS 2010 Datasets **に関すること**：Q6～Q14
  - MWS Cup 2010 **に関すること**：Q15～Q18
  - **その他**：Q19
- **アンケート収集期間**
  - 2010年11月26日～12月10日
- **アンケート対象者**
  - MWS 2010 **発表関係者**
  - **回答数**：25人 (14組織)

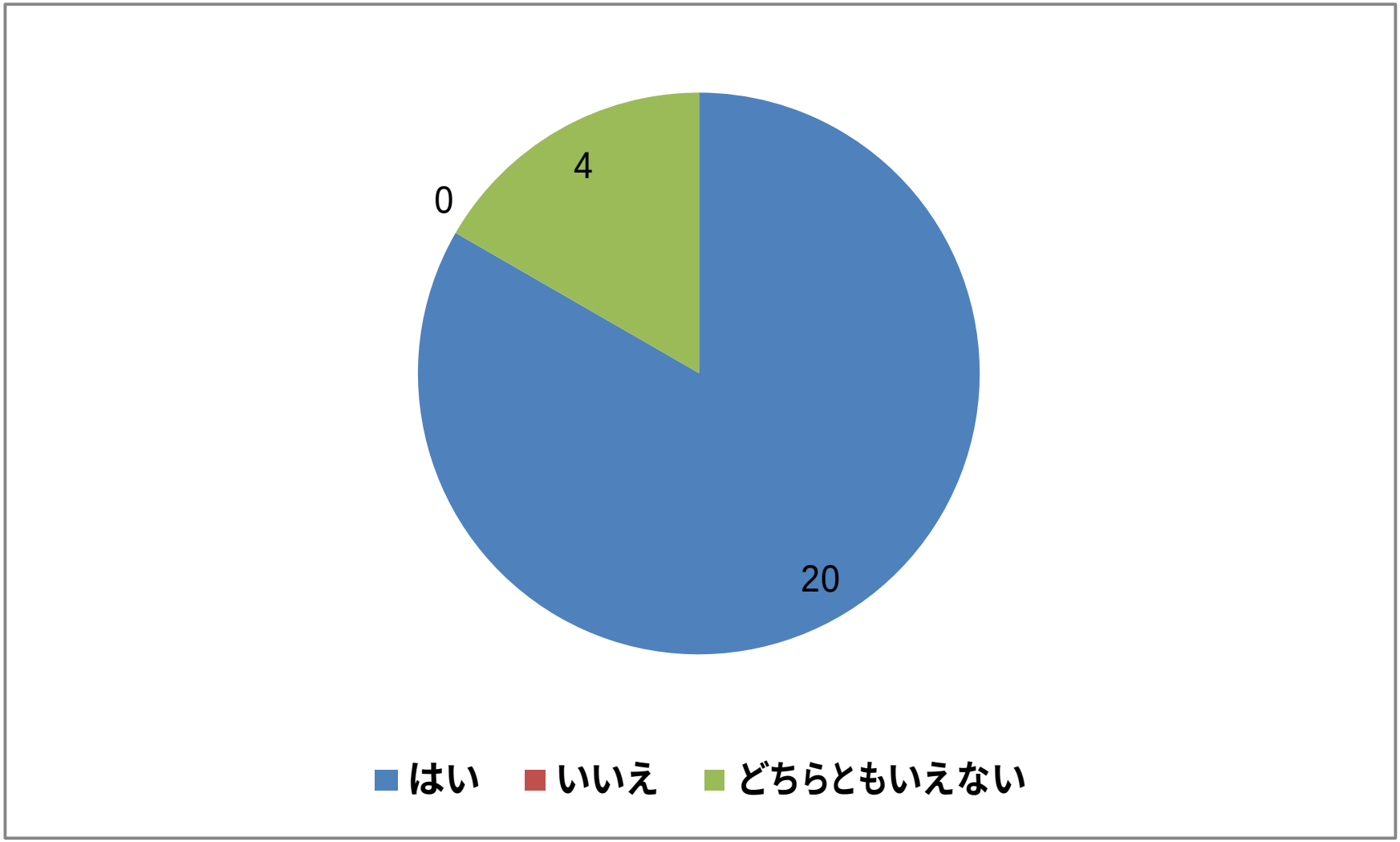
Q1　他の論文や発表から研究課題や目標が発見できた？



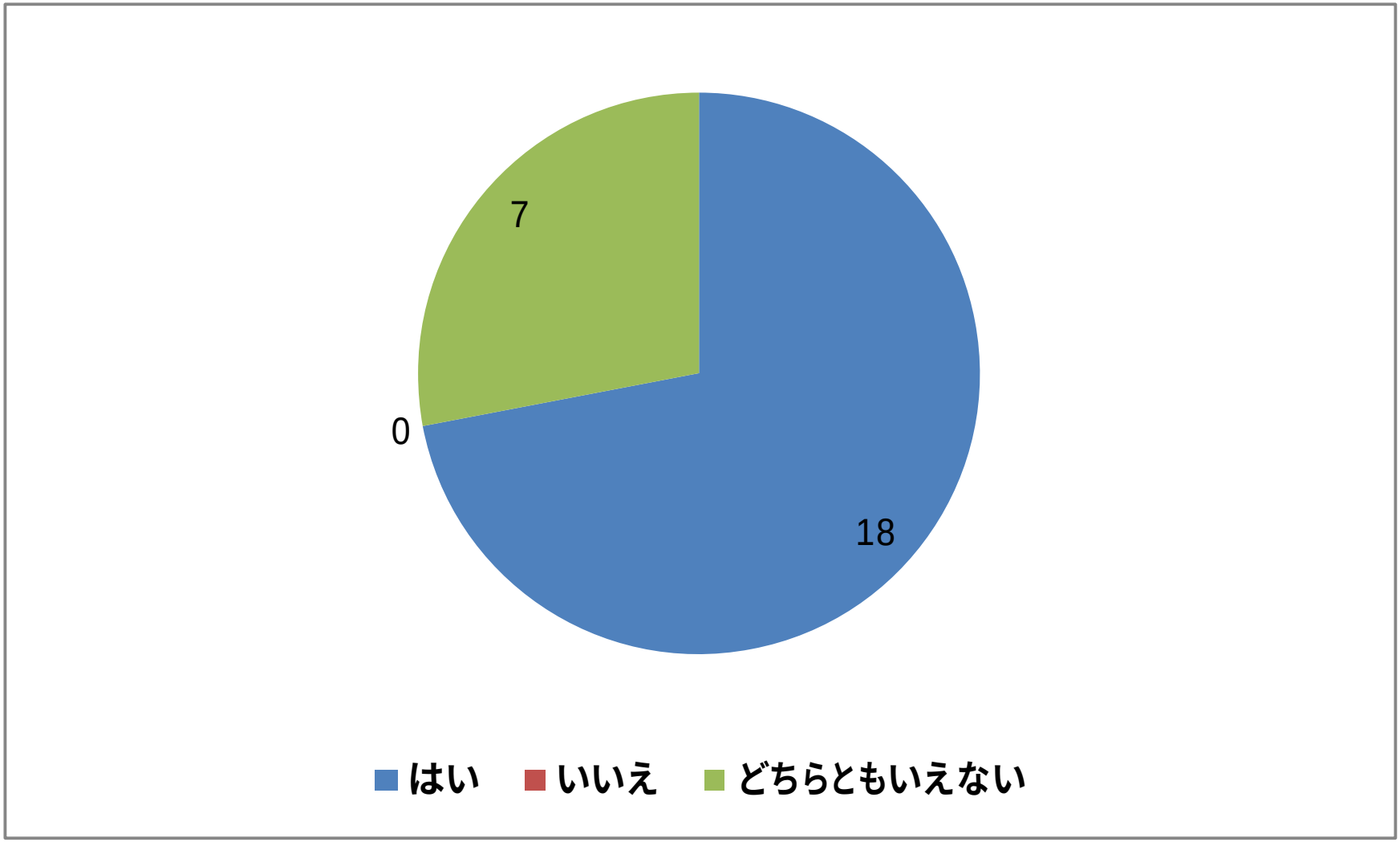
Q2　他の研究者との情報共有や意見交換ができたか？



Q3　マルウェア検体解説（1A2セッション内で実施）は有意義でしたか？



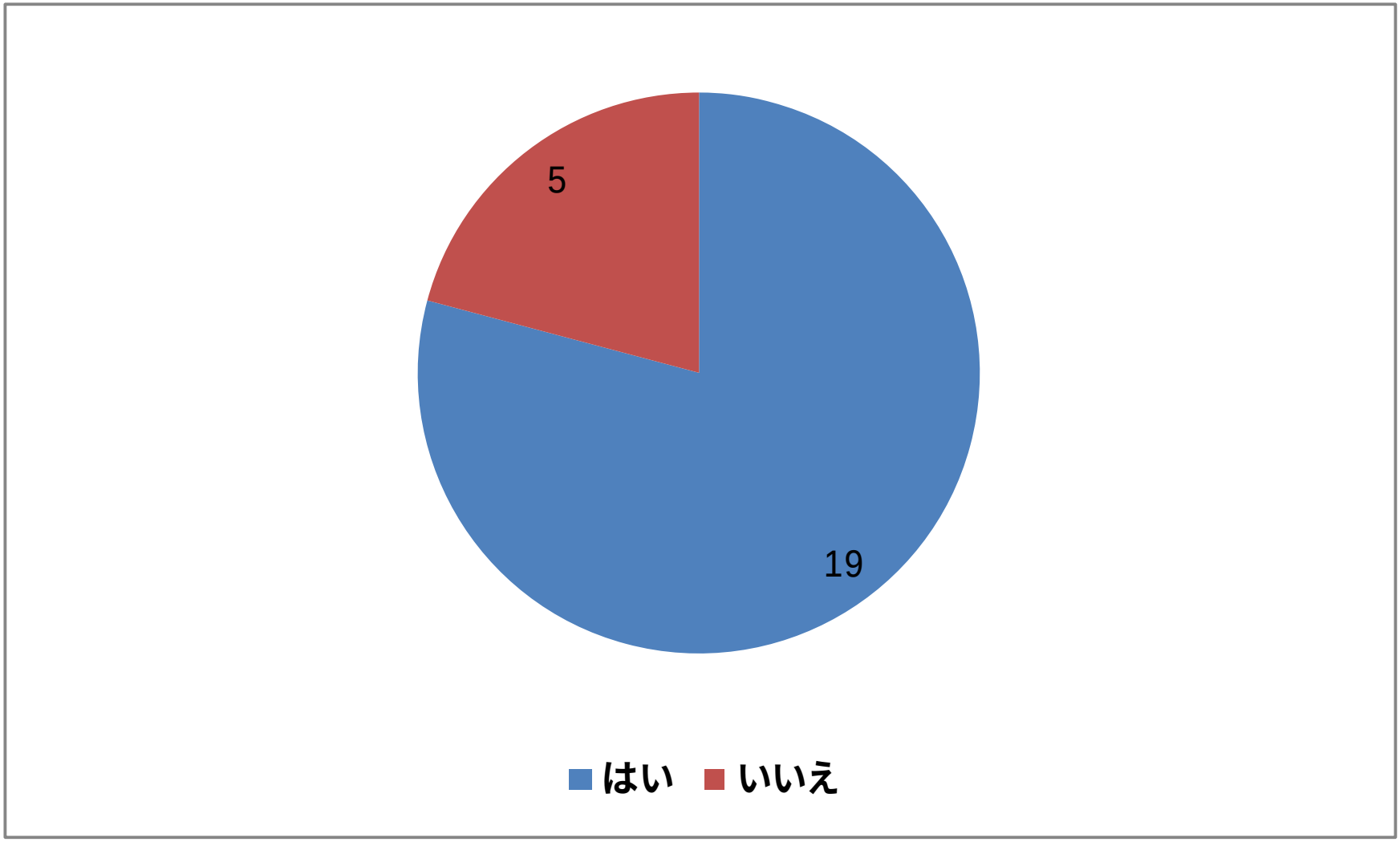
Q4　来年の MWS2011 でも発表しようと思いますか？



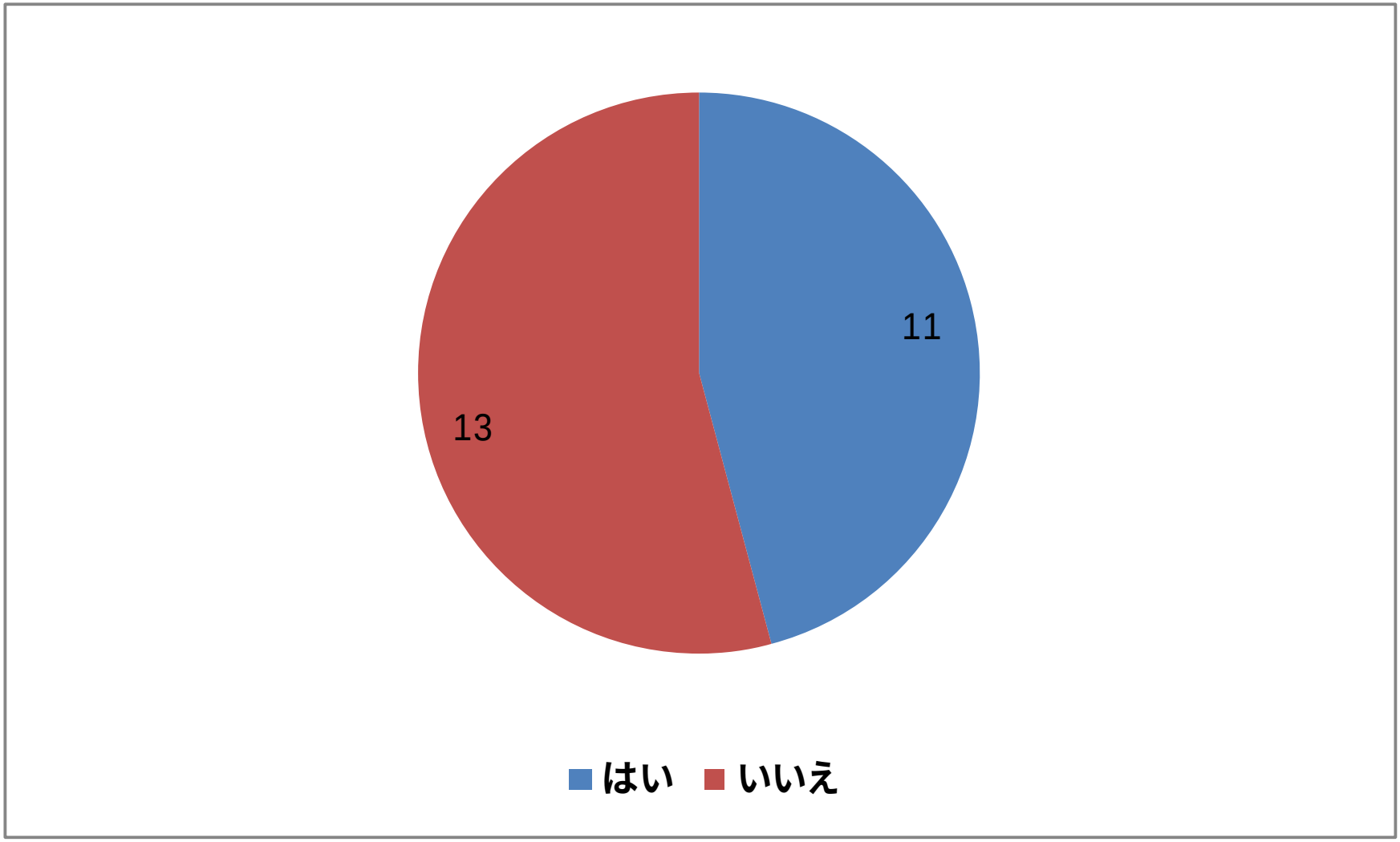
Q5　通常の研究発表以外にどんなセッションがあると良いですか？

- データセット未使用でも関連するテーマの研究発表
- セキュリティ関連企業による最先端技術やインシデント動向の紹介
- マルウェアの最新動向紹介（スマートフォンや組込み機器など）
- AVベンダによる検体解析作業や定義ファイル作成工程の紹介
- 実演マルウェア解析
- ハニーポットの構築・運用に関する苦労話
- 産学でのパネルディスカッション

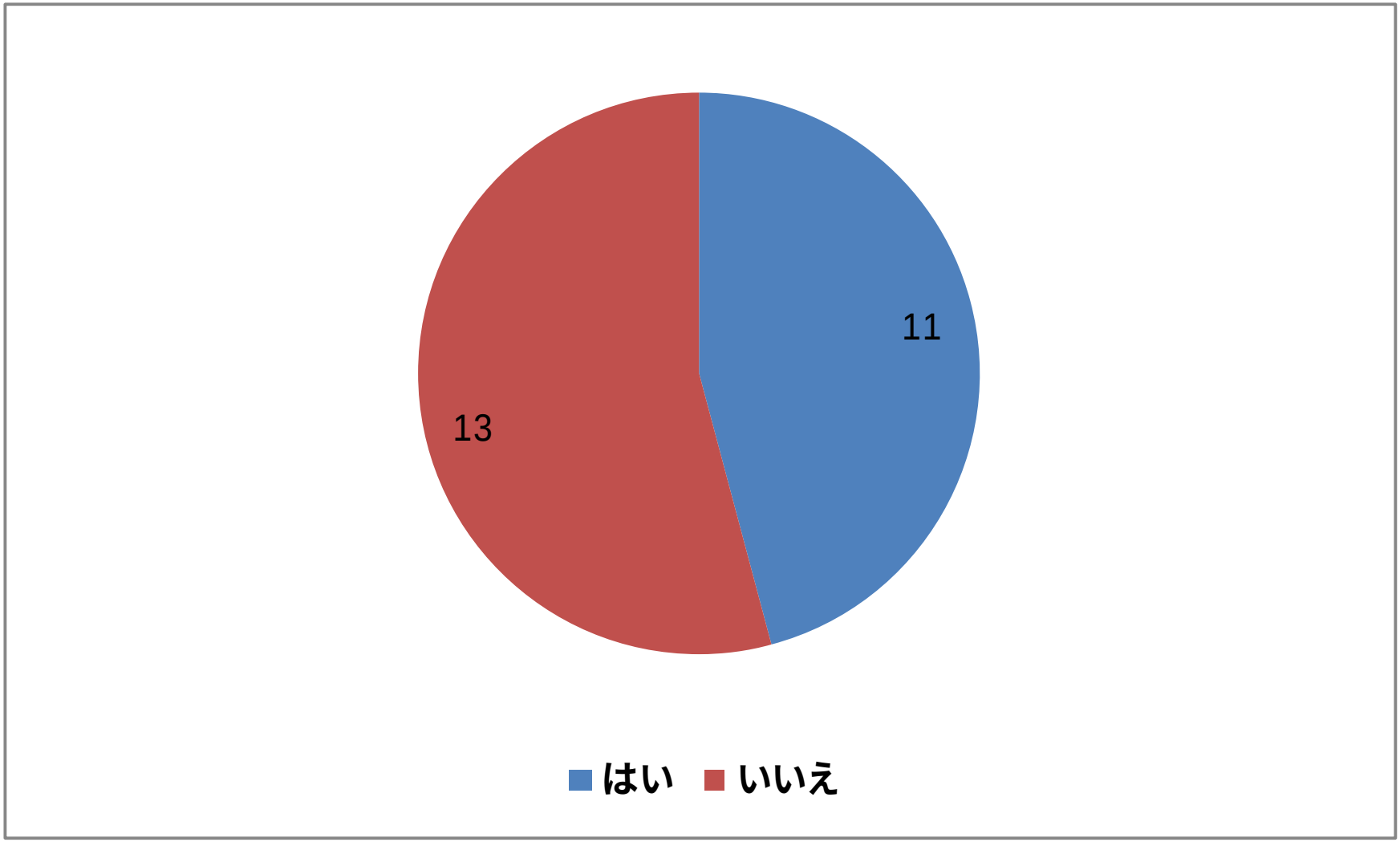
Q6　CCC DATAset 2010を発表に限らず使用しましたか？



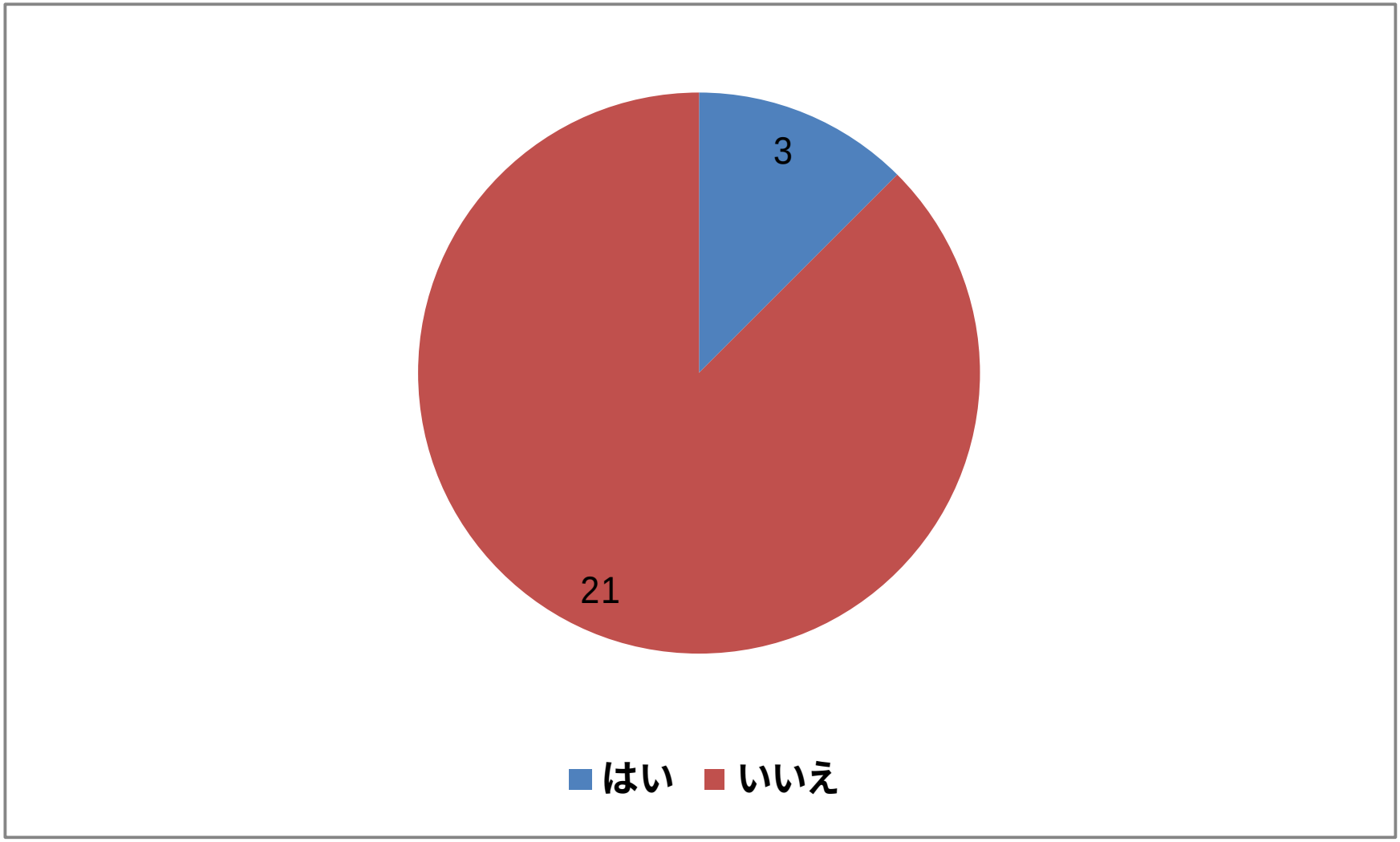
Q7　CCC DATAset 2009を発表に限らず使用しましたか？



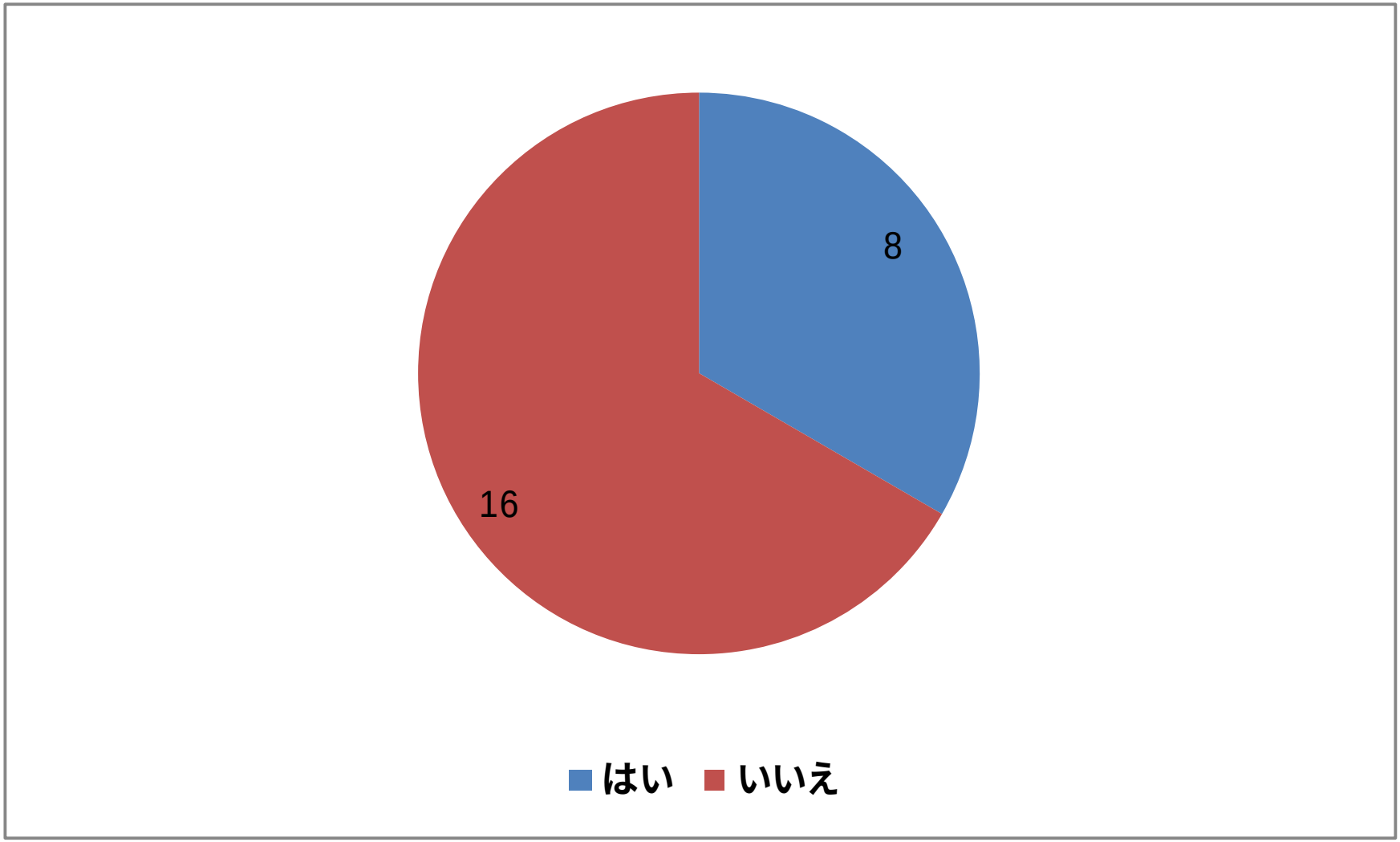
Q8　CCC DATAset 2008を発表に限らず使用しましたか？



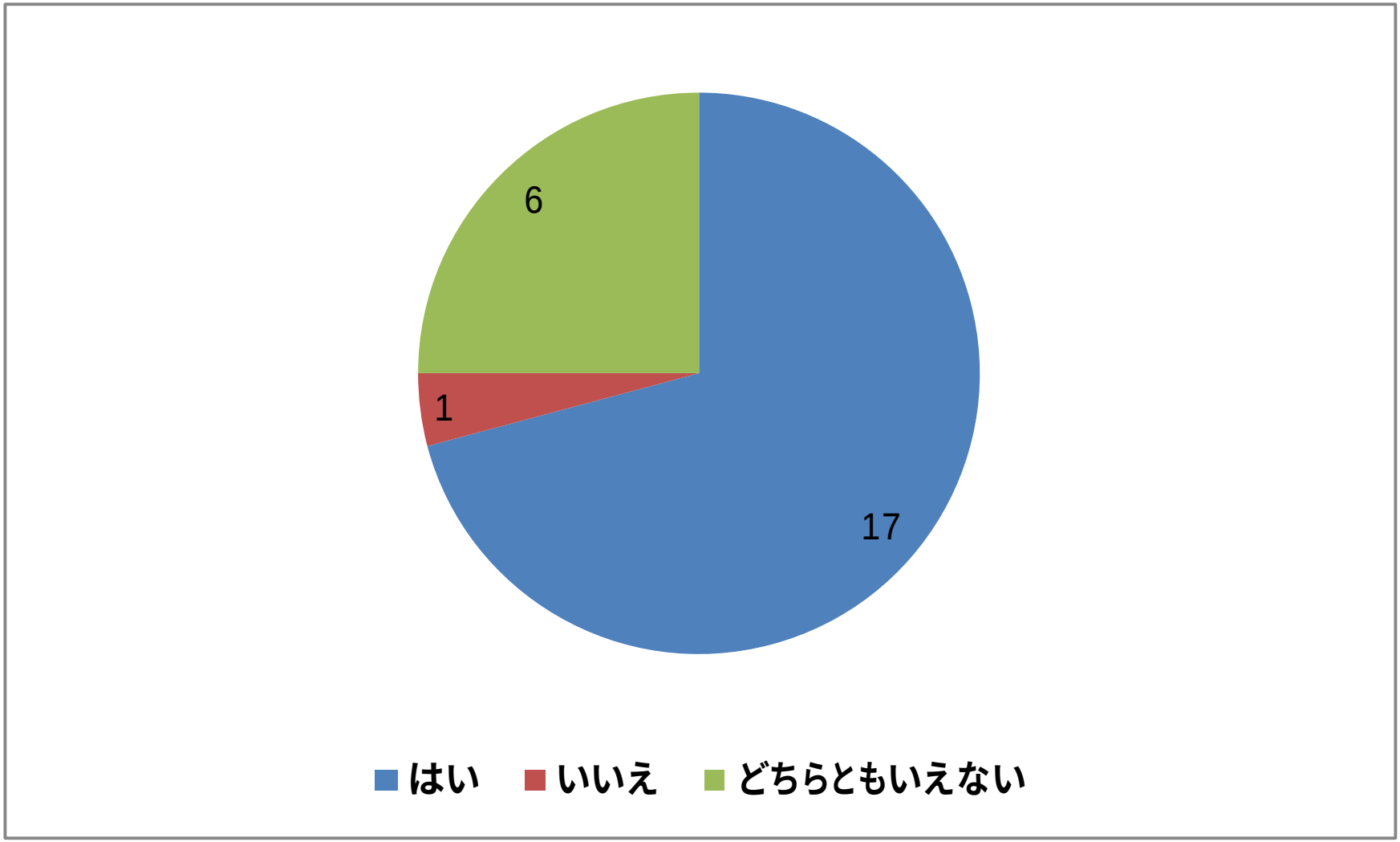
Q9　MARS for MWS2010を発表に限らず使用しましたか？



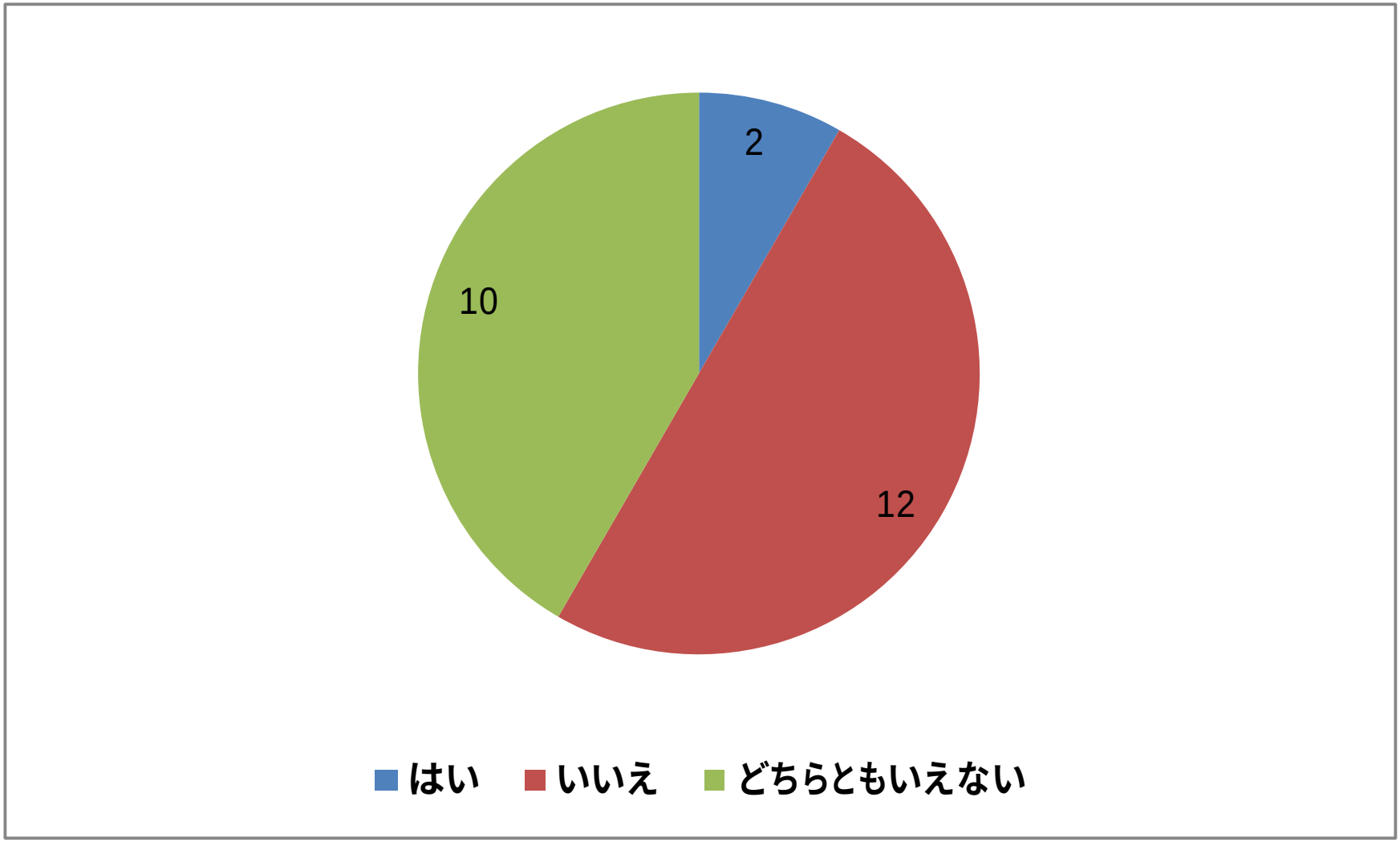
Q10　D3M 2010を発表に限らず使用しましたか？



Q11　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？



Q12 年度末までの契約期間内でMWS2010以外で発表予定はありますか？



Q13 どんなデータセットが提供されると良いですか？

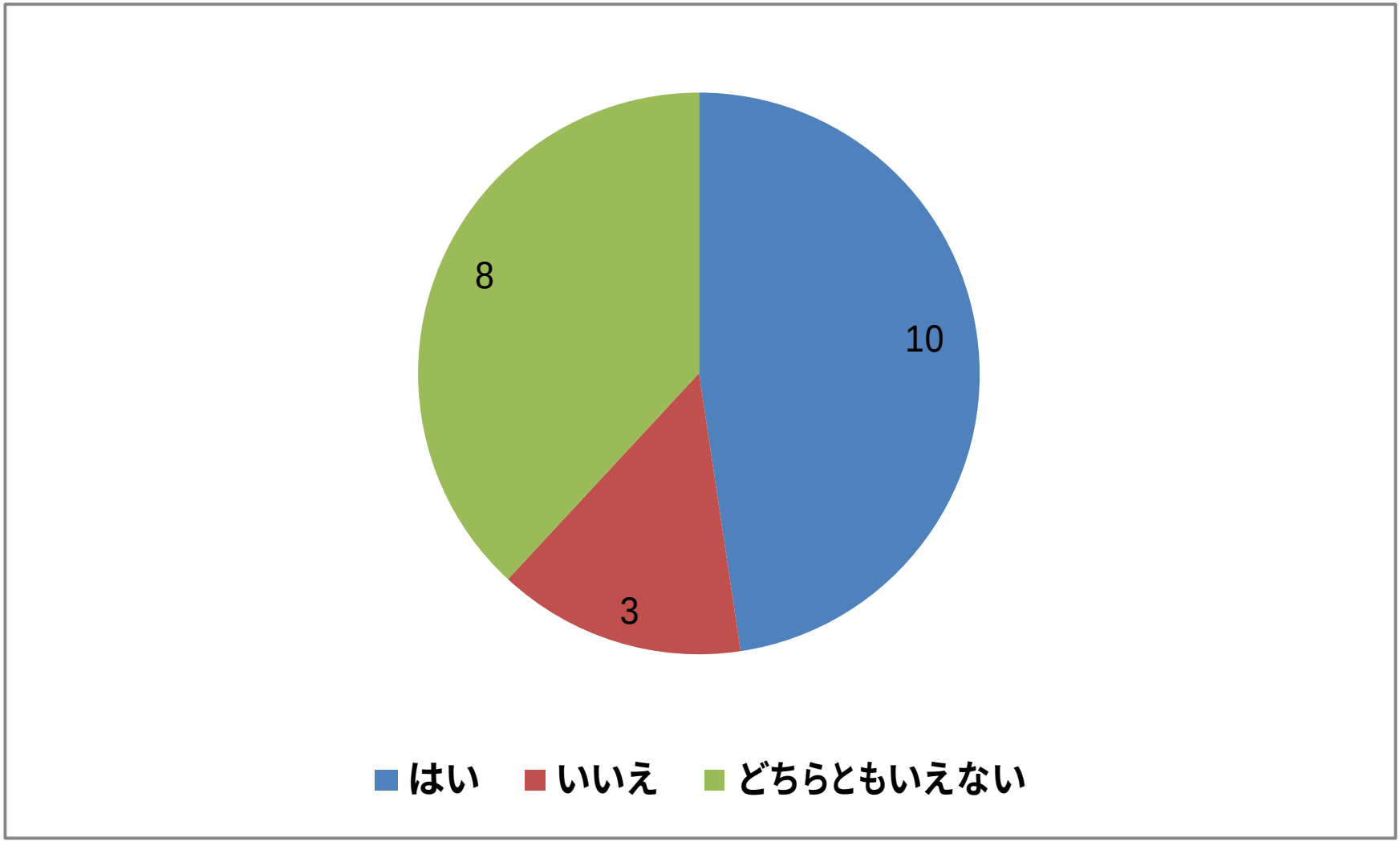
- 第三者にも検証可能（解答付）な形の公開可能なデータ
- 「攻撃通信データ」の一部として、何かが流行している時期の通信データと、流行の無い時期のものの両方
- マルウェアが実行されたマシンの実行環境を含むデータ
- C&Cサーバが動いているボットネットのマルウェア検体
- マルウェア感染ホストの長期間にわたる通信ログ(pcap)
- 大量のマルウェア検体
- ハニーポットの設置環境情報（IPアドレスやISP情報など）
- D3M の誘導後の検体（二次検体）
- スマートフォンや組込み機器のマルウェアとその挙動
- 正常時トラヒックデータ群

Q14 今後のMWSに、提供できる/できる可能性があるデータがあれば概要を教えてください

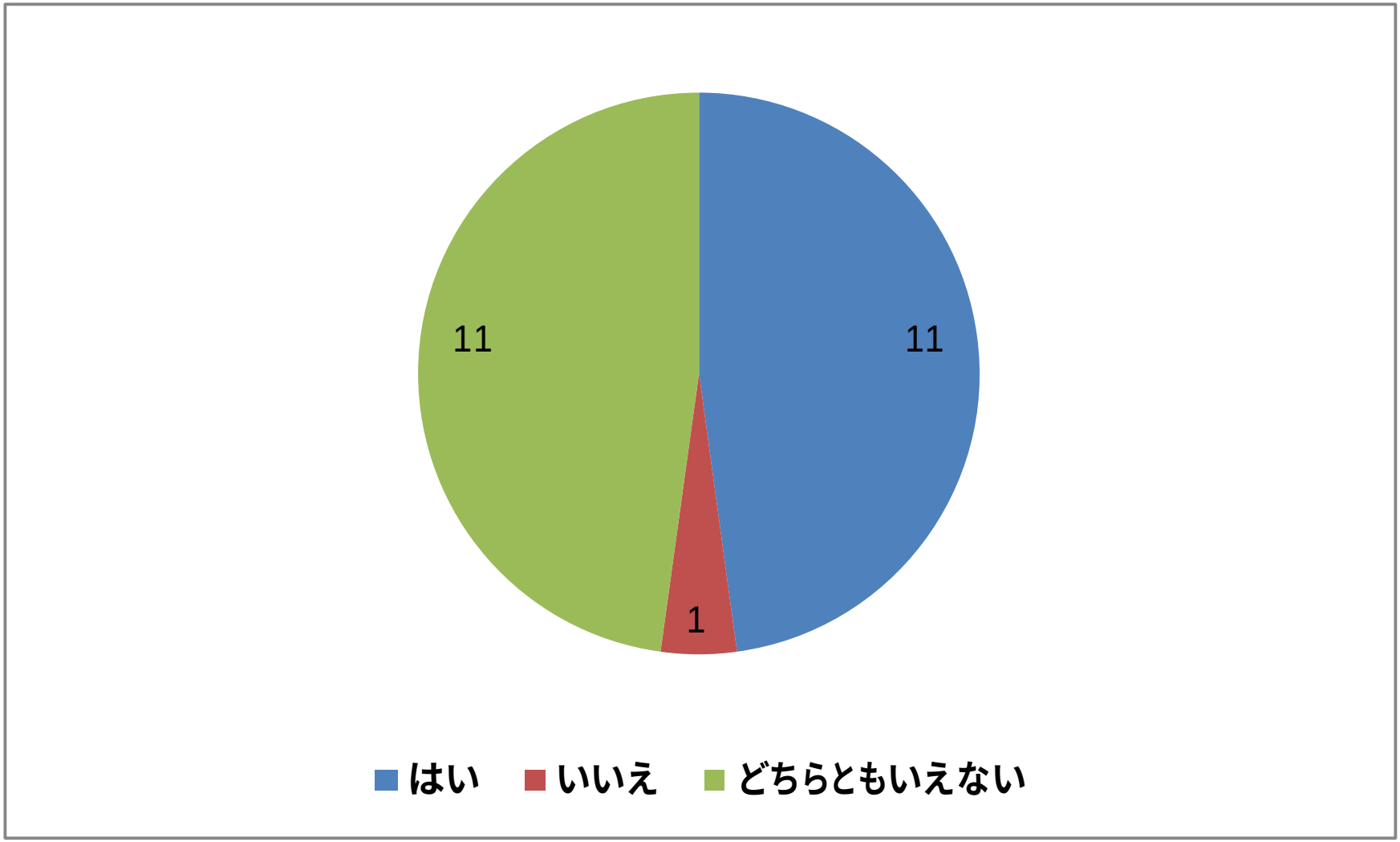
※MARSやD3Mは、CCC以外の研究者コミュニティ（組織やプロジェクト等を含む）から提供いただきました。

- http://honeywhales.com/で収集しているWeb感染型マルウェアに関するデータ
- ハニーポットで取得した検体、スパムトラップで収集した通信ログ
- マルウェア検体の制御フロー解析結果
- IIJ MITFハニーポットでの検体取得ログ(攻撃元データ)、pcapデータ(攻撃通信データ)など

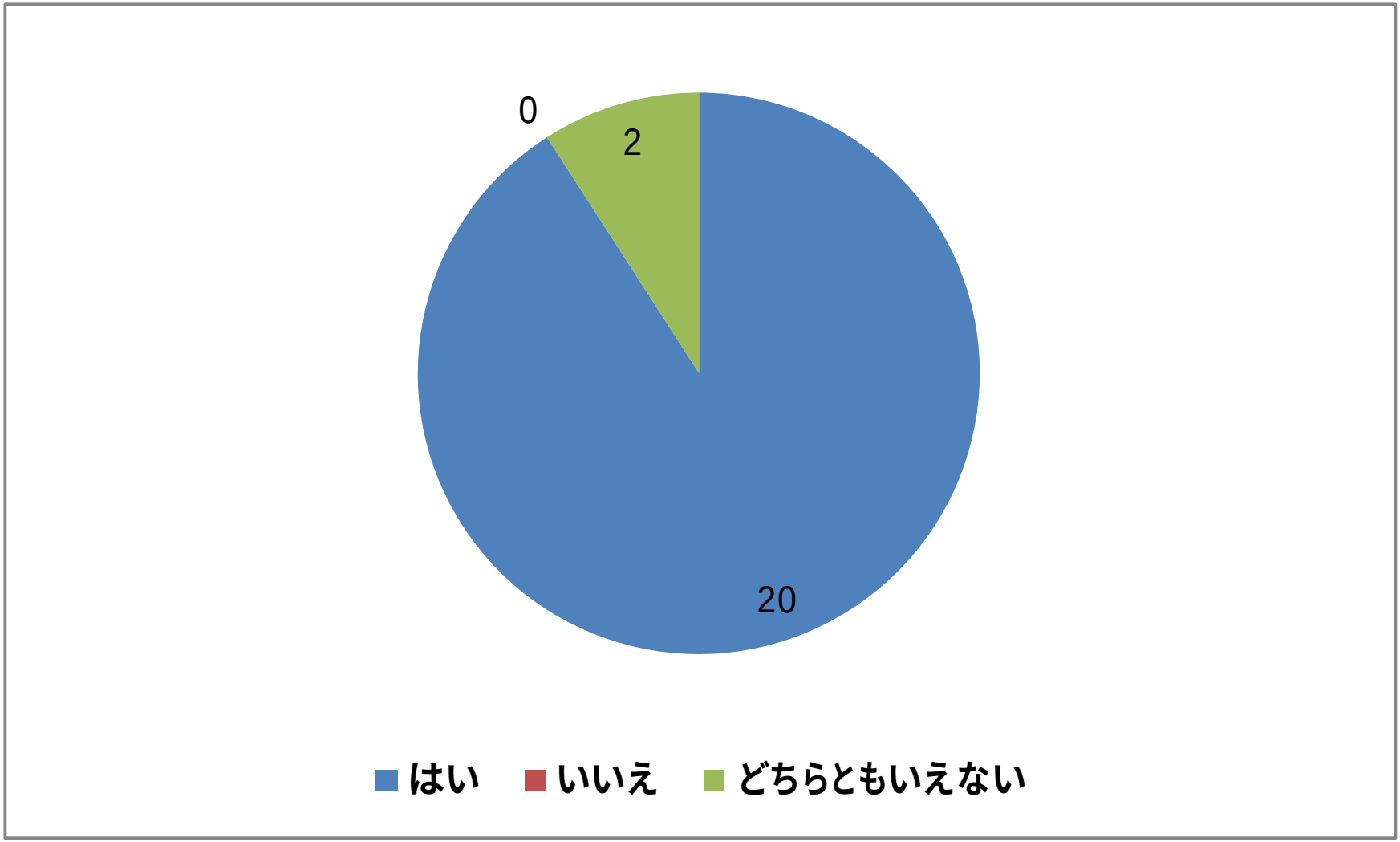
Q15 競技用データに関して最低減の事前情報は足りてましたか？



Q16 来年の MWS Cup 2011 の競技に参加しようと思いますか？



Q17 競技用データ解説（2A4セッション内で実施）は有意義でしたか？



Q18 どんな競技があると良いですか？

- pcap解析のみでは領域が限定的なので、海外のCTFのようにリバエンやWeb、トリビアなど分野を広げた競技
- 問題の難易度に応じて配点が決まる競技
- マルウェア検体（PE形式だけではなく、javascriptやpdf, swf, javaなど）を解析する競技
- Webで問題を出し、回答を入力し正解すると次の問題を表示といった、いつどこからでも参加できる形式の競技

Q19 MWS全般について率直な感想・意見、2011へ向けた提案をお待ちしております

- 今年から検体数が大幅に増え、さまざまなマルウェアに対する検討ができるようになった。MWS2011でも，同等数の検体を提供して頂けるとありがたい。
- マルウェアとの共生を図るうえで、恒常的に継続していくことが大切。
- マルウェアに起因するインシデント対応事例、マルウェアによる実害の事例など、難しい理論はないがケーススタディとして参考になる内容、論文にしずらい内容でも、気軽に発表、意見交換できる場にしたい。
- この手のデータセットは収集だけで苦労するため、対マルウェアの研究には非常に有益。

Q19 （Cont.）

- MWS2010初参加であったこともあって、とても有意義な時間を過ごせたと思います。また、学会自体も初めてだったので、学会の雰囲気というものを味わえ、とても良い経験になったと思います。
- 多くの発表があり、様々な情報が得られるため、後も継続して開催して欲しい。
- 3年実施したことで、多様な論文が出ました。今後もデータセットで論文を書く場合、ネタ切れ感が出てしまい、論文のレベルの低下が懸念されます。論文無しで、プレゼンのみで発表するセッションがあっても良い。

Q19 （Cont.）

- MWS2010が初めて参加した学会でしたが、大変有意義なものとなりました。今後も是非MWS/MWS Cupに参加させていただきたいと思います。
- MWS/MWS Cupはデータセットの配布、人材交流、人材育成のいずれの観点でも成功している大変有益なイベントだと思います。今後もより多くの後輩を引き連れて参加していきたい。
- 学生にとっては非常に思い出深いイベントだったようで、本当に良い体験をさせることができ大変感謝しております。