NIIオープンフォーラム2020@オンライン, 2020/6/9

2019年度学術機関向け 情報セキュリティガバナンス 実態調査報告

– 4年間の評価結果から見る学術機関のガバナンスの変化 –

渡邉英伸

広島大学 情報メディア教育研究センター

HIROSHIMA UNIVERSITY

発表概要

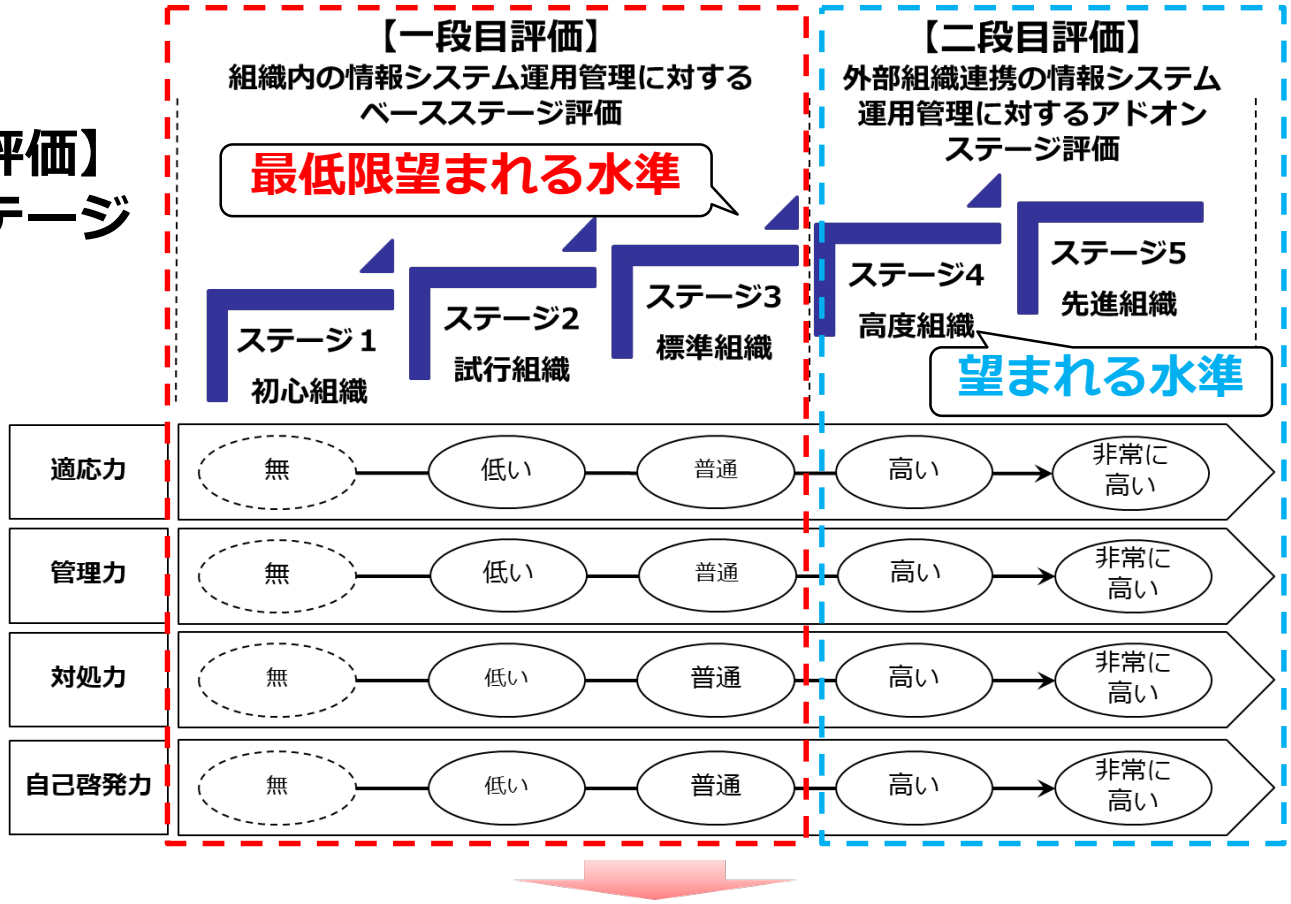
- **2016年度から2019年度の学術機関のクラウド活用度調査を実施した結果を報告**
  - 情報セキュリティガバナンス・クラウドサービス利用の実態調査アンケート
  - 事後アンケート

評価モデル

HIROSHIMA UNIVERSITY

4つの評価基準と5つのステージレベルで組織の情報セキュリティガバナンスを段階的かつ定量的に評価する（総合評価）

【一段目評価】
ベースステージ評価



【二段目評価】
総合ステージ評価

組織的情報セキュリティガバナンスの総合ステージ
（各評価基準のステージレベルの平均）※小数第二以下切捨

実態調査質問概要

HIROSHIMA UNIVERSITY

- **質問1**
  - 内容：Ⅰ．情報セキュリティに関する組織的な制度・体制、対策導入・運用、評価・点検、見直しの各実態を把握する内容
  - 出題形式：多者択一
  - 質問数：25問
  - 回答条件：必須
  - 有効回答率：100%（40／40機関）
    - 2018：100%（ 43／43機関）2017： 100%（31／31機関）、 2016：100%（28／28機関）

ガバナンスの現状の把握

- **質問2**
  - 内容：組織が運用している情報システム名、種別、オンプレミスおよびクラウドの運用・検討状況の各実態を把握する内容
  - 出題形式：記述形式＋多者択一（リスト化）
  - 回答条件：任意
  - 有効回答率：62%（25／40機関）
    - 2018：58%（ 25／43機関）2017： 58%（18／31機関）、 2016：82%（23／28機関）

情報資産の管理状況の把握

- **質問3**
  - 内容：過去1年間に発生したクラウドサービス利用に起因する場合と起因しない場合における情報セキュリティインシデントと情報セキュリティトラブルの発生件数・対処時間の各実態を把握する内容
  - 出題形式：記述形式
  - 回答条件：任意
  - 有効回答率：67%（31／40機関）
    - 2018：58%（ 25／43機関）2017： 45%（14／31機関）、2016：60%（17／28機関）

CSIRTの対応状況の把握

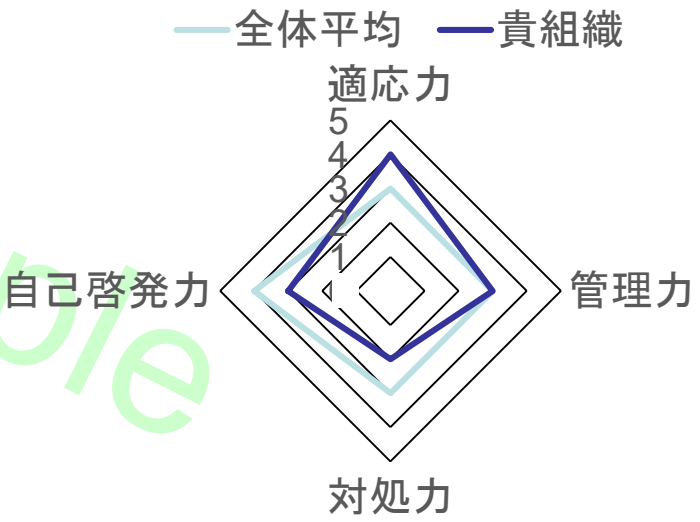
個別報告書のイメージ

HIROSHIMA UNIVERSITY

「クラウドサービス利用に向けた学術機関のための情報セキュリティガバナンス実態調査」報告書

○○大学の評価結果：ステージ3.0（昨年度：ステージ2.5）
適応力：4.0、管理力：3.0、対処力：2.0、自己啓発力：3.0
（昨年度：適応力：3.0、管理力：2.0、対処力：2.0、自己啓発力：3.0）

概説
・ステージ判定結果、平均ステージとの差分や望まれる水準との差分の状況を記載



能力毎の評点と望まれる水準との差分
・適応力4.0：
・管理力3.0：
・対処力2.0：
・自己啓発力3.0：

昨年度からの改善傾向
・評点が向上した設問を列挙し、どの能力が改善傾向にあるかを記載

今後のポイント
・水準を満たしていない設問を列挙

2016年度～2019年度
実態調査結果

HIROSHIMA UNIVERSITY

実態調査概要

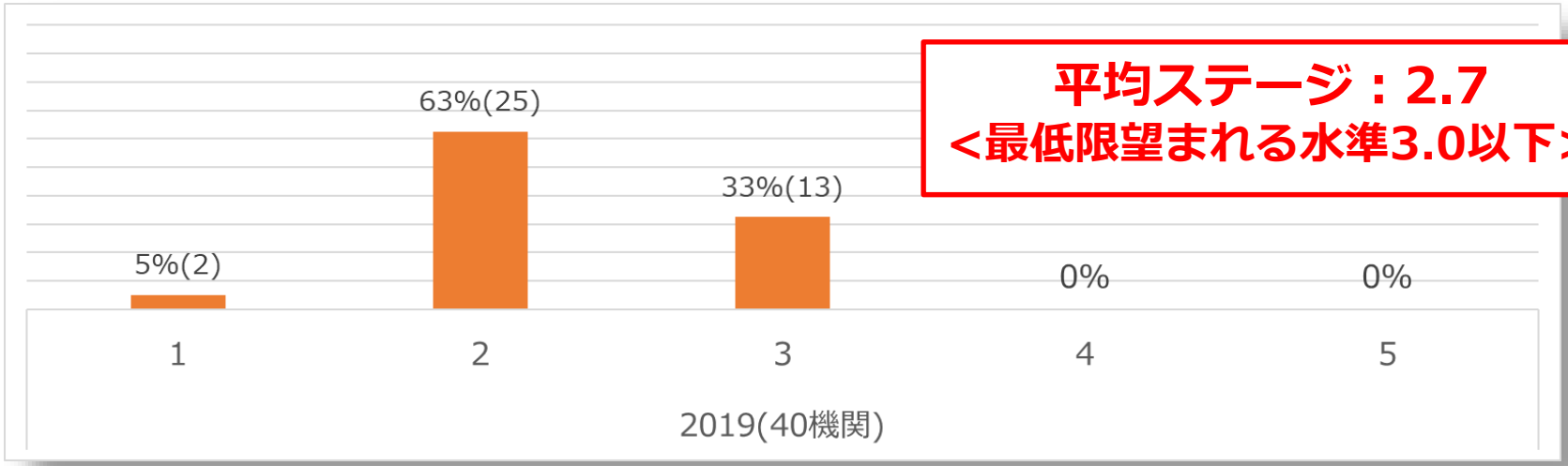
HIROSHIMA UNIVERSITY

- **2019年度調査**
  - 実施時期：2019年12月2日（月）～12月27日（金）
  - 調査方法：Web・エクセルファイルによるアンケート調査
  - 有効回答数：40機関
- **2018年度調査**
  - 実施時期：2019年1月7日（月）～2月8日（金）
  - 調査方法：Web・エクセルファイルによるアンケート調査
  - 有効回答数：43機関
    - 同一機関の複数の部署は別々の機関として扱っている
- **2017年度調査**
  - 実施時期：2018年1月5日（金）～2月2日（金）
  - 調査方法：方法：Web・エクセルファイルによるアンケート調査
  - 有効回答数：31機関
- **2016年度調査**
  - 実施時期：2017年1月18日（水）～2月24日（金）
  - 調査方法：エクセルファイルによるアンケート調査
  - 有効回答数：28機関

今回は年末に実施

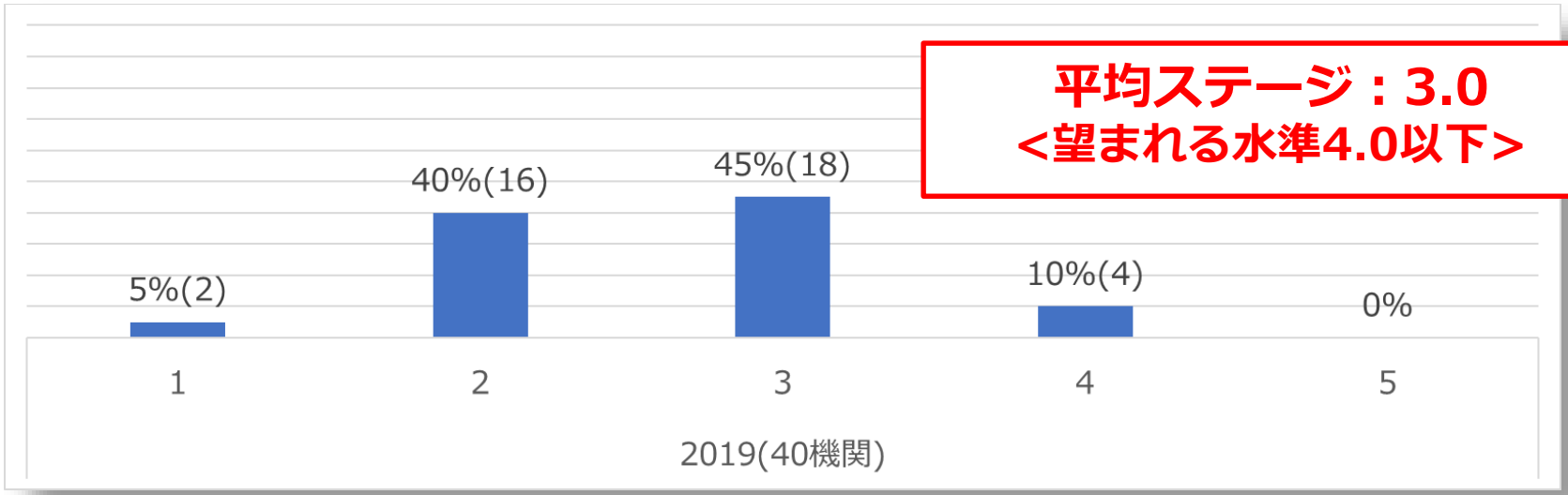
2019年度ベース／総合ステージ分布図

2019年度40機関のベースステージ分布



平均ステージ：2.7
<最低限望まれる水準3.0以下>

2019年度40機関の総合ステージ分布

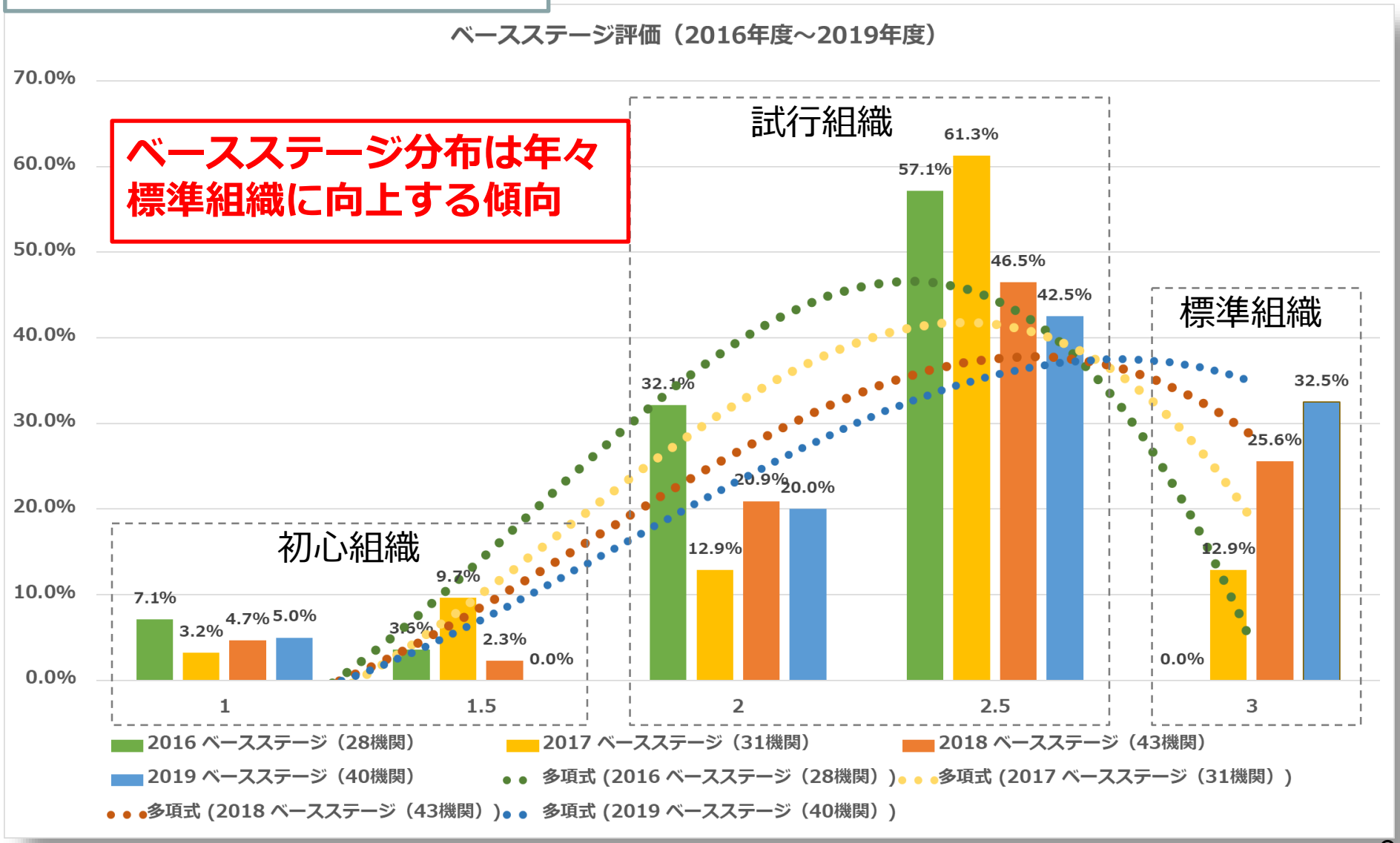


平均ステージ：3.0
<望まれる水準4.0以下>

年度別ベースステージ分布図

平均ステージ2.4→2.5→2.6 →2.7
<最低限望まれる水準3.0以下>

点線は近似曲線（多項式3次）

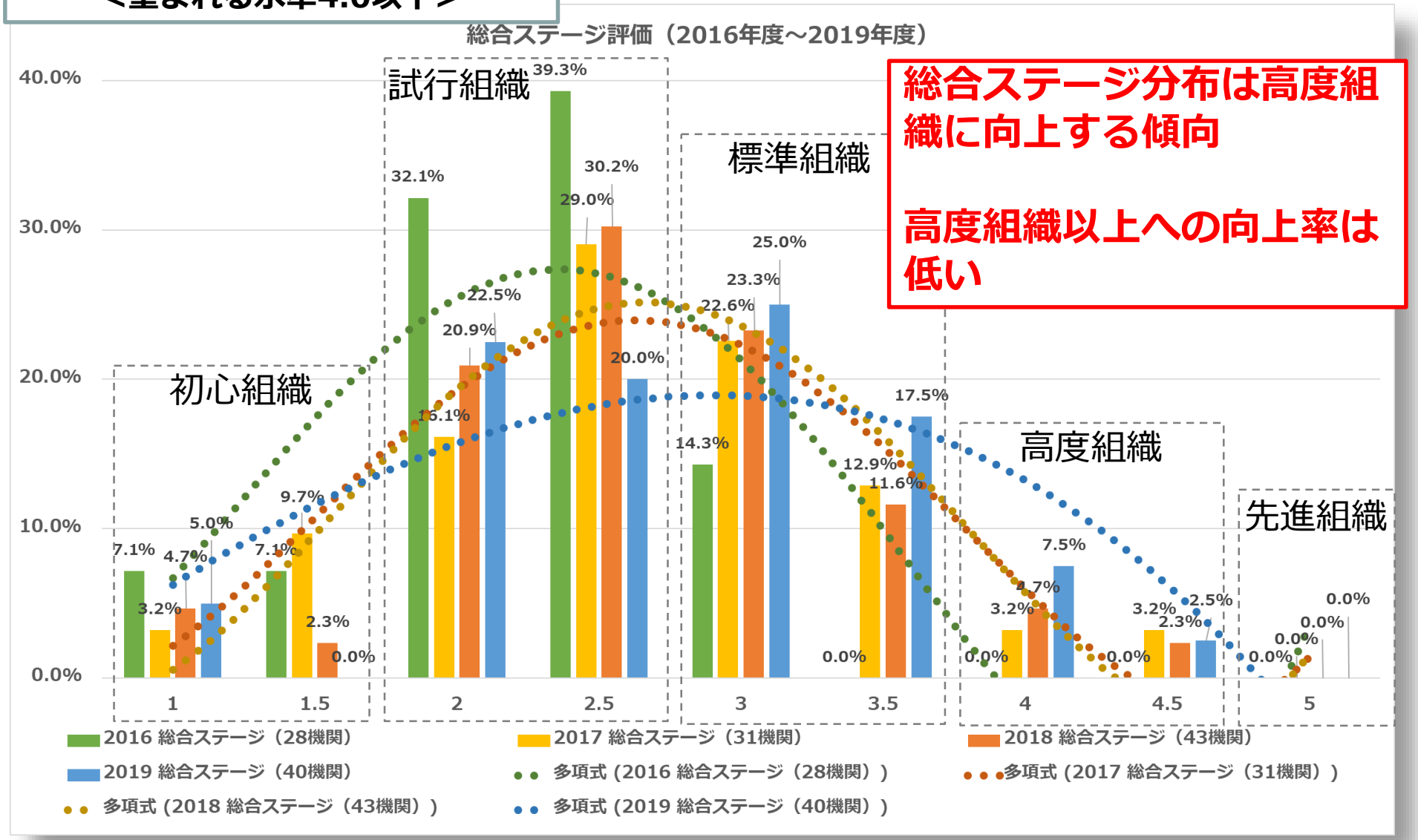


年度別総合ステージ分布図

HIROSHIMA UNIVERSITY

平均ステージ2.5→2.9→2.9 →3.0
<望まれる水準4.0以下>

点線は近似曲線（多項式3次）

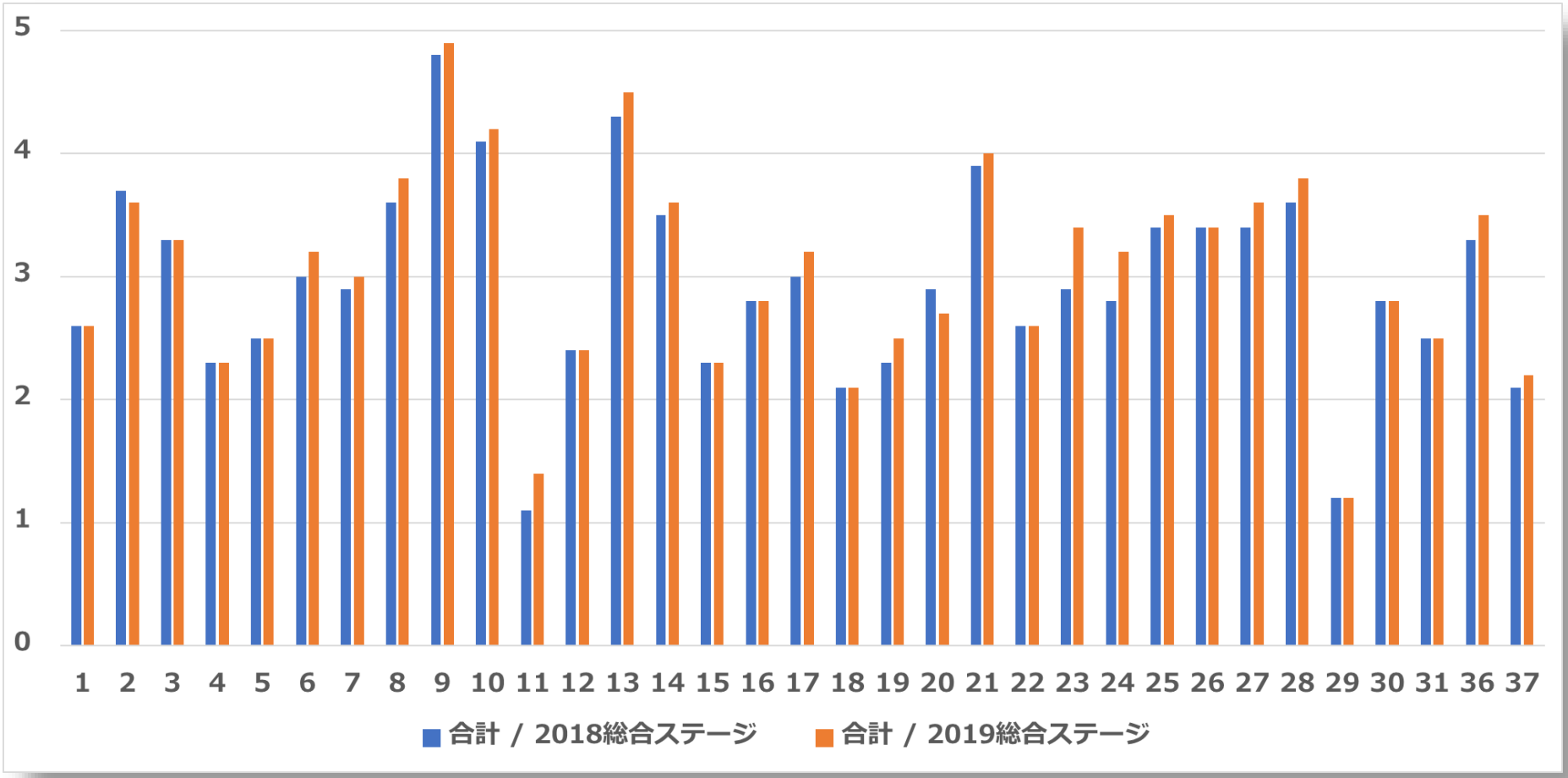


総合ステージ分布は高度組織に向上する傾向

高度組織以上への向上率は低い

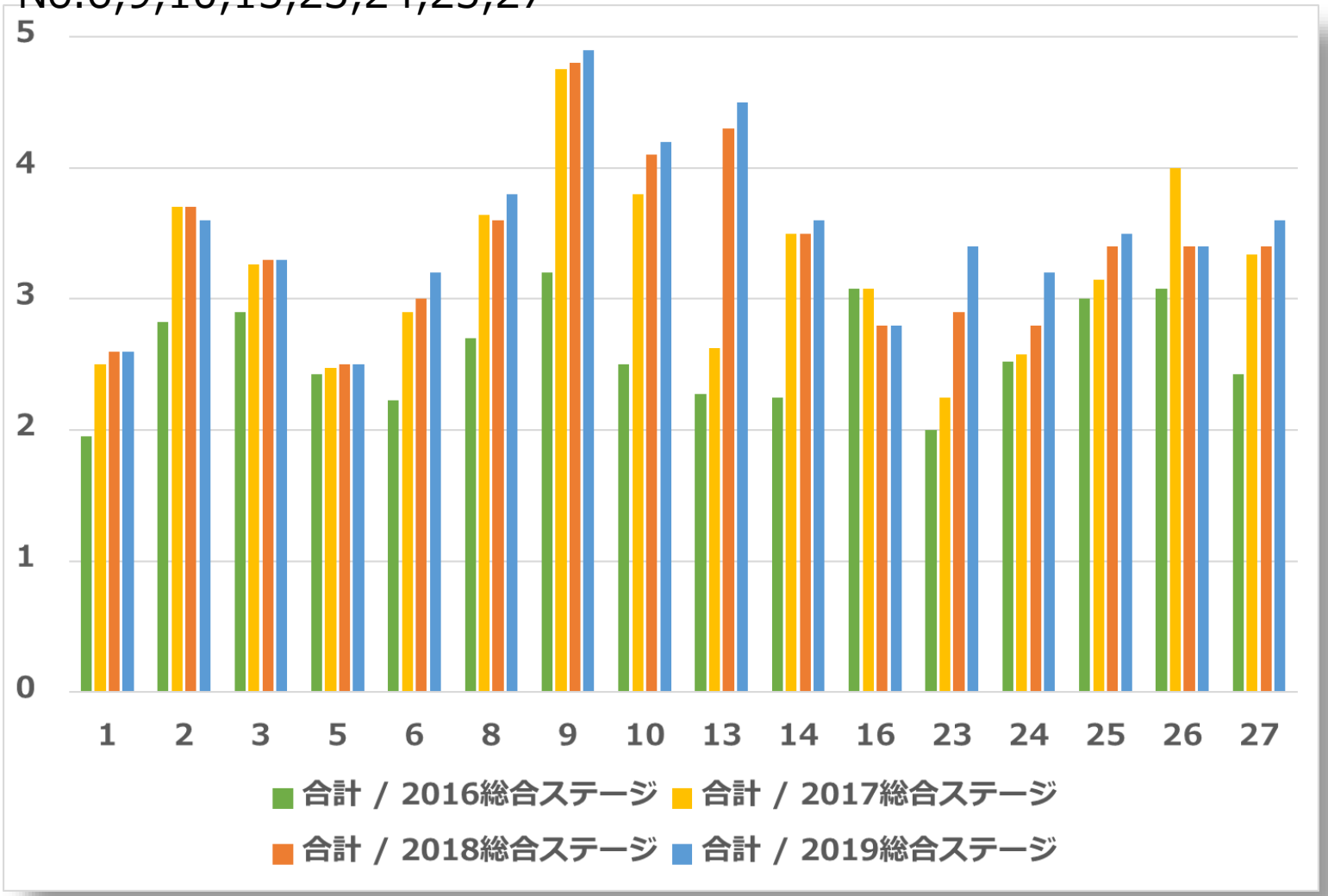
2年継続参加33機関年度別総合ステージ分布図

- **2019年度の総合ステージは、2018年度に比べて54%(18/33機関)が向上**
  - No.6,7,8,9,10,11,13,14,17,19,21,23,24,25,27,28,36,37



4年継続参加16機関年度別総合ステージ分布図

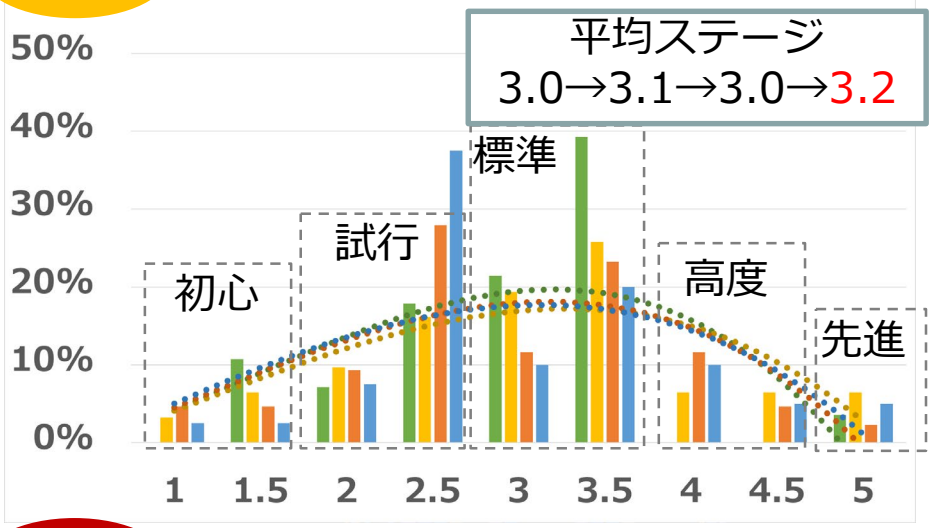
- 4年連続向上している機関は50%(8/16機関)が向上
  - No.6,9,10,13,23,24,25,27



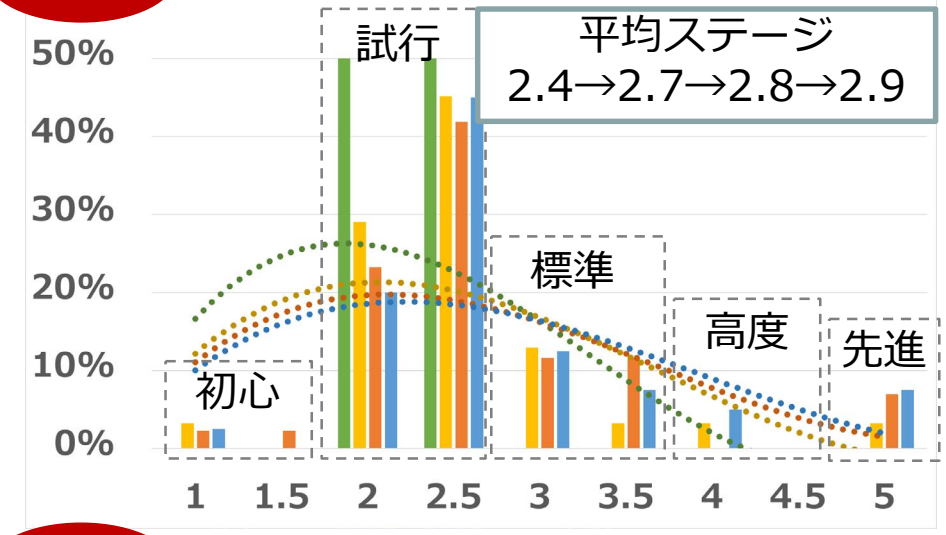
年度・評価基準別総合ステージ分布図

HIROSHIMA UNIVERSITY

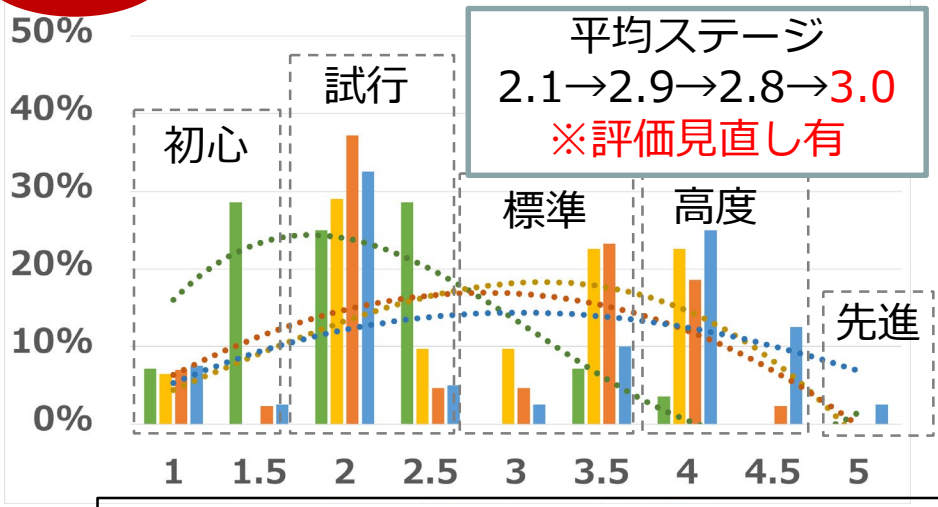
導入 適応力総合ステージ分布



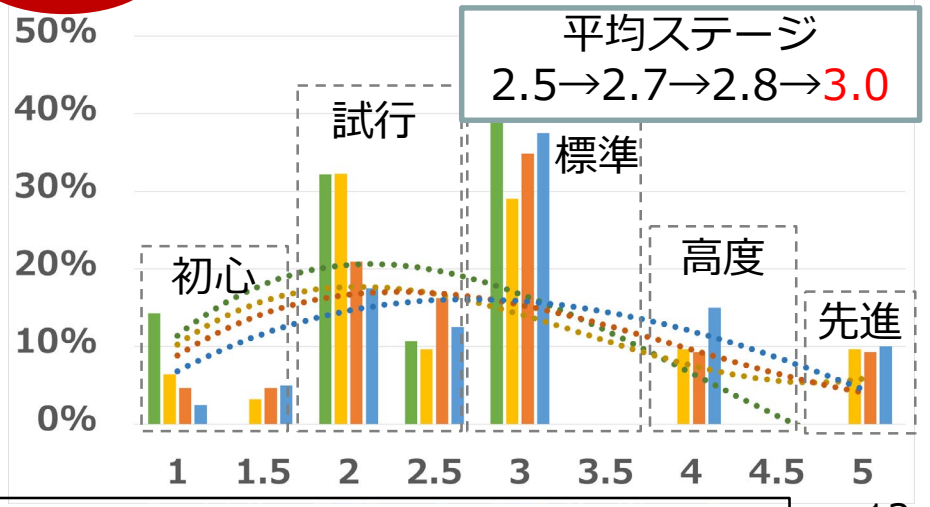
運用 管理力総合ステージ分布



運用 対処力総合ステージ分布



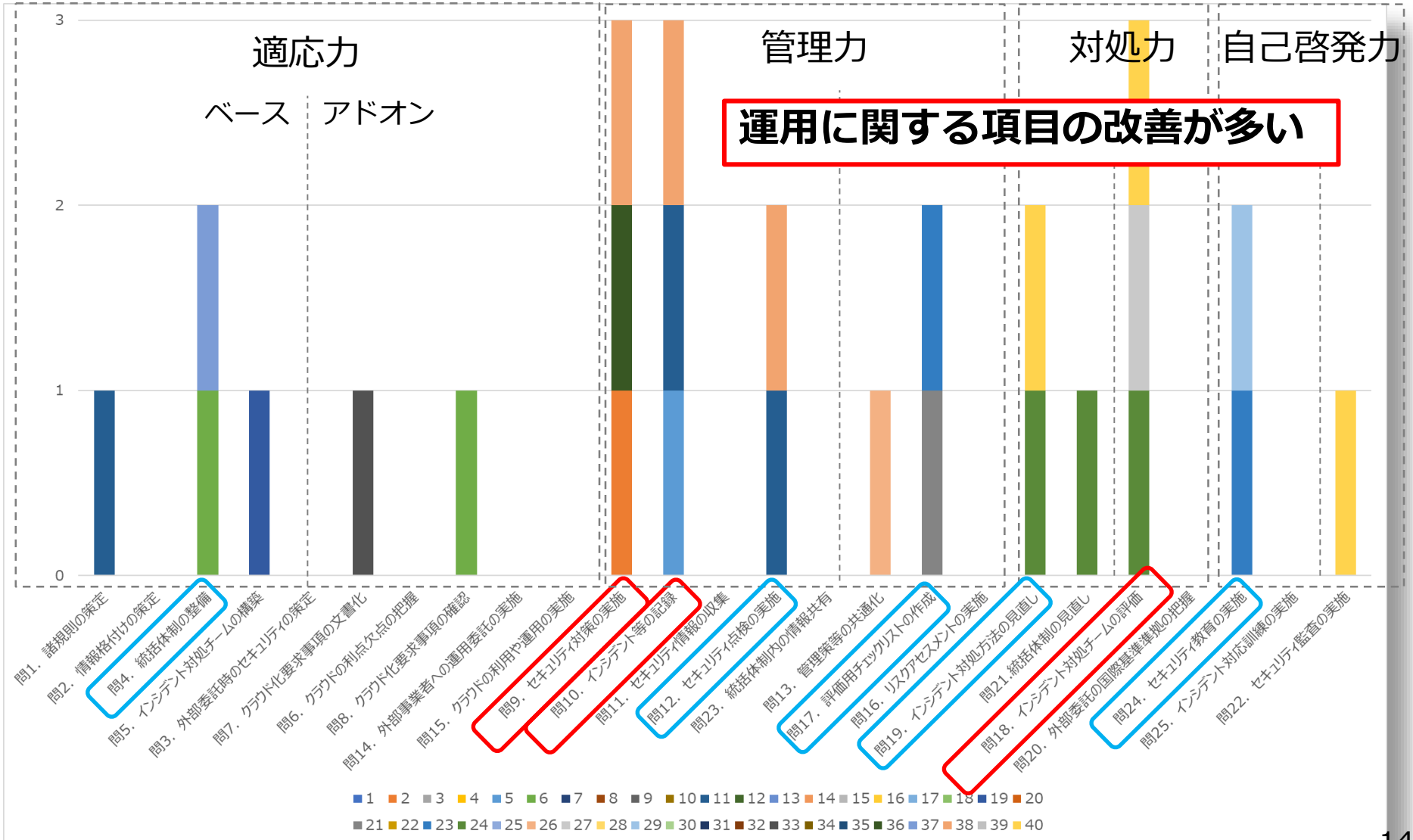
運用 自己啓発力総合ステージ分布



2016年度 2017年度 2018年度 2019年度 多項式(2016年度) 多項式(2017年度) 多項式(2018年度) 多項式(2019年度)

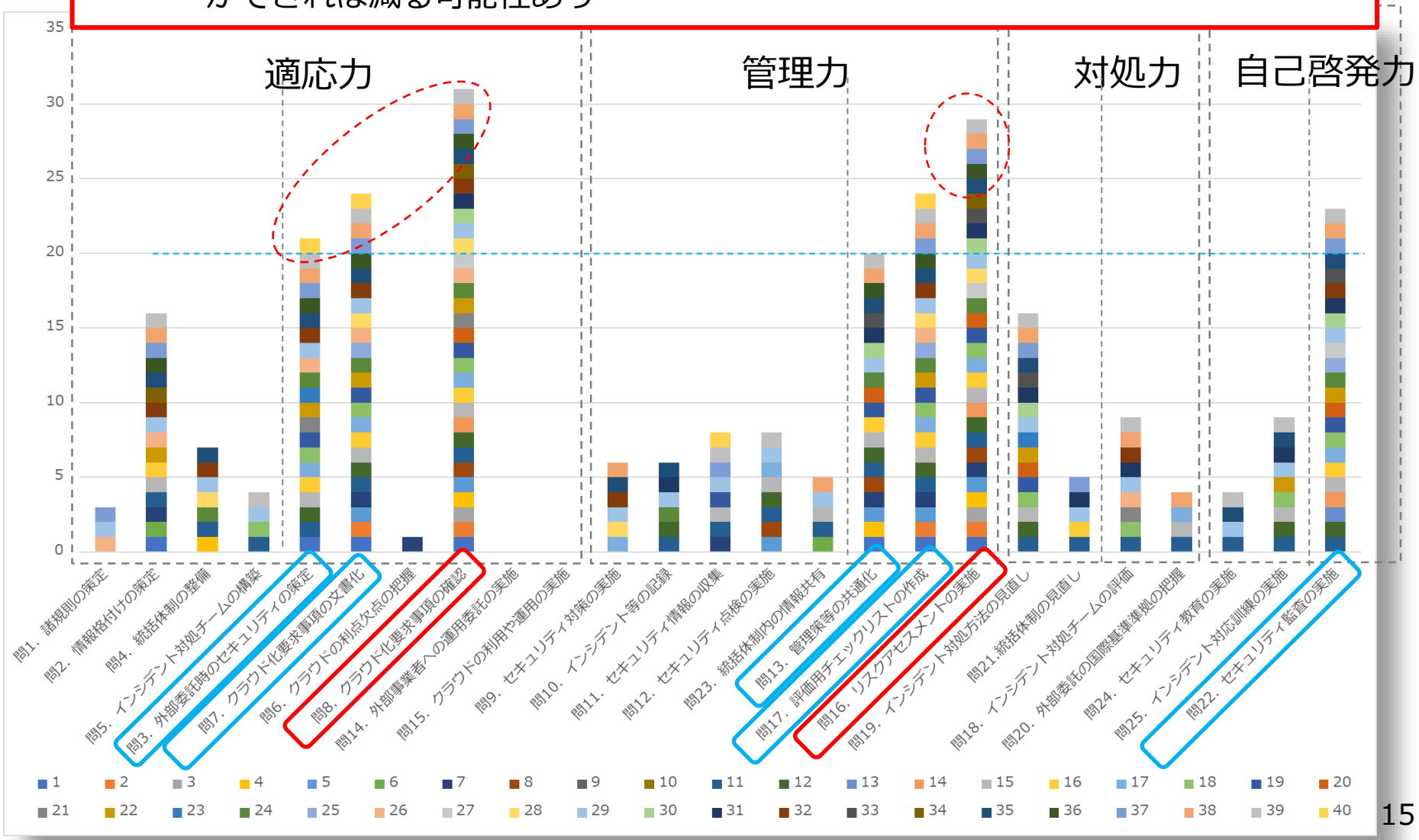
質問別改善数分布図(2018年度から継続参加の37機関)

改善傾向があった質問は、セキュリティ対策の実施(問9)、インシデント等の記録(問10)、インシデント対処チームの評価(問18)



質問別指摘数分布図(2019年度40機関)

- **クラウドに関連する質問の指摘が多い傾向**
- **水準を満たすための指摘が多い質問は、クラウド化要求事項の確認(問8)**
  - リスクアセスメント実施、外部委託時のセキュリティ策定、要求事項の文書化ができれば減る可能性あり



2019年度事後アンケート結果

HIROSHIMA UNIVERSITY

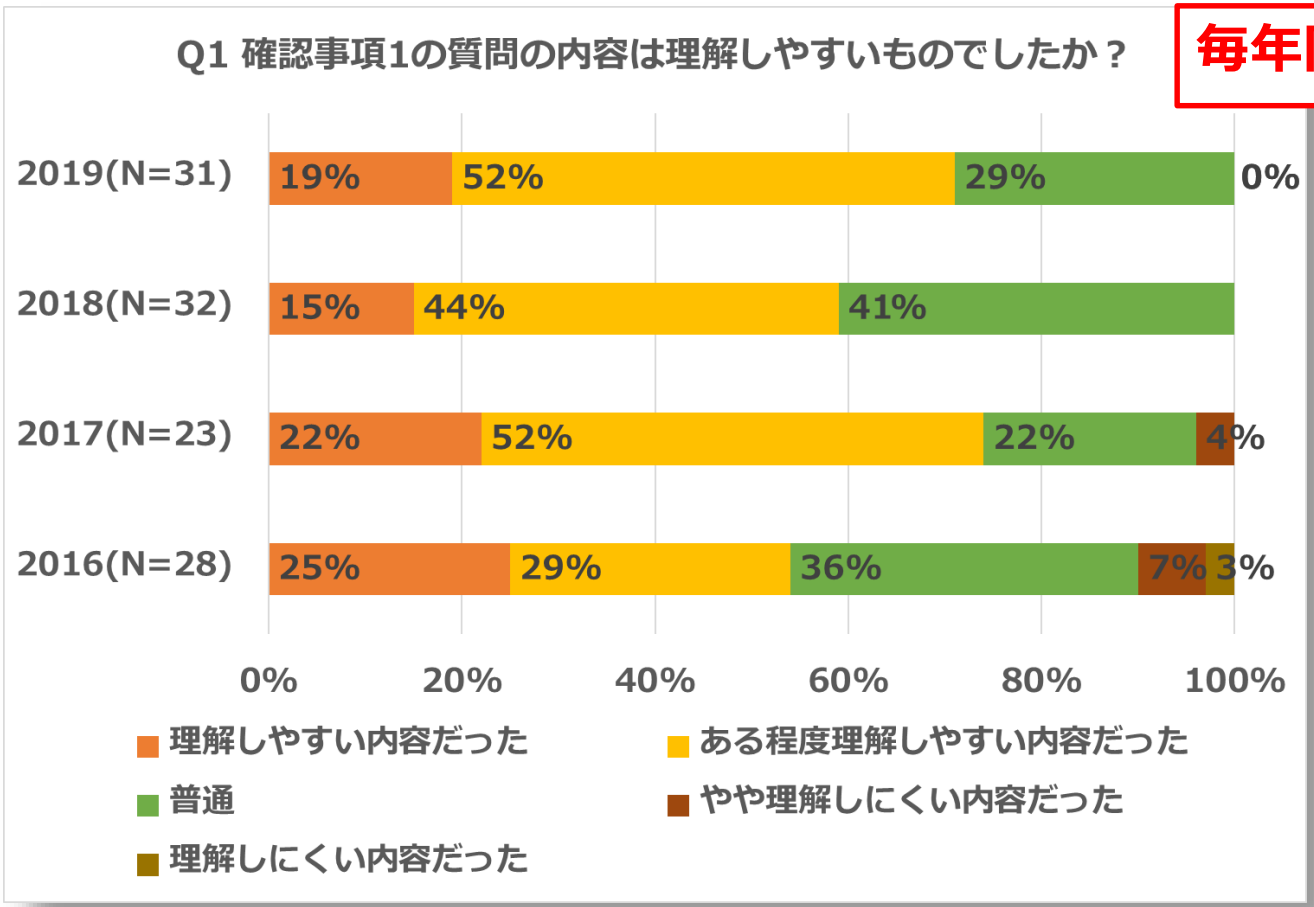
事後アンケート概要

- **内容：**
  - 質問1-3、個別報告書、取り組みに対する評価・意見を把握する内容
- **出題形式：**
  - 四者択一＋自由記述（理由、意見など）
- **質問数：**
  - 8問
- **回答条件：**
  - 任意
- **有効回答率：**
  - 77%（31／40機関）
    - 2018：74%(32／43機関)、2017：74%(23／31機関)、2016：100%(28／28機関)

質問1、報告書、取り組みに対する評価の内容に限定し紹介

質問1の問いの内容は理解しやすいものでしたか？

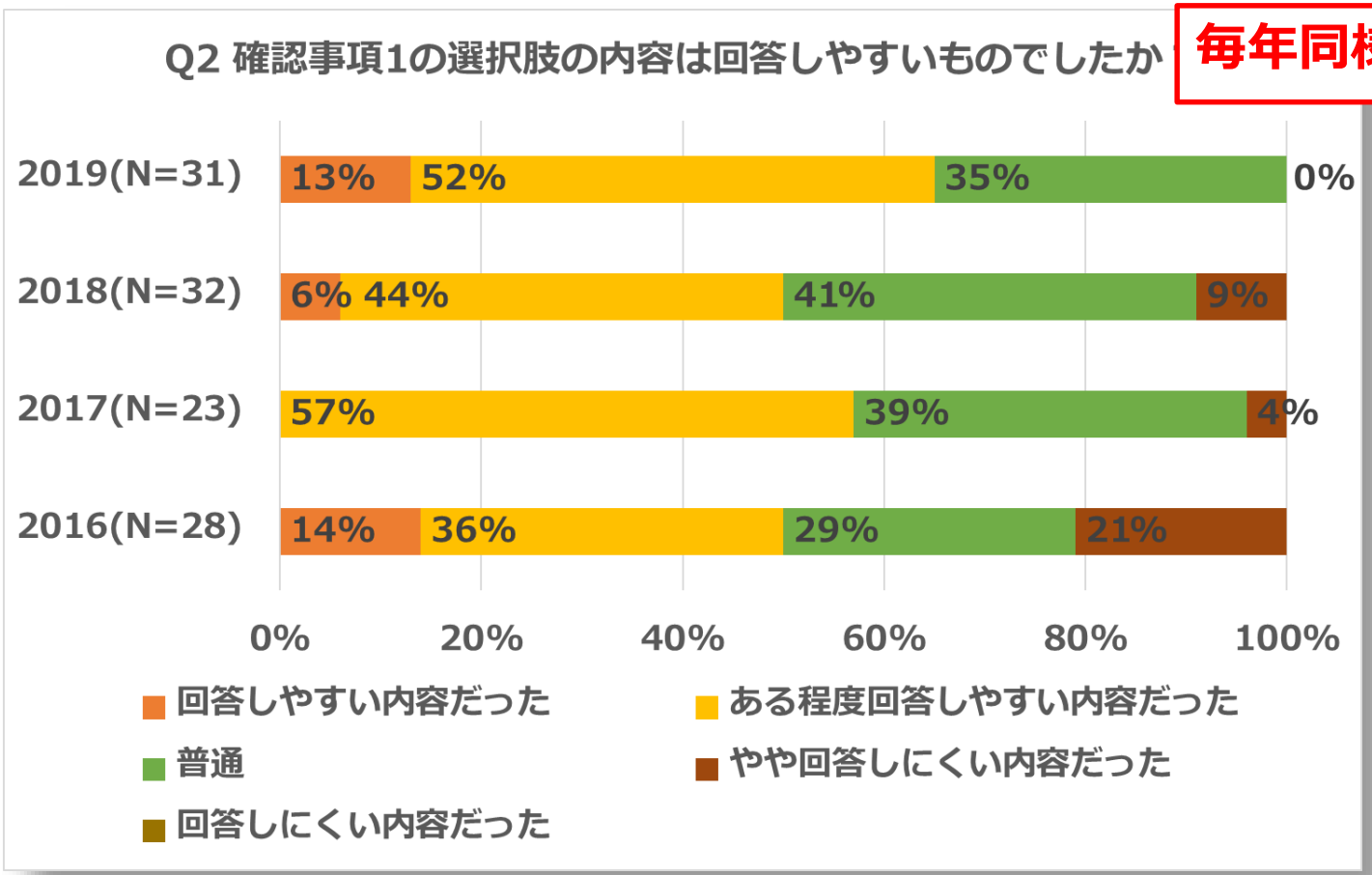
- **質問の内容は全体的に理解しやすい内容だった模様**
  - 理解しやすいが71%（理解しやすい：19%、ある程度理解しやすい：52%）、普通が29% 、理解しにくいが0%（やや理解しにくい：0%、理解しにくい：0%）



毎年同様な傾向

質問1の選択肢の内容は理解しやすいものでしたか？

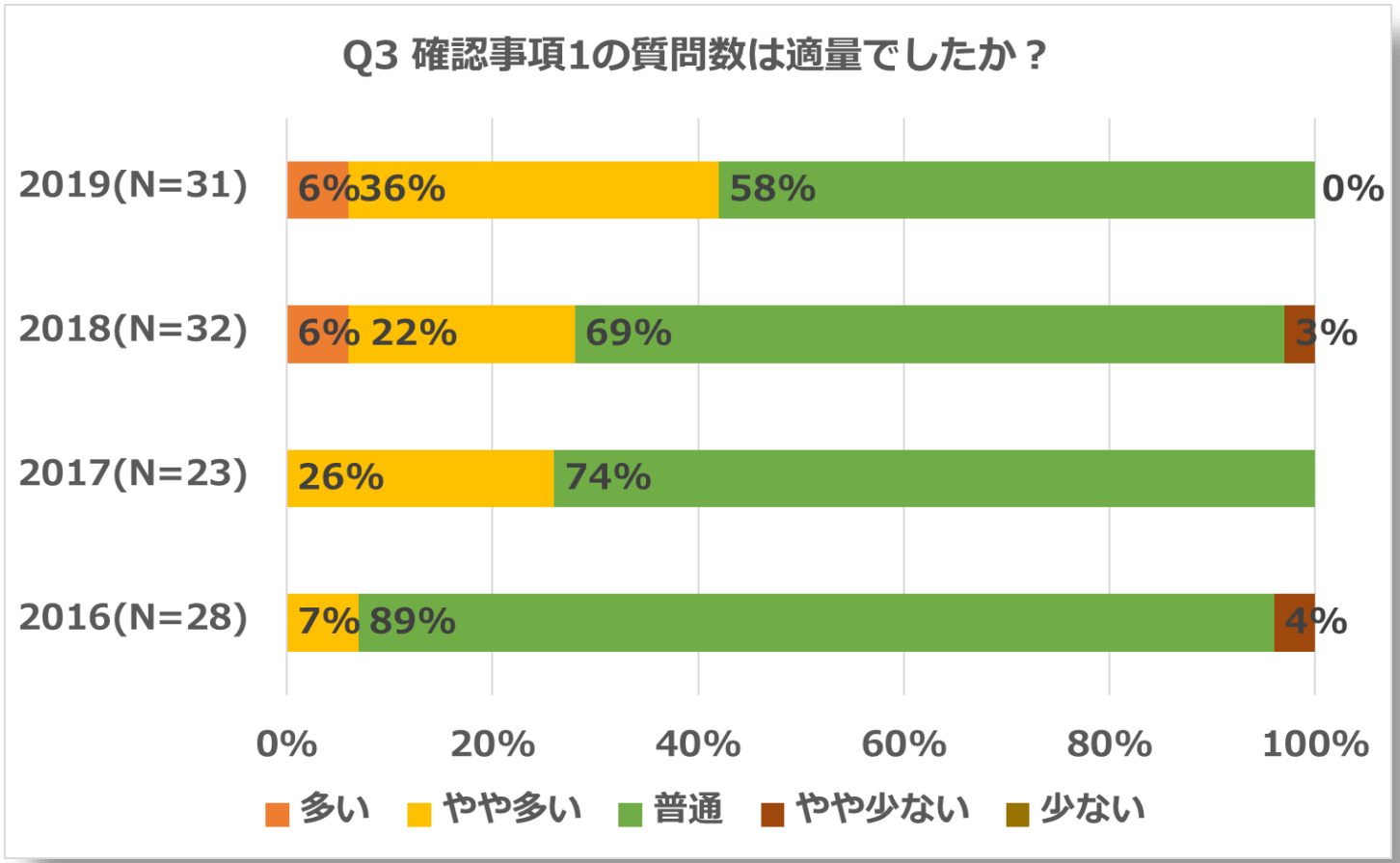
- **選択肢も全体的に理解しやすい内容だった模様**
  - 理解しやすいは65%（理解しやすい：13%、ある程度理解しやすい：52%）、普通が35% 、理解しにくいは0%（やや理解しにくい：0%、理解しにくい：0%）



毎年同様な傾向

質問1の質問数は適量でしたか？

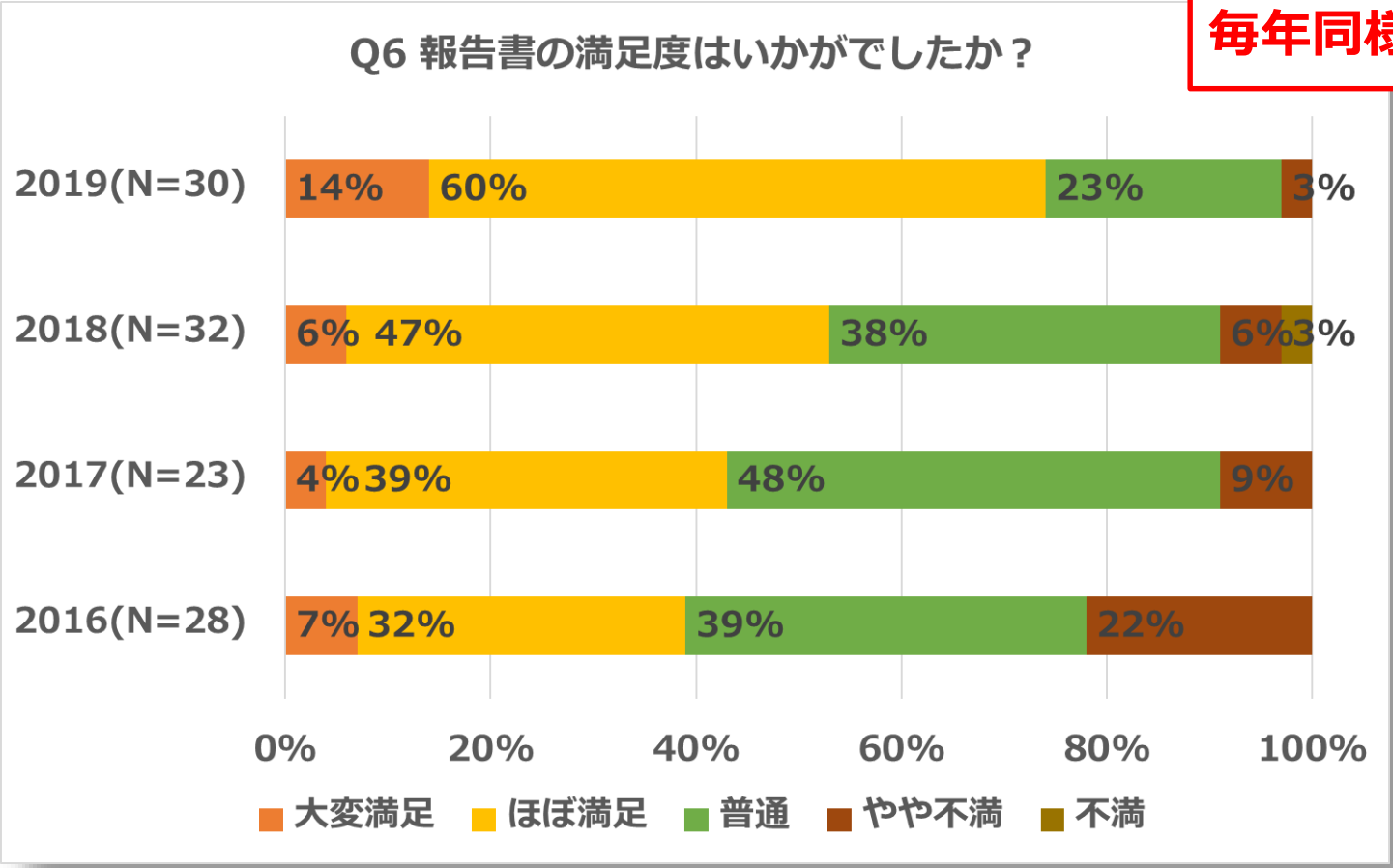
- **25問の問題数は適量だった模様**
  - 多いが6%、やや多いが36%、普通が58%、やや少ないが0%、少ないが0%
    - 徐々に「多い」の割合が増えている



報告書の満足度はいかがでしたか？

- **報告書は全体的に満足の高い内容だった模様**
  - 満足度は74%（大変満足：14%、ほぼ満足60%）
  - 評点に関しては実態を定量的かつ客観的に表しているコメントが多い

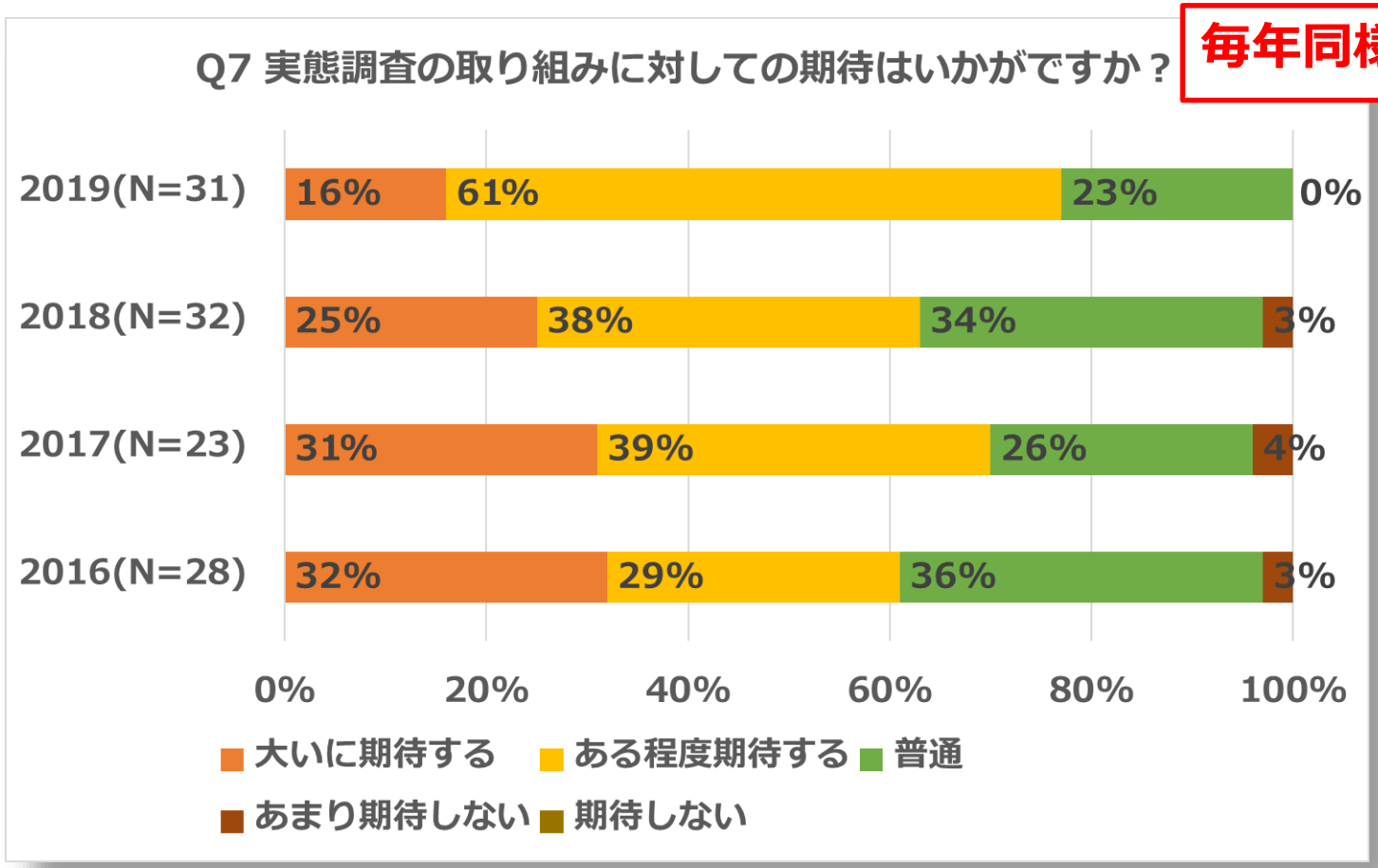
毎年同様な傾向



実態調査の取り組みに対しての期待はいかがですか？

- **取組は全体的に期待されている模様**
  - 期待は77%（大いに期待する：16%、ある程度期待する：61%）
  - 継続希望のコメントが多数あり

毎年同様な傾向



考察

- **評価方法に対して**
  - 自組織の情報セキュリティガバナンスの実態を定量的・客観的にチェックすることができる
    - 評点に関しては実態を定量的かつ客観的に表しているコメントが多い
  - 継続して実施することで情報セキュリティガバナンスの向上が期待できる
    - 特にベースステージの格上げ（最低限望まれる水準を満たす）が可能
- **学術機関情報セキュリティガバナンスに対して**
  - クラウド化要求事項の確認に関する活動が十分にできていない傾向
    - リスクアセスメント、外部委託時のセキュリティ策定やクラウド化要求事項の文書化などが実施できていない機関が多い
  - 組織的な管理方法の共通化・共有化が十分にできていない傾向
    - 管理策等の共通化、評価用のチェックリストの作成、インシデント対処方法の見直しなどの実施をしていない機関が多い
  - 望まれている水準を満たす機関は少ない傾向
  - ステージが高い機関と低い機関の差が開いてきている
    - ステージが高い機関は導入フェーズから運用フェーズに改善傾向が見られるが、低い機関は全体的に低い

- **学術機関の情報セキュリティガバナンスの実行性は高くない**

まとめ

- **2016年度から2019年度の学術機関の情報セキュリティガバナンスの実態調査結果および事後アンケート結果を報告**
  - 学術機関の情報セキュリティガバナンスの実態を定量的かつ客観的に評価できている
  - 継続して実施することで情報セキュリティガバナンスの向上も期待できる
  - 今後も継続的な調査が望まれている
  - リスクアセスメント、自己評価、見直しなど、組織的な管理の共通化に関する取り組みが十分にできておらず、学術機関の情報セキュリティガバナンスの実行性は高くないため評価上昇の余地がある
- **今後の課題**
  - 報告書の改善
  - フィードバック情報の充実
  - 協力機関の増加
  - 情報セキュリティガバナンスの自己チェック機能の提供