NIIオープンフォーラム2019@学術総合センター, 2019/5/29

2018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

-参加組織の取組みから見る評価上昇のポイント-

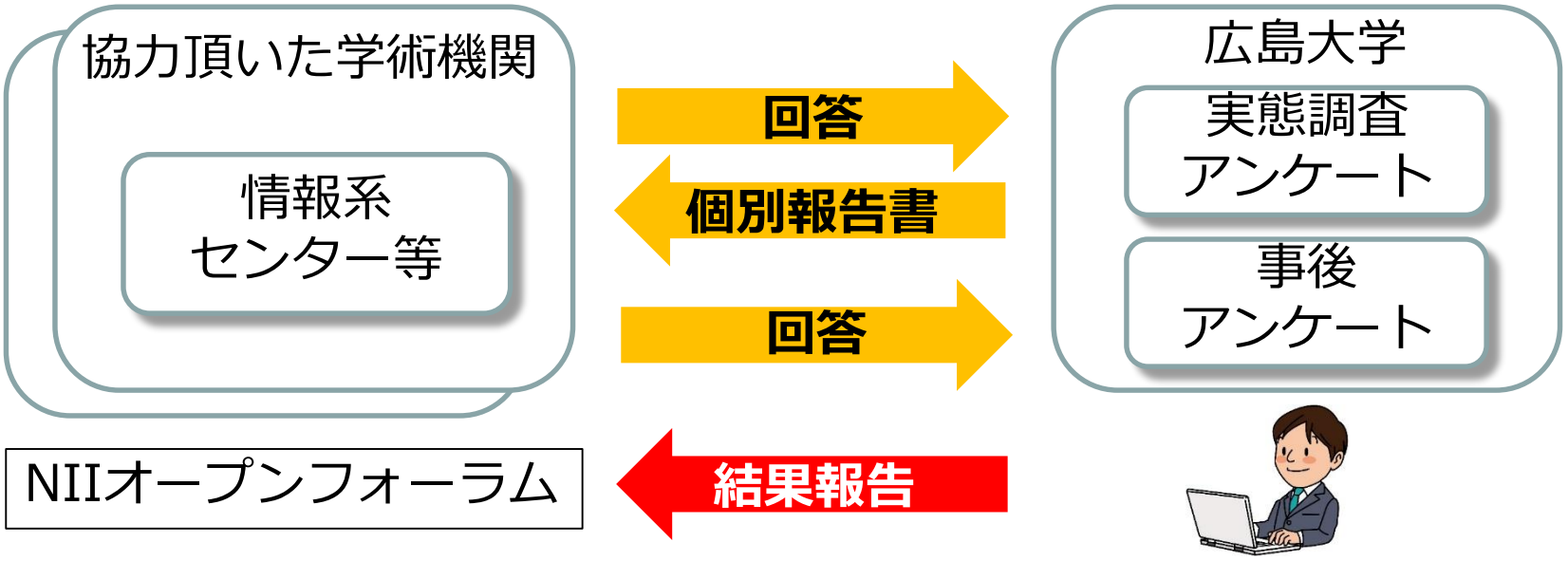
渡邉英伸

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2018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



実態調査の目的

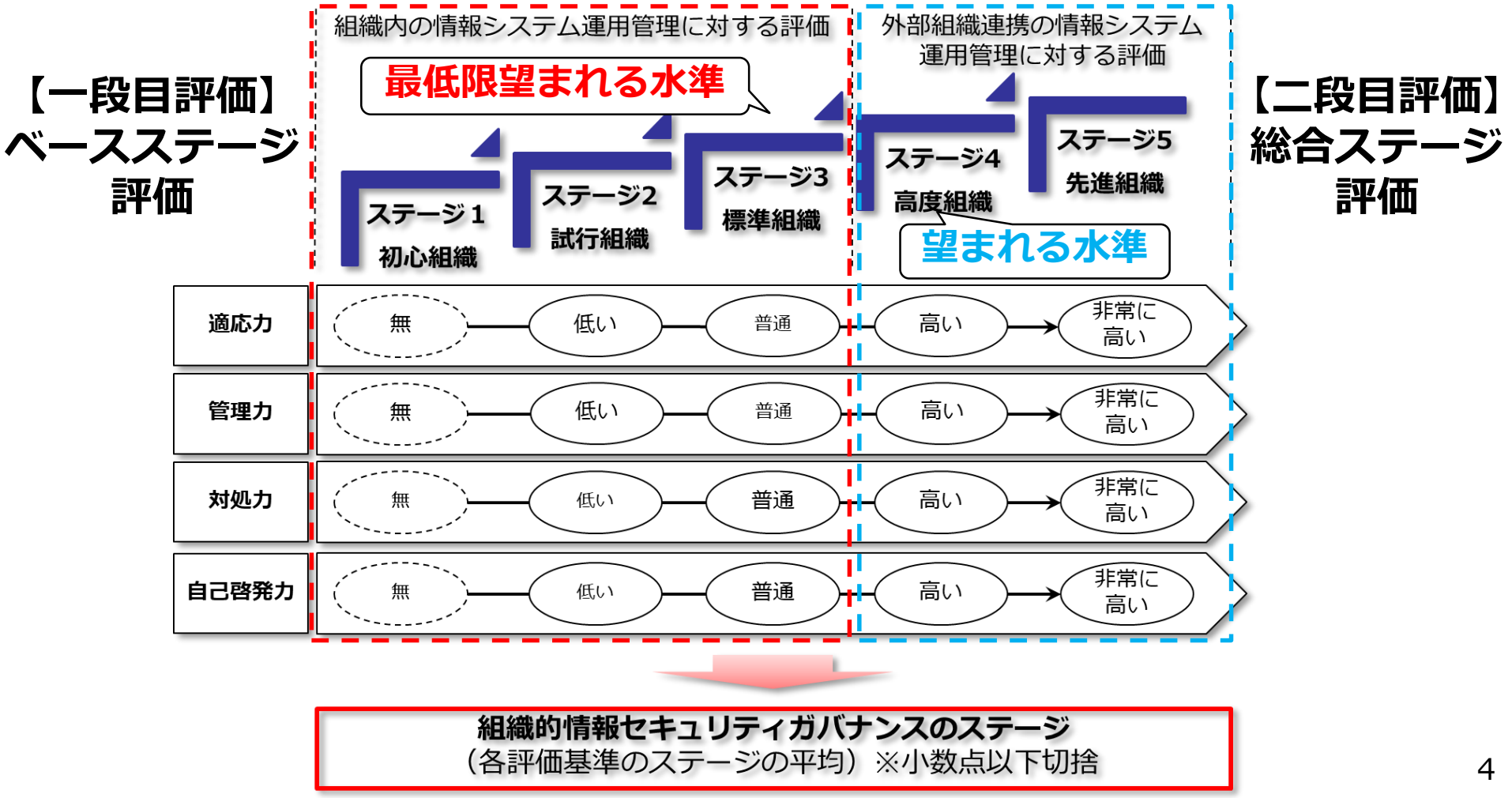
HIROSHIMA UNIVERSITY

- 本実態調査は、学術機関の情報セキュリティガバナンスの実態を把握し、クラウドサービス利用促進させるためのツールを提供することを目的としている

- 実態調査結果により、学術機関全体の傾向から自組織のクラウドサービス利用に対する意識や情報セキュリティガバナンスに関する現状の問題点・課題を明らかにすると同時に、貴組織が次に実施すべき情報セキュリティガバナンスの取組みを明確にすることを目指します。

評価モデル

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）



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%（43／43機関）
    - 昨年度： 100%（31／31機関）、 一昨年：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：58%（25／43機関）
    - 昨年度： 58%（18／31機関）、 一昨年：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：58%（25／43機関）
    - 昨年度： 45%（14／31機関） 、一昨年：60%（17／28機関）

CSIRTの対応状況の把握

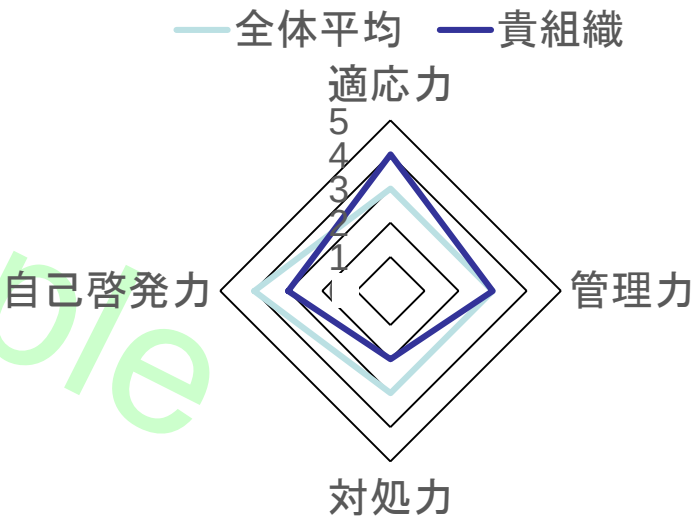
個別報告書のイメージ

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 NEW!
・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

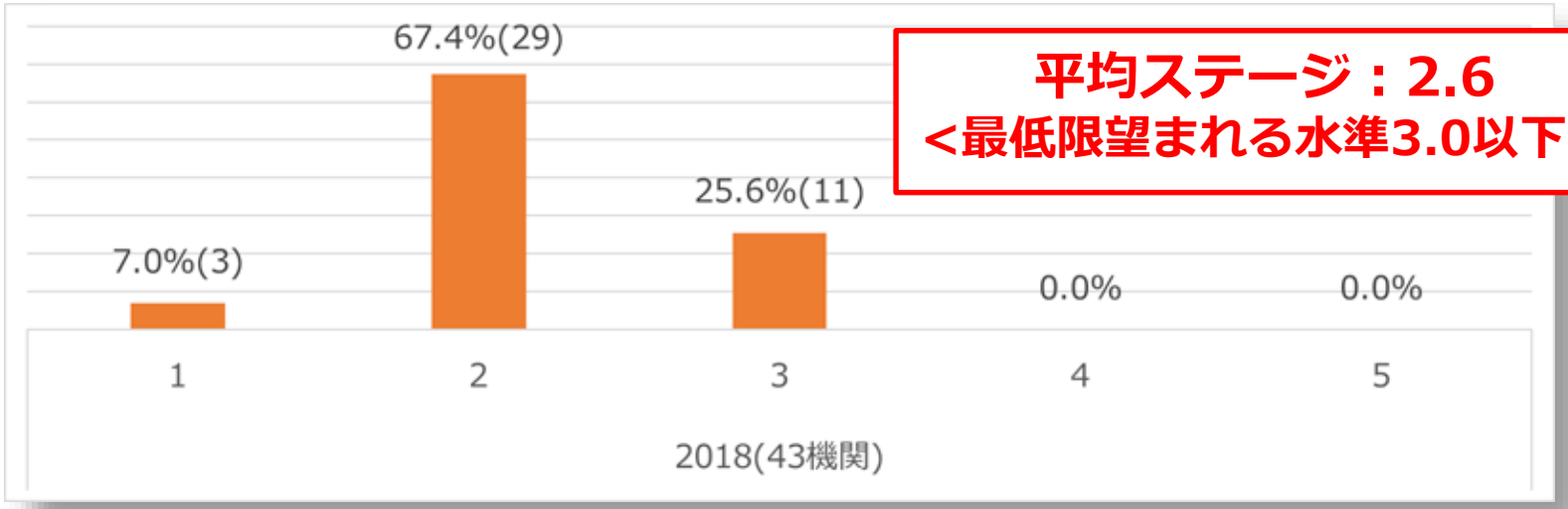
今後のポイント
・水準を満たしていない設問を列挙

実態調査概要

- **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

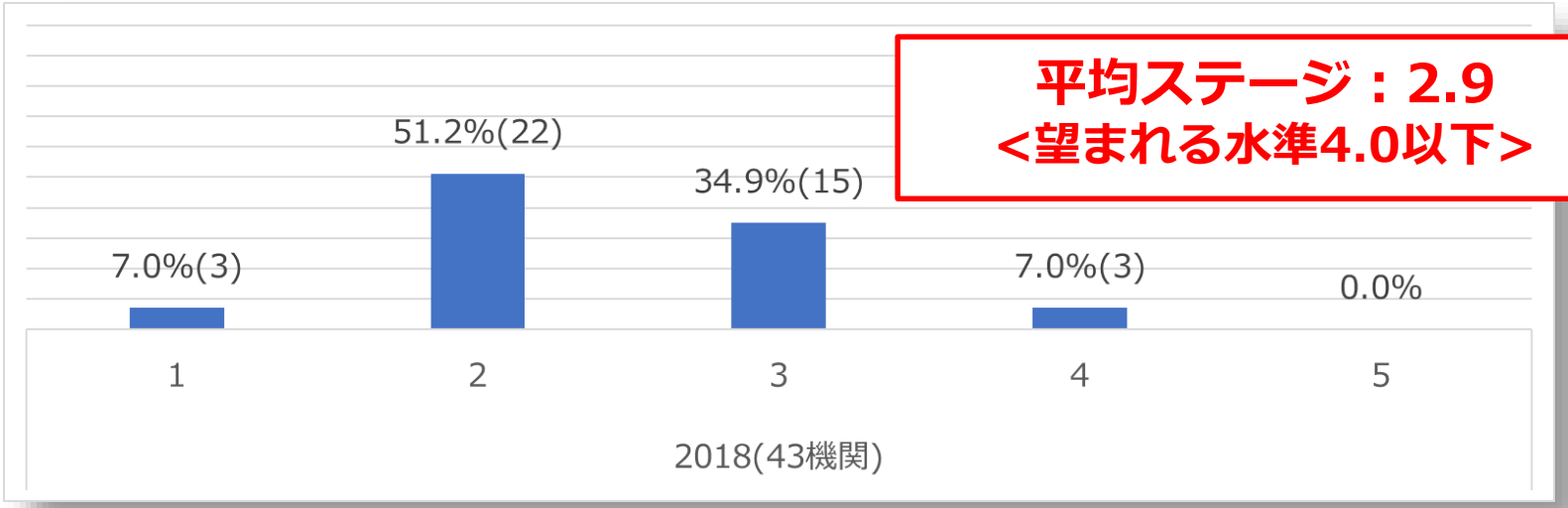
2018年度ベース／総合ステージ分布図

2018年度43機関のベースステージ分布



平均ステージ：2.6
<最低限望まれる水準3.0以下>

2018年度43機関の総合ステージ分布



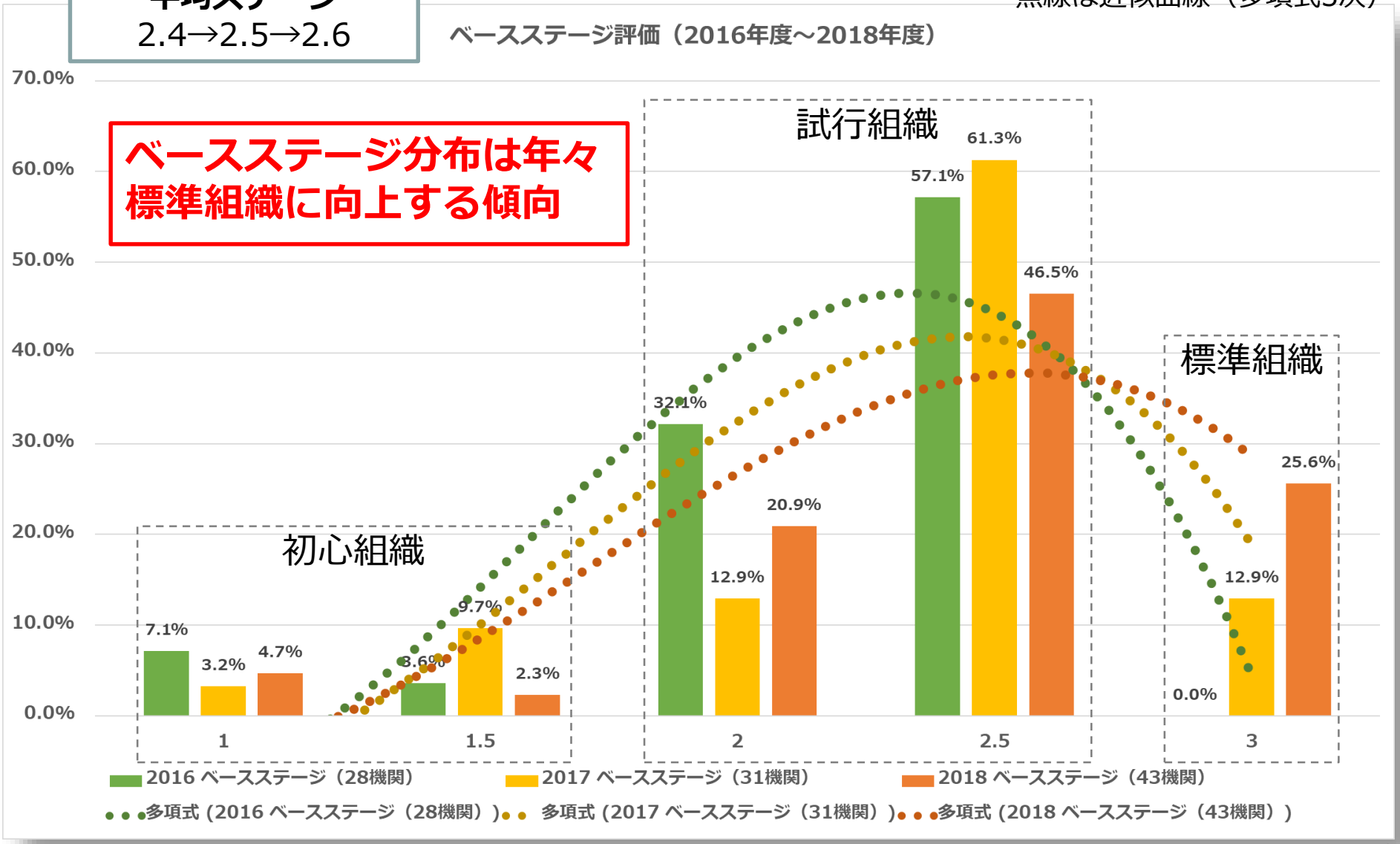
平均ステージ：2.9
<望まれる水準4.0以下>

年度別ベースステージ分布図

HIROSHIMA UNIVERSITY

平均ステージ
2.4→2.5→2.6

点線は近似曲線（多項式3次）

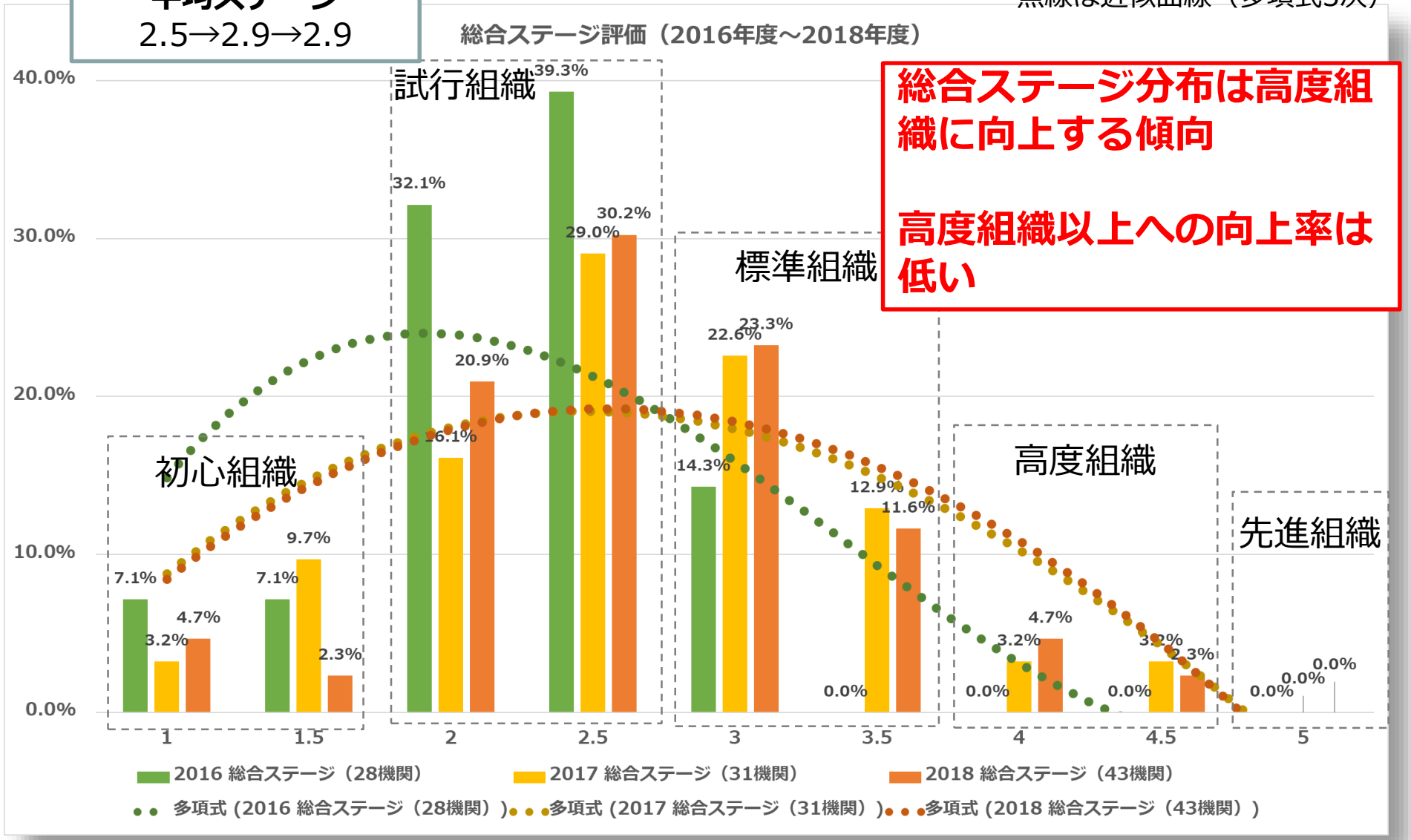


年度別総合ステージ分布図

HIROSHIMA UNIVERSITY

平均ステージ
2.5→2.9→2.9

点線は近似曲線（多項式3次）



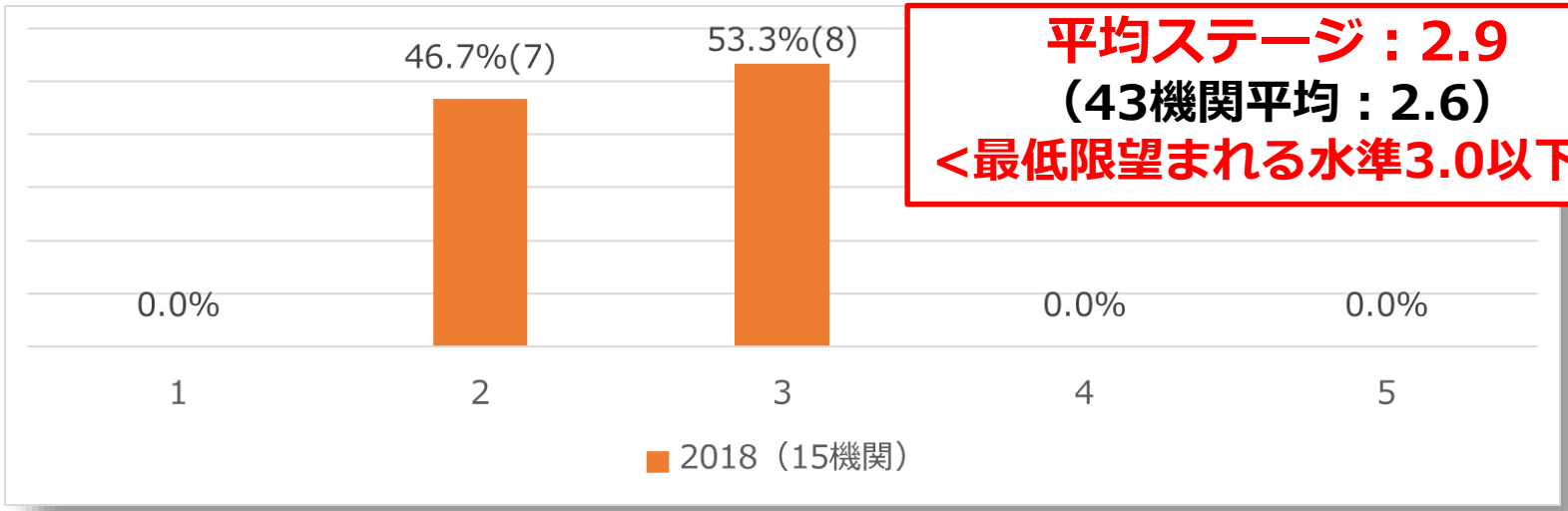
総合ステージ分布は高度組織に向上する傾向

高度組織以上への向上率は低い

継続参加機関ベース／総合ステージ分布図

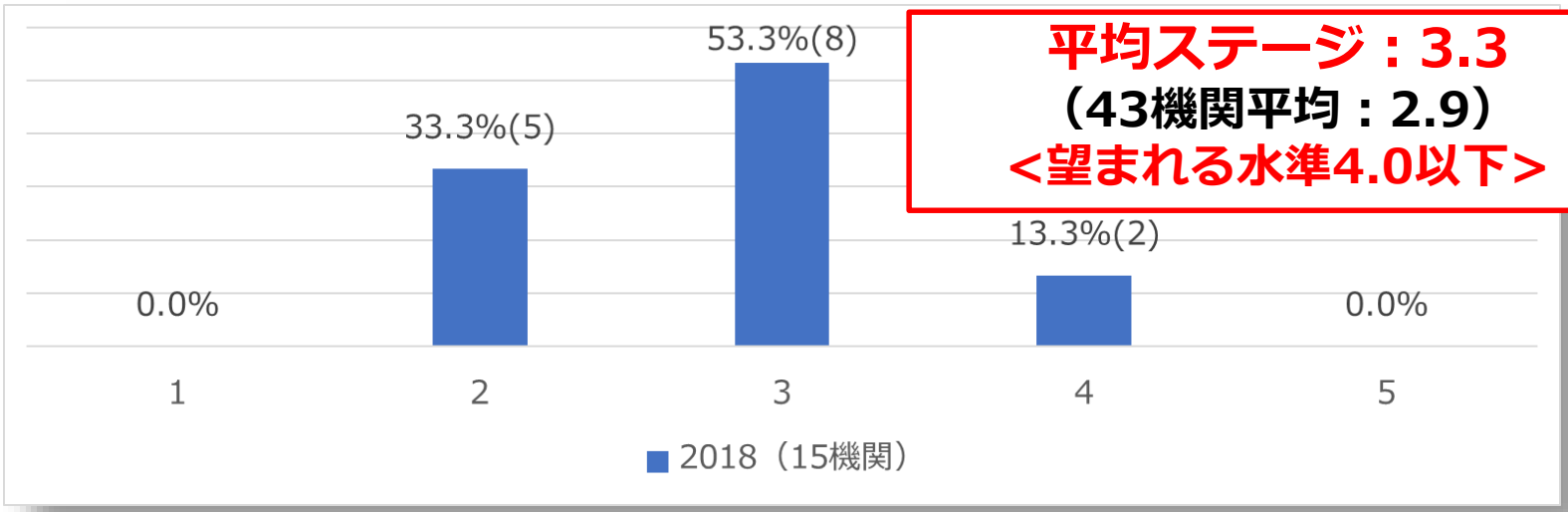
HIROSHIMA UNIVERSITY

2016年度から継続参加の15機関の2018年度ベースステージ分布



平均ステージ：2.9
（43機関平均：2.6）
<最低限望まれる水準3.0以下>

2016年度から継続参加の2018年度総合ステージ分布



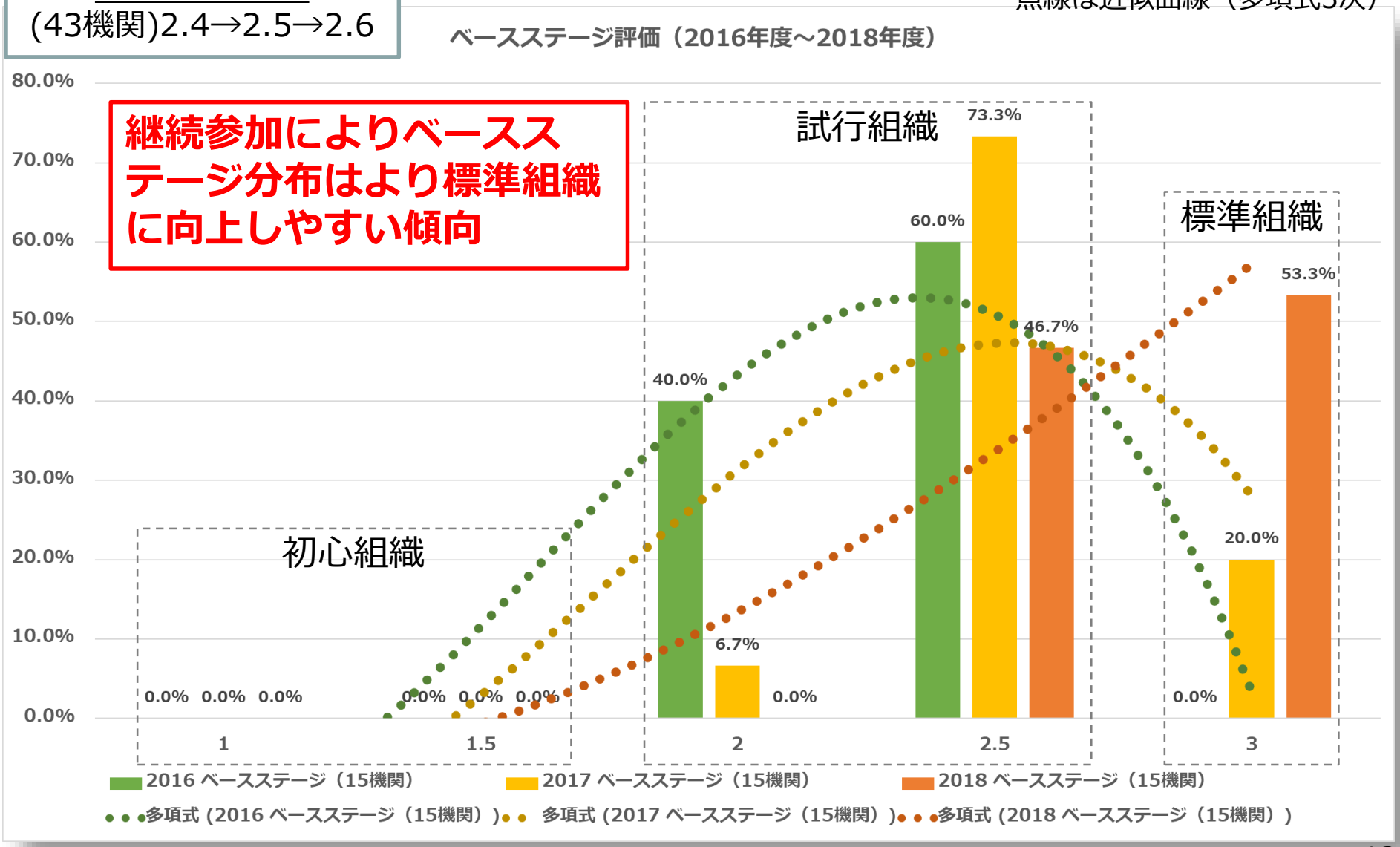
平均ステージ：3.3
（43機関平均：2.9）
<望まれる水準4.0以下>

継続参加機関年度別ベースステージ分布図

HIROSHIMA UNIVERSITY

平均ステージ
2.5→2.8→2.9
(43機関)2.4→2.5→2.6

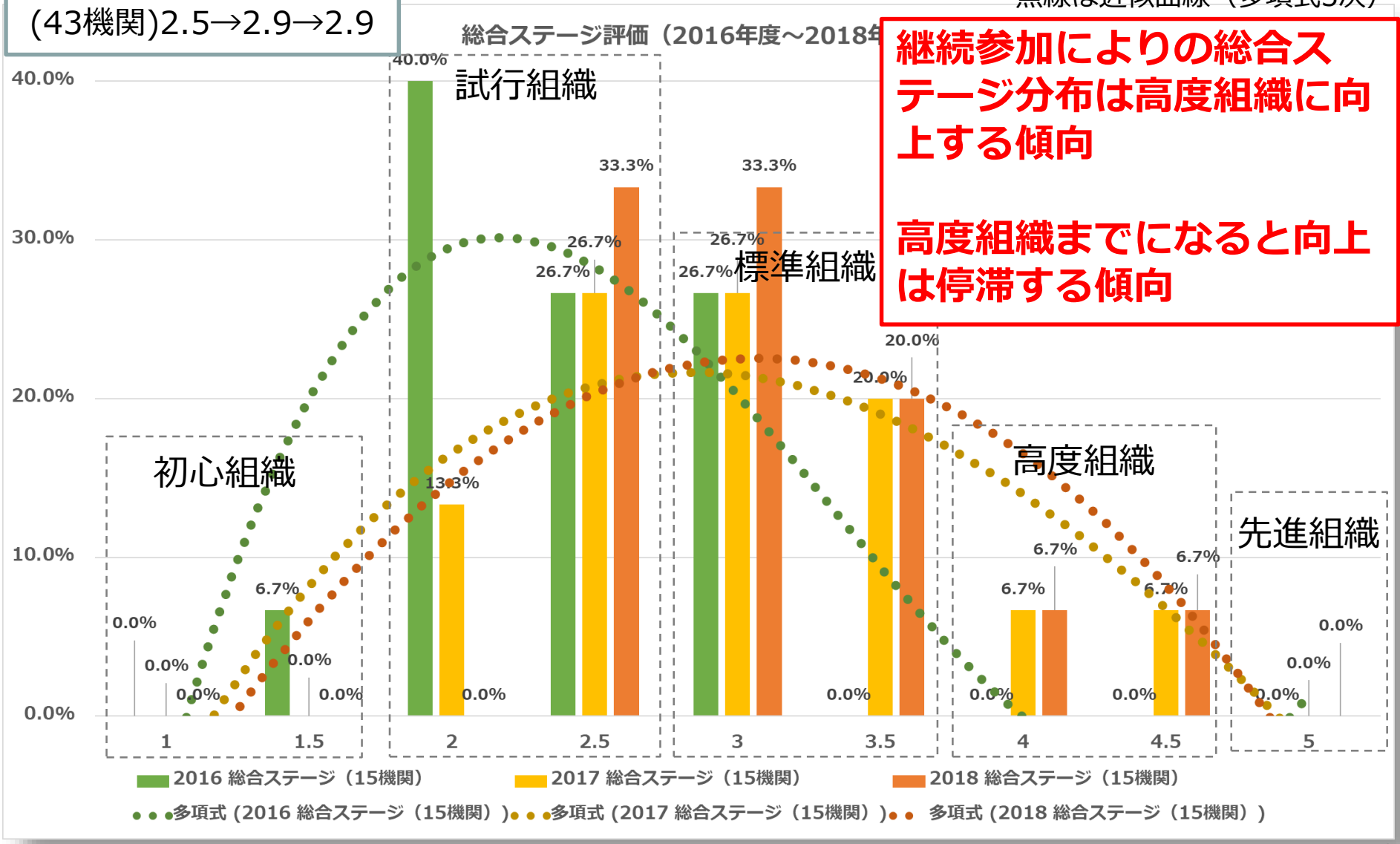
点線は近似曲線（多項式3次）



継続参加機関年度別総合ステージ分布図

平均ステージ
2.6→3.2→3.3
(43機関)2.5→2.9→2.9

点線は近似曲線（多項式3次）



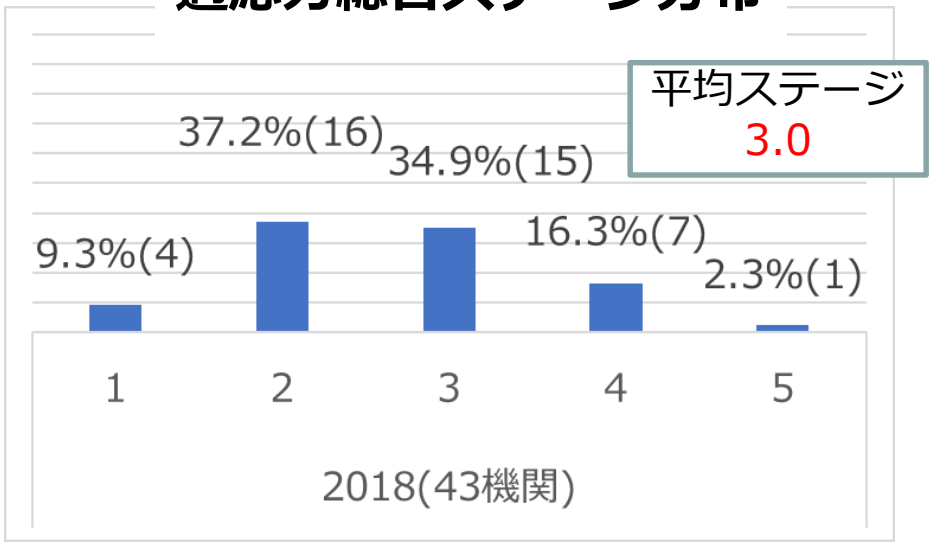
継続参加によりの総合ステージ分布は高度組織に向上する傾向

高度組織までになると向上は停滞する傾向

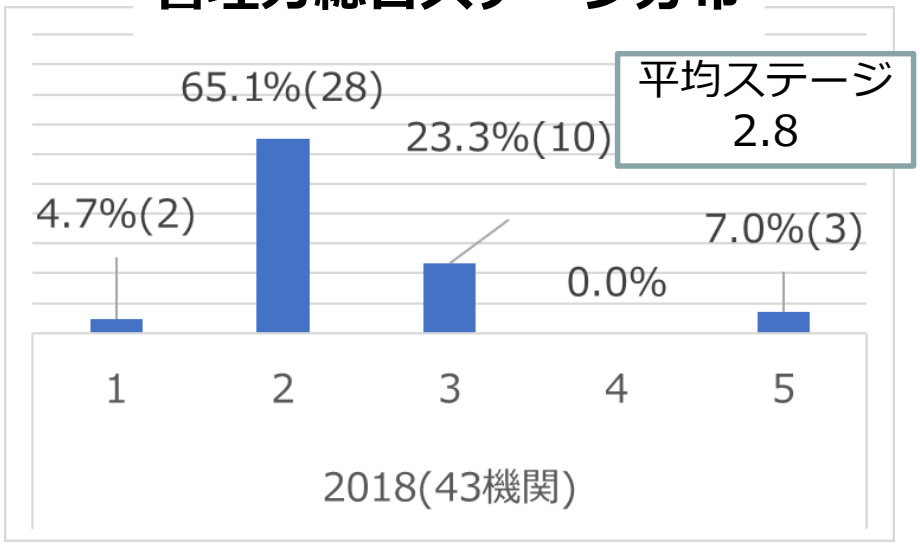
2018年度評価基準別総合ステージ分布図

HIROSHIMA UNIVERSITY

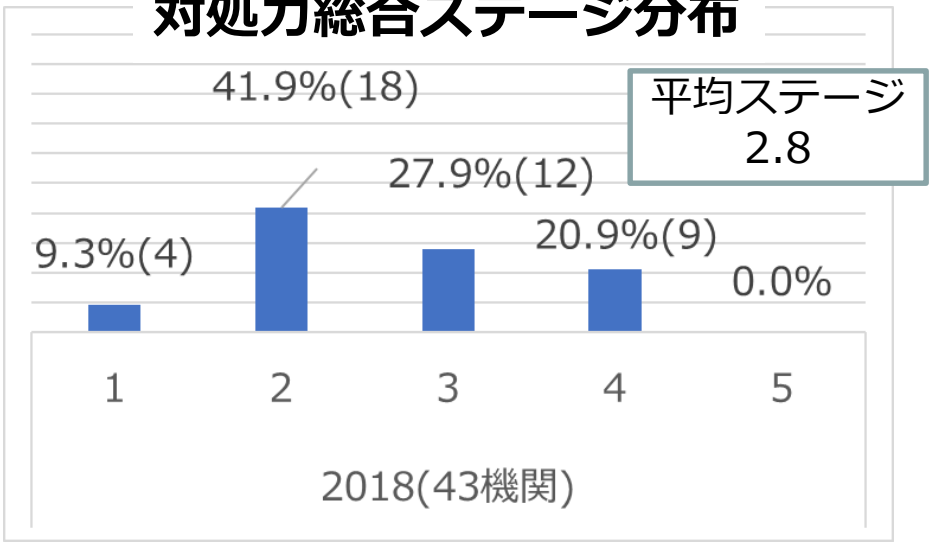
適応力総合ステージ分布



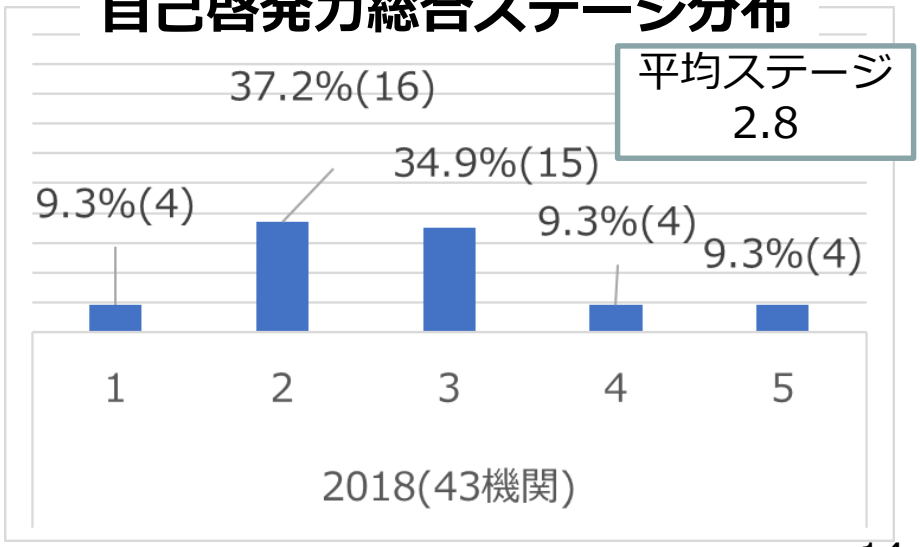
管理力総合ステージ分布



対処力総合ステージ分布

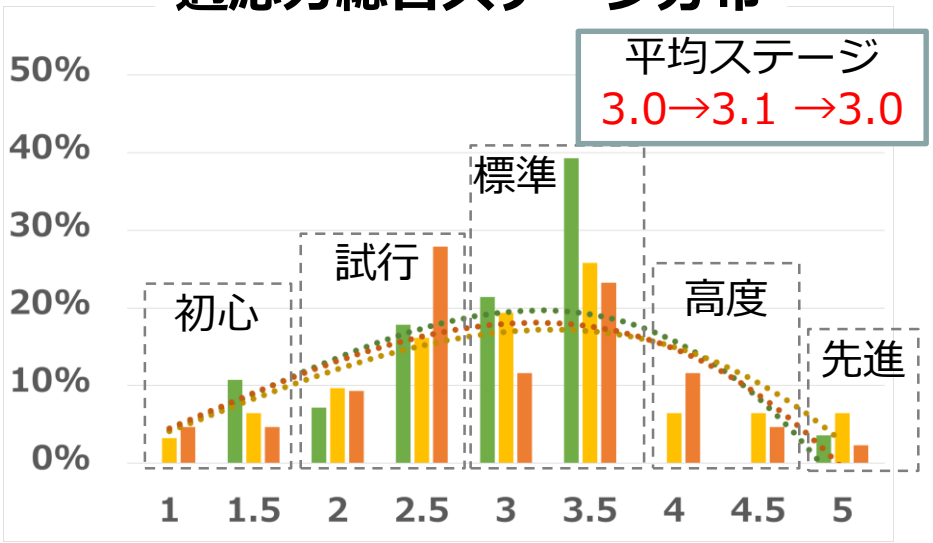


自己啓発力総合ステージ分布

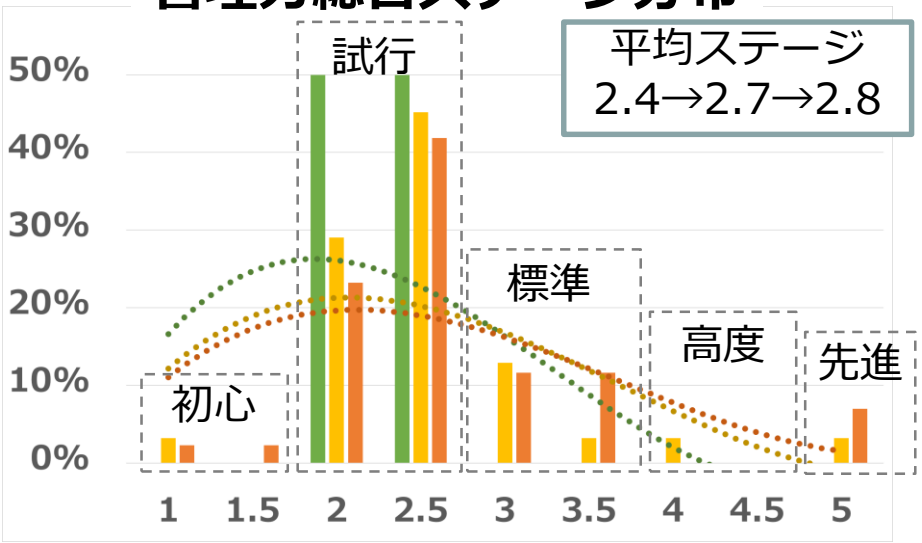


継続参加機関年度・評価基準別総合ステージ分布図

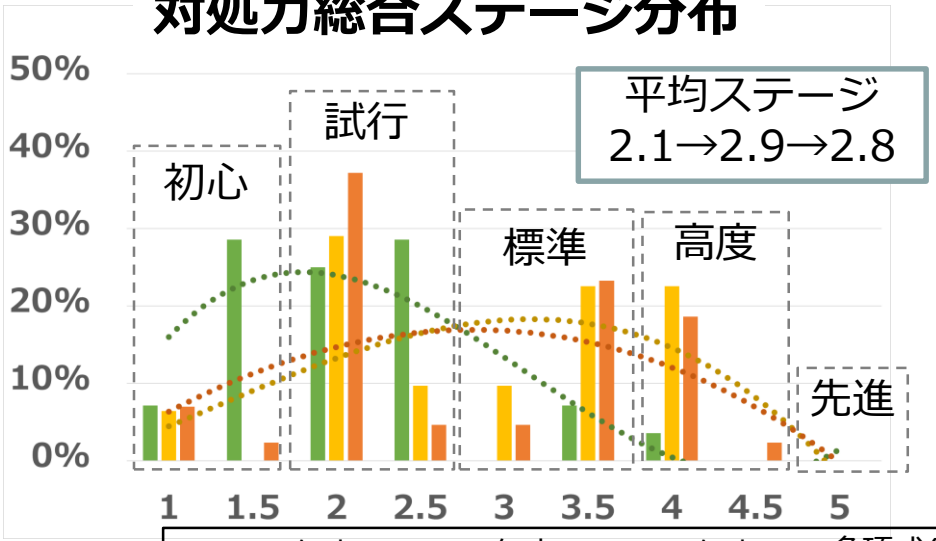
適応力総合ステージ分布



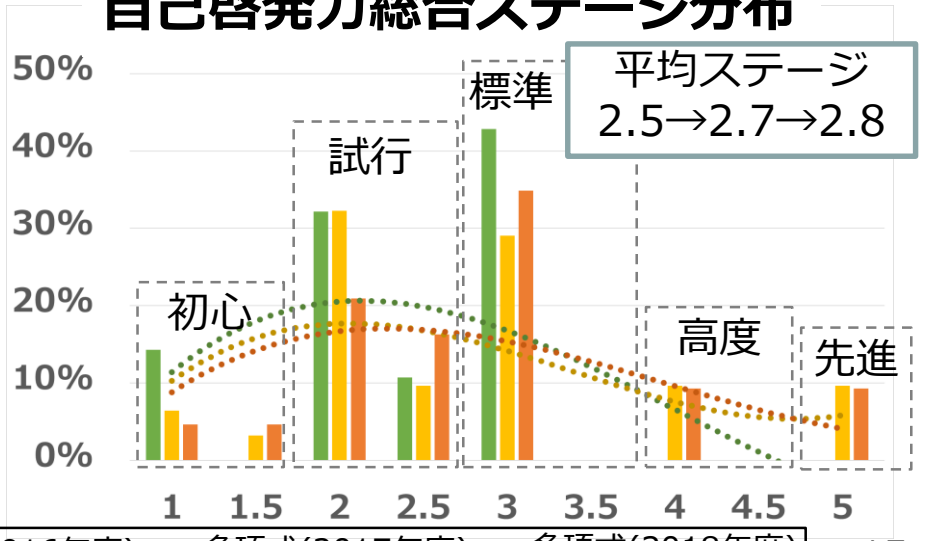
管理力総合ステージ分布



対処力総合ステージ分布



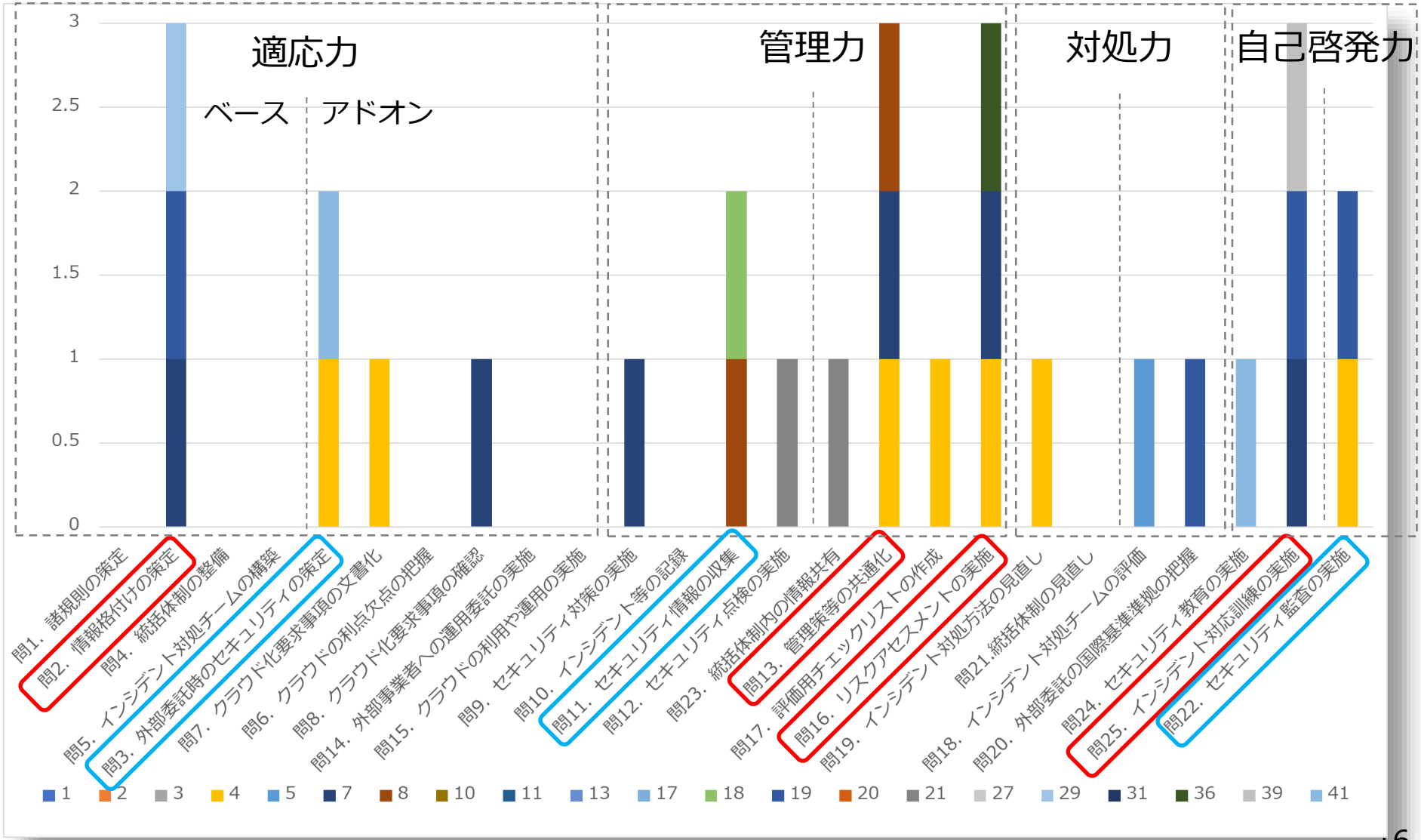
自己啓発力総合ステージ分布



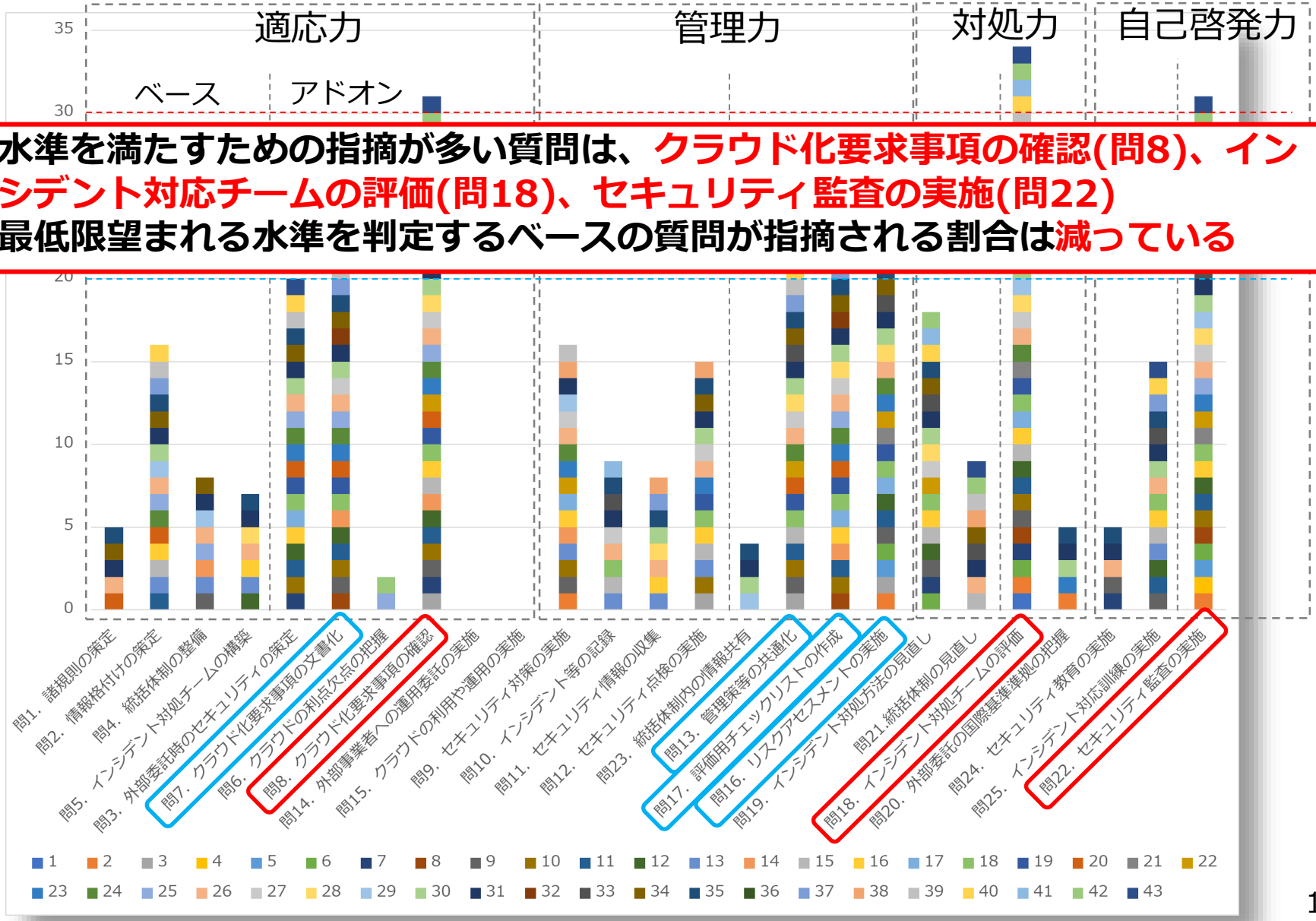
2016年度 2017年度 2018年度 多項式(2016年度) 多項式(2017年度) 多項式(2018年度)

質問別改善数分布図(2017年度から継続参加の21機関)

改善傾向があった質問は、情報格付けの策定(問2)、管理策等の共通化(問13)、リスクアセスメントの実施(問16)、インシデント対応訓練の実施(問25)



質問別指摘数分布図(2018年度)



- 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)、インシデント対応チームの評価(問18)、セキュリティ監査の実施(問22)**
- 最低限望まれる水準を判定するベースの質問が指摘される割合は**減っている**

2018年度事後アンケート結果

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：**
  - 74%（32／43機関）
    - 昨年度：74% （23／31機関） 、一昨年ど：100%（28／28機関）

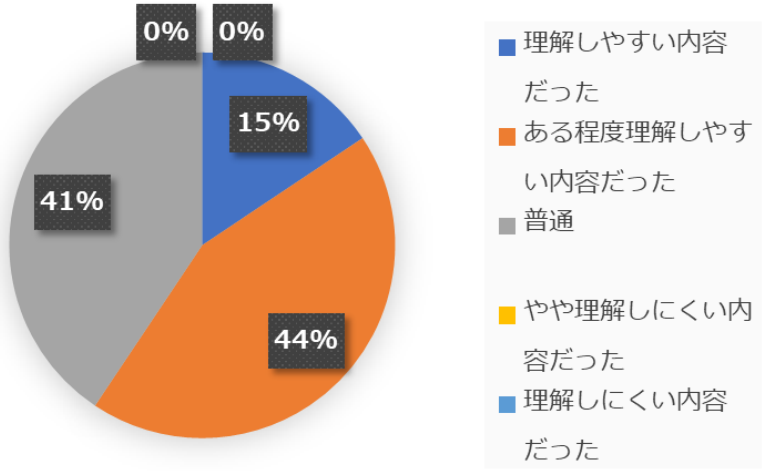
質問1、報告書、取り組みに対する評価の内容に限定し紹介

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59%（理解しやすい：15%、ある程度理解しやすい：44%）、普通が41% 、理解しにくいが4%（やや理解しにくい：4%、理解しにくい：0%）

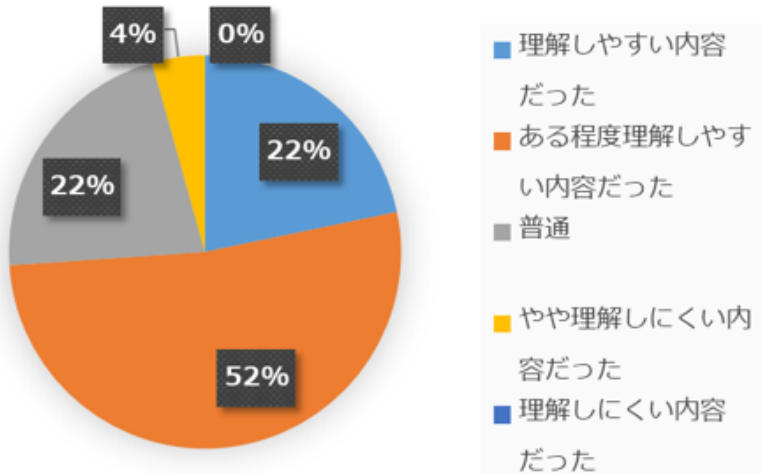
2018年度（N=32）

1	理解しやすい内容だった	5
2	ある程度理解しやすい内容だった	14
3	普通	13
4	やや理解しにくい内容だった	0
5	理解しにくい内容だった	0



2017年度（N=23）

1	理解しやすい内容だった	5
2	ある程度理解しやすい内容だった	12
3	普通	5
4	やや理解しにくい内容だった	1
5	理解しにくい内容だった	0

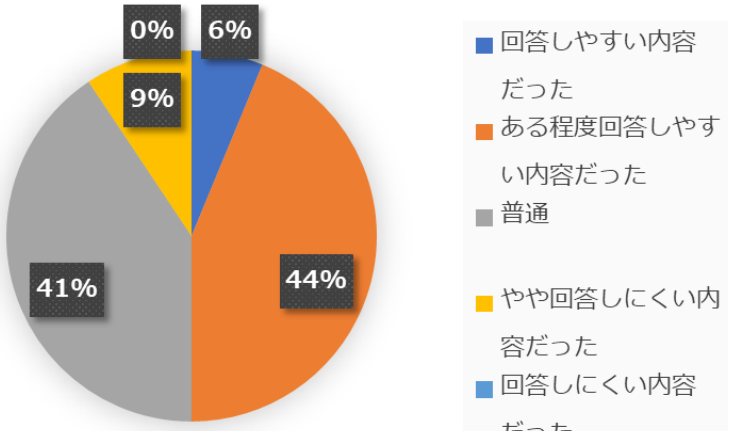


質問1の選択肢の内容は理解しやすいものでしたか？

- **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50%（理解しやすい：6%、ある程度理解しやすい：44%）、普通が41% 、理解しにくいは9%（やや理解しにくい：9%、理解しにくい：0%）

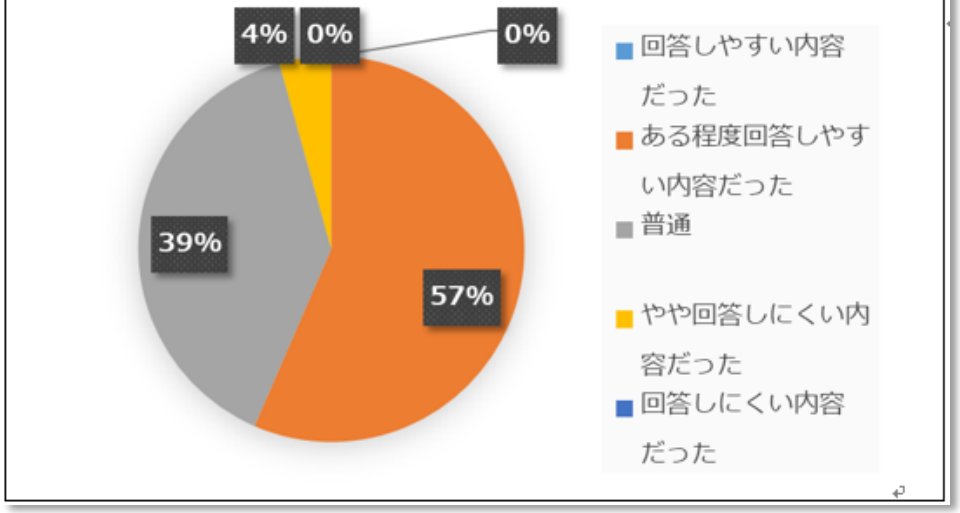
2018年度（N=32）

1	回答しやすい内容だった	2
2	ある程度回答しやすい内容だった	14
3	普通	13
4	やや回答しにくい内容だった	3
5	回答しにくい内容だった	0



2017年度（N=23）

1	回答しやすい内容だった	0
2	ある程度回答しやすい内容だった	13
3	普通	9
4	やや回答しにくい内容だった	1
5	回答しにくい内容だった	0

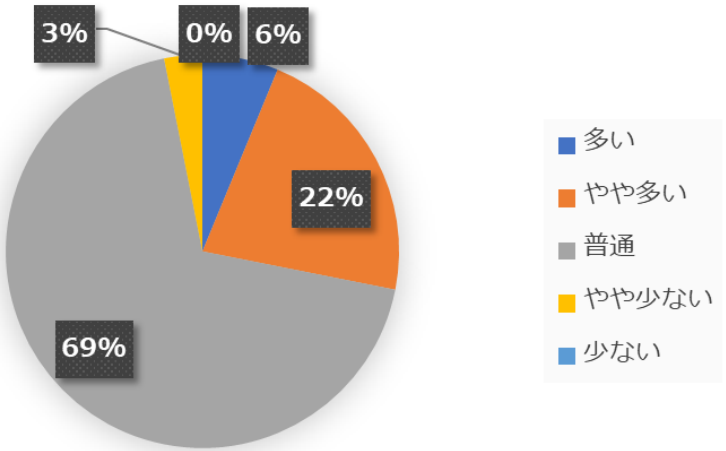


質問1の質問数は適量でしたか？

- **25問の問題数は適量だった模様**
  - 多いが6%、やや多いが22%、普通が69%、やや少ないが3%、少ないが0%

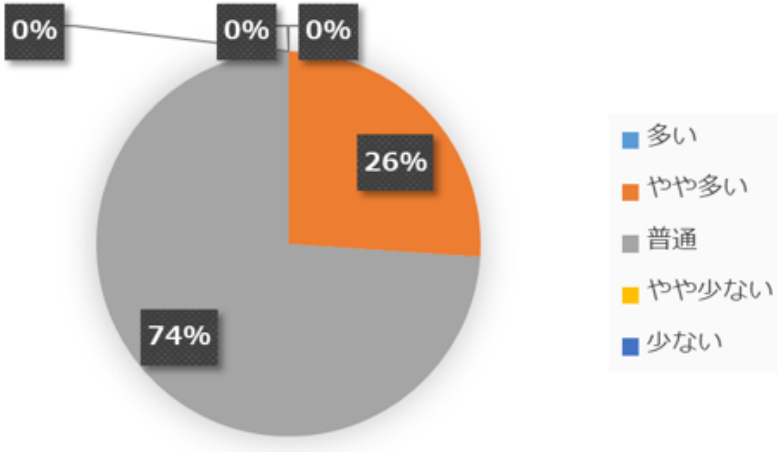
2018年度（N=32）

1	多い	2
2	やや多い	7
3	普通	22
4	やや少ない	1
5	少ない	0



2017年度（N=23）

1	多い	0
2	やや多い	6
3	普通	17
4	やや少ない	0
5	少ない	0

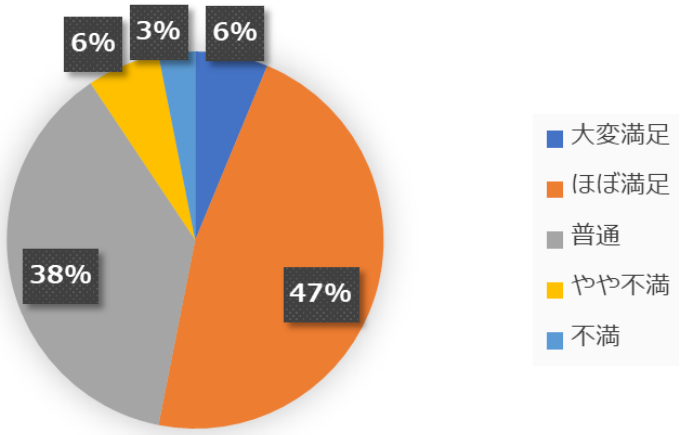


報告書の満足度はいかがでしたか？

- **報告書は全体的に満足の高い内容だった模様**
  - 満足度は53%（大変満足：6%、ほぼ満足47%）
  - 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
  - 昨年度からの改善傾向を追記したことが満足度を向上した可能性がある

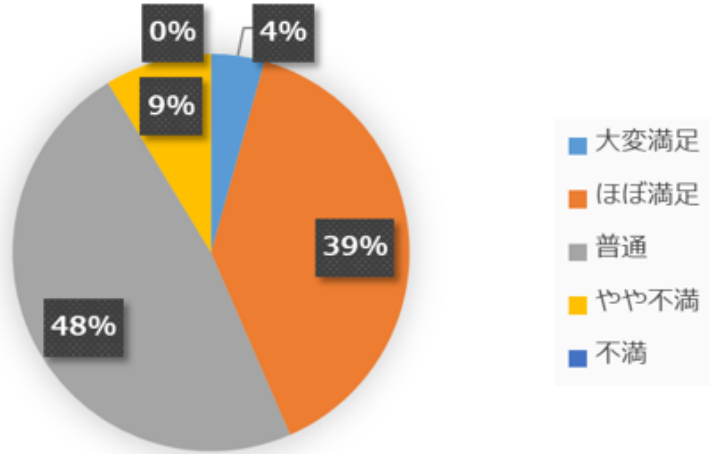
2018年度（N=32）

1	大変満足	2
2	ほぼ満足	15
3	普通	12
4	やや不満	2
5	不満	1



2017年度（N=23）

1	大変満足	1
2	ほぼ満足	9
3	普通	11
4	やや不満	2
5	不満	0

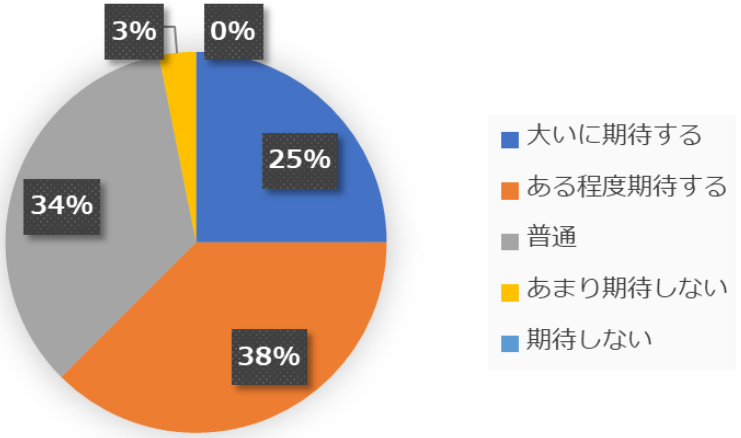


実態調査の取り組みに対しての期待はいかがですか？

- **取組は全体的に期待されている模様**
  - 期待は63%（大いに期待する：25%、ある程度期待する：38%）
  - 継続希望のコメントが多数あり

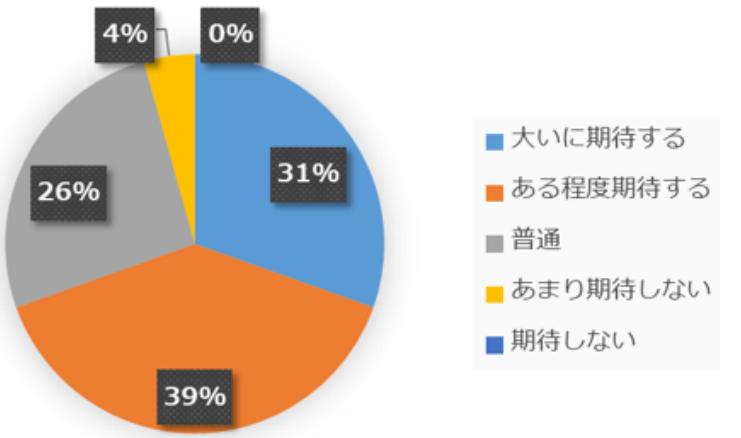
2018年度（N=32）

1	大いに期待する	8
2	ある程度期待する	12
3	普通	11
4	あまり期待しない	1
5	期待しない	0



2017年度（N=23）

1	大いに期待する	7
2	ある程度期待する	9
3	普通	6
4	あまり期待しない	1
5	期待しない	0



考察

- **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
- **自己評価や見直しに関する活動が十分にできていない傾向**
  - インシデント対応チームの評価、リスクアセスメントの実施、評価用チェックリストの作成、情報セキュリティ監査などの実施をしていない機関が多い
- **組織的な共通化・共有化が十分にできていない傾向**
  - クラウド化要求事項の確認、クラウド化要求事項の文書化、管理策等の共通化などの実施をしていない機関が多い
  - 昨年度と回答者が変わったことで総合ステージを下げた機関が1機関あった

- **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**
  - 今回クラウド化の意識が高い機関や積極的に利用している機関における結果であるが、それでも望まれている水準を満たす機関は少ない
  - 特にクラウド導入後の運用管理フェーズ（PDCAのDo,Check,Act）の上記の質問の取組が評価上昇のポイント

今後の課題（回答者からの意見より）

- **報告書の改善**
  - ITに詳しくない上位層(CIOなど)にそのまま提出可能な分かりやすく有用な報告書にしてほしいニーズがあった
- **フィードバック情報の充実**
  - 各機関で評点が向上した具体的な良い対策内容を付加情報として提供してほしいニーズがあった
- **実施時期の変更**
  - 年明け・年度末の業務が立て込む時期に実施していたため、ずらしてほしいニーズがあった
- **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**
  - いつでも情報セキュリティガバナンス実態を自己チェックできる機能を提供することでサンプル数の増加を目指したい

まとめ

- **2016年度から2018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
  - 自己評価や見直し、組織的な共通化・共有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
  - 実施時期の変更
  - 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