NIIオープンフォーラム2022@オンライン, 2022/6/1

2021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

– 6年間の評価結果から見るガバナンスの成熟度 –

渡邉英伸, 西村浩二

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2021年度の6年間における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

実態調査質問概要

HIROSHIMA UNIVERSITY

- **質問1**
  - 内容：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）
    - 2020: 100%（40機関）、2019: 100%（40機関）、2018：100%（43機関）、2017： 100%（31機関）、 2016：100%（28機関）

ガバナンスの現状の把握

- **質問2**
  - 内容：組織が運用中の情報システム名、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：70%（28／40機関）
    - 2020: 55%（22／40機関）、2019：62%（25／40機関）2018：58%（25／43機関）2017： 58%（18／31機関）、 2016：82%（23／28機関）

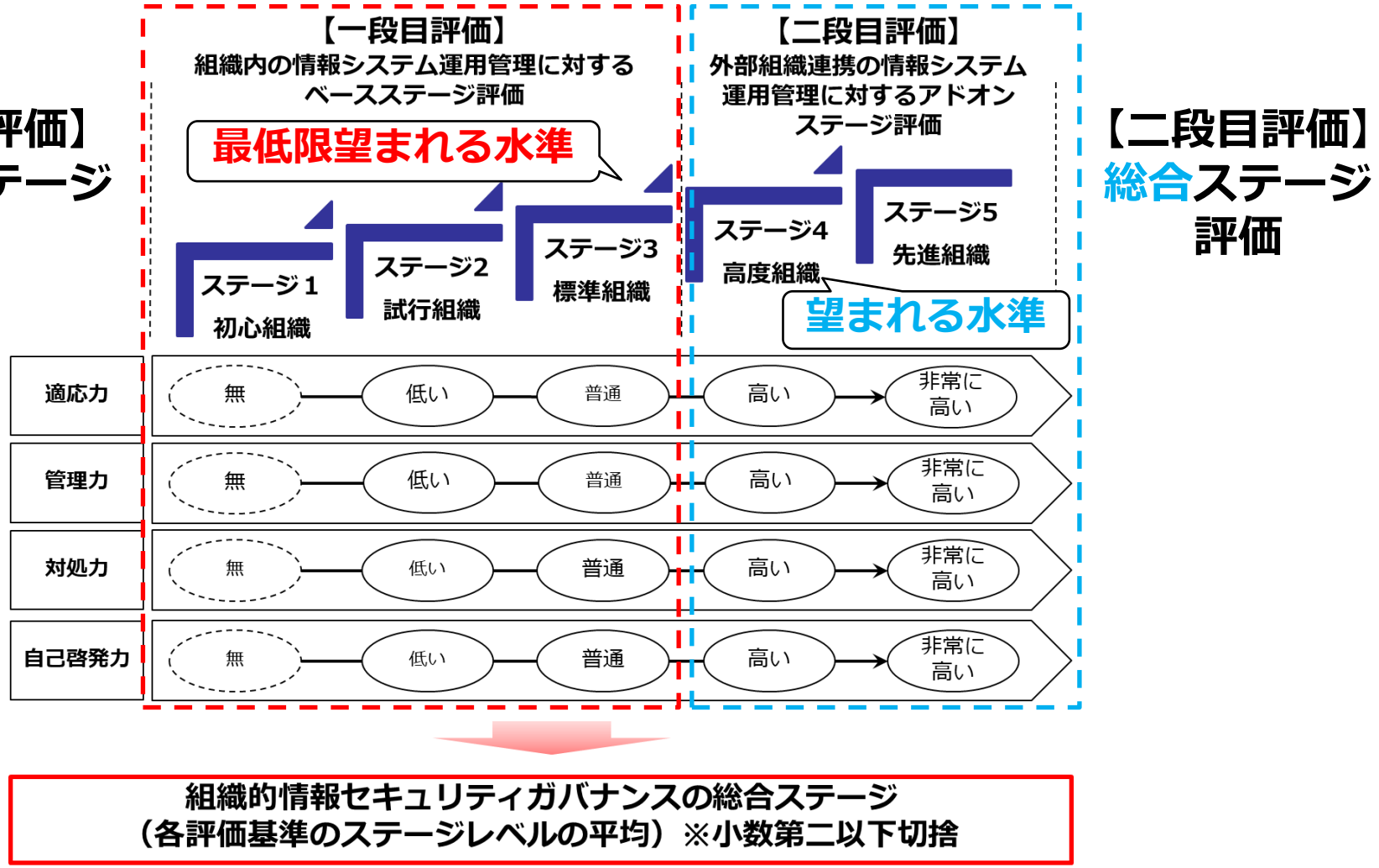
情報資産の管理状況の把握

- **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：62%（25／40機関）
    - 2020: 68%（27／40機関）、 2019：68%（27／40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

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）



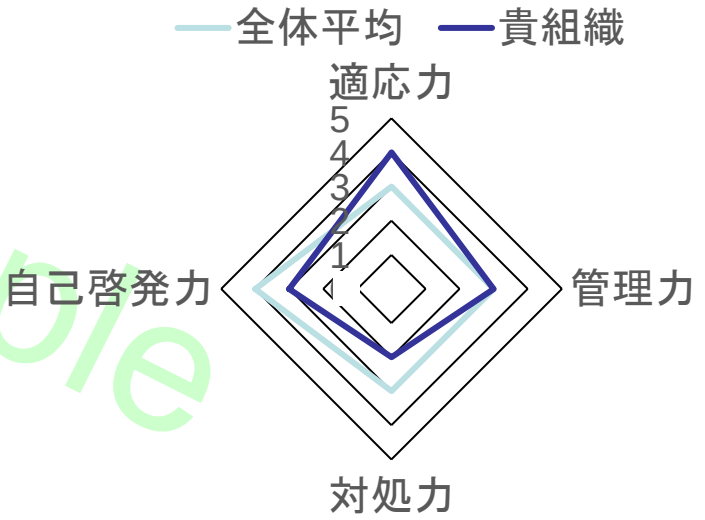
個別報告書のイメージ

「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～2021年度
実態調査結果

HIROSHIMA UNIVERSITY

実態調査概要

- **2021年度調査**
  - 実施時期：2021年12月1日（水）～12月23日（木）
  - 有効回答数：40機関（新規参入機関：7機関）
- **2020年度調査**
  - 実施時期：2020年11月30日（月）～12月25日（金）
  - 有効回答数：40機関（新規参入機関：10機関）
- **2019年度調査**
  - 実施時期：2019年12月2日（月）～12月27日（金）
  - 有効回答数：40機関（新規参入機関：4機関）
- **2018年度調査**
  - 実施時期：2019年1月7日（月）～2月8日（金）
  - 有効回答数：43機関（新規参入機関：18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）
  - 有効回答数：31機関（新規参入機関：13機関）
- **2016年度調査**
  - 実施時期：2017年1月18日（水）～2月24日（金）
  - 有効回答数：28機関

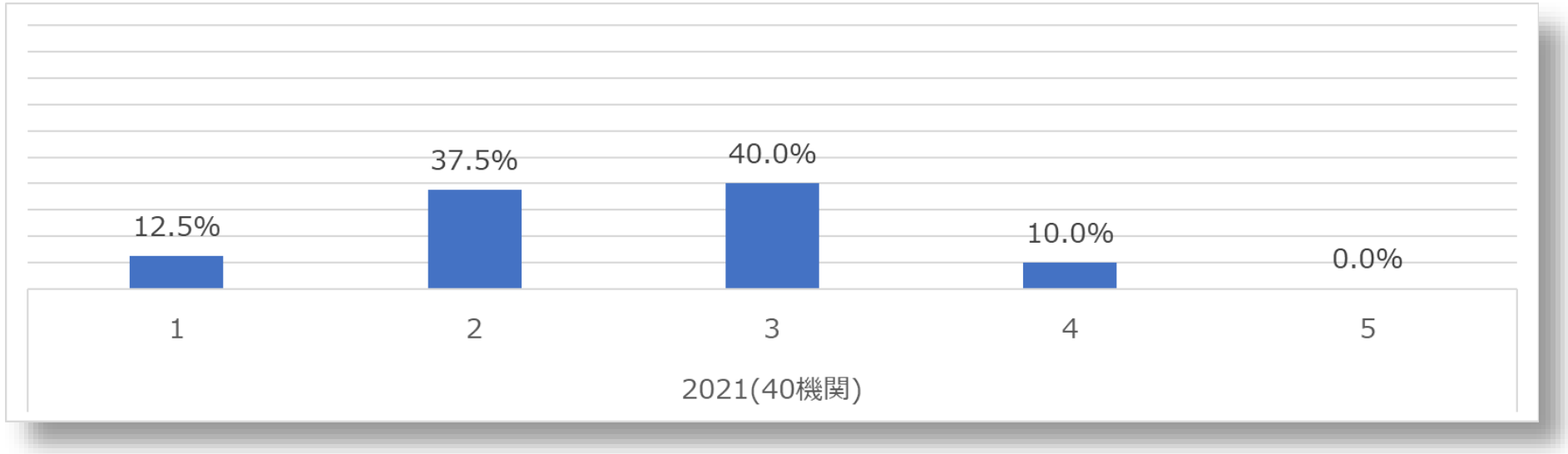
今回も昨年度同様に年末に実施

2021年度総合ステージ分布図

HIROSHIMA UNIVERSITY

- **有効回答：40機関**
  - 新規参入機関：7機関

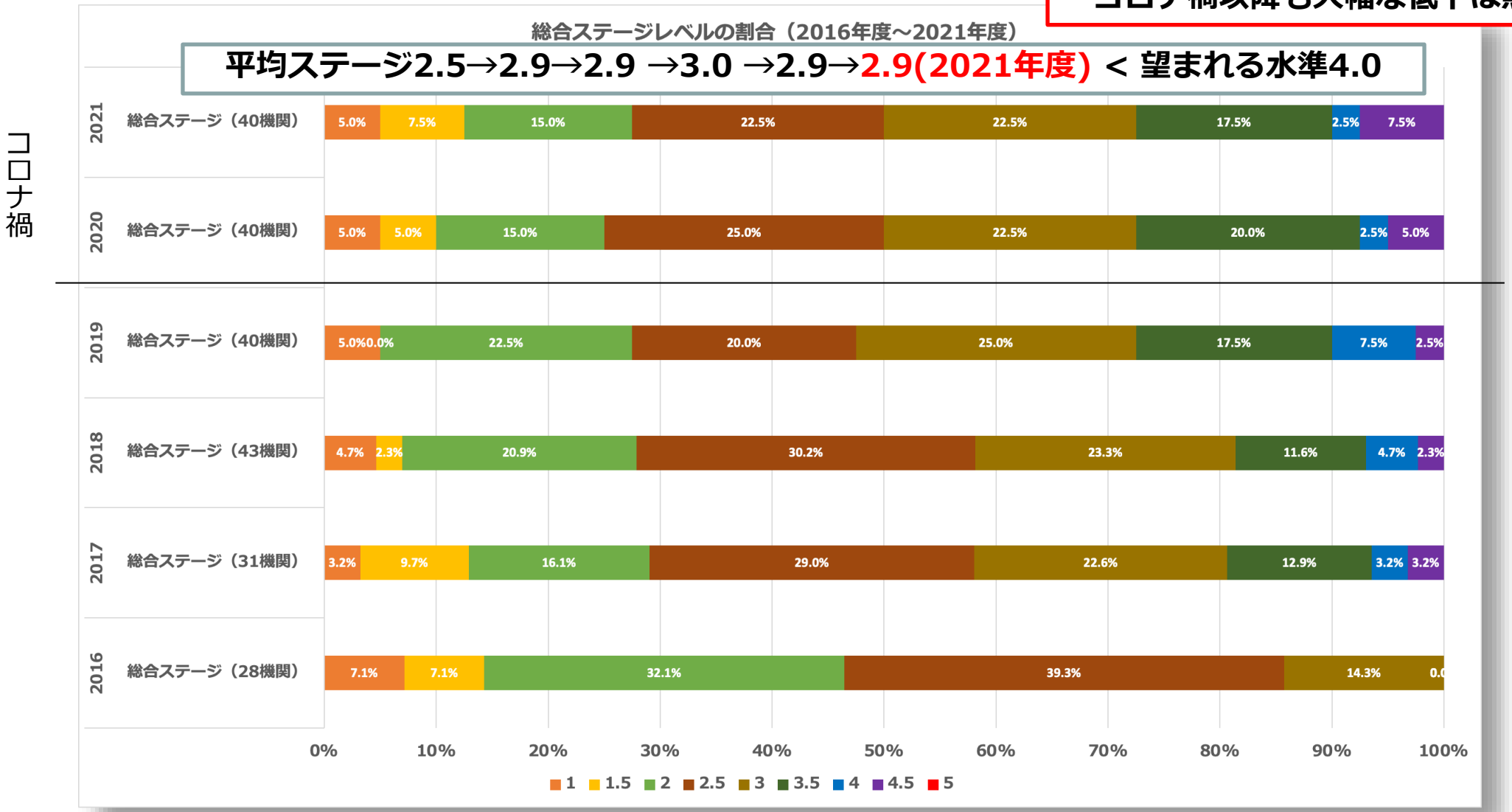
平均ステージ：2.9
<望まれる水準4.0>



年度別総合ステージ分布図

HIROSHIMA UNIVERSITY

高度組織（ステージ4）以上は10.0%
標準組織（ステージ3）以上は50%
ガバナンスの成熟度は向上・維持
コロナ禍以降も大幅な低下は無い模様

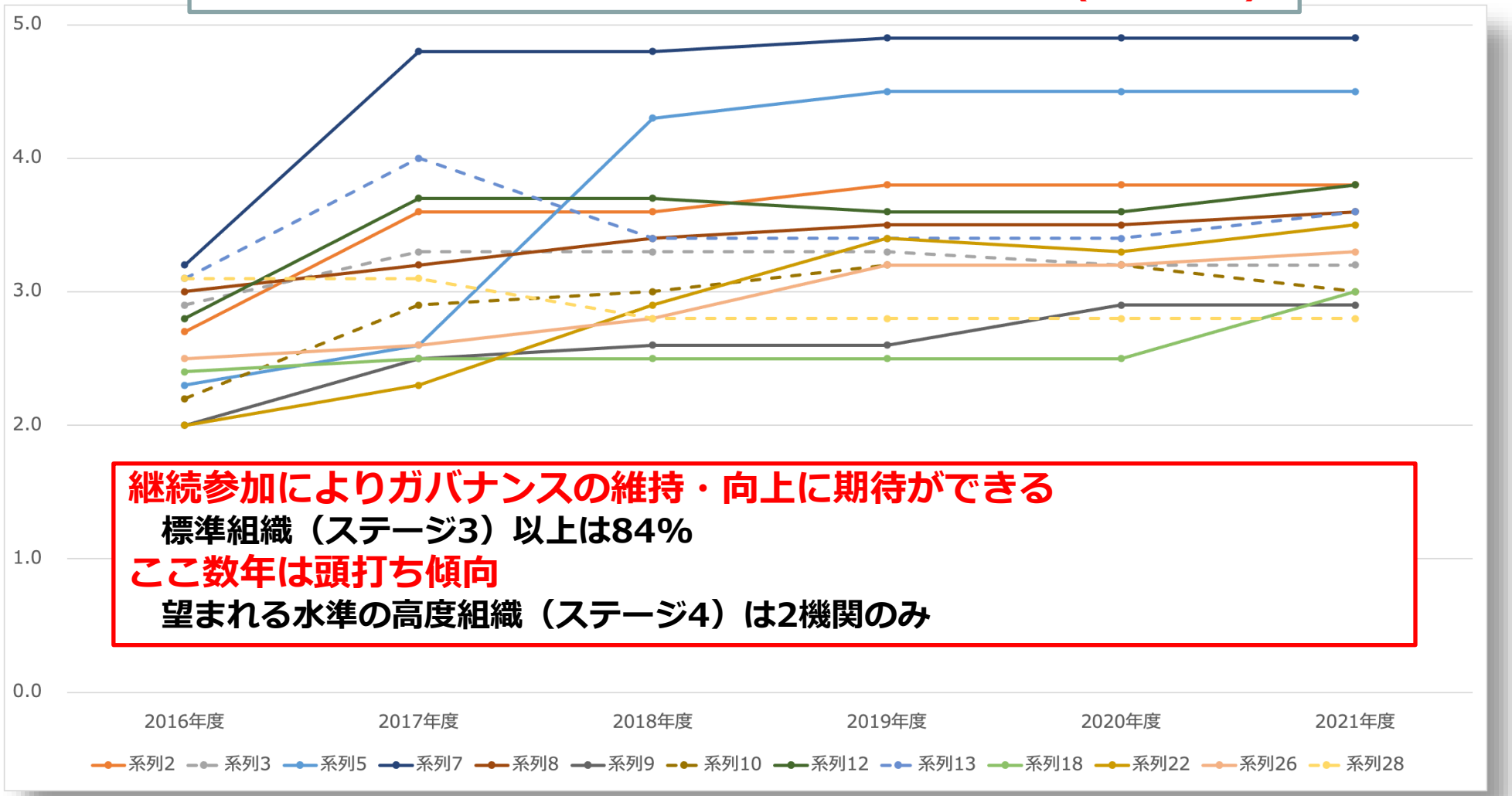


6年継続参加機関年度別総合ステージ分布図

HIROSHIMA UNIVERSITY

- 6年間で維持・向上傾向にある機関は69%(9/13機関)

13機関平均ステージ2.6→3.2→3.3 →3.4 →3.4 →3.5(2021年度)



継続参加によりガバナンスの維持・向上に期待ができる

標準組織（ステージ3）以上は84%

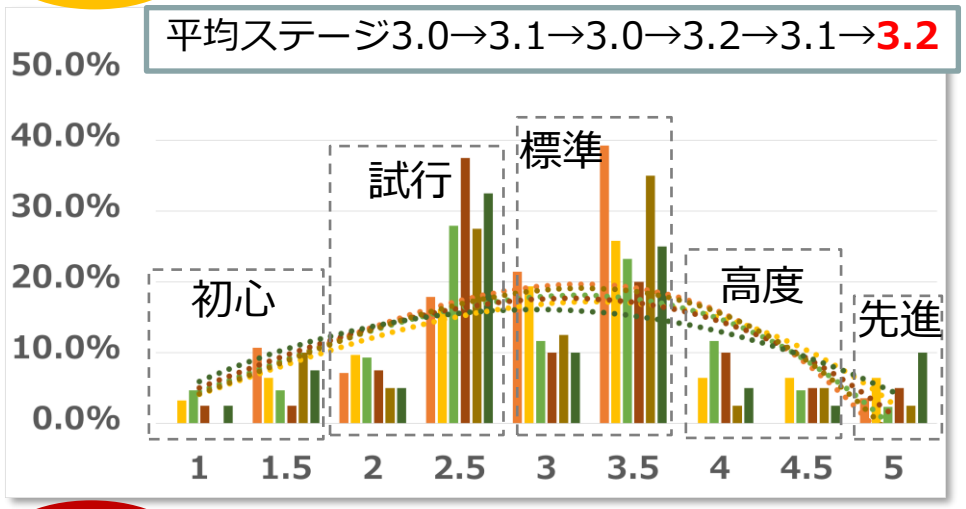
ここ数年は頭打ち傾向

望まれる水準の高度組織（ステージ4）は2機関のみ

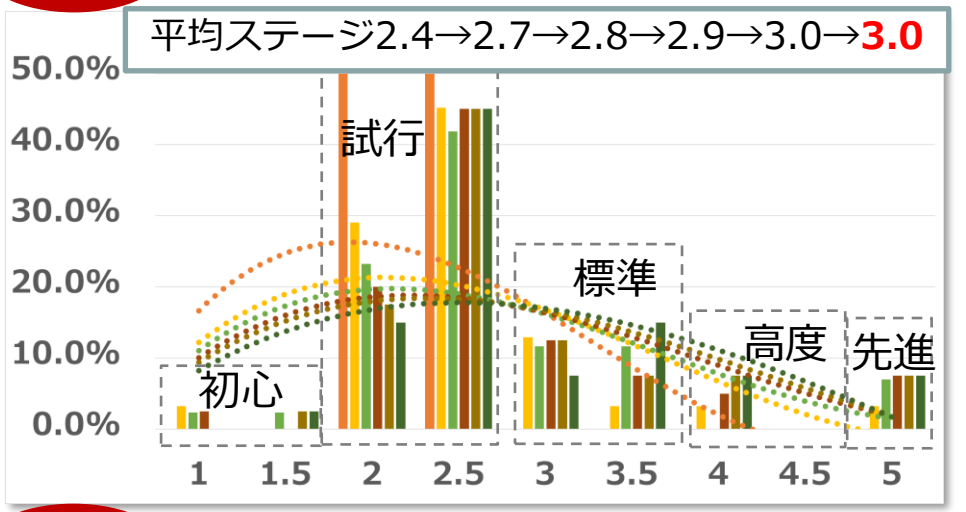
年度・評価基準別総合ステージ分布図

HIROSHIMA UNIVERSITY

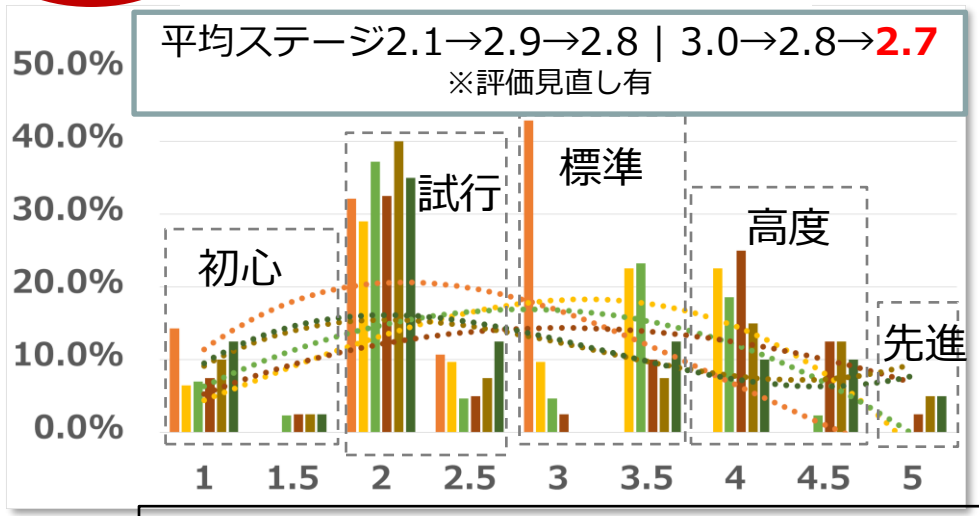
導入 適応力総合ステージ分布



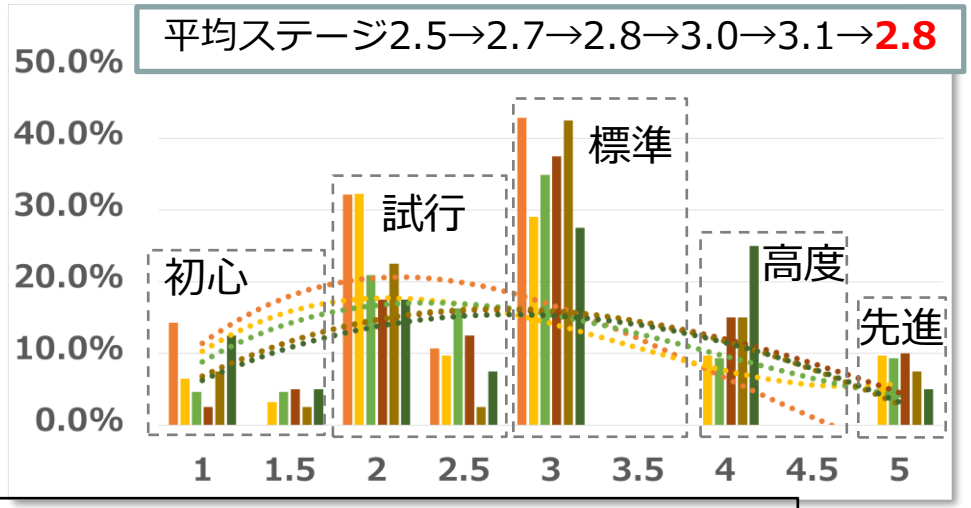
運用 管理力総合ステージ分布



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

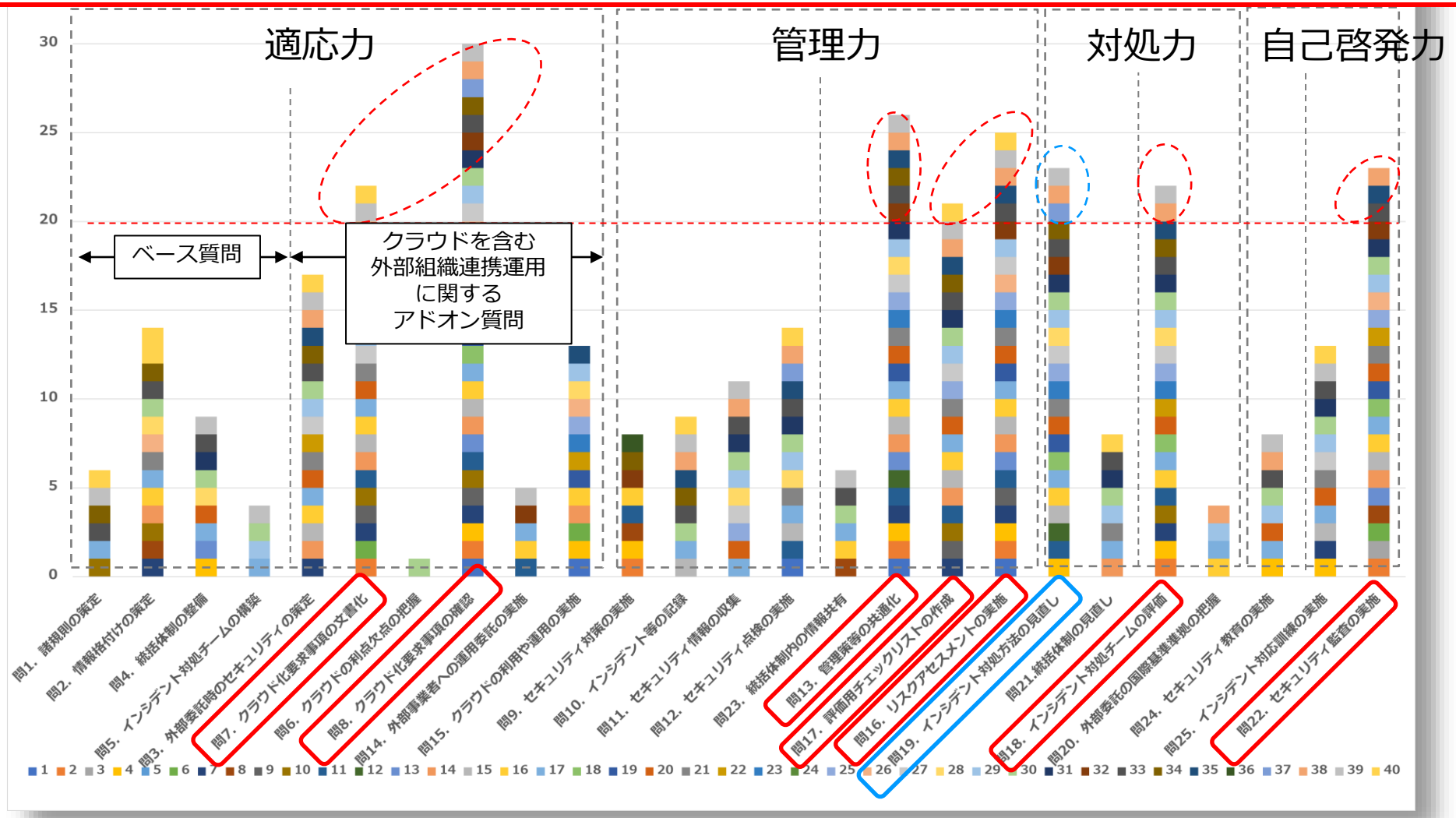


質問別指摘数分布図(2021年度40機関)

HIROSHIMA UNIVERSITY

近年傾向は同じ

- **クラウドを含む外部組織連携時の評価に関連する質問の指摘が多い傾向**
  - 導入前のクラウドに対する評価と、自組織のセキュリティ管理に対する評価（リスクアセスメントやセキュリティ監査等）の未実施
  - 2021年度は新たに**インシデント対処に関する指摘**も増えてきた
- **ISMS的な観点では定期的な評価は重要なファクター**



設問別平均ステージワーストランキング

HIROSHIMA UNIVERSITY

- **昨年から引き続き、問19. インシデント対処方法の見直し、問22セキュリティ監査の実施の平均ステージが最も低い傾向**
  - **2021年度はセキュリティ教育、インシデント等の記録の平均ステージが低下**

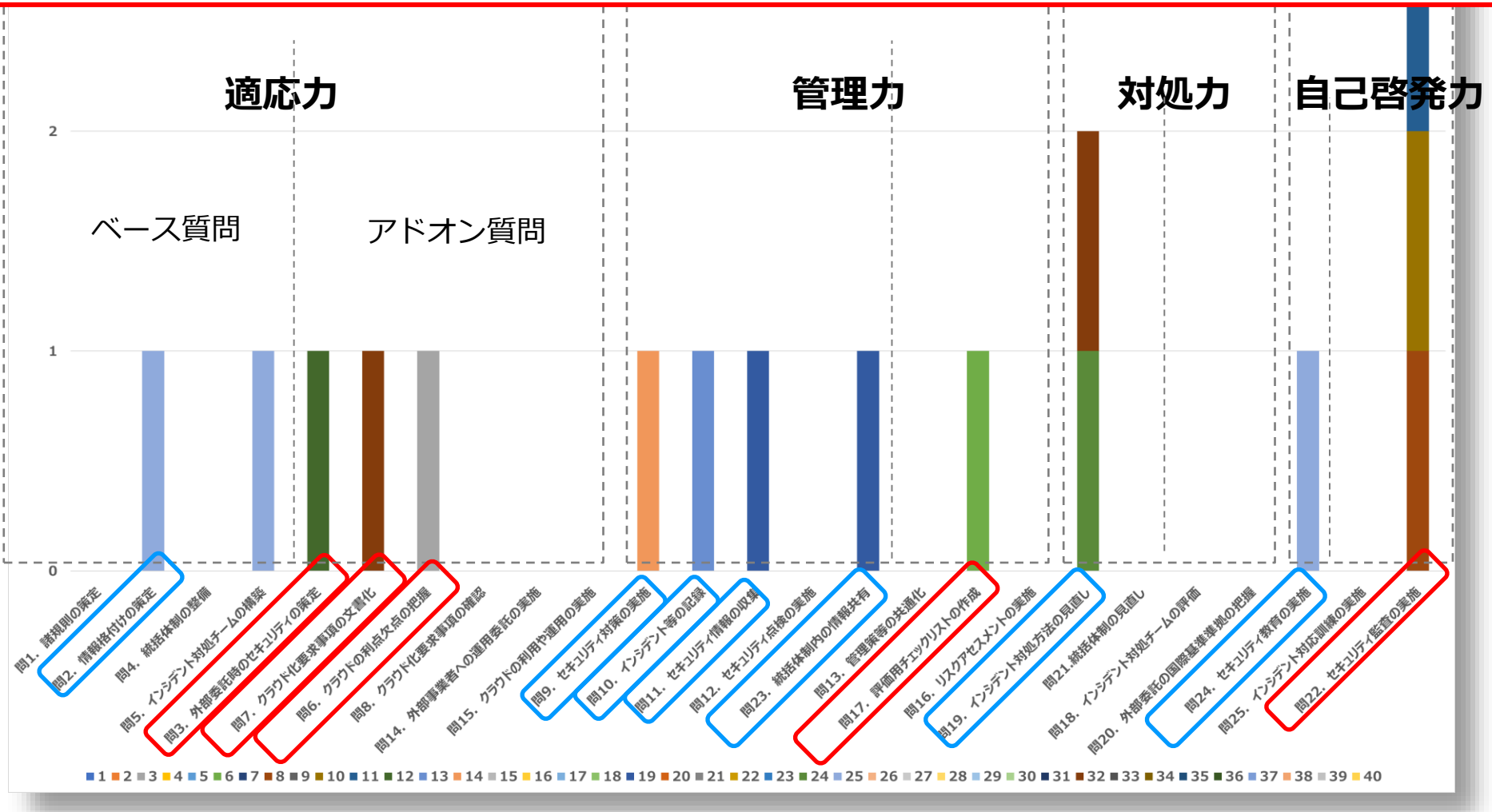
ワースト順位（昨年度順位）	設問概要	平均ステージ	最低限望まれる水準（ステージ3）に該当する評価基準	組織間連携で望まれる水準（ステージ4以上）に該当する評価基準
1（1）	問19. インシデント対処方法の見直し	2.0	対処力	
2（2）	問2. 情報格付けの策定	2.5	適応力	
3（4）	問25. インシデント対応訓練の実施	2.5	自己啓発力	
4（3）	問12. セキュリティ点検の実施	2.6	管理力	
4（10）	問24. セキュリティ教育の実施	2.6	自己啓発力	
5（5）	問4. 統括体制の整備	2.7	適応力	
5（5）	問11. セキュリティ情報の収集	2.7	管理力	
5（5）	問21.統括体制の見直し	2.7	対処力	
5（12）	問10. インシデント等の記録	2.7	管理力	
10（5）	問5. インシデント対処チームの構築	2.8	適応力	
10（5）	問23. 統括体制内の情報共有	2.8	管理力	
10（10）	問9. セキュリティ対策の実施	2.8	管理力	
10（13）	問1. 諸規則の策定	2.8	適応力	
CL1（1）	問22. セキュリティ監査の実施	3.2		自己啓発力
CL2（2）	問13. 管理策等の共通化	3.4		管理力
CL2（4）	問8. クラウド化要求事項の確認	3.4		適応力
CL4（2）	問7. クラウド化要求事項の文書化	3.5		適応力
CL4（4）	問17. 評価用チェックリストの作成	3.5		管理力
CL4（6）	問16. リスクアセスメントの実施	3.5		管理力
CL4（7）	問18. インシデント対処チームの評価	3.5		対処力
CL8（7）	問3. 外部委託時のセキュリティの策定	3.6		適応力
CL9（9）	問20. 外部委託の国際基準準拠の把握	4.2		対処力
CL9（11）	問6. クラウドの利点欠点の把握	4.2		適応力
CL11（9）	問15. クラウドの利用や運用の実施	4.3		適応力
CL12（12）	問14. 外部事業者への運用委託の実施	4.7		適応力

質問別改善数分布図(前年度継続参加の32機関)

HIROSHIMA UNIVERSITY

- **ステージが高い機関は改善へのサイクルが適切に動いている傾向にある**
  - 改善傾向の12機関の平均総合ステージは3.4
    - 前年度は改善傾向の8機関の平均総合ステージは3.2
- **ステージが低いと判定された機関は対応しやすいベース質問に対して取り掛かると改善しやすい**
  - 情報格付けの整備やインシデント対処方法の見直しなど

Goodポイントの評価は2019年度から開始



考察

- **セキュリティポリシーを遵守し望まれている水準を目指すことが重要**
  - 組織の現状を正しく把握するためのアセスメント（例えば本調査結果の精査）が必要
  - クラウドに対する自組織の要求事項の確立や確認が必要
    - クラウドを導入する上で自組織共通の要求事項を定め、満たすことを確認することは、クラウドに対するセキュリティの不安を解消する一つの取り組みになる
  - 自組織の情報セキュリティ管理において定期的な評価の確立や実施が必要
    - ISMSの観点で言えば、評価（PDCAのCheck）が不十分な機関が多い
    - 定期的なリスクアセスメントやセキュリティ監査は自組織のセキュリティ管理の脆弱性を理解する良いきっかけとなる
    - インシデント対応組織のそれぞれの機能と役割も見直すきっかけになる

⇒ 既存のチェックリストをうまく活用することが改善の近道！？

インシデント対応関連のチェックリスト

HIROSHIMA UNIVERSITY

- **セキュリティ対応組織成熟度セルフチェックシートV.2.2版**
  - 日本セキュリティオペレーション事業者協議会（ISOG-J）
  - 4つのセキュリティ組織（SOC/CSIRT）パターンと計54個の質問に回答すると、セキュリティ組織の強みと弱みや9つの業務カテゴリー別に成熟度の把握が可能

あなたのセキュリティ対応組織における"**機能別**"成熟度

201X/YY/ZZ

現状の組織（ハイブリッドパターン）における機能別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリティ対応において有効に働いている機能と、改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定にお役立てください。

機能	成熟度
A. セキュリティ対応組織運営	**4** /5
B. リアルタイムアナリシス（即時分析）	**3** /5
C. ディープアナリシス（深掘分析）	**2** /5
D. インシデント対応	**4** /5
E. セキュリティ対応状況の診断と評価	**2** /5
F. 脅威情報の収集および評価と分析	**3** /5
G. セキュリティ対応システム運用	**3** /5
H. 内部統制/内部不正対応支援	**3** /5
I. 外部組織との積極的連携	**2** /5

現状のセキュリティ対応組織の**強み**

A. セキュリティ対応組織運営
セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応
分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の**弱み**

C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

E. セキュリティ対応状況の診断と評価
脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図りにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

v0.5

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

クラウド関連のチェックリスト

学認クラウド導入支援サービス チェックリスト

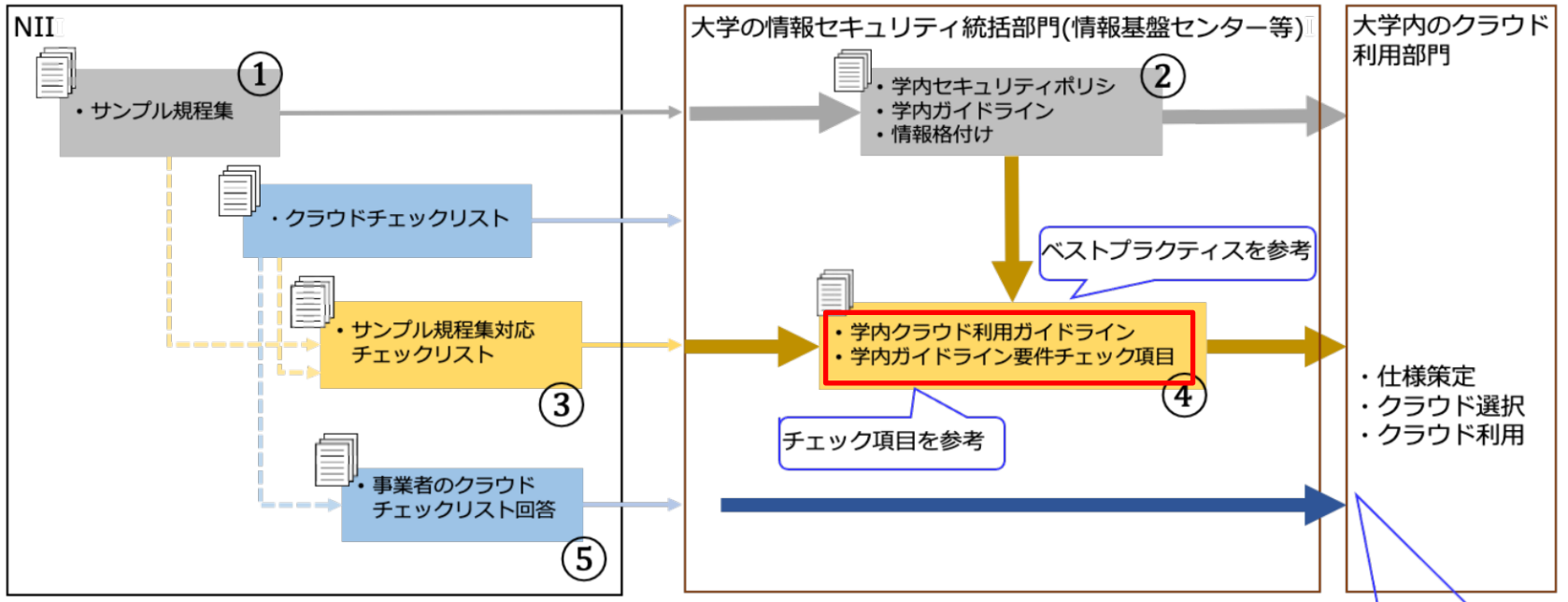
https://cloud.gakunin.jp/foracademy/

広島大学クラウドサービス利用 ガイドライン・チェックリスト

https://www.media.hiroshima-u.ac.jp/aboutus/cloudguide/

サンプル規定集対応チェックリストVer1.1

【利用イメージ】

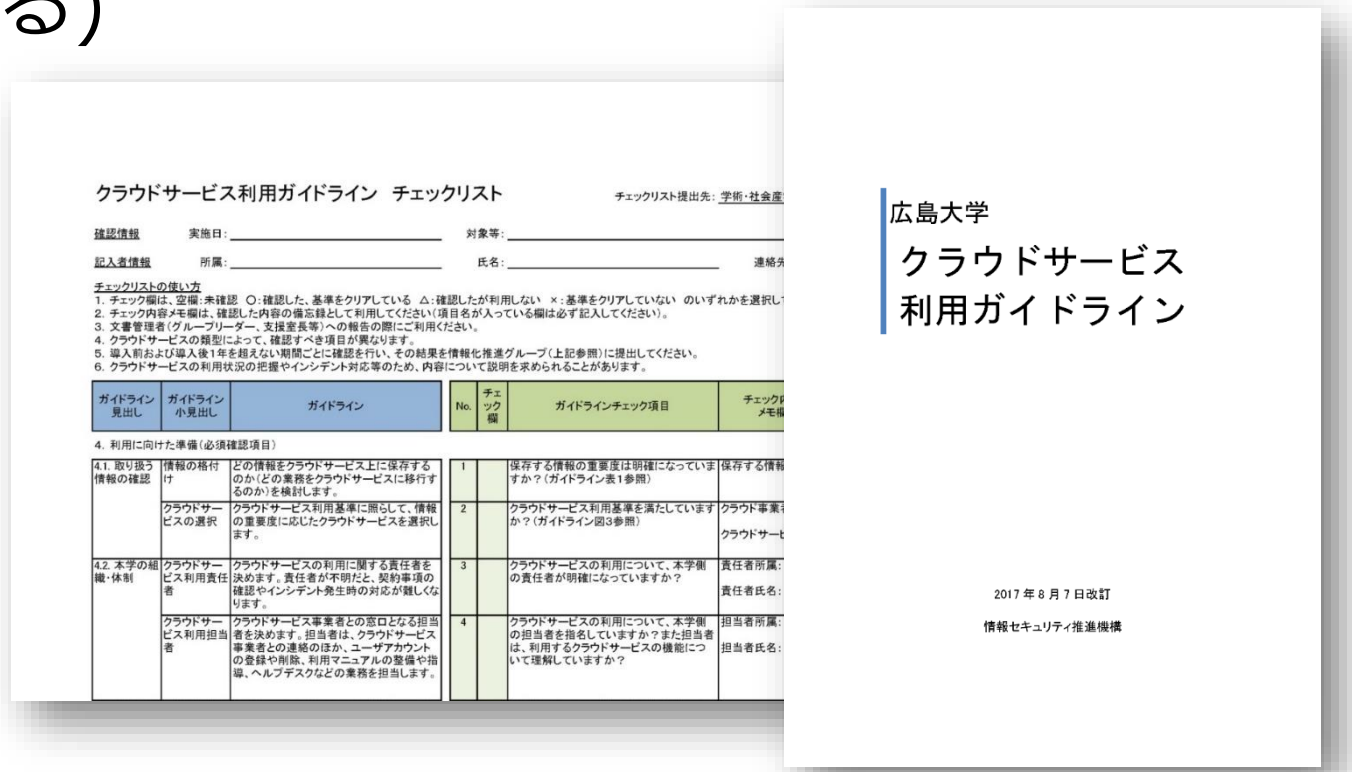


① サンプル規程集
② ①を参考に学内のセキュリティポリシ等を策定
③ サンプル規程集対応チェックリスト
④ ③を参考にして、②に基づいて学内のクラウド利用ガイドライン等を策定
⑤ 事業者のチェックリスト回答
(学認クラウド導入支援サービス参加機関の場合、参照可能)

https://cloud.gakunin.jp/dist/pdf/sp-sample-2019-ChecklistV11.pdf

広島大学クラウドサービス利用ガイドライン・チェックリスト

- **第三版(2017(平成29)年8月7日改訂)**
  - ガイドラインチェック項目：46個
  - 詳細チェック項目：88個　　(それぞれ最大、サービス類型により異なる)


クラウドサービス利用ガイドライン　チェックリスト

チェックリスト提出先：学術・社会産

確認情報　実施日：　対象等：

記入者情報　所属：　氏名：　連絡先

チェックリストの使い方
1. チェック欄は、空欄：未確認　○：確認した、基準をクリアしている　△：確認したが利用しない　×：基準をクリアしていない　のいずれかを選択して
2. チェック内容メモ欄は、確認した内容の備忘録として利用してください（項目名が入っている欄は必ず記入してください）。
3. 文書管理者（グループリーダー、支援室長等）への報告の際にご利用ください。
4. クラウドサービスの類型によって、確認すべき項目が異なります。
5. 導入前および導入後1年を超えない期間ごとに確認を行い、その結果を情報化推進グループ（上記参照）に提出してください。
6. クラウドサービスの利用状況の把握やインシデント対応等のため、内容について説明を求められることがあります。

ガイドライン見出し	ガイドライン小見出し	ガイドライン	No.	チェック欄	ガイドラインチェック項目	チェックメモ欄
4. 利用に向けた準備（必須確認項目）						
4.1. 取り扱う情報の確認	情報の格付け	どの情報をクラウドサービス上に保存するのか（どの業務をクラウドサービスに移行するのか）を検討します。	1		保存する情報の重要度は明確になっていますか？（ガイドライン表1参照）	保存する情
	クラウドサービスの選択	クラウドサービス利用基準に照らして、情報の重要度に応じたクラウドサービスを選択します。	2		クラウドサービス利用基準を満たしていますか？（ガイドライン図3参照）	クラウド事業 クラウドサー
4.2. 本学の組織・体制	クラウドサービス利用責任者	クラウドサービスの利用に関する責任者を決めます。責任者が不明だと、契約事項の確認やインシデント発生時の対応が難しくなります。	3		クラウドサービスの利用について、本学側の責任者が明確になっていますか？	責任者所属: 責任者氏名:
	クラウドサービス利用担当者	クラウドサービス事業者との窓口となる担当者を決めます。担当者は、クラウドサービス事業者との連絡のほか、ユーザアカウントの登録や削除、利用マニュアルの整備や指導、ヘルプデスクなどの業務を担当します。	4		クラウドサービスの利用について、本学側の担当者を指名していますか？また担当者は、利用するクラウドサービスの機能について理解していますか？	担当者所属: 担当者氏名:

広島大学
クラウドサービス
利用ガイドライン

2017 年 8 月 7 日改訂

情報セキュリティ推進機構

ENISA「クラウドコンピューティング情報セキュリティに関わる利点、リスクおよび推奨事項」*1をカバーできていることを確認済み

*1:ISMSクラウドセキュリティ認証の附属書Bに参考文献として記載されている

https://www2.media.hiroshima-u.ac.jp/public/aboutus/cloudguide/cloud-guideline-20170807.pdf

広島大学チェックリストの活用事例

HIROSHIMA UNIVERSITY

クラウドサービス導入前

クラウドサービス毎にチェックリストで要求事項を確認

→

仕様策定

クラウド選択

クラウド導入

→

サービス運用

クラウドサービス導入後

リスクアセスメント時にも活用

サービス運用管理

→

年1回(年末)クラウドサービス毎にチェックリストで要求事項を再確認

→

リスクの洗い出し

リスク対応

ISMSクラウドセキュリティ認証を取得・維持している

2021年度事後アンケート結果

HIROSHIMA UNIVERSITY

事後アンケート概要

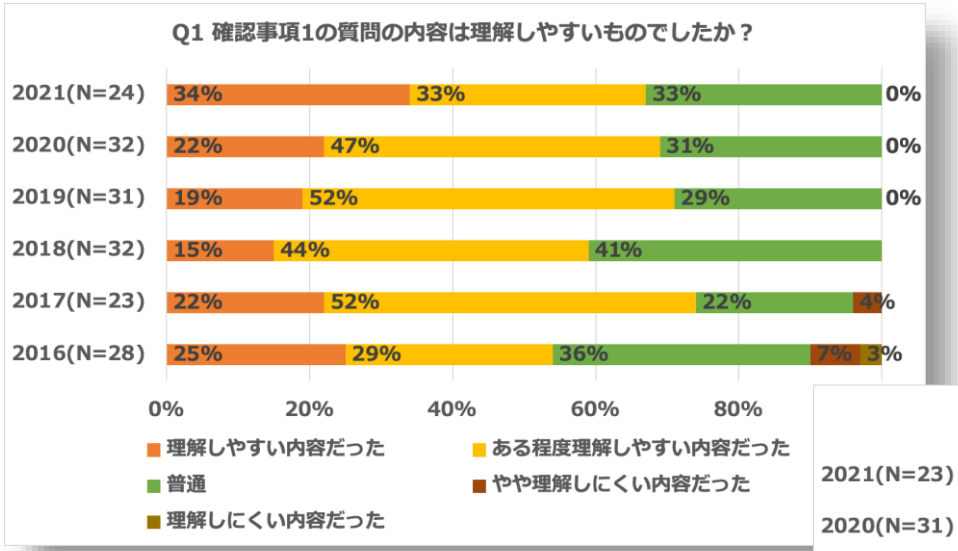
- **内容：**
  - 質問1-3、個別報告書、取り組みに対する評価・意見を把握する内容
- **出題形式：**
  - 四者択一＋自由記述（理由、意見など）
- **質問数：**
  - 8問
- **回答条件：**
  - 任意
- **有効回答率：**
  - 60%（24／40機関）
    - 2020：80%（32 ／ 40機関、2019：77%（31 ／ 40機関）、
      2018：74%(32／43機関)、2017：74%(23／31機関)、2016：100%(28／28機関)

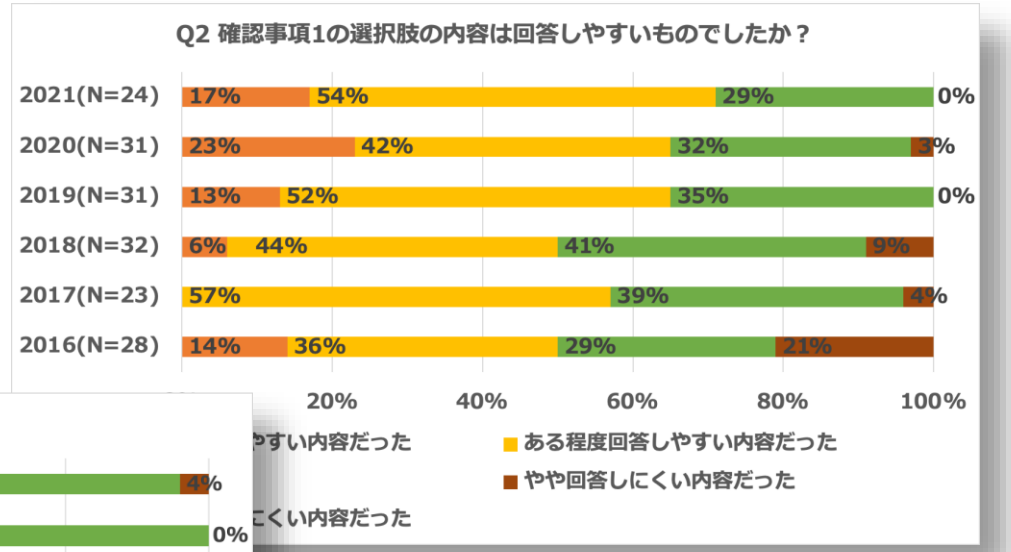
質問1、報告書、取り組みに対する評価の内容に限定し紹介

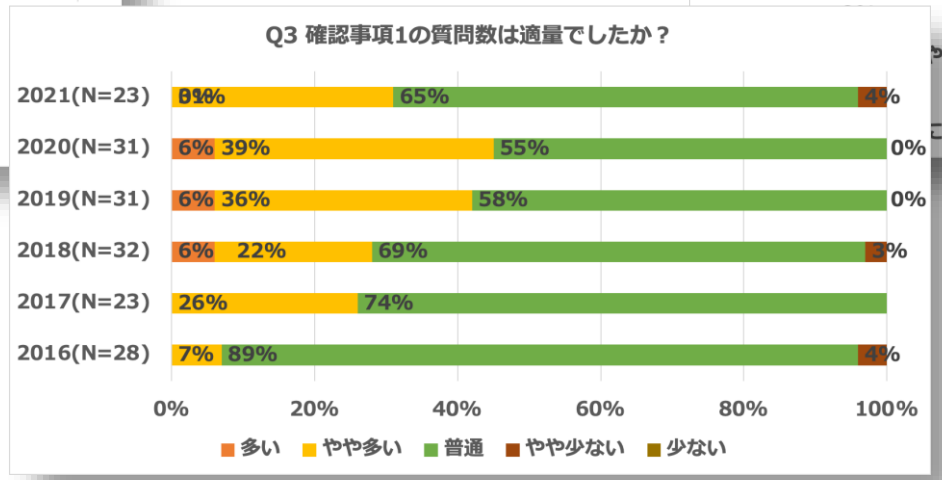
質問1の内容・選択肢は理解しやすいものでしたか？
質問数は適量でしたか？

HIROSHIMA UNIVERSITY

- **質問の内容は全体的に理解しやすく、質問数も適量だった模様**
  - 内容は理解しやすいが67%（理解しやすい：34%、ある程度理解しやすい：33%）
  - 選択肢は理解しやすいは71%（理解しやすい：17%、ある程度理解しやすい：54%）
  - 質問数は普通が65%

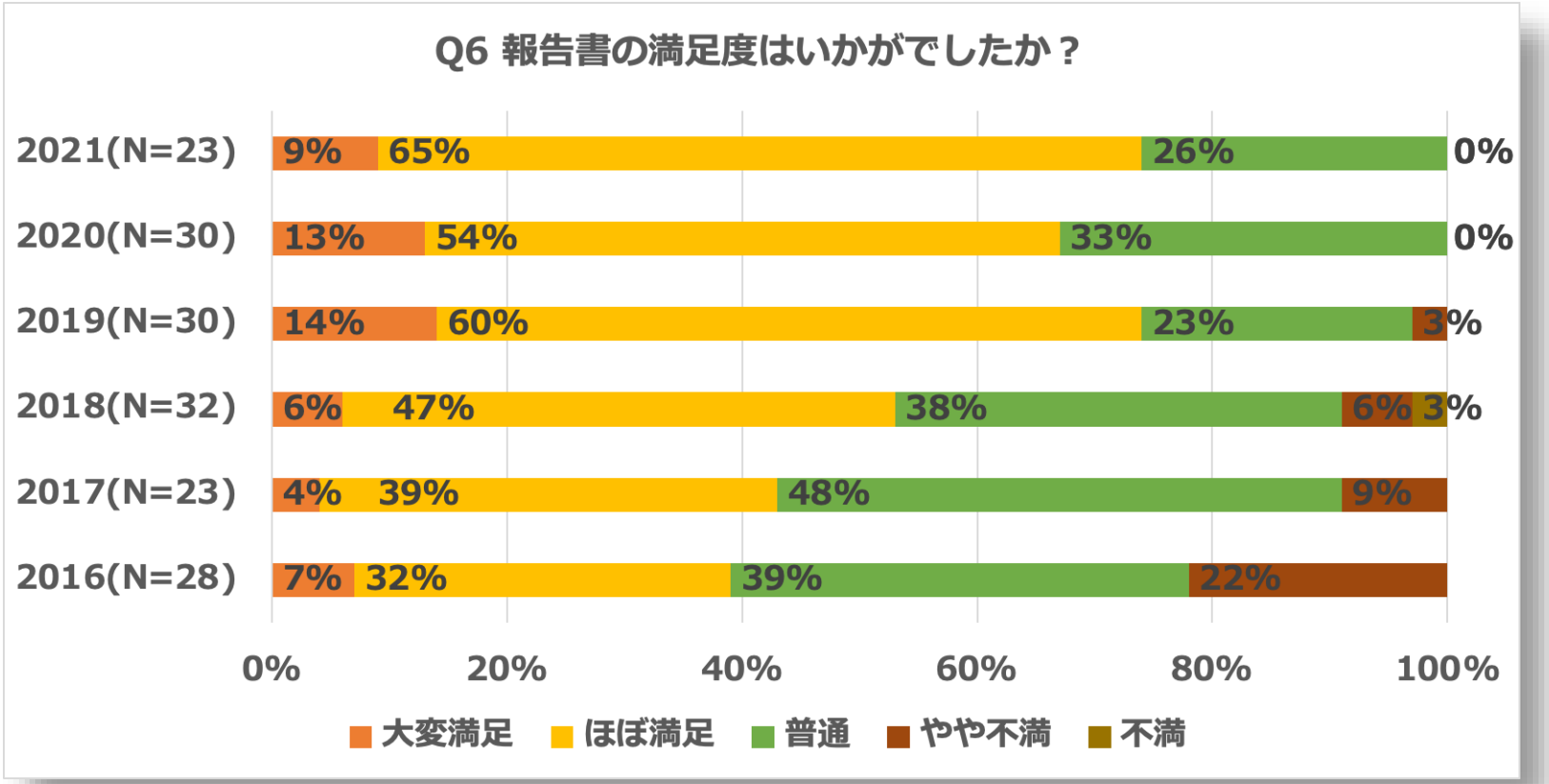






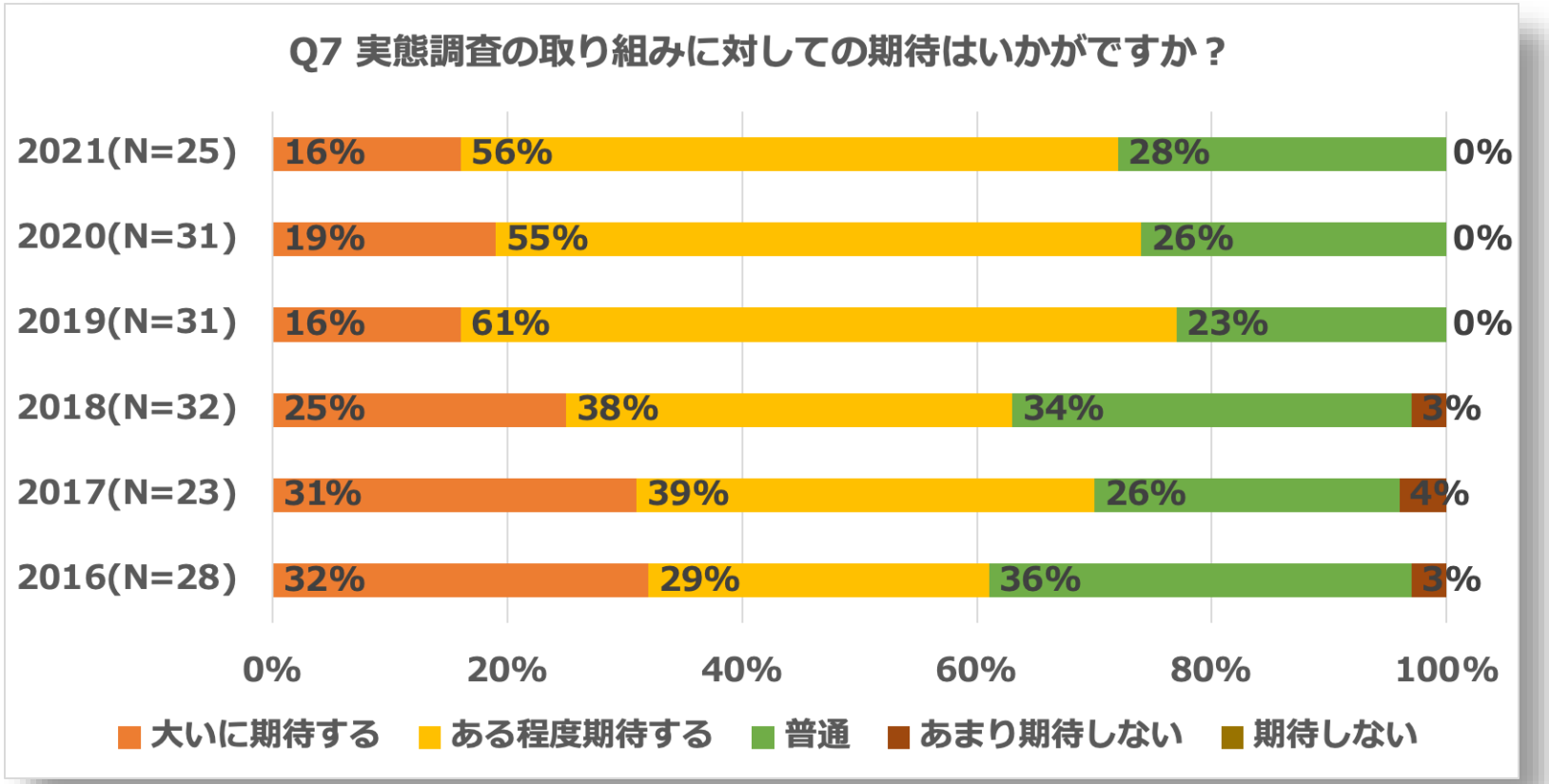
報告書の満足度はいかがでしたか？

- **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：9%、ほぼ満足65%）
  - 総合ステージの評点に関しては実態を定量的かつ客観的に表しているというコメントが多い



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72%（大いに期待する：16%、ある程度期待する：56%）
  - 継続希望のコメントが多数あり



まとめ

- **2016年度から2021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
  - 自組織の情報セキュリティ管理に対する組織的な評価が十分にできておらず、既存のチェックリストを活用することで評価上昇の余地がある
- **今後の課題**
  - フィードバック情報の充実
  - 協力機関の増加
  - いつでも自己チェックが可能なWebサイトの提供
  - 高度組織（ステージ4）の評価結果の頭打ち傾向に対する評価基準の検討