

2020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

－ 5年間の評価結果から見える実情 －

渡邊英伸, 西村浩二

広島大学 情報メディア教育研究センター



- 2016年度から2020年度の5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



● 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)
 - 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：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

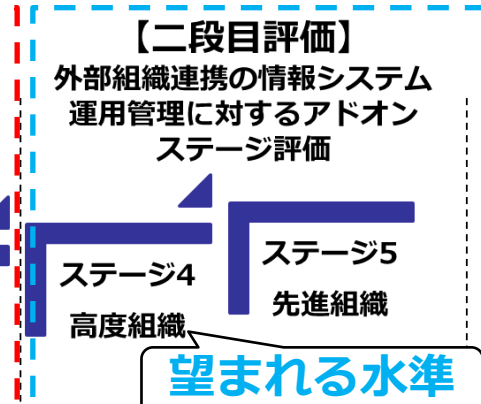
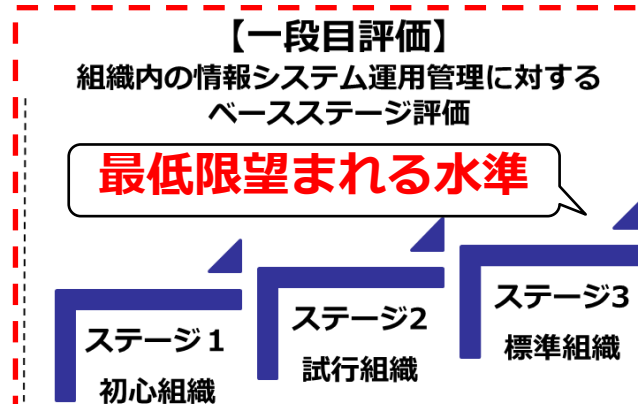
● 質問3

- 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：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

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

適応力	無	低い	普通	高い	非常に高い
管理能力	無	低い	普通	高い	非常に高い
対処力	無	低い	普通	高い	非常に高い
自己啓発力	無	低い	普通	高い	非常に高い

組織的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

「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

〇〇大学の評価結果: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

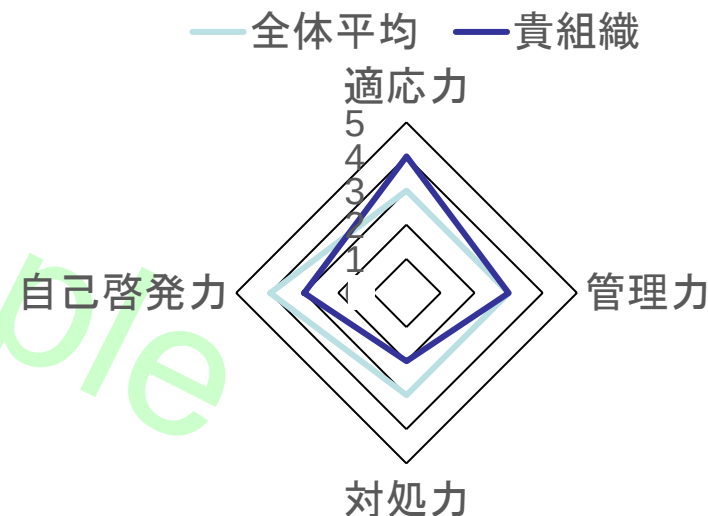
(昨年度:適応力:3.0、管理力:2.0、対処力:2.0、自己啓発力:3.0)

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～2020年度 実態調査結果



- **2020年度調査**

- 実施時期：2020年11月30日（月）～12月25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（新規参入機関：10機関）

今回も昨年度同様に
年末に実施

- **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（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）
- 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（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）
- 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（新規参入機関：13機関）

- **2016年度調査**

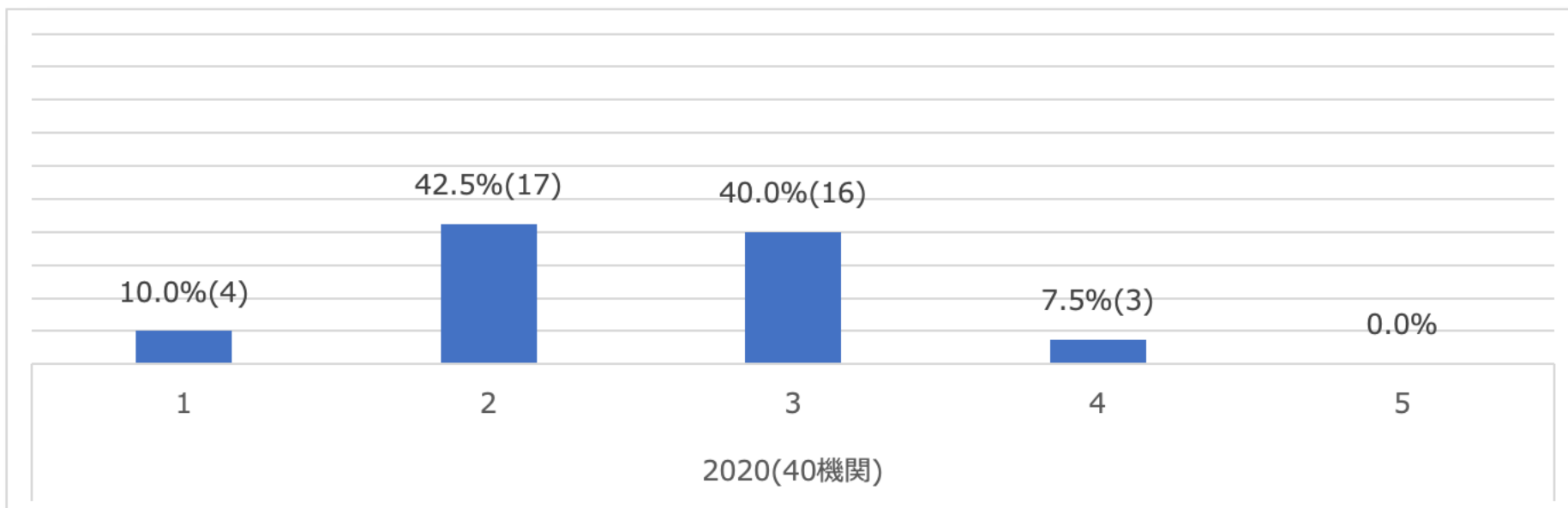
- 実施時期：2017年1月18日（水）～2月24日（金）
- 調査方法：エクセルファイルによるアンケート調査
- 有効回答数：28機関

2020年度総合ステージ分布図



- 有効回答：40機関
 - － 新規参入機関：10機関

平均ステージ：2.9
<望まれる水準4.0>



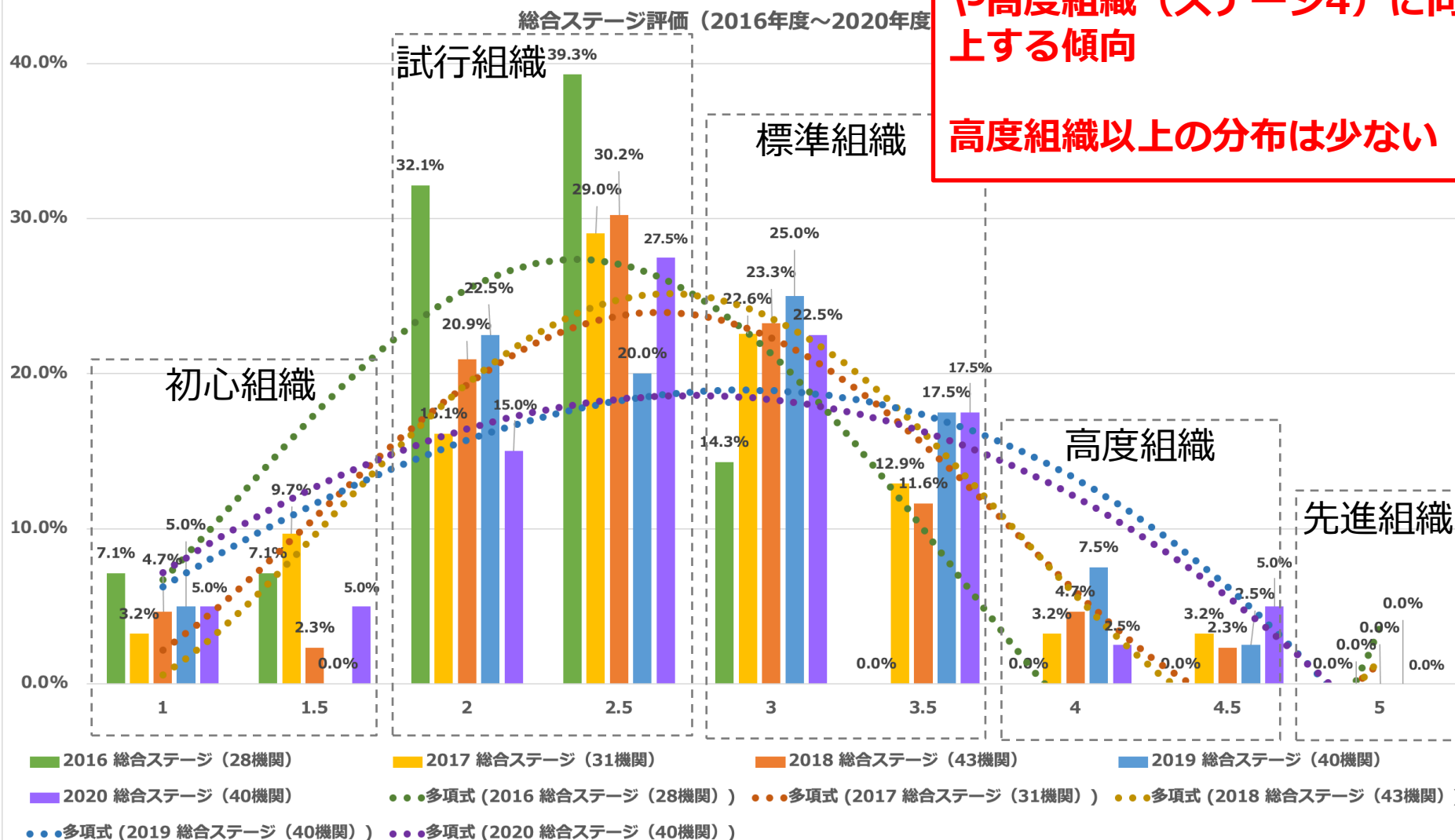
年度別総合ステージ分布図

点線は近似曲線（多項式3次）

平均ステージ2.5→2.9→2.9 →3.0 →**2.9(2020年度)**
 <望まれる水準4.0>

徐々に標準組織（ステージ3）
 や高度組織（ステージ4）に向
 上する傾向

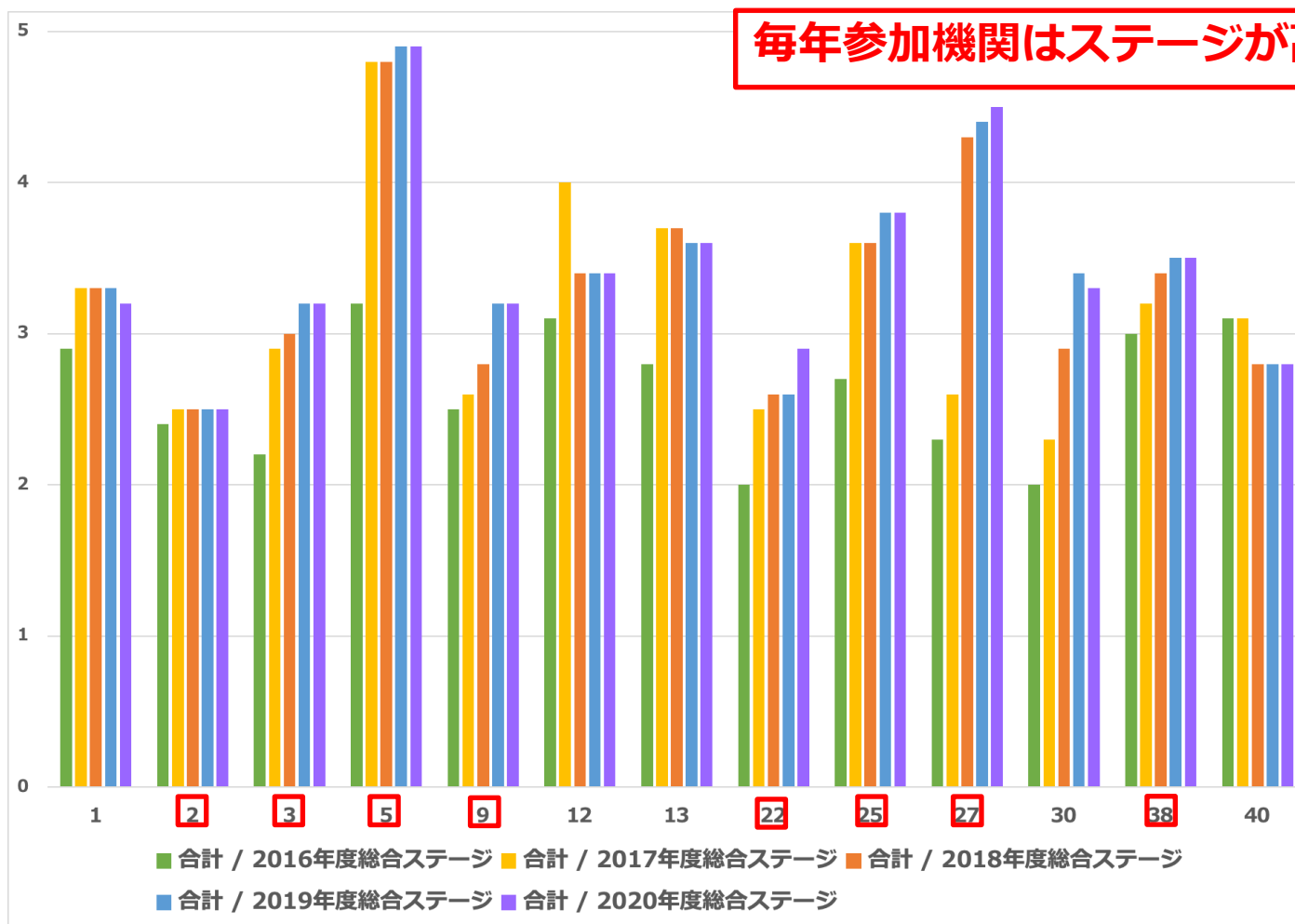
高度組織以上の分布は少ない



5年継続参加13機関年度別総合ステージ分布図

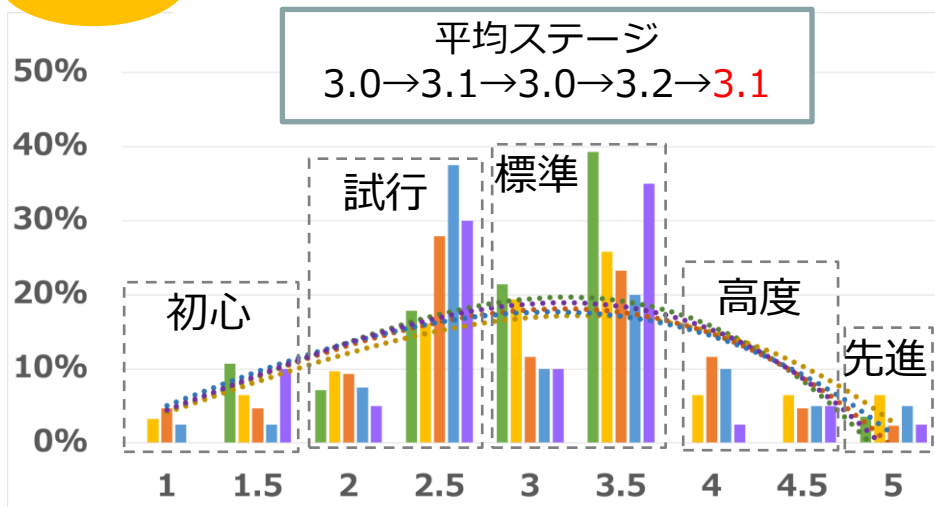
● 5年間で維持・向上傾向にある機関は61%(8/13機関)

－ 13機関平均ステージ2.6→3.2→3.3 →3.4→3.4(2020年度)

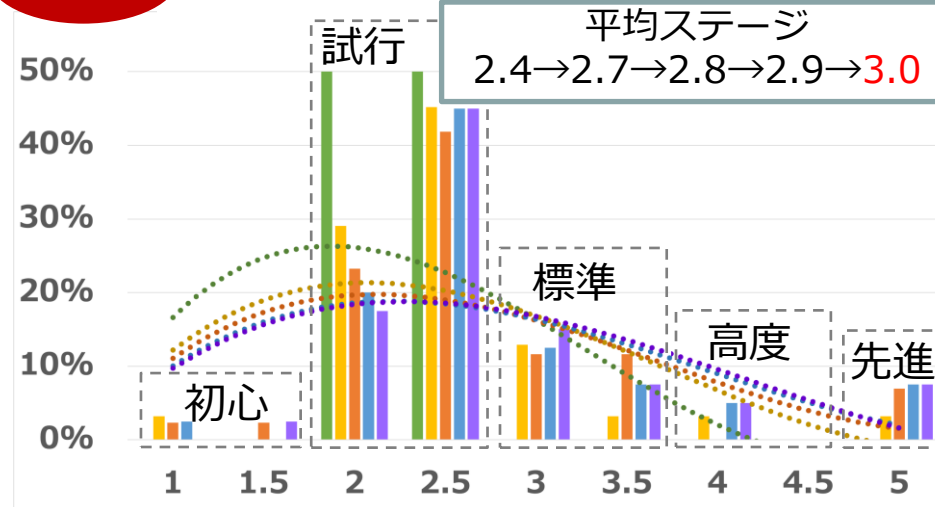


年度・評価基準別総合ステージ分布図

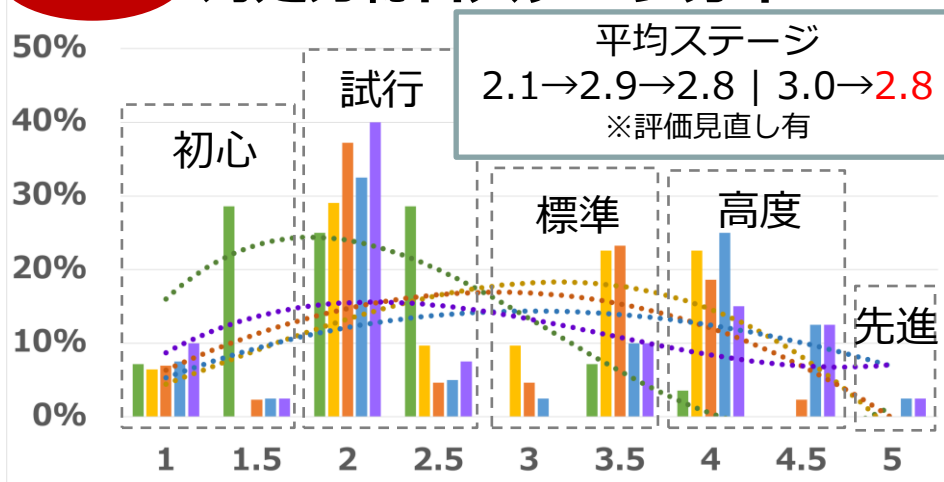
導入 適応力総合ステージ分布



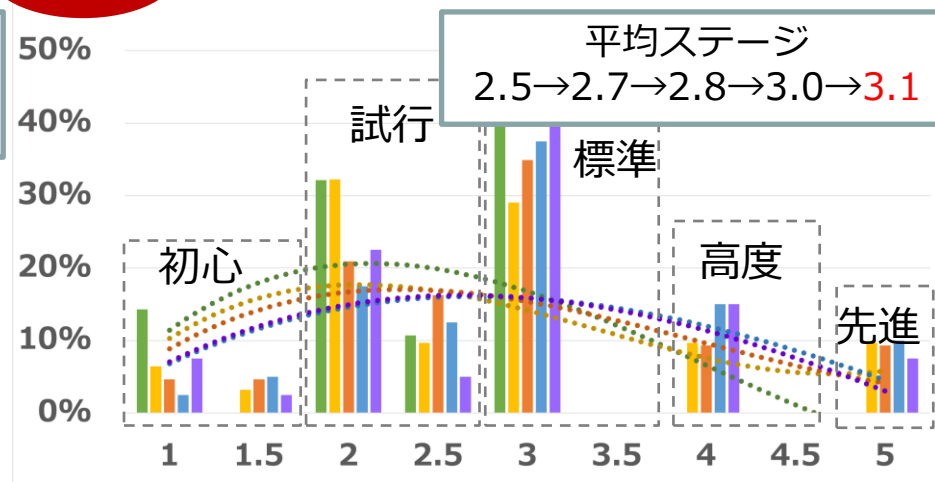
運用 管理力総合ステージ分布



運用 対処力総合ステージ分布



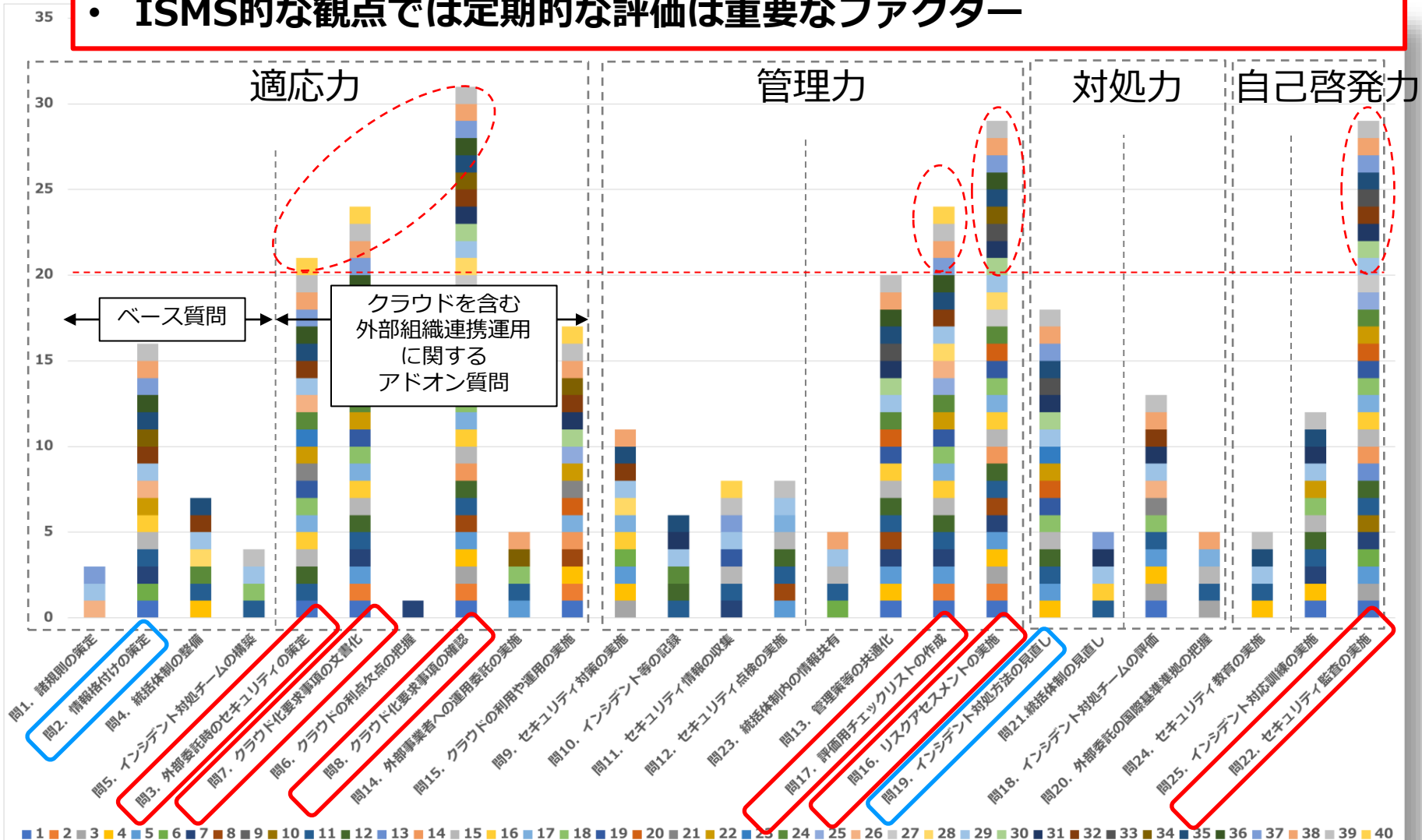
運用 自己啓発力総合ステージ分布



質問別指摘数分布図(2020年度40機関)

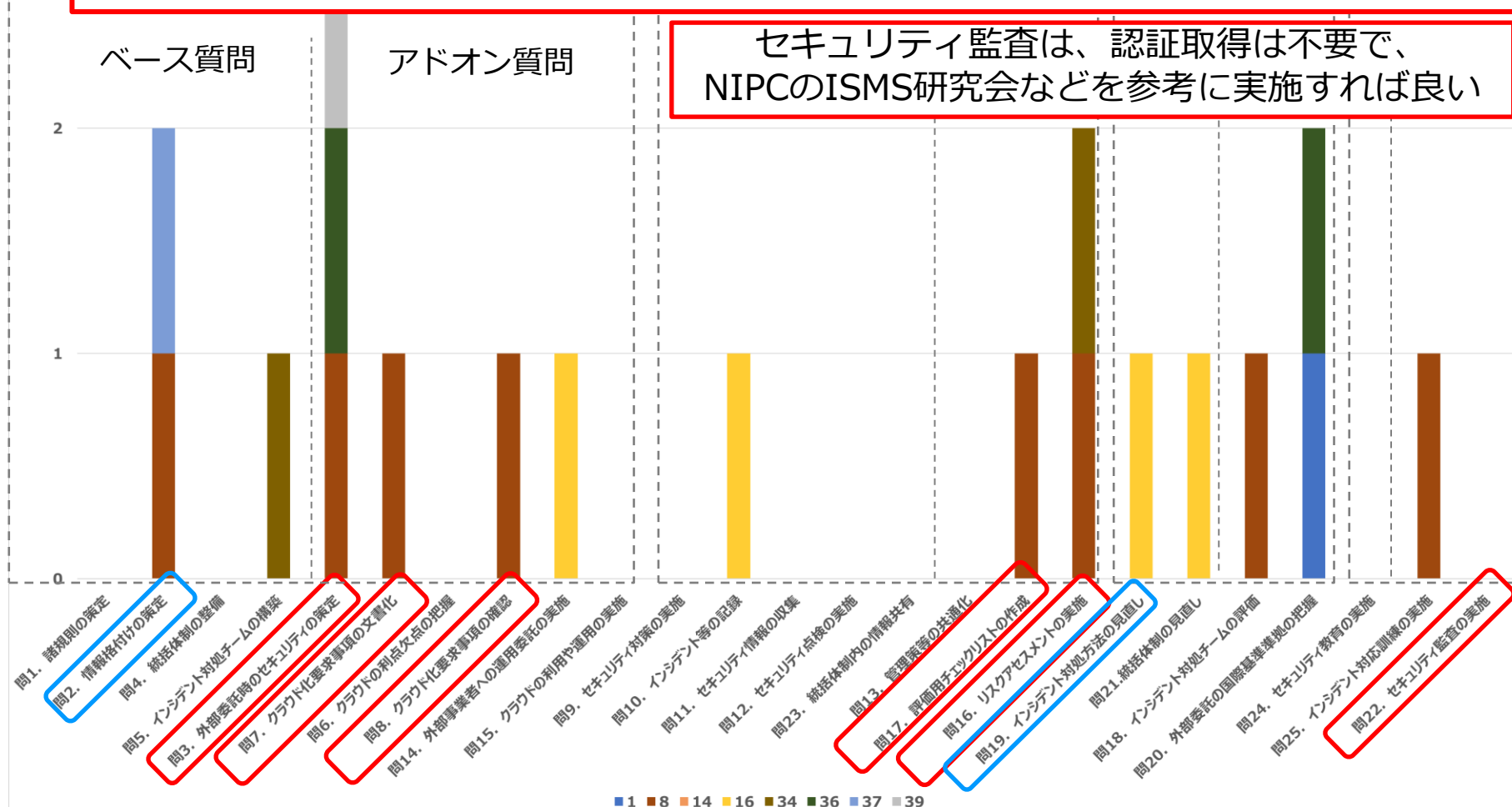
近年傾向は同じ

- クラウドと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
- ISMS的な観点では定期的な評価は重要なファクター



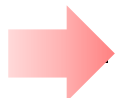
質問別改善数分布図(2019年度継続参加の30機関)

- ・ 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組みやすく改善しやすい
 - ・ 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



- セキュリティポリシーの遵守により**望まれている水準を目指すことが重要**

- 実行可能性の高いセキュリティポリシー（実施手順）の見直しが必要
- 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



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！？

クラウド関連のチェックリスト



HIROSHIMA UNIVERSITY

学認クラウド導入支援サービス チェックリスト



「学認クラウド 導入支援サービス」では、以下のサービスを提供いたします。

クラウド活用セミナー

大学・研究機関の研究者や教職員が抱えている、研究教育活動にどのようにクラウドを活用できるのかといった疑問の解消を目的として定期的にセミナーを実施しています。

→ [これまで実施したセミナーはこちら](#)

チェックリスト・スタートアップガイド

組織の情報基盤としてクラウドの導入を検討または計画している大学・研究機関の研究者や教職員を対象として、クラウドの導入・活用に関わる情報をまとめました。(チェックリストVer.5.0対応)

[スタートアップガイド](#)

[スタートアップガイド\(クラウド関連実務担当者向けダイジェスト版\)](#)

[チェックリスト\(項目のみ\)](#)

[「高等教育機関の情報セキュリティ対策のためのサンプル規程集」対応チェックリスト](#)

項目別セキュリティサンプル規程集対応チェックリストのtsvファイルを公開しましたので、ご利用ください。

本サイトで公開しているtsvファイルの文字コードはShift_JIS、ハッシュ値(SHA-256)は以下の通りです。

45337b22dd56d966456b0b592dd78ea71d65924698cddacda4410e6f54e14d2e:sp-sample-2019-ChecklistV10-item.tsv

本チェックリストはクリエイティブ・コモンズ 表示 4.0 国際 ライセンスの下に提供されています。

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



広島大学
情報メディア教育研究センター
Information Media Center, Hiroshima University

[ホーム](#) [ニュース・お知らせ](#) [すべてのサービス](#) [センター紹介](#) [FAQ・問い合わせ](#)

広島大学クラウドサービス利用ガイドライン

[ホーム](#) / [センター紹介](#) / 広島大学クラウドサービス利用ガイドライン



センター紹介

[センター沿革](#)

[スタッフ紹介](#)

[アクセスマップ](#)

[センター関連規定](#)

[広島大学クラウドサービス利用ガイドライン](#)

[大学等におけるクラウドサービス利用シンポジウム](#)

[「テクニカルトレーニング・インテンシブ」ハイブリッドプログラム](#)

[ISMSの取り組み](#)

[SDGsの取り組み](#)

[統計情報](#)

お知らせ

- 2017/8/30 [広島大学クラウドサービス利用ガイドライン第三版](#)を公開しました。
- 2015/9/1 [広島大学クラウドサービス利用ガイドライン第二版](#)を公開しました。
- 2014/2/5 [クラウドサービス利用ガイドライン説明会](#)を開催しました。
- 2013/3/15 [広島大学クラウドサービス利用ガイドライン第一版](#)を公開しました。

クラウドサービス利用ガイドラインの整備について

クラウドサービスは、サーバ管理の煩雑さを軽減し、新サービスの構築が迅速に行えることから注目を集めています。しかしその一方で、その運用の大部分がクラウド事業者の管理下で行われ、運用コストの最適化のため他の利用者とコンピュータ資源を共用する運用が行われるのが一般的であることから、データの保護・保全など情報セキュリティに関する懸念が指摘されています。

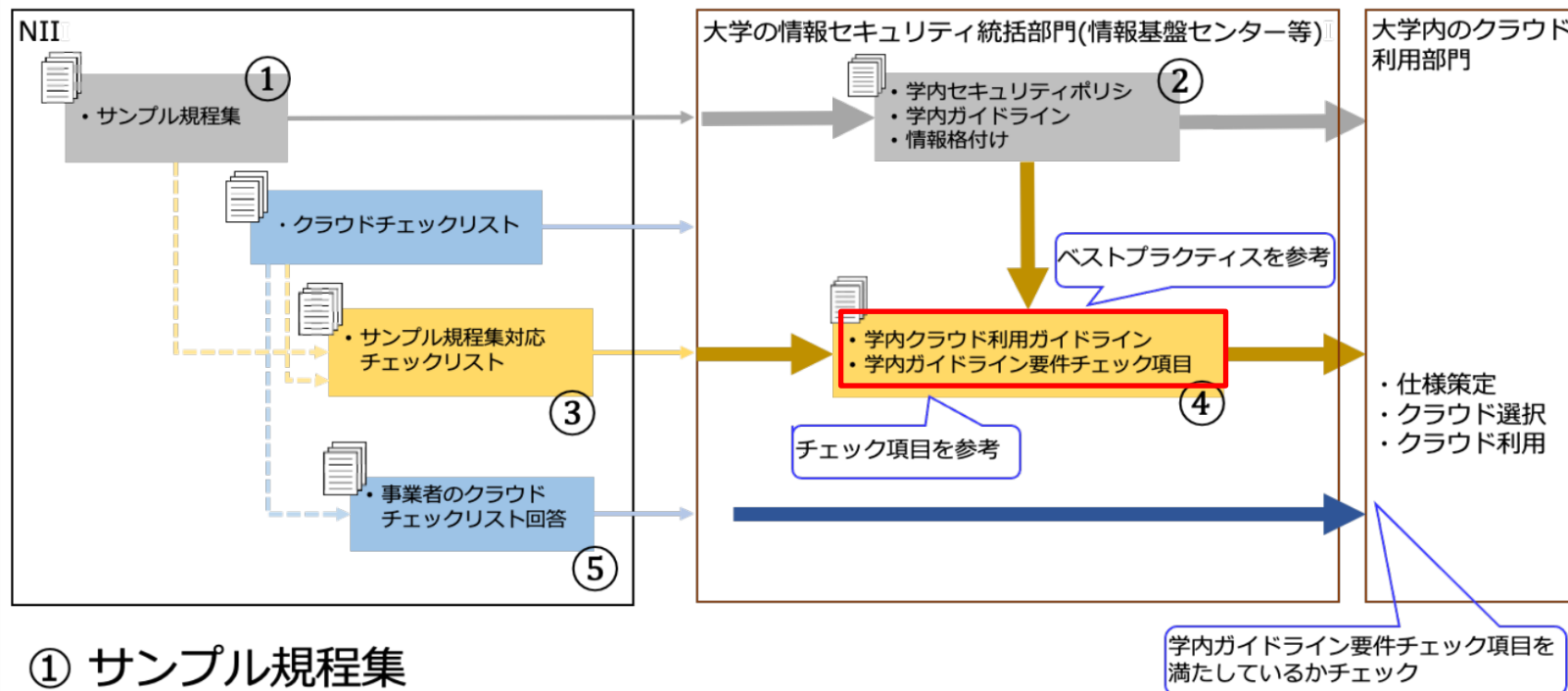
本学においても、管理運用業務の効率化の観点からクラウドサービスの積極的な活用が望まれますが、クラウドサービスの利用にあたっては、クラウド事業者の選定、サービス内容の確認、責任体制の構築等を慎重に行う必要があります。本学が保有している重要な情報(法人文書)については、広島大学法人文書管理規則によりそれぞれの重要度に応じた取扱いが求められており、本学または部局等が法人文書の保存場所としてクラウドサービスを利用する場合は特に慎重な対応が必要です。

このような状況を踏まえ、広島大学では、平成24年度に本学または部局等が法人文書の保存場所としてクラウドサービスを利用する場合を想定したガイドラインの策定を行い、平成25年度から「クラウドサービス利用ガイドライン」の運用を開始しました。

サンプル規定集対応チェックリストVer1.0



【利用イメージ】



● 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、
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か(どの業務をクラウドサービスに移行するか)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)	保存する情報
	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？(ガイドライン表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属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

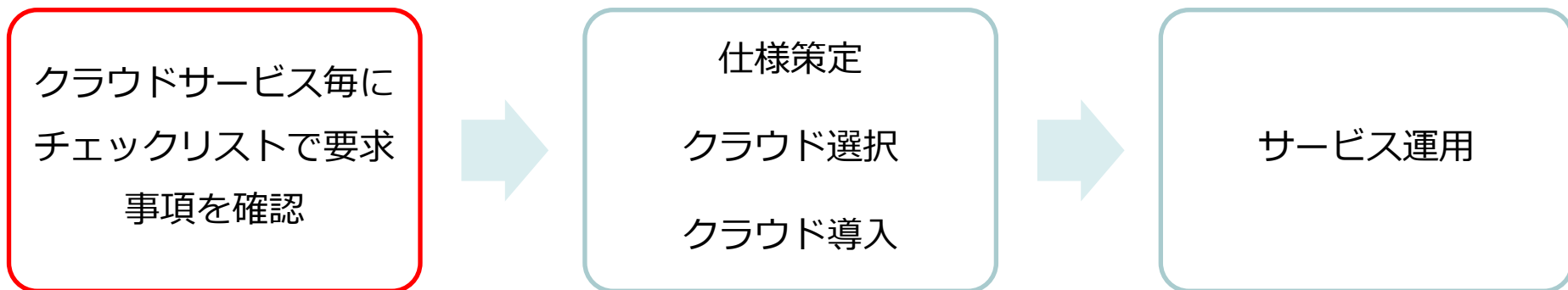
ENISA「クラウドコンピューティング情報セキュリティに関わる利点、リスクおよび推奨事項」*1をカバーできていることを確認済み

*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

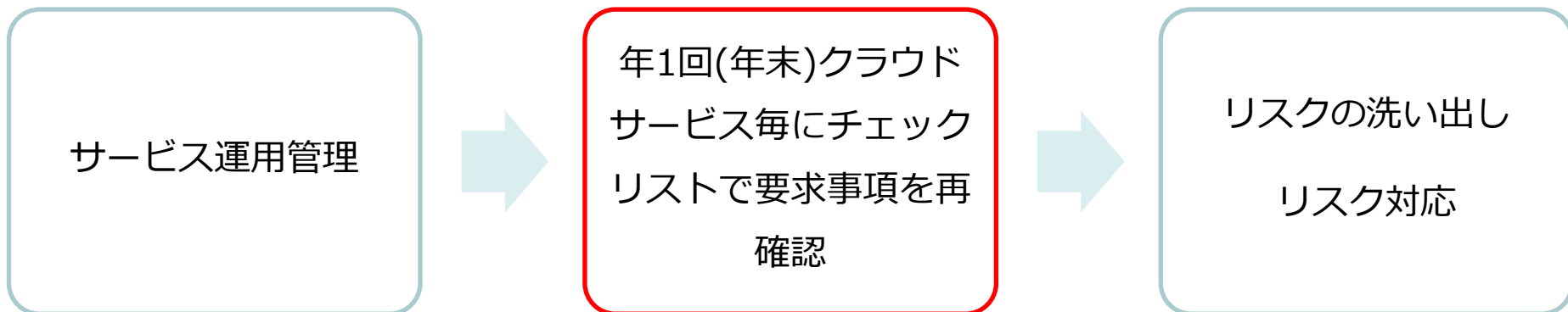
2017年8月7日改訂

情報セキュリティ推進機構

クラウドサービス導入前



クラウドサービス導入後



ISMSクラウドセキュリティ認証を取得・維持

- 運用管理の観点で工夫が必要とコメントを頂いているため、改定中

2020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：**
 - － 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

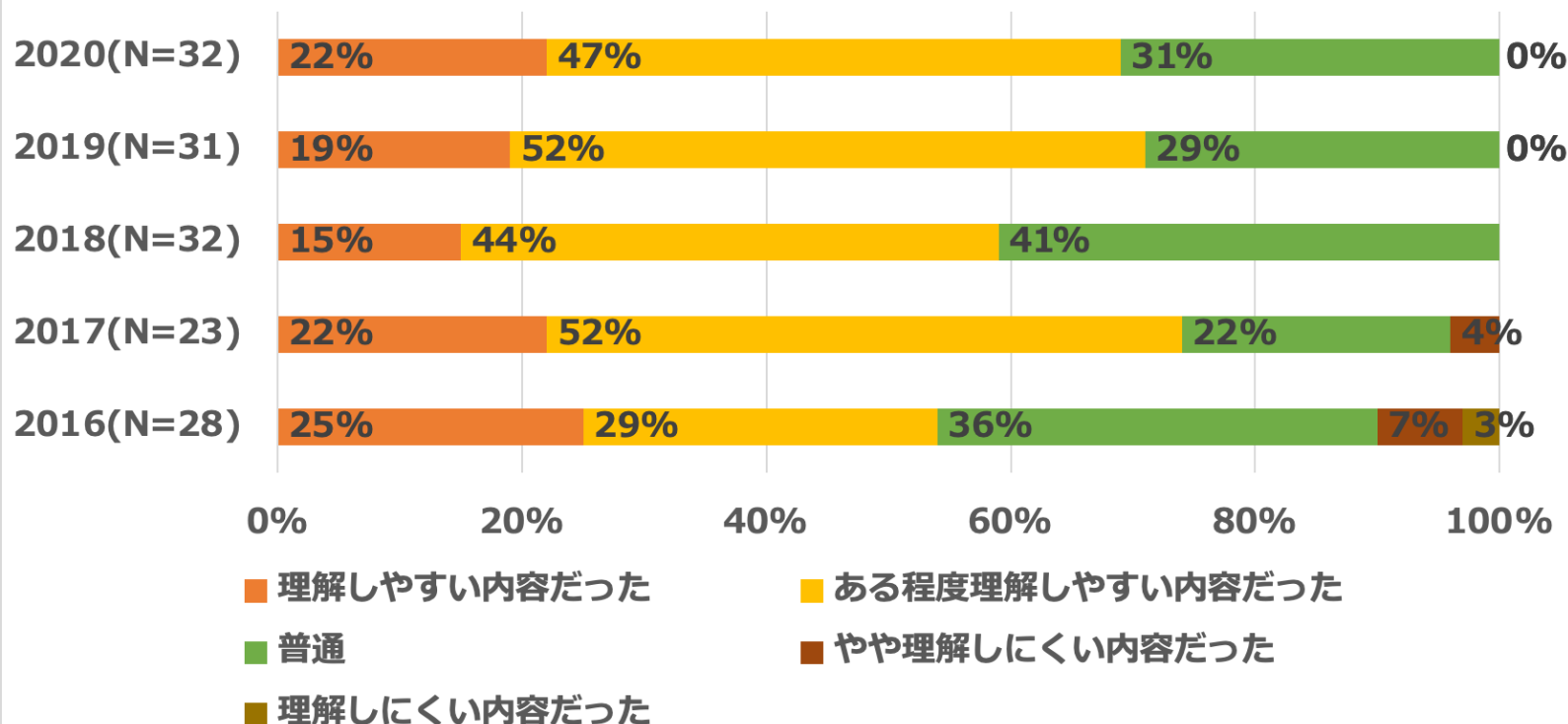
質問1の問いの内容は理解しやすいものでしたか？

● 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69%（理解しやすい：22%、ある程度理解しやすい：47%）
- 普通が31%
- 理解しにくいのが0%

経年変化が見えるよう気を付けながら、
わかりやすくなるよう見直している

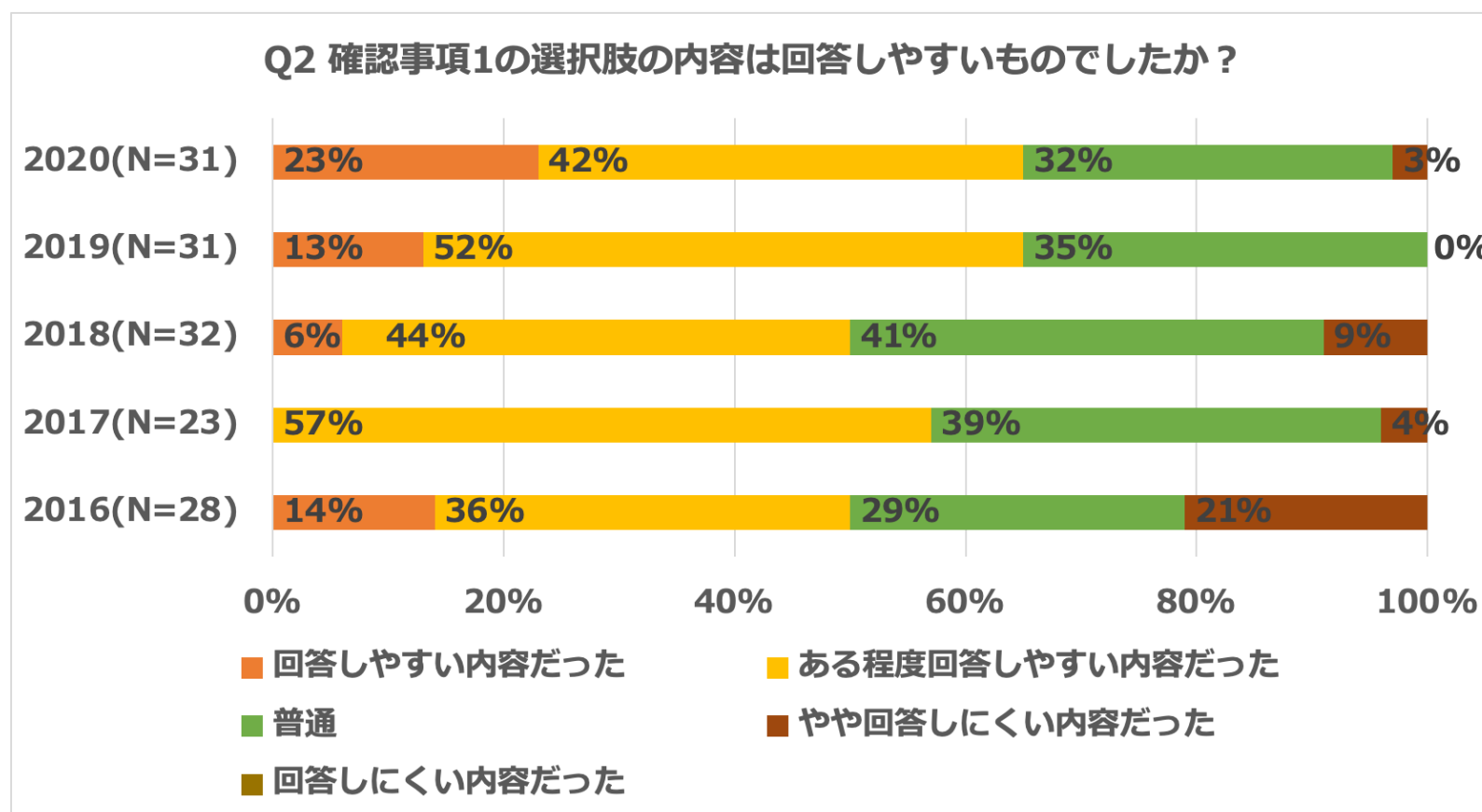
Q1 確認事項1の質問の内容は理解しやすいものでしたか？



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：23%、ある程度理解しやすい：42%）
- 普通が32%
- 理解しにくいのは3%（やや理解しにくい：0%、理解しにくい：0%）



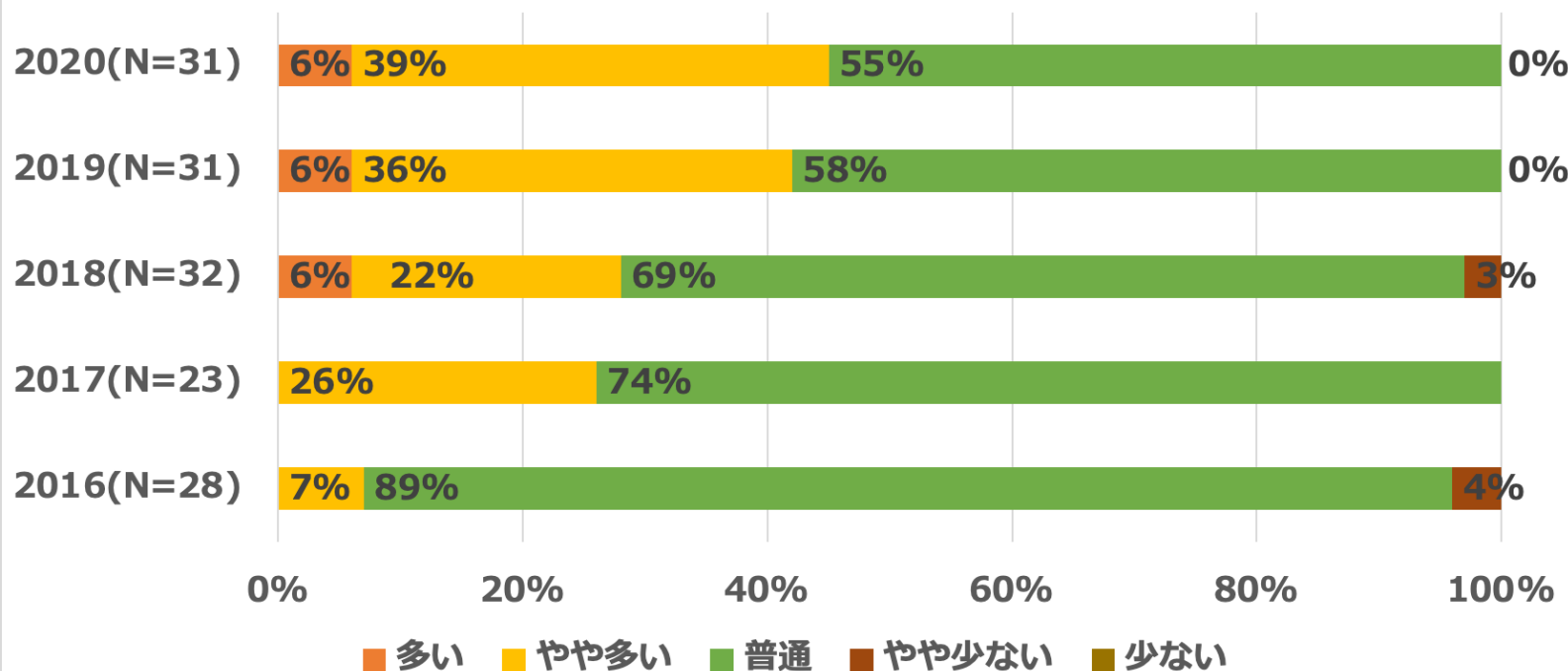
質問1の質問数は適量でしたか？

- 25問の問題数は適量だった模様

- 多いが42% (多い：6%、やや多い：36%)
- 普通が55%
- 少ないが0% (やや少ない：0%、少ない：0%)

一部「労力をもう少し減らしたい」という要望がある中で、参加機関が真剣に現状を整理し回答いただいているため、満足を得られるフィードバック情報が重要となる

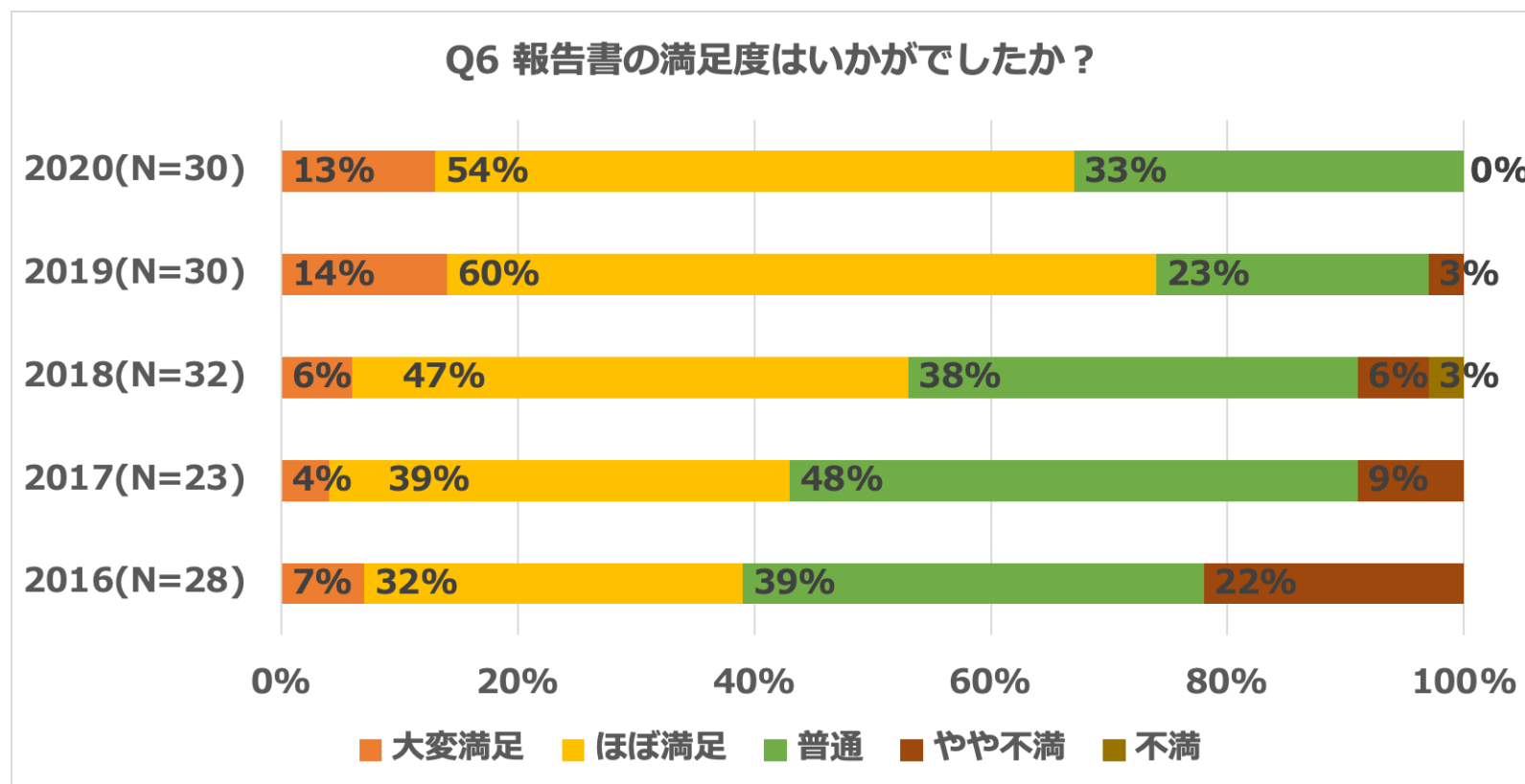
Q3 確認事項1の質問数は適量でしたか？



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67%（大変満足：13%、ほぼ満足54%）
- 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？

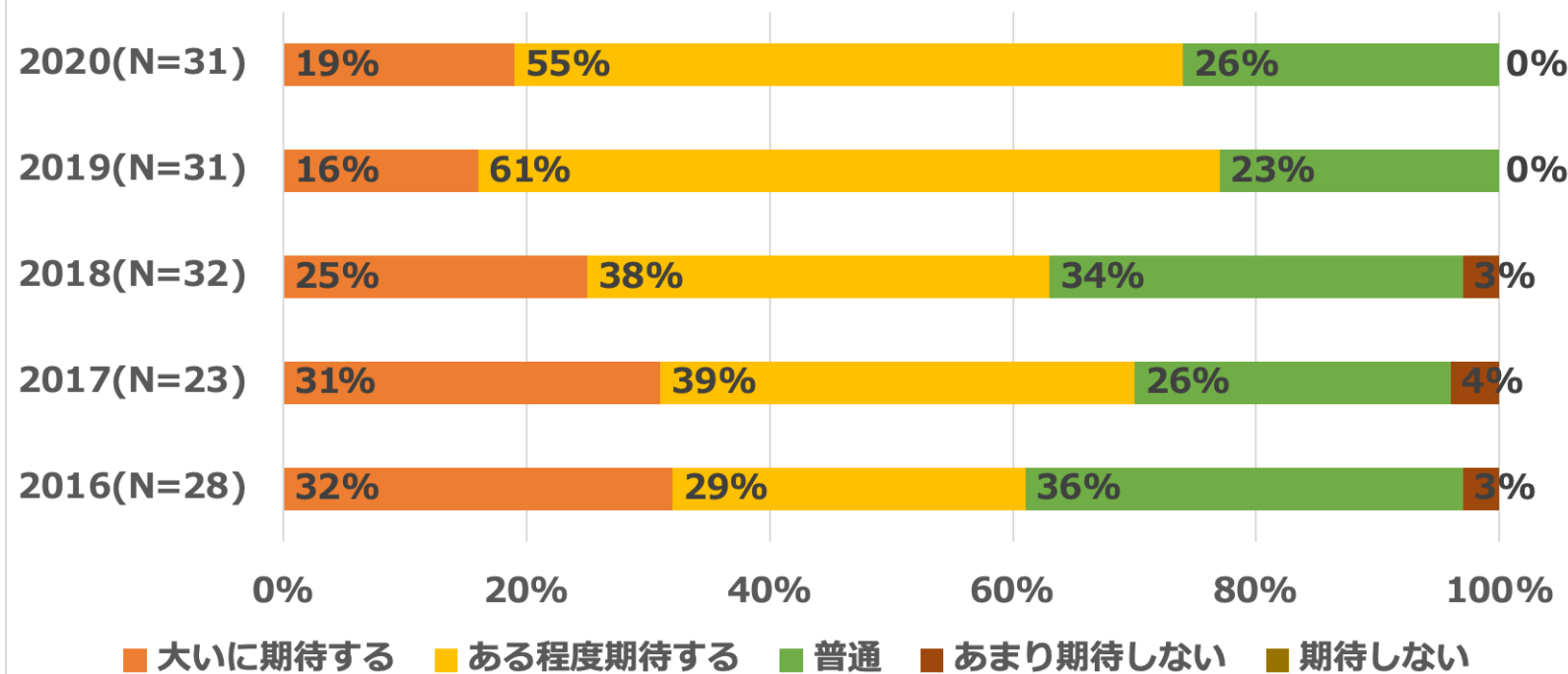
● 取組は全体的に期待されている模様

– 期待は74%（大いに期待する：19%、ある程度期待する：55%）

– 継続希望のコメントが多数あり

より効果的な調査とするため、引き続き調査に対する意見や各組織での取組みの共有をお願い致します。

Q7 実態調査の取り組みに対しての期待はいかがですか？



- **2016年度から2020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サイトとしての提供