NIIオープンフォーラム2023, 2023/5/31

「情報セキュリティガバナンス・クラウドサービス利用実態調査2022」報告

– DX推進を支える情報システムの運用管理 –

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7年連続で学術機関のクラウド活用を踏まえた情報セキュリティガバナンスの調査を実施し、その結果を報告する**
  - 2022年度からはデジタルトランスフォーメーション(DX)推進の観点を踏まえた情報セキュリティガバナンスの調査を実施

調査概要（1/2）

- **【実態調査の目的】**
  - 本実態調査は、組織運営業務に必要な情報システム・情報セキュリティの運用管理を担当されている部署等の担当者に対してアンケートを行い、個別報告書の提示により、学術機関全体の傾向から貴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的としています
- **【実態調査活動のゴール】**
  - 学術機関のクラウドサービス利活用促進と学術機関における情報セキュリティガバナンス向上に関するベンチマークの策定
  - DX推進を支えるIT基盤を想定した情報セキュリティマネジメントの共通の方向性を提示

実態調査概要（2/2）

- **2022年度調査**
  - 実施時期：2022年12月1日（木）～12月26日（月）
  - 有効回答数：36機関（新規参入機関：4機関）
- **参考**
  - 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

2022年度アンケート概要

HIROSHIMA UNIVERSITY

- **質問1（大幅な見直し）**
  - 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+記述形式
  - 質問数：27問
  - 回答条件：必須(問1～問25)、自由(問26～問27)
  - 有効回答率：100%（36／36機関）
    - 2021: 100%（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：78%（28／36機関）
    - 2021: 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）

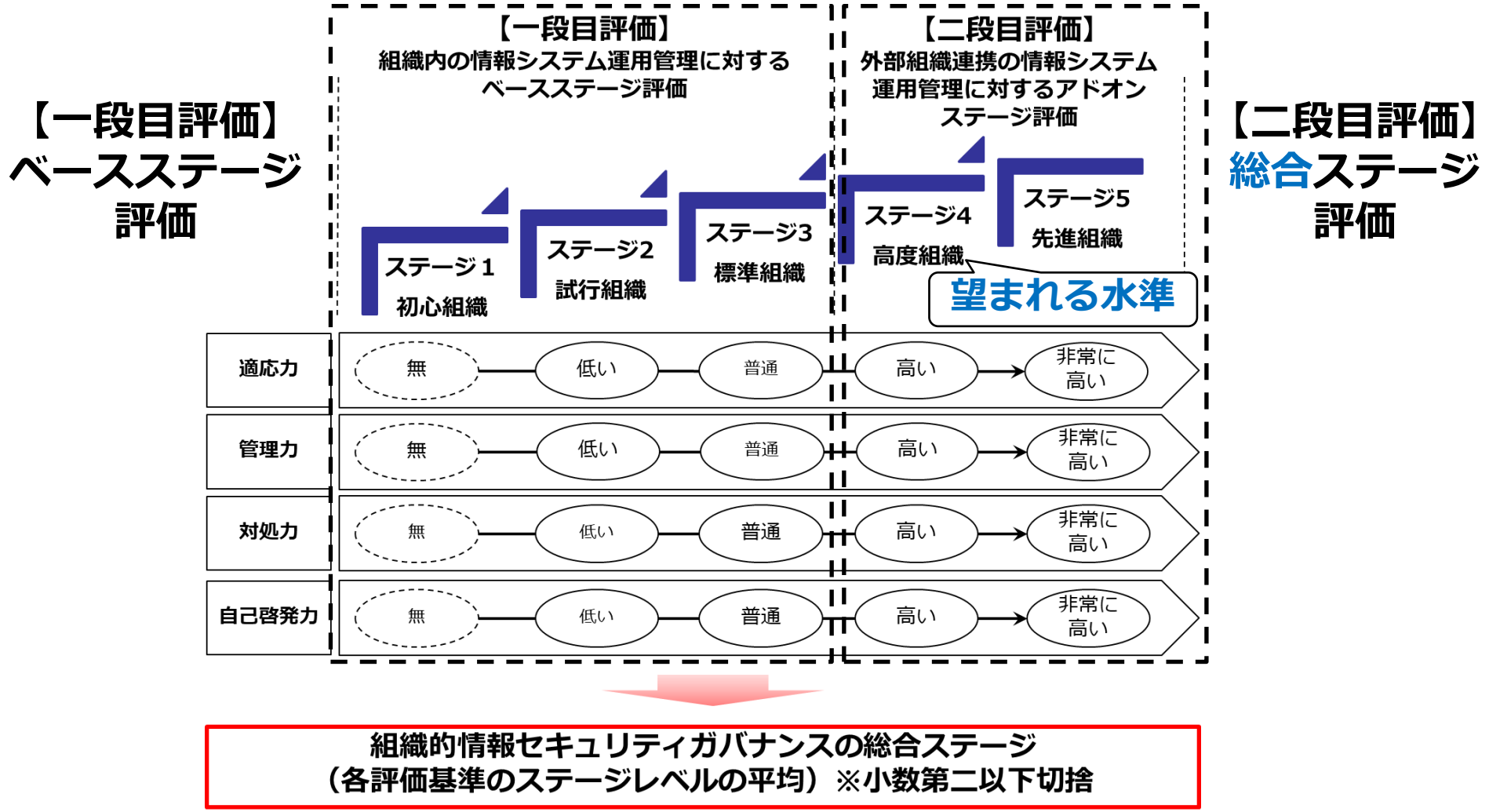
情報資産の管理状況の把握

- **質問3 （見直し）**
  - 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：72%（26／36機関）
    - 2021: 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）

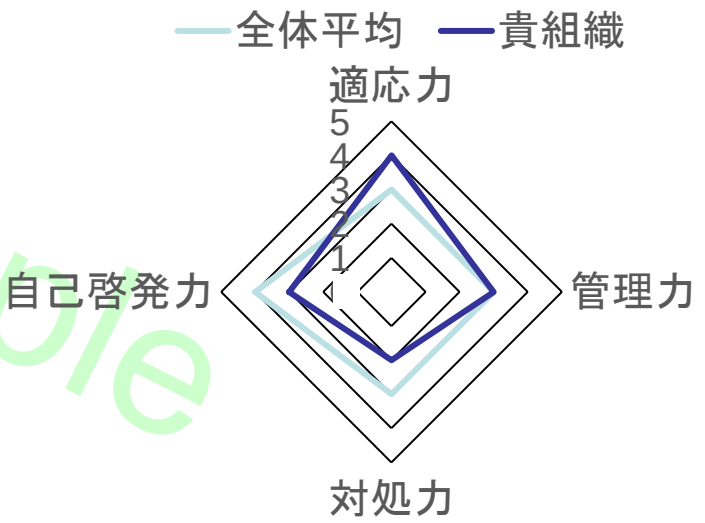


個別報告書のイメージ

「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

2022年度質問項目の見直し

見直しの方針

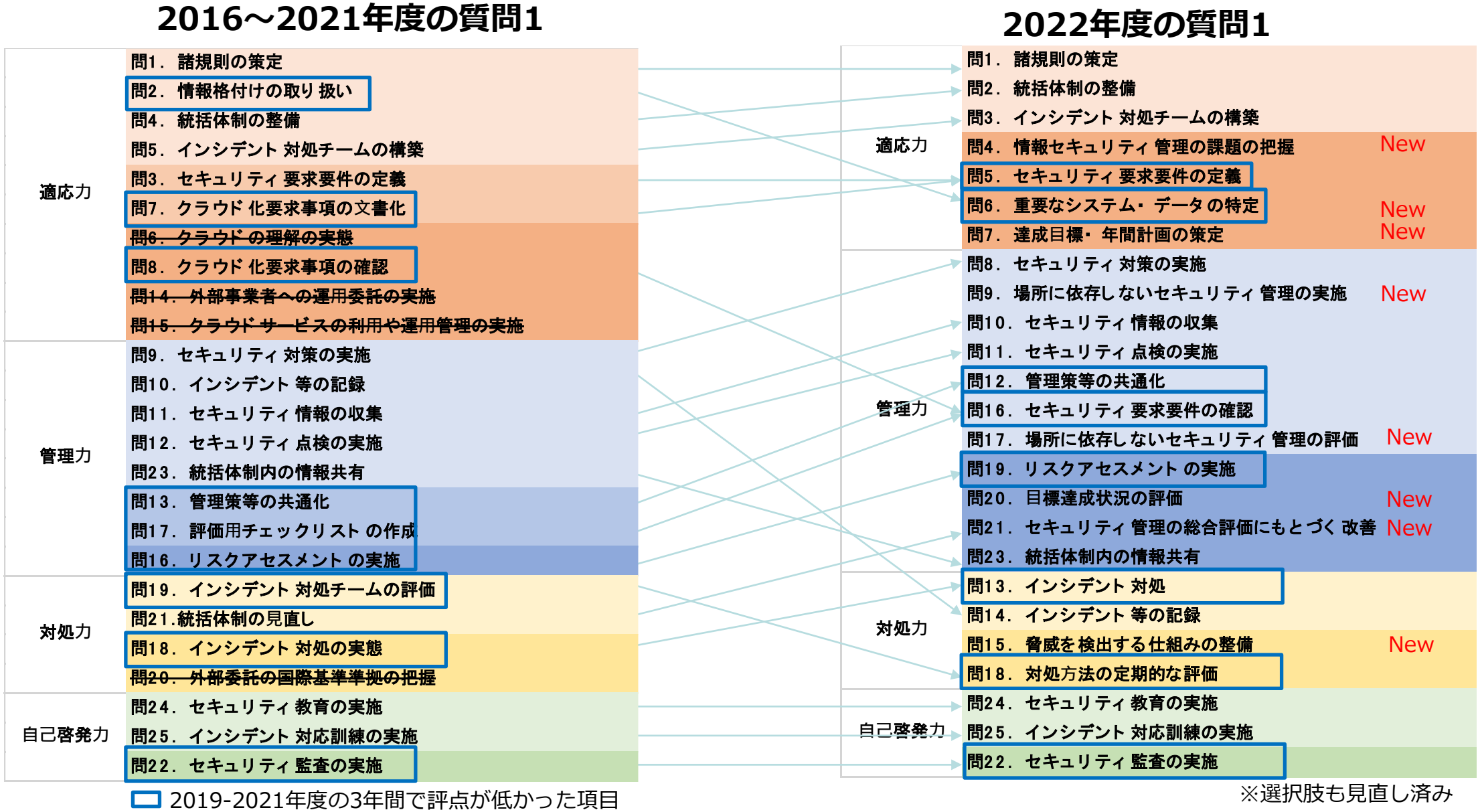
- **これまでのアンケートの質問は、情報セキュリティマネジメントシステム（ISMS）がベース**
  - セキュリティマネジメントとしての枠組みが明確なため、共通の指標や方向性を提示が容易
  - ISMS認証取得した経験も踏まえて、情報セキュリティマネジメントとしてのステージを定め、抑えておくべき内容を25問の質問に集約
    - 2015年～：ISMS認証審査合格、2017年～：ISMSクラウドセキュリティ認証審査合格
- **DX推進を支えるIT基盤は未知の領域のため、下記の資料を参考にISMSとの共通事項やDX推進基盤として必要な観点を洗い出した**
  - AXIES大学デジタルトランスフォーメーション検討タスクフォースの活動報告
    - 提言:多様な教育研究活動の高度化を支える大学ICT基盤の集約化・共通化・協働化～コロナ時代における大学のデジタルトランスフォーメーションに向けて～
  - 経済産業省
    - 「DX 推進指標」とそのガイダンス
  - 総務省
    - テレワークセキュリティガイドライン
- **DX推進を支えるIT基盤上で情報セキュリティマネジメントとして求められる共通の指標や方向性を提示を目指す**

共通事項や必要な観点

- **ISMSのポイント：Plan, Do, Check, Action**
  - P：守るべき情報資産・利害関係者・外部・内部の課題の特定、リスクアセスメント、セキュリティマネジメントにおける達成目標・年間計画の策定
  - D：目標や計画達成を示すエビデンスの確保、リスク対応、ISMS文書修正、教育・訓練
  - C：管理・対処方法の自己評価、内部監査・外部監査、マネージメントレビュー
  - A：次年度の達成目標・計画策定へのフィードバックの整理や体制の準備
- **AXIES報告書のポイント：大学ICT基盤の集約化・共通化・協働化**
  - 情報戦略立案、オープンスタンダードやオープンソースソフトウェアの推進、大学経営へのインパクト評価、サービスポートフォリオの作成、人材強化とキャリアパス
- **DX推進指標としてITシステム構築ポイント：データ活用、スピード・アジリティ、全体最適**
  - IT資産の分析・評価、廃棄、競争領域の特定、非競争領域の標準化・共通化、ロードマップ
- **テレワークセキュリティガイドラインのポイント：ゼロトラストセキュリティ、脅威インテリジェンス**
  - ガバナンス・リスク管理、資産・構成管理、脆弱性管理、特権管理、データ保護、マルウェア対策、通信保護・暗号化、アカウント・認証管理、アクセス制御・認可、インシデント対応・ログ管理、物理的セキュリティ、教育

- **今後のセキュリティガバナンス・セキュリティマネマネジメントを評価する質問1の見直しのポイント**
  - 守るべき**情報資産・利害関係者・外部・内部の課題の特定**、**達成目標・年間計画**、管理・対処方法を組織全体で**いつでもどこでも把握**が可能か？
  - セキュリティ管理項目や脆弱性・脅威に関する**エビデンスやログ等を動的に集約**し**協働的かつ迅速に分析・評価**ができるか？
  - 分析・評価、監査、マネージメントレビュー等の**結果を組織全体でいつでもどこでも把握**が可能か？

参考：質問1見直し結果



2019-2021年度の3年間で評点が低かった項目

※選択肢も見直し済み

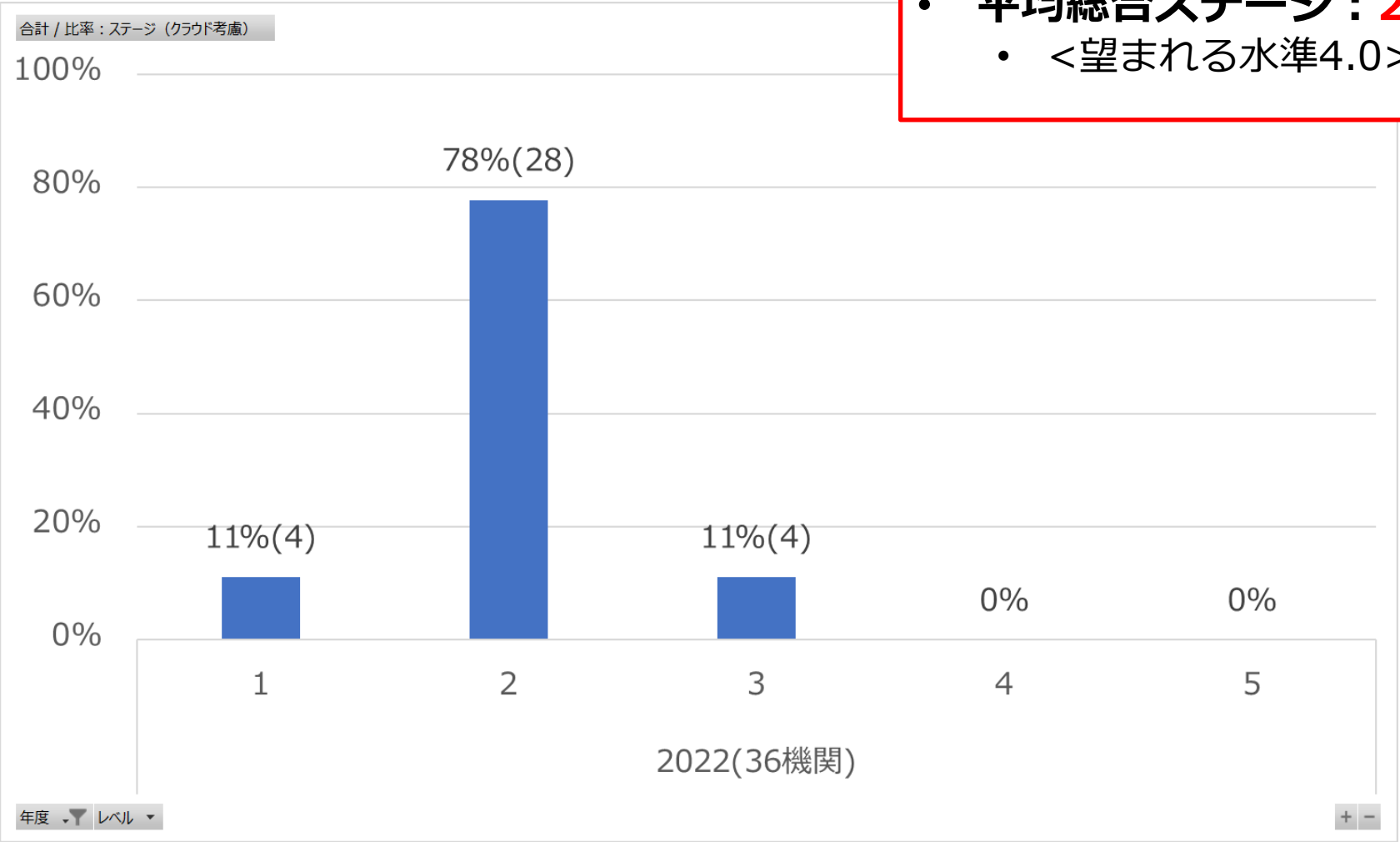
2022年度実態調査結果

HIROSHIMA UNIVERSITY

2022年度総合ステージ分布図

- **有効回答：36機関**
  - 新規参入機関：4機関

- **試行組織が多い**
- **平均総合ステージ：2.5**
  - <望まれる水準4.0>



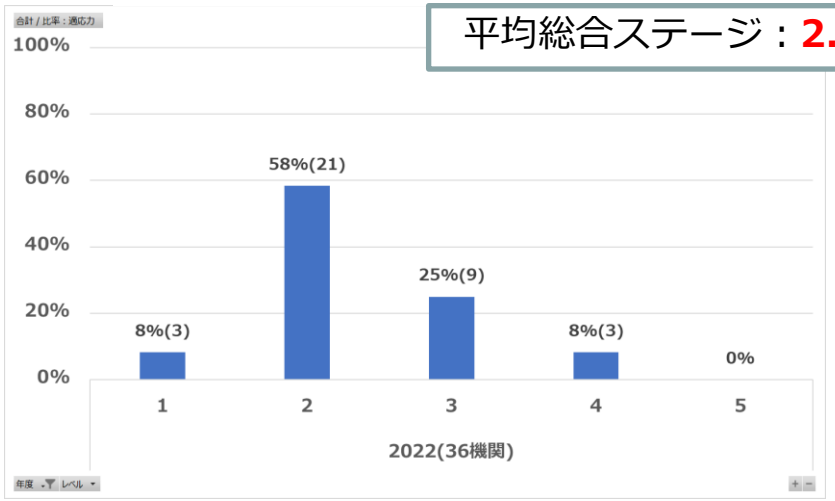
n=36（）内は組織数

2022年度評価基準別総合ステージ分布図

HIROSHIMA UNIVERSITY

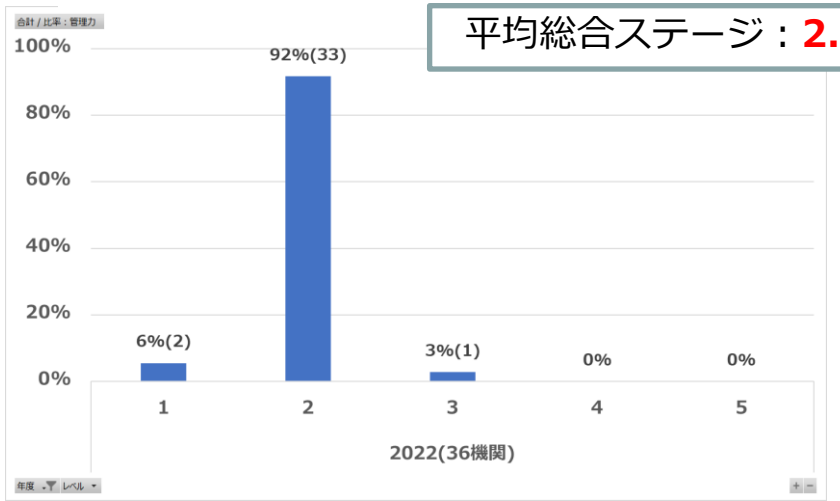
適応力総合ステージ分布

平均総合ステージ：**2.8**



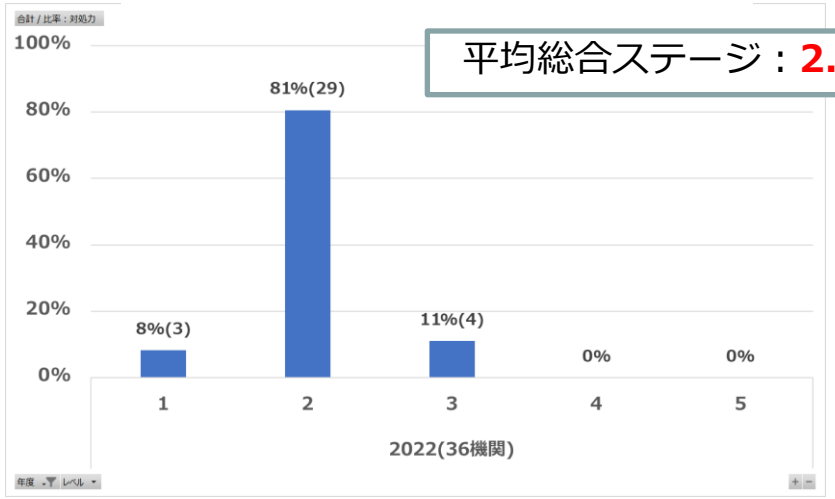
管理力総合ステージ分布

平均総合ステージ：**2.4**



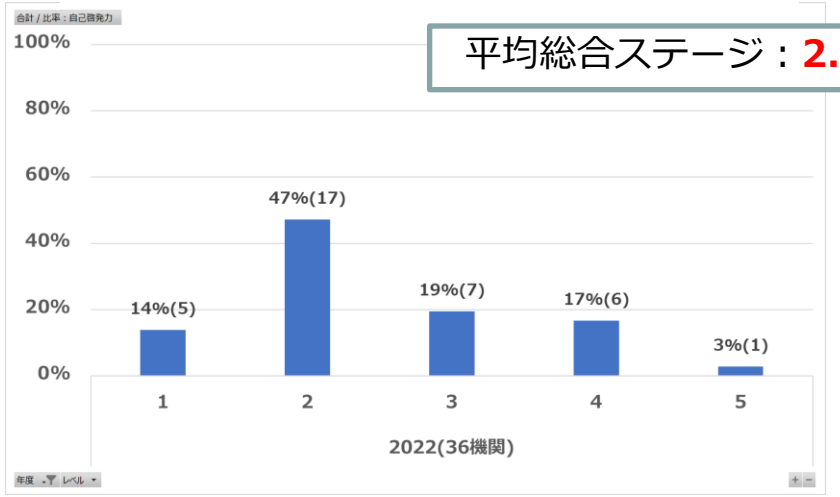
対処力総合ステージ分布

平均総合ステージ：**2.4**



自己啓発力総合ステージ分布

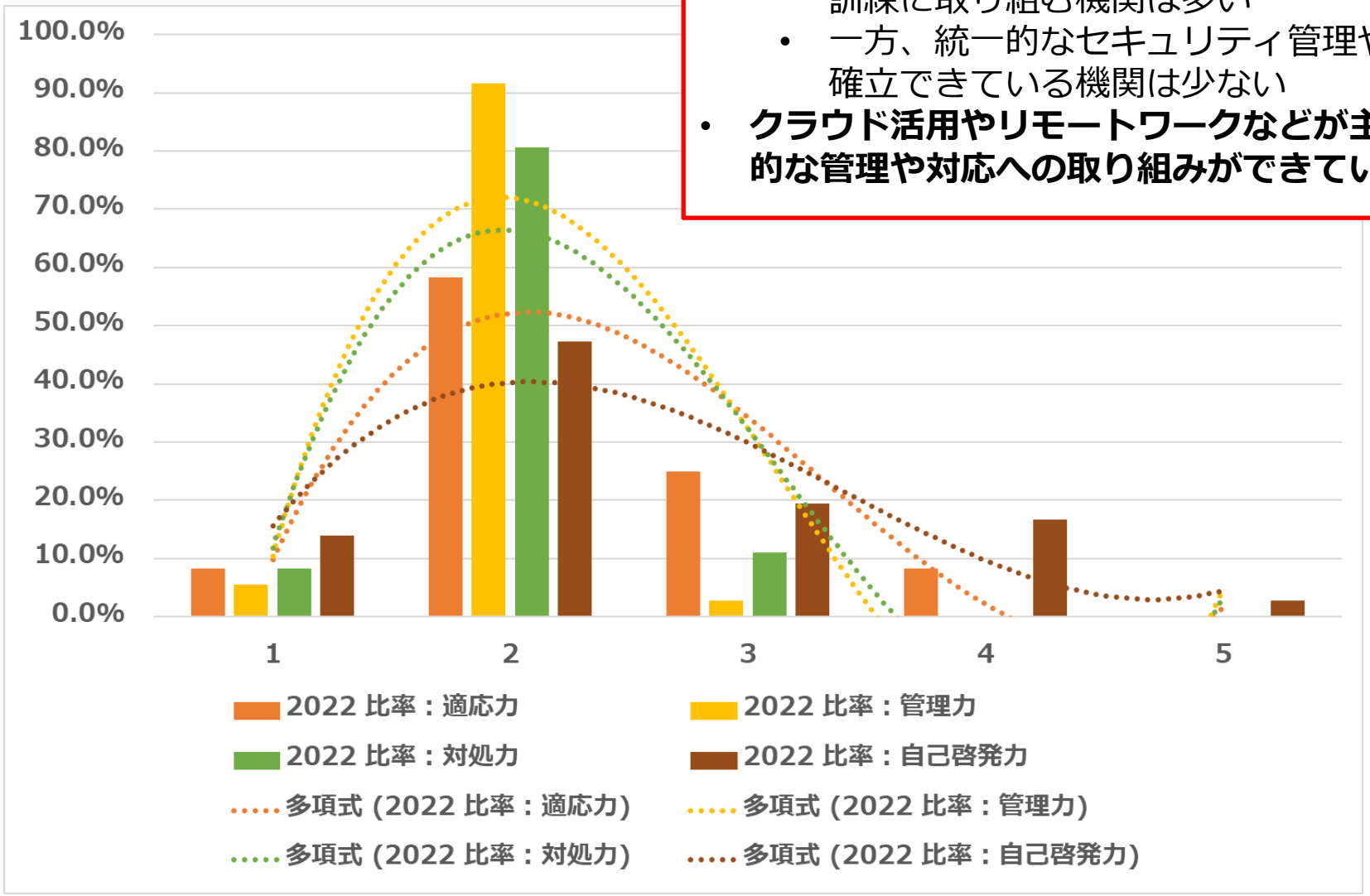
平均総合ステージ：**2.5**



n=36（）内は組織数

2022年度評価基準別比較

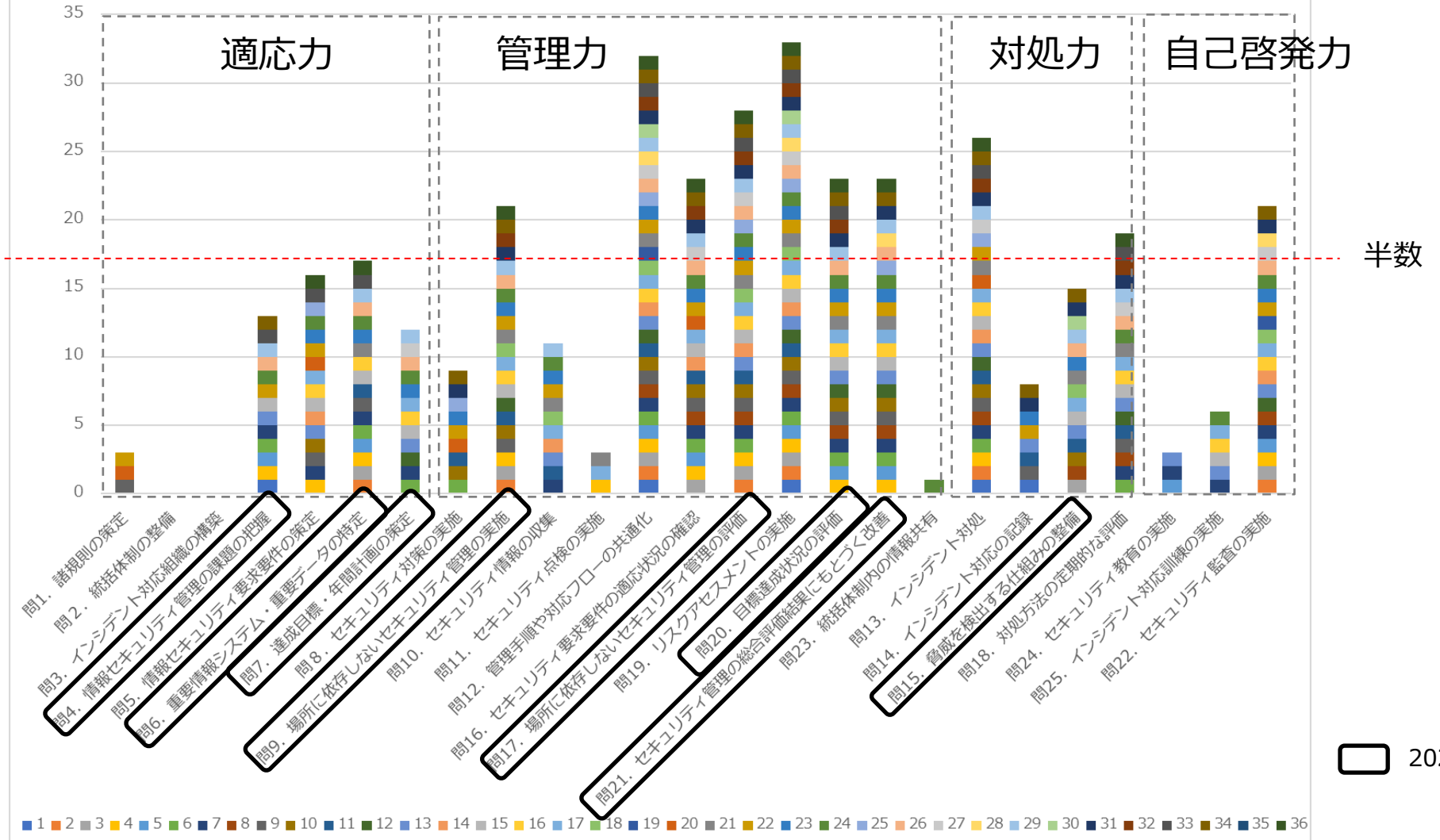
- **適応力・自己啓発力が全体の総合ステージを牽引**
  - 組織的なセキュリティ管理・対処のための整備や教育・訓練に取り組む機関は多い
  - 一方、統一的なセキュリティ管理や部署横断的な対応が確立できている機関は少ない
- **クラウド活用やリモートワークなどが主流になる中で、先進的な管理や対応への取り組みができている機関は少ない**



n=36

質問別指摘数分布図(2022年度36機関)

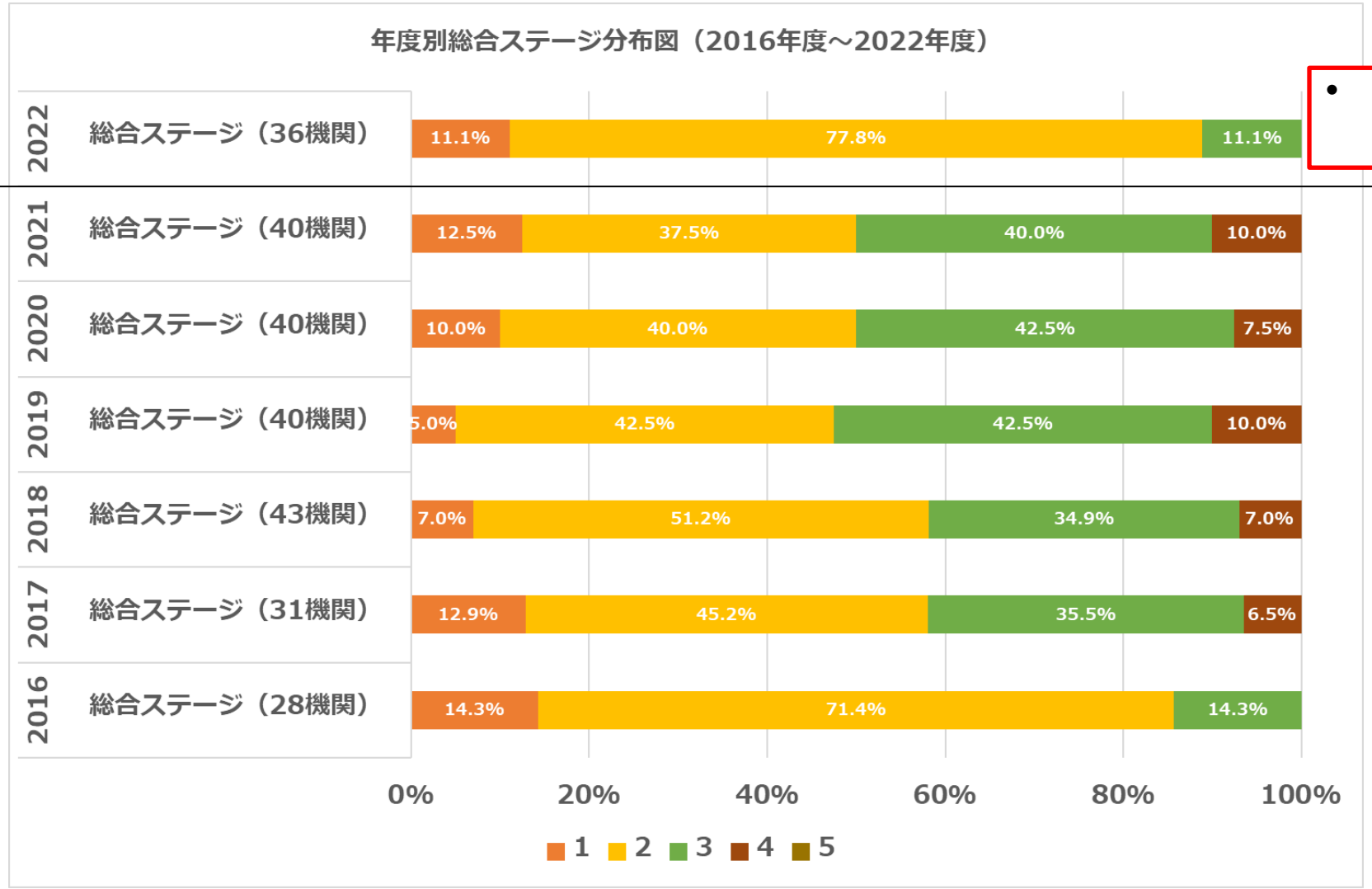
- **共通化、分析・評価(監査含む)、インシデント対処に関連する質問の指摘が多い**
- **DX推進のIT基盤として、データをリアルタイムかつ全体最適で活用しながら変化に迅速に対応が求められる中で、集約化・共通化・協働化の課題が残る**



参考：年度別総合ステージ単純平均比較

HIROSHIMA UNIVERSITY

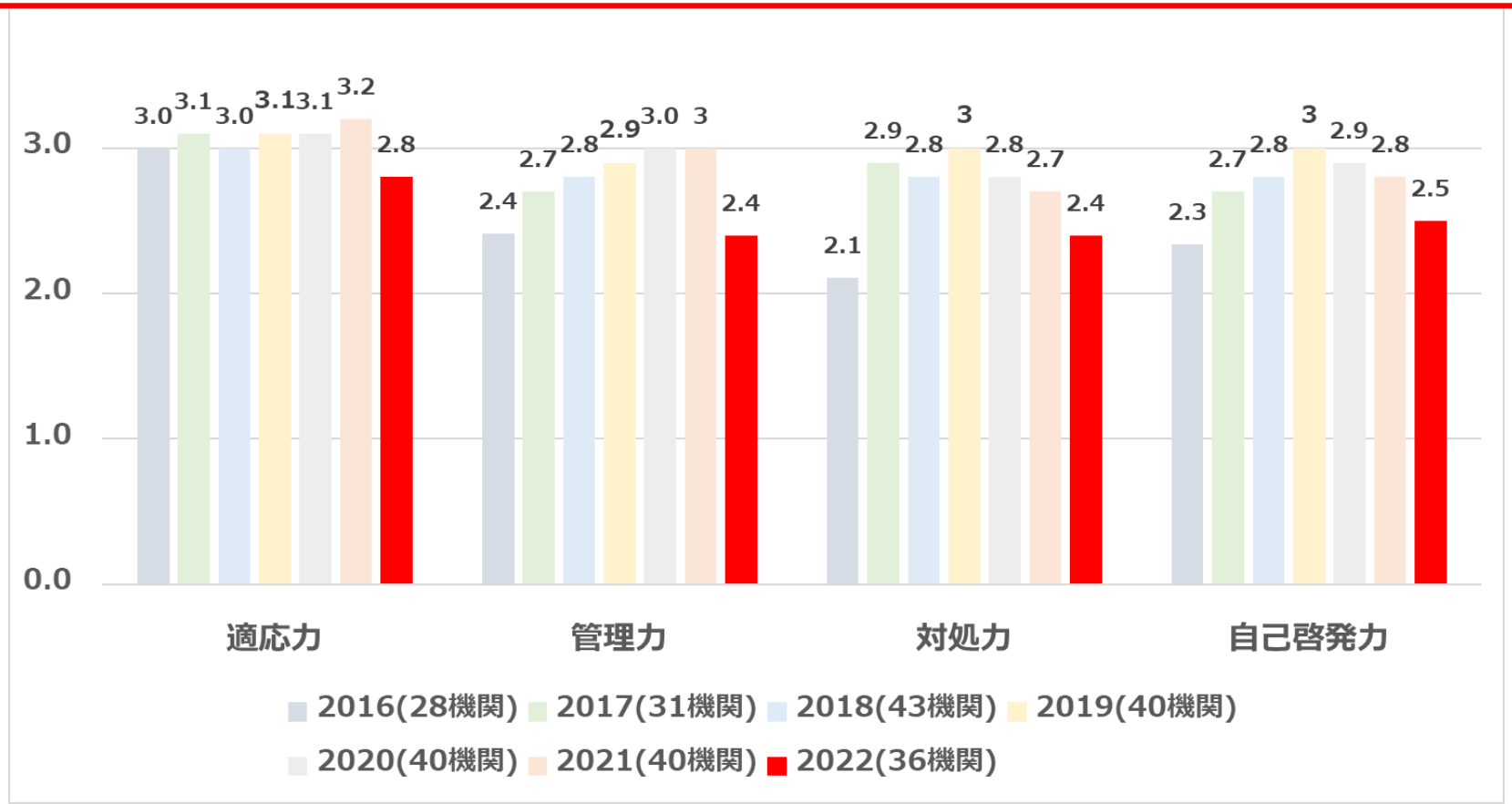
平均ステージ2.5→2.9→2.9 →3.0→2.9→2.9→2.5(2022年度)



- 初年度と似た割合となっている

参考：年度別・評価基準別単純平均比較

- **全評価基準でDX推進の観点を加えた影響を受けている**
  - 初年度から3～4年かけて、総合ステージの平均値がピークになる傾向
  - それ以降は、一定あるいは下落する傾向がある
    - 3～4年以上連続して参加する機関は総合ステージが一定あるいはゆっくりと向上し、下落する傾向はほぼ無い
    - 新規参入の機関が総合ステージが低い（初心組織あるいは試行組織）傾向がある
- **短いスパンで総合ステージが向上するための支援が今後の課題**



※2019年度に対処力の評価見直し

試行組織(ステージ2)から標準組織(ステージ3)になるために

HIROSHIMA UNIVERSITY

- **適応力**
  - 平均ベースステージは3.0
  - 総合ステージを引き上げるための項目
    1. 問5, セキュリティ要求要件(標準仕様)の定義

    New 2. 問6, 重要なシステム・データの特定

    New 2. 問7, 達成目標・年間計画の策定

    New – 問4, 情報セキュリティ管理の外部・内部の課題の把握はステージ3以上
- **対処力**
  - ベースステージを下げた項目
    1. 問13, インシデント対処（迅速さ）（※）
  - 総合ステージを引き上げるための項目
    1. 問18, 対処方法の定期的な評価

    New 2. 問15, 脅威を検出する仕組みの整備
- **管理力**
  - ベースステージを下げた項目

    New 1. 問17, 場所に依存しないセキュリティ管理の評価
    2. 問12, 管理策等の共通化
    3. 問16, 情報システムがセキュリティ要求要件を満たしていることの確認
  - 総合ステージを引き上げるための項目
    1. 問19, リスクアセスメントの実施

    New 2. 問21, セキュリティ管理の総合評価にもとづく改善

    New 3. 問20, 目標達成状況の評価
- **自己啓発**
  - 総合ステージを引き上げるための項目
    1. 問22, 監査（内部監査の実施）（※）

※2023年度に評価を見直す予定

記述式・任意回答結果

- **問２６．現在進めているDX活動があれば、活動の概要を共有できる範囲でお答えください**
  - 回答率：45%（16／36機関）
    - 事務系・教育系を中心に、これから取り組む回答が多い
      - 組織体制の構築
      - 人材育成、 DX人材の採用
      - DX基本計画策定
      - ガイドライン策定、データの管理及び利活用ポリシーの策定
      - DX勉強会
      - 一部の機関でシステム整備、アプリ開発、サービス展開も進みつつある（6機関）
        - » 6機関の平均総合ステージ：3.0

記述式・任意回答結果

- **問２７．DXを推進する上で自組織の情報システムが抱えている課題とその課題に対してクラウドサービスが寄与できる可能性について考えをお答えください**
  - 回答率：45%（16／36機関）

課題

- 部署毎にシステム構築する文化、パッケージシステムのカスタマイズ・肥大化、業務改革に伴う**合意形成**やDXを推進する**文化の醸成**が課題
- **ISMAP**クラウドサービスリスト上のサービスプロバイダーの少なさが課題
- クラウドでデータを扱うための学内の**規則化**、**暗号化と利便性を共存**してクラウド上に保存するための仕組化が必要
- 職員の気づきが必要。一般企業と違い明確な課題→目標を立案することが難しいため、文科省などが**ベストプラクティスを定義**し、それを物差しとして具体的な取り組みを啓蒙が必要
- クラウドサービスの導入により、**業務・経費コスト軽減**とはいかないのが課題
- 育成された人材の**技量維持や活用場面の創出**が課題

寄与

- サービス導入の**早期実現**、サービスの**乗り換え**、リソース**変更が容易**
- クラウドサービスは**マイクロサービス化**しており，パッケージシステムに求める要件を分離することで適用することができるため，既存の**情報システムの要件をなるべく最小化**し，パッケージシステム以外のクラウドサービスを適用することで**アジリティの高い**システム構築を効率的に実施
- **ノーコード／ローコード開発を支援**するプラットフォームを準備し、育成した人材に業務改善やサービス改善に向けた取組みに関わってもらうような仕組みを構築中である。
- **クラウド環境に慣れ**れば文化の醸成に寄与する

2022年度事後アンケート結果

HIROSHIMA UNIVERSITY

事後アンケート概要

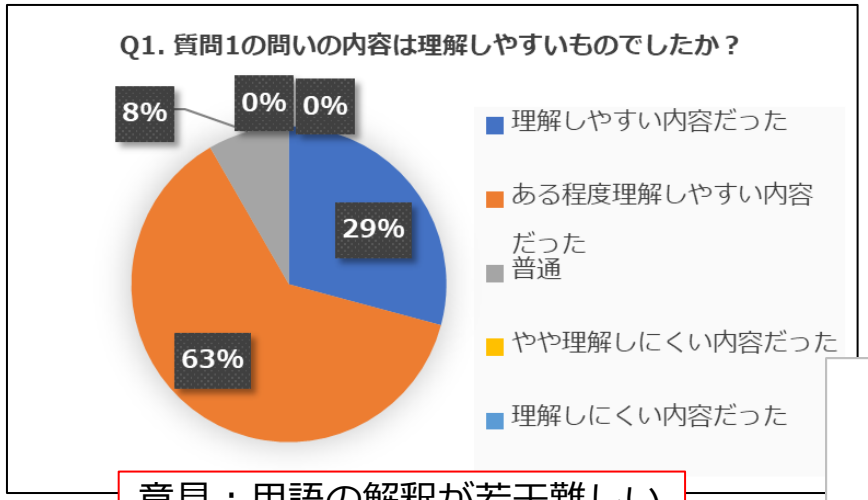
- **内容：**
  - 質問1-3、個別報告書、取り組みに対する評価・意見を把握する内容
- **出題形式：**
  - 四者択一＋自由記述（理由、意見など）
- **質問数：**
  - 8問
- **回答条件：**
  - 任意
- **有効回答率：**
  - 67%（24／36機関）
    - 2021：60%（24／40機関）2020：80%（32 ／ 40機関）、2019：77%（31 ／ 40機関）、2018：74%(32／43機関)、2017：74%(23／31機関)、2016：100%(28／28機関)

質問1、報告書、取り組みに対する事後アンケート結果に限定し紹介

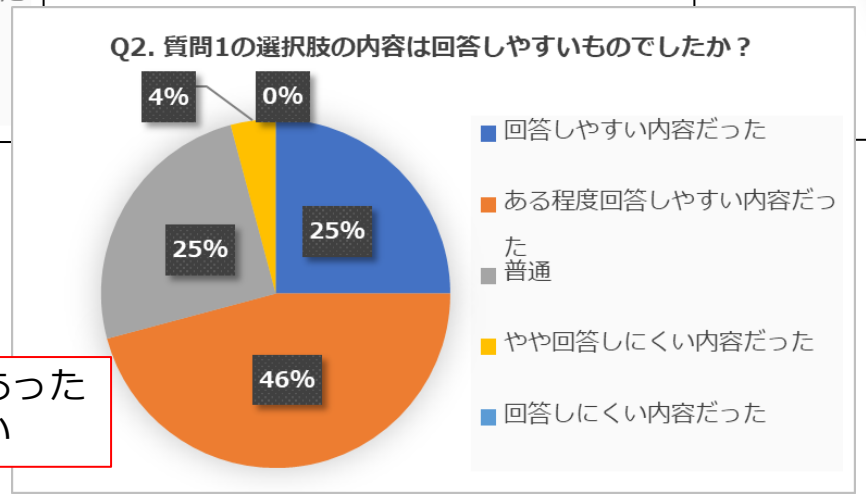
質問1の内容・選択肢は理解しやすいものでしたか？
質問数は適量でしたか？

HIROSHIMA UNIVERSITY

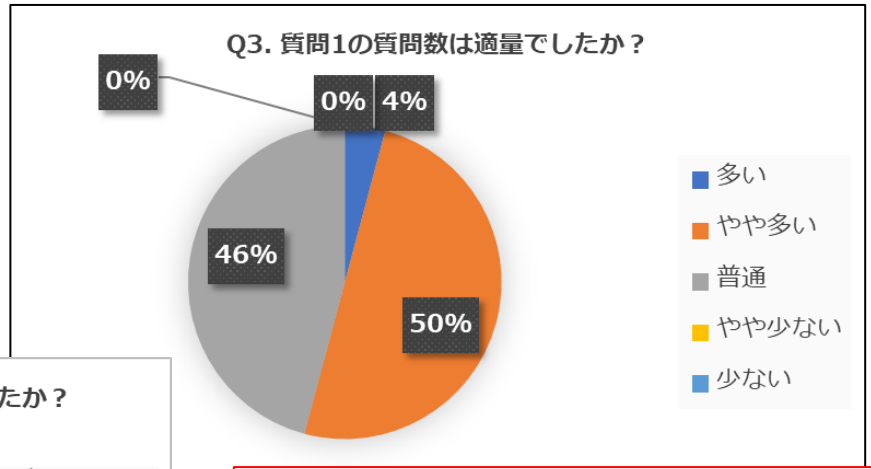
- **質問の内容は全体的に理解しやすく、質問数も適量だった模様**
  - 内容は理解しやすいが92%（理解しやすい：29%、ある程度理解しやすい：63%）
  - 選択肢は理解しやすいは71%（理解しやすい：25%、ある程度理解しやすい：46%）
  - 質問数はやや多いが50%



意見：用語の解釈が若干難しい



意見：一部回答に迷う選択肢があった
意見：選択肢の認識は少し難しい



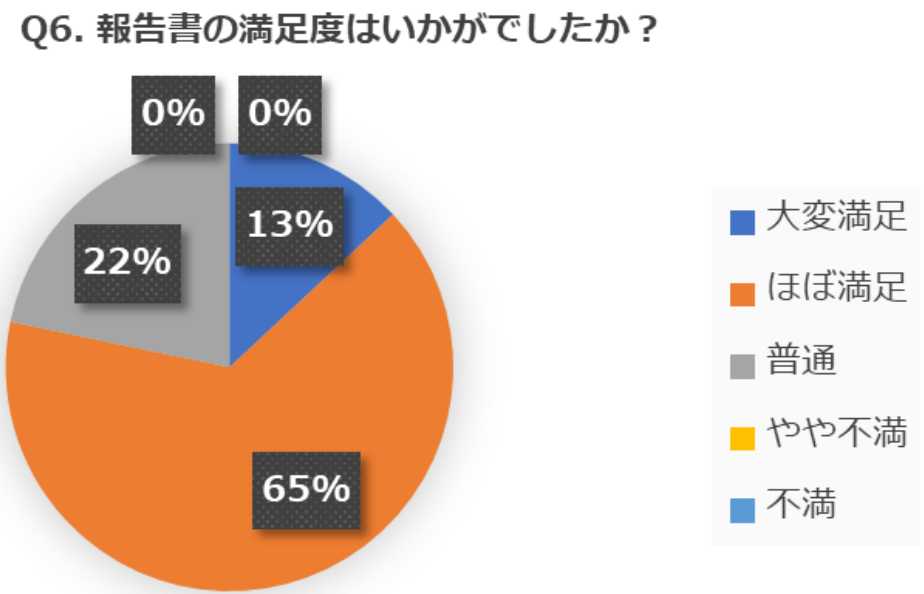
意見：量は多いが、その分フィードバックをいただいている

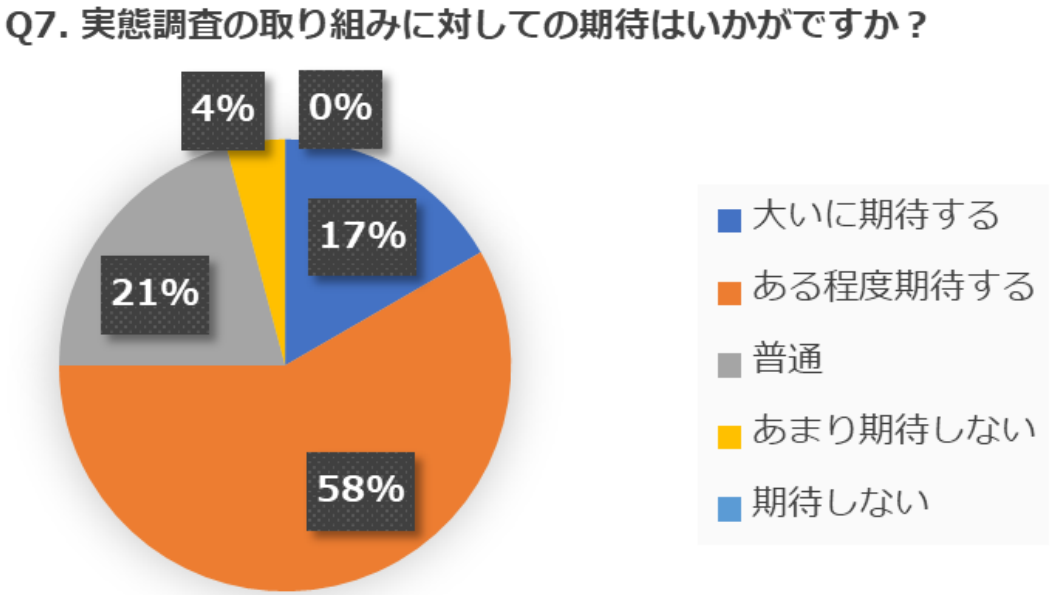
n=24

報告書の満足度、実態調査の取り組みに対しての期待はいかがですか？

HIROSHIMA UNIVERSITY

- **報告書の満足度や期待値は全体的に高い傾向**
  - 満足度は78%（大変満足：13%、ほぼ満足65%）
  - 期待は75%（大いに期待する：17%、ある程度期待する：58%）
  - 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
  - 継続希望のコメントが多数あり





まとめ

- **DX推進を支えるIT基盤上で情報セキュリティマネジメントとして求められる共通の指標や方向性を提示**
  - 守るべき情報資産・利害関係者・外部・内部の課題の特定、達成目標・年間計画、管理・対処方法を組織全体でいつでもどこでも把握が可能か？
  - セキュリティ管理項目や脆弱性・脅威に関するエビデンスやログ等を動的に集約し協働的かつ迅速に分析・評価ができるか？
  - 分析・評価、監査、マネージメントレビュー等の結果を組織全体でいつでもどこでも把握が可能か？
- **2022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**
  - DX推進を支えるIT基盤学術機関の情報セキュリティガバナンスの実態としては、試行組織が多い
  - 試行組織から標準組織に向上するためには、以下がポイント
    - セキュリティ要求要件の定義および確認、情報資産の特定、達成目標・年間計画の策定、管理策等の共通化
    - リスクアセスメント、管理方法・対処方法や目達成状況の評価、内部監査、総合評価にもとづく改善などの分析・評価の実施
- **今後の実態調査活動の課題**
  - 質問や選択肢、評価の見直し（ISMS新規格も考慮？※2022年10月25日にISMS規格が改訂）
  - フィードバック情報の充実
  - 参加機関数の増加
  - 実態調査の協力者を募集