NIIオープンフォーラム2018@学術総合センター, 2018/6/20

クラウドファースト時代における学術機関向け情報セキュリティガバナンス実態調査

-クラウドサービス利用・準備状況の見える化に向けて-

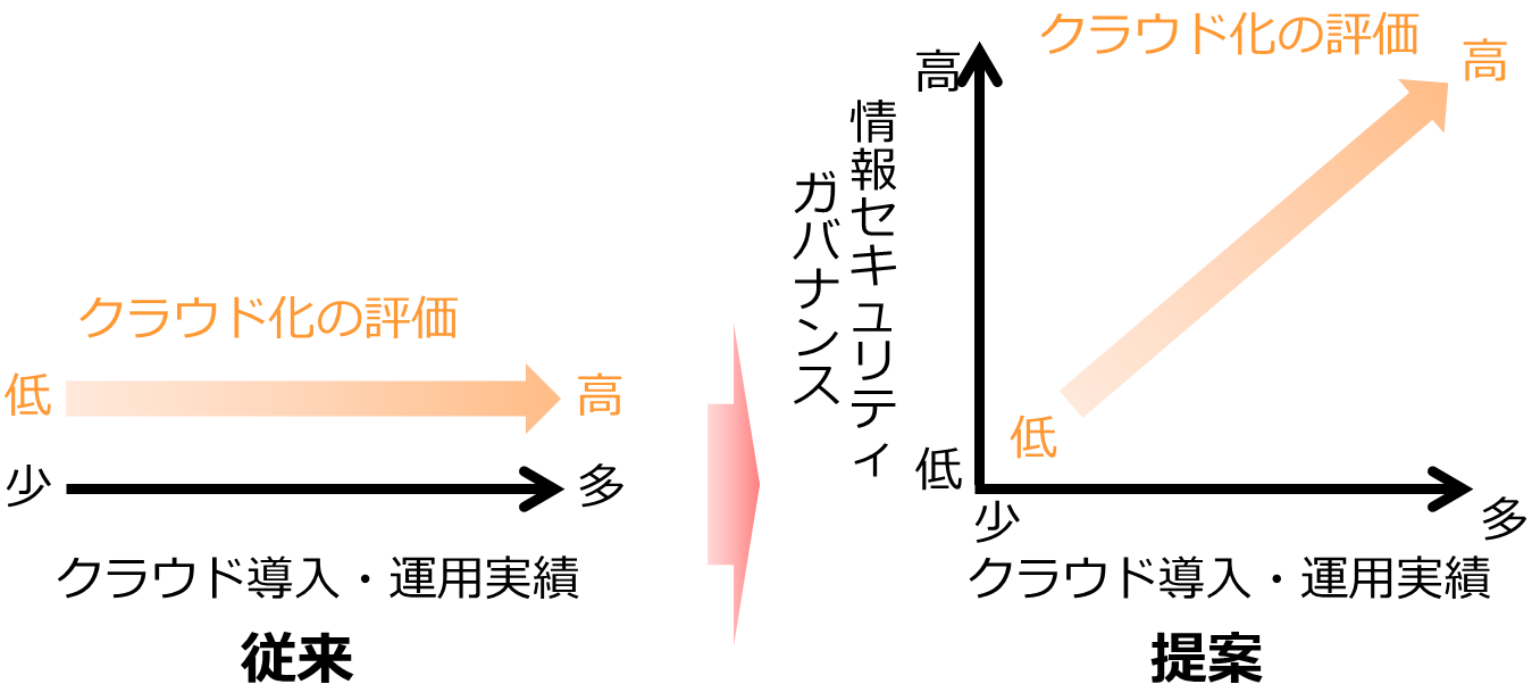
渡邉英伸

広島大学 情報メディア教育研究センター

広島大学

はじめに

- **発表概要**
  - 2016年度および2017年度に学術機関の情報セキュリティガバナンスの実態調査を実施
  - 評価モデルの説明[1][2]および実態調査結果・事後アンケート結果の報告



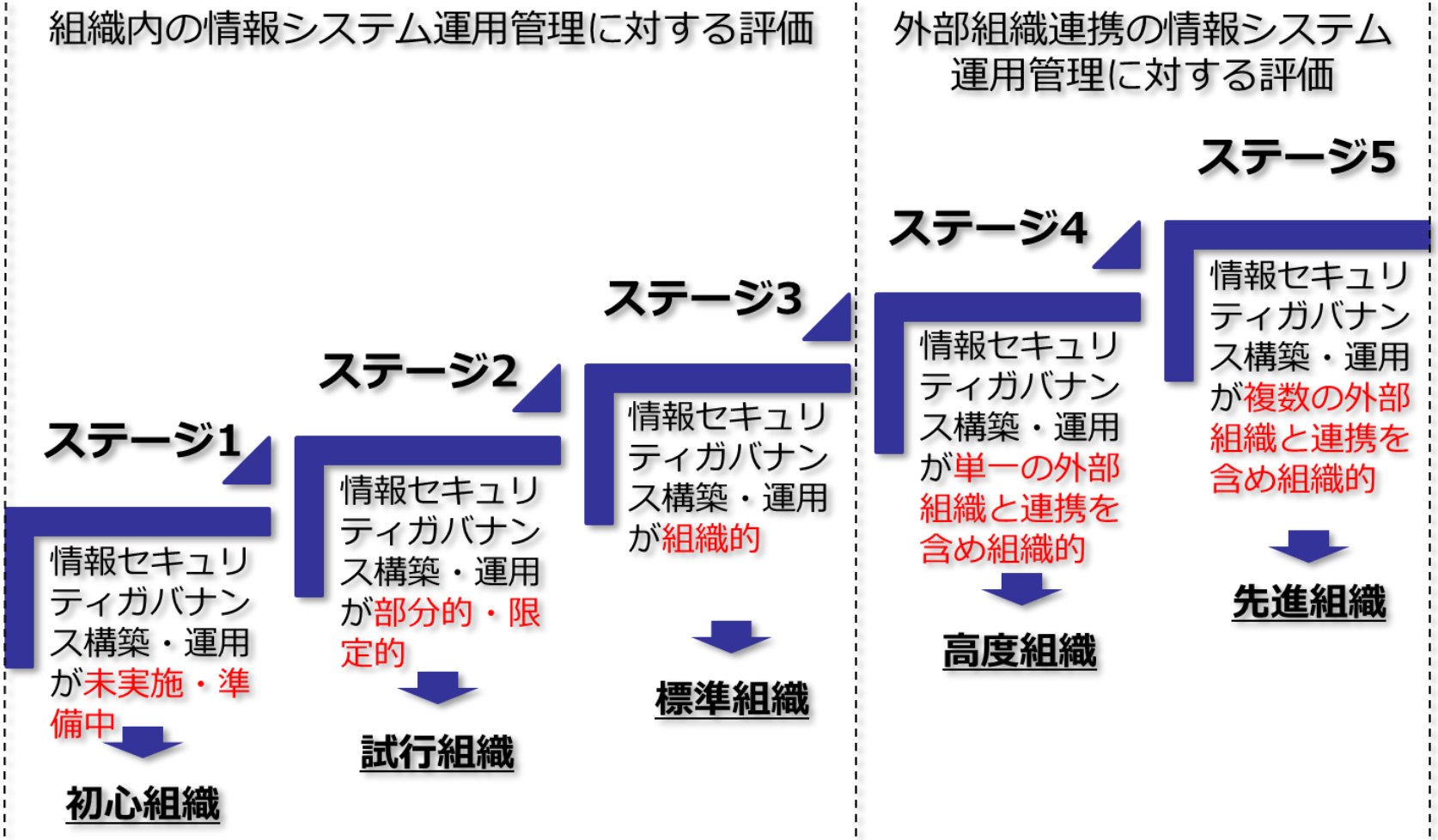
[1]渡邉英伸，他，“学術機関におけるクラウド化成熟度モデルに関する検討” 大学ICT推進協議会2016年度年次大会論文集, 2016.
[2]渡邉英伸，他，“クラウドサービス利用に向けた学術機関のための情報セキュリティガバナンスの実態調査” 情報処理学会研究報告, Vol.2017-IOT-36, No.19, 2017.

情報セキュリティガバナンス評価モデル

広島大学

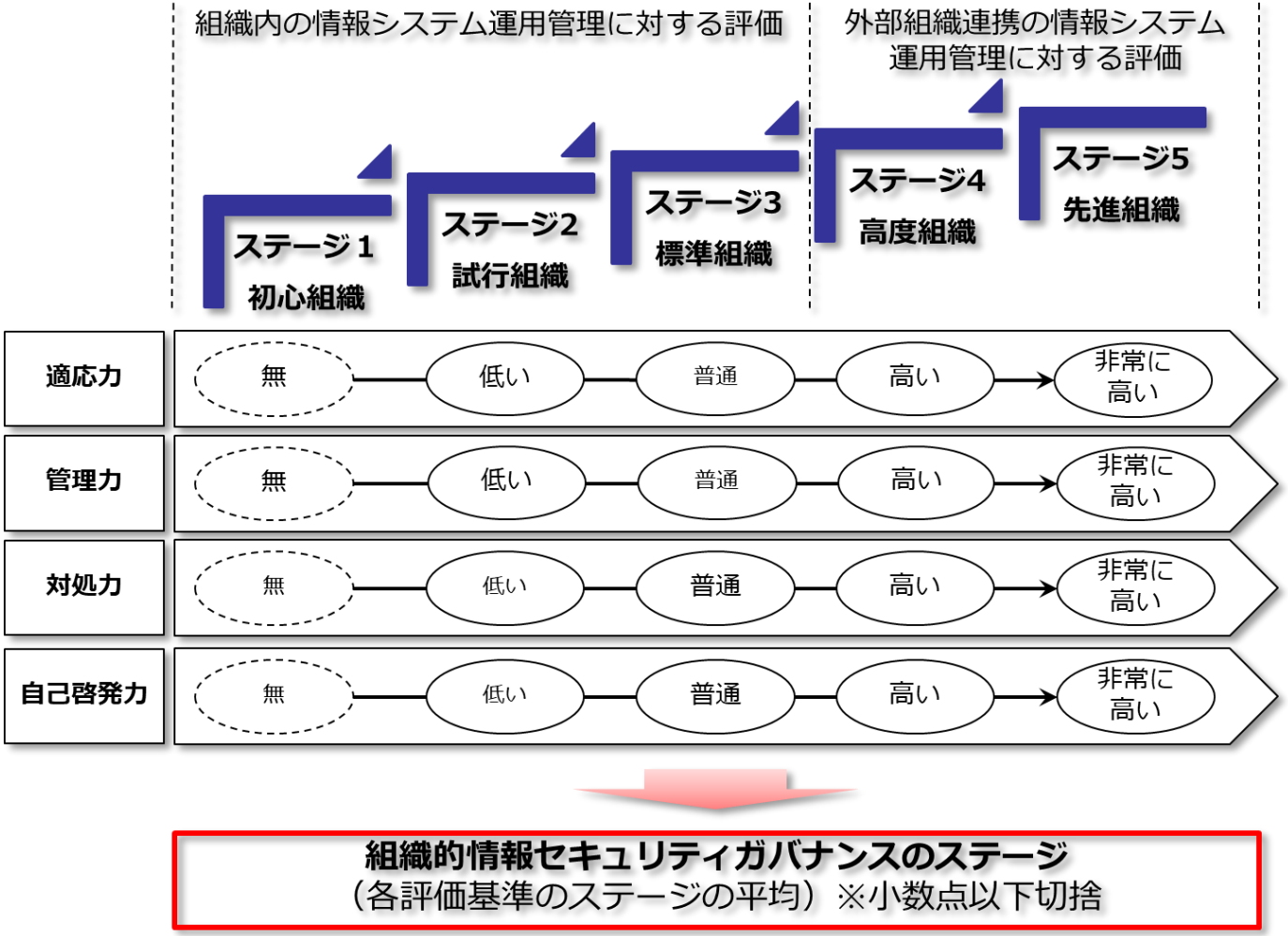
提案評価モデル

- 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定量的に評価する



ステージ求め方

- 4つの評価基準の各ステージレベルの平均を最終的なステージレベルとする（総合評価）



4つの評価基準（能力）

広島大学

- **適応力：**
  - 既存の情報システム運用管理が変化することに対して，情報セキュリティ制度の適応範囲を合わせられることを判断する評価基準
  - ➢ 適切な情報セキュリティ制度の整備できるか否か
- **管理力：**
  - 情報セキュリティの統括体制で示される担当組織が共同して諸規則等の順守を示す運用が可能であることを判断する評価基準
  - ➢ 適切な情報セキュリティマネージメントが実施できるか否か
- **対処力：**
  - 迅速な情報セキュリティインシデントの対処及び対応の評価・見直し・改善が可能であることを判断する評価基準
  - ➢ 適切な情報セキュリティインシデント管理が実施できるか否か
- **自己啓発力：**
  - 組織全体の情報セキュリティの向上を促す制度および統括体制であることを判断する評価基準
  - ➢ 適切な情報セキュリティマネージメントの教育・人材育成ができるか否か

質問事項

広島大学

25問の質問事項

広島大学

- **対象**
  - 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実際に担当している情報系センター
- **質問内容**
  - ISMS[3]および情報セキュリティガバナンス[4]の重要事項を参考
    - 望まれる水準は国際標準の情報セキュリティ管理規格相当
  - 過去の情報セキュリティ実態調査には無い質問事項を追加
- **質問構成**
  - 組織内の情報システム運用管理に伴う情報セキュリティガバナンスの取り組み状況を把握するための質問がベース
  - 運用管理の外部委託やクラウドサービス利用など外部組織連携に伴う質問をアドオンする

[3] JIPDEC, ISMSユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013)対応- リスクマネジメント編, 2015,
[4] 経済産業省, 情報セキュリティガバナンス導入ガイダンス,

質問事項と評価基準の関係

	問1. 諸規則の策定
	問2. 情報格付けの取り扱い
	問3. 外部委託の取り扱い
	問4. 統括体制の整備
	問5. インシデント対処チームの構築
	問6. クラウドの理解
	問7. クラウド化要求事項の文書化
PLAN	問8. クラウド化要求事項の確認
	問9. セキュリティ対策の実施
	問10. インシデント等の記録
	問11. セキュリティ情報の収集
	問12. セキュリティの点検
	問13. 管理策等の共通化
	問14. 外部事業者への運用委託
DO	問15. クラウドサービスの運用
	問16. リスクアセスメントの実施
	問17. 評価用チェックリストの作成
	問18. インシデント対処の実態
	問19. インシデント対処チームの評価
CHECK	問20. 外部委託の国際基準準拠の把握
	問21. 統括体制の見直し
	問22. セキュリティ監査の実施
	問23. 統括体制内の情報共有
	問24. セキュリティ教育
ACT	問25. インシデント対応訓練

	問1. 諸規則の策定
	問2. 情報格付けの取り扱い
	問4. 統括体制の整備
	問5. インシデント対処チームの構築
	問3. 外部委託の取り扱い
	問7. クラウド化要求事項の文書化
	問6. クラウドの理解
	問8. クラウド化要求事項の確認
	問14. 外部事業者への運用委託
適応力	問15. クラウドサービスの運用
	問9. セキュリティ対策の実施
	問10. インシデント等の記録
	問11. セキュリティ情報の収集
	問12. セキュリティの点検
	問23. 統括体制内の情報共有
	問13. 管理策等の共通化
	問17. 評価用チェックリストの作成
管理力	問16. リスクアセスメントの実施
	問19. インシデント対処チームの評価
	問21. 統括体制の見直し
	問18. インシデント対処の実態
対処力	問20. 外部委託の国際基準準拠の把握
	問24. セキュリティ教育
	問25. インシデント対応訓練
自己啓発力	問22. セキュリティ監査の実施

アドオン

質問事項・選択肢・ステージの関係

広島大学

適応力

問1			
情報システム（※1）の運用管理に関する諸規則（情報セキュリティポリシー、管理策等）を策定していますか？			
選択肢1	選択肢2	選択肢3	選択肢4
策定していない	策定を検討中である	運用管理する部署が個別に策定している	組織共通のものとして策定している
1	1	2	3

管理力

問9							
データ、情報システム、ネットワークへのサイバー攻撃に対して情報セキュリティ対策（※3）を実施していますか？							
選択肢1	選択肢2	選択肢3	選択肢4	選択肢5	選択肢6	選択肢7	選択肢8
実施していない	データ対策のみ実施している	情報システム対策のみ実施している	ネットワーク対策のみ実施している	データ対策・情報システム対策を実施している	データ対策・ネットワーク対策を実施している	情報システム対策・ネットワーク対策を実施している	データ・情報システム・ネットワーク全ての対策を実施している
1	2	2	2	2	2	2	3

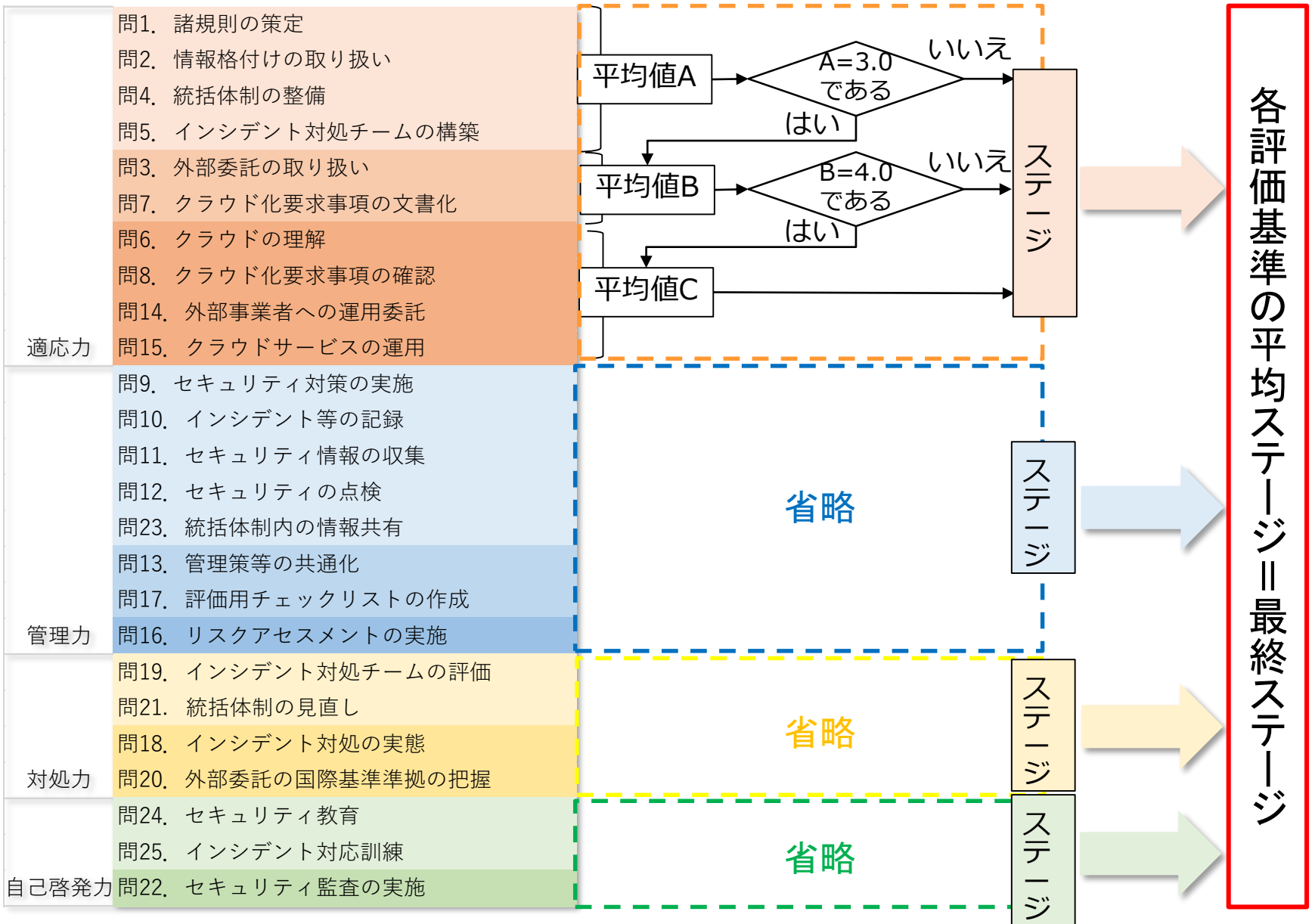
対処力

問19			
過去1年間に発生した情報セキュリティインシデントの発見から最終報告までの対処についての評価を実施していますか？			
選択肢1	選択肢2	選択肢3	選択肢4
実施していない	各部署が個別に実施している	組織として定性的な評価を実施している	組織として定量的な評価を実施している
1	2	3	3

自己啓発力

問24				問22			
情報システムの運用管理に関する諸規則や最新のサイバー攻撃に関する情報を全構成員（利用者）に周知する目的の教育を実施していますか？				情報セキュリティの観点で情報システムの運用管理に関する監査を実施していますか？			
選択肢1	選択肢2	選択肢3	選択肢4	選択肢1	選択肢2	選択肢3	選択肢4
実施していない	各部署が個別に実施している	必要に応じて組織として教育を実施している	定期的に組織として教育を実施している	実施していない	内部監査は実施している	内部監査・外部監査（ISMS等）を実施している	クラウドサービスも含めた内部監査・外部監査を実施している
1	2	3	3	2	3	4	5

最終ステージ算出例


適応力
問1. 諸規則の策定
問2. 情報格付けの取り扱い
問4. 統括体制の整備
問5. インシデント対処チームの構築
問3. 外部委託の取り扱い
問7. クラウド化要求事項の文書化
問6. クラウドの理解
問8. クラウド化要求事項の確認
問14. 外部事業者への運用委託
問15. クラウドサービスの運用
管理力
問9. セキュリティ対策の実施
問10. インシデント等の記録
問11. セキュリティ情報の収集
問12. セキュリティの点検
問23. 統括体制内の情報共有
問13. 管理策等の共通化
問17. 評価用チェックリストの作成
問16. リスクアセスメントの実施
対処力
問19. インシデント対処チームの評価
問21. 統括体制の見直し
問18. インシデント対処の実態
問20. 外部委託の国際基準準拠の把握
自己啓発力
問24. セキュリティ教育
問25. インシデント対応訓練
問22. セキュリティ監査の実施
平均値A
A=3.0である
いいえ
はい
平均値B
B=4.0である
いいえ
はい
平均値C
ステージ
省略
ステージ
省略
ステージ
省略
ステージ
各評価基準の平均ステージ＝最終ステージ

報告書のイメージ

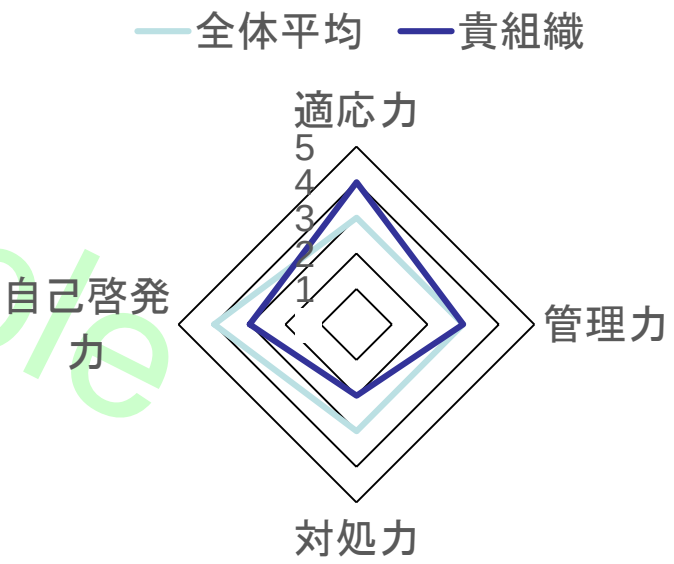
広島大学

「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

内訳説明
・適応力4.0：
・管理力3.0：
・対処力2.0：
・自己啓発力3.0：



今後のポイント
・水準を満たしていない項目を列挙

実態調査結果

広島大学

調査依頼先とスケジュール

広島大学

- **ご賛同および調査に参加して頂いた学術機関に対して実施**
  - 学認クラウド導入支援サービスの参加機関
  - NIIクラウド作業部会のメンバー機関
  - AXIESのクラウド部会
  - その他、知り合いがいる大学等
- **2017年度は31機関が協力（2016年度：28機関）**
- **調査期間：2018年1月5日（金）～2月2日（金）**
  - 実態調査アンケート：2018年1月5日（金）～2月2日（金）
  - 個別報告書返送：2018年3月16日（金）
  - 事後アンケート：2018年3月16日（金）～4月25日（水）
- **調査形式：Webアンケート・電子メール添付**
  - 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依頼

実態調査概要

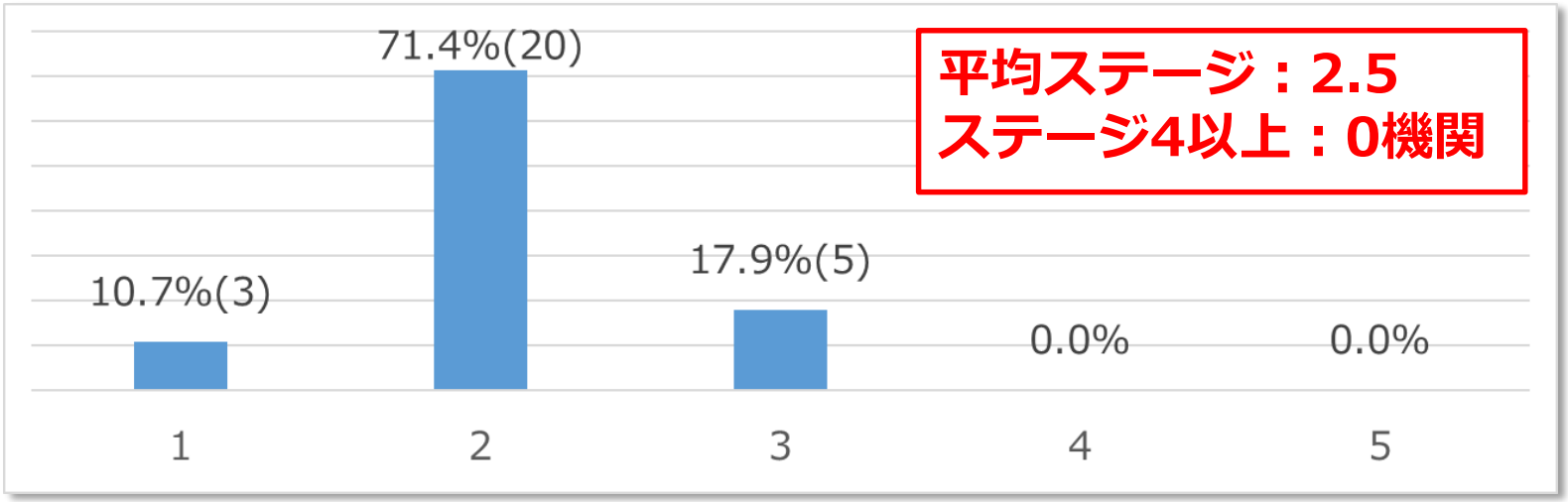
広島大学

- **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%（31／31機関）※昨年度：100%（28／28機関）
- **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
  - 回答条件：任意
  - 有効回答率：58%（18／31機関）※昨年度：82%（23／28機関）
- **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：45%（14／31機関）※昨年度：60%（17／28機関）

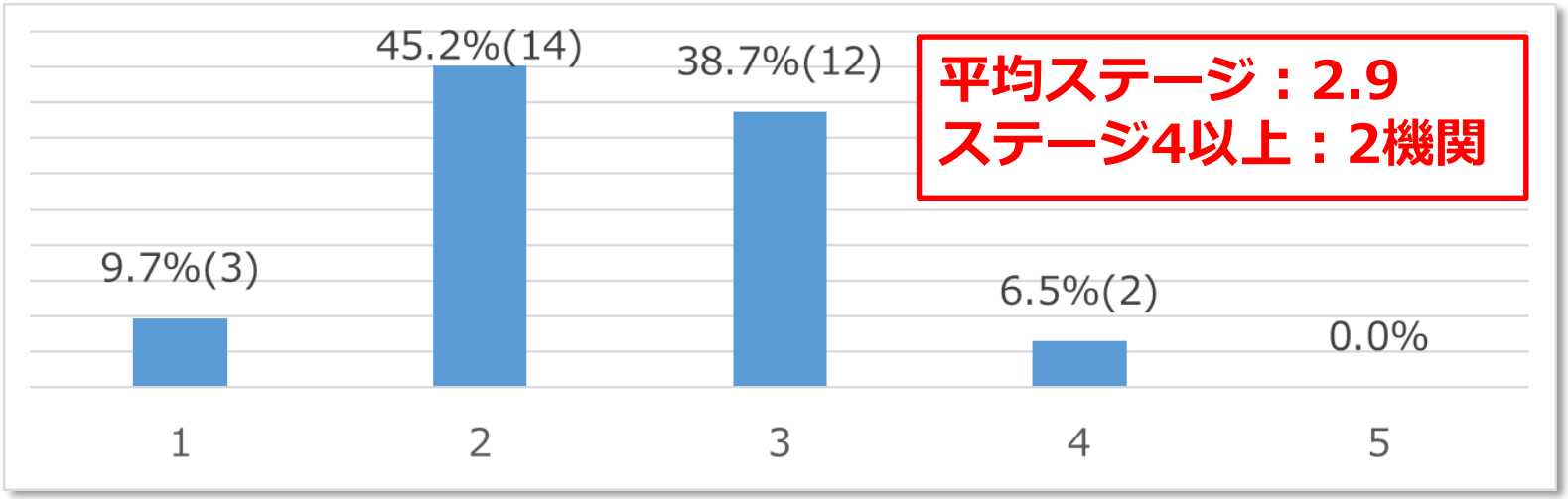
学術機関の最終ステージ

広島大学

2016年度28機関の最終ステージ分布



2017年度31機関の最終ステージ分布

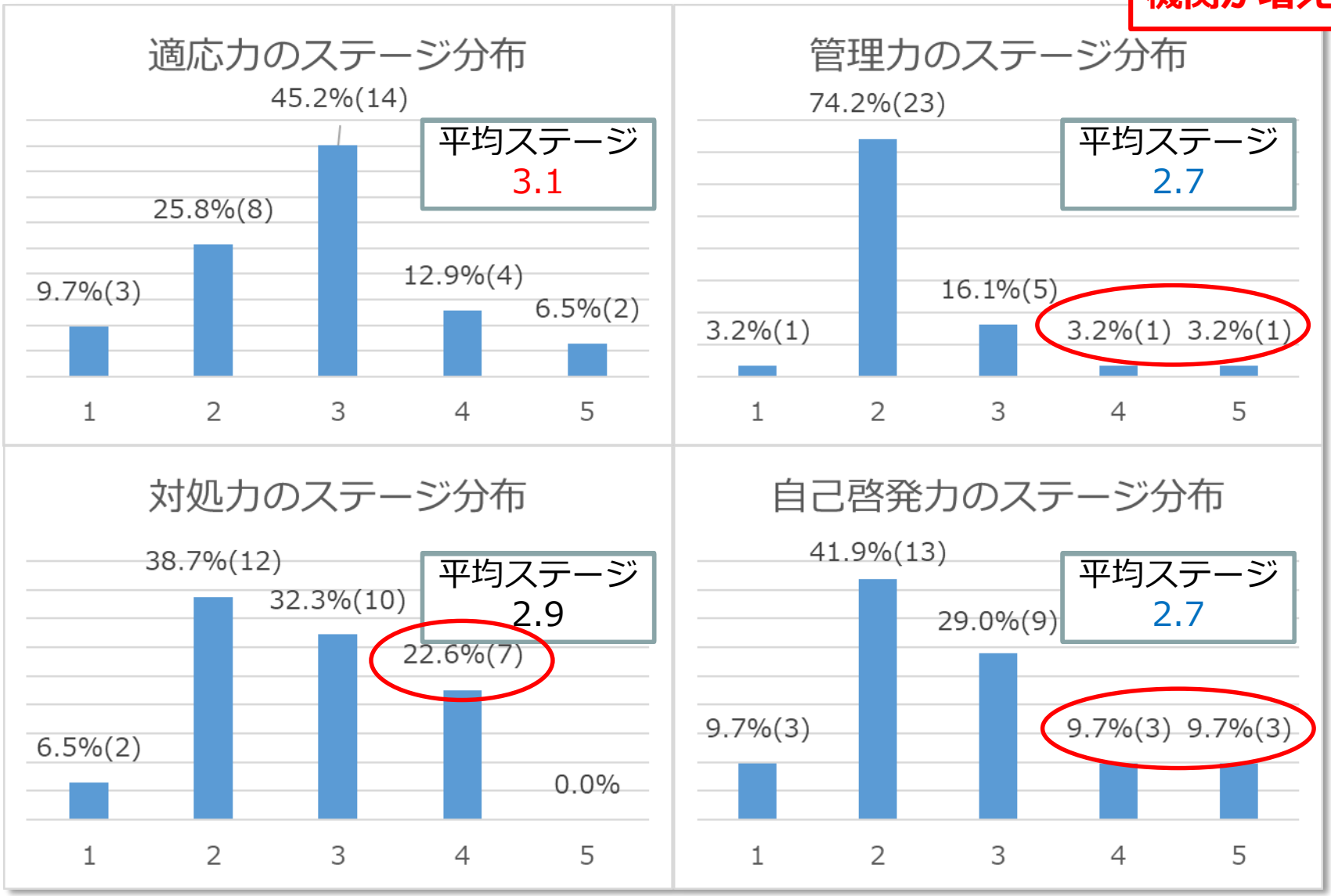


評価基準（能力）別最終ステージ

広島大学

2017年度31機関の最終ステージ分布

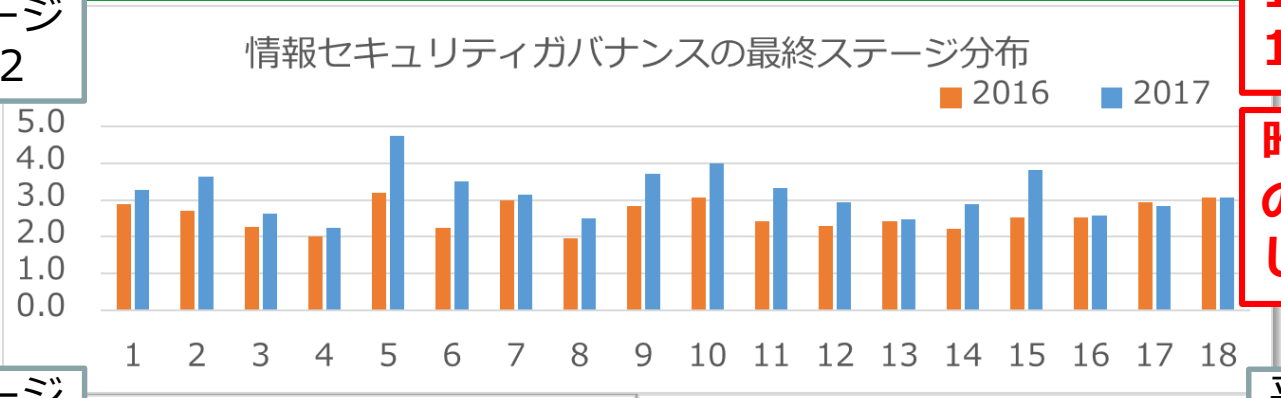
高ステージの機関が増えた



年度別最終ステージ（18機関／31機関）

広島大学

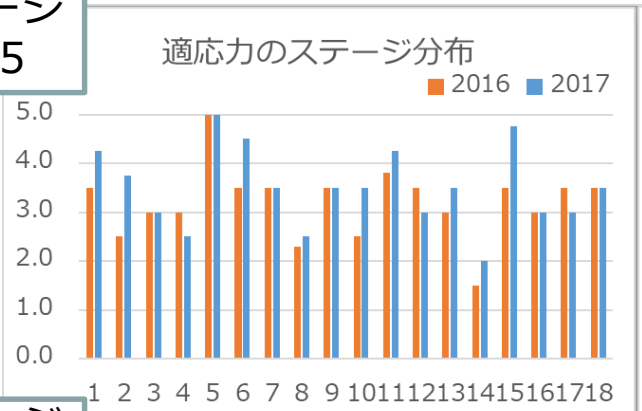
平均ステージ
2.5→3.2



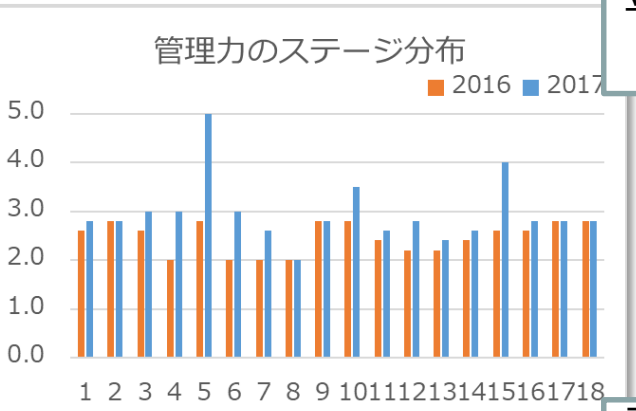
16機関は向上、
1機関が低下

昨年度高ステージの機関がより向上している傾向

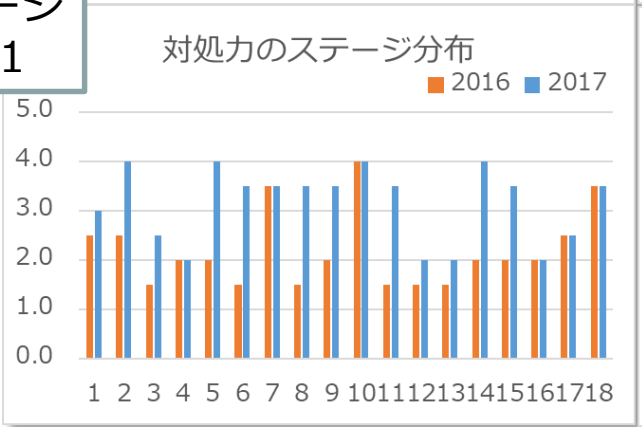
平均ステージ
3.2→3.5



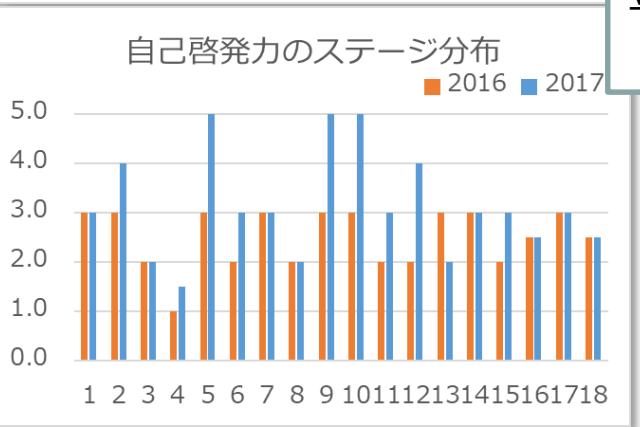
平均ステージ
2.5→3.0



平均ステージ
2.2→3.1



平均ステージ
2.5→3.1



設問別平均最終ステージワーストランキング

広島大学

昨年と同様インシデント対処チームの評価がワースト

ワースト順位（前年度順位）	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．インシデント対処チームの評価	2.3	対処力	
2（3）	問2．情報格付けの取り扱い	2.4	適応力	
3（8）	問12．セキュリティ点検の実施	2.5	管理力	
4（4）	問25．インシデント対応訓練の実施	2.5	自己啓発力	
5（5）	問9．セキュリティ対策の実施	2.5	管理力	
6（6）	問11．セキュリティ情報の収集	2.6	管理力	
7（14）	問4．統括体制の整備	2.6	適応力	
8（12）	問10．インシデント等の記録	2.7	管理力	
9（15）	問5．インシデント対処チームの構築	2.7	適応力	
10（10）	問24．セキュリティ教育の実施	2.7	自己啓発力	
11（7）	問23．統括体制内の情報共有	2.8	管理力	
12（2）	問21.統括体制の見直し	2.8	対処力	
13（16）	問22．セキュリティ監査の実施	2.9		自己啓発力
14（11）	問1．諸規則の策定	2.9	適応力	
15（9）	問16．リスクアセスメントの実施	3.1		管理力
16（13）	問18．インシデント対処の実態	3.1		対処力
17（19）	問17．評価用チェックリストの作成	3.3		管理力
18（18）	問7．クラウド化要求事項の文書化	3.3		適応力
19（17）	問13．管理策等の共通化	3.4		管理力
20（21）	問3．外部委託の取り扱い	3.4		適応力
21（20）	問8．クラウド化要求事項の確認	3.6		適応力
22（23）	問20．外部委託の国際基準準拠の把握	4.1		対処力
23（22）	問15．クラウドサービスの利用や運用管理の実施	4.2		適応力
24（24）	問6．クラウドの理解の実態	4.3		適応力
25（25）	問14．外部事業者への運用委託の実施	4.6		適応力

統括体制内の情報共有や見直しが改善傾向

外部組織連携における設問ではセキュリティ監査の実施がワースト

リスクアセスメントの実施が改善傾向

事後アンケート結果

広島大学

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%（23／31機関）※昨年度：100%（28／28機関）

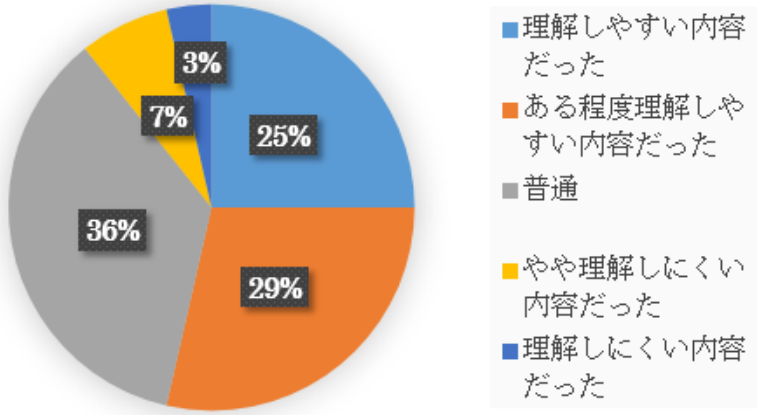
質問1、報告書、取り組みに対する評価の内容に限定し紹介

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**
  - 用語が不明確や感覚的・抽象的な内容があるとの意見を踏まえて見直したことが理解しやすさを維持したと考える

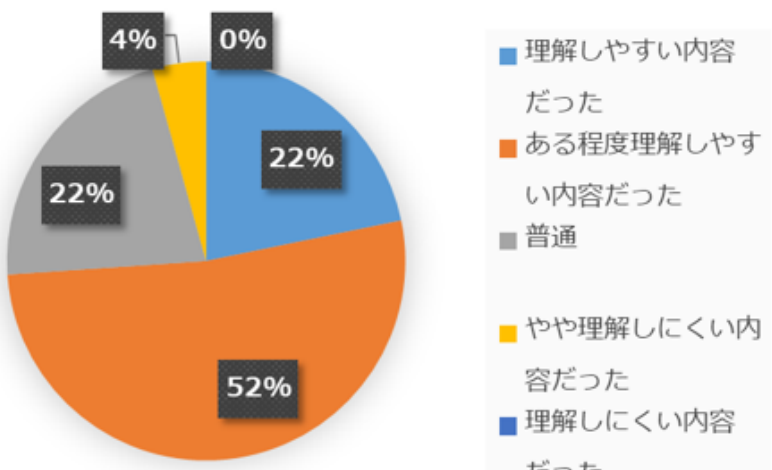
2016年度（N=28）

1	理解しやすい内容だった	7
2	ある程度理解しやすい内容だった	8
3	普通	10
4	ある程度理解しにくい内容だった	2
5	理解しにくい内容だった	1



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

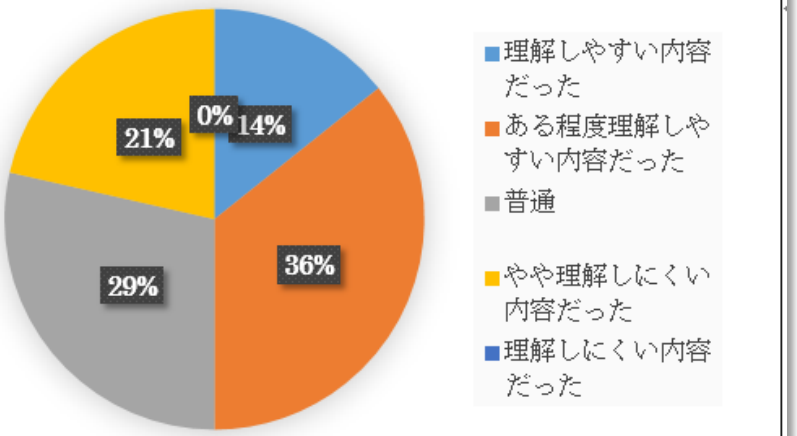


質問1の選択肢の内容は理解しやすいものでしたか？

- **選択肢も全体的に理解しやすい内容だった模様**
  - 前回いくつかの質問の選択肢に悩む・判断が難しいとのコメントを踏まえて見直したことが理解しやすさを維持したと考える

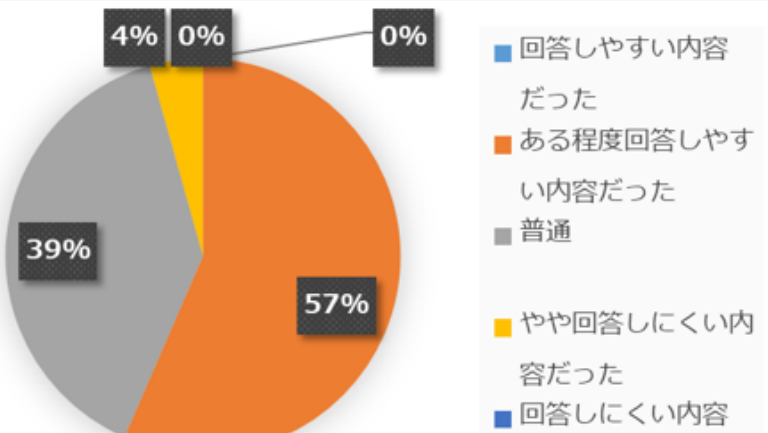
2016年度（N=28）

1	理解しやすい内容だった	4
2	ある程度理解しやすい内容だった	10
3	普通	8
4	ある程度理解しにくい内容だった	6
5	理解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

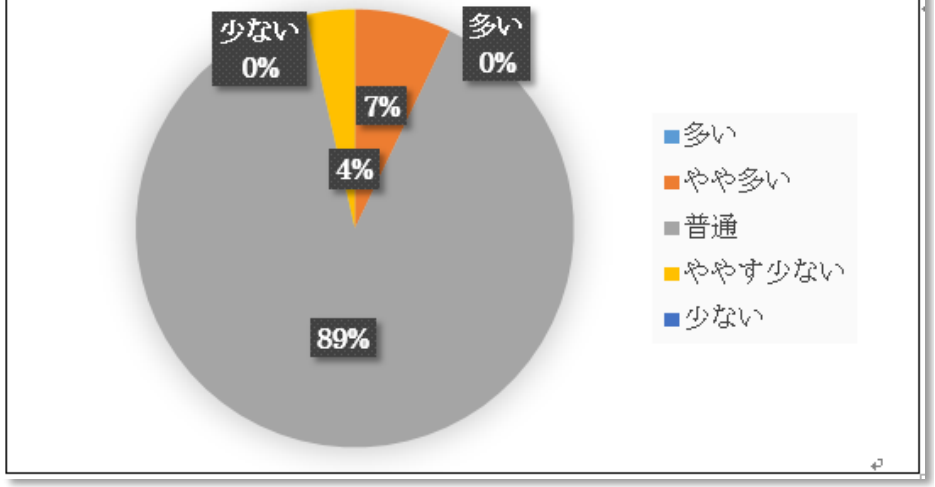


質問1の質問数は適量でしたか？

- **25問の問題数は適切だった模様**
  - 一部10問以内を希望する意見もあったが多くの機関が負担が無いというコメントを頂いた

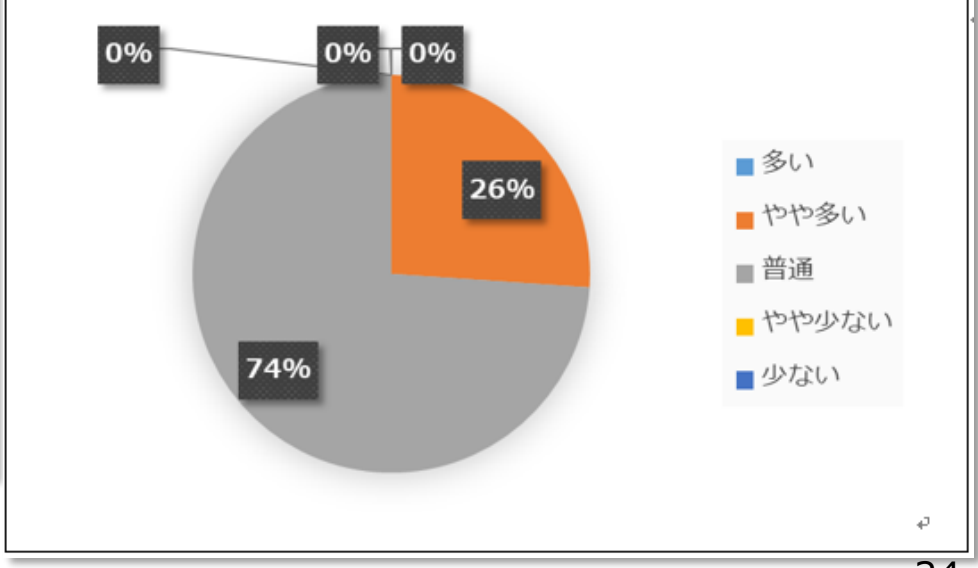
2016年度（N=28）

1	多い	0
2	やや多い	2
3	普通	25
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

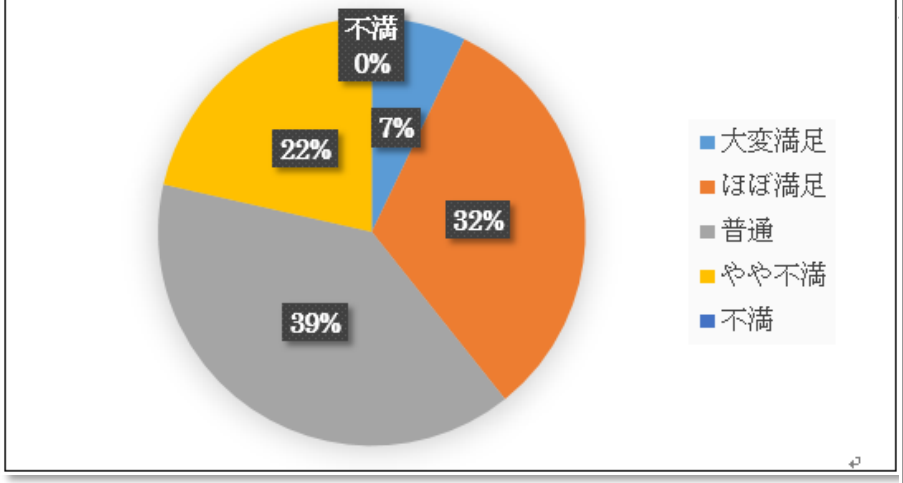


報告書の満足度はいかがでしたか？

- **報告書は全体的に満足の高い内容だった模様**
  - 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一方で、一般論過ぎで具体的な対策の根拠にするには不足の意見を頂いた

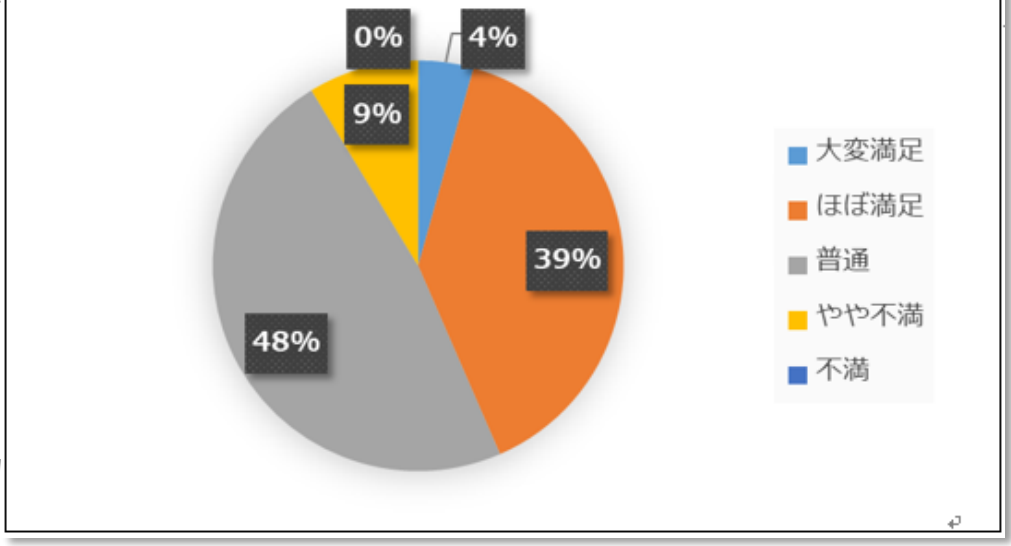
2016年度（N=28）

1	大変満足	2
2	ほぼ満足	9
3	普通	11
4	やや不満	6
5	不満	0



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

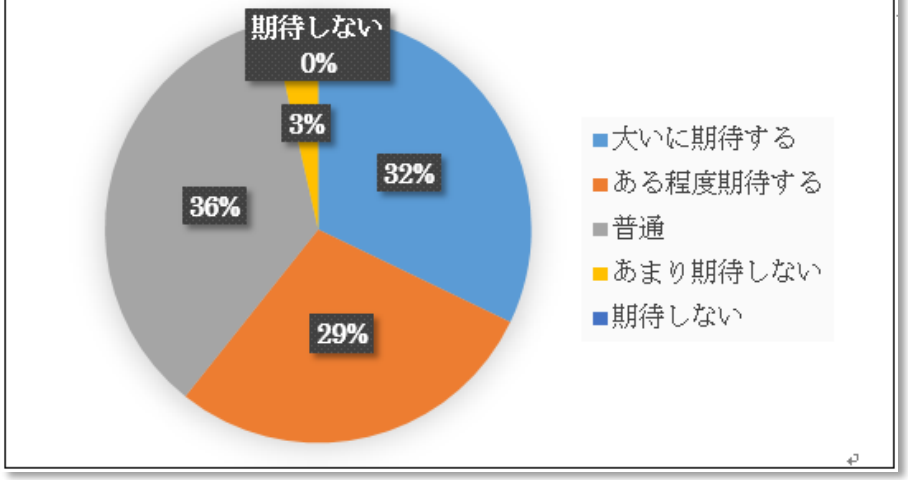


実態調査の取り組みに対しての期待はいかがですか？

- **取組は全体的に期待されている模様**
  - 継続を希望する機関が多い一方で、全国展開、他機関の状況や事例の紹介、各機関への今後の対応や必要事項の明確化などの要望を頂いた

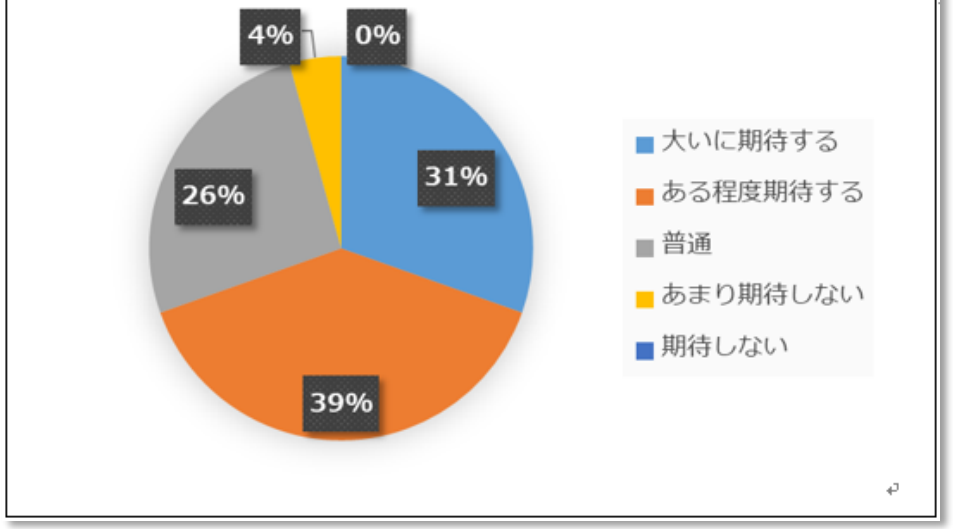
2016年度（N=28）

1	大いに期待する	9
2	ある程度期待する	8
3	普通	10
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（学術機関の特徴？）

- **情報セキュリティガバナンスの実行性は高くない傾向**
  - 今回クラウド化の意識が高い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
- **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**
  - PDCAのPlanあるいはDoのフェーズ止まりの傾向があり、PDCAを回せていない機関が見受けられる
- **データへのセキュリティの取組が十分にできていない傾向**
  - 情報の格付け（重要度に応じた取り扱い）に関する事項を定めていない機関が存在
  - 暗号化などデータに対する対策を実施していない機関も多々いる
- **組織的な共通化・共有化が十分にできていない傾向**
  - 特に情報資産管理において他の部署への確認も必要や情報関係委員会の委員では知り得ない情報が必要とする実態がある

今後の課題

- **分析結果の充実**
  - 条件が似た結果との比較によって、自組織の状況がより明確になると考えられる。
  - 評価基準別、質問別の平均値からの差分がわかるグラフを追加するなど。
- **フィードバック情報の充実**
  - 各機関の具体的な対策の根拠につながる付加情報を提供する必要があると考えられる。
  - 他機関で行われた過去の対策事例やNIIのクラウド導入支援サービスを紹介するなど
- **説明会の実施**
  - 実態調査の目的や意図を多くの機関に知ってもらい調査に協力してもらうことが重要と考える。
  - 大学ICT推進協議会（AXIES）年次大会など

まとめ

- **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の実態調査の評価モデルを説明**
  - ISMSなどの重要事項がベース
  - 組織内および外部組織連携の運用管理のセキュリティガバナンスの実態を段階的に把握する質問構成

- **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中、以下の要件を満たしていくことが今後の課題
    - 条件が似た結果との比較など分析結果の充実
    - 過去の対策事例、クラウド導入支援サービスを紹介など各機関の具体的な対策の根拠につながるフィードバックの付加情報の提供
    - 全国展開などに向けた説明会の実施