大学等におけるクラウドサービス利用シンポジウム2017@広島, 2017/3/10

クラウドサービス利用に向けた情報セキュリティガバナンス実態調査に関する取り組み

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

発表内容

広島大学

- クラウド利用実態調査の現状と課題
- 情報セキュリティガバナンス評価モデル
- アンケート質問事項
- アンケート実施結果の一部紹介
- まとめ

*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.
**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.

はじめに

広島大学

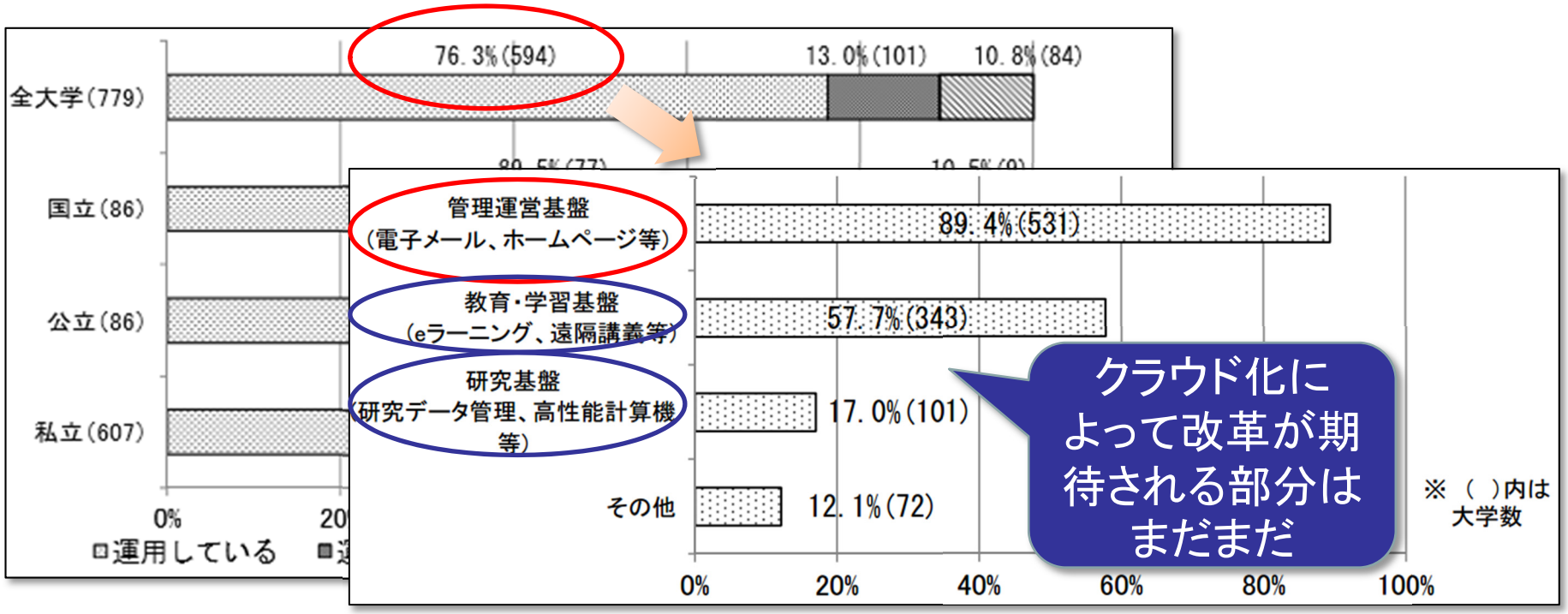
- **学術機関においてもクラウドの活用が求められる時代**
  - アカデミッククラウドに関する検討会(H24年度),文科省
  - 先導的な教育体制構築事業(H26～H28年度),文科省

- **学術機関のクラウド利用実態調査が多く実施されている**
  - コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド（平成25年度）【一般公開】
    - 主管：文部科学省、実施：九州大学ほか
    - 対象：国公私立大学、研究所783組織
  - クラウドコンピューティングの運用状況及び導入計画等（平成26年度）【非公開】
    - 主管：文部科学省、実施：国立情報学研究所(NII)
    - 対象：国立大学86校
  - 学術情報基盤実態調査（クラウド関連は平成24年度～）【一般公開】
    - 主管・実施：文部科学省
    - 対象：国公私立大学779校（国立86、公立86、私立607）
  - 国立大学法人情報系センター協議会調査書（クラウド関連は平成23年度～）【限定公開】
    - 主管・実施：国立大学法人情報系センター協議会(NIPC)
    - 対象：国立大学74校（国立大学法人情報系センター協議会加盟校）

平成27年度学術情報基盤実態調査

広島大学

- **クラウドの運用（平成27年5月1日現在）**
  - 目的：国公私立大学の大学図書館やコンピュータ・ネットワーク・クラウド環境の現状を明らかにし、その改善・充実への基礎資料とする
- **学術機関がクラウドを利用するために、改善・充実の手助けとなる基礎資料となっているか？**
  - 具体的な情報や有用性が不明では…



学術機関のクラウド活用を妨げる要因

広島大学

- **学術機関がクラウド化をしない1番の理由**
  - 情報セキュリティの不安　＞　コストの不安

数年間変化なし

パブリッククラウドサービスを利用しない、あるいは利用を妨げている理由	学術機関 (n=594)	企業 (n=722)
情報漏洩などセキュリティに不安がある	49.2	34.0
クラウドの導入に伴う既存システムの改修コストが大きい	19.0	22.6
ニーズに応じたアプリケーションのカスタマイズができない	19.0	12.8
ネットワークの安定性に対する不安がある	17.8	15.2
法制度や所属機関の諸規則が整っていない	16.8	6.3
メリットが分からない、判断できない	16.0	21.5
通信費用がかさむ	9.8	10.9
クラウドの導入によって所属機関の諸規則との整合性に支障をきたす	8.9	6.2
必要がない	8.2	41.2
その他	8.2	5.8

<出展>
コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド（セキュリティ分野）：http://www.icer.kyushu-u.ac.jp/ac
平成24年通信利用動向調査（企業編）（総務省）：http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

クラウド利用を後押しするためには？

広島大学

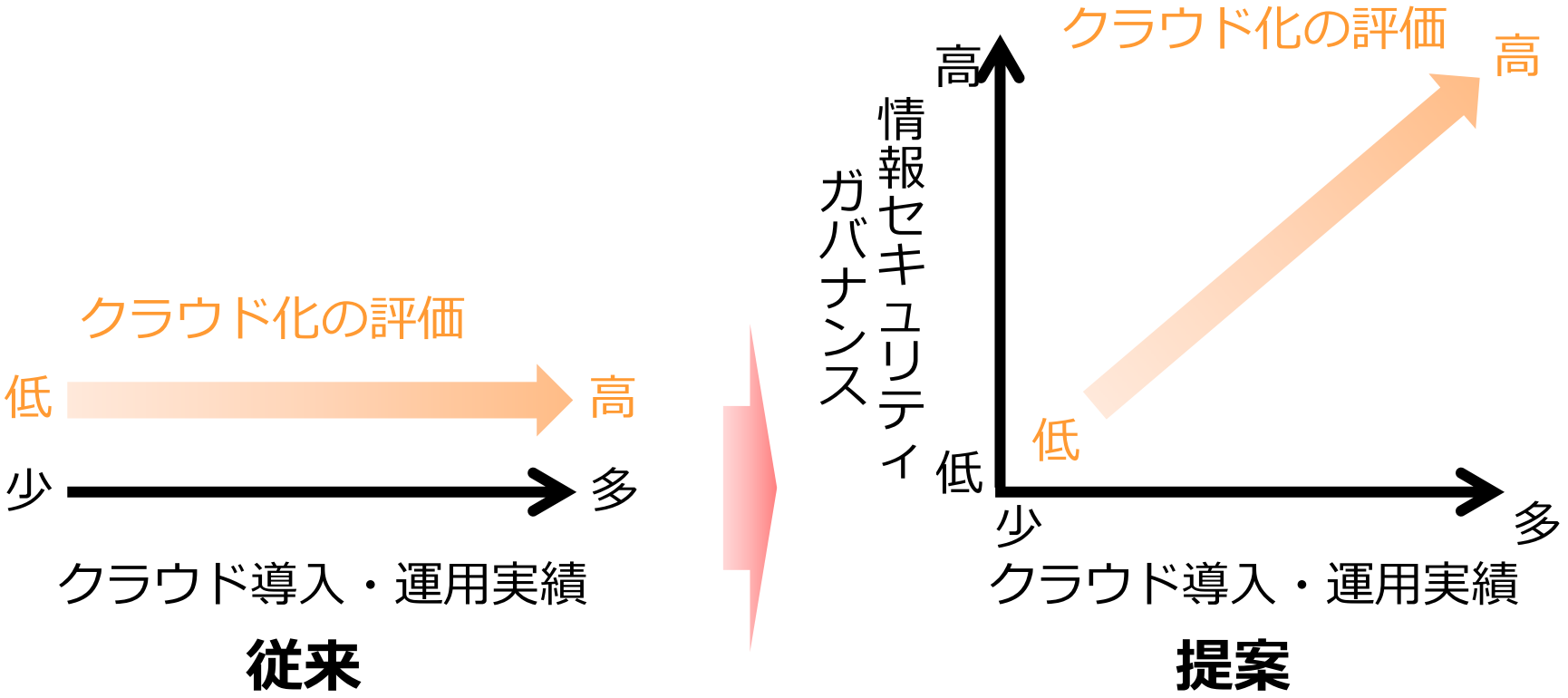
- **回答組織のセキュリティの取り組みを客観的かつ定量的に評価し、個々に適切なフィードバック情報を提供する調査が必要**
  - クラウドを導入する以前に自組織のセキュリティの取り組みは望まれる水準をみたしているか？
  - 自組織のセキュリティレベルは学術機関全体の位置付けはどの辺りか？
  - クラウド利用に向けて次に何をすればよいか？

回答組織（学術機関）がクラウド利用を促進するための新たな評価モデルが必要

クラウドサービス利用推進に向けて

広島大学

- クラウド利用の推進と公平な評価のため、**情報セキュリティガバナンス**をベースとした評価モデルを提案



情報セキュリティガバナンス
評価モデル

広島大学

評価モデルの要求事項

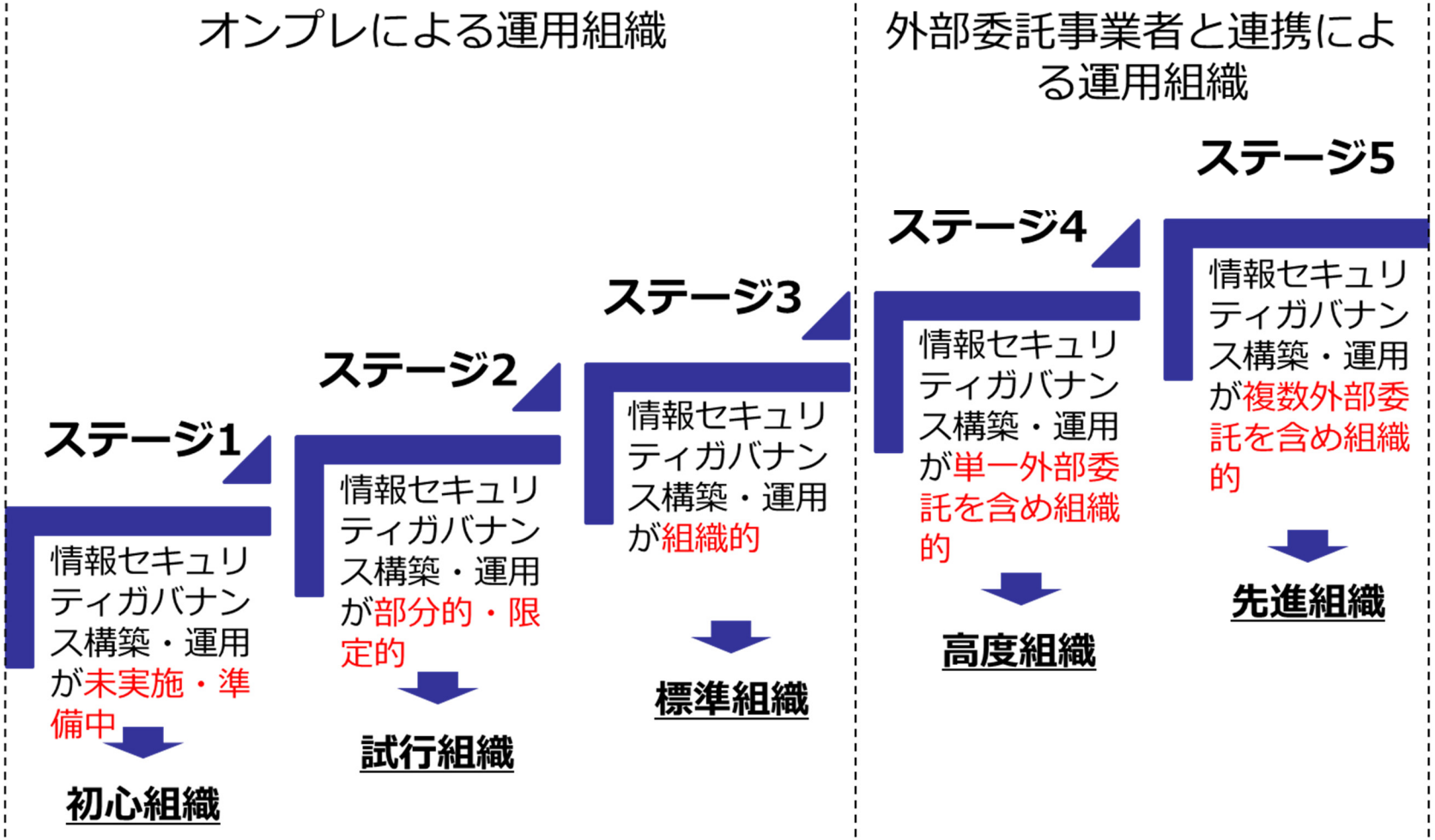
広島大学

- **学術機関全体として一定水準の情報セキュリティレベルの確保とその状況が確認できること**
  - 全体の傾向を把握するため
- **自組織のセキュリティレベルの現状と望まれる水準との差を把握し目標を明確にできること**
  - 個別の現状を把握するため
- **実態調査の回答を続けることで徐々に情報セキュリティレベルの向上を促すことが可能なこと**
  - フィードバックによりステップアップを支援するため
- **クラウドサービスを利用する場合としない場合の差を把握し目標を明確にできること**
  - クラウド利用の推進に必要な要素を示すため

提案評価モデル

広島大学

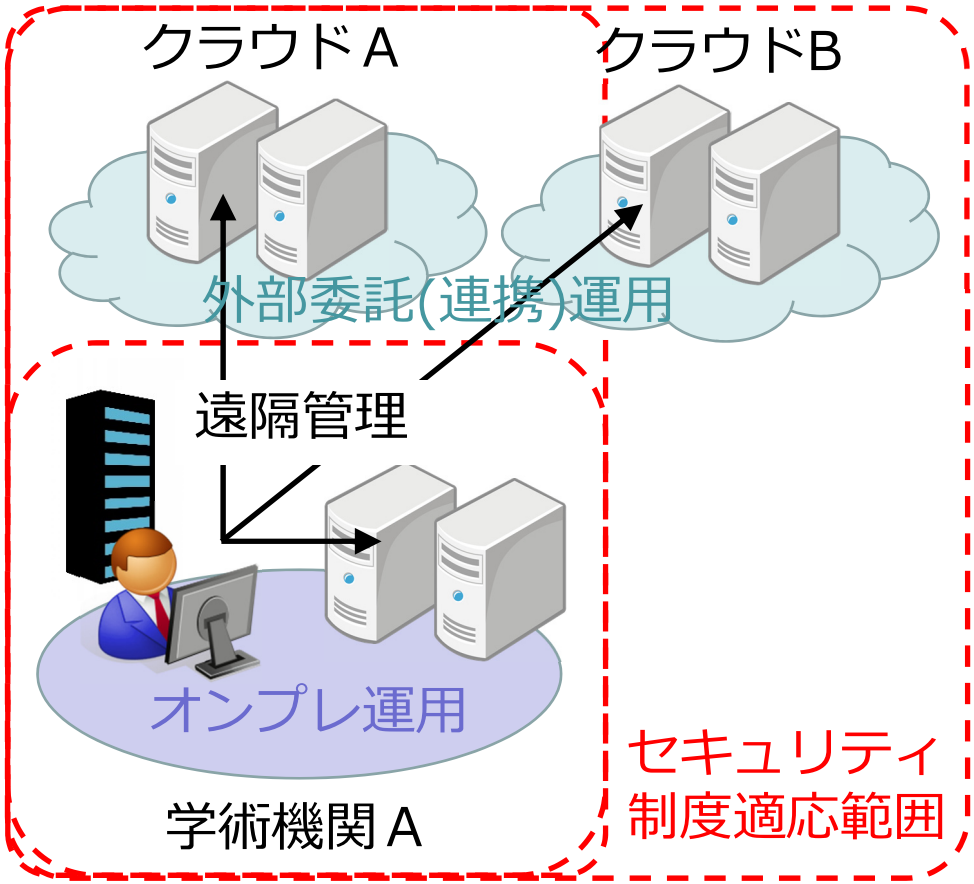
- 5つのステージレベルで組織の情報セキュリティガバナンスを定量的に評価する

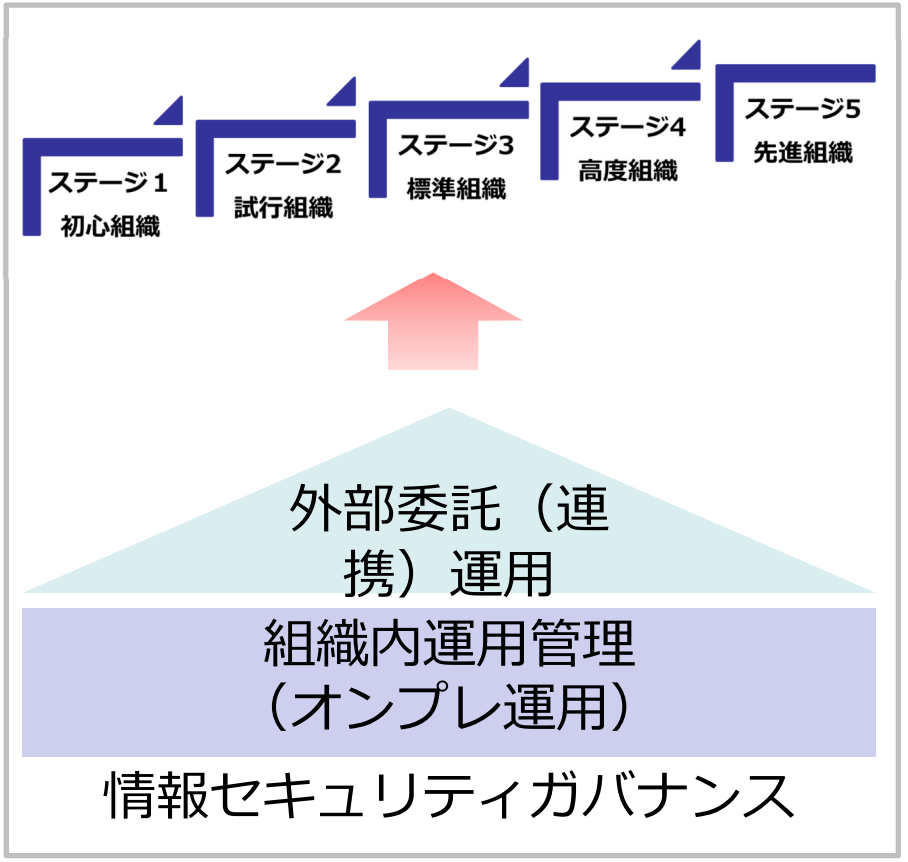


提案評価モデルの特徴

広島大学

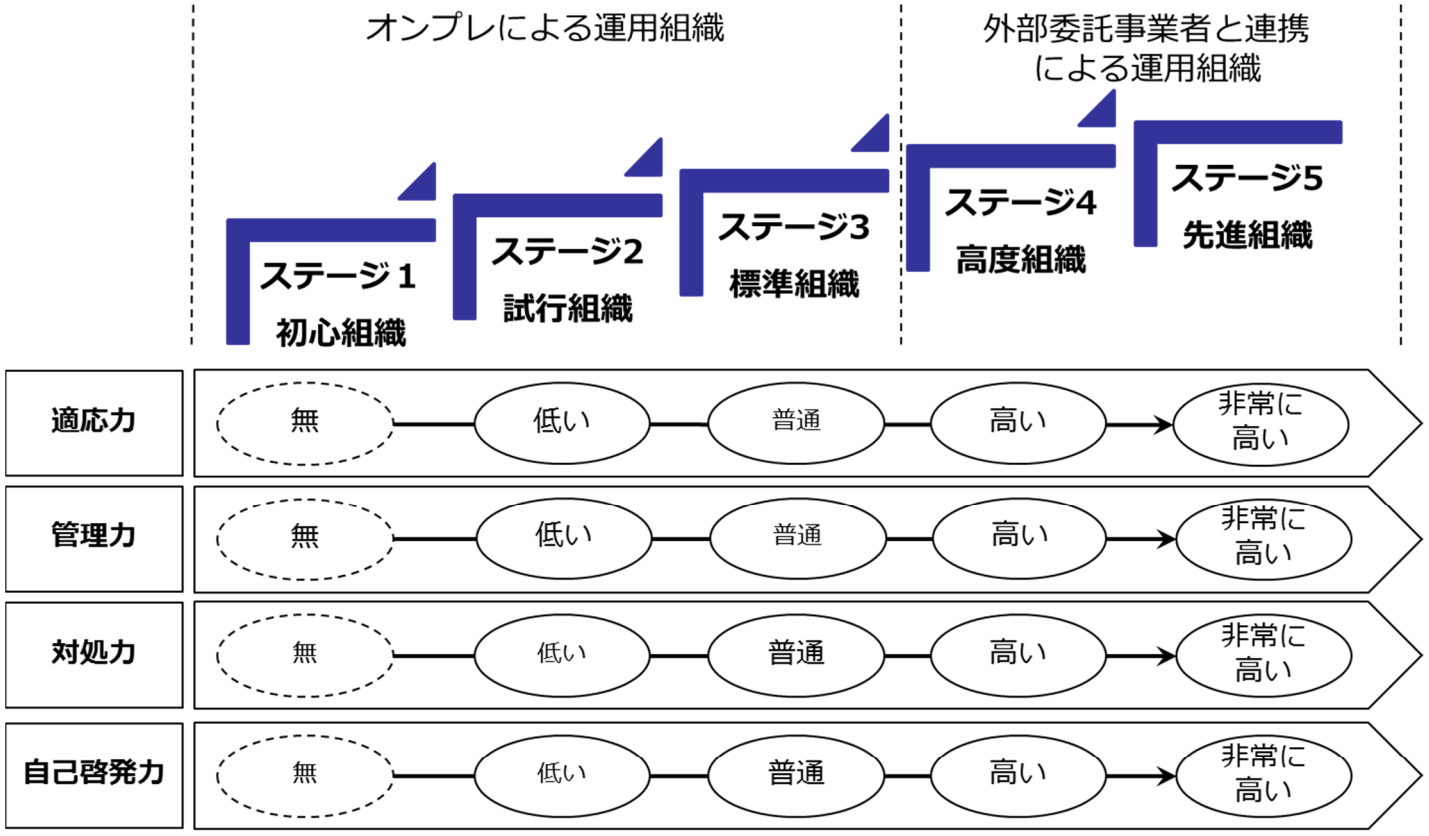
- **情報セキュリティガバナンスの多段評価方式**
  - １段階：組織内運用管理（オンプレ運用）に対する評価
  - ２段階：外部委託（連携）運用に対する加点減点評価





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）



最終ステージ（各評価基準のステージレベルの平均）※小数点第2四捨五入

4つの評価基準

広島大学

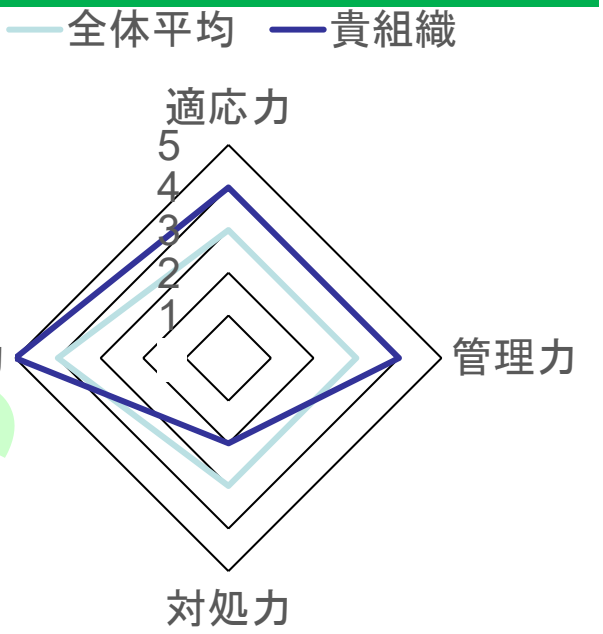
- **適応力：**
  - 既存の情報システム運用管理が変化することに対して，情報セキュリティ制度の適応範囲を合わせられることを判断する評価基準
    - 適切な情報セキュリティ制度の整備できるか否か
- **管理力：**
  - 情報セキュリティの統括体制で示される担当組織が共同して諸規則等の順守を示す運用が可能であることを判断する評価基準
    - 適切な情報セキュリティマネージメントが実施できるか否か
- **対処力：**
  - 迅速な情報セキュリティインシデントの対処及び対応の評価・見直し・改善が可能であることを判断する評価基準
    - 適切な情報セキュリティインシデント管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

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
（適応力：4、管理力：4、対処力：2、自己啓発力：5）



概説
・

内訳説明
・適応力：
・管理力：
・対処力：
・自己啓発力：

今後のポイント
・情報セキュリティガバナンスの観点：
・クラウドサービス導入・運用の観点：

アンケート質問事項

広島大学

アンケート質問（25問作成）

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**
  - オンプレ運用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
  - クラウドサービス利用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（PLAN）:8問

広島大学

- **組織的セキュリティ制度・体制状況とクラウドに対する理解・準備等の実態を把握する質問**

I	情報セキュリティに関する組織的な制度・体制の実態について
問1	情報システム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？
問2	情報システムの運用管理に関する諸規則の中で、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ますか？
問3	情報システムの運用管理に関する諸規則の中で、情報処理を外部委託する場合の情報セキュリティに関する事項を定めていますか？
問4	情報セキュリティ委員会やCISO等を中心とする情報セキュリティの統括体制を整備していますか？
問5	CSIRT等の情報セキュリティインシデントを対応するチームを構築していますか？
問6	クラウドサービスの特性や利用におけるメリット・デメリットを把握していますか？
問7	適切なクラウドサービスを利用するための情報セキュリティ関連の要求要件（標準仕様）の文書化（ガイドライン作成等）をしていますか？
問8	文書化した情報セキュリティ関連の要求要件（標準仕様）とクラウドサービスのセキュリティ対策状況の対応を確認をしていますか？

質問事項（DO）：7問

広島大学

- **組織的セキュリティ対策・情報セキュリティ運用状況とクラウドの導入・運用実態を把握する質問**

Ⅱ	情報セキュリティに関する導入・運用の実態について
問9	情報、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（※1）を実施していますか？
問10	情報セキュリティインシデント（文部科学省等の外部組織に報告するまでに至った事案）・情報セキュリティトラブル（文部科学省等の外部組織に報告するまでに至らなかった事案）の発覚から解決までの対応事項に関する記録を残していますか？
問11	警察や情報セキュリティ企業等の外部組織と連携して、脆弱性や脅威等の情報セキュリティに関連する最新情報を収集していますか？
問12	脆弱性診断等、情報システムの情報セキュリティ点検を実施していますか？
問13	管理策等を作成し、特定の運用管理者に依存しない運用・管理の共通化を実施していますか？あるいは属人化を解消する工夫を実施していますか？
問14	情報システムの運用を外部の事業者に委託しているものはありますか？
問15	クラウドサービスを運用していますか？

※1　情報に対する情報セキュリティ対策はデータの暗号化やバックアップ等を示します。情報システムに対するセキュリティ対策はウイルス対策ソフトの導入やアクセス制御の設定等を示します。ネットワークに対する情報セキュリティ対策はファイヤウォールやIPS(侵入検知システム)の設置等を示します。

質問事項（CHECK）：5問

広島大学

- **情報セキュリティインシデント対応チームの対応状況と国際標準セキュリティ基準の対応確認の実態を把握する質問**

Ⅲ	情報セキュリティに関する評価・点検の実態について
問16	情報、情報システム、ネットワークの情報セキュリティ特性（機密性・完全性・可用性）に対する情報セキュリティリスクアセスメントを実施していますか？
問17	適切なクラウドサービスを利用するための情報セキュリティ関連の要求要件（標準仕様）を満たすことを確認するチェックリストを作成していますか？
問18	発生した情報セキュリティインシデント（文部科学省等の外部組織に報告するまでに至った事案）に対して対処はできていますか？
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？
問20	契約している外部委託業者は国際的な情報セキュリティ基準(ISMS、CSゴールドマーク等)を満たしていますか？

質問事項（ACT）：5問

広島大学

- **情報セキュリティ教育・訓練状況と内部・外部監査の実態を把握する質問**

Ⅳ	情報セキュリティに関する見直しの実態について
問21	情報システムの運用管理に関する諸規則や統括体制（制度・体制的セキュリティ）、情報セキュリティ対策（システム的セキュリティ）等についての見直し・改善を過去1年間に実施しましたか？
問22	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？
問23	情報セキュリティ委員会やCISO等を中心とする情報セキュリティの統括体制の中で情報共有ができていますか？
問24	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？
問25	情報セキュリティインシデント対応関係者の対応力を向上する目的の教育・訓練を実施していますか？

補足：過去の調査から関連する質問を抽出

広島大学

クラウド導入・運用と情報セキュリティに関連する質問事項

- **コミュニティで紡ぐ次世代大学ICT環境としてのアカデミッククラウド（平成25年度）**
  - A) 情報システムの運用に関して定めている諸規則の有無
  - B) 情報の格付けに関して定めている事項の有無
  - C) 情報処理を外部委託する場合に関して定めている事項の有無
  - D) 情報システムの運用に関する諸規則を構成員に周知するための教育の有無
  - E) 情報セキュリティマネジメントシステムの認証取得の有無
  - F) 過去1年間に発生したセキュリティインシデントの有無
  - G) 利用しているクラウドサービスの種類
  - H) パブリッククラウドサービス利用の有無
  - I) 構成員のパブリッククラウドサービス利用状況の把握の可否
- **クラウドコンピューティングの運用状況及び導入計画等（平成26年度）**
  - J) 利用しているクラウドの種類（プライベートクラウド、パブリッククラウド、コミュニティクラウド）
  - K) クラウド運用している情報システムの用途（管理運営基盤、教育・学習基盤・図書館、研究基盤、その他ICT基盤）
  - L) クラウド運用している情報システムの種類
  - M) 情報システムの学外運用の有無
- **国立大学法人情報系センター協議会調査書（平成28年度）**
  - N) セキュリティポリシー策定の有無
  - O) 情報セキュリティマネジメントにおいて中心となる組織の有無
  - P) CSIRTなどの専門組織の構築の有無、または既存の組織による対応の可否
  - Q) 標的型攻撃対策として特別に実施した訓練の有無
  - R) 利用しているクラウドの種別（パブリッククラウド、プライベートクラウド、学外ネットワークからの利用）
  - S) クラウド運用している情報システムの用途（管理運営基盤、教育・学習基盤・図書館、研究基盤、その他ICT基盤）
  - T) クラウド運用している情報システムの種類
  - U) 導入前後のパブリッククラウド、プライベートクラウドの評価（ハードウェアコスト、ソフトウェアコスト、管理者の負担、システムの消費電力、障害復旧に要する時間、データの安全性）

補足：評価基準と過去の質問との対応付け

広島大学

- **評価基準１：組織的制度・体制の有無**
  - 情報セキュリティポリシー：　A), N)
  - 情報セキュリティ管理組織：　O)
  - 情報セキュリティ対応体制：　P)
  - 情報格付け・外部委託関連文書：　B), C)
- **評価基準２：組織的導入・運用の有無**
  - 情報システムの学外運用：　M)
  - パブリッククラウドサービスの導入：　H)
  - 大規模クラウドサービスの導入：　K), L), S), T)
  - 複数クラウドサービス形態の導入：　G), J), R)
- **評価基準３：組織的管理・統制の有無**
  - リスクアセスメント・管理の実施：　－
  - 研修・教育・訓練の実施：　D), Q)
  - インシデント発生時の対応：　F), I)
  - クラウド化の確認項目の文書化：　－
- **評価基準４：内部監査・外部評価等の有無**
  - 内部監査の実施：　－
  - 情報セキュリティガバナンスの評価・改善：　E)
  - クラウド導入前後の評価：　U)
  - 国際標準クラウドセキュリティ基準対応確認　－

重複しない質問を洗い出した

不足の質問を洗い出した

ステージ判定表(質問事項・能力ステージ関係)

広島大学

評価基準	設問番号	質問事項	評価軸（ステージ）				
			1	2	3	4	5
適応力	問1	情報システム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？	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	組織共通のものとして策定している	組織共通のものとして策定している
	問2	情報システムの運用管理に関する諸規則の中で、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ますか？	定めていない 定めることを検討中である	運用管理する部署が個別に定めている	組織共通のものとして定めている	組織共通のものとして定めている	組織共通のものとして定めている
	問4	情報セキュリティ委員会やCISO等を中心とする情報セキュリティの統括体制を整備していますか？	整備していない 整備を検討中である	統括体制は整備しているがトップダウン型ではない	トップダウン型の統括体制を整備している	トップダウン型の統括体制を整備している	トップダウン型の統括体制を整備している
	問5	CSIRT等の情報セキュリティインシデントを対応するチームを構築していますか？	構築していない 構築を検討中である	対応チームは構築しているが専門ではない(既存の部署等で対応)	対応チームは構築しているが専門ではない(既存の部署等で対応) 専門の対応チームを構築している	対応チームは構築しているが専門ではない(既存の部署等で対応) 専門の対応チームを構築している	対応チームは構築しているが専門ではない(既存の部署等で対応) 専門の対応チームを構築している
	問3	情報システムの運用管理に関する諸規則の中で、情報処理を外部委託する場合の情報セキュリティに関する事項を定めていますか？			定めていない 定めることを検討中である 運用管理する部署が個別に定めている	組織共通のものとして定めている	組織共通のものとして定めている
	問14	情報システムの運用を外部の事業者に委託しているものはありますか？			委託していない(オンプレミス運用形態)	情報システムを学内の情報センター等に集約する運用形態で委託しているものがある	情報システムを学外の施設に集約する運用形態で委託しているものがある 情報システムの内容により、学内外の施設に集約する運用形態で委託しているものがある
	問7	適切なクラウドサービスを利用するための情報セキュリティ関連の要求要件（標準仕様）の文書化（ガイドライン作成等）をしていますか？			文書化をしていない 文書化をすることを検討中である 導入する部署が個別に文書化をしている	組織共通のものとして文書化をしている	組織共通のものとして文書化をしている
	問6	クラウドサービスの特性や利用におけるメリット・デメリットを把握していますか？			把握していない 把握を検討中である	最低限把握している	網羅的に把握している
	問8	文書化した情報セキュリティ関連の要求要件（標準仕様）とクラウドサービスのセキュリティ対策状況の対応を確認をしていますか？			確認していない 確認を検討中である 一部のみ確認している	1つのクラウドサービス事業者において全て確認している	複数のクラウドサービス事業者において全て確認している
	問15	クラウドサービスを運用していますか？			運用していない 契約した各部署が個別に運用している	1つのクラウドサービス事業者と契約し、組織的なサービスとして運用している	複数のクラウドサービス事業者と契約し、組織的なサービスとして運用している

ステージ判定表(質問事項・能力ステージ関係)

広島大学

評価基準	設問番号	質問事項	評価軸（ステージ）				
			1	2	3	4	5
管理力	問9	情報、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（※1）を実施していますか？	実施していない	情報対策のみ実施している	情報・情報システム・ネットワーク全ての対策を実施している	情報・情報システム・ネットワーク全ての対策を実施している	情報・情報システム・ネットワーク全ての対策を実施している
				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			
				情報対策・情報システム対策を実施している			
				情報対策・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			
	問10	情報セキュリティインシデント（文部科学省等の外部組織に報告するまでに至った事案）・情報セキュリティトラブル（文部科学省等の外部組織に報告するまでに至らなかった事案）の発覚から解決までの対応事項に関する記録を残していますか？	残していない	セキュリティインシデントのみ残している	セキュリティインシデント・トラブルのどちらも残している	セキュリティインシデント・トラブルのどちらも残している	セキュリティインシデント・トラブルのどちらも残している
				セキュリティトラブルのみ残している			
	問11	警察や情報セキュリティ企業等の外部組織と連携して、脆弱性や脅威等の情報セキュリティに関連する最新情報を収集していますか？	収集していない	連携はしていないが収集している	1カ所と連携して収集している	1カ所と連携して収集している	1カ所と連携して収集している
					複数と連携して収集している	複数と連携して収集している	複数と連携して収集している
	問12	脆弱性診断等、情報システムの情報セキュリティ点検を実施していますか？	実施していない	当事者に任せている(組織的に管理していない)	定期的に実施している	定期的に実施している	定期的に実施している
				必要に応じて実施している			
	問23	情報セキュリティ委員会やCISO等を中心とする情報セキュリティの統括体制の中で情報共有ができていますか？	できていない	できているが、改善の余地が大いにある	できている	できている	できている
	問16	情報、情報システム、ネットワークの情報セキュリティ特性（機密性・完全性・可用性）に対する情報セキュリティリスクアセスメントを実施していますか？		実施していない	実施している	外部委託運用のものを含めて実施している	複数の外部委託運用のものを含めて実施している
	問13	管理策等を作成し、特定の運用管理者に依存しない運用・管理の共通化を実施していますか？あるいは属人化を解消する工夫を実施していますか？			実施していない	共通化(工夫)を組織的に実施しており、効果はある	共通化(工夫)を組織的に実施しており、効果はある
					共通化(工夫)を個々に任せている(組織的に管理していない)		
					共通化(工夫)を組織的に実施しているが、改善の余地がある		
	問17	適切なクラウドサービスを利用するための情報セキュリティ関連の要求要件（標準仕様）を満たすことを確認するチェックリストを作成していますか？			作成していない	組織共通のものとして作成している	組織共通のものとして作成している
					導入する部署が個別に作成している		

ステージ判定表(質問事項・能力ステージ関係)

広島大学

評価基準	設問番号	質問事項	評価軸（ステージ）				
			1	2	3	4	5
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？	実施していない	評価は実施しているが、見直しはしていない	評価および見直しを実施し、反映結果があった場合の対処はすべて完了している	評価および見直しを実施し、反映結果があった場合の対処はすべて完了している	評価および見直しを実施し、反映結果があった場合の対処はすべて完了している
				評価および見直しを実施しているが、反映結果があった場合の対処は一部のみである			
	問21	情報システムの運用管理に関する諸規則や統括体制（制度・体制的セキュリティ）、情報セキュリティ対策（システム的セキュリティ）等についての見直し・改善を過去1年間に実施しましたか？	実施していない	見直しを実施し、反映すべき結果の一部は反映できている	見直しを実施し、反映すべき結果はすべて反映できている	見直しを実施し、反映すべき結果はすべて反映できている	見直しを実施し、反映すべき結果はすべて反映できている
			見直しのみ実施した		見直しを実施し、反映すべき結果は無かった	見直しを実施し、反映すべき結果は無かった	見直しを実施し、反映すべき結果は無かった
	問18	発生した情報セキュリティインシデント（文部科学省等の外部組織に報告するまでに至った事案）に対して対処はできていますか？		できていない	できている	1つの外部委託事業者による運用のものを含めてできている	複数の外部委託事業者による運用のものを含めてできている
				できているが、改善の余地が大いにある			
	問20	契約している外部委託業者は国際的な情報セキュリティ基準(ISMS、CSゴールドマーク等)を満たしていますか？			満たしてしていない	満たしているが、認証は取得していない	満たしており、全ての事業者が認証を取得している
						満たしており、一部の事業者が認証を取得している	

ステージ判定表(質問事項・能力ステージ関係)

広島大学

評価基準	設問番号	質問事項	評価軸（ステージ）				
			1	2	3	4	5
自己啓発力	問24	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？	実施していない	各部署が個別に実施している	定期的に組織として教育を実施している 必要に応じて組織として教育を実施している	クラウドサービスの内容も適宜含めながら定期的に組織として教育を実施している	クラウドサービスの内容も適宜含めながら定期的に組織として教育を実施している
	問25	情報セキュリティインシデント対応関係者の対応力を向上する目的の教育・訓練を実施していますか?	実施していない	各部署が個別に実施している	定期的に組織として教育・訓練を実施している 必要に応じて組織として教育・訓練を実施している	外部委託運用の内容も適宜含めながら定期的に組織として教育・訓練を実施している	外部委託運用の内容も適宜含めながら定期的に組織として教育・訓練を実施している
	問22	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？		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

質問事項と評価ポイント

広島大学

評価軸	質問事項	評価ポイント
適応力	問1：諸規則の策定	ステージ1～3を評価
	問2：情報格付け策定	
	問4：統括体制の整備	
	問5：対応チームの構築	
	問3：外部委託の情報セキュリティ事項策定	ステージ4を評価
	問7：クラウドのセキュリティ対策の確認	
	問6：クラウドの特性の把握	ステージ5を評価
	問8：クラウド化の要求事項の文書化	
	問14：外部委託の実施	
	問15：クラウドサービスの導入・運用状況	

□ アドオン（外部委託連携運用）質問

質問事項と評価ポイント

広島大学

評価軸	質問事項	評価ポイント
適応力	問1：諸規則の策定	ステージ1～3を評価
	問2：情報格付け策定	
	問4：統括体制の整備	
	問5：対応チームの構築	
管理力	問9：情報セキュリティ対策	ステージ1～3を評価
	問10：インシデントの対応記録	
	問11：情報セキュリティ情報の収集	
	問12：情報セキュリティ点検	
	問23：統括体制の情報共有	
	問13：運用管理の共通化	ステージ2～5を評価
	問16：情報セキュリティリスクアセスメント	
	問17：クラウドチェックリストの作成	

□ アドオン（外部委託連携運用）質問

質問事項と評価ポイント

広島大学

評価軸	質問事項	評価ポイント
適応力	問1：諸規則の策定	ステージ1～3を評価
	問2：情報格付け策定	
	問4：統括体制の整備	
	問5：対応チームの構築	
管理力	問9：情報セキュリティ対策	ステージ1～3を評価
	問10：インシデントの対応記録	
	問11：情報セキュリティ情報の収集	
	問12：情報セキュリティ点検	
	問23：統括体制の情報共有	
対処力	問19：早急なインシデント対処	ステージ1～3を評価
	問21：対処チームの見直し・改善	
	問18：情報セキュリティインシデント	ステージ4～5を評価
	問20：国際標準クラウドセキュリティ基準対応の確認	

□ アドオン（外部委託連携運用）質問

質問事項と評価ポイント

広島大学

評価軸	質問事項	評価ポイント
適応力	問1：諸規則の策定	ステージ1～3を評価
	問2：情報格付け策定	
	問4：統括体制の整備	
	問5：対応チームの構築	
管理力	問9：情報セキュリティ対策	ステージ1～3を評価
	問10：インシデントの対応記録	
	問11：情報セキュリティ情報の収集	
	問12：情報セキュリティ点検	
	問23：統括体制の情報共有	
対処力	問19：早急なインシデント対処	ステージ1～3を評価
	問21：対処チームの見直し・改善	
自己啓発力	問24：構成員への教育	ステージ1～3を評価する
	問25：インシデント対応チームの訓練	
	問22：監査の有無	ステージ2～5を評価する

□ アドオン（外部委託連携運用）質問

アンケート実施結果の一部紹介

広島大学

アンケート依頼先とスケジュール

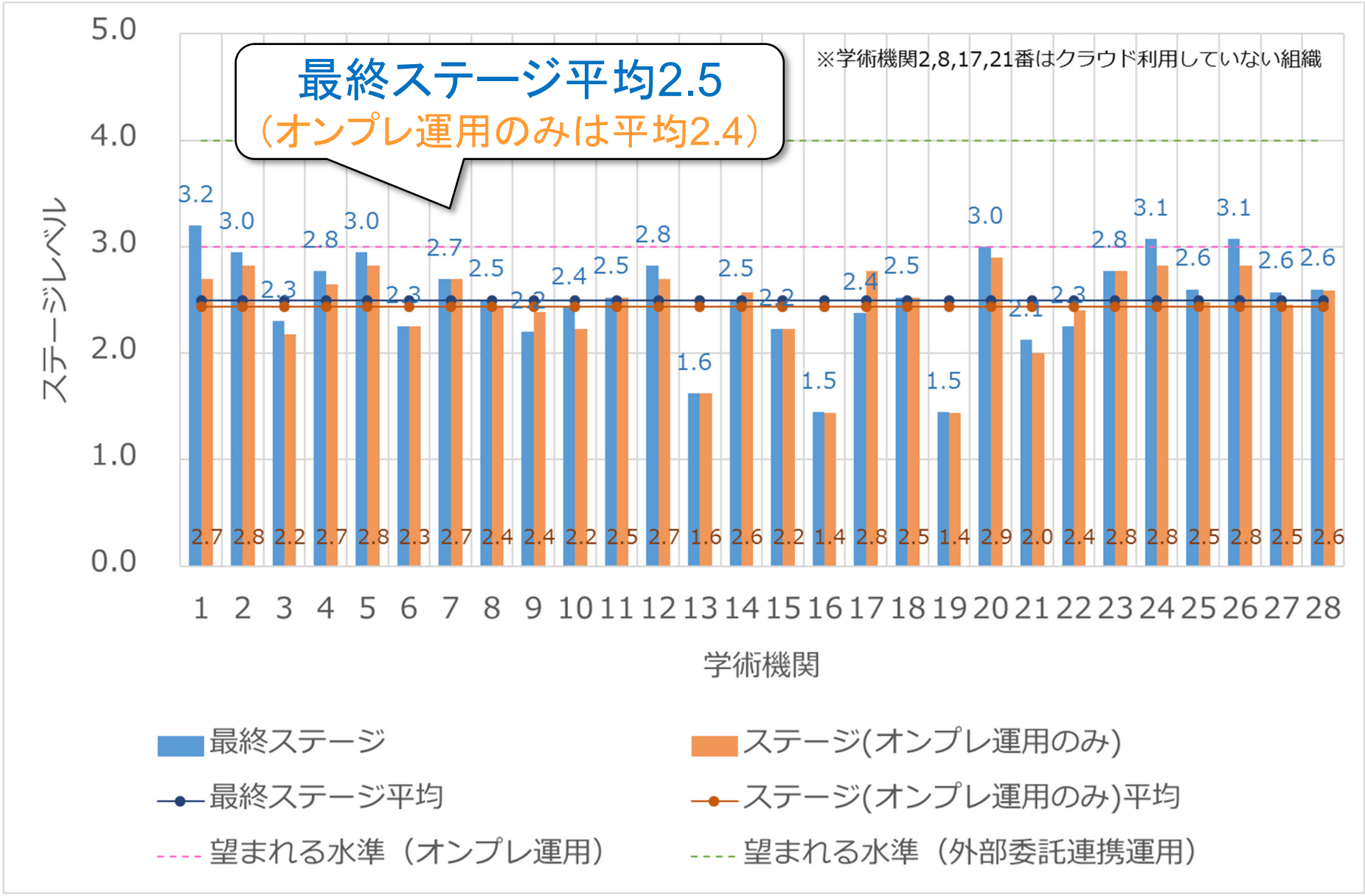
広島大学

- **以下に協力を依頼し、ご賛同および調査に参加して頂いた28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

- **調査スケジュール**
  - 1月18日 ご協力いただける機関への調査票送付
  - 2月3日　調査票回収締切
    - ２月２４日　すべて調査票を回収
  - 3月中旬　評価結果送付

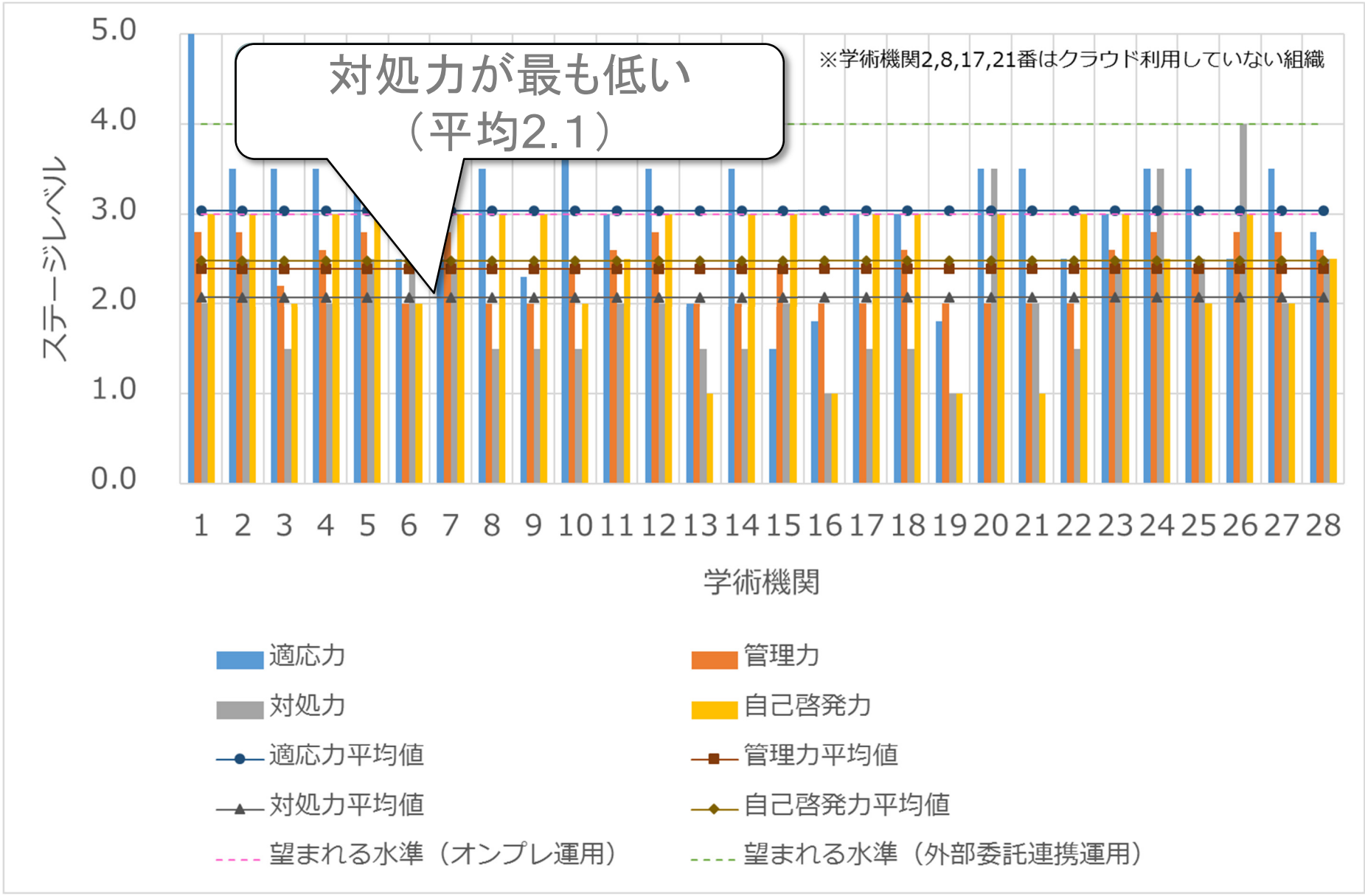
28学術機関の最終ステージ

広島大学

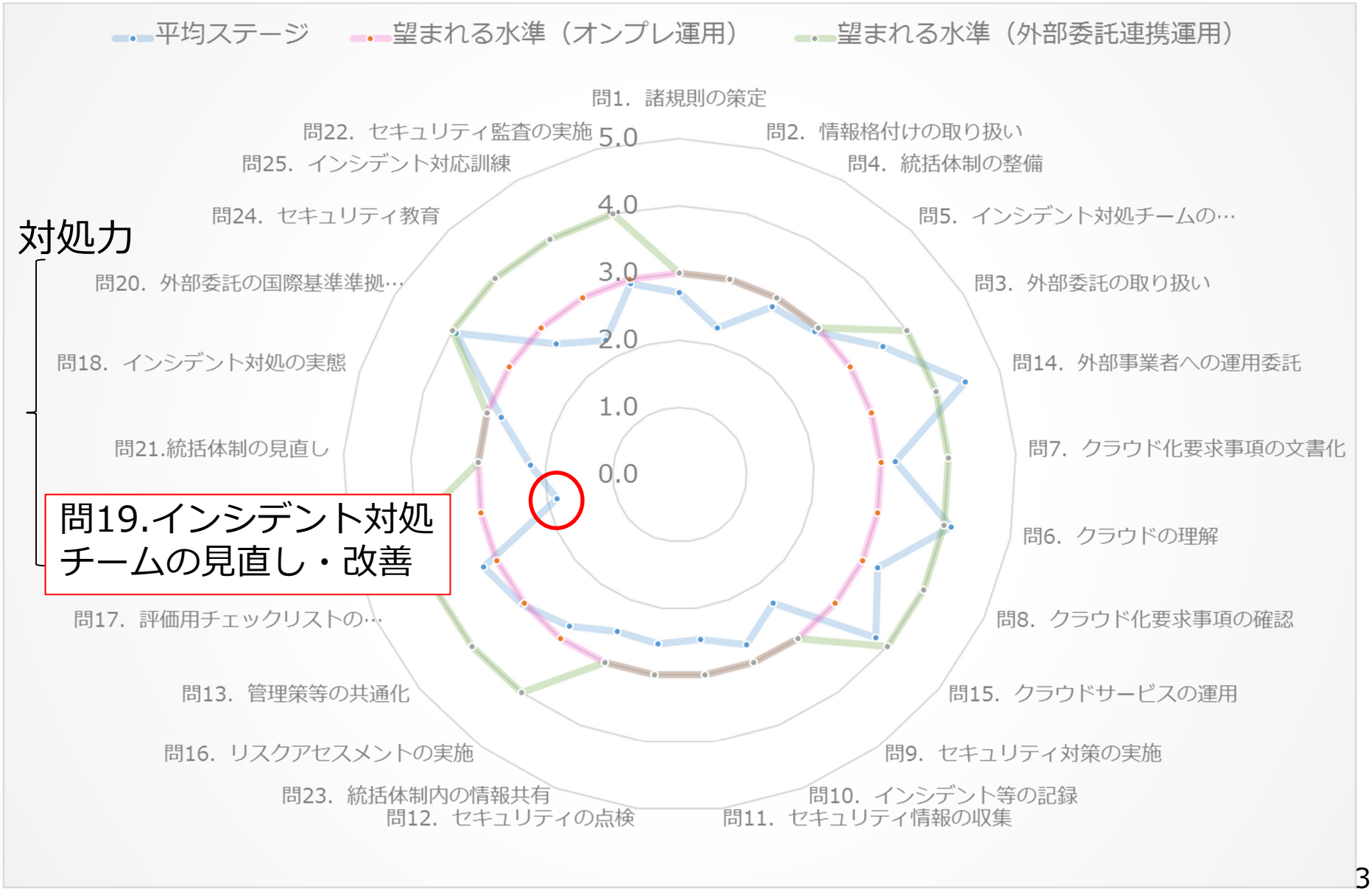


28学術機関の能力別平均ステージ

広島大学



設問別の平均ステージ


平均ステージ
望まれる水準（オンプレ運用）
望まれる水準（外部委託連携運用）
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…
問3．外部委託の取り扱い
問14．外部事業者への運用委託
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16．リスクアセスメントの実施
問13．管理策等の共通化
問17．評価用チェックリストの…
問19.インシデント対処チームの見直し・改善
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…
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
5.0
4.0
3.0
2.0
1.0
0.0
対処力

考察

広島大学

- **今回の評価結果について**
  - 自組織のセキュリティガバナンス実態を把握しフィードバックとステップアップを支援ができる見込みを得た
    - 望まれる水準との差分
    - 学術機関全体のセキュリティ取り組みの進捗具合
    - 次に実施すべき取り組み
- **改善すべきポイントについて**
  - 質問事項と選択肢
    - より簡潔かつ明瞭に
  - 評価方法
    - ステージ判定表（能力と質問事項と選択肢の関係）
    - クラウドサービス利用有無におけるステージ加点判定

まとめ

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の実態調査の評価モデルとアンケート内容を提案**
  - ISMSなどの重要事項がベース
  - オンプレ運用から外部委託(連携)運用へ段階的にセキュリティガバナンスの実態を把握する質問構成

- **今後の課題**
  - 学術機関毎の個別ステージ判定と報告書作成
  - アンケートシステムの評価と見直し
    - 回答機関からのヒアリングによる質問事項、ステージ判定の妥当性
    - 質問事項・選択肢および評価方法の見直し