Vol.2017-IOT-36 No.19
2017/3/3

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

渡邉英伸[†1]　晏康庄[†2]　西村浩二[†3]　相原玲二[†1]　合田憲人[†4]　吉田浩[†4]

概要：学術機関が運用管理する情報システムのクラウド化を推進するためには，自組織の情報セキュリティガバナンスの現状を客観的かつ定量的な評価のもと把握しておくことが重要である．一方で，現状では，学術機関のクラウドサービス活用を見据えた情報セキュリティガバナンスの観点のベンチマーク手法が確立されていない．本研究では，情報セキュリティガバナンスの現状とクラウドサービスの利用状況を把握するための評価モデルおよび質問事項を提案する．

キーワード：評価モデル，情報セキュリティガバナンス，クラウドサービス，学術機関，実態調査，

A Field Survey on Information Security Governance for Academic Institutes Accelerating the Use of Cloud Services

HIDENOBU WATANABE[†1]　YAN KANGZHUANG[†2]
KOUJI NISHIMURA[†3]　REIJI AIBARA[†1]
KENTO AIDA[†4]　HIROSHI YOSHIDA[†4]

Abstract: It is important that an academic institute comprehends an actual state of information security governance from an objective and quantitative evaluation to accelerate the use of cloud services. However, there is not a benchmark which evaluates information security governance including cloud services for academic institutes. We propose an evaluation model and questions to establish the benchmark.

Keywords: Evaluation model, Information Security Governance, Cloud Service, Academic Institute, Field Survey

1. はじめに

大学等の学術機関におけるクラウド化の推進ならびにクラウドサービス利用の在り方を検討する目的で，文部科学省をはじめ，クラウド化に関する実態調査が実施されている．本研究では，これまで実施された学術機関におけるクラウド化実態調査の現状を整理し課題について議論してきた[1]．また，学術機関においてクラウド化を推進するためには情報セキュリティガバナンスの観点が重要であることを示し，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を評価するモデルの検討をしてきた[2].

本論文では，学術機関のクラウドサービス利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に関するベンチマークの策定を目的に，情報セキュリティガバナンス実態調査のための評価モデルおよびアンケート質問事項を提案する．

以下，論文構成について述べる．2 章では，提案する評価モデルについて説明する．3 章ではアンケートの質問事項を紹介し，4 章で評価モデルと質問事項の関係ならびに評価方法について説明する．最後に，5 章で本稿のまとめを述べる．

2. 評価モデル

学術機関を対象とした情報セキュリティガバナンスの実態調査においては，学術機関全体から望まれる水準において評価されることが要求される．一方で，その水準は一様ではなく，経営層あるいは情報系センター（IT 関連部門）など実態調査の依頼先とアンケートの質問事項によって変わることが考えられる．そこで，本研究では，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実際に担当している情報系センターを対象に情報セキュリティガバナンスの実態調査の評価モデルおよびアンケート質問事項を提案することにした．

2.1 水準

提案する評価モデルの水準は，4 つの評価基準（適応力，管理力，対処力，自己啓発力）に基づいて，5 段階の評価軸（ステージ）で定義される．具体的には，アンケートの回

†1 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University
†2 広島大学大学院総合科学研究科
Graduate School of Integrated Arts and Sciences, Hiroshima University
†3 広島大学情報メディア教育研究センター／国立情報学研究所
Information Media Center, Hiroshima University/National Institute of Informatics
†4 国立情報学研究所クラウド基盤研究開発センター
Center for Cloud Infrastructure Development, National Institute of Informatics

答結果から，評価基準毎のステージを算出し，その平均ステージ（小数点以下切捨）が回答機関の最終的な水準となる．なお，5 段階の評価軸においては，情報システムのオンプレ運用を想定した評価軸（ステージ 1～3）をベースとし，クラウドサービス利用を見据えた外部委託事業者と連携による運用を想定した評価軸（ステージ 4～5）をアドオンする構成としている．これにより，組織としての情報セキュリティガバナンスが十分に構築・運用されていることを評価した上で，クラウドサービス利用といった高度な情報セキュリティガバナンスの構築・運用に導くことを可能にする．また，回答機関の水準と回答機関全体の平均水準をレーダーチャートで同時に表示し，差分を可視化した報告書を提示する．回答機関に対して優先的に取り組むべき項目を明確にすることで具体的な改善策実施へとつながるように促す．図 1 に評価モデルの概念図と報告書のサンプル例を示す．

今回，評価モデルを提案することによって，1)自組織の水準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，2)繰り返し活用することで，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，3)他の学術機関の情報セキュリティレベルの確認や外部委託事業者を含めた評価が可能なこと，4)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ならびにその状況が確認できることを目指す．

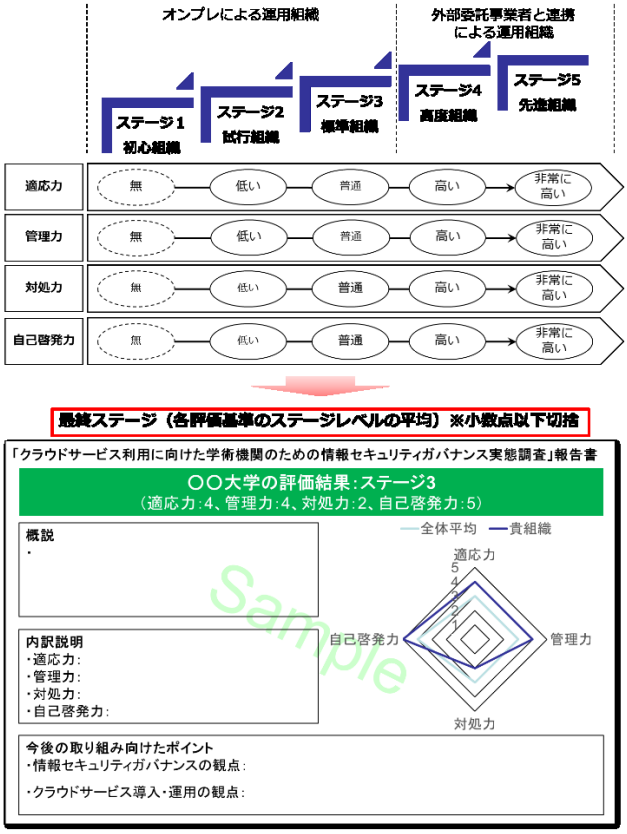

図 1　評価モデルの概念図と報告書のサンプル例
Figure 1　Image of Evaluation Model and Report Sample.

2.2 評価軸

クラウド化を見据えた情報セキュリティガバナンスの構築・運用の確立状況を判定する評価軸として，以下の 5 つのステージを定義する．

ステージ 1：初心組織

情報セキュリティガバナンスに対する取り組みが実施できていない，あるいは実施に向けて現在準備中など組織的な情報セキュリティガバナンスの構築・運用において初心組織となるステージ．

ステージ 2：試行組織

情報セキュリティガバナンスに対する取り組みが一部の組織に限定されている，あるいは取り組みが部分的であるなど組織的な情報セキュリティガバナンスの構築・運用において試行組織となるステージ．

ステージ 3：標準組織

情報セキュリティガバナンスに対する取り組みが組織的に実施され，継続的に見直し・改善が行われるなど組織的な情報セキュリティガバナンスの構築・運用において標準組織となるステージ．

ステージ 4：高度組織

情報セキュリティガバナンスに対する取り組みが単一の外部委託事業者と運用連携(シングルクラウド連携など)を含めて実施され，継続的に見直し・改善が行われるなど組織的な情報セキュリティガバナンスの構築・運用において高度組織となるステージ．

ステージ 5：先進組織

情報セキュリティガバナンスに対する取り組みが複数の外部委託事業者と運用連携（マルチクラウド連携など）を含めて実施され，継続的に見直し・改善が行われるなど組織的な情報セキュリティガバナンスの構築・運用において先進組織となるステージ．

2.3 評価基準

提案する評価基準では，各ステージを判定するために，以下の 4 つの基準を定義する．

評価基準 1：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．

評価基準 2：管理力

組織が定める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，対策基準，管理策等）の遵守が求められることに対して，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成果を示す運用が可能であることを判断する評価基準．

評価基準 3：対処力

迅速な情報セキュリティインシデント対応が要求されることに対して，情報セキュリティインシデント対応を評価しその結果から見直し・改善が可能であることを判断す

る評価基準.

評価基準 4：自己啓発力

情報セキュリティガバナンスにおける成長が期待されることに対して，情報セキュリティ教育や監査等を通して組織全体の情報セキュリティの向上を促す情報セキュリティ制度および情報セキュリティ統括体制であることを判断する評価基準.

3. アンケート質問事項

アンケートの質問事項は，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をベースとし，クラウドサービス利用に伴う運用状況を把握する質問をアドオンする構成となる．今回，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用に 25 問の質問事項を作成した．質問の内容については，ISMS[3]および情報セキュリティガバナンス[4]の重要事項を参考にした．これにより，提案モデルの水準は国際規格がベースにある状態となり，独自仕様を回避することができるだけでなく，PDCA サイクルの観点から情報セキュリティガバナンスの構築・運用の課題の指摘や次のステップに対するアドバイスが可能になる．なお，今回の質問事項は ISMS の要求事項や管理策の内容をそのまま取り入れているわけではない．したがって，評価モデルで示された結果が高評価であったとしても ISMS 認証の取得が可能であることを確約するものではないことに注意して頂きたい.

3.1 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の質問事項

組織的な制度・体制の実態についての質問は問 1～8(計 8 問)である．これらは PDCA サイクルの PLAN に該当するものである．ここでは，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），トップダウン型の体制，情報セキュリティの要求事項の文書化など組織における情報セキュリティガバナンスとして最低限求められる項目を定めている．また，問 6～8 は，情報セキュリティガバナンスのもとでクラウドサービスを運用する上で必要になる内容である．これらによって，回答機関の情報セキュリティガバナンスの構築状況ならびにクラウドに対する理解状況等を把握する．質問事項と選択肢を以下に示す.

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？
選択肢1. 策定していない
選択肢2. 策定を検討中である
選択肢3. 運用管理する部署が個別に策定している
選択肢4. 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？
選択肢1. 定めていない
選択肢2. 定めることを検討中である
選択肢3. 運用管理する部署が個別に定めている
選択肢4. 組織共通のものとして定めている

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？
選択肢1. 定めていない
選択肢2. 定めることを検討中である
選択肢3. 運用管理する部署が個別に定めている
選択肢4. 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？
選択肢1. 整備していない
選択肢2. 整備を検討中である
選択肢3. 統括体制は整備しているがトップダウン型ではない
選択肢4. 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？
選択肢1. 構築していない
選択肢2. 構築を検討中である
選択肢3. 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)
選択肢4. 専門の対応チームを構築している

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？
選択肢1. 把握していない
選択肢2. 把握を検討中である
選択肢3. 最低限把握している
選択肢4. 網羅的に把握している

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？
選択肢1. 文書化をしていない
選択肢2. 文書化をすることを検討中である
選択肢3. 導入する部署が個別に文書化をしている
選択肢4. 組織共通のものとして文書化をしている

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していますか？
選択肢1. 確認していない
選択肢2. 確認を検討中である
選択肢3. 一部のみ確認している
選択肢4. 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
選択肢5. 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

3.2 情報セキュリティに関する導入・運用の実態についての質問事項

導入・運用の実態についての質問は問 9～15(計 7 問)である. これらは PDCA サイクルの DO に該当するものである. ここでは, 情報セキュリティ対策, インシデント対応記録, 情報収集, 自己点検, オペレーションの共通化などについて問う内容を定めている. また, 問 14・問 15 は, クラウドサービス運用を見据えた外部委託およびクラウドサービス運用状況について問う内容である. これらによって, 回答機関の情報セキュリティ運用実態を把握する. 質問事項と選択肢を以下に示す.

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？(※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.)

選択肢1. 実施していない
選択肢2. 情報対策のみ実施している
選択肢3. 情報システム対策のみ実施している
選択肢4. ネットワーク対策のみ実施している
選択肢5. 情報対策・情報システム対策を実施している
選択肢6. 情報対策・ネットワーク対策を実施している
選択肢7. 情報システム対策・ネットワーク対策を実施している
選択肢8. 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

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？

選択肢1. 残していない
選択肢2. セキュリティインシデントのみ残している
選択肢3. セキュリティトラブルのみ残している
選択肢4. 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

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？

選択肢1. 収集していない
選択肢2. 連携はしていないが収集している
選択肢3. 1 カ所と連携して収集している
選択肢4. 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？

選択肢1. 実施していない
選択肢2. 当事者に任せている(組織的に管理していない)
選択肢3. 必要に応じて実施している
選択肢4. 定期的に実施している

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？

選択肢1. 実施していない
選択肢2. 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)
選択肢3. 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
選択肢4. 共通化(工夫)を組織的に実施しており, 効果はある

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？

選択肢1. 委託していない(オンプレミス運用形態)
選択肢2. 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
選択肢3. 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
選択肢4. 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 15 : クラウドサービスを運用していますか？

選択肢1. 運用していない
選択肢2. 契約した各部署が個別に運用している
選択肢3. 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
選択肢4. 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

3.3 情報セキュリティに関する評価・点検の実態についての質問事項

評価・点検の実態についての質問は問 16～20(計 5 問)である. これらは PDCA サイクルの CHECK に該当するものである. ここでは, 情報セキュリティリスクアセスメント, 自己点検のためのチェックリスト, 情報セキュリティインシデント対応の評価などの状況について問う内容を定めている. また, 問 20 は, クラウドサービス運用を見据えた外部委託の第三者認証取得状態について問う内容である. これらによって, 情報セキュリティマネージメントの実施すべき項目である評価・点検についての実態を把握する. 質問事項と選択肢を以下に示す.

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？

選択肢1. 実施していない
選択肢2. 実施している
選択肢3. 外部委託運用のものを含めて実施している

選択肢4. 複数の外部委託運用のものを含めて実施している

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？

選択肢1. 作成していない
選択肢2. 導入する部署が個別に作成している
選択肢3. 組織共通のものとして作成している

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？

選択肢1. できていない
選択肢2. できているが，改善の余地が大いにある
選択肢3. できている
選択肢4. 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
選択肢5. 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

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. 実施していない
選択肢2. 評価は実施しているが，見直しはしていない
選択肢3. 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
選択肢4. 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

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？

選択肢1. 満たしてしていない
選択肢2. 満たしているが，認証は取得していない
選択肢3. 満たしており，一部の事業者が認証を取得している
選択肢4. 満たしており，全ての事業者が認証を取得している

3.4 情報セキュリティに関する見直し・改善の実態についての質問事項

見直し・改善の実態についての質問は問 21～25(計 5 問)である．これらは PDCA サイクルの ACT に該当するものである．ここでは，情報セキュリティに関する監査，教育・訓練などについて問う内容を定めている．なお，クラウドサービス運用に関連する内容については選択肢に含めている．これらによって，情報セキュリティマネージメントの実施すべき項目である見直し・改善についての実態を把握する．質問事項と選択肢を以下に示す．

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？

選択肢1. 実施していない
選択肢2. 見直しのみ実施した 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
選択肢3. 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
選択肢4. 見直しを実施し，反映すべき結果は無かった

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？

選択肢1. 実施していない
選択肢2. 内部監査は実施している
選択肢3. 内部監査・外部監査（ISMS 等）を実施している
選択肢4. 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

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？

選択肢1. できていない
選択肢2. できているが，改善の余地が大いにある
選択肢3. できている

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？

選択肢1. 実施していない
選択肢2. 各部署が個別に実施している
選択肢3. 必要に応じて組織として教育を実施している
選択肢4. 定期的に組織として教育を実施している
選択肢5. 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？

選択肢1. 実施していない
選択肢2. 各部署が個別に実施している
選択肢3. 必要に応じて組織として教育・訓練を実施している
選択肢4. 定期的に組織として教育・訓練を実施している
選択肢5. 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

4. 質問事項・選択肢と評価モデルの関係

提案する評価モデルにおいて回答機関の最終的な水準を判定するためには，4 つの評価基準（適応力，管理力，対処力，自己啓発力）毎の評価軸（ステージ）を判定する必要がある．そこで，本節では各評価基準を判定する質問事項と選択肢と評価軸との関係を示し，その評価方法について説明する．

表 1　適応力判定のための質問事項・選択肢・評価軸の関係
Table 1　Mapping Table of Questions, Options and Stages in Adaptability Evaluation.

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

4.1　適応力の評価方法

表 1 に適応力判定のための質問事項・選択肢・評価軸の関係を示す．適応力を評価する質問事項は問 1〜8 および問 14・問 15 の 10 問である．まず，オンプレ運用であったとしても情報セキュリティガバナンスの構築においては問 1・問 2・問 4・問 5 が最低限実施できていることが求められる．よって，初めにこれらの質問の選択肢からステージ 1〜3 を判定する．一つでも実施していない場合はステージ 1 となる．部分的に実施されている場合はステージ 2 となり，すべて実施されていればステージ 3 以上と判定する．その後，問 3・問 6〜8・問 14・問 15 から外部委託あるいはクラウドサービス運用を含めた情報セキュリティガバナンスの構築状況についてステージ 3〜5 を判定する．単一の外部委託事業者と運用連携（シングルクラウド連携など）を含めて適切に実施されている場合はステージ 4 と判定し，複数の外部委託事業者と運用連携（マルチクラウド連携など）を含めて適切に実施されている場合は，ステージ 5 と判定する．

4.2　管理力の評価方法

表 2 に管理力判定のための質問事項・選択肢・評価軸の関係を示す．管理力を評価する質問事項は問 9〜13・問 16・問 17・問 23 の 8 問である．情報セキュリティ運用においては問 9〜12・問 23 が最低限実施できていることが求められる．初めにこれらの質問の選択肢からステージ 1〜3 を判定する．未実施があればステージ 1 となり，部分的な実施はステージ 2 となる．すべて実施されていればステージ 3 以上と判定する．その後，問 16・問 13・問 17 から外部委託を含めた情報セキュリティ運用についてステージ 2〜5 を判定する．オペレーションの共通化やチェックリストの作成が実施されていればステージ 4 以上となり，情報セキュリティリスクアセスメントが単一の外部委託事業者と運用連携を含めて適切に実施されている場合はステージ 4 と判定し，複数の外部委託事業者と運用連携を含めて適切に実施されている場合は，ステージ 5 と判定する．なお，情報セキュリティリスクアセスメントが実施されていない場合はステージ 2 に降格となる．

表 2　管理力判定のための質問事項・選択肢・評価軸の関係
Table 2　Mapping Table of Questions, Options and Stages in Manageability Evaluation.

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	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
	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 セキュリティトラブルのみ残している	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
	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 複数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	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
	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) 必要に応じて実施している	定期的に実施している	定期的に実施している	定期的に実施している
	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	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
	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 導入する部署が個別に作成している	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

表 3　対処力判定のための質問事項・選択肢・評価軸の関係
Table 3　Mapping Table of Questions, Options and Stages in Handling Ability Evaluation.

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	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
	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 見直しのみ実施した	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、反映すべき結果は無かった	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、反映すべき結果は無かった	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 できているが、改善の余地が大いにある	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
	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、一部の事業者が認証を取得している	満たしており、全ての事業者が認証を取得している

4.3　対処力の評価方法

表 3 に対処力判定のための質問事項・選択肢・評価軸の関係を示す. 対処力を評価する質問事項は問 18～20 の 4 問である. 情報セキュリティマネージメントとしては問 19・問 21 が最低限実施できていることが求められる. よって, これらの質問の選択肢から適応力や管理力の判定と同様に

表 4　自己啓発力判定のための質問事項・選択肢・評価軸の関係
Table 4　Mapping Table of Questions, Options and Stages in Self-Development Ability Evaluation.

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

ステージ 1〜3 を判定する．その後，問 18・問 20 から外部委託を含めた情報セキュリティインシデント対応および第三者認証取得状態についてステージ 2〜5 を判定する．情報セキュリティマネージメントが単一の外部委託事業者と運用連携を含めて適切に実施されている場合はステージ 4 と判定し，第三者認証取得した複数の外部委託事業者と運用連携を含めて適切に実施されている場合は，ステージ 5 と判定する．なお，情報セキュリティインシデントに対応が適切に実施できていない場合はステージ 2 に降格となる．

4.4 自己啓発力の評価方法

表 4 に自己啓発力判定のための質問事項・選択肢・評価軸の関係を示す．自己啓発力を評価する質問事項は問 22・問 24・問 25 の 3 問である．まず，組織全体の情報セキュリティ教育・訓練の観点では問 24・問 25 が最低限実施できていることが求められる．また,問 22 の監査を実施することも組織の情報セキュリティの信頼性を保証するためには実施できていることが望まれる．したがって，これらの質問の選択肢からステージ 1〜5 を判定する．実施していない項目が多ければステージ 1 と判定されやすく，実施項目が多くなるほど上位のステージが判定される．ステージ 4 は定期的に情報セキュリティ教育・訓練および外部監査が外部委託事業者と運用連携を含めて適切に実施されている場合に判定され，クラウドサービスを含めた外部監査が適切に実施されている場合は，ステージ 5 と判定する．

4.5 平均水準の学術機関像

提案する評価モデルでは, 次の 11 項目が実施可能であれば情報セキュリティガバナンスとして平均の水準（ステージ 3）を満たすことになる．1) 情報格付けを含む組織共通の運用管理関連諸規則の策定，2)トップダウン型の統括体制とインシデント対応の専門組織の構築，3)情報・情報システム・ネットワークに対する対策，4)インシデント・トラブルに関する記録, 5)セキュリティ情報収集, 6)定期的なセキュリティ点検, 7)統括体制内の情報共有, 8)リスクアセスメント，9)運用管理諸規則・統括体制・インシデント対応等に対する見直し･改善, 10)定期的なセキュリティ教育･訓練，11)セキュリティに関する内部監査.

これらは組織の情報システムに対する PDCA サイクルが適切に循環していることを表している．情報システム運用管理においてクラウドサービスは外部委託の一つとして位置づけられる．したがって，情報システムの一部をクラウドサービスに転換していく際には，転換により生じる差異を確認し，必要に応じて不足を補うプロセスを構築することが重要である．そのプロセスの構築は，組織の情報セキュリティガバナンスの喪失を防ぐだけでなく，クラウドサービスに対する漠然としたセキュリティ不安の払拭につながると考えられる．

5. おわりに

本論文では，クラウドサービス利用に向けた学術機関の情報セキュリティガバナンス実態調査のための評価モデルおよびアンケート質問事項を提案した．提案した評価モデルの特徴は，情報システムのオンプレ運用からクラウドサービス運用にステップアップ可能な構成と 4 つの評価基準（適応力，管理力，対処力，自己啓発力）と 5 段階の評価軸（ステージ）に基づいて総合評価する仕組みを定めている点である．

今後の課題は，実際に学術機関に対してアンケートを実施した結果をもとに，評価モデルの有用性を検証することが挙げられる．加えて，ベンチマークの策定および標準化も課題と考えている．

参考文献

[1] 晏康庄，渡邉英伸，西村浩二，近堂徹，相原玲二，合田憲人，岡田義広，学術機関におけるクラウドサービス利用に関する調査結果の分析，情報処理学会研究報告，Vol.2016-IOT-34，No.10，pp.1-7，2016.
[2] 渡邉英伸，晏康庄，西村浩二，相原玲二，合田憲人，吉田浩，岡田義広，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.
[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，http://www.isms.jipdec.or.jp/std/index.html
[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，http://www.meti.go.jp/policy/netsecurity/secgov-documents.html.