# 学認クラウドチェックリストと ISMAP 管理基準

小林 久美子 [1),2)], 吉田 浩 [1),2)], 岸 達也 [2)], 合田 憲人 [1),2)]

1) 国立情報学研究所 クラウド基盤研究開発センター
2) 国立情報学研究所 クラウド支援室

cobak@nii.ac.jp

# A Comparison of Security Measure Coverage between Gakunin Cloud Checklist and ISMAP Control Criteria

Kumiko Kobayashi[1),2)], Hiroshi Yoshida[1),2)], Tatsuya Kishi[2)], Kento Aida[1),2)]

1) Center for Cloud Research and Development, National Institute of Informatics
2) Cloud Promotion Office, National Institute of Informatics

**概要**

国立情報学研究所の学認クラウド導入支援サービスでは、大学・研究機関がクラウドを導入する場合の着眼点（信頼性、セキュリティ、契約条件等）をまとめたチェックリスト（学認クラウドチェックリスト）を策定し、セキュリティに着目した調達仕様を検討する場合の推奨チェック項目やセキュリティポリシ策定への活用を提示してきた。2021 年 3 月に政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP）のクラウドサービスリストが公開され、運用が開始された。学認クラウドチェックリストと ISMAP は、ともにクラウドセキュリティに関するチェック項目を網羅しているが、その関係が明確に整理されていない。本報告では、両者の情報セキュリティ対策としての網羅性や公開されている情報の内容を分析し、大学・研究機関におけるクラウド調達の実務面での活用方法を提案する。

## 1 はじめに

教育・研究のみならず社会活動においても、情報システムのセキュリティ対策は重要な課題であり、その解決策としてクラウドへの期待が高まっている。学術機関においては、令和 2 年度学術情報基盤実態調査 [1] によれば、調査に参加した 91.4% の大学で情報システムをクラウド化しており、そのうち 53.8% がクラウド化の効果として「セキュリティ対策の軽減」を挙げている。一方で、クラウド化していない大学のうち 55.1% がその理由として「セキュリティ面・信頼性に不安」を挙げている。

政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP）[2] は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。2021 年 3 月に ISMAP のクラウドサービスリスト [3] が公開され、運用が開始された。

国立情報学研究所（以下「NII」）では、我が国にクラウドを活用した高度な学術情報基盤を整備することを目的として、大学・研究機関（以下「大学等」）におけるクラウド導入・利活用を支援するための活動を進め、「学認クラウド」[4] として、クラウドの導入から利用までの各段階に対する 3 つの支援サービス（導入支援サービス、ゲートウェイサービス、オンデマンド構築サービス）を提供している。

学認クラウド導入支援サービス（以下「導入支援サービス」）は、大学等がクラウドを導入・利用する際の課題解決に役立つ情報の共有・流通を進めるサービスで、大学等がクラウドを導入する場合の着眼点（信頼性、セキュリティ、契約条件等）をまとめたチェックリスト [5]（以下「学認クラウドチェックリスト」）を策定し、クラウド事業者（以下「事業者」）による回答に基づくクラウドサービスの検証結果（以下「チェックリスト回答」）を大学等との間で共有している。

学認クラウドチェックリストは、大学等のクラウド導入で考慮すべき項目を網羅したものであり、合せてセキュリティ対策に重点をおいた利用を想定して、セ

キュリティに着目した調達仕様を検討する場合の推奨チェック項目 [6] やセキュリティポリシ策定への活用 [7] などを提示してきた。

学認クラウドチェックリストと ISMAP は、ともにクラウドセキュリティに関するチェック項目を列挙しているため、両者の関係について導入支援サービス参加大学等からも質問を受けている。

本報告では、両者の情報セキュリティ対策としての網羅性や公開されている情報の内容を分析し、大学等におけるクラウド調達の実務面での活用方法を提案する。

## 2　学認クラウドチェックリスト

学認クラウドチェックリストは、2015 年 9 月に Ver.1.0 が策定された後、毎年改訂されている。2021 年 7 月に改訂された最新のチェックリスト（Ver.5.1）では、軽微な文言修正等のマイナーアップデートを実施した。その構成を表 1 に示す。

本チェックリストは、19 種類のチェック項目（大項目）に分類され、それぞれの大項目は複数の詳細チェック項目（小項目）を含み、合計で 112 種類の小項目が用意されている。

事業者が回答を記入したチェックリスト（以下「チェックリスト回答」）は、NII による検証を経て、導入支援サービスに参加した大学等の担当者のみがアクセスできる Web サイト（以下「導入支援サービス参加機関専用サイト」）にて表形式で閲覧することができる。

大学等は、クラウドの導入・活用に関わる情報をまとめたガイドライン「スタートアップガイド」[6] やチェックリスト回答を参照し、クラウドの導入検討や調達に活用することができる。

## 3　ISMAP 管理基準

ISMAP は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。[8]

ISMAP 管理基準 [9] は、事業者が ISMAP 登録申請を行う上で実施すべきセキュリティ対策の一覧として策定され、第三者である監査機関が監査する際の前提として用いる基準とされている。

ISMAP では、ISMAP 管理基準のセキュリティ要求基準に基づいて安全性が評価されたクラウドサービスを ISMAP クラウドサービスリストに登録し、公開している。

表 1　チェックリスト Ver.5.1 大項目と小項目数

| 項番 | 大項目 | 小項目数 |
|---|---|---|
| A | 商品 / サービスの概要 | 4 |
| B | 運用実績 | 2 |
| C | 契約申込み | 8 |
| D | 認証関連 | 3 |
| E | 信頼性 | 4 |
| F | サポート関連 | 5 |
| G | ネットワーク・通信機能 | 9 |
| H | 管理機能 | 12 |
| I | ソフトウェア環境 | 4 |
| J | スケーラビリティ | 5 |
| K | データセンター | 7 |
| L | セキュリティ | 11 |
| M | データ管理 | 9 |
| N | バックアップ | 6 |
| O | クラウド事業者の信頼性 | 6 |
| P | 契約条件 | 6 |
| Q | データの取り扱い | 3 |
| R | リソースの引継ぎ | 4 |
| S | 第三者認証 | 4 |

本リストでは、事業者が実施している ISMAP 管理基準が統制目標番号として掲示されているが、個々のチェック項目がどのように対策されているのかといった具体的な情報は公開されていない。

要機密情報を取り扱う場合、各政府機関等のクラウドサービス利用にあたっては、暫定措置期間が設定されているものの、ISMAP クラウドサービスリストに掲載されているクラウドサービスの中から調達を行うことが原則とされている。

## 4　学認クラウドチェックリストと ISMAP 管理基準

ここでは、学認クラウドチェックリストと ISMAP 管理基準の情報セキュリティ対策としての網羅性や公開されている情報の内容を分析し、大学等におけるクラウド調達の実務面での活用方法を提案する。

### 4.1　情報セキュリティ対策としての網羅性

学認クラウドチェックリストは、大学等がクラウドサービスを導入する場合の利用者側の着眼点をまとめたものである。クラウドサービスのパフォーマンス、

信頼性、データ、ネットワーク、ソフトウェア等に係るセキュリティ対策のみならず、実際に運用する際に必要となる機能や仕様のチェック項目もある。

一方、 ISMAP 管理基準は、事業者を実施主体とした管理基準であり、ガバナンス基準、マネジメント基準、および管理策基準から構成される。情報セキュリティマネジメント (ガバナンス基準、マネジメント基準) に加えて、管理策基準では、実務実施者が行うクラウドサービスのパフォーマンス、信頼性、データ、ネットワーク、ソフトウェア等に係る個別のセキュリティ対策の実装を要求している。

表 2 に学認クラウドチェックリストのチェック項目に該当する ISMAP 管理策基準の例を示す。

なお、表 2 の SA1 は、学認クラウドチェックリストの追加資料として NII が提供しているサンプル規程集対応チェックリスト [10] の項目である。また、(A) と (B) は、ISMAP の管理策基準には掲載されていないが、ISMAP のクラウドサービスリスト詳細では公開されている内容である。(A) は ISMAP ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報で、 (B) は契約に定める準拠法・裁判管轄に関する情報である。

学認クラウドチェックリストと ISMAP 管理基準は、対象や目的が異なるため直接比較することは難しいが、網羅性に関しては、以下のような差異がある。

(1) ISMAP ガバナンス基準とマネジメント基準
これらは、事業者の経営者と管理者が実施すべき事項であり、クラウドサービスを利用する上で直接見える項目ではないと考えられるため、学認クラウドチェックリストでは対象としていない。

(2) セキュリティ対策レベルの差異
学認クラウドチェックリストと ISMAP 管理策基準は、ほとんど同じチェック項目を網羅しているが、以下の点で細かい差異があり、今後、学認クラウドチェックリストとしての対応を検討する。

- バックアップ
学認クラウドチェックリストでは、利用者のデータを保護するという観点から、N1 で利用者自身でバックアップを取得・管理する機能について質問しているのに対して、 ISMAP 管理策基準の 12.3.1 では、クラウドサービスの維持という観点から、事業者がシステムバックアップを取得することを要件としている。
- 時刻同期

表 2　チェックリストと管理策基準の例

| 学認クラウドチェックリスト | ISMAP 管理策基準 |
|---|---|
| D3:<br>多要素認証 | (9 アクセス制御)<br>9.2.3.11.PB, 9.4.2.2.B |
| F2:<br>重要情報の通知 | (12 運用のセキュリティ)<br>12.1.2.11.PB |
| H10:<br>ID とアクセス管理 | (9 アクセス制御)<br>9.2.1.6.PB, 9.2.2.8.PB, 9.4.1.8.PB |
| K1:<br>防犯設備 | (11 物理的及び環境セキュリティ)<br>11.1.1, 11.1.2, 11.1.3, 11.1.4 |
| K2:<br>入退室管理体制 | (11 物理的及び環境セキュリティ)<br>11.1.1, 11.1.2, 11.1.3, 11.1.4 |
| K3:<br>防災対策 | (11 物理的及び環境セキュリティ)<br>11.1.1, 11.1.2, 11.1.3, 11.1.4 |
| K4:<br>電力障害対策 | (11 物理的及び環境セキュリティ,<br>17 事業継続マネジメントにおける情報セキュリティの側面)<br>11.1.4, 17.2 |
| K5:<br>ネットワーク障害対策 | (11 物理的及び環境セキュリティ,<br>17 事業継続マネジメントにおける情報セキュリティの側面)<br>11.1.4, 17.2 |
| K6:<br>データセンターの設置地域 | (6 情報セキュリティのための組織)<br>6.1.3.3.PB |
| L1:<br>セキュリティポリシ | (6 情報セキュリティのための組織, 14 システムの取得、開発及び保守,15 供給者関係)<br>6.3.1.P, 6.3.1.1.PB, 14.2.1.13.PB, 15.1.2.18.PB |
| L3:<br>インシデント対応（事業者管理） | (6 情報セキュリティのための組織, 15 供給者関係,<br>16 情報セキュリティインシデント管理)<br>6.3.1.P, 6.3.1.1.PB, 15.1.2.18.PB, 16.1.5 |
| L4:<br>インシデント対応（ユーザ管理） | (6 情報セキュリティのための組織, 15 供給者関係,<br>16 情報セキュリティインシデント管理)<br>6.3.1.P, 6.3.1.1.PB, 15.1.2.18.PB, 16.1.5 |
| L5:<br>L5:バージョンアップの頻度 | (12 運用のセキュリティ)<br>12.6.1 |
| L6:<br>脆弱性情報の提供 | (12 運用のセキュリティ)<br>12.6.1.18.PB |
| L8:<br>セキュリティ対策 | (12 運用のセキュリティ)<br>12.2.1 |
| M1:<br>ログの知的財産権 | (12 運用のセキュリティ, 18 順守)<br>12.4.1.15.PB, 18.1.2.13.PB |
| M2:<br>ログの使用権（閲覧等） | (12 運用のセキュリティ)<br>12.4.1.15.PB |
| M3:<br>ログの使用（閲覧等）可能期間 | (12 運用のセキュリティ)<br>12.4.1.15.PB |
| M4:<br>M4:データの暗号化 | (8 資産の管理, 10 暗号)<br>8.1.2.7.PB, 10.1.1.9.PB |
| M5:<br>暗号化鍵の管理方法 | (8 資産の管理, 10 暗号)<br>8.1.2.7.PB, 10.1.1.9.PB |
| M7:<br>データのアクセス制限 | (9 アクセス制御)<br>9.4.1.8.PB |
| N1:<br>バックアップサービスの有無 | (12 運用のセキュリティ)<br>12.3.1 |
| N6:<br>バックアップデータのセキュリティ | (8 資産の管理)<br>8.1.2.7.PB |
| O3:<br>第三者委託 | (15 供給者関係)<br>15.1.1.16.B |
| O5:<br>サービスの監査結果の開示 | (A) |
| O6:<br>国内法人 / 国内総代理店等の有無 | (6 情報セキュリティのための組織)<br>6.1.3.3.PB |
| P1:<br>責任範囲の明確化 | (6 情報セキュリティのための組織)<br>6.1.1.13.PB, 6.3.1.P, 6.3.1.1.PB |
| P2:<br>契約条件・SLA の変更手続き | (12 運用のセキュリティ)<br>12.1.2.11.PB |
| P4:<br>準拠法 | (B) |
| P5:<br>管轄裁判所 | (B) |
| Q1:<br>データの知的財産権／使用権 | (18 順守)<br>18.1.2.13.PB |
| Q2:<br>データの削除 | (8 資産の管理)<br>8.1.5.P |
| SA1:<br>ストレージ機器などの物理的廃棄 | (8 資産の管理, 11 物理的及び環境的セキュリティ)<br>8.3.2, 11.2.7, 11.2.7.4.PB |
| - | (12 運用のセキュリティ)<br>12.4.4.4.PB |

ISMAP 管理策基準の 12.4.4.4.PB ではシステムクロックの同期について規定しているが、学認クラウドチェックリストには対応する項目がない。システムクロックの同期は、監査目的などのログ取得の詳細な実装に関わる機能として、セキュリティ対策以外にも多くのチェック項目を含む学認クラウドチェックリストには含めていなかった。しかし、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（2019 年度版）[11] にも時刻同期に関する条文があることから、学認クラウドチェックリストの次版以降での採用を検討する。

### 4.2 情報セキュリティ対策の実施状況の情報提供

NII によるチェックリスト回答検証では、事業者から提供された公開情報等をもとにチェックリスト回答の確認が行われる。事業者間での回答の粒度や用語は合わせているが、基本的にチェックリスト回答をそのまま導入支援サービス参加機関専用サイトで公開しており、NII でクラウドサービスの評価は行っていない。

チェックリスト回答には、実際に運用する際に必要となる実現レベルや方法まで記述されている場合が多い。

一方、ISMAP では、管理基準に基づいた情報セキュリティ対策の実施状況について監査機関が監査を行い、その監査結果を事業者が ISMAP 運営委員会に申請し、登録が妥当と判断されたクラウドサービスが ISMAP クラウドサービスリストに登録される。

従って、ISMAP は第三者認証に近いため、学認クラウドチェックリストの第三者認証の項目「S3：セキュリティ」では、セキュリティに関する第三者認証などを取得しているかを質問しているが、その例の 1 つとして ISMAP を挙げている。

ISMAP の公開情報からは、事業者が管理基準のどれを統制目標とし、それが実現されていることを監査結果をもとに認定されたことはわかるが、具体的な実現レベルや方法までは公開されていない。

### 4.3 クラウド調達における活用法の提案

実際にクラウドサービスを導入する際には、そのサービス内容や契約条件をよく理解した上で、個々の大学等のセキュリティポリシやガイドラインに適合したものを選択することが重要である。

従って、ISMAP クラウドサービスリストは一定のセキュリティ基準を満たしているかどうかという判断材料として利用し、当該クラウドサービスを大学等で導入する際の利用者側を含めた具体的なセキュリティ対策や運用の検討には学認クラウドチェックリストの情報を活用するという使い方も考えられる。

例えば、クラウド調達の基本的な 3 つの段階（導入検討フェーズ、仕様策定フェーズ、機関内承認フェーズ）[12] のうち、導入検討と機関内承認のフェーズでは、そのクラウドサービスが一定のセキュリティ基準を満たしているかどうかという判断材料として ISMAP クラウドサービスリストに登録されているかが利用できる。

そして、仕様策定フェーズにおけるサービスを比較し候補となるクラウドを絞り込み、実際の運用をどのように設計すればよいか検討し、調達に必要な仕様書を作成する作業では、学認クラウドチェックリストの情報が利用できる。

また、ISMAP クラウドサービスリストに登録されていないクラウドサービスの利用を検討する場合には、スタートアップガイド、学認クラウドチェックリスト、およびサンプル規程集対応チェックリストのベストプラクティスの情報を利用することで、セキュアなクラウドサービスの導入や調達を検討することができる。

## 5 おわりに

本稿では、学認クラウドチェックリストと ISMAP 管理基準の関係について説明した。

学認クラウドチェックリストは、大学等におけるクラウドの導入検討や調達などに利用されているが、学認クラウドチェックリストと ISMAP の関係をあらかじめ知っておくことによって、大学等がセキュアなクラウドサービスの導入や調達を検討する場合、より効率的に進めることができると考える。

NII は、今後も学認クラウドチェックリストを活用した大学等のクラウド導入検討を支援するために、ガイドライン等の情報提供を拡充していく予定である。

## 謝辞

「学認クラウド導入支援サービス」にご協力いただいている大学・研究機関ならびにクラウド事業者の方々に深く感謝いたします。

## 参考文献

[1] 文部科学省、「令和 2 年度学術情報基盤実態調査」の結果報告、https://www.mext.go.jp/b_menu/houdou/2020/1418398_00002.htm.

[2] 政府情報システムのためのセキュリティ評価制度（ISMAP）、https://www.ismap.go.jp.

[3] ISMAP クラウドサービスリスト、https://www.ismap.go.jp/csm?id=cloud_service_list.

[4] 学認クラウド、https://cloud.gakunin.jp/.

[5] 学認クラウド導入支援サービスチェックリスト、https://cloud.gakunin.jp/foracademy/#academy-02.

[6] 大学・研究機関のためのクラウドスタートアップガイド、https://cloud.gakunin.jp/foracademy/#acadey-02.

[7] 小林 久美子、岸 達也、吉田 浩、合田 憲人、目的別クラウド導入チェックリストの拡充 - オンラ

イン会議サービス・セキュリティポリシ -、大学 ICT 推進協議会 2020 年度年次大会、2020 年.
[8] ISMAP 概要、https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005&sys_kb_id=42de221b1bf6705013a78665cc4bcb80&spa=1.
[9] 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準、https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=e2309a581b9d301013a78665cc4bcba9&spa=1.
[10] サンプル規程集対応チェックリスト、https://cloud.gakunin.jp/foracademy/#academy-02.
[11] 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（2019 年度版）、https://www.nii.ac.jp/service/sp/.
[12] 小林 久美子、岸 達也、吉田 浩、合田 憲人、大学・研究機関におけるクラウド導入時のチェックリスト活用法、大学 ICT 推進協議会 2018 年度年次大会、2018 年.