ISMAP 情報セキュリティ監査
ガイドライン

令和２年６月３日
(令和４年１１月１日最終改定)

ISMAP 運営委員会

改定履歴

日付	改定内容
令和２年　６月　３日	ISMAP に関する規程等を施行
令和２年　８月２０日	誤記の修正などの軽微な改定
令和２年１２月２５日	誤記の修正などの軽微な改定
令和３年　６月２２日	誤記の修正などの軽微な改定
令和４年　４月　１日	4.1.1 (8) を改定
令和４年１１月　１日	ISMAP-LIU に関する記載を追加

目次

第 1 章　総則 2
1.1　本ガイドラインの目的 2
1.2　本制度における監査業務の特質 2
1.3　用語の定義 2
1.4　本制度における監査業務に関する業務依頼者、業務実施者、ISMAP 運営委員会の責任 4
第 2 章　独立性、客観性と職業倫理 4
第 3 章　品質管理 5
3.1　品質管理 5
第 4 章　本制度における監査業務の計画、実施、報告 6
4.1　業務契約の締結及び更新 6
4.2　業務チームの編成 8
4.3　計画 8
4.4　手続の実施 8
4.5　他の認証・監査制度等の証拠の利用 9
4.6　経営者確認書 9
4.7　報告 10
4.8　調書 11

第1章　総則

1.1　本ガイドラインの目的

本ガイドラインは、ISMAP 運営委員会が ISMAP クラウドサービスリスト若しくは ISMAP-LIU クラウドサービスリスト(以下、「ISMAP 等クラウドサービスリスト」という。)へのクラウドサービスの登録審査を行う際に参照する資料として利用する目的で、監査機関が情報セキュリティ監査基準、本ガイドライン及び標準監査手続（以下、「情報セキュリティ監査基準等」という。）に準拠して実施する本制度における監査業務に関して、手続の実施及びその結果の報告を行うために遵守しなければならない事項を定めるものである。なお、本ガイドラインの適用にあたっては、情報セキュリティ監査基準（平成 15 年経済産業省告示第 114 号）に準拠することを前提とするが、準拠する範囲は当該基準の助言型監査に関する部分のみとする。

1.2　本制度における監査業務の特質

本制度における監査業務は、ISMAP 運営委員会が行う ISMAP 等クラウドサービスリストの登録審査において、登録審査の対象となるクラウドサービスに関して、ISMAP 管理基準に基づいた情報セキュリティに係る内部統制の整備及び運用の状況を確認するために、クラウドサービス事業者の依頼に基づいて、監査機関が情報セキュリティ監査基準等に準拠して手続を実施し、その結果を事実に即して報告することを目的としている。業務実施者が作成した実施結果報告書は、サービス登録申請書の添付資料としてクラウドサービス事業者によって ISMAP 運営委員会に提出され、ISMAP 等クラウドサービスリストへの登録審査を行う際に参照する資料として利用される。

このため、本制度の監査業務において、業務実施者の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。また、本制度における監査業務は、結論の基礎となる十分かつ適切な証拠を入手することを目的とはしておらず、保証業務とはその性質を異にするものである。さらに、業務実施者は、本制度における監査業務において、重要性の概念の適用やリスク評価に基づく手続の決定は行わず、また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない。

1.3　用語の定義

本ガイドラインにおける用語の定義は、以下のとおりとする。なお、本項に示す定義以外については、「政府情報システムのためのセキュリティ評価制度(ISMAP)基本規程」（以下、「基本規程」という）における用語の定義に準ずるものとする。

1.3.1 本制度における監査業務

クラウドサービス事業者が ISMAP 等クラウドサービスリストへの登録申請を行う際に添付し、ISMAP 運営委員会が審査資料として使用するために、業務依頼者たるクラウドサービス事業者の依頼に基づいて実施する業務である。その内容は、登録審査の対象となるクラウドサービスに関して、

ISMAP 管理基準に基づいた情報セキュリティに係る内部統制の整備及び運用の状況について、業務実施者が情報セキュリティ監査基準等に準拠して手続を実施し、その結果を事実に即して報告するものである。

1.3.2 ISMAP 監査機関リスト

基本規程において定義されているとおり、ISMAP 運営委員会によって監査機関として本制度で定める要求事項を満たすことが確認された法人を記載する公開のリストをいう。

1.3.3 監査機関

基本規程において定義されているとおり、本制度における監査業務を実施する主体となる法人をいい、ISMAP 運営委員会による審査の結果、監査機関登録規則の要求事項を満たすことが確認され、ISMAP 監査機関リストに登録された法人をいう。

1.3.4 業務依頼者

本制度における監査業務を依頼するために、業務実施者と業務契約を締結する者を指し、基本規程において定義されているクラウドサービス事業者を指す。

1.3.5 業務執行責任者

監査機関に所属する者のうち、本制度における監査業務の責任者又は本制度における監査業務を実施する総括責任者、すなわち当該業務とその実施及び発行する実施結果報告書に対する責任を負う者をいう。

1.3.6 業務実施責任者

業務チームに所属する者のうち、個々の監査業務の実施責任者をいう。

1.3.7 業務実施者

業務チームに所属する者のうち、本制度における監査業務を実施する者をいい、業務執行責任者、業務実施責任者又は業務チームの他のメンバーを含めて使用される。

1.3.8 業務チーム

業務執行責任者が業務遂行のために自らの責任の下に編成するものをいい、業務執行責任者及び業務実施責任者を含め、原則、監査機関に所属する者で構成される。

1.3.9 実施結果の利用者

業務実施者が作成した実施結果報告書を利用する者を指し、業務依頼者、制度所管省庁、ISMAP 運

営委員会及び ISMAP 運用支援機関を指す。

1.3.10 調書

業務実施者が実施した手続、入手した証拠及び業務の過程で識別した事項の記録をいう。

1.3.11 実施結果報告書

ISMAP 管理基準に基づいてクラウドサービス事業者が実施する情報セキュリティに係る内部統制の整備及び運用の状況について、情報セキュリティ監査基準等に準拠して手続を実施した結果、業務実施者が発行する報告書をいう。

1.3.12 ISMAP 標準監査手続

業務実施者が、本制度における監査業務の手続を実施する際に遵守すべき標準的な手続を定めたもの。標準監査手続は詳細管理策に対応するよう構成される。

1.4　本制度における監査業務に関する業務依頼者、業務実施者、ISMAP 運営委員会の責任

1.4.1 業務依頼者の責任

業務依頼者は、言明の対象となるクラウドサービス、すなわち、ISMAP 等クラウドサービスリストへの登録申請を行うクラウドサービスに関して、当該サービスの内容及びセキュリティリスク分析の結果を踏まえて、ISMAP 管理基準に準拠して統制目標及び詳細管理策を選択して必要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることを言明する責任を有している。

1.4.2 業務実施者の責任

業務実施者は、情報セキュリティ監査基準等に準拠して本制度における監査業務を実施し、その実施結果を業務依頼者に報告する責任を負う。

業務実施者は、標準監査手続に準拠して業務依頼者の言明する統制に対して手続を実施する責任を負うが、その結果として関連する統制目標の有効性や手続実施結果から導かれる結論の報告を行う責任は負わない。

1.4.3 ISMAP 運営委員会の責任

ISMAP 運営委員会は、実施結果報告書を含むサービス登録に必要となる申請書類を業務依頼者から受領し、ISMAP クラウドサービス登録規則若しくは ISMAP-LIU クラウドサービス登録規則に基づいて ISMAP 等クラウドサービスリストへのクラウドサービスの登録審査を行う責任を負う。

第2章　独立性、客観性と職業倫理

2.1 業務実施者は、情報セキュリティ監査基準に定める独立性、客観性及び職業倫理に関する要求事項を遵守すること。

2.2 監査機関[1]は、前項に定める事項の他、外観上の独立性に関して以下の事項を遵守すること。

2.2.1 本制度における監査業務の対象となるクラウドサービス事業者と資本関係を有してはならない。

2.2.2 本制度における監査業務の対象となるクラウドサービス事業者との間に、本制度における監査業務と利益相反が生じる関係を有していないこと[2]。

第3章　品質管理

3.1　品質管理

監査機関は、次に掲げる品質管理要件に準拠し、実施する本制度における監査業務の全体的な品質確保に責任を負う。

3.1.1 品質管理者による品質管理

品質の維持・向上のため、組織における本制度における監査業務の品質管理に関する担当者を割り当て、品質管理者が組織的に監査の品質を管理していること。ただし、当該担当者が専属して業務品質の管理を行うことを必ずしも求めるものではない。

3.1.2 品質管理マニュアルに基づく品質の確保

品質の維持・向上のため、次に掲げる事項を含む業務品質の管理のためのマニュアルを整備し、マニュアルに基づき品質管理を行っていること。

(1) サービス提供プロセスの管理
(2) アウトプットの管理

3.1.3 品質の維持・向上に関する手続等の導入状況

品質の維持・向上のため、次に掲げる手続等を行っていること。

(1) 本制度における監査業務を行った案件について、当該案件に従事した者以外の者が監査計画及び実施結果報告書についてのレビューを行っていること。

---

[1] 1.3.3に定めるとおり、監査機関とはISMAP監査機関リストに登録された法人を指し、当該法人のグループ企業やネットワークファームは含まない。

[2] 利益相反が生じている事例として、例えば、監査機関が、本制度における監査業務の対象となるクラウドサービスに関して、当該クラウドサービスの開発・保守・運用・設計・導入業務を提供している場合等が想定される。

(2) 本制度における監査業務に従事する者に対して、次に掲げる本制度における監査業務の品質確保に資する教育又は研修等のいずれかを実施又は受講させていること。

① 業務執行責任者及び業務実施責任者

年間２０時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT（On the Job Training)、社内講習や自習を含む。）

② 業務実施者

年間５時間以上の教育又は研修（資格維持のための研修を含む。教育サービス事業者が提供する教育・研修のほか、OJT、社内講習や自習を含む。）

(3) 業務依頼者の情報を保護するための手続を設け、運用するとともに、当該手続について本制度における監査業務を行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

第4章　本制度における監査業務の計画、実施、報告

4.1　業務契約の締結及び更新

4.1.1 業務実施者は、本制度における監査業務に対する誤解を避けるため、業務依頼者が以下の事項を明確に理解していることを確かめた上で業務依頼者との業務契約の締結を行わなければならない。業務契約書等には、契約条件の内容として、以下の事項を含めること。

(1) 本制度における監査業務の性質

① 本制度における監査業務は、保証型監査又はレビュー業務等の保証業務[3]には該当せず、したがって手続実施結果から導かれる結論の報告も、また、保証の提供もしない旨

② 業務依頼者の責任

- 業務依頼者は、本制度における監査業務において、言明対象となるサービスの範囲及び手続の対象期間を決定する責任を負う旨
- 経営者確認書に 4.6.2 に規定する事項を記載し、遵守する責任を負う旨
- 業務依頼者は、言明対象となるサービスの内容及びセキュリティリスク分析の結果等を踏まえて、ISMAP 管理基準に準拠して統制目標及び詳細管理策を選択し必

[3] 「保証業務とは、主題に責任を負う者が一定の規準によって当該主題を評価又は測定した結果を表明する情報について、又は、当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務をいう。」（財務情報等に係る保証業務の概念的枠組みに関する意見書　　平成 16 年 11 月 29 日　企業会計審議会）

要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることを言明する責任を有する旨

- 業務依頼者は、言明の記載内容が正確であることを自ら評価するための体制を整備し、評価を実施する責任を負う旨
- 業務依頼者は、ISMAP 管理基準の要求事項の解釈についての責任を負う旨
- 業務依頼者は、本制度における監査業務が情報セキュリティ監査基準等に準拠したものであることを承知している旨
- 実施結果報告書の配布及び利用制限が存在する旨
- 業務依頼者は、業務実施者が要請した全ての情報、面接及び質問の機会を提供した旨
- 本制度における監査の対象期間の末日以降、経営者確認書の日付までの間において、言明対象となるクラウドサービスの統制及び情報セキュリティの状況に重大な変更を及ぼしうる事象の発生の有無（ある場合には、その内容）
- 業務の実施に影響を与える可能性のある不正及び違法行為等に関する情報の有無（ある場合には、その内容）

③ 業務実施者の責任

- 業務実施者は、業務依頼者が本制度における監査業務の実施を依頼した目的に則して、情報セキュリティ監査基準等に準拠して本制度における監査業務を実施し、その実施結果を報告する責任を負う。ただし、当該手続の対象範囲、期間及び手続の対象を決定する責任は負わない旨
- 業務実施者の報告は、手続実施結果を事実に則して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証の提供もしない。また、業務実施者は、本制度における監査業務において、重要性の概念の適用やリスク評価に基づく手続の決定は行わず、また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない旨

④ ISMAP 運営委員会の責任

- ISMAP 運営委員会は、業務実施者から報告された実施結果報告書を含む申請書類を確認し、ISMAP クラウドサービス登録規則若しくは ISMAP-LIU クラウドサービス登録規則に基づいて当該クラウドサービスの ISMAP 等クラウドサービスリストへの登録審査を行うことにある旨

(2) 業務依頼者が本制度における監査業務の実施を依頼した目的
(3) 本制度における監査業務の対象とするクラウドサービス
(4) 本制度における監査業務は情報セキュリティ監査基準等に準拠して行われる旨

(5) 実施する範囲、期間及び手続の対象等
(6) 実施結果報告書の想定される様式及び内容
(7) 実施結果報告書の配布及び利用制限
(8) 業務実施者は、ISMAP 運営委員会が ISMAP 監査機関登録規則 3.13 に基づき監査調書の閲覧を求めた場合は協力し、業務依頼者はそれを妨げない旨
(9) その他必要と考えられる事項

4.1.2 業務実施者は、以下の状況が生じている場合には、本制度における監査業務契約の新規の締結又は更新を行わないものとする。

- 業務依頼者が、本制度の趣旨及び ISMAP 管理基準に準拠した情報セキュリティに係る内部統制の整備及び運用の状況に関する責任を認識していない場合。
- 4.1.1 に定める契約条件が遵守できないことが明らかである場合。
- 法令等又はその他の状況により、実施結果報告書の利用を、1.3.9 において規定する者に制限することができない場合。
- ISMAP 運用支援機関への問い合わせの結果、ISMAP クラウドサービス登録規則「6 審査」若しくは ISMAP-LIU クラウドサービス登録規則「5 事前申請の審査」に定める期間内に審査を行うことが困難であることが判明した場合。

4.2 業務チームの編成

4.2.1 業務執行責任者は、ISMAP 監査機関要求事項に定める業務チームに関する要件を満たすよう業務チームを編成しなければならない。

4.2.2 業務執行責任者は、業務チームが情報セキュリティ監査基準等に準拠して業務を遂行するよう、監督しなければならない。

4.3 計画

4.3.1 業務実施者は、本制度における監査業務を有効かつ効果的に実施するための計画を立案しなければならない。

4.4 手続の実施

4.4.1 クラウドサービス事業者の情報セキュリティに係る内部統制の整備及び運用の状況に関して、業務実施者は下記の事項を遵守して手続を実施する。

(1) 実施する手続

本ガイドラインのほか、情報セキュリティ監査基準及び標準監査手続に従って手続を実施する。

(2) 言明書のうち、手続の対象となる範囲

・　手続は、言明書のうち、「１．言明の範囲と対象期間　（４）対象管理策と会社の統制内容」に記載されている全ての詳細管理策に対応する業務依頼者の統制に関して、整備状況評価及び運用状況評価を実施する。ただし、ISMAP-LIU については、標準監査手続 別紙３に記載されている範囲に対応する業務依頼者の統制に関して、整備状況評価及び運用状況評価を実施する。

・　業務依頼者が統制目標あるいは詳細管理策を除外している場合には、統制目標については言明書及びその別添に、また、詳細管理策については別添にそれぞれの除外理由が記載されていることを確認する。ただし、業務実施者はいずれの除外理由の妥当性についても評価を行わない

(3) 本制度における監査の対象期間

最低３ヶ月以上１年を超えない期間で、業務依頼者が指定する期間。

4.5　他の認証・監査制度等の証拠の利用

業務実施者は、標準監査手続に準拠して自ら手続を実施する。そのため、他の認証・監査制度や内部監査等の実施結果あるいはその報告書をそのまま利用することは原則認められない。ただし、業務実施者が標準監査手続を実施する際に適切とみなす場合には、他の認証・監査制度や内部監査等において収集された証拠を利用することは可能である。

4.6　経営者確認書

4.6.1　業務実施者は、実施結果報告書の発行に先立ち、業務実施期間中に業務依頼者から提示を受けた資料及びその他の説明について、業務依頼者から経営者確認書を入手しなければならない。

4.6.2　業務実施者は、経営者確認書に以下の項目が記載されていることを確認しなければならない。

・　業務依頼者は、言明対象となるクラウドサービスに関して、サービスの内容及びセキュリティリスク分析の結果等を踏まえて、ISMAP 管理基準に準拠して統制目標及び詳細管理策を選択し必要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることを言明する責任を有している旨。

・　業務依頼者は、言明の記載内容が正確であることを自ら評価するための体制を整備し、評価を実施する責任を負う旨。

・　業務依頼者は、ISMAP 管理基準の要求事項の解釈についての責任を負う旨。

・　業務依頼者は、本制度における監査業務が情報セキュリティ監査基準等に準拠したものであることを承知している旨。

・　実施結果報告書の配布及び利用制限が存在する旨。

・　業務依頼者は、業務実施者が要請した全ての情報、面接及び質問の機会を提供した旨。

・　本制度における監査の対象期間の末日以降、経営者確認書の日付までの間において、言明対象となるクラウドサービスの統制及び情報セキュリティの状況に重大な変更を及ぼ

しうる事象の発生の有無（ある場合には、その内容）。

- 業務の実施に影響を与える可能性のある不正及び違法行為等に関する情報の有無（ある場合には、その内容）。

4.7　報告

4.7.1 業務実施者は、様式 1 を踏まえて実施結果報告書を作成すること。実施結果報告書には以下の事項を全て含めなければならない。

- 表題
- 宛先
- 日付
- 監査機関名
- 業務執行責任者の署名又は記名押印
- 業務依頼者が手続を依頼した目的
- 本制度における監査業務の対象とするクラウドサービス
- 業務実施者が実施した本制度における監査業務は、情報セキュリティ監査基準等に準拠している旨
- 業務依頼者、業務実施者、ISMAP 運営委員会の責任。なお、ISMAP 運営委員会の責任に関する記載は、様式の文言から変更してはならない。
- 実施した業務の概要（対象とする範囲、期間及び手続の対象等）
- 業務実施者が実施した手続及び手続実施結果
- 業務依頼者が除外した統制目標又は詳細管理策がある場合には、その統制目標又は詳細管理策の番号及び除外理由が言明書に記載されている旨。業務実施者は当該除外理由の妥当性の評価に責任は負わない旨
- 標準監査手続のうち、実施できなかった手続がある場合には、その手続及びその理由
- 発見事項[4]。なお、業務実施者は、事実に即して発見事項を報告する責任を負うが、入手した証拠の十分性及び適切性を決定するための発見事項の評価は実施しない旨。また、特定の事実が発見事項に該当するか否かについて、業務実施者はいかなる ISMAP 管理基準の要求事項の解釈に基づく判断や、重要性に関する判断も実施しない旨。
- 本制度における監査業務は、保証型監査又はレビュー業務等の保証業務には該当せず、したがって手続実施結果から導かれる結論の報告も、また、保証の提供もしない旨。
- 実施結果報告書は、業務依頼者、制度所管省庁、ISMAP 運営委員会及び ISMAP 運用支援機関のみに配布及び利用が制限されており、サービス登録審査の他、ISMAP 監査機関登録規

[4] 発見事項とは、業務実施者が実施した手続の結果のうち、下記に該当する事項等をいう。
・整備状況の評価手続を実施した結果、内部統制に関連する規程・ルール等が存在しなかった。
・整備状況の評価手続を実施した結果、内部統制に関連する証跡が存在しなかった。
・運用状況の評価手続を実施した結果、抽出したサンプルについて内部統制の逸脱が存在した。

則に規定する審査及びモニタリングにおいて必要な範囲で利用される場合を除き、他のいかなる目的にも使用してはならない旨。

4.7.2 実施結果報告書は日本語で作成しなければならない。

4.7.3 実施結果報告書の日付は、業務実施者が業務を終了した日より前の日付を付してはならない。

4.7.4 実施結果報告書の日付は、言明書に記載される本制度における監査の対象期間の末日から原則最大3ヶ月以内とする。

4.7.5 実施結果報告書には、実施結果の利用者が、実施した手続の内容を理解できるように、標準監査手続に準拠して実施した手続の対象範囲、期間及び手続の対象を詳細に記載しなければならない。

4.7.6 業務実施者は、手続実施結果を事実に基づき客観的に記載しなければならず、曖昧な表現を用いたり、見解を述べたりしてはならない。

4.7.7 業務執行責任者は、様式1別添2に従って業務を実施した業務チームがISMAP監査機関要求事項で定める事項を満たしていることを示す資料を実施結果報告書に添付しなければならない。

4.8 調書

4.8.1 業務実施者は、実施した手続の結果とその関連資料を調書として文書化しなければならない。

4.8.2 調書の作成に当たっては、実施結果に至った過程が分かるように秩序整然と記録しなければならない。

4.8.3 調書には、例えば以下の事項を記載することが望ましい。

- 情報セキュリティ監査基準に定める独立性、客観性と職業倫理に関する規定の遵守状況
- 業務依頼者との業務契約の新規の締結又は更新に関する判断
- 実施した業務の対象とする範囲、期間及び手続の対象等
- 手続の実施結果及び入手した証拠
- 業務の過程で識別したその他の事項
- 手続を実施した者及びその完了日並びに査閲した者、査閲日及び査閲の対象

4.8.4 調書は、本制度における監査業務終了後、その保存期間が終了するまで適切に保管しなければならない。

様式1　実施結果報告書