ISMAP 標準監査手続

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	運用状況評価の実施に係る記載の改定 誤記の修正などの軽微な改定
令和３年　３月１２日	別紙１を追加 誤記の修正などの軽微な改定
令和３年　６月２２日	3.3、3.5 脚注 3 を改定 別紙２を追加
令和３年　９月１３日	表 1、3.2 を改定
令和４年　４月　１日	誤記の修正などの軽微な改定
令和４年１１月　１日	ISMAP-LIU に関する記載を追加 別紙３を追加

目次

第1章　総則

1.1　ISMAP 標準監査手続の目的

ISMAP 標準監査手続（以下、「標準監査手続」という。）は、政府情報システムのためのセキュリティ評価制度（以下、「本制度」という。）において業務実施者が本制度における監査業務を実施する際に遵守すべき標準的な手続を定めたものである。ISMAP 運営委員会の責任において定める標準的な手続を示すことにより、業務実施者の恣意的な判断や能力の違いによる手続の品質のぶれを防止し、ISMAP 運営委員会が求めるリスク対応の水準を確保することを目的としている。

なお、ISMAP 情報セキュリティ監査ガイドラインに規定しているとおり、業務実施者が標準監査手続に準拠して本制度における監査業務を実施する場合は、情報セキュリティ監査基準及び ISMAP 情報セキュリティ監査ガイドラインを始めとする本制度における規則等に準拠することが前提となる。

1.2　用語の定義

用語の定義については、「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。）及び「ISMAP 情報セキュリティ監査ガイドライン」（以下、「ガイドライン」という。）における定義に準ずるものとする。

第2章　標準監査手続の構成

標準監査手続は、ISMAP 管理基準の構成に準じて、詳細管理策に対応するよう構成されている。標準監査手続を構成する主な項目は次のとおりである。

2.1　主たる監査対象

詳細管理策において想定される手続の実施対象。ここでは、一般的に想定される手続対象として、「規程、手順書等」、「根拠となる文書・記録等①　サンプルテストを実施しないもの（設計書、仕様書等)」、「根拠となる文書・記録等②　サンプルテストを実施するもの（申請書、承認記録、システムログ、台帳等)」、「根拠となる設定（パラメータ、ステータス、コマンド等)」、「設備・建物等」の 5 種類を挙げている。

2.2　評価の種類

業務実施者は、整備状況評価及び運用状況評価を実施しなければならない。

整備状況評価：情報セキュリティに関する内部統制が ISMAP 管理基準に沿ってデザインされ、実際の業務に適用（実装）されているかを確かめるための評価。

運用状況評価：情報セキュリティに関する内部統制が、手続の対象期間にわたってデザイン通り運用されているかを確かめるための評価。なお、ISMAP 運営委員会によって指定された全ての詳細管理策に対して、運用状況評価を実施しなければならない。

ISMAP 管理基準のうち、ガバナンス基準及びマネジメント基準に対応する標準監査手続は整備状況評価に関する手続のみから構成される。また、管理策基準に対応する標準監査手続は、

主たる監査対象に応じて、整備状況評価及び運用状況評価に関する手続又は整備状況評価に関する手続のみから構成される。

2.3　監査技法

業務実施者が監査証拠を入手するための手段をいい、標準監査手続においては、ISMAP 管理基準の性質を踏まえて、質問、閲覧、観察の 3 つの技法を想定している。

質問：管理策の整備状況又は運用状況に関して、関係者に対して口頭又は文書で問い合わせ、説明や回答を求める監査技法。質問は、質問以外の監査技法と組み合わせて利用される。

閲覧：管理策の整備状況又は運用状況に関して、紙媒体、電子媒体又はその他の媒体による記録や文書を確かめる監査技法。

観察： 管理策の整備状況又は運用状況に関して、監査人自らが現場に赴き、目視によって確かめる監査技法。観察により、プロセス又は手続の実施に関する監査証拠を入手できるが、観察を行った時点に関する監査証拠に限定され、また、プロセスや手続の実施状況は観察されているという事実に影響を受けることがある。

2.4　標準監査手続

業務実施者が監査証拠を入手するために実施するプロセスを監査手続といい、ISMAP 標準監査手続においては詳細管理策に対応した標準的な手続を定めている。

2.5　留意点

手続の実施に際して、留意すべき事項や手続の実施の前提となる事項等を補足的に記載している。

上記に加えて、参考情報として、各管理策において想定される監査証跡の名称等の例示を行っている。ただし、個別管理策の実現方法はクラウドサービス事業者により様々であり、個別の証跡名に関しても標準監査手続において一律に規定することは困難であることから、当該項目については手続実施上の参考情報に留めるものとする。

以上、2.1 から 2.5 を踏まえると、主たる監査対象に応じて適切と考えられる監査技法及び定型監査手続の組み合わせは表１のとおりである。その上で、詳細管理策ごとに想定される主たる監査対象を特定し、表１の考え方に基づいて対応する監査技法及び定型監査手続を当てはめて標準監査手続とした。なお、クラウドサービス事業者によって個別管理策の実現方法が異なることを想定し、標準監査手続は特定の証拠の名称等を含まない一般化した記述としているが、これは、本制度として詳細管理策の個別具体的な実装への対応を包摂した監査手続として予め規定することを意図したものである。

表１　主たる監査対象と監査技法、定型監査手続の組み合わせ

主たる監査対象	評価の種類	監査技法	監査手続	留意点
規程、手順書等	整備	質問	コントロールオーナーに質問し、コントロールオーナーが[詳細管理策]の存在を知り、[詳細管理策]を実施していることを確認する。	―
		閲覧	主たる監査対象【文書】を閲覧（レビュー）し、 主たる監査対象【文書】に、[詳細管理策]が記載されていることを確認する。	
			主たる監査対象【文書】が、組織として検証（承認）され、関係者が常に閲覧可能な状況になっていることを確認する。	管理策において、組織による検証（承認）が要求されている場合には、左記手続も実施する。
根拠となる文書・記録等① サンプルテストを実施しないもの（設計書、仕様書等）	整備	質問	コントロールオーナーに質問し、コントロールオーナーが[詳細管理策]の存在を知り、[詳細管理策]を実施していることを確認する。	―
		閲覧	主たる監査対象【文書】を閲覧（レビュー）し、 主たる監査対象【文書】に、[詳細管理策]が記載されていることを確認する。	記録の形態、利用者、利用頻度等に応じて、適切な管理がされていることを確認する。 ・電子データ（ログ等）としての管理方法 ・紙(管理簿等)としての管理方法 ・利用者と承認者の定義 ・保管期間等
			主たる監査対象【文書】が、組織として検証（承認）され、関係者が常に閲覧可能な状況になっていることを確認する。	管理策において、組織による検証（承認）が要求されている場合には、左記手続も実施する。
根拠となる文書・記録等② サンプルテストを実施するもの（申請書、承認記録、システムロ	整備	質問	コントロールオーナーに質問し、コントロールオーナーが[詳細管理策]の存在を知り、[詳細管理策]を実施していることを確認する。	―
		閲覧	主たる監査対象【記録】を閲覧（レビュー）し、 主たる監査対象【記録】に、[詳細管理策]を実施した履歴が記録	記録の形態、利用者、利用頻度等に応じて、適切

グ、台帳等)			されていることを確認する。(サンプル１件)	な管理がされていることを確認する。 ・電子データ（ログ等）としての管理方法 ・紙(管理簿等)としての管理方法 ・利用者と承認者の定義 ・保管期間等
			主たる監査対象【文書】が、組織として検証（承認）されていることを確認する。(サンプル１件)	管理策において、組織による検証（承認）が要求されている場合には、左記手続も実施する。
	運用	閲覧	管理策に定められた頻度に応じて母集団資料よりサンプルを抽出する。 抽出したサンプル全件を閲覧（レビュー）し、 主たる監査対象【記録】に、[詳細管理策]が実施された履歴が監査対象期間を通じて継続して記録されていることを確認する。	記録の形態、利用者、利用頻度等に応じて、適切な管理がされていることを確認する。 ・電子データ（ログ等）としての管理方法 ・紙(管理簿等)としての管理方法 ・利用者と承認者の定義 ・保管期間等
			抽出したサンプル全件を閲覧（レビュー）し、 主たる監査対象【文書】が、組織として検証（承認）されていることを確認する。	管理策において、組織による検証（承認）が要求されている場合には、左記手続も実施する。
根拠となる設定（パラメータ、ステータス、コマンド等)	整備	質問	コントロールオーナーに質問し、コントロールオーナーが[詳細管理策]の存在を知り、[詳細管理策]を実施していることを確認する。	―
		閲覧	主たる監査対象【設定】に関する仕様書・設計書を閲覧し、 主たる監査対象【設定】が、[詳細管理策]のとおり設計されていることを確認する。(サンプル１件)	詳細管理策に沿って設計され、実装されていることを、『閲覧』又は『観察」により、確認する。
		観察	主たる監査対象【設定】を観察（視察）し、 主たる監査対象【設定】が、[詳細管理策] のとおり設定されていることを確認する。(サンプル１件)	

	運用	閲覧	管理策に定められた頻度に応じて母集団資料よりサンプルを抽出する。 抽出したサンプル全件を閲覧（レビュー）し、 主たる監査対象【設定】が、監査対象期間にわたって、[詳細管理策]のとおり設定されていることを確認する。	詳細管理策のとおり監査対象期間にわたって設定されていることを、『閲覧』又は『観察』により確かめる。 例） ・設定画面を閲覧し、対象期間にわたって設定されていることを確認 ・設定画面やシステムの動作を観察し、対象期間にわたって設定されていることを確認
		観察	管理策に定められた頻度に応じて母集団資料よりサンプルを抽出する。 抽出したサンプル全件を観察（視察）し、 主たる監査対象【設定】が、監査対象期間にわたって、[詳細管理策] のとおり設定されていることを確認する。	
設備・建物等	整備	質問	コントロールオーナーに質問し、コントロールオーナーが[詳細管理策]の存在を知り、[詳細管理策]を実施していることを確認する。	―
		観察	主たる監査対象【設備・建物】を観察（視察）し、 主たる監査対象【設備・建物】が、[詳細管理策] のとおり実装されていることを確認する。（サンプル１件）	―

第3章　手続の実施に関する基本的な考え方

3.1　手続の実施

3.1.1 前提

ガイドライン「4.4 手続の実施」に記載のとおり、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対して、原則１年間を対象として標準監査手続に準拠して手続を実施する[1]。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、原則１年間を対象として標準監査手続に準拠して手続を実施する。業務依頼者が統制目標あるいは詳細管理策を対象外としている場合には、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言明書の別添に対象外とする理由が記載されていることを確かめる。ただし、業務実施者は、当該対象外とする理由の妥当性の評価は行わない。

なお、手続の実施にあたっては、クラウドサービス事業者の事業概要や対象となるクラウドサービスの概要等、言明書のその他の項目に関わる事項を踏まえて手続を実施することが有益である。また、ISMAP 管理基準「2.2.2 言明の対象範囲」に記載のとおり、クラウドサービスの基盤部分に言明の対象外となるクラウドサービスを利用している場合には、当該サービスが ISMAP クラウドサービスリストに登録されているか、又は登録が予定されていることが必須であるため、手続を実施する際には言明の対象範囲にも留意する必要がある。

3.1.2 手続の実施

業務実施者は、第１章から本章までに定める考え方に従って、第４章に定める標準監査手続に準拠して手続を実施することを原則とする。ただし、管理策の実現方法によって、標準監査手続として定められている監査手続を実施できない場合等においては、業務実施者はその事実について速やかに ISMAP 運用支援機関に問い合わせを行うこと。

標準監査手続では、概ね一つの管理策に対して一種類の「主たる監査対象」を割り当てているが、一つの管理策に対して「主たる監査対象」が複数定められている場合には、規定されている全ての「主たる監査対象」に対して手続を実施しなければならない。

---

[1] 基本規程の附則３に規定のとおり、基本規程の施行から１年以内に登録の申請を行うクラウドサービスに対する監査は整備状況評価のみにより行うこととしていることから、当該期間においては、業務依頼者が言明書において言明する日を基準日として本制度における監査業務を行う。また、業務依頼者が言明の対象とする期間を一時的に１年未満とすることもありうる。

3.2　統制の同質性と母集団の設定

言明の対象となる管理策において以下の全ての特性を満たし、かつ、言明書で示したリージョンの範囲にある場合には、同一の母集団として評価を行うことが可能である。

なお、以下の全ての特性を満たすことについては業務依頼者が責任を有する。

① ガバナンス基準・マネジメント基準の内容が同一である。
② 規程・手順が同一である。
③ 管理策の内容が同一である。
④ 管理する仕組みが同一である。
⑤ 管理策を実施する個人に提供されるトレーニングが共通である等、管理策を実行する個人の能力が一貫したレベルである。

3.3　有効な証跡、サンプル数

整備状況評価において有効となる証跡は、原則として、監査対象期間内のものとする。ただし、監査対象期間内に有効な証跡が存在しない場合は、監査対象期間の末日から 1 年前までのものとする。

運用状況評価においてサンプル数を決定する場合には、業務実施者は、手続の対象として特定された母集団から、統制の頻度または前提となる母集団の構成項目数を元に、表 2 に基づいてサンプル数を決定する。サンプルは手続の対象期間内から無作為に抽出するものとする。他の認証・監査制度等の証拠の利用については、ガイドライン 4.5 の規定に準ずるものとする。

なお、手続の対象期間においてサンプルが発生していない場合には、業務実施者は実施結果報告書の発見事項欄にその旨を記載する。

表 2　運用状況評価におけるサンプル数[2]

統制頻度	母集団の構成項目数	サンプル数
年次	1	1
四半期次	4	2
月次	12	2
週次	52	5
日次	250	25
日に複数回	251 以上	25

[2] 「システム管理基準追補版（財務報告に係る IT 統制ガイダンス）」（平成 19 年 3 月 30 日経済産業省）

3.4　統制の変更

3.4.1 重大な統制の変更及び当該変更につながりうる事象

業務実施者は、業務実施の過程において、重大な統制の変更及び当該変更につながりうる事象の例示に該当する事象が発生していることに気付いた場合には、業務依頼者が ISMAP 管理基準 4.5.5.1 の規定に従って情報セキュリティリスクアセスメントを実施し、ISMAP クラウドサービス登録規則 3.5(3)の規定若しくは ISMAP-LIU クラウドサービス登録規則 7.6(3)の規定に従って ISMAP 運営委員会に報告を行っていることを確かめる。

3.4.2 統制の変更

前項の他、業務実施者は、業務実施の過程において監査対象期間内に統制の変更が発生していたことに気付いた場合には、変更の前後の統制について、それぞれ手続を実施する。

3.1.1 に規定のとおり、本制度における監査業務の対象期間は原則 1 年間とするが、監査対象期間の途中で統制の変更が発生している場合には、当該管理策が最低 3 ヶ月以上の運用期間を経ていることを確認しなければならない。確認の結果、統制の運用期間が 3 ヶ月に満たない場合は、実施結果報告書の発見事項欄にその旨を記載する。

3.5　発見事項

発見事項[3]が存在する場合、実施結果報告書の発見事項欄に手続の実施結果を記載する。記載にあたっては、ガイドライン 4.7.1 に規定する発見事項の定義を踏まえて、どの事実をもって当該手続が発見事項として記載されるに至ったかを業務依頼者及び ISMAP 運営委員会が可能な限り分かるように留意すること。

また、当該発見事項に関して、クラウドサービス事業者が ISMAP クラウドサービス登録規則 3.3 項の規定若しくは ISMAP-LIU クラウドサービス登録規則 7.4 の規定に従って改善計画書を作成していることを確認する。

---

[3] 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。
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の評価は実施しない。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。

第4章　標準監査手続（別添）

本章については、その閲覧及び配布を監査機関に限定するものとする。監査機関は、別添に記載の内容及び運用状況評価に関し ISMAP 運営委員会によって指定された詳細管理策について、本制度における監査業務についてのクラウドサービス事業者との業務契約の締結及び監査業務の実施に必要な限度を超えて漏らしてはならない。

（別紙１）ISMAP 標準監査手続 3.3 に基づきサンプル数を決定できない場合の考え方

監査対象期間が 1 年であり、かつ、ISMAP 標準監査手続 3.3 の定めに従って運用状況評価におけるサンプル数を決定できる場合には、統制頻度または前提となる母集団の構成項目数を元に、表 2 に基づいてサンプル数を決定する。

一方、監査対象期間が 1 年未満の場合など表 2 に基づいてサンプル数を決定できない場合、前提となる母集団の構成項目数のみを元に、別表 1 に基づいてサンプル数を決定する。

別表 1　表 2 に基づいてサンプル数を決定できない場合の運用状況評価におけるサンプル数

母集団の構成項目数	サンプル数
1	1
2～12	2
13～52	5
53～250	母集団の構成項目数の 10% （小数点切り上げ）
251 以上	25

（別紙 2）標準監査手続におけるアップデートテストについて

ISMAP 標準監査手続 3.3 に基づき、手続の対象期間内からサンプルを無作為抽出することを原則とするが、対象期間の始期から対象期間の末日より前の日をサンプルを抽出する期間（以下「サンプル抽出期間」という。）とすることも認める。なお、サンプル抽出期間により対応する場合、原則として以下の条件を満たす必要があり、業務実施者は事前に ISMAP 運用支援機関に問い合わせを行うこと。

・監査対象期間は 1 年
・サンプル抽出期間は、9 ヶ月以上
・監査対象期間に応じた母集団の構成項目数を見積もり、抽出するサンプル数を決定
・サンプル抽出期間において、必要なサンプル数を確保できること
・サンプル抽出期間以外の期間において、統制に変更がないかを確認するために、質問及びサンプル抽出（１件）を行う（以下「アップデートテスト」という）
・監査対象期間経過後、母集団の構成項目数を確認し、抽出したサンプル数に不足があれば、アップデートテストを行わず、ISMAP 標準監査手続 3.3 に基づくサンプル抽出を行う

【抽出するサンプル数の決定方法等（例示）】

○サンプル抽出期間（1～9 月）に毎月 5 件の申請が発生している場合を想定（アップデートテスト対象期間は 10～12 月）
・年間の発生件数を 60 件と見積もり、1～9 月に発生した申請から、別表 1 に基づき 6 件のサンプルを無作為抽出
・10～12 月の期間において統制の変更がないか質問するとともに、10～12 月に発生した申請からサンプル 1 件を無作為抽出し、統制の変更が発生していないかを確認（統制に変更があった場合は、アップデートテストではなく標準監査手続に則った監査を行う）
・なお、年間の発生件数（実績）が 250 件だった場合、抽出すべきサンプル数が 25 件となりサンプルが不足するため、アップデートテストではなく ISMAP 標準監査手続 3.3 に基づくサンプル抽出を行う

（別紙３）ISMAP-LIU における監査業務

ISMAP-LIU に関しては、ガバナンス基準・マネジメント基準の全ての詳細管理策に加えて、以下に掲げるような、クラウドサービスの基盤・構成に深刻な影響を与え重大な事故につながるリスクに関連する詳細管理策を中心として監査を実施する。

１．アクセス管理（特権の管理、ID・パスワード管理、物理セキュリティ等）
２．システムの開発・変更に係る管理（開発管理、変更管理）
３．システムの運用管理（ぜい弱性管理、障害管理、システム運用監視、ネットワーク管理、冗長性の確保等）
４．外部委託先管理（１.～３.に関するもの）