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

令和２年６月３日
(令和３年１２月２０日最終改定)

ISMAP 運営委員会

目次

第 1 章　総則

1.1　本規程の目的

本規程は、「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」（令和２年１月 30 日サイバーセキュリティ戦略本部決定。以下「戦略本部決定」という。）に基づき、内閣官房内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省が運営する「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。）について定めるとともに、本制度に関して、クラウドサービス事業者、監査機関、制度所管省庁、ISMAP 運営委員会、調達府省庁等が遵守しなければならない基本的事項を定める。

1.2　本制度の目的

本制度は、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、もってクラウドサービスの円滑な導入に資することを目的とする。

1.3　本制度の名称

本制度は、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: ISMAP（イスマップ））とする。

また、本制度のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とする仕組みの名称を、ISMAP for Low-Impact Use: ISMAP-LIU（イスマップ エルアイユー）とする。

1.4　用語の定義

1.4.1 クラウドサービス

「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年 6 月 7 日各府省情報化統括責任者（CIO）連絡会議決定）において定義された、「事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるもの」をいう。

1.4.2 クラウドサービス事業者

クラウドサービスを自ら提供する事業者をいう。

1.4.3 監査機関

本制度において 4.3 に規定する登録がなされ、クラウドサービスに対する監査を実施する主体となる法人をいう。

1.4.4 制度所管省庁

本制度を運用する省庁で、内閣官房内閣サイバーセキュリティセンター、デジタル庁、総務省及び経済産業省をいう。

1.4.5 ISMAP 運営委員会

戦略本部決定に基づき制度所管省庁の下に設置される、有識者等で構成された本制度の運用に係る最高意思決定機関をいう。また、ISMAP 運営委員会を運営する事務局を内閣官房内閣サイバーセキュリティセンターに置く。

1.4.6 ISMAP 運用支援機関

9.3 の規定に基づき、本制度の運用に係る事務を ISMAP 運営委員会から委任された機関をいう。

1.4.7 調達府省庁等

本制度においてクラウドサービスを調達する国の行政機関、独立行政法人及び指定法人をいう。

1.4.8 登録

ISMAP 運営委員会が、申請のあったクラウドサービスについて、第 3 章の規定に基づき本制度で定める要求事項を満たすことを確認した上で当該クラウドサービスを 1.4.12 の ISMAP クラウドサービスリスト若しくは 1.4.13 の ISMAP-LIU クラウドサービスリストに記載する行為、又は申請のあった法人について、第 4 章の規定に基づき監査機関として本制度で定める要求事項を満たすことを確認した上で当該法人を 1.4.~~13~~14 の ISMAP 監査機関リストに記載する行為をいう。

1.4.9 監査

本制度において、登録を求めるクラウドサービスにおいてクラウドサービス事業者が行った統制に関する言明に対し、監査機関が本制度で定められた基準・手続等に基づき実施する情報セキュリティ監査をいう。この監査における手続は整備状況評価と運用状況評価の２種類で構成される。

1.4.10 整備状況評価

クラウドサービス事業者が 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、必要な統制を監査の対象期間内の一時点において整備していることを評価することをいう。

1.4.11 運用状況評価

クラウドサービス事業者が 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、整備した統制が監査の対象期間にわたり有効に運用されていることを評価することをいう。

1.4.12 ISMAP クラウドサービスリスト

第 3 章の規定に基づき ISMAP 運営委員会が本制度で要求する基準に基づいたセキュリティ対策を実施していることを確認したクラウドサービスを記載する公開のリストのうち、ISMAP クラウドサービス登録規則に基づき登録がなされたクラウドサービスを記載するものをいう。

1.4.13 ISMAP-LIU クラウドサービスリスト

第 3 章の規定に基づき ISMAP 運営委員会が本制度で要求する基準に基づいたセキュリティ対策を実施していることを確認したクラウドサービスを記載する公開のリストのうち、ISMAP-LIU クラウドサービスリスト登録規則に基づき登録がなされたクラウドサービスを記載するものをいう。

1.4.~~13~~14 ISMAP 監査機関リスト

第 4 章の規定に基づき ISMAP 運営委員会が監査機関として本制度で定める要求事項を満たすことを確認した法人を記載する公開のリストをいう。

第 2 章　制度の体系

2.1　本制度に関する規程等

本制度に関する規程等は次のとおりとする。なお、規程等は原則公開とするが、「ISMAP 標準監査手続」については、その配布を監査機関に限る。

クラウドサービス事業者、調達府省庁等、監査機関、制度所管省庁、ISMAP 運営委員会が遵守しなければならない基本的事項を定めた文書

＜政府情報システムにおけるクラウドサービスのセキュリティ評価制度における制度文書＞	
「ISMAP 基本規程」	政府情報システムにおけるクラウドサービスのセキュリティ評価制度の全体像を定めた本規程。

制度所管省庁及び ISMAP 運営委員会が遵守しなければならない基本的事項を定めた文書

＜ISMAP 運営委員会の運営に関する文書＞	
「ISMAP 運営委員会に関する基本方針」	ISMAP 運営委員会の構成及び所掌事務等に関する基本的な事項を定めたもの。
「ISMAP 運営規則」	本制度の業務運営や ISMAP 運営委員会の組織・手続に関する詳細を定めたもの。

制度所管省庁、ISMAP 運営委員会及び登録を申請するクラウドサービス事業者が遵守しなければならない事項

＜クラウドサービスの登録に関する文書＞

「ISMAP クラウドサービス登録規則」	本制度におけるクラウドサービスの登録に関する手続きや要求事項、登録の可否を判断するための事項を定めたもの。
「ISMAP-LIU クラウドサービス登録規則」	本制度におけるクラウドサービスの登録のうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象に、登録に関する手続きや要求事項、登録の可否を判断するための事項を定めたもの。
「申請者に対する要求事項」	政府情報システムにおけるクラウドサービス事業者に対する要求事項。
「ISMAP 管理基準」	政府情報システムにおけるクラウドサービスのセキュリティに関する要求事項として監査の対象となるもの。

制度所管省庁、ISMAP 運営委員会及び監査機関としての登録を申請する法人が遵守しなければならない事項

＜監査機関の登録に関する文書＞	
「ISMAP 監査機関登録規則」	本制度における監査機関の登録に関する手続きや要求事項、登録の可否を判断するための事項を定めたもの。
「ISMAP 監査機関要求事項」	本制度における監査を実施する監査機関に対して予め求められる要求事項。

監査を行う際に監査機関が遵守しなければならない事項

＜監査の実務における規範・手続に関する文書（以下全てまとめて「情報セキュリティ監査基準等」という。）＞	
「情報セキュリティ監査基準」	経済産業省で定める「情報セキュリティ監査基準」を指し、本制度において監査を行う際に監査機関及び監査業務に従事する者が遵守すべき規範として、「ISMAP 情報セキュリティ監査ガイドライン」の適用の前提となるもの。
「ISMAP 情報セキュリティ監査ガイドライン」	本制度において監査を行う際に監査機関及び監査業務に従事する者が遵守すべき具体的な事項を定めたガイドライン。
「ISMAP 標準監査手続」	本制度において監査を行う際に監査機関及び監査業務に従事する者が遵守すべき、ISMAP 管理基準に位置づけられた個別の管理策等に関する監査の標準的な手続や手法を定めた文書。

2.2　制度を構成する者

本制度を構成する者は、クラウドサービス事業者、監査機関、制度所管省庁、ISMAP 運営委員会及び調達府省庁等とする。

2.3　制度の基本的枠組み

本制度においては、ISMAP 運営委員会が、クラウドサービスに対して求める要求事項及び情報セキュリティ管理・運用の基準たる ISMAP 管理基準を定める。その上で、ISMAP 運営委員会は、本制度において、別に定める ISMAP 監査機関要求事項を満たしていることが確認された監査機関によって、ISMAP 管理基準に基づいたセキュリティ対策の実施状況について情報セキュリティ監査基準等に基づき監査されたクラウドサービスについて、クラウドサービス事業者からの申請を受けて、ISMAP クラウドサービス登録規則又は ISMAP-LIU クラウドサービス登録規則（以下、両規則を「ISMAP 等クラウドサービス登録規則」という。）に基づき要求事項への適合状況を審査した上で、登録が妥当と判断されたクラウドサービスを ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下、両リストを「ISMAP 等クラウドサービスリスト」という。）に登録する。調達府省庁等は 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を原則とする。

第 3 章　クラウドサービスの登録

本章においては、クラウドサービスの登録に係る一連の要求・手続の基本的事項を定める。要求・手続の詳細な事項については、ISMAP 等クラウドサービス登録規則において定めるものとする。

3.1　登録の申請

クラウドサービス事業者は、自身が提供するクラウドサービスについて、本制度において登録を求める場合には、ISMAP 運営委員会に登録の申請を行わなければならない。

3.2　監査

本制度において登録を求めるクラウドサービス事業者は、登録の申請に先立ち、ISMAP 管理基準の遵守状況について言明を行い、第 4 章の規定に基づき登録された監査機関の中から監査機関を選択し、監査を受けなければならない。また、監査機関は当該管理基準の遵守状況について、情報セキュリティ監査基準等に基づいて監査を行い、その結果について実施結果報告書を作成の上、当該クラウドサービス事業者に提供する。

3.3　申請の受理及び審査

ISMAP 運営委員会は、クラウドサービス事業者からクラウドサービスの登録の申請があった場合には、特段の瑕疵がない場合には申請を受理し、登録の可否に係る審査を行う。

ISMAP 運営委員会は、審査にあたり、必要な情報の提供を当該クラウドサービス事業者及び当該クラウドサービスの監査を行った監査機関に求めることができる。

3.4　登録の決定

ISMAP 運営委員会は、申請のあったクラウドサービスについて、審査の結果、適切と判断される場合は登録を認めるものとする。

3.5　登録の更新

3.4 で認められた登録の有効期限は、登録の対象となった監査の対象期間の末日の翌日から 1 年 4 ヶ月後までとする。クラウドサービス事業者は、登録の有効期限までに、登録の更新を申請しなければならない。なお、登録の更新の申請を行った日から当該申請に対する登録の更新の判断が ISMAP 運営委員会でなされるまでは、有効期限以降も引き続き登録を有効とする。

登録の更新に係る一連の要求・手続については、本章の規定を準用する。

3.6　リストの公表と利用

ISMAP 運営委員会は、3.4 によるクラウドサービスの登録を認める場合には、当該クラウドサービスを ISMAP 等クラウドサービスリストに速やかに掲載し公表するものとし、また、3.5 によるクラウドサービスの登録の更新を認める場合は、必要な情報の更新を行うものとする。ISMAP 等クラウドサービスリストには、登録されるクラウドサービスの名称や登録の有効期限の他、ISMAP 等クラウドサービス登録規則の定める範囲で、必要な情報を掲載するものとする。

3.7　報告

クラウドサービス事業者は、登録されている自身のサービスについて、利用者に重大な影響を及ぼしうる情報セキュリティインシデントが生じた場合には、速やかに ISMAP 運営委員会にその概要を報告しなければならない。

3.8　届出

クラウドサービス事業者は、登録されている自身のサービスについて、ISMAP 等クラウドサービスリストにおいて公表されている情報に変更が生じた場合及び登録期間中に重大な統制の変更又はそれにつながりうる事象が生じた場合には、速やかに ISMAP 運営委員会に届け出なければならない。

第 4 章　監査機関の登録

本章においては、監査機関の登録に係る一連の要求・手続の基本的事項を定める。要求・手続の詳細な事項については、ISMAP 監査機関登録規則において定めるものとする。

4.1　登録の申請

本制度における監査機関の登録を求める法人は、ISMAP 運営委員会に登録の申請を行わなければならない。（以下、本規定に基づく申請を行った法人を「申請者」という。）

4.2　申請の受理及び審査

ISMAP 運営委員会は、申請者から申請があった場合には、特段の瑕疵がない場合には申請を受理し、登録の可否に係る審査を行う。ISMAP 運営委員会は、審査にあたり、必要な情報の提供を当該申請者に求めることができる。

4.3　登録の決定

ISMAP 運営委員会は、4.1 の規定に基づく登録の申請について、審査の結果、適切と判断される場合は、当該申請者の登録を認めるものとする。

4.4　登録の更新

4.3 で認められた登録の有効期限は ISMAP 運営委員会による当該登録の決定の日から２年間とする。監査機関は、登録の有効期限までに、登録の更新を申請しなければならない。なお、登録の更新の申請を行った日から当該申請に対する登録の更新の判断が ISMAP 運営委員会でなされるまでは、有効期限以降も引き続き登録を有効とする。

登録の更新に係る一連の要求・手続については、本章の規定を準用する。

4.5　リストの公表と利用

ISMAP 運営委員会は、4.3 による監査機関の登録を認める場合には、当該法人を ISMAP 監査機関リストに速やかに掲載し公表するものとし、また、4.4 による登録の更新を認める場合は、必要な情報の更新を行うものとする。ISMAP 監査機関リストには、登録される監査機関の名称や登録の有効期限の他、ISMAP 監査機関登録規則の定める範囲で、必要な情報を掲載するものとする。

4.6　報告

監査機関は、登録又は登録の更新の申請を行った日から 1 年後に、ISMAP 監査機関要求事項への遵守状況について、ISMAP 運営委員会に報告するものとする。

4.7　届出

監査機関は、登録後に申請時点の情報から変更が生じた場合には、速やかに ISMAP 運営委員会に届け出なければならない。

第 5 章　モニタリングと再監査、登録の停止又は取消し等

5.1　モニタリング

ISMAP 運営委員会は、ISMAP 等クラウドサービス登録規則又は ISMAP 監査機関登録規則の定めるところにより、必要に応じて、ISMAP 等クラウドサービスリストに登録されたクラウドサービス又は ISMAP 監査機関リストに登録された監査機関に対して、本制度への遵守状況等に関する調査を実施することができる。

5.2　再監査

ISMAP 運営委員会は、登録されているクラウドサービスについて、3.8 に規定する届出の内容、5.1 に規定するモニタリングの結果に応じて、ISMAP 等クラウドサービス登録規則に定めるところにより、当該クラウドサービス事業者に対し、監査機関による再監査を求めることができる。

5.3　再申請

ISMAP 運営委員会は、登録されているクラウドサービス又は監査機関について、ISMAP 等クラウドサービス登録規則又は ISMAP 監査機関登録規則に定めるところにより、必要に応じて、クラウドサービス事業者又は監査機関に対し、登録の再申請を求めることができる。なお、再申請後の登録の再審査や再登録については、それぞれ 3.3、3.4 又は 4.2、4.3 の規定を準用する。

5.4　登録の一時停止又は削除

ISMAP 運営委員会は、モニタリング、再審査若しくは ~~又は~~ 再監査の結果に基づき、又は情報セキュリティインシデントが発生した場合に、ISMAP 等クラウドサービス登録規則又は ISMAP 監査機関登録規則に定めるところにより、ISMAP 等クラウドサービスリストへ登録されたクラウドサービス又は ISMAP 監査機関リストへ登録された監査機関の登録の一時停止又は削除を行うことができる。また、本制度に基づく ISMAP 運営委員会の要請に正当な理由なく当該クラウドサービス事業者又は監査機関が応じなかった場合にも、同様の措置を講ずることができる。

第 6 章　登録されたクラウドサービス事業者又は監査機関の権利

6.1　登録されたクラウドサービス事業者の権利

登録されたクラウドサービス事業者は、政府情報システムにおけるクラウドサービスの調達等に際し、自らのサービスを本制度の登録済みのクラウドサービスとして、表明する権利を有する。

ただし、表明に当たっては、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストのどちらに登録されているか明示しなければならない。

6.2　登録された監査機関の権利

登録された監査機関は、本制度において登録を求めるクラウドサービス事業者からの監査の依頼に対し、本制度の監査業務を実施する権利を有する。

第 7 章　制度を構成する者の責任範囲

7.1　ISMAP 運営委員会

ISMAP 運営委員会は、本制度の運用にあたり、戦略本部決定に定められた制度の基本的な枠組みに沿うよう、制度の運用を行う責務を有するとともに、円滑な制度運用のための柔軟な制度の見直しを行う責務を有する。

また、ISMAP 運営委員会は、クラウドサービスの登録、監査機関の登録及び本制度に関する規程等の制定・改廃等について、その意思決定の最終的な責任を負う。

7.2　制度所管省庁

制度所管省庁は、本制度の運用にあたり、9.3 の規定による事務の委任について、ISMAP 運用支援機関が適正な業務を実施するよう適切に監督を行うとともに、円滑な制度運営が行われるよう、ISMAP 運営委員会及び調達府省庁等との調整及び情報提供等を行う責務を有する。

7.3　クラウドサービス事業者

クラウドサービス事業者は、本制度の規程等を遵守するとともに、本制度の規定において要求されている事項に対し、登録の申請において表明した内容を誠実に履行する責務を有する。また、ISMAP 運営委員会の求めに応じて、必要な協力を行う責務を有する。

7.4　監査機関

監査機関は、監査機関の登録に関して本制度で求められる規程等を遵守するとともに、情報セキュリティ監査基準等にしたがって、誠実に本制度の監査業務を行う責務を有する。

7.5　調達府省庁等

調達府省庁等は、本制度の趣旨を理解した上で、自身の調達する情報システム全体のセキュリティ確保を行う責務を有する。

第 8 章　ISMAP 運営委員会が行う業務

ISMAP 運営委員会は、第 3 章から第 5 章に規定された事項のほか、以下の業務を行う。

8.1　規程等の整備

ISMAP 運営委員会は、2.1 に規定する本制度の規程等のうち、「ISMAP 運営委員会に関する基本方針」及び「情報セキュリティ監査基準」以外の規程等の制定・改廃等を行うとともに、必要に応じて、これらの規程等の解釈を行う。

8.2　ガイダンスの発行と公表

ISMAP 運営委員会は、本制度の規程等に関するガイダンスを示すときは、Web サイト等で公表する。

第 9 章 その他

9.1　秘密保持

ISMAP 運営委員会、制度所管省庁、ISMAP 運用支援機関及びその委託を受けた者は、秘密情報が本制度の運用に当たって無権限の者に伝わり、情報の機密性が損なわれることがないようにしなければならない。

9.2　禁止事項

ISMAP 運営委員会、制度所管省庁、ISMAP 運用支援機関及びその委託を受けた者は、次に掲げる事項を行ってはならない。

(1)　監査、審査、登録の結果に影響する利益を得ること。
(2)　監査、審査、登録を申請する者へのコンサルティングサービスの提供をすること。

9.3　事務の委任

ISMAP 運営委員会は、ISMAP 運営規則の定めるところにより、本制度の運用に係る事務を ISMAP 運用支援機関たる独立行政法人情報処理推進機構（以下「IPA」という。）に委任するものとする。IPA は制度所管省庁の監督の下、ISMAP 運用支援機関として委任された事務を行う。

9.4　規則等

本規程で定められた事項のほか、本制度の運営にあたり必要な事項は、ISMAP 運営委員会が ISMAP 運営規則その他 2.1 に列挙する文書において定めるものとする。

9.5　サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議決定事

項への配慮

本規程第 3 章及び第 4 章の実施にあたっては、サイバーセキュリティ対策推進会議、各府省情報化統括責任（CIO）連絡会議において決定された本制度に求められる配慮事項に留意するものとする。

附則（令和２年６月３日　施行）

（施行期日）

１　この規程は、令和２年６月３日から施行する。

（制度立ち上げ時の特例）

２　本制度の施行から当面の間は、調達府省庁等に独立行政法人及び指定法人は含まないものとする。

３　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。

附則（令和２年８月２０日　施行）

（施行期日）

１　この規程は、令和２年８月２０日から施行する。

附則（令和２年１２月２５日　施行）

（施行期日）

１　この規程は、令和２年１２月２５日から施行する。

附則（令和３年６月２２日　施行）

（施行期日）

１　この規程は、令和３年６月２２日から施行する。

附則（令和３年１２月２０日　施行）

（施行期日）

１　この規程は、令和３年１２月２０日から施行する。

附則（令和４年●月●日　施行）

（施行期日）

１　この規程は、令和●年●月●日から施行する。