KPMG

KPMG Insight

KPMG Newsletter

Vol. 44

September 2020

【経営 Topic ③】
ISMAP―国が定めるセキュリティ評価制度

home.kpmg/jp/kpmg-insight

ISMAP－国が定めるセキュリティ評価制度

有限責任 あずさ監査法人
IT監査部
パートナー　　山口　達也
シニアマネジャー　柴田　裕

山口　達也
やまぐち　たつや

柴田　裕
しばた　ゆたか

2020年（令和2年）6月3日より、政府情報システムのためのセキュリティ評価制度ISMAP[1]が正式に運用開始されました。これにより、中央省庁によるクラウドサービスの調達が加速するだけなく、民間でのさらなるクラウド利用が進み、Society5.0の実現に大きな弾みがつくことが見込まれます。

本稿では「ISMAPの概要と今後の展開」について解説すると共に「言明書作成の考慮事項」「ISMAP取得計画時の考慮事項」を詳らかにしています。これらが貴社の取組みの一助となれば幸いです。

なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします（本稿執筆時2020年7月20日現在の情報に基づき作成されたものとなるため、その後情報で最新でない恐れがある点をご留意し、あくまでも参考情報としてご利用ください）。

【ポイント】

- ISMAPは、中央官庁のための仕組みに留まらず、広く外部委託先としてのクラウドベンダ管理における活用が期待される制度である。
- CSP[2]が作成する言明書は、監査機関が実施する情報セキュリティ監査を考慮する必要がある。
- ISMAP取得計画には、「ISMAP基本規程」を始めとする諸規定の内容を理解し、遵守することが必要である。

1　Information system Security Management and Assessment Program の略
2　Cloud Service Provider の略

I. ISMAPの概要と今後の展開

1. 制度概要

政府情報システムのためのセキュリティ評価制度（以下「ISMAP（イスマップ）」という）は初めて国が策定するセキュリティ評価制度であり、2020年6月3日に運用が開始されました。この制度は、国際基準等を踏まえて策定したISMAP管理基準に基づき、各管理基準が適切に実施されているかを第三者であるISMAP監査機関リストに登録された監査機関が情報セキュリティ監査を実施するプロセスを経て、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が確認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する制度です。今後、日本の各政府機関がクラウドサービスを調達する際は、原則として、この制度の公表するISMAPクラウドサービスリストに掲載されたサービスから調達を行うことになります。

このISMAPの基本的枠組みは以下の４点に収斂されます。

- 政府情報システム調達への入札参加を検討するクラウドサービスプロバイダー（以下「CSP」という）は、ISMAP管理基準への適合状況を言明書として作成する。
- 言明書に記載された内容を、監査機関が確認（情報セキュリティ監査）し、実施結果報告書を作成する。
- CSPは言明書と実施結果報告書をISMAP運営委員会に提出し、委員会の審査に合格するとISMAPクラウドサービスリストに登録され公表される。
- 登録の継続には、毎年更新審査が必要となる。

2. 本制度の設立意義

これまでもSOC２やISO認証制度等の情報セキュリティやクラウドセキュリティに関する複数の枠組みが存在していました。本制度は、必ずしも最高水準であることを保証するものではないものの、その要求水準の高低ではなく、国が一定の標準的な水準を設定し、またその状況を確認する具体的なプロセスを明示したという点で、これまで存在した認証制度とは一線を画すものとなっています。ISMAPの制度検討の過程においても、当該制度が単にわが国の各政府機関のみの利用だけでなく、今後は重要産業分野等の企業においても、活用されていくことを想定して策定するとされており、世の中に、「国としての１つのセキュリティ対応における具体的な基準を示した」という点で画期的であると考えられます。

3. 外部委託先管理への期待

本制度は、CSPからの単なる申請のみでなく、情報セキュリティ監査を経て、審査・登録される仕組みであること、また毎年継続して更新が必要であることから、登録されたサービスのセキュリティに関する内部統制が一定のレベルにあることを示すものとして、特に外部委託先管理における委託元企業の管理負担の軽減に寄与することが期待されます。

実際のサービス提供にあたっては、クラウドサービス内で多段階のサプライチェーンが形成されているほか、マルチテナントモデルを前提としているため、委託元（クラウド利用）企業の個別ニーズに対応するカスタマイズは想定しておらず、クラウド利用者が要求するセキュリティ水準の要請にCSPが個別に応えることは、現実的ではありません。さらに、他の利用者との秘密保持契約上の制約を理由に、特定の利用者による個別のモニタリングや情報開示に応じていないCSPもあります。

このような状況に対してISMAPは、登録されたサービスのセキュリティレベルを「保証」するものではないことや、制度上、報告書が非開示であるという限界があるものの、国が認める水準を維持していることが第三者により確認されたサービスとして公表されるものであるため、クラウドサービスの利用企業は、当該制度への登録状況を確認することにより、セキュリティに関して一定の内部統制が維持されていると判断することが可能となります。

本制度の枠組みは、今後の進展次第では、現在さまざまな企業で課題となっているSociety 5.0が示す水平・垂直両方向に拡大するサプライチェーンの多重化・広範囲化が進展する環境における、外部委託先管理に対する１つの実効的な管理手法を提供するプラットフォームとなる可能性も秘めていると考えられます。

4. 今後の展開

本制度は6月に運用が開始された状況であり、最初のISMAPクラウドサービスリストの公表は2020年度後半（第4四半期頃）になると想定されますが、その間にも制度の運用状況を踏まえ、細かな修正や、枠組みの拡大を継続的に検討するための新たなWG等が設置される予定となっています。「クラウドサービスの安全性評価に関する検討会とりまとめ」（2020年1月）によれば、公表されたISMAP管理基準は、政府の情報システム上で取り扱う情報の性質等により求められるセキュリティ水準による管理策基準の項目数・統制の強度等のレベル分けにおいて、レベル２に相当するものであり、将来的には、より簡易で、中堅・中小のCSPでも比較的気軽に申請ができるレベル1や、逆に安全保障に直接関係するような極めて重要性が高いサービスを対象とした、より厳格な要求水準を求めるレベル3の設定も登場する予定となっているとのことです。

また、今後、米国やオーストラリアにおける同様のクラウド評価制度との相互認証を目指すための「日本における評価制度」として位置付けられる可能性もあり、CSPのみではなく、利用する側となるわが国の企業も本制度を理解しておくことが重要であると思われます。

II. 言明書作成の考慮事項

1. 言明書作成のポイント

CSPは、ISMAPの制度が要求する管理基準に対し、自社のクラウドサービスにおいて対応する内容を個別管理策として言明書を通じ明らかにする必要があります。言明書は、言明の対象範囲、システム構成等の情報および次の３区分の管理策のうち実施している項目について記述することが求められます。

- ガバナンス基準（全18項目が必須）
  経営陣に求められる情報セキュリティガバナンスプロセスとして、すべての管理策への対応が求められる。
- マネジメント基準（全64項目が必須）
  管理者に求められる情報セキュリティマネジメントプロセスとして、すべての管理策への対応が求められる。
- 管理策基準（統制目標と詳細管理策で構成される1075項目から実施する項目を選択）
  管理策基準は、組織として対応すべき情報セキュリティ対策として必須とされる統制目標と、各統制目標に対応した詳細管理策で構成されている。原則として、すべての統制目標および基本言明要件に指定された一部の詳細管理策については対応が必須になる。基本言明要件以外の詳細管理策は、言明対象となるサービスに係る組織、環境、技術等に応じて選択する。

2. 詳細管理策の選定

管理策基準のうち、基本言明要件として必須とされる詳細管理策以外については、CSPが言明の対象を選定する必要があります。

詳細管理策のなかには相互に補完関係にあるものがあるため、基本的には、申請対象のサービスにおける情報セキュリティリスクの評価に基づき、各統制目標を実現するための有効性、効率性等を勘案したうえで必要な詳細管理策を選定します。

したがって、統制目標が実現できれば詳細管理策のすべてを対象とする必要はありませんが、選定しない詳細管理策がある場合は、その理由を記述する必要があります。また、選定した詳細管理策に不備が発見された場合には、それと補完関係にある詳細管理策を選択していないことにより統制目標が達成できないというリスクに留意する必要があります。

3. 個別管理策の記述

対象となる管理策（ガバナンス基準、マネジメント基準を含む）の選定後、実際に自社ではどのような対応を行っているかを個別管理策として記述する必要があります。ISMAPにおける管理策の理解と管理策に対する自社の内部統制のマッピングは、これまでSOC２やISO認証制度に対応してきたCSPにとっては比較的容易だと思われますが、管理策自体の数が非常に多いことから、相応の体制を用意して計画的に実施することが望まれます。

社内のリソースで対応が困難な場合は、外部のコンサルティングサービスに委託することも考えられますが、外部委託を行う場合は自社の内部統制の状況を十分理解した担当者が監督することが重要になります。

管理策の読み解きについては、管理策の元となったJIS Q27001／27002／27014／27017の解説書等を参考にすることも有効です。また、各管理策がISMAP管理基準で示される定型管理策1／2／3のいずれに該当するかを把握することで管理策がCSPに求めているレベル（管理策の実施・機能の提供・情報の提供）を理解することが可能になります。

個別管理策の記述にあたっては、対象となる規程や実際の運用において使用される証跡の固有名、および管理策を実施する役職者を明確にしておくことが望まれます。これは監査の際に証跡として提示が必要となるためで、個別管理策の記述の段階から監査を意識することで、監査対応の効率化を図ることが可能です。

4. セルフアセスメントの実施

制度初年度は、情報セキュリティ監査として整備状況の確認が行われます。自社の個別管理策についての整備が実際に行われているか、あらかじめ自社でギャップ調査（セルフアセスメント）を行うことが推奨されます。監査によって発見事項が検出された場合、報告書日付から2ヵ月以内に改善が完了する改善計画書を提出する必要がありますが、発見事項の内容によっては、対応が間に合わない恐れがあるためです。セルフアセスメントでギャップが発見された場合は、整備・運用の改善に要する期間も考慮したうえで言明書に記載する監査対象期間を検討する必要があります。

5. 情報セキュリティ監査への対応

CSPは、監査機関による情報セキュリティ監査を受け、監査機関が発行する「実施結果報告書」を言明書に添付してISMAP運営委員会に登録申請を行います。そのため、CSPは監査機関との監査契約に先立ち、言明書を作成する必要があります。

情報セキュリティ監査は、あらかじめISMAP運営支援機関により審査・登録を受けた監査機関との契約に基づき実施されます。契約に際しては、ISMAP情報セキュリティガイドラインに規定された条項について合意することが必要です。本情報セキュリティ監査自体は保証型監査ではなく、個別管理策の整備状況（制度2年目以降は運用状況も含む）について標準監査手続を適用した結果判明した事実のみを確認・報告するものですが、対象とする個別管理策すべてについて実施が必要なため、監査対応に伴う時間とコストについても見込んでおく必要があります。

III. ISMAP取得計画時の考慮事項

1. 基本事項

ISMAPに取り組むCSPにとって、言明書やISMAP管理基準を理解し、登録を目指すクラウドサービスに合わせて対象となる管理策を選定することは、重要な作業となります。

それと同様に、「政府情報システムのためのセキュリティ評価制度基本規程」をはじめとする各規程の内容を理解し、その定めを遵守しながら、どのように自社の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維持していくかの計画を立てることも重要です。各種規程から計画を検討するうえで知っておくべき基本事項を**図表1**に整理しました。

図表1　基本事項のまとめ

確認事項	制度上の規程事項	参照事項
年間のリスト承認回数	四半期に一度ISMAP運営委員会が開催	ISMAP運営規則 2.3.1
評価対象期間	最低3ヵ月以上1年を超えない期間	ISMAP情報セキュリティ監査ガイドライン 4.4.1 (3)
実施結果報告書日付	言明書に記載の監査対象期間の末日から3ヵ月以内を作成日（報告日）とする実施結果報告書	ISMAPクラウドサービス登録規則 3.2 ISMAP情報セキュリティ監査ガイドライン 4.7.4
提出期限	実施結果報告書の作成日（報告日）から1ヵ月以内に申請が必要	ISMAPクラウドサービス登録規則 4.2
登録の有効期間は？	監査の対象期間の末日の翌日から1年4ヵ月以内に更新申請が必要	ISMAPクラウドサービス登録規則8.1

細かく要件が指定されており、それらを考慮しながら、計画を検討することが重要となります。また、毎年更新が必要となるため、自社の年間イベントを考慮して申請時期を検討する必要もあります。

2. スケジュールイメージ

前述の基本事項に基づき、申請時期によるISMAP申請スケジュールをイメージしたものが**図表2**です。

制度立ち上げ当初は、多少不規則なスケジュールとなることも想定されますが、やがて安定したものになると想定されます。

監査機関による情報セキュリティ監査は、おおむね設定された監査対象期間の後半から監査対象期間の末日後1ヵ月の間で実施されることが多いと思われます。たとえば、10月1日から9月30日を監査対象期間としている場合、6月から10月の間で2回から3回の評価が実施されることになり、相応の業務負荷が想定されます。既に他の認証や監査制度に取り組まれている場合は、監査対応の業務負荷を適度に分散させるなどの検討が必要となります。

図表2　年間スケジュールイメージ

評価対象期間	10月1日から9月30日	1月1日から12月31日	4月1日から3月31日	7月1日から6月30日
実施結果報告書日付	11月中旬	2月中旬	5月中旬	8月中旬
審査文書提出	11月下旬	2月下旬	5月下旬	8月下旬
審査期間	12月から2月中旬	3月から5月中旬	6月から8月中旬	9月から11月中旬
ISMAP運営委員会承認	2月下旬	5月下旬	8月下旬	11月下旬
リスト公表	3月中旬	6月中旬	9月中旬	12月中旬

3. その他の留意事項

ISMAP基本規程附則3に「当初1年間の評価は整備評価のみを行う」とあり、施行日の2020年6月3日から1年以内の申請は整備評価のみを行うことになりますが、これ以降は整備・運用評価が必要となるため、一定の運用期間が必要となります。

ISMAPクラウドサービス登録規則5.6によると、期間内に審査が終えることができないことが明らかな場合、ISMAP運用支援機関が申請を受理しないとあります。不受理になると情報セキュリティ監査の再実施が必要となるため、監査機関との契約前に、ISMAP運用支援機関への問合せを行っておく必要があります。

ISMAP情報セキュリティ監査ガイドライン 4.5で他の認証や監査制度等の結果の利用は認められていません。しかしながらほかの監査への対応にあたって収集した証跡の利用は、容認されていますので、監査機関が同一の場合には、監査対象期間を双方で合わせるといった調整を行うことを前提にすれば監査対応を効率化できる可能性があります。

本稿に関するご質問等は、以下の担当者までお願いいたします。

有限責任 あずさ監査法人
シニアマネジャー　鈴木 雅之
TEL：03-3548-5805（代表電話）
Masayuki.b.suzuki@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
home.kpmg/jp

home.kpmg/jp/socialmedia