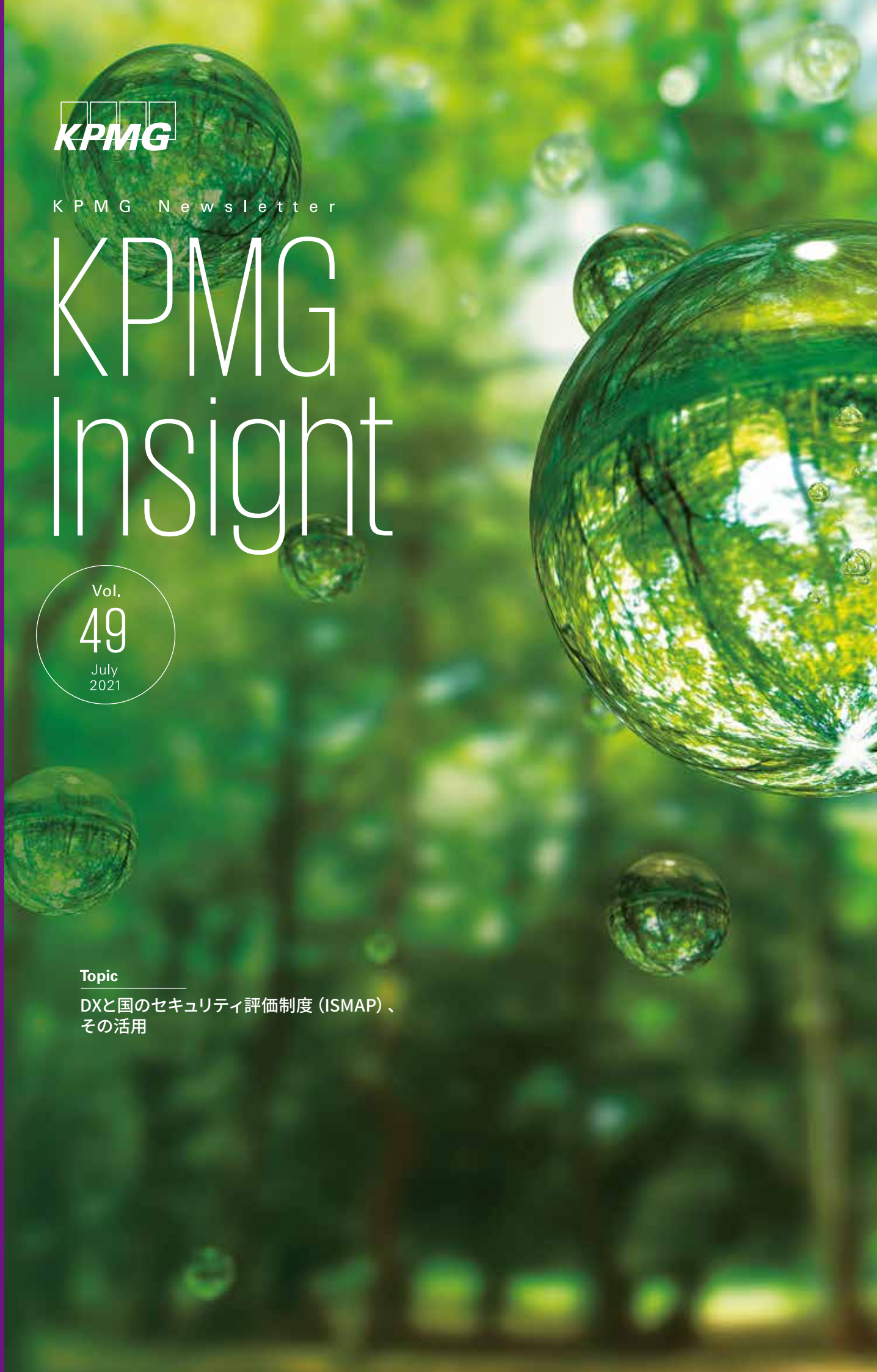

KPMG Newsletter

KPMG Insight

Vol. 49
July 2021

Topic

DXと国のセキュリティ評価制度（ISMAP）、その活用

Topic　ガバナンス・リスク

DXと国のセキュリティ評価制度（ISMAP）、その活用

あずさ監査法人
東京事務所　IT監査部
山口 達也／パートナー

今後、我が国においても、各企業・各分野においてデジタルトランスフォーメーション（以下、「DX」という）を推進していくにあたっては、クラウドサービスの活用が鍵となります。
昨年運用が開始された、日本政府として初となる情報セキュリティ評価制度となりますISMAP※の下、2021年3月12日に初のISMAPクラウドサービスリストが公開されましたが、今後の展開については継続的に検討がなされており、政府省庁以外の調達への適用、クラウド以外の新興技術への拡張等、様々な展開が考えられるため、クラウド事業者のみならず、DX推進を図る一般企業においても今後の動向を注視しておく必要があります。
現行のISMAPクラウドサービスリストについても様々な情報が公開されているため、クラウドサービスの選定、外部委託先としての利用中のクラウド事業者の管理に利用することが可能ですが、利用にあたっては、ISMAP制度を理解したうえで公開情報を読み解き、自社のITガバナンスの下で利用することが必要です。

※ ISMAP:Information system Security Management and Assessment Programの略

☑ POINT 1
我が国のDX推進において、クラウドサービスの利用は、重要な要素となる。

☑ POINT 2
2021年3月12日に初のISMAPクラウドサービスリストが公開されたが、制度としては継続的な検討がされており、クラウド事業者のみならず、DX推進を図る一般企業においても今後の動向にも目を向ける必要がある。

☑ POINT 3
ISMAPクラウドサービスリストの利用にあたっては、ISMAP制度を理解したうえで、公開情報を読み解く必要がある。

山口 達也
Tatsuya Yamaguchi

I 日本のDXとクラウド

1. DXとクラウド利用の概況

我が国におけるDX推進は、新型コロナ感染防止対策の一環として、昨年より急速に拡大したテレワーク環境整備の過程において、まずは「業務のデジタル化」に着手した企業・組織が大幅に増加し、その緒に就いた状況にあると考えられます。しかしながら業務特性や対応コストの問題で、課題は認識しつつも具体的な対応策にまでは至っていない組織・企業も少なからず存在します。現実的なDX推進を考えた場合、特に「対応コスト」と「対応スピード」の確保をいかに実現していくかという点が論点になるケースが多いですが、一時的対応ではなく、今後も対応を続けていく必要があることを踏まえますと、DX推進と表裏一体の関係にあるセキュリティリスクへの対応や、それらの対応に必要な人材確保等、一朝一夕に解決が難しい課題も多いです。

これらの課題に対する有力な解決策の1つとして、クラウドサービスの利用が挙げられるのは、既に認識されているところです。技術的には既に完成しており、また種々の企業の基幹系システムを含む様々な分野において稼働実績が存在し、かつ、導入までのスピードが速いこと、特に、デジタルインフラを保有していない場合の対応コストが従来のオンプレミス（自社運用）でのシステム構築・運用と比較し圧倒的に経済的であること、今後の環境変化への対応や日々のシステム運用に必要な人材確保が一義的にはプロパーでは必要ないこと（厳密には、後述するように、クラウドサービスを利用する場合においても、適切な利用方法やサービスの選択・評価ができるプロパー社員は必要となります）から、現実的な解決策の1つとして考えられています。

2. クラウド利用における課題

一方でクラウドサービスの利用については、様々な課題も認識されています。特に大半のクラウドサービスは、ネットワーク（インターネット）を介して提供されることから、セキュリティ、特にサイバーセキュリティリスクについては十分な対策が必要となることは、昨年来急速に拡大したテレワーク環境の例を見ても明らかです。また業務の一部を自社ではない組織・企業に委ねることから外部委託先としてのサービス提供企業に対するモニタリング、特にセキュリティ対応に関するモニタリングをどう実現していくかという点が大きな課題となります。クラウドサービスの場合は、正にセキュリティ上の理由や利用各社との守秘義務契約上の制約から、具体的な対策の実施状況を直接確認できない場合が多く、実際にはこの問題の解決に時間を要して導入に至っていない企業が少なくないのが現状です。

3. クラウドと第三者評価

この外部委託先管理上の課題を解決するための手段の1つとして認識されているものに、「第三者評価」があります。特にクラウドセキュリティに関する既存の制度として、「ISMSクラウドセキュリティ認証制度」「クラウド情報セキュリティ監査制度（CSマーク）」「SOC2保証報告書」等が存在しますが、これに加え、昨年からは「政府情報システムのためのセキュリティ評価制度（ISMAP）」が追加されました。

この制度は、そもそも政府がクラウドサービス利用を促進する方針（クラウド・バイ・デフォルトの原則：2018年6月 各府省情報化総括責任者（CIO）連絡会議決定）を決定したことに伴い、多様化・高度化するクラウドサービスに対して官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考に検討されたものです。

昨年6月の制度発足後、2021年3月12日に、最初の認定を受けた対象サービス（事業者名を含む）リストが公表されたばかりであり、まだ今後の推移を見守る段階ではありますが、我が国においては、国が定め、運用する初のセキュリティ評価制度でもあり、公表されたサービスリストは、だれでも無料で閲覧が可能であることから、クラウドサービスの外部委託先管理の課題解決の1つとしての活用が期待されるところです。

II ISMAPの沿革と今後の流れ

1. ISMAP制度概要

ISMAP制度についての詳細は、以前の記事（「ISMAP - 国が定めるセキュリティ評価制度」2020-9月号(Vol.44)）において解説しているため、ここでは割愛しますが、一言でいいますと、国が定めた管理基準への対応状況をクラウド事業者自身が言明したうえで第三者の監査を受け、ISMAP運営委員会が審査のうえ、政府が求めるセキュリティ要求水準を満たしていると判定されたクラウドサービスが「ISMAPクラウドサービスリスト」に登録され公表されるというものです。現時点では中央官庁による調達を対象とした制度ですが、公表される「ISMAPクラウドサービスリスト」については、地方公共団体や民間企業が任意で利用することは可能となっています。

2. 管理基準レベル設定と国際相互認証へ

なお、「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月総務省・経産省発表）によれば、現在策定さ

れたISMAP管理基準は、レベル2に相当するものであり、将来的には、中堅・中小事業者でも比較的気軽に申請ができるより簡易な基準（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ている、より厳格な基準（レベル3）も、今後登場が検討されており、これらは、現時点においても一部は継続して検討されている模様です。また、同様の制度として、たとえば、米国におけるFedRAMP、オーストラリアにおけるIRAP等が存在しますが、将来的にはこれらの評価制度との国際的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ることから、クラウドサービス事業者のみでなく、利用企業側（特に、グローバルにビジネスを展開する企業）においても理解しておくことが重要であると思われます。

3.ISMAPスキーム拡大へ

現時点においてISMAPは、クラウドサービスのセキュリティを対象としたものですが、評価の枠組自体は、具体的な基準を規定している「ISMAP管理策基準」を別の基準（たとえばマイナンバーに関する管理策基準等）に置き換えることで、他のセキュリティ評価や、今後登場が予想される新興技術、サービスに対する第三者評価の枠組みとして活用できる可能性もあります。そのような観点からは、本制度を、民間企業側でどう利用できるのかということを理解しておくことは、今後のDX展開において様々な新興技術の利用を検討する際にも役立つものと考えます。

Ⅲ 現時点でのISMAPの利用方法

1.第三者評価利用時の留意事項

ISMAPを含む第三者評価や認証の制度を利用する際、利用者側として認識しておくべき注意点がいくつかあります。

まずは、評価の対象ですが、多くの評価制度においては、監査人が直接、評価対象となる内部統制を決定・評価を実施してはいないケースが多いです。評価対象は、適用宣言書や、言明書、経営者確認書等（以下、「言明書等」という）といわれる、評価対象者が自ら実施している内部統制の内容を記述した文書を対象としており、監査人は、これら言明書等に記載された内容が、事実に照らし合わせて相違ないことを、それぞれの評価制度が定める監査手法を用いて確認し、相違の有無を報告します。従って、言明書等に記載されていない事項については、明示的・暗黙的のいずれにおいても評価はされていない点に留意が必要であり、言明書等の記載と自身が確認したい内容とが整合しているかを利用者は自ら確認した上で利用することが前提となっています。

次にこれら第三者評価を利用する際の利用者側の責任についてですが、現存する各評価制度においては、セキュリティの安全性を直接保証しているものはありません。前述の通り、ほとんどの評価制度は、制度が定める基準に対して、クラウド事業者がきちんと対応しているという言明書等を作成し、そこに記載されている内容が事実と相違ないことを第三者である監査人が確認したという形をとっていますが、逆をいいますと、言明書に記載していないことについては誰も確認はしていないということになります。従って、たとえば「監査人は職業専門家として十分な能力を保有しているか」「監査対象範囲は適切か」「準拠した監査基準は適切か」等の事項を利用者側として確認・判断し、その評価制度が利用できるか否かについて、利用者側が判断することが前提となっています。

なお、ISMAPにおいては、第三者評価を担当する監査機関の資格要件を制度側が定めて審査する仕組みがあります。

2.ISMAPクラウドサービスリストの公開情報

ISMAPにおける公開情報は、上記の言明書等にあたる文書となりますが、言明書の内容の全てが公開されている訳ではなく、詳細な管理策を記載した別添2は、除外されています（詳細なセキュリティ管理策の情報を公開することは、それ自体が重大なセキュリティホールになる場合が多いため）。具体的には、既に公開された情報が情報処理推進機構（IPA）のISMAPホームページ（https://www.ismap.go.jp/csm）から参照できるので、そちらをご覧ください。概略としては、リスト登録番号から始まり、サービス名称、ホームページURL、事業者名称、事業者所在地等ですが、その中に、「言明対象範囲」と「基本言明要件のうち実施している統制目的の管理策」があります（図表1参照）。

「言明対象範囲」には、この制度においてISMAP管理策基準に基づいた対応を実施し、情報セキュリティ監査（ISMAP

図表1　ISMAPクラウドサービスリスト開示項目

リスト登録番号	サービス名称
ホームページURL	事業者名称
事業者所在地	登録日
登録更新期限	言明対象範囲
実施している統制目標	監査対象期間
後発事象	改善計画の有無
資本関係及び役員等の情報	情報に対する国内法以外の法令適用に関する情報
準拠法・採番管轄に関する情報	脆弱性診断の実施状況及び受入に関する情報
特記事項	

登録監査機関による第三者評価）を受け、ISMAP運営委員会の審査を経て登録されているサービスの概要と、対象とするリージョンが記載されています。「基本言明要件のうち実施している統制目的の管理策」においては、ISMAP管理策基準（公開情報）のうち、対応していることを言明しているものと、対応していないものが、統制目的別に記載されています。なおサービスリスト上では、ISMAP管理策基準の項番のみ記載されるため、実際に実施している統制の内容については、「ISMAP管理策基準」と併せて参照することが必要です。

なお、実際に実施されている統制（個別管理策）の記述は、公開情報とはなっていませんが、統制目標を実現するために必要な手段（詳細管理策）は、別途入手可能であるので（著作権の関係で広く一般公開とはなっていないが、該当するISO/IEC基準書（ガイドライン）を保有している場合は、IPAへ問い合わせることにより無料で入手可能）、必要があればそれを確認することができます（図表2参照）。

図表2　ISMAPクラウドサービスリスト活用例

言明書対象範囲

ISMAP管理策基準に基づいて対応がされているサービスの範囲やリージョンが確認できる。

実施している統制目的

別途入手可能なISMAP管理策基準と合わせて確認することでCSPの管理状況を理解することができる。

CSP:Cloud Service Providerの略

3.ISMAPクラウドサービスリスト利用時の留意事項

ここで考慮が必要な点は、ISMAP制度において、この詳細管理策、各クラウド事業者のリスク評価に基づく判断によって取捨選択が可能となっていることです。制度設計の考え方としては、クラウドサービスには、非常に多くのサービス提供パターンがあり、これらを一律に規制する管理策基準を作成することは現実的でなく、あくまでも各社のリスク認識・評価により、各社の判断で採用する管理策を選定することを前提としています。そのため、事業者が適切なリスク評価が可能であることを保証する観点から、上位の基準であるガバナンス基準とマネジメント基準が一律必須項目として指定されており、それらが確立していることを前提に、コスト対効果も含め必要な管理策を検討して選定することを想定しています。そのため公開情報からは、実際にどの詳細管理策が選択されているかは、判断できません。

しかしながら、ISMAPにおける情報セキュリティ監査では、この詳細管理策のレベルまで個別に確認が実施されます。その確認のレベルについて、ここで詳細を述べることはできませんが、採用された詳細管理策については、基本的に文書により裏付けることを原則とし、整備状況の評価においても、統制の実在性を確かめるため、運用証跡のサンプルを1件確認しています。さらに、運用状況の評価については、あらかじめ制度が定めた基準により実際の運用証跡をサンプリングし、証跡によって確認できない場合は情報セキュリティ監査における発見事項として報告されることとなっています。なお、事業者が非採用とした個別管理策については、非採用とした理由が記載されていることまでは監査機関が確認しますが、そこに留まります。この理由の妥当性については、情報セキュリティ監査ではなく、最終的にISMAPサービスリストへの登録の可否を判断するISMAP運営委員会において審査されることとなっています。従って、公開情報とはなっていないものの、一般的な基準・感覚において妥当と判断できるレベルでの詳細管理策の実装・実施状況が登録監査機関により確認されたうえで、政府機関（ISMAP運営委員会）による統制目的の充足状況確認が実施されていると考えてよいと思われ、最終判断は、各利用者に委ねられるものではありますが、サービスリストに登録されているという状況にある程度信頼をおいても問題はないものと考えます。

4. まとめ

あらゆる第三者評価に言えることではありますが、これらの確認が実施されたことをもって、セキュリティ上の安全性が保証されているということではない点は、改めて留意が必要です。また、公開情報から得られるのは統制目的レベルでの対応状況でありますが、そもそも採用されている統制目的が、自社のセキュリティ基準と比較して必要十分であるかという点での検討がまずもって必要となること、すなわち、あくまでも判断基準は利用者自身（自社）のセキュリティ基準にあることを忘れないでいただきたいです。この点がクリアできるのであれば、ISMAPという制度は、民間企業において、クラウドサービスを外部委託先の1つとして管理する一手段としても有用であると思われます。

関連情報

ISMAP

ウェブサイトでは、ISMAPに関する情報を紹介しています。

https://home.kpmg/jp/ja/home/insights/2020/05/what-is-ismap.html

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
鈴木 雅之／シニアマネジャー

Masayuki.b.suzuki@jp.kpmg.com

KPMGジャパン

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

home.kpmg/jp/socialmedia