

政府情報システムのためのセキュリティ評価制度（^{イスマップ}ISMAP）の利用について（案）

令和 2 年 ○ 月 ○ 日
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

平成 30 年 6 月に、政府は「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）を定め、クラウド・バイ・デフォルト原則を掲げた。一方で、現状においては、クラウドサービスプロバイダに要求する統一的なセキュリティ要求基準は存在せず、「政府機関等の情報セキュリティ対策のための統一基準」を踏まえ各政府機関等が調達の際に、個別にプロバイダのセキュリティ対策を確認し調達を行っている。

こうした現状を踏まえ、「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定）において、「クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める」ことが位置付けられた。

また、「デジタル・ガバメント実行計画」（令和元年 12 月 20 日閣議決定）において、クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備がされること及び安全性評価基準、安全性評価の監査の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう環境整備等について検討を進めることが位置付けられた。

これらを踏まえ、「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」（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「基本的枠組み」という。）が決定されたところであり、本決定は、基本的枠組みに基づき、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）連絡会議で詳細を定めるとしていた原則利用や暫定措置（経過措置）のほか、各政府機関等と制度運営委員会（以下「ISMAP 運営委員会」という。）との連携や制度運営に必要な経費の分担の考え方について示すものである。

1 原則利用の考え方について

各政府機関等は、クラウドサービスの調達を行う際は「政府情報システムのためのセキュリティ評価制度（ISMAP）」（英語名：Information system Security Management and Assessment Program、通称：ISMAP（イスマップ）、以下「本制度」という。）において登録されたサービスから調達することを原則とする。なお、当面の間は原則が困難な場合の暫定措置を認めるものとする。

暫定措置による対応も困難なクラウドサービスを調達する場合は、当該調達を行う政府機関等の最高情報セキュリティ責任者の責任において、本制度の要求事項や管理基準を満たしていることを、それぞれの政府機関等で確認する。なお、その確認の実

務に当たっては、最高情報セキュリティ責任者が自らの担務を各責任者に担わせることを妨げない。

また、クラウドサービスの調達においては、クラウドサービスプロバイダの本制度への登録有無を確認の上、未登録の場合は各政府機関等においても登録を促すことが望ましい。

本制度は、政府情報システムの調達を対象とし、「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」の改正や本制度の定着状況等を踏まえ、将来的に、独立行政法人及び指定法人による調達も対象としていく。

2 暫定措置について

基本的枠組みにおいて、クラウドサービスを調達する際には、「本制度において登録されたサービスから調達することを原則」（以下「①」という。）とし、「登録がないサービスの調達については、本制度で要求する事項を満たしていると、当該調達を行う政府機関等で確認する。」（以下「②」という。）としている。

本制度の開始時点で既にクラウドサービスを利用している政府機関等や、開始直後にクラウドサービスの利用を予定している政府機関等では、登録されていないサービスを調達していることとなる可能性があり、基本的枠組みに沿うとすれば、直ちに各政府機関等自身で要求事項の充足について確認するか、サービスの利用を取りやめるなどの検討が必要である。

一方、本制度で登録されたサービスから調達する趣旨は、各政府機関等がそれぞれ独自に確認する非効率を低減し、信頼できるクラウドサービスの利用を促進するものであるところ、本制度開始直後から②の確認を実施する必要がある、却って非効率を助長し、各政府機関等の調達に著しい支障が生じることとなる。このため、自身で確認するための予算確保の必要や手続の複雑さを理由として、クラウドサービスを利用しないと判断することにもなりかねない。

したがって、本制度開始から十分な数のサービスが登録されるまでの間など、やむを得ず調達の実施当初から①を実施することができない場合には、以下の通り暫定措置を実施することとし、その上で、仮に、利用中のサービスの登録見込みがないと明らかになった場合は、各情報システム個別に、対応方針や計画を検討する。

(1) 登録されていないクラウドサービスを利用中又は利用予定の場合

各政府機関等は、やむを得ず、①を実施することができない場合は、当該クラウドサービスの名称や現時点の状況を ISMAP 運営委員会事務局に明らかにした上で、クラウドサービスを利用中の場合は本制度の開始から1年以内に、クラウドサービスを利用予定の場合は当該サービスの利用開始から1年以内に、当該サービスが申請されることを前提として、各政府機関等の責任において利用を継続する。その場合、各政府機関等は、利用中又は利用予定のサービスの提供事業者、本制度の案内、周知を行い、早期登録の推進に努める。また、クラウドサー

ビスプロバイダからその時点での本制度の要求事項や管理基準への適合状況について聴取する。

(2) クラウドサービスの登録申請の見込みがない等明らかになった場合

クラウドサービスを利用中の場合は本制度の開始から1年が経過するか1年を待たずに申請の見込みがないと明らかになった時点で、クラウドサービスを利用予定の場合は当該サービスの利用開始から1年が経過するか1年を待たずに申請の見込みがないと明らかになった時点で、各政府機関等は、速やかに、その状況について ISMAP 運営委員会事務局に報告するとともに、必要に応じて ISMAP 運営委員会事務局が実施する調査に協力する。

なお、情報システムの状況、利用しているサービスの内容は様々であり、必要となる対応や時間を一律に定めることは困難であることから、各政府機関等は、報告後、当該情報システムの対応について検討を行い、移行作業の準備や予算要求等の対応を進める。

(3) その他

今後、本制度の利用推進に資するよう、状況に応じて暫定措置の見直しを行う。

3 各政府機関等と ISMAP 運営委員会との連携について

ISMAP 運営委員会事務局は、本制度の利用者である各政府機関等との連携について、国際規格の改定に伴う管理基準の大幅な改定など、重要な制度変更の場合は、適時に、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）連絡会議に報告し、より実務的な内容に関しては、各政府機関等への説明を行うなど、緊密な連携に努める。

また、ISMAP 運営委員会事務局は、本制度の立ち上げに当たり早期に監査を開始できるように、監査機関の登録等のプロセスに配慮するとともに、必要に応じて、各政府機関等の利用が見込まれるクラウドサービスが速やかに審査されるよう支援する。加えて、各政府機関等の調達に係るクラウドサービスの本制度における申請状況等について、各政府機関等の問合せに対して可能な限り状況を開示する。

各政府機関等は、自身の利用しているクラウドサービスに制度上あるいはセキュリティ上の疑義を認知した場合には、ISMAP 運営委員会事務局に情報共有を行うよう努める。

4 制度運用に必要な経費について

本制度は、従来、各政府機関等が調達の際、個別に確認を行っていたセキュリティ対策を本制度によって一括して確認し効率化を行うものであり、また、政府によるクラウド・バイ・デフォルト原則の方針や、サイバーセキュリティ戦略本部において、本制度の原則利用が決定されていることなどを踏まえ、制度所管省庁は、令

和 3 年度以降の制度運用に必要な経費について検討の上、各政府機関等と分担について調整を行う。