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）

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。

今般、「サイバーセキュリティ戦略」及び「デジタル・ガバメント実行計画」を踏まえて、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（以下「本制度」という。）について、その基本的な枠組みを以下のとおり決定する。

１　本制度の基本的な枠組み

本制度においては、まず、制度として政府機関等（サイバーセキュリティ基本法に定める国の行政機関、独立行政法人及び指定法人をいう。以下同じ。）がクラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の基準を定める。その上で、本制度で定められた情報セキュリティ監査の枠組みを活用した評価プロセスに基づいて、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、本制度が公表するクラウドサービスリストに登録するものとする。

本制度における監査を行うことができる監査機関は、あらかじめ本制度で定める要求事項を満たすことが確認され、本制度が公表する監査機関リストに登録された機関とする。

制度の規程・基準その他の詳細については、後述する制度運営委員会及び所管省庁において決定するものとする。

本制度におけるクラウドサービスの登録は、クラウドサービス自体についての絶対的な安全やリスクゼロを保証するものではなく、本制度において要求する基準に基づき管理プロセスが適切に行われていることを合理的な範囲で確認されたときになされるものである。

従来、調達に当たっては、個々のクラウドサービスが実施していると表明している情報セキュリティ対策の実施状況を、調達する者が直接確認することが必要であったところ、本制度を利用することにより、情報セキュリティ対策の実施状況の直接確認が省略できるとともに、サービスの範囲やセキュリティ対策の範囲について情報提供がなされることで、一定の情報セキュリティ対策の実施が確認されたクラウドサービスを効率的に調達することが可能となる。

２　各政府機関等における本制度の利用の考え方

各政府機関等は、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とし、本制度における登録がないクラウド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の最高情報セキュリティ責任者の責任において、それぞれの政府機関等で確認するものとし、詳細は、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者（CIO）連絡会議において定めるものとする。

本来、情報システムの管理者がリスク評価を行い、適切なリスク管理の下、当該管理者としての責任により情報セキュリティ確保を行うものである。本制度において登録されたサービスを用いる場合であっても、この点は同様である。本制度に登録されているサービスを利用するに当たっては、当該サービスが組み込まれる情報システムの情報セキュリティに係るリスクを適切に把握した上で、当該サービスの機能の範囲や当該サービスが行っている情報セキュリティ対策を踏まえ、情報システム全体の情報セキュリティ対策を実施するとともに、情報セキュリティ確保についての最終的な責任を負わなければならないことに十分留意する必要がある。このため、情報システムの性質を踏まえ、各政府機関等が実際に調達又は運用を行うに当たり、本制度において設定された各種基準に加えて、必要に応じて追加的な要求事項を設定することは妨げられるものではない。また、本制度を運営する立場においても、政府機関等からのニーズや利用状況のフィードバックなどを踏まえ、適切な情報提供を行うなど、本制度の利用に資する取組に努めることが必要である。

なお、経過措置として、制度立ち上げ後一定期間においては登録されるクラウドサービスの数が限定される可能性があること、既に調達プロセスが進行しているクラウドサービスがあること、既に利用しているクラウドサービスがあることなどを踏まえ、各政府機関等の情報システムの調達に著しい支障が生じないよう、制度利用における経過措置、移行期間を十分に確保するものとし、具体的な期間等の詳細は、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者（CIO）連絡会議において定めるものとする。

３　本制度の所管と運用体制

本制度の所管は内閣官房（内閣サイバーセキュリティセンター（以下「NISC」という。）・情報通信技術（IT）総合戦略室）・総務省・経済産業省とする。また本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局をNISCに置く。

事務局は、本制度の運用状況について、サイバーセキュリティ戦略本部に報告するものとする。

本制度の運用に当たっては、本制度の継続的な運用の必要性及び政府の情報セキュリティに係る業務であることに鑑み、独立行政法人情報処理推進機構（以下「IPA」という。）において、制度運用に係る実務及び評価に係る技術的な支援を行うものとする。ただし、IPAは制度運用のうち、監査機関の評価及び管理に関する業務については、業務運用の効率性・実効性確保の観点から、情報セキュリティ監査制度及び監査機関の質の確保に精通した民間団体に、制度運用における中立性にも配慮しつつ、委託することとする。

なお、本制度は政府全体の情報システムの調達に関する質の向上に資するものであることから、令和３年度以降の制度運用に必要な経費の分担については、内閣官房における情報システム関係予算に関する一括計上の取組の活用等も含めた検討を行い、結論を得るものとする。