クラウドセキュリティ
――近年注目を集める「ISMAP」とは?

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
パートナー　**川本 大亮**

はじめに

近年、諸外国と同様に日本企業もテクノロジーの活用、DX推進に鋭意対応している状況です。中でもクラウド活用は重要な成功要素の1つと考えられており、日本においても企業におけるクラウドサービス利用が進んでいます。同時に、クラウド活用を含めた情報システムのセキュリティも大きな課題となってきており、総合的なセキュリティ対策および評価のためのフレームワークが必要となっています。本稿ではそのための参考となるセキュリティ評価制度「ISMAP（イスマップ）」と、ISMAPの枠組みを利用したSaaS向けの「ISMAP-LIU」について解説します。

1 日本におけるクラウド利用の状況とセキュリティに対する不安

総務省が発表した「令和2年　通信利用調査報告書（企業編）」[※1]によれば、クラウドサービスを一部でも利用している企業の割合は68.5％を超えており、日本企業においてもクラウドサービスの利用が進んできていることが分かります。

ただし、その利用の内訳を見ると、メール、ファイル保管・データ共有などのサービスが大半を占めており、業務の基幹となる領域でのクラウド利用は限定的な状況です。日本企業のクラウド利用は進んでいる印象がありますが、クラウドの利用・活用は欧米に比べるとまだまだ遅れているといえます。一方、クラウドを利用しない、もしくは利用範囲を限定している企業において、その最大の理由として挙げられるのが漠然としたセキュリティ不安となっています。

日本におけるクラウド利用の状況についてまとめると、以下のようになります。

- 日本における企業のクラウドサービス利用は年々増加しており、利用の範囲も基幹システムなどの重要システムにまで徐々に広がってきている。
- ただし、グローバルでの状況を見ると、欧米に比べて日本のクラウド利用はまだまだ遅れている。
- 企業がクラウドサービスを導入しない最大の理由は、情報漏洩などセキュリティに不安があるため。
- 日本におけるクラウド利用を加速させるためには、クラウドサービスに対する漠然としたセキュリティ不安を取り除く必要がある。

※1　https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202000_002.pdf

2 ISMAP導入の背景と概要

こうした状況の中、日本政府によるクラウド事業者に対するセキュリティ評価制度として2020年6月よりスタートした政府情報システムのためのセキュリティ評価制度「ISMAP」が注目を集めています。

ISMAP（Information system Security Management and Assessment Program）は日本語で「政府情報システムのためのセキュリティ評価制度」といい、内閣官房内閣サイバーセキュリティセンター（NISC）・デジタル庁・総務省・経済産業省の4省庁で所管している制度です。

導入の背景としては、2018年に日本政府が採用したクラウド・バイ・デフォルト原則があります。これは、今後日本政府として調達するシステムは、原則クラウドサービスの利用を第一候補とする、というものです。

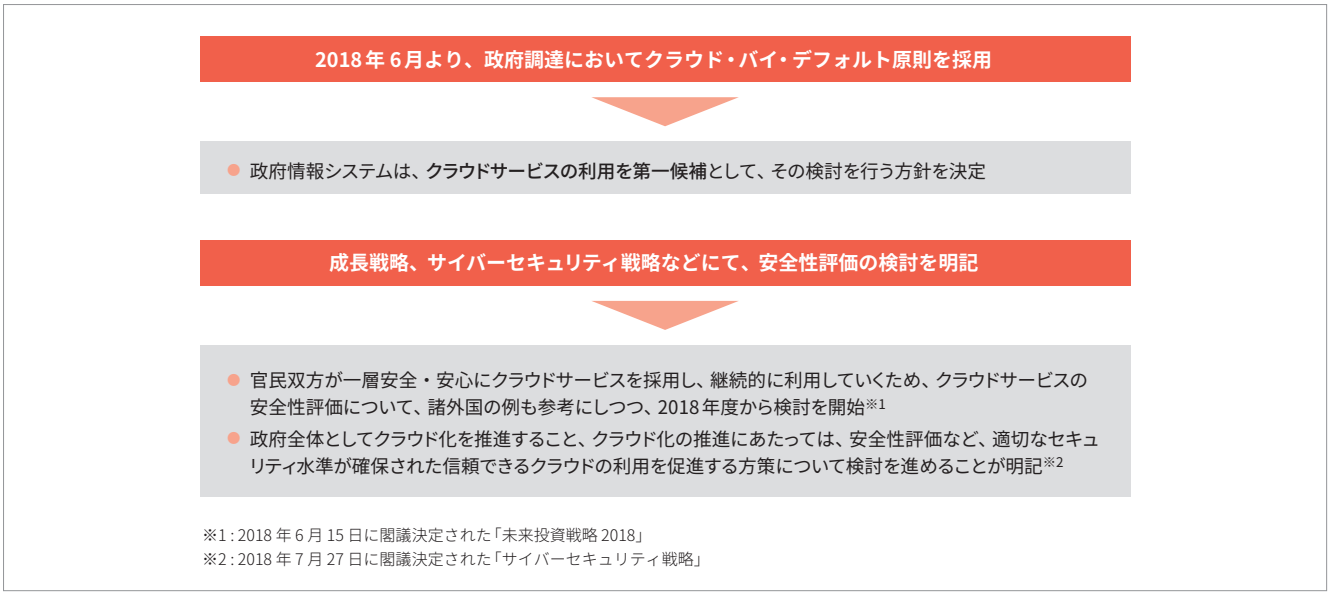
クラウド活用が進まない日本において、政府がこのような方針を打ち出したことは、民間企業にとっても非常に強いインパクトがあります。クラウドサービスを積極的に活用していく方針は打ち出したものの、前述のクラウドサービスに対する漠然としたセキュリティ不安があることは官民変わらない状況であったため、クラウド・バイ・デフォルト宣言とともに、クラウドサービス導入の円滑化を進める観点から、セキュリティに対する統一的な評価を行う仕組み作りの検討が開始されました。そのセキュリティに対する評価の仕組みこそが、政府情報システムのためのセキュリティ評価制度であるISMAPです。ISMAPは諸外国の同様の制度を参考にして設計され、クラウド・バイ・デフォルト宣言の約2年後、2020年秋口から正式にスタートしました（**図表1**）。

ISMAPはISO、NISC、FedRAMP（米国政府機関におけるクラウドセキュリティ認証制度）などの各種セキュリティの管理基準を組み合わせて作成されています。その管理基準への対応がクラウド事業者に求められますが、求められる水準は既存のセキュリティ認証制度よりも高いものとなっています。また、クラウド事業者がその管理基準に対応していることを確認するために、ISMAP監査機関リストに掲載されている監査機関から定期的にセキュリティ評価を受けることになっています。監査機関によるセキュリティ評価を受け、その後さらに制度側が審査を行い、その審査を通過したクラウドサービスがISMAPクラウドサービスリストに掲載されます。そしてその登録簿に掲載されたクラウドサービスから政府はシステム調達を行うことになります（**図表2**）。

3 ISMAP-LIUのスタート

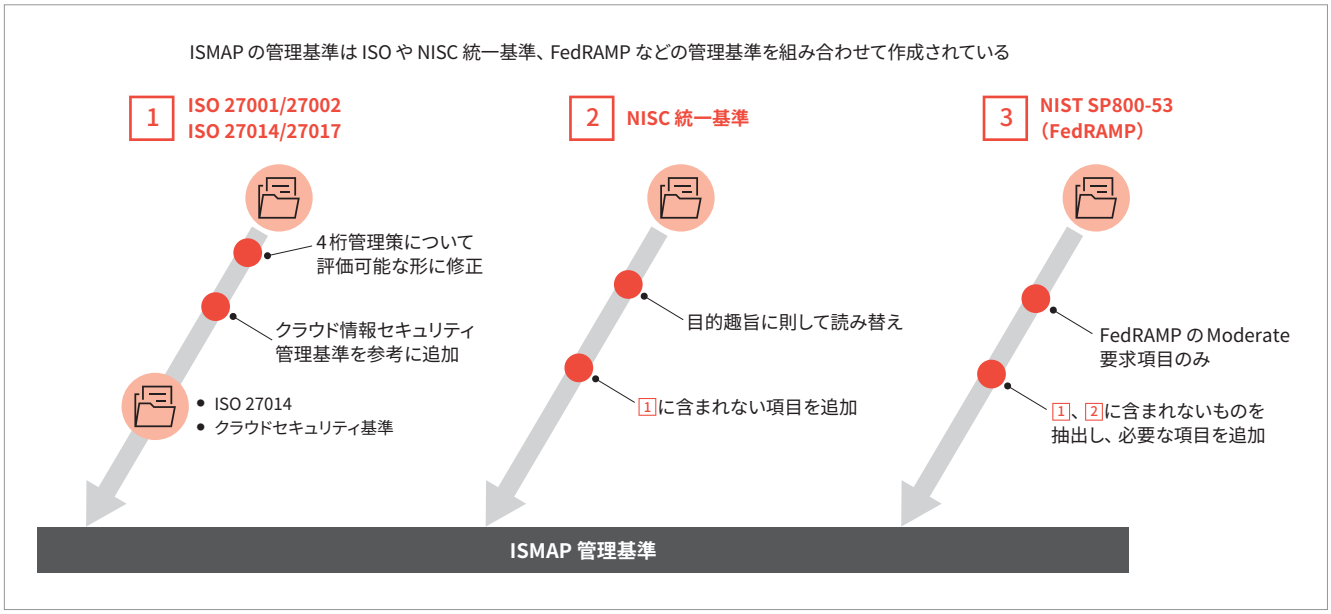
ISMAPの開始から約2年半後の2022年11月1日、ISMAP-LIU（ISMAP for Low-Impact Use）というSaaS向けの仕組

図表1：制度検討の背景



出所：「未来投資戦略2018」と「サイバーセキュリティ戦略」をもとにPwC作成
https://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/miraitousi2018_zentai.pdf
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku-c.pdf

図表2：ISMAPにおけるセキュリティ評価とは？



出所：PwC作成

みの運用が開始されました（**図表3**）。

図表3：ISMAP-LIUとは

概要	「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」に基づき、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 サービスを対象とした仕組み
通称	ISMAP-LIU（ISMAP for Low-Impact Use）
ISMAPとの比較	● 特定の対象業務での利用に制限される ● LIUの対象となるためには事前申請で「該当性あり」と判断される必要がある ● 外部監査の費用は抑えられるが、内部監査対応が必須となる

出所：PwC作成

現行ISMAPの対象となっている機密性2情報（政府におけるデータの重要性のレベルは3段階に分かれており、機密性2は個人情報、機密情報が含まれる）を扱う情報システムはIaaS、PaaS、SaaSと多岐にわたっています。

中でもSaaSはサービスの幅が広く、用途や機能が極めて限定的なサービスや、機密性2情報の中でも比較的重要度が低い情報のみを取り扱うサービス等、リスクが低いサービスもあり、それらのサービスについて現行のISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となり、それにより当該サービスの活用が進まない場合も考えられます。

このため、機密性2情報を扱うSaaSのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組みを創設することとし、現行ISMAPの枠組みをベースとして、外部監査対象範囲の縮小を含め、想定される各論点について検討を行ったものとなりました。

SaaSを対象とした新たな枠組みが登場しましたが、現行ISMAPとの一番の違いは外部監査の枠組みが簡易になった点です。現行ISMAPの詳細管理策は全てを選択した場合1,157存在しますが、LIUにおける対象の管理策数としては概ね5分の1程度になると想定されています。それに付随して、現行ISMAPとの違いとして、セキュリティの内部監査の結果の報告が求められています。また、取消・公表制度というインシデント発生時に登録を即座に一時停止する等の措置を代替的に取り込んでいるところもLIUの特徴の1つとなります。

4 民間企業におけるISMAPクラウドサービスリストの活用

ISMAPクラウドサービスリストはパブリックに公開されており、政府の各省庁だけでなく、民間企業も自由に閲覧可能となっており、登録されているサービス名だけでなく、そのセキュリティ施策の概要、対応領域も知ることができます。

多くの民間企業がクラウド導入の際に、セキュリティ上安全なクラウドサービスを選定することに頭を悩ませたり、独自のセキュリティアセスメントに工数をかけたりしている現状がありますが、ISMAPクラウドサービスリストから、一定のセキュリティ評価をすでに受けているクラウドサービスを

図表4：クラウドサービスにおける責任分界点

レイヤー	IaaS	PaaS	SaaS
アプリケーション	ユーザー	ユーザー	ユーザー／事業者
ミドルウェア（DBMSなど）	ユーザー	事業者	事業者
OS	ユーザー	事業者	事業者
仮想化基盤	事業者	事業者	事業者
物理基盤	事業者	事業者	事業者

出所：PwC作成

知ることができ、民間企業のクラウド導入の早期化にも活用できる可能性があります。

ISMAPクラウドサービスリストは当然参考にはなりますが、その情報を民間企業が利用するにはいくつかの注意点があります。ISMAPはクラウド事業者側のセキュリティ対応を評価するための制度で、その評価を受けてきたクラウドサービスは一定レベルのセキュリティ管理が行われているということは確かにいえますが、クラウドのセキュリティを考えるうえで、クラウド事業者側で対応すべき点と、クラウド利用者側で対応すべき点、いわゆる「責任分界点」をしっかりと理解しておく必要があります（**図表4**）。

企業が安全にクラウドサービスを利用するためには、まず第一に安全なクラウドサービスを選択すること、そして次に利用者として対応すべきセキュリティ管理をしっかりと行うことが必要です。前者にはISMAPクラウドサービスリストを活用することができますが、後者は引き続き企業側で対応するべき点になります。

例えば、クラウド事業者側がしっかりとしたログ機能、多要素認証の機能、暗号化機能などをサービスとして提供していたとしても、その機能をオンにすること、正しく設定すること自体を利用者側で忘れてしまえば、安全なセキュリティ対策にはなりえません。利用企業側の責任範囲を正しく理解して、そこに適切に対応していくことがクラウドサービスを安全に使うために必要な対応となります。

企業側で対応すべき点を知る際に、ISMAPクラウドサービスリストに掲載されているクラウド事業者側の情報や、クラウド事業者が別途発信しているセキュリティペーパーなどを参考にするのは非常に役に立ちます。2022年12月時点で、28社38の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ていますが、ISMAP-LIUの開始により、今後はより一層SaaSサービスの登録が増えることが予想されています。セキュリティ不安を理由にクラウド利用・活用を制限している企業において、ISMAPクラウドサービスリストは今後重要な参考情報となりえるのではないでしょうか。

川本 大亮（かわもと だいすけ）
PwCあらた有限責任監査法人　システム・プロセス・アシュアランス部
パートナー
公認情報システム監査人（CISA）
ITに関するアシュアランスおよびアドバイザリーサービスを日系・外資系企業に提供しており、外部監査、内部監査、US／J-SOXプロジェクト、セキュリティ評価、ITガバナンス、第三者に対する保証と意見表明サービスにおける、ITリスクの発見・評価の経験を豊富に有する。
PwCあらたのクラウドセキュリティチームを率い、セキュリティに関する基準の策定、評価、実装について、規制機関およびクライアントを支援。
メールアドレス：daisuke.kawamoto@pwc.com