政府情報システムのためのセキュリティ評価制度（ISMAP）への対応方法

EYストラテジー・アンド・コンサルティング(株)　Consulting　萩原義信

▸ Yoshinobu Hagiwara

ITベンダーにて業務システムの企画・開発・構築等に従事、また公的機関における大規模ネットワークの構築・運用、電子認証局の運営に従事した後、EYに参画。クラウドサービス事業者、データセンター事業者、金融機関、公的機関等を対象に、SOC1/SOC2保証業務、システム監査、情報セキュリティ監査業務等を多数手掛ける。EYストラテジー・アンド・コンサルティング(株) アソシエートパートナー。

▸ お問い合わせ先　EYストラテジー・アンド・コンサルティング(株)　E-mail：Yoshinobu.Hagiwara@jp.ey.com

Ⅰ　はじめに

2020年に、「政府情報システムのためのセキュリティ評価制度」が施行されました。この制度に取り組むべく準備にいそしんでいる企業もあれば、すでに取り組みつつも制度対応に要する手間とコストにお悩みの企業もあることでしょう。

本稿では、クラウドサービスの提供者と利用者双方にとって重要なこの制度の概要を説明するとともに、その特徴と効果的に取り組むためのポイントを解説します。

Ⅱ　政府情報システムのためのセキュリティ評価制度（ISMAP）の狙い

「政府情報システムのためのセキュリティ評価制度」はその英語名「Information system Security Management and Assessment Program」の頭文字を組み合わせてISMAP（イスマップ）と呼ばれます。内閣官房・総務省・経済産業省が所管するこの制度は、日本の政府機関等へクラウドサービスを円滑に導入することに資するべく設けられました。

日本政府は、情報システムの調達に当たってはクラウドサービスの利用を第一候補にすることとしていますが、クラウドサービスにはそのセキュリティを不安視する声もあります。この不安を払拭（ふっしょく）するには、クラウドサービスの調達時にそのセキュリティ対策の状況を綿密に評価し、問題がないことを確かめる必要があるでしょう。しかし、このような評価作業は調達側にとって大きな負担になり、クラウドサービスの調達をためらわせる要因にもなります。

そこで、政府機関等が調達する前に、あらかじめクラウドサービスの安全性を評価しておこうと制定されたのがISMAPです。評価済みのクラウドサービスから調達すれば、個々の政府機関等が評価する負担は軽減されます。調達に応じるクラウドサービス事業者も、調達のたびに政府機関ごとの対応を迫られるより、政府の共通的な評価軸が明確に打ち出されたほうが透明感があるでしょう。

さらに、本制度の評価軸となる基準と審査を経て調達対象として認められたサービスが公表されれば、クラウドサービスのセキュリティに関する有用な情報となり、政府機関等とクラウドサービス事業者にとどまらず、広く国民にとって有意義な制度になるはずです。（<図1>参照）

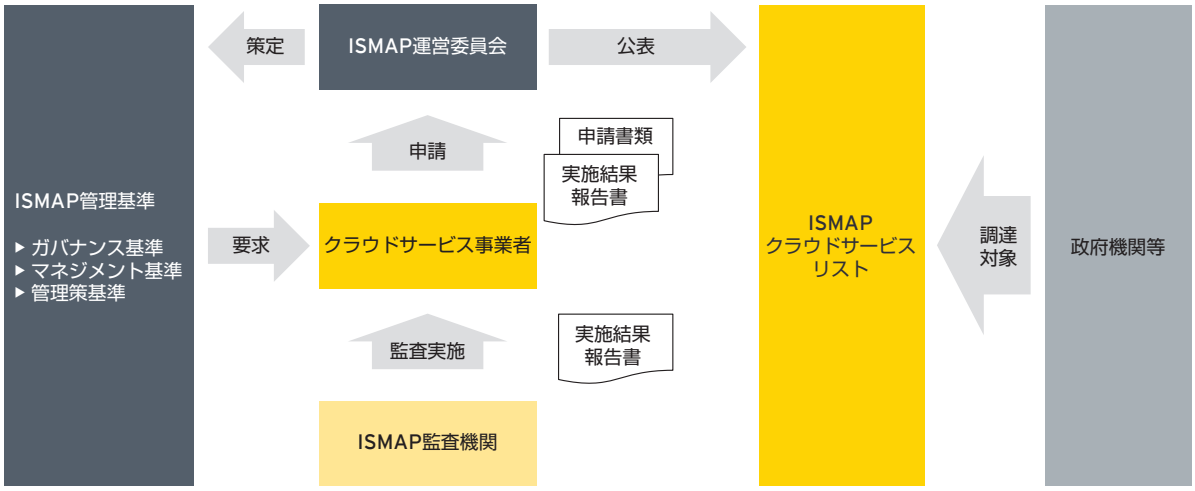
Ⅲ　政府情報システムのためのセキュリティ評価制度（ISMAP）の概要

ISMAPには次の三つの特徴と利点があります。

1. クラウドサービス事業者が満たすべき基準があらかじめ定められ、公表されていること

本制度では、制度所管省庁の下に設置されたISMAP運営委員会により、クラウドサービス事業者が満たすべきISMAP管理基準が定められています。ISMAP管理基準は、経営陣が実施すべき事項を定めた「ガバナンス基準」と、管理者が実施すべき事項を定めた「マネ

▶図1　政府情報システムのためのセキュリティ評価制度（ISMAP）の枠組み



ジメント基準」と、組織が具体的に実施すべき事項を定めた「管理策基準」から構成されています。

ISMAP管理基準が公表されることで、政府へサービスの提供を希望するクラウドサービス事業者は何を要求されるのかが明確になります。国民にとっても、政府が事業者に要求していることが分かることで、クラウドサービス上に構築された政府のサービスへの安心感が増すでしょう。

2. 第三者であるISMAP監査機関が情報セキュリティ監査を行うこと

クラウドサービス事業者のセキュリティ対策の状況を、ISMAP管理基準に照らして調べるのがISMAP監査機関です。ISMAP監査機関も審査を経て登録が認められた機関であり、ISMAP監査機関を掲載したリストも一般に公開されています。このリストを参照することで、情報セキュリティ監査等に専門性を有し、政府機関等に代わって情報セキュリティ監査に当たる機関を知ることができます。

EYは、ISMAP監査機関として本制度の監査業務を実施しています。

3. 登録されたクラウドサービスのリストが公開されること

ISMAP監査機関による情報セキュリティ監査を受けたクラウドサービスは、ISMAP運営委員会による審査を通ると、ISMAPクラウドサービスリストに掲載されます。政府機関等は、原則としてこのリストに掲載されたサービスを対象に、情報システムの調達を行います。

このリストは一般に公開されますので、政府機関ばかりでなく地方公共団体や民間企業等も審査を通ったクラウドサービスを知ることができます。このような情報の提供を通して、政府調達の透明化が図られるでしょう。

Ⅳ　他の制度との違い

情報セキュリティの評価制度というと、ISO27001やISO27017等の認証と何が違うのかという疑問が湧くかもしれません。

ISO関連の審査では、事業者は審査員の求めに応じて質問に答えたり文書を提示したりします。事業者は受け身な立場になりがちです。

一方、ISMAPでは、クラウドサービス事業者がISMAP管理基準の要求を理解し、自社のサービスにおいてどのように対処しているかを具体的に記述して、言明書として提出しなければなりません。従って、ISOの審査を受けるよりも能動的に制度に取り組む必要があります。

ISMAP監査機関が実施する手続はISOの審査より詳細なものになりますので、クラウドサービス事業者が対応に要する時間も手間も大きくなります。

Ⅴ　効果的な取り組み方

これまでISMS等に取り組んできたクラウドサービス事業者の皆さまは、ISMAPにも対応することを負担に思うかもしれません。ISMAPでは実施すべきことが細かく規定されており、対応に要する労力を削減するのは容易ではないからです。

そこで、ISMAPだけを捉えて取り組み方の効率を検討するよりも、各種制度の負荷を総合的に判断することが重要になってきます。

EYでは、ISMAPはもとより、ISO関連の審査やSOC保証業務等、各種制度に一括して対応できる体制を整えています。事業者の皆さまができるだけ負担を軽くしながら各制度に取り組んでいただけるように、ご相談に応じています。