

## 「政府情報システムのためのセキュリティ評価制度（ISMAP）対応事前診断サービス」の開始

一般社団法人日本セキュリティ格付機構（略称：JaSRO、本社：東京都中央区）は、新サービス、「ISMAP 対応事前診断サービス」を新規販売・提供開始する運びとなりましたのでお知らせいたします。

### 1. 背景

政府は2018年6月、「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、政府情報システムのシステム方式について、コスト削減や柔軟なリソースの増減等の観点から、クラウドサービスの採用をデフォルト（第一候補）とし、府省CIO補佐官の関与の下、事実に基づく客観的な比較を行いその利用を判断するための考え方等を示しました。一方で、諸外国と比較した場合、日本は国家としてクラウドサービスの安全性を評価・認定する仕組みが存在しておらず、評価・認定制度を検討することになりました。

このクラウドサービスの安全性を評価・認定する仕組みは、内閣サイバーセキュリティセンター・情報通信技術（IT）総合戦略室・総務省・経済産業省が運営する、政府情報システムのためのセキュリティ評価制度（ISMAP:Information system Security Management and Assessment Program）です。ISMAPに則り、政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することで、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスを円滑に導入することを目的としています。2021年に予定されているISMAPの運用開始により、原則としてリストに登録されているクラウドサービスから政府情報システムの調達が行われるため、政府情報システムにクラウドサービスが選定されるにはISMAPクラウドサービスリストへの登録が必須になります。

さらに、ISMAPクラウドサービスリストは一般に公開されるため、政府情報システムの調達のみならず、地方公共団体や民間企業がクラウドサービスを選定する場面においても活用される可能性があり、リストにクラウドサービスが登録されることが、数兆円規模と予想される国内クラウド市場に参入する上で重要なアドバンテージになることが予想されます。

### 2. 課題

一方、ISMAPクラウドサービスリストへの登録を目指す事業者は、各種国際基準等に基づき策定された「ISMAP管理基準」（「ご参考 ISMAP管理基準について」参照）に準拠して、自社クラウドサービスの対応状況を確認し、説明書に適合状況を表明する必要があります。1,000を超える項目に記載された標準管理策の内容と、それらに対応するリスクを理解する必要があり、自社の特定の部門のみで行うことは容易ではないことが想定されます。弊社では情報セキュリティおよび監査の専門家が「ISMAP対応事前診断サービス」として、クラウドサービス事業者が行ったリスク分析結果を踏まえ、クラウド情報セキュリティ監査に向けた効率性も考慮した上で事前準備をサポートします。

●お問い合わせ先 一般社団法人日本セキュリティ格付機構（略称：JaSRO） E-mail:info@jasro.org <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当社の意見であり、その正確性、完全性、網羅性等は必ずしも保証されていません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当社は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当社に留保され、当社に専属的に帰属するものとします。

### 3. サービス内容

弊社は、クラウドサービス事業者が自社のクラウドサービスを ISMAP クラウドサービスリストへ登録申請するための準備作業に対する助言業務を提供します。ISMAP における情報セキュリティ監査業務で実施する「ISMAP 標準監査手続」に準拠し、クラウドサービス事業者が言明するクラウドサービスに関する情報セキュリティ対策の実施状況に対する GAP 分析の実施、GAP 分析で判明した発見事項・改善案等を提供します。また、必要に応じて、クラウドサービス事業者が進める申請のための各準備作業にかかる助言業務も提供します。

#### 【ご提供するサービス内容（代表例）】

- ① 情報セキュリティ対策の実施状況把握（省略可能）
  - (ア) アセスメントシートによる事業者の方の自己評価（リスク分析）
  - (イ) 簡易診断実施、「情報セキュリティ対策の実施状況」と「ISMAP 管理基準」との GAP 可視化
  - (ウ) ISMAP 管理基準とお客様統制とのマッピング案提示
  - (エ) アセスメント結果報告会実施
- ※①：実施状況把握のみのサービス提供可能
- ② 「ISMAP クラウドサービスリスト」登録申請準備作業支援
  - (ア) 「情報セキュリティ対策の実施状況」と ISMAP 管理基準との GAP 詳細分析
  - (イ) GAP 分析で判明した発見事項の指摘
  - (ウ) GAP 分析で指摘した発見事項に対する改善案の提示
  - (エ) 言明書及び経営者確認書作成支援
  - (オ) その他登録申請するための準備作業に対する助言

#### 【実施期間（代表例）】

- ① 情報セキュリティ対策の実施状況把握 (ア) (イ) (ウ)：2 カ月から 3 カ月程度  
(エ)：半日程度（アセスメント結果報告会）
- ② 登録申請準備作業支援 (ア) (イ) (エ)：2 カ月から 6 カ月程度  
(ウ)：半日程度（発見事項・改善案報告会）  
(オ)：随時（詳細は別途取決め）

### 4. 価格

- ① 情報セキュリティ対策の実施状況把握：300 万～
  - ② 登録申請準備作業支援：600 万～
- ※いずれも予定価格、消費税別、詳細は別途見積

### 5. その他関連サービス

ISMAP サービスリスト登録における情報セキュリティ監査業務（準備中）

ISMAP サービスリスト登録以外の情報セキュリティ監査業務（対応可、個別相談）

●お問い合わせ先 一般社団法人日本セキュリティ格付機構(略称:JaSRO) E-mail:[info@jasro.org](mailto:info@jasro.org) <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当社の意見であり、その正確性、完全性、網羅性等は必ずしも保証されてはいません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当社は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当社に留保され、当社に専属的に帰属するものとします。

○セミナー開催及び打合せをTV会議システム等にて随時行います。  
ご希望の方はE-mailにて、[info@jasro.org](mailto:info@jasro.org)宛にご連絡ください。

＜お問い合わせ先＞  
一般社団法人日本セキュリティ格付機構  
企画部  
E-mail : [info@jasro.org](mailto:info@jasro.org)

以上

ご参考 ISMAP 管理基準について

ISMAP では、クラウド事業者が統制の目標を実現するために選択し、満たすべき事項として、「管理策」と呼ばれる基準が設けられています。クラウド事業者が選択した「管理策」を、外部評価機関が「評価」することになります。「管理策」「評価」には、それぞれ以下のような特徴が存在します。

＜管理策の構成＞

管理策は、「A. ガバナンス基準」「B. マネジメント基準」「C. 管理策基準」の3つの基準で構成されています。

A. ガバナンス基準

ISO/IEC 27014 をベースに作成されており、会社のセキュリティガバナンスの要求事項が記載されています。

B. マネジメント基準

ISO/IEC 27001 をベースに作成されており、情報セキュリティマネジメントシステムの確立についての要求事項が記載されています。

C. 管理策基準

ISO/IEC 27002/27017、内閣サイバーセキュリティセンター（NISC）の「政府機関等の情報セキュリティ対策のための統一基準」、National Institute of Standards and Technology（NIST） Special Publication 800-53 の内容を組み合わせて構成されています。

＜管理策の選定＞

クラウド事業者は「C.管理策基準」に該当する管理策の中から、統制目標を達成するために必要な管理策を選択し適用します。

＜必須の管理策＞

クラウド事業者は、管理策のうち「A. ガバナンス基準」「B. マネジメント基準」については、全ての管理策が必須となるため、全て実施する必要があります。

「C. 管理策基準」については、必須の管理策と選択適用の管理策があります。

必須の管理策は全て実施する必要がありますが、選択適用の管理策は「管理策の選定」で選択した管理策を実施することになります。

●お問い合わせ先 一般社団法人日本セキュリティ格付機構(略称:JaSRO) E-mail:[info@jasro.org](mailto:info@jasro.org) <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当社の意見であり、その正確性、完全性、網羅性等は必ずしも保証されていません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当社は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当社に留保され、当社に専属的に帰属するものとします。