はじめてのISMAP

- 政府情報システムのためのセキュリティ評価制度の概要 -

本パンフレットはクラウドサービス事業者・情報システム調達者の方々のISMAPへの理解促進を目的に作成しております

クラウドサービス事業者向け　情報システム調達者向け

そもそも　イスマップ

ISMAP

Information system Security Management and Assessment Program　とは・・

政府情報システムのための セキュリティ評価制度のこと。

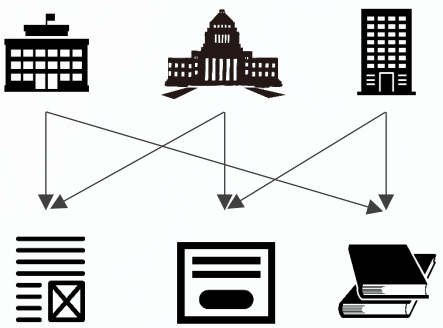
ISMAPは、国際標準等を踏まえて策定した**基準**に基づき、
登録監査機関による**監査**のプロセスを経て、クラウドサービスを**評価・登録**します。

登録されたクラウドサービスは**「ISMAPクラウドサービスリスト」**に掲載され、
政府機関等は原則としてこのリストからクラウドサービスを調達することとされています。

ISMAPは、従来各政府機関等が個別に評価していたクラウドサービスの
セキュリティ要件について統一的な評価を可能にし、
政府機関等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と**円滑な導入**を**目的**としています。

制度導入前

各政府機関等が独自に
全てのセキュリティ要件を最初から確認



クラウドサービスの導入に係る
様々な方針やガイドライン等が存在

非効率

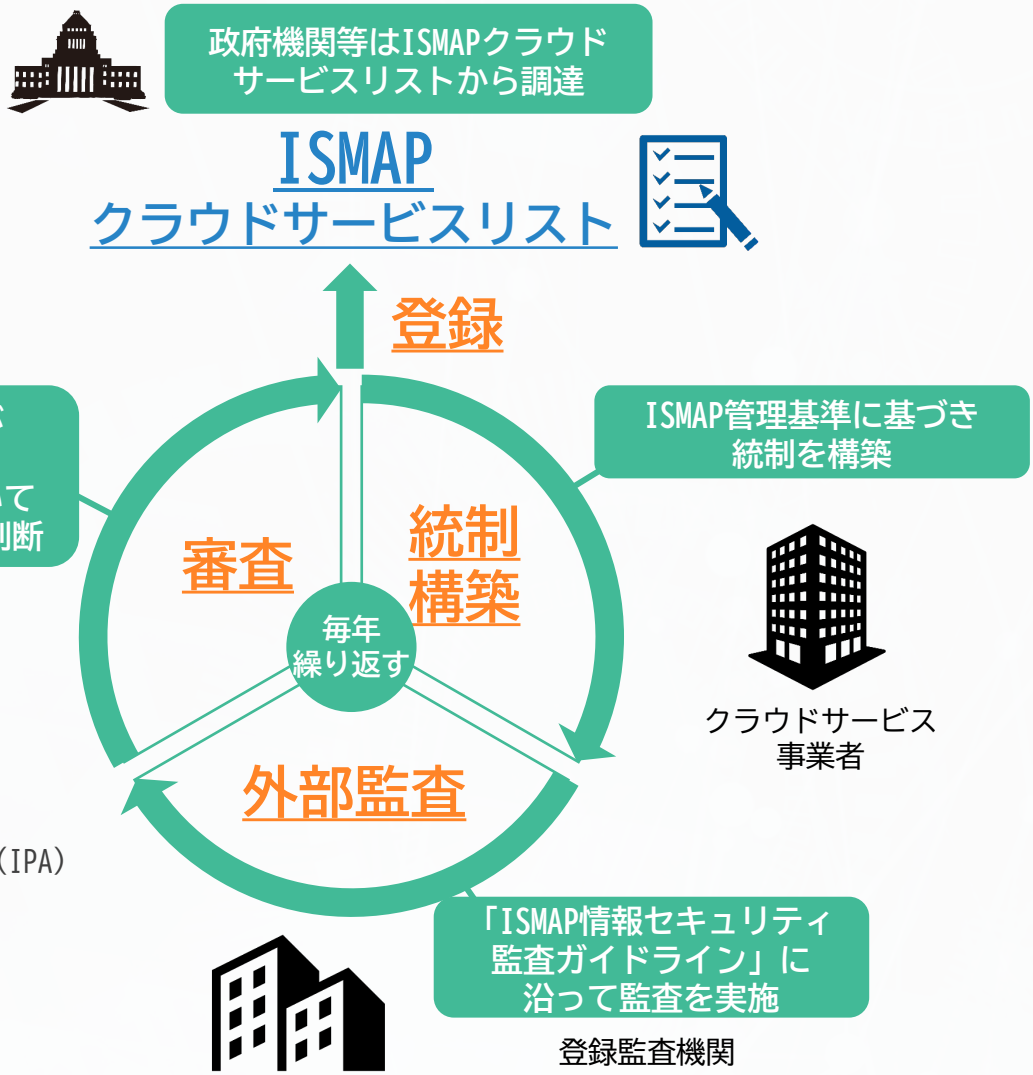
制度の目指す姿

制度は共通する
セキュリティ要件の充足を評価
各政府機関等が確認するのは追加要件のみ

統一的なセキュリティ基準

効率的

制度の基本的な枠組み



クラウドサービス事業者がリストに登録するメリット

- セキュリティ要件への対応をまとめられる
- 政府から安全性について一定の評価を受けたことの証明

クラウドサービス利用者がリストを活用するメリット

- 第三者監査を受けたサービスを選べる
- 自社サービスの安全性確認の一部に活用できる
- 自社でのクラウドサービス利用に対外的な信頼感が得られる

クラウドサービス事業者向け

サービスリストへの登録サイクル

ISMAPクラウドサービスリストの登録サイクルは
「統制構築」・「外部監査」・「審査」から構成されます

統制構築

統制構築では、「ISMAP管理基準」に基づいて、
クラウドサービス事業者が登録を希望する
クラウドサービスの管理体制を整備します。

ISMAP管理基準は
「JIS Q 27000シリーズ」「政府統一基準」「NIST SP800-53」を
取り込んだ形で作成されており、
「①ガバナンス基準」「②マネジメント基準」「③管理策基準」の
3種の基準で構成されています。

※JIS Q 27000シリーズ：JIS Q 27001・JIS Q 27002・JIS Q 27014・JIS Q 27017
※政府統一基準　　：政府機関等のサイバーセキュリティ対策のための統一基準群
※NIST SP800-53　　：米国国立標準技術研究所 組織と情報システムのためのセキュリティおよびプライバシー管理策

	対象	統制事項	実施例
ガバナンス基準 ①	経営陣 	セキュリティに関する意思決定や指示を継続的に実施している	情報セキュリティの戦略及び方針を承認する 等
マネジメント基準 ②	管理者 	組織が実施する情報セキュリティマネジメントのルールを確立し、継続的な運用や維持管理を実施している	情報セキュリティマネジメントの確立、運用や維持管理 等
管理策基準 ③	業務実施者 	実際にセキュリティ対策を実施している	アクセス管理 アカウント・ID管理 冗長性の確保 ログ取得及び監視 等

外部監査

外部監査では、「ISMAP情報セキュリティ監査ガイドライン」に沿って監査機関による第三者監査が行われます。

- クラウドサービス事業者は監査機関を**ISMAP監査機関リスト**から選定
- 契約は**クラウドサービス事業者と監査機関**で結ぶ
- 監査は定型化された**標準監査手続**に基づき実施される

クラウドサービス事業者

証跡やサンプル等の提出　等

「実施結果報告書」の作成・提出　等

登録監査機関

- 監査機関には**要求事項**が定められており**登録制**。**2年**ごとに**更新**を行う

審査

審査は、ISMAP運用支援機関によって行われ、ISMAP運営委員会にて登録の是非の判断後、クラウドサービスリストへ登録されます。

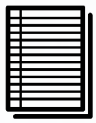
申請文書作成

登録申請

クラウドサービス事業者

ISMAPポータルサイトより申請文書の事前相談が可能

・登録申請書
・言明書
・実施結果報告書
　等を提出



登録審査

ISMAP運用支援機関

受理した申請文書について、技術的審査を実施。必要に応じ、追加の情報提供を要求

ISMAP運営委員会

最終的な登録の是非を判断する

ISMAPクラウドサービスリスト　登録

クラウドサービス事業者向け

ISMAP-LIU（イスマップ・エル・アイ・ユー）の紹介

ISMAP for Low-Impact Use

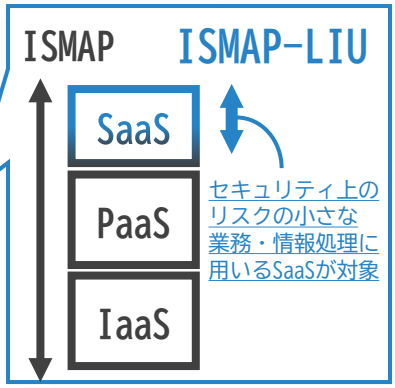
ISMAP-LIUは、リスクの小さな業務・情報の処理に用いる
SaaSサービスを対象とする枠組みです。

策定の背景

クラウドサービスのうちSaaSは、
提供される機能、取り扱う情報が多岐にわたり、
リスクの小さな業務に利用する場合、
ISMAPと同じ取扱いとすると、
過剰な要求事項となりうる。

ISMAPとの違い

対象とするクラウド
サービスの範囲を限定



ISMAP-LIU 対象業務一覧※

※ISMAP-LIUにおける業務・情報の影響度が低位である蓋然性が高い業務を例示したもの

① 公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務

② 政府機関等職員の業務上の役職・氏名等情報を扱う業務

③ 名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務

④ 民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務

⑤ オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合

⑥ 災害時等に組織構成員の被災状況確認等を行う業務

⑦ 組織構成員に対する組織ルールやビジネススキル等の教育を行う業務

⑧ 「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務

⑨ システムの維持・管理のために、性能や稼働状況を確認する業務

⑩ スケジュール調整、タスク管理、イベント管理、反復処理などの作業を効率化するために、職員を（機械的に）補助する業務

クラウドサービス事業者向け　情報システム調達者向け

ISMAPポータルサイト

https://www.ismap.go.jp/csm

ISMAPのことなら
ISMAPポータルサイトまで

規程を確認する

クラウドサービス事業者向け規程類

ISMAPクラウドサービス登録規則

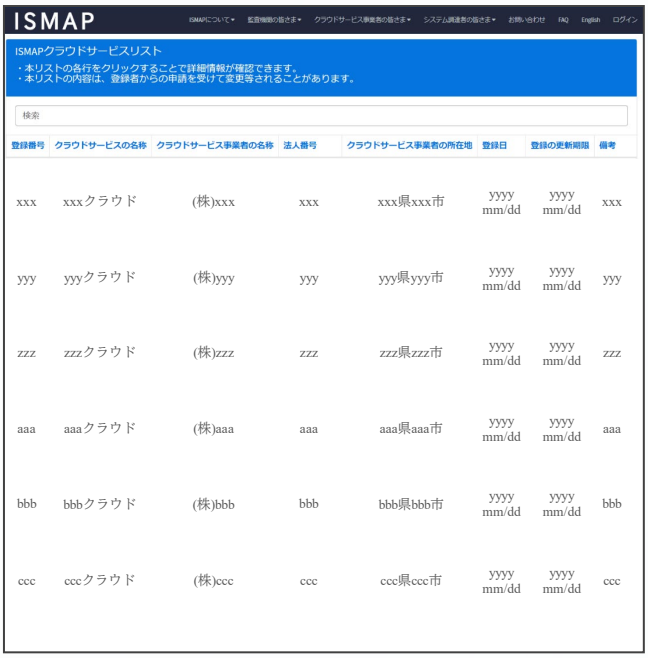
ISMAP-LIUクラウドサービス登録規則

ISMAP運営委員会が定める基本規程に基づいた
クラウドサービスの登録に関する事項が定められています。

ISMAP管理基準

クラウドサービス事業者がISMAPクラウドサービスリスト
若しくは、ISMAP-LIUクラウドサービスリストへの
登録申請を行う上で実施すべきセキュリティ対策の一覧、
及びその活用方法を示しています。

ISMAPクラウドサービスリストを確認する



リスト一覧

確認したいクラウドサービスの行を
クリックすることで
詳細情報が表示されます。

リストの詳細情報

確認できる詳細情報
- クラウドサービスの名称
- クラウドサービス事業者の名称
- 当該クラウドサービスのHPのURL
- 改善計画書の有無

等

添付文書

確認できる添付文書
- 言明対象範囲
- 実施している統制目標の管理策
- リスク評価を行うために必要な情報

等

ISMAPの歩み

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において、
クラウド・バイ・デフォルト原則が採用され、
政府情報システムはクラウドサービスの利用を
第一候補として検討を行うこととなりました。

2019年12月

デジタル・ガバメント実行計画において、
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、クラウドサービスの
安全性評価を検討することを位置付けました。

2020年6月

「政府情報システムのための
セキュリティ評価制度（ISMAP）の利用について」が
定められ**ISMAPの運用開始**。

2021年3月

「ISMAPクラウドサービスリスト」の初回登録・公開を行い、
政府機関による本制度の利用を開始。

2022年11月

ISMAPの枠組みのうち、
リスクの小さな業務・情報の処理に用いるSaaSサービスを
対象にした**ISMAP-LIUの運用開始**。

ご質問・お問い合わせ

ISMAPポータルサイト内部のお問い合わせページより
お問い合わせください。
https://www.ismap.go.jp/csm

発行者：内閣サイバーセキュリティセンター、デジタル庁、総務省、経済産業省

本パンフレットの掲載内容の一部及び全てについて、無断で複製、転載、転用、改変等の二次利用を固く禁じます。
パンフレットについてのお問い合わせ先：総務省　サイバーセキュリティ統括官室　https://www.soumu.go.jp/main_sosiki/cybersecurity/index.html