

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 -



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。

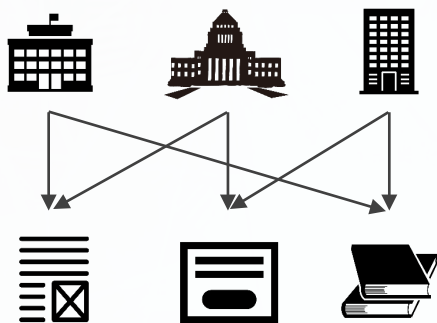
ISMAPは、国際標準等を踏まえて策定した**基準**に基づき、登録監査機関による**監査**のプロセスを経て、クラウドサービスを**評価・登録**します。

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



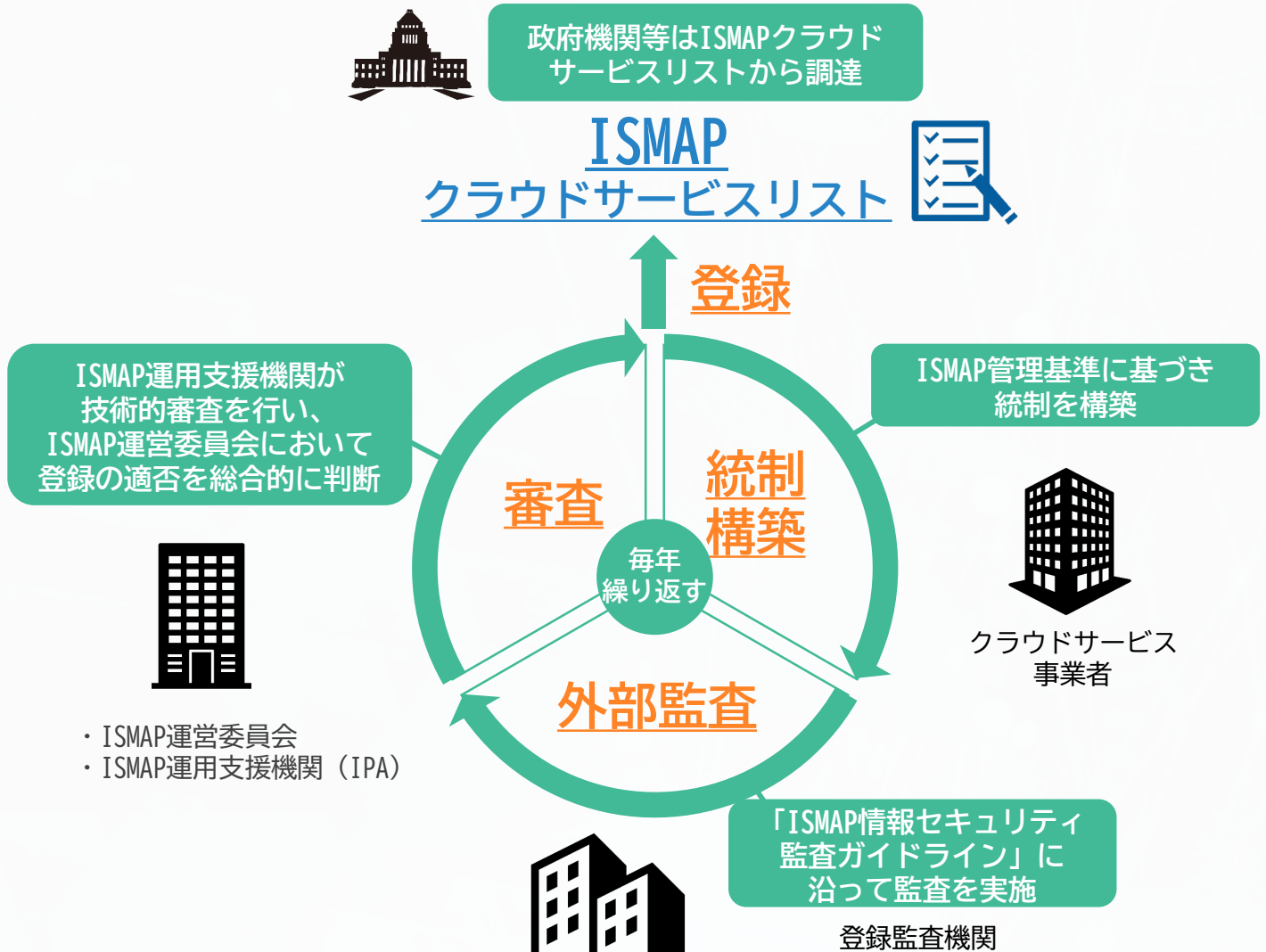
参照・引用



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

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

経営陣

① ガバナンス基準



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

管理者

② マネジメント基準



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

業務実施者

③ 管理策基準



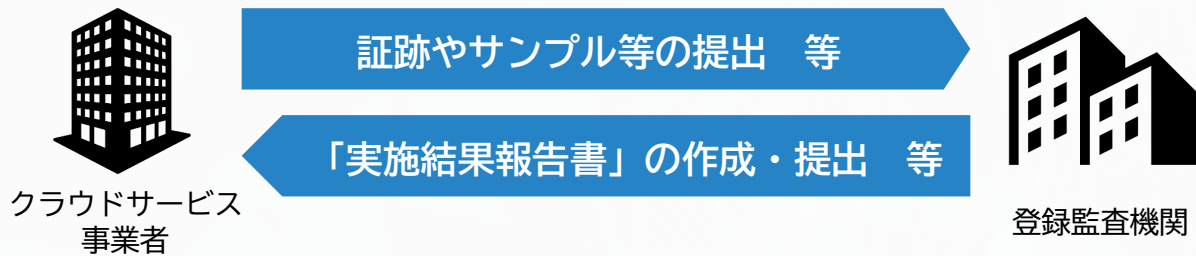
実際にセキュリティ対策を実施している

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。

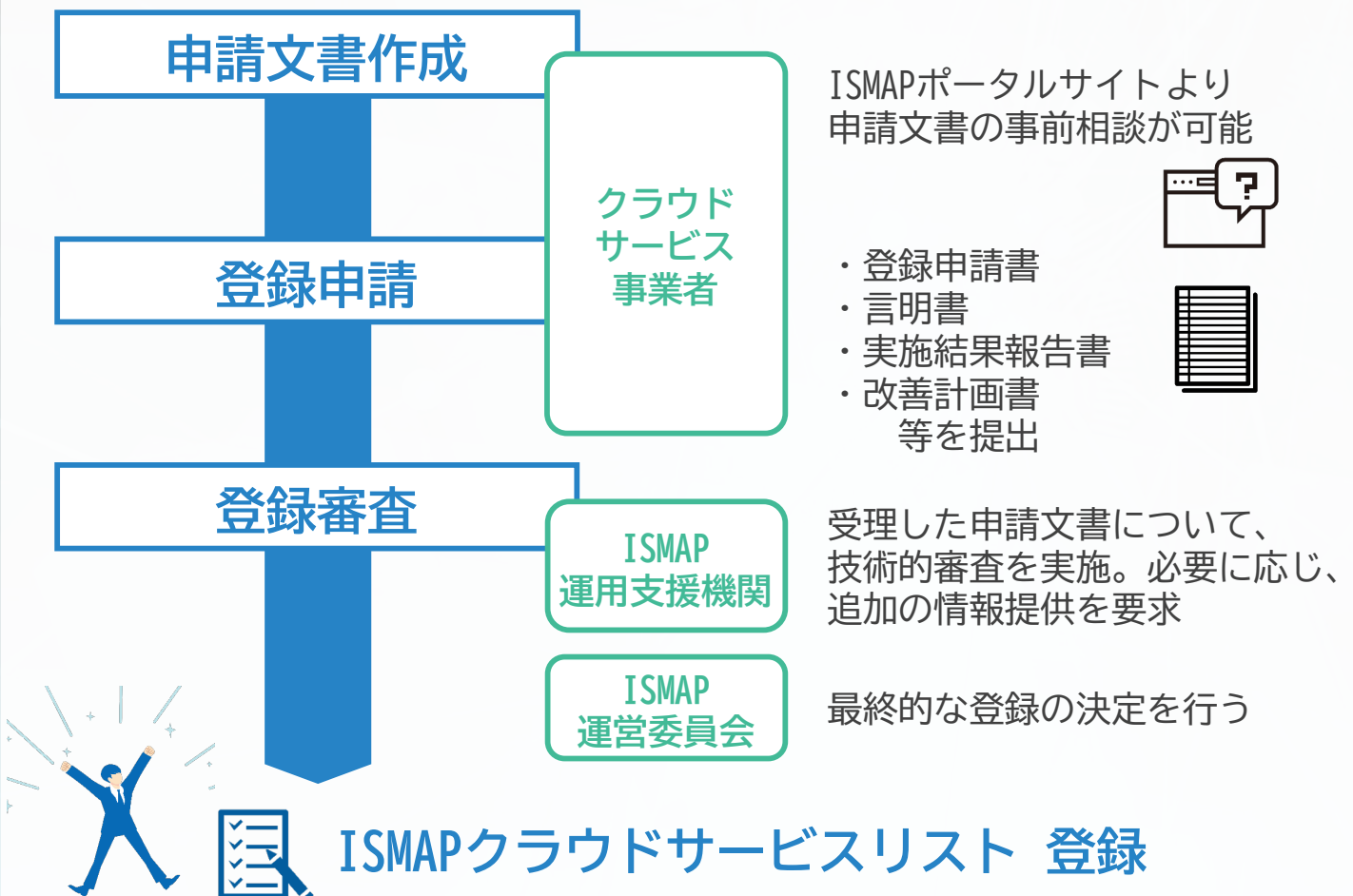
- ☑ クラウドサービス事業者は監査機関を **ISMAP監査機関リスト** から選定
- ☑ 契約はクラウドサービス事業者と監査機関の間で **民間同士の契約** を結ぶ
- ☑ 監査は定型化された **標準監査手続** に基づき実施される



- ☑ 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運営委員会の決定後、クラウドサービスリストへ登録されます。



ISMALP-LIUの紹介

ISMALP for Low-Impact Use

ISMALP-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。事前申請により、ISMALP-LIUに該当する事が認められれば外部監査の項目が縮小されるなど、クラウドサービス事業者の負担が軽減されます。

策定の背景

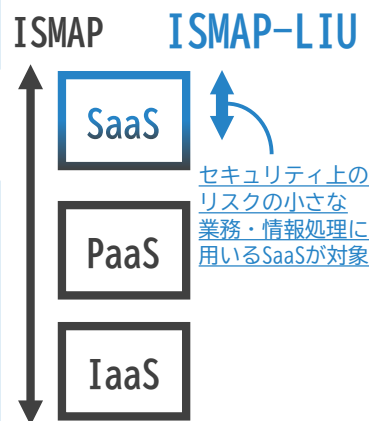
クラウドサービスのうちSaaSは、提供される機能、取り扱う情報が多岐にわたり、リスクの小さな業務に利用する場合、ISMALPと同じ取扱いとすると、過剰な要求事項となりうる。

ISMALPとの違い

対象とするクラウドサービスの範囲を限定

政府機関等による影響度評価や事前申請が必要

ISMALPよりも外部監査の対象項目を縮小



ISMALP-LIU申請の流れ

STEP 1

利用する各政府機関等においての業務・情報の影響度が低位であることを審査

STEP 2

STEP 1 の評価結果と事前申請書の提出

STEP 3

外部監査・本申請へ

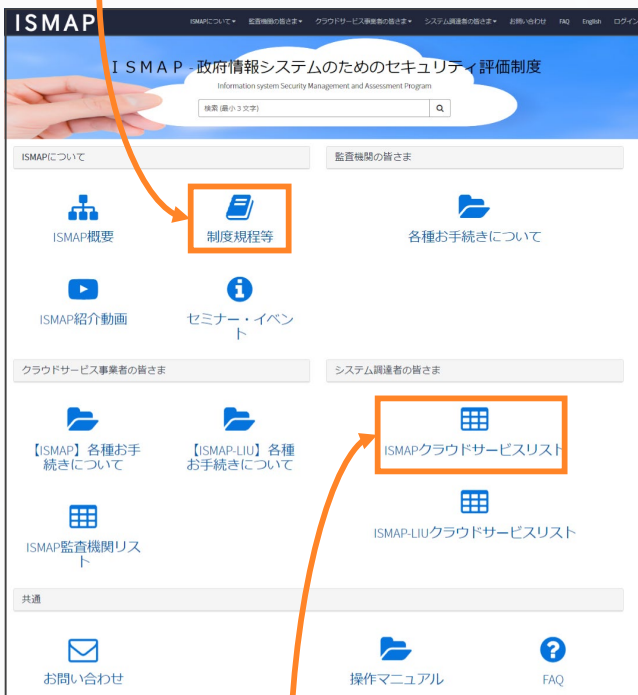
ISMAPポータルサイト

<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

登録番号	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	法人番号	クラウドサービス事業者の所在地	登録日	登録の更新期間	備考
xxx	xxxクラウド	(株)xxx	xxx	xxx県xxx市	yyyy/mm/dd	yyyy/mm/dd	xxx
yyy	yyyクラウド	(株)yyy	yyy	yyy県yyy市	yyyy/mm/dd	yyyy/mm/dd	yyy
zzz	zzzクラウド	(株)zzz	zzz	zzz県zzz市	yyyy/mm/dd	yyyy/mm/dd	zzz
aaa	aaaクラウド	(株)aaa	aaa	aaa県aaa市	yyyy/mm/dd	yyyy/mm/dd	aaa
bbb	bbbクラウド	(株)bbb	bbb	bbb県bbb市	yyyy/mm/dd	yyyy/mm/dd	bbb
ccc	cccクラウド	(株)ccc	ccc	ccc県ccc市	yyyy/mm/dd	yyyy/mm/dd	ccc

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

ISM MAP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（ISM MAP）の利用について」が定められ**ISM MAPの運用開始**。

2021年
3月

「ISM MAP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

ISM MAP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**ISM MAP-LIUの運用開始**。

ご質問・お問い合わせ



ISM MAPについて



ISM MAP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>

ISM MAP-LIUについて



デジタル庁の「ISM MAP-LIU相談窓口」よりお問い合わせください。

https://www.digital.go.jp/policies/security/ismap-liu#help_desk

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