政府情報システムのためのセキュリティ評価制度（ISMAP）について

令和２年 ８月５日

総務省　サイバーセキュリティ統括官室

本制度の名称

日本語名：政府情報システムのためのセキュリティ評価制度
英語名　：Information system Security
　　Management and Assessment Program
通称　　：ＩＳＭＡＰ（イスマップ）

１．検討の背景

クラウド・バイ・デフォルト原則

■ **2018年6月より、政府調達においてクラウド・バイ・デフォルト原則を採用。**

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

(2018 年6月7日 ＣＩＯ連絡会議決定)

2 基本方針

2.1 クラウド・バイ・デフォルト原則

政府情報システムは、クラウド・バイ・デフォルト原則、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとする。

クラウドサービスの安全性評価の必要性

未来投資戦略2018(2018 年6月15日 閣議決定　抜粋)

クラウドサービスの多様化・高度化に伴い、官民双方が一層安全・安心にクラウドサービスを採用し、継続的に利用していくため、情報資産の重要性に応じ、信頼性の確保の観点から、クラウドサービスの安全性評価について、諸外国の例も参考にしつつ、本年度から検討を開始する。

➡ 2018年８月より、**「クラウドサービスの安全性評価に関する検討会」**(座長：工学院大学名誉教授　大木榮二郎、事務局：総務省・経済産業省)を開催。

2019年度の政府決定

■ **サイバーセキュリティ戦略本部第２３回会合において、①本制度の基本的な枠組み、②本制度の利用の考え方、③本制度の所管と運営体制を決定。**

政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて

令和２年１月３０日　サイバーセキュリティ戦略本部決定

１．本制度の基本的な枠組み

本制度で定められた評価プロセスに基づいて、要求する基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、本制度が公表するクラウドサービスリストに登録。

２．各政府機関等における本制度の利用の考え方

各政府機関は、クラウドサービスを調達する際は本制度において登録されたサービスから調達することを原則とし、本制度における登録がないクラウドサービスの調達や、経過措置の詳細は、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において定める。

３．本制度の所管と運用体制

本制度の所管は内閣官房（NISC、IT室）・総務省・経済産業省とし、本制度の最高意思決定機関として、有識者と所管省庁を構成員とした制度運営委員会を設置し、事務局をNISCに置く。

事務局は、本制度の運用状況について、サイバーセキュリティ戦略本部に報告を行う。

本制度の運用に当たっては、（中略）独立行政法人情報処理推進機構（以下「IPA」という。）において、制度運用係る実務及び評価に係る技術的な支援を行うものとする。ただし、IPAは制度運用のうち、監査機関の評価及び管理に関する業務については、（中略）情報セキュリティ監査制度及び監査機関の質の確保に精通した民間団体に、（中略）委託すること。

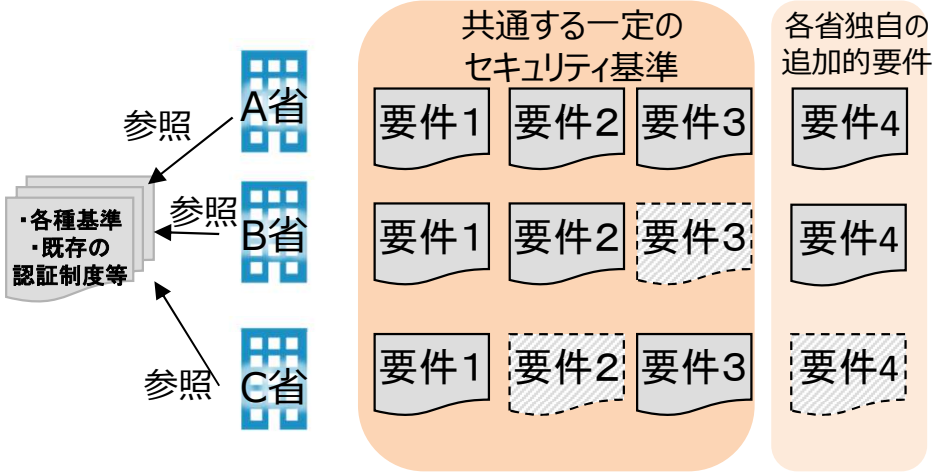
２．制度について

ISMAPの目指す姿

■ 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するが、同じクラウドサービスに対して**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することとなり、非効率**。

⇒**クラウドサービスについて、統一的なセキュリティ基準を明確化し、実効性・効率性のあるクラウドのセキュリティ評価制度(ISMAP)を検討。**

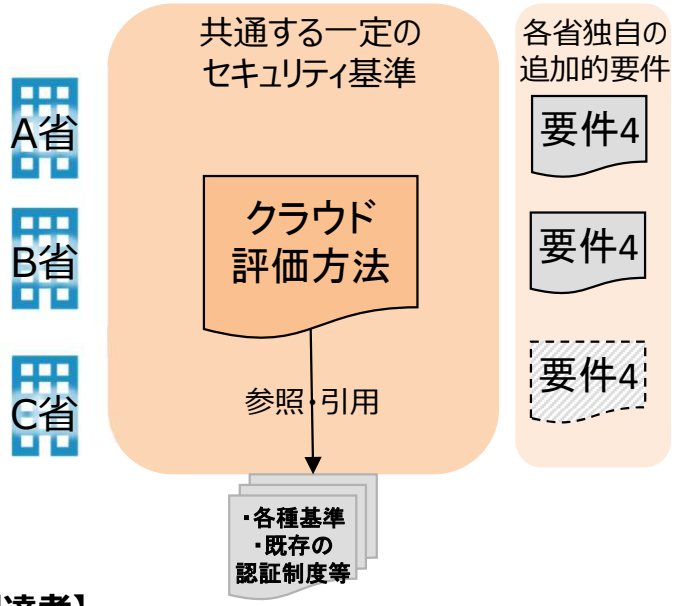
現状



【調達者】
- 各省が基準等を参照して最初から個別に要件を指定
- 調達担当によって、同じシステムでも要件の設け方にばらつきが生じ、必要なセキュリティ基準を必ずしも満たせていない可能性
- 各省共通の要件であっても、各々で確認しており非効率

【提案者】
- 同じ要件であっても、各省別個に審査を受ける必要があり非効率
- 政府調達におけるベースラインが不透明

目指すべき姿



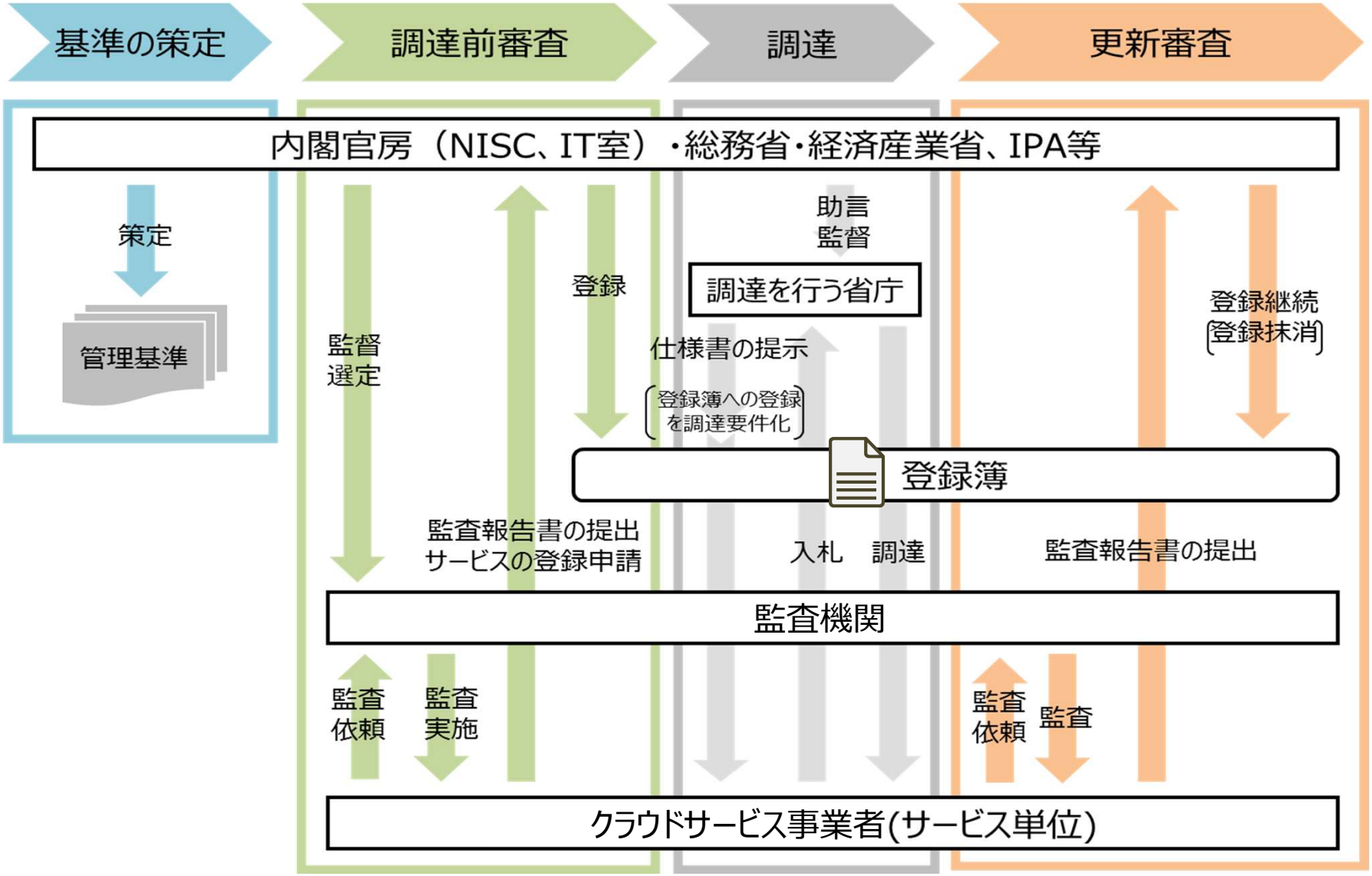
【調達者】
- 各省はクラウド評価に追加的な要件のみを指定
- 評価済みであれば、一定のセキュリティ基準を充足可能
- 各省共通の要件を相互利用可能

【提案者】
- 同じ要件について、一度の評価に共通化
- 政府調達におけるベースラインが透明化

※政府機関・情報システムは多岐にわたるため、共通するセキュリティ基準では不足している内容が存在しうる。その場合は各自共通水準に追加して評価することを想定。(上図の要件４)

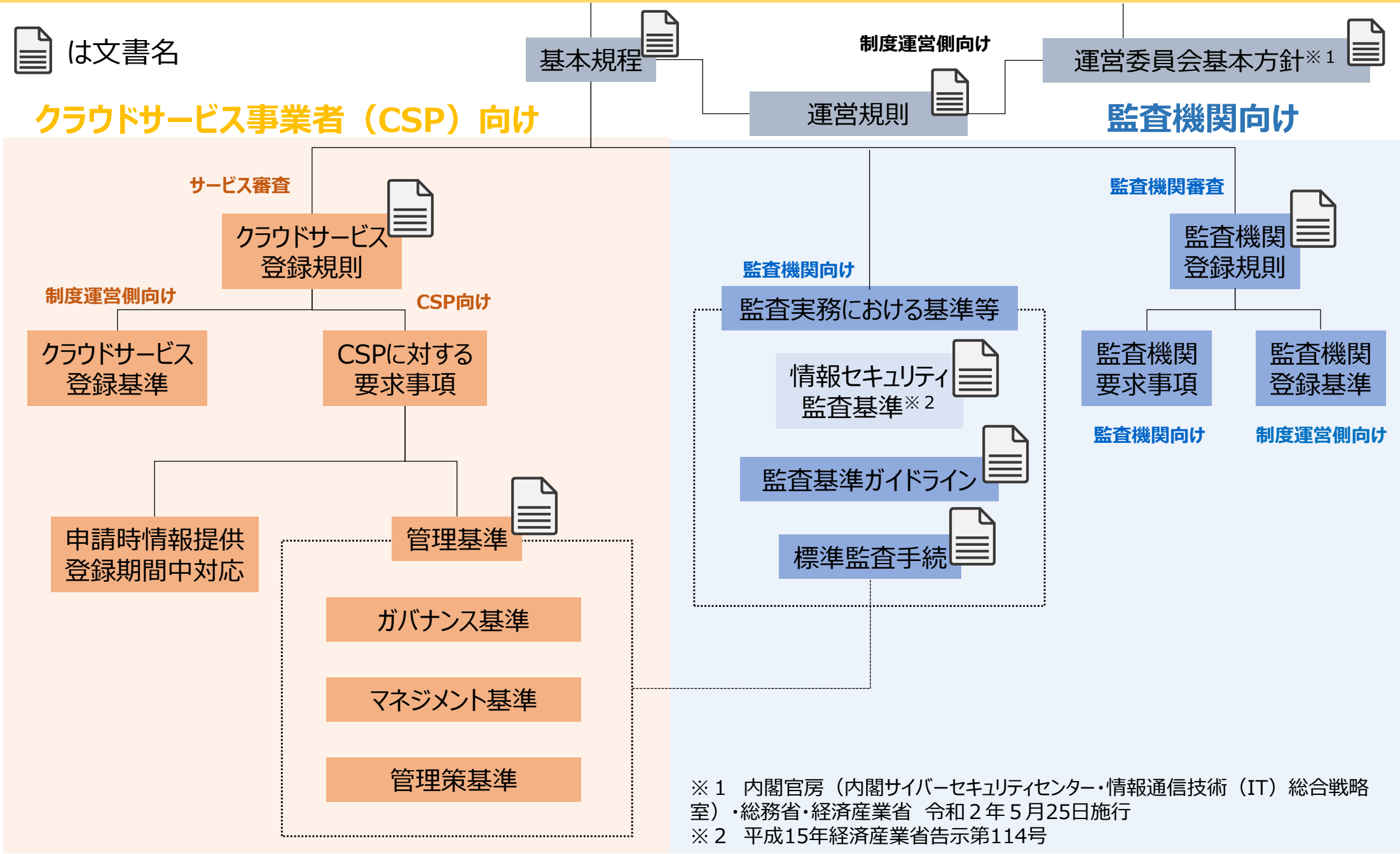
ISMAPの基本的な流れ

- 本制度の基本的な枠組みは、**国際標準等を踏まえて策定した基準**に基づき、各基準が適切に実施されているか**監査するプロセス**を経て、サービスを登録する制度
- 各政府機関は、**原則、安全性が評価され「登録簿」に掲載されたサービスから調達。**



ISMAPの全体像

「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」(サイバーセキュリティ戦略本部決定)



※1　内閣官房（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　令和２年５月25日施行

※2　平成15年経済産業省告示第114号

３．基本規程及び運営について

ISMAPの基本的な枠組み①

● ISMAPを構成する者とその責任範囲

（※）数字はISMAP基本規程の条項

ISMAP運営委員会 ※7.1	✓ 戦略本部決定に定められた制度の基本的な枠組みに沿うよう、制度の運用を行う責務 ✓ 円滑な制度運用のための柔軟な制度の見直しを行う責務 ✓ クラウドサービスの登録、監査機関の登録及び本制度に関する規程等の制定・改廃等について、その意思決定の最終的な責任を負う
制度所管省庁 ※7.2	✓ ISMAP運用支援機関が適正な業務を実施するよう適切に監督を行う責務 ✓ 円滑な制度運営が行われるよう、ISMAP運営委員会及び調達府省庁等との調整及び情報提供等を行う責務
クラウドサービス事業者 ※7.3	✓ 本制度の規程等において要求されている事項に対し、登録の申請において表明した内容を誠実に履行する責務 ✓ ISMAP運営委員会の求めに応じて、必要な協力を行う責務
監査機関 ※7.4	✓ 監査機関の登録に関して本制度で求められる規程等を遵守するとともに、監査基準等にしたがって、誠実に監査業務を行う責務
調達府省庁等 ※7.5	✓ 本制度の趣旨を理解した上で、自身の調達する情報システム全体のセキュリティ確保を行う責務

● その他の規定

✓ ISMAP運営委員会、制度所管省庁、ISMAP運用支援機関及びその委託を受けた者に対する秘密保持義務 ※9.1

✓ 本制度の運用に係る事務をISMAP運用支援機関（（独）情報処理推進機構（IPA））に委任 ※9.3

✓ クラウドサービスの登録、監査機関の登録に関する業務の実施に当たっては、サイバーセキュリティ対策推進会議、各府省情報化統括責任者（CIO）連絡会議において決定された本制度に求められる配慮事項に留意 ※9.5

４．CSPに対する要求事項について
（クラウドサービス登録規則・管理基準）

CSPに対する要求事項について①

- CSPに対しては、ISMAPクラウドサービス登録規則において、CSPの登録申請に際し、大きく分けて３種類の要求事項を課す。

CSPに対する要求事項

ISMAPクラウドサービス登録規則において直接規定

申請時の情報提供

情報提出先：ISMAP運営委員会

登録期間中の対応

情報提出先：ISMAP運営委員会

- 監査の対象とすることがそぐわない内容であるが、制度を実施・活用するために必要な内容
- 申請時に、①所定の情報の提供と、②登録期間中の対応を求める

ISMAPクラウドサービス登録規則において自身のセキュリティ対策について基本言明要件に沿った言明を行い、言明した事項について監査機関の監査を受けなければいけない旨を規定

管理基準

情報（証跡）提出先：監査機関

- 監査主体による監査の対象となる内容

CSPに対する要求事項について②

- 制度の信頼性確保、調達側での制度活用といった観点で、管理基準とは別の要求事項も定める。

登録申請にあたり、CSPに対し、①申請時の情報提供や②登録期間中の対応を求める。

＜申請時の情報提供＞

（※）数字はISMAPクラウドサービス登録規則の条項

- 申請者の資本関係及び役員等の情報　※3.4(1)
- クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、制度運営委員会及び当該省庁等がリスク評価を行うために必要な情報　※3.4(2)
- 契約に定める準拠法・裁判管轄に関する情報　※3.4(3)
- ペネトレーションテストや脆弱性診断等の第三者による検査の実施状況と受入に関する情報　※3.4(4)

＜登録期間中の対応＞

（CSP宣誓事項の例）

- 調達交渉時に、調達機関の求めに応じ、言明書の詳細、申請するクラウドサービス従事者のうち、利用者の情報又は利用環境に影響を及ぼす可能性のある者の所属、専門性、実績、国籍に関する情報を提出すること。国籍については、個々人に紐付かない形で該当する国名を提出すること。※3.5(1)
- 登録されているサービスについて、登録期間中に利用者に重大な影響を及ぼしうる情報セキュリティインシデントが発生した場合に、遅滞なくISMAP運営委員会に報告すること。※3.5(2)
- 登録されているサービスについて、登録期間中に重大な統制の変更及び当該変更につながりうる事象が生じた場合又はリストに掲載されている情報に変更が生じた場合に、遅滞なくISMAP運営委員会に届け出ること。※3.5(3)　等

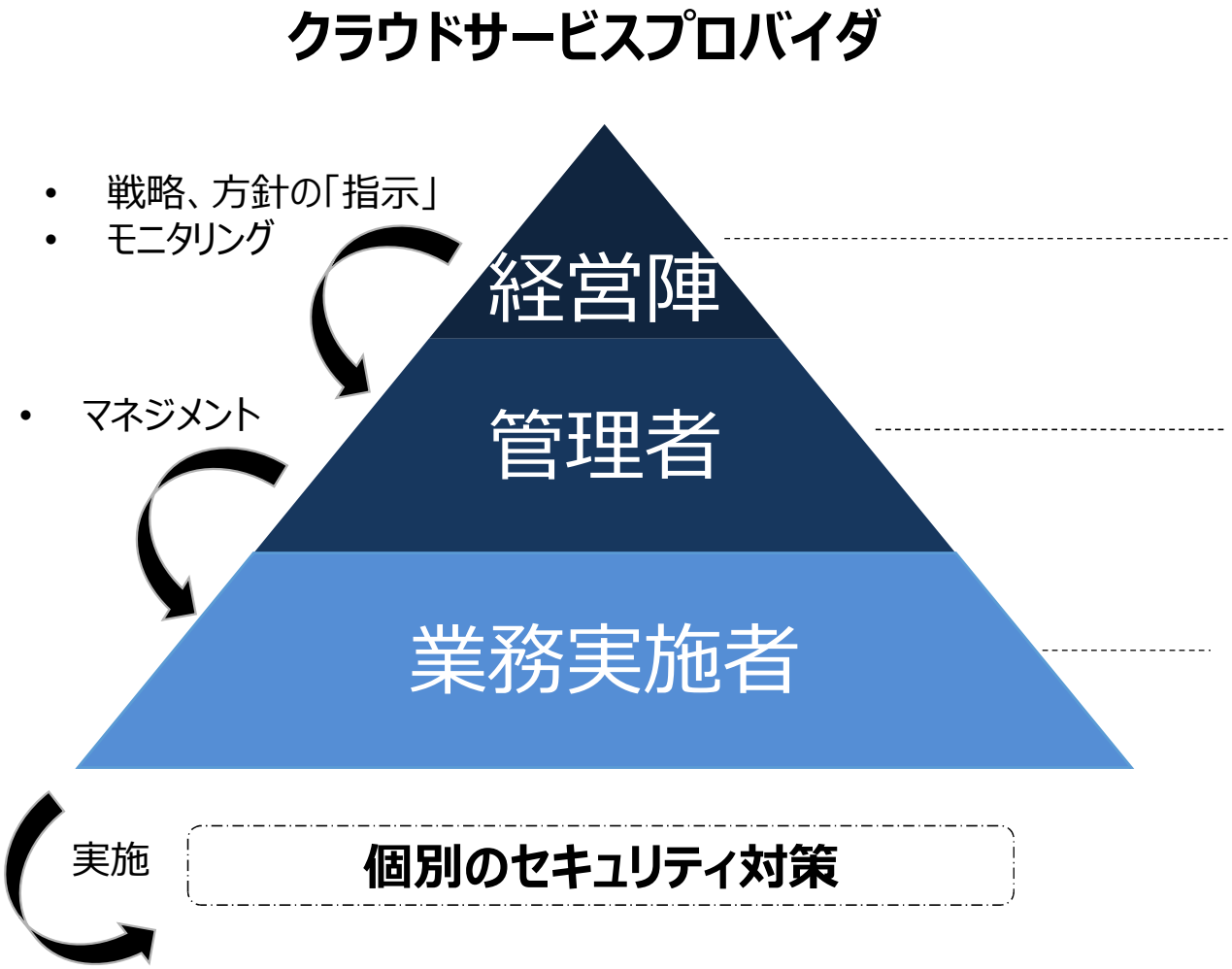
（CSP宣誓事項以外の例）

- 調達交渉時に、調達機関の求めに応じ、「IT調達に係る国の物品等又は役務調達方針及び調達手続に関する申合せ」の運用に協力すること　※3.6　等

ISMAP管理基準の構成①

■ ①クラウドサービスプロバイダの**「経営陣」が**管理者層に対して、セキュリティに関する**意思決定や指示等を継続的に実施**し、②これを受けたクラウドサービスの**「管理者」が的確にマネジメントを実施**し、③クラウドサービスの**「業務実施者」が実際にセキュリティ対策を実施**していることを確認する。

■ 上記①～③のそれぞれに対して基準を設け、確認するため、管理基準は**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種類から構成される。



①ガバナンス基準

例）
- ✓ 経営陣は、情報セキュリティの戦略及び方針を承認する。
  (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。
  (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。

②マネジメント基準

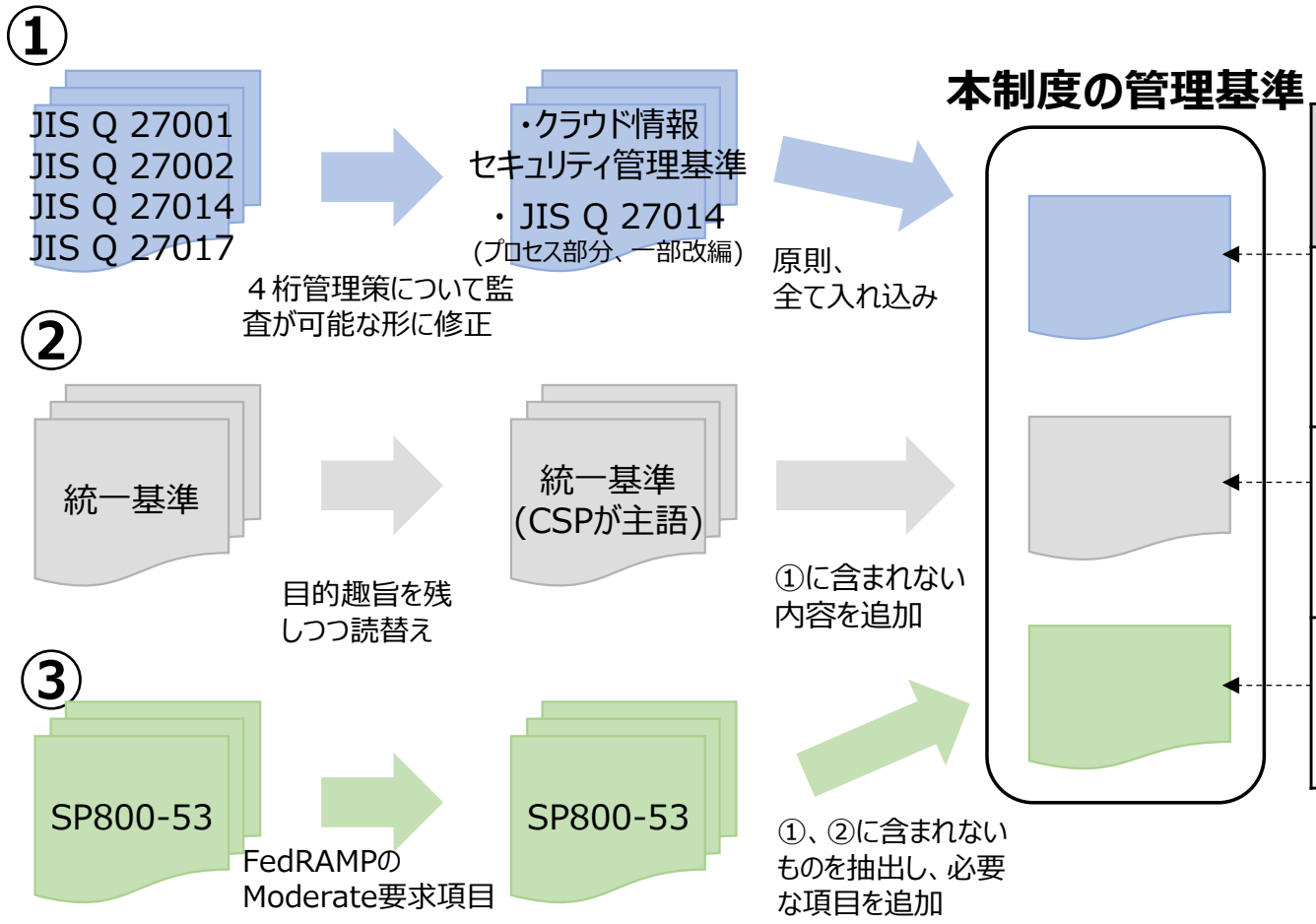
例）
- ✓ 情報セキュリティマネジメントの確立
- ✓ 情報セキュリティマネジメントの運用
- ✓ 情報セキュリティマネジメントの維持及び改善

③管理策基準

例）
- ✓ アクセス制御に対する業務上の要求事項
- ✓ 媒体の取扱い
- ✓ 暗号による管理策
- ✓ マルウェアからの保護
- ✓ ログ取得及び監視
- ✓ 冗長性

ISMAP管理基準の構成②

- **国際規格**のうち、情報セキュリティに関する**JIS Q(ISO/IEC) 27001、27002**と、クラウドサービスの情報セキュリティに関する**JIS Q(ISO/IEC) 27017を基礎**とする。
- **統一基準**の内容を、その**趣旨を残したままCSP向けに書き換え(主語をCSP、対象をCSとする)**、①に含まれない内容であり、かつCSPが実施しなければ政府において統一基準を満たすことが難しい内容を追加。
- **SP800-53の内容**から、インシデントレスポンスに関連する内容を中心に、**①、②に含まれない観点を追加**。



管理策数※１

管理策基準 〔3桁：121 4桁：1074〕	マネジメント基準 〔3桁：21 4桁：64〕	ガバナンス基準 〔4桁:18〕
全て入れ込み	全て入れ込み	ISO27014の内容をベースに再整理を実施
ISOの項目数で ・**6項目**追加 ・**3項目**追記※２	(定型管理策１に該当するため、原則ISOを採用)	(該当なし)
ISOの項目数で ・**22項目**追加 ・**29項目**追記	・**4項目**追記	(該当なし)

※１：項目数は、作業ファイル上の行数でのカウントであるため、実際の管理策数は多少増減する見込み
※２：情報の提供を求める項目については、管理基準とは別の要求事項として要求する項目も存在する。

管理基準のイメージ

- 管理基準は、**統制目標とされる3桁管理策（A.x.x.x）**と、それを達成するための手段となる**詳細管理策である4桁管理策（A.x.x.x.x）**で構成される。
- 原則、**３桁管理策を必須**、**4ケタ管理策は選択性**とし、一部の重要な管理策を必須とする。

３桁管理策：統制目標　※全て必須

管理策番号	管理策
8.1.2	目録の中で維持される資産は、管理する。
8.1.2.1	資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。
8.1.2.2	資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。
8.1.2.3	資産の管理責任者は、資産の目録を作成する仕組みを整備する。
8.1.2.4	資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。
8.1.2.5	資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。
8.1.2.6	資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。

４桁管理策：手段　※原則選択性。全て必須に規定してしまうと、動的な変化への対応が困難。

５．監査機関を対象とした基準等
（監査機関登録規則・監査ガイドライン・標準監査手続）

監査機関に対する要求事項

- 監査機関に対する要求事項として、技術的/能力的な観点および信頼性の観点から、**組織として以下の事項を満たす体制を構築可能であること**をISMAP監査機関登録規則において要求する。
- **ISMAP運営委員会が審査**を実施し、その結果、登録が認められた監査機関は**ISMAP監査機関リストに登録**され、**２年ごとに登録更新**を行う。

（※）数字はISMAP監査機関登録規則の条項

＜要求事項の概要＞

- **登録対象**：わが国において情報セキュリティ監査を業務として行っている法人 ※3.1
- **準拠規程等**：本制度に関してISMAP運営委員会が定める規程等に準拠すること ※3.2
- **法人登録**：国税庁から法人番号の登録を受けていること ※3.3
- **業務品質**：「情報セキュリティサービス基準適合サービスリスト」に「情報セキュリティ監査サービス」として登録を受けていること ※3.4
- **問題事案対応**：倫理審査機能を有する組織への所属、問題事案発生時の調査への協力 ※3.5
- **業務執行責任者の要件**：資格要件、実務経験、国籍等を要求（詳細は次頁） ※3.6
- **業務実施責任者の要件**：資格要件、研修受講、国籍等を要求（詳細は次頁） ※3.7
- **業務チームの要件**：業務執行責任者、業務執行責任者を含む最低３名以上で構成
  メンバーは原則日本人だが、やむをえない場合は、業務依頼者との契約締結前にISMAP運用支援機関に問い合わせを行う ※3.8

ISMAP情報セキュリティ監査ガイドラインについて①

- 本制度の監査業務との特質と業務依頼者、業務実施者、ISMAP運営委員会の責任について規定。

＜本制度における監査業務の特質＞ ※1.2　　（※）数字はISMAP情報セキュリティ監査ガイドラインの条項

- 本制度の監査業務において、業務実施者の報告は、手続実施結果を事実に即して報告するのみにとどまり、手続実施結果から導かれる結論の報告も、保証も提供しない。
- 本制度における監査業務は、結論の基礎となる十分かつ適切な証拠を入手することを目的とはしておらず、保証業務とはその性質を異にする。
- さらに、業務実施者は、本制度における監査業務において、重要性の概念の適用やリスク評価に基づく手続の決定は行わず、また、業務実施者の報告に基づき実施結果報告書の利用者が不適切な結論を導くリスクの評価は行わず、実施した手続や入手した証拠の十分性についても評価しない。

＜本制度における監査業務に関する業務依頼者、業務実施者、ISMAP運営委員会の責任＞ ※1.4

- 業務依頼者（＝クラウドサービス事業者）は、言明の対象となるクラウドサービス（＝ISMAPクラウドサービスリストへの登録申請を行うクラウドサービス）に関して、当該サービスの内容及びセキュリティリスク分析の結果を踏まえて、管理基準に準拠して統制目標及び詳細管理策を選択して必要な統制を整備するとともに、対象期間にわたりそれらを有効に運用していることを言明する責任を有している。
- 業務実施者は、監査基準等に準拠して本制度における監査業務を実施し、その実施結果を業務依頼者に報告する責任を負う。業務実施者は、標準監査手続に準拠して業務依頼者の言明する統制に対して手続を実施する責任を負うが、その結果として関連する統制目標の有効性や手続実施結果から導かれる結論の報告を行う責任は負わない。
- ISMAP運営委員会は、実施結果報告書を含むサービス登録に必要となる申請書類を業務依頼者から受領し、ISMAPクラウドサービス登録規則に基づいてISMAPクラウドサービスリストへのクラウドサービスの登録審査を行う責任を負う。

ISMAP情報セキュリティ監査ガイドラインについて②

- 監査機関は、情報セキュリティ監査基準に加えて、監査ガイドラインを遵守しなければならない。

＜独立性、客観性と職業倫理＞ ※第2章

（※）数字はISMAP情報セキュリティ監査ガイドラインの条項

- 業務実施者は、情報セキュリティ監査基準に定める独立性、客観性及び職業倫理に関する要求事項を遵守。
- 監査機関は、外観上の独立性に関して以下の事項を遵守。
  - 本制度における監査業務の対象となるクラウドサービス事業者と資本関係を有してはならない
  - 本制度における監査業務の対象となるクラウドサービス事業者との間に、本制度における監査業務と利益相反が生じる関係（※）を有していない

（※）利益相反が生じている事例として、例えば、監査機関が、本制度における監査業務の対象となるクラウドサービスに関して、当該クラウドサービスの開発・保守・運用・設計・導入業務を提供している場合等が想定される。

＜品質管理＞ ※第3章

- 監査機関は、品質管理者の割当、品質管理マニュアルの整備、品質の維持・向上に関する手続等の導入などの品質管理要件に準拠し、実施する本制度における監査業務の全体的な品質確保に責任を負う。

＜その他（主なもの）＞

- 業務執行責任者は、監査機関登録基準における要求事項に定める業務チームに関する要件を満たすよう業務チームを編成し、当該業務チームが監査基準等に準拠して業務を遂行するよう、監督しなければならない。※4.2
- 業務実施者は、標準監査手続に準拠して自ら手続を実施する。そのため、他の認証・監査制度や内部監査等の実施結果あるいはその報告書をそのまま利用することは原則認められない。ただし、業務実施者が標準監査手続を実施する際に適切とみなす場合には、他の認証・監査制度や内部監査等において収集された証拠を利用することは可能である。※4.5

標準監査手続について

■ 監査機関に対する要求事項として、情報セキュリティ監査基準および監査ガイドラインと並列に位置づける。

■ 実務上の要求事項であるため、登録される監査機関のみに限定して配布を予定。

＜標準監査手続の構成イメージ＞

- 4桁管理策単位で想定される監査対象（規程・マニュアル、設計書・仕様書、申請書・承認記録・ログ等、パラメータ等、設備・建物等）を特定、定型化した手続を当てはめて作成
- 原則、監査機関リストに登録された監査機関のみに提供するものとする

第１章　総則
- 趣旨
- 標準監査手続の実施のガイダンス※

第２章　標準監査手続
- 標準監査手続（ガバナンス基準部分、マネジメント基準部分、管理策基準部分）

※）各監査技法の定義や手続を実施する際のルール（「質問」のみで手続を終了することは不可等）を定めるもの。

６．最後に

ISMAP関連情報（IPAホームページ）

IPAホームページ内にISMAP専用ページ有り

[URL] https://www.ipa.go.jp/security/ismap/index.html

・ISMAPの概要や各種規程、基準群はこちらから入手可能

・その他、FAQでよくある質問が整理されている他、お問い合わせフォームも有り