経済産業省

資料3

サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会　中間とりまとめ（案）

2026年6月1日

経済産業省

商務情報政策局

１．制度の目的と位置づけ

制度の目的

【検討の背景】

- 近年、サイバーセキュリティ・サービス提供事業者の体制・措置等に起因して、当該サービスの顧客（サービス利用事業者）に被害が生じたとされる事案が国内外でみられている。また、欧米諸国では、特定のサイバーセキュリティ・サービス提供事業者について、サイバー攻撃への関与等の懸念があるとして、消費者に対する警告や当該事業者の活動禁止措置等を講じるケースもみられる。
- デジタル化の進展や地政学リスクに伴うサイバーリスクの増加等を踏まえ、**今後サイバーセキュリティ・サービス**（とりわけ、顧客の機微情報やシステムへのアクセスを許容する形態のもの）**に対するニーズが増加することが見込まれる**中、**サイバーセキュリティ・サービス提供事業者の体制・措置等に起因する事案等が生じている**ことに鑑みると、**サービス提供事業者の「適切な運営体制」の一層の強化（厳格な社内体制の整備等）が求められる**のではないか。
- 現行の「**情報セキュリティサービス審査登録制度**」では、サービス提供事業者の「適切な運営体制」について、**反社会的勢力等への関与がないことのみが要件として求められている**。同制度は、**専門知識をもたないサービス利用者向けに、最低限の基準に適合するサービス提供事業者を審査・登録する仕組み**であることから、当該制度において、**幅広いサービス提供事業者に対して「適切な運営体制」に係る追加の高度な要件を付加することは困難。**
- 以上のことから、現行の登録制度に新たな要件を付加するのではなく、**現行の登録制度の二階部分として上乗せする形**で、**国の行政機関等が運営することを想定**して、**高度な適切な運営体制を有するサイバーセキュリティ・サービス事業者を確認する「新たな制度」の整備に向けて検討**を行った。

【制度の目的（目指す効果）】

- 本制度の認定を通じて、サイバーセキュリティ・サービス事業者の体制・措置等に起因する事案の防止を図る。

（参考）サイバーセキュリティ・サービス提供事業者の体制・措置等に起因する事案の例

事業者	発生時期	事案の概要
Hacker One	2022年7月	同社の元従業員が、顧客の脆弱性情報に不適切にアクセスし、当該顧客から報奨金を得る目的で当該脆弱性情報を外部に漏えい（当該顧客に再送信）。 同社は、ロギングの改善、採用審査の強化等の改善策を公表。
Trend Micro	2019年11月	技術サポートを担当していた元従業員が最大12万人分の顧客情報を盗み出して第三者に売却。詐欺の電話に悪用されていることが発覚。 同社は、再発防止に向け、管理体制の一層の強化等を行う旨を公表。
Bitdefender	2015年7月	同社に対するセキュリティ侵害が発生し、顧客情報（.govドメインを含むメールアドレス、ユーザー名、パスワード等）が漏えい。攻撃者は、当該漏えいした情報が完全に暗号化されていなかったと主張。暗号化されていないデータの漏えいとの観点から、同社のセキュリティ姿勢を懸念する報道も。

出典：各社発表資料及び各種報道情報

（参考）サイバーセキュリティ・サービス事業者の信頼性強化に向けた政策対応に対する要請

第９回産業サイバーセキュリティ研究会（令和７年５月23日）でいただいた御意見

- 「サイバーセキュリティ産業振興戦略」の実現に向けて、**製品・サービスのセキュリティや信頼性を確保するための制度構築についてコメントする**。米国では、国家防衛やインフラ防御の際に民間事業者に対してFOCI（Foreign Ownership, Control, or Influence）規制がかけられ、サイバー空間も対象となる。IPAにも「情報セキュリティサービス審査登録制度」があるが、米国の対応に比べると弱い。**脆弱性診断サービスのようなサービスが普及するよう実効性を担保いただきたい**。

新しい資本主義のグランドデザイン及び実行計画2025年改訂版（令和７年６月13日閣議決定）（P44-45）

Ⅲ．投資立国の実現　３．ＧＸ・ＤＸの着実な推進（２）ＤＸ　④サイバーセキュリティ

IoT製品に関する「セキュリティ要件適合評価及びラベリング制度」を早期に政府機関等における調達の選定基準に含める。模擬プラントの整備、大規模演習環境の構築を通じて、高度化するサイバー攻撃に対応できる人材の育成、「サイバーセキュリティお助け隊サービス」の普及や見直しを通じた中小企業への支援を進める。

また、政府機関等におけるスタートアップ製品・サービスの積極的な活用や**信頼性の高いサービス提供事業者の認定制度の整備**、研究開発プロジェクトの拡充に向けた検討等を着実に実施する。あわせて、未知の脅威情報や脆弱（ぜいじゃく）性を検知する国産ソフトを開発し、政府端末等へ順次導入を図るとともに、情報収集やＡＩ活用による高度分析の結果の民間活用により、国内ベンダによる製品化を加速させる。

制度の位置づけ

- 本制度の目的は、「技術・品質」を確認する情報セキュリティサービス審査登録制度（以下「現行制度」という。）に加え、顧客の機微情報やシステムへのアクセスを許容するなど、顧客にとってリスクの高い形態のサービスを提供する**「事業者の適切な運営体制」を確認**することにある。また、新たな制度の普及を目指すべき初期段階においては、**既に浸透している現行制度と連続した制度設計が有効**である。したがって、**現行制度の対象サービス区分の全部を対象とする。**
- 本制度の対象事業者は、現行制度に登録しているサイバーセキュリティ・サービス事業者とする。

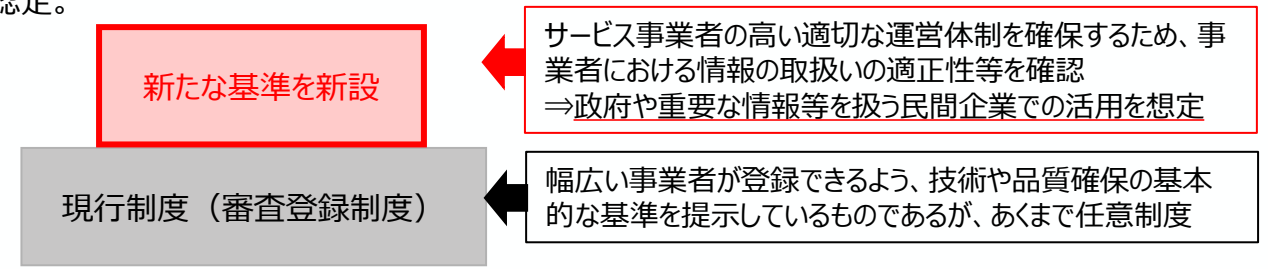
現行制度のサイバーセキュリティ・サービスの種類

（１）情報セキュリティ監査サービス
（２）脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス
（３）デジタルフォレンジックサービス
（４）セキュリティ監視・運用サービス
（５）機器検証サービス

＜制度（イメージ）＞

○サイバーセキュリティ・サービス認定制度の全体像

新たな制度では、リストに掲載された企業から申請を受け、適切な運営体制を確認、認定。



（参考）情報セキュリティサービス基準におけるサービス区分

サービス分野	定義
(1)情報セキュリティ監査サービス	**情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を**、国際的にも整合性のとれた基準に従って**検証又は評価し、もって保証・助言を行うサービス。**
(2)脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス	**1)脆弱性診断サービス** **システムやソフトウェア等の脆弱性**に関し、**評価・助言**を行うサービス。 • Web アプリケーション脆弱性診断 • プラットフォーム脆弱性診断 • スマートフォン／タブレット端末アプリケーション脆弱性診断
	2)ペネトレーションテスト(侵入試験)サービス **脆弱性診断のサービスの定義を満たすサービスのうち、攻撃者が実際に侵入等を行うために用いる手法と同様の手法**により、**アプリケーション、システム、又はネットワークのセキュリティ機能を回避して攻撃の目的を達成できるかの観点から試験**を行い、**その結果をもとに助言**を行うサービス。
(3)機器検証サービス	**IoT機器をはじめとするネットワーク通信機能を持つ機器及びその機器に対してネットワークを通じて操作・管理・データ処理等を行うアプリケーションから構成されるシステム**（IoT システム）に対して行う**脆弱性等を診断するサービス。** • 機器検証 • 機器検証及び Web アプリケーション脆弱性診断 • 機器検証及びプラットフォーム脆弱性診断
(4)デジタルフォレンジックサービス	システムやソフトウェア等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等や、それに伴う法的紛争・訴訟に際し、**電磁的記録の証拠保全、調査及び分析を行うとともに、電磁的記録の改ざん及び毀損等についての分析及び情報収集等を行う一連の科学的調査手法及び技術（デジタルフォレンジック）**についてのサービス。 • 機器や記録デバイスを対象とするデジタルフォレンジックによる調査 • デジタルフォレンジックによる調査に付帯する訴訟支援及び電子証拠開示対応（ｅディスカバリ）等のサービス
(5)セキュリティ監視・運用サービス	システムやソフトウェア等についての**情報セキュリティを確保するための監視サービス及びシステムやソフトウェア等の適切な運用**するサービス。 • マネージドセキュリティサービス（セキュリティインシデント又はその予兆の検知、防御を目的とするものをいう。） • セキュリティ監視サービス（セキュリティ製品が出力するログの分析、通知、レポート提供を継続的に提供するものをいう。） • マネージドセキュリティサービスやセキュリティ監視サービスを包含する複合的なサービス

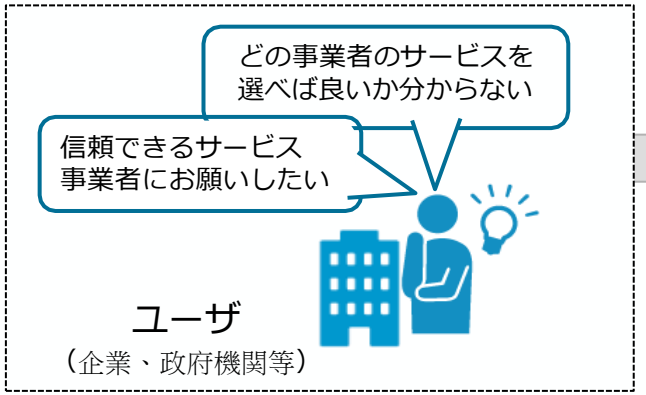
（参考）対象サービスで取り扱うデータ・リスク

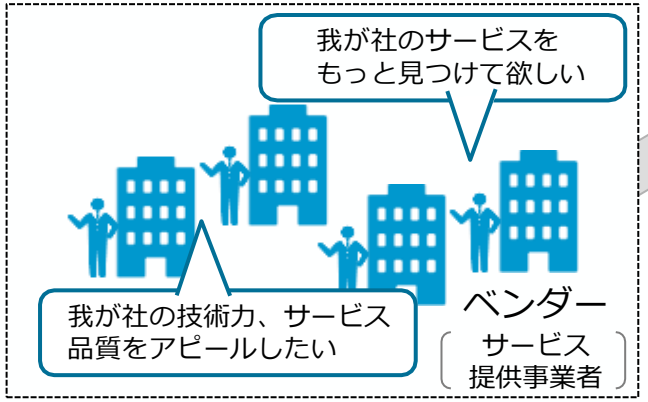
サービス分野	取り扱うデータ	想定リスク
(1)情報セキュリティ監査サービス	リスクアセスメントに基づく適切なコントロールの整備状況・運用状況に関するデータ	**リスク：中～高** • 組織的な脆弱性（規定・ルール上の不備、逸脱、不十分なリスク認識等）が悪用されるリスク
(2)脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス	●脆弱性診断サービス 稼働しているシステムやソフトウェア等の脆弱性情報 ※Web アプリケーション、プラットフォーム、スマートフォン／タブレット端末アプリケーションへの診断結果	**リスク：高** • 検査結果（システム等に潜在する脆弱性情報）の転売リスク、脆弱性が悪用され侵入されるリスク
	●ペネトレーションテスト（侵入試験）サービス 外部からの侵入方法や侵入経路等の情報 ※アプリケーション、システム、又はネットワークのセキュリティ機能を回避し攻撃目的を達成可能かの試験結果	**リスク：高・最高** • 侵入方法や侵入経路に係わる情報の転売リスク、脆弱性が悪用され侵入されるリスク
(3)デジタルフォレンジックサービス	指定されたシステムやPCに格納されていたデータ（重要データや個人情報、技術情報等）、ネットワーク機器のログ情報等	**リスク：高** • システムやPCに格納されていた重要データや個人情報等の窃取リスク • 調査対象機器への不正プログラムの導入リスク
(4)セキュリティ監視・運用サービス	使用されているセキュリティ機器情報、セキュリティ機器での攻撃の検知状況や検知能力に係わる情報 ※セキュリティインシデント又はその予兆の検知・防御に係わる情報	**リスク：中～高** • 攻撃の予兆や攻撃検知のアラートを無視したり、アラートが発生しにくい設定に変更したりし、初動対応が遅れるリスク（対応遅れによる、侵害範囲の拡大） • 監視の過程で入手した脆弱性情報の漏えいリスク
(5)機器検証サービス	IoT機器を含むネットワーク通信機器及びIoT システムの脆弱性情報 ※機器検証、および機器のWebアプリケーションやプラットフォームへの診断結果	**リスク：中～高** • IoT機器類の脆弱性情報の転売リスク、悪用され侵入されるリスク

（参考）情報セキュリティサービス審査登録制度

- 経済産業省は、**情報セキュリティサービス業の普及を促進し、国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的**に、以下の基準を策定。
  - ① **情報セキュリティサービスが満たすべき最低限の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするための基準**（「情報セキュリティサービス基準」）（2018年2月、 2023年3月第3版改訂）
  - ② **同基準への適合を審査する機関**（以下、審査登録機関）**が満たさなければならない基準**（「情報セキュリティサービスに関する審査登録機関基準」）（2018年2月、 2022年3月第2版改訂）
- これらの基準を踏まえ、登録申請のあったサービスが情報セキュリティサービス基準に適合するかを**審査登録機関が審査の上、「情報セキュリティサービス基準適合サービスリスト」に掲載。６区分のサービス**を対象として**年4回**の審査を行っており、**合計398サービスが登録**（2026年3月現在）されている。

○情報セキュリティサービスにおける課題





選定時に活用

審査を受けてリストに掲載

情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと 認められたサービスをリストにして公開

基準を満たした398サービスを掲載（2026年3月現在）

- **情報セキュリティ監査（84サービス）**
- **脆弱性診断（188サービス）**
  - **うちペネトレーションテスト(51サービス)**
- **デジタルフォレンジック（43サービス）**
- **セキュリティ監視・運用（51サービス）**
- **機器検証 （32サービス）**

情報セキュリティサービス基準（経済産業省）

対象のサービス(5サービス、1オプション)に関して技術要件・品質管理要件を定めた基準を公開

（出典）情報セキュリティサービス基準適合サービスリスト　https://www.ipa.go.jp/security/service_list.html

○本制度を通じて目指す社会

専門的知識を持たない ユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

２．構築する認定制度

制度の範囲について

- サービスの認定を行う上では、**サービスに係る技術・品質と事業者の適切な運営体制の両方を確認することが重要。**
- 今回整備を検討する**「新たな制度」の目的は、**「技術・品質」を確認する情報セキュリティサービス審査登録制度（以下「現行制度」という。）に加え、顧客の機微情報やシステムへのアクセスを許容するなど、顧客にとってリスクの高い形態のサービスを提供する**「事業者の適切な運営体制」を確認すること**にある。また、新たな制度の普及を目指すべき初期段階においては、**既に浸透している現行制度と連続した制度設計が有効**である。したがって、**当面の間、新しい制度の対象サービス区分は、現行制度と同一とする。**

※そのうえで、現行制度の対象サービス拡大の必要性については、技術・品質の基準など含めてゼロベースでの議論が必要なため将来的に現行制度の検討会等の別の場で議論を行うこととしたい。
※現行制度では、サービス提供に関連するツールやシステムのみを提供するようなサービス（例：脆弱性管理用のクラウドサービス）にも登録が付与されているケースが存在する。しかし、本来の制度趣旨（専門知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる）に反するため、現行制度で登録されたサービスであったとしても、新たな制度では当該サービスは対象外とする。（現行制度も運用面の見直しを行う予定）

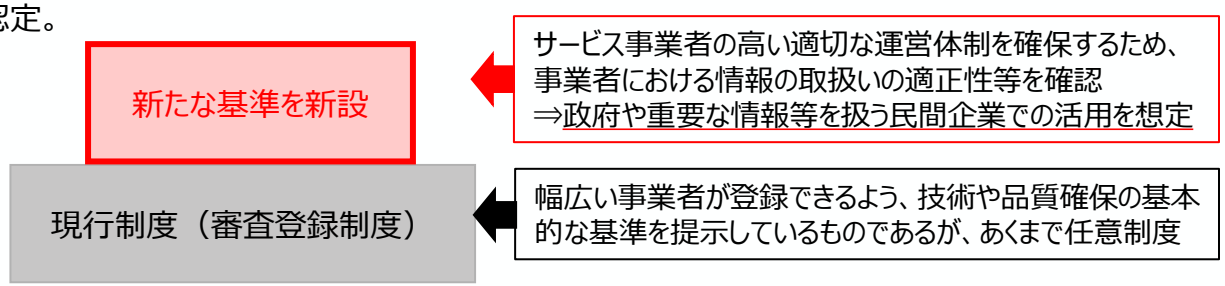
現行制度のサイバーセキュリティ・サービスの種類

（１）情報セキュリティ監査サービス
（２）脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス
（３）デジタルフォレンジックサービス
（４）セキュリティ監視・運用サービス
（５）機器検証サービス

＜制度（イメージ）＞

○サイバーセキュリティ・サービス認定制度の全体像

新たな制度では、リストに掲載された企業から申請を受け、適切な運営体制を確認、認定。



想定するリスクと認定企業に求められる対応

- 組織・人・ツール・データなど各レイヤーごとにリスクが存在。これらに対応する形で、組織規程の整備やデータのアクセス権限管理等といった組織的な対策が重要。

	組織	人	ツール	データ
リスク	• ガバナンスの不備等による情報流出等 • 外国の法的環境等による組織への影響	• 従業員による情報流出等 • 外国の法的環境等による授業員への影響	• ツールに入力したデータの流出等	• データ保管先から流出等
企業に求める防御策	• 各種規程の整備や人的教育等 • 適切な経営体制等	• 採用時又はセキュリティ関連業務の従事開始時における従事者の確認・管理等	• 安全なツールの選定・調達のための基準の策定、シャドーITを防止するための施策（標準外ソフトウェアのインストール防止等） • 利用するツールの由来、外部通信の有無の確認、ログ取得可否などの明確化	• 適切なデータ保管先の選定・調達基準の策定、シャドーITを防止するための施策（CASBの導入等独自のクラウド利用の禁止等） • 機微情報の取扱い規定の整備 • データへのアクセス管理（アクセス制限またはアクセス履歴の管理）

制度における審査項目

- 本制度における審査においては、組織・人・ツール・データなどのリスクを踏まえ、以下の項目を確認する。
- なお、一部対策の充足性については、**ISMS認証とサプライチェーン強化に向けたセキュリティ対策評価制度（以下、「SCS評価制度」という）★４の取得を通じて確認する。**

項目（案）	組織（企業）単位	サービス部門単位
会社の経営体制・資本関係等	当該企業の資本関係、所在地、代表者・役員の情報等	サイバーセキュリティ・サービスの責任者等
従業員の管理方法規程等	従業員の管理規程 ※ISMSを活用	
情報に関する管理体制	情報セキュリティ基本方針、情報セキュリティ体制（責任者等の役割任命等） ※ISMSを活用	サービスに係る情報セキュリティ体制（責任者等の役割任命等）、重要情報（業務上取得した情報）の保管先や格付け区分と取扱い可能な役職員の範囲の策定、情報システムにおける利用者・管理者のアクセス管理・権限分散規程、物理的セキュリティ上の担保、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・追跡機能の整備 ※ISMSを活用
使用ツール・データ保管先	ツールの選定・調達基準、シャドーITを防止するための施策（標準外ソフトウェアのインストール防止、CASBの導入等による独自のクラウド利用の禁止等） ※ISMSを活用	使用ツールの関連情報（名称・メーカー・データ保管先・動作ログの取得有無・外部通信の有無等）、セキュリティ・サービスで利用したデータ保管先の詳細（データ保管先・アクセスログの取得有無等） ※より詳細な審査観点等は令和8年度中に検討
自社のサイバーセキュリティ対策	サプライチェーン強化に向けたセキュリティ対策評価制度の★４以上の取得	※サプライチェーン強化に向けたセキュリティ対策評価制度の★4以上の取得を要件とするにあたり、当該サービス部門が取得範囲に含まれることを確認

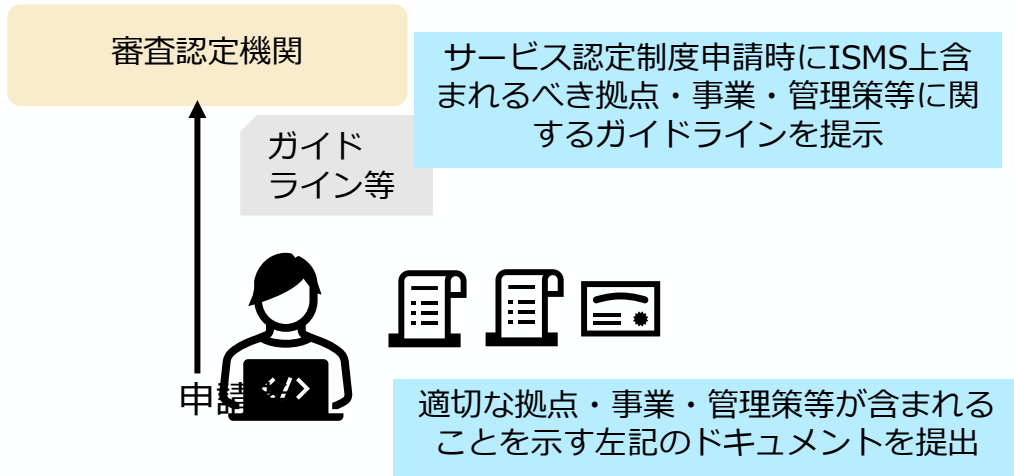
審査におけるISMSの活用

- 「情報に関する管理体制」等に関する審査項目については、ISMSとの重複が多く見られる。このため、本制度の認定に際し、**ISMS認証の取得を要件とし、取得を示す関連文書の提出を要求する**スキームとする。
- 一方、ISMSはその対象範囲（部門）および管理策等について、申請者の判断で一定程度幅を持たすことが可能であるところ、**当該制度において対象とすべき部門や審査項目が必ずしも全てのISMS認証において含まれない可能性**も考えられる。
- 従って、申請者には**「適用範囲記述書」「適用宣言書」「ISMS認証登録証」の3書類の提出を要求**し、**事務局は「認定対象となるサービスを提供する部門が含まれること」及び「対象とする審査項目に関連する管理策が適用対象となっていること」の二点を確認**する。

提出対象ドキュメント（仮）

名称	概要
適用範囲定義書	• ISMSが適用される事業、組織、場所、資産等の境界を示したもの
適用宣言書	• ISMSの管理策のうち、自社が適用するもの（しないもの）を宣言するもの
ISMS認証登録証	• 認証の取得を示すもの

スキーム（仮）



他制度との関係について

- **ISMSはリスクベースアプローチ**であり、リスクアセスメント結果等に応じて**各事業者が実装する対策水準は異なり得る**。また、**ISMS認証は未対策の箇所があったとしても、実施計画の提出で取得可能**。そのため、ISMS認証の取得とは別途、**共通に満たすべき最低限のサイバーセキュリティ対策水準を担保するために、SCS評価制度★4の取得も求める**こととする。
- Pマークについては、セキュリティ・サービス事業で個人情報を扱う機会は限定的であるため、認定要件としないものの、仮に顧客から求められた場合や個人情報等を扱う機会が多い場合は、取得を推奨する。

			SCS評価制度	ISMS適合性評価制度	プライバシーマーク(Pマーク)制度
基本情報	認証基準等		• ★3・★4 要求事項・評価基準	• ISO/IEC 27001 • JIS Q 27001	• JIS Q 15001
	目的		• サプライチェーン全体でのセキュリティリスク(情報漏えい、事業の停止等)の低減 • 様々な取引先から様々な要求事項を求められる状況下における基準統一による企業の負担軽減	• 組織が保有する情報資産の「機密性」「完全性」「可用性」を確保し、サイバー攻撃や内部不正、事故などのリスクから情報資産を保護すること	• 消費者の目に見えるプライバシーマークで示すことによって、個人情報の保護に関する消費者の意識の向上 • 適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与える
	保護対象		• 事業者のIT基盤	• 適用範囲内の情報資産	• 事業者全体の個人情報
	主なターゲット		• IT・情報通信関連の企業のみならず、製造業等に係る物品・役務のサプライヤー企業も含む。	• 特段の限定なし (ただし、取得企業はIT・情報通信関連が多くを占める。)	• 顧客の個人情報を取り扱う企業(B to C 企業)
	取得範囲		• 原則として法人単位 (評価機関等の確認を経て事業部、グループ単位等での取得も可)	• 法人単位、事業所単位、部門単位、事業単位など、柔軟に決定可能	• 原則として法人単位 (医療法人・学校法人に限り、例外有)
要求事項・管理策	考え方		• レベルごと達成すべき具体的なセキュリティ対策を要求事項・評価基準として規定 (ベースラインアプローチ)	• 附属書Aの管理策(組織的・人的・物理的・技術的)について、各組織でリスクアセスメントを実施の上決定 (リスクベースアプローチ)	• 個人情報保護の観点から、 - 個人情報に関する規程、手順などを策定 - リスク判断の上、セキュリティ対策(安全管理措置)を実施
	分類	セキュリティ 組織	• ポリシー策定、役割・責任の決定、取引先とのNDA　等	• ポリシー策定、役割・責任の決定、供給者管理　等	• 個人情報安全管理措置を実施 ※附属書D(ISO/IEC 27001附属書Aとほぼ同内容)等を参照し、リスクに応じて必要なセキュリティ対策を選択する
		セキュリティ 人	• 従業員の守秘義務、セキュリティ教育・訓練　等	• 雇用条件、セキュリティ教育・訓練　等	
		セキュリティ 物理	• サーバ管理、入退室管理　等	• 機器管理、職場管理　等	
		セキュリティ 技術	• 多要素認証、マルウェア対策ソフト、IDS/IPS　等	• アクセス制御、機器・ネットワーク保護　等	
		個人情報保護	–	–	• 個人情報保護指針の策定、個人情報保護管理者等の決定、委託先監督、個人情報の利用、開示等の手続　など

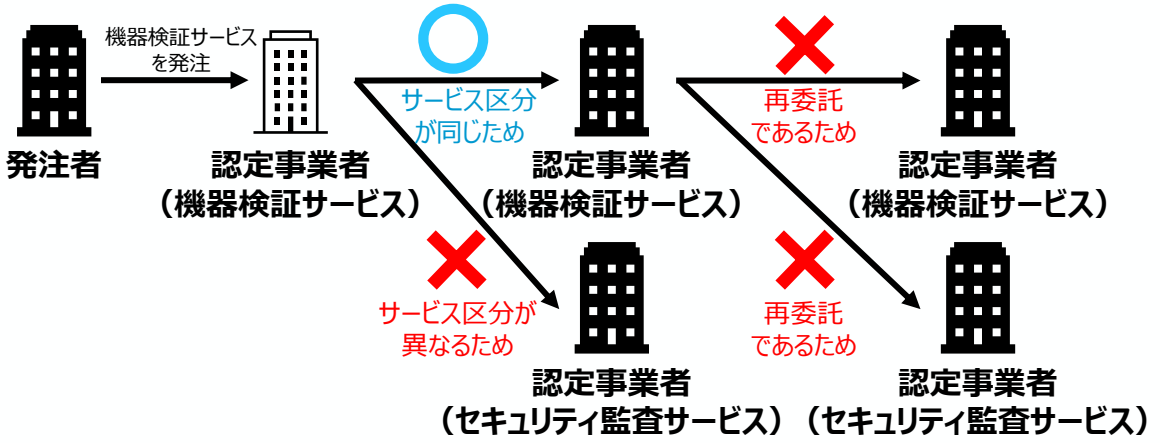
委託の制限について

- 認定事業者が自社のサービス提供に直接的に関する業務を他社に委託することについては、**いずれのサービスにおいても非常に機微なデータを取り扱うことから、一定の制限が必要**である。特に、サービス提供業務の完成責任を他社に負わせる**請負契約については、審査登録制度の要件の一つである品質管理の範囲外でサービス提供が実施されることになるため、本来ならば審査登録制度においても望ましくない**行為と定義づけるべき行為である所、**本制度においては原則、禁止する**。
  - なお、当然のことながら**自社のサービス提供に直接的に関する業務以外（システム開発等）において認定事業者が請負契約を締結することは妨げない。**
- それ以外の委託形態については、現状、**業務負荷が突発的に発生する場合等における業務委託が必要な状況も発生**していることから、以下の例外規定を設ける。
  - 別途同サービスカテゴリにおいて**本制度の認定を取得済みの事業者への委任（準委任）**
  - 認定事業者が**当該個人の信頼性評価（詳細は別途ガイドライン等で規定）を行うことを前提とした、事業者または個人事業主からの出向の受入れ**
    (出向者が不正行為等を実施した場合においては、認定事業者に対して是正要求を行い、十分な是正処置がなされないときは認定取消事由となることに加え、原則として一定期間、再申請を認めないことを想定)
  - 認定事業者が発注する委託業務について対応する審査登録制度のサービス区分が存在しない場合、**認定事業者が委託先のセキュリティ対策の実施状況を確認**し、その結果を**政府機関に提出**すること
- 認定事業者が適切な運営体制を担保し続けることが困難となることから、**自社のサービス提供に直接的に関する業務の再委託については一律禁止**する。

例外規定①

- 本制度の同区分の認定を取得済みの事業者への委任（準委任）

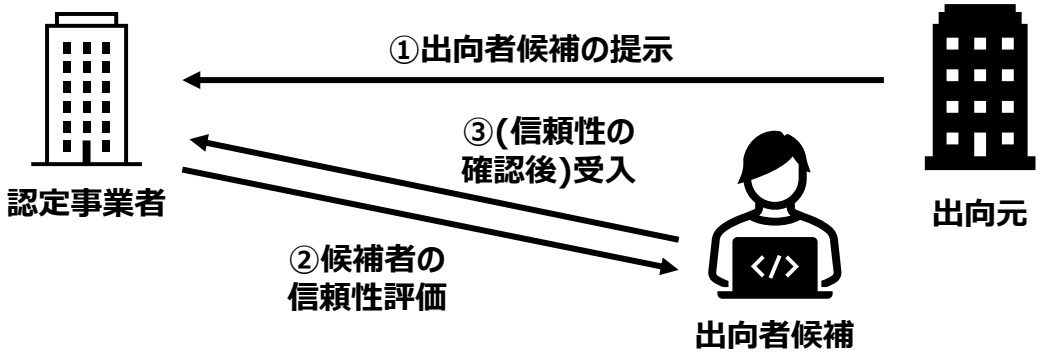
[一例]



例外規定②

- 出向者への信頼性評価を前提とした出向の受入れ

[受入までのプロセス]



認定事業者に求められる行動について

- サイバーセキュリティ・サービス事業者は、**契約の前後を通じて顧客の機微な情報を取り扱う立場にある**ため、正当な理由がない限り、顧客（見込み顧客を含む）からの情報開示の求めに応じることが望ましい。
  - 本制度では、**顧客は、認定事業者との契約の締結にあたり、必要な範囲で情報開示を求めることができる**ものとする。ただし、**契約前に扱われる情報**には、個人情報等も含まれ得ることから、その取扱いについては、**サイバーセキュリティ・サービス事業者と顧客との間でNDAを締結するなど、十分に協議した上で対応**することが必要である。

※NDA契約を締結するに当たっては、サイバーセキュリティ・サービス事業者が、顧客となり得る企業等の適切な運営体制を一定程度確認することも想定される。顧客の適切な運営体制に疑義があるなど、正当な理由があると認められる場合等には、本制度に基づく情報開示の求めに応じないことも許容される。
※国家公務員法に基づく守秘義務があることから、政府機関等が顧客となる場合には、本制度に基づく情報開示にあたり、NDA契約を締結することは要しない。

- **認定を受けたサイバーセキュリティ・サービスに関する事業**において、情報漏えい等の**インシデントが発生した際、政府機関や関係する顧客等に対する報告を求める**こととする（注）。加えて、サイバーセキュリティ・サービス事業者が**犯罪者グループに身代金を支払いを行わないなどの倫理的な対応**も求める。

（注）政府機関においては、申請内容と実態との間に大きな齟齬が認められる場合等には、サーベイランス制度を活用することも想定される。

- **認定事業者が従業員等を適切に管理していることが重要**である。このため、事業者が従業員を管理するうえでの調査・確認事項等の内容については、今後、ガイドラインにおいて整理・提示する。

＜顧客が締結に当たり、求めることができる開示項目について＞

今後ガイドラインにおいて、リスク類型ごとに確認が有効である開示項目(例) 等を整理・提示することを想定。

開示項目(例)

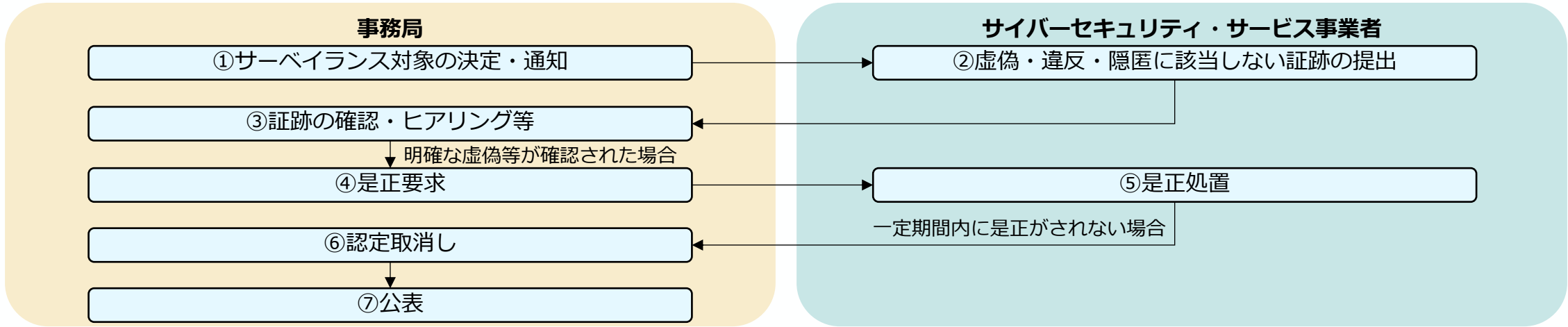
組織	サービス提供に関与する事業主体や外部関与の構造、サービス提供上の責任の所在や管理関係　等
人	サービス提供に関与する者（例：代表者・役員、サービス責任者・従事者）の属性　等
データ*1	サービス提供に伴い取り扱われるデータの取扱方法　等
ツール*2	サービス提供に際して利用されるツールの一覧　等

(*1)事業者が当該サービスの提供に際して契約者から収集するデータのうち、悪意のある第三者が取得することで、契約者に対するサイバー攻撃を引き起こす可能性のあるデータ
(*2)事業者が当該サービスの提供に際して利用するツールのうち、サービスの提供に際して直接的に利用されるまたは利用される可能性のあるツール（上段のデータの保管先としてSaaSのストレージサービス等利用している場合はそれも含む）

サーベイランス制度について

- 虚偽申告への防止策としては、**JC-STAR制度と同様にサーベイランス制度を導入する。**
- 具体的には、申請情報や誓約書上の開示情報等に関する虚偽・違反・隠匿等の疑いが生じた場合等に**事務局がサーベイランスを実施することを可能**とする。サーベイランスの結果、**明確な虚偽・違反が確認された場合は是正処置を要求**し、**一定期間内に是正が図られなかった場合は認定の取消を可能**とする。
  - 必要に応じて、**疑いがなくとも認定取得済みの事業者に対してランダムにサーベイランスが可能な制度とすることも検討。**
  - 誓約書に関する虚偽・違反行為はサービス利用者が検知することが多いと想定されるところ、**虚偽・違反の疑いを情報収集する窓口**を設けてはどうか。
- **認定が取り消された事業者については、取消しの事実を一律で公表することも可能**とする。

サーベイランスに関する手順（仮）

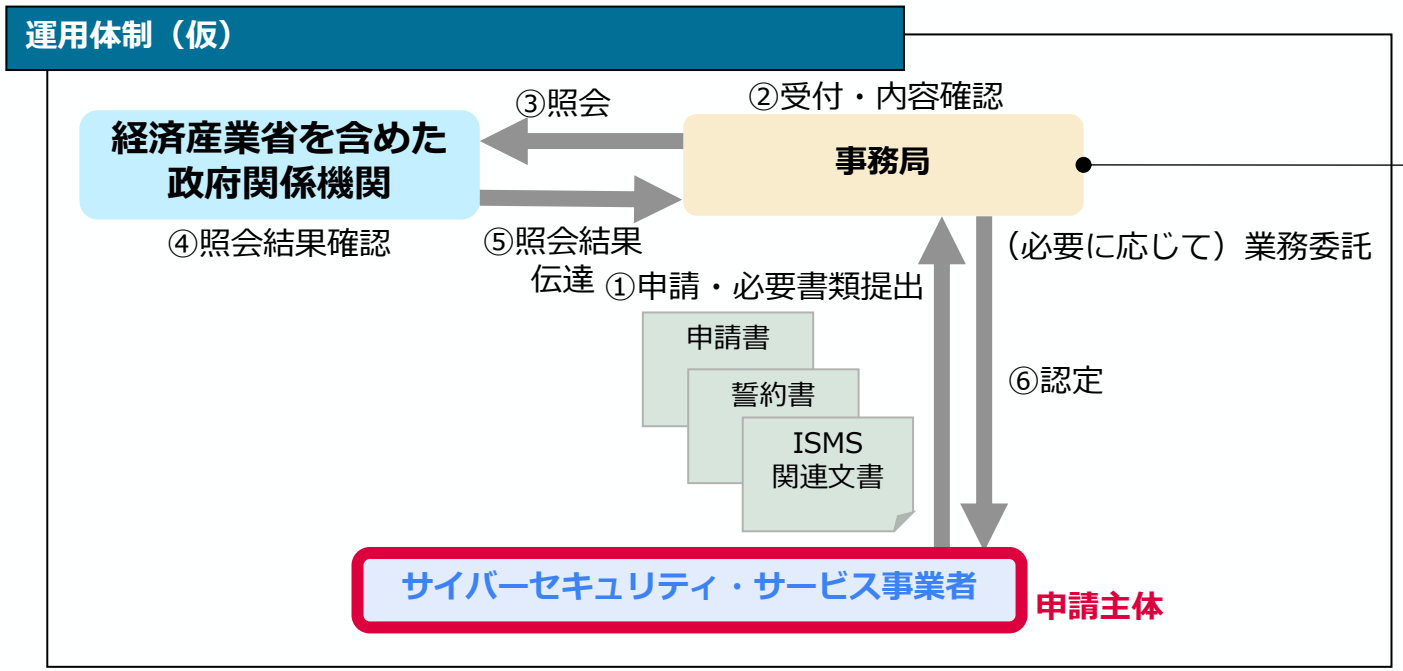


参考（JC-STAR制度のラベル取消しに関する基準）

- 認証機関又はラベル発行機関は、本制度の信頼性を確保するため、適合ラベル付与済みのIoT製品に対して、（略）**サーベイランスを実施することがある。**
- サーベイランスを実施する通知を受領した際には、申請者は、機構が実施するサーベイランスが円滑に実施できるように必要な協力をしなければなりません。**サーベイランスへの協力を拒んだ場合、直ちに適合ラベルは取り消されます。**
- 認証機関及びラベル発行機関は、**サーベイランスの結果に基づき、申請者及び登録者による申請内容、自己適合宣言の内容、ラベル取得要求事項（JSM-02）で定められた条件に反していない旨の自己宣言の内容又は適合評価・認証等に関して違反や虚偽があると認められた場合**、（略）、又は**適合ラベルの信頼性を著しく損なうような行為等が認められた場合**等、適合ラベルの取消しの事由に該当すると判断した場合には、**登録者に対して期限を区切って是正措置を要求**する。登録者は、指定された期限内に是正措置を取らなければならない。**期限内に登録者による是正措置が取られなかった場合、認証機関及びラベル発行機関は、当該適合ラベルの取消しを行うことができる。**

運用体制について

- 本制度に責任を持ち、基本的な規程類等を維持管理する**事務局は、現行の審査登録制度との連携等も踏まえながら、今後決定**する。
- 事務局は、**申請の受付、各種認定要件（適切な範囲のISMS認証の取得等）の充足性に関する確認、認定、認定後の維持管理（サーベイランスの実施含む）等を実施**する。
  - **サービス提供者の主体に関わる適切な運営体制の審査に当たっては、事務局は認定前に、経済産業省を含めた政府機関に照会をかけ、その照会結果に基づき事業者を認定**する。
  - 詳細な業務運営方針については事務局内で検討するものとする。必要に応じた業務委託も可能とする。



事務局の役割（仮）

1. 認定の申請受付・問い合わせ受付
   - 新規申請・内容変更申請・認定延長申請の受付
   - 事業者からの問い合わせ受付と対応
2. 申請者より提出された書類等の確認
   - 書類の形式確認（例：申請書に必要事項が漏れなく記載されているか、情報開示の誓約書に適切な人物が署名しているか、事業者が取得したISMS認証の範囲は適切か etc…）
3. 認定
   - 認定の通知とWebサイト等での公表
   - 認定の取消しとWebサイト等での公表
4. 認定の維持管理
   - 認定の有効・失効管理（例：有効期限の超過時）
   - 虚偽・違反・隠匿等の疑いに関する情報受付
   - サーベイランスの実施要否検討と実施 etc…

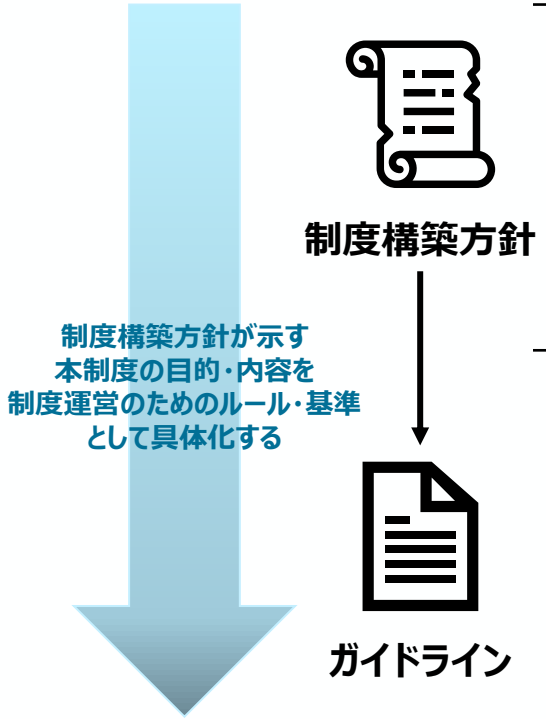
制度の有効期間について

- **本制度は、ISMSやSCS評価制度の★４とも密接に関わる**ところ、**有効期間を３年間**としてはどうか。いずれの制度においても取得時期を踏まえると、必ずしも同時期に失効するとは限らないため、**更新時に速やかに事務局に報告**するとともに、**仮に更新できなかった場合は、原則、認定を取り消す**こととしたい。
- **有効期間が２年間である審査登録制度**についても同様、**更新時に速やかに事務局に報告する**とともに、**仮に更新できなかった場合は、原則、認定を取り消す**こととしたい。
- また、**申請時の内容から大きな変更があった場合**は、**変更等の手続きを速やかに行うこと**を事業者に求めたい。

今後の進め方について

- 2026年度は、企業が本制度の取得を目指すうえで望ましい行動の具体化を含めた制度の詳細設計を行う。 制度開始は、2027年度中を目指す。

今年度の成果物イメージ



制度構築方針

概要

✓ 中間とりまとめ資料（本書）で示された本制度の基本的な考え方を踏まえ、本制度の具体化にあたり、制度の趣旨・目的、対象範囲、対処するリスクについての考え方等を整理するとともに、制度構築段階においてあらかじめ定めておくべき事項を明確化する文書。

ガイドライン

✓ 制度構築方針で整理した制度の前提を踏まえ、サイバーセキュリティ・サービス事業者に求められる対応について、制度運営上のルール・基準として整理するとともに、サイバーセキュリティ・サービス事業者の相手方である顧客による確認が可能な事項等についても示す文書。