経済産業省

資料６

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について

2025年10月

経済産業省

商務情報政策局

（論点①）検討会の議論の範囲について

- 第１回検討会では、情報セキュリティ・サービス以外のセキュリティコンサルティング業務やSI事業者等についても対象にするのかが論点となった。
- サービスの認定を行う上では、**サービスに係る技術・品質と事業者の信頼性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**」**は**、既に技術・品質の基準に基づき登録を行っている現行の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。）をベースにしつつ、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**「事業者の信頼性」を確認**することを目的とするもの。したがって、**当面の間**、**新しい制度では**、**現行制度の対象サービス区分の一部又は全部を対象とすることとしたい**。
  ※ 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。
- また、**技術・品質レベル**については、**現行制度で相当程度確認が可能**であるものの、「**新たな制度**」では、**「事業者の信頼性」を確認する観点から、ツールやデータの管理等の「技術・品質の信頼性」に係る要件を追加的に確認する**こととしたい。
- 本検討会においてAIツールについても、上記の「ツール」の一部として取り扱うこととする。
  ※ AIツールをサービスの中で使用することについては、現行制度でも、品質担保の観点から論点となっているため、**AIツールの取り扱いの妥当性は、現行制度の枠組みで議論**することとしたい。なお、AIの安全性に関する評価手法についてはAISIにおいて検討中。

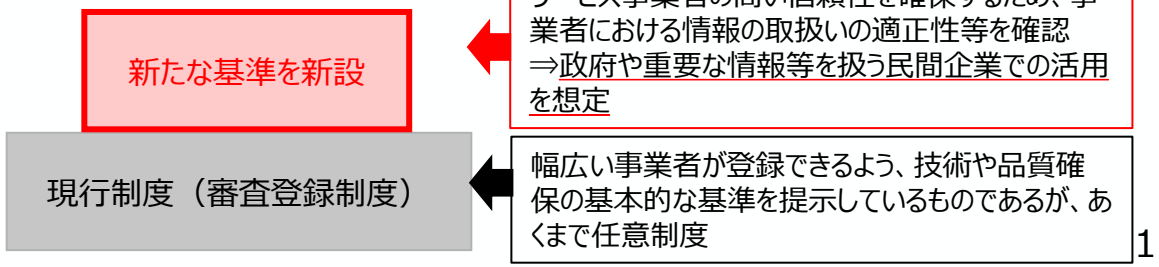
現行制度のサイバーセキュリティ・サービスの種類

（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

＜新制度（イメージ）＞

○**サイバーセキュリティ・サービス認定制度**

リストに掲載された企業から申請を受け、信頼性を確認、認定。



（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：低～中** • 規定・ルールに従ったセキュリティ対策が行えていない箇所の情報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）
(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

（論点②）審査項目の方向性について（案）

公表版

- 第１回検討会で頂いた御意見も踏まえ、**審査項目を以下のとおり定めることとしてはどうか**。事業者等の発表内容や実態を踏まえ、加除すべき項目があれば、御意見いただきたい。
- また、**審査項目の範囲については、企業のガバナンスに関するもののような、比較的普遍的なものとする必要があると考えらえるが、どうか**。

項目（案）
会社の資本関係
従業員の管理方法規程等
情報に関する管理体制の構築
業務委託
使用ツール
自社のサイバーセキュリティ対策

今後の予定

- 次回以降は、主に以下の論点を議論したい。

12月頃	第３回	第２回の議論を踏まえた審査項目案について、制度の限界について、 本制度の活用方法の例示
2月頃	第４回	第３回の議論を踏まえた制度案、制度の運用体制等について
3月頃	第５回	成案の提示　※提示後、パブコメ予定
来年度以降		詳細な判断基準について具体化 ※来年度中の制度運用開始を目指す