経済産業省

資料４

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８月

経済産業省

商務情報政策局

サイバーセキュリティ・サービスの品質の維持・向上に向けた取組

- **サイバーセキュリティ・サービス**とは、**企業のデータを保護し、サイバー攻撃のリスクを削減するために提供される専門的なサポートと技術支援**のこと。
- サービスの内容は多岐にわたり、デジタル環境で安全に業務を推進するための基盤づくりに役立つこれらのサービスの利用により、より強固で有効なセキュリティ対策が可能。
- しかし、多くのサイバーセキュリティ・サービスが提供されており、**専門知識をもたないサービス利用者が、サービス事業者の選定時にそのサービスの品質を判断することは容易ではない**。
- そのため、経済産業省では、2018年から、サイバーセキュリティ・サービスについて**一定の品質の維持向上が図られていることを第三者が客観的に判断し、その結果を台帳等でとりまとめて公開**することで、利用者が調達時に参照できるような仕組み（**情報セキュリティサービス審査登録制度**）の提供を実施。

サイバーセキュリティ・サービスの種類（例）

（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

（参考）情報セキュリティサービス審査登録制度の概要

- 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。**
- 現在、**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、**合計約370サービスが登録**されている。

＜情報セキュリティサービスにおける課題＞

どの事業者のサービスを選べば良いかわからない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

選定時に活用

我が社のサービスを もっと見つけて欲しい

我が社の技術力、サービス品質をアピールしたい

ベンダー
（サービス提供事業者）

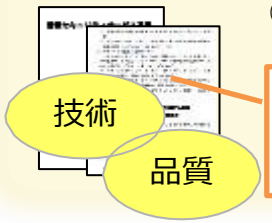
審査を受けリストに掲載

○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として公開

基準を満たした約370サービスを掲載（2025年時点）

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



○情報セキュリティサービス基準（経済産業省）

上記６サービスに関して技術要件･品質管理要件を定めた基準

本制度を通じて目指す社会

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

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

（参考）情報セキュリティサービス

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）(1)情報セキュリティ監査サービス

	定義
定義	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、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、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、もって保証を与え又は助言を行うサービスをいう。
情報セキュリティサービス提供事業者に係る審査基準 （以下、（２）～（５）についても同様のものを求める）	次に掲げる条件を満たすものであること。 ア 反社会的勢力に該当しないこと。 イ 反社会的勢力への便益の供与又はそれに類する行為を行っておらず、将来にわたっても行わないこと。 ウ 本基準の要件への適合性に関して疑義が生じた場合に、当該事項に関する調査を受け入れること。
技術要件	次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況：サービス品質の確保のため、情報セキュリティ監査サービスに従事する要員のうち、指定する専門資格(例：公認情報セキュリティ監査人)又は同等のものを有する者を技術責任者として業務に従事させるとともに、技術責任者のリスト（資格番号の表示のみでもよい。）を明示すること。 イ サービス仕様の明示：サービス品質の確保のため、基準又は同等のものに従って、情報セキュリティ監査サービスが行われていることを明らかにしていること。
品質管理要件	次に掲げる品質管理要件にすべて該当するものであること。 ア 品質管理者の割当状況：品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。 イ 品質管理マニュアルの整備：品質の維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。 （ア）サービス提供プロセスの管理　　（イ）アウトプットの管理 ウ 品質の維持・向上に関する手続等の導入状況：品質維持・向上のため、次に掲げる手続等を行っていること。 （ア）次のいずれかの品質の維持・向上に関する手続等を行っていること。 ａ 情報セキュリティ監査サービスを行った案件について、当該案件に従事した者以外の者が監査計画及び監査報告書についてのレビューを行っていること。 ｂ 情報セキュリティ監査サービスを行った案件についての査読を行っていること。 （イ）情報セキュリティ監査サービスに従事する者に対して教育及び研修等又は同等のもののいずれかを実施又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について情報セキュリティ監査サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

（参考）(2-1)脆弱性診断サービス

	定義
定義	システムやソフトウェア等の脆弱性に関する一定の知見を有する者が、システムやソフトウェア等に対して行う次に掲げるいずれか又は全てのサービスをいう。 ①Web アプリケーション脆弱性診断　②プラットフォーム脆弱性診断　③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
技術要件	次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況：サービス品質の確保のため、脆弱性診断サービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。 （ア）指定する資格(例：Certified Ethical Hacker)または汎用資格(例：情報処理安全確保支援士)又は同等のものを有する者 （イ）指定する専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関における脆弱性診断サービスの技術を対象とする講師経験を有する者 （ウ）次のいずれかの事業において基準となる日から起算して過去３年間に合計で５件（契約件数）以上の実績を有する者 a Webアプリケーション脆弱性診断　b プラットフォーム脆弱性診断 c 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 d その他ソフトウェアやシステムの脆弱性対策を目的とした診断又はテスト （エ）指定するサービス品質確保に資する研修又は同等のものを修了している者 イ サービス仕様の明示：サービス品質の確保のため、基準又は同等のものに従って脆弱性診断サービスが行われていることとともに、脆弱性診断の結果の取扱又は同等のものを明らかにしていること。
品質管理要件	次に掲げる品質管理要件に該当するものであること。 ア 品質管理者の割当状況：品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。 イ 品質管理マニュアルの整備：品質維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。 （ア）サービス提供プロセスの管理　（イ）アウトプットの管理 ウ 品質の維持・向上に関する手続等の導入状況：品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）脆弱性診断サービスを行った案件について、当該案件に従事した者以外の者が検査実施報告書についてレビューを行っていること。 （イ）脆弱性診断サービスに従事する者に対して指定する教育及び研修等又は同等のもののいずれかを実施し又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について脆弱性診断サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

（参考）(2-2)ペネトレーションテスト（侵入試験）サービス

	定義
定義	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をいう。
技術要件	脆弱性診断サービスに掲げる技術要件かつ、次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況：サービス品質の確保のため、ペネトレーションテスト（侵入試験）サービスに従事する要員のうち、次のいずれかの要件を満たす者を１名以上業務に従事させること。 （ア）指定する専門資格（例：OffSec Certified Professional）又は同等のものを有する者 （イ）次のいずれかのペネトレーションテスト（侵入試験）を含む事業に関して基準となる日から起算して過去３年間に合計で３件（契約件数）以上の、顧客が管理しているシステムに対して以下のいずれかを実施した実績を有する者 ａ 脆弱性または設定不備を利用することで、管理者権限を持つアカウントによるオペレーティングシステムへのログインや任意のコマンド実行 ｂ 脆弱性または設定不備を利用することで、一般権限を持つアカウントによるオペレーティングシステムへのログインや任意のコマンド実行 ｃ 脆弱性または設定不備を利用することで、本来アクセス権のないアカウントによる機密情報の入手・外部持ち出し ｄ 脆弱性または設定不備を利用することで、アカウントに対し本来許可していない権限での操作 ｅ ａ～ｄに限らず、脆弱性、外部に漏えいした認証情報又は内部情報を利用することで、オペレーティングシステムやアプリケーション等に対して本来許可されていない操作を実施 イ サービス仕様の明示：サービス品質の確保のため、基準又は同等のものに従ってペネトレーションテスト（侵入試験）サービスで提供する検査のプロセス、及びペネトレーションテスト（侵入試験）の結果の取扱又は同等のものを具体的に明らかにすること。
品質管理要件	脆弱性診断サービスに掲げる品質管理要件かつ、次に掲げる品質管理要件に該当するものであること。 ア 品質管理マニュアルの整備：品質維持・向上のため、ペネトレーションテスト（侵入試験）サービスについて次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。 （ア）サービス提供プロセスの管理、（イ）対象システム等に関する調査、（ウ）ペネトレーションテスト（侵入試験）方法の選定・実施 （エ）アウトプットの管理 イ 品質の維持・向上に関する手続等の導入状況：品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）ペネトレーションテスト（侵入試験）サービスを行った案件について、当該案件に従事した者以外の者が試験実施報告書についてレビューを行っていること。 （イ）ペネトレーションテスト（侵入試験）サービスに従事する者に対して指定する教育及び研修等又は同等のもののいずれかを実施し又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてペネトレーションテスト（侵入試験）サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

（参考）(3)機器検証サービス

	定義
定義	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）に対して行う次に掲げるいずれか又は全てのサービスをいう。 ①機器検証　②機器検証及び Web アプリケーション脆弱性診断　③機器検証及びプラットフォーム脆弱性診断
技術要件	次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況 （ア）サービス品質の確保のため、機器検証サービスの機器検証に従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。 ① 指定する専門資格(例：エンベデッドシステムスペシャリスト)または汎用資格(例：情報処理安全確保支援士)又は同等のものを有する者 ② 基準となる日から起算して過去３年間に合計で５件（契約件数）以上の実績（診断方法は問わない。）を有する者 ③指定するサービス品質確保に資する研修又は同等のものを修了している者 （イ）サービス品質の確保のため、機器検証サービスの脆弱性診断に従事する者は脆弱性診断サービスの「ア 専門性を有する者の在籍状況」に示す要件を満たす者を業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。 ※(ア)と（イ）の要件を同一人が満たす場合には、それぞれの要件の充足状況の確認のため、兼務者として人数を明らかにすること。 イ サービス仕様の明示 （ア）サービス品質の確保のため、指定する基準又は同等のものに従って、サービスが行われていること。 （イ）機器検証においては、指定する内容又は同等のものに従ってサービスが行われていることを明らかにするとともに、指定する検証の結果の取扱又は同等のものを明らかにしていること。脆弱性診断においては、脆弱性診断サービスの「イ サービス仕様の明示」に示す要件を満たすこと。 （ウ）検証の対象と範囲を明示し、その対象と範囲についてのみ検証に対する責任を有することを表明すること。
品質管理要件	次に掲げる品質管理要件に該当するものであること。 ア 品質管理者の割当状況：品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。 イ 品質管理マニュアルの整備：品質維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルや規則等を整備していること。 （ア）サービス提供プロセスの管理 ・サービス利用者（検証依頼者）との仕様調整（例：検証計画、検証対象範囲、実施内容、情報の取り扱い）に関する内容 ・サービス実施方法に関する内容 ・サービス利用者からの要求、意見、クレーム等への対応に関する内容 （イ）アウトプットの管理 ウ 品質の維持・向上に関する手続等の導入状況：品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）機器検証サービスを行った案件について、当該案件に従事した者以外の者が検査実施報告書についてレビューを行っていること。 （イ）機器検証サービスに従事する者に対して指定する教育及び研修等または同等のもののいずれかを実施又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続について機器検証サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

（参考）(4)デジタルフォレンジックサービス

	定義
定義	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、並びにそれらへ至るための行為（事象）等への対応等や法的紛争・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）についての次に掲げるいずれか又は全てのサービスをいう。 • 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
技術要件	次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況：サービス品質の確保のため、デジタルフォレンジックサービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させるとともに、要件を満たす者ごとの人数を明らかにすること。 （ア）指定する専門資格(例：CDFP-B)または汎用資格（例：情報処理安全確保支援士）又は同等のものを有する者 （イ）指定する専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関におけるデジタルフォレンジックの技術を対象とする講師経験を有する者 （ウ）指定するサービス品質確保に資する研修又は同等のものを修了している者 イ サービス仕様の明示：サービス品質の確保のため、基準又は同等のものに従ってデジタルフォレンジックサービスが行われていることを明らかにしていること。
品質管理要件	次に掲げる品質管理要件に該当するものであること。 ア 品質管理者の割当状況：品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。 イ 品質管理マニュアル等の整備：品質の維持・向上のため、次に掲げるものを整備していること。 （ア）サービス品質の管理のためのマニュアル （イ）報告品質に関する約款及び基準 ウ 品質の維持・向上に関する手続等の導入状況：品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）デジタルフォレンジックサービスを行った案件について、当該案件に従事した者又は（１）アの要件を満たす者が調査報告書についてレビューを行っていること。 （イ）デジタルフォレンジックサービスに従事する者に対して指定する継続的なデジタルフォレンジック技術資格維持コース又は同等のものを受講させ並びに教育及び研修を実施し又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてデジタルフォレンジックサービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

（参考）(5)セキュリティ監視・運用サービス

	定義
定義	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についての次に掲げるいずれか又は全てのサービスをいう。 • 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
技術要件	次に掲げる技術要件に該当するものであること。 ア 専門性を有する者の在籍状況：サービス品質の確保のため、セキュリティ監視・運用サービスに従事する要員のうち、次のいずれかの要件を満たす者を技術責任者として業務に従事させているとともに、要件を満たす者ごとの人数を明らかにすること。 （ア）指定する専門資格(例：Certified Network Defender)または汎用資格(例：情報処理安全確保支援士)又は同等のものを有する者 （イ）指定する専門家コミュニティ又は同等のものにおける講師若しくはリーダーの経験又は高等教育機関におけるセキュリティ監視・運用サービスの技術を対象とする講師経験を有する者 （ウ）次のいずれかの事業において基準となる日から起算して過去３年間に合計５件（契約件数）以上かつ運用年数のべ１０年以上の実績を有する者 ａ マネージドセキュリティサービス　ｂ セキュリティアプライアンス製品の運用 （エ）指定するサービス品質確保に資する研修又は同等のものを修了している者 イ サービス仕様の明示：サービス品質の確保のため、指定する内容又は同等のものに従ってセキュリティ監視・運用サービスが行われていることを明らかにしていること。
品質管理要件	次に掲げる品質管理要件に該当するものであること。 ア 品質管理者の割当状況：品質の維持・向上のため、サービス品質の管理に関する担当者を割り当てていること。ただし、当該担当者が専属してサービス品質の管理を行うことを必ずしも求めるものではない。 イ 品質管理マニュアルの整備：品質の維持・向上のため、次に掲げる事項を含むサービス品質の管理のためのマニュアルを整備していること。 （ア）サービス提供プロセスの管理 （イ）アウトプットの管理 ウ 品質の維持・向上に関する手続等の導入状況：品質の維持・向上のため、次に掲げる手続等を行っていること。 （ア）従事者の確保及び作業の実施等についてサービスの品質の維持・向上に関する管理の取組が行われていること。 （イ）セキュリティ監視・運用サービスに従事する者に対して指定する継続的な教育及び研修等又は同等のもののいずれかを実施又は受講させていること。 （ウ）顧客の情報を保護するための手続を設け、運用するとともに、当該手続についてセキュリティ監視・運用サービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保していること。

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

- 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る。
- 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。

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。
Veritaco	2025年4月	2025年４月、アメリカで、サイバーセキュリティ企業VeritacoのCEOであるジェフリー・ボウイ氏が逮捕・起訴された。病院の監視カメラ映像によると、ボウイ氏は病院内を徘徊し、複数のオフィスへの侵入を試みた後、２台のコンピュータにマルウェアをインストールしたとされている。

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。

対応の方向性（案）

- 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「信頼性」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。

- 特に、**政府機関や安全保障に関係する事業者等**においては、**高度な「信頼性」を有するサイバーセキュリティ・サービス事業者を選定・活用するニーズが想定**される。

- 現行の「**情報セキュリティサービス審査登録制度」（登録制度）**では、サービス提供事業者の信頼性について、**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事業者を認定する仕組み**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「信頼性」に係る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、**高度な信頼性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**することとしてはどうか。

本日御議論いただきたい点

- 前頁で示した「対応の方向性」の是非
  - 政策対応の必要性（足下で懸念される事案・動向、ニーズ）、現行の登録制度の上乗せとする形等
- 次回以降に検討すべき事項・論点
  - 対象分野、確認すべき項目、新たな制度の開始時期　等
- 今後の進め方
  - ヒアリング先候補　等