経済産業省

資料３

一部非公開

事務局説明資料

産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環の構築（仮題）に向けて

令和６年７月31日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバーセキュリティ産業の現状

２．これまでの産業振興政策の振り返り

３．今後の進め方・論点（本日御意見をいただきたい点）

マーケットプレーヤーの競争要因

- 前述したマーケットプレーヤー・事業内容を基に、ファイブフォースモデルを活用して競争要因を分析。以下の事柄が考えられる。

①**製品開発・流通では、国内・外資の既存企業が強みを有しており、競争が激しい**（ノウハウや販路、経営体力を上回る付加価値が必要）

②サービス領域は、参入事業者が多いので過当競争にあるが、**ニーズも多様化していることから一定の新規参入の余地はある**（実際、新規参入しているスタートアップあり）。また、**中小企業むけのサービスなど、対応している企業が少ない領域も存在**している。

③クラウド化が進む中で、**既存SIerが占めていた領域の新規参入ハードルが下がり**、クラウド関連のサービスを提供する事業者が参入。

	製品メーカー ①	ディストリビューター	サービスベンダー（国内・海外製品＋付加価値の提供） ②	サービスベンダー（サービス提供のみ）	SIer ③
新規参入	✓ ノウハウや販路、経営体力を有している外資企業が優位	✓ ノウハウや販路、経営体力を有している国内の既存企業が優位	✓ 左記と同様 ✓ 他方、EDR等のサービスが増加すると、専門性やリソースを持つ事業者が必要となるため、そうしたナレッジを有していれば戦える可能性もある。	✓ 参入事業者が多いので競争は激しい ✓ 他方で、市場の要望も多種多様であり、**ニーズに合った／独自のサービスの提供が出来れば戦える**	✓ リソースのコントロールされたり価格抑制を強いられるため利益確保が厳しい ✓ オンプレからクラウドへの移行が進む中、安価で簡易なSIサービスの提供が可能になり新規参入のハードルは低下。
競合	✓ ノウハウや販路、経営体力を有している外資企業が優位	✓ ノウハウや販路、経営体力を有している国内の既存企業が優位	✓ 左記と同様 ✓ 中小企業など、安価で基礎的な部分の運用に対するニーズはある（他方、対応する企業は少ない）。	✓ **外資系のコンサル系企業は、知名度・実績に強み**。 ✓ 運用・監視サービスは顧客ボリュームを確保できないと利益が上がらず、大手企業が有利。	✓ 多くの顧客基盤を持つベンダーが強い。 ✓ 同業種のノウハウ、類似のソリューションを持つベンダが顧客のリプレイスを争う。
売り手交渉力	✓ 製品開発の初期の段階では、知名度もないため非常に弱い。ヒット商品が生まれた段階で強くなっていく。	✓ 情報格差が存在しており、ディストリビューターが強い ✓ 多くのチャネルを有し、販売力がある場合、製品メーカーに対する交渉力は強い。	✓ 左記と同様	✓ ニーズに対して幅広いサービスを提供できるため、一定の交渉力あり。	✓ 顧客に入り込んでいるため顧客と同じ立場とみなされるので売り手の交渉力は弱い。
買い手交渉力		✓ 情報格差が存在しており、ディストリビューターが強い	✓ 左記と同様	✓ 人材不足のため、外部サービスを頼らざるを得ない側面。ただ、必要性はサービスによってばらつき。	✓ 基本的に交渉力は弱いが、他社リプレースの場合は、ユーザが強くなることもある。
代替品	✓ 外資企業による新規製品		✓ 国内製品or自社内の人材	✓ 自社内の人材	

１．サイバーセキュリティ産業の現状

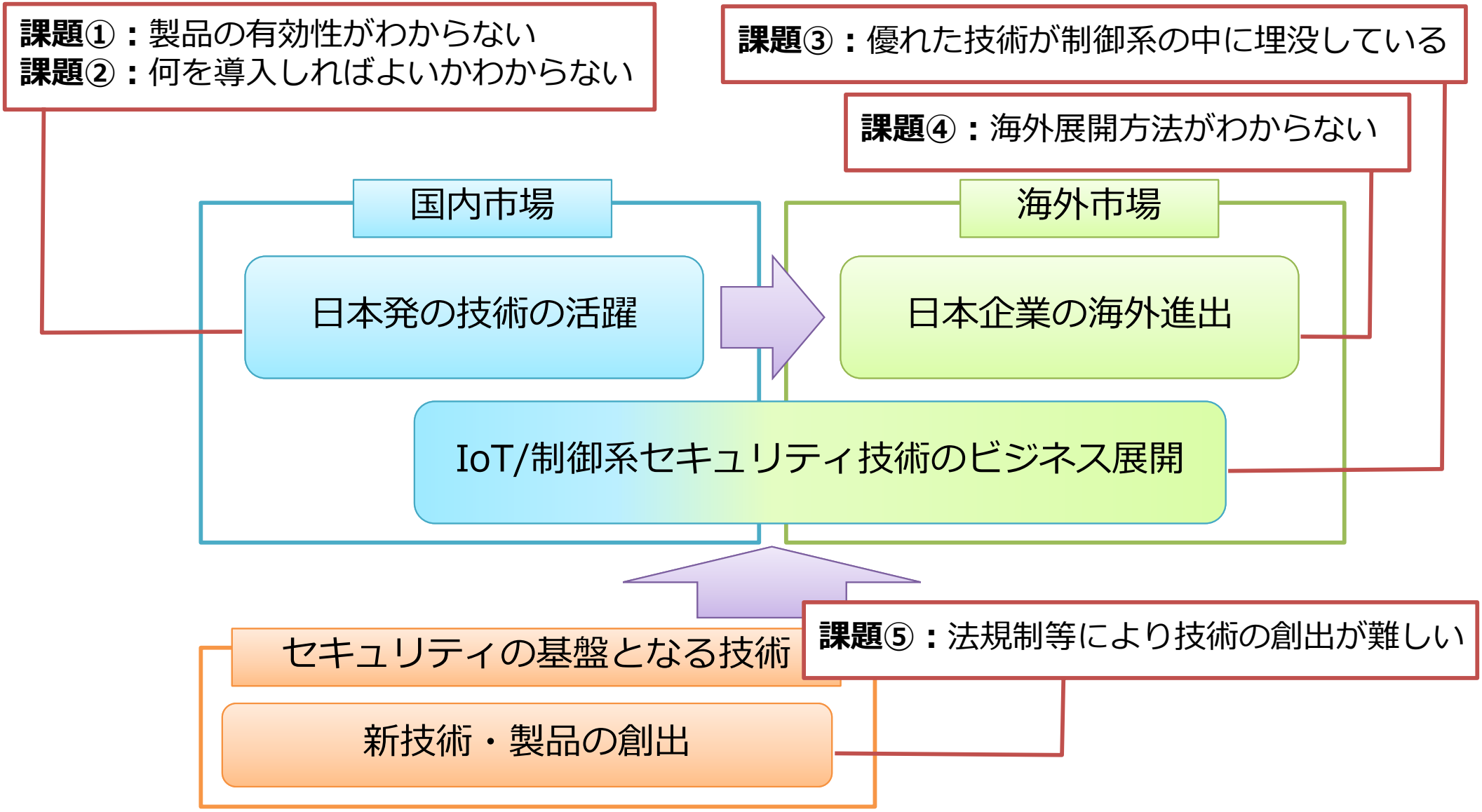
２．これまでの産業振興政策の振り返り

３．今後の進め方・論点（本日御意見をいただきたい点）

セキュリティビジネスにおける政策検討の背景

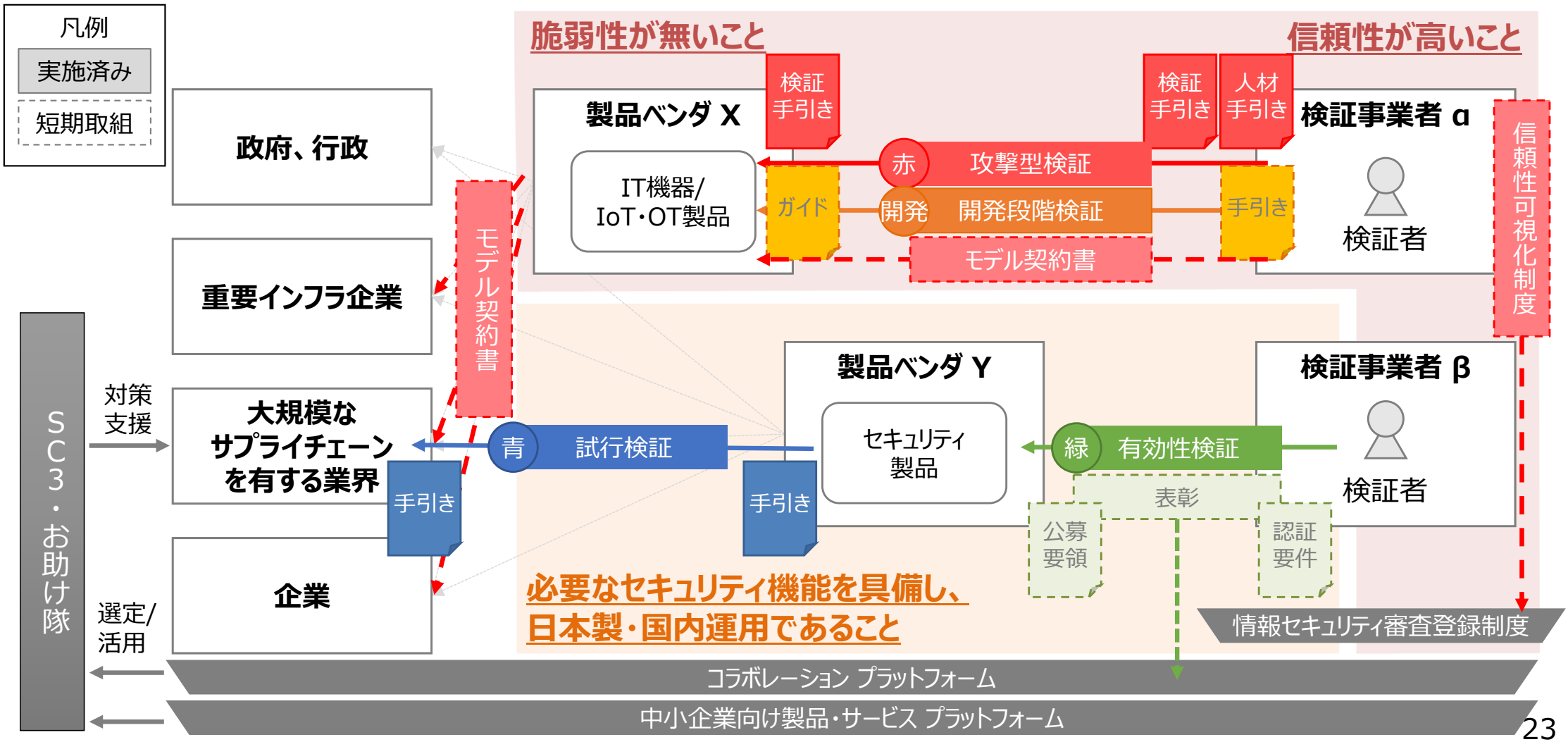
WG3第1回資料から引用
（2018年4月開催）

- **サイバーセキュリティ産業を取り巻く課題（仮説：下記）を解消する**ことによって、サイバーセキュリティの新技術の創出及びビジネス拡大を期待。



Prove in Japan （サイバーセキュリティ検証事業）の取組の全体像

- 産業サイバーセキュリティ研究会WG3(ビジネス化検討)による議論をベースに、セキュリティ検証サービスの産業化に向けて、**セキュリティ製品の有効性検証（緑検証）**や**実環境における試行検証（青検証）**、**攻撃型を含めたハイレベルな検証（赤検証）**を進め、モデル契約やコラボレーションプラットフォーム等と連携してきた。



Prove in Japan、コラボレーションプラットフォームの取組一覧

	概要	これまでの取組・成果
緑検証 セキュリティ製品の有効性を確認し発信する仕組み **青検証** 実環境への試行導入と実績公表を進める仕組み	日本発のセキュリティ製品の特長・強みを活かすことで、海外製品との差別化を図れる可能性があるため、製品の特長を専門家が中立・公平に検証しその結果をユーザー企業に公表して市場参入を促進する。 緑検証では、重要性が高い国内製品の有効性検証を実施し、検証結果を情報発信、評価製品を選定しやすい環境を構築。 青検証では、試行導入・実績公表を行う企業向け手引きを作成。試行導入に関心のあるベンダー・ユーザをマッチングし、国内ベンチャー企業の立ち上げを支援。	2019年～2020年 有識者会議を開催し、重要分野の選定と該当分野の国内製品の検証作業を実施。 実環境における試行評価も併せて実施。 検証作業と試行評価を取りまとめ、コラボレーション・プラットフォームで紹介することでマッチングを後押し。 2021年 試行導入・実績公表の手引きの検討、表彰制度の立案に向けた検討を実施。 ・重要分野マップ　成果公開2回 ・緑青検証審査体制・検証手順書公開 ・導入実績の公開方法・手引書公開 ・製品の検証結果　4製品公開（青1、緑3）
赤検証 攻撃型を含めたハイレベルな検証	サイバー攻撃増加の懸念の中、企業が導入する機器・サービスの信頼性を検証するニーズに答えるべく、攻撃手法に対する技術の構築を加速させるため、攻撃に対するセキュリティ検証に活用可能な技術を調査・追試し、評価手法として確立することを目指す。 検証サービス事業者のサービス高度化に向け、技術や情報管理等の観点において、信頼できる検証サービス事業者を判断するための基準を示す。検証の準備段階で検証依頼者が伝えるべき情報や、検証結果の報告時に検証サービス事業者が伝えるべき情報など、二者が適切なコミュニケーションを行うための留意事項等を示す。	検証サービスの信頼性向上及び検証事業の活性化のために、本編と3つの別冊によって構成されるセキュリティ検証の手引きを整備。 （2019年度作成、2021年３月拡充） 別冊1：セキュリティ検証の詳細解説書 別冊2：機器メーカに向けたセキュリティ検証の解説書 別冊3：検証人材の育成に向けた手引き （2021年3月作成） 機器検証サービスの運営開始（2023年3月から審査登録制度に追加。現状登録されているサービスは8件）
開発段階検証 セキュリティ・バイ・デザインを実現する開発段階検証	開発段階から、設計書とソースコード、実装したプロトタイプで検証を行い、脆弱性を排除した開発を実施。開発段階からの検証の効果を可視化。「セキュリティ・バイ・デザイン」の考え方を採用しコスト低減を図り、中小企業に検証の必要性を認知してもらうことを目指す。	IoT機器を開発する中小企業向け製品セキュリティ対策ガイド」2023年６月に発表。 ものづくり補助金において、当該補助金を活用して開発・導入した製品やサービス、システムに対するペネトレーションテスト・脆弱性診断も支援対象として追加（第15次公募（2023年4月）から開始）。
コラボレーション・プラットフォーム 市場のニーズとシーズのマッチングの場	国内セキュリティ産業における需要側と供給側が、メンバーを限定しない情報交換、交流を行っていただける「場」をMETI・IPAが提供。講演、パネルディスカッション等を通じて、意見交換、共同研究、ビジネスマッチングなどを促進。	2018年～2023年度までに27回開催し、のべ3,341名が参加。緑青検証で有効性が確認されたセキュリティ製品のシーズとニーズに係るマッチングの場を提供し、市場展開を促進してきた。コロナ禍以前はオンサイトが中心、以後はオンラインを中心として年数回程開催。

Prove in Japan／コラボレーション・プラットフォームに対する主な意見

【緑青検証】
- ✓ セキュリティ製品に対するPoCを実施する場合、**普通のサービスを導入するくらいのプロセスや工数を掛けて当社システムに導入して検証**するため、**多くの製品はPoCを実施する段階で挫折**している。検証基盤での検証結果を踏まえ、企業が本来PoCで検証する範囲の一部を省略したりすることができれば、**シーズ企業としては良い取組**。
- ✓ また、サイバーセキュリティ検証基盤での有効性検証がビジネス環境での検証結果であれば、**ニーズ企業にとっても良い判断材料になりうる**。
- ✓ 他方、**ITベンダーやSIerといった中間業者においては、製品導入の実績が必要との声も**。

【赤検証】
- ✓製品の信頼性・効果を検証する能力を国内で確保するため**、検証事業者側で必要となる実施手順事項の整備が出来た**。

【開発段階検証】
- ✓ 開発段階の製品検証で得られた知見を検証事業者や製品ベンダが参照するための手引きやガイドが整備されたことで、**中小企業の開発者の取組の促進及び経営者層の意識向上に役立っている**。

【コラボレーション・プラットフォーム】
- ✓参加者からは、政府施策の認識、最新動向の情報収集等、**多方面な議論を共有される場として有益だったとの声**。
- ✓他方で、
  - ①コロナ禍以降、集客を狙ったオンライン開催が主流。**テーマを需要側である中小企業にフォーカスすると集客が良いが、それが主な供給側である首都圏の大企業が売り込みたい先かどうか疑問が残る**。
  - ②ビジネスマッチングにおいて、**地方の需要側は実際に自分の会社の面倒を見てくれる契約者と話したい**のが自然。**首都圏を中心とした供給側の設定は、この部分で需要側の期待とマッチしていない**と思われる。
  - ③多様なニーズに対応するためには包括的なイベントでは難しい。**対象とテーマを業種や規模に応じた設定で実施する必要**がある。

これまでの産業振興に係わる取組の全体像

技術・ビジネス

①技術の開発
○サイバー空間の状況把握力や防御力の向上に資する技術の開発

②サービスの信頼性付与
○審査登録制度

市場創出

③国内市場の創出
○製品の有効性検証・実環境の試行導入促進（「Prove in Japan」の検証制度）
○マッチングプラットフォームの提供（「コラボレーション・プラットフォーム」）
○”With Security”の市場創出（「IoT適合性評価制度」の立ち上げ）

環境整備

④攻撃把握・分析・共有基盤の強化
○CYNEXの活用　○ハニーポット技術等を用いたサイバー攻撃観測技術の高度化

⑤人材育成・確保
○「お助け隊サービス」の提供　○ICS-CoEによる人材育成

１．サイバーセキュリティ産業の現状

２．これまでの産業振興政策の振り返り

３．今後の進め方・論点（本日御意見をいただきたい点）

今後の進め方（案）

- 「我が国サイバーセキュリティ産業の振興」を題目として、（１）**アドレスすべき政策課題を特定**し、（２）**その課題に効果的にアプローチできる政策**を検討する（政策提案に係るパッケージを示す）ことが、本検討会のゴール。

- （１）については、以下のような点を整理することが必要ではないか。

  ① そもそも、「サイバーセキュリティ産業」とは何か。その外縁をどのように考えるべきか。

  ② 今回の検討を通じてどのような世界を実現するか。

  ③ 政府（経済産業省）として、どのような主体を応援するべきなのか。また、現在、関連する製品／サービスを提供している企業等は、国内外で存在するのか、どういった状態なのか。業界に大きなインパクトをもたらしうるような企業は存在するのか。

  ④ そうした理想の姿を実現できないのは、どのような課題が存在するからなのか。

  ⑤ これまでの／既存の政策は、上記課題について、何にアプローチできていて、どのような点が欠けていたのか。

- 今回は、**事務局から提示した各種情報をもとに、上記（１）について、議論を深めていただきたい**。

- 次回以降、**有識者や関連組織から**、上記（１）及び（２）に示唆を与え得る**プレゼンテーション（情報提供）を行っていただき、検討会委員の皆様からも深堀り・議論いただく**ことを通じて、検討を深め、本検討会における上記（１）及び（２）についての仮説を洗練化させていきたい。

  ※ 別途、“Call for Opinions”といった形で、国内外に対し広く意見を募集することも一案。

論点（本日御意見をいただきたい点）①

1. そもそも、「サイバーセキュリティ産業」とは何か。その外縁をどのように考えるべきか。

仮説１）**何らかのセキュリティ機能を提供するハードウェア／ソフトウェア製品またはサービスを開発し、提供している企業群によって構成**される。広義には、海外製品を含む製品・サービスを日本において販売するディストリビュータ（製品の当該国での展開の他、一般的には当該製品の一次サポートも提供）を追加した、提供者側として活動する全てを含めたものを言う。

仮説２）民間企業のみならず、**大学等の研究機関も、研究対象がサイバーセキュリティ機能に資するものであるならば、直接的なビジネスに関係していなくとも「サイバーセキュリティ産業」の一部を構成**する。

仮説３）**IT/OT製品・システムにセキュリティの価値を加えてビジネスの拡大を図ろうとするものについても、「サイバーセキュリティ産業」の事業領域に含む**（「for security」のみならず、「with security」も含む）。

2. 今回の検討を通じて、どのような世界を実現するか。

仮説１）**政府として産業界に様々なセキュリティ対策を促し、国内マーケットが拡大**される中、**国内企業がシェアを確保**している／**ユーザー（政府・企業）が**、自らの知見・問題意識等を基に、**主体的に製品・サービスを選択**する中で、**国内企業は、そのニーズに基づいた製品・サービスを提供し、ユーザーから選択されそのニーズを獲得する存在**となる

仮説２）**優位な技術・ビジネスモデルを持つ我が国の企業が、国際市場の中でプレゼンスを発揮するとともに、デジタル赤字の解消に寄与（我が国企業が、主要なサプライヤーとなる領域も出現）**

仮説３）技術革新も踏まえたセキュリティ関連の技術開発を行うとともに、そのアウトプットとして**新しい製品・サービスを創出する主体が次々に生まれる状態（それによる経済効果も期待）**

論点（本日御意見をいただきたい点）②

３．**政府（経済産業省）として、どのような主体を応援するべき**なのか。また、現在、**関連する製品／サービスを提供している企業等は、国内外で存在するのか、どういった状態なのか。業界に大きなインパクトをもたらしうるような企業は存在するのか**。

前提）現在ニーズが存在する多くの分野については、**既存企業（特に、製品分野であれば外資企業）がシェアを占めている**状態。他方、**下記の３分野であれば、企業が新たに参入する余地も残されているのではないか。**

前提）セキュリティ業界に大きなインパクトをもたらす主体である必要（例：**他の企業が持っていない高い技術力、顧客の課題解決するビジネスモデル**　等）

仮説１）今後産業界において強化する必要がある分野（セキュリティ対策強化を政策的に促している領域）に必要な製品・サービスを提供する企業

（例）SBOM・IoT製品のセキュリティ強化に資する製品・サービス、中小企業向けの製品・サービス 等

仮説２）当該事業が技術的・ビジネス的に優位性を持っている、ないしは元来強みを持つ分野においてセキュリティ品質を加えている等、国際競争力を有していると考えられる分野の企業

（例）制御系システムのセキュリティ製品（例：検知製品）、自動車・インフラ分野でのセキュリティ 等

仮説３）技術革新に伴い、新たにセキュリティの必要性が生まれる分野の企業／研究機関

（例）機械学習におけるセキュリティ確保（データ汚染等の攻撃から守る製品等）、シャドーデータの特定 等

論点（本日御意見をいただきたい点）③

４．そうした理想の姿を実現できないのは、どのような課題が存在するからなのか。

仮説１）供給側のベンチャー企業にとって、いかに製品を扱って貰うかが重要。需要側のユーザー企業にとってはベンチャー企業の製品は不安であり、特にセキュリティ製品はその考えが顕著（**売買の際に、活用実績が求められるため、最初の実績を作れない／活用主体から活用実績として紹介することを禁止されている**、といった課題を抱えている）。

仮説２）事業展開を進めていく上では、資金や販路等のある程度の経営リソースが必要。また、一企業だけでは限界がある中で、**関連企業で協働する等の取組も必要**だが、**これらに資する枠組みが手薄。**

仮説３）海外展開を行うにあたっては、海外展開の方法がわからない。また、国際競争力を有する可能性のある、優れた技術について上手くビジネス化できていない。　等

5.　これまでの政策は、上記課題について、何にアプローチできていて、どのような点が欠けていたのか。

仮説１）各種検証事業を実施したものの、企業の実導入を大きく促す取組にはならず、そもそも事業の規模が不十分／政府等の主体が試験的に導入する実績がなければ問題の根本解決にならない可能性。

仮説２）コラボレーション・プラットフォームは、ニーズとシーズのマッチングを試みた事業であったが、**シーズ企業が直接的にニーズに働きかけるのはハードルが存在**しているのではないか。また、**ミスマッチ（例：都市部のシーズ企業ー地方のニーズ企業）があったとの声もあり、フォーカスを絞る必要**もあったのではないか。また、**シーズ同士のマッチングを求める声もあった。**

仮説３）これまでの取組は、**「製品」の「技術的な優位性」に着目**したものになっており、**サービスの観点が欠けていた／海外の販路開拓も含めた企業の経営課題の解決に着目した取組が少なかった**のではないか。

（参考）企業・有識者等からの生声

- 特に、小規模のセキュリティベンダーは、なかなか大規模な受注につながりづらい。個社ごとに動いており、セキュリティ業界の中にどういった企業がいるのかは見えないので、いきなり一緒にやりましょうと言っても上手くいかないと思う。**セキュリティ業界の中で、うまく協働できる仕組みがあると良い**（中小サービスベンダー）。

- セキュリティ製品・サービスを売り込むにあたり、ITベンダーやSIer等の中間業者が扱うが重要であるが、その際に**活用実績が最も重視**される。仮に、高い性能を持っていたとしても、実績がなければ活用になかなか結びつかないケースもある（中小製品ベンダー）。

- **販路機会をどのように創出するか**が悩ましい。特に、スタートアップが販路機会がない場合は、SIerの大手や独立系などに販路機会創出に協力的・積極的であるかが鍵（販売支援主体）。

- **海外の企業と比べると、国内企業は市場を日本に限定**している。海外をターゲットにすると、市場は大きく広がり、入ってくる情報量で差が出てくるのではないか（金融支援主体）。

- 導入実績が少ない製品は、検討の俎上に載ることが難しい。**政府機関等で導入される機会があると良い**。アメリカ等では、政府が積極的にスタートアップ製品を活用しており、政府によるフィードバックを受けることで製品の性能が向上する、という循環にあると聞いている（中小製品ベンダー）。

- セキュリティビジネスについては、企業の知名度が十分に浸透していないこと、高度な技術を理解できる人間が少ないことから、**（ファンドや金融機関等を通じた）投資・融資は過小なものになっている**と感じる。また、**セキュリティビジネスを営むプレーヤーは、経営面で弱いことも多く、資金面とともに、そうした点でもサポートできる人間が必要**（中小サービスベンダー）。

参考

過去に策定された重要領域

- セキュリティ領域の全体マップを作成し、市場性や日本発の製品が強味を発揮可能か等の観点から重要分野を選定すべく、2020年度サイバーセキュリティ検証基盤構築に向けた有識者会議において検討を進め、重要分野マップとして2020年12月に策定。
- その後、重要分野に該当する製品を公募で選定し、有効性評価、実環境における試行評価を2021年2月に実施。

＜選定された重要分野＞

① 脅威の可視化

② 脆弱性の可視化

③ IT資産管理

④ 脅威インテリジェンスの整理・管理

⑤ マルウェア感染/発症の重篤度判定

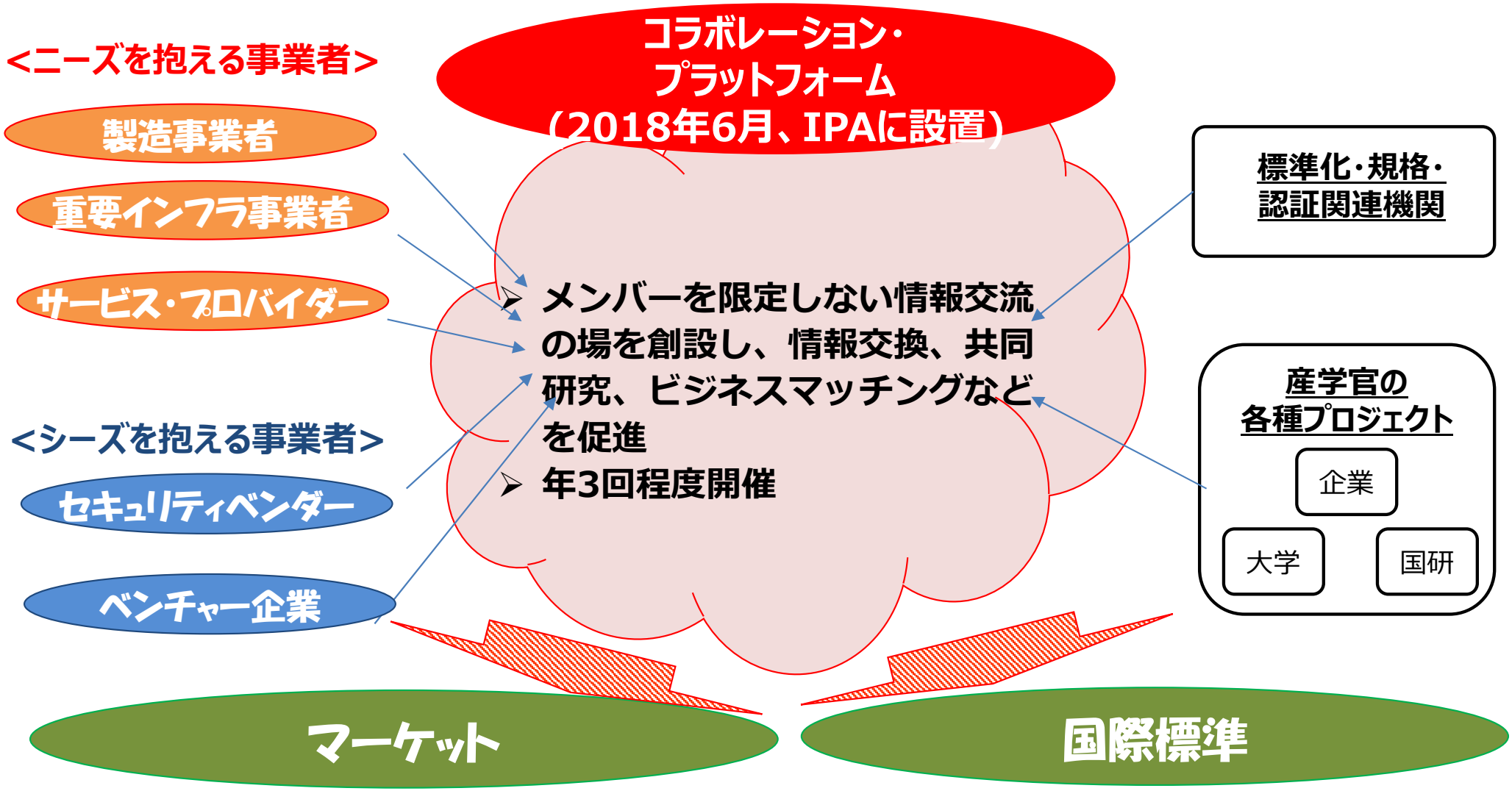
⑥ 教育・トレーニング

⑦ ハイレベルセキュリティ検証

⑧ IT資産の認証/検証

コラボレーションプラットフォームの全体像

- 各WGの活動などを通じて顕在化したニーズとシーズをマッチングする“場”となる**「コラボレーション・プラットフォーム」をIPAに設置し、2018年6月から活動を開始**。



先進的サイバー防御機能・分析能力強化のための研究開発

- 深刻化するサイバー攻撃に対して、サイバー防御機能や分析能力の強化につながる技術を確保することが重要。
- 経済安全保障重要技術育成プログラムにおいて、経済安全保障の確保・強化の観点から、「サイバー空間」を支援すべき重要技術とし、**サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等の研究開発を実施する予定（320億円を超えない範囲／5年）。
- 2023年10月に具体的な研究開発の構想を示しており、これに基づき、同年12月に公募を開始。外部有識者による審査等も踏まえた上で、実施事業者を決定。今後、研究開発を本格的に開始予定。

１．背景

- サイバー空間において提供される多様なサービスが複雑化するに伴い、サイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化。近年では、**人工知能（AI）**を活用した攻撃に代表される**新たなサイバー攻撃のリスク**や、**量子計算機の活用**の広がりに伴う**既存暗号の危殆化によりデータが漏洩するリスク**が顕在化。
- **サイバー空間の状況把握力や防御力の向上に資する技術**や、**セキュアなデータ流通を支える暗号関連技術**等を開発し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを目的とする。

２．研究開発の内容

（１）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

（２）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

（３）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

（４）セキュアな量子情報通信技術の開発

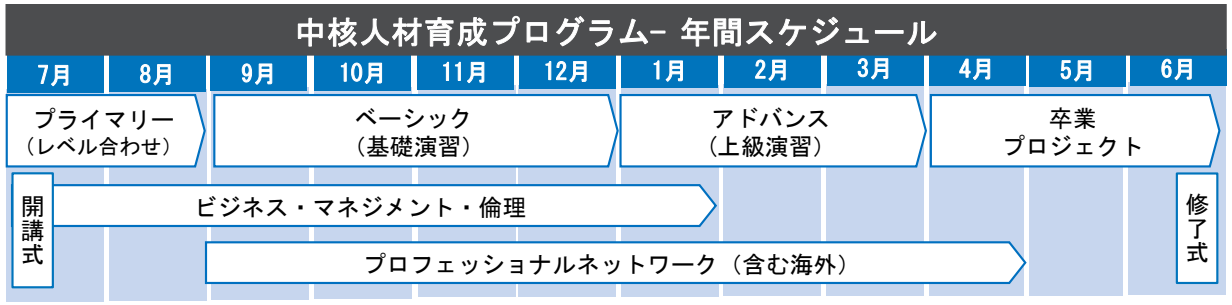
- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

IPA産業サイバーセキュリティセンター（ICSCoE）(2017年4月設置)

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**<u>世界レベルのサイバーセキュリティ対策の中核拠点</u>**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング

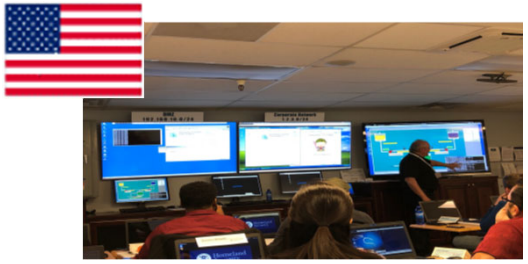
□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人）



- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施



➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。現時点で**40事業者**がサービスを提供。
- 中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。IT導入補助金による支援を拡充。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- EDR・UTM等による異常監視
- 緊急時の対応支援・駆付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスウェブページ
https://www.ipa.go.jp/security/otasuketai-pr/

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業

自社の信頼性をアピール → 取引先（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。

IT導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「インボイス対応類型」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、**申請採択における審査時に加点対象**になっている。
- 2022年８月から、新たに「セキュリティ対策推進枠」を創設。**「サイバーセキュリティお助け隊サービス」のみでの補助金申請が可能**になっている。

＜IT導入補助金2024概要＞

メインツールと組み合わせて、**オプションとして「サイバーセキュリティお助け隊サービス」**を申請可能。

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠	インボイス枠 インボイス対応類型	セキュリティ対策推進枠
要件	業務効率化やDXの推進等に資するITツールを導入	インボイス制度に対応した会計・受発注・決済の機能を有するITツール及びそのためのハードウェアを導入	サイバーセキュリティお助け隊サービスを導入
補助上限	ITツールの業務領域が 1～３まで：5万円～150万円 4以上：150万円～450万円	ITツール： １機能：～50万円 ２機能以上：50万～350万円 PC・タブレット等：～10万円 レジ・券売機等：～20万円	5万円～100万円
補助率	中小企業：１/２	～50万円以下：3/4 (小規模事業者：4/5) 50万円～350万円：2/3 ハードウェア購入費：1/2	中小企業：1/2
対象経費	ソフトウェア購入費、 クラウド利用料（最大2年分）、 導入関連費	ソフトウェア購入費、 クラウド利用料（最大2年分）、 導入関連費、 ハードウェア購入費	**サイバーセキュリティお助け隊サービス利用料（最大2年分）**

オプションとして**「サイバーセキュリティお助け隊」を申請した場合、利用料の1年分（「サイバーセキュリティお助け隊」導入は加点要素）**

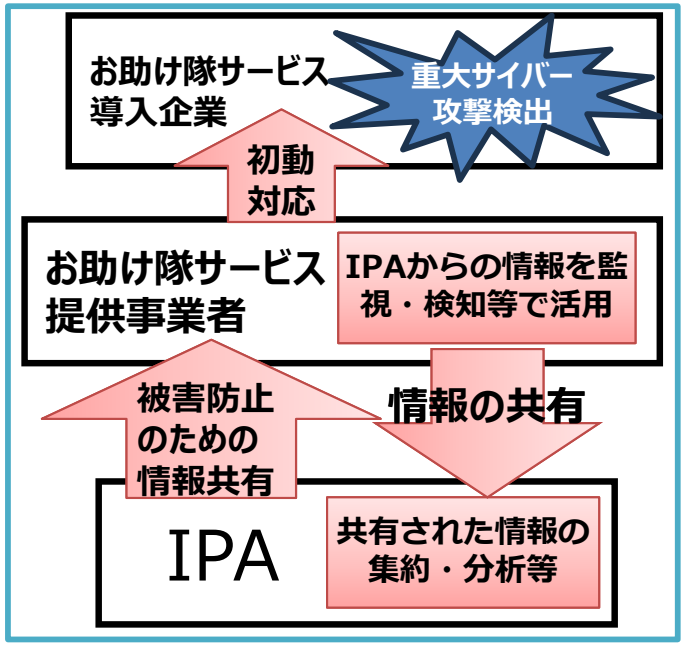
IT導入補助金のインボイス枠(電子取引類型)、複数社連携IT導入枠においては、サイバーセキュリティお助け隊サービスは補助等の対象外である。

サイバーセキュリティお助け隊サービスの新たな類型（２類）について

- 経済産業省では、ＩＰＡを通じて、システムの異常監視やサイバー攻撃時の初動対応支援、復旧費用の簡易保険など**中小企業のセキュリティ対策に必要となる各種サービスをまとめて提供する民間のセキュリティサービスを登録し公表する「サイバーセキュリティお助け隊サービス」制度を運用（2021年度開始）**。
- 現行のお助け隊サービス（１類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであるところ、**中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（２類）を創設**。
- 具体的には、現行のお助け隊サービスのコンセプトは維持しながら、**価格要件を緩和しつつ、提供中のお助け隊サービス１類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として、基準の改定を実施**（2024年３月15日に公開）。**お助け隊サービス提供事業者から共有された情報は、IPA内で集約・分析等し、お助け隊サービス提供事業者へ情報共有する**。
- **令和６年度以降、 ２類サービスの基準への適合性審査を開始し、適合した２類サービスを公表していく**。また、厚生労働省等の**関係機関や業界団体とも連携しながら**、**お助け隊サービスの更なる普及、促進を図る**。

2類のイメージ

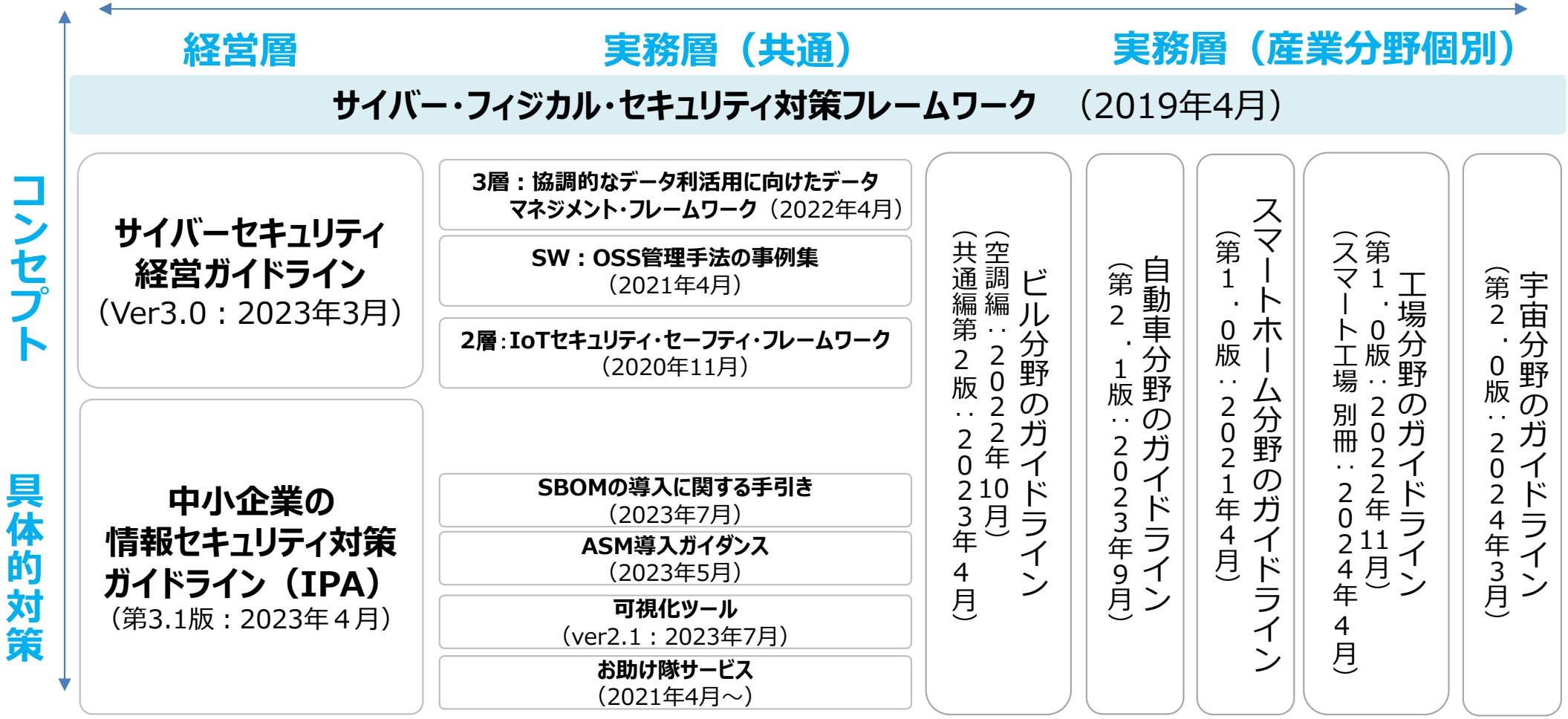
IPAとの情報共有イメージ



サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- Society5.0における産業社会での**セキュリティ対策の全体枠組み**を提示。
- 全体の枠組みに沿って、**対象者や具体的な対策を整理**し、『**サイバーセキュリティ経営ガイドライン**』や**産業分野別のガイドライン**などの実践的なガイドラインを整備。

主なガイドラインや対策ツール



サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

- これまで「サイバーセキュリティ経営ガイドライン」や産業分野別のガイドライン等を整備し、各企業等による積極的な取組を推進してきたところ。他方、**異なる取引先から様々な対策水準を要求される**といった課題や、**外部から各企業等の対策状況を判断することが難しい**といった課題は依然として存在。
- 今後は、諸外国で議論が進んでいる、「サイバー対策」のレーティング等も参考にしつつ、**各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき各企業の対策のメルクマール**や、**業界間の互換性を確保しながら**その**対策状況を可視化する仕組みを検討していく。**
- 併せて、関係省庁とも連携し**政府機関・企業による活用を促す枠組みと紐付ける**ことで、**その実効性を強化**していく。

想定される検討事項

- **既存のガイドライン等をIPAが一元的に管理・体系化し、企業のセキュリティ対策基準を明確化できないか**
- 既存ガイドライン等と整合を取りつつ、**業種横断的なセキュリティ対策レベルを評価（自己評価、第三者認証）できないか**
- 政府機関等における**調達要件**や、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話※での活用**を促進し、**実効性の強化**につなげられないか

※サイバーセキュリティへの取組に関し、投資家を含むステークホルダと企業経営者との対話（開示）の在り方等についても検討が必要ではないか。

対策レベルの可視化（イメージ）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）
レベル感の説明	サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業者、経済安全保障上、特に重要なインフラ事業者、関連サプライヤーが満たすべき基準
ガイドラインの相当性を認定	・IPA「中小企業の情報セキュリティ対策ガイドライン」	・○○業界ガイドライン ・・・・	・重要インフラ行動計画 ・・・・
ガイドライン準拠を確認する方法を定義	自己宣言型	第三者認証型	第三者認証型

政府調達・補助施策等への要件化

取引先からの対策要請による活用促進

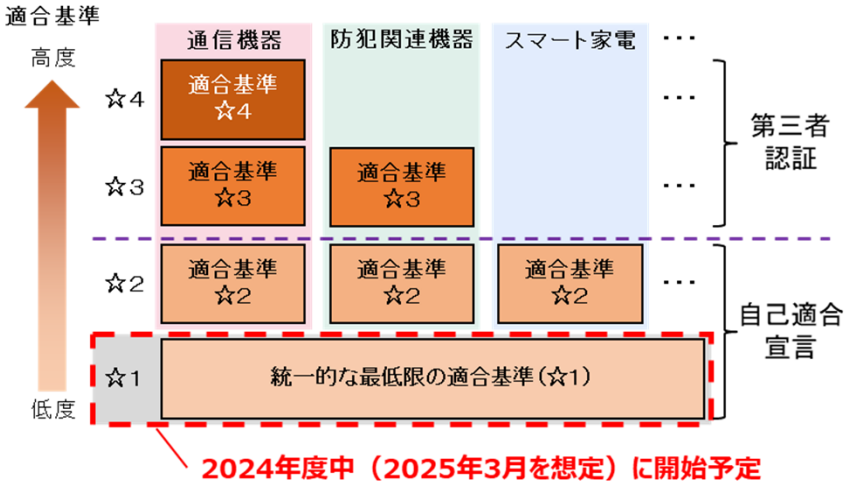
利害関係者への情報開示による対話の促進

ガイドライン等の実効性の強化
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

- セキュリティ対策レベルを評価し、それを可視化する取組の**先行例として、IoTセキュリティ適合性評価制度を検討中**。**米欧等の諸外国との制度調和を図るための議論も継続中**。
- また、**SBOM（ソフトウェア部品構成表）**導入時の課題検証のための実証や企業向けの手引書を策定。
- IoTセキュリティ適合性評価制度の実効性強化やSBOMの導入促進に向けては、**産業界との連携のほか、政府調達等の要件化等に向けて関係省庁と議論も開始**。
- さらに、米国が策定し、我が国政府も共同署名をしたセキュア・バイ・デザインのガイダンスも踏まえ、**ソフトウェア開発者が行うべき取組整理**や**安全なソフトウェアの自己適合宣言の仕組みの検討**を行っていく。

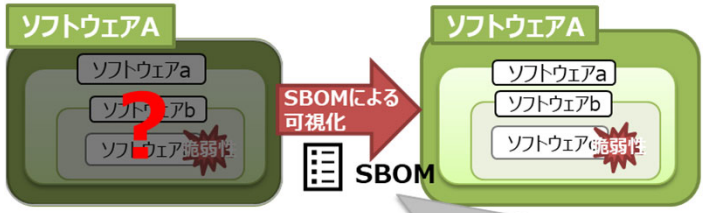
IoTセキュリティ適合性評価制度

- 幅広い**IoT製品を対象**として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、**2024年度中に一部運用を開始**予定。



SBOMのイメージ

- **SBOM（ソフトウェア部品構成表）**がソフトウェアのセキュリティの脆弱性を管理する手法の一つとして着目。



サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	|…ソフトウェアa	Ver2.1	……	…
B会社	|…ソフトウェアb	Ver5.3	……	…
C会社	|…ソフトウェアc	Ver1.2	……	…

セキュアバイデザイン・セキュアバイデフォルト

- **セキュア・バイ・デザイン**：IT製品（ソフトウェア等）が、設計段階から安全性を確保されていること。
- **セキュア・バイ・デフォルト**：ユーザーが、追加の手間をかけることなく、購入後すぐにIT製品（ソフトウェア等）を安全に利用できること。

（出典：国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」）（2023年10月28日署名）

情報セキュリティサービス審査登録制度の概要

- **一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」**を策定し、基準に適合す るサービスのリストを2018年6月よりIPAが公開。

＜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分からない

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

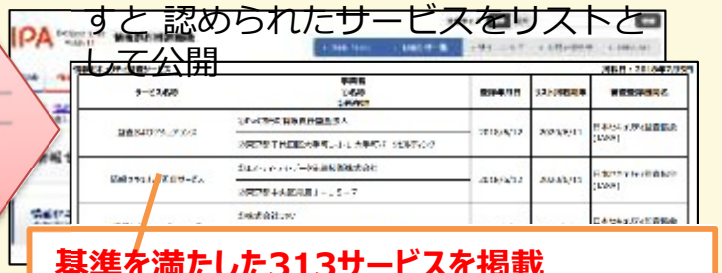
我が社の技術力、サービス品質をアピールしたい

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313サービスを掲載

- 情報セキュリティ監査（70サービス）
- 脆弱性診断（138サービス）
- ペネトレーションテスト（侵入試験）
  （2024年度第3回審査より受付予定）
- デジタルフォレンジック（39サービス）
- セキュリティ監視・運用（52サービス）
- 機器検証 （14サービス）

2024年6月

現在

技術

品質

○情報セキュリティサービス基準（METI）

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

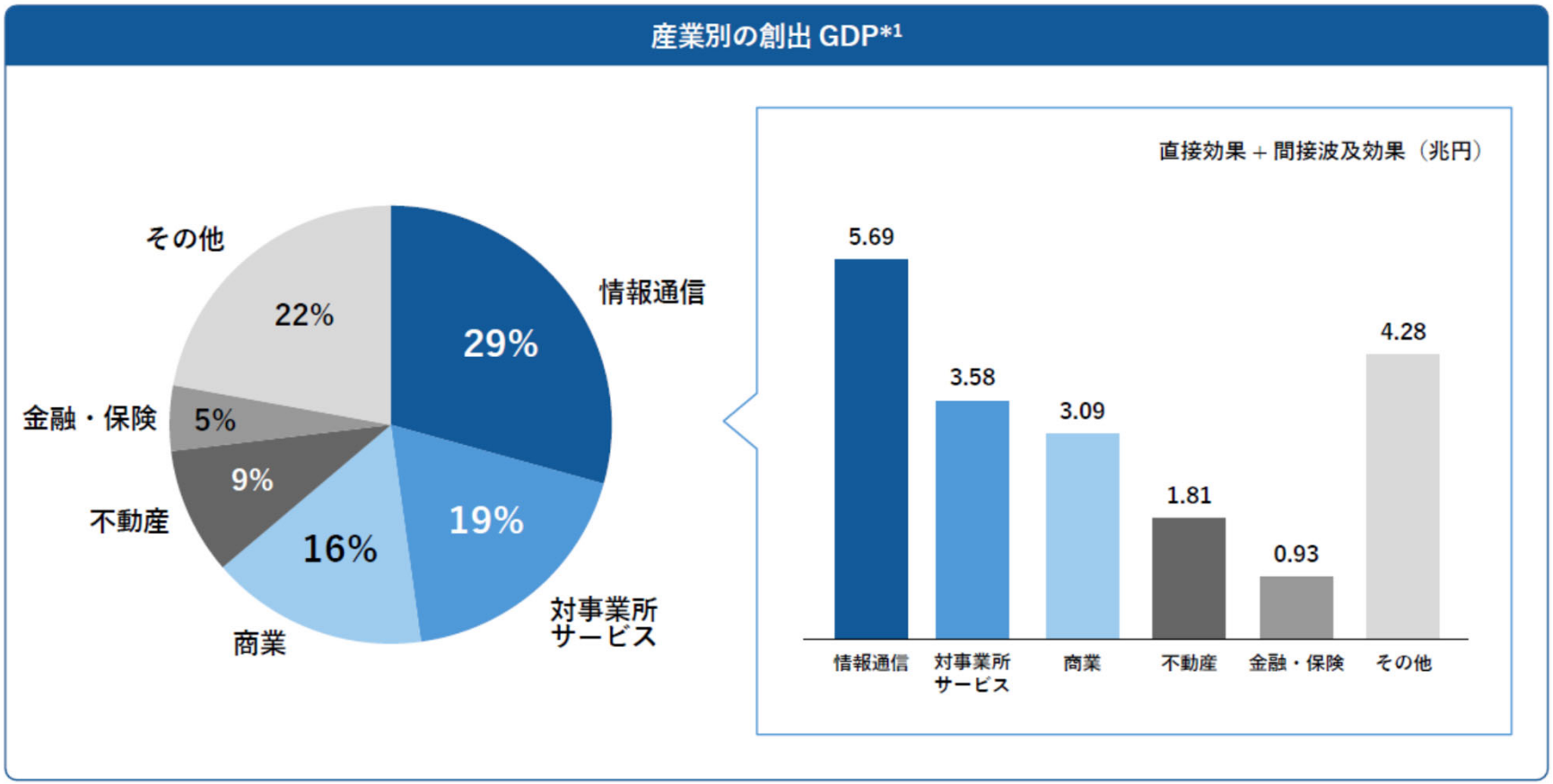
制度の普及・浸透

（参考）登録サービス事業者の所在地の内訳

- **情報セキュリティ監査**（70サービス）　東京51、神奈川8、埼玉1、兵庫2、千葉1、新潟2、京都1、大阪3、広島1
- **脆弱性診断**（138サービス）　東京102、神奈川11、大阪5、兵庫4、新潟2、福岡2、宮城1、茨城1、千葉1、富山2、石川1、徳島1、山口1、岡山1、沖縄2、奈良1
- **デジタルフォレンジック**（39サービス）　東京33、神奈川3、兵庫2、熊本1
- **セキュリティ監視・運用**（52サービス）　東京39、神奈川7、大阪2、兵庫1、福岡1、愛知1、沖縄1
- **機器検証**（14サービス）　東京11、神奈川1、愛知1、沖縄1

スタートアップによる経済波及効果

- 経済産業省が、スタートアップの経済活動及び付随するサプライヤーの経済活動や消費支出に伴う、付加価値の創出による経済効果を推計したもの。
- スタートアップによるGDP創出額は19.39兆円（間接波及効果含む）とされているところ、情報通信分野については、5.69兆円と経済効果が最も大きい。サイバーセキュリティ分野におけるスタートアップ創出を促進することは、マクロ経済面への貢献にもつながり得るのではないか。

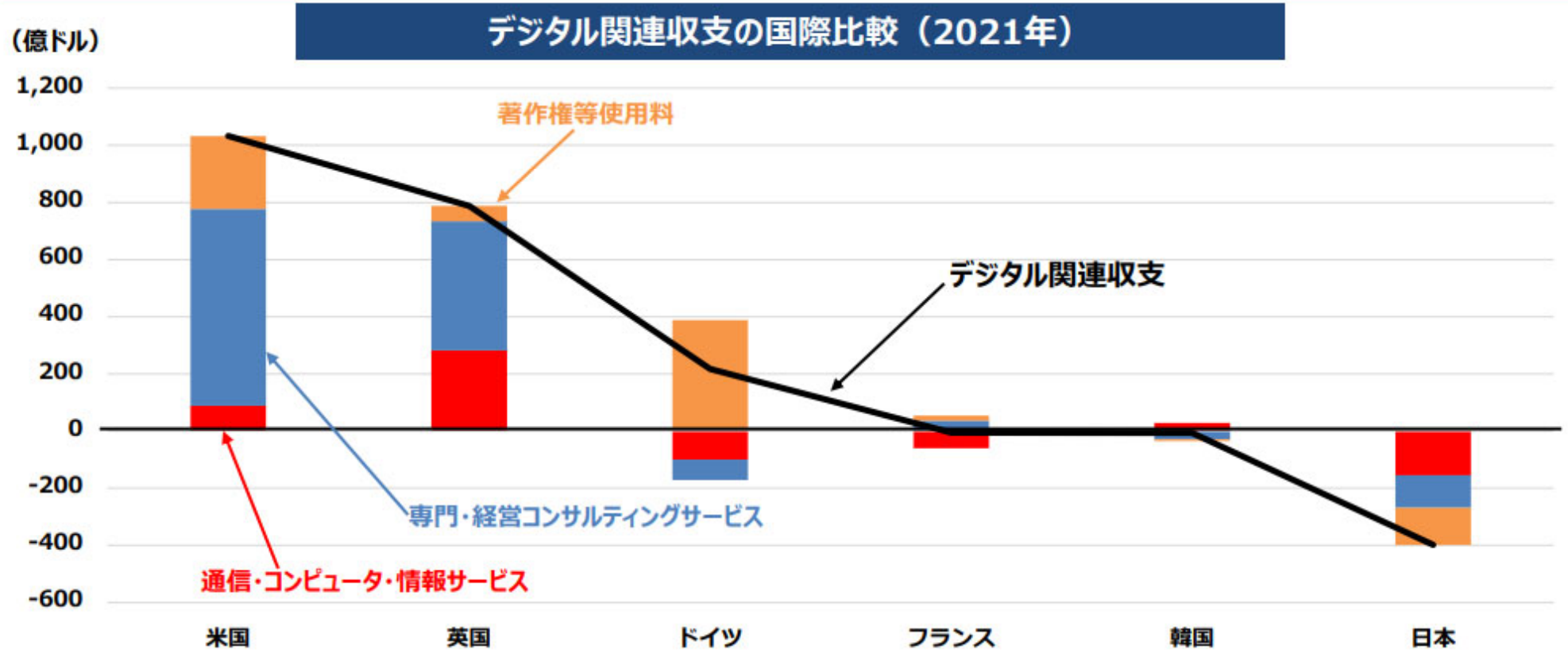


*1. 産業区分は産業連関表の統合大分類（37分類）に従う

（資料）経済産業省「『スタートアップによる経済波及効果』の調査概要」（2024年７月22日）より抜粋・加工

デジタル関連収支の国際比較

- **コンピュータ関連サービスやコンサル費用、著作権等使用料からなるデジタル関連収支での赤字は、日本が突出している。**



（注）デジタル関連収支は、日銀レビューの分類を基に、①～③の合計として算出。
①通信・コンピューター・情報サービス：ソフトウェアの委託開発やクラウド・サービス、オンライン会議システムの利用、ソフトウェアのサブスクリプション契約料等
②専門・経営コンサルティングサービス：法務、会計・経営コンサルティング、広報、広告・市場調査に係る取引
③著作権等使用料：著作物（コンピュータソフトウェア、音楽、映像、キャラクター、文芸、学術、美術等）を複製して頒布（販売、無償配布等）するための使用許諾料（ライセンス料）等。ドイツ、フランスの著作権等使用料は、EUが知的財産権等使用料の内訳を開示していないため、著作権等使用料と産業財産権等使用料の双方を対象として算出。
（出所）BUSSINES INSIDER (2024年４月 みずほ銀行チーフマーケット・エコノミスト唐鎌大輔氏)、日本銀行「国際収支統計」、日銀レビュー「国際収支統計からみたサービス取引のグローバル化」、OECD.statを基に作成

（出典）経済産業省 産業構造審議会　第3次中間整理（2024年6月公表）から引用