経済産業省

サイバーセキュリティ産業振興戦略
～我が国から有望なサイバーセキュリティ製品・サービスが次々に創出されるための包括的な政策パッケージ～

２０２５年３月

経済産業省 商務情報政策局
サイバーセキュリティ課

これまでの議論の整理

2024年7月　第1回検討会（ビジネスの現状、これまでのサイバー産業振興施策の振り返り）

9月　第2回検討会（海外の政策、大手・中小セキュリティ企業の問題意識）

意見募集の開始（約1ヶ月間／25件の意見提出）

10月　第3回検討会（大手SIer・SUセキュリティ企業・業界団体の問題意識、SU施策の紹介）

11月　第4回検討会（研究会・セキュリティベンダーの問題意識、産官学連携施策の紹介）

12月　第5回検討会（産業振興に向けた考え方の提示）

2025年1月　第6回検討会（「産業振興戦略（仮）」の素案提示）

2月　第7回検討会（「サイバーセキュリティ産業振興戦略（案）」の提示）

１．サイバーセキュリティ産業の意義

２．我が国サイバーセキュリティ産業の現状

３．目指すべき方向性と具体的な政策

４．今後のロードマップ

我が国におけるセキュリティ産業の意義

- 企業のセキュリティ対策の必要性・ニーズは足下でも飛躍的に高まっており、現状の政策動向や企業を取り巻く環境を踏まえても、今後さらに高まることが予想される。

- セキュリティ対策を行うにあたっては、自社のみでの実施は難しく、プロダクトやサービスを通じて達成されるため、**セキュリティビジネスの活性化は、我が国のセキュリティ強化のためにも不可欠**。多様なセキュリティ製品・ツールが市場に流通し、企業が自身の知見・ナレッジを基に、適切な製品を選択できる環境が存在することは、**企業が自社のリスクを認識し適切なセキュリティ対策を講じる上で重要**。

- **我が国へのサイバー攻撃の特異性が存在**する場合もあり、国内企業の存在は、国内で必要な脅威情報等の蓄積・分析をしつつ、国内の状況に沿った製品・サービスを提供することが可能となるため**安全保障上も重要**である。

- さらには、**マクロ経済的にもデジタル赤字が拡大**する中、成長市場であるサイバーセキュリティ市場における国内での製品・サービス供給拡大／海外での販路拡大は**赤字解消にも貢献**する。

１．サイバーセキュリティ産業の意義

２．我が国サイバーセキュリティ産業の現状

３．目指すべき方向性と具体的な政策

４．今後のロードマップ

我が国におけるサイバーセキュリティ産業の現状（総論）

- **製品開発・提供／サービス提供の2種類に大別される**。国内で活用されている製品の大部分が、アメリカをはじめとする海外企業が開発・提供したもの。**システムインテグレーター（以下、SI事業者）がこれを輸入し、システム構築にあわせて、海外プロダクトを併せて販売する／サービス提供を行う形態がビジネスモデルの主流となっている**。

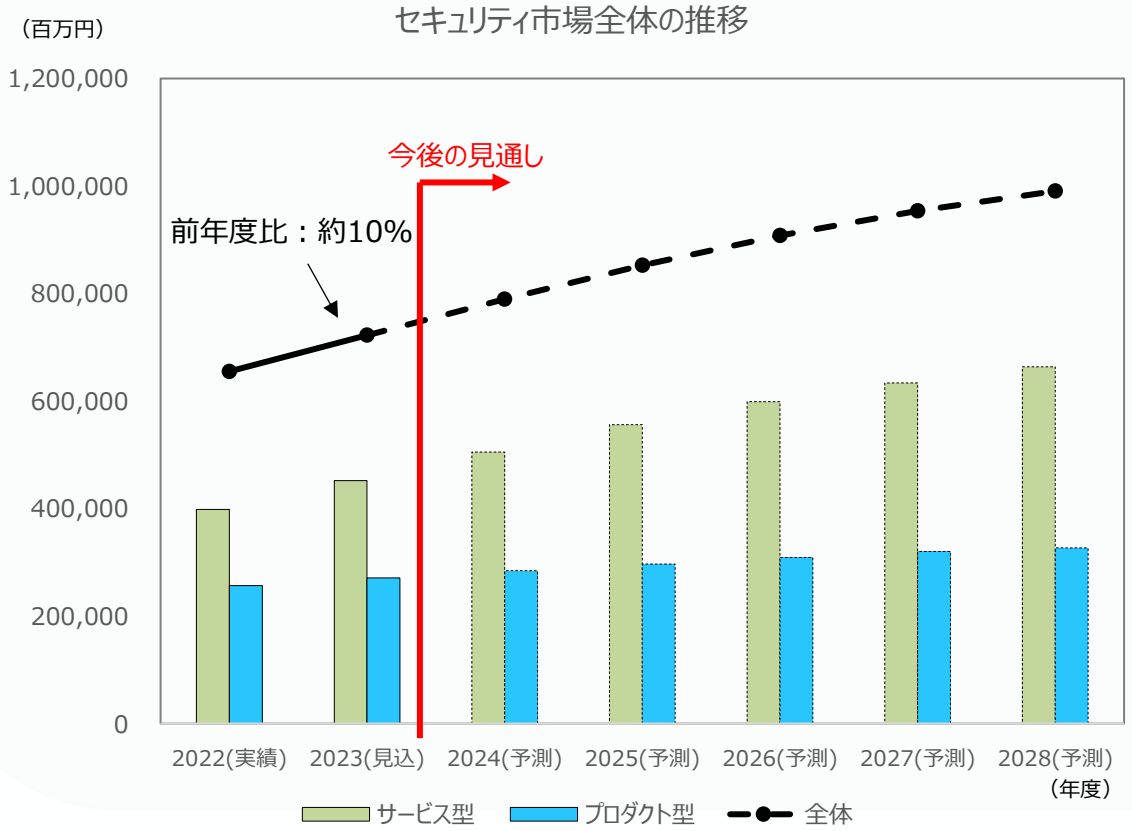
- こうしたビジネスモデルの下、**ユーザ企業は、SI事業者が提示する製品を基に、セキュリティに関する製品・サービスを選択**している状態。**選択基準**も、自社のリスクを踏まえて適切な機能や先端的な技術を持つものではなく、**これまでの利用実績（特に、政府機関や大手企業）や価格が重視されているのが現状**。

- こうした中で、**新興企業の製品**はユーザ企業にとって活用意欲が乏しいものであり、**新規参入のハードルが高い傾向が続いている**。また、**販路開拓**にあたっては、**SI事業者による寄与が大きい**が、活用実績のない新規製品は企業からのニーズが乏しいことからSI事業者からの関心も低く取り扱わず、結果として**販路を拡大することができず、事業スケールも小規模にとどまっていた**（潜在力の高いスタートアップを選定する「J-Startup」においても、セキュリティ企業は数社程度しか存在しない状態）。

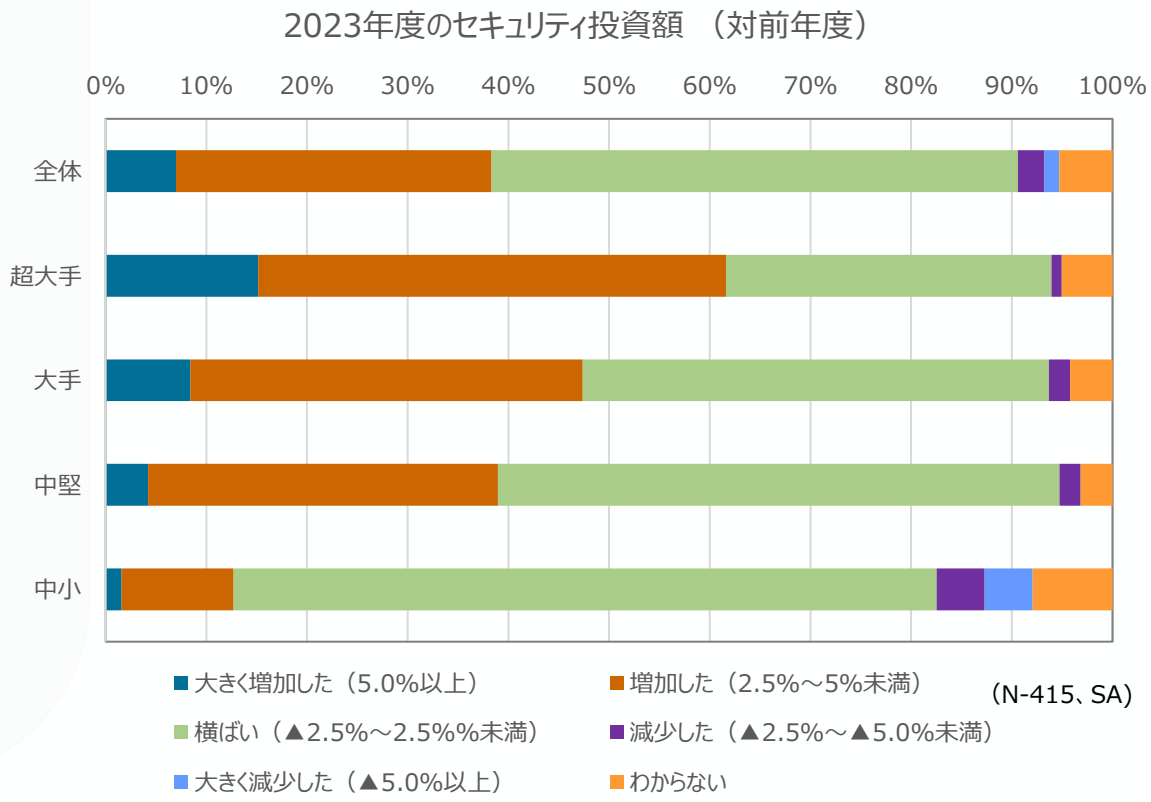
- 販路開拓・事業拡大にハードルが存在する状況下では、新興企業や新規製品・サービスを手がける企業の財務基盤が不安定なものとなり、**事業拡大に対する継続的な投資やそれに伴う製品・サービスの競争力の強化／安定的なビジネスモデルの構築を妨げている**おそれがある。

サイバーセキュリティ市場全体の現状（市場規模や投資額）

- **サイバーセキュリティ産業のマーケットは足下では拡大傾向にあり**、今後も成長していくことが予測される。特に、**大企業においてはセキュリティに関する投資や製品・サービス活用が活発化している**。
- 政府としても、ソフトウェアやIoT製品、サプライチェーンセキュリティに関する政策（例：認証制度、各種ガイドライン）等、様々な政策を講じており、**今後産業界においてセキュリティ対策をさらに進める必要性やニーズは高まる**ことが予想される。仮に**国内のサプライヤーによる製品・サービスが十分供給されなければ、企業のセキュリティ対策が滞る事態が発生する恐れ**。また、**海外製品・サービスが市場を席巻し、国内事業者の参入を妨げる恐れ**も考えられる。



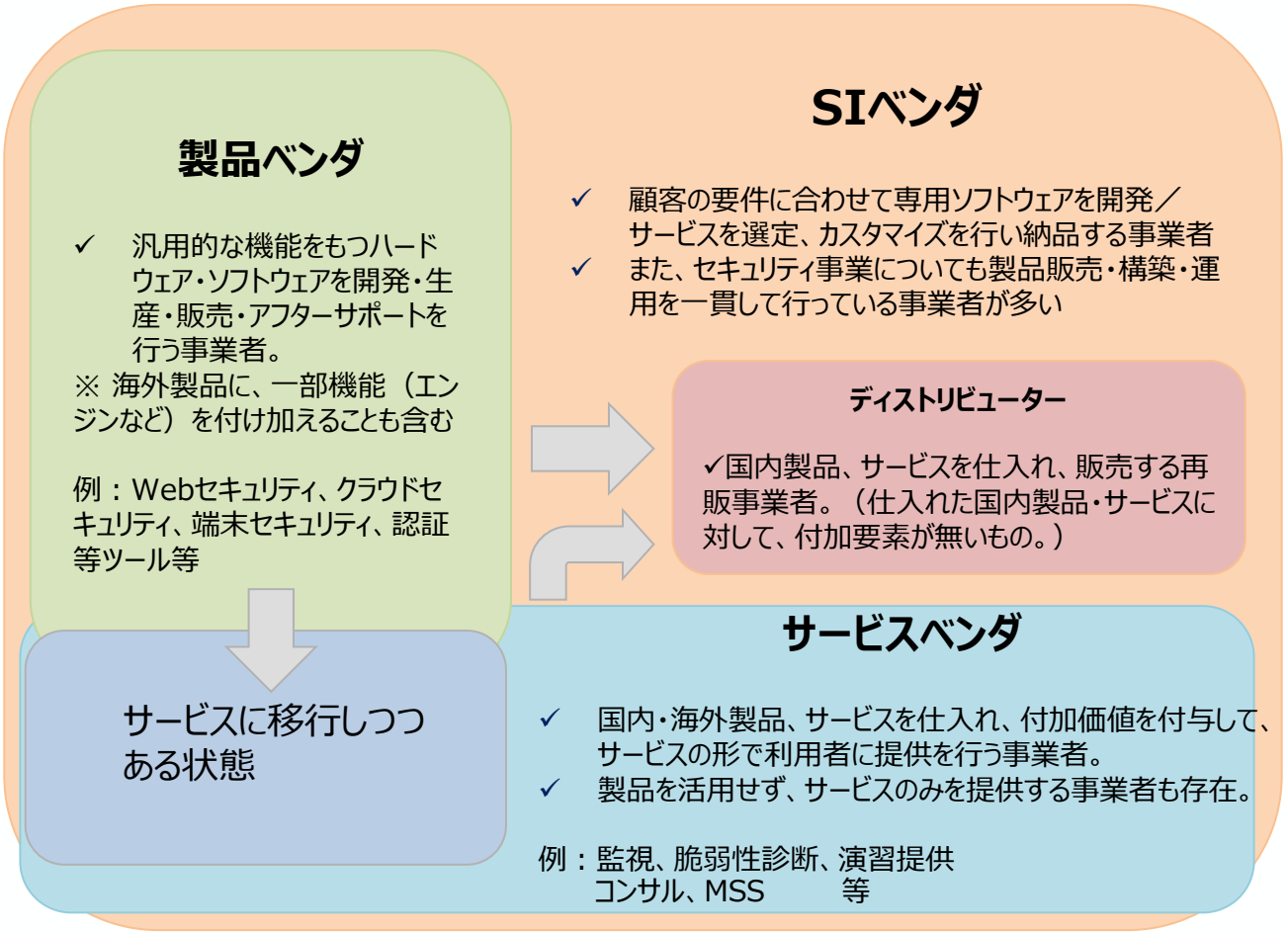
（参考）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈市場編〉」より一部加工



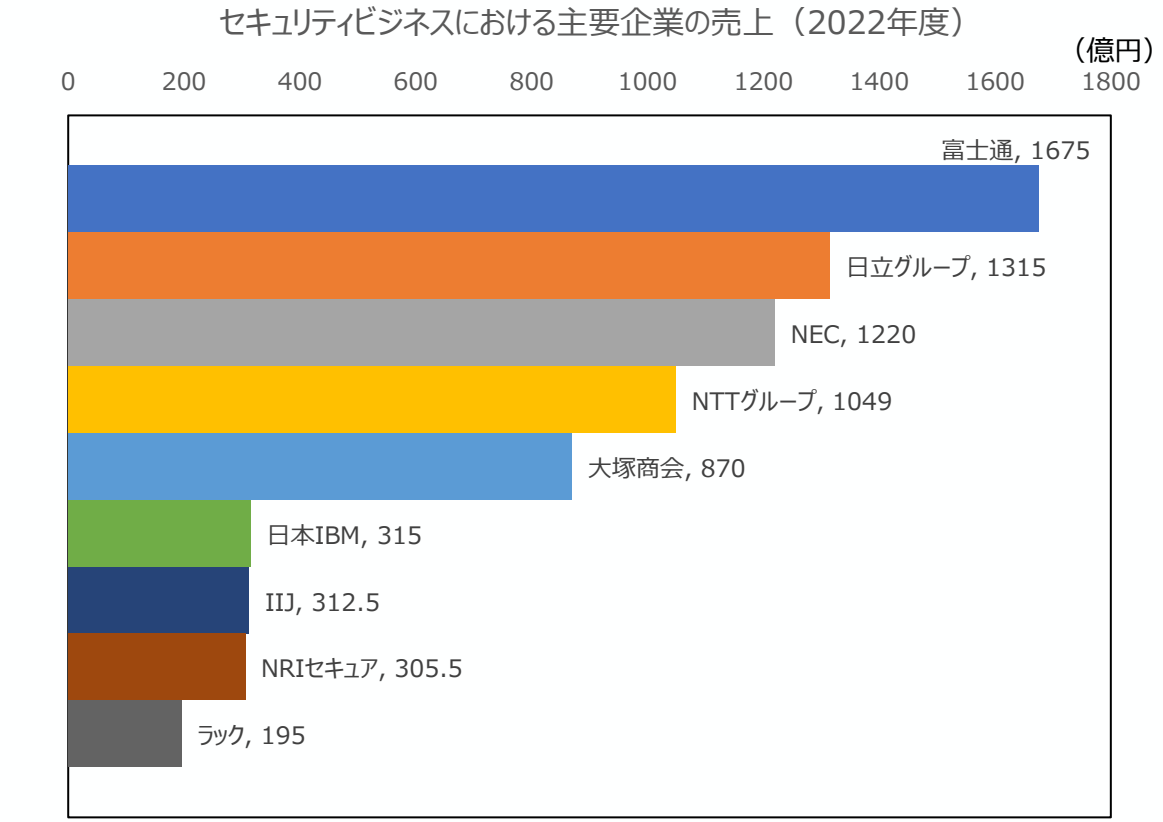
（参考）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈ベンダー戦略編〉〈アンケート調査結果〉」より一部加工

サプライサイドの現状①

- セキュリティビジネスを俯瞰すると、大きく分けて①**製品ベンダー**②**サービスベンダー**に整理されるが、**我が国においてはSIベンダーがシステム構築とあわせて、セキュリティビジネスを提供している構造**（**大手SIベンダー数社がセキュリティビジネスの売上の太宗を占めている**）。
- SIベンダーは、**海外からセキュリティソフトウェアを仕入れ、（製品も活用しつつ）サービスを提供するディストリビューター／サービスベンダーの側面が強い**。



（参考）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈ベンダー戦略編〉」より一部加工



（参考）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈ベンダー戦略編〉〈ポジション別動向〉」より一部加工

（参考）セキュリティ製品・サービスの分類

分類	特徴	具体例
ゲートウェイセキュリティ	不正侵入やウイルスなどの脅威からシステムを保護	✓ ウイルス対策ツール(ゲートウェイ) ✓ セキュリティ監視ツール ✓ 標的型攻撃対策ツール(ゲートウェイ) ✓ ファイアウォール/VPN アプライアンス/UTM ✓ SSL-VPN アプライアンス ✓ 標的型攻撃対策ツール(ゲートウェイ) ✓ ウイルス監視サービス ✓ 統合セキュリティ監視サービス ✓ 不正アクセス監視サービス
メールセキュリティ	メールの送受信時に発生するセキュリティリスク（なりすましメールやメールアドレス乗っ取り、メール添付等の攻撃）を制御	✓ 電子メールアーカイブツール ✓ メール暗号化/メール誤送信対策ツール ✓ メールフィルタリングツール ✓ メールセキュリティサービス
クラウド／Web アクセスセキュリティ	クラウド環境特有のリスクに対してセキュリティ対策を実施	✓ CASB ✓ IDaaS ✓ Web セキュリティツール ✓ Web フィルタリングツール
Web セキュリティ	ユーザーが悪意のあるWebサイトからマルウェアやその他の脅威をネットワークに持ち込むことを防御	✓ CSPM/CWPP ✓ DDoS 攻撃対策ツール ✓ WAF ✓ Web アプリケーション脆弱性検査ツール ✓ DDoD攻撃対策サービス ✓ WAF運用管理サービス ✓ Webアプリケーション脆弱性検査サービス ✓ モバイルアプリ検査サービス
アクセス・認証	WEBサイトのログイン、PCのログインなどで広く使われている認証方式（電子証明書や個人の身体的特徴を用いて認証）	✓ デバイス認証ツール ✓ 統合 ID 管理ツール ✓ 特権 ID 管理ツール ✓ 静脈認証 ✓ 指紋認証 ✓ ワンタイムパスワード ✓ 認証デバイス ✓ プライベートCA ✓ 電子認証サービス

（参考）経済産業省（富士キメラ総研提出「令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（国内セキュリティ関連市場における製品・サービス提供者及び機器検証事業者に関する実態調査） 調査報告書」より一部加工）

（参考）セキュリティ製品・サービスの分類

分類	特徴	具体例
端末セキュリティ	端末を監視して、マルウェアの検知や不正なプログラムの実行防止、デバイスの隔離等を実施	✓ 標的型攻撃対策ツール(エンドポイント／ゲートウェイ) ✓ ウイルス対策ツール ✓ DaaS ✓ EDR ✓ MDM・EMM ツール ✓ 統合エンドポイント管理ツール ✓ 端末ログ管理ツール ✓ 持ち出し制御ツール ✓ EDR運用支援サービス
サイバーレジリエンス／教育／その他	サイバー攻撃の被害が発生しても、抵抗力や回復力を高めることで、事業継続を可能にする取組や社内でのセキュリティ教育を提供するサービス	✓ XDR ✓ SIM ✓ SIEM ✓ プラットフォーム検査ツール ✓ NDR ✓ 検疫ツール（不正接続防止ツール／PC検疫ツール） ✓ サイバーセキュリティ演習サービス ✓ セキュリティ／BCPコンサルティングサービス ✓ セキュリティ教育・トレーニングサービス ✓ セキュリティ検査・監査サービス ✓ セキュリティスコアリングサービス ✓ インシデントレスポンスサービス ✓ スレットインテリジェンスサービス

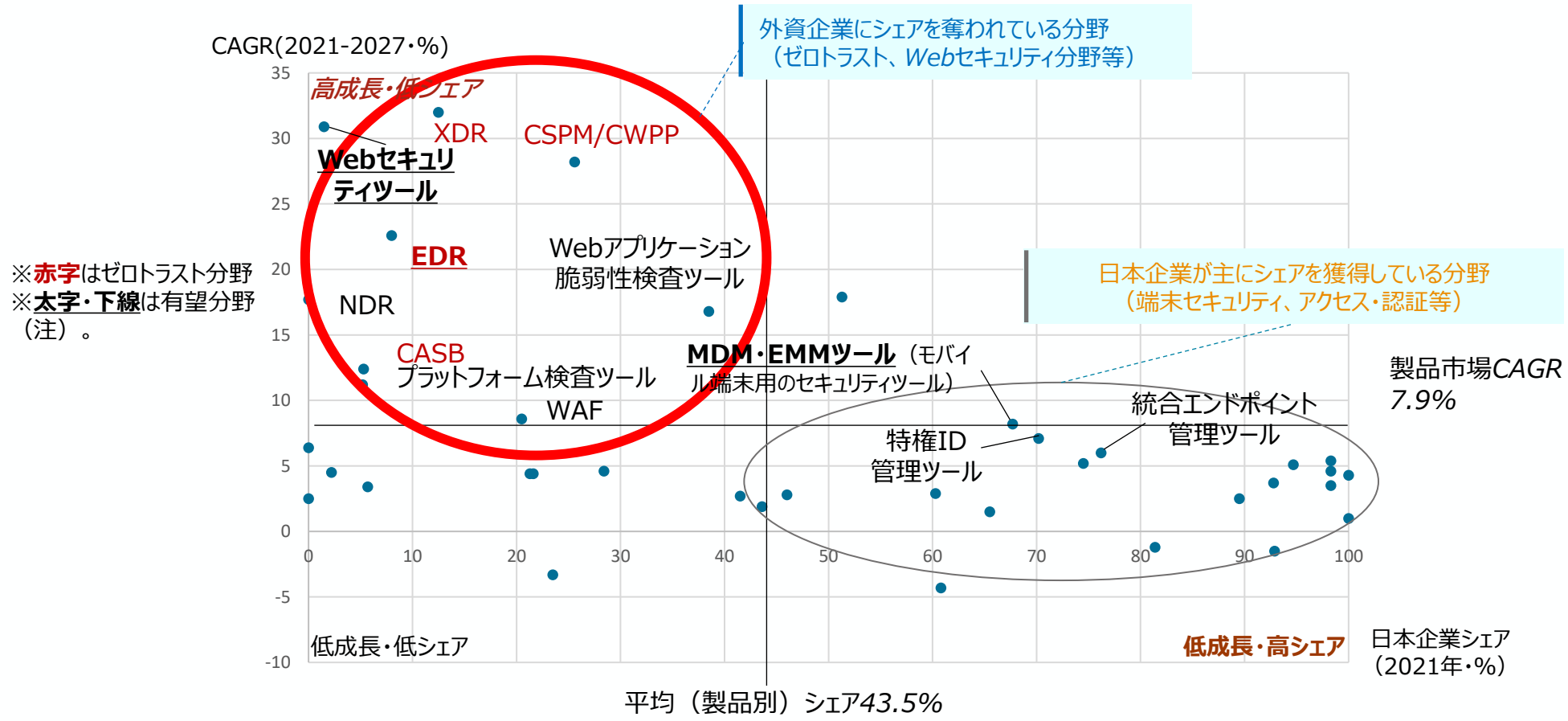
（参考）経済産業省（富士キメラ総研提出「令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（国内セキュリティ関連市場における製品・サービス提供者及び機器検証事業者に関する実態調査） 調査報告書」より一部加工）

サプライサイドの現状②

- **<u>市場規模・成長率ともに大きい有望分野</u>**（例：ゼロトラスト分野やWebセキュリティ分野）（※）の製品については、**<u>その多くで外資企業にシェアを奪われている</u>**。

（※）具体的に、2021年時点で分野別平均以上の市場規模100億円以上でかつ、製品市場全体の年平均成長率約8%以上分野

製品分野別の年平均成長率及び日本企業のシェア



（参考）経済産業省（富士キメラ総研提出「令和４年度サプライチェーン・サイバーセキュリティ対策促進事業（国内セキュリティ関連市場における製品・サービス提供者及び機器検証事業者に関する実態調査） 調査報告書」を元に作成）

サプライサイドの現状③

➢ セキュリティ製品については、攻撃に対する防護性能や誤検知・誤作動を起こさない等の観点から製品性能を評価することができるが、海外の独立機関による性能テストを踏まえると、**我が国の製品は、他国製品と比較して圧倒的に優位な性能を持つとは言えない**結果。

日本製品を含むセキュリティ製品の性能比較

独立テスト機関の視点

※オーストリアの独立製品テスト機関AV-Comperativeでは、購買者に対して、製品選定で５つの視点を提示している。

製品の性能関連	1	防護性能	• マルウェア等の様々な攻撃への防護性能
	2	誤検知・誤作動	• 誤った正常なアクセスやファイル等をブロックの程度
	3	動作性	• 導入によるPCの動作への影響の程度
サービス関連	4	価格	• アップデートも含めた価格
	5	テクニカルサポート	• テクニカルサポートの充実ぶり

（参考）AV-Comperativeの各種テスト結果を元に作成
https://www.av-test.org/en/antivirus/business-windows-client/
https://www.av-comparatives.org/tests/real-world-protection-test-july-october-2023/
https://www.av-comparatives.org/tests/real-world-protection-test-february-may-2023/

セキュリティ製品に係る性能テスト結果

防護性能

順位	国・企業名	平均点数（６点満点）
１位	チェコA社	6/6
	ルーマニアB社	
	イスラエルC社	
	ロシアD社	
	英国E社	
	米国F社	
	米国G社	
８位	米国H社	**5.9/6**
	日本I社	
	フィンランドJ社	
11位	韓国K社	5.5/6
	インドL社	

注１：オーストリアの機関AV-Comperativeが実施したマルウェアの攻撃について検証した2023年中の５回のテスト結果（OSはWindows11）の平均点数
注２：同一順位の企業については、実際の企業名のアルファベット順

誤検知・誤作動

※スコアが高いほど誤作動

順位	国・企業名	平均スコア
１位	スロバキアA社	0.5
２位	ロシアB社	1
３位	米国C社	2
４位	ルーマニアD社	2.5
	米国E社	2.5
６位	インドF社	3.75
７位	チェコG社	4
	チェコH社	4
８位	英国I社	4.5
９位	ドイツJ社	5
１０位	米国K社	6.5
１１位	ドイツL社	7.5
１２位	米国M社	14.25
１３位	フィンランドN社	18.5
１４位	スペインO社	23.75
１５位	**日本P社**	**39**

注１：オーストリアの機関AV-Comperativeが2023年に実施した検証テスト２回の平均。

サプライサイドの現状④

- **日本企業の売上に占める研究開発費は、他国企業と比較すると少ない傾向**。

各国のセキュリティ企業の研究開発額の比較（２０２２年）

国籍/企業	主要製品分野	研究開発費（億円）	売上高に対する研究開発費比率
カナダA社	エンドポイントセキュリティ等	310.5	31.6%
米国B社	エンドポイントセキュリティ等	912	29.0%
イスラエルC社	エンドポイントセキュリティ等	525	17.1%
日本D社	エンドポイントセキュリティ等	54	2.4%
日本E社	脅威検知等	2.6	0.6%
日本F社	エンドポイントセキュリティ等	0.2	0.2%

※SPEEDA上、グローバル市場及び国内市場ので上位にランクインされている企業のうち、損益計算書で研究開発費を公開している企業を掲載。
１ドル150円換算で計算。

出典：経済産業省（PwCコンサルティング合同会社提出「令和5年度度産業サイバーセキュリティ強靭化事業(サイバーセキュリティ産業の振興に関する調査) 調査報告書」）
https://www.meti.go.jp/meti_lib/report/2023FY/000408.pdf

（参考）サイバーセキュリティ関係のスタートアップ①（※）

社名	事業概要	補足
①ソフトウェア・ツールの開発		
FFRIセキュリティ	✓ 攻撃者の攻撃パターンを先読みした先端的な**エンドポイントセキュリティソフトウェア**（「FFRI yarai」）の開発。防衛省等、政府機関において活用。	✓ 経済安全保障重要技術育成プログラム（Kプロ）に参画
Powder Keg Technologies	✓ **AI技術を活用**した**全自動のペネトレーションテストツール**（「MUSHIKAGO」）の開発。ユーザーのコスト工数が低減。	✓ JETRO・内閣府・経産省によるスタートアップシティ・アクセラレーションプログラムに採択 ✓ 経済安全保障重要技術育成プログラム（Kプロ）に参画
エーアイセキュリティラボ	✓ **AI技術を活用**した**脆弱性診断ツール**「AeyeScan」の開発・提供。ユーザー企業のセキュリティ対策コスト（費用・時間・工数）が低減。	✓ 経産省・IPAによる有効性検証事業に参加 ✓ 日本サイバーセキュリティファンドに参画
SCU	✓ 通常の暗号に追加機能を加えた技術（**高機能暗号**）を、**IoT等を対象に実装。**	✓ 戦略的イノベーション創造プログラム（SIP）に参画（当時技組、のちに株式会社化）

（※）経産省関連の事業に関与している事業者を中心に抜粋。

（参考）サイバーセキュリティ関係のスタートアップ②

社名	事業概要	補足
②サービス提供		
リチェルカセキュリティ	✓ **最先端のオフェンシブセキュリティ技術**を持つ技術者による**脆弱性診断、研究開発、各種コンサルティング**の提供 （例）海外のセキュリティコンテストの上位入賞者、多数の脆弱性発見者 等	✓ 経済安全保障重要技術育成プログラム（Kプロ）に参画
セカフィー	✓ **ハードウェア（電子機器）のセキュリティ解析**、技術コンサルティング（神戸大学発のベンチャー企業）	✓ 経済安全保障重要技術育成プログラム（Kプロ）に参画
ゼロゼロワン	✓ IoT機器の検索エンジンの提供及びIoT機器の解析・車載ECUのセキュリティ評価等コンサルティングサービス、**IoT機器のセキュリティ評価、SBOM作成等を行うソフトウェアの提供**	✓ 経産省・IPAによる有効性検証事業に参加 ✓ 総務省・NICT等によるNOTICEにてファームウェア解析を実施

（参考）産業界における取組

【事例①】セキュリティ企業等によるファンドの立ち上げ

- ✓ 昨年4月、グローバルセキュリティエキスパート、兼松、兼松エレクトロニクス、ウエルインベストメントの4社で**セキュリティ企業のみに投資するファンド(日本セキュリティファンド)を立ち上げた**（※）。
- ✓ **投資先の成長ステージを問わず、幅広く国内のセキュリティ企業に対して投資を行う**とともに、**中堅・中小企業にも使いやすいサービスと商品の開発や販売を後押し**する狙い。

（※）昨年9月時点で13社が参画。

【事例②】セキュリティスタートアップによる技術連携

- ✓ 昨年12月、**国内のセキュリティスタートアップ6社**（※）が、「**トラストセキュリティコンソーシアム**」を設立し、**技術・サービスの開発や国産製品の普及、市場の活性化を目指す**旨を公表した。
- ✓ 2025年初めにも各企業の技術を連携させた新サービスの開発を進めるとともに、各社の研究やテストのためのデータ基盤の構築も目指す。

（※）構成企業は、ZenmuTech、アンカーズ、イニシャル・ポイント、炎重工、ロジック・アンド・デザイン等の6社。加えて、IPAからも登サイバー技術研究室長が参画。

（出典）各種公開情報・報道より作成。

（参考）各国におけるサイバーセキュリティ産業の振興に向けた政策

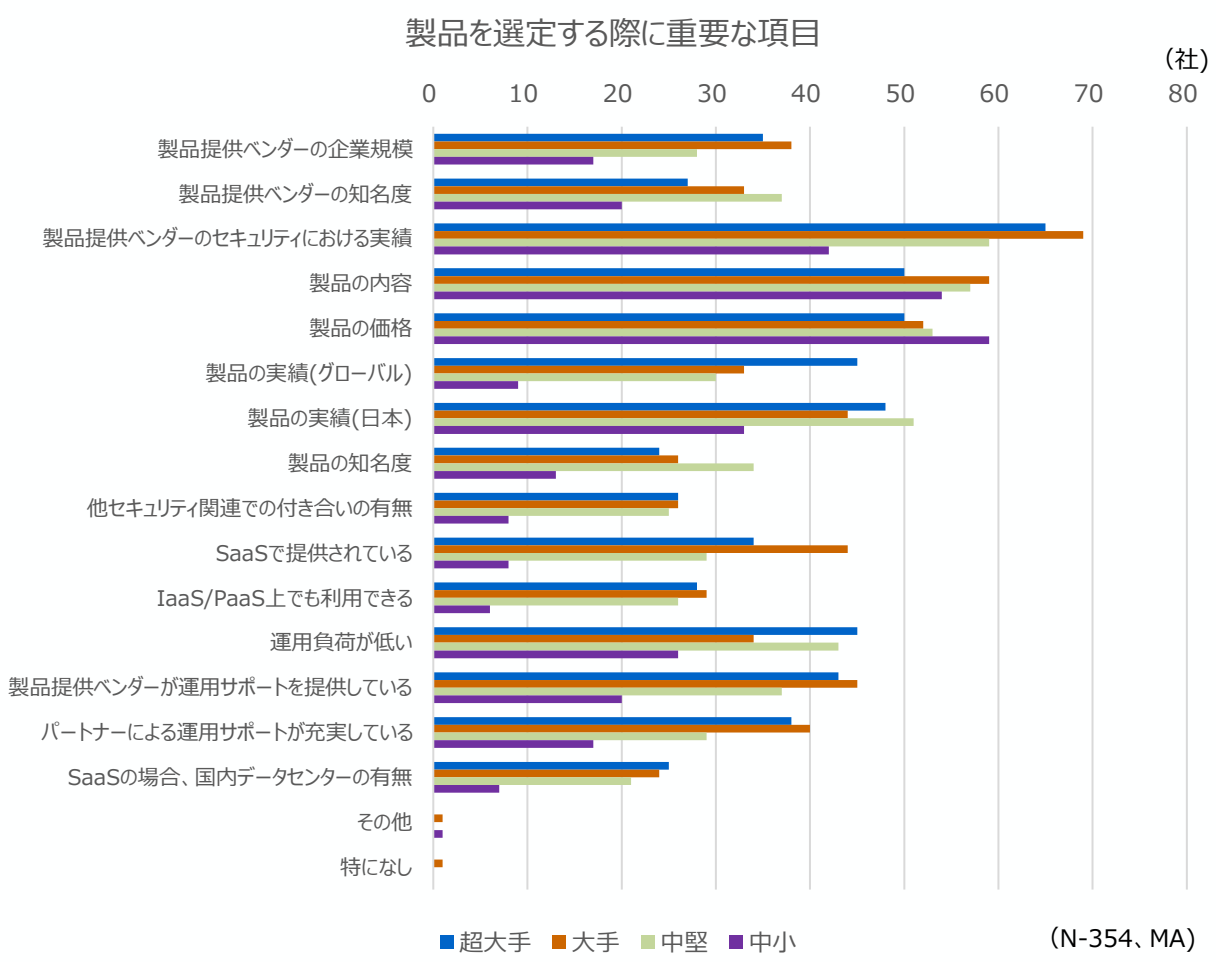
➢ 主要国では、自国内/域内のサイバーセキュリティ産業の国際競争力の強化を図っており、AI、IoT、暗号化、量子コンピューティングなどの次世代主要技術へのサイバーセキュリティ統合、研究開発支援や国外の新市場への進出支援等の各種施策を講じている。

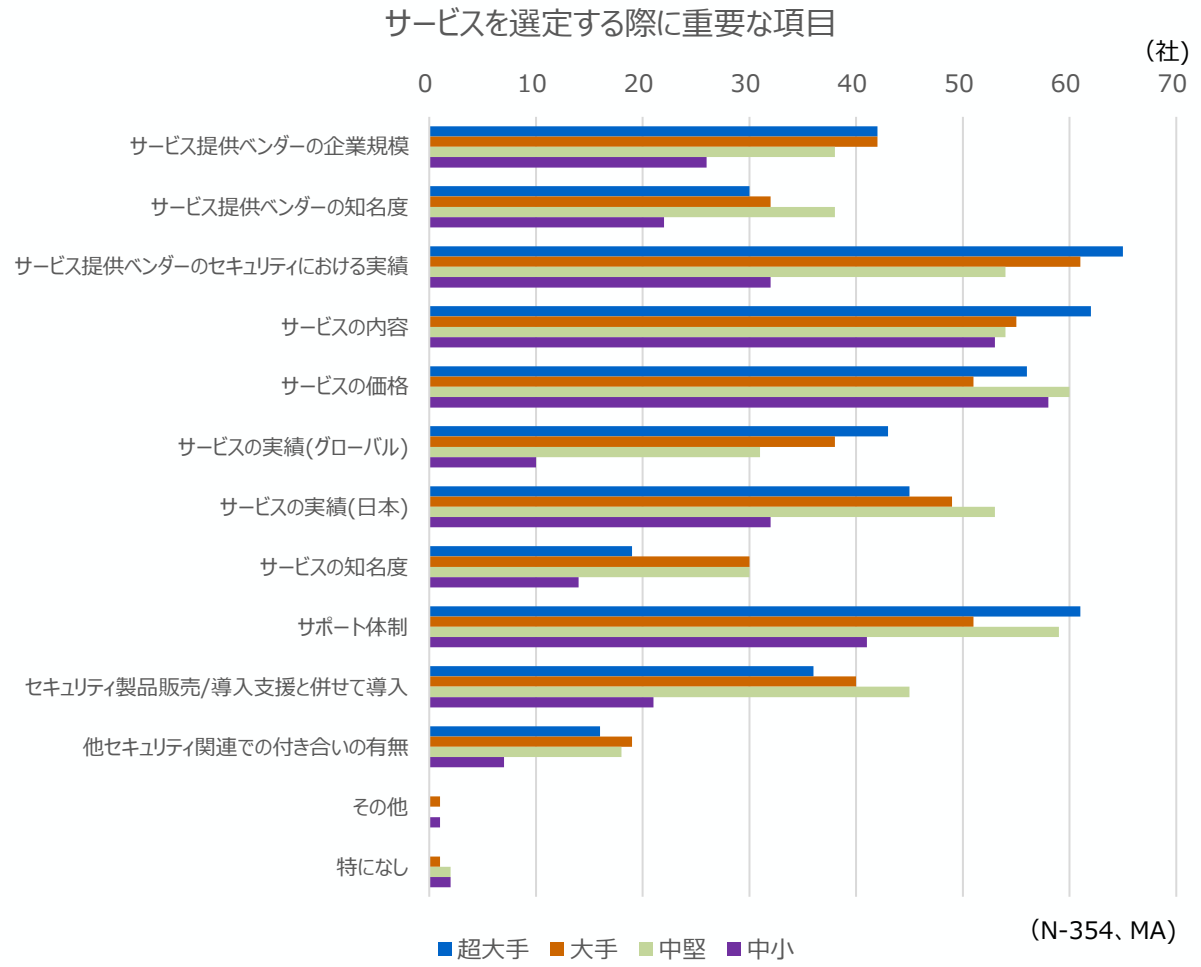
各国のサイバーセキュリティ産業振興に関する取組 （概要）	
米国 	● 2023年3月に米国ホワイトハウスが公表した『 国家サイバーセキュリティ戦略2023 』は、**サイバー空間の安全性を向上させ、未来のデジタル社会において米国が世界をリードする立場を保証する**ために現バイデン政権がとる包括的なアプローチをまとめている。 ➢ サイバーセキュリティ市場推進のため、連邦政府は**購買力と助成金**を提供し、**保険市場の安定化**を検討する。 ➢ 現政権は、デジタル・エコシステムの長期的な安全性・強靭性形成のため、**強力な個人情報保護の立法支援**、**IoT セキュリティ（IoTセキュリティラベリング制度推進）**、**ソフトウェアセキュリティ**（SBOM推進、賠償責任を課す法律策定やセーフハーバーの枠組み開発）、**重要インフラセキュリティ**研究開発等を推進する。 ➢ デジタル・エコシステムのセキュリティ確保のため、既存の投資プログラムを活用する。主なサイバーセキュリティ投資対象として**「暗号」「デジタル ID」「クリーンエネルギーグリッドの安全性」**をあげる。 他
EU 	➢ **『 デジタル10 年に向けた EU サイバーセキュリティ戦略 』にて、今後10年間は、サプライチェーン全体にわたって安全な技術の開発をEUが主導するチャンスである**とともに、サイバーセキュリティにおけるレジリエンスを確保し、 産業と技術の能力を強化するためには、必要な規制、投資、政策の手段をすべて動員すべきとする。 ➢ EUは、今後7年間にわたる EUのデジタル移行への前例のないレベルの投資を行う。特に、人工知能、暗号化、量子コンピューティングのような**主要技術の全てのデジタル投資に、サイバーセキュリティを統合**し、EU 域内のサイバーセキュリティ産業の成長を促進。 ➢ **EU一般データ保護規則**（GDPR：各国企業が「欧州経済領域（EEA: European Economic Area）」内で取得した個人データをEEA外に持ち出すことを禁止した法律）**による実質的なEU域内のIT産業・サイバーセキュリティ産業の保護。**
英国 	➢ 「**国家サイバー戦略2022**」にて、サイバーパワー（＝国益保護・増進をサイバー空間内部およびサイバー空間を通じて実現する能力）の維持・強化の第1の柱として「サイバーエコシステム」の強化を据える。策として官民パートナーシップの構築、人材育成、サイバーセクターの成長促進を掲げる。 ➢ 輸出を含めてサイバーセクターの前年比成長率が世界平均を上回ること、**サイバーソリューションとサイバー専門知識の輸出大国として世界トップ3に立つこと**を目標に掲げ、**国外への新市場への進出支援**や、**各国政府/主要企業への積極的なPR**を行う。
韓国 	➢ 「**国家サイバーセキュリティ戦略**」では、**国家の重要情報インフラ/技術としてのサイバーセキュリティ産業の保護や成長環境の醸成を強調。** ➢ グローバル企業との戦略的パートナーシップの推進や海外拠点の拡充により、**国内セキュリティ産業のグローバル競争力を強化し、グローバル市場への参入を支援する**、と戦略に記載。 ➢ サイバーセキュリティに関する研究開発、人材、認証、輸出促進の支援を行うことで産業の育成を目的とする「サイバーセキュリティ発展法」や、この法律を根拠に設立された韓国のサイバーセキュリティ企業やプロジェクトへの資金援助を行う「サイバーセキュリティ産業開発基金」等の支援がある。
イスラエル 	➢ 「**イスラエル国家サイバー防衛構想**」のコンセプトが、「**イスラエル国際サイバー戦略**」によって補完され、**グローバルサイバーレジリエンスの構築を中核的価値と位置付ける**。サイバーセキュリティの運用面、技術面、産業面での優位性を活かし、増加の一途をたどるサイバーリスクに対して、**共通の価値観と信頼に基づく国際協力の推進、能力構築・信頼醸成、新興技術への備え**の3つの取り組み方針が位置付けられる。 ➢ イスラエルのサイバー産業は、**ハイテクセクターにおける成長の重要な推進力**であり、テクノロジー、経済、国家安全保障、社会、国際協力上の国家的目標に直結するとし、**国家と経済の安全保障のために、サイバーセキュリティ産業を保護する**ための措置を講じている。

出典：経済産業省（PwCコンサルティング合同会社提出「令和5年度度産業サイバーセキュリティ強靭化事業(サイバーセキュリティ産業の振興に関する調査) 調査報告書」）
https://www.meti.go.jp/meti_lib/report/2023FY/000408.pdf

ユーザーサイドの現状（製品・サービスで購入時に重視する項目）

- 超大手～大手では、**グローバルを含めたサービスの実績**を筆頭に、**運用負荷の低さや提供ベンダーによる運用サポート・製品導入支援とあわせたサービス導入を希望**する声が多い傾向にあった（中小企業においては、中堅以上と比較すると、**サービスの内容・価格への重要度が高い**傾向）。





（参考）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈ベンダー戦略編〉」より一部加工

１．サイバーセキュリティ産業の意義

２．我が国サイバーセキュリティ産業の現状

３．目指すべき方向性と具体的な政策

４．今後のロードマップ

我が国セキュリティビジネスの現状認識

- **サイバーセキュリティ産業のマーケットは足下では拡大傾向にあり**、政府としても産業界・政府機関のセキュリティ対策を促進する政策を推し進めることから、今後もマーケットや**ニーズは高まる**ことが予想される。他方で、セキュリティ製品・サービスのマーケットシェアは海外事業者に過半数を占めるなど、我が国事業者の供給能力は高いとは言えない。
- セキュリティ製品・サービス調達の際に、**実績が重視される商慣が存在**しており、**実績のない企業・製品にとっては参入障壁が高い**。そのため、**高度な技術を有する企業や製品であっても販路を拡大することが難しく**、結果的に国産製品を開発する意欲が薄れてしまう。一部、製品開発を行っている事業者も存在するが、販路先も限られているがゆえ、市場の付加価値を新たに獲得するような研究開発や事業展開に向けた取組数は多くない。
- 結果的に、我が国のセキュリティビジネスは、**「買い手がつかないので儲からない」「儲からないので事業開発や投資が十分なされず競争力が低下」という悪循環**に陥っている。

①「売り手」の現状

- ✓ 国内マーケットシェアは海外製品が過半数を占めており、また国産製品の競争力も相対的に高いとは言えない
- ✓ 一部の大手SIerや外資企業を除くと、国内製品・サービスベンダーは小規模な企業が多く、とりわけ製品開発を志向する企業は数自体少ない
- ✓ スタートアップを中心に多くの開発事業者にとって、販路拡大にあたってSIerとの連携が不可欠。

安定的な収益基盤を得ることが難しく、市場の付加価値を新たに獲得するような開発や事業展開が困難

②「買い手」の現状

- ✓ セキュリティ製品・サービスを選択する際に、企業は、大手企業や政府機関による導入実績の有無や価格を基に判断することが大半。
- ✓ 製品やサービス性能を技術的な観点から判断することは一般的な企業にとって困難（結果として、有望な企業・製品・サービスを選択することが難しい）。

製品・サービス調達の際に、実績が重視される商慣が存在しており、企業の新規参入のハードルが高い

③「市場」を取り巻く環境

- ✓ 海外市場への進出等を通じた市場の拡大が重要であるが、企業からは海外進出に対するハードルを指摘する声が存在。
- ✓ 製品を開発するトップ人材等、人材の絶対数が足りていない。また、産官学による連携も重要であるが、十分でない。

産業のエコシステムの構築にあたっては、人材育成や国際連携等の要素も必要であるが、現状の取組としては不十分

今後の成長に向けた課題と今後の方針

- セキュリティ産業が更なる成長を遂げるには、導入実績が重視される／SIerが販路の中心に商慣習を踏まえた上で、新規参入のハードルとなっている点を打破する政策が必要。製品開発の出口を確保しつつ、新たな技術や我が国に強みを持つ分野等でシーズを発掘・事業拡大を後押しすることで、製品ベンダーの競争力を強化し、優れた国産製品・サービスが市場に受け入れられる絵姿を作っていく。

今後の成長に向けた課題

導入実績が重視される商慣習
- 新規製品が販売されても、実績が重視されるため、調達先が存在せず、事業として成り立たないため、企業が育たない

市場の付加価値を獲得しづらい産業構造
- 安定的な収益基盤が見通しづらいため、製品開発・研究開発への投資が限られる
- セキュリティ製品の販売はSIerが商流を担っており、製品ベンダーで対応できる余地は限られている

産業全体を支える基盤の存在
- 人材育成や国際市場の開拓等、産業全体で発展していく上では重要であるものの、個社での対応が難しい要素。これらについても、より一層の政策的な後押しが必要

目指すべき方向性

国産製品・サービスが活用されるための環境整備
- 政府機関による調達を通じた実績作りや有望な企業・製品・サービスを可視化する枠組みを構築し、新規参入のハードルを逓減する

優れた国産製品・サービス創出／SIer等による国産製品/サービス発掘
- 研究開発や販路拡大等に向けた支援を通じて、注力すべき領域を中心に、セキュリティに関する課題解決や技術革新を生み出すシーズを発掘するとともに、その競争力強化を図る
- 商流の中心であるSIerがより国内製品・サービスを取り上げるよう、ベンダーとのマッチングの場を設計する

産業全体を支える基盤の強化
- セキュリティ人材育成に向けた機会提供や国内企業等の海外展開支援に取り組む。

これまでの施策を踏まえて得られた知見

- ✓ 専門家による製品の検証結果の公表だけでなく、大手企業や政府機関の活用実績が、製品の導入促進に直結する
- ✓ 製品ベンダーへの支援のみならず、商流の中心的な存在となっているSIerとの連携が必要
- ✓ 経産省のみならず、様々な知見を持つ関係省庁・機関との連携が必要

サイバーセキュリティ産業振興戦略における取組（※1～3）

①国産製品・サービスが活用されるための環境整備

■スタートアップ等の新しい製品・サービスの実績作り促進

- 政府機関等が有望なセキュリティ製品・サービスの活用機会を提供することで、セキュリティ強化と活用実績のPRを通じた企業の市場参入のハードル逓減を目指す
- サイバーセキュリティ分野の有力スタートアップを一覧化して公表するとともに、政府機関等への情報展開を実施する

■有望な製品・サービス・企業の認知度向上

- 有望な製品やサービス、企業を可視化しマーケット内での活用が進むよう、業界団体とも協働した上で、製品やサービス、企業を審査・表彰を行う方策の検討を進める
- セキュアなIoT製品を認定する制度や、セキュアなソフトウェア開発に関するガイドラインへの適合を評価する制度を含め、製品・サービスのセキュリティや信頼性を確認する制度の構築・運用を進める

②優れた国産製品・サービス創出のための発掘・後押し

■有望な技術力・競争力の強化

- 様々な領域や規模の企業を対象に、サイバーセキュリティに関連する技術・社会課題の解決に貢献する技術・事業を発掘すべく、事業化支援事業を実施する（「コンテスト形式」による懸賞金型事業をイメージ）。
- 特に有望な技術については、研究・製品開発を進める上で必要なデータの提供（※4）や、事業化を進める上での専門人材の派遣等、研究開発・事業化を進めるために必要な環境整備も行う。
- ニーズ省庁・機関からの声も踏まえつつ、成果物がニーズ省庁・機関において有益な活用がなされるよう、経済安全保障重要技術育成プログラムを通じて、技術開発・社会実装を推進する

■ベンダー／SIer間協働のための枠組み構築

- 国産製品・サービスの認知・活用の機会を増やすべく、商流の中心であるSIerとベンダーのマッチングの場を、「コラボレーション・プラットフォーム」の知見や業界団体との協働も踏まえて設計する

③成長の原動力を生む基盤の強化

■セキュリティ人材の育成・確保

- 今後のセキュリティ産業を支える人材（特に製品開発やシステム提供等を担う人材）の質・量を強化すべく、AI等の専門性とセキュリティの知見を兼ね備えた人材の育成プログラムの拡大、知見共有等を目的としたコミュニティを整備する。その上で更なる人材育成のための方策や産官学が連携して人材を育成・環流するための枠組みを検討する

■国際連携の強化

- 市場や技術、標準化の観点を踏まえた上で国際的な競争力を強化するよう、業界団体とも連携しながら各国との連携や産業界への働きかけを行いつつ、既存施策も活用しながら、有望な国産製品・サービスの海外進出を後押し／スタートアップ企業や人材の関係国との交流を図る。

（※1）このほか、既存のスタートアップ政策、政府・大企業等による調達促進施策、関係省庁・機関の取組の浸透・連携強化も実施。
（※2）具体的な取組内容については、業界団体・関係機関等との議論・検討に伴い、変更がありうる点に留意が必要。
（※3）本戦略はサイバーセキュリティ市場の「供給」力の強化に焦点を当てたものであり、別途、経済安全保障政策や各個別産業政策とも連動しながら、産業界・政府機関等に対して必要なセキュリティ対策が進められ、サイバーセキュリティ市場の「需要」の拡大につながるような各種の取組（サプライチェーン対策評価制度、各個別領域におけるガイドライン策定 等）を推進していくことが前提である点にも留意が必要。
（※4）この際、関係省庁・機関（例：NICT CYNEX等）において行われてきた研究開発の成果やこれに付随して整備された環境・ノウハウを最大限活用することにも留意が必要。また、提供に際しては安全保障上の観点から共有範囲などにも留意する必要。

①国産製品・サービスが活用されるための環境整備

スタートアップ等の新しい製品・サービスの実績作り促進

＜政府機関等による有望なセキュリティ製品・サービスの活用機会の提供＞

✓ 政府全体の枠組みとして整備された**「スタートアップ技術提案評価方式」等を活用**しながら、政府関係機関等が有する政策課題を提示の上、最新技術等を活用した解決方法の提案を募集する。その提案をもとに、**政府機関等による製品・サービスの試行的な活用**を行う。

＜シーズの把握＞

✓ 後述する「有望な製品・サービス・企業の認知度向上」に向けた取組や「J-Startup」、その他各種政府関係事業での実績や業界団体からの情報提供等を踏まえ、**有望な製品やサービス、技術を有するスタートアップの情報を集約・リスト化**し、**政府機関やセキュリティ産業の関係者等に適切に提供**する。

◆ 中長期的には、**スタートアップの製品・サービスの試行的な活用を行う政府機関等の主体・取組を拡大**するとともに、**共同開発も視野に入れる**。その際には**有望なスタートアップの情報を集約したリストも活用**する。

有望な製品・サービス・企業の認知度向上

✓ 有望な製品やサービス、企業のマーケット内での活用が進むよう、業界団体とも協働した上で、**有望な製品やサービス、企業を審査・表彰**を行う方策の検討を進め、これを具体化する。

✓ 本年3月に制度が開始される「**IoT製品に対するセキュリティ適合性評価制度**」や、現在経産省のタスクフォースで議論が進められている「**サイバーインフラ事業者に求められる役割等に関するガイドライン**」や「**SSDF（セキュア・ソフトウェア開発フレームワーク）導入ガイダンス**」を活用したセキュアなソフトウェア開発の適合を確認する枠組みを構築し、適切に運用する。

◆ 中長期的には、ニーズを踏まえた上で、上記にとどまらず、**セキュリティビジネスの信頼性を確認する制度の構築・運用**を行う。

②優れた国産製品・サービス創出のための発掘・後押し

有望な技術力・競争力の強化

＜有望な技術・事業の発掘・支援＞

- ✓ 様々な領域や規模の企業を対象に、**サイバーセキュリティに関連する技術・社会課題の解決に貢献する技術・事業を発掘**すべく、**事業化支援事業を実施**する（**「コンテスト形式」による懸賞金型事業**をイメージ）。
- ✓ 特に有望な技術については、例えば**NICT CYNEX等を通じた研究・製品開発を進める上で必要なデータの提供**や、「**中小企業のイノベーション創出を支援するイノベーション・プロデューサー**」等を通じた**事業化に関する専門人材の派遣**等、研究開発・事業化を進めるために必要な環境整備も行う。
- ✓ ニーズ省庁・機関からの声も踏まえつつ、成果物がニーズ省庁・機関において有益な活用がなされるよう、**経済安全保障重要技術育成プログラム（Kプロ）**を通じて、**サイバー空間の状況把握力や防御力の向上等に資する技術開発・社会実装を推進**する。（Kプロ第1弾として「ハイブリッドクラウド利用基盤技術の開発（半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立）」を令和５年６月より、Kプロ第2弾として「先進的サイバー防御機能・分析能力強化」（約300億円）を令和６年７月より、それぞれ実施中。）
- ◆ 中長期的には、**我が国のセキュリティ確保において重要な技術・製品・サービスを特定**し、**その安定供給のために必要な取組を検討**する。

ベンダー／SIer間協働のための枠組み構築

- ✓ 国産製品・サービスの認知・活用の機会を増やすべく、**商流の中心であるSIerとベンダーのマッチングの場**を、独立行政法人情報処理推進機構（IPA）が有する「コラボレーション・プラットフォーム」の知見や業界団体（日本ネットワークセキュリティ協会等）との協働も踏まえて設計する。

③成長の原動力を生む基盤の強化

セキュリティ人材の育成・確保

- ✓ 今後のセキュリティ産業を支える人材（特に製品開発やシステム提供等を担う人材）の質・量を強化すべく、**AI等の専門性とセキュリティの知見を兼ね備えた人材の育成プログラム（「セキュリティ・キャンプ・コネクト」）を開催**するとともに、独創的なアイディア・技術をを活用する人材を発掘・育成する**「未踏事業」との連携を強化**する。あわせて、**知見共有等を目的とした修了生コミュニティを整備**することにより、セキュリティ・キャンプの取組やサイバーセキュリティ人材の価値向上につなげていく。
- ✓ **サイバーセキュリティに関する国家資格**である「**情報処理安全確保支援士（登録セキスペ）**」について、得意分野・専門領域を可視化する**「アクティブ・リスト」の整備**や**各種補助事業等への要件化・指針等への紐付け**、資格維持コスト低減を目的とした**「みなし受講制度」の導入**等の施策を行い、セキュリティ人材の活躍フィールドの拡大やキャリアの魅力向上につなげる。
- ◆ 中長期的には、人材の拡大・活用に向けた**更なる方策**や**産官学連携による人材育成・環流のための枠組み検討**を行う。

国際連携の強化

- ✓ 市場や技術、標準化の観点を踏まえた上で国際的な競争力を強化するよう、業界団体とも連携しながら各国との連携や産業界への働きかけを行いつつ、①国内外の展開支援も含む**「J-Startup」**等を活用した**海外展開支援**、②技術の標準化を通じて新たな市場の創出やユーザーの利便性向上を目指す**標準化活用支援制度**（新市場創造型標準化制度）を通じた**標準化戦略促進**、③様々な機会を通じた**海外政府・企業等に対する情報発信**等、既存施策も活用しながら、**有望な国産製品・サービスの海外進出の後押しや関係国での企業・人材の交流を図る**。
- ◆ 中長期的には、スタートアップによる有望な技術や事業の活用領域を拡大すべく、政府間でも連携しながら**産業界での協力や必要な標準化促進等の取組強化**を目指す。

（参考）活用可能な経済産業省等の支援策

【スタートアップ関連施策全般】

- ✓ 潜在力のある企業への集中投資（例：J-Startup）
- ✓ 事業を支える資金供給拡大（例：ディープテック・スタートアップ支援事業　等）
- ✓ 海外市場への事業展開・ネットワーク構築（例： J-Startup、J-StarX）

【公共調達等を通じた事業拡大】

- ✓ 「デジタルマーケットプレイス」の活用
- ✓ 「防衛産業へのスタートアップ活用に向けた合同推進会」の活用　※推進会開催にあたり、随時業界団体とも連携
- ✓ 「大企業等のスタートアップ連携・調達加速化事業」の活用 ※今後、随時公募を実施

【国際標準に向けた対応】

- ✓ 標準化活用支援制度（新市場創造型標準化制度）の活用
- ✓ 国際ルール形成・市場創造型標準化推進事業費補助金の活用 ※今後、公募を実施

（※）これまでの議論を踏まえ、特に関連性の高い施策を抜粋して掲載。

今後のロードマップ（※1）

- ✓ 製品開発を行っても買い手が存在しない
- ✓ 需要先が存在しないため、製品・サービスベンダーが小規模のまま成長しない／数が少ない

現状

来年度

- ✓ 予算編成過程等を踏まえた上での取組を具体化する
- ✓ 本検討会での議論を通じた、取組の継続的なフォローアップを行う

STEP1
（約3年以内）
【裾野の拡大】

- ✓ 調達機会の拡大を通じて、製品開発・サービス提供を行うことに対するベンダーの期待感を高め、企業数の増加につなげるとともに、政府機関等における有望な企業等の知見を深める（具体的には、J-Startup選定企業をはじめとするスタートアップ数の拡大を図る）
- ✓ 高度なサイバーセキュリティの知見を持つ人材を育成し、その数を増やす（具体的には、プロダクトを開発する「トップガン」人材の増加を図る）

STEP2
（約5年以内）
【競争力の強化】

- ✓ 優れたスタートアップを中心に、シーズの発掘・実用化・事業化促進の後押しを行うことで、企業の競争力を高め、市場でのシェアを高める（例：研究開発・販路拡大 等）（具体的には、市場における我が国企業のマーケットシェア拡大を図る）
- ✓ とりわけ、量子・AIなど、従前のサイバーセキュリティの確保策をdisruptし得る先端的な技術への対応に資する技術の社会実装を進める

STEP3
（約10年以内）
【安全保障・経済政策への貢献】

- ✓ 優れた製品・サービス・企業について、国際市場の開拓や産官学連携を促し、市場や社会的な影響力を強める
- ✓ ユーザー企業にとって、自社の状況やリスクに応じて様々な優れたセキュリティ製品・サービスを選択できる環境を構築し、社会全体のセキュリティ強化を図る
- ✓ 我が国特有の攻撃対応を通じた安全保障・経済安全保障や、企業の海外進出を通じたデジタル赤字解消にも貢献する

【KPI】国内企業の売上高を足下から3倍増を目指す（約0.9兆円⇒約3兆円超）（※2）

（※1）今後、継続的なフォローアップを図る中で、スケジュールや目標の一層の具体化を図っていく。
（※2）富士キメラ総研のデータを基に経済産業省作成。

サイバーセキュリティ産業をとりまく皆様への期待

- 今後、経済産業省を中心に本戦略に沿った政策対応を進めていくが、産業のエコシステムの構築のためには、**民間の主体それぞれ**が本戦略で掲げられた理念を実現するための**取組を自律的に進めていくことも重要**。
- ついては、サイバーセキュリティ産業をとりまく**各主体の皆様に対し、以下の取組を期待**したい。

①政府関係機関

- ✓ **政府全体の取組として進めるべく、本戦略の内容を政府全体の政策文書に反映することを目指す**。
- ✓ **関係機関・関係施策との連携を強化しながら、経済産業省を中心に、本戦略に掲げた施策の具体化・推進を着実に行う**。具体的には、本戦略記載の**各省庁施策**（※1）**の推進・他施策との連動**に加えて、**各施策を活用・対応する政府関係機関の拡大**（※2）を図る。

（※1）NICT CYNEXのデータ提供、デジタル庁のデジタルマーケットプレイス 等

（※2）政府機関等によるスタートアップの製品・サービスの試行的な活用 等

②セキュリティ関係企業（特にスタートアップ企業）

- ✓ **本戦略に掲げる施策を積極的に活用**しながら事業開発・事業拡大を進めていただく。
- ✓ 大手企業については、今後創出・発掘される**有望なスタートアップ等と積極的に連携**いただく。

③SI事業者・ファンド等

- ✓ 今後整理される有望なスタートアップのリストやベンダーとのマッチングの場等も活用しながら、**有望なセキュリティ製品・サービス・企業の発掘**や**事業化等の支援**を積極的に行っていただく。

④ユーザー企業（サイバーセキュリティ対策を実施する主体）

- ✓ 別途政府が実施する**サイバーセキュリティ対策促進に向けた各種の施策を活用**いただきつつ、今後次々に創出される**有望なセキュリティ製品・サービスを実績にとらわれず積極的に活用**いただく。

（参考）詳細資料

１．これまでいただいたご意見の整理

２．各事業概要資料

これまでいただいた御意見の整理

①サイバーセキュリティビジネスの現状認識

②現状認識から見える課題分析

③市場のプレーヤー毎の課題

④セキュリティビジネスの目指すべき方向性

⑤これまでのセキュリティビジネスに対する政策についての評価

⑥後押しすべき主体

⑦課題を踏まえた上での対応

（参考）企業等に求められるセキュリティ対策／それを促す政府のあるべき対応

これまでいただいた御意見（１／１１）

①サイバーセキュリティビジネスの現状認識

【外国製品への依存状況、外国市場におけるスピード感】

•**セキュリティソフトの大半は米国製。**
•情報提供やデータ開示のスピード感が違う。海外ではデータ提供が進めやすい状況にある一方で、日本ではそのプロセスが遅れている。

【供給主体の実績・信頼性への重視】

•セキュリティベンダーが新たな製品やサービスを開発しても、**導入実績がなければ企業の購入まで至ることが難しい**。
•EDR、ウイルス対策ソフト、Firewallなど、**直接的に外からの侵入を防ぐプロダクトについては、新興系のプロダクトが採用されることは難しい**。

【新たな技術・市場の台頭】

•サイバー攻撃の高度化に伴い、**セキュリティ市場は全体的に成長**しており、欧米と同等以上の対応力が求められている。
•クラウド市場の急速な拡大により、セキュリティ環境に変化が生じている。
•海外では、**AIや自動化技術を活用したセキュリティソリューションが注目**されている。
•銀行、クレカ決済など、**顔認証の不正があるが、今これに対応できている事業者は国内にも海外にもいない**のではないか。

【企業によるセキュリティ対策の現状】

•これまで**SIerに知見が集約**しており、**自社でサイバーセキュリティを理解し設計・運用する人材がいない**。
•セキュリティ製品を**導入して放置してしまっている企業が多い**。
•**SIerがユーザー企業のニーズに応じた提案を行うことが難しい**現状がある。
•日本のセキュリティ担当者が**新製品の導入に消極的**であることを懸念。
•ターゲットは大手企業であり、**中小企業は利益が少ないため対象外**としている。
•USトヨタとJPトヨタのセキュリティ**投資の差が40倍**もある。

これまでいただいた御意見（２／１１）

②現状認識から見える課題分析

【外国製品への依存状況、安全保障上のリスク】

•**IaaS等クラウドにおいて海外製品に依存し、その中身がブラックボックスのまま運用せざるを得ない状況が発生**しており、**データ・システム上の地政学リスクを抱えたまま**になってしまっている。

【供給主体の実績・信頼性への重視】

•**セキュリティ事業者にとってはSIerとうまくビジネスができるかが事業の成功要因**。
•今後の成長分野として、**EDRの拡大や新製品サービスの導入が挙げられるが、コストの問題が障壁**となっている。**急激な価格上昇が中小企業に与える影響を懸念**。
•**失敗を恐れる文化が新しい技術の導入を妨げており、労働環境の変化が必要**である。

【新たな技術・市場の台頭】

•**AIの対策は必須。AIを用いた不正行為が増加**している。
•サイバーセキュリティの議論がIoTやサプライチェーンに集中している中で、**アドフラウドという新たな脅威に対する認識が不足**している。
•ランサムウェア対策に焦点が当たっているが、**ID管理などの基盤的な対策が不足**している。
•日本では**共同研究のマインドが不足**していると感じている。

【企業によるセキュリティ対策の現状】

•社会実装が進まない理由として、**企業がセキュリティ対策を後回しにする傾向**がある。これを改善するための施策が必要である。
•**日本では情報漏洩が発生してもその価値低下が過少に評価されている**ため、**企業がセキュリティに投資するインセンティブが不足**している。
•大手企業がサイバー攻撃の危険性を認識していないことを指摘し、企業のセキュリティ対策が不十分。
•**セキュリティと生産性の両立が重要**である。**セキュリティがビジネスとして成立しなければ意味がない**。
•責任をどこの人が負うのか整理が必要。下請けへ押し付けない仕組みが必要。

これまでいただいた御意見（３／１１）

③市場のプレーヤーごとの課題

＜大手SIer＞

依存関係の課題: **SIerが採用しないと製品が広がらず、結果的に海外製品が選ばれる現状がある。**これにより、国産製品の普及が妨げられている。
人材不足: 自社で**サイバーセキュリティを理解し設計・運用する人材が不足しており、SIerに任せることが多い。**これが新しい提案を行いにくくしている。
実績重視の文化: 顧客が製品の**導入実績を重視するため、SIerは新しい提案を行いにくくなっている。**これがイノベーションの阻害要因となっている。

＜セキュリティ製品メーカー＞

海外製品への依存: セキュリティソフトの**大半が米国製であり、国内製品の競争力が低い。**国内製品の開発・普及が求められている。
導入実績の必要性: 新たな製品やサービスを開発しても、**導入実績がなければ企業の購入まで至ることが難しい。**実績作りが必要。
コストの問題: EDRや新製品サービスの**導入がコストの問題で障壁となっており、特に中小企業への影響が懸念**される。

＜セキュリティサービスベンダ＞

運用の課題: セキュリティ**製品を導入して放置してしまっている企業が多く**、アラートに対する迅速な対応ができていない。**運用支援が求められている。**
教育と啓蒙の不足: 顧客がサイバーセキュリティを**自社のビジネス上のリスクと認識する手助けが必要**であり、**セキュリティ文化の醸成が求められている。**
中小ユーザー企業への支援の必要性: 中小企業に対する**セキュリティ対策の働きかけと経済的な支援が必要**であり、**専門家によるサポート体制の整備**が求められている。

＜スタートアップ企業＞

資金調達の難しさ: スタートアップ企業が**官公庁に採用される流れを作ることが重要**であり、資金調達や支援の仕組みが必要。
人材育成の課題: サイバーセキュリティ人材の不足が大きな課題であり、育成プログラムの充実が求められている。
市場参入の障壁: **ISMAPなどの制度がスタートアップの参入を妨げている可能性**があり、規制緩和や**手続きの簡素化**が必要。

＜共通の課題＞

情報共有と連携の不足: **産官学の連携が不足しており、共同研究や情報共有が進んでいない。特に、AIや自動化技術の導入**においては、政府と産業界の連携が重要。
セキュリティ文化の醸成: 日本全体でセキュリティ文化を醸成する必要があり、**ユーザー企業がセキュリティ対策を後回しにする傾向を改善する施策が求められている。**
国際市場への進出: 海外市場への進出が重要であり、特に**アジアやアフリカ市場には大きな可能性**があるが、**法制度や輸出に関する知識不足が障害**となっている。

これまでいただいた御意見（４／１１）

④セキュリティビジネスの目指すべき方向性 （1/2）

【一定分野における国産製品による一定のシェア確保、外国企業との連携】

- **政府・企業のニーズに基づいた製品・サービスを提供**し、**我が国のセキュリティ向上に貢献**。
- 海外製品に依存せず、国内製品によるビジネスができる状態。経済安全保障の観点からも、国内の重要情報や個人情報のデータ越境がなされない状態が望ましい。
- 海外製ソフトに頼らざるを得ないが、**そのソフトを監視するソフトやその枠組みには国内のベンダーも貢献**できるのではないか。
- マーケットドリブンのアプローチは良いが、国産製品の推進にはつながらない。**プラットフォームは勝負がついているので特にOT分野に注目すべき。**
- **日本の特性として、SIerが採用しないと製品が広がらず結果的に海外製品が選ばれる現状。ブレークスルーのためには検証が必要。**
- **ACDは重要。米国では6兆円の市場規模があるとされ、ACDを含めると22兆円に達する可能性があると試算**。**ACDツールのコンテストを省庁で開催することを提案**したい。
- **国内ベンダを選ぶ理由を作るための施策が必要であり、教育やインセンティブ設計を通じて国内産業を育成することが求められている**。

【需要側の価値向上につながる製品・サービスの提供】

- セキュリティベンダーはセキュリティ向上支援にとどまらず、それを通して企業の価値向上につながる製品を積極的に開発すべき。
- **大企業との提携が成功の鍵であり、シェアの確保に繋がった**。
- ウイルス対策ソフトから始まったビジネスが、インターネットゲートウェイ市場の創出や脆弱性対応にまで拡大したことが成功要因。既存の枠にとらわれない柔軟な対応が重要である。

これまでいただいた御意見（５／１１）

④セキュリティビジネスの目指すべき方向性 (2/2)

【安定的・先進的な技術開発環境の確保】

- 安定した技術開発環境を整備し、**セキュリティ関連技術の開発が安定的に行われる**状態。
- **世界に先駆けて先進的な技術を開発・導入**し、安全で信頼性の高いデジタル社会の実例となるべき。

【海外市場での存在感発揮】

- **国際市場でのプレゼンスを確立**し、日本企業が主要なサプライヤーとなる領域を見据えた戦略を策定。
- 当面は国際連携が可能となることを目指し、将来的にはセキュリティサービスの海外輸出も検討すべき。
- **目指すのは「自社開発で安全なインターネットの実現」であり、国際協力活動にも力を入れている。特に、モンゴルなどの途上国では脅威情報の収集が可能**。海外展開にはリスクが伴うものの、知名度向上や新たなビジネスチャンスを得るためには重要。
- **サイバーセキュリティを海外に輸出することが重要であり、ITインフラも併せて輸出する必要がある。特にアジアやアフリカ市場には大きな可能性がある。**
- **過去にはアジア市場への進出を試みたが、法制度や輸出に関する知識不足から断念した。自社製品の優位性を信じつつも、業界全体に海外製品が優れているという偏見があると感じている。**

これまでいただいた御意見（６／１１）

⑤これまでのセキュリティビジネスに対する政策についての評価

【供給主体の信頼性確保策】

- **「情報セキュリティサービス審査登録制度」は事業者の任意であり「規制」の登録制度ではない**。国・地方公共団体の調達ですら、登録は入札参加要件にはなっていないのが実態で、登録のない事業者でも調達が可能。**政府・企業の重要なデータを扱うSOC業務については、「情報セキュリティサービス審査登録制度」からの調達を前提とすべき**。
- セキュリティ産業の振興に向けた制度については、**審査登録制度の最低限の基準を広げることが重要であり、専門人材の基準化や業者に対する認可制度の導入を提案**。これにより、信頼性の高い事業者が市場に参入しやすくなると考えている。
- 既存施策への評価として、**コラプラのようなマッチングイベントよりも、開発支援イベントが重要**。
- **製品評価や検証の支援が有効**であり、CSSCやNICTの活用を提案したいが、敷居が高いのが懸念。過去の検証プロジェクトが評価に至らなかった。**評価者をセキュリティ企業からIPAに出向させるなどの手法も考慮すべき。**
- ISMAPは、スタートアップにとっては重たい。簡略化できる方法を模索する必要がある。
- **ISMAPが海外の大手クラウドベンダーを優遇する仕組みがスタートアップの参入を妨げている可能性がある**ため、議論が必要である。

【供給を担う人材の育成・確保】

- 人材育成に関する施策として、**セキュリティ・キャンプやSecHack365**などの産学官連携によるセキュリティ人材育成プログラムが若年層へのリーチを目的として実施されてきた。**これらのプログラムは一定の成果を上げており、今後も継続すべき**。

これまでいただいた御意見（７／１１）

⑥後押しすべき主体

1. スタートアップ・新興企業

- **革新性の支援**：革新的な技術やサービスを開発する**スタートアップや中小企業を積極的に支援することで、セキュリティ市場の多様性と競争力を高める**。
- **官民連携の強化**：**行政がスタートアップに出向いて共同開発を行う**ことで、実用的な技術の開発を促進し、スタートアップの成長を支援する。
- **失敗を許容する文化: スタートアップが失敗を恐れずに挑戦できる環境を整える**ことで、イノベーションを促進する。
- **国際展開の支援**：**海外進出や上場を目指すスタートアップに対して、必要なツールや支援を提供**し、国際市場での競争力を高める。
- **マーケティングと経営の強化**：**技術に強いスタートアップには、マーケティングや経営に精通した人材を配置**し、ビジネスの成長を加速させる。

2. 増大する需要への対応を行う主体

- **コンサルティング事業者**：顧客がサイバーセキュリティを**自社のビジネス上のリスクと認識する手助けを行い、リスクマネジメントの文化を醸成**する。
- **監査機関**：自社のリスク認識に基づいた**セキュリティ対策の適切性を評価し、企業の信頼性を高める**。
- **運用監視サービスベンダ**：アラートに対する**迅速な対応ができていない企業をサポート**し、**運用の効率化**を図る。
- **トレーニング企業**：サイバーセキュリティに関するトレーニングを提供し、**企業内のセキュリティ意識を向上**させる。

3. 安全保障上の観点から重要性の高い領域の供給主体

- **データ保管企業**：国内での**データ保管を行う企業**は、**情報漏洩やデータ越境のリスクを低減**し、国の安全保障に寄与する。
- **内製化支援企業**：**セキュリティの内製化を進める企業**を支援することで、国防上の重要性を高める。

4. 供給力強化につながる人材育成を行う主体

- **リスクマネジメント文化醸成事業者**：顧客の**リスクマネジメント文化を醸成する施策**を提供し、企業全体のセキュリティ意識を向上させる。
- **トップガン育成事業者**：セキュリティ分野での専門人材を育成し、**業界全体の競争力を強化**する。

これまでいただいた御意見（８／１１）

⑦課題を踏まえた上での対応 (1/2)

１．販路開拓の支援

- **国内外の展示会への出展支援・海外展開方法の明確化**
  展示会への参加は、**企業の認知度を高め、新たな顧客を獲得する機会を提供**する。具体的な方法を示すことで、企業の国際競争力を向上させる。
- **ビジネスマッチングの場の提供**
  大企業とベンチャーキャピタルとのマッチングを通じて、資金調達やパートナーシップの機会を創出し、スタートアップの成長を促進する。
- **ビジネスマッチングやM&Aの機会の支援**
  エンドユーザ企業の意識向上や海外展開の支援が必要であり、これにより市場の活性化を図る。

2. 資金的な支援

- **サイバーセキュリティ分野のスタートアップに対する補助金・低利融資制度の創設**
  資金調達のハードルを下げ、スタートアップが成長するための基盤を提供する。
- **官民ファンドを通じた資金提供**
  初期段階での資金調達支援により、スタートアップの成長を加速させる。
- **政府調達における優遇**
  スタートアップのプロダクトを優遇することで、**公共セクターへの参入を促進し、安定した収益源を確保**する。
- **研究開発税制の拡充**
  企業が新技術の開発に投資しやすくすることで、イノベーションを促進する。

3. 技術開発に係る支援

- **技術開発のためのテスト環境**
  新技術の実証実験を行う場を提供し、製品の市場投入をスムーズにする。
- **規制緩和や手続きの簡素化**
  新技術の開発・導入を促進し、企業が迅速に市場に対応できるようにする。
- **産学官共同プロジェクトの推進**
  技術開発と人材育成を同時に進めることで、持続可能な成長を実現する。
- **AIとセキュリティの統合**
  新たな価値創造を目指し、**AI技術を活用したセキュリティソリューションの開発を促進**する。

これまでいただいた御意見（９／１１）

⑦課題を踏まえた上での対応 (2/2)

4. 供給主体間の公正な競争環境整備・競争促進

- **市場淘汰の促進**
  セキュリティ対策が不十分な製品やサービスを市場から排除することで、全体の品質を向上させる。
- **競争環境の調査と改善**
  競争阻害要因を取り除くことで、公正な競争を促進し、業界全体の成長を支援する。
- **マーケティング活動に関する倫理指針の策定**
  過度な脅威の煽りを抑制し、消費者の信頼を高めることで、健全な市場環境を構築する。

5. 人材育成・確保に係る支援

- **サイバーセキュリティ人材の充足**
  人材育成プログラムの充実を図り、業界全体の人材不足を解消する。
- **人材育成のための支援**
  新製品やサービスを評価できる人材の育成を支援し、業界の専門性を高める。
- **新製品・サービスの導入を図る外部人材の活用**
  新製品・サービスの導入を促進し、企業の競争力を向上させる。
- **人材流動性の向上**
  大学と産業界の連携を強化し、応用研究の進展を促進する。

これまでいただいた御意見（１０／１１）

（参考）企業等に求められるセキュリティ対策／それを促す政府のあるべき対応(1/2)

企業に求められる対策

１．セキュリティの取組の強化
製品の導入後に適切に運用され、**社内でセキュリティカルチャーが醸成されている状態を目指す**。

２．リスク認識の適切化
自社のリスク認識を見直し、**適切なセキュリティ対策を運用レベルで実施**する。

３．セキュリティポリシーの策定
中小企業はセキュリティポリシーを策定し、全従業員に対してセキュリティ教育を実施する。

４．取引先のレベルアップ
調達要件にセキュリティ基準を組み込むことで、取引先や業界全体の底上げを図る。

５．サプライチェーンの責任を理解
企業間のつながりを意識し、**集団的なリスクを引き受ける仕組みを構築**する。

６．セキュリティスコアリング制度の導入
自社のセキュリティ状況を評価し、改善点を明確にする。

７．持続的な競争力強化
セキュリティ対策を一時的な脅威対応ではなく、企業の持続的な競争力強化につながる**戦略的投資として位置づけ**る。

８．従業員への教育
セキュリティポリシーを分かりやすくし、全員に周知できる手法を確立する。

これまでいただいた御意見（１１／１１）

（参考）企業等に求められるセキュリティ対策／それを促す政府のあるべき対応(2/2)

政府のあるべき対応

１．強制力の確保
民間企業へのセキュリティ取組に対する**一定の強制力を確保する**。

２．経済的支援の提供
中小企業に対するセキュリティ対策の働きかけと経済的な支援、**専門家によるサポート体制の整備**を行う。

３．監査制度の導入
監査費用や**セキュリティ基準準拠のための助成・税制優遇を提供**し、企業のセキュリティ対策を促進する。

４．セキュリティ指針の策定
セキュリティ**指針と対応事項を明確化**し、**官から民への具体的な対応基準を策定**する。

５．情報連携の強化
官民連携での情報連携を進め、共通的なセキュリティ対策を提供する。

６．セキュリティの「あるべき姿」の定義
政府が**セキュリティの「あるべき姿」を明確に定義**し、業種・規模別のセキュリティベストプラクティスを策定・公表する。

７．サプライチェーンの支援
大企業が**中小企業をモチベートするための支援**を行い、サプライチェーン全体のセキュリティを強化する。

８．一般消費者に対する啓発
エンドユーザーである一般消費者に対する教育プログラムを実施する。

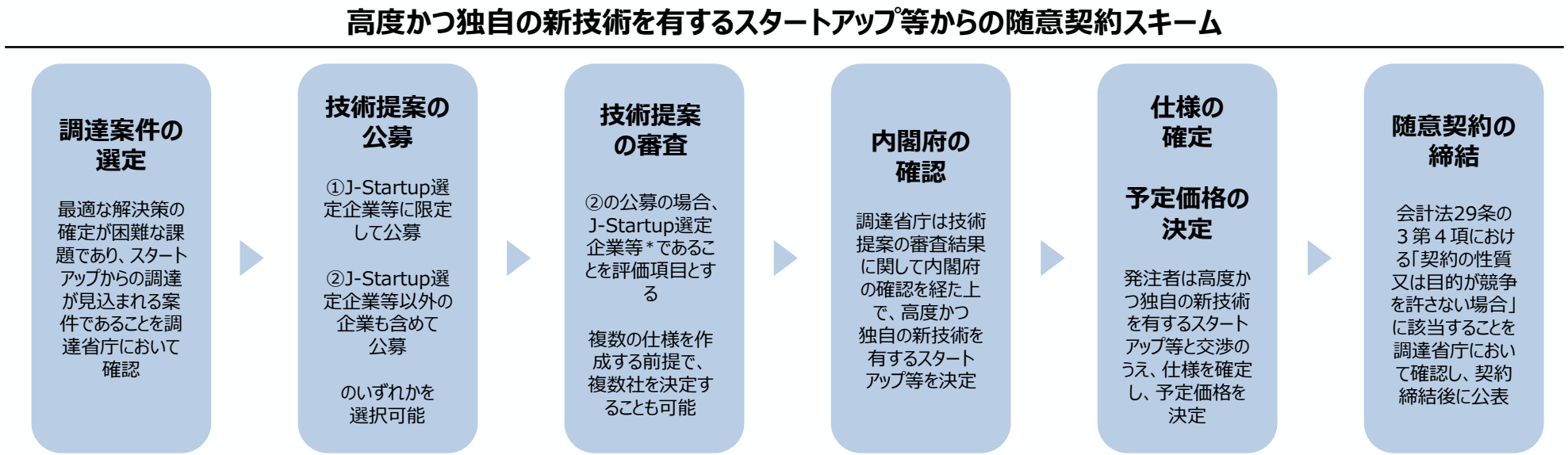
（参考）詳細資料

１．これまでいただいたご意見の整理

２．各事業概要資料

高度かつ独自の新技術を有するスタートアップ等からの随意契約スキーム

- 政府がスタートアップの技術を自ら探知し調達すること及びスタートアップが政府のニーズを詳細に把握することが困難であるとの背景を受け、本スキームではまず、**政府だけでは最適な解決策の確定が困難**であり、**スタートアップの有する新技術による解決が見込まれる行政課題**に対して、その解決のための**技術提案を公募**する。
- 調達省庁は、得られた技術提案を審査し、**内閣府の確認を経た上で**、行政課題を適切に解決しうる提案を行った者を、**「高度かつ独自の新技術を有するスタートアップ等」として決定**する。その後、調達省庁は当該スタートアップ等と案件の仕様等を確定し、随意契約を締結し、**公表**する。
- 技術提案の公募は**J-Startup選定企業等＊を対象に実施**する。また、J-Startup選定企業等以外の企業も含めて公募した場合は、**J-Startup選定企業等であることを評価項目として**、優れたスタートアップへの優遇を行う。



＊ J-Startup選定企業等とは、J-Startup、J-Startup Impact, J-Startup local選定企業等を含む、「技術力ある中小企業者等の入札参加機会の拡大について（平成12年10月10日政府調達（公共事業を除く）手続の電子化推進省庁連絡会議幹事会決定）」の３（３）から（７）までに掲げるもの（ＳＢＩＲの特定新技術補助金等の交付先、官民ファンドが出資したファンドの出資先等）及び日本スタートアップ大賞、日本ベンチャー大賞その他各省におけるスタートアップ表彰企業の受賞企業を指す。

IoT製品に対するセキュリティ適合性評価制度の概要

- 2022年11月より検討会(※1)を開催し、2024年3～4月のパブコメを経て、8月に制度構築方針を公表。**9月30日にIPAから「JC-STAR」という制度名にて制度開始の案内**(※2)を実施。
- **★１については2024年度中の制度開始**を予定。**政府調達等の要件**等とすべく関係省庁と議論中。**米欧等の諸外国との制度調和**を図るため議論中。

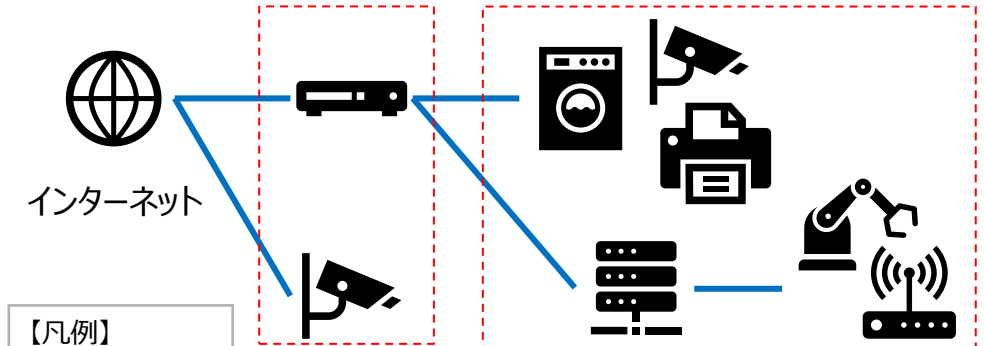
制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)

JC-STAR

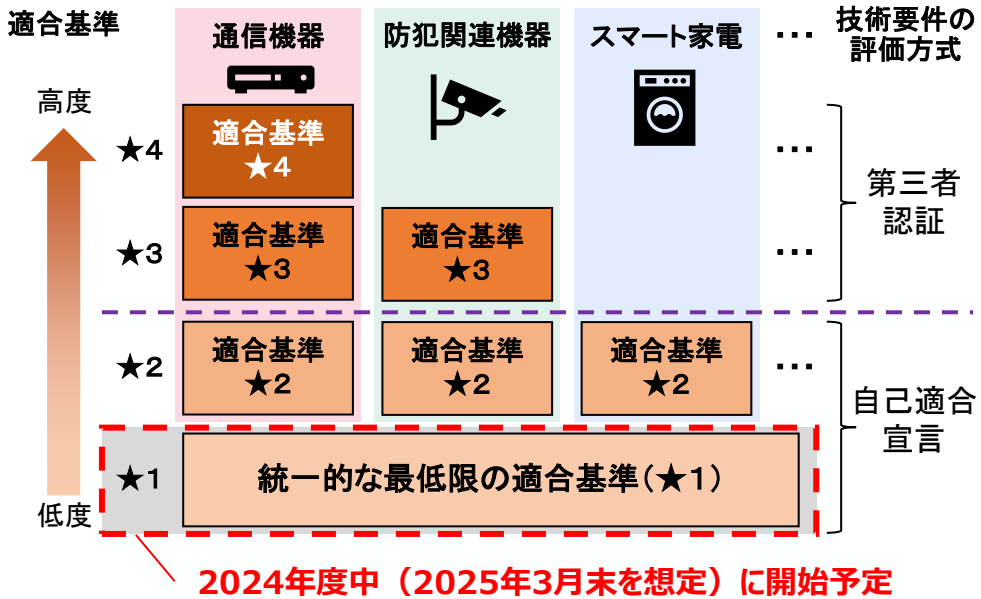
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN (IPA)

対象製品の概要



※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



(※1)経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)IPA「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」https://www.ipa.go.jp/pressrelease/2024/press20240930.html

（参考）懸賞金型研究開発事業

NEDO Challenge

問い合わせ先　イノベーション・環境局　イノベーション政策課　フロンティア推進室

概要

仕組み

- 課題に対して特定の技術・手法に寄らず、**より優れた「成果」を出した者に懸賞金**を与える

海外事例

- 海外の国費による開催例として、2004年/2005年に実施された米国DARPA Grand Challengeにおいて自動運転技術を競い合い、**Waymo(自動運転タクシー)やUber等の技術や人材にも繋がっている**と言われている

METI/NEDO取り組み

- 経済産業省/NEDOにおいては、2022年度より試行的に開始、**2024年度より本格実施**

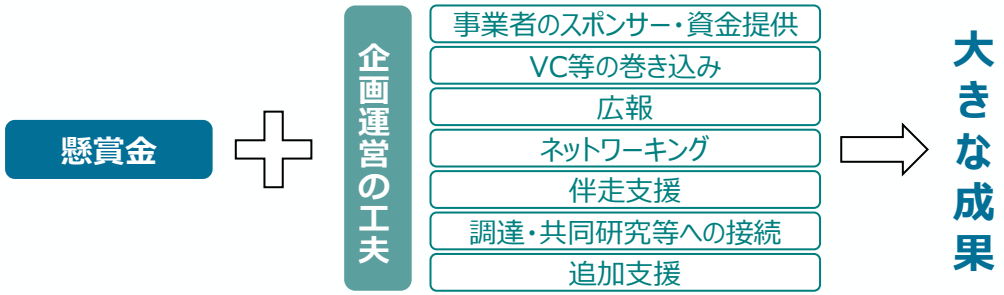
2022年度	(補正予算)	2テーマ	宇宙(衛星データを活用したサプライチェーン課題解決)、AI(ハイパーパラメータ最適化)
2023年度	6億円	3テーマ	宇宙(衛星データ環境系)、AI(筋電位×脳波による予測)、サーキュラ(LiB回収システム)
2024年度	11.5億円	3テーマ	宇宙(衛星データ)、製造DX(効率化＆質向上)、量子(ユースケースと人材発掘)
2025年度	(43億円の内数)	(検討中)	(検討中)

スキーム

※民法第529条-532条民法に基づき報酬を与える制度として実施

成果最大化に向けた工夫・考え方

- 伴走支援・ネットワーク構築などの**非金銭的支援**や、表彰者への**追加支援や調達・共同研究へ接続**などにより、**より大きな成果に繋げられる可能性**
- 大きく盛り上げることで、**資金調達や事業提携などの可能性**が高まる



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

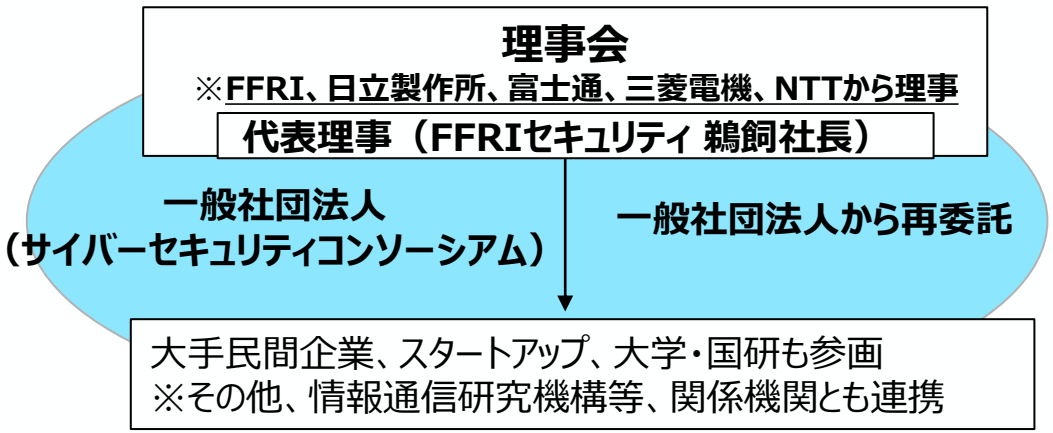
経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」

- 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**や、AIを活用したシステムの脆弱（ぜいじゃく）性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ。

実施体制

一般社団法人サイバーリサーチコンソーシアム

研究開発の体制



事業期間（予定）

2024年7月～2029年6月

事業規模など

- 事業規模：290億円以下
- 契約形態：委託事業

主な研究開発内容

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

- ✓ランサムウェアの自動抽出・分析効率化
- ✓未知攻撃の早期発見技術の開発（例：サイバー攻撃の情報収集や検知の技術開発）
- ✓サイバー攻撃を行う主体の意図分析のための情報収集・解析 等

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を活用した脆弱性の発見・防御技術、ペネトレーションテストの開発
- ✓耐量子計算機暗号（量子計算機が実用化されても、安全性確保が可能な暗号技術）の実装技術の開発
- ✓耐タンパー性（情報・機器のための、外部からの解析・改変を防ぐ能力）の向上 等

③共通基盤の整備

- ✓サイバー脅威情報の収集・集約のための基盤開発
- ✓サイバー人材の評価・管理のための基盤開発

（参考）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の内容・参画機関

研究項目	①-1 アーティファクト分析	①-2 攻撃主体情報獲得	①-3 未知攻撃早期発見	②-1 AI活用脆弱性探査	②-2 AI活用防御能力向上
主な研究内容	ランサムウェアの解析・自動分類 ランサムウェアの被害を受けたデータの復号技術の開発	サイバー攻撃を行う主体の分析（例：攻撃意図・手口の把握、能力評価）	サイバー攻撃の情報収集や攻撃検知の技術開発AI等を活用した攻撃リスク判定技術の開発 リスクに応じたセキュリティ対応ポリシーの整理	AI等を用いた脆弱性の発見や防御技術の開発	AIを活用したより効率的なペネトレーションテスト（※）の開発 （※） 脆弱性に対する侵入テストを通じて、リスク評価を行い、不正アクセスや改ざん等の予防につなげるもの
参画機関	FFRIセキュリティ 横浜国立大学 Preferred Networks	富士通 横浜国立大学	FFRIセキュリティ NTT	FFRIセキュリティ Preferred Networks NEC リチェルカセキュリティ Powder Keg Technologies	三菱電機 早稲田大学 FFRIセキュリティ 横浜国立大学

研究項目	②-3 OTペネトレフレームワーク技術	②-4 耐量子計算機暗号技術（※）	②-5 耐タンパー性向上技術	③-1 情報の効果的連携技術	③-2 高度サイバー人材関連技術
主な研究内容	制御システム（※）のペネトレーションテストの技術開発 （※）工場等の製造現場の設備・システムを動かす技術	耐量子計算機暗号の実装技術の開発（例：クラウドやハードウェアへ実装する上での効率化等） （※）量子計算機が実用化されても、安全性確保が可能な暗号技術	情報・機能の保護のための、外部からの解析・改変を防ぐ能力（耐タンパー性）の向上のための技術開発	各種攻撃・攻撃者に関する情報の集約・管理・共有手法の開発	高度サイバー人材の評価・管理ツール等の開発
参画機関	日立製作所 慶應義塾大学	産総研 東京大学 三菱電機 TOPPAN SCU PQ Shield	産総研 三菱電機 FFRIセキュリティ リチェルカセキュリティ セカフィー	サイバーリサーチコンソーシアム	サイバーリサーチコンソーシアム 情報セキュリティ大学院大学

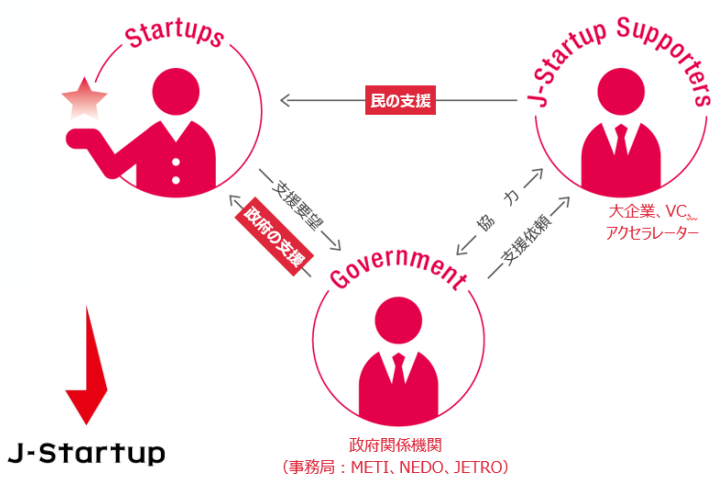
J-Startup　スタートアップ育成支援プログラム

概要

ログローバルに活躍するスタートアップを創出すべく、**外部有識者の推薦**などに基づき、潜在力のある企業を「J-Startup」企業として選定し、官民連携で集中支援するプログラム。

実績・アピールポイント

- 2018年に「J-Startup」プログラムを立ち上げ。第１次（92社：2018年）、第２次（49社：2019年）、第３次（50社：2021年）、第４次（50社：2023年）選定を実施済。
- **選定企業に対しては、各種補助金等における優遇**、民間企業「**J-Startup Supporters**」**との連携支援**などの取組を実施。



ディープテックの特徴や成長段階に応じた支援の実行

- スタートアップの創出から事業化に至るまで、**成長段階に応じた施策を充実化**。**本格的な実行フェーズ**へ。

事業の発展段階：起業前 → 起業後・シード → アーリー → ミドル以降

研究・起業準備	実用化研究開発	量産化実証	事業開発
研究、起業家育成、経営人材マッチング等	実用化に向けた要素技術等の研究開発	量産化・スケール化の実証	商用の設備投資、ソフトウェア投資、大規模ユーザー実証等

ディープテック・スタートアップの起業・経営人材確保等支援事業
約15億円（R7当初）

事業会社の有する革新的な技術等のカーブアウト加速等支援事業
約10億円（R5補正）

ディープテック・スタートアップ支援事業
約1,000億円（NEDOに基金造成）

第1回公募：23件採択（令和５年８月）
第2回公募：17件採択（令和５年12月）
第3回公募：15件採択（令和６年３月）
第4回公募：12件採択（令和６年９月）
第5回公募：7件採択（令和６年12月）
第6回公募：審査中

ディープテック・スタートアップへの事業開発支援事業
約76億円（R6補正）

- ✓ **マザープラント整備**
- ✓ **市場・需要を見据え、大規模なスケール化**を実現

GX分野のディープテック・スタートアップ支援事業410億円（NEDO交付金）

第１回公募：5件採択（令和６年９月）
第２回公募：4件採択（令和６年12月）
第３回公募：審査中

パイロット・実証プラント

（出典）ユーグレナHP（バイオ燃料製造プラント）

- ✓ **知の掘り起こし**
- ✓ 大学・研究機関等の**StoS**
  モメンタムの醸成

事業化・継続的な収益の獲得

- ➡ 新たな**需要の創出・拡大**
- ➡ 事業会社との更なる**事業連携**
- ➡ VCや金融機関等からの**大規模な資金調達**

ディープテックスタートアップ支援事業　概要（事業費1,000億円、NEDOに基金造成）

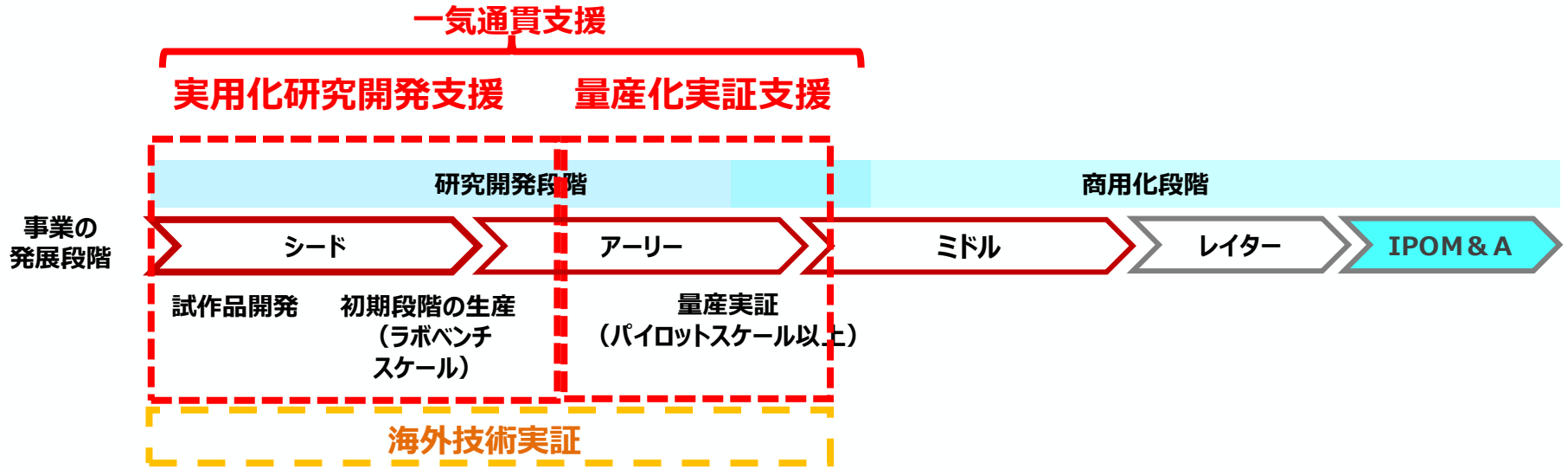
「実用化研究開発支援」事業：　試作品の開発や他社等との共同研究開発を実施するとともに、**研究開発の成果を活用したF/S調査の実施、生産技術開発**等を支援。

「量産化実証支援」事業：　量産化実証に向けた生産設備検査設備等の設計製作購入導入運用費用（安定的に稼働するまでの試運転や製品評価に係る諸費用を含む。）やこれらの**設備等を設置する建屋の設計工事費用**を支援。

これらの事業を一気通貫で行う**「一気通貫支援」**や、**相手国政府機関等との協力の下で行う海外展開のための「国際共同研究開発事業」、海外の市場規制等に適合するための研究開発や調査費用、現地での技術サービス拠点の設置費用、現地での製品サービス実証に要する費用等の一連の海外展開事業**を支援する**「海外技術実証」**も実施。

事業性の担保のため**VCとの連携**を重視する。また、**長期弾力的な支援とSG（ステージゲート）審査の組み合わせ**により、効果的な支援を行う。

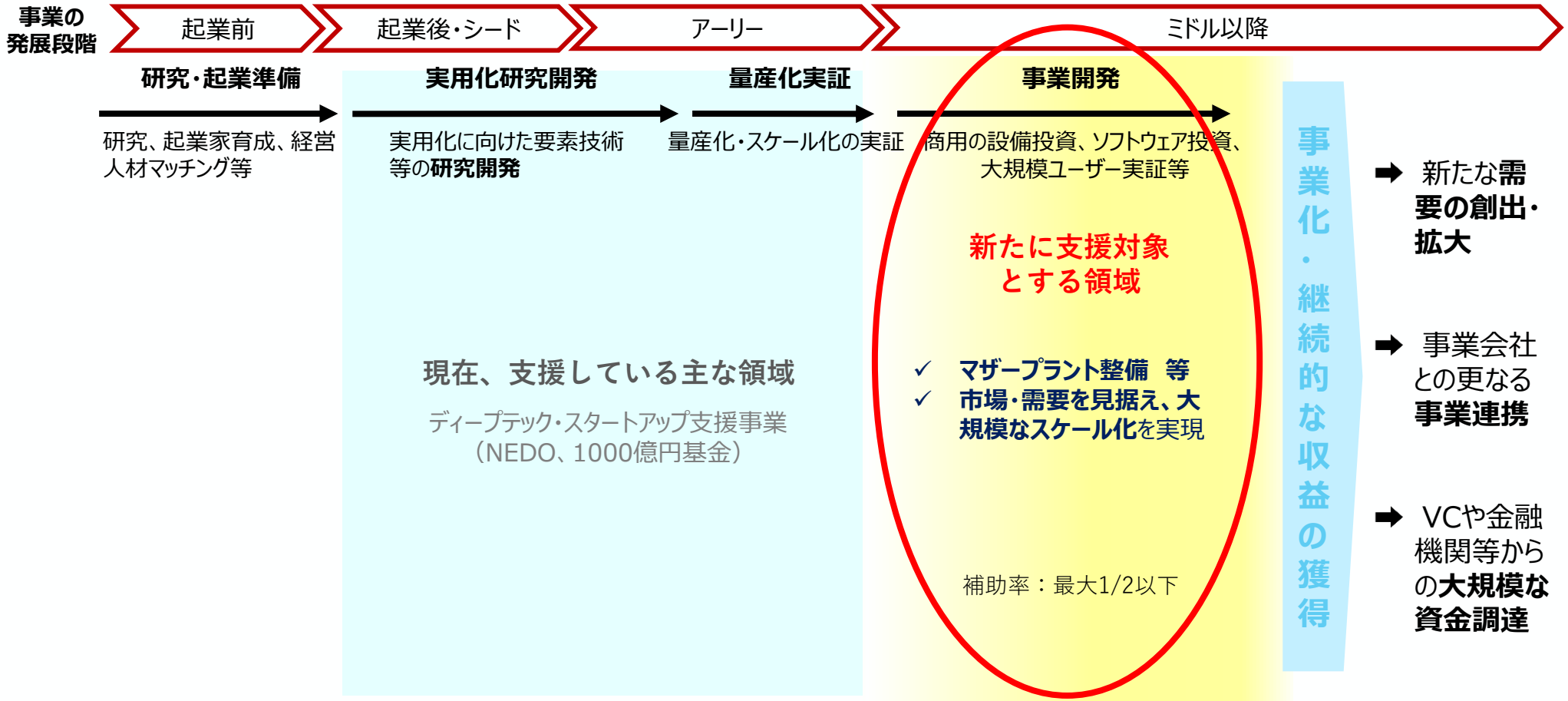
第1回公募:2023年8月採択（23件採択）　第2回公募:2023年12月採択（17件採択）
第3回公募：2024年3月採択（15件採択）　第4回公募:2024年9月採択（12件採択）
第5回公募:2024年12月採択（7件採択）



※なお、経産省で執行するSBIR指定補助金等事業も、ディープテックスタートアップ支援事業の中で併せて実施。

ディープテックスタートアップへの事業開発支援事業　概要
（事業費約76億円、NEDOに交付金として措置）

- 事業の拡大に向けた一定の研究開発（要素技術に係る開発や、量産技術の実証等）を終えたディープテック・スタートアップが、その成果を事業化するために行う**設備投資等の事業開発活動を支援**。



起業家等の海外派遣事業「J-StarX」

令和５年度「起業家等の海外派遣シリコンバレー拠点形成事業」（約62億円）の内数
令和５年度「ヘルスケアスタートアップエコシステム強化事業」（約23億円)の内数
令和６年度「スタートアップのグローバル化強化事業」（約44億円）の内数

- 「J-StarX」とは、世界で勝てるスタートアップの創出や「Born Global」な起業を促すため、**海外のイノベーション拠点人材とのネットワークの構築や、我が国のイノベーション人材の育成**を目的に、若手起業家や学生等を欧米やアジアを中心とする**世界各地のスタートアップエコシステムに派遣**する事業。
- これまでの「始動」を抜本的に拡充し、今後５年間で1000人を派遣すべく2023年度に事業を開始。2024年度は、起業家等のステージや産業領域などに合わせた以下を中心とするコースを展開した。2025年度のコースは本年春ごろに公開予定。

		Basic	Intermediate	Advanced
基本情報	目的	海外展開を進めるための成長戦略や基礎知識の習得	海外展開戦略の策定及び初動着手	資金・顧客獲得
	人数	20～30人程度	10人程度	数人程度
	期間	10日～３週間程度	10日～３か月程度	10日～２週間程度
派遣先・プログラム名称	北米	**U25（UC Berkley）** **女性起業家** **Local to Global Success**	**Beyond JAPAN Zero to X** （宇宙、バイオ等） **HealthTech Gateway** (AI Medical in the US) **Silicon Valley Extended**	**Food Frontiers USA** **Harvest Horizons** (Agri/Food tech to North America) **Global Growth** (Climate Tech、AI、Dual-Use)
	欧州	Local to Global Success	HealthTech Gateway (General in APAC/Europe) **Europe Long-term（Paris）**	**Bio UK Launchpad**
	アジア	Local to Global Success **インド派遣**	**インドネシア派遣**	

防衛産業へのスタートアップ活用に向けた合同推進会

- 防衛省と経済産業省が連携し、防衛省・自衛隊のニーズとスタートアップとのマッチングを図る機会を創出するための枠組み「防衛産業へのスタートアップ活用に向けた合同推進会」を開催。ベンチャーキャピタルも巻き込み、より幅広い連携を促進。
- 本会議への登壇をきっかけとした調達事例が出てくるなど、一定の成果に。

開催実績

第１回（R5.6.16）
・防衛省から、新規参入の取組、安全保障技術研究推進制度、先進技術の橋渡し研究、早期装備化のための取組等について紹介
・経産省から、スタートアップ支援施策、J-Startup選定企業等から防衛に活用し得る企業を紹介

第２回（R5.9.6）
・第１回で経産省から紹介された企業のうち、防衛省内の希望を踏まえ、スタートアップ企業４社を招聘し、企業毎に各自衛隊、防衛本省内部部局及び装備庁とのマッチングを実施

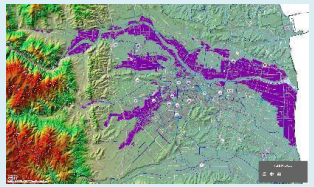
第３回（R5.10.31）
・第２回同様、防衛省内の希望を踏まえ、スタートアップ企業等４社を招聘し、企業毎に各自衛隊、防衛本省内部部局及び装備庁とのマッチングを実施

第４回（R6.1.12）
・経産省の支援策等の活用実績があるベンチャーキャピタル（VC）のうち、安全保障分野に活用しうる技術分野を投資先の１つの柱とするVC４社を招聘し、当該４社からスタートアップ企業選定時の着眼点や投資等の基準のほか、投資先スタートアップ企業の技術・製品等の紹介を受け、意見交換を実施

第５回（R6.9.18）
・ 経産省のスタートアップ企業等に関する情報や防衛省内の希望等を踏まえ、スタートアップ企業２社を招聘し、企業毎に各自衛隊、防衛本省内部部局及び装備庁とのマッチングを実施するとともに、今後の防衛省の装備政策・経産省の産業政策を連携させたエコシステムの構築に関する意見交換を実施

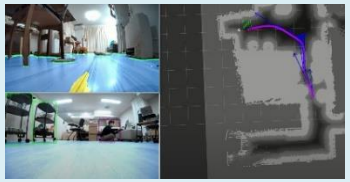
対象技術例

・長距離無人航空機等を活用した広域災害対策情報支援



・ドップラーライダー（風況リモートセンシング）を活用したドローン検知・識別

・深層学習等を活用した指揮統制支援やロボットの自律走行



大企業等のスタートアップ連携・調達加速化事業

KPI

調達を見据えた事業計画の策定や初期的な調達が30%以上実施されることを目指す。

① 調達拡大に向けた機運醸成・コミュニティの形成

概要

- **スタートアップ調達の機運を醸成**し、**調達拡大を加速的・持続的に進める**ためには、調達に関わる様々な主体による**コミュニティの形成**が必要。
- モデル契約の普及やマッチングの提供等を**官民協同で行い、ネットワークを拡大。**

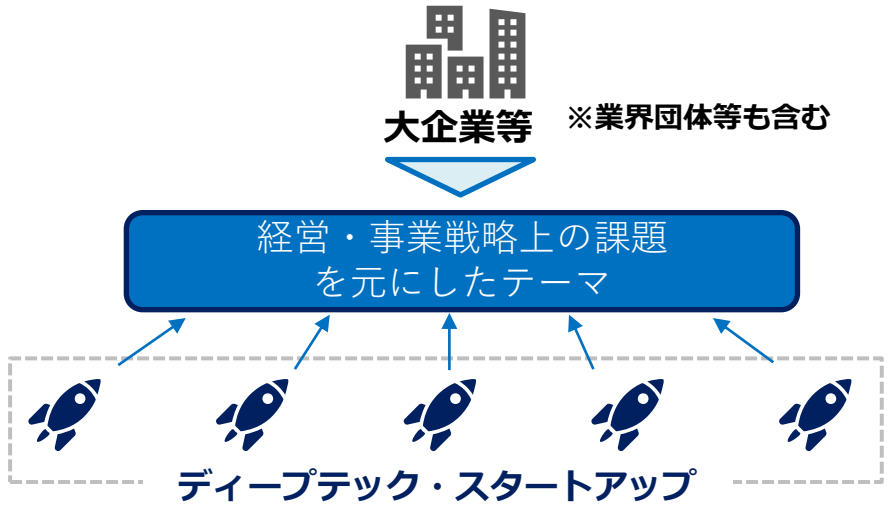
スキーム

- ネットワーキングイベントの開催
- 調達モデル契約や事例の提示
- 勉強会・研修の実施
- 情報発信

② 大企業連携・調達の加速化支援事業

概要

- **大企業の経営・事業戦略上の課題**をスタートアップが解決できると**中長期的な調達**に繋がる一方、**大企業**には“**課題解決に繋がる技術・事業を有する社を十分に探索できない**”、“可能性のあるスタートアップがいても、**コストやリスクを考えると関係構築に踏み切れない**”といった**壁**が存在。
- 既存予算事業も活用しつつ、大企業等の中長期的経営・事業戦略**課題についての整理**や、そうした**課題の解決に資するスタートアップを支援**し、**望ましい連携・調達**の事例を創出する。



（参考）サイバー安全保障分野での対応能力の向上に向けた有識者会議
サイバー安全保障分野での対応能力の向上に向けた提言（令和６年11月29日）（抄）

２ 実現すべき具体的な方向性

（１）官民連携の強化

② 高度な攻撃に対する支援・情報提供

（略）加えて、現在、内閣サイバーセキュリティセンター（NISC）のほか、警察・経済産業省・JPCERT/CC・情報処理推進機構等が個別に情報発信を行っているが、特に緊急性の高い情報発信について機関ごとに差異が生じないよう、ワンボイスで行われるべきである。また、現場レベルで官民の対応者が集結できる仕組みや、国産技術の活用、友好国との間での相互運用性にも配慮すべきである。

（４）横断的課題

③ 政府機関等の対策強化

（略）これら政府機関等の対策の強化にあたっては、日本発のサイバーセキュリティ関係のソフトウェアや中核的なセキュリティ技術がほとんどなく、公に使われているものもないという我が国の状況を踏まえると、**国家安全保障の観点からも政府主導で高品質な国産セキュリティ製品、サービス供給の強化を支援すべき**と考えられる。その際、大学等で開発された技術等の社会実装と、知見のフィードバックによる更なる技術開発の促進というエコシステムの構築を図ることも重要となる。

（参考）産業サイバーセキュリティ研究会ＷＧ３
「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（仮題）」に向けての検討会 委員等名簿

※敬称略、五十音順

（委員）

稲垣 隆一 稲垣隆一法律事務所 弁護士

鵜飼 裕司 株式会社 FFRI セキュリティ 代表取締役社長

鴨田 浩明 株式会社 NTT データ ソリューション事業本部 セキュリティ＆ネットワーク事業部 事業部長

國領 二郎 慶應義塾大学 総合政策学部 教授【座長】

下村 正洋 特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）事務局長

関 守 株式会社 AGEST 取締役専務執行役員 CGSO サイバーセキュリティ事業本部長

花見 英樹 株式会社日立製作所 インダストリアルデジタルビジネスユニットエグゼクティブテクノロジーマネージャ

丸山 満彦 PwC コンサルティング合同会社パートナー 情報セキュリティ大学院大学 客員教授

（オブザーバー）

総務省

独立行政法人情報処理推進機構