経済産業省

資料５

一部非公表

# 事務局資料
# （これまでの議論を踏まえた仮説）

２０２４年１２月２４日

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）

# セキュリティビジネスにおける仮説①

**【セキュリティビジネスを振興する意義】**

- 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**。

- また、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た上で適切なセキュリティ対策を講じる上でも重要**。

- さらに、**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。更には、**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・サービス供給拡大は**赤字解消にも貢献**する。

# セキュリティビジネスにおける仮説②

**【セキュリティビジネスの現状①（産業構造）】**

- **セキュリティビジネスは大きくは、製品開発・提供／サービス提供の2種類に分類される**。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。**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（大手SIer数社が売上の6割程度を占めている現状）**。

- 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選択**している状態。**製品選択の判断基準**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製品ではなく、**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状況**。

- 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た**。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**（「J-Startupでも、セキュリティ企業については数社程度）。

- 全体として新興企業や新規製品・サービスにおいて、販路開拓・事業拡大にハードルがある状況は、彼らの財務基盤を不安定なものにさせ、**設備・事業に対する継続的な投資と、それに伴う製品・サービスの競争力強化／安定的なビジネスモデルの構築を困難**にさせているおそれがある。

# セキュリティビジネスにおける仮説③

**【後押しすべき主体】**

- 海外製をはじめとする既存製品・サービスが存在する中で、すべての領域で同レベルの競争力を持つことは困難であるが、**技術動向も踏まえた今後の需要の高まりや我が国産業の強みを踏まえると、後押しすべき主体として以下のようなものが考えられる**（一部の分野では、こうした事業を展開するスタートアップも登場）。

  ① **AI・量子技術など新しい技術を活用した製品・サービスを提供する企業**

  ② **我が国がハードウェアの強みを持つ制御機器や工場設備向けのセキュリティ製品・サービスを提供する企業**

  ③ **海外メーカーでは十分対応出来ていない国内組織向けの製品・サービスを提供する企業**

- 変化の激しいセキュリティ対策の領域において、**こういった製品・サービスを上手く活用すれば、企業のセキュリティ強化にも貢献**されうる。今後、我が国のセキュリティ強化の必要性を踏まえると、**こうした事業者の拡大・セキュリティビジネスのエコシステムの構築が我が国のセキュリティビジネスの振興にあたって重要な点**。

# これまでの議論を踏まえたセキュリティビジネス振興に向けた考え方

| 現状 | 主な課題 | 政策対応 | 目指す姿 |
|---|---|---|---|
| ①国内企業の競争力不足（特に製品マーケットにおいて、海外製品が大半を占めている状況であり、存在感が欠落）<br>- 製品性能に相対的に強みがない<br>- 提供できる事業が限定<br>（※）大きな案件に対応できるほどの経営基盤がない | ✓ 脅威データ等、製品開発の際に必要なリソースの不足<br>✓ セキュリティベンダーによる事業連携・協業の場の不足 | ✓ 有望な技術・事業の発掘、研究や事業化促進のための支援<br>✓ 脅威データ等の活用のための支援<br>✓ ベンダー間協働のための枠組み構築 | ✓ 有望な製品・サービスを提供する企業のシェア拡大<br><br>KPI（例）：市場における我が国企業のシェア |
| ②新興企業が育ちにくい環境<br>- ニーズ企業からの認知不足／認知⇒活用に至らない<br>- 安定的な販路や収益源の確保が困難<br>- 資金調達が困難 | ✓ 導入実績が重視される商慣（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） | ✓ 政府機関・大企業における調達機会の拡大<br>✓ 有望な企業・製品・サービスの可視化 | ✓ 有望なスタートアップの増加<br><br>KPI（例）：J-Startup選定企業数 |
| ③供給力の基盤が脆弱<br>- 優れた製品・サービス供給に従事する人材の不足 | ✓ 人材育成のための場が不足<br>✓ 企業と人材のマッチングが不十分 | ✓ 人材育成プログラムの拡張<br>✓ 既存施策（登録セキスペ）の活用促進 | ✓ 十分な人材供給の実現<br><br>KPI（例）：人材育成プログラムの修了者の活動数 |

# 参考

# 論点（本日御意見をいただきたい点）①

第1回検討会資料
再掲

**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

第1回検討会資料
再掲

**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

第1回検討会資料
再掲

**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。