経済産業省

資料３

事務局説明資料
産業サイバーセキュリティ研究会
WG3 第9回

令和７年４月１７日

経済産業省 商務情報政策局

サイバーセキュリティ課

産業サイバーセキュリティ研究会の体制及び関連会議の実績

産業サイバーセキュリティ研究会

第１回：平成29年12月27日	
第２回：平成30年　5月30日	アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日	アクションプランを加速化する３つの指針を提示
第４回：令和　2年　4月17日	（電話開催）産業界へのメッセージを発信
第５回：令和　2年　6月30日	サイバーセキュリティ強化運動の展開
第６回：令和　3年　4月　2日	アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和　4年　4月11日	産業界へのメッセージを発信
第８回：令和　6年　4月　5日	新たなサイバーセキュリティ政策の方向性を提示

＜構成員＞

※2025年5月開催時点

伊藤　栄作	三菱重工業株式会社取締役社長
遠藤　信博	日本経済団体連合会サイバーセキュリティ委員長、 日本電気株式会社特別顧問
片野坂真哉	日本情報システム・ユーザー協会会長、 ANAホールディングス株式会社　取締役会長
澤田　純	日本電信電話株式会社取締役会長
寺田　航平	経済同友会副代表幹事、 寺田倉庫株式会社　代表取締役社長
東原　敏昭	株式会社日立製作所取締役会長　代表執行役
船橋　洋一	公益財団法人　国際文化会館 グローバル・カウンシル チェアマン
村井　純(座長)	慶應義塾大学教授
渡辺　佳英	日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

＜オブザーバー＞

NISC、サイバー安全保障体制制度準備室、警察庁、金融庁、総務省、外務省、
文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、デジタル庁

WG１（実効性強化・国際連携）

第１回：平成30年　2月　7日
第２回：平成30年　3月29日
第３回：平成30年　8月　3日
第４回：平成30年12月25日
第５回：平成31年　4月　4日
第６回：令和　2年　3月（書面開催）
第７回：令和　2年10月（書面開催）
第８回：令和　3年　3月15日
第９回：令和　4年　4月　4日
第10回：令和 6年　3月14日
第11回：令和 7年　4月14日

- ガイドライン等の実効性強化
- 国際的な制度調和に向けた連携

WG２（地域・中小企業支援）

第１回：平成30年　3月16日
第２回：平成30年　5月22日
第３回：平成30年11月　9日
第４回：平成31年　3月29日
第５回：令和　2年　1月15日
第６回：令和 2年8月25日
第７回：令和 3年2月18日
第８回：令和 4年3月23日
第９回：令和 5年3月27日
第10回：令和6年3月25日
第11回：令和7年4月15日

- 地域・中小企業等における対策支援

WG３（産業振興・人材育成）

第１回：平成30年4月　4日
第２回：平成30年8月　9日
第３回：平成31年1月28日
第４回：令和 元年8月　2日
第５回：令和2年3月（書面開催）
第６回：令和3年3月10日
第７回：令和4年4月　6日
第８回：令和6年4月　3日
第９回：令和7年4月17日

- セキュリティ産業振興、研究開発
- 人材育成・確保

＜新たなサイバーセキュリティ政策の全体像及び今後の方向性＞

1．サプライチェーン全体での対策強化
2．セキュア・バイ・デザインの実践
3．政府全体でのサイバーセキュリティ対応体制の強化
4．サイバーセキュリティ供給能力の強化

最近国内外で発生した主な事案

①機微技術情報等の窃取

- 2019年以降、中国の関与が疑われるグループ「MirrorFace」による、**日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーン**が実行されている。（2025年1月 警察庁及びNISCが注意喚起を発出）
- 2024年後半、中国背景と指摘されるグループ「Salt Typhoon」による、米国の通信事業者のネットワークに侵入して**政府関係者等の通話記録等、安全保障に関する情報等の窃取**を狙うような活動が報告されている。

②金銭等資産の窃取

- 2024年5月、北朝鮮を背景とする攻撃グループ「TraderTraitor」が、**ソーシャルエンジニアリング等の手法を用いて**、㈱DMM Bitcoinから**約482億円相当の暗号資産を窃取**。（2024年12月 警察庁、NISC及び金融庁が注意喚起を発出）

③事業活動の停止

- 2024年6月、㈱KADOKAWAが**ランサムウェアを含む大規模サイバー攻撃を受け、Webサービス等が停止**。大量の個人情報や企業情報が漏えいしたうえ、SNS等を通じて拡散される二次被害も発生。

④重要インフラの機能停止等

- 2024年12月～2025年１月の年末年始にかけて、航空事業者、金融機関、通信事業者等が**相次いでDDoS攻撃を受け、サービスの一時停止**等の被害が発生。（2025年2月 NISCが注意喚起を発出）
- 2024年2月、米国政府機関（CISA、NSA、FBI等）が、ファイブアイズ諸国の関係機関と合同で、中国を背景とするグループ「Volt Typhoon」による米国の重要インフラを標的とした活動について注意喚起。同グループは、**有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークへのアクセス権限を確保してOT機器に対する侵害を可能としている**旨が指摘されている。

デジタル技術の発展によるサイバー攻撃の高度化･複雑化

- AI等のデジタル技術の発展の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ**がある。

デジタル技術の発展によるサイバーリスクの増加

ITシステム、クラウド等の活用拡大、OT製品の急増など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

NICTER において2024年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,862億パケット（2018年の約３倍）。

スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成 AI ツールの登場**

2024年における**フィッシングの報告件数**は**前年比約50%増の170万件超に急増**

量子コンピュータによる暗号アルゴリズムの危殆化

- 各国が開発を加速させている**量子コンピュータが実用化**すると現在広く使用されている**公開鍵暗号（RSA暗号）アルゴリズムの危殆化される恐れ**が指摘されている。
- 現在のアルゴリズムの安全性は、古典計算機では現実的時間内では解くことが困難とされている数学的問題（素因数分解問題や離散対数問題）に依拠しているが、大規模な量子コンピューターでは高速に解読することが可能であるため。
- このため、量子コンピュータ時代にも安全に利用できる暗号技術が求められており、米国NIST等が**耐量子計算機暗号（PQC）に係る国際標準化**作業を進めている。

サイバー攻撃のエコシステム（ダークウェブ）の存在

- **ダークウェブの闇市場**では非合法で個人や企業の機密データ、**マルウェアを容易に作成できるツールキットなどが取引**されており、**サイバー犯罪を助長**している。

（出典）(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2024」、フィッシング対策協議会「月次報告書」　等

地政学動向の変化に伴うサイバーリスクの高まり

- サイバー攻撃が巧妙化・深刻化する中、**地政学リスクの増大とも相まって、安全保障にも関わるサイバー事案の脅威が高まっている状況**にある。

サイバー攻撃の変遷

■公開サーバへの攻撃
・特徴：ウェブサーバ・外向けサービスへの大量送信　等
・効果：ウェブサイト等の停止
・事例：エストニア・2007年

■IT系システムの侵害
・特徴：情報システム内部への侵入・暗号化
・効果：暗号化・システム障害、身代金要求
・事例：Wannacry・2017年　等

■有事に備えた重要インフラ等への侵入
・特徴：最深部・制御系システムに至る高度な侵入能力
・効果：インフラ機能の停止
・事例：Volt Thyphoon・2023年　等

■機微情報の窃取の危険
・特徴：情報システムへの権限外アクセス・利用
・効果：機密情報の漏えい・悪用
・事例：Black Tech・2023年

（出典）各種報道発表・報道情報等を基に作成。

CISA “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure”

ウクライナに対する主なサイバー攻撃

- 侵略開始以前：
  - ロシアは侵略開始の１年以上前からウクライナの政府機関や重要インフラ等の情報システム・ネットワークに侵入し、**破壊的サイバー攻撃を準備**。
  - 侵略開始の１か月程度前から、破壊的なサイバー攻撃等を開始。
- 2022年２月：通信衛星に対する攻撃
  - 米Viasat社が提供する**通信衛星サービス**（KA-SAT network）**が利用不能**となった。
- 2022年10月：変電所に対する攻撃
  - ウクライナの変電所が攻撃を受け、**停電が発生**。

政府機関等へのサイバー攻撃事案

- **NISCに対する不正通信事案**（2023年８月）
  - NISCの電子メール関連システムに対する不正通信があり、メールデータの一部が外部に漏えいした可能性がある旨を公表。
- **JAXAへの不正アクセス事案**（2024年７月）
  - 外部からJAXA内の業務用イントラネットの管理用サーバーに不正アクセスが行われた可能性があった旨を公表。

（参考）IPA「情報セキュリティ10大脅威」

情報セキュリティ10大脅威 2025	
順　位	組織向け脅威
1位	ランサムウェア攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

中小企業の被害が全体の6割以上を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

（出典）独立行政法人情報処理推進機構「情報セキュリティ10大脅威2025」

サイバーセキュリティ産業を取り巻く各国の動向

➢ 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

前回SWG資料

我が国サイバーセキュリティ産業の振興に向けた強化策の検討

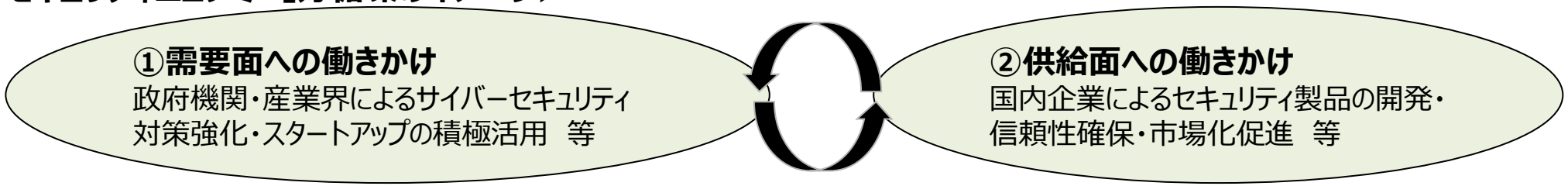
問題意識

- 我が国の**サイバーセキュリティは必要な技術や製品の多くを海外に依存をしている状況。**
- 現状のままでは、我が国ユーザー企業のデータが国内に蓄積されず、当該データを活用してより品質の高い製品・サービスを提供することが我が国セキュリティ企業において一層困難になるとの**負のスパイラルが生じる**こととなる。また、安全保障環境が厳しさを増す中、我が国ユーザー企業にとって重要なデータのセキュリティを**過度に諸外国の製品・技術に依存することにより、我が国の自立性が危ぶまれるリスク**も生じる。
- 今後重要度がますます増してくるサイバーセキュリティ関連市場において、我が国のセキュリティ企業が相対的に**強みを発揮できる領域**や、我が国のセキュリティ企業が**抑えるべき領域**を、しっかり確保していけるよう、**サプライサイドを強化**することが、①経済安全保障の観点からも、②産業政策の観点からも重要。また、そのような能力を確保することにより、同盟国・同志国との強固な連携も可能となる。

目指すべき姿

- 海外主要国では、政府や企業の需要を背景にしつつセキュリティ企業は積極的に製品開発・販路拡大を行い、スケールアップ。我が国でも、こうした構造を参考として、**需要と供給のエコシステムの構築**により、**「セキュリティエコノミー」の確立**と**主要国と同等以上のサイバーセキュリティ能力の確保**を目指す。
- もっとも、品質の高い外資製品の利用を妨げるものではなく、必要な海外連携は実施しつつも、サイバーセキュリティ市場が拡大する中で、我が国にとって重要な領域を中心に、**「高品質」な国産セキュリティ製品・サービスの供給が強化される状況**を目指す。これにより、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」政府全体の目標にも貢献。

＜「セキュリティエコノミー」好循環のイメージ＞



（参考）我が国サイバーセキュリティ産業の振興に向けた強化策の検討に係る論点例

前回SWG資料

- 「目指すべき姿」の解像度をどのように高めるか。
  - 我が国における「サイバーセキュリティ産業」はどのように構造化されるのか。市場参加者としてどのような主体があり、それぞれの収益構造はどのように構造化されるのか。
  - その中で、経済安全保障及び産業政策の観点から、我が国セキュリティ企業が抑えるべき「領域」とはどの部分か（一気にシェアを拡大できる・すべき領域、時間をかけてシェアの拡大を狙うべき領域、現状のシェアを維持しつつ市場拡大の果実を取りに行くべき領域　等）。
  - 「目指すべき姿」の実現までの時間軸をどのように設定するのか。As isの場合、X年後の世界・我が国サイバーセキュリティ産業の姿はどのような状態になっているか。
  - 我が国セキュリティ産業の「振興」とはどのような状態をいうか。定量的な目標としてどのように表現することが可能か（例：「市場規模」は適当な指標と言えるのか）。

    等
- 「目指すべき姿」をどのように実現できるか。
  - これまでのセキュリティ産業振興を目的とした政府の各種施策をどのように評価するか。
  - 米国やイスラエル等において多くのセキュリティ・スタートアップがスケールアップしている実態をどのように評価するか。我が国において同じモデルを取り入れることが可能なのか。我が国の特殊性があるとして、それを考慮した異なるモデルとしてどのような方策があり得るか。
  - 我が国においてスタートアップ製品がより活用・調達されるためには、需要面への働きかけとしてどのような仕掛けが必要か。さらに、そのためにどのような人材育成・確保施策が必要か。
  - 「需要側」は全産業を表象するところ、サイバーセキュリティ産業の振興をもたらす要素を特定するために、どのように細分化して分析するべきか。
  - グローバルなエコシステムに我が国セキュリティ企業が食い込んでいくためには、何が必要か。世界市場を目指すとの発想は、「目指すべき姿」の実現に当たって必要な要素か。

    等

今後検討を深め、今年度中に、我が国サイバーセキュリティ産業の振興に向けた強化策のパッケージを提示

前回のWG3における主なご指摘（抜粋）

- 需要者はセキュリティ要件が揃った製品を求めていると認識すべき。**国のエコシステムを作っていくためのプロジェクトと考えた場合に、これまでの取組から範囲を大きく広げていくべき**。
- 昨今、**経済安全保障の論点が重要**となる中、それを**サイバーセキュリティの観点でどのように考えるか**を今後議論されたい。
- 供給側の支援を行った上で、**それらの製品やサービスをどのように市場へ導入していくか、利用していくかを考えなければエコシステム化につながらない**と考える。
- **製品・サービス市場の見える化について意識的に発信**するとよい。**条件を満たしている会社の製品やサービスを国や自治体が積極的に使うことも重要**である。
- **情報セキュリティサービス審査登録制度**について、既に多くの事業者が参加しているが、制度の基準が低く、使う側からしてかかる制度を活用して問題ないかという点の回答になっていない場合がある。**安心を求めるユーザーの目線から、より高い段階の認定があってもいい**と思う。
- **研究開発、人材育成、体制づくりなどがなければ、取組はアドホックなものとならざるを得ない**。
- **国産ベンチャー製品の海外に対する売込み**を行っているが、**門前払いになる**ケースがある。また、**海外のカンファレンスに展示**しようと思ったが、費用がかかりすぎるため、**あきらめた**という話もある。

これまでの議論と「サイバーセキュリティ産業振興戦略」公開の経緯

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(※1)

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）

3月　「サイバーセキュリティ産業振興戦略」の公開

(※1)経済産業省「ワーキンググループ3（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）」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/enhanced_security/index.html

本戦略における問題意識／我が国セキュリティ産業の現状認識

本戦略における問題意識

- 我が国のセキュリティ産業の発展を後押しすることは、以下のような意義が存在する。

① **産業界のセキュリティ対策の強化**：企業のセキュリティ対策の必要性・ニーズが拡大する中、多様なセキュリティ製品・ツールが市場に流通し、製品選択できることは、**企業が自社のリスクを踏まえ適切なセキュリティ対策を講じる上でも重要**。

② **安全保障上の必要性**：**我が国特有のサイバー攻撃も存在**しうる中で、国内で必要な脅威情報等の蓄積・分析をした上で、必要な製品・サービスが提供されることは、安全保障上も重要。

③ **マクロ経済への貢献**：**デジタル赤字が拡大**する中、その**赤字解消にも貢献しうる**。

我が国セキュリティ産業の現状認識

- 製品開発・提供／サービス提供の2種類が存在。システムインテグレーター（以下、SI事業者）がシステム構築にあわせて製品販売／サービス提供を行う形態が主流だが、そこで**活用される製品は海外製品が中心**となっている。
- **ユーザー企業**は、（機能や技術面よりも、）**これまでの利用実績（特に、政府機関や大手企業）や価格を重視する傾向**。**新興製品・サービス**は利用実績が少なくユーザー企業にとって活用意欲が乏しいため、**新規参入のハードルが高い**。
- また、（商流の中心となる）SI事業者から取り扱われる機会も限られており、**販路拡大が十分でなく、事業スケールも小規模**なものにとどまっている。こうした状況下では、**設備・事業への継続的な投資や製品・サービスの競争力強化が困難。**
- 結果として**、我が国セキュリティ産業は、「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**に陥っていると考えられる。**海外諸国による政策や事業者による業界活性化のための取組**が進められている中で、**セキュリティ産業における悪循環を打破する取組を講じる**必要がある。

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

①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

②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

③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 ⇒P.15～P.17

■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 ⇒P.18～P.23

- 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。

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

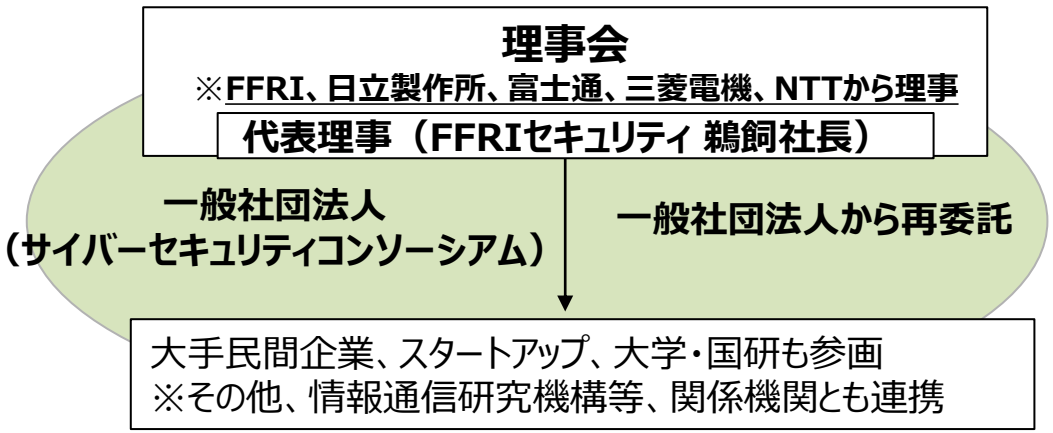
経済安全保障重要技術育成プログラム「サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」

- 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

今後の取組の方向性

＜研究成果の社会実装に向けて＞

1.高度なマルウェア解析技術を用いたツール開発：マルウェアの機能的特徴を自動的に抽出する技術や、効率的な暗号化アルゴリズム分析技術を用いた高度なマルウェア解析技術のツールを開発する。研究成果はサンドボックスとして販売する等、実装手段についても検討する。

2.高度なサイバー攻撃検知技術を用いた検知・防御サービス：高度かつ未知のサイバー攻撃に関する兆候や脅威を早期に検知するための技術を開発し、ユーザに通知する等の機能と合わせて深刻な脅威から防御するサービスとして実装することを検討する。プロジェクトで開発されたセンサー等の情報収集の仕組み、攻撃検知ロジック、攻撃対処の一元管理システム、大量データ収集・分析基盤システムを統合的に管理することを検討する。

3. 高度なサイバー攻撃に対応可能なインテリジェンスサービス：インシデント情報、攻撃者・攻撃手法・攻撃対象、マルウェアの設計実装情報等のサイバー脅威に関わる情報を大規模かつ広範囲に収集・蓄積し、高度なAI技術を用いた分析結果を提供するための手法を開発するとともに、サービスとして提供する手段を検討する。本プロジェクトで開発した、情報集約・連携するためのSTIX/TAXIIを用いた共通様式を用い、様々な対象から幅広く収集した大量の情報を、高度分析プラットフォームにおいて統合的に分析・管理し、サービス提供する。

4.高度サイバー人材に関連するサービス：本プロジェクトの研究成果を活用して、ペネトレーションテスト能力や高度なサイバー攻撃に対して防御する能力を養うための仮想環境を用いた演習・訓練サービスの実装を検討する。開発した、AIを用いたペネトレーション技術等を活用し、複数の高度サイバー人材が連携しながら、実践的にサイバー攻撃に対処する能力を養うことを可能にすることを目指す。また、高度サイバー人材の能力評価指標を用いて、人材の知識・スキルを詳細に把握し、不足する知識・スキルに対応した学習・演習・訓練シナリオを自動的に提供することで、能力向上を効果的に達成する手段の提供を目指す。

（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

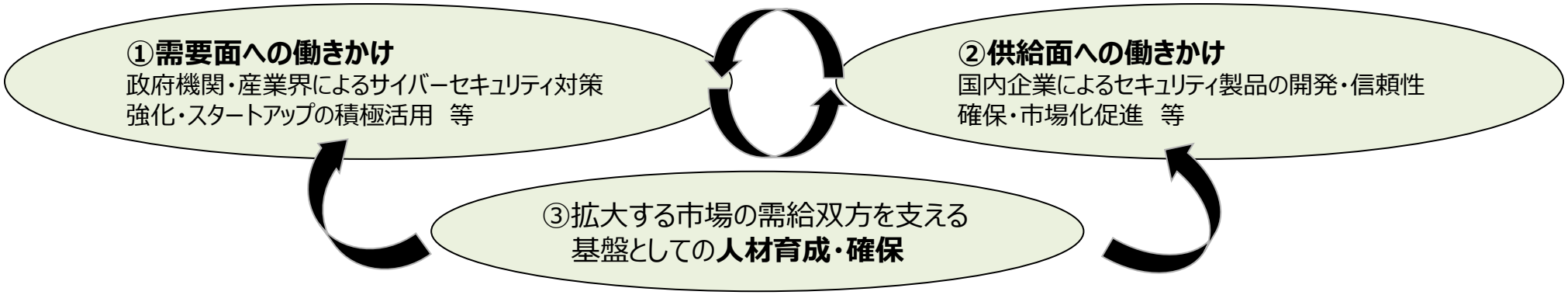
研究項目	①-1 アーティファクト分析	①-2 攻撃主体情報獲得	①-3 未知攻撃早期発見	②-1 AI活用脆弱性探査	②-2 AI活用防御能力向上
主な研究内容	ランサムウェアの解析・自動分類 ランサムウェアの被害を受けたデータの復号技術の開発	サイバー攻撃を行う主体の分析（例：攻撃意図・手口の把握、能力評価）	サイバー攻撃の情報収集や攻撃検知の技術開発AI等を活用した攻撃リスク判定技術の開発 リスクに応じたセキュリティ対応ポリシーの整理	AI等を用いた脆弱性の発見や防御技術の開発	AIを活用したより効率的なペネトレーションテスト（※）の開発 （※） 脆弱性に対する侵入テストを通じて、リスク評価を行い、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

産業サイバーセキュリティ政策における人材育成・確保施策の位置付け

- 経済産業省では、デジタル時代の社会インフラ（デジタルライフライン）を守り、国民生活や経済活動を守るとの観点から、これまでの施策の一層の普及・啓発などに取り組みながら、政府調達等への要件化を通じた**サイバーセキュリティ対策の実効性強化**や、**セキュリティ市場の拡大に向けたエコシステムを構築**、**官民の状況把握力・対処能力向上**に向けた新たな取組も進めることとしている。
- セキュリティ市場の拡大に向けたエコシステムを構築するためには、産業・技術基盤の維持・発展を支える供給側、セキュリティ対策を実装する需要側、双方の基盤となる人材の育成・確保が重要。
- さらに、 NISC改組後の「新たな組織」を含む政府機関等において十分なセキュリティ人材を確保することにより、政府全体でのサイバー安全保障分野での対応能力を向上につなげることも重要。こうしたセキュリティ人材が、産業界に留まることなく、**政府と民間との間でより活発に行き来できるようにすること**も必要。
- こうした視点の下、**セキュリティ人材の裾野を更に拡大していくために必要な施策の在り方を検討する必要。**

＜「セキュリティエコノミー」好循環のイメージ＞



（資料）第８回産業サイバーセキュリティ研究会　資料３より抜粋

サイバーセキュリティ人材の育成促進に向けた検討会議論の全体像

- サイバーセキュリティ人材不足への対応として、本検討会では、既存施策の拡充や改善などを基本として、①セキュリティ・キャンプの拡充、②登録セキスペの活用及び制度の見直し、③中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策、の３つの論点にスコープを絞って議論。

サイバーセキュリティ人材育成の現状

セキュリティに関する知識・スキル水準の程度

トップガン

例）大手セキュリティ企業に就職する者、ベンダーとして起業する者など

高度専門人材

例）規模が大きいユーザー企業のセキュリティ担当者、大手ベンダー実務担当者など

専門人材

例）中堅・中小企業のユーザーのセキュリティ担当者など

※プラス・セキュリティ人材については、セキュリティに関する知識・スキル水準の高低とは別軸であるため、対象外とする。

施策の空白地帯

各層の育成・確保に向けた主な施策

セキュリティ・キャンプ ①

中核人材育成プログラム

登録セキスペ制度 ②

③

政策的な課題

- １年間に**育成できる人数が限定的**であり、スケールしていない。
- 修了後の**状況を追跡できていない**。

- ①実態を伴う**登録セキスペの活躍イメージを提示できていない（活躍の場がない）**場合や、②人手不足の**中小企業と登録セキスペとのミスマッチ**が起きている場合がある。
- 結果として、**登録更新に係る費用を支払うだけの動機が失われ**、登録者数の大幅な増加には至っていない。

- 中堅・中小企業においてサイバーセキュリティ人材が不足している一方、**社内育成・確保は困難**。参考事例もほぼ無い。
- 中堅・中小企業といっても多様であり、必要なセキュリティ対策や体制・人材水準は**各々の状況により異なる**。

対応の方向性

- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする**新たなキャンプを実施**。
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした**コミュニティを整備**。

- **登録セキスペの得意分野・専門領域を可視化したリスト（アクティブリスト）の整備**等を通じた**市場への働きかけ**や、各種制度における登録セキスペ配置の要件化等の**企業側への働きかけ**を多層的に実施。
- **所定の実務経験を有する者を対象に資格更新時の講習の受講みなし制度を導入**する等により、資格維持コストを低減。

- 中堅・中小企業が実施すべきセキュリティ対策に応じた**人材確保・育成の実践的方策を示したガイド（実践的方策ガイド）を整理**し、様々な媒体で広報。
- **自社のセキュリティ対策における現在の立ち位置**、目指すべき姿の**参考となる事例**、人材を「育成」する際に参照できる実際の**セミナー・資格**等も提示。

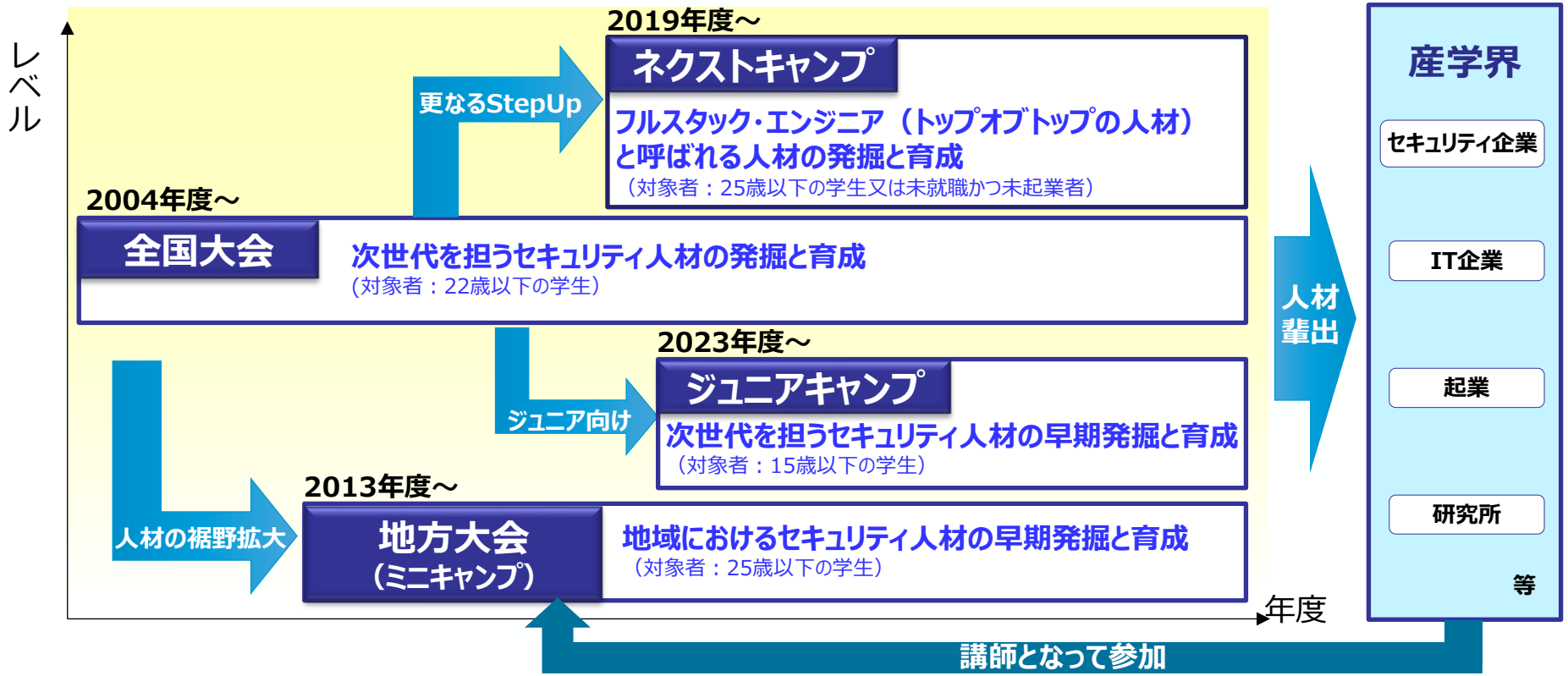
とりまとめに向けた継続議論事項

- 登録セキスペアクティブリストの詳細設計（掲載項目、活用促進策等）、更新講習の「みなし受講」の対象とする実務経験の範囲・判断方法等
- 中堅・中小企業向け「実践的方策を示したガイド」（β版）の策定、来年度におけるβ版の改善活動等（取組事例の収集、有効性の確認、普及方法）

⇒ 引き続きこれらの点について議論を行い、**令和６年度末を目途に①～③に係る具体的政策対応をとりまとめることを目指す**。

セキュリティ・キャンプの拡充

- **若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラスの人材を育成・発掘する**ため、IPAとセキュリティ・キャンプ協議会が開催。計**約1,200名**が修了。
- 今後、裾野の拡大に向けた**新たなキャンプの実施**と、修了生の知見研鑽や活躍状況の共有等を目的とした**コミュニティを整備**していく。



今後の方向性

- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなキャンプを実施。
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的としたコミュニティを整備。

（参考）新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の実施

（１）基本的な考え方

- 「Society5.0」における産業社会において、①サイバー攻撃の起点が拡大するとともに、サイバー攻撃がフィジカル空間に及ぼす影響も増大し、②サイバー攻撃の影響が社会全体に広範に及ぶ可能性がある中、③一部の業界・分野においては、その特性に応じた「サイバーセキュリティ対策」が一層求められる領域＊が生じてきていることから、**サイバーセキュリティに関する知見と、サイバーセキュリティ以外の特定の専門領域における知見をトップレベルで併有する人材が活躍**することで、**特定の専門領域の知見を踏まえた一層充実したサイバーセキュリティ対策の実装や新規ビジネス・技術開発の促進等が可能**になると考えられる。

  ＊　例えば、生成AI分野においては、悪意あるプロンプトを注入することで機密情報を盗む「プロンプトインジェクション」等の新たな脅威が出現しており、こうした特定領域に応じたセキュリティ対策の必要性が高まっている。

- また、現行のセキュリティ・キャンプの応募者の増加にもかかわらず、参加者数が横ばいとなっている状況の中で、**同キャンプの参加時に求められる知見・技術の水準には達しないものの、特定の専門領域における高度な知見・技術を有する者が一定数存在**することもうかがえる。

- こうしたことを踏まえ、セキュリティ人材の裾野の拡大に向けては、**現行のセキュリティ・キャンプの対象者を単純に拡大するのではなく、特定の専門領域における高度な知見・技能を有する者の中からサイバーセキュリティに関する一定の知見を有する者を発掘**し、**サイバーセキュリティに関する知見と、サイバーセキュリティ以外の特定の専門領域における知見をトップレベルで併有する人材を育成**する**新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））**を実施することを検討。

  ※　リソース面において、現行のセキュリティ・キャンプの単純拡大については、演習を提供する側のキャパシティの論点があるところ、新たなキャンプでは、現行のセキュリティ・キャンプとは別途の講師を確保することを想定（特定の専門領域に関する大学等の関係機関との連携を予定）。

  ※　新たなキャンプの対象者については、若年層のセキュリティ人材発掘を目的とする現行のセキュリティ・キャンプと同様に、学生を中心として想定するものの、サイバーセキュリティ以外の特定の専門領域の高度な知見・技能を有している者を対象とすることに鑑み、高等専門学校・大学の専門課程・大学院への在籍者を中心に検討。

  ※　セキュリティ・キャンプ協議会の下にワーキンググループを設置し、新たなキャンプの令和７年度中の開催に向けて、産業界とも連携しつつ検討中。

（参考）新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の実施

（２）新たなキャンプ（セキュリティ・キャンプ・コネクト（仮称））の骨子

開催イメージ

- 対象者：一定水準のサイバーセキュリティに関する知見・技能を有する者であって特定の専門領域における高度な知見・技能を有するもの（高等専門学校、大学の専門課程及び大学院の各在籍者を中心に検討）
- 全体構成：複数の専門領域に関するテーマ（ゼミ）を用意
- 受入れ人数：50人程度
- 開催期間：既存のキャンプ期間（夏休み）と重ならず、対象者が参加しやすい時期（春休みなど）を想定

対象分野の例

○AIとセキュリティ

- AIシステム・サービスの開発・提供・利用それぞれにおいて、どのようなセキュリティリスクが存在するか等をゼミ形式で議論することで、普段AIを研究・開発する立場からもセキュリティを意識して課題を討議し、AIの機密性・完全性・可用性を維持するための合理的な対策や、AIの特性を踏まえた正常な稼働に必要なシステム間の接続等を検討してもらうこと等が考えられる。

詳細制度設計については、セキュリティ・キャンプ協議会の下に設置されているワーキンググループにおいて議論。

（参考）修了生コミュニティの整備

- 修了生がセキュリティ・キャンプへの参加で培った知識・技術・人脈を活用し、**修了年次を超えて相互に、情報交換、議論、交流、パートナーシップ構築等を行う**ことを支援するためのコミュニティを整備する。（→修了生に対する継続的な価値提供）
- **修了生の知見やノウハウを社会に還元**していくために、修了生による情報発信・普及啓発・人材育成などの活動を居住地中心に展開できるよう支援する。講師の立場としてのキャンプへの参画も促進する。（→修了生の知見の社会への還元）（→政府機関等と修了生との連携・協力）
- 修了生が**政府機関や各産業分野におけるセキュリティ対策を先導する人材**として、または、**新規ビジネスの立ち上げや新規技術の開発に携わる人材**として**活躍をしている状況を広報・PR**する。（→セキュリティ・キャンプ自体の価値向上/有効性の確認）
- **令和７年度中に修了生コミュニティを開始**すべく準備を進めていく。

コミュニティ整備の趣旨

① 修了生同士のつながりを強化し相互に知見・技能を研鑽する機会を継続的に提供すること
② 講師の立場としてのキャンプへの参画や政府機関等での活動を含め、修了生の知見・技能を社会に還元していくこと
③ 修了生の活躍状況を対外的に広報・PRすることで、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ること

後方支援等（案）

修了生活躍状況の可視化による産業界へのアピール、裾野拡大支援、など

- 修了生対象のワークショップの開催支援
- 修了生コミュニティへの参加レポートのウェブページ公開
- 政府機関等の施策検討における意見募集・参加案内
- 修了生のキャンプ後の活躍状況のウェブページ公開　等

コミュニティの活動（案）

＊未踏事業：ITを駆使してイノベーションを創出することのできる独創的なアイディアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した人材を発掘・育成することを目的としたIPAが主催する事業。

コンセプト	目的	アクション
社会体験・社会貢献機会の提供	修了生が知識・技術によって「社会に貢献できる」＝「社会での成功体験を積む」機会を獲得し研究開発のモチベーション維持に繋げる	・サイバー技術研究室への参画によるサイバー攻撃情報の調査・分析/OSS開発など ・脆弱性情報の届け出
		・情報セキュリティ10大脅威選考への参加 ・情報セキュリティ白書コラムの執筆
	修了生の地元におけるサイバーセキュリティの有識者候補として、知名度の向上と人脈形成の機会を獲得	・講師としてミニキャンプ参加 ・チューターとしてミニキャンプへ参加
情報発信・情報交換機会の提供	修了生が活動状況/研究成果を発表する機会を得る	・キャンプフォーラムへの参加
	セキュリティ・キャンプの修了年次を超えた人脈形成、および同世代のIT人材との交流機会を得る	・修了生イベントへの参加 ・未踏発企業との交流/連携 ・講師/チューターとの情報交換
知識・技能の向上	修了生の”学び欲”を満たすとともに、起業等へのステップアップも目指す	・ミニキャンプの聴講 ・修了生対象のワークショップ開催 ・未踏事業イベントへの紹介/勧誘

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【裾野の拡大】

- ✓ 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。