令和5年度
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

PwCコンサルティング合同会社
令和6年3月29日

目次

※ 第2章までの調査・検討を基にサイバーセキュリティ産業振興を官民挙げて行っていくための共通の指針となるビジョンの原案を3章以降に掲載する。

1　調査概要

- 本事業では、官民が一体となった共通の目標に向けた取組の指針を示すことをゴールに据え、サイバーセキュリティ産業の振興に関する国内外の事例や論点等の調査や、「サイバーセキュリティ産業政策ビジョン」の原案作成を支援する。

背景1

政府では、2018年からWG3等でサイバーセキュリティ産業のビジネス化の検討を行ってきたが、未だ諸外国と比して国内外で活躍するサイバーセキュリティ産業が創出されたとは言い難い。

- 産業サイバーセキュリティ研究会WG3の活動の一環で、セキュリティ製品の有効性評価、コラボレーションプラットフォーム、情報セキュリティ審査登録制度等の政策パッケージを展開してきたが、国産サイバーセキュリティ産業育成の決定的な打開策にはなっていない。
- 一方、諸外国ではゼロトラストアーキテクチャやクラウドセキュリティ等の分野でスタートアップ企業が台頭している。

背景2

国際情勢の複雑化、社会経済構造の変化等により、我が国では経済安全保障の重要性が増しており、特定重要設備のサイバーセキュリティにおいて「セキュリティ自給率」の向上が求められる。

- 国家主導で作成されるガバメントマルウェアや国家による未知の脆弱性の囲い込みが懸念される中、特定の重要設備において、海外のセキュリティ技術への依存度が高い場合、我が国の安全保障が脅かされる恐れがある。
- 国家支援の攻撃者による高度なサイバー攻撃に対抗するためには、コア技術に係るノウハウ・知見を蓄積する必要がある。

目的

本事業の目的について、サイバーセキュリティ産業ビジネス化の課題明確化、官民の共通認識醸成、取組指針策定、と認識。

- **国内外の事例や論点等を調査することにより、ビジネス化における根本的な課題を明確にする。**
- **国産サイバーセキュリティ産業育成の必要性・重要性に関して、政府・産業界・国民に共通認識を醸成する。**
- **「サイバーセキュリティ産業政策ビジョン」の原案作成を通じ、官民が一体となって共通の目標に向かって取り組める指針を示す。**

1.2 実施項目・実施概要

- 本調査では、各調査項目についてデスクトップ/ヒアリング調査で必要な情報を収集した上で、諸外国と日本の比較分析を実施した。そして、その結果を踏まえ、今後の経済産業省におけるサイバーセキュリティ産業政策の展開の方向性や施策案について、サイバーセキュリティ産業ビジョン原案の形で取りまとめを行った。

		Step1 デスクトップ調査	Step2 ヒアリング調査	Step3 考察・ビジョン原案作成
調査項目	諸外国	• 調査対象国のサイバーセキュリティ産業育成政策の目的、ターゲット、育成スキーム、所管省庁、予算等 • 調査対象国のサイバーセキュリティ産業の市場規模・成長率、人材、有力なプレーヤーとその主要領域 調査対象国については米・中・英・EU・イスラエル・韓国	• デスクトップ調査では得られにくい、**各国政策の背景や評価に係る情報**を調査 – 調査対象国の各種サイバーセキュリティ産業育成政策の目的・ねらい – サイバーセキュリティ産業政策の評価・成果	【考察パート】 • 諸外国/日本の政策やそのねらい・効果について、**①需要側**(サイバーセキュリティ対策の強化、国際協調の推進)、**②供給側**(研究力・技術力の強化、独立性確保、国内事業者の確保・支援)、**③人材育成に分けて比較検証**を行う。 • **日本とグローバルの市場規模や産業競争力等**についても、①需要側、②供給側、③人材育成の観点からそれぞれ**データによる比較分析**を行う。 【ビジョン原案パート】 • 上記比較分析の結果と有識者へのヒアリング結果を踏まえ、産業ビジョン原案として、**日本のサイバーセキュリティ産業の課題と目指すべき将来像について整理**。 • 特に国内企業がシェアを拡大する必要のある領域等にも言及しながら、**将来像の実現に向けて今後講じる必要のある施策についても提案**。
	日本	• 日本のサイバーセキュリティ産業育成政策の検討経緯、支援施策のターゲット、スキーム、所管省庁、予算等 • 日本のサイバーセキュリティ産業の市場規模・成長率、人材、有力なプレーヤーとその主要領域	• デスクトップ調査では得られにくい、**政策の評価や支援対象側のニーズ**を調査 – 企業の側から見た日本のセキュリティ産業の現状(機会発掘意欲や課題)及び効果に関する認識、優先事項やニーズ	
調査手法		• 調査対象国/日本のサイバーセキュリティ産業に関する政策文書、最新の支援施策等の要綱、予算書等を調査 • 調査対象国/日本のサイバーセキュリティに関する市場レポート等をを調査 • その他、PwCでアクセス可能なデータベースを活用し企業情報・業界情報を補完	• PwCのサイバーセキュリティ部門が有するリレーションも活用し、国内外の有識者等へのインタビューを実施 • 国内については、主要セキュリティベンダー関係者に対してもインタビュー調査を依頼	

2 サイバーセキュリティ産業に関する調査

2.1

調査対象・方法

2.1.1 デスクトップ調査対象国・調査方法

- “国家的にサイバーセキュリティ戦略の強化を進めている”、”国際的に有力なプレーヤーを有する”、といった観点から、米国、EU、中国、イスラエルの4か国に加えて、韓国、英国を追加し、合計6か国の調査・分析・考察を行う。

対象国・地域		選定理由・特徴
米国	• 仕様書指定調査対象国 • サイバーセキュリティを国家戦略の一部として捉え、産学官で取り組みを進める国家	• GAFAM、Ciscoなど、サイバーセキュリティ分野でのリーダー企業が多数存在。 • 連邦情報セキュリティ管理法(FISMA)やサイバーセキュリティ情報共有法など、サイバーセキュリティ関連の法律や規制を定期的に見直し、更新。
中国		• デジタル経済大国として急速に成長。アリババ、バイドゥ、テンセントなどの大手IT企業が存在。 • 「中国製造2025」などの国家戦略において、サイバーセキュリティ技術の自主開発や産業の育成を強調。国家全体でサイバーセキュリティ産業の育成に取り組む。
EU		• 「EUサイバーセキュリティ戦略」を策定。「EUサイバーセキュリティ庁(ENISA)」によるEU各機関・各加盟国への助言や支援の提供に加え、欧州危機対応リエゾン(EU- CyCLONe)による大規模サイバー攻撃への対応支援などの強化策を明確化するなど欧州レベルでの制度設計を進める。
英国		• 定期的に国家サイバーセキュリティ戦略を発表。サイバーセキュリティに関する法律や規制も整備。 • National Cyber Security Centre (NCSC) が情報提供、技術サポート、イベント開催を通じて、産業の育成を後押し。
イスラエル		• イスラエル政府はサイバーセキュリティ分野の研究開発や起業を積極的に支援しており、資金提供や税制優遇、人材育成プログラムなどの政策を実施。米欧諸国との協力の深化も進める。 • 情報組織等、技術力を持つ政府機関出身の専門家が民間セクターでの企業や技術開発に寄与。
韓国		• 法的基盤の強化、研究開発の推進、教育プログラムの提供など、国家レベルでの対応が進む。 • 「国家安保室」が中心となって、民・官・軍が連携する体制。民間企業で発生したインシデント情報の共有等は、「未来創造科学部」を経由して、「国家サイバー安全センター(NIS)」へ情報集約。

2.1.1 デスクトップ調査対象国・調査方法

- 当面の実施事項として、調査対象国及び日本の政策/市場に関する調査として各項目建てを行い、デスクトップ調査を実施していく。

大項目	小項目	調査事項
政策関係	サイバーセキュリティ対策の強化	✓ 国のサイバーセキュリティ戦略/政策上の、サイバーセキュリティ産業の保護、振興に関する位置づけ ✓ 国のサイバーセキュリティ戦略/政策上の国家的なサイバーセキュリティのレジリエンスやリスクに係る言及 ✓ 国の重要情報インフラ（防衛システム、銀行・金融、通信、エネルギー、その他）におけるサイバーセキュリティ・システムに関する要件
	国際協調の推進	✓ サイバーセキュリティに関する標準の実施状況 ✓ グローバルなサイバーセキュリティ・アライアンスにおける、自国のサイバーセキュリティプレーヤーの位置づけ（グローバルスタンダードの策定やビジネスアライアンスの観点から、どのように参画しているか）
	研究力・技術力の強化、独立性確保	✓ 自国のサイバーセキュリティ産業の育成のために、政府が支援する研究開発の取り組み
	国内事業者の確保・支援	✓ 国家安全保障／経済安全保障の観点から、サイバーセキュリティ産業を保護するためにとられている政策／措置(外資規制、輸出管理規制等) ✓ サイバーセキュリティ産業を促進するための事業者を対象にした支援政策/施策はあるか。
	セキュリティ人材育成	✓ サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修はあるか。また、政府は、サイバーセキュリティに関する教育プログラムや学術カリキュラムを開発または支援しているか ✓ サイバーセキュリティ業界の労働環境に関する受け止め（魅力的な労働環境と考えられているか、等）
市場関係		✓ 自国のサイバーセキュリティ・プレーヤーで競争力を有する企業、グローバル市場での競争力、競争力ある分野 ✓ サイバーセキュリティ市場規模(日本/グローバル)
その他		✓ 所管省庁 ✓ サイバーセキュリティ予算 ✓ サイバーセキュリティ産業(製品・サービス群)の分類

2.1.2 ヒアリング調査対象者

- 我が国のサイバーセキュリティ産業政策に対して、各分野の有識者・専門家、特にサイバーセキュリティ産業政策に関係すると思われる業界関係者など、経済産業省サイバーセキュリティ課と相談の上、PwCのネットワークを活用してヒアリングを行った。

氏名	組織・役職	専門分野、特徴	実施した日付
梶浦 敏範	日本サイバーセキュリティ・イノベーション委員会　代表理事 日立製作所 上席研究員	経済産業省サイバーセキュリティ研究会WG2座長、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)運営委員会議長、JCIC上席研究員を兼務。	2024年1月11日
柴田 健久	OpenID Foundation Japan 理事	情報処理学会の情報規格調査会 SC 27国内委員会の委員。米国OpenID FoudationのCorporate board menber。	2024年1月12日
匿名	日本IT団体連盟 委員　サイバーインデックス担当者	官公庁や民間企業に対するサイバーセキュリティ戦略立案、サイバー演習、インシデント対応支援、M&A戦略策定に従事。	2024年1月15日
匿名	元 日系大手ソフトウェア企業 欧州事業担当	日系ソフトウェア企業の欧州事業の立上げ・運営などグローバルのテクノロジーに関わる経験を持つ。	2024年1月18日
岡田 満雄	Capy Inc. Founder and CEO	2012年にCapy Inc.をデラウエア州に設立。2017年に日本国内の事業拡大に伴いCapy株式会社を設立。	2024年1月24日
崎村 夏彦	Chairman, OpenID Foundation	日本情報経済社会推進協会データ流通促進WG委員など多数	2024年2月7日
伊藤 公祐	IoTセキュリティ普及啓発団体(CCDS)事務局長、WG主査、JPNIC理事	約15年に渡り、様々なIoTセキュリティガイドライン策定や普及活動に従事し欧米のIoTセキュリティ規制や国際標準要件に精通。	2024年2月8日
林 彦博	Panasonic PSIRTの創設者兼代表	セキュリティ診断・リスクアセスメント・ガイドライン策定・グローバルガバナンス・製品を中心したセキュリティ・インシデント対応などを推進。	2024年2月8日
足立 照嘉	APRIO Technologies(英)CEO	ロンドンを拠点に活動するサイバーセキュリティ専門家。国内外の通信会社やIT企業などのサイバーセキュリティ事業者に技術供給およびコンサルティングを提供。	2024年2月22日

2.1.3 調査対象団体

- 需要喚起、産業競争力強化、人材育成等の政策を実行する上で、経済産業省の政策を補完し、あるいは連携可能な民間団体とのその施策につき、デスクトップ調査等により、調査する。

調査の概要

目的	• 日本の民間団体が実施しているサイバーセキュリティの施策を調査することにより、官民協力等の政策を検討の資とする。
調査対象	• ① 大手企業も含め参画企業が多い等、一定の影響力があり、② サイバーセキュリティ産業（供給側）の競争力強化及び一般企業（需要側）のサイバーセキュリティの強化につき、効果的で、実態があり特徴的な施策を実施している民間団体を選定。 • 特に、産業側の課題へアプローチする施策（人材育成、海外展開支援、技術力向上等）を行っている団体や、需要側である一般企業のサイバーセキュリティ投資を促進する施策（例：中小企業支援、評価制度等）等を行っている団体に焦点を当てる。
調査手法	• 原則としてデスクトップ調査を実施。ただし、有識者へのインタビューで言及があった場合は引用。 • 各団体の施策のうち、産業活性化に資する施策を抽出して整理。経済産業省との補完的役割や連携の可能性についても分析。

調査対象団体の概要

日本ネットワークセキュリティ協会	• サイバーセキュリティベンダーを中心とし、サイバーセキュリティの必要性訴求と関連する諸問題の関係者間の解決のため、の団体。サイバーセキュリティについての調査研究、知識の共有、海外進出促進、人材育成等の施策を実施。
日本IT団体連盟	• ベンダー（供給側）の企業やベンダー参加の団体が参加。ITに関する政策提言・要望、サイバーセキュリティ強化等の諸施策を実施。
中小企業サイバーセキュリティ支援協会	• 中小企業（需要側）のサイバーセキュリティ対策強化を目的として、設立。中小企業がサイバーセキュリティ専門家集団と適切なセキュリティ体制を構築する支援を実施。
JPCERTコーディネーションセンター	• 一般企業（需要側）向けに、サイバーセキュリティインシデントへの対応支援、企業への助言等を目的とし発足。サイバーセキュリティインシデントについて、 報告の受付、対応の支援、分析、再発防止対策の検討や助言などを実施。海外のCSIRTとも連携。
重要生活機器連携セキュリティ協議会	• 生活に密接に関わる重要なIoT機器・システムのセキュリティ強化を目的とし設立。主にベンダー（供給側）の企業等が参加。IoT機器のセキュリティ向上のため、認証制度創設、関係者間での技術開発、人材育成等を実施。

2.2

諸外国におけるサイバーセキュリティ産業振興政策の調査

2.2.1 米国・中国・欧州・英国・韓国・イスラエルのサイバーセキュリティ戦略・施策を踏まえた諸外国の政策の潮流

- 諸外国のサイバーセキュリティ政策について調査し、その主な潮流を総括する。
- 諸外国では、サイバーセキュリティ対策の強化として、重要インフラ、サプライチェーンの対策強化等を実施しており、ハードローによる規制強化も実施、国際協調の推進として、自国初の標準や外国における能力開発支援等も実施するという潮流がみられる。

① サイバーセキュリティ対策の強化

諸外国の潮流考察

【国家安全保障とサイバー空間におけるレジリエンス確保】

- 諸外国のサイバーセキュリティの**国家戦略の策定**における共通項として、**国家安全保障とサイバー空間における主権・レジリエンスの確保**への言及があり、その観点から**重要インフラの保護**が特に強調されている。
- 2大国である米中に着目すれば、まず米国は政府機関のシステムについて大統領令を基に対策の強化を要請し、法的な整備に加えて、国際的にもブランド力の高い米国の**標準技術研究機関（NIST）が政府の要請を満たすための標準策を策定**し、それら標準を担ぐ**国内ベンダーによる市場原理をも活用**しながら、その延長線上に**重要インフラ、サプライチェーンの対策強化**を進める戦略と見ることができる。中国も、政府による法令に基づく要請と**中国発のセキュリティ規格・認証を広めよう**としており、米国の戦略に類似しているといえる。

【政府機関のサイバーセキュリティに関する権限強化】

- 近年、諸外国では**サイバーセキュリティ庁もしくはそれ相当の機関の権限強化**が進んできているといえる。米国のCISA、EUのENISAなどがその例である。中国は、中央サイバーセキュリティ弁公室・国家インターネット情報弁公室の指導的立場にあり、韓国も中央集権型のサイバー態勢をとる（韓国は大統領室配下に権限が集約しているのに加え、国家サイバー安全保障センターがサイバー空間の防御において、官・民・軍の連携を推進する）英国はGCHQ下のNCSCが過去6年推進してきたActive Cyber Defense（ACD）による早期脆弱性の探知とアラートが功を奏しているという評価がされている。いずれの例をみても、国の強力なサイバーセキュリティ庁、もしくは相当の機関の態勢強化が進んでいる。

【その他】

- EUは**EU市民の権利保護を強調**するところに特徴があり、サイバーレジリエンス法（案）に代表されるように、**ハードローによる強制力を伴ったセキュリティ要請をメーカー側に課す**ことで、グローバルでの影響力を行使している見ることができる（GDPRの成功体験がある）。
- 地政学的な要因から、韓国およびイスラエルは**官・民・軍が一体となった協力体制**と施策に特徴がみられる。

② 国際協調の推進

諸外国の潮流考察

【国際的なプレゼンスの強化】

- 前述のとおり、米国・中国は、自国発の標準・認証推進に積極的であり、グローバルプレーヤーがいる米国は、**市場原理に基づき、グローバルに自国発の標準が展開されていく**という強みがある。
- グローバルサウスを主な対象として、**外国へのサイバーセキュリティ能力開発支援**がホットトピックであるところ、米国と中国はこの点でも競いあっている。（中国の支援における経済パッケージが魅力的であり、米よりも優位な立場にあるという見方ある）
- 英国は、AUKUS、ファイブアイズ、NATOなどの軍事的**アライアンスでのプレゼンス**が高く、英国初のサイバーセキュリティソリューションはこれらネットワークを通じた展開とみることができる。

2.2.1 米国・中国・欧州・英国・韓国・イスラエルのサイバーセキュリティ戦略・施策を踏まえた諸外国の政策の潮流

- 諸外国では、現在のリスクだけでなく、将来のデジタル産業振興で必要となるセキュリティ領域についても研究力・技術力の強化、独立性確保を図っているほか、中小企業向けのサイバーセキュリティ対策支援やスタートアップ支援といった、国内事業者の確保・支援をおこなうという潮流がみられる。

③ 研究力・技術力の強化、独立性確保

諸外国の潮流考察

【次世代技術の開発と一体となったサイバーセキュリティ技術の強化】

- **米国、EU、中国、英国の戦略として、①現在のリスク、②将来のデジタル産業振興で必要となるセキュリティ領域を分析した上で重点分野を指定している。**（セキュリティ特化型製品が起点となるのではなく、AI、ポスト量子暗号、データセキュリティ、プライバシーコンピューティング、第5・6世代移動通信やIoT・自動車通信分野などのデジタル全般の重点分野を特定し、それに組み込んだ形でのセキュリティ産業振興といえる）

④ 国内事業者の確保・支援

諸外国の潮流考察

【企業へのセキュリティ対策強化を背景としてCS需要の創出】

- 米国はそもそも巨大テック企業の存在があるが、**中小企業の脆弱なセキュリティ体制が、サイバー攻撃の踏み台や入口となりうるなどのリスクがあるため、種々の支援策やインセンティブを設けている。**例として、IoT製品サイバーセキュリティラベリング制度である**「USサイバートラストマーク」**もその一つといえる。
- 欧州は、IoT製品を例にとれば、**サイバーレジリエンス法（案）**などハードロー型の規制に基づいて、**高額の罰金可能性も含め、メーカー側に高い義務を課す**形でサイバーセキュリティのルールを設定している。この点、現時点ではすくなくとも、外国のプレーヤーに対して、特段EU内事業者をより利するものとはなっていないものの、**グローバル企業においては、事業展開する市場において一定レベルの統一性をもったルールを策定し、製品やサービスに適用するほうが効率的であるため、欧州市場の高い水準の法規制に対応しようとする結果として、他地域においても、同等レベルのルール策定が進む**という状況がある（GDPRの成功体験）。欧州域内でのサイバーセキュリティに関わる製品・サービスの閾値を高く設定することにより、外国のプレーヤーが欧州独自の市場に対応するだけではなく、そのモデルがグローバルに輸出される（欧州の規制を軸にグローバルに影響力を行使している）とみることができる。
- 米国はまた、**外資投資規制（M&A規制）**や**輸出制限の強化**により、国の知財流出を防ぐ取り組みを強化している。
- EUや中国は**データローカライゼーション（政府や重要インフラ）の要請の強化**や、法令に基づくより強いセキュリティ体制を求めることで、国内リソースが必要な状況が作り出されているとみることができる。

【積極的なスタートアップ支援策】

- 諸外国では、**サイバー分野に関する積極的なスタートアップ支援策**がみられるところである。例として、英国はCyber Runwayを通じて160以上のスタートアップが支援を受けた実績がある。中国や韓国ではサイバーセキュリティ産業開発のための基金を立ち上げており、政府が積極的に支援しているといえる（韓国は準政府機関であるKISAがサイバーセキュリティ産業開発基金の立ち上げに携わり、直近でもサイバーセキュリティ人材育成予算を20%増額の発表を行ったところである）
- 米国はそもそもスタートアップから急成長して巨大ITが生まれるケースにみられるように、**活発なIPO市場**を背景に、元々市場環境自体が起業・スタートアップに適しているといえるが、更に、米政府もスモールビジネス・イノベーション・リサーチ（SBIR）プログラムとして、革新的なサイバーセキュリティ技術の研究開発を行う中小企業に**資金提供の機会を提供**するなどしている。

2.2.1 米国・中国・欧州・英国・韓国・イスラエルのサイバーセキュリティ戦略・施策を踏まえた諸外国の政策の潮流

- サイバーセキュリティ人材育成として、諸外国では、多様な人材の活躍や資格制度の活用等を図るという潮流がみられる。

⑤ セキュリティ人材育成

諸外国の潮流考察	**【多様な人材確保策の実施】** • 新規働き手の確保として、**女性活躍**に言及があるのが米国や英国などであるが、**諸外国においても人材確保が困難**である様子がうかがえる。そのため、諸外国においても**奨学金制度やインターンシップなどを含む種々の支援策**が存在する。 • 米国や中国の戦略ペーパーでは**資格制度**（国の資格制度や民間制度の活用）の活用にも言及。 • 韓国では大学・地方・軍などのセキュリティ教育を推進するため、サイバーセキュリティ人材育成予算を20%増額の発表があったところである。

2.2.1 米国

2.2.1 米国① 戦略の全体像 - 国家サイバーセキュリティ戦略2023

- 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(National Cybersecurity Strategy 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最強の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。同戦略では、5つの柱に基づき、各施策を講じる。

国家サイバーセキュリティ戦略2023(National Cybersecurity Strategy 2023)

5つの柱	具体的な施策
重要インフラ防護 PILLAR ONE	DEFEND CRITICAL INFRASTRUCTURE	• 重要インフラ防護のため、既存規制と調和のとれたサイバーセキュリティ規制の制定する。また、規制対象企業の安全保障を確保を推進する。 • 大統領令14028号に基づき連邦政府・民間機関の集団保護のための行動計画を策定する。 • ゼロトラスト・アーキテクチャ戦略等により連邦システム(IT/OT)の近代化、国家安全保障システム（NSS）保護計画を推進する。
脅威アクターの崩壊と解体 PILLAR TWO	DISRUPT AND DISMANTLE THREAT ACTORS	• 米国外に所在する脅威アクターに対する捜査や制裁を科すため、サイバー犯罪に関するブダペスト条約等国際法の拡大や新たな法執行メカニズムを開発する。 • 官民間インテリジェンス共有を改善し脅威アクターへ「混乱キャンペーン」を実施する。 • ランサムウェアへの対応として脅威アクターの採算がとれないよう、国際協力によりランサムウェア・エコシステム破壊や犯罪捜査による撹乱、攻撃に耐えうる強靭な重要インフラ構築、資金源となる仮想通貨の資金洗浄ができないよう施策を講じる。
セキュリティと強靭性を推進するための市場力の形成 PILLAR THREE	SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE	• 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。 • セキュリティ義務を果たさない受給者・請負業者へは民事訴訟を遂行する。
強靭な未来への投資 PILLAR FOUR	INVEST IN A RESILIENT FUTURE	• 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。 • 非政府標準化団体(SDOs) を支援し、業界リーダーとして、同盟国、学術機関、専門家協会等と提携し、新興技術を保護し、国際的な市場競争を促進、国家安全保障と経済的優位性を保護する。 • セキュリティ人材確保のため、多様性欠如に正面から取り組む。教育にはNICEやサイバーコープス等を活用する。
共通目標追求のための国際的パートナーシップ構築 PILLAR FIVE	FORGE INTERNATIONAL PARTNERSHIPS TO PURSUE SHARED GOALS	• サイバー犯罪に関するブダペスト条約の拡大、世界的なサイバーセキュリティの取り組みを支持する。また国外所在の脅威アクターが法の支配から逃れられない協力的法執行メカニズムを開発する。 • 国際的な同盟国・パートナーとサイバー空間の安全性確保のパートナーシップを推進する(日米豪印戦略対話、IPEF、APEP、3カ国安全保障技術協定等)。また北大西洋条約機構(NATO)を主導し、仮想サイバー・インシデント・システムを構築する。 • パートナーの復旧支援による外交対策等を推進する。

The White House, “National Cybersecurity Strategy 2023” (March 2023)
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

2.2.1 米国② サイバーセキュリティ産業政策調査結果（1/11）

- 大統領令等に基づきサイバーセキュリティ強化を図る。特に政府機関・重要インフラの近代化（ゼロトラスト戦略、セキュアバイデザインの採用）やサプライチェーン強化としてソフトウェア脆弱性管理としてSBOM開発やIoTセキュリティラベル制度導入を推進。

① サイバーセキュリティ対策の強化1/3

項目	方針/対策の方向性	関連する規制/政策
重要インフラのサイバーセキュリティ対策や監視体制の構築	**【重要インフラ】** • ウクライナへ軍事侵攻に先立ち、CISA（Cybersecurity and Infrastructure Security Agency）は、米国企業へセキュリティリスクや対策の説明・勧告する「シールドアップ」キャンペーンを推進・拡大する。 • 重要インフラ保護のため、ゼロトラスト・アーキテクチャー戦略を実施し、**IT・OTインフラを近代化**する。 • 米国国立標準技術研究所（NIST）が開発したNIST Cybersecurity Framework（CSF）は重要インフラ（例えば、防衛システム、金融、通信、エネルギーなど）等が**採用すべきサイバーセキュリティシステムに関する要件**が定められている。 • 連邦省庁が**最低限のサイバーセキュリティ要件実施**等の法的権限がない場合、政権は議会と協力し法的権限を持たせるよう支援する。**重要インフラに対するサイバーセキュリティ規制※を設定するにあたり、セキュア・バイ・デザインの原則の採用**する。 ※なお、規制は、既存のサイバーセキュリティフレームワーク、自主的な合意基準、ガイダンス（CISAのサイバーセキュリティー・パフォーマンス・ゴールズ（CPGs）、NISTの重要インフラのサイバーセキュリティ向上のためのフレームワークなど）を活用する。	➢ 「シールドアップ」キャンペーン 世界情勢を鑑み政府が米国企業へセキュリティリスクや対策の説明・勧告する取り組み ➢ ゼロトラスト・アーキテクチャー戦略 ➢ NIST CSF NISTにより策定、米政府が承認したサイバーセキュリティリスク管理標準。ガイドライン、ベストプラクティスのセットを提供する自主的なフレームワーク。
	【政府機関システム】 • 米国行政管理予算局(OMB)はCISAと連携し、連邦文民行政機関（FCEB）システムの安全確保のため行動計画を策定する。本計画は、**大統領令14028号「国家のサイバーセキュリティの改善」に基づき**、NISTと強調しソフトウェア・サプライチェーンリスク軽減目標として、ソフトウェア部品表（SBOM）、セキュア・ソフトウェア開発フレームワーク、オープンソースソフトウェアのセキュリティ向上などに取り組む。 • 連邦政府は、脆弱なIT・OTシステムを交換／更新する必要があるとして以下施策をあげている。 ✓ **ゼロトラスト・アーキテクチャー戦略**は、**多要素認証導入、データ暗号化、攻撃対象面全体可視化、権限・アクセス管理、クラウド・セキュリティ・ツール採用を指示**し、10年以内にレガシー・システムを撤去／リスク軽減のマイルストーンを特定（クラウドベースのサービスへの移行を加速） ✓ **FCEBシステム近代化ライフサイクル計画を策定**、維持コストが高く、脆弱なレガシーシステムを排除 ✓ 連邦政府の最も機密性の高いデータを保存・処理する国家安全保障システム(NSS)へ、内部脅威、サイバー犯罪者、国家敵対者を含む広範なサイバー的・物理的脅威から保護する施策を推進	• 大統領令14028号「国家のサイバーセキュリティの改善」 • ゼロ・トラスト・アーキテクチャー戦略 • NIST SP800-53

2.2.1 米国② サイバーセキュリティ産業政策調査結果（2/11）

① サイバーセキュリティ対策の強化2/3

項目	方針/対策の方向性	関連する規制/政策
中小企業、サプライチェーン別の対策強化	**【政府調達・助成金】** • 大統領令第13526号、第12968号、保全行政責任者指令6号等に基づき、国家機密へアクセスできる者を認定する**セキュリティクリアランス制度を整備**されている。 • 米国防総省（DoD）は、**保全が必要な情報（CUI）を取り扱う全ての調達先企業（海外下請負を含む）にNIST SP800-171の要求事項を満たすことを要請**している。 • 政府システムで使用するクラウドサービス事業者が満たさなければならないセキュリティ認証制度**FedRAMPを設定**※している。 ※FedRAMPの要求事項に関する基準はNIST SP800-53「情報システムと組織のセキュリティとプライバシー管理」 • 米国中小企業庁（SBA）は、中小企業のサイバーセキュリティ強化のため、州や政府機関に対して、**中小企業向けサイバーセキュリティ試験助成金を提供**している。 • 民事サイバー詐欺イニシアチブ(CCFI)では、偽請求法に基づく司法省の権限を利用して、サイバーセキュリティの義務を果たさない政府助成金提供者や請負業者に対する民事訴訟を遂行する。 （例：欠陥あるサイバーセキュリティ製品やサービスを故意に提供、サイバーセキュリティの慣行やプロトコルを故意に虚偽表示、サイバーインシデントや侵害を監視・報告する義務を故意に違反） **【IoT】** • 大統領令14028に基づき**IoTセキュリティ・ラベリング・プログラムを推進**する。消費者がセキュアなIoT製品か判別できるIoTセキュリティ・ラベルを拡大し、IoTエコシステム全体のセキュリティ向上を目指し、市場のインセンティブを生む。 **【ソフトウェア・サービス】** • 連邦政府は、議会・民間部門と協力し**ソフトウェア製品・サービスに対する賠償責任を確立する法律**※を策定する。※市場支配力の高いメーカーやソフトウェア企業が契約による責任放棄を防ぐ注意基準を確立 • ソフトウエア製品やサービスを安全に開発・保守企業の責任を免除する適応可能なセーフハーバーの枠組み※開発を推進する。※セーフハーバーはNISTの安全なセキュアソフトウェア開発フレームワーク (SP 800-218)等を参照 • 協調的な脆弱性開示を奨励し、SBOMのさらなる開発・使用を促進し、重要インフラに使用する未サポートのソフトウェアリスクを特定し、リスク軽減プロセスを開発する。 **【重要インフラ：医療】** • 医療保険の携行性と責任に関する法律（HIPAA）：電子化した医療情報に関する**プライバシー保護・セキュリティ確保について定めた法律**で、該当情報を取り扱う事業者は、遵守しなければならない。	➢ セキュリティクリアランス制度 ➢ NIST SP800-171 ➢ FedRAMP ➢ 中小企業向けサイバーセキュリティ試験助成金 ➢ 民事サイバー詐欺イニシアチブ(CCFI) ➢ IoTセキュリティ・ラベル ➢ 医療保険の携行性と責任に関する法律（HIPAA）

2.2.1 米国② サイバーセキュリティ産業政策調査結果（3/11）

① サイバーセキュリティ対策の強化3/3

項目	方針/対策の方向性	関連する規制/政策
セキュリティ意識の向上、対策への投資拡大	• Stop Think Connect：2010年より開始された、**デジタル市民がインターネット上で安全に過ごせるよう支援するオンライン安全啓発キャンペーン**で、毎年10月に開催される。アンチフィッシング協議会（APWG）が主導し、各国政府・非営利団体・業界とのパートナーシップを発展させる。	➢ Stop Think Connect
政府サイバーセキュリティインシデントや攻撃に対する迅速な対応体制や戦略	• 1998年大統領令PDD-63に基づき、重要インフラ業界毎にサイバー脅威の情報共有団体ISAC（Information Sharing and Analysis Center）が設置される。 • NISTは全国脆弱性データベース（NVE）を公表し、政府系研究開発機関であるMITREは、MITRE ATT&CKでは実際のサイバー攻撃手法と被害を分析し攻撃者の使用する戦術・技術を公表している。これらを基に組織は、自組織におけるサイバーセキュリティ対策を見直すことができる。 • NIST SP 800-53やNIST CSFにサイバーインシデントにおける復旧計画やインシデント対応チームの設置や対応等が規定されている。 • 2022年、重要インフラストラクチャー向けサイバーインシデント報告法(CIRCIA）が制定、重要インフラ事業者に対しサイバー攻撃認知後に72時間以内、ランサムウェア身代金を支払い後に24時間以内の報告を義務付け。 ✓ 2021年6月米国ニューヨーク州金融サービス局（NYDFS）はランサムウェアガイダンスを公表、インシデント発生後72時間以内の報告を義務付け。 ✓ 2023年6月米国証券取引所（SEC）、重大なサイバーセキュリティインシデントについて4営業日以内に現況報告を義務付け（Form 8-K、6-K）。 • 国家サイバーセキュリティ戦略では、壊滅的なサイバーインシデント発生による経済不安定化などを考慮し、市場に確実性を提供し、国家をより強靭にするサイバー保険市場支援、構造を評価するとしている。	➢ 大統領令PDD-63 ➢ NVE ➢ MITRE ATT&CK ➢ 重要インフラストラクチャー向けサイバーインシデント報告法（CIRCIA） ➢ 国家サイバーセキュリティ戦略2023
その他	**【脅威アクターの崩壊と解体】** • 米国外に所在する脅威アクターに対する捜査や制裁を科すため、**サイバー犯罪に関するブダペスト条約**等国際法の拡大や新たな法執行メカニズムを開発する。 • 官民間インテリジェンス共有を改善し脅威アクターへ「混乱キャンペーン」を実施する。 • 脅威アクターの採算がとれないよう、国際協力によりランサムウェア・エコシステム破壊や犯罪捜査による撹乱、攻撃に耐えうる強靭な重要インフラ構築、資金源となる仮想通貨の資金洗浄ができないよう施策を講じる。	➢ 国家サイバーセキュリティ戦略2023

2.2.1 米国② サイバーセキュリティ産業政策調査結果（4/11）

- 米政府のセキュリティ標準・基準（例：高度暗号技術（AES）やNIST CSF）や米国セキュリティ民間団体発行の業界ガイドラインは海外民間企業でも採用されている。また、政府の二国間・多国間パートナーシップも手広く実施し、国際協力を推進している。

② 国際協調の推進 1/3

項目	方針/対策の方向性	関連する規制/政策
国際的なサイバーセキュリティ基準や協定の策定・参加 1/2	**【政府主導の国際基準】** • 高度暗号化技術（AES）は、無線LAN・インターネット通信に用いる暗号アルゴリズム。政府標準規格として米国国立標準技術研究所（NIST）が公募・評価・採用する。AESは欧州暗号規格NESSIEや日本CRYPTRECの電子政府推奨暗号リストにも採用、国際的に共通鍵暗号の標準となっている。 • 米重要インフラで使用されるフレームワークであるNIST CSF（National Institute of Standards and Technology Cybersecurity Framework）は、様々な国・民間企業で参照されており、本書は、サイバーセキュリティ関連の国際標準（ISO, ITU, IETF, IEEEなど）を参照し開発されている。 • （再掲）米国防総省は、保全が必要な情報（CUI）を取り扱う全ての調達先企業にNIST SP800-171の要求事項を満たすことを義務化しており、米国防総省と取引する企業（海外下請負を含む）は、同ガイドラインに準拠する必要がある。日本の防衛装備庁においても、NIST SP800-171をベースとする防衛産業サイバーセキュリティ基準を設け、防衛システムにおけるサイバーセキュリティ確保を目指しており、標準化する可能性がある。 **【民間主導の国際基準推進】** • 米国に所在する自動車技術者協会（SAE）は、車両のライフサイクル全体を通じてサイバーセキュリティ活動に関するプロセスを定義するサイバーセキュリティガイドラインを**2019年に国際標準（ISO/SAE 21434）へ格上げし、義務化**するべく推進している。 • 米国クレジットカード会社4社・日本クレジットカード会社1社による**クレジットカード業界の情報セキュリティ基準（PCI DSS）**を作成、**クレジットカード情報取り扱うシステムで採用が義務化**されている。 • アプリケーションセキュリティ確保を目的とする米国サイバーセキュリティ団体OWASPのOWASPTop10等アプリケーション開発におけるセキュリティガイドラインは最低限講ずるべき対策として国際的に活用される。 • 米国クラウドセキュリティアライアンス（CSA）は、**一定のクラウドセキュリティレベルを保証するための認証制度（STAR）を独自で開発提供**しており、世界的に活用されている。 • 生体認証によりセキュリティ確保を促進する米国FIDO Allianceは、**FIDO認証のオープンで拡張性と相互運用性があるメカニズムを定義する技術仕様**を開発し、標準化を目指している。 • ファースト（FIRST）は、全世界のCSIRT連携を目的とした国際フォーラムで、インシデント対応や情報共有に関するガイドラインなどを提供し、国際的に活用されている。 • Anti-Phishing Working Group（APWG） は、フィッシング等により引き起こされるBEC詐欺や個人情報漏えいについて、インシデント分析・情報連携を行う国際的な団体。Stop Think Connectを主導。	➢NIST CSF

② 国際協調の推進 2/3

項目	方針/対策の方向性	関連する規制/政策
国際的なサイバーセキュリティ基準や協定の策定・参加 2/2	**【二国間・多国間パートナーシップ】** 二国間・多国間パートナーシップではデジタル・エコシステムを守るため、①サイバー脅威情報の共有、②サイバーセキュリティの模範事例の交換、③セクター固有の専門知識の比較、④**セキュア・バイ・デザインの原則の推進**、⑤政策やインシデント対応活動の調整などにより、サイバーセキュリティに関する共通の利益を促進する。 • 日米豪印戦略対話(QUAD)：米国、インド、日本、オーストラリア4カ国による外交・安全保障の協力体制。コンピュータ緊急対応チーム間の情報共有改善、共通価値観に基づくデジタルエコシステム開発含む。 • インド太平洋経済枠組み（IPEF）、経済繁栄のための米州パートナーシップ（APEP）：米国が地域政府とデジタル経済ルールの設定機会を創出する枠組み。技術標準の開発促進、厳格なデータローカライゼーション要件を回避しプライバシー保護する国境を越えたデータフローを可能にするメカニズム、**サプライチェーンのセキュリティ**と強靭性を促進するための活動などを推進する。 • 米英豪安全保障協力（AUKUS）：米国、オーストラリア、英国が、重要技術の安全確保、サイバー協調の改善、先端能力の共有のため緊密に協力する枠組み。 ※なお、自民党の麻生副総裁は、11月13日オーストラリアにてAUKUSへの日本加入を提案している。 • 米欧貿易技術協議会（TTC）：共有する脅威と闘い、デジタル貿易、技術、イノベーションに対する市場アプローチがいかに市民生活を向上させ、より大きな繁栄の力となり得るかを実証するために協調する。 • 国連主導の「サイバー犯罪に関するブラペスト条約」の拡大やサイバー空間を安全にするため支持する。 • 脅威アクターなど敵対者への対応として、米国は、同盟国やパートナーと協力し、デジタル時代に対応した新たな協力的法執行メカニズムを開発する。 • ランサムウェア対策イニシアチブ（CRI）：ランサムウェアの国際協力強化のため米国が呼びかけ30ヵ国以上が参加。2023年1月、オーストラリア主導でランサムウェアタスクフォースを立ち上げ、ランサムウェア攻撃主体等情報共有し、加盟国の破壊活動を支援し、加盟国間の政策・外交努力の同期化を推進する。 **[民間組織含む主なマルチステークホルダー・パートナーシップ]** • クライストチャーチ・コール宣言（CCA）：オンライン上のテロリストおよび暴力的過激派コンテンツを排除するための誓約※国内では、2020年にLINE株式会社が参加声明。 • フリーダム・オンライン連合：オンラインにおける表現の自由やその他の基本的人権を保障すべきとの観点から議論する連合（オーストリア，カナダ，コスタリカ，チェコ，フィンランド，フランス，エストニア，ガーナ，アイルランド，ケニア，ラトビア，モルディブ，メキシコ，モンゴル，オランダ，スウェーデン，チュニジア，英国，米国，グルジア，独，モルドバ，日本※2014年時点） • ジェンダーに基づくオンライン・ハラスメントおよび虐待に関する行動のためのグローバル・パートナーシップ：2022年に米国がデンマーク、オーストラリア、英国、スウェーデンの各政府とともに立ち上げ。 • Stop Ransomware：各国政府・セキュリティベンダーがランサムウェア感染被害対抗のためガイドラインや復号鍵を提供する。	➢ QUAD ➢ IPEF ➢ AUKUS ➢ TTC ➢ CRI ➢ CCA ➢ フリーダム・オンライン連合

② 国際協調の推進 3/3

項目	方針/対策の方向性	関連する規制/政策
国家間での相互承認の仕組みの構築	• 「国際的なサイバーセキュリティ基準や協定の策定・参加1/2」を参照。	
その他	**【民間主導の国際カンファレンス】** 米国では、**民間主導の国際的なサイバーセキュリティカンファレンスが多く開催されており、企業ブースが併設され、セキュリティベンダーが販促活動**をしている。主なサイバーセキュリティカンファレンスとして以下例示する。 <主にIT系> • Black Hat USA • Def Con • APWG • FIRST • RSA conference <OT/ICS> • ICS Security Conference • S4	
	【同盟国やパートナーへの重大なサイバー攻撃支援】 • 米国は重大なサイバー攻撃の被害に遭った**同盟国やパートナー国を支援（インシデント調査、対応、復旧）する**ことで、米国の外交政策とサイバーセキュリティ目標を推進する。米国政府はこれらを可能とするため方針・各省庁の資源の整理など仕組みの構築等を推進する。	➢国家サイバーセキュリティ戦略2023

2.2.1 米国② サイバーセキュリティ産業政策調査結果（7/11）

- サイバーセキュリティ産業振興のため、米国連邦政府は、連邦政府の購買力の活用、また既存の投資プログラムを活用するとしている。研究領域は、暗号技術強化、デジタルIDソリューション・インフラ強化、新たなエネルギーインフラ強化があげられている。

③ 研究力・技術力の強化、独立性確保

項目	方針/対策の方向性	関連する規制/政策
サイバーセキュリティ技術の研究・開発への投資や支援	• 連邦政府は、連邦政府の投資手段、**連邦政府の購買力**、**連邦政府の規制を総合的に活用すること**で、協調的かつ戦略的な技術革新を促進し、**信頼に足る製品やサービスの市場を創出**し、より大きな現代産業・技術革新戦略を支援する。 • 連邦政府はデジタル・エコシステムにおけるサイバーセキュリティを含むすべての災害への強靭性確保のため、既存の投資プログラムである全米科学財団(NSF)の地域イノベーション・エンジン・プログラム、サイバースペースプログラム、超党派インフラ法（Bipartisan Infrastructure Law）、インフレ削減法（Inflation Reduction Act）、CHIPS及び科学法（CHIPS and Science Act）で確立された新しい助成金プログラムおよび資金提供の機会、製造研究所、および連邦研究開発事業の他の要素を活用する。 • 連邦サイバーセキュリティ研究開発戦略計画 (Federal Cybersecurity Research and Development Strategic Plan) の一環として、サイバーセキュリティ・リスクを予防・軽減する研究・開発・実証 (RD&D) コミュニティを特定し、優先順位を付け、触媒作用を及ぼす。各省庁は、人工知能、運用技術、産業制御システム、クラウド・インフラストラクチャ、電気通信、暗号化、システムの透明性、重要インフラで使用されるデータ分析などの分野で、サイバーセキュリティとレジリエンスを推進する研究開発プロジェクトを指示する。これらの取り組みは、NSF、DOE国立研究所、その他の連邦資金による研究開発センター(FFRDC）を含む連邦研究開発事業によって、また学界、製造業者、技術企業、所有者・運営者とのパートナーシップを通じて支援される。 • 重要インフラにおける産官学共同の研究開発はナショナル・サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）やサイバーセキュリティ・マニュファクチャリング・イノベーション研究所（CyManII）で推進される。	➢ 連邦サイバーセキュリティ研究開発戦略計画 (Federal Cybersecurity Research and Development Strategic Plan) ➢ ナショナル・サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE） ➢ サイバーセキュリティ・マニュファクチャリング・イノベーション研究所（CyManII）
自国での技術開発・研究の促進や外国からの依存度の低減	• 連邦政府は、連邦政府の投資手段、**連邦政府の購買力**、**連邦政府の規制を総合的に活用**することで、協調的かつ戦略的な技術革新を促進し、**信頼に足る製品やサービスの市場を創出**し、より大きな現代産業・技術革新戦略を支援するとしており、サイバーセキュリティについては主に「暗号技術の強化」、「デジタルIDソリューションおよびインフラの強化」、「新たなエネルギーインフラのセキュリティ確保」の3つを挙げている。 • （再掲）国家サイバーセキュリティ戦略では、壊滅的なサイバーインシデント発生による経済不安定化などを考慮し、市場に確実性を提供し、国家をより強靭にするサイバー保険市場支援、構造を評価するとしている。	➢ NSM 10「脆弱な暗号システムに対するリスクを軽減しつつ、量子コンピューティングにおける米国のリーダーシップを促進する」覚書 ➢ 国家サイバーセキュリティ戦略2023

2.2.1 米国② サイバーセキュリティ産業政策調査結果（8/11）

- サイバーセキュリティ企業（中小企業等）への資金援助するとともに、民事サイバー詐欺イニシアチブ（CCFI）で脆弱なセキュリティ製品・サービス開発事業者へ民事訴訟する。また、知的財産の国外流出をさけるため、海外投資規制・輸出管理規制を活用する。

④ 国内事業者の確保・支援

項目	方針/対策の方向性	関連する規制/政策
インキュベーション、アクセラレーション、資金提供などのスタートアップ支援	• 米国政府は、スモールビジネス・イノベーション・リサーチ（SBIR）プログラムとして、革新的なサイバーセキュリティ技術の研究開発を行う中小企業に資金提供の機会を提供する。 • （再掲）連邦政府はデジタル・エコシステムにおけるサイバーセキュリティを含むすべての災害への強靭性確保のため、既存の投資プログラムである全米科学財団(NSF)の地域イノベーション・エンジン・プログラム、サイバースペースプログラム、超党派インフラ法、インフレ削減法、CHIPS及び科学法で確立された新しい助成金プログラムおよび資金提供の機会、製造研究所、および連邦研究開発事業の他の要素を活用する。 • （再掲）民事サイバー詐欺イニシアチブ(CCFI)では、偽請求法に基づく司法省の権限を利用して、サイバーセキュリティの義務を果たさない政府助成金提供者や請負業者に対する民事訴訟を遂行する。 （例：欠陥あるサイバーセキュリティ製品やサービスを故意に提供、サイバーセキュリティの慣行やプロトコルを故意に虚偽表示、サイバーインシデントや侵害を監視・報告する義務を故意に違反）	➢スモールビジネス・イノベーション・リサーチ（SBIR）
サービス認定創設、政府調達などの活用などのビジネス機会の創出	• （再掲）連邦政府の購買力と助成金を活用し、セキュリティにインセンティブを与える。 • （再掲）政府は大統領令14028号「国家のサイバーセキュリティの改善」に基づき、IoTセキュリティ・ラベリング・プログラム開発を推進する。IoTセキュリティ・ラベルの拡大により、消費者はさまざまなIoT製品が提供するサイバーセキュリティ保護を比較できるようになり、IoTエコシステム全体のセキュリティ向上を目指す市場のインセンティブを生む。	➢IoTセキュリティ・ラベル
その他	**【海外投資規制や知的財産流出の防止】** • 国家安全保障に不可欠な新興技術や基盤技術の輸出を管理するための新たな権限を米国政府に提供する輸出管理改革法（ECRA）を制定した。 • 外国投資リスク審査近代化法（FIRRMA）を制定し、対米外国投資委員会（CFIUS）による外国投資審査の範囲を、重要技術、重要インフラ、機密個人データへの非支配的投資をカバーするよう拡大。 • 大統領令13873号に基づき、商務長官に、外国の敵対者が所有・支配、またはその管轄権や指示に服する者が設計・開発・製造・供給する情報通信技術やサービスに関わる取引を禁止する権限を与えた。 **【輸出に関する方針】** • 輸出管理改革法（ECRA）として、米国政府は、国家安全保障に不可欠な新興技術や基盤技術の輸出を管理するための権限に関する法律を制定。	➢輸出管理改革法 ➢外国投資リスク審査近代化法 ➢大統領令13873号 ➢輸出管理改革法

2.2.1 米国② サイバーセキュリティ産業政策調査結果（9/11）

- 米国政府はサイバーセキュリティ人材不足解消のため、教育プログラム・奨学金制度などを提供し、新規働き手の確保として、外国人採用誘致や未経験女性の教育プログラムを実施。また、政府職員（DoD）の認定資格として民間資格CISSPが採用される。

⑤ セキュリティ人材育成

項目	方針/対策の方向性	関連する規制/政策
サイバーセキュリティ専門家の教育・トレーニングの支援、資格制度の整備	• 国家サイバー長官(ONCD)は国家サイバーセキュリティ人材・教育戦略の策定と実施を監督する。本戦略は、サイバーセキュリティ教育のための国家イニシアティブ（NICE）、サイバーコープス（CyberCorps）、NSFや他の科学機関で進行中の人材育成プログラムも活用し、連邦政府のプログラムを補強する。 • 米国政府は、サイバーセキュリティに関連する教育プログラムや学術カリキュラムの開発・支援し、例えばサイバーセキュリティ教育にかかる国家イニシアティブ（NICCS）は、サイバーセキュリティに対する認識、教育、訓練、人材育成を促進することを目的に、**約3300件の産官学の教育訓練コースを提供**(2017年時点)。 • （再掲）大統領令第13526号、第12968号、保全行政責任者指令6号等の法規制に基づき、国家機密へアクセスできる人物を認定するセキュリティクリアランス制度が整備されている。 • Certified Information Systems Security Professional（CISSP)は、国防総省指令 8570（DoD Directive 8570）に基づき、特定の職務分類に対する認定資格に指定。 • この他、民間団体が提供するサイバーセキュリティおよびプライバシー関連資格が多く存在する。 例：(ISC)2、ISACA、EC-Council、CompTIA、iapp、Google、AWSなど	➢サイバーセキュリティ教育のための国家イニシアティブ（NICE） ➢サイバーコープス(CyberCorps)政府機関への就職を前提とした奨学金プログラム ➢NISCEサイバーセキュリティ教育にかかる国家イニシアティブ（NICCS） ➢Certified Information Systems Security Professional (CISSP)
サイバーセキュリティ産業の雇用状況・労働環境の改善	米国NICCSの報告によると米国求人状況は以下のとおり（2023年12月1日閲覧時点）。 • 米国内におけるサイバーセキュリティ関連の求人件数は、57万件 • サイバーセキュリティ関連の求人件数は、昨年と比較し35%増加	
新規の働き手の確保策やリスキリングなどの支援策	• 熟練労働者の不足に直面しており、特に黒人、ヒスパニック系、女性など、社会的地位の低いグループの労働者が不足。この不足に対処するため、米国政府は高度な技能を持つ外国人サイバーセキュリティ労働者を誘致するための政策や対策をいくつか実施している。これらの政策には次のようなものがある： – 早期キャリアSTEM研究イニシアティブ：米国国務省教育文化局（ECA）は、研究、研修、教育交流訪問者プログラムを通じて STEM 研究に従事するために米国を訪れる非移民の BridgeUSA 交流訪問者を、企業を含む受入組織との間で促進するイニシアチブを開始した。 – 米国国土安全保障省（DHS）サイバーセキュリティ人材管理システム（CTSM）：CTMSは、連邦政府で働くサイバーセキュリティ専門家の雇用、訓練、維持を改善するために、DHSが2021年11月に発表したシステム。DHSに不可欠なサイバーセキュリティ人材確保・維持を目的としている。 – 非営利団体が推進する「100 日間で100人の女性を育成するサイバーセキュリティキャリアアクセラレータ（100 Women in 100 Days Cybersecurity Career Accelerator）」では、主婦など現在サイバーセキュリティに携わっていない女性を100日間で育成し、大手セキュリティ企業やビックテックのセキュリティ部門へ就職先を紹介する教育プログラム。	➢早期キャリアSTEM研究イニシアティブ（ECA：Early Career STEM Research Initiative） ➢米国国土安全保障省（DHS）サイバーセキュリティ人材管理システム（CTSM） ➢100 Women in 100 Days Cybersecurity Career Accelerator

2.2.1 米国② サイバーセキュリティ産業政策調査結果（10/11）

- 米国では、先端分野における研究開発、重要インフラや製造業のサイバーセキュリティ研究開発、中小企業の研究開発を支援するため、様々なプログラムを実施。

政策名	概要	
連邦サイバーセキュリティ研究開発戦略計画	連邦サイバーセキュリティ研究開発戦略計画（Federal Cybersecurity Research and Development Strategic Plan）の一環として、サイバーセキュリティ・リスクを予防・軽減する研究・開発・実証（RD&D）コミュニティを特定し、優先順位を付け、触媒作用を及ぼす。各省庁は、人工知能、運用技術、産業制御システム、クラウド・インフラストラクチャ、電気通信、暗号化、システムの透明性、重要インフラで使用されるデータ分析などの分野で、サイバーセキュリティとレジリエンスを推進する研究開発プロジェクトを指示する。これらの取り組みは、NSF、DOE国立研究所、その他の連邦資金による研究開発センター（FFRDC）を含む連邦研究開発事業によって、また学界、製造業者、技術企業、所有者・運営者とのパートナーシップを通じて支援される。	Link
ナショナル・サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）	ナショナル・サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）：2012年に設立された国立標準技術研究所（NIST）の一部で、サイバーセキュリティの実用的なソリューションを開発するために、政府や産業界、アカデミアと協力している。NCCoEは、エネルギー、金融、ヘルスケア、製造業などの重要なセクターにおけるサイバーセキュリティの課題に対応するために、既存の技術や標準を組み合わせて実証的なプロジェクトを実施している。	Link
サイバーセキュリティ・マニュファクチャリング・イノベーション研究所（CyManII）	• サイバーセキュリティ・マニュファクチャリング・イノベーション研究所（CyManII）：2020年に設立された公私パートナーシップで、製造業のサイバーセキュリティを強化するために、エネルギー省と産業界、大学、研究機関が協力。CyManIIは、製造業のデジタル化とエネルギー効率化を促進するとともに、サイバー攻撃から製造資産と知的財産を保護するための技術やベストプラクティスを開発している。	Link
スモールビジネス・イノベーション・リサーチ（SBIR）	• 米国政府は、国家サイバーセキュリティ戦略の中で、スモールビジネス・イノベーション・リサーチ（SBIR：Small Business Innovation Research）プログラムとして、革新的なサイバーセキュリティ技術の研究開発を行う中小企業に資金提供の機会を提供する、と言及している。	Link

2.2.1 米国② サイバーセキュリティ産業政策調査結果（11/11）

政策名	概要
連邦政府の補助金プログラム	• サイバーセキュリティを含むすべての災害への強靭性確保のため、重要インフラ（設計・開発・実戦配備・維持）への戦略的投資機会を提供する。超党派インフラ法（Bipartisan Infrastructure Law）、インフレ削減法（Inflation Reduction Act）、CHIPS及び科学法（CHIPS and Science Act）が資金提供するプログラムを通じて、インフラとそれを支えるデジタル・エコシステムへ投資を行う。 • 連邦政府： SLTT団体、民間企業、その他のパートナーと協力して、補助金申請者に対するサイバーセキュリティ要件と技術支援やその他の形態の支援とのバランスを図る。セキュア且つ強靭な設計に基づく重要な製品やサービスへの投資を促進し、製品ライフサイクル全体が強化する。 • 重要インフラ連邦政府： 重要インフラを対象としたサイバーセキュリティの研究・開発・実証(RD&D)プログラムへの資金提供を優先する。また、より優れたサイバーセキュリティの実践を大規模に推進するためのその他のインセンティブ・メカニズムを議会と協力して開発する。 • 連邦政府への販売業者に対する契約要件： 大統領令14028号「国家のサイバーセキュリティの改善」に基づき、サイバーセキュリティに関する契約要件を強化し、連邦政府機関全体で標準化する。調達を通じてサイバーセキュリティ要件を設定、実施、テストするための新しい概念を試験的に導入することは、斬新で拡張性のあるアプローチにつながる。民事サイバー詐欺イニシアチブ(CCFI)は、偽請求法に基づく司法省の権限を利用して、サイバーセキュリティの義務を果たさない政府助成金提供者や請負業者に対する民事訴訟を遂行する（例：欠陥のあるサイバーセキュリティ製品やサービスを故意に提供、サイバーセキュリティの慣行やプロトコルを故意に虚偽表示、サイバーインシデントや侵害を監視・報告する義務を故意に違反）。 • 大惨事が発生した場合： 経済を安定させ、不確実な時代に確実性を提供することは政府の責任である。壊滅的なサイバーインシデント発生時、連邦政府は経済を安定させ、復旧支援を求められる可能性がある。大惨事が発生してから慌てて支援策を練るのではなく、発生前にその対応を構築することで、市場に確実性を提供し、国家をより強靭にする。行政は、既存のサイバー保険市場を支援するような、壊滅的なサイバーインシデントに対する連邦保険対応の必要性と可能な構造を評価する。この評価を行うにあたり、行政は議会、州規制当局、業界関係者からの意見を求め、協議する。

2.2.1 米国③とりまとめ

- 米国のサイバーセキュリティ産業振興政策について特徴・傾向と、その現況・評価。

大項目	小項目	特長・傾向	現況・評価
政策関係	サイバーセキュリティ対策の強化	✓ 大統領令等に基づきサイバーセキュリティ強化を図る。特に政府機関・重要インフラの近代化（ゼロトラスト戦略、セキュアバイデザインの採用）やサプライチェーン強化としてソフトウェア脆弱性管理としてSBOM開発やIoTセキュリティラベル制度導入を推進。	国としてサイバーセキュリティ強化のため、長年取り組んでおり、これまでリスクが高いとされていたサプライチェーンのセキュリティ強化へ本格的に取り組みはじめており、さらなる強靭化がなされてるだろうと評価する。
	国際協調の推進	✓ 米国政府のセキュリティ標準・基準（例：高度暗号技術（AES）やNIST CSF）や米国セキュリティ民間団体発行の業界ガイドラインは海外民間企業でも採用されている。また、政府の二国間・多国間パートナーシップも手広く実施しており、国際協力を推進する。	米国の民間企業は、サイバーセキュリティ技術においてリードしており官民で開発されたベストプラクティス等は国際基準となる傾向にある。またStop Ransomwareなど多国間の取り組みで米国セキュリティベンダーを協力企業として記し、国際的に高い技術を誇る企業として暗に示している。
	研究力・技術力の強化、独立性確保	✓ サイバーセキュリティ産業振興のため、米国政府は、連邦政府の購買力の活用、また既存の投資プログラムを活用するとしている。研究領域は、暗号技術強化、デジタルIDソリューション・インフラ強化、新たなエネルギーインフラ強化があげられている。	既存の投資枠組みを活用することは、新規投資枠組み立案にかける工数を削減できるため良いと考える。 また、重視する研究領域は、現在のリスク・将来のデジタル産業振興で必要となるセキュリティ領域を分析した上で指定している。 そして、政府購買力、すなわち政府調達することを念頭に置き、さらには、支援金提供とともに民事訴訟リスクを同時に企業に提示することで、高品質のセキュリティ製品およびサービス開発を目指せ、国際競争力を高めることが可能となる。 また、知財流出を規制するための法規制も整備されている。
	国内事業者の確保・支援	✓ サイバーセキュリティ企業（中小企業等）への資金援助するとともに、民事サイバー詐欺イニシアチブ（CCFI）で脆弱なセキュリティ製品・サービス開発事業者へ民事訴訟する。また、知的財産の国外流出をさけるため、海外投資規制・輸出管理規制を活用する。	
	セキュリティ人材育成	✓ 米国政府はサイバーセキュリティ人材不足解消のため、教育プログラム・奨学金制度などを提供し、新規働き手の確保として、外国人採用誘致や未経験女性の教育プログラムを実施。また、国防総省職員（DoD）の認定資格として民間資格CISSPを採用する。	サイバーセキュリティ人材の求人件数が継続的に公開されており、安定した業界を要望する学生等にとって動機付けとなる。 また、政府採用前提とする奨学金制度、外国人誘致による人材確保は、大手セキュリティベンダーが多い米国では成功すると推察する（セキュリティクリアランス制度確立されていることもあり） 女性教育プログラムが成功すれば、新規働き手は一層拡大する。
予算 等		✓ 175億USドル（約2兆2737億円）	

2.2.2 中国

2.2.2 中国① 戦略の全体像 - 中国 サイバースペースセキュリティ国家戦略（国家网络空间安全战略、2016年）

- 中国のサイバースペースセキュリティ戦略は、**国家安全保障と発展利益を守る**こと主目的とし、習近平国家主席が提唱する「4つの原則（四項原則）」と「5つの命題（五点主张）」に基づく。戦略文書は、中国政府が認識する現在のサイバー空間における発展機会とリスク課題を示したうえ、戦略の目的、および戦略の4つの原則と、9つの戦略的使命を掲げる。（五点主张の詳細記述なし）

サイバースペースセキュリティ国家戦略（国家网络空间安全战略、2016年）

4つの「原則」		
	サイバー空間の主権の尊重 **尊重维护网络空间主权**	サイバー空間の主権は不可侵で、各国は自国のネットワーク管理と法規を独自に定め、国際的ガバナンスに平等に参加する権利がある。サイバー空間の秩序維持と国家安全の保護が重要で、サイバー覇権主義や他国内政への干渉は許されない。
	サイバー空間の平和的利用 **和平利用网络空间**	サイバー空間の平和的利用は人類共通の利益であり、国際連合憲章に則り、情報技術の悪用やサイバー紛争の防止に協力すべきである。相互尊重と信頼に基づき、調和のとれたサイバー世界を目指し、他国のネットワークやデータへの不当な干渉は避けるべきである。
	法律に則ったサイバー空間の管理 **依法治理网络空间**	サイバー空間において、法の支配を全面的に推進し、インターネットの健全な運営とアクセスを法に基づいて行う。良好なネットワーク秩序の構築、情報流通の秩序正しい保護、個人のプライバシーと知的財産権の保護を重視し、組織・個人が他者の権利を尊重する責任を持つべきである。
	サイバーセキュリティと開発の一体化 **统筹网络安全与发展**	サイバーセキュリティは国家安全保障の基盤であり、情報化は近代化の必要条件である。開発と安全保障は相互に依存し、**安全保障なしの発展は持続不可能で、発展なしでは安全も保証されない。情報技術の発展がサイバーセキュリティ保証の鍵である。**

9つの「戦略的使命」

サイバー空間主権を断固として守る	**ネットワーク文化の強化**	**ネットワーク・セキュリティの基盤強化**
• 法律に基づき国内のネットワーク活動を管理し、情報設備と情報資源の安全を保護する。	• ネットワーク文化の発展を促進し、社会主義の中核的価値を実践。良好なネットワーク環境を構築する。	• 技術革新を推進し、サイバーセキュリティの基盤を強化する。
国家安全保障の断固とした防衛	**サイバーテロと犯罪の撲滅**	**サイバー空間保護能力の向上**
• 国家の安全保障とネットワークの利用に対する脅威を防止し、法律に基づいて対処する。	• サイバーテロと犯罪行為に対して厳重な対策を講じ、サイバーテロと犯罪行為に対抗する。	• 国のサイバーセキュリティ保護能力を強化する。
重要インフラの保護	**ネットワーク・ガバナンス・システムの改善**	**サイバー空間における国際協力の強化**
• 国家安全保障と公共の利益の観点から、重要情報インフラの保護を強化する。	• 法に基づくオープンで透明性の高いネットワークガバナンス体制を確立する。	• サイバー空間における国際対話・協力を強化し、グローバル・ガバナンス・システムに積極的に参加する。

2.2.2 中国② サイバーセキュリティ産業政策調査結果（1/10）

- 中国サイバー三法および戦略に基づき施策を講じる。安全保障観点では、重要インフラ施設のデータローカライゼーションや中国独自のセキュリティ製品認定制度を導入。セキュリティ人材育成プログラムや国民啓発週間により全体のリテラシー向上を図る。

① サイバーセキュリティ対策の強化1/3

項目	方針/対策の方向性	関連する規制/政策
重要インフラのサイバーセキュリティ対策や監視体制の構築	【重要インフラ事業者】 • 2017年6月に施行された中国サイバーセキュリティ法に基づき、**重要情報インフラ施設運営者は、データローカライゼーション（中国領域内で保管）、年度安全評価、レスポンス体制の構築など、より強固な保護対策を講じることが要求**されている。2021年に「**重要インフラ安全保護条例**（中华人民共和国国务院令）」を制定し、**「サイバーセキュリティ法」に定める重要インフラ保護についてより具体化。重要情報インフラ施設の認定**は、内資外資を問わないとしている。 （参照）重要インフラの定義： 公共通信、ラジオ・テレビ伝送などのサービスを提供する基本情報ネットワーク、エネルギー、金融、運輸、教育、科学研究、水利、工業製造、医療・保健、社会保障、公共事業などの分野や国家機関の重要な情報システム（アプリケーション含む） • 「国家サイバー空間セキュリティ戦略（国家网络空间安全战略）」によると、技術と管理、保護と抑止を同等に重視し、識別、保護、検出、早期警戒、対応、廃棄に重点を置き、重要情報インフラ保護のためのシステムを構築・実施し、管理、技術、人材、資金面での投資を増やし、重要情報インフラのセキュリティと保護を効果的に強化するため、法律に基づいて総合的な対策を実施する。 【政府機関システム】 • 2014年に政府は、「党政府機関Website安全管理の強化に関する通知」、「党政府機関クラウドサービスサイバーセキュリティ管理に関する意見」などを次々と発し、政府系サイトの安全を強調し、**党政府機関にデータセンタ、メールサービスの提供、クラウドサービスの提供などは中国国内にあるべきで**あり、**政府調達の際に安全審査を行う。** • 「国家サイバー空間セキュリティ戦略（国家网络空间安全战略）」によると、党・政府機関のウェブサイトと重点分野のセキュリティ保護を強化する。**草の根の党・政府機関のウェブサイトを集中的に構築・運営・管理**する。政府、産業界、企業の間でネットワークセキュリティ情報を共有する秩序あるメカニズムを構築し、重要情報インフラの保護における企業の重要な役割を十分に発揮させる。	➢ 中国サイバーセキュリティ法 中国のネットワークの安全を保障し、ネットワーク空間における主権と国家安全保障、公共の利益を保護することを目的に策定された法律 ➢ 重要インフラ安全保護条例 中国サイバーセキュリティ法に基づき策定された、重要インフラ事業者におけるセキュリティ措置を定めた条例 ➢ 国家サイバー空間セキュリティ戦略（国家网络空间安全战略）中国におけるサイバーセキュリティ戦略 ➢ 党政府機関Website安全管理の強化に関する通知（关于加强党政机关网站安全管理的通知） 中国共産党のWebサイトにおけるセキュリティ施策をさだめたもの ➢ 党政府機関クラウドサービスサイバーセキュリティ管理に関する意見（关于加强党政部门云计算服务网络安全管理的意见） 中国共産党のクラウドサービスにおけるセキュリティ指針

2.2.2 中国② サイバーセキュリティ産業政策調査結果（2/10）

- ①の項目全体の中国の傾向・特徴を記載。

① サイバーセキュリティ対策の強化2/3

項目	方針/対策の方向性	関連する規制/政策
中小企業、サプライチェーン別の対策強化	**【重要インフラ事業者】** • 2017年に政府、**重要インフラが調達する製品とサービスに関する安全審査を行う「サイバーセキュリティ製品とサービス審査弁法」**が施行 • 2017年より、**インターネット重要設備とサイバーセキュリティ専用製品に関する強制認証の対象製品（网络关键设备和网络安全专用产品目录）**および、**認証済みの製品目録（网络关键设备和网络安全专用产品安全认证和安全检测结果发布）を定期的に公表**。 • 2022年、中国データ安全法等に基づき、中国サイバー空間管理局（CAC）を含む13の省庁が「サイバーセキュリティ安全審査弁法」を制定、**重要インフラ、国家安全などに係る場合、製品及びサービスについて国家安全審査**をすると規定。 **【政府機関システム】** • 党・政府機関のウェブサイトと重点分野のセキュリティ保護を強化の一部として、**ネットワークセキュリティレビューシステムを構築・実施**し、**サプライチェーンセキュリティ管理を強化**し、党・政府機関や基幹産業が調達・使用する重要な情報技術製品・サービスのセキュリティレビューを実施し、製品・サービスのセキュリティと管理性を向上させ、製品・サービス提供者やその他の組織が情報技術を利用して不正競争を行ったり、ユーザーの利益を害することを防止。 **【地方政府等】** • ・2021年に、国家発展委員会、CAC、工業情報化部、国家エネルギー省などは、**個人情報を含むビッグデータの安全性と信頼性強化のため、「全国一体化ビッグデータセンター協同イノベーションコンピューティング基幹システム実施プラン」**を公表、地域横断的なデータセンターとして運営し、セキュリティ強化も図る。	➢サイバーセキュリティ製品とサービス審査弁法（网络产品和服务安全审查办法）指定のサイバーセキュリティ製品はすべて国の認定をうける ➢サイバーセキュリティ安全審査弁法（网络安全审查办法）重要インフラ・国家安全にかかわる場合、国が該当企業を審査する権限をさだめた法律 ➢国家サイバー空間セキュリティ戦略（国家网络空间安全战略） ➢全国一体化ビッグデータセンター協同イノベーションコンピューティング基幹システム実施プラン（全国一体化大数据中心协同创新体系算力枢纽实施方案）
セキュリティ意識の向上、対策への投資拡大	• サイバーセキュリティ人材プロジェクトを実施し、サイバーセキュリティ分野と専門分野の建設を強化し、一流のサイバーセキュリティカレッジとイノベーションパークを建設し、人材育成とイノベーション・起業に資する生態環境を形成する。**全国サイバーセキュリティ意識向上週間（国家网络安全宣传周综述）**を開催し、全国的なサイバーセキュリティ広報・教育を精力的に実施する。**教材、学校、教室へのサイバーセキュリティ教育の導入を推進**し、**サイバーメディアリテラシーを向上させ、社会全体のサイバーセキュリティに対する認識と保護能力を高め、ネットユーザーの違法・有害なサイバー情報、サイバー詐欺、その他の犯罪行為を識別し、それに対抗する能力**を向上させる。	➢ 全国サイバーセキュリティ意識向上週間（国家网络安全宣传周综述）毎年9月に国民に対するサイバーセキュリティ啓発週間を実施（2023年は、セキュリティサミットフォーラム、セキュリティ博覧会などのイベントが福建省福州市で開催）

2.2.2 中国② サイバーセキュリティ産業政策調査結果（3/10）

- ①の項目全体の中国の傾向・特徴を記載。

① サイバーセキュリティ対策の強化3/3

項目	方針/対策の方向性	関連する規制/政策
政府サイバーセキュリティインシデントや攻撃に対する迅速な対応体制や戦略	• 2016年中国サイバーセキュリティ法に、**インシデント対応に必要となるログ保存期間、ネットワーク事業者へインシデント発生時の緊急時対応計画、是正措置・報告実施を義務化**。国家サイバーセキュリティおよび情報化部門（国家网信部门）は、重要インフラ事業者に対しインシデント対応支援することとなった。 • 国家サイバーセキュリティ戦略では、サイバー空間防護部隊を構築し、サイバーセキュリティ防衛を精力的に展開し、サイバー侵入を適時に検知して抵抗し、国家のサイバーセキュリティ維持のための強力な後ろ盾を構築する、としている。 • 2021年、工業情報化部、公安部、CACは「**サイバーセキュリティ製品脆弱性管理規定**」を公表 ※サイバーセキュリティ脆弱性情報はまず中国政府へ集約し、パッチ適用完了後に公開される。	➢ 中国サイバーセキュリティ法 ➢ サイバーセキュリティ製品脆弱性管理規定（工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知）
その他	• 国家サイバー空間セキュリティ戦略（国家网络空间安全战略） • 中国サイバー三法：中国サイバーセキュリティ法、データセキュリティ法、個人情報保護法という三つの基本法によって、国家・社会全体のサイバーセキュリティ強化。※特に、情報システム保有者に対するサイバーセキュリティ法第21条の「等級保護実施」の義務付けは、社会全体のサイバーセキュリティレベルの底上げにつながる制度。	

2.2.2 中国② サイバーセキュリティ産業政策調査結果（4/10）

- 他国と同じく、二国間・多国間におけるサイバーセキュリティ対話、また国連主導のサイバー空間におけるテロ対策に関する国際条約推進を支持する。特徴としては、一帯一路沿線上のデータ産業強化・規格や認証結果の相互認証促進に力をいれる。

② 国際協調の推進

項目	方針/対策の方向性	関連する規制/政策
国際的なサイバーセキュリティ基準や協定の策定・参加	• 相互尊重と信頼に基づき、サイバー空間における国際対話と協力を強化し、グローバルなインターネットガバナンス体制の変化を促進する。他国との二国間・多国間のサイバーセキュリティ対話・交流や情報通信を深化させ、差異を効果的に管理し、世界的・地域的組織とのサイバーセキュリティ協力に積極的に参加し、インターネットアドレスやルートドメインネームサーバーなどの基本資源管理の国際化を推進。 • 国連が、サイバー空間に関する普遍的に受け入れられた国際ルールおよびサイバー空間におけるテロ対策に関する国際条約の策定を推進し、サイバー犯罪との闘いにおける司法支援のメカニズムを改善し、政策・法律、技術革新、基準・規範、緊急対応、重要情報インフラの保護の分野における国際協力を深める上で、主導的な役割を果たすことを支持する。 • 国内外のデータセキュリティ企業が技術革新、製品研究開発、応用推進における交流と協力を深めるよう奨励し、データセキュリティ産業のための国際的な技術革新・協力基地の創設を検討する。 • データセキュリティに関するハイレベルの国際フォーラムや展示会の開催を支援する。データセキュリティ分野の学者や企業家が関連国際機関の活動に積極的に参加するよう奨励する。	➢他国との二国間・多国間のサイバーセキュリティ対話・交流
国家間での相互承認の仕組みの構築	• **発展途上国や後進地域へのインターネット技術の普及やインフラ整備における支援・援助を強化**し、**一帯一路（the Belt and Road）沿線諸国とのデータセキュリティ産業協力**を強化、**規格の収斂と認証結果の相互承認を促進し、製品・サービス・技術・ブランドの「発信」を促進**する。	➢一対一路におけるデジタル戦略

2.2.2 中国② サイバーセキュリティ産業政策調査結果（5/10）

- 中国政府はデジタル産業振興の一環としてサイバーセキュリティ産業振興を図っている。主な研究領域として、AI、ポスト量子暗号、データセキュリティ、プライバシーコンピューティング、第5・6世代移動通信やIoT・自動車通信分野におけるセキュリティをあげている。

③ 研究力・技術力の強化、独立性確保 1/2

項目	方針/対策の方向性	関連する規制/政策
サイバーセキュリティ技術の研究・開発への投資や支援	**【研究開発基金】** 中国政府はサイバーセキュリティスタートアップの成長を支援するための多くの基金やプラットフォームを設立した。 • 国家科学技術メジャープロジェクト (国家科技重大专项) は、サイバーセキュリティを含む中核的かつ戦略的テクノロジーの開発をサポートする主要な国家プログラム。 セキュアなオペレーティング システム、セキュアなチップ、セキュアなデータベース、セキュアなクラウド コンピューティングなどの主要なサイバーセキュリティ製品とシステムの開発に焦点を当てる。また、サイバーセキュリティ人材の育成とサイバーセキュリティ標準の推進も支援する。 • 中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会) は、サイバーセキュリティを含む自然科学の基礎および応用研究を支援する国家機関。 主要プロジェクト、大規模プロジェクト、国際協力プロジェクトなど、さまざまな種類のサイバーセキュリティ研究プロジェクトに資金を提供し、サイバーセキュリティ研究センターやプラットフォームの設立も支援する。 **【産業エコロジー：サイバーセキュリティ産業のためのインフラ強化、産業パーク・パイロット実証区の設置】** • データセキュリティの政策基礎、産業基礎、発展基礎などの要素に基づき、国家データセキュリティ産業パークの配置と建設を行い、企業、技術、資本、人材をパークに加速的に集中させ、多点配置、点から線への先導、全国的な放射という発展パターンを徐々に確立する。また、中央政府と地方政府が協力してデータセキュリティ産業チェーンとイノベーションチェーンを構築する。 • 既存の資源を最大限に活用し、健全なデータセキュリティリスクデータベース、業界分類・等級規則データベース、その他の資源データベースを構築し、データセキュリティ製品の研究開発と技術手段の構築を支援するとともに、データセキュリティのシナリオとアプリケーションのテスト環境を提供する。 • データセキュリティ産業のための公共サービスプラットフォームを構築し、イノベーション支援、需給ドッキング、産業統合協力、能力評価、職業訓練などのサービスを提供し、産業情報の集中共有、需給の的確なドッキング、公共サービスの機動的な対応を実現する。 • 先進的な技術、優れた特徴、顕著な応用成果を有するデータセキュリティのモデルケースと革新体を一括して選定し、実証と指導を強化する。主要な地域と産業でデータセキュリティの応用実証を行い、データセキュリティのイノベーションと応用の先進的な実証区を作り、データセキュリティ技術製品とソリューションの実証と応用、普及に力を入れる。	➢ 国家科学技術メジャー プロジェクト (国家科技重大专项) ➢ 中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会)

2.2.2 中国② サイバーセキュリティ産業政策調査結果（6/10）

③ 研究力・技術力の強化、独立性確保 2/2

項目	方針/対策の方向性	関連する規制/政策
自国での技術開発・研究の促進や外国からの依存度の低減	**【研究領域】** 「サイバーセキュリティ業界の人材育成レポート（网络安全产业人才发展报告）」によると以下を研究領域として言及している。 • AIセキュリティ：規制当局、学界、産業界にとって最も懸念される1つと言及。 「データセキュリティ産業の発展促進に関する工業・情報化部など16部門の指導意見」によると基礎理論・技術の研究を推進するとともに、以下を研究領域として言及。 • ポスト量子暗号アルゴリズム、デンス・ステート・コンピューティング、データセキュリティ産業におけるその他の技術の開発と応用を支援 • データ識別、分類、等級付け、データ非感覚化、データ権利管理などの一般的な基礎技術を最適化・高度化し、プライバシーコンピューティングやデータフロー分析などの主要技術を強化 • ビッグデータシナリオにおける軽量で安全な伝送と保存、プライバシーコンプライアンスの検出、データ濫用分析などの技術を研究 • データセキュリティ技術と人工知能、ビッグデータ、ブロックチェーンなどの新興技術との相互融合とイノベーションを加速し、データセキュリティの状況認識とリスク調査・判断能力を強化 • 第5・6世代移動通信、産業インターネット、モノのインターネット、自動車のインターネットの分野におけるデータセキュリティニーズの分析を強化し、特殊なデータセキュリティ技術製品の革新、研究開発、統合と応用を推進	➢ サイバーセキュリティ業界の人材育成レポート（网络安全产业人才发展报告）（2023年版） ➢ データセキュリティ産業の発展促進に関する工業・情報化部など16部門の指導意見
その他	**【技術的セーフガード】** 「国家サイバーセキュリティ戦略」や「データセキュリティ産業の発展促進に関する工業・情報化部など16部門の指導意見」において、詳細情報は確認できなかったが技術的セーフガードについて言及している。	

2.2.2 中国② サイバーセキュリティ産業政策調査結果（7/10）

- 中国政府は国家サイバーセキュリティ戦略でセキュリティ企業への優遇政策支援、サイバー保険の発展促進を言及。また法規制により重要インフラ施設ではデータローカライゼーションが義務化、セキュリティ製品（34種）は中国独自の認定を義務付けられている。

④ 国内事業者の確保・支援1/2

項目	方針/対策の方向性	関連する規制/政策
インキュベーション、アクセラレーション、資金提供などのスタートアップ支援	**【研究開発基金】**（再掲） 中国政府はサイバーセキュリティスタートアップの成長を支援するための多くの基金やプラットフォームを設立した。 • 国家科学技術メジャープロジェクト（国家科技重大专项）は、サイバーセキュリティを含む中核的かつ戦略的テクノロジーの開発をサポートする主要な国家プログラム。セキュアなオペレーティング システム、セキュアなチップ、セキュアなデータベース、セキュアなクラウド コンピューティングなどの主要なサイバーセキュリティ製品とシステムの開発に焦点を当てる。また、サイバーセキュリティ人材の育成とサイバーセキュリティ標準の推進も支援する。 • 中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会）は、サイバーセキュリティを含む自然科学の基礎および応用研究を支援する国家機関。主要プロジェクト、大規模プロジェクト、国際協力プロジェクトなど、さまざまな種類のサイバーセキュリティ研究プロジェクトに資金を提供し、サイバーセキュリティ研究センターやプラットフォームの設立も支援する。	➢ 国家科学技術メジャー プロジェクト（国家科技重大专项） ➢ 中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会)
	「データセキュリティ産業の発展促進に関する工業・情報化部など16部門の指導意見」によると以下言及 • ソフトウェア企業、集積回路企業、ハイテク企業など、適格なデータセキュリティ企業が優遇政策を享受できるよう支援する。 • 各種金融機関と社会資本がデータセキュリティ分野に投資するよう指導し、データセキュリティ保険サービスの発展を支援する。具体的には、2023年に、工業情報化部、国家金融監督管理総局は、「サイバーセキュリティ保険の標準化と健全な発展の促進に関する意見」を公表し、サイバー保険の発展を後押しする。 • データセキュリティー企業が「科学技術産業金融一体化」特別プログラムに参加し、全国産業一体化協力プラットフォームを通じて便利で効率的な金融サービスを受けられるように支援する。 • 知的財産権の適用と保護を強化し、業界の自主規制・監督メカニズムを確立・改善し、技術力とサービス能力を重視した穏健な市場競争環境を確立する。 「国家サイバー空間セキュリティ戦略（国家网络空间安全战略）」によると以下言及 • 「インターネット・プラス」イニシアティブを実施し、ネットワーク経済を力強く発展させる。 • 国家ビッグデータ戦略を実施し、ビッグデータセキュリティ管理システムを確立し、ビッグデータ、クラウドコンピューティングなど新世代の情報技術の革新と応用を支援する。市場環境を最適化し、サイバーセキュリティ企業がより大きく、より強く成長することを奨励し、国家のサイバーセキュリティを守るための産業基盤を強化する。	➢サイバーセキュリティ保険の標準化と健全な発展の促進に関する意見（国家金融监督管理总局关于促进网络安全保险规范健康发展的意见） サイバーセキュリティ保険の規格策定、保険のサービス多様化促進、サイバーセキュリティリスクの定量評価・観測手法の確立、民間企業のサイバー保険購入促進などを言及 ➢「インターネット・プラス」イニシアティブ ➢国家ビッグデータ戦略

2.2.2 中国② サイバーセキュリティ産業政策調査結果（8/10）

④ 国内事業者の確保・支援2/2

項目	方針/対策の方向性	関連する規制/政策
サービス認定創設、政府調達などの活用などのビジネス機会の創出	（再掲） • 2021年6月に施行された「中国サイバーセキュリティ法」により、重要情報インフラ施設運営者は、データローカライゼーション、年度安全評価、レスポンス体制の構築など、より強固な保護対策を講じることが要求されている。 • 2017年に政府、重要インフラが調達する製品とサービスに関する安全審査を行う「サイバーセキュリティ製品とサービス審査弁法」が施行 • 2017年より、インターネット重要設備とサイバーセキュリティ専用製品に関する強制認証の対象製品（网络关键设备和网络安全专用产品目录）※および、認証済みの製品目録（网络关键设备和网络安全专用产品安全认证和安全检测结果发布）を定期的に公表。 ※2023年12月1日時点では34項目が指定されている。 • 2022年、中国データ安全法等に基づき、CACを含む13の省庁が「サイバーセキュリティ安全審査弁法」を制定、重要インフラ、国家安全などに係る場合、製品及びサービスについて国家安全審査をすると規定。	➢サイバーセキュリティ製品とサービス審査弁法（网络产品和服务安全审查办法） ➢サイバーセキュリティ安全審査弁法（网络安全审查办法）
その他	**【市場規模】** • 2022年、中国のネットワークセキュリティ市場規模は約633億元、前年比成長率は3.1%（ほぼ前年比成長率と同等）で、業界は過去3年間、全体的な成長傾向を維持している。 • 中国のネットワークセキュリティ市場参入は遅かったが、急速に成長し、セキュリティソフトウェアとハードウェア製品の市場シェアの大半を占め、セキュリティサービスは29%を占めており成長余地は大きい。同時に、中国では市場競争が非常に活発で、TOP8のセキュリティ企業は、市場の44.91%を占める。 **【主要プレイヤー】** • Chianxin社、Qixingchen社、SZSS社、Tianrongxin社の4社の市場シェアは5%を超える。	➢ サイバーセキュリティ業界の人材育成レポート（网络安全产业人才发展报告）（2023年版）

2.2.2 中国② サイバーセキュリティ産業政策調査結果（9/10）

- 新規働き手確保のため、2017年より11の大学をサイバーセキュリティ人材育成機関として認定したWCCSを開始。2023年にはセキュリティ専科卒業生は約3.2万人になる。その他国家職業標準を制定、産学間の共同開発・インターンシップを推進する。

⑤ セキュリティ人材育成

項目	方針/対策の方向性	関連する規制/政策
サイバーセキュリティ専門家の教育・トレーニングの支援、資格制度の整備	• 2023年1月に公表された「データセキュリティ産業の発展促進に関する工業・情報化部など16部門の指導意見」では、訓練などデータセキュリティエンジニアリング技術者の国家職業標準を制定・公布し、デジタル技術エンジニア育成プロジェクトを実施、ハイレベルのデータセキュリティエンジニアチームを育成・拡大する。 • 黒竜江省デジタル技術エンジニア育成プロジェクトが正式発足 • 科学研究機関、大学、職業訓練大学、優良企業、訓練機関が産業と教育の融合を深め、協力して人材を育成することを奨励し、共同育成、共同研究室の建設、インターンシップ・訓練基地の創設、オンライン・オフライン訓練の組み合わせによって、実践的なデータセキュリティ専門家と優秀な管理人材を育成する。	➢国家職業標準 ➢デジタル技術エンジニア育成プロジェクト
サイバーセキュリティ産業の雇用状況・労働環境の改善	➢「サイバーセキュリティ業界の人材育成レポート（网络安全产业人才发展报告）2023年版」によるとサイバーセキュリティ人材には以下傾向がみられる。 ■サイバーセキュリティ実務者の傾向 • 男女比：男性77%、女性23% • 年齢別：25～40歳は全体の80%、中でも30～40歳が最も多く全体の半数を占める。 • 学歴　：短期大学と学部卒が全体の89% • 最終学歴の専攻：「コンピュータ科学技術」「情報セキュリティ」「ネットワーク工学」の出身が約32% ■雇用条件の傾向・働き方 • 年収：超一級都市（北京、上海、広州、深圳）のサイバーセキュリティ実務者の36.7%が税引前年収10～20万人民元で、全体水準よりも高い。北京、上海、広州、深圳では税引き前年収20～30万元20%、50万元以上が16.6%である。将来給与は高まると予想される。 • 福利厚生：他業種と比較し良い。休暇日贈与（61.4%）、健康診断（58.5%）、有給提供（54.6%）※交通費補助、通信費補助、無料給食、無料送迎バス、寮などは50%以下。 • 残業：サイバーセキュリティ実務者の73%が週40時間以上働いており、33.8%は週41～50時間、22.2%は週51～60時間働く。	➢該当なし
新規の働き手の確保策やリスキリングなどの支援策	• World-Class Cybersecurity Schools(WCCS／一流网络安全学院)： 2017年8月、教育省とサイバー空間局（CAC）は共同で「一流サイバーセキュリティ学部建設パイロットプロジェクト管理弁法」を制定し、世界クラスのサイバーセキュリティ大学を認定する政府認定プログラム（WCCS）を開始。11の大学を認定した。 その後、一般の大学や専門学校におけるデータセキュリティ関連の専門科目を増やし、2023年のネットワークセキュリティ関連専攻卒業生の総規模は、約3.2万人になると推計される。	➢一流网络安全学院（WCCS）

2.2.2 中国② サイバーセキュリティ産業政策調査結果（10/10）

- 中国においては、サイバーセキュリティ経済振興を目指すため、サイバーセキュリティ技術の研究開発や大学を含めた人材育成にかかる様々なプログラムを実施している。

政策名	概要	
国家科学技術メジャー プロジェクト (国家科技重大专项)	国家科学技術メジャープロジェクト (国家科技重大专项) は、サイバーセキュリティを含む中核的かつ戦略的テクノロジーの開発をサポートする主要な国家プログラム。 セキュアなオペレーティング システム、セキュアなチップ、セキュアなデータベース、セキュアなクラウド コンピューティングなどの主要なサイバーセキュリティ製品とシステムの開発に焦点を当てる。また、サイバーセキュリティ人材の育成とサイバーセキュリティ標準の推進も支援する。	Link
中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会)	中国国家自然科学基金委員会(NSFC、国家自然科学基金委员会) は、サイバーセキュリティを含む自然科学の基礎および応用研究を支援する国家機関。 主要プロジェクト、大規模プロジェクト、国際協力プロジェクトなど、さまざまな種類のサイバーセキュリティ研究プロジェクトに資金を提供し、サイバーセキュリティ研究センターやプラットフォームの設立も支援する。	Link
「インターネット・プラス」イニシアティブ（互联网+）	インターネットと他産業が結びつくことで、モバイルインターネット、クラウドコンピューティング、ビッグデータ、モノのインターネットなど新しい情報技術を従来型産業に導入し、新たな活力を与え、産業のモデルチェンジやグレードアップを推進すること。 2016年国家サイバー空間セキュリティ戦略で、セキュリティを含むネットワーク経済を力強く発展させる枠組みとして紹介されている。	Link
World-Class Cybersecurity Schools(WCCS／一流网络安全学院)	2017年に、教育部、CAC共同で「一流サイバーセキュリティ学部建設パイロットプロジェクト管理弁法」を制定し、これに基づき2017年より中国政府は、世界クラスのサイバーセキュリティ大学を認定する政府認定プログラム（WCCS）を開始。教育省とサイバー空間局（CAC）は、11の大学を認定した。 その後、一般の大学や専門学校におけるデータセキュリティ関連の専門科目を増やし、2023年のネットワークセキュリティ関連専攻卒業生の総規模は、約3.2万人になると推計される。	Link

2.2.2 中国③とりまとめ

- 中国の「サイバースペースセキュリティ国家戦略」等について特徴・傾向と、その現況・評価。

大項目	小項目	特長・傾向	現況・評価
政策関係	サイバーセキュリティ対策の強化	✓ 中国サイバー三法および戦略に基づき施策を講じる。安全保障観点では、重要インフラ施設のデータローカライゼーションや中国独自のセキュリティ製品認定制度を導入。セキュリティ人材育成プログラムや国民啓発週間により全体のリテラシー向上を図る。	自国のサイバーセキュリティ強化のため、2017年より中国サイバー三法制定により、重要インフラ保護、産官学連携、および国民におけるリテラシー向上など網羅的にセキュリティ施策を講じており、着実に強化がなされていると言える。
	国際協調の推進	✓ 他国と同じく、二国間・多国間におけるサイバーセキュリティ対話、また国連主導のサイバー空間におけるテロ対策に関する国際条約推進を支持する。特徴としては、一帯一路沿線上のデータ産業強化・規格や認証結果の相互認証を促進する。	中国では、多くのサイバーセキュリティ製品の国際標準化を推進。また中国と比較しサイバーセキュリティ技術が遅れている国に対し支援し、自国のセキュリティ規格・認証をひろめ、中国がセキュリティ基準となるよう動きを見せている。
	研究力・技術力の強化、独立性確保	✓ 中国政府はデジタル産業振興の一環としてサイバーセキュリティ産業振興を図る。主な研究領域として、AI、ポスト量子暗号、データセキュリティ、プライバシーコンピューティング、第5・6世代移動通信やIoT・自動車通信分野におけるセキュリティをあげている。	2022年、中国のネットワークセキュリティ市場規模は約633億元、前年比成長率は3.1%（ほぼ前年比成長率と同等）で、業界は過去3年間、全体的な成長傾向を維持できており、施策は成功していると言える。 今後の研究領域は、AI・量子暗号など、米国と類似する箇所も多い（サイバー保険含め）。また国が優先する先進技術におけるセキュリティニーズの分析結果を軸として研究領域を指定する。
	国内事業者の確保・支援	✓ 中国政府は国家サイバーセキュリティ戦略でセキュリティ企業への優遇政策支援、サイバー保険の発展促進を言及。 ✓ 法規制により重要インフラ施設ではデータローカライゼーションが義務化、セキュリティ製品（34種）は中国独自の認定制度を義務化。	
	セキュリティ人材育成	✓ 新規働き手確保のため、2017年より11の大学をサイバーセキュリティ人材育成機関として認定したWCCSを開始。2023年にはセキュリティ専科卒業生は約3.2万人になる。その他国家職業標準を制定、産学間の共同開発・インターンシップを推進する。	WCCSによる、2023年にはセキュリティ専科卒業生は約3.2万人と、新規働き手の確保の施策としては成功していると言える。
予算　等		✓ 非公開	

2.2.3 EU

2.2.3 EU① サイバーセキュリティに関する政策の全体像 - EU新サイバーセキュリティ戦略

- 2020年12月、欧州連合(EU) は、EUの新デジタル戦略「欧州のデジタル未来の形成」に基づき、新サイバーセキュリティ戦略を策定。旧サイバーセキュリティ戦略の取組みをベースとし、更なる強化をめざすべく、新戦略では新たに三つの柱と施策を掲げた。

デジタル10年に向けたEUサイバーセキュリティ戦略 The EU's Cybersecurity Strategy for the Digital Decade(2020)

- 新サイバーセキュリティ戦略には、下記3つの分野に取り組むための、規制、投資、政策の3つの主要な手段を展開するための提案が含まれている。
- 「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通じて、この戦略を支援することを約束する」としている。

戦略の主な目的	• 欧州の人々の安全保障と基本的権利および自由に対するリスクに対処するため、グローバルで開かれたインターネットを確保すること • 欧州の価値観に沿ったサイバー脅威へのレジリエンス確保、市民と企業にデジタル技術の便益を確保すること

「デジタル10年に向けたEUサイバーセキュリティ戦略」における3つの柱と主な施策

レジリエンス・技術的主権・リーダーシップ	1.1 強靭なインフラと重要なサービス（NIS指令の改定など） 1.2 欧州サイバーシールドの構築（欧州サイバーシールドとセキュリティオペレーションセンターの創設） 1.3 超セキュアな通信インフラ 1.4 次世代ブロードバンド・モバイル・ネットワークの確保 1.5 安全なモノのインターネット（ICT製品等のサイバーセキュリティ認証制度、自動車のサイバーセキュリティ対策） 1.6 グローバルなインターネット・セキュリティの強化 1.7 テクノロジーサプライチェーンにおける存在感の強化 1.8 サイバーに強いEUの労働力（サイバーセキュリティスキルの強化）
予防・抑止・対応のための運用能力構築	2.1 合同サイバーユニット（EUワイドのサイバー攻撃対策組織「合同サイバーユニット」の創設） 2.2 サイバー犯罪への取り組み（サイバー攻撃の防止、対応するためのEUサイバー外交ツールボックスの強化） 2.3 EUのサイバー外交ツールボックス 2.4 サイバー防衛能力の強化
グローバルで開かれたサイバー空間の推進	3.1 サイバー空間における基準、規範、枠組みに関するEUのリーダーシップ、国際標準化の強化 （サイバー空間の国際安全保障に取り組む新たな国連行動計画（POA）の提唱） 3.2 パートナーおよびマルチステークホルダー・コミュニティとの協力 （第三国、地域機関および国際機関とのサイバー対話の強化、サイバー防衛の互換性要件など） 3.3 グローバルなレジリエンスを高めるためのグローバルな能力の強化

参照：The EU's Cybersecurity Strategy for the Digital Decade
https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

2.2.3 EU② サイバーセキュリティ産業政策調査結果（1/7）

- EU域内の規制・投資・政策の手段により、サイバーセキュリティの技術開発とルールメイクを主導。代表例に、NIS指令を改定し、より広範な組織に対し、より厳格な規制を設け、サイバーセキュリティに関する戦略的イニシアチブを展開。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
国家的なサイバーセキュリティのレジリエンスやリスクに係る言及	**【サイバーセキュリティリスクに関する認識】** • 戦略では、懸念されるリスクについて以下のように指摘し、複雑な脅威環境と言及。 – 社会：Covid-19流行に起因する労働形態のデジタル化により、サイバー攻撃に対する脆弱性が増大 – 市民：EUには、サイバー脅威に対する集団的な状況認識が欠けている – 製品：IoTデバイスは既知の脆弱性を抱えたまま出荷されるため、悪意あるサイバー攻撃対象が増加 – 国家・社会：重要インフラ、経済プロセス、民主的制度に対するサイバー攻撃などのハイブリッドな脅威 **【サイバーレジリエンスの確保】** • 対策として、**サイバースキルを持つ労働力の確保・育成**、**改訂されたNIS指令**の採用、**安全なIoTのための規制措置**、**EU DNSリゾルバサービス**の開発など、戦略的イニシアチブを展開。 • 2021-2027年にかけて**最大45億ユーロ**の公共および民間投資を計画。	➢ **デジタル10年に向けたEUサイバーセキュリティ戦略（The EU's Cybersecurity Strategy for the Digital Decade）** ➢ **サイバーレジリエンス法案**
国の重要情報インフラにおけるサイバーセキュリティ・システムに関する要件	**【強靭なインフラと重要なサービスの戦略的管理：NIS指令（ネットワーク通信システム指令）の改定】** • 戦略では、**官民を問わず経済や社会にとって重要な機能を果たすすべての関連部門のサイバー体制を高める**ことに触れ、サイバーセキュリティの単一市場の中核をなす「NIS指令」の改正について言及。 • 改訂版となる「**NIS2指令**」は、NIS指令の要件を拡大し、**より厳格な監督措置**、**より厳格な施行要件**、**違反に対するより高い罰金**が導入される。さらに、社会インフラ分野のみを対象にしていたNISより、経済社会的観点から高い重要性を持つ必須組織と、新たに追加した重要組織に対象事業者を大幅に拡大し、**より広範な事業者に対策を迫る**内容になっている。	➢ **NIS指令** • EU加盟国に対して、重要なインフラのサイバーセキュリティ基準を強化することを義務付け。 ➢ **NIS2指令** • NIS指令よりもさらに広範囲の産業・事業者に対し、より厳格なセキュリティ要件と違反への罰則の強化が含まれる。

2.2.3 EU②サイバーセキュリティ産業政策調査結果（2/7）

- EU域内の規制・投資・政策の手段により、サイバーセキュリティの技術開発とルールメイクを主導。代表例に、NIS指令を改定し、より広範な組織に対し、より厳格な規制を設け、サイバーセキュリティに関する戦略的イニシアチブを展開。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
サプライチェーンにおけるサイバーセキュリティ強化に関する施策	**【サプライチェーン強化に関する取り組み】** • 戦略では、産業プロセス、業務、機器の設計によるサイバーセキュリティは、リスクを軽減し、企業だけでなく広く社会のコストを削減する可能性があり、それにより**レジリエンスを高めることができるとし、サプライチェーン全体は、セキュア・バイ・デザインでなければならない**とする。 • 上記の通り、**NIS指令をNIS2指令に改定するにあたり、より広範な組織・事業者に指令が適用される**。 • 他、欧州委員会は、分野別にサイバーセキュリティに関する規定を発出する予定である。 - **金融分野**：デジタル業務の回復力を強化し、あらゆる種類のICT関連の混乱や脅威に耐える能力を確保しなければならない。（「金融セクターのデジタル・オペレーショナル・レジリエンスに関する規制の提案および規則」） - **運輸分野**：運輸手段におけるサイバー体制強化に向けた努力を継続。航空保安に関するEU法にサイバーセキュリティに関する規定を追加。 - **民主的プロセス**：民主的プロセスと制度のサイバー体制を強化することは、自由な選挙、民主的言説、メディアの複数性を保護・促進するための欧州民主化行動計画（European Democracy Action Plan）の中核をなすものである。 - **宇宙分野**：将来宇宙計画のもとでのインフラとサービスの安全保障のために、次世代全地球航法衛星システム（GNSS）サービスのためのサイバーセキュリティ戦略の深化、および宇宙計画のその他の新しい構成用をを引き続き進めていく（政府衛星通信構想（GOVSATCOM）とスペースデブリ（SST）が含まれる）。	➢ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 ➢ Commission Implementing Regulation (EU) 2019/1583（航空保安に関するEU法）

2.2.3 EU② サイバーセキュリティ産業政策調査結果（3/7）

- 個々のカテゴリのICT製品、プロセス、サービスに合わせたEU内で統一された認証スキームが成立する環境の構築を目指し、EU全体のセキュリティレベル向上に寄与。日本企業を含むEU域内外の企業が参加するアライアンスの政策立案への関与も見られる。

② 国際協調の推進

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティに関する標準の実施状況	**【EUサイバーセキュリティ認証フレームワーク】** • 戦略では、**EUはすでに、サイバーセキュリティ法の下で、透明性のあるセキュリティ・ソリューションと認証を確保し、性能に妥協することなく安全な製品やサービスにインセンティブを与えるよう取り組んでいる**と言及。 • その具体例として、**サイバーセキュリティ法**に基づく、**EUサイバーセキュリティ認証フレームワークは、ルール、技術要件、規格、手順を含むようなセットとして、EU全体の認証スキームを提供し、認証された ICT製品およびサービスが、指定された権利に準拠していることを証明**する。**作成された証明書はすべてのEU加盟国で認められるため、企業は国境を越えて取引することが容易になり、購入者は製品やサービスのセキュリティ機能を理解できるようになる。** • 認証フレームワークの実施に関しては、 欧州サイバーセキュリティ認証グループ (ECCG)に集まった参加国によって協議、決議が行われる。	➢ **EUサイバーセキュリティ認証フレームワーク** • サイバーセキュリティ法(2019)により、EUレベルでICT製品、サービス、およびプロセスに対する自発的なサイバーセキュリティ認証スキームが設立。 • EU内でICT製品、サービス、プロセスのサイバーセキュリティレベルを適切に保証。
グローバルなサイバーセキュリティ・アライアンスにおける、自国のサイバーセキュリティプレーヤーの位置づけ	**【Charter of Trust (CoT)】** ※戦略上の記載はないが、欧州を中心とするグローバルなアライアンスと、欧州戦略・施策との関連性を記載 • Charter of Trustは、**サイバーセキュリティを強化する欧州委員会の意図を歓迎し、EU内のリスク管理とデジタルバリューチェーンの強化を支持**。サプライチェーン全体にわたるセキュリティを確保するための基本的なセキュリティ要件を提案しており、これは NIS2指令 の目標と一致する。 • サイバーセキュリティの責任を組織全体に適切に指定すること、サイバー意識の向上とスキルの必要性に焦点を当てること、そして報告義務やサプライチェーンのセキュリティ強化を支援する教育フレームワークの開発など、**NIS指令の見直しに応じた詳細な対応を行う**。 • EUのセクター固有のサイバーセキュリティ認証スキームやその他の製品関連法規の改正、サプライチェーンのセキュリティをさらに強化すること、EUのNIS指令と既存のサイバーセキュリティ関連の要件との間に一貫性を持たせることを提案。 • これらの活動を通じて、Charter of TrustはEUのサイバーセキュリティ戦略に積極的に貢献し、その実現を目指す。	➢ **Charter of Trust (CoT)** • サイバーセキュリティを強化し、信頼できるデジタル技術とインフラストラクチャを確立することを目的とした同盟。 • 2018年のミュンヘンセキュリティカンファレンスで設立され、現在、17の多国籍企業と13の関連パートナーを数える。

2.2.3 EU② サイバーセキュリティ産業政策調査結果（4/7）

- EUのデジタル領域の「技術的主権」を追求し、デジタル投資にサイバーセキュリティを統合することで、技術革新が進行中の分野と合わせて、サイバーセキュリティ産業の成長を促進。また、複数のステークホルダー間の研究協力・連携を促す動きもみられる。

③ 研究力・技術力の強化、独立性確保

項目	戦略上の記載	関連する規制/政策
自国のサイバーセキュリティ産業の育成のために、政府が支援する研究開発の取り組み	**【サイバーセキュリティのデジタル投資への統合】** • 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通じて、サイバーセキュリティ戦略を支援する。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する。** • 2021-2027年の多年度財政枠におけるサイバーセキュリティのデジタル変革のための計画された財政支援により、**データ**、**クラウド**、**次世代プロセッサ技術**、**超高セキュリティ接続**、**6Gネットワーク**などのデジタルサプライチェーン全体にわたってリーダーシップとデジタル技術を推進。 • また、サイバー防衛能力の強化など、**異なるEU政策と手段を通じて、**主要技術の開発と使用に重点を置きながら、**最先端のサイバー防衛能力の開発を促進する。** **【産学連携促進による技術開発支援】** • **ECCC（European Cybersecurity Excellence Center）**のネットワークを通じ、ヨーロッパの最高の研究チームと産業界との協力に基づく共通研究アジェンダを設計・実施するための投資を行う。各国の調整センターを結びつけ、**産業界、アカデミア、研究機関との協力を通じて共通の研究アジェンダを設計・実施**することを目指し、EUの技術革新とサイバーセキュリティの能力を強化し、敏感なインフラの保護や技術的主権を発展させることを目的としている。 **【資金調達のプログラムの活用】** • **Horizon Europe** の一部として、個々のインターネットイノベーターが開発するプライバシーを強化し、オープンソースソフトウェアとハードウェアに基づく安全な通信技術を支援。**EUの研究とイノベーションのための主要な資金援助プログラム**で、2021～2027年の予算は955億ユーロ。	➢**European Cybersecurity Excellence Center** • EUがサイバーセキュリティの技術的および産業的能力を維持・発展させるために設立した機関。 • EU全体のサイバーセキュリティ産業および研究エコシステムを相互接続されたものとして構築することを目的とする。 • 民間セクターと防衛セクターを含む関連するステークホルダー間の協力を促進。EU全域にわたる既存のサイバーセキュリティリソースと専門知識を最大限活用。 • 資金面では、EUと加盟国からの財政的貢献によって共同で資金提供され、EUの長期的な予算の重要な部分とされる。 ➢**Horizon Europe** • 研究とイノベーションのためのEUの主要な資金提供プログラム。 • 健康、気候変動、デジタル化、サイバーセキュリティなど、様々な分野における研究をサポート。

2.2.3 EU② サイバーセキュリティ産業政策調査結果（5/7）

- IoT製品のセキュリティ強化、サプライチェーンの改善、業界全体にわたるリスク管理の徹底、国内企業のセキュリティ体制の強化を推進するため、事業者への対応義務付けと、支援体制を強化を進める。

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業の保護、振興に関する位置づけ	**【サイバーセキュリティ産業の位置づけ】** • 戦略では、**今後10年間は、EUがサプライチェーン全体にわたって安全な技術の開発を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**と言及。 • 人口知能、暗号化、量子コンピューティングのような主要技術については、インセンティブ、義務、ベンチマークを用いて**サイバーセキュリティを全てデジタル投資に統合する**必要がある、とする。	➢**サイバーレジリエンス法案（CRA: Cybersecurity Resilience Act, 2022）** • 欧州で販売されるデジタル要素を持つあらゆるハードウェアとソフトウェアに適用され、技術的なセキュリティ機能と脆弱性対応を強化することを目的とする。 • 法案の要求事項には、製品のセキュリティ機能、脆弱性対応プロセス、技術文書の保管、製品のセキュア開発ライフサイクルの実施などが含まれる。
国家安全保障／経済安全保障の観点から、サイバーセキュリティ産業を保護するためにとられている政策／措置	**【IoT製品のセキュリティ向上のための安全規制】** • **IoTの普及に伴い、サイバーセキュリティ全体の強化と全体的なレジリエンスを確保するために、ネットに接続された製品と関連サービスのサイバーセキュリティ向上を目指す新しい規則を検討。**これには、接続されたデバイスメーカーにソフトウェアの脆弱性への対応、ソフトウェアとセキュリティの更新の継続、および個人データやその他の機密データの終末処理を義務付ける新たなケア義務が含まれる可能性がある。 **【EU域内の企業に対するサイバーセキュリティ対策・対応義務の強化】** • **サイバーセキュリティ法**は、**加盟国に対し、より厳格な監督・執行措置の遵守、制裁措置の調和と、エネルギー、運輸、銀行、保健、行政など様々なセクターにわたるリスク管理と情報共有のためのサイバーセキュリティ義務強化の確立を求めている。さらに、郵便サービス、廃棄物管理、製造業など「重要部門」の保護を包含しており、これらの部門の中堅・大企業がサイバーセキュリティ要件を準拠することを義務付ける。** **【欧州サイバーシールドの構築】** ※他、戦略の脚注に欧州内サイバー犯罪に対する連携の取組例が記載 • **情報共有分析センター（ISACs）**において、**サイバー脅威に関する情報交換を促進し、複数のステークホルダー間の連携を強化**することで、セクターごとのセキュリティを向上させる。 • コンピューターセキュリティインシデント対応チーム（CSIRTs）やセキュリティオペレーションセンター（SOCs）が各組織に設置され、ネットワークやコンピューターシステムの常時監視と分析を行い、侵入や異常をリアルタイムで検出し、サイバー攻撃を封じ込める。AIや機械学習技術を活用して、運用者を支援。 **【EU一般データ保護規則（GDPR）】** ※戦略上の記載はないが、EU域内のサイバーセキュリティ産業の保護施策として記載 • 2018年5月25日施行されたGDPRは、EUに在住する個人のプライバシーの権利の保護と確立を目的としており、EU在住の個人データを取り扱う企業・組織がGDPRの適用対象となる。違反者は巨額の制裁金を科せられる（米国超巨大IT企業（ビックテック）であるGARFAMもGDPR違反として制裁金を科されている）。	➢ **欧州内のサイバー犯罪に対する連携機関、組織の例** • サイバー危機連絡組織ネットワーク（CyCLONe）、欧州刑事警察機構（Europole）、欧州サイバー犯罪センター　等 ➢ **EU一般データ保護規則（GDPR）** • GDPRは各国企業が「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。

2.2.3 EU② サイバーセキュリティ産業政策調査結果（6/7）

- EU加盟国と共同で運営されるパートナーシップのもと、NIS2指令準拠や技術的支援を通じた産業界の需要の掘り起こしによるサイバーセキュリティへの投資を誘発と、供給のマッチングを進めることで、民間投資の拡大を狙う。

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業を促進するための事業者を対象にした支援政策/施策	**【テクノロジーサプライチェーンにおける存在感の強化】** • 戦略では、サイバーセキュリティ関連企業への支援政策として、CCCNI（サイバーセキュリティ産業技術研究能力センターおよび調整センターネットワーク）が中心となり、**ヨーロッパ全土にわたるサイバーセキュリティの専門技術と研究能力を強化**することが言及されている。 - **Digital Europe Programs**の一環のDigital Innovation Hubsの専用活動を通じて、**改定NIS指令の適用範囲外の中小企業や産業同盟へのサイバーセキュリティの技術的支援を行うことにより、投資需要を生み出し、CCCNを通じて、加盟国と産業界からの需給のマッチングを進める**。こうした取組により、2021年から2027年にかけて**最大45億ユーロの公共および民間投資**を目標とする。 - CCCNは、産業界や学術界からの意見を取り入れながら、EUの技術的主権を発展させるための重要な役割を果たすことが期待され、具体的には、5Gのような敏感なインフラストラクチャのセキュリティを確保し、最も重要な技術における他の地域への依存度を低下させることを目的としている。 - また、CCCNは**EU各国からの投資を引き出し**、投資を促進するという役割も担っている。 **【サイバーセクターのイノベーション支援】** ※ 戦略には、コネクティング・ヨーロッパ・ファシリティ（Connecting Europe Facility、以下CEF)への直接の記載はないが、サイバーセキュリティへの投資促進やISACの設立への言及などの共通点が見られるため掲載する。 • CEFのサイバーセキュリティ・コール2020の下で、EUは1100万ユーロの資金を、重要サービス事業者（OES）、国家サイバーセキュリティ認証局、サイバーセキュリティに関する国家所轄庁を含む選ばれた申請者に割り当てた。 - CEFの目的は、**効率的で持続可能な欧州横断ネットワークを開発することにより、成長、雇用、競争力を促進する**こと。 - 2021-2027年の予算は約207億ユーロで、加盟国全体に利益をもたらすことを目指している。 - この資金は、サイバーセキュリティ能力を開発するための**18カ国にわたる22のプロジェクトを支援。** - これらのプロジェクトには、エネルギー分野における**情報共有・分析センター（ISAC）の設立**や、保健、エネルギー、運輸などの分野における事業体の支援が含まれ、全体として、EUは**サイバーセキュリティ強化のためにCEFを通じて4740万ユーロを投資**。デジタル・ヨーロッパ・プログラムの下でさらなる提案を計画。 **※CCCNが特にサイバーセキュリティの強化に特化しているのに対し、CEFはより広範なインフラ投資とそれに伴うシナジーの促進に焦点を当てている。**	➢**CCCN（Cybersecurity Industrial Technology and Research Competence Centre and Network of Coordination Centers）** • 日本名は、「サイバーセキュリティ産業技術研究能力センターおよび調整センターネットワーク」。 • EUがサイバーセキュリティの技術的・産業的能力を維持し、発展させることを目的とする。 • 2021年から2027年の次期多年度財政枠組みの下でサイバーセキュリティ基金を管理し、EU全体のサイバーセキュリティ産業と研究エコシステムを作成することを目指す。

2.2.3 EU② サイバーセキュリティ産業政策調査結果（7/7）

- 専門的な教育プログラムと産業界の連携を通じ、サイバーセキュリティスキルを有する労働力の育成を推進し、テレワークやIoT機器の普及に伴う新たなリスクへの対応を強化。子供、若者、女性の人材育成や、労働市場全体としての意識向上を狙う。

⑤ セキュリティ人材育成

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修、教育プログラム等の開発支援	**【サイバーに強いEUの労働力の確保】** • 戦略では、**「労働力のスキルアップ、優秀なサイバーセキュリティ人材の育成、誘致、維持、世界クラスの研究と技術革新への投資といったEUの取り組みは、サイバー脅威全般から身を守るための重要な要素である」**とし、以下の取組が言及されている。 - 欧州委員会は、CCCNとともに、**サイバーセキュリティ専門の修士プログラム**の開発を支援する意向。 - **改訂デジタル教育行動計画**として、人材のアップスキル、優れたサイバーセキュリティの才能の開発への投資、世界クラスの研究とイノベーションへの投資を推進しており、サイバーセキュリティへの意識を高めるとともに、特に、**STEM教育の推進**や**女性のICT職への参画のためのアップスキル**を奨励。 - 職業教育訓練(VET)での意識向上、演習を含む教育を含め、欧州ネットワーク・情報セキュリティ機関（ENISA）、欧州防衛機関(EDA)、欧州安全保障防衛大学(ESDC)といった**EUの関連機関の活動の相乗効果の追及**を呼びかけ。 **【体系的なサイバーセキュリティ専門職の育成】** ※ 戦略には、以下の施策への直接の記載はないが、サイバーセキュリティのスキル獲得奨励への具体的な取り組み実態の一例として掲載する。 • 欧州サイバーセキュリティ・スキルフレームワーク（ECSF） • サイバーセキュリティ・スキル・アカデミー（Cybersecurity Skills Academy） • The Digital Skills and Jobs Platform	**➢欧州サイバーセキュリティ・スキルフレームワーク（ECSF）** • ENISAの重要なイニシアティブ。 • 欧州全域のサイバーセキュリティ専門職に求められる役割、スキル、コンピテンシーを理解するためのオープンツールの提供や、訓練プログラムの設計を支援。 **➢Cybersecurity Skills Academy** • サイバーセキュリティの人材格差を解消し、EUの競争力、成長力、回復力を高めるために、既存のサイバー技能イニシアチブを統合・調整することを目的とする。 • 官民のサイバーセキュリティの労働市場のニーズに対応し、サイバーセキュリティ訓練に対するEU共通のアプローチの確立に重点を置く。 **➢The Digital Skills and Jobs Platform** • EUのデジタル技能・雇用イニシアチブの中心的ハブとして、ノウハウの交換を促進し、国境を越えた新たなパートナーシップを奨励し、成功したイニシアチブの複製を支援。
サイバーセキュリティ業界の労働環境に関する受け止め	**【サイバーセキュリティ業界の労働環境・人材確保策】** • 戦略では、Covid-19の流行で**EUの労働者の40%がテレワークに切り替え、サイバー攻撃に対する脆弱性が増大した**とする一方で、「企業や個人のサイバーへの備えや意識は依然として低く、**労働力におけるサイバーセキュリティのスキルは大きく不足している**」と指摘。 • 戦略では、「より多様な人材を育成し、惹きつけ、保持することに特別な注意を払わなければならない」として、個人、特に**子供や若者、組織（特に中小企業）のサイバーセキュリティに対する意識を高める**こと、**ICT職への女性の参加を促進**することを言及。 • 欧州では、**サイバーセキュリティの専門家を募集するポストが29万1000件も埋まっていない**と推定。サイバーセキュリティの専門家の育成と雇用には時間がかかるため、早急な対策が必要と警鐘を鳴らす。	

2.2.3 EU③とりまとめ

- EU域内のサイバーセキュリティ戦略(2020)の特徴・傾向と、その現況・評価。

大項目	小項目	特長・傾向	現況・評価
政策関係	サイバーセキュリティ対策の強化	✓ EU域内の規制・投資・政策の手段により、サイバーセキュリティの技術開発とルールメイクを主導。代表例に、NIS指令を改定し、より広範な組織に対し、より厳格な規制を設け、サイバーセキュリティに関する戦略的イニシアチブを展開。	➢ NIS2への改正により、スコープとなる重要インフラ事業を拡大し、事業者に強化されたセキュリティガバナンスの実施を義務付け。
	国際協調の推進	✓ 個々のカテゴリのICT製品、プロセス、サービスに合わせたEU内で統一された認証スキームが成立する環境の構築を目指し、EU全体のセキュリティレベル向上に寄与。日本企業を含むEU域内外の企業が参加するアライアンスの政策立案への関与も見られる。	➢ 欧州ではサイバーセキュリティの標準の作りこみが具現化しつつある。産業・業界団体は、検討中の規制に対して、レジリエンス強化の方向性に賛同する一方、行政手続の負担軽減や準備期間、ガイドライン整備などの対応を要求。対話が進む。
	研究力・技術力の強化、独立性確保	✓ EUのデジタル領域の「技術的主権」を追求し、デジタル投資にサイバーセキュリティを統合することで、技術革新が進行中の分野と合わせて、サイバーセキュリティ産業の成長を促進。また、複数のステークホルダー間の研究協力・連携を促す動きもみられる。	➢ EU全体のサイバーセキュリティ認証スキーム、NIS2、サイバーレジリエンス法など、EUがサイバーセキュリティの課題に対応し、技術的主権を強化し、デジタル環境を安全に保つための戦略の一環として実施されている。
	国内事業者の確保・支援	✓ IoT製品のセキュリティ強化、サプライチェーンの改善、業界全体にわたるリスク管理の徹底、国内企業のセキュリティ体制の強化を推進するため、事業者への対応義務付けと、支援体制を強化を進める。 ✓ EU加盟国と共同で運営されるパートナーシップのもと、NIS2指令準拠や技術的支援を通じた産業界の需要の掘り起こしによるサイバーセキュリティへの投資を誘発と、供給のマッチングを進めることで、民間投資の拡大を狙う。	➢ サイバーレジリエンス法案を発表。2025年後半適用に向けて審議中。施行されると、EU域内で販売するデジタル製品について指定のセキュリティ要件を満たす必要があり、世界中の製造業者に影響を及ぼす。こうした規制や枠組によって、欧州基準を標準化し、市場をリードする動きも。
	セキュリティ人材育成	✓ 専門的な教育プログラムと産業界の連携を通じ、サイバーセキュリティスキルを有する労働力の育成を推進し、テレワークやIoT機器の普及に伴う新たなリスクへの対応を強化。子供、若者、女性の人材育成や、労働市場全体としての意識向上を狙う。	➢ EU 全体のサイバーセキュリティ専門家の需要（職場、採用）と供給（資格、訓練）の間に共通の用語と共通の理解を得ることを目標に、ENISA European Cybersecurity Skills Framework (ECSF)を展開。
予算 等		✓ 新サイバーセキュリティ戦略では、2021年から2027年にかけて、公共および民間からのサイバーセキュリティ投資として**最大45億ユーロ**に達する可能性があることが言及されている。	

Appendix.

EUのサイバーセキュリティに関する政策の全体像 - EUサイバーセキュリティ戦略・指令等の変遷

- 以下のEUの戦略、法規制は、進化する枠組みの一部であり、それぞれが以前のものを基礎とし、EUのサイバーセキュリティ体制に新たな側面を加えている。これらは必ずしも上書きされるわけではなく、新たな課題や技術に対応するために更新されたり補足されたりする。2023年現在の主要な戦略は、「デジタル10年に向けたEUサイバーセキュリティ戦略」となっている。

EUサイバーセキュリティ戦略の変遷

EUサイバーセキュリティ戦略 The EU Cybersecurity Strategy （2013）	• サイバーセキュリティに関するEU初の包括的な政策文書であり、重要インフラの保護、協力関係の改善、加盟国全体のサイバーセキュリティ能力の開発を目的とし、サイバー脅威に対するレジリエンスの構築と、市民やビジネスが信頼できるデジタル技術から恩恵を受けることを目指す。
NIS指令 NIS Directive （2016）	• EU加盟各国がそれぞれの政府機関においてサイバーセキュリティの措置を講じることがEU基本の考えであるが、サイバーセキュリティの領域においては、欧州レベルで一定水準の維持が必要であること、国境をまたいだ脅威に対しては、協力が必要であることがNIS指令制定の背景。この法律により、**EU加盟各国は、国家サイバーセキュリティ戦略（NCSS）を策定し、採用することが義務付けられる**。現在は改正版のNIS2指令が成立している（2022年5月）。
サイバーセキュリティ法 Cybersecurity Act （2019）	• 製品、サービス、プロセスに対する欧州のサイバーセキュリティ認証の枠組みを確立。 • EUサイバーセキュリティ法に基づき、「EUサイバーセキュリティ庁（ENISA）」がEU各機関や各加盟国に対してベストプラクティス、法制度、市場振興について従来と同様に助言を行うと共に、各国の国境を越えた脅威や攻撃に対する対処を支援する役割を担う。
デジタル10年に向けた EUサイバーセキュリティ戦略 The EU's Cybersecurity Strategy for the Digital Decade （2020）	• 欧州委員会が、2030年に向けた欧州のデジタル化推進についての「デジタル10年」という戦略文書を発表し、欧州連合のデジタル化における戦略・目標を提示。「欧州のデジタルの未来を形作る（Shaping Europe's Digital Future）」と「安全保障同盟戦略2020-2025（Security Union Strategy 2020-2025）」の広範な枠組みの一部。 ※本資料では「新サイバーセキュリティ戦略」と呼ぶ。
NIS2指令 NIS2 Directive （2022）	• NIS2においては、監督執行体制の強化、欧州危機対応リエゾン（EU-CyCLONe）による大規模サイバー攻撃への対応支援、脆弱性開示、主要通信インフラのサプライチェーンのサイバーセキュリティ強化、インシデントの報告プロセスなどが新たに明確化・強化されている。また、すべてのEU機関、団体、行政機関（EUIBAs）を支援するCERT-EUが存在する。

2.2.4 英国

2.2.4. 英国① 国家サイバー戦略2022

- 「国家サイバー戦略2022」は、2016年に発表した「国家サイバーセキュリティ戦略」を引き継ぐものとして策定された、英国のサイバーレジリエンスの強化の方向性を示す戦略である。
- サイバー分野の重要技術に係る能力強化、個々のサプライヤーや特定の技術への依存脱却を中心目的としている。

国家サイバー戦略2022 概要

- **ビジョン**(vision)…2030年の英国の将来像。
- **柱**(pillar)…ビジョンを実現するための5つの戦略的目標。英国の価値観と利益を反映したサイバー空間を維持することを目指している。
- **アクション**(objective)…各柱のもと、2025年までに実施すべき具体的なアクション。

ビジョン(Vision)

国家目標(安全性と強靭性、科学技術大国、経済的繁栄、国際的秩序の構築)を支え、
サイバー空間における英国の利益を維持・増加させるため、責任のある民主的なサイバーパワーをリードし続ける。

柱 1 英国のサイバーエコシステムの強化	柱 2 強靭で豊かなデジタルUKの構築	柱 3 サイバーパワーに不可欠な技術における主導	柱 4 より安全・豊か・オープンな国際秩序のためのリーダーシップ・影響力の強化	柱 5 サイバー空間におけるセキュリティ強化のための敵対者の検知・妨害・抑止
アクション • サイバーに関する社会全体のアプローチを支えるために必要なストラクチャ・パートナーシップ・ネットワークを強化する。 • 世界レベルの専門家を含め、**様々なレベルで国家のサイバースキルを強化・拡大**する。 • 持続可能で革新的で国際競争力のある**サイバー・情報セキュリティ分野の成長を促進**する。	アクション • **サイバーセキュリティや強靭性に対する効果的なアクションを促す**ために、サイバーセキュリティリスクに関する理解を深める。 • **サイバーセキュリティリスクの管理の強化や国民の保護の強化**により、効果的にサイバー攻撃を防止・抵抗する。 • サイバー攻撃の準備・対処・回復により、国家・組織レベルで強靭性を強化する。	アクション • サイバーパワーに不可欠な技術の発展を予測・評価・実行する能力を向上させる。 • セキュリティにおいて主導権や**同盟関係の優位性を向上・維持**する。 • 次世代のコネクテッド技術・インフラを実現する。 • **国際的なデジタル技術標準を開発**するため、多くの関係者コミュニティと協力する。	アクション • **国際的なパートナーのサイバーセキュリティ・強靭性を強化**し、敵対者を混乱させ抑止するために協働する。 • 自由・オープン・平和・安全なサイバー空間を促進するため、グローバルガバナンスを構築する。 • 戦略的優位性等のため、**英国のサイバー能力・専門知識を活用・輸出**する。	アクション • 英国・国益・国民のため、国家・犯罪・悪意のあるサイバー攻撃者や活動を検知・調査・情報共有する。 • 国家・犯罪・悪意のあるサイバー攻撃者や活動を混乱させ抑止する。 • 国家安全保障と重大犯罪の防止・検知を支援するため、**サイバー空間の内部およびサイバー空間を通じた対策を実行**する。

➢ **ビジョンの達成に向けて2022年から3年間で、26億ポンドの投資を行う方針を表明。**

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（1/7）

- NIS規制に加え、通信ネットワーク分野等では独自の対策強化の制度措置を行っている。また、2025年までにレガシーITインフラへの投資による政府の重要機能の大幅強化を明言している。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
国家的なサイバーセキュリティのレジリエンスやリスクに係る言及	**【サイバーセキュリティリスクに関する認識】** • 戦略では、産業界/国家・社会/消費者のそれぞれについて、懸念されるリスクを以下のとおり指摘。 – 産業界：ITシステムのレガシー化、サプライチェーンの脆弱性、サイバーセキュリティ専門家の不足 – 国家・社会：国家主体、犯罪集団の攻撃による経済的損失、知的財産盗難、重要インフラリスク – 消費者：ランサムウェア被害、デジタル依存・デジタル格差の拡大、女性へのオンライン攻撃 **【サイバーレジリエンスの確保】** • 対策として、**レガシーITインフラへ投資を行い、2025年までに政府の重要機能を大幅に強化**すること、**公共部門全体が2030年までに既知の脆弱性と攻撃手法へのレジリエンスを獲得すること**を明記。 • また、**メーカー、小売業者、サービスプロバイダー、公共部門にはサイバーセキュリティの水準を高める責任を課す**、**サプライチェーンのリスクへの幅広い介入策を講じる**といった方針も示している。	➢ **NIS規制2018** • 指定の基幹サービス運営者と関連デジタルサービスプロバイダーに対して、ネットワークおよび情報システムを保護するための技術的・組織的措置の実施を義務付ける。 • エネルギー、運輸、医療、デジタルインフラ、デジタルサービスプロバイダー等が適用対象となる。
国の重要情報インフラにおけるサイバーセキュリティ・システムに関する要件	**【重要インフラにおけるサイバーセキュリティリスクの理解と対策の促進】** • 重要国家インフラ全体を通じたサイバーセキュリティリスクに対するより精密な理解の確立に向け、**Cyber Assessment Framework または同等の枠組みを重要国家インフラセクター全体で採用し、現在使用される他のサイバーセキュリティ評価・報告の枠組みとの比較可能性を改善する**としている。 **【重要インフラにおけるサイバーセキュリティリスクの管理】** • 戦略では、政府が関与した重要インフラにおけるリスク管理として、以下の方向性を示している。 – 事業者と密接に協力して、一般的攻撃手法へのレジリエンスの獲得と、より高度な保護のため、**NIS規制で指定する基幹サービス運営者に対して、各所轄官庁が設定する基準を満たすことを要求**。 – その実現のため、**重要国家インフラ事業者がサイバーセキュリティに投資し、サプライチェーンを含むリスクが効果的に管理されるよう、政府が事業者責任を追及する権限について見直し、規制の枠組みを強化**。	➢ **2021年電気通信(セキュリティ)法** • 通信ネットワーク/サービスのセキュリティに関する新たな枠組みを定める法律。 • セキュリティ侵害対応に係るプロバイダーの義務、その遵守のためのOfcomによる評価、強制、情報要求の権限などが盛り込まれている。

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（2/7）

- 英国では独自の取組みとして、Secure by Designの考え方に基づき、コネクティッド製品を利用する消費者や企業をサイバーセキュリティリスクから保護するための立法措置を講じている。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
中小企業やサプライチェーンにおけるサイバーセキュリティ強化のための政策	**【サプライチェーンにおける安全確保】** • 大規模被害を減らすため、デジタルサプライチェーンに由来する全システム的なリスクへの対策を行うとしている。具体的には、**必要に応じてサプライチェーンの多様化促進のために介入**するほか、**重要セクターにおける外国直接投資（FDI）の審査に堅牢かつ予測可能で適切なアプローチを採用**し、政府の重要かつ共通サプライヤーについて明確な要件を確立することに言及されている。 • また、英国のデジタル・サプライチェーンの安全確保のため、2025年までにデジタルサービスプロバイダーへの既存の規制を強化・拡大し、プロバイダーが自社サービス関連リスクをより積極的に管理するようにする方針も示されている。 **【中小企業等におけるサイバーレジリエンス強化】** • **個人事業主や小規模組織、消費者等のサイバーレジリエンス向上のため、NCSC（National Cyber Security Centre）を通じた技術的アドバイスや、自助的なツール、保証された製品・サービスが容易に利用できる環境を整備**するとしている。 • 具体的な支援策として、サイバーセキュリティ市場の活用支援として、保証製品・サービスのための枠組みの拡張や、Cyber Essentialsに関する中小企業向けの商業サービスを開発などが挙げられている。	➢**PTSI法** • **英国の消費者向けコネクテッド製品のメーカーに対して、最低限のセキュリティ要件を遵守することが義務付ける法律**。(2024年4月施行予定) • スマートフォンやスマート機器等のメーカーに対して主に以下のセキュリティ要件を課す。 – 共通/容易に推測可能なデフォルトパスワードの禁止 – 製品がセキュリティ更新受けられる期間に関するメーカーの透明性向上 – メーカーによるセキュリティ更新サポート期間について顧客に知らせることを義務付け – デバイスに関連する脆弱性の報告を受け付けるための連絡先を公表 ➢**Cyber Essentials** • **オンラインによる自己診断アンケートに回答することで、最も一般的なサイバー攻撃からの幅広い保護レベルを証明する認証制度**。

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（3/7）

- グローバルなデジタル技術標準の主導を進めるとともに、国内向けにはNCSCの認定制度によりサイバーセキュリティ製品・サービスの水準確保を図っている。

② 国際協調の推進

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティに関する標準の実施状況	**【国際標準等に関する政府としての方針】** • 戦略では、**グローバルなデジタル技術標準のエコシステムに、マルチステークホルダーが積極的に参加していることを目指す**旨が示されている。 • 具体的には、**重要な標準化団体へのマルチステークホルダーの参加を強化**し、**国際電気通信連合への英国代表団を通じてモデルを示していく**こと、国連インターネットガバナンスフォーラムやその他のフォーラムを通じたオープンな議論を促進することなどが言及されている。 • さらに英国がG7議長国を務めた時に設立されたデジタル標準ポイントオブコンタクト・グループ（Digital Standards Points of ContactGroup）等を通じたパートナー諸国との連絡・調整にも言及されている。 **【重要システム等における調達基準】** • **NCSCのCyber Assessment Frameworkを全政府機関のアシュアランスフレームワークとして採用し、重要システムと共通サプライヤーのマッピングを行う**とされている。 • さらに、**公共部門の調達をより効果的に活用し、高品質のサイバーセキュリティ製品およびサービスの需要を喚起するため、NCSC認定プロバイダーの総合ディレクトリを確立を目指す**としている。	➢**Cyber Assessment Framework(CAF)** • NCSCによって開発されたフレームワークで、重要国家インフラ（CNI）部門を含む民間部門全体で広く使用される。 • CAFは一貫性のある比較可能な方法で、サイバーレジリエンスを評価し、的を絞った改善活動を可能にする。

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（4/7）

- 5G/6GやAI等のサイバー領域に重要な技術での技術優位の確保や今後対象となる新興技術の分析に注力している。
- また、研究成果のビジネス化に向けた支援プログラムによる、産学連携でのイノベーション創出を図っている。

③ 研究力・技術力の強化、独立性確保

項目	戦略上の記載	関連する規制/政策
自国のサイバーセキュリティ産業の育成のために、政府が支援する研究開発の取り組み	**【サイバーセキュリティに係る研究開発の方針】** • **将来のサイバー空間に必要不可欠な技術(5G/6G、AI、ブロックチェーン、半導体、暗号認証、IoT、量子暗号等)で主導的な役割を確立する**ことが、自国の安全保障と経済的優位を守ることになるとの認識を示している。 • その上で、英国が、サイバー大国としての目標を達成するためには、重要技術への関与を維持し、競合国や敵対国への過度の依存を回避するために、より野心的かつ積極的なアプローチが必要とされているとし、**NCSC等の技術的専門知識の主導のもと、サイバーパワーにとって最も重要な技術分野を特定する能力の強化**と、特定の分野で英国の国内の能力開発に必要な研究開発活動や戦略的パートナーシップに投資していくとしている。 **【サイバー領域に重要な分野の特定】** • NCSCの新応用研究ハブを始めとして研究能力を拡大し、コネクテッドプレイスや運輸等の分野における**新興技術の分析に焦点**を当てていくとしている。また、**4つのサイバーセキュリティ研究所と19のサイバーセキュリティ卓越研究センター（ACE）を支援**するとともに、優先的テーマを扱う研究者の表彰等を実施する旨も言及されている。 • その他、科学技術の進歩とそのサイバーへの影響を予測するために、内部的な**ホライズンスキャンニング機能を新設**するとされている。 **【研究成果のビジネス化】** • 産学連携でイノベーションおよび研究開発を活性化させる協調的アプローチが必要であるとの認識の下、英国政府は、全国の研究者が産業界のパートナーと協力して**課題ベースのアプローチを採用し、研究成果を商業化・実用化していくことを支援**するとしている。	➢ **Cyber ASAP** • 商業化される学術研究の量を増やすことを目的としたプログラム。重要分野の研究を技術、製品、サービスに転換するために必要な専門知識、トレーニングを大学の研究者等に提供する。 ➢ **サイバーセキュリティ卓越研究センター（ACE）** • NCSCが国際的に主要なサイバーセキュリティ研究を行っている英国の大学を認定する制度。 • サイバーセキュリティ研究への大学としてのコミットメント、スタッフ数、研究の影響評価等を踏まえて認定される。

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（5/7）

- 英国ではサイバーセキュリティ産業分野を輸出産業と位置付け、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を行っている。

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業の保護、振興に関する位置づけ	**【サイバーセキュリティ産業の位置づけ】** • 戦略では、**サイバーへの全社会的アプローチを中心に据え**、官民、第3セクターのパートナーシップを構築し、それぞれが役割を果たすことが必要としている。その中で、サイバーセキュリティセクターは、英国が直面する新種のサイバー脅威・課題に対応する重要な役割を担うと位置付けている。 **【「サイバーエコシステム」の確立とサイバーセキュリティセクターの成長促進】** • 戦略では、**サイバーパワー**(=国益の保護と増進を、サイバー空間の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」の強化を据えている。** • アクションとして、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。	➢**国家安全保障・投資法2021** • 国家安全保障上の懸念が生じやすい17の主要分野を対象に、これらの分野に関わる取引を行う企業や投資家が、対象英国企業の株式/議決権を25%以上取得する場合に政府への通知を義務付ける。 • 17の分野には、通信、暗号認証、データインフラ、量子技術、政府への重要なサプライヤ等が含まれる。
国家安全保障／経済安全保障の観点から、サイバーセキュリティ産業を保護するためにとられている政策／措置	**【国外からの投資規制や知的財産流出の防止】** • 大規模被害を減らすため、デジタルサプライチェーンに由来する全システム的なリスクへの対策を行うとしている。必要に応じてサプライチェーンの多様化促進のために介入するほか、**重要セクターにおける外国直接投資（FDI）の審査に堅牢かつ予測可能で適切なアプローチを採用**し、政府の重要かつ共通サプライヤーについて明確な要件を確立する。(再掲) • 重要サイバーセキュリティ技術分野におけるイノベーションと知的財産の保護のため、**対英直接投資のリスクについて、国家安全保障・投資法2021の目標に沿った助言**を行うことや、産業界・学術界と協力して信頼性の高い環境を整えること、データや知的財産の盗難を防止する強固な手段を開発していくことに言及している。 **【サイバーセクターの輸出に関する方針】** • 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、以下の取組みの実施に言及。 – 世界的なサイバーイベントの国内開催支援や、特にイノベーション力のあるサイバー企業のトレードミッションや国際サイバーフェアへの招待による、**サイバー企業の国内外の新市場への進出の支援** – **世界各国の政府と主要な商業顧客をターゲット**に、サイバーセキュリティ・アンバサダープログラムおよび国際ネットワークの下、**政府間の国際協力の活発化を通じたPR**の実施 – 有力な輸出業者として対英投資を呼び込めるよう、イノベーションから輸出に至るあらゆる段階で英国全土の企業を支援 – 新しい輸出ファカルティ（Export Faculty）の創設等、中小企業への支援強化 – サイバーパワーのキャンペーン事務局を設立し、大々的な輸出キャンペーンを体系的かつ組織的に支援	

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（6/7）

- サイバーセキュリティ産業のイノベーション強化の中核に、スタートアップの成長・拡大を位置づけ、伴走支援や投資の促進等を行う。また、地方部におけるサイバークラスターの構築にも注力している。

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業を促進するための事業者を対象にした支援政策/施策	**【サイバーセキュリティ技術・製品等の品質向上】** • サイバーセクターの成長に向けた政策として、より多くの企業が、品質基準を満たすサイバーセキュリティ技術、製品、サービスを提供し、ユーザーの信頼感を高めるために、**NCSCのブランドと専門知識を活用しつつ、消費者が安心してサービスを購入できる信頼のおけるマーケットプレイスを構築**するとしている。 • また、**公共部門の調達をより効果的に活用し、NCSC認定プロバイダーの総合ディレクトリを確立して、高品質のサイバーセキュリティ製品およびサービスの需要を喚起**することにも言及されている。 **【サイバーセクターのイノベーション/スタートアップ支援】** • サイバーセクターのイノベーション力をさらに高めるため、以下の**スタートアップの成長・拡大に取り組む**としている。 – 新たなアクセラレータープログラムの**Cyber Runway（サイバーランウェイ）**の実行 – 全国の研究者が産業界のパートナーと協力し、**研究成果を商業化・実用化していくこと**を支援 – サイバーアクセラレータ機能を持つイノベーションセンターの国家サイバーイノベーションセンターへの転換 –「National Security Technology and Innovation Exchange」などの共創促進・支援のための既存組織の専門知識の活用 – 国営英国ビジネス銀行（British Business Bank）と提携し、**初期段階にあるサイバー新興企業への高リスク投資**の促進 **【地方部におけるサイバークラスターの構築支援】** • 英国全土でサイバーネットワークを構築するため、国家サイバー部隊の常設本部をイングランド北西部地方に設置して、テクノロジー、デジタル、防衛の**各セクターの成長をロンドン以外で促進**し、地域の新たなパートナーシップの構築を支援していくほか、ロンドンおよびイングランド南東部地方以外の地域のイノベーターや起業家が、製品やサービスを開発し、ビジネスを成長させ、高スキルのスタッフを採用するための支援を強化する方針を示している。	➢**Cyber Runway** • 起業家、スタートアップ企業等を対象に、ビジネススキル、技術、資金調達等のプログラムを通じて、事業の立ち上げ、成長、規模拡大を支援する ➢**UKC3（UK Cyber Cluster Collaboration）** • 地域のサイバーセキュリティクラスターの能力を高めることを目的とした政策 • 地域内のサイバー活動への認識と理解、サイバー産業への人材パイプラインの育成、地域内での新しいサイバー・ビジネスの創出などを支援する。

2.2.4. 英国② サイバーセキュリティ産業政策調査結果（7/7）

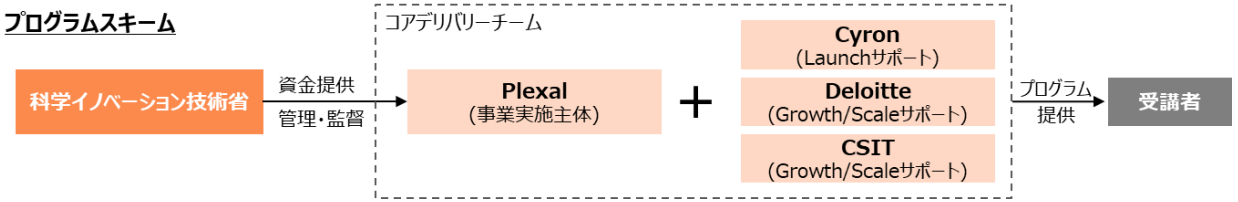
- セキュリティスキルを有する人材の拡大を大きな方針として示しつつ、サイバーセキュリティに関する職業基準の確立、政府によるサイバー専門職の採用、女性の活躍促進等が取り組みのターゲットとなっている。

⑤ セキュリティ人材育成

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修、教育プログラム等の開発支援	**【サイバー労働力として必要なスキルを持つ人材の拡大】** • 戦略では**2030年までに16歳以上のサイバー教育と訓練を、産業界主導で策定された基準に適合するよう強化する**としており、具体的に以下のような教育・スキル政策を実施するとしている – 16歳以上を対象としたサイバー労働力に必要な訓練プログラムの拡大 – サイバーセキュリティ分野の様々なスキルアップ合宿への資金提供 – 技術研究所プログラムの全国展開 – 大学生を対象としたサイバーファースト奨学金制度の継続　等 • また、**高スキル人材を国内教育制度を通じて安定的かつ多様に輩出する**ため、これまでよりも多くの若者がテクノロジー分野のキャリアを目指すよう、教育を通じた奨励・支援や、多くの学生の関心喚起に取り組む方針も示されている。 **【体系的なサイバーセキュリティ専門職の育成】** • 戦略では、**英国サイバーセキュリティ会議を中心にサイバーキャリアの職業基準を確立**した上で、これらの基準を職業全体に定着させ、卓越性と専門性が認識されるように、法律を含めてあらゆる政府の手段を検討していくとしている。 • また、**政府が率先して必要なサイバー専門職を特定、採用、訓練し、保持することが必要**であるとし、政府内でのサイバーセキュリティ実習制度の拡充を通じた若年人材への投資や、専門スキルプログラムの支援、Defence Cyber Academyの活用等に取り組むとしている。	➢ **英国サイバーセキュリティ会議** • 世界初のサイバーセキュリティ職業団体。 • 明確で一貫性のある職業基準の設定や、既存の資格の中から効果的な資格を特定するなどの取組みを行う。 ➢ **CyberFirst** • 多様な才能ある若者を発掘し、サイバーセキュリティのキャリアに育てることを目的とした人材育成プログラム。 • CyberFirst奨学金、女子学生のコンペティション、国内大学での無料のサイバー関連コースの提供等を行う。
サイバーセキュリティ業界の労働環境に関する受け止め	**【多様な人材の活躍】** • 戦略では、サイバーセキュリティ人材の現状について、**セクターの労働人口に占める女性の割合は16%にとどまり**、上級職に限って見れば女性やエスニックマイノリティの割合はわずか3%となっていると指摘している。 • その対策として、例えば、サイバー労働市場への女性の進出の支援や、少数派グループがハイレベルのキャリアを実現できるよう支援する特定の介入策等の方策を通じて、**英国内の少数派グループや不利な立場にあるコミュニティの出身者がサイバー分野の職業に就いて活躍できるよう支援を行う**としている。 • また、英国の主要プログラムであるサイバーファースト（CyberFirst）の活用についても言及されている（例えばサイバーファースト女子学生コンペティション）。	

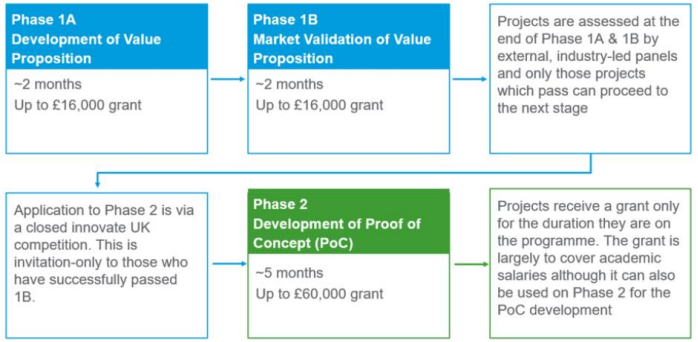
2.2.4. 英国③ サイバーセキュリティ産業政策 個別施策調査（1/3）

- 「Cyber Runway」は起業家・スタートアップ企業の育成を目的としたプログラムであり、これまで160件以上の支援を行っている。

支援施策	Cyber Runway
所管省庁・関係団体	• 科学イノベーション技術省(Department for Science, Innovation and Technology) • Plexal、Deloitte、Centre for Secure Information Technologies、Cyron
支援対象	• サイバーセキュリティ分野のスタートアップ企業、起業家
支援概要・スキーム	• 起業家やスタートアップ企業に、ビジネスを立ち上げ、成長させ、拡大するための総合的なスキル、リレーションを提供することを目的に、以下の3つのコースを提供する。 – Launch:関連するアントレプレナースキルを開発し、潜在的な共同創設者と出会い、新しいビジネスを確立するための支援 – Growth:企業の成長、資金調達、商業的成功を達成するための支援 – Scale:英国内およびグローバルで急速にビジネスを拡大させるための支援 • 各コースでは、ビジネススキルの習得、法律、財務、マーケティング等専門家による助言、技術的なサポート(機能テスト等)、投資家向けピッチ、コミニュティ構築、グローバル展開支援、e-Learningコンテンツの利用などの各種支援が提供される。 
予算規模	• 国家サイバー戦略2022実行のための26億ポンドの内数(詳細不明)
実績等	• Cyber Runwayを通じて160以上の起業家、スタートアップ企業、中小企業が支援を受けた。 • 2022年のプログラムに関するレポートでは、Growコースの20%、Scaleコースの45%の受講者が収益の増加を報告。 • 従業員についても、Growコースの22%、Scaleコースの71%が正社員数の増加を報告。
参照	• 本プログラムの必要性に関し、サイバーセキュリティセクターへの投資の対象は大企業・中堅企業に偏っていること、学術研究をビジネス化していくことには障壁があることなどが言及されている。
参照	• https://www.gov.uk/government/publications/evaluation-of-the-cyber-runway-programme • https://www.plexal.com/our-work/cyber-runway/

2.2.4. 英国③ サイバーセキュリティ産業政策 個別施策調査（2/3）

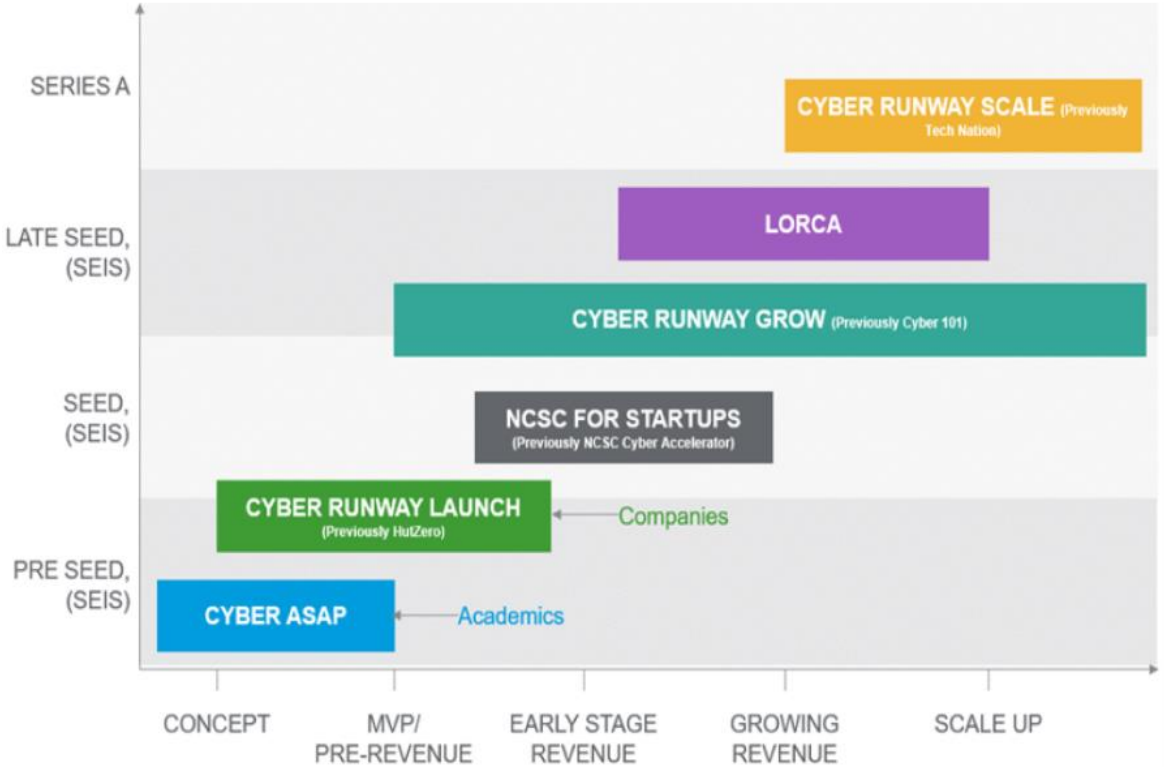
- 「Cyber ASAP」はコンペティション型の研究者向けプログラムであり、約30のスタートアップ企業が生まれている。

支援施策	Cyber ASAP
所管省庁・関係団体	• 科学イノベーション技術省(Department for Science, Innovation and Technology) • Innovate UK • Knowledge Transfer Partnership (KTP)
支援対象	• 英国の学術機関に拠点を置き、サイバーセキュリティに関するシーズを有する個人
支援概要・スキーム	• 英国のサイバーセキュリティ研究の商業化の支援と、学術研究者の起業家としてのスキルを高めることを目的としたプログラム。2017年から実施されている。 • 現在のCyber ASAPは選考フェーズと概念実証(PoC)フェーズの2つで構成(下記参照)されており、選考フェーズでは最大32,000£、PoCフェーズでは最大60,000£が資金提供される。 – **選考フェーズ**:選考フェーズはさらに2つのステージに分かれ、ステージ1ではブートキャンプ等での研究価値の開発活動と、独立審査員による評価を経て、ステージ2に進むチームが選ばれる。ステージ2ではさらに2ヶ月間の市場検証活動が行われた後、PoCフェーズに進むチームが選ばれる。 – **PoCフェーズ**:ブートキャンプやケーススタディ、プレゼンテーションスキルの習得、投資家とのミートアップ、専門家による助言等の各種支援を受けつつ、デモの開発を行う。 
予算規模	• 80万ポンド(2023年)
実績等	• 2017年の設立以来、英国全土の大学から100チーム以上のイノベーション開発を支援 • 2023年で約30のスタートアップ企業が創設されるとともに、サイバーセキュリティのアイデアのビジネス化のために、Cyber ASAPの卒業生が1,900万ポンド以上の資金を確保
参照	• Cyber Runwayと同様、本プロジェクトの背景として、サイバーセキュリティセクターへの投資の対象は大企業・中堅企業に偏っていること、学術研究をビジネス化していくことには障壁があることなどが言及されている。
参照	• https://apply-for-innovation-funding.service.gov.uk/competition/1526/overview/6d7f9d87-c620-4b64-a3ed-95d6dccc0c7d#summary • https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator/evaluation-of-the-cyber-security-academic-startup-accelerator

2.2.4. 英国③ サイバーセキュリティ産業政策 個別施策調査（参照）

- 「Cyber Runway」と「Cyber ASAP」はターゲット層を異にしており、「Cyber ASAP」はプレシード段階の概念実証に焦点を当てたプログラムである。

「Cyber Runway」と「Cyber ASAP」のターゲット領域



NCSC for Startups：NCSCが提供するスタートアップ企業向けのアクセラレータープログラム。対象は英国に籍を置く企業に限られ、NCSCの専門家からの知見やアドバイスが提供される。
LORCA：スタートアップ企業向けに、オフィス施設や投資家・専門家とのネットワークの提供を通じて規模拡大を支援する事業。(現在終了)

参照：Evaluation of the Cyber Security Academic Startup Accelerator
https://www.gov.uk/government/publications/evaluation-of-the-cyber-security-academic-startup-accelerator

2.2.4. 英国③ サイバーセキュリティ産業政策 個別施策調査（3/3）

- NCSCでは独自の基準を満たす222のサイバーセキュリティ製品・サービス等をHPで公開している。

支援施策	NCSCによるサイバーセキュリティ製品/サービスの保証スキーム
所管省庁	• NCSC
支援対象	• サイバーセキュリティ企業
支援概要・スキーム	• NCSCでは、サイバーセキュリティの特定の分野ごとに、NCSC基準に照らして独自に評価し、基準を満たすサイバーセキュリティの専門知識、製品、サービスに関する詳細をHPで公開している。 • この取り組みは、NCSCのブランドへの高い信頼を利用して、サイバーセキュリティ企業が高品質の製品またはサービスを提供していることを広く示すことを支援目的としている。 • NCSCにより認定される製品/サービスは11のカテゴリに分けられる(右記参照)。 • 認定の基準は個々のカテゴリごとに設定されている。例えば、「1. Certified Assisted Products (CAPS)」に関しては、政府の機密データを保護するための暗号化に関する承認基準を定めた「HMGポリシー」を満たしているかの確認が行われる。 **認定製品/サービスのカテゴリ** 1.Certified Assisted Products (CAPS) 2.Cyber Security Consultancies 3.Certified Cyber Professionals (CCP) 4.Certified Training 5.Certified Degrees 6.Penetration testing (CHECK) 7.Commercial Product Assurance (CPA) 8.Assured Services (CAS) 9.Cyber Incident Response (CIR) 10.Tailored Assurance (CTAS) 11.Cyber Advisor
予算規模	N/A
実績等	• 2023年11月時点で222の製品/サービスが保証済みのものとして公開されている。
参照	• 親会社が国外に位置する、いわゆる英国の現地法人の製品/サービスについても登録されている(Thales、Airbus等)。
参照	• https://www.ncsc.gov.uk/section/products-services/verify-suppliers

2.2.4. 英国④とりまとめ

- 英国の国家サイバー戦略(2022)の特徴・傾向と、その現況・評価。

大項目	小項目	特長・傾向	現況・評価
政策関係	サイバーセキュリティ対策の強化	✓NIS規制に加え、通信ネットワーク分野等では独自の対策強化の制度措置を行っている。また、2025年までに**レガシーITインフラへの投資による政府の重要機能の大幅強化**を明言している。 ✓独自の取組みとして、Secure by Designの考え方に基づき、**コネクティッド製品を利用する消費者や企業をサイバーセキュリティリスクから保護するための立法措置**を講じている。	• 政府・独法に毎年サイバーセキュリティの検証と見直しを求める新しいサイバー保証スキーム「GovAssure」を開始 • 27,000以上の組織がCyber Essentials/Cyber Essentials plusの認証を受ける • 監査と企業報告の改革を進め、大企業のアニュアルレポートに、デジタル・セキュリティに関する記載を求める、新たな「レジリエンス・ステートメント」の導入の議論
	国際協調の推進	✓グローバルなデジタル技術標準の主導を進めるとともに、国内向けには**NCSCの認定制度によりサイバーセキュリティ製品・サービスの水準確保**を図っている。	• ITU理事会の議席の確保、OECDデジタルセキュリティ勧告への貢献、フランスをはじめ11か国とのパートナーシップ(2023年) • NCSCによる保証済みの222の製品/サービスが公開(2023.11)
	研究力・技術力の強化、独立性確保	✓**5G/6GやAI等のサイバー領域に重要な技術での技術優位の確保や今後対象となる新興技術の分析に注力している**。 ✓また、研究成果のビジネス化に向けた支援プログラムによる、産学連携でのイノベーション創出を図っている。	• Cyber ASAPを通じて、30のスタートアップ企業が創設(2023年) • 19の大学がサイバーセキュリティ研究における卓越拠点(ACE, Academic Centres of Excellence)に認定
	国内事業者の確保・支援	✓英国ではサイバーセキュリティ産業分野を輸出産業と位置付け、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を行っている。 ✓サイバーセキュリティ産業のイノベーション強化の中核に、スタートアップの成長・拡大を位置づけ、伴走支援や投資の促進等を行う。また、地方部におけるサイバークラスターの構築にも注力。	• サイバーセキュリティセクターの企業数は1,979社で、売上高は104.6億ポンド超で前年比約3%の成長(2023年) • 輸出額は約50億ポンドで前年比20%増(2022年) • サイバーセキュリティ専業企業の2022年の投資調達額は、2021年比で減少
	セキュリティ人材育成	✓セキュリティ人材の拡大を大きな方針として示しつつ、サイバーセキュリティに関する職業基準の確立、政府によるサイバー専門職の採用、女性の活躍促進等が取り組みのターゲットとなっている	• 英国の全地域で5,300人以上の雇用が増加(2023年) • サイバーセキュリティ人材に占める女性の割合は約22%で、2020年から7%増
予算 等		✓国家サイバー戦略の達成に向けて2022年から3年間で、26億ポンドの投資を行う方針を表明	

2.2.5 韓国

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果（1/7）

- 「国家サイバーセキュリティ戦略」に基づき、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発展を強調。重要インフラを運営する機関に対して、国が予算上の支援を提供している。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
国家的なサイバーセキュリティのレジリエンスやリスクに係る言及	**【サイバーレジリエンスの確保】** • 「国家サイバーセキュリティ戦略」は、サイバー攻撃に対する即座の対応、中核インフラの安全性の確保、およびサイバー攻撃への耐性強化に焦点を当てている。 　• 国家情報通信ネットワークサービスのレジリエンスを強化する措置を講じることで、様々なサイバー攻撃があった場合でもサービスの提供を保証することを目指す。 　• サイバー攻撃に対して国家中核インフラのセキュリティとレジリエンスを強化し、重要なサービスの継続的な提供を保証することが強調される。	
国の重要情報インフラにおけるサイバーセキュリティ・システムに関する要件	**【国の情報通信ネットワークのセキュリティ強化 & 重要インフラのサイバーセキュリティ環境の改善】** • 6つの戦略的課題のうち、の１つめ「国家機関インフラの安全性を高める」において、国の情報通信ネットワークセキュリティの強化、および重要インフラのサイバーセキュリティ環境の改善に関して、それぞれの行動指針が示されている。（以下は一例を抜粋） 　• 多様なサイバー攻撃に直面してもサービスの提供を保証するため、システム性能の向上やバックアップ設備の拡充など、国内の情報通信ネットワークサービスの耐障害性を強化するための措置を講じる。 　• 国内情報通信ネットワークの構築において、国内および国際的な技術基準の遵守を強化し、安全保障上のインシデントが発生した場合の迅速な対応を促進する。 　• 政府が攻撃時の混乱により人々の日常生活を著しく不安定にする**重要なインフラ施設を指定し、迅速に保護できるように制度を改善**する。 　• **重要インフラを運営する機関がサイバーセキュリティ専門の部門を創設し、サイバーセキュリティに十分な予算を割り当てるよう支援**する。 　• 重要インフラを構築する初期段階でセキュリティを考慮し、関連する検査スキームを作成するためのガイドラインを発行する。 　• 民間インフラ事業者が取得したネットワーク・情報機器のセキュリティ評価を自主的に実施できる環境を整備する。 　• セクター固有のセキュリティ脆弱性の評価基準を作成し、セキュリティインシデントが発生した場合でもサービスを継続できるように対策を講じる。	➢ **情報通信インフラ保護法** • 重要情報インフラ（CII）を、国家安全保障、行政、防衛、治安、金融、通信、運輸、エネルギーなどに関連する産業制御システムや情報システムと定義し、国家的・社会的重要性を考慮した上で指定された重要CIIについて、特別な保護手続きを定めている。 • 年1回の脆弱性評価が義務付けられており、MSITはNISと協議の上、MSITが標準手順と評価基準を定める。

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果（2/7）

- 「国家サイバーセキュリティ戦略」文書上はサプライチェーン強化に関す直接的な言及はないが、重要インフラシステムの保護においては国の機関であるインターネット振興院が役割を果たしている。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
サプライチェーンにおけるサイバーセキュリティ強化に関する施策	**【サプライチェーン強化に関する取り組み】** • 直接の言及なし（ICT製品やサービスに関し「セキュリティ・バイ・デザイン」を導入する考えは示されている。）	➢ 戦略文書上はサプライチェーンに特化した言及はないもの、韓国では、インターネット振興院（KISA）内にあるサイバー侵害対応本部が、民間を含む重要インフラシステムのセキュリティ管理を行っている。

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果（3/7）

- サイバーセキュリティにおける国際協力を主導することを戦略文書で掲げており、二国間・多国間の協力体制の充実を図る。
- サイバーセキュリティに特化したものではないが、直近の事例として韓・英間で締結されたデジタルサービス強化の覚書がある。

② 国際協調の推進

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティに関する標準の実施状況	**【サイバーセキュリティにおける国際協力をリードする】** • 国際パートナーシップを強化し、国際ルールの形成を主導することにより、サイバーセキュリティの主導国となる **【二国間および多国間の協力体制の充実】** • 二国間・多国間の実務協力の手段を模索し、サイバー政策に関する協議の開催、国際機関との連携強化、国際協定への加盟等による相互支援体制を構築する。 • 戦争行為、テロ行為、犯罪行為を含むサイバーセキュリティの脅威に対応するため、国防、情報、法執行などの分野での協力や民間セクターとの交流を促進する。 • 国際協力のプロセスを通じて、関係機関が政府に政策の方向性を提案し、収集した情報を共有できるような仕組みを提供する。 **【国際協力におけるリーダーシップの確保】** • サイバーセキュリティに関する普遍的に受け入れられる国際ルールを確立するプロセスへの参加を増やし、国際ルールとベストプラクティスの普及を主導する。 • サイバー空間における誤解による国家間のエスカレーションを防ぐため、信頼構築に関する議論を積極的に行う。 • 途上国へのサイバーセキュリティ能力構築のための外国援助プロジェクトを互恵的な方法で拡大し、サイバーセキュリティ技術とシステムを共有する。	➢ **ISMS** • 国際的に認められたサイバーセキュリティ基準を実装するためのフレームワークである情報セキュリティ管理システム（ISMS）が、韓国でのサイバーセキュリティフレームワークとして公式に承認されている。 • 国内の電気通信、金融、エネルギー、運輸、公衆衛生などの公的機関や重要インフラ事業者にISMS認証の取得を義務付け。 • その他、ITU-T X.509、NIST CSF、PCI DSS、IEC 62443 などの他の国際標準とフレームワークも参照。
グローバルなサイバーセキュリティ・アライアンスにおける、自国のサイバーセキュリティプレーヤーの位置づけ	※戦略上の記載はない	➢ 韓国は英国と今年11月に政府デジタルサービスを強化するための覚書(MOU)に署名。ベストプラクティス共有を模索。 ➢ 英国NCSCと韓国NIS（国家サイバー安全センター）は、北朝鮮Lazarusが、韓国のDream Security社が開発したソフトウェアのゼロデイ脆弱性を悪用していることを警告。

- 国家の安全保障の観点からのサイバーセキュリティ態勢の強化を強調している。MSIT（科学技術情報通信部）やKISA（インターネット振興院）などの国の機関が主導し、予算上の支援も含めたサイバーセキュリティ産業支援を行う。

③ 研究力・技術力の強化、独立性確保

項目	戦略上の記載	関連する規制/政策
自国のサイバーセキュリティ産業の育成のために、政府が支援する研究開発の取り組み	**【次世代サイバーセキュリティインフラストラクチャの開発】** • 技術の融合と新技術の出現によって引き起こされる新たなセキュリティ脅威に対応するための技術的および制度的計画を準備する。 • 人々の生活に直接影響を与えるICT製品やサービスに「セキュリティ・バイ・デザイン」を導入し、安全を確保する。 • サイバー脅威から根本的に保護された高保証ネットワークを開発および配布する。 • 次世代の**セキュリティ認証インフラストラクチャを確立**し、ハイパーコネクテッドかつ AI 主導の環境で国民がオンライン サービスを便利かつ安全に利用できるようにする。 **【大規模サイバー攻撃に対する態勢強化】** • **国家の安全とサイバー戦争における利益を守るため、さまざまな戦略と戦術を開発し、軍事力を強化**し、中核技術を獲得する。 **【サイバーセキュリティ産業の成長基盤の構築】** • サイバーセキュリティ産業の革新的なエコシステムを構築し、国家のサイバーセキュリティにとって重要な技術、人材、産業の競争力を確保する。 **【サイバーセキュリティ投資の拡大】** • 国のサイバーセキュリティレベルの向上においてサイバーセキュリティ業界が重要な役割を果たせるよう、規制改革と支援を推進する。 • 政府の情報セキュリティ関連予算を継続的に拡充するとともに、大規模なサイバー攻撃への対応など、緊急時に活用できるような資金調達策を考案する。 • **「情報セキュリティの公示」制度を推進し、民間企業の投資を促進**するとともに、セキュリティ・システムや研究開発への投資に対する税制上の支援を拡充する。 **【セキュリティ人材と技術の競争力を強化する】** • サイバーセキュリティの研究開発予算を大幅に増額し、先進国との技術格差を縮め、世界市場をリードする革新的な中核技術を獲得する。	➢**サイバーセキュリティ産業開発基金** • サイバーセキュリティ産業発展法によって設立された、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基金。 • MSIT（科学技術情報通信部）とKISA（インターネット振興院）によって管理。 • この基金の総予算2016年から2025年までの1.5兆ウォン(約13億米ドル)のうち、20%をスタートアップ支援に配分。

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果（5/7）

- 戦略文書上、サイバーセキュリティ企業の成長環境を醸成することが強調されている。
- KISAが設立した政府によるスタートアップ支援の目玉として「創造経済革新センター」の取り組みがある。

④ 国内事業者の確保・支援1/2

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業の保護、振興に関する位置づけ	**【サイバーセキュリティ企業の成長環境の醸成 】** • 産学研究機関の連携による起業環境の醸成。情報セキュリティクラスターを構築し、革新的な技術やアイデアの商品化を可能にする。 • サイバーセキュリティの新興企業や中小企業が競争力のある企業に成長するよう育成するための制度を政府の支援を強化し、継続的に改善する。 • サイバーセキュリティサービスの適正価格を保証する方法を考案し、違法な下請け行為を徹底的に調査し是正する • 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。	**➢創造経済革新センター** • 政府のスタートアップ支援の目玉としてKISAによって全国各地に設立された産官学連携組織。 • サイバーセキュリティを含む「5G、IoT、ICT、人工知能」の分野のKISA認定ベンチャー企業は、京畿道にある大学キャンパスほどの施設を格安で利用できる。 • 社員は兵役免除の特典がある。 • 教育設備も充実しており、半年で4000人が1週間コースを受講。サイバー演習ができる設備もある。教育プログラムは米国のフレームワークを利用。 **➢ サイバーセキュリティ産業発展法** • 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。 **➢ 外国人投資促進法** • 特定分野への外国投資を制限。 **➢ 対外貿易法** • サイバーセキュリティに関連する技術の輸出管理。
国家安全保障／経済安全保障の観点から、サイバーセキュリティ産業を保護するためにとられている政策／措置	**【サイバーセキュリティ文化を育む】** • 人々がサイバーセキュリティの重要性を認識し、**日常生活で容易に実践できるよう、サイバーセキュリティの基本ルールを策定・配布**する。 • 学生、政府関係者、軍関係者、企業従業員など、社会の特定分野にカスタマイズしたサイバー倫理とセキュリティの教育プログラムを開発し、採用する。 • **企業の社会的責任を強化し、サイバー空間を保護**し、製品とサービスにおいて適切なレベルのセキュリティを維持する。	

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果（6/7）

- 戦略文書においてサイバー攻撃の改善を強調し、「国家安保室」が中心となり、民・官・軍が連携する体制がとられている。
- 政府の資金面での支援によって産業育成が図られている。

④ 国内事業者の確保・支援2/2

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業を促進するための事業者を対象にした支援政策/施策	**【官民軍事協力体制の促進】** • サイバー攻撃への対応を改善し、関係機関間の協力を強化し、支援機関のリソースを拡大することにより、民間部門におけるサイバーセキュリティの盲点を減らす努力をする。 • **公共部門におけるセキュリティの自己管理システムを確立**するために、専門組織や専門家を拡充し、民間部門との協力を促進する。	➢ **国家安保室（NISとKISAを配下に置いている）** ➢ **サイバーセキュリティ産業開発基金（MSITとKISAが予算管理）** ➢ **創造経済革新センター（KISAが設立）**

2.2.5. 韓国② サイバーセキュリティ産業政策調査結果 （7/7）

- 高度なサイバーセキュリティの脅威に対し、サイバーセキュリティ要員に世界レベルの専門知識と競争力を備える必要性を強調。
- 政府が後援する「情報セキュリティ大学院（GSIS）プログラム」を通じ、トップ大学への支援や奨学金・研究助成金を提供。

⑤ セキュリティ人材育成

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修、教育プログラム等の開発支援	**【セキュリティ人材と技術の競争力の強化】** • 高度なサイバーセキュリティの脅威に対応するため、サイバーセキュリティ要員に世界レベルの専門知識と競争力を備える。 • 企業、政府、軍、社会に多様な能力を備えたサイバーセキュリティ人材を提供するため、カスタマイズされた人材育成プログラムを強化する。 • サイバーセキュリティの専門性を向上させ、優秀な人材を確保するための方策を考案する。 **【韓国インターネット振興院（KISA）における施策】** 2022年に韓国政府公表した北朝鮮などからのサイバー脅威を防止するための「サイバーセキュリティ10万人材養成計画」では、2026年までに4万人の新規人材の養成を目標としていることを念頭に、韓国インターネット振興院（KISA）は、サイバーセキュリティ人材育成予算を20%増額し、大学・地方・軍などの以下セキュリティ教育を推進することを2023/12/4に公表した。 • 情報保護関連学部の支援を5大学から7大学（四年制大学）に拡大。最大6年間分のサイバーセキュリティ人材養成資金を提供。大学院も10校から12校に増設。 • 高度セキュリティ人材養成課程「K-Sheild」を通じたセキュリティ分野への就職希望者に200時間以上の集中教育。また、「K-Sheild Jr.」を通じて高校生・大学生にセキュリティ実務教育を提供。 • 地域情報保護センターを設置し、地方の中小企業と大学生へセキュリティ教育を実施。 • 「実戦型サイバー訓練場」を地域とオンラインに拡大し、インシデント対応能力を強化。 • この他、国防・軍事に特化したサイバーセキュリティ教育過程、次世代AIセキュリティ専門人材養成課程などを計画。 **【大規模サイバー攻撃に対する態勢強化】** • サイバーセキュリティ活動を効率的に実施するため、サイバー戦争専門家の育成と対応組織の育成を図る。	➢**情報セキュリティ大学院（GSIS）プログラム** • 政府が後援する韓国のSKY（ソウル大学、高麗大学、延世大学）と呼ばれるトップ大学を含む13の大学が共同で実施する、高度な情報セキュリティ専門家育成プログラム。 • 情報セキュリティの修士号と博士号、およびさまざまな奨学金と研究助成金を提供。 • GSISプログラムは、産業界や政府機関と協力して、学生に実践的なトレーニングやインターンシップの機会を提供。
	KITRI BoB（Best of Best） • 韓国情報技術研究院（KITRI）が「情報セキュリティ人材の育成を通じた国家安全保障上の困難の解決」のため、2012年から提供する韓国の次世代トップセキュリティリーダー育成プログラム。 2012年1期開始から2020年9期までに合計1,258人のセキュリティの専門家を輩出。 ※第4期BoBでグランプリ制度を開始し、文民連携コースに「情報保護専門兵士」コースが追加され、情報セキュリティに関する英語研修も開設し、研修プログラムの充実と質の向上を図っている。	➢ KITRI BoB（Best of Best）
サイバーセキュリティ業界の労働環境に関する受け止め	**※戦略上の言及はなし**	

2.2.5. 韓国③とりまとめ

- 韓国でみられる安全保障やサイバーセキュリティ産業振興における特徴や傾向。

大項目	小項目	特長・傾向
政策関係	サイバーセキュリティ対策の強化	✓「国家サイバーセキュリティ戦略」に基づき、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発展を強調。 ✓ 重要インフラを運営する機関に対して、国が予算上の支援を提供している。
	国際協調の推進	✓ サイバーセキュリティにおける国際協力を主導することを戦略文書で掲げており、二国間・多国間の協力体制の充実を図る。 ✓ サイバーセキュリティに特化したものではないが、直近の事例として韓・英間で締結されたデジタルサービス強化の覚書がある。
	研究力・技術力の強化、独立性確保	✓ 国家の安全保障の観点からのサイバーセキュリティ態勢の強化を強調している。 ✓ MSITやKISAなどの国の機関が主導し、予算上の支援も含めたサイバーセキュリティ産業支援を行う。
	国内事業者の確保・支援	✓ 戦略文書上、サイバーセキュリティ企業の成長環境を醸成することが強調されている。 ✓ KISAが設立した政府によるスタートアップ支援の目玉として「創造経済革新センター」の取り組みがある。
	セキュリティ人材育成	✓ 戦略文書においてサイバー攻撃の改善を強調し、「国家安保室」が中心となり、民・官・軍が連携する体制がとられている。 ✓ 政府の資金面での支援によって産業育成が図られている。
予算 等		✓ 2021年に策定されたK-cybersecurity Promotion Strategyにて、2023年までに情報セキュリティ分野に6700億ウォン（約630億円）を投資するとしている。

2.2.6 イスラエル

2.2.6. イスラエル① 戦略の全体像 - イスラエル国際サイバー戦略（Israel International Cyber Strategy）

- **「イスラエル国家サイバー防衛構想」**のコンセプトは3つの異なるレイヤーで構成され、それぞれ異なる機関が実行する。
- 国家サイバー防衛構想は、**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。戦略は、①グローバルなICTセキュリティのための協力、②能力構築・信頼醸成、③新興技術への備え、の3つの要素に基づく。

イスラエル国家サイバー防衛構想

第1層 市場のレジリエンス	民間セクターが独自にサイバー攻撃を防ぎ、耐える能力を確保することに重点を置く。国は重要なインフラストラクチャの規制、一般市民へのサイバーセキュリティ指導を提供、国家的な脆弱性アラートの配布、サイバー危機に備えるための施策の促進等を通じて、積極的に国家の「Attach surface（脆弱な攻撃対象）」を削減する。
第2層 サイバー攻撃への対応	サイバー攻撃への対応全般として、脅威の検出、分析、除去、機能回復、市場全体での類似攻撃からの免疫化を含む。 防衛運用サイクルが敵のそれを上回ることを目的とし、国家的な脅威が発生した場合には国家が介入する。
第3層 国家防衛	攻撃者に対する措置を講じること。国内法・国際法に従い、イスラエルの利益を損なうサイバー敵対者に対しては、外交、法執行、情報提供、経済、軍事、サイバーツールを用いて、必要に応じ国境を越え、敵対者を妨害、防御、抑止する。

この3つの層は、人、知識、機能・設備で構成される科学と産業の**サイバー・エコシステム**の上に成り立つ。これらは学術研究、産業革新、人的資本プログラムへの絶え間ない投資を必要とし、サイバー機関はその機会から、エコシステムはそこで培われた人材・経験・風評価値から得られる利益を得る。

イスラエル国際サイバー戦略（Israel International Cyber Strategy）

戦略の中核：グローバルなサイバーレジリエンスを構築する努力

グローバルなICTセキュリティのための協力	能力構築・信頼醸成	新興技術への備え
共通の課題を認識する	キャパシティ・ビルディング	共同研究開発ソリューション
集団的レジリエンスへの取り組み	自信構築（Confidence Building）	技術ポリシー
二国間共同行動	ICT貿易における信頼の醸成	国際基準
国際的なICTの安全性を確保するため、共通の課題を認識し、集団的レジリエンスの努力、二国間での共同行動を推進することを通じ、国際的な協力として、共有価値と相互利益に基づいたサイバー防衛の実現を目指す。	サイバーセキュリティの能力構築と信頼醸成を通じて、ICT取引への信頼を高めることを目的とする。情報共有プラットフォームの設立や専門の学術研究所の創設、地元のサイバー産業を活用した革新的なソリューションの提供など。	新興技術に対して、適用される国内外の法的枠組みに基づいた準備を進めることを意味する。AI、5G、IoTなどの新技術における安全性を確保するための研究開発、技術政策の形成、国際的な協力の強化が含まれる。

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（1/7）

- イスラエルは、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セキュリティリスクに対して、グローバルなサイバーレジリエンスと、共通の価値観と信頼に基づく国際協力の推進を目指す。

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
国家的なサイバーセキュリティのレジリエンスやリスクに係る言及	**【サイバーレジリエンスへの貢献】** • イスラエル国際サイバー戦略には、「イスラエルは世界のサイバーレジリエンスに貢献しており、それはイスラエル自身のサイバーセキュリティにとっても重要である」としたうえで、「共通の価値観と相互利益に基づくサーバーへの国際的関与は、他の国家目標の実現にも貢献する」とし、サイバー能力・技術を通じた海外とのパートナーシップ構築等の記述がある。 **【サイバーセキュリティリスクの認識】** • 攻撃用のサイバーツールがより洗練され、広く利用可能になっており、サイバー攻撃は増加傾向にある。国境のないサイバー空間では、国内での努力だけでは不十分であり、国際的な協力が必要だと指摘。 • 今後数年にわたって、悪意のあるアクターの洗練度が増し、攻撃用サイバー能力へのアクセスが拡大し、高価値の資産に対する攻撃を継続的に試みると予測。国際的なサイバー対話には、これらの脅威に関する共通の理解が必要。 • リスクの増大は防衛能力の構築をはるかに上回っており、サイバーセキュリティを喫緊の課題として国際社会がより早く、より多くのことを行う必要があるとする	➢ **公共団体におけるセキュリティの規制に関する法律** • イスラエル安全保障庁と国家サイバー総局（NCD）は、電気通信、インターネットプロバイダー、輸送事業者、公益事業者などの重要インフラを運営する組織に対して、サイバーセキュリティに関する拘束力のある指令を出す権限を与えてられている。 ➢ **データセキュリティ規則** • 個人データを含むデータベースを管理するすべての組織に適用され、データ対象者の数、データの機密性、アクセス資格を持つ人の数に基づいて4段階のデータセキュリティ義務を定めている。 ➢ **ISO 27001** • ISO 27001の認証を受けた組織は、ISO 27001の管理および要求事項に従っている場合、データ・セキュリティ規則のサブセットを遵守しなければならない。 ➢ **ISO 27799** • イスラエル保健省は、医療機関に対し、医療関連情報システムのデータ・セキュリティについてISO 27799の認証義務付け。
国の重要情報インフラにおけるサイバーセキュリティ・システムに関する要件	**【重要インフラに対するサイバー対応基準の設定】** • 国家サイバー防衛構想の第1層市場のレジリエンスにおいても、重要インフラに対する規制・対応基準について言及している。ただし、過去20年に渡り取り組まれているという記載も。 • 本戦略では、「重要インフラと必要不可欠なサービスの継続は、依然として国家の最優先事項である」と言及しつつ、「サイバー攻撃は、物理的な制御システムだけでなく、管理システムや中核的なデジタル資産も標的にすることで、継続性を混乱させる可能性があり、単一のチョークポイントやウイルス攻撃によって、大規模な影響を受ける可能性がある。このことは、重要インフラの一般的な定義を複雑にしている」と指摘。 **【国家輸出管理制度の更改後の要件】** • 2019年、イスラエルの内閣は外国投資審査に関する決定を採択し、外国企業に国家インフラプロジェクトを実施する許可を与える前に、イスラエルの規制当局に「防衛、外交関係、サイバー」への配慮を表明することを認めた。これは、法律で重要インフラ事業者に義務付けられているサイバーガイダンスに加えて行われる。これらの措置は、自由貿易の義務を損なうことなく、経済的利益を最大化しつつ、長期的なサイバーセキュリティリスクを軽減することを目的としている。	

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（2/7）

① サイバーセキュリティ対策の強化

項目	戦略上の記載	関連する規制/政策
サプライチェーンにおけるサイバーセキュリティ強化に関する施策	**【サプライチェーン強化に関する取り組み（集団的レジリエンスへの取り組みとして）】** • 民間セクターにおけるルーチンのサプライチェーン管理に共通のサイバーハイジーンチェック（cyber hygiene checks）を導入することで、集団的なサイバーセキュリティに波及効果をもたらすことを目指す。 • 企業内でのサプライチェーンのセキュリティ遵守を管理するため、サプライチェーンセキュリティコンプライアンスオフィサー向けの方法論、デジタルプラットフォーム、認証スキームを導入している。 • これらのスキームの国境を越えた相互運用性により、信頼構築に寄与する。	➢ **コンピュータ緊急対応チーム（CERT）** • 国家サイバーセキュリティ局が経済全体のサイバー空間を保護するため運営。 • 経済のレジリエンスを強化するための全国的な取り組みを管理・統制するため設立。 ➢ **データ・セキュリティ規制** • セキュリティ・レベルの高いデータベースに対して、少なくとも18カ月ごとにリスク評価と侵入テストを実施することを義務付け。 ➢ **クラウド・コンピューティング・ガイドライン** • 銀行監督当局は、クラウド・コンピューティング・サービスを利用する際のデータ・セキュリティを維持するためのガイドラインを定めており、これには機密情報をイスラエル国外のクラウドに保管する際の制限も含まれる。

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（3/7）

- イスラエルは、世界のサイバーレジリエンスに貢献しており、それはイスラエルのサイバーセキュリティにとっても重要であるとし、共通の価値観と相互利益に基づくサイバーへの国際的関与は、他の国家目標の実現の足がかりとなる。

② 国際協調の推進

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティに関する標準の実施状況	**【サイバーセキュリティにおける国際協力をリードする】** • イスラエルは国際的なハイテクハブであり、サイバーセキュリティの分野では、運用面でも技術面でも産業面でも世界をリードしている。 • イスラエルの成功の一部は、国のセキュリティ機関、民間の規制当局、学術研究機関、産業界、および広範なサイバーセキュリティ専門家からなる密接なサイバーエコシステムに起因している。 • イスラエルはこれまでのサイバー領域において、重要なインフラに対するサイバーレディネス基準を設定するなど、さまざまな分野で先駆者であったとされている。 **【新興技術に対する国際標準の形成を先導】** • 5Gセキュリティに関しては、イスラエルは通信ライセンスでの堅牢なサイバー標準と、通信業界とサイバー業界の両方からのセキュリティ・ソリューションにより、5Gのセキュリティ確保に取り組む。 • 国際的には、イスラエルは国際的な5Gセキュリティ原則を調整するためのプラハ・プロセスを支持。	➢ **イスラエル・サイバー防衛手法（ICDM）** • イスラエル国家サイバー総局（INCD）が指導、開発。 • ICDMは、NISTが開発したものを含め、国際的に認知されたサイバーセキュリティの標準とフレームワークを統合したもの。 • ICDMは、さまざまな分野や市場のニーズに対応できる柔軟なフレームワークを提供し、イスラエル市場の多くの組織で採用されている。 • 今後の計画としては、経済におけるICDMのアクセシビリティと同化の拡大、ICDMに基づく国家認証スキームの確立、この認証スキームを主要な国際標準と調和させるための取り組みなど
グローバルなサイバーセキュリティ・アライアンスにおける、自国のサイバーセキュリティプレーヤーの位置づけ	※戦略上の記載はない	

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（4/7）

- イスラエルの政府が支援する研究開発は、国内向けには既に複数の取り組みがある。戦略には、「キャパシティ・ビルディング」のに過去5年間の事例が紹介され、外交政策、国際開発プログラム、サイバー防衛の一環としての取り組まれている。

③ 研究力・技術力の強化、独立性確保

項目	戦略上の記載	関連する規制/政策

自国のサイバーセキュリティ産業の育成のために、政府が支援する研究開発の取り組み	**【国内産業のこれまでの育成と、今後の国際連携・外需創出】**
	• 最先端のサイバー課題に取り組むための7つの専門学術研究機関（500以上の論文）の設立、革新的なソリューションを提供するための地元サイバー産業の活用、執拗なサイバー攻撃に対するサイバー防御の実戦テストの成功など、「国際的なハイテクハブ」として成功し、運用面・技術面・産業面で世界をリードしているとする。
	• そのうえで、「サイバーという国境のない世界では、このような国内での取り組みだけでは不十分であり、国際的な強固な関与が必要である」と指摘し、戦略でも国内の研究開発の今後の方針については触れず、国際連帯に重きを置いたものになっている。国内の努力と国際的な連携を組み合わせることで、イスラエルのサイバーセキュリティ産業の成長とイノベーションを促進する。
	
	【キャパシティ・ビルディングの過去5年間の取り組み】
	• イスラエルのキャパシティ・ビルディング活動は、政治的に中立な立場で世界のレジリエンスを向上させることを目的としており、サイバーセキュリティのイノベーションを奨励する一方で、建設的かつ協力的なアプローチを採用している。イスラエルは、キャパシティ・ビルディングを外交政策、サイバー防衛のコンセプト、そして一般的な国際開発プログラムの一部として捉えている。
	  • ラテンアメリカ諸国のために米州開発銀行との能力開発基金の設立に協力し、参加。
	  • アフリカ諸国のために、世界銀行との能力開発基金の設立に協力し、参加。
	  • 世界銀行のデジタル開発パートナーシップ基金におけるサイバーセキュリティの追加的取り組みを支援。
	  • サイバーセキュリティ分野におけるより良い開発手法と実践を促進するための研究プロジェクトに投資。
	  • イスラエルの産業界と協力し、国規模の能力構築の課題に取り組む能力を備えたコンソーシアム設立。
	  • スタディーツアー、専門家ミッション、研修会、緊急技術支援、ギャップ分析など、数十件の二国間能力開発ミッションを実施し、その一部は本格的な国家能力開発プログラムに発展。
	  • GFCEやWEFなど、能力開発アジェンダを推進する国際組織に積極的に参加。
		➢イノベーション庁・経済産業省・国家サイバー局合同プログラム
		• 世界のサイバーセキュリティ分野におけるイスラエルの地位を強化することを目的とする。
		• 3年間で9000万NIS(＝2610万米ドル)の予算。
		• 世界に影響を与える可能性のある技術への投資、開発から試験・実証に移行する企業への資金援助などが含まれる。
		
		➢イノベーション・アリーナの創設
		• 健康、交通、金融等、サイバー脅威に脆弱な分野におけるイノベーション・アリーナの創設を推進。
		• 国際的なプレーヤー、規制当局、学者、イスラエルのサイバー産業を結集し、将来のサイバー課題に対する解決策を開発することを目的としている。
		
		➢ 大学・研究所との連携
		• ネゲブ・ベングリオン大学やエルサレム・ヘブライ大学などのイスラエルの大学や研究センターは、サイバーセキュリティの研究や教育に大きく関与。
		• 新技術の開発に貢献し、次世代のサイバーセキュリティの専門家を育成。

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（5/7）

- イスラエルは、サイバーセキュリティ産業がテクノロジー、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。

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業の保護、振興に関する位置づけ	**【サイバーが担う国家目標の推進】** • イスラエルのサイバーセキュリティ産業の保護と振興に関する位置づけは、国のテクノロジー、経済、国家安全保障、社会的な目標に直結している。具体的には以下のような内容が挙げられる。 　• **テクノロジー**：サイバーセキュリティは、新しい技術の開発において重要な考慮事項となっており、「セキュリティ・バイ・デザイン」の考え方と、安全な標準および安全な開発慣行を通じて推進されている。 　• **経済**：安全なサイバー空間は、経済におけるデジタルトラストを可能にし、サイバー攻撃による財務的な損害を減少させる。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。 　• **国家安全保障**：国際紛争においてもサイバー要素が増加しており、サイバーツールは運用上および情報収集上の利点を提供し、国家安全保障計画において考慮される必要がある。 　• **社会**：イスラエルのサイバー卓越性は、社会的なグルーピングを超え、包摂性を拡大し、中心地と周辺地をつなぐために活用されている。南部のベエルシェバを「サイバーの首都」として進展させる。 　• **国際協力**：イスラエルは国際的にもサイバーセキュリティの優れた能力を持っており、国際的な協力と共有価値に基づいたサイバーレジリエンスを推進している。 • これらの要素は、イスラエルがサイバーセキュリティ産業の保護と振興をどのように位置づけをしているかを示し、サイバーセキュリティ産業が各分野における成長と進展に貢献する重要な役割を果たしていることがわかる。	**➢国防輸出管理法** • イスラエル国防省の国防輸出管理局（DECA）は、サイバー輸出に対する管理を強化している。 • イスラエルのサイバー・システムの取得に関心を持つ国家に対し、輸出許可証発行の条件として「エンドユーザー宣言書」への署名を求めている。 • これによりサイバー・システムの最終的な用途が管理され、犯罪やテロの捜査・防止に限定される。 **➢外国投資審査メカニズム** • イスラエルは2019年10月、特に政府の許可が必要となる可能性のある規制産業やセクターへの特定の外国からのインバウンド投資について、一元化された投資審査メカニズムを設立。
国家安全保障／経済安全保障の観点から、サイバーセキュリティ産業を保護するためにとられている政策／措置	**【ICT貿易における信頼の醸成に向けた取り組み】** • **デジタル貿易障壁の削減**：デジタル商品とサービスの国境を越えた取引を可能にするための障壁を減少させ、グローバル経済発展を促進する。 • **リスク管理のための特別措置**：ソースコードレビュー、データのローカライゼーション要件、外国投資の監督など、リスクを管理するための特別措置を採用する。 • **国際標準の導入**：広く受け入れられている国際標準を立法に組み込んだ国家輸出管理システムを導入。 • **外国投資審査**：国家安全保障を含む複数の分野での外国投資に関する慎重な監視体制を構築。外国からの投資が国益に与える影響を評価することを目的とする。 • **技術サプライチェーンの国際信頼強化**：安全な開発慣行、技術標準における堅牢なセキュリティ規定、情報共有、協議、および適切な場合の特別な取り決めを通じて、技術サプライチェーンへの国際的な信頼を強化する。 • **技術市場の多様化**：技術市場の多様化を目指す政策を推進し、経済利益とリスク管理の両方に役立てる。	

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（6/7）

④ 国内事業者の確保・支援

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ産業を促進するための事業者を対象にした支援政策/施策	※戦略の記載上、国内のサイバーセキュリティ産業に特化した事業者への支援政策についての直接的な言及はない。しかし、イスラエルがサイバーセキュリティ能力の構築に多大な努力を注いでいること、また国内の研究機関や産業界との連携を通じて革新的なソリューションを提供していることは、間接的に国内事業者向けの支援があることを示唆している。	➢**長期的かつ画期的な研究開発への支援** • 世界市場に大きな影響を与える可能性のある技術の開発を支援。 • 高リスクの研究開発に取り組むイスラエルのサイバー技術企業は、あるプロジェクトの研究開発費の最大66%、年間最大500万NISを受け取ることができる。 ➢**パイロット・プログラムの支援** • 革新的なサイバー技術のトライアルを可能にし、その拡張性と実行可能性を主要顧客間で検証する。 • イスラエル国内外での単一または複数のパイロット・プログラムの予算が承認されたプログラムに対し、最大50%の資金を提供する。

2.2.6. イスラエル② サイバーセキュリティ産業政策調査結果（7/7）

- イスラエル国際サイバー戦略には、セキュリティ人材育成に関する具体的な方針等の記載は見当たらないものの、イスラエル国内においては既に複数のサイバーセキュリティの専門家を育成し、認定するための体系的なアプローチがある。

⑤ セキュリティ人材育成

項目	戦略上の記載	関連する規制/政策
サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修、教育プログラム等の開発支援	※本戦略上に、「サイバーセキュリティ専門家の認定制度や、政府拠る教育プログラム/研修、教育プログラム等の開発支援」に関わる今後の方針への言及は見当たらない。 ただし、序文の「サイバー国家の現状」の中に、「**120の児童向けサイバー教室**」と、リストの一つに記載されている。	➢**Cyber Security Course** • IAI-ELTAシステムズとの協力により、必要な知識とスキルを習得するための包括的なトレーニングを含む、主要なサイバーセキュリティと情報セキュリティのコースが提供。 • EC-Council認定トレーニングセンターと連携し、基準を満たした人材の就職を支援。 ➢**Curriculum and Certification** • 情報セキュリティ、ネットワーク管理、サイバーエッセンシャルなどの基礎科目を学ぶ。 • 重要な国際認定試験への準備や、シミュレーターを使用した実践的なトレーニングも含まれる。 • 修了者には、The External Studies InstituteとIsrael Aerospaceのサイバー部門から修了証書が授与。 ➢**国際サイバー職業センター（ICCP）** • イスラエル政府の財務省カレッジやイスラエル国防軍の通信・サイバー部門など、様々なパートナーとの協力のもと運営され、世界最先端の専門職資格につながるプログラムを提供。
サイバーセキュリティ業界の労働環境に関する受け止め	**【サイバーセキュリティ業界における労働力の需要が高まり】** • サイバーセキュリティ人材が需要ほどには成長しておらず、このことがサイバーセキュリティリスクの増加の一途をたどる一因でもあると指摘。	

2.2.6. イスラエル③とりまとめ

- イスラエル国際サイバーセキュリティ戦略（2021）の特徴・傾向。

大項目	小項目	特長・傾向
政策関係	サイバーセキュリティ対策の強化	✓ イスラエルは、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セキュリティリスクに対して、グローバルなサイバーレジリエンスと、共通の価値観と信頼に基づく国際協力の推進を目指す。
	国際協調の推進	✓ イスラエルは、世界のサイバーレジリエンスに貢献しており、それはイスラエルのサイバーセキュリティにとっても重要であるとし、共通の価値観と相互利益に基づくサイバーへの国際的関与は、他の国家目標の実現の足がかりとなる。
	研究力・技術力の強化、独立性確保	✓ イスラエルの政府が支援する研究開発は、国内向けには既に複数の取り組みがある。戦略には、「キャパシティ・ビルディング」のに過去5年間の事例が紹介され、外交政策、国際開発プログラム、サイバー防衛の一環としての取り組まれている。
	国内事業者の確保・支援	✓ イスラエルは、サイバーセキュリティ産業がテクノロジー、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。
	セキュリティ人材育成	✓ イスラエル国際サイバー戦略には、セキュリティ人材育成に関する具体的な方針等の記載は見当たらないものの、イスラエル国内においては既に複数のサイバーセキュリティの専門家を育成し、認定するための体系的なアプローチがある。
予算　等		✓ 非公開

2.3

我が国におけるサイバーセキュリティ産業振興関連政策の調査

2.3.1 経済産業省におけるこれまでの政策(WG3での施策を中心に)

- 経済産業省においては、これまでサイバーセキュリティ産業の活性化に資する様々な施策をWG3関連の施策を中心に実施してきている。

経済産業省におけるサイバーセキュリティ産業活性化関連主要施策	
① サイバーセキュリティ対策の強化	➢ **セキュリティ意識向上、対策への投資拡大** • 「サイバーセキュリティ経営ガイドライン」「グループ・ガバナンス・システムに関する実施指針」等の普及啓発活動、「クラウドサービス提供における情報セキュリティガイドライン」等の監査制度での普及促進活動を通じたサイバーセキュリティ経営の促進。 ➢ **中小企業、サプライチェーン別の対策強化** • **安価なサイバーセキュリティ対策をパッケージした「サイバーセキュリティお助け隊サービス」を創設し、中小企業の対策を支援。** • また、中小企業向け製品・サービスについての情報発信プラットフォームを構築。
② 国際協調の推進	➢ **国家間での相互承認の仕組みの構築** • IoTセキュリティ、暗号技術やセキュリティ製品の認証に関する国際標準化に積極的に関与。
③ 研究力・技術力の強化、独立性確保	➢ **サイバーセキュリティ技術の研究開発への投資や支援** • 経済産業省及びNEDO において、IoT・ビッグデータ・AI(人工知能)等の進化により実世界とサイバー空間が相互連関する社会(サイバーフィジカルシステム)の実現・高度化に向け、そうした社会を支えるハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を行う。
④ 国内事業者の確保・支援	➢ **スタートアップ支援** • 国産セキュリティ製品・サービスを開発するベンチャー企業に対し、ユーザー企業、システムインテグレーションベンダ・ディストリビュータにアピールする場を提供し、事業立上げを支援。 ➢ **ビジネス機会の創出** • 日本発のサイバーセキュリティ製品のマーケットインを目指し、ビジネスマッチングの場や**製品の検証基盤を提供。** • **情報セキュリティサービス審査登録制度の推進として、セキュリティサービスの品質向上と拡大を目指し、新たな機器検証サービスの区分追加や制度改善を行う。なお、本制度にはIoT機器の検証サービスも追加された。** • 地域に根差したビジネスマッチングや意見交換のためのプラットフォームを設け、地域SECUNITYの形成を推進。
⑤ セキュリティ人材育成	➢ **専門家教育** • 情報処理安全確保支援士制度の活用。 • 若年層のセキュリティ意識向上と優秀な人材の発掘・育成を目的に、セキュリティ・キャンプを開催。 ➢ **雇用状況・労働環境の改善** • 企業や団体への周知活動を通じて、人材のニーズとシーズのマッチングを促進。

2.3.2 WG3での主要施策①

- これまで産業サイバーセキュリティ研究会のもとのWG3にてサイバーセキュリティ産業の活性化に資する様々な施策が議論され、実施されてきている。

WG3の概要

概要

- 我が国の産業界がサイバーセキュリティに関して直面する課題に対応していくため、産業サイバーセキュリティ研究会のWGの一つとして、サイバーセキュリティビジネス化を検討するWG３を2018年に設置。
- サイバーセキュリティビジネスの創出支援として、① 産業サイバーセキュリティシステムを海外に展開、② サービス認定創設、政府調達などの活用を議論してきた。

WG3での主要施策（1／2）

	1 サイバーセキュリティお助け隊サービス	2 製品検証基盤（緑青検証）
目的	• 安価なサイバーセキュリティ対策をパッケージした「サイバーセキュリティお助け隊サービス」を創設し、中小企業の対策を支援。	• ベンチャー等の国内市場へのマーケット・インを促進するため、そのセキュリティ製品の有効性確認を行う基盤を構築。
概要	• 監視、インシデント対応、サイバー保険といった各種のサービスがパッケージとなり、一定の基準を満たすサイバーセキュリティサービスに「お助け隊マーク」の商標利用権を付与。ユーザー企業がIT導入補助金を本制度で活用した場合、サービス利用料が無料となる仕組みも構築。 • また、業種別業界団体が参加する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）は、本サービス事業を認定する上での基準を策定するとともに、各社に利用推奨を行う。	• 2019年度より、サイバーセキュリティ検証基盤を整備し、今後重要となる分野の製品を有識者が選定、該当する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)実施。 • 検証結果については、IPAが公表を行い、国内市場ベンダーとユーザーの間でのマッチングを図ることとする。 • なお、今後は、有効性が検証された製品の海外向けプロモーションも視野にいれる。
実績	• 従前より実施の実証事業を経て、事業者も中小企業向けのお助け隊サービスに該当するサービスを開発。基準を満たしたサービスは59件（2024年3月１日時点）。 • なお、本制度と連携しているIT導入補助金が含まれる中小企業生産性革命推進事業については、令和5年度補正予算で2000億円計上。	• これまで複数の国産製品の有効性が検証済（例として、Wifiセキュリティ、WAF（ウェブアプリケーションファイアウォール）、可視化・異常検知ツール） • 本検証結果を営業活動に活用し、大手企業２社を含む複数の商談獲得に貢献した事例あり。

2.3.2 WG3での主要施策②

- これまで産業サイバーセキュリティ研究会のもとのWG3にてサイバーセキュリティ産業の活性化に資する様々な施策が議論され、実施されてきている。

WG3の概要（再掲）

概要	• 我が国の産業界がサイバーセキュリティに関して直面する課題に対応していくため、産業サイバーセキュリティ研究会のWGの一つとして、サイバーセキュリティビジネス化を検討するWG３を2018年に設置。 • サイバーセキュリティビジネスの創出支援として、① 産業サイバーセキュリティシステムを海外に展開、② サービス認定創設、政府調達などの活用を議論してきた。

WG3での主要施策（2／2）

	3 情報セキュリティサービス審査登録制度	4 攻撃型を含めたハイレベルな検証サービスの取組（赤検証）
目的	• セキュリティサービスの品質向上と拡大を目指し、新たな機器検証サービスの区分追加や制度改善を行う。	• IoT機器等への検証事業の効果・信頼性を向上し、その信頼性を可視化することで、検証事業の活性化につなげる。
概要	• サイバーセキュリティサービスについて、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」を策定した上で、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。 • なお、基準については2022年に改訂し施行。 • また、IoT機器の検証サービスも対象に追加された（詳細は④攻撃型を含めたハイレベルな検証サービスの取組（赤検証）を参照）。	• 有識者検討会を設置し、我が国におけるIoT機器等に対する検証事業の効果・信頼性の向上方法や、検証事業者の信頼性を可視化する仕組みについて議論。 • これらの基準のもとに、情報セキュリティサービス審査登録制度に基づき、基準適合サービスリストの公開を通じて、機器メーカーが検証を実施する際に信頼性のある検証事業者を確認できる仕組みを構築 • なお、機器検証に関するモデル契約書の作成等も実施する予定。
実績	• IPAのウェブサイトには、情報セキュリティ監査、脆弱性診断、デジタルフォレンジック、セキュリティ監視・運用の４種類のサービスについて、基準を満たした300のサービスが掲載（ 2023年12月26日時点）。	• 2023年度に情報セキュリティサービス審査登録制度での機器検証サービスにかかる登録開始。情報セキュリティサービス審査登録制度における機器検証サービスは８件登録あり（2023年12月26日時点）。

2.3.3 日本政府全体におけるサイバーセキュリティに関する政策の全体像 - サイバーセキュリティ基本法

- 経済産業省の施策以外でも他省庁の取組を含め様々な施策が実施されてきている。全体像としては、サイバーセキュリティ政策の基本原則を定めた**サイバーセキュリティ基本法**と具体的な政策の目標や実施方法を定めた**「サイバーセキュリティ戦略」**が存在。
- **サイバーセキュリティ基本法**（平成27年施行）は、我が国のサイバーセキュリティ政策の基本原則を設定し、**サイバーセキュリティ戦略**の策定やサイバーセキュリティ戦略本部の設立などの政策の枠組みを規定した法律。第20条に産業振興に関する言及あり。

サイバーセキュリティ基本法 概要

基本理念（第3条）

1. 情報の自由な流通の確保を基本として、官民の連携により積極的に対応
2. 国民1人1人の認識を深め、自発的な対応の促進等、強靭な体制の構築
3. 高度情報通信ネットワークの整備及びIT活用による活力ある経済社会の構築
4. 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施
5. IT基本法の基本理念に配慮して実施
6. 国民の検知を不当に侵害しないように留意

基本的施策（第13～23条）

第13条　国の行政機関等におけるサイバーセキュリティの確保
第14条　重要インフラ事業者等におけるサイバーセキュリティ確保の促進
第15条　民間事業者及び教育機関等の自発的な取組の促進
第16条　多様な主体の連携等
第17条　サイバーセキュリティ協議会
第18条　犯罪の取り締まりおよび被害の拡大の防止
第19条　我が国の安全に重大な影響を及ぼす恐れのある事象への対応
第20条　産業の振興および国際競争力の強化
第21条　研究開発の推進等
第22条　人材の確保等
第23条　教育及び学習の進行、普及啓発等
第24条　国際協力の推進等

国は、**サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図る**ため、サイバーセキュリティに関し、**先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化**及び**新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化**及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。

3つの政策目的

- **経済社会の活力の向上及び持続的発展**
- **国民が安全で安心して暮らせる社会の実現**
- **国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること**

2.3.3 日本政府全体におけるサイバーセキュリティに関する政策の全体像 - サイバーセキュリティ戦略

- サイバーセキュリティ戦略は、国内外でのサイバーセキュリティ政策の基本的立場、目標、実施方法を定めたもの。

サイバーセキュリティ戦略（令和3年9月28日閣議決定/3回目の改定）

- **2020年代を迎えた日本を取り巻く時代認識**：デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する機体、安全保障環境の変化、新型コロナウイルスの影響・経験、オリンピック東京大会に向けた取組の活用

本戦略における基本的な理念

- 確保すべきサイバー空間は**「自由、公正かつ安全な空間」**
- 基本原則は従来の戦略で掲げた5つの原則を堅持（**情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携**）

目的達成のための施策・方針（サイバーセキュリティ基本法の3つの政策目的に準ずる）

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせるデジタル社会の実現	国際社会の平和・安定及び我が国の安全保障への関与
1. 経営層の意識改革 2. 地域・中小企業におけるDX with Cybersecurityの推進 3. 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり 4. 誰も取り残さないデジタル/セキュリティ・リテラシーの向上と定着	1. 国民・社会を守るためのサイバーセキュリティ環境の提供 2. デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 3. 経済社会基盤を支える各主体における取組（政府機関等・重要インフラ・大学教育研究機関等） 4. 多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用 5. 大規模サイバー攻撃事態等への対処体制の強化	1. 「自由、公正かつ安全なサイバー空間」の確保 2. 我が国の防御力・抑止力・状況把握能力の強化 3. 国際協力・連携

横断的施策

研究開発の推進	人材の確保・育成・活躍推進	全員参加による共同・普及啓発

2.3.3 サイバーセキュリティに関する政策の全体像 - サイバーセキュリティ戦略2023

- **サイバーセキュリティ戦略2023**は、サイバーセキュリティ戦略において、戦略に基づく施策を的確に実施するため、サイバーセキュリティ戦略本部で、各年度の施策の進捗状況を検証し、次年度の件核に反映することとしていることを踏まえて策定されている。

サイバーセキュリティ戦略2023

- サイバーセキュリティ戦略の構成に準じ、①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせるデジタル社会の実現、③国際社会の平和・安定及び我が国の安全保障への関与、④横断的施策の順で、担当府省庁、2022年度年次計画、取組の成果、進捗状況及び2023年度年次計画が記載(※別添2、左下画像参照)。

- 2023年の新規・継続施策のほか、2022年で終了となるものも含めた全344施策のうち、重複を除くと**281の施策が掲載**。
- 担当府省庁は**16機関**(経産・総務・文科・厚生・内閣・デジタル・警察・金融・個人情報保護・外務・法務・国交・消費者・内閣官房・防衛・人事院)。

【分析のポイント:サイバーセキュリティ市場の需給の拡大に影響する施策に注目】

- 民間企業等、経済活動の促進をターゲットにした施策であること。
  → **経済産業省・内閣官房(NISC)が担当する施策に絞る(140の施策)**
- 「サプライサイドの育成・強化」、または「デマンドサイドの拡大」のための施策を中心に考慮し、関連する規制/施策に記載。

2.3.4 サイバーセキュリティ産業ビジョンの作成に向けた日本政府全体における国内施策の状況整理

- 全体的な民間企業に向けての施策は、経営層の意識向上や普及啓発が主にあげられる。さらに、重要インフラ産業や中小企業等に対しては、サイバーセキュリティリスクに対する体制強化等の支援が行われている。

① サイバーセキュリティ対策の強化

戦略上の方針/方向性

- **経済社会の活力の向上及び持続的発展：DXとサイバーセキュリティの同時推進「セキュリティ・バイ・デザイン」**
  デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進
  ① 経営層の意識改革
  ② 地域・中小企業におけるDX with Cybersecurityの推進
  ③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり
  ④ 誰も取り残さないデジタル/セキュリティリテラシーの向上と定着
- **国民が安全で安心して暮らせるデジタル社会の実現 → 経済社会基盤を支える各主体における取組**
  ① 政府機関等：政府統一基準軍に基づく対策推進、監査、CSIRT訓練、GSOCの機能強化等、セキュリティ水準向上
  ② 重要インフラ：「重要インフラの情報セキュリティ対策に係る第4次行動計画」の改定を含む、諸制度整備
  ✓ 他の特徴として、東京大会での対処体制や運用により得た知見のノウハウを積極活用し、シームレスな体制を強化。

関連する規制/施策（主要な施策を抜粋）

➢ **セキュリティ意識向上、対策への投資拡大**
- 「サイバーセキュリティ経営ガイドライン」「グループ・ガバナンス・システムに関する実施指針」等の普及啓発活動、「クラウドサービス提供における情報セキュリティガイドライン」等の監査制度での普及促進活動を通じたサイバーセキュリティ経営の促進。

➢ **重要インフラのサイバーセキュリティ対策**
- 電力・ビルシステム・クレジットカード会社等の各業界別の研究会においてサイバーセキュリティリスクを考慮した議論・対策が進む。JPCERT/CC を通じて、インターネット上の公開情報を基に脆弱性等の情報を収集・分析の結果、国内の制御システム等への影響の懸念が高い場合、関連する制御システム関係者へ分析した情報の提供を行う他、経済産業省において、JPCERT/CC、金融ISAC 等の情報共有機関等を通じた情報共有網の維持・強化を進める。
- 2022年5月 **経済安全保障推進法** の成立により、①重要物資の安定的な供給の確保、②基幹インフラ役務の安定的な提供の確保、③先端的な重要技術の開発支援、④特許出願の非公開の4制度の創設が盛り込まれた。

➢ **中小企業、サプライチェーン別の対策強化**
- 情報セキュリティハンドブック、サイバーセキュリティ対策ガイドライン等、サイバーセキュリティ対策の普及啓発の推進。
- 安価なサイバーセキュリティ対策をパッケージした「サイバーセキュリティお助け隊サービス」を創設し、中小企業の対策を支援。
- サイバーレスキュー隊（J-CRAT）の運営、CSIRT/PSIRTの設立と連携強化、制御システムの事故原因の究明を行う機能の創設等、サイバーインシデント対応の体制強化。
- 中小企業における情報セキュリティ投資を促進するため、経済産業省や情報処理推進機構において、2020 年度に設立された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）を通じて、大企業等の発注元が中小企業に求めるセキュリティ対策の内容等について議論を進める。

➢ **政府インシデントや攻撃に対する迅速な対応体制や戦略**
- 情報収集・分析、調査・評価、注意喚起から対処、再発防止までの一連の取組を統合的に進めるナショナルサート（CSIRT/CERT）の枠組み強化。
- GSOCシステムの運用を通じた政府機関の情報システムに対するサイバー攻撃情報の24時間365日の収集・分析、監視業務の監督と能力向上。

2.3.4 サイバーセキュリティ産業ビジョンの作成に向けた日本政府全体における国内施策の状況整理

- IoTセキュリティ等の個別の技術やその活用に関する国際標準化活動を積極的に展開する方針を明示。同志国との連携強化、技術的に後れをとる国に対する能力構築支援等、国家間での対策も推進。

② 国際協調の推進

戦略上の方針/方向性

- **国際社会の平和・安定および我が国の安全保障への寄与 ： 安全保障の観点からの取組強化**
  - ① 自由・公正かつ安全なサイバー空間の確保
    - 国際法適用に関する議論・規範の実践の普及、サイバー犯罪に関する条約の普遍化等、サイバー空間における法の支配の推進
    - 信頼性のある自由なデータ流通（DFFT）や5Gセキュリティ等、国際的取組の進展を踏まえた国際ルールの策定
  - ② 我が国の防御力・抑止力・状況把握力の強化
    - 先端技術・防衛産業等のセキュリティ確保のための官民連携・情報共有等の強化、サイバー防衛能力の抜本的強化
    - 相手方によるサイバー空間の利用を妨げる能力の活用や外交的手段・刑事訴追等を含めた対応の活用、日米同盟の維持・強化
    - 全国的なネットワーク・技術部隊・人的情報を駆使したサイバー攻撃能力のさらなる実態解明の推進
  - ③ 国際協力・連携 ： 知見の共有・政策調整、国際サイバー演習・サイバー事案等に係る国際連携の強化、途上国への能力構築支援
    - 米豪印やASEAN等同志国との政策調整などの国際連携、国際サイバー演習の主導、能力構築支援等の取組強化

関連する規制/施策（主要な施策を抜粋）

➢ **国際的なサイバーセキュリティ基準や協定の策定・参加**
- 脆弱性対策に関連する国際標準化活動（例えばSCAPやCVSS）に参加し、情報システムの安全性確保に寄与。
- ISO/IEC JTC 1/SC 27やITU-T SG17などの国際会合に参加し、IoTセキュリティに関する国際標準化を推進。
- ISO/IEC JTC 1/SC 27が主催する国際会合に参加し、暗号技術やセキュリティ製品の認証に関する国際標準化に積極的に関与。
- 内閣官房・外務省が、各種二国間・多国間協議に参加し、サイバー空間における国際法の適用や国際的なルール作りに積極的に関与。
- IoTセキュリティに関連する国際標準化動向（ISO/IEC JTC1/SC41など）を注視し、必要に応じた支援を行う。

➢ **国家間での相互承認の仕組みの構築**
- 新型コロナウイルス感染症の影響でオンライン空間の利用が増加する中、ARFや二国間協議を通じて、サイバー攻撃の脅威認識やセキュリティ戦略の共有、国際連絡体制の構築に取り組む。
- JPCERT/CCを通じて国際的なCSIRT間の連携を強化し、インシデント対応調整や脅威情報の共有を行う。これにはFIRST、APCERT、IWWNなどの国際コミュニティへの参加も含まれる。
- 米国NISTなどの各国のサイバーセキュリティ機関と連携し、情報セキュリティに関する最新情報の交換に取り組む。
- IWWNやFIRST、日ASEANサイバーセキュリティ政策会議など、サイバーセキュリティに関する多国間の情報共有枠組みに参加し、情報収集と発信を強化。

➢ **その他**
- 情報処理推進機構を通じて、アジア地域での情報セキュリティ人材の育成に取り組んでおり、ITPEC加盟国の責任者との会合や共通試験に関する取り組みを共有。

2.3.4 サイバーセキュリティ産業ビジョンの作成に向けた日本政府全体における国内施策の状況整理

- 実践的な研究開発推進を進めるとの方針の下、経済安全保障上の重要技術に関する研究開援投資や国産技術の確保・育成支援に取り組んでいる、また、戦略では中長期的なトレンドを視野に入れた研究開発の推進にも言及されている。

③ 研究力・技術力の強化、独立性確保

戦略上の方針/方向性

- **研究開発の推進（横断的施策）**
  - ✓ 産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進。中長期的な技術トレンドも視野に対応。
  - ① 国際競争力の強化、産学官エコシステムの構築
    - 研究・産学官連携振興施策の活用、研究環境の充実 等
  - ② 実践的な研究開発の推進
    - サプライチェーンリスクへの対応、国内産業の育成・発展、攻撃把握・分析・共有基盤、暗号等の研究の推進
  - ③ 中長期的な技術トレンドを視野に入れた対応
    - AI技術の進展（AI for Security Security for AI）、量子技術の進展、耐量子計算機暗号の検討、量子通信・暗号

関連する規制/施策（主要な施策を抜粋）

➢ **サイバーセキュリティ技術の研究開発への投資や支援**
- **「経済安全保障重要技術育成プログラム」**等による技術的課題への取り組みとして、「ハイブリッドクラウド利用基盤技術の開発」、「人工知能（AI）が浸透するデータ駆動型の経済社会に必要なAI セキュリティ技術の確立」、「サプライチェーン・セキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」等があげられる。
- 経済産業省及びNEDO において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を行う。
- 第3期戦略的イノベーション創造プログラム（SIP）でも、サイバーセキュリティ関連プログラムあり。
- 国産製品のマーケットイン促進のため、IPAと製品の質を検証する基盤を構築。

➢ **自国での技術開発・研究の促進や外国からの依存度の低減**
- 内閣官房において、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携によるサプライチェーン・リスクに対応するための技術検証体制を整え、検証の技術動向や諸外国の検証体制・制度も踏まえ、不正機能や当該機能につながりうる未知の脆弱性が存在しないかどうかの技術的検証を進めている。

2.3.4 サイバーセキュリティ産業ビジョンの作成に向けた日本政府全体における国内施策の状況整理

- サプライチェーンの信頼性確保の基盤として位置づけで、日本発のセキュリティ製品の検証サービスを実施するほか、新技術実装に伴う安全確保のためのサイバーセキュリティ技術開発やガイドライン策定等に取り組む。

④ 国内事業者の確保・支援

戦略上の方針/方向性

- **経済社会の活力の向上及び持続的発展 ：DXとサイバーセキュリティの同時推進「セキュリティ・バイ・デザイン」**
  ③ 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり
  - サプライチェーンの信頼性確保 ： 産業界主導のコンソーシアム
  - セキュリティ製品・サービスの信頼性確保 ： 第三者検証サービスの普及
  - 先端技術・イノベーションの社会実装 ： 情報収集・蓄積・分析・提供等の共通基盤構築
- **国民が安全で安心して暮らせるデジタル社会の実現 → 国民・社会を守るためのサイバーセキュリティ環境の提供**
  ① 安全・安心なサイバー空間の利用環境の構築
  - サプライチェーン管理のためのガイドライン策定や産業界主導の取組、IoT、5G等の新技術実装に伴う安全確保
  - 利用者保護の観点から安全かつ信頼性の高い通信ネットワークを確保するための方策の検討

関連する規制/施策（主要な施策を抜粋）

➢ **スタートアップ支援**
- 国産セキュリティ製品・サービスを開発するベンチャー企業に対し、ユーザ企業、SI ベンダ・ディストリビュータにアピールする場を提供し、事業立上げを支援。
- マーケットインに向けたセキュリティ市場調査を実施し、国内セキュリティベンダ・ユーザ企業の動向を把握の上、国産セキュリティ製品・サービスの更なる事業機会の拡大を目的とした国産セキュリティ製品・サービス表彰制度を企画。

➢ **ビジネス機会の創出**
- 検証サービスの普及拡大 ：日本発のサイバーセキュリティ製品のマーケットインを目指し、ビジネスマッチングの場を提供。
- 情報セキュリティサービス審査登録制度の推進 ：セキュリティサービスの品質向上と拡大を目指し、新たな機器検証サービスの区分追加や制度改善を行う。
- コラボレーション・プラットフォームの開催 ：地域に根差したビジネスマッチングや意見交換のためのプラットフォームを設け、地域SECUNITYの形成を推進。

➢ **その他**
- 特定高度情報通信技術活用システム（5G・ドローンなど）の開発、供給、導入をサイバーセキュリティを確保しつつ、普及促進。
- 政府機関での無人航空機の調達においてサイバーセキュリティを確保するための方針を策定、関連するガイドラインを周知。安全な無人航空機の技術開発と普及を進める。
- 自動運転システムに関する新たなサイバー攻撃手法の動向や対策技術の調査結果を「IDS評価ガイドライン」に反映し、継続的な更新と業界団体への移管を目指す。
- IoT機器やサイバーフィジカルシステムへの脅威に対応するため、先進的なハードウェアセキュリティ技術やソフトウェア工学、暗号技術などの研究に取り組む。
- AI技術や量子技術などの中長期的な技術トレンドへの対応を検討し、関連する戦略やビジョンに基づいて適切な対応を進める。

2.3.4 サイバーセキュリティ産業ビジョンの作成に向けた日本政府全体における国内施策の状況整理

- サイバーセキュリティの専門家、全体の底上げ両面において育成の取組が進展。人材の質・量の確保に向け、専門家教育や新規の働き手確保の関連施策を多数講じている。なお、女性や外国人など特定の人材に的を絞った施策は記載がなかった。

⑤ セキュリティ人材育成

戦略上の方針/方向性

- **人材の確保、育成、活躍促進（横断的施策）**
  - ✓「質」・「量」両面での官民の取組を一層継続・深化させつつ、環境変化に対応した取組の重点化。
  - ✓ 官民を行き来しキャリアを積める環境整備も。
  - ① DX with Cybersecurityの推進
    - 「プラス・セキュリティ」知識を補充できる環境整備、機能構築・人材流動に関するプラクティス普及等（xSIRT、副業・兼業等）
  - ② 巧妙化・複雑化する脅威への対処
    - 人材育成プログラムの強化　SecHack365 / CYDER / enPiT / ICSCoE中核人材育成プログラム　等
    - 人材育成共通基盤の構築・産学への開放、資格制度活用に向けた取組　等
  - ③ 政府機関における取組
    - 外部高度人材活用の仕組み強化、「デジタル区分」合格者の積極採用、研修の充実・強化　等

関連する規制/施策（主要な施策を抜粋）

- **専門家教育**
  - 情報処理安全確保支援士制度の活用促進 ： 講習制度の充実と普及を図り、制度の登録更新や特定講習の導入、周知継続。
  - 情報セキュリティマネジメント試験の普及 ： 組織のセキュリティポリシー運用に必要な知識を問う国家試験を実施、普及を図る。
  - セキュリティ・キャンプの開催 ： 若年層のセキュリティ意識向上と優秀な人材の発掘・育成を目的に、各種キャンプを開催。
  - 未踏IT人材発掘・育成事業 ： 独創的なアイディアや技術を有する人材を発掘・育成。セキュリティ専門家をプロジェクトマネージャーとして採用。
  - CTF（Capture The Flag）ハッキングコンテストの支援 ： 攻撃・防御の視点を含むセキュリティ能力を試す競技会を後援。
- **雇用状況・労働環境の改善**
  - サイバーセキュリティ体制構築・人材確保の手引き：企業や団体への周知活動を通じて、人材のニーズとシーズのマッチングを促進。
  - 基本的なサイバーセキュリティ対策の周知活動：国民に対するサイバーセキュリティ対策の普及啓発活動の実施。
- **新規の働き手の確保策（リスキリング等）**
  - サイバーセキュリティ対策の周知活動 ：SNSやポータルサイトを利用したサイバーセキュリティ関連情報の発信と啓発活動。
  - サプライチェーン・サイバーセキュリティ強化 ：SC3と連携し、デジタル人材育成プラットフォームを通じたスキル標準の策定や人材育成プログラムの発信。
  - サイバーセキュリティ関連法令Q&Aハンドブック ：法令や情勢の変化、技術進展に伴う法的課題に関するハンドブックの改訂。
  - デジタル人材確保・育成計画 ：各府省庁におけるデジタル人材の育成と確保のための計画の策定と見直し。
- **その他**
  - GIGAスクール構想 ：文部科学省と協力して学校のICT化を進め、サイバーセキュリティに関する啓発を推進。
  - ・情報モラル/セキュリティ意識向上 ：IPA主催の標語・ポスター・4コマ漫画等の募集を通じて、児童・生徒に情報モラル/セキュリティの重要性を教育。インターネット安全教室でインターネットの安全利用に関する教育を行い、啓発教材やコンテンツを提供等も。

2.3.4 （補足）CYNEXにおける施策の状況整理

- 情報通信研究機構（NICT）において、国産サイバーセキュリティ製品の開発を促進するため、国内でのサイバーセキュリティ情報を生成・蓄積・提供できる環境と、人材育の共通基盤を構築するため、産学官の各組織が参画する、2021年4月にサイバーセキュリティネクサス（CYNEX）が組織され、研究力・技術力の強化や人材育成等の様々な施策を推進中。

（参照）CYNEXに参画する主な組織

- 産業界：セコム、NTTコミュニケーションズ、日立製作所、富士通、横河電機　等
- 官公庁等：警察庁、内閣サイバーセキュリティセンター（NISC）、情報処理推進機構（IPA）、防衛装備庁　等
- 学術界：岡山大学、金沢大学、東北大学、横浜国立大学、立命館大学　等

CYNEXにおける主な施策

研究力・技術力の強化、独立性確保

主要な施策

➢ **サイバーセキュリティ技術の研究開発への支援**
- 様々な攻撃事象の国内での解析を可能とするため、NICT開発の標的型攻撃の攻撃者を誘い込むサイバー攻撃誘引基盤（STARDUST）を参画組織に提供。
- 悪性Webサイトの情報収集を行うプロジェクト（WarpDrive）を参画組織とともに運営。
- NICTが運営するサイバー攻撃観測・分析システム（NICTER）により、攻撃情報を蓄積。
- 機械学習エンジンも活用したサイバー攻撃情報の解析及び、解析結果の参画組織での共有。

国内事業者の確保・支援

主要な施策

➢ **国産製品の検証・普及支援**
- 国産セキュリティ製品のプロトタイプをNICTに導入し、長期運用を通して機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援。

セキュリティ人材育成

主要な施策

➢ **一般企業における高度人材の育成**
- 一般企業のサイバー強化のため、高度SOC（Security Operations Center）人材育成プログラムを構築し、SOC人材の育成拠点を形成。
- 演習シナリオや遠隔演習システムをオープン化し、民間事業者や教育機関におけるセキュリティ人材育成事業を促進。

2.3.4 （補足）経済安全保障推進法における先端重要技術開発（官民技術協力）におけるサイバーセキュリティ

- 経済安全保障推進法の主要4施策の一角を担う「先端重要技術開発（官民技術協力）」は、国家戦略上の重要な先端技術を指定し、技術開発の支援などを実施することで自国産業を強化することを目的として、「海洋」「宇宙・航空」「サイバー空間」「バイオ」の4領域（＋領域横断）から、合計50の技術を特定重要技術に指定。以下の表は、「サイバー空間」に係る特定技術をピックアップ。

先端重要技術開発（官民技術協力）とは

- 「先端重要技術開発（官民技術協力）」（以下、本施策）とは、将来の国民生活や経済活動の維持に重要な先端的技術のうち、外部に不当利用された場合に国家や国民の安全を損なうおそれがあるものを「特定重要技術」と定義したうえで、官民連携を通じた伴走支援のための協議会の設置や調査研究業務の委託などを通じて、特定重要技術の研究開発の促進とその成果の適切な活用を図る施策。

研究開発ビジョン	課題解決の方向性 （「サイバー空間」カテゴリ）	特定重要技術 （「サイバー空間」カテゴリ）
第一次選定 2022年9月	AIセキュリティに係る知識・技術体系	AIセキュリティに係る知識・技術体系
	サイバ分野における不正機能検出技術	不正機能検証技術（ファームウェア/ソフトウェア/ハードウェア）
	ハイブリッドクラウド利用基盤技術	ハイブリッドクラウド利用基盤技術
第二次 2023年8月	先進的サイバー防御機能・分析能力の強化	サイバー空間の状況把握・防御技術
		セキュアなデータ流通を支える暗号関連技術
	偽情報分析に係る技術	偽情報分析に係る技術
	ノウハウの効果的な伝承につながる人作業伝達などの研究デジタル基盤技術	ノウハウの効果的な伝承につながる人作業伝達などの研究デジタル基盤技術

【参照】 内閣官房 「経済安全後生重要技術育成プログラム 研究開発ビジョン（第一次）」
内閣官房 「経済安全後生重要技術育成プログラム 研究開発ビジョン（第二次）」
※ 上記表は、合計50件の特定技術の内、「サイバー空間」カテゴリの重要特定技術をピックアップ

2.3.5 サイバーセキュリティ戦略2023(まとめ)

- 「サイバーセキュリティ戦略2023」における、経済産業省のみならず他省庁等(他省庁所管独立行政法人含む)実施のサイバーセキュリティ産業活性化関連の施策の概要としては、下記のとおりであり、これらの施策は、市場開拓(需要側の対策を強化し、需要を喚起するもの)、産業競争力強化(直接的にベンダーを支援するもの)、人材育成の三つの大きな要素が確認できる。

「サイバーセキュリティ戦略2023」中(第3部)の産業活性化関連の主要施策

章		主要な施策	分類
第1章 経済社会の活力の向上 及び持続的発展		**【サイバーセキュリティ対策の強化】** • 経営者がセキュリティ対策上果たすべき役割等を示す「サイバーセキュリティ経営ガイドライン」策定済。 **【国内事業者の確保・支援】** • 提供するサービスが基準以上である事業者を示す「情報セキュリティサービス審査登録制度」創設済。IPAと連携し、スタートアップとSIerやユーザー企業とのマッチング環境整備(イベント等)について実施。	**市場開拓及び産業競争力強化**
第2章 国民が安全で安心して暮らせるデジタル社会の実現		**【サイバーセキュリティ対策の強化】** • サイバーレスキュー隊(J-CRAT)の運営、CSIRT/PSIRTの設立と連携強化、制御システムの事故原因の究明を行う機能の創設等、サイバーインシデント対応の体制強化。	**市場開拓**
第3章 国際社会の平和・安定及び我が国の安全保障への寄与		**【国際協調の推進】** • IoTセキュリティ、暗号技術やセキュリティ製品の認証に関する国際標準化に積極的に関与。	**産業競争力強化**
第4章 横断的施策	研究開発の推進	**【研究力・技術力の強化、独立性確保】** • ベンダーの研究開発を支援する経済安全保障重要技術育成プログラムや第3期戦略的イノベーション創造プログラム(SIP)により研究開発支援等 • 国産製品のマーケットイン促進のため、IPAと製品の質を検証する基盤を構築。	**産業競争力強化**
	人材の確保・育成、活躍促進	**【セキュリティ人材育成】** • 次世代を担う高度なサイバーセキュリティ人材を発掘・育成するセキュリティキャンプを実施。 • 情報処理安全確保支援士(登録セキスペ)の制度創設。また、当該制度のユーザー企業向けプロモーションも実施。 • 高度な人材を育成する、大学での社会人向けサイバーセキュリティ人材育成プログラムやセキュリティイノベーター育成プログラム	**人材育成**
	全員参加による協働、普及啓発	**【サイバーセキュリティ対策の強化】** • 中小企業、NPO向けのサイバーセキュリティ対策について記載したハンドブックを策定・改正を実施。	**市場開拓**

※他省庁等の施策については青字。

2.3.6 (補足)これまでの経済産業省の施策と他省庁等の施策(総括)

- 市場開拓、サイバーセキュリティ産業の競争力強化、サイバーセキュリティ人材育成といったサイバーセキュリティ産業の活性化に資する3つの要素の観点から、これまで経済産業省サイバーセキュリティ課のみならず、経済産業省の他課や他省庁等(他省庁所管独立行政法人含む)実施のサイバーセキュリティ施策や潜在的に連携可能なデジタル分野の施策を整理すると下記のとおり。

これまでのサイバーセキュリティ産業活性化にかかる施策や連携可能な施策

	経済産業省サイバーセキュリティ施策	他省庁等のサイバーセキュリティ施策	その他連携可能な施策
市場開拓	• 経営者がセキュリティ対策の上で果たすべき役割等を示した「サイバーセキュリティ経営ガイドライン」は策定済。 • IPAと連携し、スタートアップとSIerやユーザー企業とのマッチング環境整備（イベント等）について実施。	• 中小企業、NPO向けのサイバーセキュリティ対策について記載したハンドブックを策定・改正を実施。【内閣官房】	• 需要喚起を後押しする可能性のある既存税制【経済産業省】や中小企業向けIT導入補助金（「セキュリティ対策推進枠」あり）【中小企業庁】
産業競争力強化	• 国産製品のマーケットイン促進のため、IPAと製品の質を検証する基盤を構築。 • 提供するサービスが基準以上である事業者を示す「情報セキュリティサービス審査登録制度」は創設済。（SIerは未着手）。	• ベンダーの研究開発を支援する経済安全保障重要技術育成プログラムや第3期戦略的イノベーション創造プログラム（SIP）により研究開発支援等を実施。【内閣府】	• 政府が企業を比較・検討を行えるHPを構築。【デジタル庁】 • 防衛産業のスタートアップ活用に向けた合同推進会を実施。【防衛装備庁・経済産業省】
人材育成	• 次世代を担う高度なサイバーセキュリティ人材を発掘・育成するセキュリティキャンプを実施。 • 情報処理安全確保支援士（登録セキスペ）の制度創設。また、当該制度のユーザー企業向けプロモーションも実施。	• 高度な人材を育成する、大学での社会人向けサイバーセキュリティ人材育成プログラム【文部科学省】やセキュリティイノベーター育成プログラムの活用。【NICT】	• 登録セキュスペの活用を後押しする可能性のある既存税制の活用。【経済産業省】

2.3.7 デスクトップ調査を踏まえた日本のサイバーセキュリティ施策の課題

- デスクトップ調査を踏まえた日本のサイバーセキュリティ施策の想定される課題を整理。

	国内施策の傾向	国内施策において今後の課題と考えられる事項
サイバーセキュリティ対策の強化	• 経営層のサイバーセキュリティへの意識向上の一環で、各種ガイドラインの整備をはじめ普及啓発活動を実施。 • 中小企業に向けては、ガイドライン等の普及啓発活動の他、事故対策、原因究明など、実務的な対策機能を強化。 • 経済安全保障推進法の実施に伴い、基幹インフラのサイバーセキュリティ強靭化の対策実施。 • サイバーセキュリティインシデントへの対応を充実化。	✓我が国では、ユーザー企業向けのサイバーセキュリティ対策強化を推進し、重要インフラや中小企業に焦点が当てられた取り組みや支援が目立つが、「経営層の意識向上」以外に、**重要インフラでも中小企業でもない組織に対するアプローチ（財政的支援やお助け隊の支援等）**が不足しているのではないか。 ✓大手企業を中心に、**サイバーセキュリティが企業への投資要素として考慮されるような環境を、政府として十分構築できていない**のではないか。
国際協調の推進	• IoTセキュリティ等の個別の技術やその活用に関する国際標準化活動を積極的に展開。 • アジア地域での情報セキュリティ人材の育成等の能力構築支援に取り組むなど、所管機関を通じてサイバーセキュリティ実務者の国際交流や貢献活動を展開。	✓国際標準に準拠した製品開発を行ったことで、市場を獲得した日本のスタートアップ企業が存在するといった状況を踏まえ、日本が強みをもつ標準分野を起点にして、サイバーセキュリティに関わる標準におけるプレゼンスを高めることも考えられるのではないか。 ✓日本による外国のサイバーセキュリティ能力開発支援が現状具体的なビジネスにつながっているとはいえず、我が国のサイバーセキュリティ産業の輸出可能性にまでつなげられるような施策が打てていないのではないか。

2.3.7 デスクトップ調査を踏まえた日本のサイバーセキュリティ施策の課題

- デスクトップ調査を踏まえた日本のサイバーセキュリティ施策の想定される課題を整理。

	国内施策の傾向	国内施策において今後の課題と考えられる事項
研究力・技術力の強化、独立性確保	• 実践的な研究開発推進を進めるとの方針の下、経済安全保障上の重要技術に関する研究開援投資や国産技術の確保・育成支援に取り組んでいる。 • また、国産製品の性能検証基盤も構築。	✓イスラエルのように、将来的に**市場で競争優位性を発揮できるような有望な企業に対する開発から試験・実証への一貫した集中的な支援**を強化していく必要があるのではないか。 ✓将来日本が優位性を持てるような分野（例：広域5G通信）におけるサイバーセキュリティの研究開発により注力していくべきではないか。
国内事業者の確保・支援	• サイバーセキュリティサービスの検証枠組みを設置し、登録した事業者にとってビジネスが促進されるよう支援。 • スタートアップ支援として、ビジネスマッチングの場の提供、製品・サービスの表彰制度など、認知度の向上に向けた取組が行われる。 • トレンドと見られる最新の技術のサイバーセキュリティの実装を前提とした、普及啓発活動を推進。	✓英国のように、明確にサイバーセキュリティ産業を輸出産業と位置付ける国とは異なり、サイバーセキュリティ戦略に産業の活性化についての明確な言及はなく、**産業活性化等を「攻め」の要素**と位置付けることが必要ではないか。 ✓諸外国と比較し、立ち上げ期から、研究開発、販路の確保に至るまでの一貫した**スタートアップ支援策**が十分とはいえないのではないか。
セキュリティ人材育成	• サイバーセキュリティの専門家、全体の底上げ両面において育成の取組が進展。人材の質・量の確保に向け、専門家教育や新規の働き手確保の関連施策を講じている。	✓韓国の「サイバーセキュリティ人材10万人養成計画」のように、**大規模に高度なサイバーセキュリティ人材を養成するという施策**が十分ではないのではないか。 ✓諸外国では、女性をターゲットにした教育プログラムが組まれており、女性等の多様な人材の活躍を目指した施策が十分ではないのではないか。

2.4

ヒアリング調査結果

2.4.1 ソリューションに係る有識者インタビューでのコメントと検討事項

- 我が国のサイバーセキュリティ産業政策に対して、各分野の有識者・専門家、特にサイバーセキュリティ産業政策に関係すると思われる業界関係者など、経済産業省サイバーセキュリティ課と相談の上、PwCのネットワークを活用してヒアリングを行った。

氏名	組織・役職	専門分野、特徴	実施した日付
梶浦 敏範	日本サイバーセキュリティ・イノベーション委員会　代表理事 日立製作所 上席研究員	経済産業省サイバーセキュリティ研究会WG2座長、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)運営委員会議長、JCIC上席研究員を兼務。	2024年1月11日
柴田 健久	OpenID Foundation Japan 理事	情報処理学会の情報規格調査会 SC 27国内委員会の委員。米国OpenID FoudationのCorporate board menber。	2024年1月12日
匿名	日本IT団体連盟 委員　サイバーインデックス担当者	官公庁や民間企業に対するサイバーセキュリティ戦略立案、サイバー演習、サイバーセキュリティインシデント対応支援、M&A戦略策定に従事。	2024年1月15日
匿名	元 日系大手ソフトウェア企業 欧州事業担当	日系ソフトウェア企業の欧州事業の立上げ・運営などグローバルのテクノロジーに関わる経験を持つ。	2024年1月18日
岡田 満雄	Capy Inc. Founder and CEO	2012年にCapy Inc.をデラウエア州に設立。2017年に日本国内の事業拡大に伴いCapy株式会社を設立。	2024年1月24日
崎村 夏彦	Chairman, OpenID Foundation	日本情報経済社会推進協会データ流通促進WG委員など多数。	2024年2月7日
伊藤 公祐	IoTセキュリティ普及啓発団体(CCDS)事務局長、WG主査、JPNIC理事	約15年に渡り、様々なIoTセキュリティガイドライン策定や普及活動に従事し欧米のIoTセキュリティ規制や国際標準要件に精通。	2024年2月8日
林彦博	元 Panasonic PSIRT(創設者兼代表)	セキュリティ診断・リスクアセスメント・ガイドライン策定・グローバルガバナンス・製品を中心したサイバーセキュリティ・インシデント対応などを推進。	2024年2月8日
足立照嘉	APRIO Technologies(英)CEO	ロンドンを拠点に活動するサイバーセキュリティ専門家。国内外の通信会社やIT企業などのサイバーセキュリティ事業者に技術供給およびコンサルティングを提供。	2024年2月22日

2.4.1 ソリューションに係る有識者インタビューでのコメントと検討事項

- これまでのインタビューを踏まえて、需要側、供給側、人材基盤の各観点のソリューションに対する言及と実施検討事項をまとめる。

大分類	ヒアリングの観点
需要側	企業へのインセンティブ付け（投資促進税制・補助金等）についての意見
	企業セキュリティの内需促進についての意見 • セキュリティ意識の向上 • 強みに特化した需要促進 • 中小企業の需要創出
	重要インフラに対する監査基準改定および監査の実施・対応強化
供給側	スタートアップ施策と統合的な取り組み
	今後需要が見込まれる次世代技術分野（AI・自動運転など）での取組
	製造業等、OT周辺セキュリティ
	海外向け輸出促進施策の関連の取組
人材基盤	サイバーセキュリティ関連人材に関する意見

※ 「実施検討事項」については、有識者から言及のあった点を踏まえて想定される施策を記載したものであり、既存施策との比較検討や精査が必要。

2.4.2 ソリューションに係る有識者インタビューでのコメントと検討事項（需要側）

		ヒアリング結果	実施検討事項
企業へのインセンティブ付け（投資促進税制・補助金等）についての意見		• 日本の中小企業の多くが税金を納めていない状況にあるため、従来の法人減税などのインセンティブは限定的な効果しか持たない可能性がある。 • 中小企業に対しては、DX with Securityの考え方をもとに、パッケージシステム等を中心とした導入コストの低い共有型を浸透させるための補助金事業を進め、中小企業を束ねて効率よくアップデートすべき。 • 標準を取得する上でもコストがかかるため、そのための人件費、事務的経費、また人材育成など、標準を取りに行くための補助金を出すなどのサポートがあると良い。 • サイバーセキュリティの重要性を理解していても、コストと感じる経営者は多く、実装にも金銭的負担が大きい。	• 中小企業向けにセキュリティサービスの導入を支援する補助金を設ける。 • 事業者のセキュリティ関連の標準取得にかかるコストを補助。 • サイバーセキュリティ専門家の育成を目的とした教育プログラムへの参加支援や、企業内でのセキュリティ研修の実施に対する補助。 • サイバーセキュリティ対策を講じたり、認証を受けた事業者（特に重要インフラ事業者とその直接サプライヤー）に対する税制上の優遇措置や補助金提供。
企業セキュリティの内需促進についての意見	セキュリティ意識の向上	• 多くの企業では、自社がサイバー攻撃の対象になることを当初は認識していないが、事業継続のリスクや顧客への影響を指摘されると、サイバーセキュリティの必要性を認識し始める。 • サイバーセキュリティの重要性を経営者に伝えるには、**誰が伝えるかが重要**であり、結局は地元で影響力のある人物や組織を通じたセミナーなどが有効だった。 • 経営者だけでなく、**部門長やスタッフレベルでのサイバーセキュリティの知識とリテラシーの向上**が必要。	• 地元の著名人や業界リーダーを活用し、経営者や一般社員向けのセミナーやワークショップを開催。（★短期施策） • 具体的なサイバー攻撃の事例や、それによる損失、対策の成功事例を共有し、リアリティと緊急性をケーススタディによって伝えること。（★短期施策） • サイバーセキュリティ対策を講じた企業に対する表彰制度や、税制優遇、補助金の提供などのインセンティブを設け、スタッフレベルでの浸透を図る。
	強みに特化した需要促進	• 日本の強みである製造業や医療分野等の、サイバーセキュリティの小規模マーケットに焦点を当てることが有効。	• 強化すべきマーケットの企業間、業界団体、政府機関とのパートナーシップを促進し、情報共有と協力体制を構築する。
	中小企業の需要創出	• 英国でも、サイバーセキュリティの資格取得や基準を設ける試みがあるが、政府案件以外にはあまりメリットがなく、中小企業には浸透しづらいという、同様の悩みを抱えている。	• 低コストで実施可能なサイバーセキュリティ対策の情報提供、専門家による相談窓口の設置、簡易的なセキュリティチェックツールの提供など、中小企業が取り組みやすい支援策を充実させる。

凡例　★短期施策：今期予算の範囲ですぐに開始可能かつ効果的な施策

2.4.2 ソリューションに係る有識者インタビューでのコメントと検討事項（需要側）

	ヒアリング結果	実施検討事項
重要インフラに対する監査基準改定および監査の実施・対応強化	• 重要インフラとその直接サプライヤーはサイバーセキュリティ強化の主要対象とすべきであり、少なくともTier 1およびTier 2レベルは明確に把握する必要がある。 • サイバーセキュリティ対策の有無を市場の判断基準とし、株主の意思決定に影響を与えるよう促すべき。 • 経済安全保障法案の厳格化に伴い、外国製品の使用制限が生じる可能性があるため、日本国内のサイバーセキュリティ産業の育成が求められている。 • 既存の認証制度を活用し、国内ベンダの利用を経済安保の観点から推進すべき。 • サイバーセキュリティはナショナルセキュリティの一環として、自由貿易とは別の問題として国内技術の強化と自立を図るべき。	• 重要インフラおよびそのサプライヤーを対象とした定期的なサイバーセキュリティ監査。 • サイバーセキュリティ対策を講じたり、認証を受けた重要インフラ事業者とその直接サプライヤーに対する税制上の優遇措置や補助金提供。 • 日本国内のサイバーセキュリティ産業の研究開発支援、人材育成プログラムの強化。 • 重要インフラの調達において一定レベルの認証基準（例：欧州のサイバーレジリエンスアクト（CRA）や米国のサイバートラストマーク等）を満たしていることを条件とする。

2.4.3 ソリューションに係る有識者インタビューでのコメントと検討事項（供給側）

	ヒアリング結果	実施検討事項
スタートアップ施策と統合的な取り組み	• 政府の支援としては、スタートアップ期の支援に焦点を当てるべきであり、資金調達、人材確保、場所、情報提供などが海外でも取り組まれている事例。 • スタートアップは、日本の市場環境において1社目の導入事例を作ることが非常に難しく、企業とのマッチング支援が有効である。 • 海外（特に米国）を拠点とする場合、資金調達やビザの取得、現地パートナーの紹介、オフィスの利用など、立ち上げ期を支援することで、スタートアップがより大きな市場で挑戦することを促進する。 • 日本のVCは、米・英のVCに比べて意思決定が遅く、工数もかかる。リスクの取り方、投資判断までの期間・プロセスへの考え方が全く異なる。起業文化や資金調達プロセスに大きな違いがあり、これらを理解することが重要。 • スタンフォード大などでコンピューターサイエンスを学ぶと、そのまま起業をする流れがあり、そのためのテンプレートやノウハウが代々蓄積されている。 • 日本初のスタートアップの事例として、オープンIDなどの国際標準への準拠と、その証明を継続し認証No.1を取り続けて市場の支持を獲得したAuthlete社の例がある。	• サイバーセキュリティ分野に特化したインキュベーターやアクセラレータプログラムを設立し、初期段階のスタートアップをサポート。 • 国内外の大手企業などの潜在顧客や投資家とスタートアップのマッチングを促進するためのイベントを定期的に開催。イベントや場の提供を通じて、スタートアップの人的ネットワーク構築を支援。（★短期施策） • ビザ取得、オフィス賃貸、資金調達などの海外進出支援を通じて大きな市場で挑戦するスタートアップを育てる。 • 意思決定の速い国外のVCを日本に呼び込む施策の推進や、サイバーセキュリティスタートアップに特化した投資基金を設立し、米・英に準ずる資金調達サイクルを作る。 • 米国などのIT・セキュリティ分野で先進的な大学への留学支援を通じて、グローバルな視野と養う人材育成を推進。 • 日本における標準を満たせば、国際標準に合致する認証プログラムを実装、普及促進し、国内外における日本製品の市場価値を高める。
今後需要が見込まれる次世代技術分野（AI・自動運転など）での取組	• 広域5G通信が次世代技術の一大産業としての潜在性を持っており（将来的に路車間通信などでの活用を見込む）、そのインフラの相互依存性が増加している。 • モビリティ、サプライチェーン、IoTなどの分野でサイバーセキュリティのプレゼンスを発揮することが重要。 • 英国の大学（Warwick University等）のように、産学連携を通じた専門的な研究・開発が重要。	• 広域5G通信、モビリティ、IoTセキュリティ等の各分野のサイバーセキュリティについて、各団体・事業者と協力しながら、協力・連携体制を構築する。 • 上記次世代技術に特化した研究機関と企業間の連携を促進する産学連携プログラム、自治体連携プログラム（実証実験の場等）を開発する。

凡例 ★短期施策：今期予算の範囲ですぐに開始可能かつ効果的な施策

2.4.3 ソリューションに係る有識者インタビューでのコメントと検討事項（供給側）

	ヒアリング結果	実施検討事項
製造業等、OT周辺セキュリティ	• 製造業で自社開発で身に着けたサイバーセキュリティ対策（ガイドライン、教育を含む）のサービスを外販する動向あり • 製造業としてのサプライチェーンの底上げは、地域産業に焦点を当てて、中小企業と束になって取り組むべき • OTセキュリティを進めていきたいのであれば、CSSC（制御システムセキュリティセンター）をうまく活用すべき	• 工場セキュリティソリューションを一定以上導入した場合の税制優遇や補助金付加。 • 地域産業で連帯したサイバーセキュリティ対策の導入検討/推進。 • 強化すべきマーケットの企業間、業界団体、政府機関とのパートナーシップ促進の観点から、CSSCとの連携可能性の再検討
海外向け輸出促進施策の関連の取組	• 日本のサイバーセキュリティ企業は国内外、双方市場においてシェア獲得できていると言えない。経済安保上問題と捉える。 • 国内市場の拡大とは別に、大きな市場がある海外市場への展開に焦点を当て、産業育成を促進するべき。 • 日本のニーズに共鳴する国々の研究者を日本に招き、日本の仕様や技術を共有し、国際基準としての地位を高める取り組みを進めるべき。 • パーソナルデータの活用について、EUなど海外で受け入れられる経済的かつ合理的なセキュアで信頼できるセキュリティ基準の確立をしてほしい。 • 海外企業（現地販売パートナーや顧客）と日本企業とのマッチングを促進し、ビジネス機会の創出を目指すことが重要。 • 国際市場において、日本のサービス面での強みや品質重視の特性を活かすことで、米国が勝負できない領域、特定の産業分野での強みを発揮することを目指すべき。	• 日本のサイバーセキュリティ製品・サービスが海外市場で受け入れられるための、各国・各地域の市場調査と展開戦略の策定する。 • 海外の研究者や技術者を積極的に日本に招き、技術交流や共同研究を進める。 • 日本企業の製品・サービスが国際標準に適応できるよう、国内で利用される標準が諸外国の標準と同等以上の基準を満たすことで、グローバル市場における信頼と競争力の強化を目指す。 • 海外企業と日本企業とのマッチングを促進し、ビジネス機会を創出、適切なパートナーシップを構築する。 • 日本ならではの高品質なサービスとガバナンスを海外市場に訴求し、特定産業分野（医療・製造業等）の強みを活かしたサイバーセキュリティ関連の製品・サービス開発とプロモーションを支援する。

2.4.4 ソリューションに係る有識者インタビューでのコメントと検討事項（人材基盤の確立）

	ヒアリング結果	実施検討事項
サイバーセキュリティ関連人材に関する意見	• ユーザー企業において、経営者はじめ、ディビジョンのリスクオーナー（部門長）やその支援スタッフも、サイバーセキュリティに関する情報・知識・リテラシーを持つ必要がある。 • サイバーセキュリティの最も脆弱な部分はPCやスマホのようなエンドポイント。1人1人の希薄な危機意識を政府が主導して醸成していく必要がある。 • 海外人材の受入強化・育成・登用を通じて、日本人のマインドを変えながら、アジアの拠点としてのIT業界の全体のボトムアップをしていくべき。 • トップガン人材の育成が韓国など他国に比べてまだ弱い。高度人材の育成を推進すべき。 • サイバーセキュリティ人材の待遇底上げをしていくべき。日本もセキュリティキャンプなどの制度はあるものの、結局セキュリティと違う仕事をすることが多い。サイバーセキュリティの仕事はあまり評価されないし、実務としては辛いことが多いため、人がなかなかついてこない。	• 経営者・企業/組織の属する中間層を対象に、サイバーセキュリティリテラシーの付加・強化を目的とした人材育成を行う。 • これまで登録セキュスペはベンダー側に偏重して就業している実態があり、ユーザー企業には少ない。ユーザー企業でのさらなる活用やセキュスペの増勢を推進する。 • トップガンの更なる育成に向けて、全国・地方で募集を拡大するなど、セキュリティキャンプの拡張を実施する。 • 高度な人材育成策として、IPAが実施する、ITを駆使したイノベーションにかかる人材育成事業「未踏事業」との連携も検討。

2.5

サイバーセキュリティ関連企業・団体の動向

2.5.1 民間団体の取り組みの調査について（概要）

- 需要喚起、産業競争力強化、人材育成等の政策を実行する上で、経済産業省の政策を補完し、あるいは連携可能な民間団体とのその施策につき、デスクトップ調査等により、調査する。

調査の概要

目的	• 日本の民間団体が実施しているサイバーセキュリティの施策を調査することにより、官民協力等の政策を検討の資とする。
調査対象	• ① 大手企業も含め参画企業が多い等、一定の影響力があり、② サイバーセキュリティ産業（供給側）の競争力強化及び一般企業（需要側）のサイバーセキュリティの強化につき、効果的で、実態があり特徴的な施策を実施している民間団体を選定。 • 特に、産業側の課題へアプローチする施策（人材育成、海外展開支援、技術力向上等）を行っている団体や、需要側である一般企業のサイバーセキュリティ投資を促進する施策（例：中小企業支援、評価制度等）等を行っている団体に焦点を当てる。
調査手法	• 原則としてデスクトップ調査を実施。ただし、有識者へのインタビューで言及があった場合は引用。 • 各団体の施策のうち、産業活性化に資する施策を抽出して整理。経済産業省との補完的役割や連携の可能性についても分析。

調査対象団体の概要

日本ネットワークセキュリティ協会	• サイバーセキュリティベンダーを中心とし、サイバーセキュリティの必要性訴求と関連する諸問題の関係者間の解決のため、の団体。サイバーセキュリティについての調査研究、知識の共有、海外進出促進、人材育成等の施策を実施。
日本IT団体連盟	• サイバーセキュリティベンダー（供給側）の企業やベンダー参加の団体が参加。ITに関する政策提言・要望、サイバーセキュリティ強化等の諸施策を実施。
中小企業サイバーセキュリティ支援協会	• 中小企業（需要側）のサイバーセキュリティ対策強化を目的として、設立。中小企業がサイバーセキュリティ専門家集団と適切なセキュリティ体制を構築する支援を実施。
JPCERTコーディネーションセンター	• 一般企業（需要側）向けに、サイバーセキュリティインシデントへの対応支援、企業への助言等を目的とし発足。サイバーセキュリティインシデントについて、 報告の受付、対応の支援、分析、再発防止対策の検討や助言などを実施。海外のCSIRTとも連携。
重要生活機器連携セキュリティ協議会	• 生活に密接に関わる重要なIoT機器・システムのセキュリティ強化を目的とし設立。主にサイバーセキュリティベンダー（供給側）の企業等が参加。IoT機器のセキュリティ向上のため、認証制度創設、関係者間での技術開発、人材育成等を実施。

2.5.2 日本ネットワークセキュリティ協会(JNSA)

- 日本ネットワークセキュリティ協会(JNSA)では、セキュリティベンダーの海外展開支援や高度な人材、多様な人材を含めた人材育成等、産業活性化に資する各種施策を実施。

団体の概要

概要	• サイバーセキュリティの必要性訴求と関連する諸問題の関係者間の解決のため、2000年に設立。271のセキュリティベンダー企業等供給側の関係者が中心に参加、サイバーセキュリティの調査研究、参加団体間での知識の共有、海外進出促進、人材育成等の施策を実施。

主な実施施策の概要（産業活性化に関する施策を抽出）

産業競争力強化	**【海外展開支援】** • 海外における外国政府向けの製品・サービス紹介セミナーを経済産業省とともに実施。（2016年に「日・ASEAN 情報セキュリティ政策会議」において日本製品・サービスを外国政府に紹介するセミナーを実施。） • 団体に参加している企業に対し、情報提供や参照資金の支援等の海外展示会参照へのサポート。
人材育成	**【多様な人材の活躍推進】** • 交流イベント開催、キャリア相談等を通じた女性キャリア支援を実施。 **【サイバーセキュリティの学校教育推進】** • サイバーセキュリティの知識・技能を大学や専門学校等で実験的に教育を実施。 **【高度な人材育成】** • 企業のCISOが能力向上できるような机上演習を実施。 • 実践的情報セキュリティ人材の発掘・ 育成、技術の実践の場の提供を目的とした情報セキュリティコンテストイベント開催。

経済産業省の政策の補完的役割及び可能な経済産業省との連携の方向性について

補完的役割	• 女性等の多様な人材育成に向けた支援活動。
連携の方向性	• 引き続きの海外展開支援における連携（海外におけるマッチングイベントの開催等）。 • 高度な人材の発掘・育成における連携（情報セキュリティコンテストイベント等）。

2.5.3 日本IT団体連盟

- 日本IT団体連盟は、一般企業向けの対策公開に関する格付け公表による対策促進を行うことで、需要創出を通じた産業活性化につながる施策を実施。

団体の概要

概要

- IT関連団体の連合体として、政府への提言等を行い、世界水準のIT社会の構築を目指すため、2016年に設立。セキュリティベンダー（供給側）の企業やベンダー参加の団体が参加。ITに関する政策提言・要望、サイバーセキュリティ強化等の諸施策を実施。

主な実施施策の概要（産業活性化に関する施策を抽出）

需要創出

【一般企業向けの対策公開に関する格付け公表による対策促進】

- サイバーセキュリティ対策強化による企業価値向上を行う目的で、有価証券報告書やコーポレートガバナンス報告書等の開示情報等を踏まえ、総合的にサイバーセキュリティへの情報発信及び取り組みが積極的である企業を「サイバーインデックス」認定事業者として評価する仕組みを構築。また、毎年度取り組みが優秀な企業を発表。
- なお、IT団体連盟の当格付け制度の担当者の認識としては、以下のとおり。
  - サイバーインデックスが公表されるたび、日本人よりも海外の人に公表結果を見られている傾向であり、7割程度が海外からのアクセスであると承知。
  - 企業側も、表彰された事実をHPやIR情報としてプレスリリースしているが、市場における売上拡大や、機関投資家からの融資への影響など、サイバーセキュリティの取り組みをしたからといって、直ちに株価に影響を与えたり企業価値に何か急激に変化が加わることは今のところ見たことはないが、企業価値の一つとして注目度が高まっているのは事実。

経済産業省の政策の補完的役割及び可能な経済産業省との連携の方向性について

連携の方向性

- 投資家と一般企業の間におけるサイバーセキュリティ対策公開のあり方を議論する場での連携（現状の格付け制度を踏まえた、公開のあり方に関する今後の課題案出等）。

2.5.4 JPCERTコーディネーションセンター(JPCERT/CC)

- JPCERTコーディネーションセンター(JPCERT/CC)では、重要インフラ事業者を対象とした対策促進・啓発等の需要創出を通じた産業活性化につながる各種施策を実施。

団体の概要	
概要	• サイバーセキュリティインシデントへの対応、企業への助言等を目的とし、1996年に発足。一般企業（需要側）向けの活動を実施。サイバーセキュリティインシデントについて、 日本国内に関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なう組織。日本の窓口CSIRTとして、海外のCSIRTとの連携も実施。
主な実施施策の概要（産業活性化に関する施策を抽出）	
需要創出	**【一般企業向けの脅威情報等の公開による対策促進】** • セキュリティ上の脅威となるトラフィックを定点観測するシステム「TSUBAME」の運用し、サイバー攻撃の予兆を監視。また、サイバー脅威に関する早期警戒情報を公開。また、登録組織同士の情報共有用のポータルサイトを運営。 **【重要インフラ事業者を対象とした対策促進・啓発】** • 重要インフラ等の制御システムのセキュリティ対策について、脅威情報発信、自己診断ツール（「J-CLICS」、「日本版SSAT（SCADA Self Assessment Tool）」）の配布、アセスメントサービスの提供、年１回のシンポジウム開催を通じた普及啓発活動等を実施。
産業競争力強化	**【サイバー攻撃に関する研究】** • インシデントを分析し、マルウェアや攻撃ツールについての分析結果などについて報告書やツールにまとめて公開。
経済産業省の政策の補完的役割及び可能な経済産業省との連携の方向性について	
補完的役割	• 日常的なサイバー脅威情報の企業への提供と継続的な企業の対策強化。 • OTセキュリティの強化推進（重要インフラ事業者向けの対策推進等）。
連携の方向性	• 事業者（重要インフラ事業者含む）のサイバーセキュリティ対策水準の定義とその普及（水準定義を前提としたアセスメントサービス実施等）。

2.5.5 中小企業サイバーセキュリティ支援協会

- 中小企業サイバーセキュリティ支援協会は、個別相談会等中小企業向けのサイバーセキュリティ対策強化支援により、中小企業の需要創出を通じた産業活性化につながる施策を実施。

団体の概要	
概要	• 中小企業（需要側）のサイバーセキュリティ対策強化を目的として、2022年に設立。具体的には、中小企業がサイバーセキュリティ専門家集団と適切なセキュリティ体制を構築する支援を実施。

主な実施施策の概要（産業活性化に関する施策を抽出）	
需要創出	**【中小企業向けのサイバーセキュリティ対策強化支援】** • 個別の会員企業に対して、サイバーセキュリティ対策の専門家による中小企業への技術的な事項に関する個別相談会、脆弱性診断を実施。また、セミナーとして、企業規模に見合ったサイバーセキュリティ対策方法について解説を行うセミナーについても開催し、中小企業の対策を促進。 • なお、将来的には、有する人材が限定的な中小企業向けのサイバーセキュリティ対策の担当者の労務管理に関する個別相談会の実施や、サイバーセキュリティに関連する社員規定等のテンプレート提供等も予定している。

経済産業省の政策の補完的役割及び可能な経済産業省との連携の方向性について	
補完的役割	• 引き続きの中小企業向け対策の個別相談対応。
連携の方向性	• 中小企業向けのサイバーセキュリティ対策水準定義における協力（当該団体が掌握する課題感の案出等）や周知。

2.5.6 重要生活機器連携セキュリティ協議会(CCDS)

- 重要生活機器連携セキュリティ協議会は、IoTセキュリティに関する企業の技術開発支援や人材育成等、産業活性化につながる施策を実施。

団体の概要

概要	• 生活に密接に関わる重要なIoT機器・システムのセキュリティ強化を目的とし、2014年に設立。主にセキュリティベンダー（供給側）の企業等が参加。IoT機器のセキュリティ向上のため、認証制度創設、関係者間での技術開発、人材育成等を実施。

主な実施施策の概要（産業活性化に関する施策を抽出）

需要創出	**【IoT機器のセキュリティ強化推進】** • サイバー保険と連動したIoTセキュリティの認証制度（認証を得た製品がサイバー攻撃をうけた被害にあった場合に、保険適用がなされる制度）の創設等を実施。
産業競争力強化	**【IoTセキュリティの研究開発の支援】** • IoT製品のセキュリティ性能を検証する共通検証基盤の整備や検証ツールの開発等により、企業の研究開発を支援。なお、当団体は、車載機器や金融端末等の分野における技術的な標準についても策定を実施。
人材育成	**【地方におけるIoTセキュリティ人材の育成】** • 内閣府の委託を受けて、沖縄におけるIoTセキュリティ人材の育成プログラムを運営。 **【高度なIoTセキュリティ人材養成】** • IoTに対するハッキングの手法を学習することで、攻撃者の視点を習得し、セキュリティ技術を向上させる研修プログラムを提供。

経済産業省の政策の補完的役割及び可能な経済産業省との連携の方向性について

補完的役割	• IoTセキュリティの向上に関する研究開発支援。
連携の方向性	• IoTセキュリティの人材育成に関する協力（人材育成の委託等）。

2.6

サイバーセキュリティ産業の意義の整理

2.6. サイバーセキュリティ産業の意義の整理

2.6.1 我が国サイバーセキュリティ産業活性化の3つの意義

- 社会におけるデジタル化が加速する中、① 我が国の経済成長への貢献（経済政策）、② デジタル社会及び多様な人材が活躍する社会の実現（社会政策）、③ 安全保障の強化と技術力の向上（経済安全保障政策）、といった各政策面でサイバーセキュリティ産業の意義が存在。

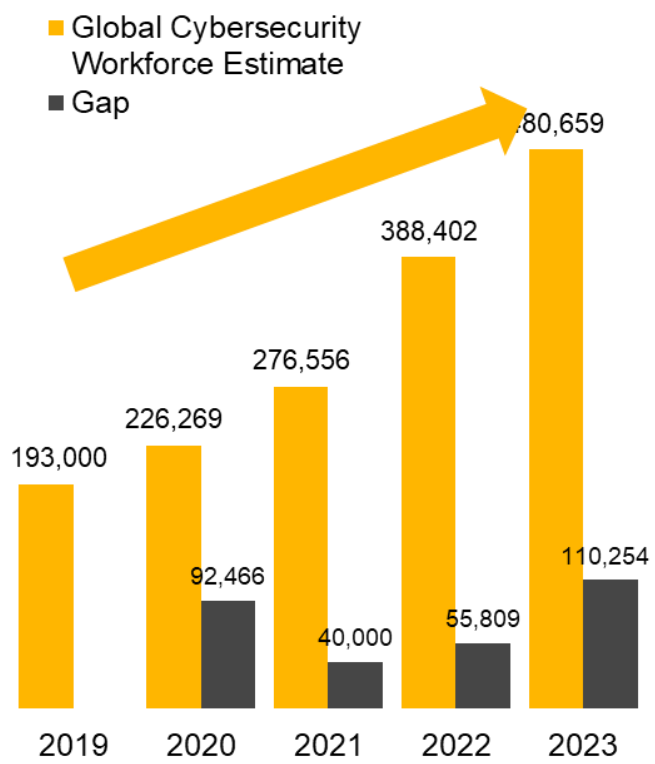
我が国サイバーセキュリティ産業活性化の3つの意義

	1 経済成長への貢献（経済政策）	2 デジタル社会や多様な人材が活躍する社会の実現（社会政策）	3 安全保障の強化と技術力の向上（経済安全保障政策）
国家としての課題	• GDPが毎年1～2%で成長すると予想されている中で、年6%程度の成長する国内サイバーセキュリティ市場は有望な市場。また、グローバルにおいてもサイバーセキュリティ市場は大きな成長を遂げる。市場成長の成果を日本企業が取り込み、我が国の経済成長に貢献する必要。 • また、サプライチェーン全体でサイバーセキュリティを強化することで、製造業等、我が国の基幹的な産業が安定的に操業を行い、利益を生み出す環境を整備する必要があり、これを保障する産業基盤が必要。	• 教育、医療、街づくり、子育て支援等の諸課題を解決するため、デジタル社会を推進する必要がある一方で、その進展に伴い、サイバーセキュリティのリスクが高まる。 • したがって、安心・安全なデジタル社会の実現にサイバーセクターで雇用される人材だけでなく、ユーザー企業・団体等で雇用されるサイバーセキュリティ人材の確保が不可欠。 • 国内の専門家は増加傾向にあり、女性割合も拡大している。背景に法令対応やガバナンスなど業務多様化による文系出身者の活躍領域拡大があげられる。人材確保に向け女性、文系出身専門家の増加は必要不可欠。	• 近年、サイバー攻撃による重要インフラの機能停止や破壊、機微情報の窃取等は、国家を背景とした形で平素から行われている。厳しい安全保障環境に直面する我が国は、その防衛のため、サイバー安全保障分野における対応能力の向上が必要となる。 • 特に、政府機関や、サイバー攻撃の標的となった際に、影響の大きい重要インフラ分野については、経済安全保障の観点から、ある程度の自律性を確保した上で、サイバーセキュリティに関する高度な技術を保持する必要がある。
意義	**産業活性化による競争力のある国内ベンダーの増勢により、サイバーセキュリティ市場の成長を取り込み、また、サプライチェーン全体のサイバーセキュリティ強化を実現することで、我が国の経済成長に貢献する。**	**産業活性化により、安心・安全なデジタル社会の基盤となるサイバーセキュリティ人材の確保につながる。**	**産業活性化により、我が国セキュリティベンダーの技術力が向上することで、一定程度の自律性を確保した上で、国や重要インフラ事業者のサイバーセキュリティが向上。**

（補足） 社会政策の観点からの意義：国内サイバーセキュリティ専門家は年々増加、女性専門家も増加傾向にある

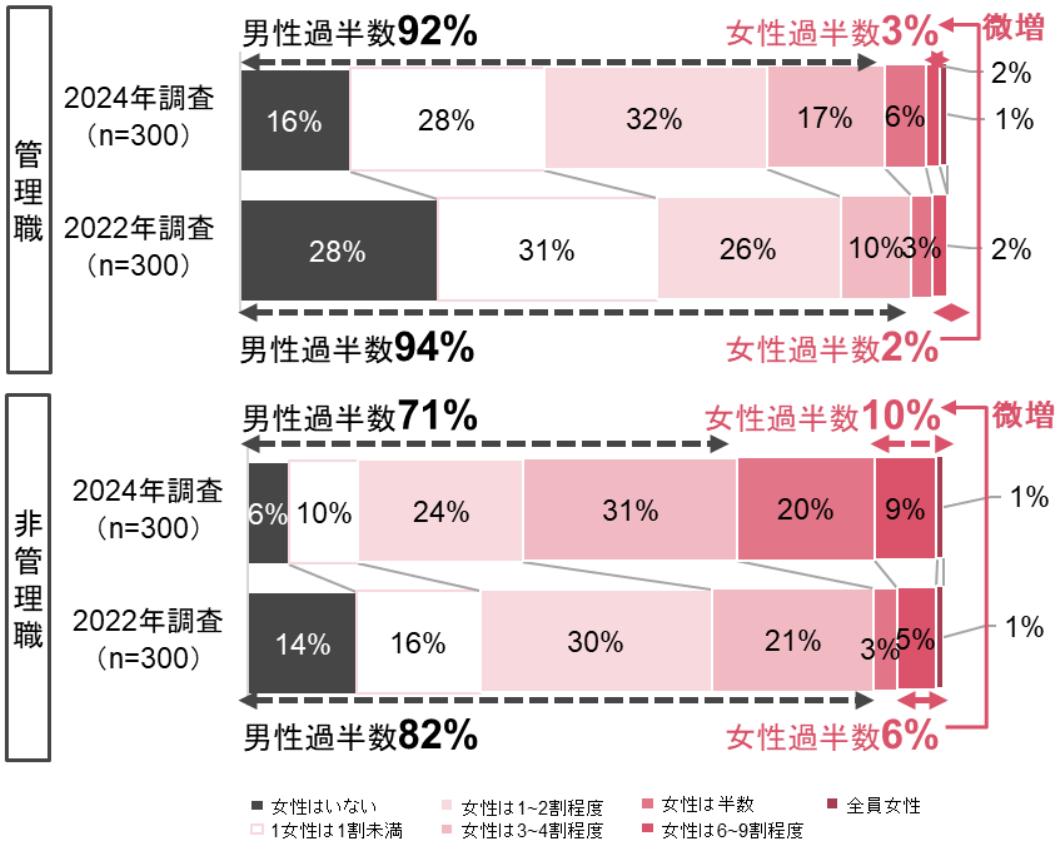
- （ISC）[2]調査によると、国内サイバーセキュリティ専門家は増加傾向、2023年に48万人に達する。
- PwC調査（2022年・2024年比較）では国内サイバーセキュリティ専門家のチームにおける男女の割合は、依然として「男性が半数を超える」と回答する割合が高いが、「男女比率は同じ」や「女性が半数を超える」職場が管理職・非管理職ともに微増しており、国内女性専門家は増加傾向にあるといえる。

図1. 国内サイバーセキュリティ専門家の増加率・過不足



出所：(ISC)[2] "Cybersecurity Workforce Study 2020-2023"を基にPwCが作成

図2. 国内サイバーセキュリティ専門家：チームにおける女性の割合

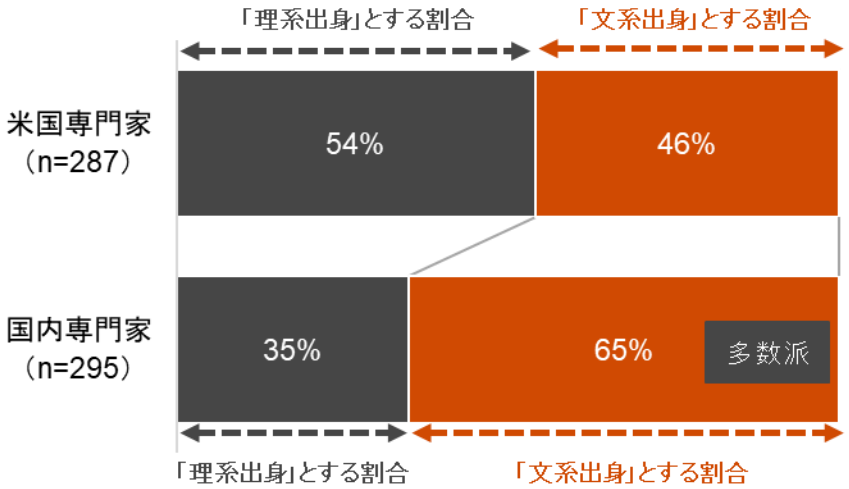


出所：PwC「サイバーセキュリティおよびプライバシー業界で働く女性の実態調査」2022年および2024年を基に作成

（補足） 社会政策の観点からの意義：最終学歴、理系・文系ともに活躍する背景に「業務の多様化」

- PwC調査の回答者属性としてサイバーセキュリティ専門家の最終学歴（専攻）をみると、日米ともに文系出身者が半数を占めた。
- 国内専門家（文系）は、「非エンジニアリング領域が多い」とする割合が半数を占める。この背景に、法規制やグループガバナンス（サプライチェーン含む）強化などセキュリティ関連業務の多様化があるとみられる。

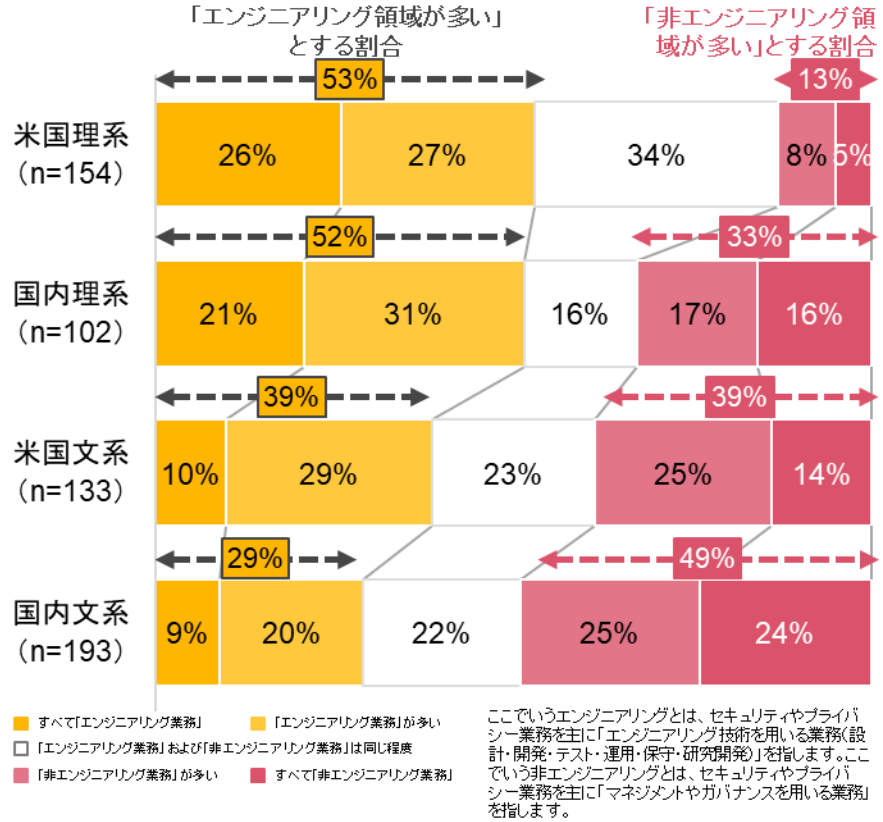
図3.回答者の属性 最終学歴における専攻分類（日米比較）



国内専門家では「文系」が65%と過半数を占め、米国では「理系」「文系」それぞれ約半数存在しており、日米ともに文系出身者が多く携わる領域であることが分かる。

ここでいう「文系」とは、文学、社会学、教育学、経済学、経営学、商学、法学・政治学、国際関係学、語学（外国語）、芸術系・音楽、体育・保健科学を指します。ここでいう「理系」とは、理学、情報学、情報セキュリティ学、工学、医・歯・薬学、看護・福祉・栄養学、農学・水産学を指します。

図4.日米専門家における「エンジニアリング業務の割合」（2024年調査）



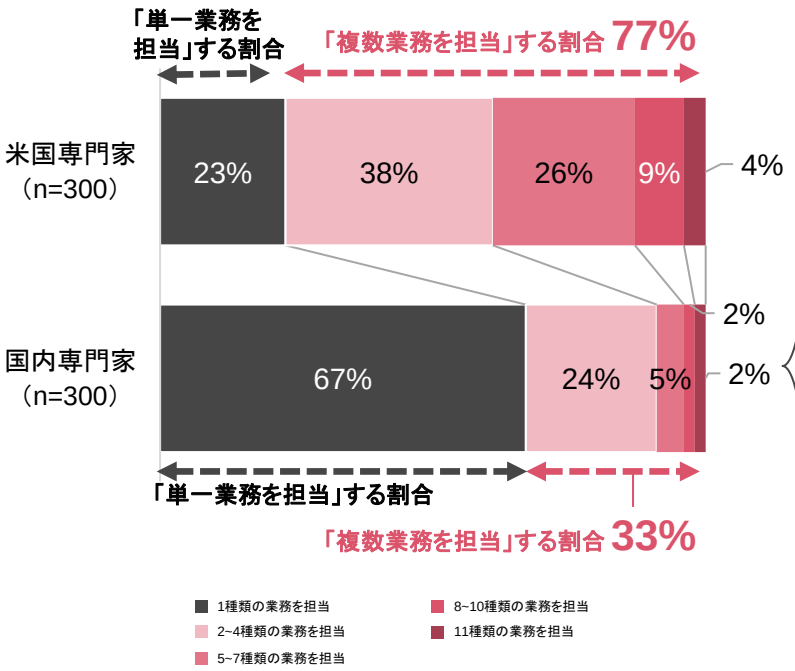
ここでいうエンジニアリングとは、セキュリティやプライバシー業務を主に「エンジニアリング技術を用いる業務（設計・開発・テスト・運用・保守・研究開発）」を指します。ここでいう非エンジニアリングとは、セキュリティやプライバシー業務を主に「マネジメントやガバナンスを用いる業務」を指します。

出所：PwC「サイバーセキュリティおよびプライバシー業界で働く男女の実態調査」2024年を基に作成

（補足） 社会政策の観点からの意義：複数業務を担当するサイバーセキュリティ専門家の割合

- サイバーセキュリティ専門家の業務内容を具体的にみると、米国では「複数業務を担当」する割合が8割と高く、日本は「単一業務を担当」する割合が7割を占め分業化の傾向が強いことが分かる。
- また、米国専門家では、「セキュリティ経営」「セキュリティ統括」「経営リスクマネジメント」「デジタルシステムストラテジー」が順に高く、国内専門家でも「セキュリティ経営」「セキュリティ監査」が最も高く、マネジメント・ガバナンス領域に携わる専門家が多いことが分かる。

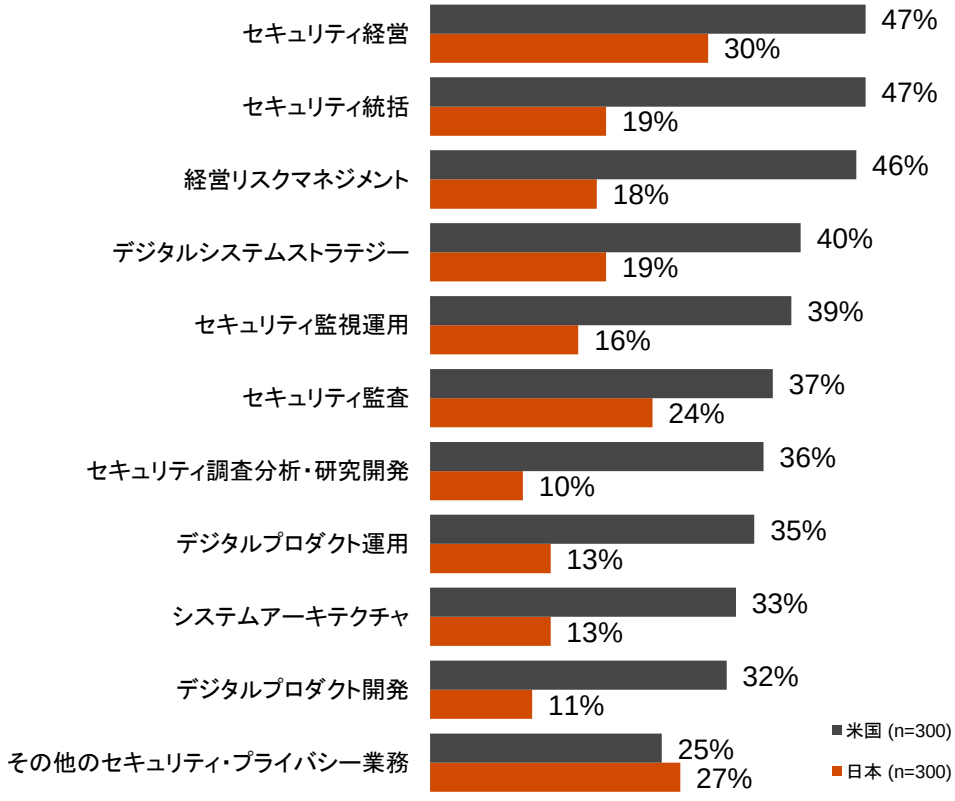
図5.複数業務を担当する割合（日米比較）



国内専門家では7割が「単一業務」に従事し、米国専門家では「複数業務」に従事する割合が8割を占める。

参照：PwC「サイバーセキュリティおよびプライバシー業界で働く男女の実態調査」2024年を基に作成。

図6.複数業務を担当する割合（日米比較）｜複数回答



経済産業省、独立行政法人情報処理推進機構「サイバーセキュリティ体制構築・人材確保の手引き」ITSS＋（セキュリティ分野）で定義されている 17 分野（p.11）を基にPwCが「業務タスクの項目」を抽出。
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

（補足） 「サイバーセキュリティおよびプライバシー業界で働く男女の実態調査」（2024）調査方法の概要

- PwCコンサルティング合同会社では、「サイバーセキュリティおよびプライバシー業界で働く男女の実態調査」として、日米合計600名のサイバーセキュリティとプライバシー業務の従事者を対象にアンケートを実施した。

調査方法の概要	
調査対象	• サイバーセキュリティ、またはプライバシー関連業務従事者 • 所属組織：従業員規模300名以上 • サイバーセキュリティ、またはプライバシー関連業務での業務経験：1年以上
調査期間	2024年1月9日（火）～2024年1月18日（木）
調査方法	インターネットによるアンケート調査
回答者数	600名 （日本：男性150名、女性150名、 米国：男性150名、女性150名）

サイバーセキュリティ産業ビジョン原案

前章までの調査・検討を基にサイバーセキュリティ産業振興を官民挙げて行っていくための共通の指針となるビジョンの原案を3章以降に掲載する。

3 サイバーセキュリティを巡る現状と課題

3.1

サイバー空間を巡る現状

3.1.1 世界におけるサイバー攻撃の状況

- 世界においてサイバー攻撃は増加傾向にあり、被害額も増加傾向にある。

図7.FBIへのサイバー犯罪の届出数

- FBIへのサイバー犯罪の届出数は5年間で約2.3倍に増加している。

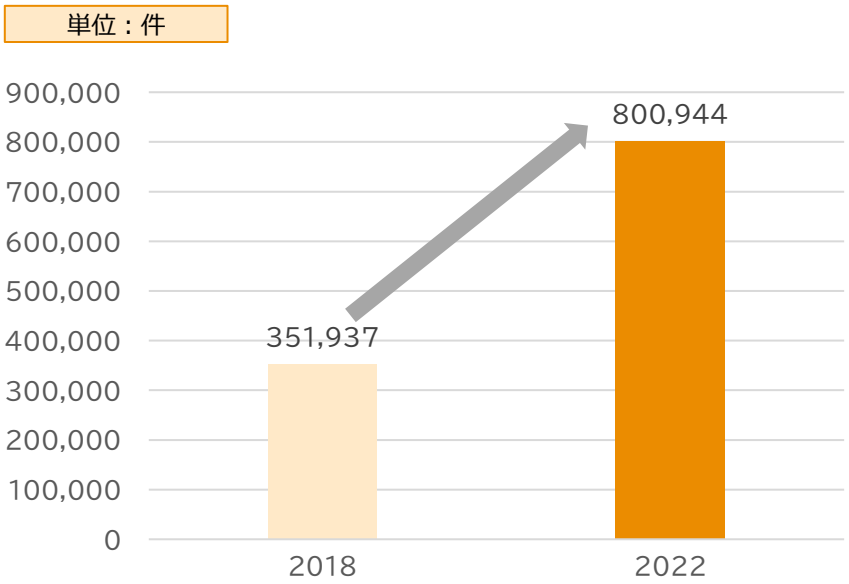
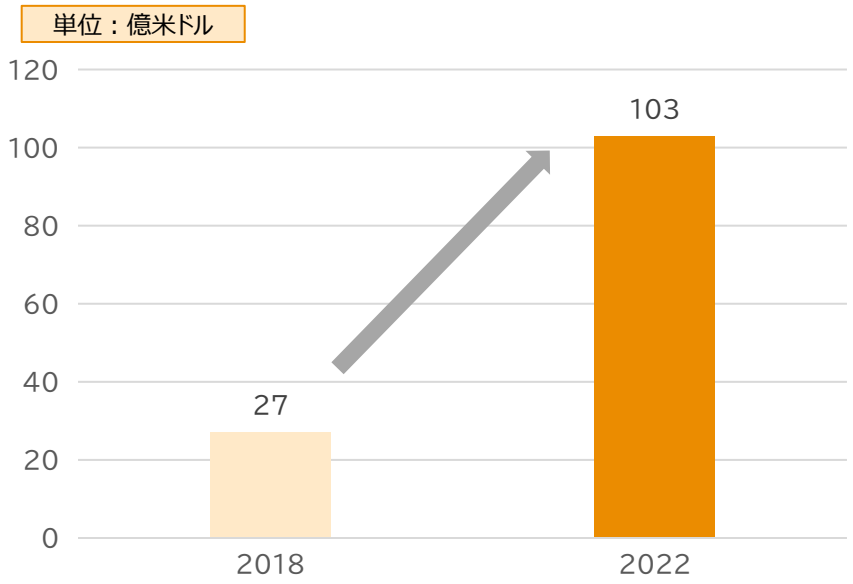


図8.FBIへ届け出られたサイバー犯罪被害額総額

- サイバー犯罪の被害総額は5年間で約3.8倍に増加している。



参照:FBI「Internet Crime Report 2022」をもとに作成。
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

3.1.2 主要国のサイバーセキュリティのこれまでの市場規模推移

- サイバー攻撃の被害が増大する中、グローバル全体及び主要各国では、サイバーセキュリティ市場が急拡大してきている。

図9.グローバルサイバーセキュリティ市場規模推移（2017年→2022年）

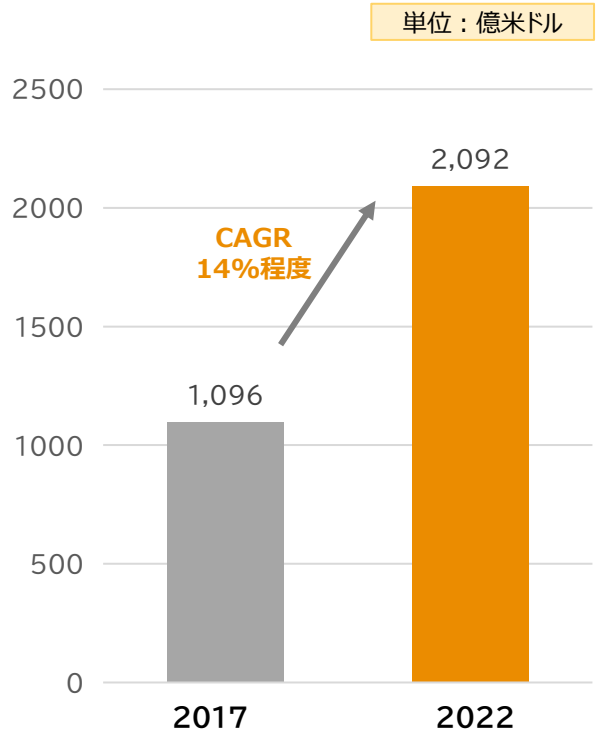
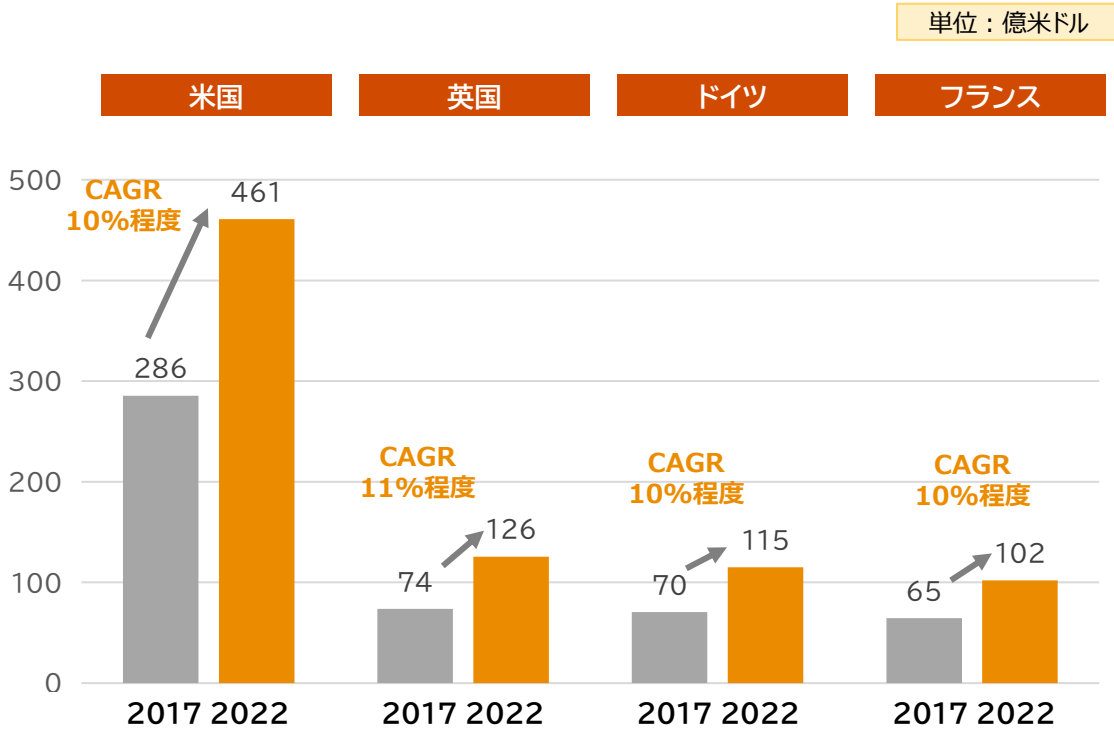


図10.主要国サイバーセキュリティ市場規模推移（2017年→2022年）



※市場規模とは、サイバーセキュリティ（製品、サービス）について、各国の市場において当該年に取引された総額。

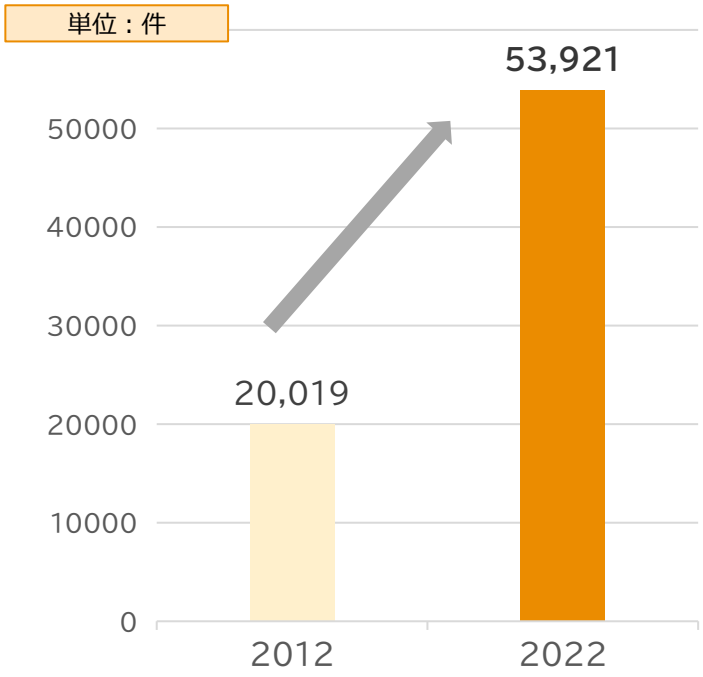
参照：PwC推計。

3.1.3 国内のサイバー攻撃の増加／サイバーセキュリティの重要性

- 直近10年間では日本においてサイバーセキュリティインシデントは増加しており、今後もその傾向は変わらないと考えられる。また、サイバー攻撃によって、現実にサプライチェーンの停止や重要インフラの機能停止といった事案が発生。

図11.日本のサイバーセキュリティインシデント報告数

- サイバーセキュリティインシデントは直近の10年間で約2.6倍に増加している。



サプライチェーンやインフラへのサイバー攻撃事例

サプライチェーンへの影響事例

◆ 自動車部品メーカーの事例（2022年）

- 中堅企業A社は、大手自動車会社に内外装部品を納入する企業。当該企業のシステムがマルウェアに感染したことにより、部品の供給がストップ。大手自動車会社の自動車の生産がストップし、約1万3000台の生産に影響。

インフラへのサイバー攻撃事例

◆ 国際拠点港湾B港の事例（2023年）

- 国際拠点港湾B港（年間貿易額21兆円）のコンテナターミナルでは、ランサムウエアによるサイバー攻撃を受け、システム障害が発生し、およそ3日間にわたりコンテナの積み降ろしができなくなった。

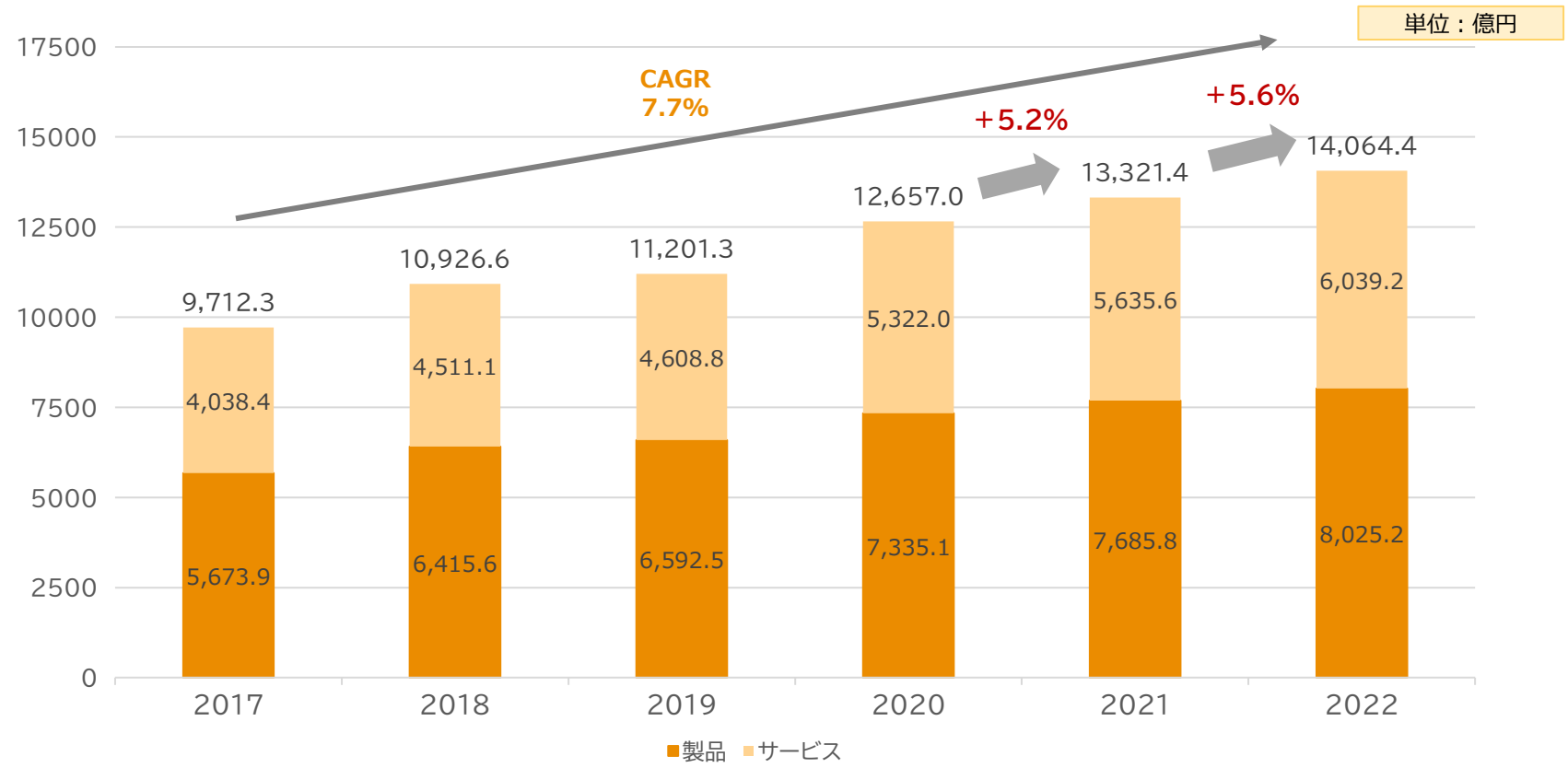
※2022年以降の間でサプライチェーンとインフラへの攻撃で大きくニュースになった事例を選定。

参照：JPCERT/CC「インシデント報告対応レポート：2023年1月1日～3月31日」、各種報道等をもとに作成。
https://www.jpcert.or.jp/pr/2023/IR_Report2022Q4.pdf

ビジョン原案

- 2022年においては約1兆4,000億円市場。直近では5～6%程度で毎年成長。

図12.国内サイバーセキュリティ市場規模の推移



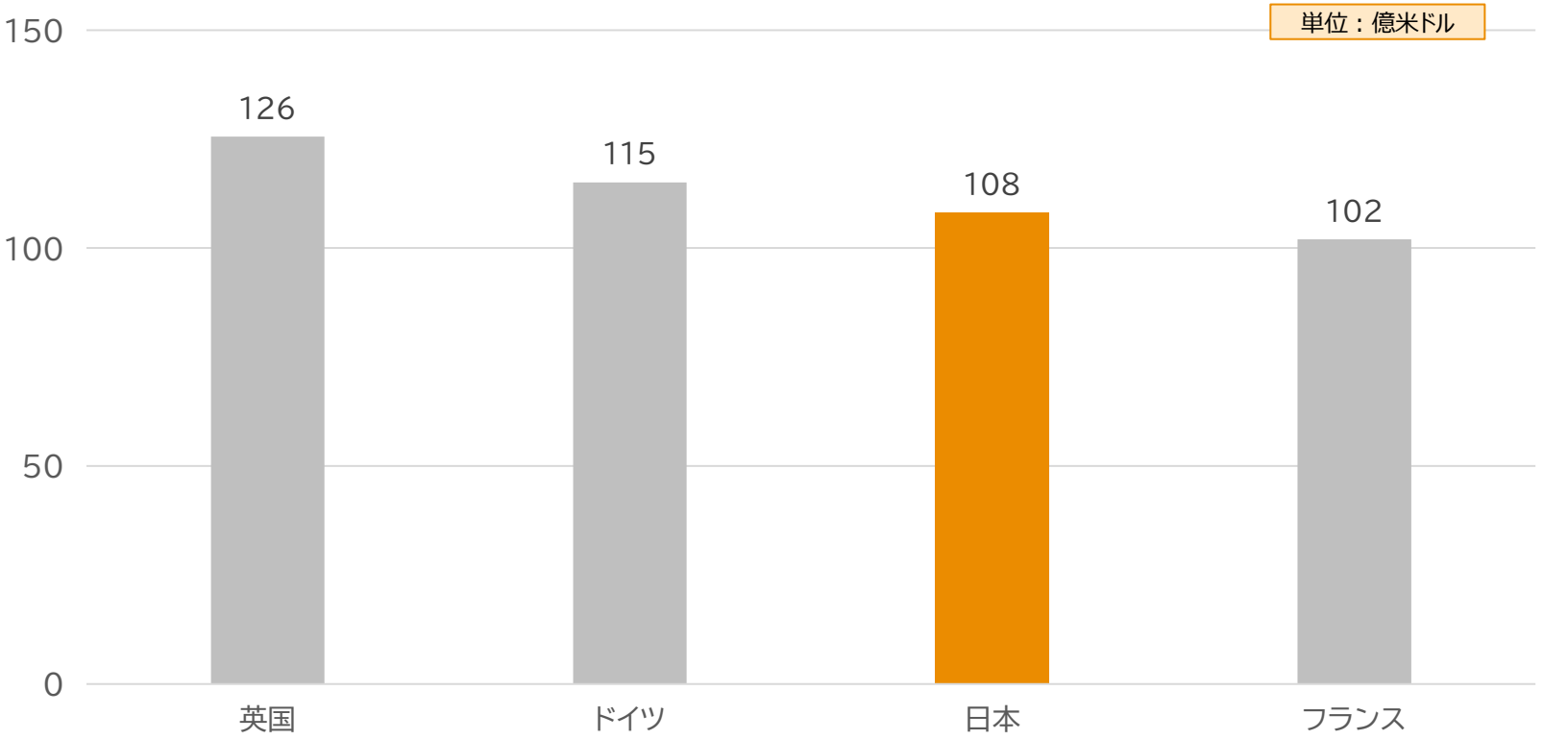
※市場規模とは、サイバーセキュリティ（製品、サービス）について、国内市場において当該年に取引された総額。なお、四捨五入により、各年の製品及びサービス市場の合計が、市場全体の合計を一致しない年がある。

参照:JNSA「2022年 国内情報セキュリティ市場調査報告書」をもとに作成。
https://www.jnsa.org/result/surv_mrk/2023/2022_securitymarket.pdf

(参考)日本と主要国のサイバーセキュリティ投資状況・市場規模

- 我が国のサイバーセキュリティ市場の規模は、英国、ドイツ、フランスと同程度と推計。

図13.2022年の主要国サイバーセキュリティ市場規模比較



※市場規模額とは、サイバーセキュリティ（製品、サービス）について、各国の市場において当該年に取引された総額。1ドル130円換算。

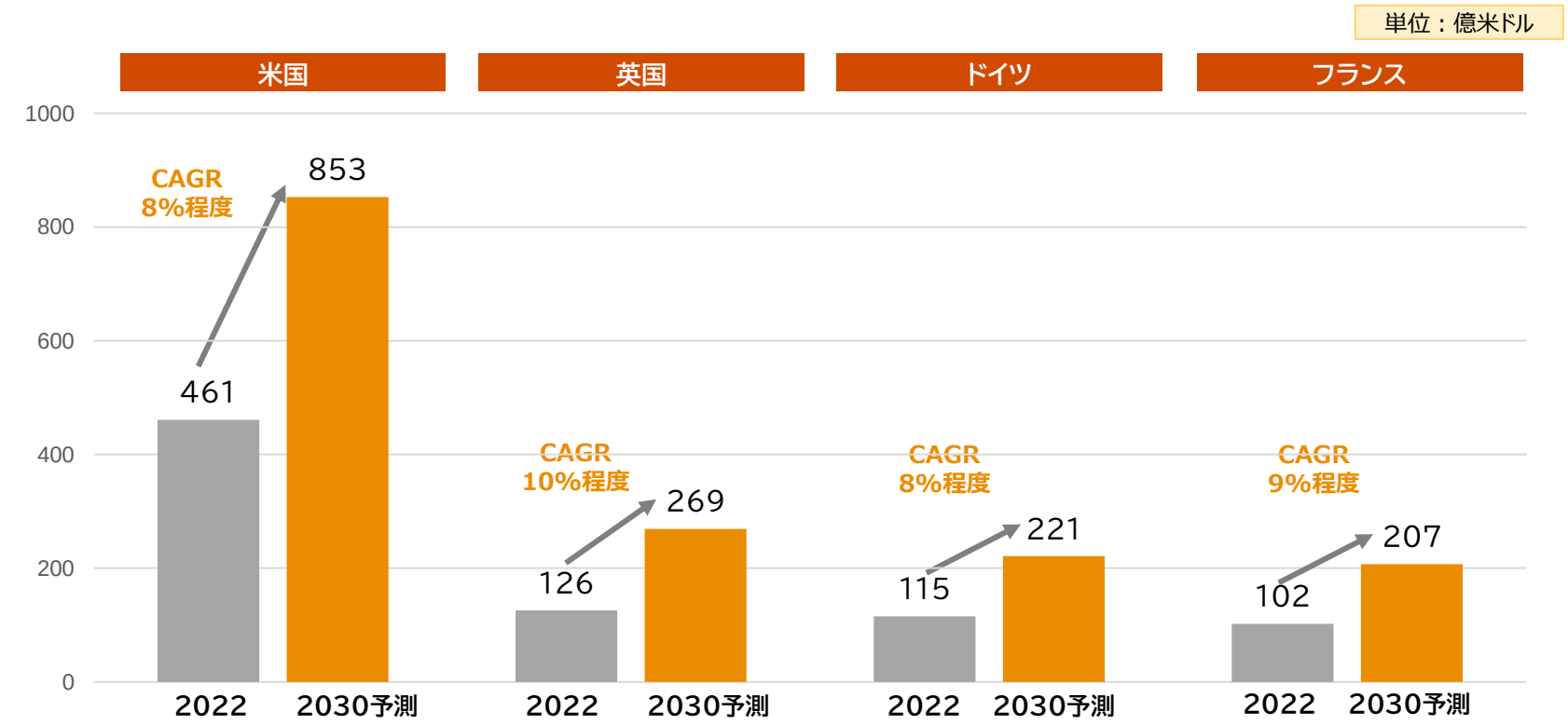
- 参照：PwC推計。

3.2

主要国のサイバーセキュリティ市場予測

- サイバー脅威の増加に備え、主要各国では、今後年平均8～10%程度でサイバーセキュリティ市場が成長し、各国とも2030年には2022年比で市場規模が2倍前後となると推計。

図14.主要国におけるサイバーセキュリティ市場規模の成長予測（2022年→2030年）



※市場規模とは、サイバーセキュリティ（製品、サービス）について、各国の市場において当該年に取引された総額。

参照：PwC推計。

3.3

サイバーセキュリティを巡る国際競争の活発化

3.3.1 サイバーセキュリティを巡る国際競争の活発化 各国の認識

ビジョン原案

- 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。

サイバーセキュリティ産業振興の各国の戦略上の記載や取り組み方針（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セキュリティリスクに対して、**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セキュリティ産業は、**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。

3.3.2 主要国のサイバーセキュリティ投資状況・市場規模（政府投資）

ビジョン原案

- 我が国と米国の中央政府（連邦政府）のセキュリティ予算を比較すると約16倍の差がある。
- 市場規模と比較した場合、米国の中央政府予算は約3割に相当、市場の中で有力な投資主体となっていると見ることが可能。

図15.日米中央政府セキュリティ予算（2023年度）比較

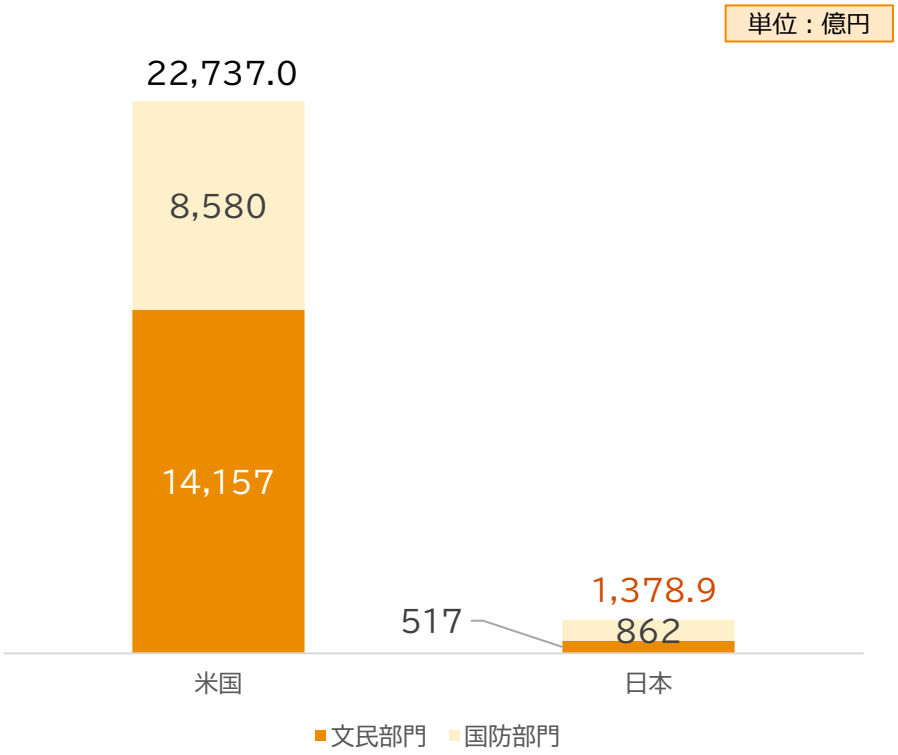
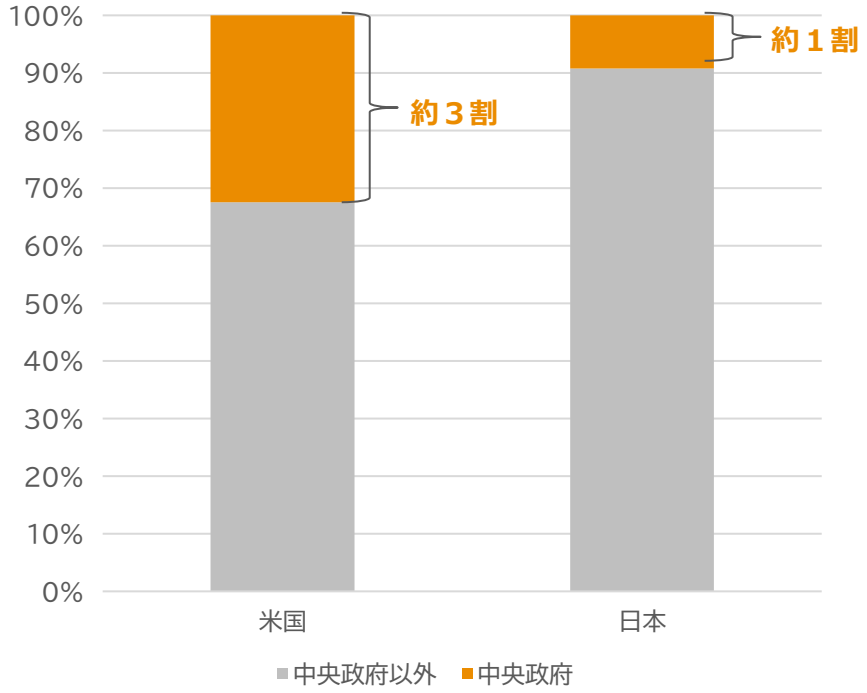


図16.市場規模に対する日米中央政府セキュリティ予算比（2023年度）

※セキュリティ市場規模を１とした場合、国防分も含めた中央政府の全体予算の割合を算出



※１ドル１３０円換算。また2023年の市場規模については、米国市場は成長率が8%との推測に基づき、推計。日本はJNSAの推計で試算。

参照：NISC「政府のサイバーセキュリティに関する予算（令和５年度予算案）」、White House "Analytical Perspectives; Budget of the US Government Fiscal Year23"、Department of Defense "Defense Budget Overview"をもとに作成。
https://www.nisc.go.jp/pdf/council/cs/dai35/35shiryou03.pdf, https://www.whitehouse.gov/wp-content/uploads/2022/04/spec_fy2023.pdf,
https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf

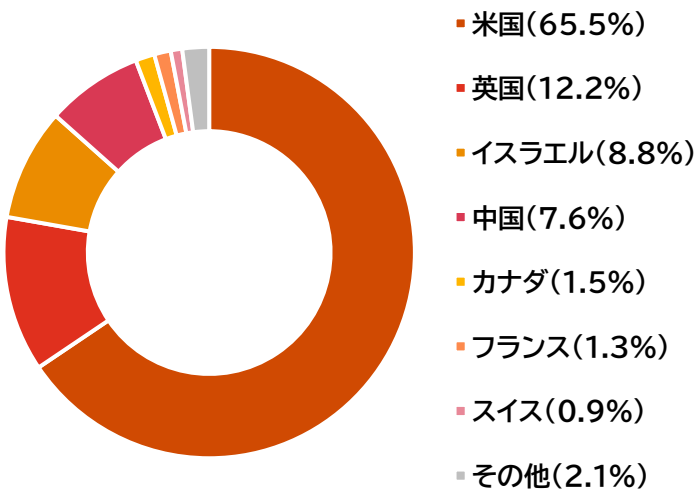
ビジョン原案

- 2024年2月時点でのサイバーセキュリティ分野のスタートアップ総資金調達額は約1350億ドル。米国、英国、イスラエル、中国の4か国で9割以上を占めている。サイバーセキュリティスタートアップの成功例は米国に集中。米国拠点のスタートアップが成功する要因は複数あるが、民間の資金調達オプションの多様性と、その金額と市場規模の大きさが主な背景としてあげられる。

図17.スタートアップ企業に関する現況

21,614	6,243	1,350億ドル	238
企業数	資金提供した企業数	総資金調達額	IPO

図18.国別資金調達シェア(%)



2022年以降ユニコーンとなったサイバーセキュリティスタートアップ企業群

企業名	国	事業分野(製品分野)	設立年	資金調達額
Abnormal SECURITY	米国	クラウド型Eメールセキュリティ	2018	$285M
JupiterOne	米国	クラウド型サイバー資産管理	2018	$119M
Material	米国	Eメールセキュリティ	2016	$166M
IMMUTA	米国	クラウド型データセキュティ・ガバナンス	2015	$267M
TELEPORT	米国	コンピューティングソースにアクセスするためのクラウド型オープンソースソフトウェア	2015	$169M
ARCTIC WOLF	米国	クラウドセキュリティ態勢管理(CSPM)	2012	$879M
Prove	米国	顔認証等のスマートフォンの機能と組み合わせた本人確認・認証	2008	$215M
quantexa	英国	AIを搭載したビッグデータ及び意思決定インテリジェンス	2016	$371M
perimeter 81	イスラエル	ネットワークセキュリティ	2014	$165M
BioCatch	イスラエル	行動的生体AI認証技術を用いた金融詐欺の防止	2011	$253M

参照:Tracxn Technologies「Tracxn Feed Report Cybersecurity February 7, 2024」をもとに作成。
https://tracxn.com/d/reports-feed/cybersecurity-feed-report/_EQ-et6Vx0kgnfLqJ0dEiCfGvm3thrFZRqhivKH1cilI

3.3.3 サイバーセキュリティを巡る国際競争の活発化 研究開発の支援例

- 米国ほどの民間投資/市場規模には及ばないものの、英国はリスク関連ビジネスの世界の中心地として、サイバーセキュリティ産業への活発な投資が行われており、特に政府は国内外のスタートアップ支援や販路の拡大等に政府主導で積極的に取り組んでいる。

英国 ロンドンを中心とするエコシステムの特徴・トレンド

投資を呼び込む大胆な施策	• イノベーション振興に取り組む政府機関のUKDITやInnovate UK、さらに350を超えるアクセラレーター・インキュベーター等、**起業支援を行うプレーヤーが官民共に豊富**で、英国内における海外発スタートアップ支援にも長けている。(次頁詳細) • 2021年の英国全体におけるスタートアップ投資額は前年の約2倍となる約270億ドルに成長。
リスク関連ビジネスの中心地	• 英国、特にロンドンがサイバーセキュリティを含むリスク関連ビジネスの中心であり、技術・人材・情報が集まっている。サイバーセキュリティというマーケットの中心的な役割を英国が担う。 • サイバーセキュリティ対策の必要性を顧客が熟知しており、啓発から始めなくも良い。
外資にも開かれた自由市場	• 英国政府は、スタートアップ等の企業側から働きかけなくても、自国の利益にとって有望な企業に対して積極的にアプローチし、コンタクトを取っている。 • 特に力を入れているのは、サイバーセキュリティ、AI、フィンテック、ゲーミングで、これらに従事する企業や労働者に対しては、外国籍であっても手厚く英国政府が支援している。 • 英国政府が認めたサイバーセキュリティの専門家に対しては、Exceptional Talent VISAを発行し、就労制限が無くなるなどの特別待遇がある。他に、Sole Representative VISAという、会社設立前に準備期間としてVISAを発行するものもある。
政府主導の専門的支援	• **Global Entrepreneur Program(GEP)**によって、政府予算で、経験のあるコンサルタントがメンターとしてスタートアップに派遣される。国外の経営者(例:英国で創業した日本人)であっても、英国内の市場や商習慣の理解促進、立ち上げからスケール等の経営の相談まで、コンサルタント自身の経営経験や考えに基づいたアドバイスを行って支援する制度。(次々頁詳細)
レベルの高い教育機関	• 国際都市のロンドンおよび、学術都市として名高いオックスフォード、ケンブリッジを含めた一帯で一大テックハブを形成しており、日系スタートアップも10社以上が拠点を構える。

ビジョン原案

- 英国政府主導により、サイバーセキュリティスタートアップの立ち上げ・育成・スケールの支援、地方域のケイパビリティ向上、若手人材育成、また商業化される学術研究の支援等、産業活性化およびレジリエンス確保のために目的や状況に応じた支援策が講じられている。

英国政府の主導する支援プログラム・施策例

Cyber Runway	• 起業家、スタートアップ企業等を対象に、ビジネススキル、技術、資金調達等のプログラムを通じて、Launch、Grow、Scaleの3つのフェーズの組織や起業家を支援する。 ➢ Launch：関連する起業家精神のスキルを開発し、潜在的な共同創設者と出会い、新しいサイバービジネスを確立するための個人をサポート。 ➢ Grow ：企業の成長、資金調達、商業的成功を支援するためのサポート。 ➢ Scale ：英国内および国際的にビジネスが急速に成長するのを支援。 • Cyber Runway は、英国のオンライン保護と促進を目的とした政府の 26 億ポンドの国家サイバー戦略の一部で、英国のサイバーセキュリティエコシステムを強化し、持続可能で革新的で国際競争力のあるサイバーおよび情報セキュリティ分野を確保するという目標が含まれている。
UKC3 （UK Cyber Cluster Collaboration）	• 地域のサイバーセキュリティクラスターの能力を高めることを目的とした政策。 • 地域内のサイバー活動への認識と理解、サイバー産業への人材パイプラインの育成、地域内での新しいサイバー・ビジネスの創出などを支援。 • 英国全土でサイバーネットワークを構築するため、国家サイバー部隊の常設本部をイングランド北西部地方に設置して、テクノロジー、デジタル、防衛の各セクターの成長をロンドン以外で促進し、地域の新たなパートナーシップの構築を支援。 • ロンドンおよびイングランド南東部地方以外の地域のイノベーターや起業家が、製品やサービスを開発し、ビジネスを成長させ、高スキルのスタッフを採用するための支援を強化する方針を示す。
CyberFirst	• 多様な才能ある若者を発掘し、サイバーセキュリティのキャリアに育てることを目的とした人材育成プログラム。 • CyberFirst奨学金、女子学生のコンペティション、国内大学での無料のサイバー関連コースの提供等を行う。
Cyber ASAP	• 商業化される学術研究の量を増やすことを目的としたプログラム。重要分野の研究を技術、製品、サービスに転換するために必要な専門知識、トレーニングを大学の研究者等に提供する。

ビジョン原案

- 英国のGlobal Entrepreneur Program（GEP）は、英国政府が主導するイニシアティブで、世界中の革新的な企業家やスタートアップを英国に誘致し、支援することを目的としている。

Global Entrepreneur Program（GEP）とその成功事例

プログラムの仕組み

- Innovator Founder VISAを提供。
- ビジネスの成長戦略の策定、資金調達のサポート、英国内でのネットワーク構築等を含む、一連のサポートを提供。
  - 経験豊富なビジネスアドバイザーや業界の専門家が関わり、ビジネスの立ち上げや拡大に関するアドバイスを提供。
  - 英国内のビジネスコミュニティや投資家、その他の関連ステークホルダーとのネットワーキング機会を提供。
  - 英国のビジネス環境へのアクセスを容易にし、法的・規制的なアドバイス、市場進出戦略などをサポート。
- ビジネスが軌道に乗れば、GEP 同窓会ネットワークの一員となる。

参加資格

- GEPへの参加資格は、以下の条件を満たす企業に限られる
  - ビジネスが概念実証の段階を超えていること
  - 英国で事業を展開していないこと（海外企業のみ対象）
  - また、事業が収益を生み出している、または収益を生み出そうとしており、強力な知的財産（IP）を有していることが理想的な条件
  - グローバル本社を英国に移転する強い意志があり、少なくとも1名の共同創業者が英国を拠点としていること
  - 英国での急成長や高スキルの雇用創出など、英国で会社を発展させるための明確な計画を持っていること

企業名/経営者出身国	成功事例概要
kuda. ナイジェリア	• ナイジェリアのフィンテック新興企業Kudaは、GEPの一環として、2019年に英国にグローバル本部を設立。 • Kudaはフルサービスのデジタル専用チャレンジャーバンクで、本社であるロンドンとラゴスにオフィスを構えている。 • インターネットにアクセスできるナイジェリア人であれば、従来の銀行手数料の負担なしに支出口座を運営し、自動的にお金を貯めることができるアプリを通じて、フルバンキング・サービスを提供。 • これにより、Kuda Bankはアフリカのネオバンクのリーダーであり、フィンテック世代の最前線にいる。
swidch 韓国	• swidchはサイバーセキュリティを専門とする企業で、当初は韓国で設立されたが、テックイベントでGEPと出会い、2018年にロンドンにグローバル本社を設立し、世界初の一方向ダイナミック認証技術「OTAC」を開発。 • これは、全てのデジタルIDに対してより安全な認証を提供し、swidchがサイバーセキュリティにおける認証の新たな基準を設定することを可能にした。 • 同社はここ数年、金融機関にとって世界で最も革新的なサイバーテック企業の1社として認められている。
The Dots オーストラリア	• The Dotsは2014年、グローバル・アントレプレナー・プログラムの支援を受けて、オーストラリアから英国に移転。 • The Dotsは、クリエイティブ・セクターのためのプロフェッショナル・ネットワーキング・サイトを開発、運営している。 • 英国に移転して以来、会員数は30万人を超え、プロジェクトの共有や雇用のためにネットワークを利用する企業は1万社を超えるまでに成長した（英国のクリエイティブ・セクターの10%以上を占める）。

3.3.4 サイバーセキュリティを巡る国際競争の活発化 各国の政策のまとめ

ビジョン原案

- 各国は、① 一般企業のサイバーセキュリティ強化策によって、サイバーセキュリティの市場創出を実現しつつ、② 自国サイバーセキュリティ産業の市場における優位性を獲得するための各種支援、そして、③ 需要側と供給側を下支えする人材の確保といった需要・供給・人材の観点から総合的にサイバーセキュリティ産業活性化を推進するという潮流がみられる。

サイバーセキュリティを巡る各国の対応の潮流（産業活性化策の方向性と代表的な施策）

	各国の戦略における産業活性化政策の方向性	代表的な施策・方針
米国	➢『国家サイバーセキュリティ戦略2023』の産業活性化政策を需要・供給・人材の観点で以下のとおり整理。（カッコ内は各観点に相当する戦略中の柱。以下の国でも同じ） ➢ ① **需要側のセキュリティ対策強化**（「重要インフラ防護」、「脅威アクターの崩壊と解体」） ➢ ② **供給側への支援**（「セキュリティと強靭性を推進するための市場力の形成」、「強靭な未来への投資」研究開発支援部分） ➢ ③ **人材育成策**（「強靭な未来への投資」人材育成策部分）。	➢ コンシューマIoT製品セキュリティの向上に関する政策として、U.S. Cyber Trust Markプログラムを実施。大手小売業者、競合他社などの参加により、IoT製品製造者は対応に迫られ、IoT製品のセキュリティ強化競争を促す狙いがある。***【市場創出】*** ➢「暗号」、「デジタルID」、「クリーンエネルギーグリッドの安全性」といった対象について、研究開発支援を実施***【供給側の競争力強化】*** ➢ 多様性を確保した人材育成策に取り組む***【人材確保】***
EU	➢『デジタル10年に向けたEUサイバーセキュリティ戦略』の産業活性化政策を需要・供給・人材の観点で以下のとおり整理。 - ① **需要側のセキュリティ対策強化**（「レジリエンス・技術的主権・リーダーシップ」、「予防・抑止・対応のための運用能力構築」） - ② **供給側への支援**（「レジリエンス・技術的主権・リーダーシップ」研究開発部分） - ③ **人材育成策**（「レジリエンス・技術的主権・リーダーシップ」サイバーセキュリティスキル強化部分）	➢ 厳格なセキュリティ要件と違反への罰則の強化が含まれるNIS2指令やEEA内で取得した個人データをEEA外に持ち出すことを禁止するGDPR（EU一般データ保護規則）等、他国と比較しても強力な規制をかけており、EU域内の産業保護と競争促進を狙う。***【市場創出と供給側の競争力強化】*** ➢ 労働力のスキルアップ、優秀なサイバーセキュリティ人材の育成、誘致、維持、世界クラスの研究と技術革新への投資は、サイバー脅威全般から身を守るための重要な要素とし、専門職育成に注力。***【人材確保】***
英国	➢『国家サイバー戦略2022』の産業活性化政策を需要・供給・人材の観点で以下のとおり整理。 - ① **需要側のセキュリティ対策強化**（「強靭で豊かなデジタルUKの構築」、「サイバー空間におけるセキュリティ強化のための敵対者の検知・妨害・抑止」） - ② **供給側への支援**（「英国のサイバーエコシステムの強化」、「サイバーパワーに不可欠な技術における主導」） - ③ **人材育成策**（「英国のサイバーエコシステムの強化」サイバースキル強化部分）	➢ サイバー犯罪への対応として、IoT製品に対するセキュリティ保護措置を導入するPSTI法を制定。IoT製品メーカーは最低限のセキュリティ基準に準拠しなければならず、消費者の意識向上とともに、IoT製品のセキュリティ強化競争を促す効果。***【市場創出】*** ➢ スタートアップ市場育成に意欲的で、外資の自国参入にも開かれ、内外問わず良い技術には政府が積極的に投資する姿勢を示す。また、人材育成策も注力。***【供給側の競争力強化、人材確保】***

我が国のサイバーセキュリティ産業の活性化を検討するにあたって、主要国と同様に、① 需要側（市場創出）、②供給側（サイバーセキュリティ産業の競争力強化）、③ 人材育成、の各側面の課題について分析を進めたうえで、検討する。

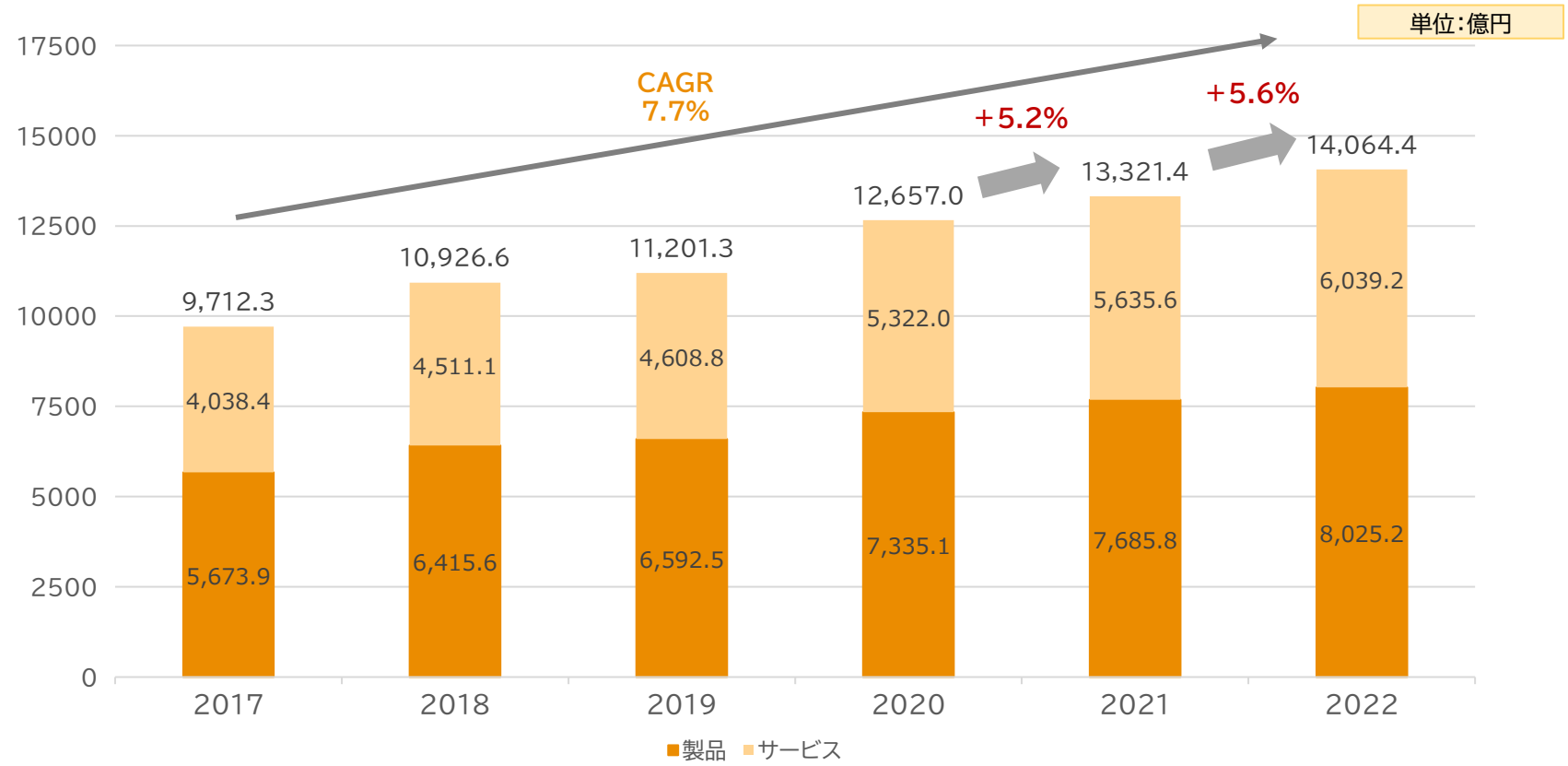
3.4

我が国のサイバーセキュリティ市場を巡る現状と課題

3.4.1　国内サイバーセキュリティ市場の推移

- 2022年においては約1兆4,000億円市場。直近では5～6%程度で毎年成長

図19.国内サイバーセキュリティ市場規模の推移



※市場規模とは、サイバーセキュリティ(製品、サービス)について、国内市場において当該年に取引された総額。なお、四捨五入により、各年の製品及びサービス市場の合計が、市場全体の合計を一致しない年がある。

参照:JNSA「2022年 国内情報セキュリティ市場調査報告書」をもとに作成。
https://www.jnsa.org/result/surv_mrk/2023/2022_securitymarket.pdf

- サイバーセキュリティ製品市場については、下記のような分類で分析

大分類	小分類
ゲートウェイセキュリティ	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)
メールセキュリティ	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
クラウド・Web アクセスセキュリティ	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	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
アクセス・認証	シングルサインオン
	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

大分類	小分類
端末セキュリティ	標的型攻撃対策ツール(エンドポイント)
	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
サイバーレジリエンス	XDR
	SIM
	SIEM
	プラットフォーム検査ツール
	NDR
検疫	不正接続防止ツール
	PC 検疫ツール

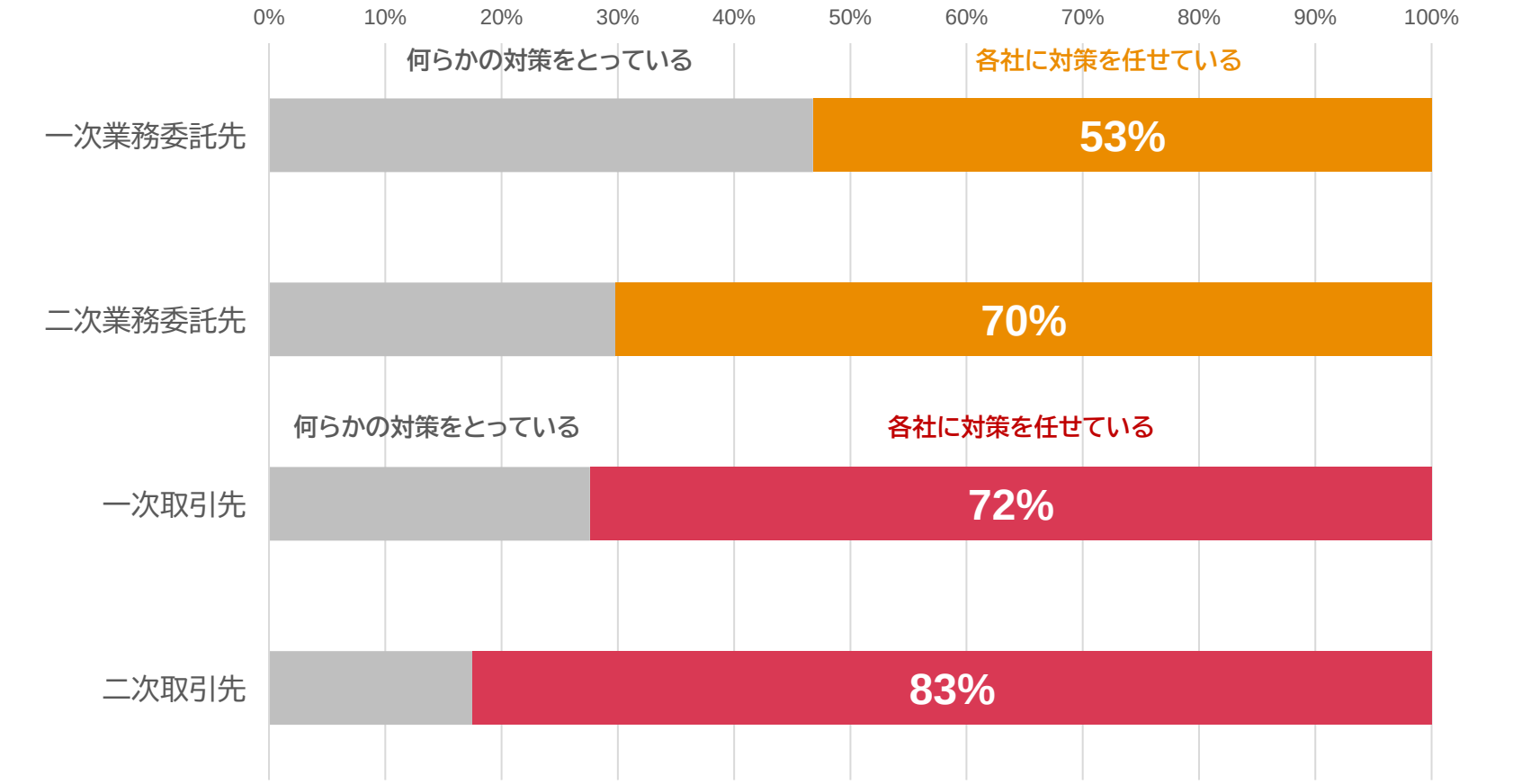
赤字はいわゆるゼロトラスト分野
※他の小分類の中にもゼロトラストに該当する製品が含まれる場合あり

参照: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」)をもとに作成
https://www.meti.go.jp/meti_lib/report/2022FY/000523.pdf

3.4.2　需要側における課題

- また、サプライチェーンの頂点企業は、自社のサプライチェーンの構成企業のセキュリティ対策を十分に把握もしておらず、サプライチェーン全体のセキュリティ対策は万全とはいえない。

図20.サプライチェーン上の他社の対策を把握している日本企業の割合(%)(2023年)

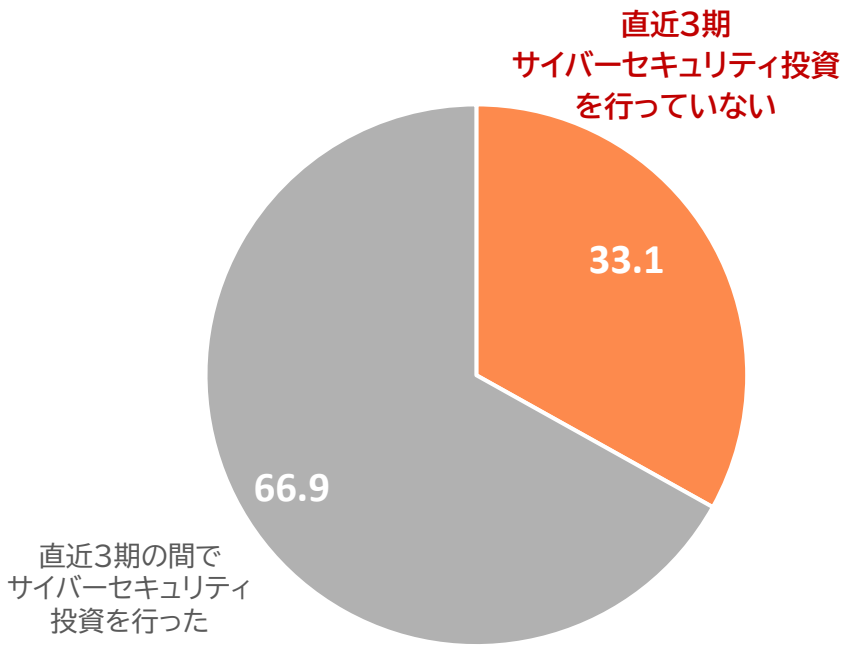


参照:日本情報システムユーザー協会「企業IT動向調査報告書2023」をもとに作成。
https://juas.or.jp/cms/media/2023/04/JUAS_IT2023.pdf

- 需要側の課題としては、中小企業のセキュリティ対策が、コスト面等の課題により、継続的に実施されていない。

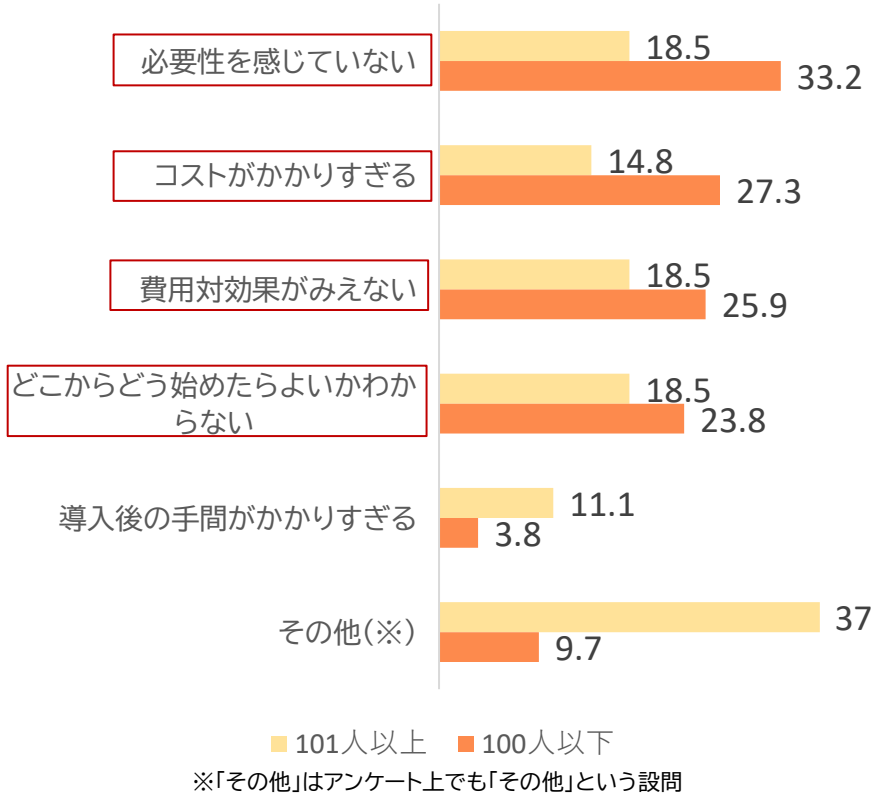
図21.中小企業におけるサイバーセキュリティ対策の現状

直近3期でサイバーセキュリティ投資を行っていない企業の割合(%)



中小企業のサイバーセキュリティ投資を行わない理由(%)

注:複数回答のため、合計が100%にならない



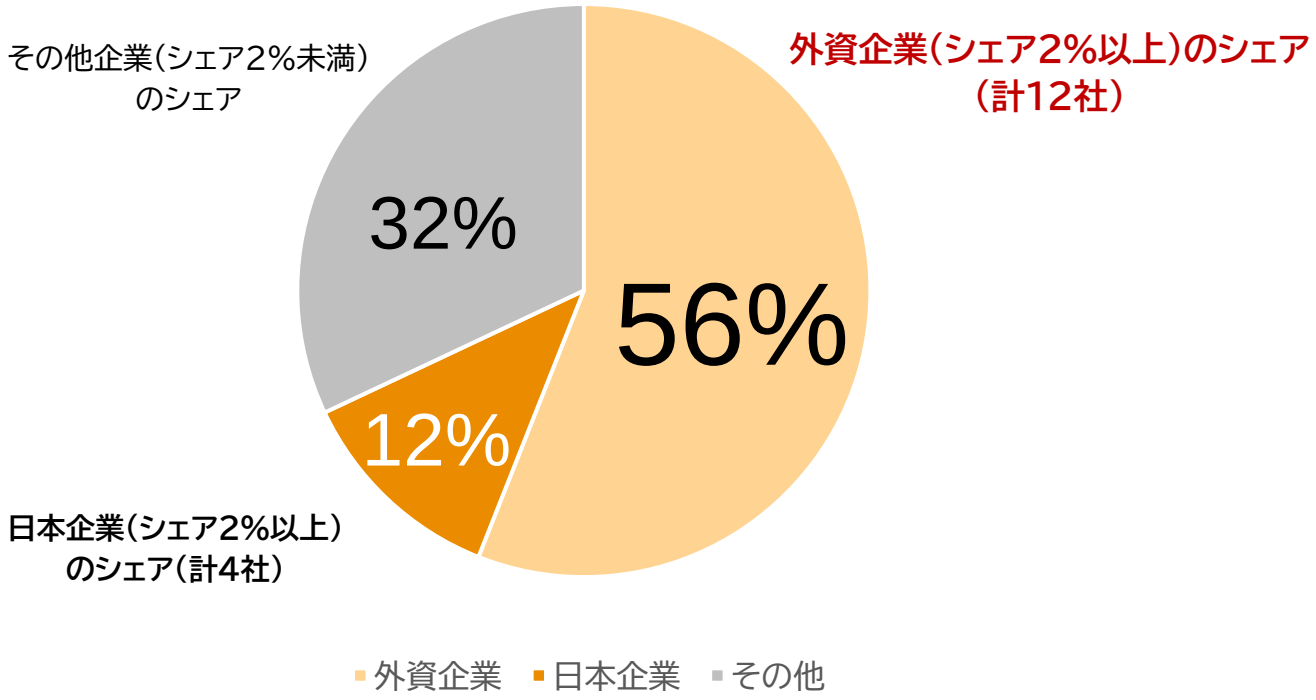
※「その他」はアンケート上でも「その他」という設問

参照:情報処理推進機構「2021年度 中小企業における情報セキュリティ対策に関する実態調査報告書」をもとに作成。
https://www.ipa.go.jp/security/reports/sme/about.html

3.4.3 供給側（サイバーセキュリティ産業）の課題

- 国内製品市場の構造として、外資企業が半分以上のシェアを獲得しており、海外依存度が高い。

図22.国内サイバーセキュリティ製品市場のシェア(2020年)



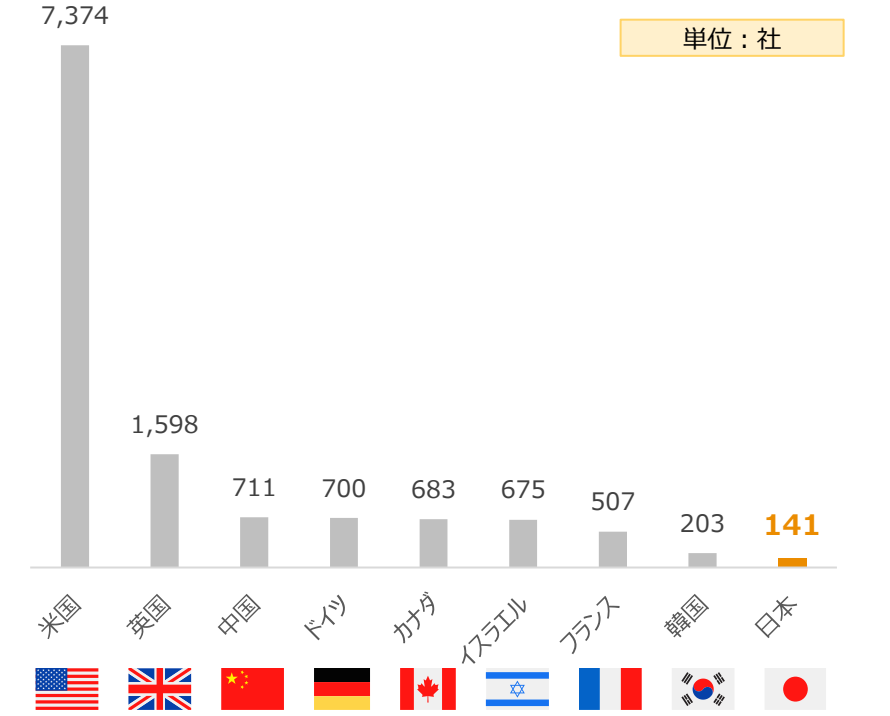
参照:総務省「令和4年情報通信白書」をもとに作成。
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nd237200.html

3.4.3 供給側(サイバーセキュリティ産業)の課題 ― スタートアップ企業数

ビジョン原案

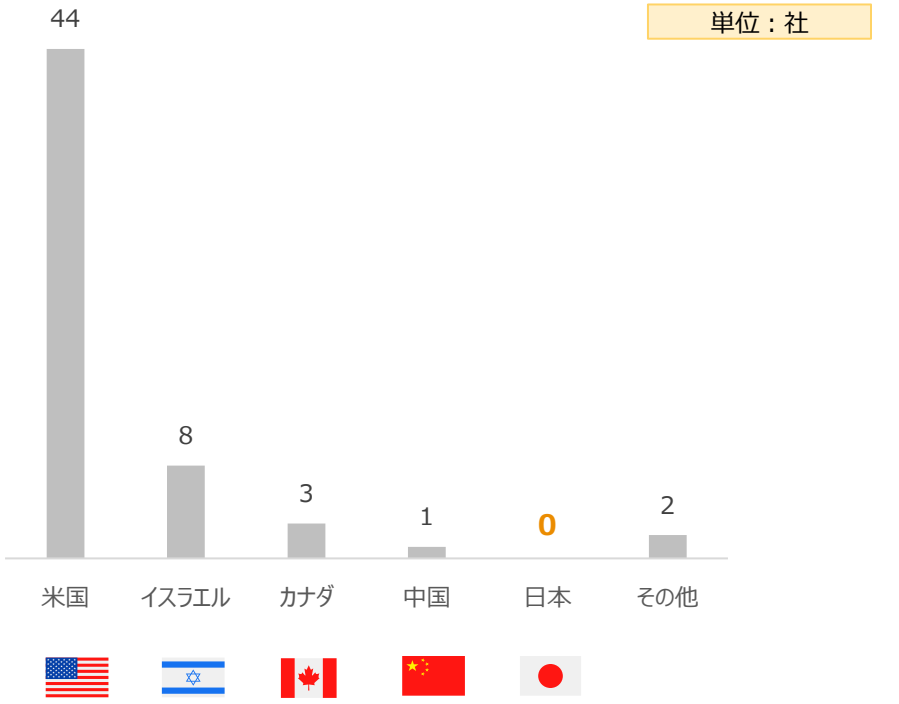
- 他の主要国と比べると日本はサイバーセキュリティのスタートアップ企業数も少なく、ユニコーン企業は皆無。

図23.スタートアップ企業数の国際比較(2023年)



※Tracxn社が集計した2023年に活動しているサイバーセキュリティ関連スタートアップ（会社設立期間が浅く、投資会社から投資を受けている企業等）数

図24.ユニコーン企業数の国際比較(2023年)



※CB Insightsが集計した2023年に活動しているサイバーセキュリティ関連ユニコーン企業（設立10年以内に企業価値が10億ドルに達した企業）数

参照:スタートアップ企業はTracxnのデータ、ユニコーン企業はCB insights" $1B+ Market Map: The world's 1,206 unicorn companies in one infographic"をもとに作成。
https://tracxn.com/d/explore/cybersecurity-startups-in-united-kingdom/_T_FlgtyiuBPRBCJB75ZXjovLQNo_LZbZQzOu1uLQRAk/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-united-states/__5VqYm8uaMl7Y7dmnWoVR_d4Iy3pZuX89LbxW9_tVZ0/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-japan/_hLs5nyrwfOItFMKpZ0yMXOx6WD_gkiu83NuEMkqZt5k/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-south-korea/_w00W5vuYwJwk-bQMwhVm9zwsmnw5Oi1L-R-1n9om458/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-china/_xI9CmkOhhUG-i-ScX4J_FYwnAh73_AJnpNryzIlNU0w/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-canada/_vLEIL9vvyxnfshuSHSj193yArV722U9bl_3OsVSI4hg/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-france/_w00W5vuYwJwk-bQMwhVm9wMWKrnFq8xUwqvOo7eU9_E/companies,
https://tracxn.com/d/explore/cybersecurity-startups-in-israel/_nVk8uu-tzSMdn3JVqQoJdN-5Dap2GafQd8ItUmAzF_M/companies,
https://www.cbinsights.com/research/report/unicorn-startups-valuations-headcount-investors/

- 他国企業と比較すると、日本企業の売り上げに占める研究開発費の額は少ない傾向にあると考えられる

各国のサイバー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	269	0.32
米国B社	エンドポイントセキュリティ等	790	0.29
イスラエルC社	エンドポイントセキュリティ等	455	0.17
日本D社	エンドポイントセキュリティ等	54	0.02
日本E社	脅威検知等	2.6	0.006
日本F社	エンドポイントセキュリティ等	0.2	0.002

※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130円換算で計算。

参照:EDINET、各社情報等より作成

3.4.4　人材面の課題

3.4.4 人材面の課題 ― 主要国におけるサイバーセキュリティ人数と不足

ビジョン原案

- 我が国ではサイバーセキュリティ人材が不足。2023年時点で約11万人が不足していると試算。人口1万人当たりのサイバーセキュリティ人材は、主要国と比較しても不足している。

図25.主要国におけるサイバーセキュリティ人材・不足数(※)の比較(2023年時点)

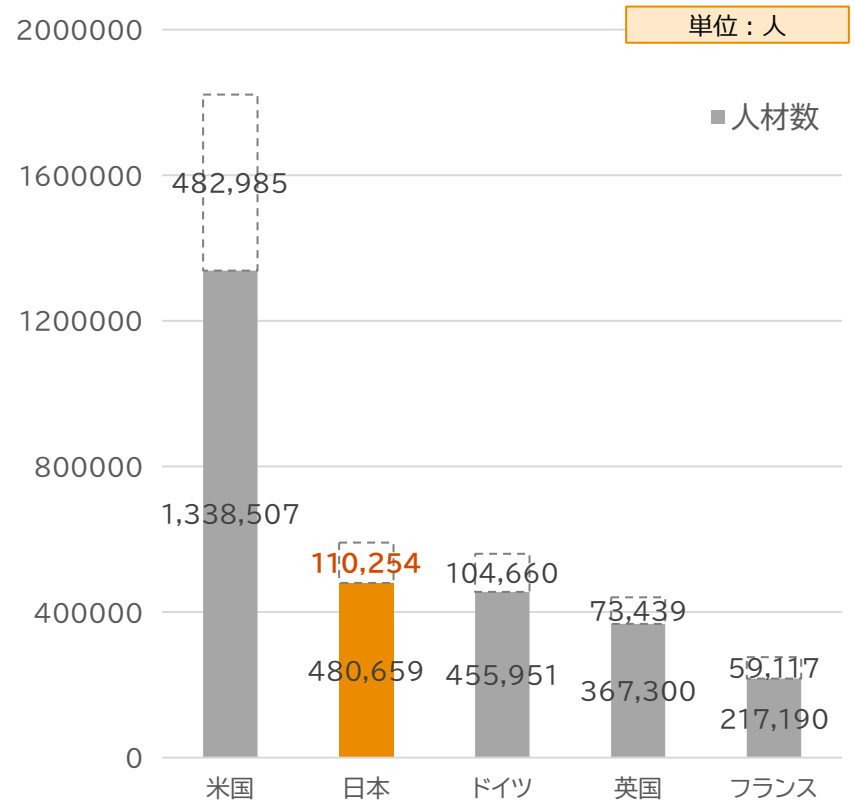
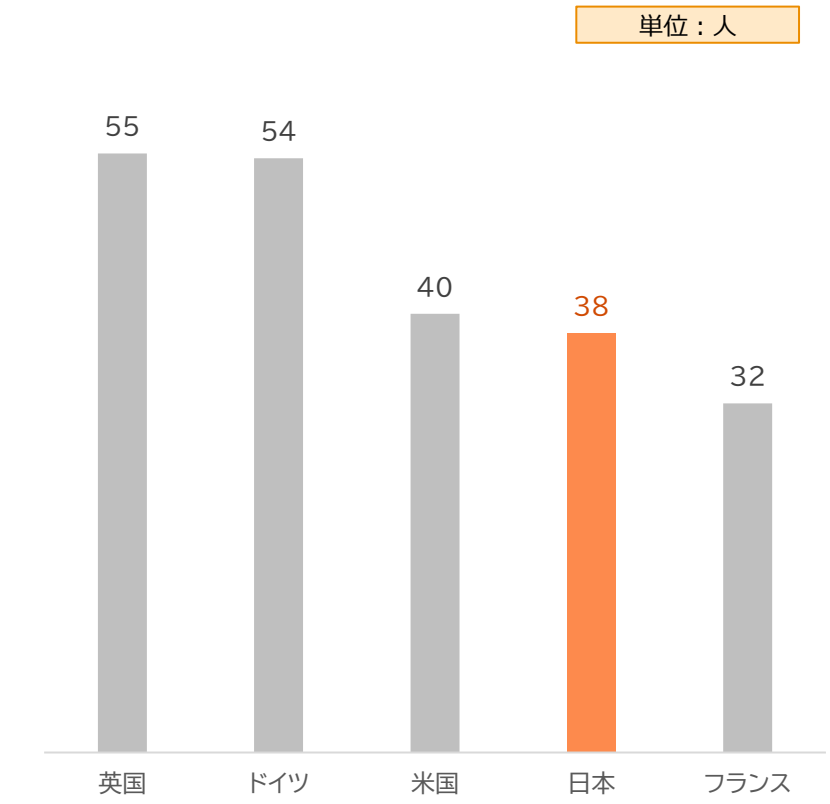


図26.人口1万人当たりのサイバーセキュリティ人材数(2023年時点)



- 米国のサイバーセキュリティ資格認証団体（ISC）２がアンケートの集計やマクロ指標から推計した世界各国の企業（ベンダーだけではなく、一般企業含む）で勤務するサイバーセキュリティ人材数及び企業からの人材需要に対する人材数とのギャップ（不足数）。

参照:(ISC)2"Cyber Workforce Study 2023"をもとに作成。
https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e&_gl=1*1i7ko1y*_ga*MzM5Mzk4NjM0LjE3MTEwODM3NzY.*_ga_7V1PGHSZT0*MTcxMTA4Mzc3NS4xLjAuMTcxMTA4Mzc3NS42MC4wLjkwMDg2NjI2Nw..

3.4.5　サイバーセキュリティ産業の構造

- グローバル企業では、2000年以降に創設された新興企業も市場で活躍している一方、日本企業の場合、情報通信系の大手か、2000年までに創設された社歴の比較的長い専門系企業のみが活躍。新興の日本企業が市場で活躍できていない/育ってきていない状況。

日本企業のサイバーセキュリティ製品主要20社

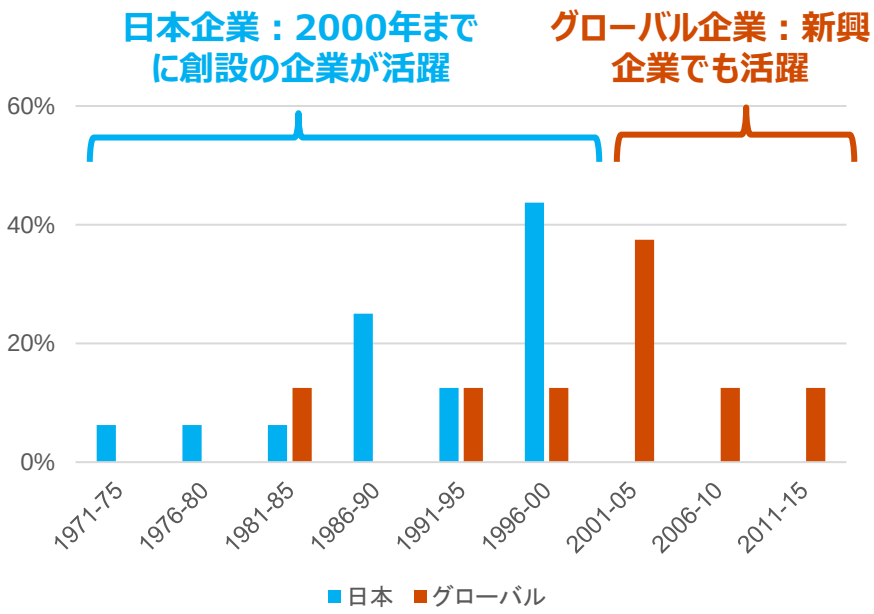
売上が大きい主要企業は、情報通信系の大企業か、2000年までに創設の専門系企業。なお、海外製品販売注力の企業も目立つ。

	企業名（日本企業）	創設年
大手系（情報通信大手企業の１部門/子会社）	NEC	1899
	日立製作所	1910
	富士通	1935
	NTTテクノクロス	1985
専門系（製品事業が主力事業）	サン電子	1971
	ソリトンシステムズ	1979
	インテリジェントウェイブ（※海外製品販売注力）	1984
	ラック（※海外製品販売注力）	1986
	ビービーシステムズ	1988
	トレンドマイクロ	1989
	アルプスシステムインテグレーション（※海外製品販売注力）	1990
	GMOグローバルサインHD	1993
	デジタルアーツ	1995
	網屋	1996
	HENNGE	1996
	アズジェント（※海外製品販売注力）	1997
	イーガーディアン	1998
	オプティム	2000
	グローバルセキュリティエキスパート（※海外製品販売注力）	2000
	サイバートラスト（※海外製品販売注力）	2000

※日本に本社がある企業のうち、セキュリティ製品の売上（グローバル）が上位20社に入ると推計される企業。順番は創設年が古い順。

図27.専門系主要日本企業/グローバル企業の創設年比較

左記の専門系売上の大きい主要日本企業16社と、海外に本社のある売上主要専門系グローバル企業8社（※）について、各年代で創設された割合を分析し、比較。



※ Canalys発表の2022年Q4グローバル市場売上上位企業のうち、専門系のPalo Alto、Fortinet、Check Point Software、Crowd Strike、Okta、Trelix、Symantec、Splunk。他の上位企業はIBM、Microsoft、Trend Micro。

参照：日本企業の主要企業については、PwC推計。グローバル企業については
Canalys" Strong channel sales propel the cybersecurity market to US$20 billion in Q4 2022"をもとに作成。
https://www.canalys.com/newsroom/cybersecurity-market-2022

3.4.5 サイバーセキュリティ産業の構造 ― SIer依存のビジネスモデル

ビジョン原案

- 日本におけるサイバーセキュリティのビジネスモデルは、システムインテグレーター（SIer）が関連するセキュリティ企業を統括しながら、導入するソリューションについて需要側と決めていく方式が一般的。
- 一方、需要側の企業ではIT人材が不足しており、必然的にセキュリティ対策（システムの導入も含め）についてSIer依存になる。

図28.日本でのサイバーセキュリティにおけるビジネスモデル

➢ セキュリティ製品のユーザー企業と各種セキュリティ製品・サービス企業との窓口をSIer企業が担う構造となっている。

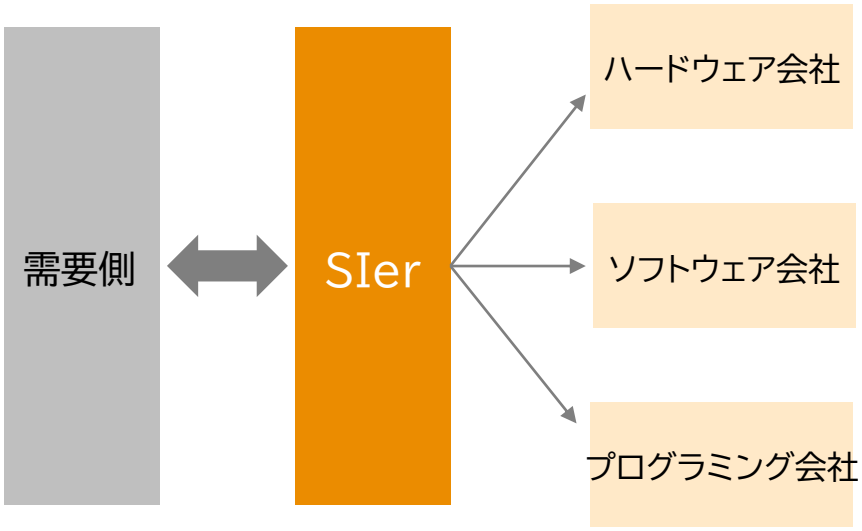
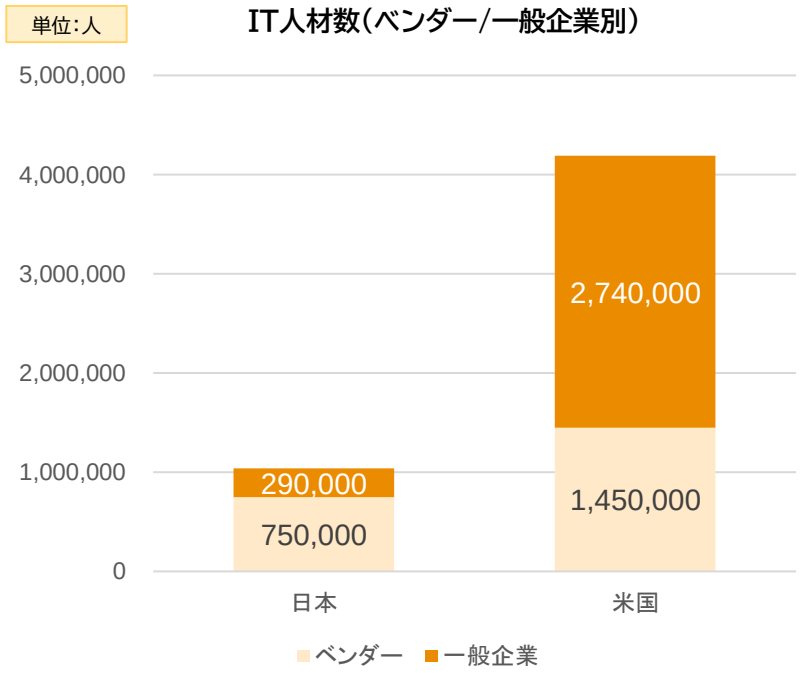


図29.SIer依存を招きやすい日本の人材の偏在

➢ 人材面では、米国と比較して、IT人材がベンダー側に偏っており、一般企業の人材が不足。必然的に知見の面でベンダー頼りとなる。



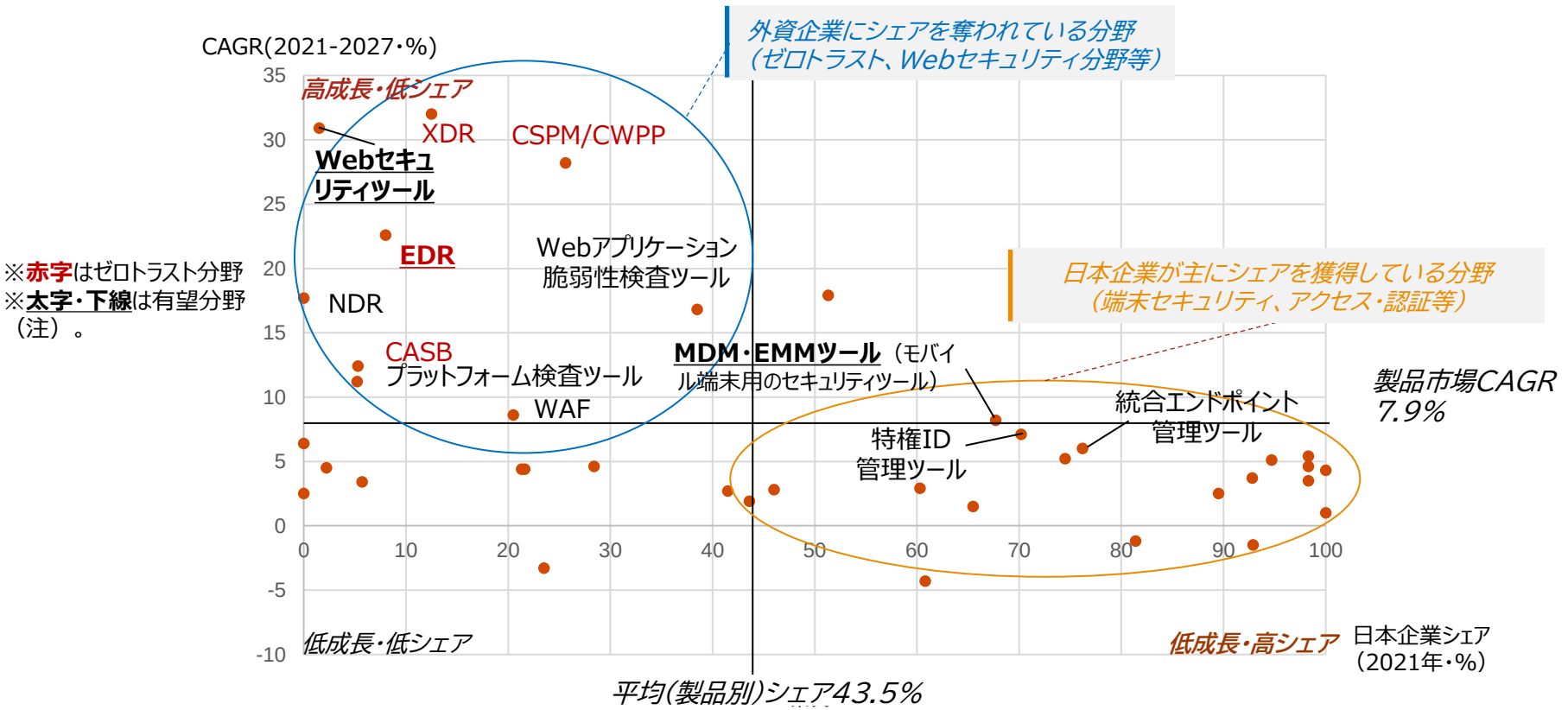
参照:IT人材数については、UB Ventures” System Integrators – the Key to Success for SaaS in Japan”をもとに作成。
https://ubv.vc/contents/trends/system-integrators/

3.4.5 サイバーセキュリティ産業の構造 ― 製品分野別の成長率と日本企業のシェア

ビジョン原案

- 最新のゼロトラスト分野やWebセキュリティ分野等企業から需要のある分野は高い成長が見込まれるものの、市場規模が大きく、成長率が製品市場全体よりも高い有望分野(注)も含め、その多くで外資企業にシェアを奪われている。一方、従来型の端末セキュリティやアクセス認証分野等、日本企業がシェアを獲得している分野は、比較的成長率が高くない分野が多い。

図30.製品分野別の年平均成長率及び日本企業のシェア



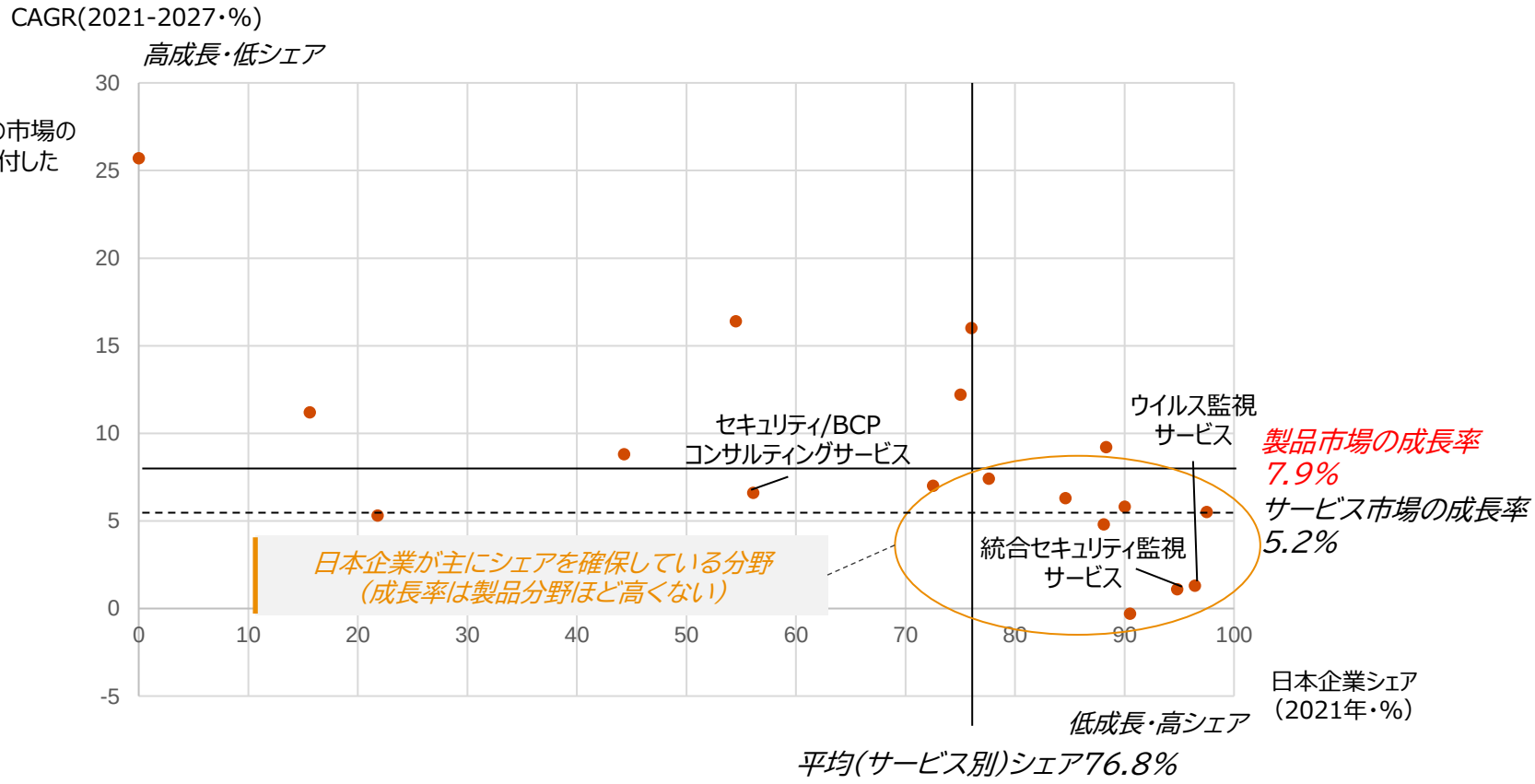
注：有望分野とは、具体的に、2021年時点で分野別平均以上の市場規模100億円以上でかつ、製品市場全体の年平均成長率7.9%以上分野

参照：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」)をもとに作成。
https://www.meti.go.jp/meti_lib/report/2022FY/000523.pdf

- なお、サイバーセキュリティのサービス分野においては、日本企業のシェア率が高い分野が一定数あるものの、外資企業にシェアを奪われている製品市場よりも成長率が高い分野は限定的。

図31.サービス別の年平均成長率及び市場規模

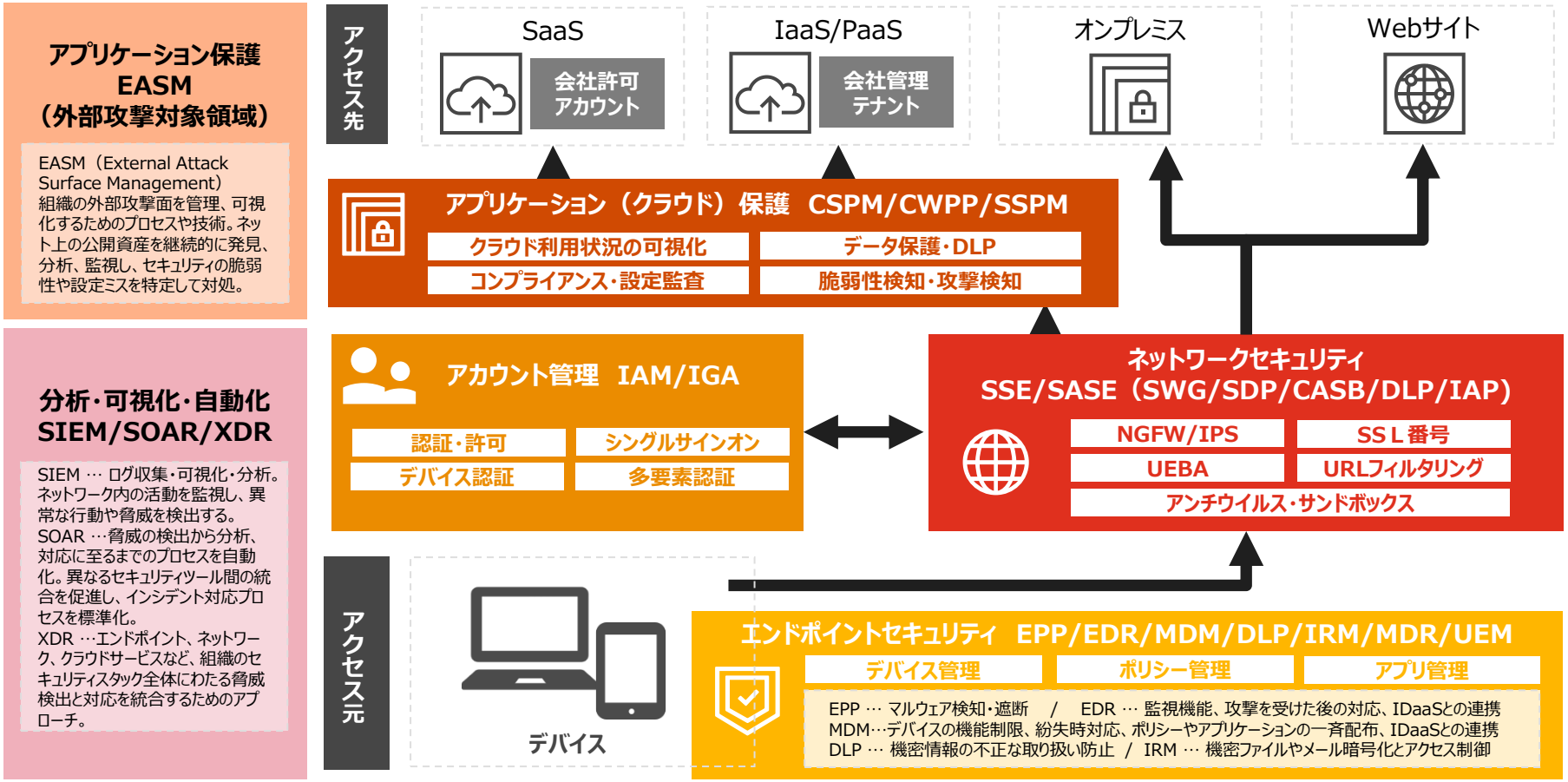
※200億円以上の市場の分野は分野名を付した



参照: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」)をもとに作成。
https://www.meti.go.jp/meti_lib/report/2022FY/000523.pdf

- ゼロトラストは、ネットワークセキュリティのモデルであり、組織が信頼できると見なす内部ネットワーク内でも、すべてのユーザーとデバイスを潜在的な脅威として扱うという考え方に基づいている。このモデルは、「信頼しない、常に検証する」という原則に従い、アクセス制御とネットワークセキュリティの強化を目指すもの。

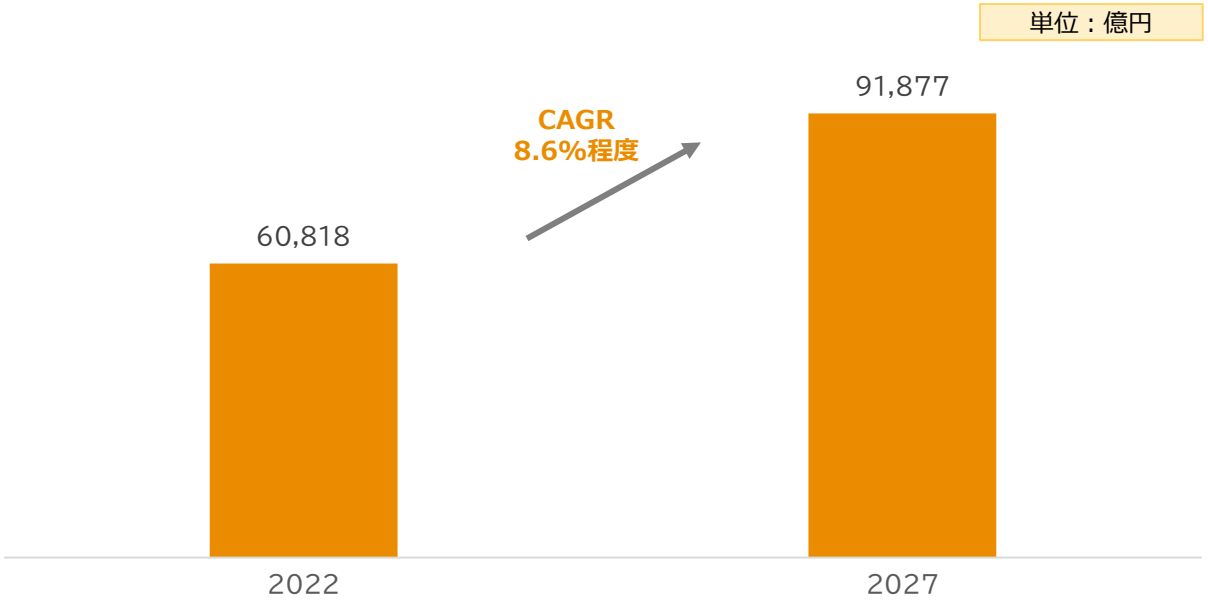
図32.ゼロトラスト分野のソリューションマップ



参照：日立ソリューションズ「ゼロトラストセキュリティソリューション」をもとに作成。
https://www.hitachi-solutions.co.jp/security/sp/solution/task/zerotrust.html

- 国内IoT市場(※)は拡大、OTセキュリティ(生産ラインやシステムの制御・運用に関するサイバーセキュリティ)市場も拡大していくと予測。今後の施策については、OTセキュリティ分野における需要の拡大と、我が国サイバーセキュリティ産業によるその取り込みに留意する必要あり。

図33.国内IoT市場(※)の推移



※IoT市場とは、国内IoT（Internet of Things）におけるユーザー支出の総額。

参照:IoT市場の推移については、IDC発表「国内IoT市場は物流や医療の分野で需要が高まる ～ 国内IoT市場 産業分野別テクノロジー別予測アップデートを発表 ～」をもとに作成。
https://www.idc.com/getdoc.jsp?containerId=prJPJ51346323

- デジタル化が進む昨今、サイバー攻撃は企業活動の根幹を成すOT（Operational Technology：生産ラインやシステムの制御・運用技術）環境にも及ぶ。企業の存在意義すらも脅かすOTセキュリティインシデントおよびその発生を防止するOTセキュリティは、重要な経営課題。なお、OT環境はFA環境（物理的な組み立て・加工等を行うプロセスを自動化するもの）、PA環境（化学的な合成・精製等を行うプロセスを自動化するものをはじめ、産業制御システム（ICS）を使用した多様なサービスシステムが存在、それぞれ異なる性質を持つ。

OT環境の類型整理　FA環境とPA環境の特徴と主な違い

カテゴリ	指標	【参照】 OA環境 Office Automation 情報機器を用いた定型的な事務作業の自動化・効率化	FA環境 Factory Automation 物理的な組み立て・加工等を行うプロセスを自動化するもの	PA環境 Process Automation 化学的な合成・精製等を行うプロセスを自動化するもの
機能や実情	構成変更の容易性	容易	比較的容易	困難
	要求される出力品質制度	低 （ベストエフォート）	高	中
	規格	TCP/IP	TCP/IP ＆ 固有プロトコル	TCP/IP ＆ 固有プロトコル
	運用体制	IT部門で全社的に一元管理	製造部門ごとに細かく分散	運用ベンダにて一定程度一元化
セキュリティ	守るべき対象	情報資産	プロセス ＆ プロセスを担う設備	プロセス ＆ プロセスを担う設備
	最優先されるセキュリティ要素	機密性	可用性	完全性
	セキュリティ侵害時の影響	データの損失	環境・安全・製品・設備の侵害	環境・安全・製品・設備の侵害

- 一般に、OT環境である工場や研究所では産業制御システム（ICS: Industrial Control System）が使用されていることから、OTのサイバーセキュリティは従来の情報セキュリティやITセキュリティとは別の取り組みとして考えられることが多い。
- これまではTCP／IP（Transmission Control Protocol ／Internet Protocol）の脆弱性を利用した情報システムへのサイバー攻撃が主流であったこと、情報管理やIT環境の所管部門とOT環境の所管部門が異なる企業が主流であることが、その主な理由。

※ 他にもBA環境、送電網、通信網などの多種多様なサービスシステムがあるがここでは扱わない。

参照:PwCインサイト「工場（OT）環境の類型整理とOTセキュリティ」
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/digitizing-factory-cyber-security01.html

4　目指すべき姿

4.1 サイバーセキュリティ産業の意義の整理

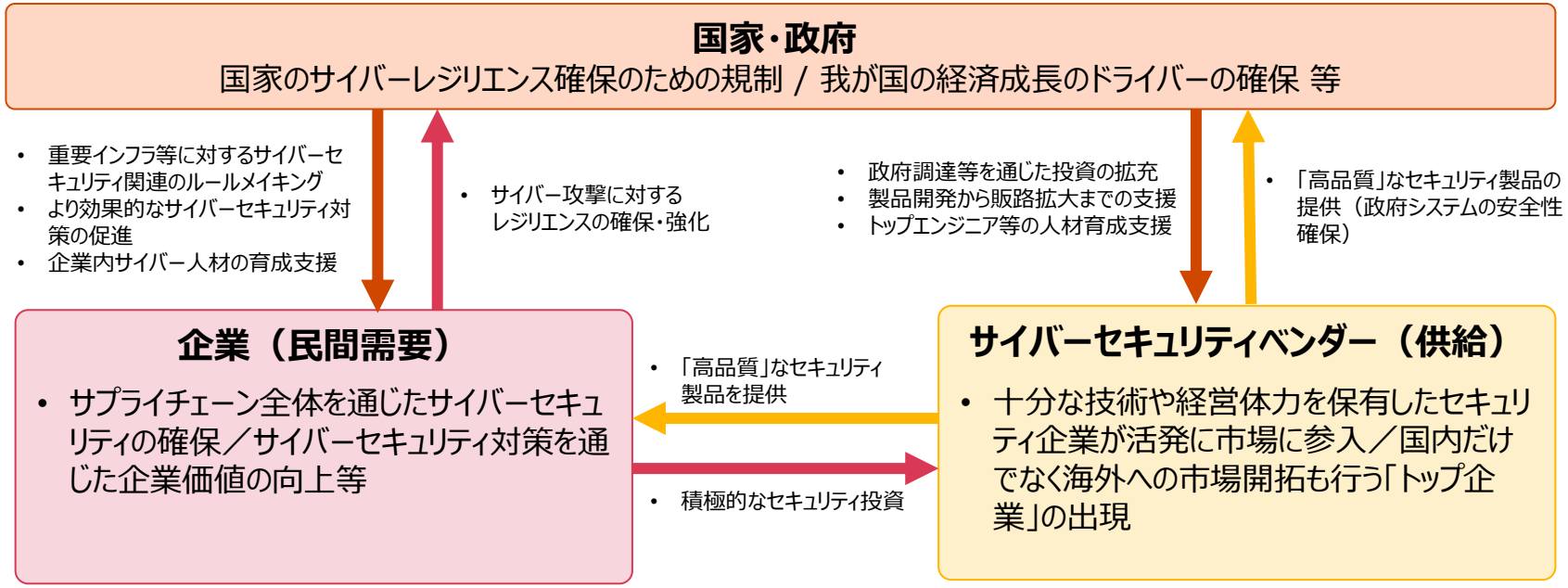
- 社会におけるデジタル化が加速する中、① 我が国の経済成長への貢献（経済政策）、② デジタル社会及び多様な人材が活躍する社会の実現（社会政策）、③ 安全保障の強化と技術力の向上（経済安全保障政策）、といった各政策面でサイバーセキュリティ産業の意義が存在。

我が国サイバーセキュリティ産業活性化の3つの意義

	1 経済成長への貢献（経済政策）	2 デジタル社会や多様な人材が活躍する社会の実現（社会政策）	3 安全保障の強化と技術力の向上（経済安全保障政策）
国家としての課題	• GDPが毎年1～2%で成長すると予想されている中で、年6%程度の成長する国内サイバーセキュリティ市場は有望な市場。また、グローバルにおいてもサイバーセキュリティ市場は大きな成長を遂げる。市場成長の成果を日本企業が取り込み、我が国の経済成長に貢献する必要。 • また、サプライチェーン全体でサイバーセキュリティを強化することで、製造業等、我が国の基幹的な産業が安定的に操業を行い、利益を生み出す環境を整備する必要があり、これを保障する産業基盤が必要。	• 教育、医療、街づくり、子育て支援等の諸課題を解決するため、デジタル社会を推進する必要がある一方で、その進展に伴い、サイバーセキュリティのリスクが高まる。 • したがって、安心・安全なデジタル社会の実現にサイバーセクターで雇用される人材だけでなく、ユーザー企業・団体等で雇用されるサイバーセキュリティ人材の確保が不可欠。 • 国内の専門家は増加傾向にあり、女性割合も拡大している。背景に法令対応やガバナンスなど業務多様化による文系出身者の活躍領域拡大があげられる。人材確保に向け女性、文系出身専門家の増加は必要不可欠。	• 近年、サイバー攻撃による重要インフラの機能停止や破壊、機微情報の窃取等は、国家を背景とした形で平素から行われている。厳しい安全保障環境に直面する我が国は、その防衛のため、サイバー安全保障分野における対応能力の向上が必要となる。 • 特に、政府機関や、サイバー攻撃の標的となった際に、影響の大きい重要インフラ分野については、経済安全保障の観点から、ある程度の自律性を確保した上で、サイバーセキュリティに関する高度な技術を保持する必要がある。
意義	**産業活性化による競争力のある国内ベンダーの増勢により、サイバーセキュリティ市場の成長を取り込み、また、サプライチェーン全体のサイバーセキュリティ強化を実現することで、我が国の経済成長に貢献する。**	**産業活性化により、安心・安全なデジタル社会の基盤となるサイバーセキュリティ人材の確保につながる。**	**産業活性化により、我が国セキュリティベンダーの技術力が向上することで、一定程度の自律性を確保した上で、国や重要インフラ事業者のサイバーセキュリティが向上。**

- 米国など諸外国の事例を踏まえつつ、政府機関や企業、セキュリティベンダーがそれぞれの役割を果たすことで、「高品質」なセキュリティ製品が市場に供給されるとともに、それを受け止める需要先が存在し、資金循環も含めた三者のサイクルが循環される「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。

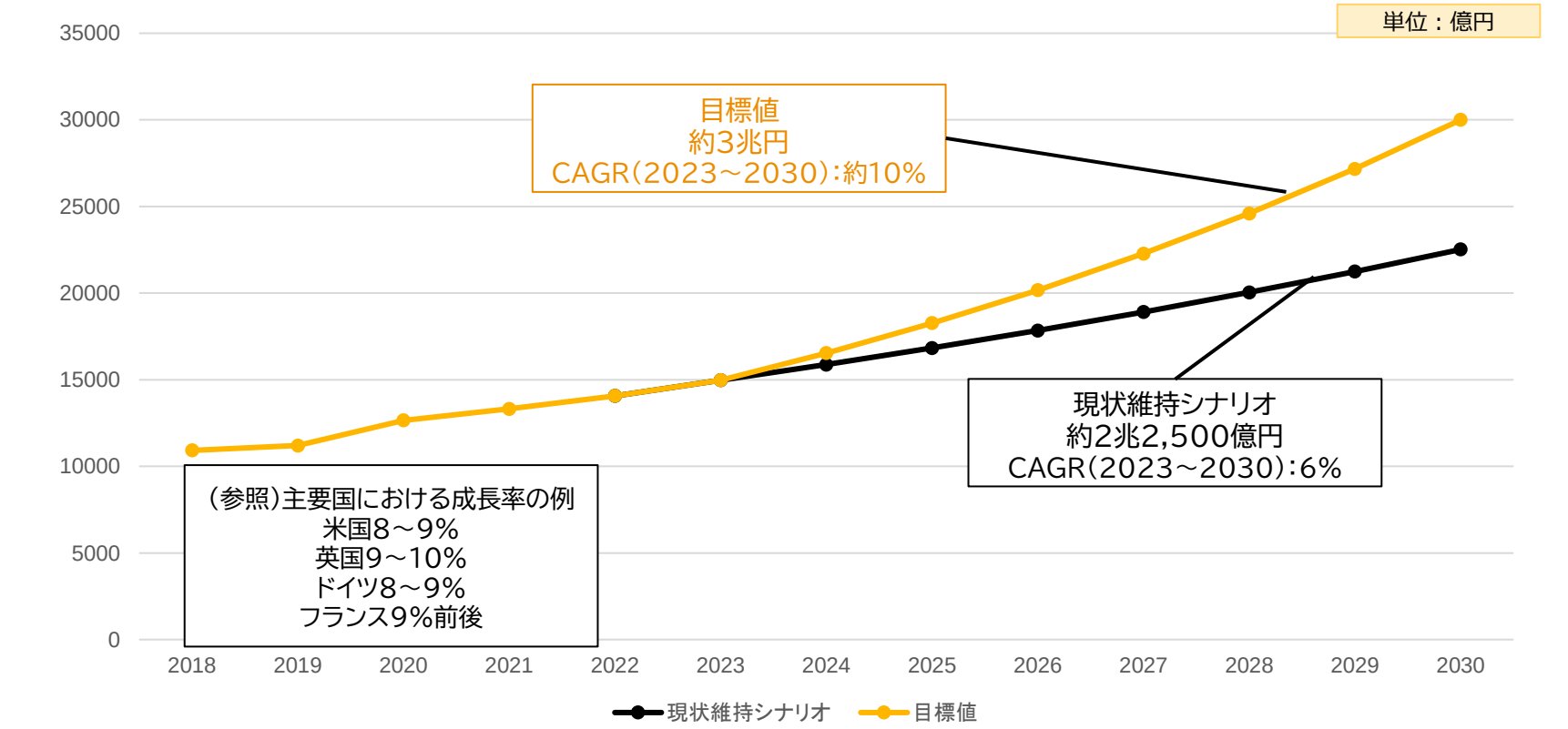
今後目指すべきセキュリティエコノミーサイクルのイメージ



○我が国でも、上記のような絵姿を目指し、サイバーセキュリティが、単に企業の負の投資として扱われるのではなく、
① デジタルエコノミーが進んでいく中で、政府・企業が必要なセキュリティを確保しており、
② セキュリティの積極投資が企業の価値の一つとして扱われ、
③ そうした土壌の中で、セキュリティを生業とした企業が活発に市場参入する
ことを包含した**「セキュリティエコノミー」の確立を目指す**。

- 近年、サイバーセキュリティ市場の伸びは6%程度であり、これを維持するとすると2030年に約2兆2,500億円となる。一方、他の主要国は、9～10%前後で今後もサイバーセキュリティ市場の成長を遂げていくとされている。我が国もこれに劣後しないよう、サイバーセキュリティの強化を図り、市場の活性化を促すことが求められる。
- これを踏まえて、市場規模として、2030年には、(現時点から)約2倍の約3兆円を目指す(年平均成長率約10%)。

図34.2030年におけるサイバーセキュリティ市場規模の目標値



5 今後の方向性

5.1 今後の対応の方向性（全体像）

ビジョン原案

- 社会全体のサイバーセキュリティの強化のため、サイバーセキュリティ市場を拡大するとともに、我が国サイバーセキュリティ産業の競争力の強化と、「質」と「量」の両面にわたる人材の確保を行う必要がある。

これまでの政策や取組上の論点を踏まえた対応の方向性

	これまでの政策	今後の取組上の論点	対応の方向性
市場創出（需要面の課題）	• 中小企業を含めた企業のサイバーセキュリティ対策を強化する観点から、ガイドライン等による普及啓発等の施策を講じてきている。	• どの程度まで対策をすべきか企業側にとっても不明確であり、企業がセキュリティ対策を行う上で満たすべきメルクマールの設定が必要。また、事前対策をすることへのインセンティブが必要。	• 我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための**我が国産業界に対するサイバーセキュリティ対策の強化の働きかけ**を行う。
産業競争力強化（供給面の課題）	• 技術開発支援（Kプロ）や製品の性能検証・実機検証（緑青検証・審査登録制度）、CYNEXによる製品開発推進等を実施し、技術力の底上げを図ってきた。	• 有望な技術や製品を持つ企業に対して集中的に支援を行う方が、効果が発揮される可能性。	• 優れたサイバーセキュリティ製品の**開発の促進**により、我が国発のセキュリティ製品供給能力の向上を図る。 • ニーズを見通しづらく製品開発に至らない／これまで活用されていない製品なので活用されないという**「負のスパイラル」の解消**を図る。
	• また、スタートアップの増勢を図る観点から、融資制度・伴走型支援制度、規制のサンドボックス／グレーゾーン解消制度、海外進出支援等の支援を実施。	• 実際に活用されている実例がないと、実導入まで結びつかず、対策が必要。	
人材面の課題解決	• 一般企業とベンダー側を支えるサイバーセキュリティ人材の確保の観点から、セキュリティキャンプ、中核人材育成、登録セキスペ制度の創設、CYNEXによる人材育成等を実施。	• 一方、既存施策では、トップガンや高度人材を育成できる量が限られている。また、中間層にアプローチできておらず、ユーザー企業で必要とされる人材も足りず、これらへの対策が必要。	• 高度人材から中間層向けを対象に、**需要・供給両方の人材育成**を行う。

5. 2 今後の対応の方向性①（市場創出）

ビジョン原案

- 我が国企業のサイバーセキュリティ対策を強化し、市場の創出を図る。そのため、我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための我が国産業界に対するサイバーセキュリティ対策の強化の働きかけを行う。

主要な対策

対応の方向性

- 我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための**我が国産業界に対するサイバーセキュリティ対策の強化の働きかけ**を行う。
- ニーズを見通しづらく製品開発に至らない/これまで活用されていない製品なので活用されないという**「負のスパイラル」の解消**を図る。

1 セキュリティ対策水準の明確化・可視化

これまで

【サイバーセキュリティ課施策】
- 経営者がセキュリティ対策の上で果たすべき役割等を示した「サイバーセキュリティ経営ガイドライン」は策定済。

【他省庁等施策】
- 中小企業、NPO向けのサイバーセキュリティ対策について記載したハンドブックを策定・改正を実施。【内閣官房】

考えられうる今後の施策
- 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対策のメルクマールや、対策状況を可視化する仕組みを構築。
- なお、中小企業、NPO向けハンドブックの改正時の連携可能性あり（企業向けのセキュリティ対策水準の明確化についても記載等）。

2 資本市場や業界関係者との対話促進

これまで

【サイバーセキュリティ課施策】
- これまで特段の施策なし

【他省庁等施策】
- 上場企業のセキュリティ対策格付け・公表をIT連が実施済。【IT連】

考えられうる今後の施策
- 開示の具体的なあり方について、議論・検討を行う場を立ち上げつつ、企業と投資家との対話においてサイバーセキュリティが考慮要素として活用される状況を目指す。

※新規・既存施策の拡充が必要な個所を赤字

5. 2 今後の対応の方向性①（市場創出）

ビジョン原案

- 我が国企業のサイバーセキュリティ対策を強化し、市場の創出を図る。そのため、我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための我が国産業界に対するサイバーセキュリティ対策の強化の働きかけを行う。

主要な対策

対応の方向性

- 我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための**我が国産業界に対するサイバーセキュリティ対策の強化の働きかけ**を行う。
- ニーズを見通しづらく製品開発に至らない/これまで活用されていない製品なので活用されないという**「負のスパイラル」の解消**を図る。

3 政府機関とスタートアップ企業のマッチング

これまで

【サイバーセキュリティ課施策】
- これまで特段の施策なし

【他省庁等施策】
- 政府が企業を比較・検討を行えるHPを構築。【デジタル庁】
- 防衛産業のスタートアップ活用に向けた合同推進会を実施。【防衛装備庁・経済産業省】

考えられうる今後の施策

- 既存の枠組みを活用することも検討しつつ、スタートアップと政府機関のニーズのマッチングさせる環境を整備する。

4 中堅・中小企業のセキュリティ対策の促進

これまで

【サイバーセキュリティ課施策】
- 安価なサイバーセキュリティ対策をパッケージした「お助け隊」などのサービスの提供。

【他省庁等施策】
- 財政支援策という観点では、これまで中小企業対策向けの補助金制度等あり。

考えられうる今後の施策

- 中堅企業や中小企業によるセキュリティ対策をさらに促進すべく、支援機関を通じた支援を進める。

※新規・既存施策の拡充が必要な個所を赤字

5. 2 今後の対応の方向性①（市場創出）

ビジョン原案

- 我が国企業のサイバーセキュリティ対策を強化し、市場の創出を図る。そのため、我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための我が国産業界に対するサイバーセキュリティ対策の強化の働きかけを行う。

主要な対策

対応の方向性

- 我が国企業によるサイバーセキュリティ分野への投資促進と関連市場の拡大を図るための**我が国産業界に対するサイバーセキュリティ対策の強化の働きかけ**を行う。
- ニーズを見通しづらく製品開発に至らない/これまで活用されていない製品なので活用されないという**「負のスパイラル」の解消**を図る。

5　セキュリティ対策を拡充する際の財政支援

これまで

【サイバーセキュリティ課施策】
- これまで特段の施策なし

【他省庁等施策】
- 財政支援策という観点では、これまで中小企業対策向けの補助金制度等あり。現在税制上の特例措置は特段なし。

考えられうる今後の施策

- 既存の枠組みを活用しながら、企業が必要なサイバーセキュリティ対策を行う際に、税制優遇等の措置を行う。

※新規・既存施策の拡充が必要な個所を赤字

5. 3 今後の対応の方向性②（産業競争力強化）

ビジョン原案

- 我が国サイバーセキュリティ産業の競争力強化を図るため、優れたサイバーセキュリティ製品の開発の促進により、我が国発のセキュリティ製品供給能力の向上を図る。また、ニーズを見通しづらく製品開発に至らない／これまで活用されていない製品なので活用されないという「負のスパイラル」の解消を図る。

主要な対策

対応の方向性

- 優れたサイバーセキュリティ製品の**開発の促進**により、我が国初のセキュリティ製品供給能力の向上を図る。

1 有望なセキュリティ企業の選定と集中的支援

これまで

【サイバーセキュリティ課施策】
- 国産製品のマーケットイン促進のため、IPAと製品の質を検証する基盤を構築。

【他省庁等施策】
- Kプログラム【内閣府】
- CYNEXでは国産セキュリティ製品の性能検証等の研究開発支援実施【NICT】
- その他第3期戦略的イノベーション創造プログラム（SIP）あり

考えられうる今後の施策
- 有望なセキュリティ製品・サービスを供給するポテンシャルを持つ企業を選定し、これらの企業に対して、製品から販路開拓までを含めて、一貫した支援を集中的に行う「枠組み」を構築することを目指す。
- なお、既存の枠組みの活用も可能。

2 事業者の責務明確化

これまで

【サイバーセキュリティ課施策】
- 提供するサービスが基準以上である事業者を示す「情報セキュリティサービス審査登録制度」は創設済。（SIerは未着手）。

【他省庁等施策】
- 特段の関連施策なし。

考えられうる今後の施策
- セキュアバイデザインの中で、事業者に対する責務の明確化が求められていること、国内企業もSIerの影響を受ける要素が大きいことから、サイバーインフラ事業者に求められる責務をガイドライン等を通じて具体化するとともに、基準を満たす企業の可視化する枠組みを構築を目指す。

※新規・既存施策の拡充が必要な個所を赤字

5. 3 今後の対応の方向性②（産業競争力強化）

ビジョン原案

- 我が国サイバーセキュリティ産業の競争力強化を図るため、優れたサイバーセキュリティ製品の開発の促進により、我が国発のセキュリティ製品供給能力の向上を図る。また、ニーズを見通しづらく製品開発に至らない／これまで活用されていない製品なので活用されないという「負のスパイラル」の解消を図る。

主要な対策

対応の方向性

- 優れたサイバーセキュリティ製品の**開発の促進**により、我が国初のセキュリティ製品供給能力の向上を図る。

3 IoT製品の評価制度の構築

これまで

【サイバーセキュリティ課施策】
- 特段の施策なしだが、現在検討中。

【他省庁等施策】
- 特段の施策なし。

考えられうる今後の施策

- IoT製品について、セキュリティ機能を評価・可視化し、調達者が求めるセキュリティ水準のIoT製品を容易に選定できる制度を構築。
- 今後、制度運営を一部開始するとともに、より高度なセキュリティ基準については、設定すべき製品類型の特定や基準設計を図る。

※新規・既存施策の拡充が必要な個所を赤字

5.4 今後の対応の方向性③（人材育成強化）

ビジョン原案

- 企業側のサイバーセキュリティ対策強化や、サイバーセキュリティ産業側の競争力強化を下支えするサイバーセキュリティ人材の確保を目指し、高度人材から中間層向けを対象に、需要・供給両方の人材育成を行う。

主要な対策

対応の方向性

- 高度人材から中間層向けを対象に、**需要・供給両方の人材育成**を行う。

1 トップガンの発掘・育成

これまで

【サイバーセキュリティ課施策】
- 次世代を担う高度なサイバーセキュリティ人材を発掘・育成するセキュリティキャンプを全国・地方で実施。

【他省庁等施策】
- 大学における社会人の学びなおしとしてサイバーセキュリティ人材を育成（「enPiT Pro Security」）【文部科学省】
- 若手のセキュリティイノベーター育成を実施（「SecHack365」）【NICT】

考えられうる今後の施策

- トップガンの更なる育成に向けて、募集を拡大するなど、セキュリティキャンプの拡張を実施。
- また、デジタル人材育成のための他施策との連携を実施。この際、他省庁等実施の既存の人材育成プログラムの拡充等にかかる連携も可能。

2 ユーザー企業における登録セキスペの活用促進

これまで

【サイバーセキュリティ課施策】
- 情報処理安全確保支援士（登録セキスペ）の制度創設。また、当該制度のユーザー企業向けプロモーションも実施。

【他省庁等施策】
- 企業価値を高めるためのDXを要件としたDX投資促進税制を措置済（ただし、セキュリティ人材に関する要件なし）【経済産業省】

考えられうる今後の施策

- ユーザー企業において、こうした人材をさらに活用できるよう、中小企業等とのマッチング実証事業や、既存施策との連動等／企業が各種支援を受ける際の要件として、登録セキュスペの活用を位置づける。
  - ➢ また、登録セキュスペの資格を有する人材を増やし、セキュリティ人材の増勢につなげるべく、重要インフラ・基幹インフラ事業者への登録セキュスペの必置化やコスト低減等を目指す。

※新規・既存施策の拡充が必要な個所を赤字

免責事項

- 私どもは本件関与者以外の第三者や本報告書の目的以外の利用に対して裁判上、裁判外及びそれらに限らない如何なる義務や責任を負いません。
- 私どもは、本報告書の日付後に発生した事象について、追加で報告をなし又は本報告書に反映させる責任を負いません。また、本報告書で記載している過去または現在の事実以外の内容については、本稿執筆時点で入手可能な情報に基づいた見通しであり、実際の動向等は種々の不確定要因によって変動する可能性があります。私どもは、当該結果等の達成可能性に対して何ら責任を負いません。
- 本報告書で取り上げる個別事例については、現状を分析する目的で選定したものであり、これを推奨するものではありません。
- 本報告書は調査委託を受けたPwCコンサルティング合同会社の責任の下で作成されており、本報告書に記載されている国内外の法令の適用関係に係る見解は、調査実施者たるPwCコンサルティング合同会社の見解に過ぎず、関係当局の確認を得たものではありません。

Thank you

www.pwc.com/jp

（様式２）

二次利用未承諾リスト

報告書の題名　令和5年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

委託事業名　令和5年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）

受注事業者名　PwCコンサルティング合同会社

頁	図表番号	タイトル
129	7	FBIへのサイバー犯罪の届出数
129	8	FBIへ届け出られたサイバー犯罪被害額総額
131	11	日本のサイバーセキュリティインシデント報告数
132	12	国内サイバーセキュリティ市場規模の推移
138	15	日米中央政府セキュリティ予算（2023年度）比較
138	16	市場規模に対する日米中央政府セキュリティ予算比（2023年度）
139	17	スタートアップ企業に関する現況
139	18	国別資金調達シェア（%）
146	19	国内サイバーセキュリティ市場規模の推移
149	20	サプライチェーン上の他社の対策を把握している日本企業の割合（%）（2023年）
150	21	中小企業におけるサイバーセキュリティ対策の現状
152	22	国内サイバーセキュリティ製品市場のシェア（2020年）
153	23	スタートアップ企業数の国際比較（2023年）
153	24	ユニコーン企業数の国際比較（2023年）
156	25	主要国におけるサイバーセキュリティ人材・不足数（※）の比較(2023年時点)
156	26	人口１万人当たりのサイバーセキュリティ人材数(2023年時点)
158	27	専門系主要日本企業/グローバル企業の創設年比較
159	29	SIer依存を招きやすい日本の人材の偏在
160	30	製品分野別の年平均成長率及び日本企業のシェア
161	31	サービス別の年平均成長率及び市場規模
162	32	ゼロトラスト分野のソリューションマップ
163	33	国内IoT市場の推移