経済産業省

資料７－４

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和６年６月７日

経済産業省

１．第8回産業サイバーセキュリティ研究会

２．「電力システムにおけるサイバーセキュリティリスク点検ガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を電気事業者向けに公表

産業サイバーセキュリティ研究会について

- **大所高所から**これまでの施策の進捗や**今後のサイバーセキュリティに関する政策の方向性を議論**するための場として、経済産業省が2017年12月に設置。
- 経済産業省のサイバーセキュリティ政策を決める年に１回を目処に開催する重要な研究会であり、**基本的に、経済産業大臣が毎回出席**。**今年度は4月5日（金）9時～11時で開催（上月副大臣御出席予定）**。

設置趣旨

- サイバー攻撃の起点が急激に拡大し、攻撃手法も高度化していることから、サプライチェーン全体、産業界全体の取組として、サイバーセキュリティ対策を強化する必要。
- 国内外問わずサイバーセキュリティに関する課題が多岐に及ぶ中、**産業界が直面する課題を洗い出し、関連政策を推進**していくため、**経営者**、**学識者**から構成される「産業サイバーセキュリティ研究会」を設置。
- 本会議で示された**政策の方向性を踏まえ**、関係省庁と連携して政策の具体化を進める。

運営要領

- 本研究会は原則非公開。
- 会議終了後、議事要旨を速やかに公開。
- 配付資料は原則公開するが、個別の事情に応じて、会議又は資料を非公開とするかどうかについての判断は、事務局と座長で相談の上決定。

委員（敬称略）

村井　純	（慶應義塾大学教授）※座長
泉澤　清次	（三菱重工業株式会社　取締役社長）
遠藤　信博	（日本経済団体連合会　副会長・サイバーセキュリティ委員長、日本電気株式会社特別顧問）
大林　剛郎	（日本情報システム・ユーザー協会会長、株式会社大林組取締役会長　兼 取締役会議長）
寺田　航平	（経済同友会副代表幹事、寺田倉庫株式会社代表取締役社長）
澤田　純	（日本電信電話株式会社　代表取締役会長）
東原　敏昭	（株式会社日立製作所　取締役会長 代表執行役）
船橋　洋一	（国際文化会館グローバル・カウンシル・チェアマン）
渡辺　佳英	（日本商工会議所特別顧問、大崎電気工業株式会社取締役会長）

オブザーバー

内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、デジタル庁、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

政府全体における経済産業省の今後の政策の位置付け

- 国家安全保障戦略（令和４年12月閣議決定）の趣旨を踏まえつつ、サイバーセキュリティ戦略（令和３年９月閣議決定）で掲げた３つの方向性に基づき、**政府全体でサイバー空間における必要な取組を推進**。
- 経済産業省では、**産業界に向けた施策を通じて**、政府機関等の防御強化等NISCをはじめとする関係省庁による取組と両輪となって、これらの戦略において掲げられている「**『自由、公正かつ安全なサイバー空間』の確保**」や「**サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる**」**目標に貢献**していく。
- **これまでの施策の一層の普及・啓発**などに取り組みながら、政府調達等への要件化を通じたサイバーセキュリティ対策の実効性強化など**新たな取組も進める**ことで、**産業界における対策水準の底上げ**につなげていく。

サイバーセキュリティ戦略（2021年９月閣議決定）（抄）

2.1.確保すべきサイバー空間

- **サイバー空間を「自由、公正かつ安全な空間」とすること**により、基本法に掲げた目的に資するべく、国は、（略）サイバーセキュリティ戦略を策定してきた。（略）その確保が危機に直面する中で、「自由、公正かつ安全なサイバー空間」を確保する必要性はこれまで以上に増しているとの認識が深められるべきである。

4. 目的達成のための施策 ～Cybersecurity for All～

- 不確実性を増す環境において「自由、公正、かつ安全なサイバー空間」を確保するため、以下の３つの方向性に基づき、施策を推進する。

(1) デジタル改革を踏まえた**デジタルトランスフォーメーションとサイバーセキュリティの同時推進**

(2) 公共空間化と相互連関・連鎖が進展する**サイバー空間全体を俯瞰した安全・安心の確保**

(3) **安全保障の観点からの取組強化**

国家安全保障戦略（令和４年12月閣議決定）（抄）

- サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、**サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる**。
- 具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、**外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防御の強化**、**政府内外の人材の育成・活用の促進等を引き続き図る**。

貢献

経済産業省における今後の政策の方向性

官民の状況把握力・対処能力向上

✓ 対応支援能力強化の観点からIPAをハブとした**サイバー情勢分析能力強化**

サイバーセキュリティ対策の実効性強化

✓ 各種ガイドライン・評価制度の**政府調達等の要件化**
→ 規模や業種等に応じて適切なセキュリティ対策レベルを評価し**可視化する仕組み**を検討
→ 一定のセキュリティ基準を満たす**IoT製品を認証する制度**や、ソフトウェア部品構成表（**SBOM**）について、政府調達等の要件化に向けて関係省庁と議論を開始

✓ **中小企業向け補助的施策の一層の強化**
→ セキュリティ人材の活用促進（マッチング実証事業）、お助け隊サービスの拡充　等

サイバーセキュリティ供給力の強化

✓ **産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環構築に向けた戦略の検討**
→ スタートアップ支援策等

✓ **高度人材の育成・確保**

第８回産業サイバーセキュリティ研究会（2024年4月5日）の開催概要①

AI等のデジタル技術の進展や近年の地政学リスクの高まり、米欧等における制度整備の動向等を踏まえた**新たなサイバーセキュリティ政策を打ち出す**とともに、民間の積極的な取組を慫慂すべく**産業界向けのメッセージを発出**する。**産業界が目指すべきサイバーセキュリティの方向性について、産業界を代表するメンバーに、大所高所から議論いただく。**

サイバーセキュリティを取り巻く現状

- ✓ 特定の国家を背景とした機微情報搾取、ランサムウェアによる広範囲な業務停止、重要インフラを標的する攻撃等の**深刻な事案も国内外で発生**。サイバー攻撃は**今後ますます高度化・複雑化**していくおそれ。
- ✓ 欧米を中心に重要インフラ事業者等における対策の強化に関する制度整備や“セキュア・バイ・デザイン”の概念に基づく、**セイバーセキュリティ対策を考慮した製品の開発・提供が問われる時代**に。

これまでの施策の主な進捗状況

NISCによる総合調整機能の下、経済産業省は、これまで**産業界に向けた取組を実施**し、政府全体として目指すべき**「自由、公正かつ安全なサイバー空間」の確保**（サイバーセキュリティ戦略2021）**に貢献**。

- ✓ **サプライチェーン全体での対策強化**
  - ・中小企業対策ツールの整備（「サイバーセキュリティお助け隊サービス」の価格要件を緩和した類型の拡充（本年３月公表））、経営者向け・産業分野別のガイドライン等の整備、IPA等を通じたセキュリティ人材の育成
- ✓ **国際連携を意識した認証・評価制度等の立上げ**
  - ・IoT製品のセキュリティ適合性評価制度の検討（本年３月方針公表、2024年度中に一部制度運用開始）とSBOM（ソフトウェアの部品表）の導入に向けた実証・手引きの策定。米国・欧州との対話、QUADの活用等。
- ✓ **政府全体でのサイバーセキュリティ対応体制の強化**
  - ・サイバー被害組織を直接支援する専門組織同士での情報共有を促進するためのガイダンス等を策定、JPCERT/CCやIPAのJ-CRATを通じた事案対処支援、IPAによるサイバー事故調査に向けた制度整備
- ✓ **新たな攻撃を防ぎ、守るための研究開発の促進**
  - ・先進的サイバー防御機能・分析能力強化のための研究開発プログラムの組成（最大320億円規模）

第８回産業サイバーセキュリティ研究会（2024年4月5日）の開催概要②

新たなサイバーセキュリティ政策の方向性

政府全体では、**国家安全保障戦略**や**サイバーセキュリティ戦略**などに基づき、サイバー空間における必要な取組を推進。経済産業省では、**産業界に向けた施策**を通じて、政府機関等の防御強化等NISCをはじめとする**関係省庁による取組と両輪となって**、これらの戦略において掲げられている**政府全体の目標に貢献**していく。

官民の状況把握力・対処能力向上

✓ IPAをハブとした**サイバー情勢分析能力強化**

サイバーセキュリティ対策の実効性強化

✓ 各種ガイドライン・評価制度の**政府調達等の要件化**

→ サプライチェーン強化のため規模や業種等に応じて企業の**適切なセキュリティ対策レベルを評価し可視化する仕組み**を検討

→ 一定のセキュリティ基準を満たす**IoT製品を認証する制度**や、ソフトウェア部品構成表（**SBOM**）について、政府調達等の要件化に向けて関係省庁と議論、**安全なソフトウェアの自己適合宣言の仕組み検討**

✓ **中小企業向け補助的施策の一層の強化**

→ セキュリティ人材の活用促進（マッチング実証事業）、お助け隊サービスの拡充・普及　等

サイバーセキュリティ市場の拡大に向けたエコシステム構築

✓ **産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環構築に向けた戦略の検討**

→ 需要と供給の好循環によるセキュリティエコノミーの確立に向けて、「セキュリティ産業」の構造化や米国・イスラエル等のセキュリティ産業振興モデルの研究などを進め、必要な政策（スタートアップ支援策等）を今後提言

→ 経済安全保障重要技術育成プログラム（320億円／5年間）

✓ **高度人材の育成・確保**（登録セキスペの活用促進**（2.3万人→5年後に5万人）**等）

第８回産業サイバーセキュリティ研究会（2024年4月5日）の開催概要③

産業界へのメッセージ

企業・団体向け

✓ 各種ガイドライン等に沿った対応を前提として、**組織幹部のリーダーシップの下**、必要な人材の育成や確保・体制の構築を進めながら、以下の対応をお願いしたい。

- サイバーセキュリティに対する投資を、**中長期的な企業価値向上に向けた取組の一環として位置付け**、その関連性について、**利害関係者から理解を得るための活動（情報開示等）を積極的に行う**こと。
- 自組織のシステム運用に係るリスク管理についてＩＴサービス等提供事業者との役割分担を明確化するなど、**ＩＴサービス等提供事業者に対してセキュリティ慣行を求める**こと。併せて、委託元として自組織で判断や調整を行わなければならない事項を把握等すること。
- サプライチェーン全体での対策強化に向けた意識を徹底する（**ASMの活用**や、サプライチェーンに参加する**中小企業等への共助**）こと。中小企業においては、「サイバーセキュリティお助け隊サービス」などの**支援パッケージの活用も検討する**こと。
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照し、 サイバー攻撃の被害に遭った場合等には、**適時の専門組織への相談及び所管省庁等への報告等を行う**こと。

ITサービス等提供事業者向け（機器やサービス等を提供する事業者）

✓ **自らの製品・サービスのセキュリティ対策に責任を持ち**、「セキュア・バイ・デザイン」や「セキュア・バイ・デフォルト」の考え方に沿った一層の対応（SBOMの採用、メモリに安全なプログラミング言語の採用等）をお願いしたい。

サイバー被害組織を直接支援する専門組織向け（セキュリティベンダ、情報共有ハブ組織等）

- サイバー攻撃による被害に関する情報共有の促進に向けて、専門組織間で必要な情報を共有することの意義等について**被害組織と共通の認識を醸成する努力**をお願いしたい。

１．第8回産業サイバーセキュリティ研究会

２．「電力システムにおけるサイバーセキュリティリスク点検ガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を電気事業者向けに公表

概要

- 2024年2月1日、第16回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 電力サブワーキンググループを開催。
- 電力制御システムにおけるサプライチェーン・リスク、日本における ERAB システムに関するセキュリティ対策実践、アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策、リスク点検ツール等について議論。
- 2024年3月22日、「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」及び「電力システムにおけるサイバーセキュリティリスク点検ガイド」を電力事業者向けに公表。

リスク点検ツールの対象事業者

- リスク点検ツールの対象事業者について、一般送配電事業者については電事連によるリスクアセスメントが推進されているところ、その他の**①発電事業者、②小売電気事業者、③アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）、④自家用電気工作物設備設置者の4区分を主な対象**とする。
- 4区分のうち、大手事業者の多くはリスク点検を既に定期的に実施しているところ、本事業で開発する**リスク点検ツールでは、中小事業者をはじめとするこれまでリスク点検を実施してこなかった事業者をメインスコープ**とし、当該事業者における簡易的かつ効率的なリスク点検を支援する内容とする。

リスク点検ツールの対象事業者

以下の4区分の事業者のうち、中小事業者をはじめとする
これまでリスク点検を実施してこなかった事業者を主な対象とする。

① 発電事業者

② 小売電気事業者

③ アグリゲーター
（アグリゲーションコーディネーター及びリソースアグリゲーター）

④ 自家用電気工作物設備設置者

リスク点検ツールの構成

- リスク点検ツールは、**「電力システムにおけるサイバーセキュリティリスク点検に関するガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」によって構成**する。
- ガイドは、国内電気事業者において自社の対策状況の確認やリスク評価に当たって活用できる文書とし、**リスク点検項目を示しつつ、リスク点検結果を踏まえた対策の改善方針も示す。**
- 対策状況可視化ツールは、各事業者が**リスク点検項目に対する対応状況を入力することで簡易に組織の成熟度や対策状況を可視化できるツール**とし、Excel形式にて作成する。

リスク点検ツールの構成

リスク点検ツール

電力システムにおけるサイバーセキュリティリスク点検に関するガイド

事業者が、自社の対策状況の確認やリスク評価に当たって活用できるガイド。具体的には以下の目次構成を設定する。

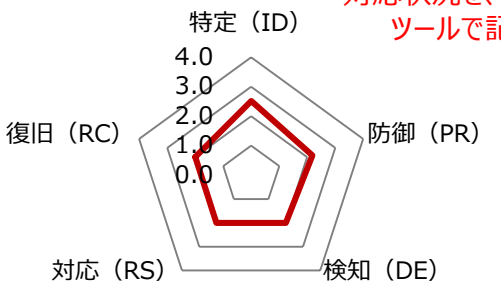
1. 背景・目的
2. 本ガイド・対策状況可視化ツールの構成
3. 本ガイド・対策状況可視化ツールの対象
4. 本ガイド・対策状況可視化ツールの想定活用方法
5. リスク点検項目・対策を怠った場合のリスク
6. リスク点検結果を踏まえた対策の改善方針
7. 参考文書
8. 用語集

＋

電力システムにおけるサイバーセキュリティ対策状況可視化ツール

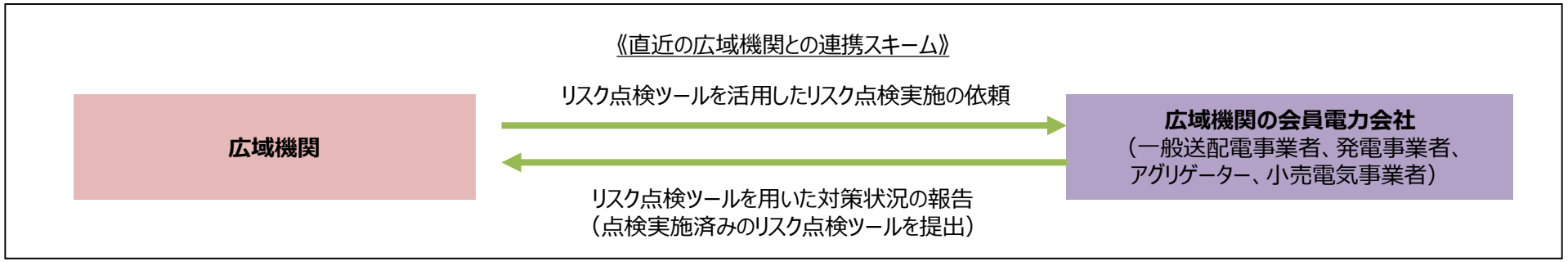
各事業者がリスク点検項目に対する対応状況を入力することで、組織の対策状況を可視化する。ヒアリング結果を踏まえ、Excel形式にて作成する。

リスク点検項目に対する対応状況を、可視化ツールで記載



意見交換を踏まえたリスク点検ツールの位置づけ

- 電気事業者の多くは広域機関の会員となるところ、リスク点検ツールの浸透・活用にあたっては、広域機関と連携した取組が効果的。
- **広域機関と連携し、ツールの浸透状況やツールに基づくリスク状況を定期的に確認しつつ、当該状況を踏まえ、より踏み込んだ要求レベルの設定や支援策等の検討を行う**。



リスク点検ツールの浸透状況の定期的な確認

提出されたリスク点検結果の分析による電力分野全体のリスク状況の把握

浸透状況・リスク状況を踏まえたリスク点検ツールの位置付けの検討
（特定区分に対する要求レベルの向上、特定区分に対する支援等）

【参考】リスク点検項目の概要

- **具体的なリスク点検項目について**、国内外の事業者において広く活用され、電事連が電力10社を対象に実施したリスク評価でも活用された**NISTのCybersecurity Framework（NIST CSF）を参考に整理**。
- NIST CSFでは、5つのセキュリティ機能（特定、防御、検知、対応、復旧）に対し、機能の詳細を定めた23のカテゴリー、108のサブカテゴリーが定義されているため、**本リスク点検ツールでは108のサブカテゴリーをリスク点検項目として設定**する。

機能	カテゴリー		サブカテゴリー数
特定(ID)	ID.AM	資産管理	6
	ID.BE	ビジネス環境	5
	ID.GV	ガバナンス	4
	ID.RA	リスクアセスメント	6
	ID.RM	リスク管理戦略	3
	ID.SC	サプライチェーンリスクマネジメント	5
防御(PR)	PR.AC	アクセス制御	7
	PR.AT	意識向上及びトレーニング	5
	PR.DS	データセキュリティ	8
	PR.IP	情報を保護するためのプロセス及び手順	12
	PR.MA	保守	2
	PR.PT	保護技術	5

機能	カテゴリー		サブカテゴリー数
検知(DE)	DE.AE	異常とイベント	5
	DE.CM	セキュリティの継続的なモニタリング	8
	DE.CP	検知プロセス	5
対応(RS)	RS.RP	対応計画	1
	RS.CO	伝達	5
	RS.AN	分析	5
	RS.MI	低減	3
	RS.IM	改善	2
復旧(RC)	RC.RP	復旧計画	1
	RC.IM	改善	2
	RC.CO	伝達	3

NIST CSFの各サブカテゴリーを、リスク点検ツールにおけるリスク点検項目として設定

【サブカテゴリーに基づくリスク点検項目の例】

PR.PT-1：監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。(ログの取得を実施している。)

PR.PT-2：リムーバブルメディアは、保護され、その使用がポリ シーに従って制限されている。(外部記憶媒体をルールに則って管理している。)　等

（参考）第8回産業サイバーセキュリティ研究会

新たなサイバーセキュリティ政策の方向性

- サプライチェーン全体での対策強化に向け、これまでソフトロー・アプローチとして、経営層の意識改革の促進、各種のフレームワーク・ガイドライン等の策定を実施。今後、関係省庁と連携し、**政府調達等への要件化を通じ、その実効性を強化**する。　※十分なリソースの確保が困難な中小企業等に対しては、支援策を一層強化。
- こうした需要側への働きかけと同時に、**国産製品の開発・普及促進や高度人材の育成・確保**といったセキュリティの供給側への働きかけを通じて、我が国におけるセキュリティ市場の拡大を図ることが重要。
- また、サイバー安全保障の実現に向けて、産業界との接点を活かしつつ、**官民のサイバー状況把握力・対処能力向上に向けた取組**を進める。

サイバーセキュリティ対策の実効性強化

<これまでの取組：フレームワーク・ガイドライン等の整備>

サイバー・フィジカル・セキュリティ対策フレームワーク

- 経営ガイドライン
- 工場ガイドライン
- ●●ガイド・・・etc

政府調達に関する基準／民間企業における調達要件
（政府機関等のサイバーセキュリティ対策のための統一基準群等）

<今後目指すべき取組：調達要件化等を通じた実効性の強化>

IPA

策定・連携

サイバー・フィジカル・セキュリティ対策フレームワーク

- 経営ガイドライン
- 工場ガイドライン
- ●●ガイド・・・etc

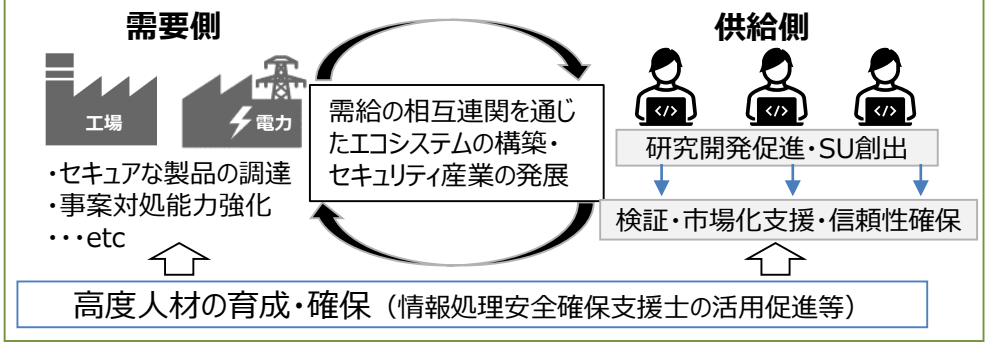
政府調達に関する基準／民間企業における調達要件
（政府機関等のサイバーセキュリティ対策のための統一基準群等）

認証製品の調達要件化等の連携（例：IoTセキュリティ適合性評価制度）

認証基準策定

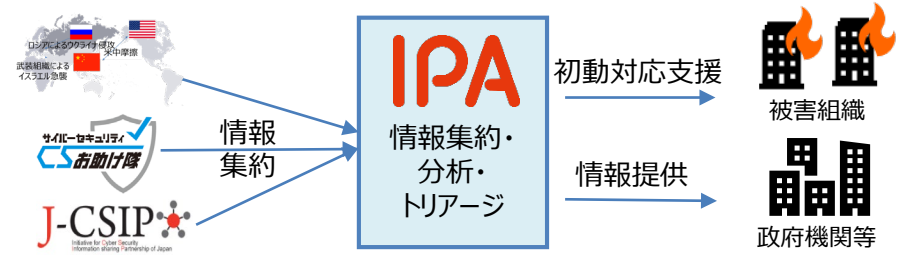
認証制度（新設）

セキュリティ市場の拡大に向けたエコシステムの構築



サイバー情勢分析能力の強化

官民の情報ハブとしてのIPAの強みを活かし、地政学等の情勢と産業界（エンドポイント）から得られるサイバー攻撃情報の集約・分析を一層推進。攻撃者の意図を把握し、攻撃の対象や手法を予見して効果的な防御策を講じる。



（参考）サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

実効性強化

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

想定される検討事項

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

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

対策レベルの可視化（イメージ）

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

政府調達・補助施策等への要件化

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

（参考）ガイドライン等の実効性の強化

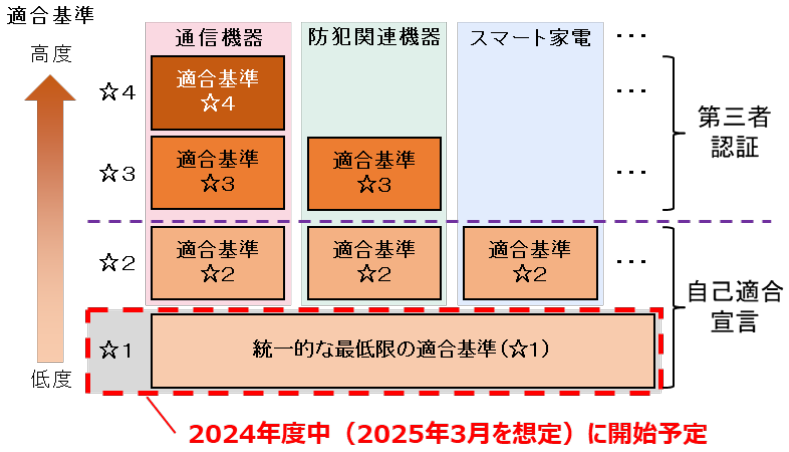
（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

実効性強化

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

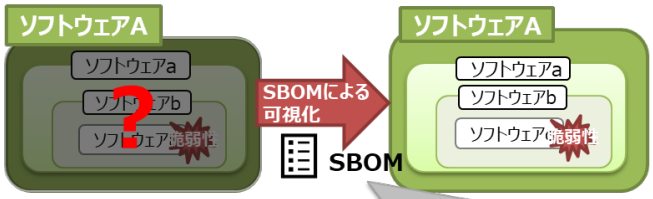
IoTセキュリティ適合性評価制度

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



SBOMのイメージ

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



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

セキュアバイデザイン・セキュアバイデフォルト

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

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

（参考）半導体関連産業におけるセキュリティの確保に向けた検討の開始

実効性強化

- 半導体関連産業の国内投資の促進が強力に進められているところ、**安定的な供給を確保する観点からも、サイバーセキュリティ対策を進めることが重要**。
- 経済産業省においても、**「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を整備**。当該ガイドラインの浸透を進めつつ、**半導体関連産業におけるセキュリティの確保に関して必要な政策を模索するため実態把握・調査等を進めていく**。また、**サイバーセキュリティ対策への取組、問題意識や事例、防御に資する脅威情報を相互にを共有できる場を設置**する。
- こうした議論の中で、**半導体関連産業において求められるセキュリティ対策を具体化**していくとともに、その内容を**経済産業省の投資促進関係施策の要件等とも紐付けること等**を検討し、**その実効性を強化**していく。

半導体セキュリティの直近の動向

海外の動向

- TSMCは、2018年に主力工場がランサムウェアの被害に遭い生産停止を余儀なくされ、影響額は最大190億円に及んだ。
- 2023年に半導体装置のセキュリティ規格であるSEMI E187を調達要件化。SEMI E187の要件を満たしていることを、認証機関によって証明されたサプライヤーも出現。

（出典）日本経済新聞、TSMC社プレスリリース

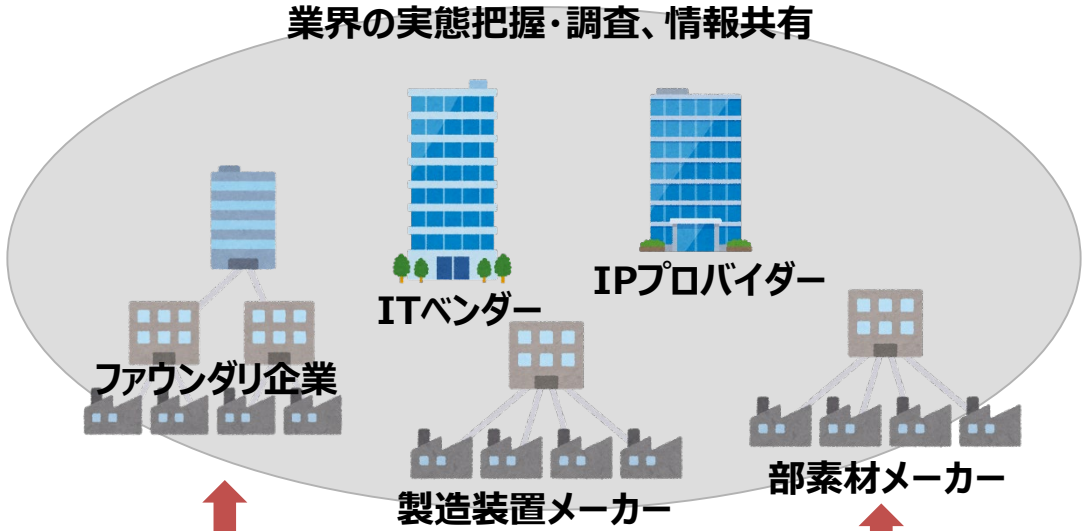
国内の動向

- 半導体向けの研磨材を扱うフジミインコーポレーテッドは、サーバへの不正アクセスがあったことから公式Webサイトを含む社内システムを全面停止し、一部製品の生産と出荷を見合わせた。
- シリコンウェハを扱うグローバルウェーハズ・ジャパンは、社内サーバーに不正アクセスを受けたことから、ネットワークから社内システムを切り離す措置を実施し、シリコンウェハの製造および出荷が不能となった。

（出典）フジミインコーポレーテッド社プレスリリース、グローバルウェーハズ・ジャパン社プレスリリース

国内の安定供給確保のためサイバーセキュリティ対策を進めていく

半導体関連産業全体でのセキュリティ水準の底上げ



工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

自ら工場のセキュリティ対策を立案・実行し、工場のセキュリティ水準の底上げを図るための、参照すべき考え方やステップを示した手引き

（参考）サプライチェーン全体での対策強化（中小企業等向けの支援の一層強化）

実効性強化

- サプライチェーン全体のセキュリティ対策を更に強化するためには、中小企業の**中堅レベルにおいては事業継続に耐えうるレジリエンスを確保、小規模レベルにおいては経営層が最低限の危機管理の認識を持つ水準**のセキュリティの確保が必須。
- 一方で、セキュリティへの対策も含め、**十分なリソースの確保が困難であるとの課題**も存在するところ、こうした中小企業等に対しては、中小企業の実態も踏まえた**適切なセキュリティ対策のあり方を提示**しつつ、**支援策を一層強化**していく。

中小企業等における課題

- IPAの調査（2021年度）によれば、中小企業のうち、合計で**４割が「どこからどう始めたらよいかわからない」「コストがかかり過ぎる」と回答。**セキュリティ対策を効果的に実践できていない状況。
- また、セキュリティに支出可能な金額は**月額３万円未満と回答する企業が４割超**。セキュリティ人材についても、多くの企業において不足している状況。

出典：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、令和３年度中小企業サイバーセキュリティ対策促進事業　（北海道におけるサイバーセキュリティコミュニティ強化に向けた調査）

- サプライチェーン単位での攻撃が増加する中、必要十分なセキュリティ対策を実施できない企業が狙われることで大きな経済的損失をもたらすおそれがある。
- こうした状況の打開に向けて、予算や人材が不足している中小企業が、**それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握**し、それを**実践できる環境を整備**していくことが必要。

中小企業等向け支援施策

- 中小企業等において効果的なセキュリティ対策を実践できるよう、**規模等に応じたセキュリティ対策を提示するとともに、対策の実践に当たって必要となるセキュリティ人材の確保やサービスの支援策を強化**。

規模等に応じたセキュリティ対策の提示

➢ 中小企業等のIT資産の内容等、実態調査も行い、**企業規模やIT資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等の提示**を図る。

セキュリティ人材の活用促進

➢ **中小企業等とセキュリティ人材とのマッチングを促す場を構築する実証を実施**し、セキュリティ人材のシェアリング促進等、中小企業が行う人材探索を支援する。

「サイバーセキュリティお助け隊サービス」の拡充

➢ **新たな類型（２類）を創設し**、中規模以上の中小企業が求める高度なサービスに対応。さらに**2類サービス事業者とIPA間で重大サイバー攻撃に関する情報共有を活性化し、効果的に中小企業のサイバー攻撃被害防止を行う体制を作る。**

- このほか、中小企業等の身近な相談先である**地場ベンダの能力強化**に向けた施策や、金融機関など**DX支援機関を通じた面的支援**の促進なども展開。

これらの施策について、各地域においてワークショップやセミナー等も開催しながら、産業界や地域SECUNITYとも連携した施策の展開・普及を実施し、産業界のサプライチェーンセキュリティ全体の向上を図る。

（参考）我が国サイバーセキュリティ産業の振興に向けた強化策の検討

供給力強化

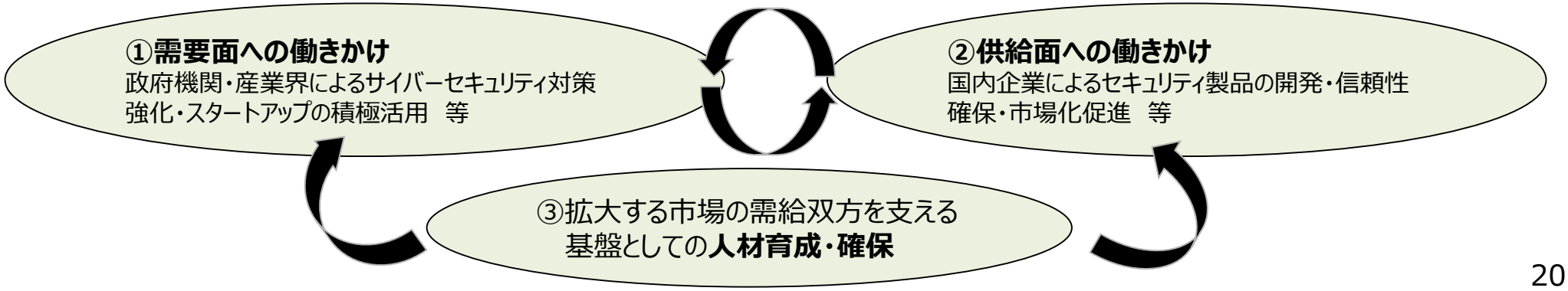
問題意識

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

目指すべき姿

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

＜「セキュリティエコノミー」好循環のイメージ＞



（参考）先進的サイバー防御機能・分析能力強化のための研究開発

供給力強化

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

目　的

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

実施内容

（１）サイバー空間の情報を収集・調査する状況把握力の向上

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

（２）サイバー攻撃から機器やシステムを守る防御力の向上

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

（３）共通基盤の整備

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

（４）セキュアな量子情報通信技術の開発

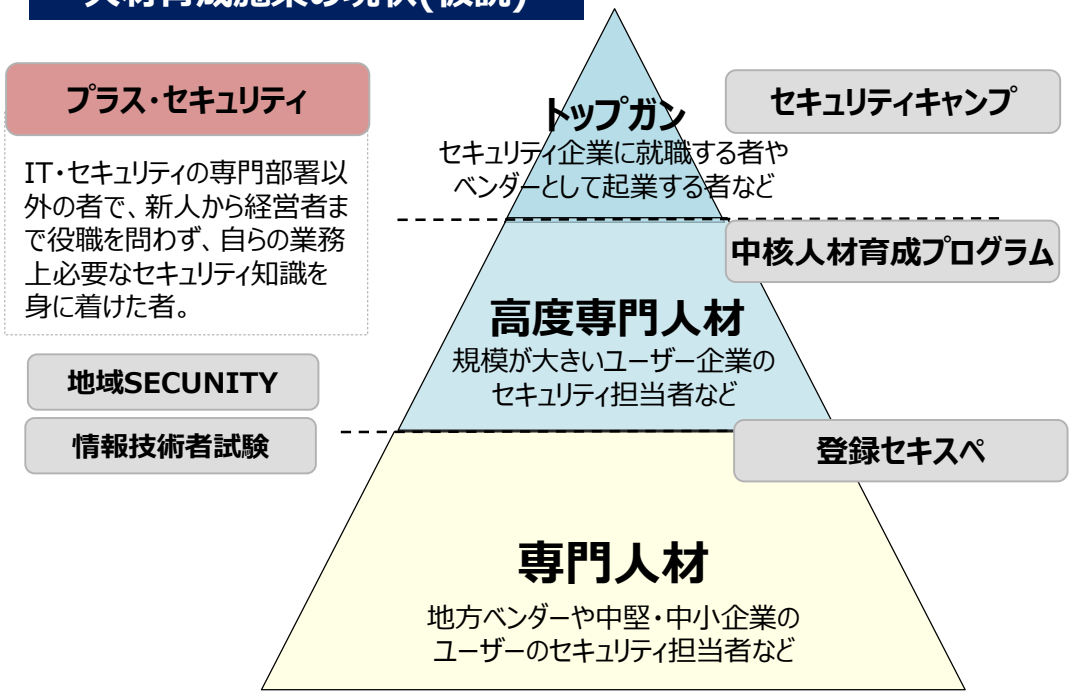
- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

（参考）サイバーセキュリティ人材の育成・確保に向けた取組の方向性

供給力強化

- セキュリティ市場の拡大に向けたエコシステムを構築するためには、産業・技術基盤の維持・発展を支える供給側、セキュリティ対策を実装する需要側、**双方の基盤となる人材の育成・確保が重要**。
- しかし、NRIセキュアの調査（※1）によると、日本においては、従業員規模に関わらず**９割の企業でセキュリティ人材が不足していると回答**。またISC2の調査（※２）によると国内のサイバーセキュリティ人材は現在約48万人存在しているが、**11万人不足**。
- セキュリティ人材施策として、セキュリティキャンプや中核人材育成PG、情報処理安全確保支援士試験を通じた**高度専門人材の育成**、地域SECUNITY活動等を通じた**プラス・セキュリティの普及**等を進めてきているが、**需給ギャップを解消するためには、セキュリティ人材の裾野を更に拡大するための施策の検討が必要**。
- また、NISC改組後の「新たな組織」を含む**政府機関等において十分なセキュリティ人材を確保する**ことにより、政府全体でのサイバー安全保障分野での対応能力を向上につなげることも重要。こうしたセキュリティ人材が、産業界に留まることなく、**政府と民間との間でより活発に行き来できるようにする**ことも必要ではないか。

人材育成施策の現状(仮説)



現状の課題

- これまで、トップガンや高度専門人材の育成は進めてきたものの、1年間に育成できる人数が限定的。
- 登録セキスペは、首都圏のベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- これまで施策では、地方ベンダーや中堅・中小企業のユーザーのセキュリティ担当者などにアプローチできない。

今後の方向性

- トップガンの発掘・育成及び事業化促進に向けてセキュリティキャンプの拡張及び未踏事業との連携を検討。
- ユーザー企業における登録セキスペの活用を促進（中小企業等とのマッチング実証事業、DX促進施策との連動等）するとともに、制度の見直しも検討。これらを通じて、**登録人数**（2024年４月現在、約2.3万人）**を2030年までに５万人まで増加を目指す**。
- 専門人材の育成に関する課題整理を行うとともに、基礎知識・スキル習得できるような環境整備に関する検討を実施。

※1　NRI Secure Insight 2023
※2　ISC2 Cybersecurity Workforce Study 2023

（参考） IPAにおけるサイバー情勢集約・分析能力の強化

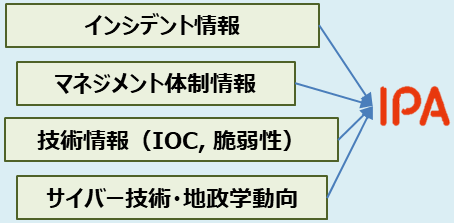
官民対処

- 国家安全保障戦略に基づく対応を強化すべく、IPA第五期中期目標において、**「サイバー状況把握力」を強化**し、**国家の安全保障・経済安全保障の確保に貢献**する旨を明記。今後は、産業界（エンドポイント）を通じて得られる**サイバー攻撃情報の集約・分析機能を強化**し、J-CRATを中心に**IPAの対応支援機能を強化**。

ＩＰＡにおけるサイバー情勢の集約・分析機能の強化

１．情報収集・検知力の向上

ＩＰＡが有する産業界とのネットワーク、セキュリティ対策に係る各種制度を駆使し、**産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブ**として機能を強化。



２．統合的な分析・脅威評価機能の強化

地政学の専門家の協力も得つつ、経済活動に影響を及ぼすサイバーリスクを統合的に分析することにより、**産業分野に関する脅威評価のハブ**として機能。

３．情報共有／ 対応支援機能の強化

政府機関、産業界の経営レベルと現場の双方との連携対話を強化し、**防御や抑止対応に資する情報共有／対応支援活動のハブ**として活動を推進。

活動イメージ）

- 政府機関や重要インフラ事業者等に対する**APT攻撃に関するハントフォワード活動**
- 主要産業に対する経済産業省関連**中小企業支援策の普及展開**、IPAによるリスクアセスメント支援等を通じたセキュリティ体制構築支援
- 攻撃の背景となる地政学動向等を踏まえた**サイバー脅威評価の共有**や、主要産業に対する**重大なサイバー攻撃関連情報の共有・注意喚起** 等

（参考）産業界へのメッセージ（令和６年４月５日）（全体像）

- 急速に普及しつつある生成AIをはじめとするデジタル化の進展や世界的な地政学リスクの高まり、サイバー攻撃の深刻化・巧妙化などにより、サイバーリスクは高まっている。このような**サイバー攻撃が、国民生活、社会経済活動及び安全保障環境に重大な影響を及ぼす可能性**も大きくなっている。また、米欧等においても産業界におけるサイバーセキュリティ対策強化に向けた制度整備の動きなどが活発化しており、**我が国においても一層の対策強化が求められる状況**。
- こうした状況を踏まえ、まずは、経済産業省として、NISC等関係省庁との連携の下、**これまでの施策の一層の普及・啓発などに取り組みながら**、政府調達等への要件化を通じたサイバーセキュリティ対策の実効性強化や、サイバーセキュリティ供給力の強化、官民の状況把握力・対処能力向上に向けた**新たな取組も進める**。今後も産業界からの御意見を聴くなど、官民の協力関係を維持・発展させつつ、**不断に取組を見直していく**。
- 各企業・団体においては、こうした状況も踏まえ、**各種ガイドラインや随時の「注意喚起」に沿った対応を前提**として、組織幹部のリーダーシップの下、必要な人材の育成や確保・体制の構築を進めながら、以下の対応をお願いしたい。

  ①　サイバーセキュリティに対する投資を、**中長期的な企業価値向上に向けた取組**の一環として位置付ける（ＤＸ、ＢＣＰ、サステナビリティ等に紐付ける。）。その上で、その関連性について、投資家を含む**利害関係者から理解を得るための活動（対話・情報開示等）を積極的に行う**。

  ②　自組織のシステム運用に係るリスク管理について**ＩＴサービス等提供事業者との役割分担を明確化**するとともに、「**セキュア・バイ・デザイン**」（※１）や「**セキュア・バイ・デフォルト**」（※２）**の製品の購入を優先**するなど、**ＩＴサービス等提供事業者に対してセキュリティ慣行を求める**。併せて、委託元として**自組織で判断や調整を行わなければならない事項を把握する**とともに、ＩＴサービス等提供事業者に**委託した業務の結果の品質を自社で評価できる体制を整備する**。

  ※１ 「セキュア・バイ・デザイン」：IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
  ※２ 「セキュア・バイ・デフォルト」：ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

  ③　**サプライチェーン全体での対策強化に向けた意識を徹底**する（ASM（Attack Surface Management）等外部サービスの活用や、サプライチェーンに参加する中小企業等への共助（取引先からの要請対応への負担配慮や脆弱性診断などの支援等））。**中小企業においては、「サイバーセキュリティお助け隊サービス」などの支援パッケージの活用**も検討する。

  ④　**「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照**し、サイバー攻撃の被害に遭った場合等には、適時の専門組織への相談及び所管省庁等への報告等を行う。

- ＩＴサービス等提供事業者においては、**自らの製品・サービスのセキュリティ対策に責任を持ち**、**「セキュア・バイ・デザイン」や「セキュア・バイ・デフォルト」の考え方に沿った一層の対応**（「顧客だけにセキュリティの責任を負わせない」、「トップ主導での実施」等の基本原則の遵守、SBOMの採用、メモリに安全なプログラミング言語の採用等）をお願いしたい。
- セキュリティベンダや調査ベンダ、情報共有活動のハブ組織等のサイバー被害組織を直接支援する専門組織においては、「サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書」に沿って、**専門組織間で必要な情報を共有することの意義等について被害組織と共通の認識を醸成する**努力をお願いしたい。