経済産業省

産業分野における
サイバーセキュリティ政策

2024年９月

商務情報政策局　サイバーセキュリティ課

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「**ランサムウェア攻撃**」やセキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ**。

情報セキュリティ10大脅威 2024

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2024.1.24>

デジタル技術の発展によるサイバーリスクの増加の例

■　情報システムの利用拡大やクラウド等の活用拡大、インターネットに接続されるIoT製品の急増（2019年：231億台⇒ 2024年：399億台）など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

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

□　NICTER において2023年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,197億パケット（2018年の約３倍）。中でも、**IoT機器を狙った攻撃関連通信が多い**。

□　フィッシング対策協議会によると、2023年における**フィッシングの報告件数は100万件超**（2019年の約20倍まで増加）。

<出典：総務省「令和５年度版情報通信白書データ集」、(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2023」、フィッシング対策協議会「月次報告書」 等>

主なサイバー攻撃事案

①個人情報や機微技術情報などが情報窃取される

- **米国SolarWinds事案（2020年12月）**主要政府機関等のシステムが2019年9月から不正アクセスを受けていたことが発覚。極めて高度な攻撃手法を用いて検知体制をすり抜けていたが判明。

②ランサムウェア攻撃やBEC (Business E-mail Compromise)などにより金銭等資産が奪われる

- **JALビジネスメール詐欺被害公表（2017年12月）**ビジネスメール詐欺で3.8億円の被害を被る。

③データ改ざんやフェイク情報拡散などによって意思決定・指示が歪められる

- **米国大統領選挙に対するロシアの干渉疑惑（2016年）**ロシア攻撃集団がサイバー攻撃やSNSを使ったプロパガンダを展開したとして、オバマ政権はロシア外交官３５人国外退去処分等の制裁を実施。

④事業活動が停止に追い込まれる

- 自動車部品メーカーが、ランサムウェア攻撃を受けサーバがダウン。同社と連係関係にある自動車メーカーは、**国内全工場の稼働を１日間停止**。（2022年３月）

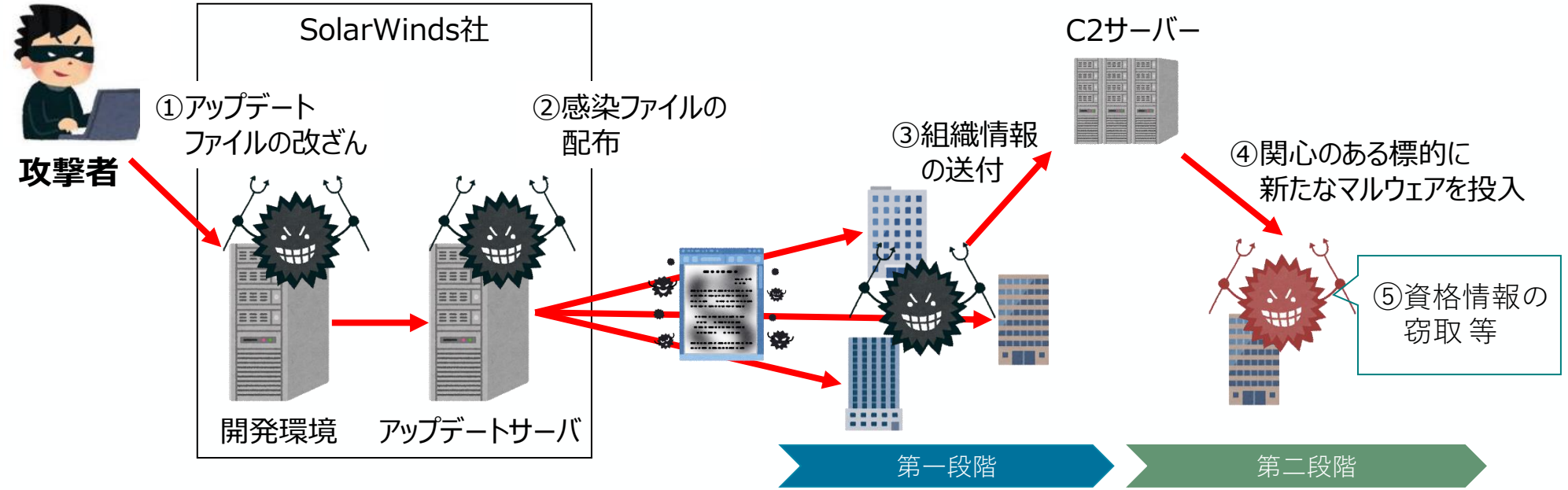
⑤社会インフラの誤作動・機能停止により社会全体に被害が発生する

- ウクライナでは、**サイバー攻撃による大規模な停電が複数発生**（2015年12月、2016年12月、2022年10月）
- **米国フロリダ州の飲用水汚染未遂（2021年2月）**水道局は制御系システムへの不正アクセスで飲用水に含まれる水酸化ナトリウムが一時的に約100倍に上昇したと発表。職員が異常に気付いて対応し、被害は発生せず。
- 名古屋港のコンテナターミナルにおいて、ランサムウエア攻撃によるシステム障害が発生し、**約3日間コンテナの搬入・搬出が停止**。（2023年７月）

SolarWinds社の正規ソフトアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 攻撃者が関心のある標的に対しては**第２段階のマルウェアが投入**され、資格情報を窃取。

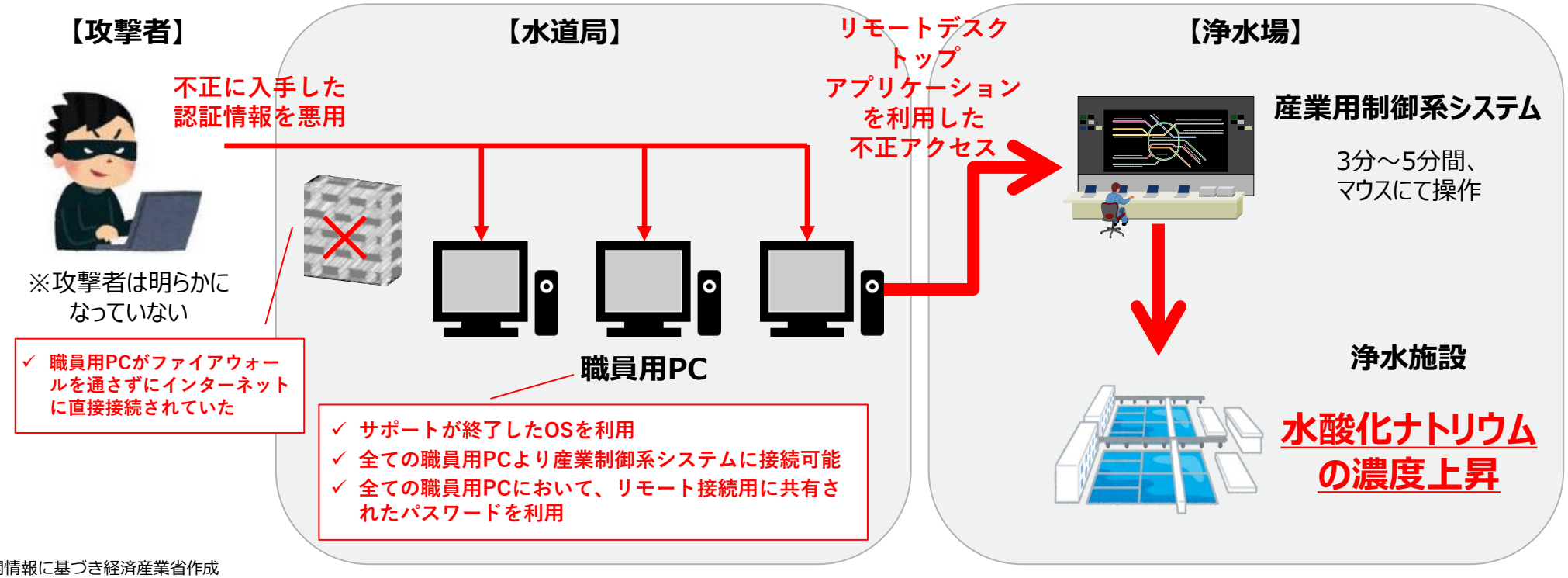
◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

水道システムへの不正アクセス事案

- 2021年2月、アメリカフロリダ州オールズマー市水道局は、**水道における産業用制御系システムを対象とした不正アクセス**によって、飲用水に含まれる水酸化ナトリウムの量が一時的に通常の約100倍に上昇したと発表した。
- オペレーターが異常に気付き、即座に設定を戻したため、実際の被害はなかったとされる。

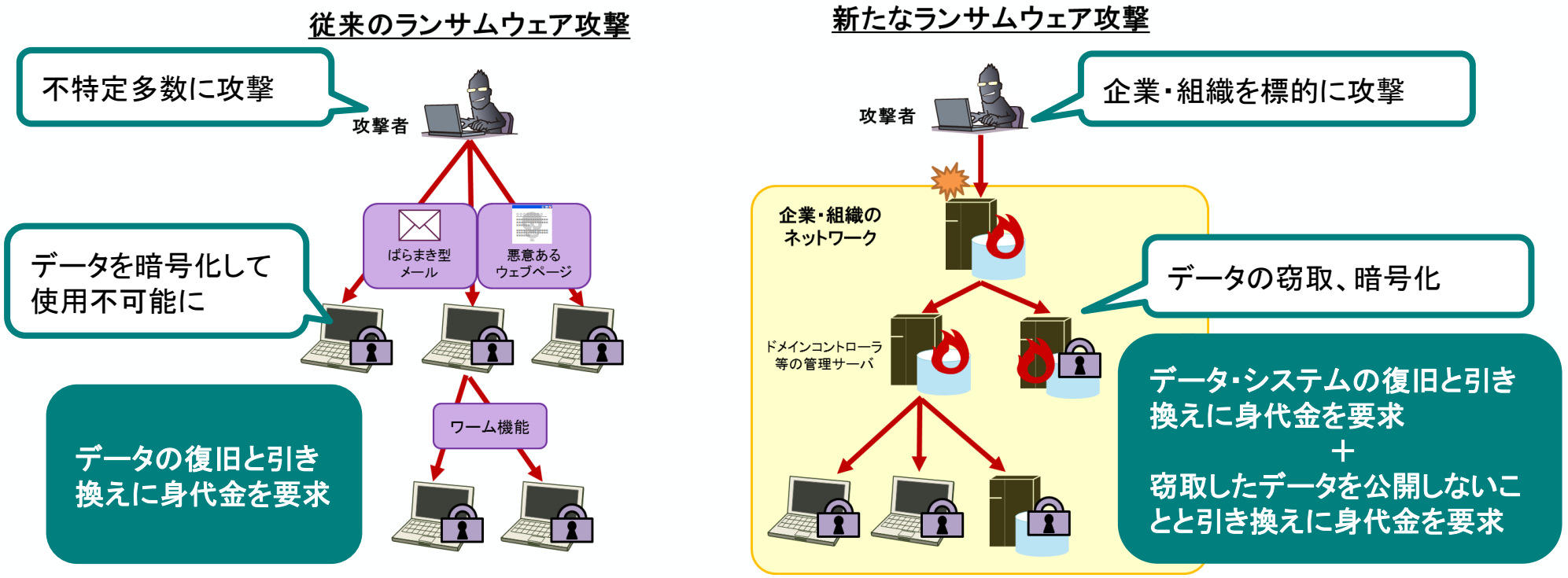


（出典）各種公開情報に基づき経済産業省作成

ランサムウェアとその手口の変化（二重の脅迫）

- ランサムウェアは「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。データを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- 新たなランサムウェア攻撃のパターン（二重の脅迫）では、**システムの復旧に対する金銭要求に加え、窃取したデータを公開しない見返りの金銭要求も行う。**

◆攻撃イメージ

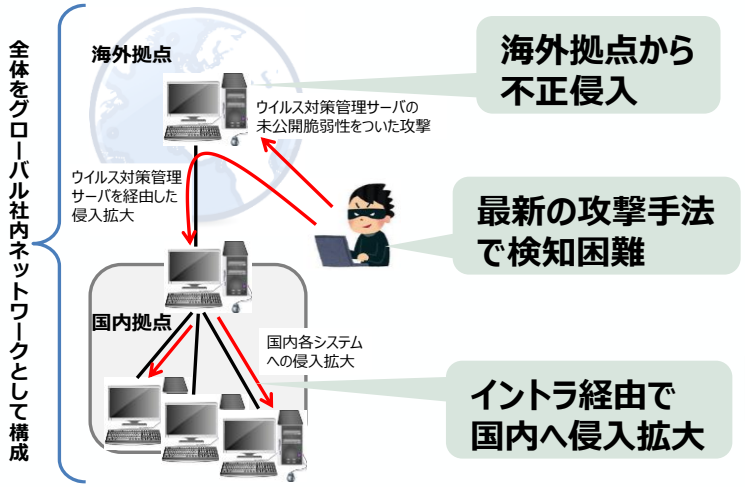


海外拠点経由の攻撃

- ビジネスのグローバル化に伴って、**海外拠点とのネットワークを国際VPN等によりWAN（広域社内ネットワーク）に取り込んで構築**しているケースが増加。
- 海外とのビジネス効率化に寄与する一方で、**海外拠点への不正侵入によって、そこを足がかりに国内ネットワークまで侵入されるケースも増加。**

※ 海外拠点（海外支社の他、関連会社、提携先、取引先等を含む）においては様々な原因により、日本国内と同等なレベルのセキュリティ対策が十分に取れないケースが多い。

A社事案における攻撃ルート



B社、他数社の事案の概要

- 指定秘密等の重要情報の漏えいは免れたとされている。
- ただし、攻撃者は社内の複数のシステムを渡り歩き、B社事案ではサーバ上の27,445件のファイルが不正アクセスを受けるなど、システム内部にかなりの侵入を許してしまっていた。
- 検知が遅れていれば、さらなる広範なシステムへの侵入を許していた可能性もある。

重要情報に係わるシステム分離、脆弱性対策の迅速なアップデート適用、振る舞い検知など最新の対策導入が重要

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

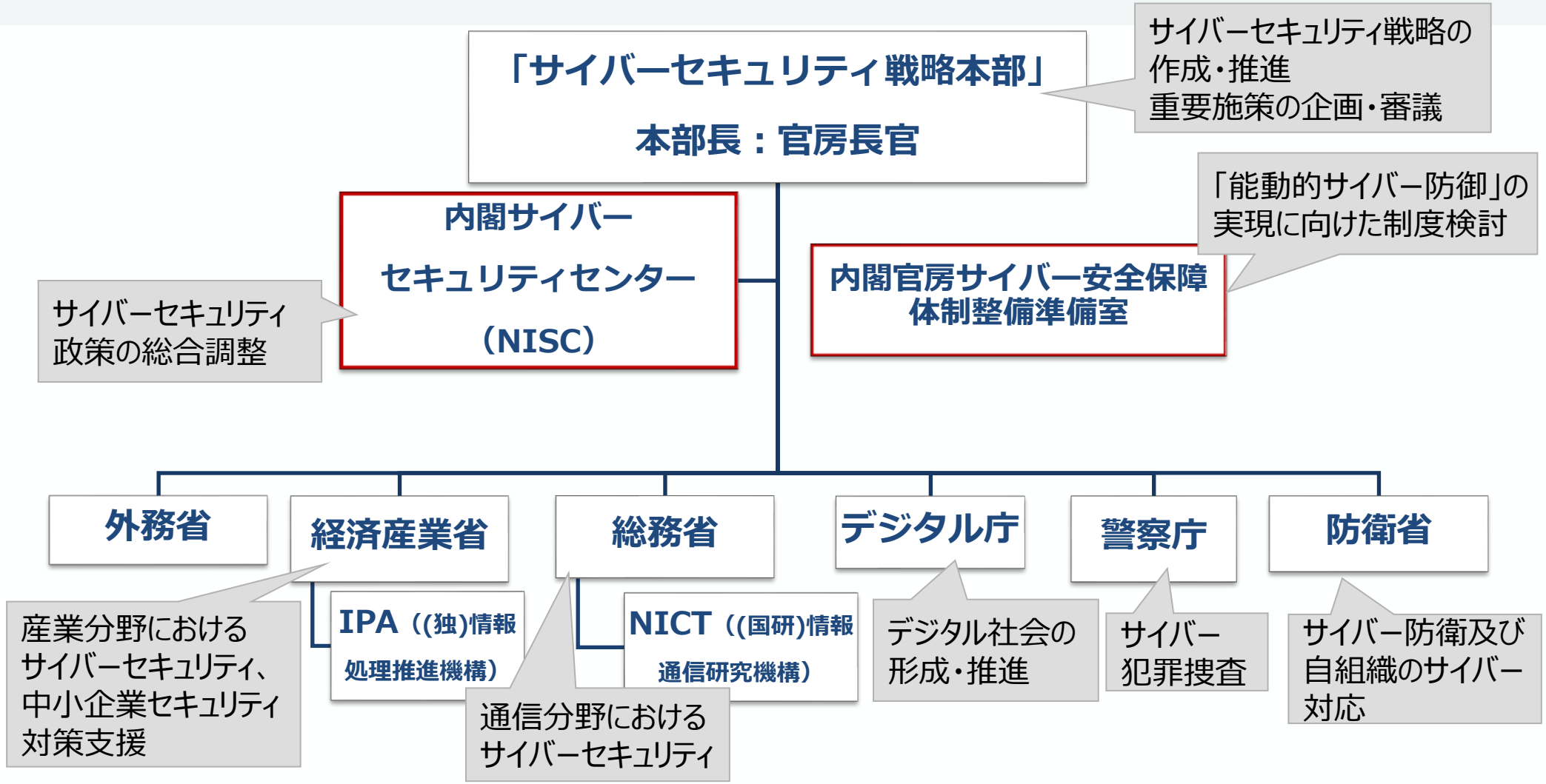
（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

サイバーセキュリティ政策の推進体制

- サイバーセキュリティ戦略本部（本部長：官房長官）の下、内閣サイバーセキュリティセンター（NISC）が総合調整を行い、各省が所管分野におけるサイバーセキュリティ政策を担う。



サイバーセキュリティ戦略2021：「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する公共空間化
- サイバー・フィジカルの相互連関・連鎖の深化
- サイバー攻撃の複雑化・巧妙化
- 安全保障上の脅威の増大

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：**経営層の意識改革、地域・中小企業の取組促進**
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○**国際協力・連携**

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

○**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**
（**産業横断的なサプライチェーン管理**、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

○深刻なサイバー攻撃から国民生活・経済を守る**包括的なサイバー防御等の展開**
（**情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化**、政府機関・重要インフラ等の各主体のセキュリティ対策）

※赤字は経産省が主体的に関与

国家安全保障戦略に基づく政府の検討の方向性

現在の課題

- 我が国に対する**安全保障上の懸念となる重大なサイバー攻撃のおそれ**がある場合、これを**未然に排除し、または既に発生した被害の拡大を防止する必要**があるが、このための**制度や体制が整備されていない。**
- このままでは、海外の脅威主体等からの重大なサイバー攻撃により**社会インフラの機能の停止や重大な犯罪被害が発生**し、**有事の際の対応にも支障を来す**可能性がある。

国家安全保障戦略の記述

- **武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入**する。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

（ア）重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

（イ）**国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

（ウ）**国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

- 能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する**。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

⇒現在、内閣官房サイバー安全保障体制整備準備室において必要な法案の検討作業を実施中。
NISCについては今夏、次官級ポストの設置など順次組織を拡大。

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

経済産業省におけるサイバーセキュリティ政策の全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのための政策を企画・実行する。
- その上で、各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ お助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

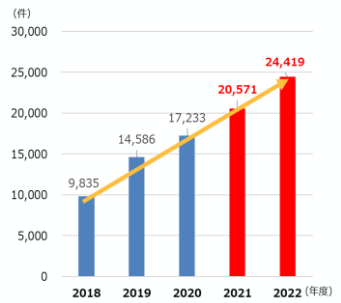
②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）



④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

サイバー・フィジカル・セキュリティ対策フレームワーク

- 「Society5.0」によって柔軟化・拡張するサプライチェーンに求められる**セキュリティへの対応指針**として、「サイバー・フィジカル・セキュリティ対策フレームワーク」（**CPSF**）を策定。※「Society5.0」においては、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要。**

「Society5.0」以前

個々の企業主体の定型的なつながりで価値を生み出す

<3層構造>

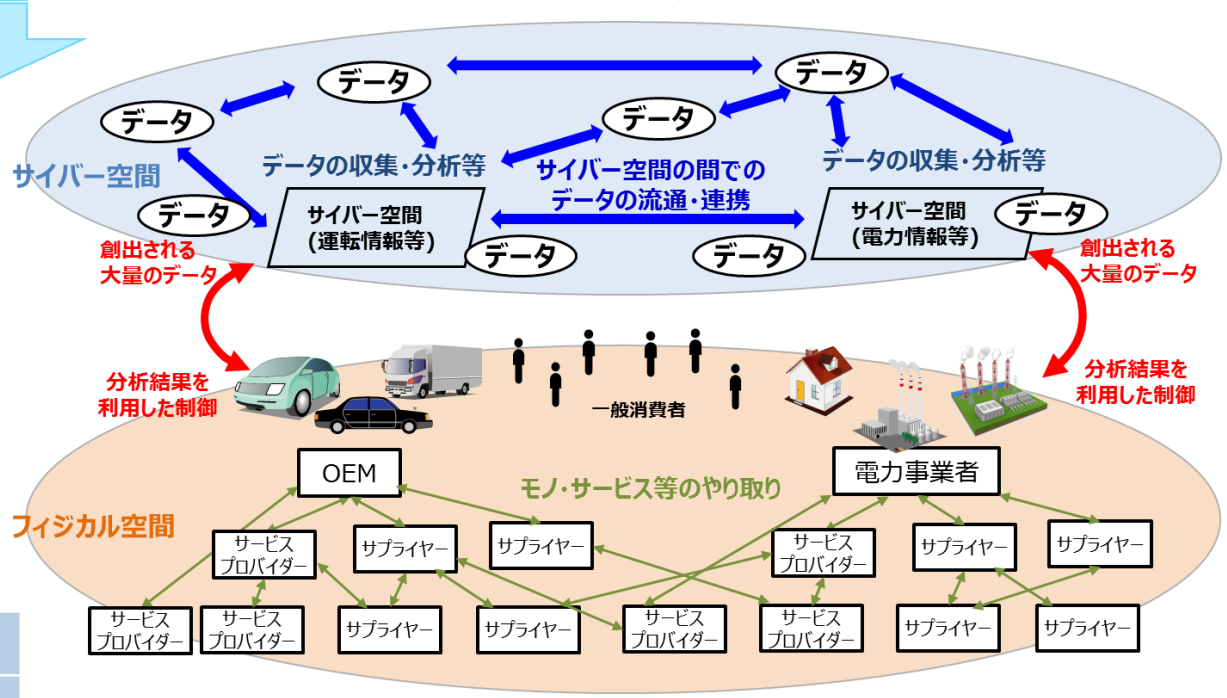
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

<6つの構成要素>

ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

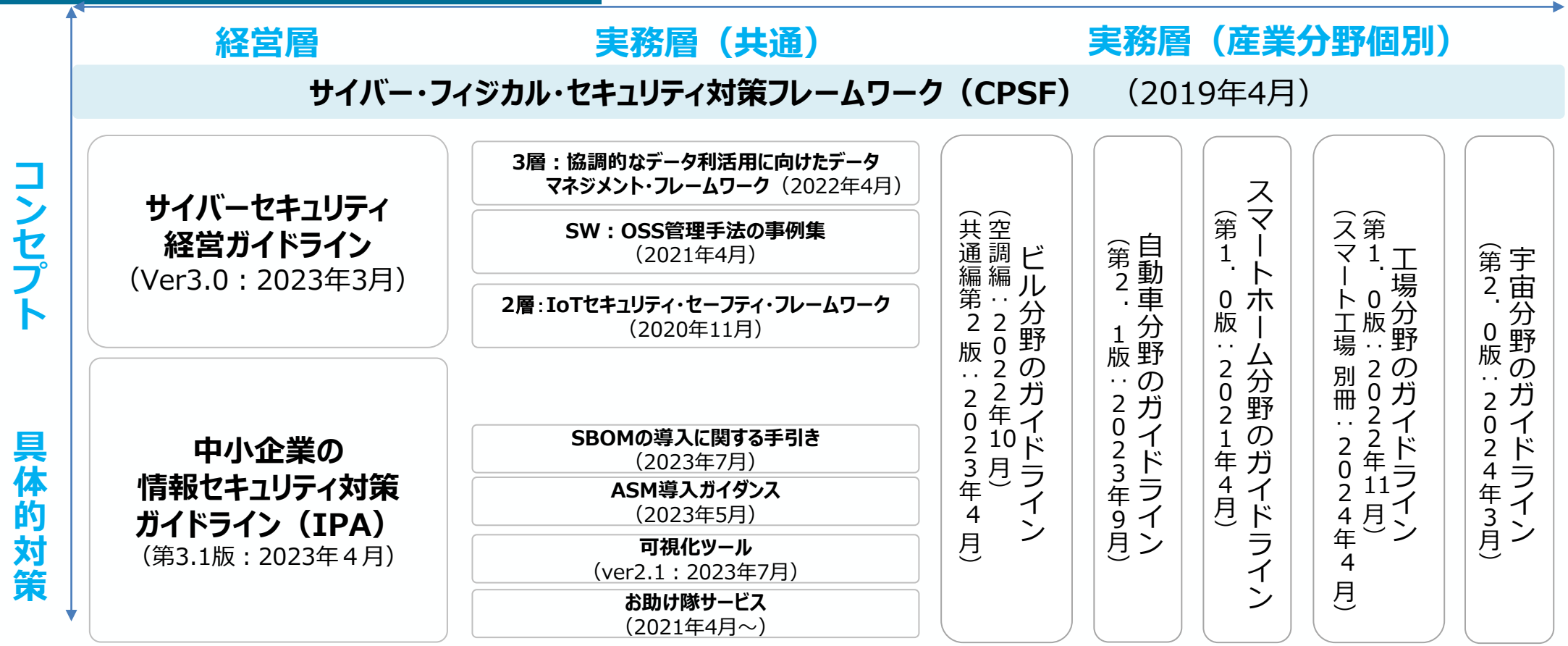
フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFを軸とした各種取組

- CPSFに沿って、**対象者や具体的な対策を整理**し、実践的なガイドラインを整備。

主なガイドラインや対策ツール



サイバーセキュリティ経営ガイドライン

平成27年12月28日策定
令和5年3月24日第3版公表

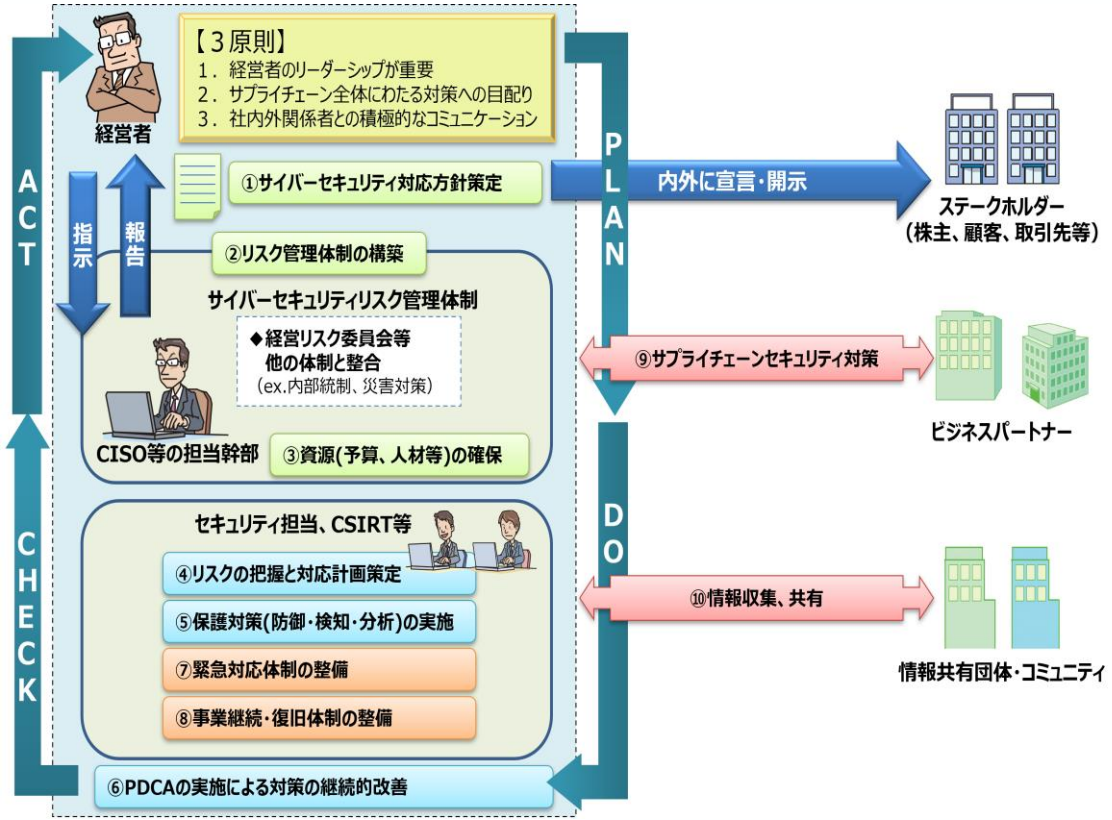
- 経営者がリーダーシップをとってセキュリティ対策を推進することが重要。このため、**経営者を対象としたガイドライン**を策定。可視化ツールや実践事例集なども整備。

1．経営者が認識すべき３原則

（1）経営者が、**リーダーシップを取って対策**を進めることが必要
（2）自社のみならず、**サプライチェーン全体にわたる対策**への目配り
（3）平時及び緊急時のいずれにおいても、**社内外関係者との積極的なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 事業継続・復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	**指示10** 情報収集、共有及び開示の促進



https://www.meti.go.jp/policy/netsecurity/mng_guide.html

ASM（Attack Surface Management）ガイダンス

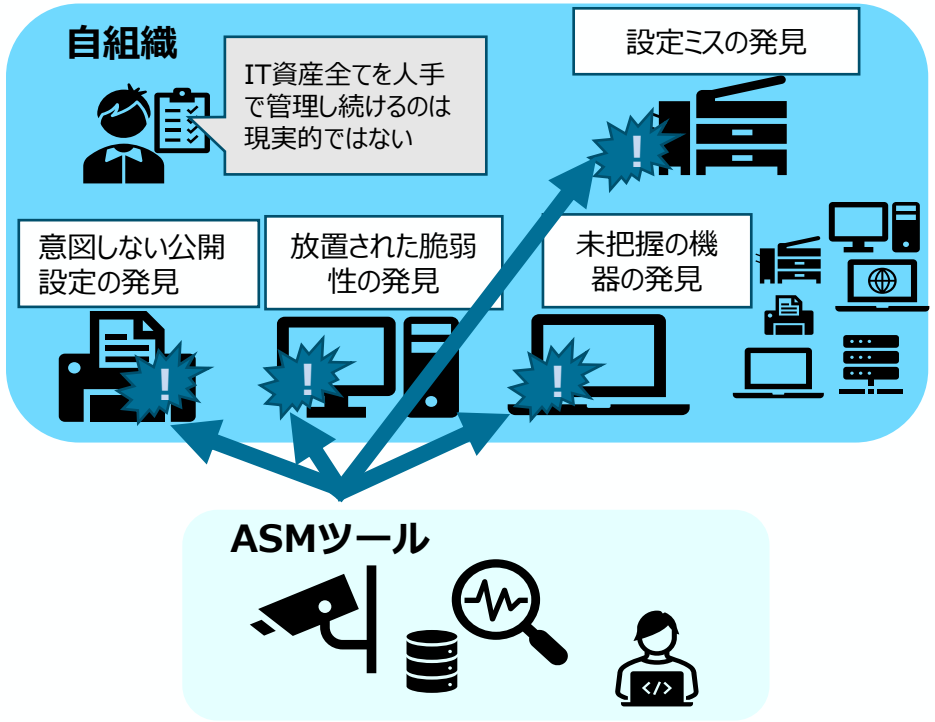
- 経済産業省では、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「**ASM（Attack Surface Management）導入ガイダンス**～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」**を令和５年５月に策定・公表。**

ASMの定義

ASMプロセス

(1) 攻撃面の発見	**企業で保有、管理するIPアドレス・ホスト名の発見** (例) 公開Webサイト、WHOIS情報を利用してドメイン名を特定 など
(2) 攻撃面の情報収集	**攻撃面の情報収集** (例) OS、ソフトウェア、バージョン情報、オープンなポート番号など
(3) 攻撃面のリスク評価	**(2)の収集情報をもとにリスク評価** (例) 公開の既知の脆弱性情報と(2)の収集情報を突合し、脆弱性存在の可能性を識別
リスクへの対応	脆弱性管理と同様の対応 (例) パッチ適用（リスク低減）や対策見送り（リスク受容）など

ASMの特徴



組織の外から機器の情報を収集しデータベース化

工場システムにおけるセキュリティ対策ガイドライン

- 2022年11月に本編、 2024年4月にスマート化を進める上でのポイント（別冊）を公表。

ガイドラインの背景・目的

● 本編　★ 別冊

- 業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」 →**工場セキュリティの底上げが目的。**
- ★ 工場がサイバー空間に密接につながっていく世界、サプライチェーンにおいて取引先に対するセキュリティ対策が要請されている →**先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進する。**

想定する読者の方

- IT関係部門、生産関係部門、監査部門
- 戦略マネジメント部門（経営企画等）
- ★ リスク管理部門、DX担当部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果・読み方

- **工場のBC／SQDCの価値がサイバー攻撃により毀損されることを防止**し、セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。
- ★ **スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるに当たっての留意点や具体例を提示。**

セキュリティ対策企画・導入の進め方

ステップ1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**　セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
  ★ スマート化の目的に照らした業務の広がり
  ★ 業務の広がりに応じたシステム範囲の拡大
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理
  ★ スマート化におけるゾーンごとのセキュリティ要件の考え方
  ★ スマート化により考慮すべき脅威と影響の考え方

ステップ2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策

①ネットワークにおけるセキュリティ対策
  ★ ネットワーク接続における対策
  ★ クラウド利用時の対策
②機器におけるセキュリティ対策
  ★ 汎用品のセキュリティ対策
③業務プログラム・利用サービスにおけるセキュリティ対策
  ★ データ活用・連携における対策

(2)物理面での対策

①建屋にかかわる対策、②電源／電気設備にかかわる対策、③環境(空調など)にかかわる対策、④水道設備にかかわる対策、⑤機器にかかわる対策、⑥物理アクセス制御にかかわる対策

ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルとサプライチェーンを考慮した対策**

(1)ライフサイクルでの対策

①運用・管理面のセキュリティ対策
  A) サイバー攻撃の早期認識と対処(OODAプロセス)
  B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
  C) 情報共有
  ★ スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現
②維持・改善面のセキュリティ対策
  ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
  ・組織　・人材のスキル向上（教育、模擬訓練等）
  ★ スマート化においてPDCAサイクルを実現する上で有効な考え方

(2) サプライチェーン対策

・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認
★ クラウド/汎用品/ソフトウェア 利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

※「ゾーン」とは、業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域

中小企業向けセキュリティ対策

- **中小企業の情報セキュリティ対策ガイドライン（第3.1版 2023年4月）**

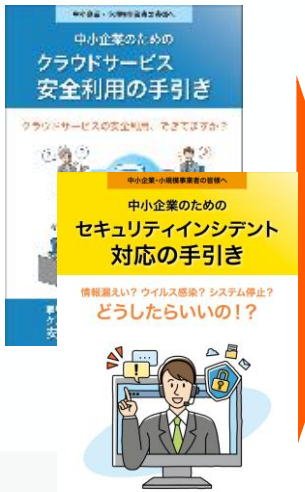
–中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、を実践する際の手順や手法をまとめたもの。付録としてクラウドサービスの安全利用やセキュリティインシデント対応に関する手引きなどがある

中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説
経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説
企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6、8:クラウドサービス安全利用の手引き、セキュリティインシデント対応手引き



【クラウドサービス導入時の考慮ポイントの例】
- ✓ 選択時のポイント（利用業務の明確化、取り扱う情報の重要度確認、クラウドサービスの安全・信頼性確認　等）
- ✓ 運用時のポイント（管理担当者、利用者範囲の決定　等）
- ✓ セキュリティ管理のポイント（利用者サポート体制の確認、利用終了時のデータ確保、適用法令や契約条件の確認　等）

【セキュリティインシデント対応時等の例】
- ✓ インシデント対応の基本ステップ（ステップ１　検知・初動対応、ステップ２　報告・公表、ステップ３　復旧・再発防止）に関する具体例
- ✓ インシデント発生時の相談窓口・報告先　等

- **「SECURITY　ACTION」**

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。30万者を超える中小企業が宣言。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

- **サイバーセキュリティお助け隊サービス**

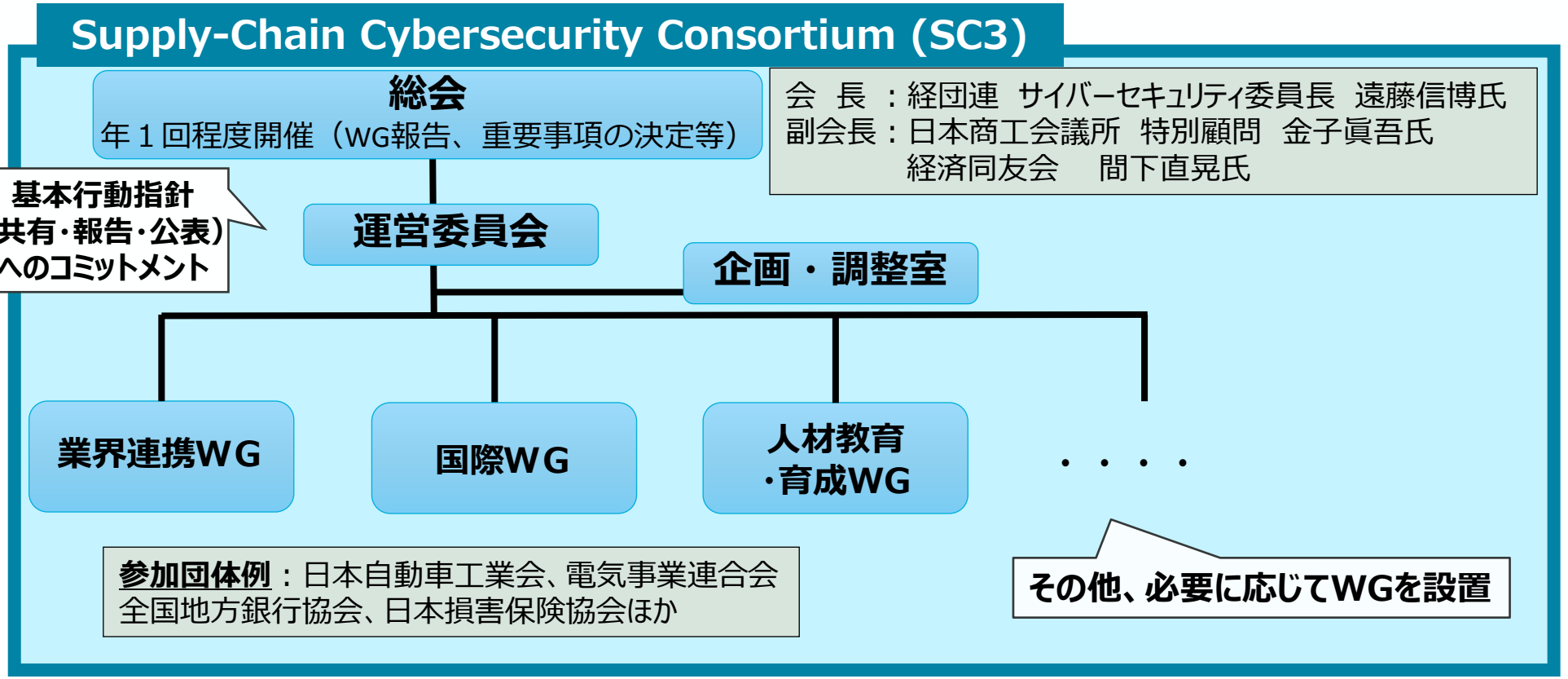
相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。（2024年４月時点で40事業者）

サイバーセキュリティ お助け隊

IT導入補助金に「セキュリティ推進枠」創設

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

- 趣　旨：産業界全体の活動として大企業と中小企業がともにサイバーセキュリティ対策を推進。
- 参加者: 経済団体、業種別業界団体　等（2024年７月時点で１８０会員）
- 設立日: 2020年11月1日（設立総会：2020年11月19日）
- 活　動: 特定の課題についてWGを設置し、具体的アクションを展開。



サイバーセキュリティ人材施策の全体像

- サイバーセキュリティに関する**高度な知見等を有する人材の育成・確保に向けた施策**とともに、セキュリティを本務としない者が業務遂行にあたってセキュリティを意識し、必要十分なセキュリティ対策を実現できる能力を身につける**「プラス・セキュリティ」の取組も推進。**

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

- セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ
- デジタルスキル標準の策定及び普及・
  デジタル人材育成プラットフォームにおける教育コンテンツの提示・実践型教育
- 大学・高専等と産業界の連携

プラス・セキュリティの普及

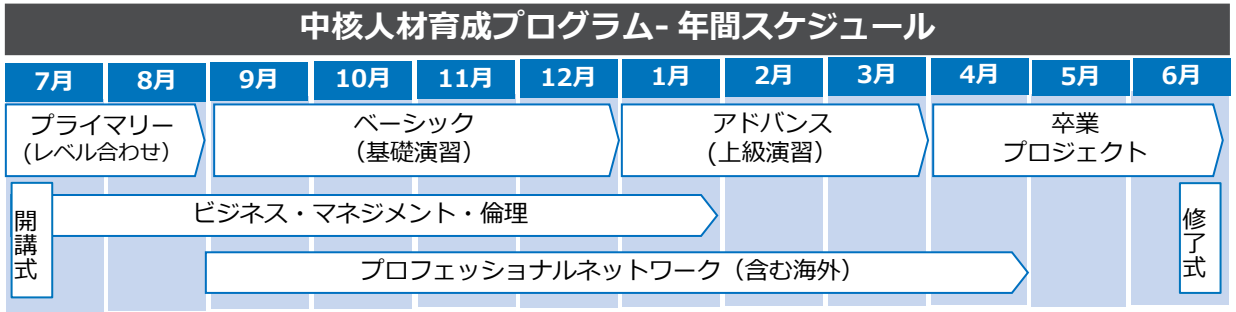
- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人）



- **IT系・制御系に精通した専門人材の育成**
- **模擬プラントを用いた対策立案**
- **実際の制御システムの安全性・信頼性検証等**
- **攻撃情報の調査・分析**

現場を指揮・指導するリーダーを育成

➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

□　米・英・仏等の海外とも協調したトレーニングを実施

など

情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、セキュリティに係る専門的な知識・技能を備えた国家資格として、「情報処理安全確保支援士」**（通称：登録セキスペ）**制度を2016年に創設。2024年４月１日時点の登録者数は22,692人。
- 2020年５月より、**登録に３年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効**する**更新制を導入**。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

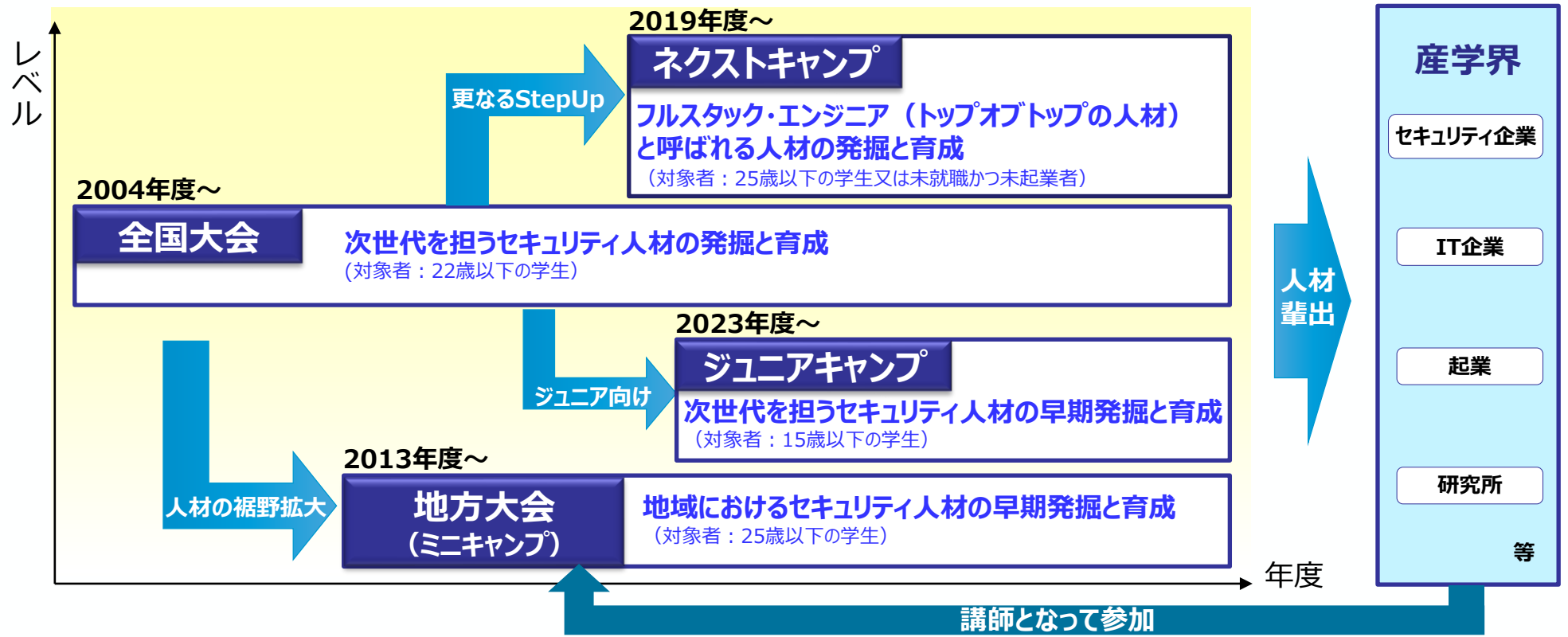
➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
※登録の更新制導入により、義務講習を受講したもののみ登録を更新。

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

セキュリティ・キャンプ

- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラスの人材を創出することが必要。**
- IPAとセキュリティ・キャンプ協議会は、**最先端のサイバーセキュリティ人材を育成・発掘するため「セキュリティ・キャンプ」**を開催。 2004年度以降これまで計で**約1,200名**が修了。



インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より毎年開催。
- 本演習では、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、IPA産業サイバーセキュリティセンターの施設を使用した**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**を実施。

2023年演習の概要

- **日時**：2023年10月9日～13日
- **場所**：IPA文京キャンパス、IPA秋葉原キャンパス、EU代表部
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）
- **参加者**：ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

ハンズオン演習

日米欧専門家による講演

インド太平洋地域参加者間のネットワーキング

※写真は2023年10月の演習の内容

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

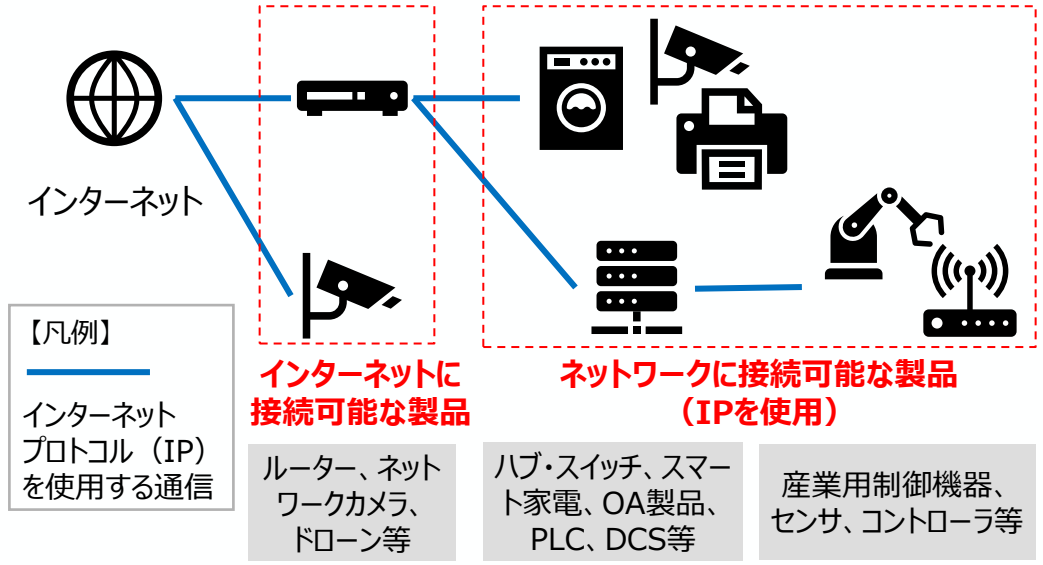
（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

IoT製品に対するセキュリティ適合性評価制度の概要

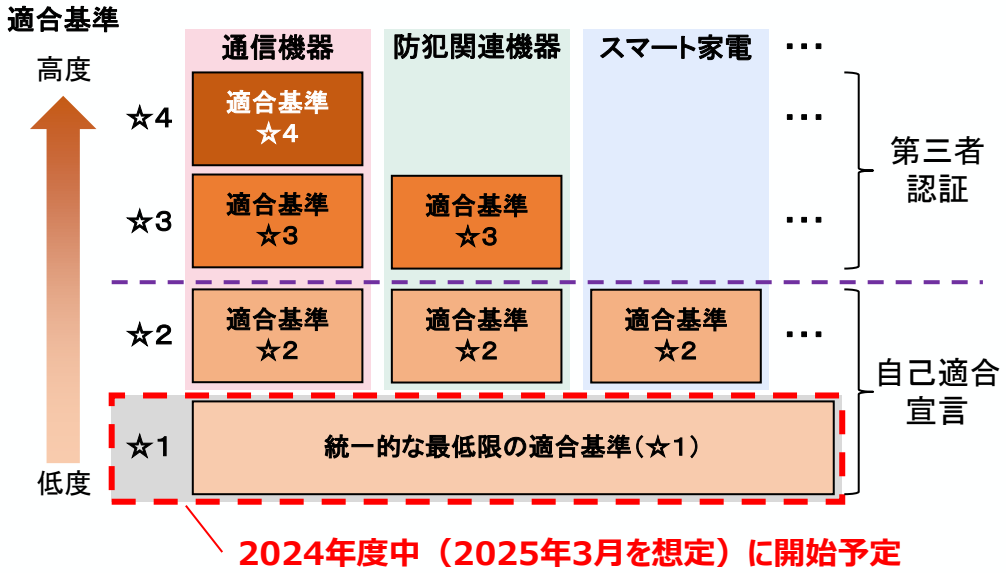
- 2022年11月より「IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会」を開催。2024年3月15日に**最終とりまとめを公開**し、制度構築方針案のパブコメを実施。
- 検討会の最終とりまとめを踏まえ、☆１については**2024年度中の制度開始**を予定。**政府調達等の要件**等とすべく関係省庁と議論中。**米欧等の諸外国との制度調和**を図るため議論中。

対象製品の概要



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

制度の概要



（参考）IoT適合性評価制度について諸外国との比較

- 国内IoT製品ベンダーの負担を抑えるため、諸外国における制度との**相互承認の調整**を図る。
- ☆1開始の正式案内時に**シンガポールと英国とは相互承認の方向性を提示**する予定。**※欧米については、順次方向性を公表**する。

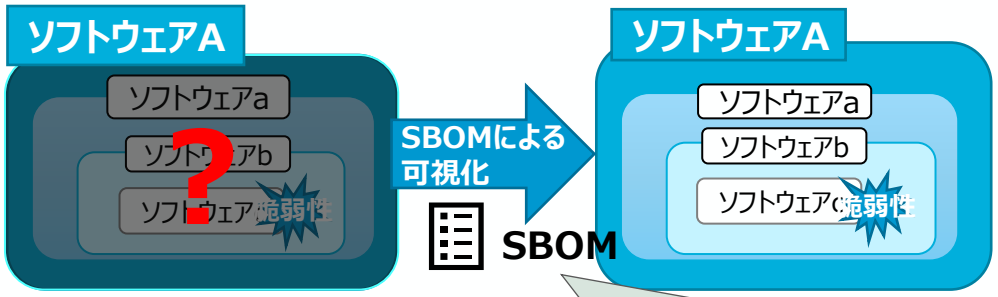
国・地域	日本	シンガポール	英国	米国	EU
制度名	検討中	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunication Infrastructure Act (PSTI法)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA) ※欧州委員会草案の内容
開始時期	• ☆1：2024年度下期(2025年3月)開始予定 • ☆2以上：2025年度以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定	未定 （報告義務を除き2027年開始想定）
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者用無線IoT製品	デジタル製品
適合基準	☆1：ETSI EN 303 645及びCLSの記載内容を中心に検討（ただし、総務省技適の要件、CCDSの要件も参照のほか、事務局にて記載内容を検討）	• ＊1：ETSI EN 303 645の基準の一部(※1) • ＊2：＊2の基準に加え、ETSI EN 303 645の基準の一部(※2) • ＊3及び＊4：＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	• 製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」、「上市後の積極的に悪用された脆弱性・インシデントの報告」等を義務付ける予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意済。発効後、基準策定機関に対して法案に伴う基準の策定が命じられる予定。
評価方法	• ☆1、☆2：自己適合宣言 • ☆3以上：第三者	• ＊1及び＊2：自己適合宣言 • ＊3及び＊4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	• 「重要なデジタル製品」以外の製品：自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（リスクが低い製品）でEUCCやEN規格の対象外の製品及びクラスⅡ（リスクが高い製品）の製品：第三者認証

(※1) ETSI EN 303 645のサイバーセキュリティ規定5.1-1、5.1-2、5.1-3、5.1-4、5.1-5、5.2-1、5.3-2、5.3-3、5.3-7、5.3-8、5.3-10、5.3-13、5.3-16
(※2) ETSI EN 303 645のサイバーセキュリティ規定5.4-1、5.4-2、5.4-3、5.4-4、5.5-5、5.5-7、5.5-8、5.6-1、5.6-2、5.6-4、5.8-2、5.8-3、5.11-1、5.13-1及びデータ保護規定6.1、6.2、6.3、6.5

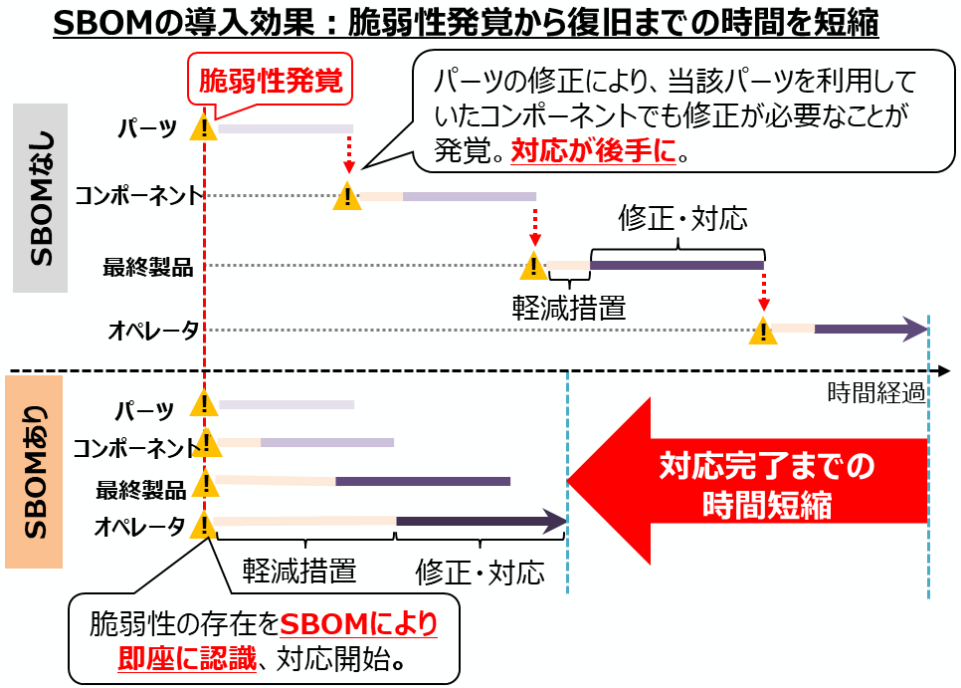
ソフトウェア・セキュリティ確保手段としてのSBOM

- SBOM （Software Bill of Materials）とは、**ソフトウェアの部品構成表**のこと。
- SBOMにより脆弱性情報の即時の特定が可能である一方、その作成効果やコストなどの課題が存在するため、実証による検証を実施。
- 2023年7月、SBOMに関する基本的な情報や導入に向けた実施事項のポイントを示した**「ソフトウェア管理に向けたSBOMの導入手引き」を公表。2024年夏頃に改訂版を公表予定。**

＜SBOMイメージ＞



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	……	…



（参考）ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引　～全体概要～

手引の背景・目的

- ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェアの利用が一般化する中で、ソフトウェアにおける脆弱性管理やライセンス管理の重要性が高まっている。ソフトウェア管理の一手法として、Software Bill of Materials（SBOM：エスボム）を用いた管理手法が注目を集めている。
- 複数の産業分野における実証を通じ、SBOM活用の効果が確認できた。一方、SBOM導入・活用に際しては様々な課題(例：脆弱性管理の効率化、分野や用途に応じたSBOMの適切な範囲、ソフトウェアの調達者と供給者の立場間の取り決め）が存在することが明らかとなった。
- 本手引では、**SBOMに関する「基本的な情報」や「誤解と事実」を提供し、**企業のSBOM導入を支援するために、**SBOM導入に向けた主な実施事項及び認識しておくべきポイント**を示す。(ver1.0)
- 加えて、ソフトウェアの脆弱性を管理する一連プロセスにおいて**SBOMを効果的に活用するための具体的な手順と考え方**、SBOM導入の効果及びコストを勘案して**SBOMを導入することが妥当な範囲を検討するためのフレームワーク**、ソフトウェアの受発注において、**調達者と供給者の間でSBOMに関して契約に規定すべき事項（要求事項、責任、コスト負担、権利等）について参考例**を示す。(ver2.0)

対象読者

- 主にパッケージソフトウェアや組込みソフトウェアに関する **ソフトウェアサプライヤー**
  - ✓ ソフトウェア開発・設計部門
  - ✓ 製品セキュリティ担当部門（PSIRTなど）
  - ✓ 経営層
  - ✓ 法務・知財部門

SBOM導入の主なメリット

- **脆弱性管理のメリット**
  - ✓ 脆弱性残留リスクの低減
  - ✓ 脆弱性対応期間の低減
  - ✓ 脆弱性管理にかかるコストの低減
- **ライセンス管理のメリット**
  - ✓ ライセンス違反リスクの低減
  - ✓ ライセンス管理にかかるコストの低減
- **開発生産性向上のメリット**
  - ✓ 開発遅延の防止
  - ✓ 開発にかかるコストの低減
  - ✓ 開発期間の短縮

SBOM導入に向けたプロセス(ver1.0)

フェーズ1	環境構築・体制整備	● 1-1. SBOM適用範囲の明確化 ● 1-2. SBOMツールの選定 ● 1-3. SBOMツールの導入・設定 ● 1-4. SBOMツールに関する学習
フェーズ2	SBOM作成・共有	● 2-1. コンポーネントの解析 ● 2-2. SBOMの作成 ● 2-3. SBOMの共有
フェーズ3	SBOM運用・管理	● 3-1. SBOMに基づく脆弱性管理、ライセンス管理等の実施 ● 3-2. SBOM情報の管理

脆弱性管理プロセスの具体化(ver2.0)

- SBOMを活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、**SBOMを活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要。**
- 脆弱性管理の一連プロセスにおいてSBOMを効果的に活用するための**具体的手順と考え方をまとめることで、SBOM活用による効果を高めるための参考情報**を提供。

SBOMを活用した脆弱性管理プロセス

フェーズ1　脆弱性特定
- マッチング手法区分選択
- 利用可能なSBOMデータ特定
- 脆弱性DBの選択
- マッチング手法の選択・作成

フェーズ2　脆弱性対応優先度付
- 予備フィルタリング
- 優先度付情報の選択・取得
- 判断ツリーに基づくカテゴリ判定
- 優先度スコア評価

フェーズ3　情報共有
- 共有情報と共有相手の特定
- 共有方法の特定と実施

フェーズ4　脆弱性対応
- 脆弱性の暫定対応
- 脆弱性の根本対応

SBOM対応モデル(ver2.0)

- SBOM導入の効果及びコストを勘案してSBOMを導入することが**妥当な範囲を検討するためのフレームワーク(5W1Hを網羅するよう体系化)**。
- 実証を通じて、**医療機器、自動車、ソフトウェア製品等の分野**において、コスト・効果を考慮して妥当な対応範囲の参考例を提示。
- 当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できる。

SBOM取引モデル(ver2.0)

- ソフトウェア部品の受発注において、調達者と供給者の間でSBOMに関して**契約に規定すべき事項（要求事項、責任、コスト負担、権利等）**について参考となる例を示す。
- 既存のソフトウェアに関するモデル契約書と組合せることで、**SBOMに対応した契約書を作成する際の項目案を提示**するもの。

日米豪印（Quad（クアッド））第５回首脳会合について

- 2023年5月20日、第５回日米豪印（「Quad（クアッド）」）首脳会合を広島で対面開催。
- 会合後、**４カ国は共同声明を発出。サイバーセキュリティ等での新たな協力**が記載された。

首脳共同声明（サイバーセキュリティ部分抜粋）

- 我々は、より安全なサイバー空間と、全ての人々のためになる国際デジタル経済を促進することへのコミットメントを再確認する。**日米豪印パートナーは、サイバー事案及び脅威への地域の能力及び強靱性を高めるため、引き続き協働する**。
- 地域のサイバー人材の能力向上支援を継続、サイバーセキュリティの啓発を目的とした**「日米豪印サイバー・チャレンジ」**の実施を歓迎。
- ソフトウェアの開発、利用、政府調達に係るセキュリティ向上を奨励する**「ソフトウェア・セキュリティに関する日米豪印共同原則」**及び**「重要インフラのサイバーセキュリティに関する日米豪印共同原則」**の発表を歓迎。

ソフトウェアセキュリティに関する共同原則（抜粋）

ソフトウェアベンダーによる安全な開発の実践に関する原則

安全なソフトウェア開発手法が実践されたソフトウェアを調達するため、当該手法を実践することを政府方針に取り入れるとともに、**ソフトウェアベンダーに対して、当該手法の実践を推奨**することを目指す。

- **組織の準備**：安全なソフトウェア開発手法を実践するため、適切な教育を受けた人材、プロセス、技術を適切に整備する。
- **ソフトウェアと開発環境の保護**：ソフトウェアに含まれるコンポーネントを、改ざんや不正アクセスから適切に保護する。また、ソフトウェアは、リリースされたバージョンごとに管理し、バージョンごとに使用されているコンポーネントの詳細情報（**SBOM等**）やサプライチェーン情報を適切に管理する。
- **安全なソフトウェアの開発**：脆弱性を最小限に抑え、セキュリティに関するテストを経て十分なセキュリティを備えたソフトウェアをリリースする。
- **脆弱性への対応**：ソフトウェアに存在する脆弱性を特定し、特定した脆弱性に適切な対処を行い、同様の脆弱性が今後発生することを防止する。

（出典）外務省HP：https://www.mofa.go.jp/mofaj/fp/nsp/page1_001702.html

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

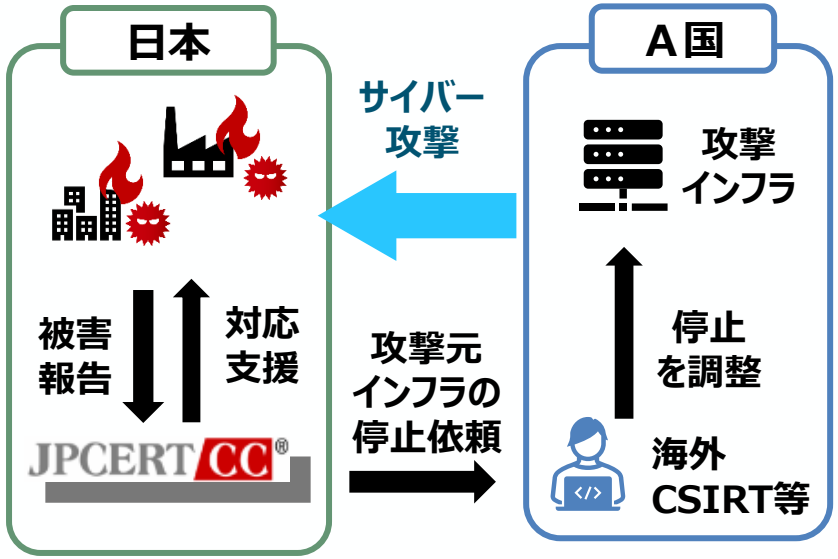
（６）今後のサイバーセキュリティ政策の方向性

サイバー被害に関する対応支援・国際調整窓口等の実施

- **JPCERT/CC※は、民間の非営利団体（一般社団法人）として、1996年から活動を実施。**
  ※Japan Computer Emergency Response Team / Coordination Center
- **我が国の調整窓口として1998年から機能し、国際的な認知度・信用度も高い。**

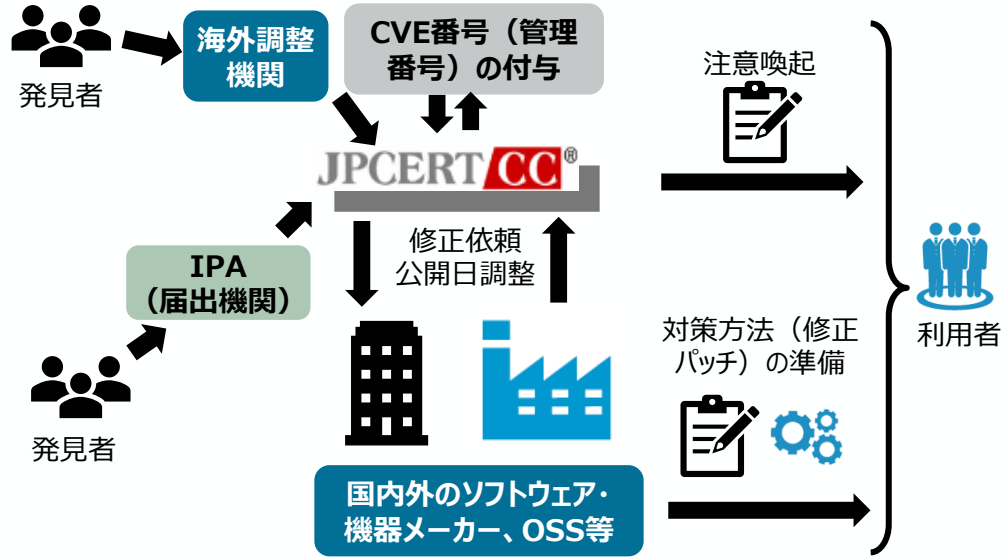
事案対応支援、国際連携強化・調整業務

- 幅広い事業者等において発生したあらゆるインシデントへの初動対応支援や啓発活動を実施。
- 国境を越えてくるサイバー攻撃については、信頼関係に基づき、各国窓口CSIRT間で、攻撃インフラとなっているサーバの停止について調整。



ソフトウェア等の脆弱性対応

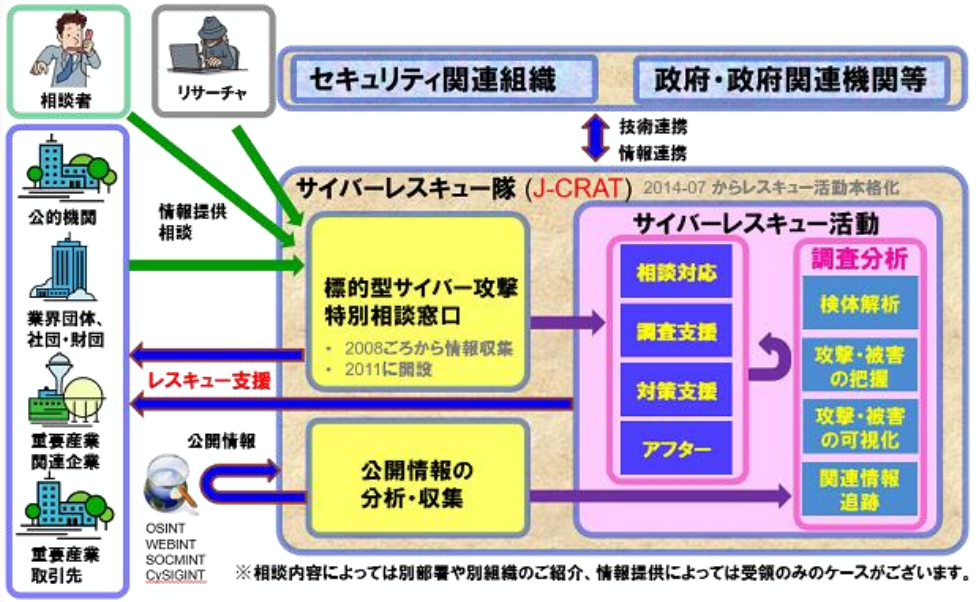
- 脆弱性が発見された場合、対策を講じずに脆弱性の情報を公表すると、攻撃者に悪用されるおそれがあることから、メーカーや主たる利用者と調整し、対策方法を準備した後に公表。
- 事業者（特に組織内PSIRT等）への脆弱性対応枠組みの周知。



IPA サイバーレスキュー隊（J-CRAT） ※2014年７月発足

- 広く一般から相談や情報提供を受付け、提供された情報を分析して調査結果による助言を実施。
- **標的型サイバー攻撃の被害の発生が予見**され、その**対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織**や、**標的型サイバー攻撃の連鎖の元となっていると推測される組織**などに対し、レスキュー活動にエスカレーションして支援。

活動イメージ



活動実績

	2014年度	2015年度	2016年度	2017年度	2018年度	2019年度	2020年度	2021年度	2022年度
相談件数	107	537	519	412	413	392	406	375	330
レスキュー支援数	38	160	123	144	127	139	102	94	163
オンサイト	11	39	17	27	31	20	17	9	43

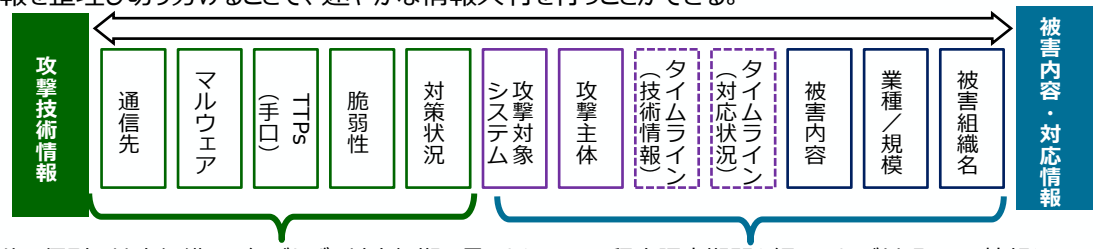
（出典）IPA「サイバーレスキュー隊J-CRAT（ジェイ・クラート）について」 https://www.ipa.go.jp/security/j-crat/about.html

サイバー被害に係る情報共有ガイダンス

- **被害組織の担当部門**（例：セキュリティ担当部門、法務・リスク管理部門等）**を主な想定読者**とし、被害組織を保護しながら、いかに速やかな情報共有や目的に沿ったスムーズな被害公表が行えるのか、**実務上の参考となるポイントFAQ形式で整理。**

どのような情報を？（様々な種類・性質の情報が存在）

情報を整理し切り分けることで、速やかな情報共有を行うことができる。



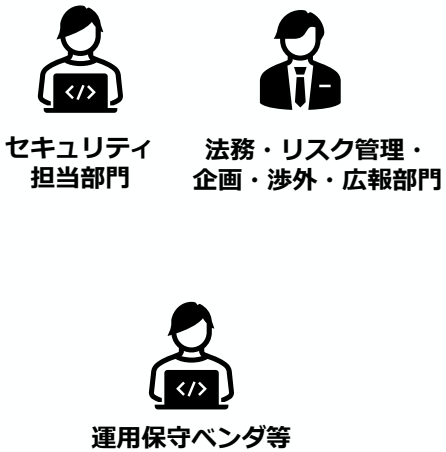
基本的に個別の被害組織には紐づかず、対応初期で見つかりやすく、早期に情報共有しなければ効果を得られない情報

ある程度調査期間を経なければ判明しない情報や、ステークホルダー等との調整が必要な機微な情報などが含まれるため、公表までに時間がかかる情報

どのタイミングで？（サイバー攻撃への対処の時系列を意識）

どのような主体と？（様々なサイバーセキュリティ関係組織が存在）

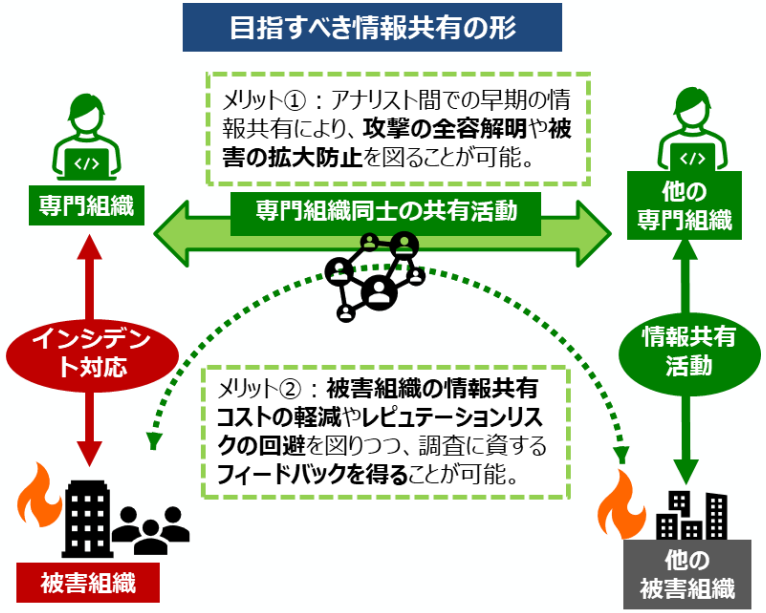
想定読者（被害組織等）



サイバー被害情報の情報共有の更なる促進に向けた対応
（専門組織間の情報共有）

- サイバー攻撃が高度化する中、攻撃の全容の把握や被害の拡大を防止する等の観点から、**被害組織を直接支援する専門組織を通じたサイバー被害に係る情報の速やかな共有が重要。**
- これまで、**被害組織における情報共有・公表**及び**専門組織を通じた速やかな情報共有**について、それぞれの組織において**実務上参考となるガイダンスや手引き等を整備**。今後、これら成果物に関し**専門組織やユーザー企業の経営層への意識啓発も含めた周知・啓発活動を行う。**

＜参考＞専門組織を通じた速やかな情報共有の促進に向けた対応



- 最終報告書において、**被害組織の同意を個別に得ることなく専門組織間で速やかに情報共有することが可能な情報として「攻撃技術情報」※を整理**し、そうした考え方に基づく専門組織間での円滑な情報共有を提言。
  ※通信先情報やマルウェア情報などから被害組織が推測可能な情報を非特定化したもの。
- 最終報告書の**提言を補完する２つの文書**（以下①②）**を提示。**
  ① 専門組織向けに、**効果的な共有対象となる情報や非特定化加工の方法**といった専門組織同士の情報共有における論点について、複数のユースケースも用いつつ解説した**手引き**
  ② 被害組織と専門組織が共通の認識を持ち、情報共有について合意するための**秘密保持契約に盛り込むべきモデル条文**
- さらに、最終報告書では、専門組織同士の情報共有促進だけでは解消されない**今後の課題として、情報共有に向けた官民連携のあり方 、サプライチェーンにおけるベンダ等の役割について提言。**

（参考）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の概要

１．情報共有の重要性と現状の課題

- サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。そのため、**攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要。**他方で、被害組織自らが情報共有を行うことについては、①被害組織側の調整コスト負担、②最適者が事案対応を行わない懸念、③処理コストのかかる情報共有、④被害現場依存の脱却の必要性などの課題が存在。

２．本検討会における提言

- **被害組織を直接支援する専門組織を通じた速やかな情報共有の促進が重要。**これにより、①全体像の解明による被害拡大の防止や②被害組織のコスト低減などが実現できる。
- 他方で、専門組織を通じた情報共有を促進するためには、**①秘密保持契約による情報共有への制約、②非秘密情報からの被害組織の特定/推測の可能性の課題に対応をする必要がある。**
- このため、本検討会では、これらの課題を乗り越え、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有を可能とするために、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の**「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得る**と整理。
- さらに、本報告書の提言を補完する観点から、**「攻撃技術情報の取扱い・活用手引き（案）」についてもとりまとめ。**本手引きでは、専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えばよいか、またどのように情報共有をおこなえばよいのかなど**専門組織として取るべき具体的な方針について整理。**
- 加えて、円滑な情報共有を促進すべく、上記考え方について**ユーザー組織と専門組織が共通の認識**を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく**法的責任を原則として負わないことを合意するための秘密保持契約に盛り込むべきモデル条文案を提示。**今後、本検討会の成果の**周知・啓発に取り組む。**

３．今後の課題

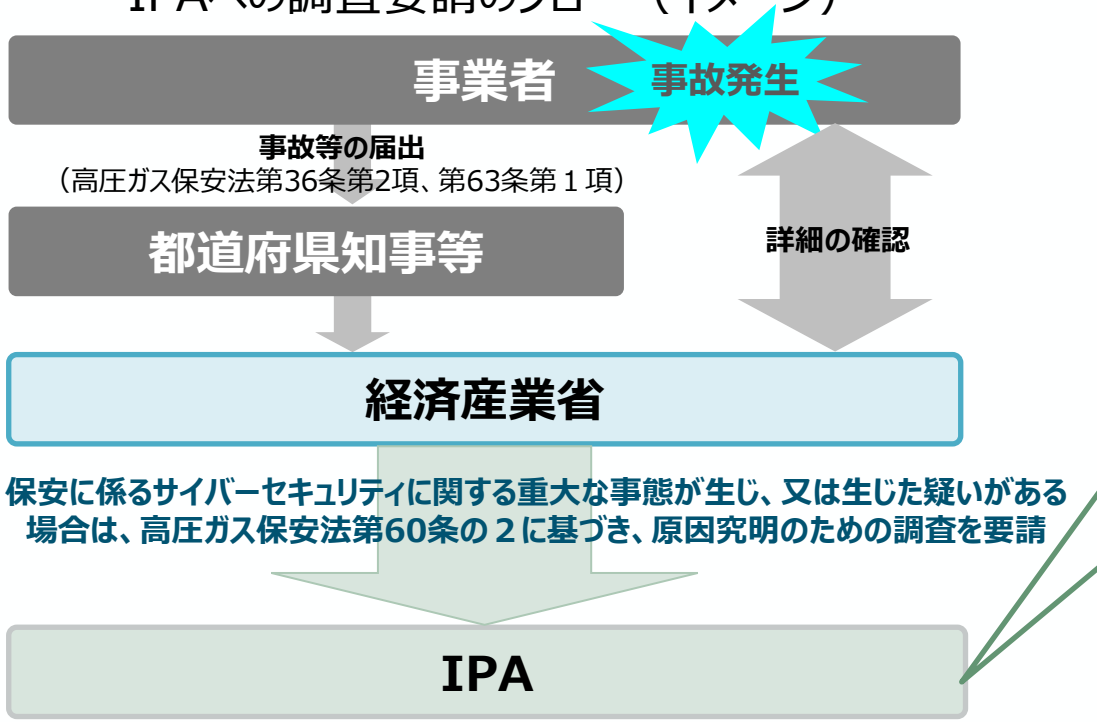
- 専門組織同士の情報共有促進だけでは解消されない**今後の課題**としては、**（１）情報共有に向けた官民連携のあり方**（行政機関への相談・報告のあり方や政府と民間事業者間の情報の共有など）、**（２）サプライチェーンにおけるベンダ等の役割**を挙げた。

保安に係るサイバーインシデントに関する事故調査の実施

- 令和４年に公布された改正保安３法に基づき、**サイバーセキュリティに関する重大な事態が生じ、又は生じた疑いがある場合**には、経産大臣は、**IPAに原因究明調査を要請。**
- 事故調査は、**原因究明による再発防止を目的に実施**。調査結果を踏まえ、サイバーセキュリティ水準の向上を図るための対策を講じることを想定。

※令和５年12月21日の施行に伴い、IPAにおいて体制を整備。

IPAへの調査要請のフロー（イメージ）



IPAによる調査のイメージ

- ✓ IPAは対象システムのログ等を確認することによって、サイバーセキュリティに関する重大な事態が生じた原因を究明するための調査を行う。
- ✓ IPAによる調査は、書面審査と現地調査の二段階で構成する。
  ※ただし、書面調査のみで十分に原因を特定できた場合には、現地調査は行わない。
- ✓ 調査日数や調査内容等は、IPAと事業者で相談の上、決定する。

改正高圧ガス保安法（抄）
第六十条の二　経済産業大臣は（中略）**保安に係るサイバーセキュリティ（中略）に関する重大な事態が生じ、又は生じた疑いがある場合**において、必要があると認めるときは、**独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。**

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

先進的サイバー防御機能・分析能力強化のための研究開発

- 経済安全保障重要技術育成プログラムにおいて、**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７月から研究開発を開始。**

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

情報セキュリティサービス審査登録制度

- 情報セキュリティサービス業の普及を促進し、**国民が情報セキュリティサービスを安心して活用することができる環境を醸成することを目的**として、**一定の技術・品質要件を定めた「情報セキュリティサービス基準」を経済産業省が2018年より策定**し、基準に適合する**サービスのリストをIPAが公開中**（2023年12月時点で300サービスが登録中）。

<情報セキュリティサービスにおける課題>

どの事業者のサービスを選べば良いかわからない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

我が社のサービスを もっと見つけて欲しい

我が社の技術力、サービス 品質をアピールしたい

ベンダー
サービス提供事業者

審査を受けリストに掲載

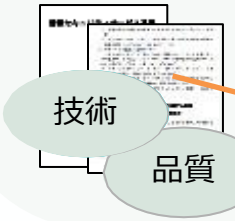
○情報セキュリティサービス基準適合 サービスリスト（IPA）：審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

選定時に活用

基準を満たした300サービスを掲載

- 情報セキュリティ監査（68サービス）
- 脆弱性診断（135サービス）
- ペネトレーションテスト（侵入試験）（2024年9月審査開始）
- デジタルフォレンジック（38サービス）
- セキュリティ監視・運用（51サービス）
- 機器検証 （8サービス）

（2023年12月現在）



○情報セキュリティサービス基準（METI）

上記６サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

1. サイバーセキュリティを取り巻く現状

2. 政府全体の体制と方向性

3. 経済産業省のサイバーセキュリティ政策

（１）経済産業省のサイバーセキュリティ政策の全体像

（２）サプライチェーン全体での対策強化

（３）国際連携を意識した認証・評価制度等の立上げ

（４）政府全体でのサイバーセキュリティ対応体制の強化

（５）研究開発の促進・サイバーセキュリティ産業振興

（６）今後のサイバーセキュリティ政策の方向性

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た実効性の強化、国産製品の開発・普及促進や高度人材の育成・確保**、サイバー安全保障の実現に向け**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。　※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。

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）

認証基準策定

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

需要側：工場　電力

・セキュアな製品の調達
・事案対処能力強化
・・・etc

需給の相互連関を通じたエコシステムの構築・セキュリティ産業の発展

供給側

研究開発促進・SU創出

検証・市場化支援・信頼性確保

高度人材の育成・確保（情報処理安全確保支援士の活用促進等）

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。

J-CSIP　サイバーセキュリティ お助け隊

情報集約

IPA 情報集約・分析・トリアージ

初動対応支援　情報提供

被害組織　政府機関等

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

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

- **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。
- 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。

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

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

- 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

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

- 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、**半導体関連産業におけるサイバーセキュリティ対策を進めることが重要。**
- **必要な政策を模索するため実態把握・調査等**を進め、サイバーセキュリティ対策への取組、問題意識や事例、脅威情報を**相互に共有できる場を設置**する。さらに、具体化した対策を**経済産業省の投資促進関係施策の要件等との紐付け等**も検討し、**実効性を強化**する。

半導体セキュリティの直近の動向

海外の動向

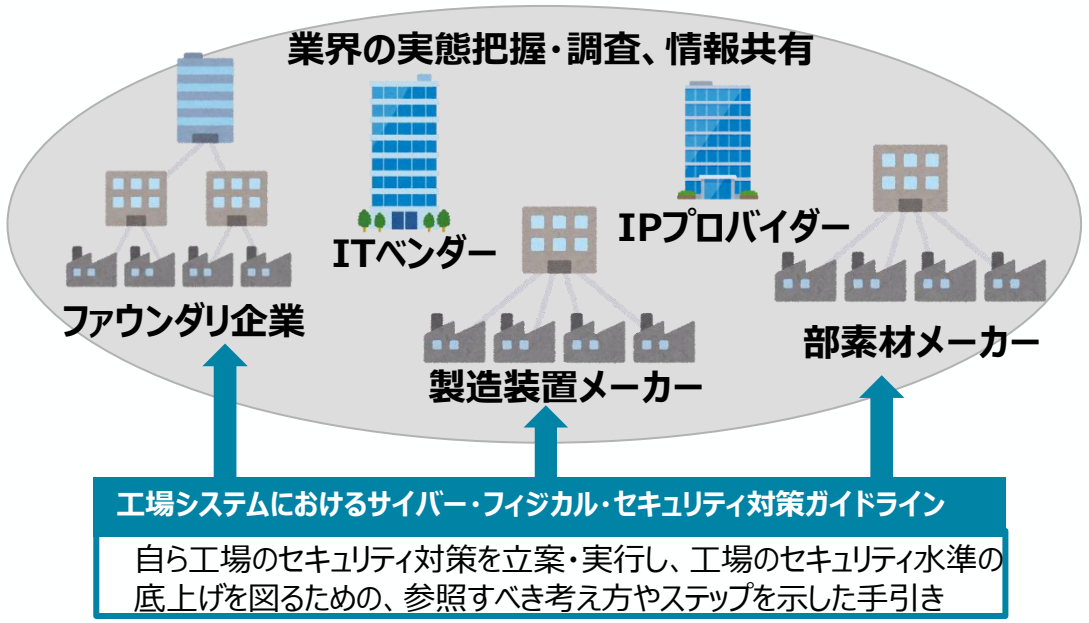
- TSMCは、2018年に主力工場がランサムウェアの被害に遭い生産停止を余儀なくされ、影響額は最大190億円に及んだ。
- 2023年に半導体装置のセキュリティ規格であるSEMI E187を調達要件化。SEMI E187の要件を満たしていることを、認証機関によって証明されたサプライヤーも出現。

（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

半導体関連産業全体でのセキュリティ水準の底上げ



（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

中小企業等向けの支援の一層強化

- サプライチェーン全体のセキュリティ対策強化には、**中堅レベルでは事業継続に耐えうるレジリエンスを確保、小規模レベルでは経営層が最低限の危機管理の認識を持つ**ことが必須。
- 一方、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との課題**を抱える中小企業等に対しては、**適切なセキュリティ対策のあり方を提示**し、**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、予算や人材が不足する中小企業が、**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**することが必要。

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。**
  - 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。
  - **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。
  - **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。

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

我が国サイバーセキュリティ産業の振興に向けた強化策の検討

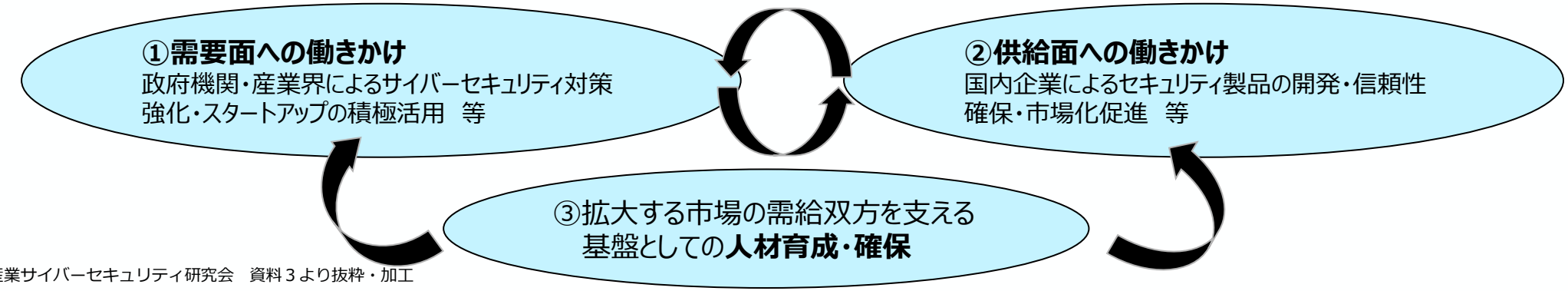
問題意識

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

目指すべき姿

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

＜「セキュリティエコノミー」好循環のイメージ＞

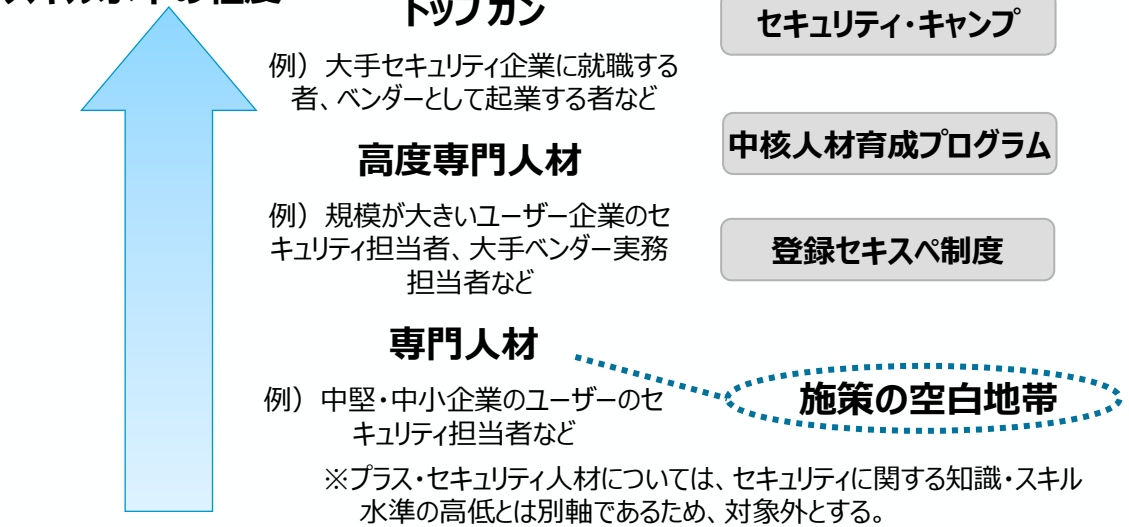


（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

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

- セキュリティ人材不足は、企業の規模に関わらない、共通の課題。今後は、**高度専門人材向けの育成を継続して実施**するとともに、**ユーザー企業や地域ベンダー等における専門人材の育成・確保についても議論**する必要。
- セキュリティ人材が**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。

人材育成施策の現状（仮説）



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

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。

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

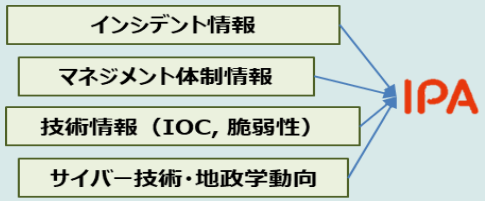
IPAにおけるサイバー情勢集約・分析能力の強化

- 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

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

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、**デジタル時代の社会インフラを守る**との観点から、*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。

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、
実務者がこれまでの取組を継続するだけでは対応困難になっています。

●**組織幹部のリーダーシップの下**、**対策の強化に努める**とともに、
被害を受けた場合の適切な対応をお願いします。

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html