経済産業省

# 経済産業省のサイバーセキュリティ政策について（サプライチェーン対策評価制度を中心に）

2025年2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．経済産業省のサイバーセキュリティ政策

３．サプライチェーン対策評価制度

# サイバー攻撃を行う主体について

## ①国家の支援を受けたグループ（APT（Advanced Persistent Threat）攻撃グループ）

- 執拗に高度で継続的な攻撃を行うことが特徴（つまり、ミッション達成優先でコスト度外視の攻撃集団）。インテリジェンス企業によれば、攻撃グループのバックについている国として中国、ロシア、北朝鮮、イランが挙げられている。

## ②サイバー犯罪組織（クライム（Crime）系）

- 情報等を盗んで現金化するグループ。2018年の被害総額は60兆円に達したという調査結果もあるようで、既に一大市場となっており、攻撃用ツール制作・販売、攻撃起点の時間貸しなど、様々な犯罪サービスの分業化が進展。

## ③ハクティビスト

- 「アクティビスト（社会活動家）」と「ハッカー」を掛け合わせた言葉で、サイバー攻撃を通じて社会的・政治的メッセージを発信していくことを主眼とした活動を行うグループ。アノニマスもハクティビストと捉えられることが多い・

## ④悪意のある個人（愉快犯、腕試し等）

- 趣味や研究の延長として個人が行う攻撃で、子供が行っているケースも少なくない。ただし、②の攻撃用ツールを使ったりしているうちに犯罪グループの活動に取り込まれているようなことも。

## ⑤産業スパイ

- 知的財産の窃取を目的とした攻撃グループ。

※実態は、上記のようにきれいに分類することは困難。例えば、普段はクライム系として活動しているグループが、要請に応じて“傭兵”となってAPT攻撃グループとして働いている可能性が指摘されている。

# 主なサイバー攻撃事案

## ①個人情報や機微技術情報などの情報窃取

- **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。

## ②ランサムウェア攻撃などにより金銭窃取

## ③データ改ざんやフェイク情報拡散などを通じた意思決定への影響

- **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事業活動の停止

- 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）
- KADOKWAグループはランサムウェアを含むサイバー攻撃を受け、大量の個人情報等の流出に加えて、**ニコニコ動画の約2ヶ月間利用不可になるなど事業継続にも影響**（2024年6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

- 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）
- 名古屋港において、ランサムウエア攻撃によるシステム障害が発生。**約3日間コンテナの搬入・搬出が停止**（2023年７月）
- ファイブ・アイズ5か国等は中国背景とされるサイバー攻撃グループVolt Typhoonが**有事における機能不全を念頭に重要インフラへの事前のアクセスを確保を目的としたサイバー攻撃が発生**していると注意喚起（2023年5月）。

# 最近のサイバー攻撃の動向（事前配置(pre-positioning)活動）

2023年５月、ファイブ・アイズ５か国及びマイクロソフト社が、中国背景とされるサイバー攻撃グループVolt Typhoonについて、注意喚起を発出。概要以下のとおり。

- 有事における機能不全を念頭に置いた、**重要インフラへの事前のアクセス確保**（pre-positioning）を目的としたサイバー攻撃が発生

- 長期間の潜伏に必要な**高度な検知回避能力**が特徴
  - ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
  - ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使（Living off the Land）
  - ✓ 侵入痕跡となるログの消去 等

- 米国においては、本土及び島嶼部の米軍基地にサービスを提供する重要インフラ（通信、エネルギー、水道など）への攻撃の脅威が高まっている


（出典）サイバー安全保障分野での対応能力の向上に向けた有識者会議第1回資料より抜粋
PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024.2) 等

# 地政学とサイバー脅威

- サイバー攻撃が国家の戦略ツールとして使われつつあり、地政学的情勢とサイバー攻撃は密接に関係

## ■物理的な紛争に伴うサイバー攻撃

- ロシアのウクライナ侵攻に伴うインフラへのサイバー攻撃（ハイブリッド戦争）（2022年）
- イスラエルとハマスの軍事衝突に伴うハッカー集団によるサイバー攻撃の応酬（2024年）
- レバノンのシーア派組織ヒズボラのポケベル同時爆発（1000人以上負傷）（2024年）
- 南シナ海の領域争いに関連するフィリピンへのサイバー攻撃の急増（政府機関のシステムへの侵入等）（2024年）

## ■機微技術情報や国家機密を狙う諜報活動

- 三菱電機へのサイバー攻撃（2019年）により、て防衛関連の情報のデータファイル2万件が流出した恐れ（2019年）
- ロシア政府を背景とする組織がSolarWinds社のシステムへのサプライチェーン攻撃により、米国連邦政府含めて膨大な数のシステムにバックドアが仕掛けられる（2020年）
- JAXAのサーバに対して複数回サイバー攻撃。個人情報や外部企業との契約などが流出した恐れ（2024年）

１．サイバーセキュリティを取り巻く現状

**２．経済産業省のサイバーセキュリティ政策**

３．サプライチェーン対策評価制度

# 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）

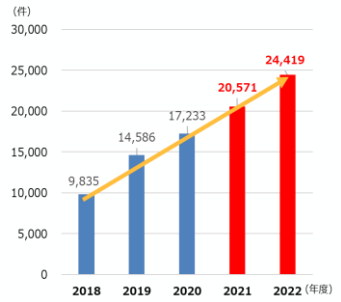
## ②国際連携を意識した認証・評価制度等の立上げ

- 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）**



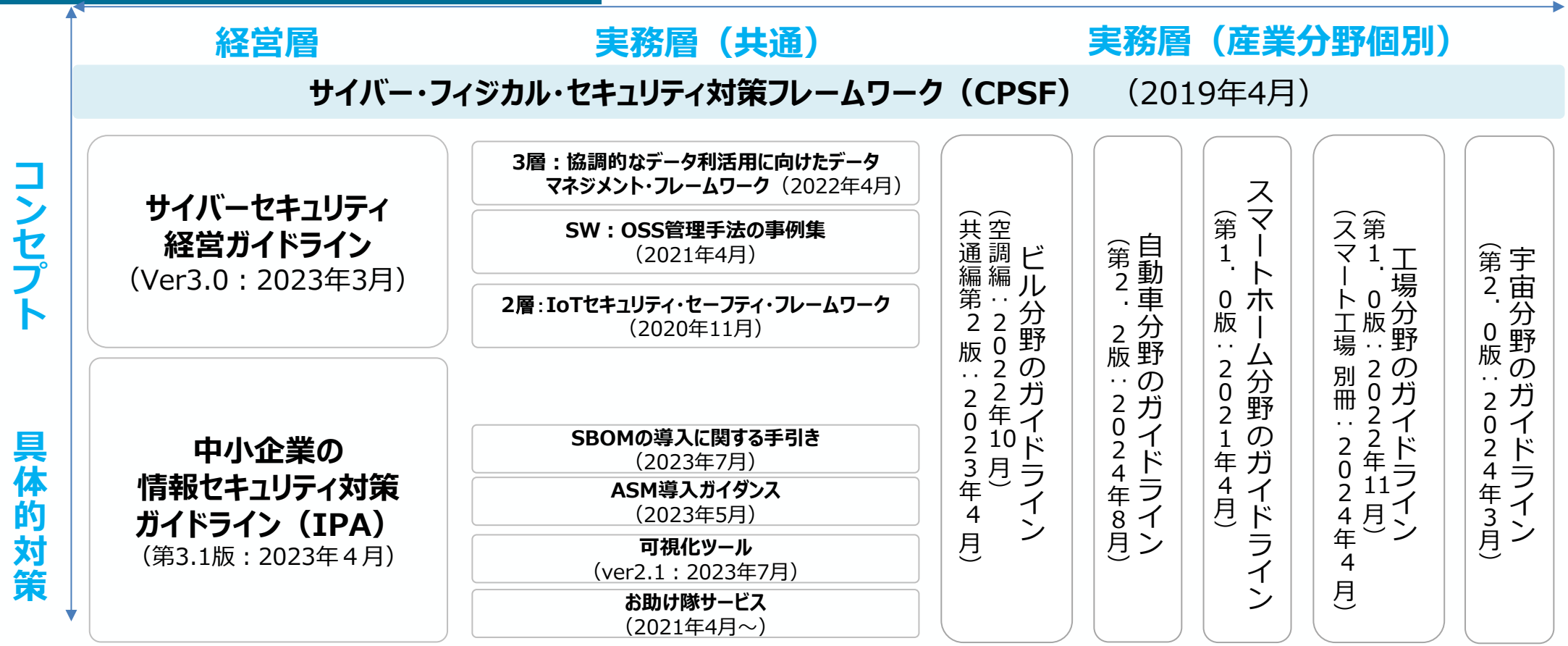

## ④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 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

# 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



# （参考）サイバー・フィジカル・セキュリティ対策フレームワーク

- 2019年4月に「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>**

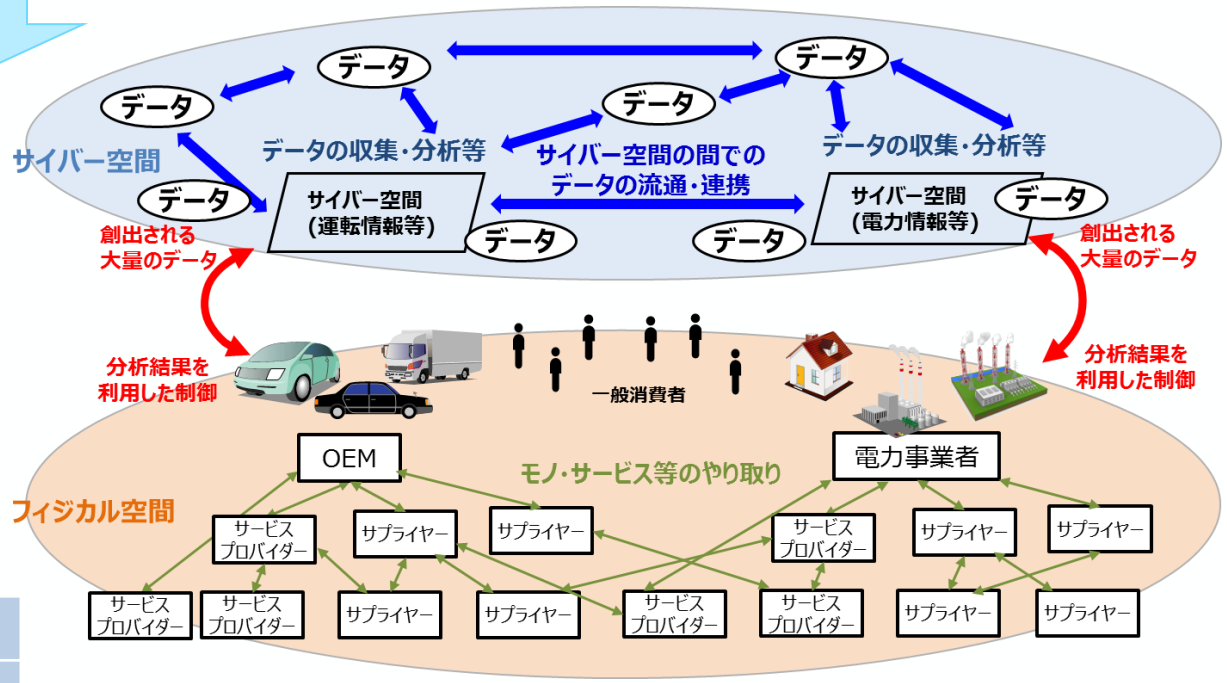
**【第３層】**
**サイバー空間におけるつながり**

**【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**

# サプライチェーン強化に向けたセキュリティ対策評価制度の検討

- **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<br>・・・・ | ・重要インフラ行動計画<br>・・・・ |
| 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

（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

１．サイバーセキュリティを取り巻く現状

２．経済産業省のサイバーセキュリティ政策

**３．サプライチェーン対策評価制度**

# サプライチェーンに起因するサイバーインシデント事例

## サプライチェーンからの情報漏洩リスク

✓通信サービス企業が、委託先企業の従業員が所持するPCがマルウェアに感染したことを契機として、第三者による不正アクセスを受け、利用者情報等約44万件の漏えいがあった旨を発表。その後の調査で従業員等約8万件の個人情報漏えい（可能性含む）も判明。（2023年11月、2024年2月）

## サプライチェーンからの不正侵入等リスク

✓公立病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生し、緊急以外の手術や外来診療が一時停止する等、２か月以上にわたって通常診療ができない状況に。（2022年10月）

## サプライヤーの停止による事業継続リスク

✓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）

✓米石油パイプライン大手がランサムウェア攻撃を受け、全ての業務を一時停止。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。（2021年5月）

✓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）

## ソフトウェアを通じたサプライチェーンリスク

✓クラウドサービス提供事業者のデータセンターのサーバーが不正アクセスされ、ランサムウェアに感染。データが暗号化され、一時サービス提供ができなくなった。（2023年6月）

# サプライチェーン対策評価制度に関する現状整理（案）①

- 本年3月に制度構想を示して以降、これまで本SWGを2回開催。また、IPAがSC3の下に「サプライチェーンサイバーセキュリティ成熟度モデル検討SWG」を立ち上げ、これまで4回検討会を開催。これまでの議論を通じて、以下の通り制度の概要を整理（個別論点については、年度末を目途とする中間取りまとめに向けて引き続き検討）。

**【現状認識（制度検討の背景）】**

- 近年、**サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発**。その対策として、政府や重要インフラ企業のみならずその取引先に対しても適切なセキュリティ対策を課す必要があるが、**複雑なサプライチェーン下で、様々な取引先から様々な要求事項を求められている**状況。**発注企業にとっては、正しいセキュリティ対策が取引先でなされているか不明確／受注企業にとっては（特に中小企業を中心に）過度な負担につながっている**。結果として、サプライチェーン全体のセキュリティ底上げにつながっていない。

**【制度趣旨】**

- **ビジネスサプライチェーン・ITサービスサプライチェーン**における、**取引先へのサイバー攻撃を起因とした情報セキュリティリスク／製品・サービスの提供途絶や取引ネットワークを通じた不正侵入等のリスクに対するセキュリティ対策の成熟度を確認する**（※1）。
- **2社間の契約における発注企業が、受注側に適切な段階（★）を提示し取得を促す**（**再委託先は発注者から見た対象にはならない**（※2））。

（※1）本制度で対象としているのは、あくまで企業体の中におけるセキュリティ対策であり、組織のガバナンス・取引先管理、自社IT基盤への検知・防御等、組織全体に影響が及ぶ範囲を対象としており、ソフトウェア開発やIoT機器のセキュリティを対象にした評価制度・取組とは目的が異なるため、**求められる対策内容や効果も基本的に異なる**。

（※2） **再委託先のセキュリティ対策は、委託先を通じて必要に応じて管理**することも想定（一部基準項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを想定）

**【目指す効果】**

- **サプライチェーンにおけるリスクを対象**にした上で（※）、その中での立ち位置に応じて必要な対策を提示することで、**企業の対策決定を容易・適切なものにする**。すべてのサプライチェーン企業が対象となるが、特に**サプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい**と想定。

（※）**本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましい**が、リソースに限りのある**中小企業を中心にただちにこれを実現できていない企業が一定数存在**する。本制度は、**包括的なリスク分析に基づき共通して求められる対策を示す**もの。将来的には、こうした企業も**より自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい**。

# サプライチェーン対策評価制度に関する現状整理（案）②

**【基準の考え方】**

- 求められるセキュリティ対策について、**各企業のサプライチェーンにおける重要性や影響度を踏まえた上で、複数区分（★3～5）に分ける**ことを想定。具体的には、**①ビジネス観点（データ保護・事業継続における重要度）②システム観点（接続の有無）の二点で整理**。
- これらの考え方や、**海外での類似制度（英Cyber Essentials）や他産業のガイドライン（自工会・部工会ガイドライン、他分野別ガイドライン等）の記載**を踏まえつつ、NISTの「サイバーセキュリティフレームワーク2.0」等にも基づき、「ガバナンス整備、取引先管理、リスクの特定、システムの防御、攻撃等の検知、インシデントの対応・復旧」の観点から、**★3・4の考え方、対策事項・要求項目について整理**を行った。
- **★3は基礎的なシステム防御策と体制整備を中心に構成**。**★4はガバナンスから防御・検知・対応まで包括的な対策**とすることを想定。

（※） ★5については、より高いレベルの対策としては、前述の通り自社やサプライチェーンに対するリスクアセスメントの考え方が求められるため、**各企業におけるリスクに応じて対策を講じることを求めるISMS適合性評価制度との制度的整合性も含めて、位置づけ・基準を検討。**

**【国内外の関連制度等との連携・整合】**

- 先行する自己評価の仕組みである**「SECURITY ACTION」「自工会・部工会ガイドライン」**や前述した国際標準である**「ISMS適合性評価制度」**とは、**相互補完的な制度として発展することを目指す**。
- 具体的には、**現在の★3・4の要求項目案は自工会・部工会ガイドラインとも対応**しており、自工会・部工会ガイドラインに基づく自己評価に際しての本制度での活用等、**連携のあり方については、運営団体とも議論を進めていく**。また、**海外の類似制度**についても、**将来的な相互認証の可能性も念頭に、引き続き調査・意見交換を実施**する。

# サプライチェーン対策評価制度に関する現状整理（案）③

**【制度において設ける段階の考え方】**

| | ★3 | ★4 | ★5（※） |
|---|---|---|---|
| 想定される脅威 | • 広く認知された脆弱性等を悪用する**一般的なサイバー攻撃** | • **供給停止**等によりサプライチェーンに**大きな影響**をもたらす企業への攻撃<br>• 機密情報等、**情報漏えい**により**大きな影響**をもたらす資産への攻撃 | • **未知の攻撃**も含めた、**高度なサイバー攻撃** |
| 対策の基本的な考え方 | • 全てのサプライチェーン企業が**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に実施 | • サプライチェーン企業等が**標準的に目指すべきセキュリティ対策**として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策**を実施 | • **高度なサイバー攻撃にも対応可能なセキュリティ対策**として、**リスクベースのアプローチ**に基づく改善プロセスを整備した上で、**リスクに応じて必要な対策**を実施 |
| 脅威に対する達成水準（イメージ） | • **組織内の役割と責任が定義**されている。<br>• 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。<br>• インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。 | • セキュリティ対策が**組織的な仕組みに基づいて実施され、継続的に改善**している。<br>• **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。<br>• **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。 | • **リスクアセスメントの結果**を踏まえ、**システムへの具体的な対策の実装や状況把握に基づく改善プロセスの運用**がなされている。<br>• 組織における**マネジメントシステムが確立**されている。 |
| 評価スキーム | **自己評価**<br>（※）記入内容については、専門家が問題ないか評価を実施 | **第三者評価** | **第三者評価（★4と同等）** |
| ベンチマーク<br>（対象企業やリスクが同様であり、対策項目を検討する上で参考） | • 自工会・部工会ガイドLv1<br>• Cyber Essentials<br>⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出 | • 自工会・部工会ガイドLv2～3<br>• 分野別ガイドライン 等<br>⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出 | • ISO/IEC27001 等<br>（※）各企業におけるリスクに応じて対策を講じることを求める**ISMS適合性評価制度との制度的整合性も含めて、位置づけ・基準を検討** |

# 本制度の推進にあたって必要な検討事項

| 事項 | 論点 | 検討の方向性 |
|---|---|---|
| ①企業に対する働きかけ①（発注企業のためのルール整備） | • 制度を活用すること（取引先に対する対策の要請）が、下請法等の既存のルールに抵触しないか、わかりやすく示す必要。 | • これまで、経産省・公正取引委員会によるガイドライン（「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」）等が示されているが、これらの既存の取組も踏まえた上で検討を進める必要。 |
| ②企業に対する働きかけ②（取得企業に対する支援） | • 中小企業に対しては、これまで「サイバーセキュリティお助け隊」を通じて安価で利用可能なサービスが提供されてきたが、お助け隊でカバーされない対策が求められるのか。<br>• お助け隊のみならず、中小企業が対応するにあたって、専門人材等の人的リソースが不足している懸念点も考えられるが、どのようなアプローチを行うのか。 | • 中小企業からは、下記のような懸念を持つことを想定。<br>①対策項目を踏まえてどのような対応を行えばよいかわからない<br>②金銭的／人員的リソースが不足している<br>• これらについて、「サイバーセキュリティお助け隊」や登録セキスペの拡張・活用等も含め、必要な対策を講じる。 |
| ③企業に対する働きかけ③（制度普及にあたっての初期ターゲットの設定） | • 今後、本制度の普及を進めていく中で、どのような業界で優先的に進めていくべきか。どのような考え方で決めるべきか。<br>• また、当該業界において普及を進める際、どのような施策を講じることが効果的か。 | • 政府機関や重要インフラ分野、主要製造業が想定されるが、詳細についてはSC3下での検討会でも議論の上、今後本SWGでも提示予定。 |
| ④制度の導入促進にあたっての環境整備 | • 企業が本制度を取得する上で、評価機関や検証事業者、助言専門家（例：登録セキスペ）等の環境整備が必要になるが、その確保のためにどのような取組を行うべきか。 | • SC3下での検討会でも議論の上、今後本SWGでも提示予定。 |
| ⑤制度の運用体制 | • 評価スキームをどのように構築すべきか。また、制度を運営していくにあたり、運営主体や認定機関はどういった者が望ましいか。 | • 評価スキームについてはSC3下の検討会で議論を行い、海外制度も踏まえ、★3を自己評価／★4は第三者評価とする形で検討中。<br>• その上で、制度運営者に必要な機能・体制をSC3下の検討会でも議論した後、本SWGでも提示予定。 |