サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ①

実務層向け

- 最近の国内外の動向を踏まえ、**特に以下の取組を強化していただきたい**（詳細は次ページ以降）。
  - ※ 経済産業省が策定した実務担当者向けガイドライン（被害情報共有・公表ガイダンス等）や関係制度（JC-STAR等）概要など各種政策文書については、次ページ以降のリンクや経済産業省ウェブサイトを参照いただきたい。

1．セキュア・バイ・デザイン等の実践

- 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**」や「**セキュア・バイ・デフォルト**」**の製品の購入**（例えば、**JC-STARのラベル取得製品**）**を優先する**など、**ＩＴサービス・製品等提供事業者に対してセキュリティ慣行を求める**
- ＩＴサービス等を外部委託する際には、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よう必要な人材を確保する**

2．サプライチェーン全体での対策強化に向けた対応

- VPNなど**自組織の**不正侵入経路となりうるポイントを把握する上で**有効な対策**とされるASM（Attack Surface Management）等の外部サービスを活用する
- 特に大企業においては、サプライチェーンに参加する中小企業等への助言・支援を行う（**「サイバーセキュリティお助け隊サービス」などの支援施策の紹介**、**対策状況調査・改善に向けた対話等**）

3．被害時の専門組織等への情報共有

- 「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
- 特に、国家支援型と推定される標的型サイバー攻撃の場合には、まずは警察やIPAなどの相談窓口に相談する

経済産業省「サイバーセキュリティ政策」

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ②

実務層向け

- 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（例えば、JC-STARのラベル取得製品）を優先する**など、**ＩＴサービス・製品等提供事業者に対してセキュリティ慣行を求める**
- ＩＴサービス等を外部委託する際には、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よう必要な人材を確保する**

※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。

趣旨・背景・補足

- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が追うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。2023年10月に我が国を含む13か国が共同署名した**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンス**の中でも、**ユーザ組織（顧客）への提言も含まれているところ、今後、当該提言を踏まえたユーザー組織における対応が全世界レベルで求められていくことが想定される**。
- 経済産業省では、本文書も踏まえ、**「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」**を2025年3月に公表したところ。この中で、ユーザー組織（顧客）に求められる責務として、リスク管理とセキュアなソフトウェアの調達・運用についても提示している。加えて、**IoTセキュリティ適合性評価制度（JC-STAR）を構築・2025年３月に制度運用開始**し、セキュアなIoT製品を容易に選択できる環境整備を進めているところ。引き続き、各企業・団体が上記メッセージをより具体的に理解し、実践しやすい環境を整備していく。
- ITサービス・製品等提供事業者に対してセキュリティ慣行を求めることに関して、外部委託契約書等に、**セキュリティインシデント発生時の連携体制**や、**契約違反時の具体的なペナルティ**（損害賠償、契約解除の条件等）を**明文化**することも考えられる。

関係する政府文書・窓口等

- 内閣サイバーセキュリティセンター「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年10月）
- 経済産業省／内閣サイバーセキュリティセンター「サイバーインフラ事業者に求められる役割等に関するガイドライン案」（2025年3月）
- IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ③

実務層向け

- VPNなど**自組織の**不正侵入経路となりうるポイントを把握する上で**有効な対策**とされるASM（Attack Surface Management※）等の外部サービスを活用する

※ASM（Attack Surface Management）：組織の外部（インターネット）からアクセス可能なIT資産（=攻撃面）を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスをいう。

趣旨・背景・補足

- サプライチェーン全体での対策を強化する上で、まずは自社のセキュリティ対策を確認・強化することが第一歩である。例えば、経済産業省の「サイバーセキュリティ経営ガイドライン」では、PDCA サイクルによるサイバーセキュリティ対策の継続的改善の重要性に触れており、必要に応じて、**目的に応じた脆弱性診断やペネトレーションテスト、情報セキュリティ監査等の外部サービスを利用する**といった対策例を示している。
- また、DXの進展等に伴い**サイバー攻撃の起点が増加する中**で、外部（インターネット）から把握できる情報を用いてIT資産の適切な管理を可能とする**ASMは**、VPN（Virtual Private Network）などの不正侵入経路となりうるポイントを把握する上で**有効な対策**とされている。経済産業省が公表している「ASM（Attack Surface Management）導入ガイダンス」などを参照することができる。

関係する政府文書・窓口等

- 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」
- 経済産業省「『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～』を取りまとめました」（令和５年５月）

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ④

実務層向け

- 特に大企業においては、サプライチェーンに参加する中小企業等への助言・支援を行う（**「サイバーセキュリティお助け隊サービス」などの支援施策の紹介**、**対策状況調査・改善に向けた対話等**）

趣旨・背景・補足

- サプライチェーン全体のセキュリティ対策水準を強化するためには、自社のサプライチェーン上にある（＝取引先である）、**中小企業等におけるセキュリティの確保も求められる**。「サイバーセキュリティ経営ガイドライン」においても、以下の対策例が掲げられている。
  - サプライチェーン上での対策の底上げの手段として、「サイバーセキュリティお助け隊」等の中小企業向け施策を活用する
    ※　「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。約7,000件の利用実績（2024年９月末時点）がある。IT導入補助金「セキュリティ対策推進枠」を活用することで、最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助を受けられる。
  - サプライチェーンにおけるサイバーセキュリティ対策を担保する手段として、**第三者による評価検証結果を活用する**（認証制度の活用、助言型外部監査の実施等）
- さらに、中小企業庁「パートナーシップ構築宣言取組事例集Ver1.2」においても、**サプライヤー向けの対策状況調査（アンケート調査）・フィードバック（リスクの解説や改善方法のヒント提供）**に努めている事例も掲載されており、**取引先とのパートナーシップ構築**の観点からも、こうした取組を参考とすることが有用。
- なお、取引先に対してサイバーセキュリティ対策を要請するケースも想定されるが、その際、独占禁止法等**関係法令の適用関係**が論点となる。こうした課題に対応するため、経済産業省と公正取引委員会は、2022年10月に、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表したところ。現在、関係省庁と連携して、**更なる具体化（事例や解説の提示等）に向けた検討**を進めており、発注者・受注者双方が良好な関係を構築してサプライチェーンのセキュリティ対策強化に取り組むことを促していく。
- 経済産業省としては、今後も**「サイバーセキュリティお助け隊サービス」の継続的な見直し**など、中小企業向け**支援策を強化**していく。

関係する政府文書・窓口等

- 中小企業庁「『パートナーシップ構築宣言』ポータルサイト」
- 経済産業省「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」（令和４年10月）
- 経済産業省「中小企業のサイバーセキュリティ安心サービスのご紹介」
- 中小企業庁「中小企業の情報セキュリティ」
- IPA「ここからセキュリティ！」
- IPA「中小企業の情報セキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

サイバーセキュリティを実践する各企業・団体（実務層）の皆様へ⑤

実務層向け

- 「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
- 特に国家支援型と推定される標的型サイバー攻撃の場合には、まずは警察やIPAなどの相談窓口に相談する

趣旨・背景・補足

- サイバー攻撃が深刻化・巧妙化するなど、サイバーリスクが高まる中、**どのような企業・団体においても**、自組織がサイバー攻撃の被害に遭った場合に**適切なハンドリング（インシデント対応）を行うことが**、**一層重要な状況**。
- インシデント対応の一環として、被害組織がサイバーセキュリティ関係組織（被害組織を直接支援する専門組織等）と**サイバー攻撃被害に係る情報を共有することは、攻撃の全容を解明する観点から重要**。政府機関や専門組織からは、報告したことによる不利益が生じないような配慮を前提として、**関連する情報の提供や対応に関して助言を受けることなども期待**できる。また、自組織が受けたサイバー攻撃被害の状況や対応内容について、**適切なタイミングで対外的に公表することは**、利害関係者からの信頼を確保し**当該企業・団体のレピュテーションを保護する観点からも重要**。ただし、国家支援型と推定される標的型サイバー攻撃を受けた場合には、サイバー対処能力強化法の趣旨も踏まえ、対応についてまずは政府機関に相談することが、被害組織・政府機関の双方にとって、状況把握の観点から望ましい。
- こうした背景の下、2023年３月に経済産業省及び関係省庁等にて実務者向けのガイダンスを公表したところ。当該ガイダンスでは、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をFAQ形式で整理しており、サイバー攻撃の被害時における情報共有・公表の在り方として参考**となる。
- また、サイバーセキュリティ経営ガイドラインの**付録C「サイバーセキュリティインシデントに備えるための参考情報」**でも、インシデントにおいて経営者が行うべき事項や組織内で整理しておくべき事項を提示しており、一つの参照点となり得る。
- 経済産業省では、これら文書の周知・啓発活動に加え、**IPAやJPCERT/CCを通じた被害組織への情報提供・初動対応支援**を行っている。政府全体としても、被害組織の負担軽減と政府の対応迅速化を図るため、インシデント**報告様式の一元化**等にも取り組んでいる。

関係する政府文書・窓口等

- サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月）
- サイバーセキュリティ経営ガイドラインの付録C「サイバーセキュリティインシデントに備えるための参考情報」（令和５年３月）
- 個人情報保護委員会「漏えい等の対応とお役立ち資料」
- 警察署又は都道府県警察本部「相談窓口」
- 経済産業省サイバーセキュリティ課（代表：03-3501-1511　内線：3964）
- IPA 「コンピュータウイルス・不正アクセスに関する届出」「企業組織向けサイバーセキュリティ相談窓口」
- JPCERT/CC「インシデント対応依頼」
- 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「サイバー安全保障分野での対応能力の向上に向けた提言」（令和６年11月）