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。

（参考）産業界へのメッセージに対応した政府文書・窓口等

- 各企業・団体向け

①関係

- 経済産業省「サイバーセキュリティ経営ガイドライン　Ver3.0」（令和５年３月改訂）
- 経済産業省「デジタル・ガバナンス・コード2.0」（令和４年９月改訂）
- 経済産業省「価値共創ガイダンス2.0」（令和４年８月改訂）

②関係

- 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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

③関係

- 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「『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）
- 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「中小企業のサイバーセキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

④関係

- 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「情報セキュリティ安心相談窓口」「コンピュータウイルス・不正アクセスに関する届出」「J-CRAT 標的型サイバー攻撃特別相談窓口」
- JPCERT/CC「インシデント対応依頼」

- ＩＴサービス等提供事業者向け
  - 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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）
- サイバー被害組織を直接支援する専門組織向け
  - 経済産業省「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　報告書等」（令和６年３月）

産業界へのメッセージ（１）（背景）

- サイバーリスクの高まりや米欧等の動向を背景に、**我が国においても一層の対策強化が求められる状況**。
- 経済産業省では、**これまでの施策の一層の普及・啓発**や**新たな取組**を進め、**不断にその見直し**もしていく。
- 他方で、**産業界における積極的な取組も不可欠**。そのため、次頁以降で、**各主体に向けたメッセージを提示**。

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	こうしたデジタル技術の取扱いに当たっては、サイバーセキュリティの確保は必須。
世界的な地政学リスクの高まり	特定の国や地域における地政学的な問題が、企業活動上のリスクとなりつつある。危機管理対応の中でサイバーセキュリティ上のリスクも考慮した対応が求められる。（※１）
サイバー攻撃の深刻化・巧妙化（※２）	サイバー攻撃による事業の停止や情報の漏えい等、企業の信用を毀損する事例が多発。企業経営を行う上でこうしたサイバー攻撃の高度化への対応は必須。
米欧等での制度整備活発化	グローバルに活動する企業や海外企業と取引する企業にとっても、こうした制度整備への対応が必要。

（※１）経済安全保障推進法に基づく基幹インフラの安定的な提供の確保に関する制度が令和６年５月17日より運用開始。特定重要設備の導入時等にサイバーセキュリティの観点を含む国の事前審査が特定社会基盤事業者に対し義務付け。

（※２）「相対的に 露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。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も平素から行われている。」（国家安全保障戦略（令和４年12月16日閣議決定））

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。**我が国においても一層の対策強化が求められる状況**。

経済産業省としての取組

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・啓発に取り組みながら**、①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、②サイバーセキュリティ供給力の強化、③官民の状況把握力・対処能力向上、それぞれに向けた**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**。

産業界における積極的な取組

組織幹部による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**も進めながら、当省のサイバーセキュリティ政策の方向性に沿った**積極的な取組を行っていただくことも不可欠**。

次頁以降で、**それぞれの主体**（※）**に向けたメッセージを提示**。

（※）
- 各企業・団体
- ＩＴサービス等提供事業者（機器やサービス等を提供する事業者）
- サイバー被害組織を直接支援する専門組織（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）

産業界へのメッセージ（２）（各企業・団体向け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（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**ことをお願いしたい。

趣旨・背景

- 米国においてサイバーセキュリティに関するリスク管理や戦略、ガバナンスに係る年次開示等が義務付けられ、また、我が国においても企業のサステナビリティ情報開示が義務化されるなど、**企業におけるサイバーセキュリティに関する取組が、（企業価値に結び付くものとして）資本市場により評価される時代**となってきている。
- すなわち、企業においては、**サイバーセキュリティ対策を、中長期的な企業価値向上に向けた「投資」として捉え、利害関係者に対して積極的に開示すること等が、一層求められる状況**となる。
- 経済産業省が2023年３月に改訂した「サイバーセキュリティ経営ガイドライン」においても、**サイバーセキュリティ対策を「投資」**（将来の事業活動・成長に必須な費用）**と位置付けることの重要性について言及**しており、サイバーセキュリティ経営の重要項目の一つとして、「サイバーセキュリティに関する情報の収集、共有及び開示の促進」を掲げているところ。本文書で示した考え方は、各企業等にとって一つの参照点となり得る。
- 今後、経済産業省としては、**外部から各企業等の対策状況を判断することが難しい**といった課題等に対応するため、関係省庁とも連携しながら、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、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**。

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　Ver3.0」（令和５年３月改訂）
- 経済産業省「デジタル・ガバナンス・コード2.0」（令和４年９月改訂）
- 経済産業省「価値共創ガイダンス2.0」（令和４年８月改訂）

産業界へのメッセージ（３）（各企業・団体向け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**ことをお願いしたい。

  ※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。

- 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**ことをお願いしたい。

趣旨・背景

- 「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4月に米国サイバーセキュリティー・インフラセキュリティー庁（CISA）が一部有志国と共に**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を作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した。同年10月に本文書が改訂され、我が国を含む13か国が共同署名。**当該文書には、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**。

- 今後、経済産業省としても、本文書も踏まえ、**ソフトウェア開発者が行うべき取組整理など推進のための取組を検討**していく予定。その中で、**ユーザ組織（顧客）が行うべき取組も提言する**ことで、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。

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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

産業界へのメッセージ（４）（各企業・団体向け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**すること（ ASM（※）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））をお願いしたい。 ※ 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。
- **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**も検討することをお願いしたい。

趣旨・背景

- サイバーセキュリティ対策不足の企業がサプライチェーン上に存在することは、大きなリスク。サプライチェーン全体での対策を更に強化するためには、資金的な余力の観点等から大企業と同じような対策を講じることが難しい**地域の中小企業等における**一定水準以上の**セキュリティの確保が必須**。
- こうした観点から、経済産業省と公正取引委員会は、 2022年10月に、中小企業等におけるサイバーセキュリティ対策を支援するための施策と、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、整理を実施。**こうした整理も参照しつつ、サプライチェーンに参加する中小企業等への共助を実践することが重要**。
- また、経済産業省が2023年３月に改訂した「サイバーセキュリティ経営ガイドライン」において、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。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、こうした**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）こと も有用。
- さらに、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**、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**とされており、これを実施することも、サプライチェーン全体での対策を強化する上で効果的と考えられる。
- 今後、経済産業省としては、中小企業等に対して、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、**「サイバーセキュリティお助け隊サービス」の拡充**をはじめ、**支援策を一層強化**していく。

関係する政府文書・窓口等

- 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「『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）
- 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「中小企業のサイバーセキュリティ」
- IPA「サイバーセキュリティお助け隊サービス制度」

産業界へのメッセージ（５）（各企業・団体向け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**等を行うことをお願いしたい。

趣旨・背景

- 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**。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**。
- 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では、サイバー攻撃を受けた**被害組織がサイバーセキュリティ関係組織とサイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス**を公表。
- 当該ガイダンスは、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形式で整理したもの**。
- 今後、経済産業省として、本ガイダンスについて、**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・啓発活動を進めていく**。

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）
- 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「情報セキュリティ安心相談窓口」「コンピュータウイルス・不正アクセスに関する届出」「J-CRAT 標的型サイバー攻撃特別相談窓口」
- JPCERT/CC「インシデント対応依頼」

産業界へのメッセージ（６）（ＩＴサービス等提供事業者向け）

- **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」**（※１）**や「セキュア・バイ・デフォルト」**（※２）**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。

※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

- 「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4月に米国サイバーセキュリティー・インフラセキュリティー庁（CISA）が一部有志国と共に**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を作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した。同年10月に本文書が改訂され、我が国を含む13か国が共同署名。その中でも、組織の変革を実行できる**経営層の意思決定者による**、製品開発の重要な要素としてセキュリティを優先させるという**コミットメントの重要性**が言及されている。**今後、当該提言を踏まえた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**。
- 今後、経済産業省としても、本文書も踏まえ、**ソフトウェア開発者が行うべき取組整理など推進のための取組を検討**していく予定。それにより、ITサービス等提供事業者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。

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「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

産業界へのメッセージ（７）（被害組織を直接支援する専門組織向け）

- 「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。

趣旨・背景

- 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**。
- 経済産業省では、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、**被害組織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**し、検討会の最終報告書として2023年11月に公表。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。
- その補完文書として、①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良いかなど**専門組織として取るべき具体的な方針について整理した「攻撃技術情報の取扱い・活用手引き」**と、②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、経済産業省として、これらの成果物について、**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**とともに、**情報を共有する専門組織自体の信頼性を確保するための検討**を行う。

関係する政府文書・窓口等

– 経済産業省「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　報告書等」（令和６年３月）