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

資料４

- 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）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）