サイバーセキュリティ対策の抜本強化に向けた提言 ～サイバーセキュリティ対策の「自律性」確保に向けて～ （概要）

✓ サイバー対処能力強化法等の施行に係る体制の強化、世の中全体のサイバーセキュリティ（CS）対策の抜本強化、CS分野における我が国の「自律性」確保のため、以下の施策を強力に推進するべき。

1 官民の情報共有の強化

（１）司令塔組織の体制強化
- 大規模な情報収集・分析・共有のためのシステム整備や質・量両面での人材確保、政府機関等の能力・機能の抜本的強化・高度化 等
- 外国機関との情報交換、連携、サイバー外交の「顔」の育成・確保 等

（２）官民通じた情報共有の結節点としての機能
- 政府が率先して、民間に対する適時適切な情報提供
- 様式統一、報告対象明確化、報告先一元化を通じた民間の負担軽減 等

2 地方公共団体のCS確保

- 都道府県が外部人材をプールし、市町村に派遣する事業の拡充
- 国が地公体に対し、CSに関する指導ができるような仕組みの検討

3 民間部門のCS確保

（１）ISAC※1の活動促進
- 政府との連携促進、対策強化が求められる分野のISACの支援

（２）セキュアなソフトウェア・IoT製品が流通し、選ばれるエコシステムの形成
- 開発手法に関する指針策定、SBOM※2活用、JC-STAR※3普及促進 等

※1：「Information Sharing and Analysis Center」の略。CSに関する情報収集や、収集した情報の分析等を行う組織。
※2：「Software bill of materials」の略。ソフトウェア部品構成表。
※3：「セキュリティ要件適合評価及びラベリング制度」 一定のセキュリティ基準を満たすIoT製品にラベルを付与する制度。

4 中小企業のCS確保

（１）普段の構え
- 中小企業経営層の意識改革、CSお助け隊サービスの充実・周知、サイバー保険の普及促進、「サプライチェーン企業のセキュリティ対策評価制度」等CS対策の可視化の検討加速、独禁法等の解釈明確化

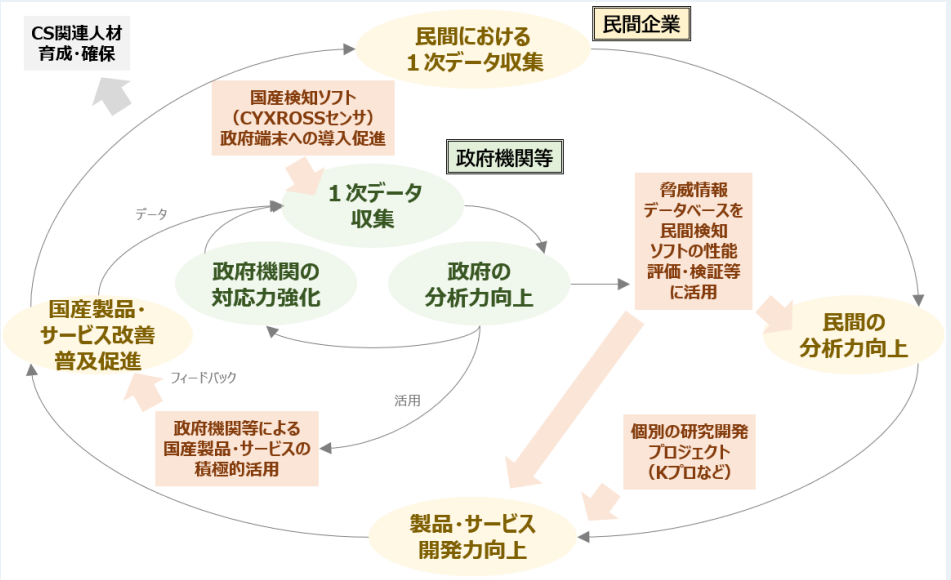
（２）インシデント発生時の支援
- 緊急時の相談窓口の浸透、初動対応支援強化の検討

5 国産技術を核としたサイバー対処能力向上のためのエコシステムの形成と人材育成

（課題）CS分野における海外依存度が極めて高く、CS対策が進むほど、デジタル赤字が拡大し、経済・国家安全保障上の深刻な脅威も招きかねない。

（１）国産技術を核としたサイバー対処能力向上のためのエコシステムの形成
- 政府機関等へ国産検知ソフト（CYXROSS※4センサ）を導入し、一次データ収集、分析力向上、対応力強化の官のエコシステムを構築
- 上記を民間に波及させ、民間の一次データ収集、分析力/開発力向上、国産製品の普及促進に繋げ、官民連携によるエコシステム形成

※4：「政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業」



（２）人材育成
- 「CS人材フレームワーク」の作成、役職や段階に応じたきめ細やかな人材育成施策の展開、高度大規模演習環境の構築

6 耐量子計算機暗号（PQC）

- 政府機関等のPQC移行ロードマップの策定に向け、司令塔の明確化、関係省庁会議の立上げによる作業の加速