(続)新しい経済安全保障とクラウド

株式会社ITリサーチ・アート
弁護士
高橋郁夫

2022年11月から2023年5月までの議論

- 特定重要物資の指定について(2022年12月)
  - クラウドプログラムが指定
- 安保三文書
  - 能動的サイバー防御
- 経済安保有識者会議の動向(特許出願の非公開にむけた動きなど)
- アメリカのサイバーセキュリティ戦略(2023年3月2日)
- 自民党 (2023年4月4日)
  - 「経済安全保障上の重要政策に関する提言」
- 生成系AIとクラウドサービスとの諸問題

特定重要物資の指定について(2022年12月)

- クラウドプログラムが指定
  - 安定供給確保に取り組む民間事業者等を支援することを通じて、特定重要物資のサプライチェーンの強靱化を図ることとしています
    - 認定を受けた事業者は、取組の実施に当たって必要な資金について、株式会社日本政策金融公庫が提供する長期・低利のツーステップローンを原資とした指定金融機関による融資等の金融支援や、安定供給確保支援法人又は安定供給確保支援独立行政法人による助成等の支援を受けられま

「国家安全保障戦略」

- 令和４年１２月１６日
  - 国家安全保障会議及び閣議
  - 安全保障関連3文書の決定
    - 国家安全保障戦略
    - 国家防衛戦略
    - 防衛力整備計画
- 「能動的サイバー防御を導入」
  - 武力攻撃に至らないものの（even if they do not amount to an armed attack）、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合
  - 目的
    - これを未然に排除し（eliminating in advance the possibility of serious cyberattacks）/または
    - このようなサイバー攻撃が発生した場合の被害の拡大を防止するために（preventing the spread of damage in case of such attack）
  - 能動的サイバー防御（active cyber defense）を導入

能動的サイバー防御(active cyber defense)の概念

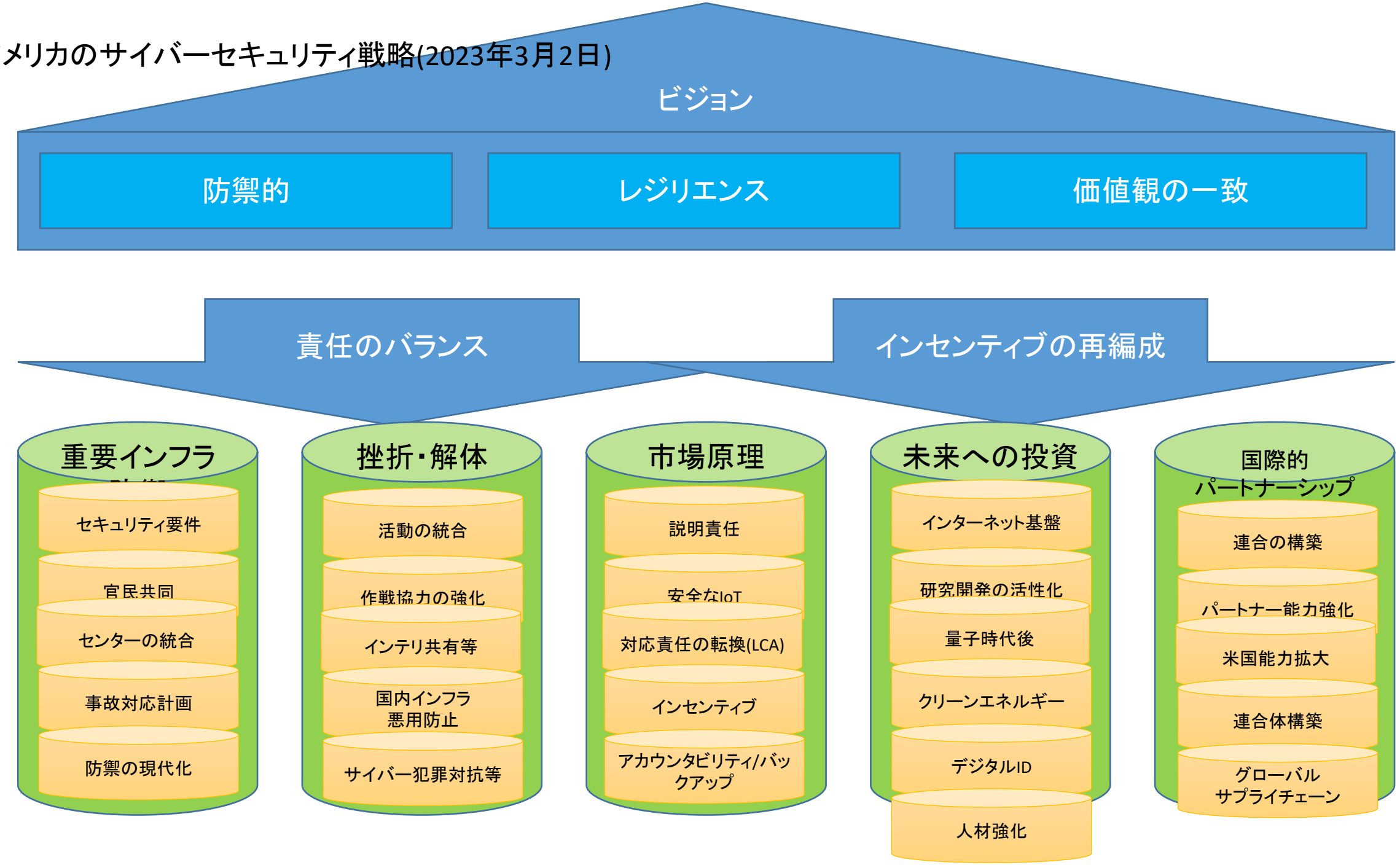
- 以下の概念(とくに(ウ))と自衛隊のサイバーオペレーションとの関係？
  - (ア)(日本は、)重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。
  - (イ)(日本は、)国内の通信事業者が役務提供する通信に係る情報(information on communications services provided by domestic telecommunications providers.)を活用し、攻撃者による悪用が疑われるサーバ等を検知(detect servers and others suspected of being abused by attackers)するために、所要の取組を進める。
  - (ウ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化(penetrate and neutralize attacker's servers and others)ができるよう、政府に対し必要な権限が付与されるようにする。

法的には、ほとんど概念として特定の意味をもっていない

経済安全保障有識者会議の議題と動向

- 令和5年2月8日
  - 特許出願の非公開についての議論
  - 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針(案)の概要
- 令和5年4月5日
  - 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針(案)のパブリックコメント
  - 特許出願の非公開についてのパブリックコメント
  - サプライチェーンの強靱化に向けた取組について
    - など

アメリカのサイバーセキュリティ戦略(2023年3月2日)



経済安全保障上の重要政策に関する提言

- 自由民主党政務調査会 2023年4月4日
  - 経済安保推進本部、安全保障調査会、サイバーセキュリティ対策本部、デジタル社会推進本部
- 3本柱
  - (1)いわゆる「セキュリティ・クリアランス（SC)」制度の導入
  - (2)サイバーセキュリティ（CS)の確保
    - 能動的サイバー防御の実施等を中心に必要な態勢と機能の骨格を提言
  - (3)経済インテリジェンス（EI）の強化

サイバーセキュリティ（CS)の確保

- 能動的サイバー防御の採用-> 前出
- 内閣サイバーセキュリティセンター(NISC)は発展的に改組
  - CS戦略本部の事務機能(政策　企画立案調整)とは別に、全く新しく実運用機能を内閣官房に設置
  - ACDの実施機能、民間及び行政セクターのCS対処機能、インテリジェンス収集分析共有機能、官房機能等を設置し、実効的な権限を付与
  - その他、CS分野の政策の一元的な総合調整機能、国際連携の推進等に関する一元的な司令塔機能を整備すること。
  - 新組織には、必要に応じて本提言のSCを含む情報保全制度を適用すること。
  - 新組織は、拡大インテリジェンスコミュニティに加えること。
  - 新組織と、関連組織のCS戦略本部(CS政策司令塔)、NSS(国家安全保障司令塔)、デジタル社会推進会議(標準化を含むデジタル政策司令塔)との関係については、政策と運用の適切な連携を念頭に置き、関係を整理すること。
  - 防衛省・自衛隊及び警察庁等については、それぞれの目的に応じたACD実施が可能となるよう制度設計を行うこと。
  - ガバナンス体制を構築し、制度的に担保すること。

経済インテリジェンス（EI）の強化

- 従来の枠に捉われない体制及び機能の抜本強化
- インテリジェンス・サイクルが確実に稼働するEIエコシステムを構築する
  - 政府内でEI情報収集の意義・目的等の共有を図る必要(経済安全保障戦略策定の意義の一つ)
  - 各省庁のEI収集分析能力、政策部門(国家安全保障局(NSS)及び各省庁等)及び情報部門(内閣情報調査室(CIRO)及び各省庁等)の集約分析共有能力等、を強化

生成系AIとクラウドサービスとの諸問題

- 生成系AI のイノベーション
  - AIは、一人前になると画像認識・機械学習とか、犯罪予測とか、具体的な名前がついてくる
  - LLMによる言語の対応のイノベーション
- 種々の法律問題
  - 人間の知能ってなんだったのか
  - 著作権まわり
  - 倫理まわり
  - セキュリティまわり
  - 安全保障まわり
  - 専門職と代替問題