

# 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

# ガバメントクラウド調達のお話

(地方公共団体情報システムのガバメントクラウドの利用に関する基準【第 1.0 版】)参照

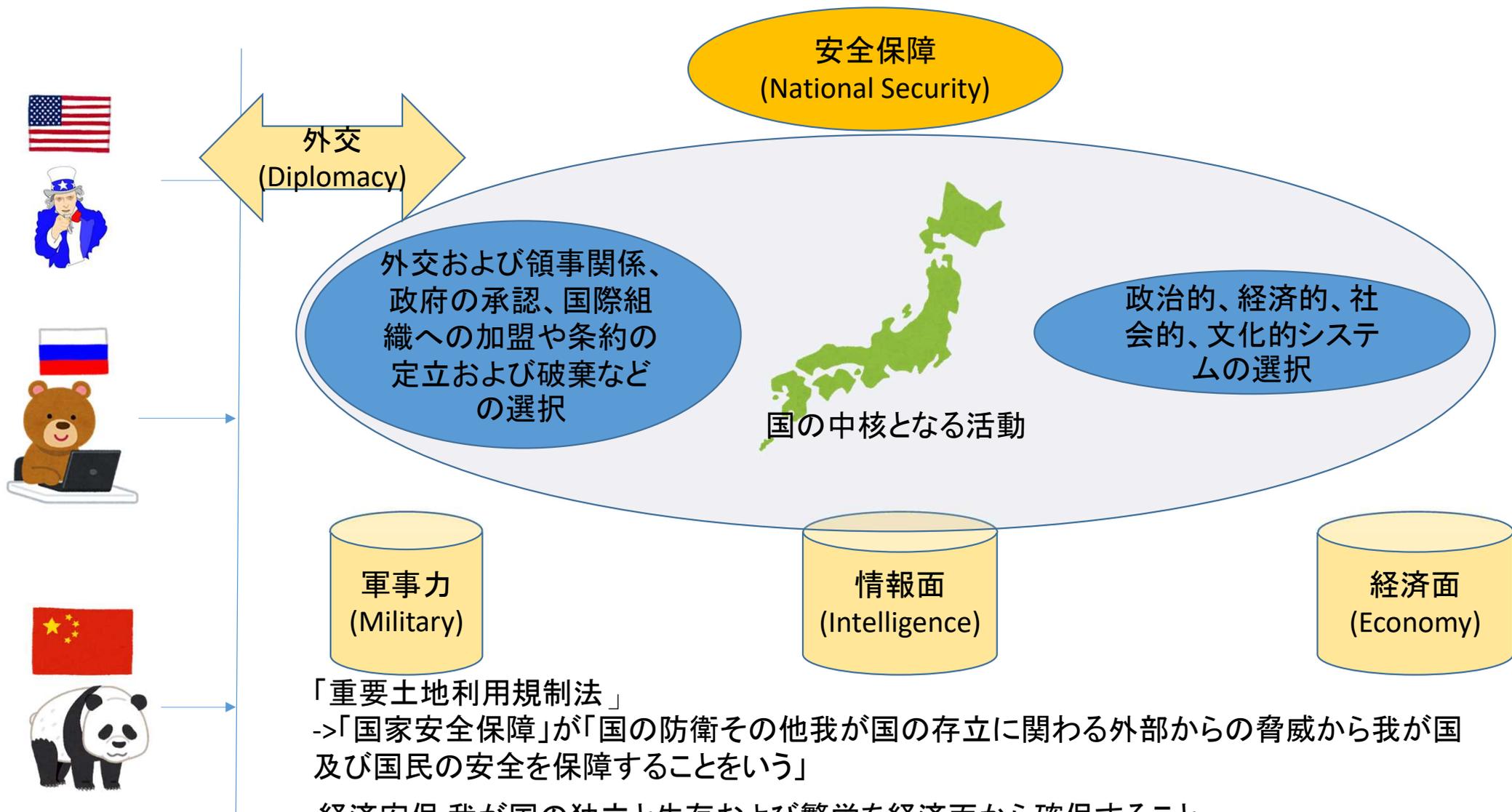
## • ガバメントクラウドの概念

### • 定義は？

- 「政府共通のクラウドサービスの利用環境です。」
- ガバメントクラウドとは、(ア)デジタル庁が 3.1 のとおり調達するものであって、(イ)当該クラウド上で標準準拠システム等(略)が利用できるよう、(ウ)地方公共団体に対し提供するクラウドサービス等(略)をいう
  - 赤字は、筆者

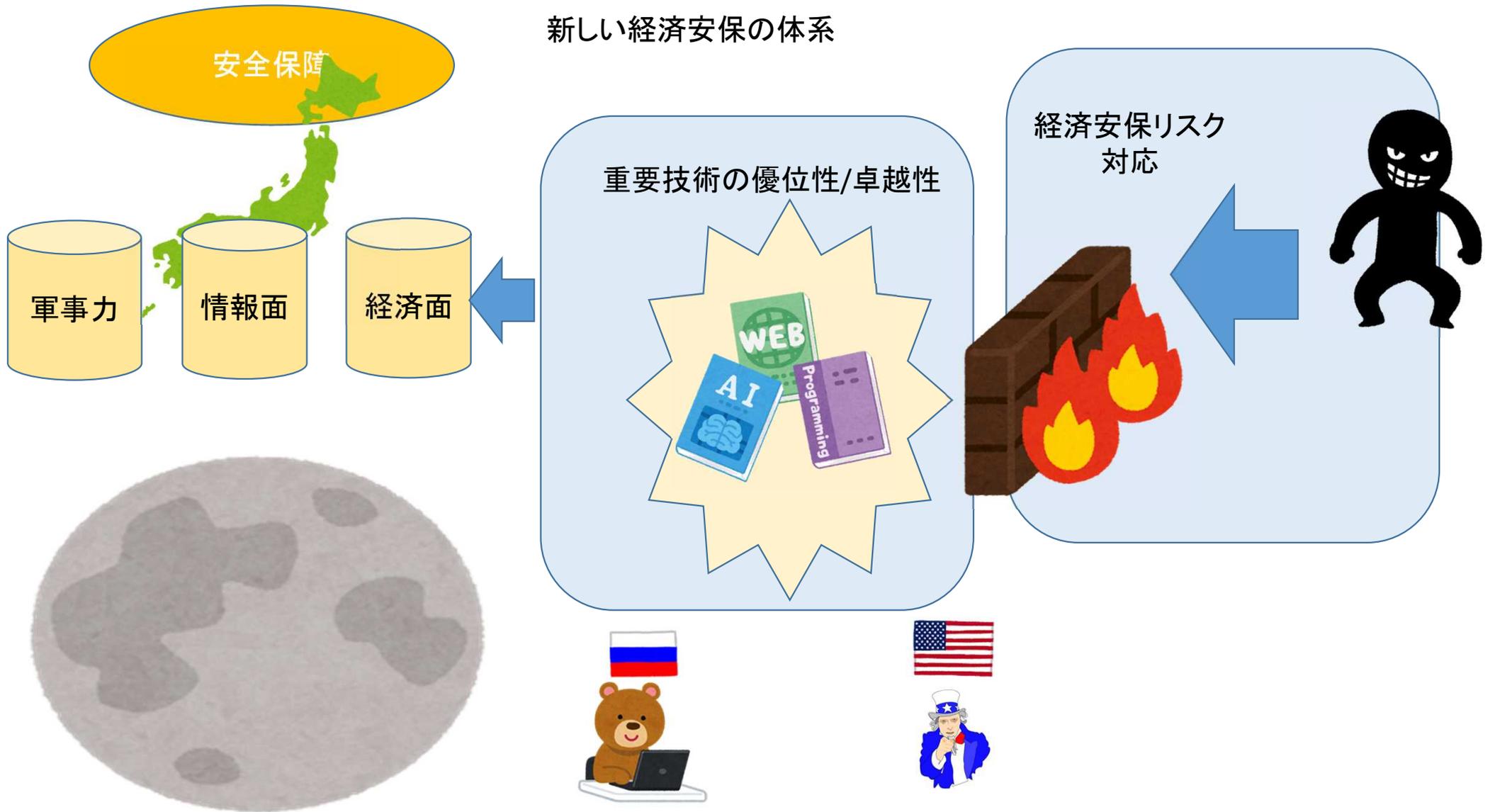
### • 調達は何？

- デジタル庁は、CSP からクラウドサービス等の提供を受け、ガバメントクラウドとして
- 当該クラウドサービス等を利用する環境を、地方公共団体に対し提供する



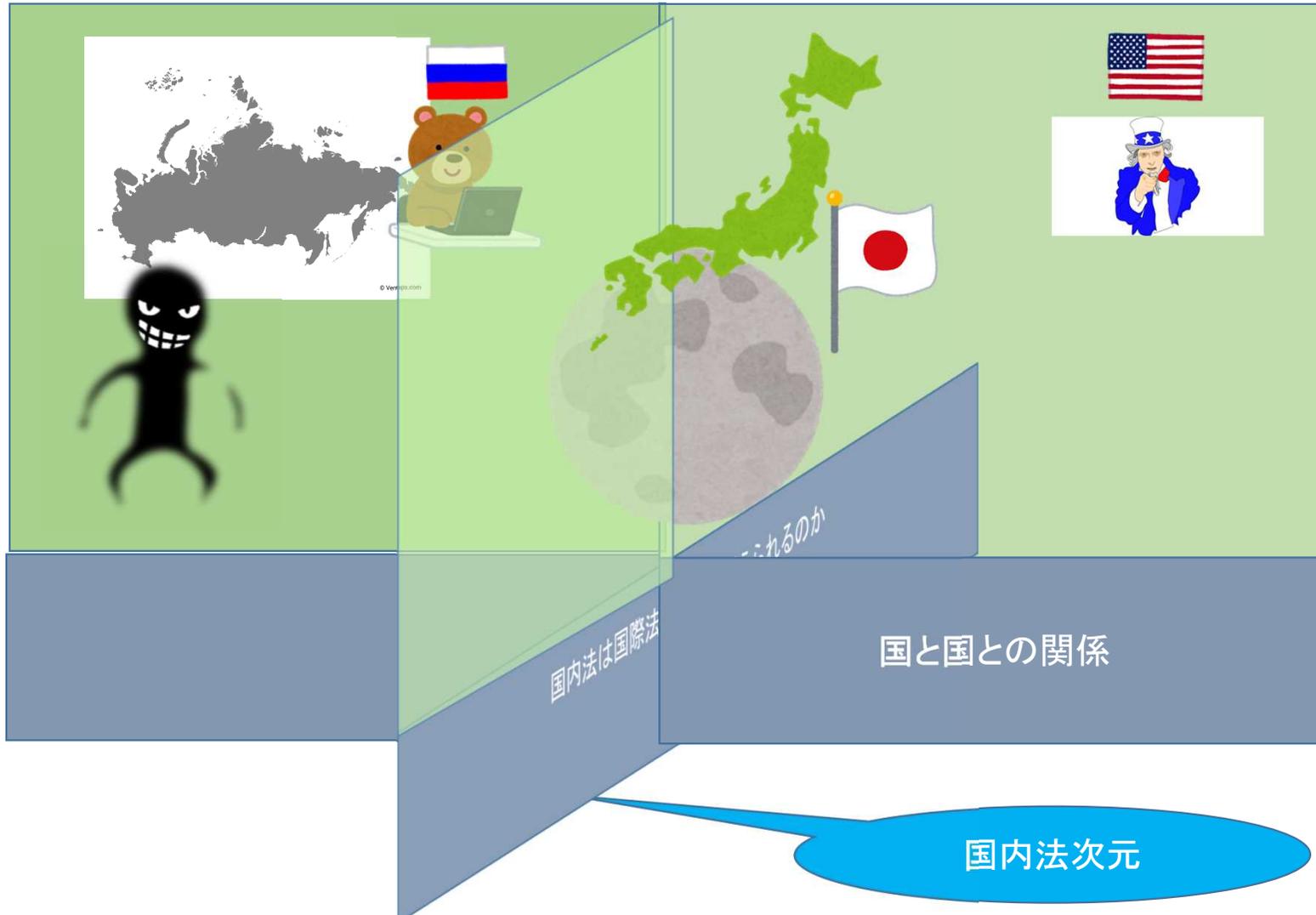
ただし、国会審議において「経済安全保障は多岐にわたる新しい課題であって、我が国を含めて、その定義という意味では、主要国において確立したものがあるわけではありません」「あえて分かりやすく申し上げれば、国家そして国民の安全を経済面から確保すること」という答弁あり

# 新しい経済安保の体系

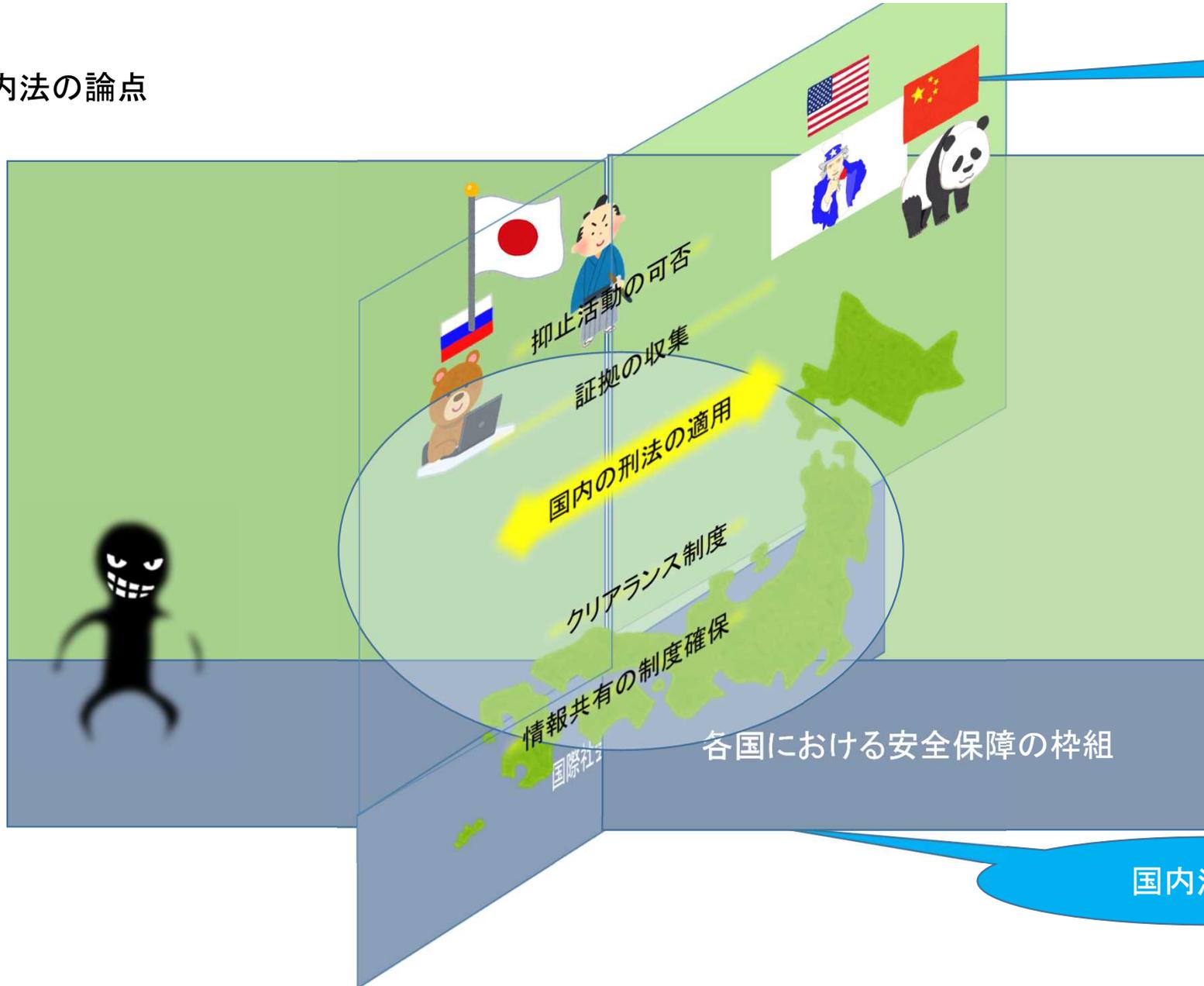


# 法の二つの世界と安全保障

国際法次元



# 国内法の論点



国際法次元

国内法次元



ファーウェイ  
排除

サプライチェーン

国内  
ドローン問題

積水化学  
事件

人的  
基盤

コロニアル  
パイプライン  
事件

産業  
基盤

サイバー窃  
取キャンペー  
ン

サイバーセキュ  
リティ

LINE問題

データ  
の場所

楽天資本  
問題

対内投資  
と  
経済の  
独立性

国の中核となる経済活動  
重要技術

# リスク(1) データの保存場所-LINE事件

- LINEの中国の会社および資本関係のない中国法人 1社に対して委託
  - 同社が、日本ユーザーの個人情報やメッセージの内容の取扱を業務再委託先である中国からのアクセスがある状態だったことなどに対して、問題ではないかという指摘がなされた事件。
    - 国家情報法・ネットワークセキュリティ法などの存在を指摘
  - 法律違反があったのかというと、明確にそこまではいえない
  - 「政府機関・地方公共団体等における業務での LINE 利用状況調査を踏まえた今後の LINE サービス等の利用の際の考え方(ガイドライン)」が公表(2021年4月30日)
    - 要機密情報を取り扱わせることは原則として禁止されている
      - 約款による外部サービスが提供されている場合、通常、要機密情報の取り扱いや管理などに関して各行政主体のポリシーに沿ったセキュリティー要件を担保できない

# LINE事件で守られるべき利益はなんであったのか

- 個人情報保護法上の利益なのか？
  - 情報主体が十分な情報を与えられた同意したのであれば、問題はないはずである。
- 記事としてのインパクトはあった
  - 2021年 新聞協会賞
    - (授賞理由)朝日新聞社は、無料通信アプリを運営する「LINE」が利用者に十分な説明がないまま、中国の関連会社から個人情報を閲覧できる状態にしていたことを、2021年3月17日付朝刊1面で特報した
  - 何故に、インパクトがあったのか
    - ガバメント・アクセスの問題

# 渥美さんの問題提起

- データをクラウド保存することによって生じるリスクってどういうことでしょうか。
- 取り扱う組織・人・システムのリスクにどう対応するのか？

# ガバメントアクセスの問題とは？

## • リスクの要点

- データが保存されている場所の主権を有する国家が、我が国の経済安全保障に関するデータを対外通信として傍受・分析するという脅威

## • 顕在化する場合

- クラウドのサーバーの所在地である外国にデータが保存される場合
- 情報システムに関わる処理を外国の会社に委託した際

## • 世界における対外情報行為

- 中国
  - 国家情報法
- 米国
  - 対外諜報監視法
- 英国(2016IPA)、ドイツ(G10法、BND法など)...

# ガバメントクラウドの要件での対応

- ④ 契約から開発、運用、廃棄に至るまで国によって統制ができること。
- ⑤ データセンタの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外への持ち出しを行わないこと。
- ⑥ 一切の紛争は、日本の裁判所が管轄するとともに、契約の解釈が日本法に基づくものであること。

# サイバーセキュリティの確保にむけた官民連携の強化

- 自民党経済安全保障対策本部 中間とりまとめ提言6頁
  - 主要国においては、サイバーインシデント情報の共有のための官民連携を進める動きがある
  - 官民連携の強化について制度整備を含めた所要の措置を講ずるべく検討を進めるべきである
    - NISC「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」
- 政府は、情報の機密性等に応じたクラウドサービスを利用することとし、クラウドの技術開発や実証を進め、その成果をクラウド等にかかる政府調達に反映すべきである。

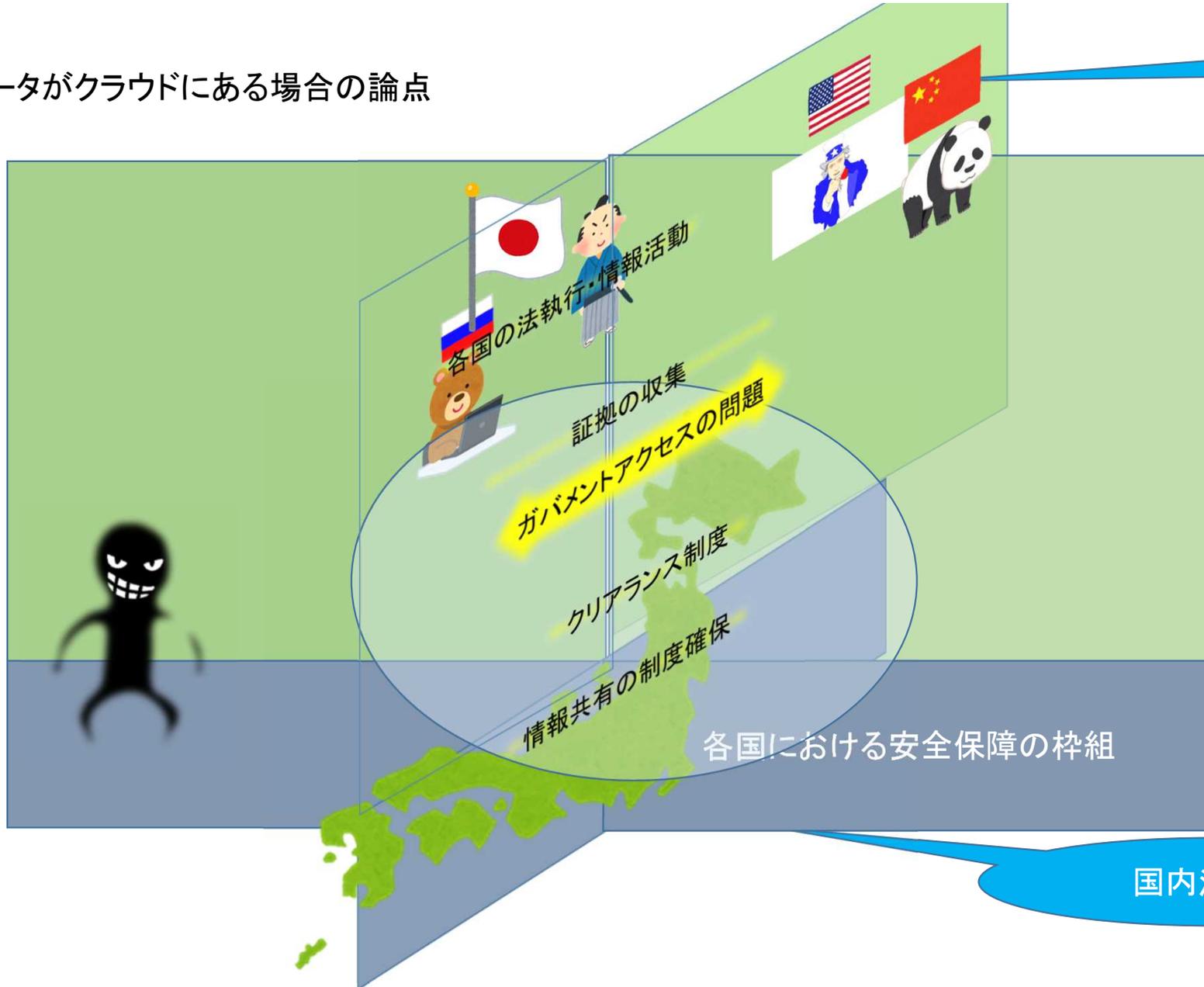
# データのローカル化の動きと問題点/バランス

- 「データのローカル化」
  - 重要なデータを外国に保存しない
  - 安全保障・国内産業育成等を理由とする
  - 類似の概念として、データナショナリズム、スプリンターネット
- その根拠
  - 個人データの問題のみではない
  - ガバメントアクセス・有効な行政規制・健康/医療データの保護・金融情報など
- 問題点
  - インドの失敗
  - コストの増大を招き、国内産業育成につながらない
- デメリットも大きいので、データの性質と「データの保存場所」リスクとの総合評価によって決まってくるとすべきではないか
- 重要なデータ
  - (1) 政府(政府機関のみならず地方公共団体も含み)が取り扱う場合においては、その取り扱うデータすべて
  - (2) 民間企業が取り扱う場合については、
    - (ア) データが、その性質上、支払いデータ、健康・医療データ、などの範疇に属する場合と、
    - (イ) 個人情報について、一定数についてデータベースを構成している場合

# どのように考えるべきか？

- 企業は、「データの保存場所」についてのリスク評価をしなければならない
  - これは、個人情報保護の問題だからではなくて、国家の経済的独立性の観点からくる「重要なデータ」に対する規範の一種と位置づけられる
  - 明文化はされていない。
    - 例外 医療情報について/政府クラウド
  - メディアが意識しないで批判する可能性
  - もっとも、このリスクを民間企業が評価しうるのか？
- 世界的に、どのような規制がなされているのか
  - 「令和3年度サイバー・フィジカル・セキュリティ対策促進事業（サイバーセキュリティ法制度の国際動向等に関する調査の第2部）」  
([https://www.meti.go.jp/meti\\_lib/report/2021FY/000150.pdf](https://www.meti.go.jp/meti_lib/report/2021FY/000150.pdf))で公開

# データがクラウドにある場合の論点



# セキュリティクリアランスの問題

- 問題提起

- 残された課題であるセキュリティクリアランス制度について、国際共同研究や諸外国で産業界に求められている枠組等の具体的事例の検証等をふまえつつ、重要情報を取り扱うものへの資格付与について可及的速やかに制度検討を含めた所要の措置を講ずるべく検討を進めるべきである。

- 本来の米国でのセキュリティクリアランスの制度

- セキュリティ・クリアランスの目的は、国家安全保障の機密情報へのアクセスを個人に許可すること
- 三つの制度
  - ①国家セキュリティクリアランス (National Security Clearance)
  - ②(連邦職員に関する)雇用適合性 (Employment Suitability) / 雇用健全性 (Employment Fitness)
  - ③国家安全保障大統領令12 (HSPD-12) による資格証明)
- 国際共同研究や諸外国で産業界に求められている枠組とは？
  - 特定秘密保護法におけるクリアランス制度は存在している
  - わが国の制度の限界(情報と行為による制限)

# よくある質問

- Q「データ」の保存場所のリスクをどのように考えたらいいのでしょうか
- A 考え方
  - 一概にはいえないでしょう。
  - 個人情報について、情報主体が十分な情報のもと、同意しているというのを考えるものではないだろう。ガバメント・アクセスが一定程度あったとして、維持しうるのかという観点
- クレジット業界-決済データの取扱を国内処理を義務づけたインドの挑戦は、失敗
- 一定の数の個人情報について
  - 中国はサイバースペース管理局の「データ域外移転のセキュリティ評価手段(数据出境安全评估办法)」
    - (3) 中国国外で個人情報を提供する100万人に達する個人情報を取り扱う個人情報処理業者。
    - (4) 外国への個人情報の累計提供数が10万人以上、または1万人以上の機微な個人情報の提供。

# シン・経済安保のご案内



## ・特徴

- 経済安保を法律の観点からみた入門書としては唯一の存在
- 「重要技術」の観点から経済安保をみることを提唱しており、近時の問題意識に適合している。
- 企業に対する経済安保リスクに対処するためのガイドランス
- ネットワークが経済安保でしめる位置に対応している(データの保存場所リスク、サイバーセキュリティと国家)

# シン・経済安保のご案内



## • かなわなかったこと

- 書籍作成の都合上、令和3年10月上旬までの情報に限られている(経済安保法制の4項目が新聞で報道された段階)
- 政府の対応・国家としての対応については、あまり重視していません
- 輸出管理規制等については、深い分析はできていないです

## • 経済安全保障推進法案の国会提出

## • 世界の安全保障の変動の影響

- ロシアのウクライナ侵略の影響等
- 企業に対する影響も大きい