

サイバー分野報告

令和3・4年度内閣府委託事業

「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」

令和5年3月28日

プロジェクト・マネージャー

手塚 悟 慶應義塾大学環境情報学部教授

分野 2 サイバーセキュリティ領域 22年度報告

2023年3月28日

**慶應義塾大学
手塚 悟**

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

1章 サイバー防衛の日米の比較

● 日本を取り巻く背景

● ウクライナ情勢

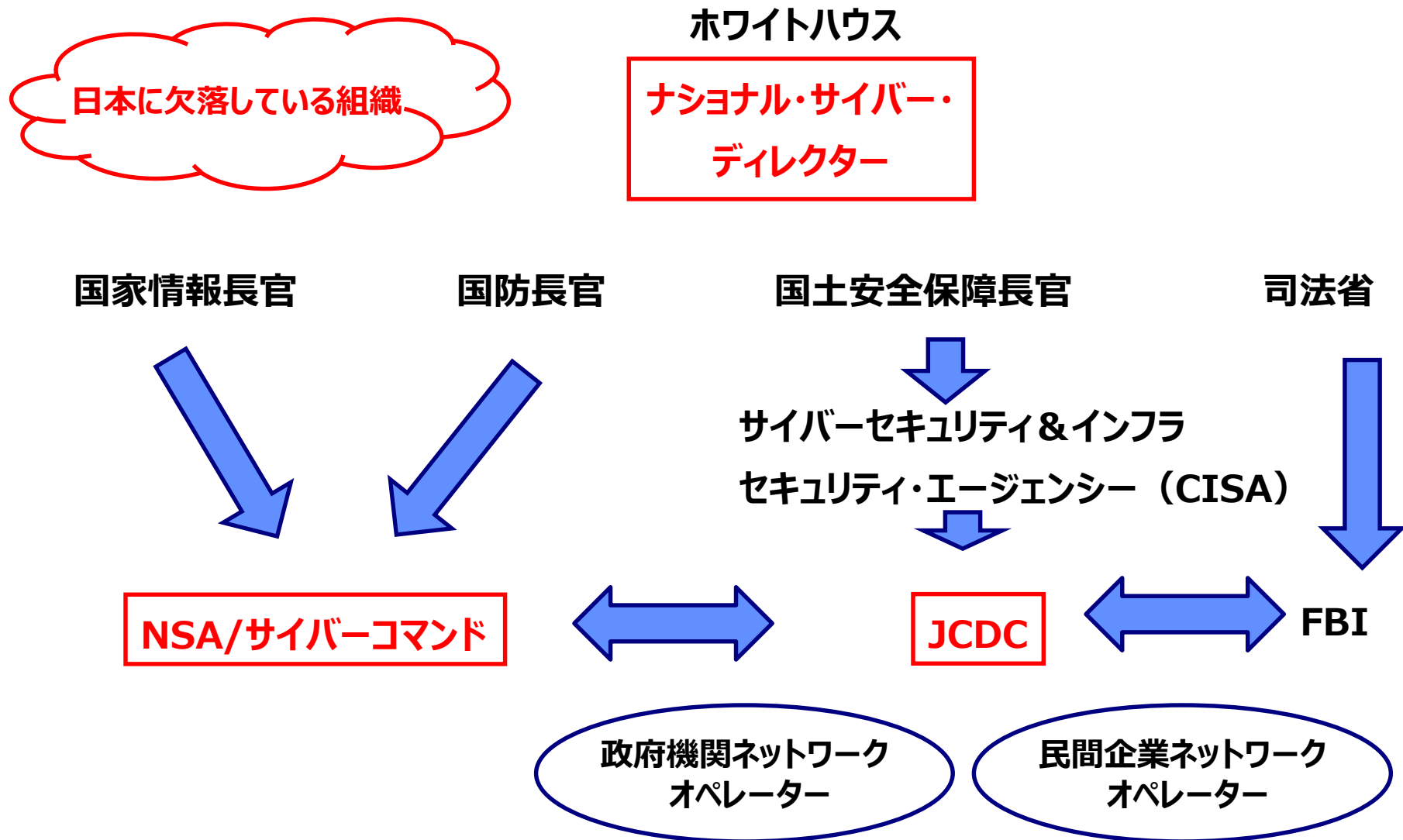
- ロシアは重要インフラのネットワークを攻撃し、偽情報を流している
- ウクライナのサイバー防衛隊は、国際的な支援を受けて、攻撃を撃退することに成功した
- 日本のサイバー防衛隊は関与していない

● 台湾海峡の平和と安定への懸念の高まり

- 日本は、ウクライナや他のファイブ・アイズ諸国のような強力なサイバー防衛能力を有していない
- 米国や他のファイブ・アイズ諸国は、有事の際に支援できるが、サイバーセキュリティの連携は遅く、弱い
- 日本は、サイバースペースにおいて自国を防衛し、米国や他のパートナーと連携するための予算、人材、法律、組織を整備する必要がある

1章 サイバー防衛の日米の比較

● 米国のサイバー防衛能力の構成要素



1章 サイバー防衛の日米の比較

● 日米同盟におけるサイバー防衛のカウンターパート

新規

日本ナショナル・サイバー・ディレクター

総理大臣直属/少人数のスタッフ



米国ナショナル・サイバー・ディレクター

新規

日本サイバーインテリジェンス機構

6,000人のスタッフ/30億ドルの予算/海外ネットワークに対する権限



NSA / US Cyber Command /
ファイブ・アイズ

数十億ドル/数万人規模のスタッフ

権限付与と
再組織化

NISC GSOC/Japan
National CERT/デジタル庁

政府内のサイバーセキュリティのリーダーシップと
官民協力のための権限を確立する。



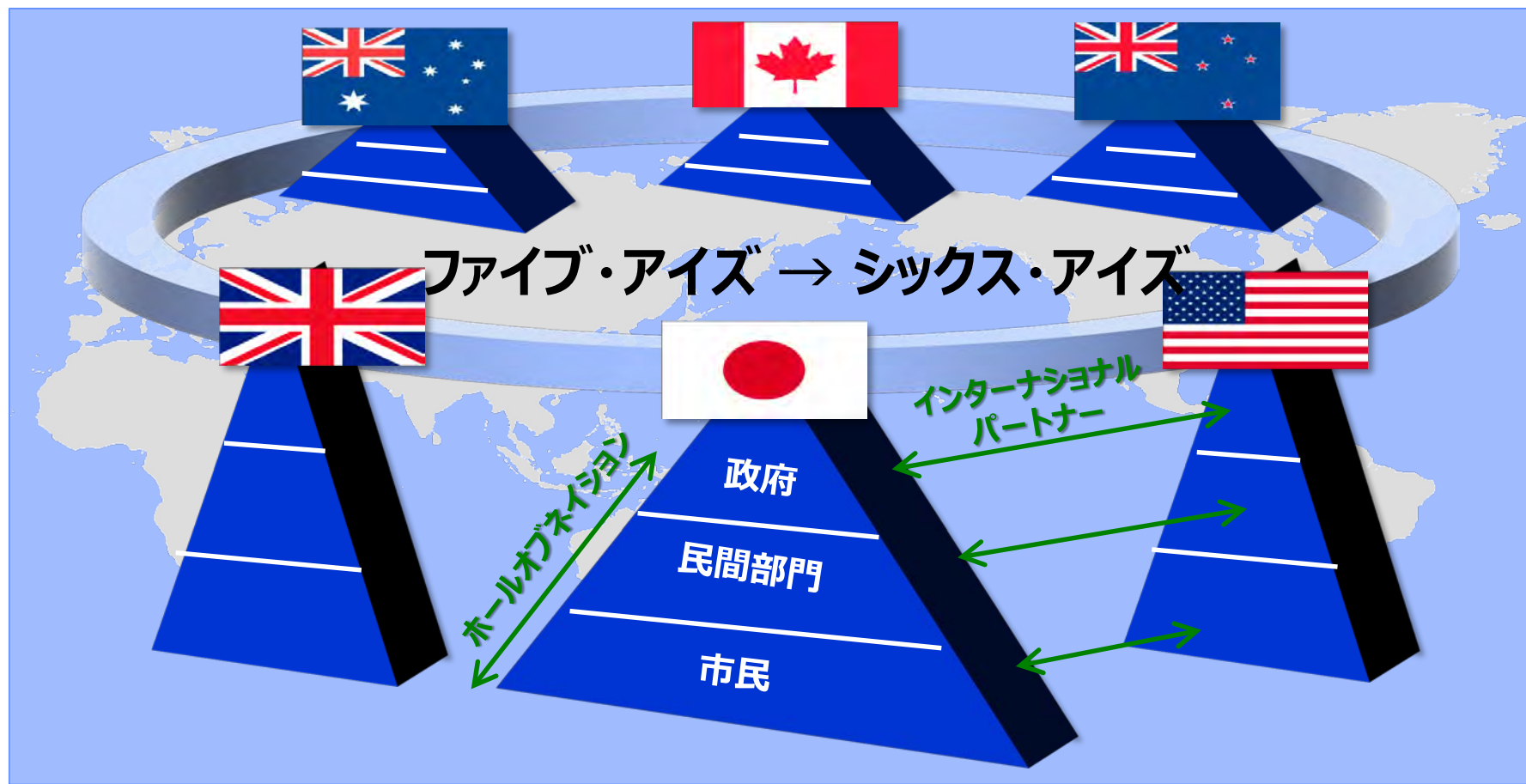
JCDC

JCDC: Joint Cyber Defense Collaborative

1章 サイバー防衛の日米の比較

● 国家サイバー防衛能力 - 国際

- サイバーインテリジェンスに貢献できれば、日本は歓迎される
- 日本は、サイバーインテリジェンスシステムでクローズドソースインテリジェンスを生み出せること、他国にgiveできること



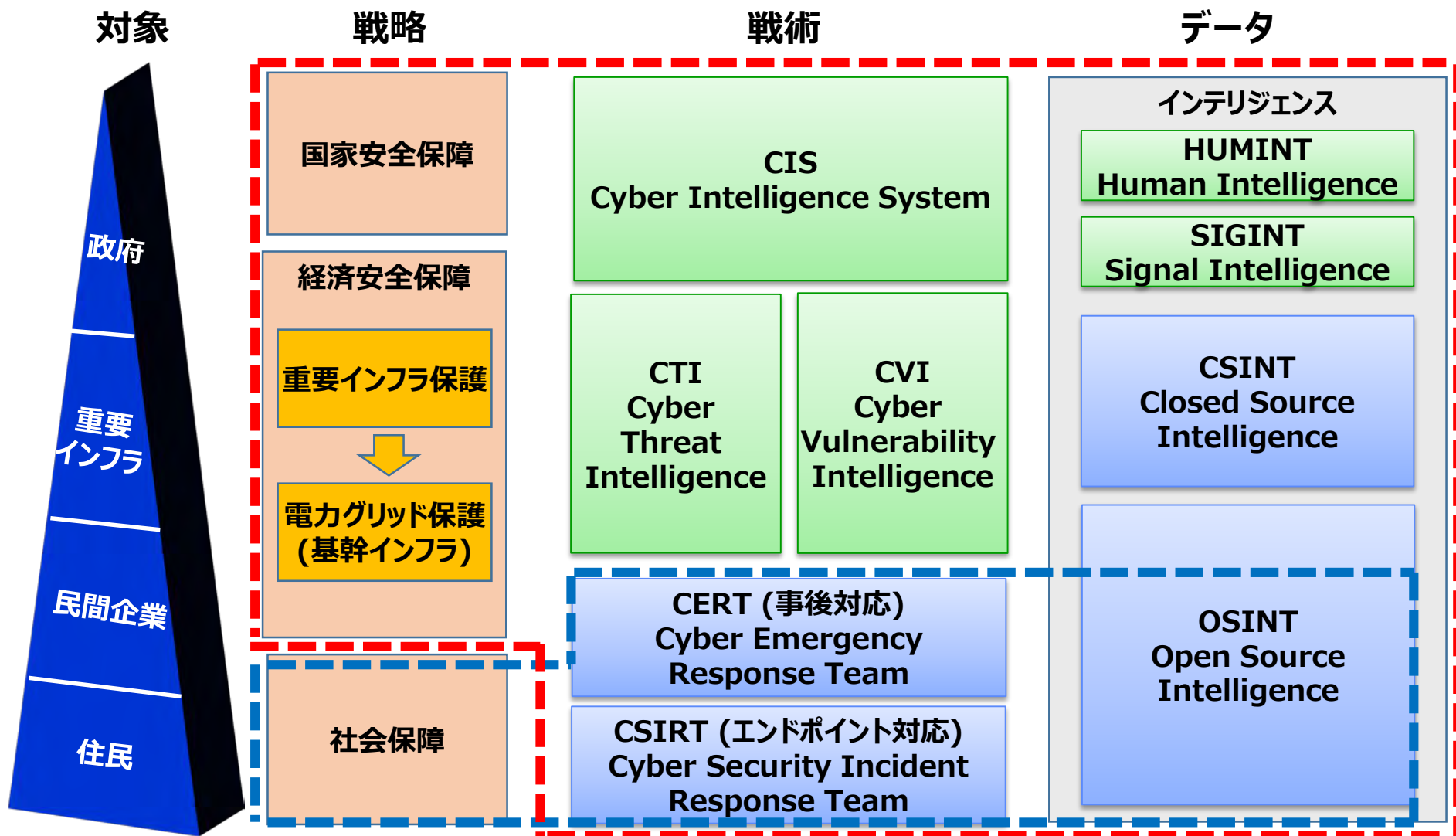
1章 サイバー防衛の日米の比較

● 国家サイバーインテリジェンスの全体像



1章 サイバー防衛の日米の比較

● インテリジェンスの策定範囲



目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

2章 サイバーインテリジェンスシステム

● システムの全体像

- 「サイバーインテリジェンスシステムでクロードソースインテリジェンスを生み出すこと、他国に give できること」のためには、サイバーインテリジェンスシステムの構築が不可欠である

セキュリティ クリアランス

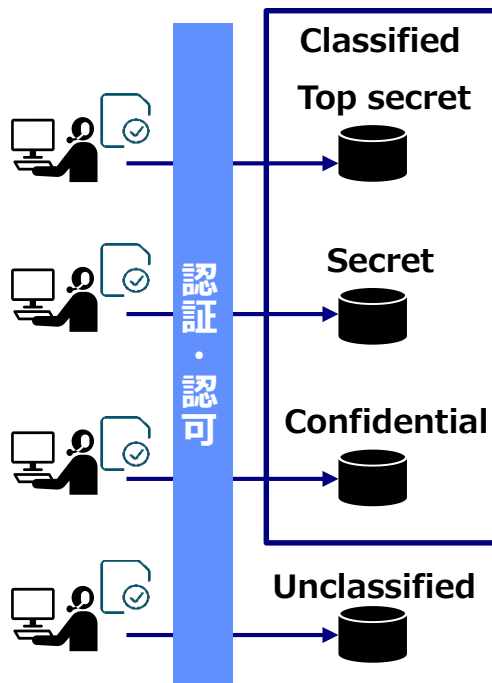


クリアランス付与

3レベルで審査
・Eligibility
(Need to Know)
・Suitability
・Credentialing

国家サイバーインテリジェンスセンタ

コントロールプレーン



データプレーン

サイバーインテリジェンスシステム (クラウド)

アプリ

OSINT(オープンソース
インテリジェンス)



アクティブディフェンス



インフラ

AIシステム



サーバ(→スーパーコンピュータ)



ストレージ



Top secret /
Secret /
Confidential

通信(→量子通信)



2章 サイバーインテリジェンスシステム

● サイバーインテリジェンスシステムの機能および開発項目

CTI

- データ収集
- キュレーションと重複排除
- 機械学習
- データのエンリッチメント(優先順位つけ)
- 関連付けと統合
- 形式(容易に取り込めるような)
- インテリジェンスレポートと分析

CVI

- 倫理的ハッカー(人材管理)
- ペネトレーションテスト
- 脆弱性スキャン
- バグ・バウンティ(報奨の仕組み)
- 組織的な脆弱性開示
- 敵対的レッドチーム(運用)
- セキュリティ・コントロール評価(適切な実装の確認)
- セキュリティコードレビュー(ソフトウェアを対象)

アトリビュション

- サイバーヒューミント(AI活用)
- 犯行自白誘導
- 犯罪情報の露呈誘導
- 侵入分析(犯罪グループの証跡)
- 痕跡からの犯罪者特定
- データの収集
- クラスタリング
- 動機・意図の特定
- 結果公開

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

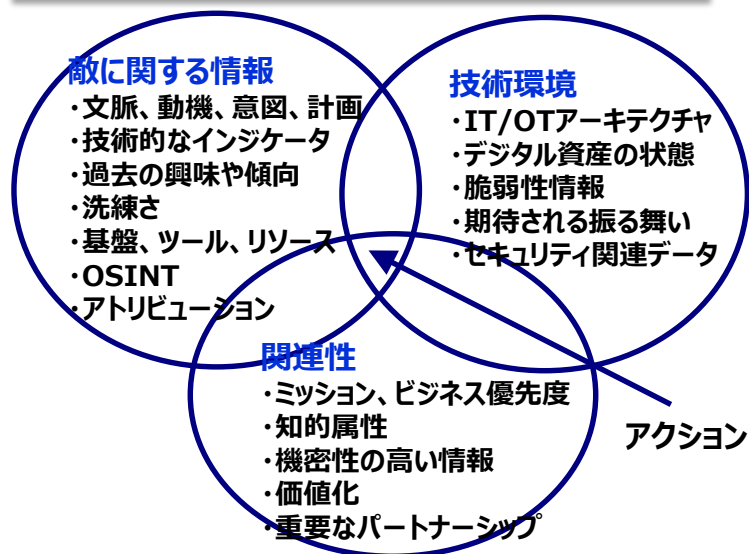
2.5 節 アトリビューション

3 章 まとめ

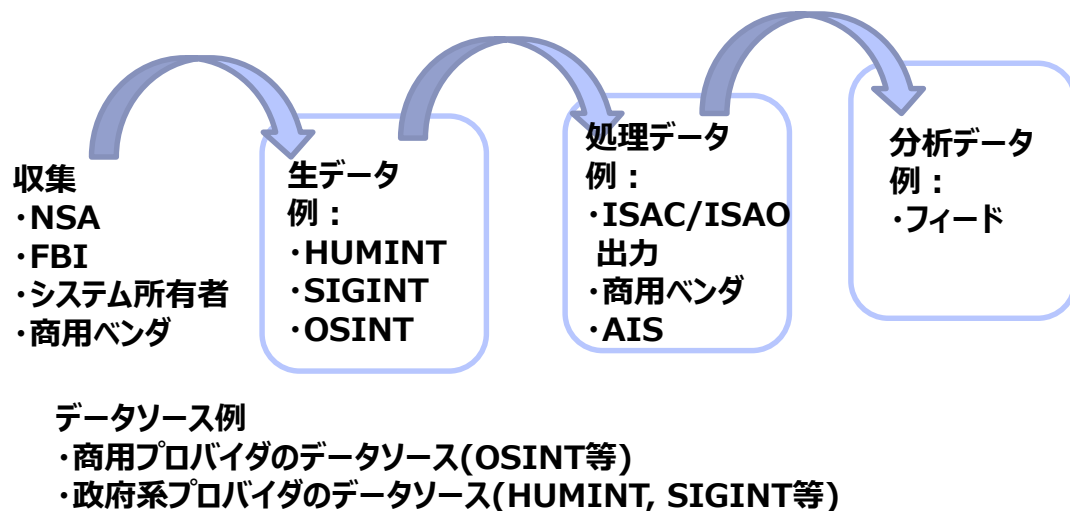
2章 サイバーインテリジェンスシステム

- サイバーインテリジェンスシステムが扱う、2大インテリジェンス
 - CTI (Cyber Threat Intelligence)
 - CVI (Cyber Vulnerability Intelligence)

効果的なCTIプログラム



CTI形成のイメージ



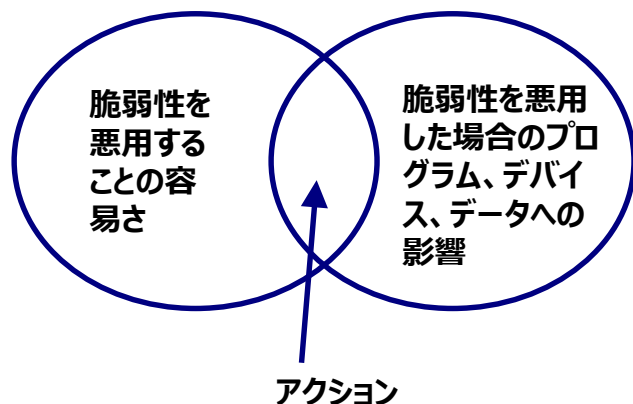
CTIの評価基準

- (1) 適時性
- (2) 精度
- (3) 使い勝手の良さ
- (4) カバレッジ
- (5) リソース
- (6) (データ処理の)スケーラビリティ
- (7) (機能の)拡張性
- (8) コンテキスト

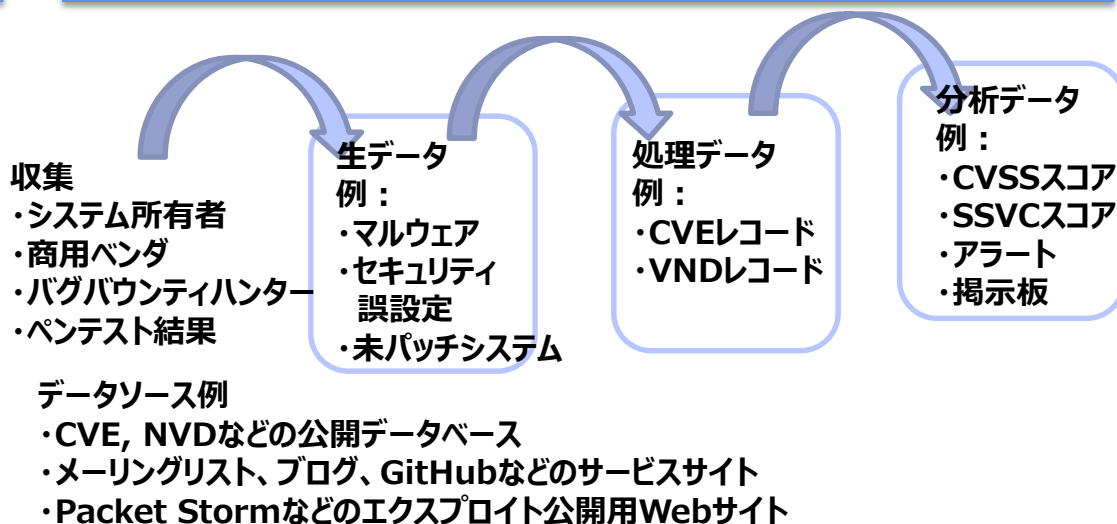
2章 サイバーインテリジェンスシステム

- サイバーインテリジェンスシステムが扱う、2大インテリジェンス
 - CTI (Cyber Threat Intelligence)
 - **CVI (Cyber Vulnerability Intelligence)**

効果的なCVIプログラム



CVI形成のイメージ



CVIの評価基準

- (1) 特定された脆弱性がシステム固有のものか、意図的な脅威アクタや不注意によってシステムに導入されたものか
- (2) 既知の脆弱性が存在するか
- (3) 個々のステークホルダーが、自らが管理・支配するシステムの脆弱性を明らかにすることに消極的な場合があることへの理解
- (4) 特定の脆弱性についてのペネトレーションテストやネットワーク評価の結果を含める
- (5) 評価対象のシステムのベンダやサプライヤが新規で未試験であるか

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

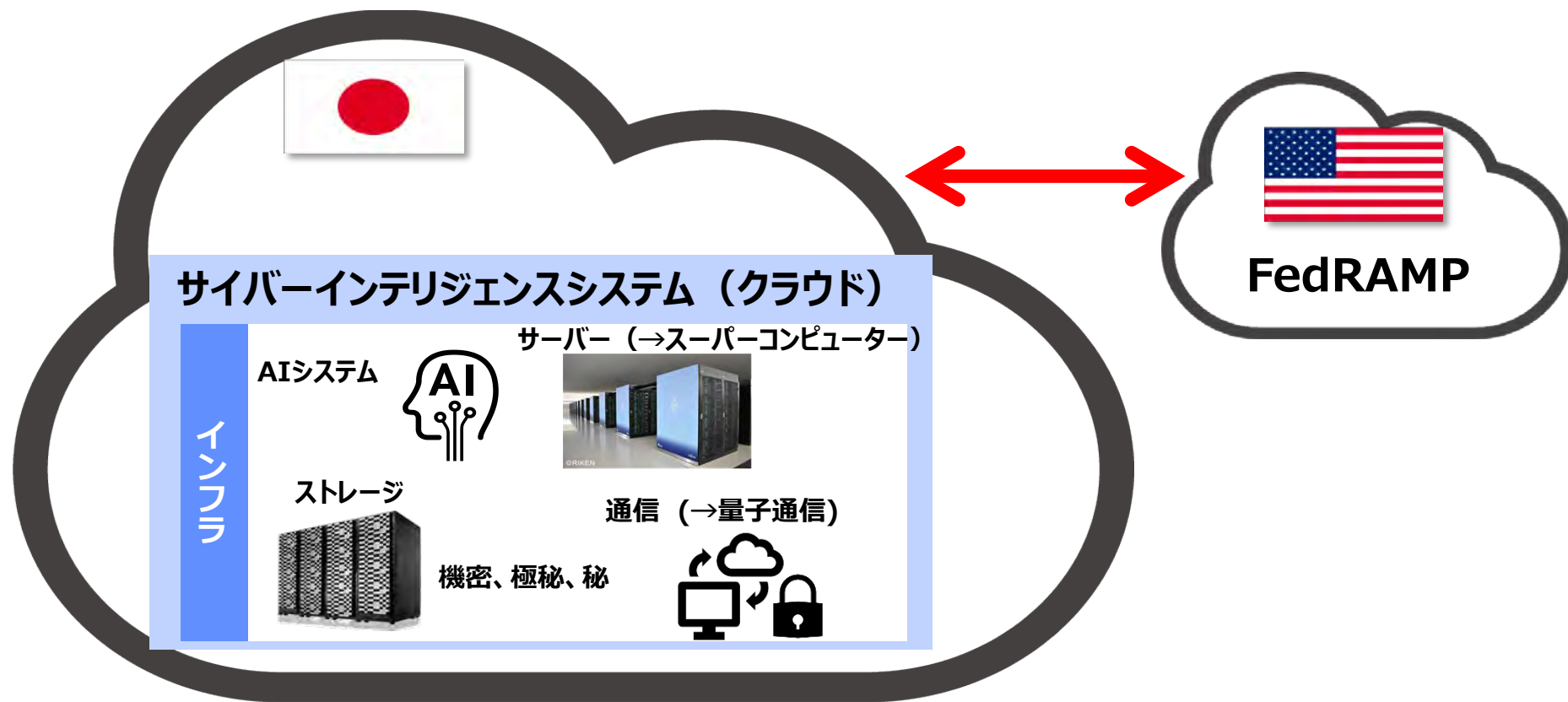
2.5 節 アトリビューション

3 章 まとめ

2章 サイバーインテリジェンスシステム

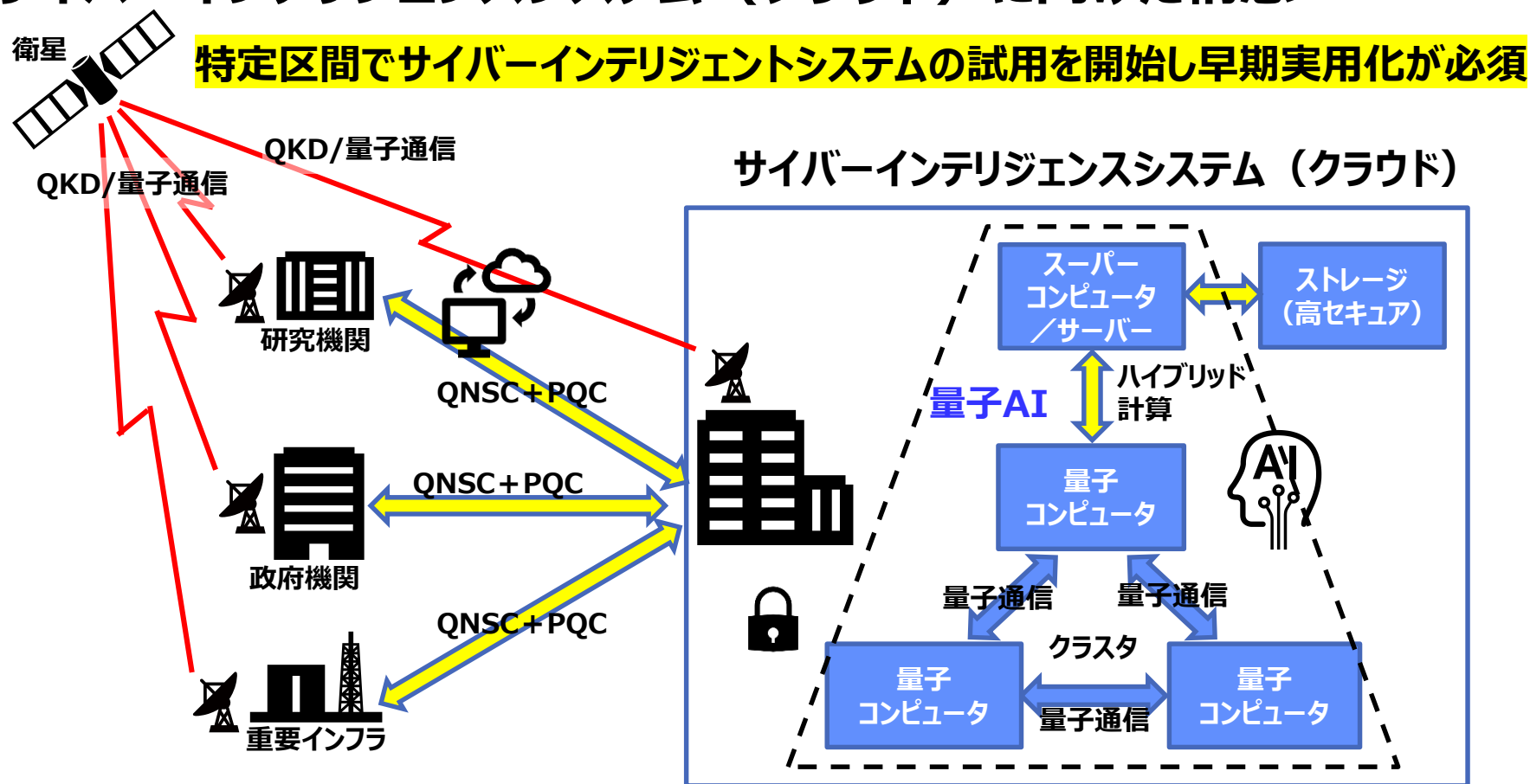
● インフラストラクチャ

- 国家的なサイバーインテリジェンスシステムは、政府のクラウドによって実現される必要がある
- 日本が「ファイブ・アイズ・ギブ&テイク」の情報共有の枠組みに参加するためには、米国におけるFedRAMP（クラウドセキュリティ認定制度）に相当するものを整備する必要がある



2章 サイバーインテリジェンスシステム

● サイバーインテリジェンスシステム（クラウド）に向けた構想



量子通信が実現できると、量子コンピュータは高機能化のために量子ビット数を増やすだけでなく、量子コンピュータ同士を量子通信で接続するクラスタ化が進み、更にスーパーコンピュータとも連携した**ハイブリッド利用**による両システムの優位性を活かした効率の良い利用形態へと進化する

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

2章 サイバーインテリジェンスシステム

● データの区分： Classification Levels (EO 13526)

- **Controlled Unclassified Information(CUI)**は、**大統領令 Executive Order 13556 (2010)**によって定義された情報カテゴリ
- NARAはその指示を受けて連邦政府全体に対してCUI保護の態勢を作る役割を負った
- NISTはNARAの指示のもと、CUIを保護するための基準をSP800-171として策定した
- CUIは、我が国（防衛省）の「保護すべき情報」に近い領域とみなせる

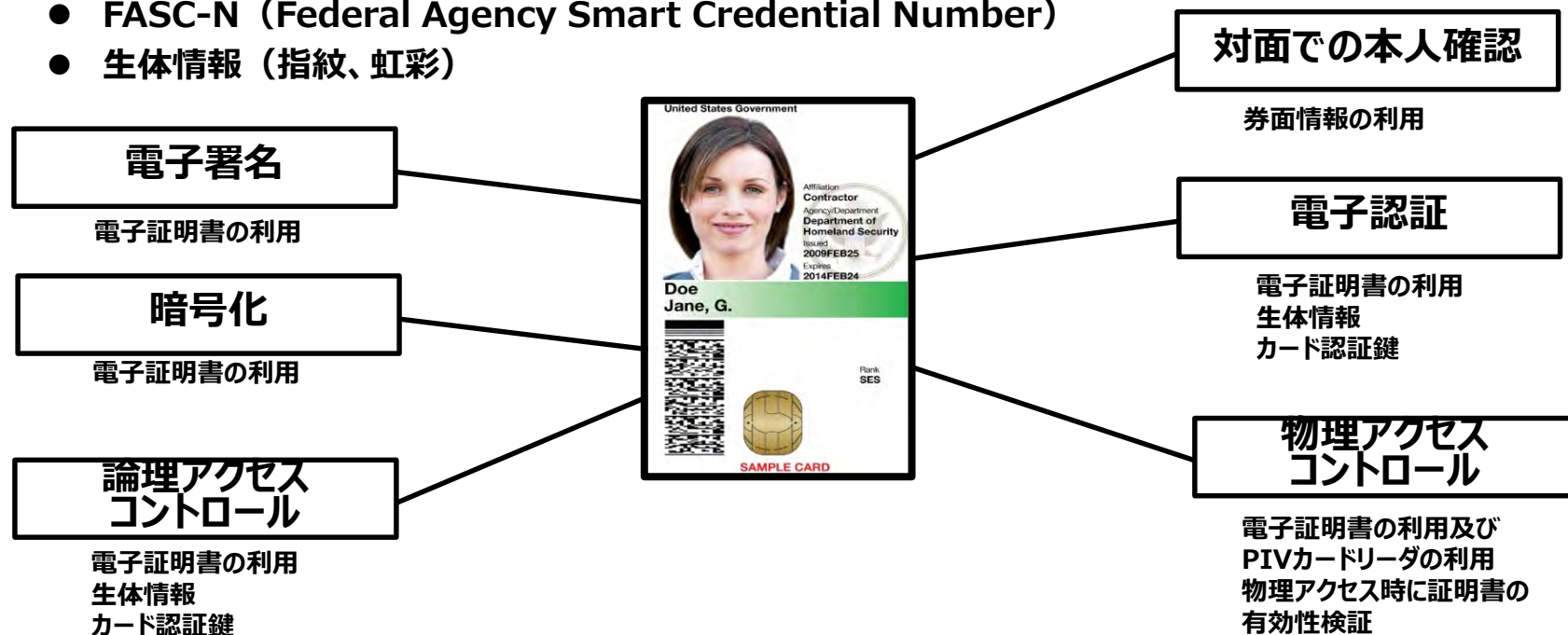


秘匿性	←-----		
米国	Classified Information Top Secret・Secret・Confidential	CUI	Unclassified Information
日本	機密・極秘・秘	保護すべき情報	一般情報

2章 サイバーインテリジェンスシステム

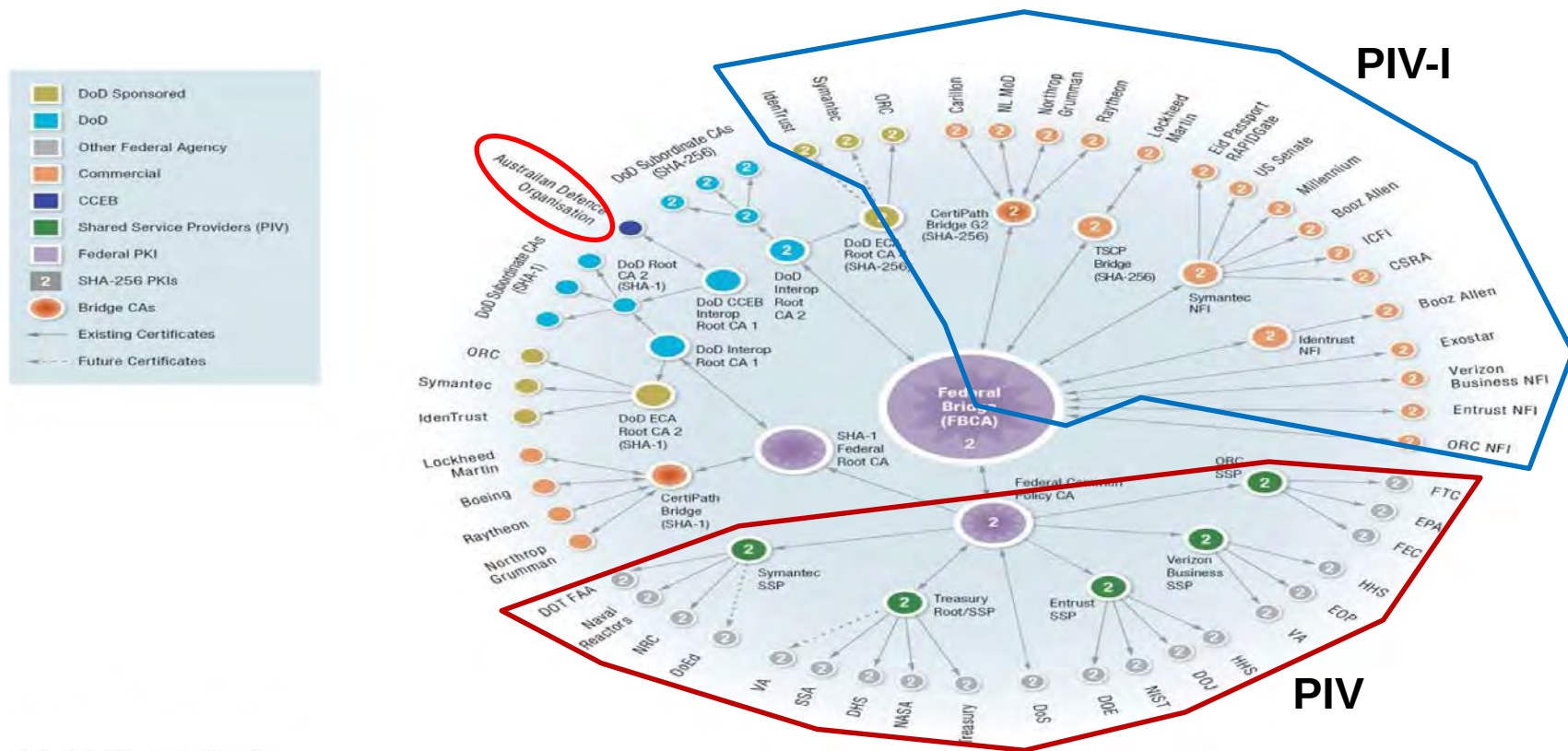
● ヒトの区分： Security Clearance (EO 13526)

- Personal Identity Verification (PIV) カード：連邦政府職員所有
- Common Access Card (CAC): 国防総省職員所有
- PIV- I (Interoperable) カード：セキュリティクリアランスをパスした民間職員所有
 - 券面情報（対面での本人確認用）
 - 電子証明書（LoA4）
 - 暗号鍵
 - FASC-N（Federal Agency Smart Credential Number）
 - 生体情報（指紋、虹彩）



2章 サイバーインテリジェンスシステム

● PIVとPIV-Iを発行するFBCAをルートとする認証局のトポロジー



● デジタル安全保障

我が国が米国と国家レベルでの情報共有をするためには、FBCAとの国際相互連携が必要不可欠である

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

2章 サイバーインテリジェンスシステム

- 米国の枠組みでは、信頼されるポジションの候補者を3段階に分類
 - クレデンシャリング (Credentialing)
信頼の基礎となるレベルで、通常、**個人の身元と市民権の確認**が含まれる
 - 適性 (Suitability)
連邦機関は、**個人の性格と行動を評価**し、その人がどの連邦機関の職員としても適していることを確認する
 - 適格性 (Eligibility)
連邦機関は、調査に関する国家標準とそれに基づく決定を活用して、**個人が国家機密情報へのアクセスに適格**であるかどうかを判断する
- 人事考課 (Personal vetting) とは、雇用のライフサイクルを通じた個人の履歴を調査するシステムである

管理予算局(OMB)は、政府全体の審査システムを改善するためのイニシアティブを管理
米国の審査人員は、全省庁で7,000人を超える

2章 サイバーインテリジェンスシステム

● 裁定ガイドラインのトピック

- 国家への忠誠
- 海外影響力
- 外国人優先順位（該当する場合）
- 性行動
- 個人的な行動
- 財務上の考慮事項
- アルコール摂取量
- 薬物への関与と薬物乱用
- 心理的条件
- 犯罪行為について
- 保護された情報の取り扱い
- 外部活動
- 情報技術の活用

2章 サイバーインテリジェンスシステム

● 日本版のデータ区分と人の区分に関するフレームワーク案

パート1：日本版データ区分体系（案）

セクション1.1 基準

情報が機密扱いされる前に満たさなければならない条件

セクション1.2 レベル

保護が必要な国家安全保障情報に対して、3段階の区分を定義

セクション1.3 権限

どの職員が情報を区分する権限を持つか、また、どのような条件でその権限を他者に委譲できるかを規定

セクション1.4 カテゴリ

機密扱いされる可能性のある国家安全保障情報のカテゴリをリストアップ

セクション1.5 期間

情報の機密解除の権限と、機密解除が行われる条件

セクション1.6 識別と表示

機密情報を文書（紙媒体、電子媒体を問わず）内にマーキングする方法

セクション1.7 手引き

何を区分するかという決定をどのように記録し、情報をいつ、どのレベルで区分すべきかというガイダンス

セクション1.8 ガイダンスの適用

作業レベル担当者が、どのように機密資料を作成し、取り扱うかについて説明

セクション1.9 機密情報の共有と保護

機密資料を可能な限り低いレベルで作成するための明確なガイダンス

パート2：セーフガード

セクション2.1 アクセスに関する一般的な制限

経歴調査や職務に関連したNeed to Knowなど、個人が機密情報へのアクセスを許可されるための要件

セクション2.2 普及のためのコントロール

情報を安全に共有する必要性と、正式なセキュリティ・クリアランスを持たない人物と機密情報を共有することが日本政府の利益になる場合の特別な状況

パート3：実施と見直し

セクション3.1 一般的な責任

日本の区分システムの実施を担当する職員の責任

セクション3.2 説明責任と懲戒処分

本プログラムで確立された機密情報手続きに違反した場合に、どのような結果がもたらされるかについて説明

パート4：コスト

費用について簡単に説明

パート5：まとめ

結論となる考え

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

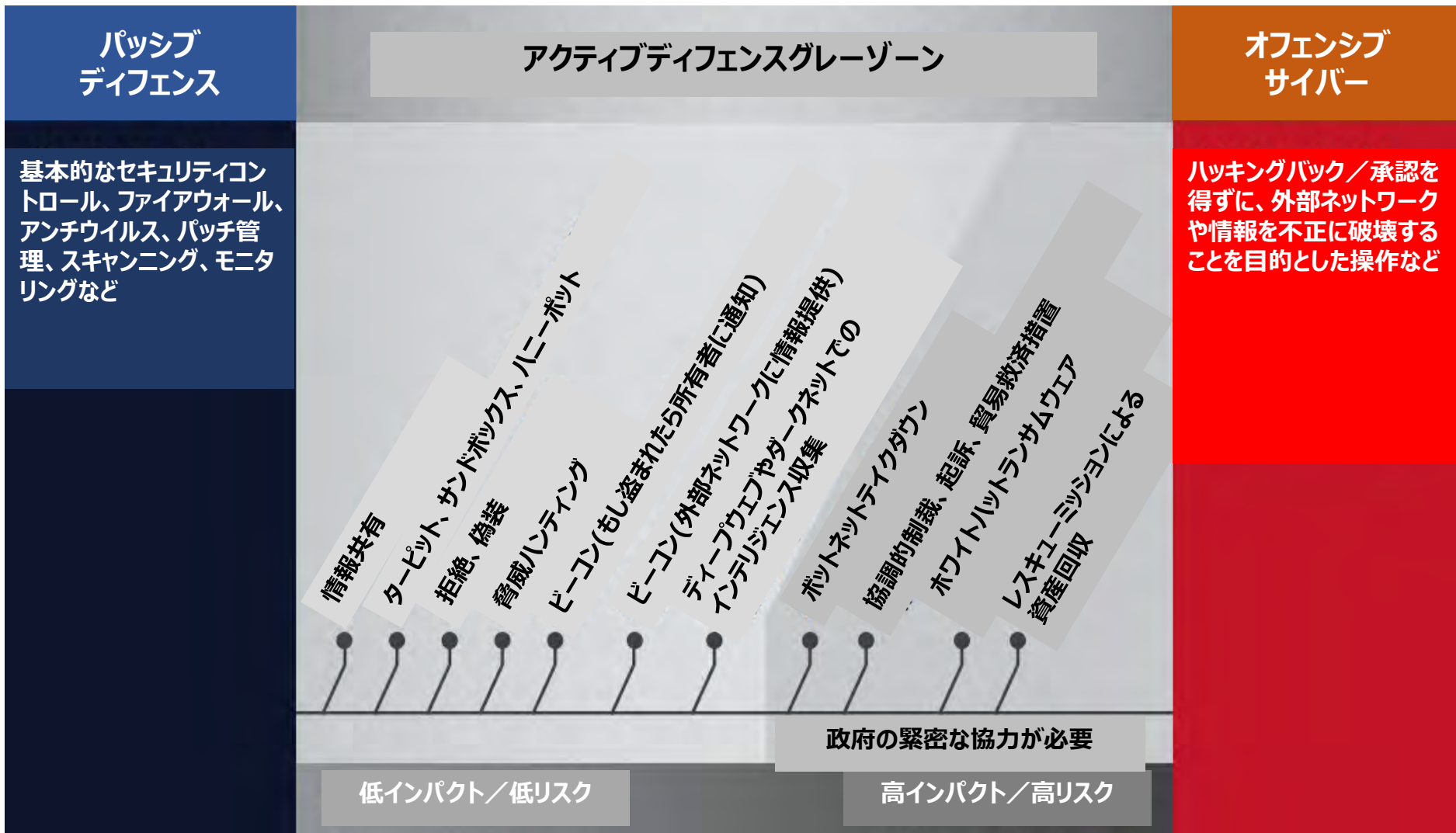
2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

2章 サイバーインテリジェンスシステム

● 積極的サイバー防御のグレーゾーンでアトリビューションは効果を発揮



2章 サイバーインテリジェンスシステム

- 我が国独自のインテリジェンスシステムの重要性
 - 他国にgiveするに値するクローズドインテリジェンスを作り出す

オープンソースインテリジェンス	クローズドソースインテリジェンス
● 他国も同じOSINTを入手可  ● インテリジェンスをgiveするに値しない	● 地政学的な強みを生かした日本ならではの情報を収集 ● 例えば、インド太平洋経済枠組み (IPEF)  ● インテリジェンスをgiveするに値する

目次

1 章 サイバー防衛の日米の比較

2 章 サイバーインテリジェンスシステム

2.1 節 システムの全体像

2.2 節 データプレーン

2.2.1 項 アプリケーション

2.2.2 項 インフラストラクチャ（量子関係を含む）

2.3 節 コントロールプレーン

2.4 節 セキュリティ・クリアランス

2.5 節 アトリビューション

3 章 まとめ

3章 まとめ

● 我が国が対等な立場で、海外と交流・共同作業をできるようにする

項目	米国の整備状況	我が国の未整備状況
データを 守る	・Classified/Unclassified CUI (Controlled Unclassified Information) ・Need to Knowの原則	・機密情報区分の進化 ・知るべき情報、知ってはならない情報を分ける → データ区分の改定
人を守る	・セキュリティクリアランス ・FICAM (Federal Identity, Credential, and Access Management) ・PIV (Personal Identity Verification)	・ID管理システムの進化 ・情報を知るべき人、知ってはならない人を分ける → セキュリティクリアランスの制定
システム を守る	・FedRAMP クラウドセキュリティ認定制度	・政府クラウドの認定制度の進化 → ISMAPの改定 ハイブリッドクラウドの推進

3章 まとめ

● 日本のサイバー能力強化のための重要提案6項目

1. ウクライナ戦争においては、ハイブリッドの戦争が現実となった。台湾海峡の平和と安定への懸念が高まっている。日米同盟の最大の弱点はサイバーセキュリティである。日本の通信網や電力網がダウンすれば、戦闘が始まる前に在日米軍や自衛隊が敵対国軍隊によって倒される可能性がある。
2. 日本は、米国だけでなく、同盟国となりうる英国やオーストラリアに追いつくために、多くの宿題をこなす必要がある。
 - (1) 官邸にサイバーセキュリティ司令官を設置し、自衛隊を含むスタッフを配置すること
 - (2) サイバー司令官のための法的権限を確立すること
 - (a) サイバー状況認識、サイバースペースの監視
 - (b) 物理的な国境を越えたサイバー攻撃者の特定
 - (c) 物理的な境界を越えて持続的かつ反復的に行われる攻撃を阻止するアクティブディフェンス
 - (3) 強固なファイアウォールを備えたガバメントクラウドを構築すること
 - (a) 日本のインテリジェンスコミュニティのデジタル統合
 - (b) 機密性の高いハイテク企業や防衛産業を政府のクラウドに取り込む
 - (c) AIを活用した効果的な検索エンジンにより、良質な情報報告書を作成する
 - (d) AIとスパコンを備えたサイバーインテリジェンスのためのOSINTセンタを設立する
 - (e) データフロー全体をスパコンに保存し、オープンソースのインテリジェンス分析を行う
 - (4) 政府のIntelligenceイントラネットを、場合によっては量子技術を用いた高度な暗号化で構築すること
 - (5) 政府職員が外国人エージェントと癒着している可能性を精査するクリアランス制度を確立すること
 - (6) 安全保障分野、インテリジェンス、産業、科学技術のシナジーを高めるために、量子サイバー研究センタを設立すること
 - (a) 外国人の研究者にも門戸を開く
 - (b) 十分な政府や民間のファンドが必要である