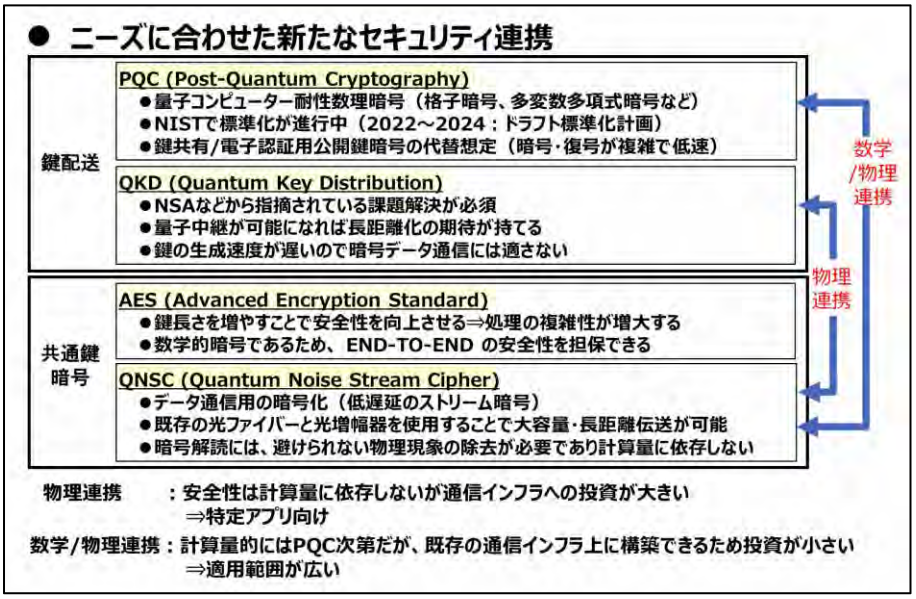

図 2-2-f 量子通信の構成要素

量子通信の適用イメージを図 2-2-g に示す。本局どうしの通信や本局と端局との通信はいわゆる専用線で接続されることが多く盗聴のリスクは低い。その一方で、端局から先のネットワークやデータセンターに接続する回線では、ターゲット（加入者や企業）を特定しやすく攻撃者が狙いやすい。これらの回線は拠点間や局舎、データセンターと Peer to Peer で接続されているため、量子通信はまずはここから守ることが考えられる。

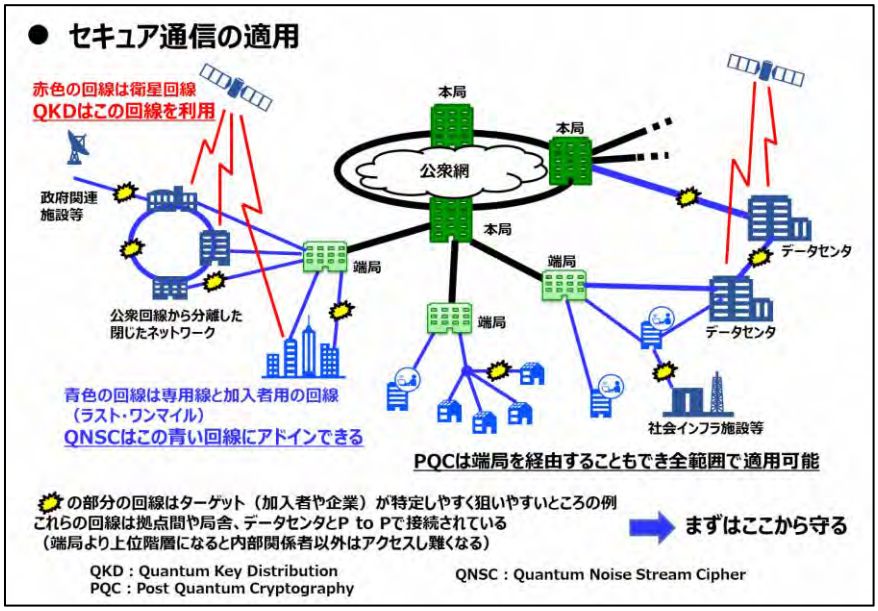

図 2-2-g 量子通信の適用イメージ

量子通信のクラウド適用に向けたイメージを図 2-2-h に示す。クラウドの中では、量子コンピュータどうしを量子通信で接続するクラスタ化が進む。さらに量子コンピュータと従来のスーパーコンピュータの間や、スーパーコンピュータとストレージの間は、ハイブリッド利用による両システムの優位性を活かす。このように特定区間で量子通信の試用を開始し早期実用化することが必須である。

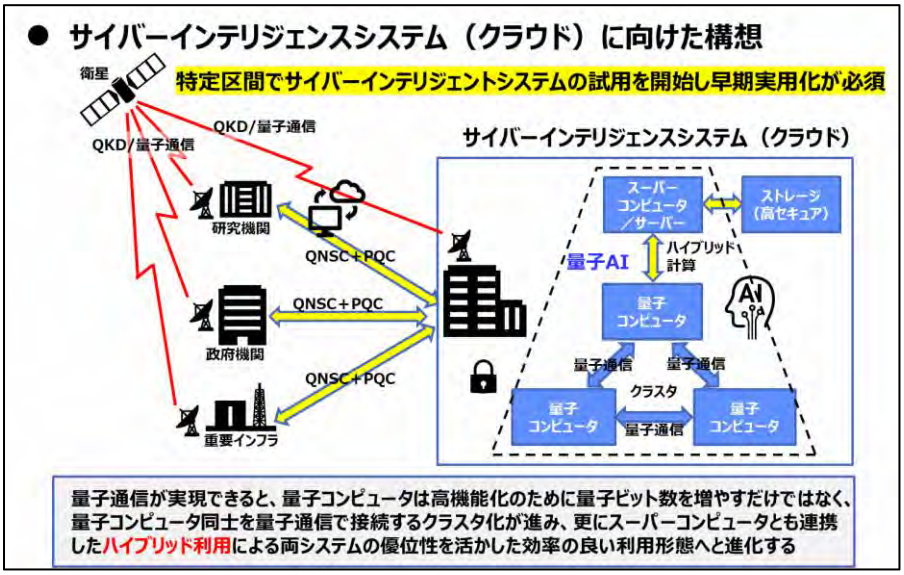

図 2-2-h 量子通信のクラウド適用イメージ

第３節 コントロールプレーン

本節では、米国のコントロールプレーンを中心に説明し、日本としての在り方を述べる。

コントロールプレーンは、政府機関に限らず、政府機関からの委託を受ける民間企業までを含めてのトラストサービスを確立する（図 2-3-a）。米国では、米国防総省（DoD）が契約業者に対して NIST が定めたセキュリティ対策ガイドライン「NIST SP800-53」「NIST SP800-171」の遵守を義務化している。DFARS の適用範囲は、米国における DoD の契約業者に限らず、日本の防衛関連業者にまで影響が及ぶ。日本としてもこのような海外にまで影響を及ぼす義務化を行うべきである。

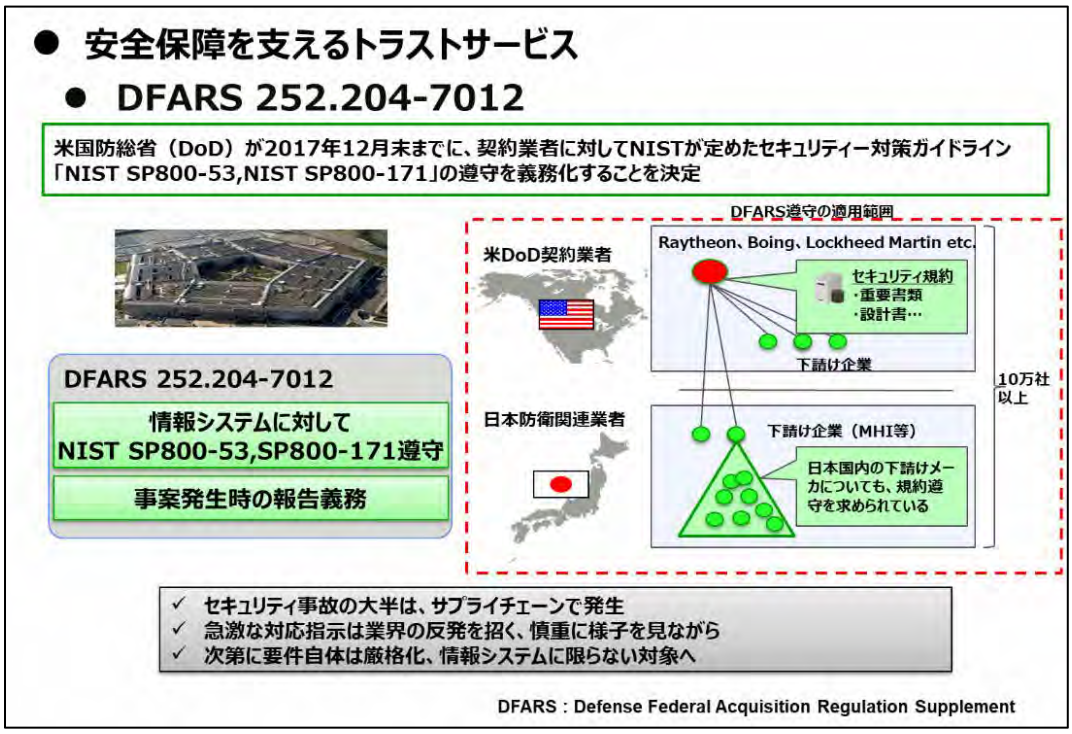

図 2-3-a 安全保障を支えるトラストサービス

コントロールプレーンで扱うデータの区分を図 2-3-b に示す。米国では大統領令 13526 号によってクラシファイド・インフォーメーション（Classified Information）を定義し、さらに大統領令 13556 号によってコントロールド・アンクラシファイド・インフォーメーション（Controlled Unclassified Information, CUI）を定義した。CUI により、クラシファイドではないが保護すべき情報という定義がなされた。CUI は、日本の防衛省における「保護すべき情報」に近い領域とみなせる。

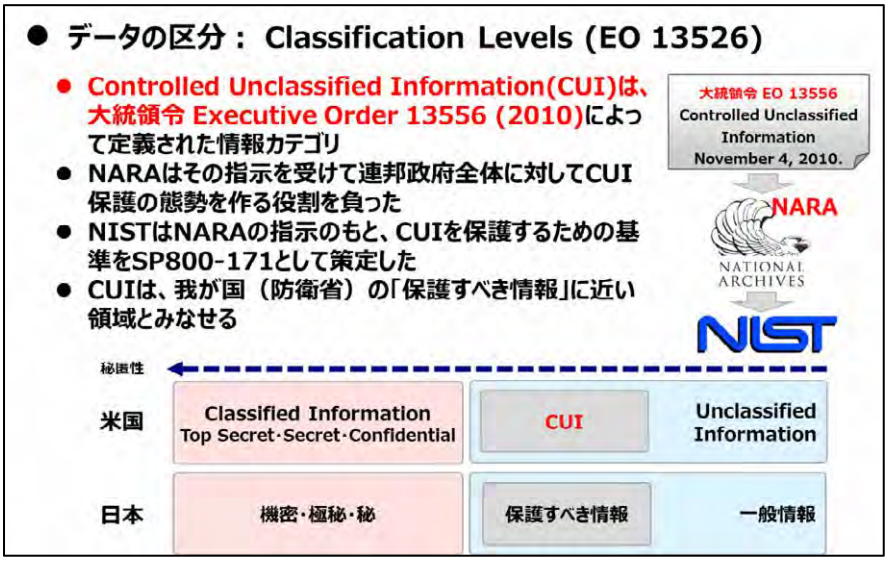

図 2-3-b データの区分

区分されたデータにアクセスするにあたり、人の区分も図 2-3-c に示すように行う。米国では 3 種類のカードを活用する。

- 連邦政府職員が所有するパーソナルアイデンティティ・ベリフィケーション（Personal Identity Verification, PIV）カード
- 国防総省職員が所有するコモンアクセスカード（Common Access Card, CAC）
- セキュリティクリアランスをパスした民間職員が所有する PIV-I（Interoperable）カード

これらのカードは、物理アクセスコントロールと論理アクセスコントロールの両方とも 1 枚のカードで実現する。

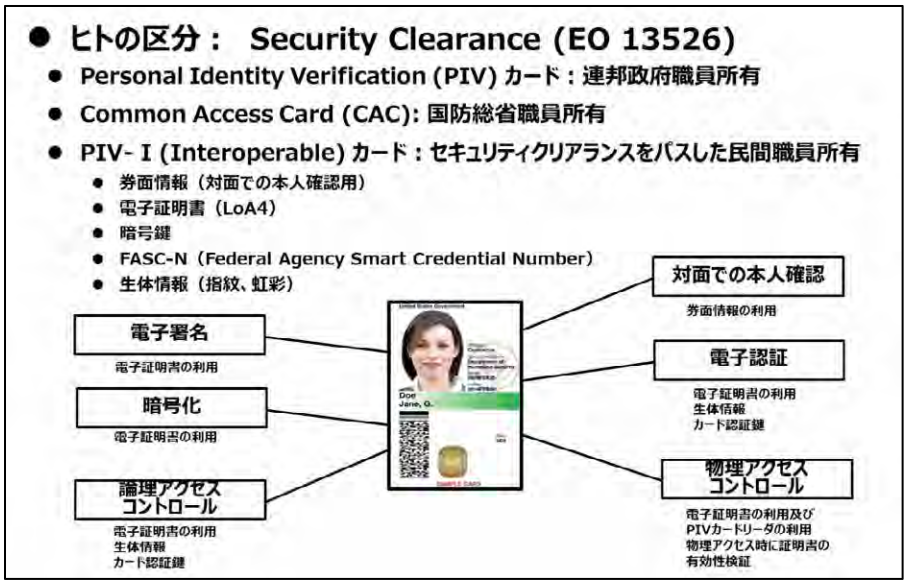

図 2-3-c ヒトの区分

ヒトの区分で述べた各種カードでは、それぞれの人に割り当てられた X.509 証明書が格納される。X.509 証明書を発行する認証局は、認証局どうしの構造（トポロジ）により相互接続するという関係をもつ（図 2-3-d）。米国の場合には、連邦ブリッジ認証局（Federal Bridge Certificate Authority, FBCA）を中心に、PIV を発行する認証局や、PIV-I を発行する認証局や、さらには海外の認証局（オーストラリア国防省）が相互接続する関係にある。

日本においてもデジタル安全保障を実現するには、米国と国家レベルでの情報共有のためには、FBCA との国際相互連携が必要不可欠である。

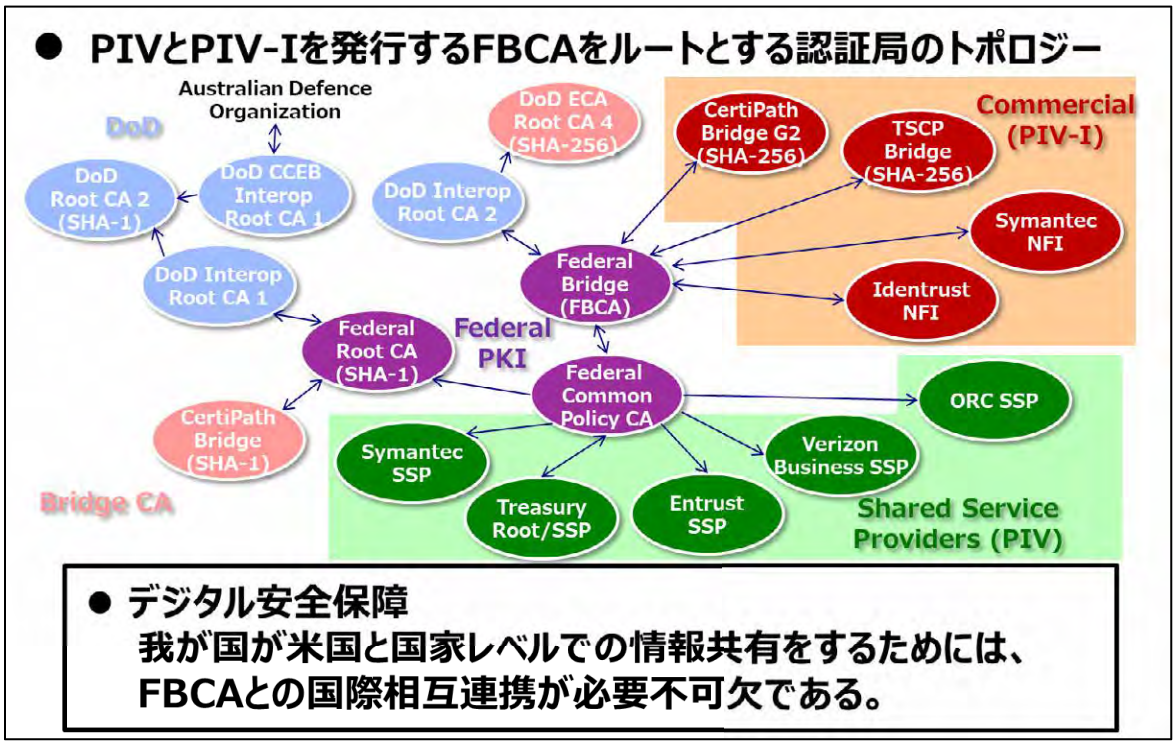

図 2-3-d トラストサービスの認証局のトポロジ

第４節 セキュリティクリアランス

セキュリティクリアランスは米国の枠組みでは、信頼されるポジションの候補者の裁定に 3 段階に分けて審査を実施する。

- 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。ライフサイクルでは以下のことを行う。

- 信頼される立場に置かれる前に、審査を行う
- 人事考課では、その役職の信頼度に応じた調査・判断基準を用いる
- 政府との雇用関係を通じて、その個人の信頼性と信用性を監視し続ける
- ライフサイクル全体の中で雇用の変化や勤務の中断を考慮し、変化に対応し、必要であれば信頼と継続雇用について新たな決定を下す

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。

裁定ガイドラインでのトピックを以下に示す。

- 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

セキュリティクリアランスは、区分システムとアクセスコントロールの連携を行う。機密情報にアクセスする適格性(Eligibility) は、米国の区分システム内のレベルに関連する。

- Top secret - 開示が国家安全保障に格別の重大な損害をもたらす情報
- Secret - 開示することにより重大な損害が発生する情報
- Confidential - 開示することで損害が発生する情報

付与される機密情報のレベルにより、適格性調査の深さは異なる

- Top secret - 最も詳細な調査
- Secret & Confidential - それほど詳細ではないが、ほとんどがこのレベルである

アクセスコントロールは、Need to Know 原則と適格性の組合せにより実施する。

日本版のデータ区分体系のフレームワーク(案)を以下に示す。

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　カテゴリー
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ーをリストアップ

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

第５節 アトリビューション

アトリビューションとは、サイバー攻撃の背後に誰がいて、何故攻撃したのか、その答えを発見する分析プロセスである。アトリビューションでは、着目する脅威が持つ意図や能力を攻撃の痕跡などを分析することによって明らかにし、攻撃グループを特定する（出典： T. Steffens. ''Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage'', Springer, 2020）。

アトリビューションの実施レベルは、低い順から高い順に並べると、以下のようになる。

（低い実施レベル）

- 既知の侵入セット・攻撃キャンペーンとの適合性確認
- 未知の侵入セット・攻撃キャンペーンの特定
- 攻撃グループの動機の特定（犯罪組織型 vs. 国家犯罪型）
- 攻撃グループの属性情報の特定
- 攻撃グループの特定

（高い実施レベル）

繰り返し利用される侵入セットや攻撃キャンペーンを見つけるためには多数のインシデント関連情報が

必要となる。そのため、「未知の侵入セット・攻撃キャンペーンの特定」より高いレベルのアトリビューションはセキュリティベンダや政府機関の役目となることが多い。

アトリビューションのプロセスは、図 2-5-a に示すように 4C モデルと言われる。

- データの収集（Collect）
- 収集したのデータのクラスタリング（Clustering）
- 攻撃グループや攻撃の動機の特定（Charge）
- アトリビューション結果の公開（Communication）

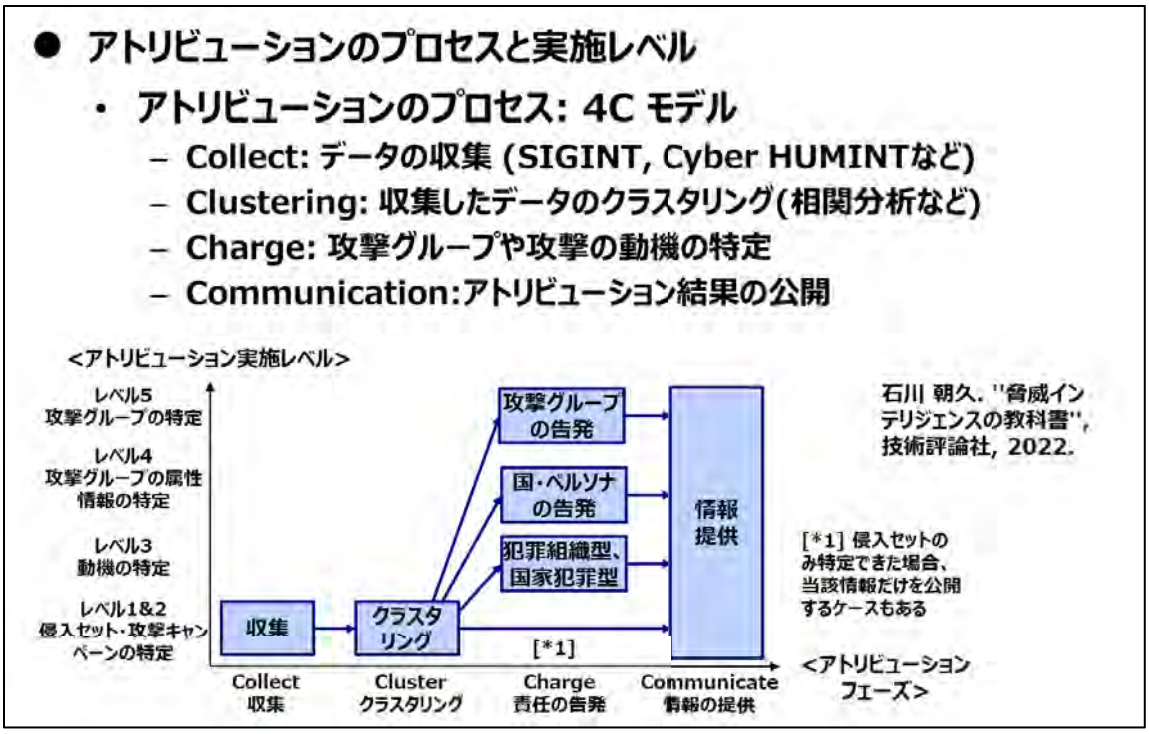

図 2-5-a アトリビューションのプロセス：4C モデル

技術的なアトリビューション手段の分類は、4 種類である（出典：R.M. Lee. “Analyzing the DHS/FBI's GRIZZLY STEPPE Report”）

- Intrusion Analysis: 侵入分析。犯罪グループの証跡により実施
- Adversary Admission: 犯罪グループ自身による犯行自認
- Leaks/OPSEC Failures: 犯罪グループ内からの情報漏洩
- Direct Access: 犯罪グループとの直接のやりとりによって実施

なお上記のうち Direct Access は、法律面・倫理面でクリアすべき課題が多い。

- Cyber HUMINT: 当該犯罪グループが存在するコミュニティに潜り込み協力者やコミュニティから情報を引き出す技術（出典：R. Burkett. “An Alternative Framework for Agent Recruitment: From MICE

to RASCLS”）

- Offensive Countermeasures(OCM): 当該犯罪グループの情報が露呈するような技術を用いてアトリビューションする技術（出典：J.Strand, P. Asadoorian, B. Donnelly, B. Galbraith, E. Robish. ''Offensive Countermeasures: The Art of Active Defense'', CreateSpace, 2017）

日本では、相手の許可を得ずに Offensive Countermeasures を実施すると日本国内法では犯罪となる。そのため、技術的な手段だけでなく、政治的・経済的・社会的な観点などから多角的にアトリビューションを加えることが重要である。

アトリビューションを実現できたとしてさらに、日本独自のインテリジェンスシステムでは、他国に give するに値するクローズド・ソース・インテリジェンスを作り出すことが重要となる。オープンソースインテリジェンス（OSINT）は、他国も同じ OSINT を入手できるため、そこで作られたインテリジェンスは他国に give するに値しない。そうではなく、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（Indo-Pacific Economic Framework, IPEF）などを活用し、他国に give するに値するクローズド・ソース・インテリジェンスを作り出すことが必要不可欠である。

第３章 アトリビューション

第１節 本章の調査研究方針

我が国は、特に APT（Advanced Persistent Threat）グループによるサイバー脅威の増大に直面し、サイバーセキュリティ能力の強化、特に日本政府および日本の重要インフラに対するサイバーリスクをより適切に管理するためのサイバー脅威情報（CTI）の収集と有効活用を強化する必要がある。CTI は、サイバーリスク管理の取り組みに不可欠な要素であり、包括的な CTI プログラムは、我が国が直面する新たな脅威や変化する脅威を把握し、シナリオの立案、テスト、演習に不可欠だ。サイバー脅威の全体像を完全に理解することは、日本の全体的なサイバーリスクを理解するためだけでなく、多数のリスクの中から優先順位を決め、適切な緩和活動を行い、デューディリジェンスを実証し、保証活動に必要なベースラインを提供するためにも不可欠である。

現在の我が国における国家的なサイバーセキュリティの取り組みに対する責任と権限は、各府省庁から構成される政府のエコシステムに分散している。国家的な CTI の取り組みには、これらの異なる組織間の効果的な調整が必要である。さらに、効果的な CTI プログラムには、海外の同盟国との緊密な協力が必要である。特に日本は、サイバー関連の様々な問題や懸念について、日米豪印戦略対話（Quad）や主要 7 ヶ国首脳会議（G7）の同盟国とより密接に協力することを求めている。

本章では、攻撃者の意図と能力を含むエンドポイント動作に焦点を当てたサイバー脅威のアトリビューション技術の研究および分析を、以下のように実施する予定である。

- 安心・安全シンクタンク事業のサイバー班の昨年度の成果物の一つである Cyber Intelligence Landscape Review に記載されている Cyber Intelligence (CI) Ecosystem の文脈で、サイバー脅威のアトリビューションを説明する。
- 米国で現在使用されているサイバー脅威のアトリビューションプロセスのアーキテクチャを説明する。この説明には米国におけるアトリビューションの取り組みに従事している関連組織を特定することを含む。
- 米国におけるサイバー脅威のアトリビューションに関する現在の代替的アプローチについて説明する。
- サイバー脅威のアトリビューション活動を成功させるための、技術的なツールを含むベストプラクティスを説明する。

第２節 アクティブ・サイバー・ディフェンス（ACD）を取り巻く状況

悪意のあるサイバー活動は、国家および経済の安全保障に重大な悪影響を及ぼす可能性がある。例えば、大企業や米国政府の大部分が使用しているソフトウェア「SolarWinds」がロシアからハッキングされた事件

では、被害者の損害額とシステムの復旧費用が 1000 億ドル以上に上ると推定されている[1]。コロニアル・パイプラインに対するランサムウェア攻撃では、パイプラインが停止させられ、米国東海岸の燃料供給が停止し、燃料不足、ガソリン販売店でのパニック購入、ガソリン価格の上昇を招いた。この問題を解決するために、パイプライン運営会社は、攻撃者である DarkSide と呼ばれるハッキンググループに約 500 万ドルの身代金を支払った。

世界では、企業のサイバースパイ活動、産業情報や個人情報の窃取、政府機関の監視、重要インフラへの攻撃などの事件が増え続けている。同時に、ファイアウォールの強化、脆弱性の修正、正当なアクセスに対する障壁の増加など、純粋に受動的なサイバー防御活動だけでは、巧妙化する攻撃の流れを食い止めることはできないことがますます明らかになってきている。ネットワーク防御者は、より積極的なアプローチを取りたいと考えており、攻撃者が境界線に到達する前に阻止し、さらに進行中の攻撃も阻止しようとする。その結果、これまで ACD と呼ばれてきた技術を利用しようとする防衛者が増えている。

しかし、サイバー空間におけるルールは、防御者がネットワークとその中に含まれるデータを保護するためにどのような手段を講じることができるかについて、必ずしも明確ではない。現在、国益を守ろうとする政府に適用されるルールを定義するための国際的な作業が進行中である。受動的なサイバー防衛活動（すべてのサイバー防衛者に一般的に認められている活動）とサイバー攻撃者のネットワークに侵入する攻撃的なサイバー防衛活動（一般的に政府に限定されている）の間に位置するサイバー防衛活動の範囲は、いわゆる「グレーゾーン」に属すると特徴づけられている。このグレーゾーンには、受動技術の上端から攻撃技術の下端まで、考えられる防衛活動の数々が含まれ、どの技術を、誰が使うことができるかは明白ではない、という事実が言及されている。

日本政府は、現在のサイバー環境では受動的なサイバー防御だけでは不十分であることを認識し、最新の国家安全保障戦略の中で、サイバー態勢を改善するために ACD 技術を導入する意向を明確に示している。

本章では、ACD 技術について、その使用をめぐる政策的・法的制約、および使用に関する実際的な懸念事項を検討する。また、米国のアプローチを含め、ACD が今日までどのように使用されてきたかを検証する。日本政府が ACD に関する国策と展望を練り直す際には、自国の「グレーゾーン」の境界線と、その範囲内での技術の使用に適用される制約を決定する必要がある。

1. ACD の定義

アクティブ・サイバー・ディフェンス」という用語は広く使われているが、一貫して定義されていない。この明確性の欠如は、どの防御活動がどのタイプの防御者に適切であるかの議論を複雑にしている。

ACD は一般に、サイバーインシデントの発生前、発生中、発生後に、組織がリアルタイム、またはほぼリアルタイムでネットワークをサイバー脅威から防御するために使用する運用上のインシデント対応プロセスおよび技術的能力を指している。これらの活動は、一般的な性質で、進行中の特定の脅威とは別に存在す

[1] Ropal Gatnum, “Cleaning up SolarWinds hack may cost as much as $100 billion,” Roll Call, January 11, 2021, https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/