個別調査分析 2
サイバーセキュリティ領域

Project Manager
手塚悟 慶應義塾大学 教授

Project Member
甲斐 賢 政策研究院 リサーチ・フェロー
原澤克嘉 政策研究院 リサーチ・フェロー
近藤賢郎 政策研究院 リサーチ・フェロー

目次

第１章 サイバー防衛の日米の比較

サイバー領域では、日本が海外に比べて出遅れているサイバー脅威インテリジェンスを中心に、深堀調査と幅広調査を行った。本章では、それらの調査および比較の結果を示す。

第１節 日本を取り巻く背景

2022 年 2 月に開始したウクライナ軍事進攻では、ロシアは重要インフラのネットワークを攻撃し（図 1-1-a）、偽情報を流した（図 1-1-b）。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。ただし、日本のサイバー防衛隊は関与していないのが現状である。

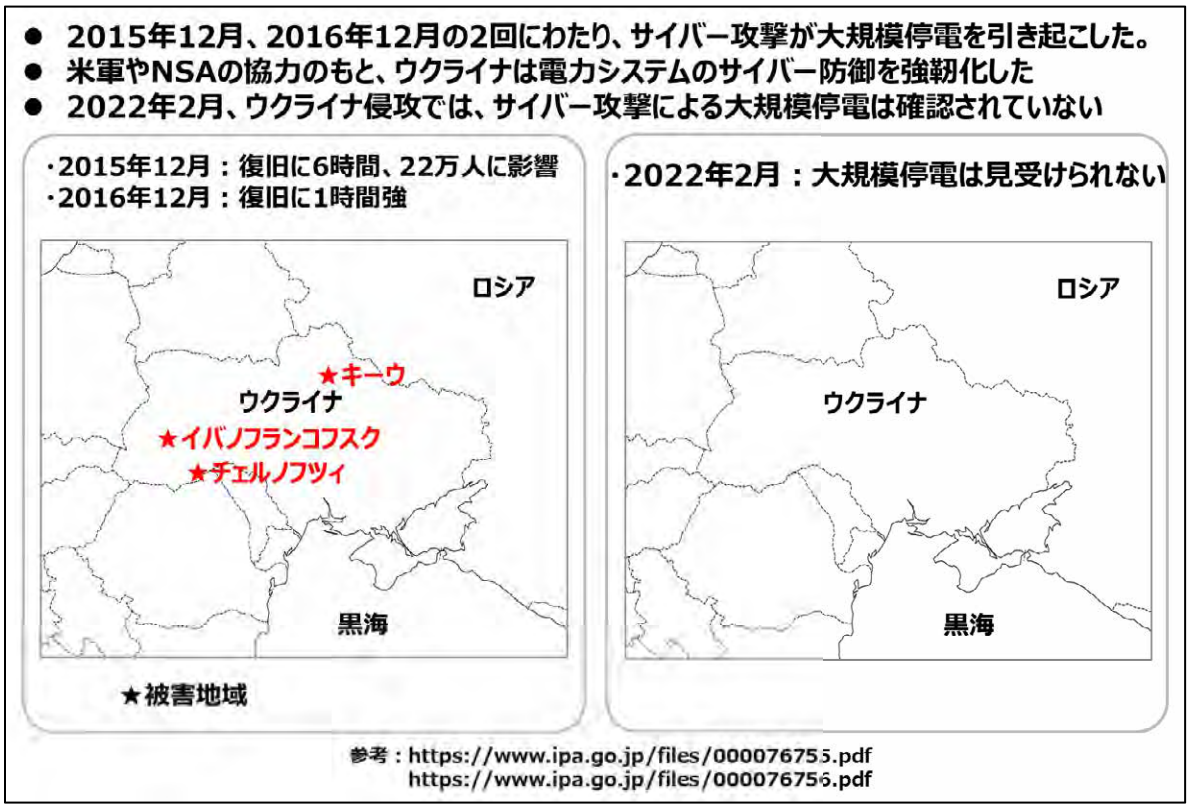


図 1-1-a ロシアによるウクライナ重要インフラへのネットワーク攻撃

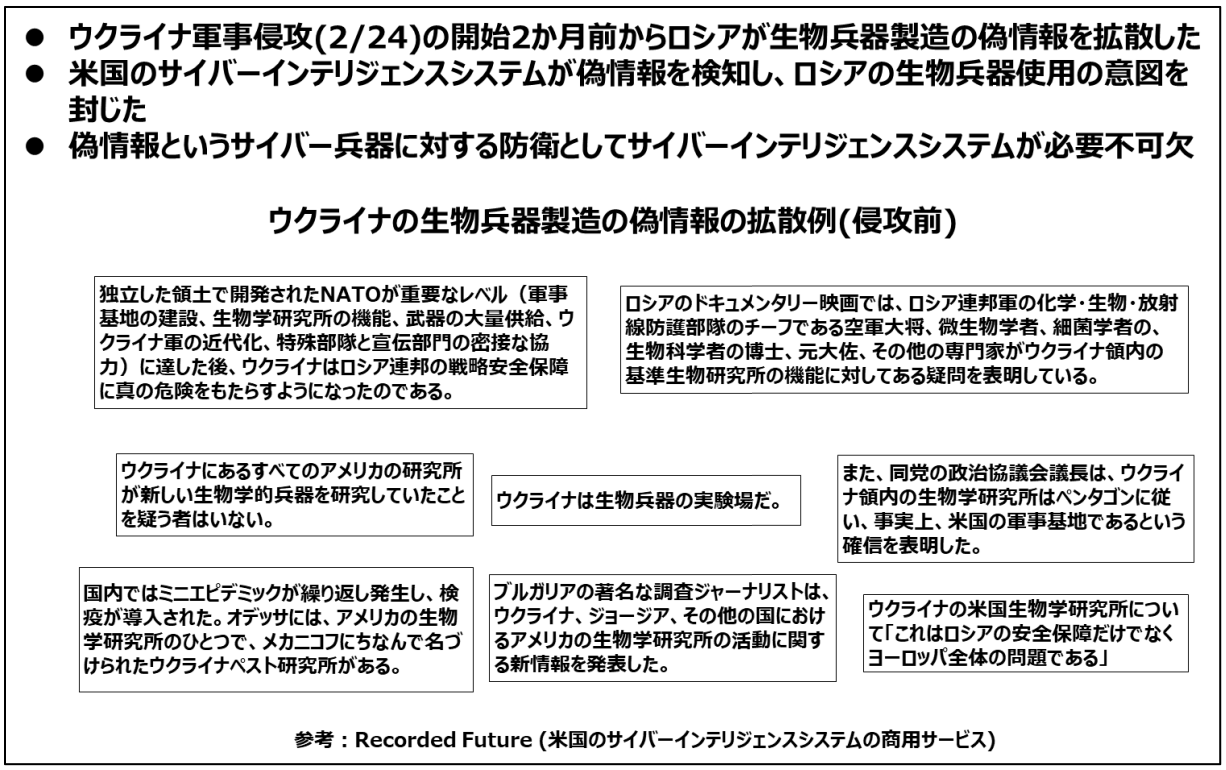


図 1-1-b ロシアによる偽情報の流布

台湾海峡の平和と安定への懸念が高まっている（図 1-1-c）。ただし、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。

図 1-1-c 台湾重要インフラへのネットワーク攻撃と偽情報の流布

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。

第２節 米国のサイバー防衛能力

米国政府におけるサイバー組織と各種委員会の全体像を図 1-2-a に示す。本図は Cyberspace Solarium Commission が策定した図であり、ホワイトハウスを頂点に、政府組織、重要インフラ、民間企業および住民や、パートナーとの連携までを含む、ビッグピクチャである。

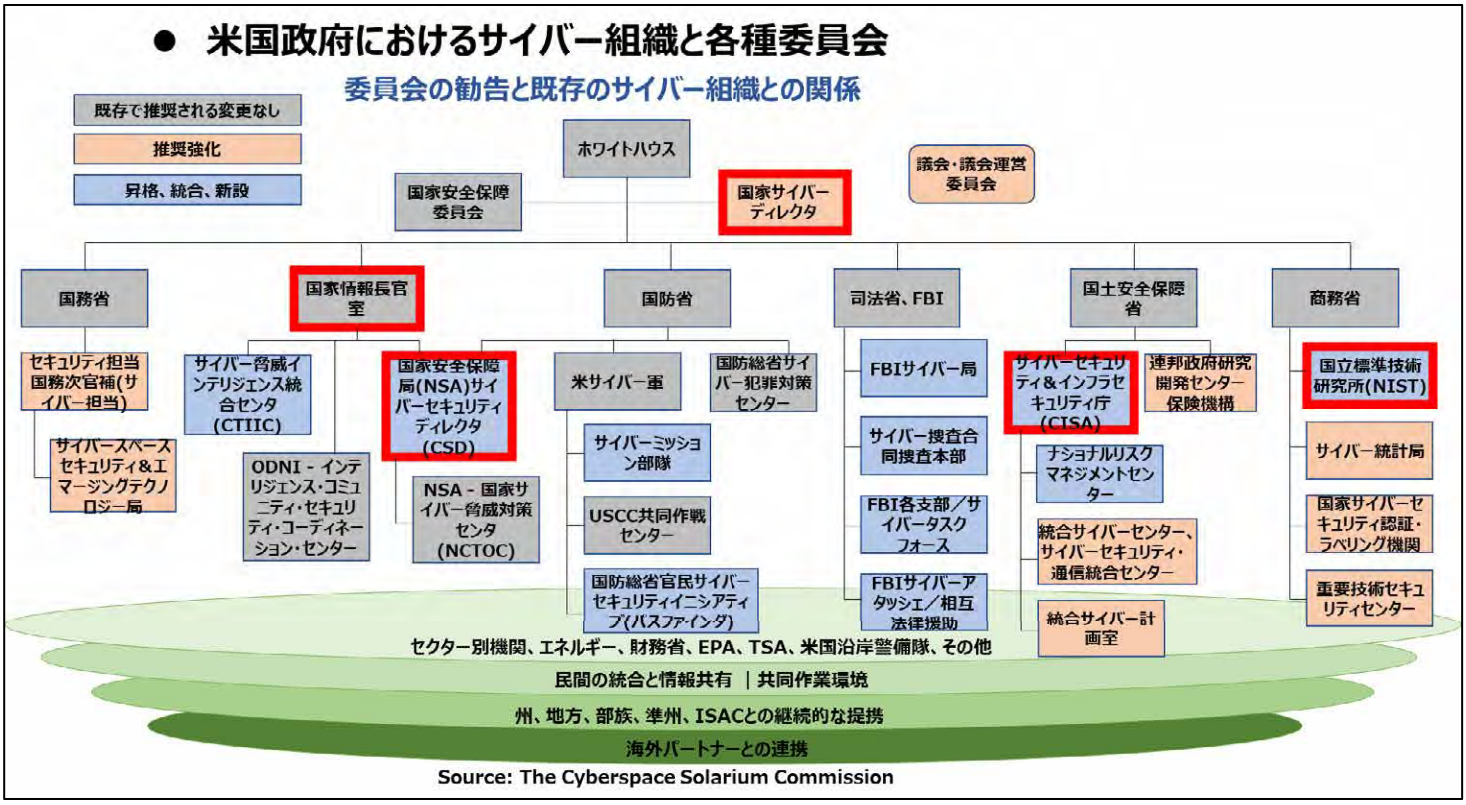


図 1-2-a 米国政府におけるサイバー組織と各種委員会

米国のサイバー防衛能力の構成要素と簡素化して図 1-2-b に示す。ポイントは 3 点である。

- ホワイトハウスのもとに、ナショナル・サイバー・ディレクターを配置する。本ナショナル・サイバー・ディレクターは、各省庁に横断的に指揮するための司令塔の役割を担う。
- 国家情報長官と国防長官のもとに、国家安全保障局（National Security Agency, NSA）とサイバー・コマンドを配置する。NSA/サイバー・コマンドは、有事にならないように平時からの情報収集や事前の実行部隊となるための役割を担う。
- サイバーセキュリティとインフラ・セキュリティ・エージェンシー（Cybersecurity and Infrastructure Security Agency, CISA）のもとに、ジョイント・サイバー・ディフェンス・コラボレーティブ（Joint Cyber Defense Collaborative, JCDC）を配置する。JCDC は、政府機関ネットワーク・オペレーターや、民間企業ネットワーク・オペレーターとの情報共有や調整のための役割を担う。

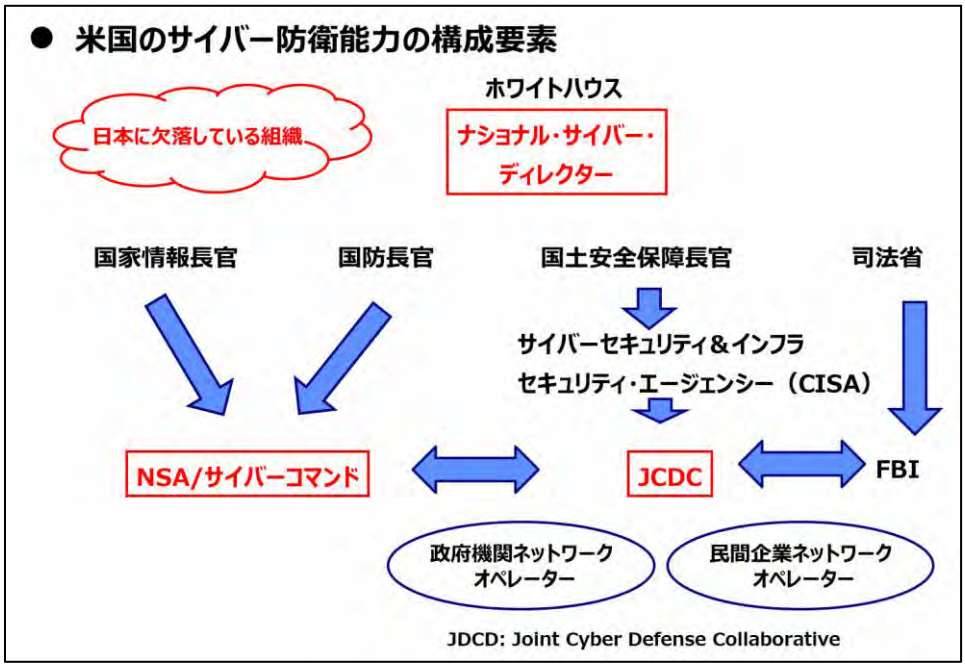


図 1-2-b 米国のサイバー防衛能力の構成要素

日本とのイコールフッティングにおいて、日本に欠落している組織が「ナショナル・サイバー・ディレクター」「NSA/サイバー・コマンド」「JCDC」の 3 つである。

第３節 日本のサイバー防衛能力

日本の省庁の強みと弱みをまとめる。弱みを下線に示す。

内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity, NISC）は、ポリシーや脅威アラートを提供するが、政府機関や民間企業に対するサイバーセキュリティの運用権限はない。また、タイムリーな運用情報を提供しない。さらに、海外との接続が遅く、弱い。

デジタル庁は、政府ネットワーク（防衛省を除く）を集中的に提供しているが、運用上のサイバーセキュリティに関する指令は出せない。

警察庁は、国内のサイバー犯罪を起訴し、児童ポルノ、ATM 窃盗、ランサムウェアなどの国際的なサイバー犯罪についてはインターポールを通じて活動している。

日本におけるサイバー防衛の活動は、憲法解釈と通信規制が日本のネットワークの積極的な防衛を阻んでいる。

米国の NSA や英国の GCHQ（Government Communications Headquarters）に匹敵するサイバー情報機関が日本にはない。防衛省は、サイバー担当者を 800 人から 5,000 人に拡大する計画を発表した。ただし、防衛省は現在、外国のネットワークに侵入する権限を持っていない。

日本の民間企業の強みと弱みをまとめる。弱みを下線に示す。

民間企業では、脅威に対する認識が広まっている NTT ドコモ、ソフトバンク、KDDI などの通信事業者は、ネットワークセキュリティが充実している。JPCERT や ISAC が設置されている。

経済産業省の産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が、発電所、工場のスタッフに優れたトレーニングを提供し、 米国とのつながりも深い。

三菱電機、NEC といった日本の大手企業が深刻な情報漏えいに見舞われた。中小企業は非常に脆弱である。

日本のサイバーセキュリティ分野は、必要性の大きさに比べて、僅かである。日本では CERT や ISAC といった連携した脅威対応の仕組みが遅れている。

日本のサイバー防衛能力をまとめると図 1-3-a に示す評価となる。多層的なサイバー抑止の評価として、1 番目の行動規範の形成、2 番目の便益の非提供、3 番目のコストの強要のうち、日本の目標は 3 番目のコストの強要であるのに対して、日本の現状は 1 番目の行動規範の形成にありこれから 2 番目の便益の非提供にさしかかるところである。

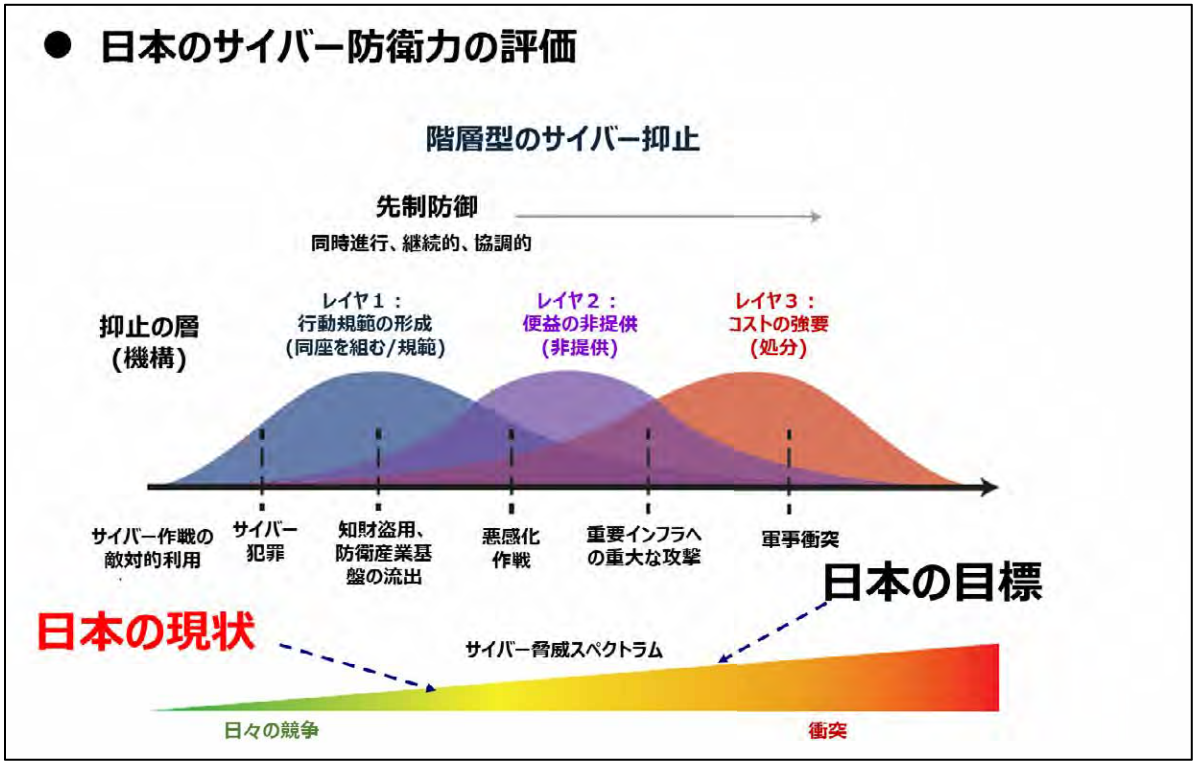


図 1-3-a 日本のサイバー防衛力の評価

第４節 日本のサイバーセキュリティ開発の次のステップ

日本のサイバーセキュリティ開発の次のステップをまとめる。

- 海外と互角なサイバーインテリジェンス機関の設立
  - セキュリティクリアランス制度
  - 出発点 - GCHQ 程度の規模（スタッフ 6,000 人、予算 20 億ポンド） https://www.gchq.gov.uk/

- NISC と JDA（Japan Defense Agency）のどちらの機関が、政府ネットワークのサイバー防衛に関する指揮を執るかを決定する
  - 指揮を執ることが決まった機関への指示権限の付与

- 政府・民間のオペレーションセンターの設立
  - 米国 JCDC（Joint Cyber Defense Collaborative）と同等の機関
  - サイバーセキュリティに責任を持つすべての主要な政府機関を含む
  - 主要な通信事業者を含む
  - 主要なインフラ事業者に拡大する

- 外国のネットワークに侵入するための憲法解釈と法的権限を与える

- 国家サイバー担当大臣を設置
  - 内閣総理大臣の直属の部下
  - 少人数のスタッフ
  - 政府および民間ネットワークにおけるサイバーセキュリティの向上と、脅威への対応の統括を行う

米国情報報告書の 4 分の 3 は、NSA によるものと言われている。サイバーインテリジェンス機関の設立は必須である。さらに、外国のネットワークに侵入することは、ウクライナ経験から導かれたものである。

これらステップを進める上では、日米同盟におけるサイバー防衛のカウンターパートの整備も行う（図 1-4-a）。まず、日本のナショナル・サイバー・ディレクターを新規に置く。つぎに、日本のサイバーインテリジェンス機構を新規に置く。さらに、NISC GSOC や、日本のナショナル CERT、デジタル庁の権限付与と再組織化を行う。

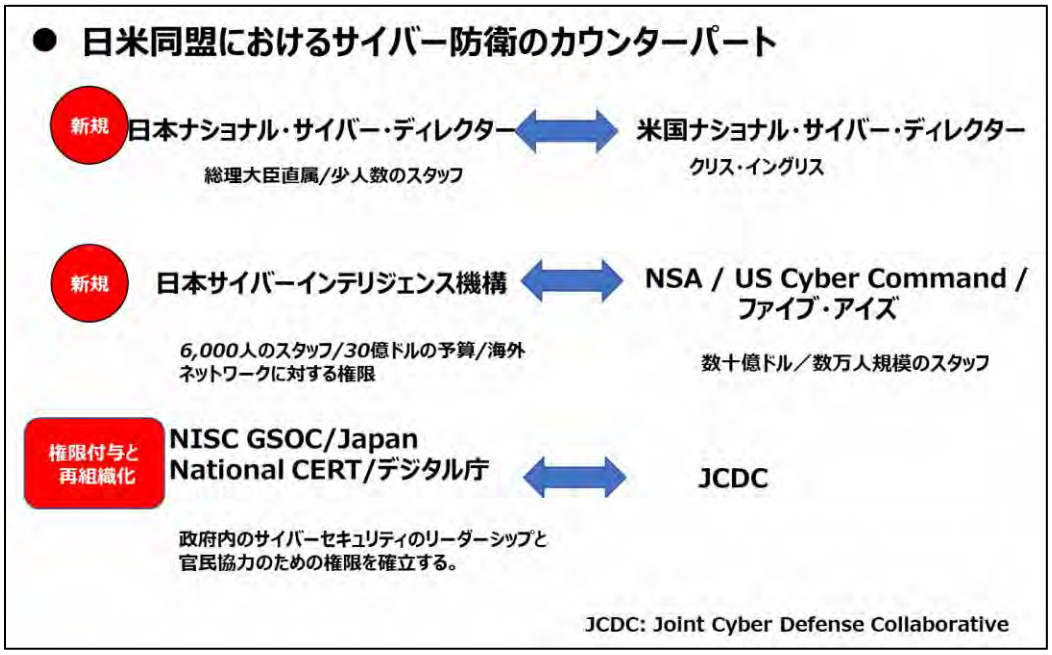


図 1-4-a 日米同盟におけるサイバー防衛のカウンターパート

第５節 国家サイバーインテリジェンスの全体像

日本はサイバーインテリジェンスに貢献できるなら、歓迎される立場にある（図 1-5-a）。そのためには、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 できることが必要である。

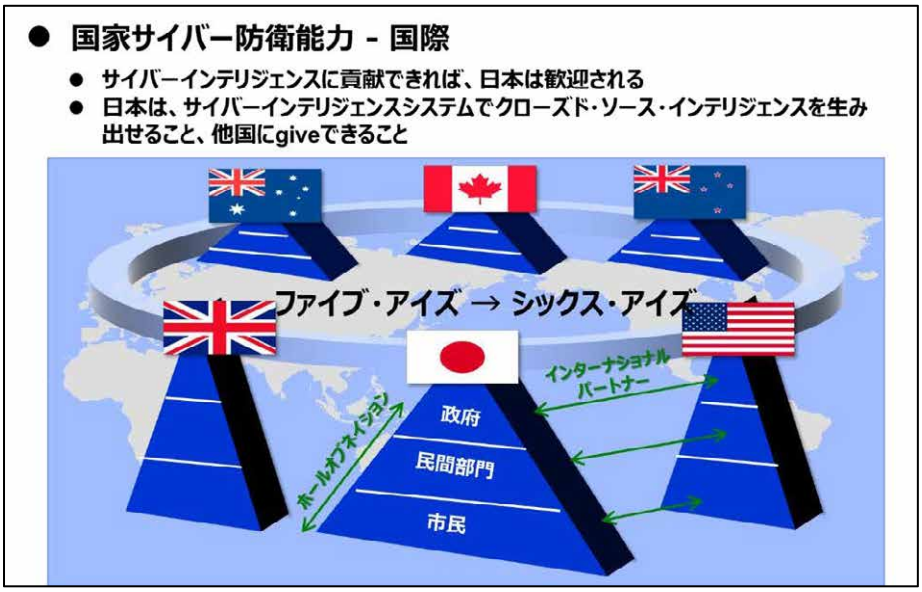


図 1-5-a 国家サイバー防衛能力の国際的な連携

国家サイバーインテリジェンスの全体像を図 1-5-b に示す。国家サイバーインテリジェンスは、大きく４つの階層「政府」「重要インフラ」「民間企業」「住民」で構成する。

「政府」階層では、国家サイバーインテリジェンスセンターを設け、本センタが、民間、防衛、警察を含むトータルな意味での司令塔の役割を担う。本センタは機能として、省庁横断的に、脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。さらに、本センタは国際パートナーとの窓口となる役割も担う。さらに以降に述べる、重要インフラ、民間企業、住民の階層における CERT/CSIRT とも連携を行う。

「重要インフラ」階層では、各セクターに設置される CERT/CSIRT が、セクターごとの脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。セクター間の連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。

「民間企業」階層では、民間企業や自治体のそれぞれに設置される CERT/CSIRT が、民間企業および自治体それぞれの脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。民間企業どうしや自治体どうしの連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。

「住民」階層では、官民連携としての情報共有センタ、情報共有組織、学会、市民社会が脅威/リスク分析、インシデント追跡、対処協調、インシデント調査、サイバーセキュリティ状況認識、標準整備を行う。住民の階層どうしの連携を行うとともに、前述の政府の階層の CERT/CSIRT とも連携する。

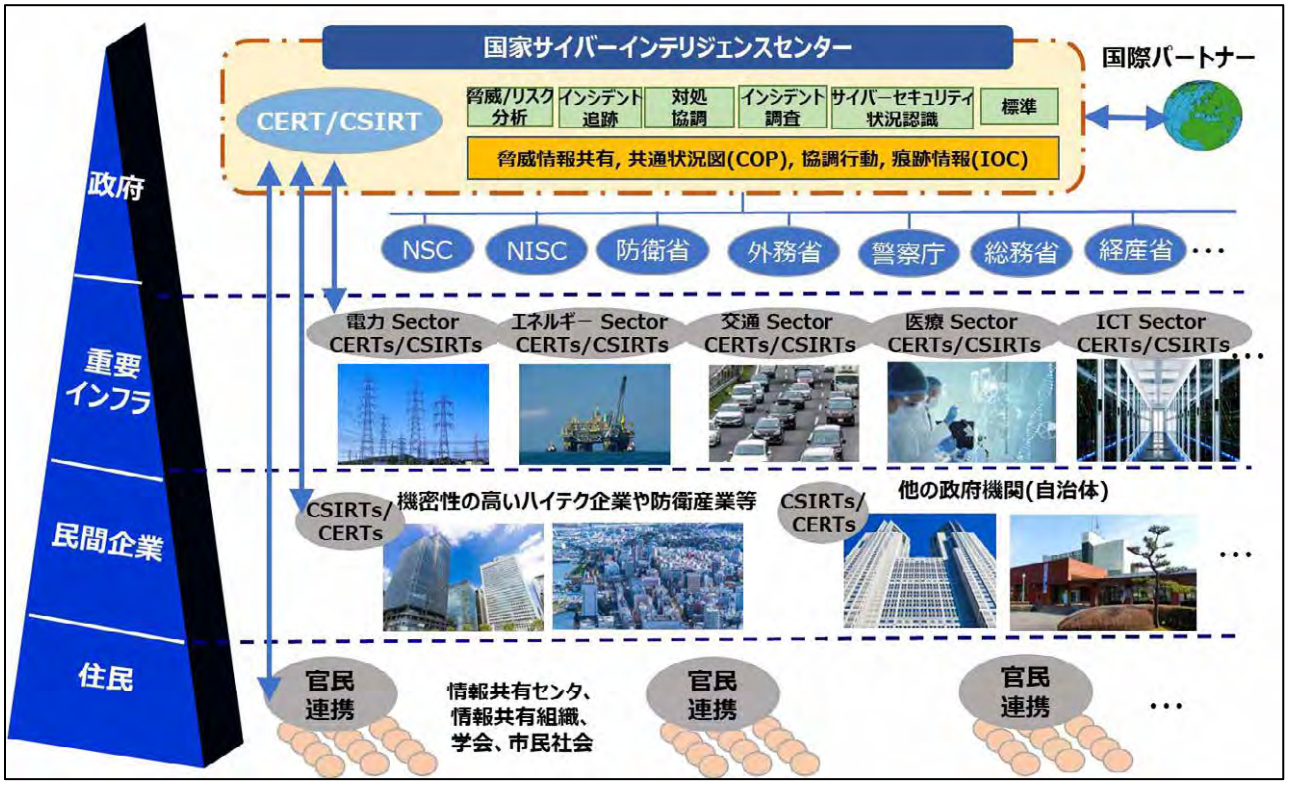


図 1-5-b 国家サイバーインテリジェンスの全体像

サイバーインテリジェンスの策定範囲を図 1-5-c に示す。オープン・ソース・インテリジェンスにあたる部分は当然であるが、さらに日本ならではのクローズド・ソース・インテリジェンスまでが策定範囲である。

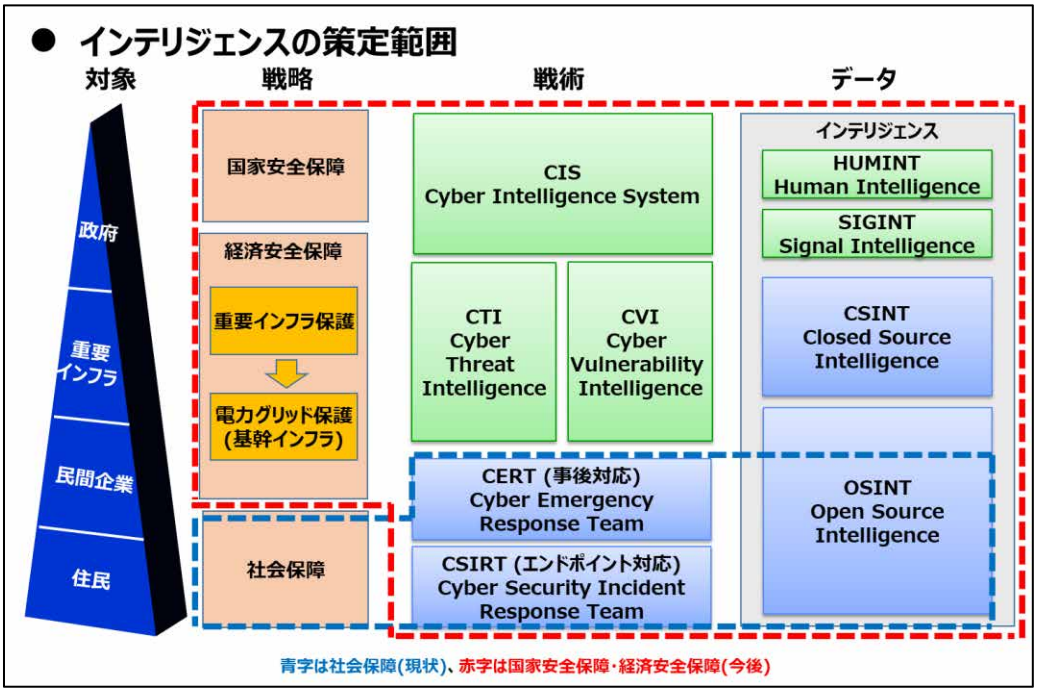


図 1-5-c サイバーインテリジェンスの策定範囲

サイバーインテリジェンスシステムが果たす機能の全体を図 1-5-d に示す。インテリジェンスを活用しての、政策提言、国際連携、安全保障の調査・分析の機能を持つべきである。

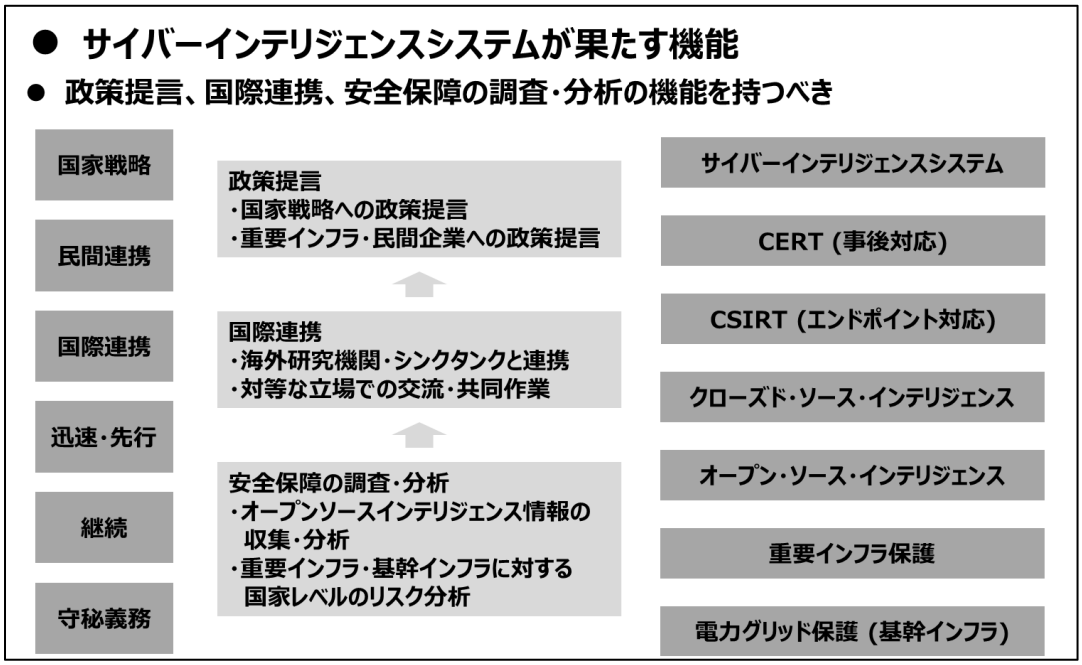


図 1-5-d サイバーインテリジェンスシステムが果たす機能

第２章 サイバーインテリジェンスシステム

第１節 システムの全体像

国家サイバーインテリジェンスの「政府」の階層にあたる、国家サイバーインテリジェンスセンターの全体像を図 2-1-a に示す。国家サイバーインテリジェンスセンターは、「セキュリティクリアランス」「コントロールプレーン」「データプレーン」の３つの階層で構成される。

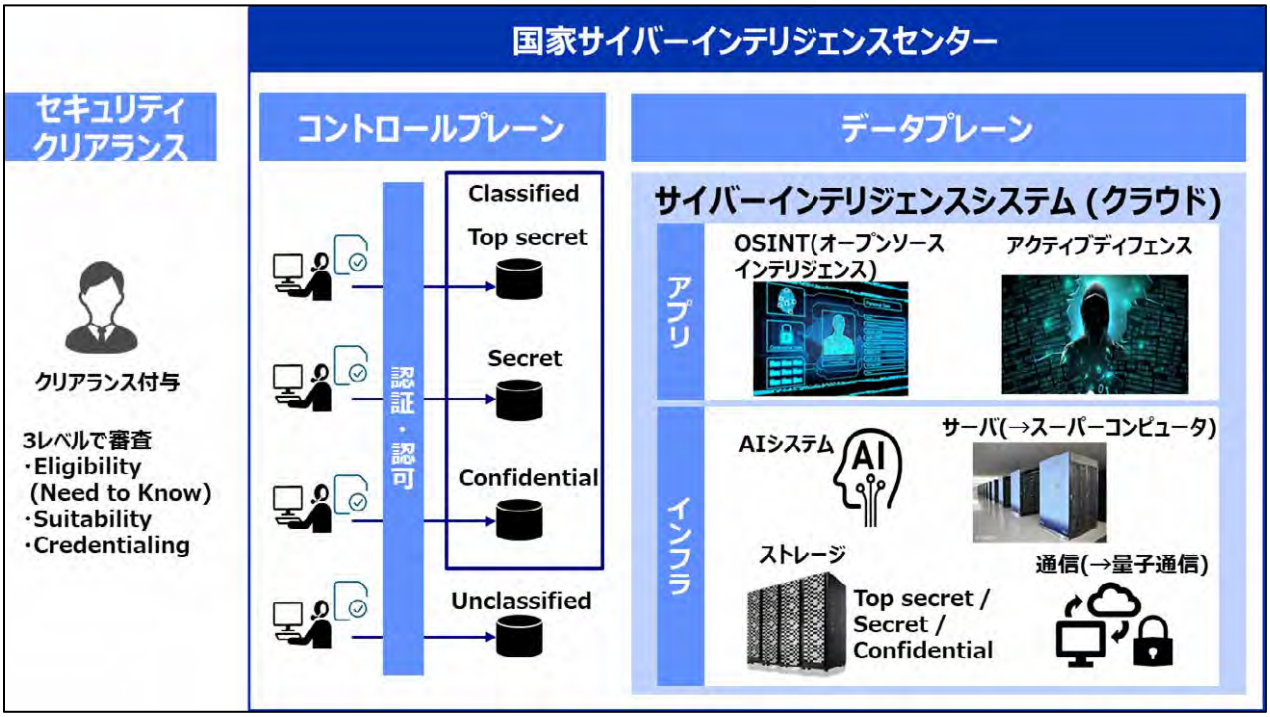


図 2-1-a 国家サイバーインテリジェンスセンターの概要

「セキュリティクリアランス」では、国家サイバーインテリジェンスを扱う権限のある者に適切に権限を与えるとともに、Need to Know の原則にしたがい必要に応じて機密情報を共有すべき人物であることを特定する。セキュリティクリアランスの付与のための審査は、厳格性（Eligibility, Need to Know）、適切性（Suitability）、クレデンシャル付保（Credentialing）のすべての手順を行うことで実施する。とくにクレデンシャル付与では、耐タンパ機能を備えた可搬性のある IC カードなどに、当該人物を物理的およびサイバー的に一意に識別するための情報（多くの場合は X.509 証明書）を格納して、当該人物だけが所有するような形で渡すものである。

「コントロールプレーン」では、クリアランスを与えられた者が、物理的およびサイバー的に認証され、必要なデータにアクセスするための、識別・認証・認可を適用する基盤である。本プレーンは、当該人物が与えられたデジタルアイデンティティのもとに、トップシークレット、シークレット、コンフィデンシャル、

アンクラシファイドの情報にアクセスするための基盤を構成する。

「データプレーン」では、サイバーインテリジェンスシステムを構成し、多くの場合にはクラウドサービスとして提供する。サイバーインテリジェンスシステムは、アプリケーション層とインフラ層とから構成される。アプリケーション層は、サイバーインテリジェンスを、広く流通する OSINT（オープンソースインテリジェンス）から収集し分析するとともに、もし国家がサイバー攻撃を受けた際に攻撃者を特定し反撃可能な能力を示すための、アクティブディフェンスも担う。また、インフラ層は、民間で広く使われるクラウドサービスに比べてさらに「AI システム」「サーバー（スーパーコンピュータ）」「ストレージ」「通信（量子通信）」を備えるものである。

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を以下に示す。

- サイバースレットインテリジェンス（Cyber Threat Intelligence, 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

- サイバーバルネラビリティインテリジェンス（Cyber Vulnerability Intelligence, 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)

- アトリビューション
  - 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

第２節 データプレーン

1. アプリケーション

サイバーインテリジェンスシステムは、2 大インテリジェンスとして CTI と CVI を扱う。

CTI とは、サイバー脅威に関わるインテリジェンスである（図 2-2-a）。CTI が効果的であるとは、「敵に関する情報」「技術環境」「関連性」の共通部分に焦点をあててアクションを施すことである。CTI を形成するには、商用プロバイダのデータソースや、政府系プロバイダーのデータソースからデータを収集し、生データ、処理データ、分析データへと次第にインテリジェンスを濃縮する。CTI の良否を決める評価基準は、「適時性」「精度」「使い勝手の良さ」「カバレージ」「リソース」「（データ処理の）スケーラビリティ」「（機能の）拡張性」「コンテキスト」である。

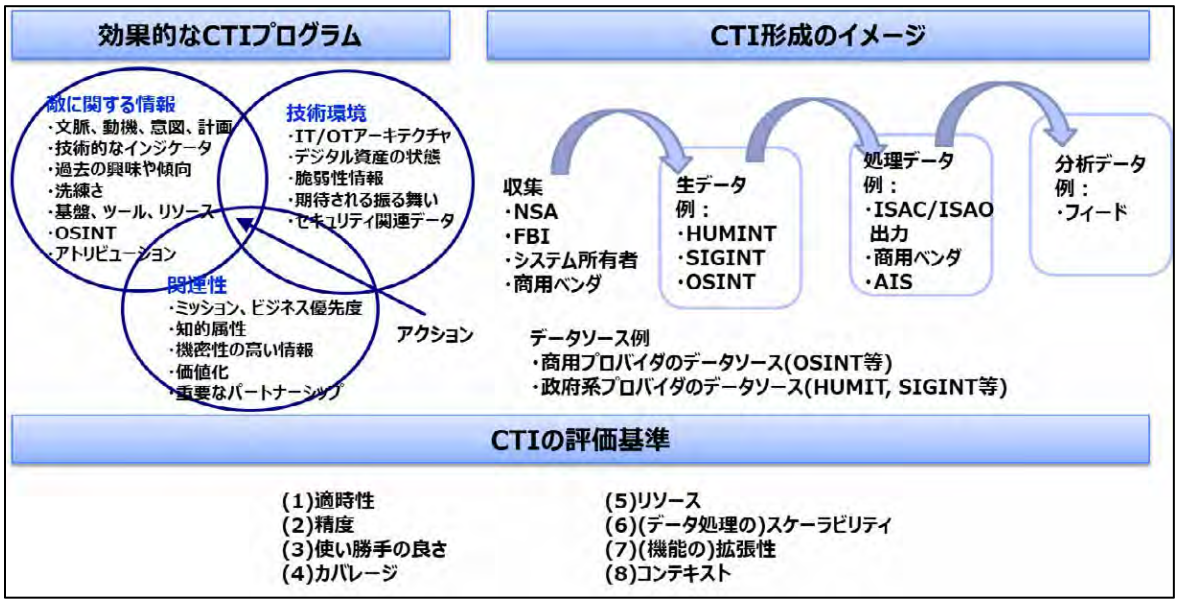


図 2-2-a サイバースレットインテリジェンス（CTI）の概要

CVI とは、サイバー脆弱性に関わるインテリジェンスである（図 2-2-b）。CVI が効果的であるとは、脆弱性を悪用することの容易さと、脆弱性を悪用した場合の影響の大きさの共通部分に焦点をあててアクションを施すことである。CVI を形成するには、公開データベースや商用サービスサイトなどからデータを収集し、生データ、処理データ、分析データへと次第にインテリジェンスを濃縮する。CVI の良否を決める評価基準を以下に示す。

- 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ーや不注意によってシステムに導入されたものか
- 既知の脆弱性が存在するか
- 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の理解
- 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
- 評価対象のシステムのベンダーやサプライヤーが新規で未試験であるか

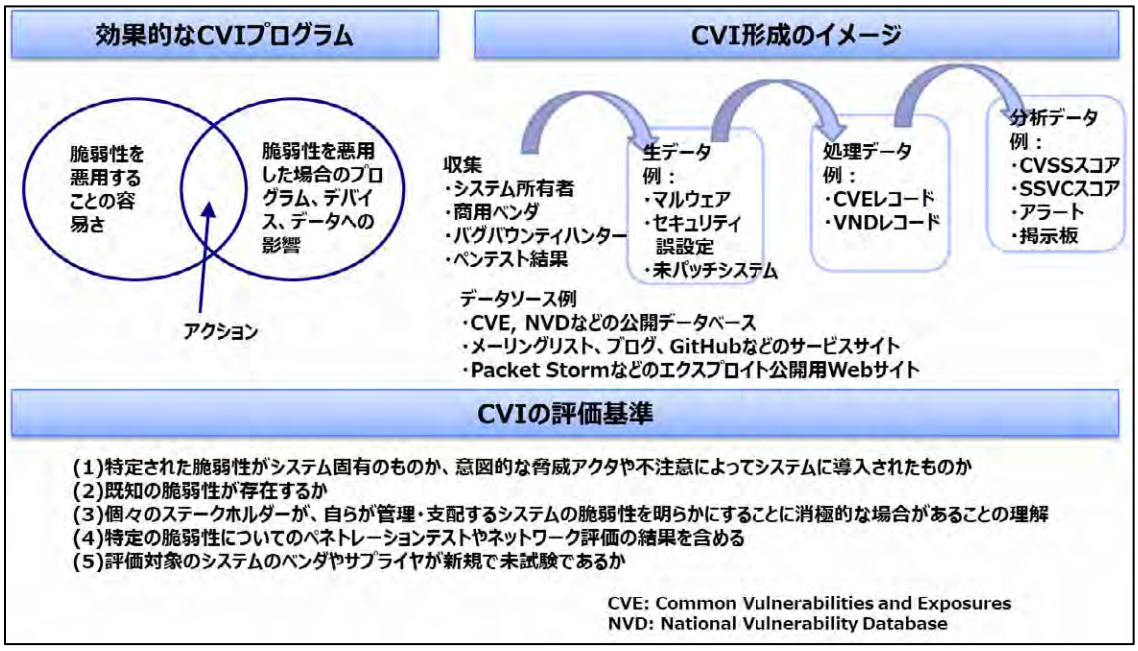


図 2-2-b サイバーバルネラビリティインテリジェンス（CVI）の概要

2. インフラストラクチャ（量子関係を含む）

国家サイバーインテリジェンスシステムは、クラウドサービスとして特に政府クラウドで実現する必要がある。政府クラウドとして実現するためには、一般に広く知られているクラウドサービスのサイバーセキュリティ基準を守るだけでは不足し、国家安全保障に関わる情報を扱えるだけの、高いセキュリティレベルに到達する必要がある。図 2-2-c に示すように、米国ではこのような高いセキュリティレベルは、FedRAMP と呼ばれるクラウドセキュリティ基準のもっとも高いレベル High に位置するものであり、日本の政府クラウドもまた、前記 FedRAMP の High レベルの環境整備が必要である。

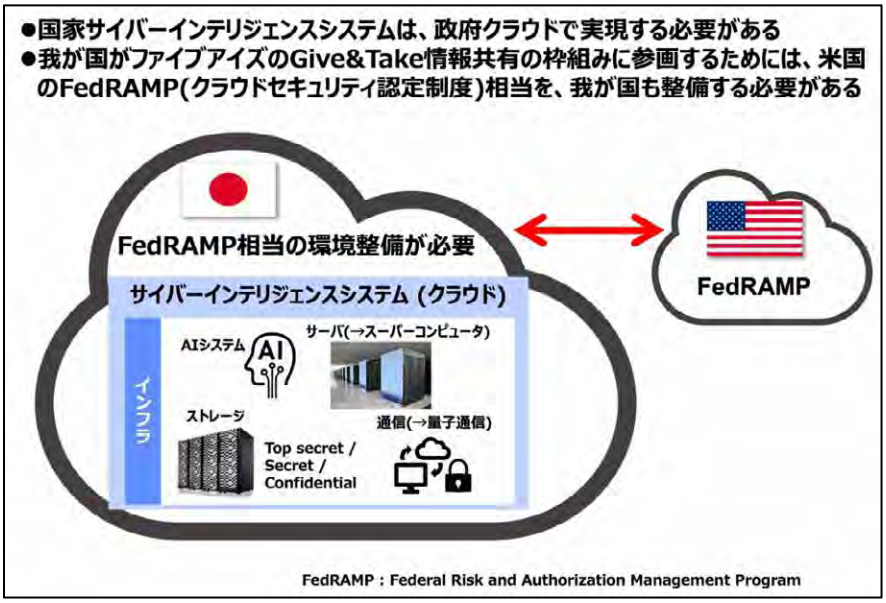


図 2-2-c クラウドサービスの活用イメージ

AI システムは、サイバーインテリジェンスを OSINT 情報からつくるために利用する。AI の活用イメージを図 2-2-d に示す。まず AI システムでは、構造化されたあるいは非構造化な、多種多様で大量に集められた OSINT データを、AI システムが理解できる情報（インフォメーション）に加工する。つぎに集まった情報（インフォメーション）を AI システムが処理し、国家安全保障に資する情報（インテリジェンス）を創出し提示する。

こうしたデータからインフォメーションさらにはインテリジェンスを作り出す工程においては、AI システムに限らず、超高速な処理を実現するためのスパコンや、大量のデータを保存するためのストレージや、クラウドサービスにアクセスするまでの通信路を確実に盗聴されないようにするための量子通信を組み合わせることで実現するものである。

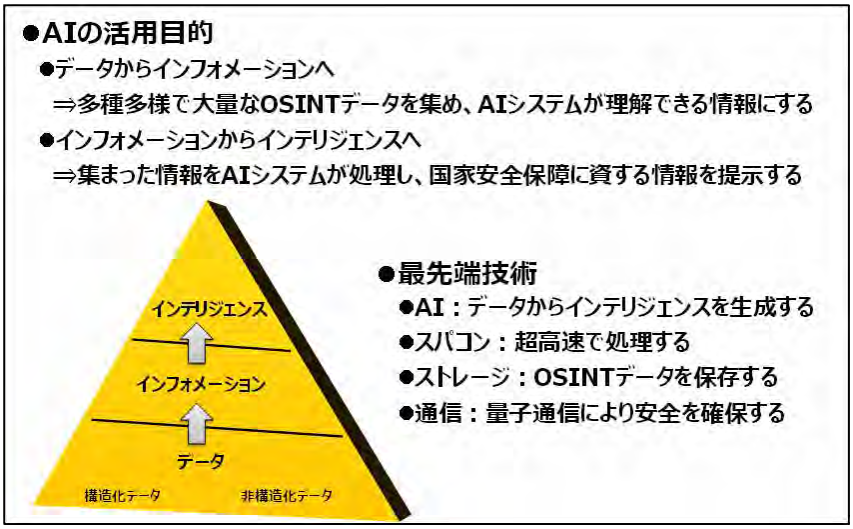


図 2-2-d AI の活用イメージ

ストレージは大容量であることは当然であるが、それだけに限らず、地政学的なバックアップを視野に、パブリッククラウドとセルフソブリンクラウドとの連携を行う（図 2-2-e）。国内におけるセルフソブリンクラウドどうしは大容量回線で接続する。一方、国内のクラウドが物理的に破壊されることが懸念される場合には、パブリッククラウドへのオフライン転送も視野にいれる。オフライン転送の事例としては Amazon Snowball が有名であり、ウクライナ侵攻の際にもウクライナ国内のデータをパブリッククラウドに転送するのに活躍した。

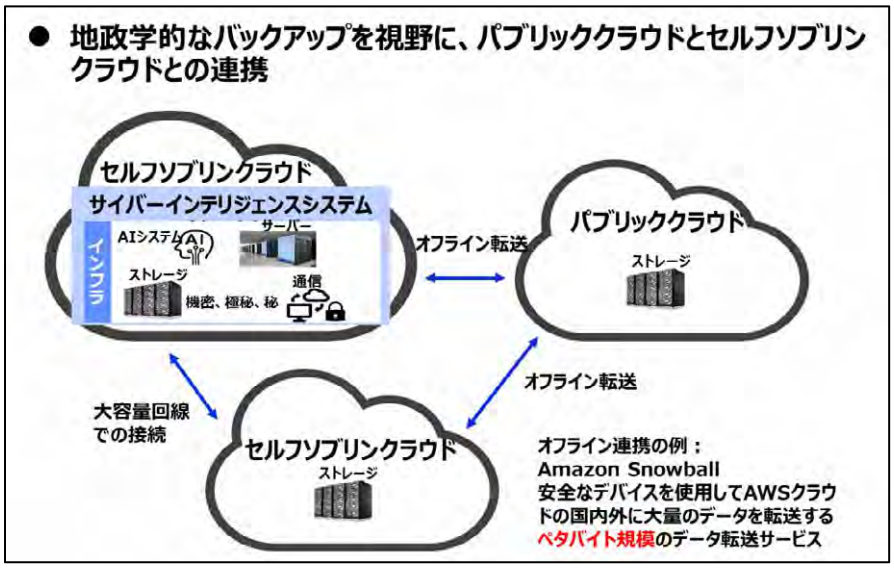


図 2-2-e ストレージとバックアップの活用イメージ

量子通信では、従来からの数学的な安全性に加えて、物理的な安全性を備えた鍵配送や共通鍵暗号の利用が考えられる（図 2-2-f）。

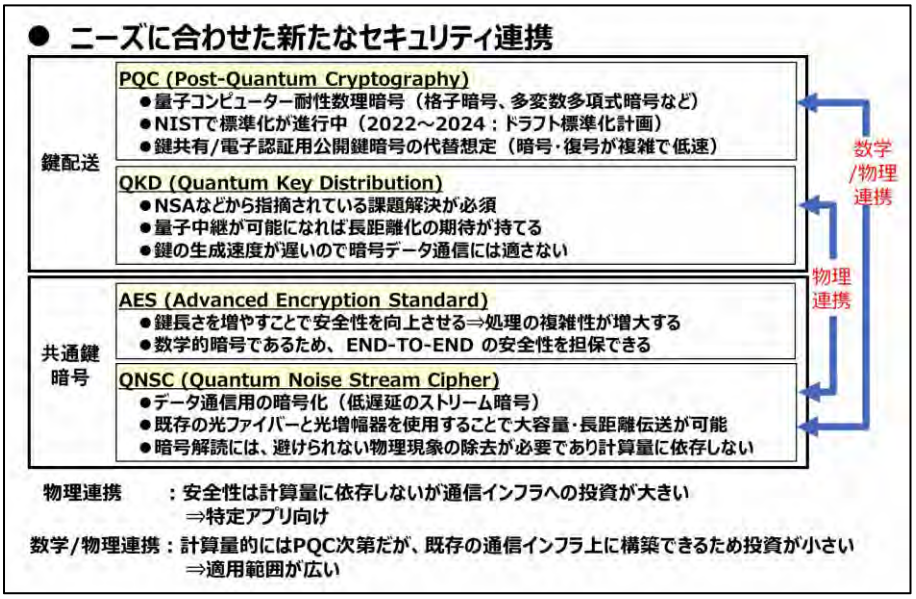


図 2-2-f 量子通信の構成要素

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。

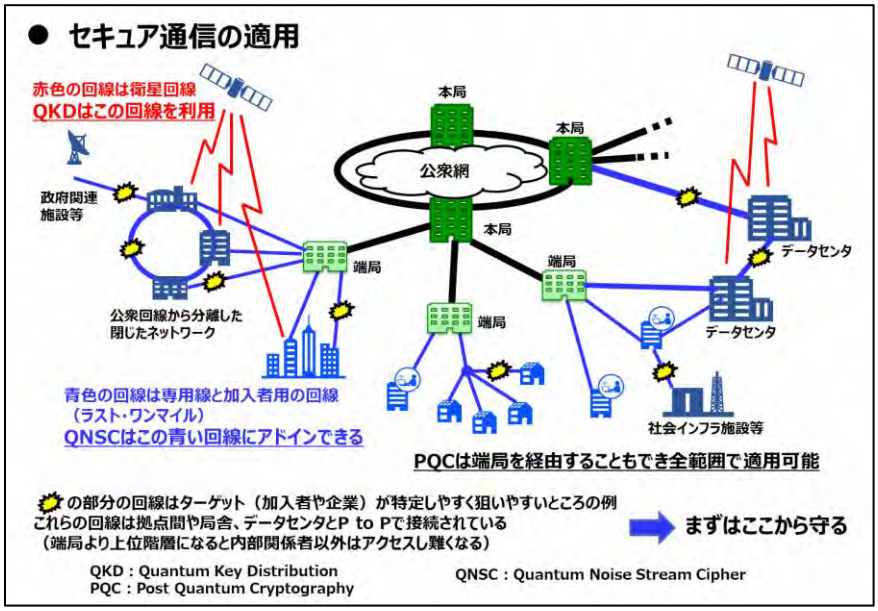


図 2-2-g 量子通信の適用イメージ

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。

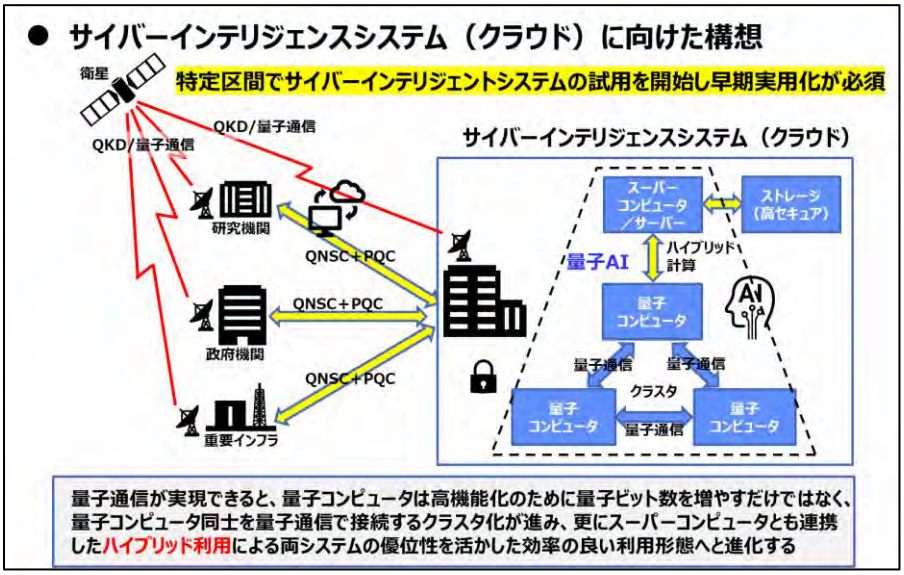


図 2-2-h 量子通信のクラウド適用イメージ

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。

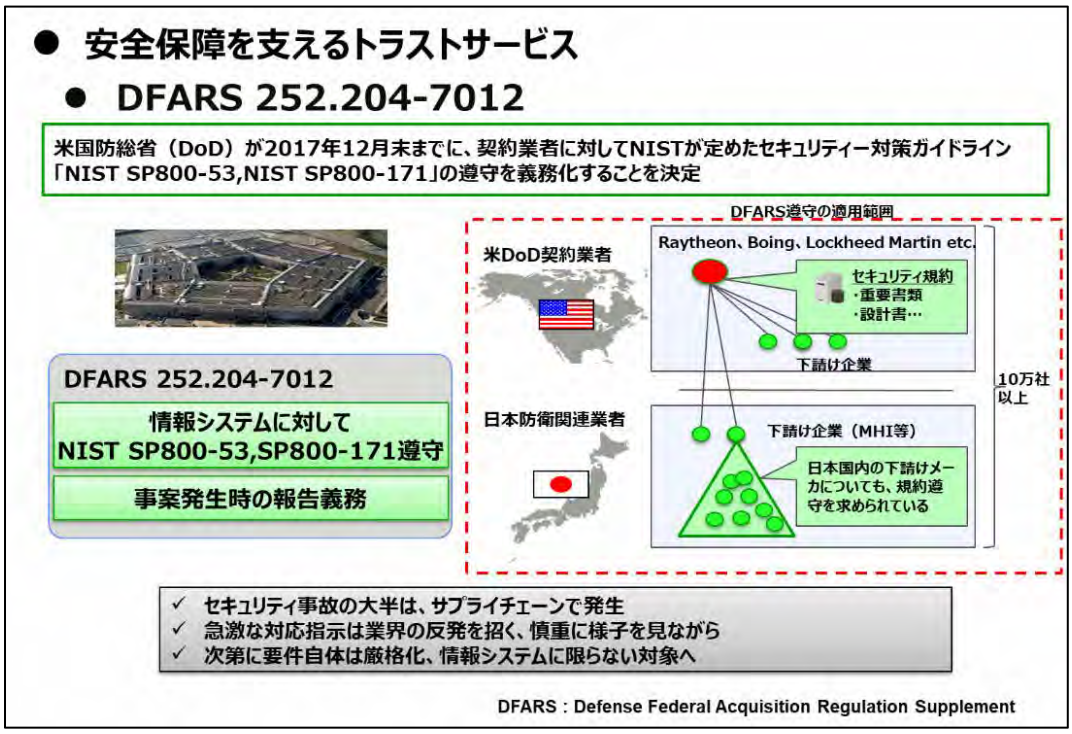


図 2-3-a 安全保障を支えるトラストサービス

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。

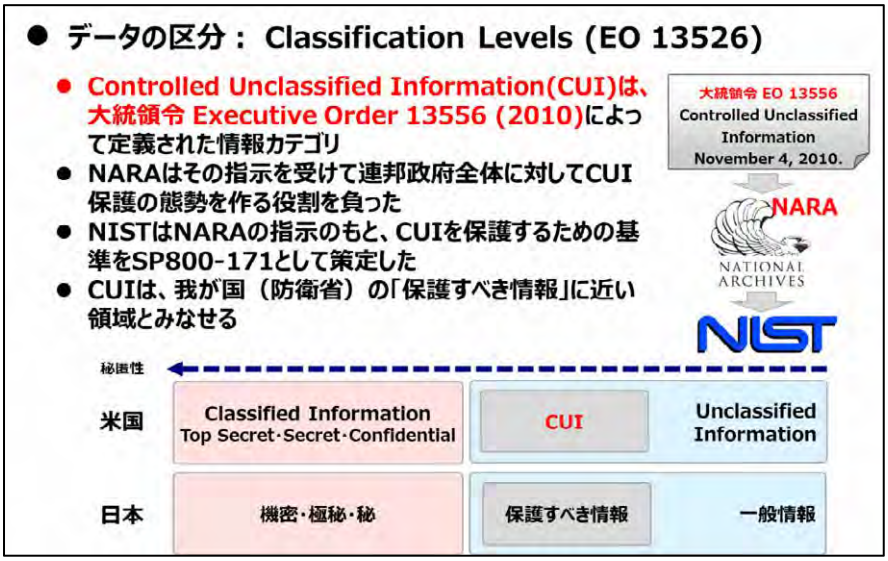


図 2-3-b データの区分

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。

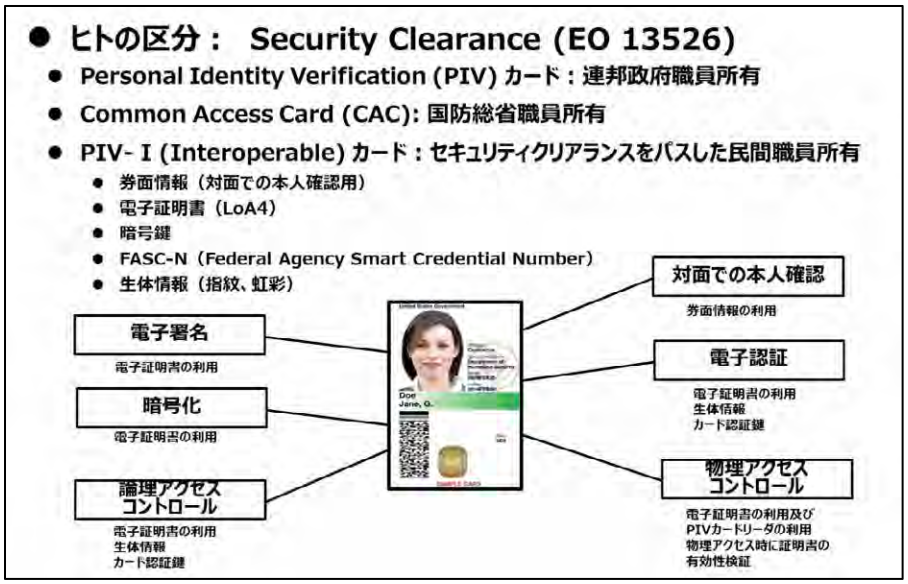


図 2-3-c ヒトの区分

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。

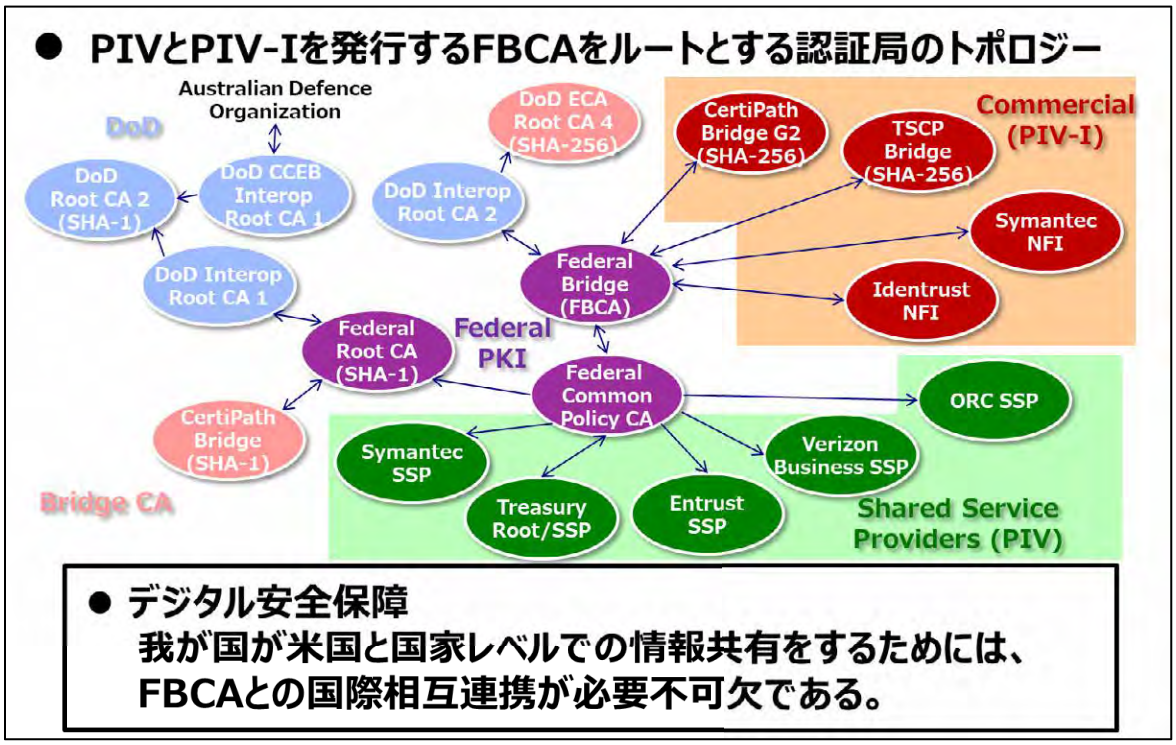


図 2-3-d トラストサービスの認証局のトポロジ

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）

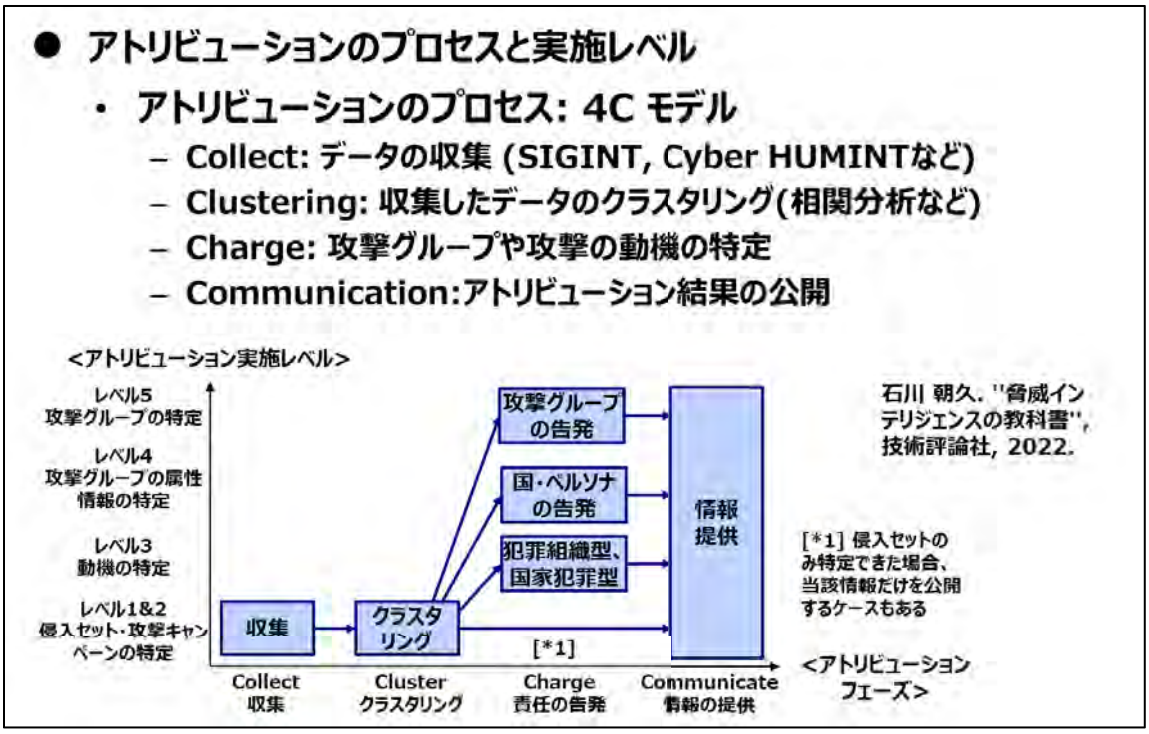


図 2-5-a アトリビューションのプロセス：4C モデル

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/

る受動的な防衛活動とは区別される。例えば、脆弱性へのパッチ適用やファイアウォールの強化は、受動的な防御であり、能動的な防御とはみなされない。能動的な防衛活動は、脅威と脆弱性を発見、検知、分析、緩和するための同期化された能力によってサポートされる。ACD の一部として実施される応答活動は、信頼できるソースから取り込まれた情報の分析に 反応して、部分的に自動化されることがある。ACD の技術には、防御側のネットワークに対する不正な活動の継続を中断させることや、攻撃者の行動を監視して将来の侵入防止やサイバー防御の技術開発に役立てることが含まれる場合がある。また、ACD は、敵対的な活動が疑われる場合に、敵対者のネットワークを混乱させるように設計されているが、「ハッキングバック」には至らない活動を意味し、より積極的な積極的防御を伴う「前方防御」のための活動を含む場合もある。

Gray Zone Report では、ACD を実際に定義しているわけではなく、以下のように特徴づけている。アクティブディフェンスとは、従来のパッシブ・ディフェンスとオフェンスの間に位置するプロアクティブなサイバーセキュリティ対策のスペクトルを捉えた用語である。これらの活動は 2 つの一般的なカテゴリーに分類され、1 つ目は防御者と攻撃者の間の技術的な相互作用をカバーするものだ。第二のカテゴリーである能動的防御には、防御者がインターネット上の脅威行為者や指標に関する情報を収集することを可能にするオペレーションや、悪意のある行為者の行動を修正することができるその他の政策手段（制裁、起訴、貿易救済など）が含まれる。アクティブディフェンスという用語は、「ハッキングバック」と同義ではなく、両者を同義に用いるべきではない。

(1) ACD の共通定義特性

最も広い意味では、ACD は、ネットワーク防御のすべての層（ティア）で侵害の指標をリアルタイムで共有し、保護、検知、対応、状況認識のための活動をほぼリアルタイムで行うことにより、サイバー イベント検知と緩和の統合、同期、自動化を可能にするアーキテクチャ上のアプローチであると言える。

Gray Zone Report と同様に、ACD は、使用される活動の特性によって最も一般的に「定義」される。一般的な ACD の特性の例としては、以下のようなものがある。

- 各ネットワーク層に独自の検知機能を提供する。
- これらの機能を「ネットワーク速度」で動作させ、リアルタイムの反応を可能にする。
- センサー、ソフトウェア、インテリジェンスを使用して、悪意のある活動が組織のネットワークとシステムに影響を与える前に検知し、阻止する。
- センサーによる分析、クラウドを活用した高度な分析、複数の脅威情報ソースとの融合により、脅威と可能な対応を特定する。
- ビッグデータ解析により、隠れたパターン、未知の相関関係、その他の有用な情報を発見し、攻撃の性質と可能な対応策を判断する。
- ローカルおよびクラウドの分析に基づき、対策を展開する。
- 進行中の脅威に直接対応し、自ネットワークの防御を意図した活動を行う。
- 政府の許可や介入なしに実行できる比例した対応を発行する。
- 人との直接のやりとりを必要とせず対応する
- 防御側のネットワーク、攻撃側のネットワーク、またはその両方に現れる効果が含まれる。
- 指標と対策の共有と配備に依存する。

要約すると、ACD とは、ネットワークとその中に含まれるデータに対する脅威から保護するために、積極的に行動することを意味する。ACD の能力は、基本的または基礎的なサイバーセキュリティの「衛生」（ファイアウォールの導入、スキャンの実施、パッチの適用など）を超えるものだ。これらの活動は、効果的なサイバー防御の必要な部分である一方、一度設定されると受動的に実行される傾向があり、能動的なサイバー防御の閾値を満たしていない場合も多い。ACD の一連の技術に該当するためには、システムはサイバー敵対者を阻止するために適切な対抗策を展開する能力をリアルタイムまたはほぼリアルタイムで示すことができなければならない。

2. ACD の活動範囲

ACD の定義が統一されていないのと同様に、ACD を構成する具体的な活動や、それらが相対的な影響やリスクのどの範囲に位置するかについても見解が分かれている。また、特定の活動が受動的な防御の範疇を超え、攻撃的なサイバー技術へと一線を画す時期についても、議論はさまざまである。ACD は一般的に、イベントの検出と対応という防御的な領域にとどまり、反撃のような領域には踏み込まない。図 3-1 に見られるように、Gray Zone Report は、ACD 活動のスペクトルを視覚化するための比較的簡単なアプローチを提供している。

図 3-1. アクティブディフェンスグレーゾーン.[2]

[2] "INTO THE GRAY ZONE: The Private Sector and Active Defense against Cyber Threats", The George Washington University's Center for Cyber and Homeland Security, 2016

これらのグレーゾーンの活動については、以下のように説明されている（影響度・リスクの低いものから高いものへと順に記載されている）。

- 情報共有：サイバー脅威の指標、緩和ツール、回復戦略を防衛者間で共有し、広範囲の状況認識と防衛能力を向上させること。
- ターピット、サンドボックス、ハニーポット：ハッカーをネットワークの境界で停止させ、孤立したオペレーティング・システムで信頼できないコードの正当性をテストし、ハッカーの行動に関する情報を収集するために監視できるように、ハッカーを囮のセグメント化されたサーバーに引き寄せる技術ツール。
- 妨害と欺瞞：敵対者が正規の情報に確実にアクセスできないように、偽の情報を混ぜて疑心暗鬼にさせ、悪意のある行為者の間に混乱を生じさせる。
- ハンティング：受動的防御を回避して防御側のネットワークに侵入してきた敵対者を検知し、外科的に退去させるための迅速な手順と技術的措置。
- ビーコン（Notification）：ファイル内に隠されたソフトウェアやリンクで、不正ユーザーがホームネットワークからファイルを削除しようとすると、防御側にアラートを送信する。
- ビーコン（Information）：ファイル内に隠されたソフトウェアやリンクで、不正にシステムから削除された場合、防御側との接続を確立し、通過した海外のコンピュータシステムの構造や位置に関する詳細な情報を送信することができる。
- ディープウェブ／ダークネットにおける情報収集：ハッカーの動機、活動、能力に関する情報を得るために、悪意のあるサイバーアクターが通常集まるインターネット上の領域で、秘密の観察、なりすまし、資産の虚偽表示などの人的情報技術を使用する。
- ボットネットのテイクダウン：マルウェアに感染した多数のコンピュータを特定し、感染したコンピュータのネットワークのコマンド・コントロール・インフラから切り離す技術的な行動。
- 制裁、起訴および貿易救済の調整：既知の悪意のあるサイバー行為者に対して、その資産の凍結、法的告発、および行為者やその国家スポンサーを標的とした懲罰的貿易政策の実施によりコストを課すための民間部門と政府間の協調行動。
- ホワイトハット・ランサムウェア：悪意のある行為者のシステムに転送された盗難情報を含む第三者のコンピュータシステム上のファイルを暗号化するために、合法的に許可されたマルウェアを使用すること。官民パートナーは、被害を受けた第三者に対して、自分たちが危険にさらされ、盗まれた財産を所有していることを知らせ、ファイルへのアクセスを回復するためにそれを返却するよう要求する。
- 資産回収のための救出作戦：ハッキングツールを使って、情報を盗んだ敵のコンピュータネットワークに侵入し、情報の漏えいの程度を特定し、最終的に情報を回収しようとすること。まれに成功することがある。

ACD の活動は、図 3-1 の左から右へ進むにつれて、より攻撃的な能力に近づいていく。特に右端では、攻撃的手法とほとんど区別がつかないものもある。例えば、ハッキングバックは攻撃型に該当するが、グレーゾーンに表示される資産回収のための救出作戦は、目的を達成するために敵のネットワークをハッキ

ングする必要がある。グレーゾーンとオフェンシブゾーンの区別はごくわずかで、この場合、防御側が盗んだ情報を取り戻すという明確な目的のためにハッキングバックするのに対して、攻撃側のネットワークに損害を与えるためにハッキングバックするというように、しばしば意図に左右されることがある。

ACD の手法がよりアグレッシブになればなるほど、組織にとってのメリットは大きくなる可能性がある。しかし、ACD がより積極的になればなるほど、法的リスク、ポリシーリスク、エスカレーションリスクも増大する可能性もある。組織は、これらの手法を戦略的に導入しながら、直面するリスクを最小限に抑える必要がある。

(1) 攻撃ステージに合わせた ACD 活動

以下の図 3-2 に示すように、ACD 活動は、望ましい影響を与える可能性が最も高い、攻撃の主要な 3 つの段階（準備、侵入、違反）に合わせることができる。攻撃の適切な段階でこれらの活動を行うためのコンテキストとアプローチは、ACD 活動の有用性に大きな影響を与える。

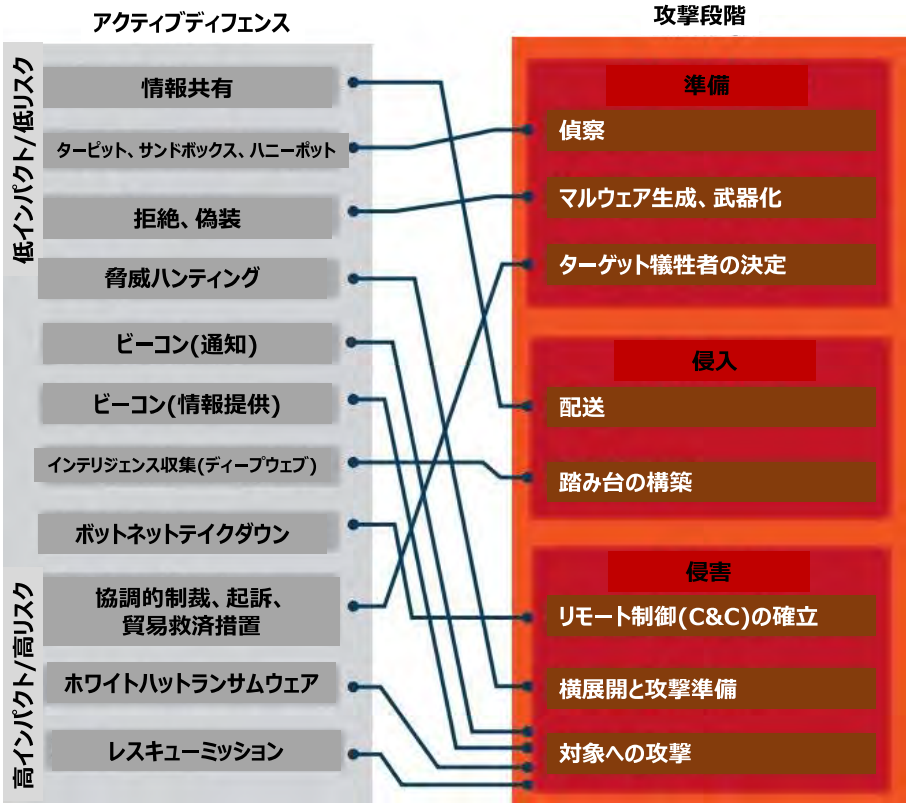


図 3-2：攻撃に影響を与えるアクティブ・サイバー・ディフェンスの活動.[3]

[3] "INTO THE GRAY ZONE: The Private Sector and Active Defense against Cyber Threats", The George Washington University’s Center for Cyber and Homeland Security, 2016

ACD 活動を攻撃段階の観点から考えることは有益だが、組織のインシデント対応アプローチの観点から考えることも有益であり、このアプローチにも 3 つの段階がある。

- 検知とフォレンジック: この活動の目的は、攻撃の種類を理解し、被害を評価し、攻撃の背後にいる人物を特定することである。これには、組織内のネットワークにおける攻撃者の活動（例：ログの確認、ハニーポット）および組織外の活動を検知・追跡するための組織内の情報収集活動が含まれる場合がある。
  注意: 外部活動の中には、「グレーゾーン」領域や、違法または国際的なパートナーと対立する領域に入り込むものもある。)
- 欺瞞: これらの活動の目的は、攻撃者の注意とリソースをそらし、その戦術、技術、手順（TTP）を観察することである（例：敵対者を引き付け、行動パターンを調べるためのハニーポット、偽または誤解を招く情報の提供など）。
- 注意: 防御者が欺瞞技術を使用していることを敵対者が認識した場合、敵対者は今度は組織を欺くための行動を取る可能性がある。また、ハニーポットのデータが流出し、本物であるかのように見せかけられた場合、組織は損害を受ける可能性がある。
- 攻撃終了: この活動の目的は、攻撃者のプロセスを中断させることである（例えば、攻撃マシンに対するサービス拒否（DoS）攻撃など）。
- 注意: 検知技術やフォレンジック技術と同様に、攻撃終了技術は「グレーゾーン」領域や、違法または国際的なパートナーと対立する領域に入り込む可能性がある。

特定の技術を特定の攻撃段階やインシデント対応段階で使用することで、防御側はより意味のあるリスク/リターン分析を行い、展開する技術や回避する技術に関する決定を導くことが容易になる。

3. サイバーインテリジェンス（CI）エコシステムにおける ACD

抽象的なレベルでは、運用型 ACD の活動は、政策、技術、法律が交わるところに存在する。政策の議論はリスク主導で、ACD の範囲に入る措置、それぞれの ACD 措置の利点とリスク、様々なタイプの防御者に最も適した ACD 措置、措置が適切な場合と不適切な場合の定義に役立つ状況、規範、国の価値と利益、政策決定の実施を導く技術の進化に基づく枠組みの構築について熟考する。

テクノロジーは、次のような二面性を持ち、独自の複雑性を提供している。1) 技術の進歩により、不注意に新しい脆弱性や予期せぬ能力が導入され、それが悪用される可能性があること、2) ACD 活動を実施し、組織が自衛しなければならない敵の能力の急速な進化に対応するために必要なツールが提供されること。

法律は、用語の定義、役割と責任の規定、許可される活動と許可されない活動の明確化、違反に対する罰則、ACD 活動や ACD が影響を与えるその他の重要な分野（例：市民の自由、プライバシー）に対する保護を提供することによって、ACD 政策の枠組みに一致する重要なガードレールを提供する。また、法律により、コラボレーション環境に関するサポート・インフラや、様々な利害関係者間の調整と協力が可能となる。

政策立案者が ACD と帰属にどのように対処するかを検討する際には、それらがより大きな CI エコシステムの中にどのように位置づけられるかを考慮することが有用である。ACD を実施する能力は、共通基盤エコシステムの 3 つの主要な構成要素（コミュニティ、データ、インフラストラクチャ）それぞれの側面に

依存する。本事業の昨年度報告書においては、CI エコシステムを、CI 関連活動を効果的に実施・管理するための資源と能力の基盤となるエコシステムとし、構成要素間の緊密な相互関係にも言及している。

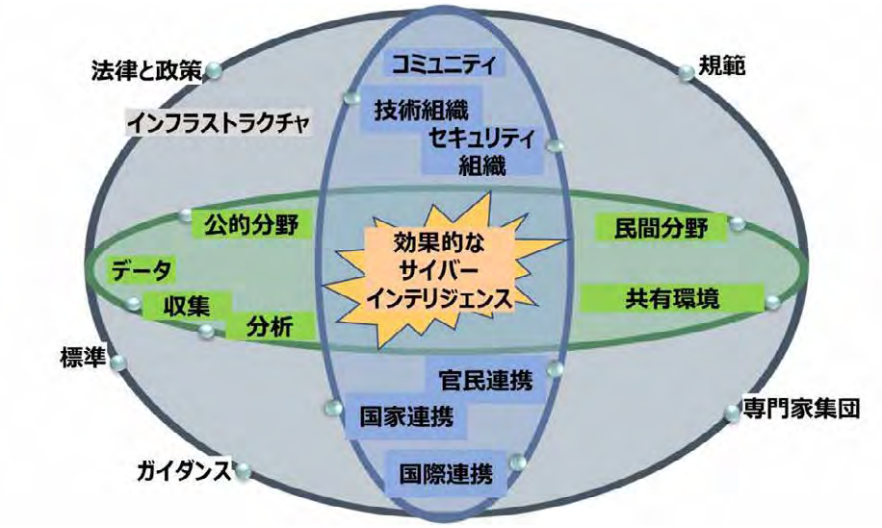


図 3-3. CI エコシステム.

より戦術的なレベルでは、ACD とアトリビューション技術を実施する能力は、複数のサイバーセキュリティの能力と機能に依存する。表 3-1 は、さまざまな ACD 活動と CI エコシステムの構成要素および下位要素における実現手段の例を示している。3 つの構成要素はすべて、ACD とアトリビューションの実践を成功させるために連携している。

表 3-1. 国内 CI エコシステムにおける ACD 活動とその実現方法の例.

アトリビューションにおけるコンポーネントの役割	サブコンポーネント	ACDの活動	実現可能な施策

インフラ ACDを含む情報セキュリティ活動を行うために必要な権限を与え、一貫したアプローチを可能にする情報セキュリティの非技術的側面の枠組み	法律と政策	ACD活動やアトリビューションを行うためのガードレールを定義	以下のような政策的枠組み • 官民間のコラボレーションを支援 • 情報共有を奨励し、障壁を取り除き、規制の影響に対する恐怖を抑制することで、情報共有を促進 • 政府との調整を必要とする活動の種類の特定を含む、許容される ACD の役割、責任、およびそれぞれの許容される ACD 活動の定義 • 常に進化し続ける技術や敵に対応する柔軟性の提供 • ACD活動がサイバー戦争に踏み込む可能性を含め、他国と取引する際の外交政策上の影響の認識 • 適切な場合には、協調的な起訴、制裁、貿易救済、およびその他の外交手段を用いることの許可 • 市民の自由とプライバシーの保護 • リスクドリブンアプローチ
	規格	アトリビューションにつながる可能性のあるインサイトを効果的かつ効率的に共有することを促進し、必要に応じて自動化機能を実装	
	ガイダンス	組織や実務者が組織レベルのACD能力を確立し、アトリビューションを実行する方法を理解する際に、法律、ポリシー、標準の実施を支援	
	コード	ACD活動に参加する組織や個人に対する期待値を設定し、信頼を促進	
	プロフェッショナリズム	ACD活動やアトリビューションを実施するためのスキル開発で人材を支援 ACDとアトリビューションの運用能力をサポートするために必要な人材とスキルを持つ人材を特定し、育成することで組織を支援	

データ 日常業務からCIが生成するソース	公共部門	ACD活動を実施・管理するための組織の権限を規定 アトリビューション、ACD、その他の対応活動を支援するために、民間部門と共有すべき情報技術を特定し、共有するための仕組みを提供	• 情報の生成と共有のためのプラットフォーム • 情報の表示と伝達（例：トラフィックライトプロトコル、クリアランスレベル）、および情報を受け取ることができるステークホルダーの確認のための標準化された規則 • 自動的な共有と利用を促進するための規格
	民間部門	インシデントに関する情報を政府及び産業界のパートナーと共有	
	コレクター	組織的な対応能力を示す CIを提供	
	分析装置	ACDを実施すべきか否かを判断するための情報など、インシデント対応に資するCIを分析・共有	
	共有環境	ACD活動の分析結果や成果を含むCI情報を共有し、利用するために、共有パートナーに信頼され保護された空間の提供	
コミュニティ アトリビューションやその他のACD活動に情報を提供するインテリジェンスのコラボレーションと共有に役割を果たすクラウドソ	技術系組織	ネットワークやシステムで何が起こっているかを理解するために、製品に監視機能を構築。 自社製品に関連するインシデント観測に関する洞察を提供 敵の行動や特定の技術との相互作用の、時系列的なパターンの提示	• ACDやアトリビューションの実施、情報共有のための法的機関 • 組織やパートナーシップの責任と義務の明確な認識 • エコシステムへの情報や分析を提供しやすいテクノロジー・セキュリティベンダー

ーシング組織	セキュリティ関連組織	サイバーインテリジェンス活動の実施（しばしばアトリビューションを目標とする場合もある）	• 協力と情報共有を可能にするパートナー国との正式な協定 • 敵対者とその動機の理解 • 重要資産、産業、サプライチェーン、情報共有環境、データ処理エコシステムの理解 • 情報共有のインセンティブ
	官民パートナーシップ	情報共有、インシデント対応、アトリビューションを促進するための洞察を提供することができる協力的なハブ	
	国内パートナーシップ	政府主導でコラボレーションのためのガイダンスとサポート・インフラを提供	
	国際的なパートナーシップ	パートナー国間で、インシデント対応とアトリビューションに関して協力するための正式な共有協定を締結	

4. 組織のサイバーセキュリティ・プログラムにおける ACD と関連活動のライフサイクル

政府機関であれ民間企業であれ、個々の組織が ACD 活動の大部分を実施している。ACD に関する効果的な国家政策を設計するためには、組織が ACD 活動に対する個々のアプローチを通じてどのように推論する必要があるかを理解することが有益である。米国標準技術局（NIST）の「重要インフラのサイバーセキュリティ向上のためのフレームワーク」（「サイバーセキュリティ・フレームワーク」）は、組織のサイバーセキュリティ・プログラムが達成しようとする成果の種類を特徴づけるための背景を提供している。図 3-4 は、これらの 5 つの機能、それらの相互に関連する継続的な性質、および組織が検討するのに役立つ質問の種類を描いる。

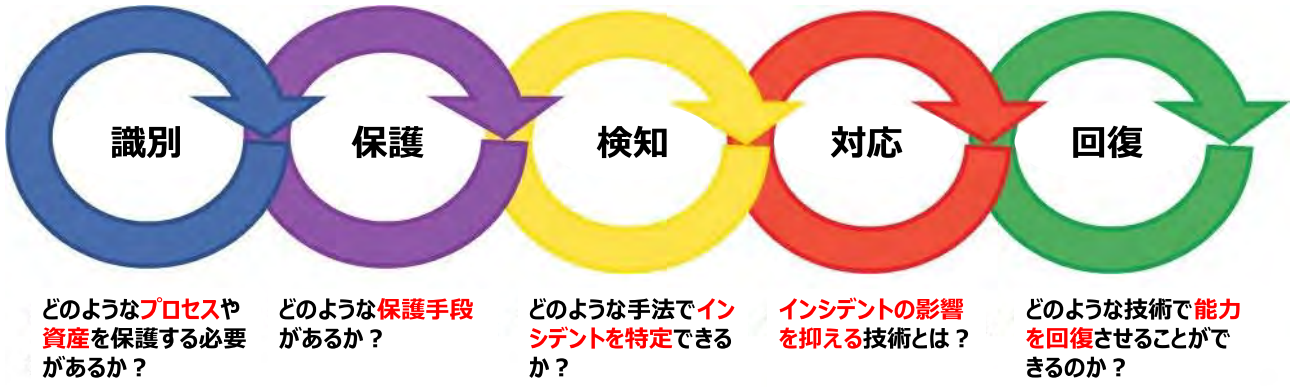


図 3-4：NIST サイバーセキュリティ・フレームワークのコア・ファンクション

組織がこれら 5 つの機能分野のそれぞれで実施する活動は、リスクベースの ACD 機能を実装するための戦略的および戦術的な基盤となる。表 3-2 は、ACD 機能の実装をサポートするサイバーセキュリティ活動の例を示しており、それらが組織の ACD アプローチにどのように反映されるかを説明している。

表 3-2.サイバーセキュリティの取り組みが ACD のアプローチに与える影響.

サイバーセキュリティ機能	ACDに関連する活動	インフォメーション
識別	資産と情報の流れを棚卸しし、組織の目的とリスク戦略に対する相対的な重要性を判断し、リスクを評価	• ACDの能力をどこに集中させるか • 反応のレベル・種類
	重要インフラ，産業，サプライチェーン，情報共有環境，データ処理エコシステムにおける組織の役割，及び法的義務やリスク許容度を考慮したリスク管理戦略の維持	• 脅威と脆弱性の評価 • ACD戦略/アプローチ • 許容されるACDの行動
	組織の優先事項、法的義務、及びリスク許容度をサポートするためのガバナンス構造の維持	• ACDの役割と責任
	顧客，第三者パートナー，サービス・プロバイダーを含む，社内外のステークホルダーの役割と関係を理解	• サイバーイベントやインシデント時の監視や調査の対象となりうる脆弱性のポイント • 確立しなければならないコミュニケーションとコラボレーションのためのチャンネル
防御	リスク管理戦略をサポートするプロセス、手順、および技術的なセーフガードの実装	• イベントやインシデントの種類と、実施されている保護メカニズムに基づくモニタリングのポイント
	期待通りの性能を確保するための資産の維持管理	• ACD機能更新のためのトリガー
検知	環境において期待される活動や行動のベースラインを確立	• 期待された状態や行動からの逸脱の理解
	必要な保護措置が有効であること、保護措置、システム、技術が意図したとおりに機能していること、およびサイバーセキュリティ上の潜在的事象を特定するためのスキ	• ACD機能が運用されるプロセスおよびセンサー

	ャンと監視機能の導入	
応答	必要に応じた対応策の実行・更新	• ACD能力の運用 • 新しい情報をもとにしたACD能力の改善 • インシデント対応の教訓
	社内外のステークホルダーとのコミュニケーション	• ACDの成果に関する報告 • サイバー脅威情報（CTI）共有の実践と情報提供 • 連携した分析・対応
復旧	必要に応じた復旧計画の実行と更新	• 教訓に基づく ACD 戦略・手法の改善
	社内外のステークホルダーとのコミュニケーション	• 復旧活動 • 必要に応じた広報活動

5. 依存関係

ACD の技術を使用するかどうか、またどのような状況で使用するかは、単独では決定できないことを理解することが重要である。情報セキュリティ・エコシステムにおける ACD とアトリビューションの実現方法、および ACD プログラムを実施するために組織が行う運用上のサイバーセキュリティ活動の検証から、日本の文脈における ACD の意味を決定する際に日本政府が考慮すべき複数の重要なサイバーセキュリティ上の依存関係があることが明らかになった。以下の表 3-3 は、これらの重要な依存関係と、ACD とアトリビューションの実践を成功させ、かつ認可する上でのそれらの役割の概要を示している。

表 3-3.ACD の重要なサイバーセキュリティ依存事項の概要.

サイバーセキュリティへの	重要な役割

依存度	
法的根拠・方針	• 明確な境界と期待を設定し、期待される行動と境界を組織が理解できるようにする。 • CIエコシステムの参加者にインセンティブを与え、敵対者を思いとどまらせる。 • 国家的価値の保護と意図の明確化
モニタリング	• ネットワークやシステムで何が起こっているかを理解するためのツールや生の情報を提供する。 • 急速に変化する環境に対応するため、学んだことを継続的に取り入れる分析支援ツールやテクニックを使用する。
コミュニケーション	• 適切な行動をとるために、業務に不可欠な情報資源を適切な時間内に利用できるようにする。 • 他環境への侵入を防ぐ指標を共有する方法を導入
アトリビューション	• 敵対者または脅威の主体が誰であるかを、程度の差こそあれ、確立している。 • 法執行機関やサイバーセキュリティを担当する他の政府機関と共有する、潜在的な犯罪行為を判断するための有用な証拠を提供する。
同意	• 組織と関係する他の団体と連携し、その団体のネットワーク上でACD活動を行うことを許可することを支援する（相互防衛協定）。

6. ACD 手法の使用における法的・政策的制約事項

ACD の領域における第一の依存事項は、法的な権威とポリシーである。上の図 1 で受動的防御の右側に見える活動がグレーゾーンと呼ばれるのは、これらの活動が許されるのか、許されるとしたらどの活動が、誰によって行われるのかが不明だからである。これらの活動の中には、私企業が行った場合、米国の法律では違法となる可能性が高いものがあることに異論はないだろう。

強固な ACD プログラムを追求するための技術的能力は、民間部門の洗練されたプレーヤーがますます利用しやすくなっているが、既存の法律と政策の枠組みは、民間部門がこれらの技術の多くを使用することを禁止している。以下は米国の法体系を前提とした議論となるが、我が国において ACD プログラムの実装を検討する際に必要な論点を抽出するために参照する。

主な法的根拠はコンピュータ不正行為防止法（合衆国法律集第 18 編第 1030 条他）で、無許可でコンピュータにアクセスする行為や、許可されたアクセスを超えて何らかの不特定の損害を与える行為を禁止している。したがって、他人のコンピュータ上のデータを復元、消去、または変更するような行為は、たと

えそのデータが自分のネットワークから盗まれたものであっても、確実に禁止されている。実際、自分のネットワーク以外のネットワークでの活動を含む活動は疑わしい。特に、他の事業者が所有・運営するクラウド環境にデータを保存している事業者にとっては、難しい問題である。データ所有者は、クラウド環境からデータを盗まれたり、クラウド環境で破損したりする可能性があるが、その環境で ACD 技術の多くを使用するには、ほぼ間違いなくクラウド環境の所有者から許可を得る必要がある。

もう一つの関連法は、電子通信プライバシー法（ECPA）（合衆国法律集第 18 編第 2510 条他）の盗聴規定で、有線、口頭、電子通信の内容を傍受する（または傍受しようとする）ことを違法とするものである。シンクホーリングやビーコンのような ACD 技術の一部は、電子通信の傍受とみなされる可能性がある。

さらに、ECPA のペン・レジスタ／トラップ・アンド・トレース規定（合衆国法律集第 18 編第 3121-27 条他）は、受信データを捕捉し、その活動を特定の行為者やシステムに帰属させようとするハニーポットやシンクホールに関与している可能性がある。

これらの法律は、民間企業が行うことのできる行為と政府機関が行うことのできる行為の間に二項対立を生じさせる。確かに、ACD の活動がハッキングバックの領域に踏み込んだり、他の事業者のネットワーク上で活動を行ったりする場合、民間事業者は法的に大きな制約を受けることになる。

米国の法律では違法（または少なくとも疑わしい）とされているが、米国企業が特定された攻撃者に対して積極的な行動を取ろうとするケースは顕著だ。被害者が自社システムへの攻撃に対応するために使用した ACD 技術が、1 つ以上の米国法に違反している可能性が高いにもかかわらず、起訴されることはなかった。

非政府組織が様々な ACD 技術を使用しようとする際に陥りうる法的な罠を一つ一つ検証することなく、日本では、ACD プログラムの一部として誰がどの技術を使用できるかを決定するために、現存の法律と政策を見直す必要があることは明らかである。日本にとって特に重要なのは、攻撃的な軍事行動を禁止している憲法第 9 条である。例えば、日本が防衛省内にサイバー・コマンドを設立した場合、その部署はどのような ACD 技術を使用することができるのか制約を受けるのか大いに検討する必要がある。

米国では、悪意のあるサイバー活動の被害を受けた民間企業による特定の ACD 活動には法的な障壁があるものの、多くの民間企業が APT（Advanced persistent threats）の標的になっているという認識があり、しかし政府は民間企業のすべて、あるいは多くを守る立場にはないのが現状だ。そのため、特に米国の重要インフラの所有者や運営者など、より積極的に資産を保護できるようになる必要がある民間企業には同情的な意見も多い。その結果、民間企業が脅威の主体に対してより影響力のある形で関与するための、より大きな自由を与える可能性が議論されてきた。米国では最近、ACD の政策と合法的かつ適切であるべき境界を明確にする試みがなされている。さらに、ACD を行う際には以下のような問題を避けるよう、議員も勧告している。

- 他人または法人のコンピュータに保存されている、被害者のものではない情報を意図的に破壊したり、操作不能にしたりすること。
- 無謀にも身体的傷害または金銭的損失を引き起こすこと。
- 公衆の健康または安全に対する脅威を生じさせること。
- 持続的サイバー侵入の発生源の帰属を可能にするために中間のコンピュータ上で偵察を行うために必要な活動レベルを意図的に超えること。

- 中間のコンピュータへの侵入またはリモートアクセスを意図的に獲得すること。
- 個人または法人のインターネット接続に持続的な障害を意図的に引き起こし、損害を与えること。
- 司法、国防、国家安全保障を推進するために政府機関によって、または政府機関のために使用される情報技術（IT）または運用技術（OT）システムに影響を与えること。

一方、民間企業に自由度を与えすぎることへの懸念もある。ACD 活動の多くは、外国または少なくとも外国にいるエンティティが指揮する APT を対象とするため、積極的な ACD 手法によって、サイバー戦争まで含めた重大な国際的影響が引き起こされる危険性がある。民間事業者が政府の許可なく、どの活動を行うかについてリスクベースの決定を行うことを許可すれば、破滅的な事態を招く可能性がある。

これらの修正はまだ実施されていないが、被害者が潜在的なリスクを理解しながらより積極的に行動できるように、議論を続けることが重要である。日本が ACD の利用を拡大しようとする場合、法律や政策に関して他国が直面している課題を理解し、どの技術を誰がどのような状況で利用できるかを明らかにし、既存のグレーゾーンがもたらす混乱を最小限に抑える必要がある。

ACD 活動の法的境界を理解することは、組織が保護的対応として価値のある行動を取り、財政的または法的問題を引き起こしたり、国家目標を損なうような行動を回避するのに役立つ。

7. まとめ

ACD の技術は、様々な種類の政府や組織がサイバー攻撃にプロアクティブに対処するための重要なインシデントレスポンス機能を提供する。しかし、ACD は、強力なサイバー防御と能力をサポートする CI エコシステムの多くのツールのうちの 1 つに過ぎない。

さらに、ACD は、以下のような慎重な検討に値する複数のタイプのリスクをもたらす。

- インシデントを正しい脅威者に正しく帰属させることの難しさ

  ACD の手法の多くは、期待される効果を得るために、特定の脅威者に少なくともある程度帰属させることが必要だ。ACD 技術を無実の者に適用することは、特に望ましくない結果である。しかし、帰属は依然として不正確な科学であり、その多くは経験、直感、仮定に依存する。正確な帰属を行うには、何年もかかる場合もある。さらに、国家と非国家の脅威要因にどのように対処すべきかは、区別が必要である。人工知能のような技術的なツールは、このプロセスをサポートするほど成熟していない。多くの場合、分析者が脅威行為者の組織、特に個人を絶対的な信頼性をもって名指しすることは困難である。分析者が攻撃の帰属を正しく判断する唯一の方法は、攻撃を実行している敵対者を観察することだが、そのためには時に敵対者が管理するコンピュータにアクセスする必要がある。複数の方法を用いてアトリビューションを判断することで、攻撃者が正しく特定されたことの確実性を高めることができる。
- 傍観者的な組織への影響

  攻撃者はしばしば、自分たちのネットワークが攻撃に利用されていることに気づいていない別の組織を通じてターゲットに接続したり、接続したように見せかける措置をとる。防御側が特定の ACD 技術を採用した場合、傍観者である第三者機関が仮想的な十字砲火に巻き込まれる可能性がある。例えば、防御側が攻撃しているコンピュータを無効化するためにボットネット・テイクダウンを実行すると、無意識のうちに傍観者である第三者の重要なシステムを無効化し、その結果、第三者の

業務に意図せずして影響を与える可能性がある。防御側には、その行動を抑制する能力が不可欠である。

- 限られたリソースの活用
  ACD 活動は、あらゆる種類の攻撃に対する適切・必要な対応策とまでは言えない。各組織は、利用可能なリソースの制約の中で、ACD がリスクに応じた効果的な対応となるかどうかを判断するためのアプローチ/戦略を決定し、効果のない活動にリソースを浪費しないようにする必要がある。
- ACD 手法の有効性
  ACD の各活動は、特定のサイバー攻撃やステージに対して様々な影響を及ぼす。組織は、脅威への対処の有効性と活動のメリットおよびリスクのバランスを考慮し、特定の状況に対してどの ACD 手法が適切かを推論する方法を必要としている。
- ACD 活動の影響を理解する
  組織は、自分たちの ACD 活動が他の組織や国家にどのような影響を与えるかを理解する必要がある。例えば、重要なインフラや国際関係を混乱させるような活動は、意図したよりも長く続く影響を与える可能性が高く、危険である（例：環境や人体の安全問題を引き起こす運用技術の不具合を引き起こす）可能性がある。さらに極端な例では、企業スパイやサイバー戦争の火種になるなど、受け入れがたい行為につながる活動もある。

ACD を成功させ、国家や組織にもたらすリスクのいくつかを回避するためには、明確な目的と境界線を持ち、慎重に検討された法的・政策的枠組みの中で導入されなければならない。

第３節 アトリビューションを取り巻く状況

能動的なサイバー防衛活動に関する議論から明らかなように、これらの手法の多くを効果的に利用するためには、誰がネットワークを攻撃しているのかについてある程度理解し、ACD 手法を無実の傍観者ではなく、実際の悪意ある行為者に対して適用することが必要だ。このセクションでは、アトリビューションの概要と、それが ACD プログラムのサポートにどのように使用され得るかについて説明する。

1. アトリビューションの価値

アトリビューションとは、特定の悪意ある行為に関与した脅威者を正確に特定する行為だ。サイバー脅威の行為者の帰属を成功させることは、ネットワーク防御、法執行、抑止力、および外交関係の改善を含むいくつかの理由で重要である。アトリビューションがもたらす潜在的なメリットを例示すると以下となる。

- 悪意あるサイバー行為者は、その行為に対して責任を負わされる。
- その行為に責任を負わされることになり、特定され責任を問われることへの恐怖、あるいは単に風評被害を受けることで、攻撃に対する抑止力となる可能性がある。
- アトリビューションが公開されることで、悪意あるサイバー行為者は、今後の追跡を避けるためにデバイスやインフラの使用を中止し、その動きを鈍化させることができる。
- アトリビューションは、攻撃者、ターゲット、TTP について知ることで、組織のネットワーク防御を強化するのに役立つ。

- アトリビューションは、サイバー防御と運用に向けたリソースの優先順位付けを支援することができる。
- 被害組織に関連する政府は、攻撃者に関連する政府に対して、制裁措置や規制の強化などの措置を講じることができる。
- アトリビューションは、組織が攻撃の責任を誰に負わせるべきかというニーズを満たす。
- 攻撃をある国に帰属させた後、非難している政府は、その国に対する支援のために同盟国を結集させることができる。
- 攻撃を帰属させることで、政府は攻撃者を追跡する能力があることを国民に示すことができる。
- 攻撃を帰属させることで、政府は悪意のあるサイバーアクターに対して、彼らを追跡する能力があることを示すことができる。
- 政府が攻撃を特定の行為者に帰属させると、民間企業は、情報セキュリティの取り組みにおいて政府と接触し、協力する動機付けを得ることができる。
- 帰属は、民間企業がどの法執行機関に連絡すればよいか、また法的な選択肢を決定するのに役立つ。

アトリビューションプロセスでは、技術的、分析的、法的、および政治的な証拠を融合して、悪意のある活動の背後に誰がいるのか、またそれに対して何をすべきかを判断するための全体像を可能な限り明らかにする。技術的な原因究明の努力は必要だが、責任の所在の問題に答えるには不十分である。悪意のある行為者による誤誘導や、攻撃開始時にキーボードを操作していたのが誰であったかを特定できないなどの理由で、技術的証拠の限界を超えるには、法執行機関と情報ソースに基づく従来の分析技術がしばしば必要とされる。法的証拠は、活動が法律に違反しているかどうかを調べ、プライバシーの権利など個人の権利を侵害することなく使用できる技術を決定したり、国際法の違反があったかどうかを評価したりすることができるものだ。最後に、政治的証拠は、特定の活動が特定の国家または民間団体と結びついているという判断を可能にする最後の断片を提供することができる。

アトリビューション能力は、プラスとマイナスの両方の意味を持つ可能性がある。オンライン活動の帰属は、システムにアクセスする人がその人であると主張することを確認するための ID 管理機能にとって望ましい場合がある。たとえば、オンラインで自分の銀行口座にアクセスする個人は、承認されたユーザーだけが口座にアクセスできるようにするシステムを望んでいる。したがって、活動を認可されたユーザーに帰属させることができる ID 管理ツールは、積極的な使用の一例である。一方、抑圧的な政府は、政府に反対するコンテンツへのアクセスを求めたり作成したりする個人を特定し、そのような活動を停止したりその個人を罰したりするために、属性付与技術を使用することができる。

本章では、他者のネットワークや情報システムに損害を与えようとする悪意ある行為者に対する抑止効果を高めるとともに、悪意ある行為者からの攻撃に対するシステムの防御と応答を改善することを目的としたアトリビューション技術に焦点を当てる。ここでいうアトリビューションとは、ネットワーク上の攻撃者、または攻撃者の仲介者の身元および/または位置、あるいはネットワークに含まれるデバイスを特定することと定義される。

正確なアトリビューションは、防御を強化したり攻撃者に苦痛を与えたりする上で高い価値があるものの、高度に洗練されたアトリビューションは、一般に政府機関や高い能力を持つサイバーセキュリティ企業のみが可能な、時間とコストのかかる活動であることを認識する必要がある。さらに、政府機関以外の団体

が責任者に対して意味のある行動を取る能力が限られているため、帰属の価値が損なわれる可能性がある。したがって、包括的な帰属の取り組みを行うかどうかに関するあらゆる決定は、特定の活動を特定の行為者に帰属させることができることから得られる可能性のあるプラスの成果のレベルが、希少なリソースの使用に見合うものかどうかを判断する必要がある。

サイバーセキュリティサービスプロバイダとして有名な Mandiant が指摘するように、分類されていない活動を最初に特定してから、それを特定の APT または金融脅威（FIN）グループに割り当てるまでには、「通常、何年もの丹念な収集、調査、分析、数千の証拠、数百時間の作業が必要」であり、短期のインシデント対応活動に価値があるとは思えない。しかし、Mandiant は、初期の未分類情報（「UNC」と呼ばれる）であっても、攻撃者の識別特性を提供することで、サイバー・ディフェンダーにとって価値がある可能性があると主張する。以下の表 3-4 は、その潜在的な価値を示している。

表 3-4：様々なステージにおけるアトリビューションのインテリジェンスの価値.

	Uniform Naming Convention特性	インテリジェンスの価値
戦術的	マルウェア、ドメイン、IP、悪用されたCVEなどの指標	ブロックリスト、検出シグネチャ、パッチの優先順位
運用的	行動パターン（例えば、活動の頻度、よく使う道具、標的の場所や分野など）	既知のTTPの監視と緩和策を確立し、新しいインフラの登録やその他のパターンを特定し、活動を予測
戦略的	動機、目標、潜在的なスポンサー、仲間	どのような脅威が組織に影響を及ぼす可能性が最も高いか、またその理由は何かを検討し、侵害による最悪のシナリオを特定

また、アトリビューションは単一の概念ではないことを認識することが重要である。アトリビューションが意図される目的によって、必要とされるアトリビューションのレベルが異なるのである。図 3-5 は、アトリビューションの異なる「レベル」または「タイプ」を示している。最も簡単なレベルは、技術的なデータにのみ依存するため、技術的なアトリビューションだ。このレベルのアトリビューションは、攻撃の種類とその発信元であるシステムについて迅速に判断し、攻撃を停止させる必要があるため、通常、インシデント対応の最初のステップとなる。次のレベルでは、発信国を調べる。これは、攻撃がどのように行われているのか、またその動機について、ある程度の文脈を与えることができるため有用である。また、どのような TTP に注目し、対策を講じるべきかという点についても洞察が得られる場合もある。次の段階は、攻撃の背後にある国内の特定のグループに帰属させることだ。これにより、より大きな文脈が得られ、動機が明確になり、予想される悪意のある行動が絞り込まれる可能性がある。最後に、キーボードを操作し、攻撃を行った人物を特定する「個人アトリビューション」だ。この最高レベルの帰属を達成することは最も困難であり、帰属の結論に確信が持てるレベルを達成するためには、あらゆる種類のインテリジェンスが必要となる。このレベルの帰属情報は一般に、起訴または外交上の決断を下す必要がある場合にのみ必要とされる。このレベルの帰属判定は非常に時間がかかり、何年もかかる場合がある。

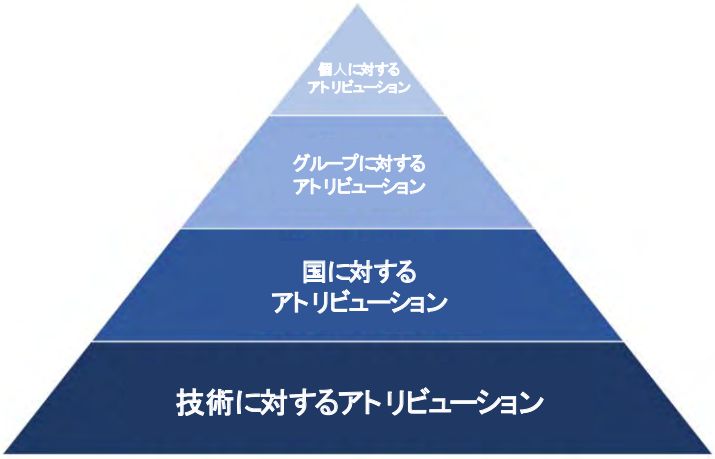


図 3-5. アトリビューションのピラミッド.

どのレベルのアトリビューションが可能であるかにかかわらず、基本的なアトリビューション技術を実行することさえできれば、何らかの価値を提供できることは明らかである。ただし、アトリビューションはそれ自体のために行われるのではなく、他のサイバー防衛やインテリジェンス活動を支援するために行われる点は重要だ。したがって、最初のステップは、防御者がどのような対応を希望するかを決め、その希望する対応をサポートするためにどのレベルのアトリビューションが必要かを判断することである。IT 企業で深刻な異常や事象が発見されると、通常、その事象を特徴づけ、原因と結果を判断するために、複雑な調査やインシデント対応のプロセスが開始される。特定のインシデントの調査および対応サイクルの異なる時点では、異なるレベルの帰属が望まれる場合がある。組織によって、このような調査の実施方法は、時間、順序、スタイル、および利害関係者によって大きく異なる。しかし、一般的には、特定の中核的な機能、プロセス、および意思決定ポイントが関与している。

2. ステークホルダー アトリビューション情報の作成者と利用者

前節では、組織がそれに応じて対応できるように、誰が攻撃しているのかを理解するのに役立つアトリビューション情報の一般的な価値について述べた。アトリビューション情報は、攻撃者の動機および防御者が攻撃に応答して適用することが望ましい ACD 技術に関する仮定に情報を与え、それぞれの攻撃者およびその行動に関する全体的な知識体系に貢献するものである。また、アトリビューションは、国家や情報通信エコシステムにおけるステークホルダーの役割に応じて、様々な形で具体的な利益を提供し、ステークホルダーを支援する。

アトリビューションの対象者を分類する方法は複数ある。このセクションでは、サイバー対応における一般的な役割の観点からアトリビューションの対象者を検討する。アトリビューションは、集合的なアトリビューションの知識ベースへの貢献者と、攻撃の犠牲者または防御者の両方をサポートする。組織によっては、攻撃の貢献者であると同時に被害者または防御者でもある場合がある。同様に、組織によっては、複数の分類に該当する可能性がある（たとえば、重要インフラの所有者および運用者は、民間部門の組織または政府の文民機関でもある）。これらの活動はすべて、組織が ACD 活動の利用をその組織固有のニーズとリソ

ースに合わせて調整するのに役立つ。表 3-5 は、アトリビューション情報の利用者のカテゴリー間の基本的な区別を示したものである。

表 3-5.アトリビューションが様々なオーディエンスを支援する方法.

オーディエンス	アトリビューションによる支援の仕方	配慮事項
政府：政策立案者	• 脅威が発生したときの対応に重点を置く • 法律や政策の枠組みの変更に関する情報提供 • 国際的なパートナーを含むCIエコシステムへの貢献 • 法執行機関の対応に情報を提供 • 政府が容認できないと考えることを敵対勢力に伝えるためのサポート • 同盟国やパートナーの結集の支援	• 国益を直接かつ実質的に脅かさない脅威には対応しにくい • 複数の政府機関の関与 • 脅威への対応は、その影響とアトリビューションの確実性に比例させる必要 • 慎重な対応が必要であり、対応が遅れる可能性 • ネットワークとその国家・経済安全保障への影響、軍事的支援に重点 すべてのプレーヤーの役割、責任、ルールを定義する責任がある
政府：法執行	• 悪意のあるサイバー行為者を特定し、訴追および懲罰的措置を講じる 公知のためのアトリビュート結果の公開を支持	• 管轄をまたぐ事象への対応が難しい 政策と手順が高度な敵対的手法に対応していない
政府：民生関係	• サイバーディフェンダーに計画と準備のための情報を提供 • CTIデータのユニークなソースを取得し、提供 敵対する外国人情報機関を対象とした防諜調査を支援	政府システムに対する脅威への対応と対策に注力
政府：軍関係	• サイバーディフェンダーに計画と準備のための情報を提供 • 軍事ネットワークに対する	軍事システムに対する脅威への対応と対策に注力

	より高度な対応能力をサポート • 敵の意図と能力の情報を提供 • 潜在的な行動に対する敵対者の特定を支援 • All source intelligenceをCTI分析に統合可能 • 軍事情報の敵対者を対象とした防諜調査の支援	
重要インフラ所有者・運営者	• より高度なレスポンス能力をサポート リスクと脆弱性を特定するための敵対的エミュレーションとペネトレーション・テストの強化	• 重要インフラへの脅威への対応と対策に特価 ITとOTの両データを取り込んだCTIデータが必要
技術開発事業者	顧客と共有するための技術固有の洞察の開発を支援	継続的な信頼を醸成し、有料セキュリティ・モデルを阻止するため、すべての顧客および自社技術のユーザーと共有するよう奨励する必要
テクノロジーサービス事業者（例：ISP、ウェブホスティング、クラウドサービスなど）	• より高度なレスポンス能力をサポート リスクと脆弱性を特定するための敵対的エミュレーションとペネトレーション・テストの強化	• CIエコシステム全体でACD活動を可能にするソリューションを含む、ネットワークとシステムのコンポーネントの提供 • 技術的な問題は、他の多くの組織にも浸透している可能性 クライアントのネットワークにアクセスできる可能性
サイバーセキュリティサービス事業者（例：FireEye、	• 民間企業からの委託でインシデントレスポンス活	• 潜在的な監督要件に制限されない

Mandiant)	動を実施 • 商用CTIデータおよびレポートの強化 • 独自のインシデント対応活動やソースによる、より高度なCTIアトリビューションデータの提供 オープンソースのアトリビューションレポートを作成し、広く配布	• 十分なリソースを持つ組織は、「グレーゾーン」での活動を行う可能性が高い • 報告及び正確性に関する標準化された要件がない 報告されるデータは、入手可能な情報源に依存
民間事業者	• より高度なレスポンス能力をサポート リスクや脆弱性を特定するための敵対的エミュレーションやペネトレーション・テストを強化	• ニーズは業界やリソースによって異なる • 資金力のある組織は、「グレーゾーン」で活動する可能性が高い • 政府が十分な支援をしていないと判断した場合、不正を行う可能性が高い • 顧客を保護しながら迅速に対応することへの懸念

3. 米国における政策と法的枠組み

米国では、サイバー活動、法的権限、および政策のための単一の中心地が存在しない。サイバー空間に対して効果を与える権限は行政府に分散している。ホワイトハウスは、大統領令（E.O.）と国家安全保障政策メモランダム（NSPM）という形で政策を発表している。議会は、特定の種類の組織が取るべき行動に直接的または間接的に影響を与える一連の法律を可決している。これらの法律のいくつかについては前述した（第2節(6)参照）。

一般的に ACD 活動、特にアトリビューション活動を行う主要な省庁には、国家安全保障局（NSA）、米国サイバー軍 （USCYBERCOM）、国土安全保障省のサイバーセキュリティ＆インフラセキュリティ局（CISA）、連邦捜査局（FBI） が含まれる。ACD 活動や対話型ツールに明確に焦点を当てているわけではないが、NIST National Cybersecurity Center of Excellence (NCCoE) もサイバーセキュリティ・ソリューションのデモンストレーションに一役を担う。

NSA と USCYBERCOM の積極的な ACD 活動、さらには攻撃的な活動を行う権限は、サイバー空間に対して効果を与える活動を行う権限を得るための明確な手順を開発した NSPM 13 に大きく基づいている。USCYBERCOM は、これまでに実施した ACD 活動の種類をいくつか公表している。NSA の一般向けウェブサイ

トに掲載されている活動には、持続的関与、前方防衛、前方狩猟作戦（HFO）の 3 種類がある。持続的関与とは、サイバー・オペレーターが「サイバー脅威を傍受して阻止し、敵対者の能力とネットワークを低下させ、DOD ミッションを支援する国防総省情報ネットワーク（DODIN）のサイバーセキュリティを継続的に強化する」ために絶えず活動することと定義される。永続的な関与は、DOD と USCYBERCOM のサイバースペースにおける姿勢を、事後的なものから積極的なものにする。

前方防御は、武力紛争のレベルを下回る活動を含む、悪意のあるサイバー活動をその発生源で混乱させる活動であると説明されている。つまり、デバイス、ネットワーク、組織、または敵対国が、米国のネットワークや機関に対する脅威として認識されているか、サイバースペース内またはサイバースペースを通じて積極的に攻撃している場合、米国がそれに対してコストを課すことが期待できる。前方を守るには、敵の活動の発生源にできるだけ近い場所で活動し、米国のサイバー・オペレーターの活動範囲を広げ、脅威を発生源で無力化する必要がある。

HFO は、厳密に防御的であり、ホスト国の招待によるものである。HFO の間、USCYBERCOM のオペレーターは、パートナーと並んで、敵国のネットワークにおける悪意あるサイバー活動と脆弱性を探す。HFO で得られた知見は、他の USCYBERCOM の活動と同様、一般に公開される。2021 年、USCYBERCOM はロシア情報局（SVR）APT 29 に起因する 8 つのファイルをもたらしたソーラーウィンズのサプライチェーン攻撃に対応し、サイバーセキュリティ・インフラ安全保障局（CISA）と共同 HFO を実施した。これらの作戦により、敵対者の戦術、技術、手順、意図に関する情報が得られた。[4]

NSA と USCYBERCOM の積極的な ACD 活動、さらには攻撃的な活動を行う権限は、サイバー空間に効果を与える活動を行う権限を得るための明確な手順を開発した NSPM 13 に大きく基づいている。

CISA は、ガイダンスの提供、脅威に関する情報の共有、ツールの提供を通じて、民間企業、特に重要インフラ運用者のネットワーク防御を支援する役割を担っている。CISA は、特定の活動を特定の行為者に帰属させる警告を公に提供する例として、2022 年 1 月にロシアの国家が支援する米国の重要インフラへの攻撃に関して発した警告を挙げている[5]。民間企業のアトリビューション評価の例については、以下の表 3-6 を参照されたい。

表 3-6：民間企業のアトリビューションの評価.

[4] U.S. Cyber Command Public Affairs, "CYBER 101: Hunt Forward Operations", 2022, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

[5] CISA, Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

公表日	タイトル	内容説明
2022年4月27日	Microsoft: ウクライナでのハイブリッド戦争	Microsoftは、ウクライナに対するハイブリッド戦争で観測されたロシアの破壊的なサイバー攻撃の詳細をブログで発表
2022年3月7日	Google: ウクライナでのハイブリッド戦争	Googleの脅威分析グループ(TAG)は、ロシアの脅威者の多くから、エソポネージからフィッシング詐欺に至る活動を観測
2022年2月28日	Microsoft: ウクライナでのサイバー脅威活動、分析と情報源(更新版)	Microsoftは、ウクライナで激化するサイバー活動を監視し、潜在的な攻撃に関するインテリジェンスと、今後の攻撃に対する予防的防御を実施するための情報を組織に提供
2022年2月4日	Microsoft: ACTINIUMがウクライナの組織を狙う	Microsoft脅威情報センター（MSTIC）は、約10年前から活動し、ウクライナの組織やウクライナ問題に関連する組織へのアクセスを追求してきたACTINIUMという脅威グループに関する情報を共有
2022年1月20日	Palo Alto Networks: 脅威の概況、ロシアとウクライナのサイバー紛争が進行中	1月14日未明、ウクライナ政府の多数のウェブサイトを標的としたロシアによる一連のサイバー攻撃について報道。この攻撃の結果、多くのサイトが改ざんされたり、アクセス不能になったりしていることが判明

CISA と FBI は、脅威とサイバー攻撃に関する情報を共有する重要な責任を負っている。SolarWinds、Microsoft Exchange、Colonial Pipeline の攻撃を受け、2022 年 5 月にホワイトハウスは大統領令 14028 "Improving the Nation's Cybersecurity "を発行した。この命令は、FBI、CISA、情報機関の一部のメンバーなど、サイバー攻撃の調査や修復を担当する米国政府機関間の情報共有を改善することを目的としている。

また、FBI は、悪意のある行為者を阻止するために、正確なアトリビューション技術に支えられた ACD 技術を使用している。FBI は、その権限により、「捜査、情報収集、および悪意のあるサイバー活動のターゲットと緊密に連携して、犯人を特定し、再犯を阻止し、責任を負わせる」ことができると報告している。大統領政策指令（PPD）41 は、重要なサイバー事件が発生した場合の脅威への対応について、FBI を連邦政府の主導機関に指定し、大統領令 12333 は、米国内での情報活動の暴露、防止、調査について FBI を主導機関に指定し、合衆国法典第 18 編第 1030 条は、スパイ行為と対外防諜に関わるサイバー調査を指揮するよう FBI を指定している。FBI は最近、ランサムウェア・グループのネットワークに数カ月間侵入し、身代金を支払うことなく被害者のデータを解放するための復号化キーの取得とネットワークの完全シャットダウンに成功し、「ハッカーをハックした」と報告している。悪意のあるサイバー行為者を起訴する場合、FBI は必然的に、刑事訴追のための「合理的疑いを超える」基準に耐えられるようなアトリビューションの結論を出さなければならない。

これらの省庁は、自らの業務のために ACD やアトリビューション活動を行うだけでなく、これらの分野で民間企業への支援も行っている。例えば、NSA は、産業界、特に国家安全保障、国防総省、防衛産業基盤の分野と連携し、サイバーセキュリティ・コラボレーション・センター（CCC）を運営している。

- CCC を通じて、NSA は、産業界のサービス・プロバイダーと協力して、民間部門に向けられた国家によるサイバー活動や悪意のあるサイバー活動を検知し、それに対処している。
- 敵の戦術、技術、手順を迅速に検知し、そのツールや技術を妨害するために、民間団体やサービス・プロバイダーと共同で分析的な技術開発を行う。
- 民間企業やそのサービス・プロバイダーに対する脅威や脆弱性に関する積極的な情報提供や二国間情報交換を推進する。
- 特定された脆弱性について、民間企業や NSS への技術提供者に通知し、協力し、共同で緩和策を開発する。

また、CISA は組織がセキュリティ能力をさらに向上させるのに役立つ、無料のサイバーセキュリティツールとサービスのリストを編集している。この生きたリポジトリには、CISA が提供するサイバーセキュリティサービス、広く使われているオープンソースツール、サイバーセキュリティコミュニティ全体の民間および公共セクター組織が提供する無料のツールやサービスが含まれている。提供されるツールのカテゴリーは、以下の目標によって構成される。

- 損害を与えるサイバーインシデントの可能性を低減する
- 侵入の可能性を迅速に検知するための手段を講じる
- 侵入が発生した場合の対応策を組織が確実に準備する
- 破壊的なサイバーインシデントに対する組織の回復力を最大化する

ISA は、サイバーセキュリティ評価ツール（CSET）も提供している。CSET は、「運用技術と情報技術を評価する体系的なプロセスを通じて、資産所有者と運用者をガイドするスタンドアロン・デスクトップ・アプリケーション」である。CSET は、組織がそのシステムとネットワークのセキュリティ状況を評価するのに役立ち、要約レベルおよび詳細レベルの両方の結果を提供する。CSET は、一連のアンケートを通じてユーザーをガイドする。評価結果は、長所と短所を示す一連のチャートと優先順位付けされた推奨事項、および組織がサイバーセキュリティリスクの姿勢を改善するのに役立つ他のリソースとして提供される。CSET にはいくつかの標準が組み込まれており、ユーザーの選択に応じて評価に含めることができる。これらのオプションの標準の例としては、NIST Cybersecurity Framework、NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations、Committee on National Security Systems Instruction (CNSSI) No.1253, Categorization and Control Selection for National Security Systems、さらに重要インフラ（産業制御システム、スマートグリッド、原子力施設など）向けの様々なサイバーセキュリティ標準が挙げられる。

NIST NCCoE は、産官学の専門家を集め、複雑な IT システムのセキュリティと国家の重要インフラの保護という現実的なニーズに取り組むコラボレーション拠点だ。NCCoE の目標は、企業や商取引のサイバーセキュリティを向上し、サイバーセキュリティの学習曲線を下げ、セキュリティ技術の革新を促進することである。NCCoE が提供する重要なリソースの 1 つに、NIST Special Publications series の実践ガイド達がある。各実践ガイドは、NCCoE が様々な技術や産業領域におけるサイバーセキュリティの課題に対処するために、市販の技術や標準をどのように適用してきたかを示している。産業ドメインには、5G、AI、モノのインターネット、サプライチェーン保証、ゼロトラストアーキテクチャなどの領域が含まれる。産業ドメインは、主に重要インフラに焦点を当て、エネルギー、金融サービス、製造業などの産業が含まれる。

4. 効果的なアトリビューションのための潜在的な障害

アトリビューションは、悪意のある行為者を特定し、サイバー防御を強化し、指導者に情報を提供する上で重要だ。しかし、特定の行為を正しい行為者に確実に帰属させることは、必ずしも容易ではない。そもそも誰の指がキーボードに触れていたのか、そもそも誰がこの人たちにキーボードに触れるように指示したのかを掘り下げることは難しい場合がある。もう一つの課題は、サイバーインシデントが発生した場合、アトリビューションに長い時間がかかり、すぐに価値を見いだせない可能性があることだ。

表 3-7 は、CTI およびアトリビューション情報をサイバーセキュリティ情報共有組織と共有する際の潜

在的な障壁の詳細を示す。

表 3-7. 効果的なアトリビューション情報発信を阻むもの.

障壁	説明
法務/ポリシー	個人情報や知的財産に関するプライバシーへの懸念、および不正な開示による法的影響についての認識
技術的障壁	共有組織のシステム間の相互運用性/互換性の欠如
インフォメーショナル	共有する情報が多すぎて処理できない、共有情報の適用性がない、信頼性のないデータ
オペレーショナル・セキュリティ	機密性の高い情報源や方法、あるいは情報の入手経路を推測できるような情報を広めないという要件
コラボレーション	プロセスの複雑さ、信頼関係の確立の難しさ、互恵性の欠如、参加者のタイプ、グループのサイズ
管理上の障壁	組織を「制御不能なリスク」にさらすことによる内部リスク回避と不信感、情報交換の非効率的な方法、共有情報の管理不備、情報共有のための信頼経路を確立する合意がないこと
組織上の障壁	リソースが限られているため消費できない、情報の利用を管理・制御する仕組みがない
パフォーマンス	必要なシステム技術のコストが高い、古い/信頼性のないデータに基づく誤検出のコスト、共有データを処理するためのリソースが限られている。
コスト	必要なシステム技術のコストが高い、古い/信頼性のないデータに基づく誤検出のコスト、共有データを処理するためのリソースが限られている。

第４節 アトリビューション機能の実装

前節では、アトリビューションの概要について説明した。本節では、アトリビューション活動が実際にど

のように行われるのか、またアトリビューションが基本的に分析プロセスであることを説明する。

アトリビューションは、観察された悪意のある活動の特定の要素を用いて、誰がという問いに答えようと試みる。

- TTPs（どのように）
- インフラストラクチャ、ツール、マルウェア（どこで、どのように、何を）。
- 動機（なぜ）
- ターゲット（どこで、いつ、なぜ）

初期のインシデントレスポンス活動とデータ収集が完了すると、収集したインテリジェンスとデータをレビューして分析し、その活動を特定の国、グループ、悪意のあるサイバー行為者に帰属させるという手作業のプロセスが続く。分析プロセスの後に、アトリビューション情報は、適切な事後措置や防御策を策定するために、組織の幅広い知識ベースの中に織り込まれる必要がある。組織の CTI および分析能力が成熟するにつれて、アトリビューション情報をますます活用して戦術、運用、および戦略の見通しを改善し、指導者や意思決定者を支援する必要がある。

帰属の疑いを立証できれば、たとえそれが単一の脅威要因に絞り込めなかったとしても、インシデント対応担当者が、特に調査の初期段階では容易に明らかにならなかったかもしれない特定のアーティファクトや方法論に焦点を当てることができるようになる。例えば、MITRE ATT&CK のようなフレームワークと最初のアトリビューション決定を組み合わせることで、悪意のあるイベントの前または後に脅威者が取った行動を分析者が特定するのに役立つ。

アトリビューションの確立は、一連の技術的なツールを使用するだけでは不可能であることを忘れてはならない。ツールによって明らかになったことを評価するためには、熟練し、訓練されたサイバーセキュリティ・アナリストの集団が必要だ。組織のサイバーセキュリティ運用は、アトリビューションに焦点を当てた成熟した分析能力なしには成熟しない。この小節では、アトリビューションプロセスの一部である情報と分析の種類を特定るが、これらのインプットだけでは、アトリビューションの結論を導き出すのに十分ではない。この作業には、好奇心と判断力を備えた経験豊富なアナリストが必要である。

Timo Steffens 氏は、「アトリビューションはプロジェクトのように組織化できず、分析を行うためのチェックリストも存在しない」と指摘した。アトリビューションへの取り組みは、確立された一連のプロセスや手法に従うことはできず、効果的なレベルのアトリビューションを達成することは期待できない。しかし、分析者が利用すべき最低限のベストプラクティスは存在する。ステファンズ氏は、マルウェア、インフラ、コントロールサーバ、テレメトリ、インテリジェンス、キュイボノ（MICTIC）フレームワークに従ってアトリビューションを確立するための 1 つの可能なアプローチを示しており、同氏はこれをダイヤモンド・モデルの「よりきめ細かいバージョン」と呼んでいる。

1. 企画・準備

サイバー攻撃におけるアトリビューションには、通常、技術的（どのように）、戦術的（TTP）、作戦的（何を）、戦略的（誰が、なぜ）の 4 つのレベルの脅威情報が分析される。技術的なレベルでは、特定のサイバー攻撃に使用された技術を示す、調査官が利用可能なさまざまなツールがある。同じツールや技術の多くは、インシデントレスポンス活動で利用される。

図 3-6：脅威インテリジェンスのレベル.[6]

アトリビューションを立証しようとする場合、作戦レベルと戦略レベルのインテリジェンスを明確に区別することは困難であり、両者はかなりの程度重複している。さらに、これら 4 つのレベルの分析は、決められた時系列や順序に従った段階的なプロセスであることはほとんどない。場合によっては、技術的な指標で悪意ある活動を特定する前に、地政学的な背景やその他の非フォレンジックな情報源が、帰属の最初の手がかりとなることもある。したがって、戦略的なレベルでの分析は、技術的な側面を検討する前に始めることができる。戦略的分析には、敵対者の動機に関する知識が必要であり、商業、軍事、経済など、他国の優先事項に対する理解によって導かれる。

2. アトリビューションプロセスをサポートする情報カテゴリー

アトリビューションプロセスはしばしば反復され、前述したように多くの種類の情報が利用される。本小節では、帰属プロセスで使用される情報のタイプについて説明する。

(1) 動機

サイバーイベントの調査が悪意のある意図的な行動を示すと仮定すると、その真の結果を評価するために、調査には数週間とは言わないまでも、数日かかる可能性がある。インシデント対応作業が進行している間、次の段階として、敵対的な行為の背後にある動機を確認することが自然だ。犯罪を目的とした行為なのか？不満を抱いた従業員による行動なのか？イデオロギー的な敵対者による抗議なのか？それとも、外国勢力の国家安全保障に起因するものなのか？もし、その行為が国家によるものと判断されれば、また新たな疑問が生じ、それぞれの動機を正確に把握するための緻密な追跡調査が必要となる。

[6] EC-Council. "https://twitter.com/eccouncil/status/12923949925106073"

図 3-7：攻撃者のタイプに関連する動機.

特定の国家や国内の活動家の活動を特定しようとする場合、分析者は以下に示すような一連の質問をすることになる。

- 悪意のある活動は、情報収集のような単純なサイバースパイ活動か？もしそうなら、それは典型的な情報収集活動なのか、それとも国家が支援する商業スパイの活動の一部なのか？
- 後続の攻撃のための基礎固め（プレ・アタック）なのか？
- 特定のメッセージやシグナルを伝達するためのものなのか。その場合、メッセージは何か？
- 他の方法でターゲットの認識を形成することを意図しているのか（影響力の行使）、またその目的は何か。
- 選挙結果を左右するため、あるいはその信憑性に疑念を抱かせるためなのか。
- 敵対者を弱体化させるために、混乱と混沌を招くこと、または反対意見を煽ることを意図しているのか。
- 動機を決定する際、加害者が自らの行動をどのように見ているかを理解することが役立つ場合がある。彼らはいわれのない（サイバー）行動を意図しているのか。あるいは、（サイバー領域であれ他の場所であれ）自分たちに行われたことに対する報復行動と見ているのか。あるいは、相手が自分たちに対して行おうとしていると加害者が予想する動きに対する防御的な行動（予防的または先制的）として正当化するのか。

重要なのは、加害者（特に国家のエージェントや代理人）が自らの行動を隠そうとせず、その真の意図を隠そうとしたケースがあることだ。例えば、被害者のネットワークに危害を加えることを真の目的としていながら、自分たちの行動をランサムウェアと称して見せかけることがある。このような戦術は、特徴づけとアトリビューションの課題を複雑にしている。特定の悪意あるサイバー事象の徹底的な調査、加害者が時間をかけて公開した追加情報（故意または無意識）、および文脈的要因（地政学的動向など）の考

慮が、最終的に攻撃者の根本的な動機に関する重要な洞察をもたらす。

(2) 悪意ある行為者の背後にいるのは誰なのか？

悪意のある行為者の身元を確認する際に考慮すべきもう一つの要素は、誰が、あるいはどの組織が、悪意のある活動を指示または後援していた可能性があるかということだ。また、組織の指導層のどのレベルにおいて、悪意のある活動が承認されたのか、あるいは少なくとも支援/容認されたのかも考慮される。

近年、サイバーフォレンジックは著しく進歩しているが、悪意のある行為者の正体（別の悪意のある行為者になりすましているかどうかも含む）を隠蔽するための技術の高度化もそれに歩調を合わせて進んできている。フォレンジックによる TTP の調査は、サイバー攻撃者の身元を確認する上で非常に有効だが、インテリジェンスは、アトリビューション結果の信頼性を高め、さらに重要なことに、悪意のある活動のスポンサーまたは指示者を確認するのに役立つ。悪意のある活動を指揮する組織に関するインテリジェンスは、広範なネットワーク監視、センサーの持続的な前方展開と監視、そして特に、こうした攻撃の元となる敵対的ネットワークへの侵入から得ることができる。後者の 2 つの情報源は、ほぼ間違いなく機密情報であり、民間企業のアナリストには一般に入手不可能であろう。

悪意のあるサイバー事象の特定と対応は、悪意のある行為者または他の者がサイバー事象の手柄を立てたり、責任を否定したりすると、さらに複雑になる可能性がある。フォレンジックが重要なのは、インテリジェンスと同様に、どちらかの証明または反証を助けるからである。アトリビューションによって明確な特定に至る上で大きな障害となっているのは、一部の国家がプロキシやその他の非国家機関を利用してサイバー攻撃を行うことが一般的であることだ。このような悪質なケースでは、フォレンジックとインテリジェンスだけでは、帰属やどの組織がその活動を促したかを明確に示すことができない場合がある。例えば、2020 年 7 月、2 人の中国人が、国家安全部（MSS）の広東省国家安全局（GSSD）と協力しながら、個人的な利益を得るために被害者を狙ったとして、米国司法省に起訴されたことがある。[7]

(3) 攻撃手法の高度化

サイバー脅威の主体は、その能力や洗練度において平等ではない。彼らは、その活動に必要な様々な資源、訓練、支援を受けている。サイバー脅威の主体は、単独で活動することもあれば、より大きな組織（すなわち、国民国家や組織的犯罪集団）の一部として活動することもある。熟練した悪意のある行為者は、例えば、セキュリティ研究者が使用している商用セキュリティツールを活用するなどして、与えられたタスクに有効であり、かつ／または防御側がその活動を特定することを困難にするため、容易に入手できるツールやテクニックを使用することがある。

最も巧妙な攻撃を行うことができる行為者の数は、国家を含めて比較的少ないため、攻撃の巧妙さのレベルを決定することで、悪意のある攻撃者の可能性を迅速に絞り込み、アトリビューション分析の焦点も

[7] U.S. Department of Justice, Public Affairs Notice, 20-675, July 21, 2020., https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

絞り込むことができる。以下に示す悪意のある攻撃者の種類とその巧妙さのレベルは、アトリビューション分析の出発点となる。

- Advanced Persistent Threats（APT）とは、高度な技術と技能を持つ最上位の脅威者のことを指す。APT は、高度な技術を駆使して、目標を達成するために複雑かつ長期的なキャンペーンを行うことができる。この呼称は、通常、国家や非常に熟練した組織犯罪集団にのみ使用される。
- 国家に代わって活動する国家支援型サイバー脅威主体は、主に地政学的な目的を達成するためにサイバー脅威活動を行う。彼らは、専用のリソースと人員を持ち、大規模な計画と調整を行う、最も洗練された脅威主体であることが多い。先進的なサイバープログラムを持たない国家は、高度なサイバー脅威活動を可能にするために、商業的なサイバーツールや世界的に増加する人材を利用することができる。また、一部の国家は、民間企業や組織的犯罪シンジケートと業務上の関係を結んでいる。
- サイバー犯罪者は、主に金銭的な動機で行動し、その精巧さは千差万別だ。組織的な犯罪集団は、多くの被害者に影響を与えることができる専門的な技術的能力に加えて、計画立案やサポート機能を有していることが多い。サイバーツールやサービスの違法なオンライン市場によって、サイバー犯罪はよりアクセスしやすくなり、サイバー犯罪者はより複雑で高度なキャンペーンを行うことができるようになった。犯罪的サイバー行為者、特に経済的利益を動機とする者は、身元を隠し、訴追を避けようとする。彼らは、ガバナンスや政策上の条件から、身元を隠すことが容易な場所を探す。
- ハクティビストは、イデオロギー的な動機でサイバー悪意ある活動を行い、一般的に国家が支援するサイバー脅威の行為者や組織的なサイバー犯罪者よりも洗練度は低い。これらの行為者は、テログループと同様に、多くの場合、展開にあまり技術的なスキルを必要としない、広く利用可能なツールに依存している。彼らの行動は、ターゲットに対して評判以上の永続的な影響を与えないことが多い。しかし、時には、これらの行為者は、ターゲットに物理的および金銭的な損害を与えることができる。
- インサイダー脅威は、組織内で働く個人で、セキュリティ境界で保護されている内部ネットワークにアクセスできるため、特に危険だ。インサイダー脅威は、不満を持つ従業員である場合もあれば、他の脅威要因に関連する場合もある。

(4) 攻撃の重大性

悪意のあるサイバー事象の重大性、または影響力は、悪意のあるサイバー行為者の特定をさらにサポートすることができる。この重大性の判断は、主観的である場合もあれば、事実に基づく場合もある。

さらに、重大性または影響の決定をサポートするために、サイバーセキュリティ組織の外部の利害関係者と他の考慮事項が必要な場合がある。攻撃の重大性はすぐには明らかにならないかもしれないので、この帰属の要素は価値を持つようになるまで時間がかかるかもしれない。以下に列挙する基準は、インシデントの重大性の評価と特徴付けを支援することができ、実際の被害がすぐに明らかにならない場合に役立つことがある。

1. 敵の目的と意図された効果

2. 実際に発生した影響(脅威の主体が意図したよりも大きい、小さい、局地的、または広範囲に及ぶ可能性がある)
3. 関与した標的(政府、重要インフラ、金融など)
4. 攻撃で使用された TTP
5. その悪意ある行為が、より広範で大胆な行動パターンを示しているのか、それとも単なる単発の行為なのか

(5) 脅威行為者のスコアリング

インシデントレスポンスやイベントの分析時には必要ありませんが、スコアリング手法を適用することで、組織は脅威をより詳細に特定し、対応に優先順位をつけることができる。スコアリングの方法論はさまざまだ。一般に、スコアリング方法には、定義された一連の基準と、その基準を解釈するための水準が含まれる。組織によっては、数学的なスコアを適用して基準をさらに拡張し、そのスコアを比較に使用する方法を選択する（例：スコアの平均、重要性に基づく基準の重み付け、スコアの高さと低さに意味を持たせるなど)。

本小節では、分析者が帰属プロセスで最もリソースを投入すべき脅威の優先順位付けに役立つ、スコアリング基準の例を示す。

脅威行為者を評価するための基準

脅威のランク付けは、脅威行為者の意図と脅威行為者の能力に基づいて行われる。これらのランク付けを組み合わせると、総合的な脅威レベルが算出される。表 8 と表 9 は、脅威のスコアリング基準の例を示している。

表 3-8. 脅威行為者の意図のスコアリング.

脅威行為者のインテントのスコアリング	
意図レベル	**基準説明**
非常に高い (Focused)	脅威の主体は、着目しているシステムまたはサービスを攻撃することを主な目的としている。これらは通常、既知の、敵対的な、主要な外国の諜報機関によるものだ。 脅威行為者が標的システムまたはサービスについて詳細な調査を行い、システムまたはサービス固有の攻撃を作成したことを示す証拠がある。これには、特定のユーザーの行動(業務に関連すると思われるメールの添付ファイルを開くなど)に訴えかける、またはそれを利用するように設計された攻撃が含まれる。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を行い、攻撃の情報提供と促進を試みる可能性が非常に高い。 脅威行為者は、滅多に発生しない攻撃機会を利用するために待機し、攻撃を実行するために、複数の脅威行為者が連携する形でリソースを急増させる準

	備をしている可能性が高い。
高 (Committed)	脅威の発生源は、持続的かつ頻繁にシステムまたはサービスを攻撃しようとしている。これらは、典型的には、外国の諜報機関、高度な能力を持つハクティビストグループ、テロリストグループ、および主要な犯罪組織によるものだ。 脅威行為者は、ユーザーの行動を特に利用することを目的とした攻撃の開発を含め、攻撃に数人を割くことをいとわないという証拠がある。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を行い、攻撃の情報提供と促進を試みる可能性がある。
中位 (Interested)	脅威の行為者は、頻繁にシステムまたはサービスを攻撃しようとしている。これらの行為者は、典型的には、小規模なテロ組織、ハクティビスト組織、組織犯罪集団であり、そのシステムまたはサービスがその組織にとって特に関心のあるものである場合である場合が多い。 脅威行為者は、攻撃に数人の人員を割くことをいとわない。脅威行為者は、ユーザーコミュニティに対して直接的な説得、贈収賄、強要を試みることはないだろう。
低い (Curious)	脅威行為者は、時折、または偶然にシステムやサービスを攻撃しようとしている。このような行為者は、通常、単一問題の政治的圧力団体、アマチュアハッカー、テロリストに感化された個人（ローンウルフ）、調査ジャーナリスト、学者、商業的ライバルとなる場合が多い。 脅威行為者は、攻撃のためにごく少数の人々を割くことを望んでいる。脅威行為者は、ユーザーコミュニティに対して直接的な説得や強制を試みる可能性は極めて低い。
非常に低い (Indifferent)	脅威行為者がシステムやサービスに対して何らかの攻撃を試みる可能性は極めて低い。このような行為者は、通常、ビジネスパートナーであり、システムまたはサービスを攻撃していることが知られれば損害を受けるような、良い評判を持つ組織である。

表 3-9. スレットアクター能力スコアリング.

スレットアクター能力スコアリング	
能力レベル	**基準説明**

手強い (Formidable)	脅威の主体が極めて有能で、十分な資金を持つ外国の諜報機関のような場合。 • システムまたはサービスの侵入に数人年を割く • 標的を特定した攻撃を展開 • 標的システムやサービスに関する情報を複数の情報源から収集し、調整 • 長期的な攻撃のためにインサイダーを育成 • 大量の機器の導入 • 複数の脅威行為者を利用した攻撃の調整
重大な (Significant)	脅威の主体が有能で、大きな資源を持っている場合。例えば、中程度の資源を持つ外国の諜報機関、よく組織されたテロリストや犯罪者集団など。 • システムやサービスへの侵入に数人週を割く • 一般に公開されている攻撃ツールをすべて使用 • 特定の攻撃のためにインサイダーに影響を発揮 • 適度な量の機器を配置
限定的 (Limited)	小規模で組織化されたテロリストや犯罪者集団、あるいは有能な個人ハッカーなど、脅威の主体が適度な能力と資源を持っている場合 • システムやサービスへの侵入に数人日を割く • 一般に公開されている有名な攻撃ツールを使用 • 少量の機器を展開
小規模 (Little)	脅威の主体が、一般的なインターネットユーザーなど、ごくわずかな能力とリソースしか持たない場合。 • システムやサービスへの侵入に数人日を割く • ごく少量の機材で展開
非常に小さい (Very Little)	脅威の主体が、コンピュータやインターネットの初心者のように、能力やリソースをほとんど持たない場合。 • シンプルな「プラグアンドプレイ」プラグインデバイスとリムーバブルメディアの使用 • システムやサービスへの侵入に数時間を割く

ある時点では複数の脅威者が存在する可能性があるため、スコアは最も高い脅威者の意図と能力のレベルを反映する必要がある。サイバー脅威の性質や潜在的な脅威者に関する情報は常に進化しているため、脅威が大きく変化し、特定のシステムに対するリスクの再評価が必要であるかどうかを判断するために、定期的に脅威評価を見直すことが必要である。

脅威行為者の意図と能力に関する相対的なスコアは、全体の脅威レベルマトリックスで確認する必要が

ある。表 3-10 に示すように、脅威のレベルと意図が最も高く、意図を実行する能力が最も高いものを「重要」とする。そして、全体的な脅威は「深刻」へとスケールダウンしていく。最も懸念の少ない脅威は、「無視できる（Negigible）」と分類される。

表 3-10．脅威レベルマトリックス脅威レベルマトリックス．

意図のレベル	能力レベル					
		非常に小さい	小規模	限定的	重大な	手強い
	非常に高い	中程度	中程度	シビア	シビア	クリティカル
	高	低	中程度	大幅な	シビア	クリティカル
	中位	低	低	中程度	大幅な	シビア
	低	無視できる	無視できる	低	中程度	大幅な
	非常に低い	無視できる	無視できる	低	低	中程度

この可能性スコアを、ある脅威者が攻撃を成功させた場合に起こりうる結果と照らし合わせて、リスクの高さを判断し、他の特定されたリスクに対して優先的に対策を講じるべきかどうかを決定することができる。

(6) 偽装工作の可能性の判断

欺瞞、または難読化とは、悪意のある脅威行為者がその身元、目標、技術を隠すために使用する TTP のことを指す。防御者が活動を特定するための手がかりを残さないようにするため、脅威者はインターネット上でデータを密かに送信するツールやテクニックを使用することができる。

また、洗練された脅威行為者は、偽旗作戦を行うことがある。これは、ある行為者が他の行為者の既知の活動を模倣することで、防御者にその活動を他の行為者のものと誤認させることを狙ったものだ。例えば、ある国家は、サイバー犯罪者や他の国家が広く使用していると思われるツールを使用し、攻撃が無関係の行為に起因すると誤認されることを期待することができる。

サイバー犯罪者が自らの行動をうまく隠蔽する能力は、その巧妙さと動機づけのレベルに応じて異なる。一般に、国家や有能なサイバー犯罪者は、他の脅威行為者よりも難読化に長けている。

最近の悪意のあるサイバー行為者の手法には、「欺瞞」が含まれる。悪質なサイバー行為者は、偽装した別の ID を採用することで活動を隠したり、別の国にサイバー攻撃の濡れ衣を着せたりすることもある。一連のスパイ行為では、他国のハッキングインフラを乗っ取り、被害者をスパイしたり、マルウェアを配信するために利用したことがある。例えば、ロシアのハッカー集団「Turla」や「Waterbug」は、「OilRig」と呼ばれるイランのハッカー集団のサーバーを乗っ取り、ロシアの目的に利用するという複雑

なスパイ行為を長年にわたって行っている。[8]

3. アトリビューションプロセスを支援するモデル

CTI フレームワークの主な利点は、組織が敵の活動方法、および敵が最初のアクセスの獲得、発見、横方向への移動、データの流出を計画する手順について理解できるようになることだ。これにより、攻撃者の視点から活動を見ることができ、アトリビューション理論を構築する際に不可欠な動機と戦術をより深く理解することができる。さらに、組織はこの理解と知識を活用して、セキュリティ体制のギャップを特定し、脅威の検知と対応を改善することができる。これは、チームが攻撃者の次の行動を予測し、迅速に対処することを可能にする。

さらに、サイバーセキュリティのスキル不足が深刻化している現在の職場環境において、このフレームワークは、若手や新規採用のセキュリティスタッフに必要な知識と調査ツールを提供し、脅威データベースの構築をサポートする組織内のすべてのセキュリティ専門家の集合知を活用して、特定の悪質な脅威要因に迅速に対応できるようにすることが可能だ。

(1) ダイアモンド・モデル

セキュリティ・チームは、ネットワーク侵入の「誰が、何を、いつ、どこで、なぜ、どのように」するかを理解し、進行中の攻撃への対応と、攻撃を事前に軽減するアプローチの両方を開発する必要がある。これらの質問に対する回答の価値を高めるために、ネットワーク防御者は、脅威のデータを合成し、関連付け、文書化する能力が必要だ。

侵入分析のダイヤモンド・モデルは、これを実現するための 1 つのフレームワークだ。このアプローチでは、すべてのインシデントをダイヤモンド型のレンズを通して見る。ダイヤモンドの 4 つの要素（敵対者、能力、インフラ、被害者）は、攻撃の関係性と特徴を特定し、強調する。これら 4 つの中核的要素を検証することで、特定の悪意ある行為に関する洞察を得て、知識を得ることができる。4 つの要素を以下に示す。

- 敵対者：目標を達成するために、被害者に対してある能力を活用する責任を負う組織または脅威行為者である。
- ケイパビリティ：敵対者があるイベントで使用するツールやテクニックを指す。
- インフラストラクチャ：敵対者がケイパビリティを提供するために用いる、インターネット・プロトコル（IP）アドレスや電子メールアドレス、ドメイン名などの物理的または論理的な通信構造を含む。
- 被害者：攻撃が開始され、脆弱性が悪用され、または能力が使用される標的のこと。被害者は、組織、人、またはターゲットの電子メールや IP アドレス、ドメインなどの資産である。

要約すると、侵入分析のダイヤモンド・モデルは、「敵対者」が「被害者」に対して「インフラ」上で「能

[8] Turla Espionage Group Hacks OilRig APT Infrastructure, 2019, https://www.bleepingcomputer.com/news/security/turla-espionage-group-hacks-oilrig-apt-infrastructure/

力」を使用することを説明している。このモデルの原理は、以下の図 3-8 に示すように、すべての侵入に対して、敵対者は被害者に対してインフラ上の能力を活用し、インパクトを与えることで目標に向かって進むというものだ。

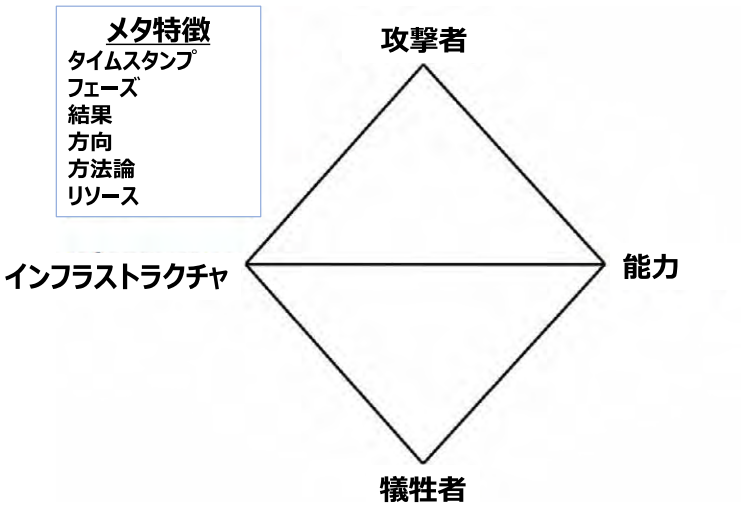


図 3-8：分析のダイアモンド・モデル.[9]

ダイヤモンド・モデルは、文脈に応じた指標を提供することにより、脅威情報の共有と他の計画フレームワークとの統合を向上させる。また、インテリジェンスのギャップを検出し、サイバー分類法、オントロジー、脅威インテリジェンスの共有プロトコル、および知識管理の基礎を築く。さらに、仮説の生成、テスト、文書化を促進することで、セキュリティ・チームは分析の精度を高め、分析プロセスの精度を向上させることができる。

ダイヤモンド・モデルの使用例

- 分析的ピボッティング

ピボットとは、あるデータ要素を取得し、データソースと連携してそれを活用し、他の関連する要素を特定する分析手法である。ピボットとは、仮説検証のことである。ピボッティングの成功は、セキュリティアナリストが要素間の関係を理解し、データ要素とそのソースを活用する能力を備えているかどうかにかかっている。

- 知識ギャップの発見

イベントに含まれていないダイヤモンド・ノードや、アクティビティ・スレッドに欠落しているイベントを、ダイヤモンド・モデルで接続することができる。これにより、ナレッジギャップを特定し、インシデン

[9] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "Diamond Model of Intrusion Analysis," Center for Cyber Threat Intelligence and Threat Research, Technical Report ADA586960, 2013.

ト対応と脅威のインフラおよび能力に焦点を当てることができる。

- 中心型アプローチ (Centered Approach

中心型アプローチは、ダイヤモンド・モデルの特定の機能に焦点を当て、新たな悪意のある活動を検出し、他の関連する機能に影響する活動を公開する。中心型アプローチには、敵対者中心型、能力中心型、インフラ中心型、被害者中心型、社会・政治中心型、技術中心型という 6 つの中心型アプローチがある。最初の 4 つはダイヤモンドのノードに焦点を当て、残りの 2 つはダイヤモンドのメタフィーチャーに焦点を当てる。

ダイヤモンド・モデルはどのような場合に有効か？

- 異なる侵入を比較し、グループ化する
- 一見、異質な活動間の類似性を検証する

ダイヤモンド・モデルの限界

- 高次のレベル
- 柔軟性が高すぎる - 情報をどのように「ビン詰め」するかは、ユーザー自身がチーム内で決める必要がある

ダイヤモンド・モデルはアトリビューションを判断する上で非常に重要なモデルである。ダイヤモンド・モデルは意思決定者やリーダーとの帰属に関する議論の枠組みを作るのに役立つ。

(2) Q モデル

Thomas Rid と Ben Buchanan の論文「Attributing Cyber Attacks」で紹介された Q モデル (図 3-9) は、アトリビューションが一本の直線的な経路ではないことを強調したものである。その目的は、技術的な詳細とアトリビューションに使用される方法を提供することで、アナリストがより多くの情報に基づいた疑問を持ち、結論に疑問を持てるようにすることである。

Qモデルは4つの情報レベルを持っている。黒字の外側のレベルは戦術的、灰色の中間のレベルは作戦的、白字の内側のレベルは戦略的である。最後のレベルは、Qの「フック」であるコミュニケーションである。例えば、アナリストがする質問は、レベル別に分けることができる。「何を」「どのように」は戦術的、「誰が」は作戦的、そして「なぜ」は戦略的となる。そして、これらの質問に対する答えは、攻撃への対応に関する意思決定を行うために、リーダーシップやその他の利害関係者に伝達するために使用される。

Qモデルは、アトリビューションの質が、アナリストの質問、方法、プロセス全体の概観の関数であることを強調する。Qモデルは、これらの構成要素を調査プロセスの4つのレベルで考えるための有用な構造を提供する。

- 戦術的/技術的レベル：何が／どのようにして攻撃が起こったのか、技術的な疑問を提起する。侵害の指標、侵入経路、ペイロード、ネットワーク活動など、技術的な証拠を評価する。
- 運用レベル：情報の統合により、何が起こったのか、より高度なアーキテクチャを理解し、攻撃の犯人を突き止める。これには、攻撃の技術的精巧さの評価、国家および非国家主体による既知の能力との比較、事件の地政学的背景の理解などが含まれる。

- 戦略的レベル：なぜそのような攻撃が行われたのかを判断する。このレベルでは、結論を導き出すためのストレステストを行い、悪意のある出来事の根拠を理解しようとし、一連の出来事が意味のある前例となったかどうかを判断する必要がある。
- コミュニケーション・レベル：帰属の結論がどのように伝達されるべきかを記述している。このモデルでは、より詳細な情報、推定的な表現、分析の限界などを伝えることで、より優れた集団防衛を可能にし、帰属の信頼性を高め、帰属自体を向上させることを主張している。

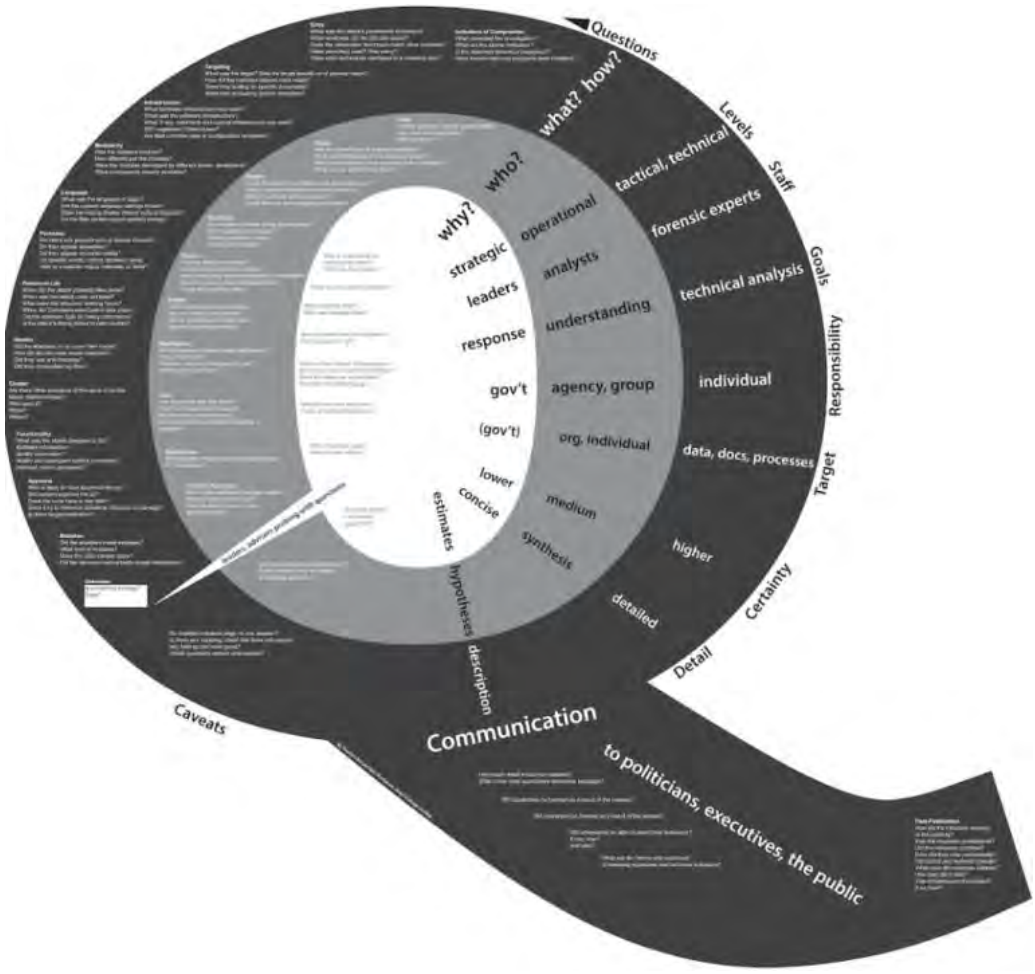


図 3-9. Attributing Cyber Attacks における Q モデル.[10]

[10] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks", Journal of Strategic Studies, Volume 38, 2015

Q Modelの限界

- Qモデルは、多くの組織や民間企業で採用されていないため、運用に制限がある。
- 国家安全保障上の脅威となる事象のアトリビューションに焦点を当てすぎており、犯罪的なサイバー侵入の事象のアトリビューションには焦点が当てられていない。
- 国家によるアトリビューションを公にすることでメリットが得られる場合もあるものの、敵対者を抑止するために公的なアトリビューションが必要なわけではない。

(3) MITRE ATT&CK モデル

MITRE ATT&CK (図3-10) は、実世界の観察に基づく敵対者の戦術と技術に関するグローバルにアクセス可能な知識ベースである。 MITRE ATT&CKは、APTグループがサイバー攻撃で使用した悪質な行為に関する情報をまとめている。ATT&CKは、Adversarial Tactics, Techniques, and Common Knowledgeの略で、これらのグループのTTPの詳細な説明が含まれている。ATT&CKの知識ベースは、民間企業、政府機関、サイバーセキュリティ製品・サービスコミュニティにおいて、特定の脅威モデルや方法論を開発するための基盤として使用されている。MITREは、ATT&CKが敵対者の行動の詳細な情報を提供し、特定の攻撃の背後にいる人物に関する結論をサポートするために使用される事例を文書化している。

MITRE ATT&CKは、敵対者が使用するTTPの説明、特定の技術に対する検出のための提案や一般的な緩和策の提供、APTグループの既知の手法、特徴、特定の攻撃起因のプロファイリングを行う百科事典のようなものだ。ATT&CKはまた、攻撃に使用されるソフトウェア（マルウェア、合法的または悪意を持って使用できる市販およびオープンソースのコードの両方）の広範なリストも提供する。ATT&CKに取り込まれたすべての情報は、一般に公開されているデータやレポート、およびコミュニティから提供されたものだ。最新版のATT&CK for Enterpriseには、14の戦術、188のテクニック、379のサブテクニック、129のグループ、および637のソフトウェアに関連する情報が含まれている。

ATT&CKは、世界中の知識豊富なサイバー専門家によって提供され、攻撃者のタイプやカテゴリー別に構成されているため、日本政府に最も関連するものを含め、攻撃者が使用しているTTPを特定するための重要なリソースとなっている。

ATT&CKは、世界中の洗練されたネットワーク防御者にとって、脅威に関する情報を確実に入手するためのCTIパズルの基礎となる部分となりつつある。例えば、英国のサイバーセキュリティ情報共有パートナーシップ（CiSP）は、ATT&CKの知識ベースを情報共有プログラムに統合する最善の方法について取り組んでいる。日本を含む多くの民間企業は、ネットワーク防御を強化するために、TTPに関するATT&CKの情報を活用することの重要性を認識している。

ATT&CKはどんな時に役に立つのか？

- 敵対者の行動を詳細なレベルで追跡する
- 特定の行動に関して、防衛側や他の組織と共通言語でコミュニケーションをとることができる

ATT&CKの制限事項とは？

- CTIの全側面や全技法をカバーしているわけではない
- 戦術的な側面が強い
- 複雑で、学習曲線が急な場合がある

MITRE は、ほとんどのモデルやフレームワークが ATT&CK を補完するものであり、ネットワーク防御者が 1 つのフレームワークだけを選択する必要はないと考えている。例えば、ATT&CK とダイヤモンド・モデルは補完関係にある。ATT&CK は敵の詳細な行動を記録し、Diamond Model は防御側が侵入のクラスタリングを行う場合に役に立つ。また、両者を併用するケースもある。例えば、ATT&CKでマップされた技術は、敵の能力を分析するためのダイヤモンド・モデルへの有効な入力ソースとなり得る。MITRE ATT&CK フレームワークは有用であるものの，それだけではアトリビューションの結論を支持するのに十分ではないこともある。MITRE ATT&CKは、ダイヤモンド・モデルなどの他の分析モデルと組み合わせることで、アトリビューションに関する結論をより確かなものにすることができる。

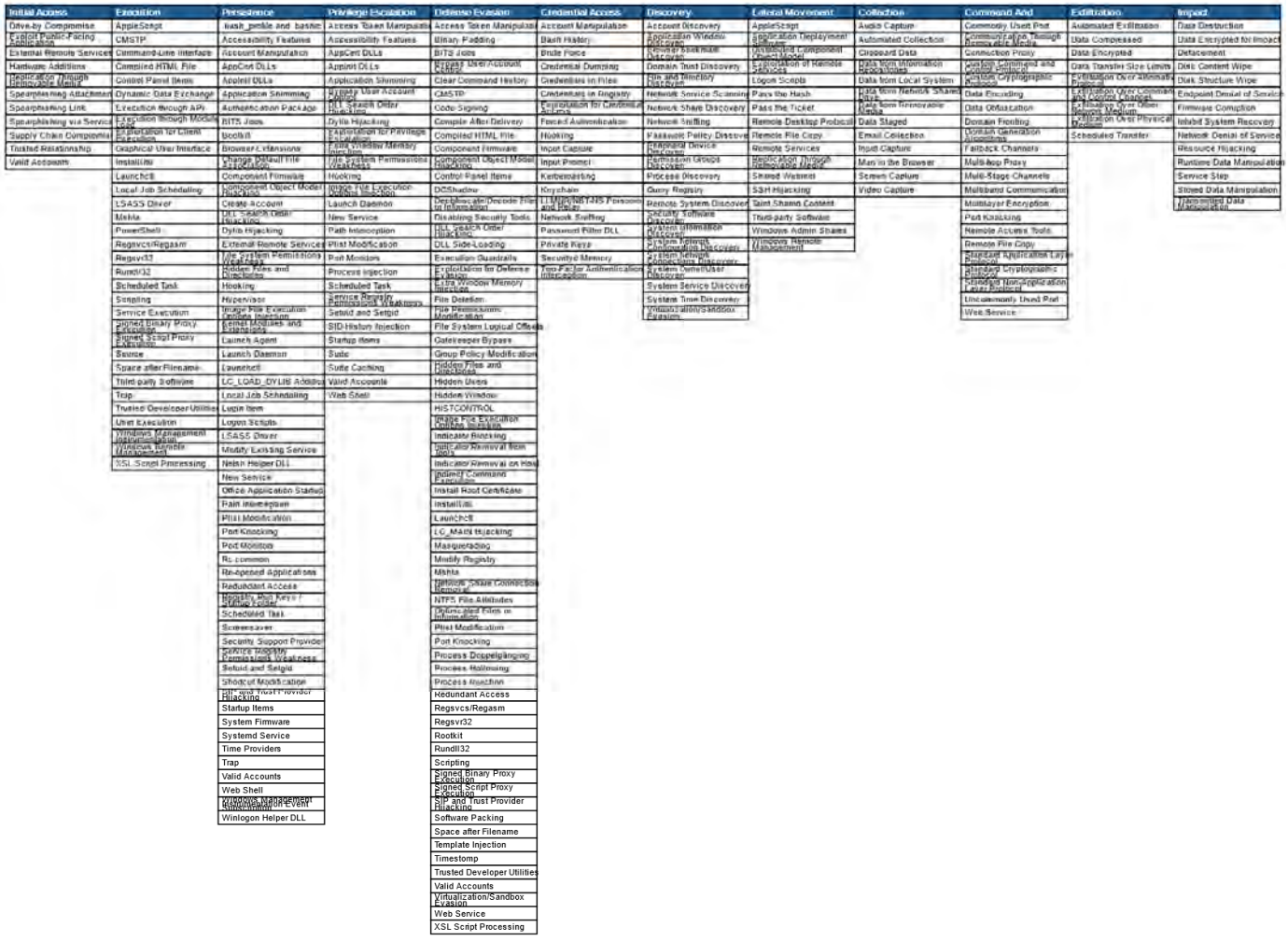


図 3-10. MITRE ATT&CK フレームワークの例.

4. アトリビューションのための分析ツール

前述のとおり、悪意のある活動に対する責任について正当な結論を導き出すには、一連のツール、技術、および分析が必要だ。ネットワーク上で観測されたアクティビティの責任を確認しようとする個人にとって、次のような種類の分析が有用である。

(1) マルウェア分析

マルウェアは、あらゆる種類の悪意のある不要なソフトウェアを指す一般的な用語だ。マルウェアは、サイバースペースにおける最も主要な犯罪の原因となっている。悪意のあるコードは、物理的なアクセスまたはネットワーク手段によってホストに侵入することができる。マルウェアベースの解析による悪意のある行為者の特定は、実際の攻撃者の特定が複雑であるため、依然として困難だ。ほとんどの場合、マルウェアベースの解析は、使用された悪意のあるソフトウェアまたはコードを特定するために利用される。また、既知の攻撃との類似性が確認された場合、マルウェアベースの解析により攻撃者の地理的な位置の特定に成功する場合もある。

(2) 静的解析

マルウェアの解析には、静的解析と動的解析がある。静的解析では、コードは実行されずに解析される。プログラムのソースコード、または逆アセンブルされたバイナリのいずれかになる。その後、悪意のあるコードを検出するために、コードを既知のシグネチャと比較する。静的解析は、難読化技術のために制約があり、解析されたコードが実際に実行されるコードでない可能性がある。

(3) 動的解析

動的解析では、仮想マシン（VM）のような制御された環境でコードを解析する。VMを使用することで、解析のために悪意のあるコードを実行すること自体が重大な懸念となるため、安全性が確保さる。動的解析では、悪意のあるコードをVM環境で直接実行できるため、静的解析手法の多くの制限を克服することができる。

(4) 類似性アトリビューション

類似性ベースのアトリビューションにより、悪意のあるイベントで使用されたマルウェアは、以前の攻撃で使用されたマルウェアと比較することができる。例えば、Kaspersky Labのリサーチャーである Kurt Baumgartner氏は、2014年のソニーへの侵入と、一般的に北朝鮮が関与したとされる他の事件との間に、いくつかの類似点があることを指摘する。Baumgartner 氏は、攻撃者は、「Destover」と呼ばれる破壊的なワイパー型マルウェアを展開し、全社的にハードディスクの上書きを行うことで痕跡を消したことを指摘する。また、「同じマルウェアが、韓国を標的としたDarkSeoul攻撃で使用されたと報告されており、これは同国の北の隣国によるものとされている」とも述べている。類似性ベースのアトリビューションの大きな限界は、以前に知られていたマルウェアとの類似性が、必ずしも以前にアトリビューションされた

攻撃者の攻撃であるとは限らないということだ。これは、以前に使用されたマルウェアのシグネチャを盗用またはコピーして、攻撃のアトリビューションを誤らせることも可能なためだ。さらに、多くの悪意ある攻撃者は、市販のソフトウェア（COTS）を利用することが知られており、その起源をさらに難解なものにしている。

(5) 間接的なアトリビューション方法

敵対者は、マルウェアのコードを難読化したり、偽造または盗難されたIDを使用したりできるため、ネットワーク・トレースバックなどの直接的なアトリビューション技術には限界がある。代替手法として、間接的なアトリビューション技術を検討する必要がある。特に、複数のコンピュータを標的とした多段攻撃や犯罪に当てはまる。間接的帰属とは、攻撃者の行動に関する統計的モデルを使用して、悪意のあるサイバー事象（または犯罪）を攻撃者（または犯罪者）に帰属させるプロセスだ。これらの行動モデルは、文体、ソーシャルネットワーク分析、コーディングの類似性など、さまざまな属性に基づいて構築される。これらの特性は互いに関連付けられ、悪意のある行為者のプロファイルを生成するために使用できる。間接的アトリビューションでは、ニューラルネットワーク、遺伝的アルゴリズム、サポートベクターマシンなどの技術を組み込んで、犯罪者プロファイルを生成できる可能性がある。しかし、脅威となる行為者の正確なプロファイルを生成するためには、広範なデータを利用できることが必要だ。

(6) 機械学習技術

機械学習技術は、サイバー犯罪のアトリビューション問題を解決するために、悪意のあるソースを特定するために使用することができる。このような技術は、長期間にわたってネットワークログを収集し、それを分析して、悪意のある活動に関与しているIPソースの集合を特定することに依存している。分析は、クラスタリング、ニューラルネットワーク、サポートベクターマシンなど、さまざまな機械学習技術によって行うことができる。

(7) 行動分析

Dacierらは、クラスタリング技術を適用して、信頼できるIPと悪意のあるIPのソースを特定した。この情報は、サイバー犯罪の発生源を特定するために適用された。行動分析は、悪意のあるソースを特定する上で効率的だが、膨大な量のデータを利用できることに依存する。そのため、他の手法と組み合わせて使用されることも少なくない。例えば、IPアドレスクラスタリングの場合、ハニーポットやウェブサーバーなど、さまざまなソースからログを収集することが可能だ。このような手法の大きな制約として、スプーフィングや匿名化手法の存在により、マルウェアの発生源の信憑性が低くなってしまうことが挙げられる。

(8) 遺伝的アルゴリズム

遺伝的アルゴリズムも、マルウェアのアトリビューションに使用されている。この手法では、マルウェアの遺伝学、進化の過程、およびその特性を利用して、攻撃者の出自を特定し、将来の攻撃の特性を予測する。さらに、攻撃の意図も考慮し、包括的なシステムを構築している。行動解析や機能解析を用いるこ

とで、マルウェアの出所や機能、系統の特徴など、いくつかの機能を特定することができる。しかし、遺伝子解析は、マルウェアの特徴を把握する必要があるため、簡単にはいかない。

(9) ニューラルネットワーク

ニューラルネットワークに基づく手法も、作者の特定に使用されている。この手法には、電子メールなどの文書の実際の作成者を特定することも含まれる。電子メールのアトリビューションは、スパム、フィッシング、サイバーテロに関連するサイバー犯罪に必要とされる。サポートベクターマシンやニューラルネットワークなどの技術を用いることで、異なる文体を識別してクラスタリングし、電子メールの作成者を特定することができる。つまり、電子メールのような文書が特定の人物に由来すると断定することはできない。さらに、電子メールは複製される可能性があり、アトリビューションを決定的なものにすることはできない。

(10)ソーシャルネットワーク

ソーシャルネットワークの準識別子（QID）を利用することによってもアトリビューションを試みることができる。QID（性別や郵便番号など）は、公共データセットから何らかの情報を明らかにするための識別子である。QIDは一意な識別子ではないが、他のQIDと組み合わせることで一意な識別子を作成することができる。ソーシャルネットワークは大規模なネットワークで構成されているため、ソーシャルネットワークからの膨大なデータセットを活用し、サイバー攻撃を悪意のあるサイバー行為者に正確にアトリビューションするためには、膨大なデータと分析が必要となる。さらに、この手法の重大な懸念は、ハッカーが偽の識別子を使用して不正な目的を達成することができることだ。

間接的アトリビューション技術を強調する学術研究論文は数多くあるが、それらはシミュレーションされた事象に依存しており、現実の事象に効果的に適用されたことはない。また、これらの技術を有効に活用するためには、大量のデータが必要であり、現在までのところ、この量は容易に入手できないことに注意する必要がある。マルウェアや悪意のあるサイバーイベントの検出、特定、アトリビューションを支援するための機械学習（ML）や人工知能（AI）の活用など、高度な技術を論じた研究論文があるものの、これらの研究のほとんどは、限られたデータと現実のサイバー運用に熟練していない人材がいるアカデミックな環境で行われていることが問題である。ML、AI、ニューラルネットワークの使用に関する研究は今後も継続され、さらにデータが利用可能になれば、これらの技術が悪意のあるサイバーイベントの検出、防止、帰属の強化を支援することが期待される。

以下の表3-11は、これらの手法の概要、手法の簡単な説明、および各手法の可能な制限を示したものである。

表3-11．アトリビューション手法の概要.[11]

アトリビューション技術		説明	制限
デジタルフォレンジック			
ストレージベース	静的データ	ディスクファイルを、犯罪行為を検索するために使用	ストレージ容量の増加に伴い、大容量ディスクの分析にはコストがかかる
RAMベース	動的データ	RAMの中身を解析し、マルウェアの有無を確認	プログラム間でRAMの内容を読み出す必要があるため、費用がかかる
トレースバックとロギング偽装		ネットワークパケットをマークし、中間ルーターまでさかのぼって追跡	大規模な導入と実行が難しい
		ハニーポットやシンクホールを使って犯人を欺き、犯行パターンを分析	収集された情報は、完全なアトリビューションにつながらない場合がある
マルウェアに基づくアトリビューション			
静的解析		プログラムコードを実行することなく解析	検査で結論が出ない場合がある。コードの難読化により、攻撃者は解析結果を欺くことができる
動的解析		仮想化環境での実行によるコードの検査	攻撃者は、コードが仮想環境上で実行されているかどうかを検出することができる。コードの難読化により、攻撃者は解析を欺くことができる
コード類似性		マルウェアの類似性を確認	この方法は、過去に知られていたサイバー犯罪と類似していることが判明した場合にのみ有効。また、マルウェアが盗用・複製されている可能性もあるため、類似しているからといって、必ずしも決定的なアトリビューションにつながるとは限らない
リバースエンジニアリング		リバースエンジニアリングプロセスによるマルウェアの特定	これは進化している技術である。さらなる発展が必要
間接的アトリビューション			
振る舞い分析	機械学習にもとづくアトリビューション	犯罪者、攻撃者、侵入者の行動をクラスター化し、先行する特徴を特定	膨大な量のデータが必要。なりすましや匿名化技術により、マルウェアの発信元の信頼性が低くなる可能性がある
遺伝的アルゴリズム		マルウェアの遺伝や起源などの特徴を把握することで、犯罪者の特定につながる	マルウェアの遺伝子情報を収集することは自明ではない
ニューラルネットワーク		サポートベクターマシンやニューラルネットワークを利用して、メールや文書の作成者を特定	文書や電子メールの作成者のアトリビューションに限定した技術
ソーシャルネットワーク		ソーシャルネットワークを通じて構築される、サイバー犯罪者のプロフィール	サイバー犯罪者は、ソーシャルネットワーク上で偽の情報を使用することがある。推測される情報量が限定される場合がある
地政学的なリンク		政治的なシナリオは、アトリビューションの改善につながる可能性があるよう検討	アトリビューションは疑わしい

5.　脅威インテリジェンス・プラットフォーム

脅威インテリジェンス・プラットフォーム（TIP）は、複数のソースとフォーマット（通常は様々な脅威インテリジェンス・フィード）から脅威インテリジェンス・データを収集、集約、整理する。TIPを使用することで、セキュリティおよび脅威インテリジェンスチームは、脅威インテリジェンス・データを他の関係者やセキュリティシステムと容易に共有することができる。TIPは、Software-as-a-Service (SaaS) またはオンプレミスソリューションとして導入することができる。

TIPは、技術、インフラ、マルウェア、意図といった属性指標と、外部ソースからの指標を提供するレポートをアナリストに提供する。これらの指標は、IOC（indicators of compromise）と同じではなく、アトリビューションを決定するために使用される指標であることに留意が必要だ。TIPの目標は、アナリストが技術的なデータ（TTPや観測値など）と非技術的な情報（帰属の示唆、被害者像など）を活用できる包括的なプラットフォームを構築することであり、各情報間のリンク、最初と最後の目撃日、信頼度などの機能を使って、それぞれの情報を主要ソース（レポート、MISPイベントなど）にリンクする。調査中に収集されるフォレンジックやインテリジェンスの多様な性質を考えると、TIPは悪意のあるイベントの帰

[11] Security and Communication Networks, Vol 8, Issue 14, 2015.

属を得ることを目的とした取り組みを支援する重要なツールであると言える。

これらのプラットフォームは、特定の組織や団体の内部でのみ使用される場合もあれば、政府機関や民間団体が提供し、より大規模なデータのコレクションや、処理・分析されたインテリジェンスにアクセスできる場合もある。プラットフォームは、分析されたマルウェア・サンプルに対する IOC の交換を提供する場合もある。また、個人対個人、組織対組織の共有モデルを反映させることもできる。プラットフォームは、同じ事件や事象に取り組んでいる異なる個人に情報を引き渡すことを可能にする。さらに、データのエンリッチメントや、センサーからの「イベント」の自動追加も可能だ。

オープンソースの脅威情報プラットフォームの一例として、マルウェア情報共有プラットフォーム（MISP）がある。このプラットフォームは、標的型攻撃、脅威情報、金融詐欺情報、脆弱性情報、あるいはテロ対策情報などにおける侵害指標の収集、共有、保管、関連付けに使用されている。

分析エンジンとサイバー脅威データベースを組み合わせたWebベースのツール Collaborative Research into Threats (CRITs) は、攻撃データやマルウェアのリポジトリとして機能するだけでなく、マルウェア分析、マルウェアの関連付け、データのターゲティングなどを行うための強力なプラットフォームとしてアナリストに提供されている。また、これらの分析や相関関係をCRITs内に保存し、活用することができる。CRITsは、サイバー脅威の情報を構造化するために、シンプルでありながら非常に有用な階層構造を採用している。この構造により、アナリストはメタデータを「ピボット」して、これまで知られていなかった関連コンテンツを発見する力を得ることができる。元々、MITREのシステムを保護する方法の研究から開発されたCRITsは、単一の、しばしば異種の攻撃から集められたサイバー脅威情報をまとめ、分析と情報共有を容易にするためにこのデータを標準化されたフォーマットで表現する。この情報は、将来の攻撃から組織のネットワークを保護するために使用することができる。

また、ThreatConnect、Threat Quotient、Anomali、Threatvineなどが提供する市販のオプションもある。例えば、英国のCiSPは、Threatvineをプラットフォームとして使用している。日本のサイバーセキュリティ情報共有プラットフォーム（JISP）は、富士通が運営するプラットフォームを使用している。

どのプラットフォームが良いかという質問に対する答えは、「組織の特定のニーズに依存する」ということだ。それぞれのプラットフォームは、異なる方法で動作し、異なる強みを持っている。ほとんどのプラットフォームは、脅威データを分析し、共有する機能を備えている。これらのツールは、ネットワーク上の脅威のシグネチャを特定し、その情報を他の設備に中継したり、脅威のフィードから新しい危険に関する情報を取得したりすることができる。一部のプラットフォームでは、データをトリアージし、脅威が特定されたときに警告を発することができる。これらのプラットフォームは、正当な脅威が発生した場合にのみアラートを送信し、セキュリティレベルを向上させずに防御者の注意をそらすような通知でユーザーを圧倒することを回避する。プラットフォームによっては、リスク・スコアを割り当てて、セキュリティ・チームが対応に優先順位を付けられるようにするものもある。

6. ネーミングスキーマの意義

脅威インテリジェンスとデータの商用ベンダーは、悪意のあるサイバー行為者やグループを特定し、その属性を明らかにするために命名規則を利用している。混乱しやすいのは、特定した脅威グループや行為

者について、ベンダーごとに異なる命名規則があることだ。すべての商用サイバーセキュリティ・ベンダーは、独自の遠隔測定、データ、標準、手順、および信頼レベルを持っている。このように、ベンダーはそれぞれ異なる命名規則に従っているため、同じサイバー脅威グループやアクターに対して異なる名称を付けている可能性があることを認識することが重要だ。例えば、CrowdStrikeは動物（例：Wizard Spider）、Microsoftは化学元素（例：NOBELIUM）、Mandiantは数字（例：APT38）を使用している。1つの脅威グループが8つの異なる脅威組織名で呼ばれる場合もある。これは、サイバー脅威インテリジェンスアナリストにとって混乱を招く可能性があるため、脅威行為者を追跡調査する際には、様々な名称（エイリアス）を付与したリストがあると便利である。

また、政府機関は、アナリストがアトリビューション情報やCTI情報を追跡・整理する際に役立つよう、脅威行為者グループやキャンペーンに具体的な名称を付与することにしている。多くの場合、政府機関が使用する命名規則は本質的に機密であるため、公開されることはない。このため、新米のサイバーセキュリティ・アナリストはさらに混乱する可能性がある。

7. 情報発信

情報共有とは、「参加者（人、プロセス、システム）が情報を利用できるようにすること」と定義される。情報共有には、ある参加者が他の参加者が保有または作成した情報を活用するための文化的、管理的、技術的な行動が含まれる。共有は、組織内部で行われることもあれば、情報共有を目的とした複数の組織を通じて外部で行われることもある。

重要インフラ（運用に不可欠なハードウェアやソフトウェアを含む）の大半は民間所有であるため、官民のパートナーシップは国家を守るために必要な情報を共有する上で非常に重要である。しかし、企業は商業用のプライベートなネットワークへの洞察を政府機関に提供することに消極的な場合が多い。一方、政府は、州や地方自治体が管理する商業インフラや重要なシステムのサイバーセキュリティ保護に関与することをためらっている。

CTI 情報、特にアトリビューションに関連する情報には、機密性が高く、拡散すると機密性の高い情報源や方法を開示することになる政府情報が含まれることがある。さらに、その情報は、組織（知的財産、欠陥、コンプライアンス違反に関する情報など）や個人（個人情報など）にとって機密性の高いものである可能性もある。また、組織によっては、組織名などの所属情報を共有することに抵抗がある場合もある。組織によっては、未解決のリスクがより広く知られること、または、そのようなリスクが発生した場合に不利益を被ることを懸念し、CI 情報を共有する際に組織名などの所属情報を開示しない場合がある。組織によっては、未解決のリスクをより広く知られることになる、あるいはレピュテーションにマイナスの影響を与えるなどの懸念から、情報共有の際に組織名などの所属情報を明かさない場合もある。

8. 分類

アトリビューション情報の普及は慎重に検討され、管理または分類のいずれかに分類される必要がある。選択された利害関係者への普及は、情報がどのようにさらに普及または利用されるかを指定するための管理マークとともに検討されるべきである。機密性の高い CTI を管理マークを付けて、一部の利用者のみに配布することは可能である。

データ分類または情報分類は、組織の情報を重要なカテゴリーに分類して、機密情報を確実に保護するプロセスである。例えば、悪意のある脅威者に関するサイバーセキュリティの機密データは、セキュリティ担当者以外がアクセスできるファイルと一緒に保管すべきでない。代わりに、機密性の高いサイバーデータと情報を扱う権利を持つ個人のみがアクセスできる別のフォルダに保管する必要がある。

政府機関では、機密性の高い政府の計画や政策、財務記録、コンピュータシステム内の従業員データなど、毎日機密性の高いデータを取り扱っている。しかし、すべてのデータが同じように重要なわけではなく、一部のデータは他のデータよりも保護が必要になる。このような機密性の高い重要な情報は、セキュリティ上の脅威に対する脆弱性から保護する必要があり、そのために情報の分類が重要になる。情報分類は、どの情報が特別な保護を必要とするかを判断し、データをどのようにラベル付けし、分類するかを決めるのに役立つ。

情報の分類は、データを整理し、アクセスしやすく、安全に保つための基盤として機能する。大量、多様、かつ関連性のある情報を分類するのは、複雑な作業だ。機密性の高い CTI は、不用意な公開から保護し、さらに重要なこととして敵対者にアクセスを許さないようにすることが重要である。悪意のあるサイバー行為者がセキュリティ企業や政府機関のセキュリティ担当者を標的にした例もある。特に、敵対者の情報または分析を含むデータでは、このことが非常に重要となる。セキュリティ組織のためによく計画されたデータ分類システムは、機密情報の操作と追跡を容易にし、さらにデータの所在と検索を容易にする。
データの暗号化、強力なファイアウォールを備えた安全なサーバーへのデータ保存、データ保護基準の遵守は、外部の脅威から守るために非常に有効だ。さらに、意図的なデータ盗難や偶発的なデータ漏洩など、内部にも同様に危険な脅威が存在する可能性がある。したがって、情報を制限し、脅威を防止することが非常に重要である。

9. アトリビューション強化型アクティブ・サイバー・ディフェンス

前述したように、ACD の技術を展開するためには、責任の所在が重要である。このセクションでは、帰属の決定がどのように ACD 活動の効果を高めるかについて例を挙げて説明する。

(1) 脅威ハンティング

多くの企業は、サイバー脅威ハンティングが、最新のセキュリティオペレーションセンターと成熟したサイバーディフェンス運用の次のステップであることを認識している。脅威ハンティングとは、既存のセキュリティソリューションを回避する高度な脅威を検出し隔離するために、ネットワークを積極的かつ反復的に探索するプロセスである。ハンティングは、SIEM や SOAR などの自動化されたシステムだけに依存するのではなく、手動または機械による支援技術で構成される。アラーティングは重要ではあるものの、成熟したサイバーセキュリティ・プログラムの唯一の焦点ではない。効果的な脅威ハンティングのプログラムを運用するためには、敵対者の行動に特化した充実した TTP と情報が必要だ。サイバー脅威ハンター／アナリストは、攻撃者の行動、手法、目標について可能な限り多くの情報を収集し、すでに持っている情報を充実させる。また、収集したデータを分析し、組織のセキュリティ環境の傾向を把握し、現在の脆弱性を排除し、将来のセキュリティ強化のための予測を立てる。

(2) 敵対的エミュレーション

アトリビューションデータ、特に脅威のプロファイルが大いに活用できるもう 1 つの領域は、一般に敵対的エミュレーションと呼ばれるものだ。敵対的エミュレーションは、ある組織を狙うことが知られている攻撃者の既知の TTP と手法を模倣した、一連の非常に特殊なレッドチーム活動として説明されることがよくある。この種の対策の目的は、組織がこの種の攻撃を検知できるようにすること、そしておそらくより重要なのは、セキュリティアナリストと既存のプロセスがこの種の攻撃を効果的に識別、トリアージ、対応できるようにすることの 2 つである。

ネットワークの脅威シミュレーションと侵入テストを効果的に実施するには、敵の TTP に関する情報と敵の知識が不可欠である。さらに、脅威のモデル化と攻撃シミュレーションのほとんどは手作業で行われており、リソースが集中し、熟練した人材が必要で、ミスが発生しやすいという問題がある。ネットワークベースの攻撃シミュレーションを自動化するために、MITRE ATT&CK フレームワークに基づいて、戦術レベルでの敵のモデリングに焦点を当てた自動敵対的エミュレーション・テストベッドが提案されている。CALDERA は、敵対者に能力を関連付け、敵対者の作戦を実行することにより、敵対者の成功に対するネットワークの感受性の自動評価を可能にする。敵対者のエミュレーションは、特定の敵対者の戦術、技術、行動をエミュレートするプロセスとなる。

敵対的エミュレーションの目的は、特定の敵対者の技術や攻撃に対して、組織がどの程度回復力があるかを評価し、改善することである。敵対者の行動は、TTP を使用して分類される。敵対者の TTP は、特定の敵対者がどのように活動するかの概要を示すために使用される。したがって、敵対者の行動に関する情報が多ければ多いほど、敵対者のエミュレーションの精度を高めることができる。

CALDERA はクライアント・サーバー方式を採用しており、サーバーがエージェント（クライアント）をセットアップし、オペレーションを開始するために使用される。あらゆる規模のセキュリティ・チームにとって、敵対的エミュレーション演習の有用性は、いくら強調してもし過ぎることはない。

- レッド・チーム：敵対的エミュレーション演習は、レッド・チームにとって不可欠だ。これは、レッド・チームが攻撃側の仕事をより効果的に遂行できるようになることが主な理由である。敵対的エミュレーションを実施することで、レッド・チームは、脅威がネットワークに侵入する際に使用する実際の活動を試すことに集中することができる。
- ブルー・チーム：敵対的エミュレーションを行うことで、ブルー・チームは是正措置に集中し、最も必要とされる場所で作業を行うことができる。敵対的エミュレーション演習を実施することで、ネットワークの防御のギャップを明確に指摘することができ、組織はギャップや最大の脆弱性をより速いペースで特定し、解決することができる。
- パープル・チーム：敵対的エミュレーションは、組織のセキュリティ・チーム内でパープル・チームの環境を確立するために不可欠な要素だ。敵対的エミュレーション／シミュレーションがレッド・チームとブルー・チームの橋渡し役となり、両チームがより効果的に、より緊密に連携し、組織全体のセキュリティ態勢を強化することができるからである。

すべての敵対的エミュレーション演習が「パープル・チーミング」と呼ばれるわけではありませんが、パ

ープル・チーミングでは、敵対的エミュレーション演習を相当量実施し、両チームの努力を結集して、通常では不可能な可視化と検知を可能とする。

(3) 敵対的エンゲージメント

熟練したサイバー防衛者が CTI とアトリビューション情報に大きく依存して利用する追加のサイバー防衛活動は、敵対者の関与だ。敵対的エンゲージメントは、サイバー防衛者が攻撃者の悪意のあるサイバー操作のコストを引き上げ、その価値を下げる機会を提供する。

MITRE Engage は MITRE ATT&CK フレームワークを取り入れた敵対的エンゲージを実施するためのフレームワークである。MITRE Engage Matrix は、MITRE Engage フレームワークの構成要素であり、敵対者の関与、欺瞞、および拒否の活動について議論し、計画するために利用される。Engage は、実社会で観察される敵対者の行動から情報を得て、戦略的なサイバー成果を推進することを目的としている。Engage は、民間企業や政府が敵対的エンゲージメント戦略や技術の利用を計画・実行する際に役立つよう作成された。敵対的エンゲージメントの主な目的は、ネットワーク上の敵対者を明らかにすること、敵対者とその TTP についてより詳しく知るための情報を引き出すこと、敵対者の活動能力に影響を与えること、のいずれかの組み合わせとなる。敵対的エンゲージメントは、防御側にとってツールのデモンストレーション、仮説の検証、脅威モデルの改善などの機会を提供するが、これら全ては敵対者に悪影響を与えるという付加的なメリットもある。

(4) MITRE ATT&CK

ATT&CK マトリクスは、攻撃者や競合他社を演じるレッドチーム、脅威ハンター、セキュリティ製品開発エンジニア、脅威インテリジェンスチーム、リスク管理専門家など、幅広い IT およびセキュリティ専門家によって活用されている。

レッドチームは、MITRE ATT&CK フレームワークを青写真として使用し、企業のシステムやデバイスの攻撃対象領域や脆弱性を明らかにするとともに、悪意のある脅威行為者について貴重な洞察を得るのに役立てることができる。これには、攻撃者がどのようにアクセスしたのか、影響を受けるネットワーク内でどのように移動しているのか、検出を回避するためにどのような方法が用いられているのかが含まれる。これにより、組織は TTP を他の攻撃事象と関連付けることができ、攻撃者をより深く理解し、さらに潜在的に特定することができる。

脅威ハンターは、ATT&CK フレームワークを使用して、攻撃者が防御に対して使用している特定のテクニック間の相関関係を見つけ、エンドポイントおよびネットワーク境界全体の両方で、防御を標的とした攻撃の可視性を理解するためにフレームワークを使用しる。

セキュリティプラットフォームの開発者やエンジニアは、自社製品の有効性を評価し、これまで知られていなかった弱点を発見し、サイバー攻撃のライフサイクルにおいて自社製品がどのように動作するかをモデル化するツールとして MITRE ATT&CK を使用する。

10. まとめ

悪意のあるサイバー犯罪者を特定することで、政府および他の被害者は、攻撃の全体像を把握し、適切な

対応レベルに関する情報に基づいた決定を下し、将来の攻撃に対する防御を強化する最善の方法を決定することができる。アトリビューションを確定することは困難だが、不可能ではない。悪意のあるサイバー行為者のアトリビューションを決定するための単純な技術的プロセスや自動化されたソリューションは存在しない。多くの場合、この困難な作業には、情報およびデジタルフォレンジックの分析に数週間を要し、犯人を評価する必要がある。場合によっては、インシデント発生から数時間以内にアトリビューション結果を決定することも可能だが、アトリビューション結果の決定の精度と信頼度は、利用可能なデータと分析者の能力によって異なる。

悪意があるかどうかにかかわらず、あらゆる種類のサイバー操作には、アトリビューションにつながる分析をサポートする証拠が残されている。サイバーセキュリティのアナリストは、この情報を、過去の出来事や既知の悪意ある行為者の TTP に関する知識とともに使用して、これらの操作の発生源を突き止めようとする。したがって、信頼性の高いアトリビューション決定には、熟練した訓練を受けたサイバーセキュリティ・アナリストの集団が鍵となる。ソフトウェアと分析ツールは、確かに分析プロセスを支援し、充実させるが、帰属に焦点を当てた高度に熟練したサイバーセキュリティ・アナリストの中核集団がいなければ、組織のサイバーセキュリティ運用は成熟しない。

悪質なサイバー行為者はすべて、自分たちの利益を増進するための低コストなツールとしてサイバー作戦を使用している。このような行為に対する明確な影響に直面しない限り、彼らはそうし続ける。したがって、サイバー攻撃へのアトリビューションは、そのような攻撃に対する効果的な国家的対応を策定する上で重要なステップとなる。

第５節 英国のアプローチ

英国の政府通信本部（GCHQ）の一部門であるの National Cyber Security Centre (NCSC) は Active Cyber Defence プログラムは、公共および民間組織の安全を大規模に維持することを目的としている。このプログラムは「英国の大多数の人々を、大多数のサイバー攻撃による大多数の被害から、大多数の時間をかけて守る」ことを掲げており、適格な組織に対して、多くの ACD サービスを無償で提供している。

本節では ACD サービスの実装例として英国 NCSC による本プログラムを取り上げる。表 3-13 には本プログラムにおいて提供される機能の概要を示す。

表 3-13. 英国 NSCS における ACD サービス.

サービス	商品説明	対象組織
NCSCツールで実施するセルフサービスチェック		
早期警戒	NCSCが受信したイベント情報（商用フィードからのデータなど）を、組織がNCSCに監視を依頼したIPアドレスとドメイン名に基づいて相関させる。 ネットワークに対するサイバー攻撃の可能性を組織に	固定IPアドレスまたはドメイン名を持つ英国のあらゆる組織

	通知する。以下の種類のアラートを提供する。 • **インシデント通知** - 組織のシステムに対する能動的な侵害を示唆する活動。 • **ネットワーク不正使用イベント** - 組織の資産が悪意のある、または望ましくない活動に関連付けられたことを示す指標。 • **脆弱性とオープンポートの警告** - 組織のネットワーク上で実行されている脆弱なサービス、または潜在的に望ましくないアプリケーションがインターネットに公開されていることを示す。 NCSCは、参加組織の情報を直接スキャンすることはない。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/early-warning-service	
エクササイズ・イン・ア・ボックス (EIAB)	NCSCが提供するオンラインツールで、組織がサイバー攻撃への対応をテストし、練習するのに役立つ。複数の種類の演習を提供し、セットアップ、計画、実施、および演習後の活動に必要なすべてが含まれる。次のステップと関連する実施ガイダンスを特定するのに役立つカスタマイズされたレポートを受け取るには、登録が必要。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/exercise-in-a-box	任意のユーザー
メールチェック	メールセキュリティのコンプライアンスを評価するための無料プラットフォーム。ドメイン所有者が、メールドメインの悪用を特定、理解、防止するのを支援。以下のコントロールの実装をサポート。 • **電子メールのなりすまし防止制御（SPF、DKIM、DMARC）**：これらの規格は、組織のメールドメインを利用してメール受信者を騙すさまざまな攻撃（例えば、フィッシングやマルウェアのキャンペーン）を防ぐのに役立つ。 • **電子メールの機密性（TLS）**：インターネット上で	中央政府 地方自治体 分立行政機関 緊急サービス NHS 組織 アカデミア（英国のすべての学校） 慈善団体（パイロットユーザーのみ） 英国の登録社会住宅プ

	送信されるメッセージを暗号化し、プライバシーを保つ。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/mailcheck	ロバイダー ALMOs
ウェブチェック	一般的なWebの脆弱性や設定ミスをWebサイトでチェックすることで、組織がWebサイトに共通するセキュリティ上の問題を特定し、修正することを支援。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/web-check	中央政府 地方自治体 分立行政機関 緊急サービス NHS 組織 アカデミア（英国のすべての学校） 慈善団体（パイロットユーザーのみ） 英国の登録社会住宅プロバイダー ALMOs
メール・セキュリティ・チェック（BETA）	公開されている情報を見て、すでにインターネット上で犯罪者が簡単に公にしている脆弱性を特定。以下の2項目の検証をサポート。 • **メールのなりすまし対策**：サイバー犯罪者が組織からのメールを装って送信することを防止する。 • **電子メールのプライバシー**：サイバー犯罪者が転送中の組織の電子メールを傍受して読むことを困難にする。 問題が見つかった場合、NCSCは組織が何をすべきかについて、段階的なガイダンスを提供する。 詳細は以下のリンクを参照： https://emailsecuritycheck.service.ncsc.gov.uk/	任意のユーザー
各組織で導入されている検出器		
ホスト・ベースド・ケイパビリティ（HBC）	政府公用端末で使用可能なソフトウェアエージェント。NCSCが分析するための技術的なメタデータを収集するために、分析を行い、バックグラウンドで動作する。悪意のある活動を検出する。 セキュリティベースラインレポートを提供し、利用者が深	中央政府

	刻な脆弱性にさらされている場合には警告する。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/host-based-capability	
プロテクティブ・ドメイン・ネーム・サービス (PDNS)	悪意のあるコンテンツが含まれていることが分かっているドメインやIPにユーザーがアクセスすることを防ぎ、すでにネットワーク上にあるマルウェアがC2サーバーと通信することを阻止する。 内閣府が中央省庁に使用を義務付けているが、それ以外の組織でも利用可能。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/pdns	中央政府 地方自治体 分立行政機関
脆弱性の開示	脆弱性の疑いがあるものを報告するための脆弱性報告サービス。スコットランド政府に関連する脆弱性の報告や、NSCSのWebプラットフォームに特化した脆弱性の報告への追加リンクが含まれる。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/vulnerability-reporting	任意のユーザー
	脆弱性開示のベストプラクティスを採用した Vulnerability Disclosure Pilot。	中央政府
	脆弱性開示プロセスの実装について詳しく知りたいあらゆる規模の組織のための脆弱性開示ツールキット。脆弱性開示プロセスの設定に不可欠なコンポーネントが含まれている。また、検証やトリアージなど、情報開示プロセスの実施に関する追加情報も含まれている。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/vulnerability-disclosure- ツールキット	任意のユーザー
脅威の除去		
不審メール報告サービス (SERS)	不審な電子メールを一般の方が通報できるようにする。電子メールを分析し、悪意のあるサイトへのリンクが含まれていることが判明した場合、インターネットからそれらのサイトを削除し、被害の拡大を防止することを目的として	任意のユーザー

	いる。	
テイクダウンサービス	ホスティングプロバイダーと協力し、インターネットから悪意のあるサイトやインフラを削除する。サイトを削除し、攻撃用インフラをブロックすることで、攻撃者の投資収益率を低下させ、これらの攻撃が引き起こす被害を抑制することを目的とする。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/takedown-service	公共部門 (英国政府ブランドおよびサービス)
脅威の除去		
MyNCSC	ACDを含むNCSCのデジタルサービスへのシングルエントリー・ポイント。各ユーザーに最も適したコンテンツ、脆弱性、サービス、アラートを表示するよう調整され、NCSCのサービスを1つの一貫したサービスに纏める。 詳細は以下のリンクを参照： https://www.ncsc.gov.uk/information/myncsc	Webチェックとメールチェックのユーザーのみ利用可能 (今後、NCSC の他のサービスの利用者への拡充予定)

第６節 フォレンジック・分析ツールおよびリソース

一般に ACD 活動、特にアトリビューション活動は、しばしばインシデントレスポンス活動の要素になる。インシデントレスポンス（IR）ツールキットを構築する主な目的は、インシデントレスポンス計画によって指示されたインシデントレスポンス活動のライフサイクル全体を実行するためのハードウェア、ツール、ソフトウェアを揃えることである。IR を実施するには、通常のセキュリティオペレーションセンター（SOC）の業務とは異なる専用の機器が必要だ。IR の状況はプレッシャーが高く、業務に大きな影響を与える可能性があるため、事前に適切なツールを準備しておくことが重要である。

本節では、インシデント対応と分析を行うサイバーセキュリティ・アナリストと技術者をサポートするツールおよびその他のリソースをリストする。

1. ツール

(1) 敵対的エミュレーションツール

- APT SImulator: 一連のツールと出力ファイルを使用して、システムが侵害されたように見せかける Windows バッチスクリプト。
- Atomic Red Team (ART): MITRE ATT&CK フレームワークにマッピングされた、小型で移植性の高い検出テストを提供する。

- Auto TTP: 自動化された戦術技術および手順で、回帰テスト、製品評価、研究者のためのデータ生成のために複雑なシーケンスを手動で再実行する。
- Blue Team Training Toolkit (BT3): ネットワーク分析トレーニング、インシデント対応ドリル、レッドチームの活動を改善することを目的とした、防御的セキュリティトレーニング用ソフトウェア。
- Caldera: Windows エンタープライズネットワークにおいて、侵害後の敵対的な振る舞いを行う自動化された敵対者エミュレーションシステム。MITRE の Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) データベースに基づくプランニングシステムと事前設定された敵対者モデルを使って、運用中にプランを生成する。
- DumpsterFire: 反復可能で時間遅延のある分散型セキュリティイベントを構築するためのモジュール式、メニュー駆動型、クロスプラットフォームツール。ブルー・チームの訓練やセンサー/アラートマッピングのためのカスタムイベントチェーンを作成する。レッド・チームはこのツールを使って、おとりインシデント、気晴らし、ルアーを作成し、作戦を支援・拡大することができる。
- Metta: 敵対的なシミュレーションを行うための情報セキュリティ対策ツール。
- Network Flight Simulator: 悪意のあるネットワーク・トラフィックを生成するための軽量なユーティリティ。セキュリティ・チームがセキュリティ対策やネットワークの可視性を評価するのに役立つ。
- Red Team Automation (RTA): RTA は、MITRE ATT&CK をモデルとして、ブルー・チームが悪意のあるトラデクラフトに対する検出能力をテストできるように設計されたスクリプトのフレームワークを提供する。
- RedHunt-OS: 敵対者のエミュレーションと脅威のハンティングのための仮想マシン。

(2) オールインワンツール

- Belkasoft Evidence Center: ハードディスク、ドライブイメージ、メモリダンプ、iOS、Blackberry、Android のバックアップ、UFED、JTAG、チップオフダンプを分析し、複数のソースからデジタル証拠を抽出するツールキット。
- CimSweep: CIM/WMI ベースのツールで、Windows のすべてのバージョンでインシデントレスポンスとハンティングのオペレーションをリモートで実行できるようにするツール群。
- CIRTkit: インシデントレスポンスとフォレンジック調査プロセスの継続的な統一を支援するためのツールとフレームワークのコレクション。
- Cyber Triage: エンドポイントデータをリモートで収集・分析し、侵害の有無を判断するためのツール。エージェントレスで、使いやすさと自動化を重視しているため、インフラを大きく変更することなく、またフォレンジックの専門家チームを編成することなく、インシデントに対応することができる。その結果は、システムを消去すべきか、さらに調査すべきかを決定するために使用される。
- Doorman: osquery フリートマネージャで、ノードから取得した osquery コンフィギュレーションをリモートで管理することができる。osquery の TLS 設定、ロガー、分散型読み取り/書き込みエンド

ポイントを活用し、管理者は最小限のオーバーヘッドと侵入でデバイスのフリート全体を可視化することができる。

- Falcon Orchestrator: ワークフローの自動化、ケース管理、セキュリティ対応機能を提供する拡張可能な Windows ベースのアプリケーション。
- Flare: マルウェア解析、インシデントレスポンス、ペネトレーション・テストのための、完全にカスタマイズ可能な Windows ベースのセキュリティ・ディストリビューション。
- Fleetdm: セキュリティ専門家向けにカスタマイズされたホストモニタリングプラットフォーム。Facebook の osquery プロジェクトを活用し、Fleetdm は継続的なアップデート、機能、大きな疑問への迅速な回答を提供する。
- GRR Rapid Response: リモート・ライブ・フォレンジックに特化したインシデントレスポンス・フレームワーク。ターゲットシステムにインストールする Python エージェント（クライアント）と、エージェントを管理し、エージェントと対話できる Python サーバー基盤で構成されている。PowerGRR は Python API クライアントに加え、Windows、Linux、macOS で動作する PowerShell の API クライアントライブラリを提供し、GRR の自動化とスクリプティングを実現する。
- IRIS: インシデント対応アナリストが技術レベルで調査を共有するためのウェブ・コラボレーション・プラットフォーム。
- Kuiper: デジタル・フォレンジック調査プラットフォーム
- Limacharlie: クロスプラットフォーム（Windows、OSX、Linux、Android、iOS）の低レベル環境を提供し、機能拡張のための追加モジュールを管理し、メモリにプッシュするための小さなプロジェクトの集合体で構成されたエンドポイント・セキュリティプラットフォーム。
- Matano: AWS 上のオープンソース・サーバーレス・セキュリティレイク・プラットフォーム。
- MozDef: セキュリティインシデントの処理プロセスを自動化し、インシデントハンドラーの活動をリアルタイムに促進する。
- MutableSecurity: サイバーセキュリティ・ソリューションのセットアップ、設定、使用を自動化するための CLI プログラム。
- NightHawk: ElasticSearch をバックエンドとして使用した、非同期フォレンジックデータ提示のためのアプリケーション。Redline のコレクションを取り込むように設計されている。
- Open Computer Forensics Architecture: オープンソースの分散型コンピュータ・フォレンジック・フレームワーク。このフレームワークは Linux プラットフォーム上に構築され、データの保存に postgreSQL データベースを使用している。
- osquery: SQL ライクなクエリ言語を使って、Linux や macOS のインフラに関する質問をすることができるようにする。提供されるインシデント・レスポンス・パックは、ユーザーが侵害を検知し、対応するのに役立つ。
- Redline: メモリやファイルの解析、脅威評価プロファイルの作成を通じて、悪意のある活動の兆候を特定するためのホスト調査機能を提供する。
- SOC Multi-tool: セキュリティ専門家のための調査を合理化する強力なブラウザ拡張機能。
- The Sleuth Kit & Autopsy: コンピュータのフォレンジック分析を支援する Unix および Windows

ベースのツール。ディスクイメージの解析、ファイルシステムの詳細な解析、その他の作業を支援するツールが含まれている。

- TheHive: SOC、CSIRT、CERT、およびセキュリティインシデントに対処する情報セキュリティ専門家のために設計された、拡張性の高い 3-in-1 のオープンソースかつ無料のソリューション。
- Velociraptor: エンドポイント可視化・収集ツール。
- X-Ways Forensics: ディスクのクローニングとイメージングを行うフォレンジック・ツール。削除されたファイルの検索やディスクの解析に利用できる。
- Zentral: osquery のエンドポイントインベントリ機能と、柔軟な通知・アクションフレームワークを組み合わせたツール。これにより、ユーザーは OSX および Linux クライアント上の変更を特定し、対応することができる。

(3) ディスクイメージ作成ツール

- AccessData FTK Imager:あらゆる種類のディスクから復元可能なデータをプレビューすることを主な目的としたフォレンジックツール。FTK Imager は、32 ビットおよび 64 ビットシステム上のライブメモリとページング・ファイルを取得することもできる。
- Bitscout Vitaly: Kamluk 氏による Bitscout は、完全に信頼できるカスタマイズ可能な LiveCD/LiveUSB を構築するのに役立つ。リモートデジタルフォレンジック（または他のタスク）に使用するイメージを作成する。これは、システムの所有者が透過的に監視でき、フォレンジック的に健全で、カスタマイズ可能で、コンパクトであることを意図している。
- GetData Forensic Imager: 一般的なフォレンジックファイル形式のフォレンジック・イメージを取得、変換、または検証する Windows ベースのプログラム。
- Guymager: Linux でメディアを取得するためのフリーのフォレンジック・イメージャー。
- Magnet ACQUIRE: Magnet Forensics の ACQUIRE は、Windows、Linux、OSX、モバイル OS 上で様々なタイプのディスク取得を可能にする。

(4) 証拠収集ツール

- artifactcollector: artifactcollector プロジェクトは、システム上のフォレンジック・アーチティファクトを収集するソフトウェアを提供している。
- bulk_extractor: ディスクイメージ、ファイル、またはファイルのディレクトリーをスキャンし、ファイルシステムまたはファイルシステム構造を解析せずに有用な情報を抽出するコンピューター・フォレンジック・ツール。ファイルシステム構造を無視するため、このプログラムは速度と完全性の点で際立っている。
- Cold Disk Quick Response: フォレンジック・イメージ・ファイル（dd、E01、vmdk など）を迅速に解析し、9 つのレポートを出力するための合理的なパーサー・リスト。
- CyLR: CyLR ツールは、NTFS ファイルシステムを持つホストからフォレンジック・アーティファクトを迅速かつ安全に収集し、ホストへの影響を最小限に抑える。
- Forensic Artifacts: デジタル・フォレンジック・アーティファクト・リポジトリ。

- ir-rescue: Windows バッチスクリプトと Unix Bash スクリプトで、インシデントレスポンス時にホストのフォレンジックデータを包括的に収集する。
- Live Response Collection: Windows、OSX、*nix ベースの OS から揮発性データを収集する自動化されたツール。
- Margarita Shotgun: リモートメモリ取得を並列化するためのコマンドラインユーティリティ（Amazon EC2 インスタンスの有無にかかわらず動作する）。
- UAC: UAC (Unix-like Artifacts Collector) は、インシデントレスポンス用のライブレスポンス収集スクリプトで、ネイティブバイナリとツールを利用して AIX, Android, ESXi, FreeBSD, Linux, macOS, NetBSD, NetScaler, OpenBSD, Solaris システムの成果物を自動的に収集することができる。

(5) インシデント管理ツール

- Catalyst: アラート処理とインシデント対応プロセスの自動化を支援する無償の SOAR システム。
- CyberCPR: センシティブなインシデントを処理しながら GDPR のコンプライアンスをサポートする Need-to-Know が組み込まれたコミュニティおよび商用のインシデント管理ツール。
- Cyphon: Cyphon は、単一のプラットフォームを通じて多数の関連タスクを合理化することで、インシデント管理に伴う頭痛の種を解消する。Cyphon は、イベントの受信、処理、トリアージを行い、データの集約、アラートのバンドルと優先順位付け、アナリストによるインシデントの調査と文書化を可能にする、分析ワークフローの包括的なソリューションを提供する。
- CORTEX XSOAR: Palo Alto Security のオーケストレーション、自動化、および対応プラットフォームで、インシデント・ライフサイクルを完全に管理し、自動化を強化するために多くの統合機能を備えている。
- DFTimewolf: フォレンジックの収集、処理、データ・エクスポートをオーケストレーションするためのフレームワーク。
- DFIRTrack: インシデントレスポンス追跡アプリケーションで、ケースやタスクを通じて、影響を受けるシステムや成果物が多数ある 1 つまたは複数のインシデントを処理する。
- Fast Incident Response (FIR): 敏捷性とスピードを念頭に置いて設計されたサイバーセキュリティインシデント管理プラットフォーム。サイバーセキュリティインシデントの作成、追跡、報告を簡単に行うことができ、CSIRT、CERT、SOC に有用。
- RTIR: Request Tracker for Incident Response (RTIR)。コンピューター・セキュリティ・チームを対象としたオープンソースのインシデント処理システム。世界中の 10 以上の CERT と CSIRT チームと一緒に開発された。RTIR は Request Tracker の全機能を基に構築されている。
- Sandia Cyber Omni Tracker (SCOT): 柔軟性と使いやすさを重視したインシデントレスポンスのコラボレーションとナレッジキャプチャツール。ユーザーに負担をかけることなく、インシデントレスポンス・プロセスに付加価値を与えることを目標としている。
- Shuffle: アクセシビリティを重視した汎用的なセキュリティ自動化プラットフォーム。
- threat note: セキュリティ研究者が研究に関連する指標を登録・取得できる軽量な調査ノート。

- Zenduty: エンドツーエンドのインシデント警告、オンコール管理、対応オーケストレーションを提供する新しいインシデント管理プラットフォーム。インシデント管理のライフサイクルをよりコントロールし、自動化することを可能にする。

(6) ログ解析ツール

- AppCompatProcessor: AppCompatProcessor は、企業全体の AppCompat/AmCache データから、従来のスタッキングやグレッピングの技術を超えた付加価値を抽出するために設計されている。
- APT Hunter: APT-Hunter は、Windows イベントログのための脅威ハンティングツール。
- Chainsaw: Chainsaw は、Windows イベントログ内の脅威を迅速に特定するための強力な「ファーストレスポンス」機能を提供する。
- Event Log Explorer: ログファイルやその他のデータを迅速に分析するために開発されたツール。
- Event Log Observer: Microsoft Windows のイベントログに記録されたイベントを、GUI ツールで表示、分析、監視することができる。
- Hayabusa: Windows イベントログの高速フォレンジック・タイムライン生成ツール。
- Kaspersky CyberTrace: 脅威データフィードを SIEM ソリューションと統合する脅威インテリジェンス融合・分析ツール。既存のセキュリティ運用のワークフローにおいて、脅威インテリジェンスをセキュリティ監視やインシデントレポート（IR）活動に即座に活用することができる。
- Log Parser Lizard: サーバーログ、Windows イベント、ファイルシステム、Active Directory、log4net ログ、カンマ/タブ区切りテキスト、XML、JSON ファイルなどの構造化ログデータに対して SQL クエリを実行する。また、Microsoft LogParser 2.2 の GUI を提供し、シンタックスエディタ、データグリッド、チャート、ピボットテーブル、ダッシュボード、クエリマネージャなどの強力な UI 要素も備えている。
- Lorg: 高度な HTTPD ログファイルのセキュリティ分析とフォレンジックのためのツール。
- Logdissect: ログファイルやその他のデータを分析するための CLI ユーティリティと Python API。
- LogonTracer: Windows のイベントログを可視化し分析することで、悪意のある Windows ログオンを調査するツール。
- Sigma: 豊富なルールセットを持つ SIEM システム向けの汎用的なシグネチャーフォーマット。
- StreamAlert: サーバーレスでリアルタイムのログデータ分析が可能なフレームワークで、カスタムデータソースを取り込み、ユーザー定義のロジックでアラートを発動させることができる。
- SysmonSearch: イベントログを集約し、Windows イベントログの解析をより効果的に、より短時間で行えるようにする。
- WELA: Windows Event Log Analyzer は、Windows イベントログのためのスイスアーミーナイフとなることを目的としている。
- Zircolite: EVTX や JSON のための、スタンドアロンで高速な SIGMA ベースの検出ツール。

(7) メモリ解析ツール

- AVML: Linux 用のポータブルな揮発性メモリ取得ツール。

- Evolve: Volatility Memory Forensics Framework のウェブ・インターフェース。
- inVtero.net: ネストされたハイパーバイザーをサポートする Windows x64 用の高度なメモリ解析ツール。
- LiME: Linux および Linux ベースのデバイスから揮発性メモリを取得できる LKM（Loadable Kernel Module）、以前は DMD と呼ばれていた。
- MalConfScan: MalConfScan は、Volatility のプラグインで、既知のマルウェアの設定データを抽出する。Volatility は、インシデントレスポンスとマルウェア解析のためのオープンソースのメモリー・フォレンジック・フレームワーク。このツールは、メモリー・イメージからマルウェアを検索し、設定データをダンプする。また、悪意のあるコードが参照する文字列をリストアップする機能も備えている。
- Memoryze: インシデントレスポンダーがライブメモリー内の不正を発見するための無料のメモリー・フォレンジック・ソフトウェア。メモリー・イメージの取得や解析が可能で、ライブ・システムではページング・ファイルを解析に含めることができる。
- Memoryze for Mac: Mac 用の Memoryze。機能は少なくなっている。
- Orochi: Orochi は、フォレンジック・メモリー・ダンプを共同で解析するためのオープンソースのフレームワーク。
- Rekall: 揮発性メモリ（RAM）サンプルからデジタル・アーティファクトを抽出するためのオープンソースのツール（およびライブラリ）。
- Responder PRO: Responder PRO は、業界標準の物理メモリおよび自動マルウェア解析ソリューション。
- Volatility: 高度なメモリ・フォレンジック・フレームワーク。
- Volatility 3: 揮発性メモリ抽出フレームワーク（Volatility の後継）。
- VolatilityBot: バイナリ抽出の段階から推測や手作業を削減し、メモリ解析調査の最初のステップで調査者を支援する調査者向け自動化ツール。
- VolDiff: Volatility に基づくマルウェアのメモリー・フットプリント解析。
- WindowsSCOPE: Windows カーネル、ドライバ、DLL、仮想および物理メモリの解析機能を提供する、揮発性メモリの解析に使用されるメモリー・フォレンジックおよびリバース・エンジニアリング・ツール。

(8) メモリー・イメージング・ツール

- Belkasoft Live RAM Capturer: アンチデバッグまたはアンチダンピングシステムで保護されている場合でも、コンピューターの揮発性メモリーの全コンテンツを確実に抽出する小型の無料フォレンジックツール。
- Linux Memory Grabber: Linux メモリーをダンプし、Volatility プロファイルを作成するためのスクリプト。
- Magnet RAM Capture: マグネット RAM キャプチャ。容疑者のコンピューターの物理メモリーをキャプチャーするために設計された無料のイメージング・ツール。Windows の最近のバージョンをサポ

ートしている。
- OSForensics: 32 ビットおよび 64 ビットシステム上のライブメモリーを取得するためのツール。個々のプロセスのメモリ空間のダンプや物理メモリのダンプを行うことができる。

(9) その他のツール
- Cortex: IP アドレス、メールアドレス、URL、ドメイン名、ファイル、ハッシュなどの観測値を、Web インターフェースを使って 1 つずつ、または一括で解析するツール。また、REST API を使用してこれらの操作を自動化することもできる。
- Crits: 分析エンジンとサイバー脅威データベースを組み合わせた Web ベースのツール。
- Diffy: Netflix の SIRT が開発した DFIR ツールで、インシデント発生時にクラウドインスタンス（現在は AWS 上の Linux インスタンス）の侵害を迅速に特定し、ベースラインとの差異を示すことでフォローアップアクションのためのトリアージを効率的に行うことができる。
- domfind: Python の DNS クローラーで、異なる TLD の下で同一のドメイン名を見つけることができる。
- Fileintel: ファイルハッシュ単位で情報を取得するツール。
- HELK: スレットハンティングプラットフォーム。
- Hindsight: Google Chrome/Chromium 用のインターネット履歴フォレンジック。
- Hostintel: ホスト単位で情報を取得するツール。ホスト単位で情報を取得するツール。
- imagemounter: フォレンジック・ディスク・イメージのマウントを容易にするコマンドライン・ユーティリティと Python パッケージ。
- Kansa: PowerShell によるモジュラー型インシデントレスポンス・フレームワーク。
- MFT Browser: MFT ディレクトリー・ツリーの再構築と記録情報。
- Munin: VirusTotal などのオンライン・ハッシュ・チェッカー。
- PowerSponse: セキュリティインシデント対応時の標的型封じ込めと修復に特化した PowerShell モジュール。
- PyaraScanner: マルウェア・ズーと IR のためのマルチ・スレッド多ルール多ファイルの YARA スキャン Python スクリプト。
- rastrea2r: Windows、Linux、OSX 上で YARA を使用してディスクやメモリをスキャンし、IOC を検出するツール。
- RaQet: 意図的に構築されたフォレンジック OS で再起動されたリモートコンピューター（クライアント）のディスクをトリアージすることができる、従来にないリモート取得・トリアージツール。
- Raccine: ランサムウェア対策ツール。
- Stalk: 問題発生時に MySQL に関するフォレンジックデータを収集するためのツール。
- Scout2: Amazon Web Services の管理者が、自社環境のセキュリティ状況を評価するためのセキュリティツール。
- Stenographer: すべてのパケットをディスクに高速にスプールし、そのパケットのサブセットに簡単かつ高速にアクセスできるようにすることを目的としたパケット・キャプチャー・ソリューショ

ン。可能な限り多くの履歴を保存し、ディスクの使用量を管理し、ディスクの限界に達した場合は削除する。すべてのネットワーク・トラフィックを保存する必要はないが、インシデントの直前や最中のトラフィックをキャプチャーするのに便利である。

- sqhunter: osquery と Salt Open (SaltStack) をベースにした脅威ハンターで、osquery の tls プラグインを使用せずにアドホックまたは分散クエリを発行できる。sqhunter では、ユーザがオープン・ネットワーク・ソケットをクエリして、脅威情報ソースと照合することができる。
- sysmon-config: デフォルトの高品質なイベント・トレース機能を持つ sysmon 設定ファイル・テンプレート。
- sysmon-modular: sysmon 設定モジュールのリポジトリ。
- traceroute-circl: CSIRT (または CERT) オペレーターの活動を支援するための拡張トレースルート。通常、CSIRT チームは受け取った IP アドレスに基づいてインシデントを処理しなければならない。このツールは Computer Emergency Response Center Luxembourg によって作成された。
- X-Ray 2.0: AV ベンダーにウイルスサンプルを提出するための Windows ユーティリティ(メンテナンスが不十分か、もはやメンテナンスされていない)。

(10)プロセス・ダンプ・ツール

- Microsoft ProcDump: 実行中の Win32 プロセスのメモリイメージをオンザフライでダンプできるようにするツール。
- PMDump: プロセスを停止させることなく、プロセスのメモリ内容をファイルにダンプするツール。

(11)サンドボックス／リバーシングツール

- AMAaaS: Android Malware Analysis as a Service の略で、Android のネイティブ環境で実行される。
- Any Run: あらゆる環境を利用して、ほとんどの種類の脅威を動的および静的に調査できる、インタラクティブなオンラインマルウェア解析サービス。
- CAPEv2: マルウェアの設定とペイロードの抽出を行うツール。
- Cuckoo: オープンソースの高度に設定可能なサンドボックスツール。
- Cuckoo-modified: コミュニティによって開発された、高度に修正された Cuckoo のフォーク。
- Cuckoo-modified-api: Cuckoo-modified のサンドボックスを制御するための Python ライブラリ。
- Cutter: Radare2 によるリバース・エンジニアリング・プラットフォーム。
- Ghidra: ソフトウェア・リバース・エンジニアリング・フレームワーク。
- Hybrid-Analysis: ハイブリッド解析。CrowdStrike 社による無料の強力なオンライン・サンドボックス。
- Intezer: Windows バイナリに潜り込み、既知の脅威とのマイクロコードの類似性を検出し、正確かつ分かりやすい結果を提供する。
- Joe Sandbox (Community): Joe Sandbox は、Windows、Android、Mac OS、Linux、iOS 上の潜在的な悪意のあるファイルや URL を検出・分析し、疑わしい活動を検知して、包括的かつ詳細な分析レポ

ートを提供する。

- Mastiff: さまざまなファイルフォーマットから重要な特徴を抽出するプロセスを自動化する静的解析フレームワーク。
- Metadefender Cloud: メタデフェンダー・クラウド。ファイルのマルチスキャン、データサニタイズ、脆弱性評価などを行う無料の脅威インテリジェンス・プラットフォーム。
- Radare2: リバース・エンジニアリング・フレームワークとコマンドライン・ツールセット。
- Reverse.IT: CrowdStrike が提供する Hybrid-Analysis ツールの代替ドメイン。
- Rizin: UNIX ライクなリバース・エンジニアリング・フレームワークとコマンドライン・ツールセット。
- StringSifter: マルウェア解析のための関連性に基づいて文字列をランク付けする機械学習ツール。
- Threat.Zone: サンドボックス、CDR、研究者向け対話型分析を含む、クラウドベースの脅威分析プラットフォーム。
- Valkyrie Comodo: Valkyrie は、ファイルからランタイムの動作と数百の機能を使用して分析を実行する。
- Viper : Python ベースのバイナリ解析・管理フレームワークで、Cuckoo や YARA と連携して動作する。
- Virustotal: ファイルや URL を解析し、ウイルス対策エンジンや Web スキャナで検出されたウイルス、ワーム、トロイの木馬などの悪意のあるコンテンツを特定できる無料のオンラインサービス。
- Visualize_Logs: オープンソースのログ可視化ライブラリとコマンドライン・ツール (Cuckoo, Procmon, さらに追加予定)。
- Yomi: Yoroi が管理・運営する無料のマルチサンドボックス。

(12)スキャナツール

- Fenrir: シンプルな IOC スキャナ。あらゆる Linux/Unix/OSX システムの IOC をプレーンな bash でスキャンすることができる。THOR と LOKI の作者によって作られた。
- LOKI: YARA ルールと他のインジケータ(IOC)でエンドポイントをスキャンするためのフリーの IR スキャナ。
- Spyre: Go で書かれたシンプルな YARA ベースの IOC スキャナ。タイムラインツール。
- Aurora Incident Response: インシデントの詳細なタイムラインを簡単に構築するために開発されたプラットフォーム。
- Highlighter: Fire/Mandiant から無料で提供されているツールで、ログ/テキストファイルを表示し、キーワードに対応するグラフィック上の領域をハイライトすることができる。感染症や感染後に何が行われたかを時系列で把握するのに適している。
- Morgue。Etsy による死後管理用の PHP ウェブアプリ。
- Plaso: log2timeline の Python ベースのバックエンドエンジン。
- Timesketch: フォレンジック・タイムラインの共同解析のためのオープンソースツール。

2. 証拠収集

(1) Linux 証拠収集

- FastIR Collector Linux: ライブの Linux 上で様々なアーティファクトを収集し、その結果を CSV ファイルに記録する。

(2) OSX 証拠収集

- Knockknock: OSX 上で自動的に実行されるように設定されている永続的なアイテム（スクリプト、コマンド、バイナリなど）を表示する。
- macOS Artifact Parsing Tool (mac_apt): ライブマシン、ディスクイメージ、または個々のアーティファクトファイルで動作する、迅速な mac のトリアージ用のプラグインベースのフォレンジックフレームワーク。
- OSX Auditor: 無料の Mac OSX コンピュータ・フォレンジック・ツール。
- OSX Collector: ライブレスポンス用の OSX Auditor の分派。
- The ESF Playground: Apple Endpoint Security Framework (ESF)のイベントをリアルタイムで表示するツール。

(3) Windows 証拠収集

- AChoir: Windows 用ライブ収集ユーティリティのスクリプト作成プロセスを標準化・簡略化するためのフレームワーク/スクリプト作成ツール。
- Crowd Response: インシデントレスポンスやセキュリティ対策のためのシステム情報収集を支援するために設計された、軽量な Windows コンソールアプリケーション。多数のモジュールと出力形式を備えている。
- DFIR ORC: DFIR ORC は、MFT、レジストリハイブ、イベントログなどの重要なアーティファクトを確実に解析し収集するための専用ツールの集合体。DFIR ORC は、データを収集するが、それを分析するわけではない。Microsoft Windows を実行しているマシンのフォレンジックに関連するスナップショットを提供する。コードは GitHub で見ることができる。
- FastIR Collector: 稼働中の Windows システム上のさまざまなアーティファクトを収集し、結果を csv ファイルに記録するツール。これらのアーティファクトを分析することで、侵害を早期に発見することができる。
- Fibratus: Windows カーネルを調査・追跡するためのツール。
- Hoarder: フォレンジックやインシデントレスポンス調査のために、最も価値のあるアーティファクトを収集する。
- IREC: RAM イメージ、$MFT、イベントログ、WMI スクリプト、レジストリハイブ、システム復元ポイントなどをキャプチャするオールインワン IR エビデンスコレクター。無料で、高速かつ簡単に使用できる。
- Invoke-LiveResponse: Invoke-LiveResponse は、ターゲットを絞った収集のためのライブ・レスポンス・ツール。

- IOC Finder: Mandiant 社が提供する、ホストシステムのデータを収集し、Indicators of Compromise (IOC)の存在を報告するための無料ツール。Windows のみサポート。メンテナンスは終了しており、Windows 7/Windows Server 2008 R2 までしか完全にサポートされていない。
- IRTriage: Incident Response Triage - フォレンジック解析のための Windows の証拠収集。
- KAPE: Eric Zimmerman による Kroll Artifact Parser and Extractor (KAPE)。最も一般的なデジタルアーティファクトを見つけ出し、素早く解析するトリアージツール。
- LOKI: YARA ルールやその他の指標（IOC）でエンドポイントをスキャンする無料の IR スキャナ。
- MEERKAT: Windows 用の PowerShell ベースのトリアージと脅威ハンティング。
- Panorama: ライブの Windows システム上でインシデントの概要を迅速に表示する。
- PowerForensics: PowerShell を使用したライブディスクフォレンジックプラットフォーム。
- PSRecon: PowerShell（v2 以降）を使用して、リモート Windows ホストからデータを収集し、データをフォルダに整理し、抽出したすべてのデータをハッシュし、PowerShell と様々なシステムプロパティをハッシュして、セキュリティ・チームにデータを送信する。データは、共有にプッシュしたり、電子メールで送信したり、ローカルに保持したりすることができる。
- RegRipper: レジストリから情報（キー、値、データ）を抽出/解析し、分析用に表示するための、Perl で書かれたオープンソースツール。

第 7 節 参考文献

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

[2] Michael D. Shear, Nicole Perlroth and Clifford Krauss, “Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers,” The New York Times, May 13, 2021, available at https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline- ransomware.html.

[3] Tallinn Manual published by NATO’s Cooperative Cyber Defence Centre of Excellence explores the international laws and perspective regarding cyber warfare. Version 2.0 was published in 2013 and work is underway to develop version 3.0. More information available at: https://ccdcoe.org/research/tallinn-manual/.

[4] “INTO THE GRAY ZONE: The Private Sector and Active Defense against Cyber Threats,” The George Washington University’s Center for Cyber and Homeland Security, 2016.

[5] Jon Bateman, “The Purposes of U.S. Government Public Cyber Attribution,” Carnegie Endowment for International Peace, March 28, 2022, available at https://carnegieendowment.org/2022/03/28/purposes-of-u.s.-government-public-cyber-attribution-pub-86696.

[6] U.S. Cyber Command PAO. "CYBER 101 - Defend Forward and Persistent Engagement", 2022

[7] "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure", Cybersecurity Advisory AA22-011A, 2022

[8] "FBI says it 'hacked the hackers' of a ransomware service, saving victims $130 million", The Verge, 2023, available at https://www.theverge.com/2023/1/27/23574257/fbi-us-justice-department-seizes-hive-ransomware-network-servers

[9] Steffens Timo, "Attribution of Advanced Persistent Threats; How to Identify the Actor Behind Cyber-Espionage", Springer-Verlag GmbH, Springer Nature, 2020.

[10] "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research ", U.S. Department of Justice, Public Affairs Notice, 20-675, 2020., available at https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

[11] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies, Volume 38, 2015

[12] Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C. Reverse social engineering attacks in online social networks. In Detection of Intrusions and Malware, and Vulnerability Assessment. Springer: Berlin Heidelberg, 2011; 55-74.

[13] Egele M, Scholte T, Kirda E, Kruegel C. "A survey on automated dynamic malware-analysis techniques and tools." ACM Computing Surveys (CSUR) 2012; 44(2):6.

[14] Donohue B. Is North Korea really behind the Sony breach. Kaspersky Lab. http://blog.kaspersky.com/sony-hack-north-korea/. Last accessed October 2, 2015.

[15] Clark DD, Landau S. "The problem isn't attribution: it's multi-stage attacks." In the Proceedings of the Re-architecting the Internet Workshop. ACM, 2010.

[16] Dacier M, Pham VH, Thonnard O. The WOMBAT attack attribution method: some results. In Information Systems Security. Springer: Berlin Heidelberg, 2009; 19-37.

[17] Pfeffer A, Call C, Chamberlain J, Kellogg L, Ouellette J, Patten T, Zacharias G, Lakhotia A, Golconda S, Bay J, Hall R, Scofield D. "Malware analysis and attribution using genetic information." In the Proceedings of the 7th IEEE Conference on Malicious and Unwanted Software (MALWARE), 2012; 39-45.

[18] Diederich J, Kindermann J, Leopold E, Paass G. "Authorship attribution with support vector machines". Applied Intelligence 2003; 19(1-2):109-123.

[19] Matwin S, Nin J, Sehatkar M, Szapiro T. A review of attribute disclosure control. In Advanced Research in Data Privacy. Springer International Publishing, 2015; 41-61.

[20] The Solarium Commission, Final Report, 2020, available at https://www.solarium.gov/report.

第４章 セキュリティクリアランス

本章では、日本でセキュリティクリアランス制度を構築することに向けて、米国の状況をまとめるとともに、日本の制度への提言を示す。

第１節 本章の調査研究方針

本件調査では、日本政府に対して、人事考課、情報保護フレームワーク、および政府システムにおける情報保護と信頼できるアイデンティティとアクセス管理を可能にするデジタル技術に関する政策と能力の開発および実施について助言するという顧客の取り組みを支援するものである。日本が国家安全保障情報だけでなく、商業・経済情報を保護することにも関心を持っているという認識のもと、それぞれの情報以下のように整理される。

情報領域	**審査の種類**	**保護レベル**
商業・経済	社会的信頼性・適性	Controlled Unclassified
国家安全保障	機密情報へのアクセス資格	Secret / Top Secret

本調査のアプローチは、米国セキュリティクリアランスの専門家が GRIPS の研究者及び GRIPS が特定するその他の者と会合を持ち、遠隔で行われる一連の作業セッションに参加することである。このアプローチは、連邦政府認証、連邦政府保証および信頼サービスレベル、および人事考課など、米国セキュリティクリアランスの専門家が過去に顧客に提供した製品で推奨されているアクションに対応するものである。具体的には以下の項目に対する調査研究が実施される。

- 人事考課（パーソナル・ベッティング）
    - 日本に必要な人事評価政策と実務のあり方についての前提条件の確認。フレームワークと提言を形成する GRIPS との前提条件の議論と検証。
    - 日本政府向けのフレームワーク、ハイレベルな提言、人材調査のベストプラクティスおよび標準を提供する。フレームワークは、政策や法律の変更、調査や意思決定の権限の一元化の可能性、情報技術の必要性など、今後必要とされる検討を行う。

- データ区分フレームワーク
    - 日本に必要なセキュリティ区分政策と実務の状況に関する仮定の特定。フレームワークと提言を形成する GRIPS による前提条件の議論と検証。

- 日本政府向けにセキュリティ区分のためのフレームワーク、ハイレベルな推奨事項、ベストプラクティス、標準を提供する。このフレームワークは、区分を必要とする情報のカテゴリー、保護レベル、管理された非区分情報の必要性、その他の潜在的なニーズなどを扱う。

- 技術開発フレームワーク
  - 日本に必要な政策と実践の状況に関する前提条件の確認。フレームワークと提言を形成するGRIPSとの前提条件の議論と検証。
  - 日本政府のアイデンティティ、認証、認可をサポートするポリシーと技術開発のためのフレームワーク、高レベルの推奨事項、技術的なベストプラクティスや標準を提供する。PIV、F/D02、FedRAMP クラウドサービス、アクセス制御システム、資格認定、適合性、適格性の決定、および上記の項目「セキュリティの区分」の作業の流れで開発された潜在的区分レベルに対応するセキュリティ領域に関するシステム要件の考慮が含まれる。

第２節 人事考課（パーソナル・ベッティング）

1. エグゼクティブサマリー

日本の国家、経済、社会の優先順位は重要な問題である。これらの分野は表裏一体であり、重要なつながりの一つは、これらの課題分野で働く人々が、ミッションの成功に不可欠な機密情報の取り扱いと保護に信頼できることを保証する必要がある。しかし、日本の政府や産業界には、これらの環境下で一貫して適用される明確な人事考課制度は存在しない。さらに、現在使用されている数少ない審査プロセスは、個人の信頼性と信用性を確実に評価するのに十分なデータを提供しない。これらの属性は、あらゆる分野の資産や利益を保護するための効果的なプログラムにおいて、極めて重要な要素である。リスクは、これらの重要な分野で機密情報にアクセスする政府や民間の職員の側で、意図的な行動と不注意や不注意の両方から発生するものである。このようなリスクは、機密情報にアクセスする政府職員や民間職員の意図的な行動と不注意によって引き起こされる。効果的な審査プログラムを開発することの重要な成果は、政府内および国際的な同盟国との信頼関係を大幅に改善することである。

本節は、国家安全保障、経済安全保障、社会保障の優先事項に関するデータ保護/セキュリティ区分/サイバーセキュリティの目的とリンクする政府全体の人事考課システムの構築について、日本政府関係者に情報を提供することを目的とする。また、信頼レベル、審査の原則、調査、クリアランスの決定、情報技術システムなどの主要な要素を含む、確立されるべき審査システムの属性について説明する。また、区分やサイバーセキュリティシステムとの連携も確立する必要がある。重要な最初のステップは、プログラムの詳細を策定し、その実行を監督するハイレベルな政府機関の設立（法令による）である。

2．問題点

国際的な敵は、防衛であれ製造であれ、所有する国や組織が優位に立てるような重要かつ機密性の高いプログラムへのアクセスを得るため、あらゆる機会をうかがっている。これまでの経験から、その対象は防衛や国家安全保障上の秘密に限られないことが分かっている。企業の商業的な利得が侵害されることもよくある。どのような場合でも、一度情報が失われると、その交換や回復は、たとえ可能であったとしても、一般的には容易なことではない。このような侵害を容易にする攻撃や手法はさまざまであるが、重要なポイントは、重要な情報にアクセスできる、あるいは不注意にアクセスを容易にできる従業員や関連会社、つまり内部関係者を侵害する手法が大半を占めていることである。この危険な情報は、日本のインフラのほぼすべての部分に存在する。

内部関係者が意図的に情報を漏洩させる決断をすることもある。そのような行動の動機は、個人的な金銭的利益から怒りや復讐まで様々であるが、その理由にかかわらず、一度暴露された情報は、取り戻すことができない。国家や経済の競争相手は、常にインサイダーからそのような情報を受け取り、競争力を高めることを望んでいる。米国における 2 つの例は、エドワード・スノーデンとマニング二等兵であり、彼らはいずれも重要な機密情報を意図的に削除し、外国企業に暴露する決定を下したのである。

内部関係者の不注意や不作為が侵害の重要な要素になることもある。施設や情報システムへの外部からの侵入の成功例の多くは、ネットワーク上で働く信頼できる従業員の不注意やミスによって促進されることが分かっている。代表的な例として、2014 年のソニー株式会社の事業基盤の侵害と、2014 年の米国人事管理局のファイル流出がある。いずれも、外国政府による無防備な従業員へのフィッシング詐欺の結果、認証情報が盗まれ、対象となるデータベースへのフルアクセスが容易になったものである。

国家安全保障や経済などの機密が漏洩し、その情報が国家に与えていた優位性が損なわれるか破壊されるからである。共通するのは、信頼される立場にある人間が、意図的かどうかにかかわらず、秘密の漏洩をもたらす扉を（実際に、または仮想的に）開いてしまったということである。このため、機密性の高い分野や任務で働く従業員や請負業者の信用と信頼性を、当初から継続的に評価することが決定的に重要である。

3．審査による信頼の評価

新規および既存の従業員の審査に使用できる積極的かつ徹底したプロセスは、機密情報およびアクセスを保護するための取り組みにおいて、基本的かつ重要な要素である。審査プロセスの目的は、1) 採用を検討する時点で個人の信用と信頼性を判断し、2) 在職中も信用と信頼を評価し続け、3) 発生し得る懸念に対処するために適切な行動をとることである（図 4-2-a）。

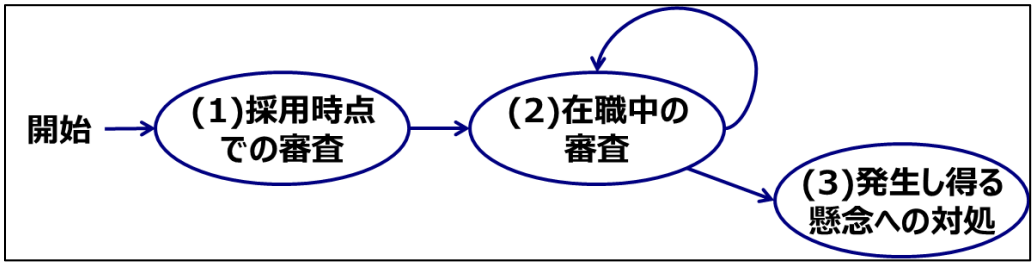


図 4-2-a 従業員の審査プロセスの全体像

これは、特に新入社員レベルでは、ほとんどの場合、予測的な作業となる。応募者は通常、保護された情報にアクセスしたことがないため、信頼性の判断は、要件を理解し責任を持って実行できるかどうかを示す、私生活と公生活の両方における過去の行動や振る舞いの評価に基づいて行う必要がある。

4. プログラムの確立

国家レベルでは、米国とその同盟国での経験から、あらゆる種類の機密情報や資料を扱う政府や民間の職員、請負業者を評価・監視する必要性を指摘する国家レベルのマンデートを作成することが最初のステップであることが分かっている。この指令は、すべての関連省庁にまたがるプロセスと使命を可能にするため、国の最高権威から発せられるべきである。日本では、国会から発行される法令が適切な基盤であると考える。

この法令は、例外なくすべての政府役員および職員、ならびに機密情報、システム、施設にアクセスできるすべての請負業者が、この審査プロセスに含まれることを定めるべきである。さらに、調査の範囲は、充てようとする地位の占有者が国家安全保障にもたらし得る悪影響の程度によって決定されるべきであると指示すべきである。また、この法令は、最初の審査決定が唯一の評価点ではなく、時間の経過とともに定期的に決定を再評価する必要性があることを認めるべきである。

審査要件の設定にとどまらず、長期的な成功を確保するために、これらの業務の継続的な監視を含めることが重要になる。また、プログラムの範囲も考慮しなければならない。1 人の人物に対する調査や評価は比較的簡単であるが、どの国にとっても、国家レベルで何千人もの個人に対してそのようなプロセスを確立し、一貫して維持することは困難である。従って、この法律は、指定し、権限を与えるべきである。

- 政府全体の審査システムの構築と継続的な運用を管理する監督機関（内閣府など）。この組織は、システムに関与するすべての省庁・組織のパフォーマンスと進捗を監視し、進捗状況を立法府に報告する。
- 関係省庁・機関において、調査の実施、調査に基づくクリアランスの決定、およびこれらの業務を支援する情報技術システムの開発・運用に関する方針、基準、手続きを策定する団体または組織。
- 全庁的に調査を行う主体。
- すべての審査業務をサポートする情報技術システムを開発・運用する事業者。

審査プログラムの体制図を図 4-2-b に示す。監督機関は国家レベルで一つであり、複数の調査機関に対する監督を行う。調査機関は、省庁ごとに設置される機関であり、裁定者と調査者とからなる。調査者は、対象者に対して各種の調査を行う。また、調査機関にある情報システムは、調査報告書の入力、検索、アーカイブなどを行うとともに、対象者に対して PIV カード（Personal Identity Verification Card）や CAC カード（Common Access Card）を発行する。

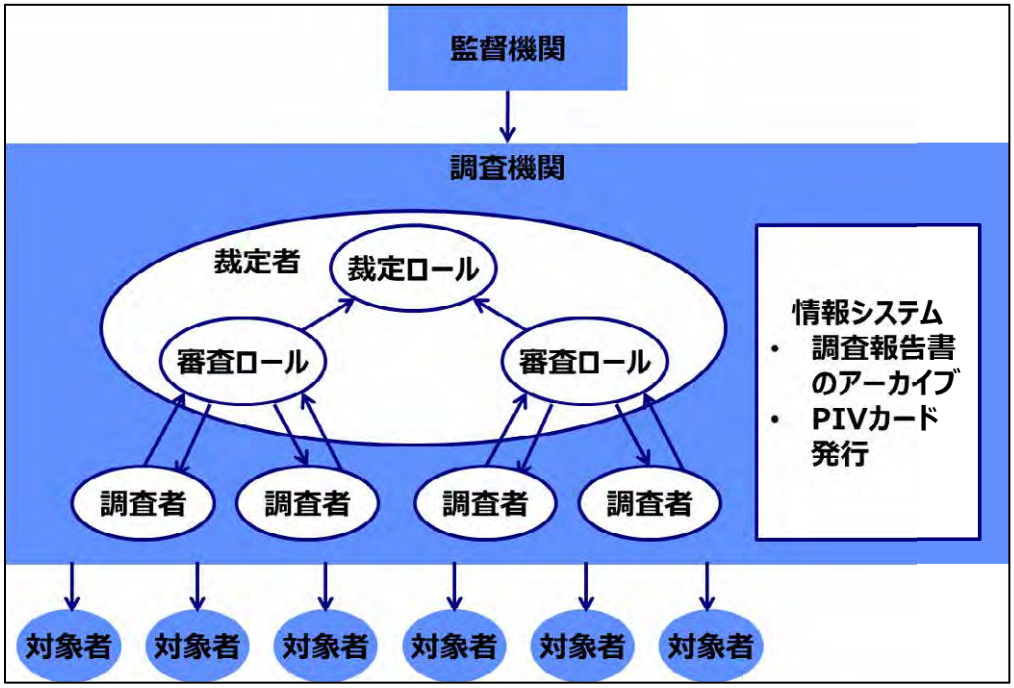


図 4-2-b 審査プログラムの体制図

米国政府（USG）のプロセスは、1947 年の国家安全保障法の制定以来、最近では非常に包括的なトラステッド・ワークフォース 2.0 活動を通じて発展してきた。USG は、情報収集、分析、意思決定の複雑な階層システムを採用し、連邦政府機関内または連邦政府機関 と共に働く可能性のある要員を信頼するかどうか、またどの程度信頼するかを決定している。このシステムは、広義には人事考課と呼ばれる。

5. トラステッド・ワークフォースの定義

人材の審査に使用される具体的な手順と基準は、その人が政府とどのように仕事をするか、また、その人の職責に応じて政府がその人に置くべきだと判断する信頼の度合いによって決まる。個人が政府と仕事をする方法は、以下のように様々である。

- 連邦政府機関の職員。

- 国の機関と契約し、その機関の労働力の一部として働く民間企業の従業員（一般にコントラクターと呼ばれる）。
- 国家政府と契約している民間企業の従業員で、主に連邦政府機関の従業員とは別に企業拠点で働きながら、政府プロジェクトに従事する者（一般にコントラクターとも呼ばれる。）
- 連邦機関に物品またはサービスを供給する民間企業の従業員で、そのために連邦施設への立ち入りが必要となる場合がある。従業員に対する信頼のレベルは、その職責によって異なる。信頼度が高いほど、USG は個人の経歴を理解するために多大な努力を払い（バックグラウンド調査）、より高い基準を設定する。

米国のシステムでは、これらの信頼レベルは階層化されており、その間に重複があるが、以下のように構成される（図 4-2-c）。
クレデンシャル、適性、および適格性。

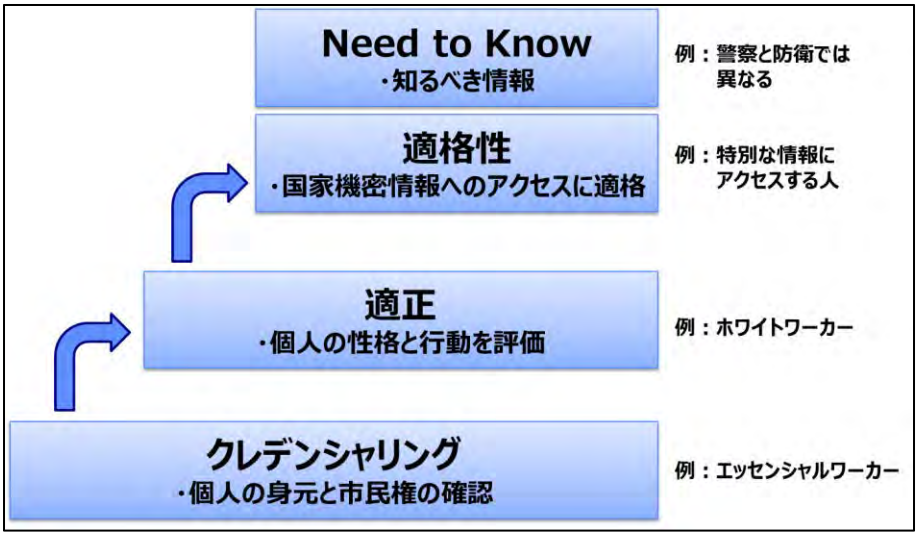


図 4-2-c 信頼レベルの階層化

- クレデンシャルは、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。クレデンシャルは、連邦施設への労働者のアクセス（業者、清掃員、造園作業員など）を許可するための独立したプロセスとして実施される場合もあるが、適性と適格性を決定するための連続した各レベルの審査の最初のステップとしても実施される。

- 適性は、個人の性格と行動を評価し、連邦政府の労働力の一員となるのにふさわしいかどうかを確認するものである。適性とは、政府で働く、または政府と共に働く個人に寄せられる公的信頼のレベルを指す。公的信頼には、2 つの明確なレベルがある。基本的な公的信頼はすべての連邦職員に適用され、高い公的信頼は、指導的地位にある者、および機関の指導、財務管理、買収、または安全/セキュリティ機能など特定の職務を伴う責任を負う地位に適用される。

- 適格性は、特に国家安全保障の機密情報へのアクセスを必要とする職種に関連するものである。米国政府の区分システムには、いくつかの区分レベルがあり、各区分レベルに固有の意思決定のための手順と基準が使用されている。これらの基準は、ある機関の決定を、情報を共有し、または同じ人物と仕事をする他の機関が信頼できるようにするために、すべての連邦機関で統一的に採用されることになっている。

なお、クレデンシャル、適正、適格性をパスした後に、さらに、政府機関ごとに必要となる情報が異なるために、Need to Know の原則によって必要な信頼レベルが付与される。

6. 人事考課のライフサイクル

このような背景のもと、典型的な事例をもとに、審査のライフサイクル（図 4-2-d）に沿って、そのプロセスや各主体の役割について説明する。

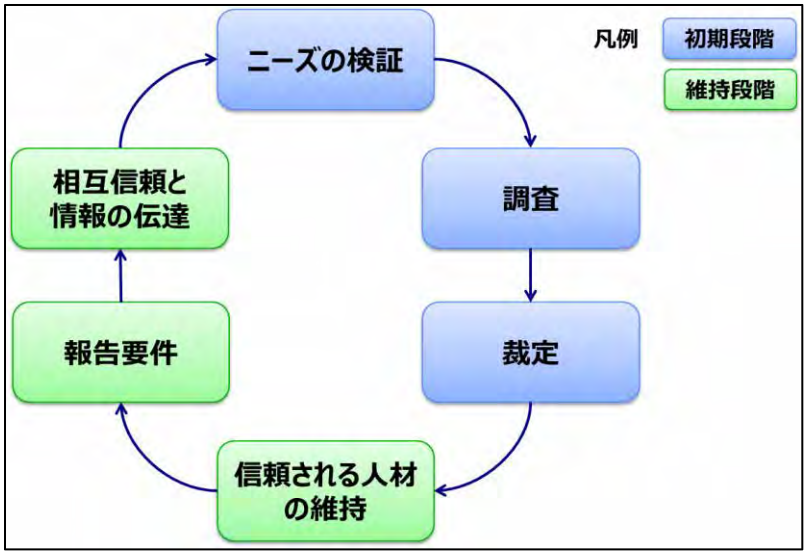


図 4-2-d 人事考課のライフサイクル

- ニーズの検証

個人の雇用形態が確立されると、政府関係者は、その人物が信頼される立場にいる必要性を検証し、最終的な判断につながる調査プロセスを開始しなければならない。この政府関係者は、ある機関の雇用権限者あるいは、契約社員やベンダーが機関のプロジェクトで働く必要があると判断した契約担当者あるいは、ある個人が政府施設に立ち入る必要があると判断した政府関係者かもしれない。いずれにせよ、調査プロセスは常に、政府関係者がその人物の必要性を確認し、どの程度の信頼が必要かを判断し、どのような種類の調査が必要かを決定することから始まる。

- 調査

機関は、特定の信頼レベルの従業員の必要性を検証した後、調査サービス提供者に調査を依頼する。依頼された調査は、監督機関が定めた基準に従って、雇用形態と信頼レベルに対応するものである。調査プロセスは、個人の人格、行動、信頼性について判断できるように、個人の履歴の基本的な要素を確認することを目的としている。

調査プロセスは、調査対象となる個人（調査対象者と呼ぶ）から情報を収集することから始まる。調査対象者の個人履歴情報の収集は、求める信頼の度合いに応じて、標準的なフォーマット（図 4-2-e）を使用する必要がある。

このような書式は、政府が管理する一元的なオンライン・アプリケーションを通じて記入できるようにする必要がある。このプラットフォームは、一連の質問を行い、対象者の回答に応じて、必要に応じてフォローアップの質問をしたり、次の話題に移ったりして、対象者からすべての関連情報を収集できるようにすべきである。

被験者から直接情報を収集することには、2 つの目的がある。1) 対象者は通常、自分の経歴について最も正確な情報を持っている、2) 対象者は、この情報を提供する際に、真実かつ完全であることを法的に証明する。対象者が書式に虚偽又は誤解を招く情報を記入したことが判明した場合、裁決者はこの事実を考慮し、信用レベルを付与するか否かを決定することができる。書式には、対象者及び第三者の情報源から情報を収集するために、日本の法律の下で必要 なあらゆるリリース又は同意が含まれるべきである。

調査によってカバーすることが不可欠な個人履歴の要素は、出生、市民権、忠誠心、教育、雇用、軍務、婚姻状況/履歴、家族、個人的および職業上の照会、住居、財政責任、犯罪歴、心理的および感情的健康、違法薬物の使用、アルコール使用、情報技術の使用、政府に敵対するグループとの提携、外国人との接触、ビジネスまたはその他の関連（資格および国家安全保障上の機密職の場合）である。

調査の範囲は、対象者の年齢、求める信頼の度合い、過去に政府による調査を受けたことがあるかどうかによって異なるが、何年分の履歴をカバーするかは、対象者の年齢によって異なる。一般的に、最初の調査は対象者の 18 歳の誕生日までさかのぼり、年齢が高い場合や過去に調査を受けたことがある場合は、過去 7 年、10 年、15 年などさまざまな期間をカバーすることになる。

調査における情報収集の手段としては、対象者の申請書の入手、訓練を受けた調査員による対象者へのインタビュー、自動化された手段または訓練を受けた調査員による公的記録（出生、教育、雇用、居住、犯罪行為など）の入手、個人および職業上の推薦人、隣人、同僚、家主、その他事件に関連する人へのインタビュー（すべて訓練を受けた調査員により行われる）などがある。

すべての取材が完了したら、報告書または調査書を依頼元に提供し、依頼元が対象者について信頼性の判断を下せるようにする。調査報告書は、電子的にアーカイブされ、将来の問い合わせの際に他のオフィスが発見できるようにする必要がある。

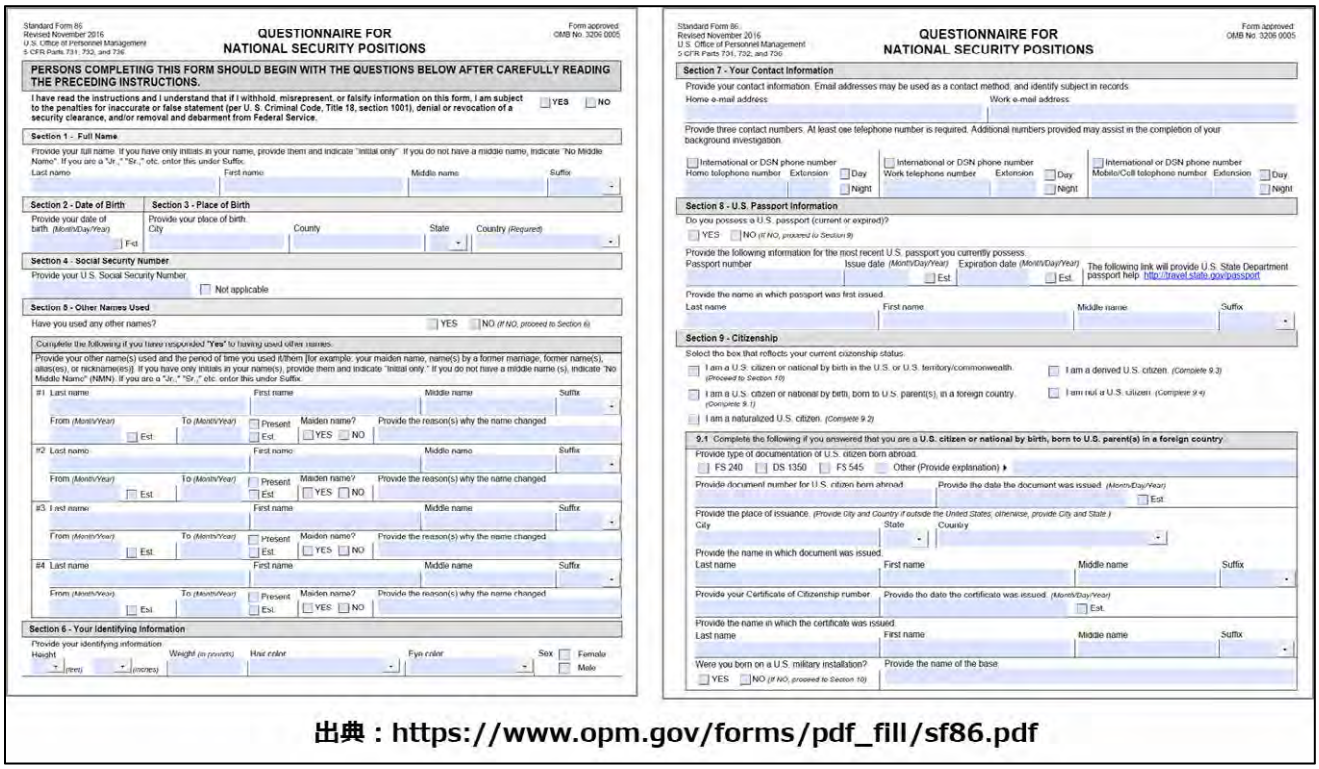


図 4-2-e Standard Form 86 の抜粋（質問票 100 ページ以上にのぼる）

- 裁定

裁定は、機関がその対象について信頼判断を下すステップである。大まかに言えば、これらの基準は、性格、行動、および意思決定のパターンに関する同様の問題を対象としているはずであるが、注目に値するいくつかの違いがある。前述のとおり、適性および資格認定基準は、国家安全保障裁定ガイドラインとして知られる、機密情報へのアクセス資格の基準には存在しない柔軟性を、省庁の長に認めている。また、外国の影響力や外国人の好みに関する事項は、適格性基準にのみ含まれ、適性および資格認定には含まれない。

裁定ガイドラインのトピックは以下の通りである。

- 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

裁定プロセスでは、訓練を受けた裁定者が、調査で収集されたすべての情報を評価し、対象がその信頼レベルの調査基準を満たしていることを確認し、その結果を分析して、集合的に対象者の積極的な性格、行動、信頼性を確認するかどうかを決定する。もし調査が、上記の裁定ガイドラインに関して対象者に否定的な情報を含む場合、裁定者はその情報を分析し、最終決定（承認または不承認のいずれか）を下すのに十分な情報があるかどうか、発生した問題を解決するためにさらなる情報が必要であるかどうかを判断する。さらなる情報が必要な場合、さらなる調査のために案件を差し戻すか、対象者と直接問題を解決するために対象者の面接を実施することがある。裁定ガイドラインには、この分析を支援するガイドラインのトピックごとに考慮すべき特定の要因が含まれている。対象者が承認された場合、検証された必要性に応じて、雇用、クレデンシャル付与、またはアクセス権付与を行うことができる。対象者が不承認となった場合、信頼される地位への雇用形態を進めない可能性がある。機密情報へのアクセス資格が否定された場合、USG の方針により、対象者はこの決定を行った機関の長に上訴することができる。この決定は、後のセクションで説明するように、政府全体のデータベースにも記録される。

- 信頼される人材の維持

政府機関は、裁定が下された後も、信頼される従業員の行動の変化と考えられるリスクレベルを確実に認識するために、様々なプロセスやツールを使用する必要がある。米国の古い慣行では、5 年から 10 年の間隔で定期的に再調査することが義務付けられていたが、この方法の有効性に関する最近の評価により、継続的評価として知られる、よりダイナミックで効果的なアプローチが生み出された（図 4-2-f）。米国セキュリティクリアランス専門家は、この戦略の採用を推奨している。

このプロセスでは、関連する電子データソースが継続的に参照されるため、機関は、5 年または 10 年のサイクルよりも早く、セキュリティ関連情報を知るために対象者をより継続的に調査することができる。機関は、この継続的な報告から発生する問題を解決し、その個人が機密情報にアクセスする資格を持ち続けるかどうかを判断することが求められている。

注：米国政府の政策は、再調査の要件を継続的審査モデルに置き換える方向に進んでいるが、この取り組みはまだ発展途上にある。米政府機関は現在、継続的な審査要件をカバーするプログラムを試験的に実施しており、監督当局は最近、政府全体にわたるセキュリティ、適性、および資格認定プログラムをよりよく統合するために計画された改革を各機関に知らせるため、政策の一般声明を発表した。初期の結果は有望であっ

た。

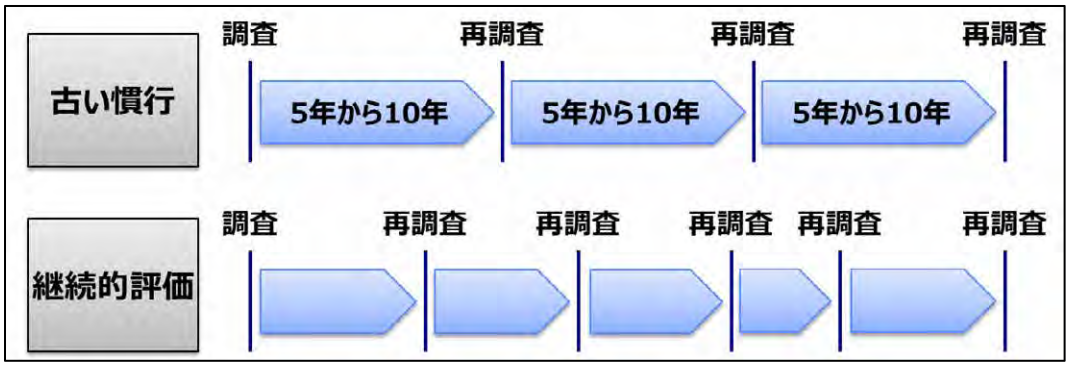


図 4-2-f 再調査の比較イメージ

- 報告要件

機密情報へのアクセス資格を維持するために、職員は特定のセキュリティ関連情報を、その許可を与えたセキュリティ担当者に報告することが義務付けられている。こうした職員からの報告は、図 4-2-g に示すように、継続的評価を有効なものとするために役立つ。

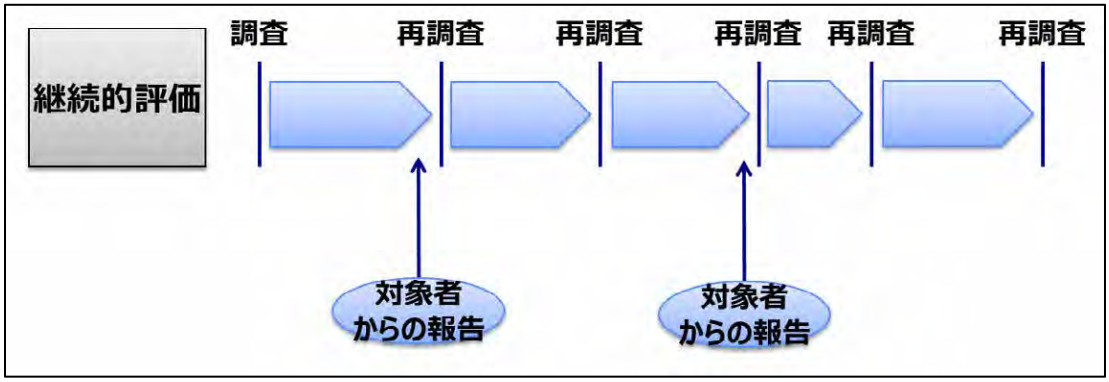


図 4-2-g 報告要件が役立つイメージ

- 相互信頼と信頼の伝達

他の労働力と同様、政府の職員や請負業者は、時間の経過とともに職を変える。政府は、人材を審査する際にかなりのリソースを費やすため、ある機関（または政府プログラムに携わる請負業者）で行われた信頼の決定を、その個人が別の機関で信頼される立場になったときに認識することは、政府の利益となるのである（図 4-2-h）。このプロセスは、信頼の移転と呼ばれ、次のようないくつかの形態がある。ある機関の政府職員が別の機関の職員になる、ある政府プログラムに従事している契約者が別の政府プログラムに従事するために再配置される、契約者が自分の会社を辞めて政府職員になる、政府職員が政府プログラムのための仕事をする会社に勤めるために政府を離れるなどである。

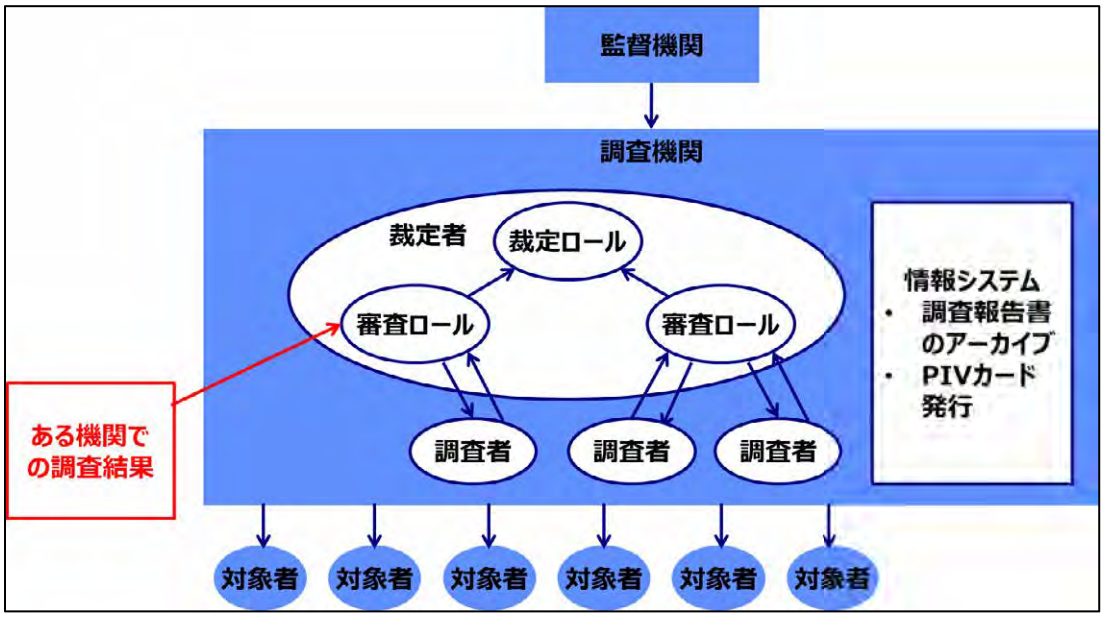


図 4-2-h 信頼の移転のイメージ

7. 人事考課の予算上の留意点

以下は、人事考課プログラムを開発する際に考慮すべき重要な予算と資金調達の項目である。これらの項目は、米国の制度における既知または推定コストに基づく。

- 調査

これは、機密または極秘情報へのアクセスのための資格に関する裁決を通知するために関連情報を収集する審査プロセスの部分である。国防総省防諜安全保障局は、米国政府で最大の統合調査機関である。米国政府の職員、請負業者、その他の関連会社に対する調査の約 95%を実施している。DCSA は、その調査機能を運転資金によって運営しており、以下の費用は、顧客機関への請求価格 に基づいている。この価格設定には、調査要員およびインフラ（施設、IT、機器、車両など）の全費用が含まれる。

調査 1 件あたりの 2024 年のコスト予測。

- ハイティア（トップシークレットまたはパブリックトラスト） - 5,190 ドル
- ミドルティア（秘密または適性） - 715 ドル
- ローティア（クレデンシャル） -180 ドル

- 開始と裁定

これは調査のフロントエンドとバックエンドである。開始は、機関が調査の対象となる候補者を特定し、行動を開始するプロセスである。裁定は、調査結果に基づいて、機関が適格性または適性を最終的に判断す

るプロセスである。米国の制度では、この 2 つの活動は、各雇用機関によって個別に実施され、資金が提供される。さらに、クリアランスの判定によっては拒否されることもあり、また既存のクリアランスの中には理由があって取り消されることもあるので、各機関は不服申し立てプロセスを計画し、予算を立てる必要がある。これらの費用は、依頼する機関の規模によって異なるが、現在の経験に基づく推定では、上記の調査費用に 10〜20%上乗せされると思われる。調査と裁定の両方を中央の組織に組み込むことで、ある程度の節約になる可能性がある。

米国の国家安全保障環境では、職員の審査にかかる費用は政府のみが負担する。産業界は、人事調査のための調達と支払いを行うことは許可されていない。これは主に、1) 産業界が調査プロバイダーに追加要件をいっぱいにさせ、政府のリソースで処理できる量を超えてしまうことが懸念される、2) 誰かのクリアランスを開始するかどうかは、本質的に政府の決定である、3) クリアランスにかかる費用は政府が吸収し、通常契約には含まれない、などの理由による。

8. 結論

本節は、日本における人事評価制度の構築、整備、実行のための有効な根拠と枠組みを提供するものである。信頼の裏切りによるリスクは現実のものであり、国家、経済、社会の各分野にわたって対処されるべきものである。このプログラムのための権限を与える法律の制定は、この努力の成功のための重要な触媒となるであろう。

第３節 データ区分フレームワーク

本節では、日本の国益を守るために特定の情報を機密として保持するための、データ区分のフレームワークについて述べる。

1. エグゼクティブサマリー

敵対者は、国家の防衛や経済的な優位性を高めるために開発された機密情報や技術を発見、収集、利用する機会を常にうかがっている。すべてのものを同じレベルで保護する必要があるわけでも、保護できるわけでもないことを理解した上で、機密情報を明確に特定し、その潜在的な損失のリスクと影響を理解し、そのデータに対して優先順位をつけた保護スキームを開発することが重要である。このようなプログラムは、今日の日本のインフラでは広く開発されておらず、受け入れられていない。プロトコルがないため、政府や業界の関係者は、意図的・偶発的な暴露や侵害から情報を保護する方法について十分な指針を得られないままとなっている。

日本にとって、国家、経済、社会の優先事項を保護するためには、これらの優先事項の成功に不可欠な情

報と技術を保護する必要がある。このような努力の基礎となるのは、重要な情報および技術の要素を特定し、リスク値を割り当てること、つまり本質的にはセキュリティ区分システムであり、これにより保護システムに情報を与え、定義することが義務付けられることであろう。このようなプログラムは、国家資産の保護に向けた国家的な取り組みとして展開されれば、その効果は大きく高まるだろう。同時に、企業も自社の専有情報や技術を特定し、保護するための同様のプログラムを企業規模で開発することを検討する必要がある。

日本の国益を守るためには、特定の情報を機密として保持し、権限を与えられた関係者の間で安全に共有することが必要である。この区分の枠組みは、日本の国民、利益、制度、国家安全保障、および同盟諸国との交流を保護することのみを目的として設定される。

2．フレームワーク概要

この推奨されるフレームワークは、日本政府および関連省庁の管理下にある国家安全保障およびその他のクラスの情報を区分し、保護し、機密指定を解除するための統一的なシステムを説明するものである。最初のステップは、このプログラムのための権限を定義することである。この権限は首相官邸にあり、監督責任は内閣レベルの省庁にあることが推奨される。この提言には 2 つの例がある。米国（US）の情報区分システムは、国家安全保障法（1947 年）にそのルーツがある。これは政府全体で統合された最初の区分の枠組みであり、第二次世界大戦中の情報保護と共有に関する教訓と課題に対応して策定されたものである。その権限は行政府にあり、省庁レベルで実行され、国立公文書記録管理局の一部門である情報セキュリティ監視局（ISOO）が監督している。同様に、イギリス（UK）のシステムは、1911 年に制定された Official Secrets Act（公的秘密法）に端を発し、最近では 1989 年に更新されている。英国のプログラムは陛下の政府の下にあり、実行は内閣府によって行われる。

このフレームワークの多くは米国の区分システムに基づいているが、効率化のために 3 段階（最高機密、機密、極秘）から 2 段階（最高機密、極秘）に引き下げられている。この削減案は、米国や他の国々が 3 段階の国家安全保障区分システムを管理した経験に基づいている。米国では、機密と秘密の資料保護については、審査プロセス、物理的セキュリティ、サイバーセキュリティの要件が実質的に同じである。英国の制度では、国家安全保障の正式なレベルはトップシークレットとシークレットの 2 つだけで、このことを認識している。オーストラリアもこの方向で動いている。プログラムの実行において、国家安全保障情報を 2 つのレベルに圧縮することで、複雑さを軽減し、セキュリティプログラムのすべての側面で効率とコスト削減の両方を実現することができる。

同時に、米国と英国はそれぞれ、国家安全保障情報の閾値を満たさない機密情報を認識し、保護するためのプロトコルを備えている。米国では、それは CUI（Controlled Unclassified Information）と呼ばれるものである。英国では、政府公式情報（Official Government Information）となっている。このアプローチでは、広く共有しない行政情報や個人情報を特定し、カタログ化し、保護要件を定めている。

また、経済安全保障と産業情報の保護についても懸念がある。この文書で推奨するプロセスは、産業環境における国家安全保障情報の保護要件を対象としている。企業独自の情報や機密性の高い企業戦略情報は多岐にわたるため、この推奨プロセスは企業環境には容易に適応できない。我々は、企業が組織内でこのフレームワークを検討し、さらに、重要な情報を保護するために利用可能な物理的およびサイバー的なツールや標準を活用することを推奨する。

本節は、マルチレベルの国家安全保障区分システムを構築するためのガイドを提供するものであるが、複雑な情報管理システムへの移行は、多大な労力を要することがある。移行を簡素化するために、日本では段階的な導入アプローチを検討することが推奨される。中央当局は、政府情報を国家安全保障上の機密（および機密と指定）と公的機密（および公式または内部と指定）に分けることによって、システムを開始する必要がある。国家機密のカテゴリーには、国家安全保障に不可欠とみなされるもの、および紛失すると国家安全保障計画に明らかな損害を与えるものすべてを含めるべきである。このプロセスを成功裏に開始し、経験を積んだ後、各省庁は、広範な秘密カテゴリーを、より個別な最高機密と秘密区分の決定へと絞り込むべきである。最終的に、これは 3 段階の情報保護の枠組みをもたらすことになる。最終的には、トップシークレット、シークレット、オフィシャルという 3 段階の情報保護の枠組みになる。

3．フレームワーク目次と注釈

これは、フレームワークのドラフトを構成する各セクションの概要を説明し、各セクションの目的を説明するためのものである。

パート 1：日本版データ区分体系（案）

セクション 1.1　基準
本セクションでは、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について述べる。これには、情報が不正に開示されることによって損害が生じる場合は機密扱いされるという前提が含まれる。

セクション 1.2　レベル
本セクションでは、保護が必要な国家安全保障情報に対して、3 段階の区分を定義する。

セクション 1.3　権限
本セクションでは、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定めている。また、そのような職員は、これらの責任について定期的な訓練を受ける必要があることを定めている。

セクション 1.4　カテゴリー

本セクションでは、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している。これは米国の制度が使用している区分のリストを適応したものである。日本政府は、国土安全保障省の経験と既存の慣行に基づき、国土安全保障省と協議の上、そのリストを作成・精緻化することが望ましいと思われる。

セクション 1.5　期間

本セクションでは、情報の機密解除の権限と、機密解除が行われる条件について説明する。

セクション 1.6　識別と表示

本セクションでは、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について説明する。これは米国のシステムを参考にしたものであるが、第 1.2 項で説明した 2 段階システム案に準拠する。

セクション 1.7　手引き

本セクションでは、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として、従業員に提供するかについて説明する。

セクション 1.8　ガイダンスの適用

本セクションでは、作業レベル担当者が、彼ら自身はもともと情報を区分する権限がないにもかかわらず、どのように機密資料を作成し、取り扱うかについて説明する。

セクション 1.9　機密情報の共有と保護

本セクションでは、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を提供し、「write to release」の概念を紹介する。

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

本セクションでは、経歴調査や職務に関連した知る必要性など、個人が機密情報へのアクセスを許可されるための要件について述べる。また、そのような人が従わなければならない安全な取り扱いと保管の手順についても説明する。

セクション 2.2　普及のためのコントロール

本セクションでは、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について説明する。

パート 3：実施と見直し

セクション 3.1　一般的な責任

本セクションでは、日本の区分システムの実施を担当する職員の責任について説明する。

セクション 3.2　説明責任と懲戒処分

本セクションでは、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する。

パート４：コスト

本パートでは、費用について簡単に説明する。

パート５：まとめ

本パートでは、結論となる考えを述べる。

4．パート１：日本版データ区分のフレームワーク（案）

セクション 1.1　基準

(a)情報は、以下の条件をすべて満たす場合にのみ、最高機密または機密レベル（セクション 1.2(a)を参照）に区分することができる。

(1)権限を与えられた区分担当者が情報を区分する。

(2)その情報が日本政府によって所有され、日本政府のために作成され、または日本政府の管理下にある場合。

(3)このフレームワークの 1.4 節に記載されている情報のカテゴリーの一つ以上に該当すること。

(4)権限のある区分担当者が、情報の不正な開示が国家安全保障に損害を与えることが合理的に予想されると判断し、かつ、権限のある区分担当者がその損害を特定または説明できる場合。

(b)情報を区分する必要性について重大な疑念がある場合、その情報は区分されないものとする。

セクション 1.2　レベル

(a)情報は、以下の 2 つのレベルのいずれかに区分されることがある。

(1)「最高機密」は、不正に開示されることにより日本の国益または国の安全が著しく損なわれることが合理的に予想される情報で、権限を与えられた区分担当者が特定または説明できるものに適用されるものとする。

(2)「秘密」は、不正に開示されることにより日本の国益または国の安全が損なわれることが合理的に予想される情報で、権限を有する区分担当者が特定または説明できるものに適用される。

(b)法令に別段の定めがある場合を除き、日本の機密情報を識別するために、他の用語を用いてはならない。

(c)適切なレベルの区分に重大な疑義がある場合は、より高いレベルで区分されるものとする。

セクション 1.3　権限

(a)情報を区分する権限は、以下に限定して行使することができる。

(1)内閣レベルの国家安全保障局（NSS）構想の事務局長に就任した。

(2)外務省、国防省、国家安全保障局長の各長官、および。

(3)本項(c)に従ってこの権限を委任された日本政府の職員。

(4)基準 1、2 又は 3 に該当する職員は、日本国民でなければならず、上記 2 又は 3 により委任又は指定された職員は、区分権者としての役割を果たす組織の事項に関し、明白な資格及び経験を有する者でなければならない。

(b)情報を区分する権限のある職員は、あらゆるレベルの区分を行う権限を有する。

(c)区分の権限を委譲する。

(1)区分権限の委譲は、この枠組みを運用するために必要な最小限のものに限定されなければならない。権限を与えられた区分担当者は、委任された下位の職員が、この権限を行使する実証的かつ継続的な必要性を有することを確認する責任がある。

(2)区分の権限の委任は、それぞれ文書で行わなければならず、本規定に定める場合を除き、その権限を再委任してはならない。各委任は、氏名又は職名により職員を特定しなければならない。

(d)すべての区分担当者は、適切な区分と機密解除に関する研修を受けなければならない。

セクション 1.4　カテゴリー

(a)情報は、その不正な開示が、本命令の 1.2 項に従って、日本の国益又は国の安全保障に識別可能又は記述可能な損害をもたらすことが合理的に予想される場合でなければ、区分の対象となるものとみなしてはならない。

(b)この枠組みは、日本の国家安全保障を保護するために情報を区分することと、その他の省業務の遂行に関連する、国家安全保障以外の利益のために区分することを区別する。国家安全保障情報の保護、取り扱い、共有、機密解除にのみ適用される具体的な慣行は、この枠組み全体を通じて規定される。このため、国家安全保障に関連する情報の特定のカテゴリーは、以下の 1 つ以上を含むものとして定義される。

(1)日本当局が検討している審議事項。

(2)軍事計画、兵器システム、または作戦。

(3)国の安全保障に関わる外国政府の情報。

(4)情報活動、情報源や情報方法、暗号学。

(5)日本国の外交関係または対外活動（秘密情報源を含む）。

(6)国家安全保障に関連する法執行情報。

(7)国家安全保障に関連する科学、技術、または経済的な事項。

(8)国家安全保障に関連するシステム、施設、インフラ、プロジェクト、計画、または保護サービスの脆弱性または能力。

(c)国家安全保障業務に関する区分の定義については、各省庁の権限に委ねられる。各省庁の長は、このような指定に関する最終的な権限を持つ。

セクション 1.5　期間

(a)情報を機密解除する権限は、その情報が国家安全保障上の理由で機密化されているか、あるいは、セクション 1.4 で詳述されているように、省庁が行う国家安全保障以外の業務で機密化されているかによって決まる。国家安全保障上の機密情報の場合。

(1)NSS のみが、セクション 1.4(b)に記載されているように、国家安全保障上の理由から区分されていた記録、文書、その他の資料の機密を解除することができる。

(2)情報は、1.1 項の区分の基準を満たさなくなったとき、あるいは NSS の判断により、公共の利益が情報保護の必要性を上回ったときに、機密解除可能であるとみなされる。

(3)情報は、本セクションに従って機密解除が命じられるまで、機密のままでなければならない。

(4)機密情報は、NSS が決定した場合のみ公開される。

(5)閣僚は、NSS に国家安全保障情報の機密解除を要請することができる。要請は NSS のスタッフを通じて行われ、NSS のスタッフは、NSS に問題を提示し決定する際に、すべての省庁の公平性を考慮することを保証する。

(b)省庁が行う国家安全保障以外の業務案件の場合。

(1)セクション 1.4 に記載されているように、国家安全保障以外の理由で区分された記録、文書、その他の資料の機密解除は、省庁の長のみが行うことができる。

(2)情報は、セクション 1.1 の区分の基準を満たさなくなったとき、又は省令で定めるところにより、公共の利益が情報の保護の必要性を上回ったときに、機密解除可能であるとみなされるものとする。

(3)情報は、本セクションに従って機密解除を命じられるまで、機密扱いのままであること。

(4)機密扱いの情報は、省庁の長が決定した場合のみ公開される。

セクション 1.6　識別とマーキング

(a)資料が最初に区分された時点で、NSS が発行する指示に従い、以下の事項を一目でわかるように表示しなければならない。

(1)本パートのセクション 1.2 に定義された 3 つの区分レベルのうちの 1 つを指す。

(2)権限のある区分担当者の名前と職位、または個人識別情報による身元。

(3)特に明記されていない場合は、原産省および原産地。

(4)セクション 1.4(b)項の該当する区分項目、または本省固有の主題領域のいずれかを引用した、簡潔な区分理由。国家安全保障上の理由が引用される場合、文書の表示において、セクション 1.4(b)のサブパラグラフを明示するものとする。

(5)適用可能な普及コントロール（セクション 2.2 に記載）。

(b)各区分された文書に関して、その文書を作成した省は、マーキングまたはその他の手段により、どの部分が区分され、どの部分が非区分であるかを示すものとする。

セクション 1.7　手引き

(a)区分ガイドとは、区分を必要とする個々の情報要素を特定する、当初の区分決定の記録である。組織

内で標準化され、使用されることにより、情報の適切かつ均一な区分が可能になる。
(b) NSS は、権限のある区分担当者に区分ガイドの適切な作成方法を指導するためのマニュアルを発行するものとする。
(c)権限ある区分担当者は、自らが権限を有する情報のための区分ガイド（又はガイド）を作成しなければならない。　これらのガイドは、NSS が発行したマニュアル及び上級省職員が定めた関連する省内手続きに従わなければならず、少なくとも年 1 回は最新の状態に保たなければならない。NSS は、すべての区分ガイドのための中央保管庫を維持しなければならない。

セクション 1.8　ガイダンスの適用
(a)機密情報の保有者は、機密情報を含む文書の作成、編集、複製、要約、またはその他の作業を行う際に、区分ガイドのすべての指示を参照し、これに従わなければならない。このような保有者は、NSS が提供するガイダンスに従って区分記号を適用しなければならない。
(b)区分記号を適用する者は、以下を行わなければならない。
(1)各区分の派生的な行動において、氏名と職位、または個人識別情報によって、すぐにわかるように識別されること。
(2)権限のある区分担当者の決定を遵守し、尊重すること。
(3)新たに作成された文書には、原文にある適切な区分記号を適用する。
(c)機密情報の保有者は全員、その適切な運用に関する訓練を受けなければならない。

セクション 1.9　機密情報の共有と保護
(a)機密文書または資料は、最も広範な普及と利用を保証するために、可能な限り低い区分レベルで作成されるものとする。より高い保護が必要な機密情報は、アクセスを適切に管理するための配布コントロールを使用する、より高いレベルで区分された文書または添付資料で提供されるものとする。
(b)より広範な情報共有が必要な場合、職員は必要に応じて機密情報を排除し、より低い機密、あるいは非機密の文書を作成し、利用者に有用な情報をできるだけ低いレベルで提供する「ライティング・トゥ・リリース」を行う。

5．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
(a)ある者は、次の条件を満たせば、機密情報にアクセスすることができる。
(1)人事課による調査及び人事課からの勧告を受け、アクセス資格の有利な決定が省庁によってなされた場合。
(2)その人が承認された秘密保持契約に署名していること。
(3)そのような決定に責任を負う省庁の上級職員によって決定された、その情報を知る必要がある人。
(b)本セクション(a)の機密情報へのアクセス基準を満たした者は、機密情報の適切な保護に関する訓練を受けなければならない。

(c)日本政府の役人または職員は、政府の管理下から機密情報を取り除くこと、または政府の管理下から取り除くために情報の機密解除を指示することはできない。
(d)機密情報は、適切な許可なく日本政府の公式施設から持ち出すことはできない。
(e)NSS 外で機密情報を発信する権限を有する者は、NSS 内で提供されるのと同等の方法で、情報の保護を確保するものとする。
(f)NSS は、機密情報を収集、作成、通信、計算、配布、処理、保管するネットワークや電気通信システムを含む自動情報システムに対して、統一された手順を確立しなければならない。
(1)不正なアクセスを防止する。
(2)情報の完全性を確保すること、および
(3)以下を実務上可能な限り使用する。
(A)認可された利用を促進する形式と方法で、情報の利用可能性とアクセスを最大化する共通の情報技術標準、プロトコール、インターフェース
(B)本パートのセクション 2.1(a)に記載されている基準を満たす人が情報に最大限アクセスできるように、標準化された電子フォーマット。
(g)NSS は、機密情報が適切な保護を提供し、無権限者によるアクセスを防止する条件下で使用、処理、保管、複製、伝送、破棄されることを保証するために、物理的及び技術的なセキュリティ管理を確立しなければならない。
(h)機密情報の権限保持者である要員は、外国政府の情報を、その情報を提供した政府または政府の国際組織が要求する保護と少なくとも同等の程度を提供する基準に基づいて保護しなければならない。
(i)NSS に由来する機密情報は、本枠組みのセクション 2 に基づくアクセスと保護に関する基準を満たす限り、他省庁に広めることが可能である。

セクション 2.2　普及のためのコントロール
(a)機密文書を作成する場合、その文書を受け取ることができる者または受け取ることができない者に関する制限は、承認された配布管理マークを使用することにより、文書上に明確に示されるものとする。例としては、以下のようなものがある。
NODIS=省外への配布禁止
NOFORN=日本人以外の職員への配布禁止
ORCON=発信者管理、受信者は発信元の省庁に相談することなく文書を再配布してはならない、など。
(b)NSS は、承認された配信制御マーキングのマニュアルを発行し、当該マーキングが標準化され、政府全体で統一的に使用されることを確保するものとする。
(c)上級省職員は、本命令のセクション 2.1(a)に規定された基準を満たす個人が、機密情報に最大限アクセスできるようにするための手続きを確立するものとする。
(d)緊急事態において、人命に対する差し迫った脅威に対応するため、または国土防衛のために必要な場合、事務局長またはその指名する者は、機密情報（本枠組みのセクション 2.1（i）に従ってマークされた情報を含む）を、通常アクセス権を持たない個人または個人に開示する権限を付与することができる。本規定に基づき開示された情報は、当該開示またはその後の受領者による使用の結果、機密解除されたと

はみなされないものとする。このような開示は、機密情報の発信者に速やかに報告されるものとする。

6．パート３：実施と見直し

セクション 3.1　一般的な責任

機密情報を発信または取り扱う省庁の長は、以下を行う。

(a)このフレームワークで確立されたプログラムを成功裏に実施するために、上級管理職が個人的なコミットメントを示し、コミットすること。

(b)日本の安全保障上の区分プログラムを効果的に実施するために必要な資源を投入する。

(c)省内の記録システムが、機密情報の適切な共有と保護を最適化するように設計され維持されるようにすること、及び

(d)セキュリティ区分プログラムを指揮・管理する省政府高官を指名し、その責任には以下が含まれるものとする。

(1)NSS が発行するポリシーマニュアルに定められた基準にすべての要素が合致していることを確認するため、省内の区分プログラムを監督すること。

(2)省職員向けの実施規則を発行すること。そのような規則は、NSS と協議の上、作成されるものとする。

(3)省庁のセキュリティ区分ガイドの制作を統括する。

(4)セキュリティ教育・訓練プログラムの確立と維持。

(5)継続的な自己点検プログラムを確立し、維持すること。このプログラムには、同省の区分行動の代表的なサンプルの定期的な点検を含む。

(6)NSS と協働して、区分システムの適切な運用を確保する。

(7)機密情報への不要かつ／または不正なアクセスを防止するための手順を確立すること。

(A)管理上のセキュリティクリアランス手続きを開始する前に、機密情報へのアクセスの必要性を確立することを要求すること。

(B)機密情報へのアクセスを許可された人数が、省内のミッションの必要性を満たすようにすること。

(8)敵対的または潜在的な地域で使用される機密情報を保護するための特別な緊急時対応計画を策定すること。

(9)政府職員を評価するために使用される年次業績評価システムが、以下の職員に対する機密情報の適切な取り扱いに関する評価を含むことを確保すること。

(A)権限を持った区分担当者

(B)セキュリティ管理者またはセキュリティ専門家

(C)その他、機密情報にアクセスできるすべての人員。

(10)省内で区分の責任を与えられた職員が、その職員が区分の責任を持つことになる事項に関して、明白な資格と経験を有していることを確実にすること。

セクション 3.2 説明責任と懲戒処分説明責任と懲戒処分

(a)日本政府の機密情報へのアクセスを許可された者は、故意または過失により適切な懲戒処分の対象となる。

(1)この命令または前任の命令の下で適切に区分された情報を、権限のない者に開示すること。

(2)本枠組みまたは実施指令に違反して情報を区分または区分を継続すること。

(3)本フレームワークの要件に反して、特別なアクセスプログラムを作成または継続すること。

(b)制裁には、譴責、無給の停職、解任、区分権限の終了、機密情報へのアクセスの喪失または拒否、または適用される日本の法律および方針に従ったその他の制裁が含まれる場合がある。

(c)大臣または上級省職員は、少なくとも、本命令の区分基準の適用において無謀な無視または誤りのパターンを示す個人の区分権限を速やかに削除しなければならない。

7．パート４：コスト

この活動には、NSS の少人数のスタッフと、国の区分システムを確立し維持するための各省庁の追加職員が必要である。より正確な数字は、どの省庁が区分の権限を持つか、またどの情報を区分するかという決定によって決まる。より大きなコストは、職員の審査活動と情報システムの安全性報告書にかかるものである。

8．パート５：まとめ

この国家安全保障区分システムの提案は、当然ながら非常に複雑であるが、いったん情報が適切に識別・区分されれば、そのマークは、情報の相対的重要性と機密性、および不正な放出や開示から情報を保護する責任について、情報利用者に最初に通知する役割を果たすことになる。区分システムの開発と維持における厳密さは、省庁間および産業界全体における情報サービスの開発者と提供者に情報を提供する上で重要である。

第４節 技術開発フレームワーク

1．エグゼクティブサマリー

敵対者は、常に人間関係を構築し、機密情報や技術を発見、収集、利用する機会を狙っている。日本政府が包括的な審査プロセスを通じて政府全体の信頼できる人材を確立するのに伴い、政府はその審査をサポートするための技術システムを開発する必要がある。物理的およびデジタル的な識別、認証、アクセスの承認を提供する標準化されたクレデンシャルが最重要である。さらに、政府全体の日本式区分システムの確立に伴い、政府は、個人のクリアランス審査を支援し、適切な区分レベルの機密情報を相応の保護付きで作成、処理、保管するための技術システムを開発する必要がある。

日本の国益を保護するためには、ID 認証およびポリシー・ベースの認可決定を提供することによって、機密情報および施設の基礎的な保護を促進するために、政府全体のクレデンシャルが必要である。この区分の枠組みは、日本の国民、利益、制度、国家安全保障、および同盟国との交流を保護することのみを目的として確立されている。

2．フレームワークの概要

推奨される枠組みは、人員の吟味、区分のための統一システム、および ID、認証、認可のための政府全体のクレデンシャル・システムの確立を支援する技術的な開発について述べている。最初のステップは、プログラムの権限を定義し、包括的な標準と方針を確立することである。人事審査および区分システムのための技術開発は、これらのプログラムの標準、方針、および実行の確立と入れ子になっていなければならない。

日本政府のための ID、認証、および承認システムを含む国家クレデンシャル・システムの確立は、 関連する技術開発と密接に関連している。日本がこの国家プログラムを確立するとき、この権限を首相官邸に発し、監督責任を閣僚レベ ルの省庁に持たせることが推奨される。米国（US）のクレデンシャル標準は、個人識別検証（PIV）クレデンシャルと呼ばれ、2004 年の国土安全保障 大統領指令 12 号（HSPD-12）によって連邦政府内または連邦政府と働く個人向けに確立され、政府 全体の ID、認証および承認システムを提供している。

本書の標準および政策の枠組みの多くは、米国のクレデンシャル・システムに基づいている。これは、米国立標準技術研究所（NIST）が発行した連邦情報処理標準出版物 201-2（FIPS 201-2）の技術的強度と国際的採用により、ID 証明、登録、発行および相互運用性を含む、PIV クレデンシャルのアーキテクチャと技術標準が確立されているためである。さらに、米国で使用される PIV クレデンシャルは、1）物理的識別と認証、および 2）非区分政府ネットワークおよびサービスでのハードウェアに裏付けられたデジタル識別と認証の両方を達成する。スタイルおよび具体的な実装に若干の違いがあるが、同じ FIPS 201-2 標準が多数の国際的パートナーによって採用され、NATO 軍人のジュネーブ条約準拠クレデンシャルにも使用されている。

また、経済的安全性および産業情報の保護に対する懸念も存在する。この文書で推奨するプロセスは、産業環境における国家安全保障情報のクレデンシャル要件を対象としている。企業は、組織内でこの枠組みを検討し、さらに重要な情報および重要な施設を保護するために利用可能な物理的およびデジタルクレデンシャルの枠組みのツールおよび標準を利用することを推奨する。

この文書は、マルチレベルの国家安全保障クレデンシャル・システムを構築するためのガイドを提供するものであるが、その実施には多大な努力が必要である。移行を単純化するために、日本は段階的なアプローチを考慮することが推奨される。中央当局は、最も機密性の高い情報および施設から始めて、クレデンシャル化、物理的および論理的アクセス制御の両方の展開を順次行うことによって、システムを開始すべきである。最終的には、物理的および論理的アクセスの両方に強力な識別、認証、および承認メカニ ズムを与える包括的なクレデンシャル・システムに帰結することになる。

3. クレデンシャルの原則

これは、クレデンシャル用語の概要とそれらに関連する定義を提供し、曖昧さをなくし、フレームワーク全体の一貫性を確立するためである。

(1) アイデンティティ

この報告の目的では、ID は個人が一意に認識できる物理的および行動的特性の集合である。ID の証明とも呼ばれる ID の検証、および信頼とリスクの判断に使用される明示（ポリシー、プロセス、技術）は、検証および信頼された後にその ID の真正性を認証するために使用されるメカニズム とは異なり、別個のものである。

(2) 認証

認証は、真正性の信頼を確立するプロセスである。この場合、人の ID およびその物理的またはデジタルクレデンシャルの検証においてである。クレデンシャル（PIV または運転免許証など）は、「信用または権限に対する自分の権利を証明する証拠、および ID（およびオプションで追加属性）をその個人に権威的に結びつける個人に関連するデータ要素」である。

認証は、3 つの要因の組み合わせに依存する。1) 個人が認知しているもの（パスワードなど） 2) 個人が所有しているもの（バッジ、電話番号、電子メールアカウント、暗号鍵など） 3) 個人の生体的な証し（指紋などの生体データなど）である。 認証プロトコルは、より安全でユーザーフレンドリーな標準に進化し続けている。

物理的認証は、最も一般的には ID バッジで実装される。バッジの中には、視覚的認証のみを提供するものもあるが、磁気ストリップ、無線周波数識別（RFID）パッシブ認証、バーコード、集積回路チップに格納された暗号キーなど、追加の認証メカニズムを持つものが多い。

最も一般的なデジタル認証は、「あなたが知っている何か」としてパスワードを使用することに変わりはない。ユーザー名と組み合わせた場合、ほとんどのシステムやウェブサイトでは、これがデフォルトになっている。

多要素認証は、しばしば MFA または 2 要素認証の 2FA と呼ばれ、2 つ以上の要素を使用して、セキュリティと真正性の信頼性を向上させるものである。公開鍵基盤（PKI）暗号を使用する MFA は、クレデンシャルの真正性を数学的に検証するメカニズムを提供し、セキュリティが重要なアプリケーションでよく使用される。

X.509 公開鍵暗号化標準は、認証用の暗号クレデンシャルを生成するために一般に使用される。X.509 証明書は、認証局によって署名されるか、または自己署名されるデジタル署名を使用して、ID を公開かぎと暗号的に結合する。証明書が信頼できる認証局によって署名されるか、または他の手段によって検証されると、証明書および対応する公開鍵は、他の当事者との安全な通信を確立したり、対応する秘密鍵によってデジタル署名された文書を検証するために使用することができる。X.509 のライフサイクルには、4 つの重要なステップがある。

·登録 - 認証局がユーザーのために証明書を発行する前に、ユーザーが直接または（認証局から委任された）登録機関を通じて、認証局（CA）に自己を明らかにするプロセス。

·初期化 - クライアントが、インフラストラクチャ内の他の場所に保管されている鍵との適切な関係を持つ鍵材料をインストールするプロセス。例えば、クライアントは、証明書パスの検証に使用するため、信頼できる認証機関の公開鍵及び その他の保証情報とともに安全に初期化される必要がある。クライアントは通常、自身の鍵ペアで初期化される必要がある。

·認証 - CA がユーザーの公開鍵に対する証明書を発行し、その証明書をユーザーのクライアントシステムに返却し、その証明書をリポジトリに掲載するプロセス。

·失効 - 証明書が失効または無効にされ、証明書とシリアルナンバーが一般に公開されている証明書失効リスト（CRL）に追加されるプロセスである。証明書は発行されたとき、その有効期間中ずっと使用されることが期待されている。しかし、様々な事情により、証明書が早期に無効となることがある。

Fast Identity Online 2 (FIDO2) は、FIDO アライアンスの最新仕様の包括的な用語で、モバイルとデスクトップ環境の両方でオンラインサービスを容易に認証するために、一般的なデバイスを活用するように設計されている。FIDO プロトコルは、X.509 などの標準的な公開鍵暗号を使用し、より強力な認証を提供する。オンラインサービスに登録する際、ユーザーのクライアントデバイスは新しいキーペアを作成する。秘密鍵を保持し、公開鍵をオンラインサービスに登録する。認証は、クライアントデバイスがチャレンジに署名することで、秘密鍵を所有していることをサービスに証明することで行われる。クライアントの秘密鍵は、ユーザーによってデバイスのローカルロックが解除された後でのみ使用できる。ローカルロック解除は、指のスワイプ、PIN の入力、マイクへの発話、セカンドファクターデバイスの挿入、ボタンの押下など、ユーザーフレンドリーで安全な操作で実現される。

(3) オーソライズ

認証とは、NIST SP 800-162 に概説されているように、認証されたユーザーに対して以下のような特定の要求を許可または拒否するために使用される一連のポリシーおよび属性である。1) 情報および関連情報処理サービスの取得と使用、2) 特定の物理的施設（建物や軍事基地など）への立ち入りなど。

アクセス制御の判断は、1) 採用時など一度だけ、2) 定期的に、3) 個別に行うことができる。1) 個人の採用時など一度だけ、2) 機密情報へのアクセスのための「適格性」判断など定期的に、3) 建物へのバッジやウェブサイトへのログインなどリクエストごとに判断されるような個別的な場合である。アクセス制御の実装は、ポリシーや標準的な慣行に基づき、その決定を行うために必要なリクエストと認証に固有のものである。この報告では、アクセス制御の実装を詳しく説明しない。アクセス制御の実装は多数あり、微妙に異なる。物理的なアクセスに対する認証が標準化されていても、米国の省庁は、個々の施設や部屋に対して個別にアクセス制御の決定を行うことが多い。

4．パート１：人事考課を支援する技術開発

政府全体の人事審査を確立するためには、必要な情報の収集、資格証明書、適性、および資格判定をサポートする技術システムを開発する必要がある。技術システムは、人事考課をサポートするためにいくつかの機能を実行しなければならない。

(a)国の方針で、候補者が自分自身について提供することが要求されている、または認められているすべての情報を収集する。

(1)テキスト入力、画像、文書のスキャン、転写など、さまざまな種類の情報を必要とすることを考慮する必要がある。

(2)候補者一人ひとりの個人情報は、安全に保護・保管されなければならない。

(3)必要な情報を集めて入力するのは面倒なので、入力システムは、候補者が意図的に完成したパッケージを提出するまで、すべての情報を下書きとして保存しておく必要がある。

(4)情報の入力は、個人のアイデンティティと安全な認証メカニズムに結びつけられるべきである。

(b)必要な身分証明情報を取得する。

(1)パスポートや運転免許証などの身分証明書との相関性について、国家政策を満足させるに足る情報を保存する。

(2)指紋、網膜スキャン、顔画像、DNA、声紋など、国の政策で必要とされる生体情報を取得する。

(c)素行調査の結果を記録する。

(1)要求される様々な種類の情報と報告を考慮しなければならない。

(2)ほとんどの調査は、インタビュー、物理的な場所の訪問、デジタル記録へのアクセスを伴うため、システムはモバイルと定置のユースケースとインターフェースを考慮する必要がある。

(3)調査員は多くの候補者の機密情報にアクセスすることになるため、強力な認証と承認が重要になる。

(d)候補者情報を提供するデジタルシステムとのインターフェース。

(1)可能な限り、国の政策で必要とされるデジタル記録の収集は自動化されるべきである。

(2)金融信用調査、成績表、警察記録、軍歴、納税記録、係争中の訴訟などは、自動プログラミングインタフェース（API）を通じて容易にアクセスできるようにする必要がある。

(3)情報がデジタル化されていない、あるいはプログラム的にアクセスできない場合、国の政策として、これらの投資を義務付ける、あるいはインセンティブを与えることを検討する必要がある。

(e)審査員に候補者のすべての情報を確認する手段を提供すること。

(1)候補者の提供、背景調査、個人の記録情報を一貫したユーザーインタフェースで提供し、裁定者による検討をサポートする。

(2)情報が不足している場合、フォローアップのための重要な質問事項の把握や調査タスクを促進する必要がある。

(f)判定結果の記録

(1)裁決の決定と補足情報を把握する。

(2)自動的または人事担当者による候補者通知のトリガー。

(g)申請者および従業員の裁定状況を確認するための一元的なメカニズムを提供する。
(1)権限のある関係者が一元的にアクセスできる、すべての裁決の記録を提供する。
(2)国の方針に従い、裁決に関連する情報を必要なだけ、あるいは最小限に保存する。

5．パート 2：データ区分フレームワークを支える技術開発

セクション 2.1 クリアランス検討のための技術システム

区分フレームワークの実装には、上記の人事審査システムの強化、またはクリアランスの検討のための別のデジタルシステムが必要となる。技術システムは、人事審査に必要な要件に加え、いくつかの機能を果たす必要がある。

(a)国の方針で、候補者が自分自身について提供することが要求されている、または認められているすべての情報を収集する。
(1)人事考課に必要な情報以外に、クリアランスの検討に必要な追加情報を考慮する必要がある。
(2)候補者は、審査とクリアランス検討の両方に同時に情報を提供するか、クリアランス検討システムにデータを取り込み、候補者に正確さを確認する必要がある。

(b)素行調査の結果を記録する。
(1)人事考課に必要な情報以外に、クリアランスの検討のために必要な追加情報および報告を考慮しなければならない。
(2)国の政策に従ったクリアランスの検討は、テーマの範囲と時間軸の両方において、より広範な調査を必要とすると思われる。国の方針で認められている場合、複数の調査員が同時にクライアントを調査することができるため、システムは複数の入力を考慮する必要がある。
(3)システムは、研究者が文脈上隔離されて作業すべきか、同じ候補者を研究している他の研究者の調査結果を見ることができるようにすべきかを検討する必要がある。

(c)審査員に候補者のすべての情報を確認する手段を提供すること。
(1)すべての審査とクリアランスの検討情報を裁定者に提供すること。
(2)検討するために要求された区分レベルを特定する。

(d)判定結果の記録
(1)許可された区分レベルや補足情報など、判定に関する情報を取得する。
(2)自動的または人事担当者による候補者通知のトリガー。
(3)潜在的な利益相反など、特別な配慮が必要な場合は、裁決の一部として把握する。

(e)個人が機密施設、ネットワーク、情報にアクセスする際に、そのクリアランス状況を確認するための一元化されたメカニズムを提供すること。
(1)審査とクリアランスの両方を含むすべての判定記録を提供し、権限のある関係者が一元的にアクセスできるようにする。
(2)適切な権限を持つ政府内のセキュリティ担当者が、個人の現在のクリアランスレベルを検証できるようにする。

(f)従業員からの定期的な更新情報を取得するための手段を提供する。

(1)テキスト入力、画像、文書のスキャン、転写など、さまざまな種類の情報を必要とすることを考慮する必要がある。

(2)候補者一人ひとりの個人情報は、安全に保護・保管されなければならない。

(3)情報の入力は、ID および認証のために個人の政府全体のクレデンシャルに関連付けられるべきである。

(4)個人は更新された新しい情報を提供し、以前に提供した情報の正確性を再度確認する必要があるため、人事審査とクリアランスの検討のために個人が以前に提供した情報を考慮する必要がある。

(g)定期的な再調査を把握するための手段を提供する。

(1)国の政策により再調査が必要とされる範囲とテーマを説明する。

(2)要求される様々な種類の情報と報告を考慮しなければならない。

(3)再調査のためのインタビューでは、本人およびその同僚は機密情報を議論する必要があるため、システムは機密情報を保存する手段、または他のシステムに保存されている情報への参照を提供する手段を備えていなければならない。

(h)個人によるセキュリティ関連情報の継続的な自己申告の仕組みを提供する。

(1)国の政策で要求されるように、個人は海外旅行、海外との接触、または軽蔑的な出来事を自己報告できるようにする必要がある。

セクション 2.2 機密情報システム

現代における機密情報の生産と保管は、一つ以上の機密ネットワークの開発も必要となる。日本の機密情報を作成、処理、保管するために作成された情報システムは、以下の基準を満たさなければならない。

(a)機密情報を処理または保存するシステム（データセンタを含む）は、不正アクセスや不注意による開示から機密情報を物理的に保護する能力が評価された施設または部屋である安全作業区域（SWA）内に収容され、使用される。商業機密用ソリューション（CSfC）モバイルアクセス能力パッケージ（MACP）アーキテクチャおよび要件を満たすデバイスは、ミッション要件を考慮したリスクバランスの決定に基づき、ユースケースと個人が書面で許可された場合、SWA 外で機密情報にアクセスするために使用することができる。

(b)非区分された長距離輸送手段を用いて区分された情報を保護するために、商用国家安全保障アルゴリズム・スイートのハードウェアまたは強力なソフトウェア暗号分離を使用する。

(c)機密情報を保護するために、コンピューティングデバイスとローカルエリアネットワークの物理的な分離を使用する。機密とトップシークレットなどの機密レベル間では、デジタルポリシー決定ポイントによって実施される強力な権限制御を使用して、機密情報を保護し、全体的なコストを削減することができる。

(d)機密ネットワーク、特に 802.11 Wi-Fi または 802.15 Li-Fi のための無線ネットワークの使用は、CSfC MACP デバイスのための非区分および信頼されないトランスポートとして無線ネットワークを使用して許可されるべきである。CSfC デバイスは、機密インフラとこれらの特別に構成されたデバイスの間で層状の暗号化を使用し、無線ネットワーク内の悪用から機密情報を保護する。

(e)適切な日本の標準および参照アーキテクチャに従って開発され、ポリシー決定ポイントを介したポリ

シーの実施として属性ベースのアクセス制御の決定を使用して認可を容易にする。
(f)国の政策要件に基づき、セキュリティ評価、認定、リスクマネジメントを受ける。

6. パート 3 : 日本版クレデンシャルフレームワークの草案

セクション 3.1 政府機関共通のクレデンシャル基準

このセクションは、以下を含む日本の PIV クレデンシャル標準を確立する。
(a)PIV は、連邦機関の職員、連邦機関で働く民間企業の職員、政府プロジェクトに従事する民間企業の職員、政府に商品やサービスを供給し連邦施設へのアクセスを必要とする可能性がある民間企業の職員など、信頼される労働力に対して発行される予定である。
(b) PIV クレデンシャルには、識別および認証のために物理的カードに印刷された 6 つの必須項目がある、具体的には以下の項目である。
(1)写真 - 頭頂部から肩までの正面からのポーズで、解像度 300 ドット/インチ（dpi）以上で撮影すること。
(2)氏名 - 大文字で印字されたフルネーム、苗字、名前の順で記載される。
(3)Employee Affiliation - "Employee", "Contractor", "Active Duty", "Foreign National", "Civilian "など、省庁によって定義された個人の所属先。白が政府職員、緑が請負業者、青が外国人を示し、対応する色のバーと対応するブロック文字（色覚異常者用）が追加される。
(4)個人が所属する機関、部署、または組織。
(5)カードの有効期限 - YYYYMMDD 形式で 1 回、MMMYYYY 形式で右上に大きく太字で 2 回印字されている。
(6)汎用一意カード・シリアル番号-背面に印刷された、PIV クレデンシャルの汎用一意シリアル番号。
(c)PIV クレデンシャルには、物理的識別および認証に使用される 7 つの必須データ・フィールドがある。
(1)カード能力コンテナ - カードの製造およびモデルに関する情報、および様々なアプリケーション間の相互運用性を可能にし、カードが進化する際の後方互換性を提供するために使用される関連データモデルを指定する。
(2)カード保持者固有識別子-技術的実装ガイダンスに従って発行される固有のクレデンシャル 番号。接触型（例 : 集積回路チップ）および非接触型（例 : RFID）インターフェース間で共有されるスマー ト・カード有効物理アクセス制御システムに従って発行された固有のクレデンシャル番号。
(3) PIV 認証用 X.509 証明書 - カードおよびカード所有者を認証するために使用される、FIPS 201-2 に定義される X.509 証明書およびその関連秘密鍵。
(4)カード認証用 X.509 証明書 - 物理的なカードを認証し、アクセスコントロールアプリケーションをサポートするために使用される非対称の X.509 証明書とその関連する秘密鍵。
(5)カード保持者の指紋 - 指紋データオブジェクトは、FIPS 201-2 および NIST Special Publication (SP) 800-76 に従って、オフカード照合をサポートするために、カード保持者の一次および二次指紋を指定する。

(6)カード保持者顔画像-警備員による視覚的認証のため、およびオペレーターが立ち会う PIV 発行、再発行、検証データ・リセット・プロセスにおいて、NIST SP 800-76 に規定される顔画像データオブジェクト。

(7)セキュリティ・オブジェクト - チップに格納されたすべてのファイルのハッシュ値、およびこれらのハッ シュのデジタル署名を、機械可読旅行書類パート 2 の第 IV 章付録 3（出典は ICAO）に従って実装し、中央発行者のデジタル署名によってカードの真正性を確認し、クレデンシャル置換を防止するもの。

(d) PIV クレデンシャルには、具体的には、デジタル認証のための 2 つのデータ・フィールドがある。

(1)デジタル署名用 X.509 証明書 - FIPS 201 に定義される、デジタル署名を目的とした X.509 証明書とそれに関連する秘密鍵。電子署名用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクトインタフェースを介してのみ利用可能である。暗号機能は、電子署名鍵の操作の直前に毎回 PIN を提出し検証しなければならないような「PIN Always」アクセスルールで保護される。

(2)鍵管理のための X.509 証明書 - FIPS 201 で定義された、機密保持を目的とした X.509 証明書とそれに関連する秘密鍵。鍵管理の秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクトインタフェースを介してのみ利用可能である。暗号機能は「PIN」アクセスルールで保護され、一旦 PIN が提出され検証されると、その後の鍵管理操作はそのセッション中に再度 PIN を要求することなく実行できるようになる。

(e)電子署名および鍵管理の証明書は、NIST SP 800-63A に従って証明および登録される必要がある。

(f)中央発行機関は、デジタル認証のための派生 PIV クレデンシャルをプロビジョニングしライフサイクルする能力を提供する。 派生クレデンシャルは、ID 証明プロセスを重複させないように、以前に発行されたクレデン シャルに関連する認証子の所有および制御の証明に基づいて生成される。派生クレデンシャルは、具体的には次の 2 つの方法でサポートされる。

(1)カード・リーダのない政府が管理するスマートフォン、タブレット、ラップトップのセキュリティ・モジュールまたは要素（Trusted Platform Module 2.0、Apple Secure Element、Google Titan Chip など）内の仮想派生クレデンシャル。

(2)派生証明書を含む秘密鍵および X.509 証明書をネイティブにサポートする FIDO2 準拠のハードウェアトークン。これらのトークンが、他の FIDO2 鍵、Open Authentication (OATH) の時間ベースのワンタイムパスワード、他のプライベート 鍵および対応する X.509 証明書（または派生証明書）、および OpenPGP プライベート鍵などの追加クレデンシャルを同時にかつ安全に保持できる場合は許容される。

セクション 3.2 機密アクセスに関する資格認定

このセクションは、以下を含む機密アクセスのための機密アクセス PIV（CAPIV）クレデンシャル標準を確立する。

(a) CAPIV クレデンシャルは、日本の機密情報や施設にアクセスできる個人に発行されるもので、PIV とは別物だが技術的には相関している。

(b) CAPIV は、個人が許可されている範囲において、区分レベルを超えて機密リソースにアクセスするた

めに使用される。
(c)個人の PIV からの身元証明は、CAPIV の生成時に検証され使用される。
(g) CAPIV は、本人確認と認証のために、物理的なカードに 4 つの必須項目が印刷される。
(1)氏名 - 大文字で印字されたフルネーム、苗字、名前の順で記載される。
(2)個人が所属する機関、部署、または組織。
(3)カードの有効期限 - YYYYMMDD 形式で 1 回、MMMYYYY 形式で右上に大きく太字で 2 回印字される。
(4)汎用一意カード・シリアル番号-背面に印刷された、PIV クレデンシャルの汎用一意シリアル番号。
(5)なお、個人の許可されたアクセスレベルは、カードに印刷されてはならない。
(h) CAPIV クレデンシャルには、物理的な識別と認証に使用される 6 つの必須データ・フィールドがある。
(1)カード能力コンテナ - カードの製造およびモデルに関する情報、および様々なアプリケーション間の相互運用性を可能にし、カードが進化する際の後方互換性を提供するために使用される関連データモデルを指定する。
(2)カード保持者固有識別子-技術的実装ガイダンスに従って発行される固有のクレデンシャル 番号。接触型（例：集積回路チップ）および非接触型（例：RFID）インターフェース間で共有されるスマー ト・カード有効物理アクセス制御システムに従って発行された固有のクレデンシャル番号。
(3) PIV 認証用 X.509 証明書 - カードおよびカード所有者を認証するために使用される、FIPS 201-2 に定義される X.509 証明書およびその関連秘密鍵。
(4)カード認証用 X.509 証明書 - 物理的なカードを認証し、アクセス・コントロール・アプリケーションをサポートするために使用される非対称の X.509 証明書とその関連する秘密鍵。
(5) PIV ユニバーサル・ユニーク・カード・シリアル番号-CAPIV は、PIV および PIV アイデンティティ・プルーフィングに直接関連付けられ、それに応じて PIV シリアル番号を格納する。
(6)セキュリティ・オブジェクト - チップに格納されたすべてのファイルのハッシュ値、およびこれらのハッ シュのデジタル署名を、機械可読旅行書類パート 2 の第 IV 章付録 3（出典は ICAO）に従って実装し、中央発行者のデジタル署名によってカードの真正性を確認し、クレデンシャル置換を防止するもの。
(i) CAPIV クレデンシャルには、個人が持つ区分アクセスのレベルごとに、デジタル認証のための 2 つのデータ・フィールドがある、具体的には。
(1)デジタル署名用 X.509 証明書 - FIPS 201 に定義される、デジタル署名を目的とした X.509 証明書とそれに関連する秘密鍵。電子署名用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクト・インターフェイスを介してのみ利用可能である。暗号機能は、電子署名鍵の操作の直前に毎回 PIN を提出し検証しなければならないような「PIN Always」アクセスルールで保護される。
(2)鍵管理のための X.509 証明書 - FIPS 201 で定義された、機密保持を目的とした X.509 証明書とそれに関連する秘密鍵。鍵管理用秘密鍵およびそれに対応する証明書は、集積回路チップのコンタクト・インターフェースを介してのみ利用可能である。暗号機能は「PIN」アクセスルールで保護され、一旦 PIN が提出され検証されると、その後の鍵管理操作はそのセッション中に再度 PIN を要求することなく実行できるようになる。

(j)中央発行局は、各区分レベルの機密情報を保有するすべてのシステムでアクセス可能なネットワークパスのある認証局および証明書失効リストを提供する。

(k)中央発行局は、機密施設または空間へのアクセスを許可するすべての物理的アクセス制御システムからアクセス可能なネットワークパスのある認証局および証明書取り消しリストを提供する。

(l)中央発行機関は、デジタル認証のための派生 CAPIV クレデンシャルをプロビジョニングしライフサイクルする能力を提供する。派生クレデンシャルは、ID 証明プロセスを重複させないように、以前に発行されたクレデンシャルに関連する認証子の所有および制御の証明に基づいて生成される。派生的クレデンシャルは、具体的には次の 2 つの方法でサポートされる。

(1)カード・リーダのない政府が管理するスマートフォン、タブレット、ラップトップのセキュリティ・モジュールまたは要素（Trusted Platform Module 2.0、Apple Secure Element、Google Titan Chip など）内の仮想派生クレデンシャル。

(2)派生証明書を含む秘密鍵および X.509 証明書をネイティブにサポートする FIDO2 準拠のハー ドウェアトークン。これらのトークンが、他の FIDO2 鍵、Open Authentication (OATH) の時間ベースのワンタイムパスワード、他のプライベート 鍵および対応する X.509 証明書（または派生証明書）、および OpenPGP プライベート鍵などの追加クレデンシャルを同時にかつ安全に保持できる場合は許容される。

セクション 3.3 機密情報システム、機微・機密情報システム

このセクションは、相互運用性、情報共有、再利用、ポータビリティ、サイバーセキュリティを促進するために、日本政府全体で使用する技術標準を開発するための枠組みを確立するものである。標準は、以下の基準に基づいて検討される。

(a)実用性この規格の主な特徴や機能は要求事項を満たしている。

(b)相互運用性。アプリケーションやサービスを接続し、アクセスし、共有するための要件を満たす規格。

(c)技術的な成熟度。規格が確立され、安定しており、市場での支持も確立している。

(d)実装可能であること。規格が連邦政府または民間企業内のアプリケーションで使用されている。

(e)セキュリティ規格は、環境に対して許容できないサイバーセキュリティのリスクを導入しない。

(f)適用性規格が適切であり、潜在的なリスク、コスト、スケジュール、性能、セキュリティへの影響を含むプログラムのニーズに合致していること。

(g)知的財産権規格は一般に公開されており、関連する知的財産の所有者が、その知的財産を非差別的、ロイヤリティフリー、または妥当なロイヤリティベースですべての利害関係者に提供することに同意したことを要求する条項を含んでいる。

(h)一般に公開されていること。規格は一般に公開され、無制限に使用できる。

セクション 3.4 機密情報システムのリスク管理

このセクションは、審査、クリアランスの検討、資格認定をサポートするシステムを含め、機密情報または極秘情報を作成、処理、保管するすべてのシステムのためのリスク管理の枠組みを確立する。

(a)リスクマネジメントの考え方

(1)情報技術リスクマネジメントの主要な目標は、システムが含む情報の保護と、そのシステムが主要な機能を効果的に実行する能力のバランスをとることでなければならない。
(2)リスクマネジメントは、セキュリティへの配慮と設計がシステム開発にしっかりと織り込まれている場合に最も効果的である。
(3)リスクは完全に排除することはできないので、リスクマネジメントプロセスにより、意思決定者はシステム要件と運用上の必要性に照らし合わせて、保護手段の運用コストと経済コストのバランスをとることができなければならない。例えば、非常に高いレベルのセキュリティは、リスクを非常に低いレベルまで下げるかもしれないが、非常に高価であり、許容できないほど重要なオペレーションを阻害する可能性がある。
(4)情報システムに要求されるセキュリティのレベルは、システム内に含まれる情報の機密性を考慮し、情報共有と協力を可能にするシステムの能力と必要性を評価することによって決定されるものとする。
(5)省庁の技術システム間の相互運用性と効率的な連携は、重要な機能を追加するが、リスクも発生させる。個々の要素のセキュリティ評価と認可の決定を企業全体で信頼し、相互に受け入れるための健全な基盤を提供するために、各省は共通の基準を適用し、共通のプロセスに従ってシステムのリスクを管理するものとする。

(b)セキュリティ評価

(1)セキュリティ評価とは、情報技術システムまたは情報技術の特定の項目における管理、運用、技術的なセキュリティ管理について、認可の決定を支援するために必要な包括的な評価である。
(2)セキュリティ評価は、情報システムまたは情報技術項目の運用を許可するかどうかについて、信頼できるリスクベースの決定を行うために必要な、本質的な情報技術システムのセキュリティ分析を提供するものでなければならない。
(3)セキュリティ評価は、認可担当者または委任された認可担当者が認可の決定の基礎とする要因、同等性、および懸念事項のうち情報技術システムセキュリティの部分として機能し、それによってリスクを適切に受容するものとする。

(c)セキュリティ認可

(1)認可決定は、省庁に代わって、特定の環境下で特定のセキュリティレベルの情報技術システムの運用に関連する定義されたリスクレベルを明示的に受け入れる公式の管理決定である。
(2)情報システムを認可することにより、総務省は特定の環境において特定のセキュリティレベルで運用することを承認し、システムの運用に関連するリスクのレベル、および運用、資産、または個人に対する関連する影響を確立する。
(3)情報技術システムの運用に関連する許容可能なリスクのレベルを決定する際、省庁は、上記のリスク管理の概念および本書で付与された権限に従って後に発行される可能性のある基準に従って認可を決定するものとする。
(4)省庁による認可の決定は、システム内の情報の機密性に見合ったリスクが、可能な限り軽減されることを保証するものとする。各省庁は、システムの認可が、運用上の要件を満たすのに十分な協力及び情報共有を可能にすることを確保しなければならない。
(5)各大臣は、省を代表して認可の決定を行う 1 名以上の認可担当者を指名するものとする。大臣は、

大臣に代わって行われる全ての認可及び関連するリスク管理の決定について最終的な責任を保持するものとする。

(d)互恵関係

(1)省庁の認可担当者は、適切なセキュリティ認可の決定文書を他の省庁に提供するものとする。

(2)各省庁の権限ある職員は、情報技術システムまたはその他の情報技術の項目に関する適切なセキュリティ評価文書を他の省庁が利用できるようにしなければならない。

(3)省庁の認可担当者は、他の省庁によるシステムまたは情報技術の他の項目のセキュリティ・アセスメントを、システムまたは情報技術の項目の追加のバリデーションまたは検証テストを要求または要請することなく、受け入れるものとする。

セクション 3.5 民間企業や国際的なパートナーとの連携

(a)連盟は標準化され、民間企業や国際的なパートナーとの機密情報共有が必要な場合に使用されるものとする。

(1)フェデレーションは、接続またはネットワーク化された一連のシステム間で、検証者から依拠当事者への ID および認証情報の伝達を可能にするプロセスである。

(2)依拠当事者とは、通常、トランザクションを処理したり、情報またはシステムへのアクセスを 許可するために、加入者の認証子およびクレデンシャル、または請求者の ID に関する検証者の主張に依拠するエンティティのことである。

(3)フェデレーションアシュアランスとは、フェデレーションが使用するプロトコルが、認証情報や属性情報を依存者に伝達する際の信頼性のことである。

(b)機密情報の共有は、日本政府がフェデレーションを決定し、関係者間の作業関係及び技術的なフェデレーションを確立するためにフェデレーション・オーソリティとして設計したエンティティを通じてフェデレーションされるものとする。フェデレーション・オーソリティは、政府のネットワークやシステムとフェデレーションされる当事者に対し、 NIST SP 800-63C に概説されている少なくともフェデレーション保証レベル 2 のセキュリティおよび完全性基準への準拠を確認するため、 標準化されたレベルの審査を実施する。

(c)機密情報共有は、日本政府によって設計された、フェデレーションを決定し、当事者間の技術的なフェデレーションを確立するための機関である機密フェデレーション機関を通じてフェデレーションされるものとする。機密フェデレーション機関は、フェデレーションされる当事者に対して、NIST SP 800-63C に概説されるフェデレーション保証レベル 3 のセキュリティ及び完全性基準への準拠を確認するために、標準化されたレベルの審査を実施する。

7．パート 4：実施と見直し

セクション 4.1 一般的な責任

法令で指定され、認可されることになる。

(a)集中化された政府全体のクレデンシャル・システムの確立と継続的な運用を監督する実体。

(1)この組織は、この制度に関わるすべての省庁や組織のパフォーマンスと進捗を監視し、進捗状況を立法府に報告する。これらの業務の監視を設立後も継続することは、長期的な成功のために不可欠である。

(b)すべての政府全体の PIV および CAPIV クレデンシャルを発行し取り消す、中央クレデンシャル発行機関 として機能する実体。このエンティティは、以下を行うものとする。

(1)資格情報を認証し、取り消された資格情報をチェックするための分散型高可用性システムを確立する。

(2)十分なアクセス権を持つユーザーが、提供されたクレデンシャルで常に ID を確認できるように、ID をグローバルに検証可能で標準クレデンシャルに結び付けたシステムを構築する。

(3)不変、非エクスポート、ハードウェアベースの証明書と FIDO2 標準に基づく中央ルート認証局から X.509 デジタルクレデンシャルを発行する。

(4)任意の中間認証局の作成を管理し、中間認証局の X.509 証明書に署名を行う。

(5)デジタル認証のための派生的な CAPIV クレデンシャルの提供およびライフサイクル

(6)個人が複数の役割を持つ場合でも、単一のアイデンティティしか持たないようにし、認証された同一人物が、ある時点における現在の機能またはその他の要因に基づいて属性ベースの認可を受けた結果、異なるアクセスを持つことができるようにする。

(c)政府全体のクレデンシャル・システムのポリシー、基準、および手順を監督および維持する主体。このエンティティは、以下を行う。

(1)物理的およびデジタルなクレデンシャル標準と、それらのクレデンシャルを使用する物理的およびデジタルな認証標準を確立する。

(2)情報への物理的または論理的アクセス、および建物や施設へのアクセスの承認に関する方針と基準を確立する。

(d)機密情報および機密情報を処理または保存するネットワークおよび通信機器への物理的または論理的アクセスに関する認可方針および基準を設定し、維持する主体。

(e)公的な機密情報を処理または保管するシステムのリスク評価と管理のための方針と基準を確立し、維持する事業者。

(1)また、政府のネットワークやシステム間のフェデレーション、民間企業や海外パートナーとのフェデレーションのためのポリシーや基準を確立し、維持すること。

(f)民間企業や国際的なパートナーとの機密情報共有が必要な場合に、政府の機密ネットワークやシステムを連携させるためのフェデレーション・オーソリティとして機能する団体。

(g)民間企業や国際的なパートナーとの機密情報共有が必要な場合に、政府の機密ネットワークやシステムを連携させるための機密連携機関として機能するエンティティ。

(h)相互運用性、情報共有、再利用、ポータビリティ、サイバーセキュリティを促進するために、日本政府全体で使用する標準および標準プロファイルの特定、開発、処方を担当する組織である。

(i)デジタルポリシーに基づく認可を可能にする情報技術を開発・運用し、日本政府のシステムおよびネットワーク間で安全なフェデレーションを推進し、民間企業や国際的なパートナーとのフェデレーションが必要な場合には技術的な専門知識を提供する事業体である。

セクション 4.2 説明責任と懲戒処分

(a)日本版 PIV または CAPIV を付与された者は、故意または過失により、適切な懲戒処分を受けるものとする。

(1)物理的なクレデンシャルまたはデジタル証明書を無許可の個人に提供する。

(2)不正な目的でクレデンシャルを使用または乱用すること。

(b)懲戒処分には、譴責、無給の停職、解任、解雇、機密情報へのアクセスの喪失または拒否、あるいは適用される日本の法律および政策に従ったその他の懲戒処分が含まれる場合がある。

(c)大臣又は上級省職員は、少なくとも、本命令の区分基準の適用において無謀な無視又は誤りのパターンを示す個人については、速やかに CAPIV を削除するものとする。

8. パート 5：コスト

この活動には、中央発行機関および関連スタッフの設置、または中央発行機関として指定された既存の機関または省庁のスタッフの増強が必要である。さらに、国家安全保障事務局（NSS）または他の監督機関は、基準の策定と実施の調整のために小規模なスタッフを必要とする場合がある。必要な物理的、デジタル的認可システムおよび機密ネットワークの確立には、これらのシステムを確立、維持、および保護するために、各省に追加的な職員が必要となる。

人材の審査とクリアランスの検討を支援するシステムの導入には、初期のソフトウェア開発費用と、その後の継続的なメンテナンス、ホスティング、セキュリティの費用がかかる。

物理アクセス制御システムのコストは、具体的な導入方法によって大きく異なる。クレデンシャル認証と認可のアクセス制御を施設のエントランスにのみ配置することは、建物全体に多層に配置するよりもコスト効率が良いが、安全性は低くなる。同様に、デジタル認証の導入は、認証ポリシーの複雑さによって異なる。

機密ネットワークには、初期費用と、各区分レベルにおけるユーザーごとの関連費用がかかる。ギャップ・ネットワークの導入にはいくつかの方法があるが、いずれも機密ネットワークの構築には避けられない初期費用がかかる。ベストプラクティスは、SWA に設置された「ゼロクライアント」端末にクライアントセッションを提供する大規模な仮想化環境である。このモデルは、ハードウェア暗号でネットワーク化された 2 つの高可用性データセンターのために約 1500 万ドルの初期費用と、すべてのハードウェア、メンテナンス、IT サポートのライフサイクルコストをカバーするためにユーザーあたり年間 1500 ドルがかかる。SWA を 1 つ追加するごとに、さらに 100 万ドルの初期費用と年間 50 万ドルの費用がかかる。米国と英国では、Commercial Solutions for Classified capability package を利用したセキュアモビリティが一般的になってきており、現在のワークフローへの影響を最小限に抑えるために適切であると思われる。これは、ユーザーに安全なラップトップを提供し、SWA 内で、非 SWA、自宅、または旅行中の信頼できる Wi-Fi 接続で暗号トンネルを介して動作するようになる。このモデルのスタートアップ費用は、ソフトウェア暗号でネットワーク化された高可用性データセンター2 か所に 15,000,000 ドル、そしてすべてのハードウェアのライフサイクルコスト、メンテナンス、IT サポートとして 1 ユーザーあたり年間 3,500 ドルとなる。SWA を追加す

る場合の追加費用は発生しない。また、ほとんどが「ゼロクライアント」端末で、一部にセキュアモビリティラップトップを使用するハイブリッドモデルの導入も可能である。初期費用は 2,500 万ドル近くになり、その後は個別のアプローチと同じユーザーごとの価格設定になる。日本以外の国では、セキュリティ担当者は、電子機器、特にすべての機密 IT からの発散を制御するための追加コストを考慮する必要がある。

9．パート 6：結論

この国家安全保障クレデンシャル・システムの提案は、コンセプトとしては単純だが、適切に実施するためには膨大な努力と資源が必要となる。職員の審査と区分の実施と並んで、これは日本政府にとって重要な取り組みであり、幅広い支持と参加を得るためには、期待、スケジュール、およびリソースについて優れたコミュニケーションが必要である。これらのシステムを導入するために時間と資源を投入することは、日本の国家安全保障情報のセキュリティを大幅に向上させるだけでなく、重要情報、知的財産、技術の保護の基盤を提供することによって、日本経済にも利益をもたらすことになる。時間と資源を投入することで、意図した効果を発揮する安全で信頼性の高いシステムを実現するためには、これらのシステムの開発と実装における厳密さが重要になる。

10.パート 7：参考文献

[1] Computer Security Division, Information Technology Laboratory, "FIPS PUB 201-2:Personal Identity Verification (PIV) of Federal Employees and Contractors," National Institute of Standards and Technology, NIST FIPS 201-2, Aug. 2013. doi: 10.6028/NIST.FIPS.201-2.

[2] D.Cooper et al. , "RFC5280:Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." https://datatracker.ietf.org/doc/html/rfc5280 (accessed Nov 29, 2021).

[3] "FIDO 2.0:Overview." https://fidoalliance.org/specs/fido-v2.0-rd-20170927/fido-overview-v2.0-rd-20170927.html (accessed Nov 30, 2021).

[4] "FIDO2。Moving the World Beyond Passwords using WebAuthn & CTAP," FIDO Alliance. https://fidoalliance.org/fido2/ (accessed Nov. 29, 2021)。

[5] V.C. Hu ら、「NIST SP 800-162:Guide to Attribute Based Access Control (ABAC) Definition and Considerations," National Institute of Standards and Technology, NIST SP 800-162, Jan.2014. doi: 10.6028/NIST.SP.800-162.

[6] G. W. Bush, "Homeland Security Presidential Directive 12," Department of Homeland Security, Aug. 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive-12 (accessed Nov 28, 2021)。

[7] Rigas, Michael J., "Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials," p.15, Dec. 2020.

[8] D. Deasy and J. N. Stewart, "Modernizing the Common Access Card - Streamlining Identity and Improving Operational Interoperability." Dec. 07, 2018. Accessed: Nov. 28, 2021. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Cyber/modernizing_the_cac.pdf

[9] P.A. Grassi, M. E. Garcia, and J. L. Fenton, "NIST SP 800-63r3:Digital identity guidelines," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-63-3, Jun.2017. doi: 10.6028/NIST.SP.800-63-3.

[10] D.A. Cooper, H. Ferraiolo, K. L. Mehta, S. Francomacaro, R. Chandramouli, and J. Mohler, "NIST SP 800-73r4: Interfaces for Personal Identity Verification," National Institute of Standards and Technology, NIST SP 800-73-4, May 2015.doi: 10.6028/NIST.SP.800-73-4.NIST SP 800-73r4.

[11] P.Grother, W. Salamon, and R. Chandramouli, "NIST SP 800-76r2: Biometric Specifications for Personal Identity Verification," National Institute of Standards and Technology, NIST Special Publication (SP) 800-76-2, Jul. 2013. doi: 10.6028/NIST.SP.800-76-2.

[12] W.Polk, D. Dodson, W. Burr, H. Ferraiolo, and D. Cooper, "NIST SP 800-78r4: Cryptographic Algorithms and Key Sizes for Personal Identity Verification," National Institute of Standards and Technology, NIST Special Publication (SP) 800-78-4, May 2015.doi: 10.6028/NIST.SP.800-78-4.NIST SP 800-78r4, 2015.5.1.

[13] H. Ferraiolo, R. Chandramouli, N. Ghadiali, J. Mohler, and S. Shorter, "NIST SP 800-79r2: Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)," National Institute of Standards and Technology, NIST Special Publication (SP) 800-79-2, Jul. 2015. doi: 10.6028/NIST.SP.800-79-2.

[14] H. Ferraiolo et al., "NIST SP 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials," National Institute of Standards and Technology, NIST Special Publication (SP) 800-157, Dec. 2014. doi: 10.6028/NIST.SP.800-157.

[15] "Personal Identity Verification Guide Introduction." https://playbooks.idmanagement.gov/piv/ (accessed Nov. 30, 2021).

[16] General Services Administration, "FIPS 201 Approved Products List - PIV Cards." https://www.idmanagement.gov (accessed Nov 28, 2021.)。

[17] Physical Access Interagency Interoperability Working Group, "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems," Dec. 20, 2005. https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf (accessed Nov. 30, 2021).

[18] International Civil Aviation Organization, "ICAO 9303: Machine Readable Travel Documents, Part 3, Volume 2." Third Edition 2008. Accessed: Dec. 02, 2021. [Online]. Available: https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

[19] P. Grassi et al., "NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing," National Institute of Standards and Technology, NIST Special Publication (SP) 800-63A, Mar. 2020. doi: 10.6028/NIST.SP.800-63a.

[20] P. Grassi et al., "NIST SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, NIST Special Publication (SP) 800-63B, Mar. 2020. doi: 10.6028/NIST.SP.800-63b.

[21] P. Grassi et al., "NIST SP 800-63C: Digital Identity Guidelines: Federation and Assertions," National Institute of Standards and Technology, NIST SP 800-63C, Mar. 2020. doi: 10.6028/NIST.SP.800-63c.

[22] R. T. Vought, "M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management," p. 13, May 2019.

[23] N.Keller, "Cybersecurity Framework," NIST, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Dec. 15, 2021).

[24] N.Grayson, "Privacy Framework," NIST, Jan. 08, 2020. https://www.nist.gov/privacy-framework/privacy-framework (accessed Dec 15, 2021)。

[25] "rfc1422." https://datatracker.ietf.org/doc/html/rfc1422 (accessed Dec 15, 2021).

[26] "TPM 2.0 Library," Trusted Computing Group. https://trustedcomputinggroup.org/resource/tpm-library-specification/ (accessed Dec. 02, 2021)。

[27] "Secure Enclave," Apple Support. https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web

(accessed Dec. 02, 2021)。

[28] "Why Yubico," Yubico. https://www.yubico.com/why-yubico/ (accessed Dec. 02, 2021).

[29] "U2F and FIDO2 Keys," TOKEN2 MFA Products and Services. https://www.token2.com/shop/category/u2f-and-fido2-keys/1 (accessed Dec 02, 2021)。

[30] "A single sign-on and digital identity solution for government - Government Digital Service." https://gds.blog.gov.uk/2021/07/13/a-single-sign-on-and-digital-identity-solution-for-government/ (accessed Nov. 29, 2021).

第５節 日本向けセキュリティクリアランスの提言

1. エグゼクティブサマリー

日本政府は最近発表した 3 つの文書で、日本の国家安全保障と防衛に関する詳細な戦略を示した。この戦略は、日本の国家、経済、社会の優先事項を重要かつ関連性のある問題として特定し、競合国からの脅威の高まりを認識し、効果的な防衛を開発し、同盟国との関係を改善・拡大する必要性を強調している。この戦略の実行を開始するにあたり、重要な基盤となるのは、防衛や製造の分野において、日本の優位性をもたらす機密情報、プログラム、活動を保護するためのセキュリティシステムの開発である。　本報告で述べたように、機密性の高いデータや製品を効果的に特定し、保護するためのプログラムには、3 つの重要で基礎的な分野があることが判明した。その 3 つの領域とは、1) 人事考課、2) データ区分フレームワーク、3) 技術開発フレームワークである。セキュリティプログラムの重要性から、これら 3 つの活動の開発は並行して行われ、国家安全保障と防衛戦略の実行の中で早期の成果物として開始されるべきである。

人事考課（パーソナル・ベッティング）

政府と契約の従業員に対する信頼と信用の確立と維持は、セキュリティプログラムの最も基本的かつ長年の要件である。このように信頼された従業員は、重要な機密情報の知識を持ち、それらにアクセスすることができる。機密プログラムの侵害のほとんどは、職員または関連会社による故意または無意識の行動が原因で、防衛、国家安全保障、または製造の要素に戦略的、戦術的、または競争上の優位性を与える機密情報または能力が露呈している。信頼と信用を確立し、維持することができなければ、広範な戦略を成功裏に実行することができなくなる。

データ区分フレームワーク

日本が国家、経済、社会の優先事項を保護するためには、これらの優先事項の成功に不可欠な情報と技術を保護する必要がある。このような努力の基礎となる要素は、これらの重要な情報および技術の要素を特定

し、リスク値を割り当てること、つまり本質的にはセキュリティ区分システムであり、これは保護システムに情報を与え、定義するものである。このようなプロトコルの確立は、何かが秘密であるかどうかという大まかなレベルから始まり、特定されたリスクに基づいて保護戦略を強化するためにより微妙なニュアンスへと拡大する必要がある。

技術開発フレームワーク

日本政府が政府全体の信頼される労働力を確立するのに伴い、その審査と、物理的およびデジタルな識別、認証、およびアクセスの承認を提供する標準化されたクレデンシャルをサポートする技術システムを開発する必要が付随している。さらに、データ区分システムの確立に伴い、政府は個人のクリアランス審査をサポートし、適切な区分レベルの機密情報を相応の保護とともに生成、処理、保管するための技術システムを開発する必要がある。

これら 3 つのセキュリティ要素はまだ始まったばかりであることを認識した上で、どのように進めていくかの推奨事項を提供する。この 3 つの活動はすべて早期に、かつ並行して開発を始めるべきであるが、それぞれの中に優先順位をつけることができるステップがある。開発は、協力的で同期化されたプログラムであることを保証するために、単一の組織によって監督されるべきである。

2．人事考課に関する提言

ポリシーと審査機関

適切な法律が立法され、実行可能な資金源が特定されたら、最初のステップは、審査プログラムの実施を開発・監督する政府機関の設立である。この組織は、当初から独自の信頼性を確立することが重要であるため、人事審査プログラムの確立と成長を構築・実行するために割り当てられる人材は、防衛省（MOD）など既存のプログラムのいずれかを通じて審査されることをお勧めする。このコアグループは、その後、より強固な国家プログラムを構築し始めることができる。このプログラムが完全に運用された場合の規模は、何千人もの政府職員、請負業者、関連会社をカバーすることになり、この全範囲を直ちにサポートすることができないであろう。我々は、基礎を築き、適用範囲を拡大するために、段階的なアプローチを推奨する。

参加省庁及び段階的初期アプローチ

最初のステップは、最も大量の機密データを持つ機関及び省庁を特定することであろう。次に、これらの機関内で、この機密データに日常的にアクセスする役職と人員（従業員、請負業者、および関連会社）を特定する。特定できたら、これらの個人について初期調査プロトコルの実施を開始し、機密データへのアクセスに対する適格性を肯定的に判断する。これにより、これらの機関や省庁の中に信頼できる人材のコアグループを確立することができる。

プログラムの拡大

第一段階が順調に進んだら、この最初のグループの省庁は、最終的に機密データにアクセスできるすべて

の職員を対象とした「人事審査プロトコル」の拡大を開始すべきである。同時に、残りの省庁も上記のベッティング・プログラム確立計画に従い始めるべきである。最終的な目標は、機密データにアクセスできるすべての政府職員が徹底的かつ一貫して審査されるようになることである。

トラストの維持

人事考課を通じた最初の信頼確立の推進は、次の要素である継続的審査（Continuous Vetting）の基礎となるもので、各人員について行われた最初の信頼判断が長期にわたって有効であることを保証するプロセスである。この活動の重要な要素は、信頼された人物の行動や活動に関する疑問や懸念に対応し、適切な情報を収集し、懸念を解決または軽減するために適切な手順を踏むことができる機関を省庁内に設置することである。

完全に実施されれば、日本政府は、国民全体に強固で永続的な信頼を確立するための、信頼性が高く再現可能なプロセスを手に入れることができる。その結果、政府内および同盟国との信頼関係を改善できる。

3．データ区分フレームワークに関する提言

基礎的な政策と権限

人事考課と同様、最初に必要なステップは、適切な権限の法的割り当てと実行可能な資金調達の特定である。安全保障区分の枠組みを確立する作業には、政府全体の枠組みの開発を推進し、その後、その枠組みにおける政策の実施と遵守を監督する責任を負う中央組織を指定すること、どの省庁が機密および区分された情報を開発、利用、共有、保護するかを決定し、政策開発プロセスにおけるこれらの省庁の代表的な参加を確認し、次に政府全体の枠組みのための政策を開発すること、が含まれる。

政府全体の中央当局

法制化の最初の検討課題は、政府全体のセキュリティ区分の枠組みを調整し、最終的に実現するための中央当局として、ある組織を選ぶことである。この組織は、国家安全保障、経済安全保障、市民・社会保障の各省庁など、政府のすべての関係部門からの参加を促し、バランスをとることができる首相官邸に置くことを提案する。また、政府内に設置することで、予算面でも政府のパフォーマンス面でも、人事審査とサイバーセキュリティの取り組みを統合することができるようになる。

参加省庁

次に、中央当局は、セキュリティシステムの影響を受ける／参加する省庁を指定する必要がある。各省庁は、首相と中央当局に責任を持つ省庁の高官を指定して、政府のパートナーと協力し、各省庁の高官を動員して実施計画を立てなければならない。そのような高官は、人事審査やサイバーセキュリティの問題に取り組むパートナーと連携し、すべての取り組みが全体的な戦略に対応するようにする必要がある。

政策展開の取り組み

中央官庁と参加省庁が特定されれば、中央官庁はフレームワークを構成する政策プロセスを主導し、日本のニーズを満たすフレームワークの基本要素について意思決定を開始することができる。本報告で述べたデータ区分フレームワークは、フレームワークの多くの構成要素に関するガイドであり、日本の政策開発プロセスに応じて使用または修正することができる。

実施

枠組みができあがると、各省庁による新政策の実施に取り組み、中央当局の焦点は各省庁の実施努力の推進と監督に移る。このような取り組みは、政府全体の取り組みに関する各省のパフォーマンスをレビューする既存のメカニズムに統合されるべきであり、目標が達成され、より広範な安全保障戦略が成功するよう、各省の実施のペースを推進することも含まれるべきである。

4. 技術開発フレームワークに関する提言

適切な権限が立法され、実行可能な資金源が特定されたら、最初のステップは、審査プログラムをサポート し、標準化されたクレデンシャルを発行し、クリアランス検討をサポートし、機密情報を保護する技術を開発 し、その実施を監督する政府機関を設立することである。

人事考課システムと標準化されたクレデンシャルの開発

物理的およびデジタルな識別、認証、アクセスの認可を提供する審査プログラムをサポートする技術の開発と実行を監督するために特定されたエンティティは、迅速に推進する必要がある。このエンティティは、当初から独自の信頼性を確立することが重要であるため、人事考課プログラムへの技術サポートを構築および実行し、標準化されたクレデンシャルを開発するために割り当てられる人員は、MOD などの既存のプログラムの 1 つを通じて審査されることを推奨する。このコアグループは、その後、より強固な国家プログラムの構築を開始することができる。人事考課プログラムをサポートする技術システムは、大規模な審査プロセスを開始する前段階として開発されるべきであり、そのようなシステム開発への早期投資は重要である。このプログラムが完全に運用された場合の規模は、数千人の政府職員、請負業者、および関連会社に信任状を発行することになり、この全範囲を直ちにサポートすることはできないと認識している。最初は基盤を構築し、適用範囲を拡大するための段階的なアプローチを推奨する。

物理的および論理的アクセス制御

クレデンシャルが確立され発行されると、物理的および論理的アクセス制御システムは政府の施設およびシステム全体に展開される必要がある。所定の施設で働く職員は、標準化されたクレデンシャルを与えられると、アクセスのためにそれを使用し始めるべきである（同じ施設内の他の人がまだクレデンシャルを持っていない場合でも）。所定の施設の労働力が完全にクレデンシャル化されたら、施設アクセスにそのクレデンシャルを使用するよう全員に要求することを強制するものとする。

クリアランス審査システムの開発

人事考課を支援する組織の設立後直接、またはそれと並行して、個人のクリアランス審査を支援し、適切な区分レベルの機密情報を相応の保護とともに作成、処理、保管するための技術システムの開発及びその実施を監督する組織は、主要システムの開発に投資するべきである。クリアランス検討システムの開発は、質問事項や情報の重複が多いため、人事調査システムと慎重に調整する必要がある。この開発の一環として、事業体は、ID、認証、およびアクセスの許可のための機密クレデンシャル・システムを開発し、実施すべきである。

機密ネットワークの実装

その後直ちに、責任ある事業体は、機密として識別される情報、およびその情報の生産、処理、保管に関連するリスクに基づき、優先順位をつけて機密ネットワークおよびシステムの開発に投資する必要がある。これらのシステムで働く個人は、前述のクリアランス検討プロセスで評価され、有利なクリアランス判定を受けている必要がある。リソースの制約に基づき、責任主体はこれらのシステムの開発に優先順位をつけるための自治権と、必要な投資を実行するための予算を有するべきである。これらのシステムの開発と実装における厳密さは、時間と資源の投資によって、意図した影響を与える安全で信頼できるシステムを生み出すために、非常に重要である。

5. 実現に向けたロードマップ

セキュリティクリアランス、データ区分フレームワーク、技術開発フレームワークを実現するための、推奨される一連の実施手順を表 4-5-a に示す。

表 4-5-a 実現に向けたロードマップ

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
人事考課のフレームワーク	法案は、身元調査プログラムの開発と実施を監督する政府機関を設立する	機密情報およびセキュリティクリアランス保持者のために、中央当局および省庁に認可され割り当てられた資金	人事評価プログラムの構築と成長を担う人材は、防衛省(MOD)などの既存のプログラムのいずれかを通じて審査されることを推奨する	人事考課の対象を拡大し、最終的には関係省庁の全職員を対象とする
	事業体は、各省庁と協力して、調査、裁定、継続的な審査に関する基準を設定する。		機密データを持つ機関や省庁を特定する	継続的審査（Continuous Vetting）を計画・確立する
			日常的な業務を行う役職や担当者を特定するは、この機密データにアクセスすることができる	
			選ばれた人物を調査し、	

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
			裁定する	
データ区分フレームワーク	情報区分プログラムの策定と実行を監督する政府機関を設立する法案[首相府が推奨]	機密情報およびセキュリティクリアランス保持者のために、中央当局および省庁に認可され割り当てられた資金	どの省庁が機密情報を開発、利用、共有、保護するか指定する	中央当局は、フレームワークを構成するような政策プロセスの主導を開始し、日本のニーズに合ったフレームワークの本質的な要素について意思決定を行う
			政策立案プロセスに参加するよう指定された省庁の上級職員	
技術開発フレームワーク	法案は、審査プログラムを支援し、標準化されたクレデンシャルを発行し、クリアランスの検討を支援し、機密情報を保護するための技術を開発し、その実施を監督する政府機関を設置する	中央省庁が機密情報やセキュリティクリアランス保持者を持つために認可され、割り当てられた資金	技術開発プログラムを開発し、実行を監督する主体を早急に特定する必要がある	クレデンシャルが確立され、発行されるようになったら、物理的およびデジタルアクセス制御システムを政府施設およびシステム全体に展開する必要がある
	政府全体のクレデンシャル基準および技術的なルート証明書（クレデンシャル）権限を確立する事業体		人事審査プログラムの技術サポートを構築・実行し、標準化された資格を開発するために割り当てられた人材は、MODなどの既存のプログラムのいずれかを通じて審査される	所定の施設で働く要員に標準化されたクレデンシャルが提供されたら、アクセスのためにそれを使い始めるべきである（同じ施設内の他の人がまだクレデンシャルを持っていない場合でも）。所定の施設の労働力が完全にクレデンシャル化されたら、施設アクセスにそのクレデンシャルを使用するよう全員に要求することを強制する
			人事審査プログラムを支える技術システムは、審査プロセスを大規模に開始する前段階として開発されるべきである	責任主体は、機密と認定された情報及びその情報の作成、処理、保管に関連するリスクに基づき優先順位をつけて、各省庁の機密ネットワーク及びシステムの開発に投資すべきである
			クリアランスの検討を支援する技術的なシステムは、質問や情報の重複が多いため、人事	機密プログラムおよびシステムに従事する個人は、前述のクリアランス検討プロセスによ

節との対応	基本的な方針と権限	承認され配分される資金	中央省庁が策定するフレームワーク	各省庁が連携してプログラムを開発・実行
			審査システムと慎重に調整する必要がある	って評価され、有利なクリアランス判定を受けている必要がある
			責任ある事業者は、ID、認証、およびアクセスの承認のための区分されたクレデンシャルのシステムを開発し、実装する必要がある	責任主体は、これらのシステムの開発に優先順位をつけるための自律性と、必要な投資を実行するための予算を持つべきである。時間と資源を投資することで、意図した効果を発揮する安全で信頼できるシステムを作り上げるためには、機密システムの開発と実装における厳密さが重要である

第５章 量子関係

最近、量子コンピュータ、量子センサー、量子暗号等々情報科学の分野で量子技術を利用した新たな情報通信システムの実用化に向けた革新的な展開が大きな話題になっている。また、昨年（2022 年）のノーベル物理学賞の受賞は、量子力学の分野で「量子もつれ」と、それを利用した「量子テレポーテーション」の研究者が受賞した。これらの技術は、量子コンピュータや量子通信の実現には欠かせない技術であり、今後の量子技術を利用したシステムの基盤になる。この量子技術は、世の中の一般的な現代科学技術（ニュートン力学やマックスウェルの電磁気学に基づく現在の一般的な科学技術。量子に対して古典技術と呼ばれている）が進化すると、理論の上で成り立っていた量子論が実験により確認、検証することができるようになり、より具体的に実社会への応用が検討できるようになってきた。これは、進化した古典技術を利用しシステムを具現化できるようになってきたからである。

本章では、量子コンピュータ関連および量子コンピュータの解読計算に耐性のある暗号における昨今の公開情報を基に、情報セキュリティおよび安全保障の観点から俯瞰的な視点で、捉え、その対策を考察していく。なお、この章で記述する量子コンピュータとは、特に説明の記載がない限り、超電導量子ビット型の量子コンピュータのことである。

第１節 各国の量子技術の動向とその取り組み

近年、各国の量子技術への研究開発投資は、非常に大きくなってきている。表 5-1 に各国の量子技術に対する政策と研究開発投資予算を纏めて示す。各国ともに、量子技術を先行して有することは、現代の社会活動におけるイニシアティブを確保する上で大きな影響を与えるため積極的に投資を行っている。特に、中国は、先行する米国や他国からの巻き返しのため巨額な研究開発投資を行ってきている。その額は、1 兆円をこえる投資額であり、中国東部にある安徽省・合肥市に大規模な研究拠点を整備している。

日本においても近年ようやく欧州並みの予算額がついてきているが、現在のシステムへの適用や実社会への実装例は、非常に少なく、実用化の面での更なる加速が必要である。そのためには、一般社会への実用化（実装）開発と、純粋な科学技術の発展のための研究との両輪での研究開発投資が必要と考えられる。

表 5-1　各国の量子技術に対する政策と研究投資予算

国	政策動向	内容・予算規模
米国	量子情報科学の国家戦略概要（2018.9） 国家量子イニシアティブ法（2018.12）	約1,400億円($1.28B)（2019-2024） 「国家量子イニシアティブプログラム」 DOE:140億円（$125M）/年 量子情報研究センタ NSF:56億円（$50M）/年 量子研究・教育センタ NIST:89億円（$80M）/年 量子情報研究・計量標準、ワークショップ
中国	科学技術イノベーション 第13次5ヶ年計画（2016-20） 第14次5カ年計画（2021-25）	1,200億円/(2016-20)以上 「国家重点研究計画」 「量子情報科学国家実験室」（合肥市）。 第1研究棟完成（2020年） 「量子情報技術を含むフロンティア分野における主要な国家科学技術プロジェクト」（金額等詳細は非公開）
EU	Quantum Manifesto (2016.5)	約1,300億円(€1B)/(2019-28) 「Quantum Flagship」20課題が採択
独国	ハイテク戦略2025(2018) BMBF「量子技術」(2018.9) 未来パッケージ(2021.1)	約840億円(€650M)/(2019-22) 両子計算、量子通信、計測、量子分野の技術移転と産業の参画推進 ~2,600億円(€2B)/(2021-2025) 両子通信、量子コンピューティング、量子センサおよび周辺技術（電子機器、光源、光学部品、材料、インターフェースなど）の研究開発
英国	量子技術国家戦略(2014.12)	約600億円(~£400M)/(2015-19) 「UK National Quantum Technologies Programme」 量子イメージング、量子センシング、量子通信、量子コンピューティング ＆シミュレーションの4つのハブ構築など
仏国	MESRI「国家量子戦略」(2021.1)	約2,300億円(€1.8B)/(2021-25?) 両子戦略の7本の柱（量子コンピュータ、量子センサ、量子暗号通信等）を中心に産業のバリューチエーン、人材育成・科学研究・技術実験を大幅に強化
日本	「量子技術イノベーション戦略」	2022年度政府予算を約800億円に積み増し 前年度予算比2倍

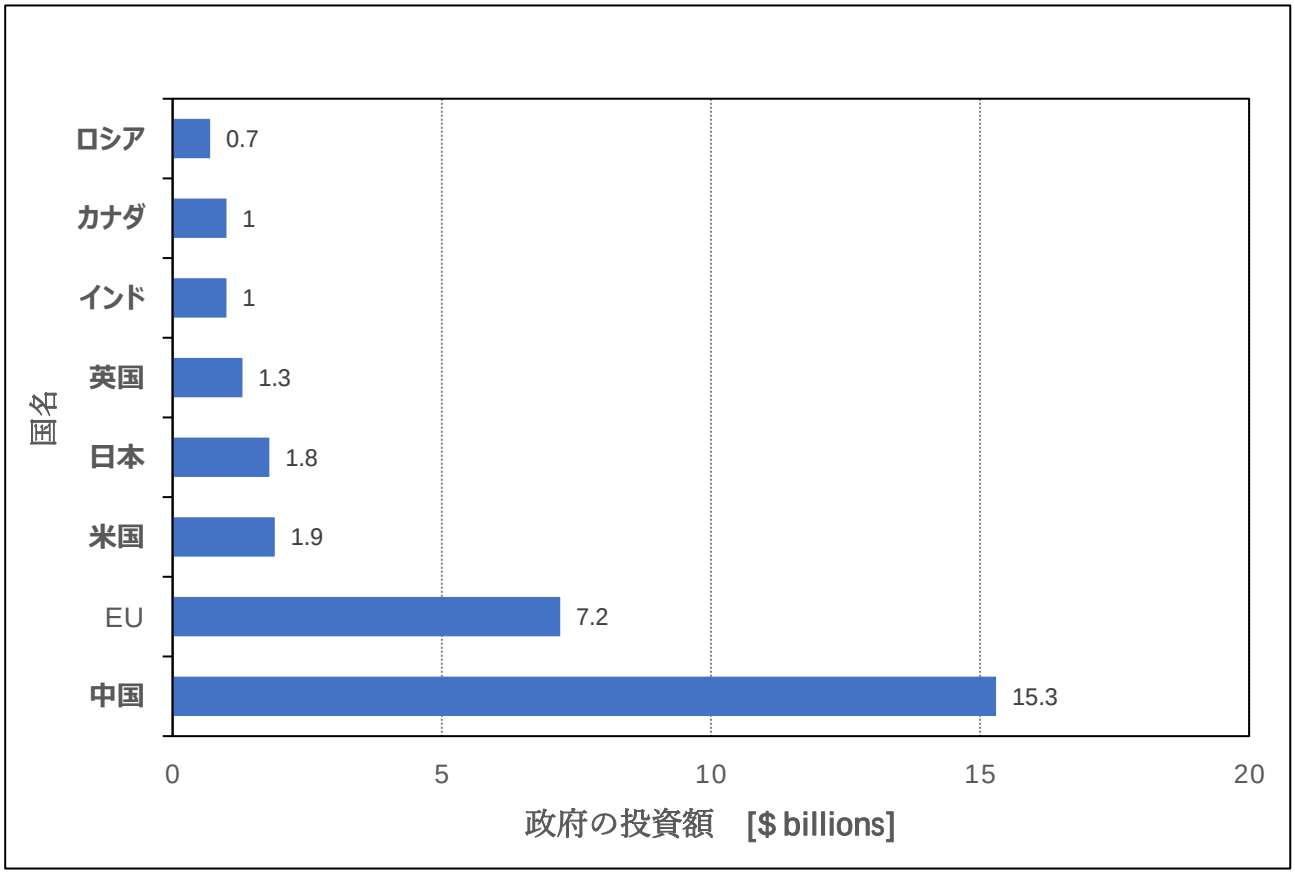
中国：https://www.zdnet.com/article/quantum-computing-networks-satellites-and-lots-more-qubits-china-reveals-ambitious-goals-in-five-year-plan/

日本：　https://www.nikkei.com/news/print-article/?R_FLG=0&bf=0&ng=DGKKZ079508920U2A120C2PD0000

https://ainow.ai/2022/04/24/264447/

各国の量子戦略の投資の中でも、特にサイバーセキュリティの観点から直接的に影響のある量子コンピュータと量子通信、量子暗号等が挙げられる。その中でも特に量子コンピュータについて、コンサルティング会社の McKinsey & Company, Inc.が 2021 年 12 月に発表したレポートを纏めている（図 5-1）。このレポート「Quantum computing use cases are getting real-what you need to know（量子コンピューティングのユースケースが現実味を帯びてきた ― 知っておくべきこと）」では、量子コンピュータ研究開発はまだ黎明期にあるため、多額の公的資金が投じられており、その投資額が纏められている。そうした資金を国別に見ていくと、中国が 150 億ドルともっとも多く、次いで EU の 72 億ドル、アメリカの 13 億ドルと続いている。日本は 10 億ドルでインドと同等である。EU の公的資金源となっている加盟国はドイツが 41.9%ともっとも多く、次に多いのがフランスの 28%である。

なお、技術的に先行しているアメリカにはすでに多数の量子コンピュータ企業が存在しており、こうした企業には公的資金ではなく民間ベンチャーキャピタルからの投資と考えられる。



https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know

（データを抜粋）

図 5-1　各国の量子コンピュータへの投資額

中国は、EU の 2 倍、米国の 10 倍以上の投資額であるが、米国（IBM や Google）の様な明確なアウトプットは公開されていない。量子コンピュータの開発の目的は、現代の情報化社会における利便性の向上とともに、暗号等の解読への応用による安全保障の優位性の確保等が考えられ、各国ともに技術情報の公開は、慎重であり、技術のクローズド戦略等が考えられている。

第２節 量子技術と安全保障

諸外国では、「量子技術は、安全保障における様々な局面で、大きなインパクトをもたらす」と考えられ、量子技術に関する研究が積極的に進められている。量子技術が進歩することによる情報通信におけるセキュリティへの影響は大きく、今すぐにでも真剣に考え対応する必要がある。しかし、量子技術に対する考え方は、様々であり、特に実用化に対して量子技術の課題の大きさを理由にし、先延ばしした意見も多く、新

たに発生するセキュリティに影響を及ぼす脅威に対しての対策が先送りになっている場合が多く見受けられる。特に日本においては、量子関連の技術革新と安全保障の観点において、他国に比較すると安全保障の感度が低いように思える。今までの日本における量子技術の研究開発は、学術的な視点からの研究開発が主流であり、安全保障に対する様々な脅威の可能性やその対策について、具体的に議論される場が少なく、安全保障の観点から専門的に調査、研究する機関（組織）も少ない。その一つの要因は、量子技術の実用化と脅威においては、前述の様に、俯瞰的かつ多面的な分析が十分なされておらず、まだ先の未来社会ビジョンに向けた取り組みの一つであると考えられているケースが多い。確かに未来社会ビジョンの実現は、国をより豊かにするために非常に重要であるが、それがあまりにも主眼となってしまうと現時点での安全保障の観点での危機感が薄れ、様々な分野で量子技術に対するセキュリティ対策までも先送りにされているケースが多くなっている。

海外では、安全保障の観点で量子技術を先行して実用化させることによるイニシアティブは大きいと強く考えられており、軍関係の研究機関と企業や大学が連携し、具体的な実装をイメージした開発に取り組んできている。特に米国では、直ぐに実際のフィールドで利用できる技術と、実装のために、まだ課題解決に時間がかかり、先になりそうな技術を俯瞰的に分析し明確にすみ分け、前者に対する対策や代替手段採用に積極的に取り組んでいる。また、考えられる脅威に関しては、常にワーストケースを考え、先送りすることなく取り組にできている。日本においても将来的な社会実装とは別に国家安全保障に特化した研究・分析・開発、実装を推進し実行的に牽引できる組織が必要と考える。

特に量子コンピュータの開発競争においては、最初に現代暗号の解読を実現できた組織が、現代の情報化社会や安全保障の分野における優位性を獲得できると言われている。量子コンピュータや量子暗号など、その目的を達成する量子技術には様々な技術やアプローチがあり、それらの一つだけにフォーカスした研究開発では不十分である。それら様々な技術を客観的に捉え、他国の状況、対策すべき時期と実現時期との関係、実装条件や実現に向かうアプローチ等を柔軟に判断すべきである。

第３節 量子コンピュータと AI

量子コンピュータの物理的な動作が、理論にようやく追いつき始め、実機（クラウド利用）を使った実用的な研究開発が可能になった。そのため、その処理能力を AI（Artificial Intelligence：人工知能）に活用しようと、量子コンピュータによる機械学習（量子機械学習）への応用が重要視され、そのキーテクノロジーの研究開発が各国で盛んに行われている。量子コンピュータを利用した AI（量子 AI）は、少ないデータで機械学習アルゴリズムを作成できると考えられている。量子機械学習アルゴリズムの研究としては、個別の計算ステップを高速化だけでなく、量子コンピュータは、少ないデータでモデルを学習させたり、データ構造の検出や分類の精度を高めたりできる可能性があるため、より低い抽象化レベルで動作する量子アルゴリズムの研究が進められてきている。現在、量子機械学習は、量子カーネル法のような量子機械学習に加えて、量子 CNN（ Convolutional Neural Networks：畳み込みニューラルネットワーク）のような量子ディープラーニングの研究も進んでいる

https://techtarget.itmedia.co.jp/tt/news/1904/08/news06.html

https://ainow.ai/2022/04/24/264447/

また、ニューラルネットワークを中心とした人間の知能の根底には、量子学的な現象があることを示唆する研究成果も報告されており、現在の小規模量子ビットの量子コンピュータ（IBM Q Experience）で動作する、人工ニューラルネットワークに関する AI アルゴリズムの開発も行われている https://iopscience.iop.org/article/10.1088/2058-9565/abb8e4/pdf。

100 万量子ビットを超える実用的な量子コンピュータの実現は、Google や IBM のような有力開発企業のロードマップを考慮すると、2030 年前後になると予想されている。しかし、既存のスーパーコンピュータと量子コンピュータをハイブリッド利用するコンピューティング（ハイブリッドコンピューティング）の研究開発が現在盛んに進められており（図 5-2）、それらは実際に利用しながら進化していくと考えられる。日本においても経済産業省で「量子・古典ハイブリッドコンピューティングの基盤ソフトウェア開発」として 2022 年度補正予算を提案しており、2023 年度には「量子・AI ハイブリッド技術のサイバー・フィジカル開発事業」として量子・AI 融合型コンピューティングシステムによるアプリケーション開発を実施するとともに、ユースケースの創出を推進していく予定である https://www8.cao.go.jp/cstp/ryoshigijutsu/13kai/siryo2-4.pdf。

この様な流れからハイブリッドコンピューティングの活用は数年以内に始まり、今後は、量子機械学習の PoC が盛んに行われるだろうと考えられる。AI 業界をリードする Google は、量子技術を AI に応用するフレームワークとしてハイブリッドコンピュータを応用した TensorFlow Quantum（TFQ）を提供している。TFQ は、量子と古典のハイブリッド 機械学習 モデルのラピッド プロトタイピングのための量子機械学習ライブラリである。量子アルゴリズムとアプリケーションの研究では、すべて TensorFlow 内から Google のフレームワークを活用されている。 https://www.tensorflow.org/quantum。

これらハイブリッドコンピュータの進化は、量子コンピュータ単体より早期に実現でき、それぞれの利点を生かした計算処理の分担を行えるため、非常に有効な計算手段となる。これは、同時にサイバーセキュリティを考える上でも、重要な要因であるため早急に検討が必要となる。

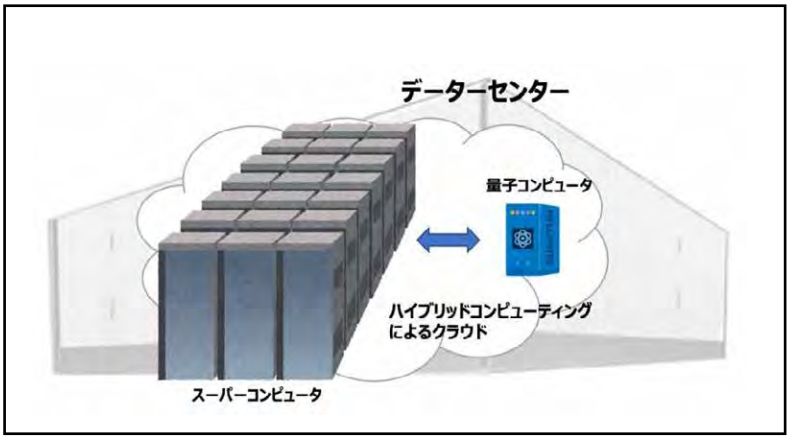


図 5-2　ハイブリッドコンピューティングのイメージ

第４節 暗号と量子コンピュータ

■PQC（Post-Quantum Cryptography）

表 5-2 は、2009 年から 2018 年まで 10 年間の各国の量子コンピュータの研究費推計を纏めたものである。前項（図 5-1）の 2021 年の投資額と比較すると、特に中国の変化が著しく大きい。これは、2020 年前後に急激な進化を遂げだす量子コンピュータの進化の変曲点が大きく影響しているものと思われる。

量子コンピュータは、ビットの「量子の重ね合わせ」と「量子もつれ」を利用し、量子コンピュータ用のアルゴリズムを利用することにより処理が大幅に高速化するため、暗号を直接解読することや、暗号鍵の発見に必要な時間を短縮することが可能になる。現在の量子コンピュータは、まだ量子ビットの少ない開発の初期段階であるが、2030 年以前には、RSA 等の公開鍵暗号は瞬時に解読可能になると予測されている。現在、AES に対しては、指数的に高速に鍵を発見できる量子アルゴリズムである Grover のアルゴリズムが開発されているが、鍵の解読に対して更なる脅威を与えるほどの強力で持続的な処理を実行できるアルゴリズムは、現在まだ発表されていない。しかし、現在進行中の量子コンピュータの研究は、そのような解読処理を実現できるよう進化する可能性がある。（既に水面下での開発で実現されているかもしれないという考え方もある。仮に暗号解読が可能になった量子コンピュータを実現できたとしても、自国の優位性を保つためには、絶対に公開することはない

米国の NIST（米国国立標準技術研究所）や各国のサイバーセキュリティ関連組織は、盗聴者が現在、暗号化されたデータを盗聴（ダウンロード）し、量子コンピュータ等の解読可能なコンピュータを実用化できた途端に復号化する「steal-now and decrypt-later 攻撃」を想定しており、既に、現時点での通信インフラの安全性に対して懸念を抱いている。そのため現在利用している標準暗号を今後も使用し続けるシステムは、セキュリティが侵害される危険性があると考えている。米国の National Security Memorandum 10（NSM10：国家安全保障覚書）は、この予測を見越して、その対策について要件を示しており、NIST は、量子耐性暗号（QRC：Quantum Resistant Cryptography）標準に関する新たなプロジェクトを開始している。（後述で詳細説明）

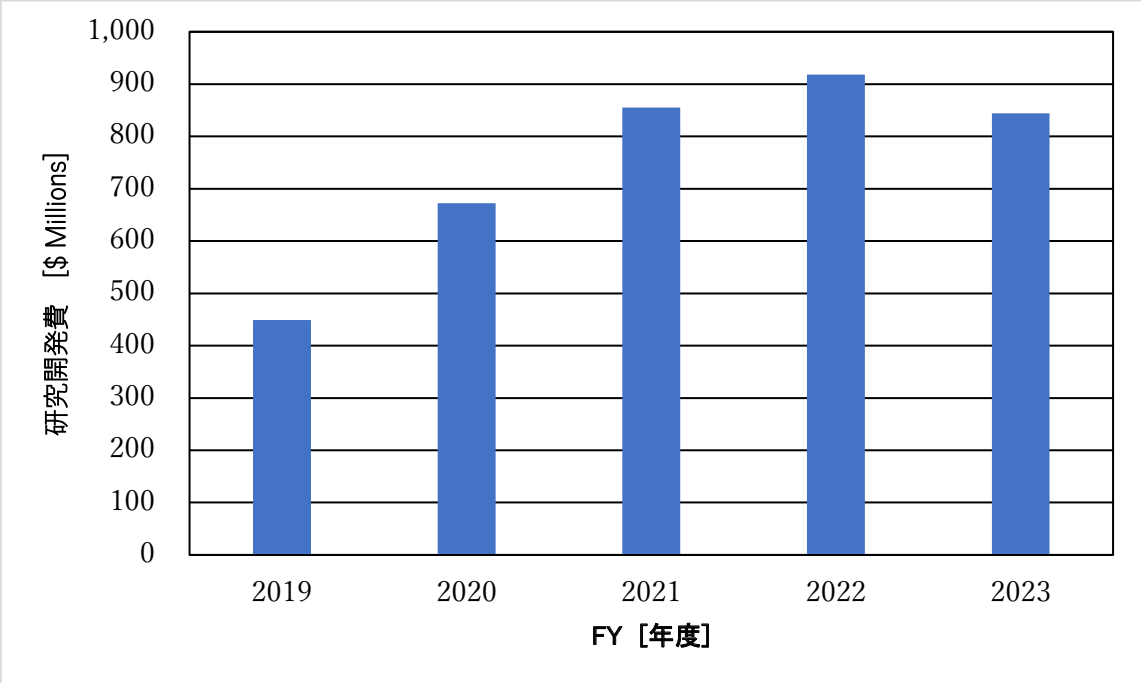
https://crsreports.congress.gov/product/pdf/IN/IN11921/1

表 5-2　主要各国が 10 年間に注いだ量子コンピュータ関連技術の研究費推計（2009 年～2018 年）

国 名	量子コンピュータ 関連技術全体	量子ビット 集積化・システム化	量子コンピュータ クラウドサービス	量子コンピュータ 製造技術
米 国	1060	520	320	640
英 国	830	640	430	760
中 国	630	340	110	280
豪 州	300	160	140	150
日 本	230	80	50	120

US＄　Millions

表 5-2 は、2009 年から 2018 年まで 10 年間の各国の量子関連技術研究投資総額である。また、図 5-3 に示すように米国においては、量子情報科学の予算は、2019 年に 400M$強であり、2022 年の要求額は、900M$弱と倍増している。



https://quantumcomputingreport.com/u-s-qis-budget-proposed-to-grow-10-6-to-877-million-in-fy2022/

図 5-3　米国の量子情報科学の研究開発予算

量子技術の中でも、特に情報通信におけるセキュリティに大きく関与する量子コンピュータ開発は、加速しており、開発投資も長期的に増大していくと考えられる。そのため情報通信の安全性を維持するための対策の緊急性と早期実現（実装）が重要である。現在、米国の NIST で行われている耐量子計算機暗号（PQC：Post Quantum Cryptography）の標準化も、その一連の危機感の流れである。

日本においても、量子コンピュータと現代暗号の安全性の関係を理解し、量子コンピュータの技術課題に対する考え方を多角的に調査し俯瞰的な視点で開発ロードマップを予測し、最悪のケースを考えた対応策の推進が重要である。数理的なソフトウェア暗号においても、物理的な暗号においても実装し整備するには時間がかかるため先行した早期対策が必要である。

■量子コンピュータの開発をリードする IBM の状況（図 5-3）

現在、一般的に入手可能な情報の中で、最も進んでいると思われる量子コンピュータ開発グループは、IBM である。既に 2021 年に実用化している 53 ビットクラスの量子コンピュータは、日本を始め、世界中で稼働し、量子コンピュータアルゴリズムやソフトウェア開発に利用され出している。量子コンピュータの性能を表す量子ビット数も今年（2022 年）に 128 ビットを達成し、更に 400 ビットクラスのデバイスの集積化も実現（IBM Osprey プロセッサー）しており、2023 年には、400 ビットクラスの量子コンピュータが、リリースされる予定になっている。このデバイスは、IBM の量子プロセッサの中でも最大の量子ビット数（433 ビット）であり、古典的なビットの数に単純換算すると 2^{433} ビット相当となるため（量子コンピュータの量子ビット数は、古典コンピュータと違い、1 ビット増えるごとに、指数的に計算能力が向上する）、利用シーンによっては、古典コンピュータの計算能力をはるかに超えるポテンシャルを持つ。更に、従来、プロセッサとの信号の接続は同軸ケーブルを利用していたが、極低温下でも動作するフラットケーブルに変更している。また、量子回路の状態を途中で観測して、マルチレベル配線を利用した信号ルーティングとデバイスレイアウトを柔軟に対応できるよう回路の変更が可能な「動的回路」も搭載する。更に、ノイズを低減して安定性を向上させるための統合フィルタリングも追加されている。

2023 年には 1121 量子ビットの「Condor」を発表する予定であり、同時期に、周辺の高周波部品の高密度化も実行される。更に新たにモジュール化の概念を導入した量子プロセッサ、「Heron」も公表する。また、量子と従来のワークフローをシームレスに統合するハイブリッドクラウドミドルウェアを採用しながら、スケーリングを可能にし、「量子通信」と「計算」を組み合わせて計算能力を向上させるモジュラーコンピューティングアーキテクチャである量子中心のスーパーコンピュータの実現を開始すると宣言している。2024 年には 1,386 量子ビット以上となる見通しの「Flamingo」を公開する計画である。これらは、モジュール化の概念を導入しており、複数のチップ間を 1m 以上の電気配線で結んだ製品となる見通しだ。同年には複数のプロセッサ同士を短い配線で接続した「Crossbill」も公開する予定である。2025 年には、4,158 量子ビットの「Kookaburra」を公開し、それ以降も量子ビット数の向上に取り組む方針である。

一方、課題である誤り訂正技術においては、ハードウェアとソフトウェアの技術を組み合わせることで、実用的なアルゴリズムが動作するようになる。古典コンピュータのリソースを量子コンピュータと協調動作させることで、複数のタスクを実行しても誤りを抑制できる技術の実装などが進む。また IBM で

は、長時間かけて量子回路の計算を実行する際にエラーの発生頻度を抑えるため、実行単位を小さく分けつつ古典コンピュータのリソースで相互につなげる、「回路編み（サーキットニッティング）」の技術についても研究を進めている。

<table>
<tr><th></th><th>2019</th><th>2020</th><th>2021</th><th>2022</th><th>2023</th><th>2024</th><th>3025</th><th>2026+</th></tr>
<tr><td></td><td>IBMクラウドで
量子回路を実行</td><td>量子アルゴリズムと
アプリケーションを
実証および
プロトタイプ</td><td>Oiskitランタイムで
Quantumプログラム
を100倍速く実行</td><td>Qiskitランタイムに
ダイナミックサー
キットを持ち込んで、
より多くの計算の
ロックを解除</td><td>柔軟なコンピュー
ティングとOiskitラ
ンタイムの並列化に
よるアプリケーショ
ンの強化</td><td>スケーラブルなエ
ラー軽減により、
Oiskitランタイムの
精度を向上</td><td>oiskitランタイムを
制御する回路編み
ツールボックスを使
用したスケール量子
適用</td><td>エラー補正のOiskitラ
ンタイムへの統合によ
り、量子ワークフロー
の精度と速度を向上</td></tr>
<tr><td rowspan="2">カーネル開発</td><td colspan="2" rowspan="2">回路</td><td rowspan="2">Oiskit ランタイム</td><td colspan="5"></td></tr>
<tr><td>動的回路</td><td>スレッドプリミティブ</td><td colspan="2">エラーの抑制と軽減</td><td>エラー訂正</td></tr>
<tr><td>システム
モジュール化</td><td>ファルコン
27量子ビット</td><td>ハミングバード 65
量子ビット</td><td>イーグル
127量子ビット</td><td>オスプレイ
433量子ビット</td><td>コンドル
1,121量子ビット</td><td>フラミンゴ
1,386+量子ビット</td><td>クッカブラ
4,158+量子ビット</td><td>古典的および量子的な
1万-10万 量子ビット
へのスケーリング
コミュニケーション</td></tr>
<tr><td colspan="5"></td><td>ヘロン
133量子ビット x p</td><td>クロスビル
408 量子ビット x p</td><td colspan="2"></td></tr>
</table>

https://jp.newsroom.ibm.com/2022-11-10-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

図 5-3　IBM の開発ロードマップ

このような量子コンピュータの進化が、今日のデータ通信の暗号を解読する能力を持つため、新しい暗号システムへの移行が必要である。但しこれには前述の様に時間がかかるため、今から準備を開始することが重要である。2016 年以降、IBM は NIST と協力して、量子コンピュータの脅威に備えるため PQC の標準化にも協力してきている。

2022 年 7 月に NIST は、PQC の 4 つのアルゴリズムを標準化した。これらのアルゴリズムのうちの 3 つ IBM がサポートし開発された。現在 IBM では、この専門知識を業界にもたらし、PQC への移行に向け、ユーザーに IBM Quantum Safe オファリングを提供しており、IBM とボーダフォンは、ボーダフォンと通信業界が量子耐性のある暗号に移行する準備を整えている。

上記の内容を踏まえて、改めて量子コンピュータの性能予測を纏めると、図 5-3 で示したようなロードマップの実現性は高いと考えられる。

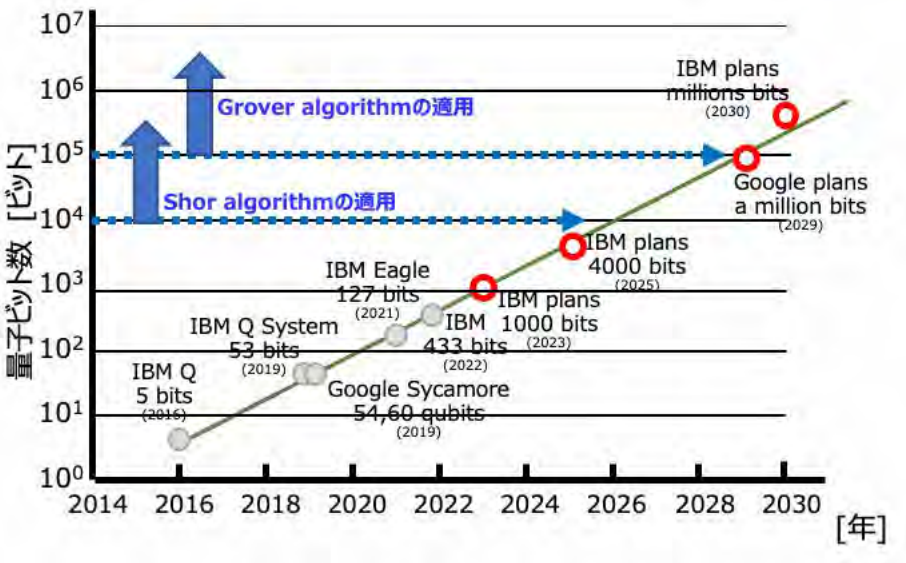


図 5-4　コンピュータの性能予測

現在、既に研究開発されている量子コンピュータ用の代表的なアルゴリズムである Shor のアルゴリズムと Grover のアルゴリズムを使うと、IBM、Google のロードマップ上でも、2030 年前後には、現在主流の公開鍵暗号の RSA や共通鍵暗号の AES は解読されてしまう可能性が非常に高くなる。Shor のアルゴリズは、1994 年、Grover のアルゴリズムは 1996 年に発明されており、まだ量子コンピュータが実現される以前に開発されたものである。現在の利用可能な量子コンピュータは、小規模ではあるが実際に操作させ、クラウド上で利用できる様に運用されているため、実機を利用した更に高度なアルゴリズムの開発も進んでいくと考えられる。(図 5-4)

光ファイバの盗聴においては、前回（2021 年度）報告した様に、光ファイバケーブルから簡単に盗聴することが可能である。工事などを装い、ターゲット拠点近くの通信用マンホールからとう道などへ侵入し、目的の光ファイバケーブルにアクセスしタッピングすることや、架線においては、架線工事を装いユーザー拠点に引き込まれている目的の光ファイバをタッピングすることで信号を確実に抜き取ることが可能である（図 5-4)。

盗聴で得られる信号は、非常に小さく、利用者には気付かれることなく抜き取り続けることも可能であり、この小さな信号は、光ファイバアンプを利用し元の信号を復元することが容易にできる。抜き取った信号が暗号化されている信号であったとしてもそのまま保存することができる。これらの情報は、大規模計算が可能な量子コンピュータが実現できると解読することが可能になる。これが前述の「steal-now and decrypt-later 攻撃」である。

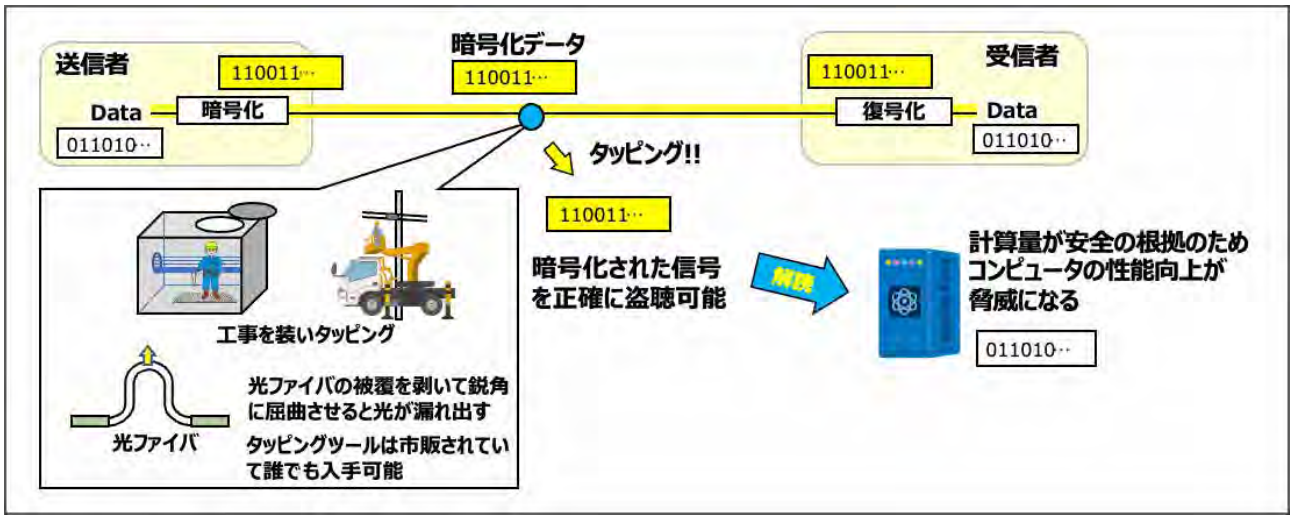


図 5-5　光ファイバの盗聴

前述の様に、IBM を筆頭に、量子コンピュータの開発は、激化しており、また様々な課題に対する隘路事項も同時に解決できる道筋が着実に示されてきており、大規模計算が可能な量子コンピュータの開発において IBM や Google のロードマップを無視する訳にはいかない。

大規模な量子コンピュータが実現できると今日の公開鍵暗号の標準である RSA と楕円曲線暗号は shor のアルゴリズムで破ることができ、ハッカーが次のことが可能になるためデジタル化された経済は機能しなくなる。

・人々の銀行口座や仮想通貨のウォレットを空にする
・機密性の高い通信の傍受と復号化か可能になる
・電力網や通信ネットワークなどの重要なインフラを無効にする
・秘密にしておきたい事実上すべての秘密を暴露する

https://www.insidequantumtechnology.com/news-archive/quantum-news-briefs-september-26-cheng-the-path-to-pqc-migration-biden-administrations-newest-sanctions-on-russia-and-belarus-include-a-ban-on-quantum-computing-pritzker-molecular-engineering-pr/

現在、大規模な量子コンピュータの実用化タイミングは多くの議論があり、多くの予測は 20 年以上先であるとの意見が多い。しかし、脅威は商用量子コンピュータの実用化ではない。クローズドされた実験室等の条件下で進められている暗号解読を可能にするような技術開発の可能性である。それは商用ベースよりもはるかに早くに実現できると考えられる。また、このようなコンピュータが実現できているとしても自国の優位性を保つためには決して公開されることは無い。

以上の様に、我々の情報は、現在既に「盗聴と蓄積」の脅威に曝されているかもしれない。収拾された情報には、政府の秘密、R&D イノベーション、金融サービスの取引データ、および戦略計画等が含まれる可能性がある。いくつかのファイブアイズ・エージェンシーもこの現象がより頻繁になっているとコメントして