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）。

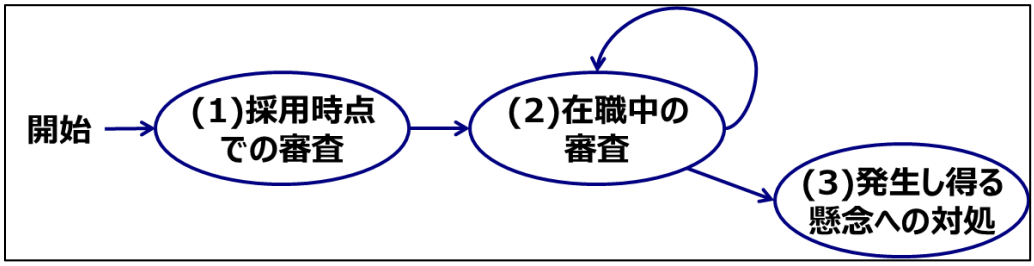

図 4-2-a 従業員の審査プロセスの全体像

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。

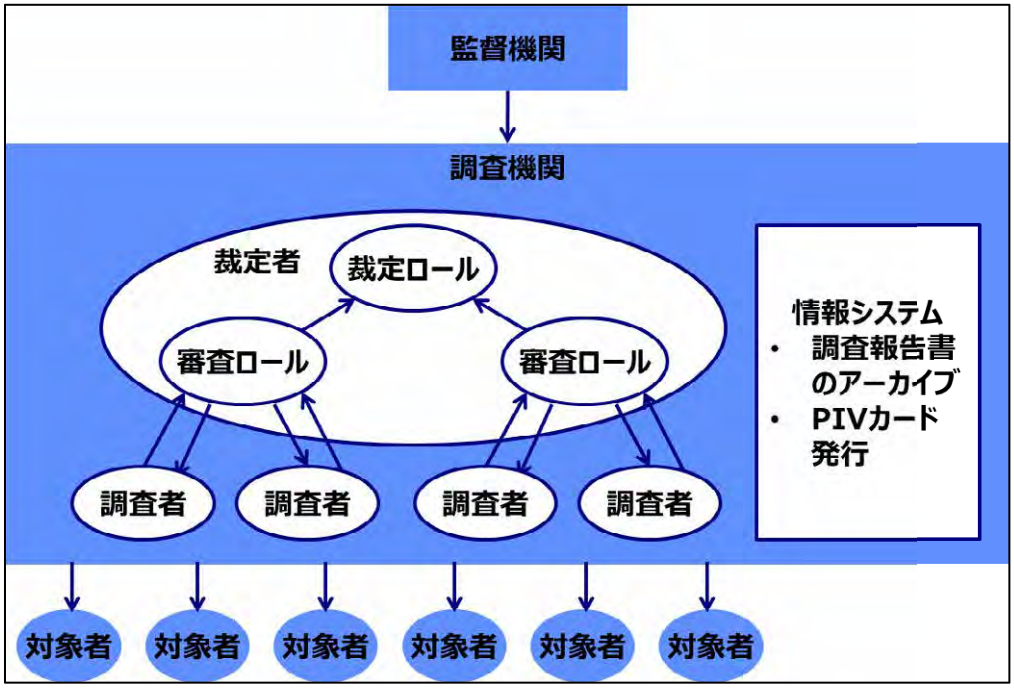

図 4-2-b 審査プログラムの体制図

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。