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。

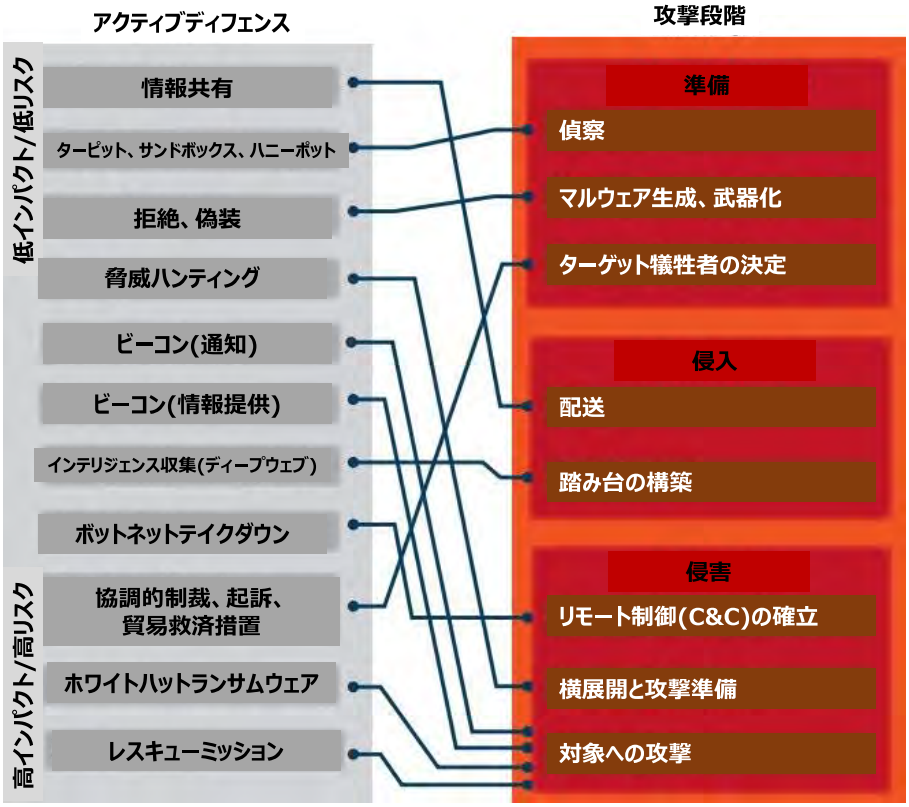

図 3-2：攻撃に影響を与えるアクティブ・サイバー・ディフェンスの活動.[3]

[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。

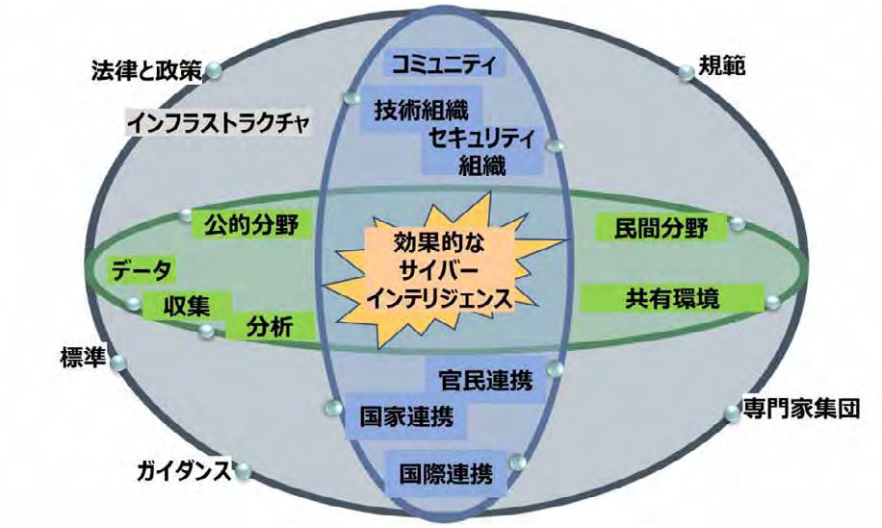

図 3-3. CI エコシステム.

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。

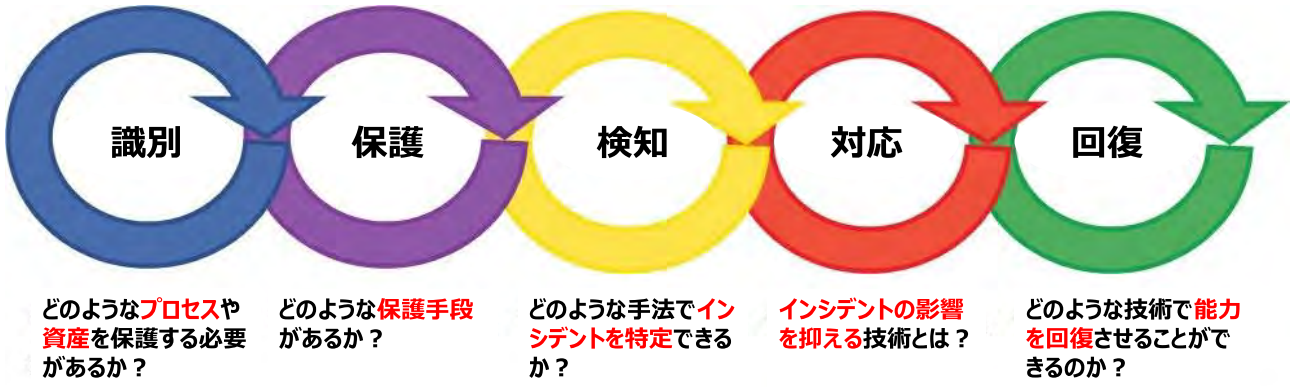

図 3-4：NIST サイバーセキュリティ・フレームワークのコア・ファンクション

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。

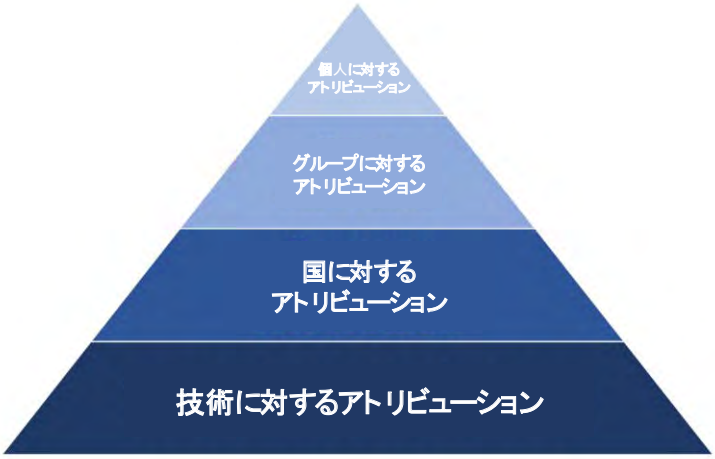

図 3-5. アトリビューションのピラミッド.

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