Active Cyber Defense の背景と論点（Ver.2.0 2023.11.18 掲載）

サイバーディフェンスイノベーション機構　研究部会
アクティブサイバーディフェンス　アドホック
監修　三宅功

はじめに

この White paper は 2023 年末に開催される CYDEF2023 のテーマである「アクティブサイバーディフェンス(Active Cyber Defense)[1]の国際連携」に関して有意義な議論を行うため、サイバーディフェンス研究会の有志[2]により「アクティブサイバーディフェンス」に関するグローバルな視点での論点を調査し、背景、概念等の整理を図ったものである。

CYDEF2023 において「アクティブサイバーディフェンス」をテーマとして取り上げたのは、2022 年末に公表された我が国の国家安全保障戦略に関する防衛 3 文書の中で「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合これを未然に排除し/またはこのようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御の能力を保有する」と言及されたことによる。しかしサイバーセキュリティの観点で、アクティブサイバーディフェンス＝能動的サイバー防御とするなら、グルーバルな議論の中での能動的サイバー防御は上記の議論には止まらない。また、そもそも国家安全保障の観点での能動的サイバー防御は具体的にどのようにあるべきかの議論を進めていく必要がある。

そこで、この White Paper ではサイバーセキュリティの観点でのアクティブサイバーディフェンスとはどのような概念なのか？また、これを議論する上でのサイバーセキュリティの具体的な状況をどう捉えておくべきか？といった議論のための共通理解を促進する枠組の整理、体系化を図ることを目指している。整理の観点として、現在グローバルな議論の中で主にどのような事態を想定して実行可能な技術とプロセスが考え得るかの観点を中心に概念整理する。これを実際にどのように政策的、戦略的に展開するか、或いは国際法含めた法的根拠をどこに置き、構築して行くかは、いまだ議論が進行中であり参考範囲にとどめている。

この White paper はサイバーディフェンス研究会研究部会の有志による議論を通じて整理したものでありその正確性含め極力吟味しているが、問題点も多々存在する可能性がある。これに関しては最終的には監修にあたった三宅に責任がある。また、この White paper は個人的見解の表明であり、特定の組織による意見表明を行うものではないことを付言しておく。

---

[1] 一般的和訳として国内では「能動的サイバー防御」とされているが、この資料ではアクティブサイバーディフェンスと能動的サイバー防御は同じ概念を表すものとする。また、以降 ACD と略記する場合もある。

[2] 参加頂いた方々のお名前を巻末に掲載しています。

本資料の構成とあらまし

第 1 章　現代のサイバー攻撃の背景　- サイバー空間の拡大と進化

そもそも、アクティブサイバーディフェンスが必要と考えられてきた背景は、近年のサイバー攻撃の高度化・多様化と被害の拡大に対して、既存の防御中心のサイバーセキュリティ対策の限界を克服することにある。このようなサイバーセキュリティの状況を認識するには、まず現在のサイバー空間がどのように発展し問題を内在化させてきたかを理解しておく必要がある。そこで、第 1 章では主に現代のサイバー空間の構成、特徴とそのサイバーセキュリティに対する影響についてまとめる。また、そもそもサイバーセキュリティの観点でサイバー空間をどう体系化しておくか、に関する最近の国際的な議論の動向についてもまとめる。

最初に、現代のサイバー空間を形作る、デジタル通信網、インターネットなどのグローバルなデジタルネットワークの基本構造を示すとともに、その普及の状況、さらにはインターネットを中心としたサイバー空間がどのように進化してきたかを簡単にまとめた。ここ数十年という短期間でグローバルにサイバー空間の拡大を可能にした要因は、拡大を促進してきた反面でサイバー攻撃の環境を拡大してきたという負の側面も存在していることを説明する。例えば、インターネットの匿名性の根本原因はその自律分散的な管理に原因があり、インターネットの急速な拡大を支えた一方で、サイバー攻撃元の帰属判断を困難にしていることを解説する。最後に、最近になっていわゆるサイバーセキュリティを理解する上で、サイバー空間をどう認識するかという国際標準化（ISO）での階層化による整理の試みを紹介する。サイバー空間は、単に電気通信網、インターネットといった技術面での構成だけでなくこれを利用する人間及び組織のネットワーク化の側面もあり、サイバーセキュリティもこれらの階層に固有或いは相互に連携した視点が必要であることが示されている。

第 2 章　サイバー攻撃の現状

アクティブサイバーディフェンスを考える場合、実際のサイバー攻撃がどのように行われているかを理解しておく必要がある。そこで第 2 章では現在のサイバー攻撃、特に高度なサイバー攻撃がどのように行われているかについてまとめている。ここでは、まず現在までに観測されているサイバー攻撃をそのアクター、狙い、実行の難易度、影響度といった観点で俯瞰する。現代のサイバー攻撃は、いたずらレベルのものから、組織犯罪による金銭窃取、さらにはテロ組織や国家主体による国家安全保障レベルのものまで多様化している。サイバー攻撃の手法自体もそのアクターや目的に応じて高度化している。ここでは、特に国家主体によるサイバー攻撃に使われる手法として APT[3]攻撃を詳しく取り上げる。Active Cyber Defense が議論される前提の多くが APT 攻撃である。またこのサイバー攻撃の特徴であるボーダレスなサイバー空間を経由しての攻撃手法と攻撃の帰属を含めた抑止、攻撃の無力化の困難さの原因を説明する。ここでは、理解を促進するために、いくつかの典型的な事例をあげることにする。これらの事例より、国家安全保障レベルでの APT 攻撃の具体像の理解促進、課題認識が行えると考えている。

第 3 章　米国、欧州の動向と国連のサイバー規範

[3] Advanced Persistent Attack:第 2 章でその具体的な手法を解説するが、以降では APT 攻撃と記述する。

第 3 章では、Active Cyber Defense に関連した米国及び欧州の具体的な政策、戦略の動向について整理した。また、国連におけるサイバーセキュリティのための国際規範に関する議論と課題の状況を Active Cyber Defense の観点でまとめた。

米国では、2000 年代に入ってサイバー攻撃が拡大する中でこれに対する効率的な抑止方法として Active Cyber Defense がとりあげられるようになった。特に 2010 年代に入り米軍サイバーコマンド(USCYBERCOM)の設立、米国国防総省のサイバーセキュリティ戦略の一環として Active Cyber Defense の実施が提唱された。そこでまず USCYBERCOM のサイバー空間に関する軍事ドクトリンを概観する。また、その中でのサイバー空間における Active Cyber Defense の具体的な実施形態として Hunt Forward について説明する。この概念は、米国内のネットワークを離れ、同盟国・友好国のネットワークに対し USCYBERCOM と連携してサイバー攻撃元の摘発に取り組むものであり一種の Active Cyber Defense の方法と言える。

一方で重要事業者等、民間レベルにおける Active Cyber Defense としては SANS による Threat Hunting が 1 つの手法として提案されている。また、最近になって MITER 社による一種の Active Cyber Defense のフレームワークである MITER Engage が提案されている。これらは APT 攻撃を前提に、各組織のネットワーク内で単に侵入防御だけでなくより積極的に攻撃に対抗するフレームワークとなっている。

EU ではロシアのウクライナへの軍事進攻を受け、欧州議会・理事会がサイバー防衛戦略に関する政策コミュニケを公表した。この中で、Active Defense という用語が使用されているが具体的な政策に関してはこのコミュニケの実現に向けての法案の中で徐々に明確化されていくと思われる。

NATO は 2016 年の NATO サミット（ワルシャワ）で NATO の防衛的任務を再確認し、サイバースペースを NATO が自らを守らなければならない作戦の領域として認識している。また、2021 年の NATO サミット（ブリュッセル）では、ケースによっては武力攻撃と見なされる可能性があり、集団的自衛権の発動（NATO 第 5 条）があり得ることを認識した。通常の武力紛争とは異なり、サイバー領域では絶え間ない摩擦と継続的な活動(偽情報キャンペーン、スパイ活動、ランサムウェア、重要なサービスや重要インフラの機能不全を含むサイバー作戦)が存在するとの認識であり、これがある種の閾値を超えれば、武力紛争に相当すると見做せるとの立場を取っている。この考え方は、米国の立場と同じと言える。2023 年 7 月の NATO サミット（ビリュニス）では、サイバー空間における効果的な防御としてより積極的なアプローチをとることが再度認識されており、詳細は公表されていないもののサイバー防御への包括的なアプローチを採用することが表明された。

英国では、2022 年に策定された策定された国家サイバーセキュリティ戦略の中の 1 つとして Active Cyber Defense を意味する「サイバースペースにおいて、またサイバースペースを通じて英国の安全保障を強化するために、敵対勢力を検知し、混乱させ、抑止する」が取り上げられた。この戦略実施のための指針として、「英国の国益と市民を保護するために、国家、犯罪者、その他の悪意のあるサイバー行為者とその活動に関する情報を検出、調査、共有及び抑止或いは排除」。「国家安全保障と重大犯罪の防止・発見を支援するため、サイバースペースにおいて、またサイバースペースを通じて行動を起こす。」が出されている。この戦略実施のため、政府通信本部(GCHQ)配下に 2016 年に設置された NCSC 及

び、2020 年に英国防衛省と政府通信本部からの要員で構成、設置された英国サイバー軍(NCF)が役割り分担して対応している。

ドイツは、コンピュータ及び通信のセキュリティを管轄する BSI(Federal Cyber Security Authority)を中心に、攻撃緩和のためのインターネットのルーチングの変更、攻撃元の IP アドレス、ドメイン名のハイジャック、脆弱性を持つシステムに対する自動的で大規模な緩和措置の実施、といった一種の Active Cyber Defense が行われている。

フランスでは、民間サイバー防衛に対応する Cybersecurity Agency：ANSSI は Active Cyber Defense を公式には採用はしていないが、国防省が 2019 年に採用したドクトリンでは" lutte informatique offensive (LIO)" Offensive Cyber Fight：軍事目的のためのサイバー攻撃、という軍事ドクトリンを採用している。紛争時のサイバースペースにおける軍事的優位、サイバー脅威を予測、検知、対応することでフランス軍のサイバーレジリエンスを確保するといった観点での検討が行われている。

第 4 章　Active Cyber Defense の概念

第 4 章では、アクティブサイバーディフェンスに関する現在までの議論の状況をまとめる。現時点で、国際的に Active Cyber Defense に関する明確な定義は行われていない。これは、これまでの議論で、Active Cyber Defense を適用する対象事象（実行主体、攻撃強度・リスク等）、適用手法、実施主体（政府機関、民間組織等）、適用範囲（組織内、組織がのネットワーク等）などの前提条件と要件が様々であり、これに依存しない一般的な定義が現状では困難なことによると言える。しかし、大まかな方向としては主に国家主体を中心に行われている、高強度の攻撃である APT 攻撃に着目し、その Kill Chain に対応した Active Cyber Defense の手法とその期待効果、技術面、法制度面含めた議論が主流を占めていると言える。そこで、ここでは APT 攻撃の Kill Chain に対応して考えられている ACD の手法について整理するとともに、これらが用いられる領域（自ネットワーク内、外等）と適用にあたっての問題点等を整理する。

第 5 章　まとめ

この章では、まとめに代えて今回の CYDEF2023 で注目したいいくつかの視点についてまとめてみた。もちろん、会議を通じて新たな視点、論点も出てくることを期待している。

第 1 章　現代のサイバー攻撃の背景　- サイバー空間の拡大と進化

21 世紀に入り、サイバー空間の技術とサービスの進化と拡大、これへの国際社会の依存度が高まることと並行して、サイバー攻撃の多様化、グローバル化、高度化が進んだ。サイバー空間の進化と拡大は国際的にも社会活動や経済の拡大と効率化を促進したが、一方でリスクももたらしている。リスクの 1 つがサイバー攻撃の拡大である。この両者の関係を十分に理解しておくことがサイバーセキュリティの基本であり、Active Cyber Defense を理解する上での前提ともなる。

1.1 デジタル通信網とインターネットの普及

20 世紀後半より通信ネットワークのデジタル化が進展し、音声中心のネットワークである電話網のデジタル化を含め基本的な通信サービスのデジタル化が行われた。特に、1990 年代より半導体技術、無線通信技術の急速な進化により、デジタル移動体通信網のコモディティ化が進展した。2000 年代初頭に行われた第 3 世代デジタル移動体通信の国際標準化はその流れを加速させ、いわゆる開発途上国にもデジタル移動体通信網が拡大した。一方で、パーソナルコンピュータの普及と相まってコンピュータネットワークとしてのインターネットが 1990 年代後半より主に先進国の間で普及拡大した。インターネットは電子メールや Web といった利便性の高いアプリケーションとセットで進化することが、その急拡大に繋がった。インターネットはデジタル通信網の上に階層的に構築されたネットワークである。2000 年代に入り、デジタル移動体通信網を介したインターネットの利用が可能になることで開発途上国でのインターネットの利用も拡大した。図 1.1、1.2 にグローバルな観点でのデジタル移動体通信網とインターネットの普及状況を示す。

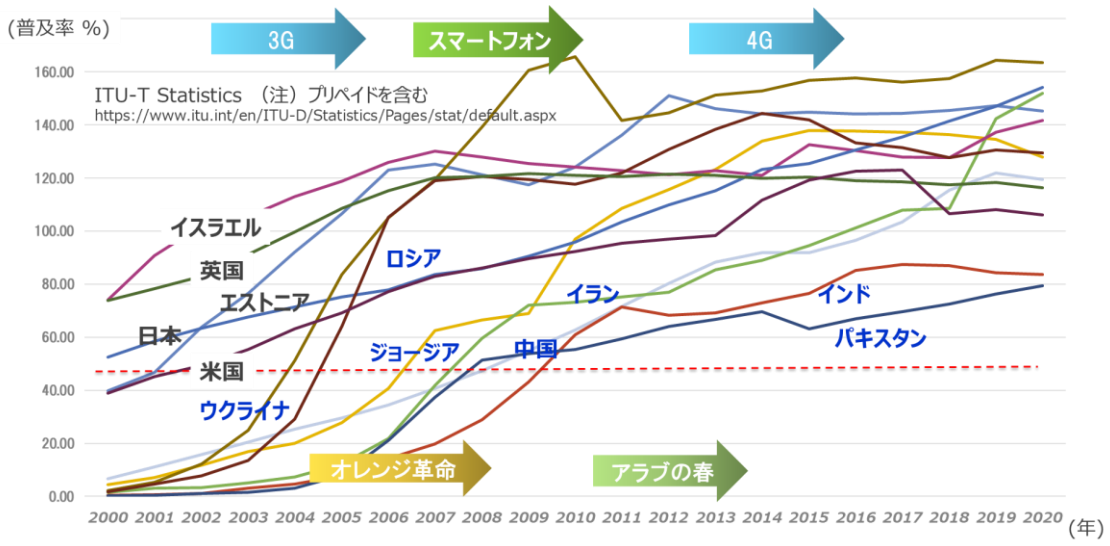

図 1.1　デジタル移動体通信網の国別普及状況

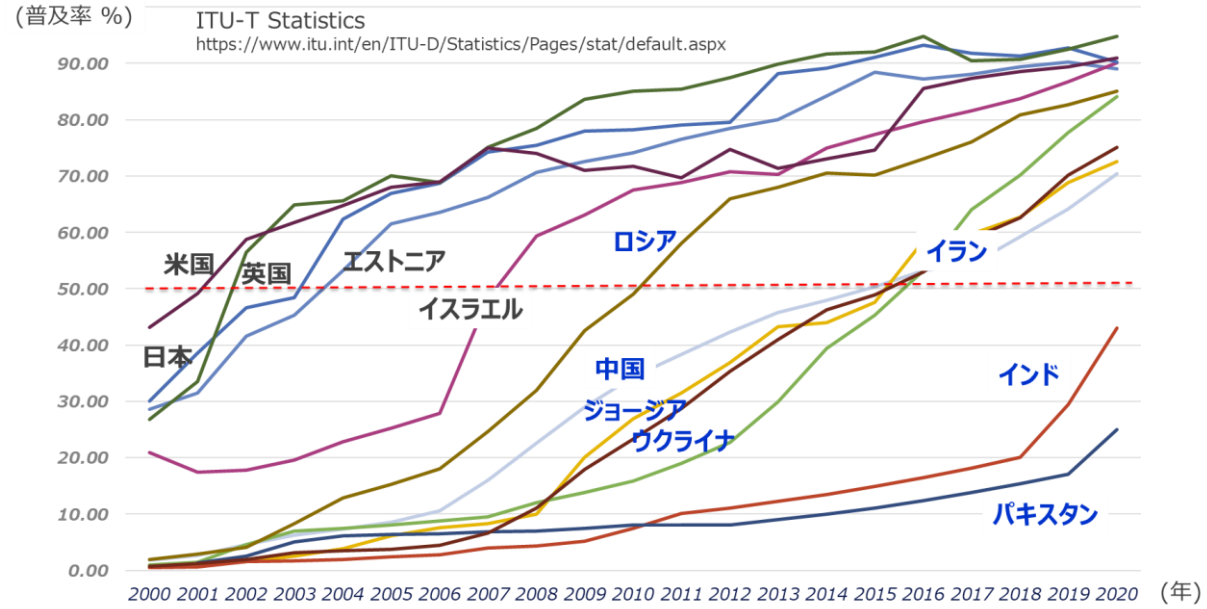

図 1.2 インターネットの国別普及状況

デジタル移動体通信網やインターネットの世界的なコモディティ化はオレンジ革命や、アラブの春といった開発途上国における民主化の流れを加速したことはよく言われる話であるが、以上の普及状況を見ると確かに相関性が高いことが見て取れる。さらに言えば、このような民主化の流れに対抗してロシアや中国において国家主体によるインターネットやデジタル移動体通信網の監視、統制がとられるようになったのも首肯できる。

また、サイバーセキュリティの観点では、信頼性が必ずしも保証されないユーザ、システムのインターネットの参加が拡大したことも見逃せない。後でも述べるが、インターネットが保証するのはあくまでエンドポイント間の接続であり、エンドポイントの信頼性を保証するものではない。従って、セキュアなインターネット接続のためにはエンドポイントの信頼性を保証、保護する機能の実装や、それを規範、制度的に保証する社会的な仕組みが必要になる。しかしながら、20 世紀後半から普及したインターネット上の様々なアプリケーションやサービスは利便性が先行し、信頼性を保証する仕組みは後手に回った。また、21 世紀に急拡大した発展途上国でもこれらの整備が後手に回り、踏み台も含めサイバー攻撃の温床になってしまったということも言える。

2023 年現在、世界の携帯電話保有数は 54 億 8,000 万（世界人口の 68.3%）、インターネット接続ユーザ数は 51 億 8000 万人（世界人口の 64.4%）との統計結果も報告されており[4]今や移動体通信とインターネットはサイバー空間を形成する世界的なインフラになったと言える。

1.2 デジタル通信網とインターネットの階層構造

[4] DataReportal より https://datareportal.com/reports/digital-2023-april-global-statshot

現代のデジタル通信網とインターネットの関係は図 1.3 に示すような階層構造となっている。基本デジタル通信サービスの公衆サービスである電話網や移動体通信網は国毎にその運営事業者（通信キャリア）が存在し、グローバルには ITU-T[5]により割り当てられた国別の識別番号と国毎のキャリアが割り当てた加入者番号がユーザ端末識別のために付与されている。これによってグローバルな相互接続が可能となっている。つまり、公衆電話網、移動体通信網は各国の通信キャリアによってユーザ端末がその加入者番号によって管理され、通信も発着番号によって明確に識別されている。

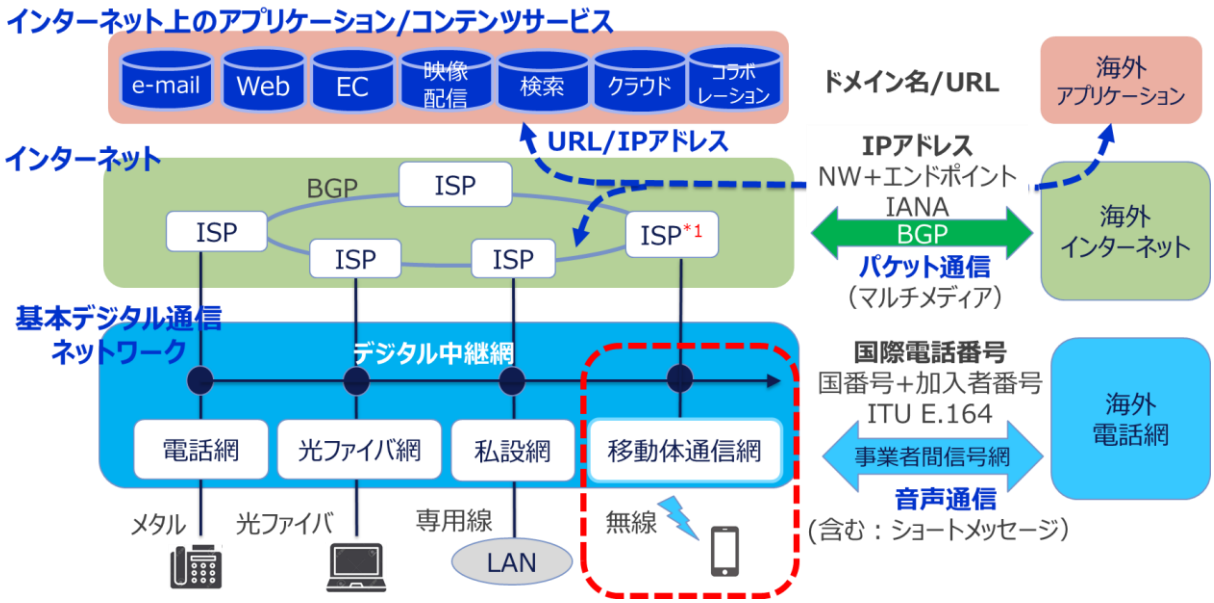

図 1.3 デジタル通信網とインターネットの階層構造

一方で、インターネットとはその言葉の意味する通り、個々に構成されたコンピュータネットワークを相互に接続するサービスを提供している。コンピュータ間の通信は IETF[6]で標準化されたパケット通信の技術標準(TCP/IP)によって行われる。インターネットが意味するところは標準化された技術仕様に基づいたコンピュータネットワークを繋ぐネットワークであり、インターネット全体を管理する組織は無い。次節で述べるが様々な要因によりインターネットは自己増殖的に拡大し、グローバルなサイバー空間を形成してきた。

1.3 インターネットとそのセキュリティ課題

以下ではインターネットの概要とこれが内包するセキュリティの課題について概観する。

インターネットアーキテクチャの概要

[5] ITU-T：International Telecommunication Union Telecommunication Standardization Sector。ここで、国際電話番号の付与標準である E.164 が規定されている。

[6] Internet Engineering Task Force：インターネットの技術標準を作成するグローバルな民間組織。

① パケット通信は、通信データをパケットと呼ばれる単位でまとめ、パケット毎に送信元・受信先を示す IP アドレスが付与されている。これによりインターネット上でパケットが転送され、双方向の通信を行うことができる。

② パケットのデータ形式は、伝送媒体（イーサネット、無線 LAN、移動体通信、光ファイバ等）によらず同じ形式で通信相手まで送られる。つまり、パケットの転送は様々な伝送経路を繋いで構成することができる。異なる伝送路を相互に接続するにはゲートウェイが用意される。ゲートウェイには必要となるパケットの転送機能に応じてスイッチやルータといった種類のものがある。

③ インターネットを構成する個々のネットワークには一意のネットワークアドレスが付与されており、これに接続されるコンピュータに付与するホスト[7]アドレスと組み合わせて 1 つの IP アドレスが構成される[8]。これにより、インターネットに接続される個々のホストは、ネットワーク全体で唯一のアドレスを持つことになり、エンドツーエンドの通信が可能となる。

④ パケットはネットワークアドレスに基づいて複数のネットワークを繋いで転送処理される。該当するネットワークアドレスを持つネットワークにパケットが到着した段階でホストアドレスが参照され該当するホストに転送される。

⑤ グローバルな環境で異なるネットワーク間を繋いでパケットを転送可能とするために、AS(Autonomous System)が定義されている。AS は複数のネットワークで構成可能だが、他の AS との接続は必ず AS 間ゲートウェイを介して行われる。AS 毎にこれを一意に識別するための AS 番号が付与されておりこの番号を用いて IETF で標準化されたルーチングプロトコル BGP(Border Gateway Protocol)によって AS 間のパケット転送が行われる。

⑥ インターネット上での発着間ホストのパケット通信はこの間にある複数の AS がパケットを中継処理することで行われる。中継ルートは固定的なものではなく途中の AS の状態に依存して変動し、必ずしも通信可能性が保証されているわけではない。通信の保証や保護（正確性、秘匿性等）は、あくまで発着間ホストのパケットの再送制御など、インターネット上のパケット転送とは別のメカニズムで実現することが前提となっている。インターネットインターネット上のパケット転送にはこれを保証する仕組みはない。これはベストエフォートの原則と言われている。

⑦ IP アドレスはコンピュータが処理しやすい構造で定義されており必ずしも人にとっての可読性が良いわけではない。そこで、特定のホストを識別するためにホストの名前を示すドメイン名が導入されている。従って、ドメイン名はそのホストの IP アドレスとは一意に対応している。また、ドメインネームもインターネット上での一意性を保証するために、一定のルールに基づいて階層的に記述されるようになっている[9]。

---

[7] ホストとは一般的にネットワークに接続されたコンピュータを意味している。従来は複数の端末から接続されるサーバの概念を意味していたが、現代ではパソコンやスマートフォン、IoT 機器含めたインターネットへの接続機能を有するコンピュータを含んでいると考えてよい。ここでは従来からインターネットで使われているこの用語を使用している。

[8] 例えば次を参照 https://www.kagoya.jp/howto/it-glossary/network/ipaddress/

[9] 詳しくは JPNIC https://www.nic.ad.jp/ja/dom/system.html を参照。

⑧ ドメイン名と IP アドレスの対応関係をインターネット全体に公開するために DNS(Domain Name Server)が IETF の標準に基づいて用意されている。この DNS もドメイン名の階層に対応して階層的に用意されている [6]。

インターネットのリソース管理と匿名性

以上のアーキテクチャにより、インターネットを構成する基本単位はこれに接続された個々のネットワークであり、共通の技術標準に基づいて接続を行うことでインターネット全体の任意のホストに接続できる構造を形作っている。ホスト間の任意の接続を保証する主な要素はネットワーク全体で個々のホストに一意に割り振られた **IP アドレス、ドメイン名**及びネットワーク間のルーチングを保証する **AS 番号**になる。この 3 要素は**インターネットリソース**とも呼ばれ、その一意性を保証するためのリソース割り当てと管理は ICANN（Internet Corporation for Assigned Names and Numbers）が中心になり、その傘下で世界の地域別に設立されている RIR(Regional Internet Registry)[10]及びさらにその傘下の国別に設けられた NIR[11]（National Internet Registry)に権限が委譲されて行われている。

このようにインターネットではネットワーク全体で管理されているのは相互接続に必要な最低限のリソースであり、そのリソースを自ネットワーク内でどのようにホストに割り振り、管理するかは個々のネットワークで実施されている。さらに言えば、IP アドレスとホストの対応関係も固定的なものではなく、IP アドレスはあくまでインターネットを経由してグローバルな通信を行うためのインデックスである。つまり、インターネット自体はこれに参加するホストが何であるかには一切関与していない。どのようなホストをインターネットに接続させるかは、あくまで個々のネットワーク単位に管理されることになっており、インターネットへの参加の自由度を著しく向上させている一方、誰が参加しているかわからないといった"**匿名性**"の問題を内在させることになる。

インターネットのネットワーク管理

インターネット全体を管理している組織体は存在しない。その参加者（ステークホルダ）が相互に協調して管理を行うことを前提として構成されている。従って、インターネットを介した信頼性の高い通信のためには、インターネットの状態の可視化とエンドエンド間の通信保証のためのホスト情報の取得が最低限必要となる。これを実現するために、インターネット上では様々なステークホルダが開発、構築或いは利用する通信プロトコル、オープンソースツール、データベースが用意されている。以下いくつかの代表例をあげる。

①whois 検索：インターネットのリソースである IP アドレス、AS 番号、ドメイン名は ICANN 傘下でこれを分散管理しているインターネットレジストリに登録、管理されている。Whois 検索はこの情報を自由に検索できるサービスでありインターネットレジストリから提供されている。IP アドレスで検索した場合、そのネットワークアドレス情報、ドメイン名、それを登録している組織の情報（組織名とその住所）などが得られる。通信しているホストがどこの組織に属するかをこれで検索できる。登録組織の住所から

---

[10] ARIN:北米（メキシコを除く）地域、RIPE NCC：ヨーロッパ、中近東、北アフリカ、アジアの一部、APNIC：アジア太平洋地域、LACNIC：ラテンアメリカ、カリブ海、

[11] ICANN 及び RIP はそれぞれ民間組織であるが、NIR は国によって異なっており、米国、日本、欧米は民間組織だが中国は工業情報化部の下部組織で行われている。

該当する IP アドレスの地理的な位置をある程度推定できる。ただしこの Whois 検索の情報は登録事業者側が維持管理しており、必ずしも最新のものではないことには注意を要する。

②ping, traceroute, ICMP：接続元のコンピュータが接続先のコンピュータへの接続可能性、接続経路、或いは障害の有無等を確認する通信プロトコル。コンピュータのオペレーティングシステム（OS）レベルで実装されており、原則としてインターネットで相互接続可能なコンピュータには必ず実装されている必要がある。

③BGPlay, BGPmon :AS 間のルーチング状態を監視するツール群でありインターネットレジストリが保有する AS 及び BGP のルーチング情報に基づいてこれらが正常なネットワーク接続を維持できているかを監視するツールである。

④Shodan, Censys：IP アドレスに基づいて、これに接続されているコンピュータの属性情報（利用可能なポート番号、提供サービスとその属性情報、サーバ証明書等）を検索できるオープンソースのツール。

これらのツールを利用して個々のネットワークの運用管理者がインターネットの接続性を監視し、相互に協力しながら問題対応にあたっている。またネットワーク運用管理者のコミュニティといったある意味ボランティアの組織を通じて相互の技術情報や障害情報の共有が行われている。

以上のようなインターネットを運用管理するツール群は必要に応じて、IETF 等で技術標準が整備されるとともに主にオープンソースソフトウェア[12]で実装が行われている。これらは、あくまでインターネットを正常に運用管理するためのものだが、一方でサイバー攻撃のための情報収集やツールとしても利用可能であり実際に利用されている。

インターネット上の様々なアプリケーション、サービスの進化とセキュリティ問題

インターネットの急速な展開は利便性の高いアプリケーションやサービスが誰でも利用可能な環境で開発・導入された点にある。以下では、利便性が高いことから急速に拡大する一方で、セキュリティの観点での問題が顕在化しているアプリケーション、サービスをいくつか取り上げる。

①電子メール

最初のキーラーアプリケーションは e-mail(電子メール)である。元々、電子メールには ISO を始めとしたいくつかの国際規格の流れがあったが、IETF によるインターネット上での電子メール普及のための様々な技術の標準化が推進され[13]、またこれに必要な基本ソフトウェアがオープンソースとして公開されたこともあり、インターネット上の基本サービスとして普及、拡大した。

ただし、初期の標準は電子メールの送受信に必要な基本機能のみが実装され、送信元の確認、メールの暗号化などのセキュリティ対策は後手に回ったことも事実である[14]。セキュリティ機能実装のためにはク

---

[12] 一定のライセンス条件の下で公開され、誰でも無料で自由に利用可能なソフトウェア

[13] 利用される文字コード、送受信・リレー機能、インターネット上で一意にユーザを識別するためのドメイン名を利用したユーザ名の記述法など。例えば次を参照 https://jprs.jp/related-info/event/2013/0409EAI.html

[14] 初期の uucp 接続での中継のような「性善説による」設計があり、そこに添付ファイルや各種セキュリティ機能など様々な拡張を後から追加するなど古い土台に拡張を続けており、根本的なセキュリティ対策が難しいという見方があり

ライアント側の電子メールソフトだけでなくこれを送受信・転送処理するための POP/IMAP[15]サーバソフトの更改が必要でありコストもかかる。実際に更改するか否かはこれを利用している個々のネットワークの判断にゆだねられている。このことは電子メールのセキュリティ対策がなかなか普及しない課題の１つである。

②Web(World Wide Web)[16]

Web は欧州原子核研究機構（CERN）のティム・バーナーズ＝リーにより開発された文書中に別の文書の URL[17]への参照を埋め込むことで（これをハイパーリンクと呼ぶ）インターネット上に散在する文書同士を相互に参照可能にする書式を規定したものである。この書式に基づいて記述された文書（コンピュータ上ではファイル）をハイパーテキストと呼び、このファイルが保存されているサーバを Web サーバ、これを端末側（クライアント）で標準化された通信手順(http: hyper text transfer protocol[18])で取り込んで表示するソフトウェアがブラウザである。この Web の仕様は IETF や W3C[19]を中心に様々な機能拡張が行われ現代のインターネット上の情報空間を形成する基盤技術となっている。

例えば、ハイパーテキストではブラウザ側で実行するソフトウェアも記述することが可能であり、このソフトウェアを取り込んだクライアント側で様々な処理が実行可能な仕様に拡張されている。Web は標準化された仕様が公開されるとともに、構築に必要な基本的なソフトウェアがオープンソースの形で提供されることで、インターネットのキラーアプリケーションとして爆発的に普及した。

しかしながら、初期の仕様には電子メールと同じくセキュリティ的な脆弱性を含むものであった。例えば、http の仕様にはサーバ、クライアント間の認証、通信の暗号化に必要な手順が含まれていなかったため、その後仕様が拡張され https[20]として標準化された。しかし https を実装するにはサーバのソフトウェアの更改や証明書の取得、更新といった付加的な費用がかかることから現在でも全ての Web サーバに実装されているわけではない[21]。また、Cookie[22]といった機能はクライアント側での処理状態を保存し Web サーバ側に通知する機能であるが、クライアント側の処理に付随する個人情報やクライアント・サーバ間の認証情報が含まれることからある種のセキュリティホールを生む原因になっており、その利用範囲の議論は現在でも続いている。

③商用インターネットサービスプロバイダ(ISP)の普及拡大

---

15 POP: Post Office Protocol https://ja.wikipedia.org/wiki/Post_Office_Protocol
IMAP: Internet Message Access Protocol https://ja.wikipedia.org/wiki/Internet_Message_Access_Protocol

16 https://ja.wikipedia.org/wiki/World_Wide_Web

17 Uniform Resource Locator インターネット上のコンピュータにある文書（ファイル）を一意に識別するための記法。
https://ja.wikipedia.org/wiki/Uniform_Resource_Locator

18 初期の基本的な仕様は RFC2616 等で規定

19 https://www.w3.org/

20 正確には RFC2818 HTTP Over TLS で規定。その後 RFC 9110 に更改。https://ja.wikipedia.org/wiki/HTTPS

21 最近では Let'sEncrypt など無料の証明書の普及により https が普及。google は 2014 年から SSL のサイトを優先、2018 年からは Chrome で平文 http のサイトは警告が出るようになっている。一方で、https 化以前に設置され更改されていない Web サーバも依然として残っている。

22 https://ja.wikipedia.org/wiki/HTTP_cookie

電子メールや Web といったアプリケーションの普及と並行して、1990 年代以降、商用 ISP サービスが広く普及した。インターネットを利用するには、パソコンやサーバ、スマートフォンといった端末を基本デジタル通信サービスを提供している通信事業者を経由してインターネットに接続する必要がある。商用 ISP は自らが管理する IP アドレスを各端末に割り振るとともに、これに基づいたインターネット接続を提供するプロバイダである。

元々インターネットを利用するにはこれに参加する組織が個々にインターネットリソースを獲得し、接続のための機器（ルータや DNS サーバ等）を設置して運用管理する必要があった。この場合、インターネットの利用ユーザはその組織のメンバに限定されることになる。商用 ISP はこのインターネットへの接続機能を共用化し、商用サービスとして提供する。商用 ISP にはインターネット接続に特化したものから通信事業者のサービスとバンドル化されて提供されるも、電子メール等のサービスをバンドルしたものまで様々な提供形態があるが、一般ユーザや中小企業はほとんどが商用 ISP を利用している。商用 ISP は自らデジタル回線を所有する必要が無くインターネットへの接続基盤を用意すれば良い事、規制が緩やかなことなど[23]から数多くの事業者が生まれ、インターネットサービスの普及に拍車をかけた。また、商用 ISP を相互接続することに特化した事業者も現れた。

商用 ISP はインターネットサービスの基盤を形成している分セキュリティ対策が重要となる。ただし、現状でもグローバルで見て基本的な対策が共通して取られているとは言い難状況にある[24]。

④フリーWeb メール

基本的に電子メールを利用するには、インターネットに参加している個々のネットワーク毎にメールサーバを設置し、このメールサービスに対応したドメイン名を DNS に登録するとともに、このドメイン名に紐づいたユーザのアカウント登録管理も個別ネットワーク毎に行う必要がある。また、利用にあってはユーザ側でメールの作成、送受信を行うメーラと呼ばれるソフトウェアを用意しておく必要もある。従って、ユーザから見ればインターネットに接続できる環境ではあっても必ずしもメールアドレスを個々人が取得して電子メールを利用できるわけではなかった。商用 ISP が提供するメールサービスも基本的にはメールアカウント毎に料金が発生する仕組みになっている。

これに対して、1990 年代後半からフリーWeb メールサービスが提供されるようになり、電子メールの普及に拍車をかけた。代表的なものとしてはマイクロソフトが始めた hot メール、ヤフーが提供した yahoo メール、さらには Google の G-mail などがある。これは基本的にクラウド型のサービスのため汎用のブラウザからサービスを提供しているサーバに接続し、ID とアカウント名を登録するだけで簡単に個人のメールアドレスが取得できる仕様になっている。メールソフトを自分の端末にダウンロードして個別に設定する必要は無い。このことから、その利用が急速に拡大した。

一方で、メールアカウントの作成はユーザの登録だけで利用可能となる。ユーザの本人確認は一切不要であることから、世界中誰もが自由にアカウントを作成可能であり匿名性を持たせることが可能である。このため、実在しないユーザのアカウントを作成し、サイバー攻撃のための機密情報の取得や情報交換に

---

[23] 我が国でも届け出制

[24] 例えば次を参照 https://blog.barracuda.com/2020/01/27/world-economic-forum-launches-isp-initiative-to-curb-cybercrime

利用するケースが発生している。基本的に通信の秘密遵守のため裁判所の令状が無い限り通信内容のモニタリングはできないため、この種のサイバー攻撃の発見は他の状況証拠がない限り困難になっている。

⑤電子掲示板、SNS[25]

電子掲示板は特定の話題に関して Web サーバを通じて情報を共有する仕組みと言って良い。基本的にはユーザ登録を求められるが、これも自己申告ベースであり匿名性が高い。電子掲示板は様々な情報共有に利用されているが、中には会員限定サービスとして参加者を厳密に制限（例えば既存参加者からの招待しか受け付けない）したものもある。

一方 SNS は”インターネットを利用したコミュニティ型の会員制の情報共有サービス“として立ち上がったが、現在ではユーザ間のコミュニケーション、不特定多数のユーザへの情報配信、利用メディアも単なる文字情報から映像情報へと多種多様なものが開発され利用されるようになった。具体的には Facebook, YouTube、Twitter(現 X)、WhatsApp, Instagram, WeChat, TikTok など様々なものが出されている。基本的なビジネスモデルはターゲット広告といった広告収入に依存しており、サービス自体は無料で提供されるがユーザの嗜好に合わせた広告が挿入される。これは、不明朗な個人情報の取得に繋がりかねないことから、現在でもその在り方の議論が続いている。

2023 年現在、世界のインターネットユーザ数 51 億 8000 万人（世界人口の 64.4%）のうち 93.5%の約 48 億人が何らかの SNS アカウントを持っていることが報告されている。これらの利用動機のトップは情報の取得（第 2 位は家族、友人との繋がり）であり、テレビや新聞といった旧来のマスメディア以上の新たなメディアになっていると言える[26]。

このことから、SNS で形成された情報空間は、デマやプロパガンダ、偽情報といった情報操作の温床になりえることを示している。実際に大きな問題になっているのが「トロール」行為である。元々トロール[27]とはオンラインゲームなどを中心に特定のユーザが、あらし、迷惑行為を実行して対戦相手を妨害するといった意味で使われていた。これが、政治問題に対する情報操作、テロ行為の拡散、選挙介入といった面で組織的に利用されるようになっている事例が確認されるようになってきている[28]。実際、組織的にトロール用のアカウントを作成し IS（イスラム国）がリクルートやハイブリッド戦に利用した事例、ロシアが「トロール工場」により組織的にプロパガンダ、情報操作を実行し、米国を始めとした複数の国の選挙戦に影響を与えた例など多くの事例が報告されている。特に、現在はアカウントの自動生成だけでなく、AI を利用した画像、文書等の自動生成によるトロールの自動化までが確認されており、SNS の兵器化ともいえる状況を呈している。

⑥インスタントメッセンジャー

インスタントメッセンジャー(IM)はインターネットを利用したリアルタイムコミュニケーションの位置づけで登場したサービスであるが、現在は文字情報の転送だけでなく音声、ビデオ通信といった機能も利用可能な

---

[25] SNS の進化と問題については以下にまとめられている。
電子情報通信学会　通信ソサエティ誌　2020 春号
https://www.ieice.org/~cs-edit/magazine/ieice/spsec/Bplus52_sp.pdf

[26] DataReportal より https://datareportal.com/reports/digital-2023-april-global-statshot

[27] https://ja.wikipedia.org/wiki/%E8%8D%92%E3%82%89%E3%81%97

[28] 例えば”「いいね！」戦争 兵器化するソーシャルメディア”、P・W・シンガー他、2019 年

サービスが続々と生まれている。いわゆるチャットも現在では同様の機能を持ったものが出てきており、広義のインスタントメッセンジャーとも考えられる[29]。インスタントメッセンジャーにはエンドツーエンド暗号化が可能で秘匿性の高い Telegram[30], Signal[31]といったアプリが開発利用されており、政府機関、司法機関に対する盗聴、検閲の防止が可能となる。この問題は、もろ刃の刃要素があり、ロシア、中国、香港などで反体制運動に利用されている一方で、一般の司法機関がそれまで一定のルールの下で犯罪捜査として可能であった盗聴行為も無効になる。最近訴訟問題となって話題の NSO[32]はこれを可能にするためにスマホ端末にスパイウェアを仕込んで盗聴するソフトウェアを提供しているが、その違法性に関する議論は進行中である。

⑦インターネットを利用した決済処理

インターネットを利用する一般ユーザの拡大に伴って、これを利用した決済処理も急増している。銀行口座に対する入出金処理、物販・サービスに対するオンラインでのクレジットカード、電子通貨によるキャッシュレス決済処理[33]から公共料金・税金の処理まで様々なサービスが社会生活で利用されるようになってきた。我が国においても例えばキャッシュレス決済に関しては 2022 年の段階で総額 111 兆円、決済処理の 36%を占めるようになっている[34]。利用拡大に伴い、主に金銭窃取を目的としたサイバー犯罪も年々増加の傾向にあり例えば我が国において 2022 年のクレジットカードの総被害額は約 437 億円と推定されている[35]。最近の傾向は、サイバー攻撃の分業化であり、サイバー攻撃で取得した大量のクレデンシャルをダーク Web 上で販売し、これを利用して別の犯罪グループが実際の金銭窃取を実行するといった傾向が高くなってきている。

⑧スマートフォンの普及

2023 年第一 4 半期の時点で世界のモバイルユーザ 54 億 8000 万のうち 6 分の 5 がスマートフォンになっているとの推定が行われている。スマートフォン市場の OS は Google が提供する Android と Apple の iOS であり両者で世界市場、日本国内市場とも 2 分している（図 1.4）。Android は様々なハードウェアベンダが端末機器を Android OS を搭載した形で供給するのに対して、iOS は Apple が端末と一体型の iPhone のブランドで供給している。両者ともアプリケーション開発用のインタフェースと開発環境が用意され、またアプリケーション自体も Google Play, Apple Store から一定のセキュリティチェックを行った上でダウンロードされる。

---

[29] https://ja.wikipedia.org/wiki/%E3%82%A4%E3%83%B3%E3%82%B9%E3%82%BF%E3%83%B3%E3%83%88%E3%83%A1%E3%83%83%E3%82%BB%E3%83%B3%E3%82%B8%E3%83%A3%E3%83%BC#cite_note-5

[30] https://ja.wikipedia.org/wiki/Telegram

[31] https://signal.org/ja/

[32] https://ja.wikipedia.org/wiki/NSO_Group

[33] キャッシュレス処理はオンラインのものと対面販売でのキャッシュレス決済を含んでいる。

[34] https://www.meti.go.jp/press/2023/04/20230406002/20230406002.html

[35] 日本クレジット協会資料 p34
https://www.j-credit.or.jp/information/statistics/download/statistics_domestic_2022.pdf

両者とも一定のセキュリティ対策は行っているものの、懸念が一掃されているわけではない。Android の場合は、端末がマルチベンダで供給されることからハードウェアベンダ側のセキュリティに対する脆弱性が懸念される。具体的にはベンダが供給するハードウェアにバックドアが仕込まれる、或いはファームウェアにマルウェアが仕込まれるといったサプライチェーン上の懸念が指摘されており、5G に関して米国では Huawei 端末の利用が禁止されたのは周知のことである。また、アプリケーションに関しても jailbreak[36]といった OS の脆弱性を突いくことで正規のダウンロードサイト以外からアプリケーションをダウンロードさせて利用するといった行為が古くから行われている。

スマートフォンの脅威は、これだけに止まらない。例えば、現在のスマートフォンアプリは、端末内のアドレス帳、位置情報、通信履歴などの基本的な個人情報にアクセス可能である。ユーザはこれらを許容することで利便性の高いサービスを受けることが可能になる反面、その漏洩リスクが高まることになる。アプリを通してアクセスするサービス提供事業のセキュリティ管理が重要になる。

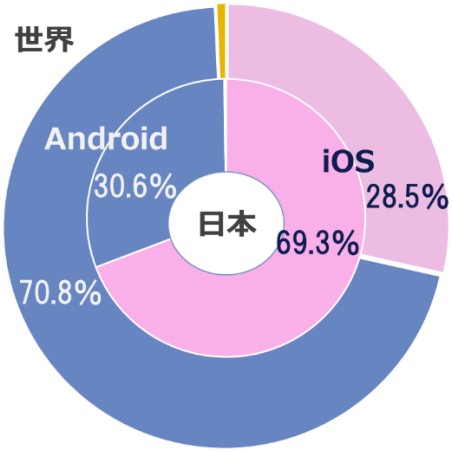

図 1.4 スマートフォン OS のシェア

⑨IoT 機器の普及

インターネットの普及に合わせて、IoT(Internet of Thing)機器が急速に拡大した。ホームルータ、AV 機器、その他多くの家電製品がインターネットに接続される。また、監視カメラ、自動車、或いは複合機などのオフィス機器、電子カルテシステムや MRI といった医療機器、センサーなどの産業用機器などあらゆるところに導入されてきている。これらの製品は、セキュリティ対策の甘さ（アカウント/パスワード設定、脆弱性対策）から格好のサイバー攻撃対象になってきた。設置台数も多く、一度侵入方法が確立すれば大規模な DDoS 攻撃基盤が構築可能である。また、一般の端末と異なり、侵入されていても気づきにくいといった特性もあり、サイバー攻撃によって乗っ取られてボットネット化したり、カメラ映像を盗まれたり

[36] https://ja.wikipedia.org/wiki/Jailbreak

といった被害が実際に多数発生している。また、現在でもサイバー攻撃の格好の対象であり増加傾向にある[37]。

⑩仮想通貨

仮想通貨（暗号通貨）は元々2008 年 10 月サトシ・ナカモトという人物がネット上で「ブロックチェーン技術を使った中央管理者のいない決済システム」という論文を公開したのがきっかでビットコインと言う名称で開発されたインターネット上の決済システムである。 今までの決済システムは決済を管理する管理者（銀行など）が存在し決済（価値の移転）を記録すること（台帳）で、取引を成立させていた。この取引台帳を参加者全員で改竄されることなく、共有する仕組みがブロックチェーンである。取引台帳は参加者の間で P2P で共有される。改竄されないことを保証するためのナンスと呼ばれる特殊なハッシュ値を生成する必要があるが、これはマイナーと呼ばれる参加者が生成する。生成にはかなりの計算能力が必要でありその生成のためのインセンティブとしてマイナーには一定のビットコインが与えられる。このシステムへの参加者はワレットと呼ばれる公開鍵と秘密鍵のペアを生成、保持するだけである。参加者がビットコインを取得するには交換所と呼ばれる場所で実際の通貨との交換を行うことができる。この仕組みは、参加者のみでの決済処理が可能であり、極めて匿名性の高い取引が可能となることである。

サイバー攻撃の観点では、ビットコインの窃取の観点とビットコインを利用したサイバー犯罪の決済への利用の 2 点が挙げられる。前者で言えば、有名な事案として 2019 年の国連北朝鮮専門家パネル報告書[38]で公開された北朝鮮による仮想通貨取引所への攻撃がある。これは現在も継続的に行われている模様である。また、後者の例では、ランサムウェアの身代金支払いに利用されることである。これもビットコインの匿名性が高いことを利用したものである。

⑪ダーク Web

ダーク Web とはインターネット上に作られた、匿名性の高い Web サイトのネットワークである。これにアクセスするには通常のブラウザとは異なるブラウザが必要であり、Web サイト自体は通常の Google や Bing などの検索エンジンでは検索できない。元々米国海軍研究所によって開発されたインターネット上で匿名性、秘匿性を保証するための「オニオン・ルーティング」という技術に基づいている。極めて匿名性の高い通信を実現できるため、中国やイランなど Web の閲覧に制限がある国々で、その制限をすり抜ける、或いは独裁国家の活動家たちが当局の監視をくぐり抜けてやりとりをする、といったことに利用できることもあり、現在は Tor（The Onion Router）という名称で非営利団体などが運営している。

一方で、児童ポルノや麻薬など違法性が高いさまざまなコンテンツや物品が取引されるコミュニティも形成された。サイバー攻撃の観点では、Web サイトへのログイン情報、個人情報、クレジットカード等のリストに始まり、不正にソフトウェアや OS を利用する目的でのアクティベーションコード、マルウェアとその作成のためのツールキット、脆弱性情報、さらにはサイバー攻撃に利用可能な C&C サーバやボットネットなどが取引できるようになっている。これらの違法取引では、取引の決済が重要になるが匿名性の高い仮想通貨ビットコインの登場で活況を呈する状態になり、現在でも活発に利用されている。

---

[37] 例えば次を参照 Check Point 2023.4.12 https://blog.checkpoint.com/security/check-point-registers-patent-for-uniquely-profiling-and-autonomously-enforcing-security-for-iot-devices/

[38] https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

現在、インターネット上では様々なアプリケーション、サービスが利用されるようになってきている。それぞれが、ある意味でコンテンツレベルの情報空間を形成していると言える。

1.4 インターネットアーキテクチャのコモディティ化とマイクロソフト Windows

インターネットアーキテクチャの基本はコンピュータ間通信アーキテクチャでもある。元々は UNIX 系サーバの分散処理技術であるオペレーティングシステムの基本機能として発展してきた。このアーキテクチャに基づいて様々な分散コンピュータシステムが開発されてきた。その代表的なものの 1 つとして開発されたものがマイクロソフト社の Windows95 と言える。マイクロソフトは元々DOS 系のオペレーティングシステム MS-DOS を 1980 年代から販売していたが、1995 年に販売開始した Windows95 はそれまでの UNIX 系ワークステーションで標準装備されていたインターネット接続機能を取り込んだ新しい OS で、ワークステーション並みの機能を低価格のパソコンで実現するというコンセプトが一般ユーザに受け入れられ商用インターネットサービス[39]の普及と並行して利用が拡大した。また、マイクロソフトは Windows95 と前後してサーバ用の OS，Windows-NT も開発、販売していたが、これに企業内ネットワークの分散環境を管理する上で欠かせない技術であるディレクトリ機能を”Active Directory”として標準装備した。Active Directory が利用した通信プロトコルはインターネットと同じ TCP/IP であり、これも含めて多くのインターネットアーキテクチャを取り込んでいる。

マイクロソフトは MS ワード、Excel、パワーポイントといった Windows 上の汎用アプリケーションの開発、普及にも力を入れることで、Windows と Windows サーバはインターネットを利用した企業内ネットワークの構築に欠かせない製品として世界市場をほぼ独占する製品となった（図.1.4, 1.5）。

以上のように、マイクロソフト製品は現代のインターネットの普及に大きく貢献したと言えるが、一方でサイバーセキュリティ上の脆弱性も数多く発生させている。OS や DB といった基盤ソフトウェアや Internet Explorer といったブラウザ、さらにはアプリケーションソフトの脆弱性などはサイバー攻撃の格好の対象にされてきた。また、アプリケーションには文書、データ処理効率化のためにマクロコマンドが用意されているが、これがバックドアとして悪用され現在でもフィッシングメールに頻繁に利用されている。マクロコマンドの悪用はマイクロソフトのアプリケーションの知識があれば比較的簡単に行えることから、サイバー攻撃のハードルを下げたとも言える。

マイクロソフト製品の脆弱性は、その製品が汎用的であることからインパクトが大きい。特に、未知の脆弱性がサイバー攻撃に使われた場合（いわゆるゼロデイ攻撃）、これを発見して修復するまでには時間がかかることから重大な侵害に繋がることになる[40]。その他、Windows ネットワークや Active

---

[39] 元々インターネット教育研究機関向けのネットワークとして提供され、商用利用は制限されていたが 1995 年にこの制限はが完全に撤廃された。
https://ja.wikipedia.org/wiki/%E3%82%A4%E3%83%B3%E3%82%BF%E3%83%BC%E3%83%8D%E3%83%83%E3%83%88%E3%81%AE%E6%AD%B4%E5%8F%B2

[40] 例えば、2021 年 3 月に報告された侵害はマイクロソフト Exchange の未知の脆弱性を突いたものであり、中国由来の HAFNIUM による攻撃であることが報告されている。
https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

Directory への攻撃は数多く観測されており、これらの攻撃手段の多くは、ダーク Web を経由して攻撃者側で共有されている。

このようにマイクロソフト製品に対する攻撃は、ある意味汎用化が招く弊害とも言える。マイクロソフトはセキュリティ対策に力を入れており、様々な角度からの対策を行っている。特に製品の脆弱性に対しては迅速な更新ファイルの提供を実施しているが、現在でも APT 攻撃のような高度な攻撃はマイクロソフト製品をターゲットにしたものが大部分であると言える。

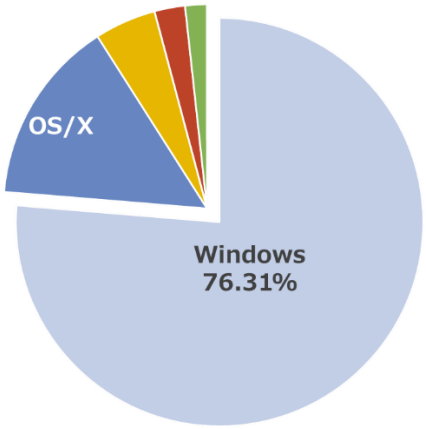

図 1.5 Disktop OS の世界シェア[41] 2022 年

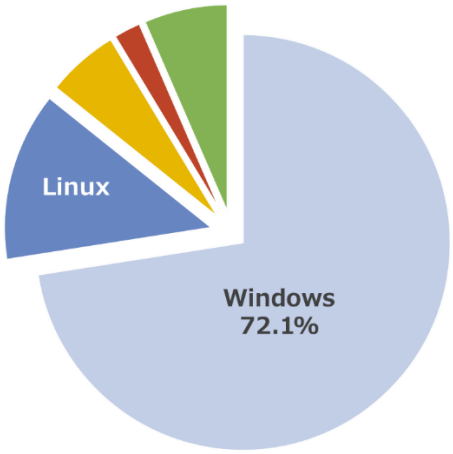

図 1.6 server OS の世界シェア[42]2022 年

1.5 サイバーセキュリティの概念と ISO TS 27100 について

サイバーセキュリティという用語は 2000 年代に入って使われるようになってきた。しかし、そもそもサイバー空間とは何を意味するかを含め、その概念は変化してきている。例えば、米国標準技術研究所(NIST)での 2010 年頃の定義では、サイバー空間とは「グローバルな領域で、特定の情報を利用するために独立したネットワークで構成される情報システム基盤。インターネット、電気通信網、コンピュータシステム、組込型処理・制御システムなどを含む。」とされ、一言で言えば"分散コンピュータシステム"といった技術的な定義がなされていた。サイバー攻撃とは「サイバー空間を経由して意図的にその機密性、完全性、可用性を棄損するもの」であり、サイバーセキュリティとは「サイバー攻撃からサイバー空間を保護すること」といった技術的な概念でまとめられていた。

しかしながら、サイバーセキュリティとしてのサイバー空間を考える場合は、単にシステムのみならずこれを利用する側の人、組織、及びシステムが存在する物理的環境（建物施設、地理的環境等）を含めて考える必要がある。このため、タリンマニュアル 2.0 ではサイバー空間を「物理層、論理層、社会層からなる。物理層はハードウェアなどの物理的構成要素からなる。論理層は各機器の間を往来するアプリケーシ

[41] https://gs.statcounter.com/os-market-share/desktop/worldwide/

[42] Statista https://www.statista.com/statistics/915085/global-server-share-by-os/

ョンソフトウェア、データ及びプロトコルを指す。社会層はサイバー行動に従事する個人、集団からなる。」と定義し、これに基づく議論を行っている。

2020 年に標準化された ISO TS 27100 ” Cybersecurity - Overview and concepts”はこの考え方をより精緻化したものと言える。図 1.6 に ISO TS 27100 で導入されたサイバー空間の階層構造を示す。３つの階層で構成されそれぞれの階層はさらに 2 つずつのサブ階層で構成されている。

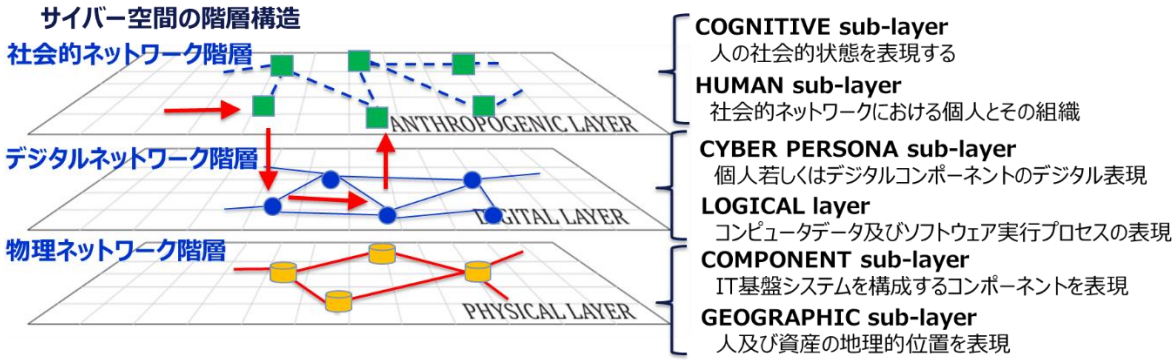

図 1.6 ISO TS 27100 2020 版におけるサイバー空間の階層構造

各階層の要素は、階層間で相互に連結されてサイバー空間としての機能、サービスを提供していると捉えることができる。従って、各階層に固有の脆弱性が発生し得る(表 1.1)が、サイバー空間としての機能、サービスを期待通りに利用するには、一連の連結構造のいずれか或いは複合的に発生する脆弱性に対応する必要がある。

社会的ネットワーク階層	デジタルネットワーク階層	物理ネットワーク階層
違法情報の流布（薬物、ポルノ、著著作権違反等）Dark Net、フェイクニュース、影響工作	デジタルIDのなりすまし、サプライチェーン攻撃、マルウェアの混入、不正アクセス（バックドア、機密情報窃取、構成情報改竄/破壊）	機器障害、電力障害、電磁的盗聴(TEMPEST)・妨害、模造品混入、物理的盗聴（スニーファー、キーロガー等）
個人情報搾取、個人レベルのなりすまし（ソーシャルエンジニアリング、アカウントハッキング等）	BGP改竄、DNS欺瞞、サーバの乗っ取り（C&Cサーバ）、DoS攻撃、ソフトウェアのバグ/脆弱性	

表 1.1 階層毎の脅威(ISO TS 27100 に一部加筆)

さらにこの標準では、サイバーセキュリティに関して以下のような特徴をあげている。

・サイバー空間（攻撃）の脅威

i) グローバルなサイバースペースは、誰もが自由に出入り可能であり、利用主体は匿名化が可能。このため、脅威アクターはどこからでも攻撃可能。

ii) サイバースペースにおける脅威は非対称性を有し、攻撃源の特定、抑止、防御が困難であり、攻撃による損失が攻撃に必要なコストに比較し極端に大きくなる可能性（非対称性）がある。

・サイバーセキュリティの対象

サイバース空間における脅威により影響を受ける対象は、

a) 社会、組織、国家の安定と継続

b) 人および組織の財産（情報を含む）

c) 人命と健康

サイバー空間を構成するシステムとそこで扱われる情報の棄損だけでなく、これに依存する実空間の活動の棄損まで考慮する必要がある。

・サイバーセキュリティの特徴

i) 他のアクターに悪影響を与えないように自らの脆弱性を管理する必要があり、他者と連携してサイバーリスクを低減する必要がある。

ii) サイバーセキュリティは、サイバースペースでのサイバーセキュリティインシデントによって引き起こされる実空間での社会的・人的損失を低減する必要がある。

iii) 情報セキュリティインシデントの即時検知と適切な対応は、サイバーセキュリティの重要な要素。

1.6 情報セキュリティマネジメントとサイバーセキュリティの関係

ここで、2000 年代に入って以降広く普及してきた情報セキュリティマネジメント（ISMS）[43]とサイバーセキュリティの関係について整理しておく。両者は補完関係にあるが、セキュリティマネジメントの観点では異なる観点での対応が必要になると言える。両者の関係を図 1.7 に示す。

図 1.7 の右側に示すように、情報セキュリティマネジメントは基本的には個々の個人、組織が情報及び情報システムに対する機密性、完全性、可用性を維持するために守るべき規範を与えたものである。この規範の 1 つにサイバーセキュリティへの対応が含まれている。これに対して、サイバーセキュリティはこれを構成する個人/組織、システム/プロセス、流通する情報の機密性、完全性、可用性を維持するために守るべき規範を与えることが目的となる。このことは、抽象的ではあるが、「サイバー空間を共有する、エンティティ、ステークホルダがセキュリティを維持するための責任をどう共有するか」という問題の解決を目指しているという事が出来る。

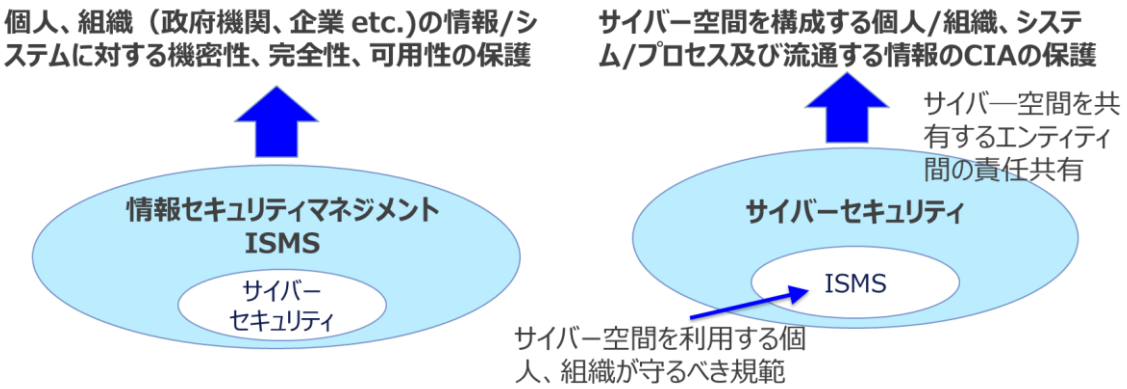

図 1.7 情報セキュリティマネジメントとサイバーセキュリティ

[43] ISMS Information Security Management System, ISO/IEC 27001, 27002 で標準化

第 2 章　サイバー攻撃の現状とそのメカニズム

2.1 サイバー攻撃の現状

インターネットの普及・拡大に応じて、サイバー攻撃による被害は拡大の一途を辿っている。図 2.1 ではグローバルに見たサイバー攻撃の被害の状況を示す。サイバー攻撃による被害はここ数年急激に拡大している（左図）[44]。また、国家由来による深刻なサイバー攻撃も急激に増加していることが推定されている（右図）[45]。

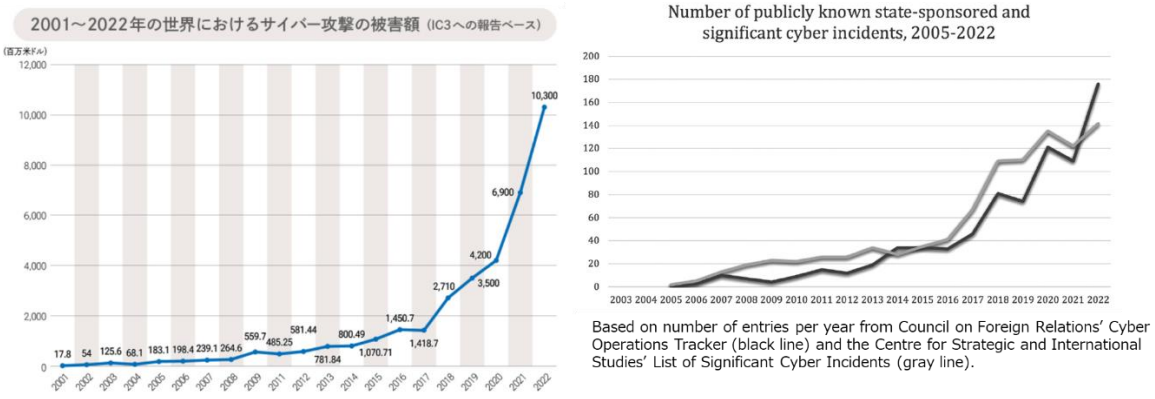

図 2.1　サイバー攻撃の現状

特に近年では、新たな攻撃手法としてサプライチェーンに対する攻撃が頻発するようになった。欧州ネットワーク・情報セキュリティ機関 ENISA(European Network and Information Security Agency[46])が 2021 年に公開した報告書[47]によると、次のようなことが判明している。

・2020.1 から 2021.7 までの期間で発生した 24 のサプライチェーン攻撃を攻撃手法、ターゲット等の分類に基づいて分析

・50%の攻撃は既知の APT グループから実行されていた。一方 42%は現在まで帰属が不明。
62%の攻撃は、サプライアに対する信頼を利用。また、62%の攻撃にマルウェアが使用されていた。

・攻撃対象の資産の内 66%はサプライアのコードを狙ったものであり、攻撃対象のユーザ（アクアイア）に対する侵害を狙ったものであった。

・58%のサプライチェーン攻撃はデータ（個人及び企業秘密などの顧客データ）侵害、16%は個人に対する直接のアクセスを狙ったものであった。

---

[44] 左図 https://www.jica.go.jp/information/topics/2023/20230517_01.html

[45] 右図 The UN Cyber Norms: Bart Hogeveen
https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/08_Hogeveen.pdf?ver=BYnHYWAYLrW_PpP4lljm5A%3D%3D

[46] https://www.enisa.europa.eu/

[47] ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS July 2021.7
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

・すべての攻撃がサプライチェーン攻撃と呼べるとは限られなかったが、その性質上、多くの攻撃は将来的に新たなサプライチェーン攻撃のベクトルとなる可能性があった。

・組織は、サプライチェーンへの攻撃を念頭に置いてサイバーセキュリティの手法を更新し、すべてのサプライヤーをその保護とセキュリティの検証に組み込む必要がある。

2.2 一般的なサイバー攻撃の手法

サイバー攻撃の侵入経路

現在のサイバー攻撃のほとんどは、攻撃対象組織に対して図 2.2 に示す侵入経路が使われている。初期アクセスに成功した後、様々なマルウェアが送り込まれたり、遠隔操作が実施される。

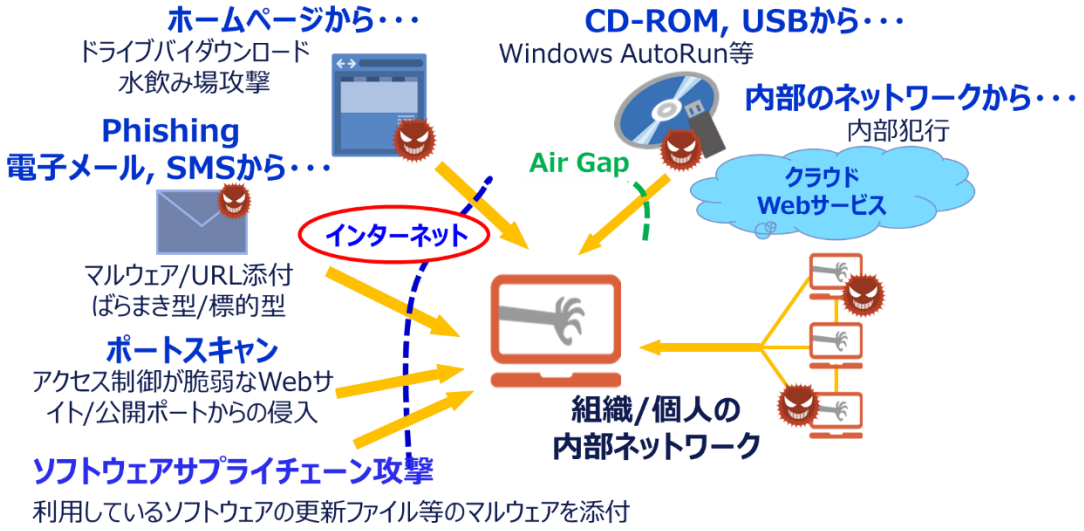

図 2.2 サイバー攻撃の代表的な侵入経路

このような侵入経路から見た場合の攻撃方法、攻撃の目的と特徴を簡単にまとめたのが表 2.1 である。水色のハッチを掛けた部分がインターネット経由で直接行われるものである。

表 2.1 攻撃方法の類型と特徴

類型	攻撃手法	目的/特徴
DDoS攻撃	インターネットへのアクセス、公開サーバ等を利用できないようにするためにトラヒック、ワークロード、DNS等を過負荷にする攻撃	インターネットを利用している組織、企業活動のサービス提供の妨害。特定の個人のインターネット利用妨害。
ポートスキャン	侵入に対して脆弱性のあるサーバを発見して侵入。基本的にはIPアドレスとTCPポートを総当たりでスキャン	インターネットに接続されている組織、企業、個人のネットワークへの遠隔からの侵入。機密情報の窃取、改竄等
フィッシング(メール/SMS等)	マルウェア若しくは悪性のURLが添付されたメール、SMS等の配信。バラマキ型、標的型等がある。	インターネットに接続されている組織、企業、個人へのマルウェアの送り込み。金銭/機密情報の窃取、改竄等
悪性の公開Webサーバ	マルウェアがダウンロードされる公開Webサーバ。水飲み場攻撃（標的とする被害者が集まりやすいサイト）等により実行。	同上
ソフトウェアサプライチェーン攻撃	ユーザが利用しているソフトウェア若しくはその更新ファイルにマルウェアを仕込み侵入する。	機密情報窃取等の諜報活動、ランサムウェアの大規模な配布等。侵入の難しい組織に対する高度な攻撃。
Air Gapの侵害	マルウェアが混入されたUSB，CD-ROM等の記憶媒体を経由した侵入	OT系システム等Air Gapの存在する機密性の高いネットワークへの侵入。
内部犯行	悪意を持った内部ユーザによるアカウント/クレデンシャルの侵害	金銭目的から政治目的まで様々な理由が存在。人に依存した攻撃であり技術的対処が難しい。

ソーシャルエンジニアリング

ソーシャルエンジニアリングとは一般的には被害者の心理的な隙や行動の失敗に付け込んで、機密情報を窃取したり目的の行動に誘導したりする手法を指し様々なものが存在する。

現在において、もっとも主流となっているサイバー攻撃の侵入経路はフィッシングと言われている[48]。ターゲットに対してバックドアやマルウェア付きのファイルの添付或いはこれがダウンロードされる Web サイトの URL を送り込むものである。ここでマルウェア付きファイルを開かせる、URL をクリックさせるといった、被害者に送り込んだメールを信用させるのに良く使われる手法がソーシャルエンジニアリングである。送り込んだメールの送信元の偽装、あるいは被害者が信頼していると思われる送信元のアカウントのハッキングなどがまず行われる。メール内容に関しては、以下のような心理的な脆弱性を突いたものが利用されると言われている[49]。

① 権威：サイバー犯罪者が、有名企業や組織の上司などの権威を持つ人間を装うと、ターゲットはそれを信じてしまう傾向にある。

② 脅迫：サイバー犯罪者は、ある行動をとらないと悪い結果になることを知らせたり、暗示をかけたりすることで、ターゲットを惑わせる。

③ 社会的証明：人間の「他人がやっているのを見ると自分もやりたくなる」という特性を悪用して、ソーシャルエンジニアリング攻撃を仕掛けることもある。

④ 希少性：「手に入りにくいものほど価値があると感じ、手に入れたくなる」という特性を利用することで、人を意のままに操ることができる。

⑤ 好意：私たちは、好意を持っている人から頼まれると、簡単に承諾してしまう傾向にある。

⑥ 緊急性：希少性に関連して、サイバー犯罪者はソーシャルエンジニアリングのために、時間に基づく心理的原理として緊急性を利用することもある。

2.3 サイバー攻撃の特徴 C&C サーバとボットネット

章末に示す事例分析においても頻繁に用いられているのが C&C サーバとボットネットである。その特徴を一言で言えば、グローバルな環境下で自動化されたサイバー攻撃を行うインフラである。通常攻撃側は侵入先への感染活動（フィッシングメール等）、マルウェアのダウンロード、DDoS 攻撃、遠隔操作、不正送金など様々な活動を行う。これらを極力人手をかけずに自動的に行うシステムを一般的に C&C サーバとボットネットと呼んでいる。C&C サーバは攻撃側の支配下にあるサーバ、ボットネットはインターネットに接続されたサーバが乗っ取られ、そのサーバの所有者には意識されずにサイバー攻撃の拠点を与えるものである。事例分析 4 Emotet の例でも理解できると思うが、C&C サーバとボットネットは複数の攻撃グループで共有されたり、一種のサービスとしてブラックマーケットで販売されたりしている。

---

[48] 海外の状況 https://www.zscaler.jp/resources/industry-reports/2022-threatlabz-phishing-report.pdf
国内の状況 https://www.antiphishing.jp/report/phishing_report_2022.pdf

[49] ロバート・チャルディーニ https://nordvpn.com/ja/blog/social-engineering-attacks/

また、C&C サーバもボットネットもインターネットに接続されたサーバであれば、どこにでも存在することができる。特にボットネットは通常セキュリティ対策が不十分なサーバが乗っ取られることから、開発途上国等が狙われやすい。従って、C&C サーバやボットネットをインターネットから排除しようとしても（一般的には Take Down と呼んでいる）特定の国の執行機関が単独で行うのは困難である。このことがサイバー攻撃の活発化を招いているとも言える。

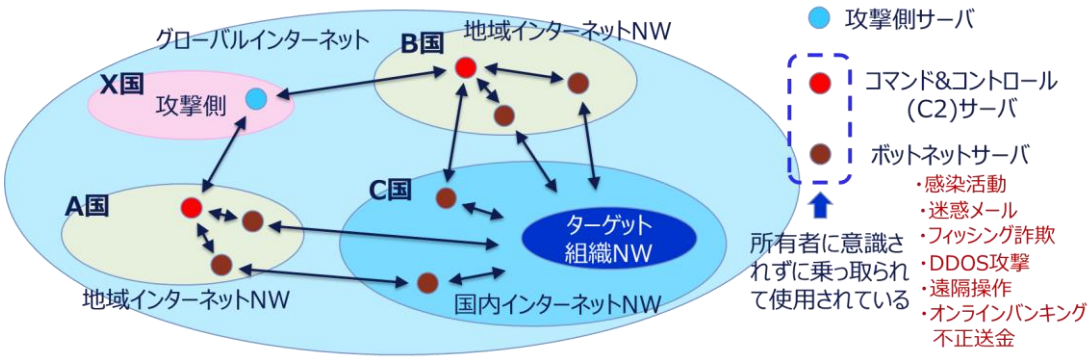

図 2.3　C&C サーバとボットネットの構成

2.4 サイバー攻撃の類型　攻撃者と意図、影響の多様性

現代のサイバー攻撃は様々な目的で、様々な主体（アクター）により様々な技術と攻撃プロセスにより行われている。攻撃の目的、目標によりその影響も様々になる。図 2.4 には以下のようなサイバー攻撃の類型に対応した発生頻度、実行（難易度）と実行に必要なコスト、影響度（強度）の関係を示している。この図はあくまで定性的な関係を示しているが、サイバー攻撃のタイプによるリスク判断、対象方法の指標にもなる。

① 軽度な犯罪レベル（Script Kiddy/いたずら、個別犯罪）：これには違法コンテンツの流通、個人の SNS 等のアカウントハッキングによるなりすまし、誹謗中傷、或いはゲーマー間での妨害行為などが発生している。インターネットへの接続環境と簡単な知識があれば実行可能であり、必要となる参入コスト/技術能力は低いと言える。ただし、違法コンテンツを収容しているサーバ或いはネットカジノなど国境を越えて実行されるものは効果的な取り締まりが難しいものもある。

② 組織犯罪：組織犯罪は、違法コンテンツや薬物の売買、金融機関関連のクレデンシャル窃取、仮想通貨窃取、ランサムウェアによる身代金窃取といった高額の金銭窃取を目的としたものまで多岐にわたる。複数のメンバのよる比較的軽度なものから、大規模なものまで多岐に渡る。特に、大規模なものは、犯罪者によるグローバルなネットワークが構成され、高度なマルウェアの開発と共有、脆弱性情報の共有、取得したクレデンシャルの売買、或いはボットネット等のサービス提供などが組織的に分業されて行われている。金融資産の窃取は一部国家（北朝鮮）などもこれを実行していると言われる。

③ テロ組織：非合法なテロ実行のための通信、プロパガンダ、要員のリクルート、或いは資金獲得のための活動が行われている。組織犯罪のネットワークも利用される。具体的には、米国の 9.11 テロや欧州のテロ、或いはイスラム国の活動などがある。一般的に、非合法な実力行使と組み合わせて行われる。

④ 国家組織（平時）：明確な紛争状況ではないが、国家による敵対国に対する諜報活動、干渉・影響工作或いは経済安全保障として認識される重要企業機密の窃取、紛争時に想定される重要インフラの侵害/破壊活動の準備などが行われている。外交、経済等での干渉・優位性確保が主な目的と考えられる。高い技術力と実行コスト、長期間の準備が必要と考えられる。

⑤ 国家組織（紛争時）：国家間の紛争時に軍事力行使の一環として実行されるサイバー攻撃である。ロシアによるウクライナへの武力行使にもその一環としてのサイバー攻撃が観測されている。単に敵対国の軍事指揮命令システムに対する侵入：諜報活動、妨害・破壊だけでなく電子戦等との連携も必要になってくる。また、重要インフラに対するサイバー攻撃、プロパガンダ、情報操作など様々な攻撃が想定される。高度な技術力とともに物理的軍事力との連携が重要になる。

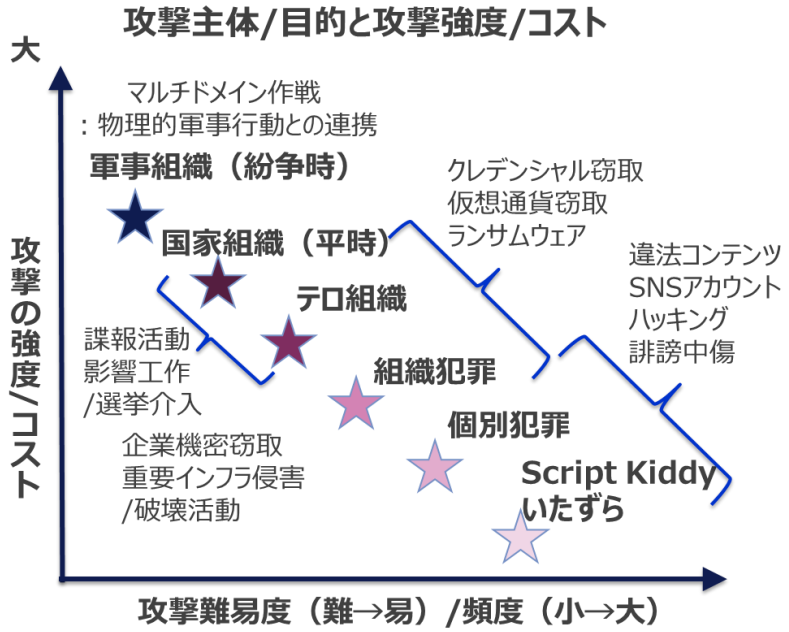

図 2.4 サイバー攻撃の類型

Active Cyber Defense の議論の対象の主流は高度で組織的なサイバー攻撃に対するものと言える。これは、今までに開発・導入されてきている防御中心（境界防御、縦深防御、Zero Trust 等）の対応だけでは費用対効果の面でも限界にきていることが背景にあると言える。その観点では、サイバー攻撃の類型としては高度な組織犯罪から国家レベルのものが主な対象になっていると言える。

2.5 APT 攻撃の Cyber Kill Chain[50]

[50] 2010 年代後半にロッキード・マーチンが提唱を始めた概念　APT 攻撃を特徴付けることが可能になると言える。
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

現在、攻撃強度の高いサイバー攻撃は一般に APT 攻撃と言われるものである。この攻撃の特徴は高度な Kill Chain が用いられていることにある。Kill Chain という用語自体は、軍事用語として攻撃の手順等を表現したものである。ロッキード・マーチンが提唱した Cyber Kill Chain はこれを模したものと言えるが、考え方としては様々な APT 攻撃に共通した攻撃手順が観測されつと言う分析に基づいている。現在までに様々な APT 攻撃が観測されているが、これらは図 2.5 のような共通の Kill Chain を有している。この章末に示した事例分析でもそれぞれの事案ごとに特徴的な Kill Chain が利用されている。各ステップで利用される個別技術は攻撃グループに固有ものであると言われており、攻撃グループを特徴付けている。MITER ATT&CK[51]は各ステップで利用される手法をデータベース化し攻撃元の Kill Chain 対応させることができるデータベースを整備したものであり、サイバー攻撃の検出や攻撃元の帰属の判断或いは防御手段の検討に利用されている。これが有効な理由としては、APT 攻撃のような多段階の Kill Chain を複数回に渡って利用するために、攻撃毎に個別の新しい技術を利用すると攻撃コストが一気に上昇するため、攻撃者は利用する技術や手法を繰り返し用いることでコストの上昇を抑えるとともに、技術や手法の改良を期待することによると考えられる。

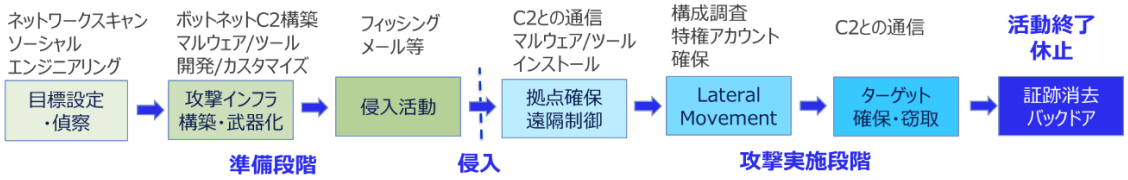

図 2.5 Cyber Kill Chain

事例分析でもわかるように実際の APT 攻撃ではネットワークでつながった複数の組織に対して段階的侵入が行われる。これを表現したものが図 2.6 である。よく行われるのは、グローバル企業において他国におかれた支店や系列企業の脆弱性が狙われて侵入され、これが企業内ネットワークを経由して本国のシステムにまで侵入されるケースである。また、事例分析 3 のようなソフトウェアアプライチェーン攻撃もこの多段階に渡る APT 攻撃が併用されていると言って良い。

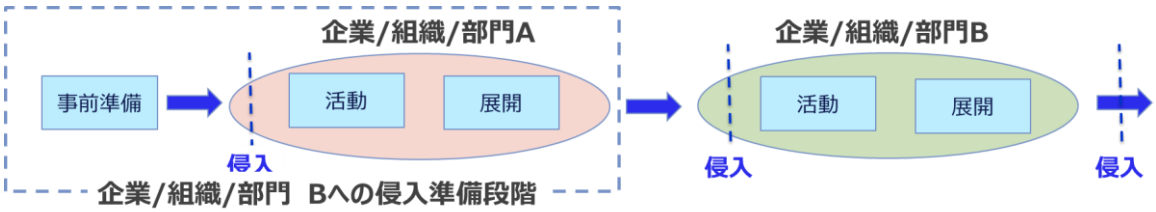

図 2.6 多段階に渡る APT 攻撃

APT 攻撃に対する防御はこの Kill Chain ベースで検討されている。先に述べた MITER ATT&CK では、Kill Chain の各要素で利用される手法や技術に対する対策がまとめられている。従って、Active Cyber Defense を検討する上でもこの Kill Chain に従った分析が有効と考えられる。

[51] https://attack.mitre.org/

事例分析 1　2010 年　Operation Aurora[52]

2010 年 1 月に Google が特定の G-mail アカウントに盗聴が試みられていたことを公表した。この活動は 2008 年頃まで遡れると分析され、監視されていたアカウントは盗聴対象は中国の人権活動家とその関係者であった。Google の分析によると、攻撃元は中国の人民解放軍に繋がる組織からのものであった。 その後の分析で、攻撃は米国の 30 社以上の組織に及び、Google に対しては単に G-mail アカウントの盗聴だけでなく、社内のソフトウェア開発用のソースコードレポジトリへの侵入の痕跡も発見されるという深刻なものであった。また、報道によると米国政府によって外国情報監視法（FISA）第 702 条[53]で指定されたアカウントへのアクセスも行われていた模様であった[54]。

これに対して米国は当時のクリントン国務長官が中国に対して非難声明を行うとともに、最終的には Google が中国本土より撤退するという事態になった。また、この事案を受けて Google は現在の Zero Trust アーキテクチャに繋がる独自のアーキテクチャである Beyond Corp の開発に着手したと言われている。

分析された攻撃の状況を図 2. に示す。ここでは以下のような攻撃が実施されたことが判明している。
①Google の社員に向けての Phishing メールを送信。
②これに添付された台湾に存在した攻撃側の C&C サーバの URL に Internet Explorer でアクセス。
③Internet Explorer の未知の脆弱性を突く JavaScript コードが C&C サーバから送りこまれる。
④さらに様々なツールが入ったマルウェアの仕込まれた画像データファイルが被害者のパソコンに送り込まれる。攻撃側は、これらのツールを利用して被害者のネットワークに侵入し、偵察、アカウントのハッキング等を実施し、別の C&C サーバへのアクセスを行う。これにより標的とした G-mail アカウントの監視情報を報告するルートを確立。
⑤さらに被害者のネットワーク内部を偵察し、ソフトウェア管理システムへのアクセス権を取得。このシステムの脆弱性を突いて新たなマルウェアを埋め込むことを試みた。

Google やその他のセキュリティ企業の分析から、以下のようなことが判明し攻撃元の帰属が中国由来のものであることが推定された。
①Internet Explorer の未知の脆弱性を突くマルウェアが中国のブラックマーケットで流通していた。
②通信を行った台湾の C&C サーバは踏み台であり中国の上海交通大学、山東省の IT 関連の職業訓練校のサーバに繋がっていた。これらのサーバは、人民解放軍及び Baidu と密接な関係があることが判明している。

---

[52] 2010.3 Protecting Your Critical Asset, McAfee その他参考資料を元に作成
https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

[53] https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf

[54] https://www.cio.com/article/289150/government-aurora-cyber-attackers-were-really-running-counter-intelligence.html

この帰属調査の段階で、Google が台湾にある踏み台サーバに侵入し、詳細な情報を取得したとの報告も出されている[55]。ただし、Google はこれが不正侵入にあたるとして否定している。

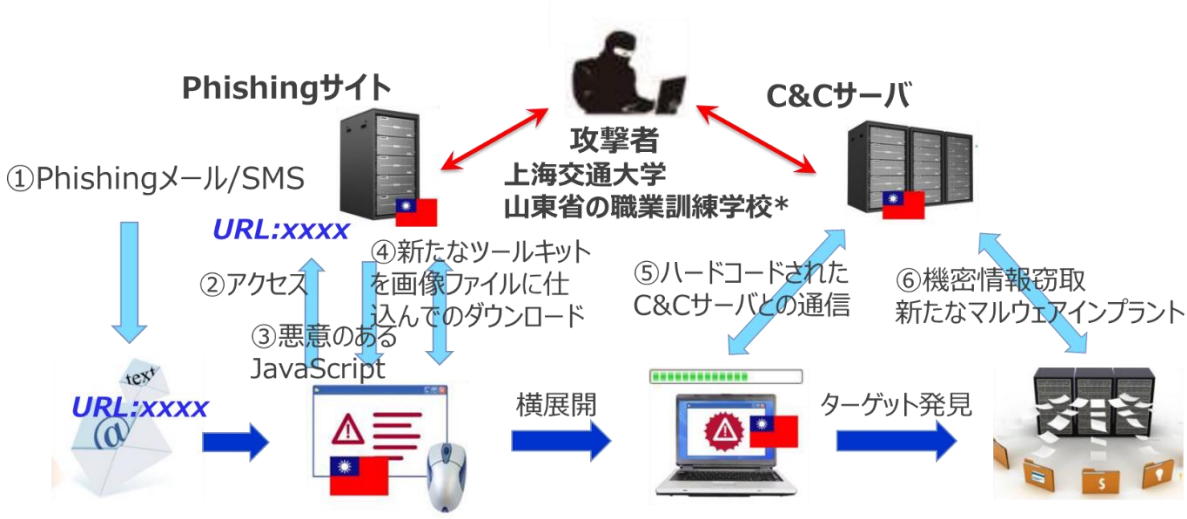

図 2.7　Operation Aurora の攻撃ステップ

事例分析 2　2013 年　Mandiant 社[56]による APT1 レポート[57]の公開

2013 年 2 月に米国のセキュリティ企業 Mandiant 社により中国由来のサイバー攻撃が遅くとも 2006 年以降継続的に行われていること証拠づけるレポートを公開した。Mandiant はこのグループを APT1 と命名している。詳細はレポートを見て欲しいが、公開内容は以下の通り。

①APT1 を中国人民解放軍（PLA）総参謀部（GSD）の第 2 局 61398 部隊（上海）に結び付ける根拠。

②2006 年以来、複数の業界にわたる 141 人の被害者に対して行われた APT1 経済スパイ活動のターゲットとタイムライン

③APT1 の手口（ツール、戦術、手順）[58]

④40 を超える APT1 マルウェア ファミリのタイムラインと詳細

⑤APT1 の広範な攻撃インフラストラクチャのタイムラインと詳細

---

[55] 例えば、次を参照。2013 Hackback, Jan E. Messerschmidt, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1004&context=national_security_law

[56] Mandiant は米空軍の Kevin Mandia 氏により設立された会社。その後 FireEye 社の傘下にいるが、2022 年に Google に買収され Google cloud 傘下に入っている。

[57] https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units

[58] 典型的な APT 攻撃の Kill Chain その具体的な手順は Youtube で公開されている。https://www.youtube.com/watch?v=mYaTCvA2VLQ

このレポートに関しては帰属の問題が議論となった。公開された情報は極めて詳細ではあるものの、あくまで状況証拠であり、最終的な帰属を人民解放軍 61398 部隊とするまでには至らないと言うのが論点であった。

このレポート公開後、米国司法省は米国の原子力、金属、太陽電池製品産業への侵入、機密情報の窃取の容疑として人民解放軍 61398 部隊に所属するハッカー5 人の起訴に踏み切った[59]。司法省による海外の国家主体に帰属するサイバー攻撃に対しての初めての訴追であった。

この間の経緯は、2018 年に出版されたデービット・サンガー氏の「The Perfect Wepon(邦訳　サイバー完全兵器 2019 年[60])」の中で詳しく紹介されており、Mandiant 社は 61398 部隊の帰属を明らかにするために、彼らが利用していた Facebook のアカウント経由で一種のビーコンマルウェアを送り込み、61398 部隊の要員が実際に侵入操作を行っている場面のスクリーンショットを取得したことが明らかにされている。この記述に関して Mandiant 社は正確ではないとして否定している[61]ものの、民間セキュリティ企業による一種のハックバックの事例を示唆している。

事例分析 3　2020 年 12 月　SolarWinds 社

2020 年 12 月 13 日 米国セキュリティ会社 FireEye が SolarWinds 社の IT 管理システム Orion のソフトウェアパッチ経由でマルウェアが送り込まれるハッキングを公表。典型的なソフトウェアサプライチェーン攻撃であった。同時に侵害が広範囲かつ重要な組織に対するサイバー攻撃であるとして、米国政府が国家安全保障会議を招集し官民あげての緊急対策[62]を開始した。

同年 12 月 18 日にマイクロソフト社により被害情報の一次発表が行われ、SolarWinds 社 Orion の顧客約 18000 社（最終的には 16000 社）にマルウェアが配信され、200 社（最終的には 100 社程度）近くにセキュリティ侵害（下図）が行われたことが公表された。

米国政府は調査結果に基づいて攻撃元はロシアの対外情報庁(SVR)であるとしてロシアを非難。さらにこの事案を受けて、2021 年 5 月 15 日、米国大統領令 E.O.14028[63]が発出され、米国政府機関を中心にサイバーセキュリティ対策の全面的な見直しと強化が指示された。官民での一層の情報共有体制の確立、政府機関のシステムに対する Zero Trust の導入、ソフトウェアサプライチェーンのセキュリティ対策等が指示されており、現在もその対策は進行中である。

この攻撃は以下でも見るように、ソフトウェアサプライチェーンを利用した極めて高度な攻撃であると同時に攻撃対象が単に政府機関に止まらず米国の主要 IT 企業が対象となっており、これらが侵害されると IT 製品全体のサプライチェーンが破壊されるという深刻な影響が考えられる。

---

[59] https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[60] https://www.amazon.co.jp/dp/4022516097

[61] https://cyberscoop.com/fireeye-hack-back-david-sanger-book/

[62] https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-Solarwindss-orion-code-compromise

[63] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

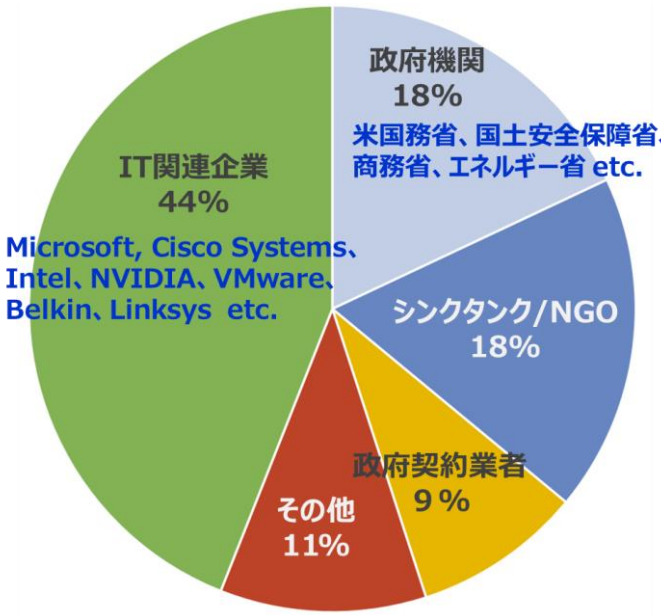

図 2.8 Solarwinds 社 Orion 経由で実施された攻撃の被害組織

以下、具体的な侵害の概要を示す。図 2.9 には SolarWinds 社の Orion を利用しているユーザに対してどのような攻撃が実行されたかを示す[64]。

①被害者は Solarwinds 社 Orion のマルウェア(SUNBURST)付きの更新ファイルをダウンロード。この更新ファイルには正規のデジタル証明書が付けられていた。

②ダウンロードされたバックドアはダウンロードされた環境が実際の Orion の環境であること、マルウェア検出ソフトの確認、一定の潜伏期間の後、あらかじめ用意されていた C&C サーバと通信を開始。収集した侵入環境情報の情報とともに様々なツールを持つ新たなマルウェア(TEADROP)をダウンロード。この時の通信は Solawinds 社との通信に偽装されていた。

③Living off the land 攻撃：新たなマルウェアは侵入した環境を調査。この時、侵入先で利用可能なコマンドラインインタフェースやマイクロソフト管理コンソール、などが使用された。また、Cobalt Strike フレームワークを実装した C&C サーバに接続し、永続化のためのビーコンが埋め込まれた。

④この段階で、初期の侵入に利用したツール等の痕跡を消去。

⑤Golden Ticket 攻撃：Active Directory サーバのクレデンシャルを取得し認証用の Ticket を窃取。これを利用してクラウドサービスと連携する Active Directory Federation Serve に侵入。クラウドサービス認証のための SAML を偽装、クラウドサービスへの侵入路を確保した。

⑥Golden SAML 攻撃：偽装したク SAML チケットを利用してクラウドサービスの AzureAD に永続的にアクセスできる侵入路を確保。

⑦遠隔操作によりクラウドサービスに直接侵入できる経路を確保。

---

[64] マイクロソフト社：https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/ 等を参考に作成。

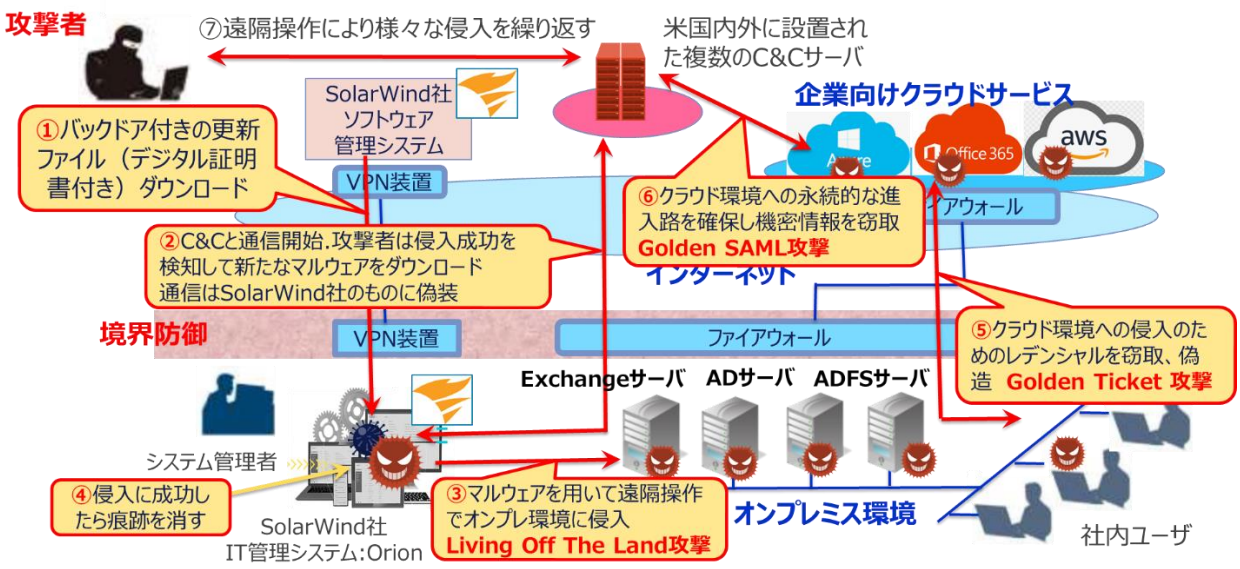

図 2 .9 Solarwinds 社 Orion ユーザへの侵害

それでは、元々の Solarwinds 社への侵害はどのようにおこなわれたのであろうか。図 2.10 に Sloarwind 社の開発環境に対する侵害の状況の解析結果を示す。攻撃は以下のような段階を踏んで実行された模様である。

①Solarwinds 社の開発者が利用している Office365 のアカウントを経由して侵入。3rd パーティソフト若しくはデバイスの脆弱性、パスワード攻撃、標的型フィッシング攻撃のいずれかによる内部アカウント侵害によるとされているが、詳細は明らかにされていなが 2019 年 1 月頃に侵害された模様。

②開発環境侵害のための偵察を実行後、マルウェア(SUNSPOT)を仕込み、ソフトウェアの開発環境を乗っ取る[65]。これは 2019 年 9 月頃の模様。この間、開発環境の偵察結果に基づき、侵害に必要な標的の環境に合わせたマルウェア（SUNSPOT）を開発していたと推定される。

③開発環境の乗っ取りの成功を引き金に攻撃用の C&C サーバの構築を開始。これは一般に市販されているペネトレーション試験用のフレームワークである Cobalt Strike を利用したものであった。

④開発環境で使用されていた Orion 用の正規の DLL にマルウェア SUNBURST を埋め込み。並行して SUNBURST 用の C&C サーバの設置を開始。SUNBURST が設置されたのは 2020 年 2 月頃と推定されている。

⑤この結果、Orion 用の更新ファイルは正規のデジタル署名が付けられて配布されることになった。配布は 2020 年 4 月～6 月にかけて開始された模様（FireEye による発見の約 6 カ月～8 カ月前）。

以上のように、この事案では初期侵入の成功からマルウェアの配信まで約 1 年半以上が費やされる大変手の込んだ攻撃であり、高度な技術力とともに十分な組織力と資金力が用いられたと考えられる。

[65] このマルウェアの挙動と開発環境の乗っ取りに関しては次を参照
https://www.crowdstrike.jp/press-releases/sunspot-malware-technical-analysis/

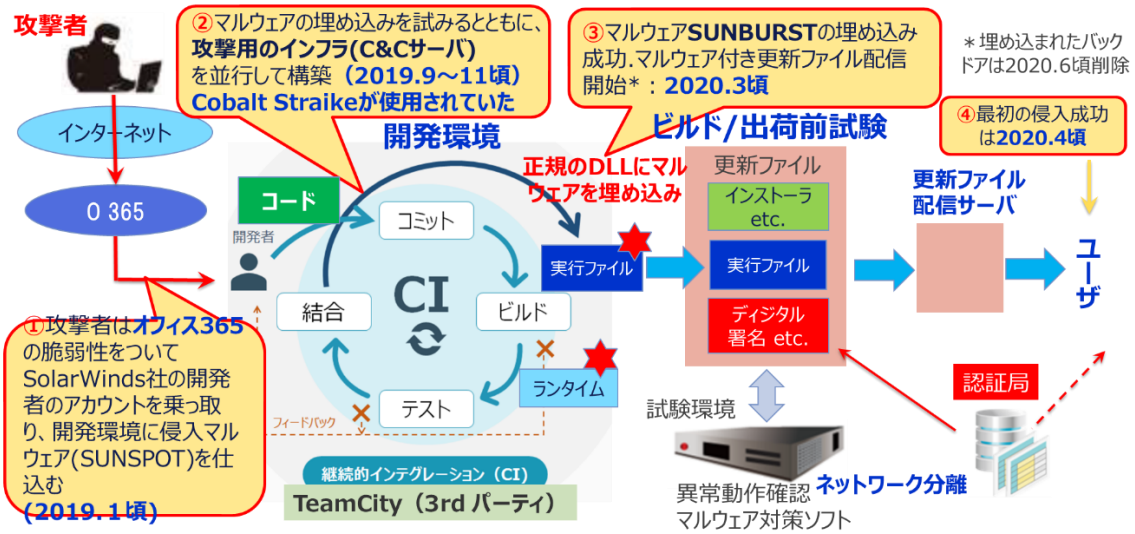

図 2.10 Solarwinds 社の開発環境の侵害手順

この事案で注目される点の 1 つは、サプライチェーン攻撃のために周到に準備された C&C サーバのインフラである。これはマルウェア配布後の攻撃ステップに合わせて以下のように周到に準備されていた[66]。

ステージ 1 初期侵入用の C&C サーバ。侵入の隠蔽のため主に米国内で調達。利用されたドメイン名は、転売、オークション等により入手されていた模様

ステージ 2 侵入先から取得した情報に基づいてターゲットを選定し、これに合わせた C&C サーバを個別に設置。これにより 1 カ所の侵入が判明して C&C サーバが Take Down されても他に影響を及ぼさないようにしていた。海外のサーバが利用されていた。

ステージ 3 クラウド環境に対する永続的な接続を確保する C&C サーバ。主に海外に設置。

以上の攻撃インフラの設置状況を図 2.11 に示す [23]。

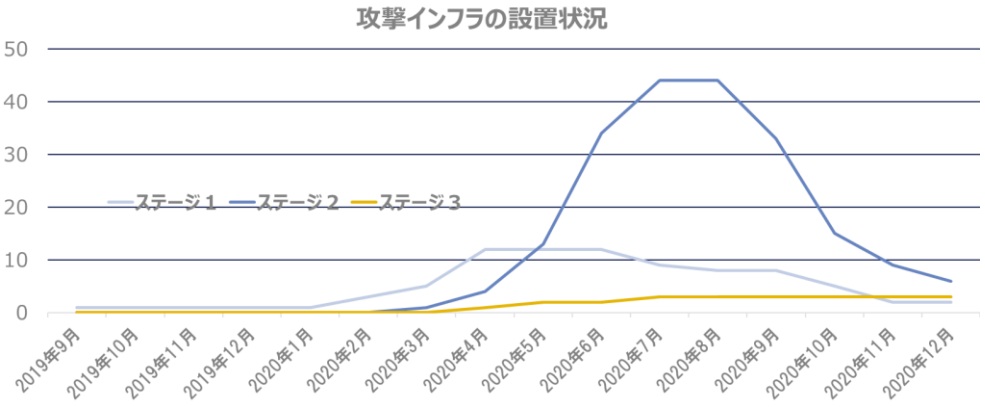

図 2.11 攻撃インフラの設置状況の変化 参考 23 を元に作成

[66] RISKIQ の調査レポートに基づいて整理 https://community.riskiq.com/article/9a515637

もう 1 つの特徴は C&C フレームワークとも呼ばれる一般に利用可能なソフトウェアである Cobalt Strike[67]の使用である。これは Raphael Mudge により 2012 年に開発され、レッドチームシミュレーション、ペネトレーションテストツール等で（合法的）利用されるが、主に正規版がクラッキングされて APT 攻撃で悪用されることも頻繁に行われるようになっている[68]。

図 2.12 に Cobalt Strike のアーキテクチャを示す。以下のプロセスを実行する Beacon, C2 サーバ、Team Server 及び Cobalt Strike Client を構成するクライアントサーバソフトウェアから構成されている。利用されるソフトウェアコンポーネントが柔軟にカスタマイズ可能な特徴を持っている。

Beacon: デフォルトのマルウェアペイロード。Target の環境に設置され、侵入、調査、活動の展開と環境に合わせて様々な機能が追加される。状態に合わせて各種の通信プロトコルが使用される。

C2 サーバ：Beacon の侵入、展開に対応した複数種類のサーバが設置される。

Team Server:複数の C2 サーバを集約して制御可能とするとともに、複数の Cobalt Strike ユーザでシェアされ、分業が行える。

Cobalt Strike Client：Cobalt Strike ユーザが Team Server を介して C2/Beacon を操作する Client ソフト

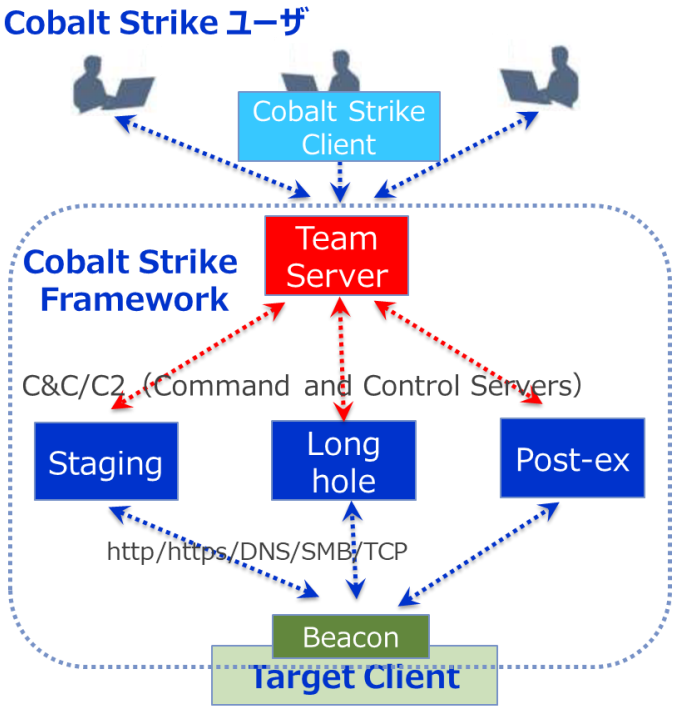

図 2.12 Cobalt Strike のアーキテクチャ

[67] https://www.cobaltstrike.com/

[68] 次にあるように不正利用防止の取り組みが行われているが不正利用は後を絶たない模様である。
https://cloud.google.com/blog/ja/products/identity-security/making-cobalt-strike-harder-for-threat-actors-to-abuse

事例分析４　Emotet

Emotet とは

2014 年に最初にバンキングマルウェア（銀行口座情報の窃取）として検出されたマルウェア。ウクライナを拠点とするサイバー犯罪者集団が作成したと想定されている。その後、これを利用する複数の犯罪集団が拡大（表 2.2）した。これとともに継続的に改良が加えられ、ボットネット拡散の強力なツールとして機能するようなる。Emotet に感染した PC/サーバ(Windows 系）に対して、永続化機能（自律的な起動、C&C への接続、PC/サーバ情報窃取等）がインストールされ、C&C サーバを経由して目的に合わせた様々なマルウェアを送り込むことが可能となっている（図 2.13）。

表 2.2 Emotet を利用する主な犯罪者集団

攻撃G	特徴
TA578	盗用画像」や「著作権侵害」などのメールテーマを使用してマルウェアを配信。2020年6月以降観測
TA551	スレッドハイジャックを使用して、Word文書、PDF、最近ではOneNote文書などの添付ファイルを配信。2018年11月以降観測
TA577	スレッドハイジャックを使用してマルウェアを配信。2021年2月以降観測
TA544	主にイタリアと**日本の組織**を標的としており、通常、Ursnifマルウェア（情報窃取、ランサムウェア）を配信。2022年6月以降観測
TA581	給与計算、顧客情報、請求書、注文書などのビジネスに関連するテーマを使用し、さまざまなファイルタイプやURLを配信。2022年以降観測

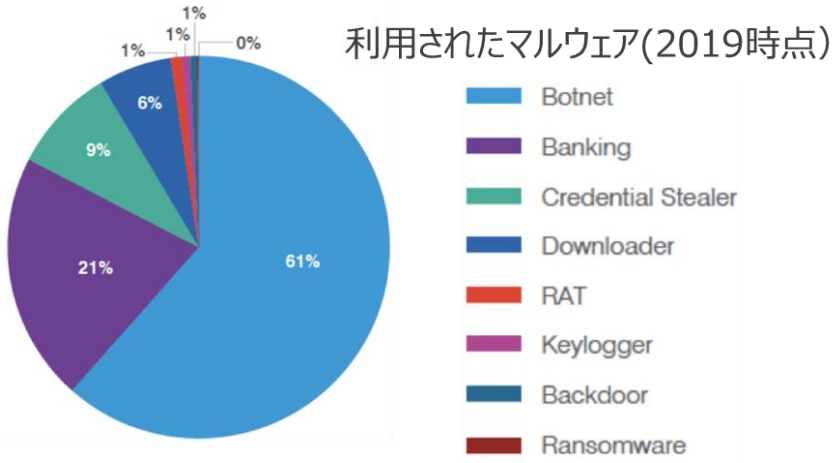

図 2.13 Emotet で利用されたマルウェア

Emotet の侵入・拡散活動の Kill Chain

Emotet の侵入・拡散活動の Kill Chain を図 2.14 に示す[69]。大まかには以下の「手順を踏んでいる。

①攻撃準備：攻撃側はターゲットに対するソーシャルエンジニアリングなどによる偵察活動を実施し、標的型フィッシングメールを送り付ける。このメールには、悪意のあるマクロコマンドが仕込まれたマイクロ

[69] Sophos のレポートを参考に作成
https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-1-the-spam-lure/

ソフトのワード、パワーポイント或いは PDF などのファイルが用いられる。マルウェアをダウンロードする Web サイトの URL も利用される場合もある。これらは極めて古典的な手法と言える。

②侵入、永続化：被害者が添付ファイルを開いた段階で C&C サーバとの通信が開始され被害者の PC に Emotet がダウンロードされる。ダウンロード後、Emotet は実行ファイルコピー、Auto start registry（PC が再起動した際に自動的に実行されるソフトウェアリスト）作成などの永続化活動、侵入先マシン情報、実行プロセス情報などの情報収集を自動的に実行する。この段階で被害者の PC はボット化している。

③横展開：収集した情報を Zip ファイル化して C&C サーバに送信する。この情報に基づいて、被害者の環境に合わせたプラグインが Emotet に対してダウンロードされ実行される。これによって、被害者環境内にあるパスワード等クレデンシャル情報収集、Outlook からの連絡先（メール）リストの収集、マイクロソフトウィンドウズネットワーク内の共有フォルダへのアクセス権取得などの活動を行う。

④拡散：収集したメールアドレスを利用して、被害者環境から外部のユーザに向けてのフィッシングメールを送信する。この際、送信元アドレスはボット化した被害者 PC のアドレスが利用できるため欺瞞度の高いフィッシングメールとなる。また、被害者の内部ネットワークでは共有フォルダに Emotet 感染用のファイルを設置することで、拡散を図る。

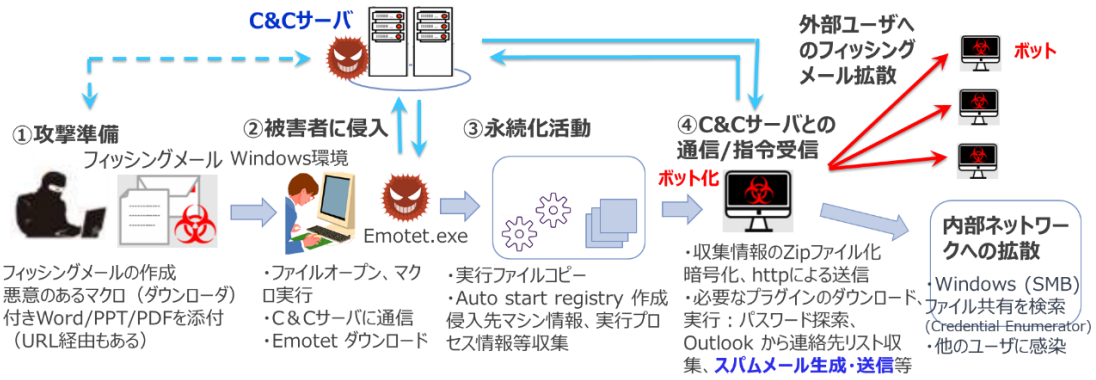

図 2.14 Emotet の侵入・拡散活動の Kill Chain

Emotet の最大の特徴は、様々な利用に対応したマルウェアを配信可能としている点（④の段階）である。資格情報、金融機関のクレデンシャル窃取からランサムウェアの配信など用途に合わせたマルウェアコンポーネントを配信することが可能である。また、Emotet 自体は高度な難読化によるポリモーフィック(Polymorphic)型マルウェアであり既存のアンチウィルスソフトによる検出を困難にしている。一度 Emotet に感染すると感染端末はボット化し、これを踏み台に新たな感染拡大が行われる。ボット化した端末の一部は新たな C&C サーバとしても利用可能となる。

図 2.15(1), (2)に Emotet の C＆C サーバ及びボットネットの分布状況を示す（2022 年 3 月時点の集計）[70]。C&C サーバは欧州、北米を中心に分布する一方でボットネットはアジア地域への集中

[70] 2022.5.8 Emotet Redux, Black Louts Lab より再掲 https://blog.lumen.com/emotet-redux/

度が高くなっている。いずれにしてもこの時点で約 160 万台のコンピュータが感染していることが報告されている。

図 2.15 (1)　Eomote C&C サーバの分布

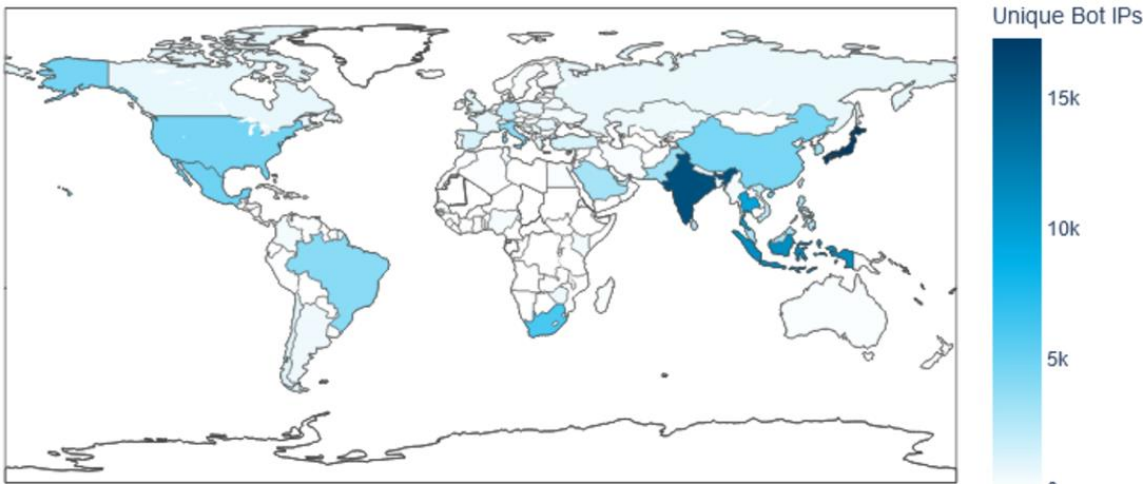

図 2.15(2) Emotet ボットネットの分布

Emotet Take Down の実施と問題点

Emotet の世界的拡散による被害の拡大を受けて、European Union Agency for Criminal Justice Cooperation (欧州連合刑事司法協力庁)により 2021 年 1 月から Emotet のボットネットワーク Take Down が実施された[71]。この作戦はオランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ、ウクライナの司法当局及び欧州連合のサイバー犯罪対策組織 EMPACT(European Multidisciplinary Platform Against Criminal Threats)[72]を中心に実施された。実施のプロセスを図 2.16 に示す。次のようなプロセスで実施されている。

①参加各国に設置された C&C を差し押さえ。

[71] https://www.eurojust.europa.eu/news/worlds-most-dangerous-malware-emotet-disrupted-through-global-action

[72] https://www.europol.europa.eu/crime-areas-and-statistics/empact

②Emotet のボットとの通信及びペイロード更新プロセスに侵入し、Eomotet の通信を遮断する無害化コンポーネントを挿入。
③ボットが Emotet のコンポーネント更新のために C&C サーバにアクセスした段階で上記無害化のコンポーネントをボットが受信
④ボット側でこのコンポーネントを展開すると C&C サーバとの通信が遮断される。

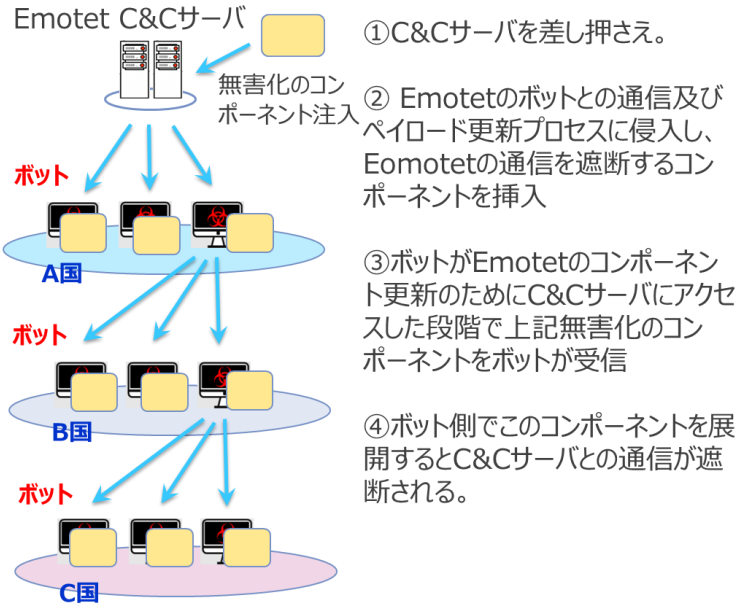

図 2.16 Emotet Take Down のプロセス

この Take Down の実施にあたっては、ボット自体の所有者、該当国の同意を取らずに実施されていることから法的な問題も指摘されている。[73]

[73] https://www.cpomagazine.com/cyber-security/emotet-malware-taken-down-by-global-law-enforcement-effort-cleanup-patch-pushed-to-1-6-million-infected-devices/

第３章　米国、欧州の動向と国連のサイバー規範

ここでは、米国及び欧州において国家レベルのサイバー攻撃に対する認識と Active Cyber Defense に対する考え方について、現在までの動向をまとめる。また、2015 年に策定された国連におけるサイバー規範についても紹介する。

3.1 米国の動向

米国では、2000 年代に入りサイバー攻撃の多様化・高度化と被害拡大に対して、組織毎の受け身のサイバーセキュリティ対策では、これを防ぐことはできないと言った議論により、Active Cyber Defense の概念が主に民間レベルで議論されるようになった[74]。

米国において最初の Active Cyber Defense(この段階では Hack back とも呼ばれていた)の具体例は、1998 年のハッカー集団 Electronic Disturbance Theater に対する米国国防総省によるものと言われている。これは、2 人の米国人によってインターネット上で政治的抗議活動を実行する組織 Electronic Disturbance Theater が結成され、FloodNet と呼ばれる Java アプレットを使用して、国防総省の Web サイトにサービス拒否攻撃(DoS 攻撃)が仕掛けられた。これに対して国防総省は攻撃元のサーバに Java アプレットをリダイレクトしてクラッシュさせる反撃を行ったが、関係ない第 3 者への影響が考慮されていないことにより国防総省でも認められていない行為として論争になった[75]。

また、2000 年 1 月 Conxion Inc.（米国カリフォルニア州サンノゼ）がホストしていた世界貿易機関（WTO）のサーバーが、英国を拠点とするオンライン活動家グループ Electrohippies（E ヒッピーズ）により DoS 攻撃を受けた。これに対して Conxion は攻撃元の IP アドレスを特定し、攻撃パケットをこれにリダイレクトすることで、攻撃元の活動を制限することに成功した。しかしながら、誤った IP アドレスへのリダイレクト、海外サーバへの反撃の問題、などが指摘されている[76]。

当時米国では、ハッカー集団により頻発する DoS 攻撃等のサイバー攻撃対策としてネットワークの境界におかれたファイアウォールにサイバー攻撃を検知した場合何らかの反撃手段を取る機能を実装する流れが出来ていた模様である。ある調査では、フォーチュン 500 企業 320 社のうち 32%が反撃ソフトウェアを導入していることが判明した[77]。

このような中で、Active Cyber Defense の一定の効果は認められるものの、上記のような民間レベルでの攻撃元への反撃は、技術的に攻撃元の特定が曖昧になる可能性があり、また反撃方法によっても無関係な第 3 者に被害が及ぶ可能性がある。そもそもサイバー攻撃自体が不法行為であり、同じレベルで反撃するのは違法行為となるため、何らかの法整備、或いは政府機関による実施、さらに実施にあたってのサイバー攻撃の閾値の設定の必要性といった議論が行われた[78]。

---

[74] 例えば, ”Hunting Hackers: How to Fight Back”, by Deb Radcliff 2000.2.14
この段階では Active Defense, Hack back などに明確な定義は与えられていなかった模様。
https://www.computerworld.com/article/2592630/hunting-hackers--how-to-fight-back.html

[75] https://timeline.com/electronic-disturbance-theater-bace73446dda

[76] https://www.computerworld.com/article/2589346/should-you-strike-back-.html

[77] http://edition.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/

[78] 例えば、Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?, Vikas Jayawal el al. IEEE 2002 International Symposium on Technology and Society (ISTAS'02)

さらに 2000 年代後半より、国家安全保障上の懸念としてのサイバー攻撃が認識されるにあたって、これを抜本的に抑止するための検討が、全米科学国家情報長官(DNI)の要請で全米研究評議会(NRC)の中に設けられた「サイバー抑止委員会」により多面的、総合的に行われた[79]。

以上の動きの中から、国家戦略としての Active Cyber Defense の概念が公式に"Department of Defense Strategy for Operating in Cyberspace"[80]として DoD より表明されたのは 2011 年である。この文書で、DoD として Cyber space を新たな軍事オペレーションの領域として認識し、DoD だけでなく民間の重要インフラに対するサイバー攻撃増加への対抗戦略（５つの Strategic Initiative としてまとめている）を示している。その中で「Strategic Initiative 2:新たな防衛作戦」において、次の４つの指針の１つとして ACD を提唱している。

1) Cyber hygiene 強化のためのベストプラクティス（ソフトウェア/OS を最新の状態に保つ、プロセスの継続的更新、システムのセキュアな構成 etc.）の採用、

2) 内部要員のセキュリティ強化(内部脅威の削減)、

3) ACD の採用

ここでの ACD の概念は、「実際の攻撃による被害が発生する前に、リアルタイムでの脅威の発見、検出、対抗、脆弱性緩和を実施する。侵入は、発見困難な場合が多いことから、ネットワーク内部での監視、対抗方法を進化させる」こととしている。

4)新たなサイバー防衛コンセプトとコンピューティングアーキテクチャ（モバイル、クラウド等）への対応。

これ以降、米国における ACD の主な具体化の流れとして以下のようなものがある。

(1)米軍サイバーコマンド（ USCYBERCOM ）における ACD の採用

(2)SANS の提案による Threat Hunting の一環としての Active Cyber Defense,

(3)最近検討が活発化している、MITER 社による MITER engaged が挙げられる。

(4)現在廃案にはなったものの、民間レベルでの Active Cyber Defense を許容することを目指した法案「Active Defense Certainty Act:ADCA」について

以下では、これらの概要を紹介する。

3.1.1 米軍サイバーコマンド（ USCYBERCOM ）のミッションと ACD に対する考え方

USCYBERCOM 設立の背景[81]

---

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=72f537f7ace2def3a17eeaf6a24a50e6278e567b

[79] この検討の結果は以下のワークショップの会議録としてまとめられている。

Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, 2010 http://www.nap.edu/catalog/12997.html

[80] https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

[81] A Cyber Force for Persistent Operations, Paul Nakasone, 2019 などを参考に作成
https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf

米軍は、米国の安全保障を維持するため、第 2 次世界大戦、冷戦期を通じて米国領土外に世界規模で展開し、対ソ連抑止を含め様々な軍事活動を行ってきている。これに対応し、戦略的優位を維持するために情報通信技術を積極的に活用してきた。例えば、通信衛星の利用による世界規模でのネットワークの構築、利用がその典型例と言える。

一方、冷戦終了後、不安定な政情により発生する地域紛争への介入、2001 年の 9.11 以降開始される対テロ作戦など、国家レベルの紛争以下で行われる軍事作戦としての非正規戦への対処(司法機関レベルでは対処できない活動）が求められるようになった。さらに、2000 年代に入って以降情報通信技術の世界的普及の結果として、サイバー空間領域での国家安全保障のための軍事活動レベルの活動の必要性が認識されるようになった。

特に国家主体を背景としたサイバー攻撃は、グローバルに接続されたサイバー空間を経由して行われ、武力紛争未満の活動ではあるものの、自国の国力を高めるとともに相手国に不利な状況を作り出す、戦略的優位を得る手段を提供している。例えば、サイバー攻撃を利用した知財窃取、機密情報窃取、諜報活動、機密情報の開示、選挙妨害・情報操作による混乱・内政干渉などがこれにあたる。米軍は 2010 年にサイバー軍(USCYBERCOM)を設立したが、2012 年以降は新たにこの領域を作戦領域として定義し、サイバー軍が対応する領域としている。先の P Nakasone の文献で挙げられている事例をこの節の最後に参考として示すが、ここに挙げられた事例だけには止まらない。

USCYBERCOM の体制と進化

2010 年 5 月サイバー軍が設立された。この段階では、陸海空及び海兵隊にサイバー関連のミッション部隊が設立。この段階での主なミッションは、紛争時或いは非正規戦において各軍の物理的行動を支援する情報活動(情報通信システムの防護と敵対勢力に対する攪乱等)が主なミッションであり、陸、海、空、海兵の各組織毎のミッションフォースを統括する組織として編成された。

・米陸軍サイバー司令部（ARCYBER)
・第 24 空軍（2019 年 10 月 11 日付けで第 25 空軍と合併し、第 16 空軍サイバー（AFCYBER）となる）
・米国第 10 艦隊/艦隊サイバー司令部（FLTCYBER)
・米海兵隊サイバースペース司令部（MARFORCYBER)

2012 年サイバー任務部隊（CMF：Cyber Mission Force)が 133 チーム、6200 名の要員で設立。2018 年までに目的とする作戦遂行能力を達成したことが認定された。 この段階で、133 チーム、約 5000 名の軍民要員が所属。以下の 3 つの任務部隊がある。また、米軍の各作戦地域に対応した統合軍におけるサイバー活動の支援も実施することになっている。

・国家任務部隊(National Mission Force Teams)：敵の活動を確認し、攻撃を阻止し、敵を倒すための機動を実施
・戦闘任務部隊(Combat Mission Force Teams)：戦闘員の指揮を支援する軍事サイバー作戦を実施
・サイバー保護部隊(Cyber Protection Teams)：国防総省情報ネットワークと優先任務を保護し、サイバー部隊の戦闘を支援。

以上の体制に対応した USCYBERCOM のサイバー作戦領域のイメージを図 3.1 に示す。

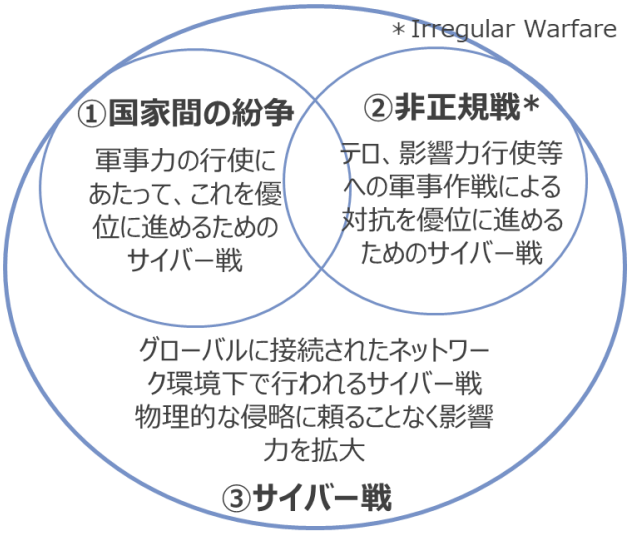

図 3.1 米軍が認識している軍事活動領域とサイバー戦

①、②の領域でのサイバー戦は、それぞれの領域での軍事作戦を有利に進めるための情報通信技術の活用が主（ICT システムの保全、諜報活動、プロパガンダ対応、電子戦など）。これに対して③の領域はサイバー環境で行われる敵対活動に対して優位性を確保する領域。前記の Cyber Mission Force はこの③の領域に対応したものと言える。

Cyber Mission Force の戦略と活動

USCYBERCOM の戦略の特徴は、以下の Persistent engagement と Defend forward にある[82]。Defend forward は Active Cyber Defense の一種と考えられる。

Persistent engagement（持続的関与）

サイバー攻撃への対応部隊(response force)から国家の安全保障に関わるサイバー攻撃への持続的対応部隊(persistence force)に進化させる。この背景には以下の戦略がある。

・ サイバー環境はその技術革新を含め急速に進化。これに即応する継続的関与が必要。

・ サイバー領域での優位性確保；攻撃インフラ等への対応により攻撃を行う側のコストを持続的に増大させる。

・ このためには、持続的な監視・偵察から対応能力の向上まで持続的関与(Operation)が必要。

この戦略実現のためには、サイバー領域における敵対国家等の活動を持続的に監視しておく必要がある。現在でも USCYBERCOM の司令官と NSA 長官はいわゆる Double Cap として兼任されていることも首肯される。

Defend forward（前進防御）

[82] Achieve and Maintain Cyberspace Superiority 2018 Command Vision for US Cyber Command https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

敵対活動の発生源にできるだけ近いところで前方防御を行い、サイバー空間からの攻撃者と持続的に争うことで、戦術的、作戦的、戦略的優位性を継続的に生み出す（この部分は、いわゆる Threat Hunting の領域と考えられる：後述）。これにより、サイバー攻撃がネットワークやシステムに到達する前に阻止する。また、敵対側のリソースを防御にシフトさせ、攻撃頻度を減少させる。具体的に公開されている活動に以下の Hunt Forward がある（攻撃元に直接関与する活動については非公開となっている模様）。

Hunt Forward ミッション

同盟国或いは民間部門と連携し、サイバー攻撃の発生源にできるたけ近い環境でサイバー攻撃者を検出・除去する。具体的には、 Hunt Forward チームを同盟国に派遣し、そのネットワーク環境で同盟国のサイバー部隊と連携した活動を実施し、攻撃側の活動領域を狭めるとともに、活動の早期発見などを積極的に行う。USCYBERCOM のホームページでは以下の活動が明らかにされている。

・2020 年リトアニアにおいて Hunt forward 開始
・2022 年ウクライナに過去最大の Hunt Forward チームを派遣
・2023 年アルバニアにて Hunt forward 作戦を実施
・ 同　　カナダ、ラトビアとの Hunt forward 実施合意。

＜参考＞

表 3.1 具体的事例

発生年	事案	概要
2008	Operation Buckshot Yankee[83]	米国防総省ネットワークへの大規模なハッキング。中東軍から USB 経由でマルウェアが送り込まれ、大規模に汚染。除去に 14 カ月を要した。Operation Buckshot Yankee はこの除去作戦の名前。USCYBERCOM 設立のきっかけになったと言われている。ロシア帰属の分析報告が出される。
2012	Operation Ababil[84]	Bank of America, JPMorgan Chase, Wells Fargo 他の米国金融機関の Web サイトが DDoS 攻撃を受けインターネットバンキングが利用不能となる。イランの核開発に対する経済制裁の報復と見なされている。容疑者のイラン人 7 名訴追されている。
2014	Sands Hotel and Casino[85]	ラスベガスの Sans Hotel の情報システムがイラン由来のサイバー攻撃によりハッキングを受ける。クレジットカードを含む顧客データの流出と情報消去が行われた。Sans Hotel の社長で親イスラエルのアデルソン sh 氏によるイラン非難のスピーチが原因と言われ、イランからの攻撃と見なされている。

[83] https://en.wikipedia.org/wiki/2008_malware_infection_of_the_United_States_Department_of_Defense
https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[84] https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013
https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

[85] https://www.theverge.com/2014/12/11/7376249/iran-hacked-sands-hotel-in-february-cyberwar-adelson-israel

2014	Sony Pictures hack[86]	Sony Pictures の情報システムがハッキングを受け機密情報の漏洩、北朝鮮の金正恩暗殺を描いた映画「ザ・インタビュー」公開中止を求める。北朝鮮由来の攻撃として米国政府は非難。最終的に FBI が北朝鮮偵察総局所属のハッカーを訴追。
2013~2015	GitHub[87]	中国のユーザが国内の検閲を避けるために利用していた GitHub（中国の反検閲プロジェクト GreatFire.org が存在）に対して度々攻撃が行われた。DNS ブロックによる接続妨害、中間者攻撃による検閲、DoS 攻撃等。2015 年の大規模な DDoS 攻撃には中国政府が開発したサイバー攻撃ツール Great Canon が使われたと想定されている。中国は GitHub に代わる独自のサイト Gitte を立ち上げている。

3.1.2 SANS の Threat Hunting と Active Cyber Defense

SANS はいわゆる APT 攻撃の対象になると考えられる組織において、これによる被害の防止若しくは最小化のための Threat Hunting を推奨している[88]。Threat Hunting は組織における一般的なセキュリティ対策に加えて「すでに組織内の存在していることが想定される攻撃者の正体を暴き、対策を試みるアナリストの活動」としており、具体的には図 3.2 に示す活動において ACTIVE DEFENCE 以降の活動を実施できる能力としている。

下図のプロセスの最後にある OFFENSE は、組織や国家が自国の法律に則り、自衛のために採用できる対策具体的活動」としており、例えば偽のバックドア付きのファイルを攻撃側に送り込み攻撃元を特定する、或いはハックバックといった行為を意味するが、SANS はこの活動は推奨していない。これは Threat Hunting の実行主体が民間組織であると想定していることによると考えられる。

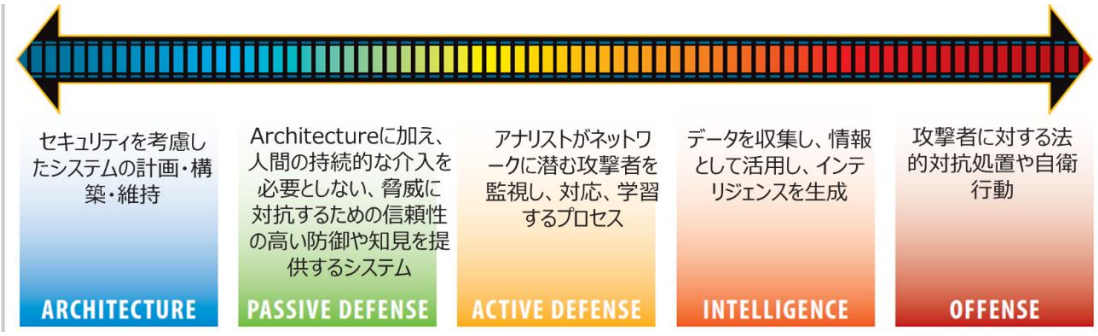

図 3.2　SANS による Threat Hunting のプロセス

SANA が提案している Active Defense はサイバー脅威インテリジェンスモデルに基づくインテリジェンスとの連携による。図 3.3 に両者の関係を示す。インテリジェンスモデルの具体例としては、サイバーキルチェーン、侵入分析のダイヤモンドモデルの 2 つを挙げている。サイバーキルチェインに関しては、これに基づく詳細なデータベースが MITER ATT&CK として用意されておりこの具体的にはこれの活用が想定される。ダ

[86] https://en.wikipedia.org/wiki/Sony_Pictures_hack#Threats_surrounding_The_Interview

[87] https://en.wikipedia.org/wiki/Censorship_of_GitHub
https://www.bankinfosecurity.com/github-hit-by-its-largest-ddos-attack-a-8058
https://www.yamdas.org/column/technique/pin-pointing-chinas-attack-againstj.html

[88] SANS　効果的なスレットハンティングに求められる様々な要素　2016
https://www.sans.org/white-papers/various-factors-required-effective-threat-hunting-japanese/

イアモンドモデルはサイバーキルチェーンで確認された指標を構造化し、攻撃を定義および理解する取り組みをサポートする。図 3.3 に示されているように、アクティブディフェンスはインテリジェンスと相互に連携した活動であり、キルチェーンの可能な限り早い段階で脅威の情報を取得し、その情報を正確に分析したうえで脅威に対処し、得られた教訓を再利用できるプロセスの構築を意味している。

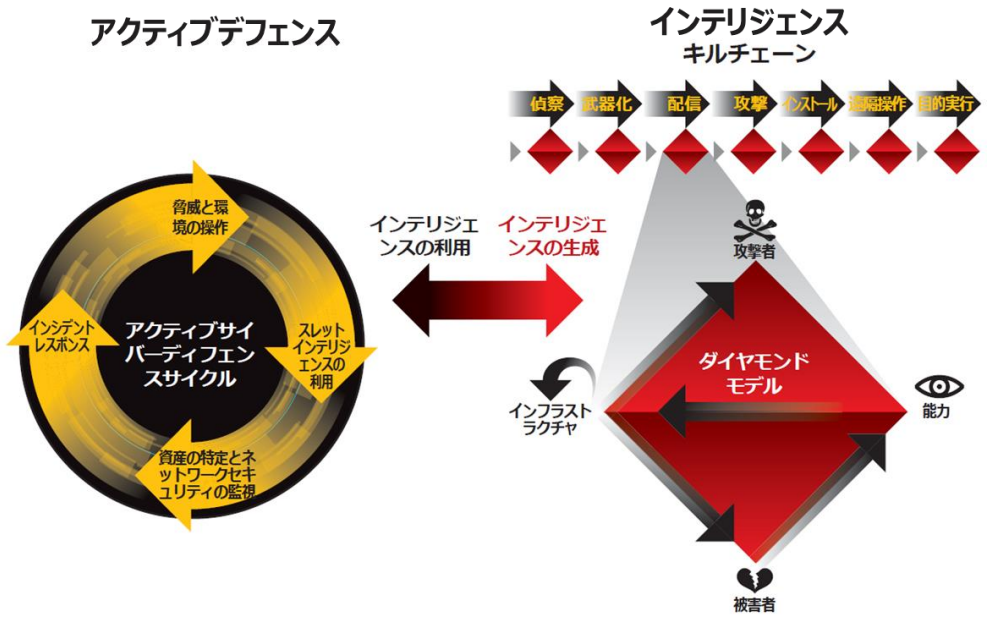

図 3.3 アクティブディフェンスとインテリジェンスの連携

3.1.3 MITER Engage[89]

基本コンセプト

MITER Engage とは、サイバー攻撃活動（APT 攻撃）を検知・分析し、これと交戦(Adversary engagement)することで攻撃を失敗させることを目指したフレームワークである。基本コンセプトには、「攻撃側が 1 つでもミスを犯せば、その帰属が明らかになるとともに攻撃に失敗する」といったコスト上昇を攻撃側に与える Active Cyber Defense の考えが反映されている。

Adversary engagement の状態は、APT 攻撃の Kill Chain の侵入後の活動段階としている。具体的な防御側の手段としては、攻撃側の活動に対する欺瞞(Deception)、妨害（Denial)がある。ただし、MITER Engage はあくまで組織内部での活動であり、組織の境界を越えた活動までは含まれていいない。

これらの手法は、例えば NIST SP800 53rev.5 2020 版[90]の管理策として、3.18 システムおよび通信の保護、SC-26 デコイ、SC-30 秘匿化と誤認誘導、SC-48 センサの再配置、に対応している。

---

[89] https://engage.mitre.org/

[90] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final IPA による和訳が以下にある。
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092657.pdf

ただしこれらは SP800 53 2020 年版で指定されている管理策ベースラインには指定されておらす、組織が自らのリスク判断に基づいて利用可能な管理策の扱いになっている。

開発の経緯

MITER 社は APT 攻撃の Kill Chain に従って、攻撃グループ毎に用いられる具体的な手法を MITER ATT&CK として 2013 年からデータベース化してきた。さらにこれらの手法に積極的に対抗する技術手法の一覧が 2020 年 8 月に MITER Shield として公開された。MITER engage はこれをさらにフレームワーク化して利用されやすいものにすると同時に手法のデータベースとしての MITRE Engage Matrix が用意されている。MITER Engage は 2021 年 8 月にベータ版が公開されのコンテンツは次のサイトで豊富なドキュメントが用意されている。

MITER Engage の構成[91]

MITER Engage のフレームワークの全体像を図 3.4 に示す。フレームワークは攻撃側に対する阻止・妨害、欺瞞といった手法群とこれらを用いての攻撃側との交戦、及びこれを計画し実行後の分析まで含む交戦計画の策定の 4 つの部分から構成されている。

図 3.4 MITER Engage フレームワークの全体像

それぞれの意味は以下の通り。

■攻撃側の活動の阻止/妨害：計画に合わせて、以下のような手法を実装する。

・攻撃軸に対する防御

・ネットワーク変更制御

・コンテナの変更制御

・境界分離 etc.

■攻撃側に対する欺瞞手法：計画に合わせて、以下のような手法を実装する。

・意図的脆弱性

[91] A Practical Guide to Adversary Engagement を参考にまとめた https://engage.mitre.org/wp-content/uploads/2022/04/EngageHandbook-v1.0.pdf

・おとりのクレデンシャル

・ダミーデータ

・Tripwire　etc.

■攻撃側との交戦：自組織の交戦環境の下での具体的な交戦プロセス（表 3.2）に従った交戦の実行と情報収集・分析の実行。

■攻撃側との交戦計画の策定：Engage Matrix(図 3.5)による交戦計画/利用手法の分析。そのために作戦目標を設定した上で以下の４要素を整理する

・欺瞞のナラティブ

・交戦環境の設計

・交戦環境の運用設計

・分析環境の設計

ここで、交戦プロセスは以下の表 3.2 にまとめられている。これは、Barton Whaley, “The Art and Science of Military Deception”を参考に作成されている。

表 3.2 攻撃側との交戦ステップ

	Step	内容
準備	1	攻撃側の目的、能力、手法等を評価・分析する
	2	作戦目標の設定
	3	期待される攻撃側の反応の特定
	4	攻撃側に認識させる状況（欺瞞）の設定
	5	攻撃側に欺瞞を信じさせるための通知手段の設計
	6	成功基準、作戦遂行のゲート設定
交戦	7	作戦の実行
理解	8	データの収集・分析によるインテリジェンスの作成
	9	インテリジェンスのフィードバック
	10	成功/失敗分析とフィードバック

ここまでで理解できるように、MITER Engage は実際に自らの環境に侵入されることを前提に、侵入者に対し関与（交戦）し侵入側の挙動を誘導しながら観察しその属性（IOC データ、マルウェア等）攻撃を防御しつつ、情報の取得を狙ったものと言える。ただし、このフレームワークを実装するには想定される脅威（攻撃グループ）が用いる戦術、手法は実際の交戦を通じてその精度向上を行うという PDCA サイクルを回す必要がある。 Engage Matrix はこれを円滑に行うためのツールと考えられる。

Engage Matrix を図 3.5 に示す。

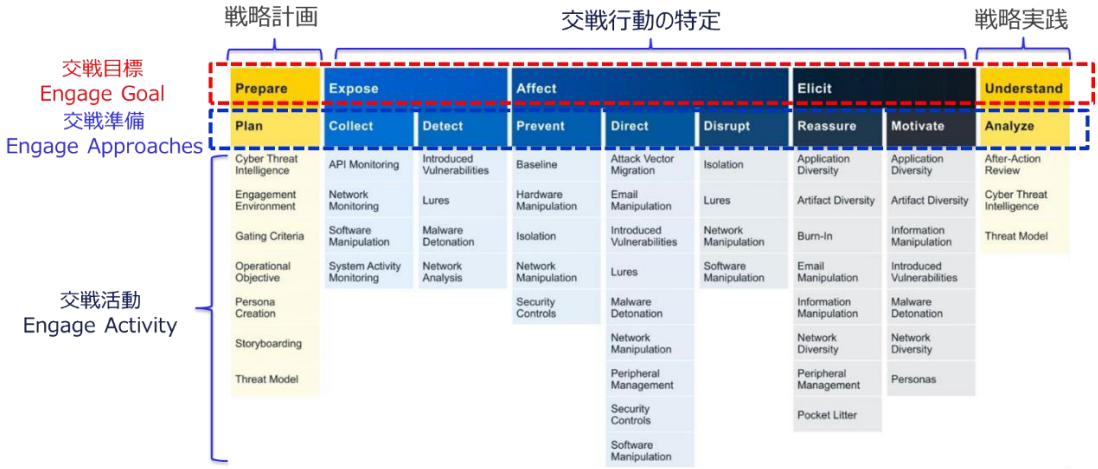

図 3.5 Engage Matrix

図に示される通り、Engage Matrix では交戦計画策定そのための交戦行動の特定、最後に交戦と交戦後のフィードバックまでの一連の流れが可視化されている。実際の交戦計画策定活動は表 3.3 のようにまとめられている。

表 3.3 交戦計画策定活動

Prepare:戦略計画	
Plan	どのような交戦を実施し結果を得るかを特定
Expose:暴露	
Collect	敵の戦術・ツールを観察・収集し、その他の関連情報を収集
Detect	敵の行動に対する認識を確立する
Affect:影響	
Prevent	敵の作戦遂行能力の一部または全部を阻止する
Direct	敵が意図した作戦を遂行させる或いは阻止する
Disrupt	敵の作戦遂行能力を低下させる
Elicit:誘導	
Reassure	欺瞞的なコンポーネントに真正性を付加し、敵に環境が本物であると確信させる
Motivate	敵にミッションの一部または全部を遂行するよう促す
Understand:理解	
Analyze	作戦実行の振り返り

この活動に従えば、最初の計画の要素は計画以下の計画策定プロセスの各ステップの要素に対応することになる（⇒で示す部分が Matrix の Plan で示された要素に対応している。

Step0 作戦目標設定：どのような敵と交戦しどのような成果を得るか等

⇒ Operational objective, Threat modeling

Step1 欺瞞のナラティブ：想定する敵に対して、交戦環境をどう認識させるかのストーリ作成

1)どのような ICT 環境を利用していると思わせるか？

2)利用者（ペルソナ）とその役割、所有データ等

3)ペルソナの活動状況（何時、何を、どの程度）

⇒ Storyboarding, Persona creation

Step2 おとり環境設計・構築：作戦目標、ナラティブに従った交戦環境の構築。全く独立した環境、本番環境への埋め込み、の 2 形態がある。また、敵を誘導するための pocket litter, lure などを埋め込む。 ⇒ Engagement environment

Step3 運用監視計画：おとり環境の運用監視。この際、一定の交戦規則(RoE)を策定しておく。これは、敵の活動が一定限界を超えた場合（踏み台として外部サーバを攻撃等）直ちに運用を停止する、といったものになる。 ⇒ Gating criteria

Step4 分析計画：敵の活動ログを収集し、新たなインテリジェンスを生成するための分析手法と環境の準備 ⇒ Cyber Threat Intelligence

特定の攻撃グループを 1 つの脅威モデルと考えた場合、攻撃側の Kill Chain に対応した様々な手法が ATT&CK のデータベースとしてまとめられている。MITER Engage の交戦行動の特定は、攻撃側の特定の手法を適用した場合、どのようにしてそれを弱点にするかを分析し、これを実行する手法を特定する活動となる。その具体例を図 3.6 に示す。Engage Matrix では弱点化するための手法が体系化されているが、実際の交戦活動では、攻撃側の脅威モデル（具体的な攻撃グループ）を想定した上での手法の選択が行われると考えられる。

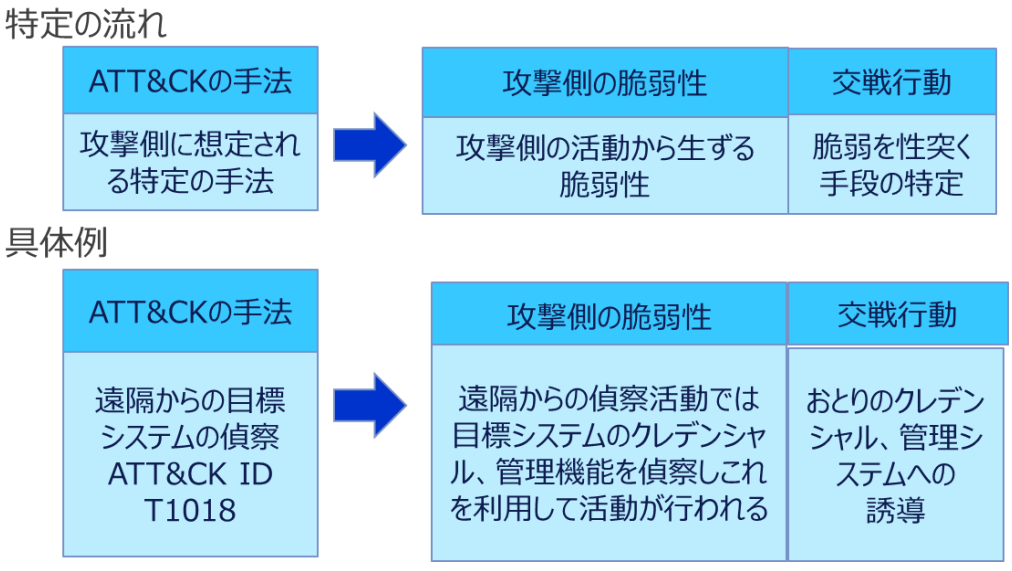

図 3.6 想定される脅威（攻撃グループ）に対応した活動の選択

以上、MITER Engage の概要を見て来たが、SANS の Threat Hunting と同様に、Active Defense とインテリジェンスの連携の仕組みを反映したものと見ることができる。ここでのインテリジェンスの基は MITER ATT&CK が対応し、交戦活動によってフィードバックが行われると考えられる。

3.1.4 Active Defense Certainty Act(ADCA)

HR3270 Active Cyber Defense Certainty Act (ACDC)は共和党ジョージア州選出の下院議員 Tom Graves を代表として 2019 年に提案された法案である。2020 年末に廃案となるが、その内容の一部はまだ法制化の可能性が残されていると言われている。元々は同様の法案が 2017 年に HR4036 として提案されたが否決されている。

この法案の主旨は、民間のハッキング被害者が自ネットワーク外での自己防衛：Active Cyber Defense を実行できることを許容するものである。これは、サイバー攻撃が増加する中で、司法機関での対応が限界であり、民間部門が自ら攻撃側の帰属を明確化できることで、サイバー攻撃を抑止することが狙いであり、法案の有効性はあくまで期間限定であった。

許容される行為は、攻撃側の帰属を明らかにするための、ビーコンの設置を含む、プログラム、コード、またはコマンドを攻撃側のコンピュータに送信することである。これにより、攻撃側の帰属・属性、攻撃の手法等の情報をえることで、攻撃の抑止、防止等を実施することが狙いである。これらの活動は「コンピュータ詐欺および不正使用法 (CFAA[92])」に違反しているが、この適用を除外することが法案の目的であり、実行にあたっては、以下のような制約が設けられていた。

1) 正当な権限を持つ者による実施。 ⇒被害を受けたことを前提に、事前に FBI への届け出、承認を得る。

2) 攻撃側のコンピュータのデータの破壊や障害の原因となる重要な操作機能の破壊の禁止。

3) 攻撃側コンピュータへの侵入を可能にするバックドアの使用禁止

4)無謀に身体的傷害や 5,000 ドルを超える経済的損失を引き起こすこと、公衆衛生や安全に脅威を与えること、インターネット アクセスを永続的に妨害することは禁止。

5)国防システム、政府システム、法執行システム関連システムへの適用は禁止。

この法案の問題点は、これを実行可能なサイバー攻撃の閾値が明確化されていないといったところと考えられる。例えば Kesan らの文献[93]では、

・刑事制裁、訴訟、純粋に防衛的な救済策では対応できない要件が必要

・正確なTrace back

・罪のない第三者に損害を与えた場合に責任を負う

・報復のためではなく必要かつ相応の武力のみを行使すること（正当防衛の要件）

などを明確化しておくことを要請している。

---

[92] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

[93] Thinking Through Active Defense in Cyberspace, Jay P. Kesan 2010
https://nap.nationalacademies.org/read/12997/chapter/23

3.2 欧州の動向

以下では、EU, NATO 及びドイツ、フランス、英国の動向について述べる。

3.2.1 EU の状況

ロシアのウクライナへの軍事進攻を受け、欧州議会・理事会は EU におけるサイバー防衛戦略に関する政策コミュニケを 2022 年 11 月に公表した。この中で、Active Defense という用語が以下のように使用されている。しかし、これが具体的に何を意味するかの明確な定義はない。

"The EU needs to take on more responsibility for its own security. This requires modern and interoperable European armed forces. Member States must therefore, with urgency and priority, commit to increase investments in full-spectrum cyber defence capabilities, including **active defense capabilities**."

（EU Cyber Defense Policy Communication, Nov 2022）[94]

この政策コミュニケの中で明確化されている戦略をまとめると以下のようになる。

・EU 加盟国間での高度なサイバー関連技術の官民連携した開発強化と連携強化。サイバー領域では技術的優位性の獲得が重要。

・サイバー脅威の早期発見、対処のための加盟国間の連携。このための能動的情報技術センサーシステム、サイバー緊急対応チームなどを検討。

・加盟国は連携してサイバー危機管理を強化する。EU サイバー防衛調整センター（EUCDCC）の設立、EU サイバー司令官会議など。

・具体的な対応強化のための Military Computer Emergency Response Team Operational Network (MICNET)を構築する。これは EU 加盟国の防衛システムに影響を及ぼすサイバー脅威に迅速に対応するための情報共有基盤、ツール、能力開発プログラムからなる。ゆくゆくは各国の民間 CERT とも連携を図る。

・EU のセキュリティ・オペレーション・センター（SOC）のインフラ配備を促進するイニシアティブを準備。最新の AI 技術等民間の高度な技術を利用しデジタル欧州プログラムの支援を受けて各国の SOC をグループ化した複数の国の SOC プラットフォームで構成される。これにより集団的検知能力を向上させる。

・EU のリスク評価に基づいた重要インフラに対する脆弱性チェック、信頼できる民間プロバイダーによるサービスを備えた EU レベルのサイバー予備軍の段階的設立等を実施する。

・加盟国間の相互運用性向上のためのセキュリティ基準、認証制度等の統合（ENISA,欧州国防標準化委員会等）。

さらに EU ではこの政策コミュニケの実現に向けて法案を検討中である。2023.4 に提案が行われ、2024 年成立見込みであり、以下のような具体的な内容と必要な予算措置が盛り込まれている[95]。

---

[94] https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

[95] https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

１）EU 域内を中心とした国境をまたがる SOC 基盤で EU からの支援を受けた European Cyber Shield の構築。

・加盟国は少なくとも 1 つの国レベルの SOC を設置。これは、国内の他の官民間組織の SOC の参照点、ゲートウエイの役割を果たすとともに国レベサイバーセキュリティの脅威とインシデントに関する情報を収集・分析する。

・SOC は最新の技術を用いてサイバー脅威、インシデントの検知、統合、分析のためのデータ分析基盤を備える。

・国境を越えたセキュリティ・オペレーション・センター（SOC）の 3 つのコンソーシアムがすでに選ばれており、彼らは AI やデータ分析を利用したサイバー脅威検知ツールやサービスを調達する。

２）EU の重大なセキュリティ脅威に対するレジリエンス向上のための Cyber Emergency Mechanism の確立。

・同メカニズムは、極めて重要な分野（金融、エネルギー、医療など）で活動する事業体に対する協調的な試験など、セキュリティ対応の体制構築を支援するための行動を規定する。欧州委員会は、ENISA と協議の上、関係部門を決定する。

３）この法案に基づき、信頼できるプロバイダーによるインシデント対応サービスで構成される EU Cybersecurity Reserve を設立する。これらの「サイバーファイター」は、重要な事業体に影響を及ぼす重大かつ大規模なサイバーセキュリティ・インシデントが発生した場合、加盟国の要請に応じて介入できるようにしておかなければならない。サイバーファイターは、介入するために事前に契約される。

・サイバーファイターの選考基準には機密情報の保護、セキュリティ・クリアランス、安全な IT システム、短期間での納品、透明性の高い運営体制などを含める。

・このモデルは、サイバーセキュリティを確保するためのウクライナの官民協力のアプローチにヒントを得たものと言われている。

3.2.2 NATO の動向

NATO は 2016 年の NATO サミット（ワルシャワ）で NATO の防衛的任務を再確認し、サイバースペースを NATO が自らを守らなければならない作戦領域として認識した。また、2021 年の NATO サミット（ブリュッセル）では、ケースによっては武力攻撃と見なされる可能性があり、集団的自衛権の発動（第 5 条）があり得ることを認識している。

通常の武力紛争とは異なり、サイバー領域では絶え間ない摩擦と継続的な活動(偽情報キャンペーン、スパイ活動、ランサムウェア、重要なサービスや重要インフラの機能不全を含むサイバー作戦)が存在するとの認識であり、これがある種の閾値を超えれば、武力紛争に相当すると見做せるとの立場を取っている[96]。

[96] 例えば最近のアルバニアに対するイランのサイバー攻撃が該当するとの認識 https://gigazine.net/news/20220908-albania-cuts-diplomatic-ties-iran-cyberattack/

さらに、2023 年 7 月の NATO サミット（ビリュニス）では、サイバー空間における効果的な防御とは、より積極的なアプローチをとることが再度認識され、サイバー防御への包括的なアプローチを採用することが表明された。具体的には、

・NATO の 3 つのサイバー防衛レベル（政治、軍事、技術）をさらに統合し、政治レベルでは価値観の共有とこれに基づく国際規範によるサイバー空間の安定性確保、軍事レベルでは平時、危機、紛争を通じて常に軍民協力を確保する。技術レベルでは悪意のあるサイバー活動を検出、防止、保護するための十分な装備を確保する。

・NATO 加盟国間の連携を一層強化し、全体の抑止力と防衛態勢に対するサイバー防衛の貢献を強化。これに対応して、2016 年の加盟国間の”Cyber Defense Pledge”を更新（内容は非公開）。

・重大な悪意のあるサイバー活動に対応する国家的な緩和努力を支援するために、NATO の新しい仮想サイバーインシデント支援能力（VCISC）を立ち上げ同盟国に対しての支援ツール提供体制を確立（具体的内容は非公開）。

以上の動きは、単なるサイバー防衛から NATO 全体で軍民連携してサイバー領域での悪意ある活動を抑止する一種の”Active Defense”活動と見ることができる。

3.2.3 ドイツの動向

ドイツでは、コンピュータ及び通信のセキュリティを管轄する BSI(Federal Cyber Security Authority)[97]を中心に以下のような Active Cyber Defense が行われている模様である。

1）ある種のサイバー攻撃に対しては、インターネットトラフィックに変更を加えることで阻止または軽減することができる。例えば、インターネットトラフィックの経路を短期的に設定変更することで、特定の形態の攻撃を無効化することができる（再ルーティング規定）。

2）サイバー攻撃側が活動に利用しているインターネットリソース(ドメイン名、IP アドレス等）のハイジャック或いは変更を行う。

－　BSI はこれらの不適切なリソースを利用してくるトラヒックをブロックし、攻撃側及び被害側のトラヒックをモニタリングできる。

3）脆弱性を持つシステムに対する、自動的で大規模な緩和措置の実施。

4）攻撃者が使用するコンポーネントに介入することで、進行中の攻撃を阻止し、将来の攻撃に対する予防を向上させる。BSI は攻撃者の IT システムに侵入することはできないが、有害なデータ・トラフィックを特定することはできる。

但し、ハックバックに対する法規定はない。被害が非常に深刻で、侵襲性の低い手段では目的を達成できない場合にのみ、正当化されると想定される。

3.2.4 フランスの動向

[97] https://www.bsi.bund.de/EN/Home/home_node.html

フランスでは、Active Cyber Defense はフランスの Cybersecurity Agency ANSSI (民間サイバー防衛)は公式に採用はしていない。一方、国防省が 2019 年に採用したドクトリンでは” lutte informatique offensive (LIO)”：軍事目的のためのサイバー攻撃という軍事ドクトリンを採用している。これは国防省管轄 (COMCYBER)で”Offensive IT Fight”として実施に移されている模様である。

フランスにおけるサイバー防衛には以下の２つの柱がある

Offensive IT Fight:敵の軍事能力を評価し、敵の分析能力を修正し、サイバースペースにおける軍事的優位に貢献する。

Defensive IT Fight:サイバー脅威を予測、検知、対応するすることでフランス軍のサイバーレジリエンスを確保する。

ここで指摘されている Offensive IT Fight[98]の特徴は以下の通りである。

- 他の軍事手段との併用により、効果は倍増する可能性があるが、具体的な実行準備には長期を要する。
- 統一された指揮系統と専門部隊を中心に組織され、グローバルな共同作戦行動の戦略レベル、作戦地域で軍の構成要素を機動させるための戦術レベルの両面で実施
- 実施にあたっては、政治的、法的、軍事的リスクのコントロールが必要であり、法律、費用対効果、作戦状況、一般的な政治的背景に基づいて実行される。国際法の原則/規則ならびに国内法と規範に遵守する。
- 欧州レベル及び国際レベルでの連携を進める。
- 実行にあたっての課題は、具体的な技術・人材の開発、欧州を中心としたパートナーシップの構築がある。

3.2.5 英国の動向

英国では、2021 年に行われた”安全保障、防衛、開発、外交政策に関する統合レビュー”[99]に基づいて 2022 年に策定された国家サイバーセキュリティ戦略[100]の柱として以下の５つが挙げられている。

Pillar１． 英国におけるサイバーエコシステムを強化し、人材とスキルに投資し、政府、学界、産業界のパートナーシップを深める。

---

[98] Doctrine militaire de lutte informatique offensive
https://www.defense.gouv.fr/sites/default/files/ministere-armees/Lutte%20informatique%20offensive%20%28LIO%29.PDF

[99] このレビューでは、①科学技術による戦略的優位性の維持、②開かれた国際秩序を形成、③国内外の安全保障と防衛の強化、④国内外のレジリエンスの強化、の 4 点が目標設定されている。
https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

[100] National Cyber Strategy 2022　2030 年までの戦略的方向性により 2025 年を目途に達成する目標として公表されている。
https://www.gov.uk/government/publications/national-cyber-strategy-2022

Pillar2．強靭で豊かなデジタル・UK を構築し、そのサイバー・リスクを軽減することで企業はデジタル技術の経済的利益を最大限に活用できるようになり、市民はオンライン上でより安全に、データが保護されていることを確信できるようにする。

Pillar3．サイバーパワーに不可欠な技術をリードし、産業能力を構築し、将来の技術を確保するための枠組みを開発する。

Pillar4．より安全で豊かで開かれた国際秩序のために、英国のグローバルなリーダーシップと影響力を推進し、政府や産業界のパートナーと協力し、英国のサイバーパワーを支える専門知識を共有する。

Pillar5．サイバースペースにおいて、またサイバースペースを通じて英国の安全保障を強化するために、敵対勢力を検知し、混乱させ、抑止する。

ここで、Active Cyber Defense に関連した戦略の Pillar 5 の内容はさらに以下の 3 つの指針に集約されている。

1．英国の国益と市民を保護するために、国家、犯罪者、その他の悪意のあるサイバー行為者とその活動に関する情報を検出、調査、共有する。

2．英国の国益及び国民を害する、国家、犯罪組織、その他の悪意のあるサイバー行為者を抑止或いは排除する。

3．国家安全保障と重大犯罪の防止・発見を支援するため、サイバースペースにおいて、またサイバースペースを通じて行動を起こす。

これらの戦略実行のためには国家安全保障、司法、外交、経済、及び軍事関連の英国政府の組織及び民間組織との連携が必要になる。このため組織横断的な戦略遂行のために、以下の 2 つの組織が設立され具体的な戦略の実行が行われている。

①National Cyber Security Centre (NCSC)[101]

政府通信本部(GCHQ: Government Communications Headquarters)傘下に、サイバーセキュリティに関する知識の共有、脆弱性の組織的管理、国家レベルのサイバーセキュリティに関する課題への対応と民間組織に対する支援などを目的に 2017 年に設立された組織である。NCSC の設立により、サイバーセキュリティに関して複数の組織に別れて運営されていた政府組織を統合し、運営体制が簡素化され、国家レベルのサイバーインシデントに対する英国の対応能力の向上と、革新的なデジタルサービスの展開が開始された。

NCSC では、前記の戦略指針の 1 、2 に対応して、Active Cyber Defense の実行を”多くのサイバー攻撃から英国民の大多数を保護しサイバー攻撃にさらされる時間を最小にする”ことを目標に掲げ、一元的に推進されている（Active Cyber Defense Program）。

このプログラムでは、脅威に関する知識の共有、脆弱性の封鎖、侵害への対応といった、サイバーセキュリティに関する永続的な課題に取り組むこととが Active Cyber Defense 推進の有力な手段であると認識されている。現状では、これを自動化により効率的に実行し、必要な規模と範囲を生み出す唯一の現実的な方法と考えられている。

101

このプログラムは 2016 年より開始されている。開始当初は、政府組織の保護が中心であったが、現在では英国の国家サイバー戦略の中核にある「社会全体」への取り組みへの対応に変化している。このために MyNCSC プラットフォームと言う、一般人含めて ACD のサービスを享受できるプラットフォームの提供を開始している。このプラットフォーム上では NCSC が提供している各施策で個人が利用可能なもの（メールチェック、Web チェック、早期警報等）が一元的に提供されている。

現在実施されている施策を表 3.に示す。毎年実施施策の効果測定が行われるとともに各施策のスクラップアンドビルドが実施されている。

表 3.4 NCSC の Active Cyber Defense プログラム[102]

実施施策	概要	想定効果
有害サイトのTake Down	英国でホストされている悪質な活動を監視し、これをホスティングしているサーバーの所有者に通知することでTake Downを実行。英国政府機関を装うメール、URLが対象。	悪意のあるC&C、ボットネット抑止
疑わしいEメール報告サービス	一般の人々が疑わしい電子メールやウェブサイトをNCSCに報告、これが分析用にテイクダウン・プロバイダーに送られ、悪質なサイトへのリンクが発見された場合、インターネットからそれらのサイトを削除するよう努める。	フィッシング抑止
メールチェック	電子メールのなりすまし対策（SPF、DKIM、DMARC）、機密性（TLSとMTA-STS）対策を導入する組織を支援。簡単なメールセキュリティチェックサイトを提供。	メールなりすまし、盗聴抑止
脆弱性チェック	一般ユーザ向けに簡易なインタフェースで①送信e-mail、IPアドレス・Webサイト、Webブラウザの脆弱性チェックサービス、②一般的なウェブの脆弱性や設定ミスがないかウェブサイトをチェック、③サブドメイン乗っ取り警告および報告サービス、を提供。	悪意のあるC&C、ボットネット抑止
DNS保護	悪意のある活動に関連するドメインの名前解決を防止するサービス。1,200を超える英国の組織の保護している。	DDoS抑止
早期警報サービス	英国内組織がサインアップすることでインシデント通知、悪意のある可能性のある活動、脆弱性情報を受ける。	セキュリティ情報共有
Exercise in a Box	一般的なサイバーセキュリティインシデントへの対応を、安全でプライベートな環境で練習できる環境の提供。	インシデント対応向上
ルーティング/シグナリング保護	BGPハイジャック検知のためのモニタリングプラットフォーム及びSMS を利用したフィッシング対策のためにし依頼できるSMSのIDを登録保護するSenderID保護レジストリの提供	BGPハッグ、SMS フィッシング抑止
ホスト保護(Host Based Capability)	主に政府が認定した重要な情報を扱うサーバに対してソフトウェアエージェント（EDR)を配備し、サイバーセキュリティ関連のメタデータを収集・分析し、脅威レベルが最も高い悪意のあるアクティビティを検出する。	脅威ハンティング
脆弱性の報告/開示	政府機関のシステムに脆弱性が発見された場合の報告及びトリアージを一元的に行うプラットフォーム及び開示のための脆弱性開示ツールキットの提供	セキュリティ情報共有

②National Cyber Force (NCF)[103]

NCF は 2020 年に設立された組織であり、英国防衛省と政府通信本部からの要員でほぼ均等に構成され、単一の指揮系統の下に、それぞれの専門知識、資源、権限を結集している。その主なミッションは先の指針 3 に対応したものであり、英国及びその同盟国に対して危害を加えるアクターに対してサイバー空間上或いはサイバー空間を通して、対抗し、混乱させ、劣化させ、対抗することにより英国の安全を維持し、国内外における英国の利益を保護・促進することである。NCF は、国防の支援、英国の経済的福祉、重大犯罪の防止など、国家安全保障の幅広い成果を求められており、その活動は、戦術的なものから戦略的なものまで、また国家行為者と非国家行為者の両方に対して多岐に渡っている。より具体的には、以下のような指針が挙げられている。

i) 英国や他の民主主義社会に危害を加えるために、インターネットを利用し国境を越えて活動するテロリスト、犯罪者、国家からの脅威に対抗する。

ii) サイバースペースにおけるデータやサービスの機密性、完全性、可用性を破壊する脅威にサイバーセキュリティを支援すること等で対抗する。

[102] Active Cyber Defense 6th year 、 https://www.ncsc.gov.uk/files/acd6-summary.pdf に基づいて整理

[103] https://www.gov.uk/government/organisations/national-cyber-force/about

iii）英国の国防活動に貢献し、英国の外交政策課題の実現に寄与する（例えば、民間人を保護するために人道危機に介入する）。

NCF の活動は、脅威を及ぼす個人や集団に対する影響、オンラインの活動や通信システムの混乱、物理的システムの運用の低下といったものであり、いわゆる**攻撃的サイバー（Offensive Cyber）**と呼ばれものである。

NCF の活動は、Intelligence Services Act 1994[104], Investigatory Powers Act 2016[105]といった英国国内法、及び紛争に関する国際法に厳密に準拠して実施されるとし、内閣及び司法機関の承認と監督及び議会のよるレビューなど厳密な手続きが取られることとなっている。ここで、Investigatory Powers Act 2016 に関しては一定の手続きの下で、外国に焦点を当てた情報を入手し、英国に脅威を与える海外の個人、グループ、組織を特定するためのバルクデータの一括傍受[106]、及び安全保障・諜報機関、軍隊、法執行機関が、疑わしい機器から電子データを入手する目的で機器に侵入できる Targeted Equipment interference[107]などの権限が認められている。

NCF の具体的な活動プロセスと実績に関しては、機密扱いの部分も多く詳細は不明であるが、いわゆる攻撃的サイバーに関する一般的なプロセスは英国国防省が発行した文献[108]に次のような説明が行われている。

攻撃的サイバー活動の実行プロセスは図に示す 7 つの段階を経て実行される。このプロセスはロッキード・マーチンが開発した APT 攻撃分析のためのキルチーン分析（2.5 節参照）に類似したものとなる。

---

[104] https://en.wikipedia.org/wiki/Intelligence_Services_Act_1994

[105] https://en.wikipedia.org/wiki/Investigatory_Powers_Act_2016#cite_note-44

[106] Factsheet – Bulk Interception、他の方法では特定できない脅威を発見するために、英国外にいる人の通信情報を一括収集することを許可するものであり、傍受の対象として個人または施設を名指ししたり記述したりすることは無いが、特定の目的が定められていなければならない。例えば、「シリアの ISIL による英国に対する攻撃計画」などがある。
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf

[107] Factsheet – Targeted Equipment Interference、この中ではターゲットのログイン認証情報を使用して、コンピュータに保存されているデータにアクセスする、遠隔操作でデバイスにソフトウェアをインストールして情報を得るといったこのが認められている。
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473740/Factsheet-Targeted_Equipment_Interference.pdf

[108] Ministry of Defense, “Cyber Primer, 3rdedition”, 2022.10

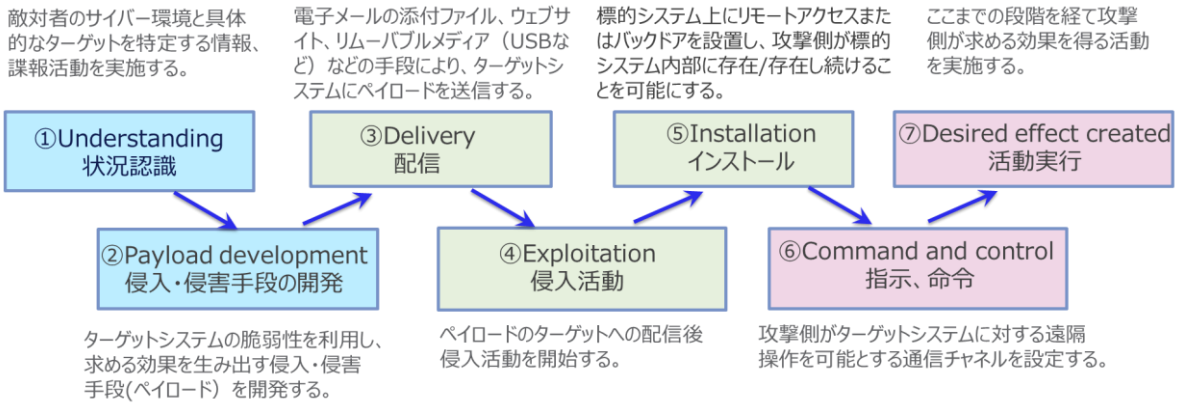

図 3.7　攻撃的サイバーの実行プロセス

3.3 国連におけるサイバー規範について

国連においてはサイバー領域に関する責任ある国家に求められる自主的な行動規範として、2015 年に政府専門家グループによって合意され、国連総会において採択された次の 11 項目がある[109]（国連決議 70/237）。この規範は、国家及び非国家主体による ICT の悪意のある利用が、その範囲、規模、深刻さ及び洗練度を増しており、将来の国家間の紛争において国際平和、安全、安定に対するリスクとなることを鑑みて、そのリスクを軽減するために責任ある国家が遵守すべき規範としてまとめられものである。この規範の拡張に関しては、2015 年以降国連専門家会議等を通じて様々な議論が行われてきてい、現時点でもこの 11 項目が合意されたものの基本と考えられる[110]。

a) **セキュリティに関する国家間の協力**：国際平和及び安全の維持を含む国際連合の目的に沿って、国家は、ICT の利用における安定及び安全を高めるための措置並びに国際平和と安全に対する脅威となり得ると認められる ICT プラクティスを事前に排除するための措置を開発、適用するために協力すべき。

b) **全ての適切な情報の考慮**：ICT に関するインシデントが発生した場合、国家はそのインシデントの全体的な背景、ICT 環境における帰属の問題、結果の性質と程度を含む、すべての関連情報を考慮する必要がある。

c) **自国領域内での不適切な使用の防止**：国家は、自国の領土が ICT を利用した国際的に不正な行為に利用されることを故意に許してはならない；

d) **犯罪及びテロの阻止に向けた協力**：各国は、情報交換、相互支援、ICT を利用したテロリスト及び犯罪者の訴追、並びにそのような脅威に対処するためのその他の協力的な措置を実施するため

[109] https://digitallibrary.un.org/record/799853

[110] 2015 年以降国連の Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace において 2019 年から 2021 年まで検討が行われ、報告書としてまとめられている。この中では 11 項目に対する追加はないもののこれの理解促進のための見解がまとめられている。
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement

に、どのように協力するのが最善かを検討するべきである。各国は、この点に関して新たな措置を開発する必要があるかどうかを検討する必要があるかもしれない；

e) **人権とプライバシーの保護：**国家は、ICT の安全な利用を確保するにあたり、インターネットにおける人権の促進、保護および享受に関する人権理事会決議 20/8 および 26/13、ならびに総会決議 20/8 を尊重すべきである。デジタル時代のプライバシーの権利に関する 68/167 と 69/166 は、表現の自由を含む人権の完全な尊重を保証するものである

f) **重要基盤に対する損害の禁止**：国家は、国際法上の義務に反して、意図的に国家の重要基盤に損害を与え、または公衆にサービスを提供するための重要基盤の使用および運用を損なう ICT 活動を実施及び故意に支援してはならない；

g) **重要基盤の保護：**国家はサイバーセキュリティの世界的な文化の醸成および情報基盤の保護に関する総会決議（58/199）およびその他の関連決議を考慮し、自国の情報基盤を ICT の脅威から保護するための適切な措置を講じる必要がある；

h) **支援要請に対する対応**：国家は、悪意のある ICT 行為の対象となっている他国の支援のための適切な要請に応じるべきである。また、国家は、主権を十分に考慮した上で、自国の領土から発信される他国の ICT を対象とした悪意のある ICT 行為を阻止するための適切な要請に応じるべきである

i) **サプライチェーンセキュリティの確保**：国家は、エンド・ユーザーが ICT 製品のセキュリティに信頼を寄せることができるように、サプライ・チェーンの完全性を確保するための合理的な措置をとるべきである。国家は、悪意のある ICT ツール及び技術の拡散並びに有害な隠された機能の使用を防止するよう努めなければならない；

j) **ICT 脆弱性の報告**：国家は、ICT およびこれに依存した基盤に対する潜在的な脅威を防止あるいは排除するために、ICT の脆弱性について責任ある報告を奨励し、そのような脆弱性に対して利用可能な救済策に関する関連情報を共有するべきである；

k) **緊急対応チームの保護**：国家は、他国の公認緊急対応チーム（CERT:コンピュータ緊急対応チームまたはサイバーセキュリティ事件対応チームとして知られている）の情報システムに害を与える行為を行ったり、この行為を故意に支援してはならない。また国家は、公認緊急対応チームを使用して、悪意のある国際的なアックビティに関与してはならない。

Bart Hogeveen[111]はこの国連規範が、「国家が攻撃的なサイバー能力を責任持って保有し、使用するという点での関連するガイダンス：許容される範囲」を提供しているとしている。ここで、攻撃的サイバー能力とは「標的とするコンピュータ、情報システムとネットワークを操作、拒否、混乱、劣化、破壊する作戦を資源、技能、知識、作戦概念、手順を保有していること」と定義している。そして、この規範は国家が

[111] Bart Hogeveen, “The UN Cyber Norms: How Do They Guide the Responsible Development and Use of Offensive Cyber Capabilities?”, THE CYBER DEFENSE REVIEW, 2022 Fall https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/08_Hogeveen.pdf?ver=BYnHYWAYLrW_PpP4lljm5A%3D%3D#:~:text=The%20UN%20norms%20further%20state,form%20of%20review%20and%20oversight.

政治的・軍事的緊張や経済的対立の中で、意図的または不注意に行う攻撃を防止・軽減するための手段を与えているとし、攻撃的なサイバー能力の保持もこの中に含まれる立場を取っている。

最近になって、2015 年の国連サイバー規範以降、ここ数年の国連でのオープンエンド作業部会及び政府専門家グループ(GGE)での議論の状況が、日本政府代表を務められた赤堀大使によりまとめられている[112]。この中で、主に国家主体を中心としたサイバー攻撃を抑止するための規範、国際法の議論の状況が詳しく述べられている。Active Cyber Defense に関連した文脈での議論の状況を大胆にまとめてみると、

①サイバー攻撃に関しては、既存の国際法、国連憲章が適用可能。また、武力攻撃に相当するサイバー攻撃があり得る。

②武力攻撃に相当するようなサイバー攻撃は国連憲章第 2 条の国家間紛争解決のための武力の行使の禁止に違反する。

③従って、第 51 条の自衛権の発動が可能。

といった方向性はコンセンサスを得ていると考えることができる。

然しながら、現在発生しているサイバー攻撃の状況を見ると、直接人の生命を棄損すると考えられるものはまれであり、大規模な事例もない。むしろ、平時においては深刻ではあるが諜報活動、インフラ設備等の妨害・破壊活動、金銭窃取、知的財産窃取、プロパガンダ・影響工作のための活動と言った武力攻撃の閾値を下回る活動が主体と考えられる。従って何をもって武力攻撃と見なせるかは議論が分かれるところであり、ケースバイケースの判断が必要となっている。要するに、物理的軍事行動を伴う紛争発生時、軍事行動の一環として行われるサイバー攻撃に関しては自衛権の一環としてその行使が認められるが、物理的軍事行動にまで至っていない場合の判断がまだ困難な状況と言える。

[112] 赤堀毅、"サイバーセキュリティと国際法の基本"、東信堂、2023.10

第 4 章 Active Cyber Defense の概念と課題

4.1 論点整理

現時点で、国際的に Active Cyber Defense に関する明確な定義は行われていない考えられる。これは、これまでの議論で、Active Cyber Defense を適用する対象事象（実行主体の帰属、攻撃強度・リスク等）、適用手法、実施主体（政府機関、民間組織等）、適用範囲（組織内、組織がのネットワーク等）などの前提条件と要件が様々であり、これに依存しない一般的な定義が現状では困難なことによると言える。しかしながら、主に議論されているサイバー攻撃の類型としては国家主体を中心とした紛争時及び紛争には該当しないいわゆるグレーゾーンでの活動が対象となっている（2.4 参照）。その意味で、いわゆる軍事用語としての Active Defense「敵に優位性や地位を与えないための攻撃行動や反撃の考え方」とは異なった概念が必要なことに関しては一定のコンセンサスがあると言える[113]。

表 4.1 に従来型の軍事介入と国家主体によるサイバー攻撃の特徴比較をまとめてみた[114]。第 2 章でも見た通り、この種のサイバー攻撃はグローバルなネットワーク環境下で、直接関係のない第 3 国、組織、サプライチェーンを利用して行われることが多いことから、以下のような特徴を持っていると言える（あくまで例示、引き続き議論が必要）。

1）予測、帰属の判断が難しい

第 2 章でも見た通り、サイバー攻撃はグローバルな環境を利用して行われるため、直接の侵入経路だけではその帰属を判断できない。侵入された後のログ分析や利用されたツール等によって帰属は一定程度推定されるが、攻撃自体を事前に予測することは難しい。これは、攻撃側の準備活動、攻撃活動が秘密裡に行われていることにも起因する。また、予測のためのインターネットトラヒックの監視や、ドメイン、メール、SNS 等の疑わしい特定アドレス、アカウントの監視は自国内だけでも個人情報保護、不正侵入防止といった規制と相反する面があり抑制的、事後的な活用に止まざるを得ない。

2）防御・対抗は単独の国家、組織だけでは難しい

サイバー攻撃は、複数の国、組織を経由して実行されるが攻撃情報を共有することが難しい状況である。これはサイバー攻撃に対する監視・検知・防御の能力が国、組織毎で異なっていること、情報共有の仕組みが整っていないことなどに起因する。また、インターネットそのものはあくまで情報をエンドエンドでトランスペアレントに転送することに特化している。従って、サイバーセキュリティはインターネットの利用者及びアプリケーション、サービスの提供事業者などが責任をもつ必要があるが、インターネット全体でこれを維持・管理する仕組みは存在していない。

3）攻撃手段、コストの非対称性

---

[113] 例えば The “Triptych of Cyber Security”: A Classification of Active Cyber Defense”, Robert S. Dewar, 2014, Cycon2014、” Active Cyber Defense: Applying Air Defense to the Cyber Domain”, Dorothy E. Denning and Bradley J. Strawser,2017 などを参照。

[114] Applying Irregular Warfare Principles to Cyber Warfare Frank C. Sanchez, Weilun Lin, and Kent Korunka, 2019 を参考にまとめた。
https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1737001/applying-irregular-warfare-principles-to-cyber-warfare/

費用対効果の観点では、現時点で攻撃側のコストと得られる効果は防御側と比較して少なくて済むという傾向を有している。攻撃手段に関しては、ダーク Web の利用やいわゆるオープンソースの活用が可能であり必要なコストを低下させている。また、最近のマルウェアはモジュール化が進んでおり、ある種のプラットフォームの上でその機能を柔軟に変更できるという特性を持っている（例えば第 2 章　事例分析 3 、4 など）。このため、軍事的介入に比べれば比較的少数のエキスパートで構成された組織の関与で攻撃が可能と言える。

また、サイバー攻撃の活動はネットワークに接続された組織に対してある意味無差別に実施し得る。このことは、攻撃側の目標とする組織以外にも予測不能な影響、重大な結果を引き起こす可能性が大きいが、攻撃側が事前にこれを防ぐ手段を考慮していないことがほとんどと言える。これは攻撃コストを引き下げる一因でもある。一方で、防御側は既存の法制度（不正アクセス禁止法、通信の秘密保持等）や規範（サイバー攻撃のエスカレーション防止、報復ではなく抑止のための行動）などを考慮する必要があり、技術的手段含めかなりの制約が発生する）。

表 4.1 従来型の軍事介入と国家主体によるサイバー攻撃の比較

	従来型の軍事介入	国家主体によるサイバー攻撃
目的・意図	政治的、経済的、イデオロギー的、社会的、宗教的な優位性・支配を（一定期間）**地理的優位性を通じて**獲得する。意図は比較的明瞭。	政治的、経済的、イデオロギー的、社会的、宗教的な優位性・支配の獲得を支援する**情報の獲得、操作、破壊**。国家主体によるものかを含め意図の判断が難しいケースが多い。
戦略	公然/秘密作戦を実施。露骨であり、**帰属は明確**。	秘密作戦を実施。帰属が**不明確**。
実行主体	軍人若しくは準軍人	影響を与える**ネットワークに接続するデバイスを持つ全ての人**が参加可能。但し高度な攻撃には高スキルが必要。
目標	人若しくは目に見える目標、**人命に直接かかわる**もの	主に情報などの無形物や情報システムなどの有形物であり、重要インフラの場合は間接的に人命に影響を与える可能性がある。
攻撃場所	地理的空間。領土、領空、領海の境界が存在。	**ネットワークに接続が可能なあらゆる地理的空間。明確な国家主権は定義されていない。**
準備期間	比較的長期	比較的短期
コスト	比較的高価	軍事介入に比べれば高価ではない
予測可能性	比較的予測可能	攻撃後に判明、予測が難しい
介入条件	明瞭	不明瞭
影響範囲と直接の被害者	地理的に展開する人・ビジネス	**ネットワーク全体に影響を与える可能性**があり、接続された人・ビジネスが直接の被害者となる。意図しない被害も発生
成果	明快	あまり明快ではない

Cycon2014 において”Active Cyber Defense”をテーマとして技術的、戦略的、政治的、法的側面が学術的観点で総合的に議論された[115]。そこで整理されている Active Cyber Defense の具体的な活動の側面は、以下の（1）サイバー状況認識（Cyber Situation Awareness）、(2)サイバー防御行動（計画、実施）の 2 つに分けられることが指摘されている。

(1) サイバー状況認識（Cyber Situation Awareness）：情報通信基盤の状態のセンシング、リアルタイムのデータ収集とその情報の統合化、分析、攻撃の検知といったリアルタイムのタスクが含まれる。

(2) サイバー防御行動（計画、実施）：攻撃の無力化、攻撃者に対する欺瞞、攻撃対象のマスキング、サイバーフォレンジック、攻撃に対してミッション継続を保証するためのサイバーインフラとミッションの

[115] https://ccdcoe.org/uploads/2018/10/CyCon_2014.pdf

適応・自己組織化、脅威エージェントに対する攻撃的措置の実施、将来の潜在的脅威の予測とそれに対応したサイバーインフラの再構成などのリアルタイムかつプロアクティブな措置など。

また、このカンファレンスで先にもあげた Dewar は、それまでに行われている Active Cyber Defense と言う用語を検討した上で次のように定義した。

"an approach to achieving cyber security predicated upon the deployment of measures to detect, analyze, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities including action in those entities' home networks."

"通信システムおよびネットワークに対する脅威をリアルタイムで検出、分析、特定、緩和するための手段の展開と、脅威および脅威の主体（これらの主体のホームネットワークにおける行動を含む）に対して事前または攻撃的な行動をとるための能力およびリソースを組み合わせた、サイバーセキュリティを達成するためのアプローチ"

さらにこれを実現する方法として以下の 3 つの分類を示すとともにこれらが相互に関連し、総合的な対策としてとらえることを指摘している。

1）サイバー状況認識（Cyber Situation Awareness）

①自 NW・情報資産の外部 NW との接続/利用状況の把握

⇒ファイアウォール、Proxy サーバ等を利用した接続のモニタリング

②サイバー攻撃の全体的な活動状況、脆弱性情報のモニタリング （Passive)

⇒（合法的な）インターネットトラヒック疎通情報の監視

⇒脆弱性情報の共有

⇒攻撃情報（kill chain, マルウェア、攻撃グループ等）の共有

③欺瞞等による攻撃情報の Pro-active なモニタリング

⇒ハニーポット等の利用

④サイバー攻撃が疑われる活動主体のモニタリング(Pro-active)

⇒DDoS 攻撃等 ISP 等による異常トラヒック監視。

⇒特定ドメイン、IP アドレス、アカウント等の秘密裏の監視

2) 自 NW 内の防御・レジリエンスの強化：以下の 2 つのタイプを指摘

防御の堅牢化（Fortified defense）:システム的に安全な通信・情報ネットワークを構築し、重要な資産の周囲に防御的な境界線を確立し、意図的または非意図的な事故や損害を最小限に抑える

⇒侵入特定のための欺瞞、攻撃対象資産のマスキング、

攻撃耐性の強化(Resilient defense): 意図的・非意図的なインシデントに耐えうるシステム的な能力を備えた通信・情報ネットワークを構築し、システムの機能性とサービス提供の継続性を確保すること。

3）自 NW 境界を越えた積極的攻撃活動

⇒ 欺瞞：ビーコン付きの欺瞞情報

⇒ ハックバック：攻撃側へのバックドアの設置、攻撃の無効化操作・マルウェアの配置

以上はすでに約 10 年前の議論であるため、現時点での政治的環境、技術環境などは大きく変化している。とは言え、3 つのカテゴリー自体は現在も有効と考えられる。次節ではこのカテゴリーを参考に現代における Active Cyber Defense を「サイバー攻撃の発生を抑止し、攻撃に対する防御とレジリエンスを積極的に向上させる活動」ととらえ現在必要と考えられる実行プロセスとその課題について整理してみる。

4.2 必要と考えられる Active Cyber Defense の実行プロセスと課題

Active Cyber Defense の実行プロセスを体系的に分析するにあたって、ここでは攻撃側の活動プロセスを構造化してみる。これによって攻撃プロセスに対応した Active Cyber Defense の取り得るプロセスを分析することが可能になると考えられる。ただし、サイバー攻撃の脅威は様々な要因、目的に応じて多様な形態をとることから、攻撃側の活動プロセスを網羅的に分析することは困難である。従って、ここでは国家によるサイバー攻撃の典型的な形態である APT 攻撃に絞って検討することとする。

4.2.1 攻撃側の活動プロセスの想定

攻撃側の活動は、まず攻撃意図、機会、必要な能力といったマクロな戦略を策定する戦略立案のフェーズ（戦略レベルの活動）と、これを具体的に実行する戦術レベルの活動フェーズに分けて考えることができる。

戦略レベルの活動

攻撃意図の例としては、2.4 節で挙げたサイバー攻撃の類型が対応してくる。特に国家レベル（平時、紛争時）、テロ組織、組織犯罪など高度かつ攻撃成功時の影響が大きい攻撃アクターに対応して様々な意図が想定される。これに対して機会は攻撃側の目的に合致した何らかの資産を持ちアクセス可能でかつ脆弱性を有する組織や個人である。また、攻撃成功、失敗の可能性とそれぞれのメリット、デメリットの評価も必要になる。能力は攻撃を実行可能な技術と人材・資金といったリソースである。これらは、実際にどのような戦術レベルの活動が必要となるかにも依存して決定されると考えられる。

戦術レベルの活動

戦術レベルの活動はサイバー攻撃側の戦略に応じて様々なものが考えらえる。例えば、DDoS 攻撃のようにある種の政治的意図をもった威嚇、威圧あるいは情報操作、認知戦を目的とした活動などが挙げられる。ここでは APT 攻撃に関する戦術レベルの活動プロセスを考える。これは 2.5 節で紹介した Kill Chain に対応したものになる。具体的には①攻撃準備段階、②侵入活動、③侵入後の活動、の 3 段階に分かれる。さらにそれぞれの段階では表に示すような活動が行われることが想定される。

表 4.2 攻撃プロセスの構造

活動フェーズ		活動の具体例
①攻撃準備段階	目標特定と調査・偵察	ターゲット設定、計画、組織化、脆弱性の発見
	攻撃基盤構築、武器化	C&C/ボットネット構築、マルウェア/バックドア開発、ツール構築等
②侵入活動	侵入活動	フィッシングメール、フィッシングサイト等によるバックドアの設置。ポートスキャン、ソフトウェアアプライチェーン攻撃等（2.2 節参照）

③侵入後の活動	拠点確保、遠隔操作	C&C/ボットネット経由の通信路確保、ウィルス対策ソフトの回避 バックドアの永続化等
	横展開	内部ネットワークトラヒック盗聴、共有サーバ（メール、ファイル等）、ディレクトリサーバ侵害、ネットワーク管理者権限窃取等
	ターゲットの確保	目的に合致した情報窃取、操作、破壊
	痕跡消去、潜伏	活動痕跡の消去（ログ削除、改竄等）、ロジックボムの設置等

4.2.2 戦略レベルでの対応

第 1 章、2 章でも述べた通り、現在のサイバー空間には様々な脆弱性とリスクが存在する。サイバー攻撃それ自体は不法行為であるが、これを実行するアクターは後を絶たない。これを抑止するには攻撃側に対して、攻撃の実行及び攻撃が失敗した場合も含めたコストを上げることがまず考えられる。戦略レベルでの対応はこれを目指した活動になり、以下のようなものが想定される（あくまで例示であり全てではない）。

1）サイバー状況認識による予測と情報共有

実際の攻撃が実行される前の段階で、攻撃の可能性、意図、機会と能力に対するハードルを上げるための活動としては以下のようなものが考えられる。ただしインターネットを経由した攻撃活動には国境の概念が存在しない。従って、できるだけ正確なサイバー状況認識を得るには官民及び自国だけでなく信頼関係を持つ他の国家との活動の連携と情報の共有が必須となると考えられる。

①国家間若しくは非国家主体、テロ組織との対立構造、潜在的な攻撃国の政治・経済的状況、技術水準等の OSINT ⇒攻撃意図、可能性の推定

②攻撃インフラとなり得る C&C サーバ/ボットネットの検出・監視 ⇒攻撃インフラの構築阻止、抑止

③OSS サプライチェーン等のソフトウェアサプライチェーンの監視 ⇒サプライチェーンセキュリティの確保

④ダーク Web 等の監視 ⇒マルウェア開発、サイバー攻撃情報（例えばクレデンシャル）・サービス等の収集

2）サイバー衛生(Cyber hygiene)の向上

第 1 章でも見た通り、現在のインターネットには様々な脆弱性が存在する。これらの脆弱性を極力削減し、より安全なインターネットの構築を実施することで、攻撃の機会のハードルをあげる。具体的には以下のようなことが考えられるが、あくまで例示であり全てではない。

①メール、Web、SNS 等のインターネット上のサービスの

ex. メール；SPF, DKIM, DMARC 等の導入、Web；https の導入と安定運用、SNS；違法コンテンツ、偽情報等の監視と制限

②インターネット自体の可視化とセキュア化

ex. DNS サービスのセキュア化、BGP 等の監視、ドメイン名利用のセキュア化

③インターネット上の ID 管理のセキュア化

ex. FIDO2 対応等

3）自 NW 境界を越えた Active Cyber Defense 実行条件の整備

Active Cyber Defense の具体的な活動には、①攻撃側の属性を特定する活動、②攻撃側の活動を抑止、混乱、破壊する活動。が考えられる。具体的に想定される活動例は以下の 4.2.5 で述べるがこれらの実行には自管轄のネットワークを超えた活動が必要になる（図 4.1）。この場合、攻撃には無関係な国を含め、他国の主権、管轄権に影響を与える活動が必要になると考えられる。従って、国際法、国内法含め許容される範囲、実行手続きとその監査などの実行条件を事前に想定、準備しておく必要がある。

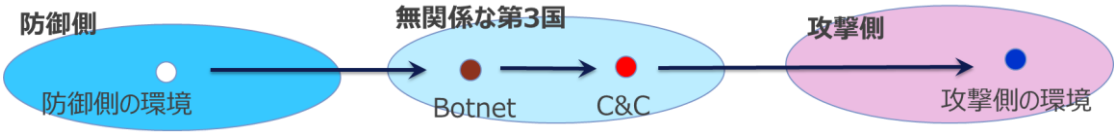

図 4.1 NW 境界を越えた Active Cyber Defense の実行

4.2.3 戦術レベル　攻撃準備段階での対応

この段階では、戦略レベルで得た状況認識と関連して以下のような対応が考えられる。

①狙われそうな資産、業務などから攻撃が想定されるグループの予測、その攻撃手法、プロセスの予測（例えば、MITER ATT&CK 等のデータベースの活用）

②自組織に関連した脆弱性情報、IOC の収集

③境界防御(ファイアウォール、IPS/IDS、Web Proxy 等)、外部との通信トラヒックの監視強化、フィッシングメール対策強化

4.2.4 戦術レベル　攻撃段階での対応

以下は、現在提案若しくは開発されている積極的防御強化策を例示する。

防御の堅牢化（Fortified defense）

・Zero Trust の導入

・セキュリテ設計の強化（例えば、システム制御ツール（コマンドライン IF 等）の最小化/削除等）

・ハニーポット、欺瞞アカウントの設置・監視

攻撃耐性の強化(Resilient defense)

・Threat Hunting/Engagement 能力の獲得

・重要データのマスキング、透かし情報付与

・システム基盤のコンテナ化によるシ機動的再配置（不稼働期間の短縮）

4.2.5 自 NW 境界を越えた積極的攻撃活動

以下で示す自 NW 境界を越えた積極的攻撃活動のどこまでが Active Cyber Defense かといった議論はあるが、ここではあくまで想定される活動とその問題点について示す。

①攻撃側の属性を特定する活動

・観測された攻撃元（必ずしも本来の攻撃元ではない）サーバのアクセス制御を回避して遠隔から侵入。ログ情報等の収集。

・ビーコンの設置

ビーコン付きの欺瞞情報を自組織内に設置し、これを攻撃側が取得することで攻撃元を特定する。攻撃の帰属の明確化が狙い。ジョージアがロシアに対して用いた例がある。

・欺瞞情報の設置

攻撃元特定のための欺瞞情報を設置し、攻撃側がこれを利用した場合に証跡として利用する。

②攻撃側の活動を抑止、混乱、破壊する活動

・ホワイトワーム

悪意のあるソフトウェア（攻撃元）を特定し（被害を受ける前或いは受けてもできるだけ軽微な状態で）無効化する。Emotet の Take Down に利用された無効化ファイルがこれに相当する。

・ハックバック

攻撃元に対してこれを無効化するサイバー攻撃を実施する。DDoS 攻撃、マルウェアの送り込みなどが考えられる。現在攻撃側で一般化している APT 攻撃と同等以上の Kill Chain を用意する必要がある。攻撃インフラとマルウェアに関しては、諜報活動から破壊活動まで攻撃側と同等以上の優位性の確保が必要と考えられる。正確にはハックバックではないが Stuxnet がこれに相当する？

積極的攻撃活動の技術的課題

以上の積極的攻撃活動は攻撃側のサイバー攻撃とは対称ではない。技術的実現性の問題点を表 4.2 に示すが、これらのいわゆる副作用の発生を防止するだけでなく、そもそも攻撃元の帰属が証明可能かといった問題もある。現実には、サイバー攻撃の強度が軍事的介入以上の深刻な状況をもたらす場合に限定されると考えられる。また、実行主体も国家機関特に国家の主権侵害に対応可能な軍事組織に限定されると考えられる。

要素	内容	具体的事例/問題
制御	感染する可能性のあるすべての環境において、コードの動作を制御できるか？	マルウェア自体は侵入先のシステムがターゲットであるか否かを認識せずに拡散する可能性がある（Netptya，Wanncry etc.過去の事例でもほとんどの場合、ターゲット以外への拡散が観測される）
検出	コードが発見される前に任務を完了することを保証できるか？	侵入先の環境は事前に全てわかっているわけではない。従って、どの時点でミッション終了とするかの判断が難し。通常は、バックドアを仕掛けて終了。
帰属	必要に応じて、コードが否認可能か、クレーム可能かを保証できるか？	現代のマルウェアは極めて高度な機能を有する大規模ソフトウェアであり様々な既存コンポーネントを利用せざるを得ないことから、例え難読化が行われていてもこれらを解析することで帰属が判明する可能性が高い。
合法性	そのコードが展開されている司法管轄区では違法になるか？	通常は違法。
倫理性	そのコードの展開は条約、法規その他の国際規範に違反していないか？	諜報活動と見なされた場合これを規制する国際法はない。
誤用	コードとその技術、戦略、設計原理が敵対者、競合者、犯罪者によってコピーされないことを保証できるか？	適切なタイミングでマルウェア等の実行コードの消去が必要だが部分的には可能であっても全てを消去することは困難であり重要な部分がコピーだれる恐れあり。
悪影響	そのコードの展開が、その展開に関する知識も含めて、市民の信頼に有害な影響を与えないこと、貿易や通商を含むその国の政府や制度に対する市民の信頼に悪影響を与えないことを保証できるか？	悪意のあるサイバー攻撃者と同じことを隠密裏に実行することから市民の信頼を得にくい。むしろ組織への不信の増長に繋がる恐れがある（過去の米国NSAのケース等）

第 5 章　まとめ

ここまでで、限られた時間ではあるが可能な限り現在までに議論されている”Active Cyber Defense”の概念、論点についてまとめてきた。主に、米国、欧州を中心とした議論であり、すでに 10 年以上前から活発に議論されている。これに対して我が国では様々な分野の専門家を交えて具体的かつアカデミックな立場からも含め十分な議論が行われているとは言えない状況と考えられる。その意味で、今回の CYDEF2023 においてこの分野における海外の著名な方々をお招きして講演と議論ができることは大変有意義な活動と考えられる。以下、今回の CYDEF2023 において注目したい論点をいくつか指摘してまとめに代える。

サイバーセキュリティは端的に言えば、サイバー空間を安全に利活用していく上でのリスクマネジメントである。ただし、これは個人、組織、国家がそれぞれ個別に行うリスクマネジメントとは異なり、サイバー空間を利活用する全てのステークホルダが一定の責任を共有して実践する必要がある。責任の共有には状況認識の共有がまず必要である。特に、ここ約 20 年間にわたってサイバー空間のグローバル化が急速に進み、国家の安全保障レベルでのリスクも顕在化してきている現状がある。地政学的リスクに比較して、サイバー空間はグローバルなある意味国境と明確な国家主権が定義されていない環境下でのリスクである。一方で、ある意味地政学的リスクと相関する面も持っている。この点を考慮した上でのサイバーセキュリティに関する具体的な状況認識と脅威をどのように捉え、共有していくかが必要である。一例としては、この White paper では取り上げることができなかった情報戦、認知戦の分野がある。これはインターネット上の SNS 等が急速に発達、拡大することで新たな脅威という認識ができている。この問題にいかに対処すべきか状況認識と脅威の共有が行われればと思う。

技術的観点で見ると、Active Cyber Defense には様々な手法を取ることが可能である。一方で、我が国では法的制約、その整備の遅れ等により具体的な技術手段の研究開発が活発とは言えない状況に見える。いわゆる研究開発とこれの実践、実行することとは区別する必要があると考えられる。リスクマネジメントの観点は脅威に対する対抗としても多様な検討が行われる必要があると考えられる。

サイバー空間における国家主権、責任分担の共有という観点では、国際法・規範、国内法といった観点でもグローバルスタンダードの在り方を理解しておく必要がある。この分野でも、様々な立場の専門家による議論が必要であり、今回の CYDEF2023 を通じて理解が深まることを期待する。

アクティブサイバーディフェンス　アドホック　メンバ
井手達夫
時藤和夫
仲間力
植草祐則
三宅功

White paper 利用にあたっての制限

本ペーパーの著作権は著者にあり、所有権はサイバーディフェンスイノベーション機構にある。著作権者もしく所有権者が許可したサイトから電子的に配布される本ペーパーを入手し、非営利目的で利用、再配布する場合、著作権者および所有権者に不利益を与えない限り、入手したときの状態のまま使う限り、自由に使え何ら制限はない。出展とタイトルを明示して参照が明確な形で、一部内容を他文書中で流用することができる。直接的営利目的（販売など）で使うことはできない。ただし、広い営利活動の一部で利用する場合、所有権者が許可をし、かつ定めた利用条件の中で、非営利目的の場合のように使うことができる。