サイバー戦入門　その２

－サイバー戦の概念と作戦－

三村　守（防大情報工学科）

１　はじめに

陸・海・空・宇宙に続き、サイバースペースという第５のドメインが提唱され、サイバー戦という言葉ぐらいは誰もが耳にするようになった。近年ではサイバースペースの重要性は広く認知され、各国がサイバー戦能力の向上に積極的に取り組んでいる。国内では、従来の電子戦の概念がサイバースペースにも拡張され、包括的電子戦としての概念の整理及び、それに対応するための新体制の検討が実施されるようになってきた。しかしながら、その発端となったサイバースペースの特性については驚くほど理解されていない。これは、サイバースペースの重要性についてはある程度理解されつつあるものの、その変化に対応するための具体的な人材育成については、少数の専門家に重点が置かれているためであると考えられる。それにもかかわらず、全体の底上げを図るための組織的な取り組みは進んでいるとは言いがたい。

陸・海・空の従来のドメインは、各種戦に体系化されて整理されており、各々の規定が定められている。例えば、海上のドメインでは、対潜戦、対空戦、対水上戦等に体系化されており、各戦闘の規定が明確に定められている。このような規定を策定するためには、各戦闘の特性が十分に理解されていなければならない。例えば、ミサイルが飛来したときにどのような対処をするべきかについては、各対抗手段の効果がどの程度か、あるいはそれらの対抗手段のコストはどの程度なのか等の特性が理解されていなければ策定のしようがない。陸・海・空の従来のドメインについては、将来の技術の進歩に伴って変化がある可能性はあるものの、このような特性は比較的に組織全般に理解されていると言える。

しかしながら、サイバースペースについては、サイバー戦に関する具体的な規定がなく、体系的な整理も不十分である。この原因の一端は、サイバー攻撃とは何かが組織全般に理解されていないためであると考えられる。これが組織全般に理解されていなければ、サイバースペースに関する組織的な取り組みを適切に進めることは困難である。また、サイバー作戦を立案して意思決定をする必要が生じた場合にも、そもそも作戦を立案することすら困難である。平時においても、新聞報道などでサイバー攻撃や情報流出の事件を目にする機会は増えてきている。それらの事件におけるサイバー攻撃が、自分たちの組織にどのようなインパクトを与えるのかを検討するためには、サイバー攻撃とは何か

を理解することが不可欠である。しかしながら、専門家以外にはサイバー攻撃はおろか、それを理解するためのサイバースペースに関する基本的な仕組みもほとんど教育されていないのが現状である。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試みた。本稿ではそれに引き続き、サイバー戦の概念とサイバー作戦の種類について平易に解説することを試みる。以下、第２節ではまずサイバー戦の定義と範囲について考察する。第３節では、近年焦点となっている包括的電子戦の概念を理解するために、サイバー戦と電子戦の違いについて、その重複部分を中心に考察する。第４節ではサイバー作戦の種類について説明し、第５節以降ではサイバー作戦の攻勢的な構成要素であるサイバーＩＳＲ[1]及びサイバー攻撃について説明し、最後に全体をまとめる。

２　サイバー戦の定義と範囲

（１）伝統的なサイバー戦

サイバー戦とは何かを定義するのは簡単ではなく、コンセンサスが得られた明確な定義は存在しない。しかしながら、サイバースペースについてはこれまでにいくつかの定義が示されている。米国防省は２００６年に、サイバースペースは「デジタル化された情報がコンピュータ・ネットワークを通じてやりとりされる国際的な環境」と定義した[2]。当時の「コンピュータ・ネットワーク」とは、コンピュータとコンピュータの間を主にＴＣＰ／ＩＰという共通のプロトコル[3]を通じてやりとりするネットワークのことであった。この頃のコンピュータ・ネットワークは、主としてインターネットとそれに接続するＬＡＮ[4]によって構成されていた。この「コンピュータ・ネットワーク」に「国際的な環境」をかけあわせると、主としてひとつの国に属する組織が運用するＬＡＮはその範囲から外れる。よって、当時のサイバースペースの範囲は、主にインターネットを示していたものと考えられる。したがって、２００６年頃のサイバー戦とは、主としてインターネットにおいて不正アクセスやサービス拒否攻撃等のサイバー攻撃を実施することを示していたものと考えられる。例えば２００７年４月のエストニアに対して実施されたとされるサイバー攻撃や、２００８年８月に発生した南オセチア紛争でのグルジア[5]に対するサイバー攻撃等はインターネットを経由して実施され

---

[1]ISR (Intelligence Surveillance and Reconnaissance)
[2]Joint Publication 3-13 Information Operations
[3]通信を実施するための共通の約束事のことであり、通信規約と呼ばれる。
[4]LAN (Local Area Network)
[5]現在のジョージア

たとされている。これらは、従来のサイバースペースの定義の枠にあてはまる伝統的なサイバー戦の例である。しかしながらその後、この定義の枠にはあてはまらないサイバー攻撃が生起するようになり、サイバースペースは拡大することになる。

（２）拡大するサイバー戦

２００７年９月、シリアの防空レーダーシステムがサイバー攻撃により錯乱され、イスラエルによる空爆を許したとされる事件（オーチャード作戦）が生起した[6]。この作戦には、イスラエルの諜報機関である８２００部隊がかかわったとの指摘がある。詳細は公式には明らかにされていないが、防空レーダーシステムに対する攻撃がインターネット経由で実施されたとは考えにくい。また、２０１０年６月には、スタックスネットと呼ばれるＵＳＢメモリ経由で産業用制御システムを攻撃するマルウェアが発見された。このマルウェアは、コンピュータ・ネットワークを経由せずに、伝統的な狭い意味でのコンピュータではなく産業用制御システムを攻撃する機能を備えていた[7]。さらに２０１１年には、米国の無人機に偽のＧＰＳ信号を受信させ、イラン国内に着陸させて捕獲したとされる事件が発生した[8]。この事例でも、伝統的な狭い意味でのコンピュータではなく、無人機の組込システムが攻撃の対象となっている。また、伝統的なコンピュータ・ネットワークの範囲を超えた電磁波を介して実施されている点も注目に値する。これらのサイバー攻撃は、明らかに従来のサイバースペースの範囲を超えて実施されている。

このような伝統的な定義に当てはまらないサイバー攻撃が実施可能となった理由は、伝統的なコンピュータとネットワークで使用されてきた共通のアーキテクチャ[9]やプロトコルが、対象となった機器でも用いられるようになったことによる。例えば、代表的な産業用制御システムであるＳＣＡＤＡ[10]は、伝統的なコンピュータと共通のアーキテクチャで動作し、通信方式を拡張してＴＣＰ／ＩＰ上で動作することも可能となっている。日常生活においても、ほとんどのスマートフォン、家電、車等の利便性の高い機能を提供する基本ソフトウェアは、伝統的なコンピュータで用いられてきたＯＳ[11]をベースとして開発され、組込システムとして実装されている。さらに、車以外にも船舶、無人機等のあらゆるビークルにおいて、伝統的なコンピュー

---

[6]Fulghum, D.A. (2007). Why Syria's Air Defenses Failed to Detect Israelis, Aviation Week and Space Technology
[7]Kushner, D. (2014). The Real Story of Stuxnet, IEEE Spectrum
[8]Iran’s Alleged Drone Hack: Tough, but Possible, https://www.wired.com/2011/12/iran-drone-hack-gps/
[9]基本設計や設計思想等の基本設計概念
[10]SCADA (Supervisory Control And Data Acquisition)
[11]OS (Operating System)

タで使用されてきたアーキテクチャが用いられるようになってきている。これらの機器は、やはり従来のコンピュータ・ネットワークで使用されてきた共通のプロトコルを用いてネットワークに接続される。このネットワークは、従来のインターネットやＬＡＮに限らず、無線電波等のあらゆる通信ネットワークを含むようになってきている。このように、近年ではあらゆる機器が、伝統的なコンピュータと同じアーキテクチャで動作し、同じプロトコルで相互にやりとりするようになってきており、この仕組みはＩｏＴ（モノのインターネット）[12]と呼ばれている。つまり、ＩｏＴの普及はサイバー戦の範囲を拡大するものであると言える。

このような状況の中、米国防省は２０１０年になって、サイバースペースの定義を「インターネット、通信ネットワーク、コンピュータシステム、組込プロセッサと制御装置を含む情報技術基盤による相互に独立したネットワークから構成される情報環境の全体的なドメイン」に拡大している[13]。この定義によると、サイバースペースとはコンピュータと共通のアーキテクチャやプロトコルが適用された環境であり、その範囲は陸・海・空・宇宙のこれまでのドメイン全般におよぶ。したがって、サイバースペースは、今後ますます機器のスマート化が進み、共通のアーキテクチャやプロトコルが普及すればするほど拡大していくであろう。このような例は身近にも確認できる。例えば、近年の水上艦艇の内部ネットワーク、新野外通信システムのソフトウェア無線機、ＶｏＩＰ[14]を採用した自動即時電話網等がある。これらは、伝統的な通信システムや組込システムに、コンピュータと同じアーキテクチャやプロトコルが採用され、サイバースペースが拡大した例である。より身近な例としては、ガラケーからスマートフォンへシフトが進んでいることが挙げられる。ガラケーは日本独自のアーキテクチャにより動作していたが、スマートフォンはコンピュータのＯＳをベースに開発したアーキテクチャを採用している。これらの例が示すように、現状ではサイバースペースに含まれない伝統的な機器も、スマート化によりサイバースペースに含まれるようになる可能性が高い。

３　サイバー戦と電子戦の重複

サイバースペースはコンピュータと共通のアーキテクチャやプロトコルが適用された環境であり、その範囲は電磁波を含めた陸・海・空・宇宙のこれまでのドメイン全般におよぶようになってきた。２０１１年に発生した米国の無

[12]IoT (Internet of Things)
[13]Joint Publication 3-13 Information Operations
[14]Voice over IP

人機がイラン国内に着陸させられて捕獲された事件は、サイバー戦と電子戦に重複する部分があることを示唆するものであると考えられる。ＲＡＮＤ社のレポート[15]によると、サイバー作戦と電子戦の概念は図１に示すように重複している。伝統的な電子戦と、電子戦とサイバー戦（サイバー作戦）の重複部分は、あわせて包括的電子戦と呼ばれることもある。

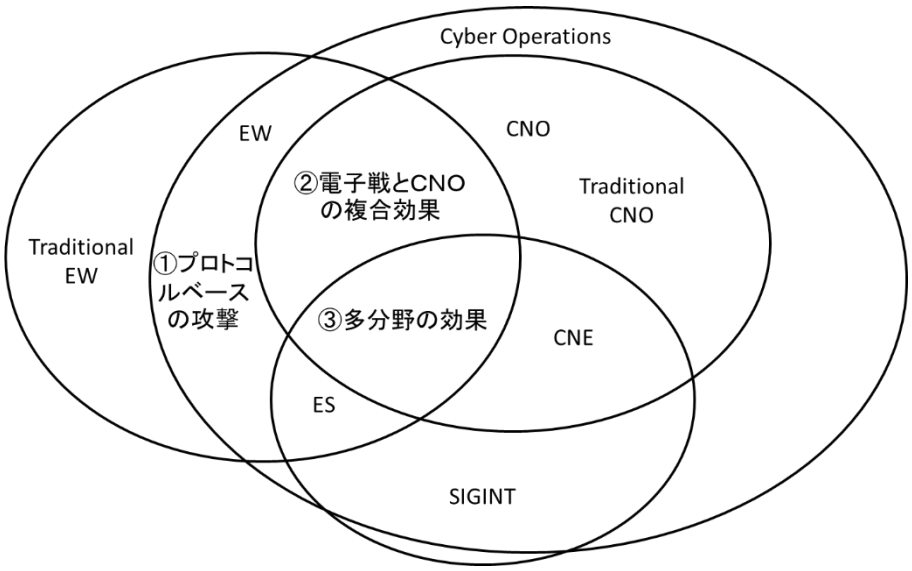


図１：サイバー戦と電子戦の関係

（１）伝統的なサイバー戦と電子戦

まず、図１において互いに重複しない伝統的なサイバー作戦（ＣＮＯ[16]）と電子戦の概念について考察する。伝統的なサイバー作戦の概念には、インターネットにおける不正アクセスやサービス拒否攻撃等のサイバー攻撃が含まれる。これらの伝統的なサイバー攻撃は、前節で示したとおり、電磁波を介さずに主にインターネット上で実施される。したがって、電子戦の概念との重複する部分はないものと考えられる。伝統的な電子戦の概念には、対艦ミサイル対処時の電波妨害等が含まれる。伝統的な対艦ミサイル対処時の電波妨害等は、伝統的なコンピュータで使用されてきたアーキテクチャやプロトコルを用いない専門機器によって実施される。したがって、サイバー戦の概念と重複する部分はないものと考えられる。

（２）サイバー戦と電子戦の重複部分

次に、図１においてサイバー作戦と電子戦の概念が重複する部分について

[15]Porche III I.R.et al. (2013). Redefining Information Warfare Boundaries for an Army in a Wireless World

[16]CNO (Computer Network Operations)

考察する。この重複する部分は、包括的電子戦の概念において拡張された部分でもある。先に示した米国の無人機がイラン国内に着陸させられて捕獲された事件では、偽のＧＰＳ信号を受信させて無人機を誘導したとされている。この事件では、偽のＧＰＳ信号という電磁波の一種が使用されている。したがって、これは電子戦の概念に含まれると解釈することができる。しかしながら、伝統的な電子戦の概念では、ミサイルを妨害電波により無力化することはできたとしても、その制御を奪うことまではほとんど想定されていない。この事件では、無人機の制御を奪ってイラン国内に着陸させている。このような従来はほとんど想定していなかったことが実施可能となった原因は、伝統的なコンピュータとネットワークで使用されてきた共通のアーキテクチャやプロトコルを用いた組込機器が、無人機に実装されるようになったことによるものと考えられる。

偽のＧＰＳ信号を発信するためには、そのプロトコルに従った電磁波を発信する機材（ハードウェア）が必要となる。したがって、このサイバー攻撃はプロトコルベースの攻撃（図１①）に分類されるものと考えられる。ここからさらに無人機の組込システム等の脆弱性を突いて攻撃することができれば、それにより電子戦とＣＮＯの複合効果（図１②）が得られるものと考えられる。また、同様に無人機の組込システムに電磁波を通じてアクセスし、その応答から何らかの情報が得られれば、多分野の効果（図１③）が得られる可能性もある。図１で示した概念によると、包括的電子戦における拡張部分は①～③に分類することができ、これらの新たな概念における脅威とその対策が必要になってきている。

４　サイバー作戦の種類

（１）伝統的なサイバー作戦（ＣＮＯ）

伝統的なサイバー作戦の主要な構成要素であるＣＮＯは、サイバー情報収集（ＣＮＥ[17]）、サイバー攻撃（ＣＮＡ[18]）及びサイバー防護（ＣＮＤ[19]）に分類される。

ア　サイバー情報収集（ＣＮＥ）

米国防省の定義[20]によると、ＣＮＥは「対象や相手の自動化された情報システムやネットワークからデータを集めるために、コンピュータ・ネットワークの利用を通じて実行する情報収集の能力や作戦を実行可能とす

[17]CNE (Computer Network Exploitation)
[18]CNA (Computer Network Attack)
[19]CND (Computer Network Defense)
[20]Joint Publication 1-02Department of Defense Dictionary of Military and Associated Terms

ること」とされている。平たく言うと、ＣＮＥはコンピュータ・ネットワークを通じた情報収集のことである。ここで言うＥｘｐｌｏｉｔは情報の搾取のことであり、サイバー・セキュリティ分野における脆弱性を突くことを意味するわけではない。情報収集にはインターネット等から収集できる公開情報を活用したＯＳＩＮＴ[21]や、不正アクセス等の非合法な手段を用いたＡＰＴ[22]による手法等がある。大規模なＣＮＥが実施された事例としては、国内では２０１１年に政府機関や防衛産業で発生した情報流出事案や、２０１５年に年金機構等で発生した情報流出事案が記憶に新しい。これらの事例では不正アクセスが実施されているため、場合によっては広義のサイバー攻撃との見方もある。しかしながら、これらの事例における攻撃者の目的は、システムの錯乱、無力化、機能低下、あるいは破壊ではなく、情報の搾取であったとされている。そのため、サイバー作戦（ＣＮＯ）においては、これらの事例はサイバー情報収集（ＣＮＥ）に区分される。

イ　サイバー攻撃（ＣＮＡ）

ＣＮＡは「コンピュータとコンピュータ・ネットワークに内在する情報、あるいはコンピュータやネットワークそれ自体を錯乱、無力化、機能低下、あるいは破壊するためにコンピュータ・ネットワークの利用を通じてとられる活動」と定義されている。こちらはいわゆる狭義のサイバー攻撃のことである。サイバー攻撃（ＣＮＡ）では、その手法として不正アクセスを伴う点はサイバー情報収集（ＣＮＥ）におけるＡＰＴと同様であるが、その目的は情報収集ではなく、システムの錯乱、無力化、機能低下、あるいは破壊である点が異なっている。大規模なＣＮＡが実施された事例は国内では確認されていないが、海外では２００７年９月にシリアの防空レーダーシステムが無力化されたとされる事案や、２０１０年６月に発見された産業用制御システムの機能低下を目的としたとされるスタックスネットが有名である。

ウ　サイバー防護（ＣＮＤ）

ＣＮＥ及びＣＮＡは、実施側が主体となって能動的に実施する攻勢的な作戦であると言える。これに対し、ＣＮＤは「国防省の情報システムとコンピュータ・ネットワーク内を保護、監視、分析、検知し、不正な活動に対応するためにとられる活動」と定義されている。つまり、ＣＮＤはＣＮＥ及びＣＮＡに対し、受動的に実施する防勢的な作戦であると言える。今日ではサイバー防護（ＣＮＤ）は、情報システムを運用するほとんどの組

[21]OSINT (Open Source Intelligence)
[22]APT (Advanced Persistent Threat)

織において実施されている。大規模な組織においては、組織内にＳＯＣ[23]とＣＳＩＲＴ[24]を構築、あるいはこれらの業務を外部に委託してサイバー防護（ＣＮＤ）を実施している。ＳＯＣでは侵入検知装置等のセキュリティ機材で情報システムとコンピュータ・ネットワーク内を保護、監視し、マルウェアや不正アクセスの兆候を検知した場合にはその内容を分析する。そして、何らかの対応が必要な場合には、ＣＳＩＲＴがそのハンドリングを実施する。この対応は、インシデント・レスポンスと呼ばれる。

（２）拡大したサイバー作戦（ＣＯ[25]）

米国防省のサイバー作戦のドクトリン[26]によると、サイバースペースにおけるサイバー作戦（ＣＯ）は、攻勢的サイバー作戦（ＯＣＯ[27]）と防勢的サイバー作戦（ＤＣＯ[28]）に分類される。攻勢的サイバー作戦は、「サイバースペースを通じ、あるいはサイバースペースへの強制干渉により、戦力投射を企図したサイバー作戦」と定義されている。ここで言うサイバースペースを通じた作戦は、コンピュータ・ネットワークを対象とした伝統的なサイバー作戦（ＣＮＯ）を含み、文字通りサイバースペース内で完結する作戦を示すものと解釈することができる。サイバースペースへの強制干渉は、前節で示したプロトコルベースの攻撃のように、外部からサイバースペースへの干渉も含むようになったことを示唆しているものと解釈することができる。これに対し、防勢的サイバー作戦は、「国防省あるいは他の友好的なサイバースペースの防護を企図したサイバー作戦」と定義されている。伝統的なサイバー防護（ＣＮＤ）が国防省のみを対象としていたが、防勢的サイバー作戦では友好的なサイバースペースもその対象に含んでいる。このように、サイバー作戦（ＣＯ）は、伝統的サイバー作戦（ＣＮＯ）を拡大した概念であることが定義からも確認できる。

（３）サイバー活動

従来の伝統的なサイバー作戦の主要な構成要素であったサイバー情報収集（ＣＮＥ）、サイバー攻撃（ＣＮＡ）及びサイバー防護（ＣＮＤ）は、サイバー作戦のドクトリン[29]ではサイバー活動に整理されている。表１にサイバー活動の種類を示す。

---

[23]SOC (Security Operation Center)
[24]CSIRT (Computer Security Incident Response Team)
[25]CO (Cyberspace Operations)
[26]Joint Publication 3-12R Cyberspace Operations
[27]OCO (Offensive Cyberspace Operations)
[28]DCO (Defensive Cyberspace Operations)
[29]Joint Publication 3-12R Cyberspace Operations

表１：サイバー活動の種類

サイバー活動	定義
サイバー防護	国防省の情報ネットワークを保証、運用、防護するための、国防省のサイバースペース内での通常の活動
サイバーＩＳＲ[30]	一時的に委任された信号情報作戦任免権者の下の付属の信号情報ユニット、あるいは命令によって認証された統合部隊指揮官によって実施される情報活動
サイバー作戦環境準備	可能性のある次の軍事作戦のための計画及び準備を可能にする情報活動以外の活動
サイバー攻撃	サイバースペースにおいて様々な直接的な無力化効果を生み出すサイバー活動や、物理ドメインにおいて密かに、あるいは明確に無力化する細工を生み出すサイバー活動

サイバー防護は、伝統的なサイバー防護（ＣＮＤ）に相当する活動である。サイバーＩＳＲ及びサイバー作戦環境準備は、伝統的なサイバー情報収集（ＣＮＥ）に相当する活動であり、情報活動とそれ以外の活動に分類されている。サイバー攻撃は、伝統的なサイバー攻撃（ＣＮＡ）を拡大した活動であり、スタックスネットの事例のような物理ドメインへの干渉も含まれることが明確に定義されている。

５　サイバーＩＳＲの概要

サイバーＩＳＲは、こちらから主体的に目的に応じた対象を選定して実施するインテリジェンス活動と、サイバー攻撃を受けた場合にその発信源や攻撃者を特定するためのカウンター・インテリジェンス活動に区分される。

（１）インテリジェンス活動

サイバー戦におけるインテリジェンス活動を実施するためには、作戦目的の設定が必要である。逆の言い方をすると、インテリジェンス活動の対象となる情報は、その作戦目的に応じて決定される。

まずは単純な例から考えてみると、例えばサービス拒否攻撃を実施するためには、その対象となるサービスのＵＲＬ等の論理的な場所や、アプリケーションの名称等のそのサービスを提供する仕組みを調査する必要がある。また、ある組織に標的型メール攻撃を実施するのであれば、その組織に所属する対象者のメールアドレスを知っている必要があるし、その後の攻撃をより効果的に実施するためにはその情報システムの仕組みに関する情報も必要

[30]ISR (Intelligence Surveillance and Reconnaissance)

になってくる。攻撃対象がわからなければ攻撃のしようがないのは当然のことである。これらの単純な例では、対象のＵＲＬやメールアドレス等の論理的な場所や、対象のアプリケーション等の情報システムに関する情報がインテリジェンス活動の対象となる。

次に、より複雑な洗練された事例について検討してみる。例えば、２０１０年６月に発見されたスタックスネットの事例では、その作戦目的は原子炉で用いられる遠心分離機の機能低下であったとされている。この事例では、対象とする遠心分離機で用いられる産業用制御システムや関連する情報システムに関する情報だけでなく、ネットワークを経由せずに人間を介した社会工学的な侵入経路を検討するためのあらゆる情報がインテリジェンス活動の対象となってくるものと考えられる。そのため、インテリジェンスの情報源は信号情報だけでなく人的情報等にもおよび、膨大な情報を収集して分析する必要が出てくる。よって、このような洗練されたサイバー攻撃を実施するためのインテリジェンス活動は、あらゆる目的や対象に対して網羅的に実施できるものではない。

したがって、効果的なインテリジェンス活動を実施するためには、その作戦目的の設定が不可欠となる。しかしながら、サイバー攻撃によって何ができるのかが組織全般に理解されていなければ、この作成目的の設定は非常に困難な作業となり、あいまいで不明瞭なものにならざるをえない点には注意が必要である。「ニワトリが先か？タマゴが先か？」の悩ましい問題である。

（２）カウンター・インテリジェンス活動

サイバー戦におけるカウンター・インテリジェンス活動は、サイバー攻撃の発信源や攻撃者を特定し、その攻撃を抑止することが目的とされている場合が多い。

一般にサイバー攻撃では、その攻撃者を特定することは極めて困難とされている。なぜならば、洗練されたサイバー攻撃は乗っ取られたサーバ等の踏み台を経由して実施される場合が多く、攻撃の発信源となったサーバを管理する人物、組織、国が、その攻撃の実施者であるとは限らないからである。インターネットにおいては、ネットワークに接続するサーバを一元的に管理する組織は存在せず、そのサーバの管理は様々な国の様々な組織に委ねられている。そのため、複数の踏み台が使用された場合には、それらのサーバが法律の異なる複数の国々にまたがっている場合も少なくなく、その調査は実質的に不可能である場合が多い。

そこで、サイバー攻撃の攻撃者を推定するために、複数のサイバー攻撃の相関分析を実施するのが一般的である。例えば、ある攻撃と別の攻撃で同一のサーバが用いられた場合、それらの攻撃は同一の攻撃者によって実施され

た可能性がでてくる。同様に、ある攻撃と別の攻撃で、同じメールアドレスを用いて登録された別のサーバが用いられた場合や、同じマルウェアが用いられた場合にも、やはり同一の攻撃者によって実施された可能性がある。このように、サイバー攻撃の相関分析の基本は、伝統的な情報分析の場合と同様に相互参照（クロス・リファレンス）によって共通点を抽出することである。したがって、これまでのサイバー攻撃に関して相互参照に利用できる情報を蓄積し、それらを共有することは極めて重要である。相互参照に利用できる情報には様々な種類があり、その信頼性や重要度は異なる。相互参照により、ある攻撃に関する単一の情報が一致したからといって、それらの攻撃が同一の攻撃者によるものと判断するのは難しい。それらの情報には、偽造することが容易な情報もあれば、困難な情報もある。また、攻撃者との関連性が強い情報もあれば、弱い情報もある。したがって、その信頼性や重要度に応じ、アナリストは優先すべき情報を選択する必要が出てくる。２００９年にサイバー・キル・チェーン[31]という概念を提唱したロッキード・マーティン社のレポート[32]では、この情報はインディケータと呼ばれ、「単一で分離不能なもの」、「加工により得られたもの」及び「振舞いに関するもの」の３種類に整理されている。これらのインディケータのうち、もっとも攻撃者に近い重要なインディケータは「振舞いによるもの」と言われている。これらのインディケータを積み重ねることで、サイバー攻撃の主体像を構築することが可能となる。これは、犯罪心理学におけるプロファイリングのようなものである。相関分析によって攻撃者を明らかにしたとされる例としては、２０１３年２月に米国のマンディアント社が公表したレポート[33]が有名である。

（３）非対称戦

サイバー空間におけるインテリジェンス活動の相手は対称ではない。これは前述のとおり、サイバー空間では相手を特定することが極めて困難であることに起因している。

インテリジェンス活動ではその作戦目的に応じ、インテリジェンスの関連部署がその達成に必要な情報を収集する。この対象は、相手のインテリジェンス部門やカウンター・インテリジェンス部門に限定されるわけではなく、組織全般が対象となってくる。この関係を図示すると図２のとおりとなる。このように、インテリジェンス活動における攻撃側と防御側は、ほとんどの

---

[31]標的型攻撃の段階を連鎖的に偵察、武器化、配送、攻撃、インストール、遠隔操作、目的実行に区分したモデル

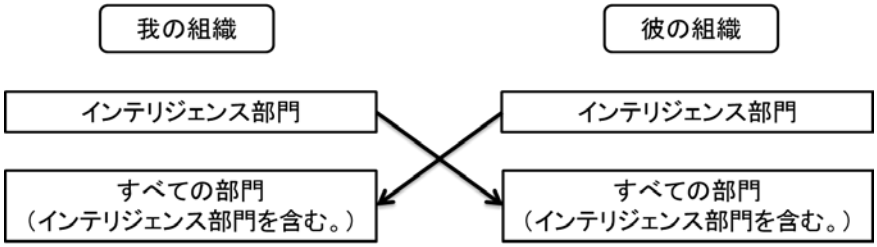
[32]Hutchins, E.M. et al. (2009). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

[33]Mandiant(2013). APT1: Exposing One of China's Cyber Espionage Units

場合に対称とはならない。カウンター・インテリジェンス部門は、このすべての部門に対するインテリジェンス活動への対策を検討することになる。この関係は、インテリジェンス活動であるＣＮＥの場合だけでなく、ＣＮＡの場合にも同様に当てはまる。

このように、サイバー戦は非対称戦であるという認識は、サイバー作戦を検討する上では非常に重要である。彼の可能行動を見積もるにあたっては、彼は何かを取り違えてはならない。我のインテリジェンス部門のカウンター・パートは彼のインテリジェンス部門であるが、インテリジェンス活動の対象はほとんどの場合にインテリジェンス部門ではない。わかり易く例えると、サイバー戦は攻撃側と防御側が同一の騎馬戦ではなく、攻撃側と防御側が異なる棒倒しのようなものである。

図２：インテリジェンス活動の対象



（４）サイバーＩＳＲの手段

サイバーＩＳＲは、その対象とする時間軸に着目すると、「偵察」と「サーベイランス」に分類できる。両者は類似の概念であるが、「偵察」はある状況単一の観測を示す概念であるのに対し、「サーベイランス」は継続した観測を示す概念である点に違いがある。サイバー情報収集を、その手段に着目して分類すると、「ＯＳＩＮＴ」、「受動的偵察」及び「ＡＰＴ」に分類できる。これらのうちの「ＯＳＩＮＴ」及び「受動的偵察」は「偵察」の主な手段であり、「ＡＰＴ」は「サーベイランス」の主な手段としての位置づけが強い。

公開情報を収集する「ＯＳＩＮＴ」は、サイバー情報収集の最も基本的かつ重要な手段であり、サイバー戦のあらゆる局面において活用できる手段である。「ＯＳＩＮＴ」は、インテリジェンス・コミュニティが利用する情報の８０～９５％を占める[34]とも言われている。攻撃者が対象の偵察を実施する場合には、その意図を気づかれないように公開情報を収集する。例えば、公開情報から職務に関連する情報を抽出し、さらにその情報を、Ｇｏｏｇｌ

[34]Pallaris, C. (2008). Open Source Intelligence: A Strategic Enabler of National Security

ｅ等の検索エンジンを用いて検索する。人物を調査するに当たっては、Ｌｉｎｅ、Ｆａｃｅｂｏｏｋ、Ｔｗｉｔｔｅｒ等のＳＮＳ[35]も非常に有益な情報源となる。ここからメールアドレスを入手することができれば、さらにそのドメイン[36]に関する情報を調査することで、対象の情報システムのＩＰアドレスを特定することができる。このように、「ＯＳＩＮＴ」により具体的な対象に関する情報を入手することができれば、その対象に対する受動的偵察を実施することが可能となる。なお、インターネットにおいて相手に気づかれないように「ＯＳＩＮＴ」を実施するためには、対象となる情報を収集している第３者機関のサイトを利用する、あるいはＴＯＲ[37]等の通信元を秘匿するシステムを利用するのが基本である。

「受動的偵察」は、対象とする環境の情報を引き出すより直接的なステップである。「受動的偵察」では、様々なツールを用いて段階的に、対象とするネットワークの論理的構成、提供されているサービスの内容、ＯＳの推定、脆弱性の推定等を実施する。例えば、対象とする環境のパケットを傍受することができれば、そのパケットに含まれる情報を分析することで、ネットワークの論理構成等を把握することができる。この調査は、相手に気づかれないように受動的にネットワークを盗聴して実施するのが理想的であるが、難しい場合にはこちらから能動的に少量のパケットを送信してその応答を観測して実施することも可能である。次に、各サーバにおいて開放されているポートを調査し、そのポートで提供されているサービスやアプリケーションを調査するとともに、そのサーバで用いられているＯＳを推定する。これらの調査は、ある情報を送信してその応答内容を調査する[38]ｎｍａｐ等のツールを用いることで容易に実施することが可能である。そのサーバで用いられているＯＳやアプリケーションを特定することができれば、各ＯＳやアプリケーションの脆弱性を「ＯＳＩＮＴ」によって調査することで、不正アクセスの手段を得ることが可能となる。

不正アクセスを伴う「ＡＰＴ」は、さらに直接的でサイバー攻撃（ＣＮＡ）と共通のプロセスを踏むが、その主要な目的はあくまでもシステム内部に保管されている情報の抽出である。したがって、「ＡＰＴ」は相手に攻撃されたことが気づかれないように慎重に実施され、用意周到に計画される。例えば、相手の情報システムに重大な影響を与えることがないように特別にカスタマイズされたマルウェアが用いられたり、端末の脆弱性を突く受動的な攻

[35]SNS (Social Network Service)
[36]メールアドレスの＠より後の部分
[37]TOR (The Onion Router) インターネット上の通信を多重に暗号化し、多数のサーバを経由することで通信元の特定を極めて困難にするシステム
[38]プローブと呼ばれる。

撃が用いられたりする。「ＡＰＴ」の手順については、次節のサイバー攻撃の概要において解説する。

６　サイバー攻撃の概要

サイバー攻撃は、一般的に表２に示すプロセスで実施される。これらのすべてのプロセスは、攻撃されていることに気づかれないように、かつ攻撃元を特定できないように隠蔽することに留意して実施される。例えば、通信元を秘匿するために攻撃はＴＯＲ経由で実施され、証拠隠滅のためにアクセスログが削除される場合もある。

表２：サイバー攻撃のプロセス [39]

隠蔽(Obfuscate)	偵察(Recon)	対象とするシステムの構成、環境等の情報を偵察する。
	スキャン(Scan)	対象とするシステムのポート、ＯＳ、サービス等をスキャンする。
	アクセス(Access)	対象とするシステムへのアクセス権を得る。
	昇格(Escalate)	アクセス権を昇格させる。
	搬出(Exfiltrate)	発見した情報をアクセスできる場所に搬出する。
	襲撃(Assault)	対象とするシステムを欺瞞、錯乱、拒否、機能低下、あるいは破壊する。
	継続(Sustain)	アクセスを継続できるようにする。

（１）偵　察(Recon)

サイバー攻撃を実施するためには、対象とするシステムの構成、環境等の情報が必要である。このプロセスはサイバーＩＳＲと共通であり、その手段については前節で示したとおりである。したがって、継続的に対象のサイバーＩＳＲを実施していれば、対象とするシステムの構成、環境等の情報はすでに入手している場合もある。

（２）スキャン(Scan)

次に、その対象とするシステムのポート、ＯＳ、サービス等のスキャンを実施する。このプロセスもＣＮＥと共通であり、その手段は前節で示したとおりである。スキャンにより対象とするシステムで用いられているＯＳやアプリケーションを特定することができれば、そのシステムにおいてアクセスを得るための脆弱性を調査することができる。

---

[39]Andress, J. and Winterfeld, S. (2013). Cyber Warfare, p.184

（３）アクセス(Access)

様々な手法で対象とするシステムへのアクセス権を得る。いわゆる不正アクセスを実施するプロセスである。アクセス権を得る手段としては、主としてこれまでに入手した情報を用いて発見した脆弱性を利用するのが一般的である。あるいは、情報システムのユーザ名の推測、パスワードのクラック、電子証明書の搾取、社会工学的な手法など他にも様々な手段がある。脆弱性を利用する不正なプログラムを配送する手段としては、マルウェアをメールに添付して送付する手法、リンクをクリックさせて不正なＷｅｂサイトに誘導する手法、ＵＳＢメディアにマルウェアを仕込んで挿入時に感染させる手法等様々である。これらの技術的な仕組みについては、「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」を参照されたい。

（４）昇　格(Escalation)

何らかの脆弱性を用いて得られた対象とするシステムのアクセス権は、一般ユーザの制限された権限であることが多い。一般ユーザの権限では、入手できる情報や実施できる事項にも様々な制約がある。したがって、攻撃者は次にその権限を昇格させ、アクセスできる範囲を拡大しようとする。具体的には、そのコンピュータのあらゆる情報にアクセス可能であらゆる事項が実施可能である管理者権限の入手を試みる。権限の昇格には、アクセスの場合と同様に脆弱性を利用するのが一般的である。

近年では、情報システムのアカウントやパスワード等のアクセス権に関する情報は、ドメイン・コントローラと呼ばれる特別なサーバで一元管理されていることが多い。したがって攻撃者は、一般ユーザの端末に侵入した後、ドメイン・コントローラの管理者権限の奪取を目的として権限の昇格を試みることが多い。ドメイン・コントローラの管理者権限を奪取した場合には、その管理下にあるすべてコンピュータへのアクセスが可能となる。したがって、ドメイン・コントローラの管理者権限が奪取された場合には、その管理下にある情報システムはすべて制圧されたと判断するべきであろう。

（５）搬　出(Exfiltrate)

権限の昇格によりアクセスできる範囲が拡大すると、目的とする情報、あるいは攻撃者やその依頼主にとって有益な情報を入手できる機会は増加する。攻撃者は、これらの情報を集約した後に圧縮して外部に搬出する。搬出の手段としては、一般的なファイル転送用のアプリケーション、メール、カスタマイズされた転送用のソフトウェア等が用いられる。これらの情報は、圧縮時にパスワードをかけて暗号化されることもしばしばであり、その場合にはどのような情報が含まれていたかが判明せず、流出した情報の中身が判明しない場合も珍しくない。

（６）襲　撃(Assault)

サイバー攻撃の最終的な目的を達成するためのプロセスであり、対象とするシステムを欺瞞、錯乱、拒否、機能低下あるいは破壊する。これらを実行するためには、これまでのプロセスで対象とするシステムの必要な権限を奪取しておく必要がある。

欺瞞は直接的な攻撃よりも巧妙な戦術である。例えば、通信サーバの権限を奪取することができれば、偽のメールやメッセージの送信、配送中のメールやメッセージの改ざん、あるいは単純にそれらを破棄することができる可能性がある。システムの錯乱はもう少し単純である。例えば、あるシステムにおいて必要な権限があれば、プロセスの停止、ファイルの移動や削除が可能である。特に定期的に実施される大規模なアップデート作業、財務処理、大規模な軍事作戦に必要なシステムであれば、実際のイベントにも大きなパニックを引き起こす可能性がある。サービス拒否は、インターネットにおいても頻繁に発生している。これらの攻撃は、主にＷｅｂサーバ、メールサーバ、あるいはその他の公開されているサービスを対象として実施されることが多い。しかしながら、同様の攻撃が電気、水道、交通、航空等の重要インフラの制御システムを対象として実施される可能性は否定できない。機能低下はシステムのパフォーマンスを低下させ、対応に必要な労力と時間を割くことを強要する。例えば、２０１０年に発見されたスタックスネットは、遠心分離機の機能を低下させる機能が組み込まれていたとされている。機能低下は、破壊等の直接的な攻撃よりも検知することが困難である。もっとも直接的な攻撃である破壊は、様々な範囲において実施することが可能である。論理的な観点では、データやアプリケーション、あるいはそのＯＳを消去することが可能である。例えば、２０１３年３月に韓国の放送局や銀行がサイバー攻撃を受けた事件[40]で使用されたマルウェアには、ハードディスクのＭＢＲ[41]と呼ばれる領域を初期化し、強制的に再起動させてＯＳが起動しない状態にする機能が組み込まれていたとされている。これが重要なデータやシステムで実施された場合、その影響ははかり知れないものとなる。物理的な観点ではその対象は限られてくるが、ハードウェアや制御システムを破壊するポテンシャルをひめている。例えば、２００７年３月に米国で実施された「オーロラ発電機テスト」では、サイバー攻撃により発電機を物理的に破壊することに成功したとされている。また、２０１５年１２月には、ロシアのサイバー攻撃によってウクライナの１４０万世帯で停電が発生したとされている。

---

[40]韓国においては「３・２０電算大乱」と呼ばれている。

[41]MBR (Master Boot Record) ハードディスクの起動時に読み込まれる領域

（７）継　続(Sustain)

一時的に対象とするシステムへのアクセス権を得た後、その権限を恒久的なものにして再度アクセスできるようにするプロセスである。インターネットに公開されたサーバが対象の場合には、侵入後にバックドアとなるサービスを起動して再度アクセスできるようにする。内部ネットワークの端末が対象の場合には、侵入後に端末に遠隔操作ウイルス[42]をインストールし、指令サーバ[43]を経由して遠隔操作をできるようにする。

以上が、サイバー攻撃の一連のプロセスである。

７　おわりに

本稿では、「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」に引き続き、サイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。第２節ではまずサイバー戦の定義と範囲について考察し、第３節では、近年焦点となっている包括的電子戦の概念を理解するために、サイバー戦と電子戦の違いについて、その重複部分を中心に考察した。第４節では伝統的なサイバー作戦であるＣＮＯと、拡大したサイバー作戦であるＣＯの関係について説明した。さらに、第５節ではＣＯの攻勢的な要素であるサイバーＩＳＲの特徴及び手段について説明し、第６節ではサイバー攻撃のプロセスについて説明した。

本稿は、専門家以外の方々のサイバー・セキュリティに関する素養の底上げを図り、サイバー・セキュリティに関する理解を促進することを目的として執筆した。冒頭で述べたとおり、陸・海・空の従来のドメインは、各種戦に体系化されて整理されており、各々の規定が定められている。オペレータはこれらの規定や各ドメインの特性を考慮して作戦を立案し、意思決定をすればよい。しかしながら、サイバー・ドメインには具体的な規定がないばかりか、体系的な整理も不十分である。そのため、組織内で認識を共有することは極めて困難であると言わざるを得ない。このような状況では、適切な意思決定はおろか、作戦の立案も容易ではない。サイバー作戦を立案するためには、少なくともそのドメインの特性やその概念に関する理解は不可欠である。今日、サイバー戦の範囲はインターネットのみならず、制御システムやネットワーク化されたビークルにまで急速に拡大しており、ＳＦ小説や映画で描かれたサイバー攻撃の脅威が現実のものとなりつつある。また、シリアの防空システム、スタックスネット、米国の無人機等の事例を考慮すると、サイバー・ドメインは単独で考慮すべき対象ではなく、すでに各種戦や平時の活動とも密接に関係していると

---

[42]RAT (Remote Access Trojan or Remote Administration Tool)
[43]C&C or C2 (Command and Control) Server

言える。

　したがって、サイバースペースの特性は少数の専門家だけが理解していれば良い問題ではなく、組織全体で素養として理解していなければならない基本的な事項であると考えられる。本稿により、サイバースペースの特性を理解するために必要なサイバー戦の概念と作戦について、専門家以外の方々に少しでもご理解いただければ幸いである。