第２部
「サイバー」

執筆担当

第１章「サイバー総論」　２等空佐　井上 貴雄
第２章「サイバーの概念」　２等空佐　井上 貴雄
第３章「サイバー空間に係る技術」　２等空佐　井上 貴雄
第４章「米軍のサイバー空間作戦」　３等空佐　土持 太郎
第５章「サイバー空間での対応に関係する国内法及び国際法」
２等空佐　鳥居 真由子

(Intentionally Blank)

目次

ア　国際法の適用可能性
イ　サイバー攻撃に対する自衛権行使の可能性
ウ　日米安全保障条約第５条との関係
エ　『タリン・マニュアル』に対する評価

(Intentionally Blank)

１　サイバー総論

ほぼ全ての兵器システムがネットワーク化されている現代の戦争、紛争、国家間競争において軍事組織が自らの任務を遂行するためには、サイバー領域に係る能力の獲得と継続的な向上が不可欠となっている。本書は、サイバー領域における脅威とその対策について航空自衛隊の全ての隊員が保持すべき基礎的な知見を提供するものである。

本章では、初めに軍事的な観点でインパクトを与えたサイバー攻撃事例を紹介し、軍事組織にとって、サイバー攻撃が脅威になっていることを示す。次に、サイバー能力の主体であるコンピュータ及びネットワークが発展してきた歴史と、軍事組織によるサイバー能力への依存度の高まりについて説明する。さらに、サイバー領域における脅威とその対策について説明し、第２章以降に係る基礎的知識の必要性について述べる。

（１）軍事的な観点でインパクトを与えたサイバー攻撃事例

ここでは、軍事的な観点でインパクトを与えたサイバー攻撃事例を 3 つ挙げ、これらの事例がどのような教訓があるのかを説明する。

ア　イスラエルによるシリア空爆に伴うサイバー攻撃

2007 年 9 月、イスラエル空軍の 4 機の F15 と 4 機の F16 がシリアの首都ダマスカス北東約 450 キロのデリゾール地方で「完成間近」の原子炉を空爆し破壊した[1]。当時の報道によれば、シリア軍の防空システムはイスラエルの攻撃を探知できなかったと言われている。この攻撃に際してイスラエル軍が利用した技術は、英 BAE システムズ社が開発した航空ネットワーク攻撃システム「Suter」と同等のものであったとされている。この技術を利用すれば、無人機に搭載した Suter から電磁波を利用して、敵国の通信ネットワークに侵入して敵の防空システムの表示を見ることができるほか、これを操作して航空機のシンボルを消して画面に表示させないことができるという[2]。

Suter によるサイバー攻撃が事実ならば、航空作戦以前に、サイバー戦と電子戦が融合したノンキネティックな作戦が行われた事例として見る

[1] 渡辺丘「イスラエル、シリアの原子炉空爆を認める 2007 年に」朝日新聞デジタル、2018 年 3 月 21 日、https://www.asahi.com/articles/ASL3P52S5L3PUHBI016.html.
[2] シャロン・ワインバーバー「イスラエルによるシリア空爆：防空システムをハッキングか」WIRED.jp、2007 年 10 月 10 日。

ことができる。他にも防空システムに対するサイバー攻撃として、航空ネットワーク攻撃に限らず、インサイダー（内部犯行者）によるマルウェアの埋め込みやサプライチェーン攻撃などが考えられる。これらは、ネットワークが外部と繋がっていなくとも決して安全ではないことを意味する。そこで、次に、インサイダーによって引き起こされた格好の事例を紹介する。

イ　米国及びイスラエルの共同によるサイバー攻撃：スタックスネット

2010 年 6 月、イラン政府高官は、イランのナタンツに所在する原子力関連施設がスタックスネットというコンピュータ・ウイルスに感染したことを認めた。この悪性のウイルスは、ウラン濃縮施設の中の特定の機器を探して潜伏するように設計されていた。このウラン濃縮施設におけるガス遠心分離機のコンピュータプログラムに影響を与え、制御不能にして破壊するものであった。ガス遠心分離機は高濃度のウラン製造に使われる可能性があると考えられていた。また、このウイルスはその足跡を消すことによって、ウラン濃縮施設のオペレーターに「機器は正常に動いている」と勘違いさせる機能を持っていた。そのため、この破壊は 1 年以上も気づかれることはなかった。この事案により、イランの核開発が数年間遅れたと考えられている[3]。

この事案は、その後「オリンピック・ゲームズ」という名称の米国とイスラエルの共同作戦であったことが報道された[4]。ウラン濃縮施設にウイルスを感染させるに当たり、現地スパイを雇い情報収集し、ガス遠心分離機を攻撃するために特注のウイルスを作成し、USB メモリを介して感染させたと考えられている[5]。

ガス遠心分離機はネットワークが外部と繋がっていなかったが、緻密な情報収集とスパイを活用することによって、サイバー攻撃を成功させた。これはサイバー攻撃とインテリジェンスが高度に融合した事例である。そこで、次に、情報作戦の一部としてサイバー攻撃が行われた事例を紹介する。

ウ　ウクライナ紛争におけるサイバー攻撃

---

[3] エリノア・スローン「現代の軍事戦略入門　増補新版」、芙蓉書房出版、2019 年、308 頁。

[4] David E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” The New York Times, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html? pagewanted=all&r=0.

[5] 「核施設を狙ったサイバー攻撃『Stuxnet』の全貌」WIRED.jp、https://wired.jp/2012/06/04/confirmed-us-israel-created-stuxnet-lost-control-of-it/

2014年、ウクライナでクリミア半島の帰属を巡りロシアとの間で政治的危機が生起した。クリミア地域は共和国としてウクライナから分離独立し、親ロシア国家として誕生した。このクリミア独立を受け、ロシア語を使う人々が多いウクライナ東部地域でも、分離独立運動が始まった。やがて、運動は武力を伴う内乱に発展したが、ウクライナ政府軍の活動により分離独立派は制圧される。しかし、ロシアによる介入があり形勢が逆転したが、その後、ウクライナ政府と分離独立派の間で停戦が成立した。この武力紛争中、ハッカーたちによるサイバー戦が行われていた。彼らは、お互いに自分たちの政治的立場を有利にするために、戦闘行動に連携し、サイバー技術を駆使して活動を行った。ウクライナ側のハッカーは、公共の監視カメラを乗っ取り、ロシア軍の動きなどを観察した。さらに、ハッキングにより得られた情報を、実際の戦闘における射撃目標特定のために提供した。また、ネットワークプリンターを乗っ取り、プロパガンダを印刷配布することもしたという。一方、親ロシアの分離独立派は、ウクライナの内務大臣の通信をハッキングして、それを公開した。また、大型野外映像ディスプレイを乗っ取って、彼らのプロパガンダを掲示した。さらに、ウクライナ国会議員選挙に先立ち、電子投票システムの妨害や、ウクライナ国防省のデータ窃取や破棄等の妨害工作を行ったとされている[6]。

この事例におけるサイバー攻撃は、内外の世論が自分たちに味方するように訴えようとするプロパガンダ活動が多く、サイバー攻撃が情報作戦の一部として利用されることを示している。サイバーは、戦略的に情報発信するツールとして重要であるとともに、サイバー能力を利用した情報操作により、人の認知が誘導され、軍事組織の活動に混乱を生じさせるツールにもなり得るため、敵のフェイクニュースに惑わされないような対策が必要となる場合も考えられる。

（２）サイバーの発展に係る歴史

サイバー能力の主体であるコンピュータ及びネットワークの歴史について説明し、軍事組織がサイバー能力への依存度を高めている実態について述べる。

ア　コンピュータ及びネットワークの歴史

コンピュータは1930年代にアラン・チューリングがコンピュータの全

[6] 伊藤寛『サイバー戦争論　ナショナルセキュリティの現在』原書房、2016年、136-142頁。

般概念を提唱し、1945 年にフォン・ノイマンが現在使用されている入出力装置を伴ったコンピュータの基本概念を提唱したとされている。

この頃のコンピュータはコンピュータ同士が接続されていない単独での動作（いわゆるスタンドアローン）であった。これが現在のようなコンピュータ同士が接続される状況になったのは、1969 年に米国国防省高等研究計画局（ARPA：Advanced Research Projects Agency）が軍事目的で開始した ARPANET であり、これが現在のインターネットの始まりとも言える[7]。このシステムは世界初のパケット通信によるネットワークであった。このシステムを構築した目的は、米国が他国からの核攻撃に備えて指揮系統（UNIX コンピュータ）を分散させることであったと言われている[8]。当時の技術は UNIX コンピュータ同士を TCP/IP で相互接続しただけであったが、これが発展し現在のネットワークの基本となった。

イ　軍事組織によるサイバー能力への依存度の高まり

現代の軍事活動はサイバー能力を利用した C4ISR[9]の機能に依拠していることから、軍事組織はコンピュータ、ネットワーク及びセンシングを構成要素とするサイバー能力に大きく依存しており、サイバー能力なくして軍事活動は成り立たない。さらに、コンピュータの処理速度やネットワークの接続性が向上したことにより、センサーからシュータまで戦力のネットワーク化が進み、指揮統制能力、情報収集能力及び精密攻撃能力等を向上させている。一方、軍事組織によるサイバー能力への依存度が高まるにつれ、サイバー能力が喪失もしくは低下した場合の影響が極めて大きくなっている。

（３）サイバー領域における脅威

軍事組織のあらゆる活動がサイバー能力に依存しているということは、裏を返せば、サイバー能力の喪失や低下並びにサイバー能力を利用した情報操作は、軍事組織としての任務遂行を阻害する要因となり得ることを意味する。ここでは、軍事組織の任務遂行を阻害する要因となり得るサイバー領域における脅威について説明する。

---

[7] 総務省「通信白書」1999 年、
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h11/html/B1Z20000.htm.

[8] 核攻撃の指揮統制機能の拡散を目的として開発されたと言われているが、インターネット協会は否定している。ARPANET が軍事用に開発され、それが民間に転用されたという設計目的については現在多くの議論があるが、核兵器の指揮統制システムに ARPANET の技術が転用されている。

[9] C4ISR とは、指揮（Command）、統制（Control）、通信（Communication）、コンピュータ（Computer）、情報（Intelligence）、監視（Surveillance）、偵察（Reconnaissance）を指す。

ア　サイバー領域における脅威の分類

軍事組織の任務遂行を阻害するサイバー領域における脅威は、物理的な脅威と論理的な脅威の二つに大きく分けられる。

物理的な脅威とは、コンピュータ及びネットワーク等の物理的な機器に対する脅威のことであり、戦闘、テロ、災害及び事故などにより、サイバーインフラとそれを維持するために必要な電源・空調設備が受ける物理的な障害がある。サイバーインフラとは、サイバー能力を提供するインフラのことであり、コンピュータ及びネットワークのハードウェアやケーブル等を指す。これらが物理的に被害を受ければ、サイバー能力が喪失もしくは低下し、軍事組織の任務遂行に支障を来たす。

論理的な脅威とは、コンピュータ及びネットワーク等内のデータ及びプログラムに対する脅威のことであり、サイバー攻撃や人為的な誤操作等により生起するデータの障害及び流出、並びに人の認知に影響を与える情報操作がある。

サイバー能力を構成するコンピュータ及びネットワークには、設計及びプログラム上に多数の脆弱性が存在する。この脆弱性を利用して、不正アクセス、情報の窃取や改ざん、コンピュータシステムの作動停止や誤動作等を生起させる手段が、サイバー攻撃である。また、データの障害及び流出をさせる要因の中には、サイバー攻撃だけでなく、人的な誤操作も含まれる。

さらに、サイバー能力は、戦略的及び作戦的に情報発信するツールとしても利用することも可能であり、悪意のある攻撃者がデータ操作を行うことにより人の認知に対して影響を及ぼす場合がある。

イ　サイバー攻撃の変遷と特性

近年、サイバー攻撃は高度化・巧妙化・複雑化している。そして、その技術の進化は極めて速く、サイバー攻撃への対応は極めて困難となっている。ここでは、サイバー攻撃の変遷とその特性について説明する。

（ア）サイバー攻撃の変遷

2000 年代までは、個人によるサイバー攻撃が主体で、攻撃者は自身の能力を誇示するための愉快犯的なものが多かった。しかし、2000 年代後半からは、個人を対象としたものだけでなく、組織、社会インフラ、国家を対象としたサイバー攻撃が頻繁に行われるようになった。軍事組織に対するサイバー攻撃も例外なく頻繁に行われており、軍事アセ

ットだけを対象にした標的型のサイバー攻撃も現実に行われる可能性が高まっている。サイバー攻撃の手法は、日を追うごとに高度化・巧妙化・複雑化している。

これまでのサイバー攻撃の事例は表 1-1 のとおり。

表 1-1　サイバー攻撃の事例[10] [11]

年	攻撃者 (推定を含む。)	攻撃対象	概要
2008	中国	米国	ロッキード・マーティン社のネットワークに侵入し、F35 関連計画の情報を窃取
2009	中国	米国	グーグル社のシステム内に暗号化したマルウェアを埋め込み、米国在住の中国人活動家の動向、米国の主要な政策決定者の通信等の機密情報を窃取、同時期にその他約 35 社にハッキング
2012	中国	カナダ	石油・ガスのパイプラインに関するソフトの開発会社であるテルベントという会社のシステムに侵入し、プロジェクトのデータを窃取
2014	中国	米国	米連邦人事管理局のシステムに侵入し、約 2,200 万人の個人情報を窃取
1999	ロシア	米国	ロシアのハッカーが複数のシステムに 2 年前から潜伏、数千ページの文書を窃取（ムーンライト・メイズと呼称）
2008	ロシア	米国	国防総省の機密ネットワーク（SIPRNet）に侵入、データ窃取
2014	ロシア	ウクライナ	選挙システムに侵入し、ウクライナ大統領選関連のデータの消去、改ざん等を実施
2014	ロシア	米国	ソーシャル・メディア上で偽アカウントを作成してフェイクニュースを流布し、米国世論の分断を企図
2015	ロシア	ウクライナ	電力インフラに対する攻撃による停電

[10] David E. Sanger, *THE PERFECT WEAPON: war, sabotage, and fear in the cyber age*, Scribe Publications, June 21, 2018.
[11] 株式会社 ICS 研究所「サイバー攻撃の事例集」、2020 年 1 月 27 日、https://www.ics-lab.com/pdf/journal/28/journal-28-20200127.pdf.

2015	ロシア	米国	米国 DNC（民主党全国委員会）のネットワークに侵入したのを足掛かりに、米大統領選ヒラリー・クリントン候補陣営のデータ窃取、選挙への干渉等を実施
2017	ロシア	ウクライナ	マルウェアによる攻撃を実施し、ウクライナ国内のサイバーインフラに損害（国内の 30%のコンピュータが機能停止）
2013	北朝鮮	韓国	銀行 3 社と放送局 2 社のコンピュータ・ネットワークに対してマルウェアを送り込み、企業活動を阻害（ダーク・ソウルと呼称）
2014	北朝鮮	米国	北朝鮮をパロディ化した映画の公開に対するソニー・ピクチャーズ・エンタテインメントへの抗議が聞き入れられなかったため、フィッシング・メールを使用して同社のシステムに侵入し、データの消去、窃取、金銭の要求等を実施
2012	イラン	サウジアラビア	ウイルスをサウジアラコム社のシステム内に散布（PC3,000 台とサーバ約 1,000 台）し、ファイル等を消去、当該企業は本社と事業者のネットワークを隔離
2014	イラン	米国	ラスベガスのカジノのコンピュータシステムを停止させ、当該カジノのオーナーの政治的発言を撤回するよう脅迫
2010	米国・ イスラエル	イラン	「スタックスネット」と呼ばれるマルウェアにより、イランの原子力関連施設に所在する遠心分離機約 1,000 基を破壊
2013	米国	中国	中国のサイバー部隊「61398 部隊」に所属するハッカーを監視等するため、当該部隊の端末に侵入し、カメラを操作
2005	不明	米国	米国において、外部から持ち込まれて接続されたノート PC により、独ダイムラー社の工場が不正プログラムによって操業停止になり、1400 万ドルの損害
2008	不明	トルコ	トルコにおいて、石油パイプラインに設置されている監視カメラの通信ソフトに関する脆弱性を利用して内部ネットワークに侵入、不正に動作制御系にアクセスし、管内

			の圧力を異常に高めて石油パイプラインを爆破
2011	不明	日本	日本の半導体メーカで USB メモリを介して品質検査を行う検査装置へマルウェアが感染、多数の不具合が発生し、最終的に生産ラインが停止
2012	不明	サウジアラビア	サウジアラビアの石油会社の PC がマルウェアに感染し、ネットワークに接続されていた PC のデータが削除
2014	不明	ドイツ	ドイツの製鉄所においてマルウェア（攻撃者の電子メールに添付）により、内部のシステムのコントロールを行うユーザ ID とパスワードが窃取され、溶鉱炉を不正操作され被害発生
2017	不明	米国	米国原子力運営会社の情報システム系ネットワークがハッキングを受けた。制御系システムに侵入された形跡はなく、調査目的と推定

（イ）サイバー攻撃の特性[12]

サイバー攻撃は、次の特性を持っており、その脅威度は極めて高い。また、サイバーに係る国際法は第 5 章で述べるとおり未成熟であるため、サイバー攻撃の抑止を更に困難にしている。

a　多様性

サイバー攻撃に必要な技術は、安価に入手でき使用が容易であることから、国家のみならず、国家以外の組織や個人といった多様なアクターがサイバー攻撃の主体となりうる。

近年では、サイバー傭兵（サイバー攻撃代行業）やハクティビスト（行動主義的なハッカー集団）等の組織が国家の要請等（注：国家としての関与は否定される傾向にある。）によりサイバー攻撃を行う場合がある。

b　匿名性

サイバー攻撃の実行者は、自らを隠蔽・偽装することが容易であり、痕跡を残すことなく攻撃を実行することが可能である。一方、被害者が真の攻撃者を特定することは非常に困難である。

c　隠密性

[12] 防衛省「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」、2012 年 9 月。

サイバー攻撃手法には隠密性の高いものがあるため、防御側が攻撃を察知し難い場合や、被害を認識することが困難な場合が多い。

d　攻撃側の優位性

攻撃側は、サイバー攻撃の実施時期、対象、手法を自由に選択することが可能である。一方、防御側は、守るべきコンピュータ及びネットワークの脆弱性を完全に排除することが困難であるため、サイバー空間においては、攻撃側が防御側に対して圧倒的な優位にある。

e　抑止の困難性

サイバー攻撃を抑止することは、容易ではない。「懲罰的抑止[13]」として、攻撃者に対して「サイバー攻撃を行えば、同等或いはそれ以上の被害をもたらすような報復を行う」意思を明示したとしても、防御側が報復手段を有していない場合には抑止効果は働きにくい。また、攻撃源の特定が困難であることから、報復の警告は攻撃者にとって説得力の乏しいものとなる。「拒否的抑止[14]」のためには、「サイバー攻撃を行っても効果が得られない」という心証を攻撃者に与える必要があるが、サイバー攻撃を完全に思いとどまらせる高いレベルにまで防御水準を高めることは困難である。

（４）サイバー領域における脅威の対策

軍事組織にとって、サイバー領域における脅威の対策は、任務保証としての大きな意義がある。サイバーは、様々な能力の基盤となっているため、陸・海・空・宇宙といったあらゆる活動領域で活用されている。このため、サイバーの部分だけを考えても十分な備えにはならず、他領域とのつながりを含めて全体を俯瞰し、「何のためのサイバーなのか」を頭に置いておかなければ、「何をすべきか」が見えてこない。この特性を踏まえた上で、次のとおりサイバー領域における脅威に対応する必要がある。

物理的な脅威に対しては、関連設備の入退出管理やサイバーインフラ等の物理的防御が不可欠であり、攻撃を受けにくくする欺瞞といった手段や、代替、再構成及び多重化などの抗たん化施策も重要である。この対策にはサ

---

13 懲罰的抑止とは、耐えがたい打撃を与える威嚇に基づき、敵のコスト計算に働きかけて攻撃を断念させることをいう。

14 拒否的抑止とは、特定の攻撃的行動を物理的に阻止する能力に基づき、敵の目標達成可能性に関する計算に働きかけて攻撃を断念させることをいう。

イバー領域と他領域の活動との連携が必要となる。

論理的な脅威であるサイバー攻撃に対しては、予防、検知、対処及び復旧といった各フェーズの対策が必要となる。サイバー空間内の状況把握を常続的に行うとともに、サイバー攻撃に関する兆候を察知したならば即時に対応することが必要となる。特にサイバー攻撃は、技術の進化が速いため、サイバー攻撃に関する脅威情報の早期入手が極めて重要である。サイバー攻撃が行われる前に、能動的に対処していくことが肝要である。

また、サイバー攻撃によるものなのか、物理的な障害によるものなのかを判断するためには、整備活動との連携が必要である。さらに、サプライチェーンリスク（ハードウェアに内在するプログラム上の問題）への対策は、補給活動との連携も求められる。

人の認知に悪影響を与える情報操作については、情報活動や広報活動と連携して、フェイクニュース等による影響の分析をした上での対策が必要となる。

以上のように、サイバー領域における脅威に対抗し、軍事組織の任務を保証するためには、サイバー領域とあらゆる活動が連携をしなければ、総合的かつ最適な対策を講ずることはできないのである。

（５）まとめ

サイバー領域における戦いは、「見えない戦場」での戦いであり、過去のどのような「戦い」とも異なる。サイバー領域における兵器はサイバー技術である。そして、サイバー攻撃は、目に見えず、地理的、時間的制約がなく、誰がどこから攻撃しているのかすぐには分からず、被害が不特定多数に及ぶ場合がある。仮に攻撃者が特定できても、サイバー領域における報復の方法はない。物理的兵器であれば、ミサイル発射地が直ちに特定され、攻撃された数十分後には反撃できる可能性があるが、サイバー攻撃の場合は、サイバー技術の分析から「攻撃者」の推定ができても、相手は攻撃を認める可能性が極めて低く、反撃も難しい。つまり、人類の戦争の歴史で初めて「見えない戦場」の中での戦いを強いられているのである。また、サイバー攻撃の最大の特徴は、（物理的兵器において）軍事的に劣勢にある国でも優位に立ち得ることである。サイバーを知らなければ、サイバー領域の戦いだけでなく、航空領域、そして宇宙領域においても戦いを制することはできない。したがって、サイバー領域における戦いは航空自衛隊にとって喫緊の課題であり、航空自衛隊の全ての隊員がサイバー攻撃の脅威や威力を知り、いかに

対処すべきかを考えなければならないのである。そこで第２章以降、全隊員が有すべき基礎知識を説明していく。

第２章では、サイバー領域の本質的事項ついて説明する。サイバー分野で頻繁に使用される、空間、領域、能力等の用語と関係について説明する。また、サイバー領域における戦いの本質と特徴について説明する。

第３章では、サイバー空間に係る技術について、コンピュータ及びネットワークの技術並びにサイバー攻撃と防御に関する技術を中心に説明する。

第４章では、米軍におけるサイバー空間作戦について、米軍の統合ドクトリン「Cyberspace Operations」の内容を紹介しながら説明する。

第５章では、サイバー空間での活動に関連する国内法及び国際法について概略を説明する。

2　サイバー領域の本質的事項

本章では、サイバー領域の本質的事項について説明する。サイバー分野で頻繁に使用される、空間、領域、能力等の用語と関係について説明する。また、サイバー領域における戦いの本質と特徴について説明する。

（1）サイバーの概念

サイバーについては様々用語があるが、ここでは、サイバーに関する概念を表現している主な用語について説明する。なお、用語の定義に当たっては、米軍の統合ドクトリン（Joint Publication 3-12 Cyberspace Operations）（以下「米軍ドクトリン」という。）や辞書等を参考にしている。

サイバーに関する用語の定義は、表 2-1 のとおり。

表 2-1　サイバーに関する用語の定義

用語	定義
サイバー	人もしくは組織を情報システム及び機械システムと一体的に運用する術（art）又は運用されている状態
サイバー空間	人の意思が反映された電気信号情報をやり取りするためのコンピュータ及びネットワークにより創出された仮想的な空間
サイバー領域	サイバー空間に関する３つの要素（物理要素、論理要素、人的要素）を総合したもので、サイバー空間及び関係する物理領域で構成されたもの
サイバー能力	サイバー領域に係る能力のことで、ネットワーク、コンピュータ及びセンシングといった技術的要素を一体的に運用する能力

ア　サイバー（Cyber）

サイバーとは、一般的には、「他の名詞の上に付いて、コンピュータやネットワークに関する意を表わす。」とあり、通常「サイバービジネス」

や「サイバーテロ」の例のように接頭語として用いられる[15]。

「サイバー」の語源は、1947 年に米国の数学者のノーバート・ウィーナーが提唱したサイバネティクス（cybernetics という、生物と機械における通信、制御、情報処理の問題を統一的に取り扱う総合科学の学問分野）と言われている[16]。その後、1984 年にウィリアム・ギブソンが出版した小説、『ニューロマンサー』内で用いられた「サイバースペース（電脳空間）」という造語が世間に広く知られるようになったことにより、「サイバー」は「コンピュータやネットワークに関すること」という意味で使われるようになり現在に至る[17]。

一方、日本では、サイバーは「電脳」と訳され[18]、生命体と自動制御系技術の融合体である「サイボーグ（Cybernetic　Organism）」のように生物と機械装置が電気信号情報[19]をやりとりすることで一体的に運用されるシステムを表す接頭語として用いられるようになった[20]。

以上のことから、「サイバー」とは、人もしくは組織を情報システム及び機械システムと一体的に運用する術（art）又は運用されている状態を表すと言える。また、サイバーを構成する３つの要素は、①:人もしくは組織、②:情報システム及び機械システム並びに、③:①と②の要素が一体的に運用されていること、となる。

イ　サイバー空間（Cyberspace）

サイバー空間とは、一般的には、「コンピュータ・ネットワーク上の仮想的な空間[21]」と定義されている。コンピュータは、人の意思等の情報をキーボード、マイク、カメラ、ディスプレイなどにより、電気信号情報に変換して処理するものを指し、その役割は計算にとどまらない。また、ネットワークは、通信方式（デジタル／アナログ）及び通信手段（無線／有線）を問わず、電気信号情報を伝達する機能の全てを指す。

これらを踏まえ、本書では、「サイバー空間」を「人の意思が反映された電気信号情報をやり取りするためのコンピュータ及びネットワークに

---

15 『精選版　日本国語大辞典』第二版、小学館の「サイバー（cyber）」による。
16 『世界大百科事典第２版』、平凡社の「サイバネティクス（cybernetics）」による。
17 『日本大百科全書』、小学館の「サイバースペース（cyberspace）」による。
18 『大辞林第三版』、三省堂の「サイバー（cyber）」による。
19 信号は電気だけではなく、磁気や光なども含む。このため、電磁等信号情報とすることが妥当であるが、本書では理解を容易にするため電気信号情報としている。
20 『日本大百科全書』、小学館の「サイボーグの由来」による。
21 『デジタル大辞泉』、小学館の「サイバースペース（cyberspace）」による。

より創出された仮想的な空間」と定義する。

ウ　サイバー領域（Cyber domain）

本書では、サイバー領域を、サイバー空間に関する３つの要素（物理要素、論理要素、人的要素）を総合したものとし、サイバー空間及び関係する物理領域で構成されたものとする。サイバー領域の関係図は、図 2-1 のとおり。

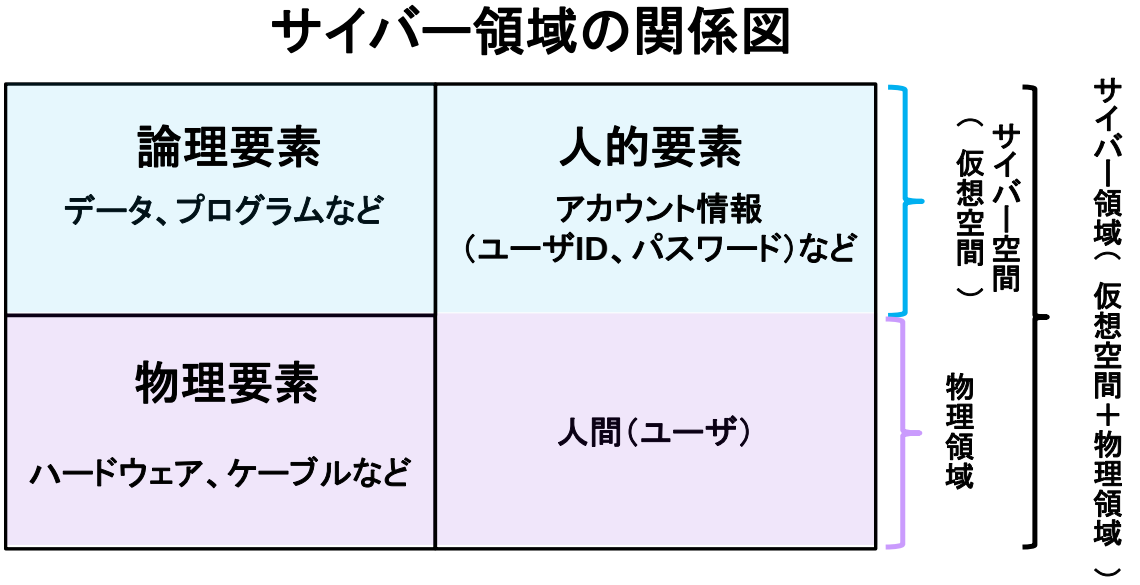

図 2-1　サイバー領域の関係図

エ　サイバー能力（Cyber capability）

本書では、サイバー能力を、「サイバー領域に係る能力のことで、ネットワーク、コンピュータ及びセンシングといった技術的要素を一体的に運用する能力」とする。各技術的要素の詳細は次のとおり。

（ア）ネットワーク

命令、情報、各種データ等を伝送、交換し伝達する技術的要素

（イ）コンピュータ

各種情報を蓄積し、利用価値の高い情報等に処理し、表示等を行う技術的要素

（ウ）センシング

主に電磁波を利用した各種センサー等により、各種情報（位置情報や航跡情報等）を収集する技術的要素

オ　サイバー能力と他分野との関係

現代においてサイバー能力は軍事的機能の土台となる役割を果たす。その中でも、サイバー能力が重要な分野は次のとおり。

（ア）指揮統制（Command and Control（C2））

サイバー能力により、指揮官の指揮統制に必要な情報を迅速かつ適時に提供することが可能である。

情報システムの発達により、現代の軍事組織においては、迅速確実な指揮統制活動のため、本質的にネットワークに依存する性質を有する。また、NCW(Network Centric Warfare:ネットワーク中心の戦い)が提唱され、その方向性に拍車がかかり、現在においては情報システムなしに軍事組織の指揮統制をすることは極めて困難である。

（イ）情報（Intelligence、Information）

情報とサイバー能力の関係は非常に強い。世界各国の軍事サイバー組織の発達の過程を見ると、インテリジェンス組織に必要な情報収集ツールとして攻撃に関するサイバー能力が重視された。また、このような攻撃を防ぐために防御に関するサイバー能力が整備されてきている。

（ウ）他の作戦領域（陸・海・空・宇宙）

指揮統制でも述べたとおり、陸・海・空・宇宙の作戦の指揮統制を直接的に支えているものは、情報システムを効果的に運用するためのサイバー能力である。さらに、昨今の各種装備品等はネットワークを介して連接され、自動かつ遠隔制御による運用が常態化している。そのため、いかなる軍事組織のアセットであってもサイバーに密接な関係を有しており、今後さらにこの傾向は強まるものと考えられる。

（エ）電磁波

電磁波は、情報通信インフラとともにサイバー能力を構成する要素であり、電気信号情報を伝達するための一手段としてサイバー能力に欠かすことのできないものである。また、サイバー空間作戦と電磁波作戦を融合させた作戦体系を理論化している国家も存在する[22]ことから、サイバー空間作戦と電磁波作戦が一体となった攻防にも留意する必要がある。

---

[22] 中国軍の運用構想の一つに「網電一体戦」がある。サイバー空間の攻撃手段と従来の物理的な電子戦の能力を一体として運用する概念である。

（２）サイバー領域における戦いの本質と特徴

ここでは、サイバー領域における戦いの本質と特徴について説明する。

ア　サイバー領域における戦いの本質

「サイバー領域における戦い」は、「航空領域における戦い」と同様の概念では、適切に理解することができない。サイバー領域と航空領域では、戦いの様相が全く異なる。そもそもサイバー領域は仮想空間を含むので、物理領域における戦いの原理が適用できないことの方が多い。また、戦闘行為そのものも全く異なり、これを支える技術も異なり、環境も全く異なる。したがって、航空領域の戦いの概念でサイバー領域の戦いを考えてはならない。航空作戦のために必要なサイバー領域における活動は存在するが、それだけに焦点を当てると、サイバー領域における戦いの本質を見落とすことになる。すなわち、「航空作戦を成立させるためのサイバー領域の戦い」もあるが、それとは別に「サイバー領域を制するための戦い」もあり得るということである。サイバー領域の戦いは、航空領域における戦いの付帯的・支援的な活動に留まるものではないということである。

イ　サイバー領域における戦いの特徴

サイバー領域における戦いの特徴は、以下のとおり様々な特徴があり、それらは相互に関連しあっている。サイバー領域における戦いは攻撃側が圧倒的有利なため、抑止が極めて困難である。攻撃を仕掛けてきた相手方を突き止め反撃する対策に重点を置くべきではなく、如何に任務保証をすべきかに重点を置くべきである。

（ア）主体の多様性

サイバー空間内における主体は国家だけでなく、個人や組織といった様々な主体が活動するため、サイバー領域においては国家対国家という構図が当てはまらないケースが多い。

（イ）攻撃主体の判別（attribution）が困難

サイバー空間を利用するに当たり、身元を明らかにする必要がないため、基本的に攻撃の主体が誰なのかわからない。隠蔽・偽装をされると更にわからなくなり、攻撃を受けた側が攻撃者の身元を特定しようとしても、確実にはわからないことの方が圧倒的に多い。

（ウ）効果の確認及び予測が困難

例えば、航空機から爆弾を投下すれば、攻撃によって何が変わったのかを観測することができる。しかし、サイバー領域においては、電子戦

のごとく、相手に効いているのかどうかを確認することが困難である。仮に、ある時点の脆弱性情報を元にサイバー攻撃を組み立てたとしても、相手方がその脆弱性を修正してしまっていると、効果がなくなる。また、あるサイバー攻撃が副次的な作用を及ぼすのかを完全に予測することは困難である。

（エ）技術や戦術の急速な進展

サイバー攻撃・防御の技術、戦術及び原則などは、急速に変遷していく。技術の発展が日進月歩であることに加え、これを利用する方法（戦術）も急速にバリエーションが拡大してきている。例えば、サイバー領域と別の領域の要素を組み合わせることにより、従来存在しなかった攻撃手法が次々に生み出される状況になっている。

（オ）攻撃側の優位性

サイバー攻撃に対しては、いわゆる策源地攻撃によって防御の負担を軽減することは困難である。サイバー攻撃に係る拠点を特定すること自体が困難であり、仮に、当該拠点を特定し、サイバー攻撃機能を失わせることができても、直ちに全く別の拠点からサイバー攻撃を受ける可能性がある。

（カ）ネットワークの内部に潜む脅威が大

サイバー攻撃は、防御を固めているインターネット経由よりも、防御を固めていない我のネットワーク内から犯行される、内部犯行者やサプライチェーン攻撃の方が脅威である。また、ＳＮＳによる個人情報の収集やフェイクニュース等の脅威が高い。

軍事組織で警戒すべきは、内部犯行者や、他の手段との組み合わせによる攻撃であり、長期的で地味な取組（サプライチェーン攻撃等）である。

（キ）抑止の困難性

サイバー攻撃と防御の非対称性により、抑止が効かない。懲罰的抑止を行うためには、反撃できる必要がある。しかし、反撃するためには攻撃元を特定する必要があり、上手くいかない可能性が高いため、抑止は機能しないと考えられている。また、拒否的抑止のためには、防御能力を見せつける必要があるが、見せつけた途端に相手方も対応するため、結果的に拒否的抑止にはならない。そして、輪をかけて国際的なルールも未成熟であることからサイバー攻撃を抑止することは困難である。

（ク）サイバーには多様な側面が混在

サイバーには、いわゆる「サイバー防衛」のみならず、国際・国内の法執行、情報作戦、国家安全保障技術戦略、インテリジェンスなど、多様な側面が存在する。サイバーは、様々な能力の基盤となっている。このため、サイバーの部分だけを考えても十分な備えにはならず、「何のためのサイバーなのか」により、「何をすべきかが絶えず変わる」。これは、任務保証の基本的な考え方となる。

（ケ）常に他領域と相関

仮想空間内のことだけを考えていては、サイバー領域における戦いには太刀打ちできない。サイバー空間内で閉じる活動はほとんどなく、他領域における活動（例えば、インテリジェンス活動や整備活動）と連携して行われる。また、物理領域におけるアセット（人、サイバーインフラ、電源）に依存するため、物理的防御も重要である。

（コ）戦いの場が「平場」

サイバー領域における戦いの場は、「平場」であり、サイバー攻撃は平時から行われる。この平場では、民間力も無関係ではなく、如何に軍民連携できるかが大きな鍵となる。さらに、攻撃者は国際法的な違法性をいかようにも回避できるため、正当性を主張できる理論武装が必要となる。

３　サイバー空間に係る技術

本章では、サイバー空間に係る技術の中で、コンピュータ及びネットワーク上の脆弱性の存在とそれを巡る攻防の技術について述べる。

（１）コンピュータ及びネットワーク上の脆弱性

ア　コンピュータ上の脆弱性

（ア）コンピュータ構造とその問題

現在のコンピュータの基礎的な構造を作った人物は、米国のフォン・ノイマンと言われている[23]。コンピュータの主な構成要素は、入出力部、計算部、そして記憶部である。記憶部にはプログラムやデータが記録され格納される。コンピュータの構造図は下図のとおり。

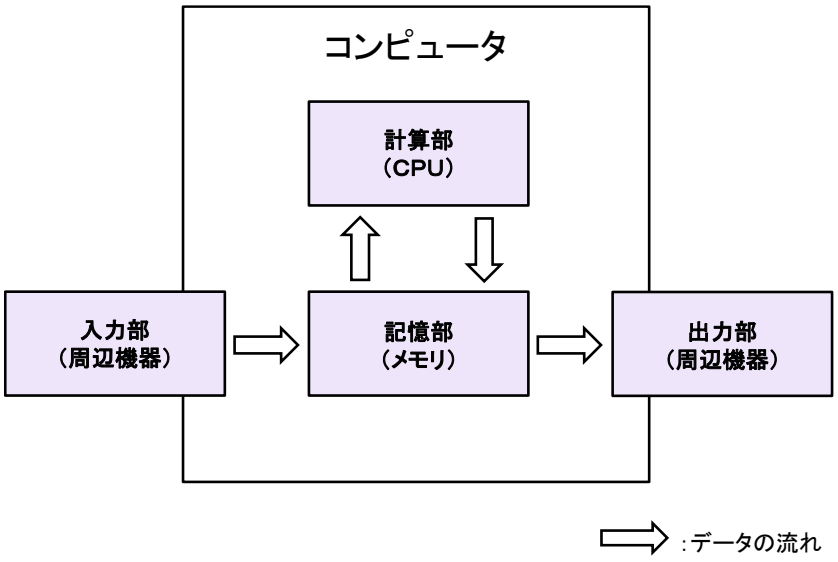

図 3-1　コンピュータの構造図

研究開発当時（1940 年代後半頃）の問題は、内部記憶として利用される、現在では一般にメモリと呼ばれている半導体素子の価格であり、当時は、このメモリの価格が極めて高いため、コンピュータに多くのメモリを使うことができなかった。

この問題に関して、ノイマンはプログラムとデータを同じ器（メモリ）内においてもコンピュータは機能させることができるという着想を持

[23] 伊藤寛『サイバー戦争論　ナショナルセキュリティの現在』原書房、2016 年、147 頁。

った。実は、彼が思いつくまではプログラムとデータは全くの別物なので、別の器（メモリ）に入れておくのが自然であり便利であると当時の科学者は考えていた。例えば、1944 年に作られた電気機械式の計算機、ハーバードマーク 1 では、プログラムは紙テープに保存され、データは電気機械的な装置（リレー）を利用して格納されていた。

しかし、ノイマンは同じメモリの中を区分してプログラムもデータも一緒に入れることを提案した。こうすることにより無駄が省け、高価なメモリを効率よく使えるようにした[24]。

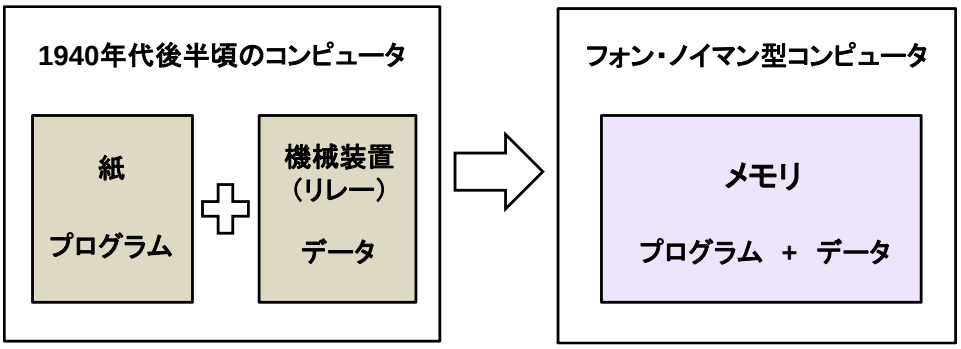

図 3-2　コンピュータの変遷

現在のコンピュータは全てこの方法を引き継いでいる。そのため、現在のパソコンは、フォン・ノイマン型コンピュータと呼ばれる。

現在では、半導体の値段も安くなったため、新たにコンピュータをゼロから設計するならば、プログラムとデータを物理的に別々の器（メモリ）に入れておくという構造とすることもできる。しかし、そのための新しい設計には、時間とコストがかかるとともに、これまでの仕組みを変えることになり、過去のプログラム資産が利用できなくなることやハードウェア設計の知見も使えなくなることから、研究は行われているがまだ普及していない[25]。

一方、メモリの中に、プログラムとデータを混在させるノイマンの方法は、画期的であったと同時に、コンピュータに大きな弱点を作ることにもなった。悪意を持った者が、データを格納すべきメモリのある領域に、データを装った悪意あるプログラムを入れることができるからである。すなわち、コンピュータはデータとして入力された悪意あるプロ

[24] 同上、148 頁。
[25] 同上、149-150 頁。

グラムを実行してしまうことがありうる。これを実行した場合、コンピュータで持ち主の全く知らないプログラムが動くということになり、コンピュータは悪者に乗っ取られたということになる。以上のように、コンピュータはその黎明期において、構造中に本質的な弱点を抱え込んでしまった[26]。

（イ）プログラム上の問題

論理的で一見、間違いを犯さないように見えるコンピュータも、結局はプログラムと呼ばれる計算等の手続きを記述したソフトウェアで動いているに過ぎない。プログラムを記述するのは人間であり、人間が書いている以上、常に何らかのミスがありうる。それは、単純なタイプミスのような些細なものから論理的な誤り、そして想定外の入力動作まで多種多様である。このような悪意のない問題や見落としは一般的にバグと言われる。ちなみに、悪意を持った者が、犯行を行うために意図を持って最初からプログラムに不正侵入するための何らかの欠陥を仕込んでおく場合もあり、これをバックドア（裏口）と呼ぶ。これらの様々なバグや欠陥から生起するコンピュータの弱点を脆弱性と呼び、悪意を持って意図的に利用された場合にサイバー攻撃の糸口となる。

このような脆弱性は、発見されると、その部分を修正するための小さなプログラム、いわゆるパッチというものを適用して修正することで安全性や安定性を高めることができる。しかし、ソフトウェアが時間とともに安全で安定したものになった頃には、新たな機能等が追加された新しいソフトウェアがリリース（アップデート）されることが多い。その場合にも当該ソフトウェアが新たな脆弱性を抱えている可能性が高く、その脆弱性を利用される恐れがある。こうして、ソフトウェアの脆弱性の問題は繰り返されることになる。

さらに、これはソフトウェアだけの問題ではなく、ハードウェア（ファームウェア[27]）に関しても同じような危険性がある。つまり、コンピュータを構成する物理的な装置や構成部品における例えば集積回路等の半導体素子自体にあらかじめ悪意のあるプログラムを入れ込んでおくというサイバー攻撃（サプライチェーン攻撃）も実際に考えられてい

[26] 同上、150 頁。
[27] ファームウェアとは、コンピュータや電子機器などに内蔵されるソフトウェアの一種で、本体内部の回路や装置などの基本的な制御を司る機能を持ったもの。（出典：IT 用語辞典 e-Words）

る[28]。

イ　ネットワーク上の脆弱性

インターネットはもともと米国の軍事研究に基づくものであった。その起源は、1969 年に米国国防省高等研究計画局（ARPA：Advanced Research Projects Agency）が軍事目的で開始した ARPANET であるとされ、将来の核戦争を想定し、米国本土が核攻撃を受けた場合に連邦政府と州政府間の通信が切れるような事態を避けるための通信ネットワークの仕組みを作ることであったと言われている。一方、インターネットの設計段階から、本来、軍事システムであれば、付加されるべき「通信者相互の信頼性の確保」や「通信文の安全を守る」という機能がなかった。この原因としては、組織内のネットワークとして人が相互に信頼し合っている前提のもとで機能する設計であったからと考えられる。

これらの問題点は現在に至るまで根本的に解消されていないため、インターネットを犯罪に利用した犯人を捕まえることが簡単にはできない状況となっている[29]。

（２）サイバー攻撃技術

ア　サイバー攻撃とは

「サイバー攻撃等」とは、防衛省の情報保証に関する訓令において、「サイバー攻撃（ネットワークを通じた電子的な攻撃をいう。）並びにサイバー攻撃と同様の影響を発生させる情報システムの誤操作及びサイバー攻撃以外によるコンピュータ・ウイルスの混入等」と定義づけられている。また、防衛省 HP[30]ではさらに詳しく「サイバー攻撃については、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤動作、不正プログラムの実行や DDoS（Distributed Denial of Service）攻撃[31]等として整理されている。」と記載されている。以上を踏まえると、防衛省では情報システムの情報保証を目的としているため、情報保証を脅かす全てのサイバー空間上の活動を、サイバー攻撃とみなし

---

[28] 伊藤寛『サイバー戦争論　ナショナルセキュリティの現在』原書房、2016 年、150-154 頁。
[29] 同上、156-157 頁。
[30] 防衛省「防衛省・自衛隊の『ここが知りたい！』　自衛隊のサイバー攻撃への対応について」、https://www.mod.go.jp/j/publication/shiritai/cyber/index.html.
[31] DDoS 攻撃とは、分散型サービス不能攻撃のこと。インターネット上の多数の機器から特定のネットワークやコンピュータを一斉に接続要求を送信し、過剰な負荷をかけて機能不全に追い込む攻撃手法。（出典：IT 用語辞典 e-Words）

ていると言える[32]。

本書では、防衛省の情報保証に関する訓令と同様の定義とする。

イ　サイバー攻撃方法

サイバー攻撃は、高度化・巧妙化・複雑化の一途を辿っている。第 1 章でも述べたとおり、2000 年代までは、個人によるサイバー攻撃が主体で、攻撃者は自身の能力を誇示するための愉快犯的なものが多かった。しかし、2000 年代後半からは個人を対象としたものだけでなく、企業や国家を標的としたサイバー攻撃が頻繁に行われるようになり、組織的な攻撃が行われている。

近年頻発している標的を絞った緻密な攻撃、いわゆる標的型攻撃には「攻撃の流れ」がある。これを「サイバーキルチェーン」という。まずは、攻撃の流れを理解することにより、どこで断ち切れば攻撃の流れを止められるのかを考えることが肝要である。

また、システムやソフトウェアの脆弱性を悪用する「マルウェア」の感染方法や要素についても説明する。サイバーキルチェーンの中で、マルウェアは中心的な役割を果たすため、これを理解することはセキュリティ対策を講ずる上で重要である。

（ア）サイバーキルチェーン

近年、サイバー攻撃はフェーズを踏んで行われるようになった。この攻撃を構造化したものが「サイバーキルチェーン」である。サイバーキルチェーンは、2009 年に米国のロッキード・マーティン社が提唱したもので、サイバー攻撃における攻撃者の動きを 7 つのフェーズに分類している[33]。分類は、表 3-1 のとおり。

---

[32] 海外の例として、NATO サイバー防衛センター（NATOCCDCOE）が策定した「タリン・マニュアル」の定義では、サイバー攻撃とは、「攻勢としてであるか防御としてであるかを問わず、人に対する傷害もしくは死、又は物に対する損害もしくは破壊を引き起こすことが合理的に予期されるサイバー行動 」とある。なお、これは、武力紛争法上、サイバー空間におけるどのような行動が「武力攻撃」に当たるものかという定義である。

[33] Eric M. Huthins, "*Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*," Lockheed Martin Corporation, 2012.https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

表 3-1　サイバーキルチェーンにおけるフェーズの分類[34]

フェーズ	説明
偵察 (Reconnaissance)	標的となる個人、組織を調査する。例えば、インターネット、名刺交換、組織への潜入等が挙げられる。
武器化 (Weaponization)	攻撃のためのエクスプロイトキットやマルウェア等を作成する。
配送 (Delivery)	マルウェアを添付したメールや悪意あるリンク付きメールを仕掛ける。あるいは直接対象組織のシステムへアクセスする。USB メモリ等の使用を含む。
エクスプロイト (Exploitation)	標的にマルウェア等攻撃ファイルを実行させる。または、悪意あるリンクにアクセスさせ、エクスプロイトを実行させる。
インストール (Installation)	エクスプロイトを成功させ、標的がマルウェアに感染する。これでマルウェアを実行可能となる。
遠隔操作 (Command &Control)	マルウェアと C&C サーバが通信可能となり、リモートから標的への操作が可能となる。
目的の実行 (Actions on Objectives)	情報窃取や改ざん、データ破壊、サービス停止等、攻撃者の目的が実行される。

この分類を活用し攻撃者の行動パターンを知ることでセキュリティ対策に繋げられることが期待できる。また、サイバーキルチェーンを利用したセキュリティ対策が、様々なセキュリティ企業等で発表されている。サイバーキルチェーンを利用したセキュリティ対策の一例は、図 3-3 のとおり。

[34] 本表は、ニュートン・コンサルティング「サイバーキルチェーン」、2019 年 1 月 16 日、https://www.newton-consulting.co.jp/itilnavi/glossary/cyber_kill_chain.html を基に筆者作成

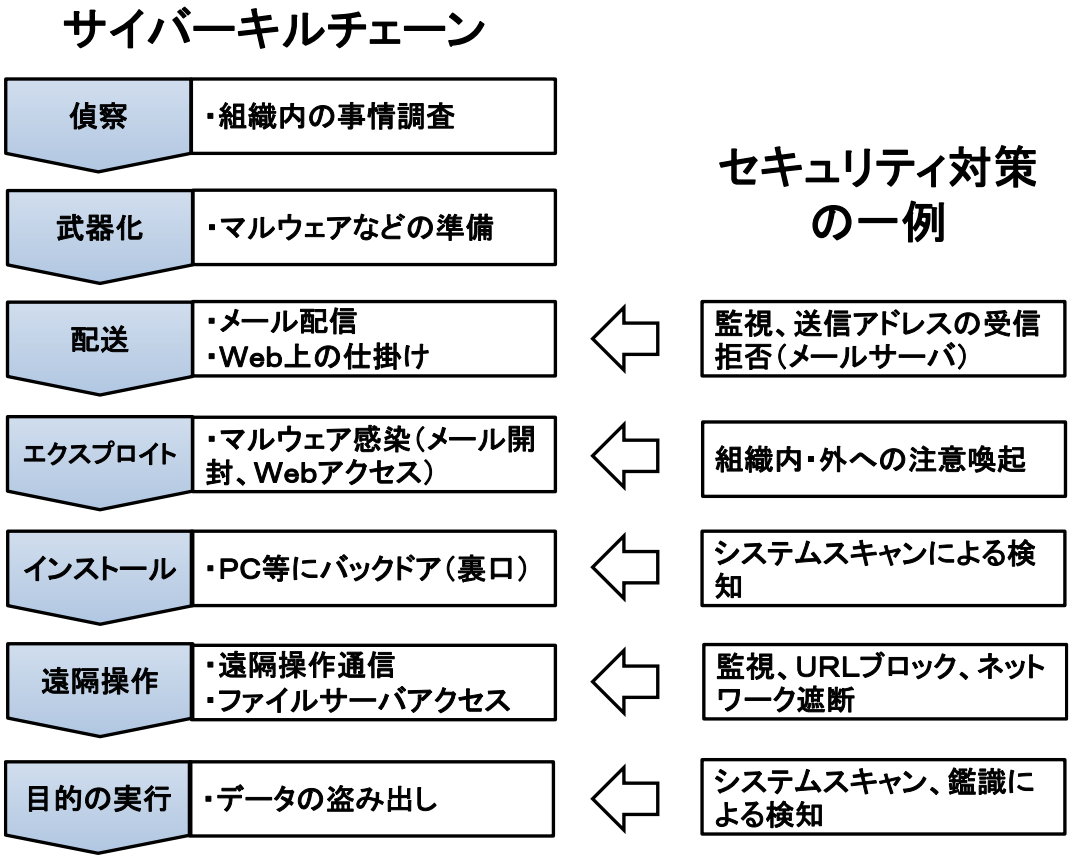

図 3-3　サイバーキルチェーンを利用したセキュリティ対策の一例[35]

サイバーキルチェーンは、攻撃パターンの一例を示しているものであり、常に同じパターンで攻撃してくるとは限らない。このため、防御側は、全てのフェーズであらゆる対策を行わなくてはならない。

（イ）マルウェアの感染方法と要素

サイバー攻撃には特別に作られたソフトウェアを利用する場合がある。それらは、ツールと呼ばれ民間においてもハッカーがシステムに侵入するために利用しており、有料無料の様々なものが出回っている。他にも、自律型のマルウェア、いわゆるコンピュータ・ウイルスを利用する方法もある。マルウェアは、システムやソフトウェアの脆弱性を悪用するものであり、攻撃対象によってカスタマイズされる。

マルウェアは、その性質を大きく「マルウェアの感染方法（システムへの侵入方法）」と「マルウェアの要素（侵入後の攻撃方法）」に分けて

[35] 本図は、後藤厚宏「IoT 時代のサイバーセキュリティ確保に向けて」情報セキュリティ大学院大学、https://www.ipa.go.jp/files/000057703.pdf を基に筆者作成

分析することができる。

a　感染方法による分類

マルウェアの感染方法による分類は表 3-2 のとおり[36]。

表 3-2　マルウェアの感染方法による分類

名称	感染方法
ウイルス	既存のソフトウェアに寄生し、その動きを利用して感染を広げるもの
ワーム	独立して自立的行動を行うもの
トロイの木馬	パッチや更新データ等、何か役に立ちそうなソフトウェアやデータのふりをしてユーザ自らに取り込ませるもの
水飲み場攻撃	罠が仕掛けられたＨＰを訪れると感染するもの
サプライチェーンリスク	ハードウェアにあらかじめ仕込まれているもの

それぞれ攻撃者にとっての利点と不利点があるが、最近の民間での事件では、ウイルスやワームによる犯罪は減っており、トロイの木馬が多用されている。これは標的型メール攻撃に代表されるように、無害に見える添付資料などにマルウェアが潜んでいるというパターンである。ユーザが自ら開いてしまうので、アンチウイルスソフト等による自動化された対処は困難である。この理由は、アンチウイルスソフトは外部から侵入しようとするものは警戒するが、ユーザの操作により開く等、ネットワーク内部の操作に対しては働きにくい特性があるからである。

またこれらのマルウェアは、アンチウイルスソフトに検知されないように、暗号化などの工夫がされている。そもそも、攻撃者は一般に販売されているようなアンチウイルスソフトを事前に分析しているので、少なくともそれらに対しては、検知されないことを確認してから攻撃してくると考えられる。そのために、アンチウイルスソフトでマルウェアを確実に検知できると期待することはできない。

続いて、水飲み場攻撃は、一般的に犯人が用意したホームページに

[36] 伊藤寛「サイバー戦争論　ナショナルセキュリティの現在」原書房、2016 年、159 頁。

罠が仕掛けてあり、そこにアクセスする者を待ち構えている。もしアクセスして来た者が狙った相手の場合は、マルウェアをダウンロードさせるという手法が多用されている。この際、狙った相手でなければダウンロードさせないことでターゲットを確実に攻撃するとともに、アンチウイルスソフトなどによるマルウェアの探索からも逃れることができる。

サイバー領域におけるターゲットは、軍事的な情報システムだけでなく、隊員個人のパソコンやスマホにも及ぶことを認識する必要があり、標的型メール攻撃や水飲み場攻撃等に注意する必要がある。

また、軍事的な情報システムへの侵入については、最初は、USBメモリの持ち込み、あるいは、捕虜、内通者等の獲得により正規ユーザとしてシステムに加入すること等から始まる可能性が高い。そして、侵入に成功した後、ウイルスやワーム等のマルウェアを当該システム内で感染させるということが考えられる。

b　マルウェアの要素による分類

マルウェアの要素は、表 3-3 のとおり[37]。

表 3-3　マルウェアの要素による分類

要素区分	概要
攻撃目的	システム全体あるいは関連する物理的目標の性能低下、混乱、停止あるいは破壊を目的とするもの：論理爆弾
	情報収集を目的とするもの：スパイウェア
機能発揮のタイミング	決められた時間が来ると自動的に機能発揮するもの
	外からの信号に応じて機能発揮するもの
	指揮統制サーバとの通信が切れたら機能発揮するもの
秘匿	検知されないように隠れるもの
	自分自身をバージョンアップしたり、発見されにくいように形状を変えたりしていくもの
	いったん消去されても復活するもの
	用が済めば、自分自身を消去して痕跡まで消してしまうもの

[37] 同上、162 頁。

まず、攻撃目的を区分とした要素は、スタックスネットのようにハードを攻撃し、その機能発揮を妨害したり破壊したりしようとするものと、相手のソフト的な機能を攻撃し、情報収集等をするものに大きく区分される。

続いて、機能発揮するタイミングを区分とした要素は、攻撃者の目的や意図によって異なり、実行したいタイミングによってそれぞれ区分される。

また、秘匿を区分とした要素は、マルウェアが、相手に気づかれないように、隠密に行動させるものであり、それらの行動方法でそれぞれ区分される。

これらのマルウェアの保有する要素は、複数の要素を併せ持ち、状況に応じて組み合わせて使用されるものである。

（３）サイバー防御技術[38]

サイバー防御手法には、大きく２つある。DoS（Denial of Service）攻撃のように内部に侵入することなくあからさまにシステムに負荷をかけてくるものへの備えと、システムへ密かに侵入をしてくるものへの備えである。

また、サイバー攻撃を受け被害が生じたとしても、任務を継続する能力としてサイバーレジリエンスという防御手法の考え方がある。

ア　システムに負荷をかけてくる攻撃に対する防御方法

DoS 攻撃のように侵入することなく、システムに負荷をかけるなどしてその機能を阻害しようとする攻撃に対しては、システム全体の対処能力を上げるために次の対策が考えられる。

（ア）コンピュータを多数用意すること

（イ）コンピュータの処理能力を向上させること

（ウ）ネットワークを構成する回線の通信容量を大きくすること

（エ）迂回路を形成すること

その他、サーバなどの脆弱性を狙う攻撃に対しては、パッチを当てるなどの対策が必要である。

イ　システムへ侵入をしてくる攻撃に対する防御方法

システムへ侵入してくる攻撃に対する防御方法の一例は次のとおりであり、細部を説明する。

---

[38] 同上、84-95 頁。

表 3-4　防御方法の一例

方法	一例
予防	ハード及びソフトに係る脆弱性の発見と除去
	システム監査による問題の早期発見
	人的ミスの低減、根絶のための対策（教育訓練）
検知	アンチウイルスソフトや IDS[39]等により検知
	AI やビックデータを活用した監視
対処	ファイヤーウォール等の利用による侵入阻止
	任務継続のための措置（縮退運用、代替運用）
復旧	システム二重化等による早期復旧
	優先順位に基づく復旧手順の確立

（ア）予防

予防の要訣は、システムのセキュリティを強くして、攻撃を受けないように態勢を整え、仮に攻撃を受けても損害を局限し、じ後の復旧を速やかに実施可能としておくことである。

具体的には、利用しているハードウェアの信頼性を担保すること、ソフトウェアを常に最新のバージョンに更新して既知のバグや脆弱性のない状態にすること、人間の健康診断に相当するシステム監査を行い問題の早期発見に努めることである。さらに、規則の確立と徹底、関係者に対する訓練とセキュリティ意識を上げるための教育などを行うことも重要である。

（イ）検知

検知は、民間でも使われているようなアンチウイルスソフトや IDS（Intrusion Detection System）等の侵入検知システムを防御対象システムに導入し、常時、不審なパケットの出入りの有無やパソコンやサーバ等の状態を監視する技術が中心となる。

IDS はシステム上の状況を収集、分析、統合して、異常を発見すると監視員に対して警告を発することができる。ただし、これらの器材は誤検知することもあり、また、そもそも攻撃者はそれらの器材の働きを分析した上で攻撃してくると考えられるので、これらの器材だけで攻撃を全て検知できるとは言えない。器材等が検知した結果からそれがサ

[39] IDS（Intrusion Detection System）とは侵入検知システムのこと。（出典：IT 用語辞典）

イバー攻撃かどうか判断し、敵対者の侵入を検知することができる監視員は必要不可欠である。

一方、監視員つまり人間の関与する割合はできるだけ減らさなければならない。単に人件費の問題ではなく、敵対者が自動化した攻撃を行っているとき、それに対応する「人間の速度」は「機械の速度」より遅く、対処が遅れる可能性がある。したがって、ネットワーク監視やマルウェア解析などにビックデータやAI等の活用が期待されている。

（ウ）対処

対処は、侵入を阻止する仕組みであるファイヤーウォール等、民間で活用されているような様々な技術が中心である。

対処の基本は、まずシステム内部に侵入させないことである。しかし、現状、ファイヤーウォール等を活用しても、100%の侵入阻止はできない。したがって、防御を突破されシステム内部へ侵入を許したとしても、被害を最小化し簡単にはシステム全体に被害が広がらないような仕組みが必要である。例えば、攻撃を受け感染した部分を迅速に切り離して被害が他に波及しないようにする仕組みや、損害を受けた機能を迅速に代替できる用意しておくことが考えられる。

また、ハニーポットと呼ばれる侵入者をおびきよせる「おとり」のシステムを用意しておき、そこに入ってきた攻撃者の活動を観察して事後の対処に役立てる防御方法もある。さらに、攻撃元に対して反撃を行うハックバックも防御方法の一つであるが、攻撃ルートを遡っていき、攻撃元サーバ等を攻撃するため、法的な制約が伴うとともに、技術的にも難しい。

（エ）復旧

復旧の仕組みも重要である。敵対者は戦闘の最初に烈度が高いサイバー攻撃を仕掛けてきて、こちらのシステムの混乱を図ることが考えられる。それを完全に防御することはできないとしても、システムの復旧時間をできる限り短くすることが必要である。そのため、システムを二重化しておき、一つをネットワークから切り離した状態でスタンバイさせておくことや、データのバックアップの仕組みや攻撃によりシステムがダウンしても全体の機能停止に陥らないような設計をしておくことが重要である。

ウ　サイバーレジリエンス

サイバーレジリエンスとは、サイバー攻撃を受け被害を生じたとしても、任務を継続する能力のことである。この能力は、レジリエンス（抗たん性）を高めることで、任務の継続性を脅かすサイバー攻撃を受けたとしても、早期に正常な運用環境を復元し、通常の運用を再開することである。

具体的には、サイバー攻撃によるリスクを総合的に判断し、強靭に任務を継続するための一連の対応（予測する、耐える、回復する、適応する等）を行う。

この考え方は、米国の NIST（National Institute of Standards and Technology）により公表されたもので、「サイバーレジリエンスの技術と実装のためのアプローチ」として、表 3-5 で示す 14 項目が挙げられている[40]。

サイバー攻撃の烈度が増している昨今においては、サイバー攻撃を完璧に防御して被害を受けないということは極めて困難であるため、サイバー攻撃により被害を受けることを前提として、あらゆる対策を講じておくことが重要である。

表 3-5　サイバーレジリエンスの技術と実装のためのアプローチ[41]

テクニック	アプローチの一例
適応的対応 Adaptive Response	・動的な再構成（ルータのルール、ＩＤＳのパラメータなど） ・動的なリソース割り当て（負荷分散、緊急遮断など） ・適応的管理（動的アクセス無効化、システムの自動無効化など）
分析的監視 Analytic Monitoring	・監視とダメージ評価（ハードウェア障害検出やＩＤＳの利用など） ・センサーの融合と分析（異なるツールからデータの関連付け） ・鑑識及び行動分析（リバースエンジニアリングなど）
協調的な保護 Coordinated Protection	・多層防御（ネットワークとホストのＩＤＳの組み合わせなど） ・全般調整（インシデントハンドリングの調整など） ・自己テスト（侵入テストやレッドチームの演習など）
状況認識 Contextual Awareness	・動的なリソース認識（リアルタイムの統合された状況認識） ・動的な脅威認識（インシデント及び脅威データの取り込みなど） ・ミッションの依存関係とステータス（広範な視点の構築）
欺瞞 Deception	・難読化（暗号化、通信パターンの隠蔽またはランダム化など） ・偽情報（偽の資格情報とトークン、誤った情報の投稿など） ・誤った方向づけ（ハニーポット、おとりファイルなど）

[40] NIST SP 800-160 Volume 2[Final Draft, November 27,2019],「Developing Cyber Resilient Systems: A Systems Security Engineering Approach」

[41] 本表は、NIST SP 800-160 Volume 2[Final Draft, November 27,2019]を基に筆者作成

多様性 Diversity	・アーキテクチャの多様性（異なるＯＳでのログの取得など） ・設計の多様性（多様なプログラム、異なる通信方式など） ・回線の多様性（代替通信サービス（地上、衛星回線等）の確立など）
動的ポジショニング Dynamic Positioning	・センサーの機能的再配置（ＩＤＳ等の仮想化または再構成など） ・サイバーリソースの機能移転（ストレージサイトの変更など） ・機器の分散（構成機能を分散するアプリケーションの設計など）
非永続性[42]の生成と保持 Non-Persistence Generate and retain	・情報の非永続性（価値のある情報を処理後削除など） ・サービスの非永続性（時間や非活動ベースのセッション終了など） ・接続の非永続性（時間や非活動ベースのネットワーク切断など）
特権 (Privilege Restriction)	・権限管理（最小限の特権、時間によるアカウント制限） ・使用制限（役割に応じたアクセス制御など） ・動的な特権（任務に応じた権限に対する時間ベースの調整など）
再調整 (Realignment)	・目的化（未承認アプリケーションのインストール防止など） ・制限（必須の機能のみを提供するシステムの構成など） ・置き換え（サポートされないシステムコンポーネントを置き換え）
冗長性 (Redundancy	・バックアップとリストア（バックアップ情報の維持と保護など） ・余剰能力（予備部品の維持、外部システムとのサービス契約など） ・複製（代替データベース、代替ストレージの維持など）
セグメンテーション[43] (Segmentation)	・セグメント化（仮想化による個別の処理ドメインの維持） ・動的なセグメンテーション（システムコンポーネントの動的な分離）
実証済みの完全性 (Substantiated Integrity)	・完全性チェック[44]（データ品質チェック用の自動化ツールなど） ・出所追跡（サプライチェーンリスクマネジメントのための追跡管理） ・動作検証（機能検証の実装、動作プロセスの完全性の確認など）
予測不能性[45] (Unpredictability)	・一次的な予測不能性（ランダム間隔で再認証の要求など） ・状況の予測不能性（役割と責任の交代など）

エ　サイバー脅威の増大に対する適切な認識

サイバー攻撃の技術や手法が高度化・巧妙化・複雑化し、サイバー脅威が増大しているところであるが、我々が利用しているネットワークの構成や仕組みがセキュリティを損なっており、サイバー脅威を更に増大させている。

一般的に、ネットワークの構成は、従来から比較すると、有線 LAN だけでなく無線 LAN を加えた複合的なネットワークへと変遷している。また、テレワーク等、インターネット環境を活用して組織内のネットワークにアクセスする機会が増えている。これらは、ネットワークの利便性を向上させる一方、ネットワークのアクセスポイントが増え、それを利用した

42 非永続性とは、ある状態が長く続かないようにする性質のこと。
43 セグメンテーションとは、区分け、分割すること。全体を何らかの基準や規則に基づいて、いくつかの部分・断片（セグメント）に分割すること。（出典：IT 用語辞典）
44 完全性チェックとは、データ等の品質が故意・過失・災害などで改ざんや破壊されていないかをチェックすること。
45 予測不能性とは、第 3 者が規則的な行動を予測することができない性質のこと。

脆弱性が増えている。

したがって、サイバー攻撃の現状とネットワークの脆弱性を相対的に考えると、サイバー脅威は拡大している。

我々は、ネットワークの構成や仕組みによる脆弱性を理解し、セキュリティ対策を万全にする必要がある。まずは、サイバー脅威の増大に対する適切な認識を持たなければならない。

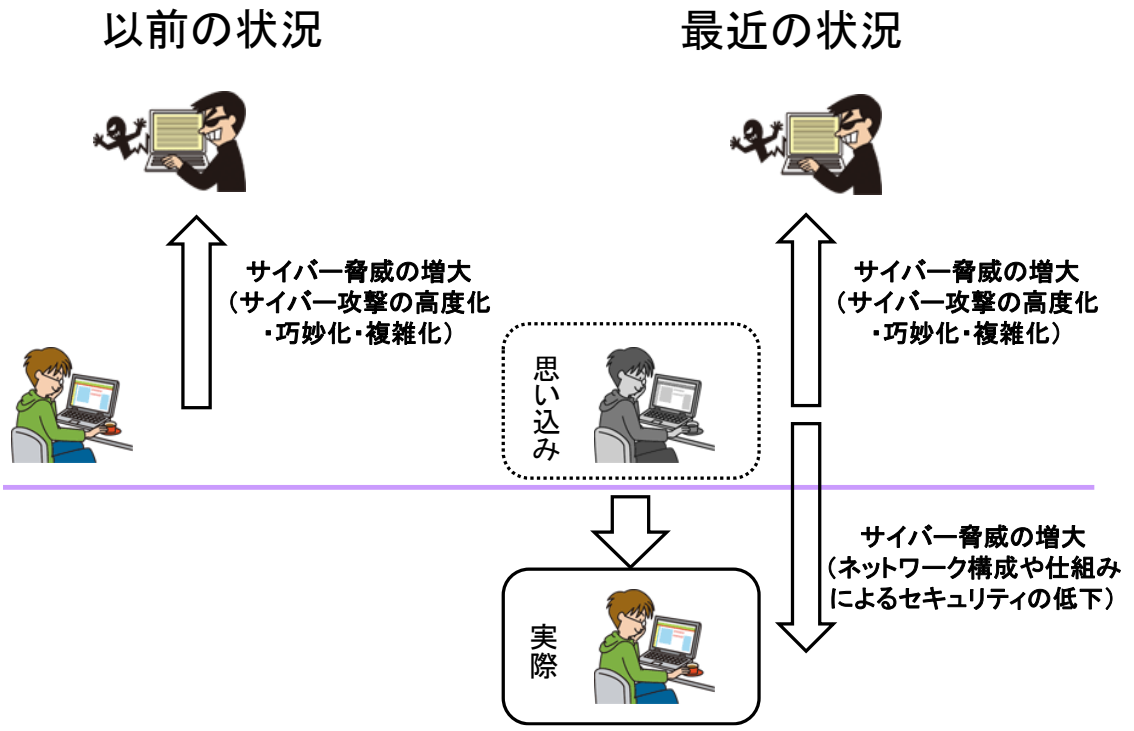

図 3-4　サイバー脅威の増大に対する適切な認識

４　米軍のサイバー空間作戦

本章では、米軍ドクトリンを引用して、米軍のサイバー空間作戦の一部を説明する。サイバー空間の特徴及びサイバー空間の利用に係る課題をそれぞれ記述したのち、サイバー空間に関する軍事作戦に焦点を当て、サイバー空間任務及び行動について整理する。

（１）サイバー空間の特徴

ア　物理領域との関係（Relationship with the Physical Domains）

情報環境の一部であるサイバー空間は、陸、海、空及び宇宙の物理領域に依存している。

サイバー空間作戦は、物理領域に設置されるリンク（通信接続）及びノードを使用し、論理的な機能を実行してサイバー空間内に作用を作り出し、必要に応じてサイバー空間外にも作用する。サイバー空間内の複合的な作用が注意深く統制された行動は、物理領域における行動の自由を可能とする。

イ　サイバー空間の層モデル（Cyberspace Layer Model）

サイバー空間作戦の計画立案及び実行を補佐するため、サイバー空間は３つの関連する層で構成される。これは、①物理層、②論理層、③人的層である。

ウ　国防省サイバー空間（Department of Defense Cyberspace）

国防省情報ネットワーク（以下「DODIN」という。）は、相互接続されているかスタンドアローンであるかに関係なく、戦闘員、政策立案者及び支援要員の要求に応じて情報を収集、処理、保存、配布及び管理するための一連の情報能力とそのプロセスの組み合わせである。

エ　接続性及びアクセス（Connectivity and Access）

標的を含め、運用上有益なサイバー空間へのアクセスを得ることは、法律、政策、運用の限界により制約を受ける。このような理由から、アクセスは保証されたものではない。加えて、指揮官が示す標的へのアクセスは、敵対者、同盟者、中立者、他の米国政府機関等が使用するサイバー空間の特殊な要素により、極めて複雑になりうる。

オ　運用環境（The Operational Environment）

運用環境は、条件、状況、及び影響の複合体であり、能力の使用に影響

を与え、指揮官の意思決定に強い影響を及ぼす。情報環境は物理領域に浸透し、ゆえにどの運用環境にも存在する。

カ　情報環境（The Information Environment）

情報環境は、個人及び組織並びに収集、処理、配布及び情報分野における行動の集合体である。

与えられたサイバー空間は情報環境に完全に包含され、情報作戦の主目的は情報環境内に作用を作り出すことにある。このため情報作戦とサイバー空間作戦には極めて強い相関がある。

（２）サイバー空間の利用に係る課題

ア　脅威（Threats）

サイバー空間は、統合軍の作戦に対し、国家規模から個人レベルまでの意図的な事故から自然発生的な災害まで、多くの脅威を提供する。

イ　匿名性と識別困難性（Anonymity and Difficulties with Attribution）

適切な防御的対応を始めるには、サイバー空間内における脅威の識別（attribution）が、承認された自衛の範囲を超えたサイバー空間外でのいかなる行動のためにも、決定的に重要である。

ウ　地理的課題（Geography Challenges）

サイバー空間内は、国家不在で行動できる空間ではない。このため、米軍が他国のサイバー空間で行動する際には、任務及び政策の要件により、インフラが存在する国家の承認なく密かに行動する場合がある。

エ　技術的課題（Technology Challenges）

標的における技術的脆弱性の悪用に依存するサイバー空間能力を使用すると、その能力が明らかになり、将来の任務に対する能力の有効性が損なわれる可能性がある。

オ　私企業と公的インフラ（Private Industry and Public Infrastructure）

国防省の重要な機能と運用の多くは、インターネットサービスプロバイダ（ISP）やグローバルサプライチェーンなど、契約された商業資産に依存しており、国防省と軍にはそれらに対する直接の権限はない。

カ　グローバル化（Globalization）

サイバー空間と関連する技術に依存した国防省の全世界的な作戦は、国防省が任務の中核的な情報技術製品やサービスを海外のベンダーからしばしば調達することを意味する。

キ　抑制（Mitigations）

国防省は防衛産業基盤（DIB : Defense Industrial Base）と連携して、DIB の秘匿化されていないネットワークに常駐又は通過する国防省プログラムに関する情報のセキュリティを強化している。

（３）サイバー空間に関する軍事作戦

ア　サイバー空間で可能となる活動（Cyberspace-enabled activities）

多くの国防省におけるサイバー空間活動は、サイバー空間を使用して任務を果たす活動であるが、これらの活動は攻勢的サイバー空間作戦（以下「OCO」という。）、防勢的サイバー空間作戦（以下「DCO」という。）又は DODIN 作戦には含まれない。サイバー空間で可能となる活動には、指揮統制又は後方システムの操作、電子メールの送信、ブリーフィング資料の作成などが含まれる。

サイバー空間の使用を通じて、DODIN における脆弱性の大部分が敵にさらされ、悪用されている。課題は、サイバー空間の脅威の重要性を理解し、脅威の戦術を認識するように全ての DODIN ユーザを訓練して、サイバー空間の使用が任務に不要なリスクを引き起こさないようにすることである。

イ　サイバー空間任務（Cyberspace Missions）

サイバー空間で可能となる活動以外の、サイバー空間内の全ての活動は、OCO、DCO 及び DODIN 作戦の 3 つの任務に分類される。この 3 つの任務は、サイバー空間部隊の諸活動を総合的にカバーしている。サイバー空間作戦の成功にはこれらの任務の組み合わせ及び同調が要求される。

サイバー空間任務の概念図、は図 4-1 のとおり。

サイバー空間任務の概念図

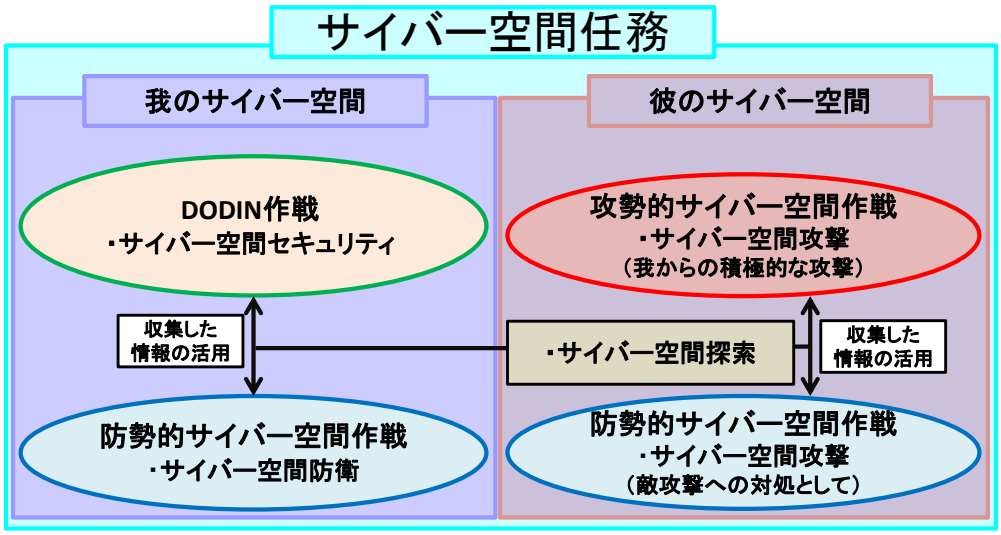

図 4-1：サイバー空間任務の概念図

（ア）DODIN 作戦

DODIN 作戦の任務は、DODIN を防御、構成、運用、拡張及び維持すること並びに機密性、可用性及び完全性を創出し、維持するために実行される活動を含む。これらには、DODIN の脆弱性に対処する予防的なサイバー空間セキュリティ活動、ネットワーク拡張のためのセットアップ、DODIN の維持に必要な整備活動、セキュリティ評価とそのテストが含まれる。

DODIN 作戦は、ネットワークに焦点を当て、脅威にとらわれないものである。この任務を遂行するサイバー空間部隊と労働力は、防御するためのネットワークやシステムに脅威が悪影響を及ぼさないように努めている。これらは、脅威に関する情報に基づいており、脅威に関する全ての利用可能なインテリジェンスを使用して、ネットワークのセキュリティ態勢を改善する。

（イ）防勢的サイバー空間作戦（Defensive Cyberspace Operations）

DCO の任務は、DODIN 又は国防省のサイバー空間部隊が防御を命ぜられたサイバー空間を、サイバー空間内の脅威から防御するために行われる。具体的には、我のサイバー空間に対する悪意ある活動を無力化し、我のサイバー空間作戦能力を運用可能な状態に維持するとともに、データ、ネットワーク、サイバー空間作戦遂行上必要な装備品やシステムを防御することを企図して行う一連の任務をいう。セキュリテ

ィ対策を回避又は侵害する脅威に対処する DCO は、脅威活動に先立って脅威から国防省のサイバー空間を防御しようとする DODIN 作戦とは区別される。

DCO は、攻撃、探索、又は悪意のあるサイバー空間活動をする特定の脅威に対応して実施されるため、必要に応じて、インテリジェンスの収集、諜報活動、法執行機関及びその他の情報源からの情報を活用する。

DCO には、防御されたサイバー空間に対して行動を起こす敵対者を阻止すること、あるいは差し迫った内部及び外部のサイバー空間の脅威に対応することが含まれる。従って、DCO の目標は、敵対者の脅威を克服すること、及び侵害されたネットワークを安全で機能的な状態に戻すことである。

（ウ）攻勢的サイバー空間作戦（Offensive Cyberspace Operations）

OCO の任務は、指揮官又は国家目的を支援するため、サイバー空間内又はサイバー空間を通じて敵対者に対して力を投射することを企図して行われる。

OCO は、敵対者のサイバー空間における活動能力を標的にするか、又はサイバー空間において一次効果を創出し、その一次効果をサイバー空間から物理領域に波及させることによって、敵対者の兵器システム、指揮統制プロセス、後方拠点、高価値目標に対し影響を及ぼすために実行する[46]。

OCO の態様や程度によっては、DCO の一部と同様に、敵対者のシステムに対する物理的破壊を伴うものが含まれ、国際法上の武力の行使に該当しうる。また、OCO の実行に当たっては、軍事的統制を適切にするとともに、作戦の範囲、交戦規定及び目的について慎重な検討が必要不可欠である。

ウ　サイバー空間行動（Cyberspace Actions）

サイバー空間任務の実行には、戦術レベルの行動が求められる。これらの諸行動は、下記の組み合わせによって行われる。

---

[46] スタックスネットを例に挙げて一次効果について説明する。スタックスネット（Stuxnet）とは、2010年にイランのウラン濃縮工場の制御システムに感染しその制御を奪った高度かつ複雑なマルウェアのこと。スタックスネットは周波数変換装置の出力周波数を変化させることで遠心分離機を物理的に破壊するよう設計されている。ここでいう一次効果とは、「サイバー空間内でスタックスネットに感染させ周波数変換装置の出力周波数を変化させること」であり、その効果により遠心分離機を物理的に破壊させることが、その一次効果をサイバー空間から物理空間に波及するという意味である。

（ア）サイバー空間セキュリティ（Cyberspace Security）

サイバー空間セキュリティは、我のサイバー空間内において実行する行動であって、我のコンピュータ及びネットワークに対する不正アクセス、探索、損害等を予防するとともに、コンピュータ及びネットワークで取り扱われるデータの機密性、完全性、可用性、識別認証、否認防止を確保するものである。これは、セキュリティ侵害の前に実施するDODIN 作戦任務の主要な行動の一部である。

また、サイバー空間セキュリティは、脅威の存在有無に関わらず、平素の段階から常続的に実行すべき行動であり、我のサイバー空間内における脆弱性を除去し敵対者によるサイバー攻撃の機会を与えないようにするとともに、敵対者による我のサイバー空間に対する悪意ある活動を探知する行動を含む。

サイバー空間セキュリティの例としては、パスワードの強化、脆弱性を排除するためのソフトウェアの更新、データの暗号化、ユーザに対する教育訓練、疑わしいサイトへのアクセス制限などがある。

（イ）サイバー空間防衛（Cyberspace Defense）

サイバー空間防衛は、我のサイバー空間内において実行する行動であって、我のサイバーセキュリティ対策を破り、又はその恐れのある特定の脅威を無効化するための行動である。これには、マルウェアやユーザの不正な活動の探知、特定、対処及び脅威の減殺並びにシステムの復旧に必要な行動を含む。

（ウ）サイバー空間探索（Cyberspace Exploitations）

サイバー空間探索は、我のサイバー空間外において実行する行動であって、サイバー空間攻撃に該当する効果を含まないインテリジェンス活動、情報収集、その他将来の軍事作戦に備えるために必要とされる行動が含まれる。

サイバー空間探索は、対象とするネットワーク、システム、軍事的に価値の高いノード（端末）等に対するアクセス権を獲得・維持し、事後の行動に資するため、サイバー空間能力遂行に必要な機能を配備することを含む。また、現行作戦及び将来作戦に資するため、敵対者又は第３国のサイバー空間の状況を明らかにして脆弱性と標的を発見し、作戦計画の立案、実行及び分析を支援する。

（エ）サイバー空間攻撃（Cyberspace Attack）

サイバー空間攻撃は、攻撃対象のサイバー空間内における機能低下、混乱又は破壊といった顕著な拒否的効果を引き起こす行動、又はサイバー空間内における効果を波及させて物理領域における拒否的効果を引き起こす行動をいう。

サイバー空間探索行動は隠密裏に遂行されるが、サイバー空間攻撃行動は、攻撃対象となったユーザやシステム管理者に容易に検知されることから、敵対者にとってその行動が明らかになるものである。

５　サイバー空間での対応に関係する国内法及び国際法

防衛省・自衛隊は、いかなる状況においても防衛省・自衛隊のシステム・ネットワークの機能を確保するため、24 時間態勢での通信ネットワークの監視、マルウェア解析を含めたサイバー攻撃[47]対処等を実施している。また今後は、有事における我が国への攻撃に際して、当該攻撃に用いられる相手方のサイバー空間の利用を妨げる能力の強化も図ることとされている[48]。ここでは、こうした取組をめぐる国内法及び国際法の状況について整理する。

（１）国内法

国の行政機関として防衛省を設置する旨を定める防衛省設置法は、防衛省の任務及び所掌事務を定め、自衛隊法は、実力組織としての自衛隊の任務、組織及び編成並びに行動及び権限等について定めている。ただし、その遂行に当たっては、防衛省設置法及び自衛隊法に加え、その他の関係法令の遵守も求められる。このため、サイバー空間での自衛隊の対応に関係する国内法について理解するに当たっては、防衛法制に関する政府の解釈とあわせて次のような主要な情報セキュリティ関連法を踏まえる必要がある。

ア　主要情報セキュリティ関連法

サイバーセキュリティに関する法律は、体制整備に関して定めるサイバーセキュリティ基本法（平成 26 年法律第 104 号）と、侵害行為の規制に関して定める不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）及び刑法（明治 40 年法律第 45 号）の関係規定とに大別できる。

（ア）サイバーセキュリティ基本法

サイバーセキュリティ基本法は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、サイバーセキュリティの定義、基本理念、国等の関係者の責務等[49]を明らかにし、サイバーセキュリティ

---

47 サイバー攻撃には、情報通信ネットワークや情報システムなどの悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行や DDoS 攻撃（分散サービス不能攻撃）などがある。防衛省『令和 2 年度防衛白書』2020 年、271 頁注 6。

48 同上、271 頁。

49 国（第 4 条、第 10 条、第 11 条）、地方公共団体（第 5 条）、重要社会基盤事業者（第 6 条）、サイバー関連事業者その他の事業者（第 7 条）及び教育研究機関の責務（第 8 条）並びに国民の努力義務（第 9 条）が規定されている。なお、重要社会基盤事業者とは、「国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれがあるものに関する事業

戦略の策定、サイバーセキュリティ確保のための基本的施策並びにサイバーセキュリティ戦略本部及びサイバーセキュリティ協議会[50]の設置等を規定している。なお、内閣サイバーセキュリティセンター（NISC）は、この法律を踏まえて内閣官房組織令によって設置された組織である。

防衛省・自衛隊は、自らの情報システム・ネットワークに対するサイバー攻撃に対処する一方、サイバー空間そのものの安定的な利用についてまで防衛省・自衛隊のみによって達成することは困難である[51]。このため、政府全体としての取組については、司令塔機能を担う内閣サイバーセキュリティセンター等関係省庁との連携が必要とされている。こうした観点から、以下では、政府全体の取組の中心となるサイバーセキュリティ戦略本部の組織及び所掌事務、サイバーセキュリティ戦略に定めるべき事項等並びに司令塔機能を担う内閣サイバーセキュリティセンターの所掌事務について概説する。

ａ　サイバーセキュリティ戦略本部

サイバーセキュリティ基本法は、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣にサイバーセキュリティ戦略本部を設置することを規定している（第 25 条）。

同本部は、関係閣僚及び有識者によって構成されており[52]、内閣サイバーセキュリティセンターが事務局を務める（第 35 条、内閣官房組織令第 4 条の 2）。

同本部の主な所掌事務は、次のとおり（第 26 条第 1 項各号）。

① サイバーセキュリティ戦略の案の作成及び同戦略の実施の推進

② 国の行政機関、独立行政法人及び指定法人における対策基準の

者」と定義されており（第 3 条第 1 項）、いわゆる重要インフラ事業者を指す。重要インフラ分野として、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道、物流、化学、クレジット及び石油の分野が指定されている。サイバーセキュリティ戦略本部「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（平成 29 年 4 月 18 日決定、令和 2 年 1 月 30 日改定）、59 頁。サイバー関連事業者とは、「インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者」と定義されている（第 7 条）。

[50] 平成 30 年の改正で規定され、令和元年 4 月 1 日に発足した。サイバーセキュリティ協議会は、サイバーセキュリティ関連施策について情報共有及び協議を行うものであり、サイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣が組織する。本部長等が必要と認めるときは、協議して、行政組織、自治体、重要社会基盤事業者、サイバー関連事業者、教育研究機関等からも構成員を加えることができる（第 17 条）。

[51] 「防衛省・自衛隊の『ここが知りたい！』自衛隊のサイバー攻撃への対応について」防衛省・自衛隊、https://www.mod.go.jp/j//publication/shiritai/cyber/index.html.

[52] 本部長は、内閣官房長官であり、副本部長には国務大臣が充てられる。また、本部員は、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣及びこれら以外の国務大臣のうち特に内閣総理大臣が指定する者並びに有識者のうち内閣総理大臣が任命する者によって構成される。

作成及び同基準に基づく施策の評価（監査を含む。）その他同基準に基づく施策の実施推進

③ 国の行政機関、独立行政法人又は指定法人で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明調査を含む。）

④ サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整

⑤ その他サイバーセキュリティに関する重要施策の企画に関する調査審議、府省横断的計画・関係行政機関の経費見積もり方針・施策の実施に関する指針の作成、施策の評価その他の実施推進及び総合調整

同本部は、サイバーセキュリティに関する重要事項については高度情報通信ネットワーク社会推進戦略本部と、また、我が国の安全保障に係るサイバーセキュリティに関する重要事項については国家安全保障会議と緊密な連携を図らなければならない（第 26 条第 3 項及び第 4 項）。

b　サイバーセキュリティ戦略

サイバーセキュリティ基本法は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、政府に対して、サイバーセキュリティ戦略を定めることを義務付けている（第 12 条第 1 項）。

サイバーセキュリティ戦略には、次に掲げる事項が定められる（第 12 条第 2 項各号）

① サイバーセキュリティに関する施策についての基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保に関する事項

③ 重要社会基盤事業者等におけるサイバーセキュリティの確保の促進に関する事項

④ その他サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項

なお、内閣総理大臣は、サイバーセキュリティ戦略の案について閣議決定を求めなければならず（第 12 条第 3 項）、政府は、同戦略を策定したときは、遅滞なくこれを国会に報告するとともに、インター

ネット等で公表しなければならない[53]（第 12 条第 4 項）。

c　内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンターは、次の事務をつかさどる（内閣官房組織令第 4 条の 2 第 1 項各号）。

① 情報通信ネットワーク又は電磁的記録媒体[54]を通じて行われる行政各部の情報システムに対する不正な活動の監視及び分析

② 行政各部におけるサイバーセキュリティの確保に支障を及ぼし、又は及ぼすおそれがある重大な事象の原因究明調査

③ 行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助

④ 行政各部におけるサイバーセキュリティの確保に関し必要な監査

⑤ その他行政各部の施策に関するその統一保持上必要な企画立案及び総合調整のうちサイバーセキュリティの確保に関するもの

同センターは、①に基づき、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）を運用しており、24 時間態勢でサイバー攻撃等の不審な通信の横断的な監視、不正プログラムの分析や脅威情報の収集を実施し、各組織へ情報提供を行っている[55]。

（イ）不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律は、高度情報通信社会の健全な発展に寄与することを目的として、不正アクセス行為等を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めている。

防衛出動時には、武力の行使に際し自衛隊が国内法令に従えない場合があるとしても、自衛隊法第 88 条の要件を満たしている限りにおいて、同法に基づく正当な行為として違法性が阻却されるものと考えられている[56]。したがって、武力の行使の一環として不正アクセス行為等に該当す

---

53 令和 2 年 8 月 19 日時点の最新のサイバーセキュリティ戦略は、平成 30 年 7 月 27 日のものであり、内閣サイバーセキュリティセンターのウェブサイト上で公開されている。内閣サイバーセキュリティセンター『サイバーセキュリティ戦略』平成 30 年 7 月 27 日、https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf.

54 電磁的記録媒体とは、「情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体」をいう（サイバーセキュリティ基本法第 2 条）。

55 内閣官房内閣サイバーセキュリティセンター（NISC）『サイバーセキュリティ関係法令 Q&A ハンドブック Ver.1.0』、令和 2 年 3 月 2 日、13 頁。

56 「衆議院議員岡田克也君提出『武力攻撃事態における我が国の平和と独立並びに国及び国民の安全の確

る行為を行う場合は違法性が阻却されると考えられ得る一方、それ以外の場合については、この法律に従って刑事罰の対象とされる可能性がある。よって、以下では、不正アクセス行為等について概説することとする。

a　不正アクセス行為

不正アクセス行為は、他人のコンピュータに無権限でアクセスする行為であり、当該行為はさらに、不正ログイン[57](第 2 条第 4 項第 1 号)及びコンピュータプログラムの不備を衝く行為[58]（第 2 条第 4 項第 2 号、第 3 号）の 2 類型に分けられる。

なお、不正アクセス行為の禁止（第 3 条）に違反した者は、3 年以下の懲役 又は 100 万円以下の罰金に処せられる（第 11 条)。

b　その他の禁止行為

① 他人の識別符号を不正に取得する行為[59]（第 4 条）
② 不正アクセス行為を助長する行為[60]（第 5 条）
③ 他人の識別符号を不正に保管する行為[61]（第 6 条）
④ 識別符号の入力を不正に要求する行為[62]（第 7 条）

保に関する法律案』等有事関連三法案に質問に対する答弁書」内閣衆質 154 第 74 号、平成 14 年 5 月 31 日、16-17 頁。

[57] 他人の識別符号を悪用することにより、本来アクセスする権限のないコンピュータを利用する行為、すなわち、正規の利用権者等である他人の識別符号を無断で入力することによって利用制限を解除し、特定利用ができる状態にする行為。コンピュータ・ネットワークを通じて行われるものに限定されている。警察庁サイバー犯罪対策プロジェクト「不正アクセス行為の禁止等に関する法律の解説」6-8 頁、https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf.

[58] この行為は、いわゆるセキュリティ・ホール（アクセス制御機能のプログラムの瑕疵、アクセス管理者の設計上のミス等のコンピュータシステムにおける安全対策上の不備）を攻撃する行為である。セキュリティ・ホールがあるシステムに対して、特殊な情報又は指令を入力することにより、本来は識別符号を入力しなければ行うことができない特定利用ができる状態にする行為が該当する。コンピュータ・ネットワークを通じて行われるものに限定されている。同上。

[59] この禁止に違反した者は、1 年以下の懲役又は 50 万円以下の罰金に処される（不正アクセス行為の禁止等に関する法律第 12 第 1 項第 1 号)。

[60] 不正アクセスを助長する行為とは、業務その他正当な理由による場合を除いて、アクセス制御機能に係る他人の識別符号を第 3 者に提供する行為をいう。提供される識別符号について、どの特定電子計算機の特定利用に係るものであるかが明らかでない場合も禁止されている。警察庁サイバー犯罪対策プロジェクト「不正アクセス行為の禁止等に関する法律の解説」9-10 頁。この禁止に違反した者は、30 万円以下の罰金に処される（不正アクセス行為の禁止等に関する法律第 13 条)。この禁止に違反して、相手方に不正アクセス行為の用に供する目的の情を知ってアクセス制御機能に係る他人の識別符号を提供した者は、1 年以下の懲役又は 50 万円以下の罰金に処される（不正アクセス行為の禁止等に関する法律第 12 条第 1 項第 2 号)。

[61] 不正アクセス行為に供する目的での保管に限られる。この禁止に違反した者は、1 年以下の懲役又は 50 万円以下の罰金に処される（不正アクセス行為の禁止等に関する法律第 12 第 1 項第 3 号)。

[62] いわゆるフィッシング行為。この禁止に違反した者は、1 年以下の懲役又は 50 万円以下の罰金に処される（不正アクセス行為の禁止等に関する法律第 12 第 1 項第 4 号)。

（ウ）刑法

刑法は元来、コンピュータデータの不正な改ざんやコンピュータシステムに対する攻撃を想定していなかったため、そうした行為の処罰規定を持っていなかったが、情報化社会の進展に対応して整備が進められていった。下表は、サイバー攻撃又はその前段階の行為等（不正アクセス行為等を除く。）を対象とした行為の犯罪化の過程である。

表5-1　関係刑法規定の新設及び改正の状況

	関係刑法規定の新設及び改正の内容
昭和62年	○ 電磁的記録の概念の導入（第7条の2） 刑法上、電磁的記録とは「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう」。例として、ハードディスク、USBメモリ、DVD-R等に保存された記録が該当する。 ○ 以下の犯罪の新設 ・電磁的記録不正作出罪（第161条の2第1項及び第2項） ・不正作出電磁的記録供用罪（第161条の2第3項及び第4項） ・電子計算機損壊等業務妨害罪（第234条の2） ○ 以下の犯罪の客体に電磁的記録を追加 ・偽造公文書行使等罪（第158条） ・公用文書等毀棄罪（第258条） ・私用文書等毀棄罪（第259条）
平成23年	○ 以下の犯罪の新設 （サイバー犯罪に関する条約締結に関連する法整備の一環） ・不正指令電磁的記録作成・提供罪（第168条の2第1項） ・不正指令電磁的記録供用罪（第168条の2第2項） ・不正指令電磁的記録取得・保管罪（第168条の3）

刑法上も、不正アクセス行為の禁止等に関する法律の場合と同様に、武力の行使の一環としてサイバー攻撃等を行う場合には違法性が阻却されると考えられ得る一方、それ以外の場合については、上述の犯罪として刑事罰の対象とされる可能性がある。よって、以下では、昭和 62 年に新設された電磁的記録不正作出罪、不正作出電磁的記録供用罪及び電子計算機損壊等業務妨害罪、並びに平成 23 年に新設された不正指令電磁的記録作成・提供罪、不正指令電磁的記録供用罪及び不正指令電磁的記録取得・保管罪について概説する。

a　電磁的記録不正作出罪

電磁的記録不正作出罪は、人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作る行為を処罰するものである。この犯罪が成立する場合、客体

が私電磁的記録の場合には、5 年以下の懲役又は 50 万円以下の罰金に処せられ、客体が公電磁的記録の場合には、10 年以下の懲役又は 100 万円以下の罰金に処せられる。

b　不正作出電磁的記録供用罪

不正作出電磁的記録供用罪は、不正に作出された電磁的記録を、人の事務処理を誤らせる目的でその用に供する行為を処罰するものである。この犯罪が成立する場合、客体が私電磁的記録の場合には、5 年以下の懲役又は 50 万円以下の罰金に処せられ、客体が公電磁的記録の場合には、10 年以下の懲役又は 100 万円以下の罰金に処せられる。未遂の場合も処罰される。

c　電子計算機損壊等業務妨害罪

電子計算機損壊等業務妨害罪は、電子計算機に対する加害行為を手段とする業務妨害を処罰するものである。この犯罪が成立する場合、5 年以下の懲役又は 100 万円以下の罰金に処せられる。未遂の場合も処罰される[63]。

電子計算機に対する加害行為として、例えば、次の行為等が該当し得る。

① 電子計算機又は電磁的記録の損壊

② 電子計算機に虚偽の情報又は不正な指令を与えること

d　不正指令電磁的記録作成・提供罪

不正指令電磁的記録作成・提供罪は、正当な理由がないのに、他人の電子計算機における実行の用に供する目的[64]で、不正な指令を与える電磁的記録（いわゆるコンピュータ・ウイルス[65]）の作成・提供を刑事罰の対象とするものである。この犯罪が成立する場合、3 年以下の懲役又は 50 万円以下の罰金に処せられる。未遂の場合も処罰される。

なお、コンピュータ・ウイルスの作成・提供に正当な理由がある場

---

63 電子計算機損壊等業務妨害罪の未遂罪は、平成 23 年の改正の際に規定された。

64 「実行の用に供する」とは、不正指令電磁的記録を、電子計算機使用者にはこれを実行しようとする意思がないのに実行され得る状況におくことをいう。すなわち、他人のコンピュータ上でプログラムを動作させる行為一般を指すものではなく、不正指令電磁的記録であることを知らない第 3 者のコンピュータで実行され得る状態に置くことをいう。法務省「いわゆるコンピュータ・ウイルスに関する罪について」6 頁、http://www.moj.go.jp/content/001267498.pdf.

65 いわゆるコンピュータ・ウイルスには様々な種類のものがあるが、他のプログラムに寄生して事故の複製を作成し感染する形態のものに限らず、一般に、トロイの木馬、ワーム、スパイウェアなどと呼ばれるものであっても、不正電磁的記録に当たるのであれば、対象となり得る。同上、3 頁。

合には、この犯罪は成立しない。例えば、専ら、自己のコンピュータで、あるいは、他人の承諾を得てそのコンピュータで作動させるものとして不正プログラムの研究やウイルス対策ソフトの開発を行う場合には、不正プログラムを作成したとしても正当な理由があるといえ、また、他人の電算機における実行の用に供することにも当たらない[66]。

また、ウイルスを発見した者がウイルスの研究機関やウイルス対策ソフトの制作会社に対し、研究や対策ソフトの更新に役立ててもらう目的で、ウイルスであることを明らかにした上で提供する場合も同様である[67]。

e　不正指令電磁的記録供用罪

不正指令電磁的記録供用罪は、正当な理由がないのに、不正プログラムを他人の電子計算機における実行の用に供することを刑事罰の対象とするものである。この犯罪が成立する場合、3 年以下の懲役又は 50 万円以下の罰金に処せられる。未遂も処罰される。

例えば、次の行為が該当し得る[68]。

① 不正プログラムの実行ファイルを電子メールに添付して送付し、そのファイルを、事情を知らず、かつ、そのようなファイルを実行する意思のない使用者のコンピュータ上でいつでも実行できる状態に置く行為

② 不正プログラムの実行ファイルをウェブサイト上でダウンロード可能な状態に置き、事情を知らない使用者にそのファイルをダウンロードさせるなどして、そのような実行ファイルを実行する意思のない使用者のコンピュータ上でいつでも実行できる状態に置く行為

f　不正指令電磁的記録取得・保管罪

不正指令電磁的記録取得・保管罪は、正当な理由がないのに、他人の電子計算機における実行の用に供する目的で、不正指令電磁的記録を取得・保管することを刑事罰の対象とするものである。不正プログラムの保管を開始した時点でこの目的を有していなかった場合であっても、その後、保管を継続する中でこの目的を有するに至った場

66 同上、8 頁。
67 吉田雅之「第 19 章の 2　不正指令電磁的記録に関する罪」大塚仁、河上和雄、中山善房、吉田佑紀編『大コンメンタール刑法第三版 第 8 巻〔第 148 条～第 173 条〕』青林書院、2014 年、352 頁。
68 同上、10 頁。

合には、保管罪が成立し得る。この犯罪が成立する場合、2年以下の懲役又は30万円以下の罰金に処せられる。

例えば、他人の電子計算機における実行の用に供する目的を持って行う次の行為が該当し得る[69]。

① 不正プログラムを自己の使用するパソコンのハードディスクや自己が自由にダウンロードできるサーバに保存しておく行為

② 不正プログラムが保存されている記憶媒体やウイルス・プログラムのソースコードが印刷された紙媒体を所持する行為

イ　自衛隊のサイバー攻撃対処に関する法解釈

（ア）サイバー空間における脅威に関する情報収集

サイバー空間における脅威に関する情報収集は、平素においては、防衛及び警備等の事務に必要な情報の収集整理に関することとして、防衛省設置法第4条第1項4号及び同18号を法的根拠としており、関係法令を遵守して法令の範囲内で適切に実施するものと位置付けられている[70]。

武力攻撃が行われた場合には、それに対する自衛権の行使として自衛隊に対して防衛出動が下令され、武力の行使が認められる。このため、情報収集に関しても、その範囲内において様々な措置を講じ得るものと考えられている[71]。

（イ）サイバー空間の利用を妨げる能力

a　サイバー空間の利用を妨げる能力を行使し得る場合

武力攻撃が発生していることを前提として、自衛隊は、現行法に基づき、武力攻撃を行った相手方によるサイバー空間の利用を妨げることができる[72]。この能力を自衛隊が発揮する場面は、武力の行使の3要件を満たす場合であって、それは存立危機事態も排除されないものと考えられている[73]。

b　サイバー攻撃に起因する武力攻撃事態の可能性

サイバー攻撃であっても、物理的手段による攻撃と同様の極めて

---

69 吉田雅之「第19章の2　不正指令電磁的記録に関する罪」375頁。
70 第201回国会衆議院安全保障委員会議録第4号（令和2年4月7日）、13頁、河野太郎防衛大臣答弁。
71 同上、槌道明宏防衛省防衛政策局長答弁。
72 同上、14頁、河野太郎防衛大臣答弁。
73 第201回国会参議院外交防衛委員会議録第9号（令和2年4月16日）、5頁、槌道明宏防衛省防衛政策局長答弁。

深刻な被害が発生し、これが相手方によって組織的、計画的に行われている場合には、武力攻撃に当たり得ると考えられている[74]。他方、どのようなサイバー攻撃であれば、それだけをもって武力攻撃に当たるかというのは、その時点のさまざまな情勢、相手方の明示された意図、攻撃の手段、態様等を踏まえて個別的に判断せざるを得ない。武力攻撃に当たるサイバー攻撃に関して、着手がいかなる時点であったかということについても、さまざまな情勢を判断して個別具体的に判断されることとなる[75]。

c　サイバー攻撃に起因する存立危機事態の可能性

存立危機事態に該当するか否かの判断は、あくまでも我が国と密接な関係にある他国に対する武力攻撃が発生したということを前提とした上で、我が国の存立が脅かされ、国民の生命、自由、幸福追求の権利が根底から覆される明白な危険がある場合に該当するか否かということになる。サイバー攻撃であっても同様に、具体的な対応については、その事態、推移を個別具体的に見た上で判断するということとなる[76]。

d　マルウェアの作成、保持、解析

サイバー空間の利用を妨げる能力にも応用し得るマルウェアに関しては、必要に応じて自衛隊自ら作成、保持、解析する必要がある。このため、これらの行為は、それ自体禁じられてはいないと考えられており、前述の不正指令電磁的記録作成罪（刑法第 168 条の 2 第 1 項）との関係でも、正当行為として違法性を阻却されるものと考えられている[77]。

（２）国際法

国際法は、条約と慣習国際法からなるが、サイバー・オペレーションを特別に取り扱う条約はほとんど存在せず、締結されたわずかな条約の適用範囲も限定的である[78]。また、サイバーに関する国家実行は軍や情報機関が行

---

74 第 201 回国会衆議院安全保障委員会議録第 4 号（令和 2 年 4 月 7 日）、14 頁、河野太郎防衛大臣答弁。
75 同上。
76 第 201 回国会衆議院安全保障委員会議録第 3 号（令和 2 年 4 月 3 日）、12 頁、河野太郎防衛大臣答弁。
77 第 201 回国会衆議院安全保障委員会議録第 4 号（令和 2 年 4 月 7 日）、13 頁、槌道明宏防衛省防衛政策局長答弁。
78 例えば、欧州評議会を中心として成立したサイバー犯罪に関する条約（2001 年署名、2004 年効力発生）は、インターネットその他のコンピュータ・ネットワークを通じて実行される犯罪に関する最初の国際条約であり、特に、国内立法及び国際協力を助長することにより、サイバー犯罪から社会を守ることを目的とした共通の刑事政策を追求することを主たる目的としている。著作権の侵害、コンピュータ関連詐欺、

う場合が多いことから秘密であることが多く、国家がサイバーに関してどのような国際法上の義務があると考えているのかということも公に表明されることが少ない。このため、サイバー・オペレーションに固有の慣習国際法を特定することは難しい状況にあることから、ここでは自衛隊によるサイバー空間での対応に関係する現時点での我が国政府の国際法解釈について概説する。

ア　国際法の適用可能性

我が国は、国際連合憲章を含む国際法がサイバー空間において適用可能であるとする立場を取っている[79]。しかしながら、国際法の個々の規則及び原則の適用方法については、情報通信ネットワーク技術固有の特性を考慮し、さらなる検討が必要であると述べるにとどまる[80]。

イ　サイバー攻撃に対する自衛権行使の可能性

我が国は、一定の場合には、サイバー活動が国際連合憲章及び慣習国際法上の武力の行使又は武力攻撃になり得、また、サイバー空間を通じた武力攻撃に対し、国家は、国際人道法を含む国際法に従い、国際連合憲章第 51 条において認められている個別的又は集団的自衛の固有の権利を行使し得るとの立場を取っている[81]。

ウ　日米安全保障条約第５条との関係

2019 年 4 月 19 日、日米安全保障協議委員会（日米「2+2」）において、一定の場合にはサイバー攻撃が第 5 条の規定の適用上武力攻撃を構成し得ることが確認された。ただし、いかなる場合にサイバー攻撃が第 5 条の下で武力攻撃を構成するかは、他の脅威と同様に、日米間の緊密な協議を通じて個別具体的に判断される[82]。

児童ポルノ及びネットワーク・セキュリティの侵害について取り扱っており、違法なアクセス、違法な傍受、データの妨害、システムの妨害、装置の濫用、コンピュータに関連する偽造、コンピュータに関連する詐欺等について国内法によって犯罪化することを求めている。また、コンピュータ・ネットワークの捜査や傍受のような権限及び手続についても規定している。ブダペスト条約ともいう。2020 年 8 月 19 日時点の締約国は、65 か国。日本は、2012 年にこの条約の締約国となった。アイルランド、ロシア、スウェーデンについては、欧州評議会の構成国であるが、この条約の締約国ではない。欧州評議会構成国以外の締約国には、日本のほか、オーストラリア、カナダ、イスラエル、フィリピン、米国等がある。他方、中国、インド、北朝鮮、韓国はこの条約の締約国ではない。“Details of Treaty No.185: Convention on Cybercrime,” Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

79 外務省「サイバーに関する G7 の原則と行動」1 頁、https://www.mofa.go.jp/mofaj/files/000160315.pdf.

80 United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 68th Session, UN Document A/68/156/Add.1, September 9, 2013, p. 15.

81 外務省「サイバーに関する G7 の原則と行動」1 頁。

82 外務省「日米安全保障協議委員会共同発表（仮訳）」2 頁、https://www.mofa.go.jp/mofaj/files/000470737.pdf.

エ　『タリン・マニュアル』に対する評価

2013 年、NATO サイバー防衛協力センターのもとで、サイバー空間を利用した行為に適用される国際法に関する研究の成果として『タリン・マニュアル』が取りまとめられた。当該マニュアルは、NATO の公式見解ではなく、サイバー安全保障分野及び国際法分野の専門家によって形成された成果物である。サイバー空間を利用した行為に対して従来の国際法が適用可能であるということを前提としている面で、当該マニュアルと我が国の立場は一致している[83]。

[83] 第 186 回国会衆議院予算委員会第 1 分科会議録第 1 号（平成 26 年 2 月 26 日）、15 頁、石原宏高外務大臣政務官答弁。なお、『サイバー戦に適用可能な国際法に関するタリン・マニュアル』（2013 年）は、平時のサイバーセキュリティに関する内容が追加され、『サイバー・オペレーションに適用可能な国際法に関するタリン・マニュアル 2.0』として改めて 2017 年に出版されている。同マニュアルは、サイバー行動に適用可能な国際法規則を条文の形で記述し解説を付している。Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.