公益財団法人 日本国際問題研究所（外務省外交・安全保障調査研究事業）
平成 26 年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート

「グローバル・コモンズとしてのサイバースペースの課題」

土屋大洋（慶應義塾大学）

1. サイバー攻撃のシナリオ

サイバー攻撃やサイバー犯罪の多発により、サイバースペース全体が不安定になってきている。小説の題材としても取り上げられるようになっており、現実の事件に基づいて構成されているものも多い。人気作家のトム・クランシーがマーク・グリーニーの助けを借りて執筆した小説『米中開戦』においては、軍事的なサイバー攻撃のシナリオが示された。また、マルク・エルスベルグの小説『ブラックアウト』では、2001 年の対米同時多発テロ（9.11）、2008 年のリーマン・ショック、2010 年のイランの核施設に対するスタックスネット攻撃、2011 年の東日本大震災といった事件にヒントを得て、民間の重要インフラストラクチャへのサイバー攻撃が甚大な被害を及ぼす可能性を描いている。

しかし、インターネットそのものがすぐに停止させられるというシナリオは必ずしも示されていない。他の社会的な機能の多くが失われるのに伴い、インターネットやその他の通信手段が失われる可能性は高いが、少なくともサイバー攻撃の初期段階においては、攻撃者側もインターネットに依存しているからである。インターネットがあるからこそ彼らは攻撃ができるのであり、初期段階でそれを使えなくしてしまっては、目的に達することができない。いわば、攻撃者や犯罪者を含めて多くの人にとってサイバースペースがコモンズ（commons）になっていることを示している。

本レポートでは、コモンズとしてのサイバースペースを今一度捉え直し、その課題を検討したい。

2. 土地としてのサイバースペース

コモンズは「共有地」と訳されることが多い。しかし、英英辞書の一つ（New Oxford American Dictionary）を見てみると、「コミュニティ全体に属したり影響を与えたりする土地や資源（land or resources belonging to or affecting the whole of a community）」とも書いてあり、必ずしも土地だけを意味するわけではない[1]。共有地の牧草が、家畜の過放牧で荒れてしまうというとき、問題なのは共有地の土地ではなく、共有地に生えている資源としての牧草であるともいえる。

そうすると、サイバースペースをグローバル・コモンズとして考える場合、世界各国の人々によって共有されている「土地」としてのアナロジーと、「資源」としてのアナロジーの両面から考えることができるだろう。

[1] なお、「commons」は、「common」の複数形ではなく、「commons」という単数名詞として使われている。ギャレット・ハーディン（Garrett Hardin）の「共有地の悲劇」の論文でも、例えば「sharing a commons」という表現があるように、単数形で使われている。Garrett Hardin, “The Tragedy of the Commons,” *Science*, Vol. 162, No. 3859 (December 13, 1968), pp. 1243-1248. http://www.sciencemag.org/content/162/3859/1243

無論、サイバースペースは、物理的な空間に存在する土地としては考えられない。それがどこにあるかと聞かれれば、世界各地に分散しているコンピュータの記憶装置の中であり、そうした装置が取り外されたり、新たに接続されたりすることで、絶えず縮小・拡大を繰り返していることになる。サイバースペースの利用者が増加傾向にある現在では、接続される装置のほうが多く、土地としてのサイバースペースは拡大基調にあるといえるだろう。しかし、やがては、世界人口に比してサイバースペースが飽和状態に陥ったり、人々が使わなくなったりすれば、それが縮小に転じることもあり得ないわけではない。

記憶装置が単に存在するだけではサイバースペースは構成されない。数多くの記憶装置が相互接続されるとともに、そこに収蔵されているさまざまなデータが処理・活用されなければ意味がない（そのデータこそが、サイバースペースの資源だが、これについては後述する）。記憶装置を繋ぐのは多くの場合は各種の有線ケーブルであり、時には無線電波ということになる。

ますます多くの人が携帯電話を使ってサイバースペースにアクセスするようになっている。携帯電話は特定の周波数帯で電波をやりとりできる端末であり、固有の番号を振られ、特定の呼び出し番号にしか反応しないようにプログラムされている。

無線 LAN を使って携帯電話やパソコンなどからサイバースペースにアクセスすることも多くなっている。携帯電話とは違う周波数帯とプロトコル（通信規約）を使ってアクセスすることになるが、外形的にはあまり変わらない。

ラジオやテレビなどの放送も技術的・法的には通信の特殊形態であり、放送用アンテナから一方的に発せられる電波を専用端末が受信することで視聴可能になっている。

マイクロ波や短波を使った通信は、有線ケーブルが使いにくいところで広く使われてきたが、近年では光ファイバーが実用化され、電波に比べて通信容量が飛躍的に大きくなったため、有線ケーブルが優先的に使われるようになってきている。大海を越える国際通信は、19 世紀後半に海底ケーブルが発明されるまでは船舶に依存していた。海底ケーブルが大西洋や太平洋を越えてつながることで、地球の裏まで数時間、数分、数秒でメッセージを送ることができるようになった[2]。

1970 年代に人工衛星が使えるようになると、国際通信は無線に頼るようになったが、1980 年代後半に光ファイバーが実用化され、光ファイバーを使った海底ケーブル（光海底ケーブル）が敷設されるようになると、国際通信はふたたび有線ケーブルの時代に戻っている。

中長距離の陸線でもまた光ファイバーのケーブルが使われるようになっている。オフィスの中、家庭の中ではイーサーネットと呼ばれる回線でコンピュータ同士を繋ぐことが多い。

そして、ここで、データを収蔵する記憶装置とつながり（時には内包しながら）携帯電話やパソコンといった端末からの処理要請を処理する機械を「サーバー」としておこう。上記のような有線・無線の回線は、記憶装置＝サーバー＝端末の間の無数のチャンネルをつなぐことになる。この全体像が、土地としてのサイバースペースになる。

[2] 初期の電信では、人手を使ってメッセージを中継していたため、数時間を要することもあった。

この土地としてのサイバースペースを攻撃するにはどうすれば良いか。それには、それらをつなげる有線・無線の回線を切断すること、あるいは、回線がつながっている装置・端末を破壊することになる。

回線の切断には、まず、それらの物理的な切断がある。海底ケーブルや陸上ケーブルを切断することは可能である。特定のオフィスにつながる回線を切断するために、電柱に架かる回線を切断したり、地下に埋設されているケーブルをマンホールなどからたどって切断したりすることも可能だろう。

無線回線の場合は、使われている周波数を妨害したり干渉したりする電波を出すこと（ジャミング）が考えられる。電波の利用は、場所、周波数、出力に依存している。同じ場所で同じ周波数で、ターゲットを上回る出力で妨害電波を出せば簡単に邪魔することができるだろう。

特定の個人のサイバースペースへのアクセスを邪魔したければ、その人の携帯電話やパソコンなどの端末を破壊したり、奪ったりすることがあり得る。不特定多数をターゲットとする場合には、事業者の装置や端末を破壊したり、不能にしたりすることもあり得るだろう。あるいは電力供給を止めるということも多大な影響を与える。バッテリーの充電がなくなれば、使えなくなる。

放牧地を使えなくするには、囲いを作ったり、武力で脅して近寄らせなかったりといったことが必要であり、かなりのコストを要することになる。しかし、多くの場合、土地そのものを消し去ることは、ほぼ不可能であろう。例えば、島を爆破して海上への露出部分をなくしたり、地形を変えてしまったりはできるだろうが、土地そのものを存在しない状態にするのは難しい。

それに対し、土地のアナロジーで考えるサイバースペースを存在しない状態にするのは比較的簡単である。回線を切断したり、装置・端末を破壊したりするだけで、すぐに消えてしまう。人工のスペースとしてのサイバースペースは、物理的なスペースよりもはるかに脆弱であるといえるだろう。

3. 資源としてのサイバースペース

それでは、土地において提供される資源としてサイバースペースを考えるとどうなるだろうか。土地そのものを消し去るのは難しいとしても、牧草のような資源を使えなくするのは比較的簡単であろう。牧草を枯らすには、家畜に残らず食べさせてしまったり、適切な間隔で水をやらないようにしたり、毒薬をまいたり、アスファルトで舗装してしまったりすることができる。

土地利用は牧草ばかりではない。そこにオフィスビルや家屋を建てたり、商店街を設けたり、鉄道を敷設したりすることもできる。しかし、そうした利用法を妨害する方法はたくさん考えられるだろう。

サイバースペースの資源としてのデータはどうだろうか。サイバースペースで使われる資源としてのデータは無体物であり、デジタル情報である。牧草は再生可能な資源だが、化石燃料は有限の資源である。デジタル情報は、貯蔵・複製されていなければ、再生不可能な資源である。しかし、貯蔵・複製されていれば、簡単に再生可能な資源でもある。化石燃料のように使えば枯渇するものでもなく、電力や記憶装置の制約がなければ、無限の資源だといって良いだろう。

サイバースペースにおける資源としてのデータとは、具体的には何なのか。それは、電子メールのように個人間でやりとりされるメッセージでもあり、ウェブのように不特定多数によって共有・消費されるコンテンツでもある。

しかし、それらの中には有限のものもある。本研究プロジェクトの昨年度の報告書でも指摘したように、ドメインネームや IP（インターネット・プロトコル）アドレスといった、サイバースペース上で一意に決まらなければならない文字列や数列は、共有しにくく、有限性を持つ資源である。apple.com というドメインネームを、コンピュータを作るアップル社や、レコードを作るアップル・レコード社、リンゴを作る農家が共有するのは難しい。

それ以外のデータは、サイバースペース上ではほぼ自動的にコピーされるといっても過言ではない。電子メールが送信されると、メッセージそのものは送信者のコンピュータにも残っているし、途中で経由するサーバーの中にも設定次第では残る。そして、受信者のコンピュータの中で複製される。ウェブページを閲覧するということは、ウェブサーバーの中にある情報を自分のパソコンや携帯電話の中に（一時的にせよ）コピーするという行為に他ならない。

グーグルのような検索エンジンは、世界中で生成されているウェブコンテンツを自動で複製し、それを自社のサーバーの中で保存しており、その複製・保存したコンテンツを参照しながら検索結果を表示し、それに基づいて検索者を元のウェブページに誘導している。元のウェブページが更新・改変されていれば、中身が違ったり、行き着けなかったりすることもある。いずれにせよ、大量のコピーが自動的に生成されている。

無論、グーグル社が検索可能にしているコンテンツは、サイバースペース全体のコンテンツ資源の 4 割程度ではないかと見積もられている。検索エンジンを通じて行き着けないウェブページは、ダークネットと呼ばれることがある。これらは例えば、ID とパスワードを使わないとたどり着けないページや、企業内のイントラネットのように外部からのアクセスを遮断しているコンテンツ、検索エンジンによる複製を拒否しているサイト、どこからもリンクされておらず孤立しているサイトなど、数多くある。個々人のパソコンはサイバースペースの一部でありながら、その中身を他者に自由に見せるようにしている人はまずいないだろう。牧草地のアナロジーでいえば、柵で囲われてたどり着けない牧草、川があって渡れないところにある牧草、そもそも見えないところにある牧草といったところだろう。

そうすると、資源としてのサイバースペースを妨害するにはどうすれば良いだろうか。

まず、データそのものを破壊する行為があるだろう。端末に不正にアクセスして消去したり、改変したりすることが考えられる。最近ではデータをロックしたり、暗号化してしまったりして、本来の所有者がデータにアクセスできないようにし、金銭を要求する脅迫も行われるようになっている。

検閲、ブロッキング、フィルタリングなども、データへのアクセスを阻害する措置である。検閲は、政府当局者などがコンテンツの中身を政治的に判断し、出版・公開を差し止めたり、改変を求めたりする行為である。ブロッキングは、政府当局者や事業者が、あらかじめ決められたリストに基づいて、利用者に特定のコンテンツへアクセスさせないことである。フィルタリングは、利用者自身の判断によって特定のコンテンツへのアクセスを遮断する行為である。親が子供のアクセスするコンテンツをコントロールしたり、スパム・メールがメールボックスに入ってこないようにすることも含まれる。

あるいは、著作権法などを行使することによって、データの利用を阻止することもできる。ただし、この場合の強制力は、相手の法遵守規範のレベル次第であり、悪意を持った相手には意味をなさないだ

ろう。

4. 重要インフラストラクチャとしてのサイバースペース

上記の試論は、あくまでサイバースペースが単体のスペースとして存在しているという仮定の下にある。しかし、実際は、サイバースペースは現実のさまざまなスペースと切り離すことはできない。電子商取引は、ソフトウェアやコンテンツの売買においてはサイバースペースだけで完結する場合もあるが、本や CD、その他の物品の購入にインターネットを使う場合には、物流のネットワークと結びついている。電気やガス、水道、輸送システム、工場などの制御システムと接続されている場合もある（現在ではなるべく切り離す方向になっているが)。軍隊でさえも、調達部門を中心に一般的なインターネットとつながっている。

サイバースペースは、陸、海、空、宇宙に次ぐ第五の作戦領域だと米軍は指摘しているが、実際には、軍事的に見れば、サイバースペースはそれら四つの自然のスペースをつなぐ神経系になっている。例えば、エア・シー・バトルという戦術概念が議論されつつあるが、空軍と海軍が連携するには通信が必要である。並んで歩きながら連携するならまだしも、現代における大規模な軍事作戦は、通信なくして成り立たない。

軍事ばかりでなく、ほとんど全ての社会システムが広義の（インターネットにつながっていないものも含む）サイバースペースに依存するようになっている。つまり、サイバースペースは重要インフラストラクチャそのものであり、その中心的存在でもある。

2001 年の対米同時多発テロ（9.11）を検証した結果、アルカイダが本当に狙っていたのは米国経済の神経網への攻撃であり、米国経済を麻痺させることであったとの見方がされるようになった。いわば、9.11 の数千人の犠牲者は「副産物」であり、本当の狙いは米国経済にあっただろうというのである[3]。

米国経済を日本経済やグローバル経済に置き換え、攻撃者をアルカイダ以外のアクターに置き換えることもできる。どこかのテロリスト・グループがグローバル経済を麻痺させることを狙ってサイバー攻撃を実施するとすれば、何を狙うだろうか。一つには、「土地」としてのサイバースペースの破壊である。先に述べた考えを敷衍すれば、その攻撃は物理的な設備に対する破壊となるだろう。海底ケーブルの回線や陸揚げ局、人工衛星そのものや通信回線、地上局が物理的破壊のターゲットとなる。個々の端末を狙うよりも手っ取り早いであろう。

「資源」としてのサイバースペースを攻撃するならば、ドメインネームや IP アドレスの管理システムを破壊することでかき乱すことができる。例えば、日本国際問題研究所の研究員に電子メールを送ろうとしても、「jiia.or.jp」というドメインネームがどの IP アドレスに対応するのか分からなくしてしまえば、メールは届かなくなる。メールだけなら良いが、サイバースペースに依存を深める金融取引には大きな打撃になるだろう。街中の店舗は、銀行業界の合併淘汰を経て減らされており、窓口業務はすべてのニーズをさばききれないだろう。各所に保管されているデータを破壊・改ざんすることできれば大きな混

[3] ダン・バートン（星睦訳）『ブラックアイス―サイバーテロの見えない恐怖―』インプレス、2003 年、106～107 頁。

乱がもたらされる。

土地に対する攻撃と資源に対する攻撃の両方を合わせた攻撃として EMP（electromagnetic pulse）爆弾の可能性を完全には否定できない。EMP はサイバー戦の前の電子戦の時代にはよく議論されたが、現在ではあまり意識されていない。しかし、現実に起こり得る問題である。1962 年に米軍が太平洋で核実験（Starfish Prime）を行ったが、それが EMP 爆弾と同じ効果を引き起こし、1445 km 離れたハワイの街灯が消え、盗難警報器を鳴らし、マイクロ波通信回線を不能にした。当時はまだパソコンが普及していない時代だったが、現代で同じことが起きれば各種コンピュータを不能にするなど広範な被害が出る可能性がある。

5. 米軍と米インテリジェンス機関の動き

1991 年の湾岸戦争において米軍はハイテク兵器の圧倒的な威力を見せつけた。そして、クリントン政権時代の RMA（軍事革命）や、ブッシュ政権時代のトランスフォーメーションの流れの中で、情報通信技術をいっそう積極的に軍事の中に取り入れてきた。

しかし、1997 年に米軍が行った「エリジブル・レシーバー」演習では、NSA が地域別統合軍の一つである太平洋軍等をサイバー攻撃したところ、太平洋全域の作戦を担う米軍の指揮統制システムを損なうことができた。それ以来、米軍はサイバー攻撃の可能性を懸念し、徐々に対応を行ってきた。

もともとのインターネットの発想に従い、米軍内のネットワークも「自律、分散、協調」の影響を少なからず受けてきた。各軍・各部隊でそれぞれのニーズにあったシステムが構築されてきた。それは、一方では成功であった。米軍の一つのシステムが攻略されても、米軍全体に及ぶ可能性は低い。被害は一部にとどめることができる。しかし、他方では、バラバラのシステムは全体の防御のコストをあげることになる。個別のシステムに応じた防御を行えば、それだけ時間的なコストも金銭的なコストもかかる。一括して守ることはできない。もともと軍は、ヒエラルキー型の中央集権的統制を求める。そこで、米軍は徐々に、情報通信システムのアーキテクチャを変えようとしてきている。

そこでのキーワードが統合情報環境（JIE：Joint Information Environment）である。

米国防総省の資料によれば、米軍の現役の軍人は 140 万人、それに加えて 78 万 3000 人の民間人が請負等で働いている。120 万人の州兵と予備役、550 万人以上の家族と退役兵もいる。それらの人々が世界 146 カ国以上に散らばり、拠点の数は 5000 を超える。ビルや建物の数にして 60 万を上回る。情報通信システムでみれば、システム数は１万を超え、データセンターは 1850 近くもある。サーバーの数は 6 万 5000 台弱、コンピュータその他の端末は 700 万台以上ある。

脆弱性は無数にあるといっても過言ではない。インターネットにつながっていなくても、これだけの人間がいればミスをする。クランシーは『米中開戦』の中で、ウイルスを仕込んだ USB メモリを駐車場に落としておくという作戦を描いている。拾った人の何割かは中身を確かめようと自分のコンピュータにそれを差し込んでしまうだろう。あっという間にシステム全体に影響が及ぶ。

あるいは、自宅で使っている個人的なパソコンや iPad などを職場に持ち込むことを「ブリング・ユア・オウン・デバイス（略して BYOD）」と呼ぶが、BYOD は「ブリング・ユア・オウン・ディザスター（災

厄の持ち込み)」だと揶揄する声もある。もはや、「自律、分散、協調」ではセキュリティに対応できない。

そこで、米軍は、収拾が付かなくなっている情報通信システムを統合し、管理・防御しやすくするためのアーキテクチャ改造をし始めている。それが JIE である。

JIE のキーワードは、安全性（secure)、抗堪性（resilient)、統合性（consolidated）になる。バラバラに運用されていた各種システムを統合して数を減らし、安全かつ使いやすくする。攻撃されないのが一番だが、されてもすぐに回復できる抗堪性が求められる。

こうした改革は民間企業でも常に行われているし、米軍でもこれまでも求められてきた。そもそもジョージ・W・ブッシュ政権時代にドナルド・ラムズフェルド国防長官が求めたトランスフォーメーションは、冷戦時代の重厚長大型の米軍をポスト冷戦時代の機敏な軍隊に変えることであり、情報通信システム等のハイテクの導入も、まさにそのためであった。しかし、システムの肥大化はかえって作戦を困難にしつつあり、オバマ政権の国防予算カットの波の中で、システムのアーキテクチャ見直しは不可避になっている。

新しい環境への移行は、米軍だけではできない。当然のことながら民間の情報通信業界との連携が不可避になる。そこには昔の軍産複合体さながらのサイバー軍産複合体が形成されつつある。ワシントン・ポスト紙のデイナ・プリーストとウィリアム・アーキンが『トップシークレット・アメリカ』で明らかにしたように、9.11 以降の米国は、湯水のように情報通信システムを使ってきた。

6. ハッカーたちの反応

サイバーセキュリティが問題になり、サイバースペースへの軍事的な影響が拡大する現状に対して、ハッカーたちはどう反応しているのだろうか。

毎夏、米国ラスベガスのカジノ併設巨大ホテルで「デフコン」が開かれる。軍事用語の「デフコン」は「ディフェンス・レディネス・コンディション」の略で、防衛準備態勢のレベルを示すが、ネット業界での「デフコン」といえば、1993 年から開かれているハッカーのための会議である[4]。2014 年 8 月 7 日から 10 日に開かれた 22 回目のデフコンには 1 万 4000 人が参加した。

ハッカーといっても、現在のマスコミで使われるハッカーとは違う。もともとハッカーは技術に精通した人たち一般を指す言葉で、必ずしも犯罪行為に携わる人たちではない。彼らの技能が常人離れしていたために、ハッカーは中世の魔女のような扱いを受け、いつの間にか悪人の代名詞になってしまった。実際、デフコンでさまざまなハッキングを実演し、「ほら」と結果を見せられると、素人には魔法を見せられている気がする。

しかし、デフコンに集うハッカーは、本来の意味のハッカーであり、公然と悪事を働く人はほとんどいない。むしろ、技術の脆弱性を公表・共有することがデフコンでは奨励されている。最初に見つけ、

[4] 会議の創設者ジェフ・モスは、友人の送別パーティーをカジノの街ラスベガスで企画していた。しかし、その主役の友人がパーティーに参加できなくなったため、ハッカーの友人たちを招いたのがデフコンの始まりである。1983 年に公開されたハッカー映画『ウォーゲーム』で核戦争のターゲットになるのがラスベガスだったことから、遊び心で会議をデフコンと名付けた。

実演することを誇りとしている。

実はデフコンには少なからぬ政府職員が聴衆として参加している。連邦捜査局（FBI）や国防総省、州や市などの警察関係者などである。彼らからすれば、最新の技術情報や犯罪に使われる可能性のある手法を学ぶことができる。ハッカーたちもそれをある程度受け入れてきたが、会場で「連邦政府職員を見分けろ（spot the fed)」というゲームが毎年行われ、見つかった職員は壇上に上げられ、さらし者にされてしまう。

NSA 長官であり、サイバー軍の司令官でもあったキース・アレグザンダーがデフコンに登場したことがある。NSA の契約社員だったエドワード・スノーデンが機密を暴露したのは 2013 年の 6 月だが、その前年の 2012 年のデフコンである。陸軍の大将として普段は軍服を着ているアレグザンダーが、この日は黒の T シャツにジーンズという姿で現れた。アレグザンダーは、第二次世界大戦中のドイツのエニグマ暗号や、日本のパープル暗号の話を持ち出し、政府と民間の協力が必要なのだと聴衆に呼びかけた。政府と民間は責任を共有しているというのが彼のメッセージであった。

しかし、ハッカーと NSA の蜜月は、翌年のデフコンでは消え失せていた。2013 年 6 月にスノーデンの機密暴露が行われ、2 ヶ月後に開かれたデフコンでは、「連邦政府よ、我々はしばらく離れている必要があるね」というかけ声が使われ、NSA／サイバー軍だけでなく、その他の連邦政府職員もデフコンから閉め出された。

米国の IT 企業は、米国政府と密接な関係を築いてきた。しかし、その関係はスノーデンの告発で変わり始めている。IT 企業は公然と政府を批判し始め、簡単には政府からの情報共有要請に協力しなくなってきている。今後、大手の IT 企業がどこまで政府からの要請を突っぱねられるのかはまだ分からない。しかし、個人のハッカーたちの間では、再び政府への警戒感が高まってきている。

ハッカーたちはサイバースペースにおけるプライバシーを尊重している。しかし、彼らの技術がいったん「敵」に対して向けられれば、さまざまな情報の暴露（ウィキリークス事件やスノーデン事件のように）に向かったり、サイバー攻撃に使われたりする。米国政府だけでなく、各国政府にとってもハッカーたちとどう折り合いを付けるかが課題の一つになるだろう。

7. おわりに

コモンズとしてサイバースペースをとらえれば、それは単なる共有地というだけでなく、「土地」のアナロジーと、「資源」のアナロジーの両方を見なくてはならなくなる。サイバースペースの場合、物理的な土地は存在しないが、それは世界中の多様な設備の集合として見るべきであり、常に大きさを変えつつあり、むしろ複合主体ないし社会のアナロジーとして考えるほうが適切かもしれない。しかし、それ故に、脆弱なコモンズかもしれない。

サイバースペースの資源は、一般的にはデータやコンテンツといったデジタル情報だが、それと物理的な設備を支える法制度やルールも含めるべきだろう。法制度やルールは、インターネット・ガバナンスという言葉で議論が続けられている一方、データやコンテンツはプライバシーの文脈で議論されることが多い。しかし、セキュリティという面からもデータやコンテンツの保護を考えておく必要があるだ

ろう。

グローバル・コモンズとして見た時、サイバースペースの今後の課題は、これまで注目されてきたような「資源」としてのコモンズに対する攻撃はいうまでもなく、「土地」としてのコモンズに対する攻撃、言い換えれば物理的な設備としてのコモンズに対する攻撃にいっそう備えるということになるだろう。電力設備、海底ケーブル、人工衛星といった重要インフラストラクチャを対象に含めた群発攻撃に備えなければならない。群発攻撃とは、物理的な設備に対する攻撃とデータ／コンテンツ／プログラムに対する攻撃の両方を含む、複数のターゲットを狙った同時多発的な攻撃である。

かつてのサイバー攻撃は、無料で入手できるツールを使って誰でもできた。しかし、サイバーセキュリティに対する意識が高まってきている現在、最前線のサイバー戦はプロ同士のものになりつつある。そうした争いが、サイバースペースというコモンズをさまざまな形で荒らし始めている。

主要参考文献

- Hardin, Garrett, “The Tragedy of the Commons,” *Science*, Vol. 162, No. 3859 (December 13, 1968), pp. 1243-1248. http://www.sciencemag.org/content/162/3859/1243
- エルスベルグ、マルク（猪股和夫、竹之内悦子訳）『ブラックアウト（上・下）』角川文庫、2012 年。
- クラーク、リチャード、ロバート・ネイク（北川知子、峯村利哉訳）『世界サイバー戦争―核を超える脅威　見えない軍拡が始まった―』徳間書店、2011 年。
- クランシー、トム、マーク・グリーニー（田村源二訳）『米中開戦 1～4』新潮文庫、2013 年～2014 年。
- バートン、ダン（星睦訳）『ブラックアイス―サイバーテロの見えない恐怖―』インプレス、2003 年。
- プリースト、デイナ、ウィリアム・アーキン（玉置悟訳）『トップシークレット・アメリカ―最高機密に覆われる国家―』草思社、2013 年。