中央大学政策文化総合研究所年報　第 20 号（2016）pp. 71-85

重要インフラを標的とするサイバー攻撃と国際安全保障への影響

出　口　雅　史*

Cyber Attack on Critical Infrastructure and Its Influence on International Security

DEGUCHI Masafumi

Since the internet appeared, with increasing cyber threats, the vulnerability of critical infrastructure has become a vital issue for international security. Although cyber attack was not lethal in the past, new type of cyber assaults such as stuxnet are able to damage not only computer system digitally, but also critical infrastructure physically.

This article will investigate how the recent cyber attacks have threatened critical infrastructure and their influence on international security. The impact of the September 11 terrorist attacks strengthened the necessity of protecting critical infrastructure, but the scope of cyber attack was limited in those days. Stuxnet that destroyed the Iranian nuclear facility has had a strong impact because it proved that cyber attack could be a strategic weapon.

While the threats of cyber attack have been increasing, corresponding methods are not developed enough to protect critical infrastructures. In the sphere of cyber security, an offensive is generally superior than a defensive because the origins of cyber attacks can be hidden and costs of the attack are considerably low. The norms of cyber security have been undeveloped, so that states will not expect the international cooperation to resolve conflicts in cyber issues that are related with political matters. This environment will lead states to expand the capability of cyber attack to deter the decisive destruction on critical infrastructure.

キーワード：サイバーセキュリティ，サイバー攻撃，重要インフラ，スタックスネット
Key Words: Cybersecurity, Cyber Attack, Critical Infrastructure, Stuxnet

＊　中央大学政策文化総合研究所準研究員
Associate Fellow, The Institute of Policy and Cultural Studies, Chuo University

はじめに

従来の通信システムと比べて，極めて高速かつ低コストの通信を可能にしたグローバルなネットワークとしてのインターネットが20世紀末から急速に普及して以来，サイバー攻撃の脅威は質量共に拡大する傾向にある．近年では，サイバー攻撃は国際安全保障を揺るがす脅威として認識されるようになり，サイバー攻撃はただの犯罪行為ではなく，政治的，軍事的に国家が対応すべきハイ・ポリティックスの問題として取り上げられるようになった[1)]．本論文では多種多様なサイバー攻撃の中でも，物理的被害を含む重要インフラに対する攻撃の登場が国際安全保障にどのような影響を及ぼすのか検討する．サイバー攻撃の中で最も頻繁に発生しているものは，データの改ざんや流出といった情報の安全性に関わる種類の攻撃であり，このような攻撃によっても機密情報の流出といった深刻な被害が生ずるが，それらの攻撃は従来から行われてきたインテリジェンスの延長線上にあるサイバースパイ活動であり，この攻撃自体が人命を損なう武力紛争を招くものではない．

それに対して重要インフラへのサイバー攻撃は，現代国家にとって必要不可欠となったコンピュータ制御を標的とすることで，国家機能の基盤である重要インフラを機能停止させることが可能となる．これに対してはアメリカ政府が自衛権の発動を含む強力な対応を行うことを表明しており，サイバー攻撃は潜在的に武力攻撃に匹敵するような脅威であると見なしていることが分かる．

しかし，エストニアへの大規模サイバー攻撃やイランの核燃料施設に対して使われたスタックスネットのケースを見た場合，実際には武力攻撃に相当する脅威として反撃を行うといった手段は取られておらず，むしろ被害そのものを公開しないという対応が取られたこともあり，総じて重要インフラへのサイバー攻撃を受けた被害国は抑制的な反応を示している．このことはエストニアが攻撃の発信源とされるロシアに対して取り得る対抗手段が限定されるという政治的事情に加えて，サイバー攻撃の性質が武力紛争へのエスカレートに至ることを防いでいるのではないかという仮説が成り立つ．リッド（Thomas Rid）はこの点についてサイバー攻撃の暴力性という観点から，サイバー攻撃は従来の武力攻撃とは区別されると述べており，批判的な見解を示している[2)]．本論文ではこの点を踏まえサイバー攻撃と武力攻撃の違いを考察し，何故サイバー攻撃が重大な脅威として認識されているにも拘わらず武力攻撃に相当するような対応を取ることが難しいのかを明らかにしたい．また，サイバー攻撃が物理的被害を伴う性質を帯びた一方で，サイバー攻撃に対する規範化が不明確な現状にあり，サイバー軍拡をもたらしうるという点で国際安全保障の不安定要素になる可能性があることを考察に加えたい．

1. 重要インフラへのサイバー攻撃

1.1 国際安全保障とサイバー攻撃

始めに，サイバー攻撃の脅威と国際安全保障がどのような関係があるのか整理する．安全保障とは，ウォルファーズ（Arnold Wolfers）の定義によると「獲得した価値に対する脅威の不在」であり，国家の生存や国民の生活水準の維持といったものが「獲得した価値」に該当する[3)]．国際政治の代表的な理論であるリアリズムの伝統では，国際社会は上位の統治形態が存在しないという意味においてアナーキーな性質を帯びているとみなされ，安全保障を追求する為に，国家は軍事的なパワーを保有し，外交を駆使してきた．国際政治の舞台では，伝統的に安全保障とは，国家の生存を追求する国家安全保障を意味してきたが，近年では「人間の安全保障」や「環境安全保障」などの「非伝統的安全保障」が登場してきており，必ずしも国家の生存だけが安全保障の目的とは限らなくなっている．本論文では国際安全保障を，伝統的な国家安全保障に加えて，核の拡散や環境問題などの国際社会全体に関わる脅威を抑制し「獲得した価値」を維持することと定義する．サイバーセキュリティは国家の生存や国民の財産に関わる為，国家安全保障とも密接に関係するが，国境を越えてグローバルな通信が可能なサイバー空間を舞台し，非国家主体の影響など国家以外のアクターが影響力を増していることから，国家安全保障の枠を超えた問題であると捉え，国際安全保障の一部として取り扱う．

次に重要インフラへのサイバー攻撃の脅威について述べる前に，サイバー攻撃について概略する．サイバー攻撃には多様な定義が存在するが，最大公約数的に定義するならば，大きく２つの要素から構成される[4)]．第１の要素は，原則的に ICT（情報通信技術）を用いてコンピュータシステムを標的とした攻撃だということであり，第２の要素はサイバー攻撃が運動エネルギーを用いた攻撃ではないことである．例えば無人機による攻撃は，確かに無人機の制御に情報通信技術が用いられているが，無人機から射出されるミサイルや爆弾は運動エネルギーを用いた攻撃であり，第２の要素に該当しない為にサイバー攻撃とは言えない．これに対して，交通機関の制御システムに不正アクセスしデータを改ざんすることでシステムの機能が一時停止し，交通管制の機能不全から事故が起こったというケースは，結果的に物理的被害が生じたとしてもサイバー攻撃である．サイバー攻撃の定義については，特定の政治的動機に基づくもののみを対象とすることもあるが，本論文では前述のような広義の定義として取り扱う．

サイバー攻撃の脅威は，２つの理由で年々拡大傾向にある．１つは，社会全体の情報化が進展することでサイバー攻撃の対象が増加し，より多くの攻撃が可能になったことである．

インターネットユーザーの増加に加えて，近年ではIoT（Internet of Things，モノのインターネット）が普及し始めたことで，家電から自動車に至るまで社会に普及する様々なモノにコンピュータが組み込まれインターネットに接続されるようになり，従来よりも一層サイバー攻撃の対象が拡大傾向にある，攻撃対象の増加は大規模サイバー攻撃による被害の拡大を招く可能性があり，社会全体のサイバー攻撃に対する脆弱性が深刻化することを意味する．

インターネットは相互通信的なシステムであることから，インターネットに接続した時点でサイバー攻撃を行うことが可能であると同時にサイバー攻撃を受ける危険性も発生する．その為サイバーセキュリティ対策として，インターネット自体に接続しないという方法が考えられる．しかし，インターネットに接続しなければ，サイバー攻撃を受ける可能性がないというわけではない．USB接続を経由して不正ファイル（マルウェア）が侵入したり，サイバー攻撃を行う要員が標的施設に直接送り込まれて不正な操作を受けたりする事態が実際に起きている[5)]．事実上全てのコンピュータ制御を受ける装置はサイバー攻撃を受ける可能性があると言えるだろう．サイバー攻撃はインターネットを媒介に容易に国境を越えて一瞬で世界の別の地域に到達することが可能である為，インターネットに接続している施設は世界の裏側から瞬時にサイバー攻撃を受け情報の流出や機能の停止といった被害を受ける恐れがある．このようにサイバー攻撃は越境的な性質を帯びており国内だけでは対処しきれない問題である一方で，サイバー攻撃における規範が未発達である為，国境を超えたサイバー攻撃を摘発することが難しい状況にある．とりわけ，政治的な動機で行われるサイバー攻撃については，国家が関与していることもあり，尚更犯人を摘発する国際協力が成立しにくい状態に陥ってしまう．

1.2 サイバー攻撃の脅威の変容

サイバー攻撃の脅威は，物理的な被害を含む重要インフラへのサイバー攻撃の登場により一層深刻なものになった．重要インフラとは，国家の社会経済活動を支える上で特に重要な領域の産業や施設を項目別に定義したものである．重要インフラがサイバー攻撃の領域で注目される原因は，高度情報化が進んだ現代社会では，大半のインフラがコンピュータ制御を受けるようになり，それだけサイバー攻撃に対する社会全体の脆弱性が増しているからである．もし重要インフラが大規模なサイバー攻撃を受ければ，広範囲の停電や交通機関の混乱といったライフラインに関わる被害が想定される．もし，この攻撃が国家によって主導されるような複合的かつ持続的なものであった場合は，一時的に近代的な国家の機能を妨害される恐れすらある．

重要なインフラであればサイバー攻撃に対して相応のセキュリティ対策がされるはずで

あるが，それにも拘わらず脆弱性が改善されない原因は何であろうか．サイバー攻撃に対する脆弱性は，コンピュータに対する依存度とセキュリティ能力の 2 つの要素で決定される．コンピュータへの依存度が高まれば高まるほど，サイバー攻撃を受ける機会が拡大し，また攻撃によって生ずる損害も深刻化することになる．アメリカのように卓越した情報通信技術を有する先進国において特にサイバーセキュリティへの関心が高いことは，依存度の高さの裏返しであると言える．アメリカ軍は RMA（軍事における革命）によって湾岸戦争以降，情報通信技術による軍事的革新に世界で最も成功したが，一方で情報通信技術に依存したシステムがアメリカ軍にとってのアキレス腱となり，サイバー攻撃に対する脆弱性を高めることになった．高度情報化したアメリカ軍に対抗する為に他国がサイバー攻撃能力を利用する可能性は既に 1990 年代から指摘されてきた[6]．この原理は民間においても同様であり，クリントン政権が 1998 年に発表した PDD-63 で重要インフラの脆弱性が指摘されている[7]．PDD-63 は重要インフラの脆弱性に対する危機感を示し「物理攻撃，サイバー攻撃の標的となるサイバーシステムを含む我々の重要インフラが抱えている脆弱性を排除する必要な手段を取るべきである」と言及している．

ただし，1990 年代までに行われたサイバー攻撃の脅威は限定的であり，安全保障問題としては当時マイナーな課題であった．このような認識を大きく変える一因となったのが，2001 年の 9.11 同時多発テロである．9.11 テロはサイバー攻撃ではないが，甚大な被害を受けたことから重要インフラ保護が重視されるようになり，事件後にアメリカで創設された国土安全保障省（DHS）が国内の重要インフラの保護を担当し，サイバー攻撃への対応もその中に含まれることになる．

2007 年にアメリカのアイダホ国立研究所が行った制御システムに対するサイバー攻撃実験「オーロラテスト」では，サイバー攻撃で電力網のシステムをどのようにして物理的に破壊可能であるかのデモンストレーションが行われた．この実験では，ディーゼル発電機の回路遮断機を操作して異常動作を引き起こすことで発電機を損傷させ操業停止させる様子が動画で公開された[8]．

サイバー攻撃の標的となる産業用制御システムは SCADA と呼ばれ，コンピュータによって製造，送電などの産業プロセスの制御と監視を担っている．こうした制御装置は自動化だけでなくコンピュータの集中管理により操業の効率化に貢献するが，遠隔操作の操業に依存した結果，サイバー攻撃によって SCADA が単に機能停止するだけでなくシステムそのものが書き換えられてあたかも正常に操業しているかのように見える為，被害に気づくのが遅れるという問題も起きている[9]．産業用制御システムにとって最も重要なことは正常に操業を続けることであり，運用に支障をきたす物理的被害が生ずる攻撃は，スパイ型の攻撃と異なり発見が容易であるはずだが，攻撃側の洗練性次第である程度被害を隠蔽

することが可能である．もし異常な事態が起きればコンピュータ側からのシグナルが起こる為，異常停止しない限り操業を続ければいいという固定観念が被害に気付くことが遅れる原因となっている．

2. 重要インフラの攻撃事例

2.1 エストニアへのサイバー攻撃

国際的に注目を浴びた最も有名なサイバー攻撃の 1 つが，2007 年のエストニアへのサイバー攻撃である．この攻撃で使われた手法は DDoS（分散型サービス拒否攻撃）と呼ばれ，主に遠隔操作により大量に 1 つのシステムへアクセスを集中させることで標的の機能を停止させる攻撃である．この DDoS は，ハクティビスト（政治的ハッカー）の間では古くから行われている比較的単純な方法の攻撃である．エストニアのケースで注目を浴びたのはその規模と組織的な連携にあり，エストニアのマスメディア，政府，金融関連の Web サービスの多くが一時的に停止するという被害を受けた．国家そのものを標的とするような大規模かつ組織的な攻撃であった為，「サイバー戦争」が現実化したような大きなインパクトを国際社会に残した[10]．

エストニアのケースで注目すべきは，エストニアが NATO に対して北大西洋条約第 5 条に基づく集団的自衛権の要請を検討したが，結果的には断念したことにある[11]．エストニアに対するサイバー攻撃は，集団的自衛権の根拠となる武力攻撃とは認められなかった．ただし，その後 2014 年に NATO はサイバー攻撃を第 5 条の適用範囲であると宣言しており，サイバー攻撃が武力攻撃の一種として認められようになった[12]．一方で実際にサイバー攻撃が武力攻撃として認定された事例はない為，どのような条件下であれば集団的自衛権が行使し得るか不明確である．最大の問題は，エストニアへの攻撃は金融やマスメディアなど国家全体にまたがるサービスを一時的に停止させるほど大規模なものであったが，人命を損なうような人的被害を出したわけではないことである．原則的に国際法では戦争行為が禁止されている一方で，例外的に自衛権の行使による反撃が認められるのは，武力攻撃が人命の損失を含む重大な結果を引き起こすからであり，1 人の人命も失っていない状態で武力行使を引き起こすような対応が認められるかは従来の法規範と照らし合わせると極めて厳しいと言わざるを得ないだろう．

2.2 スタックスネットの登場と物理的被害を伴うサイバー攻撃

エストニアへのサイバー攻撃が大規模性で注目されたことに対して，2010 年に発見されたスタックスネット（Stuxnet）は，重要インフラに対して物理的被害を生じさせたとい

う点でエストニアのケースとは異なり，標的の性質，洗練性，損害から重要インフラに対するサイバー攻撃としては最も顕著な事例となった．スタックスネットとはイランのナタンツ（Natanz）にある核燃料濃縮施設に設置されてある遠心分離機の制御システムに感染し，遠心分離機に物理的損害を与えて一時的に停止させたことで知られるマルウェアの名称である[13)]．スタックスネットの存在が公表されたのは 2010 年であるが，実際に活動していたのはその 1 年以上前からであり，中東を中心に数万台のコンピュータに感染した．スタックスネットは，ナタンツの核施設で使われていたシーメンス社製の制御システムを主な標的として余計な被害を出さないように設計されており，高い隠密性を備えていた[14)]．その為，長期間潜伏し適切なタイミングで駆除されることなく効果を発揮することが可能になったと考えられる．スタックスネットは，イラン政府によって実際に被害が生じたことが報告され，核施設という安全保障上極めて重要な施設に物理的な損傷を与えたサイバー攻撃であるとして国際的な注目を集めた．スタックスネットに感染した制御装置によって遠心分離機の回転数が異常に操作され，遠心分離機の構成装置の一部が破損し，イランの濃縮プロジェクトに遅延が生じたと見られている[15)]．遠心分離機のモーター回転速度を異常に上げた後に再び下げることで振動や歪みによる故障を狙ったものと考えられる．スタックスネットの具体的な侵入経路を当事者であるイラン政府が明かすことはセキュリティ上あり得ないが，核施設のような秘匿性が高い施設をインターネットに常時接続させることは考えにくい為，USB 接続を使用した侵入などが想定される．DDoS 攻撃と異なりスタックスネットのように産業制御装置を標的としたサイバー攻撃には，通常のコンピュータ技術だけでなく産業システムに対する知識ももちあわせていなければ実行することはできない為，個人的なハッカーが興味本位で実行したというのは想定し難い．スタックスネットは Windows の未知の脆弱性を利用した複数のゼロデイ攻撃が利用されており，技術的洗練性では 2007 年のエストニア攻撃よりもはるかに水準が高いと評価される．それに加えて，ウラン濃縮を行う遠心分離機を標的としていることから，イランの核開発を妨害するという政治目的があると考えられるが，NewYork Times のサンガー（David Sanger）記者によればアメリカとイスラエルが「Olympic Games」というコード名が与えられた作戦で，事前に該当施設の情報を収集した上でシーメンス社と協力しスタックスネットを作成して送り込んだ（Sanger 2012）．このような攻撃をアメリカ政府とイスラエル政府が公式に認めたことはないが，前記の NewYork Times の記事ではスタックスネットの計画はブッシュ Jr. 政権の時に既に計画されており，空爆によってイランの核施設を破壊する代替手段として引き継がれたと報じられている．

スタックスネットのインパクトは被害そのものよりも，この種の「サイバー兵器」の実用化が及ぼす将来的な危険性にあるだろう．仮に，原子力発電所の原子炉をメルトダウン

させることを目的としたサイバー攻撃が実施され，それが成功した時の被害は，既存のサイバー攻撃とは比較にならない規模になるだろう．また，スタックスネットの事例で注目すべきは，この攻撃を行った主体からは勿論，被害者であるイランからも自らこの事件を公表することはなく，この事件が明るみに出たのはスタックスネットが何らかの原因でインターネット上に流出しマルウェアが解析されたからである．イランが安全保障上極めて重要な核燃料施設に対する物理的被害を伴うサイバー攻撃に対して直接的な反応を示さなかった原因はいくつか考えられる．第一に誰がこの攻撃を行ったか判明しなかった，または明確な証拠を得られなかった為，対抗措置を取る正当性が確保できなかったことが考えられる．また，イランの核燃料施設が攻撃を受けたことが安全保障上の機密事項にある為，攻撃を公開することそのものがリスクだと捉えられた可能性もある．

スタックスネット以外にも重要インフラに物理的な損傷をもたらす事例は年々増加している．2007年にシリアの核開発施設とされる建造物をイスラエルが爆撃した際に行われたのは戦術レベルで武力攻撃を支援するタイプのサイバー攻撃であった．別の言い方をすれば，サイバー攻撃と武力攻撃が一体化したと言ってもいいだろう．クラークによれば，シリアが北朝鮮との協力により建造していた核関連施設を破壊する目的でイスラエルが空爆を行ったが，レーダー施設が機能しないよう事前にサイバー攻撃を仕掛けていた為，シリアは空爆に対して有効な迎撃を行うことができなかったとされる[16)]．関係国であるシリアやイスラエルからは公式な発表は出されていない．サイバー攻撃は攻撃側にとっても防御側にとってもその詳細を明かすことは自身の手口や機密情報を披露することになり，エストニアのケースのように誰にでも分かるような事例ではなく，被害が局地的な影響に止まる場合は，事例そのものが明るみに出にくいという事情がある．こうした攻撃がより洗練されていけば，戦術的手段だけでなく，電力供給網を遮断することで相手の継戦能力や意思を奪う戦略的な攻撃方法が行われる危険性もある．

3. 国際安全保障への影響

重要インフラに対する物理的被害を伴うサイバー攻撃が実現化したことで，サイバー攻撃に従来は存在しなかった暴力性が生じ，その一方でサイバー攻撃の匿名性やインターネットの越境的な性質から，有効的な対策を取るのが困難な状態にある．実際に，サイバー攻撃が武力攻撃に相当する脅威であるとして自衛権の発動を含む強力な反撃措置を国家が行った事例はなく，金融制裁といった別の手段による対応も数が限られている状況にある．アメリカがサイバー抑止を政策として取り入れているにも拘らず，その有効性は不透明であり，決定的な対応方法は存在しない．何故サイバー攻撃は武力攻撃と異なるのか，考察

を加えたい．

3.1　サイバー攻撃と武力攻撃の比較

サイバー攻撃を通常の武力攻撃として扱うことが難しい特徴の一つとして，非対称性が挙げられる．主権国家同士の伝統的な戦争を対称的な脅威とした場合，テロリストやゲリラのような非国家アクターが主体となる攻撃は非対称的脅威である．非国家アクターは国家よりも利用できる軍事的資源に劣る為，本来武力で国家に対抗することは困難だが，テロリズムのような非対称的手段を用いることで政治的目的を達成しようとする．サイバー攻撃においても低コストや隠蔽性といった非対称戦の特徴を備えており，物理的被害を伴うような攻撃であっても，国家が責任を認めず，非国家主体を隠れ蓑にする可能性も考えられる．エストニアやスタックスネットのケースを見ても分かる通り，国家が自身の関与を明らかにすることはサイバー攻撃の世界では考えにくい為，こうしたケースにおいて果たして武力攻撃に相当する対応を国家が取ることが可能なのかが政策上重要な問題となる．

サイバー攻撃が武力攻撃やそれに準ずる脅威として軍事的な手段で反撃された事例は今までに存在せず，サイバー攻撃に対して同様の手段であるサイバー攻撃で反撃するという事例も限定的である．ただし，このことをもって将来的にサイバー攻撃が武力攻撃と扱われて反撃されることがないと決めつけることはできない．重要インフラに対するサイバー攻撃は近年その被害が明らかになったものが多く，その被害が限定的である為，そこまで強硬な対応を取る必要性がなかった，または国家が単にそのような事態に対処する準備ができていなかっただけと論ずることも可能である．このような将来の不確定性が存在するものの，サイバー攻撃は一般的に暴力性が限定されることから，武力攻撃のように扱われることがないとする議論が存在する．リッドは，サイバー攻撃の本質についてクラウゼヴィッツ（Karl von Clausewitz）の戦争論における戦争の定義を持ち出して次のように論じている．クラウゼヴィッツの戦争の要件では，暴力性，政策としての性格，政治的性質という 3 つの要素が必要だと述べられているが，サイバー攻撃はいずれの要素においても戦争だと認められる基準を満たさないとリッドは主張している[17)]．リッドはまた，仮にサイバー攻撃によって結果として物理的な被害がもたらされたとしても，暴力を手段として用いることで相手に自らの意思を強制させる戦争行為とは区別され，そのような目的で行われたサイバー攻撃は一度もないとしている．サイバー攻撃は自らの社会的な属性を隠蔽しながら行われることが多く，このことも，自らの帰属を明確にして政策的に行われる戦争の本質から大きく外れるとリッドは主張している．

単に物的又は人的被害が生ずるだけでは戦争行為とは言えないというリッドの主張は妥当であり，実際に過去に戦争に相当するようなサイバー攻撃が行われたことがないのも事

実である．一方でいくつかの点で，将来的にもサイバー攻撃による戦争は発生しないというリッドの主張には反論し得ると考えられる．第一にサイバー攻撃が単独的に行われるとは限らず，武力攻撃を補助する形で行われる可能性があることである．2008 年のグルジアとロシアの間で発生した南オセチア紛争の際に行われたグルジアに対する大規模サイバー攻撃や，2007 年のシリアに対する空爆の事前準備として行われたサイバー攻撃は，武力攻撃を直接的，間接的に補助する形で起こり得ることを示している．このようなケースではサイバー攻撃それ自体が武力攻撃に相当するような被害をもたらすわけではないが，武力行使の一部であると見なすことは可能である．ただしこのような場合，シリアの場合に見られるようにまだ武力攻撃が発生していない段階で，重要施設に対するサイバー攻撃が行われた場合，実質的に武力攻撃の着手が行われたものと認められるかが課題となるだろう．第二の論点は，サイバー攻撃の暴力性の拡大はまだ途上にある為，これまでに武力攻撃に該当するような事例がないのはそれだけの影響力を及ぼす条件が整っていなかったからであり，IoT の普及やサイバー攻撃技術の発達により限定的な武力攻撃の代替手段として利用することが想定できることにある．このことは，クラウゼヴィッツが想定した時代から戦争の性質が変化していることも考慮する必要がある．19 世紀から 20 世紀前半までは主権国家同士の戦争が圧倒的な脅威であった．第二次世界大戦以後，国家同士の戦争が減少した一方で，国内紛争や 9.11 事件に代表されるテロリズムの脅威が顕著になり，非国家主体の国際安全保障に対する影響力が増すことになった．また，アメリカが近年多用しているドローン攻撃のように，大規模な戦力を動員する武力行使を行わなくなった一方で，限定的な手段により目的を達成しようという傾向が強まっている．サイバー攻撃もこのような限定的な武力攻撃の手段には適用性があり，イランへのスタックスネットの攻撃は，実際に空爆の代替措置として使われたという報道が NewYork Times のサンガー記者の記事で示唆されている．このようにサイバー攻撃は部分的には武力攻撃の一形態として使用される可能性はあるが，既存の武力攻撃と完全に同列に扱える存在ではなく，とりわけサイバー攻撃に対する非対称性の問題が有効な対策を取ることを難しくしている．手段としては限定的な武力攻撃の代替措置とし使われる可能性がある一方で，それに対抗する措置は武力攻撃として扱うことが難しい状況は，次に述べるサイバー攻撃に関する規範の問題と組み合わされることで，国際安全保障の不安定要素としてサイバー攻撃が働くことに導く．

3.2 国際安全保障における不安定要素としてのサイバー攻撃

前述までのサイバー攻撃の特徴から，サイバー攻撃の脅威が増大する一方で，安全保障問題としての国家による対応は不透明なものとならざるを得ない．即ち国家がどのように武力攻撃に相当する程度の重大なサイバー攻撃に対応すればいいのか，前例がなく規範も

未発達な状態においては，国際社会共通の認識を持つことが困難である．このようなサイバー攻撃を取りまく国際環境においては，国家がサイバー攻撃の責任を問われるリスクが限定されることから，サイバー攻撃を実行することによって得られる利得と潜在的な敵対者に対する報復能力の獲得を目的として，サイバーセキュリティに関して各国が攻撃的な戦略を採用することで国際社会を不安定にする恐れがある．

サイバー空間に関する規範は，サイバー攻撃の定義といった最も基本的な概念すら国際的に統一された見解は存在せず，非常に希薄であると言える．サイバー攻撃に対しては既存の国際法が適用されるのか，新しい国際法が適用されるのか，それすら決まっていないのが現状である[18)]．サイバー攻撃について規範化の動きが一切ないわけではない．その代表的な例はタリンマニュアルの作成である．タリンマニュアルでは既存の国際法の枠にサイバー攻撃を解釈することで適用しようとしている．ただし，中国やロシアは既存の国際法ではなく新しい国際法の形成を主張しており，国際的な合意は成立していない．また規範化の最たる障害は，インターネットの構造そのものにある．自律的かつ分散的な性格を有するインターネットは，ともすれば責任の不在という現象を招くことになる．米中首脳会談でサイバーセキュリティが最重要テーマとして取上げられるように国家同士の対話も行われるようになったが，国家が自らの責任を認めにくいサイバー攻撃について明確な成果が得られるか今後の見通しは不透明である．

また，サイバー攻撃の存在が不安定要素として働くもう１つの原因として，主権国家がサイバーセキュリティを完全にコントロールできるわけではないことが挙げられる．本来国家による武力攻撃は国家の専決事項であり，国家同士の対話や協調関係で危機をコントロールすることができるが，非国家主体がサイバー攻撃の行為主体の多くを占めている状況においては，国家同士の協調関係のみでは不十分である．とりわけサイバー攻撃の世界では，主権国家は帰属を隠し場合によっては非国家アクターを利用して目的を達成しており，サイバー空間における主権国家の権威は独占的なものではない．姿を隠してサイバー攻撃を行う非国家主体との交渉は国家との交渉よりも一層困難であり，サイバー空間における規範化の形成の障害の１つとなっている．

サイバー空間の規範が未発達で相手との交渉が可能であるか不透明な状況では，国家はサイバーセキュリティを国家間の交渉や国際組織の調停といった手段よりも，自らのパワーの増大により安全保障を維持しようとする傾向を強めることが予測される．サイバー攻撃は手法を隠蔽し，自身の関与を否定することが常套手段となっている為に，交渉自体が成り立ちにくいこともそうした状況を作り出す一因となる．ただし国際協調が十分見込めない代わりに，サイバー攻撃の特徴である匿名性や低コスト，低リスクの問題から，一般的に攻撃より防御が優位であるという状況下においてどのように安全保障を追求するかが

問題となる．第一の可能性として考えられるのは，サイバー攻撃に対する抑止政策の強化である[19)]．

サイバー抑止は既存の抑止理論の類推から成立しており，抑止を実現する為に攻撃を実行した際のコストを引き上げる懲罰的抑止と，攻撃によって利益を得られないようにする拒否的抑止が存在することは変わりない．サイバー抑止は従来のサイバーセキュリティには存在しなかった新しい概念である為，新たな技術によって発生した脅威であることと，攻撃が優位であるという2つの特徴に着目し，核抑止との比較も行われてきた．しかし，マーティン・リビッキ（Martin Libicki）が指摘するようにサイバー抑止と核抑止には多くの差異があり，核抑止による理論をそのままサイバー抑止に適用することは無理があると考えられる[20)]．それにも関わらず，サイバー抑止が政策として導入されているのは，防御的なセキュリティ対策では十分に対応しきれないという危機感に加えて，サイバー攻撃能力の開発に何の制限も加えられていない状況では，懲罰的抑止に必要な報復能力を高めるインセンティブが働くものと考えられる．こうした状況は他国のサイバー攻撃を抑止する能力が他国に対する脅威として働くことで，サイバー空間上の「安全保障のジレンマ」を引き起こす可能性がある．

また，アメリカやロシアのような先進的なサイバー攻撃能力を有する国家だけでなく，後発の国家もサイバー攻撃能力を先鋭化させている兆候が既に出ている．イランはスタックスネットの攻撃後，10億ドルをサイバー攻撃能力に費やし，翌年の2011年12月にアメリカのステルス無人偵察機（UAV）RQ-170を乗っ取り無傷で不時着させた[21)]．イランのサイバー作戦能力がスタックスネットに触発されたものであるならば，アメリカとイスラエルのサイバー攻撃がイランのサイバー攻撃能力を推進させる契機となってしまったと言えるだろう．2010年に行われたサウジアラビアの国営石油会社サウジアラムコに対するサイバー攻撃は，スタックスネットのような物理的損害を与える種類の攻撃ではないが，これもイランの関与が疑われており，その他にも後発国がサイバー攻撃を積極的に行うようになれば，サイバー兵器の拡散という現象が本格化することになる．エストニアが2007年の大規模攻撃の後に，サイバー防衛の研究に注力し，世界有数のサイバー防衛技術を有するようになったように，サイバーセキュリティ能力を高める最も有力な動機は，サイバー攻撃を実際に受けることである．サイバー攻撃の低コスト，低リスクという特性もこのような拡散現象を促進する要因となるだろう．

おわりに

サイバー攻撃による脅威の進展は現在進行形であると共に，不確定要素の多い不安定な

状況にある．サイバー攻撃が技術的進歩によって徐々に暴力性が増してきたとはいえ，その実態や限界は十分把握されていない．戦場における不確定要素は「戦場の霧」と言われるが，サイバー空間をフィールドとした争いはまさに「霧」の中にあり，サイバー攻撃を防ぐことが困難である上に規範も未形成であることによって生じる不安感が，サイバーセキュリティに多大な労力が費やされる原動力になっている．

このような不安定な状況においては，協調関係を築き双方にとっての最高の利益を追求するよりも，相手の裏切りを警戒し最低限の利益を確保する為に自助を何よりも優先する傾向が今後も持続するだろう．自助を最優先するシステムで協調関係が働かなければ，双方が抑止力を向上させることにより緊張関係が深化し，サイバー攻撃能力の発展によって高まる脅威により各国は更なる抑止力を追求することになる．サイバー空間の原理を左右する最大の要素である技術的革新もセキュリティに多大な投資をする要因となる．果たして攻撃者の帰属をどの程度判明させることができるのか，サイバー攻撃が及ぼす暴力性はどこまで到達し得るのか，非国家主体の脅威はどこまで膨らむのかといったサイバーセキュリティの基盤を揺るがすような基本原理は，将来の技術的革新で大きく変化する可能性がある．人類のコンピュータに対する依存度は 21 世紀中に更に深まる為，技術的なセキュリティの向上だけでなく，サイバー空間における規範をどのように発達させるかが問われることになる．

注

1）例えばアメリカでは，2010 年にウィリアム・リン米国防副長官が論文を寄稿し，サイバー空間は陸海空宇宙に次ぐ作戦領域であり，武力による反撃も辞さないと宣言した．（Lynn 2010: 101–102）

2）リッドは主にクラウゼヴィッツの戦争論を引用して，サイバー攻撃が如何に戦争に該当しないかを述べている．（Rid 2012：7–10）

3）安全保障の定義については（土山 1998：2–3）を参照．

4）サイバースパイ等暴力性を含まないサイバー攻撃の定義としては，タリンマニュアルにおける「サイバー攻撃は，攻撃的であれ防御的であれ，人的物的被害を予期して行われるサイバー活動である」のような例がある．この例では，サイバー攻撃を武力攻撃の一種として捉え，結果として武力攻撃と同等の被害が生ずるかを重要な基準として設けている．（Schmitt 2013: 91–92）

5）USB 接続によるマルウェアの侵入は 2010 年に発覚したスタックスネット，直接操作による攻撃は 2008 年の BTC パイプライン爆破事件で知られている．

6）湾岸戦争においてアメリカが見せた圧倒的な軍事力に衝撃を受けた中国の現役将校が執筆した『超限戦』では，相手の長所こそが弱点になるとしてサイバー攻撃にも言及しており，あらゆる領域のあらゆる手段が戦争になりうるとしている．（王 2001：58–59）

7）PDD-63 については以下の URL を参照．<http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

8）オーロラテストについては以下の URL を参照．財団法人未来工学研究<http://www.nisc.go.jp/inquiry/pdf/so_honbun.pdf>

9）スタックスネットの発見が遅れ長期間に渡って駆除されずに潜伏できたのはシステム書き換え機能のおかげであると考えられる．（Denning 2012：674）

10）ヒーリーはエストニアのサイバー攻撃について，技術的洗練性は特にないが，国家政策と強い相関性があり，適度の物理的強制力があると評価している．（Healy 2013：273）

11）エストニアの国防大臣は「NATO は現在サイバー攻撃を明確な軍事行動だと定義していない，北大西洋条約第 5 条に基づく集団的自衛権の適用は困難だろう」と説明した．国防大臣の発言については以下の URL を参照 <https://www.theguardian.com/world/2007/may/17/topstories3.russia>

12）NATO のサイバー攻撃への集団的自衛権適用については以下の URL を参照 <http://www.cnn.co.jp/tech/35095306.html>

13）マルウェアとは不正な目的で作られたファイルの総称である．広義の意味での「コンピュータウィルス」とほぼ同義である．

14）スタックスネットは「撃ちっぱなし」の機能を備えており一度侵入させれば，インターネットによる遠隔操作を必要としない．「撃ちっぱなし」という表現は一度発射した後に手動で誘導しなくても自動で追跡する種類のミサイルになぞらえている．（Farwell 2011：24）

15）サンガー記者によればスタックスネットによって 2008 年から 2009 年にかけての遠心分離機の稼働率は 23％低下した．NewYork Times の記事全文については以下の URL を参照 <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>

16）リチャード・クラーク（Richard Clark）はブッシュ政権期のサイバーセキュリティ担当大統領補佐官で，イスラエルの手法は湾岸戦争で計画されたイラク軍の防空システムを無効化する案に触発されたと述べている．（クラーク 2011：7-16）

17）（Rid 2012: 7-10）

18）サイバー空間における国際法適用の現状は（土屋 2012：30-31）を参照.

19）サイバー攻撃の一般的な優位性については，（Healey 2013: 14-25）を参照し帰属問題（匿名性），低コスト，低リスク及び非対称性の理由から成り立つメカニズムであると考える

20）核抑止とサイバー抑止の違いについては次を参照（Libicki 2009: 39-73）

21）イランのサイバー攻撃については（土屋 2012：45-47）を参照.

参 考 文 献

1. 洋書文献

Clark, Richard（2010）*Cyber War: The Next Threat to National Security and What to Do About It,* NewYork: Ecco.

Denning, Dorothy E.（2012）Stuxnet: What Has Changed?, *Future Internet*, Vol. 4, No. 3, pp. 672-687.

Farwell, James P. Rafal Rohozinski（2011）, Stuxnet and the Future of Cyber War, *Survival*, Vol. 53, No. 1, pp. 23-40.

Healey, Jason（2013）*A Fierce Domain: Conflict in Cyberspace,* Virginia: Cyber Conflict Studies Association.

Libicki, Martin C.（2009）, *Cyberdeterrence and Cyberwar,* Pittsburgh: RAND Corporation, pp. 39-73.

Lynn III, William J.（2010）, Defending a New Domain: The Pentagon's Cyberstrategy, *Foreign Affairs,* vol. 89, No. 5, pp. 97-108.

Nye Jr., Joseph S.（2010）*Cyber Power,* Cambridge: Belfer Center for Science and International Affair.

Rid, Thomas（2012）CyberWar Will not Take Place, *The Journal of Strategic Studies,* Vol. 35, No. 1, pp. 5–32.

Schmitt, Michael N.（2013）*Tallin Manual on the International Law Applicable to Cyber Warfare Draft,* Cambridge: Cambridge University Press.

2. 和書文献

王湘穂，喬良（2001）『超限戦　21 世紀の「新しい戦争」』坂井臣之助・劉琦訳，共同通信.

土屋大洋（2012）『サイバー・テロ　日米 vs. 中国』文藝春秋.

土屋大洋（2013）「サイバースペースのガバナンス」『グローバル・コモンズにおける日米同盟の新しい課題』日本国際問題研究所，27–41 頁 .

土山實男（1998）「国際安全保障の理論と政策」『国際政治』，2 頁.

リチャード・クラーク，ロバート・ネイク（2011）『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』北川智子・峯村利哉訳，徳間書店.

3. URL

IPA, 重要インフラの制御システムセキュリティと IT サービス継続に関する調査 <https://www.ipa.go.jp/files/000013981.pdf>

Jordan Robertson and Michael Riley, Mysterious 08 Turkey Pipeline Blast Opened NewCyberwar <http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>

US Department of Defense（2010）Quadrennial Defense Review Report <http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.PDF>

US Department of Defense（2011）Department of Defense Cyberspace Policy Report <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>

White House, PDD-63 <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

財団法人未来工学研究，制御システムのオープン化が重要インフラの情報セキュリティに与える影響の調査 <http://www.nisc.go.jp/inquiry/pdf/so_honbun.pdf>

4. 新聞資料

Sanger, David E.（2012）Obama Order Sped Up Wave of Cyberattacks against Iran, New York Times, June 1, 2012.