中央大学社会科学研究所年報　第 19 号（2014）

# 非対称脅威としてのサイバー攻撃と国内法整備および国際連携による対応の必要性

鈴　木　洋　一

# Cyber Assaults as Non-Symmetric Threats and the Necessity of Further Domestic Law Preparation and International Cooperation

Yoichi Suzuki

In recent years, with the rapid ICT development, cyber assaults through vertual space against individuals, businesses, organizations, or even governments have become increasingly intense and create serious security problems and important damages to them. In extreme cases, these trigger even international conflicts. Cyber attacks are generally treated as a crime, while some countries/region regard them as a war, which is contrary to conventional international laws.

The report regards traditional warfare as a symmetric threat and a cyber assault including cyber terrorism as a non-symmetric threat and differentiates their attributions. In conclusion, it emphasizes the necessity of further enriching domestic laws and international cooperation as countermeasures.

## はじめに

近年，インターネット空間で展開するサイバー攻撃は，情報通信技術の飛躍的発達に伴って，官民にわたり世界の重大な脅威となって，時として，国家間に敵対関係をもたらす事態にまで発展している．本稿は，サイバー攻撃の本質･特徴･問題を考察するに当たり，国家をアクターとする伝統的国家間戦争と，非国家アクターが実行するサイバー攻撃（戦争）の属性の違い，即ち，「対称性」と「非対称性」に注目する．サイバー攻撃を「戦争」と捉える諸国・地域の動き，犯罪あるいはテロとして解釈することにまつわる問題および対策上の困難を考察した後，関連する国際法および国内法の更なる充実の必要性を考える．最後に，サイバー攻撃の実行主体を自律分散型の個人から構成される層（マルチチュード）として捉え，彼らがサイバーネットワークという国際公共財を超法規的に活用しながら連帯・越境しつつ，国際体系への「抵抗者」として機能するイメージを想定する．

# 1．サイバー攻撃

## 1-1. 定　　義

サイバー攻撃とは，サイバー空間（インターネットでつながる地球上に存在するコンピュータネットワークの全てと，これらのネットワークに接続・制御されるもの全て）で行われる攻撃の総称である[1)]．これは，戦闘主体が国家であった20世紀とは異なり，非国家主体が戦闘主体であり，技術依存性が高いという側面を強調して，「新しい戦争」・「21世紀型戦争」と捉えられることもある．事実，サイバー攻撃を「戦争」とみなす動きが諸国，地域で広がっている．（後出 2．を参照）

サイバー空間において，国境を越える非国家主体による「継続的かつ大規模な戦闘行為（「サイバー攻撃」）」が顕著に増加し，国家同士の敵対も生むケースが増加してきていることが背景にある．（「軍事と民間の連続性」）

## 1-2. サイバー攻撃を「戦争」とみなせるかどうかの問題

1）日本には，「我が国の平和と独立並びに国及び国民の安全の確保に関する法律」（武力攻撃事態対処法）が存在している．

この法律は，「武力攻撃事態」について「武力攻撃が発生した事態」又は「武力攻撃が発生する明白な危険が切迫していると認められる事態に至った事態」という 2 つのケースを想定している．（同法 2 条）

－すると，「サイバー手段のみの攻撃が武力攻撃事態に含まれるのかどうか」の問題が出てくる．

－更に，攻撃手段の種類とその有効性の検討も必要になる．

－これに関連するものとして，「武力攻撃事態等におけるアメリカ合衆国の軍隊の行動に伴い我が国が実施する措置に関する法律」が存在するが，日米安全保障条約に即して，サイバー的防衛をどう扱うのかという未検討課題への対応も必要となる．

## 1-3.「サイバー犯罪」の定義については，「サイバー犯罪条約第二編第 1 章第 1 条」で規定されていて，「コンピュータ・データ及びコンピュータ・システムの秘密性，完全性及び利用可能性に対する犯罪」とされている．

1）代表的なサイバー犯罪としては，無制限アクセス，無権限傍受，データ妨害，システム妨害，デバイスの濫用，コンピュータ関連偽造・同詐欺などが含まれる．

2）形態には，個人による犯罪の他，組織犯罪（大規模なフィッシング詐欺等）がある．（サイバー犯罪条約でも，批准および実態法の整備が進捗中である．

3）国家と個人の関係については，民間人の行為を国家の行為として認定できるかどうかの

問題がある．例としては，後述のエストニアのケースおよびグルジア（平成27年４月22日，国名をジョージアに変更）のケースなどが挙げられる．（174頁参照）

―認定が不確実な場合，①国家は内国人による他の国家に対する違法なサイバー攻撃を抑止する立場にあるのか，②能力的に抑止できるかの問題が出てくる．前記の，エストニア，グルジアのケースからも明らかなように，今日的に，国家と同規模の攻撃を非国家主体がしかけられるようになっていることがこの問題の根底にある．

４）ただ，「越境犯罪」の場合，サイバー攻撃の「匿名性」の高さから，攻撃者の所在地を特定し刑事罰を課すといった伝統的法執行が，サイバー攻撃については有効に機能していない点が問題になっている．

５）サイバー攻撃が純粋に非国家主体の攻撃行為である場合は，「サイバー犯罪」として，コンピュータのセキュリティに対する「犯罪」であり，犯罪の構成要件に該当する違法・有責な行為として国内の刑法などの処罰法で対処できるので，対処に伴う困難は比較的少ない．

―ただ，その場合には，国内法がどの程度サイバー攻撃に対応できているかが問題になる．

この点については，日本の国内法との関わりを表４で簡単に検討したが，そのレベルでも，対処しきれない事項が存在するため，あらゆる可能性，リスクを想定して，予防的見地からの対策を講じる方向で，刑法その他の規定の拡充が要請される．

### 1-4. サイバー攻撃＝「テロ」とみなす動きもある[2)].

１）「サイバーテロ」には一定の定義はないが，「重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で，電子的攻撃による可能性が高いものとされており，一般的にはコンピュータ・システムに侵入し，データを破壊，改ざんするなどの手段により，国家又は社会の重要な基盤を機能不全に陥る行為であり，サイバー犯罪の中でも最も甚大で深刻な被害を及ぼす危険がある[3)].」電子計算機損壊等業務妨害罪および共同正犯に抵触する可能性のある威力業務妨害（刑法犯罪）である．

本論では，「準国家的，秘密のエージェントまたは個人による情報・コンピュータシステム，コンピュータプログラム，データに対する計画的な，政治な動機による攻撃であり，非戦闘員を対象とする暴力をひきおこすもの」と捉えておく．

２）日本には，テロリズムに関する法令がいくつかあるが，サイバー攻撃はテロリズムの一環とされ，対応の管轄組織は警視庁である．警視庁令第39号が，国際テロリズム対策課の職務を規定しており，テロリズム＝犯罪として捉えている．そこでは，「警護施設もしくはその区域」における犯罪を防止するため特別の必要があると認められる場合には，特に自衛隊が出動できるとしている．

―逆に言えば，民間への攻撃は対象外で出動要件を満たさないことになる．

この点を改善する目的で「サイバーセキュリティ戦略」（2013年 6 月）が策定されたことを後述した．（7-1）

3）また，サイバー攻撃＝テロが，「反体制」行為として自国政府に向けられる場合，「移行期正義」などの「正統性」の問題との関わりが出てくる．

－実際，諸国でテロ行為を含む民衆運動の展開で政府が打倒され，打倒して樹立された政権が正統性を内外にアピールする例は多い．次いで，新政権にテロを行使して，打倒を狙う動きも頻発している．（正統性という価値の奪い合い）

ただ，注意すべきは，これまで多くの国々で，あるいは国際的に，サイバー攻撃を戦争行為として扱うのか，犯罪として扱うのか，テロとして扱うのかに関する一律の合意がなかったということである．理由は，サイバー攻撃が特定の対象（個人・組織）だけに被害を与えようとするものなのか，重要な社会インフラや国家の中枢機能を標的にしているのか，判断がつかない場合があるからである．

サイバー攻撃を戦争行為とする流れを次に述べる．

## 2．サイバー攻撃は「戦争行為」とする世界の動向

### 2-1. 米国国防総省の見解

1983年のベイルートにおける米軍海兵隊司令部の爆破テロ以降，テロを犯罪とみなす姿勢を変更し，戦争として対処する方向に転じてきた[4]が，2010年，サイバー空間は，同省の『4 年ごとの国防計画見直し』（2010年 2 月）[5]（7 頁も参照）で，陸・海・空・宇宙に次いで，戦場となりえる「第 5 の領域」“The fifth Domain”と位置付け，翌2011年 7 月に公表した「サイバーセキュリティ戦略」を通して，「外国政府からのサイバー攻撃を戦争行為とみなし，米国が受けた攻撃の度合いと被害の深刻さに応じて，サイバー攻撃にとどまらず，ミサイルなどの通常戦力による武力報復も辞さない.」との方針を打ち出した[6]．

ただし，同戦略は，サイバー攻撃の発信元の特定，戦闘行為に相当するサイバー攻撃に関する定義にまでは踏み込んでいない．

### 2-2. その他の国・地域の姿勢

サイバー攻撃を戦争行為であるとみなす立場は，米国にとどまらず，EU，ロシア・中国，台湾，韓国，北朝鮮など世界の20を超える国・地域で国家安全保障戦略，軍幹部によるサイバー戦略の概念化，サイバー部隊創設，サイバー戦争に対する演習，サイバーセキュリティ戦略の作成の動きなどに表れている．更に，専門家・研究者による国際ルールの提唱である「サイバー戦争に関するタリンマニュアル」（5．⑵を参照）にも共通している．

### 2-3. 英　　国

１）2008年，国家安全保障戦略（National Security Strategy）を公表し，「国家の安全の確保に関する全ての省庁，部局，軍の目標と計画を統合する単一の包括的戦略」とした．（Cabinet Office, The Naitonal Security Strategy of the United Kingdom: Security in an Interdependent World）

２）ただし，同戦略が，サイバースペースを重要な国家安全保障の領域としたのは，翌2009年である．

サイバー攻撃・脅威の範囲：不道徳なコンテンツから詐欺的な犯罪行為，スパイ活動，インフラストラクチャーに対する破壊行為に至るまで，広範にわたる．国家安全保障に関しては，従来，国家と国益の保護においてきたが，今は，民間部門（個人や企業）も対象となるとの認識を示している．

### 2-4. 中　　国

中国では，喬良と王湘穂（喬良と王湘穂は当時の空軍大佐）が1999年に著した『超限戦』[7]の中でサイバー戦を見越した戦術が描かれており，2002年頃から人民解放軍は各軍管区傘下部隊に，情報戦民兵組織を設置し，民間のIT企業，大学，人民解放軍のコンピュータ・ネットワークと連携させることが示唆されている．

米軍との戦争において中国の軍事力では勝てないとして，勝つためにはテロ・生物兵器・化学兵器・心理戦などあらゆる手段，戦術を用いるべきであるとし，サイバー攻撃をその重要な手段のひとつに位置付けている．

軍の能力だけでは不十分で，要員の育成が間に合わず，民間の有能な人材を会社ごと軍に組み入れ，必要に応じて社長を隊長にして，軍の指揮下におくとする．

－ちなみに，中国は，人民解放軍総参謀部第３部がサイバー戦略を担当する．（要員13万人）[8]

Richard A. Clarke　によると，中国では，1990年代末に，「アメリカとの軍事力の質の格差を埋めるためにはサイバー攻撃が選択肢となりえる」とした上で，国家として戦略を練ってきたとされる．2003年にはサイバー戦略部隊を創設し，2007年までには欧米のネットワークに幅広い継続的な侵入を行い，各種のサイバー攻撃をしかけたとされる[9]．

### 2-5. 欧州連合（EU）

「Cyber Europe 2010」：2010年11月４日，汎欧州レベルで大規模なサイバー攻撃に備えた初の合同演習を実施している．サイバー戦争の際に加盟国間で協力しながら対応するための演習で，EU加盟国に加え，スイス，ノルウェイ，アイスランドなど近隣諸国も参加した．

－EUがギリシャにもつEuropean Network and Information Security Agency（ENISA）の主導の

下に実施.

－想定・対応：攻撃によって，加盟国間のインターネット相互接続が段階的に使えなくなっていくため，代替手段として各国間の個別ネットワークを使って情報を共有する形で，サービスのリルーティングを行い，疑似ネットワークを構築してサービスのアベイラビリエィを確保する.

－ENISAはこの演習に向けて１年かけてシミュレーションテストを開発した上で，当日はENISAスタッフが運用を管理.

－インターネットが市民の日常生活や経済活動の重要なインフラになったことから，EUでは，サーバー攻撃対策をEUのデジタル推進指針（Digital Agenda）に盛り込んでいる.

（参考）EU加盟国であるエストニアは，既に2007年４月に大規模なサイバー攻撃（DDos）を受けている．議会，銀行，新聞社などの需要なインターネット・サービスが攻撃に晒され，当時，関係が悪化していたロシア政府の関与が取り沙汰されたが，その後，ロシア系エストニア人が逮捕されている．この攻撃は「Web War １」と呼ばれている[10].

## ３．サイバー戦争の特徴と対応の難しさ

元ハーバード大学のヤン・シュライバー教授（刑法学）は，テロリズムを「究極の兵器」と捉え，理由を対症療法的に処理することの不可能性に求めた[11].（３-２⑵参照）

### 3-1. 特　　徴

１）個人でも攻撃できるため，戦争はもはや軍人の独占的行為ではなくなっている.

①つまり，21世紀は戦争への抑止力が低く，戦争勃発の危険性が高く，コントロールが効きにくい.

②加えて，多くの市民がこれに容易に参加できる（DDos攻撃など）．言い換えれば，「愛国無罪」の標榜，グルジア（現在のジョージア：155頁参照）の事例のような多数の「オンライン・パルチザン」の出現・参入による拡大もあり得る.

（参考）グルジアの事例

2008年８月，ロシアがグルジアに軍事侵攻した際，多くの市民が戦闘に呼応して，グルジアの大統領府，議会，外務省，国防省，メディアなどの国家中枢部へのサイバー攻撃が行われた.

結局，これはロシア軍の攻撃ではなく，ロシアの愛国ハッカーたちが行ったものと結論付けられたが，市民（文民）が国家と同規模の攻撃をしかけられることを世界に示すところとなった[12].

③20世紀型戦争では制空権を握った側が勝利したが，21世紀型戦争ではサイバー空間を制する側が勝利する.

④低コストで，短時間の内に，地球のどこからでも攻撃できる．特殊ソフトを使用すること

で多くのルートを経由・迂回し，発信元を隠ぺいしつつ，他国のコンピュータやアドレスすら使用することができるため，匿名性が非常に高く，直接身を危険に晒す（特定される）ことなく攻撃できることから，防御側や司法当局による攻撃者の特定が困難を極める．

⑤サイバー攻撃は圧倒的に攻撃側に有利であり，専守防衛では，サイバー戦争に敗北する．攻撃が比較的簡単であるのに対し，防御が難しいからである．

特に攻撃対象となる相手側のシステム内にウイルスによって論理爆弾（logical bomb）が組み込まれた場合，相手側は，いつ攻撃が発生するかを予想することが全くできない．

加えて，攻撃の事実そのものも直ぐには察知しにくく，察知した時点では，既に重大な被害を被っていたり，能力を奪われていたりするため，攻撃する側が常に有利で，守る側は後追いとなり劣勢に立たされる（先手必勝）．

従って，「専守防衛」の場合，劣勢は決定的である．攻防にこうした非対称性があるため，サイバー戦争では，完全な勝利か完全な敗北しかなく，過去の戦争のような僅差での勝敗は存在しない．

### 3-2. 攻撃への対応の難しさ

Scott Charneyは，自書[13]の中で，サイバーセキュリティでの対応が難しい6つの理由を挙げているが，彼が強調した特に困難な3つの理由と1つの提言を以下に記述する．

1）インターネットは統合された共有のドメインである．

市民，企業，政府によって共有されており，それぞれを分離することは困難である．

－自由な言論，商取引，諜報活動，サイバー戦争などがこの共有ドメインで全てが同時に，同一の輸送媒体上で発生している可能性がある一方，活動の主体とその内容を解析する能力が限定されている中，様々な脅威への対応を事前に整えておくことは極めて困難．

2）攻撃の潜在的な結果を予測することが非常に困難である．

ネットワークスキャンや許可されていないシステムアクセスなどの不正な行動は，結果的には，情報の窃盗やデータの一体性の侵害，サービス中断の前触れなどであるかも知れない．

更に，システム間の複雑な相互連関を通して予期せぬ影響や結果が生じる可能性があり，予想を上回る重大な事態に至ることがある．

－重要なインフラストラクチャーに対するサービス拒否（DDos）などの明白な攻撃に対しては比較的迅速な対応ができる一方，検出が難しい攻撃がある．（例えば，データの窃盗に比して，データの改ざんは，変更された時点を識別しにくいため，正常な状態への「ロールバック」が難しくなる．

3）攻撃がもたらす事態が，官民のインターネットシステムにわたり複雑であるために，結果の解釈に関する当事者間でのコンセンサスの確立が困難である一方，回復プロセスが人知を

超える可能性がある．

社会の重要なインフラストラクチャーサービスの中断，主要な経済機能の妨害，治安や国家の安全保障の危機などが最悪のシナリオに含まれるが，これらに対する攻撃からの迅速な回復は難しい．社会が複雑な情報通信技術（ICT）システムとそこに含まれるデータに依存する度合いが非常に高まっているため，訓練された人材が行う手動の回復プロセスでは間に合わなくなっている．

4）サイバースペースを実現するインフラストラクチャーの殆どを構築・運用するのは産業界である．更に，脆弱性の公開管理，安全な開発，セキュリティリスクの管理，セキュリティインシデント（事故）への対応などに関するベストプラクティスと技術的なサイバーセキュリティの 規範を生み出し，革新を続けているのも産業界である．

［提言］・このことから，国家をベースとする国際的な協議およびインターネットの信用とセキュリティメカニズムを損なわない方向で官民が協働する国際規範づくりが必要不可欠である．

これらの視点に立って眺めてみると，サイバー空間の共有を通して，安全保障は，個人レベルから国家レベルまでシームレスに重層化しており，いずれかの層で発生した攻撃が広範に伝搬し，極端なケースでは，攻撃が察知されない内に，突然，国家の基幹システムが停止して，サイバー戦争が終結することさえも起こりうる．（いわゆる「国家の脳死」）従って，安全保障概念の再検討が要請される．

## 4．非対称脅威としてのサイバー攻撃

非対称脅威という概念は，既述（2-4）した『超限戦』の中にも登場した考え方である．

国連などの国際機関でサイバー攻撃を含むテロの防止に関する論議・条約がまとまらない大きな原因は，「移行期正義」や「正統性」と関わるテロの定義自体が困難だからである．

この点に考慮すると，分析的には，定義の吟味は一旦おいて，国家間の戦争である伝統的脅威と対比した場合のテロの特徴である「非対称性」の視点からを捉えてみる方法が注目される．サイバー攻撃＝非対称脅威（asymmetric threat）と見るアプローチである[14)]．

公式文書に非対称脅威というタームが登場したのは，米国の 4 年ごとの国防計画見直し報告書 Quadriennal Defence Review: QDR 1997年である[15)]．［非対称脅威］とは，「軍隊同志の交戦ではなく，敵の強みを避け，弱者が敵の弱点を予期できないような斬新な方法で攻撃すること」と捉えられたが，そのスタンスは，翌1998年の米国防衛大学での第 9 次戦略会議で概念が深められている（表-1）[16)]．

国家間の戦争を対称脅威として置き，実行主体，実行目的，実行対象，実行手段，実行方法・形態などの基準で，サイバー攻撃・テロなどの非対称性を浮かび上がらせるものである．

**表-1**　対象脅威と非対称脅威の属性比較

| | ［対称脅威：Symmetric threat］ | ［非対称脅威：Asymmetric threat］ |
|---|---|---|
| 1）脅威領域： | ・陸海空 | ・サイバー空間 |
| 2）脅威形態： | ・武器による戦争 | ・インターネットを通した攻撃 |
| 3）攻撃主体： | ・国家 | ・非国家（個人・組織・結社など／連携もある：テロか内戦か峻別が困難）<br>（多くの場合，水面下で行動） |
| 4）攻撃対象： | ・敵対国家の軍事力／国力（個人・民生施設は対象外） | ・官民のインフラ・所有物／・人間（自国，他国）ほぼ無制限 |
| 5）攻撃手段： | ・軍事力（生物兵器・化学兵器は除外） | ・軍事力以外の超法規的，非通常兵器（通常兵器のとの併用もある） |
| 6）攻撃目的： | ・敵国軍隊の侵略／侵入の排除 | ・攻撃対象の無能化／自己の目的への誘導 |
| 7）「非対称脅威」に関する特記 | | |
| ・抑止や防止が困難　　・対応には官民協力が不可欠<br>・国家安全保障と人間の安全保障がシームレスに重層化している<br>・人間の安全保障とグローバリズムのTrade-Off<br>（グローバリゼーションとともにテロも広がる） | | |

（筆者作成）

（参考１）20世紀の戦争は「総力戦」であった[17]．そこでは……

１）「公的空間」が社会全体を取り込もうとする（国民全体のエネルギーの総動員）ため，「公」と「私」の区別が不明瞭化し，あるいは消滅した．このディメリットを補うため，「共通の目標」や「戦争の正当性」の強調が必要になり，「愛国心の擁護」，「民主主義の擁護」，「悪に対する正義の戦い」といったスローガンが掲げられるようになった．

加えて，総力戦を通して，「公と私」にとどまらず，「軍人と市民」，「国内と国外」の区別も瓦解しつつあり，下記のように「戦争と平和の区別」も不明瞭になり，疑問視され始めている．第二次世界大戦終結までの，国家が戦争行為者であった時代が，〈対称脅威〉の時代であり，以降，次第に，〈非対称脅威〉の時代に移っていく．（これは，私，筆者の見方）

２）G.オーウェルも，「戦争こそ平和である」と述べているが[18]，これは，核兵器が抑止力として機能し，実際に米ソ間では使用できない兵器であるとの暗黙知の下で，熾烈な核開発競争が繰り広げられていた冷戦期に関する解釈であり，現実には，世界各地で（米ソ代理戦争を含む）戦争・紛争が繰り広げられ，第二次世界大戦期の死者を上回る程の累積死者が出ていたと言われているので，「戦争と平和の区別」の不明瞭化の時代の幕開けを言い当てたものである．換言すれば，〈対象脅威〉から〈非対称脅威〉への過渡期を象徴する解釈といえる．

そこでのポイントは，それらが従来型の国家間戦争の形を取らなかったことから，通常の戦争概念に合致せず，それらが戦争として認識されていなかったことである．

３）冷戦期の後に，中東を中心とする内戦時代，つまり闘争主体が，国家の他にも国家未満の単位であるアイデンティティ集団（安全保障共同体ともみなせる）を含む形での紛争が頻発してきた．表-1 のように，国家未満の闘争主体は，非対象脅威を形成する．これにかぶさるように，情報通信（ICT）技術を駆使したサイバー空間での攻撃を含むテロの時代，すなわち本稿が扱う〈非対称脅威〉の時代が展開していく．

（参考２）テロリズムは「究極の兵器」，核兵器との共通性

前記したように，元ハーバード大学のヤン・シュライバー教授（刑法学）は，サイバー攻撃を含むテロリズムを「究極の兵器」と捉え，理由を対症療法的に処理することの不可能性に求めた．この意味では，テロリズムと核兵器には共通性がある．

核ミサイルによる攻撃に対する防衛措置はいまだ不確実性が伴うことから，最も信頼できる対抗措置は核兵器による攻撃ということになる．結果，核兵器開発競争は熾烈を極めながら際限なく進展し，関係国間の国際合意として削減・廃棄を求めるしかなくなった．（核兵器削減条約）

他方，テロリズムの場合，国家というより国家未満の行為者が行うことが多いため，国家間合意は実質的ではなく，また国家内で軍事的に封じ込める対症療法を取れば社会全体が武力・暴力で覆われ，混乱と不安定で満たされることになる．更には反テロリズム戦争の名の下に基本的人権の侵害が日常化し，民主主義諸制度が崩壊しかねない．また，国際社会の不平等な現実を容認したままグローバリゼーションが進行すると，テロリズムも同様にグローバル化する．

－そこでは，国内法，国際法を無視した地球規模のネットワークが自由な行動の手段となる強靭な非対称性が生み出される．

今日，既にテロリズムは，サイバー空間の領域で横行して・陸・海・空・宇宙に次ぐ第五の戦争領域化しており，前記のように，米国その他の諸国・ＥＵなどの地域は，サイバー攻撃を戦争として捉え，通常兵器を含む対抗措置を講じるとしている．このように，攻防における際限のなさ，最大限の信頼をおける手段による対抗・報復という意味で，テロリズムの一環としてのサイバー攻撃と核兵器による攻撃には共通性がある．

（参考３）核抑止力・原発使用済み燃料・テロリズム

「核抑止力」は非協力ゲームにおけるナッシュ均衡で，同等の痛手を相手に与える報復力をもたないと成立しない．（ゲーム理論）このため，核の非保有国は，核武装する（核の拡散―インド・パキスタン・イラン・北朝鮮など）か，核の保有国と相互安保障協定を締結する（核の傘に入る）ことを考える．（例：日米安全保障条約など）

一方，核を保有せずに報復力を持つ方法が存在する．原子炉の使用済み燃料はトン当たり160エクサベクレル（10の18乗）もの核分裂物質を含み（核兵器をはるかに上回る），しかも，崩壊熱除去のために一定期間，地上のプールに中間貯蔵される．これを通常兵器（クルーズ・ミサイル搭載）で攻撃する＝報復能力となるため，相手側に対する核抑止力となりうる．このためには，自己が保有する原発を全て廃炉にして，使用済み燃料を通常兵器で破壊されない場所に保管することになる．（例：ドイツの脱原発への政策転換をこうした視点で捉えることも可能）

潜在的脅威は，テロリストがこの方法で破壊能力を獲得することである．

次節「サイバー攻撃の実態」は，安全保障が正にサイバー攻撃によって広範囲にかつ深刻に脅かされ，危機的状態にあることを示している．

## 5．サイバー攻撃の事例・実態

### 5-1．象徴的な事例

⑴ イランの核関連施設を狙った「Stuxnet」[19)]

2010年７月に判明したイランのウラン濃縮施設を含む諸施設が狙われた攻撃は，“サイバー

テロ”のとてつもない脅威を国際社会に知らしめた．Windowsのセキュリティ脆弱性を突いて侵入したコンピュータウイルス「Stuxnet」がイランの核濃縮施設を乗っ取り，ウラン施設内の遠心分離機の回転数を操作し，一部を破損させ，ウランの濃縮・精製度を低下させ，核弾頭が不発弾化したと言われている．かつ，その後，ウイルスが流出し，５重のゼロディ・アタック（zero-day attack）が仕掛けられた．

この時のStuxnetウィルスは，インターネット接続で感染したコンピュータに使用したUSBメモリーに感染し，それを使ったPCに感染して広がった．独シーメンス製ソフトウェアを攻撃対象とする特徴を持つものであったが，イントラ・ネットワーク間の接続を通して拡散．
－従来安全だと考えられていたインターネット非接続のスタンドアロンの産業制御システムであっても，サイバー攻撃を受ける危険が十分にあることがわかり，世界中に大きな衝撃を与えた．

（参考）「Stuxnet」

一部の軍事専門家は，サイバー攻撃が人的被害を伴わずに核開発の進捗を遅らせる効果を示したことから，核不拡散政策に有効な新しいツールとしての可能性を指摘している[20]．

⑵　韓国のテレビ局や金融機関が攻撃されATM１万6000台が停止[21]

2013年３月20日に韓国で発生した複数企業への大規模サイバー攻撃は，その発生日にちなんで，通称「320サイバーテロ」とも呼ばれている．この同時多発攻撃により，同国の３つの主要テレビ局（KBS，MBC，YTN）放送局と２つの大手銀行を含む複数企業のコンピュータおよびネットワークが一斉にウイルスによる被害を受けた．その結果，銀行のATM １万6000台とインターネットバンキングが停止するなど，社会に大きな混乱を招いた．

障害を受けたサーバーやPCの台数は約４万8700台に及んだと言われる．セキュリティ製品ベンダーのマカフィーが公表している調査結果によると，この攻撃で用いられたウイルスはコンピュータのマスターブートレコード（MBR）を書き換えるもので，感染した端末を起動不能にしてしまうという．

⑶　ソニーの米映画子会社，ソニー・ピクチャーズエンタテインメント（SPE）に対するサイバー攻撃　（2014年12月）

（参考）－米連邦捜査局（FBI）は19日，ソニーの米映画子会社，ソニー・ピクチャーズエンタテインメント（SPE）に対する「平和の守護者」を名乗るグループによるサイバー攻撃について，「われわれの捜査や，米政府部内との緊密な連携の結果，これら行動の責任は北朝鮮政府にあると結論付ける十分な情報がそろった」とし，北朝鮮政府が関与していたと正式に結論付けた．（SPEは，北朝鮮の金正恩（キム・ジョンウン）第１書記の暗殺計画を描いた映画「ザ・インタビュー」を制作．この攻撃で一旦上映中止を決めたが，各界・政界の批判（以下参照）から，一部の映画館とオン・ラインでクリスマスに合わせて上映した．）

「北朝鮮の行動には，米企業に著しい害を与え，米国市民が表現する権利を抑圧する意図があ

る」と批判.「こうした脅迫行為は，受容できる国家の行動範囲を逸脱するものだ」と断じ，「米国や米国の国益を脅かすサイバー上の手段を用いる個人や集団，国家を特定，追跡し，費用や結果（責任）を負わせる」と表明した.（[ワシントン　19日　ロイター]）オバマ大統領は同日，ホワイトハウスで行った今年最後の記者会見で，北朝鮮に「相応の対応をとる」と警告し，報復措置に踏み切る意向を表明した[22].

これと平行して，FBIは，中国，イランによる米国企業へのハッカー攻撃に関する警鐘をならしている.

## 6．サイバー戦争に関わる法律と制度の整備

### 6-1. サイバー犯罪条約（2001年，欧州議会発案，2004年発効，日本は2004年批准し，2012年11月1日発効）：欧米主導の規制であるとして，中国，ロシアは無視.

### 6-2. タリンマニュアル

英米独やオーストリアなどの国際法，情報技術，軍事専門家23名がNATOのサイバー防衛研究所（エストニア・タリン）の委託を受けて3年かけて編纂し，2013年3月に公表した「サイバー戦争」の国際ルールのあり方に関する世界初の文書（全282頁）．まとめ役は，米海軍防衛大学のマイケルシュミット法学部長（当時）．サイバー攻撃が人を死傷させたり，重大な物的損害をもたらすサイバー戦争に至った場合の軍の対応を巡る国際的なルール作りの先駆的業績である.

主眼は次の2点.

1）通常の開戦法規や戦時国際法をサイバー空間に適用して，ルールを明確にし，潜在的な敵の行動を阻止する.

2）国際法にかなった軍事行動を可能にする.

タリンマニュアルは，「サイバー戦争」を，不正プログラムを使い，堤防を決壊させ，人口密集地域の河川を氾濫させたりして人を死傷させたり，物的損害をもたらす大規模なサーバー行動と定義している.

その上で，国連憲章，疾病者や捕虜の待遇などを定めたジュネーブ条約（1997年），国際司法裁判所範例などからなる既存の戦争法規は「サイバー空間に適用される」と明記した.

主要な提言を次表に列挙した.

**表-2**　サイバー戦争についてタリンマニュアルが提示した主な戦争ルール

①［武力行使の定義］
　・サイバー作戦は，規模と効果が通常の武力と同じならば，武力行使に当たる
②［武力行使・威嚇の禁止］
　・他国の領土の一体性や独立を脅かしたり，国連の目的に反するサイバー戦略は違法
③［対抗措置］
　・これによって損害を被った国は相応の対応措置を取ることが可能
④［集団的自衛権］
　・集団的自衛権の行使はサイバー空間でも認められる
⑤［国家責任］
　・自国内あるいは政府管理下のサーバー施設が他国の攻撃に使われていることを政府は積極的に認めてはならない
⑥［保護対象］
　・一般市民，医療従事者，医療部隊，輸送手段は保護されねばならず，攻撃対象としてはならない
などを含め，計95項目のルールを提唱している．

（筆者作成）

（参考）「テロ」と「犯罪」と「戦争」を巡る若干の論点

「テロという概念には，国際的に合意された明確な定義がない」[23)]

国連総会決議第60号：「国際連合加盟国は，テロリズムのあらゆる行為，方法及び実行（諸国及び諸国民の間の友好関係を害し並びに国の領土保全及び安全を脅かすものを含む）を，行われた場所及び行った者のいかんを問わず，犯罪であり正当化することができないものとして無条件に非難することを厳粛に再確認する．」としており，一般に，現行の条約および諸国の国内法はいかなるテロも「犯罪」として規定している．

テロ＝犯罪として規定すると，国内法で実行者を犯罪者として処罰することが可能となる．

テロ＝ある政治目的を達成するために非国家主体によって行われる暴力行為」とする捉え方は存在する．

－「政治目的のない暴力行為」も，通常の犯罪として処罰の対象となっている．

国家をその攻撃対称とする非国家主体によるテロ＝戦争と規定すると，実行者を個別的あるいは集団的に自衛権の行使として反撃することが可能となる．

－ちなみに，2011年９月11日に発生した同時多発テロに際して，米国は首謀者と目されたテログループに対して，自衛権による軍事行動をとった．各国の反応は注目すべきもので，NATOはその発足以来初めてNATO条約第５条に基づく集団的自衛権の行使を容認した[24)]のである．重要な点は，米国に対する大規模テロをNATO加盟国に対する武力攻撃と同等視すると認定したことである．

更には，前記したタリンマニュアルには，国家に対する大規模なサイバー攻撃を戦争とみなし，集団的自衛権を適応拡大・行使できるとする重大な考え方も出てきている．

－これを，戦争と捉えることは，国際法上，大きな問題をはらむものの，国家を攻撃対象とする場合のテロを「犯罪」としてのみ処罰することも問題をはらむ[25)]．

## ７．日　　本

### 7-1. 法律・制度の整備

日本は現行憲法第９条（戦争放棄）により「専守防衛」を旨とし，サイバー攻撃に関しての

対応の整備が遅れていたが，近年，「サイバー攻撃から国民を守る」目的での防衛省・自衛隊の出動を行う方向が打ち出されるようになった．（内閣情報セキュリティ・センター「サイバーセキュリティ戦略」2013年 6 月）

従来，自衛隊の出動要件は，「武力攻撃」による物理的破壊・損傷を受けた場合の「防衛」とされ，武力攻撃を伴わないサイバー攻撃は出動要件を満たさないとして対象外におかれてきた．（自衛隊法第 6 章「自衛隊の行動」第76条）

他国では，サイバー攻撃への対応は軍を中心になされるが，日本には軍はない．かつ，自衛隊は上記の自衛隊法に基づき当該任務は与えられていなかった．

従来，自衛隊が守るのは，自衛隊の指揮系統などのシステムであり，サイバー攻撃の対象になりうる国の重要インフラではない．まして民間は管轄外である．

この現状を打開する方向が上記2013年 6 月の「サイバーセキュリティ戦略」．

これとともに，防衛省は，ハッカーの採用を検討し，陸海空 3 自衛隊の統合部隊としての「サイバー空間防衛隊」の新設を決定した．

情報セキュリティに関する日本政府の対応の主な流れは表-3 のようである．

**表-3** 情報セキュリティに関するこれまでの日本政府の対応の略史

・1998.8 「不法アクセス行為の禁止等に関する法律」
・1998.9 情報セキュリティ関係省庁局長等会議の設立
・2000.1 「ハッカー対策等の基盤整備に係る行動計画」
・2000.2 内閣官房情報セキュリティ対策推進室の設置
・2005.4 内閣官房情報セキュリティ・センター（NISC）へ改組
・2010.5 NISCと情報セキュリティ政策会議が「国民を守る情報セキュリティ戦略」発表
　① サイバー攻撃発生を念頭にした政策・対処強化
　② 情報セキュリティ政策の確立
　③ 受動的な情報セキュリティから能動的な情報セキュリティへ
・2013.6 NISC「サイバーセキュリティ戦略」発表
現在，NISCが日本のサイバー防衛の主体である．
　・センター長は，内閣官房，安全保障・危機管理担当副長官補
　・副センター長は，総務庁，経済産業省，警察庁，防衛庁などから任用
　・内閣官房内の一機関であるため，インテリジェンス機関ではなく，政策立案機能を有する．

（筆者作成）

### 7-2. サイバー攻撃に関わる法的規制の諸側面

表-4 は，サイバー戦争，戦争に関するジュネーブ条約，物理的攻撃に関する日本の刑法の取り扱い具合，今後検討を要すると考えられる主な項目を記したものである．

**表-4**　サイバー攻撃の法的規制について

| |
|---|
| ①　適用法規（国内・国際） |
| 1）　国際法：「サイバー犯罪条約」，平成24年条約第７号および外務省告示第231号<br>・平成13年にストラスブールで採択．日本も批准．平成24年（2014年）11月１日に発効<br>2）国内法としては，批准したサイバー犯罪条約との関連で，刑法などの改正が行われている．<br>［情報処理の高度化等に対処するための刑法などの一部を改正する法律（平成23年法律第74号）］<br>3）武力行使および戦争については，サイバー攻撃に対応した条約などは作成されておらず，現行の戦時法規が適用される． |
| ②　国境と国際協力 |
| ・サイバー攻撃の場合，外国に物理的に身を置きながら日本国内に所在するコンピュータに対して攻撃を加えることが可能であることから，国際捜査共助が物理的攻撃の場合に比べて格段に重要で必要不可欠となる． |
| ③　主体・客体 |
| 1）サイバー攻撃の場合，私人が国家に対して攻撃する際のハードルが低くなっていることが挙げられる．例えば，Staxnet（162−163頁参照）などを用いれば，日本国内において日本国の主要機関を壊滅させることも可能であると考えられる．逆も然り．（外国私人による日本国家への攻撃）例えば，著作権法の改正に際してアノニマスによって財務省などの国家機関のウェブサイトが攻撃されている[26]．<br>2）更には，内国私人による外国国家に対する攻撃も現実的になっている．<br>・これまで，内乱罪および私戦予備罪の適用例はないが，適用すべき事態も想定される． |
| ④　保護法益 |
| 1）プライバシー権を保護する規定：サイバー犯罪条約２条に対応する違法なアクセス罪は，国内法では，不正アクセス禁止法として整備されている．なお，不正アクセス罪を物理攻撃との対比で捉えれば，住居侵入罪と一対のものとして考えることも可能であるが，最高裁は，不正アクセス罪とこれを手段として犯された私電磁的記録不正作出，同供用罪の判例では，両者を併合罪の関係に立つものとしている．（最２小判平成19年８月８日（刑集61巻５号576頁）<br>2）財産権の侵害：コンピュータに関連する詐欺罪（サイバー犯罪条約８条），著作権及び関連する権利に関する犯罪（同10条）が規定されている．性的自由の侵害については，児童ポルノに関する犯罪（同９条）が規定されており，児童ポルノ処罰法とわいせつ物頒布等罪（刑法175条）の改正が行われた．<br>3）他者の生命・身体の侵害，社会の平穏の侵害，国家の存立の侵害，その他の様々な保護法益の侵害が措定されるものとして，データの妨害（サイバー犯罪条約４条），システムの妨害（サイバー犯罪条約５条），装置の乱用（サイバー犯罪条約６条），がある．マルウェアを作成・作動させることは，これらに該当する．<br>国内法としては，マルウェアの作成については，不正指示電磁的記録に関する罪（刑法19章の２．168条の２．以下）によって，処罰されることになった．<br>−マルウェアの作動によっておこる損害については，それぞれの犯罪類型に応じて処罰されることになる．（例：コンピュータネットワークに接続している自動車の制御コンピュータを乗っ取り，運転者の意図しない動作を行わせて事故を起こし，運転者を死に至らしめた場合には，殺人罪の適用が考えられる．ただ，現実には，困難を伴っている． |
| 総　括<br>①サイバー攻撃による犯罪は，物理的攻撃と対応させて検討でき，サイバー犯罪条約＋国内法（特にマルウェアが規制されたことによって，最小限の法的規制は整備された）で対応できる．<br>②一方，上記で検討されていない分野がまだいくつもある．<br>1）社会インフラ設備に対するサイバー攻撃の規制：<br>・国家の存立を脅かすほどの犯罪の場合−内乱罪<br>・他国に対する同程度の犯罪−私戦予備罪<br>の２つがあり得るが，現実には，その適用可能性は低い．特に，私戦予備罪は，その結果の重大性に比べて，法定刑（３か月以上５年以下の禁固）が低過ぎ，抑止効果が働かない．この理由は，物理攻撃において，私戦がほぼ不可能だったからと考えられる． |

しかし，サイバー空間が高度に発達した現代社会では，国家機関や社会の基幹インフラもコンピュータに依存しており，私人がこれを攻撃することが可能になっていることから，これに対する法定刑を準備しておく必要がある．特に，（本稿で例を記述したが）私人が外国の国家機関に対して大規模な攻撃を仕掛けるケースが実際に相当起きて国際問題化しているので，これを抑止する適切な刑を準備しておく必要がある．（本稿に記したように，最悪，戦争とみなされ，通常兵器を用いた交戦状態に入る可能性があるため）

2）情報窃盗：現行の刑法の解釈では，財物とは有体物件であり，情報は該当しない．営業秘密の場合は，不正競争防止法21条で保護される．
・しかし，サイバー攻撃において盗まれる情報（特に国家機密など）の重要性に鑑みれば，刑法に情報も含む形に修正する必要があろう．

3）サイバー攻撃が武力行使や戦争にあたる場合の法規制:
・現状では，ジュネーブ条約などの戦時法規を適用するとされるが，サイバー攻撃では，本稿に事例として引用したように，一般人（文民）が容易に戦闘行為に加担できる．
－しかし，同条約第４条，第１追加議定書第４編以下に規定されるように，直接に敵対行為に参加すると，攻撃からの保護を失うことから，これに関する法整備が必要．
・同条約第１追加議定書で，攻撃目標を破壊した場合で周辺住民に「重大な損失」が生じる場合には攻撃が禁止される．
－この点について，サーバー攻撃の場合に関する検討が必要である．

（筆者作成）

以上のように，予防原則の観点に立ち，あらゆる可能性，リスクを想定して，対策を講じる必要がある．

## 8．多極化・超国家組織・マルチチュード[27)]

中世以降，自然資源，知識，情報，言語，情動といった社会資源（公共財）を私有化することで経済は発達してきた．（封建時代から資本主義時代の流れである）ただ，弊害が生まれたことから公共財を公有化する試み（社会主義や共産主義）が出てきた．しかし，失敗した．

今後，世界は米国を頂点（大方の識者はいずれは「衰退」すると見ているが）とする「超国家」を形成していくと見られる．ジョゼフ・ナイもこうした見解を持っている．しかし，もし，列強の協調もしくは超国家組織化，地域同盟が失敗すると世界は，近代以前に逆戻りし「地域覇権国家」が台頭してくる．

こうした全体的シナリオの中，マルチチュードは，この超国家組織（帝国）の底辺に位置するメンバー（もろもろの国家，国際組織，国内組織，アイデンティティ集団）の一部であるが，ネットワークで連帯する自律分散的な個人から構成される（つまり，司令塔を持たない）集団であり，自由に越境して移動する人々である．このような勢力に対しては，中央集権的正規軍は対応できない．

この諸々の底辺階級より上の部分が「貴族層」であるが，貴族層が恐れるのは，「マルチチュードの抵抗」である．その理由は，知らぬ間に（また，超法規的に）公共財（例えば，サイバー空間）に自由にアクセス・利用しながら攪乱的に目的を遂げるからである．サイバー攻撃は，組織的形としてではなく，自然発生的なセルを単位として実行されている点を特徴とする．本

稿が考察したサイバー攻撃の主体もこのマルチチュードの一部をなすと筆者は見ている．

## おわりに

世界の共有空間あるいは公共財であるサイバー空間における攻撃の高度化に伴い，実態的に，犯罪とテロと戦争の区別が不明瞭になってきている．個人やグループ・組織などの非国家主体が対象国に対して国家と同程度の規模での損害を与えることが可能となったことがその根底にある．匿名性の高い越境行為であるサイバー攻撃をテロして対応するにせよ，一般的には，犯罪として国内法で処罰している．攻撃を受けた国がこれを戦争と捉えて対応する動きも出てきているが，国際法上の問題に直面せざるをない．国内法の整備とともに，国際的な連携・協力を通した対応が不可欠である．

### 注

1) Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do about It, New York : ECCO, 2010（邦訳　リチャード・クラーク，ロバート・ネイク（北川知子，峰村利哉訳）『核を超える脅威　世界サイバー戦争　見えない軍拡システムが始まった』徳間書店，2011年 3月，88頁）
2) 「国際社会におけるテロの現状と今後の展望についての調査」（財団法人　平和・安全保障研究所）2005年 5月） 6頁，21−24頁
3) 警視庁サイバー対策協議会．いくつかの定義を簡潔に紹介したものとしては，『軍事力としてのサイバー攻撃の形態及び諸外国の法的取り扱いに関する調査研究』財団法人ディフェンスリサーチセンター，2000年，2−51頁を参照
4) 西井正弘「テロリズム」『辞典』，570頁
5) United States Department of Defense, Quadrinnal Defence Review, February 2010
6) United States Department of Defense, Quadrinnal Defence Review, July 2011
7) 喬 良／王 湘穂 著（坂井 臣之助【監修】／劉碕 訳）共同通信社，2001年 12月
8) 伊東寛『「第 5の戦場」サイバー戦の脅威』，祥伝社新書，2012年 2月
9) 注1)と同じ
10) The Guardian 17 May 2007: Russia accused of unleashing cyberwar to disable Estonia by Ian Traynor
11) Schreiber, Jan: The Ultimate Weapon.Terrorists and World Order, New York, 1978
12) 伊藤寛　前掲書
13) Scott Charney，Rethinking Cyber Threat-A Framework and A Path Forward 1984
14) Challenging the US Asymmetrically: Can America be Defeated?, The 9 th Strategic Conference, War College, 1998
15) United States Department of Defense, Quadrinnal Defence Review, 1997
16) Challenging the US Asymmetrically: Can America be Defeated?, The 9th Strategic Conference, War College, 1998
17) メリー・カルドー（山本武彦・渡部正樹訳）『新戦争論―グローバル時代の組織的暴力』岩波書店，2003年
18) George Orwell's Nineteen Eighty-Four : From the Perspective of the “Surveillance Society”and

“Liberty” 1984

19) 塚越健司「拡大する戦場化したサイバー空間「スタックスネット」の脅威とは」,『エコノミスト』90巻20号（毎日新聞社，2012)38頁以下

20) 注19)と同じ

21) 방송사・금융기관 해킹사고 피해시스템의 조속한 복구, 사고원인・공격주체 규명에 주력，KCC，2013/03/24アクセス

22) 産経新聞　2014年12月21日，7時55分配信

23) 坂本義和「テロと《文明の政治学》」，藤原帰一編『テロ後―世界はどう変わったか』岩波新書，2003年，7頁

24) 米国の 9.11同時多発テロが発生した翌日（9.12)，NATOが集団的自衛権を発動したという事実は，国家を攻撃対象とするテロが「戦争」であるとの認識が既に存在したということを示唆するものである．

25) A. D'amatoは，“International Law, Cybernetics, and Cyberspace,chapter *in* Computer Network Attack and International Law（Naval War College International Law Studies“Blue Book” Volume76, pp.59-71, publication in 2000)で，サイバー攻撃の広範化などのような社会状況の変化に応じて国際法を含む従来の法解釈を柔軟に変化させるべきであると主張している．

26) 読売新聞　平成24年6月29日付

27) アントニオ・ネグリ，マイケル・ハート 著（水嶋一憲・酒井隆史・浜邦彦・吉田俊実 訳）『帝国グローバル化の世界秩序とマルチチュードの可能性』以文社，2003年