2016 年

第 10 回全日本高校模擬国連大会

議題概説書

Background Guide

【議場】国連総会軍縮・安全保障委員会（第１委員会）政府専門家会合

United Nations General Assembly
Disarmament and International Security Committee (1st Committee)
Group of Governmental Experts

【議題】国際安全保障の文脈における情報及び電気通信分野の進歩

Development in the field of information and
telecommunications in the context of international security

会議監督より

サイバー空間は、陸・海・空・宇宙に続く、「第 5 の戦場」である。――これは、2011年にアメリカの国防総省が発表した「サイバー戦略」の一節です。

「サイバー空間」と聞くと耳慣れない言葉かもしれませんが、みなさんが持っているスマートフォンやパソコンによってつながることの出来る「インターネット」はサイバー空間の一部です。ご存知の通り、インターネットの発達により我々の暮らしはとても豊かになりました。しかし、他人のパソコンを乗っ取り、悪用することも容易にできるようになってしまいました。

国家レベルで考えてみましょう。サイバー技術の発展によって、産業構造が大きく変化しています。本議題概説書においても触れていますが、様々な作業が効率化されています。一方で雇用を奪いかねないのではないか、という懸念もあります。また、軍事分野においてもサイバー技術が活用されています。最近では、機械が自律的に対象を決定し、追跡し、攻撃する兵器が開発されています。この兵器は、味方側の犠牲を伴わずして攻撃できるという側面を持つ一方で、対象を決定するメカニズムが軍事機密とされており、民間人の犠牲を防げないのではないか、という懸念もあります。

このように、サイバー空間の発展にあたっては多くの利点と多くの欠点があります。今回は皆さんに、サイバー空間の利点をいかに活かして、欠点をいかに克服するか、について考えていただきたいと思います。

また、今回の会議では以下のポイントに留意してほしいと思います。

①国際的なルール作り

今回の会議設定においては「国際的なルール」の作成が最大の目標となっています。1 カ国でも納得できないルールや漠然としたルールは意味がありません。全参加国が納得できる形で、最大限に実効的なルールを作成できるように最大限努力してください。

②限られた情報からの推測

今回の議題はテーマの特性上、国の考え方に直結する情報を収集するのは難しいでしょう。担当国の様々な特性を考慮した上で、限られた情報の中から国の立場・考え方を推測してみてください。

サイバー空間におけるルールづくりは緊急性が高まっています。しかし、国際的議論においては複雑な対立が顕在化しています。サイバー空間を通して国際問題の複雑さを体感したうえで、サイバー空間における問題について高校生らしい視座で柔軟に解決への糸口を見出すことを期待しています。

第 10 回全日本高校模擬国連大会　会議監督　神保真宏
杉野実紀

目次

はじめに　　議題概説書の手引き

今回の会議では、「国際安全保障の文脈における情報及び電気通信分野の進歩（Development in the field of information and telecommunications in the context of international security）」という議題のもと、情報通信技術の活用を促進する上で解決すべき課題として3つの論点を設けている。議題概説書では何が課題なのか、現時点でどのような国際的議論が重ねられてきたのかを中心にまとめ、読み進める上で皆さんが何を考えて会議準備するとよいか分かるようになっている。

0-1　議題概説書の構成

第 1 章で大まかに今回の会議の設定を概観した上で、第 2 章で専門用語や基礎知識を整理してまとめた。第 2 章の一部は今回の議論に直結するものではないが、ここで説明した事項は今後「サイバー」や「ICT」といった分野について考える際に有効な知識であろう。そして、第 3 章ではこれまでの国際的な議論を詳述し、第 4 章において今会議で話し合われる論点について概観した。最後に第 5 章において会議準備を進める上で参考になるようなポイントをまとめた。

今回の議論の枠組み（論点）についてまとめたのは第 4 章である。しかし、**最初は第 1 章から順に読むことをおすすめ**する。今回の論点は過去行われてきた国際的な議論（第 3 章）の延長線上であり、それを読むにはある程度の前提知識（第 2 章）が必要となるからだ。また、第 5 章においてはこの会議特有の注意点をいくつか示したので最後まで一読することを勧める。

0-2　議題概説書の位置づけ

議題概説書はあくまで概要であり、個々の国における情報通信技術の活用状況やサイバー空間における課題について詳細に記述したものではない。そのため各国大使として会議準備をする際には、あくまで一般的な議論として本書の内容を理解した上で、自分の担当国が情報通信技術から得ている恩恵やサイバー空間において解決すべき課題を調べ、改めて議題概説書の内容を捉えなおしてほしい。担当国により関心があるポイントは異なるため、インターネットなどを活用して更にリサーチをして知識を深め、解決策を考えてみてほしい。なお、会議準備については第 5 章で詳述するので参照してほしい。

0-3　用語について

本書はあくまでも議論を円滑に進めるための入門書であるため、わかりやすさを重視し、

厳密には正しくない用語の運用[1]をしている場合もあることをご了承願いたい。

また、議題の性質上、本書においては「ICT」や「サイバー」などの用語を用いることとなる。本書の読者としては高校生を想定しているため、多くの人が目にしたことのない用語も多いことと思う。そこで、第 2 章において本書に頻出する専門用語については基本的な解説を加えることとする。また、その他の専門用語についても随時脚注などを用いて解説しているので参照してほしい。

また、脚註の中に散見される「A/C.1/53/L.17」や「A/RES/68/143」という記号は、国連文書の記号である。この会議ではいくつかの国連文書を前提として議論が行われる。詳しくは第 5 章にまとめたので参照してほしい。

[1] 「クラッカー（Cracker）」」と「ハッカー（Hacker）」の使い分けなど。専門的にはクラッカーは悪意に基づくハッキングを行う者のことを指す。

第 1 章　　会議設定

この章では今会議の設定について、議場である国連総会第 1 委員会の政府専門家会合について、そしてそこで採択される成果文書についてまとめる。議場や成果文書の性質は議論の内容や世界への影響を決める会議の核と言えるところであるから、会議準備の際には随時この章へ戻って確認してほしい。

1-1　議場設定

議場：国連総会軍縮・安全保障委員会（第 1 委員会）第 5 回政府専門家会合

議題：（日本語）国際安全保障の文脈における情報及び電気通信分野の進歩

（English）Development in the field of information and telecommunications in the context of international security

開催日時：2016 年 11 月 12・13 日

1-2　議場説明

今回模擬するのは、国連総会の常設委員会である第 1 委員会の内部組織であり、2016 年 8 月から行われている第 5 回政府専門家会合である。ここでは、国連総会とはどのようなものか、そしてその中でも第 1 委員会、および専門家会合がどのような役割、目的を担っているのかを見ていく。

国連総会

国連総会とは、国際連合に加盟している全ての国が参加する審議機関である。各国 1 票を有しており、予算や新加盟国の承認などの重要事項については出席国の 3 分の 2 の多数を必要とするが、それ以外では単純過半数で成果文書である決議を採択する。

国連総会およびその関連会合に参加するのは、各国政府の大使である。大使はその国を代表して会議に参加し、決議案の作成や投票に関する権限を国家から与えられている。大使はその国の主張を議場で明らかにし、国家のためにその会議で行動することが求められている。

第 1 委員会

国連総会は、軍事、経済、環境、人道、文化、法律など非常に広範な範囲における問題を取り扱う。これらの問題を効率よく審議するために国連総会には 6 つの常設委員会が存在する。多くの議題は各委員会で話し合われることとなる。

そのうち、軍縮や安全保障に関わる問題について議論を行っているのが第 1 委員会である。第 1 委員会では 1998 年より「国際安全保障の文脈における情報及び電気通信分野の進

歩」という議題で議論が行われている。近年は、後述する政府専門家会合の結果の影響を強く受けた議論が展開されている。

政府専門家会合

2001 年より第 1 委員会での議論を深化させることを目的に、数十カ国に参加国を限定し具体的な議論を行う政府専門家会合が開催されている。通常 2 年間に数回会合が開かれ、その結果が国連事務総長のレポートという形で第 1 委員会に提出される。過去 4 回開かれ、2016 年より第 5 回が開催されている。

1-3 成果文書

前節で述べた通り、政府専門家会合の結果は国連事務総長によるレポートという形で第 1 委員会に送られ、それをもとに第 1 委員会の議論が展開される。詳しくは第 3 章に譲るが、近年の第 1 委員会での議論は形骸化しており、政府専門家会合での決定内容が、第 1 委員会の決議案に色濃く反映されることとなる。

また、国連総会において、国連改革などを除く多くの議題は、国連総会の各常設委員会で審議され、成果としての決議案が可決されれば総会本会議へと送られ、最終的に国連総会本会議において決議として正式に採択されるという流れを踏む。なお、最終的な本会議での投票結果は各常設委員会での決議案採択時とほとんど変わらず、本会議での採択は形式的なものと考えてもらって構わない。

よって、今回作成してもらうのは、「政府専門家会合のレポート」であるが、その政府専門家会合の決定内容が、第 1 委員会、延いては国連総会での決定に大きな影響を及ぼすことに留意してほしい。

なお、第 3 章以降で詳述するが、今回作成する「政府専門家会合のレポート」は国際的な取り決めについてまとめたものであるため、**コンセンサス（全会一致）をもって発行されたもの以外はこれまでの会合になく、コンセンサスの取れなかったレポートは採択されても国際社会にとってあまり意味のないものとなることに留意してほしい。**

第 2 章　　ICT･サイバーに関する基本事項の整理

「はじめに」で述べたように、ICT およびサイバー空間における問題について概説するのにはどうしてもある程度の専門用語の知識が必要となる。この章では、ICT・サイバーに関する基本知識を概観する。特に*赤斜字*で示した用語については、会議で用いるかは別にしても、ICT・サイバー分野における重要用語であり、ぜひ覚えていただきたい。

2-1　情報通信技術（Information and Communications Technologies: ICT）

まずは今回の議題について考えるにあたり、欠かせない用語である*情報通信技術（Information and Communications Technologies :ICT）*について概観する。

情報通信技術（ICT）

ICT という言葉に聞き馴染みのない人でも、「IT」は聞いたことがある人がいるのではないだろうか。IT は *Information Technologies* の頭文字をとったもので、「*情報技術*」と訳される。『広辞苑』第六版（2008）では「コンピューターや通信など情報を扱う工学およびその社会的応用に関する技術の総称」とされている。ICT は「通信・コミュニケーション」という分野により重要性をおいた用語である。しかしながらその使い分けは曖昧なもので、近年は IT よりも ICT という言葉が多用され、IT よりも進んだ概念としてとらえられているくらいの認識で構わない。本書においては ICT という表現で統一することとする。

なお、今回の議題は「国際安全保障の文脈における情報及び電気通信分野の進歩（Development in the field of information and telecommunications in the context of international security）」である。この議題の国連総会第 1 委員会における成果文書[2]の中には information technologies and means of telecommunication という用語がみられるが、これも ICT と同じことを指していると考えてもらって構わない。

人工知能（AI）

直接議論には関係しないかもしれないが、1 つ、理解しておくと ICT の利点・課題がつかみやすい話題に触れておく。それは*人工知能（Artificial Intelligence: AI）*についてである。

人工知能とは人間が知能を使ってすることを、コンピュータを用いて実現させようというものである。皆さんの身の回りではスマートフォンに搭載されている「音声認識ソフト」が例として挙げられる。また先端技術の領域では「自動運転車」の開発が進んでいることを知っている人も多いだろう。

現代社会は大量のデータにあふれている。これを分析してそこから何かに役に立つ規則

[2] A/RES/53/70 など

性を見出す、*機械学習（Machine Learning）*という技術が現代の AI 開発の基本となっている。というのも、膨大なデータはもはや人間が解析できないレベルに達しており、コンピュータが何かしらの規則性を導き出すことができれば新しいチャンスが生まれうるのである。

例えば、ネットショッピングにおける「おすすめ機能」があげられる。この機能はユーザ A が閲覧した商品または購入した商品をデータとして蓄積し、趣向性が似ていると思われる、同じ商品を購入したユーザをグループ化し、そのグループ内でよく購入されているが、ユーザ A が購入していないものをリストアップするという仕組みである。この過程では膨大なデータを扱うことは想像に難くなく、コンピュータでないと効率的に解析できないというのがお分かりいただけるであろう。

また、機械学習の技術を応用すると、機械翻訳が可能になる、電気通信を自動解析してテロや国際犯罪の予防にも役に立つ、など様々な進化の余地が期待されている。

一方で、AI の発展が進むにつれ、問題点も噴出している。今回は 2 つだけ紹介することとする。一つは軍事面における「自律的兵器」である。もともと熱や光を検知して敵をどこまでも追いかけていく追尾ミサイルは存在した。しかし、現在、標的の探索や攻撃判断をも自ら行う兵器の開発が進められている。このような兵器が危険とされる理由には、一般に、(1)誤判断が生じ、味方や無関係の市民に攻撃を加える可能性が排除できないこと。(2)戦場で兵士が犠牲になるケースを減らすことができる一方で、却ってそのことが戦争を引き起こしやすくすること。――などが挙げられている。[3]

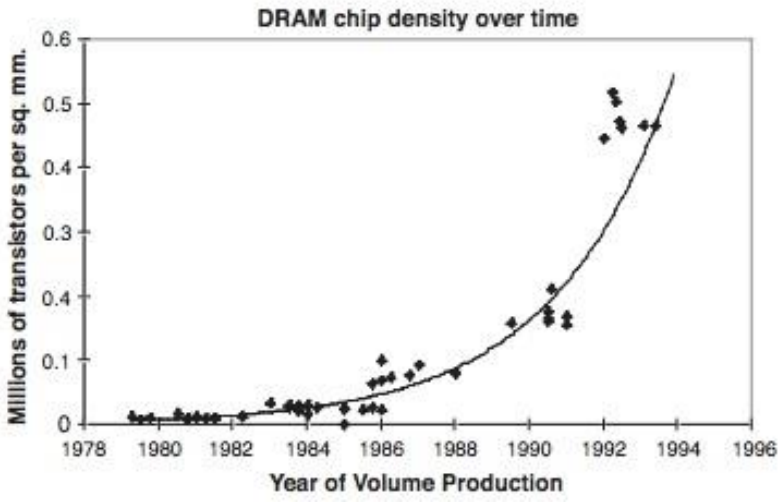
もう一つは、技術的特異点（シンギュラリティ・Singularity）の問題である。これは、人工知能が人間の能力を超えてしまい、技術の発展が急速に変化し、それにより甚大な影響がもたらされ、人間の生活が後戻りできないほどに変容してしまうとする未来予測のことである。一般的にシンギュラリティに到達してしまうと、人類が AI を制御できなくなり人類滅亡の危機が訪れるなどの問題点が指摘されることが多い。SF の話のようだが、国際連合が主催するイベントにおいてもそのような主張[4]がされるなど、科学者の中でも肯定する人が多いのは事実である。なお、シンギュラリティに到達するか否かについては未だ議論が分かれていることも事実である。

次頁に示したのが、「ムーアの法則」を示したグラフである。ムーアの法則とは、半導体メモリの性能が 1 年半ごとに 2 倍になるというものであり、コンピュータ技術の飛躍的な向上をデータで示した。また、人工知能の世界的権威である Ray Kurzweil 氏は「2045 年、1000 ドルのコンピュータは全人類の知能をかけ合わせたものより知的になるだろう」と予

[3]「『ロボット戦争』数年で現実に」（産経新聞）<http://www.sankei.com/life/news/150802/lif1508020014-n2.html>

[4] “Experts Warn UN Panel About the Dangers of Artificial Superintelligence”（Gizmodo）<http://gizmodo.com/experts-warn-un-panel-about-the-dangers-of-artificial-s-1736932856>

測している[5]。



《Figure 2-1》　半導体メモリ 1mm² 当たりのトランジスタの数の変化
（トランジスタの密度が高いと半導体メモリの性能もよくなる。）

※なお、この「AI」の項については、会議との直接の関連性がほとんどないが、皆さんの今後にきっと役立つ知識であろうという判断から、あえて掲載している。

2-2　サイバー（Cyber）

続いて、今会議において重要性の高い*サイバー（Cyber）*について概観する。そもそもサイバーとはいわゆる接頭語であり、「コンピュータネットワークに関する」、「インターネットが形成する情報空間に関連した」という意味である。よって今会議のテーマとして掲げていた「*サイバー空間（Cyberspace）*」は、「コンピュータネットワークに関する空間」と定義することができる。以下、サイバーに関連した語をいくつか紹介することとする。

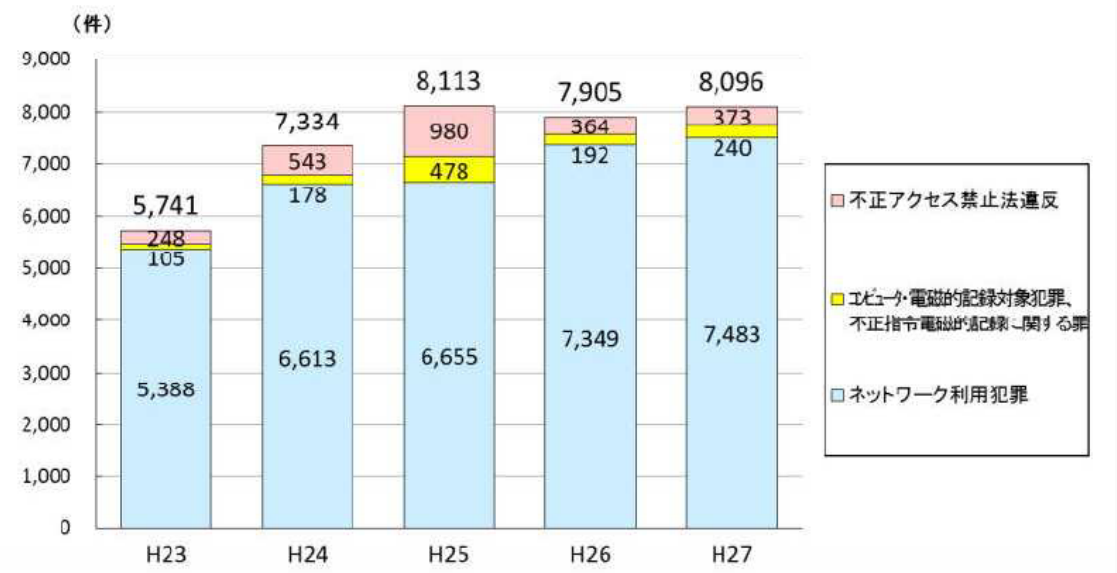
● サイバー攻撃（Cyber Attack）

コンピュータウイルスやワンクリック詐欺という言葉を知っている人は多いであろう。*サイバー攻撃（Cyber Attack）*とは、それらを総称したもので、主にインターネットなどを利用して、標的のコンピュータやネットワークに不正に侵入してデータの詐取や破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせたりすることである。3 節の事例 B でも述べるが、近年、攻撃経路はインターネットだけではなく、USB メモリなどを介したウイルス感染という事例も増えている。

この攻撃が日本でいうところの「不正アクセス禁止法」などに抵触するものであれば、

[5] Ray Kurzweil. “The Singularity Is Near: When Humans Transcend Biology”

*サイバー犯罪（Cyber Crime）*と呼称することになる。警察庁によると、2011 年以降日本におけるサイバー犯罪の検挙件数はおおむね増加しており、2015 年度の検挙件数は 8096 件であった。また、インターネットバンキングに係る不正送金事犯の被害額は約 30 億 7300 万円で、過去最高であった昨年を更に上回るなど、状況は悪化している。



《Figure 2-2》　サイバー犯罪の検挙件数の推移

また、国際的な定義は存在しないが、他国の政治組織、軍事組織、原子力発電所や電気・ガス・水道などの生活インフラなどに対してサイバー攻撃を行うなどの情報通信ネットワークや情報システムを利用した電子的な戦争のことを*サイバー戦争（Cyber War）*と呼称したり、政治的目的や主義主張を達成するために、人に危害を加えたり、国家または社会機能に打撃を加えたりするサイバー攻撃のことを*サイバーテロ（Cyber Terrorism）*と呼称したりすることもあるので頭の片隅に置いておいてほしい。

● サイバーセキュリティ（Cyber Security）

*サイバーセキュリティ（Cyber Security）*とは、簡単に言うとサイバー攻撃に対する防御行為[6]のことを指す。身近なものであればアンチウイルスソフトなどがこれにあたる。コンピュータやソフトウェアは人間が開発したものであり、多くの場合どうしても脆弱性（Vulnerability）が残ってしまう。不正アクセス者はこのミスを見逃さず、それをきっかけにサイバー攻撃を仕掛け、それに対し防御者は、そのセキュリティの穴を塞ぎ、攻撃を防いでいる。現在もコンピュータ技術の発展は著しいが、それに伴い新たな脆弱性は常に生

[6] 防御行為については特にサイバーディフェンス（Cyber Defense）と呼称することもある。

まれ続けている。よってサイバー空間では攻撃者と防御者のいたちごっこが繰り広げられているのである。

また、類似した言葉として、*情報セキュリティ（Information Security）*という言葉がある。これは ISO/IEC 27002[7]において「情報の機密性、完全性および可用性を維持すること」と定義されていて、サイバーセキュリティに包含される概念である。

①**機密性（Confidentiality）**	許可されていない人が情報にアクセスすることができない性質
②**完全性（Integrity）**	情報が破壊、改ざん又は消去されていない状態
③**可用性（Availability）**	許可された人ならば必要時に情報にアクセスできる状態

この 3 要素を俗に情報セキュリティの CIA と呼ぶ。情報セキュリティの CIA が欠けると、様々な被害や影響のリスクがあらわれる。機密性が欠けると情報漏えいに繋がり、完全性が欠けると情報の改ざんに繋がり、可用性が欠けると情報利用者の不便に繋がる、といった具合である。

この**情報セキュリティについて国際的に話しあおう、というのが次章にて紹介する国連総会第 1 委員会での議論の発端である。**

2-3　サイバー攻撃の事例

前節ではサイバー関連の言葉の整理をした。この節ではその中でも「サイバー攻撃」についての実例をいくつか紹介する。

事例 A　エストニアに対する攻撃（2007）

エストニアは 1991 年の独立以来 IT 立国を進めており、国内の電子化を促進し、インターネットを利用した選挙を世界で初めて行うなどインターネット先進国の一つであった。このインターネットへの依存度の高さがサイバー攻撃への脆弱性を生んでしまった。

2007 年 4 月、エストニアに対するサイバー攻撃が行われた。**史上初の対国家のサイバー攻撃**である。攻撃は 3 週間以上も続き、大統領府、議会、外務省、国防省などの政府機関、銀行、新聞社などのウェブサイトが停止させられた。また携帯電話網へも被害が出た。

この攻撃の背景として、「民族間の衝突」があった。ソ連からの独立後、エストニアは反ロシア的政策を進めており、半ロシア系住民とロシア系住民との間で軋轢が高まっていた。そんな中、首都タリンにあった旧ソ連軍将兵の記念像の撤去を巡って反ロシアの市民と親ロシアのロシア系市民との間で騒動が起きた。それとほぼ同時にエストニアへのサイバー攻撃が始まったのである。

---

[7] 企業などの組織における情報セキュリティマネジメントシステムの仕様を定めた国際的な規格。日本語では「情報セキュリティマネジメントの実践のための規範」と呼称する。

この攻撃は乗っ取られた世界 50 カ国以上、約 100 万台ものパソコンによって行われ、同国には通常の 400 倍以上の情報が流入した。これにより国内のインターネットサービスはほぼ全て利用不可能になった。またこういった DDoS 攻撃（Distributed Denial of Service Attack）[8]だけでなく、Web ページの改竄なども行われた。エストニアはどうにか対処を試みたが、ネットが遮断された状態では関係者の連絡すら難しく迅速な対処は困難を極めた。

エストニアは攻撃元の一部がクレムリンやロシア政府のコンピュータであったことなどを突き止めロシアを非難したが、ロシア政府はこれを否定し、ハッカー集団がロシア政府を偽って攻撃を行った可能性を指摘した。このことは**サイバー攻撃が「攻撃者の特定が困難である」という性質を持つ**ことを如実に表している。

事例 B　イランに対する攻撃（2010）

2010 年 9 月、イランの核施設である事件が起こった。ウラン濃縮施設で 1000 台(全体の 10%)の遠心分離機が破壊されたり、遠心分離機のパフォーマンスが低下したりしたのである。これにより核開発が数年遅れたといわれている。一体何が起こったのだろうか。

これは Stuxnet（スタックネット/スタクスネット）と呼ばれるウイルスにより行われたサイバー攻撃であった。Stuxnet は核燃料施設のコンピュータに侵入し、ドイツのシーメンス社製の制御装置に偽の信号を送りこみ、分離機に障害を発生させたのである。通常このような産業制御システムはインターネットに接続していない外部から隔離されたものになっており、何者かが Stuxnet に感染した USB を持ち込んだものと考えられている。

この Stuxnet は非常に高度なウイルスであり、国家による関与が濃厚とされている。イランの核開発に懸念を持つアメリカやイスラエルによる作戦であったと The New York Times 紙は報じた[9]が、この報道に対してアメリカ政府は肯定も否定もしていない。

この事件は**実際に重要インフラを破壊することが出来るウイルスが存在しているということを世界中に知らしめた。**このような形でのサイバー攻撃は今後さらに生み出されていくだろう。

事例 C　日本年金機構における個人情報流出事案（2015）

2015 年 6 月 1 日、日本年金機構は、外部から送付された不審メールに起因する不正アクセスにより、機構が保有している個人情報の一部（約 125 万件）が外部に流出したことが判明したとして、報道発表[10]を行った。

---

[8] ターゲットであるシステムに複数のマシンから大量にデータを送信し、システムやネットワークを麻痺させ、正規の利用を妨害する攻撃。具体的には、ある Web ページの表示を 1 秒間に何千回もリクエストするといった行為があげられる。

[9] “Cyberattacks on Iran — Stuxnet and Flame”（NY Times） <http://www.nytimes.com/topic/subject/cyberattacks-on-iran-stuxnet-and-flame>

[10] 「日本年金機構の個人情報流出について」（日本年金機構）<http://www.nenkin.go.jp/oshirase/topics/2015/20150721.files/0000150601ndjIleouIi.pdf>

原因はコンピュータウイルス付きのメールであった。機構が使用しているメールアドレスの中には、その使用目的の性格上、ウェブサイトで公開されているものがある。攻撃者は、このような機構の公開メールアドレスを入手するとともに、「厚生年金基金制度の見直しについて（試案）に関する意見」や「厚生年金徴収関係研修資料」という件名で、年金業務に関連があるように偽装したメールを準備し、不正プログラムを添付ファイルやURL といった形で送付した。

この攻撃において、攻撃者は標的とする組織に狙いを定め、精巧な技術と相当程度の資源を投入して、標的とする組織の情報を窃取し、業務を妨害することを狙ったとされている。また、機構の対応のずさんさを逆手にとって、長期間にわたって、機構のシステムを乗っ取り、繰り返して攻撃をしかけ、「個人情報を引き出す」という目的を着実に遂行した。

この事件によって、公的機関の職員であっても第三者から送られてきたメールに添付されているファイルを開封してしまうという、日本におけるネットリテラシーの低さを露呈してしまったのみならず、**日本においてもサイバー攻撃のリスクがあることが広く認知された。**

2-4　サイバー攻撃の特性

最後に従来の兵器と比べたサイバー攻撃の特性についてまとめ、なぜサイバー攻撃が脅威たりえるのかについて考えたい。前節の事例内で下線を引いた部分も併せて参照してほしい。以下にサイバー攻撃者にとっての 5 つの利点と 2 つの欠点を挙げる。他にもサイバー攻撃ならではの利点や欠点は存在するだろう。ぜひ考えてみてほしい。

利点① 秘匿性

サイバー戦の大きな特徴は、コンピュータやネットワークに問題が起きた時、それが「故障」なのか「攻撃」なのか判別しにくい点である。この秘匿性を利用して、攻撃者は「故障に見える攻撃」を仕掛けてくる可能性が高い。従来の戦闘であれば、攻撃を受けているということは瞬時に判断可能な事柄であり、その後の対処も迅速に行うことが出来た。

利点② 柔軟性

サイバー攻撃を受けていることが分かったとしても、それへの対処も難しい。どこから、誰によって攻撃されているのかがとても分かりにくいからだ。このため攻撃者は、

- 攻撃する時期を自由に選べる
- 発見されるまで長期にわたり継続的に攻撃出来る
- 短時間攻撃した後、ただちに自分の痕跡を消すことが出来る
- 目標をピンポイントで狙い打つことも、広域に大きな混乱を引き起こすことも出来る

などの柔軟性を得る。

従来の兵器では、いつでも効果的に攻撃を行うことは出来ないし、瞬時に発見される。また攻撃の痕跡を消すことは出来ない。

利点③ 非対称性

サイバー戦では攻撃者は身元を隠せるが、標的はそれが出来ない。このように攻撃が一方的に行われる戦いを「非対称な戦い」という。この非対称性により、サイバー戦では攻撃者が圧倒的に有利であり、標的とされた側は反撃が困難となる。攻撃者は国なのか、非国家組織なのか、個人なのか。それすらも完全な特定は難しい。

利点④ 費用対効果の高さ

従来、兵器の開発には多くの資金を必要とした。兵器を製造できない貧しい国は強国に対して効果的な攻撃を行うことはまず不可能であった。一方、サイバー攻撃においては、優秀なハッカーを育成し、従来の兵器と比べ格段に規模の小さい情報インフラ（コンピュータなど）を整備するだけで効果的な攻撃が可能になる。

利点⑤ 手軽さ

サイバー攻撃は「お手軽」な攻撃であるとも言える。攻撃を目的としたプログラムさえ入手することが出来れば、一般人でもサイバー攻撃を行うことが出来る。DoS 攻撃（Denial of Service Attack）などがその好例である。DoS 攻撃とは、サーバやネットワークなどに意図的に過剰な負荷をかけたり脆弱性をついたりすることでサービスの正常な動作を侵害することである。俗に「F5 攻撃」と呼ばれる、Web ブラウザの「再読み込み」機能を何度も連続して行うことにより、過大な負荷をかけて正常な動作を停止させるものも DoS 攻撃の一種である。

また、サイバー戦争では、上で紹介した「非対称性」もあいまって、一般人も自分の身を危険にさらすことなく民兵として容易に戦闘に参加することが出来るのである。

欠点① 一過性

以上のように攻撃者側に有利な特性がある反面、欠点も存在する。例えばコンピュータウイルスを作り、それを拡散させたとしても一度使ったウイルスは二度と通用しないと考えたほうがよい。それに対応するワクチンソフトが作られる可能性が高いからである。コンピュータウイルスに限らず、多くのサイバー攻撃について、一度用いた方法については対策が取られ、有効に攻撃できなくなる可能性が非常に高いといえる。

欠点② 不完全性

同じ攻撃が二度通用する可能性が低いということから、サイバー攻撃の手段については、その存在は使用直前まで隠しておく必要がある。つまり、事前のテストはほぼなしで攻撃

しなければならないということであり、サイバー攻撃は効果を完全に予測することができない、不完全な兵器と言えよう。サイバー攻撃のみである場合はまだしも、サイバー攻撃の成功を前提とした物理的攻撃がセットであった場合など、効果が担保出来ていないということが危険につながることもある。

Column DoS 攻撃と DDoS 攻撃

多くの専門用語が出てきた第 2 章ですが、シンギュラリティや DoS 攻撃などかなり専門性の高い用語もあえて掲載しました。会議に参加するにあたって覚える必要のある語ではありませんので安心してください。

さて、このコラムでは紛らわしい 2 つの単語「DoS 攻撃」と「DDoS 攻撃」の違いについて簡単にまとめておきたいと思います。ずばり、DDoS 攻撃は、DoS 攻撃の進化版なのです。

DoS 攻撃は攻撃者が手元のコンピュータを用いて直接攻撃します。それに対して DDoS 攻撃は攻撃者が多数の無関係なコンピュータに侵入してそこから一斉に攻撃します。ご想像の通り、DDoS 攻撃のほうが威力は強いのですが、十分な対策を講じていない Web ページに対しては DoS 攻撃を用いても致命的なダメージを与えることができます。

《Figure 2-3》　DoS 攻撃と DDoS 攻撃の違い

皆さんの中には自分でブログをやっている人や Web ページを運用している人もいるかもしれません。ソーシャルネットワーキングサービス（SNS）をやっている人はかなり多いでしょう。デジタルネイティブ世代と言われている皆さんにはぜひ、ICT やサイバー空間に関する正しい知識をつけていただきたいと思います。

第 3 章　　サイバーに関する国際的な議論

この章では、サイバーに関してこれまで行われてきた国際的な議論を今回の論点（第 4 章で解説する）にかかわる議論を中心に簡単にまとめる。特に 1 節、2 節は今回の議論の背景となる部分なので、本書を読むとともに、該当する決議や議事録を合わせて読むことで理解が深まるだろう。

3-1　国連総会第 1 委員会

国連総会第 1 委員会では、「国際安全保障の文脈における情報及び電気通信分野の進歩（Development in the field of information and telecommunications in the context of international security）」という議題で毎年サイバー分野における規制などについて話し合われている。議論は 1998 年、ロシアによる決議案（Draft Resolution: DR）[11]の提出から始まった。この議題の決議は現在に至るまで毎年採択されている。

冷戦の終結後、サイバー分野での発展が進んでいたロシアはサイバー空間の有用性と危険性を認識し始めた。そこで、アメリカとの間でサイバー空間における規制の枠組みを作ることを目論んだ。しかし当時のアメリカは、ICT の商業的・軍事的価値の重要性を強く認識し、ICT 分野の発展を妨げるとして規制には後ろ向きであった。その結果、1998 年に行われた米露首脳会談の中では、サイバーセキュリティに関する話し合いはされたものの、結論となる共同声明では「われわれは、今起こりつつある情報技術革命のポジティブな側面を促進し、ネガティブな側面を軽減する重要性を認識する。それは両国の将来の戦略的安全保障利害を確かなものとする際の重要な挑戦である。[12]」と今後の対話姿勢を表明するにとどまり、ロシア側の規制の枠組みの作成という思惑は達成されなかった。

国際的なサイバーセキュリティに関して米露二国間交渉で妥結できなかったことで、ロシアは、サイバーセキュリティを促進する場として国連を選択した。第 1 委員会における議論は、主にアメリカや西欧の民主主義国とロシアや中国など**上海協力機構[13]（Shanghai Cooperation Organization: SCO）**に所属する国々の、情報セキュリティという言葉の異なる認識により、対立の激しいものとなった。

具体的に見ていきたい。ロシアは**ICT や情報それ自体の安定とその脅威をなくすことを情報セキュリティと捉えていた**が、アメリカや西欧諸国は表現の自由の尊重という立場か

[11] A/C.1/53/L.17
[12] Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century
[13] 中国・ロシア・カザフスタン・キルギス・タジキスタン・ウズベキスタン・インド・パキスタンの 8 か国による多国間協力組織。

ら情報自体が規制の下にあるという考えには反対し、**インフラとネットワークの保護を強調した**のであった。また、国際的に法的な枠組みを作ることについても議論が行われたが、ロシアなどがその必要性を主張する一方で、そういった枠組みは民間（及び軍事分野）における技術の発展を妨げてしまうので好ましくない上、従来の国際法などで十分に対応可能だと主張する国もあり、議論はまとまらなかった。

そんな中、2001 年、ロシアによって政府専門家会合（Group of Governmental Experts: GGE）の開催が提案された。提案された GGE の目的は、情報セキュリティにおける現状の、また潜在的な脅威を検討すること、可能な協力策を検討すること、国際的な情報セキュリティに関して研究を行うことであった。2004 年になり、初めての GGE が開催された。

その後、GGE は何度も開催されることになった。**国連総会第 1 委員会での議論は、GGE の結果として提出される国連事務総長レポートに則って行われるようになり**、**決議についても**「各国が GGE のレポートを踏まえた調査・研究を行うことを求める」ことを主眼においた**形式的なものに変容していった。**

3-2　政府専門家会合（Group of Governmental Experts: GGE）

GGE はこれまで①2004～05 年、②2009～10 年、③2012～13 年、④2014～15 年の 4 回開かれており、今年 8 月から 5 回目が開催されている。その概要および結果については国連事務総長がレポートとして国連総会第 1 委員会に提出することとなっている。

GGE の参加国は地域的衡平性を考慮して決定されることとされている。過去 4 回とも参加しているのは、ベラルーシ、中国、フランス、ドイツ、ロシア、イギリス、アメリカの 7 カ国である。

第 1 回 GGE（2004 年 7 月、05 年 4 月、同年 7 月）

参加国：ベラルーシ、ブラジル、中国、フランス、ドイツ、インド、ヨルダン、マレーシア、マリ、メキシコ、韓国、ロシア、南アフリカ、イギリス、アメリカ

第 1 回 GGE ではベラルーシ、ブラジル、中国、ロシアが制約なしに自国の情報セキュリティを守る各国の権利、また同時に新たな国際的制度を採択することを主張した。また、加えて、ICT 分野での軍縮についても言及することを求めた。しかしアメリカ、EU 諸国との間の認識の差異は埋まらず、コンセンサスによって何かしらの結論を出すことができないまま会議は終了してしまった。

この GGE の後、2005 年から 2008 年までアメリカは加盟国で唯一国連総会第 1 委員会におけるサイバー分野の決議に反対票を投じることとなった。

第 2 回 GGE（2009 年 11 月、2010 年 1 月、同年 6 月、同年 7 月）

参加国：ベラルーシ、ブラジル、中国、エストニア、フランス、ドイツ、インド、イスラエル、イタリア、カタール、韓国、ロシア、南アフリカ、イギリス、アメリカ

第 2 回 GGE を迎えるまでに、エストニア、ジョージア、リトアニアなどにサイバー攻撃の被害が出て、**サイバー空間における制度設計について緊急性が高まっていた。**アメリカはロシアや中国との二国間交渉を開始し、そのロシアや中国は上海協力機構の下でウズベキスタンらと情報セキュリティに関する協定を結んだ。

そのような背景もあり、第 2 回 GGE では、拘束力のある枠組みに関しての議論など対立点を抱えつつも、コンセンサスによってレポートを提出することが出来た。その内容は、**国際的な ICT の利用規範についての議論を継続すること**、国有の、また国際的なインフラを保護することなどであった。加えて、国際的な ICT 利用に関する安定を図ること、引き続きリスクを減らす措置などを行っていくことが推奨された。第一回の GGE と比較して国際的に関心が高まる中で、対立点を乗り越え、何らかの成果を残せたという意味で意義のある会議となったと言える。

情報セキュリティのための国際行動規範

第 2 回の GGE を受けて、ICT 利用及びサイバー空間における国際的規範の確立に向けた動きが加速した。中でも特筆すべきなのは、中国、ロシア、ウズベキスタン及びタジキスタンの 4 か国による**「情報セキュリティのための国際行動規範（International code of conduct for information security）」の共同提案**[14]である。この行動規範は 11 の項目からなっており、情報セキュリティの確保に関し、各国の**主権の尊重を強調**する内容となっている。以下に主な条文を抜粋[15]する。

- テロリズム、分離主義、過激主義を扇動する情報や、他国の政治、経済、社会的安定性や精神的・文化的環境を弱体化させる**情報を阻止するために協力する**こと
  （条文 c）
- 他国の政治経済社会の安全保障に脅威を与えるためにそのリソース、重要インフラ、中核技術やその他の優位性を使用することを防ぐため、ICT 製品や ICT サービスの安全を確保するよう努力すること
  （条文 d）
- 情報を検索、取得、頒布するなどの情報スペースにおける権利及び自由については、**関連する国内法令に従うという前提で**十分に尊重すること
  （条文 f）

[14] A/66/359

[15] 「サイバー空間の在り方に関する国際議論の動向」（総務省） <http://www.soumu.go.jp/menu_seisaku/ictseisaku/cyberspace_rule/>

- インターネットにおける資源の公平な分配を確保し、全てのアクセスを容易にし、安定して安全な機能を確保するために、多国間にわたる、民主的な国際インターネット管理システムの構築を推進すること
  （条文 g）

この行動規範は結果的には国際的に受け入れられなかった。アメリカや西欧諸国が難色を示したためである。例えば、条文 c については、政府の考え方とは異なる情報の流通を阻止すると解釈することができ、表現の自由を尊重する考え方と対立するように見える。また条文 f については、情報空間における権利、自由の尊重を原則としてうたいつつも、国内法令によって政府が情報の検索、取得、頒布等を規制することができると解釈することが出来る。

第 3 回 GGE（2012 年 8 月、2013 年 1 月、同年 6 月）

参加国：アルゼンチン、オーストラリア、ベラルーシ、カナダ、中国、エジプト、エストニア、フランス、ドイツ、インド、インドネシア、日本、ロシア、イギリス、アメリカ

「情報セキュリティのための国際行動規範」は受け入れられなかったとはいえ、**ICT、サイバーについての国際的規範への必要性は強く認識され始めていった。**2001 年以降の国連総会第 1 委員会の決議においては、毎度「次回の GGE における成果を国連事務総長がレポートとして報告することを要求する」旨の条文が存在するが、2011 年の決議に[16]おいて、「国際的な規範、規則、あるいは原則（norms, rules, or principles）を含める」という具体的な記述が登場し、その決議が採択されたことからもそれがうかがえる。

第 3 回 GGE では、ロシアや中国が「情報セキュリティのための国際行動規範」に基づいた規範の作成を求めたものの、アメリカなどが国際法や国連憲章など既存の枠組みの中で規範を作成していくべきという共通見解を追求するなど、依然食い違いが見られた。結果的に報告書では、中国、ロシア等 4 か国の「情報セキュリティのための国際行動規範」の提案について留意したとされたが、それ以上にその内容には立ち入らなかった。

報告書は、第 2 回より量が増え、中身についても具体性が増した。報告書の内容は大きく分けて、「国際協調体制の構築」「各国家の責任ある行動についての規範、規則、あるいは原則」「情報のやりとりに関する信頼醸成措置[17]」「サイバー途上国におけるキャパシティ・ビルディング」の 4 つに分かれる。報告書については是非一読していただきたいのだが、以下、要約部から簡単に抜粋[18]した。

[16] A/RES/66/24

[17] 国家間の相互不信を軽減・除去し，信頼関係を構築することによって軍事衝突を未然に防止することを目的にとられる措置。

[18] A/68/98

国際協調体制の構築

Member States have frequently affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. International cooperation is essential to reduce risk and enhance security. Further progress in cooperation at the international level will require actions to promote a peaceful, secure, open and cooperative ICT environment. Cooperative measures that could enhance stability and security include norms, rules and principles of responsible behaviour by States, voluntary measures to increase transparency, confidence and trust among States and capacity-building measures. States must lead in these efforts, but effective cooperation would benefit from the appropriate participation of the private sector and civil society.

各国家の責任ある行動についての規範、規則、あるいは原則

The report recognizes that the application of norms derived from existing international law relevant to the use of ICTs by States is essential to reduce risks to international peace, security and stability. The report recommends further study to promote common understandings on how such norms apply to State behaviour and the use of ICTs by States. Given the unique attributes of ICTs, the report notes that additional norms could be developed over time.

The report reflects the Group's conclusion that international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. The Group also concluded that State sovereignty and the international norms and principles that flow from it apply to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory; States must meet their international obligations regarding internationally wrongful acts attributable to them.

情報のやりとりに関する信頼醸成措置

サイバー途上国におけるキャパシティ・ビルディング

The report contains recommendations on voluntary measures to build trust, transparency and confidence, as well as international cooperation to build capacity for ICT security, especially in developing countries. The Group recommends the holding of regular institutional dialogue on these issues under the auspices of the United Nations as well as regular dialogue in other forums, to advance these measures.

特に、国際的規範については、時間をかけて発展させることができる可能性を示唆しつつも、現状は既存の国際法などの枠組みで十分であることが明記された。（赤字部分も参照のこと。）また、ここには抜粋しなかったが、表現の自由等の尊重が、情報セキュリティへの努力においても不可欠であることが明記されるなど、アメリカ側から見た際に、一

定の前進があったと評価される文言となった。

ただ、未だ現状の枠組みのどの規定がサイバー空間に適用されるのかという具体性に欠けるほか、ロシア等による「情報セキュリティのための国際行動規範」の是非に関する議論はまだ決着を見ていないということに留意したい。

また、「各国は自国に起因する国際違法行為について、その国際的な義務を果たす必要がある」と、サイバー攻撃について国家が責任を負う可能性を含む決定がなされたことも大きな変化と言える。（青字部分も参照のこと。）

第 4 回 GGE（2014 年 7 月、2015 年 1 月、同年 4 月、同年 6 月）

参加国：ベラルーシ、ブラジル、中国、コロンビア、エジプト、エストニア、フランス、ドイツ、ガーナ、イスラエル、日本、ケニア、マレーシア、メキシコ、パキスタン、韓国、ロシア、スペイン、イギリス、アメリカ

第 3 回 GGE についての国連事務総長レポートが国連総会第 1 委員会に提出されると、「既存の枠組みで対処可能ならば具体的にどの規定が適用されるのか」という疑問が噴出した。そこで、2013 年の決議[19]以降、次回の GGE において「どのように既存の国際法が国家による ICT 技術に活用されるのか（how international law applies to the use of information and communications technologies by States）」について議論することを要求する文言が現れた。

第 4 回 GGE は第 3 回 GGE の議論を進化させる形で進められた。特に前述の「どのように既存の国際法が国家による ICT 技術に活用されるのか」という論点については、後述の通り報告書において 1 章分割かれていることから、重要であったことがうかがえる。今回の報告書は「サイバー空間における現在の脅威」「各国家の責任ある行動についての規範、規則、あるいは原則」「信頼醸成措置」「ICT セキュリティにおける国際協調体制とキャパシティ・ビルディング」「ICT の利用においてどのように国際法が適用されるか」の 5 章立となっている。「サイバー空間における現在の脅威」については、前回の報告書のイントロダクション部に記載があったものが発展した形になっている。

「各国家の責任ある行動についての規範、規則、あるいは原則」については、前回の報告書に加えて、人権理事会の議論の内容が引用される[20]など、具体性に少し進歩がみられるものの、未だロシア等による「情報セキュリティのための国際行動規範」については留意するとの表現にとどめられ、その是非に関する議論に決着はつかなかった。

[19] A/RES/68/243
[20] A/HRC/RES/26/13 が引用された。

第 5 回 GGE（2016 年 8 月～）

第 4 回 GGE についての国連事務総長レポートが国連総会第 1 委員会に提出されると、未だ具体性に欠けることや、サイバー空間における変化が激しいことを理由に 2016 年から第 5 回の GGE を開催することを盛り込んだ決議が提案された。

議論の中身については、特に追加の論点の提示などは見られず、引き続き「サイバー空間における現在の脅威」「各国家の責任ある行動についての規範、規則、あるいは原則」「信頼醸成措置」「ICT セキュリティにおける国際協調体制とキャパシティ・ビルディング」「ICT の利用においてどのように国際法が適用されるか」の 5 論点について引き続き議論をすすめるよう要請された。

今回模擬する第 5 回 GGE については、2016 年 8 月に第 1 会合が行われ、2017 年にかけて議論が進められる予定である。

なお、GGE については回を追うごとに開催間隔が狭まっている。一つの要因として、2011 年のジャスミン革命を発端とした「アラブの春」において、インターネットやソーシャルメディアが民主化運動に大きな役割を果たしたことを受けて、新興・途上国においてネットへの規制や政府の管理を強化する動きが強まったことがあげられる。2012 年に始まった第 3 回 GGE から今年までは毎年会合が行われている。それだけ緊急性の高い話題であることをぜひ理解してほしい。

3-3　その他の国際的議論

今回模擬する議論については、主に国連総会第 1 委員会及び GGE で行われてきたものの延長線上にあるため、他の国際的議論については概要をまとめるにとどめる。

国際電気通信連合 (International Telecommunication Union: ITU)

国際電気通信連合（International Telecommunication Union: ITU）は国連の機関の中で最もサイバーセキュリティに関わっている機関である。ITU は国際連合の専門機関の一つで、その目的は「①あらゆる電気通信の改善と合理的利用のため、国際協力を維持増進すること。②電気通信業務の効率化と可及的普及のため、技術の改良とベストな運用を促すこと。」の 2 つである。具体的には 2003 年に世界情報社会サミット（World Summit on the Information Society: WSIS）を主催したり、各国のサイバーセキュリティ向上のために法整備支援など行ったりしている。

ITU においては定期的に WSIS のレビューが開催され、効果的にサイバーの脅威に対応するための専門的知識の交換がされており、サイバーセキュリティ文化創成の一助となっている。

国連総会経済・財政委員会（第 2 委員会）

国連総会第 2 委員会は、経済や開発に関する議題を扱う常設委員会である。そこでは、「サイバーセキュリティに関する世界文化の創成（Creation of a global culture of cybersecurity）」および「開発のための ICT（Information and Communication technologies for development）」という議題のもとにサイバー関連の事柄を話し合っている。具体的には、主に WSIS の議論を確認し、その内容を周知徹底するようなフォローアップが行われている。

国連安全保障理事会

国際連合安全保障理事会（United Nations Security Council: UNSC）は、国連機関の中でも国際の平和と安全の維持に対して重大な責任を持つと国連憲章内に規定されている機関である。UNSC の決定は国連加盟国を法的に拘束できるなど、実質的に国際連合の中で最も大きな権限を持つ、事実上の最高意思決定機関である。UNSC においても近年サイバー空間について話し合われており、2013 年 12 月には、サイバーテロの取締りの強化について具体的措置を講じるよう初めて各国に明確に求める決議[21]が全会一致で採択されている。

国連人権理事会

国連人権理事会（United Nations Human Rights Council: UNHRC/HRC）は、人権と基本的自由の保護・促進及びそのための加盟国への勧告や、大規模かつ組織的な侵害を含む人権侵害状況への対処及び勧告などを目的とした国連総会の下部組織である。

2002 年以降インターネット上での人権侵害について議論されるようになり、主にインターネット上での言論・表現の自由について議論が続けられている。

サイバー犯罪条約

実は GGE の報告書にも明記されているのだが、サイバー空間に関する国際的な議論においては、地域機構の果たす役割も大きい。その中でも欧州評議会（European Council）[22]が果たした役割は大きく、サイバー空間に関する唯一の条約を起草した。この項では、そのサイバー犯罪条約（Convention on Cybercrime）に関して簡潔にまとめる。

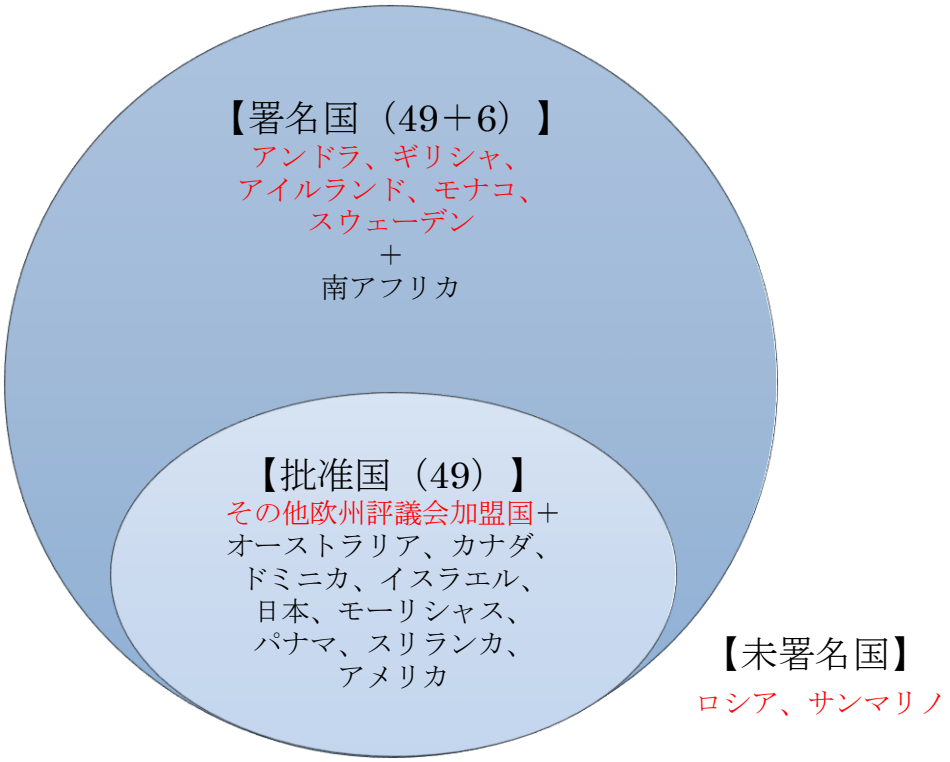
そもそも、サイバー犯罪は国境を越えて実行されるものであり、取り締まりに国境を越えた犯罪捜査が必要である。また、サイバー犯罪の定義が国際的に一致していないと犯罪捜査が困難になる。そこで、1997 年、欧州評議会に設置されたサイバー犯罪対策の専門家会合[23]において、本条約が起草され、2004 年に効力を生じるに至った。この条約は、性質上、

[21] S/RES/2129

[22] 人権、民主主義、法の支配の分野で国際社会の基準策定を主導するヨーロッパの国際機関。「欧州連合（European Union: EU）」とは異なる。

[23] アメリカ、カナダ、オーストラリア、日本、南アフリカの 5 か国もオブザーバーとして起草作業に参加している。

欧州評議会加盟国でなくとも批准することができる。



《Figure 3-1》　サイバー犯罪条約の署名・批准状況
（赤字は欧州評議会加盟国）

サイバー条約の内容は大きく以下の 3 つの部分に分けられる。

①　定義条項：何がサイバー犯罪であるかの定義 サイバー犯罪を国内犯罪とすることの義務化
②　捜査関連：証拠収集のための手続を法的に整備することの義務化
③　国際協力：犯罪人の引渡しや、他の締結国への捜査協力の義務化

つまり、この条約の批准国では、「①サイバー犯罪は『犯罪』として認められており、②あらゆる犯罪においてデータや機器の証拠を法的に収集することができ、 ③批准国同士での捜査協力や犯罪者の引渡しができる」という条件を満たす必要がある。

この条約には以下のような問題点がある。

国内法の整備

この条約を批准するためには、国内法を整備する必要がある。本条約の中で国内法を整

備すべきと定められているものについては、早急に法令作成や矛盾するものの削除などといった法制整備をしなければならない。そのため、署名から批准まで時間のかかるケースが多い。

国家主権との対立

ロシアや中国は、「インターネット空間上でも国家主権が尊重されるべき」としてこの条約に反対している。犯罪者の処罰やそのための捜査、特に強制捜査は、国家主権に属する事項とされるため、両者との折り合いを付けることは難しい。

未批准国との関係

「そもそも、サイバー犯罪は国境を越えて実行されるものであり、取り締まりに国境を越えた犯罪捜査が必要である」と記述したが、この条約がすべての国に批准されるまではこの目的は達成され得ず、サイバー犯罪の効率的な取り締まりは不可能である。

プライバシーの侵害

サイバー犯罪条約によって、市民のインターネット上のプライバシーの保護、通信の秘密などの人権が侵害されるおそれがある。犯罪取り締まりと人権問題のバランスを考えることが不可欠である。

現在の取組みとしては、批准国各国ベースで、上記の問題点を考慮しつつ、条約の批准国の増加に向けた取り組みを強調して行うとともに、未批准国の取り締まり当局とも捜査協力を深化させるなどの多面的な対応を進めている。

その他

他にも、「ロンドン国際サイバー会議」、「ブダペスト国際サイバー会議」、「ソウル国際サイバー会議」などの国際会議が行われている。この会議においても国連総会第 1 委員会と同様に、サイバー空間における国際安全保障のあり方に関する議論が行われている。

前項で触れたとおり、サイバー空間や ICT に関しては地域機構において議論されることも多い。具体的には北大西洋条約機構（North Atlantic Treaty Organization: NATO）、欧州連合（EU）、アジア太平洋経済協力（Asia-Pacific Economic Cooperation: APEC）、上海協力機構（SCO）などが挙げられる。個々の取り組みは多岐にわたるため、本書では記述しないが、皆さんの担当国が属する機構がこの議題についてどのようなスタンスでどのような取り組みを行っているのかについては調べてみても良いだろう。

サイバー空間に関する国際的な議論の流れのまとめ

国連総会第１委員会（軍縮・国際安全保障）

国際安全保障面からの ICT 開発

政府専門家会合（GGE）

情報セキュリティ領域の脅威

それに対抗するための協力施策

情報セキュリティ強化のための国際的規範の作成

国連総会第２委員会（経済・開発）

サイバーセキュリティに関する世界文化の創成

開発のための ICT

国連人権委員会（UNHRC）

インターネット上の言論・表現の自由

欧州評議会（サイバー犯罪条約）

国際的なサイバー犯罪の取り締まりに関する取り決め

各種国際会議

地域機構　　など

インターネット上の知的財産の取扱い

サイバー空間上の国際的行動規範に向けた取り組み　など

第４章　　論点説明

第 3 章で国際的なこれまでの話し合いの流れを俯瞰した。それでは今回の会議ではどのような論点で話し合いを行うのかについてこの章ではまとめたい。今回の会議は、論点 1 として**情報セキュリティを確保するためのアプローチ**、論点 2 として**国際的規範**のうち**各国家の責任ある行動についての規範**、論点 3 として**国際的規範**のうち**サイバー途上国・新興国のキャパシティ・ビルディング**について話し合ってもらう。

4-1　論点 1　情報セキュリティを確保するためのアプローチ

どのようにして情報セキュリティを維持するかについての見解は、第 3 章で説明したとおり分かれている。この論点では、情報セキュリティを確保するためのアプローチとは「インターネットやインフラなどという技術のみを保護するもの」なのか、それとも「情報の統制なども含めたもの」なのか検討してほしい。

初めて ICT･サイバー空間に関する議題が国連総会第 1 委員会に持ち込まれた 1998 年（53 会期）の決議[24]はコンセンサスで採択されたものの、アメリカが今後の話し合いに向けて消極的であったり、オーストラリアやエジプトは決議案の曖昧な文言に懸念を示したり[25]と、今後の議論に向けて不安の残るものであった。

しかしながら、第 3 章で説明したように、第 1 委員会での議論は GGE の議論を追う形とはいえ、かなり進んできた。決議の内容についても、サイバー空間の脅威について確認する漠然としたものから、サイバー空間上にある脅威への対処のしかたや、国際的な取り決め作りにまで言及されるようになってきている。

ただし、冒頭で挙げた、情報セキュリティの捉え方、情報セキュリティの維持のアプローチについては未だ議論の決着を見ていない。本来ならこれを前提として、サイバー空間の脅威への対処ならびに国際的な取り決め作りという点に話が及んでいくべきではなかろうか。したがって、この論点の議論は、大論点 2・3 の議論と密接に関連するものとなる。

予想される対立

ICT やサイバー空間の中心となっている「インターネット」はアメリカを中心に発展したものであり、インターネットを維持する団体の 1 つ[26]がアメリカの商務省と強いつながりを持つなど、ICT・サイバー空間についてアメリカが主導権を握っていた。それに対し、中国やロシアなどの国が強い危機感を持ち、サイバー空間の主導権を奪還したいと考えている。

[24] A/RES/53/70
[25] A/C.1/53/PV.24
[26] Internet Corporation for Assigned Names and Numbers: ICANN

第 3 章で触れた「情報セキュリティのための国際行動規範（International code of conduct for information security）」の提出についてもサイバー空間の取り決めを主導したいという気持ちが表れている。

そのような対立のほかにも、アメリカや西欧諸国は、ICT の発展を目論んでおり、それに伴う、適切なインフラやインターネットの技術に対する保護は必要としながらも、民間分野での発展においては情報の自由な流通が不可欠であるため、国家による情報の統制など認められないのに対し、ロシア、中国は ICT や情報それ自体の安定とその脅威をなくす、すなわち、情報を国家の統制下に置きたい、また、自国の情報へのアクセスを制限したいという国家主権の尊重を由来とする思惑があるため、情報セキュリティのとらえ方には第 3 章 1 節で述べたような差異が出てしまった。

そのような対立が未だ続いていることの証左として、第 3 章で述べた「サイバー犯罪条約」がある。ロシアと中国はサイバー犯罪条約第 32 条「蔵置されたコンピュータ・データに対する国境を越えるアクセス」という条文に強く拒否反応を示している。この条文は、相互援助のためならば、批准国にあるコンピュータやデータに互いにアクセスできるという趣旨の内容であり、前述のロシア、中国の考えとは矛盾することがわかる。

加えて、2011 年のジャスミン革命を発端とした「アラブの春」における市民同士のリアルタイムな連絡や国内外への情報の発信にインターネットや SNS が活用されたことを受け、新興国・途上国についても、インターネットへの規制や政府の管理を強化する動きが強まり、言論・表現の自由に反するとして不快感を示す西欧諸国などとの対立がますます根深くなっている。

論点 1 まとめ

- 議論の前提である「情報セキュリティ」の捉え方について、いままで国際的な議論の決着が見られなかった。
- 主に「表現の自由」と「国家主権」の対立などが見られる。
- 「アラブの春」以降、途上国も巻き込んだ議論となっている。

情報セキュリティとはインターネットやインフラなどという「技術」のみを保護するものなのか、それとも「情報の統制」なども含めたものなのか議論してほしい。

4-2　論点 2　国際的規範――各国家の責任ある行動についての規範

この論点において議論してほしいのは主に以下の 2 点である。

①第 4 回 GGE の事務総長レポートの該当部分の具体化（と拡張）

②「情報セキュリティのための国際行動規範」の扱い

国連総会第 1 委員会において目標とされているものの一つとして、「サイバー空間における国際的な規範」の作成がある。これは第 2 回 GGE から議論が始まったもので、2008 年以降のサイバー攻撃の増加や、2011 年の「アラブの春」が背景となって、その重要性は高まっているといえる。

各国家の規範については過去の GGE でも繰り返し議論されており、第 3 章で触れたが、2011 年に中国・ロシア・タジキスタン・ウズベキスタンの 4 カ国が「情報セキュリティのための国際行動規範（International code of conduct for information security）」を提出するなど、活発な議論が行われている。

今回の議場は第 5 回 GGE である。第 5 回 GGE においては、サイバー空間におけるこれまで作成されてきた規範がより具体的・実効的になることが期待されている。そのため、各国家の行動についての規範に関する議論は、**第 4 回 GGE の国連事務総長レポート[27]第 3 章を踏まえ、それを具体化したり、それに実効力を持たせたりして**いただきたい。

第 4 回 GGE 事務総長レポート 第 3 章

第 3 章でも軽く触れたが、第 4 回 GGE の第 3 章は「各国家の責任ある行動についての規範、規則、あるいは原則（Norms, rules and principles for the responsible behaviour of States）」についてまとめた章である。その前提、および規範作りで目指す目標は以下のとおりである。

> 9. The ICT environment offers both opportunities and challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities. One objective is to identify further voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment.

皆さんにはこの前提、規範作りで目指す目標を踏まえたうえで議論していただきたい。

実際に過去の議論において具体化がすすめられたのは、第 4 回 GGE の報告書でいう 13 条の部分にあたる。

> 13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous

[27] A/70/174

Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

赤字で示した通り、この条文には具体的な提案が続く。会議準備の際に必ず参照してほしいが、「サイバー犯罪の検挙における国際協力（d 項）」「表現の自由の尊重（e 項）」など条文が未だ具体的とは言えない項や、「悪質なサイバー攻撃への国家の関与の禁止（k 項）」などの未だ対立が予想される項がある。皆さんには、「各条文が国際規範に必要なのか」「他にどのような条文が必要か」「各条文に書かれたことを実施するためにはどのような取り組みが必要か」などについて各国家の立場から考えたうえで、冒頭で挙げた「①**第 4 回 GGE の事務総長レポートの該当部分の具体化（と拡張）」「②『情報セキュリティのための国際行動規範』の扱い」**について議論していただきたいと思う。

もちろん国際的なルール作りであるから、国際的な合意が必要不可欠であるが、同時に具体性がなかったり、ICT・サイバー空間特有の性質（本書第 2 章 4 節で触れたサイバー攻撃の性質を含む）を捉えられていなかったりするルールにはあまり意味がなく、国際社会に与える影響も小さくなってしまうだろう。

必読文書

なお、この論点については前述の通り以下の国連文書を読んだことを前提とした議論を行う。資料の検索方法については第 5 章 2 節を参照のこと。

- **A/70/174** “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security Note by the Secretary-General”
- **A/66/359** “Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General”

論点 2 まとめ

- 「各国家の責任ある行動についての規範」については第 2 回 GGE から毎回議論が行われている。
- 第 4 回 GGE の報告書第 3 章や、「情報セキュリティのための国際行動規範」が現状の提案として挙げられる。
- しかし、未だ抽象的な論にとどまっている、ICT・サイバー空間の特性を捉えられていないなど課題点が多い。

国際的な規範であることに注意しながら、現状の提案を踏まえて、より具体性・実効性のある国際的規範を作成してほしい。

4-3　論点 3　国際的規範――サイバー新興国・途上国のキャパシティ・ビルディング

サイバー空間には国境がない。それゆえ悪意のある ICT の利用に対処するためには、国際的な協調が必要である。この論点は、サイバー新興国・途上国を具体的にどのように支援すべきなのかについて考えてもらう。

GGE において、毎回議論が行われている論点の一つとして、サイバー後進国・途上国のキャパシティ・ビルディングが挙げられる。サイバー空間は全世界とつながっている。したがって、1 国だけがセキュリティを強化しても、繋がっている地域のセキュリティが脆弱だと、効果が薄くなってしまう。しかし、だからといってセキュリティが脆弱な地域との繋がりを断つということは難しい。国連憲章で認められている、開発のための機会均等の原則を侵害しかねないなどの問題があるからだ。

よって、サイバー新興国・途上国のセキュリティは強化されなければならないのだが、その国自身に技術がなかったり、インフラを維持する金銭的余裕がなかったりする場合が多い。そのような国にどのような援助を行っていくのかが重要な課題となっている。

また、論点 2 とも関連するのだが、「規制と発展のバランス」という問題も考慮しなければならない。「アラブの春」以降サイバー新興国・途上国の中には、民主化運動を懸念してインターネットへの規制や、政府での管理を強化している国も多いのは前述したとおりである。当事国に取ってみると、サイバーテロリストを撲滅するための規制であるが、それがサイバー空間の発展（や表現の自由をはじめとした人権）を阻害している一面もある。そういった国内規制と共存した形で援助を進めるのか、はたまた規制を撤廃しないと援助ができないのかについても検討しなければならない。

キャパシティ・ビルディングとは

第 3 章より注釈なしで「キャパシティ・ビルディング」という用語を用いてきたが、具体的にどういうことを指すのかについて簡単にまとめる。

国際連合工業開発機関（United Nations Industrial Development Organization: UNIDO）では「工業開発のために必要な途上国側の組織的能力を構築すること」と定義[28]している。つまり、技術援助はもちろん、途上国側でも内発的に自己成長できるように社会制度や政策を整備し、社会システムを改善していくことを指す。なお、近年はキャパシティ・デベロップメント（Capacity Development）と呼称されるケースも多く、これはより「内発的な自己成長」に焦点を当てた用語である。

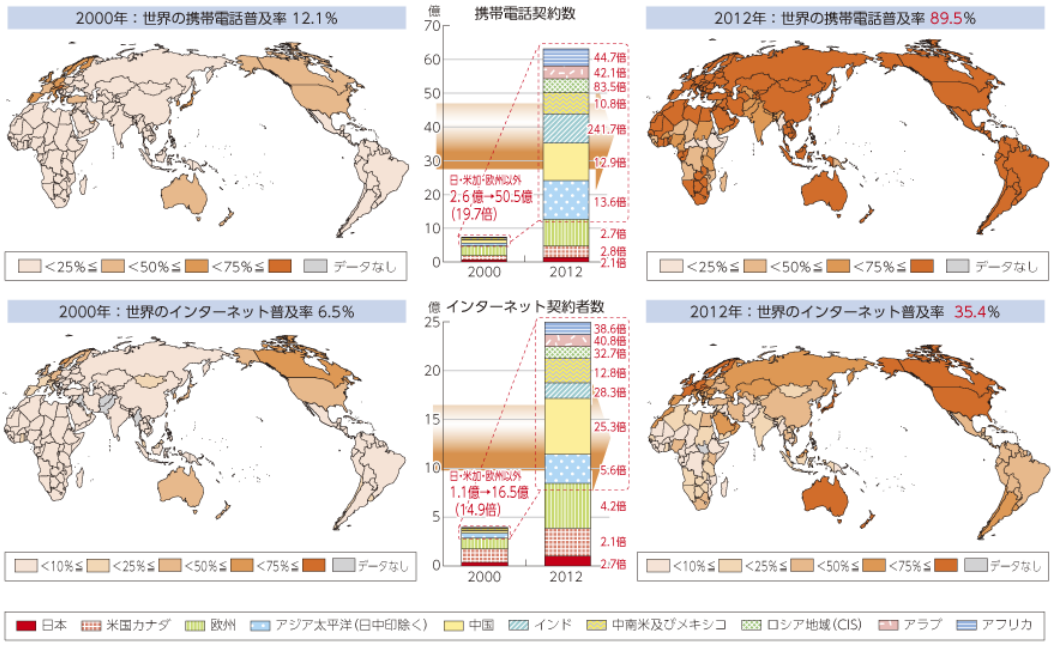
皆さんが政策を考える際にも、先進国と途上国にある「技術開発におけるギャップを埋める」ことだけではなく、持続的に ICT 開発が進められるように、途上国自身による意思

[28] 「キャパシティ・ビルディング」（UNIDO）<http://www.unido.or.jp/outcome/capacity_building/>

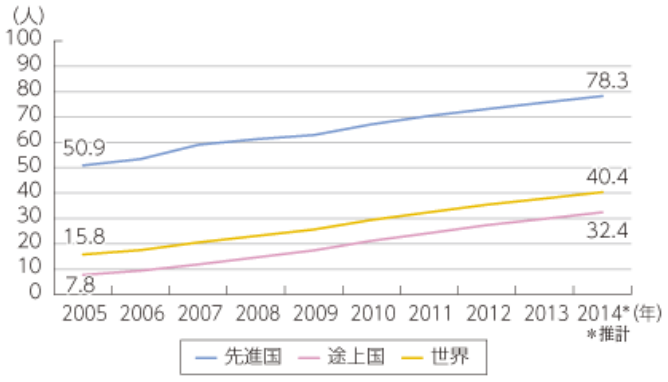
決定や行動を助ける知識やアイデアを共有する、といったような「内発的な開発を後押しする」ことを念頭に置いてほしい。

ICT の国際格差

ICT は国際的に急速に浸透しているといえる。《Figure 4-1》は 2000 年時点と 2012 年時点の携帯電話とインターネットの普及状況を世界地図で示したものである。2000 年現在では、日本や韓国、ヨーロッパの一部の国で普及率が 75%を超えているものの、途上国においては 25%に届かない国も多い。しかしながら、2012 年には、先進国はもとより、多くの途上国でも普及率は 75%を超えており、先進国・途上国を問わず、世界的に携帯電話の普及が進んでいることが見て取れる。インターネットについても同様に、世界的に普及が進んでいると言えるが、先進国と途上国の間で普及率に差があることは、《Figure 4-2》を見てもよく分かる。



《Figure 4-1》　世界における携帯電話およびインターネット普及率の変化



《Figure 4-2》
住民 100 人あたりの
インターネットユーザー数

一方でアフリカでは、農業や医療分野などさまざまなところで ICT の活用が進んでおり[29]、今後インターネット普及率などの格差は縮小すると予想されている。

しかし、ICT が普及することで、サイバー攻撃者が増えるという側面もある。そこで、特に途上国におけるサイバーセキュリティの向上をどのように援助できるかについて皆さんには考えてもらわなければならない。

論点 3 まとめ

- サイバー空間の繋がりを考慮すると、サイバー新興国・途上国への援助は必須である。
- 「アラブの春」以降、サイバー新興国・途上国の中には、自国における規制を強化する国も多い。
- しかし、その規制がサイバー空間の発展を阻害している側面もある。

ICT やサイバー空間の発展にどのように援助する/されるべきなのか、また、サイバー新興国・途上国における規制との兼ね合いをどうするべきか、考えてほしい。

[29]「平成 26 年度版情報通信白書[第 1 部第 3 節様々な社会的課題と ICT による課題解決]」（総務省）<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc113000.html>

4-4　アウトオブアジェンダ

模擬国連会議において、会議中に議論できない話題のことを「アウトオブアジェンダ」と呼ぶ。アウトオブアジェンダとされた内容に関する条文は決議に載せることはできない。

国際的規範――信頼醸成措置

第 4 回 GGE についての事務総長レポートが 5 つの要素で構成されていることは本書第 3 章にて述べた。そのうち「信頼醸成措置」については、論点との関係が特に薄いと判断し、議論の内容から外すこととした。

なお、レポートのうち、「国際協調体制の構築」や「サイバー空間における現在の脅威」、「ICT の利用においてどのように国際法が適用されるか」という部分については、論点との関連性が認められる範囲で話し合いを認める。

国連総会第 1 委員会および GGE における議論を逸脱したもの

今回の議場は、第 5 回 GGE である。GGE は国連総会第 1 委員会の議論を踏まえて専門家が議論する場である。そのため、国連総会第 1 委員会における「国際安全保障の文脈における情報及び電気通信分野の進歩（Development in the field of information and telecommunications in the context of international security）」という議題のもとで行われた議論、及び 4 回開かれた GGE の議論から大きく逸脱した議論は認めない。

例えば、サイバー犯罪条約の是非に関する議論などが該当する。

その他、あまりに専門的すぎる議論

議題の性質上、前提となる専門知識に顕著な差が見られる可能性がある。会議準備の中でも様々な専門用語に出会うことが予想される。そこで、自分が知っていることを相手が知っているとは限らないという前提のもと、紳士的な議論を行っていただくよう強く要請する。また、議論の中で技術的な議論や法的な議論が白熱してしまうことが予想されるが、議場全体が理解しているかどうかには常に気を配って欲しい。なお、専門的すぎる議論の判定は会議監督が行う。

第 5 章　　会議準備の手引き

この章では、会議準備において注意すべきこと、および会議準備に役に立つツールなどを紹介する。一般的な会議準備については、グローバル・クラスルーム日本委員会発行の「模擬国連マニュアル 2015」が詳しいので併せて参照してほしい。

5-1　情報収集に際して

会議準備をすすめるにあたって、皆さんは様々な情報を収集するかと思う。その際に特に留意してほしいことを 3 つ示す。

少ない公開情報

ここまで本書を読み進めた皆さんなら気づくかもしれないが、今会議の一番の難しさは、**各国に関する情報が完全には公開されていない**ことである。ICT やサイバー空間は、我々の暮らしをより便利にするという側面がある一方、軍事的には最先端分野であり、多くの国が重要な分野として捉えているため、各国がどのような戦略のもと、ICT やサイバー空間の発展や規制に取り組んでいるかがわかる資料はとても少ない。それゆえ、情報収集したうえで、その限られた情報の中から自国の考えを推測、想像しなければならない。

不正確な情報

また、**不正確な情報が多い**というのも残念ながら事実である。今回のテーマは公開情報が少ないからこそ、様々な憶測が飛び交ってしまう一面がある。本書を執筆するにあたり、様々な書籍や論文、インターネット記事にあたったが、推測にすぎない情報やそもそも事実と異なる情報も一部見られた。会議準備の際にも、自分が得た情報が果たして正確なものかどうか、細心の注意を払ってほしい。

情報の鮮度

ICT やサイバー空間は近年特に注目が集められている分野である。また、第 2 章で「ムーアの法則」という話題に触れたが、技術の進歩が著しい分野でもある。それゆえ、**情報の更新スピードが早い**という一面がある。例えば 10 年前 iPhone は存在しなかったわけで、その時代の ICT の情報と現在の ICT の情報が大きく異なるのは用意に想像がつくだろう。したがって、自分が持つ情報がいつの情報なのかについて常に意識する必要がある。

5-2　リサーチに役立つ資料

議題概説書には議題に関する一般的な情報をできるだけ多く掲載し、各国の事情にはあまり踏み込んでいない。よって、皆さんはここから自分の担当国の事情について調べていくことになるが、その上で参考になる資料やツールを紹介する。

書籍、Web 資料

特に参考になるものは参考文献一覧に載せているが、書籍、Web 資料はそれ以外にも多数存在する。しかしながら、ICT やサイバー空間については様々な考えが存在し、一方の考えに立脚した資料が多い。資料を取捨選択しながらリサーチすることが大事である。

その上で、どの国を担当するにしろ、国際的なパワーバランスを概観するために参考になる書籍として以下の 2 冊を挙げる。もちろん全部読む必要は無いが、いずれか 1 冊について概要をつかむだけでも現在のサイバー情勢が見えてくると思う。

- **伊東寛『「第５の戦場」サイバー戦の脅威』**

サイバー軍拡や悪意のある ICT 利用について、国際的な情勢をまとめられている。日本の現状に警鐘を鳴らす意図で書かれているため、全体的にやや不安感を煽る要素が強く、憶測と思われる部分も多々あるが、専門の技術用語などは用いず平易に説明されているため初学者でも読みやすい。

- **リチャード・クラーク、ロバート・ネイク『核を超える脅威　世界サイバー戦争』**

アメリカ政府に関係のあるサイバーセキュリティ専門家である著者が、国家レベルのサイバーセキュリティについてまとめている。全体を通して国家レベルでの議論であるため、サイバー空間によっていかに国際的なパワーバランスが変容したかなどについてわかりやすい。少々専門用語が多い点、アメリカ寄りの考え方である点には留意する必要がある。

Cyberwellness Profiles[30]

Cyberwellness Profiles とは ITU が発行している各国のサイバー空間に解する情勢についてまとめた資料である。どの国の資料も「Legal Measures（法律の整備状況）」「Technical Measures（技術の発展状況）」「Organizational Structures（政府としてのサイバー空間への取り組み状況）」「Capacity Building（キャパシティ・ビルディングの状況）」「International Cooperation（国際協調の状況）」の 5 つの領域についてまとめられている。各国のサイバー情勢を概観する上では一番わかりやすく、各国のサイバー空間に対する政策の資料へのリンクもあることもあるため、少なくとも担当国の資料は見ておきたい。

[30] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx

国連文書の調べ方

今会議の準備にあたっては、国連の決議、議事録、作業文書などを読むことが多くなると思う。そこで今回は国連文書の調べ方についてまとめる。

文書記号がわかっている場合

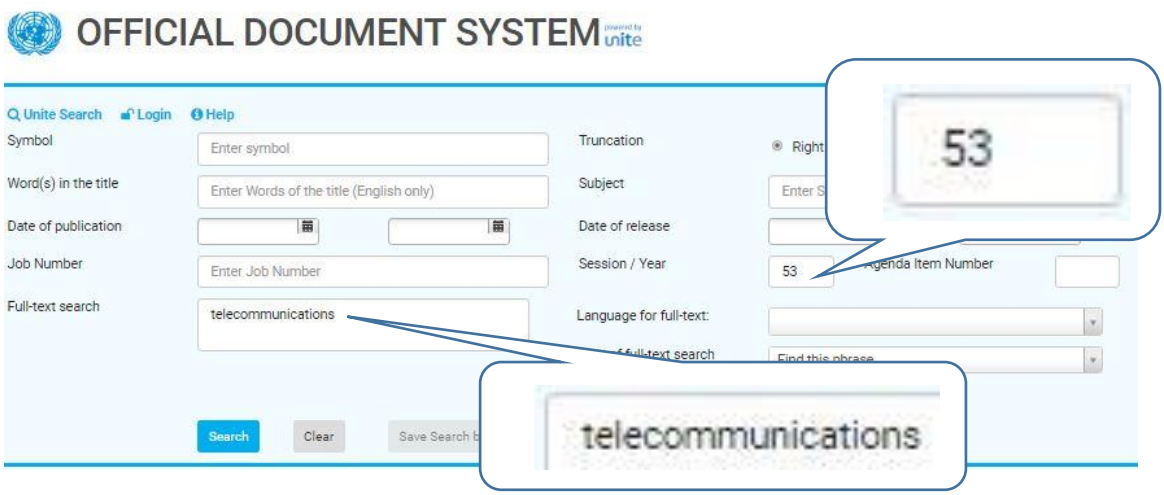
国連文書には固有の文書記号[31]が付されている。本書においても重要な文書や引用した文書については脚注に文書記号を付している。例えば、第 4 回の GGE の報告書は［A/70/154］である。このように文書記号がわかっている国連文書を閲覧する際は、「http://undocs.org/A/70/154」のように、「http://undocs.org/(文書記号)」と直接 URL に入力するのが便利である。

文書記号がわからない場合

もちろん閲覧したい国連文書の文書記号がわからない場合もあるだろう。そういった場合は、国連文書検索サービスである、United Nations Official Documents System（ODS・https://documents.un.org/prod/ods.nsf/home.xsp）を利用する。ここでは、今回の議題、「国際安全保障の文脈における情報及び電気通信分野の進歩」が最初に話し合われた第 53 会期の国連総会第 1 委員会に関連する資料を調べてみたい。

[31] 文書記号について詳しくは、国連広報センターの Web ページ上にある「文書記号」（http://www.unic.or.jp/texts_audiovisual/libraries/research_guide/research/symbols/）を参照すると良い。

①「Full text search」欄に”telecommunications”などと入力[32]し、「Session / Year」欄に”53”と入力する。



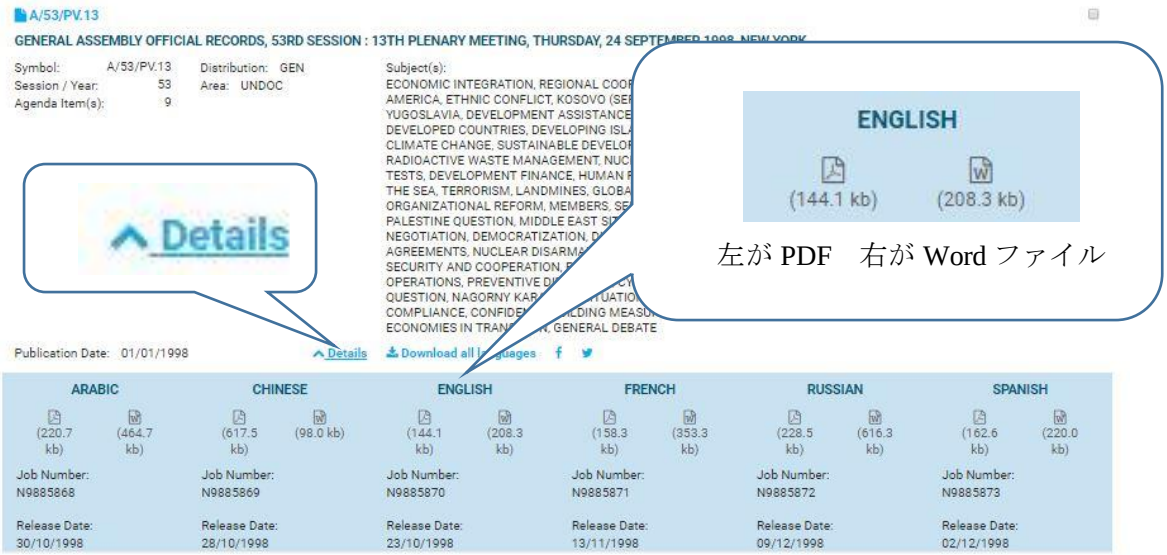
《Figure 5-1》　ODS 検索画面

②様々な資料の中から閲覧したい資料を見つける。

《Figure 5-2》　ODS 検索結果画面

[32] 単語の数が多すぎると検索できなくなることが多いので、議題に特有な単語を入れると良い。

③今回は議事録（A/53/C.1/PV.53）を閲覧してみる。「Details」をクリックすると、各言語の資料が表示されるので、目的の資料をクリック。PDF か Word ファイルの形でダウンロードすることが可能である。



《Figure 5-3》　A/53/PV.13 詳細画面

図版出典

《Figure 2-1》

Mollick E. *Establishing Moore's Law.* <http://ieeexplore.ieee.org/document/1677462/>

《Figure 2-2》

「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」（警察庁）

《Figure 2-3》

「DoS/DDoS 攻撃について」（Andmem）<http://andmem.blogspot.jp/2014/02/dosattack.html>

《Figure 3-1》

”Convention on Cybercrime”（Council of Europe）<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

《Figure 4-1》

総務省（2016）「情報通信白書平成 28 年度版」

《Figure 4-2》

同上

《Figure 5-1》

United Nations Official Documents System <https://documents.un.org/prod/ods.nsf/home.xsp>

《Figure 5-2》

同上

《Figure 5-3》

同上

参考文献

書籍

- 伊東寛、『「第５の戦場」サイバー戦の脅威』、祥伝社、2012 年
- 小林雅一、『AI の衝撃　人工知能は人類の敵か』、講談社、2015 年
- リチャード・クラーク　ロバート・ネイク、『核を超える脅威　世界サイバー戦争』、徳間書店、2011 年
- Ray Kurzweil. (2006). “The Singularity Is Near: When Humans Transcend Biology”. Viking.

論文

- 市川類（2010）「米国連邦政府のサイバーセキュリティ政策を巡る動向」、『ニューヨークだより（IPA）』、2010 年 3 月号
- Franz-Stefan G. & Greg A. (2009). *Russia, The United States, And Cyber Diplomacy: Opening the Doors*. East West Institute.
- Mollick E. (2006). *Establishing Moore's Law.* IEEE Annals of the History of Computing, 28(3), 62-75.
- Tim M. (2011). *Cyber Norm Emergence at the United Nations–An Analysis of the UN's Activities Regarding Cyber-security*. Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project.

国連決議等

国連総会決議

- “Creation of a global culture of cybersecurity and the protection of critical information infrastructures” （A/RES/57/239～A/RES/64/211）
- “Development in the field of information and telecommunications in the context of international security” （A/RES/53/70～A/RES/70/237）
- “Information and communication technologies for development” （ A/RES/62/182 ～ A/RES/70/184）
- “Integrated and coordinated implementation of and follow-up to the outcomes of the major United Nations conferences and summits in the economic and social fields” （A/RES/57/270B）
- “World Summit on the Information Society” （A/RES/56/183～A/RES/60/252）

国連総会作業文書

- “Development in the field of information and telecommunications in the context of international security” （A/60/202、A/65/201、A/66/359、A/68/98、A/70/174）

国連総会第 1 委員会議事録

- “Development in the field of information and telecommunications in the context of

international security”（A/C.1/53/PV.5 など）

国連総会第 1 委員会作業文書（決議案）

- “Development in the field of information and telecommunications in the context of international security”（A/C.1/53/L.17 など）

その他

- “Convention on Cybercrime”
- “Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century”

各種報告書・Web 資料（最終閲覧日は 9 月 30 日）

- インターネット政策に関する国際的な議論の動向（総務省）
  <http://www.soumu.go.jp/iicp/chousakenkyu/data/research/lecture/20121116-hachinohe.pdf>
- インターネット国際公共政策課題に関する国際的な議論(国連及び ITU)の動向について（日本インターネットプロバイダー協会）
  <http://www.jaipa.or.jp/event/IGF-J/140314/IGF-Japan_ichikawa.pdf>
- 「キャパシティ・ビルディング」（UNIDO）
  <http://www.unido.or.jp/activities/capacity_building/>
- 「国連を舞台に、サイバースペースをめぐって大国が静かにぶつかる」（Newsweek）
  <http://www.newsweekjapan.jp/tsuchiya/2015/09/post-3.php>
- 「サイバーセキュリティ政策推進に関する提言」の公表（総務省）
  <http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000093.html>
- 「情報通信白書平成 28 年度版」（総務省）
  <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/index.html>
- 「日本年金機構における個人情報流出事案に関する 原因究明調査結果」（内閣府・サイバーセキュリティ戦略本部）<http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf>
- 平成 27 年におけるサイバー空間をめぐる脅威の情勢について（警察庁）
  <http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf>
- 「ロボット戦争」数年で現実に　ＡＩ兵器開発禁止訴え、ホーキング博士ら研究者が警告（産経ニュース・2015 年 8 月 2 日）
  <http://www.sankei.com/life/news/150802/lif1508020014-n2.html>
- Cyberwellness Profiles(ITU)
  <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx>
- Development in the field of information and telecommunications in the context of international security (United Nations) <http://www.un.org/disarmament/topics/informationsecurity/>
- Experts Warn UN Panel About the Dangers of Artificial Superintelligence (Gizmodo)
  <http://gizmodo.com/experts-warn-un-panel-about-the-dangers-of-artificial-s-1736932856>