サイバースペースの安定性に関する
グローバル委員会

サイバースタビリティの向上

最終報告書
2019年11月

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

平和と繁栄を築くためのサイバースペースの安定性の促進

サイバースペースの安定性に関するグローバル委員会（GCSC）は国際的な安全保障と安定性を強化し、サイバースペースにおける国家と非国家の責任ある行動を導くための規範と政策の提案を策定する。

本レポートの和訳は、慶應義塾大学から資金提供されました。

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

サイバースタビリティの向上

最終報告書
2019年11月

ハーグ戦略研究所
Lange Voorhout 1
2514 EA The Hague
info@hcss.nl
www.hcss.nl

イーストウェスト研究所
ニューヨーク | ブリュッセル
モスクワ | サンフランシスコ
cyber@eastwest.ngo
www.eastwest.ngo

委員長

Michael Chertoff（米国）
Latha Reddy（インド）
Marina Kaljurand（エストニア）*【前委員長】*

委員

Abdul-Hakeem Ajijola（ナイジェリア）
Virgilio Almeida（ブラジル）
Isaac Ben-Israel（イスラエル）
Scott Charney（米国）
Frédérick Douzet（フランス）
Anriette Esterhuysen（南アフリカ）
Jane Holl Lute（米国）
Nigel Inkster（イギリス）
Khoo Boon Hui（シンガポール）
Wolfgang Kleinwächter（ドイツ）
Olaf Kolkman（オランダ）
Lee Xiaodong（中国）
James Lewis（米国）
Jeff Moss（米国）
Elina Noor（マレーシア）
Joseph S. Nye, Jr.（米国）
Christopher Painter（米国）
Uri Rosenthal（オランダ）
Ilya Sachkov（ロシア）
Samir Saran（インド）
Marietje Schaake（オランダ）
土屋 大洋（Motohiro Tsuchiya）（日本）
Bill Woodcock（米国）
Zhang Li（中国）
Jonathan Zittrain（米国）

特別代表・アドバイザー

Carl Bildt（スウェーデン）
Vint Cerf（米国）
Sorin Ducaru（ルーマニア）
Martha Finnemore（米国）

ディレクター

Alexander Klimburg（オーストリア）
Bruce W. McConnell（米国）

研究アドバイザリーグループ委員長

Sean Kanuck（米国）
小宮山功一朗（Koichiro Komiyama）（日本）
Marília Maciel（ブラジル）
Liis Vihul（エストニア）
Hugo Zylberberg（フランス）

事務局

The Hague Centre for Strategic Studies

EastWest INSTITUTE

パートナー

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

スポンサー

スイス連邦外務省
GLOBSEC
エストニア共和国外務省
日本総務省

支援機関

アフリカ連合委員会
ブラックハットUSA
DEF CON
国際連合在ジュネーブ欧州連合代表部
サイバー専門的知識に関するグローバルフォーラム
グーグル
ハーグ基礎自治体
パケット・クリアリング・ハウス
テルアビブ大学
国連軍縮研究所

目次

委員長からのレター

サイバースペースは人類の最大の発明の一つであり、個人、社会、ビジネス、政治的関係を再形成しています。残念なことに、サイバースペースへの攻撃やサイバースペースを介した攻撃により、その安定性を確保するために緊急対策が必要とされています。このサイバースペースの安定性という概念には、その近親者である国際的安定性と同様に、地政学的な意見の相違やサイバースペースに影響を与える変化が比較的平和に管理されなくてはならないこと、そしてサイバースペースの安定性が保証されなければならないことを全ての関係者が認識するという共通のビジョンが求められています。

サイバースペースの安定性に関するグローバル委員会は、国際平和と安全保障という本来は国家が対処するものであった問題が、他の利害関係者を巻き込むことなく対処することがもはや可能ではなくなっているという信念から取り組みに着手しています。サイバースペースはマルチステークホルダーの環境です。サイバースペースを構築し管理する者や、サイバースペースへの攻撃やサイバースペースを介した攻撃に対応する者が、政府の高官である可能性と同様に非国家主体である可能性があるのです。我々の委員はこの特徴を反映するように選出しています。国際安全保障問題について経験を有する元上級政府高官の他に、インターネット・ガバナンス、人権や開発に関するコミュニティ、技術や産業における著名な指導者も含まれています。16カ国から集まった28人の委員が協力し、幅広い経験や意見を提供し、委員会によるアウトリーチに反応したパブリックコメントにも助けられました。

委員会の最終報告書は、3年間にわたる多大な努力の成果です。これを可能にしてくださった委員、アドバイザー、研究者（その多くはボランティアとして活動してくださいました）、財政的支援者、運営委員会の皆様には感謝の意を表します。最後に、プロセスを適切に管理してくださっただけでなく、市民社会のイニシアチブとしての当委員会の設立に尽力してくださった事務局に感謝の意を表したいと思います。

委員会は、作業を通じて過去と現在の両方のサイバースペースに関する取り組みについて認識しておりました。我々の報告書「*サイバースタビリティの向上（原題：Advancing Cyberstability）*」は、他の研究を補完し補強する一方で、サイバースペースの安定性を高めるための新しいアイデアを提供します。

Michael Chertoff
共同委員長
サイバースペースの安定性
に関するグローバル委員会

Latha Reddy
共同委員長
サイバースペースの安定性
に関するグローバル委員会

エグゼクティブ・サマリ

我々は、25年間にわたって大国間の戦略的な安定性と相対的な平和が維持されてきた期間の終わりを迎えた。国家間の紛争は新たな形態で行われるようになり、サイバー活動は新しく変わりやすい環境において主導的な役割を果たしている。過去十年間の間に、国家や非国家主体によるサイバー攻撃の数と洗練度が上がり、そのためサイバースペースの安定性が脅かされている。簡単に述べると、人々や組織はサイバースペースを安全かつ安定的に使用する能力について自信を失っているか、サービスや情報の可用性と完全性が保証されなくなっていると感じている可能性がある。

このような背景の下、サイバースペースの安定性に関するグローバル委員会（GCSC）を召集し、サイバースタビリティの向上に向けた勧告を作成した。我々はまず、サイバースタビリティの枠組みを構成する七つの要素を特定した。この枠組みには以下の7点が含まれている。1. マルチステークホルダー・エンゲージメント、2. サイバースタビリティの原則、3. 自主的な規範の策定と実施、4. 国際法の遵守、5. 信頼性構築に向けた施策、6. キャパシティ・ビルディング、7. サイバースペースがレジリエンスを有していることを担保する技術基準の公布と広範な使用。この枠組みを定義した後、委員会はマルチステークホルダー・エンゲージメント、原則、規範の三要素をさらに詳しく検討した。

マルチステークホルダー・エンゲージメントは多くの国際合意において呼びかけられているが、争点のままであり続けている。国際的な安全保障と安定性の確保がほぼ完全に国家の責任であると考えて続けている者もいる。しかし実際には、サイバー戦場（すなわちサイバースペース）は主に非国家主体によって設計、展開、運営が行われており、我々はサイバースペースの安定性を確保する上で彼らの参加が必要であると考えている。さらに、非国家主体はサイバー攻撃に最初に対応し、さらには帰属することも多いため、彼らの参加は避けられない。

委員会では、これらの非国家主体がサイバースペースの安定性を確保する上で重要であるだけでなく、彼らもまた原則によって導かれ、規範によって拘束されているべきであると結論づけている。四つの原則はこの視点を反映しており、全ての関係者に責任を持ち、自制を心がけ、行動を取り、人権を尊重するように呼びかけている。

- 責任：誰もがサイバースペースの安定性を確保するための責任を負っている。
- 自制：国家も非国家主体もサイバースペースの安定性を損なうような行動を取るべきではない。
- 行動義務：国家または非国家主体はサイバースペースの安定性を確保するために合理的で適切な措置を講じるべきである。
- 人権の尊重：サイバースペースの安定性を確保するために努力するにあたり、人権と法律を尊重しなければならない。

これらの原則を基に、委員会は他の組織による成果を補完しつつ重複しないように注意しながら、サイバースペースの安定性をよりよく確保しこれまでに宣言された規範における技術的な懸念やギャップに対応するように設計された八つの規範を策定した。

1. 国家および非国家主体は、インターネットのパブリック・コアの全体的な可用性または完全性、そしてそれによってサイバースペースの安定性に大幅な損害を意図的に与えるような活動を行ったり、そのような活動を故意に許したりしてはならない。
2. 国家および非国家主体は、選挙、住民投票、直接投票に不可欠な技術的インフラを破壊することを目的としたサイバー活動を追求・支援・許容してはならない。
3. 国家および非国家主体は、開発中・生産中の製品やサービスを改ざんしてはならず、また、サイバースペースの安定性が実質的に損なわれる可能性がある場合も改ざんを許してはならない。

4. 国家および非国家主体は、ボットネットや同様の目的で利用ために一般市民のICT資源を徴用してはならない。

5. 国家は、情報システムや技術に関する未公開の脆弱性や欠陥を開示すべきか否か、またいつ開示すべきかを評価するために、手続き的に透明性のある枠組みを構築すべきである。基本的には開示することを前提とすべきである。

6. サイバースペースの安定性を構成している製品やサービスの開発者や生産者は1. セキュリティと安定性を優先し、2. 製品やサービスに重大な脆弱性がないことを担保するための合理的な措置を講じ、3. 後になって発見された脆弱性を適宜緩和するための措置を講じるとともにそのプロセスについて透明性を確保しておくべきである。全ての行為主体は、悪意のあるサイバー活動を防ぎ緩和するために脆弱性に関する情報を共有する義務を負う。

7. 国家は法律や規制を含む適切な施策を制定し、基本的なサイバー衛生を確保すべきである。

8. 非国家主体は攻撃的なサイバー活動に従事してはならず、国家行為主体はそのような活動を防止し、発生した場合には対応すべきである。

勧告

最後に、マルチステークホルダー・エンゲージメントの重要性と、行動規範を宣言したからといって、それが規範になるわけではないという事実を両方とも認識した上で、委員会は、マルチステークホルダー・モデルの強化、規範の採択と実施の促進、規範に違反した者の説明責任の確保に焦点を当てた六つの提言を行っている。

具体的には、委員会は以下の通り勧告を行う。

1. 国家と非国家主体は自制を促進し、行動を促すことによってサイバースペースの安定性を高めるような規範を採用し実施すること。

2. 国家と非国家主体は、それらの責任と限界に沿って規範の違反に適切に反応し、規範を犯した者が予測可能で有意義な結果に直面することを保証すること。

3. 国際機関を含む国家と非国家主体は職員の訓練、能力の開発、サイバースペースの安定性の重要性に関する共通理解の促進に向けた取り組みを増やし、異なる関係者の多様なニーズを考慮すること。

4. 国家と非国家主体は規範の違反とそのような活動による影響に関する情報を収集、共有、評価、公表すること。

5. 国家と非国家主体は利益共同体を確立し支援することでサイバースペースの安定性を確保すること。

6. 安定性に関わる問題に対処するため、国家、民間部門（技術コミュニティを含む）、市民社会が適切に関与し協議に参加するような自立したマルチステークホルダー・エンゲージメントのメカニズムを確立させること。

本報告書の出版は終着点であるとともに出発点でもある。委員会はその義務を果たした。しかし、GCSCのメンバーと支援者や、GCSCの目標を支持している者にとって、これらの原則、規範、勧告を実施するために必要な多大な取り組みは始まったばかりである。サイバースペースの安定性を確保できなければその便益が失われてしまうため、取り組みを始めなければならない。

1. はじめに

デジタルの進化とサイバースペースは人々の暮らしを劇的に変えた[1]。世界中のデータをデジタル化しそれを保存、分析、送信できるようになったことで、社会のあらゆる分野に多大な影響がもたらされ、私事、ビジネス、政治の在り方が変わったのである。今日では世界の人口の約半数がインターネットを利用し[2]、この利用者数は急増している。しかし、個人的にサイバースペースに接続していない者であっても、その影響を受けている。それはそのような個人に物品やサービスを提供する企業がサイバースペースをコミュニケーションや流通、財務のために活用していることが多いからである。

サイバースペースの利点とその安定性を確保する必要性については、その課題とともに頻繁に議論されてきた。特にサイバースペースが高貴な目的と下劣な目的の両方を支え得ることが挙げられる。例えば、グローバルな接続性、匿名性、およびトレーサビリティの欠如により、個人や機械に身元を明かすことを強いることなくデータやシステムに接続することを許可する反面、犯罪者もこれらの特徴を利用し、罰を受けることなく罪を犯すことができるのである。その結果、政府、企業、そして世界中の人々は難題に直面している。政府はサイバースペースを保護し、公共サービスを提供し、その他の重要な活動（教育、オンラインバンキングなど）を促進させることに関心を示しているものの、同時に法の執行、インテリジェンス、軍事能力を含む国家安全保障上の利益を推進させたいとも考えている。顧客や評判、利益を守りたい企業も攻撃を受け、悪意のある活動を調査したり、政府からデータの提供を要求されたりしている。また、人々は、自ら接続しているかどうかにかかわらずデジタルテクノロジーへの依存度を高め受け入れるようになっているが、その継続的な利用可能性と完全性について心配している。過去十年間にわたり、政府のシステムや重要インフラに対するものも含め、サイバー攻撃の数が増し、その手口も更に巧妙化している[3]。このように、現状であれ観測されている傾向であれ、いずれも決して明るいものではない。

国家と非国家主体の両方が実施しているサイバー攻撃は、世界にサイバースタビリティ枠組みが必要であることを明確に示している。そのような枠組みはサイバースペースのメリットを損なわせ、権利や自由を含む人々の幸福を削減するようなサイバースペースにおける重大な破壊をもたらす可能性を削減する上で役に立つ。設計が不十分であったり過失が

1 「サイバースペース」は様々な形で定義されている。https://en.wikipedia.org/wiki/Cyberspace辞書による定義は「世界中のコンピュータユーザーがお互いとコミュニケーションを図ったり、あらゆる目的で情報にアクセスすることを可能にしたりする電子システム」である。https://dictionary.cambridge.org/us/dic-tionary/english/cyberspace英国によると、「サイバースペースとは情報を保管、修正、発信するために使用するデジタルネットワークの電子媒体を記述するための用語である。インターネットだけでなく、ビジネスやインフラ、サービスを支援しているその他の情報系も含む。」https://www.cpni.gov.uk/cyber。そのため、一般的な用語では「世界中のデバイスをリンクするためにインターネット・プロトコル・スイート（TCP/IP）を用いる相互接続したコンピュータネットワークのグローバルシステム」として記述されているインターネットよりも広い範囲を指していると考えられる。https://en.wikipedia.org/wiki/Internetを参照すること。また、次も参照すること：国際電気通信連合「インターネットを定義する（Defining the Internet）」ディスカッション・ペーパー（2013年5月）、https://www.itu.int/dms_pub/itu-s/md/13/wtpf13/inf/S13-WTPF13-INF-0008%21%21MSW-E.docx。

2 「インターネット利用統計」インターネット世界統計局、最終更新日2019年10月4日、https://internetworldstats.com/stats.htm。

3 戦略国際問題研究所（CSIS）*「2006年以降発生の重大サイバー・インシデント（Significant Cyber Incidents Since 2006）」*https://csis-prod.s3.amazonaws.com/s3fs-public/190904_Significant_Cyber_Events_List.pdf。Louis Marinos及びMarco Lourenço編集*「ENISA Threat Landscape Report 2018」*ENISA（2019年一月号）https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018。Abhishek Agrawal等著*「マイクロソフト・セキュリティ・インテリジェンス・レポート（Microsoft Security Intelligence Report）」*第24巻（2018年12月号）https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original。国連総会*「国際安全保障の文脈における情報通信分野での発展：国連事務総長報告（Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General）」*A/74/120（2019年6月24日）https://undocs.org/A/74/120。

あった製品やサービス、または不十分であったり過失のある運用上方法がそれらを損なわせるように、ITのプロフェッショナルやコンピュータのユーザーがよく管理し設計も開発もしっかりしている製品やサービスはセキュリティや安定性を高めることは明らかである。しかし、特に国家や非国家主体がサイバースペースを政治的、軍事的、経済的な優位性を得るための洗浄としてサイバースペースを見なしている状況では、開発や運用の改善のみでは十分ではない。執拗な攻撃者はセキュリティ対策を破ることができ、「インターネットでは守備よりも攻撃が優る」という格言をもたらすとともに不安定性を生み出している[4]。そのため、技術だけでなく行動にも焦点を当てることが重要である。サイバースペースの安定性を高める（そして脅かさない）ような責任ある形で全ての行為主体が行動するように促すにはどうすればよいのか？

この疑問に答えるため、複数の政府および非政府団体がサイバースペースの安定性に関するグローバル委員会（Global Commission on the Stability of Cyberspace; GCSC）[5] の創立を支持している。

> 我々は、25年間にわたって大国間の戦略的な安定性と相対的な平和が維持されてきた期間の終わりを迎えた。国家間の紛争は新たな形で勃発し、サイバー活動がこの変わりやすく新しい環境において主導的な役割を果たす可能性が高く、それによって経済成長と個人の自由の拡大を促進するためのサイバースペースの平和的な利用を覆すリスクが増大することになる。
>
> これらの動きに対抗するために、サイバースペースの安定性に関するグローバル委員会は国際的なセキュリティと安定性を強化し、サイバースペースにおける国家や非国家による責任ある行動を導くための規範と政策の提案を立案する。GCSCは共通の理解を深めるためにあらゆる利害関係者を巻き込み、その取り組みは情報交換、キャパシティ・ビルディング、基礎研究、提唱を支援することでサイバースタビリティを向上させる[6]。

特筆すべき点として、委員会自体が多様な経歴と専門性を有する個人によって構成されていることから、複数の利害関係者を抱えたグローバルな委員会となっている。委員の中には自ら政府に務め、サイバー問題の二国間・多国間交渉に携わった者もいれば、インターネットそのものの構築、維持、保護における経験を経てきた者もいる。その他の委員は市民社会を代表している。

委員会の取り組みは真空の中にあるのではなく、他の数多くの機関やプロセス（過去・現在の療法）がサイバースペースの安定性について関心を持っていることを認識しているGCSCは、その業務が他の者による取り組みと重複しないように努めた。それよりも、GCSCは他のマルチステークホルダーや政府によるプロセスを基に、今後の取り組みに影響を与えるよう試みてきた。これらのプロセスには国連政府専門家会合（UN GGE）[7] による基礎的で現在も継続している取り組み、国連公開作業部会（UN OEWG）による作業をはじめ、サイバー専門的知識に関する

4　例えば次を参照すること：P.W.Singer 及び Allan Friedman「サイバー攻撃のカルト（The Cult of the Cyber Offensive）」『*Foreign Policy*』（2014年1月15日 号 ）、https://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/。世界経済フォーラム（WEF）「*ザ・グローバルリスク・レポート（The Global Risks Report）2019*」（2019年）http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

5　GCSCに関するさらなる情報については補足資料C：GCSCの歴史・目標・プロセスを参照すること。

6　サイバースペースの安定性に関するグローバル委員会、https://cyberstability.org/。

7　重要な決議として、2015年度国連総会ではUN GGEの結論を全会一致で確認した。国連総会決議70/237、*2015年12月23日に国連総会が採択した決議［第一委員会の報告書（A/70/455）］*、https://undocs.org/en/A/RES/70/237を参照すること。このように、国際法、特に国際連合憲章は、サイバー作戦にも適用される敵対行為への国際的な対応のための排他的な枠組みを確立している。我々の取り組みは2015年の国連総会での全ての国による、ICTの利用における安定性とセキュリティを高めるための責任ある行動の規範によって導かれ、デューデリジェンスや協力のための国際法の下で約束を果たすという合意の上に成り立っている。

グローバルフォーラム（GFCE）[8]、世界情報社会サミット（WSIS）、インターネット・ガバナンスに関する世界委員会（Bildt委員会）、インターネット・ガバナンス・フォーラム（IGF）、サイバー空間に関する国際会議（GCCS／ロンドンプロセス）、NETmundialイニシアチブ、欧州安全保障協力機構（OSCE）、アフリカ連合委員会（AUC）、信頼性憲章、サイバーセキュリティ・テック協定、ハーグ・サイバー規範プログラム、国連軍縮研究所（UNIDIR）、サイ始めペースにおける信頼とセキュリティに関するパリ・コール（「パリ・コール」）、国連デジタル協力に関する国連事務総長のハイレベル パネルらによる努力が含まれる。また、委員会の業務では委託研究やパブリックコメントの募集によっても知見を得てきた。

これらの取り組みの中には、部分的にサイバースペースの安定性に焦点を当て、サイバースペースの安定性とガバナンスが表裏一体であることを懸念しているものもあった。つまり、強固なガバナンスモデルがなければ、社会は安定性を確保するために必要な相互作用や意思決定プロセスを欠いてしまうのである。例えば、Bildt委員会は、「インターネットに対する信用を回復し、信頼を高めることを目的とした、市民と選挙で選ばれた代表者、司法、法執行・情報機関、企業、市民社会、インターネット技術コミュニティの間における」デジタル・プライバシーとセキュリティのためにマルチステークホルダーによる社会的コンパクトを提案している[9]

我々は、激動の新ドメインであるサイバースペースにおける行動に適用するための原則、規則、規範を開発しようとするこれまでの努力を称賛するとともに、サイバースペースの安定性を高めるために包括的な枠組みが必要であると考えている。歴史的な記録によると、社会や政府は、重要な破壊的な新技術のための広範で正式な国際的なガバナンス構造を構築するのに数十年かかることもある[10]。経済・社会・安全保障上の世界的な相互依存における重要な側面としてのサイバースペースの出現は、ワールド・ワイド・ウェブが広く利用され始めた1990年代後半からのことである。そのため、進化するガバナンスのプロセスは、規範的な一貫性と非一貫性が共存している領域であり、早期段階にある[11]。例えば、ドメインネームシステムに関連する規範や制度は十分に整備されているが、コンテンツの規制に関連して国家間や企業間で大きな意見の不一致が見られる。国家や非国家主体が知的財産権や貿易などの他の制度による規範を適用することもあり、また民間企業が自ら規範を設定することも増えてきている[12]。我々の委員会の目的は、ガバナンスに関するこれらの様々な疑問を整理することではなく、サイバースペースの安定性を確保するための一般的な枠組み内に収めることである。

また、サイバースペースの安定性に関心を持つ人々は、サイバースペースを弱体化させようとする人々を追いかけ、技術開発や地政学的紛争の進化に追いつくのに苦労してきた点にも注意が必要である。この課題の一部は、サイバースペースが行為主体による政治的・軍事的目標の追求方法を一変させたことであり、参入障壁が低いため、従来の軍事勢力になるよりおサイバー勢力になることの方が難しくない。さらに、新たな技術をツールキットに加えたことにより、特に制約が広く遵守されていない場合には制約を採用することに消極的である者もいる。必要とされているのは、サイバースペースの安定性を促進させながらも、技術変化のペースが速まり続けている中で役に立ち続けるような国際コミュニティのための包括的なサイバースタビリティの枠組みである。そのため、我々は「サイバースペースの安定性を守る」というコアとなる目的の定義から着手する。

8　GFCEはキャパシティ・ビルディングに関して特に積極的に取り組んできている。例えば次を参照すること：「サイバー・キャパシティー・ビルディングに関するGFCEグローバルアジェンダについてのデリー・コミュニケ（Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building）」サイバー専門的知識に関するグローバルフォーラム（GFCE）（2017年11月24日）、https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique。

9　インターネット・ガバナンスに関する世界委員会「*One Internet*」（2016）、IX頁、https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf。「我々は政府、民間企業、市民社会、技術コミュニティ、個人が一緒になり、デジタルの時代のための新たな社会的コンパクトを創出するよう呼びかける。」

10　この種のガバナンス構造の最適な例は、多大な時間と労力をかけて確立された核兵器に関するガバナンス構造であろう。核兵器不拡散条約（NPT）から60年が経過した現在でも、核兵器のガバナンスは安全保障上の懸念事項であり続けている。

11　この初期段階は「レジーム複合体（regime complex）」と呼ばれてきた。次の文献を参照すること：Joseph Nye「複雑なグローバルサイバー活動を管理するためのレジーム・コンプレックス（The Regime Complex for Managing Complex Global Cyber Activities）」インターネット・ガバナンスに関する世界委員会、第一号（2014年5月）、https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf。

12　例えばISOCとマイクロソフトが策定した規範を参照すること：「ルーティングセキュリティに関する行動規範（Mutually Agreed Norms for Routing Security (MANRS)）、インターネットソサエティ（2014年）、https://www.manrs.org/。Angela McKay等著「*インターネットに依存する世界における紛争を低減する国際サーバーセキュリティー規範（International Cybersecurity Norms Reducing Conflict in an Internet-dependent World）*」マイクロソフト（2014年12月）、https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA。そしてScott Charney等「*明文化から実施まで：サイバーセキュリティ規範を進展させるには（From Articulation to Implementation：Enabling Progress on Cybersecurity Norms）*」マイクロソフト（2016年6月）、https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8。

2. サイバースペースの安定性とは何を意味するのか？

定義：

サイバースペースの安定性とは、誰もが安全かつ確実にサイバースペースを利用できることに合理的な自信を持てること、サイバースペース内およびサイバースペースを介して提供されるサービスや情報の可用性と完全性が一般的に保証されていること、変化が比較的平和的に管理されていること、および緊張状態がエスカレートしない方法で解決されることを意味している。

委員会の定義は「安定性」[13] の標準的な定義の上に成り立っているものの、二通りのニュアンスも抱えている。第一に、ユーザーの信頼性について言及している。人間の意思決定は事実だけでなく認識に基づいて行われる場合もあり、安定性の欠如を認識すると、サイバースペースを利用してその恩恵を享受することに消極的になる可能性があるため、信頼性が重要となる。例えば、サイバースペースの利用はプロセスを簡素化して効率を高める可能性があるため、サイバースペースを活用することで特定の機能（政府サービスへのアクセス、オンライン・バンキングなど）が便益を得られる可能性があることを示唆している。しかし、そのようなシステムが信頼性に欠けるものであるか、そのようなシステムが信頼性に欠けるものであると認識されている場合には、その利用は制限され、技術がもたらしている利益は失われてしまう。

第二に、サイバースペースは常に変化するドメインであることを忘れてはならない。技術、ビジネスモデル、機能性、日常生活において技術が果たす役割に対する社会の期待にも変化が伴う。そのため、「元の状態に戻る」ことを含めている辞書が定義する「安定性」とは異なり、ここで必要としているのは技術が進化する中でサイバースペースの安定性を確保するアジャイルな仕組みなのである。簡単に言えば、サイバースペースとそれを囲む世界が変わりながらも、誰もがサイバースペースの可用性と完全性を信用し続けなければならないのである。

13 「安定性」は「安定している状態」として定義されている。https://www.lexico.com/en/definition/stability。「安定」とは1. 屈したり覆されたりする可能性が低いこと、しっかり固定されていること、2. 変化や故障がおきる可能性が低いこと、しっかりと確立されていること、3. 物理的な変化を受ける可能性がないことを意味している。https://en.oxforddictionaries.com/definition/stableを参照。国際関係では、国際安定という用語の最も一貫した定義の一つは「国際システムがその本質的な特性をすべて保持している確率、単一の国家が支配的にならない確率、システムを構成する国家の大部分が存続し続ける確率、大規模な戦争が起こらない確率」である。Karl W. Deutsch 及びJ. David Singer「多極パワーシステムと国際的安定性（Multipolar Power Systems and International Stability）」『*World Politics*』、第16巻、第3号（1964年4月）：90-406頁、http://users.metu.edu.tr/utuba/Deutsch.pdf。

3. GCSCサイバースタビリティの枠組み

上述の課題に対処するため、他の組織と同様に[14]、GCSCも包括的なサイバースタビリティの枠組みを提案している。上述の課題に対処するため、他の組織と同様に、GCSCも包括的なサイバースタビリティの枠組みを提案している。この枠組みには1. マルチステークホルダー・エンゲージメント、2. サイバースタビリティの原則、3. 自主的な規範の策定と実施、4. 国際法の遵守、5. 信頼性構築に向けた施策、6. キャパシティ・ビルディング、7. サイバースペースがレジリエンスを有していることを担保する技術基準の公布と広範な使用、の7点が含まれている。GCSCによる取り組みは主にマルチステークホルダーによるアプローチ、原則、規範の三つに重点を置き、それぞれについて第4節、5節、6節で述べている。規範に関しては、その策定のみならず、採択、実施、違反者の説明責任といったより難しい問題についても焦点を当てている。

このサイバースタビリティ・フレームワークの個別の要素に対処している取り組みは数多く存在し、サイバースペース自体のように分散化されている点は留意すべきである。進歩を遂げるためには、GCSCではマルチステークホルダーによる協調的かつグローバルな努力が必要であると考えている。したがって、実質的な問題に対処することに加えて、GCSCでは既存の取り組みを活用・補完し、可能であればそれらに新たな活力を与えることを試みるようなプロセスの勧告を行う。

14　例えば次を参照：「*デジタル相互依存の時代（The Age of Digital Interdependence）」国連事務総長のデジタル協力に関する高レベルパネルの報告書*（2019年6月）、39頁、https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf。「我々は共有ビジョンを形成し、デジタルの安定性の属性を特定し、責任ある技術利用のための規範の実施を解明・強化し、行動の優先順位を提案するために、デジタル信頼性・セキュリティへのグローバル・コミットメントを策定することを提言する。」

サイバースタビリティ・フレームワークの画像にはwww.flaticon.comのFreepik、monkik、smalllikeart、Eucalyp、Itim2101が作成した画像を用いている。

4. マルチステークホルダー・エンゲージメント

マルチステークホルダーによるアプローチの重要性について言及している国家間の国際な合意が無数にあるにもかかわらず、これは論争の的であり続けている。一部の者にとってこの議論は哲学的なものであり、技術政策と国際問題における国家と非国家主体の比較的な役割に焦点を当てている。他の者にとっては、マルチステークホルダーによるプロセスは実践的であり、単独で行動していたり最小限の非国家によるインプットのみを参考にしたりしている国家はサイバースペースの安定性を確保することはできないと考えている[15]。我々はこの後半の視点に同意する。

マルチステークホルダー・エンゲージメントの是非に関する議論は何十年も続いてきた。多くの場合、この課題はインターネット資源の管理という文脈において浮かび上がってきたが、規範と国家の安全保障という問題も提起されている。例えば、情報社会に関する国連世界サミットの第2フェーズでは、国連インターネット・ガバナンス作業部会（WGIG）が単一の利害関係者によるリーダーシップの概念を否定している。むしろ、インターネットは単一の利害関係者グループや単一の組織だけで管理するには大きすぎると結論づけ、マルチステークホルダー・アプローチを提案している。このようにして、2005年のWSISチュニス・アジェンダにおいて首脳が「インターネット・ガバナンスの作業的定義は、政府、民間部門、市民社会がそれぞれの役割において、インターネットの進化と利用を形作る共通の原則、規範、規則、意思決定手順、プログラムを開発し、適用することである」と宣言している[16]。

この見解は10年後に開催されたWSISによる成果の実施の全体的なレビューに関する国連総会の高レベル会合で再確認され、国連決議70/125（2015）にも以下のように記載されている。

> さらに、我々は情報社会に関する世界サミットがその発足以来のプロセスを特徴づけてきたマルチステークホルダーの協力と関与の価値と原則を再確認し、政府、民間部門、市民社会、国際機関、技術・学術界、その他すべての関連する利害関係者が、それぞれの役割と責任の範囲内で、特に発展途上国からのバランスのとれた代表者とともに、効果的な参加、パートナーシップ、協力を行ってきたことが情報社会の発展に必要不可欠であり、今後も欠かせないものであることを認識している[17]。

15　WSISの定義（2005）では、『それぞれの役割』という概念と『共有』という思想を紹介している。NETmundial宣言（2014）では重要な要素をボトムアップ、開放性、透明性、包摂性、人権ベースと定義している。言い換えると、マルチステークホルダーによるアプローチに関する一般的なガイドラインはいくつかあるものの、単一のマルチステークホルダー・モデルが欠けている。これまで、協議型と協調型という二つのマルチステークホルダー・モデルが現れている。」Wolfgang Kleinwächter「インターネット関連の公共政策作成における総合的アプローチに向けて（Towards a Holistic Approach for Internet Related Public Policy Making）」サイバースペースの安定性に関するグローバル委員会（2018年1月）、https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf。マルチステークホルダー・モデルに関する追加の議論については、Virgilio Almeida等「マルチステークホルダー・モデルの起源と進化（The Origin and Evolution of Multistakeholder Models）」『*IEEE Internet Computing*』　第19巻（2015年1-2月号）：74-79頁、https://doi.ieee-computersociety.org/10.1109/MIC.2015.15を参照。

16　「情報社会についてのチュニスアジェンダ（Tunis Agenda for the Information Society）」世界情報社会サミット（WSIS）（2005年11月18日）、第34項、https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html。

17　国連総会決議70/125、*世界情報社会サミットの成果実施状況をレビューした国連総会のハイレベル会合の成果文書*、A/RES/70/125（2015年12月11日）第3項、https://undocs.org/en/A/RES/70/125を参照。

ここでも、声明は重要なインターネット資源の管理の範疇を超えて国家安全保障の核にある問題に直接迫っている。

> 我々は、国家安全保障に関わるサイバーセキュリティの問題において政府が主導的に果たす役割を認識している。さらに、全ての利害関係者がそれぞれの役割と責任において果たす重要な役割と貢献も認識している[18]。

特に規範に関しては、主要国首脳会議（G8）が2011に以下の通り宣言している。

> インターネット上のネットワークとサービスのセキュリティはマルチステークホルダーの問題である。政府、地域・国際組織、民間部門、市民社会の間で連携する必要があり……サイバースペースの利用に関する行動規範や共通のアプローチの策定を支援する上で、政府はあらゆる利害関係者からの情報を参考にして果たすべき役割を持っている[19]。

その2年後の2013年には、UN GGEが*「国際安全保障の文脈における情報通信分野での発展（Developments in the field of information and telecommunications in the context of international security）」に関する報告書*を発表している。UN GGEは「平和で、安全で、回復力があり、開かれたICT環境のための協力の構築」と題する節において「これらの課題に対処するためには各国がリードしなければならないものの、効果的な協力は、民間部門と市民社会の適切な参加することで恩恵を受けるだろう」[20] と指摘している。更に報告書では「各国家における責任のある行動規範、ルール、及び原則に関する勧告」と題する節において以下のように指摘している。

> 加盟国は、民間部門や市民社会組織が果たす役割を含め、上述の規範や責任ある行動の原則を実施する上でどのように協力するのが最善か、検討すべきである[21]。

これらの立ち位置はUN GGEが2015年に発表した報告書において再確認されており、以下のように宣言されている。

> 国家は安全で平和なICT環境を維持するための主な責任を負っているが、効果的な国際協力は民間部門、学界、市民社会組織による適切な参加のためのメカニズムを特定することで便益を享受できるだろう[22]。

この声明は、2018年の国連総会決議「*国際安全保障の文脈におけるサイバースペースにおける責任ある国家の行動の推進*」[23] でも繰り返されている。他の国際協定も同様の感情を明確に表現しており、例えばパリ・コールでは「我々は強化されたマルチステークホルダーによるアプローチと、サイバースペースの安定性に対するリスクを軽減し、信頼、能力、信頼を構築するためにさらなる努力をする必要性を認識している」[24] と述べている。

18　同上、第50項。
19　G8主要国首脳会議、「G8首脳宣言：自由及び民主主義のための新たなコミットメント（G8 Declaration: Renewed Commitment for Freedom and Democracy）」ドーヴィルG8サミット（2011年5月27日）、第17項、http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html。
20　国連総会、「*国際安全保障の文脈における情報通信分野での発展に関する国連における政府専門家会合の報告書（Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security）*」A/68/98（2013年6月24日）、7頁、第12項、https://undocs.org/A/68/98、（以下国連GGE 2013年報告書UN GGE 2013 Report）。
21　同上、8頁、第25項。
22　国連総会、「*国際安全保障の文脈における情報通信分野での発展に関する国連における政府専門家会合の報告書（Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security）*」A/70/174（2015年7月22日）、13頁、第31項、https://undocs.org/A/70/174、（以下、国連GGE 2015年報告書）。
23　国連総会決議73/266、「*国際安全保障面でのサイバー・スペースに対する責任ある国家の姿勢の促進（Advancing responsible State behaviour in cyberspace in the context of international security）*」A/RES/73/266（2018年12月22日）、https://undocs.org/en/A/RES/73/266。
24　フランス共和国ヨーロッパ・外務省「サイバーセキュリティにおける信頼とセキュリティのためのパリ・コール」（2018年11月11日）、https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf。NETmundial、「NETmundial マルチステークホルダー・ステートメント（NETmundial Multistakeholder Statement）」（2014年4月24日）、http://netmundial.br/wp-content/up-loads/2014/04/NETmundial-Multistakeholder-Document.pdfも参照。

直近では、2019年6月に国連事務総長のデジタル協力に関する高レベルパネルがその報告書「*デジタル相互依存の時代*」の中で次のように述べている。

> 効果的なデジタル協力を行うためには、現在の緊張した関係にかかわらず、多国間主義を強化することが必要である。また、多国間主義を補完するために、政府のみならず市民社会、学者、技術者、民間部門など、より多様なステークホルダーを巻き込んだマルチステークホルダー主義の協力が求められる[25]。

マルチステークホルダーによるアプローチの考え方は成功していることが証明されているが、万人に支持されているわけではない。一部の政府は国際的な安全保障と安定性の確保がほぼ独占的に国家の責任であると考え続けている。このような従来型の安全保障の見方は、国家には武力による攻撃から市民を守る責任があるという考え方に由来するものであり、国連憲章第24条において成文化されている国連安全保障理事会の責任にも反映されている[26]。このような考え方は、物理的なドメインでは政府が武力の正当化された行使を独占してきただけでなく、そのドメインの攻防に用いられる軍事レベルの武器（航空機、戦車など）も管理してきたという過去の経験によっても補強されている可能性がある。

実際には、サイバー戦場（すなわちサイバースペース）は、主に民間部門によって設計、展開、運営が行われている。政府は独自の責任を負っているが、このドメインの独占的な保護者ではない。仮に政府がサイバースペースにおける*合法的な*武力行使を事実上独占していたとしても、このドメインを攻撃し守るための現実的な独占権はもはやなく、強力なサイバー兵器の拡散や使用を防ぐこともできない。むしろ、技術コミュニティ、市民社会、個人もまた、基準の公布を含め、サイバースペースの保護において大きな役割を果たしている。したがって、成果を向上させ、サイバースペースの安定性を支える規範や政策が十分に形成され、望ましくない結果を回避するためには、マルチステークホルダーのアプローチが必要である。

同様に重要な点として、これは国家が単独でやりたくてもできないことである。サイバースペースの安定性に影響を与える問題への非国家主体の参加は避けられない。例えば、民間部門や技術コミュニティの多くのメンバーが、重要なプロトコルやサービスに責任を持っている可能性があり、また彼らの商用製品やオープンソース製品を使用している国家を保護していることも考えられる。さらに、政府の伝統的な役割であり政治的特権であった攻撃の調査と帰属さえも、もはや政府のみが持つ知識と責任の領域ではなくなっており、いくつかの国家に対する著名な攻撃が非政府機関によって特定され公表されている。簡潔に述べると、攻撃の間や攻撃後において国家が果たすべき役割（法執行活動や外交行動などを含む）は独特であるものの、調査や帰属に関する独占権はなく、また非国家主体を効果的に排除することもできないのである。その結果、サイバースペースの規範と政策を成功させ、それらを確実に遵守するためには、すべての利害関係者の参加が必要であり、その責任はすべての利害関係者にあるとともに、政府は民間部門、技術コミュニティ、学界、市民社会におけるその他の代表による酸化を効果的に取り込むようなメカニズムの創出に集中しなければならない。これはまさに多くの政府が呼びかけてきたことである。

25 「*デジタル相互依存の時代（The Age of Digital Interdependence）*」7頁、https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf。
26 国際連合憲章、「第5章安全保障理事会」国連機関実務一覧、http://legal.un.org/repertory/art24.shtml。

5. 原則

規範的な行動は価値観から派生する。そのため、個人の責任、国家の責任、または基本的人権のいずれに関係しているにせよ、これらの価値観を宣言することが我々の出発点でなくてはならない。事実、異なる価値観はコンセンサスを得る過程を難しくし、国や地域による国際的な合意内容の解釈や実施が異なるという結果をもたらす可能性がある。これは進歩を遂げる上で原則に関する合意が必要であることを示唆している訳ではない。場合によっては、関係者間で動機が異なっても受け入れられる行動について合意に至ることがある。しかし、共有された原則と相互依存性はさらに深いコミットメントにつながり、今後意見の不一致や衝突が発生するリスクを下げることができる。そのため、各関係者はそれぞれの思考を導き、規範の源泉となる高レベルの原則に関する忌憚のない議論を行うことが重要となる。

サイバースペースの安定性を確保する上で以下の四つの原則が重要である。

1. **責任：**誰もがサイバースペースの安定性を確保するための責任を負っている。
2. **自制：**国家も非国家主体もサイバースペースの安定性を損なうような行動を取るべきではない。
3. **行動義務：**国家または非国家主体はサイバースペースの安定性を確保するために合理的で適切な措置を講じるべきである。
4. **人権の尊重：**サイバースペースの安定性を確保するために努力するにあたり、人権と法律を尊重しなければならない。

A. 責任の原則

一つ目の原則はサイバースペースの分散化されている性質に言及している。この原則はサイバースペースの安定性を確保するにあたりマルチステークホルダーのアプローチの必要性を再確認し、特に「ステークホルダー」をすべての個人にまで拡大している。サイバースペースの安定性を確保するために、全ての個人が個人的またはプロフェッショナルとして責任を負っている。政府のサイバー政策の責任者やクラウドサービスを管理する従業員にも役割があることは明らかだが、サイバースペースに接続しているすべての個人も自分のデバイスが危険に晒されないように、そして攻撃に利用されないように、合理的な努力をしなければならない。インターネットに接続していない者でも物品やサービスを受け取るためにインターネットの機能に依存している可能性があり、彼らもまた自分たちのコミュニティにおいてサイバースペースに関する政策が適切に施行されていることを保証することについて利害関係を有している。

B. 自制の原則

二つ目の原則では自制に関する一般的な要件が含まれている。国家にとっては、これはサイバースペース[27]における責任ある国家の行動に関する2018年の国連総会（UNGA）決議や、「国際的な平和と安全の維持を含む国連の目的と一貫して、国家は……有害であると認められる、または国際的な平和と安全に脅威をもたらす可能性のあるICTの実践を防止すべきである」という2015年の国連GGE報告書と一致している[28]。しかし、非国家主体も攻撃者をハッキングするなどといったサイバースペースの安定性を損なう可能性のある行為に従事することができるため、国家のみの問題ではない。

27　国連総会決議73/27「*国際安全保障面における情報・遠距離通信分野の開発（Developments in the field of information and telecommunications in the context of international security）*」、A/RES/73/27（2018年15月5日）、https://undocs.org/en/A/RES/73/27及び国連総会決議73/266、https://undocs.org/en/A/RES/73/266。

28　国連GGE 2015年報告書、7頁、第13項(a)、https://undocs.org/A/70/174。

C. 行動義務の原則

三つ目の原則には、サイバースペースの安定性を温存させるために肯定的な行動を取るという一般的な要件が含まれている。行動を取る際、国家は緊張を不意に深めたり不安定性を高めたりしないよう注意すべきである。これは2015年の国連GGE報告書で指摘されている「ICTの利用における安定性とセキュリティを向上させるための措置の開発と適用において協力する」[29] という義務と一致している。しかしながら、これも国家のみに該当することではなく、民間企業や個人もサイバースペースの安定性を確保する上で協力的なステップを取ることができる。例えば、民間企業はサイバー脅威を軽減するためにお互いに協力し、個人はアップグレード、パッチング、多要素認証の利用などのベストプラクティスを採用することで、ボットネットが自分のマシンを乗っ取り、サイバースペースの安定性を脅かす広範な攻撃に利用されるリスクを削減できる。

D. 人権の原則

四つ目の原則では、サイバースペースの安定性における重要な要素として、人権保護の重要性を認識している。個人による情報通信技術への依存度が高まるにつれて、情報通信技術の可用性や完全性に対する脅威によってもたらされる人間の活動への破壊的影響も増幅されている。したがって、国家がサイバースペースにおける国家戦略的利益を追求する際には、その結果として生じる個人への影響、特に人権への影響も十分に考慮することが必要不可欠である。同様に、非国家主体は、その活動が個人によるオンラインおよびオフラインでの権利享受に及ぼすリスクを考慮し、最小化しなければならない。最低でも、人権の原則を遵守するために、国家はサイバースペースにおける活動に従事する際に国際法に基づく人権義務に沿って行動することが求められる。

普遍的に受け入れられている人権は世界人権宣言に明記されている[30]。さらに、様々な特定の人権を規定する多数の国際協定が採択され、締約国を拘束する法的義務が生じている。サイバースペースの文脈では、国際人権法の適用可能性は国連総会[31]、国連人権理事会（HRC）[32]、2013年および2015年の国連GGE報告書[33] になど、数回にわたって明示的に確認されている。権利を擁護し、ユーザーの権利が尊重されていることへの信頼を確保することは、サイバースペースの安定性を確保する上で極めて重要である。

これら四つの原則は全てを網羅することやサイバースペース政策のあらゆる側面を網羅することを意図しておらず、様々な問題を網羅した広範かつ基本的な原則を作成している組織は数多く存在する。また、インターネット・ガバナンスやオンライン上の人権（プライバシー、表現の自由、結社の自由を含む）に関連する問題に注目している組織もある。我々は、特に規則が不明確であったり、たとえ明確であったりしても受け入れられず施行されない可能性があるような前例がなく高度な敵対的活動の時代において、サイバースペースの安定性を支える原則が広く受け入れられるようになることを目指している。

29 Id.

30 国連総会決議217 A (III)、*世界人権宣言*（1948年12月10日採択）、https://www.un.org/en/universal-declaration-human-rights/。

31 国連総会決議68/167「*デジタル時代におけるプライバシーの権利（The right to privacy in the digital age）*A/RES/68/167（2013年12月18日）、https://undocs.org/A/RES/68/167及び国連総会決議69/166,「*デジタル時代におけるプライバシーの権利（The right to privacy in the digital age）*A/RES/69/166（2014年12月18日）https://undocs.org/A/RES/69/166を参照。

32 国際連合人権理事会「*インターネット上の人権の促進、保護及び享受（The promotion, protection and enjoyment of human rights on the Internet）*」A/HRC/20/L.13（2012年6月29日)、https://undocs.org/A/HRC/20/L.13。

33 国連GGE 2013年報告書https://undocs.org/A/68/98 及び国連GGE 2015年報告書 https://undocs.org/A/70/174。

6. 規範

原則は政策を確立させ戦術的行動を導くための重要な出発点であるが、その抽象度の高さから、より詳細な合意によって許容される行動を定義することで補う必要がある。これは、原則が規範によって補完されなければいけないことを意味している。規範は期待される適切な社会的行動を表している[34]。他の組織、特に国連GGEによる2015年の報告書[35]に言及せずに規範を議論することは不可能である。国連GGEは「ICT固有の特性を考慮し、時間をかけて追加の規範を策定することができる」[36]と認識しており、実際にGCSCの任務も「国際安全保障と安定性を高めるための規範と政策に関する提案の策定する」ことであった。これまでの成果を踏まえて追加の規範が必要とされる可能性のある領域を特定するためには、2015年に合意された規範から始めることが重要であり、これについては補足資料Aでその全容を紹介している。

2015年に国連GGEが指摘したように、国連GGEは特に「ICTの複雑性と固有の特性を考慮した追加の規範を策定する必要がある可能性がある領域を特定する」[37]ことを任務としていた。それ以来、ICT製品やサービス、そしてその乱用は変化し続けてきた。これに対処するために、GCSCは現在の一連の規範におけるギャップを埋めること、規範の議論に技術的な特異性を加えること、実施に関する問題に対応することに注目した。例えばギャップを埋めるという点では、GCSCはインターネットのパブリック・コアを保護するための規範[38]と選挙システムを保護するための規範を承認した[39]。同様に、国連GGEの規範が「サプライチェーンの完全性」[40]に言及しているのに対し、GCSCの規範ではサプライチェーンに対する攻撃のうち対処すべき種類についてより具体的に述べている[41]。

34　https://en.oxforddictionaries.com/definition/norm
35　国連GGE 2015年報告書、https://undocs.org/A/70/174
36　同上、8頁、第15項。
37　同上、7頁、第11項。

38　サイバースペースの安定性に関するグローバル委員会（GCSC）「インターネットのパブリック・コアを守るための呼びかけ（Call to Protect the Public Core of the Internet）」（ニューデリー、2017年11月）、https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf。特別な保護のためにインターネットのパブリック・コアを特定することを最も早く提唱したのはオランダの研究者Dennis Broedersであった。Dennis Broeders「*インターネットのパブリックコア：インターネット・ガバナンスの国際アジェンダ（The Public Core of the Internet: An International Agenda for Internet Governance）*」（アムステルダム：アムステルダム大学出版、2015）、http://www.oapen.org/download?type=document&docid=610631を参照。
39　サイバースペースの安定性に関するグローバル委員会（GCSC）、「*選挙インフラを守るための呼びかけ（Call to Protect the Electoral Infrastructure）*」（ブラチスラバ、2018年5月）、https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf
40　国連GGE 2015年報告書、8頁、第13項(i)。「国家はエンドユーザーがICT製品のセキュリティについて安心できるようにするために、サプライチェーンの完全性を確保するための合理的な措置を取るべきである。国家は悪意あるICTツールや技術の拡散や、有害な隠れた機能の使用の防止に努めるべきである。」
41　サイバースペースの安定性に関するグローバル委員会（GCSC）、「*シンガポールを通した規範（Norms Through Singapore）*」（2018年11月号）、https://cyberstability.org/wp-content/uploads/2019/04/singaporenew-digital.pdf。「国家および非国家主体は、開発中・生産中の製品やサービスを改ざんしてはならず、また、サイバースペースの安定性が実質的に損なわれる可能性がある場合も改ざんを許してはならない。」

国連GGEの規範とGCSCが提案した規範の間におけるもう一つの大きな違いとして、GCSCではサイバースペースの安定性を確保するために自制を行使したり、積極的な措置を取ったりしなければならないため、非国家主体にも責任を課すべきであると考えている点が挙げられる。ここで言うサイバー攻撃とは犯罪者によるサイバー攻撃のことではない（政府の行動によって抑止されない犯罪者は規範によって抑止されることもない）。しかし、技術は急速に変化するものの法律はそうではないため、法律が制定されていない場合でも、どのような非国家主体による行動が奨励されるべきか、または抑制されるべきかを正確にしておくことは有用である。例えば、ハッキングの被害者に「ハッキングし返す」ことを認めるべきだと主張する者もいる。GCSCでは、そのような行為を許可または禁止する法律がない場合でも、最初の攻撃者が第三者のシステム（例えばクラウド プロバイダや病院）を経由して攻撃を行っている可能性があり、ハッキングし返すことによって無実のユーザー（例えばクラウドの顧客や患者）に影響を与えてしまう可能性があることなど、いくつかの理由によりそのような行為は望ましくないと考えている。加えて、無実の被害者に対するこれらの攻撃により、ハッキングし返すことは衝突を激化させる行為であると見なされる可能性がある。簡単にまとめると、提示されている複雑性により、法律がない場合でも民間部門の行為主体を抑制する規範が行動に影響し、それによって功を奏する可能性がある。

A. GCSCが提唱する規範

上述の論点を念頭に置き、GCSCは提唱する規範を以下の通り開発した。

1. 国家および非国家主体は、インターネットのパブリック・コアの全体的な可用性または完全性、そしてそれによってサイバースペースの安定性に大幅な損害を意図的に与えるような活動を行ったり、そのような活動を故意に許したりしてはならない。

2. 国家および非国家主体は、選挙、住民投票、直接投票に不可欠な技術的インフラを破壊することを目的としたサイバー活動を追求・支援・許容してはならない。

3. 国家および非国家主体は、開発中・生産中の製品やサービスを改ざんしてはならず、また、サイバースペースの安定性が実質的に損なわれる可能性がある場合も改ざんを許してはならない。

4. 国家および非国家主体は、ボットネットや同様の目的で利用ために一般市民のICT資源を徴用してはならない。

5. 国家は、情報システムや技術に関する未公開の脆弱性や欠陥を開示すべきか否か、またいつ開示すべきかを評価するために、手続き的に透明性のある枠組みを構築すべきである。基本的には開示することを前提とすべきである。

6. サイバースペースの安定性を構成している製品やサービスの開発者や生産者は1. セキュリティと安定性を優先し、2. 製品やサービスに重大な脆弱性がないことを担保するための合理的な措置を講じ、3. 後になって発見された脆弱性を適

宜緩和するための措置を講じるとともにそのプロセスについて透明性を確保しておくべきである。全ての行為主体は、悪意のあるサイバー活動を防ぎ緩和するために脆弱性に関する情報を共有する義務を負う。

7. 国家は法律や規制を含む適切な施策を制定し、基本的なサイバー衛生を確保すべきである。

8. 非国家主体は攻撃的なサイバー活動に従事してはならず、国家行為主体はそのような活動を防止し、発生した場合には対応すべきである。

規範を表現するための最も適切な文言を見つけることが難しい場合があることは注目に値する。規範が精確すぎて解釈の余地が与えられていなければ、コンセンサスを得ることが難しくそのカバレッジに多大なギャップが生じる可能性がある。反対に規範が曖昧すぎると、行動を導き、特定の行為主体群に対して明確な期待値を設定するために必要なガイダンスの種類を提供しないことになる。正しいバランスを見つけ、必要な箇所はさらなる規範を開発し、望まれざる行動に対処することが目標なのである。例を挙げると、2015年に採択された国連GGEの規範では重要インフラを保護しているが、インターネットのパブリック・コアがこの用語の対象となるかどうかは明確になっておらず、多くの者が重要インフラをユーティリティやサービス（例えば電力、通信、バンキング）として捉えている[42]。さらに、国連GGEは選挙システムについても特に言及しておらず、これは2015年以降に懸念が深刻化している領域である。[43]一部の国では参照によって選挙システムがカバーされている場合もあるが（すなわち、選挙システムを重要インフラと見なし、重要インフラの規範の範囲内に含めるようになった国がある）[44]、特定の国ではこのアプローチに従わない場合もある。そのため、サイバースペースはグローバルでありながらも、規範的な保護はそうではないことがある。GCSCによる規範に関する解釈の問題に対処するために、委員会では上述の核規範について背景について説明することにした（補足資料Bを参照）。

最後に、サイバースペースにおける行動に関する規範は静的であってはならない。GCSCの規範は変わり続ける技術の景観におけるある瞬間を反映している。国家と非国家主体は技術の進歩に応じて、そして既存の技術が持つ意味合いに対する我々の理解が変わるにつれて、新たな規範を作成する準備を整えておくべきである。

国連GGEの規範、GCSCの規範、その他の提案のいずれに注目しても、規範が有効であるためには規範が採用・実施されることが必要であり、規範違反者は説明責任を負わなければならないことを認識しなければならない。ここで、世界中に分散している非国家主体がまとまり、サイバースタビリティの問題に対する実践的な解決策に政府と協力して取り組むためにどうすればよいのか目を向ける前に、まずこれらの問題に対処する。

B. 規範の採用

規範が効果的であるためには幅広く受け入れられればならない。一部の者が潜在的な規範違反者として

42 重要インフラは「物理的または仮想的なものであるかどうかにかかわらず、そのようなシステムや資産の能力不足や破壊が安全保障、国家経済の安全保障、国民の健康や安全、またはそれらの組み合わせに衰弱的な影響を与えるほど重要なシステムや資産」を含むものとして定義されている。」*2001年の重要なインフラストラクチャ保護法（Critical Infrastructures Protection Act of 2001）*、42 U.S. Code § 5195c(e)、（2001）。それはまた「人々の社会的機能、健康、安全保障、経済及び社会的福祉の維持に不可欠な資産またはシステム」とも定義されている。欧州連合理事会、2008年12月8日に採択された「*欧州の重要インフラの特定と指定、および保護の改善の必要性評価（Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection）*」に関する理事会指令2008/114/EC、欧州連合公式ジャーナル、（2008年12月8日）、https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114。

43 Erik Brattberg と Tim Maurer、*「ロシアによる選挙干渉：フェイクニュースとサイバー攻撃に対する欧州の対抗策（Russian Election Interference:Europe's Counter to Fake News and Cyber Attacks）」*、カーネギー国際平和財団（2018年5月23日）、https://carnegieendowment.org/2018/05/23/russian-election-int europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435。また、Michael McFaul編集「*アメリカの選挙の保護（Securing American Elections）*」、スタンフード・ポリシーセンター（2019年6月）、https://cyber.fsi.stanford. edu/securing-our-cyber-futureも参照。

44 例えばアメリカ合衆国国土安全保障省の声明文「国土安全保障長官Jeh Johnsonによる選挙インフラを重要インフラのサブセクターとして指定することについて（Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector）」（2017年1月6日）、https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastruc-ture-criticalを参照。

見なしている行為主体さえも規範を受け入れることで、規範の違反やそのような違反に対する適切な集団的行動を呼びかける行為の正当性が強化されることになる。広く普及することが最善であるが、似た考えの国家同士やその他の主体が特定の規範について合意し実施するために小グループを形成することも可能である。これに対応するために、GCSCでは、国家やその他の利害関係者が一部の規範を受け入れる一方で他の規範を否定または棄権することを可能にする柔軟で拡張可能なアプローチを提案している。このアプローチは意見が一致または不一致している具体的な領域を強調することによって明確化しているだけでなく、他の規範を評価するためにより多くの時間が必要であっても特定の規範を受け入れ、洗練させ、実施することを可能にしている。いずれにせよ、規範が広く普及することは長期的な取り組みである。

規範の採用を促進させる上で、いくつかの独特かつ実践的な課題もある。比較的新しく、不安定化させるような行動について対処することを試みている点は独特の課題である。規範が「普通、一般的、または標準的」[45] である分には、将来の行動に関する規範の草案は興味深い演習となる。全員が既に特定の形で行動しているのであれば、記述した規範は既存の慣行の単なる成文化にすぎない。しかし、「典型的な行動」がない場合は、規範の草案は、今日において共通の行動がない場合でも将来に共通の行動を促すことを試みる行為となる。単に何か望ましいものを宣言することでそれを規範にすることにはならないため、採用を促進させる必要がある。

第二に、提案された規範を実施する能力のある主体や、規範が保護することを意図している主体が、その規範についてより深く認識する必要がある。国連やその他の多くのフォーラムで大きな活動が行われているとはいえ、規範の採択はまだ初期段階にあり、特に世界の特定の地域において提案された規範を促進させ、受け入れを実現するために多くの取り組みを行う必要がある。そのため、この領域におけるキャパシティ・ビルディングに向けた努力は非常に重要となる。キャパシティの高い組織ほど規範の採択を効果的に支援しやすく、さらに多くの支持者を獲得することは、どのような世界的な規範構造においても基本的なことである。加えて、規範によって守られる者は潜在的な影響について認識していない可能性があるため、アウトリーチを行う必要がある。例えば、コンピュータ緊急対応チーム（CSIRT/CERT）の間では、国家CSIRTを攻撃しておらず、防衛に関する目的のみに沿って使用している国に関する国連GGEの規範について認識が広まっているようには見えない。後述するように、被保護主体は（提案されている規範の設計と同様に）実施と説明責任において役割を果たすことが多いが、国家や非国家主体による提案について認識や洞察がなければその役割を果たすことはできない。提案している規範が支援することを意図しているコミュニティに手を差し伸べるために、政府や国際組織がさらに多くのことに取り組む必要があることは明らかである。

C. 規範の実施

採択後、国家と非国家主体は規範を実施するために具体的な措置を講じる必要がある。現在進行中の国連のプロセス（OEWGとGGE）や地域の取り組みの中では、規範の実施が優先事項であるというコンセンサスが進化しているように思われる[46]。一部にとっては、規範の実施とは規範の採択、キャパシティ・ビルディングの取り組みや信頼構築のための措置への参加、あるいは合意された規範の意味についてより詳細なコンセンサスを得ることを意味している[47]。これらの措置は規範の実施について重要な前提条件であるものの、規範の実施そのものではない。例えば、各国が自らの安全保障を確保し、国際的に関与するための帯域幅を確保するためにはキャパシティ・ビルディングが必要であるが、規範を採択したり実

45 https://www.lexico.com/en/definition/normを参照。

46 国連総会決議73/266、3頁、第1項(b)、https://undocs.org/en/A/RES/73/266、国連総会決議73/27、5頁、第5項、https://undocs.org/en/A/ RES/73/27。欧州安全保障協力機構（OSCE）、*Thomas Greminger事務局長の開会挨拶*、2019年議長職OSCE全体のサイバー・ICTセキュリティ会議（Bratislava, 2019）も参照のこと。「地域組織は、CBMに関連した新しいアイデアや実践的な取り組みのインキュベーターとなり得るだけでなく、GGE報告書のような世界的に認められた協定の実施者となり得る。つまり、各地域組織はインキュベータでもあり実装者でもあるのだ。」

47 国連総会は、すべての加盟国に対し、GGE及びOEWGの報告書に記載された評価及び勧告を考慮に入れ、*特に*「情報セキュリティを強化し、この分野における国際協力を促進するために国内レベルで取られた努力」及び「世界レベルで情報セキュリティを強化するために国際社会が取ることができる可能性のある措置」についての意見及び評価を引き続き事務総長に報告するよう求めるものである。国連事務総長報告書74/120、https://undocs.org/A/74/120。加盟国の国家的な視点についてはhttps://www.un.org/disarmament/ict-security/を参照。

施したりせずともキャパシティ・ビルディングは可能である。同様に、信頼の構築に向けた対策も、サイバー教義に関する各国の意見交換の促進、各国のサイバー専門家間の迅速なコミュニケーショ ンのためのホットラインの設置、ベストプラクティスやセキュリティ基準の共有の奨励などによってサイバースペースの安定性を維持するために役立つが、これらも規範の実施なしに実現することはできない。むしろ、規範の実施はそれに力を与えるための具体的なステップを踏むことが伴う。国内では、これには提唱されている規範を国内政策、法律、戦闘教義へと取り込むことが考えられる。国際的には、攻撃を帰属したり、外交上の行動に出たりする際に規範の規定を引用することが考えられる。このような形で規範を操作化することで、さらに精確な定義を与えることもできる。

D. 説明責任

いったん規範が採用され実施されると、それに違反した者に対する説明責任が必要となる。これは帰属と対応という複雑な問題を提起しており、その両方がサイバー攻撃に対処する上で難しい問題であることが証明されている。

国家または非国家主体が不正な行為を行ったという主張を裏付けるためには信用できる帰属が必要である。これは証拠の収集と分析から始まり、帰属の品質と適時性を改善するために今取り組むことができる技術的な作業と手続き的な作業の両方がある。具体的には、他の技術分野と同様に、証拠の収集と分析のために十分受け入れられているプロトコルを用意しておくことが調査の質を高める上で重要になってくる。そのため、帰属をケースバイケースで決めなくてはならなくても、調査手法の標準化が証拠の完全性に対する懸念を減らす可能性があるため重要である。技術的な問題として帰属を改善することに加えて、帰属の決定に関する官僚的なプロセスを短縮し、適切なタイミングで公表するためにできることは多い。事象の発生から責任の宣言が行われるまでに長い時間がかかることが多いのは、国家レベルでそのような決定に到達するためのプロセスが不明確または扱いづらかったりすることが少なからず原因となっており、複数の国家が集団的な帰属声明の作成に関与している場合にはさらに悪化する。国家レベルと国際レベルで帰属に至るプロセスを設計・行使し、国家間の情報共有を改善することにより、帰属声明の適時性と有効性を大幅に改善し、更なる適切な行動を促進することができる。

証拠が特定の行為主体を示している後でも、次のステップ（帰属）が引き続き困難である可能性もある。過去には、帰属が不可能であるか、絶対的な証拠を必要とすると一部の国家や非国家主体が主張していた。しかし、絶対的な証拠は必要ではなく、帰属は難しい可能性があるものの、一部の者が示唆しているような乗り越えられない問題ではない。国民国家の文脈では、サイバーの領域であれ物理的な領域であれ、帰属は政治的な行為であることが多く、証明の基準について特に合意されているものはないものの、各国は信頼性を失うことを恐れ、偽りの申し立てをしないよう強いインセンティブを持っている。要するに、帰属が他国や国民にとって納得のいくものである必要がある。

不満がある側が特定の行為主体に責任があると納得したとしても（実際に国際的な事例では帰属が発生している）、行為者に真に説明責任を負わせることは困難であることが明らかになっており、規範の価値を損なわせている。結局のところ、受け入れられた規範に違反した者に対して不利な結果がなければ、その規範は机上の空論に過ぎず、不安定化する活動を抑止することはできないだろう。

非国家主体によるサイバー攻撃に対する説明責任は比較的簡単であり、一般的には関係国の国内法に基づいて民事責任または刑事責任を課すことで達成している。多くのサイバー攻撃の国際的な性質や証拠収集に関する技術的な課題が国家の行動を阻害する可能性があるため、このような行為には確かに課題がある。しかし、今後どう前進すべきかは概念的には明確であり、すなわち国際法の執行プロセスを簡素化し、サイバー犯罪者の特定と起訴を確実にするよう取り組むことである。

規範違反について国家の説明責任を問うことはさらに困難である[48]。これはサイバースペースでの攻撃への対応はその文脈・状況背景に大きく依存するからである。説明責任が要求されるかどうかについては、国家と非国家主体は異なる要因を考慮している。例えば、規範違反に対応する国家は政治的な影響を考慮し、民間企業はビジネスや評判に対する影響を考慮する。規範違反にどのように対処すべきかについては、規範違反への対応は軽微（例えば私訴）、重大（例えば経済制裁）、または劇的（例えば高度に可視化された運動による反応）などが考えられるため、対応するための国家の行動は連続体に沿って捉えることができる。万能型の対応はなく今後も現

48　国家はサイバー活動に関して、自らが行う行為、指示、または許可することに関しては責任を問われることとなり得る。デューデリジェンスの原則は、サイバースペースにおいて活動する国家に求められるケアの水準を定義するのにも役立つ。Joanna Kulesza「*国際法におけるデューデリジェンス（Due Diligence in International Law）*」（Leiden:Brill Nijhoff, 2016）、https://doi.org/10.1163/9789004325197。 ま た、2001年に国際法委員会の第53回会期にて採決され、同年12月12日に国連総会決議56/83にて取り入れられ、その後文書A/56/49（Vol I)/Corr4にて訂正された第4条及び11条を含む「*国際違法行為に対する国家責任（Responsibility of States for Internationally Wrongful Acts）*」*の条文を参照*。http://legal.un.org/ilc/texts/instruments/draft_articles/9_6_2001.pdf。

れないものの、規範や国際法の違反に対しては有意義な結果がなくてはならないことは明らかである。規範を施行するための過去の取り組みによる成功は限定的であったため、より効果的で時宜を得た対応を行い、そのような対応がさらなる不安定性を最小限に抑えることを目指すべきであることを認識する必要がある。

非国家主体も規範違反者がその行動について説明責任を負わせるように努めている。例えばGFCE[49]は、規範の採用、実施、説明責任の必要な前提条件であるキャパシティの構築に向けて取り組みを連携させるよう政府、市民社会、民間部門のメンバーをまとめ支援している。加えて、民間部門は攻撃の原因を特定する役割を拡大しており、独自の情報と公開情報の両方を利用し行為主体を暴露し、それらがもたらした損害について説明している。最後に、より体系的に（そして可能であればより大きなスケールで）大規模なサイバーイベントを監視し曝露するように設計されている「サイバー・ピース・インスティチュート」[50]など、一部の民間部門の主体が新たな取り組みの提案や立ち上げを行っている。

非国家主体は、規範違反者の違反に対する責任を問う上で、より大きな役割を果たすべきである。民間部門による規範の施行は新しい発想ではない。例えば、南アフリカの反アパルトヘイト闘争中の1977年、ゼネラル・モーターズは南アフリカでビジネスを行うために（およびビジネスを行わないために）広く採用されている一連の原則を推進し、125社以上の外国企業が同国から引き上げる結果を招いた[51]。最近では、比較的象徴的な形ではあるが、多くの企業（および政府）がサウジアラビアの野党記者ジャマール・カショギ殺害事件に対応し、不支持のメッセージを発信するために未来投資イニシアチブをボイコットした[52]。これらの取り組みはさらに検討するに値する。

E. 利益共同体

規範の採択、実施、説明責任に対するマルチステークホルダーのアプローチは重要であるが、これらのグループのエネルギーと能力を活用することは困難である。政府は似たような考え方の国家グループを表すために「志を同じくする国家」という言葉をよく使用するが、特定の問題について同じ見解を共有する国家、民間企業、非営利組織（標準化団体を含む）、市民社会、個人の集合体を包括する同等の言葉はない。これは、国連GGEとGCSCによって提案された規範が異なる構成員に影響を与える可能性があり、また、異なる組織や社会のメンバーが他のものよりも特定の規範を擁護することに関心を持っている可能性があるため重要である。政府、民間企業、技術コミュニティ、学界、市民社会は一枚岩ではないため、集中的な努力ではなく、規範に関連する問題に多様なコミュニティを巻き込むような協調的な取り組みをどのように作るかを考えることが重要である[53]。共通の興味を抱く共同体や利害が一致する共同体など（称して利益共同体、Communities of Interest）を形成することで、特定の規範について専門性を有する者たちがさらなる開発と実施について取り組むことができる。例えば、選挙システムの責任者が選挙システムに関するGCSCの規範に特に関心を持っているように、コンピュータ緊急対応チーム（CERT/CSIRT）はそのコミュニティを保護することを目的とした国連GGE規範の実施と監視に特に関心を持っている可能性がある。同様に、インターネットのコミュニティには、インターネットのパブリック・コアの保護について委員会が提案している規範の推進、実施、監視を支援できる可能性がある一方で、開発者は製品の改ざんに関わる規範に最も強い関心を持っているかもしれない。

利益共同体の形成は指導することもできれば、アドホックなボトムアップ型の過程で行われることもある。メンバー自体が共同体を形成できるという事実は、それらの発展と成功が運に任せられることであることを示唆していない。その代わり、共同体に成功をもたらす要素に集中することが大事であり、それらはすなわち1. 共有された原則、2. 問題への集中、3. テーマに対する専門性、4. 財務・運営上のサポート、5. 透明なプロセス、である。実際には、共同体がどのように作成され実施されるべきかについてベストプラクティスのテンプレートを特定できる可能性があり、それによって様々な規範設定プロセスが同様の共同体モデルを活用することが可能になることが考えられる。これは、効率性と集中力を確保するために異なる作業の流れを調整するのに役立つだけでなく、規範の採択、実施、説明責任のためのベストプラクティスを活用する上でも役立つだろう。

49 サイバー専門的知識に関するグローバルフォーラム、https://www.thegfce.com/。

50 サイバー・ピース・インスティチュート、https://cyberpeaceinstitute.org/.

51 「サリバン原則（Sullivan Principles）」ウィキペディア（英語版）（アクセス日2018年8月12日）https://en.wikipedia.org/wiki/Sullivan_principlesを全体的に参照。

52 「Western boycott of Future Investment Initiative 2018（未来投資イニシアチブ2018をボイコットする西洋）」、*Royal News*、2018年10月16日、https://en.royanews.tv/news/15500/2018-10-16を参照。

53 「*デジタル相互依存の時代（The Age of Digital Interdependence）*」、https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCo-operation-report-for-web.pdfを全体的に参照

7. 勧告

サイバースペースの安定性を確保するための六つの勧告は責任、自制、行動義務、人権の尊重の原則から流れている。サイバースペースの安定性を確保する上では全員が責任を持ち、マルチステークホルダーによるアプローチが重要であるため、我々の勧告では一部を「利益共同体」を通じて国家と非国家主体の能力を活用することを模索している。まとめると、我々は行うべきことと、それをどのように行うことができるのかについて集中している。

1. **国家と非国家主体は自制を促進し、行動を促すことによってサイバースペースの安定性を高めるような規範を採用し実施しなければならない。**規範に既に合意している国家行為主体は用いている用語をより明確に定義し、さらなる交渉や既存の規範の実施に関する実践的な経験を通じて達成できる結果である可能性がある。国家と非国家主体の両方が公的な声明と政策および行動における変化を通じて規範を採用し実施していることを明確に示す証拠を提示すべきである。

2. **国家と非国家主体は、それらの責任と限界に沿って規範の違反に適切に反応し、規範を犯した者が予測可能で有意義な結果に直面することを保証しなければならない。**規範に違反した者がそのような行為に代償がないことを学べば、規範の策定と実施は効果的ではなくなる。そのため、国家と非国家主体は、行動義務の原則に沿って違反行為を評価し、適切な個別および集団的な反応を素早く決めて実施するための内部能力を開発すべきである。

3. **国際機関を含む国家と非国家主体は職員の訓練、能力の開発、サイバースペースの安定性の重要性に関する共通理解の促進に向けた取り組みを増やし、異なる関係者の多様なニーズを考慮すべきである。**キャパシティ、能力、理解を高めることで、人権を尊重しつつサイバースペースの安定性を強化するように設計された国際法、規範、その他の信頼を醸成するような施策を実施する世界の能力が拡大する。全ての関係者は、規範の採択と実施、説明責任の確保、その他の安定性に関する対策の実施、人権の尊重において前提条件であるキャパシティ・ビルディングに重点を置いているマルチステークホルダー組織であるサイバー専門的知識に関するグローバルフォーラムを含む既存の組織を活用すべきである。

4. **国家と非国家主体は規範の違反とそのような活動による影響に関する情報の収集、共有、評価、公表を行うべきである。**世界では国際連合で定められ、GCSCが提案している規範の違反となるような行動が見られているが、それらの報告は包括的というよりは逸話的なものである傾向がある。組織の中でも特に国家や商業的関心から独立しているものは、規範違反とその影響について情報を体系的に収集し公表すべきである。

そうすることで、国家と非国家主体による規範違反への対応を促し、規範に対する遵守度を向上させることができる。

5. **国家と非国家主体は利益共同体を確立し支援することでサイバースペースの安定性を確保すべきである。**共同体の確立と支援は、国家、民間部門、技術コミュニティ、学界、市民社会を含む全ての利害関係者がサイバースペースの安定性を担保する責任を果たすことにつながる。これらの共同体は、特に本報告書やその他の場所で提唱されているサイバーセキュリティ規範の解釈、採用および実施、帰属のための証拠基準がしっかりしているかどうか、規範違反者が適時かつ効果的な方法で説明責任を問われるかどうかに集中できる。

6. **GCSCは、安定性に関わる問題に対処するため、国家、民間部門（技術コミュニティを含む）、市民社会が適切に関与し協議に参加するような自立したマルチステークホルダー・エンゲージメントのメカニズムを確立させることを勧告する。**責任の原則は、サイバースペースの安定性を確保する上で全員が役割を果たしていることを認識し、マルチステークホルダーによるアプローチの必要性を強調している。2011年から2017年にかけて、そのような関与のために「サイバー空間に関する国際会議（Global Conference on CyberSpace、GCCS）」が他の文脈における世界的な安定性を達成することを担当する外務省や安全保障省の閣僚レベルの参加者を集めたプラットフォームを提供し、キャパシティ・ビルディングに向けた重要な取り組みであるサイバー専門的知識に関するグローバルフォーラムも立ち上げた。インターネット・ガバナンス・フォーラム（IGF）もマルチステークホルダーによる議論のための重要なプラットフォームを提供している。さらに最近では、サイバーセキュリティに関する規範の支持者による史上最大のマルチステークホルダーなコミュニティがパリ・コールで結集した。これらの取り組みは、本報告書や他の場所で提唱されているサイバーセキュリティの規範の実用的な実施に集中したグローバルで包括的かつ行動指向のマルチステークホルダーを発展させる上で機が熟していることを示唆している。このメカニズムは、持続的で継続的な努力を確実にするための立体構造によって支えられるべきである。

補足資料A：国連GGEによって採択された規範[54]

a. 国際的な平和と安全の維持を含む国際連合の目的に沿って、各国は、ICTの利用における安定性と安全性を向上させ、有害であると認められているか国際的な平和と安全を脅かす可能性のあるICTの実践を防ぐ対策の開発及び適用に協力すべきである。

b. ICT関連のインシデントが発生した場合、各国は、インシデントを囲む文脈、ICT環境における帰属の問題、結果の性質と程度を含むすべての関連情報を考慮すべきである。

c. 各国は、自国の領土がICTを利用した国際的に不当な行為に利用されることを故意に許してはならない。

d. 各国は、情報交換、相互支援、テロリストや犯罪者によるICTの利用を告発し、そのような脅威に対処するための他の協力措置を実施する上で最善となる協力方法を検討すべきである。この点について新たな対策を策定する必要があるかどうか、各国が検討する必要性が生じる場合もある。

e. ICTの安全な利用を確保するために、各国はインターネット上での人権の促進、保護及び享受に関する人権理事会決議20/8及び26/13、並びにデジタル時代におけるプライバシーの権利に関する総会決議68/167及び69/166を尊重し、表現の自由の権利を含む人権を完全に尊重することを保証すべきである。

f. 国家は、重要なインフラを故意に損傷させたり、一般市民にサービスを提供するために重要であるインフラの使用および運用を損なうようなICT活動を行うような国際法下における義務に反するような活動を行ったり故意に支援してはならない。

g. 各国は、世界的なサイバーセキュリティ文化の創造及び重要情報インフラの保護に関する総会決議58/199及びその他の関連決議を考慮し、ICTの脅威から重要なインフラを保護するための適切な措置を講じるべきである。

h. 各国は、重要インフラが悪意のあるICT行為の対象となっている他国による援助要請に適切に対応すべきである。また、各国は、他国の主権を十分に考慮しつつ、自国の領土から発せられている他国の重要インフラを狙った悪意あるICT活動を削減するための適切な要請にも対応すべきである。

i. 国家は、エンドユーザーがICT製品のセキュリティに対する信頼を得ることができるよう、サプライチェーンの完全性を確保するための合理的な措置を講じるべきである。国家は、悪意のあるICTツールや技術の拡散ならびに有害な隠れた機能の使用の防止に努めるべきである。

j. 各国は、ICTおよびICTに依存するインフラに対する潜在的な脅威を制限し、さらに可能であれば排除するために、ICTの脆弱性の責任ある報告を奨励し、そのような脆弱性に対する利用可能な解決策に関する関連情報を共有すべきである。

k. 他国の認定緊急対応チーム（コンピュータ緊急対応チームやサイバーセキュリティ・インシデント対応チームと呼ばれることもある）の情報システムに危害を加える活動を行ったり、そのような行動を故意に支援したりしてはならない。国家は、認定緊急対応チームを利用して悪意のある国際的な活動に従事してはならない。

54 国連総会、「*国際安全保障の文脈における情報通信分野での発展に関する国連における政府専門家会合の報告書（Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security）*」A/70/174 (2015年7月22日)、https://undocs.org/A/70/174を参照。

補足資料B：
GCSCの規範

1. パブリック・コアへの不干渉

規範：

国家および非国家主体は、インターネットのパブリック・コアの全体的な可用性または完全性、そしてそれによってサイバースペースの安定性に大幅な損害を意図的に与えるような活動を行ったり、そのような活動を故意に許したりしてはならない。

背景

インターネットのパブリック・コアを定義することは、数々の異なるタイプの攻撃が最終的にはインターネット全体の可用性や完全性（回避すべき結果）を損なう可能性があるため、難しいことである。とはいえ、このような広範な影響を与えようとする場合に対象となる構成要素は明らかに存在しており、少なくともそのような重要な要素の非網羅的なリストを提供することは可能である。最高レベルでは、委員会は、行為主体の行為が一般市民にかなりの影響を与えることを意味するものとして「全体的な可用性」という言葉を定義している。したがって、この規範では、それを支持する国家が、目的と範囲がより限定され、一般市民に実質的な影響を与えることがない活動を行ってもよいことを認識している。

委員会は、「インターネットのパブリック・コア（public core）」という言葉を、パケットのルーティングと転送、命名・採番システム、セキュリティとアイデンティティの暗号化メカニズム、伝送媒体、ソフトウェア、データセンターなどのインターネットに関するインフラの重要な要素を含むものとして定義している。

パケットルーティングおよび転送の要素には、1. パケット化された通信の送信元から送信先への転送を容易にする機器、設備、情報、プロトコル、システム、2. インターネット相互接続点（インターネットの帯域幅が生成される物理的なサイト）、3. その帯域幅をユーザーに伝送する主要ネットワークのピアリングルータおよびコアルータ、4. ルーティングの真正性を保証し、不正行為からネットワークを守るために必要なシステム、5. 上記の目的で使用される機器の設計、生産、サプライチェーン、6. ルーティングプロトコル自体の完全性およびその開発、標準化、保守プロセスなどが含まれるが、これらに限定されるものではない。

命名・採番システムには1. インターネットのドメインネームシステムの運営に使用されるシステムや情報（レジストリ、ネームサーバー、ゾーンコンテンツ、インフラ、暗号化されたレコードに署名するために使用されるDNSSECなどのプロセスを含む）、2. ルートゾーン、逆アドレス階層、国別コード、ジオグラフィック、国際化されたトップレベルドメイン、および新規のジェネリックおよび非軍事的なジェネリックトップレベルドメインのためのWHOIS情報サービス、3. 頻繁に使用されるパブリック再帰DNSリゾルバ、4. インターネットプロトコルアドレス、自律システム番号、インターネット・プロトコル識別子の一意な割り当てを利用可能にし、維持するインターネット割り当て番号局と地域インターネットレジストリのシステム、5. 命名プロトコルと採番プロトコルそのものやプロトコルの開発・維持のための標準化プロセスと結果のインテグリティなどが含まれるが、これらに限定されるものではない。

セキュリティとアイデンティティの暗号化メカニズムには1. ユーザーとデバイスの認証とインターネット取引の安全性を確保するために使用される暗号キー、2. それらのキーの生成、通信、使用、廃止を可能にする機器、設備、情報、プロトコル、システム、3. PGPキーサーバー、認証局とそのパブリックキー・インフラ、4. DANEとそれをサポートするプロトコルおよびインフラ、5. 証明書の失効メカニズムと透明性ログ、6. パスワードマネージャ、7. ローミングアクセス認証子、8. ネットワーク時間プロトコルとそのインフラなどの正確な時間と時間的優先順位の確立のためのメカニズム、9. 暗号化アルゴリズムとプロトコルの開発および保守のための標準化プロセスと結果の完全性、10. 暗号化プロセスを実装するために使用される機器の設計、生産、サプライチェーンなどが含まれるが、これらに限定されるものではない。

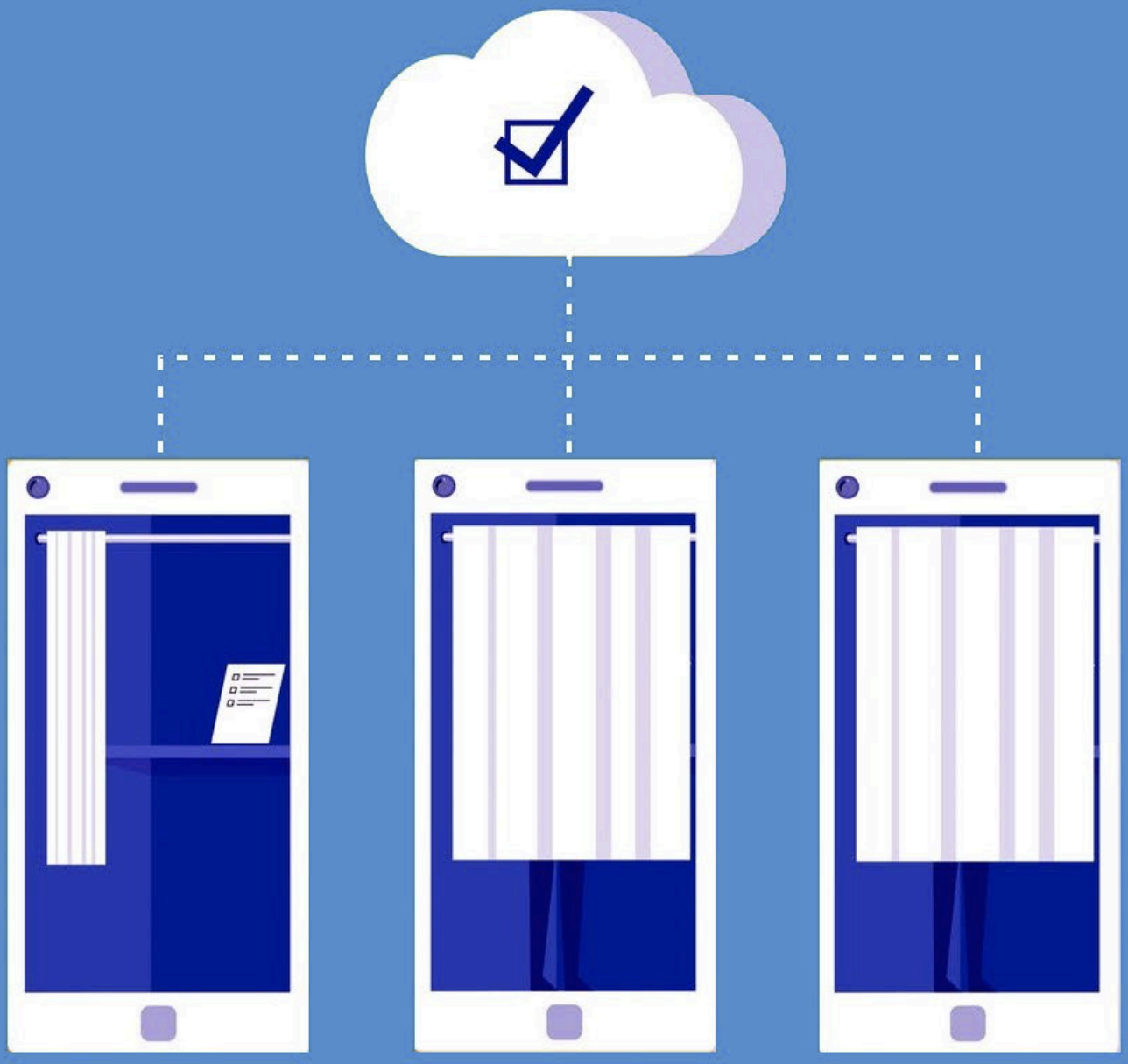
伝送媒体には、1. 光ファイバー、銅線、無線のいずれであっても公衆にサービスを提供する通信のためのインフラ、システム、および設備、2. 地上および海底ケーブル、およびそれらをサポートする陸揚げ局、データセンター、およびその他の物理的施設、3. 携帯電話およびその他の無線音声およびデータ通信、4. 規制された放送通信および規制されていない放送通信、5. 伝送、信号再生、分岐、多重化、および信号対雑音識別のためのサポートシステム、および6. 地域または人口にサービスを提供するものの、個々の企業の顧客にはサービスを提供しないケーブルシステムなどが含まれるが、これらに限定されるものではない。

ソフトウェアには、インターネットのコアおよびインターネット利用者の大部分が使用するソフトウェアの開発プロセス、ソースコード、パッチ配布インフラの可用性と完全性が含まれるが、これらに限定されるものではない。

データセンターには1. サーバー、コンテンツ、インターネットインフラを収容する物理的施設、2. データセンターの安全性、セキュリティ、物理的アクセス制御、運用、管理、保守、冗長システムを確保するために使用されるシステム、3. データセンターとの間やデータセンター内で通信を行うために使用される通信システムが含まれるが、これらに限定されるものではない。

専門家はインターネットおよびICT対応インフラの保護に値するカテゴリの数は遥かに多いと考えているため、この定義は今後拡大される可能性がある。

2. 選挙関連のインフラの保護



規範：
国家および非国家主体は、選挙、住民投票、直接投票に不可欠な技術的インフラを破壊することを目的としたサイバー活動を追求・支援・許容してはならない。

背景

国家共同体における各国の行動の指針となるすべての規則、教訓、原則の中でも、不干渉の規範が最も神聖視されていると考えられる。国際連合憲章第2条(4)はこの規範を明確化し、法的（ひいては拘束力のある）原則へと昇華させている。

> 国際関係において、すべての加盟国はいかなる国の領土的完全性や政治的独立性に対しても威嚇や武力行使、またはその他国際連合の目的に反する方法での武力行使を控えるものとする。

この規定により、本憲章の作成者らは、不介入の原則に対する最大の脅威が、国家の主権にとって必要不可欠である物理的または政治的自治権に向けられた強圧的な措置によるものであることを認めている。国家が支配する領土は国家の主権能力の表れであると考えられるものの、政治的主体性と独立性を享受することなくしては価値がない。さらに、自由かつ公平に行われる選挙などの全国的な参加プロセス以上に純粋な政治的独立性を反映している行為はない。国連の憲章は外部からの不当な干渉に対する強力な保護を与えることを模索している。

デジタルの時代になり、これらの保護措置は改めて問われるようになっている。

専門家の間では、最近見られるサイバー関連の選挙妨害が不法な主権侵害（本来政府の機能の行使を妨害するものであるため）なのか、不法な介入なのかについて議論が行われている[55]。しかし、国際法違反が発生したかどうかにかかわらず、悪意のある行為主体が（単独、集団、あるいは国家を代表して）行動し、デジタルな手段を使って選挙を操作する可能性は明らかに存在する。全国的な参加型プロセスの規模と高度化が進むにつれ、それを管理するためのデータ、制度、インフラが急増している。今日、多くの国では投票操作や不正行為に対する基本的かつ伝統的な保証である選挙人名簿をオンラインで公開しており、このようなデータベースはサイバー攻撃や悪用に晒されている。同様に、選挙管理者がデジタル操作に関連するリスクや懸念事項を十分に把握していない国における遠く離れた遠隔地では電子投票機器が用いられている。投票ソフトウェアの供給者やローカルまたは「投票記入所」レベルでのコンピュータシステムはそのような侵入による被害を受けやすいままである。

参加型プロセスに対する脅威の数と強度が増していることを踏まえ、このような攻撃は容認できないことを認識した上で、GCSCは、技術的な選挙インフラに対するサイバー攻撃を防止、緩和、対応するために、より強力な国内対策と効果的な国際協力を実現することを勧告する。委員会は、地域、地方、連邦レベルでの選挙や参加型プロセスを実際に行うことは、それぞれの国の法律に従って実施されるべき国家の揺るがぬ権限であることを認識している。しかしながら、選挙用インフラへのサイバー攻撃は国境の外に由来している可能性もあり、多国間協力による解決が求められている。選挙に用いる機械のデジタル化を選択する国が増えるほど、そのようなインフラに関連するリスクや脆弱性、そして大規模なサイバー攻撃の可能性は何倍にも増大していく。そのため、各国の政府は別の国家における技術的な選挙インフラに対するサイバー活動に従事することを控えるようコミットする必要がある。この規範を推奨するにあたり、委員会は選挙への干渉が、国際法違反と見なされるかどうかにかかわらず許しがたいことであることを肯定したにすぎない。

55　Michael N. Schmitt「バーチャルな公民権はく奪：国際法のグレーゾーンにおけるサイバー選挙干渉（'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law）」『*Chicago Journal of International Law*』第19巻、第1号及び Nicholas Tsagourias「選挙へのサイバー干渉、自決権、そしてサイバー空間における不干渉の原則（Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace）」https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/を参照。

3. 改ざんを回避するための規範

規範：
国家および非国家主体は、開発中・生産中の製品やサービスを改ざんしてはならず、また、サイバースペースの安定性が実質的に損なわれる可能性がある場合も改ざんを許してはならない。

背景

「インターネットのパブリック・コアへの不干渉」に焦点を当てた規範の中で、GCSCは国家や非国家主体に対し、インターネットのパブリック・コアの全体的な可用性や完全性に実質的な損害を意図的に与えないよう呼びかけた。この規範を支持して、委員会は、他のインフラによる安定した安全なインターネットへの依存度が高まっており、インターネットの崩壊が劇的な結果をもたらす可能性があることを指摘した。パブリック・コアの規範は「インターネットのコア」に焦点を当てているが、個人や組織は、パブリック・コアにアクセスしそれが提供している接続性を活用する上で、特定の商用製品に大きく依存している。その結果、ソフトウェアおよびハードウェアIT製品（オペレーティング・システム、産業用制御システム、スイッチ、ルータ、その他の重要なネットワーキング機器、重要な暗号化製品および標準、マイクロチップ設計、および広く使用されているエンドユーザー向けのコンシューマー・アプリケーションを含むが、これらに限定されない）の主要な構成要素を改ざんすることによっても、インターネットを安全かつセキュアな環境で活用する能力を社会から同様に奪われ、インターネットの適切な機能に対する全体的な信頼が弱まる可能性がある。そのような攻撃はニュースでよく耳にするものの、製品やそのアップデートが市場に到達する前にも既に攻撃が発生しうるという事実はあまり注目されていない。例えば、製品は、その設計・製造段階や、アップデート適用中に脆弱性の挿入（またはセキュリティ機能を秘密に除外する行為）による攻撃を受けることがある。言い換えると、製品はそのリリースや生産前に改ざんされることがあり、一般市民が被るその影響も大きい。脆弱性を挿入する時点と悪意ある使用のために脆弱性を活性化させる時点は様々である。

情報技術製品に対応する上で、国家は矛盾した利害と責任を抱えている。一方では、悪意のある行為主体による将来のサイバー攻撃を阻止し、デジタル・エコシステム全体をより安全にするためにサイバーインフラの回復力と完全性を促進させる義務を負っている。もう一方では、国家は国の安全保障を守り、サイバースペースにおける犯罪者やその他の悪意のある行為主体と戦う義務を国民に対して負っている。敵対者が使用するデジタル製品やサービスにおける脆弱性は、国の安全保障と公共安全のミッションを達成するために国家によって活用されてきた。したがって、国家が脆弱性を悪用することがその責任を果たすための効果的なアプローチであると考える程度には、 敵対者が使用する製品やサービスに意図的に弱点やバックドアを導入することも有用であると考えるかもしれない。非国家主体も、その目的がサイバースペースの安定性を破壊する能力によって助けられることもあり、製品やサービスを改ざんする可能性がある。ここで、サイバースペースの安定性をリスクに晒すような製品またはサービスラインの改ざんをこの規範では禁止している点は留意すべき重要なことである。この規範はサイバースペースの全体的な安定性に対するリスクが少ない標的型の国家行動を禁止するものではない。例えば、軍事スパイや犯罪捜査を容易にするために、限られた数のエンドユーザーのデバイスを標的にして傍受したり、改ざんしたりすることが例として挙げられる。パブリック・コアそのものの基幹インフラ内で発生したり、ユーザーによるインターネットに対する世界的な信頼を決定的に弱めたりしない限り、この種の活動がサイバースタビリティの条件であるサイバースペースに対する全体的な信頼を弱めるとは考えにくい。非国家主体は限定的な形でシステムを標的とすることもありうるが、そのような活動は既存の刑事法や民法に違反する可能性がある。

国家や非国家主体は開発・生産中の製品を断定的に買い残すべきではないが、業界内の行為主体にもそのような活動を防止する義務がある。したがって、製品やサービスの開発者はセキュリティを優先し、それによって脆弱性の可能性、頻度、悪用可能性、重度を低減するような製品やサービスの設計、開発、提供において、合理的な程度の勤勉さを約束しなければならない。また、関係者は、製品やサービスを危殆化させようとする国家や非国家主体の明白な行動を拒否するとともに、改ざんのリスクを低減し、改ざんが発見された場合の対応を可能にする慣行を採用しなければならない。

4. ICT機器のボットネット化に対する規範

規範：
国家および非国家主体は、ボットネットや同様の目的で利用ために一般市民のICT資源を徴用してはならない。

背景

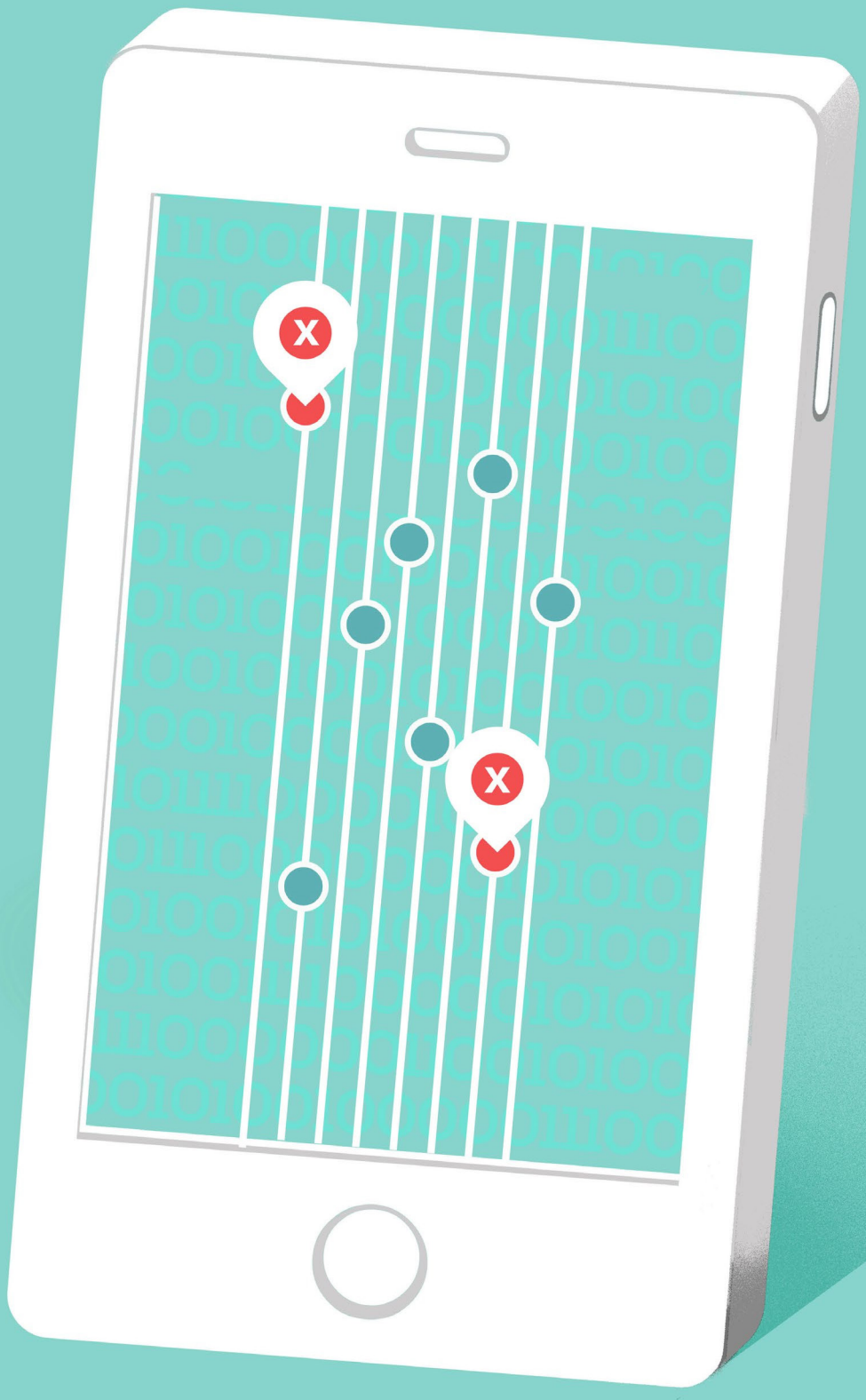
インターネットに接続している機器は世界中の人々の生活に欠かせないものになりつつある。私たちは様々な計算、ネットワーク、センシング、駆動能力を搭載した機器に囲まれている。温度計、テレビ、医療機器、目覚まし時計、自動車には流用し乱用できるような計算、保管、ネットワークキャパシティが搭載されている。その根底にあるコードにおける脆弱性の悪用により、その機器を使用している個人に対する物理的安全性の問題に至る恐れがある。設計パラメータの範囲外で動作しているデバイスは火災に巻き込まれたり、予期せぬドアの施錠、家の中からのビデオ放送、（医療）機器の故障などといったりしたその他の危険な状況を生み出す可能性がある。

我々は、ソフトウェアのエージェントが同意なしに大量にインストールされ、機器の計算、保管、ネットワーク資源を利用しようとすることをボットネットと呼んでいる。これらのボットネットは、最終標的のデータ機密性、可用性、完全性への影響を含め、異なる標的システムに直接的な影響を与えるために用いられる。そのため、関与していない可能性のある「第三者」機器とその所有者・操作者は知らないうちに悪意のあるサイバー活動の当事者となってしまう。悪意のあるソフトウェア・エージェントをインストールするために機器を侵害することは、他の攻撃（例えば犯罪者からの攻撃）から機器の防御力を弱めたり機器の正常な機能を侵害したりするだけでなく、最終的な標的に与えられた損害に対して所有者・操作者が責任を負う可能性ももたらしている。これは、機器の危殆化によって、国家間の敵対関係において機器とその所有者・操作者が不意に好戦的な立場に置かれてしまい、それによって報復を招いたり責任を問われたりする可能性がある場合には特に顕著に見られる。

個人的な環境におけるテクノロジーへの依存度が高まりより多くのコネクテッドデバイスが市場に出回るようになるにつれ、コンシューマーデバイスの悪用やボットネット化は信頼の喪失を増大化させ、社会を不安定化させるものとなっている。委員会は、例えば法執行を目的とする場合など、許可された国家行為主体が、特定の標的となる個人敵対者や敵対集団のデバイスにソフトウェア・エージェントをインストールする必要があると考える場合があることを認識している。しかし、国家や非国家主体は、動機の本質にかかわらず、攻撃的なサイバー作戦を容易にしたり直接的に実行したりするために一般市民の機器を（一斉に）徴用すべきではない[56]。

56　この規範はリリース前の製品の改ざんを国家や非国家主体が回避するための前述に提案した規範を補完するものである。前述の規範はサプライチェーンの観点に注目しているのに対し、本規範は既に展開した機器を対象としている。

5. 脆弱性公平プロセスを規定するための国家の規範



規範：

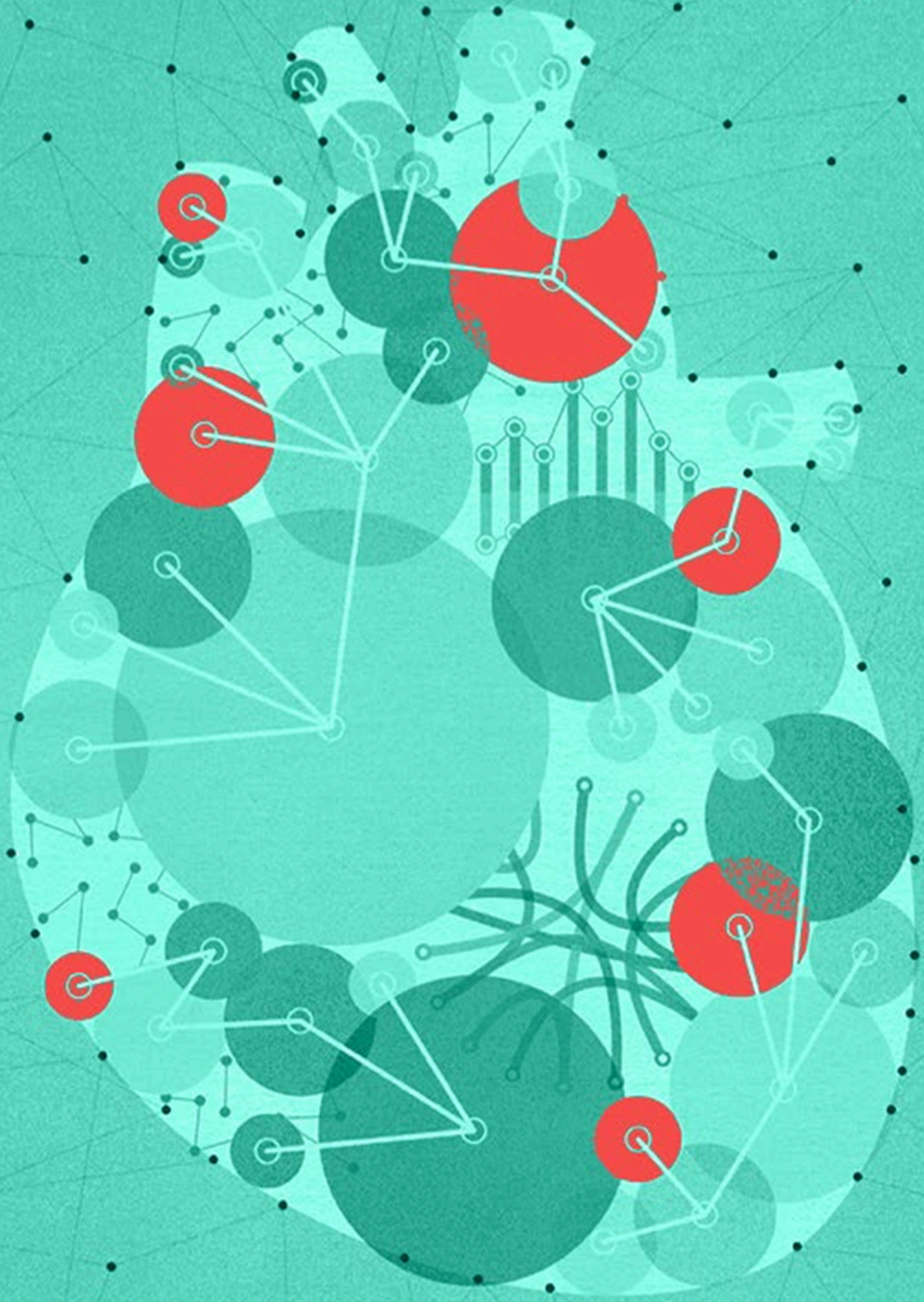
国家は、情報システムや技術に関する未公開の脆弱性や欠陥を開示すべきか否か、またいつ開示すべきかを評価するために、手続き的に透明性のある枠組みを構築すべきである。基本的には開示することを前提とすべきである。

背景

オペレーティング・システム、クリティカルなソフトウェア、コンピュータのハードウェアなどの複雑さが増すにつれて、抱えている脆弱性も増えている。これらの脆弱性は国家や非国家主体が利用できるものである。新たに発見された脆弱性に対応する上で、国家は矛盾した利害と責任を抱えていることがある。一方では、サイバースペースの安定性に必要不可欠なインフラの回復力と完全性を促進させ、悪意のあるサイバー攻撃を阻止することですべてのユーザーにとってデジタル・エコシステム全体をより安全にする義務を負っている。このことは、国家が新たに発見された脆弱性をベンダーや製造業者に迅速に開示してパッチを当て、必要に応じて広く公開して国民を保護することを主張している。その一方で、国家には犯罪者から国民を守りサイバー犯罪の捜査と起訴を行う義務があり、将来の悪意ある活動に対する特定の抑止力としても一般的な抑止力としても機能する制裁措置を課す権利を保持している。悪意のある行為主体、特にならずもの国家のような洗練された行為主体を追求するために不可欠な手段は、彼らが依存しているデジタル・インフラストラクチャの脆弱性を利用することである。そのため、国家は未公開の脆弱性の利用を含め、少なくともいくつかの選択された能力を維持しなければならず、さもなければ能力の非常に高い悪意ある行為主体の発見と確認ができないままであると主張することが多い。

発見したすべての脆弱性を国家が自主的に開示することは考えにくいが、最近、いくつかの国家では、すべての未公開の脆弱性が保持されるという考え方から離れ、より大きな体系的なサイバーセキュリティの利益のために開示を支持するという考え方へと移行している。そのためには、政策的、経済的、社会的、技術的な公平性の全範囲を考慮に入れた、公開の是非を評価するための公的に記述されたプロセスを各国家が作成することが肝心である。より具体的には、そのプロセスは手続き的に透明性があり、ネットワークのセキュリティと回復力、ユーザーとそのデータのセキュリティ、法執行と国家安全保障の有用性、外交的・商業的な意味合いなどの要素を含む、あらゆる意見を考慮するべきである。アメリカ合衆国は近年そのようなプロセスの新しいバージョンを公布し、他の国々も独自の脆弱性公平プロセス（VEP）指針の作成を検討している。脆弱性の発見と開示はどの国家よりも範囲の広いものであることを踏まえると、国家安全保障を守りながらネットワークの回復力を促進するためには、全ての国がこのようなプロセスを設けることがサイバースペースの長期的な安定性にとって有益となると考えられる。加えて、国家は互換性があり予測可能なプロセスに向けて取り組むべきである。そのようなプロセスの存在は、妥当な公平性や利害衝突が完全に考慮されていることをある程度保証するため、国家間での信頼を構築する手段となる。勿論、どの国家も能力が異なり機関間の構造も独特であるが、いかなる有効なVEPプロセスも幅広い観点や公平性を視野に入れて設計されるべきである。加えて、個別のケースにおける実際の決定が必然的に機密でなくてはならないものの、そのような意思決定に至った全体的な手順と枠組みについては透明性を担保すべきである。最後に、この規範は公開するという決定が行われるプロセスの確立のみについて言及している。政府またはその他の法人が公開する判断をする場合、そのような公開は責任ある形で行われ、公共安全を促進させるとともにその脆弱性の悪用につながらないようにすべきである。

6. 重大な脆弱性を削減し緩和するための規範



規範：

サイバースペースの安定性を構成している製品やサービスの開発者や生産者は1. セキュリティと安定性を優先し、2. 製品やサービスに重大な脆弱性がないことを担保するための合理的な措置を講じ、3. 後になって発見された脆弱性を適宜緩和するための措置を講じるとともにそのプロセスについて透明性を確保しておくべきである。全ての行為主体は、悪意のあるサイバー活動を防ぎ緩和するために脆弱性に関する情報を共有する義務を負う。

背景

特定のIT製品やサービスはコアでの名前解決やルーティングなどのコア技術インフラ内での使用、ユーザーによるインターネット体験の広範な促進、または重要なインフラ内での使用により、サイバースペースの安定性にとって必要不可欠なものとなっている。製品やサービスの開発者はセキュリティを優先し、それによって脆弱性の可能性、頻度、悪用可能性、重度を低減するような製品やサービスの設計、開発、提供において、合理的な程度の勤勉さを約束しなければならない。

ソフトウェアやハードウェアの複雑性が高まっていることにより、これらの製品における脆弱性は珍しくなくなっている。これらの脆弱性は通常は意図的ではないものの、サイバースペースの安定性を損なうような方法で発見された場合には、悪意のある国家や非国家主体がこれらの脆弱性を悪用することが多い。

さらに、ハイパーコネクテッドかつハイパー依存型の世界では、発見された脆弱性は異なる生産者や環境による複数の製品やサービスに影響を与える可能性もある。ある製品の根底にある脆弱性を公開せずにその製品にパッチを当てることで製品が保護されるかもしれないが、サイバースペース全体の安定性は保護されない。ある脆弱性の影響を評価するのに最も適した立場にあるのは、多くの場合、その脆弱性が影響を与える製品を開発、生産、インストール、運用している者たちである。セキュリティの脆弱性を修復したり攻撃の防止、制限、または緩和に資したりするような情報の共有は重要である[57]。

新規にリリースされた製品や更新された製品に脆弱性が存在しないことを保証することは現在では非常に困難であるものの、提案されているこの規範は、そのような製品の開発や製造に関与する者が発生する頻度や重度を軽減させるような「合理的な措置」を講じることを提案している。

「改ざん禁止」規範が重要な製品やサービスへの意図的な脆弱性の挿入に対処し、「衛生」規範が最終的にエンドユーザーの義務に対処しているのと同様に、この規範では重要な製品の開発・製造に携わる者が、重要な脆弱性の数と範囲を最小限に抑え、効果的かつ適時に脆弱性を緩和し、適切な場合には発見され次第その旨を開示することを確実にするための合理的な措置を取るよう求めている。使用するプロセスは透明性であり、予測可能で安定した環境を創出すべきである。

57　国連GGEによる2015年度報告書（A/70/174）における国家の責任ある行動に関する規範の一つでは「国家はICTにおける脆弱性の責任ある報告を奨励し、ICTとICTに依存するインフラに対する潜在的な脅威を制限し、さらに可能であれば排除するために、そのような脆弱性に対する利用可能な解決策に関する関連情報を共有すべきである」と述べている。

7. 基礎的な防衛としての基本的なサイバー衛生に関する規範

規範:
国家は法律や規制を含む適切な施策を制定し、基本的なサイバー衛生を確保すべきである。

背景

インターネットの接続性が世界中に広まり現代生活のあらゆる面に浸透している中で、個人、組織、企業､政府などあらゆる種類のユーザーは、この技術とインターネット上で利用可能な情報へのアクセスへの依存度をますます高めている。政治、経済、公共情報、教育、開発、その他あらゆる形で行われる社会的相互作用はインターネットと関連する技術に決定的に頼りきっている。しかし、この現代の驚異は依然として広範な安全性が確保されておらず、誰もその危険性を免れることはできない。

サイバースペースにおける有望な技術を最適化しつつ一般市民を保護するための最も効果的な方法についてはまだコンセンサスが得られていない。しかし、サイバースペースにおける本質的なセキュリティに関する合意された基準がなければ、デジタルに接続された生活から得られる便益を今後も維持することはできないという点ではほとんどの人の意見が一致している。この目的のために、委員会は、基本的なサイバー衛生基準の広範な採用と検証された実施を強く支持している。この「サイバー衛生」とは、サイバースペースにおける回避可能な危険に対して防御し、それを防止および迅速に緩和するための優先化された必要不可欠な措置を表す基礎的な対策によって構成される体制のことである。

実際、オンラインでの相互接続性の幅広さを踏まえると、これらの対策は全てのユーザーに求めるべき基本的なケアの義務を構成している。衛生体制では、信頼性の高い実施方法を取り入れ、技術情報とベストプラクティスを広く共有し、適切な監視の対象になるべきである。日増しにスマートになっていくデバイスやプロセスはスマートな法律や規制を求めている。サイバーケアという基本的な義務に対する説明責任をさらに創出する上で、政府はイノベーションを抑制したりインターネットの基本的な特性を変えたりするべきではない。

サイバー衛生の基準は既にさまざまな形で存在している[58]。既知のマルウェアの危険性を予防し、迅速に軽減するために実証された手順を踏むことの重要性を政府や企業が理解しつつあるため、これらの基準は国際的に広く受け入れられるようになってきている。さらに、これらの基準はベストプラクティスであり、賢明で定期的な監視の重要性を強調し、可能な限り自動化された 情報共有を行うことで他のユーザーにトラブルを警告することの重要性を明確に示している。これらのアプローチで概説しているこのような基本的なサイバー防御は政府や組織、ユーザーの集合体が単独ですべてのサイバー関連のリスクを緩和することはできないという現実を考慮している。また、全てのレベルにおけるユーザーがサイバーセキュリティの強化において重要な役割を担っている点も認識している。

GCSCでは、サイバー衛生の普及を通じた基本的なサイバーセキュリティの防御がインターネットの責任ある利用と有益な成長にとって必要不可欠になっていると考えている。セキュリティは、適切な説明責任を確保するために自動化した報告や情報共有などの仕組みが整備され、全ての関係者の間で責任が分散されている継続的なプロセスと見なされなければならない。

また、委員会は世界中の多くの社会が情報通信技術の利用に関して大きな課題に直面していることを認識し、この規範の効果拡大に向けて、基本的なサイバー衛生体制を効果的に実施するためのプロセスを確立するために知識を共有し、キャパシティ・ビルディングを提供するよう各国に呼び掛けている。

58　例えば欧州電気通信標準化機構（ETSI）、非営利団体であるインターネット・セキュリティ・センター（CIS）、オーストラリア信号局（ASD）などによる基準などが挙げられる。

8. 非国家主体による攻撃的なサイバー作戦に対する規範

規範：
非国家主体は攻撃的なサイバー活動に従事してはならず、国家行為主体はそのような活動を防止し、発生した場合には対応すべきである。

背景

情報通信技術は社会を良き方向へと変革させてきたと同時に、新たな安全保障上の課題ももたらしている。サイバー作戦のスピードと普遍性は、国家の司法制度や国際法の執行に関する協力において多大な困難をもたらしていることが多い。これらの困難にもかかわらず、国家の主権は規則に基づいた平和と安全保障の国際システムの礎である点を思い出すべきである。国家は国際法によって厳密に拘束されている合法的な武力行使の権限を独占してきた。非国家主体（主に民間企業）の中には国境を越えて攻撃的なサイバー作戦を実施する権利を支持する者もおり、サイバーの脅威から自身を十分に保護する能力を国家が持っていないため必要な防衛行動であると主張する可能性がある。このような非国家主体による攻撃的なサイバー作戦は防衛目的で行われるため、いわゆる「ハックバック」も含め、婉曲的に「攻撃的サイバー防衛」[59] などと呼ばれることもある。

サイバースペースの安定性とセキュリティに影響を与えるリスクがあるにもかかわらず、国によってはこのような活動を管理していないか、積極的に無視している場合もある。しかし、多くの国ではそのような活動は不法行為となり、さらには犯罪として扱われる場合もあるが、その一方でそのような活動の禁止も明示的な承認も行っていないように見える国家もある。しかしながら、一部の国家では非国家主体による攻撃的なサイバー活動を正当化することを検討している。実際に、非国家主体による攻撃的な活動を許可する国内法を可決または提案している国もある。

GCSCでは、これらの慣行がサイバースペースの安定性を損なわせるものであると考えている。これらの行為は深刻な混乱と損害を第三者にまでもたらす可能性があり、そのため複雑な法的紛争の引き金となって紛争をエスカレートさせる恐れもある。国家が自らの目的または第三者の目的のために攻撃的な作戦を敢行する許可を非国家主体に対して明示的に与えたり故意に許可したりした場合、危険な前例を創り出すとともに国際法の違反というリスクも負うことになる。委員会は、攻撃的な措置は国家のみに留保されるべきであると考えており、国際法は、サイバー作戦にも適用される敵対的行為に対する国家の対応について、厳格かつ排他的な枠組みを確立している点を想起している。同様に、国際法の下では、国家を代表して行動する非国家主体は国家の代理人と見なされなければならず、したがって国家の延長線上にあると捉えられる[60]。

国家がそのような行為を許可した場合は国際法の下で責任を問われる可能性がある[61]。国家は非国家主体による攻撃的なサイバー活動を防ぐために、国内的にも国際的にも行動しなければならない。

59 「積極的なサイバー防衛」は被害者のネットワーク上での自衛から攻撃者のネットワーク上での破壊活動に至るまでの一連の措置として理解されるべきである。この連続体における攻撃的なサイバー活動は、防衛側の意図（攻撃か防衛か）やその行為の法的資格とは無関係に防衛側が自分のネットワーク外で行動することを意味している。攻撃的なサイバー活動と積極的なサイバー防衛の定義についてはさらなる取り組みが必要である。

60 国際法における本件の広範な取り扱いについては、次のURLより「追記」を参照のこと：https://cybersta-bility.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Of-fensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

61 Id.

補足資料C：
GCSCの歴史・目標・プロセス

2017年2月のミュンヘン・セキュリティ会議においてオランダ王国外務省のBert Koenders大臣による後援の下で発足して以来、「サイバースペースの安定性に関するグローバル委員会」は、サイバースペースの安定性に特化した最初のマルチステークホルダーによるイニシアチブの1つとして考えられている。元アメリカ合衆国国務長官のMichael Chertoff氏と元インド国家安全保障副顧問のLatha Reddy氏が委員長を務め、その前には欧州議会議員で元エストニア外務大臣のMarina Kaljurand氏が委員長を務めた本委員会は、世界の異なる地域出身で国際的なサイバーセキュリティに関連した様々なバックグラウンドを持つ28人の著名な人物で構成されている[62]。また、本委員会は特別アドバイザー、ハーグ戦略研究所とイーストウェスト研究所によって構成される事務局、研究アドバイザリーグループ、さらにオランダ王国およびフランス共和国の外務省、シンガポールのサイバーセキュリティ庁、マイクロソフト、インターネットソサエティ、アフィリアスなどの数々のパートナーやスポンサーによって支援されている。

同委員会は「インターネット・ガバナンスに関する世界委員会」を含む過去の市民社会による委員会の活動を継続し、「サイバー空間に関する国際会議（GCCS）」の活動につなげたいという思いから生まれた。2015年、ハーグ戦略研究センター（HCSS）は、国際平和と安全保障に特化したGCCSのハーグ会議の準備セッションの開催を依頼された。その後のGCCS宣言の多くは準備会合による成果を直接反映したものであり、国際的なサイバーセキュリティ問題を議論するためのマルチステークホルダー形式の必要性を明確に示していた。それに伴い、HCSSは支援者と資金提供者（当初はマイクロソフト、インターネットソサエティ、オランダ王国外務省）によって構成されるコアグループを招集し、戦略計画を策定した。2016年8月、事務局のパートナーとしてイーストウェスト研究所（EWI）が参画することになり、HCSSはハーバード・ケネディスクールでGCSCインセプション・グループの会議を招集し、GCSCの運営・メンバー・構造・目標とミッション・ステートメントの両方に関する主な要件を起草した。

ミッション・ステートメントは以下の通りである。

> サイバースペースの安定性に関するグローバル委員会（GCSC）は国際的な安全保障と安定性を強化し、サイバースペースにおける国家と非国家の責任ある行動を道行くための規範と政策の提案を策定する。GCSCは共通の理解を深めるためにあらゆる利害関係者を巻き込み、その取り組みは研究、情報交換、キャパシティ・ビルディングを支援することでサイバースタビリティを向上させる。

GCSCはその発足当初から一般的に「国際的なサイバーセキュリティ」と呼ばれるサイバースペースに関連する国際的な平和と安全保障のアジェンダに影響を与えることを目的としていた。インセプション・

62　4頁に記載している委員の一覧を参照。

グループは、現在進行中の国際的なサイバーセキュリティの議論において、特にインターネット・ガバナンスや技術に関するコミュニティからの多様な意見を募る必要性を認識した。その目的は軍備管理や平和安全保障に関するコミュニティにおける審議に参考となる情報を提供することであり、特に規範に関する優れた成果の多くは、こうした市民社会や民間部門の行為主体によるインプットと受け入れが不足しているために妨げられていると考えられた。したがってマルチステークホルダーによるアプローチは思想の問題ではなく実践的なアプローチであると見なされた。

GCSCは「ボトムアップからトップダウンへ」という形で審議を行っている。第一に、メンバーが表明し、他の場所では扱われていない、最も明白であり緊急の国際的なサイバーセキュリティのニーズを満たす運用規範を特定した。第二に、これらの既存の規範から、サイバースタビリティの作業定義とその基礎となる原則を推定した。第三に、その定義を満たすために国際的な平和とセキュリティのアーキテクチャが何をすべきかをより明確に理解するために、安定性の枠組みを策定した。最後に、これをどのようにして達成するかについて国家および非国家主体に向けた勧告を作成した。

これらの目標に向けた委員会の審議は、地理的な境界線や利害関係者グループの垣根を越えて行われた。委員会は当初から、幅広い利害関係者からの意見が得られるよう、関連する会議の余白で会議を開催することに重点を置いていた[63]。また、研究や広範なコミュニティを通じて積極的にインプットを求めた。GCSCの活動をより広範な学界と結びつけるために、200人以上の専門家を登録したメールリストの管理を担当する委員長と4人の副委員長[64] を擁する研究アドバイザリーグループを発足させた。また、本グループは広範な研究プログラムの基礎にもなり、最終的に世界中の研究機関や個人から20件以上もの研究を委託された[65]。これらの研究の大半は専用の「サイバースタビリティ・ヒアリング」において委員会のメンバーに対して直接プレゼンテーションを行った。

本報告書の公表と過去に発行された規範の前に、委員会では政府、市民社会、業界の利害関係者など幅広い範囲で 一貫して意見を求めてきた。委員会の任期全体に納品期を分散させることで、外部者の意見やコメントを常に求めることが可能となった。GCSCの規範とサイバースタビリティの定義についてはオンラインでの協議依頼を出した。世界中の関係者から23件以上の提出があり、委員会の審議に情報を提供した。さらに、委員会は70以上の会議やイベントに積極的に参加し、円卓会議、サイドイベント、サイバースタビリティに関する専用のヒアリングを幅広い範囲の国家や非国家の利害関係者とともに開催した。

最後に、各委員らもそれぞれのコミュニティとの活発な連携を維持した。これらのグループからのインプットとフィードバックはより広い範囲での国家と非国家の専門家のコミュニティとの相互作用の基盤となり、今後の報告書の提唱に向けた基礎を形成する。

63　委員会の正式な会合は以下のイベントで召集された。2017ミュンヘン・セキュリティ会議（ドイツ・ミュンヘン）、CyCon（エストニア・タリン）、BlackHat USA（アメリカ合衆国・ラスベガス）、サイバー空間に関する国際会議（インド・ニューデリー）、2018 FIC International Cybersecurity Forum（フランス・リール）、2018ミュンヘン・セキュリティ会議（ドイツ・ミュンヘン – 授与）、GLOBSEC（スロバキア・ブラティスラヴァ）、 イスラエル・サイバーウィーク（イスラエル・テルアビブ – 授与）、シンガポール国際サイバーウィーク（シンガポール）、パリ平和フォーラム&インターネットガバナンスフォーラム（フランス・パリ – 授与）、2019 国連軍縮研究所（スイス・ジュネーヴ）、ICANN 64 コミュニティーフォーラム（日本・神戸市）、EuroDIG（オランダ・ハーグ）、GFCE年次会合（エチオピア・アディスアベバ）。

64　国際平和と安全保障、国際法、インターネット・ガバナンス、及び技術といった四つのテーマ領域をカバー。

65　「謝辞」節を参照。

謝辞

サイバースペースの安定性に関するグローバル委員会（GCSC）はスポンサー、研究アドバイザリーグループ、論文執筆者、査読者、補助職員など、委員会の活動を支援、貢献、促進してくださった多くの機関や個人の方々に御礼申し上げます。以下に、委員会の成功に貢献してくださった方々のほんの一部を紹介致します。

事務局

ハーグ戦略研究所（HCSS）

Alexander Klimburg, Director, サイバースペースの安定性に関するグローバル委員会イニシアチブおよび事務局長
Louk Faesen, サイバースペースの安定性に関するグローバル委員会事務局プロジェクトマネージャー
Elliot Mayhew, サイバースペースの安定性に関するグローバル委員会事務局プロジェクトアシスタント

以下の方々から追加の支援を受けています。**Timon Domela Nieuwenhuis Nyegaard**, **Koen van den Dool**, **Niels Renssen**, **Kaja Karlson.**

イーストウェスト研究所（EWI）

Bruce W. McConnell、サイバースペースの安定性に関するグローバル委員会共同事務局長
Anneleen Roggeman、サイバースペースの安定性に関するグローバル委員会事務局プロジェクトマネージャー

以下の方々から追加の支援を受けています。
Abagail Lawson、**Dragan Stojanovski**、**Conrad Jarzebowski**。

パートナー・スポンサー・支援機関

ハーグ戦略研究所、イーストウェスト研究所、および委員会は、ご支援いただいた以下の組織を認識し、感謝の意を表します。

パートナー：

- **オランダ王国外務省**、**Timo Koster**と**Dimitri Vogelaar**
- **マイクロソフト**、**Jan Neutze**と**Kaja Ciglic**
- **シンガポール政府サイバーセキュリティ庁**、**David Koh**と**Sithuraj Ponraj**
- **インターネットソサエティ（ISOC）**
- **フランス共和国外務省**、**Henry Verdier**と**David Martinon**
- **アフィリアス**、**Ram Mohan**と**Philipp Grabensee**

スポンサー

- **スイス連邦外務省**
- **GLOBSEC**
- **エストニア共和国外務省**
- **日本総務省**

支援機関

- **アフリカ連合委員会**
- **ブラックハットUSA**
- **DEF CON**
- **国際連合在ジュネーブ欧州連合代表部**
- **サイバー専門的知識に関するグローバルフォーラム**
- **グーグル**
- **ハーグ基礎自治体**
- **パケット・クリアリング・ハウス**
- **テルアビブ大学**
- **国連軍縮研究所**

これらの組織や機関は、サイバースペースの安定性に直面しているいくつかの喫緊の課題について議論を推進し、創造的な解決策を提示することに尽力しています。

研究者

委員会は、GCSCと幅広い学界とをつなぐ200人以上のオンラインメンバーからなる研究アドバイザリーグループのメンバーに感謝の意を表したい。特に、委員会の審議に情報を提供するためのブリーフィングやメモの作成を依頼した研究者の皆様に感謝します。

GCSC問題摘要1（2017月11月）

Alex Grigsby、元外交問題評議会議員（CFR）
Deborah Housen-Couriel、コンフィダス・デジタル
Joanna Kulesza、ウッチ大学、**Rolf H. Weber**、チューリッヒ大学
Oluwafemi Osho、**Joseph A. Ojeniyi**、**Shafi'I M. Abdulhamid**、連邦工科大学ミンナ校
Analía Aspis、ブエノスアイレス大学、**Robert Morgus**元ニュー・アメリカ、**Max Smeets**、元スタンフォード大学国際安全保障協力センター、**Trey Herr**、ハーバード・ケネディスクール
Arun Mohan Sukumar、**Madhulika Srikumar**、**Bedavyasa Mohanty**、オブザーバー研究財団（ORF）

GCSC問題摘要2（2018年5月）

Shen Yi、**Jiang Tianjiao**、**Wang Lei**、復旦大学サイバースペース・ガバナンス研究センター
Elana Broitman、**Mailyn Fidler**、**Robert Morgus**、元ニュー・アメリカ所属
Elonnai Hickokと**Arindrajit Basu**、インターネット・社会センター
Thomas Uren、**Bart Hogeveen**、**Fergus Hanson**、オーストラリア戦略政策研究所（ASPI）
Dragan Mladenovićと**Vladimir Radunović**、ディプロ財団
Thomas Reinhold、ハンブルグ大学平和研究・安全保障政策研究所

コンサルテーション

本委員会は、「シンガポール規範パッケージに関する協議依頼」（2018年12月17日から2019年1月17日まで）及び「サイバースペースの安定性の定義」（2019年8月14日から2019年9月6日まで）に対して、以下の個人・団体から広範なコメントを提出していただきましたことに感謝いたします。

Hussein Abul-Enein、アクセス・パートナーシップ
Kayode Akanni、デザインIT
Jonathan D. Aronson、南カリフォルニア大学（USC）
Aviram Atzaba、イスラエル国家サイバー総局
Arindrajit Basu、**Gurshabad Grover**、**Elonnai Hickok**と**Karan Saini**、インターネット・社会センター
Vytautas Butrimas、NATOエネルギー安全保障センター
サイバーセキュリティ・テック・アコード
Michael Daniel、サイバー脅威アライアンス
グローバル・パートナーズ・デジタル
Arvind Guptaと**Dickey Kumar**、ヴィヴェカナンダ国際財団
Tara Hairstonと**Anastasiya Kazakova**、カスパースキー
Sven Herpig、Stiftung Neue Verantwortung（SNV）
Drew Mitnick、アクセス・ナウ
George M. Moore、ジェームズ・マーティン不拡散研究センター
Brett van Niekerkと**Trishana Ramluckan**、ワズール・ナタール大学
Peter Swire、**Justin Hemmings**、**Sreenidhi Srinivasan**、ジョージア工科大学シェラー・カレッジ・オブ・ビジネス
Johan de Wit、シーメンス/デルフト工科大学

最後に、それぞれの研究と専門性を通じて本委員会を導き審議の参考となってくださった以下の専門家に感謝の意を表します。

Dennis Broeders、ライデン大学
Deborah Brownと**Verónica Ferrari**、進歩的コミュニケーション協会
Michael Daniel、サイバー脅威アライアンス
François Delerue、Institut de Recherche Stratégique de l'École Militaire – IRSEM
Akhil Deoおよび**Arun Mohan Sukumar**、オブザーバー研究財団（ORF）
Martha Finnemore、ジョージ・ワシントン大学
Aude Géry、ルーアン大学
Duncan Hollis、テンプル大学法科大学院
Joanna Kulesza、ウッチ大学
Peter Rowland、パケット・クリアリング・ハウス
Michael Schmitt、エクセター大学法科大学院

Patra Kongsirimongkolchai / EyeEm / ゲッティ イメージズ

事務局

The Hague Centre for Strategic Studies

EastWest INSTITUTE

パートナー

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

スポンサー

スイス連邦外務省

GLOBSEC

エストニア共和国外務省

日本総務省

支援機関

アフリカ連合委員会

ブラックハットUSA

DEF CON

国際連合在ジュネーブ欧州連合代表部

サイバー専門的知識に関するグローバルフォーラム

グーグル

ハーグ基礎自治体

パケット・クリアリング・ハウス

テルアビブ大学

国連軍縮研究所

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE